Citrix Application Delivery Management-Service

Machine translated content

Disclaimer

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

Contents

Übersicht

April 28, 2021

Citrix Application Delivery Management (früher NetScaler Management and Analytics Service) ist eine webbasierte Lösung zur Verwaltung aller Citrix Bereitstellungen, die Citrix ADC MPX, Citrix ADC VPX, Citrix ADC SDX, Citrix ADC CPX, Citrix ADC BLX, Citrix Gateway, Citrix Secure Web Gateway und Citrix SD-WAN umfassen. -Appliances, die lokal oder in der Cloud bereitgestellt werden.

Mit dieser Cloud-Lösung können Sie die gesamte globale Anwendungsbereitstellungsinfrastruktur über eine einzige, einheitliche und zentrale cloudbasierte Konsole verwalten, überwachen und beheben. Citrix Application Delivery Management (ADM) bietet alle Funktionen, die zum schnellen Einrichten, Bereitstellen und Verwalten der Anwendungsbereitstellung in Citrix ADC Bereitstellungen erforderlich sind, sowie umfassende Analysen zu Anwendungsstatus, Leistung und Sicherheit.

Citrix ADM bietet die folgenden Vorteile:

- **Agilität** — Einfach zu bedienen, zu aktualisieren und zu verwenden. Das Dienstmodell von Citrix ADM ist über die Cloud verfügbar, sodass die Funktionen von Citrix ADM einfach zu bedienen, zu aktualisieren und zu nutzen sind. Die Häufigkeit von Updates in Kombination mit der automatischen Update-Funktion verbessert die Citrix ADC Bereitstellung schnell.
- **Schnellere Wertschöpfung** — schnellere Erreichung von Geschäftszielen. Anders als bei der herkömmlichen lokalen Bereitstellung können Sie Ihren Citrix ADM Dienst mit wenigen Klicks verwenden. Sie sparen nicht nur die Installations- und Konfigurationszeit, sondern vermeiden auch Zeit- und Ressourcenverschwendung für potenzielle Fehler.
- **Multi-Site-Management** — Ein einzelner Fensterbereich für Instanzen in Rechenzentren mit mehreren Standorten. Mit dem Citrix ADM können Sie Citrix ADCs verwalten und überwachen, die sich in verschiedenen Bereitstellungstypen befinden. Sie haben One-Stop-Management für Citrix ADCs, die on-premises und in der Cloud bereitgestellt werden.
- **Betriebseffizienz** — Optimierte und automatisierte Methode zur Erzielung höherer Betriebsproduktivität. Mit dem Citrix ADM werden Ihre Betriebskosten gesenkt, indem Sie Zeit, Geld und Ressourcen für die Wartung und Aktualisierung der herkömmlichen Hardwarebereitstellungen sparen.

Funktionsweise von Citrix ADM

Citrix ADM ist als Dienst in der Citrix Cloud verfügbar. Nachdem Sie sich für Citrix Cloud registriert und den Dienst verwendet haben, installieren Sie Agenten in Ihrer Netzwerkumgebung oder initiieren Sie den integrierten Agenten in den Instanzen. Fügen Sie dann dem Dienst die Instanzen hinzu, die Sie verwalten möchten.

Ein Agent ermöglicht die Kommunikation zwischen Citrix ADM und den verwalteten Instanzen in Ihrem Rechenzentrum. Der Agent sammelt Daten von den verwalteten Instanzen in Ihrem Netzwerk und sendet sie an das Citrix ADM.

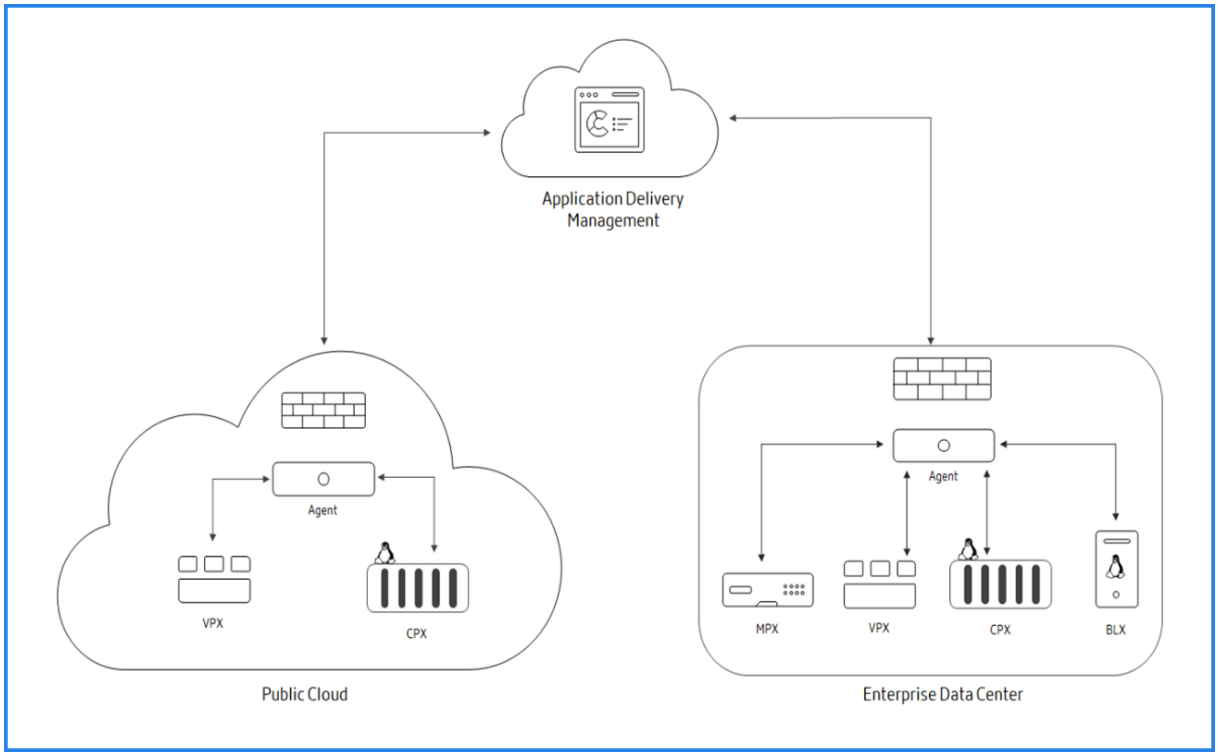
Wenn Sie Citrix ADM eine Instanz hinzufügen, fügt sie sich implizit als Trap-Ziel hinzu und sammelt die Bestandsaufnahme der Instanz.

Der Dienst sammelt Instanzdetails wie:

- Hostname
- Softwareversion
- Laufende und gespeicherte Konfiguration
- Zertifikate
- Entitäten, die für die Instanz konfiguriert sind, usw.

Citrix ADM fragt regelmäßig verwaltete Instanzen ab, um Informationen zu sammeln.

Die folgende Abbildung veranschaulicht die Kommunikation zwischen dem Dienst, Agenten und Instanzen:



Versionshinweise

April 28, 2021

Die Citrix Application Delivery Management (Citrix ADM) -Versionshinweise beschreiben die neuen Features, Verbesserungen an vorhandenen Features, behobenen Problemen und bekannten Problemen, die in einer Service-Version verfügbar sind.
Die Versionshinweise enthalten einen oder mehrere der folgenden Abschnitte:

- **Neue Features**: Die neuen Funktionen, Verbesserungen bestehender Funktionen und Fehlerbehebungen, die in der aktuellen Version verfügbar sind.
- **Bekannte Probleme**: Die Probleme, die in der aktuellen Version vorhanden sind, und ihre Problemumgehungen, wo immer zutreffend.
- **Vorherige Veröffentlichungen**: Die neuen Funktionen und Erweiterungen, die in den vorherigen Versionen veröffentlicht wurden.

Neue Features

April 28, 2021

In diesem Thema werden die neuen Features, Verbesserungen vorhandener Features und Korrekturen aufgeführt, die in einer Version verfügbar sind.

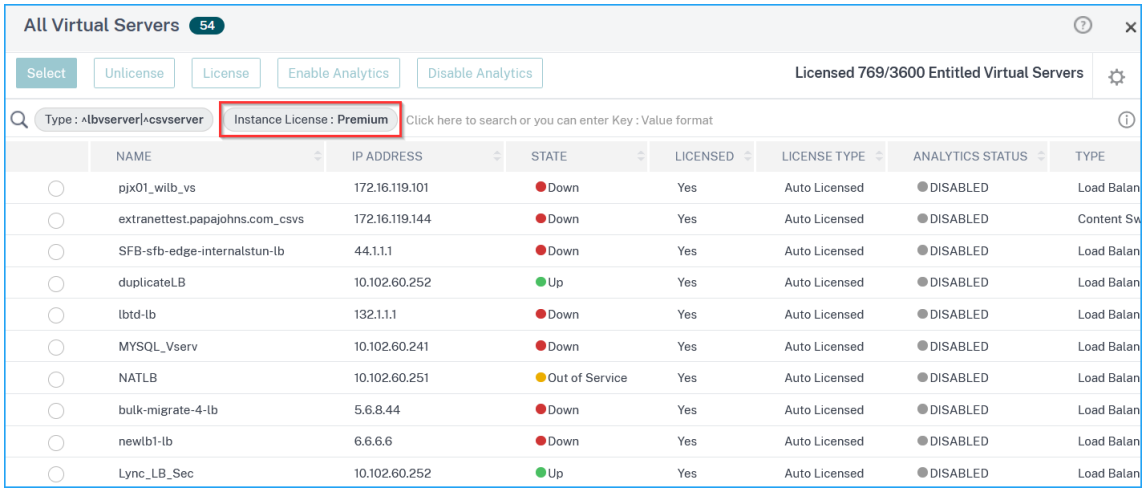
Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf den neuesten Build von Citrix ADM aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

17. April 2021

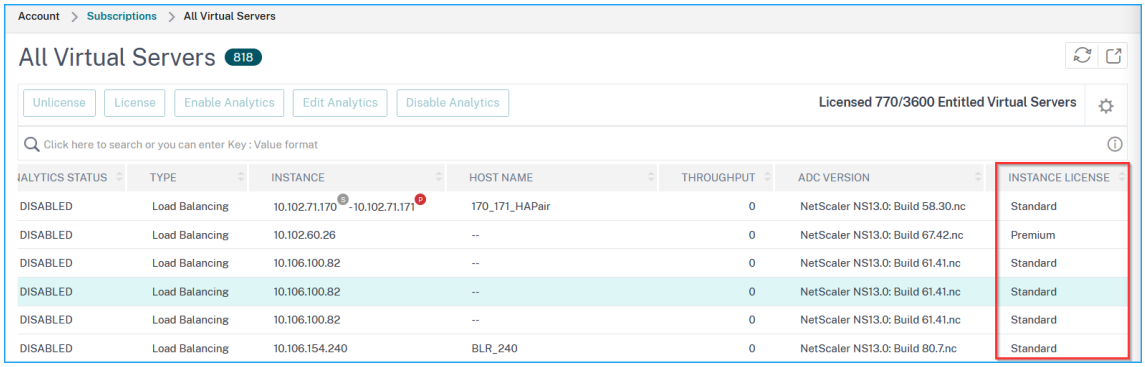
Verbesserungen bei Sicherheitsverstößen

In **Analytics > Sicherheit > Sicherheitsverletzungen**können Sie jetzt die folgenden Verbesserungen einsehen:

- Wenn Sie Analysen für **Kontoübernahme**, **Website-Scanning**und **Content-Scraping-Verstöße** aktivieren, werden **Advanced Security Analytics** und **Web Insight** Einstellungen ebenfalls automatisch aktiviert.
- Wenn Sie aus der Einstellungsoption die Anwendung auswählen, um die Voraussetzungseinstellungen für **Kontoübernahme**, **Website-Scanning**und **Content Scraping-Verstöße** zu konfigurieren, wird der Premium-Lizenzfilter angewendet. Diese Verbesserung ermöglicht es Ihnen, nur die Premium-lizenzierten Anwendungen anzuzeigen und auszuwählen.



- Über die Einstellungsoption können Sie **auf der Konfigurationsseite für die Voraussetzung für Website-Scanning und -Scraping** zuerst die **Sitzungsverfolgungsmethode** und dann die Anwendung auswählen.
- Auf der Seite **Alle virtuellen Server** unter **Konto > Abonnements** wird die Option **Instanzlizenz** angezeigt, mit der Sie den Lizenztyp der Instanz analysieren können.



[NSADM-68058]

Sicherheitsverstöße im App Dashboard anzeigen

In **Analytics > Sicherheit > Sicherheitsverstöße > Anwendungsübersicht**sind die Verstoßdetails, die Sie für WAF und Bot anzeigen konnten, jetzt auch im **Anwendungs-Dashboard**verfügbar. Navigieren Sie zu **Anwendungen > Dashboard**, wählen Sie eine Anwendung aus und klicken Sie auf die Registerkarte **Sicherheit**, um die für die ausgewählte Anwendung geltenden WAF- und Bot-Verstöße anzuzeigen.

Neben der Sichtbarkeit der Anwendungsleistung und -nutzung ermöglicht Ihnen diese Verbesserung auch, die Verstoßdetails in einer Einzelbereichsansicht zu visualisieren.

[NSADM-66876]

Der Farbcode der IP-Adresse ändert sich dynamisch, um den Instanzstatus anzuzeigen

In der ADM-GUI ändern sich unter **Netzwerk > Instanzen > Citrix ADC**in der Spalte IP-Adresse die Farbcodes für IP-Adressmarken dynamisch, um den Instanzstatus anzuzeigen. Wenn sich beispielsweise eine bestimmte primäre Instanz im Status “oben” befindet, ändert sich der Farbcode für die kreisförmige P-Marke für die entsprechende IP-Adresse in Grün. Sie können auch den Mauszeiger über die kreisförmige Markierung bewegen, um den Instanzstatus zu überprüfen. Zuvor waren die Farbcodes für IP-Adressen statisch: Blau für Primär- und Grau für Sekundär.

[NSADM-67681]

Problem behoben

Bei SSL-Zertifikaten zeigt die ADM-GUI den Ausstellertyp als “Nicht empfohlen” an, selbst wenn die Zertifikate in den **SSL-Dashboard-Einstellungen** konfiguriert sind.

[NSHELP-26123]

30. März 2021

Bot Insight - Log-Nachricht für Bot-Management anzeigen

Wenn Sie in **Analytics > Sicherheit > Sicherheitsverstöße > Anwendungsübersicht**unter **Bot**eine Anwendung auswählen und auf **Protokolle** klicken, um Bot-Details anzuzeigen, können Sie jetzt die

Bot-Kategorie anzeigen, die als Signatur und Signatur-ID identifiziert wurde. Mit der Signatur-ID können Sie analysieren, ob der erkannte Bot ein guter Bot oder ein schlechter Bot ist. Für jede andere Bot-Kategorie zeigt die Signatur-ID N/A an.

Weitere Informationen zur Signaturkategorie und ID finden Sie unter Update der Bot-S.

[NSADM-63099]

App-Sicherheitsverletzung - Bot

In **Analytics > Sicherheit > Sicherheitsverstöße > Alle Verstöße**können Sie jetzt die dynamische Bot-Erkennung von Tastatureingaben und Maus unter der Kategorie BOT-Verstoß anzeigen. Weitere Informationen finden Sie unter Verletzung der App-Sicherheit.

[NSADM-61855]

Behobene Probleme

- In Infrastructure Analytics wird der UI-Begriff “Paket verworfen” für SSL-Verstoßindikatoren (PE-CPU-Limit, PPS-Limit, Durchsatzlimit, SSL-Durchsatzlimit, SSL-TPS-Limit) jetzt in “Verstöße gegen das Zinslimit” geändert.

  [NSADM-69007]

- Das von ADM generierte Tech-Support-Bundle kann nicht entpackt werden.

  [NSHELP-26726]

17. März 2021

Schützen Sie Ihr Unternehmen mit Security Advisory

Citrix ADM Security Advisory hilft Ihnen, ADC-Instanzen zu identifizieren, die von Citrix Common Vulnerabilities and Exposures (CVEs) betroffen sind, und geeignete Korrekturen anzuwenden. Der Ratgeber hebt Citrix CVEs hervor, um Ihre ADC-Instanzen zu gefährden, und empfiehlt Abgrenzungen und Korrekturen. Sie können die Empfehlungen überprüfen und geeignete Maßnahmen ergreifen, indem Sie den ADM-Service verwenden, um die Gegenmaßnahmen und Behebungen anzuwenden.

Im Folgenden sind die Sicherheitsberatungsfunktionen aufgeführt:

- Scan: enthält den standardmäßigen Systemscan und den Scannen auf Anforderung.
  - Systemscan: scannt alle verwalteten Instanzen standardmäßig einmal pro Woche. ADM entscheidet über Datum und Uhrzeit von Systemscans, und Sie können diese nicht ändern.
  - Anforderungsscan: ermöglicht es Ihnen, die Instanzen bei Bedarf manuell zu scannen. Wenn die nach dem letzten Systemscan verstrichene Zeit erheblich ist, können Sie den

Anforderungs-Scan ausführen, um die aktuelle Sicherheitslage zu beurteilen. Oder scannen Sie, nachdem eine Behebung oder Minderung durchgeführt wurde, um die überarbeitete Haltung zu beurteilen.

- CVE-Wirkungsanalyse: zeigt Ergebnisse aller CVEs, die sich auf Ihre Infrastruktur auswirken, und alle ADC-Instanzen, die betroffen sind, und schlägt eine Abhilfe und Minderung vor. Verwenden Sie diese Informationen, um Minderung und Abhilfe zu beantragen, um Sicherheitsrisiken zu beheben.
- CVE berichtet: speichert Kopien der letzten fünf Scans. Sie können diese Berichte herunterladen und analysieren.
- CVE-Repository: gibt einen detaillierten Überblick über alle ADC-bezogenen CVEs, die Citrix seit Dezember 2019 angekündigt hat und die Auswirkungen auf Ihre ADC-Infrastruktur haben könnten. Sie können diese Ansicht verwenden, um die CVEs im Bereich Security Advisory zu verstehen und mehr über den CVE zu erfahren.

Weitere Informationen finden Sie unter Sicherheits-Advisory.

[NSADM-69280]

Neue Funktionen zum Citrix Low-Touch-Onboarding-Workflow hinzugefügt

Der neue Citrix Low-Touch-Onboarding-Workflow verfügt über eine verbesserte GUI mit mehreren neuen Funktionen und einer besseren Benutzererfahrung. Zwei neue Registerkarten, Security Advisory und Upgrade Advisory, werden eingeführt. Citrix ADM Security Advisory informiert Sie über Schwachstellen, die Ihre ADC-Instanzen gefährden, und empfiehlt Abgrenzungen und Abhilfemaßnahmen. Sie können den Upgrade Advisory verwenden, um ADC-Instanzen zu überprüfen, die sich am Ende des Lebenszyklus (EOL) oder in älteren Versionen nähern. Wir können diese ADCs auf die neuesten Releases upgraden und von den neuesten Verbesserungen und Korrekturen profitieren. Um mehr zu erfahren, siehe Berührungsarmes Onboarding von Citrix ADC-Instanzen mit Citrix ADM Service Connect.

[NSADM-69280]

Überwachen des ADC-Instanz-Lebenszyklus mithilfe von Citrix ADM Upgrade-Advisory

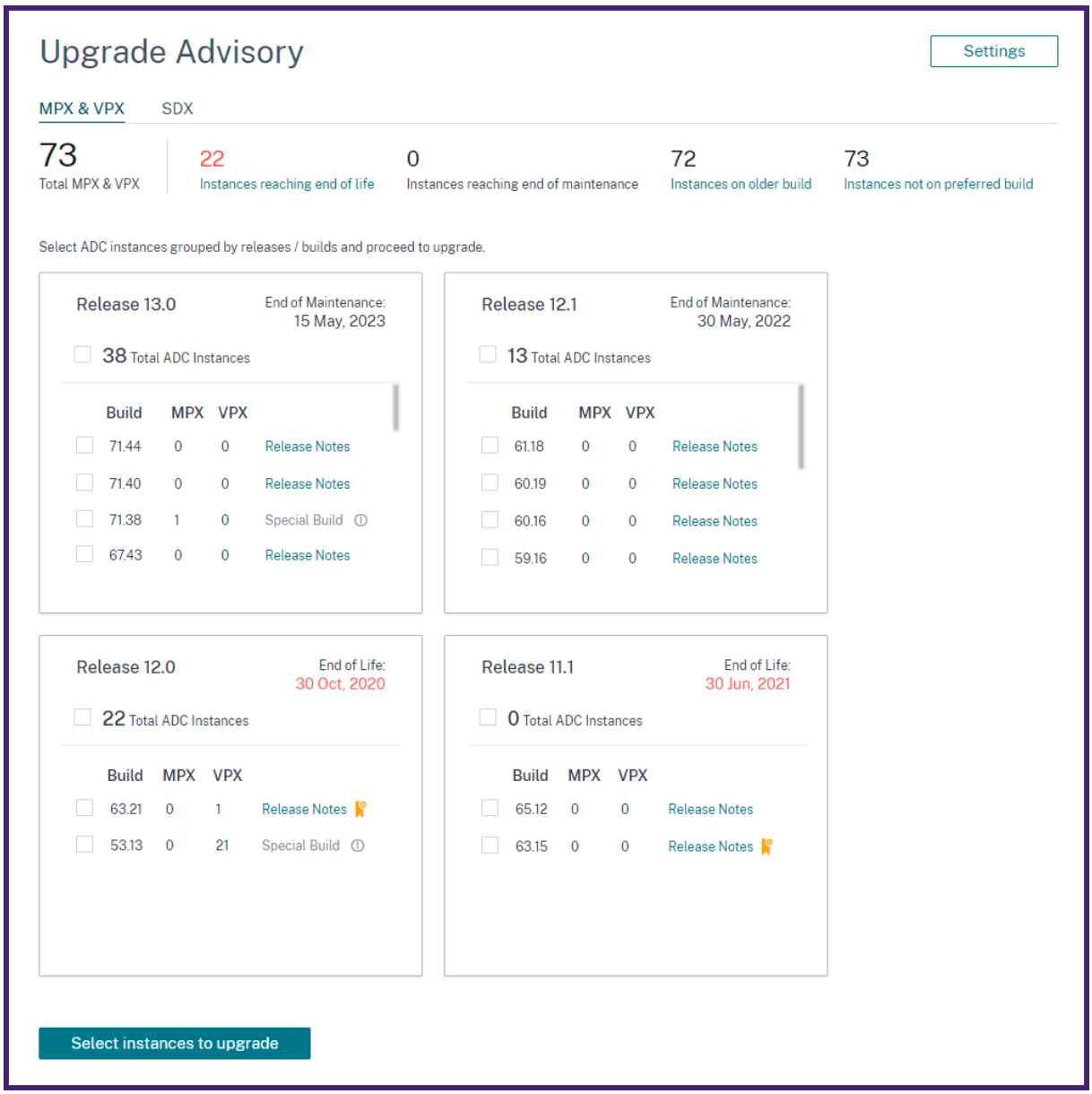
Citrix ADM Upgrade-Advisory hilft Ihnen, den Lebenszyklus Ihrer ADC-Instanzen zu überwachen. Als Netzwerkadministrator verwalten Sie möglicherweise viele Instanzen, die auf verschiedenen ADC-Versionen in Citrix ADM ausgeführt werden. Die Überwachung des Lebenszyklus jeder ADC-Instanz kann eine umständliche Aufgabe sein. Um diesen Prozess zu vereinfachen, bietet ADM upgrade Advisory die folgenden Informationen:

- Identifiziert Instanzen, die EOL oder EOM erreichen oder erreicht haben. Sie können also ADC-Upgrades vor dem EOL- oder EOM-Datum planen.

- Hebt die Instanzen hervor, die nicht auf der neuesten Version oder dem neuesten Build Sie können diese Instanzen auf die neueste Version oder Build upgraden, um von neuen Funktionen und Fehlerbehebungen zu profitieren.
- Hebt die Instanzen hervor, die sich nicht auf bevorzugten ADC-Builds befinden. Einige Organisationen haben möglicherweise bevorzugte ADC-Builds für ihre Instanzen. In ADM können Sie den bevorzugten Build für Ihre Organisation abhängig von Funktionen, behobenen Problemen und anderen Überlegungen festlegen. Überprüfen und aktualisieren Sie dann die Instanzen, die nicht auf bevorzugten Builds sind. Instanzen, auf denen die bevorzugten Builds ausgeführt werden, sind mit einem Sternsymbol gekennzeichnet.
- Hebt Instanzen hervor, die in den beliebtesten Versionen oder Builds ausgeführt werden. Instanzen, auf denen die beliebten Builds ausgeführt werden, werden durch ein Ribbon-Symbol gekennzeichnet

Nachdem Sie die oben genannten Punkte überprüft haben, können Sie auf der Seite Upgrade-Advisory einen Wartungsauftrag erstellen, um ADC-Instanzen zu aktualisieren.

> **Wichtig**
>
> Upgrade-Advisory überwacht nur EOM oder EOL von ADC-Softwareversionen. Es überprüft nicht die EOL von ADC-Hardware-Appliances.



Weitere Informationen finden Sie unter Upgrade-Beratung.

[NSADM-56646]

Analysieren Sie die Ursache für die Langsamkeit der Anwendung

Anwendungsverlangsamung ist ein wichtiges Anliegen für jede Organisation, da dies zu geschäftlichen Auswirkungen oder Produktivität führt. In **Applications > Web Insight**können Sie jetzt eine neue Metrik, Anwendungen mit Antwortzeitanomalien, anzeigen. Mithilfe dieser Metrik können Sie als Administrator analysieren, ob die Langsamkeit der Anwendung aus folgenden Gründen resultiert:

- Latenz des Client-Netzwerks

- Servernetzwerklatenz
- Serververarbeitungszeit

Weitere Informationen finden Sie unter Analysieren Sie die Ursache für die Langsamkeit der Anwendung.

[NSADM-63170]

3. März 2021

Entdecken Sie API-Endpunkte in ADM

Sie können jetzt die API-Endpunkte, die sich in Ihrem Unternehmen befinden, mithilfe des API-Gateways ermitteln. In Citrix ADM werden auf der Seite **Anwendungen > API Gateway > API Discovery** die API-Endpunkte angezeigt, die Teil von ADC-Instanzen und API-Bereitstellungen sind.

Wenn Sie in API Discovery einen virtuellen Server oder eine API-Bereitstellung auswählen, zeigt die ADM-GUI die API-Endpunkte und ihre Details an, wie zum Beispiel:

- **Methode** - Es zeigt die Methode an, die in einem API-Endpunkt verwendet wird. Zum Beispiel GET und POST Methoden
- **Gesamtzahl der Anforderungen** - Es zeigt die Anzahl der API-Anfragen auf dem API-Endpunkt an.
- **Antwortstatus** - Es zeigt die Anzahl für jeden Antwortstatus an. Zum Beispiel, 2xx3xx, 4xx, und 5xx.
- **In Spec gefunden** - Diese Spalte wird nur für API-Bereitstellungen angezeigt. Manchmal erhalten die internen APIs, die nicht Teil der API-Definition sind, Verkehr von außen. Diese Spalte hilft Ihnen festzustellen, ob der API-Endpunkt und die beobachtete Methode Teil der API-Definition sind.

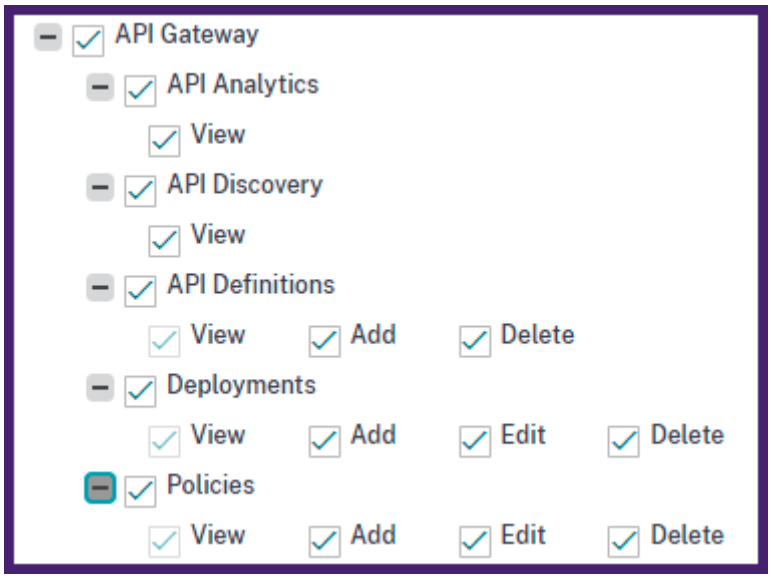
Virtuelle Server:

API-Bereitstellungen:

[NSAPISEC-1234]

Erteilen von API-Gateway-Konfigurations- und Verwaltungsberechtigungen

Als Administrator können Sie eine Zugriffsrichtlinie erstellen, um Benutzerberechtigungen für die Konfiguration und Verwaltung des API-Gateways zu erteilen. Die Benutzerberechtigungen können Anzeigen, Hinzufügen, Bearbeiten und Löschen sein. Navigieren Sie dazu zu **Konto > Benutzeradministration > Zugriffsrichtlinien**.



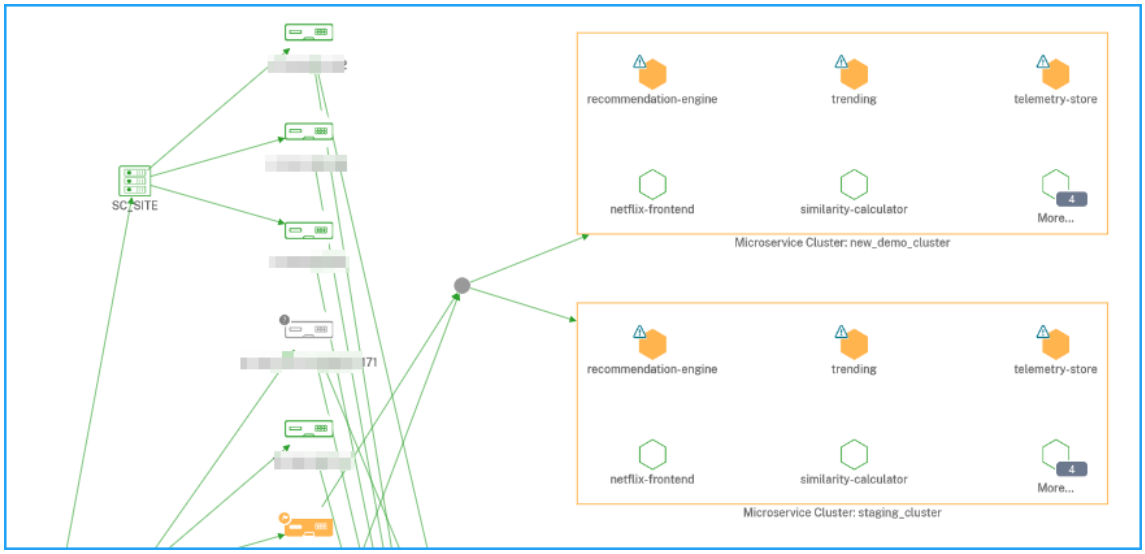
[NSADM-63097]

Verbesserungen des globalen Service-Graphen

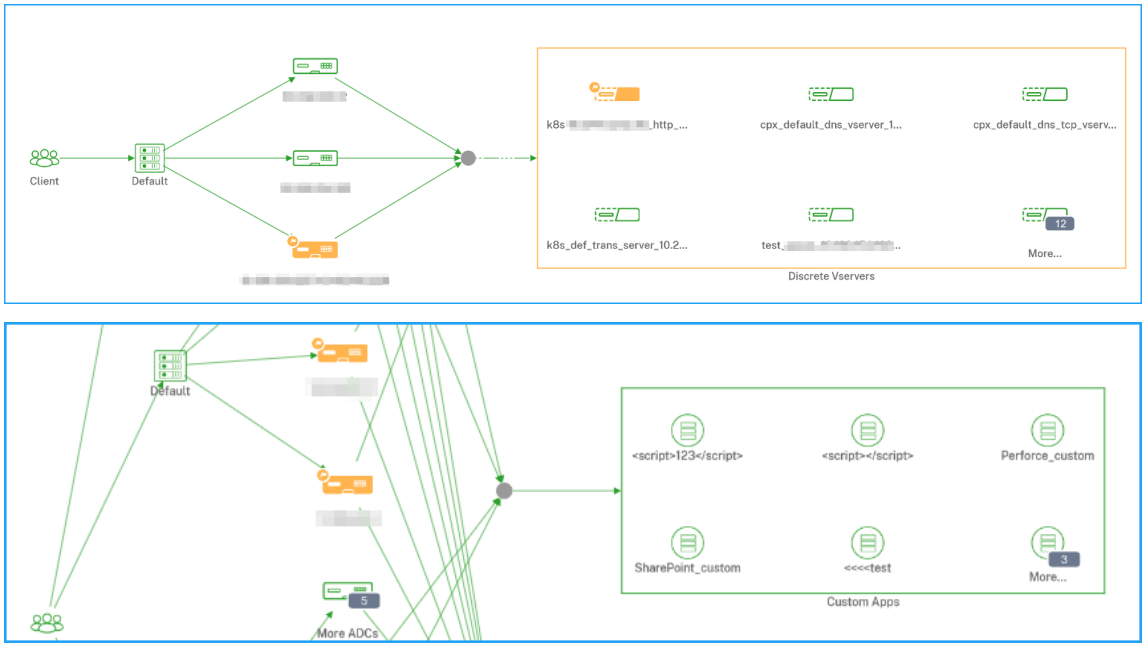
In **Anwendungen > Service Graph > Global**können Sie jetzt Folgendes anzeigen:

- Die Microservices basieren auf dem Clusternamen.

  > **Hinweis**
  >
  > Sie können Microservices für nur drei Cluster anzeigen.



- Die erweiterte Ansicht der diskreten virtuellen Server und benutzerdefinierten Apps



Venafi Integration in Citrix ADM

Um die digitale Sicherheit aufrechtzuerhalten, müssen Sie die Verwaltung von SSL-Zertifikaten in Ihrer Umgebung automatisieren. Abgelaufene SSL-Zertifikate können zu Sicherheitsrisiken führen. Jetzt können Sie die Server der Venafi Trust Protection Platform so konfigurieren, dass sie SSL-Zertifikate über die ADM-Dienst-GUI verwalten.

Mit der Integration von Venafi können Sie Zertifikate neu ausstellen und die Erneuerung von auf den ADC-Instanzen installierten Zertifikaten über die ADM-Dienst-GUI automatisieren. Weitere Informationen finden Sie unter Automatisieren Sie die SSL-Zertifikatsverwaltung.

[NSADM-58047]

Behobene Probleme

- Wenn Sie einen Job in **Networks > Configuration Jobs** erstellen und die Ausführungshäufigkeit als bestimmten Tag einer Woche oder das Datum eines Monats auswählen, wird der geplante Job nicht nach der angegebenen Zeit ausgeführt.

  [NSHELP-26034]

- ADM kann sich nicht ohne DNS-Server registrieren oder aktualisieren, wenn ein Proxy-Server aktiviert ist und der Agent seine IP-Adresse nicht abrufen kann.

  [NSHELP-25835]

- Für Nicht-Admin-Benutzer dauert es mehr als eine Minute, bis die Daten von GSLB unter **Netzwerke > Netzwerkfunktionen > GSLB** in der ADM-GUI angezeigt werden.

  [NSHELP-25740]

- Sie erhalten E-Mail-Benachrichtigungen zu Lizenzpool-Schwellenwerten, auch wenn diese nicht konfiguriert sind.

  [NSHELP-25723]

- Wenn Sie in **Gateway Insight**einen Bericht planen (**Berichte exportieren > Export planen**), zeigt der generierte Bericht **Seite nicht gefunden**an.

  [NSHELP-25496]

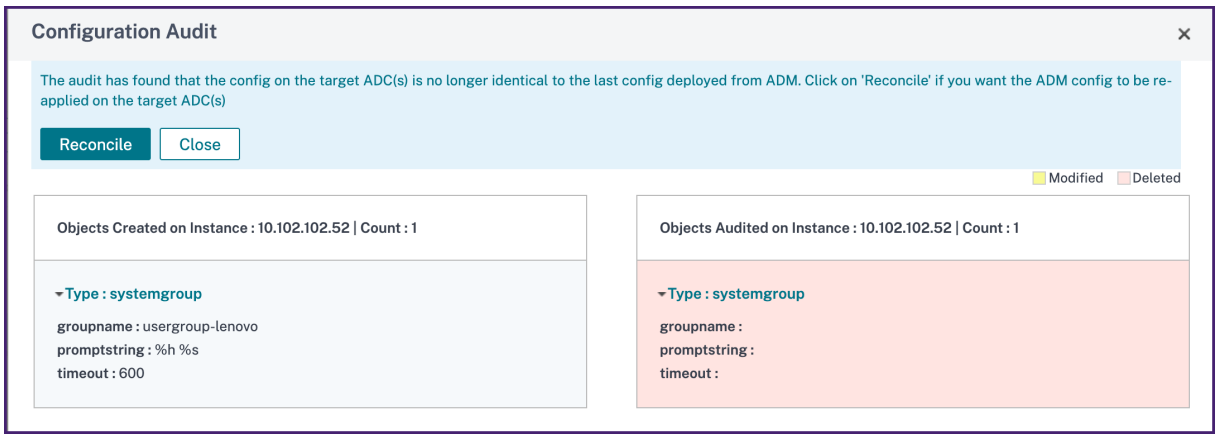
- Manchmal zeigt die ADM-GUI keine Instanzlizenzen an.

  [NSADM-67697]

11. Februar 2021

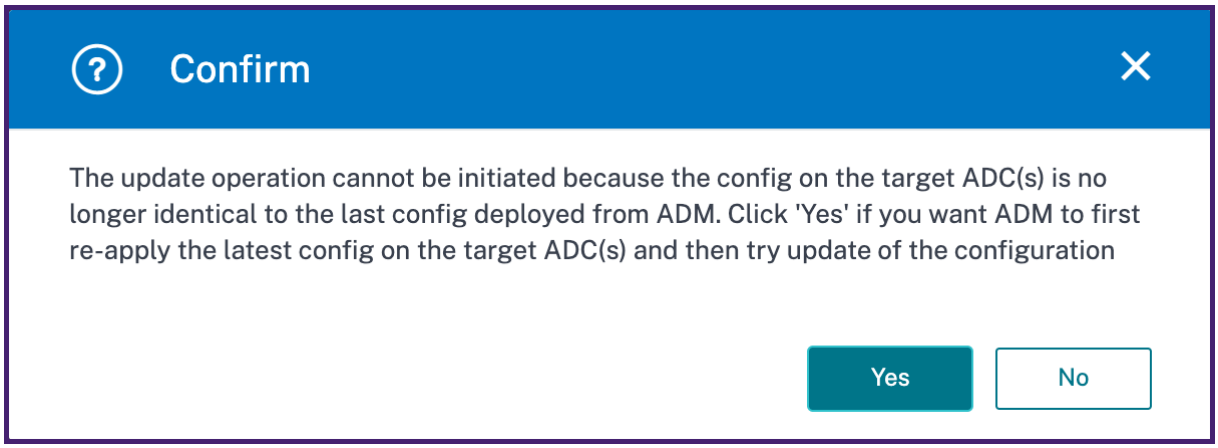
Stimmen Sie Ihre StyleBook-Konfiguration ab

Wenn Sie die ADC-Konfiguration mit dem StyleBook-Konfigurationspaket prüfen, können Sie jetzt alle auf der ADC-Instanz erkannten Änderungen oder Abweichungen in Einklang bringen. Diese Aktion stellt die ADC-Konfiguration wieder her, die mit der Version des Konfigurationspakets auf ADM übereinstimmt.



Bedenken Sie, dass Sie ein Objekt in der ADC-Instanz mithilfe der StyleBook-Konfiguration erstellt haben. Wenn dieses Objekt aus der ADC-Instanz gelöscht wird, identifiziert die Seite " **Konfigurationsprüfung** " die Änderung und ermöglicht es Ihnen, sie abzugleichen. Die Aktion **Abgleichen stellt** das gelöschte Objekt auf der ADC-Instanz wieder her, wie im Konfigurationspaket definiert.

Wenn während der Aktualisierung des Konfigurationspakets festgestellte Änderungen oder Abweichungen vorgenommen wurden, wird eine Bestätigungsmeldung angezeigt, um die Änderungen abzugleichen.



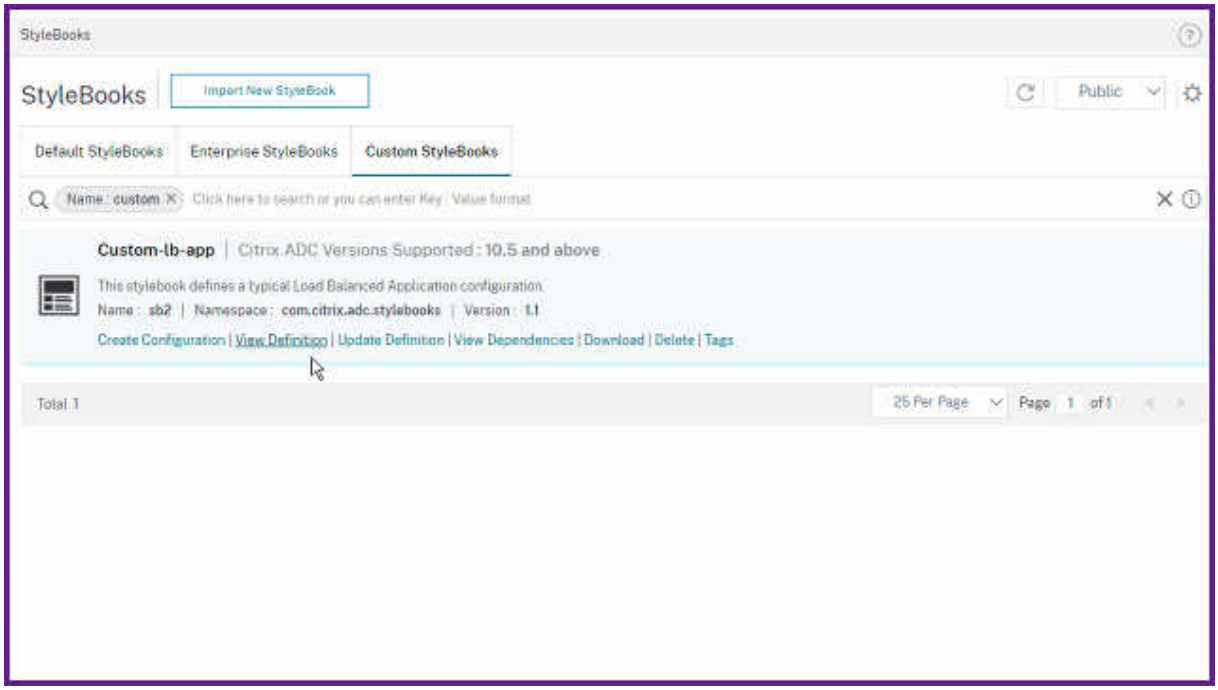
[NSADM-62742]

Aktualisieren von benutzerdefinierten StyleBook-Definitionen in der GUI

Sie können jetzt eine benutzerdefinierte StyleBook-Definition über die ADM-GUI selbst aktualisieren.

> **Hinweis**
>
> Bevor Sie die StyleBook-Definition von der ADM-GUI aus aktualisieren, stellen Sie Folgendes sicher:
>
> - Die StyleBook-Definition hat keine abhängigen StyleBooks.

- Aus der StyleBook-Definition wurden keine Konfigurationspakete erstellt.



Früher mussten Sie Folgendes tun:

1. Laden Sie das StyleBook herunter
2. Lösche es aus ADM.
3. Aktualisieren Sie die Definition offline.
4. Importieren Sie es zurück in ADM.

Mit dieser Funktion können Sie die Definition aktualisieren.

[NSADM-67726]

Neuer Datentyp und integrierte IP-Funktionen für die StyleBook-Definition

Die ADM StyleBooks unterstützen jetzt den `ipnetwork` Datentyp, um neue IP-Funktionen zu ermöglichen. Dieser Datentyp besteht aus zwei Teilen. Der erste Teil ist die IP-Adresse und der zweite Teil ist die Netzmaske.

Die Netzmaske wird mit einer Netzmaskenlänge (`netmask-len`) oder einer Netzmaske (`netmask_ip`) dargestellt. Die Netzmaskenlänge ist eine Ganzzahl zwischen 0-32 und 0-128 für eine IPv6-Adresse. Es wird verwendet, um die Anzahl der IP-Adressen in einem Netzwerk zu bestimmen.

Im Folgenden sind die neuen integrierten IP-Funktionen aufgeführt:

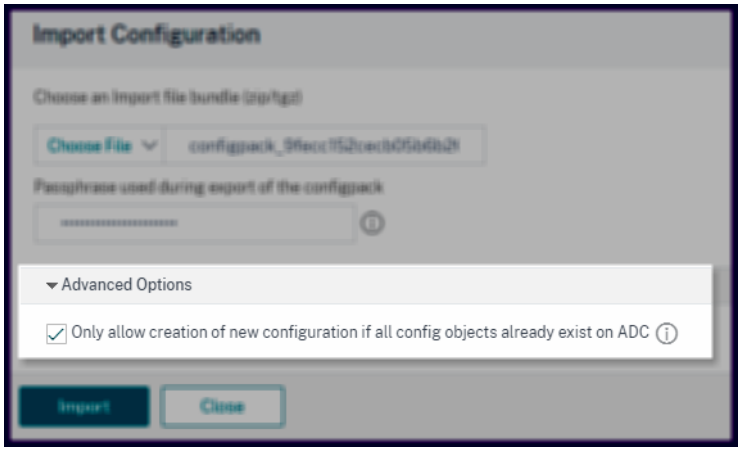
- `ip_network()`: Gibt eine IP-Netzwerknotation zurück, wenn sie die IP-Adresse und die Netzmaskenlänge als Eingabe erhält.
- `network_ip()`: Gibt die erste IP-Adresse des angegebenen IP-Netzwerks zurück.

- `subnets()`: Gibt die Liste der Subnetze des angegebenen IP-Netzwerks und der Netzmaskenlänge zurück.
- `netmask_ip()`: Gibt die Netmask-IP-Adresse für das angegebene IP-Netzwerk zurück.
- `broadcast_ip()`: Gibt die Broadcast-IP-Adresse für das angegebene IP-Netzwerk zurück.
- `cidr()`: Gibt eine CIDR-Notation für das angegebene IP-Netzwerk zurück.
- `is_cidr()`: Diese Funktion akzeptiert einen `ipnetwork` Wert. Und es gibt zurück, `True` ob der angegebene Wert mit der CIDR-Notation des IP-Netzwerks übereinstimmt.
- `is_in_network()`: Diese Funktion akzeptiert `ipnetwork` und `ipaddress` wertet. Und es gibt zurück, `True` ob die angegebene IP-Adresse im angegebenen IP-Netzwerk vorhanden ist.

[NSADM-56083]

Einführung einer erweiterten Option beim Importieren einer StyleBook-Konfiguration

In **StyleBooks > Configurations**enthält die Option **Importkonfiguration** jetzt eine erweiterte Option. Diese Option ist nützlich, wenn Sie das Konfigurationspaket importieren, das bereits die Konfigurationsobjekte auf der ADC-Instanz enthält.



Bedenken Sie, dass dieselbe ADC-Instanz auf zwei ADM-Servern hinzugefügt wird. Und einer der ADM-Server hat ein Konfigurationspaket für diese ADC-Instanz bereitgestellt. Wenn Sie dieses Konfigurationspaket auf einen anderen Server (oder auf den ADM-Dienst) migrieren möchten, exportieren Sie es auf Ihren lokalen Computer. Verwenden Sie dann diese Option auf dem ADM-Server, auf den Sie das Konfigurationspaket importieren möchten. Diese Option wird importiert, ohne die Konfigurationsobjekte auf der ADC-Instanz erneut bereitzustellen.

[NSADM-62743]

Anzeigen von API-Analysen für den gesamten API-Verkehr

Auf der Seite **API Gateway > API Analytics** werden jetzt alle API-Anfragen und -Antworten angezeigt. Zuvor wurde auf dieser Seite nur der API-Verkehr angezeigt, der das Ratenlimit oder die Authen-

tifizierungsrichtlinie konfiguriert hat.

[NSADM-62936]

Verbesserungen des Service-Graphen

Im Microservices-Dienstdiagramm können Sie als Administrator jetzt Folgendes analysieren:

- Die Anzahl der Treffer zwischen den Services basierend auf der Kantenbreite.
- Die Gründe für die zu überprüfenden oder kritischen Dienste.

Service-Symbol	Beschreibung
	Die Kantenbreite gibt die Anzahl der Treffer an. Je größer oder mehr die Kantenbreite ist, gibt an, dass die Anzahl der Treffer höher ist.
	Der Dienst mit einem Warnsymbol zeigt an, dass der Dienst Fehler enthält.
	Der Dienst mit einem Stoppuhrsymbol zeigt an, dass der Dienst Latenz- oder Reaktionszeitprobleme aufweist.
	Der Dienst mit Stoppuhr- und Warnsymbolen weist darauf hin, dass der Dienst sowohl Fehler als auch Probleme mit Latenz-/Reaktionszeiten hat.

> **Hinweis**
>
> Wenn ein Dienst kein Warn- oder Stoppuhrsymbol hat, zeigt dies an, dass der Dienst Anomalien oder Schwellenwertverletzungen für Hits aufweist.

[NSADM-65798]

Behobene Probleme

- Wenn Sie in **Gateway Insight**einen Bericht planen (**Berichte exportieren > Export planen**), zeigt der generierte Bericht “Seite nicht gefunden” an.

  [NSHELP-25496]

- Während Sie eine ADC-Instanz in ADM hinzufügen und SNMP v2 als Citrix ADC-Profil auswählen, wird die ADM-IP-Adresse als SNMP-Manager hinzugefügt.

  [NSHELP-26245]

- In **Netzwerke > Konfigurationsjobs**wird der geplante Konfigurationsauftrag nicht gemäß der angegebenen Zeit ausgeführt, zu der die **Ausführungshäufigkeit** wie folgt festgelegt ist:
  - Bestimmter Tag einer Woche.
  - Spezifisches Datum eines Monats.

  [NSHELP-26034]

- ADM kann sich nicht ohne DNS-Server registrieren oder aktualisieren, wenn die folgenden Bedingungen erfüllt sind:
  - Ein Proxyserver ist aktiviert.
  - Der Agent erhält seine IP-Adresse nicht.

  [NSHELP-25835]

- Manchmal zeigt die ADM-GUI keine Instanzlizenzen an.

  [NSADM-67697]

29. Januar 2021

IPAM zeigt die Ressourcen der zugewiesenen IP-Adresse

Sie können jetzt weitere Details zu zugewiesenen IP-Adressen aus einem IPAM-Netzwerk anzeigen:

- **Modul**: Zeigt das ADM-Modul an, das die IP-Adresse reserviert hat. Wenn die IP-Adresse beispielsweise von StyleBooks reserviert ist, zeigt diese Spalte StyleBooks als Modul an.
- **Ressourcentyp**: Zeigt den Ressourcentyp in diesem Modul an. Für das StyleBooks-Modul verwendet nur der Konfigurations-Ressourcentyp das IPAM-Netzwerk. In dieser Spalte werden also Konfigurationen angezeigt.
- **Ressourcen-ID**: Zeigt die genaue Ressourcen-ID mit einem Link an. Klicken Sie auf diesen Link, um auf die Ressource zuzugreifen, die die IP-Adresse verwendet. Für den Konfigurations-Ressourcentyp wird die Konfigurationspack-ID als Ressourcen-ID angezeigt.

[NSADM-62751]

Behobene Probleme

Sie können eine Citrix ADC SDX-Instanz nicht aus Citrix ADM entfernen, wenn die Instanz als FQDN konfiguriert ist und einen Bindestrich (“-“) im Namen enthält.
[NSHELP-26022]

ADM kann sich nicht ohne DNS-Server registrieren oder aktualisieren, wenn ein Proxy-Server aktiviert ist und der Agent seine IP-Adresse nicht abrufen kann.
[NSHELP-25835]

13. Januar 2021

Servicegragramm — Wichtige Metriktrends für Services anzeigen

In Service Graph können Sie jetzt die tabellarische Ansicht verwenden, um Folgendes zu sehen:

- Die wichtigsten Kennzahlen für den Dienst
- Wichtige Metriken zwischen einem Quelldienst und einem Zieldienst

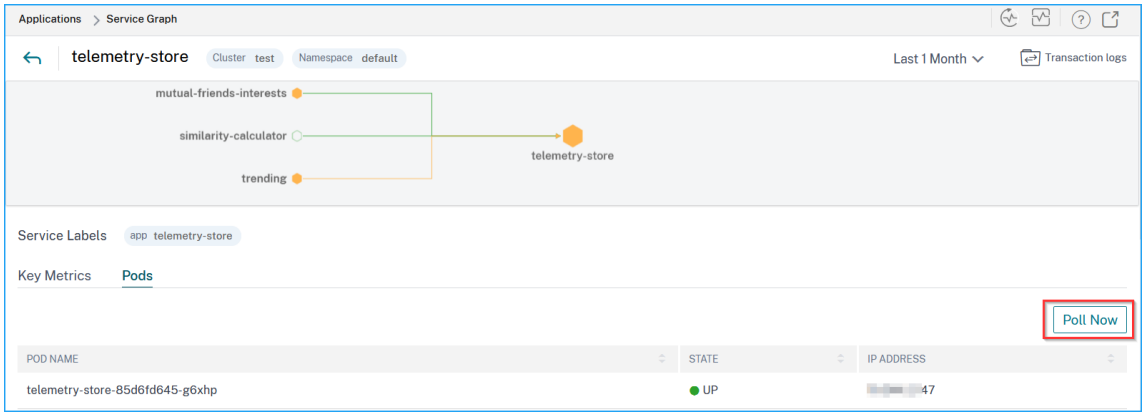
Als Administrator können Sie mithilfe dieser wichtigen Metriken die Trends der goldenen Signale für die ausgewählte Zeitdauer analysieren. Weitere Informationen finden Sie unter Service-Details anzeigen.

[NSADM-65163]

Servicediagramm - Verwenden Sie die Option “Jetzt abfragen”, um den Pod-Status zu ermitteln

In Service Graph können Sie jetzt die Option “Jetzt abfragen” verwenden, um den neuesten Pod-Status zu erhalten. Die Option “Jetzt abfragen” ruft den neuesten Podstatus vom Cluster ab.

1. Klicken Sie auf einen Knoten und wählen Sie **Details anzeigen**
2. Klicken Sie auf der Registerkarte **Pods** auf **Jetzt abfragen**



[NSADM-62963]

Neues StyleBook-Attribut zum Hinzufügen einer dynamischen Liste

In der **StyleBook-Definition** können Sie jetzt das `allow-new-values` Attribut hinzufügen, um eine dynamische Liste für einen Parameter hinzuzufügen. Wenn ein Benutzer dieses StyleBook auswählt, um eine Konfiguration zu erstellen, kann der Benutzer der Liste neue Werte hinzufügen.

Sie können die `allowed-values` Attribute `allow-new-values` und in einer Kombination verwenden. Diese Kombination ermöglicht es Ihnen, eine Liste gültiger Werte für einen Parameter zu definieren und neue Werte zu akzeptieren.

Beispiel:

```
-
      name: port
      type: tcp-port
      allowed-values:
            - 80
            - 81
            - 8080
      allow-new-values: true
<!--NeedCopy-->
```

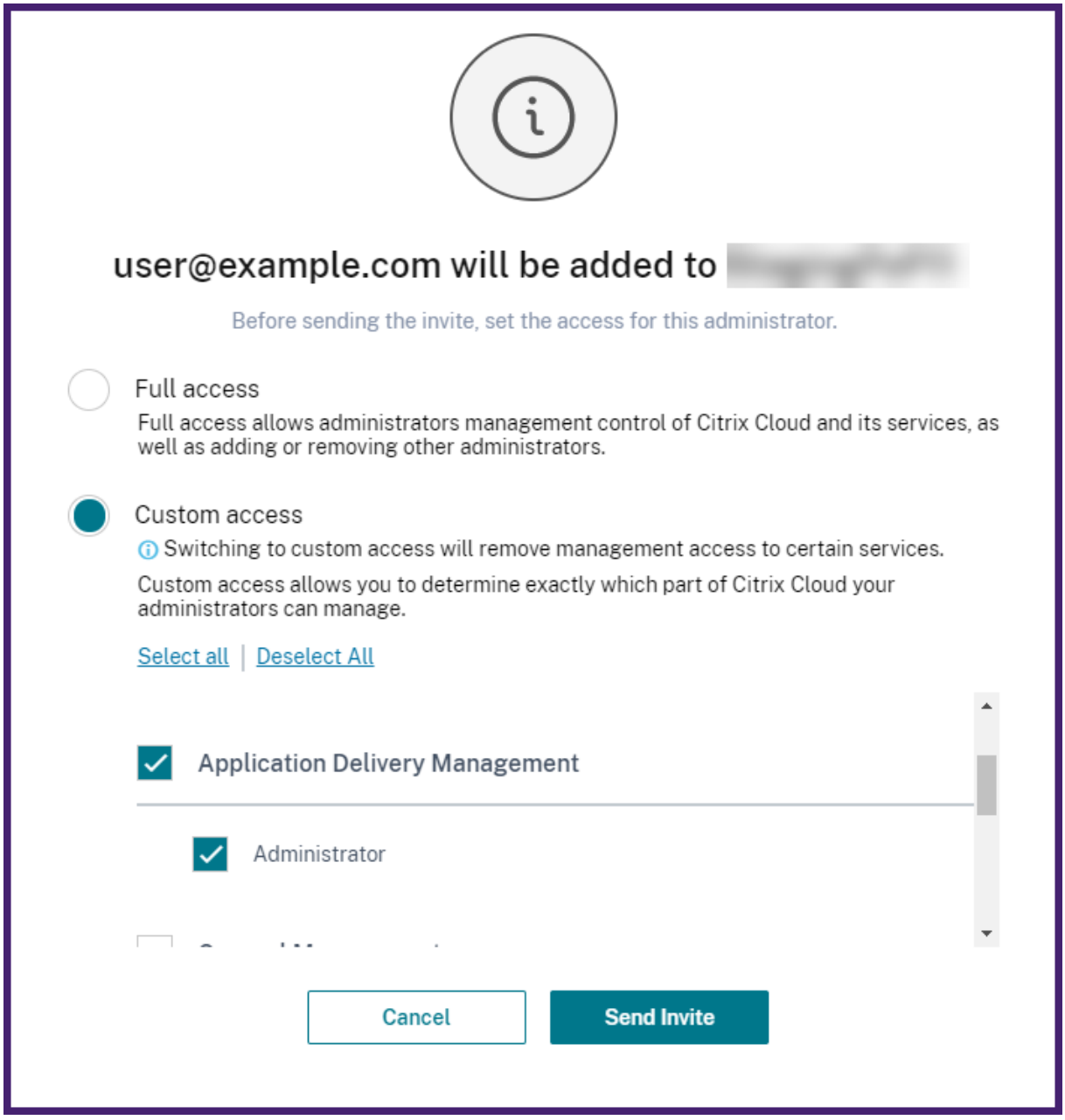
In diesem Beispiel kann ein Benutzer entweder aus 80, 81, 8080 auswählen oder beim Erstellen/Aktualisieren eines Konfigurationspakets einen neuen Wert für den Parameter-Port eingeben. Weitere Informationen finden Sie unter allow-new-Werte.

[NSADM-62749]

Laden Sie Benutzer mit einem benutzerdefinierten Zugriff auf den ADM-Dienst ein

Als Superadministrator können Sie jetzt neue Benutzer mit dem benutzerdefinierten Zugriff zur Verwendung des ADM-Dienstes einladen. Mit dieser Option können Sie den Benutzerzugriff nur auf den ADM-Dienst in Citrix Cloud einschränken. Zuvor konnten Sie Benutzer nicht dazu einladen, nur auf den ADM-Dienst zuzugreifen. Sie mussten also eine Einladung mit vollem Zugriff senden.

Um neue Benutzer in Citrix Cloud einzuladen, navigieren Sie zu **Identity Access Management > Administratoren**. Wählen Sie in der Option Benutzerdefinierter Zugriff die Option **Anwendungsbereitstellungsverwaltung**aus. Standardmäßig ist die **Administratorrolle** ausgewählt.



Der Einladungslink wird an die angegebene Benutzer-E-Mail-Adresse gesendet. Und der Benutzer

kann sich mit diesem Link als Administrator bei Citrix ADM anmelden. Bei einem administrativen Zugriff kann der Benutzer Folgendes tun:

- Fügen Sie ADC-Instanzen in ADM hinzu und verwalten Sie sie.
- Stellen Sie Konfigurationen auf ADC-Instanzen mit StyleBook bereit.
- Konfigurieren Sie gebündelte Kapazitätslizenzen für ADC-Instanzen.
- Erstellen und konfigurieren Sie Autoscale-Gruppen.

> **Hinweis**
>
> Der Administrator kann von Citrix Cloud aus auf die ADM-GUI zugreifen. Die Seite " **Konto > Benutzerverwaltung** " ist jedoch eingeschränkt. Ein Superadministrator kann bei Bedarf Zugriff auf diese Seite gewähren.

Weitere Informationen darüber, wie Sie eine Einladung senden und die Benutzer konfigurieren, finden Sie unter Konfigurieren von Benutzern auf Citrix ADM.

[NSADM-55384]

Behobene Probleme

- In Gateway Insight ist die Gesamtzahl, die unter Gateway angezeigt wird, falsch.

  [NSHELP-25729]

- Wenn Sie unter Konfigurationsquelle in **Netzwerken > Konfigurationsjobs > Job erstellen**die Option Aufnehmen und wiedergeben auswählen, wird die folgende Fehlermeldung angezeigt:

  ```
  Unable to get config diff for: <instance IP>
  ```

  [NSADM-63986]

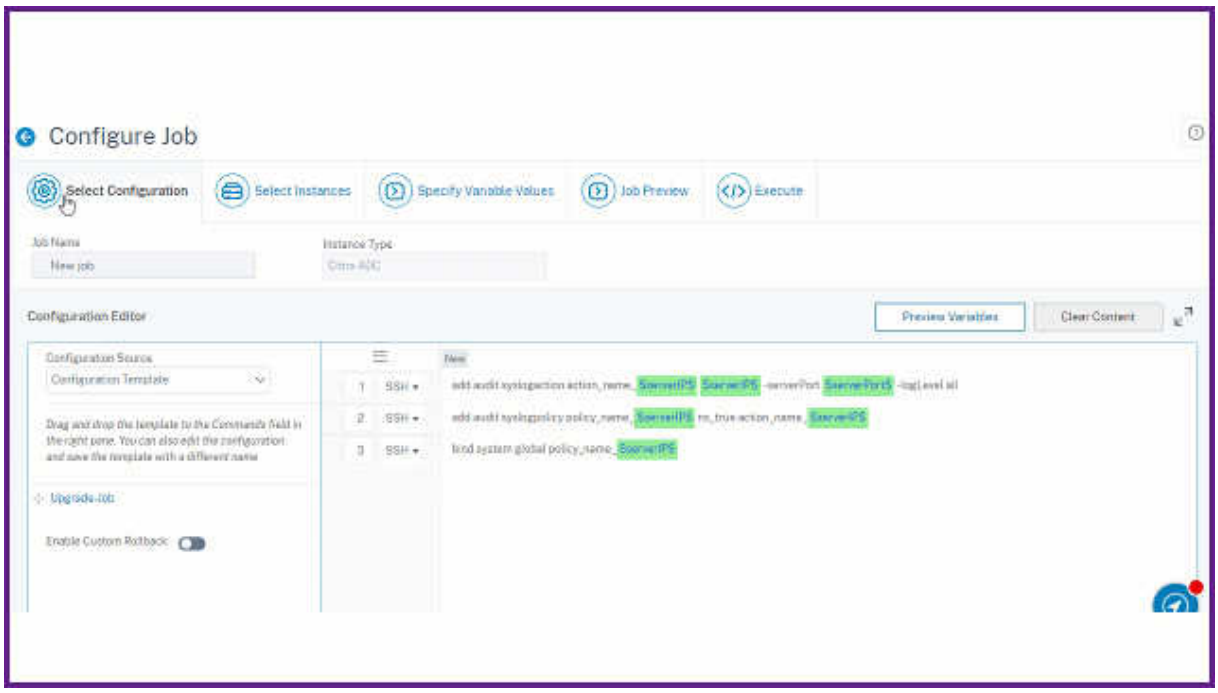
- Wenn Sie eine ungültige Regex in der Anwendung für eine Gruppe bereitstellen und einige Anwendungen manuell auswählen, sind die manuell ausgewählten Anwendungen nicht sichtbar, wenn der Regex ungültig ist.

  [NSHELP-25739]

17. Dezember 2020

Wechseln zwischen den Registerkarten eines bestehenden Konfigurationsauftrags

Wenn Sie einen vorhandenen Konfigurationsauftrag bearbeiten, können Sie jetzt zu einer beliebigen Registerkarte wechseln. Wenn Sie sich beispielsweise auf der Registerkarte **Konfiguration auswählen** befinden, können Sie auf die Registerkarte **Job-Vorschau** wechseln. Zuvor konnten Sie nur linear zum nächsten Tab gehen. Auf der Registerkarte " **Konfiguration auswählen** " konnten Sie beispielsweise nur zur Registerkarte " **Instanzen auswählen** " wechseln.

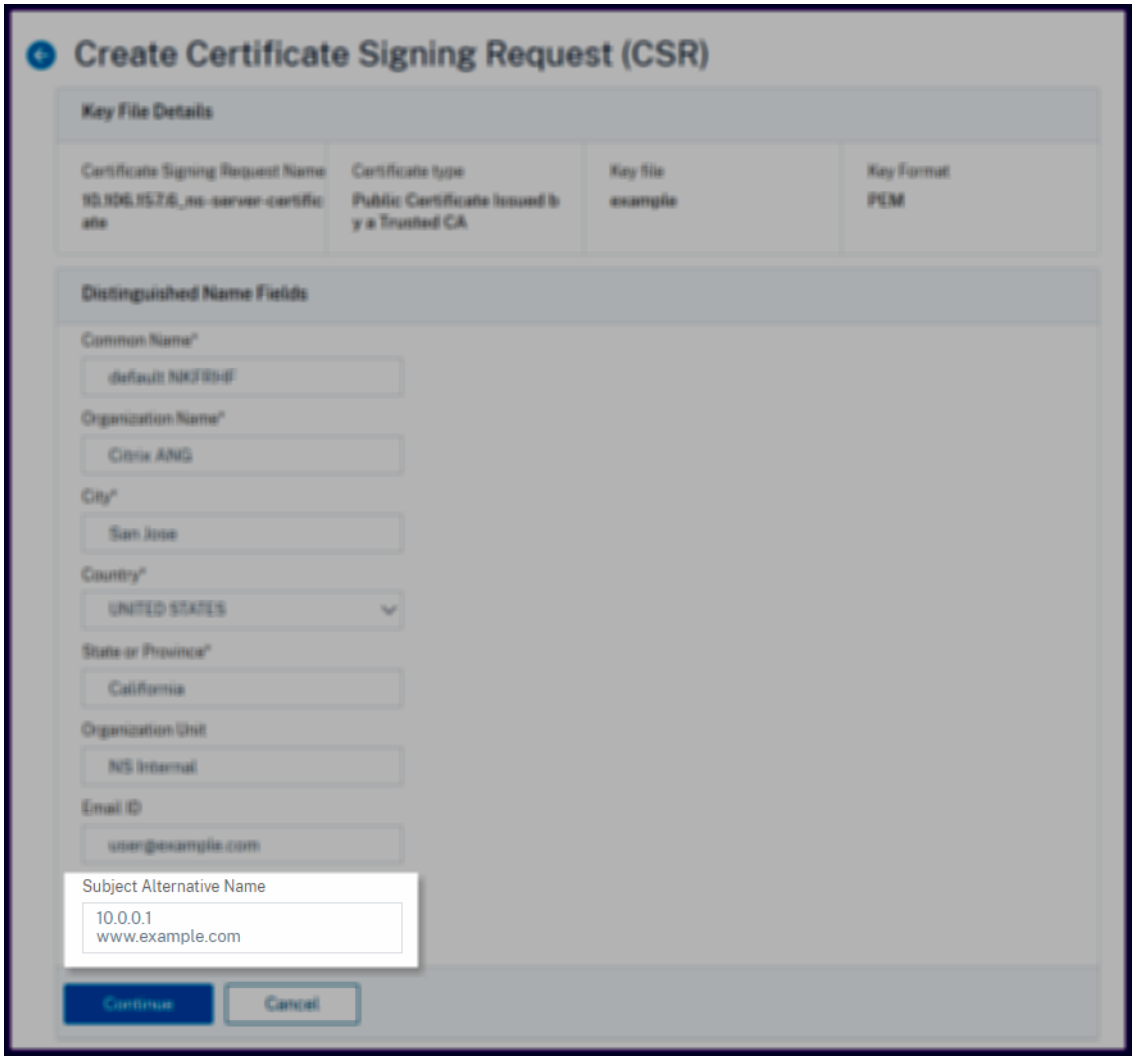


[NSADM-42944]

Erstellen Sie eine CSR mit alternativen Namen des Betreffs

Sie können jetzt eine Certificate Signing Request (CSR) mit alternativen Namen des Betreffs erstellen. Mit dieser Funktion können Sie mehrere Domains mit einem einzigen Zertifikat sichern.

Während einer CSR-Erstellung des ausgewählten SSL-Zertifikats können Sie jetzt mehrere alternative Antragstellernamen einschließen. Diese Werte können Domänennamen und IP-Adressen sein. Weitere Informationen finden Sie unter Erstellen einer Zertifikatsignieranforderung (CSR).



[NSADM-51556]

App-Sicherheitsverletzung - Bot

In Sicherheitsverletzungen können Sie jetzt die **Kontoübernahme für Citrix Gateway** unter der Kategorie Bot-Verstoß anzeigen. Weitere Informationen finden Sie unter Verstöße Kategorien.

[NSADM-57698]

Bot Insight - Bot-Kategorien für mobile (Android) Anwendungen anzeigen

In Bot Insight können Sie jetzt die folgenden Bot-Kategorien anzeigen, die über ein Mobilfunknetz erkannt werden:

- Preislimit für Web-Clients
- Android Rate Limit

- Webclient-Gerät
- Android-Gerät

Weitere Informationen finden Sie unter Bot Einblick.

[NSADM-57724]

Behobene Probleme

- Wenn Sie unter **Netzwerke > Ereignisse > Ereignisübersicht**auf ein beliebiges Citrix ADC SDX-bezogene Ereignis klicken, leitet die GUI auf die Ereignisseite um, zeigt jedoch keine Daten an.

  [NSHELP-25630]

- Der ADM-Dienst hat keine Zeitüberschreitung für den Ablauf von Anmeldesitzungen und die Abmelde-API. Infolgedessen bleibt die Benutzersitzung gültig.

  [NSADM-63819]

- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt.

  [NSADM-5882]

2. Dezember 2020

Anzeigen von Anomalien bei der Anwendungsnutzung

Als Administrator müssen Sie sicherstellen, wie die Anwendung genutzt wird. Die Kennzahlen für Anwendungsschlüssel können Ihnen helfen, die Anwendungsnutzung zu identifizieren. Da die Reichweite der Datenverkehrsreichweite für die Anwendung unvorhersehbar ist, können einige ungewöhnliche Abweichungen bei der Anwendungsleistung für eine bestimmte Dauer auftreten. In solchen Szenarien sollten Sie als Administrator solche plötzlichen Anomalien anzeigen und sicherstellen, dass eine sofortige Fehlerbehebung erforderlich ist.
Citrix ADM erkennt solche Anomalien und liefert notwendige Details.

Weitere Informationen finden Sie unter Anwendungsverwendung und Anomalien.

[NSADM-54677]

Wählen Sie die Empfindlichkeitsstufen für Sicherheits

Bei Verstößen gegen übermäßige Clientverbindungen und Website-Scans können Sie jetzt ein Profil für Verhaltensüberprüfungen erstellen und die Empfindlichkeitsstufe als Niedrig, Mittel und Hoch wählen. Durch das Erstellen eines Profils können Sie entscheiden, wie Citrix ADM die Gesamtzahl der Anomalien für diese Verstöße melden soll.

Weitere Informationen finden Sie unter Konfigurieren von Verhaltensüberprüfungs.

[NSADM-59536]

CPU-Auslastung der Anwendung zum Berechnen des App

Als Administrator können Sie jetzt die von einer Anwendung genutzte CPU überwachen. Sie können auch Schwellenwerte für die CPU-Auslastung der App konfigurieren, um den endgültigen App-Score zu bestimmen. Auf der Seite App-Score konfigurieren können Sie die **App-CPU-Auslastung** auswählen und die niedrigen und hohen Schwellenwerte konfigurieren.

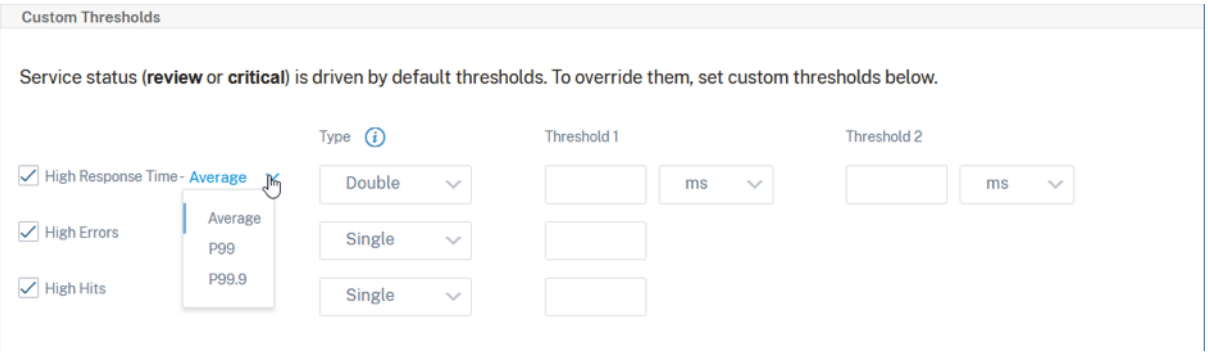
Weitere Informationen finden Sie unter durchschnittliche CPU-Auslastung der Anwendung und App-Score-Komponenten auswählen und Schwellenwerte festlegen.

[NSADM-57468]

Konfigurieren von Schwellenwerten im Dienstdiagramm

In Service Graph können Sie jetzt Schwellenwerte für die folgenden Metriken auswählen und konfigurieren, um den Servicebericht und den Status zu berechnen:

- Hohe Reaktionszeit (Durchschnitt, P99 und P99,9)
- Hohe Fehler
- Hohe Treffer



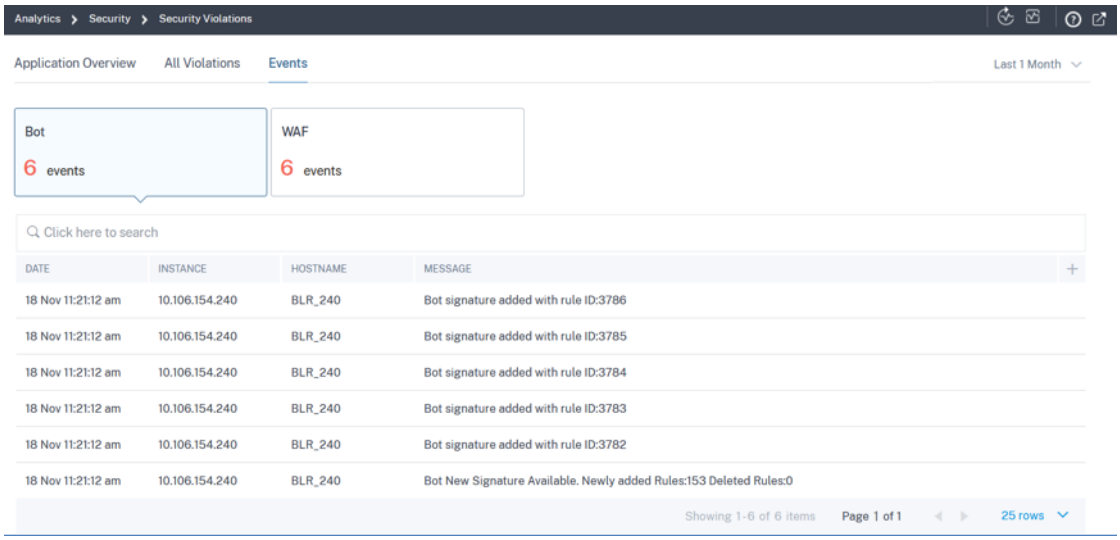
> **Hinweis**
>
> Citrix ADM berechnet den Endstand und den Status des Service basierend auf den ausgewählten Metriken. Wenn Sie beispielsweise nur High Hits für die Schwellenwertkonfiguration auswählen, verwendet Citrix ADM den Standardschwellenwert (Reaktionszeit = 200 ms und Fehleranzahl = 0) und hohe Treffer, um den Service Score zu berechnen.

Weitere Informationen finden Sie unter Konfigurieren von Schwellenwerten im Dienstdiagramm.

[NSADM-59731]

Anzeigen des Ereignisverlaufs in Sicherheitsverletzungen

Bei Sicherheitsverletzungen können Sie jetzt den Ereignisverlauf für Bot-Einblicke und Sicherheitseinblicke anzeigen. Navigieren Sie zu **Analytics > Sicherheit > Sicherheitsverletzungen** und klicken Sie auf die Registerkarte **Ereignisse**, um die Bot- und WAF-Ereignisse anzuzeigen.



[NSADM-62684]

Verbesserungen bei Infrastructure Analytics

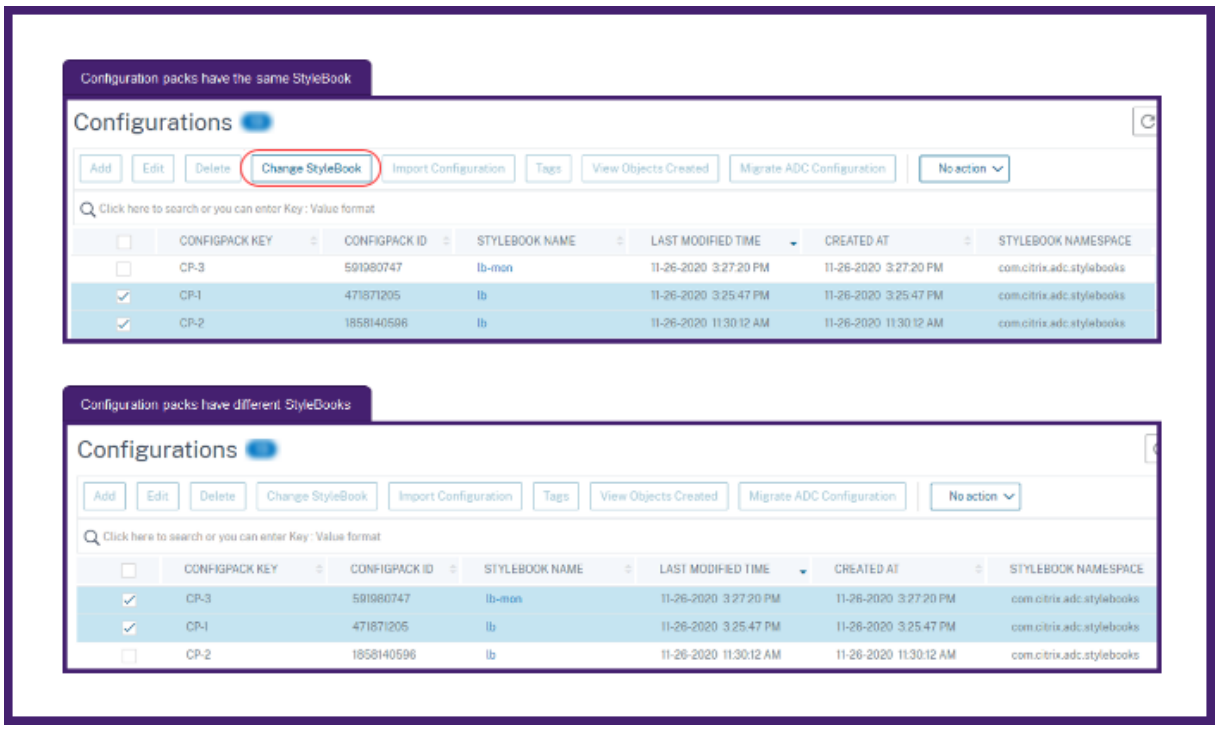
In Infrastructure Analytics werden einige thematische Aktualisierungen an der Benutzeroberfläche vorgenommen, die die Benutzererfahrung verbessern.

[NSADM-57697]

Ändern Sie das StyleBook mehrerer Konfigurationspakete gleichzeitig

Sie können jetzt das StyleBook mehrerer Konfigurationspakete gleichzeitig ändern. Wenn Sie ein vorhandenes StyleBook durch ein neues ersetzen, können Sie das StyleBook aller oder mehrerer zugehöriger Konfigurationspakete in einem Vorgang ändern. Zuvor mussten Sie jedes Konfigurationspaket nacheinander auswählen, um das StyleBook zu ändern.

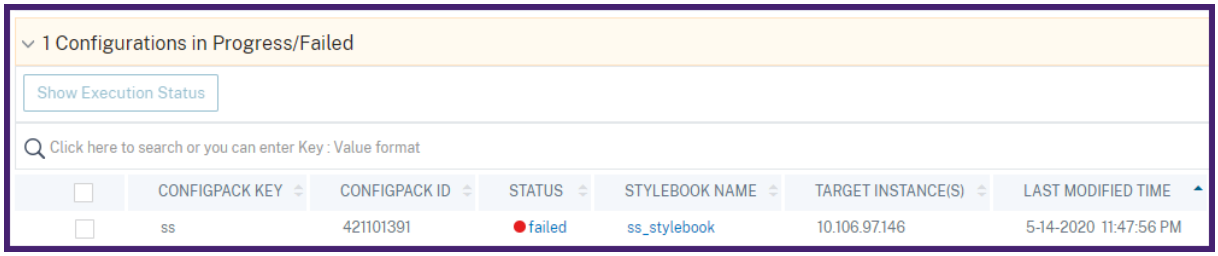
> **Hinweis**
>
> Stellen Sie sicher, dass Sie die Konfigurationspakete auswählen, die mit demselben StyleBook verknüpft sind. Andernfalls ist die Option StyleBook ändern nicht verfügbar.



Für die ausgewählten Konfigurationspakete ändert das ADM erfolgreich das StyleBook, wenn die folgenden Bedingungen erfüllt sind:

- Alle Konfigurationsparameter des vorhandenen StyleBook müssen im ausgewählten StyleBook enthalten sein.
- Die neuen Parameter aus dem ausgewählten StyleBook sind optional.

Um den Fortschritt der ausgewählten Konfigurationspakete anzuzeigen, wählen Sie **Konfigurationen in Fortschritt/Fehlgeschlagen** auf der Seite **Konfigurationen** aus.



Weitere Informationen finden Sie unter Ändern des StyleBook mit mehreren Konfigurationspaketen.

[NSADM-57941]

Ändern des Zugriffstyps einer Autoscale-Anwendung

Der ADM unterstützt jetzt die Änderung des Zugriffstyps für die Autoscale-Anwendungen, die über DNS- oder Route 53-Verkehrsverteilung verfügen. Sie können also den Zugriffstyp für alle Autoscale-Anwendungen ändern.

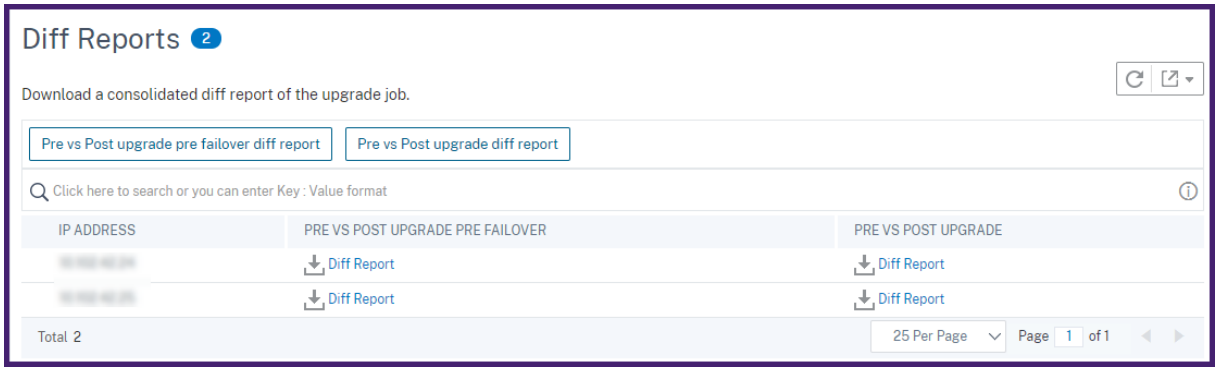
Zuvor wurde die Änderung des Zugriffstyps nur für die Anwendungen unterstützt, die eine ALB- oder NLB-Verkehrsverteilung hatten.

[NSADM-57029]

Laden Sie einen konsolidierten Diff-Bericht über einen ADC-Upgrade-Job

Sie können jetzt einen konsolidierten Diff-Bericht über einen ADC-Upgrade-Job herunterladen. Dieser Bericht enthält die Unterschiede zwischen den Ausgaben des Pre-Upgrade- und Post-Upgrade-Skripts. So können Sie bestimmen, welche Änderungen bei der ADC-Instanz nach dem Upgrade aufgetreten sind.

> **Hinweis**
>
> Der Diff-Bericht wird nur generiert, wenn Sie dasselbe Skript in den Phasen vor dem Upgrade und nach dem Upgrade angeben. Stellen Sie daher sicher, dass Sie in den Phasen nach dem Upgrade dasselbe Skript wie Pre-Upgrade verwenden auswählen.



Sie können die folgenden Arten von Diff-Berichten herunterladen:

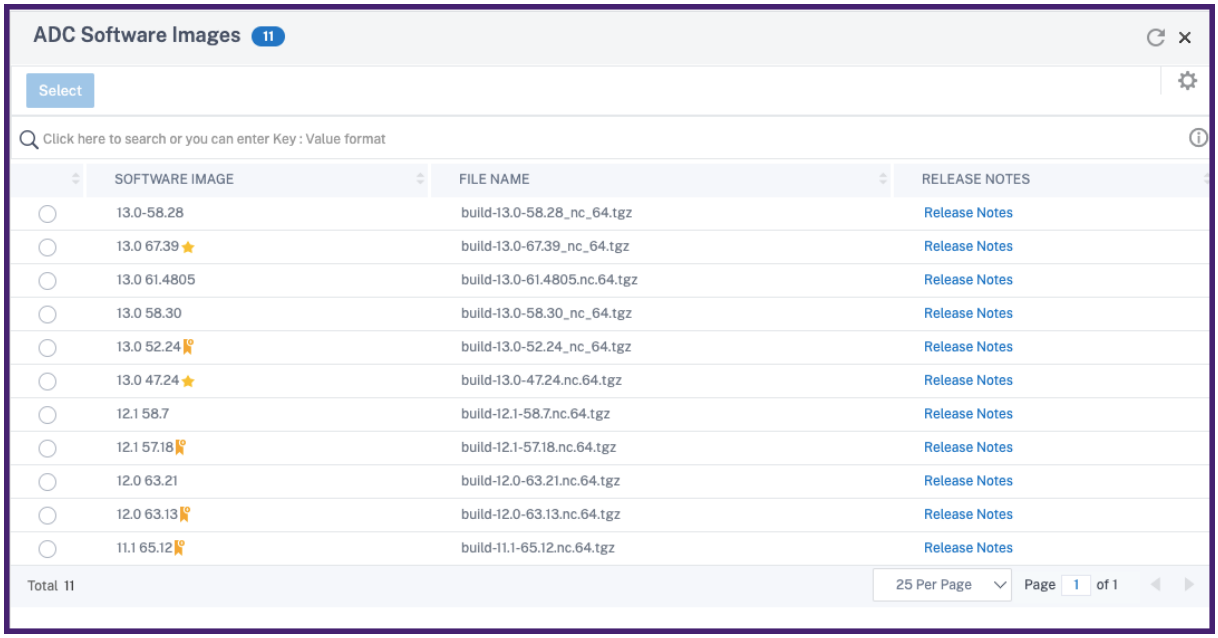
- **Vor und nach dem Upgrade vor dem Failover-Diff-Bericht**
- **Pre-vs. Diff-Bericht nach dem Upgrade**

Weitere Informationen finden Sie unter Laden Sie einen konsolidierten Diff-Bericht über einen ADC-Upgrade-Job.

[NSADM-50200]

Wählen Sie ein ADC-Image aus, ohne es hochzuladen

Wenn Sie einen ADC-Upgrade-Auftrag erstellen, können Sie jetzt ein ADC-Image auswählen, ohne es hochzuladen. Diese Option listet alle ADC-Images auf, die auf der Citrix Downloads-Website verfügbar sind. Das ausgewählte ADC-Image wird vom Citrix Download-Dienst heruntergeladen.



Weitere Informationen finden Sie unter Verwenden von Aufträgen zum Aktualisieren von Citrix ADC-Instanzen.

[NSADM-52471]

Problem behoben

Wenn ein Benutzer zur **Abonnementseite** navigiert und auf **Lizenz**klickt, wird der Fehler **Nicht autorisiert** angezeigt, selbst wenn der Benutzer über Anzeige- oder Bearbeitungsberechtigungen für die **Abonnementseite** verfügt.

[NSHELP-25351]

Der ADM-Dienst hat keine Zeitüberschreitung für den Ablauf von Anmeldesitzungen und die Abmelde-API. Infolgedessen bleibt die Benutzersitzung gültig.

[NSADM-63819]

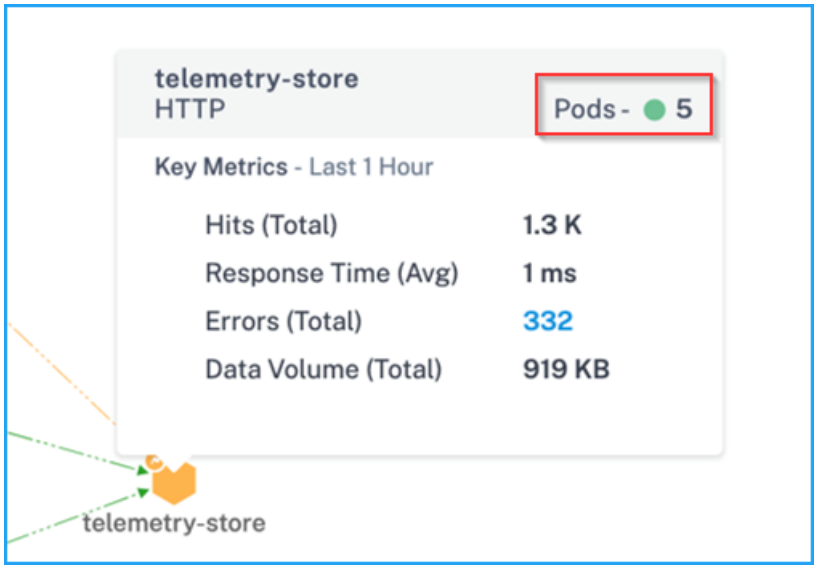
In **Analytics > Sicherheit > Sicherheitsverletzungen**zeigt der Indikator für **übermäßige Clientverbindungen** keine Anomalien an, selbst wenn ein hohes Volumen an Clientverbindungen empfangen wird.

[NSADM-64548]

11. November 2020

Servicegraf — Alle zugehörigen Backend-Pod-Details anzeigen

Wenn Sie in Service Graph den Mauszeiger auf einen Dienst bewegen, können Sie jetzt die Gesamtzahl der mit dem Dienst verknüpften Pods anzeigen.



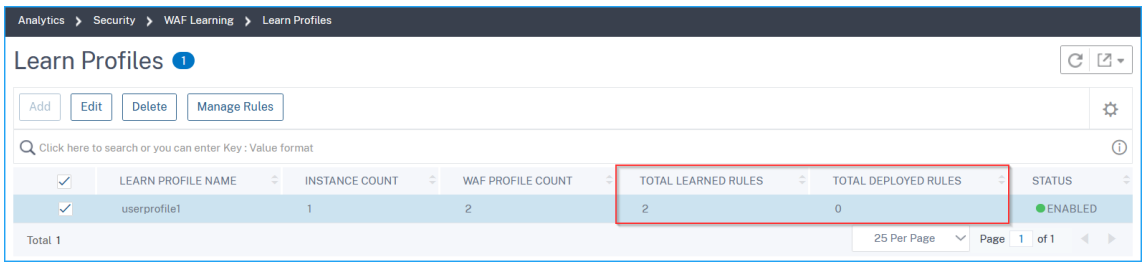
Weitere Informationen finden Sie unter Service-Details anzeigen.

[NSADM-47395]

Verbesserungen der WAF-Lernmaschine

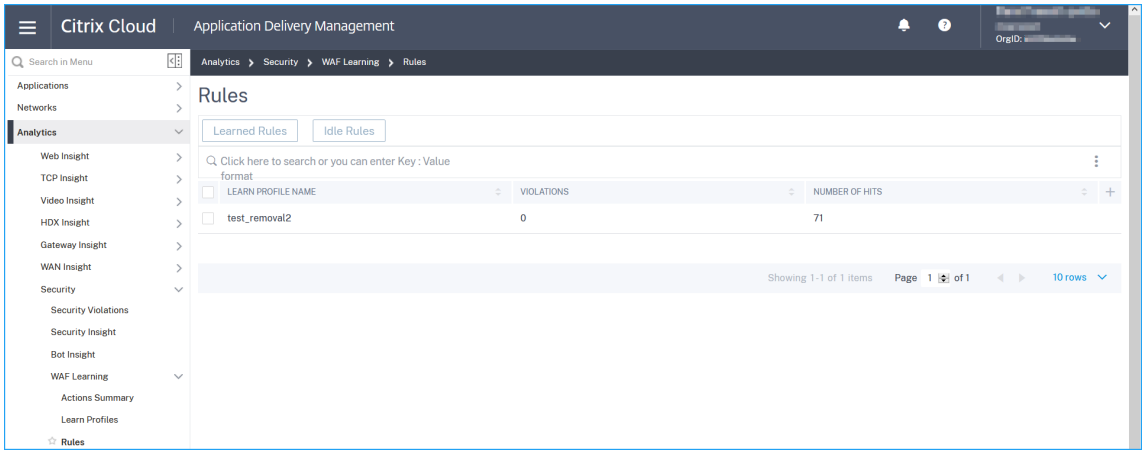
In der WAF-Lernengine können Sie jetzt die folgenden Verbesserungen anzeigen:

- Auf der Seite " **Lernprofile** " können Sie die **Total Learned Rules** und **Total Deployed Rules**anzeigen.

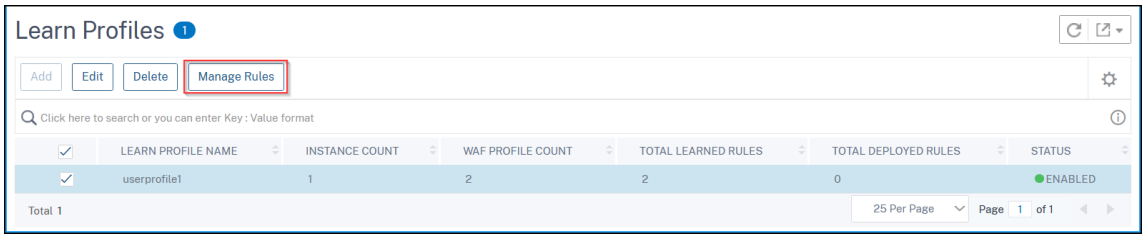


- Die Seite " **Regeln** " ist nicht mehr verfügbar. Die Option **"Regeln verwalten** " wird der Seite " **Lernprofile** " hinzugefügt. Die relevanten Informationen zu erlernten Regeln, Leerlaufregeln und bereitgestellten Regeln sind zugänglich, indem Sie den Profilnamen auswählen und auf die Schaltfläche **Regeln verwalten** klicken.

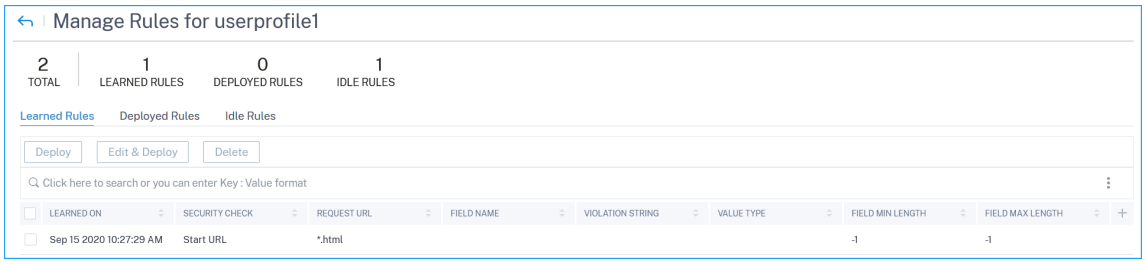
  Vorhin:



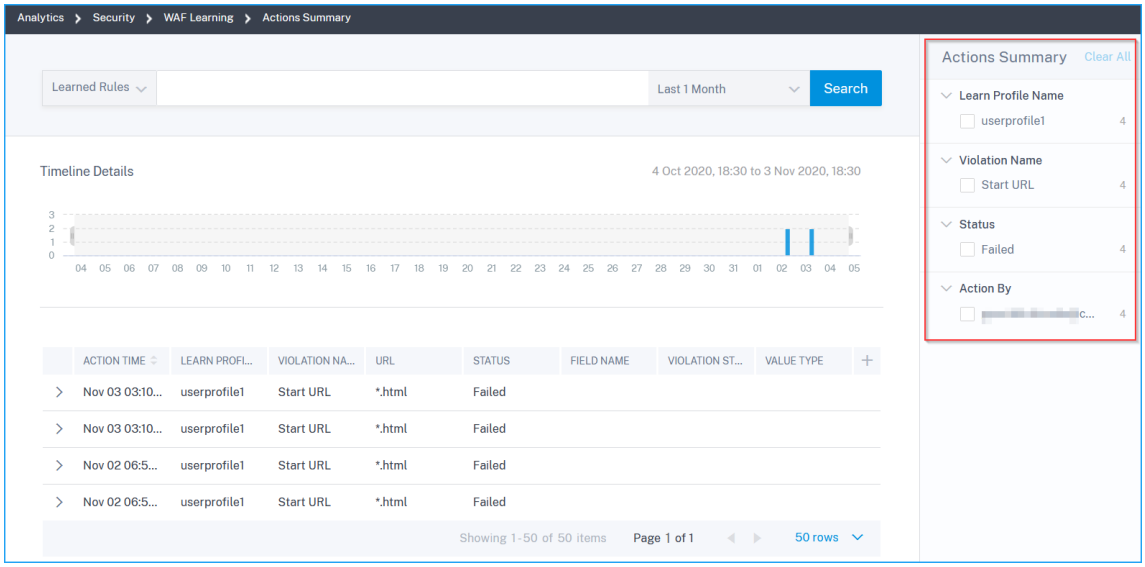
Jetzt:



- Nachdem Sie auf **Regeln verwalten**geklickt haben, können Sie die Gesamtregeln, die gesamten erlernten Regeln, die Gesamtzahl der bereitgestellten Regeln und die vollständigen Leerlaufregeln für das ausgewählte Profil anzeigen.



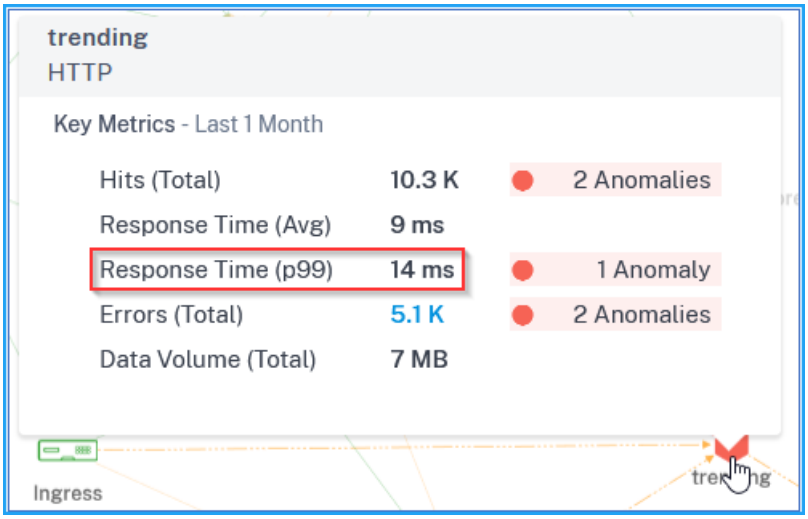
- Auf der Seite “ **Aktionszusammenfassung** “ können Sie Ergebnisse filtern, indem Sie die Optionen unter “ **Aktionsübersicht**” auswählen.



Weitere Informationen finden Sie unter WAF-Lernmaschine.

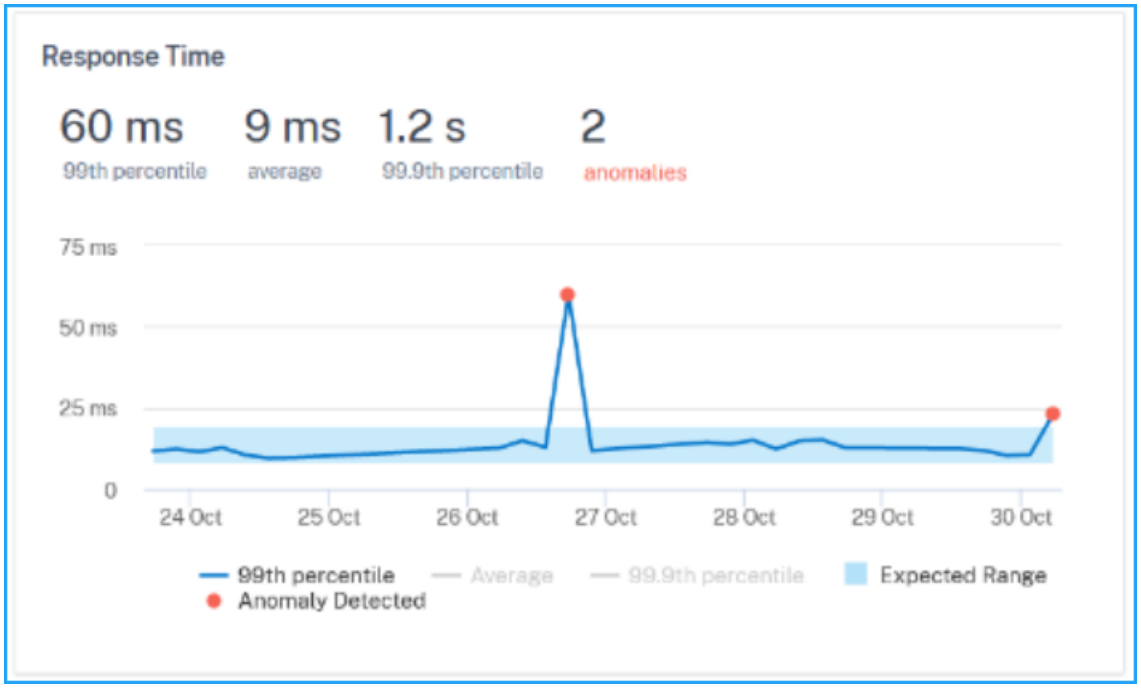
Servicegragramm — Pxx Wert für die Reaktionszeit des Dienstes

Wenn Sie in Service Graph den Mauszeiger auf einen Dienst bewegen, können Sie jetzt den Pxx Wert für die Reaktionszeit anzeigen.



Reaktionszeit (p99) — Gibt an, dass die 99% der Service-Reaktionszeit für die ausgewählte Dauer kleiner als der **p99-Wert** ist.

Wenn Sie einen Drilldown zur Anzeige der Servicedetails anzeigen, können Sie auch das 99-te Perzentil und das 99,9. Perzentil der Reaktionszeit für die ausgewählte Dauer anzeigen.



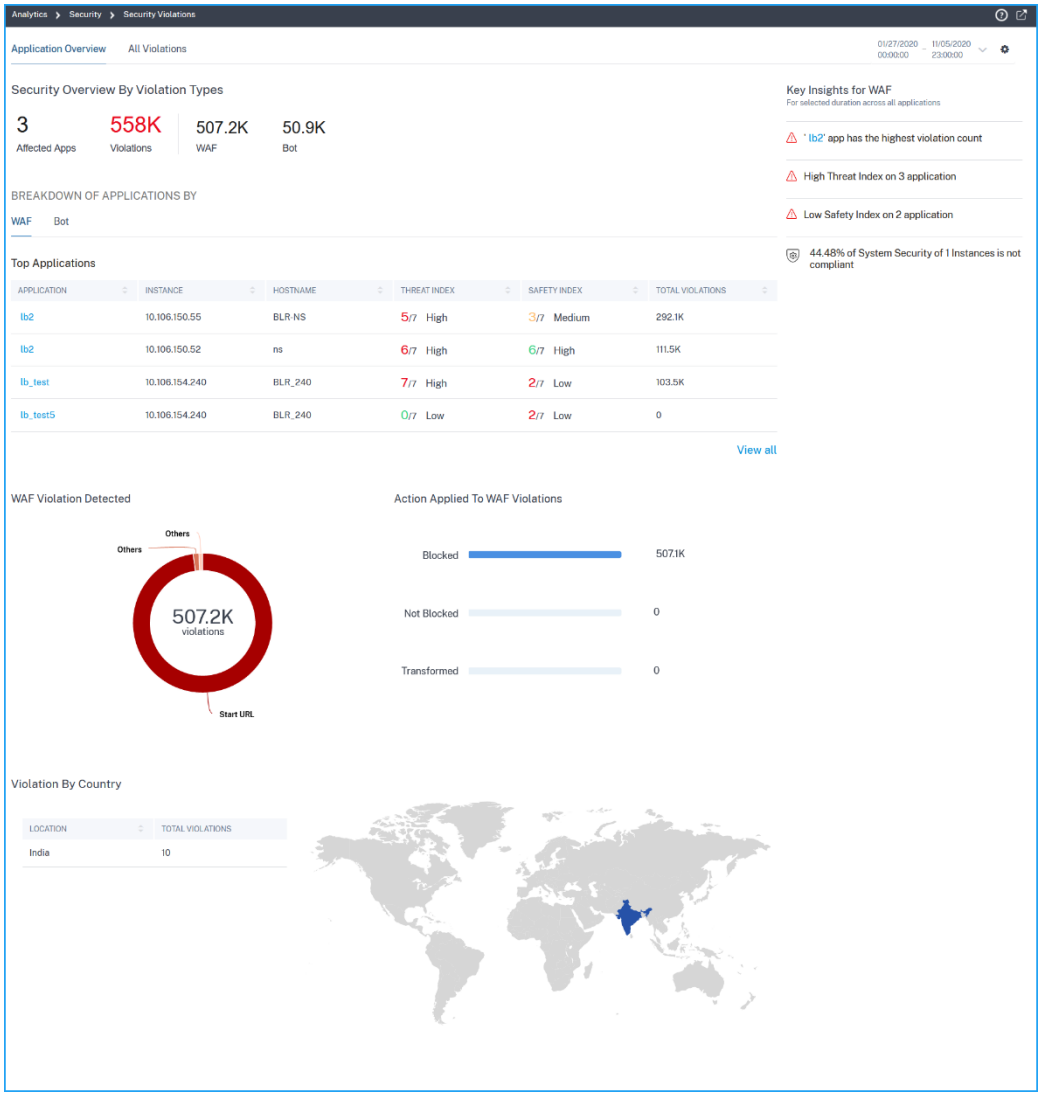
Als Administrator können Sie anhand des pxx Werts die Service-Reaktionszeit besser verstehen. Weitere Informationen finden Sie unter Service-Details anzeigen.

[NSADM-57729]

Verstöße gegen die App-Sicherheit — Visualisieren Sie Anwendungen mit Sicherheitseinblicken und Details zu Bot Insight

In **Analytics > Sicherheit > Sicherheitsverstöße**können Sie jetzt Anwendungen mit umfassendem Einblick in die Bedrohungsdetails visualisieren, die sowohl mit Sicherheitseinblicken als auch mit Bot-Einblicken verbunden sind. Die Seite " **Sicherheitsverletzungen** " enthält jetzt **Alle Verstöße** und **Anwendungsübersicht**.

- **Alle Verstöße** — Zeigt die Details zur Verletzung der Anwendungssicherheit an.
- **Anwendungsübersicht** — Zeigt eine Übersicht mit Informationen wie totalen Verstößen, totalen WAF- und Bot-Verstößen, Top-Anwendungen, Verstößen nach Ländern usw. an.



Weitere Informationen finden Sie unter Details zu Anwendungssicherheitsverletzungen anzeigen.

[NSADM-57174]

Servicediagramm - Überwachen Sie Kubernetes-Dienste anhand der Metriken des goldenen Signals

Die Goldsignal-Metriken für Dienste, die in einem Kubernetes-Cluster ausgeführt werden, beziehen sich auf eine Reihe von Metriken, mit denen Sie potenzielle Anomalien für eine bestimmte Dauer erkennen können. Wenn Sie 100 s Microservices im Kubernetes-Cluster haben, kann es schwierig sein, einen Dienst zu identifizieren, der häufig auftretende Probleme hat. Die folgenden drei wichtigen Metriken sind die Golden Signal-Metriken, mit denen Citrix ADM Service Graph Ihnen helfen kann, potenzielle Anomalien für einen Kubernetes-Service zu identifizieren:

- Treffer

- Reaktionszeit (Durchschn.) und Reaktionszeit (P99)
- Fehler

Als Administrator können Sie mit diesen Metriken:

- Identifizieren des Servicestatus
  - **Kritisch** — Dienst hat Anomalien oder Schwellenwertverletzungen in mehreren Metriken
  - **Review** - Der Dienst hat Anomalien oder Schwellenverletzungen in einer der Metriken
  - **Gut** — Service ohne Anomalien oder ohne Schwellenverletzung
- Analysieren Sie, wie viele Anomalien in jeder Metrik identifiziert werden
- Beheben Sie das Problem und vermeiden Sie größere Auswirkungen

Weitere Informationen finden Sie unter Service-Details anzeigen.

[NSADM-56399]

Problem behoben

StyleBooks

- In StyleBooks zeigen die vorhandenen Konfigurationspakete im Feld **Erstellt um ein ungültiges Datum an**.

[NSADM-62160]

27. Oktober 2020

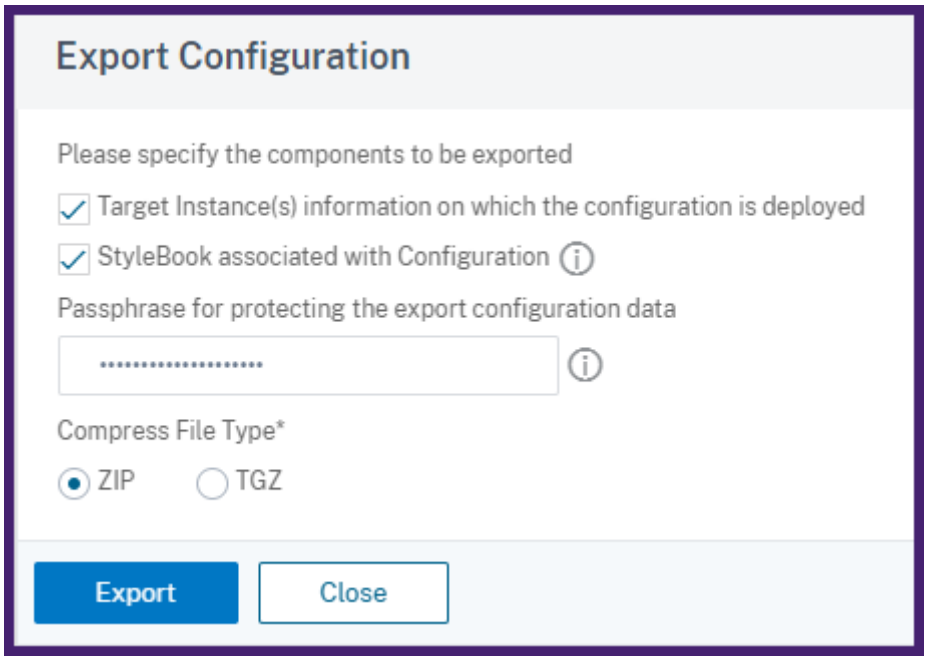
Exportieren oder Importieren eines StyleBook-Konfigurationspakets

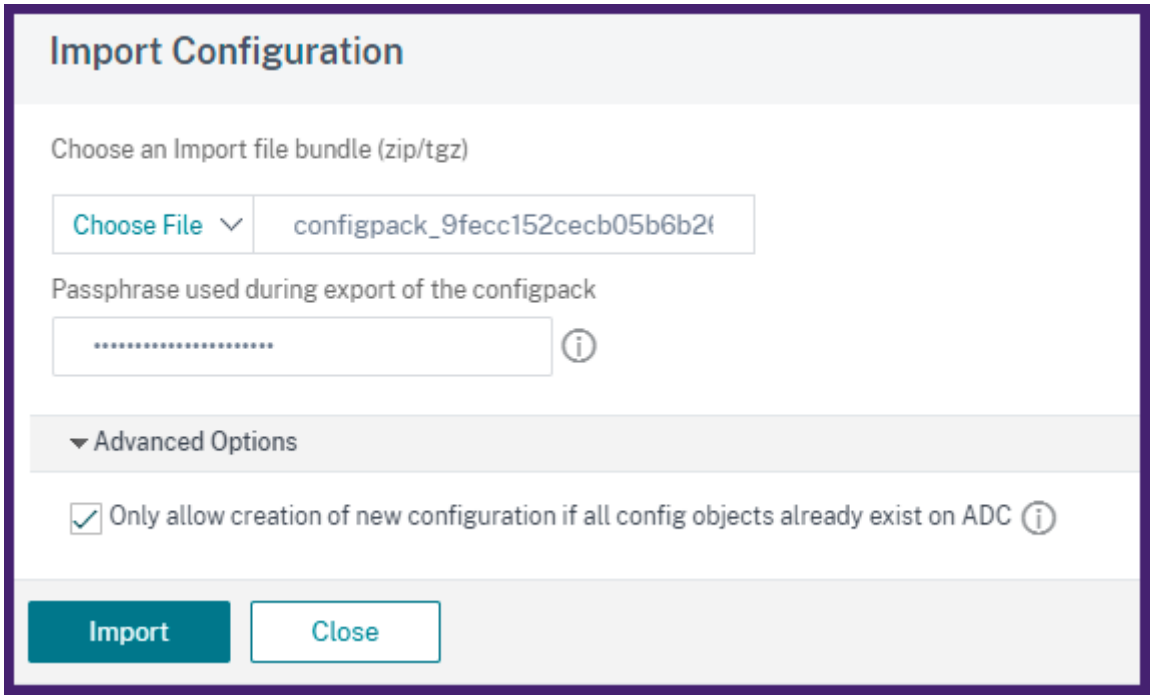
Sie können jetzt ein Konfigurationspaket wie StyleBooks exportieren oder importieren. Mit dieser Funktion können Sie die StyleBook-Konfiguration problemlos mit einem anderen ADM-Server teilen. Zuvor mussten Sie ein StyleBook herunterladen, es auf einen anderen ADM-Server importieren und dann eine Konfiguration daraus erstellen.

Wenn Sie ein Konfigurationspaket exportieren, wird ein `tgz` oder `zip` Paket auf Ihren lokalen Computer heruntergeladen. Dieses Bundle enthält eine JSON-Datei mit allen in einem Konfigurationspaket definierten Parameter. Es enthält auch die Informationen von Zielinstanzen, falls angegeben. Für das Konfigurationspaket eines benutzerdefinierten StyleBook können Sie das StyleBook in das Export-Bundle aufnehmen. Geben Sie eine Passphrase an, um das Export-Bundle zu verschlüsseln. Diese Passphrase sichert die sensiblen Daten eines Konfigurationspakets.

Sie können ein Konfigurationspaket von Ihrem lokalen Computer auf einen anderen ADM-Server importieren. Um ein Konfigurationspaket zu importieren, verwenden Sie die Passphrase, die Sie beim

Export angegeben haben. Weitere Informationen finden Sie unter Exportieren oder Importieren von Konfigurations.





[NSADM-57935]

Konfigurieren eines ADM-Servers nur für die gepoolte Lizenzfunktion

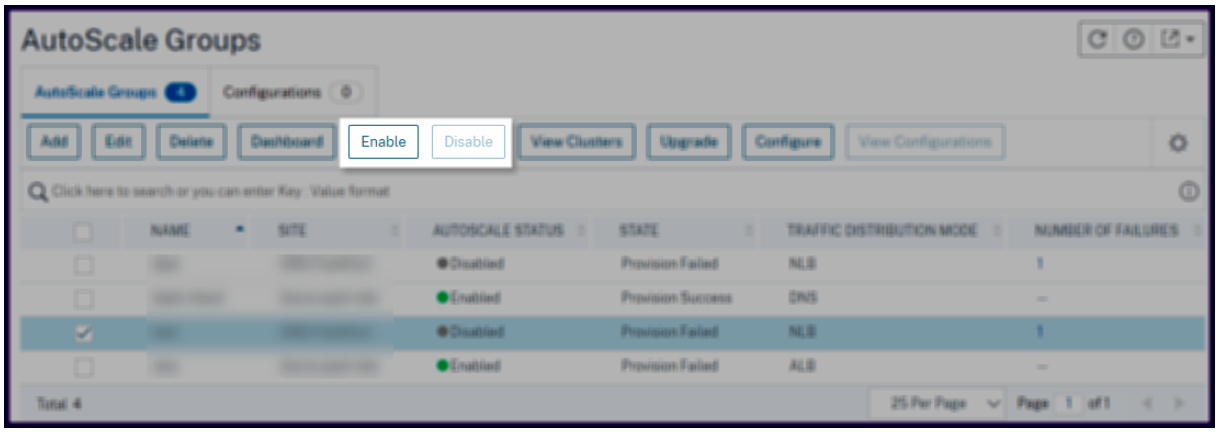
Als Administrator können Sie jetzt einen ADM-Server nur für die gepoolte Lizenzfunktion konfigurieren. Diese Konfiguration hilft, wenn Sie die regulatorischen Vorschriften haben, die ADC-Daten in-

nerhalb einer Zone einzuschränken. Der ADM-Dienst erhält nur Lizenzdaten von Ihren ADC-Instanzen. Und ermöglichen es Ihnen, gepoolte Kapazitätslizenzen dynamisch für Ihre global bereitgestellten ADC-Instanzen zuzuweisen. Weitere Informationen finden Sie unter Konfigurieren Sie den ADM-Dienst nur als Lizenzserver.

[NSADM-47930]

Aktivieren oder deaktivieren Sie eine Autoscale-Gruppe, ohne sie zu bearbeiten

Sie können jetzt eine Autoscale-Gruppe aktivieren oder deaktivieren, ohne sie zu bearbeiten. Die Optionen zum Aktivieren oder Deaktivieren werden jetzt auf der Seite **Netzwerke > AutoScale-Gruppen** angezeigt. Und Sie können eine Autoscale-Gruppe in der Option **Bearbeiten** weiterhin aktivieren oder deaktivieren.



[NSADM-57802]

Führen Sie benutzerdefinierte Skripte in den verschiedenen ADC-Upgrade-Stufen aus

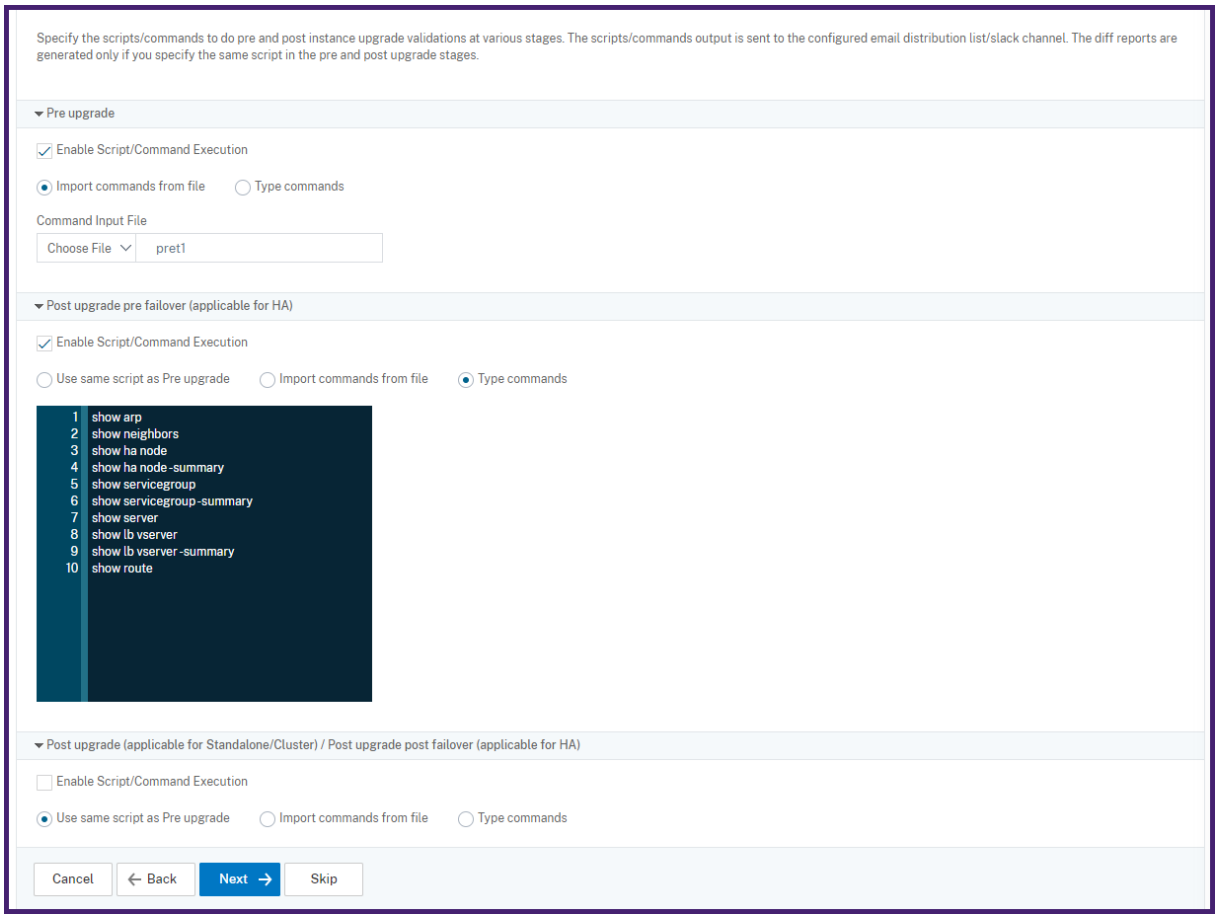
Die benutzerdefinierten Skripte werden verwendet, um die Änderungen vor und nach einem ADC-Instanz-Upgrade zu überprüfen. Ein Instanz-Upgrade hat mehrere Phasen. Sie können jetzt festlegen, dass diese Skripte in den folgenden Phasen ausgeführt werden:

- **Vor dem Upgrade**: Das angegebene Script wird vor dem Upgrade einer Instanz ausgeführt.
- **Vorab-Failover nach dem Upgrade (gilt für HA)**: Diese Phase gilt nur für die Bereitstellung mit hoher Verfügbarkeit. Das angegebene Skript wird nach dem Upgrade der Knoten, jedoch vor ihrem Failover ausgeführt.
- **Upgrade nach dem Upgrade (gilt für Standalone)/Nach dem Upgrade nach dem Failover (gilt für HA)**: Das angegebene Skript wird nach dem Upgrade einer Instanz in der eigenständigen Bereitstellung ausgeführt. Bei der Bereitstellung mit hoher Verfügbarkeit wird das Skript nach dem Upgrade der Knoten und ihres Failovers ausgeführt.

Mit dieser Funktion können Sie die Änderungen überprüfen, die in jeder Instanz-Upgrade-Phase vorgenommen wurden.

> **Hinweis Stellen Sie**
>
> sicher, dass Sie die Skriptausführung in den erforderlichen Phasen aktivieren Andernfalls werden die angegebenen Skripts nicht ausgeführt.

Sie können eine Skriptdatei importieren oder Befehle direkt in die ADM-GUI eingeben. In den Phasen nach dem Upgrade können Sie das gleiche Skript verwenden, das in der Pre-Upgrade-Phase angegeben ist. Weitere Informationen finden Sie unter Verwenden von Aufträgen zum Aktualisieren von Citrix ADC-Instanzen.

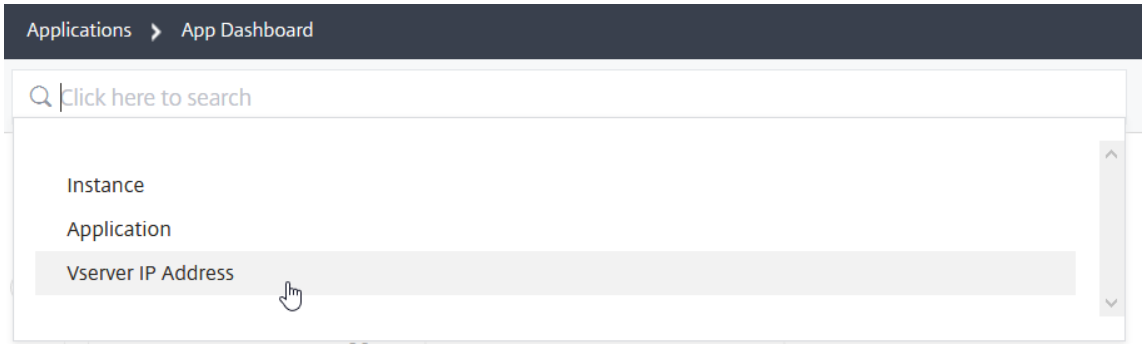


[NSADM-56649]

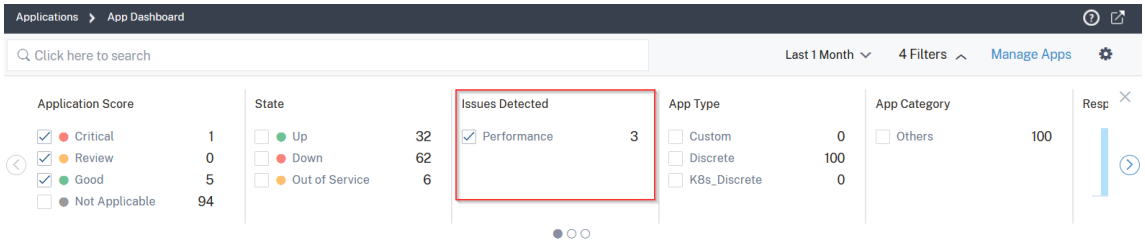
Verbesserungen am Anwendungs-Dashboard

Sie können jetzt die folgenden Verbesserungen im App Dashboard anzeigen:

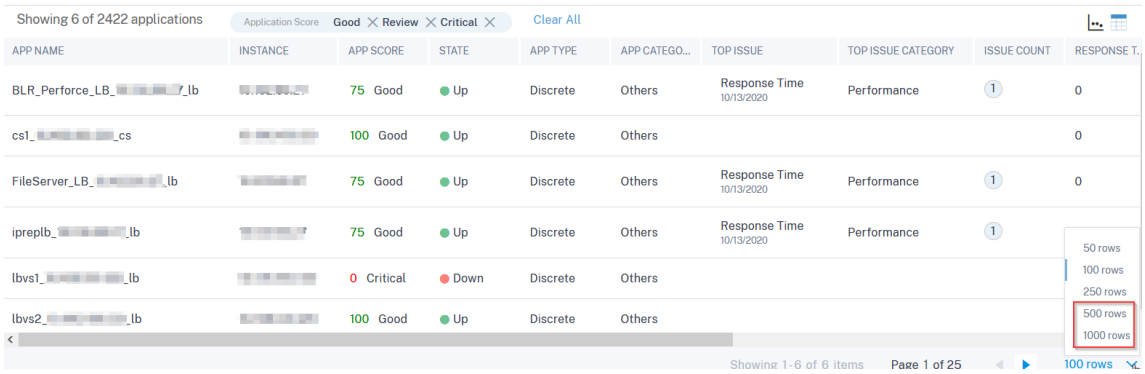
- In der Suchleiste können Sie die Ergebnisse basierend auf der IP-Adresse des virtuellen Servers filtern.



- Sie können eine Liste der Anwendungen abrufen, die mit einem bestimmten Problem betroffen sind, indem Sie den Problemtyp (Performance, Instanz Health, Config und System Resources) aus dem Filter auswählen.

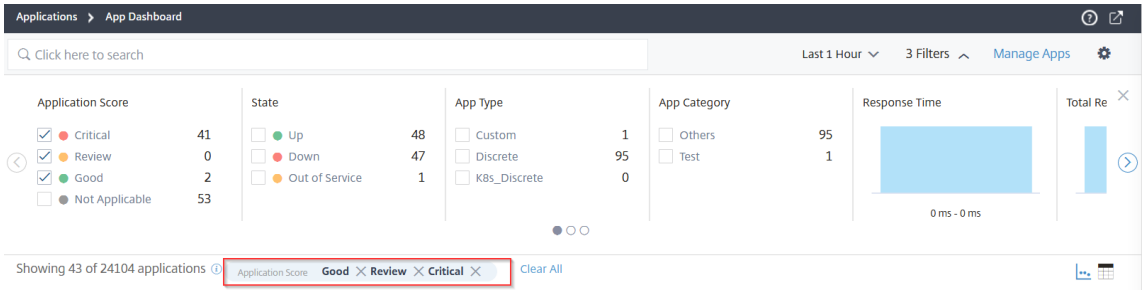


- In der tabellarischen Ansicht können Sie die Option 500 Zeilen und 1000 Zeilen auswählen, um die maximale Anzahl von Anwendungen anzuzeigen.



> **Hinweis**
>
> Wenn Sie die Option 500 Zeilen oder 1000 Zeilen auswählen, benötigt Citrix ADM ungefähr 20 Sekunden, um alle Anwendungen anzuzeigen.
>
> Nachdem alle Anwendungen geladen wurden, können Sie die Option für die Diagrammansicht auswählen.

- Standardmäßig können Sie Anwendungen anzeigen, die den Status “Kritisch”, “Überprüfen” und “Gut” aufweisen. Um Anwendungen anzuzeigen, die sich im Status N/A befinden, müssen Sie unter dem Filter “Nicht zutreffend” auswählen.



- Im Problem der Server-Antwortzeit können Sie Anomaliedetails anzeigen, nachdem Sie den virtuellen Server ausgewählt haben.

[NSADM-57049]

Behobene Probleme

System

- Wenn unter **Konto > Benutzeradministration > Gruppen**ein externer Benutzer zu mehreren Gruppen gehört und keine Anwendung für eine oder mehrere Gruppen ausgewählt ist, kann der externe Benutzer den virtuellen Server oder andere Entitäten nicht anzeigen.

  [NSHELP-25181]

- Wenn Sie unter **Konto > Benutzerverwaltung > Gruppen**eine Gruppe mit SDX-Instanzen hinzufügen oder bearbeiten, dauert es länger als üblich, die Gruppe zu erstellen oder zu ändern.

  [NSHELP-25081]

Lizenzierung

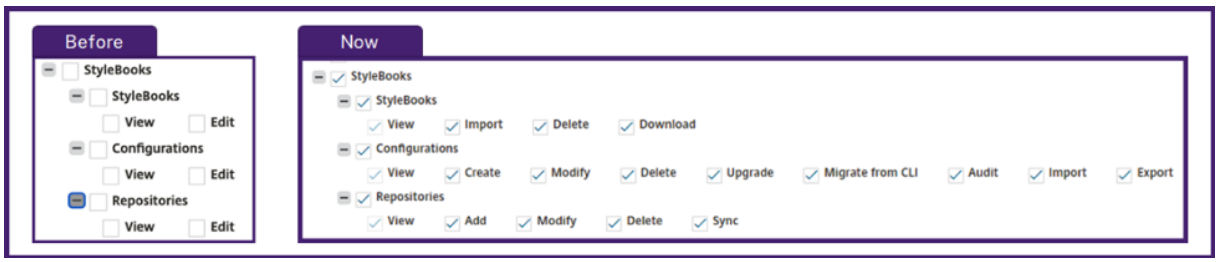
Wenn Sie nicht verwalteten Instanzen Lizenzen zuweisen, wird der Prozentsatz der Lizenzzuweisung im Donut-Diagramm falsch angezeigt.

[NSADM-60798]

14. Oktober 2020

Erteilen Sie Benutzern neue StyleBook-Berechtigungen

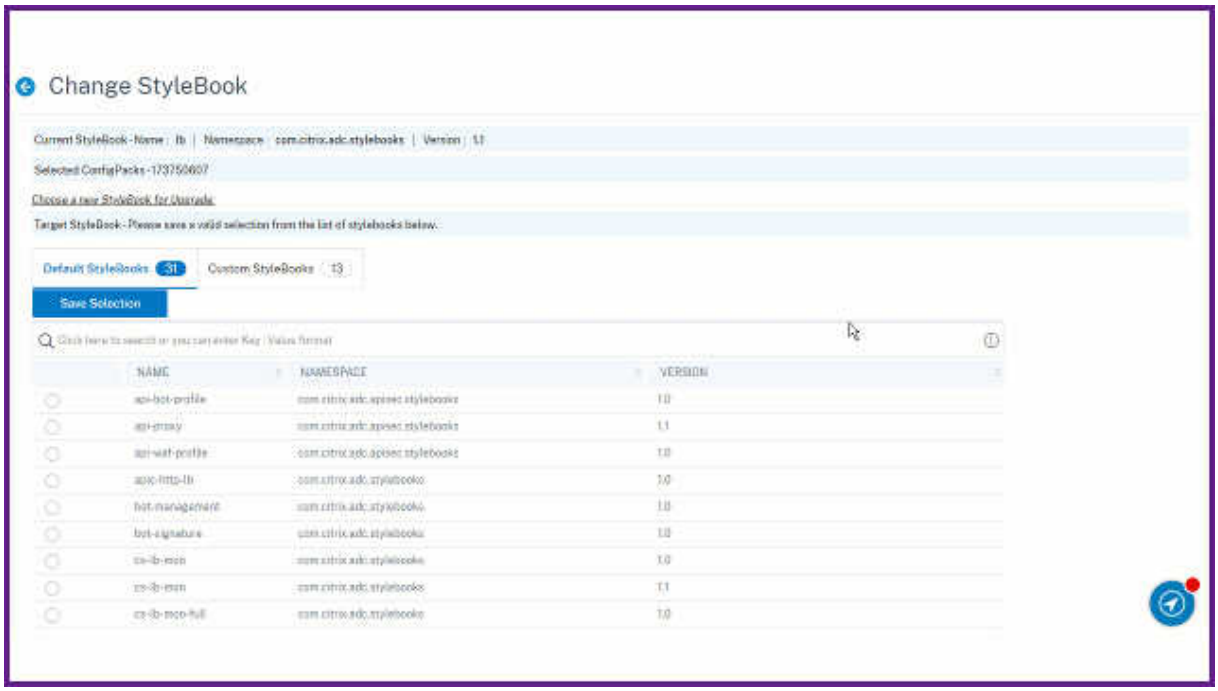
Wenn Sie als Administrator eine Zugriffsrichtlinie erstellen, können Sie Benutzern jetzt neue StyleBook-Berechtigungen wie Importieren, Löschen, Herunterladen und mehr erteilen. Navigieren Sie dazu zu **Konten > Benutzerverwaltung > Zugriffsrichtlinien** und klicken Sie auf **Hinzufügen**. Zuvor konnten Sie nur Anzeige- und Bearbeitungsberechtigungen auswählen. Weitere Informationen finden Sie unter Erteilen von StyleBook-Berechtigungen für Benutzer.



[NSADM-57672]

Bearbeiten eines Konfigurationspakets, um sein StyleBook

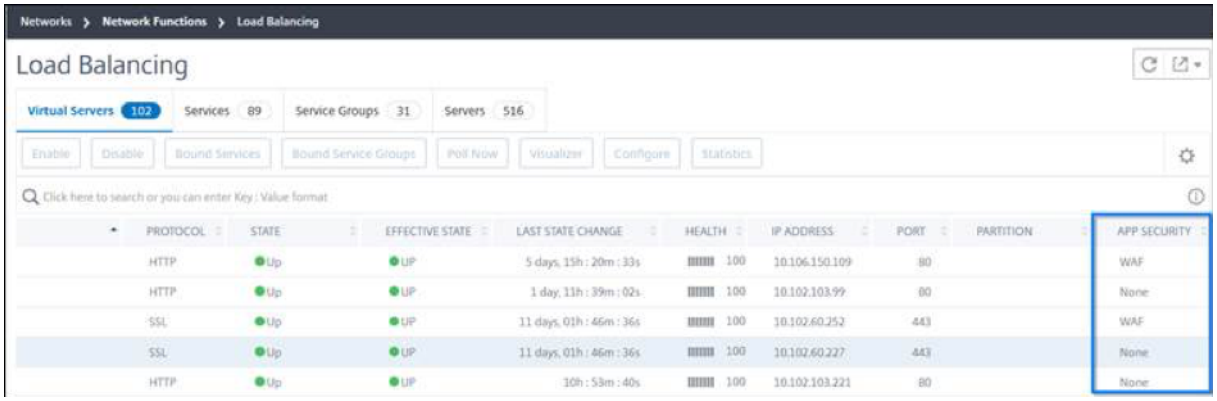
Sie können jetzt ein Konfigurationspaket bearbeiten, um das StyleBook zu ändern. Zuvor konnten Sie dies mit der Option “ConfigPack migrieren” tun. Weitere Informationen finden Sie unter Ändern des StyleBook eines Konfigurationspakets.



[NSADM-58245]

Netzwerkfunktionen: Hinzufügen der App-Security-Spalte

In **Netzwerke > Netzwerkfunktionen > Load Balancing und Content Switching**können Sie jetzt die Spalte **App Security**x anzeigen.



Als Administrator können Sie analysieren, ob die virtuellen Server mit folgenden Verbindungen verbunden sind:

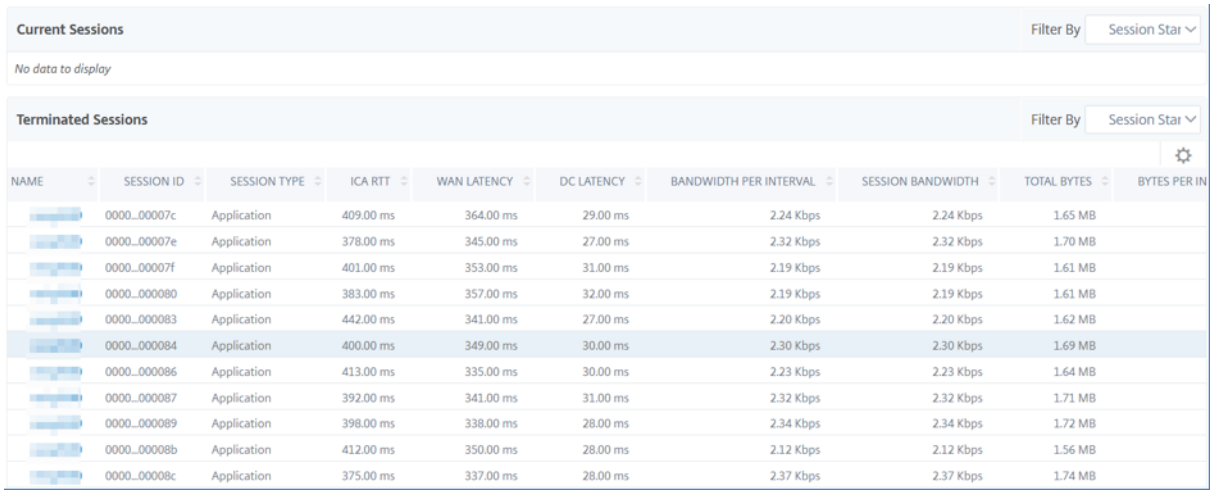
- **WAF** — Der virtuelle Server ist mit der App-Firewall-Richtlinie konfiguriert und zeigt die WAF-Sicherheitsverletzungen an.
- **Bot** — Der virtuelle Server ist mit einer Bot-Richtlinie konfiguriert und zeigt die Sicherheitsverletzungen des Bots an.
- **Bot, WAF** — Der virtuelle Server ist sowohl mit App Firewall- als auch mit Bot-Richtlinien konfiguriert und zeigt sowohl WAF- als auch Bot-Sicherheitsverletzungen an.
- **Keine** — Der virtuelle Server ist weder mit App Firewall noch mit Bot-Richtlinien konfiguriert.

Weitere Informationen finden Sie unter Details zu Anwendungssicherheitsverletzungen anzeigen.

[NSADM-54300]

HDX Insight: Verbesserungen zur Anzeige aller aktiven und beendeten Sitzungen

In **Analytics > HDX Insight > Benutzer**können Sie jetzt eine konsolidierte Ansicht aller aktiven und beendeten Benutzersitzungen visualisieren.



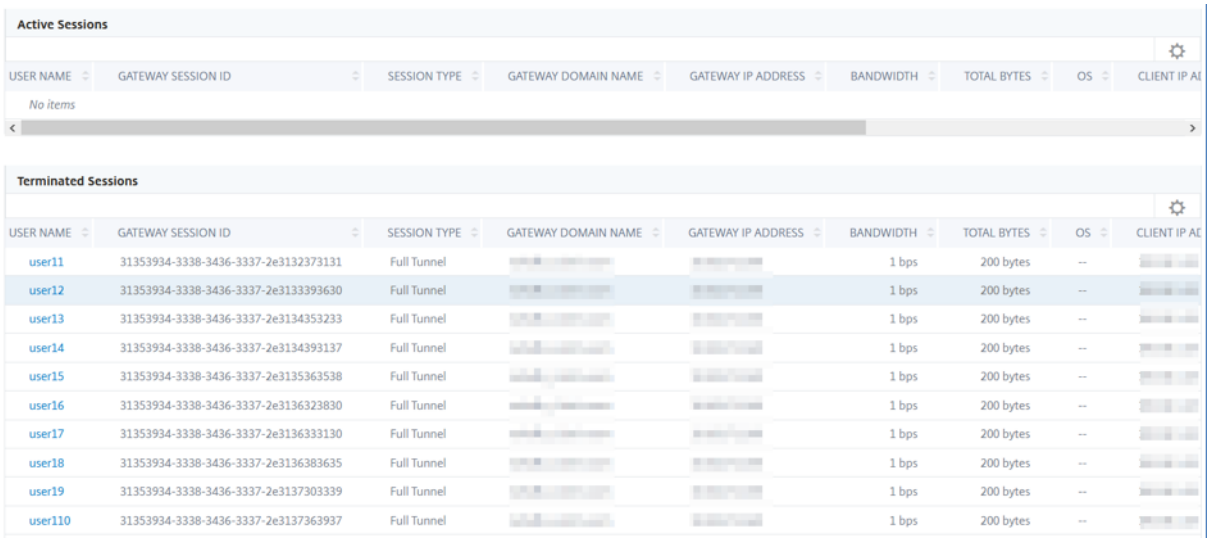
Als Administrator ermöglicht Ihnen diese Verbesserung:

- Zeigen Sie alle Benutzerdetails in einer Einzelbereichs-Visualisierung an
- Eliminieren Sie die Komplexität bei der Auswahl der einzelnen Benutzer und beim Anzeigen der aktiven und beendeten Sitzungen

[NSADM-57685]

Gateway Insight: Verbesserungen zur Anzeige aller aktiven und beendeten Sitzungen

In **Analytics > Gateway Insight > Benutzer > Gateway-Benutzer**können Sie jetzt eine konsolidierte Ansicht aller aktiven und beendeten Benutzersitzungen visualisieren.



Als Administrator ermöglicht Ihnen diese Verbesserung:

- Zeigen Sie alle Benutzerdetails in einer Einzelbereichs-Visualisierung an
- Eliminieren Sie die Komplexität bei der Auswahl der einzelnen Benutzer und beim Anzeigen der aktiven und beendeten Sitzungen

[NSADM-60800]

Sicherheitseinblick — SQL-Injection-Grammatik-Verstoß

In Security Insight können Sie jetzt einen neuen Verstoßtyp, SQL Injection Grammar, anzeigen. Um die SQL Injection Grammatik-Verletzung in Security Insight zu generieren, müssen Sie die folgenden Befehle in der Citrix ADC-Instanz konfigurieren:

1. `add ns ip <IP> <subnet mask> -type SNIP`
2. `add lb vs http_vs http <VS_IP> 80`
3. `add service http_svc <SVC_IP> http 80`

4. `bind lb vs http_vs http_svc`
5. `add appfw profile abc -startURLAction none -SQLInjectionGrammar ON -SQLInjectionType None`
6. `set appfw settings -defaultProfile abc`

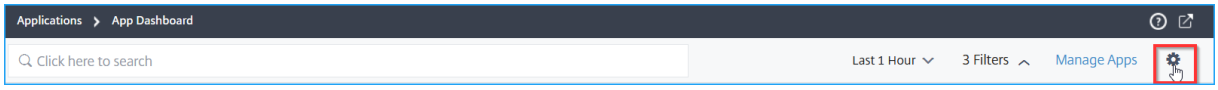
Weitere Informationen finden Sie unter Sicherheitshinweise.

App-Dashboard: Wählen Sie die App-Score-Komponenten aus und konfigurieren Sie Schwellen

Im **App Dashboard**können Sie jetzt als Administrator entscheiden, die Komponenten auszuwählen und Schwellenwerte für die App-Score-Berechnung zu konfigurieren. **App Score** ist das Punktesystem, das definiert:

- Wie gut funktioniert eine Anwendung
- Ob die Anwendung hinsichtlich der Reaktionsfähigkeit gut funktioniert

Navigieren Sie zu **Anwendungen > Dashboard** und wählen Sie dann das Einstellungssymbol aus, um die App-Score-Komponenten anzuzeigen.



Weitere Informationen finden Sie unter Wählen Sie App-Score-Komponenten und legen Sie Schwellenwerte.

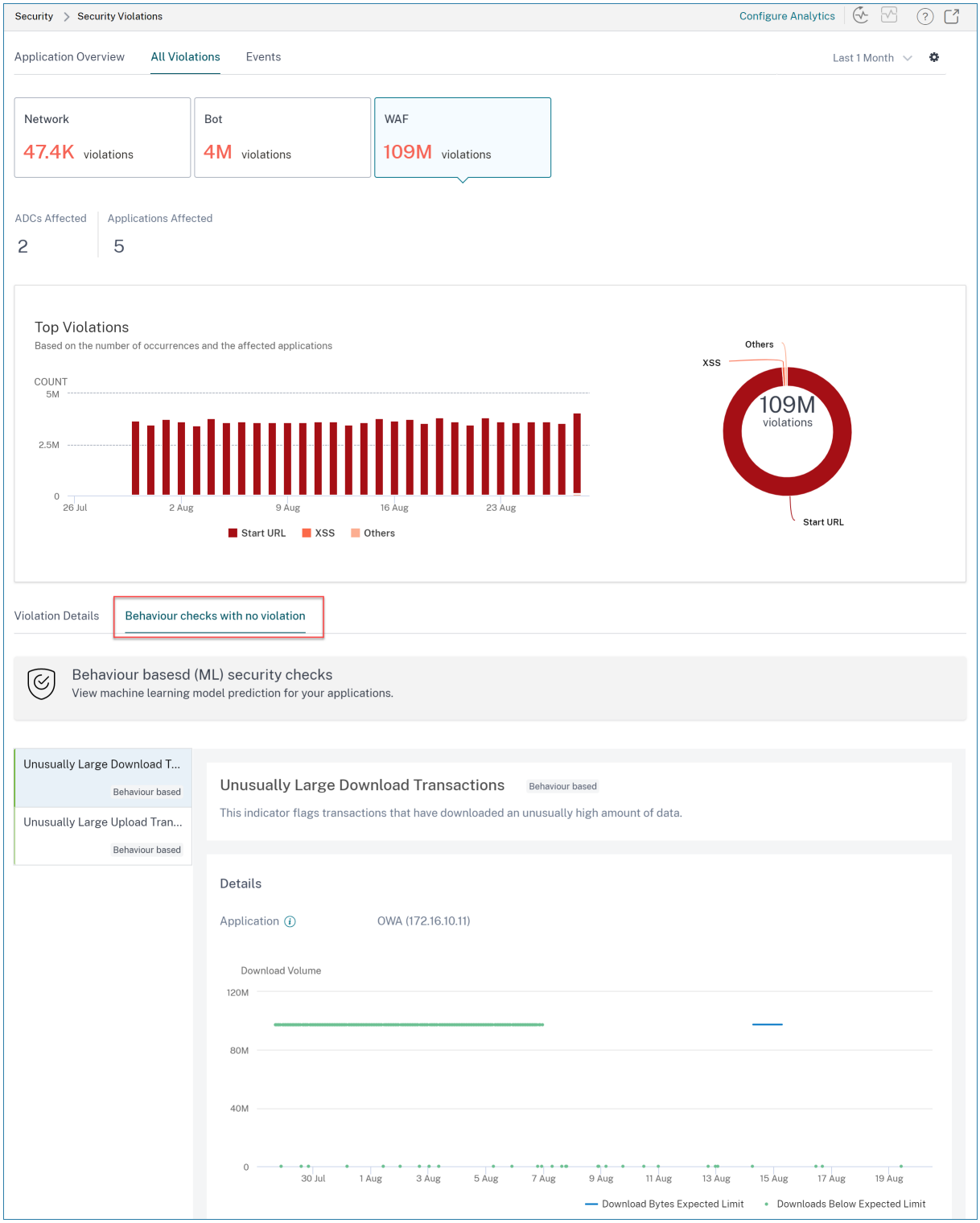
[NSADM-52870]

App-Sicherheitsverletzungen: Visualisieren Sie Prognosen basierend auf den Verkehrsmustern

In **Analytics > Sicherheit > Sicherheitsverstöße**können Sie für alle Sicherheitsverstöße (WAF und Bot), abgesehen von Verstoßdetails, jetzt eine dreiwöchige Verkehrsvorhersage basierend auf dem Algorithmus für maschinelles Lernen visualisieren. Als Administrator ermöglicht Ihnen diese dreiwöchige Vorhersage:

- Analysieren Sie das Verkehrsmuster, auch wenn keine Verstöße beobachtet
- Ergreifen Sie Fehlerbehebungsmaßnahmen für ungewöhnliche Verkehrsmuster, die aus den Prog
- Beachten Sie, dass Citrix ADM neben den Anomalien Daten verarbeitet

Klicken Sie auf der Seite **Sicherheitsverletzungen** auf die Registerkarte **Verhaltensüberprüfungen ohne Verstoß**, um die dreiwöchige Verkehrsprognose anzuzeigen.



Weitere Informationen finden Sie unter Verletzungen der App-Sicherheit.

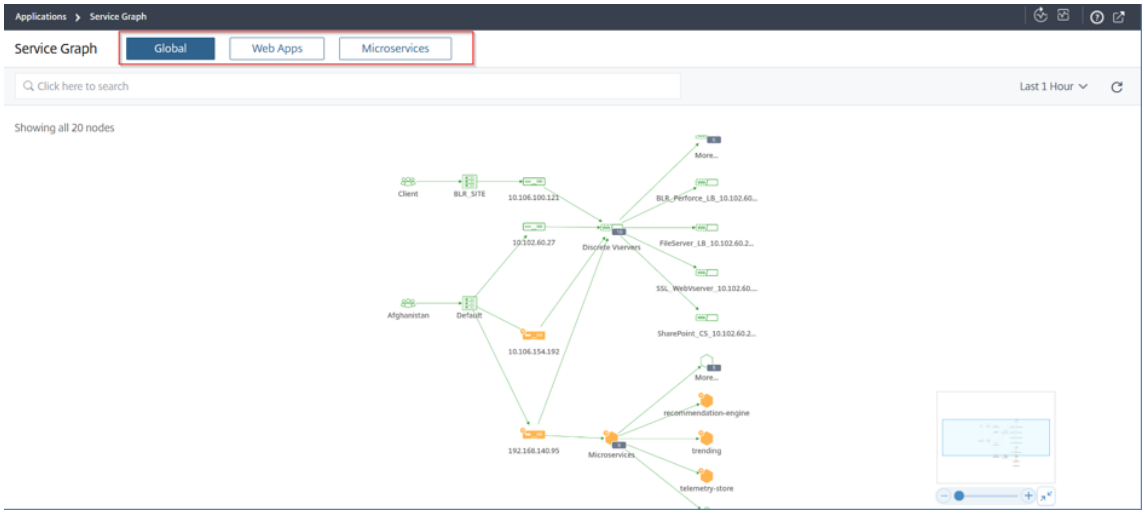
[NSADM-58721]

Verbesserungen des Service-Graphen

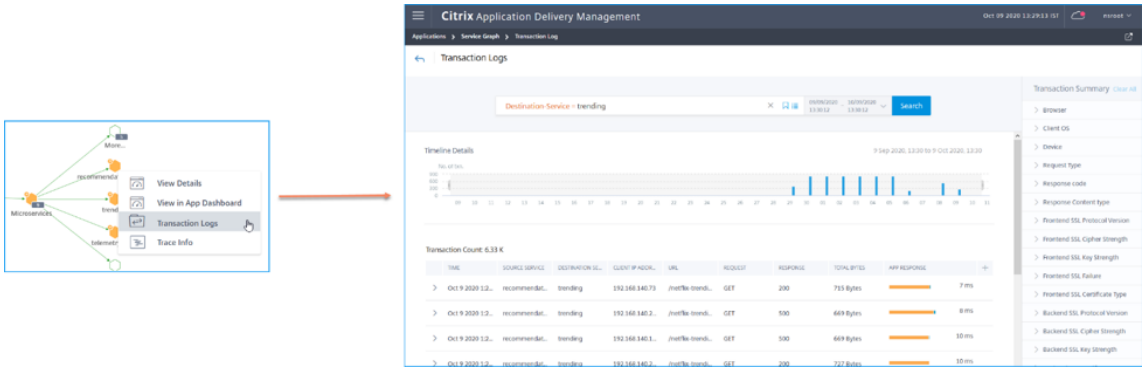
In **Applications > Service Graph**können Sie jetzt die folgenden Verbesserungen anzeigen:

- Die Service-Diagrammseite hat drei Registerkarten:
  - **Global** — Zeigt das Service-Diagramm für Anwendungen in allen Citrix ADC-Instanzen an
  - **Web-Apps** — Zeigt das Service-Diagramm für 3-Tier-Webanwendungen an (Load Balancing, Content Switching und GSLB)
  - **Microservices** — Zeigt das Servicediagramm für Kubernetes-Microservices

  Klicken Sie auf jede Registerkarte, um das entsprechende Service-Diagramm anzuzeigen.



- Im globalen Servicediagramm können Sie auf die Microservice-Details zugreifen. Wenn Sie auf einen Dienst klicken und die Option auswählen, wird auf die entsprechende GUI umgeleitet.



- Das Microservices-Dienstdiagramm hat eine Suchleiste, in der Sie den Mauszeiger zeigen und die folgenden Kategorien auswählen können, um den Filter zu erstellen:

- **Kunden-Geo-Standort** — Zeigt den Ingress und seine Dienste an, auf die der Kunde zugreift
- **ingress-IP** — Zeigt alle mit dem Ingress verbundenen Dienste an

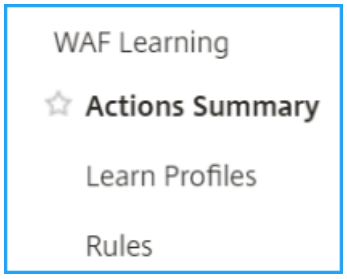
[NSADM-57696]

29. September 2020

Verbesserungen der WAF-Lernmaschine

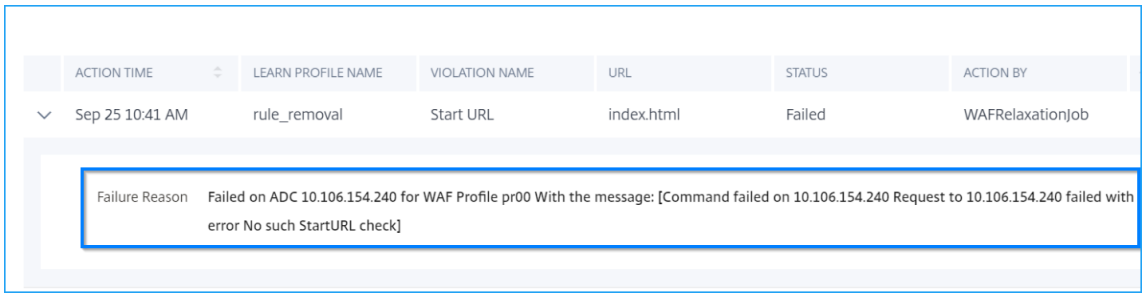
In der WAF-Lernengine können Sie jetzt die folgenden Verbesserungen anzeigen:

- **WAF Learning > Dashboard** wird durch **WAF Learning ersetzt > Aktionen-Zusammenfassung**



- Mit der Option **Aktion nach** können Sie verstehen, ob die erlernten Regeln von Citrix ADM automatisch bereitgestellt werden oder ob der Administrator die Option **Bereitstellen** oder **überspringen** manuell ausgewählt hat.

- Wenn eine bereitgestellte Learne-Regel fehlgeschlagen ist, können Sie den Fehlergrund auf der Seite **Aktionen-Zusammenfassung** anzeigen.

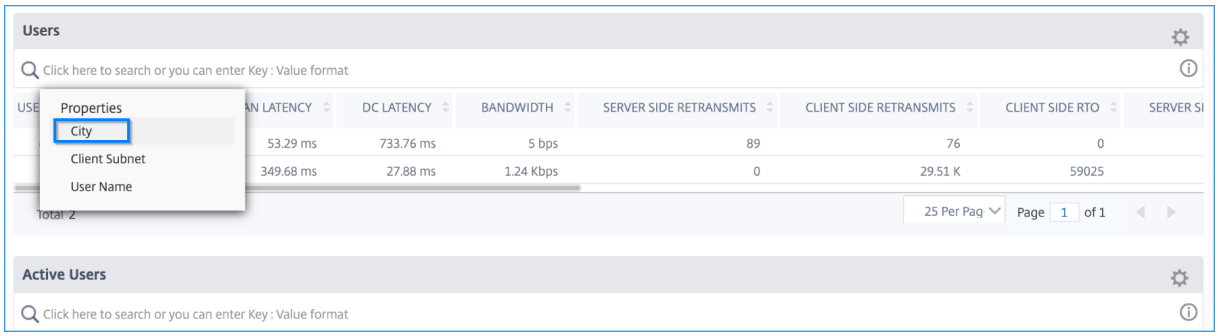


- Für jedes konfigurierte erlernte Profil können Sie bis zu 1 Million erlernte Regeln einsehen.

  [NSADM-57220]

HDX Insight — Suche unter Verwendung des Städtenamens

In HDX Insight können Sie jetzt die Ergebnisse anhand des Stadtnamens filtern.

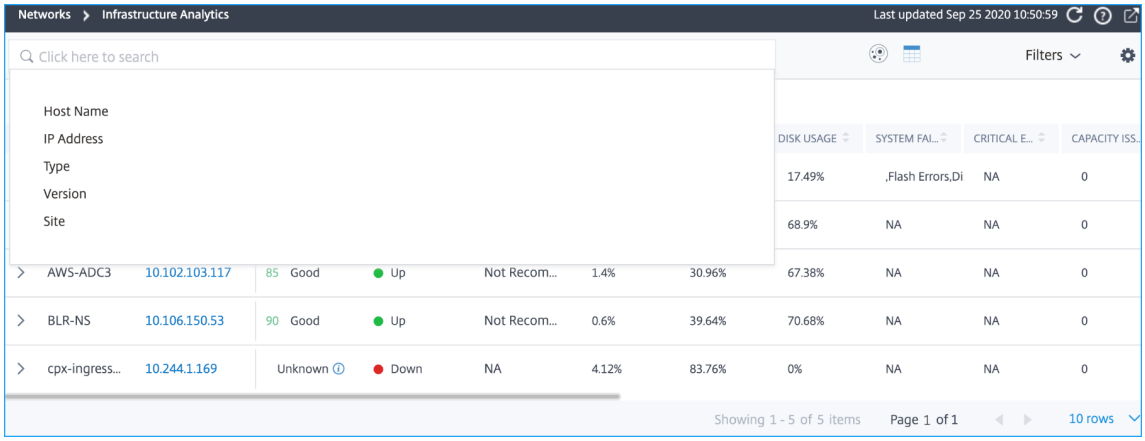


[NSADM-57366]

Infrastructure Analytics — Suchattribute

In **Infrastructure Analytics**können Sie jetzt den Mauszeiger auf die Suchleiste setzen und die folgenden Suchattribute auswählen, um die Ergebnisse zu filtern:

- Hostname
- IP-Adresse
- Typ
- Version
- Site

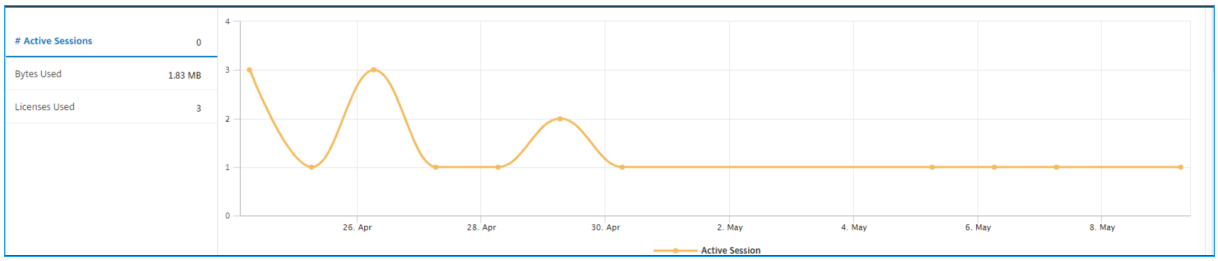


[NSADM-59453]

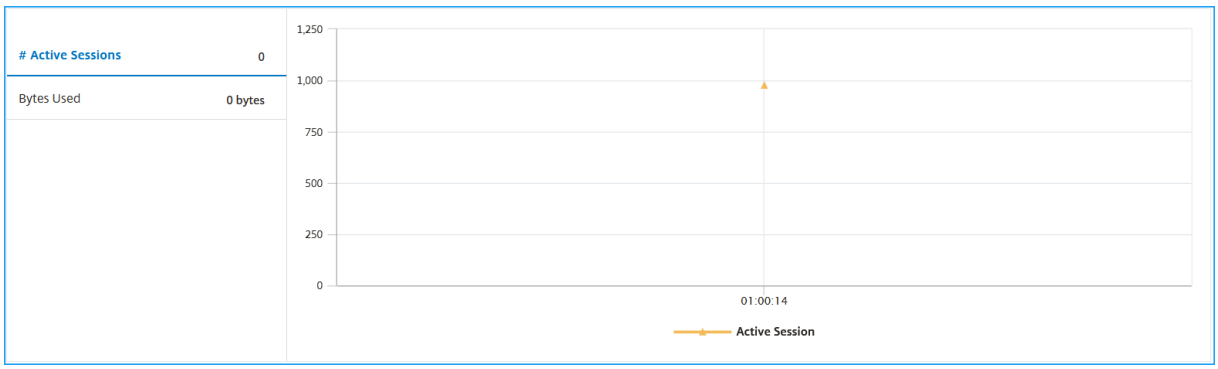
Verbesserungen bei Gateway Insight

In **Gateway Insight > Benutzer**werden die Lizenzinformationen jetzt entfernt.

Vorhin:



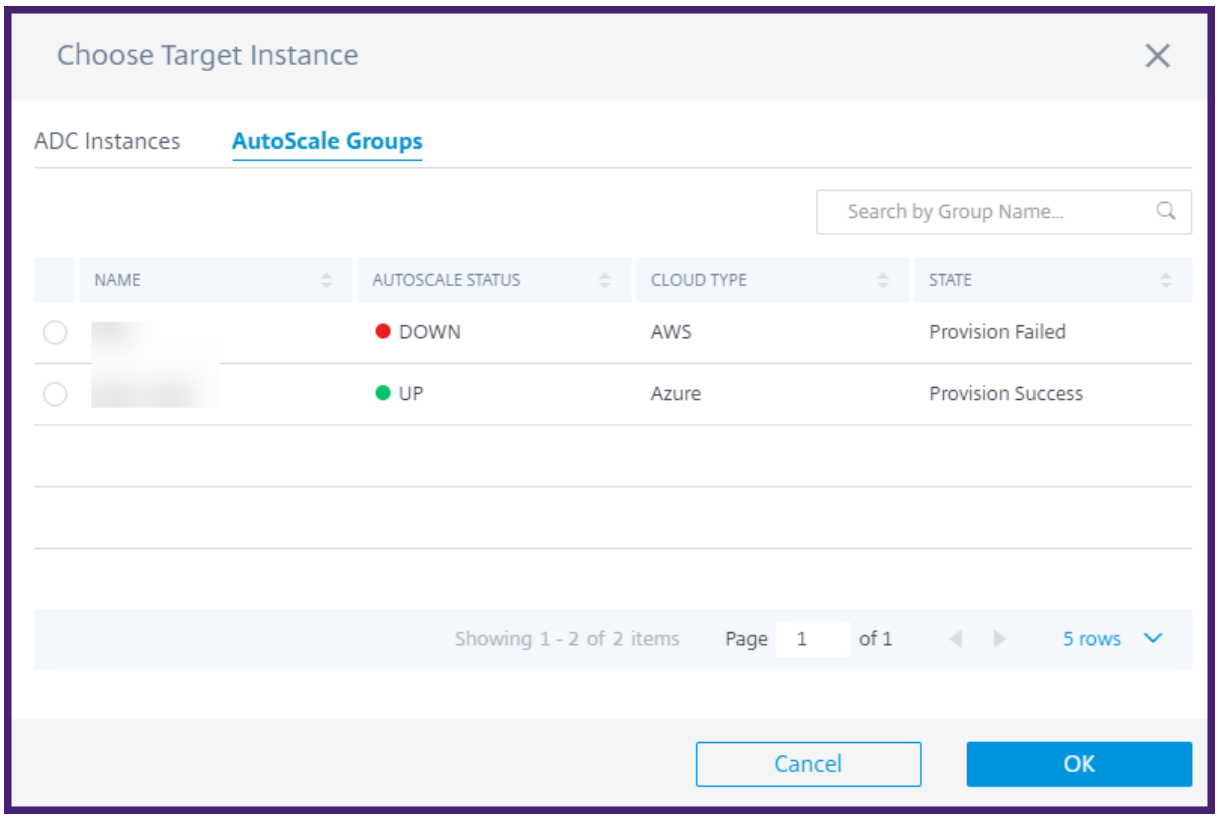
Jetzt:



[NSADM-53494]

Migrieren der ADC-Konfiguration auf eine Autoscale-Gruppe mit StyleBook Configuration Builder

Im StyleBooks-Konfigurations-Builder können Sie jetzt die ADC-Konfiguration auf eine Autoscale-Gruppe migrieren. Wählen Sie dazu die erforderliche Autoscale-Gruppe als Zielinstanz aus.



[NSADM-51470]

Behobene Probleme

Bereitstellung

Das ADM-Agenten-Image funktioniert nicht im AWS M5-Instanz-Typ. Mit diesem Fix werden unterstützte Treiber hinzugefügt, damit das ADM-Agent-Image in M5-Instanz-Typen funktioniert.

[NSHELP-24250]

Netzwerke

Wenn Sie einen Konfigurationsauftrag mit dem Zeichen “<” ausführen, schlägt der Job fehl.

[NSADM-53465]

16. September 2020

Berührungsarmes Onboarding von ADC-Instanzen mit ADM Service Connect

Jetzt können Sie den neuen Onboarding-Workflow für den Citrix ADM Service verwenden, der eine schnellere Möglichkeit bietet, ADC-Instanzen für den ADM-Dienst zu integrieren und Einblick in Ihre

hybride Multi-Cloud-Bereitstellung zu erhalten. Die Auto-Onboarding-Funktion in diesem Workflow nutzt die neue ADM Service Connect-Funktion in ADC-Instanzen, mit der ADC-Instanzen mit dem ADM-Dienst verbunden werden können. Weitere Informationen finden Sie unter Berührungsarmes Onboarding von Citrix ADC-Instanzen mit Citrix ADM Service Connect.

> **Hinweis:**
>
> Dieser Workflow wird stufenweise durch Kanarienfreisetzung eingeführt (GA). Sie erhalten eine E-Mail, wenn diese Funktion in Ihrer ADM-Serviceumgebung verfügbar ist.

[NSADM-51952]

Kubernetes Servicegragramm - Zusammenfassung der Clienttransaktion

In der Kubernetes-Servicegrafik können Sie jetzt die detaillierten Transaktionsprotokolle für alle Kunden von einem bestimmten Standort aus anzeigen. Mit dieser Funktion können Sie Folgendes anzeigen:

- Reaktionszeit > 500 ms
- 5xx Fehler

> **Hinweis:**
>
> Sie können nur einige 2xx- und 4xx-Transaktionen für den ausgewählten Kunden anzeigen.

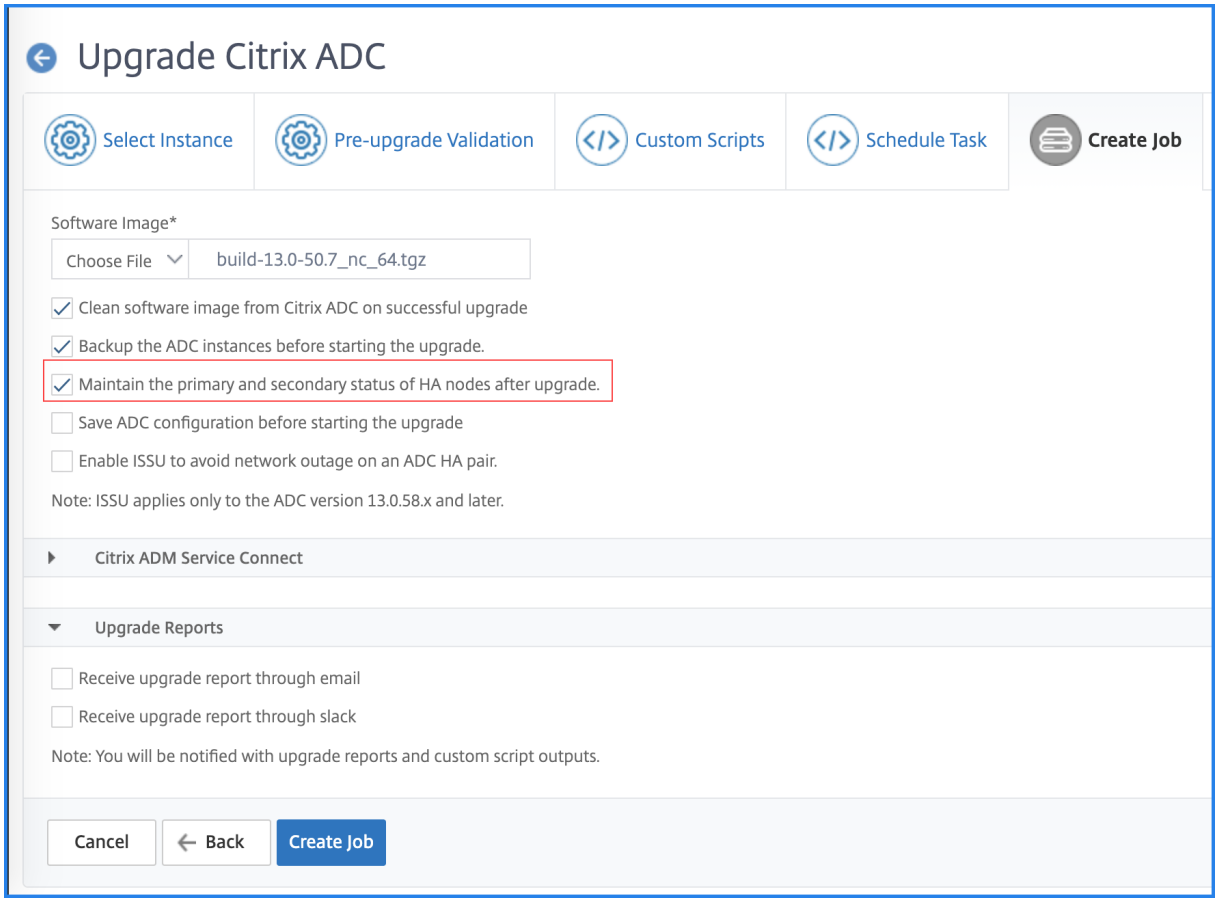
Mit dieser Funktion können Sie nicht nur die detaillierten Transaktionen untersuchen, sondern auch die Metriken (wie Client-RTT, SSL-Metriken und Server-Reaktionszeit) verstehen, die auf Client, ADC und Server aufgeteilt sind.

Weitere Informationen finden Sie unter Client-Metriken anzeigen.

[NSADM-58342]

Behalten Sie den Status von ADC-Knoten mit hoher Verfügbarkeit nach dem Upgrade

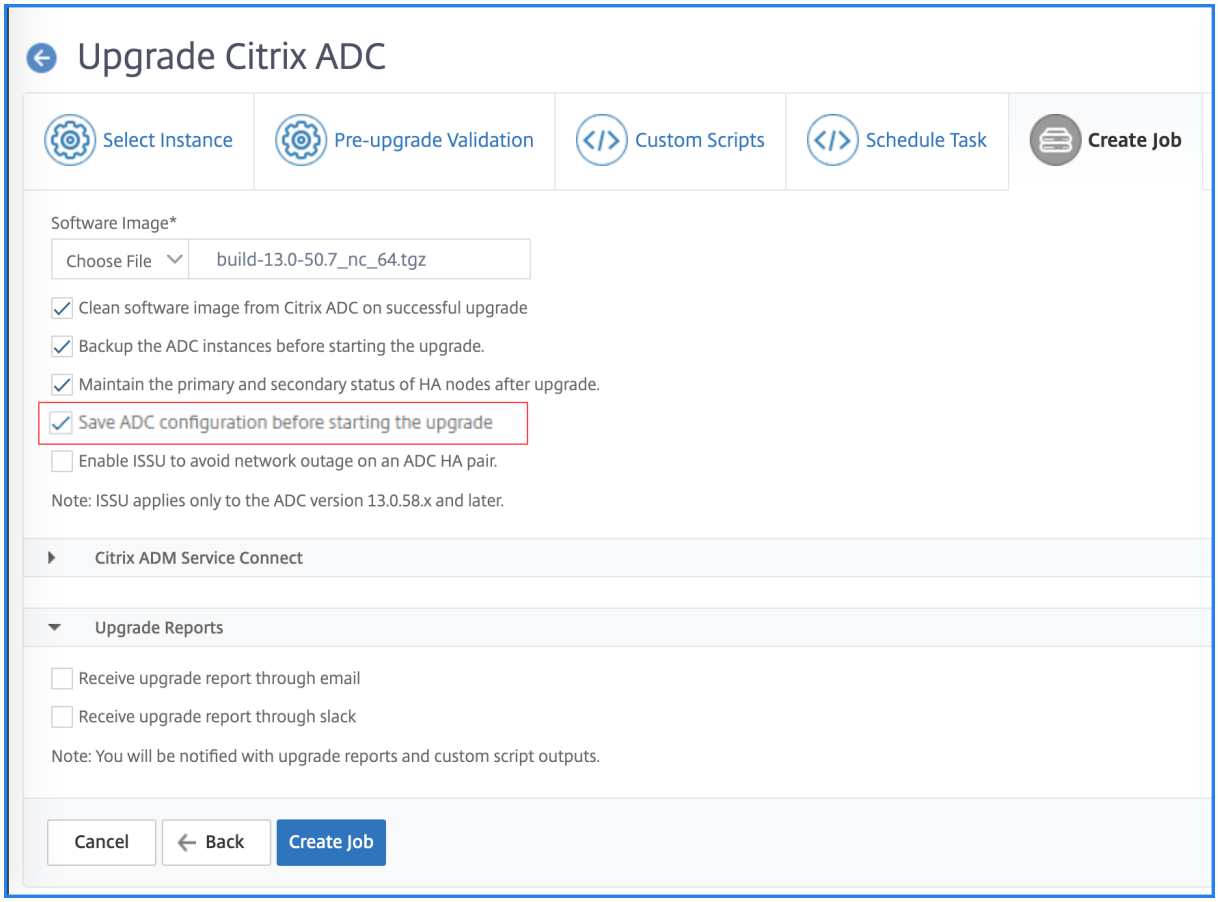
Wenn Sie einen Upgrade-Auftrag für ein ADC-Hochverfügbarkeitspaar erstellen, wird eine neue Option **Nach dem Upgrade den primären und sekundären Status von HA-Knoten beibehalten** angezeigt. Diese Option wird auf der Registerkarte “ **Job erstellen** “ angezeigt. Wählen Sie diese Option, wenn der Upgrade-Auftrag nach dem Upgrade jedes Knotens ein Failover auslösen soll. Zuvor gab es keine GUI-Option, und der Upgrade-Auftrag initiierte das Failover standardmäßig nach dem Upgrade jedes Knotens.



[NSADM-47736]

Speichern Sie die ADC-Konfiguration vor einem Upgrade

Wenn Sie einen Upgrade-Auftrag für eine ADC-Instanz erstellen, können Sie jetzt die laufende ADC-Konfiguration speichern, bevor Sie die Instanz aktualisieren. Wählen Sie die Option **ADC-Konfiguration speichern, bevor Sie die Upgrade-Option auf** der Registerkarte " **Job erstellen** " starten.



[NSADM-52470]

Problem behoben

Analytics

Die Größe der Spalten auf der Seite **Analytics > HDX Insight > Benutzer** konnte nicht angepasst werden.

[NSHELP-24288]

02. September 2020

Ändern des Zugriffstyps einer Autoscale-Anwendung

Sie können jetzt den Zugriffstyp einer Autoscale-Anwendung ändern. Wenn Sie den Zugriffstyp ändern, können Sie auch Folgendes ändern:

- FQDN-Typ
- Domänenname
- Zone der Domäne.

[NSADM-52810]

Verbesserungen des API-Gateways

Die API-Gateway-Funktion wurde jetzt mit den folgenden Funktionen verbessert:

- API Analytics: Wenn Sie auf Mehr anzeigen klicken, um eine Kachel zu erweitern, können Sie API-Instanzen und Endpunkte nach ihren Teilnamen durchsuchen. Siehe API-Analysen anzeigen.
- Bereitstellungen: Aktivieren Sie Analysen für eine API-Bereitstellung. Siehe Aktivieren der API-Analytik.
- Richtlinien: Konfigurieren Sie WAF- und BOT-Richtlinien für eine API-Bereitstellung. Siehe Hinzufügen von Richtlinien zu einer API-Definition.

  > **Hinweis**
  >
  > Bevor Sie WAF- und BOT-Richtlinien konfigurieren, stellen Sie sicher, dass Sie mit StyleBooks ein Profil in ADM erstellen. Die folgenden Standard-StyleBooks werden neu hinzugefügt, um Profile zu erstellen:
  >
  > `api-waf-profile`
  >
  > `api-bot-profile`

  Weitere Informationen finden Sie unter Erstellen von WAF- und BOT-Profilen mit StyleBook.

[NSADM-52804]

Symbole in das StyleBooks-Bundle einschließen

Wenn Sie mehrere StyleBooks aus einem Bundle importieren, können Sie jetzt jedem StyleBook Symbole hinzufügen. Laden Sie die Icons und die `icon_mapping.json` Datei in den `resources` Ordner hoch. Wenn der Name der Symboldatei und der Name des StyleBook übereinstimmen, werden die Symbole automatisch den StyleBooks zugeordnet. Andernfalls ordnen Sie StyleBooks und Symbole in der `icon_mapping.json` Datei wie folgt zu:

```
<StyleBook file name> : <icon file name>
```

Wenn Sie nur den `defaulticon` Eintrag angeben, werden alle StyleBooks im Bundle dem angegebenen Symbol zugeordnet.

```
defaulticon: <icon file name>
```

In **Application > StyleBooks**werden die importierten StyleBooks mit den zugeordneten Symbolen angezeigt.

Weitere Informationen finden Sie unter Importieren von benutzerdefinierten StyleBooks.

[NSADM-52330]

Verbesserungen der Seite “Pooled Capacity”

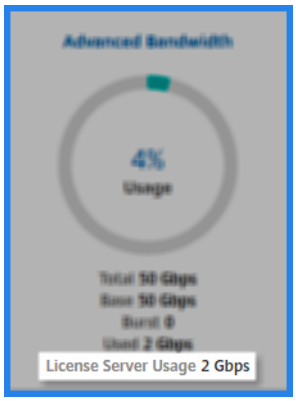
Die **Seite “Pooled Capacity”** wurde jetzt mit den folgenden GUI-Änderungen verbessert:

- **Nicht verwaltete Instanzen** — Dies ist eine neue Registerkarte. Es zeigt die Instanzen an, die in Citrix ADM erkannt, aber nicht verwaltet werden. Zuvor wurden diese Instanzen auf der Registerkarte “Dashboard” mit dem Status “Nicht verwaltete Lizenz” aufgeführt.

- Lizenzstatus - In dieser Spalte werden die folgenden Status entfernt:
  - Nicht gemanagt
  - Synchronisierung wird ausgeführt

  Die Spalte “ **Allocation Details** “ wird jetzt aus der Instanzliste entfernt.

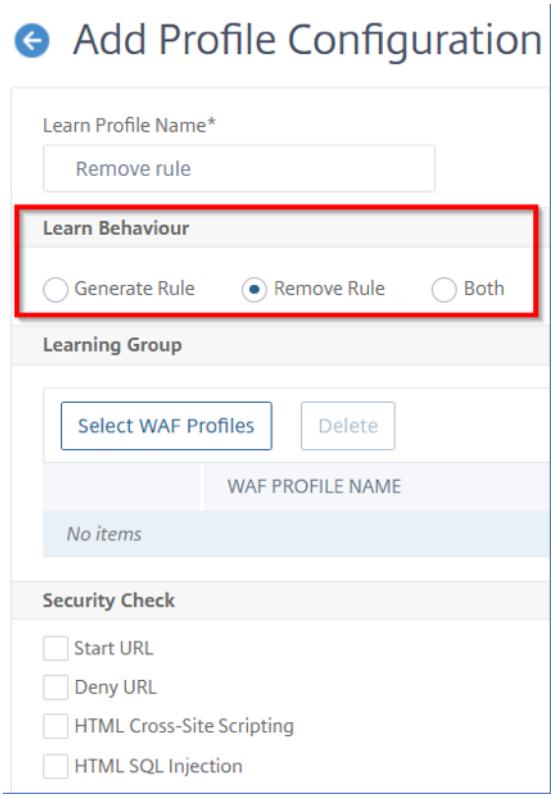
- Lizenzserver-Nutzung — Ein neuer Indikator, der der Nutzungstabelle hinzugefügt wurde. Es zeigt den gepoolten Kapazitätsverbrauch des Lizenzservers an.



[NSADM-52770]

WAF Learning Engine - Unterstützung für das Entfernen von Regeln

Sie können jetzt das Lernverhalten ändern, um die Relaxationsregeln zu entfernen, wenn in der Citrix ADC-Instanz kein eingehender Datenverkehr mit Sicherheitsprüfungen empfangen wird. Navigieren Sie zu **Analytics > Sicherheit > WAF-Learning > Profile lernen** und klicken Sie auf **Hinzufügen**, um die Optionen für das Lernverhalten anzuzeigen.



- **Regel generieren** — Generiert die Ausnahmeregel und ermöglicht es dem Administrator, die Regel entweder bereitzustellen oder zu überspringen.
- **Regel entfernen** — Entfernt die Ausnahmeregel, wenn die konfigurierte Leerlaufzeit den Schwellenwert überschreitet.
- **Beide** — Erzeugt die Ausnahmeregeln und entfernt die Regel, wenn kein eingehender Datenverkehr vorhanden ist.

Sie können die Option Regel entfernen nur für die folgenden Sicherheitsüberprüfungen anwenden:

- Start-URL
- URL verweigern
- HTML Cross-Site-Scripting
- HTML SQL Injection

Wenn eine Regel entfernt wird, wird in Slack, SMS, Email und ServiceNow eine Benachrichtigung generiert. Sie können Details auch im **WAF Learning Dashboard**anzeigen.

Weitere Informationen finden Sie unter Konfigurieren Sie das Lernprofil.

[NSADM-52871]

Verletzungen der App-Sicherheit - Bot

In **App Security Violations**können Sie jetzt **Website-Scanner** unter der Kategorie BOT-Verstoß anzeigen. Weitere Informationen finden Sie unter Verletzung der App-Sicherheit.

[NSADM-53289]

Verletzungen der App-Sicherheit - Netzwerk

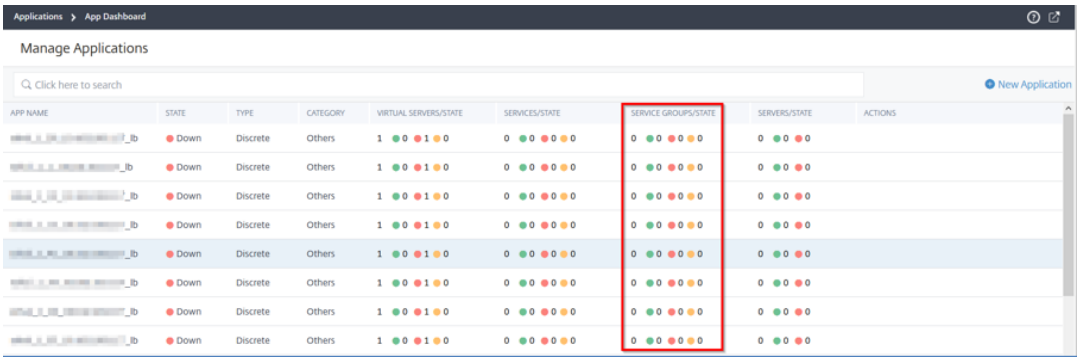
In **App Security Violations**können Sie jetzt Small Window Attack unter der Kategorie Netzwerkverletzung anzeigen. Weitere Informationen finden Sie unter Verletzung der App-Sicherheit.

[NSADM-46023]

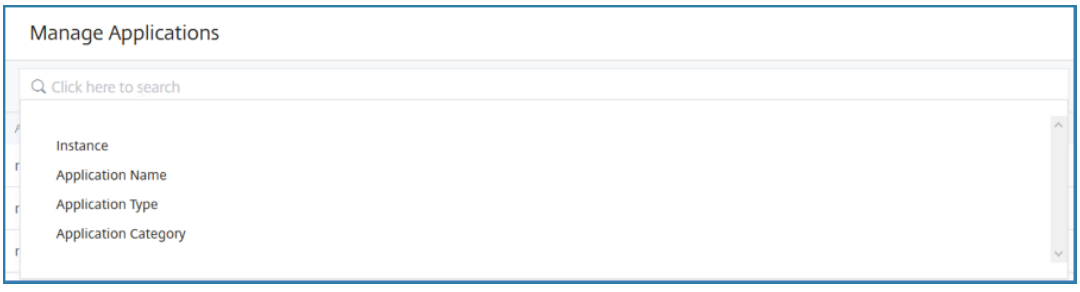
Verbesserungen am App Dashboard

In **App Dashboard**können Sie jetzt die folgenden Verbesserungen anzeigen:

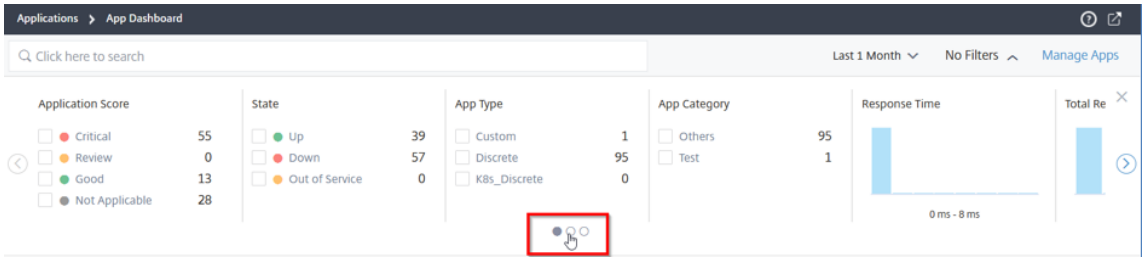
- Auf der Seite **“Anwendungen verwalten** “:
  - Sie können die gesamten Servicegruppen und den Status der Servicegruppen anzeigen, die “Nach oben”, “Nach unten” oder “Ausgelassen” sind.



  - Sie können den Mauszeiger auf die Suchleiste setzen und die Kategorie auswählen, um die Suche zu verfeinern.



- Auf der **App Dashboard-Seite** wird die Bildlaufleiste durch einen Karussell-Schieberegler ersetzt, der Ihnen den Zugriff auf alle Optionen erleichtert.



[NSADM-52759]

Web Insight-Dashboard

Sie können jetzt eine verbesserte Web Insight-Funktion anzeigen, die detaillierte Metriken für Webanwendungen, Clients und Citrix ADC-Instanzen bietet. Dieses verbesserte Web Insight ermöglicht es Ihnen, die vollständigen App-Informationen aus den Perspektiven von Leistung und Nutzung gemeinsam auszuwerten und zu visualisieren. Als Administrator können Sie Web Insight anzeigen für:

- Eine Anwendung. Navigieren Sie zu **Anwendungen > Dashboard**, klicken Sie auf eine Anwendung und wählen Sie die Registerkarte **Web Insight** aus, um die detaillierten Metriken anzuzeigen. Weitere Informationen finden Sie unter Analyse der Anwendungsnutzung.
- Alle Anwendungen. Navigieren Sie zu **Applications > Web Insight** und klicken Sie auf die einzelnen Registerkarten (Anwendungen, Clients, Instanz), um die folgenden Metriken anzuzeigen:

Anwendungen	Kunden	Instanzen
Anwendung	Kunden	Instanzmetriken
Server	Geo-Auslösevorstellungen	Anwendungen
Domänen	HTTP-Anforderungsmethoden	Domänen
Geo Standorte	HTTP-Antwortstatus	URLs
URLs	URLs	HHTP-Request-Methoden
HTTP-Anforderungsmethoden	Betriebssystem	HTTP-Antwortstatus
HTTP-Antwortstatus	Browser	Kunden
SSL-Fehler	SSL-Fehler	Server
SSL-Nutzung	SSL-Nutzung	Betriebssystem
-	-	Browser

Weitere Informationen finden Sie unter Web Insight-Dashboard.

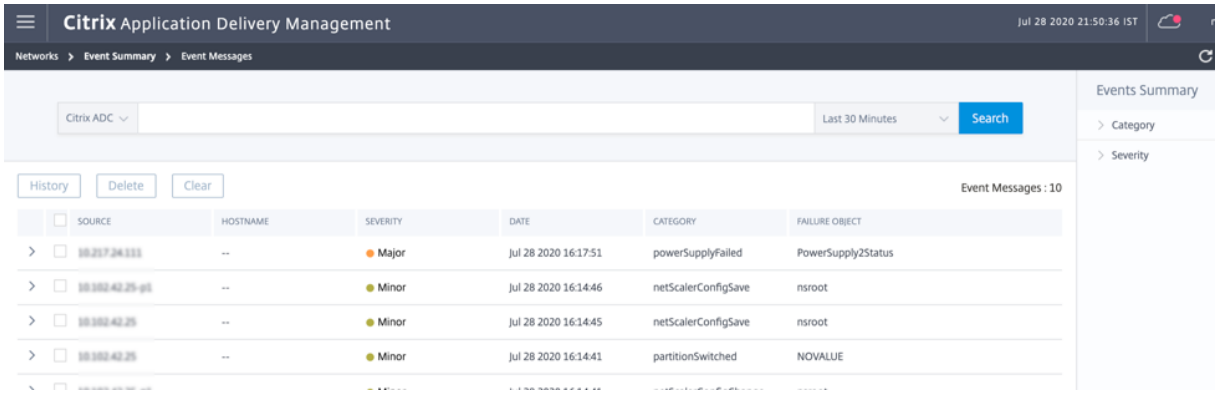
Unterstützung für ADM-Agenten auf GCP

Citrix ADM-Agenten werden jetzt auf Google Cloud Platform (GCP) unterstützt. Weitere Informationen finden Sie unter Installieren Sie den Citrix ADM Agenten auf GCP

[NSADM-31980]

Neue Suchfunktion für Ereignisnachrichten

In **Netzwerke > Ereignisse > Ereignisnachrichten**können Sie jetzt logische Operatoren wie AND/OR zum Beispiel zur Suche verwenden. Sie können Daten auch mithilfe benutzerdefinierter Zeiträume filtern. Außerdem bietet das Übersichtsfeld für Ereignisse eine Anzahl der einzelnen Ereigniskategorien und jeden Schweregrads.



Behobene Probleme

Analytics

Der Analysebericht in Citrix ADM zeigt nur Daten von 14 bis 28 Tagen an, selbst nachdem die Zeitdauer als 1 Monat ausgewählt wurde

[NSHELP-23836]

System

ADM generiert nicht das technische Supportpaket für Agenten, wenn die Dateigröße groß ist.
[NSHELP-24620]

Lizenzierung

Wenn Sie eine Lizenzdatei auf der ADM-GUI mit einem Lizenzzugangscode installieren (**Netzwerke > Lizenzen > Lizenzdatei hinzufügen**), wird die Meldung “Lizenzinformationen nicht analysieren” angezeigt. Das Problem tritt auf, wenn die Lizenzdateien auf einem Jazz-Server gespeichert werden,

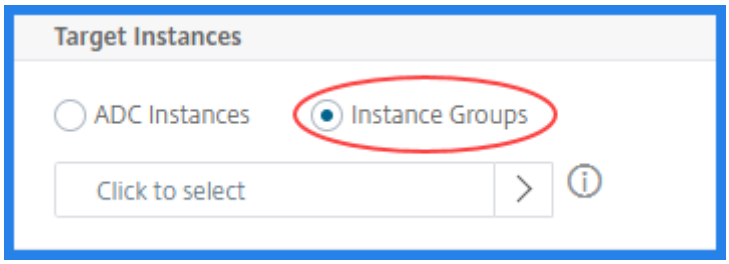
der nicht unterstützt wird. Mit diesem Fix werden Jazz-Server für das Hinzufügen von Lizenzdateien zu ADM unterstützt.

[NSADM-59338]

17. August 2020

Zielinstanzgruppen auswählen, um ein Konfigurationspaket bereitzustellen

Wenn Sie auf der Seite " **StyleBooks > Configurations** " eine neue Konfiguration hinzufügen, können Sie jetzt eine ADC-Instanzgruppe auswählen, um ein Konfigurationspaket bereitzustellen. Und diese Konfiguration gilt für alle Instanzen in der Gruppe. Wählen Sie dazu im Bereich **Target Instanzen die Option**Instanzgruppen** aus.



[NSADM-56605]

Geben Sie eine IP-Adresse aus dem IPAM-Netzwerk

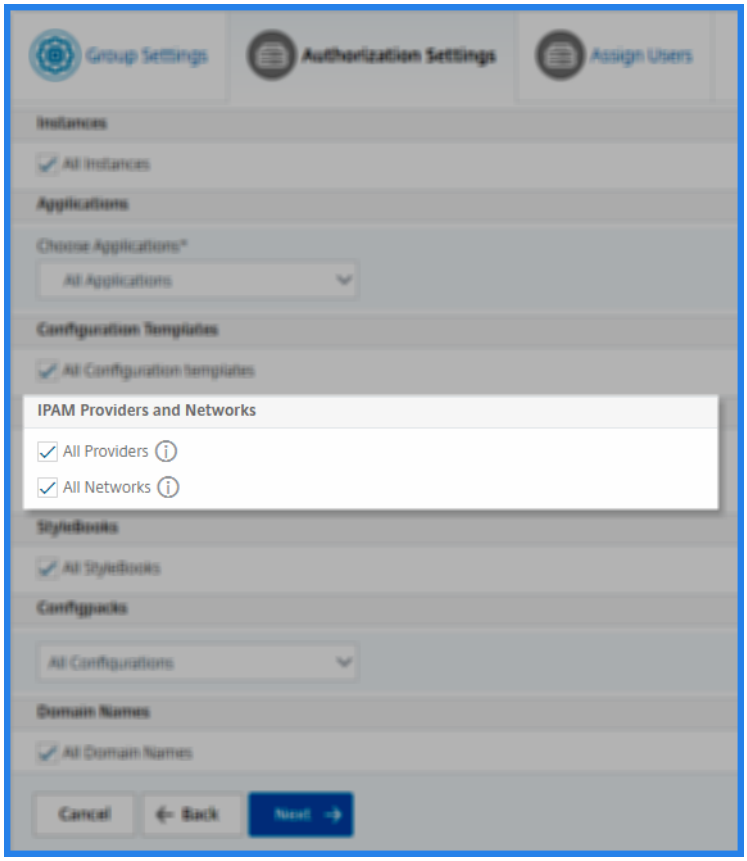
Wenn Sie den `dynamic-allocation` Attributwert in der **StyleBook-Definition** auf true setzen, kann ein Benutzer jetzt eine IP-Adresse aus dem ausgewählten IPAM-Netzwerk angeben. Der ADM weist die angegebene IP-Adresse einem virtuellen Server zu.

[NSADM-56068]

Verwalten der Benutzerautorisierung für IPAM

Als Administrator können Sie jetzt **IPAM-Anbieter** und -Netzwerke auswählen und einem Benutzer oder einer Gruppe Zugriff gewähren.

1. Navigieren Sie auf die Seite **System > User Administration**.
2. Fügen Sie IPAM-Anbieter und Netzwerke auf der Registerkarte **Autorisierungseinstellungen** hinzu.



[NSADM-54377]

Verbesserungen der integrierten Funktionen von StyleBook

Verwenden Sie beim Erstellen von StyleBook-Definitionen die folgenden integrierten Funktionen mit ihren verbesserten Funktionen:

- `replace()` — Ersetzt jetzt die in der Liste angegebenen Zeichen oder Zeichenfolgen. Zuvor konnten Sie keine Listeneingabe für diese Funktion bereitstellen.
- `ip()` — Akzeptiert jetzt einen Ganzzahlwert und wandelt diesen in eine entsprechende IP-Adresse um. Es unterstützt auch die Addition und Subtraktion von IP-Adressen.
- `int()` — Akzeptiert jetzt eine IPv4-Adresse und gibt den entsprechenden ganzzahligen Wert zurück.

[NSADM-56310],[NSADM-55209]

Verwenden Sie neue integrierte Funktionen von StyleBook

Beim Erstellen von StyleBook-Definitionen unterstützt ADM StyleBooks jetzt die folgenden integrierten Funktionen:

- `distinct()` - Extrahiert die eindeutigen Elemente aus einer Inputliste.
- `split()` - Teilt eine Eingabezeichenfolge in Listen auf.

[NSADM-56103],[NSADM-55958]

Konfigurieren einer Autoscale-Gruppenanwendung ohne StyleBooks

Sie können jetzt eine Anwendung in einer ADC Autoscale-Gruppe konfigurieren, ohne StyleBooks auszuwählen. Wenn Sie jedoch in Zukunft StyleBooks verwenden möchten, bearbeiten und erneut einreichen, wählen Sie im Bestätigungsfenster **Ja** aus.

Zuvor war die Auswahl von StyleBook erforderlich, um eine Autoscale-Gruppenanwendung zu konfigurieren.

[NSADM-52814]

Verbesserungen bei Gateway Insight

In **Gateway Insight**können Sie jetzt Folgendes anzeigen:

- Eine Suchleiste, mit der Sie Ergebnisse anhand des Benutzernamens filtern können. Navigieren Sie zu **Analytics > Gateway Insight > Benutzer**, um die Suchleiste für **Benutzer** und **Aktive Benutzer** anzuzeigen. Platzieren Sie den Mauszeiger auf die Suchleiste, wählen Sie **Benutzername** und geben Sie einen Benutzernamen ein, um die Ergebnisse zu filtern.

- Eine Geomap, die die Benutzerinformationen basierend auf dem geografischen Standort des Benutzers anzeigt. Als Administrator ermöglicht Ihnen diese Geomap, die Zusammenfassung der gesamten Benutzer, der gesamten Apps und der Gesamtsitzungen für einen bestimmten Standort anzuzeigen.

    1. Navigieren Sie zu **Analytics > Gateway Insight**, um die Geo-Karte anzuzeigen

2. Klicken Sie auf ein Land. Beispiel: USA
   Die Geokarte zeigt die Details wie Benutzerliste, aktive Sitzungen, beendete Sitzungen, Anwendungen für das ausgewählte Land an.

- Eine Geomap für Gateways, mit der Sie Benutzer basierend auf einem bestimmten Standort filtern können.

  1. Navigieren Sie zu **Analytics > Gateway Insight > Gateways**
  2. Wählen Sie einen Gateway-Domainnamen aus, um die Geomap anzuzeigen
  3. Klicken Sie auf ein Land. Zum Beispiel United States

     Die Geomap zeigt die Details wie Benutzerliste, aktive Sitzungen, beendete Sitzungen und Anwendungen für das ausgewählte Land an.

[NSADM-55504],[NSADM-55506]

Verletzungen der App-Sicherheit — Netzwerk

In **App Security Violations**können Sie jetzt **SYN Flood Attack** unter der Kategorie Netzwerkverletzung anzeigen. Weitere Informationen finden Sie unter Verletzungen der App-Sicherheit.

[NSADM-46021]

Verbesserungen des globalen Service-Graphen

In Global Service Graph können Sie jetzt die Suchleiste verwenden, um Ergebnisse zu filtern. Als Administrator können Sie mit dieser Suchleiste schnell auf eine bestimmte Instanz/einen bestimmten Client/eine bestimmte Anwendung/Rechenzentrum eingrenzen, wenn Sie:

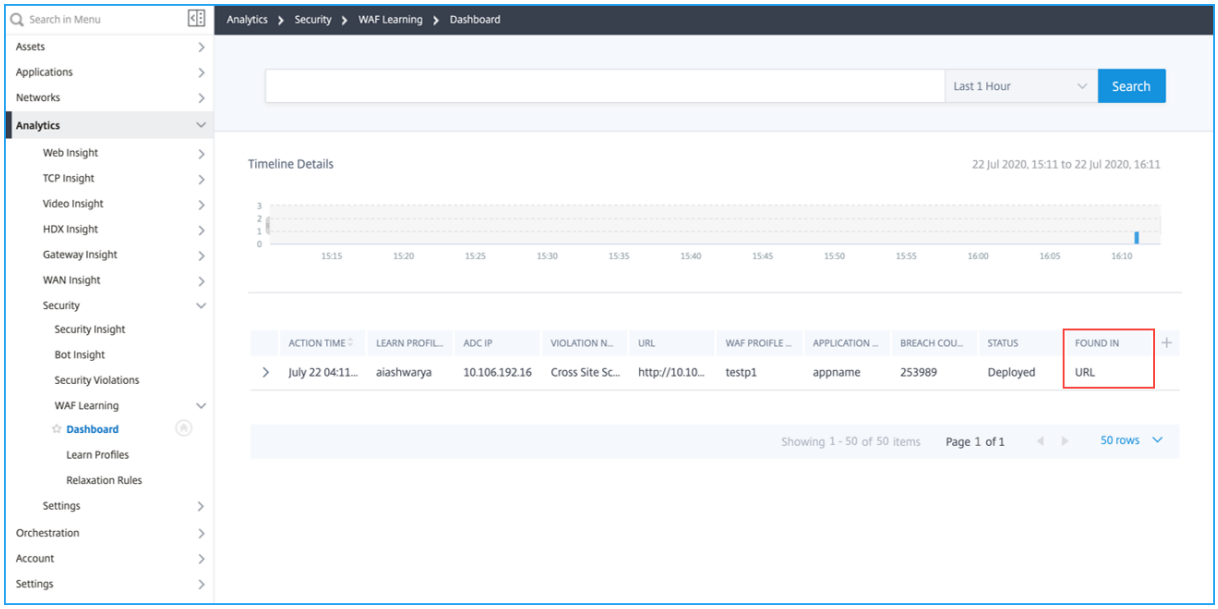
- Ein großes Unternehmen mit vielen Rechenzentren
- Viele Citrix ADC-Instanzen für jedes Rechenzentrum konfiguriert
- Viele Anwendungen konfiguriert, die über jede Citrix ADC-Instanz bereitgestellt oder darauf zugegriffen werden
- Clients, die von verschiedenen Standorten aus auf die Anwendung zugreifen

Weitere Informationen finden Sie unter Service Graph - Ganzheitliche Sicht auf alle Anwendungen

[NSADM-52149]

Verbesserung der Protokollnachrichten für standortübergreifende Skriptverletzungen

Das **WAF-Lern-Dashboard** mit bereitgestellter Website-Scriptverletzung ermöglicht es Ihnen jetzt, ein neues Attribut anzuzeigen. Dieses neue Attribut gibt den Speicherort für standortübergreifende Skriptverletz Der Verstoßort kann Formularfeld, URL, Header, Cookie oder andere Orte sein.



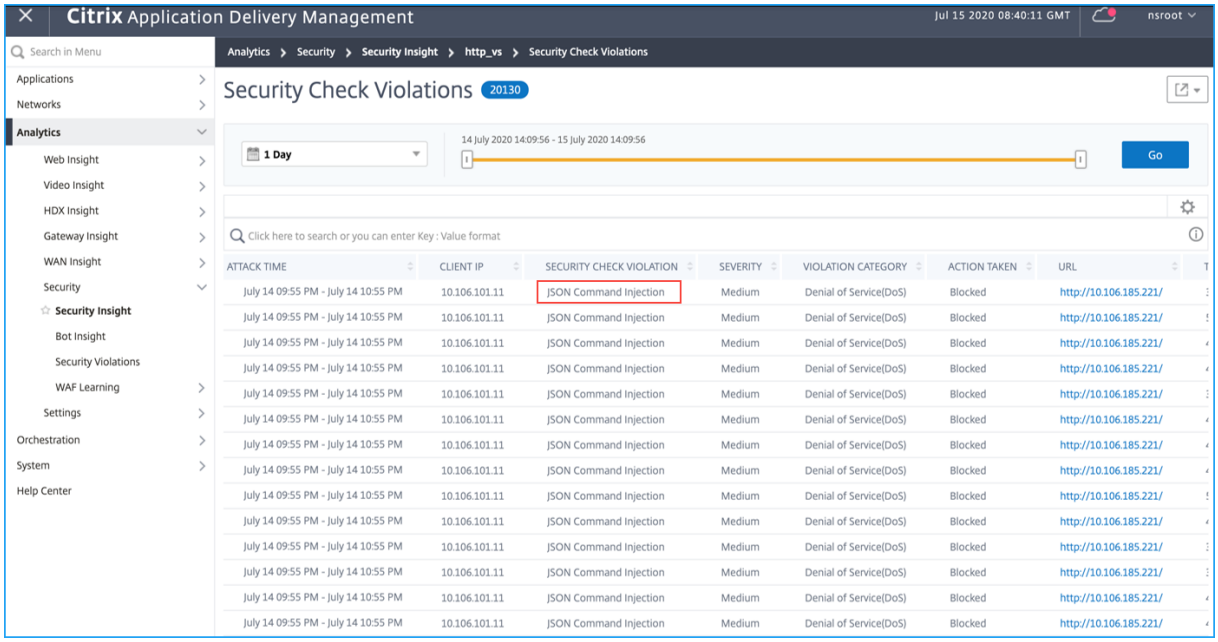
[NSADM-52941]

Security Insight — JSON Command Injection

In **Security Insight**können Sie jetzt einen neuen Verstoßtyp, JSON Command Injection, anzeigen. Um die JSON Command Injection-Verletzung in Security Insight zu generieren, müssen Sie den folgenden Befehl in der Citrix ADC-Instanz konfigurieren:

```
add appfw profile abc_js -type JSON -startURLaction none -starturlclosure
off -jsoncmdinjectionaction block log stats -jsoncmdinjectiontype cmdkeyword
```

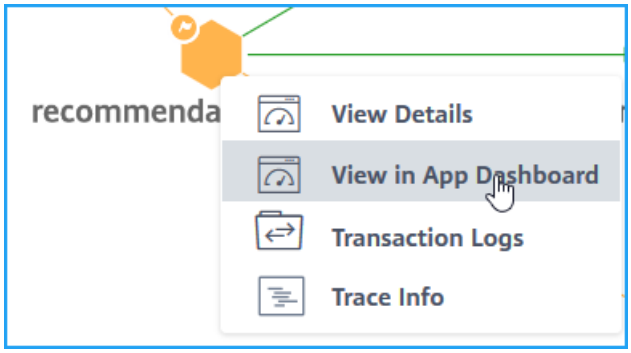
Nach der Konfiguration können Sie den JSON Command Injection-Angriff in Security Insight anzeigen.



[NSADM-52869]

Servicegragramm für Kubernetes-Anwendung — App-Details im App-Dashboard anzeigen

Wenn Sie im Servicegrar auf einen Dienst klicken und **In App Dashboard anzeigen**auswählen, werden die Details für die ausgewählte **App im App-Dashboard**angezeigt.



Weitere Informationen finden Sie unter Anwendungsdetails für Microservices-Anwendungen.

[NSADM-56583]

Anzeigen von Sicherheitseinblicken und Details zu Bot-Insight-Angriffen in App Security Violations

In **App Security Violation**können Sie jetzt Sicherheitsinformationen und Details zu Bot-Insight-Angriffen unter den Kategorien **WAF** bzw. **Bot** anzeigen. Navigieren Sie zu **Analytics > Sicherheit > Sicherheitsverletzungen**, um die folgenden Verstöße anzuzeigen:

WAF	Bot
Pufferüberlauf	Crawler
Inhaltstyp	Feed Fetcher
Konsistenz von Cookies	Link Checker
CSRF-Formular-Tagging	Marketing
URL verweigern	Scraper
Konsistenz von Formularfeldern	Screenshot Creator
Feld-Formate	Suchmaschine
Maximale Uploads	Service Agent
Referrer Header	Sitemonitor
Sicherer Handel	Geschwindigkeitstester
Sicheres Objekt	Tool
HTML SQL Inject	Nicht kategorisiert
Start-URL	Viren-Scanner
Site-übergreifendes Scripting **(XSS)**	Vulnerability Scanner
XML DoS	DeviceFP-Wartezeit überschritten
XML-Format	Ungültiger DeviceFP
XML WSI	Ungültige Captcha-Antwort
XML SSL	Captcha-Versuche wurden überschritten
XML-Anhang	Gültige Captcha-Antwort
XML SOAP	Captcha-Kunde stummgeschaltet
XML-Validierung	Captcha-Wartezeit überschritten
Andere	Größenbeschränkung der Anfrage überschritten
IP-Reputation	Ratenlimit überschritten
HTTP DOS	Sperrliste (IP, Subnetz, Richtlinienausdruck)
TCP Small Window	Positivliste (IP, Subnetz, Richtlinienausdruck)
Signatur-Verletzung	Null-Pixel-Anfrage
Datei-Upload-Typ	Quell-IP
JSON Site-Cross-Scripting **(XSS)**	Host

WAF	Bot
JSON SQL	Geografischer Standort
JSON DOS	URL
Befehlseinschleusung	
Infer Content Type XML	
Cookie Hijack	

[NSADM-54296]

Spitzenauslastung und Lean-Periodenanalyse - Bewerten der App-Skalierungsgrenzen und Identifizieren des Top-5-App-Wartungs

Als Administrator müssen Sie den Datenverkehr analysieren und einen geeigneten Zeitpunkt finden, um zu entscheiden:

- Wenn Sie die Anwendung in der Produktionsumgebung skalieren möchten
- Wenn Sie die Ausfallzeit der Anwendung planen möchten

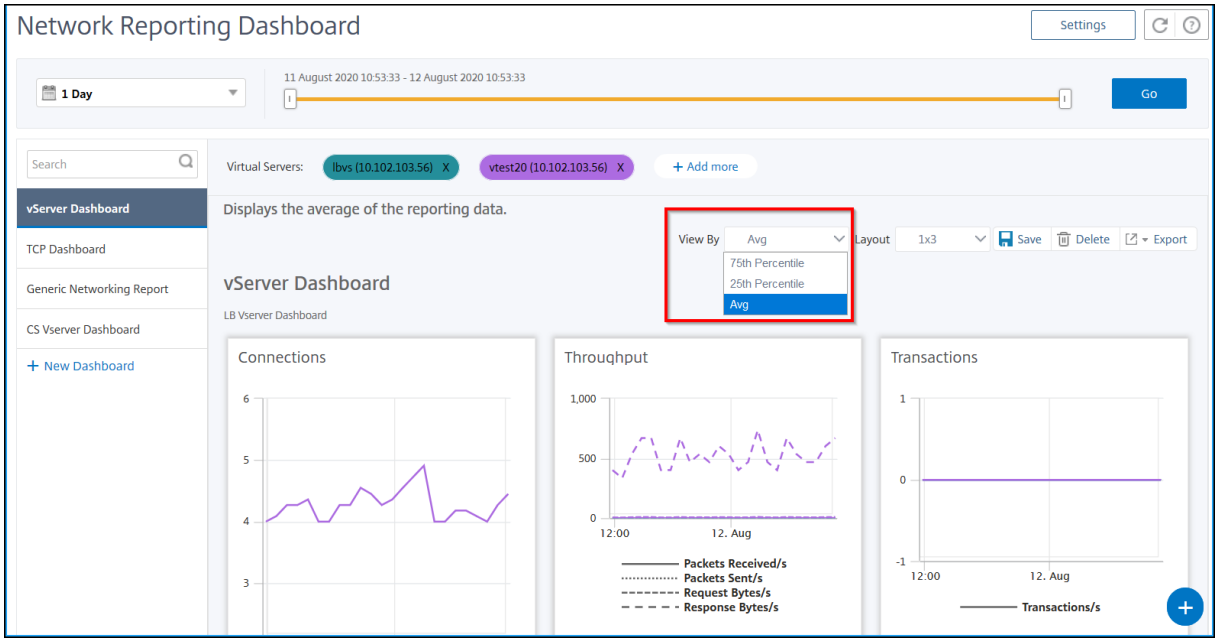
Die Analysefunktion für Spitzenauslastung und Lean Period in Citrix ADM ermöglicht es Ihnen, die wichtigsten Kennzahlen für eine ausgewählte Zeitdauer zu analysieren. Anhand dieser Metriken können Sie den Datenverkehr analysieren und entscheiden, wann Sie die Webanwendung vergrößern oder eine geplante Ausfallzeit planen möchten.

Weitere Informationen finden Sie unter Anwendungen Spitzennutzung und Lean Period Analytics.

[NSADM-52167],[NSADM-52140]

Anzeigen von Netzwerkberichtsdaten durch Anwendung von Aggregationen

Sie können jetzt Aggregationen auf die Netzwerkleistungsdaten anwenden und die Anwendungsleistung im Dashboard anzeigen. Sie können die Ergebnisse auch basierend auf Ihren Anforderungen exportieren. Mithilfe dieser Aggregationen, die auf die Daten angewendet werden, können Sie analysieren und sicherstellen, dass alle Ressourcen optimal genutzt werden. Navigieren Sie zu **Netzwerk > Network Reporting** und wählen Sie die Zeitdauer 1 Tag oder später aus, um die Option Anzeigen nach zu erhalten.



In den vorhandenen Daten können Sie Aggregationen anwenden, indem Sie die Option aus der Liste **Anzeigen nach** auswählen. Weitere Informationen finden Sie unter Anzeigen von Netzwerkberichtsdaten durch Anwenden von Aggregationsfiltern

[NSADM-56494]

Wählen Sie den Evaluierungslizenztyp in der intelligenten Bereitstellung

Sie können jetzt die ADM Autoscale-Lösung mit der Evaluierungslizenz erleben. Wenn Sie die Option **Smart Deployment** wählen, um ADC-Instanzen in AWS bereitzustellen, können Sie jetzt den Lizenztyp **Evaluierung** auswählen. Mit dieser Option können Sie das Citrix ADC VPX Express-Produkt bereitstellen. Und es kann bis zu drei Instanzen Autoscale.

[NSADM-52143]

Behobene Probleme

Lizenzierung

Die Lizenzen in Citrix ADM sind aufgrund des Neustarts des Agenten deaktiviert.

[NSHELP-23539]

Netzwerke

Der Status des Citrix ADM-Agenten wird angezeigt `reset:requested`, auch wenn die Agentenregistrierung erfolgreich ist.

[NSHELP-23413]

StyleBooks

Wenn Sie eine Autoscale-Gruppenanwendung mit standardmäßigen StyleBooks konfigurieren, werden die DNS- und UDP-Monitortypen nicht unterstützt. Mit diesem Fix werden die Versionen der folgenden Autoscale-Gruppe StyleBooks aktualisiert:

- lb-mon-autoscale-v1.5
- cs-lb-mon-autoscale-v1.4

[NSADM-55982]

24. Juli 2020

Verletzungen der App-Sicherheit - Netzwerk

Sie können jetzt den Segment Smack Attack als Teil der Netzwerkverletzungen in App Security Violations anzeigen. Weitere Informationen finden Sie unter Verletzungen der App-Sicherheit.

[NSADM-46025]

Service-Diagramm für Kubernetes-Anwendungen - Client-Metriken zur Problembehandlung anzeigen

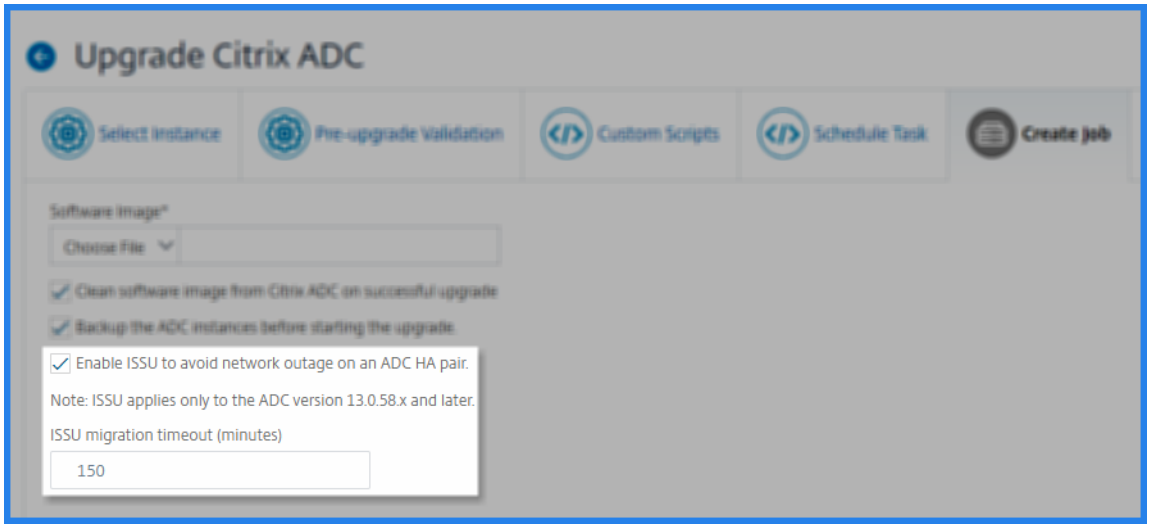
In Service Graph für Kubernetes-Anwendungen können Sie jetzt anzeigen, von welchem Standort der Client auf den Service zugreift. Als Administrator können Sie die Client-Metriken visualisieren und die Probleme analysieren, die vom Kunden auftreten.

Weitere Informationen finden Sie unter Details im Service-Diagramm anzeigen.

[NSADM-54335]

Unterstützung für In-Service-Software-Upgrade

Sie können jetzt die Option In-Service-Software-Upgrade (ISSU) auswählen, während Sie einen Upgrade-Auftrag erstellen. ISSU stellt das Upgrade auf null Ausfallzeiten bei einem ADC-Hochverfügbarkeitspaar sicher. Die ISSU-Funktion bietet eine Migrationsfunktion, die die vorhandenen Verbindungen während des Upgrades berücksichtigt. Sie können also ein ADC HA-Paar ohne Ausfallzeiten aktualisieren.



[NSADM-43357]

Listen Sie die ADM IP Address Management (IPAM) -Netzwerke in StyleBooks dynamisch auf

Sie können jetzt ein StyleBook erstellen, das es einem Benutzer ermöglicht, ein ADM-IPAM-Netzwerk auszuwählen, von dem er automatisch eine IP-Adresse zuweist. Die IPAM-Netzwerkliste wird dynamisch von ADM abgerufen. Zuvor konnten Sie die IPAM-Netzwerke auswählen, die in der **StyleBook-Definition** erwähnt werden.

In der Parameterdefinition von `dynamic-allocation` wird jetzt ein neues Attribut hinzugefügt `type :ipaddress`. Es kann **`true`** oder **`false`** als Input dauern. Wenn Sie seinen Wert auf festlegen **`true`**, kann ein Benutzer ein Netzwerk aus der Liste der IPAM-Netzwerke in ADM auswählen. Anschließend weist der ADM automatisch eine IP-Adresse aus dem ausgewählten Netzwerk zu.

Beispiel:

```
1   -
2     name: virtual-ip
3     label: ”Load Balancer IP Address”
4     type: ipaddress
5     dynamic-allocation: true
6     required: true
7  <!--NeedCopy-->
```

In diesem Beispiel listet das `virtual-ip` Feld die IPAM-Netzwerke auf, die sich in ADM befinden. Wählen Sie ein Netzwerk aus der Liste aus, um eine IP-Adresse automatisch aus dem Netzwerk zuzuweisen. Die IP-Adresse wird beim Löschen der Konfiguration wieder an das Netzwerk freigegeben.

[NSADM-54246]

Verbesserungen der Benutzerberechtigung für StyleBooks und Konfigurationspakete

Als Administrator können Sie jetzt auf der Seite **Konto > Benutzerverwaltung > Gruppen eine bessere Kontrolle über die Autorisierung bestimmter StyleBooks und Konfigurationspakete für Benutzergruppen** haben. Die Bereiche **StyleBooks** und **Configpacks** in den **Autorisierungseinstellungen** wurden jetzt mit den folgenden Änderungen verbessert:

- **StyleBooks** — Sie können jetzt die autorisierte Liste von StyleBooks mit einem Filterausdruck angeben, der reguläre Ausdrücke enthalten kann.

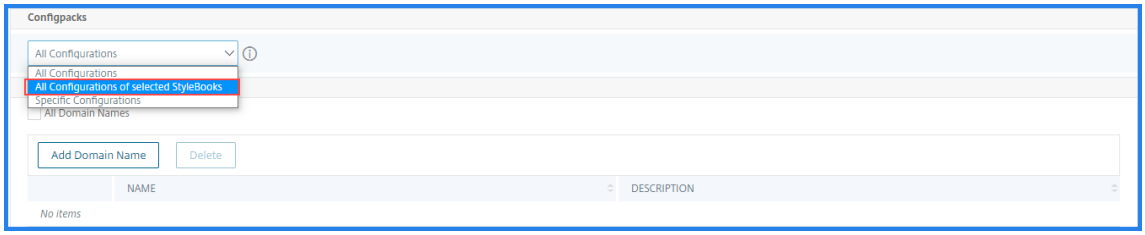
  Beispiel:

  ```
  name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND version=1.0
  ```

  Diese Query listet die StyleBooks auf, die die folgenden Bedingungen erfüllen:

  - StyleBook-Name ist entweder `lb-mon` oder `lb`.
  - StyleBook Namespace ist `com.citrix.adc.stylebooks`.
  - StyleBook-Version ist `1.0`.

- **Konfigurationspakete** — Sie können den Benutzer jetzt für Konfigurationspakete autorisieren, die zu den ausgewählten StyleBooks gehören. Wählen Sie dazu im Abschnitt **Configpacksdie Option Alle Konfigurationen der ausgewählten StyleBooks** aus.

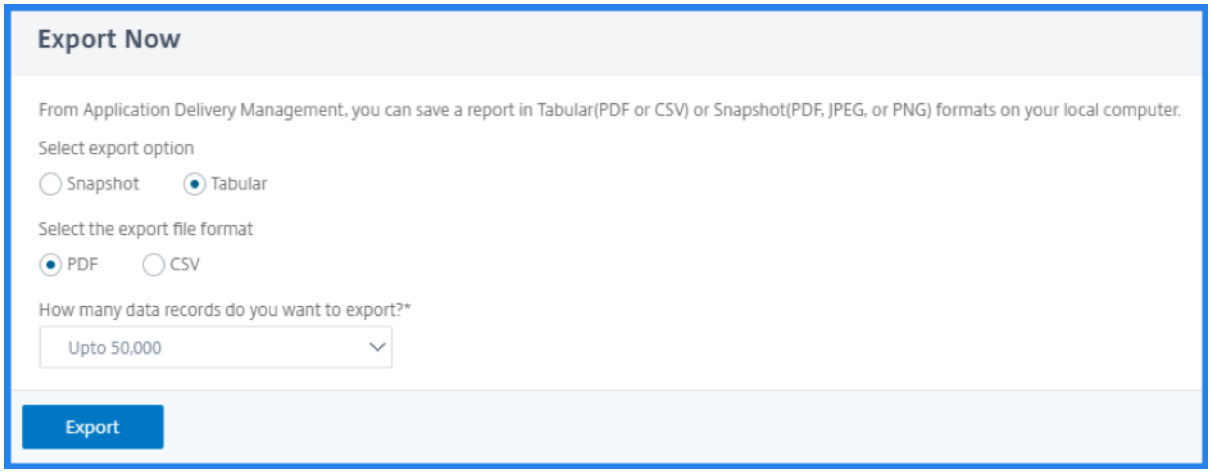


[NSADM-52334]

15. Juli 2020

Exportieren von ADM-Berichten in einem tabellarischen Format

Sie können jetzt ADM-Berichte in einem tabellarischen Format oder einem Snapshot exportieren. Sie können auch auswählen, wie viele Datensätze in einem tabellarischen Format exportiert werden sollen. Zuvor konnten Sie Berichte nur als Momentaufnahme exportieren.

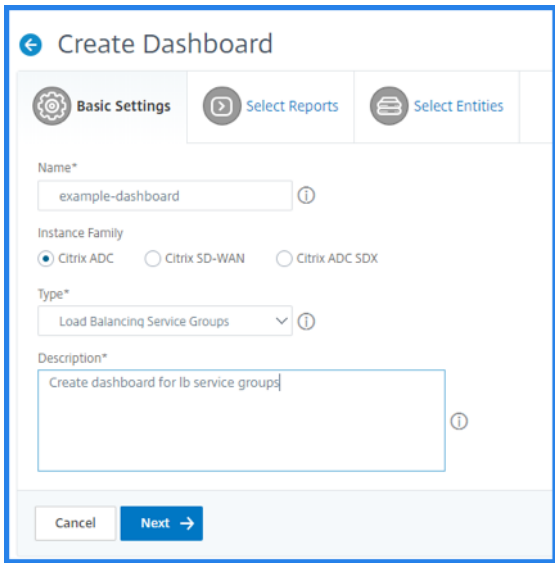


Weitere Informationen finden Sie unter Exportieren oder Planen von Exportberichten.

[NSADM-52461]

Generieren von Netzwerkberichten für Lastenausgleich Dienstgruppen

Sie können jetzt ein Dashboard für die Netzwerkberichterstattung sowohl für Lastenausgleichs-Servicegruppen als auch für Services erstellen. Zuvor konnten Sie ein Dashboard nur für Lastenausgleichsdienste erstellen.



Dieses Dashboard kann die folgenden Berichte für die ausgewählten Dienstgruppen anzeigen:

- Verbindungen: für die Client- und Server-Verbindungszähler.
- Durchsatz: für Anforderungs- und Antwortbytes Zähler.
- Time to First Byte (TTFB): für die durchschnittliche Zeit, die zum Senden eines Anforderungspakets an eine Dienstgruppe und das Empfangen des ersten Pakets von der Servicegruppe aufgefordert wird. Diese Antwortzeit wird als TTFB bezeichnet.

Weitere Informationen finden Sie unter Netzwerkberichterstattung.

[NSADM-51596]

Unterstützung für Authentifizierung, Autorisierung und Auditing von Polling- und Netzwerkberichten

Citrix ADM fragt jetzt Authentifizierungs-, Autorisierungs- und Auditing-Ereignisse (Citrix ADC AAA) von einer ADC-Instanz ab und ermöglicht es Ihnen, ihren Trend in Network Reporting zu visualisieren. Die ADM-GUI enthält die folgenden Citrix ADC AAA-Netzwerkberichte zum Erstellen eines Dashboards:

- **HTTP-Authentifizierungserfolg gegenüber Fehlern**
- **Erfolg der Nicht-HTTP-Authentifizierung im Vergleich zu Fehlern**
- **AAA-Sitzungen**
- **Aktuelle AAA-Sitzungen**
- **Aktuelle ICAOnly-Sitzungen**
- **Aktuelle ICAOnly-Verbindungen**
- **Aktuelle ICA- (SmartAccess-) Verbindung**
- **Erfolg bei der Authentifizierung und Misserfolge**

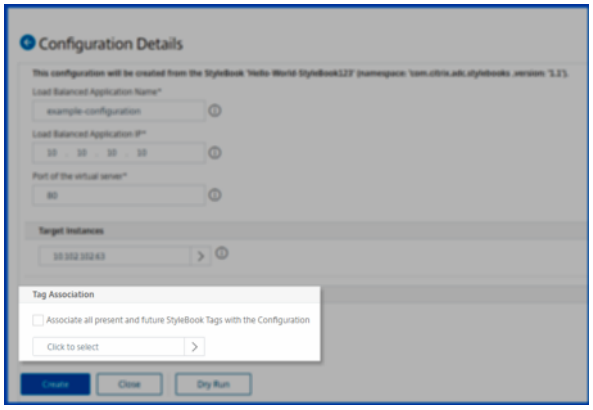
Weitere Informationen finden Sie unter Netzwerkberichterstattung.

[NSADM-51372]

Verknüpfen Sie StyleBook-Tags mit ihrer Konfiguration

In StyleBooks wird der Begriff **Label** in **Tag**umbenannt. Sie können jetzt die StyleBook-Tags seinem Konfigurationspaket zuordnen. Sie können also die Konfigurationspakete mithilfe der StyleBook-Tags selbst durchsuchen.
Wenn Sie ein Konfigurationspaket erstellen, verwenden Sie eine der folgenden Optionen im Abschnitt **Tag-Zuordnung** :

- **Verknüpfen Sie alle gegenwärtigen und zukünftigen StyleBook-Tags mit der Konfiguration** — Diese Option ordnet alle StyleBook-Tags einem Konfigurationspaket zu. Es stellt auch sicher, dass Sie die neuen Tags verknüpfen, die Sie den StyleBooks in Zukunft hinzufügen könnten.
- **Tags auswählen** — Diese Option zeigt die Tags des ausgewählten StyleBook an. Sie können die erforderlichen StyleBook-Tags auswählen und einem Konfigurationspaket zuordnen.



Weitere Informationen finden Sie unter Erstellen Sie ein Tag für das StyleBook.

[NSADM-53600]

StyleBooks unterstützen bedingte Parameter

Sie können jetzt die Darstellung eines Parameters oder seinen Anfangswert im StyleBook-Konfigurationsformular dynamisch steuern, basierend auf dem in einem anderen Parameter angegebenen Wert. Verwenden Sie dazu das `dependent-parameters` Attribut in der Parameterdefinition. Dieses Attribut wurde als neues `gui` Unterattribut neu hinzugefügt.
Geben Sie dieses Attribut für einen Quellparameter an, der das Verhalten des Parameters im Formular steuert. In diesem Attribut können Sie mehrere Bedingungen einschließen, die andere Parameter steuern.
Beispielsweise kann ein Quellparameterprotokoll ein Abhängigkeitsparameter-Zertifikat haben, das nur angezeigt wird, wenn der Wert des Protokollparameters SSL ist.
Jede Bedingung kann die folgenden Attribute haben:

- `target-parameter`: Geben Sie den Zielparameter an, für den diese Bedingung gilt.
- `matching-values`: Geben Sie die Liste der Werte des Quellparameters an, der die Aktion auslöst.
- `action`: Geben Sie eine der folgenden Aktionen für den Zielparameter an:
  - `read-only`: Der Parameter wird schreibgeschützt.
  - `show`: Der Parameter wird im Formular angezeigt, wenn er ausgeblendet ist.
  - `hide`: Der Parameter wird aus dem Formular entfernt.
  - `set-value`: Der Parameterwert wird auf den im value-Attribut angegebenen Wert festgelegt
- `value`: Der Wert des Zielparameters, wenn die Aktion `set-value`

Wenn eine Benutzereingabe den angegebenen Werten für den Quellparameter entspricht, ändert sich das Aussehen oder der Wert des Zielparameters entsprechend der angegebenen Aktion.

Weitere Informationen finden Sie unter dependent-Parameter.

[NSADM-52329]

Benutzer anzeigen, die eine StyleBook-Konfiguration erstellt oder aktualisiert haben

In **StyleBook > Configurations**wird eine neue Spalte hinzugefügt, in der Benutzer angezeigt werden, die das Konfigurationspaket erstellt oder zuletzt aktualisiert haben. Wenn Sie Konfigurationspakete nach Benutzern filtern möchten, wählen Sie die Option Erstellt von aus der Eigenschaftenliste aus, um Konfigurationspakete zu filtern.

[NSADM-52336]

Verwenden Sie ein Skript, um den Zero-Touch-Agenten in A

Wenn Sie einen ADM-Agenten in AWS starten, können Sie jetzt ein Skript zur automatischen Registrierung für Agenten als Benutzerdaten angeben. Ein Beispielskript wird in bereitgestellt Installieren des Citrix ADM Agenten in AWS. Dieses Skript ruft die Authentifizierungsdetails vom AWS Secrets Manager ab und führt das Skript deployment.py aus, um den Agenten beim ADM-Dienst zu registrieren. Alternativ können Sie immer noch einen der folgenden Schritte ausführen:

- Geben Sie die tatsächlichen Authentifizierungsdetails in Benutzerdaten an, die den Agenten beim Hochfahren automatisch registriert.
- Verwenden Sie das Skript deployment_type.py, um einen Agenten zu registrieren, nachdem er erfolgreich gestartet wurde. Weitere Informationen finden Sie unter Installieren des Citrix ADM Agenten in AWS.

[NSADM-55322]

WAF-Lernen in Citrix ADM

Als Administrator können Sie jetzt Lernprofile konfigurieren, um die Liste der Relaxationsregeln zu erstellen:

- Nur für die ausgewählten Web-Anwendungen
- Nur für die ausgewählten Profilnamen

Weitere Informationen finden Sie unter Konfigurieren des Lernprofils.

[NSADM-49494]

Verletzungen der App-Sicherheit - Netzwerk

Abgesehen von den bestehenden Sicherheitsverletzungen für Apps können Sie jetzt die folgenden Verstöße als Teil der Netzwerkverletzungen anzeigen:

- HTTP-Desync-Angriff

- Bleichenbacher Angriff

Weitere Informationen finden Sie unter Details zur Verletzung der Anwendungssicherheit.

[NSADM-49468],[NSADM-46460]

Anzeigen von Ingress-Metriken und Ingress-Details zur Problembehandlung

Im Service-Diagramm können Sie nun Folgendes anzeigen:

- Ingress-Metriken
- Details zum Eindringen (Drilldown)
- Die Art des verwendeten Eindringens
  - **Tier 1-Eintritt** — Citrix Ingress Controller innerhalb des Kubernetes-Clusters konfiguriert eine Citrix ADC-Instanz (VPX/MPX/SDX/BLX) außerhalb des Kubernetes-Clusters.
  - **Tier 2 Ingress** — Citrix Ingress Controller läuft zusammen mit der Citrix ADC CPX-Instanz im Kubernetes-Cluster als Sidecar.

    > Hinweis: Sie können Tier 1 Ingress und Tier 2 Ingress nur anzeigen, wenn Sie eine zweistufige Architektur (Tier 1 Ingress mit ADC als MPX/VPX/SDX/SDX/BLX und Tier 2 Ingress mit ADC as CPX) im Kubernetes-Cluster konfiguriert haben.

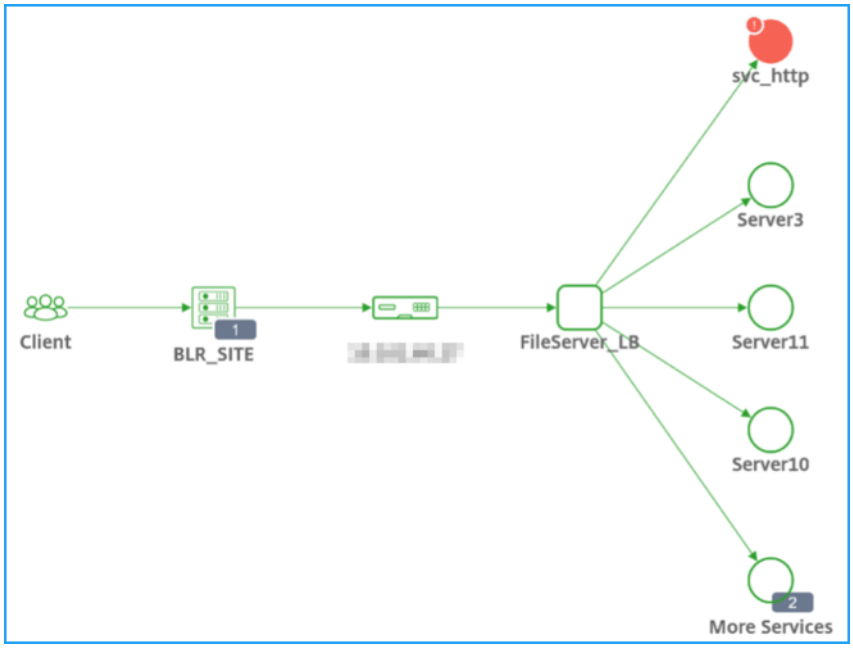
Weitere Informationen finden Sie unter Anzeigen von Ingress-Details zur Problembehandlung

[NSADM-53755]

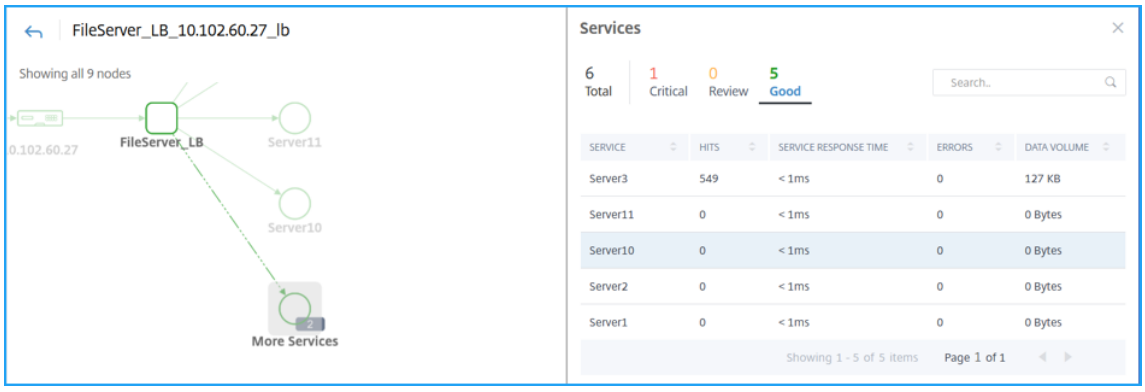
Verbesserungen des dreistufigen Servicediagramms für Web

Das dreistufige Servicediagramm für Webanwendungen ist jetzt mit den folgenden Änderungen improvisiert:

- Die Dienste sind gruppiert und nur die vier besten Low-scored-Dienste werden angezeigt.

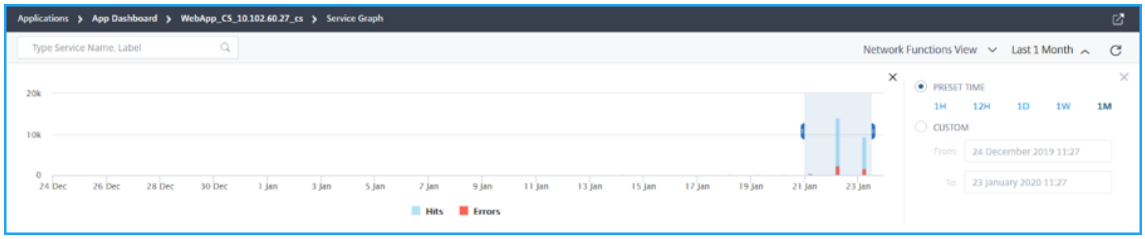


Klicken Sie auf **Weitere Dienste**, um alle Services basierend auf ihrem Status wie **Critical**, **Review**und **Good**anzuzeigen.

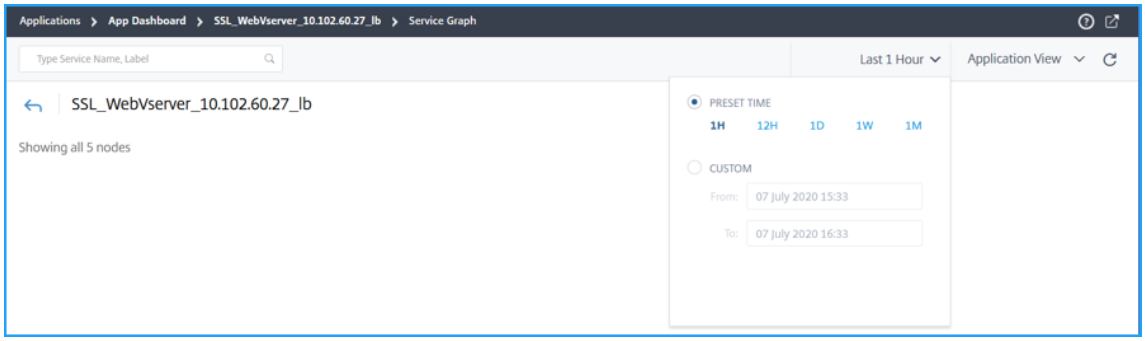


- Das Balkendiagramm **Hits and Errors** ist nicht sichtbar.

  Früher

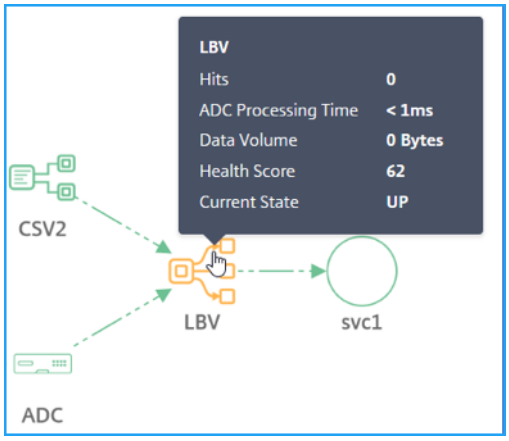


  Jetzt

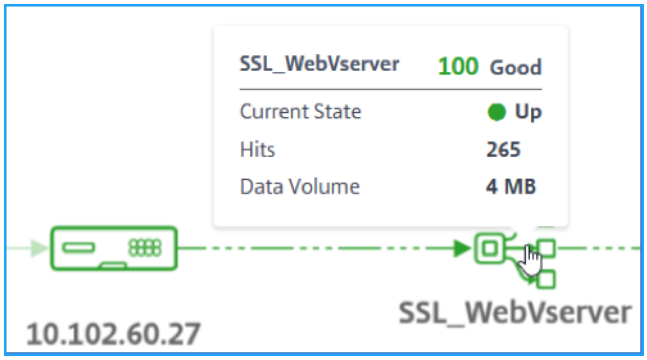


- Die Metriken der Netzwerkfunktionen werden aktualisiert.

  Früher



  Jetzt

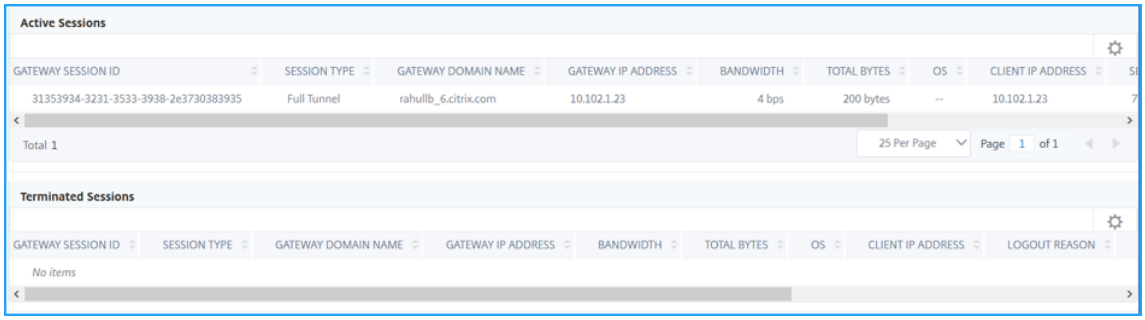


[NSADM-52147]

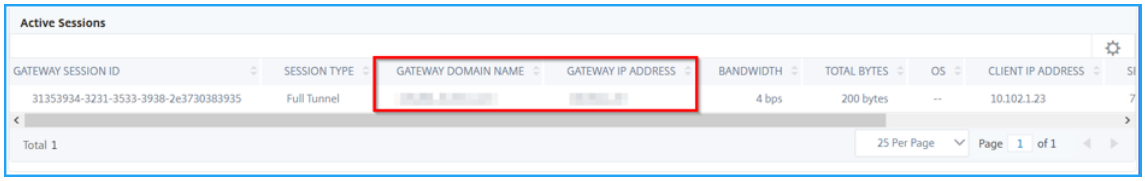
Verbesserungen bei Gateway Insight

In Gateway Insight können Sie jetzt die folgenden Verbesserungen für die Gateway-Benutzer anzeigen. Als Administrator ermöglichen Ihnen diese Verbesserungen, beim Exportieren des Berichts vollständige Benutzerinformationen zu erhalten. Navigieren Sie zu **Analytics > Gateway Insight > Benutzer** und wählen Sie einen Benutzer aus, der angezeigt werden soll:

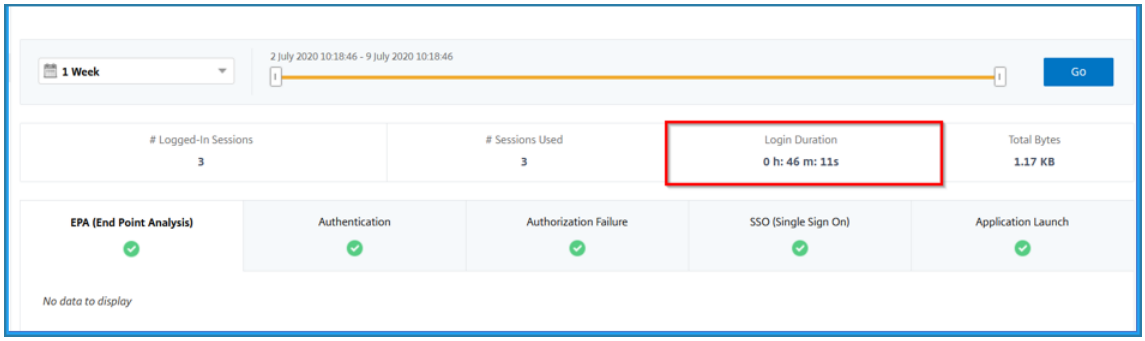
- **Active Sessions** und **Terminated Sessions** der Benutzer.



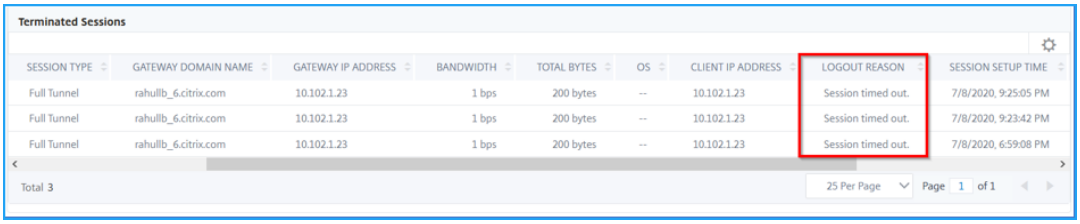
- Der Gateway-Domänenname und die Gateway-IP-Adresse in **Active Sessions**



- Die Dauer der Benutzeranmeldung.



- Der Grund für die Logout-Sitzung des Benutzers. Die Gründe für die Abmeldung können sein:
  - Zeitüberschreitung der Sitzung
  - Ausgeloggt wegen internem Fehler
  - Abgemeldet wegen zeitlich abgelaufenen inaktiven Sitzungen
  - Der Benutzer hat sich abgemeldet
  - Der Administrator hat die Sitzung beendet



[NSADM-52763], [NSADM-52767], [NSADM-52764], [NSADM-53496]

Unterstützung für integrierte Agenten für SDX-Instanzen

Integrierte Citrix ADM Agents sind jetzt auf SDX-Instanzen verfügbar. Außerdem können Sie den integrierten Agenten mithilfe von initiieren `MASTools`. Weitere Informationen finden Sie unter Konfigurieren des integrierten ADC-Agenten zur Verwaltung von Instanzen

Behobene Probleme

Analytics

Wenn ADM die ADC-Metrikinformationen sammelt, wird die CPU-Auslastung hoch.

[NSADM-56374]

Systeme

Wenn Sie **Prompt Credentials for Instanz Login** auf der Seite **Systemeinstellungen** aktivieren, zeigt die ADM-GUI die Lizenzinformationen im **Instanz-Dashboard** nicht an.

[NSHELP-23944]

Netzwerke

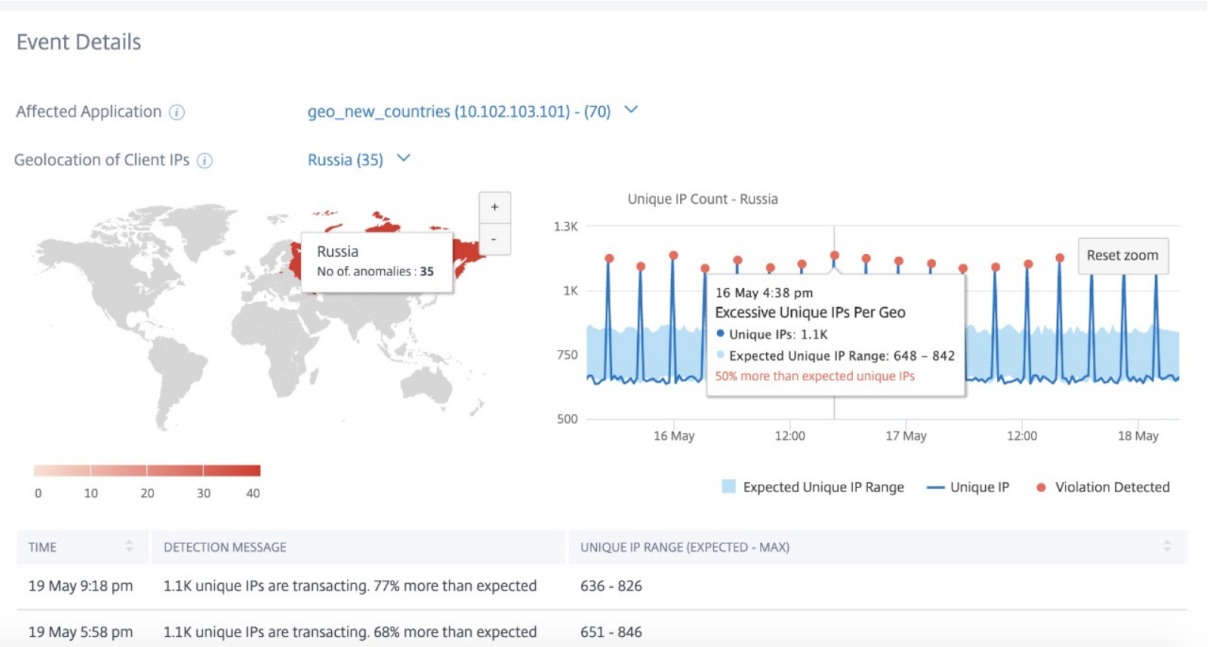
Unter **Netzwerke > Lizenzen**zeigt die ADM-GUI falsche Lizenzinformationen für verwaltete Instanzen an, wenn die Anzahl der verwalteten Instanzen über dem Höchstwert von 58 Instanzen liegt. Mit dem Fix wird das Limit für maximale Instanzen auf 1000 erhöht.

[NSHELP-23956]

30. Juni 2020

Verstöße gegen die App-Sicherheit — Übermäßige eindeutige IPs pro

Mit dem Indikator " **Übermäßige eindeutige IPs pro Geo** " können Sie jetzt eine Geokarte anzeigen, die die gesamten Anomalien basierend auf Regionen anzeigt. Die Grafik zeigt die relevanten Verstoßdetails aus der ausgewählten Region an.



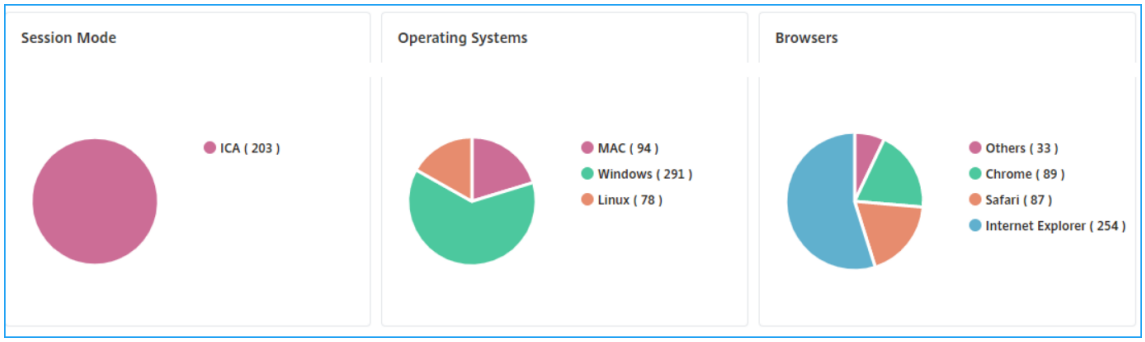
Weitere Informationen finden Sie unter Übermäßige eindeutige IPs pro Geo.

[NSADM-52555]

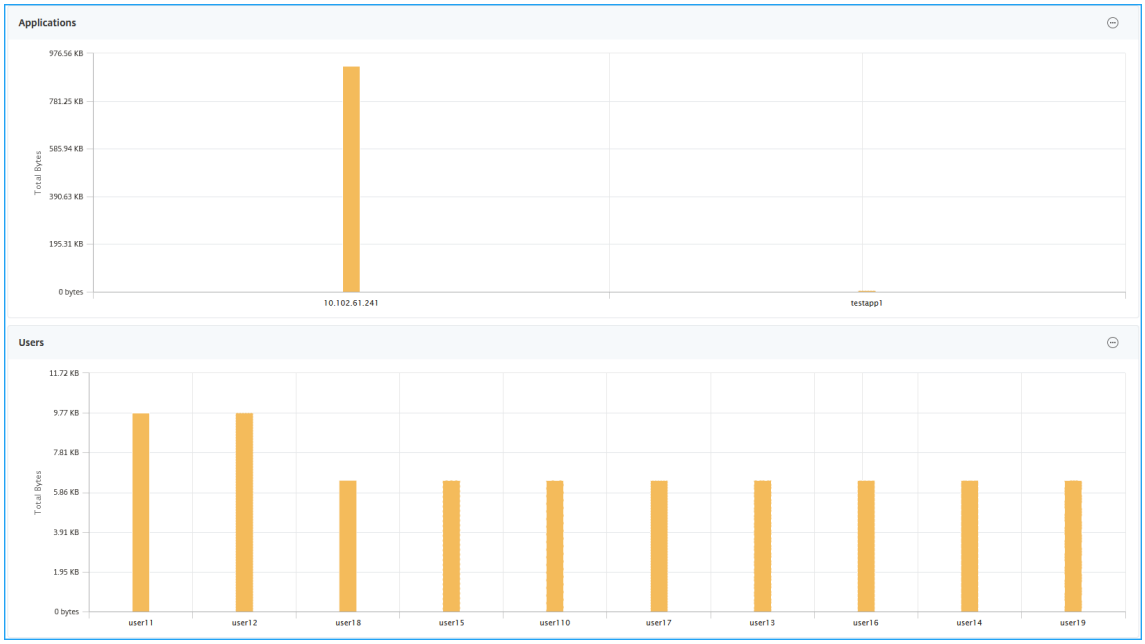
Verbesserungen bei Gateway Insight

In Gateway Insight können Sie jetzt die folgenden Verbesserungen anzeigen:

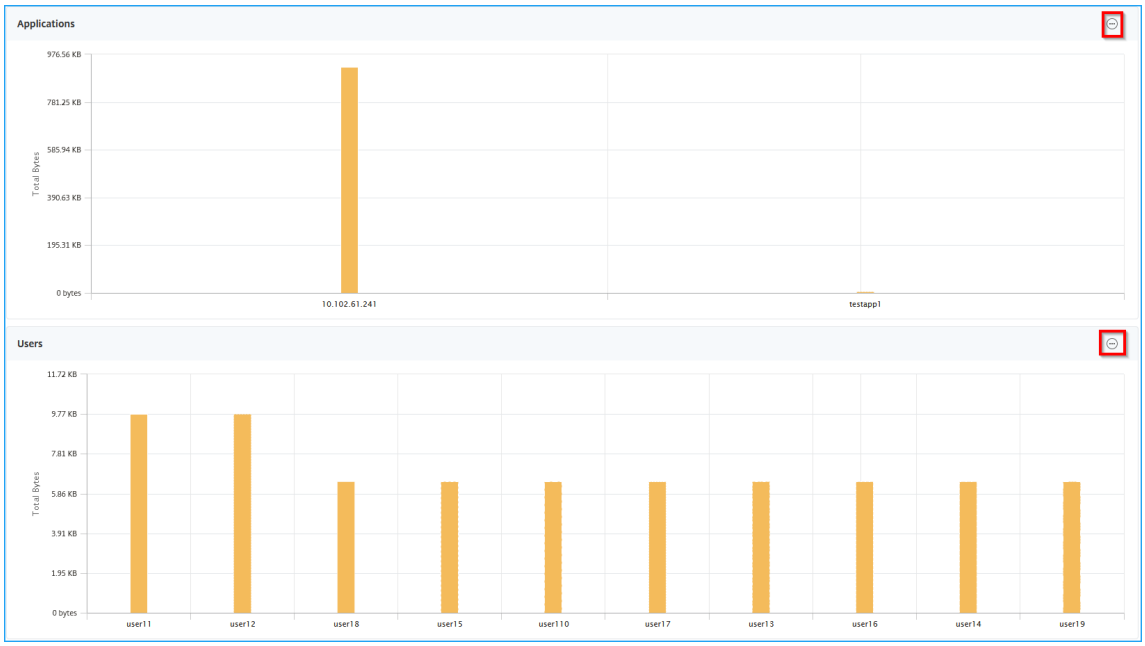
- **Benutzerdetails** - Sie können Erkenntnisse für jeden Benutzer anzeigen, der mit den ADC Gateway-Appliances verknüpft ist. Navigieren Sie zu **Analytics** > **Gateway Insight** > **Benutzer** und klicken Sie auf einen Benutzer, um Erkenntnisse für den ausgewählten Benutzer wie Sitzungsmodus, Betriebssystem und Browser anzuzeigen.



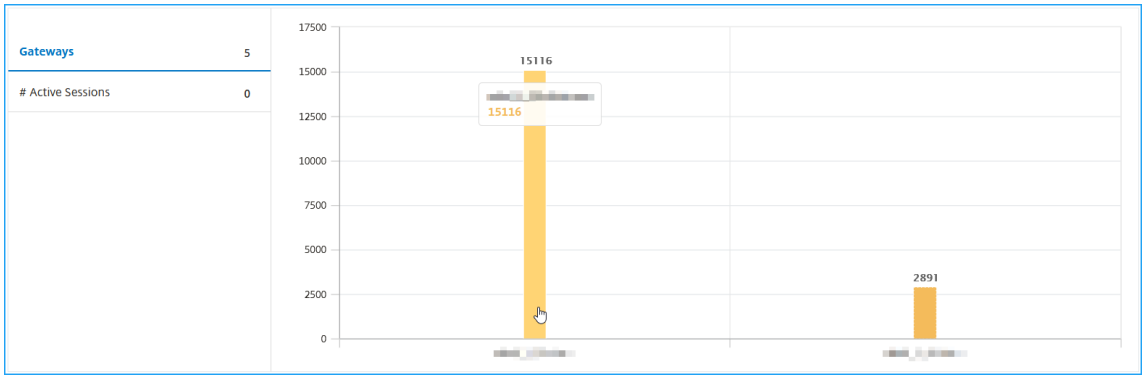
- **Benutzer und Anwendungen für das ausgewählte Gateway** - Navigieren Sie zu **Analytics** > **Gateway Insight** > **Gateway** und klicken Sie auf einen Gateway-Domänennamen, um die 10 wichtigsten Anwendungen und Top-10-Benutzer anzuzeigen, die mit dem ausgewählten Gateway verknüpft sind.



- **Weitere Optionen für Anwendungen und Benutzer anzeigen** — Für mehr als 10 Anwendungen und Benutzer können Sie auf das Mehr-Symbol in Anwendungen und Benutzer klicken, um alle Benutzer- und Anwendungsdetails anzuzeigen, die mit dem ausgewählten Gateway verknüpft sind.



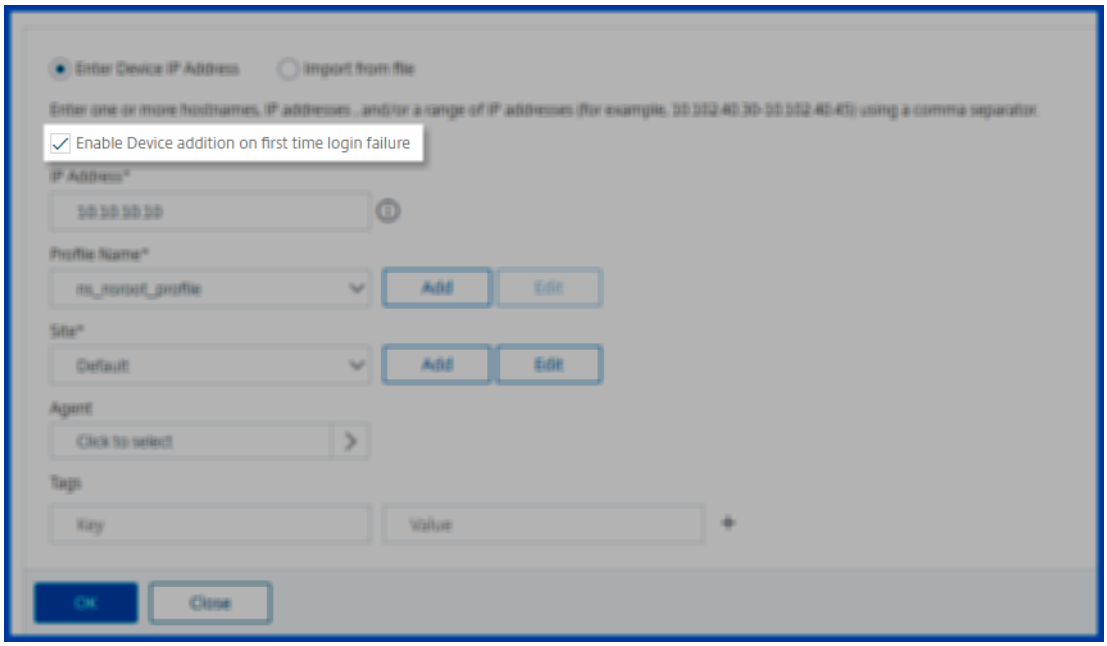
- **Zeigen Sie Details an, indem Sie auf das Balkendiagramm klicken** — Wenn Sie auf ein Balkendiagramm klicken, können Sie die relevanten Details anzeigen. Navigieren Sie beispielsweise zu **Analytics > Gateway Insight > Gateway** und klicken Sie auf das Gateway-Bar-Diagramm, um die Gateway-Details anzuzeigen.



[NSADM-53489], [NSADM-53508], [NSADM-53906], [NSADM-52768]

Möglichkeit, eine ADC-Instanz ohne gültige Anmeldeinformationen hinzuzufügen

Wenn Sie zum ersten Mal eine Instanz in Citrix ADM hinzufügen, können Sie die Instanz jetzt auch ohne gültige Anmeldeinformationen hinzufügen. Nachdem die Instanz hinzugefügt wurde, wird sie im Status DOWN auf der Seite **Netzwerke > Instanz > Citrix ADC** mit einer Warnung "Anmeldung fehlgeschlagen" angezeigt. Geben Sie die richtigen Anmeldeinformationen für die Verwaltung der Instanz in ADM an.



Wenn die Instanz nicht lizenziert ist, wird die Option **Lizenz** angezeigt, wenn Sie die Instanz auswählen. Klicken Sie auf **Lizenz**, um die Lizenz auf eine Instanz aus dem Lizenzpool anzuwenden.

[NSADM-44856]

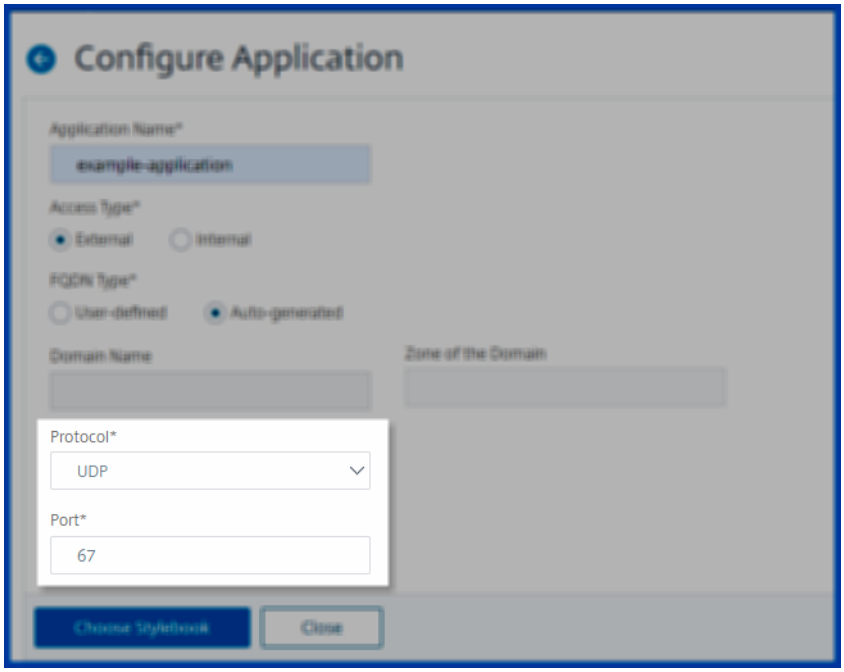
Anzeigen des ADC FIPS-Instanz-Pools auf der Seite Pooled Capacity

Die ADC FIPS-Instanzen können jetzt Lizenzen aus dem FIPS-Instanzpool auschecken. Daher zeigt die ADM-GUI die zugewiesenen gepoolten Lizenzen für FIPS-Instanzen auf der Seite **Netzwerke > Lizenzen > Bandbreitenlizenzen > Pooled Capacity** an.

[NSADM-51207]

Autoscale-Gruppenanwendungen in Azure unterstützen UDP-Verkehr

Die Autoscale-Gruppenanwendungen, die sich in Azure befinden, können jetzt UDP-Datenverkehr empfangen. Wenn Sie eine Anwendung für die Autoscale-Gruppe konfigurieren, wählen Sie das **UDP-Protokoll** und den Portwert aus, um UDP-Datenverkehr zuzulassen.



Mit dieser Funktion werden die folgenden Autoscale-Gruppe StyleBooks neu hinzugefügt, um eine Anwendung zu konfigurieren:

- `lb-mon-autoscale-v1.4`
- `cs-lb-mon-autoscale-v1.3`

[NSADM-53288]

Behobene Probleme

Lizenzierung

Der Instanz-Lizenzstatus wird als **Sync-In-Progress** anstelle von **Managed** angezeigt, wenn die folgenden Bedingungen erfüllt sind:

1. Die Mehrfachlizenzen gehören zur selben Edition und zum selben Pool.
2. Eine ADC-Instanz checkt die Lizenz aus dem Pool aus.

[NSADM-55928]

System

- Syslog-Nachrichten werden nicht in der ADM-GUI angezeigt.

  [NSADM-55822]

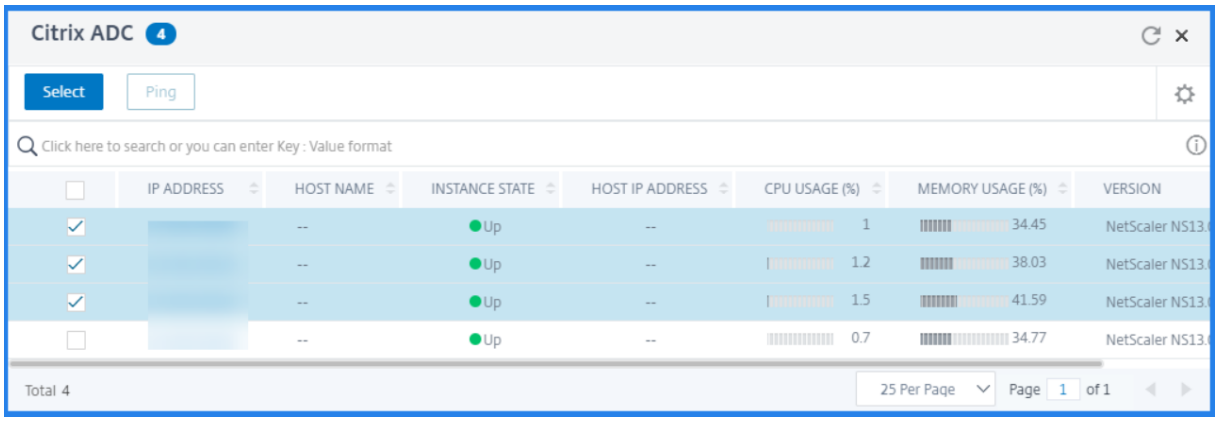
- Wenn Sie die Gruppe des Benutzers ändern, wird der Fehler bei der Kennwortkomplexität angezeigt.

  [NSHELP-23497]

22. Juni 2020

Mehrere Zielinstanzen gleichzeitig auswählen

Wenn Sie dasselbe Konfigurationspaket für mehrere ADC-Instanzen bereitstellen möchten, können Sie nun die erforderlichen ADC-Instanzen gleichzeitig auswählen. Früher mussten Sie die Instanzen einzeln auswählen, um das Konfigurationspaket bereitzustellen. Mit dieser Funktion können Sie auch Instanzen filtern, um die erforderlichen Instanzen auszuwählen.



[NSADM-50115]

Anzeigen der Instanzverteilung nach ihren Nebenversionen

Das Instanz-Dashboard zeigt nun die Verteilung der verwalteten Instanzen nach ihren Nebenversionen an. Mit dem Versionsdiagramm können Sie die Anzahl der Geräte für jede Nebenversion visualisieren.

[NSADM-42183]

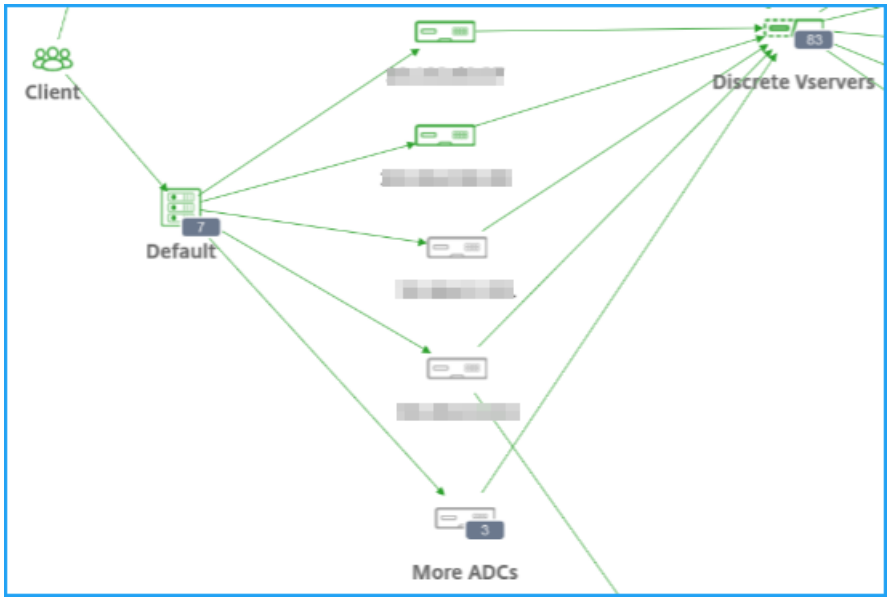
Verbesserungen des globalen Service-Graphen

Als Administrator kann die Einzelbereichsansicht im globalen Servicediagramm für Sie schwierig sein, die Ansichten der Infrastruktur für Anwendungen zu überwachen, wenn Sie Folgendes haben:

- Ein großes Unternehmen mit vielen Rechenzentren
- Viele Citrix ADC-Instanzen für jedes Rechenzentrum konfiguriert
- Viele Anwendungen konfiguriert, die über jede Citrix ADC-Instanz bereitgestellt oder darauf zugegriffen werden

Das verbesserte globale Service-Diagramm eliminiert jetzt die unorganisierte Ansicht und ermöglicht Ihnen folgende Anzeigen:

- Das Rechenzentrum gruppiert mit den gesamten Citrix ADC-Instanzen
- Nur die vier besten Citrix ADC-Instanzen mit niedriger Punktzahl aus jedem Rechenzentrum



Klicken Sie auf **Weitere ADCs**, um alle Citrix ADC-Instanzen anzuzeigen, indem Sie die entsprechenden Registerkarten “Kritisch”, “Prüfen”, “Gut” und “Nicht anwendbar” auswählen. Klicken Sie auf die Instanz-IP-Adresse, um die Instanz-Details wie Instanz-Bewertung, Schlüsselmetriken und Probleme im Zusammenhang mit der ADC-Instanz anzuzeigen.

> **Hinweis**
>
> Sie können auch im globalen Dienstdiagramm auf die Instanz klicken, um die Details der Citrix ADC-Instanz anzuzeigen.

[NSADM-53249]

Behobene Probleme

Analytics

- In **Web Transaction Analytics**werden die gespeicherten Suchen nach einer Seitenaktualisierung nicht angezeigt.

  [NSADM-53722]

- In **Analytics** > **Web Insight**werden die erwarteten Daten nicht für alle Metrikseiten angezeigt (Client, Server, URLs, Anforderungsmethoden, Antwortstatus, Benutzeragenten und Betriebssysteme).

  [NSADM-53632]

- Selbst nach der Konfiguration des richtigen RBAC zeigen die Anwendungen unter " **Anwendungen** " > " **App Dashboard** " und die virtuellen Server unter " **Netzwerkfunktion** " > " **Lastausgleich** " nicht die erwarteten Daten an, sobald ein neues stylebook/configpack vom Benutzer von der Gruppe.

  [NSHELP-23101]

Grafische Benutzeroberfläche (GUI)

- Bei einer VPN-Verbindung kann sich ADM nicht über SSO (Single Sign On) mit der ADC-GUI verbinden.

  [NSHELP-23099]

04. Juni 2020

Bereitstellen Ihrer AWS-Anwendung in drei Schritten bei der ersten Anmeldung

Wenn Sie sich zum ersten Mal an der ADM-GUI anmelden, können Sie in nur drei Schritten eine Anwendung bereitstellen, die sich in AWS befindet, indem Sie ADC-Instanzen verwenden:

1. Registrieren Sie Ihr AWS-Konto beim Citrix ADM -Service, indem Sie ein Cloud Access-Profil erstellen.
2. Bereiten Sie Ihre AWS-Umgebung vor, indem Sie die AWS-Region, VPC-Details und ADC-Lizenzen angeben.

   Die AWS-Umgebung umfasst AWS-Infrastruktur, ADM-Agenten und ADM Autoscale-Gruppe. In diesem Schritt erstellt der ADM Folgendes:

   - Ein CloudFormation-Stack in AWS zum Erstellen der erforderlichen Infrastruktur, die Subnetze, Sicherheitsgruppen, NAT-Gateways usw. umfasst.
   - Ein ADM-Agent in der VPC zur Verwaltung von ADC-Instanzen.

- Eine ADC Autoscale-Gruppe. Sie können diese Gruppe später auf der Seite **Netzwerke > Gruppe automatisch skalieren** anpassen.

3. Nach erfolgreicher Umgebungsvorbereitung, Konfigurieren von Anwendungen mit StyleBooksum Ihre Anwendung zu liefern.

Wenn Sie ADC-Instanzen nach der ersten Anmeldung automatisch skalieren möchten, finden Sie weitere Informationen unter Automatische Skalierung von Citrix ADC mit Citrix ADM.

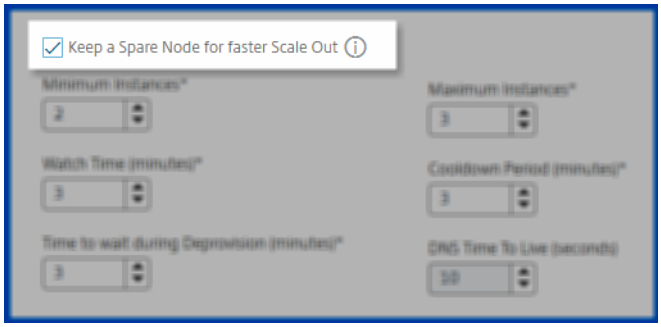
Weitere Informationen finden Sie unter Erste Schritte.

[NSADM-47626]

Pflegen Sie einen Ersatzknoten in Ihrer Autoscale-Gruppe

Wenn Sie Parameter zum Erstellen einer Gruppe für die automatische Skalierung angeben, können Sie nun einen Ersatzknoten beibehalten, um eine schnellere Skalierung zu erreichen.

ADM stellt einen Reserve-Knoten bereit, bevor die Scale-Out-Aktion ausgeführt wird, und beendet ihn. Wenn die Scale-Out-Aktion für die Autoscale-Gruppe auftritt, startet der ADM den bereits bereitgestellten Ersatzknoten. Infolgedessen reduziert es die Zeit für das Scale-Out.



Weitere Informationen finden Sie unter Konfigurieren von Parametern für die automatische Skalierung.

[NSADM-48191]

Konfigurieren einer Autoscale-Gruppenanwendung mithilfe des automatisch generierten FQDN

Wenn Sie eine Anwendung für die Autoscale-Gruppe konfigurieren, können Sie nun den automatisch generierten FQDN-Typ auswählen. Mit dieser Option wird automatisch der Domänen- und Zonenname generiert.

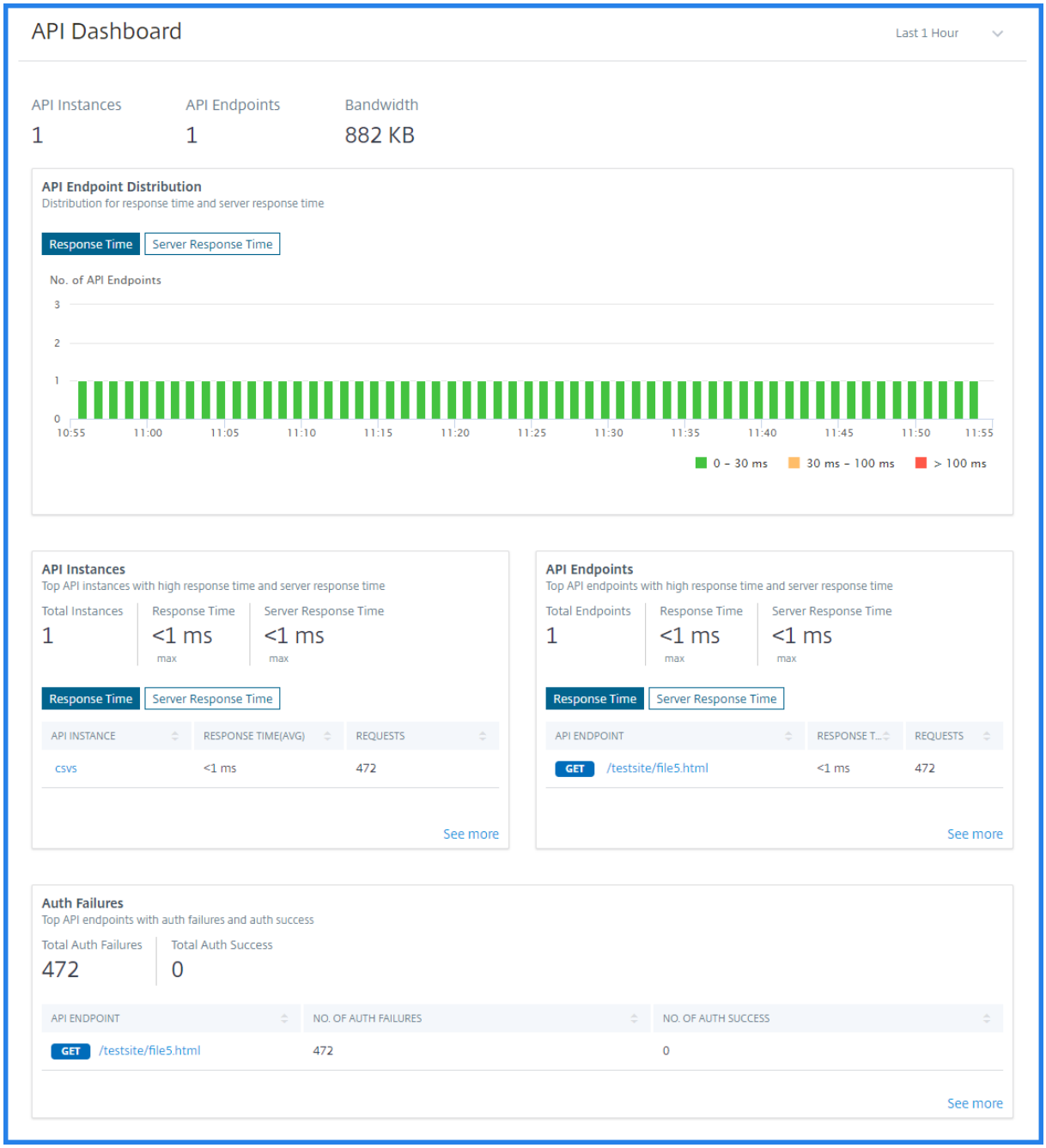
Wenn Sie einen benutzerdefinierten FQDN-Typ auswählen, müssen Sie den Domänen- und Zonennamen angeben, um eine Anwendung zu konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von Anwendungen mit StyleBooks.

[NSADM-51494]

Überwachen von API-Instanzen und Endpunkten in ADM

Als Administrator können Sie API-Definitionen auf einem API Gateway in Citrix Application Delivery Management (ADM) hinzufügen und bereitstellen. Mit dieser Funktion können Sie Richtlinien hinzufügen, um die Auswahlkriterien für den Datenverkehr zu definieren, um eingehende API-Anforderungen zu authentifizieren.
Auf der Seite " **API Analytics** " werden die folgenden Metriken von API-Instanzen und Endpunkten angezeigt:

- Verteilung der Anwendungs- und Server-Antwortzeit für API-Endpunkte.
- API-Endpunkte mit hoher Reaktionszeit für Anwendungen und Server.
- API-Endpunkte, die mehr Anforderungen und Bandbreite aufweisen.
- Standorte, von denen die Endpunkte API-Anforderungen empfangen.
- Der Trend der gesamten API-Anforderungen und der abgesenkt an einen Endpunkt.
- HTTPS-Antwortstatus.
- API-Endpunktbandbreitenverbrauch.
- SSL-Fehler und Verwendung auf einem API-Endpunkt.



Weitere Informationen finden Sie unter API-Definitionen verwalten.

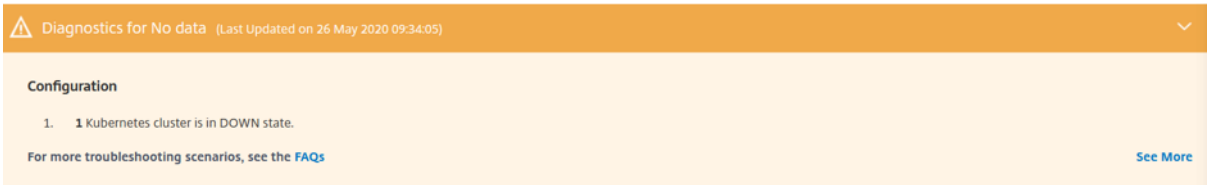
[NSADM-47869]

Verbesserungen des Service-Graphen

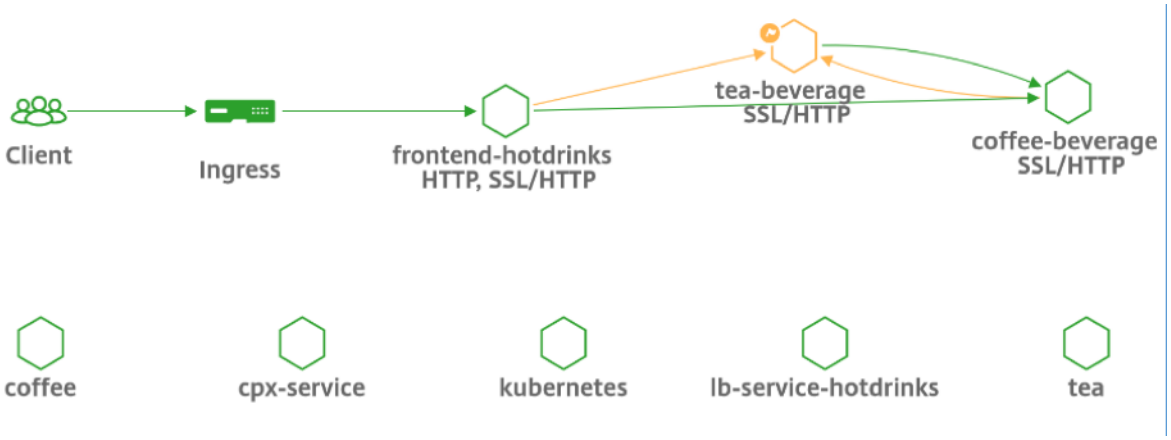
Service Graph wird mit einigen thematischen Änderungen aktualisiert. Sie können auch einige kleinere UI-Updates erleben:

- FAQs Link — Weitere Fehlerbehebungsszenarien für Service-Graph anzeigen, die partielle und

keine Datenprobleme anzeigen.



- Änderung der ADC-Verarbeitungszeitmetrik — Diese Metrik zeigt 0 anstelle von < 1 ms an. Diese Änderung gilt nur für ADC-Instanzen, die den Status “Abgemeldet” oder “Heruntergefahren” aufweisen.
- Hexagon zur Darstellung einer Microservice-Anwendung — Dienstdiagramm zeigt jetzt eine Microservice-Anwendung im Sechseck-Symbol an.



- ADC-Instanzdetails anzeigen — Klicken Sie auf eine ADC-Instanz aus Service-Graph für Anwendungen (**Anwendungen > [App-Name] > Service-Graph**). Auf dieser Seite werden ADC-Instanz-Details wie Instanz-Bewertung, wichtige Metriken und Probleme angezeigt.
- Globales Service-Diagramm zur Anzeige von Microservice-Anwendungen — Die Microservice-Anwendungen werden basierend auf den konfigurierten Schwellenwerten angezeigt.

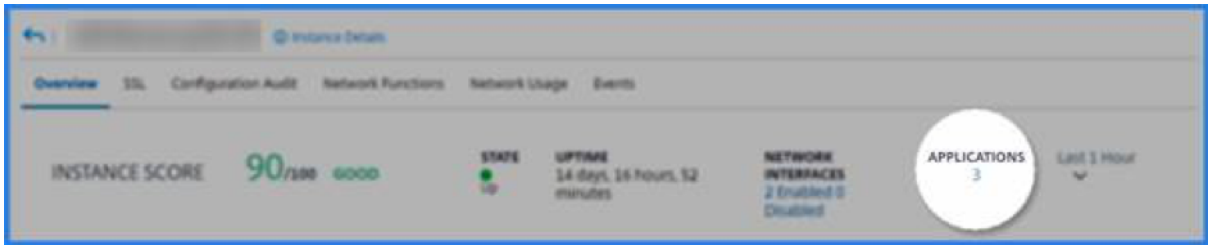
Je nach Punktzahl können Sie die Microservice-Anwendungen in Rot (kritisch), Orange (Überprüfung) und Grün (gut) anzeigen.

- Namespace-Filter zur Anzeige entsprechender Dienste — Das Dienstdiagramm zeigt nun die entsprechenden Dienste zusammen mit Client und Ingress an.

[NSADM-51973]

Anzeigen von Anwendungen auf der Seite “Infrastructure Analytics”

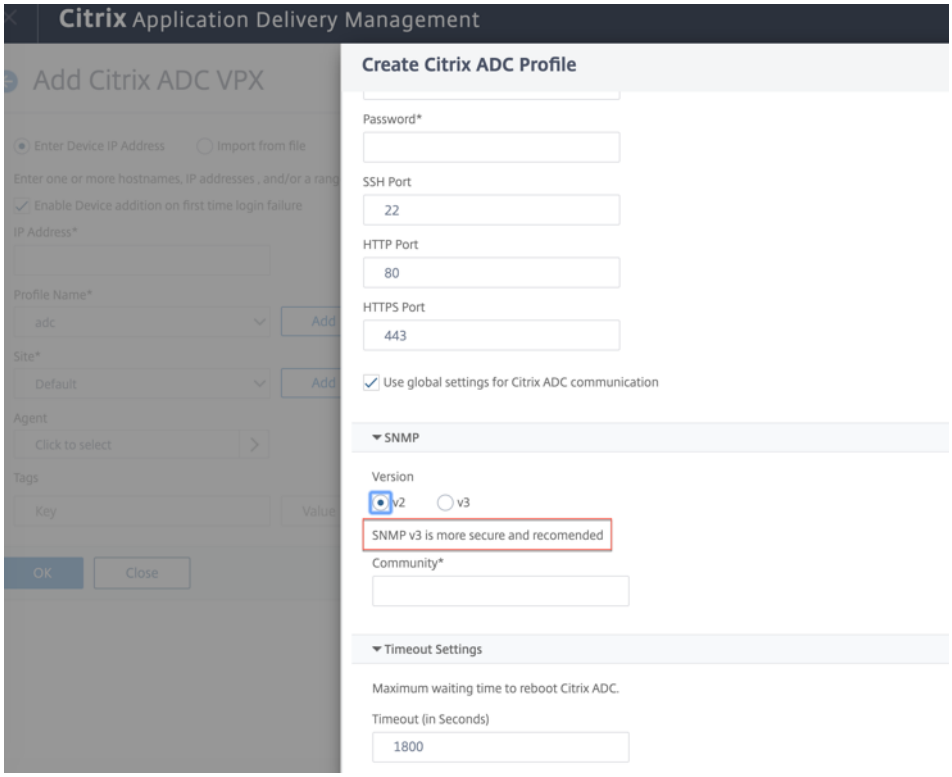
Wenn Sie eine Instanz auf der Seite Infrastructure Analytics auswählen, können Sie die Anzahl der auf der Instanz bereitgestellten Anwendungen anzeigen. Klicken Sie auf den Link Anwendungen, um diese Anwendungen anzuzeigen.



[NSADM-43848]

Ein neuer UI-Text für SNMP V2

Wenn Sie beim Hinzufügen einer ADC-Instanz in der ADM-GUI unter **SNMP**SNMP V2 jetzt die folgende Meldung auswählen: “SNMP V3 ist sicherer und empfohlen.” Standardmäßig ist SNMP V3 ausgewählt.

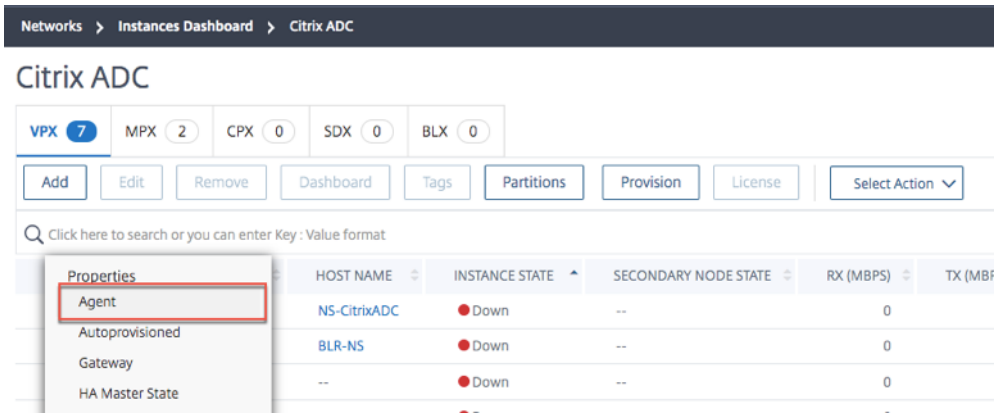


Weitere Informationen finden Sie unter Instanzen hinzufügen.

[NSADM-51179]

Agent als neue Sucheigenschaft

Unter **“Netzwerke” > “Instanzen” > “Citrix ADC**” können Sie Instanzen vom zugehörigen Agent durchsuchen. Klicken Sie auf das Suchsymbol und wählen Sie **Eigenschaften > Agent**aus.

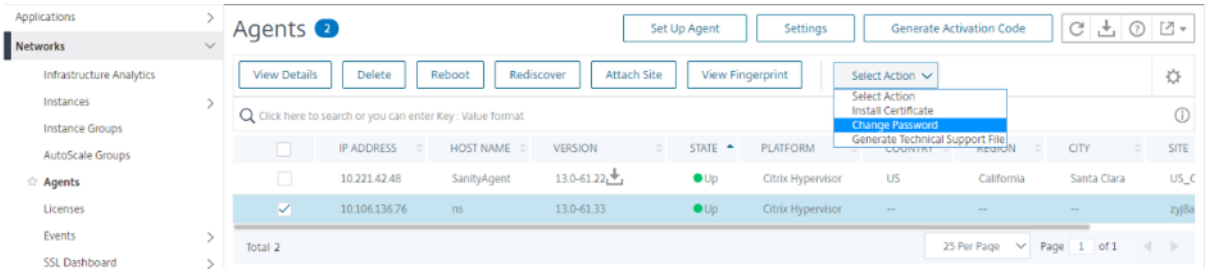


Weitere Informationen finden Sie unter So suchen Sie Instanzen mithilfe von Werten von Tags und Eigenschaften.

[NSADM-47424]

Ändern des Agent-Standardkennworts

Um die Sicherheit Ihrer Infrastruktur zu gewährleisten, können Sie jetzt das Standardkennwort eines Agenten ändern.
Um das Kennwort zu ändern, navigieren Sie in der GUI zu **Netzwerke > Agents**, klicken Sie auf **Aktion auswählen** und wählen Sie **Kennwort ändern**aus.

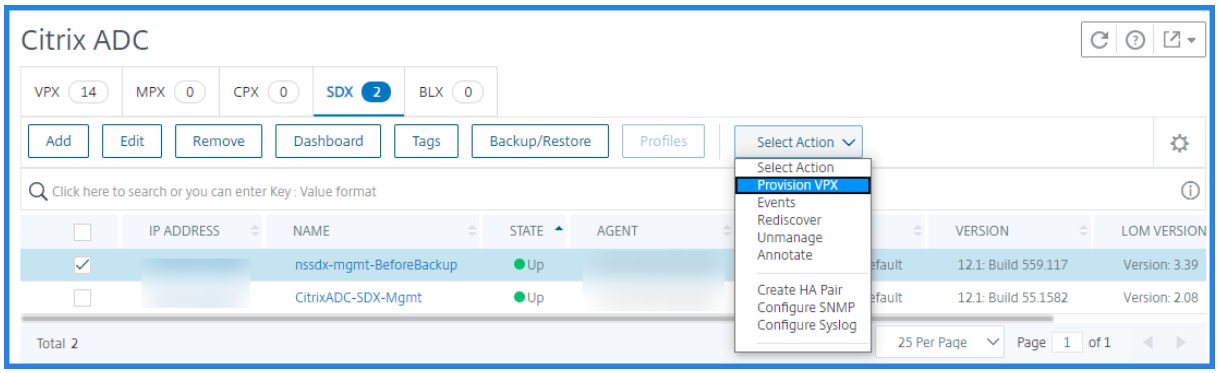


Weitere Informationen finden Sie unter Erste Schritte.

[NSADM-47521]

Verwenden von ADM zum Bereitstellen von ADC-Instanzen auf SDX

Sie können jetzt eine oder mehrere Citrix ADC-Instanzen auf der SDX-Appliance mithilfe von ADM bereitstellen. Der ADM-Dienst stellt implizit die Citrix ADC-Instanz auf der SDX-Appliance bereit und lädt dann Konfigurationsdetails der Instanz herunter.



Weitere Informationen finden Sie unter Bereitstellen von ADC VPX-Instanzen auf SDX mithilfe von ADM.

[NSADM-23845]

Behobene Probleme

Analytics

In Gateway Insight funktioniert der Exportbericht für das CSV-Format nicht wie erwartet.

[NSHELP-22780]

Grafische Benutzeroberfläche (GUI)

Das Menü Favoriten speichern zeigt manchmal einen JavaScript-Fehler an.

[NSADM-52856]

Lizenzierung

Die nicht behandelten Timeout-Ausnahmen und Deadlock-Bedingungen führen dazu, dass die gepoolte Lizenzierungsfunktion nicht wie erwartet funktioniert.

[NSHELP-22729]

15. Mai 2020

Anzeigen von Diagnosedetails für partielle oder keine Daten im Service-Diagramm

Nachdem Sie die erforderliche Dienstdiagrammkonfiguration abgeschlossen und den Kubernetes-Cluster in Citrix ADM hinzugefügt haben, beginnt das Dienstdiagramm mit dem Auffüllen der Daten. In einigen Szenarien können Sie beobachten, dass Service-Graph entweder Teildaten oder keine Daten anzeigt. Einige der möglichen Gründe für die Teildaten oder keine Daten im Service-Diagramm sind:

- Statische Route ist nicht konfiguriert
- Kubernetes Clusterstatus ist ausgefallen
- CPX-Registrierung ist fehlgeschlagen
- Virtuelle CPX-Server sind nicht lizenziert
- Die erforderliche Analytics-Konfiguration ist nicht festgelegt, die verhindert, dass Service-Graph alle Daten laden kann.

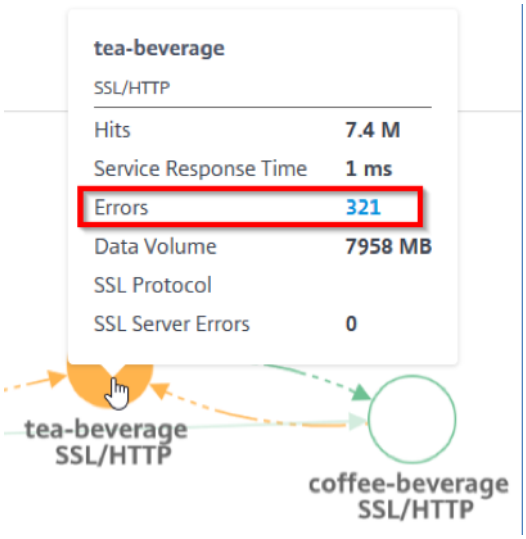
Als Administrator ist es Ihnen möglicherweise schwierig, die Gründe zu analysieren, wenn das Service-Graph-Feature Teildaten oder keine Daten anzeigt.

Auf der Seite “Service Graphs” können Sie nun die möglichen Gründe und erforderlichen Aktionen anzeigen, um die Teildaten oder kein Datenproblem zu beheben.
Weitere Informationen finden Sie unter Diagnosedetails anzeigen.

[NSADM-47865]

Ein vereinfachter Prozess zum Anzeigen von Fehlern im Service-Graph

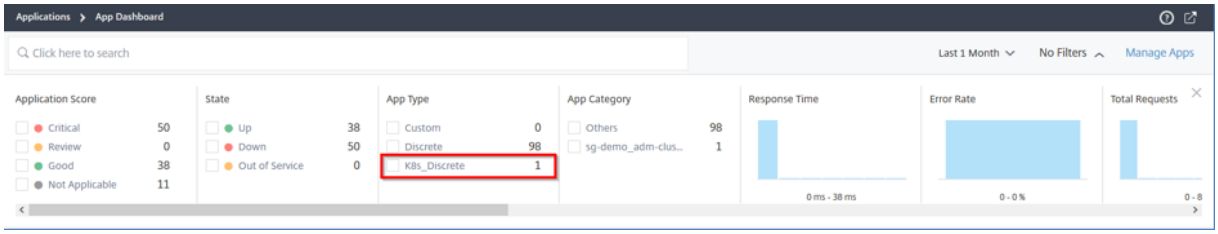
Im Dienstdiagramm wird der Prozess zum Anzeigen der HTTP- und SSL-Fehler vereinfacht. Sie können nun die Gesamtfehler anzeigen, indem Sie den Mauszeiger auf einen fehlerhaften Dienst bewegen und auf die Fehleranzahl klicken.



[NSADM-47864]

Anzeigen von Microservice-Anwendungen im App-Dashboard

Im **App Dashboard**können Sie die Details der Microservice-Anwendungen anzeigen, die von der Citrix ADC CPX-Instanz im Kubernetes-Cluster konfiguriert wurden. Der **App-Typ-Filter** verfügt über eine neue Option **K8S_Discrete**, mit der Sie Filter anwenden und die Details der Microservice-Anwendung anzeigen können.



Weitere Informationen finden Sie unter Details der Microservice-App anzeigen.

[NSADM-47863]

WAF-Lernen in Citrix ADM

Citrix Web App Firewall (WAF) schützt Ihre Webanwendungen vor böswilligen Angriffen wie SQL-Injection und Cross-Site Scripting. Um Datenschutzverletzungen vorzubeugen und den richtigen Sicherheitsschutz zu bieten, müssen Sie Ihren Datenverkehr auf Bedrohungen und umsetzbare Echtzeitdaten bei Angriffen überwachen. Manchmal sind die gemeldeten Angriffe möglicherweise falsch positiv, und diese Angriffe müssen als Ausnahme bereitgestellt werden.
Die Lern-Engine in Citrix ADM ist ein sich wiederholender Pattern-Filter, mit dem WAF das Verhalten (die normalen Aktivitäten) Ihrer Webanwendungen erlernen kann. Basierend auf der Überwachung

generiert die Engine eine Liste der vorgeschlagenen Regeln oder Ausnahmen für jede Sicherheitsprüfung, die auf den HTTP-Datenverkehr angewendet wird. Als Administrator können Sie diese Verstöße dann in Citrix ADM anzeigen und entscheiden, ob Sie sie bereitstellen oder überspringen möchten. Weitere Informationen finden Sie unter WAF-Lernen in Citrix ADM.

[NSADM-44341]

App-Sicherheitsverletzungen - Übermäßige eindeutige IPs pro Geo

Abgesehen von den bestehenden App-Sicherheitsverletzungen können Sie jetzt **Exzessive eindeutige IPs pro Geo** als Teil der Bot-Kategorie anzeigen. Mit dem Indikator " **Exzessive eindeutige IPs per Geo** " können Sie schlechte Bots analysieren und blockieren, die mehr Besuche einer Webanwendung von einem bestimmten Standort aus durchführen.
Weitere Informationen finden Sie unter Übermäßige eindeutige IPs pro Geo.

[NSADM-43982]

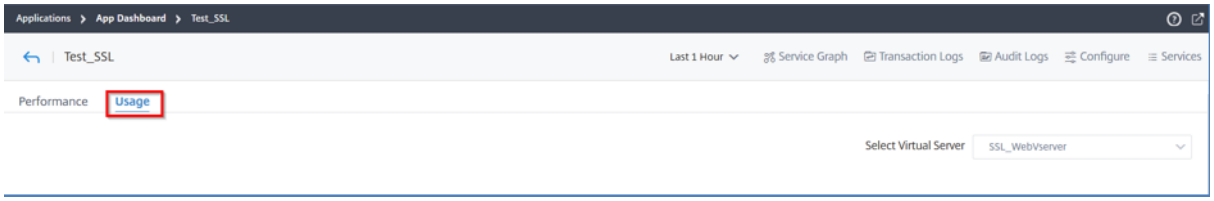
Analyse der Anwendungsverwendung

Anwendungseigentümer müssen die Möglichkeit haben, die gesamte Anwendung aus den Perspektiven der Leistung und Nutzung auszuwerten und zu visualisieren.

Mit dem improvisierten App Dashboard können Sie alle Anwendungsleistungen und Nutzungsmetriken zusammen anzeigen. Wenn Sie neben den vorhandenen Metriken für die Anwendungsleistung auf eine Anwendung klicken, werden auf der Registerkarte **Verwendung** die Metriken angezeigt, die Ihnen helfen:

- Verstehen Sie Ihre Anwendungsnutzung.
- Korrelieren Sie alle Performance-Abweichungen mit den Verwendungsmetriken.

Wenn die Anwendung über zwei oder mehr virtuelle Server verfügt, wählen Sie den virtuellen Server aus der Liste aus.



Mit dem App Dashboard können Sie als Administrator eine Einzelansicht für die folgenden Metriken visualisieren:

- Kunden
- Server
- Geo Standorte

- URLs
- HTTP-Antwortstatus
- Betriebssystem
- Browser
- SSL-Fehler
- SSL-Nutzung

Weitere Informationen finden Sie unter Analyse der Anwendungsverwendung.

Globales Service-Diagramm: Eine ganzheitliche Visualisierung von Benutzern, Infrastruktur und Anwendungen

> **Hinweis**
>
> Diese Funktion befindet sich in der Vorschau.

Die globale Service-Graph-Funktion ermöglicht es Ihnen, eine ganzheitliche Visualisierung der Ansicht `clients to infrastructure to application`zu erhalten. In dieser Dienstdiagrammansicht mit einem einzigen Fensterbereich können Sie als Administrator folgende Möglichkeiten haben:

- Verstehen, aus welcher Region die Benutzer auf die spezifischen Anwendungen zugreifen (3-Tier-Web-Apps und Microservices-App)
- Visualisieren der Infrastrukturansicht (Citrix ADC-Instanz), dass die Clientanforderung verarbeitet wird
- Verstehen, ob die Probleme vom Client, der Infrastruktur oder der Anwendung auftreten
- Weitere Drilldown zur Behebung des Problems

Navigieren Sie zu **Anwendungen > Service-Diagramme > Globales Service-Diagramm**, um Folgendes anzuzeigen:

- End-to-End-Details aller Anwendungen, die vom Client zu Back-End-Servern verbunden sind.
- Alle Citrix ADC-Instanzen, die mit den jeweiligen Rechenzentren verbunden sind. **Hinweis**: Sie können Rechenzentren nur anzeigen, wenn Sie GSLB-Apps haben.
- Die Informationen zur Client-Metriken.
- Die Citrix ADC Metrikinformationen.
- Alle Citrix ADC-Instanzen mit diskreten Anwendungen, benutzerdefinierten Anwendungen und diskreten Microservice-Anwendungen.
- Die vier besten Anwendungen mit niedriger Punktzahl, die zu benutzerdefinierten Apps, diskreten Apps und Microservices-Apps gehören.
- Die Metrikinformationen für die vier besten virtuellen Server mit niedriger Punktzahl.
- Der Status von Anwendungen (separate Apps, benutzerdefinierte Apps und Microservices-Apps), z. B. **Kritisch**, **Überprüfen**, **Gut** und **Nicht anwendbar**.

Weitere Informationen finden Sie unter Ganzheitliche Ansicht aller Anwendungen im Service-Graph.

[NSADM-47425]

Anpassen des StyleBooks-Filters, um Benutzerberechtigung bereitzustellen

Als Administrator können Sie bestimmte StyleBooks für einen Benutzer auf der Seite **Konto > Benutzerverwaltung > Gruppen** autorisieren. Sie können nun eine benutzerdefinierte Filterabfrage verwenden, um StyleBooks zu suchen. Eine Abfrage ist eine Zeichenfolge von Schlüssel-Wert-Paaren, wobei Schlüssel wie folgt lauten:

- Name
- Namensraum
- Version

Beispiel:

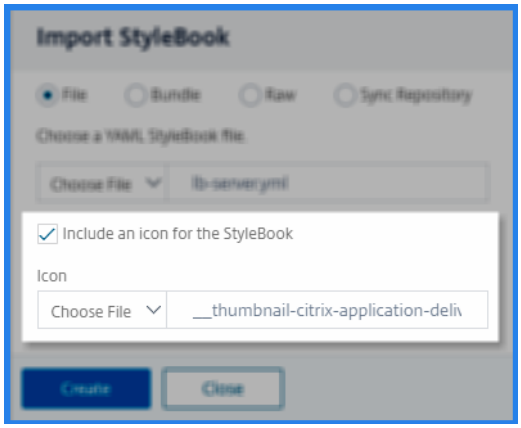
```
name=lb-mon OR namespace=com.citrix.adc.stylebooks OR version=1.0
```

Das Suchergebnis listet die StyleBooks basierend auf dem angegebenen Schlüssel-Wert-Paar auf. Basierend auf der angegebenen Abfrage bietet der ADM Benutzerzugriff auf diese Stylebooks.Weitere Informationen finden Sie unter Konfigurieren von Gruppen in Citrix ADM.

[NSADM-49446]

Importieren von StyleBooks mit einem Symbol

Wenn Sie ein StyleBook importieren, können Sie nun ein Symbol hinzufügen. In **Anwendungen > StyleBook**wird das importierte StyleBook mit einem Symbol angezeigt.



Weitere Informationen finden Sie unter Importieren von benutzerdefinierten StyleBooks

[NSADM-45810]

Neue integrierte Funktionen in StyleBooks verwenden

Beim Erstellen von StyleBook-Definitionen unterstützt ADM StyleBooks jetzt die folgenden integrierten Funktionen:

- `startswith()` — Bestimmt, ob eine Zeichenfolge mit einem bestimmten Präfix beginnt. Weitere Informationen.
- `contains()` — Bestimmt, ob eine Zeichenfolge eine bestimmte Teilzeichenfolge enthält. Weitere Informationen.
- `endswith()` — Bestimmt, ob eine Zeichenfolge mit einem angegebenen Suffix endet. Erfahren Sie mehr](/en-us/citrix-application-delivery-management-service/stylebooks/stylebooks-grammar/built-in-functions.html#endswith)
- `substring()` — Extrahiert eine Teilzeichenfolge aus einer Zeichenfolge. Erfahren Sie mehr](/en-us/citrix-application-delivery-management-service/stylebooks/stylebooks-grammar/built-in-functions.html#substring)

[NSADM-45889]

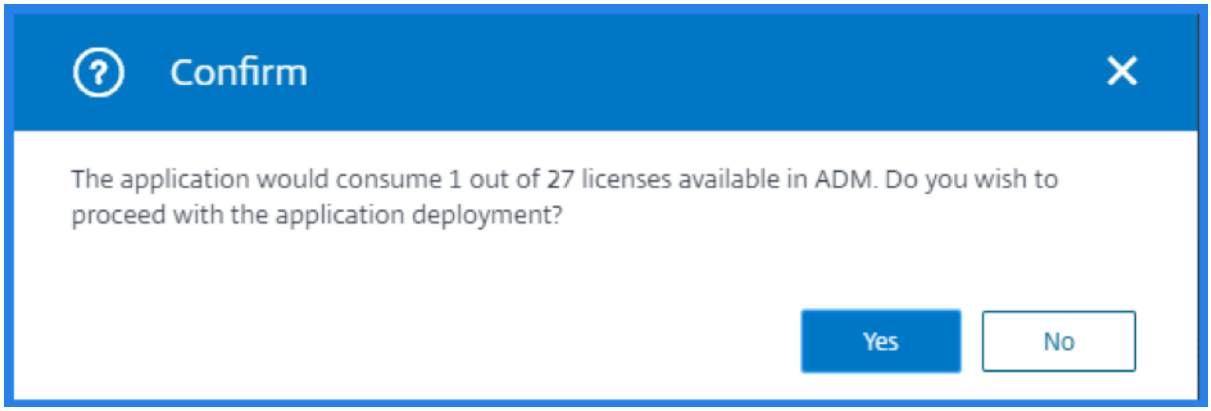
StyleBook-Konfigurations-Builder unterstützt ADC-WAF-Funktion

Der StyleBook-Konfigurations-Builder erkennt und unterstützt nun die WAF-Funktion in einer ADC-Quellkonfiguration. Weitere Informationen zu unterstützten ADC-Funktionen finden Sie unter Migrieren der Citrix ADC Anwendungskonfiguration mit dem StyleBooks Configuration Builder.

[NSADM-48941]

Lizenzverbrauch vor der Anwendungsbereitstellung bestätigen

Wenn Sie eine Anwendung mit StyleBooks erstellen, können Sie vor der Bereitstellung der Anwendung den erforderlichen Lizenzverbrauch bestätigen. Die folgende Meldung wird angezeigt, nachdem Sie die Schritte zum Erstellen einer Anwendung ausgeführt haben:



Klicken Sie auf **Ja**, um die Bestätigungsmeldung anzuzeigen. Der ADM weist einer Anwendung die erforderlichen Lizenzen zu.
Früher mussten Sie die Option Virtuelle Server automatisch lizenziert aktivieren, um eine Anwendung mit StyleBooks zu erstellen. Jetzt können Sie eine Anwendung auch dann erstellen, wenn die Option Virtuelle Server automatisch lizenziert deaktiviert ist.

Weitere Informationen finden Sie unter Erstellen einer Anwendung mit StyleBook.

[NSADM-51306, NSADM-47184]

Behobene Probleme

Netzwerke

Wenn Sie einen CSV-Bericht für alle Leistungsberichte einschließlich des Berichts für den Lastausgleich virtueller Server exportieren, wird der exportierte Bericht leer angezeigt.

[NSHELP-22465]

Unter Netzwerke > Konfigurationsüberwachung > Überwachungsberichtefunktionieren für jede ausgewählte ADC-Instanz die folgenden Aktionen nicht:

- Versionsverlauf Diff
- Pre-vs. Diff nach dem Upgrade
- Download-Konfiguration

[NSADM-51310]

Upgrade-Skripte können nicht heruntergeladen werden, und die Fehlermeldung “Datei nicht gefunden” wird angezeigt. Dieses Problem tritt auf, wenn Sie die Skripts herunterladen, nachdem ein Wartungsaktualisierungsauftrag erfolgreich abgeschlossen wurde.

[NSADM-48809]

Analytics

Die ungewöhnlich großen Upload- und Download-Transaktionsindikatoren in der Citrix ADM GUI zeigen Analysedaten nicht wie erwartet an.

NSADM-50930]

28. April 2020

Details zu Anwendungssicherheitsverletzungen anzeigen

Neben den bestehenden Netzwerkverletzungen können Sie nun Verstöße für Bot- und WAF-Kategorien anzeigen. Im Folgenden werden die Verstöße aufgeführt, die Sie in Citrix ADM visualisieren können:

BOT	WAF
Übermäßige Clientverbindungen	Ungewöhnlich hohe Upload-Transaktionen
Übernahme von Konten	Ungewöhnlich hohe Download-Transaktionen
Ungewöhnlich hohe Upload-Volumen	Übermäßige eindeutige IPs
Ungewöhnlich hohe Anforderungsrate	
Ungewöhnlich hohes Downloadvolumen	

Weitere Informationen finden Sie unter Details zu Anwendungssicherheitsverletzungen anzeigen.

[NSADM-40227], [NSADM-43969], [NSADM-43974], [NSADM-43977], [NSADM-43980], [NSADM-43984]

Berichte für Bot-Signatur-Updates anzeigen

In Bot-Insight können Sie jetzt die Bot-Signaturaktualisierungen im **Ereignisverlauf**anzeigen, wenn:

- Neue Bot-Signaturen werden in Citrix ADC-Instanzen hinzugefügt.
- Vorhandene Bot-Signaturen werden in Citrix ADC-Instanzen aktualisiert.

Navigieren Sie zu **Analytics > Sicherheit > Bot Insight**, und rufen Sie die Signaturaktualisierungsübersicht unter **Ereignisverlauf**auf.

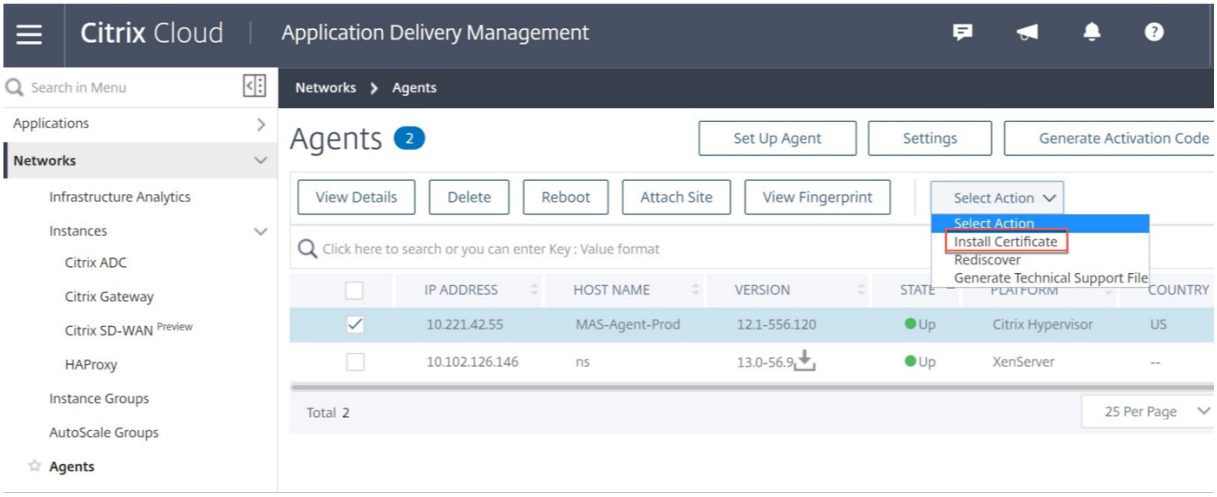
Weitere Informationen finden Sie unter Bot Einblick.

[NSADM-40228]

Installieren eines Agentenzertifikats

Um Ihre Sicherheitsanforderungen zu erfüllen, können Sie jetzt mithilfe der ADM-GUI ein Zertifikat auf den ADM-Agent hochladen. Um das Zertifikat zu installieren, navigieren Sie von der GUI zu **Netzwerke > Agents**, klicken Sie auf **Aktion auswählen** und wählen Sie **Zertifikat installieren**aus.

Weitere Informationen finden Sie unter Schnelleinstieg.



[NSADM-47904]

Festlegen von Zeichenfolgen vom Typ wörtlich in einem neuen Format

Die wörtlichen Zeichenfolgen können komplexe Eingaben wie PI-Ausdrücke in ihrem ursprünglichen Format ohne Escape-Zeichen annehmen (z. B. \\).

Um PI-Ausdrücke in eine StyleBook-Definition aufzunehmen und das Format in der Ausgabe beizubehalten, können Sie diese nun mit der folgenden Syntax angeben:

- Die neue Syntax:

```
~{
<pi-expression> }
~

Example:

~{
”HTTP.REQ.COOKIE.VALUE(”jsessionid”) ALT HTTP.REQ.URL.BEFORE_STR(
    ”=”).AFTER_STR(”;jsessionid=”) ALT HTTP.REQ.URL.AFTER_STR(”;
    jsessionid=”)” }
~
<!--NeedCopy-->
```

- Die alte Syntax:

```
 “ <pi-expression>\” ”

```



```
Example:

""HTTP.REQ.COOKIE.VALUE(\\"jsessionid\\") ALT HTTP.REQ.URL.
    BEFORE_STR(\\"=\\").AFTER_STR(\\";jsessionid=\\") ALT HTTP.REQ
    .URL.AFTER_STR(\\";jsessionid=\\")""

<!--NeedCopy-->
```

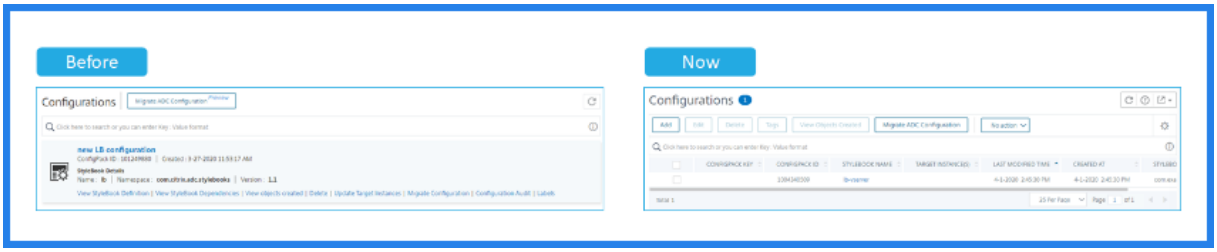
Die angegebenen PI-Ausdrücke ändern ihr Format in der Ausgabe nicht.

[NSADM-45888]

StyleBooks-Konfigurationen - Listenansicht

Die ADM-GUI zeigt die StyleBooks-Konfigurationen in der Listenansicht an. Früher wurde es in einer Kachelansicht angezeigt.

Mit dieser Änderung können Sie StyleBook-Konfigurationen nach Spaltenüberschriften sortieren. Beispielsweise können Sie Konfigurationen nach LAST MODIFIED TIME sortieren.

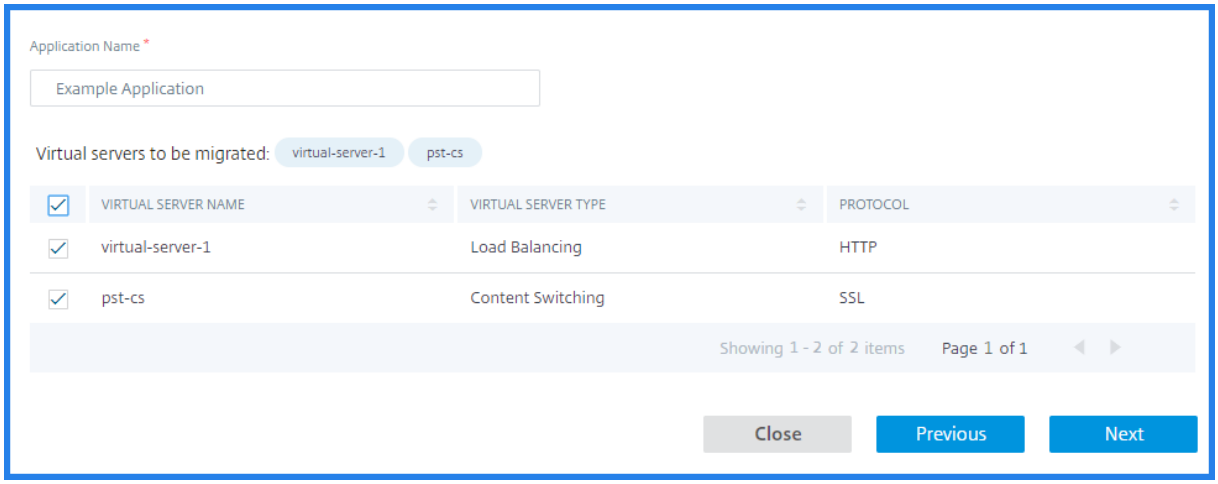


[NSADM-48918]

Migrieren mehrerer virtueller Server mit dem Konfigurations-Builder

Im Konfigurations-Builder von StyleBooks können Sie nun einen oder mehrere virtuelle Server auswählen, die von der Konfigurationsquelle zur Zielinstanz migriert werden sollen. Zuvor konnten Sie nur einen virtuellen Server auswählen, der gleichzeitig migriert werden soll.

Mit dieser Funktion können Sie die erforderlichen virtuellen Server auswählen und migrieren, die eine Anwendung zur Zielinstanz erstellen.



[NSADM-49602]

Behobene Probleme

Analytics

- Wenn Sie in **Security Insight**den Zeitschieberegler verwenden, wird die **Anwendungsübersicht** leer angezeigt.

[NSADM-50809]

Anwendungen

- Wenn Sie eine Anwendung im **App-Dashboard**auswählen, wird der Wert für die **Antwortzeit-Metrik** unter **Schlüsselmetriken** in einem falschen Format angezeigt.

  [NSADM-50274]

- Die Seite **“Anwendungen verwalten** “ wird leer angezeigt, wenn:
  - Sie löschen eine benutzerdefinierte App. Erst nach dem Klicken auf die Schaltfläche Aktualisieren werden die anderen Apps angezeigt
  - Sie ändern die Anzahl der anzuzeigenden Zeilen
  - Sie klicken auf die nächste Seite, falls mehr als eine Seite verfügbar ist

  [NSADM-50224]

- In Service Graph für Anwendungen werden die End-to-End-Transaktionsdetails vom Client zum Dienst nicht aufgefüllt, falls die Transaktion über Server mit IPv.6 stattfindet.

  [NSADM-50201]

Netzwerke

- Wenn Sie unter **KonfigurationsauftragInstanz**aus der Liste**Konfigurationsquelle**auswählen und die Option**Running Configuration**oder**Saved Configuration** auswählen, `Please provide Citrix ADC IP Address` wird eine Fehlermeldung angezeigt.

  [NSADM-50810]

- Einrückungsproblem führt zu einem Fehler bei der Agentenregistrierung

  [NSADM-50596]

- Wenn Sie in der **Konfigurationsüberwachung**den Bericht im CSV-Format exportieren, werden keine Daten angezeigt. Citrix ADM GUI hängt auch manchmal ab, wenn Sie mehrere Exporte ausführen.

  [NSADM-48322]

StyleBooks

- Falsche Fehlermeldung wird beim Kompilieren einer StyleBook-Abhängigkeit gerendert.

  [NSADM-50466]

Infrarot

- Protokollinformationen für alle Aktivitäten `mpsgroup`, die in Citrix ADM angezeigt werden sollen.

  [NSHELP-22370]

14. April 2020

Unterstützung für IPAM in ADM

ADM unterstützt IPAM (IP Address Management), um IP-Adressen in ADM-verwalteten Konfigurationen automatisch zuzuweisen und freizugeben. Sie können IP-Adressen aus Netzwerken oder IP-Bereichen zuweisen, die mit den folgenden IP-Anbietern definiert wurden:

- Integrierter IPAM-Anbieter von ADM.
- Infoblox IPAM-Lösung. Weitere Informationen finden Sie unter Infoblox DDI.

Derzeit können Sie ADM IPAM in folgenden Bereichen verwenden:

- **StyleBooks**: Automatische Zuweisung von IPs zu virtuellen Servern, wenn Sie Konfigurationen erstellen.
- **Kubernetes Ingress**: Weisen Sie einer Ingress-Konfiguration in einem Kubernetes-Cluster automatisch eine virtuelle IP-Adresse zu.

Sie können auch die zugewiesenen und verfügbaren IP-Adressen in jedem Netzwerk oder IP-Bereich verfolgen, der von ADM verwaltet wird. Weitere Informationen finden Sie unter IPAM konfigurieren.

[NSADM-48377]

Bereitstellen von internen Anwendungen in einer Autoscale-Gruppe

Sie können jetzt sowohl interne als auch externe Anwendungen in einer Autoscale-Gruppe bereitstellen, um ADM-Lösung für die automatische Skalierung zu verwenden. Zuvor konnten Sie nur externe Anwendungen bereitstellen.
Informationen zum Bereitstellen einer internen Anwendung in der Autoscale-Gruppe finden Sie unter Automatische Skalierung der Konfiguration in AWSund Automatische Skalierung der Konfiguration in Azure.

[NSADM-47520]

Neue Spalten im SSL-Dashboard hinzugefügt

Neue Spalten werden den folgenden Registerkarten im **SSL-Dashboard**hinzugefügt:

- SSL-Zertifikate — Die Spalte Key Strength wird hinzugefügt. Sie können SSL-Zertifikate mit dem Wert “Key Strength” filtern.
- SSL-Protokolle — Die Spalte Protokolltyp wird hinzugefügt. Sie können SSL-Protokolle mithilfe des Protokolltyps filtern.

[NSADM-42191]

Details zu Anwendungssicherheitsverletzungen anzeigen

Webanwendungen, die dem Internet ausgesetzt sind, sind drastisch anfällig für Angriffe geworden. Mit Citrix ADM können Sie ausführbare Verstöße visualisieren, um Anwendungen vor Angriffen zu schützen. Navigieren Sie zu **Sicherheit** > **Sicherheitsverletzungen** für eine einzelne Lösung, um:

- Greifen Sie auf die folgenden Anwendungssicherheitsverletzungen zu:
  - HTTP Slow Loris
  - DNS Slow Loris
  - Langsame HTTP-Post
  - `NXDomain` Flood Angriff
- Ergreifen Sie Korrekturmaßnahmen, um die Anwendungen zu sichern

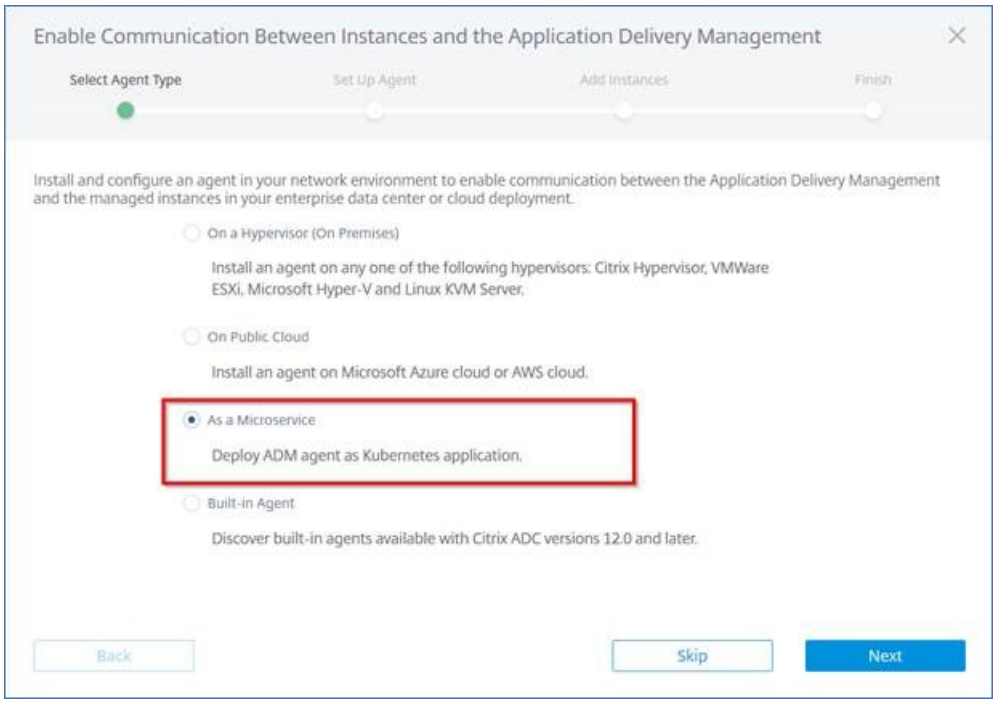
Weitere Informationen finden Sie unter Details zu Anwendungssicherheitsverletzungen anzeigen.

[NSADM-48069]

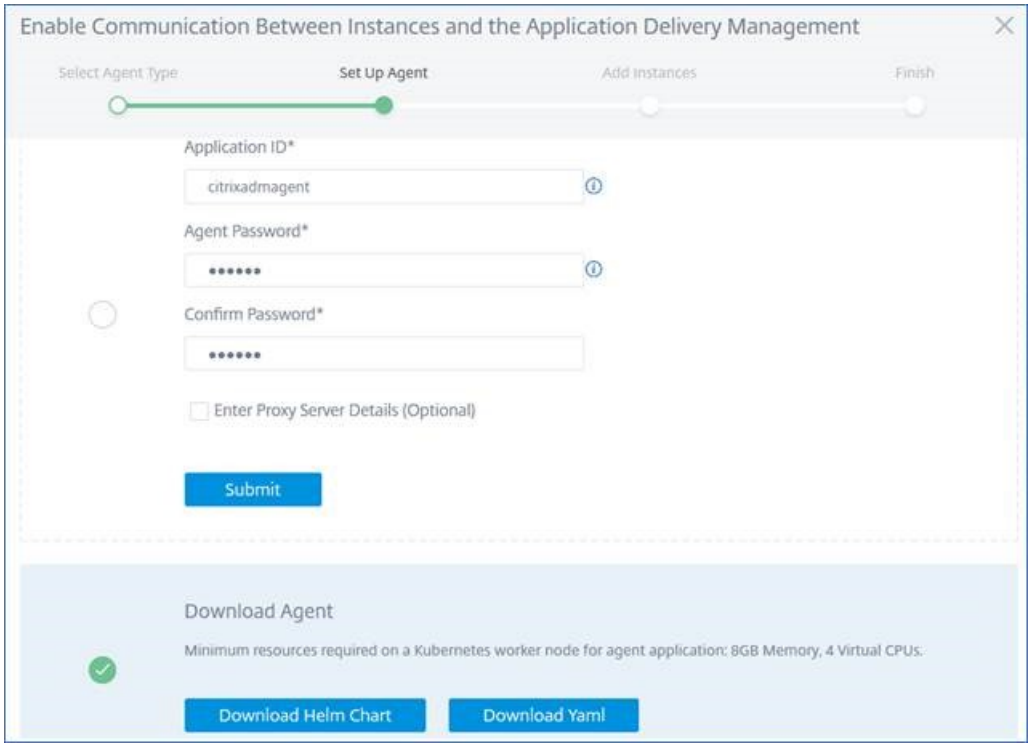
Bereitstellen von Citrix ADM Agent als Microservice

Sie können jetzt einen Citrix ADM -Agent als Microservice im Kubernetes-Cluster bereitstellen. In Citrix ADM,

1. Navigieren Sie zu **Netzwerke** > **Agents**, und klicken Sie auf **Agent einrichten**.
2. Klicken Sie auf **Erste Schritte**, wählen Sie die Option **Als Microservice** aus, und klicken Sie auf **Weiter**



3. Geben Sie die folgenden Parameter an:
    a) **Anwendungs-ID** — Eine String-ID zur Definition des Dienstes für den Agenten im Kubernetes-Cluster und zur Unterscheidung dieses Agenten von anderen Agenten im selben Cluster
    b) **Agenten-Kennwort** — Geben Sie ein Kennwort für CPX an, um dieses Kennwort zum Onboard des CPX-zu-ADM-Dienstes über den Agenten zu verwenden.
    c) **Kennwort bestätigen** — Geben Sie dasselbe Kennwort für die Bestätigung an.
    d) Klicken Sie auf “ **Senden”**.
4. Nachdem Sie auf “ **Senden**” geklickt haben, können Sie die YAML- oder Helm-Karte herunterladen



5. Speichern Sie im Kubernetes-Master die YAML-Datei und verwenden Sie den Befehl `kubectl create -f <yaml file>`

   Weitere Informationen finden Sie unter Schnelleinstieg

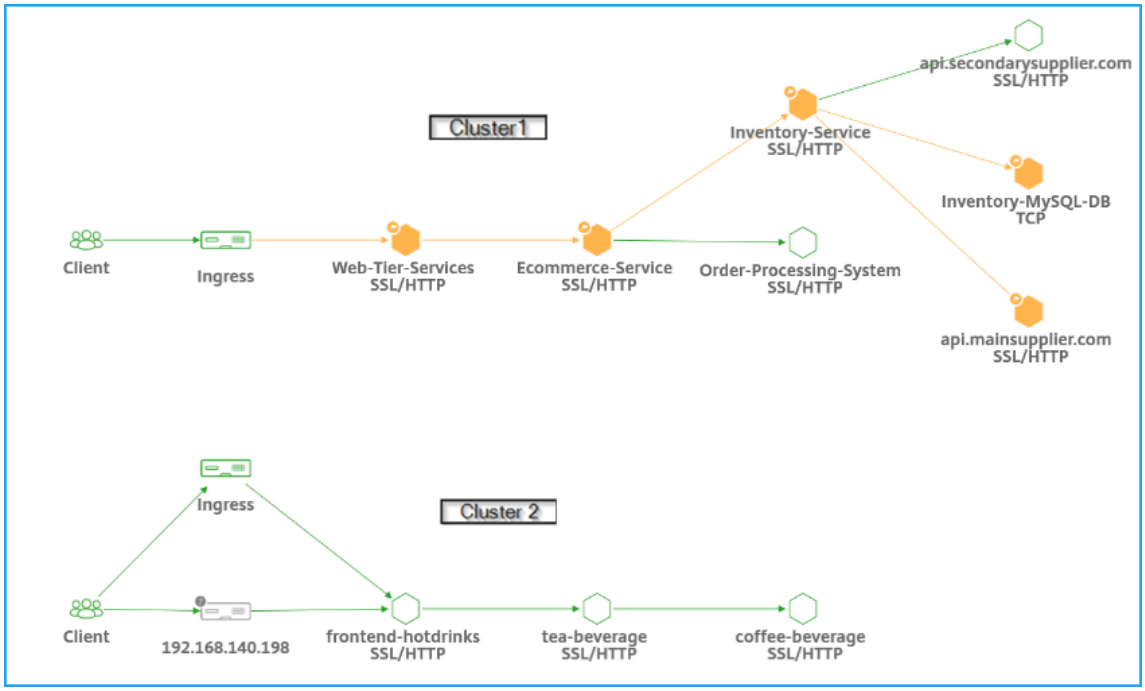
[NSADM-43971]

31. März 2020

Anzeigen mehrerer Cluster und weiterer Filter im Service-Graph

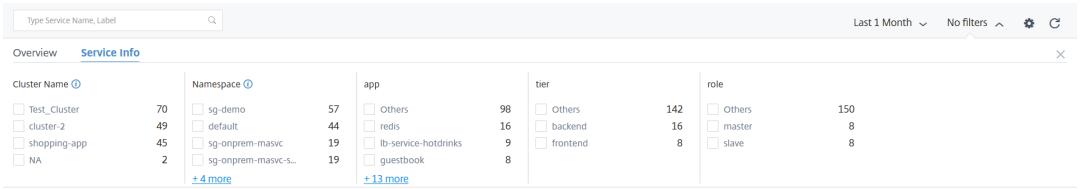
Im Service-Diagramm können Sie nun Folgendes anzeigen:

- Dienste, die jedem Cluster zugeordnet sind.



- Weitere Filter für:
  - **Cluster** — Zeigt alle Dienste an, die für den ausgewählten Cluster oder die ausgewählten Cluster gelten.
  - **Namespace** — Zeigt alle Dienste an, die für den ausgewählten Namespace gelten.

    > **Hinweis**
    >
    > Abhängig von den Labels, die für den Dienst in der Kubernetes-Service-Definition YAML konfiguriert sind, können Sie auch weitere Filteroptionen anzeigen.



[NSADM-43985]

Verteilte Ablaufverfolgung

In Service Graph können Sie nun die Trace-Informationen verwenden, um:

- Analyse der Gesamt-Serviceleistung
- Visualisieren des Kommunikationsflusses zwischen dem ausgewählten Dienst und seinen voneinander abhängigen Diensten

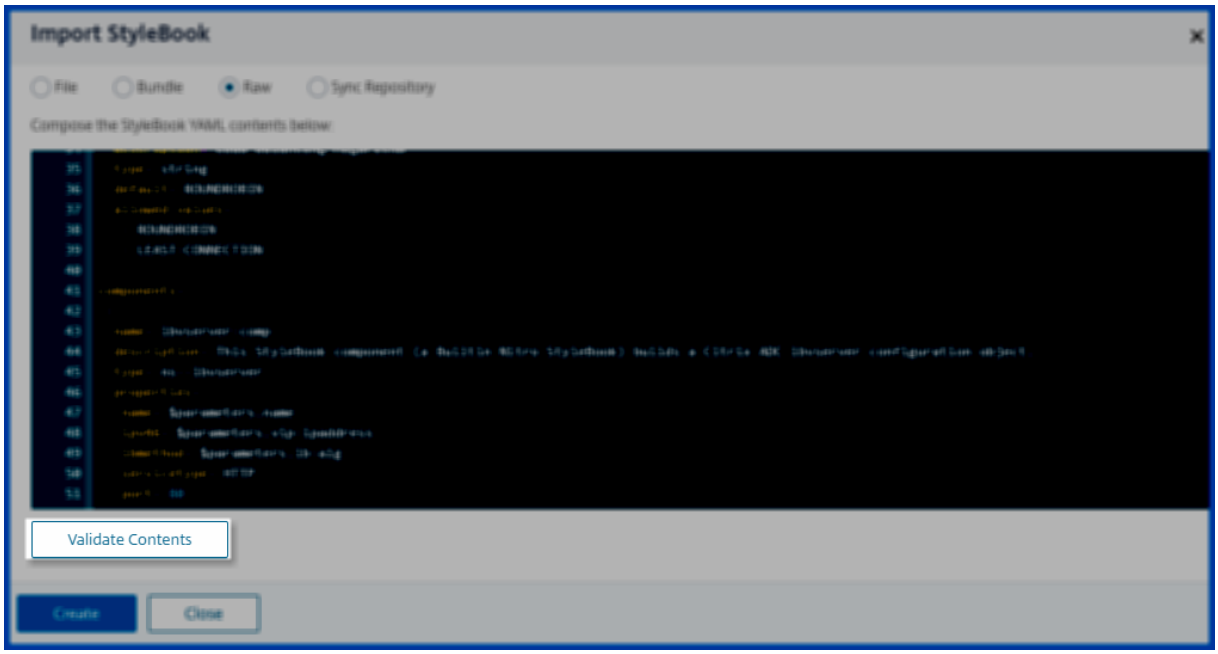
- Identifizieren Sie, welcher Dienst Fehler anzeigt, und beheben Sie den fehlerhaften Dienst
- Zeigen Sie Transaktionsdetails zwischen dem ausgewählten Service und seinem voneinander abhängigen Service an. Weitere Informationen finden Sie unter Verteilte Ablaufverfolgung

[NSADM-43976]

Überprüfen Sie den StyleBook-Inhalt, bevor Sie in ADM importieren

Wenn Sie ein StyleBook im ADM YAML-Editor erstellen, können Sie nun nach StyleBook-Grammatikfehlern suchen, ohne in ADM zu importieren.

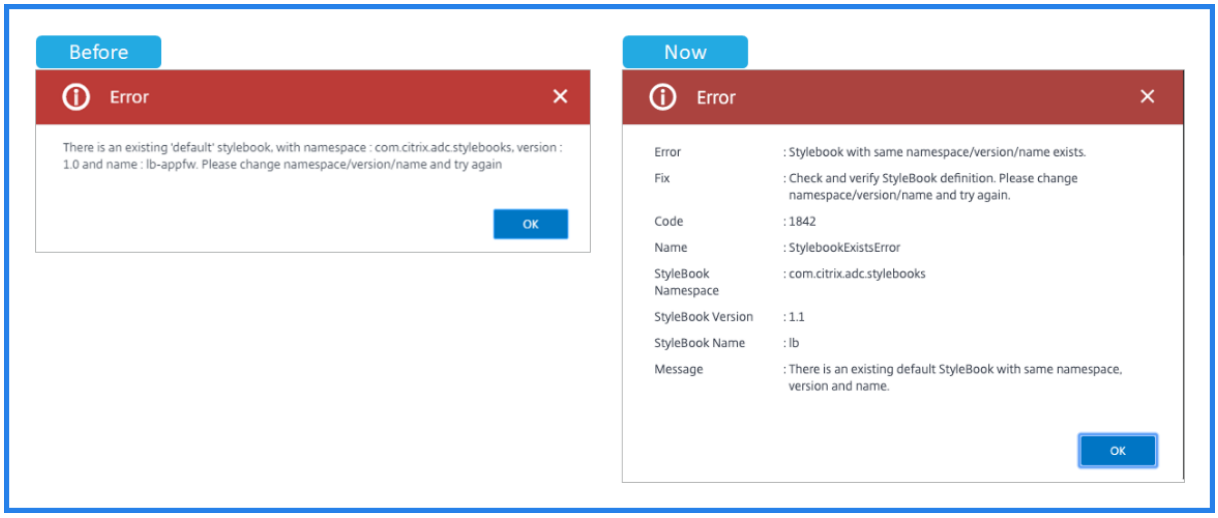
Wenn im StyleBook-Inhalt Fehler auftreten, zeigt die ADM-GUI die Fehlerdetails an. Sie können die angegebenen Fehler korrigieren und mit der Bearbeitung fortfahren oder das StyleBook importieren.



[NSADM-47978]

Verbesserte Anzeige der StyleBooks-Fehlermeldung

Die ADM-GUI zeigt eine Fehlermeldung an, wenn Sie ein StyleBook importieren, das StyleBook-Grammatikfehler aufweist. Einige Fehlermeldungen sind nun so organisiert, dass die Fehlerdetails angezeigt werden. Die Fehlerdetails umfassen Fehler, Fix, Code, Name und mehr, abhängig von den Fehlertypen. Das Feld “ **Fix** “ enthält Informationen zur Behebung eines Problems.



[NSADM-44274]

Importieren von StyleBooks aus einem beliebigen Ordner in einem GitHub-Repository

Sie können nun StyleBook-Dateien aus einem beliebigen Ordner in einem GitHub-Repository mit ADM synchronisieren. Zuvor konnten Sie nur StyleBook-Dateien importieren oder synchronisieren, die im **Stammordner des GitHub Repository** vorhanden sind.

Weitere Informationen finden Sie unter Importieren und Synchronisieren von StyleBooks aus GitHub-Repository.

[NSADM-46147]

ADC-Konfiguration anhand des Konfigurationspakets überwachen

In **StyleBooks** > **Konfigurationen**können Sie jetzt explizit die von einem StyleBook-Konfigurationspaket vorgenommenen Änderungen mit der aktuellen ADC-Konfiguration vergleichen. Mit dieser Funktion können Sie Folgendes tun:

- Erkennen Sie die Konfigurationsdrift zwischen StyleBook-Konfigurationspaket und ADC-Konfiguration.
- Identifizieren Sie alle geänderten und gelöschten Objekte im ADC, die die vom Konfigurationspaket vorgenommenen Änderungen nicht widerspiegeln.

Um die Änderungen des Konfigurationspakets mit der ADCs-Konfiguration zu vergleichen, klicken Sie im gewünschten **Konfigurationspaket auf Configuration Audit**.

Weitere Informationen finden Sie unter ADC-Konfiguration anhand des Konfigurationspakets überwachen.

[NSADM-45866]

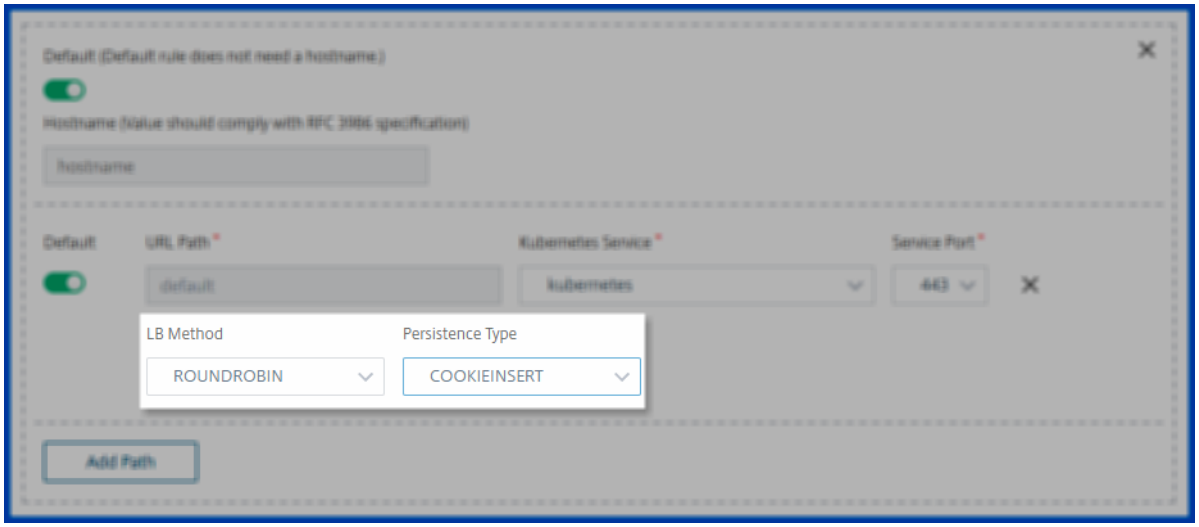
Unterstützung für Citrix Anmerkungen zum Bereitstellen einer Ingress-Konfiguration

Wenn Sie einer Eindringkonfiguration Content-Routing-Regeln hinzufügen, können Sie nun die folgenden Citrix Anmerkungen in die ADM-GUI aufnehmen:

- **LB-Methode** — Wählen Sie die bevorzugte Lastausgleichsmethode für den ausgewählten Kubernetes-Dienst aus.
- **Persistenz-Typ** — Wählen Sie den bevorzugten Load-Balancing-Persistenztyp für den ausgewählten Kubernetes-Dienst aus.

Nachdem Sie die Content-Routing-Regeln hinzugefügt haben, können Sie die ausgewählte LB-Methode und den Persistenztyp in der Ingress-Spezifikation anzeigen. Überprüfen und Bereitstellen der Ingress-Konfiguration.

Weitere Informationen finden Sie unter Bereitstellen der Ingress-Konfiguration.



[NSADM-48414]

Instanzen geben den Bereitstellungstyp mit einer Notation an

In ADM-GUI geben die Instanz-IP-Adressen nun den Bereitstellungstyp an. Die folgenden Hinweise beschreiben den Bereitstellungstyp:

- In Hochverfügbarkeitspaar, P — Primärserver und S — Sekundärer Server.
- C-Cluster
- A-Autoscale Gruppe

Wenn eine Instanz keine Notation hat, gibt sie die eigenständige Bereitstellung an.

[NSADM-41859]

März 03, 2020

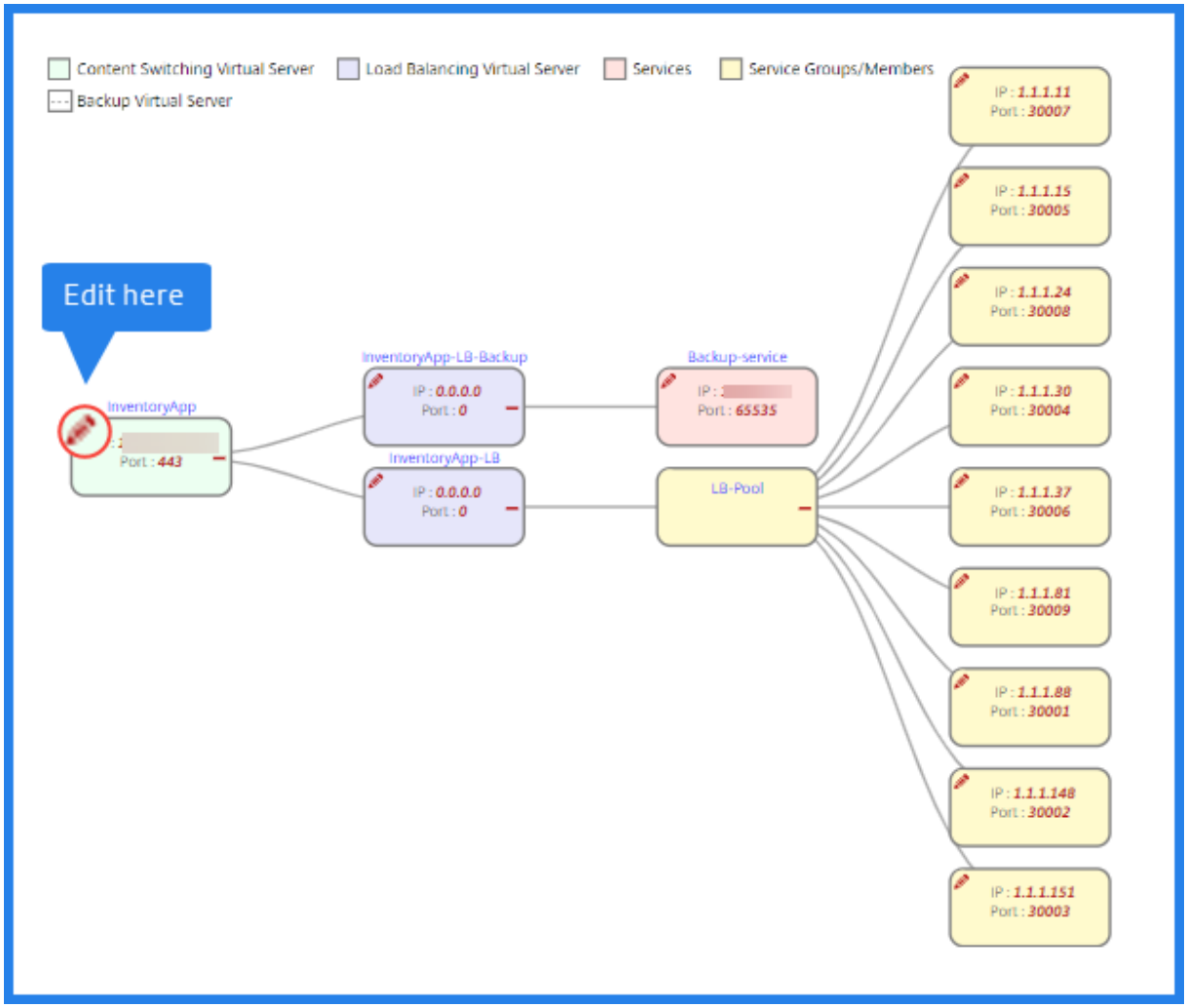
Bearbeiten der Bereitstellungsattribute im StyleBooks Configuration Builder

> **Hinweis**
>
> Diese Funktion befindet sich in der Vorschau.

Mit dem StyleBooks Configuration Builder können Sie ein StyleBook und ein Config-Paket für die Anwendungskonfiguration aus einer vorhandenen ADC-Konfiguration erstellen. Der Konfigurations-Builder automatisiert auch die Migration der Anwendungskonfiguration von einer ADC-Instanz zu einer anderen Instanz.

Mit dem Konfigurations-Builder-Assistenten können Sie jetzt Bereitstellungsattribute für die ausgewählte Anwendung bearbeiten, bevor ein StyleBook und ein Config-Paket erstellt werden. Sie können nun die IP-Adresse und den Portwert der virtuellen Server, Dienste und Dienstgruppenmitglieder in der ursprünglichen Konfiguration bearbeiten.

Nachdem die Anwendungserstellung und -migration abgeschlossen ist, wird zusammen mit dem entsprechenden StyleBook ein ConfigPack in Citrix ADM erstellt. Dieses Konfigurationspaket enthält die neuen IP-Adressen und Port-Werte. Um das erstellte ConfigPack anzuzeigen, navigieren Sie zu **Anwendungen > StyleBooks > Konfigurationen**.



Weitere Informationen finden Sie unter Migrieren der ADC-Anwendungskonfiguration mit StyleBooks Configuration Builder.

[NSADM-44197]

Möglichkeit, alle Anwendungen anzuzeigen, aber nur eine Teilmenge von Anwendungen zu bearbeiten

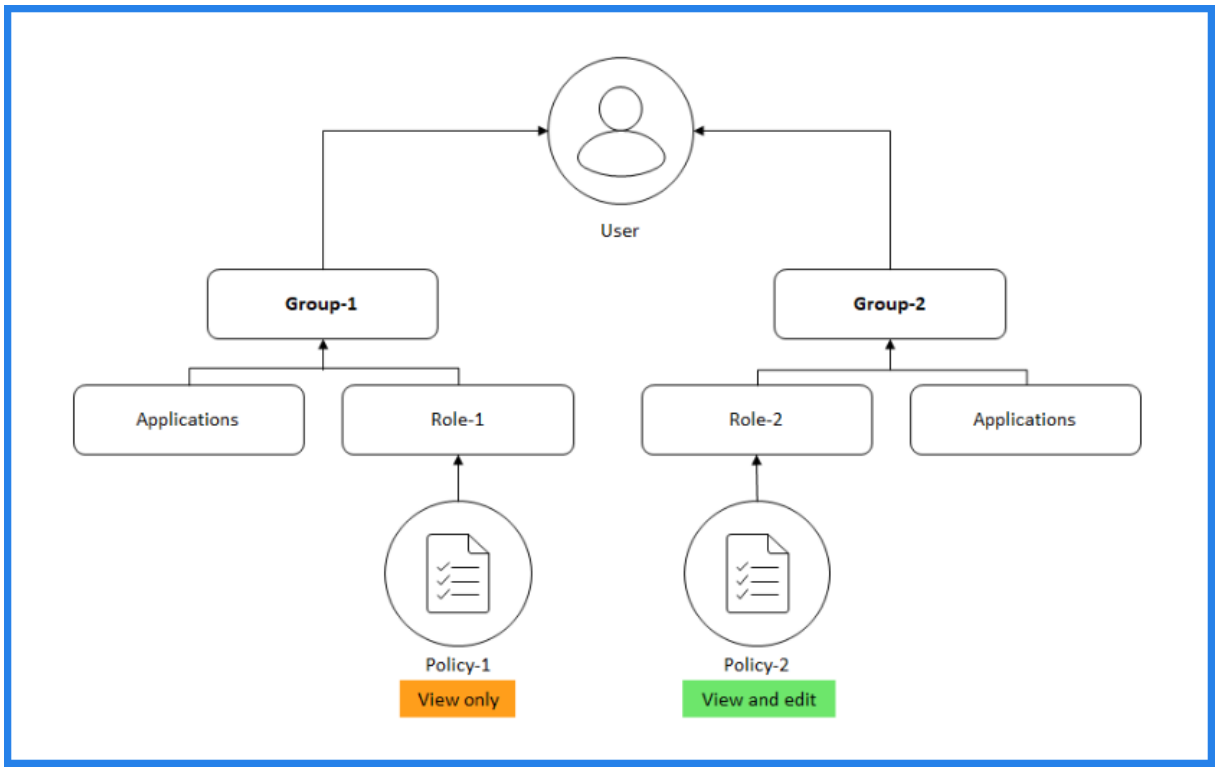
Wenn ein Administrator einer Gruppe mit unterschiedlichen Zugriffsrichtlinieneinstellungen einen Benutzer hinzufügt, wird der Benutzer mehreren Autorisierungsbereichen und Zugriffsrichtlinien zugeordnet.

In diesem Fall gewährt das ADM dem Benutzer je nach Berechtigungsumfang Zugriff auf die Anwendungen.

Betrachten Sie einen Benutzer, der einer Gruppe zugewiesen ist, die zwei Richtlinien Policy-1 und Policy-2 hat.

- Richtlinien-1 — Nur Berechtigung für Anwendungen anzeigen.
- Policy-2 — Berechtigung zum Anzeigen und Bearbeiten von Anwendungen.

Jetzt kann der Benutzer Anwendungen anzeigen, die in Policy-1 angegeben sind. Außerdem kann dieser Benutzer die in Policy-2 angegebenen Anwendungen anzeigen und bearbeiten. Der Bearbeitungszugriff auf Gruppe-1-Anwendungen ist eingeschränkt, da er nicht unter dem Berechtigungsumfang von Gruppe 1 liegt.



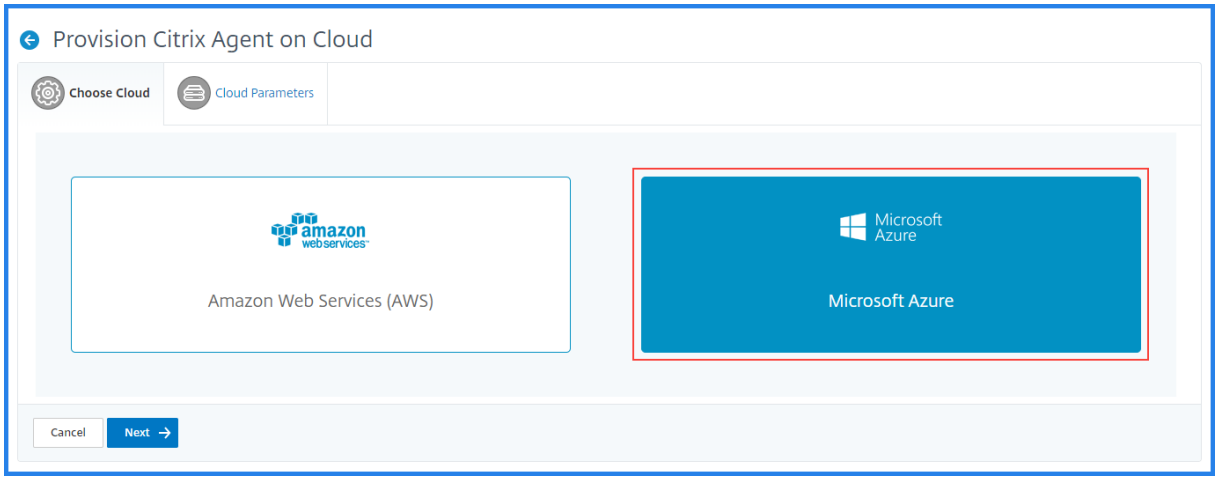
Früher betrachtete der ADM die Vereinigung aller Gruppenberechtigungen, um einen Benutzer zu autorisieren. Basierend auf dem oben genannten Beispiel konnte der Benutzer alle Anwendungen von Group-1 und Group-2 aus anzeigen und bearbeiten. Aufgrund dieser Berechtigung konnte der Benutzer die Ressourcen bearbeiten, die nicht primär durch die Zugriffsrichtlinie autorisiert wurden.

Weitere Informationen finden Sie unter Ändern des Benutzerzugriffs basierend auf dem Berechtigungsbereich

[NSHELP-5854]

Bereitstellen des Citrix ADM -Agents in Azure

Sie können jetzt einen ADM-Agent in Azure mithilfe der ADM-GUI bereitstellen. Der ADM-Agent in Azure registriert sich automatisch bei Citrix ADM. Sie können den registrierten Agent auf der Seite **Netzwerke > Agents** anzeigen. Informationen zum Bereitstellen eines ADM-Agenten in Azure finden Sie unter Bereitstellen des Citrix ADM -Agents in Azure.

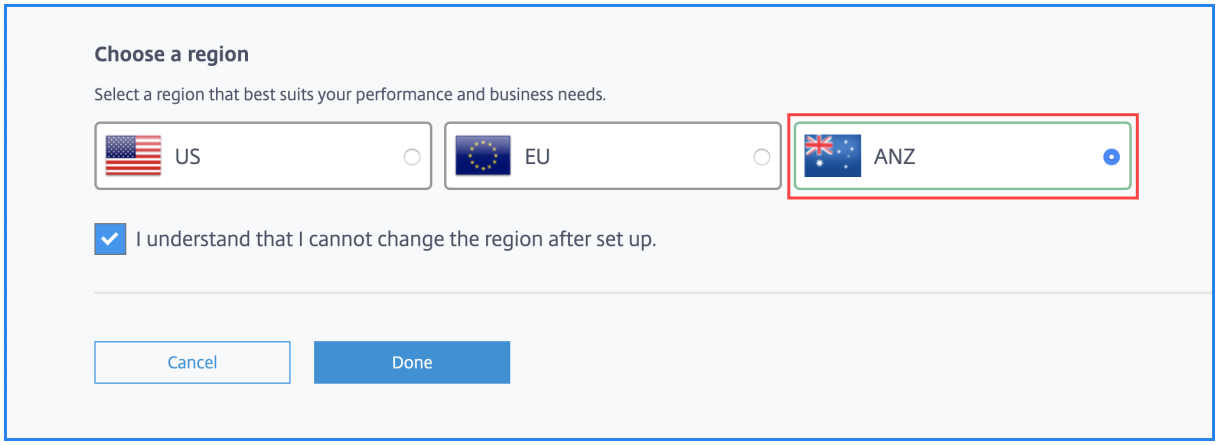


Alternativ können Sie den Citrix ADM -Agent über Azure Marketplace installieren. Weitere Informationen finden Sie unter Installieren von Citrix ADM Agent auf Azure.

Wählen Sie die Region Australien aus, um den ADM-Service einzurichten

Sie können nun die Region Australien (ANZ) auswählen, um den ADM-Service einzurichten. Citrix ADM unterstützt jetzt die folgenden Regionen:

- Vereinigte Staaten (US)
- Europa (EU)
- Australien (ANZ)



Weitere Informationen finden Sie unter Schnelleinstieg.

[NSADM-44447]

Führen Sie benutzerdefinierte Skripts vor und nach dem Upgrade-Wartungsauftrag aus

Wenn Sie Ihre ADC-Instanz aktualisieren, indem Sie einen Wartungsauftrag erstellen, führt ADM die Instanzen vor der Validierung durch, die Sie aktualisieren möchten. Auf der Registerkarte **Validierung**

vor dem Upgrade werden folgende Optionen für die ausgewählten Instanzen überprüft:

- Prüft auf Anpassungen.
- Überprüft die Datenträgerauslastung und zeigt einen Fehler an, wenn der Speicherplatz niedrig ist.
- Prüft auf Datenträgerhardwareprobleme.

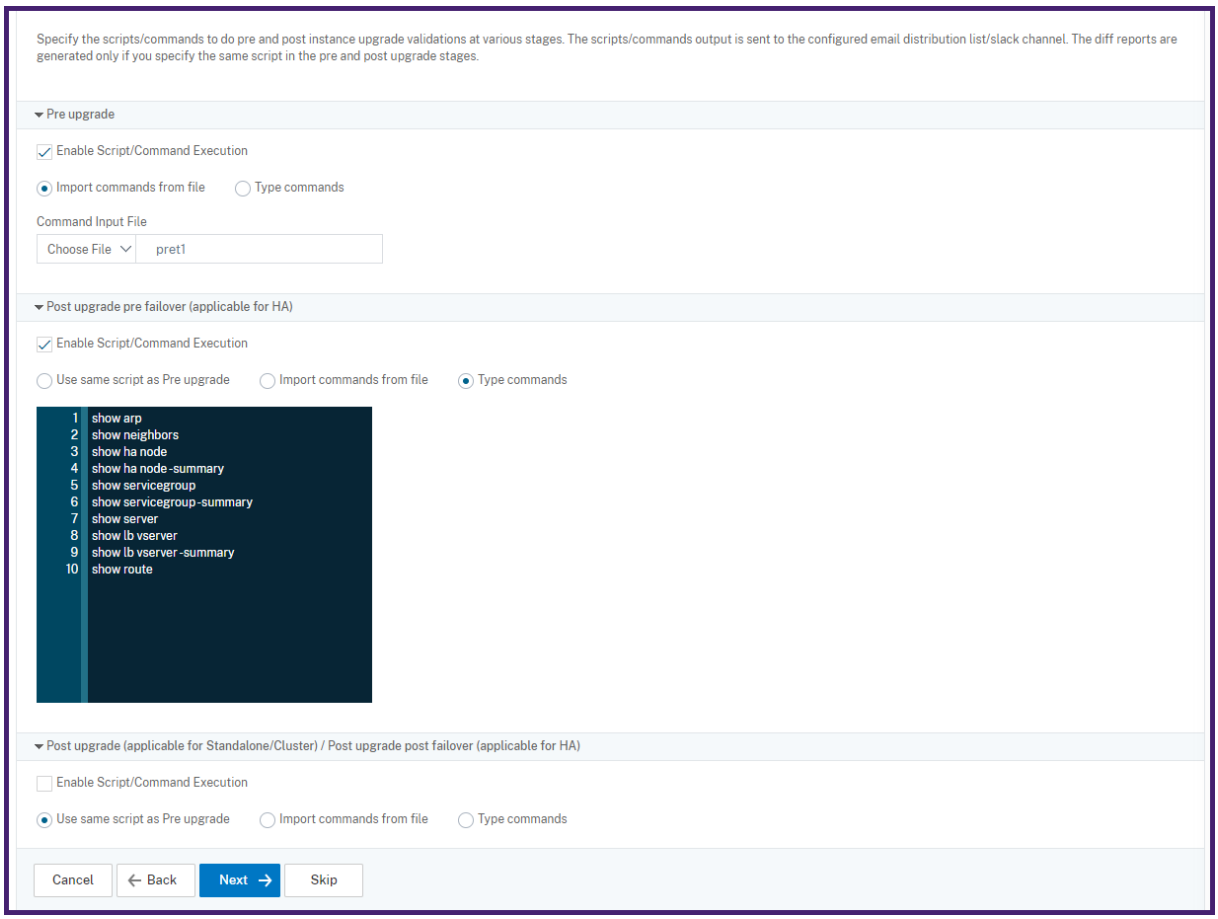
Sie können die fehlgeschlagenen Instanzen entfernen und mit dem Erstellen eines Upgrade-Wartungsauftrags fortfahren.

Geben Sie in **Custom Scripts**benutzerdefinierte Skripts an, die vor und nach einem Instanz-Upgrade ausgeführt werden sollen. Verwenden Sie eine der folgenden Möglichkeiten, um die Befehle auszuführen:

- Importieren von Befehlen aus einer Datei.
- Geben Sie Befehle direkt auf der Citrix ADM GUI ein.

Diese Skripte helfen Ihnen, die Änderungen vor und nach dem Upgrade zu überprüfen. Beispiel:

- Die Instanzversion vor und nach dem Upgrade.
- Der Status von Schnittstellen, Hochverfügbarkeitsknoten, virtuellen Servern und Diensten vor und nach dem Upgrade.
- Die Statistiken der virtuellen Server und Dienste.
- Die dynamischen Routen.



Weitere Informationen finden Sie unter Verwenden von Aufträgen zum Aktualisieren von Citrix ADC-Instanzen.

[NSADM-40534]

Upgrade-Image während der Ausführung des Auftrags in eine Instanz hochladen

Wenn Sie einen Upgrade-Wartungsauftrag planen, können Sie entscheiden, wann Sie ein Upgrade-Image in eine ADC-Instanz hochladen möchten. Wählen Sie unter Auftrag erstellen eine der folgenden Optionen:

- **Jetzt hochladen** — Mit dieser Option wird das Image sofort in eine Instanz hochgeladen.
- **Zum Zeitpunkt der Ausführung hochladen** — Diese Option lädt das Image auf eine ADC-Instanz hoch, wenn der ADM den geplanten Upgrade-Wartungsauftrag ausführt.

Weitere Informationen finden Sie unter Planen des Upgrades von Citrix ADC-Instanzen.

[NSADM-44855]

Die ADM Autoscale-Gruppen unterstützen AWS-Instanz-Typen C5, M5 und C5n

Wenn Sie ADM Autoscale-Gruppen in der AWS-Cloud erstellen möchten, können Sie jetzt ADC-Instanzen mit den AWS-Instanz-Typen C5, M5 und C5n bereitstellen. Sie können diese Instanztypen auswählen, um die automatische Skalierung von ADM mit hoher Performance zu erreichen.

> **Hinweis:**
>
> Die ADM-GUI füllt automatisch die empfohlenen AWS-Instanz-Typen für die ausgewählte ADC-Version aus. Siehe Erstellen von Gruppen mit automatischer Skalierung.

Weitere Informationen zu AWS-Instanz-Typen finden Sie unter AWS-Instanz-Typen.

[NSADM-40089]

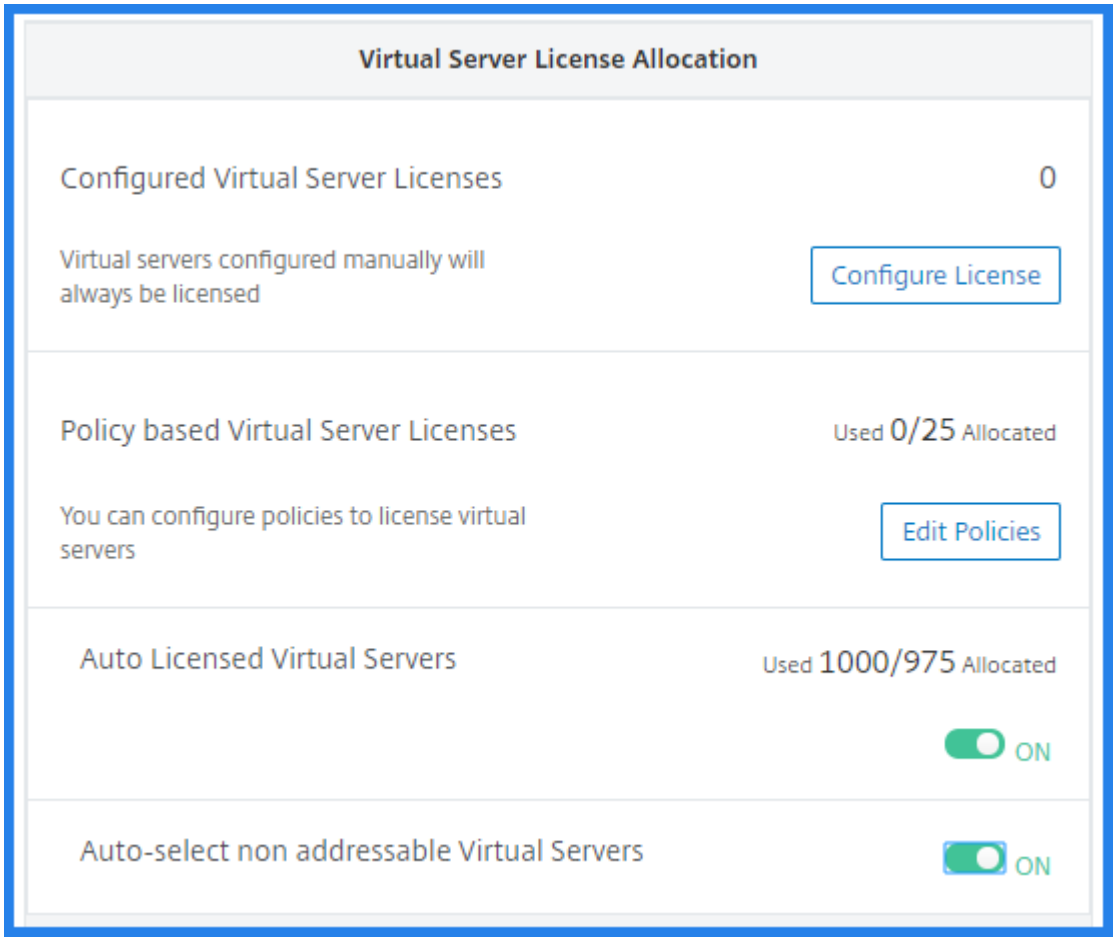
Anwenden einer Lizenz auf virtuelle Server mithilfe einer Richtlinie

In **Abonnements** können Sie jetzt eine Richtlinie konfigurieren, um eine Lizenz auf virtuelle Server anzuwenden. Zuvor konnten Sie Lizenzen nur manuell oder automatisch auf virtuelle Server anwenden. Sie können die Lizenz jetzt mithilfe einer Richtlinie oder manuell oder automatisch anwenden.

Mithilfe der Richtlinie können Sie die Anzahl der virtuellen Server steuern, die Sie automatisch lizenzieren möchten. Wenden Sie die Lizenz nur auf die virtuellen Server ausgewählter Instanzen an.

Wenn Sie eine Richtlinie bearbeiten, können Sie Folgendes angeben:

- Legen Sie die Begrenzung virtueller Server für CPX-Instanzen separat fest, um Lizenzen anzuwenden. Der ADM wendet eine Lizenz auf virtuelle Server auf CPX-Instanzen bis zu einem festgelegten Limit an.
- Legen Sie das Limit für virtuelle Server für ausgewählte ADC-Instanzen (MPX/VPX/BLX) fest, um Lizenzen anzuwenden. Der ADM wendet Lizenzen auf virtuelle Server auf ADC-Instanzen bis zu einem festgelegten Limit an.
- Wählen Sie die prioritären ADC-Instanzen aus, die virtuelle Serverlizenzen angewendet werden sollen. Daher kann der ADM eine Lizenz nur auf die virtuellen Server der ausgewählten Instanzen anwenden.



Die Optionen " **Automatisch lizenzierte virtuelle Server** " und **"Nicht adressierbare virtuelle Server automatisch auswählen** " sind jetzt unabhängig. Zuvor konnten Sie **nicht adressierbare virtuelle Server automatisch auswählen** nur aktivieren, wenn Sie **automatisch lizenzierte virtuelle Server**aktivieren.

[NSADM-35724]

Anzeigen von ADC-Kapazitätsproblemen in ADM

Wenn eine ADC-Instanz die meiste verfügbare Kapazität verbraucht hat, kann ein Paketablegen während der Verarbeitung des Clientdatenverkehrs auftreten. Dieses Problem verursacht eine geringe Leistung in einer ADC-Instanz. Wenn Sie solche ADC-Kapazitätsprobleme verstehen, können Sie proaktiv mehr Lizenzen zuweisen, um die ADC-Leistung zu stabilisieren.

So zeigen Sie ADC-Kapazitätsprobleme an:

1. Navigieren Sie zu **Netzwerke > Infrastructure Analytics**.
2. Erweitern Sie die Instanz, für die Sie Kapazitätsprobleme anzeigen möchten.

Der ADM ruft diese Ereignisse alle fünf Minuten von der ADC-Instanz ab und zeigt die verworfenen

Pakete oder Rate-Limit-Zähler-Inkremente an, falls vorhanden. Die Probleme werden nach den folgenden Kapazitätsparametern kategorisiert:

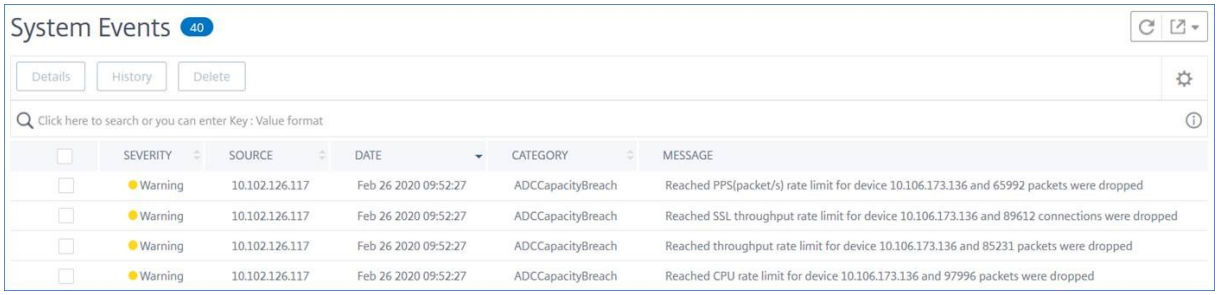
- **Durchsatzlimit erreicht** — Die Anzahl der Pakete, die in der Instanz gelöscht wurden, nachdem das Durchsatzlimit erreicht wurde.
- **PE-CPU-Limit erreicht** - Die Anzahl der Pakete, die auf allen Netzwerkkarten gelöscht wurden, nachdem das PE-CPU-Limit erreicht wurde.
- **PPS Limit erreicht** — Die Anzahl der Pakete, die in der Instanz gelöscht wurden, nachdem das PPS-Limit erreicht wurde.
- **SSL-Durchsatzrate Limit** — Gibt an, wie oft das SSL-Durchsatzlimit erreicht wurde.
- **SSL-TPS Rate Limit** — Gibt an, wie oft das SSL-TPS Limit erreicht wurde.

Der ADM berechnet die Instanzbewertung auf dem definierten Kapazitätsschwellenwert.

- Niedriger Schwellenwert — 1 Schrittweite für Paketabfall oder Ratenbegrenzungszähler
- Hoher Schwellenwert — 10000 Pakete fallen oder Rate-Limit-Zähler-Inkrement

Wenn eine ADC-Instanz den Kapazitätsschwellenwert überschreitet, wird die Instanz-Bewertung beeinträchtigt.

Wenn Pakete fallen oder Rate-Limit Zähler inkrementiert werden, wird ein Ereignis unter der Kategorie `ADCCapacityBreach`generiert. Um diese Ereignisse anzuzeigen, navigieren Sie zu **Konten > Systemereignisse**.



Wenn Sie die ADC-Kursbegrenzungsstatistiken für den ausgewählten Zeitraum (Stunde/Tag/Woche/-Monat) anzeigen möchten, navigieren Sie zu **Netzwerk > Netzwerkberichterstattung**.

[NSADM-40183]

Service-Details im Service-Diagramm anzeigen

Zeigen Sie in Service Graph mit dem Mauszeiger auf einen Dienst, und klicken Sie auf einen Dienst, um die folgenden Optionen anzuzeigen:

- **Details anzeigen**
- **Transaktionsprotokolle** - Ermöglicht das Anzeigen der HTTP- und SSL-über-HTTP-Transaktionsdetails. Weitere Informationen finden Sie unter Anzeigen von Web-Transaktionsprotokollen.

Mit der Option **Details anzeigen** können Sie Folgendes anzeigen:

- Der Clustername, in dem der Dienst gehostet wird
- Der Namespace und die Service-Labels des Dienstes
- Alle zugeordneten eingehenden und ausgehenden Dienste, die mit dem ausgewählten Dienst verbunden sind
- Service-Schlüssel-Metriken in einem Diagrammformat wie **Hits**, **Service-Reaktionszeit**, **HTTP-Fehler**, **Datenvolumen, SSL-Front-End-Fehler**, **SSL-Back-End-Fehler**, **TCP-Front-End-Fehler**und **TCP-Back-End-Fehler**

Mithilfe dieser wichtigsten Metrik-Trends können Sie analysieren, wie der Service für die ausgewählte Zeitdauer abläuft.

Weitere Informationen finden Sie unter Service-Details anzeigen.

[NSADM-41297]

Dienstdiagramm für Anwendungen anzeigen (GSLB)

> **Hinweis**
>
> Diese Funktion befindet sich in der Vorschau.

Sie können jetzt GSLB-Anwendungen in Service Graph anzeigen, um Folgendes anzuzeigen:

- Wie die Anwendung konfiguriert wird (mit GSLB-Anwendung, Rechenzentrum, ADC-Instanz, CS- und LB-Servern)
- End-to-End-Ansichten vom Client zu Services
- Der Name des Rechenzentrums, in dem die Clientanforderungen verarbeitet werden, und die zugehörigen Citrix ADC Metriken für Rechenzentren
- Der Status des virtuellen GSLB-Servers, z. B. Kritisch, Überprüfen und Gut. Citrix ADM zeigt den Status des virtuellen Servers basierend auf der App-Bewertung an.
- **Kritisch (rot)** — Zeigt an, wann die App-Bewertung < 40
- **Review (orange)** - Zeigt an, wenn die App-Punktzahl zwischen 40 und 75 liegt.
- **Gut (grün)** - Zeigt an, wenn die App-Punktzahl > 75 ist

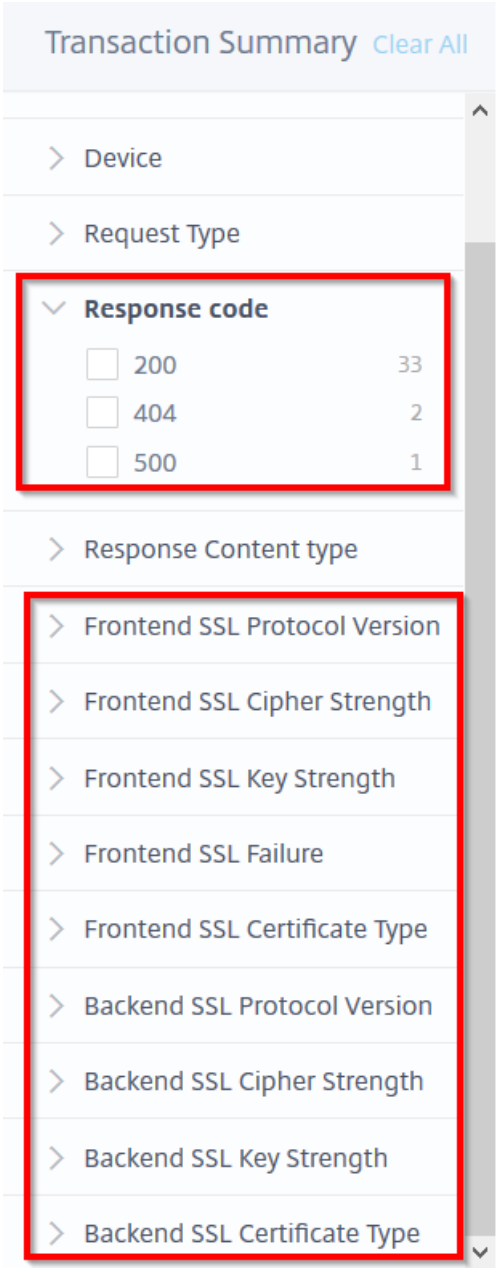
Weitere Informationen finden Sie unter Service-Diagramm.

[NSADM-43967]

4xx- und SSL-Metriken im Transaktionsübersichtsfenster anzeigen

Im Fenster “ **Transaktionsübersicht” für Web-Transaktionsanalysen** können Sie nun Folgendes anzeigen:

- 4xx Fehler
- SSL-Front-End- und SSL-Backend-Metriken



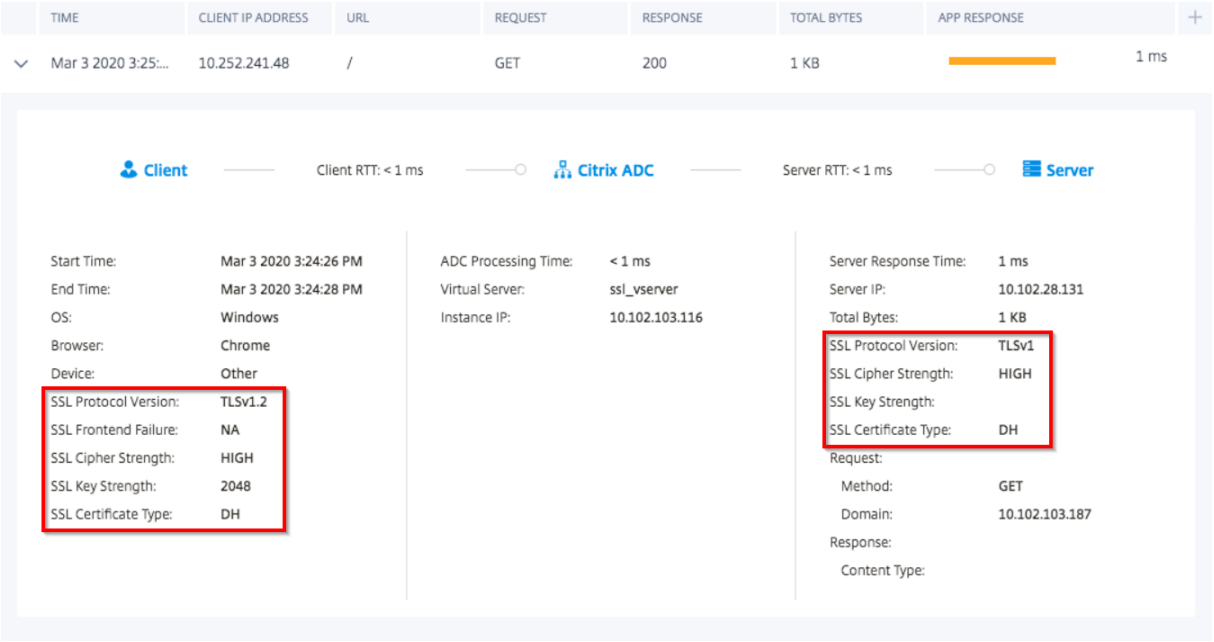
Weitere Informationen finden Sie unter Anzeigen von Analysen für Web-Transaktionen.

[NSADM-43841]

Anzeigen von SSL-Metriken in Web-Transaktionsanalysen

Wenn Sie in Web-Transaktionsanalysen auf eine Transaktion klicken, können Sie jetzt weitere Metriken für SSL-Transaktionen anzeigen. Anhand dieser Metriken können Sie analysieren, ob die SSL-Fehler vom Client oder Server auftreten.

Die folgenden Metriken werden für Client und Server angezeigt:

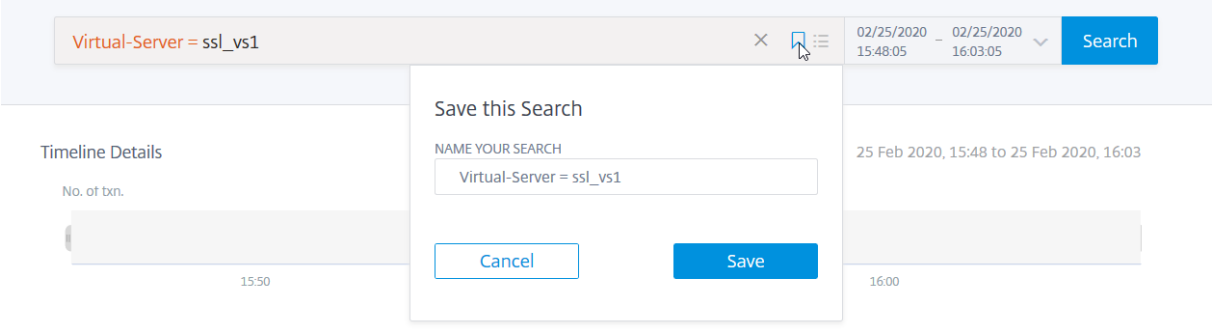


Weitere Informationen finden Sie unter Anzeigen von Analysen für Web-Transaktionen.

[NSADM-43844]

Suchoption in der erweiterten Web-Transaktionsanalyse speichern

Mit der erweiterten Suchoption in der Web-Transaktionsanalyse können Sie nun die Suchanfragen speichern. Sie können dann in der Liste auf die gespeicherte Suchanfrage klicken, anstatt die Vorschläge und Operatoren erneut zu verwenden.
Um eine Suchabfrage zu speichern, klicken Sie auf das Lesezeichensymbol, geben Sie einen Namen Ihrer Wahl an und klicken Sie auf **Speichern**.



Weitere Informationen finden Sie unter Anzeigen von Analysen für Web-Transaktionen.

[NSADM-43843]

Behobene Probleme

Anwendungen

- Das Anwendungs-Dashboard zeigt keine Anwendungen von ADC-HA-Paar und -Cluster an.

[NSADM-47668]

- Citrix ADM zeigt eine Fehlermeldung im Anwendungs-Dashboard an, wenn kein Agent hinzugefügt wird.

[NSADM-47444]

- Anwendungs-Dashboard wird im **IE 11-Browser** leer angezeigt.

[NSADM-47812]

Analytics

- Wenn Sie Client Side Measurement auf ADC-Instanzen AppFlow aktivieren, schlägt der Citrix ADM AppFlow Decoder-Protokolldateiprozess fehl.

[NSHELP-21462]

Netzwerke

- Der ADC-Hostname wird nicht unter **Netzwerkfunktionen > GSLB**angezeigt.

[NSADM-47335]

- Das **Network Reporting Dashboard** zeigt keine vollständigen Daten für einen Monat an.

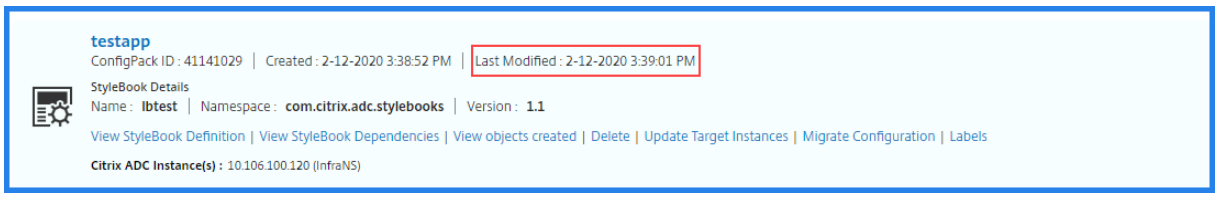
[NSHELP-21731]

Februar 11, 2020

Neue und erweiterte Features

StyleBooks-Konfiguration zeigt eine neue Spalte an

Unter **Anwendungen** > **StyleBooks** > **Konfigurationen**zeigt eine StyleBook-Konfiguration (Config-Paket) nun den Zeitpunkt der letzten Aktualisierung auf der Konfigurationskachel an.



[NSADM-45811]

Behobene Probleme

Analytics

- Die wöchentlichen Berichte für Web Insight und HDX Insight werden nicht angezeigt.

  [NSADM-46149]

Anwendungen

- Die Standarddauer im Anwendungs-Dashboard zum Anzeigen von App-Analysen wird auf 15 Minuten geändert.

  [NSADM-46980]

- Wenn Sie eine benutzerdefinierte Anwendung mithilfe der StyleBook-Konfiguration erstellen, funktionieren die Bearbeitungs- und Löschoptionen nicht wie erwartet.

  [NSADM-46821]

Lizenzierung

- Die Option für die gepoolte Kapazität wird zum ersten Mal nicht unter Bandbreitenlizenztyp angezeigt.

  Workaround:

  1. Wählen Sie in der Liste Lizenztyp die Option Virtuelle CPU-Lizenzen aus.
  2. Ändern Sie die Auswahl in Bandbreitenlizenz, um die Option Pooled Capacity auszuwählen.

  [NSADM-40129]

Netzwerke

- Wenn Sie einen Konfigurationsauftrag mit vielen Befehlen erstellen, wird die Option **Abbrechen** auf der Registerkarte **Aktion** nicht angezeigt.

  [NSADM-47041]

03. Februar 2020

Neue und erweiterte Features

Service Graph für Anwendungen

Mit der Service-Graph-Funktion aus dem Anwendungs-Dashboard können Sie Folgendes anzeigen:

- Details zur Konfiguration der Anwendung (mit dem virtuellen Content Switching Server und dem virtuellen Load Balancing Server)
- End-to-End-Ansichten von Clients zu Services
- Der Speicherort, von dem aus der Client auf die Anwendung zugreift
- Metrikdetails für Client-, Dienst- und virtuelle Server
- Wenn die Fehler vom Client oder vom Dienst stammen
- Der Dienst, der virtuelle Server und der Clientstatus wie **Kritisch**, **Überprüfen**und **Gut**.

Weitere Informationen finden Sie unter Service-Diagramm.

[NSADM-41898]

Ein verbessertes Anwendungs-Dashboard

Mit dem Anwendungs-Dashboard können Sie nun die folgenden neuen Funktionen anzeigen:

- Anwendungsstatus (kritisch, fair, gut und nicht anwendbar)
- Details zur Konfiguration der Anwendung (Load Balancing oder Content Switching)
- Details zu den Diensten, die mit der ausgewählten Anwendung verknüpft sind
- Metrikdetails für die ausgewählte Anwendung, wie Reaktionszeit der Anwendung, Durchsatz, Anforderungen pro Sekunde, Fehlerprozentsatz, Gesamtverbindungen und Datenvolumen in Form eines Diagramms
- Alle für die ausgewählte Anwendung anwendbaren Probleme

Weitere Informationen finden Sie unter Anwendungen.

[NSADM-32894]

Leistungsindikatoren in App Analytics

Citrix ADM zeigt nun die folgenden neuen Leistungsindikatoren für Anwendungen an, die in der Citrix ADC Webanwendung auftreten:

- Unsachgemäßer Persistenz-Typ
- Instabiler Server (5xx)
- Empfehlung zur Wiederverwendung von Sitzungen (SSL)
- SSL-Echtzeit-Datenverkehr
- Ungewöhnlich große HTTP-Header

- TCP-Treffer für die Wiederzusammensetzung der Warteschlange
- SurgeQueue-Aufbau

Sie können diese Anwendungsprobleme anzeigen, indem Sie zu **Anwendungen > Dashboard** navigieren und dann eine Anwendung auswählen.

Weitere Informationen finden Sie unter Leistungsindikatoren für Anwendungsanalysen.

[NSADM-39779]

Unterstützung der Webanwendungsfirewall in Citrix ADM

Die folgenden neuen WAF-Schutzrichtlinien (Web Application Firewall) sind in Security Insight aktiviert, die Verstöße für WAF hervorheben:

- APPFW_BUFFEROVERFLOW_QUERY
- APPFW_BUFFEROVERFLOW_TOTAL_HDR

[NSADM-43541]

StyleBooks-Konfiguration ADC-Instanz-Hostname anzeigen

Eine StyleBooks-Konfiguration (Config-Paket) zeigt nun den Hostnamen der ADC-Instanz zusammen mit der IP-Adresse auf der Konfigurationskachel an. Sie können nun StyleBook-Konfigurationen mithilfe des Hostnamens oder der IP-Adresse durchsuchen.

[NSADM-42517]

Entfernen von nicht erreichbaren Kubernetes-Clustern

Sie können Kubernetes Ingresses jetzt auch dann aus dem ADM-Dienst entfernen, wenn der Cluster nicht erreichbar ist oder nicht mehr vorhanden ist. Nachdem Sie die Ingresses auf dem Cluster gelöscht haben, können Sie den übergeordneten Cluster unabhängig von seiner Erreichbarkeit auch löschen.

[NSADM-45612]

Verarbeiten von Ingress-Ereignissen mit der Citrix Ingress-Klasse

Citrix ADM ServiceNow verarbeitet die Ingress-Ereignisse, die nur Citrix Ingress-Klassenannotation (`kubernetes.io/ingress.class: Citrix`) enthalten. Außerdem enthalten Ingress-Spezifikationen, die vom ADM-Dienst generiert werden, die Citrix Ingress-Klassenanmerkungen.

[NSADM-45613]

Konfigurieren der gepoolten Kapazitätslizenz für Citrix ADC FIPS-Instanzen

Jetzt können Sie eine gepoolte Kapazitätslizenz für die Citrix ADC MPX- und VPX FIPS-Lizenz konfigurieren. Weitere Informationen finden Sie unter Konfiguration der gepoolten Kapazität.

[NSADM-31742]

Neue Standard-Abrufzeit für Netzwerkfunktions-Entitäten

Die Standardabrufzeit von Netzwerkfunktionseinheiten wird von 30 auf 60 Minuten geändert. Standardmäßig ruft der Citrix ADM Dienst konfigurierte Netzwerkfunktionsentitäten automatisch alle 60 Minuten ab.

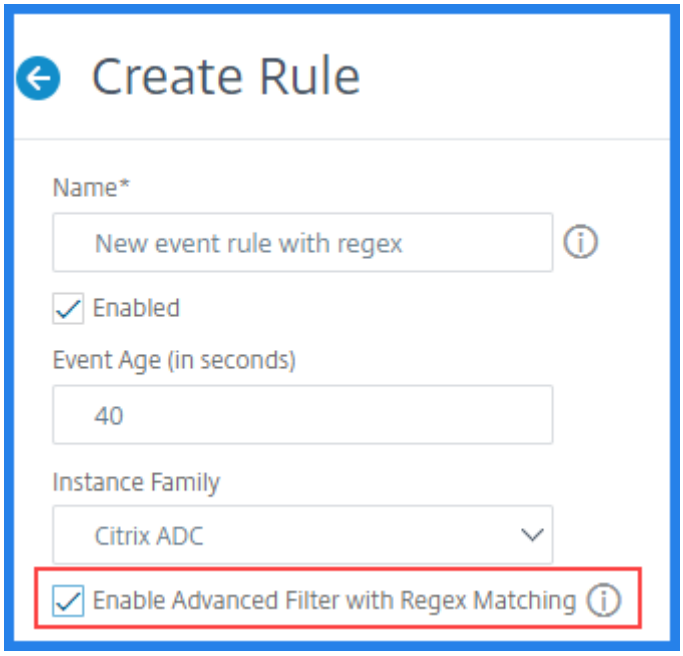
Weitere Informationen finden Sie unter Wie Citrix ADM verwaltete Instanzen und Entitäten abfragt.

[NSADM-44078]

Erweiterter Filter mit Regex-Musteranpassung

Sie können nun Fehlerobjekte, Konfigurationsbefehle und Nachrichten filtern, indem Sie Musterabgleich für reguläre Ausdrücke verwenden. Zuvor konnten Sie nur einen Sternchenmusterabgleich (*) verwenden, um Ereignisse zu filtern.

Weitere Informationen finden Sie unter Definieren einer Ereignisregel.



[NSADM-43614]

Feature-spezifische Exportberichte anzeigen und bearbeiten

Citrix ADM zeigt funktionsspezifische geplante Exportberichte unter einzelnen ADM-Features an, die Sie anzeigen, bearbeiten oder löschen können. Um beispielsweise die Exportberichte von Citrix ADC-Instanzen anzuzeigen, navigieren Sie zu **Netzwerk > Instanzen > Citrix ADC** und klicken Sie auf das Exportsymbol. Auf der Seite " **Berichte exportieren** " werden alle Exportberichte von ADC-Instanzen angezeigt. Früher wurden geplante ADM-Exportberichte unter **Konto > Exportzeitpläne** aufgelistet.

Weitere Informationen finden Sie unter Exportieren oder Planen von Exportberichten.

[NSADM-43329]

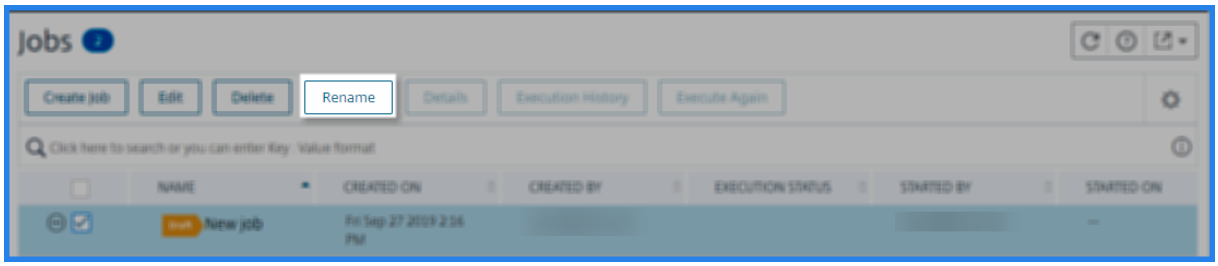
Anzeigen und Herunterladen von Citrix ADC SSL-Zertifikaten

Die Citrix ADM GUI zeigt alle SSL-Zertifikate der erkannten Citrix ADC-Instanzen an. Um SSL-Zertifikate von ADC-Instanzen anzuzeigen und herunterzuladen, navigieren Sie zu **Netzwerke > SSL-Dashboard > SSL-Zertifikatdateien in Citrix ADC**.

[NSHELP-6556]

Umbenennen von Konfigurationsaufträgen und -vorlagen

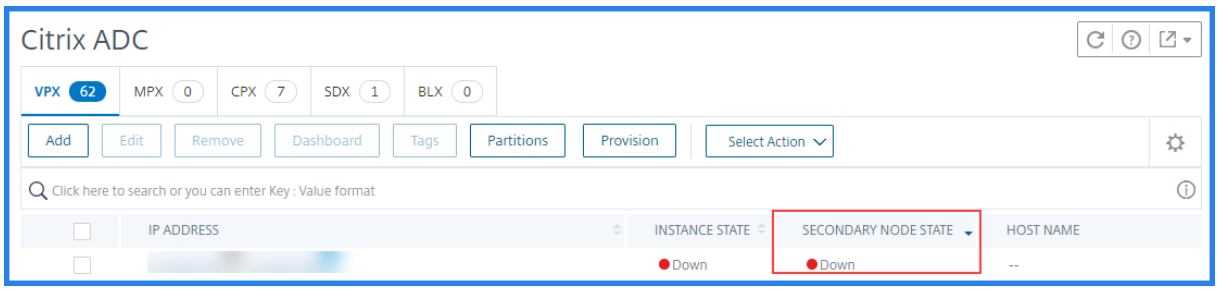
Sie können jetzt benutzerdefinierte Konfigurationsaufträge und benutzerdefinierte Überwachungsvorlagen in Citrix ADM umbenennen.



[NSADM-42945, NSHELP-6488]

Eine neue Spalte für den Status der sekundären Instanz

In der Citrix ADM GUI können Sie nun den Status der sekundären Instanz eines Hochverfügbarkeitspaars unter **Netzwerke > Instanzen**überprüfen. Wenn Sie beispielsweise auf **Citrix ADC**klicken, wird eine neue Spalte für den Status der sekundären Instanz angezeigt. Die Citrix ADM GUI zeigt den Status der sekundären Instanz auf der Übersichtsseite der Instanz an. Jetzt können Sie den Status in der Spalte **Sekundärknotenstatus** und im Dashboard anzeigen.



[NSHELP-6236]

Behobene Probleme

- Wenn Sie im **App Dashboard**eine benutzerdefinierte Anwendung mithilfe von StyleBooks definieren, werden die StyleBooks am unteren Rand der Seite angezeigt, die schwierig zu navigieren war.

  Mit diesem Fix werden die StyleBooks auf der neuen Seite angezeigt. Nachdem Sie die Details für das ausgewählte StyleBook angegeben haben, wird die neue Anwendung im **App-Dashboard**angezeigt.

  [NSADM-45241]

- Wenn Sie eine Datei hochladen, die mehrere Perioden (.) im Dateinamen enthält, um einen Konfigurationsauftrag zu erstellen, zeigt die Citrix ADM GUI einen Fehler an. Daher wird kein Konfigurationsauftrag erstellt.

  [NSADM-45748]

17. Dezember 2019

Neue und erweiterte Features

Unterstützung für Citrix ADM Agent-Failover

Das Agenten-Failover kann an einem Standort mit zwei oder mehr registrierten Agenten auftreten. Wenn ein Agent in der Site inaktiv wird (DOWN Status), verteilt der Citrix ADM Dienst die ADC-Instanzen des inaktiven Agents mit anderen aktiven Agenten neu.

Um ein Agent-Failover zu erzielen, wählen Sie nacheinander die erforderlichen Citrix ADM -Agents aus und fügen Sie sie an dieselbe Site an. Weitere Informationen finden Sie unter Konfigurieren von Citrix ADM -Agenten für die Bereitstellung mehrerer Sites.

[NSADM-30048]

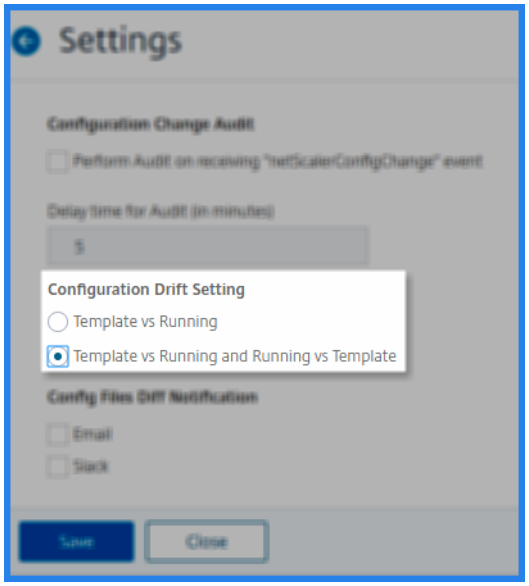
Anzeigen der Citrix ADC Konfigurationsdrift in zwei Modi

In der Citrix ADM GUI können Sie nun die Konfigurationsdrift in zwei Modi anzeigen.

1. **Vorlage vs Ausführen**: Der ADM-Dienst vergleicht die Konfiguration der Überwachungsvorlagen mit der laufenden Konfiguration auf der Instanz.
2. **Template vs Running und Running vs Template**: Der ADM-Dienst vergleicht die Konfiguration auf beiden Arten:
    - Vergleicht die Konfiguration der Überwachungsvorlagen mit der laufenden Konfiguration auf der Instanz.
    - Vergleicht die laufende Konfiguration auf der Instanz mit der Überwachungsvorlage.

Nach dem Vergleich zeigt die Citrix ADM GUI den Unterschied zwischen der Überwachungsvorlage und der laufenden Konfiguration an. Außerdem werden die Befehle zum Korrigieren der laufenden Konfiguration in der Überwachungsvorlage angezeigt.

Standardmäßig ist die Einstellung “Template vs running drift” ausgewählt. Um die Drift-Einstellung zu ändern, wählen Sie in der ADM-GUI **Einstellungen** auf der Seite **Configuration Audit (Konfigurationsüberwachung**).



Weitere Informationen finden Sie unter Vorlage vs Laufende Diff.

[NSHELP-6463]

Ausführen eines Konfigurationsauftrags auf einem sekundären Citrix ADC-Knoten

In einem Citrix ADC Hochverfügbarkeitspaar können Sie jetzt entweder den primären Knoten oder den sekundären Knoten oder beide Knoten auswählen, um einen Konfigurationsauftrag auszuführen.

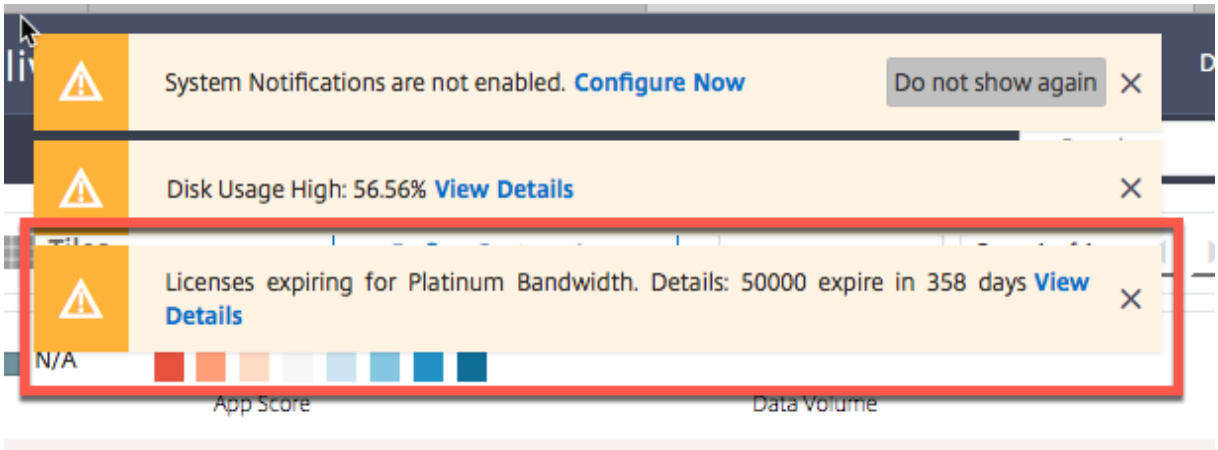
Wenn Sie den Knoten nicht angeben, wird der Konfigurationsauftrag automatisch auf dem primären Knoten ausgeführt.

Zuvor konnten Sie Konfigurationsaufträge nur auf dem primären Knoten ausführen. Weitere Informationen finden Sie unter So erstellen Sie einen Konfigurationsauftrag.

[NSHELP-6567]

Ablaufbenachrichtigung für Check-in-Check-out-Lizenz

Wenn Sie sich beim ADM-Dienst anmelden, wird eine Systemwarnungsmeldung angezeigt, wenn Ihre Check-In-Check-out-Lizenz bald abläuft. Um die Warnung zu erhalten, müssen Sie die Lizenzbenachrichtigung konfigurieren. Weitere Informationen zum Konfigurieren finden Sie unter Ablaufüberprüfungen für virtuelle Serverlizenzen.



[NSADM-42655]

Bandbreitendetails in gepoolter Kapazitätslizenzbenachrichtigung

Die Ablaufbenachrichtigung für ADM-gepoolte Kapazitätslizenzierung enthält jetzt Bandbreitendetails. Sie können die Bandbreite sehen, die im Begriff ist, aus dem gesamten Pool abläuft. Bisher waren die Bandbreitendetails nur in der GUI verfügbar. Um eine Ablaufbenachrichtigung zu erhalten, müssen Sie den ADM-Dienst konfigurieren. Weitere Informationen finden Sie unter Ablaufüberprüfungen für virtuelle Serverlizenzen.

[NSADM-39332]

Anzeigen von Instanzdetails in Infrastructure Analytics

Wenn Sie in Infrastrukturanalysen auf eine Instanz-IP-Adresse klicken, können Sie nun die folgenden Details auf der Registerkarte **Übersicht** anzeigen:

- Instanzbewertung, Ausgabekategorien, die sich auf die Instanzbewertung auswirken, und andere Instanzdetails.
- Wichtige Metriken der Instanz wie CPU-Auslastung, Speicherauslastung, Durchsatz, HTTPS-Anforderungen/Sek, TCP-Verbindungen und SSL-Transaktionen.
- Details zu allen Problemen, die sich auf die Instanzbewertung auswirken.

Weitere Informationen finden Sie unter Infrastrukturanalyse.

[NSADM-42276]

Bekannte Probleme

April 28, 2021

Citrix Application Delivery Management (Citrix ADM) weist die folgenden bekannten Probleme auf:

Analytics

Wenn Sie in Gateway Insight einen Bericht planen (**Berichte exportieren > Export planen)**, zeigt der generierte Bericht “Seite nicht gefunden” an.

[NSHELP-26283]

Netzwerke

- In der **Security Advisory** GUI unter **Networks>Instanz Advisory>Security Advisory**werden möglicherweise nicht alle CVEs angezeigt, und nur ein CVE kann in Berichten oder im Beratungs-Dashboard angezeigt werden.

  Problemumgehung: Klicken Sie auf **Jetzt scannen**, um einen Anforderungsscan auszuführen. Nachdem der Scan abgeschlossen ist, werden alle CVEs im Bereich (ungefähr 15) in der GUI oder im Bericht angezeigt.

[NSADM-69920]

- Wenn Sie einen laufenden Konfigurationsauftrag abbrechen, werden die erfolgreichen Befehle nicht zurückgesetzt, wenn die Option für erfolgreiche **Rollback-Befehle** auf der Seite “Bei **Befehlsfehler” auf** der Seite “Einstellungen **ausführen** “ ausgewählt ist.

[NSADM-34246]

- ADM kommuniziert nicht mit ADC BLX-Instanzen über SSH, und einige ADC-Funktionen wie Config Audit und Config Jobs funktionieren möglicherweise nicht mit BLX.

  [NSADM-68985]

Lizenzierung

Wenn Sie Citrix ADM-Lizenzen wählen, um eine Autoscale-Gruppe zu erstellen, werden die gepoolten Lizenzen nicht angezeigt.

[NSADM-62727]

Vorherige Veröffentlichungen

April 28, 2021

In diesem Thema finden Sie die Liste der vorherigen Versionen für Citrix Application Delivery Management (Citrix ADM).

03. Dezember 2019

Neue und erweiterte Features

Konfigurieren von Schwellenwerten in Service Graph

Als Administrator können Sie jetzt Schwellenwerte für Kubernetes-Dienste konfigurieren. Citrix ADM zeigt den Dienststatus (Kritisch, Prüfen und Gut) basierend auf der Reaktionszeit des Dienstes und der Fehleranzahl an. Standardmäßig können Sie den Standardschwellenwert (Service-Reaktionszeit = 200 ms und Fehleranzahl = 0) anzeigen, der auf alle Dienste angewendet wird.

Weitere Informationen finden Sie unter Konfigurieren von Schwellenwerten in Service Graph

[NSADM-41290]

TCP- und SSL-Metriken für Services

In Service Graph können Sie neben HTTP-Transaktionsdetails nun die Abhängigkeiten und Metriken von TCP- und SSL-Diensten anzeigen. Das Dienstdiagramm wird nun mit dem Protokoll angezeigt, das von den Diensten verwendet wird. Mit den TCP- und SSL-Metriken können Sie:

- TCP-Verbindungsdetails zwischen Diensten anzeigen
- Bestimmen Sie, ob TCP-bezogene Probleme vom Quell- oder Zieldienst stammen
- Anzeigen, ob der SSL-Fehler vom Quell- oder Zieldienst stammt
- Anzeigen der SSL-Protokollversion, die von SSL-Diensten verwendet wird

Weitere Informationen finden Sie unter Service-Diagramm.

[NSADM-41295],[NSADM-41296]

Keep-Alive-Intervall konfigurieren

Jetzt können Sie Keep-Alive intern konfigurieren, um die Verbindung zwischen ADM-Dienst und Agent aufrechtzuerhalten. Der interne muss 30 bis 120 Sekunden betragen. Um das Intervall zu konfigurieren, navigieren Sie von der ADM-Dienst-GUI zu **Einstellungen > Systemeinstellungen > Systemkonfigurationen > Agent und Zeitzone**.

[NSADM-43641]

Unterstützung kontextsensitiver Hilfe

Um die Benutzerfreundlichkeit zu verbessern, verfügt die Citrix ADM GUI nun über ein Hilfefenster. Wenn Sie sich beim ADM-Dienst anmelden, klicken Sie auf das Fragezeichen (?) in der oberen rechten Ecke des Dienstbildschirms, um das **Hilfefenster** zu öffnen.

Dieses Hilfefenster enthält Optionen zum Anzeigen der folgenden Informationen:

- Kontextbezogene Hilfe: Starten Sie Inhalte, die für den angezeigten UI-Bildschirm spezifisch sind. Derzeit wird der Hilfe-Link in einer neuen Browser-Registerkarte geöffnet und zeigt kontextsensitive Inhalte aus der Produktdokumentation an.
- Dokumentation: Starten Sie die Übersichtsseite der ADM-Service-Dokumentation und navigieren Sie zu den gewünschten Inhalten.
- Diskussionsforum: Starten Sie die Forenseite, um zu sehen, was unsere Expertengemeinschaft diskutiert.
- Kauf: Starten Sie die Website citrix.com, von der aus Sie ADM-Service erwerben können.
- Kundensupport: Starten Sie die Support-Website, um unser Support-Team zu kontaktieren.

[NSADM-39656]

Behobene Probleme

Netzwerke

Wenn Sie unter **ADM GUI > Netzwerke > Infrastructure Analytics**oben rechts auf die **Circle Pack-Ansichtoder Tabellenansicht** klicken, wird die Seite im Firefox-Browser nicht ordnungsgemäß gerendert.

[NSADM-40660]

Auf der Seite zum Hinzufügen einer Autoscale-Gruppe (**ADM GUI > Netzwerke > AutoScale-Gruppen > Hinzufügen**) wird die Option zur Auswahl der Lizenzedition (z. B. Citrix ADC VPX Advanced Edition-10Mbps) auf der Registerkarte **Cloud-Parameter** anstelle der Registerkarte **Lizenz** angezeigt.

[NSADM-43759]

E-Mail-, SMS- oder Slack-Benachrichtigung, die für den Ablauf des ADC SSL-Zertifikats konfiguriert ist, funktioniert nicht.

[NSADM-44008]

Analytics

Wenn der AppFlow Collector einen benutzerdefinierten Namen hat, wird die ADM Analytics-Funktion möglicherweise deaktiviert.

[NSADM-43723]

12. November 2019

Neue und erweiterte Features

Erhöhen Sie die Bandbreite mit Burst-Lizenzierung

Die Burst-Lizenzierung ist ein spezielles Programm, das zusätzliche Bandbreite oder Instanzlizenzen für die gepoolte Kapazität bereitstellt. Für die virtuelle CPU-Abonnements werden virtuelle CPU-Lizenzen hinzugefügt. Wenn Ihr Basisabonnementlimit erreicht ist, können Sie leicht verfügbare Lizenzen verwenden, ohne eine brandneue Lizenz erwerben zu müssen. Diese Burst-Lizenzen werden basierend auf Ihrer tatsächlichen Nutzung pro Monat berechnet. Das Burst-Lizenzprogramm ist nur für ausgewählte Kunden auf Bedarfsbasis verfügbar.

Sie können die monatliche und jährliche Zusammenfassung anzeigen, um die Bandbreitennutzung der gepoolten Kapazität zu verfolgen. Um die Lizenzverwendung anzuzeigen, navigieren Sie in der Citrix ADM GUI zur Seite " **Pooled Capacity > License Usage** ".

[NSADM-36649]

Anzeigen von Eingangs- und Client-Metriken im Service-Diagramm

Im Service-Diagramm wird die Netzwerkkarte jetzt mit Diensten angezeigt, die über ein Ingress verbunden sind. Sie können jetzt Folgendes anzeigen:

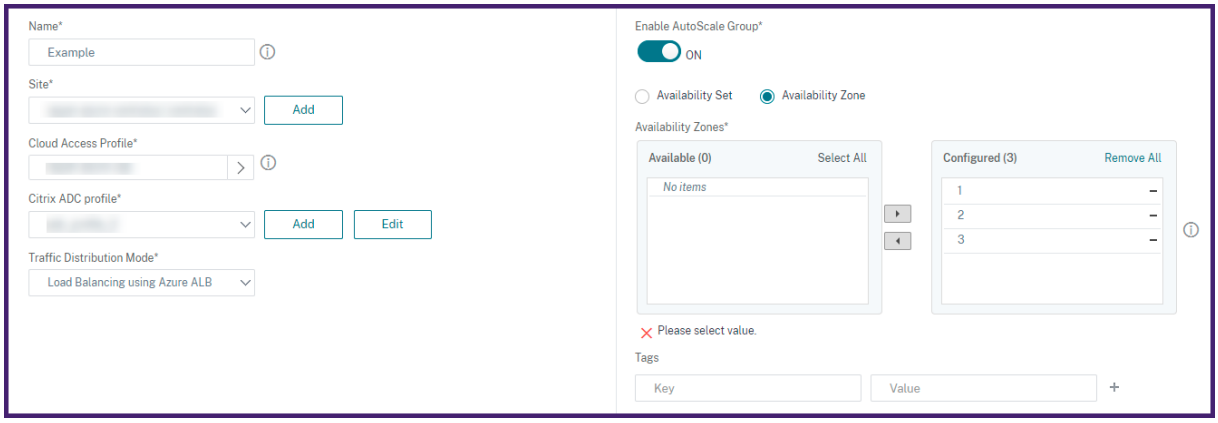
- Die durchschnittliche Zeit, die ADC-Instanzen (MPX, VPX und CPX) für die Verarbeitung der Anforderungen verwendet.
- Die Client-RTT für die Kommunikation zwischen Client und Ingress.

Weitere Informationen finden Sie unter Service Graph für Cloud-native (Kubernetes) Apps

[NSADM-41287]

Azure Availability Set-Unterstützung für Citrix ADM Autoscale-Gruppen

Wenn Sie eine Autoscale-Gruppe im Citrix ADM-Dienst erstellen, um Citrix ADC VPX-Instanzen Autoscale, die in Azure Cloud bereitgestellt werden, können Sie jetzt entweder **Availability Set** oder **Availability Zone**auswählen. Zuvor war **Availability Zone** die einzige Option.



Weitere Informationen finden Sie unter Konfiguration.

[NSADM-42598]

Behobene Probleme

Netzwerke

Wenn Sie einen virtuellen Server auswählen, klicken Sie auf die Registerkarte **Visualizer** unter **ADM GUI > Netzwerke > Netzwerkfunktionen > Content Switching**, wird die folgende Fehlermeldung angezeigt:
“Fehler: Citrix ADC Konfiguration konnte nicht abgerufen werden.”

[NSADM-42066]

Die GSLB-Netzwerkfunktion benötigt mehr Verarbeitungszeit für Citrix ADC Metriken. Dieses Problem fügt Latenz beim Erkennen einer GSLB-Site hinzu und stimmt nicht mit den ADC-Geräten in Citrix ADM Analytics überein. Dieses Problem kann auftreten, wenn Sie mehrere GSLB-Geräte für mehrere Mandanten konfigurieren.

[NSADM-40997]

Orchestrierung

Wenn Sie einen bereits vorhandenen Kubernetes-Cluster im Citrix ADM Dienst bearbeiten, wird die folgende Fehlermeldung angezeigt: “Fehler in Antwort” und Antwortstatus “500”.
Mit diesem Fix konfiguriert ADM den Kubernetes-Cluster auf dem Agent mit den bearbeiteten Werten neu. Und die Citrix ADM GUI zeigt eine Meldung mit dem Status der Cluster-Neukonfiguration an. Im Folgenden sind die möglichen Status der Clusterkonfiguration aufgeführt:

- Citrix ADM wird erfolgreich zum Kubernetes-Cluster hinzugefügt.
- Token verfügt nicht über die erforderlichen Berechtigungen zum Konfigurieren des bearbeiteten Clusters.
- Citrix ADM konnte keine Verbindung zum Kubernetes-Cluster herstellen.

[NSADM-41023]

Analytics

Wenn Sie Analytics aktivieren, wird Web Insight standardmäßig in ADM-GUI ausgewählt.

[NSADM-40606]

17. Oktober 2019

Neue und erweiterte Features

Verbesserte Infrastrukturanalyse mit neuen zusätzlichen Indikatoren

Neben den vorhandenen Indikatoren können Sie nun die folgenden zusätzlichen neuen Indikatoren in Infrastructure Analytics anzeigen, um die Citrix ADC-Instanzbewertungen zu bereichern:

- Fehlgebildete IP-Header
- Ungültige L4-Prüfsummen
- Erhöhte CPU-Auslastung durch IP-Verschiebung
- Übermäßige Paketsteuerung
- TCP-Paket fällt aufgrund von Reassembly-Limit Treffern
- Layer-2-Schleife
- Tagged VLAN mismatch

Weitere Informationen finden Sie unter Verbesserte Infrastrukturanalyse mit neuen Indikatoren.

[NSADM-39152]

Download-Option für Agent-Image

Sie können jetzt das neueste Agent-Image von der ADM-Benutzeroberfläche herunterladen, auch wenn keine Agenten im ADM-Dienst vorhanden sind. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

[NSADM-40097]

Verwalten von Kubernetes Ingress-Konfigurationen auf mehreren Clustern

Kubernetes verwendet die Ingress-Funktion, über die der Client-Datenverkehr auf die Microservices einer Anwendung zugreift. Die Citrix ADC-Instanzen können als Ingress für die Anwendungen fungieren, die in einem Kubernetes-Cluster ausgeführt werden. Die Citrix ADC-Instanzen werden zu Load Balancer und Proxy für den (Nord-Süd) Datenverkehr von den Clients zu den Microservices innerhalb des Kubernetes-Clusters. Und die Instanzen aktualisieren die Endpunkte für die Microservices, sobald sie sich in der Kubernetes-Umgebung ändern.

Sie können mehrere ADC-Instanzen so konfigurieren, dass sie als Ingress fungieren und jeden ADC basierend auf der Ingress-Richtlinie verschiedenen Anwendungen zuweisen. Geben Sie Folgendes an, um eine Ingress-Konfiguration bereitzustellen:

- **Cluster** — Ein Kubernetes-Cluster, in dem Sie eine Ingress-Konfiguration bereitstellen möchten. Informationen zum Hinzufügen eines Kubernetes-Clusters finden Sie unter **Orchestration > Kubernetes > Cluster**.
- **Richtlinien** — Die Richtlinien entscheiden, dass die ADC-Instanz, der Cluster und der Namespace eine Ingress-Konfiguration bereitstellen. Um eine Richtlinie zu definieren, navigieren Sie zu **Orchestrierung > Kubernetes > Richtlinien**.
- **Eingangskonfiguration** — Diese Konfiguration umfasst die Regeln für Content Switching und die entsprechenden URL-Pfade der Microservices und ihrer Ports. Sie können die SSL/TLS-Zertifikate auch mithilfe eines Kubernetes-Geheimnisses angeben, um HTTPS-Datenverkehr auf der ADC-Instanz zu entlasten.

Citrix ADM ordnet automatisch die Ingress-Konfigurationen und ADC-Instanzen zu. Citrix ADM wählt die ADC-Instanz aus und hostet je nach den angegebenen Ingress-Richtlinien eine Ingress-Konfiguration. Um den Ingress Bereitstellungsstatus anzuzeigen, navigieren Sie zu **Orchestration > Kubernetes > Ingress**.

Für jede erfolgreiche Ingress-Konfiguration generiert Citrix ADM ein StyleBooks ConfigPack. Das ConfigPack stellt die ADC-Konfiguration dar, die auf die ADC-Instanz angewendet wird, die der Ingress-Konfiguration entspricht. Um das Config Pack anzuzeigen, navigieren Sie zu **Anwendungen** > **StyleBooks** > **Configurations**.

Weitere Informationen finden Sie unter Verwalten der Kubernetes Ingress-Konfiguration in Citrix ADM.

[NSADM-40847]

Autorisieren von Netzwerkfunktions-Entitäten für einen Benutzer

Als Administrator können Sie bestimmte Netzwerkfunktions-Entitäten auswählen und einem Benutzer Zugriff gewähren. Mit dieser Option können Sie den Benutzerzugriff auf einer einzelnen Ebene von Netzwerkfunktionsobjekten verwalten. Mit dieser Funktion können Sie dem Benutzer oder der Gruppe dynamisch bestimmte Berechtigungen auf Entitätenebene zuweisen.

Um die Netzwerkfunktionsobjekte zu autorisieren, **wählen Sie beim Konfigurieren einer Gruppe die Option Individuelle Entitätstypen** auswählen. Sie können die folgenden Netzwerkfunktions-Entitätstypen in der Citrix ADM GUI autorisieren:

- Anwendungen (virtuelle Server)
- Service
- Servicegruppen
- Server

Sie können entweder einzelne Entitäten hinzufügen oder alle Entitäten unter dem erforderlichen Entitätstyp auswählen, um einem Benutzer den Zugriff zu gewähren. Weitere Informationen finden Sie unter Konfigurieren von Gruppen auf Citrix ADM.

Die Option **Auf gebundene Entitäten auch anwenden** autorisiert die Entitäten, die an den ausgewählten Entitätstyp gebunden sind. Wenn Sie z. B. eine Anwendung auswählen und auch **auf gebundene Entitäten anwenden auswählen, werden auch**die an eine Anwendung gebundenen Entitäten autorisiert.

Sie können die Netzwerkfunktionsobjekte mit regulären Ausdrücken auswählen. Die Entitäten werden in Abhängigkeit von den angegebenen regulären Ausdrücken ermittelt. Wenn Sie die Option Gebundene Entitäten zulassen für die erkannten Entitäten auswählen, kann der Benutzer automatisch auf die Entitäten zugreifen, die an die ausgewählte Entität gebunden sind.

> **Hinweis**
>
> Stellen Sie sicher, dass Sie nur einen Entitätstyp ausgewählt haben, wenn Sie gebundene Entitäten autorisieren möchten.

[NSHELP-6078]

Neues Konfigurations-Auditdiagramm

Das Diagramm **Status der Citrix ADC Konfigurationsdatei** wird auf der Seite **Konfigurationsüberwachung** hinzugefügt. Dieses Diagramm enthält den Status der Citrix ADC Dateien, die im`nsconfig` Ordner vorhanden sind. Citrix ADM zeichnet Änderungen in Dateien innerhalb des Ordners `nsconfig`auf und vergleicht diese und zeigt die Unterschiede an.

Mit diesem Diagramm können Sie überwachen, ob Dateien im `nsconfig`Ordner hinzugefügt, geändert oder entfernt werden.

Beispiel: Wenn die Lizenzdatei auf einer ADC-Instanz aktualisiert wird, können Sie überprüfen, wann diese Datei zuletzt aktualisiert wurde, und entsprechende Maßnahmen ergreifen.

Sie können eine Warnung festlegen, um Benachrichtigungen über das geänderte Dateistatusereignis zu erhalten. Unter **Konfigurationsdatei-Diff-Benachrichtigung**können Sie E-Mail- oder Pufferinfor-

mationen angeben. Weitere Informationen finden Sie unter Konfigurationsüberwachungsänderungen über Instanzen hinweg.

[NSADM-36469]

Behobene Probleme

Netzwerke

- Die von Citrix ADM `certkeys`heruntergeladenen Dateien sind beschädigt.

  [NSADM-41630]

- Wenn Sie eine neue Autoscale-Gruppe unter **Netzwerke** > **AutoScale Groups**erstellen, sind HTML-Tags auf der Registerkarte **Lizenz** sichtbar.

  [NSADM-42234]

Orchestrierung

Wenn ein Citrix ADM Agent geändert oder ungültig ist, kann der Cluster nicht gelöscht werden.

[NSADM-41021]

Oktober 03, 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf den neuesten Build von Citrix ADM aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Erstellen von Netzwerkberichten für Lastenausgleichsdienste

Sie können jetzt ein Netzwerkberichterstattungs-Dashboard für Lastenausgleichsdienste erstellen. In diesem Dashboard können die folgenden Berichte für die ausgewählten Services angezeigt werden:

- Verbindungen: für die Client- und Server-Verbindungszähler.
- Durchsatz: für Anforderungs- und Antwortbytes Zähler.
- Time to First Byte (TTFB): Für die durchschnittliche Zeit, die zum Senden eines Anforderungspakets an einen Dienst und zum Empfangen des ersten Pakets vom Dienst gebraucht wird. Diese Antwortzeit wird als TTFB bezeichnet.

Weitere Informationen zum Erstellen eines Netzwerkberichterstattungs-Dashboards finden Sie unterNetzwerkberichterstattung.

[NSADM-18228]

Behobenes Problem

Netzwerke

Wenn sich ein RBAC-Benutzer an der ADM-GUI anmeldet, wird eine Fehlermeldung angezeigt, wenn der Benutzer Zugriff auf ein untergeordnetes Menü hat, aber nicht auf sein übergeordnetes Menü hat.

[NSHELP-20409]

18. September 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf den neuesten Build von Citrix ADM aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Automatische Generierung von Vorfällen in ServiceNow mithilfe des Citrix ADM Dienstes

Sie können ServiceNow-Vorfälle für Citrix ADC Ereignisse, SSL-Zertifikatsereignisse und Citrix ADM -Lizenzereignisse automatisch generieren.

- **Citrix ADC Ereignisse**: Citrix ADM kann ServiceNow-Vorfälle für ausgewählte Citrix ADC Ereignisse aus ausgewählten verwalteten Citrix ADC-Instanzen generieren.

  Um ServiceNow-Benachrichtigungen für Citrix ADC Ereignisse von den verwalteten Instanzen zu senden, müssen Sie eine Ereignisregel konfigurieren und die Regelaktion als **ServiceNow-Benachrichtigungen senden** zuweisen.

  Erstellen Sie eine Ereignisregel für den ADM-Dienst, indem Sie zu **Netzwerke** > **Ereignisse** > **Regeln** navigieren. Weitere Informationen finden Sie unter ServiceNow-Benachrichtigungen senden.

- **Das SSL-Zertifikat und die ADM-Lizenzereignisse**: Citrix ADM kann die ServiceNow-Vorfälle für das Ablaufdatum des SSL-Zertifikats und das Ablaufdatum der ADM-Lizenz generieren.

  Informationen zum Senden von ServiceNow-Benachrichtigungen für den Ablauf des SSL-Zertifikats finden Sie unter Das Ablaufdatum des SSL-Zertifikats.

  Informationen zum Senden von ServiceNow-Benachrichtigungen zum Ablauf der ADM-Lizenz finden Sie unter Ablauf der Citrix ADM -Lizenz.

> **Wichtig**
>
> - Diese Funktion wird nur in ServiceNow Cloud unterstützt.
> - Stellen Sie sicher, dass der Citrix Cloud ITSM Adapter für ServiceNow konfiguriert und in den Citrix ADM Dienst integriert ist. Siehe Integrieren von Citrix ADM Service mit ServiceNow-Instanz.

[NSADM-23783]

Anzeigen von Analysen für Bot-Angriffe

Sie können nun Einblicke für die Bot-Erkennungstechniken anzeigen, die auf Ihren Citrix ADC-Instanzen konfiguriert sind. Navigieren Sie zu **Analytics** > **Bot Insight**, um Bot-Angriffe für Ihre Citrix ADC-Instanzen anzuzeigen. Aktivieren Sie **Bot Insight**, um Analysen für Bot-Angriffe anzuzeigen.

Weitere Informationen finden Sie unter Bot Einblick.

[NSADM-36648]

Verwalten des Citrix ADM Dienstes mit einem Express-Konto

Ab dieser Version wird Ihnen beim Erstellen eines Citrix ADM Dienstkontos automatisch ein Express-Lizenzkonto zugewiesen. Eine separate Testlizenz ist nicht mehr erforderlich. Wenn Sie sich bereits im Testzeitraum befinden, wird Ihr Konto nach Ablauf der Testphase in ein Express-Konto umgewandelt.

Wenn Ihr Citrix ADM -Lizenzabonnement und Ihre Kulanzfrist endet, wird Ihr Konto in ein Express-Konto umgewandelt.

Weitere Informationen finden Sie unter Citrix ADM Express-Konto.

[NSADM-31715]

Anpassen von Rollback-Befehlen zum Erstellen von Konfigurationsaufträgen

Wenn Sie einen Konfigurationsauftrag erstellen, können Sie jetzt die gewünschten Rollback-Befehle angeben, die bei einem Befehlsfehler ausgeführt werden sollen. Sie können die Option Rollback anpassen aktivieren, indem Sie zu **Netzwerke** > **Konfigurationsaufträge** navigieren.

[NSADM-31710]

Ein Info-Tipp für die erweiterte Suche

Es wird ein Info-Tipp hinzugefügt, der die Operatoren und logischen Operatoren beschreibt, die für die Suche nach Syslog- und Überwachungsprotokollmeldungen verwendet werden. Um den Info-Tipp anzuzeigen, klicken Sie auf die Suchleiste auf der ADM-Benutzeroberfläche, und klicken Sie dann auf **Hilfe benötigen**.

Weitere Informationen finden Sie unter Syslog-Nachrichten durchsuchen.

[NSADM-38406]

Behobene Probleme

Lizenzierung

- Wenn Sie die Zeitzone in Lizenzverwendung von lokal in GMT ändern, wird die benutzerdefinierte Zeit nicht in GMT geändert. Und der Lizenznutzungsbericht wird nicht generiert.

[NSADM-17670]

Netzwerke

- Wenn Sie unter **Netzwerke** > **Netzwerkfunktionen** auf **Jetzt abfragen** klicken, hängt die Citrix ADM GUI für einige Zeit und die Daten sind nicht wiederherstellbar.

[NSHELP-20143]

- Citrix ADM zeigt die Fehlermeldung “Mindestens ein Agent ist erforderlich, damit die Lizenzierung funktioniert” an, auch wenn alle Dateien gelöscht wurden und kein Agent hinzugefügt wurde.

[NSADM-38386]

Orchestrierung

- Wenn Sie in Citrix ADM mehrere Cluster hinzufügen, zeigt Citrix ADM in **Orchestrierung** > Cluster nur 1 **Clusterinformationen** an.

[NSHELP-41020]

03. September 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf den neuesten Build von Citrix ADM aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Service Graph für Cloud-native (Kubernetes) Apps

Mit der Service Graph-Funktion in Citrix ADM können Sie:

- Sicherstellen der End-to-End-Beobachtbarkeit der Gesamtleistung Ihrer Anwendung.
- Identifizieren Sie Engpässe, die durch die gegenseitige Abhängigkeit verschiedener Komponenten Ihrer Anwendungen entstehen.
- Sammeln Sie Einblicke in die Abhängigkeiten verschiedener Komponenten Ihrer Anwendungen.
- Überwachen Sie Dienste innerhalb des Kubernetes-Clusters.
- Überwachen Sie, welcher Dienst Probleme hat.
- Überprüfen Sie die Faktoren, die zu Leistungsproblemen beitragen.
- Detaillierte Sichtbarkeit von Service-HTTP-Transaktionen.
- Analysieren Sie die folgenden Metriken:
  - Gesamtzahl der Treffer
  - Service-Reaktionszeit
  - Datenvolumen
  - Fehler

Weitere Informationen finden Sie unter Service Graph für Cloud-native (Kubernetes) Apps.

[NSADM-23832]

Ändern der Instanzeinstellungen in Citrix ADM

Das Citrix ADM bietet Ihnen die Optionen zum Ändern der Instanzeinstellungen. Diese Einstellungen gelten für die von Citrix ADM erkannten Instanzen. Um die Instanzverwaltungseinstellungen zu ändern, navigieren Sie zu **Einstellungen** > **Systemeinstellungen** > **Instanzeinstellungen**.

[NSADM-37277]

Behobene Probleme

Netzwerke

- In **Netzwerke** >**Netzwerkfunktionen** > **Lastenausgleich** nimmt die Citrix ADM GUI längere Zeit in Anspruch, um virtuelle Server anzuzeigen.

  [NSHELP-20050]

- Während der Erstellung der Autoscale-Gruppe hat die Registerkarte Autoscale-Parameter die Mindestanzahl von Informationen zu Citrix ADC-Instanzen verpasst. Daher kann Citrix ADM keine ADC-Instanzen von Autoscale verwenden.

  [NSADM-40501]

- Wenn Sie im Citrix ADM versuchen, Zertifikate und Schlüsseldateien auf Citrix ADC-Instanzen hochzuladen und zu installieren, die über Agents entdeckt wurden, wird möglicherweise ein Fehler angezeigt.

  [NSADM-34558]

System

- Wenn der Citrix ADM Dienst eine Instanz mit dem Agenten entdeckt, verwendet die NITRO -Anforderung das HTTP-Protokoll anstelle des im Profil konfigurierten Protokolls. Diese NITRO Kommunikation erfolgt während des geplanten Inventars, der Statistik oder der Überwachung der Entitäten.

  [NSADM-39555]

- Die Citrix ADM GUI reagiert nicht mehr, wenn Sie die folgende Navigation verwenden, um Analysen zu aktivieren:

  1. Navigieren Sie zu **Konten** > **Abonnement**.
  2. Klicken Sie auf **Lastenausgleich**.
  3. Klicken Sie auf **Analytics aktivieren**.

  [NSADM-40760]

13. August 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf den neuesten Build von Citrix ADM aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Sehen Sie sich die Lizenzen von ADM für ADM Autoscale-Gruppen an

Jetzt können Sie die im Citrix ADM-Dienst vorhandenen ADC-Lizenzen verwenden, um die für ADM Autoscale-Gruppen bereitgestellten Citrix ADC-Instanzen zu lizenzieren.

Auf der Seite **AutoScale-Gruppen erstellen** ist eine neue Registerkarte **Lizenz** verfügbar. Auf dieser Registerkarte können Sie gepoolte Kapazität, VPX-Lizenzen und virtuelle CPU-Lizenzen konfigurieren, während Sie die Autoscale-Gruppe erstellen. Wenn also eine neue Instanz für die Autoscale-Gruppe bereitgestellt wird, wird der bereits konfigurierte Lizenztyp automatisch auf die bereitgestellte Instanz angewendet.

Wenn die bereitgestellten Instanzen zerstört oder die Bereitstellung aufgehoben werden, werden die angewendeten Lizenzen automatisch an Citrix ADM zurückgegeben.

Früher können Sie beim Erstellen der Autoscale-Gruppe nur Citrix ADC-Lizenzen konfigurieren, die auf dem jeweiligen Cloud-Marktplatz verfügbar sind. Wenn also eine neue Instanz für die Autoscale-Gruppe bereitgestellt wird, wird die Lizenz von ihrem Cloud-Marktplatz bezogen.

Weitere Informationen finden Sie unter den folgenden Links:

- AWS-Lizenzanforderungen
- Azure-Lizenzanforderungen

[NSADM-37694, NSADM-33422]

Vereinfachte Migration der Citrix ADC Anwendungskonfiguration mit StyleBooks

> **Hinweis**
>
> Diese Funktion ist in der Vorschau

Der StyleBooks Configuration Builder hilft Ihnen, ein Citrix ADC Anwendungskonfigurations-StyleBook aus einer vorhandenen ADC-Konfiguration zu erstellen. Diese Funktion automatisiert auch die Migration der Anwendungskonfiguration von einer Citrix ADC-Instanz zu einer anderen Instanz. Sie starten die Migration, indem Sie eine der folgenden Konfigurationsquellen angeben:

- Citrix ADC-Instanz — Mit dieser Option werden die aktiven Anwendungen auf der ausgewählten ADC-Instanz ermittelt.
- Eine Reihe von CLI-Befehlen — Diese Option analysiert die CLI-Befehle und extrahiert die Anwendungen in.

Nachdem die Quelle angegeben wurde, erkennt ADM alle Anwendungen, die in der Quelle gefunden wurden. Anschließend können Sie die Anwendungskonfiguration auswählen, die Sie auf die Ziel-ADC-Instanz migrieren möchten. Weitere Informationen finden Sie unter Migrieren der Citrix ADC Anwendungskonfiguration.

Nach der Migration wird in Citrix ADM ein ConfigPack zusammen mit dem entsprechenden StyleBook erstellt. Um das ConfigPack anzuzeigen, navigieren Sie zu **Anwendungen** > **StyleBooks** > **Konfigurationen**.

[NSADM-36438]

Vereinfachtes Upgrade von Citrix ADC-Instanzen in der Autoscale-Gruppe

Sie können jetzt nahtlos alle Instanzen in den Cloud-Services aktualisieren, die Teil der Autoscale-Gruppe sind. Weitere Informationen, siehe Planen der Aktualisierung der Autoskalierungsgruppe.

> **Hinweis**
>
> Während des Upgrades wird die automatische Skalierung von Citrix ADC-Instanzen für die ausgewählte Autoscale-Gruppe deaktiviert.

Wenn die Autoscale-Gruppe nach dem Upgrade eine neue Instanz zur Verfügung stellt, hat die neue Instanz dieselbe Version zum Zeitpunkt des Upgrades angegeben.

[NSADM-34401, NSADM-34285]

Suchen von Citrix ADM Überwachungsprotokollmeldungen mithilfe von Filtern

Jetzt können Sie Filter verwenden, um Citrix ADM Überwachungsprotokollmeldungen zu durchsuchen, Ihre Ergebnisse einzuschränken und genau das zu finden, wonach Sie suchen. Die neuen Filterkategorien sind Quelle, Ereignis, Schweregrad und Nachricht.

Um Überwachungsprotokollmeldungen für alle im ADM vorhandenen Anwendungen zu durchsuchen, navigieren Sie über die ADM-Benutzeroberfläche zu **Netzwerke** > **Netzwerkfunktionen** > **Auditing**.

Um Überwachungsprotokollmeldungen für eine bestimmte Anwendung auf dem ADM zu suchen, navigieren Sie über die ADM-Benutzeroberfläche zu **Anwendung** > **Dashboard** und wählen Sie den virtuellen Server aus, nach dem Sie die Überwachungsprotokollmeldungen durchsuchen möchten. Klicken Sie als Nächstes auf die Registerkarte **Überwachungsprotokoll**.

Weitere Informationen finden Sie unter Anzeigen und Exportieren von Syslog-Nachrichten

[NSADM-38705]

Behobene Probleme

Konto

- Die Option**Syslog-Server** ist jetzt in der Citrix ADM GUI nicht verfügbar.

  [NSADM-39256]

Analytics

- Wenn Sie Analysen aktivieren, ist die Geodatenerfassung ebenfalls standardmäßig aktiviert, aber Geomaps wurden in Citrix ADM nicht angezeigt.

  [NSADM-39543]

Netzwerke

- Einige der lizenzierten virtuellen Server werden nach dem Upgrade nicht lizenziert. Dieses Problem führte zu einem Verlust von Analysedaten.

[NSADM-39379]

- Die gesamten virtuellen Server wurden fälschlicherweise im Dashboard für Netzwerkfunktionen angezeigt.

  [NSADM-39512]

- Wenn Sie Berichte mit der Option **Export planen** konfigurieren, wird in den über E-Mail/Pufferzeit empfangenen Berichten ein leeres Fenster angezeigt.

  [NSADM-38974]

- Wenn die Anzahl der Threads im Ereignissubsystem 15 überschreitet, kann Citrix ADM Syslogs nicht verarbeiten. In dieser Version wird die Thread-Grenze auf 20 erhöht.

  [NSADM-39518]

31. Juli 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 41.12 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Web-Transaktionsanalyse

Web-Transaktionsanalyse ermöglicht es Ihnen, mehrere detaillierte Transaktionen zu durchsuchen, um fehlerhaften 5xx Antwortcode anzuzeigen. Auf der Seite **Transaktionsübersicht** können Sie die detaillierten Transaktionen auch für eine langsamere Antwortzeit anzeigen. Mit dieser Funktion können Sie nicht nur die detaillierten Transaktionen betrachten, sondern auch die Aufteilung der Antwortzeit auf Client, ADC und Server visuell verstehen.

Diese Funktion ist in das Anwendungs-Dashboard integriert und Sie können auf die Seite Transaktionsübersicht für Serverfehler - 5XX zugreifen. Weitere Informationen finden Sie unter Web-Transaktionsanalyse für Serverfehler.

[NSADM-34701]

Zwei neue Indikatoren für Marker

Kritische Ereignisse und **wichtige Ereignisse** sind die neuen Indikatoren, die einem Marker hinzugefügt werden. In **Netzwerke** > **Instanzen** kennzeichnen Marker auf einer Karte die in Citrix ADM erstellten Sites. Nun wird die Anzahl der kritischen und wichtigsten Ereignisse, die auf den Instanzen aufge-

treten sind, auf den Markern angezeigt. Diese Informationen helfen Ihnen, schnell die Ereignisse zu beurteilen, die Ihre Aufmerksamkeit erfordern.

Weitere Informationen finden Sie unter Überwachen global verteilter Standorte in Citrix ADM.

[NSADM-38638]

Intelligente App Analytics mit maschinellem Lernen und regelbasierten Algorithmen

Intelligent App Analytics ermöglicht es Ihnen, Probleme mit der Anwendungsleistung mithilfe von maschinellem Lernen und regelbasierten Algorithmen zu identifizieren. Mit diesen Algorithmen können Sie als Administrator die Ursachenanalyse der Anwendungsleistung schneller identifizieren. Zuvor, als Sie auf eine Anwendung doppelgeklickt haben, konnten Sie Analysen für Komponenten wie Reaktionszeit, Durchschnittliche CPU-Auslastung, Speicherauslastung usw. anzeigen. Sie können nun die folgenden neuen Indikatoren anzeigen:

- Serververzögerungsanomalien (verwendet maschinellen Lernalgorithmus)
- Sitzungsaufbauereignisse (verwendet regelbasierten Algorithmus)
- Service-Flaps Ereignisse (verwendet regelbasierten Algorithmus)

Weitere Informationen finden Sie unter Intelligente App Analytics

[NSADM-33674]

Verbesserte Infrastrukturanalyse mit neuen Indikatoren

Zuvor konnten Sie mit Infrastructure Analytics in Citrix ADM die Bewertungen von Citrix ADC-Instanzen überwachen, indem Sie mehrere Datenquellen korrelieren. Sie können jetzt neue Indikatoren in Infrastructure Analytics anzeigen, um die Citrix ADC-Instanzbewertung zu bereichern. Diese neuen Indikatoren helfen den Administratoren auch, die Ursache von Problemen schnell zu analysieren.

Navigieren Sie in Citrix ADM zu **Netzwerke** > **Infrastructure Analytics**, um Indikatoren für:

- Fehler bei der Port-Zuweisung
- Keine Standard-Routenkonfiguration
- IP-Konflikt
- VRID-Konflikt
- VLAN-Unstimmigkeit
- TCP-Angriff mit kleinem Fenster
- GSLB-Sitenname stimmt nicht überein

Weitere Informationen finden Sie unter Infrastrukturanalyse

[NSADM-30188]

Behobene Probleme

System

Wenn die Anzahl der Threads im Ereignissubsystem 15 überschreitet, kann Citrix ADM Syslogs nicht verarbeiten. In dieser Version wird die Thread-Grenze auf 20 erhöht.

[NSADM-39518]

16. Juli 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 40.24 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Option zum Aktivieren oder Deaktivieren von Planungsaufträgen

Jetzt können Sie Planungsaufträge wie Instanzsicherung, Instanzkonfiguration Audit, Instanznetz-Berichterstellung und Instanz-SSL-Zertifikate aktivieren oder deaktivieren. Zuvor wurden diese Aufträge standardmäßig aktiviert, ohne dass sie deaktiviert werden konnten.

Um einen Planungsauftrag zu aktivieren oder zu deaktivieren, navigieren Sie über die Citrix ADM GUI zu **Einstellungen, Systemeinstellungen und Konfigurierbare Funktionen**.

[NSADM-36650]

Analytics in Partitionen über Logstream als Transportmodus aktivieren

Wenn Sie Admin-Partitionen auf Ihren verwalteten Instanzen erstellen, sollten Sie Analyseberichte auf Citrix ADM für jede Admin-Partition separat anzeigen. Citrix ADM hat zuvor konsolidierte Analyseberichte basierend auf der IP-Adresse der Instanzen angezeigt und **IPFIX** als Transportmodus verwendet. Sie können nun **Logstream** als Transportmodus auswählen, um Analyseberichte für Administratorpartitionen zu erhalten.

> **Hinweis**
>
> Für Citrix ADC Version **vor 13.0 36.27**ist **IPFIX**die Standardoption für den **Transportmodus**. Für Citrix ADC **ab 13.0 36.27**können Sie entweder **Logstream**oder **IPFIX**als Transportmodus auswählen

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**, und wählen Sie dann den Instanz-Typ aus. Zum Beispiel VPX.

2. Klicken Sie auf **Partitionen**.
3. Wählen Sie auf der Seite **Adminpartitionen** die Partition aus, und wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
4. Wählen Sie den virtuellen Server aus, und klicken Sie dann auf **Analytics aktivieren**.
5. Im Fenster **Analytics aktivieren**:
   a) Wählen Sie den Einsichtstyp aus (Web Insight)

   > **Hinweis**
   >
   > Bei Partitionen wird nur Web Insight unterstützt.

   b) **Logstream** als Transportmodus auswählen
   c) Der Ausdruck ist standardmäßig true
   d) Klicken Sie auf **OK**.

[NSADM-30252]

Anwenden virtueller Serverlizenzen und Aktivieren von Analysen in einem einzigen Workflow

Der Prozess der Lizenzierung virtueller Server und anschließende Aktivierung von Analysen auf den lizenzierten virtuellen Servern wurde vereinfacht. Um Analysen für einen virtuellen Server zu aktivieren, müssen Sie zuvor zu **Netzwerken** > **Instanzen** > **Citrix ADC** navigieren und dann den virtuellen Server auswählen, um die Analyse zu aktivieren. Wenn virtuelle Server nicht für eine Instanz lizenziert sind:

- Sie müssen zuerst den virtuellen Server lizenzieren, indem Sie zu **Konto** > **Abonnement** navigieren
- Navigieren Sie dann erneut zu **Netzwerken** > **Instanzen** > **Citrix ADC**, um die Analyse für den virtuellen Server zu aktivieren.

Citrix ADM eliminiert diesen doppelten Prozess jetzt und ermöglicht es Ihnen, virtuelle Server zu lizenzieren und Analysen in einem einzigen Workflow anzuwenden.

Weitere Informationen finden Sie unter Analytics aktivieren

[NSADM-32893]

Unterstützung für gepoolte Kapazitätslizenzierung über mehrere Rechenzentren hinweg

Sie können den Lizenzpool jetzt über mehrere Rechenzentren hinweg freigeben. Die gepoolten Lizenzen, die Citrix ADM hinzugefügt werden, können verwendet werden, um den verwalteten Citrix ADC-Instanzen Lizenzen zuzuweisen.

So importieren Sie Lizenzen automatisch aus Ihrem Citrix Cloud-Konto:

1. Navigieren Sie zu **Netzwerke** > **Lizenzen**.
2. Klicken Sie auf der Registerkarte **Lizenzdatei** auf **Lizenzdatei hinzufügen**.
3. Wählen Sie die Option Lizenzzugriffscode verwenden aus.
4. Klicken Sie auf **Lizenzen abrufen**.
5. Wählen Sie das Produkt aus der Liste aus.
6. Klicken Sie auf **Download**.

Weitere Informationen finden Sie unter Konfiguration der gepoolten Kapazität.

[NSADM-36695]

Berechtigungen zum Aktivieren und Deaktivieren von Benutzern erteilen

Sie können die benutzerdefinierten Zugriffsrichtlinien auf einen Benutzer, eine Gruppe oder eine Rolle anwenden. Mit diesen Richtlinien können Sie Benutzerberechtigungen für die Citrix ADM Funktionen definieren.

In dieser Version wird die Option **Enable-Deaktivieren** nur den **Netzwerkfunktions-Features** hinzugefügt, die Aktivieren oder Deaktivieren Aktion zulassen. Mit dieser Berechtigung können Sie auch die Aktion **Jetzt abfragen** ausführen.

Wenn Sie einem Benutzer die Berechtigung **Enable-Disable** erteilen, wird auch die Berechtigung **Anzeigen** erteilt. Sie können diese Option nicht aufheben. Informationen zum Erteilen der Berechtigung **Enable-Disable** für ein Feature finden Sie unter Konfigurieren von Zugriffsrichtlinien auf Citrix ADM

> **Hinweis**
>
> Wenn Sie vor dem Upgrade die Berechtigung **Bearbeiten** für ein Feature erteilt haben, werden die Berechtigungen **Aktivieren** und **Anzeigen** ebenfalls erteilt. Sie können die Auswahl der automatisch ausgewählten Optionen nicht aufheben.

[NSADM-37684, NSHELP-18635]

Unterstützung für das Hinzufügen von Citrix ADC BLX-Instanzen in Citrix ADM

Citrix ADC BLX Appliance ist ein leichtgewichtiges Softwarepaket, das auf Ihrer bevorzugten Serverhardware ausgeführt wird. Jetzt können Sie Citrix ADC BLX-Instanzen mithilfe von Citrix ADM verwalten. Weitere Informationen finden Sie unter Instanzen hinzufügenund Konfiguration der gepoolten Kapazität

[NSADM-29983]

Vereinfachte anwendungsbasierte Autorisierung für RBAC-Benutzer

In Citrix ADM können Sie nun als Administrator andere Administratoren für die erforderlichen Anwendungen autorisieren, ohne dass Sie Instanzen auswählen müssen. Zuvor müssen Sie die Instanzen auswählen und dann die Anwendungen aus diesen Instanzen auswählen. Und es kann Fälle geben, in denen ein Administrator nicht wissen muss, welche Citrix ADC-Instanz die Anwendung gehostet wird. Mit dieser Funktion können Sie die Anwendungen direkt auswählen.

So fügen Sie einer Gruppe Anwendungen hinzu:

1. Navigieren Sie zu **Konten** > **Benutzerverwaltung** > **Gruppen**.
2. Klicken Sie auf **Hinzufügen**.

   Die Seite “Systemgruppe erstellen “ wird angezeigt.
3. Geben Sie die erforderlichen Details auf der Seite **Gruppeneinstellungen** an, und klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Autorisierungseinstellungen** eine der folgenden Optionen aus der Liste **Anwendungen auswählen**:
   - **Alle Anwendungen**: Diese Option ist standardmäßig aktiviert. Es fügt alle Anwendungen hinzu, die im Citrix ADM vorhanden sind.
   - **Alle Anwendungen ausgewählter Instanzen**: Diese Option wird nur angezeigt, wenn Sie Instanzen aus der Kategorie **Alle Instanzen** auswählen. Es fügt alle Anwendungen, die auf der Instanz vorhanden sind.
   - **Bestimmte Anwendungen**: Mit dieser Option können Sie die erforderlichen Anwendungen hinzufügen, auf die Benutzer zugreifen sollen. Klicken Sie auf **Anwendungen hinzufügen**, und wählen Sie die erforderlichen Anwendungen aus der Liste aus.
5. Klicken Sie auf **Gruppe erstellen**.

   Weitere Informationen finden Sie unter Konfigurieren von Gruppen auf Citrix ADM.

[NSADM-37213]

Greifen Sie auf die Benutzeroberfläche der Citrix ADC-Instanz zu, indem Sie auf den Hostnamen klicken

Zuvor konnten Sie nur über die IP-Adresse auf die GUI zugreifen. Jetzt können Sie über das Citrix ADM auf eine Citrix ADC-Instanz-GUI zugreifen, indem Sie auf den Hostnamen oder die IP-Adresse der Instanz klicken.

Weitere Informationen finden Sie unter Instanzen hinzufügen.

[NSADM-37503]

Suchen von Syslog- und Überwachungsprotokollmeldungen mithilfe von Filtern

Jetzt können Sie Filter verwenden, um Syslog-Nachrichten und Überwachungsprotokollmeldungen zu suchen, um Ihre Ergebnisse einzuschränken und genau das zu finden, wonach Sie suchen. Die neuen Filterkategorien sind Instanz-, Modul-, Ereignis-, Schweregrad und Nachricht, die für Syslog- und Überwachungsprotokollmeldungen gleich sind.

Um Syslog-Nachrichten zu durchsuchen, navigieren Sie über die ADM-Benutzeroberfläche zu **Netzwerke** > **Ereignisse** > **Syslog-Nachrichten**.

Um Überwachungsprotokollmeldungen zu durchsuchen, navigieren Sie über die ADM-Benutzeroberfläche zu **Konto**> **Überwachungsprotokollmeldungen**.

Informationen zum Suchen finden Sie unter Anzeigen und Exportieren von Syslog-Nachrichten.

[NSADM-25835]

Automatische Discovery von Entitäten

Wenn Sie einer Citrix ADC-Instanz eine Entität hinzufügen, die auf Citrix ADM konfiguriert ist, wird die Entität innerhalb von 10 Minuten automatisch auf dem ADM angezeigt. Und jede Änderung in der Entität wird sofort auf dem ADM reflektiert.

Damit diese Funktion funktioniert, muss SNMP für die ADC-Instanz über das ADM aktiviert sein. Um SNMP zu aktivieren, navigieren Sie über die ADM-Benutzeroberfläche zu **Netzwerke** > **Instanzen** > **Citrix ADC**. Wählen Sie die Instanz aus, klicken Sie auf das Menü **Aktion auswählen** und klicken Sie auf **SNMP konfigurieren**.

Wenn Sie virtuelle Server in der Citrix ADC-Instanz global konfigurieren, werden einige der virtuellen Server automatisch innerhalb von 10 Minuten angezeigt. Die anderen virtuellen Server dauern möglicherweise länger, bis sie angezeigt werden (bis zu 20 Minuten).

[NSADM-23622]

Eine neue Registerkarte für die Provisioning Citrix ADC-Instanzen in der Cloud

Jetzt können Sie schnell eine Citrix ADC VPX-Instanz in Microsoft Azure Cloud und AWS Cloud **bereitstellen, indem Sie auf Bereitstellen** auf Citrix ADM GUI klicken. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**, um die Option Provisioning anzuzeigen. Zuvor war die Provisioningoption in der Liste **Aktion auswählen** verschachtelt. Um das Provisioning aufzuheben, wählen Sie die Instanz aus, und klicken Sie auf **Provisioning aufheben**.

Weitere Informationen:

Provisioning von Citrix ADC VPX Instanzen in AWS

Provisioning von Citrix ADC VPX Instanzen unter Microsoft Azure

[NSADM-38057]

Agenten- und Site-Spalten

Sie können nun Standort- und Agent-Informationen anzeigen, wenn Sie eine Instanz unter **Netzwerke > Instanzen > Citrix ADC** anzeigen.

[NSADM-38057]

Behobene Probleme

Netzwerke

- Der Latenzwert in Citrix ADM wird als 0 ms angezeigt und wurde auf < 1 ms geändert.

[NSADM-38207]

- Citrix ADM hat CPX-Instanzen als MPX-Instanzen erkannt. Dieses Problem wurde behoben.

[NSADM-37725]

- `masd` Neustart-Befehl auf Agenten fehlgeschlagen. Dieses Problem wurde behoben.

[NSADM-37447]

Einstellungen

- Im Dashboard Access Control werden die Daten für den Zeitraum nach Ablauf des Citrix ADM Dienstabonnements nicht angezeigt. Dieses Problem tritt auf, wenn Sie auch Abonnement für den Zugriffssteuerungsdienst haben.

[NSADM-37827]

02. Juli 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 39.14 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Übertragen einer Backupdatei auf ein externes System

Als Vorsichtsmaßnahme können Sie eine Kopie Ihrer Backupdatei auf ein anderes System übertragen. Wenn Sie die Konfiguration wiederherstellen möchten, müssen Sie zuerst die Backupdatei auf den Citrix ADM -Server hochladen und dann den Wiederherstellungsvorgang ausführen.

So übertragen Sie eine Citrix ADM -Sicherungsdatei:

1. Navigieren Sie zu **Netzwerke > Instanzen > Citrix ADC**, und wählen Sie dann den Instanztyp aus. Zum Beispiel VPX.
2. Wählen Sie die Instanz aus, und wählen Sie in der Liste **Aktion auswählen** die Option **Sicherung/Wiederherstellung** aus.
3. Wählen Sie die Backupdatei aus, und klicken Sie dann auf **Übertragen**.

   Die Seite **Backupdatei übertragen** wird angezeigt. Geben Sie die folgenden Parameter an:

   a) **Server** - IP-Adresse des Systems, an das Sie die Backupdatei übertragen möchten.

   b) **Benutzername** und **Kennwort** — Benutzeranmeldeinformationen des neuen Systems, in das die gesicherten Dateien kopiert werden.

   c) **Port** — Portnummer des Systems, in das die Dateien übertragen werden.

   d) **Übertragungsprotokoll** — Protokoll, das verwendet wird, um die Backupdateiübertragung durchzuführen. Sie können SCP-, SFTP- oder FTP-Protokolle auswählen, um die Backupdatei zu übertragen.

   e) **Verzeichnispfad** — Der Speicherort, an den die gesicherte Datei auf dem neuen System übertragen wird.
4. Klicken Sie auf **OK**.

[NSADM-31702]

Namensänderungen für Lizenztypen

Die folgenden Lizenztypen werden umbenannt:

Vorhandene Lizenznamen	Neue Lizenznamen
Standard	Standard (keine Änderung)
Enterprise	Erweitert
Platinum	Premium

[NSADM-36694]

Aktualisieren eines installierten SSL-Zertifikats und Erstellen eines CSR

Jetzt können Sie ein installiertes SSL-Zertifikat aktualisieren und eine Certificate Signing Request (CSR) erstellen.

- **Aktualisieren eines installierten Zertifikats**

Nachdem Sie ein erneuertes Zertifikat von der Zertifizierungsstelle (Certificate Authority, CA) erhalten haben, können Sie vorhandene Zertifikate von Citrix ADM aktualisieren, ohne sich bei jeder Citrix ADC-Instanz anzumelden.
So aktualisieren Sie ein SSL-Zertifikat, einen Schlüssel oder beides von Citrix ADM:

1. Navigieren Sie zu **Netzwerke > SSL-Dashboard**.
2. Klicken Sie auf eine der Diagramme, um die Liste der SSL-Zertifikate anzuzeigen.
3. Wählen Sie auf der Seite SSL-Zertifikate ein Zertifikat aus, und klicken Sie auf **Aktualisieren**. Alternativ können Sie auf das **SSL-Zertifikat** klicken, um die Details anzuzeigen, und klicken Sie dann oben rechts auf der Seite SSL-Zertifikat auf **Aktualisieren**.
4. Ändern Sie auf der Seite **SSL-Zertifikat aktualisieren** das Zertifikat, den Schlüssel oder beides entsprechend Ihren Anforderungen, und klicken Sie auf **OK**.

- **Erstellen einer CSR**

Eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) ist ein Block mit verschlüsseltem Text, der auf dem Server generiert wird, auf dem das Zertifikat verwendet wird. Sie enthält Informationen, die im Zertifikat enthalten sind, z. B. den Namen Ihrer Organisation, den allgemeinen Namen (Domänenname), den Ort und das Land.

So erstellen Sie eine CSR mit Citrix ADM:

1. Navigieren Sie zu **Netzwerke > SSL-Dashboard**.
2. Klicken Sie auf eines der Diagramme, um die Liste der installierten SSL-Zertifikate anzuzeigen, und wählen Sie dann das Zertifikat aus, für das Sie eine CSR erstellen möchten, und wählen Sie in der Liste **Aktion auswählen die OptionCSR erstellen** aus.
3. Geben Sie auf der Seite **Certificate Signing Request (CSR)** einen Namen für die CSR an.
4. Führen Sie einen der folgenden Schritte aus:
    a) **Schlüssel hochladen** - Um Ihre Schlüsseldatei hochzuladen, wählen Sie entweder Lokal (Ihr lokaler Computer) oder Appliance (die Schlüsseldatei muss auf der virtuellen Citrix ADM Instanz vorhanden sein).
    b) **Erstellen Sie einen Schlüssel** - Geben Sie die folgenden Parameter an:

Verschlüsselungsalgorithmus	Typ des Schlüssels (z. B. RSA)
Schlüsseldateiname	Name der Datei, in der der RSA-Schlüssel gespeichert ist.
Schlüsselgröße	Schlüsselgröße in Bits.

Verschlüsselungsalgorithmus	Typ des Schlüssels (z. B. RSA)
Öffentlicher Exponentenwert	Wählen Sie entweder 3 oder F4 aus der bereitgestellten Liste. Dieser Wert ist Teil des Verschlüsselungsalgorithmus, der zum Erstellen Ihres RSA-Schlüssels erforderlich ist.
Schlüsselformat	Be default PEM ist ausgewählt. PEM ist das empfohlene Schlüsselformat für Ihr SSL-Zertifikat.
PEM-Kodierungsalgorithmus	Wählen Sie in der Liste den Algorithmus (DES oder DES3) aus, den Sie zum Verschlüsseln des generierten RSA-Schlüssels verwenden möchten. Wenn Sie diesen Algorithmus auswählen, müssen Sie eine PEM-Passphrase angeben.
PEM-Passphrase	Wenn Sie den PEM-Kodierungsalgorithmus gewählt haben, geben Sie eine Passphrase ein.
PEM-Passphrase bestätigen	Bestätigen Sie Ihre PEM-Passphrase.

5. Klicken Sie auf **Weiter**.
6. Geben Sie auf der folgenden Seite weitere Details an. Wenn Sie die CSR erstellen möchten, ohne die Standardeinstellungen zu ändern, klicken Sie auf **Weiter**.

> **Hinweis**
>
> Die meisten Felder haben Standardwerte, die aus dem Betreff des ausgewählten Zertifikats extrahiert wurden. Der Betreff enthält Details wie den allgemeinen Namen, den Namen der Organisation, den Bundesstaat und das Land.
>
> Die meisten Zertifizierungsstellen akzeptieren Zertifikatsübermittlungen per E-Mail. Sie erhalten ein gültiges Zertifikat von der Zertifizierungsstelle an die E-Mail-Adresse, die Sie den CSR übermittelt haben.

[NSADM-37278]

Neue Erkenntnisse in Citrix ADM Analytics

Sie können nun die folgenden Erkenntnisse unter Analytics in Citrix ADM anzeigen:

- Video Insight
- TCP Insight

- WAN-Einblick
- SSL-Forward-Proxyanalyse

[NSADM-36692]

Bereitstellen von Citrix ADC-Instanzen im Hochverfügbarkeitsmodus in AWS und Azure

Jetzt stellen Sie Citrix ADC-Instanzen im Hochverfügbarkeitsmodus auf AWS- und Microsoft Azure-Clouds mithilfe von Citrix ADM bereit.
Führen Sie zum Bereitstellen die folgenden Schritte aus:

1. Navigieren Sie zu **Netzwerke > Instanzen > Citrix ADC**.
2. Klicken Sie in **VPX**auf **Aktion auswählen** und wählen Sie **Bereitstellung in Public Cloud** aus.
3. Wählen Sie auf der Seite **Citrix ADC VPX bereitstellen** den Clouddienst aus, in dem Sie die Citrix ADC VPX Instanzen bereitstellen möchten.
4. Wählen Sie unter **Basisparameter** in der Liste **Instanztyp** die Option **HA** aus.
5. Wählen Sie den **Zonentyp** aus den folgenden Optionen:
   - **Einzelne Zone**: Mit dieser Option werden die Citrix ADC VPX Instanzen in derselben Zone bereitgestellt.
   - **Multi-Zonen**: Mit dieser Option werden die Citrix ADC VPX Instanzen über mehrere Zonen verteilt. Stellen Sie sicher, dass Sie die Netzwerkdetails in **Cloud-Parametern** für jede Zone angeben, die in Ihrer Cloud erstellt werden.

   Weitere Informationen finden Sie unter Bereitstellen von Citrix ADC VPX auf AWS und Bereitstellen von Citrix ADC VPX auf Microsoft Azure.

[NSADM-31108, NSADM-30099]

Neue optionale Felder zum Anzeigen von Citrix ADC-Instanzen von Citrix ADM

Die folgenden neuen optionalen Felder werden hinzugefügt, um Citrix ADC-Instanzen von Citrix ADM anzuzeigen. Um diese Felder auszuwählen, gehen Sie zu **Citrix ADM GUI > Netzwerke > Instanzen > Citrix ADC** und klicken Sie auf das Symbol Einstellungen.

- Status von HA-Master
- HA-Synchronisierungsstatus
- Administratorprofil
- Integrität
- Betriebszeit

- Modell-ID
- Paket-Engines
- SSL-Karten
- CPU
- Hardware-Version
- LOM-Version
- Host-ID
- Seriennummer
- Codierte Seriennummer
- UUID

Hier ist ein Beispiel, in dem das Einstellungssymbol und die neuen Felder hervorgehoben werden.

[NSHELP-6170]

Behobene Probleme

Netzwerke

- Wenn Sie versuchen, eine Citrix ADC SDX-Instanz über Citrix ADM zu aktualisieren, schlägt das Upgrade fehl, und die folgende Fehlermeldung wird angezeigt:

  ```
  ”SCP: Unable to open a session on <IP address of the SDX instance>.
  Agent id not found”
  ```

  [NSHELP-19767]

- Wenn Sie mehrere Autoscale-Gruppen in derselben Region erstellen, schlägt die Anwendungsbereitstellung für solche Autoscale-Gruppen möglicherweise fehl. Dieses Problem tritt auf, wenn Sie ALB als Verkehrsverteilungsmodus für diese Autoscale-Gruppen auswählen.

  [NSLB-4934]

System

- Wenn ein Citrix ADM -Superadministrator andere Benutzer aus Citrix Cloud einlädt, ist die Standardberechtigung für eingeladene Benutzer admin mit Ausnahme der Benutzerverwaltung. (Um die Benutzerverwaltung anzuzeigen, navigieren Sie zu **Citrix ADM GUI > Systeme > Benutzerverwaltung**.) Zuvor war die Standardberechtigung schreibgeschützt. Weitere Informationen finden Sie unter Konfigurieren der rollenbasierten Zugriffssteuerung.

  [NSADM-37914]

19. Juni 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 38.20 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Registerkarte GSLB-Dienstgruppen

Die Citrix ADM GUI zeigt nun die Registerkarte **Dienstgruppen** unter **Netzwerke** > **Netzwerkfunktionen** > **GSLB** an.Auf dieser
Registerkarte können Sie alle Servicegruppen für die erkannten Instanzen im ADM anzeigen. Mithilfe der Registerkarte **Dienstgruppen** können Sie Aufgaben wie das Aktivieren und Deaktivieren einer Dienstgruppenentität sowie das Überprüfen der an diese Entität gebundenen Mitglieder und virtuellen Server ausführen. Außerdem können Sie die Entität abfragen, um ihren aktuellen Status zu erhalten.

31. Mai 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 37.26 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Infrastrukturanalytik — Übersichtsfenster

Sie können jetzt die Citrix ADC-Instanzstatistiken für die **SSL-Konfiguration** und **Konfigurationsabweichung** im Bedienfeld **Zusammenfassung anzeigen**.

- **SSL-Konfiguration** — Zeigen Sie die Instanzen an, auf denen SSL-Zertifikate installiert sind:
  - **Aussteller: Nicht empfohlen** - Citrix empfiehlt den Aussteller des SSL-Zertifikats nicht.
  - **Algorithmus: Nicht empfohlen** - Die Signaturalgorithmen von auf der ADC-Instanz installierten SSL-Zertifikaten entsprechen nicht den Citrix Standards.
  - **Schlüsselstärke: Nicht empfohlen** - Die Schlüsselstärke der SSL-Zertifikate entspricht nicht den Citrix Standards.
- **Konfigurationsabweichung** — Zeigt die Liste der Instanzen an, die die Konfigurationsabweichungen für:

- **Saved vs Running** - Der Unterschied zwischen der gespeicherten Konfiguration auf der Instanz und der aktuell laufenden Konfiguration auf derselben Instanz.
- **Running vs Template** - Die Vorlage vs Running enthält alle Vorlagen außer **Saved vs Running**.

[NSADM-24161]

Signaturregelbenachrichtigung in Citrix ADM

Signaturbasierte Bedrohung zeigt die Erkennung bekannter Bedrohungen basierend auf der zugewiesenen Signatur an. Jedes Mal, wenn Sie der Citrix ADC Web AppFirewall ein Signaturobjekt hinzufügen, sendet Citrix ADM Benachrichtigungen über E-Mail, Slack, PagerDuty, Ereignisnachricht und Sicherheitsinformationen. Weitere Informationen finden Sie unter Signaturen.

Wenn Sie eine Ereignisregel in Citrix ADM erstellen, können Sie nun eine neue Kategorie namens **appFwNewSignatureAdded** anzeigen. Um Benachrichtigungen für neue Signaturobjekte zu Citrix ADC Web AppFirewall zu aktivieren, erstellen Sie eine Ereignisregel:

1. Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Regeln**, und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie`signature` im **Kategoriefenster** die Suchleiste ein, und wählen Sie dann **appFwNewSignatureAdded** aus.
3. Informationen zum Erstellen einer Ereignisregel finden Sie unterEreignisregeln erstellen.

Nach dem Erstellen der Ereignisregel erhalten Sie Benachrichtigungen basierend auf der konfigurierten Ereignisregelaktion. So zeigen Sie Benachrichtigungen an:

- Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Ereignismeldung**.
- Navigieren Sie zu **Analytics** > **Security Insight**, und wählen Sie dann die Instanz aus, für die Sie Signaturbenachrichtigungen anzeigen möchten.

  Die Signaturbenachrichtigungen werden auf der Registerkarte **Ereignisverlauf** aufgeführt.

[NSADM-34153]

Unterstützung für das Hinzufügen von Etiketten zu StyleBooks

Sie können nun jedem StyleBook in Citrix ADM Beschriftungen hinzufügen. Labels sind Schlüssel-Wert-Paare, mit denen Sie StyleBooks nach unterschiedlichen Kriterien gruppieren können. Sie können diese Labels beim Suchen oder Filtern von StyleBooks in Citrix ADM verwenden. Weitere Informationen finden Sie unter Erstellen eines Labels für das StyleBook

[NSADM-34877]

Citrix ADM Autoscaling in Microsoft Azure unterstützt Azure-Load Balancer für die Verteilung des Datenverkehrs

Die automatische Skalierung von Citrix ADC-Instanzen in Microsoft Azure unterstützt zwei Modi Verkehrsverteilung:

- über Azure-Verkehrs-Manager
- über Azure-Load Balancer

Weitere Informationen finden Sie unter Autoskalierungsarchitektur von Citrix ADC VPX in Microsoft Azure mit Citrix ADM

[NSADM-33423]

Behobene Probleme

Netzwerke

- Wenn Sie versuchen, einen abgebrochenen Konfigurationsauftrag auszuführen, wird möglicherweise ein Fehler “Ungültige Anfrage” angezeigt.

  [NSADM-34242]

- Wenn Sie auf der Seite **Agents hinzufügen** die Option **Site anhängen** auswählen, aktualisiert Citrix ADM die Site für die Instanz, die zu dieser Site oder dem Agenten gehört.

  [NSADM-35049]

- Beim Erstellen oder Konfigurieren einer Instanzgruppe zeigt die Citrix ADM GUI möglicherweise doppelt so viele IP-Adressen von Citrix ADC-Instanzen mit hoher Verfügbarkeit an. Wenn Sie eine IP-Adresse auswählen, werden beide Instanzen zur Instanzgruppe hinzugefügt.

  Dieses Update gilt für das Erstellen einer Instanzgruppe nach dem Upgrade. Für die zuvor erstellten Gruppen müssen Sie die doppelten Einträge aus der Gruppe entfernen

  [NSHELP-19176]

Einstellungen

Wenn der Citrix ADM-Agent nicht den richtigen Zeitwert vom Anwendungsserver erhält, werden die Erkenntnisse nicht in Citrix ADM angezeigt.

[NSHELP-18898]

April 25, 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 36.21 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents**

anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Möglichkeit, die Standard-Zielseite festzulegen

Im Citrix Application Delivery Management (ADM) Portal können Sie Ihre bevorzugte Seite als Standardlandesseite festlegen. Klicken Sie auf das Lesezeichensymbol auf der Registerkarte, die Sie als Standardlandesseite festlegen möchten.

Im Folgenden finden Sie ein Beispiel, um SSL Dashboard als Standardlandesseite festzulegen:

[NSADM-21938]

Erstellen einer technischen Supportdatei für den Citrix ADM Agent

Sie können eine technische Supportdatei für einen ausgewählten Citrix ADM Agent über die GUI generieren. Sie können diese Datei auch herunterladen und zur Untersuchung und Fehlerbehebung an den technischen Support von Citrix senden.

[NSADM-30238]

Verbesserungen am Dashboard für Infrastrukturanalysen

Infrastrukturanalyse-Dashboard wurde aktualisiert, um thematische Änderungen zu integrieren, und auch Tabellenspalten werden zur besseren Lesbarkeit angepasst. Sie können nun auf den Hostnamen klicken, um zur Instanz im instanzierten Dashboard zu navigieren. Es gibt auch einige kleinere Updates in der Benutzeroberfläche, die die Benutzererfahrung bei der Verwendung des Dashboards für Infrastrukturanalysen verbessern.

[NSADM-30191]

Behobene Probleme

Analytics

- In **HDX Insight** > **Benutzer** wird in der in der Tabelle Aktuelle Sitzungen ausgewählten Sitzung eine andere Client-IP-Adresse angezeigt als die IP-Adresse, die in der Tabelle Aktuelle Sitzungen angezeigt wird.

  [NSHELP-6395, TSK0715071]

Anwendungen

- Citrix ADM GUI reagiert nicht mehr, während AppFlow für mehrere virtuelle Server in bestimmten Fällen aktiviert wird. Dieses Problem tritt in der Regel auf, wenn Sie mehrere Typen von Lastausgleichsservern auswählen, die TCP enthalten, und wenn TCP am Anfang der Liste ist.

  Problemumgehung: Führen Sie eine Sortierung in der Spalte Diensttyp in aufsteigender Reihenfolge durch. Daher bewegen sich die TCP-Typen an den unteren Rand der Liste und aktivieren Sie dann AppFlow.

  [NSADM-35039]

- Derzeit enthalten die von Citrix ADM gesendeten E-Mails nicht die verstoßenen Schwellenwerte.

  [NSHELP-6093]

Netzwerke

- Wenn Sie mithilfe der Suchkriterien Typ nach Konfigurationsvorlagen suchen, zeigt Citrix ADM True oder False an. Beachten Sie, dass True = Standardkonfigurationsvorlagen und False = Benutzerdefinierte Konfigurationsvorlagen. Sie müssen entsprechend wählen.

  [NSADM-34802]

- Wenn Sie eine Ereignisregel mit Aktion unterdrücken erstellen, werden die Ereignisse für Instanzen, die über Agenten erkannt werden, auch nach Ablauf der geplanten Zeit unterdrückt.

  [NSADM-35023]

- Das Slack profil ist im Config-Job-Modul nicht sichtbar, während der Bericht an den Pufferkanal gesendet wird.

  [NSADM-35079]

- Wenn Sie einen Citrix ADC VPX mit Partitionen aus Citrix SDX entfernen, wird der ADC VPX aus Citrix ADM entfernt, die Partitionen werden jedoch weiterhin beibehalten.

  [NSADM-34829]

April 04, 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 35.17 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

UI-Erweiterung beim Abbrechen eines Konfigurationsauftrags

Die Abbruchoption wurde nun für die Aktion Ignorieren und Fortsetzen entfernt. Sie können die Konfigurationsaufträge nicht abbrechen, die ausgeführt werden, wenn Sie die Option **Fehler ignorieren und fortsetzen** für Befehlsausführungsmodus auswählen.

[NSADM-32836]

Möglichkeit, den Sortiertyp in den Spalten in Citrix ADM -Tabellen anzuzeigen

In der Citrix ADM Standardansicht können Sie die Spalten zwar in der erforderlichen Reihenfolge sortieren, aber die Spaltenüberschriften verfügen nun über einen Indikator, der anzeigt, ob die Datensätze in aufsteigender oder absteigender Reihenfolge angeordnet sind. Diese Änderung wird für die entsprechenden Citrix ADM Seiten angewendet.

[NSADM-21463]

Designänderung in Citrix ADM GUI

Citrix ADM GUI wurde nun auf einigen Seiten mit Designänderungen aktualisiert. Möglicherweise stellen Sie fest, dass die Bestätigungs- und Fehlerfenster jetzt mit einem neuen Farbdesign und einer Reihe neuer Schriftarten angezeigt werden.

[NSADM-22535]

Behobene Probleme

Analytics

- Wenn Sie zu **Benutzer** > **Transaktionen** navigieren, wird der Transaktionsbericht für mehr als 0,1 Millionen Transaktionen möglicherweise nicht angezeigt.

  [NSHELP-18785]

- Wenn Citrix ADM zwei Citrix ADC Gateways mit demselben Namen verwaltet, unterscheidet Citrix ADM die Sitzungen, die zu diesen Citrix ADC Gateways gehören.

  [NSHELP-18716]

- Das Anwendungs-Dashboard zeigt keine korrekten Metriken im App-Zusammenfassungsfenster für Anwendungen an, die auf dem Citrix ADC Hochverfügbarkeitspaar konfiguriert sind.

  [NSHELP-18733]

- Auf Application Dashboard werden einige Zeichen wie Data Volume nicht ordnungsgemäß angezeigt, wenn die Zeichenfolgenlänge lang ist.

  [NSADM-31818]

- Das Anwendungs-Dashboard zeigt keine korrekten Daten an, da die CPU- und Speicherinformationen aus dem Knoten nicht an alle virtuellen Server angehängt werden.

  [NSHELP-18736]

- AppFlow wird auf dem virtuellen Cache-Umleitungsserver nicht unterstützt. Daher wird die Option AppFlow aktivieren für den virtuellen CR Server in Citrix ADM entfernt.

  [NSHELP-18817]

Lizenzierung

- Citrix ADM liest die Lizenzportkonfiguration nicht, wenn sie als Lizenzserver konfiguriert ist.

  [NSADM-33966]

System

- In der Standardansicht fehlte die Spalte beim Sortieren der Spalten in der erforderlichen Reihenfolge an dem Indikator, um anzuzeigen, ob die Sortierung in aufsteigender oder absteigender Reihenfolge erfolgt. Nun werden Indikatoren zur Verfügung gestellt, um zu zeigen, ob die Datensätze in aufsteigender oder absteigender Reihenfolge angeordnet sind. Diese Änderung wird für die entsprechenden Citrix ADM Seiten angewendet.

  [NSHELP-18647]

Januar 01, 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 34.25 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Unterstützung zum Generieren von Netzwerkberichten für Citrix SDX-Instanzen in ADM

Mit Citrix ADM können Sie Berichte nicht nur für Instanzen auf globaler Ebene erstellen, sondern auch für Entitäten wie virtuelle Server und Netzwerkschnittstellen. Die Instanzfamilie umfasst jetzt Citrix ADC, Citrix SDX und Citrix SD-WAN Instanzen.

[NSADM-25092]

Unterstützung zum Erstellen von Config Packs mit StyleBooks ohne Auswahl von Instanzen

Citrix ADM ermöglicht es Ihnen, Config Packs mit den StyleBooks zu erstellen, ohne die Instanzen auszuwählen. Sie können das Config Pack später aktualisieren, indem Sie Zielinstanzen auswählen, auf denen Sie die Konfiguration bereitstellen möchten. Mit dieser Funktion können Sie Konfigurationspakete für Ihre Anwendungen erstellen, auch wenn Sie nicht auf die Instanzen zugreifen können.

[NSADM-25552]

Citrix ADM Autoscaling in Microsoft Azure unterstützt nur DNS-Datenverkehr mit Azure Traffic Manager

> **Hinweis**
>
> Diese Funktion befindet sich derzeit in der Vorschau.

Citrix ADM Autoscaling fügt Citrix ADC Clusterknoten in Azure hinzu oder entfernt sie je nach tatsächlicher Nutzung der Netzwerkressourcen. Der Citrix ADM sammelt Statistiken (CPU-Auslastung, Speichernutzung und Durchsatz) aus den von Autoscale bereitgestellten Clustern. Diese Statistiken werden anhand des vom Kunden konfigurierten Schwellenwerts ausgewertet. Das Scale-In oder Scale-Out wird ausgelöst, je nachdem, ob die Statistik den maximalen Schwellenwert überschreitet oder unter dem Mindestschwellenwert arbeitet.

Die Vorteile der automatischen Skalierung sind:

- Stellt sicher, dass die Anwendung ständig einsatzbereit ist und ausgeführt wird, unabhängig von den Anforderungen des Datenverkehrs.
- Citrix ADC-Instanzen werden dynamisch hinzugefügt und entfernt, indem sie zu einer manuellen Zero-Touch-Konfiguration führen.
- Die DNS-Verwaltung erfolgt automatisch.
- Ermöglicht ein besseres Kostenmanagement.

Die automatische Skalierung in Microsoft Azure unterstützt nur DNS-Datenverkehr mit Azure Traffic Manager.

> **Hinweis**
>
> Derzeit wird die Verteilung des Datenverkehrs mit ALB nicht unterstützt.

Um die Autoscale-Funktion verwenden zu können, müssen Sie Autoscale-Gruppen erstellen und die Anwendung mit StyleBooks bereitstellen. Diese Version unterstützt die automatische Skalierung von Anwendungen in Microsoft Azure Virtual Machine Scale Set. Weitere Informationen finden Sie unter Konfigurieren einer Anwendung für die Autoscale-Gruppe.

[NSADM-31259]

Verbesserte Citrix ADM Benutzeroberfläche

Diese Version verbessert die Benutzeroberfläche im Citrix ADM Portal. Im Folgenden sind die Highlights solcher Änderungen an der Benutzeroberfläche aufgeführt:

LOM-Versionen sind nur für Citrix ADC SDX-Appliances anwendbar. Daher werden auf der Seite Instanzen Dashboard die LOM-Versionen nur für die Citrix ADC SDX-Appliances angezeigt.

Die Schaltfläche **Filter unterdrücken** wird auf der Seite Syslog-Nachrichten bereitgestellt. Früher war diese Option unter Syslog-Nachrichten in der linken Navigation vorhanden.

[NSADM- 32322]

GUI-Erweiterung zur Anzeige von Daten basierend auf der Zeitdauer

Sie können nun die Zeitintervallliste verwenden und die Zeitdauer auswählen, um die Details für Anwendungsanalysen und Ereignisberichte anzuzeigen.

[NSADM-22529]

PagerDuty-Unterstützung in Citrix ADM

Früher können Sie in der Citrix ADM GUI Benachrichtigungen per E-Mail, SMS und Slack senden. Sie können jetzt Benachrichtigungen an PagerDuty basierend auf Ihren Konfigurationen senden, die Sie in PagerDuty vorgenommen haben. PagerDuty ermöglicht es Ihnen, Benachrichtigungen wie E-Mail, SMS, Push-Benachrichtigung und Telefonanruf auf registrierte Nummer zu konfigurieren.

Sie können Ihr PagerDuty-Profil als eine der Optionen auswählen, um Benachrichtigungen für die folgenden Funktionen zu erhalten:

- Ereignisse — Liste der Ereignisse, die für Citrix ADC-Instanzen generiert werden.
- Lizenzen — Liste der Lizenzen, die derzeit aktiv sind, etwa ablaufen usw.
- SSL-Zertifikate — Liste der derzeit aktiven, ablaufenden SSL-Zertifikate usw.

Stellen Sie vor dem Hinzufügen eines PagerDuty-Profils in Citrix ADM sicher, dass Sie die erforderlichen Konfigurationen in PagerDuty abgeschlossen haben. Weitere Informationen finden Sie unter PagerDuty-Dokumentation.

[NSADM-25940]

Behobene Probleme

Analytics

- Wenn Sie AppFlow für virtuelle Cache-Umleitungsserver aktivieren, wird möglicherweise eine Fehlermeldung angezeigt, und Sie können AppFlow möglicherweise nicht für diesen virtuellen Server aktivieren.

[NSHELP-18817]

Anwendungen

- Auf den Applikations-Dashboard-Info-Panels und den detaillierten Dashboard-Seiten wurden die Daten unter dem Titel Transaktionen unterschiedlich angezeigt. Es waren kumulative Daten zu einem Ort und Transaktionsrate an der anderen Stelle. Mit diesem Fix werden die Daten nun korrekt als Gesamttransaktionen angezeigt und der Abschnitt Schlüsselmetrik-Trends zeigt die Transaktionen pro Sekunde an.

  [NSHELP-18799]

Netzwerke

- Möglicherweise werden Fehler bei der CPX-Registrierung in Citrix ADM angezeigt, da der ADM-Dienstagent keine automatische CPX-Registrierungsanforderung zulässt.

  [NSADM-33020]

- Wenn Sie ein vorhandenes SSL-Zertifikat aktualisieren müssen, navigieren Sie zu **Netzwerke** > **SSL-Dashboard**. Das SSL-Dashboard zeigt die Details zu Citrix ADC -SSL-Zertifikaten, virtuellen SSL-Servern und SSL-Protokollen an. Klicken Sie auf einen der Links Gesamt Zertifikate, um Details zu SSL-Zertifikaten, virtuellen SSL-Servern oder SSL-Protokollen anzuzeigen. Wenn Sie nun ein Zertifikat auswählen und auf **Aktualisieren**klicken, müssen Sie das Format des zu aktualisierenden Zertifikats nicht angeben. Citrix ADM kann das Format nun aus den zuvor hochgeladenen Zertifikatsdateien ableiten.

  [NSHELP-18763]

System

- Wenn Sie zu **System** > **Ereignisse** navigieren, ein Ereignis auswählen und auf **Historie** klicken, wird im **Ereignisverlauf** das Hauptfenster Ereignisse angezeigt und nicht der erwartete Verlauf für dieses Ereignis. Sie müssen die Seite Ereignisverlauf schließen und die Auswahl wiederholen, um den korrekten Verlauf für dieses Ereignis anzuzeigen. Dieses Problem wurde behoben.

  [NSHELP-18651]

- Sie konnten in Citrix ADM -Tabellen nicht mit Sonderzeichen suchen. ADM ermöglicht jetzt die Suche mit Sonderzeichen wie $, & oder ‘.

  [NSHELP-5927]

28. Februar 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 33.23 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Unterstützung für die automatische Skalierung von Citrix ADC-Instanzen, die in Microsoft Azure bereitgestellt werden

> **Hinweis**
>
> Diese Funktion befindet sich in der Vorschau.

Die automatische Scaling-Funktion von Citrix ADM unterstützt jetzt die Skalierung von Citrix ADC-Instanzen in Microsoft Azure. Mit der automatischen Skalierungsfunktion von Citrix ADM werden Citrix ADC Clusterknoten hinzugefügt oder entfernt, die in Azure bereitgestellt werden, abhängig von der tatsächlichen Nutzung der Netzwerkressourcen. Der Citrix ADM sammelt Statistiken (CPU-Auslastung, Speichernutzung und Durchsatz) aus den von Autoscale bereitgestellten Clustern. Diese Statistiken werden anhand des vom Kunden konfigurierten Schwellenwerts ausgewertet. Je nachdem, ob die Statistiken den maximalen Schwellenwert überschreiten oder unter dem Mindestschwellenwert arbeiten, wird Scale-In bzw. Scale-Out ausgelöst.

Die Vorteile der automatischen Skalierung sind:

- Stellt sicher, dass die Anwendung ständig einsatzbereit ist und ausgeführt wird, unabhängig von den Anforderungen des Datenverkehrs.
- Citrix ADC-Instanzen werden dynamisch hinzugefügt und entfernt, indem sie zu einer manuellen Zero-Touch-Konfiguration führen.
- Die DNS-Verwaltung erfolgt automatisch.
- Ermöglicht ein besseres Kostenmanagement.

Die automatische Skalierung in Microsoft unterstützt zwei Modi Verkehrsverteilung:

- über Azure-Verkehrs-Manager
- über Azure-Load Balancer

Um die Autoscale-Funktion verwenden zu können, müssen Sie Autoscale-Gruppen erstellen und die Anwendung mit StyleBooks bereitstellen.

> **Hinweis:**
>
> Backend Autoscale wird in dieser Citrix ADM-Version nicht unterstützt.

[NSADM-24780]

Unterstützung zur Anzeige der Aktivierung von Analytics auf der Seite Lizenzierung virtueller Server

Citrix ADM zeigt nun die Liste der virtuellen Server an, für die Analysen aktiviert sind. Navigieren Sie zu **Netzwerke** > **Lizenzen**, und klicken Sie im Abschnitt Lizenzierte virtuelle Server auf die Schaltfläche, um die virtuellen Server für die Lizenzierung auszuwählen. Wählen Sie einen der virtuellen Servertypen aus, und wählen Sie die Registerkarte **Lizenziert**. In der Spalte **AppFlow Protokollierung** wird angezeigt, welche Analyse auf den virtuellen Servern aktiviert ist.

[NSADM-25857]

Konsolidierte Anzeige aller virtuellen Server auf der Seite Lizenzierung virtueller Server

Citrix ADM zeigt nun eine konsolidierte Ansicht aller virtuellen Server im Netzwerk an. Sie können nun zu **Netzwerke** > **Lizenzen** navigieren und im Abschnitt Lizenzierte virtuelle Server auf die Schaltfläche klicken, um die virtuellen Server für die Lizenzierung auszuwählen. Auf der Seite **Virtuelle Server lizenzieren** wird eine Registerkarte **Alle virtuellen Server** angezeigt, auf der alle virtuellen Server aufgelistet werden, unabhängig davon, ob sie Lastenausgleichs-, Content Switching- oder ein anderer Typ von virtuellen Servern sind. Sie können die erforderlichen virtuellen Server auswählen und Lizenzen darauf anwenden.

[NSADM-25194]

Unterstützung zum Anzeigen von Details einer Instanz auf der Seite Infrastrukturanalyse

Mit der Funktion Infrastructure Analytics in Citrix ADM können Sie die Faktoren visualisieren, die zu einem Problem in den Instanzen geführt haben oder zu einem Problem führen können. Sie können nun in der Tabellenansicht auf die Instanz-IP-Adresse klicken, um weitere Details zu dieser Instanz als Dashboard-Anzeige anzuzeigen. Das Instanz-Dashboard bietet eine Übersicht über die Instanz, in der Sie die CPU, den Arbeitsspeicher und die Datenträgernutzung der Instanz anzeigen können. Sie können auch Details zu SSL-Zertifikatsverwaltung, Config-Audit, Netzwerkfunktionen und einem Netzwerkbericht anzeigen, der detaillierte Netzwerkauslastung der Instanz anzeigt.

[NSADM-30194]

Behobene Probleme

Analytics

- Wenn Sie während der Konfiguration von Analysen auf einer ADC-Instanz nach Details des virtuellen Servers suchen und dann die Suche abbrechen, listet ADM möglicherweise auch virtuelle Server aus anderen ADC-Instanzen auf.

  [NSHELP-18623]

- Wenn Sie ein Benutzer mit schreibgeschützten Berechtigungen sind, können Sie die Diagnosesymbole auf keiner der Analyseseiten sehen.

  [NSHELP-6407]

- Wenn Sie AppFlow für die SD-WAN-WO-Instanz in Citrix ADM konfigurieren, wird die IP-Adresse des Dienstagenten nicht als Collector-IP-Adresse konfiguriert. Mit diesem Update wird der Agent konfiguriert, um die AppFlow Daten von den SD-WAN-WO-Instanzen zu empfangen.

  [NSADM-32565]

Hybrid und Multi-Cloud

- **AWS Autoscale**: Sie können Citrix ADC Release 12.1 Build 51.16 Image zum Erstellen von Autoscale-Gruppen verwenden.

Netzwerke

- Unter **Netzwerke** > **Konfigurationsüberwachung** kann es zu einer Situation kommen, wenn Sie im Abschnitt Top 10 Instanzen nach Konfigurationsänderung auf Instanzen klicken, ADM möglicherweise keine Daten für diese Instanz anzeigen. Wenn Sie einen bestimmten Zeitraum auswählen, z. B. täglich und dann im Abschnitt Top 10 Instanzen by Configuration Change eine Instanz auswählen, zeigt ADM möglicherweise Daten für einen anderen Zeitraum an.

  [NSHELP-18452]

- Betrachten Sie ein Szenario, wenn Sie zu **Netzwerke** > **Konfigurationsüberwachung** navigieren. Im Abschnitt Top 10 Instanzen nach Konfigurationsänderung zeigt der Tooltip möglicherweise nicht die vollständigen ADC-Informationen an, wenn Sie den Mauszeiger über den ADC bewegen. Dies liegt an der Begrenzung der Anzahl der Zeichen, die im Tooltip angezeigt werden kann.

  [NSHELP-18470]

- Citrix ADM kann SNMPv3-Pakete, die von der ADC-Instanz empfangen werden, nicht zeitweise verarbeiten. Dieser Fehler kann auftreten, nachdem die Citrix ADC-Instanz oder Citrix ADM selbst aktualisiert oder die ADC-Instanz neu gestartet wurde. Solche Fehler können auftreten, weil ungültiger Speicher (freier Speicher) für eine andere Speicherzuweisung verwendet wird.

  [NSHELP-5880]

System

- Dieses Problem wird nach dem Upgrade auf Citrix ADM Version 12.1 Build 50.28 festgestellt. Denken Sie daran, dass Sie zu **System** > **Benutzerverwaltung** > **Gruppe** navigieren und eine

Benutzergruppe erstellen. Dort deaktivieren Sie zunächst alle Optionen auf der Registerkarte **Autorisierung** und wählen manuell einige Instanzen aus und schließen die Erstellung der Gruppe ab. Wenn Sie später dieselbe Gruppe bearbeiten und die Registerkarte **Autorisierung** auswählen, werden die Instanzen nicht mehr angezeigt.

[NSHELP-18442]

- Möglicherweise stellen Sie fest, dass Sie in den folgenden zwei Szenarien keine virtuellen GSLB-Server in Benutzergruppen hinzufügen können:

  1. Beim Erstellen einer Gruppe: Wenn Sie versuchen, ein paar weitere GSLB virtuelle Server zu einer vorhandenen Liste von GSLB virtuellen Servern hinzuzufügen.
  2. Beim Bearbeiten einer vorhandenen Gruppe: Wenn Sie versuchen, GSLB-Server zu einer vorhandenen Gruppe hinzuzufügen, die bereits eine Liste der virtuellen GSLB-Server hat.

[NSHELP-18152]

08. Februar 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 32.32 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Diese Version ist eine Erweiterung der früheren Version von Citrix ADM 13.0 Build 32.30. In dieser Version wurden verschiedene Verbesserungen, einschließlich Plattform und Analysen, vorgenommen, um die Performance von Citrix ADM weiter zu verbessern.

28. Januar 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 32.30 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Unterstützung zum Anzeigen aller aktiven Knoten im Autoscale-Dashboard

Citrix ADM unterstützt jetzt die Anzeige aller aktiven Knoten für einen Cluster, der in AWS erstellt wurde. Sie können jederzeit die Anzahl der aktiven Knoten anzeigen, die Teil der Availability Zone sind. Weitere Informationen finden Sie unter Dashboard automatisch skalieren.

[NSADM-25785]

Unterstützung für den Export von Network Reporting-Dashboard

Sie können einen Export der Dashboardseite “ Network Reporting “ auf wiederkehrender Basis planen. Sie können beispielsweise eine Option festlegen, um wöchentlich einen Dashboard-Bericht für die vorherige Stunde zu generieren. Der Bericht wurde jede Woche für den vom Benutzer festgelegten Zeit- und Datumsstempel erstellt und nicht auf dem aktuellen Dashboard basiert. Mit der neuen Erweiterung überschreibt der Report den eingestellten Zeit- und Datumsstempel und zeigt den Status des Dashboards an. Weitere Informationen finden Sie unter Exportieren von Netzwerkberichten.

[NSADM-20017]s

Unterstützung für die Anzeige von Insight-Berichten nur für autorisierte Anwendungen

Citrix ADM Analytics unterstützt jetzt virtuelle IP-Adressen basierte Autorisierung. Wenn Sie die Benutzer für bestimmte Anwendungen oder virtuelle Server autorisieren, können Benutzer nun die Analyseberichte nur für die Anwendungen (virtuelle Server) anzeigen, für die sie autorisiert sind.

[NSADM-17971]

Unterstützung beim Planen des Exports von Berichten in Citrix ADM

Citrix ADM unterstützt die Planung des Exports von Berichten auf verschiedenen Seiten. Sie können verschiedene Aktionen ausführen, während Sie den Export von Berichten planen.

- Planen Sie die Generierung und den Export des Berichts in regelmäßigen Abständen.
- Geben Sie die Einstellungen für die Berichtsgenerierung an, und erstellen Sie ein E-Mail-Profil, in das der Bericht exportiert wird.
- Exportieren Sie die Berichte in einen bestimmten Slack Kanal.

Diese Erweiterung ähnelt der Funktion in Citrix ADM Software.

[NSADM-24829]

16. Januar 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 30.15 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

In dieser Version wurden Plattformverbesserungen vorgenommen, um die Leistung zu verbessern.

04. Januar 2019

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 30.14 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

07. Dezember 2018

Diese Version enthält Verbesserungen und Fehlerbehebungen.

Die Citrix Application Delivery Manager (ADM) -Agents werden standardmäßig automatisch auf Citrix ADM 13.0 Build 30.14 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Infrastrukturanalyse

> **Hinweis**
>
> Diese Funktion ist derzeit in der Vorschau verfügbar.

Die Citrix ADM-Infrastruktur-Analysefunktion vereint alle Daten, die aus den Citrix ADC-Instanzen gesammelt wurden, in einer visuellen Darstellung auf einer einzigen Seite in Citrix ADM. Mit der Funktion Infrastructure Analytics können Sie die Faktoren visualisieren, die zu einem Problem in den Instanzen geführt haben oder zu einem Problem führen könnten. Diese Visualisierung hilft Ihnen auch, die Aktionen zu
bestimmen, die ausgeführt werden müssen, um das Problem und seine Wiederholung zu verhindern.

Gehen Sie folgendermaßen vor, um Infrastructure Analytics in einer Circle-Pack-Ansicht anzuzeigen:

1. Navigieren Sie zu **Netzwerke > Infrastructure Analytics**.
2. Wählen Sie das Symbol für die Ansicht Circle-Pack aus.

Weitere Informationen finden Sie unter Infrastrukturanalyse.

[NSADM-23680]

Integrieren von Citrix ADM mit Citrix Virtual Citrix Director

Citrix ADM ist jetzt in Citrix Director integriert. Auf diese Weise kann Director HDX Insight Berichte von Citrix ADM im Netzwerk und auf der Seite Benutzerdetails anzeigen und den Benutzer, Anwendungen,

Desktops, Instanzen und lizenzspezifische Informationen bereitstellen.
Weitere Informationen finden Sie unter Integrieren von Citrix ADM mit Citrix Virtual Citrix Director.

[NSADM-17085]

Unterstützung zum Herunterladen von SSL-Zertifikaten

Sie können nun die SSL-Zertifikate von Citrix ADM herunterladen, indem Sie zu **Netzwerke** > **SSL-Dashboard** navigieren. Wählen Sie ein SSL-Zertifikat aus, und klicken Sie in der Liste Aktion auf **Herunterladen**. Weitere Informationen finden Sie unter SSL-Zertifikate herunterladen.

[NSADM-19790]

Unterstützung für die Sicherung und Wiederherstellung von Citrix ADC SDX-Instanzen

Es ist nun möglich, eine Citrix ADC SDX-Instanz von Citrix ADM zu sichern und wiederherzustellen. Weitere Informationen finden Sie unter Sichern und Wiederherstellen von Citrix ADC-Instanzen.

[NSADM-19882]

Behobene Probleme

Anwendungen

- In der Applikations-Dashboard-Aggregationslogik wird der neueste Datenvolume-Wert beibehalten, da es sich um den Gesamtindikator handelt. Aber manchmal werden Werte höher gesehen, was deutlich höher ist als der neueste Wert.

  [718359]

19. November 2018

Diese Version enthält Verbesserungen und Fehlerbehebungen.

Citrix Application Delivery Manager (Citrix ADM) Agents werden standardmäßig automatisch auf Citrix ADM 12.1 Build 505.130 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Konfigurieren von AppFlow auf mehreren virtuellen Servern und Anzeigen von Fortschrittsinformationen

Wenn Sie AppFlow auf mehreren virtuellen Servern gleichzeitig konfigurieren, zeigt ein Popup-Fenster den schrittweisen Fortschritt der AppFlow-Konfiguration an. Die Informationen zeigen die Anzahl der virtuellen Server, die auf Instanzebene konfiguriert werden. Die Fortschrittsinformationen sind nützlich, wenn Sie AppFlow auf vielen virtuellen Servern konfigurieren.

> **Hinweis**
>
> Citrix ADM unterstützt IPFIX als Standardtransportmodus bei der Konfiguration von AppFlow auf virtuellen Servern. Ab dem Citrix ADC 12.0-Release unterstützt Citrix ADM **Logstream**, und Sie müssen bei Bedarf explizit **Logstream**auswählen.

Achten Sie beim Aktivieren von AppFlow auf Citrix Gateway Instanzen darauf, dass Sie entweder ICA oder TCP als Transportmodus auswählen. Wenn Sie beide auswählen, hat ICA Vorrang vor TCP. Die Auswahl von HTTP zusammen mit ICA oder TCP ist zulässig. Weitere Informationen zum Aktivieren von AppFlow mit ADM finden Sie unterAktivieren von AppFlow mit Citrix ADM

Behobene Probleme

Analytics

- Wenn der Name des virtuellen Servers 60 Zeichen überschreitet, bewirkt dies, dass der AppFlow Aktionsname 128 Zeichen überschreitet. Das Aktivieren der Konfiguration solcher Aktionsnamen kann dazu führen, dass die ADC-Instanz nicht mehr funktioniert.

  [717663]

- Es ist eine längere Zeit erforderlich, um klare AppFlow Konfigurationen für mehrere virtuelle Server auf einer ADC-Instanz zu aktivieren.

  [717675]

Netzwerke

- Sie können zwar eine beliebige Zertifikats- oder Zertifikatschlüsseldatei von Ihrem lokalen Speichersystem in Citrix ADM hochladen, die Leseberechtigungen für solche Dateien werden jedoch nicht von ADM beibehalten. Wenn solche Dateien von ADM auf entsprechende ADC-Instanzen hochgeladen werden, zeigt ADC solche Dateien als ungültige Dateien an.

  [716691]

- Manchmal kann Citrix ADM aufgrund unsachgemäßer Ausnahmebehandlung möglicherweise nicht mit vertrauenswürdigen Citrix Diensten kommunizieren. Möglicherweise können Sie sich nicht am Citrix ADM Dienst anmelden. Möglicherweise gibt es auch einen Ressourcenverlust im ADM-Dienst.

  [717571]

- Wenn Sie zwei Ereignisregeln konfigurieren, die demselben Ereignis entsprechen, aber unterschiedliche Ereignisalter aufweisen, berücksichtigt Citrix ADM nur die Regel, für die ein geringeres Ereignisalter konfiguriert ist. Mit diesem Update berücksichtigt Citrix ADM beide Ereignisregeln.

  [716930]

- Syslog-Meldungen werden in Citrix ADM auf mehreren Seiten angezeigt. Wenn Sie auf einer Seite nach Syslog-Nachrichten suchen, indem Sie ein Schlüsselwort eingeben, werden dieselben Suchergebnisse nicht beibehalten, wenn Sie zu einer anderen Seite wechseln. Sie müssen erneut suchen, indem Sie dasselbe Stichwort eingeben. Mit diesem Update zeigt Citrix ADM das Ergebnis der Suche auf allen Seiten an.

  [715671]

27. Oktober 2018

Diese Version enthält Verbesserungen und Fehlerbehebungen.

Citrix Application Delivery Manager (Citrix ADM) Agents werden standardmäßig automatisch auf Citrix ADM 12.1 Build 504.131 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Möglichkeit, die Anzahl der angezeigten Syslog-Nachrichten zu steuern

Standardmäßig zeigt Citrix ADM 50 Syslog-Nachrichten auf jeder Seite an. Sie können nun mehr Nachrichten auf einer Seite anzeigen, indem Sie 100, 250, 500 oder 1.000 Nachrichten pro Seite auswählen.

Behobene Probleme

Analytics

- Wenn Sie über schreibgeschützte Berechtigungen verfügen, können Diagnosesymbole in keiner Analytics-Ansicht angezeigt werden.

  [715785]

Anwendungen

- Citrix ADM zeigt nicht die Anzahl der Transaktionen und das Datenflussvolumen für GSLB-Anwendungen auf dem Anwendungs-Dashboard an.

  [716878]

- Citrix ADM zeigt keine Informationen für virtuelle Server an, die sich auf Anwendungen beziehen, die auf ADC-Instanzen erstellt wurden, die mit hoher Verfügbarkeit bereitgestellt werden.

  [716906]

Netzwerke

- Citrix ADM Performance-Subsystem stürzt alle paar Stunden ab, was sich auf die Netzwerkberichterstattung auswirkt.

  [715483]

- Das Performance-Subsystem von Citrix ADM meldet eine hohe CPU-Auslastung, die sich auf die Netzwerkberichterstattung auswirkt.

  [716235]

- Wenn ASG in mehreren Availability Zones bereitgestellt wird, unterstützt das Graceful/Non Graceful Deletion von Back-End-Servern möglicherweise nicht die Amazon EC2 Auto Scaling Group.

  [716031]

- Wenn Sie SSL-Zertifikate basierend auf einer Suchoption exportieren, listet der CSV-Bericht alle SSL-Zertifikate unabhängig von den Suchkriterien auf.

  [714674]

- Wenn Sie zu Netzwerke > Ereignisse navigieren, werden die Ereignisse nicht zum ersten Mal in der Reihenfolge angezeigt. Wenn Sie auf die Spaltenüberschrift Datum klicken, werden die Ereignisse chronologisch sortiert angezeigt.

  [716615]

- In zeitweiligen Zeitabständen kann Citrix ADM das Sammeln von Datenpunkten für den täglichen Bericht verpassen. Dies wirkt sich auf die wöchentlichen und monatlichen Berichte aus.

  [716778]

System

- Sie können die Dateien nun in der Citrix ADM GUI nach den Datumsangaben sortieren, anstatt sie als Zeichenfolge zu sortieren.

  [715491]

12. Oktober 2018

Diese Version enthält Verbesserungen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf Citrix ADM 12.1 Build 502.127 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Unterstützung für EDT-Sitzungen in HDX Insight Berichten

Die HDX Insight zeigt nun die Anzahl der EDT Sitzungen und Nicht-EDT Sitzungen als Teil des aktiven Sitzungsberichts an. In der Tabelle Benutzer wird ein detaillierter Bericht aller Benutzer im System angezeigt. Außerdem wurde ein neues Donutdiagramm eingeführt, mit dem Sie die vom Benutzer verbrauchte Bandbreite und die Gesamtzahl der Bytes basierend auf dem von den Benutzern verwendeten Protokolltyp sehen können.

Unterstützung für die Anzeige von Load Balancing und Content Switching virtueller Server im Web Insight-Bericht

Die Web Insight-Berichte zeigen nun Daten von virtuellen Load Balancing Servern an, die an Content Switching virtuelle Server gebunden sind. Sie können Daten für beide virtuelle Server separat anzeigen. Weitere Informationen finden Sie unter An Content Switching-Server gebundene Lastausgleichsserver.

Unterstützung für die Anzeige von Citrix ADC-Instanzen sowohl in Hochverfügbarkeit als auch in Cluster in Web Insight-Berichten

In den Citrix ADM Analyseberichten werden nun Berichte für ADC-Instanzen angezeigt, die sowohl im Hochverfügbarkeitsmodus als auch im Clustermodus bereitgestellt werden. Sowohl die Gesamtzahl des Sitzungsstarts als auch die Gesamtzahl der Anwendungen in diesen beiden Szenarien als kombinierten Bericht anstelle von einzelnen Berichten für jede Instanz in der Gruppe.

> **Hinweis**
>
> - Alle Daten, die zuvor vor dem Upgrade auf Citrix ADM 12.1 Build 503.x gesammelt wurden,

werden weiterhin als unabhängige Berichte für den Zeitraum angezeigt, bis die Daten weiterhin bestehen.

- Bei ADC-Instanzen, die im Clustermodus bereitgestellt werden, wird der Name der Beobachtungsdomäne ID/Observation Domain durch CLIP Hostname und CLIP ersetzt. Alle zuvor gesammelten Daten melden weiterhin Observation Domain ID/Observation Domain Name. Weitere Informationen finden Sie unter Citrix ADC-Instanzen, die im Hochverfügbarkeits- und Clustermodus bereitgestellt werden.

Hinzufügen von Citrix ADC CPX-Instanz in Citrix ADM

Citrix ADM wurde erweitert, um die Verbesserungen der CPX-Funktionalitäten zu unterstützen. Citrix ADC CPX-Instanz wird jetzt in Citrix ADM auf eine der folgenden zwei Arten hinzugefügt:

- Durch Angabe einer IP-Adresse für den CPX zusammen mit einem Geräteprofil, wenn die CPX-Instanz für die Verwaltung des Nord-Süd-Datenverkehrs verwendet wird
- Durch Angabe der IP-Adresse des Docker Hosts, wenn Citrix ADC CPX-Instanz von Citrix ADM nicht erreichbar ist. Dies ist, wenn der CPX erforderlich ist, um den Ost-West-Datenverkehr in einem Rechenzentrum zu verwalten.

Wenn das Gerät über eine Docker IP erkannt wird, wird die IP-Adresse in der Datenbank als NSIP_DOCKERIP dargestellt. Wenn das Gerät über ein erreichbares NSIP des CPX erkannt wird, wird die IP-Adresse durch das NSIP des CPX in der ADM-Datenbank dargestellt.

Der Prozess der Zugabe einer CPX-Instanz ist jetzt ähnlich wie andere ADC-Typen wie VPX oder MPX in ADM hinzugefügt werden. Wenn Sie das Geräteprofil bereitstellen, können Sie den SSH-, HTTP-, HTTPS-Port im Geräteprofil konfigurieren, anstatt ihn explizit zu konfigurieren. Außerdem wurde die Registrierung von CPX in ADM verbessert. Wenn ein CPX gestartet wird, erkennt Citrix ADM automatisch die CPX-Instanz und registriert sie.

Sie müssen keinen Docker Host in Citrix ADM hinzufügen, um Citrix ADC CPX-Instanzen zu ermitteln.

Unterstützung für die automatische Skalierung von Citrix ADC-Instanzen, die in AWS bereitgestellt werden

Die automatische Citrix ADM Funktion unterstützt jetzt die Skalierung von Citrix ADC-Instanzen in AWS. Die Citrix ADM-Autoscaling-Funktion fügt in AWS bereitgestellte Citrix ADC-Cluster-Knoten hinzu oder entfernt sie, je nachdem, wann und in welchem Umfang die Back-End-Server Autoscale. Der Citrix ADM sammelt Statistiken (CPU-Auslastung, Speichernutzung, Durchsatz) aus den bereitgestellten Autoscale-Clustern. Diese Statistiken werden anhand des vom Kunden konfigurierten Werts ausgewertet. Je nachdem, ob die Statistiken den maximalen Schwellenwert überschreiten oder unter dem Mindestschwellenwert arbeiten, wird Scale-In bzw. Scale-Out ausgelöst.

Die Vorteile der automatischen Skalierung sind:

- Stellt sicher, dass die Anwendung ständig einsatzbereit ist und ausgeführt wird, unabhängig von den Anforderungen des Datenverkehrs.
- Citrix ADC-Instanzen werden dynamisch hinzugefügt und entfernt, indem sie zu einer manuellen Zero-Touch-Konfiguration führen.
- Die DNS-Verwaltung erfolgt automatisch.
- Ermöglicht ein besseres Kostenmanagement.

Um die Autoscale-Funktion verwenden zu können, müssen Sie Autoscale-Gruppen erstellen und die Anwendung mit StyleBooks bereitstellen. Weitere Informationen finden Sie unter Automatische Skalierung von Citrix ADC in AWS mit Citrix ADM.

Behobene Probleme

Analytics

- In der Tabelle Anwendungsübersicht unter Security Insight > Total Violations wird die Angriffszeit für alle historischen Datensätze als NA- angezeigt.

  [715905]

Netzwerke

- Statistiken der virtuellen Server werden nicht angezeigt, wenn die virtuellen Server Teil von Citrix ADC-Instanzen sind, die in hoher Verfügbarkeit bereitgestellt werden.

  [715243]

- Wenn Sie einen virtuellen GSLB-Server in Citrix ADM hinzufügen, der Teil einer benutzerdefinierten Anwendung ist, zeigt ADM möglicherweise die Statistiken für den hinzugefügten GSLB-Server nicht korrekt an.

  [715639]

- Wenn Sie Citrix ADC SDX-Plattform in ADM hinzufügen und wenn die Version des ADC SDX kleiner als 11.0 ist, zeigt das Dashboard von SDX, das in Citrix ADM sichtbar ist, möglicherweise Fehler an.

  [715803]

System

- Manchmal können Sie Citrix ADC-Instanzen möglicherweise nicht von Citrix ADM neu starten. Dies liegt daran, dass einige Instanzen länger als zehn Minuten für den Neustart benötigen und Citrix ADM nur zehn Minuten wartet, bis die Instanzen neu gestartet werden. Mit diesem Update können Sie jetzt die Citrix ADM Neustartzeit bis zu 30 Minuten konfigurieren.

  [716178]

14. September 2018

Diese Version enthält Verbesserungen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf Citrix ADM 12.1 Build 502.127 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Einschließlich aggregierter Angriffszeit in Security Insight-Berichten

Im Bericht **Total Violations** in Security Insight wurde die Angriffszeit als NA angezeigt, wenn die ausgewählte Dauer länger als eine Stunde beträgt. Wenn Sie nun 1 Tag aus der Liste auswählen, zeigt der Bericht alle aggregierten Angriffe an und die Angriffszeit wird in einer Stunde angezeigt. Wenn Sie 1 Woche oder 1 Monat wählen, werden alle Angriffe aggregiert und die Angriffszeit wird in einem Tagesbereich angezeigt. Weitere Informationen finden Sie unter Sicherheitshinweise.

[686874]

Behobene Probleme

System

- Wenn Sie in Citrix ADM Benutzeradministratorprofile ändern, werden Citrix ADC-Instanzen nicht wiederentdeckt, und Sie können sich nicht bei Citrix ADC-Instanzen anmelden. Die Instanzen werden nicht mit den neuen Benutzerdetails aktualisiert, und die Instanzen verwenden weiterhin die ursprünglich angewendeten Administratorprofile.

  [699435]

Netzwerke

- Die folgenden beiden Probleme werden in Citrix ADM im Zusammenhang mit virtuellen Servern festgestellt:
  - Wenn ein virtueller Server mit einem DNS-Server mit mehreren IP-Adressen konfiguriert ist, kann Citrix ADM diese virtuellen Server nicht erkennen.
  - Wenn ein virtueller Server einige nicht englische Zeichen im Kommentar oder in einem anderen Feld enthält, gibt Citrix ADM einen Fehler zurück und kann keine virtuellen Server für diese Instanz erkennen.

  [713472]

23. August 2018

Diese Version enthält Verbesserungen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf Citrix ADM 12.1 Build 501.123 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue und erweiterte Features

Umbenennen von NetScaler Management and Analytics Service

NetScaler Management and Analytics Service wird jetzt in Citrix Application Delivery Management (ADM) umbenannt. Dies ist Teil des einheitlichen Produktportfolios von Citrix.

Möglicherweise bemerken Sie neue Namen in unseren Produkten und Produktdokumentation. Dies ist das Ergebnis der Erweiterung des Citrix Portfolios und der Cloud-Strategie. Weitere Informationen zum einheitlichen Citrix Portfolio finden Sie unterCitrix product guide.
Die Implementierung dieser Umstellung in unsere Produkte und deren Dokumentation ist ein kontinuierlicher Prozess.

- Inhalte in Produkt und Dokumentation enthalten möglicherweise noch die früheren Namen. Beispielsweise können Sie Instanzen der früheren Namen in Konsolentext, Meldungen, Verzeichnis-/Dateinamen, Screenshots und Diagrammen sehen.
- Es ist möglich, dass einige Elemente (wie Befehle) weiterhin ihre früheren Namen behalten, um bestehende Kundenskripte zu verhindern.
- Die zugehörige Produktdokumentation und andere Ressourcen (z. B. Videos und Blogposts), zu denen es Links in dieser Produktdokumentation gibt, verwenden möglicherweise weiterhin die früheren Namen.

[715090]

Behobene Probleme

Netzwerke

- Doppelte Einträge werden angezeigt, wenn Sie alle aufgelisteten Einträge in der Netzwerkfunktion wie Lastenausgleich, Content Switching, Cache-Umleitung usw. filtern.

  [704095]

- Wenn Sie zu **Netzwerke** > **Instanzen** navigieren und **Analytics für eine Citrix ADC-Instanz konfigurieren** auswählen, um Insight auf virtuellen Servern zu aktivieren, werden auf der Seite

Analytics konfigurieren die Details des virtuellen Servers nicht angezeigt, wenn die virtuellen Server haben ein Leerzeichen in ihren Namen.

[713945]

- Wenn Sie Collectors konfigurieren, die direkt in der Citrix ADC-Instanz konfiguriert sind, werden im Spaltenfeld **Transportmodus** auf der Seite “Analytics konfigurieren” keine Daten angezeigt.

  [713946]

03. August 2018

Diese Version enthält Verbesserungen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf Citrix ADM 12.1 Build 500.126 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue Features

GitHub importieren und synchronisieren für StyleBooks

Sie können jetzt die Funktion Repositories in Citrix ADM verwenden, um StyleBooks direkt aus GitHub-Repositories zu importieren und zu synchronisieren. Sie können StyleBooks von mehreren GitHub-Repositories synchronisieren. StyleBooks, die in GitHub erstellt und aus GitHub Repositories importiert werden, sind immer noch von Citrix ADM RBAC-Richtlinien abhängig wie StyleBooks manuell importiert. Sie können ein GitHub-Repository konfigurieren, indem Sie entweder den GitHub-Benutzernamen und das Kennwort oder ein API-Token verwenden.

> **Hinweis**
>
> - Sie können StyleBooks nur importieren und synchronisieren, denen keine abhängigen StyleBooks zugeordnet sind (d. h., das StyleBook muss alle Konfigurationen in dieser Datei definiert haben).
> - Die Sync aus einem GitHub-Repository muss manuell von der Citrix ADM GUI oder API initiiert werden (d. h. der Import von StyleBooks erfolgt nicht automatisch basierend auf der GitHub-Commit-Aktivität.)

Weitere Informationen finden Sie unter.Importieren und Synchronisieren von StyleBooks aus dem GitHub-Repository

[699790]

Verwenden von StyleBooks zum Erstellen von Lastenausgleichs-Servern mit Anwendungsfirewall

Sie können jetzt die Konfiguration der Citrix WAF-Funktion (Web Application Firewall) mithilfe des neuen Standard-WAF-StyleBook in Citrix ADM automatisieren. Dieses StyleBook ermöglicht es Benutzern, einen virtuellen Lastausgleichsserver mit den zugehörigen App-Firewall-Richtlinien und -Einstellungen zu erstellen.

> **Hinweis**
>
> Bevor Sie die App Firewall-Signaturen konfigurieren können, müssen Sie die Signaturobjekte in der Citrix ADC-Instanz aus der entsprechenden Standardsignaturobjektvorlage erstellen. Sie können die Standardsignaturobjekte nicht über das WAF StyleBook konfigurieren oder ändern.

Weitere Informationen finden Sie unter Webanwendungs-Firewall-StyleBook.

[708597]

Möglichkeit zum Ändern des Kennworts für Citrix ADM Agent

Sie können nun das Skript change_agent_system_password.py in der Befehlszeile ausführen, mit dem Sie das Kennwort des Citrix ADM Agenten aktualisieren können, nachdem Sie den Agenten bereitgestellt haben. Weitere Informationen finden Sie unter Ändern des Agent-Kennworts nach der Registrierung des Agenten.

[712517]

Behobene Probleme

Netzwerke

- Beim Erstellen von Konfigurationsaufträgen mit der Master-Konfigurationsvorlage müssen Sie möglicherweise dieselbe Konfigurationsdatei mehrmals nach dem Bearbeiten der Datei hochladen. Sie können die Datei beim ersten Mal erfolgreich hochladen. Spätere Uploads schlagen ohne Benutzerbenachrichtigung fehl.

  Problemumgehung: Dies geschieht aufgrund des Browser-Standardverhaltens. Wenn Sie dieselbe Datei nach Änderungen erneut hochladen möchten, klicken Sie auf Zurück, um zur Registerkarte Instanzen auswählen zu gehen, und klicken Sie dann auf Weiter, und laden Sie die gleiche Datei erneut hoch.

  [711593]

- Citrix ADM kann nicht alle gebundenen Dienstgruppenmitglieder analysieren

  [712022]

Analytics

- Es ist nicht möglich, Informationen in Web Insight zu sehen, wenn Sie mit “schreibgeschützten” Rechten auf Citrix ADM zugreifen.

  [713404]

- Wenn Sie einen zuvor erstellten IP-Block auf der Seite **IP-Blöcke konfigurieren** unter **Analytics** > **Einstellungen** bearbeiten, indem Sie Stadt, Region und Land ändern, und wenn Sie versuchen, die Einstellungen erneut zu bearbeiten, wird auf der Seite IP-Blöcke konfigurieren der Name der vorherigen Stadt angezeigt. Dieser Build behebt dieses Problem.

  [712110]

- Es kann vorkommen, dass eine Tabelle auf mehrere Seiten verteilt wird, da Citrix ADM nur 25 Zeileneinträge auf einer Seite anzeigt. Früher konnten Sie Zeileneinträge nur auf der aktuellen Seite sortieren. Auf den anderen Seiten wurden nie sortierte Einträge angezeigt. Sie können die Tabelle nun auf einer beliebigen Seite sortieren, und alle Seiten dieser Tabelle zeigen die sortierten Ergebnisse an.

  > **Hinweis:** Diese Funktion funktioniert nur, wenn die Anzahl der Datensätze in einer Tabelle weniger als 25.000 beträgt.

  [689564]

Bekannte Probleme

Anwendungen

- Wenn Sie zu **Netzwerke** > **Instanzen** navigieren und **Analytics für eine Citrix ADC-Instanz konfigurieren** auswählen, um Insight auf virtuellen Servern zu aktivieren, spiegelt die Seite **Analytics konfigurieren** nicht den richtigen Status des virtuellen Servers wider, wenn die virtuelle Server haben einen Space in ihren Namen. Obwohl die AppFlow Protokollierung beispielsweise auf dem virtuellen Server aktiviert ist, wird sie möglicherweise auf der Seite **Analytics konfigurieren** als deaktiviert angezeigt.

  [713945]

- Wenn Sie Collectors direkt in der Citrix ADC-Instanz konfigurieren, werden im Spaltenfeld Transportmodus auf der Seite Analytics konfigurieren keine Daten angezeigt.

  [713946]

Analytics

- In bestimmten Fällen werden HDX Insight - und Citrix Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.

Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut.

[690327]

Netzwerke

- Doppelte Einträge werden angezeigt, wenn Sie alle aufgelisteten Einträge in der Netzwerkfunktion wie Lastenausgleich, Content Switching, Cache-Umleitung usw. filtern.

  [704095]

- Wenn Sie zu Netzwerke > Instanzen navigieren und Analytics konfigurieren für eine Citrix ADC-Instanz auswählen, um Insight auf virtuellen Servern zu aktivieren, werden auf der Seite Analytics konfigurieren die Details des virtuellen Servers nicht angezeigt, wenn die virtuellen Server einen Space im Namen haben.

  [713945]

- Wenn Sie Collectors konfigurieren, die direkt in der Citrix ADC-Instanz konfiguriert sind, werden im Spaltenfeld Transportmodus auf der Seite “Analytics konfigurieren” keine Daten angezeigt.

  [713946]

Einstellungen

- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter Einstellungen > Benutzerverwaltung > Benutzer angezeigt.

  [686581]

12. Juli 2018

Dieses Release enthält Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf den Build 516.126 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue Features

Testschaltfläche für die E-Mail-Konfiguration für Citrix ADM Ereignisbenachrichtigungen

Beim Senden von E-Mails für Ereignisbenachrichtigungen möchten Sie möglicherweise eine Test-E-Mail senden, um die konfigurierten Einstellungen zu testen. Mit der Schaltfläche Testen können Sie

nun eine Test-E-Mail senden, nachdem Sie einen E-Mail-Server, zugehörige verteilte Listen und andere Einstellungen konfiguriert haben. Diese Funktion stellt sicher, dass die Einstellungen einwandfrei funktionieren. Weitere Informationen finden Sie unter Ereignisregeln erstellen.

[684948]

Anpassung der Betreffzeile der Ereignisbenachrichtigung

In einem großen Netzwerk, in dem viele virtuelle Server konfiguriert sind, erhalten Sie als Administrator möglicherweise täglich eine hohe Anzahl von E-Mails. Möglicherweise möchten Sie jedoch den Namen der betroffenen Entität im E-Mail-Popup sehen, wenn die E-Mail empfangen wird, damit Sie die betroffene Entität bestimmen können, ohne die E-Mail öffnen zu müssen. Wenn Sie unter **Netzwerke** > **Ereignis** > **Regeln** eine Regel erstellen und E-Mail-Benachrichtigungsregeln festlegen, haben Sie jetzt die Option, einige zusätzliche Informationen wie den Namen der betroffenen Entität (Fehlerobjekt) aufzunehmen. Weitere Informationen finden Sie unterEreignisregeln erstellen.

[705142]

Verbesserungen bei der Funktion Pooled Capacity

Einige Änderungen wurden auf der Seite Pooled Lizenzen in Citrix ADM für Citrix VPX-Instanzen vorgenommen. Bei der Zuweisung von Lizenzen im Lizenzpool zu Citrix ADC-Instanzen bei Bedarf wurde ein neuer Satz von Zuständen eingeführt. Der Status ist wie folgt:

- Zugeteilt
- Kulanzzeitraum
- Synchronisierung wird ausgeführt
- Teilweise zugeordnet
- Gerät nicht verwaltet
- Zugeteilt. Nicht auf das Gerät angewendet
- Verbindung unterbrochen

Außerdem wurden einige weitere Details zum Status der Lizenzzuweisung zu Citrix ADM hinzugefügt. Weitere Informationen finden Sie unter Gepoolte Kapazität.

[709975]

Verfügbarkeit von Lizenzierungsfunktionen in Citrix ADM

Citrix ADM hostet jetzt einen gemeinsamen Bandbreiten- und Instanzpool, der die Citrix VPX- und MPX-Instanzen, die in Citrix ADM hinzugefügt werden, Server. Aus diesem gemeinsamen Pool wird jede Citrix ADC-Instanz in Ihrem Rechenzentrum unabhängig von der Plattform oder dem Formfaktor eine Instanzlizenz und nur die erforderliche Bandbreite ausgecheckt. Weitere Informationen finden Sie unter Gepoolte Kapazität.

[709679]

Konfigurierbare automatische Lizenzunterstützung für nicht adressierbare virtuelle Server

Citrix ADM wendet standardmäßig keine Lizenzen auf nicht adressierbare virtuelle Server an. Für die Lizenzierung nicht adressierbarer virtueller Server müssen Sie die Option für die automatische Lizenzierung deaktivieren und die nicht adressierbaren virtuellen Server manuell auswählen. Dies erhöht den Aufwand, die nicht adressierbaren Server zunächst manuell auszuwählen, wenn Sie die Lizenzen anwenden, und auch wenn Sie die neuen nicht adressierbaren virtuellen Server auswählen müssen, wenn sie Ihrem Netzwerk hinzugefügt werden.

Die neue Option in Citrix ADM unter **Netzwerke** > **Lizenzen** > **Systemlizenzen** lautet Automatische Auswahl nicht adressierbarer virtueller Server. Wenn Sie diese Option aktivieren, können Sie jetzt explizit angeben, dass die Lizenzierung auch nicht adressierbare virtuelle Server enthalten muss.

> **Hinweis**
>
> - Citrix ADM wählt standardmäßig noch nicht automatisch nicht adressierbare virtuelle Server für die Lizenzierung aus.
> - Anwendungsanalysen (App Dashboard) sind die einzige Analyse, die derzeit auf lizenzierten, nicht adressierbaren virtuellen Servern unterstützt wird. Weitere Informationen finden Sie unter Abonnements verwalten

[707843]

Möglichkeit zur Bereitstellung von Citrix ADC VPX Instanzen in AWS mit Citrix ADM

Mit Citrix ADM können Sie jetzt Citrix ADC VPX Instanzen auf der Amazon Web Services Plattform (AWS) als eigenständige Bereitstellung bereitstellen. Mit Citrix ADC VPX auf AWS können Sie AWS Cloud Computing-Funktionen nutzen und Citrix ADC Load Balancing und Traffic-Management-Funktionen für ihre geschäftlichen Anforderungen nutzen. Citrix ADC auf AWS unterstützt alle Funktionen der Datenverkehrsverwaltung einer physischen Citrix ADC-Appliance. Weitere Informationen finden Sie unter Provisioning von Citrix ADC VPX Instanzen in AWS.

[680526]

Behobene Probleme

Hohe Verfügbarkeit

- Wenn Sie einen Knoten in einem Paar von Citrix ADC-Instanzen im Hochverfügbarkeitsmodus mit der IP-Adresse im Bereich 171.31.200.x konfigurieren, werden dieses Citrix ADC-Instanzen nicht von Citrix ADM erkannt.

  [710589]

Netzwerke

- Beim Erstellen von Konfigurationsaufträgen mit der Master-Konfigurationsvorlage müssen Sie möglicherweise dieselbe Konfigurationsdatei mehrmals nach dem Bearbeiten der Datei hochladen. Sie können die Datei beim ersten Mal erfolgreich hochladen. Spätere Uploads schlagen ohne Benutzerbenachrichtigung fehl.

  Problemumgehung: Dies geschieht aufgrund des Browser-Standardverhaltens. Wenn Sie dieselbe Datei nach Änderungen erneut hochladen möchten, klicken Sie auf Zurück, um zur Registerkarte Instanzen auswählen zu gehen, und klicken Sie dann auf Weiter, und laden Sie die gleiche Datei erneut hoch.

  [711593]

- Die Netzwerk-Ereignisübersichtsdaten werden aufgrund von Formatierungsproblemen abgeschnitten.

  [704980]

- Die SNMP v3-basierte Ereignisberichterstattung funktioniert nach dem Upgrade von Citrix ADM auf Version 12.1 nicht. Citrix empfiehlt die folgende Problemumgehung für Citrix ADC-Instanzen in Version 12.1, 48.13 Build in Citrix ADM hinzugefügt.

  Problemumgehung: Verwenden Sie SNMP v2-Traps, bis das SNMP v3-Problem behoben und freigegeben ist.

  [710564]

- Wenn für Citrix ADC-Instanzen ein Failover in einem Hochverfügbarkeitsmodus bereitgestellt wird, erhält der mas_afdecoder-Prozess keine Benachrichtigung zum Aktualisieren der Lizenzinformationen. Der mas_afdecoder-Prozess löscht das vom primären Knoten empfangene Datenpaket. Daher werden Web Insight-Berichte nicht auf der Citrix ADM GUI angezeigt.

  [711503]

System

- Agentenregistrierung schlägt fehl, wenn der Name der Stadt ein Unicode-Zeichen hat.

  [711737]

- Wenn Sie versuchen, einen neuen Citrix ADM Agent zu aktivieren, wird möglicherweise eine Fehlermeldung Ungültige Instanz-ID angezeigt.

  [706527]

StyleBooks

- Sharepoint StyleBook muss das SSL-Protokoll für alle Back-End-Services unterstützen.

  [706507]

- Feld Autor zeigt null in der API-Antwort verwendet, um Informationen über ein StyleBook abzurufen.

  [711021]

Bekannte Probleme

Analytics

- In bestimmten Fällen werden HDX Insight - und Citrix Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.

  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut.

  [690327]

Netzwerke

- Doppelte Einträge werden angezeigt, wenn Sie alle aufgelisteten Einträge in der Netzwerkfunktion wie Lastenausgleich, Content Switching, Cache-Umleitung usw. filtern.

  [704095]

Einstellungen

- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter Einstellungen > Benutzerverwaltung > Benutzer angezeigt.

  [686581]

14. Juni 2018

Dieses Release enthält Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf den Build 515.116 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue Features

Rollenbasierte Zugriffssteuerung auf GSLB-Domänen

Sie können jetzt nur autorisierte Benutzer erlauben, die GSLB-Konfiguration mit StyleBooks durchzuführen, da RBAC derzeit auch auf GSLB-Domänen unterstützt wird.

Citrix ADM unterstützt jetzt eine neue Entität namens DNS-Domänenname. Navigieren Sie in Citrix ADM zu **Netzwerke** > **DNS-Domänenname**, und fügen Sie die Einträge für DNS-Domänennamen hinzu. Navigieren Sie zu **System** > **Benutzeradministration** > **Gruppen**. Definieren Sie RBAC-Einstellungen für eine Benutzergruppe für ausgewählte Domänennamen aus der verfügbaren Liste der Domänennamen.

Diese RBAC-Einstellung gilt für Ihre Benutzer, wenn sie versuchen, GSLB mit StyleBooks zu konfigurieren. Die Benutzer können nur einen oder mehrere DNS-Domänennamen verwenden, zu denen sie berechtigt sind.

[706988]

Verbesserte Funktionalität für die Suche von Citrix ADC-Instanzen

Betrachten Sie ein Szenario, in dem Citrix ADM viele Citrix ADC-Instanzen verwaltet. Möglicherweise möchten Sie die Flexibilität, die Inventarisierung von Instanzen basierend auf einigen Suchparametern zu durchsuchen. Citrix ADM bietet nun zwei Suchkriterien: Tags und Eigenschaften, um effizient nach einer Teilmenge von Citrix ADC-Instanzen zu suchen, die die Suchparameter qualifizieren.

Beispiel: Sie möchten alle Citrix ADC-Instanzen durchsuchen, die sich auf Version 12.0 befinden und sich im Status UP befinden. Weitere Informationen finden Sie unter Tags erstellen und Instanzen zuweisen.

[709997]

Möglichkeit zur Kennzeichnung von Citrix ADC-Instanzen

Tags sind Begriffe oder Schlüsselwörter, die Sie einer Citrix ADC-Instanz zuweisen können, um eine zusätzliche Beschreibung über die Citrix ADC-Instanz zuzuordnen. Mit Citrix ADM können Sie Ihre Citrix ADC-Instanzen nun Tags zuordnen. Mit diesen Tags können Sie Citrix ADC-Instanzen gruppieren, identifizieren und suchen. Weitere Informationen finden Sie unter Tags erstellen und Instanzen zuweisen.

[708603]

Möglichkeit, Ereignisbenachrichtigungen an Slack zu senden

Früher hatten Sie in der Citrix ADM GUI die Option, E-Mail-Benachrichtigungen für Ereignisse zu senden. Sie können jetzt auch eine Ereignisbenachrichtigung an den Slack Kanal senden.

Konfigurieren Sie den erforderlichen Slack Kanal, indem Sie den Profilnamen und die Webhook-URL in der Citrix ADM GUI angeben. Die Ereignisbenachrichtigungen werden dann an diesen Kanal gesendet. Weitere Informationen finden Sie unter Ereignisregeln erstellen.

[656472]

Behobene Probleme

Netzwerke

- AppFlow kann nicht auf virtuellen Servern konfiguriert werden, wenn Citrix ADM mit einer anderen Schnittstelle als 0/1 konfiguriert ist. [705330]
- Leerzeichen nicht in den Namen[708003]der Konfigurationsüberwachungsvorlagen einschließen

StyleBooks

- Sie können keine Entität mit StyleBooks erstellen, wenn Sie benutzerdefinierte Header im StyleBook definiert haben. [709094]

Einstellungen

- Obwohl Sie Systembenachrichtigungen über die Abmeldung von Benutzern sehen können, erhalten Sie möglicherweise keine E-Mail-Benachrichtigungen. [704344]
- Citrix ADM kann die Citrix ADC-Instanz nicht vorvalidieren, wenn die NTP-Details in der Datei rc.netscaler hinzugefügt werden. Sie können diese Citrix ADC-Instanzen nun auswählen und beim Upgrade der Instanzen entfernen. [708466]
- Citrix ADC exportiert Datensätze für die gleiche Anwendung multiple application terminate. Dies führt zum Absturz des Citrix ADM `afdcoder` ADM-Prozesses. [709462]

Hohe Verfügbarkeit

- Wenn einer Benutzergruppe eine Citrix ADC-Instanz im Hochverfügbarkeitsmodus zugewiesen wird und wenn das Instanzpaar ein Failover ausgeführt wird, wird die Instanz nicht mehr der Benutzergruppe zugewiesen. [709202]

Bekannte Probleme

Analytics

- In bestimmten Fällen werden HDX Insight - und Citrix Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt. **Problemumgehung**: Aktualisieren Sie die Seite und versuchen Sie es erneut. [690327]

Netzwerke

- Doppelte Einträge werden angezeigt, wenn Sie alle aufgelisteten Einträge in der Netzwerkfunktion wie Lastenausgleich, Content Switching, Cache-Umleitung usw. filtern. [704095]

Einstellungen

- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]

Mai 24, 2018

Dieses Release enthält Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf den Build 514.117 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Behobene Probleme

Netzwerke

- Betrachten Sie ein Szenario, in dem Sie RBAC-Zugriff nur auf Netzwerke, Analytics und Systemknoten haben. Das Standardverhalten besteht darin, dass der erste Knoten im Navigationsbereich, d. h. Netzwerke, die Zielseite sein muss, wenn Sie auf Citrix ADM zugreifen. Aber jetzt ist der Analytics-Knoten die Zielseite. [705347]
- Wenn Sie einen Konfigurationsauftrag mit Internet Explorer 11.0, Firefox Version 31.0 und Google Chrome Version 31.0 erstellen, wird der folgende Fehler angezeigt:

```
SCRIPT5017: Syntax error in regular expression rdx.js (61,583910)
    ”
<!--NeedCopy-->
```

[707767]

- Eine Statusmeldung Kein Unterschied wird im Diagramm Verletzungen der Citrix ADC Überwachungsvorlage angezeigt, wenn zwei geplante Überwachungsvorlagen, die dieselbe Instanz abfragen, eine Instanz mit Verletzungen aufweisen. [708404]
- Sie können den Namen der Überwachungsvorlage nicht ändern oder bearbeiten.[708407]
- In Überwachungsvorlagen wird das Zeichen '&' in Variablenwerten durch das Zeichen '&' in der Eingabedatei ersetzt.[708766]
- Wenn Sie unter Network Reporting einen Schwellenwert für Instanzen festlegen, enthält die Liste der Instanzen zusätzlich zu Citrix ADC SDX-Instanzen Citrix.
  [707980]
- Wenn Sie Citrix SD WAN-WO-Instanz zu Citrix ADM hinzufügen, ist die SNMP-Verbindung nicht erfolgreich, und die GUI reagiert nicht mehr.
  [709146]

Analytics

- Wenn Sie einen Gateway Insight-Bericht basierend auf dem Benutzernamen filtern, kann Citrix ADM benutzerspezifische Details nicht filtern.
  [701514]
- Der Prozess mas_afdecoder schlägt gelegentlich fehl, wenn ein hohes Volumen an HTTP-Transaktionen vorhanden ist.
  [706509]

Bekannte Probleme

Analytics

- In bestimmten Fällen werden HDX Insight - und Citrix Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut.
  [690327]

Netzwerke

- Doppelte Einträge werden angezeigt, wenn Sie alle aufgelisteten Einträge in der Netzwerkfunktion wie Lastenausgleich, Content Switching, Cache-Umleitung usw. filtern.
  [704095]

Einstellungen

- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt.
  [686581]

04. Mai 2018

Dieses Release enthält Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf den Build 513.120 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Behobene Probleme

Analytics

- Die kombinierte grafische Ansicht in HDX Insight zeigt falsche Zeitzone. [703906]
- Die Web Insight-Berichtsgenerierung wird aufgrund einer falschen HTTP-POST-Transaktionszeitberechnung beendet. [707146]

Netzwerke

- Wenn Berichte im CSV-Format exportiert werden, werden in der Zeitspalte Daten im Epoch-Format und nicht im vom Benutzer lesbaren Format angezeigt.
  [704828]
- Die Ausführungsübersicht für einen Konfigurationsauftrag wird auf Citrix ADM als abgeschlossen angezeigt, selbst wenn die Befehle im Konfigurationsauftrag nicht vollständig auf der Citrix ADC-Instanz ausgeführt werden.
  [707317]

Bekannte Probleme

Analytics

- In bestimmten Fällen werden HDX Insight - und Citrix Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut.
  [690327]

Netzwerke

- Doppelte Einträge werden angezeigt, wenn Sie alle aufgelisteten Einträge in der Netzwerkfunktion wie Lastenausgleich, Content Switching, Cache-Umleitung usw. filtern.
  [704095]

Einstellungen

- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt.
  [686581]

12. April 2018

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf Build 512.119 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue Features

Möglichkeit zum Ausblenden von Standard-StyleBooks vor Citrix ADM

Sie können jetzt alle Standard-StyleBooks aus der Liste der verfügbaren StyleBooks in Citrix ADM ausblenden. Navigieren Sie zu **Anwendungen** > **Konfigurationen** > **Einstellungen**. Aktivieren **Sie das Kontrollkästchen Standardformatbücher ausblenden**. Alle Standard-StyleBooks sind jetzt ausgeblendet und sind für Ihre Benutzer nicht zugänglich. Sie können die Seite **Einstellungen** selbst vor den Benutzern weiter ausblenden. Mit der RBAC-Funktion können Sie eine geeignete Zugriffsrichtlinie erstellen, bei der die Seite Einstellungen für Benutzer unzugänglich gemacht werden kann. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Zugriffsrichtlinien**. Erstellen Sie eine Richtlinie und deaktivieren Sie im Abschnitt Berechtigungen unter **Alle** > **Anwendungen** > **Konfiguration** die Option Einstellungen. Weitere Informationen finden Sie unter Alle Standard-StyleBooks ausblenden.

[686914]

Suche nach allen benutzerdefinierten StyleBooks in Citrix ADM

Citrix ADM ermöglicht jetzt die Suche nach StyleBooks basierend auf ihrem Typ. Das heißt, Sie können jetzt auf der Listing-Seite StyleBooks in Citrix ADM nach allen benutzerdefinierten StyleBooks suchen. Weitere Informationen finden Sie unter Benutzerdefinierte StyleBooks verwenden.

[681949]

Behobene Probleme

Analytics

- Wenn der AppFlow Datenverkehr von einem Citrix ADC Cluster stammt, speichert Citrix ADM die Daten nicht länger als sieben Tage.
  [706348]

Netzwerke

- Wenn Sie eine Vorlage importieren oder eine Konfigurationsvorlage zum Erstellen eines Auftrags verwenden, werden die Variablenwerte nicht angezeigt. Klicken Sie nach der Vorschau auf **Fertig**, um die Variablenwerte anzuzeigen.
  [705884]
- Konfigurationsaufträge werden nicht vollständig ausgeführt, wenn mehrere Konfigurationsaufträge gleichzeitig mit zahlreichen Befehlen und in mehreren Fällen ausgeführt werden. Die Ausführung von Jobs stagniert und erscheint im Status In Bearbeitung.
  [706201]
- Konfigurationsvorlagen werden auch dann in Citrix ADM hochgeladen, wenn der Import der Konfigurationsvorlagen abgebrochen wird.
  [706219]
- Wenn Sie in Citrix ADM zu **Netzwerke** > **Ereignisse** > **Syslog Messages**navigieren, werden zuerst die ältesten Nachrichten angezeigt, obwohl das Fenster Sortieren die Option “Neueste zuerst” anzeigt. Erst wenn Sie Älteste zuerst auswählen und dann Neueste zuerst auswählen, werden die Meldungen korrekt angezeigt.
  [702305]
- Wenn Sie die Ereignisregel “unterdrücken” für ein Ereignis zusätzlich zu anderen Ereignisregeln konfigurieren, führt Citrix ADM alle konfigurierten Ereignisregeln aus.
  [702517]

System

- Sie können nicht mehr auf dieselbe Citrix ADC-Instanz zugreifen, nachdem Sie sie geschlossen haben, obwohl Sie Anmeldeinformationen für einmaliges Anmelden verwenden.
  [699435]

Bekannte Probleme

Analytics

- In bestimmten Fällen werden HDX Insight - und Citrix Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.

Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut.
[690327]

Einstellungen

- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM **unter Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt.
[686581]

22. März 2018

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf Build 511.118 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue Features

Einführung in das Hilfecenter in Citrix ADM

Citrix ADM verfügt jetzt über ein Hilfecenter, mit dem Sie auf Links für die verschiedenen Aufgaben zugreifen können, die Sie möglicherweise ausführen. Beispielsweise erfahren Sie, wie Sie Citrix ADM zum ersten Mal einbauen. Sie können auch die neuesten Versionshinweise anzeigen oder lernen, wie Sie Ihre Abonnements verwalten.

[706025]

Konfigurieren von Citrix ADC-Instanzen als ADFS-Proxy mit einem StyleBook

Sie können jetzt eine Citrix ADC-Instanz so konfigurieren, dass sie mit StyleBooks als Reverseproxy für Active Directory Federation Services (ADFS 2.0) funktioniert. Die Citrix ADC-Instanz kann nun das einmalige Anmelden (SSO) -Erlebnis für Active Directory-authentifizierte Clients auf Ressourcen außerhalb des Enterprise-Rechenzentrums erweitern. Die Instanz kann nun sowohl die aktive als auch die passive ADFS-Authentifizierung unterstützen. Weitere Informationen finden Sie unter Microsoft ADFS-Proxy-StyleBook.

[696203]

Verbesserungen des Instanz-Dashboards

Das Instanz-Dashboard in Citrix ADM zeigt Daten an, die von einer bestimmten Instanz abgefragt wurden. Standardmäßig werden verwaltete Instanzen jede Minute zur Datenerfassung abgefragt. Statistische Informationen wie Status, HTTP-Anfragen pro Sekunde, CPU-Auslastung, Speicherauslastung und Durchsatz werden kontinuierlich mit NITRO -Aufrufen erfasst. Als Administrator können Sie all diese gesammelten Daten auf einer einzigen Seite anzeigen. Sie können auch Probleme in der Instanz identifizieren und sofortige Maßnahmen ergreifen, um sie zu beheben.

Um das Dashboard einer bestimmten Instanz anzuzeigen, navigieren Sie zu **Netzwerke > Instanzen >** (Instanztyp). Wählen Sie die Instanz aus, die Sie anzeigen möchten, und klicken Sie auf **Dashboard**.

Die Registerkarte **Übersicht** zeigt CPU, Speicherauslastung und Ereignisse einer bestimmten Instanz an. Sie können andere instanzspezifische Dashboards anzeigen, um detailliertere Informationen über Ihre Instanz zu erhalten. Die anderen Registerkarten sind SSL, Konfigurationsaudit, Netzwerkfunktionen und Netzwerknutzung.

[687676]

Verbesserungen der Netzwerkinventarisierung

Sie können nun die vollständige Liste der Instanzen anzeigen, die von Citrix ADM verwaltet werden. Sie können den Bestandsbericht anzeigen, indem Sie zu **Netzwerke > Dashboard** navigieren und oben rechts auf dem Bildschirm auf **Alle Instanzen** klicken. Der neue Lagerbericht zeigt folgende Informationen an:

- Alle Instanzen
- Instanzversionen
- Seriennummern

[687676]

Indikator für den Abfragefortschritt

Sie können nun den Status Ihrer Abrufaktion für Instanzen in Citrix ADM anzeigen. Wenn Sie zuvor die Aktion **Jetzt abfragen** wählen (z. B. Zertifikate, Konfigurationsaudits und Erkennung), wurde die GUI nur angezeigt, wenn die Abfrage initiiert wurde. Jetzt können Sie den Fortschritt der Polling, wann sie ausgeführt wird und ob sie abgeschlossen ist, sowie die Informationen sehen, die während der Polling-Aktion von der Instanz abgerufen wurden.

Weitere Informationen finden Sie unter Citrix ADC-Instanzen und Entitäten abfragen.

[688916]

Behobene Probleme

- Auf der Seite **“Einstellungen” > “Abonnements** “ wird der Speicherdatenverbrauch möglicherweise größer als das zulässige Speicherlimit von 5 GB angezeigt.
  [689330]
- Citrix SD-WAN WO oder Citrix ADC SDX-Instanzen können nicht von Citrix ADM 506.119 Build aktualisiert werden.
  [699814]
- Die Citrix Cloud-Navigationsleiste ist nicht sichtbar, wenn Sie sich mit Internet Explorer 11 anmelden.
  [702339]

Bekannte Probleme

Netzwerke

- Wenn Sie in Citrix ADM zu Netzwerke > Ereignisse > Syslog-Nachrichten navigieren, werden zuerst die ältesten Nachrichten angezeigt. Im Fenster Sortieren wird jedoch die Option Neueste zuerst angezeigt. Erst wenn Sie Älteste zuerst auswählen und dann Neueste zuerst auswählen, werden die Meldungen korrekt angezeigt.
  [702305]

Analytics

- In bestimmten Fällen werden HDX Insight - und Citrix Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut.
  [690327]

Einstellungen

- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt.
  [686581]

März 3, 2018

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf den Build 510.120 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann

die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue Features

Verbessertes Dashboard für Netzwerkberichte

Sie können nun benutzerdefinierte Dashboards mit mehreren Widgets erstellen, die unterschiedliche Berichtsdaten anzeigen. Sie können mehrere Berichte für eine beliebige Anzahl virtueller Server und bis zu zehn Instanzen auf Ihrem angepassten Dashboard anzeigen. Sie können auch die Dauer Ihrer Berichte anpassen und zur weiteren Analyse exportieren. Weitere Informationen finden Sie unter Netzwerkberichterstattung.

[702016]

Berichtdauer anpassen

Sie können jetzt den Schieberegler verwenden, um die Dauer der Berichte anzupassen, die auf der Citrix ADM-GUI generiert werden. Zuvor konnten Sie Berichte für eine Stunde, einen Tag, eine Woche oder einen Monat erstellen und anzeigen. Weitere Informationen finden Sie unter Netzwerkberichterstattung.

[666018]

Neue Netzwerkberichte

Sie können jetzt Leistungsberichte für jede Schnittstelle der ausgewählten Citrix ADC-Instanz generieren und exportieren. Die erfassten Performance-Daten basieren auf den ausgewählten Leistungsindikatoren und den von der Citrix ADC-Instanz übertragenen und empfangenen Daten. Weitere Informationen finden Sie unter Netzwerkberichterstattung.

[683417]

Sie können jetzt Berichte für ausgewählte Citrix ADC-Instanzen für Durchsatz und Bandbreite generieren. Mithilfe der generierten Durchsatzberichte können Sie Netzwerkberichtsdaten für jede einzelne Instanz im Network Reporting-Dashboard überwachen. Weitere Informationen finden Sie unter Netzwerkberichterstattung.

[687555]

Bereitstellen von Oracle e-Business Suite auf Citrix ADC-Instanzen mit StyleBook

Mit StyleBooks können Sie nun den Load Balancing-Bereitstellungsprozess für Oracle E-Business Suite 12.2 mit Citrix ADC definieren. Die Konfiguration des Lastenausgleichs besteht in der Definition von

virtuellen Servern und Services mit Lastenausgleich, die mit den virtuellen LB-Servern verbunden und an die einzelnen Oracle E-Business Suite-Server gebunden sind. Weitere Informationen finden Sie unter Oracle e-business StyleBook.

[679553]

Integrieren von StyleBooks in das Anwendungs-Dashboard zum Erstellen von Konfigurationen auf Citrix ADC-Instanzen

Mit Citrix ADM können Sie nun benutzerdefinierte Anwendungen mithilfe von Standard- oder benutzerdefinierten StyleBooks erstellen. StyleBooks vereinfachen die Verwaltung komplexer Citrix ADC Konfigurationen für Ihre Anwendungen. Wenn Sie benutzerdefinierte Anwendungen auf der Anwendungs-Dashboardseite definieren, können Sie nun ein StyleBook auswählen, das in Citrix ADM vorhanden ist. Citrix ADM erstellt dann die Konfiguration auf den Citrix ADC Zielinstanzen basierend auf dem ausgewählten StyleBook. Citrix ADM erstellt auch eine benutzerdefinierte Anwendung, die aus allen virtuellen Servern im Config Pack besteht.

> **Hinweis**
>
> Ein benutzerdefiniertes Anwendungs- und Konfigurationspaket wird erstellt, wenn genügend Citrix ADM-Lizenzen verfügbar sind und die virtuelle Serverlizenzierung nicht auf manuell eingestellt ist. Weitere Informationen finden Sie unter Erstellen einer Anwendungsdefinition.

[684460]

Möglichkeit, vorhandene Konfigurationspakete auf ein anderes StyleBook zu migrieren

Mit Citrix ADM können Sie Ihr Konfigurationspaket jetzt auf ein neues StyleBook migrieren (oder aktualisieren), ohne das Konfigurationspaket zu entfernen und neu zu erstellen. Mit dieser Funktion können Sie alle Konfigurationen auf den Zielinstanzen beibehalten.

Beachten Sie, dass die Parameter des neuen StyleBook eine Obermenge der Parameter im vorhandenen StyleBook sind. Dann kann Citrix ADM Ihr Config Pack auf das neue StyleBook migrieren, ohne dass Sie Parameterwerte erneut eingeben müssen.

> **Hinweis**
>
> Hierbei wird davon ausgegangen, dass alle neuen Parameter, die Teil des neuen StyleBook sind, optional sind.

Während der Migration führt Citrix ADM eine Konfigurationsabfrage zwischen der vorhandenen Konfiguration und der neuen Konfiguration durch, die vom neuen StyleBook generiert wird. Citrix ADM entscheidet dann, welche Konfigurationsobjekte für die Citrix ADC Zielinstanzen hinzugefügt, entfernt oder aktualisiert werden müssen.

Es gibt keine Einschränkung für die Migration Ihres Config-Pakets zwischen zwei beliebigen StyleBooks in Citrix ADM. Sie können das migrierte Konfigurationspaket auch auf das vorherige StyleBook zurücksetzen. Weitere Informationen finden Sie unter Migrieren des Konfigurationspakets eines StyleBook auf ein anderes StyleBook.

[699789]

Anzeigen der Regelkennung der Signatur im Security Insight-Bericht

Der Security Insight-Bericht für Signaturverletzungen enthält jetzt die Regelkennung jeder Signatur.

Weitere Informationen finden Sie unter Sicherheitshinweise.

[701416]

Behobene Probleme

Analytics

- Erhöhte NITRO -Aufrufe führen dazu, dass Citrix ADM nicht mehr reagiert.
  [696032]

Netzwerke

- Citrix ADM zeigt die Anzahl der Backupdateien auf der Seite Systemsicherungseinstellungen nicht an.
  [703421]
- Vor der Übermittlung wird eine Eingabeaufforderung angezeigt, wenn unter **Netzwerke** > **Lizenzeinstellungen** > **Systemlizenzen** mehr als zulässige virtuelle Server ausgewählt sind.
  [687058]

Bekannte Probleme

Netzwerke

- Wenn Sie in Citrix ADM zu Netzwerke > Ereignisse > Syslog-Nachrichten navigieren, werden zuerst die ältesten Nachrichten angezeigt. Im Fenster Sortieren wird jedoch die Option Neueste zuerst angezeigt. Erst wenn Sie Älteste zuerst auswählen und dann Neueste zuerst auswählen, werden die Meldungen korrekt angezeigt.
  [702305]

Analytics

- In bestimmten Fällen werden HDX Insight - und Citrix Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut.
  [690327]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen.
  [689330]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt.
  [686581]
- Citrix SD-WAN WO oder Citrix ADC SDX-Instanzen können nicht von Citrix ADM aktualisiert werden.
  [699814]

GUI-Problem

- Die Citrix Cloud-Navigationsleiste ist nicht sichtbar, wenn Sie sich mit Internet Explorer 11 anmelden.
  [702339]

9. Februar 2018

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf den Build 509.119 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neue Features

Verbesserungen des Anwendungs-Dashboards

In der Citrix ADM GUI wurden die folgenden Änderungen vorgenommen, um die Benutzerfreundlichkeit des Anwendungs-Dashboards zu verbessern:

1. Die Bewertung der *0 App* stellt die Anzahl der virtuellen Anwendungsserver dar, die ausgefallen sind oder außer Betrieb sind. Diese *0 App-Score* ist jetzt Teil der vorhandenen App-Score-Legende in der Dashboard-Ansicht der Anwendung.
2. Im Zusammenfassungsfenster der App wird nun der Text *Anzeigen von N/N Apps* anstelle des früheren *Gesamtzahl der Apps N/N* angezeigt. Betrachten Sie ein Beispiel, in dem Sie 60 im App-Score-Diagramm auswählen. Es gibt 16 Anwendungen von insgesamt 26 Anwendungen, die eine App-Score zwischen 40 und 60 haben. Das App-Zusammenfassungsfeld wird angezeigt *Anzeigen 16/26 Apps*. Wenn keine Kriterien ausgewählt sind, wird im Zusammenfassungsfenster der App *Anzeigen 26/26 Apps*angezeigt.
3. Das App-Zusammenfassungsfenster zeigt nun ein neues Diagramm an, um Anwendungen basierend auf den entsprechenden Kategorien zu filtern. Ein neues Anwendungskategoriediagramm wird dem App-Zusammenfassungsfenster hinzugefügt. Dieses Diagramm zeigt ein Histogramm für alle in Citrix ADM definierten Kategorien an. Alle diskreten Anwendungen werden nun unter der Kategorie *Andere* angezeigt, und benutzerdefinierte Anwendungen werden unter ihren jeweiligen Kategorienamen angezeigt. Diese Kategorienamen werden beim Definieren benutzerdefinierter Anwendungen zugewiesen.

Weitere Informationen finden Sie unter Anwendungsanalyse und -verwaltung.

[695980]

Möglichkeit zum Auswählen des Lastausgleichszustands des virtuellen Servers und des prozentualen Zustands als Parameter zum Filtern von Anwendungen

Im Integritätsbalkendiagramm des virtuellen Servers klassifiziert Citrix ADM Anwendungen basierend auf dem Prozentsatz der Integrität des virtuellen Servers. Das Balkendiagramm zeigt die Anzahl der Anwendungen an, die gruppiert sind, um den Integritätswert zwischen 0% und 100% zu haben.

Die Integrität virtueller Server stellt die Integrität virtueller Server dar, die unter diskreten Anwendungen gruppiert sind. Wenn es jedoch benutzerdefinierte Anwendungen gibt, die zwei oder mehr virtuelle Server umfassen, wird die geringste Virtual Server Integrität in der Gruppe berücksichtigt.

Sie können nun einen Filter anwenden und nur die Anwendungen im Anwendungs-Dashboard anzeigen, die den Auswahlkriterien entsprechen.

Weitere Informationen finden Sie unter Anwendungsanalyse und -verwaltung.

[694425]

Integrierter Citrix ADM Agent in einer Citrix ADC-Instanz

Citrix ADC-Instanzen, auf denen Version 12.0 Build 56.20 und höher ausgeführt wird, enthalten einen integrierten Citrix ADM Agent. Dieser Agent ermöglicht die Kommunikation zwischen der Instanz und Citrix ADM. Sie müssen keinen externen Agent installieren.

Die Verwaltungs-, Überwachungs- und Anwendungs-Dashboard-Funktionen werden für Citrix ADC-Instanzen mit integrierten Agents unterstützt. Die folgenden Features werden nicht unterstützt: Web Insight, SSL Insight, HDX Insight, Citrix Gateway Insight, Security Insight und Intelligent App Analytics.

Um diesen integrierten Agenten verwenden zu können, müssen Sie Ihre Citrix ADC-Instanz auf Version 12.0 Build 56.20 aktualisieren und den Agenten initiieren.

> **Hinweis:**Der
>
> integrierte Agent ist nur für die folgenden Citrix ADC-Instanztypen verfügbar:
>
> - Citrix ADC MPX-Appliance
> - Citrix ADC VPX Appliance
> - Citrix Gateway
> - Citrix Secure Web Gateway

Weitere Informationen und Anweisungen zur Verwendung des integrierten Agenten finden Sie in den folgenden Artikeln:

- Erste Schritte mit Citrix ADM
- Initiieren des integrierten Agenten

[694701]

Unterstützung für Web Insight

Citrix ADM unterstützt jetzt Web Insight. Die Web Insight-Funktion bietet Einblick in Unternehmens-Webanwendungen. Es ermöglicht IT-Administratoren, alle vom Citrix ADC bereitgestellten Webanwendungen zu überwachen, indem sie integrierte und Echtzeitüberwachung von Anwendungen bereitstellen. Weitere Informationen finden Sie unter Web Insight.

Web Insight verarbeitet Daten von Citrix ADC unter Verwendung eines Approximationsalgorithmus. Es bietet die 1.000 besten Datensätze der Metriken, die mit den Webanwendungen in Ihrem Unternehmen zusammenhängen.

[688206]

Unterstützung für SSL-Einblicke

Citrix ADM unterstützt jetzt SSL Insight. Die SSL-Insight-Funktion bietet Einblick in sichere Transaktionen im Web (HTTPs). Es ermöglicht IT-Administratoren, alle vom Citrix ADC bereitgestellten Webanwendungen zu überwachen, indem sie eine integrierte Echtzeit- und historische Überwachung von Web-Transaktionen bereitstellen. Weitere Informationen finden Sie unter SSL Insight.

SSL Insight verarbeitet Daten aus Citrix ADC unter Verwendung eines Approximationsalgorithmus. Es bietet die 1.000 besten Datensätze der Metriken, die mit den Web-Transaktionen in Ihrem Unternehmen zusammenhängen.

[688206]

Unterstützung für SAML-Authentifizierungseinträge in Citrix Gateway Insight

Citrix Gateway Insight bietet jetzt Einblicke in SAML-Authentifizierungsfehler. Sie können die SAML-Authentifizierungsfehler auf der Registerkarte **Authentifizierung** auf der Seite **Analytics > Citrix Gateway Insight > Übersicht** anzeigen.

[634094]

Möglichkeit zum Hinzufügen von Citrix ADC-Instanzen zu Standorten durch Bereitstellung von Standortinformationen

Mit Citrix ADM können Sie jetzt Citrix ADC-Instanzen hinzufügen und Sites zuordnen. Beim Erkennen einer Instanz können Sie entweder eine Site erstellen oder eine vorhandene Site auswählen. Geben Sie die Citrix ADM Agent-Details an, und ordnen Sie den Agenten immer mit der Site zu.

So fügen Sie eine Instanzhinzu:

1. Navigieren Sie zu **Netzwerke** > **Instanzen**.
2. Wählen Sie den Typ der Citrix ADC-Instanz aus, und klicken Sie auf **Hinzufügen**.
3. Geben Sie die IP-Adresse ein und wählen Sie das Profil aus.
4. Wählen Sie die Site und den Agenten aus.
5. Klicken Sie auf das Symbol Bearbeiten neben dem Feld Agent.
6. Wählen Sie den Agenten aus, und klicken Sie auf **Site anhängen**, und wählen Sie die gewünschte Site aus.
7. Klicken Sie auf **OK**.

Die Instanz ist nun mit der Site verknüpft. Navigieren Sie zum Netzwerk-Dashboard, um die neu hinzugefügten Instanzen unter der zugeordneten Site anzuzeigen.

Weitere Informationen finden Sie unter So überwachen Sie global verteilte Standorte.

[702019]

Möglichkeit, Citrix ADC-Instanzen mit derselben privaten IP-Adresse zu erkennen

Sie können jetzt Citrix ADC-Instanzen mit denselben privaten IP-Adressen in verschiedenen Netzwerken erkennen, wenn Instanzen mithilfe des integrierten Agents mit Citrix ADM registriert werden.

[699962]

Behobene Probleme

Netzwerke

- Falsche Werte für DH (Diffie-Hellman) und Ephemeral RSA-Schlüssel werden angezeigt, wenn ein SSL-Profil mit unterschiedlichen Eigenschaften an einen virtuellen SSL-Server angeschlossen ist. Werte werden nur für virtuelle SSL-Server-IPs korrekt angezeigt, die kein SSL-Profil haben.
  [702680]
- Doppelte Dienst- oder Dienstgruppeneinträge werden für den Dienst oder die Dienstgruppe jeder Partition nach einem Citrix ADC Failover angezeigt. Dieses Problem tritt nicht bei Diensten oder Dienstgruppen auf, die zur Standardpartition gehören.
  [699224]

Bekannte Probleme

Analytics

- In bestimmten Fällen werden HDX Insight - und Citrix Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut.
  [690327]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen.
  [689330]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt.
  [686581]
- Citrix SD-WAN WO oder Citrix ADC SDX-Instanzen können nicht von Citrix ADM aktualisiert werden.
  [699814]

GUI-Problem

- Die Citrix Cloud-Navigationsleiste ist nicht sichtbar, wenn Sie sich mit Internet Explorer 11 anmelden.
  [702339]

18. Januar 2018

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf den Build 508.116 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neuigkeiten

Importieren eines Zertifikats aus einer bestimmten Citrix ADC-Instanz

Sie können nun ein Zertifikat aus einer bestimmten Citrix ADC-Instanz importieren und es auf andere zielgerichtete Citrix ADC-Instanzen von der Citrix ADM GUI anwenden. Mit dieser Erweiterung müssen Sie das Zertifikat nicht auf Ihr lokales System herunterladen und dann das heruntergeladene Zertifikat auf die ausgewählten Instanzen anwenden. Weitere Informationen finden Sie unter Installieren von SSL-Zertifikaten auf einer Citrix ADC-Instanz.

[688029]

Anzeigen von Netzwerkberichten für mehrere Citrix ADC-Instanzen

Mit Citrix ADM können Sie mehrere Citrix ADC-Instanzen (und bis zu fünf virtuelle Server) auswählen, während Sie einen Netzwerkbericht erstellen. Sie können jetzt Netzwerkberichtsdaten für mehrere Instanzen gleichzeitig überwachen.

Sie können den Bericht auch exportieren und planen, der über die **Netzwerkberichterstattungsfunktion** im Citrix ADM generiert wurde. Weitere Informationen finden Sie unter Netzwerkberichterstattung.

[665989]

Upgrade der Citrix ADC-Instanz im Hochverfügbarkeitsmodus

Das Upgrade Ihrer Citrix ADC-Instanzen im Hochverfügbarkeitsmodus von Citrix ADM wurde verbessert. Sie können eine Wartungsaufgabe erstellen, um das HA-Paar in zwei Stufen zu aktualisieren. Sie können das Upgrade zunächst auf dem anfänglichen Knoten planen oder durchführen und später das Upgrade für den zweiten Knoten planen. Der Administrator kann mit dem Upgrade des zweiten Knotens nur fortfahren, wenn das Upgrade des ersten Knotens erfolgreich ist.

> **Hinweis**
>
> - Derzeit wird der zweite Knoten des HA-Paares zuerst aktualisiert, und das Upgrade für den ersten Knoten wird später geplant.
> - Synchronisation und Weitergabe der Knoten werden deaktiviert, bis beide Knoten erfolgreich aktualisiert wurden.
> - Es wird eine Warnung angezeigt, wenn sich die Knoten im HA-Paar auf verschiedenen

> Builds oder Versionen befinden, wenn der erste Knoten aktualisiert wird. Sie können den Upgrade-Prozess für den zweiten Knoten abbrechen, bis er sich im gleichen Build und Version befindet. Oder Sie können es für einen späteren Zeitpunkt planen, nachdem sich die Knoten im gleichen Build und Version befinden.

Weitere Informationen finden Sie unter Upgrade von Citrix ADC-Instanzen.

[694907]

Anzeigen gebundener Entitäten für Server

Sie können nun die gebundenen Entitäten auf Ihren verwalteten Citrix ADC-Instanzen für einen bestimmten Server anzeigen. Sie können nun Folgendes sehen:

1. Sie können nun die gebundenen Dienste und gebundenen Dienstgruppen für einen ausgewählten Lastenausgleichsserver anzeigen.

   Navigieren Sie zu **Netzwerke** > **Netzwerkfunktionen** > **Lastausgleich** > **Server**. Wählen Sie einen Server aus, und klicken Sie auf **Gebundene Diensteanzeigen oder Gebundene Dienstgruppen** anzeigen. Auf der Seite Gebundene Dienste können Sie den Dienst aktivieren oder deaktivieren und die Entität abfragen. Ebenso können Sie auf der Seite Gebundene Dienstgruppen die Dienstgruppe aktivieren oder deaktivieren, die gebundenen Dienstgruppenmitglieder anzeigen und die Entität abfragen.

2. Sie können die gebundenen virtuellen LB-Server für einen Server auf einem virtuellen Content Switching-Server anzeigen.

   Navigieren Sie zu **Netzwerke** > **Netzwerkfunktionen** > **Content Switching**. Wählen Sie einen Server aus, und klicken Sie auf **Gebundene LB Virtuelle Server anzeigen**. Auf der Seite Gebundene LB-Server können Sie den virtuellen Server entweder aktivieren oder deaktivieren und abfragen.

   > **Hinweis:** Wenn Sie einen virtuellen Content Switching-Server auswählen und auf **Bound LB Virtual Server anzeigen** klicken. Citrix ADM listet den standardmäßigen LB-Server und den richtlinienbasierten virtuellen Ziel-LB-Server auf.

3. Sie können die gebundenen virtuellen Ziel-LB-Server für einen Server auf einem virtuellen Cache-Umleitungsserver anzeigen.

   Navigieren Sie zu **Netzwerke** > **Netzwerkfunktionen** > **Cache-Umleitung**. Auf der Seite **Virtuelle Server der Cache-Umleitung wird eine neue Spalte Virtueller Ziel-LB** angezeigt, die den Namen des virtuellen Zielservers für LB auflistet.

[698772]

Durchsatzdetails für lizenzierte virtuelle Server anzeigen

Sie können Ihren virtuellen Servern Lizenzen basierend auf den Durchsatzdetails verwalten und zuweisen (d. h. der Summe der Anforderungsbytes und Antwortbytes). Dies wird als Spalte auf der Seite **Systemlizenzen** angezeigt. Sie können die Spalte **Durchsatz** sortieren, um zu sehen, welcher virtuelle Server weniger oder mehr Durchsatzauslastung hat, und Lizenzen entsprechend zuweisen.

So zeigen Sie Durchsatzdetails an:

1. Navigieren Sie zu **Netzwerke** > **Lizenzen** > **Systemlizenzen**.
2. Stellen Sie auf der Seite **Systemlizenzen** unter **Verwaltete virtuelle Server** sicher, dass die Option zum **automatischen Auswählen virtueller Serverdeaktiviert** ist. Sie können nun die virtuellen Server, die Sie verwalten möchten, explizit auswählen.
3. Wählen Sie zum Auswählen von virtuellen Servern **Klicken Sie zum Auswählen**auf.
4. Auf der Seite **Virtuelle Server auswählen** können Sie nun die Durchsatzdetails als Spalte unter jedem virtuellen Server anzeigen.

[687056]

Neuer Konfigurationsfluss zum Einrichten von Agents und Hinzufügen von Citrix ADC-Instanzen

Citrix ADM bietet jetzt eine neue intuitive Benutzeroberfläche zum Einrichten von Citrix ADM Agents und zum Hinzufügen von Citrix ADC-Instanzen zu Citrix ADM. Weitere Informationen finden Sie unter Schnelleinstieg.

[700033]

Python SDK-Unterstützung für StyleBooks

In Citrix ADM unterstützt das Python SDK jetzt NITRO-Aufrufe für StyleBooks.

[672420]

Weitere Informationen zu Citrix ADC-Instanzen anzeigen

Sie können jetzt Informationen zu den folgenden Parametern der Citrix ADC-Instanz auf Citrix ADM anzeigen.

- **Modell-ID**: Zeigt die Modell-ID an, die vom Lizenztyp abgeleitet wird, der auf eine Citrix ADC-Instanz angewendet wird. Sie können die Modell-ID auf der Seite Instanzen und im Instanz-Dashboard anzeigen.
- **Host-ID**: Zeigt die Host-ID an, bei der es sich um die Mac-ID einer Citrix ADC-Instanz handelt. Die Host-ID wird verwendet, um die Lizenz für die Instanz zu generieren. Sie können die Host-ID auf der Seite Instanzen und im Instanz-Dashboard anzeigen.

- **NetScaler UUID**: Universally Unique Identifier (UUID), die eindeutige Internetgeräte oder Daten identifiziert. Ein Algorithmus generiert die UUID anhand von Werten, die auf der Netzwerkadresse der Instanz basieren. Sie können die NetScaler UUID im Instanz-Dashboard anzeigen.
- **CPU**: Zeigt die aktuelle Frequenz der CPU an. Die CPUs arbeiten je nach Belastbarkeit mit unterschiedlichen Frequenzen. Die Zunahme/Abnahme von MHz wird durch CPU, Motherboard-Architektur und Temperatur bestimmt. Sie können die CPU-Auslastungsdetails im Instanz-Dashboard anzeigen.
- **Hergestellt am**: Zeigt das Herstellungsdatum einer Citrix ADC-Instanz im Instanz Dashboard an.

> **Hinweis** Standardmäßig werden die Modell-ID und die Host-ID einer Instanz nicht auf der Seite Instanz angezeigt.

So zeigen Sie die neuen Parameter an:

1. Navigieren Sie zu **Netzwerke** > **Instanzen**, und wählen Sie den Typ der Citrix ADC-Instanz aus, für die Sie die Parameterinformationen anzeigen möchten.
2. So zeigen Sie die Modell-ID und die Host-ID an:
   a) Klicken Sie oben rechts auf das Symbol **Einstellungen** neben **Suchen**.
   b) Wählen Sie Modell-ID und Host-ID aus, und klicken Sie auf **Fertig**.
   Die Model-ID- und Host-ID-Werte werden wie in der folgenden Abbildung dargestellt angezeigt.
   c) So zeigen Sie Host-ID, NetScaler UUID, CPU und Herstellungsdatum auf dem Dashboard an:
      i. Wählen Sie die Instanz aus, und klicken Sie auf **Dashboard**.
      ii. Im Abschnitt **Informationen** können Sie die Details von **Model ID**, **Host ID**, **NetScaler UUID**, **CPU** und **Manufactured on** anzeigen, wie in der folgenden Abbildung dargestellt.

[699550, 700266]

Behobene Probleme

Analytics

- Beim Zugriff auf Sitzungsberichte in HDX Insight schlägt Citrix ADM zeitweise fehl. [701042]

Netzwerke

- Wenn Geräte-API-Proxy-Anforderungen an Citrix ADM gesendet werden, gibt es die Content-Length und Transfer-Encoding im Antwort-Header zurück, was im Widerspruch zu RFC 2616 steht. [700717]
- Derzeit werden Berechtigungen für einige abhängige Ressourcen (ns_lbvserver, ns_csvserver usw.) als Teil der Netzwerkberichterstattungsberechtigung erteilt. Im Rahmen der neuen Erweiterung müssen diese Berechtigungen jedoch nur gewährt werden, wenn Benutzer unter Netzwerkfunktionen Zugriff auf den entsprechenden Knoten haben. Wenn Benutzer beispielsweise die Berichterstellung auf virtuellen Lastenausgleichsservern ausführen möchten, müssen sie nur Zugriff auf die virtuellen Load Balancing-Server unter Netzwerkfunktionen haben und umgekehrt.
  [700859]

Bekannte Probleme

Analytics

- In bestimmten Fällen werden HDX Insight - und Citrix Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut.
  [690327]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen.
  [689330]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt.
  [686581]
- Citrix SD-WAN WO oder Citrix ADC SDX-Instanzen können nicht von Citrix ADM aktualisiert werden.
  [699814]

28. Dezember 2017

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf den Build 507.114 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neuigkeiten

Konfigurieren von Zugriffsrichtlinien für RBAC auf Citrix ADM für Netzwerkfunktions-Unterknoten

Mit der Zugriffsrichtlinienverwaltung für rollenbasierte Zugriffssteuerung (RBAC) in Citrix ADM können Sie jetzt auch Berechtigungen für Netzwerkfunktions-Unterknoten konfigurieren. Zugriffsrichtlinieneinstellungen können für alle Unterknoten wie virtuelle Server, Dienste, Dienstgruppen und Server konfiguriert werden. Derzeit können Sie eine solche granulare Zugriffsberechtigung nur für Unterknoten unter Lastenausgleichsknoten und auch für Unterknoten unter GSLB-Knoten bereitstellen. Weitere Informationen finden Sie unter Konfigurieren von Zugriffsrichtlinien für Citrix Application Delivery Management.

[692034]

Möglichkeit zum Exportieren und Planen von Berichten für ausgewählte Netzwerkfunktionen

Sie können einen umfassenden Bericht für ausgewählte Netzwerkfunktionen wie Load Balancing, Content Switching, Cache-Umleitung, Global Server Load Balancing (GSLB), Authentication und Citrix Gateway in Citrix ADM erstellen. Dieser Bericht ermöglicht Ihnen eine übergeordnete Ansicht der Zuordnung zwischen den Citrix ADC-Instanzen, Partitionen und den entsprechenden gebundenen Entitäten (virtuelle Server, Dienstgruppen und Dienste), die im Netzwerk vorhanden sind. Sie können diese Berichte im CSV-Dateiformat exportieren.

Der Bericht zeigt die folgenden virtuellen Serverdaten an:

- NetScaler-IP-Adresse
- Hostname
- Partitionsdaten
- Typ des virtuellen Servers
- Name des virtuellen Servers
- Virtueller Zielserver für LB
- Dienstname
- Name der Dienstgruppe.

Weitere Informationen finden Sie unter Exportieren oder Planen des Exports von Netzwerkfunktionenberichten.

[696259]

Importieren von StyleBooks mit Dateien oder ZIP-Paketen

Mit Citrix ADM können Sie mehrere StyleBooks im YAML-Format importieren. Sie können mehrere YAML StyleBook-Dateien im Zip- (.zip) -Format oder Tarball-Format (.tgz,.gz) komprimieren. Weitere Informationen finden Sie unter So verwenden Sie benutzerdefinierte StyleBooks.

[694938]

Ausschließen von Standard-Citrix ADC Zertifikaten im SSL-Dashboard

Mit Citrix ADM können Sie standardmäßige Citrix ADC Zertifikate anzeigen oder ausblenden, die auf den SSL-Dashboard-Diagrammen basierend auf Ihren Einstellungen angezeigt werden. So blenden Sie Standardzertifikate auf dem SSL-Dashboard ein oder aus:

1. Navigieren Sie zu **Netzwerke** > **SSL-Dashboard** in der Citrix ADM GUI.
2. Klicken Sie auf der Seite **SSL-Dashboard** auf **Einstellungen**.
3. Klicken Sie auf der Seite **Einstellungen** auf das Symbol Bearbeiten.
4. Deaktivieren Sie im Abschnitt **Zertifikatfiltereinstellungen** das Kontrollkästchen **Standardzertifikate anzeigen**.

Weitere Informationen finden Sie unter Ausschließen von standardmäßigen Citrix ADC Zertifikaten im SSL-Dashboard.

[687609]

Behobene Probleme

Netzwerke

- Um einen Konfigurationsauftrag mit benutzerdefinierten Vorlagen aus der Vorlagenliste zu erstellen, müssen Sie die Vorlagen in den Editor ziehen und die Variablen bearbeiten, indem Sie neue Werte angeben. Wenn der Konfigurationsauftrag jedoch ausgeführt wird, werden die Variablen nicht durch die von Ihnen bereitgestellten neuen Werte ersetzt. [698812]
- Wenn in Citrix ADM Ereignisalter in einer Regel für ein Ereignis festgelegt ist, werden diese Ereignisse in der GUI nicht angezeigt. Da die EntityUp-, EntityDown- und EntityOFs-Entity korreliert sind, müssen sie für dasselbe Ereignis aktualisiert werden. Aber diese Fallen werden separat in Ereignismeldungen gesehen. [699487]
- Wenn Citrix ADM die HDX Insight Berichte exportiert, ist der Wert der Kanalbandbreite nicht korrekt. [700011]
- Citrix ADM zeigt in Ereignissen eine Meldung an, die immer besagt, dass die Lizenzen in den nächsten 30 Tagen ablaufen, obwohl die Lizenzen möglicherweise früher ablaufen. [696976]

Bekannte Probleme

Analytics

- In bestimmten Fällen werden HDX Insight - und Citrix Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.

Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut. [690327]

Netzwerke

- Derzeit(`ns\\_lbvserver,ns\\_csvserver etc`) werden Berechtigungen für einige abhängige Ressourcen als Teil der Berechtigung für die Network Reporting-Funktion erteilt. Im Rahmen der neuen Erweiterung müssen diese Berechtigungen jedoch nur gewährt werden, wenn Benutzer unter Netzwerkfunktionen Zugriff auf den entsprechenden Knoten haben. Wenn Benutzer beispielsweise die Berichterstellung auf virtuellen Lastenausgleichsservern ausführen möchten, müssen sie nur Zugriff auf die virtuellen Load Balancing-Server unter Netzwerkfunktionen haben und umgekehrt. [700859]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen. [689330]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]
- Citrix SD-WAN WO oder Citrix ADC SDX-Instanzen können nicht von Citrix ADM 506.119 Build aktualisiert werden. [699814]

07. Dezember 2017

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf den Build 506.122 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neuigkeiten

Erweiterungen des Multicloud GLB StyleBook zur Unterstützung der Eltern-Kind-Bereitstellung und statistikbasierten GLB-Algorithmen

Die GLB-Lösung (Global Load Balancing) ermöglicht Benutzern die Verteilung der Clientanforderungen auf mehrere Rechenzentren und Anwendungsserver. Die Rechenzentren sind auf mehrere Clouds verteilt und die Anwendungsserver werden on-premises bereitgestellt. Diese Lösung unterstützt die folgenden Funktionen:

- Topologie mit über- und untergeordneten Elementen. Die Topologie wird verwendet, wenn statistische GLB-Algorithmen verwendet werden, um GLB- und LB-Knoten zu konfigurieren. Diese Topologie wird auch verwendet, wenn die LB-Knoten auf einer anderen Citrix ADC-Instanz bereitgestellt werden.

- Spilloverpersistenz. Der virtuelle Sicherungsserver verarbeitet die empfangenen Anforderungen weiterhin, auch wenn die Last auf dem primären Schwellenwert unterschritten wird.
- Internet Protocol Version 6 (IPv6).
- Metrikbasierte, nicht-metrische und proximitätsbasierte GLB-Methoden.

Verwenden Sie das "Multi-Cloud GLB StyleBook", Version 1.1, um die GLB-Konfiguration auf der ausgewählten GLB Citrix ADC-Instanz auszuführen. Verwenden Sie das Multi-Cloud GLB StyleBook for LB Node, um jeweils einen LB-Knoten für die Erstellung der GLB-Topologie in einem der folgenden Fälle zu konfigurieren:

- Wenn Sie die metricbasierten GLB-Algorithmen (Kleinste Pakete, geringste Verbindungen, geringste Bandbreite) verwenden, um GLB- und LB-Knoten zu konfigurieren
- Wenn die LB-Knoten auf einer anderen Citrix ADC-Instanz bereitgestellt werden
- Wenn Sie die Standortpersistenz konfigurieren möchten

Sie können bis zu 1024 untergeordnete Sites konfigurieren.

Weitere Informationen finden Sie unter Globaler Citrix ADC Lastenausgleich für Hybrid- und Multi-Cloud-Bereitstellungen.

[694250]

RBAC-Unterstützung für StyleBooks beim Erstellen von Gruppen

Mit Citrix ADM können Sie ausgewählte StyleBooks hinzufügen, auf die Ihr Benutzer beim Erstellen von Benutzergruppen zugreifen kann.

So fügen Sie ausgewählte StyleBooks zu Gruppen hinzu:

1. Navigieren Sie in Citrix ADM zu **System** > **Benutzerverwaltung** > **Gruppen**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Gruppenname** den Namen der Gruppe ein, und wählen Sie die gewünschte Rolle aus.
4. Deaktivieren Sie auf der Registerkarte **Anwendungen und Vorlagen** das Kontrollkästchen StyleBooks und wählen Sie die erforderlichen StyleBooks aus, auf die Ihr Benutzer zugreifen kann.
5. **Wählen Sie auf der Registerkarte Benutzer** auswählen die Benutzer aus, die der Gruppe hinzugefügt werden sollen.
6. Klicken Sie auf **Fertig stellen**.

Weitere Informationen finden Sie unter Konfigurieren von Gruppen in Citrix Application Delivery Management.

[657834, 664844]

Beschreibung für Gruppen bereitstellen

Wenn Sie in Citrix ADM Gruppen erstellen, können Sie jetzt im Feld Gruppenbeschreibung eine **Beschreibung Ihrer Gruppe** eingeben. Geben Sie eine gute Beschreibung der Gruppe an. Eine gute Beschreibung hilft Ihnen, die Rolle und Funktion der Gruppe zu einem späteren Zeitpunkt besser zu verstehen. Weitere Informationen finden Sie unter Konfigurieren von Gruppen in Citrix Application Delivery Management.

[685186]

Integration von Citrix ADM Intelligent App Analytics

Die Intelligent App Analytics-Funktion von Citrix ADM überwacht die für eine Anwendung konfigurierten virtuellen Server und Dienste und zeigt kritische Informationen über diese an. Diese Funktion unterstützt Sie bei der Überwachung, Verwaltung und Entscheidungsfindung bei Ausfällen und anderen Ereignissen. Einige Schlüsselfunktionen von Intelligent App Analytics sind wie folgt aufgeführt:

- Nutzt maschinelles Lernen Algorithmen
- Ermittelt das Traffic-Verhalten
- Unterscheidet zwischen akzeptablen und inakzeptablen Mustern
- Vermittelt klare Einblicke für Administratoren
- Ermöglicht Administratoren, geeignete Maßnahmen zu ergreifen

Weitere Informationen finden Sie unter Intelligente App Analytics.

[698730]

Citrix ADM Agent automatisch in AWS bei Citrix ADM registrieren

Sie können den Citrix ADM-Agent jetzt automatisch bei Citrix ADM registrieren, indem Sie die Service-URL und den Aktivierungscode von Citrix ADM angeben, während Sie den Citrix ADM-Agent in Amazon Web Service (AWS) bereitstellen. Weitere Informationen finden Sie unter Installieren von Citrix ADM Agent in AWS.

[688901]

Konfigurationsüberwachung, wenn Citrix ADM ChangeConfig SNMP-Trap empfängt

Wenn eine Konfigurationsänderung in einer Citrix ADC-Instanz im Netzwerk stattfindet, aktualisiert die Instanz die Konfiguration. Die Instanz sendet dann ein ConfigChange-SNMP-Trap an Citrix ADM. Sie können Citrix ADM aktivieren, um die Konfigurationsüberwachung für diese Instanz auszuführen. Sie können Citrix ADM so konfigurieren, dass bei jedem Empfang eines ConfigChange-SNMP-Traps ein Konfigurationsüberwachungsdiff generiert wird. Weitere Informationen finden Sie unter Generieren von Konfigurationsüberwachungs-Diff für ConfigChange SNMP-Traps.

[682007]

Unterstützung bei der Planung der Wartungsaufgaben

Mit Citrix ADM können Sie jetzt alle folgenden Wartungsaufgaben zu einem bestimmten Datum und einer bestimmten Uhrzeit planen.

- Upgrade von Citrix ADC-Instanzen
- Upgrade von Citrix SD WAN-WO-Instanzen
- Upgrade von Citrix ADC SDX-Instanzen
- Konfigurieren des HA-Paares von Citrix ADC-Instanzen
- Konvertieren von HA-Instanzen in Cluster

Sie können auch die E-Mail-Benachrichtigung während der Planung der Wartungsaufgabe konfigurieren. Nach der Konfiguration wird jedes Mal eine E-Mail-Benachrichtigung gesendet, wenn ein Auftrag ausgeführt oder geplant wird.

[681934]

Integrierter YAML Viewer/Editor zum Anzeigen/Erstellen von StyleBook-Definitionen

Citrix ADM bietet Ihnen einen integrierten YAML-Editor, mit dem Sie Ihr StyleBook erstellen können, das den YAML-Richtlinien entspricht. Der Inhalt wird nach YAML-Standards validiert und jede Abweichung wird hervorgehoben. Anschließend können Sie den Inhalt korrigieren und das StyleBook in Citrix ADM importieren. Der integrierte YAML-Editor bietet zwei Vorteile beim Schreiben Ihres eigenen StyleBook:

- Farbcodiert. Die Farbcodierung des Inhalts hilft Ihnen, leicht zwischen den Tasten und den im YAML-Inhalt definierten Werten zu unterscheiden.
- YAML-Validierung. Der Inhalt wird bei der Eingabe auf YAML-Fehler überprüft und jede Abweichung wird sofort hervorgehoben.

Weitere Informationen finden Sie unter So verwenden Sie benutzerdefinierte StyleBooks.

[695951]

Anzeigen von privaten StyleBooks in Citrix ADM GUI

Da die Anzahl der StyleBooks - sowohl öffentliche als auch private - zunimmt, benötigen Sie die Möglichkeit, nach dem bestimmten StyleBook zu suchen, auf das Sie zugreifen möchten. Sie benötigen auch die Möglichkeit, beide Arten von StyleBooks separat anzuzeigen. In Citrix ADM GUI, wenn Sie zu Anwendungen > StyleBooks navigieren, können Sie eine Liste der StyleBooks anzeigen, die im System vorhanden sind. Beide Arten von StyleBooks haben unterschiedliche Symbole, die sie als privat oder öffentlich deklarieren. Weitere Informationen finden Sie unter So zeigen Sie verschiedene Gruppen von StyleBooks an.

[686913]

HAProxy-App-Dashboard-Integration

In Citrix ADM wird die Anwendungsanalyse- und Verwaltungsfunktion auf die Unterstützung von HAProxy-Anwendungen erweitert. Das Anwendungs-Dashboard bietet eine vollständige Ansicht aller Anwendungen, die von Citrix ADM überwacht werden, d. h. sowohl Citrix ADC - als auch HAProxy-Anwendungen. HAProxy-diskrete Anwendungen werden automatisch für jedes verwaltete HAProxy-Frontend erstellt. Sie können diese Anwendungen auch gruppieren, um benutzerdefinierte Anwendungen zu erstellen, die Citrix ADC Anwendungen ähnlich sind.

> **Hinweis**
>
> App Activity Investigator ist für HAProxy-Anwendungen nicht verfügbar. Weitere Informationen finden Sie unter HAProxy-Anwendungen im Anwendungs-Dashboard.

[693309]

Exportieren von Berichten über App-Dashboard und Security Dashboard

Mit Citrix ADM können Sie die Seiten App Dashboard und Security Dashboard als Berichte exportieren.

1. Klicken Sie auf der Seite **Application Dashboard** auf das Export-Symbol oben rechts auf der Seite.
2. Wählen Sie die Exportoption entweder als PDF- oder PNG-Datei.
3. Klicken Sie auf **OK**.

Der Bericht wird auf Ihr System heruntergeladen. Derzeit können Sie Berichte zu jeweils nur einer Anwendung herunterladen. Weitere Informationen finden Sie unter Exportieren von Berichten über App-Dashboard und Sicherheits-Dashboard.

[693753]

Konfigurieren der App Score in Citrix ADM

Mit Citrix ADM können Sie App Scores konfigurieren. Die Berechnung des App-Score basiert auf den Durchschnittswerten der folgenden drei Schlüsselkomponenten:

- Performance Score (APDEX Score der Anwendung)
- Citrix ADC-Instanzressource
- Serverressource

Die App-Scores werden für alle erkannten Anwendungen und die benutzerdefinierten Anwendungen angezeigt, die Sie im Anwendungs-Dashboard definieren. Weitere Informationen finden Sie unter Analyse der Anwendungsleistung.

[693758]

Details zu Schwellenverletzungen für AppScore-Komponenten im App Activity Investigator anzeigen

Der App Activity Investigator auf der Registerkarte Dashboard zeigt wichtige Informationen einer ausgewählten Anwendung an, wie App-Score-Komponenten, Fehler, Ereignisse und Anomalien. Jede der Legenden wird im Intervall von einer Minute aggregiert, wenn die ausgewählte Dauer eine Stunde beträgt, und in einem einstündigen Intervall, wenn die ausgewählte Dauer einen Tag beträgt. Diese Abweichungen werden als rechteckige Legenden im Diagramm angezeigt. Diese Legenden werden aggregiert und werden entsprechend der Anzahl der aufgetretenen Ereignisse farbcodiert.

[693769]

Erstellen von Schwellenwerten und Konfigurieren von Regeln und Warnungen für HDX Insight

Mit der Schwellenwertverwaltung für HDX Insight in Citrix ADM können Sie Warnungen proaktiv konfigurieren, wenn die festgelegten Schwellenwerte überschritten werden. Diese Schwellenwertverwaltung wird erweitert, um eine Gruppe von Schwellenregeln zu konfigurieren und die Gruppe anstelle einzelner Regeln zu überwachen. Eine Schwellenregelgruppe besteht aus einer oder mehreren benutzerdefinierten Schwellenwertregeln für Metriken, die aus Entitäten wie Benutzern, Apps und Desktops mit einem erwarteten Wert ausgewählt wurden.

[652441]

Erstellen von Schwellenwerten und Konfigurieren von Regeln, Warnungen und Geolocations für HDX Insight

Mit der Schwellenwertverwaltung für HDX Insight in Citrix ADM können Sie Warnungen proaktiv konfigurieren, wenn die festgelegten Schwellenwerte überschritten werden. Diese Schwellenwertverwaltung wird erweitert, um eine Gruppe von Schwellenregeln zu konfigurieren und die Gruppe anstelle einzelner Regeln zu überwachen. Eine Schwellenregelgruppe besteht aus einer oder mehreren benutzerdefinierten Schwellenwertregeln für Metriken, die aus Entitäten wie Benutzern, Apps und Desktops mit einem erwarteten Wert ausgewählt wurden. Schwellenwert-Gruppen können auch an Geolokationen gebunden werden, um die geospezifische Überwachung für Benutzer-Entität zu überwachen.

[652447]

Behobene Probleme

Netzwerke

- In Citrix ADM GUI wird der Hostname der Citrix ADC-Instanz nicht auf der Detailseite des SSL-Zertifikats angezeigt. Mit diesem Fix ist der Hostname sichtbar.

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf der Seite **SSL-Dashboard** auf einen der Kreise.
3. Wählen Sie auf der Seite **SSL-Zertifikate** ein Zertifikat aus, und klicken Sie auf **Details**. [670374]

- Beim Planen der Instanzsicherungseinstellungen gibt es einen Unterschied von wenigen Stunden zwischen der geplanten Sicherungszeit und der auf der Citrix ADM GUI angezeigten Zeit. [695489]
- Wenn Sie versuchen, zwei Diagramme von der Seite Netzwerkberichte in der Citrix ADM GUI zu exportieren, wird nur das erste Diagramm als Bericht exportiert. Mit diesem Update werden alle Diagramme auf der Seite Netzwerkberichte exportiert.

  > **Hinweis**
  >
  > Die Berichte werden im PDF-, PNG- oder JPEG-Format exportiert. [699380]

- Wenn Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufgaben** navigieren und **NetScaler aktualisieren** auswählen, schlägt das Upgrade von Citrix ADC-Instanzen fehl. [692538]

Hohe Verfügbarkeit

- Die Citrix ADC-Instanzsicherung wird sowohl für primäre als auch für sekundäre Citrix ADC-Instanzen ausgelöst, wenn die Instanzen in hoher Verfügbarkeit bereitgestellt werden. [698903]
- Wenn Citrix ADC-Instanzen im HA-Setup ein Failover durchführen und wenn der neue primäre Zugriff über Citrix ADM nicht mehr möglich ist, wird die Instanz in der Citrix ADM-GUI nicht mehr angezeigt. [697017]

Einstellungen

- Wartungsaufgaben in Citrix ADM funktionieren nicht. [696952]

Bekannte Probleme

Analytics

- In bestimmten Fällen werden HDX Insight - und Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut. [690327]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen. [689330]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]
- Citrix SD-WAN WO oder Citrix ADC SDX-Instanzen können nicht von Citrix ADM 506.119 Build aktualisiert werden. [699814]

17. November 2017

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf den Build 505.117 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neuigkeiten

Proxyserver-Unterstützung für Agents auf Citrix ADM

Sie können Ihre Agents nun über einen Proxyserver mit dem Citrix ADM verbinden. Mithilfe dieser Erweiterung leiten Agents alle Daten an den Proxyserver weiter, der die Daten dann über das Internet an das Citrix ADM sendet.

Um Daten über den Proxyserver weiterzuleiten, geben Sie die Proxy-Serverdetails auf dem Agenten mithilfe des folgenden Skripts ein: proxy_input.py, und folgen Sie den Anweisungen des Skripts, um weitere Informationen einzugeben. Der Agent ruft diese Informationen ab, während er über den Proxyserver eine Verbindung zum Citrix ADM herstellt.

Sie können Ihren Proxy-Server authentifizieren, indem Sie Ihren Benutzernamen und Ihr Kennwort angeben. Wenn der Agent die Daten sendet, authentifiziert der Proxyserver die Anmeldeinformationen des Benutzers, bevor er sie an den Citrix ADM weiterleitet.

> **Hinweis** Proxy-Server unterstützt nur die grundlegende Authentifizierung.

[697617]

Aktivieren von Single Sign-On für Google Apps in Citrix ADC-Instanzen mit StyleBook

Mit dem Standard SSO Google Apps StyleBook in Citrix ADM können Sie Single Sign-On für Google-Anwendungen in Citrix ADC-Instanzen aktivieren. Das StyleBook konfiguriert die Citrix ADC-Instanz als SAML-Identitätsanbieter für die Authentifizierung von Benutzern für den Zugriff auf Google Apps. Weitere Informationen finden Sie unter So verwenden Sie SSO Google Apps StyleBook.

[697027]

Fähigkeit, den Spitzennutzungstrend der Anwendung mit der Anwendungsleistung zu bewerten

Sie können nun den Spitzennutzungstrend einer Anwendung beurteilen. Sie können die Auswirkungen auf die Anwendungsleistung anhand von App Score auch im Application Dashboard in Citrix ADM vergleichen. Sie können den Spitzennutzungstrend und die Auswirkungen auf die Performance auf die Anwendungsinformationen verwenden und die erforderlichen Änderungen in Ihrer Bereitstellung vornehmen. Dies hilft, die Leistung der Anwendung zu verbessern.

Um den Spitzennutzungstrend einer Anwendung anzuzeigen, navigieren Sie zu **Anwendungen** > **App-Dashboard**. Wählen Sie die Anwendung aus, und klicken Sie auf **Spitzenauslastung**.

Weitere Informationen finden Sie unter Anwendungstrend

[688208]

Behobene Probleme

Netzwerke

- Wenn eine Zeile einen blauen Hintergrund hat, ist auf der Seite Citrix ADM **Configurations Job** > **Jobs** die Schaltfläche **Job erstellen** deaktiviert. Mit diesem Update ist die Schaltfläche **Job erstellen** aktiv und wird nicht deaktiviert. [695397]
- In Citrix ADM **Netzwerke** > **Ereignisse** > **Ereignismeldungen**, wenn Sie versuchen, die Ereignismeldungen basierend auf Datum zu sortieren, wird die Sortierung nicht korrekt durchgeführt. Die Nachrichten werden in umgekehrter Reihenfolge in Richtung der Sortierpfeile sortiert. Wenn die Nachrichten beispielsweise von neueren nach älteren sortiert werden, zeigt der Pfeil nach oben. [696737]
- Beim Hochladen der Datei ns.conf in Citrix ADM zur Konfigurationsberatung ist ein Validierungsfehler aufgetreten. [696920]
- Eine an Citrix ADM gesendete Trap-Nachricht zeigt den Namen der Entität zusammen mit der IP-Adresse des virtuellen Servers, auf dem der Trap stammt, und dem Port an. Das folgende Beispiel zeigt den Entitätsnamen in Trap-Nachricht, die von Citrix ADM empfangen wird:

```
1     Entity Name
2      server_svc_NSSVC_IPFIX_10.102.29.150:4739       (service_10
          .102.29.150_33554)_DOWN
3  <!--NeedCopy-->
```


- Citrix ADM zeigt den Namen der Entität, die IP-Adresse und die Portnummer nicht als separate Parameter in der Spalte Nachricht in der Tabelle **Netzwerke** > **Ereignisse** > **Ereignismeldungen** an. [696639]
- Wenn Sie in einer Ereignisregel ein Skript ausführen, das eine Nachricht mit Leerzeichen (“ “) enthält, wird das Skript nicht aktiviert. [696896]
- Einige Netzwerkberichte dauern länger, bis sie in Citrix ADM generiert werden. Wenn solche Berichte exportiert werden sollen, werden unvollständige Berichte exportiert. Mit diesem Update wartet Citrix ADM, bis die Berichte vollständig erstellt wurden, bevor sie exportiert werden. [695500]
- In Citrix ADM können Sie keine Berichte für einige tabellarische Ansichten und Dashboards exportieren. Mit diesem Fix können Sie nun den Inhalt der Tabellen und Dashboards exportieren. [670226]
- Beachten Sie in Citrix ADM, dass Sie sich in einer Listenansicht befinden und Sie sich weiter in bestimmte Seiten navigieren. Sie können nicht mit dem Navigationsbereich auf der linken Seite der GUI zurücknavigieren. Möglicherweise müssen Sie mithilfe der Breadcrumbs oben auf der Seite navigieren. Angenommen, Sie befinden sich derzeit auf der Seite **Netzwerke** > **Instanzen** > **NetScaler VPX** > **Sicherung/Wiederherstellung**. Wenn Sie den Citrix ADC-Instanztyp unter **Netzwerke** > **Instanzen** auswählen, wird die entsprechende Citrix ADC-Instanzliste nicht geöffnet, nachdem Sie im Navigationsbereich auf NetScaler VPX geklickt haben. [684922]
- In Citrix ADM schlägt das Upgrade der Citrix ADC-Instanz mit Citrix ADM fehl. Wenn Sie zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufgaben** navigieren und **NetScaler aktualisieren** auswählen, schlägt das Upgrade von Citrix ADC-Instanzen fehl. [692538]
- Konfigurations-Audit-Vorlagen, die zu einem bestimmten Zeitpunkt ausgeführt werden sollen, werden auch während der globalen Abfrage ausgeführt, was zu einer wiederholten Ausführung von Konfigurationsauditvorlagen führt. [697157]
- Die Konfigurationsüberwachung mit bestimmten Variablenwerten funktioniert nicht für Citrix ADC-Instanzen, die sich im HA-Modus befinden. [696990]
- Beim Erstellen einer Konfigurationsüberwachungsvorlagen können Sie keine Eingabedatei für Variablenwerte hochladen. [697137]
- In Citrix ADM führt jeder Fehler bei der Verarbeitung des Konfigurationsüberwachungsberichts zu einer leeren E-Mail, die an die E-Mail-Empfänger gesendet wird. [697138]

Einstellungen

- Zum Zeitpunkt der Knotenregistrierung und -bereitstellung in Citrix ADM in HA muss das Kennwort beider Knoten das Standardkennwort “ns root” sein. Die Knotenregistrierung schlägt fehl, wenn sich das Kennwort von dem unterscheidet `nsroot`. [691836]

- Wenn Sie in Citrix ADM Sonderzeichen wie & in die Eingabefelder wie Name und Beschreibung eingeben, wird & durch & ersetzt. [692656]
- Wenn Sie in Citrix ADM Sonderzeichen wie & in die Eingabefelder wie Name und Beschreibung eingeben, wird & durch & ersetzt. [692656]
- Sie können Anwendungen zu einer Gruppe hinzufügen und auch eine Regex angeben, um die Suchkriterien anzuwenden, um Anwendungen zur Gruppe hinzuzufügen. Wenn Sie eine Gruppe mehrmals bearbeiten, wird der Name der Anwendung in einen ungültigen Regex-Ausdruck konvertiert. Dies führt dazu, dass der RBAC fehlschlägt und die Benutzer können alle Anwendungen sehen.

  1. Navigieren Sie in Citrix ADM zu **System** > **Benutzerverwaltung** > **Gruppen**, und klicken Sie auf **Hinzufügen**. Geben Sie den Gruppennamen ein, wählen Sie auf der Registerkarte **Autorisierungseinstellungen** die gewünschte Anwendung aus, fügen Sie sie der Gruppe hinzu, und klicken Sie auf **Gruppe erstellen**.
  2. Wenn Sie eine Regex hinzufügen möchten, navigieren Sie zur Seite **Gruppen**, wählen Sie die Gruppe aus und klicken Sie auf **Bearbeiten**.
  3. Fügen Sie auf der Registerkarte **Autorisierungseinstellungen** die Regex im Textfeld **Regulären Ausdruck hinzufügen** hinzu, und speichern Sie die Einstellungen.
  4. Wenn Sie die Gruppe erneut bearbeiten, können Sie auf der Registerkarte **Autorisierungseinstellungen** feststellen, dass der Name der zuvor hinzugefügten Anwendung in eine Regex konvertiert wird. Da dies eine ungültige Regex ist, schlägt RBAC fehl und Ihr Benutzer kann alle Anwendungen sehen. [696515]

Hohe Verfügbarkeit

- Wenn Citrix ADC-Instanzen im HA-Setup ein Failover durchführen und wenn der neue primäre Zugriff über Citrix ADM nicht mehr möglich ist, wird die Instanz in der Citrix ADM-GUI nicht mehr angezeigt. [697017]
- Wenn Sie eine Backupdatei von einer Citrix ADC-Instanz in einem Paar wiederherstellen, das sich im HA-Setup auf eine andere Instanz desselben Paares befindet, wird auf diese Citrix ADC-Instanz aufgrund eines Konflikts in der IP-Adresse nicht zugegriffen. Citrix ADM prüft, ob die IP-Adresse in der Backupdatei und die IP-Adresse der Instanz, auf der die Wiederherstellung ausgeführt wird, identisch ist. Wenn die IP-Adressen nicht übereinstimmen, wird eine Fehlermeldung angezeigt und die Wiederherstellung wird beendet. [686829]
- Wenn Sie ein Paar von Citrix ADC-Instanzen aktualisieren, die sich in HA befinden, sind die Citrix ADC-Instanzen instabil. Die Instanzen müssen möglicherweise einige Zeit warten, bevor sie auf die von Citrix ADM gesendeten NITRO -Aufrufe reagieren.
- Mit diesem Fix können Sie eine Wartezeit im Instanzprofil festlegen, so dass Citrix ADM auf die

eingestellte Zeit wartet, bevor Sie einen NITRO -Aufruf an die Instanzen senden. Die Standard-Wartezeit beträgt 60 Sekunden. [690860]

Bekannte Probleme

Analytics

- In bestimmten Fällen werden HDX Insight - und Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite, und versuchen Sie es erneut. [690327]

Netzwerke

- Wenn Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufgaben** navigieren und **NetScaler aktualisieren** auswählen, schlägt das Upgrade von Citrix ADC-Instanzen fehl. [692538]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen. [689330]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]
- Wartungsaufgaben in Citrix ADM funktionieren nicht. [696952]

27. Oktober 2017

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Standardmäßig werden die Citrix ADM Agents automatisch auf den Build 504.115 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen. Sie können auch angeben, wann die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Neuigkeiten

Möglichkeit zum Importieren und Exportieren der Konfigurationsvorlagen

Sie können die Konfigurationsvorlagen exportieren und die Vorlage in denselben oder einen anderen Mandanten im Citrix ADM importieren. Die exportierten Vorlagendaten (wie Konfigurationsbefehle, Variablendefinitionen und Parameter) gehen nach dem Import nicht verloren.

Um die Konfigurationsvorlage zu exportieren, navigieren Sie zu **Netzwerke > Konfigurationsaufträge > Konfigurationsvorlagen**. Wählen Sie die Konfigurationsvorlage aus, und klicken Sie auf **Exportieren**. Die exportierten Konfigurationsvorlagen werden im lokalen System im **JSON-Dateiformat** gespeichert. Sie können diese Datei dann in denselben oder einen anderen Mandanten im Citrix ADM importieren, um eine Konfigurationsvorlage zu erstellen. Um die Konfigurationsvorlage zu importieren, klicken Sie auf **Importieren** und wählen Sie die **JSON-Datei** aus, die Sie lokal gespeichert haben.

Weitere Informationen finden Sie unter Importieren und Exportieren von Konfigurationsvorlagen.

[691585]

Unterstützung für Revisionsverlaufsdifferenz und Überwachungsvorlage für Adminpartitionen

Der Unterschied zum Versionsverlauf und die Überwachungsvorlage für die Administratorpartition werden jetzt in Citrix ADM unterstützt.

Versionsverlaufsunterschied für Administratorpartition ermöglicht es Ihnen, den Unterschied zwischen den fünf neuesten Konfigurationsdateien für eine partitionierte Citrix ADC-Instanz anzuzeigen. Sie können die Konfigurationsdateien miteinander vergleichen (Beispiel: Konfigurationsversion - 1 mit Konfigurationsversion -2) oder mit der aktuellen laufen/gespeicherten Konfiguration mit Konfigurationsversion. Neben den Unterschieden in der Konfiguration werden auch die Korrekturkonfigurationen angezeigt. Sie können alle Korrekturbefehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.

Überwachungsvorlagen für Partition ermöglichen es Ihnen, eine benutzerdefinierte Konfigurationsvorlage zu erstellen und sie einer Partitionsinstanz zuzuordnen. Jede Variation in der laufenden Konfiguration der Instanz mit der Audit-Vorlage wird in der Spalte “Vorlage vs Laufendes Diff” der Seite “ Auditberichte “ angezeigt. Neben den Unterschieden in der Konfiguration werden auch die Korrekturkonfigurationen angezeigt. Sie können auch alle Korrekturbefehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.

[657300]

Möglichkeit, mehrere Vorlagen unterschiedlicher Typen in Konfigurationsaufträgen hinzuzufügen

Sie können jetzt mehrere Vorlagen verschiedener Typen im Konfigurations-Job-Editor hinzufügen, während Sie einen Konfigurationsauftrag erstellen. Um mehrere Vorlagen hinzuzufügen, navigieren Sie zu **Netzwerke > Konfigurationsaufträge**, und klicken Sie auf **Job erstellen**. Geben Sie auf der Seite **Job erstellen** den Jobnamen ein, und wählen Sie den Instanztyp aus. In der Dropdownliste **Konfigurationsquelle** können Sie die gewünschte Quelle auswählen und dann mehrere Vorlagen, die Sie

benötigen, in den Konfigurationseditor ziehen. Die Quelltypen der Vorlage sind **Konfigurationsvorlage**, **Inbuilt Template**, **Hauptkonfiguration**, **Record and Play**, **Instanz**und **File**.

Weitere Informationen finden Sie unter Erstellen eines Konfigurationsauftrags unter Citrix ADM.

[686881]

Fähigkeit, die Eingabevariablenwerte in Konfigurationsaufträgen zu erhalten

In Citrix ADM werden beim Erstellen der Konfigurationsaufträge die angegebenen Eingabevariablenwerte einschließlich Eingabedateien beibehalten. Sie können diese Werte und auch die zuvor hochgeladenen Eingabedateien beim Erstellen des Konfigurationsauftrags anzeigen und bearbeiten. Um die Werte der Eingabevariablen anzuzeigen, navigieren Sie zu **Netzwerk > Konfigurationsaufträge**, wählen Sie den Job aus, und klicken Sie auf **Bearbeiten**. Auf der Registerkarte **Variablenwerte angeben** können Sie die persistenten Variablenwerte anzeigen. Die zuvor hochgeladene Eingabedatei bleibt ebenfalls erhalten. Sie können die Eingabedatei herunterladen, die Datei bearbeiten und dann dieselbe Eingabedatei hochladen, ohne den Namen zu ändern.

[691584]

Möglichkeit, Befehle im Konfigurations-Job-Editor neu anzuordnen

Sie können die Befehle jetzt im Konfigurations-Job-Editor neu anordnen und neu anordnen. Sie können die Befehle nun von einer Zeile in eine andere verschieben, indem Sie die Befehlszeile ziehen. Sie können die Befehlszeile auch von einer Zeile zu einer beliebigen Zielzeile verschieben oder neu anordnen, indem Sie einfach die Befehlszeilennummer ändern.

[684164]

Konfigurieren von Netzwerkberichterstattungseinstellungen für Citrix ADM

Sie können jetzt das Schnittintervall von Netzwerkberichtsdaten in Citrix ADM konfigurieren. Dadurch wird die Menge der Netzwerkberichtsdaten begrenzt, die in der Datenbank des Citrix ADM -Servers gespeichert werden. Standardmäßig erfolgt die Beschneidung alle 24 Stunden (um 01.00 Uhr) für das Netzwerk, das historische Daten meldet.

[692461]

Möglichkeit zur Vorschau und Änderung der Variablen im Konfigurationsauftrag

In Citrix ADM können Sie nun alle Variablen anzeigen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags in einer einzigen konsolidierten Ansicht definiert haben.

Klicken Sie im **Konfigurations-Job-Editor** auf die Registerkarte **Variablen anzeigen**, um die Variablen in einer einzigen konsolidierten Ansicht anzuzeigen. Ein neues Popup-Fenster wird angezeigt, in

dem alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem tabellarischen Format angezeigt werden. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf **Fertig**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.

Sie können eine der folgenden Aktionen ausführen, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:

- **Erstellen eines Konfigurationsauftrags**. Navigieren Sie zu **Netzwerke > Konfigurationsaufträge**und wählen Sie **Auftrag erstellen**aus. Auf der Seite **Job erstellen** können Sie eine Vorschau aller Variablen anzeigen.
- **Bearbeiten eines Konfigurationsauftrags**. Navigieren Sie zu **Netzwerk > Konfigurationsaufträge**, wählen Sie den Auftragsnamen aus und klicken Sie auf **Bearbeiten**. Auf der Seite **Job konfigurieren** können Sie eine Vorschau aller Variablen anzeigen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.

[684166]

Platzhalterunterstützung für dynamisches Hinzufügen von Anwendungen zu Gruppen in Citrix ADM

Wenn Sie Anwendungen zu einer Gruppe in Citrix ADM hinzufügen, können Sie Regex verwenden, um die Anwendungen zu suchen und den Gruppen hinzuzufügen, die die Regex-Kriterien erfüllen. Die Benutzer, die an diese Gruppen gebunden sind, können nur auf diese spezifischen Anwendungen zugreifen. Der angegebene Regex-Ausdruck wird in Citrix ADM beibehalten. Wenn dem System eine neue Anwendung hinzugefügt wird, wendet Citrix ADM die Suchkriterien auf die neue Anwendung an, und die Anwendung, die die Kriterien erfüllt, wird dynamisch Teil der Gruppe. Sie müssen die neue Anwendung nicht manuell zur Gruppe hinzufügen. Die Anwendungen werden dynamisch im System aktualisiert, und die jeweiligen Gruppenbenutzer können die Anwendungen unter entsprechenden Modulen in Citrix ADM sehen.

Weitere Informationen finden Sie unter Konfigurieren von Gruppen auf Citrix ADM.

[692032]

Bestimmte Variablenwerte in Konfigurationsüberwachungsvorlagen zuweisen

Mit Citrix ADM können Sie Variablen erstellen und Variablen Werte zuweisen, während Sie Konfigurationsüberwachungsvorlagen erstellen. Auf der Registerkarte **Variablenwerte angeben** unter **Netzwerke** > **Konfigurationsüberwachung** > **Überwachungsvorlagen** > **Hinzufügen** > **Vorlage erstellen** haben Sie zwei Optionen, um Variablen Werte zuzuweisen:

1. **Allgemeine Variablenwerte für alle Instanzen**. Wählen Sie diese Option, um gemeinsame Werte in die Variablen einzugeben, die auf dieser Seite für die ausgewählte Instanz aufgeführt sind.

2. **Laden Sie die Eingabedatei für Variablenwerte**hoch. Wählen Sie diese Option aus, um die Datei herunterzuladen, Werte für die Variablen einzugeben und dann die Datei in Citrix ADM hochzuladen.

Weitere Informationen finden Sie unter Überwachungsvorlagen erstellen.

[691127]

Exportieren des Konfigurations-Audit-Diff-Berichts

Mit Citrix ADM können Sie den Konfigurationsüberwachungsbericht im Abschnitt Konfigurationsüberwachung herunterladen. Im Konfigurationsüberwachungsabschnitt können Sie den zusammenfassenden Bericht über alle Instanzen und pro Instanz exportieren. Außerdem können Sie für jedes Instanzvorlagenpaar granulare Diff-Berichte exportieren.

Weitere Informationen finden Sie unter Überwachungsberichte anzeigen.

[679736]

Möglichkeit, Konfigurationsüberwachungsvorlage und E-Mail-Konfigurations-Diff-Bericht zu planen

Mit Citrix ADM können alle Überwachungsvorlagen unter **Netzwerke** > **Konfigurationsüberwachung** > **Überwachungsvorlagen** zu einem Zeitpunkt ausgeführt werden, der einzeln oder global gemäß Ihren Anforderungen geplant wird. Sie können planen, dass die Konfigurationsüberwachungsvorlage zu einem bestimmten Zeitpunkt ausgeführt wird, anstatt die Vorlage zu einer vom System konfigurierten Standardzeit auszuführen. Wenn Sie die Option **Vorlagenplan anpassen** auswählen, können Sie planen, dass die Vorlage täglich, an einem bestimmten Tag in der Woche oder an einem bestimmten Tag im Monat ausgeführt wird. Für jede Option müssen Sie auch die Planzeit eingeben, zu der Citrix ADM die Vorlage ausführen muss. Citrix ADM bietet Ihnen die folgenden Optionen, um den Export des Config-Audit-Diff-Berichts zu planen.

- **Verwenden Sie das globale Abrufintervall**. Wählen Sie diese Option aus, um die Vorlage auf den Instanzen zu einem Zeitpunkt auszuführen, der global auf Citrix ADM konfiguriert ist.
- **Anpassen des Vorlagenzeitplans**. Verwenden Sie diese Option, um die Zeit und die Häufigkeit zu konfigurieren, mit der die Vorlagen ausgeführt werden müssen.
- **Senden Sie den Bericht per E-Mail**. Verwenden Sie diese Option, um das E-Mail-Profil zu konfigurieren, an das der Diff-Bericht als E-Mail-Anhang gesendet werden muss.

Weitere Informationen finden Sie unter Überwachungsvorlagen erstellen.

[681957]

Möglichkeit, Abhängigkeiten eines StyleBook als Graph zu visualisieren

Sie können nun alle Abhängigkeiten eines StyleBook visualisieren, also alle anderen StyleBooks, von denen Ihr ausgewähltes StyleBook abhängt. Abhängigkeiten werden durch das Erstellen neuer StyleBooks mit vorhandenen erstellt. Abhängigkeiten werden als Diagramm von Feldern und Pfeilen visualisiert, wobei jedes Feld ein StyleBook darstellt und jeder Pfeil eine Richtungsabhängigkeit von einem StyleBook zu seinem abhängigen darstellt. Navigieren Sie zu **Anwendungen** > **Konfigurationen** > **StyleBooks**, und klicken Sie in der Liste der StyleBooks, die auf der rechten Seite angezeigt werden, auf den Link **Abhängigkeiten anzeigen** für das StyleBook, das Sie visualisieren möchten.

[697175]

Benutzerdefinierte StyleBooks und abhängige benutzerdefinierte StyleBooks herunterladen

Sie können nun ein benutzerdefiniertes StyleBook und seine abhängigen StyleBooks im YAML-Format als ZIP- oder TGZ-Datei auf Ihr System herunterladen. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfigurationen** > **StyleBooks**, und klicken Sie in der Liste der StyleBooks, die auf der rechten Seite angezeigt wird, auf den Link **Download** für das StyleBook, das Sie herunterladen möchten.

> **Hinweis** Sie können keine Standard-StyleBooks herunterladen.

[696383]

Benutzerdefinierte StyleBooks und abhängige benutzerdefinierte StyleBooks löschen

Sie können ein benutzerdefiniertes StyleBook und seine abhängigen StyleBooks aus dem Citrix ADM Ordnersystem entfernen. Navigieren Sie zu **Anwendungen** > **Konfigurationen** > **StyleBooks** und in der Liste der StyleBooks, die auf der rechten Seite angezeigt wird, und klicken Sie auf "**X** " Symbol rechts neben dem StyleBook, das Sie löschen möchten. Sie haben die Möglichkeit, nur die Datei oder alle abhängigen StyleBooks zu löschen.

> **Hinweis** Sie können Standard-StyleBooks nicht löschen.

[696384]

Verwalten und Überwachen von HAProxy-Instanzen

Sie können nun HAProxy-Instanzen in Ihrer Bereitstellung mit Citrix ADM verwalten und überwachen. Wenn Sie Citrix ADM einen HAProxy-Host hinzufügen, erkennt er automatisch die HAProxy-Instanzen auf dem Host und ermöglicht Ihnen, diese zu verwalten und zu überwachen, indem Sie Folgendes bereitstellen:

- **HAProxy App Dashboard**: Zeigt Echtzeitstatistiken der Frontends auf den HAProxy-Instanzen an. Das Dashboard listet die Front-Ends als erkannte Anwendungen auf und zeigt Echtzeit-Transaktionen, Durchsatz und Sitzungsinformationen zu den Anwendungen an.

- **Möglichkeit, eine HAProxy-Instanz neu zu starten**: Sie können eine HAProxy-Instanz von der Citrix ADM GUI neu starten. Außerdem können Sie eine HAProxy-Instanz über die Citrix ADM GUI einen harten Neustart durchführen oder einen weichen Neustart durchführen.

Weitere Informationen finden Sie unter Verwalten und Überwachen von HAProxy-Instanzen.

[637830]

Behobene Probleme

Die folgenden Probleme wurden in dieser Version behoben.

Analytics

- Die Analytics-Funktion zeigt keine Daten an, wenn Sie Citrix ADC CPX-Instanzen in Citrix ADM hinzugefügt haben.
  Problemumgehung: Fügen Sie Citrix ADC CPX-Instanzen nicht zu Citrix ADM hinzu. [694792]

Agents

- Wenn Sie zu **Netzwerke** > **Agents** navigieren und versuchen, einen **Agenten** vom Agent-Bildschirm herunterzuladen, wird möglicherweise ein Fehler wie Datei nicht gefunden angezeigt.
  Problemumgehung: Um einen Agenten herunterzuladen, navigieren Sie zu **Einstellungen** > **Agent einrichten**, wählen Sie den Hypervisor aus, und klicken Sie dann auf **Image herunterladen**. [695998]

Bekannte Probleme

In diesem Release bestehen die folgenden bekannten Probleme:

Analytics

- In bestimmten Fällen werden HDX Insight - und Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut. [690327]

Netzwerke

- In Citrix ADM schlägt das Upgrade der Citrix ADC-Instanz mit Citrix ADM fehl. Wenn Sie zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufgaben** navigieren und **NetScaler aktualisieren** auswählen, schlägt das Upgrade von Citrix ADC-Instanzen fehl. [692538]

- Konfigurations-Audit-Vorlagen, die zu einem bestimmten Zeitpunkt ausgeführt werden sollen, werden auch während der globalen Abfrage ausgeführt, was zu einer wiederholten Ausführung von Konfigurationsauditvorlagen führt. [697157]
- Die Konfigurationsüberwachung mit bestimmten Variablenwerten funktioniert nicht für Citrix ADC-Instanzen, die sich im HA-Modus befinden. [696990]
- Beim Erstellen einer Konfigurationsüberwachungsvorlagen können Sie keine Eingabedatei für Variablenwerte hochladen. [697137]
- In Citrix ADM führt jeder Fehler bei der Verarbeitung des Konfigurationsüberwachungsberichts zu einer leeren E-Mail, die an die E-Mail-Empfänger gesendet wird. [697138]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen. [689330]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]
- Wenn Sie in Citrix ADM Sonderzeichen wie & in die Eingabefelder wie Name und Beschreibung eingeben, wird & durch & ersetzt. [692656]
- Wartungsaufgaben in Citrix ADM funktionieren nicht. [696952]
- Sie können Anwendungen zu einer Gruppe hinzufügen und auch eine Regex angeben, um die Suchkriterien anzuwenden, um Anwendungen zur Gruppe hinzuzufügen. Wenn Sie eine Gruppe mehrmals bearbeiten, wird der Name der Anwendung in einen ungültigen Regex-Ausdruck konvertiert. Dies führt dazu, dass der RBAC fehlschlägt und die Benutzer können alle Anwendungen sehen.

  1. Navigieren Sie in Citrix ADM zu **Einstellungen** > **Benutzerverwaltung** > **Gruppen**, und klicken Sie auf **Hinzufügen**. Geben Sie den Gruppennamen ein, wählen Sie auf der Registerkarte **Autorisierungseinstellungen** die gewünschte Anwendung aus, fügen Sie sie der Gruppe hinzu, und klicken Sie auf **Gruppe erstellen**.
  2. Wenn Sie eine Regex hinzufügen möchten, navigieren Sie zur Seite **Gruppen**, wählen Sie die Gruppe aus und klicken Sie auf **Bearbeiten**.
  3. Fügen Sie auf der Registerkarte **Autorisierungseinstellungen** die Regex im Textfeld **Regulären Ausdruck hinzufügen** hinzu, und speichern Sie die Einstellungen.
  4. Wenn Sie die Gruppe erneut bearbeiten, können Sie auf der Registerkarte **Autorisierungseinstellungen** feststellen, dass der Name der zuvor hinzugefügten Anwendung in eine Regex konvertiert wird. Da dies eine ungültige Regex ist, schlägt RBAC fehl und Ihr Benutzer kann alle Anwendungen sehen.

  [696515]

7. Oktober 2017

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Die Citrix ADM Agents werden automatisch auf den Build 503.115 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen.

Neuigkeiten

Die folgenden Verbesserungen sind in dieser Version verfügbar.

Agent-Upgrade-Zeit konfigurieren

Standardmäßig wird ein Agent automatisch aktualisiert, wenn eine neuere Version verfügbar ist. Sie können jedoch angeben, wann das Agent-Upgrade durchgeführt werden soll. Wenn Sie eine bestimmte Zeit auswählen, werden die Agents zu dem angegebenen Zeitpunkt aktualisiert, jedoch in der Zeitzone, in der Ihre Agents bereitgestellt werden. Während des Upgrades kann es zu einer Ausfallzeit von etwa 30 Minuten kommen. Um die Agent-Upgradezeit anzugeben, navigieren Sie zu **Netzwerke** > **Agents**, klicken Sie auf **Upgradeeinstellungen konfigurieren**, und geben Sie dann an, wann der Agent aktualisiert werden soll. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgradeeinstellungen.

Zugriff auf die GUI einer verwalteten Citrix ADC-Instanz über Citrix ADM

Sie können nun über Citrix ADM auf die Benutzeroberfläche einer verwalteten Citrix ADC-Instanz zugreifen. Um Citrix ADC-Instanzen zu verwalten und zu überwachen, fügen Sie sie dem Citrix ADM hinzu. Sie können dann über das Citrix ADM darauf zugreifen. Stellen Sie sicher, dass Sie mit dem Citrix Netzwerk verbunden sind.

Um über Citrix ADM auf eine Citrix ADC-Instanz-GUI zuzugreifen, navigieren Sie zu **Netzwerke** > **Instanzen**. Wählen Sie unter Instanzen den Instanztyp aus, den Sie anzeigen möchten (z. B. Citrix ADC VPX), und klicken Sie dann auf die IP-Adresse der Instanz, auf die Sie zugreifen möchten.

[693970]

Verwalten von Citrix SWG-Instanzen von Citrix ADM

Citrix ADM unterstützt jetzt die Erkennung, Verwaltung und Überwachung von Citrix Secure Web Gateway (SWG) Instanzen. Sie können die Citrix SWG-Instanzen unter **Netzwerke** > **Instanzen** anzeigen, wie in der folgenden Abbildung dargestellt:

[692493]

Support für die Gnadenfrist nach Ablauf der Lizenz

Nach Ablauf der Lizenz bietet Citrix ADM 90 Tage Nachfrist an. Während des Kulanzzeitraums werden die von Citrix ADM gesammelten Daten 30 Tage lang aufbewahrt und die Konfigurationen 90 Tage lang aufbewahrt. Während des Kulanzzeitraums können Sie nicht auf Citrix ADM zugreifen.

[691069]

Unterstützung für Entitätsspezifische Abfragen

Mit Citrix ADM können Sie bestimmte Entitäten abfragen, die auf einer Instanz konfiguriert sind. Dies reduziert die Aktualisierungszeit, die Citrix ADM benötigt, um den neuesten Status der an eine Instanz gebundenen Entitäten anzuzeigen. Sie können nun die folgenden Entitäten für alle Aktualisierungen ihres Status abfragen: Dienste, Dienstgruppen, virtuelle Server mit Lastenausgleich, virtuelle Server zur Cache-Reduzierung, virtuelle Server zum Wechseln von Inhalten, virtuelle Authentifizierungsserver, virtuelle VPN-Server, virtuelle GSLB-Server und -Anwendungsserver. Ausführliche Dokumentation finden Sie unterAbfragen von Citrix ADC-Instanzen und Entitäten.

[692958]

Behobene Probleme

Die folgenden Probleme wurden in dieser Version behoben.

Agent

- Wenn Sie einen Agenten verwenden, der in der Microsoft Azure-Cloud bereitgestellt wird, werden die verwalteten Instanzen, die diesem Agent zugeordnet sind, in der Citrix ADM GUI im Status Heruntergefahren angezeigt. [690941]
- Nachdem die Agentenregistrierung abgeschlossen ist, können Sie sich möglicherweise nicht über die Hypervisor Konsole am Agent anmelden. [691181]

Netzwerke

- In Citrix ADM werden die Dateien beim Erstellen von Konfigurationsaufträgen nicht automatisch hochgeladen. Sie müssen die Dateien auswählen, die Sie hochladen möchten, und auf die Schaltfläche **Hochladen** klicken. Die Schaltfläche **Hochladen** ist jetzt nicht verfügbar und die Datei wird automatisch hochgeladen, nachdem Sie die Dateien ausgewählt haben, die Sie hochladen möchten. [686889]
- In **Netzwerke** > **Konfigurationsaufträge** > **Vorschau** können Sie die zugehörigen Rollback-Befehle des Konfigurationsauftrags auf der Vorschauseite anzeigen. [687621]

Einstellungen

- In Citrix ADM ist Citrix SD-WAN WO Advanced Plattform-Backup nicht mit dem benutzerdefinierten Geräteprofil kompatibel. [690508]

Bekannte Probleme

In diesem Release bestehen die folgenden bekannten Probleme:

Agents

- Wenn Sie zu **Netzwerke** > **Agents** navigieren und versuchen, einen **Agenten** vom Agent-Bildschirm herunterzuladen, wird möglicherweise ein Fehler wie Datei nicht gefunden angezeigt.
  Problemumgehung: Um einen Agenten herunterzuladen, navigieren Sie zu **Einstellungen**> **Agent einrichten**, wählen Sie den Hypervisor aus, und klicken Sie dann auf **Image herunterladen**. [695998]

Analytics

- In bestimmten Fällen werden HDX Insight - und Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut. [690327]
- Die Analytics-Funktion zeigt keine Daten an, wenn Sie Citrix ADC CPX-Instanzen in Citrix ADM hinzugefügt haben.
  Problemumgehung: Fügen Sie Citrix ADC CPX-Instanzen zu Citrix ADM hinzu. [694792]

Netzwerke

- In Citrix ADM schlägt das Upgrade der Citrix ADC-Instanz mit Citrix ADM fehl. Wenn Sie zu **Netzwerke > Konfigurationsaufträge > Wartungsaufgaben** navigieren und **NetScaler aktualisieren**auswählen, schlägt das Upgrade von Citrix ADC-Instanzen fehl. [692538]
- In Citrix ADM ersetzt & im Textfeld der Formulareingabe, wenn Sie Sonderzeichen wie & in die Eingabefelder wie Name und Beschreibung eingeben, &. [692656]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen. [689330]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]

> **Hinweis** [XXXXXX] Labels sind interne Tracking-IDs, die vom Citrix ADM Team verwendet werden.

14. September 2017

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Die Citrix ADM Agents werden automatisch auf den Build 502.119 aktualisiert. Sie können die Agentendetails auf der Seite **Netzwerke** > **Agents** anzeigen.

Neuigkeiten

Die folgenden Verbesserungen sind in dieser Version verfügbar.

Citrix ADC Global Load Balancing-Lösung für Hybrid- und Multi-Cloud-Bereitstellungen

Die Global Load Balancing (GLB) -Lösung ermöglicht es Benutzern, die Clientanfragen über mehrere Rechenzentren in mehreren Clouds und auf on-premises bereitgestellte Anwendungsserver zu verteilen. Diese Lösung unterstützt sowohl Multi-Cloud- als auch Hybrid-Cloud-Bereitstellungen. Die Kernvorteile dieser Lösung sind:

- Ermöglicht das Erstellen, Verwalten und Überwachen von GLB-Knoten über geografische Standorte hinweg über eine einzige einheitliche Konsole.
- Bietet die Flexibilität, einen Teil der Infrastruktur in die Cloud zu verschieben.
- Unterstützt aktive und passive Topologie für Disaster Recovery
- Unterstützt mehrere globale Load Balancing-Methoden, wie statische Proximity, Round Robin, Quell-IP-Hash und Round-Trip-Zeit.

Das zugehörige Multi-Cloud GLB StyleBook in Citrix ADM hilft bei der Bereitstellung einer einzigen Benutzeroberfläche für die Verwaltung aller GLB-Knoten in mehreren Rechenzentren. Vorteile der Verwendung eines StyleBook sind:

- Das Ändern der vorhandenen Konfiguration ist einfach, da die Änderungen an einem Ort vorgenommen werden müssen.
- Das Verschieben der Konfiguration auf alle GLB-Knoten mit StyleBooks ist schneller.

Eine vollständige Dokumentation finden Sie unterGlobaler Citrix ADC Lastenausgleich für Hybrid- und Multi-Cloud-Bereitstellungen.

[691937]

Verwalten und Überwachen von HAProxy-Instanzen (Vorschau)

Sie können nun HAProxy-Instanzen in Ihrer Bereitstellung mit Citrix ADM verwalten und überwachen. Wenn Sie Citrix ADM einen HAProxy-Host hinzufügen, erkennt er automatisch die HAProxy-Instanzen

auf dem Host und ermöglicht Ihnen, diese zu verwalten und zu überwachen, indem Sie Folgendes bereitstellen:

- **HAProxy App Dashboard**: Zeigt Echtzeitstatistiken der Frontends auf den HAProxy-Instanzen an. Das Dashboard listet die Front-Ends als erkannte Anwendungen auf und zeigt Echtzeit-Transaktionen, Durchsatz und Sitzungsinformationen zu den Anwendungen an.
- **Möglichkeit, eine HAProxy-Instanz neu zu starten**: Sie können eine HAProxy-Instanz von der Citrix ADM GUI neu starten. Außerdem können Sie einen harten Neustart oder einen weichen Neustart einer HAProxy-Instanz über die Citrix ADM GUI durchführen.

Weitere Informationen finden Sie unter Verwalten und Überwachen von HAProxy-Instanzen.

[637830]

Option Überspringen auf dem Bildschirm Erstmalige Benutzererfahrung von Citrix ADM

Mit Citrix ADM können Sie jetzt den Agentenregistrierungsschritt überspringen und direkt zum Citrix ADM App-Dashboard navigieren. Klicken Sie auf der Seite Agent **einrichten auf Überspringen, um die Agentenregistrierung** zu **überspringen**.

Darüber hinaus enthält die Citrix ADM Seite zur Erstanbietung jetzt ein Video, das einen Überblick über diesen Citrix Cloud-Dienst bietet.

[693963]

Erweiterungen auf der Seite Abonnements

Auf der Seite Abonnements werden nun die Abonnementübersicht, virtuelle Server und virtuelle Server von Drittanbietern angezeigt. Sie können die folgenden Änderungen auf der Seite **Einstellungen** > **Abonnements** anzeigen.

- Lizenzierungszusammenfassung pro virtuellem Servertyp.
- Lastausgleichslizenzen von Drittanbietern.
- Möglichkeit, die automatische Lizenzierung virtueller Server auszuwählen oder aufzuheben.

Sie können auch auf die virtuellen Servertypen klicken, um die Liste der virtuellen Server anzuzeigen, auf die die Lizenzen angewendet werden.

Weitere Informationen finden Sie im Abschnitt Anzeigen der lizenzierten virtuellen Server inAbonnements verwalten.

[693954]

Behobene Probleme

Die folgenden Probleme wurden in dieser Version behoben.

Netzwerke

- Wenn der Kontrollproxy während des Startvorgangs des Agenten nicht verfügbar ist, kann der Agent die SNMP-Trapeinstellungen von Citrix ADM nicht abrufen, und alle Traps, die von Citrix ADC-Instanzen empfangen wurden, werden gelöscht. [687027]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden keine E-Mails für die Ereignisse gesendet, die den Filterkriterien entsprechen. [688985]
- Upgrade der Citrix ADC Funktion in Wartungsaufgaben wird in Citrix ADM nicht unterstützt. Sie können die Option jedoch immer noch in der GUI anzeigen. [689068]
- In Citrix ADM ändert sich das Hamburger-Symbol (Menüsymbol in der linken Ecke) in das Schließen-Symbol (X), wenn Sie darauf klicken, um das Dropdown-Menü Navigation zu öffnen. Mit diesem Fix, wenn wir eine Konfigurationsseite öffnen, zum Beispiel Instanz hinzufügen, Insight konfigurieren und andere, ist das Navigationsmenüfenster ausgeblendet und das **X**-Symbol ist deaktiviert. [687203]
- Wenn Sie unter **Netzwerke** > **Ereignisse** > **Ereignismeldungen** ein Ereignis auswählen und auf die Registerkarte **Details** klicken, fehlen die Werte der folgenden Parameter wie Benutzername, Konfigurationsbefehl, Autorisierungsstatus, Ausführungsstatus und Entitätstyp auf der Seite **Ereignisdetails**. [686791]
- In **Netzwerke > Netzwerkfunktionen > Lastenausgleich > Service-Gruppen** können Sie die Anwendungen nun nach ID filtern und in Python SDK verwenden. [692061]
- Unter **Netzwerke > Netzwerkfunktionen > Lastenausgleich > Virtuelle Server**werden bei einigen virtuellen Servern, die sich länger als 248 Tage im Status **UP** befinden, falsche Werte angezeigt. [693146]

Einstellungen

- Wenn Sie in Citrix ADM einen Gruppennamen mit Leerzeichen erstellen, funktionieren bestimmte Funktionen, z. B. das Abrufen von Apps, die Gruppennamen für Berechtigungen verwenden, möglicherweise nicht wie erwartet. [692629]
- Das Upgrade von Citrix ADC-Instanzen im HA-Modus von Citrix ADM schlägt fehl, da der sekundäre Knoten einige Zeit benötigt, um den Neustart des sekundären Knotens zu verursachen, wodurch das Failover vom primären Knoten fehlschlägt. [693119]

StyleBooks

- Das "*****" wird als gültige Eingabe für den `tcp-port` Parameter im CLI-Befehl akzeptiert. [694155]

Bekannte Probleme

In diesem Release bestehen die folgenden bekannten Probleme:

Agent

- Wenn Sie einen Agenten verwenden, der in der Microsoft Azure-Cloud bereitgestellt wird, werden die verwalteten Instanzen, die diesem Agent zugeordnet sind, in der Citrix ADM GUI im Status Heruntergefahren angezeigt. [690941]
- Nachdem die Agentenregistrierung abgeschlossen ist, können Sie sich möglicherweise nicht über die Hypervisor Konsole am Agent anmelden.
  Problemumgehung: Melden Sie sich mit einem SSH-Client beim Agenten an. [691181]

Analytics

- In bestimmten Fällen werden HDX Insight - und Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut. [690327]
- Die Analytics-Funktion zeigt keine Daten an, wenn Sie Citrix ADC CPX-Instanzen in Citrix ADM hinzugefügt haben.
  Problemumgehung: Fügen Sie Citrix ADC CPX-Instanzen nicht zu Citrix ADM hinzu. [0694792]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen. [689330]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM **unter Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]

> **Hinweis** [XXXXXX] Labels sind interne Tracking-IDs, die vom Citrix ADM Team verwendet werden.

25. August 2017

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Neuigkeiten

Die folgenden Verbesserungen sind in dieser Version verfügbar.

Upgrades für Citrix ADM Evergreen Agent

In Citrix ADM werden Agents, die auf Softwareversion 12.0 Build 501.117 und höher ausgeführt werden, automatisch von Citrix ADM auf neuere und empfohlene Versionen aktualisiert.
Um diese Funktion für Citrix ADM Agents zu aktivieren, müssen Sie Ihre vorhandenen Agents manuell auf Citrix ADM-Agent Version 12.0 Build 501.117 aktualisieren.

Behobene Probleme

Die folgenden Probleme wurden in dieser Version behoben.

Netzwerke

- Wenn Sie in Citrix ADM versuchen, die Standardzertifikate aller erkannten Citrix ADC-Instanzen zu löschen, wird eine Fehlermeldung angezeigt. Nachdem Sie nun die Standardzertifikate ausgewählt haben, ist die Schaltfläche Löschen deaktiviert.
  [687610]
- Wenn Sie in Citrix ADM eine Citrix ADC-Instanz löschen, werden Fehlerobjekte, die den jeweiligen Citrix ADC-Instanzen zugeordnet sind, nicht gelöscht.
  [690059]
- Ereignisberichte (Netzwerke > Ereignisse > Berichte) werden nicht angezeigt, wenn die gewählte Dauer 1 Monat ist.
  [692054]
- Wenn in Citrix ADM bei der Durchführung von Entitätsabfragen die Anzahl der zu ermittelnden Citrix ADC-Instanzen sehr hoch ist, reagiert die Citrix ADM Benutzeroberfläche möglicherweise nicht mehr.
  Problemumgehung: Schließen Sie Ihren Webbrowser, und melden Sie sich nach 10-15 Minuten erneut an Ihrem Citrix ADM an.
  [692617]

On-Boarding

- Nachdem Sie einen neuen Mandanten in Citrix ADM einbauen und auf die Schaltfläche Verwalten klicken, wird möglicherweise der Fehler Seite funktioniert nicht zum ersten Mal angezeigt.
  [691018]

Bekannte Probleme

In diesem Release bestehen die folgenden bekannten Probleme:

Agent

- Wenn Sie einen Agenten verwenden, der in der Microsoft Azure-Cloud bereitgestellt wird, werden die verwalteten Instanzen, die diesem Agent zugeordnet sind, in der Citrix ADM GUI im Status Heruntergefahren angezeigt. [690941]
- Nachdem die Agentenregistrierung abgeschlossen ist, können Sie sich möglicherweise nicht über die Hypervisor Konsole am Agent anmelden.
  Problemumgehung: Melden Sie sich mit einem SSH-Client beim Agenten an. [691181]

Analytics

- In bestimmten Fällen werden HDX Insight - und Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut. [690327]

Netzwerke

- Wenn der Kontrollproxy während des Startvorgangs des Agenten nicht verfügbar ist, kann der Agent die SNMP-Trapeinstellungen von Citrix ADM nicht abrufen, und alle Traps, die von Citrix ADC-Instanzen empfangen wurden, werden gelöscht.
  Problemumgehung: Wird `masd restart` auf dem Agenten ausgeführt, wenn die Verbindung mit Citrix ADM hergestellt wurde. [687027]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden keine E-Mails für die Ereignisse gesendet, die den Filterkriterien entsprechen. [688985]
- Upgrade der Citrix ADC Funktion in Wartungsaufgaben wird in Citrix ADM nicht unterstützt. Sie können die Option jedoch immer noch in der GUI anzeigen. [689068]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen. [689330]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]

> **Hinweis** [XXXXXX] Labels sind interne Tracking-IDs, die vom Citrix ADM Team verwendet werden.

August 13, 2017

Dies ist eine Fehlerkorrektur-Version. Es gibt keine neuen Funktionen in dieser Version.

Behobene Probleme

Die folgenden Probleme wurden in dieser Version behoben.

Analytics

- Bei der Verwendung von HDX Insight in Citrix ADM funktionieren Geomaps möglicherweise nicht für IP-Blöcke, die über einen privaten IP-Block erstellt werden. [691947]
- Beim Erstellen von zwei IP-Block-Sites wird der Geo-Standort der ersten IP-Site nicht ordnungsgemäß angezeigt. Wenn Sie die erste IP-Site löschen und neu erstellen, werden in der Geo-Map keine Informationen über die erste IP-Site angezeigt. [691965]

Netzwerke

Um das Debugging in Citrix ADM zu erleichtern, werden in den Protokolldateien des Subsystems die Mandantennamen für alle ausgelösten Datenbankausnahmen angezeigt. [692663]

Bekannte Probleme

In diesem Release bestehen die folgenden bekannten Probleme:

Agent

- Wenn Sie einen Agenten verwenden, der in der Microsoft Azure-Cloud bereitgestellt wird, werden die verwalteten Instanzen, die diesem Agent zugeordnet sind, in der Citrix ADM GUI im Status Heruntergefahren angezeigt. [690941]
- Nachdem die Agentenregistrierung abgeschlossen ist, können Sie sich möglicherweise nicht über die Hypervisor Konsole am Agent anmelden.
  Problemumgehung: Melden Sie sich mit einem SSH-Client beim Agenten an. [691181]

Analytics

- In bestimmten Fällen werden HDX Insight - und Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut. [690327]

Netzwerke

- Wenn der Kontrollproxy während des Startvorgangs des Agenten nicht verfügbar ist, kann der Agent die SNMP-Trapeinstellungen von Citrix ADM nicht abrufen, und alle Traps, die von Citrix ADC-Instanzen empfangen wurden, werden gelöscht.
  Problemumgehung: Wird `masd restart` auf dem Agenten ausgeführt, wenn die Verbindung mit Citrix ADM hergestellt wurde. [687027]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden keine E-Mails für die Ereignisse gesendet, die den Filterkriterien entsprechen. [688985]
- Upgrade der Citrix ADC Funktion in Wartungsaufgaben wird in Citrix ADM nicht unterstützt. Sie können die Option jedoch immer noch in der GUI anzeigen. [689068]

On-Boarding

- Nachdem Sie einen neuen Mandanten in Citrix ADM einbauen und auf die Schaltfläche Verwalten klicken, wird möglicherweise der Fehler Seite funktioniert nicht zum ersten Mal angezeigt.
  Problemumgehung:

Warten Sie eine Stunde (60 Minuten), und melden Sie sich erneut an. Die Verzögerung ist auf die Zeit zurückzuführen, die für die Provisioning des neuen Mandanten in Anspruch genommen wird. [691018]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen. [689330]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]

> **Hinweis** [XXXXXX] Labels sind interne Tracking-IDs, die vom Citrix ADM Team verwendet werden.

10. August 2017

Diese Version enthält neue Funktionen und Fehlerbehebungen.

Neuigkeiten

Die folgenden Verbesserungen sind in dieser Version verfügbar.

Syslog-Nachrichten in Citrix ADM unterdrücken

Citrix ADM empfängt alle konfigurierten Syslogs, die von den verwalteten Citrix ADC-Instanzen an ihn gesendet werden. Aufgrund der großen Anzahl von Syslog-Nachrichten belegen die Syslogs großen Speicherplatz in der Datenbank. Viele dieser Nachrichten sind möglicherweise nicht von Bedeutung für Sie und Sie möchten möglicherweise nur die wichtigen Syslog-Nachrichten erhalten.

Sie können nun einige der Syslogs unterdrücken, die in Citrix ADM empfangen werden, indem Sie Filter einrichten. Die beiden Filter, mit denen Sie Syslogs unterdrücken können, sind Schweregrad und Einrichtung. Sie können Nachrichten von einer oder mehreren Citrix ADC-Instanzen unterdrücken.

Sie können auch Textmuster verwenden, um Nachrichten zu suchen und zu unterdrücken. Citrix ADM löscht alle Nachrichten, die den angegebenen Kriterien entsprechen. Die gelöschten Syslogs werden weder auf Citrix ADM angezeigt noch in der Kundendatenbank gespeichert. Daher wird eine große Menge an Speicherplatz auf dem Speicherserver gespeichert.

Weitere Informationen: Unterdrücken von Syslog-Nachrichten in Citrix ADM

[6779274]

Erstellen und Anzeigen von Berichten von Lastausgleich-Entitäten, die auf Citrix ADC-Instanzen konfiguriert sind

Sie können Berichte über Load Balancing-Entitäten erstellen, z. B. virtuelle Server und Dienste, die auf verwalteten Citrix ADC-Instanzen konfiguriert sind. Sie können konsolidierte Berichte aller Entitäten anzeigen. Mit diesen Berichten können Sie Folgendes auf höchster Ebene anzeigen:

- Citrix ADC-Instanzen
- Lastenausgleich virtueller Server
- Admin-Partitionen
- Services
- Servicegruppen

Der konsolidierte Bericht hilft Ihnen, eine Zuordnung zwischen diesen Entitäten zu erstellen. Weitere Informationen: Erstellen von Berichten für Lastausgleich-Entitäten

[663174]

Speichern von Variablenwerten, wenn ein Konfigurationsauftrag zur späteren Ausführung gespeichert wird

Beim Erstellen von Konfigurationsjobs können Sie Variablenwerte angeben, speichern und führen den Auftrag jedoch später oder planen, dass der Auftrag später ausgeführt wird. In einem solchen Szenario behält Citrix ADM nun die Variablenwerte in gespeicherten Aufträgen bei.

[637830]

Unterstützung für benutzerdefinierten SSH-Port für Citrix ADC-Instanzen

Sie können nun einen benutzerdefinierten SSH-Port für die Kommunikation zwischen Citrix ADM und den Citrix ADC-Instanzen angeben.

So legen Sie den SSH-Port für die Instanzprofile fest

1. Melden Sie sich mit einem unterstützten Webbrowser bei Citrix ADM an.
2. Navigieren Sie zu **Netzwerke**, und wählen Sie den Instanztyp der Citrix ADC-Instanz aus, die Sie in Citrix ADM ermitteln möchten.
3. Klicken Sie auf **Profile**.
4. Klicken Sie auf der Seite **Admin-Profile** auf **Hinzufügen**.
5. Geben Sie in **SSH-Port** die konfigurierte benutzerdefinierte SSH-Port für Citrix ADC-Instanzen für die Kommunikation mit Citrix ADM ein.
6. Klicken Sie auf **OK**.

[689369]

Behobene Probleme

Die folgenden Probleme wurden in dieser Version behoben.

Agent

Standardmäßig hat nur der Superadministrator-Benutzer (der erste Benutzer Ihrer Organisation, der sich registriert und sich bei Citrix ADM anmeldet) die Berechtigung, den Aktivierungscode zu generieren, der für die Registrierung eines Agenten beim Dienst erforderlich ist. Ein delegierter Administrator (jeder nachfolgende Benutzer, der sich anmeldet) verfügt nicht über die Berechtigung, den Aktivierungscode zu generieren. Wenn ein delegierter Administrator auf Aktivierungscode generieren klickt, wird der folgende Fehler angezeigt: “Nicht autorisiert, diesen Vorgang auszuführen. “
[690576]

Anwendungsanalyse und -verwaltung

Application Dashboard in Citrix ADM zeigt falsche Sicherheitsmetriken für benutzerdefinierte Anwendungen an.

[689041]

Netzwerke

- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden SNMP-Traps nicht an externe Trap-Ziele gesendet.
  [689018]
- Wenn Sie eine Regel konfigurieren, um bestimmte Ereignisse in Citrix ADM zu überwachen, wird kein Auftrag für die Ereignisse ausgeführt, die den von Ihnen angegebenen Filterkriterien entsprechen. [688986]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden Ereignisse für den konfigurierten Zeitraum nicht unterdrückt. [688988]
- Wenn Sie eine Gruppe in Citrix ADM unter Einstellungen > Benutzerverwaltung > Gruppe erstellen, wird die Erfolgsmeldung angezeigt, die darüber informiert, dass die Gruppe erstellt wird, bevor alle Schritte im Assistenten abgeschlossen sind. [684944]

Bekannte Probleme

In diesem Release bestehen die folgenden bekannten Probleme:

Agent

- Wenn Sie einen Agenten verwenden, der in der Microsoft Azure-Cloud bereitgestellt wird, werden die verwalteten Instanzen, die diesem Agent zugeordnet sind, in der Citrix ADM GUI im Status Heruntergefahren angezeigt. [690941]
- Nachdem die Agentenregistrierung abgeschlossen ist, können Sie sich möglicherweise nicht über die Hypervisor Konsole am Agent anmelden.
  Problemumgehung: Melden Sie sich mit einem SSH-Client beim Agenten an. [691181]

Analytics

- In bestimmten Fällen werden HDX Insight - und Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut. [690327]

Netzwerke

- Wenn der Kontrollproxy während des Startvorgangs des Agenten nicht verfügbar ist, kann der Agent die SNMP-Trapeinstellungen von Citrix ADM nicht abrufen, und alle Traps, die von Citrix ADC-Instanzen empfangen wurden, werden gelöscht.
  Problemumgehung: Wird `masd restart` auf dem Agenten ausgeführt, wenn die Verbindung mit Citrix ADM hergestellt wurde. [687027]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden keine E-Mails für die Ereignisse gesendet, die den Filterkriterien entsprechen. [688985]
- Upgrade der Citrix ADC Funktion in Wartungsaufgaben wird in Citrix ADM nicht unterstützt. Sie können die Option jedoch immer noch in der GUI anzeigen. [689068]

On-Boarding

- Nachdem Sie einen neuen Mandanten in Citrix ADM einbauen und auf die Schaltfläche Verwalten klicken, wird möglicherweise der Fehler Seite funktioniert nicht zum ersten Mal angezeigt.
  Problemumgehung:
  Warten Sie eine Stunde (60 Minuten), und melden Sie sich erneut an. Die Verzögerung ist auf die Zeit zurückzuführen, die für die Provisioning des neuen Mandanten in Anspruch genommen wird. 691018[]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen. [689330]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]

> **Hinweis** [XXXXXX] Labels sind interne Tracking-IDs, die vom Citrix ADM Team verwendet werden.

23. Juli 2017

Dies ist eine Fehlerkorrektur-Version. Es gibt keine neuen Funktionen in dieser Version.

Behobene Probleme

Die folgenden Probleme wurden in dieser Version behoben.

Citrix Cloud

Nach der Anmeldung bei citrix.cloud.com, klicken Sie auf die Schaltfläche **Verwalten** auf der Citrix ADM -Kachel zeigt die folgende Fehlermeldung Seite nicht verfügbar.
[690267]

Netzwerke

Wenn Sie den Secure Only Zugriff auf Ihre Citrix ADC-Instanzen aktiviert haben, werden diese Instanzen in Citrix ADM nicht ordnungsgemäß erkannt, und der Status wird möglicherweise als Out of Service angezeigt, nachdem der Erkennungsprozess abgeschlossen ist.
[690431]

Bekannte Probleme

In diesem Release bestehen die folgenden bekannten Probleme:

Agent

- Wenn Sie einen Agenten verwenden, der in der Microsoft Azure-Cloud bereitgestellt wird, werden die verwalteten Instanzen, die diesem Agent zugeordnet sind, in der Citrix ADM GUI im Status Heruntergefahren angezeigt. [690941]
- Nachdem die Agentenregistrierung abgeschlossen ist, können Sie sich möglicherweise nicht über die Hypervisor Konsole am Agent anmelden.
  Problemumgehung: Melden Sie sich mit einem SSH-Client beim Agenten an. [691181]
- Standardmäßig hat nur der Superadministrator-Benutzer (der erste Benutzer Ihrer Organisation, der sich registriert und sich bei Citrix ADM anmeldet) die Berechtigung, den Aktivierungscode zu generieren, der für die Registrierung eines Agenten beim Dienst erforderlich ist. Ein delegierter Administrator (jeder nachfolgende Benutzer, der sich anmeldet) verfügt nicht über die Berechtigung, den Aktivierungscode zu generieren. Wenn ein delegierter

Administrator auf **Aktivierungscode generieren**klickt, wird der folgende Fehler angezeigt: Nicht autorisiert, um diesen Vorgang auszuführen.
Problemumgehung: Superadministrator muss dem delegierten Administrator die erforderlichen Berechtigungen zuweisen. Einzelheiten finden Sie unter Zuweisen zusätzlicher Berechtigungen für delegierte Administratorbenutzer. [690576]

Analytics

- In bestimmten Fällen werden HDX Insight - und Gateway Insight-Knoten möglicherweise nicht auf der Citrix ADM GUI angezeigt.
  Problemumgehung: Aktualisieren Sie die Seite und versuchen Sie es erneut. [690327]

Anwendungsanalyse und -verwaltung

- Wenn Sie den Safari-Browser unter Microsoft Windows-Betriebssystem verwenden, werden App Dashboard und Security Analytics Dashboard nicht geladen. Sie können andere Funktionen von Citrix ADM sehen. [688617]
- Application Dashboard in Citrix ADM zeigt falsche Sicherheitsmetriken für benutzerdefinierte Anwendungen an. [689041]

Netzwerke

- Wenn der Kontrollproxy während des Startvorgangs des Agenten nicht verfügbar ist, kann der Agent die SNMP-Trapeinstellungen von Citrix ADM nicht abrufen, und alle Traps, die von Citrix ADC-Instanzen empfangen wurden, werden gelöscht.
  Problemumgehung: Wird `masd restart` auf dem Agenten ausgeführt, wenn die Verbindung mit Citrix ADM hergestellt wurde. [687027]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden keine E-Mails für die Ereignisse gesendet, die den Filterkriterien entsprechen. [688985]
- Wenn Sie eine Regel konfigurieren, um bestimmte Ereignisse in Citrix ADM zu überwachen, wird kein Auftrag für die Ereignisse ausgeführt, die den von Ihnen angegebenen Filterkriterien entsprechen. [688986]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden Ereignisse für den konfigurierten Zeitraum nicht unterdrückt. [688988]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden SNMP-Traps nicht an externe Trap-Ziele gesendet. [689018]
- Upgrade der Citrix ADC Funktion in Wartungsaufgaben wird in Citrix ADM nicht unterstützt. Sie können die Option jedoch immer noch in der GUI anzeigen. [689068]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen. [689330]
- Möglicherweise werden Sie abrupt von Citrix ADM abgemeldet.
  Problemumgehung: Melden Sie sich neu bei Citrix ADM an. [689012]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]

> **Hinweis** [XXXXXX] Labels sind interne Tracking-IDs, die vom Citrix ADM Team verwendet werden.

16. Juli 2017

Dies ist eine Fehlerkorrektur-Version. Es gibt keine neuen Funktionen in dieser Version.

Behobene Probleme

Die folgenden Probleme wurden in diesem Release behoben:

Analytics

- Wenn Sie den Citrix ADM-Agenten in AWS (AWS) verwenden, werden Analysedaten nicht angezeigt, da das Telemetrie-Paket, das ULFD-Funktionen enthält, im AMPI des Agenten fehlt. [690225]
- Das Exportieren von Berichten in PDF/JPEG/PNG funktioniert in Citrix ADM nicht. [683778]
- Wenn Sie Insight von Citrix ADM aktivieren, wird das Häkchen neben AppFlow nicht aktiviert angezeigt. Die Konfiguration zum Aktivieren von AppFlow wird jedoch an Citrix ADC-Instanzen übertragen. [688309]

Netzwerke

- Sie können keine Befehlsdatei hochladen, während Sie einen Konfigurationsauftrag erstellen, obwohl **Netzwerke** > **Konfigurationsaufträge** > **Auftrag erstellen** die Option zum Hochladen einer Datei anzeigt.
  [688967]
- Die Agentenregistrierung schlägt fehl, wenn Sie den Groß-/Kleinschreibung im Kundennamen verwenden. Zum Beispiel `Haroldmas`: `kimiRKN`.
  [689648]

Bekannte Probleme

In diesem Release bestehen die folgenden bekannten Probleme:

Anwendungsanalyse und -verwaltung

- Wenn Sie den Safari-Browser unter Microsoft Windows-Betriebssystem verwenden, werden App Dashboard und Security Analytics Dashboard nicht geladen. Sie können andere Funktionen von Citrix ADM sehen. [688617]
- Application Dashboard in Citrix ADM zeigt falsche Sicherheitsmetriken für benutzerdefinierte Anwendungen an. [689041]

Netzwerke

- Wenn der Kontrollproxy während des Startvorgangs des Agenten nicht verfügbar ist, kann der Agent die SNMP-Trapeinstellungen von Citrix ADM nicht abrufen, und alle Traps, die von Citrix ADC-Instanzen empfangen wurden, werden gelöscht.
  Problemumgehung: Wird `masd restart` auf dem Agenten ausgeführt, wenn die Verbindung mit Citrix ADM hergestellt wurde. [687027]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden keine E-Mails für die Ereignisse gesendet, die den Filterkriterien entsprechen. [688985]
- Wenn Sie eine Regel konfigurieren, um bestimmte Ereignisse in Citrix ADM zu überwachen, wird kein Auftrag für die Ereignisse ausgeführt, die den von Ihnen angegebenen Filterkriterien entsprechen. [688986]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden Ereignisse für den konfigurierten Zeitraum nicht unterdrückt. [688988]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden SNMP-Traps nicht an externe Trap-Ziele gesendet. [689018]
- Upgrade der Citrix ADC Funktion in Wartungsaufgaben wird in Citrix ADM nicht unterstützt. Sie können die Option jedoch immer noch in der GUI anzeigen. [689068]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen. [689330]
- Möglicherweise werden Sie abrupt von Citrix ADM abgemeldet.
  Problemumgehung: Melden Sie sich erneut bei Citrix ADM an. [689012]
- Wenn Sie die Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM unter **Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]

> **Hinweis** [XXXXXX] Labels sind interne Tracking-IDs, die vom Citrix ADM Team verwendet werden.

30. Juni 2017

Dies ist die erste Version von Citrix ADM. Eine Liste der verfügbaren Funktionen finden Sie unterFunktionen und Lösungen.

In diesem Release bestehen die folgenden bekannten Probleme:

Analytics

- Das Exportieren von Berichten in PDF/JPEG/PNG funktioniert in Citrix ADM nicht. [683778]
- Wenn Sie Insight von Citrix ADM aktivieren, wird das Häkchen neben AppFlow nicht aktiviert angezeigt. Die Konfiguration zum Aktivieren von AppFlow wird jedoch an Citrix ADC-Instanzen übertragen. [688309]

Anwendungsanalyse und -verwaltung

- Wenn Sie den Safari-Browser unter Microsoft Windows-Betriebssystem verwenden, werden App Dashboard und Security Analytics Dashboard nicht geladen. Sie können andere Funktionen von Citrix ADM sehen. [688617]
- Application Dashboard in Citrix ADM zeigt falsche Sicherheitsmetriken für benutzerdefinierte Anwendungen an. [689041]

Netzwerke

- Wenn der Kontrollproxy während des Agentenstartvorgangs nicht verfügbar ist, kann der Agent die SNMP-Trap-Einstellungen von Citrix ADM nicht abrufen, und alle Traps, die von Citrix ADC-Instanzen empfangen werden, werden gelöscht.
  Problemumgehung: Wird `masd restart` auf dem Agenten ausgeführt, wenn die Verbindung mit Citrix ADM hergestellt wurde. [687027]
- Sie können keine Befehlsdatei hochladen, während Sie einen Konfigurationsauftrag erstellen, obwohl **Netzwerke** > **Konfigurationsaufträge** > **Auftrag erstellen** die Option zum Hochladen einer Datei anzeigt. [688967]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden keine E-Mails für die Ereignisse gesendet, die den Filterkriterien entsprechen. [688985]
- Wenn Sie eine Regel konfigurieren, um bestimmte Ereignisse in Citrix ADM zu überwachen, wird der Auftrag nicht für die Ereignisse ausgeführt, die den von Ihnen angegebenen Filterkriterien entsprechen. [688986]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden Ereignisse für den konfigurierten Zeitraum nicht unterdrückt. [688988]
- Wenn Sie eine Regel zum Überwachen bestimmter Ereignisse in Citrix ADM konfigurieren, werden SNMP-Traps nicht an externe Trap-Ziele gesendet. [689018]
- Upgrade der Citrix ADC Funktion in Wartungsaufgaben wird in Citrix ADM nicht unterstützt. Sie können die Option jedoch immer noch in der GUI anzeigen. [689068]

Einstellungen

- Auf der Seite **Einstellungen** > **Abonnements** kann der Speicherdatenverbrauch höher als das berechtigte Speicherlimit von 5 GB erscheinen. [689330]
- Möglicherweise werden Sie abrupt von Citrix ADM abgemeldet.
  Problemumgehung: Melden Sie sich erneut bei Citrix ADM an. [689012]
- Wenn Sie Benutzer aus Citrix Cloud löschen, werden die gelöschten Benutzernamen weiterhin in Citrix ADM **unter Einstellungen** > **Benutzerverwaltung** > **Benutzer** angezeigt. [686581]

> **Hinweis** [XXXXXX] Labels sind interne Tracking-IDs, die vom Citrix ADM Team verwendet werden.

Erste Schritte

April 28, 2021

In diesem Dokument erfahren Sie, wie Sie mit dem Onboarding und dem erstmaligen Einrichten von Citrix Application Delivery Management (Citrix ADM) beginnen. Dieses Dokument richtet sich an Netzwerk- und Anwendungsadministratoren, die Citrix Netzwerkgeräte verwalten (Citrix ADC, SD-WAN WO, Citrix Gateway, Citrix Secure Web Gateway usw.). Befolgen Sie die Schritte in diesem Dokument, unabhängig vom Gerätetyp, das Sie mit Citrix ADM verwalten möchten.

Bevor Sie mit dem Onboarding beginnen, überprüfen Sie die Browser-Anforderungen, die Installationsanforderungen für Agenten und die Anschlussanforderungen.

Schritt 1: Registrieren für Citrix Cloud

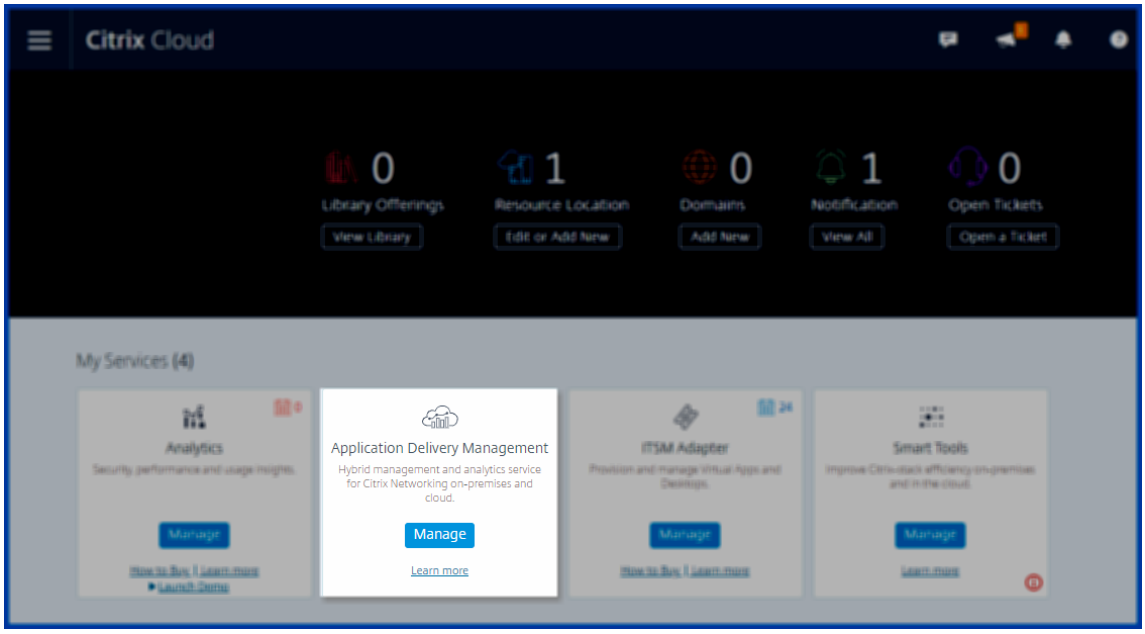
Um Citrix ADM zu verwenden, müssen Sie zunächst ein Citrix Cloud-Unternehmenskonto erstellen oder einem vorhandenen Konto beitreten, das von einer anderen Person in Ihrem Unternehmen erstellt wurde. Ausführliche Prozesse und Anweisungen zum Vorgehen finden Sie unter Registrierung bei Citrix Cloud.

Schritt 2: Verwalten von Citrix ADM mit einem Express-Konto

Führen Sie nach der Anmeldung bei Citrix Cloud die folgenden Schritte aus:

1. Wechseln Sie zum Abschnitt **Verfügbare Dienste**.
2. Klicken Sie auf der Kachel **Anwendungsbereitstellungsverwaltung** auf **Verwalten**.

   Die Kachel **Anwendungsbereitstellungsverwaltung** wird in den Abschnitt **Meine Dienste** verschoben.

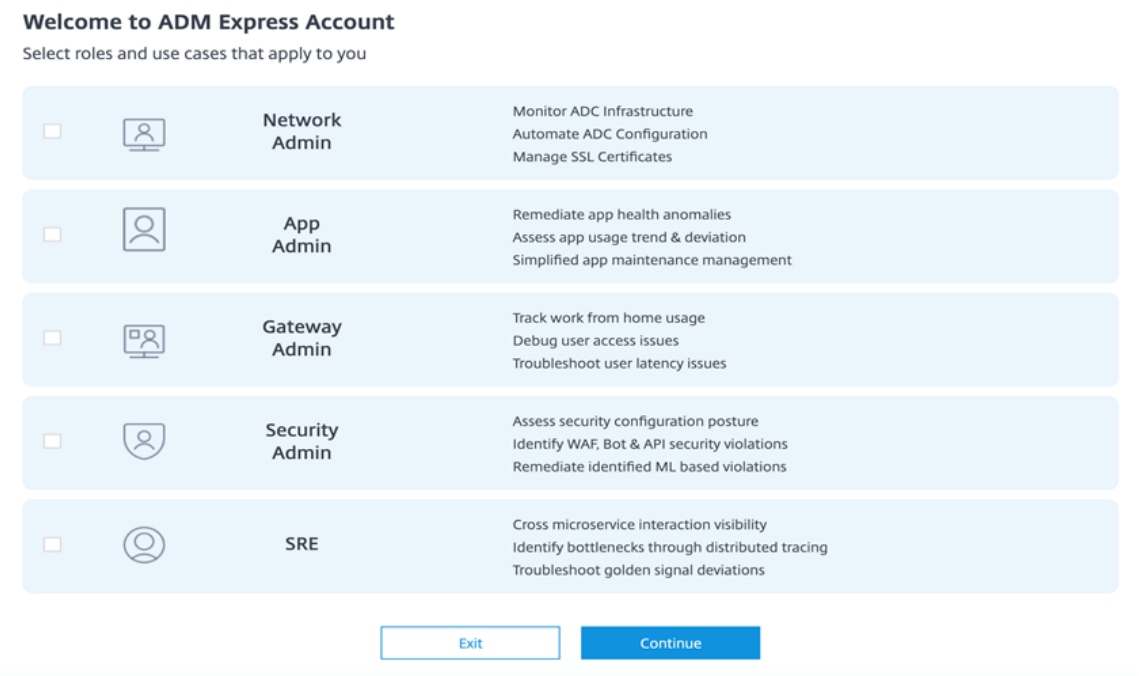


3. Wählen Sie eine der folgenden Regionen aus, die Ihren geschäftlichen Anforderungen entspricht:

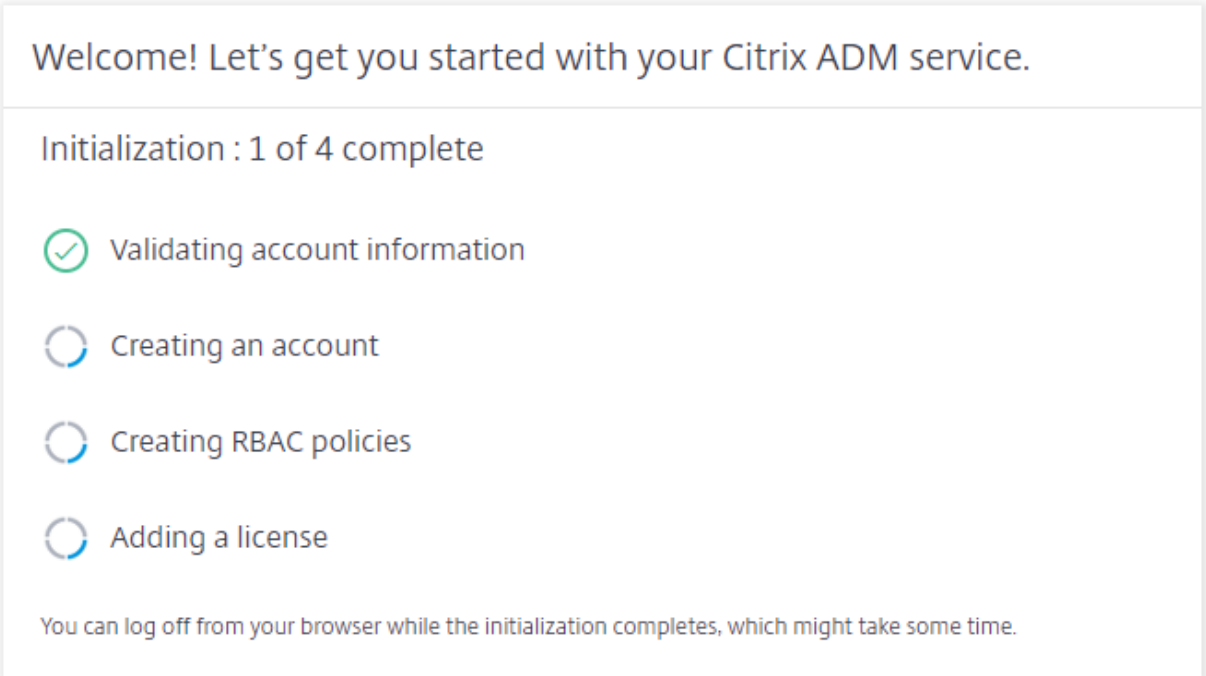
   - Vereinigte Staaten (US)
   - Europa (EU)
   - Australien (ANZ)

   > **Wichtig**
   >
   > Die Region kann später nicht geändert werden.

4. Wählen Sie Rollen und Anwendungsfälle aus, die auf Sie zutreffen.



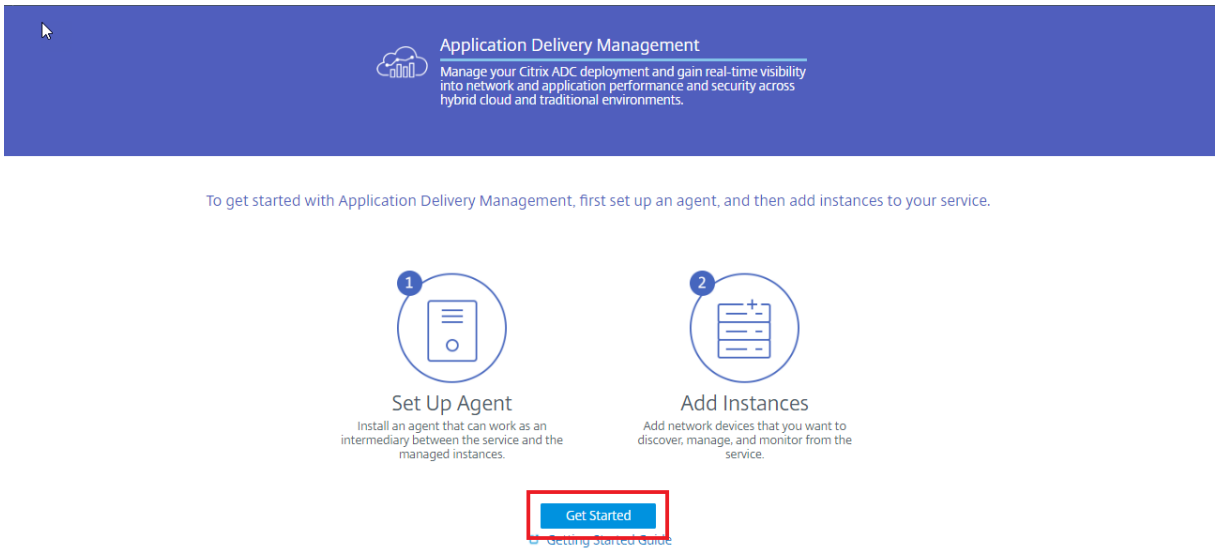
Sie können sich vom Browser abmelden, während die Initialisierung im Hintergrund abgeschlossen ist. Dies kann einige Zeit in Anspruch nehmen.



Hinweis

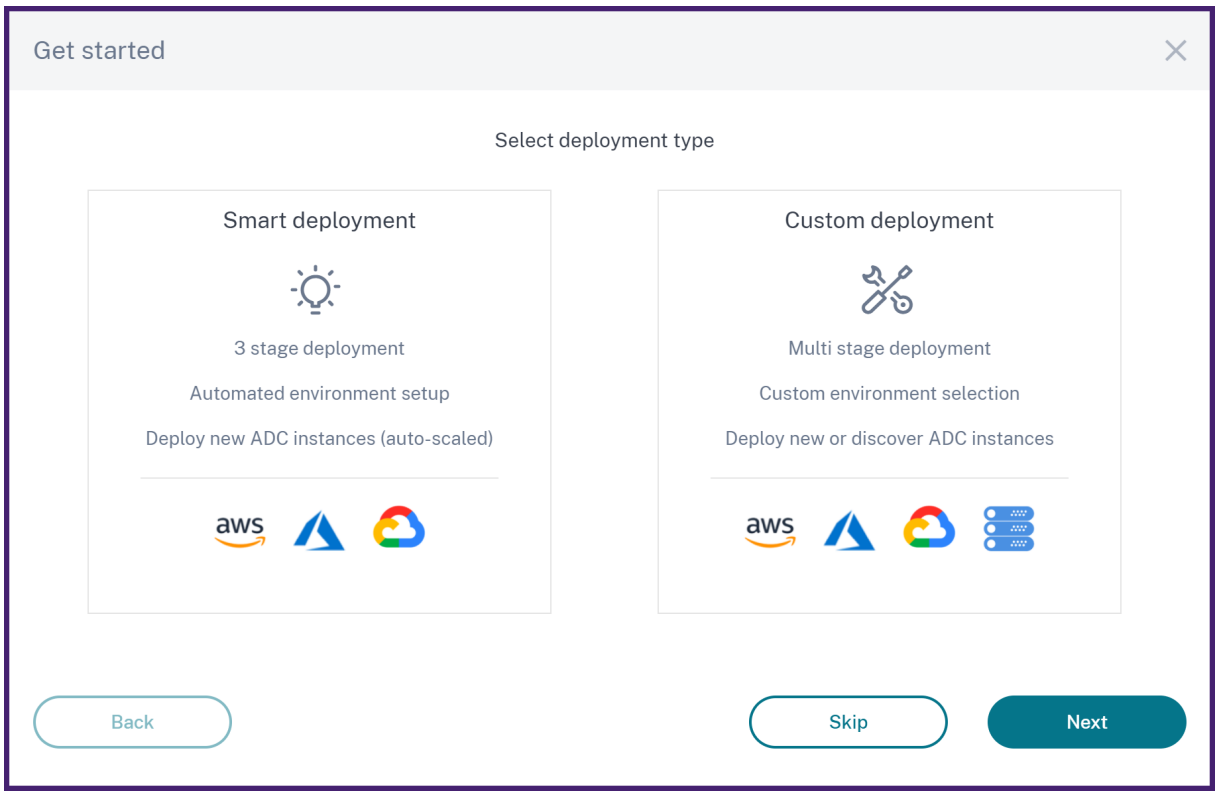
Citrix weist ein Express-Konto zur Verwaltung von ADM-Ressourcen zu. Wenn Ihr Citrix ADM Express-Konto 90 Tage lang inaktiv bleibt, wird das Konto gelöscht. Weitere Informationen finden Sie unter Verwalten von Citrix ADM Service mit Express-Konto.

Wenn Sie sich wieder bei Ihrem Citrix Cloud-Konto anmelden, wird das **Citrix ADM GUI-Fenster** angezeigt. Klicken Sie auf **Erste Schritte**, um den Dienst zum ersten Mal einzurichten.



Schritt 3: Auswählen eines ADC-Bereitstellungstyps

Wählen Sie eine der folgenden Bereitstellungsoptionen aus, die Ihren Geschäftsanforderungen entspricht:



- Smarte Bereitstellung - Diese Option ist ein automatisiertes Umgebungs-Setup zur Bereitstellung neuer ADC-Instanzen. Es wird automatisch ein Agent installiert, um die Kommunikation zwischen dem Citrix ADM und den verwalteten Instanzen zu ermöglichen.

  Diese Option unterstützt derzeit nur die AWS-Umgebung. In drei Schritten können Sie eine Anwendung bereitstellen, die in AWS mit ADC-Instanzen vorhanden ist.

- Benutzerdefinierter Einsatz - Diese Option ist eine mehrstufige Bereitstellung. Sie können jede Umgebungsoption auswählen und ADC-Instanzen bereitstellen oder ermitteln.

Wählen Sie eine intelligente Bereitstellung

Diese Bereitstellungsoption schafft die folgende Infrastruktur in AWS:

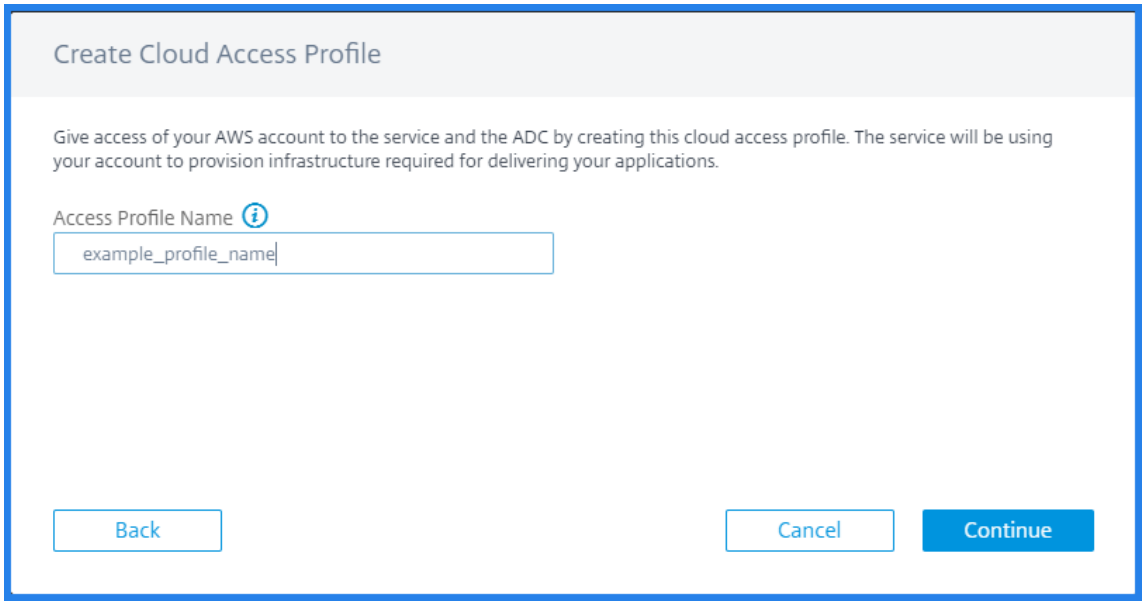
- Ein CloudFormation-Stack in AWS zum Erstellen der erforderlichen Infrastruktur, die Subnetze, Sicherheitsgruppen, NAT-Gateways usw. umfasst.
- Ein ADM-Agent in der VPC zur Verwaltung von ADC-Instanzen.
- Eine ADC Autoscale-Gruppe. Sie können diese Gruppe später auf der Seite **Netzwerke > Gruppe automatisch skalieren** anpassen.

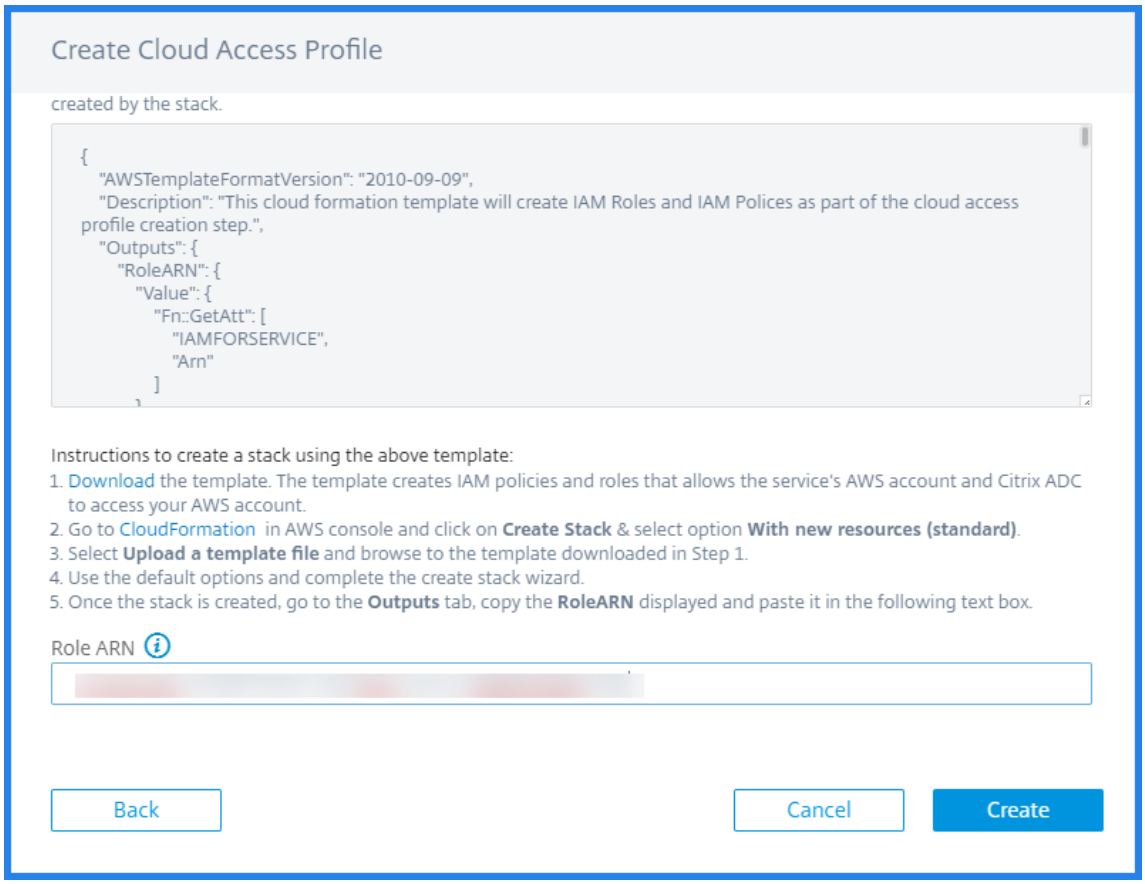
Stellen Sie vor der Bereitstellung von ADC-Instanzen Folgendes sicher:

1. Sie besitzen bereits ein AWS-Konto.
2. Sie haben einen IAM-Benutzer mit allen Administratorberechtigungen erstellt.

Um ADC-Instanzen bereitzustellen, führen Sie die folgenden Schritte aus:

1. Geben Sie **den Zugriffsprofilnamen und denRollen-ARN** an, um ein Cloud Access-Profil zu erstellen



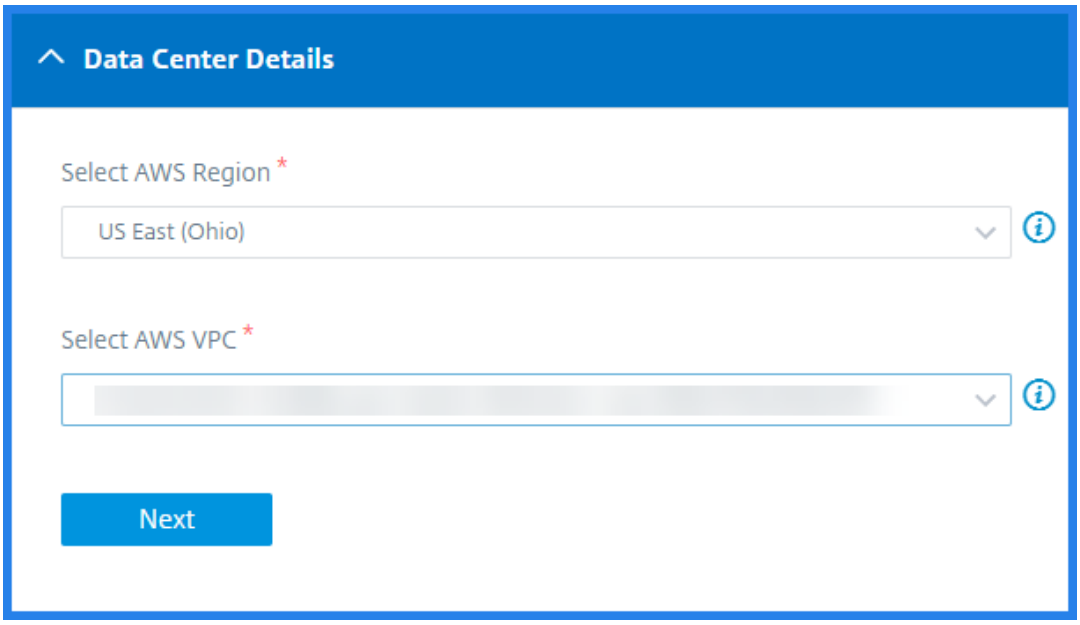


Der ADM-Dienst verwendet das Cloud Access-Profil, um auf ein AWS-Konto zuzugreifen.

2. Geben Sie die folgenden Details an, um die AWS-Umgebung vorzubereiten:

   a) Wählen Sie in **Data Center Details** die Option **AWS Region** und **AWS VPC** aus, in der Sie ADC-Instanzen bereitstellen möchten.

AWS VPC listet die in der ausgewählten **AWS-Region** vorhandenen VPCs auf.



b) Geben Sie in **ADC AutoScale Group Details** Folgendes für Autoscale ADC Instanzen in der AWS-Cloud an:

- **AutoScale Group Name** - Ein Name zur Identifizierung einer Autoscale-Gruppe.
- **Availability Zones** - Wählen Sie die Zonen aus, in denen Sie die Autoscale-Gruppen erstellen möchten.

  Sie können mehrere Zonen aus der Liste auswählen.
- **Bereitstellungstyp** - Wählen Sie entweder die Option **Bewertung** oder **Produktion** aus.

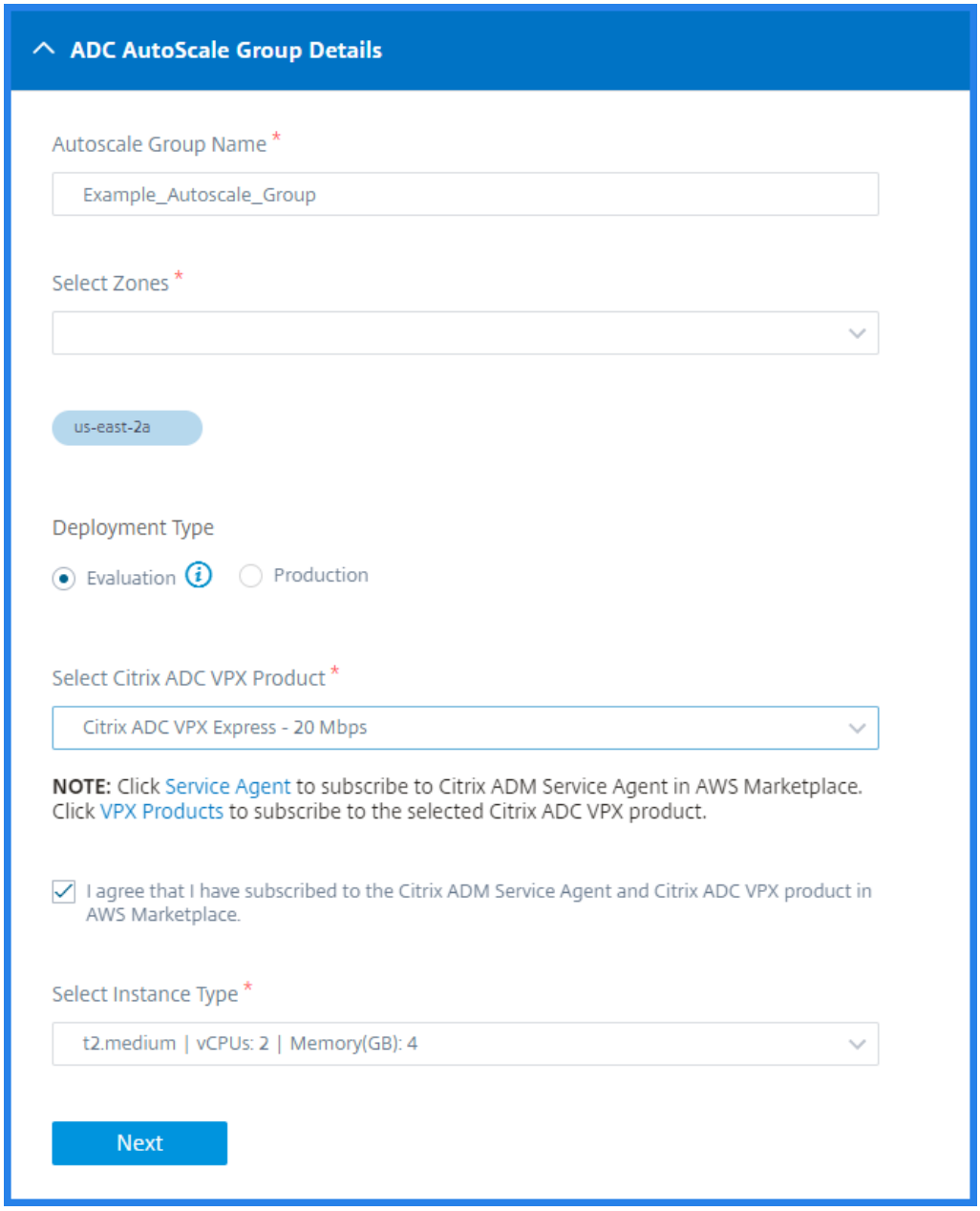
  Wenn Sie die ADM Autoscale-Lösung vor dem Kauf der Produktionslizenz bewerten möchten, wählen Sie die Option **Evaluierung** aus.

  > **Wichtig**
  >
  > – Die Evaluierungsoption unterstützt nur eine Availability Zone.
  > - Mit der Auswertungsoption können Sie nur Citrix ADC VPX Express auswählen. Und die ADM Autoscale-Lösung kann bis zu drei ADC-Instanzen skaliert werden.
- **Citrix ADC VPX Produkt** - Wählen Sie Lizenzen zur Bereitstellung von ADC-Instanzen aus.

  Abonnieren Sie die ausgewählte Lizenz auf der AWS-Marketplace-Site und kehren Sie zu dieser Seite zurück.

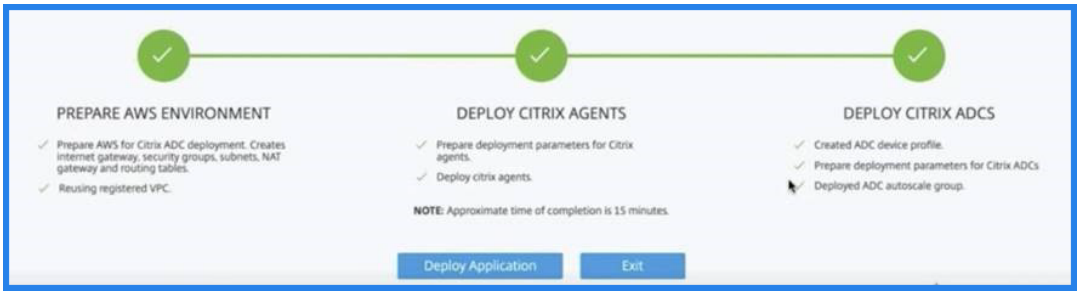
  Überprüfen Sie die Einwilligungsnachricht des Benutzers und wählen

- **Instanz-Typ** - Wählen Sie den erforderlichen Instanz-Typ aus.



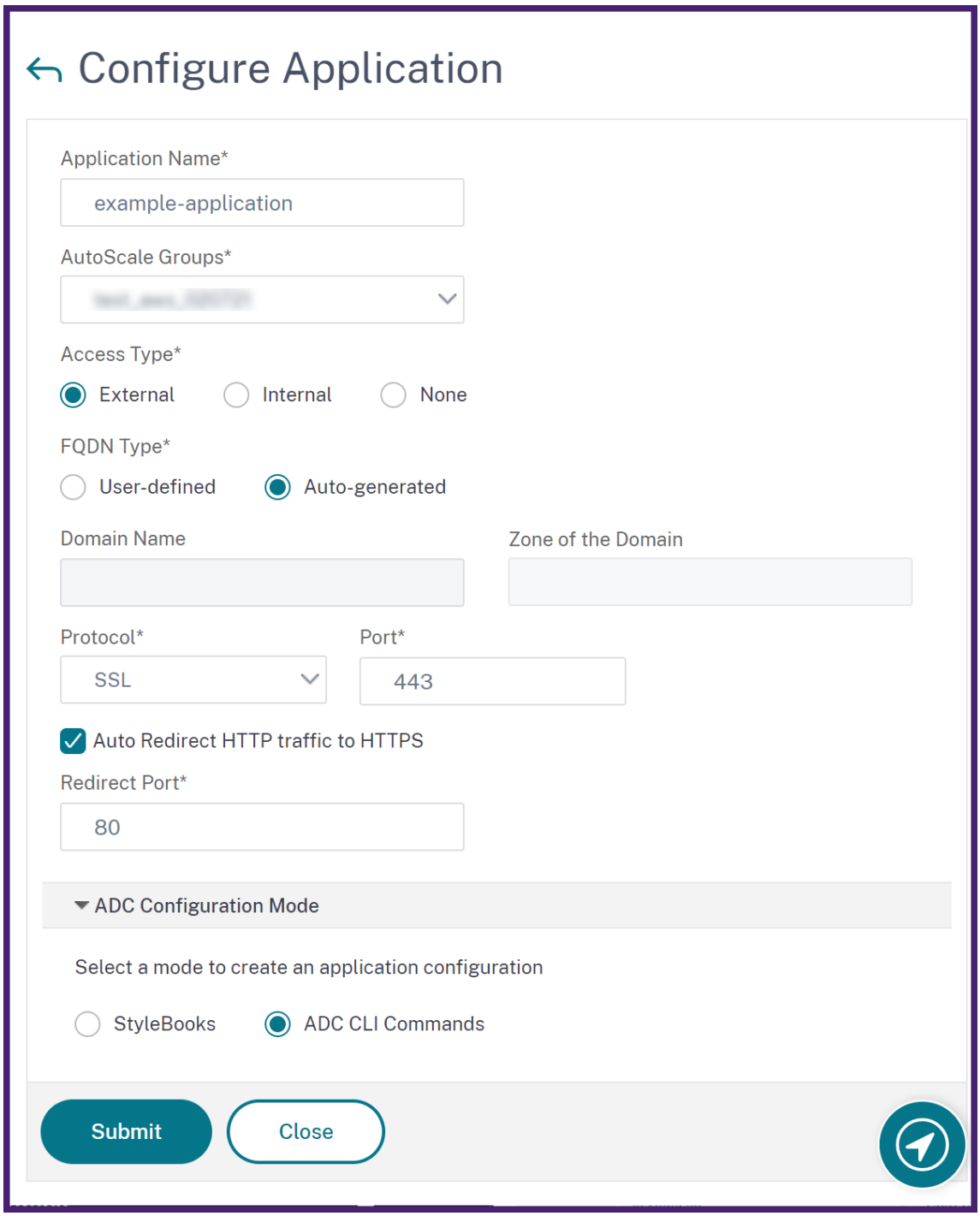
c) Klicken Sie auf **Weiter**.

Klicken Sie nach erfolgreicher Validierung auf **Erstellen**, um ADC-Instanzen in AWS bereitzustellen und eine Autoscale-Gruppe zu erstellen.

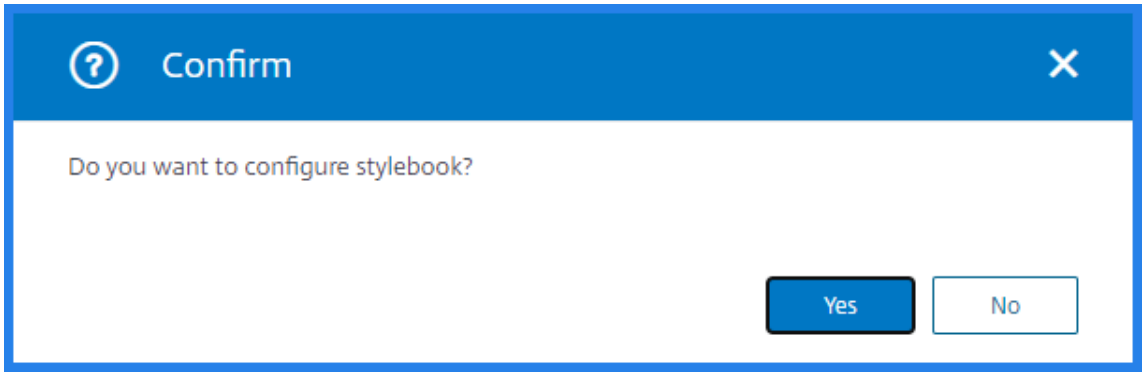


3. Klicken Sie nach der erfolgreichen ADC-Bereitstellung auf **Anwendung bereitstellen**.

   a) Geben Sie unter **Configure Application** die erforderlichen Details an und klicken Sie auf **Submit**.



Wenn Sie eine Anwendung mit StyleBooks konfigurieren möchten, wählen Sie im Bestätigungsfenster **Ja** aus.



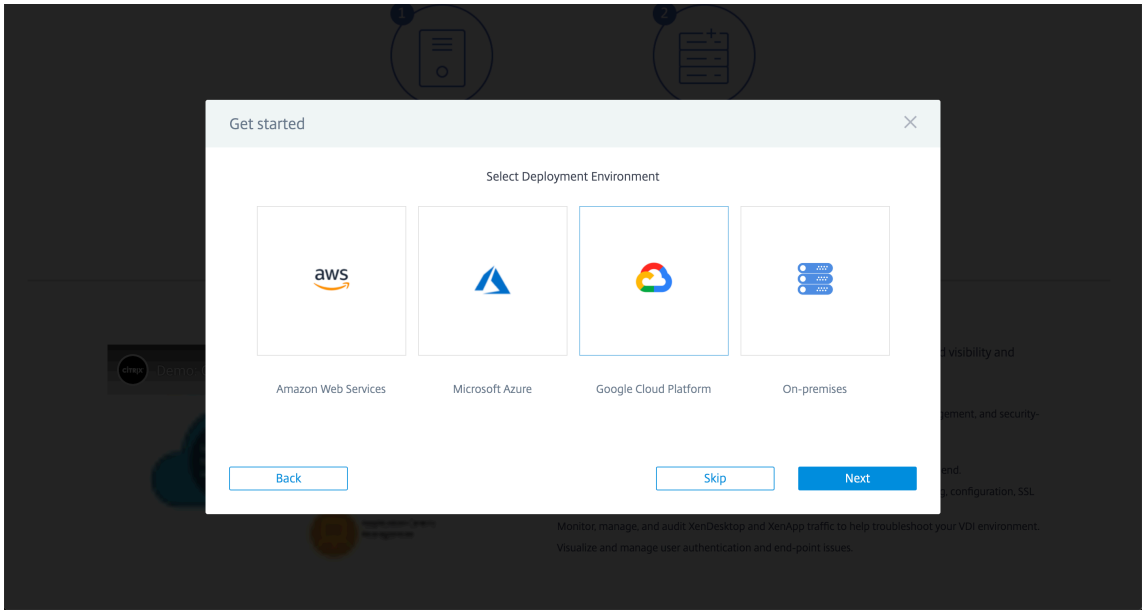
Weitere Informationen finden Sie unter Konfigurieren einer Anwendung für die Autoscale-Gruppe.

Wählen Sie eine benutzerdefinierte Bereitstellung

Diese Option bietet eine mehrstufige Bereitstellung. Wählen Sie diese Option, um ADC-Instanzen aus verschiedenen Umgebungen zu ermitteln. Mit dieser Option können Sie auch neue Instanzen bereitstellen, indem Sie benutzerdefinierte Umgebungsoptionen angeben.

Führen Sie die folgenden Schritte durch, um ADC-Instanzen bereitzustellen oder zu erkennen:

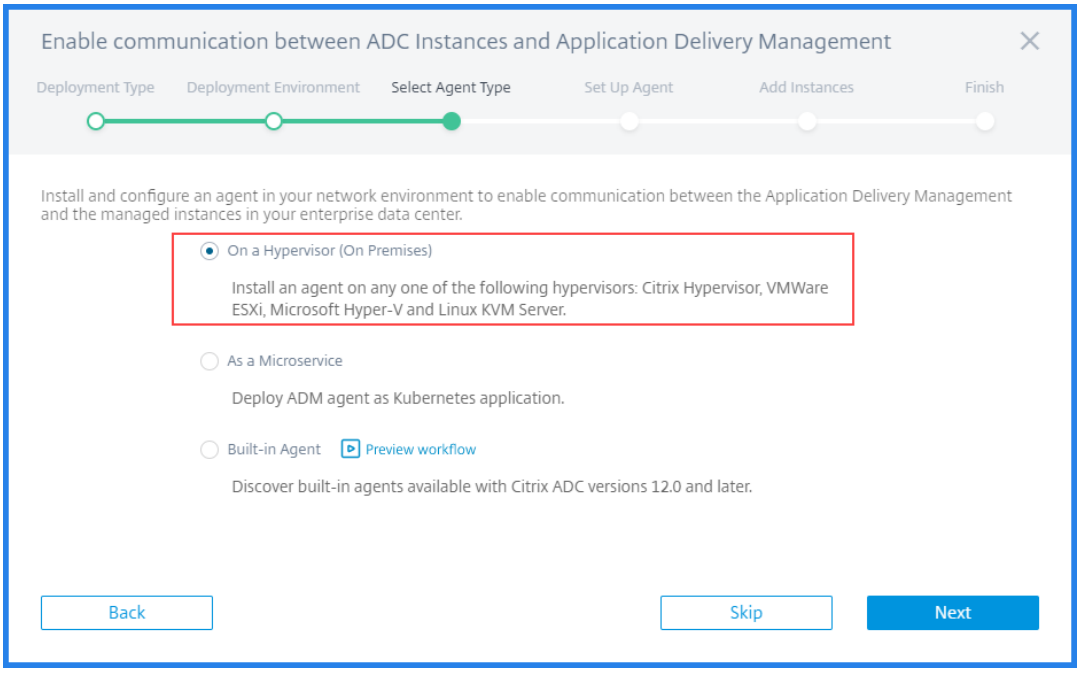
1. Wählen Sie eine der folgenden Umgebungen aus:
    - **Amazon Web Services**
    - **Microsoft Azure**
    - **Google Cloud Platform**
    - **On Premises**



2. Installieren Sie den Citrix ADM Agent, um die Kommunikation zwischen dem Citrix ADM und den verwalteten Instanzen in Ihrem Rechenzentrum oder Ihrer Cloud zu ermöglichen.

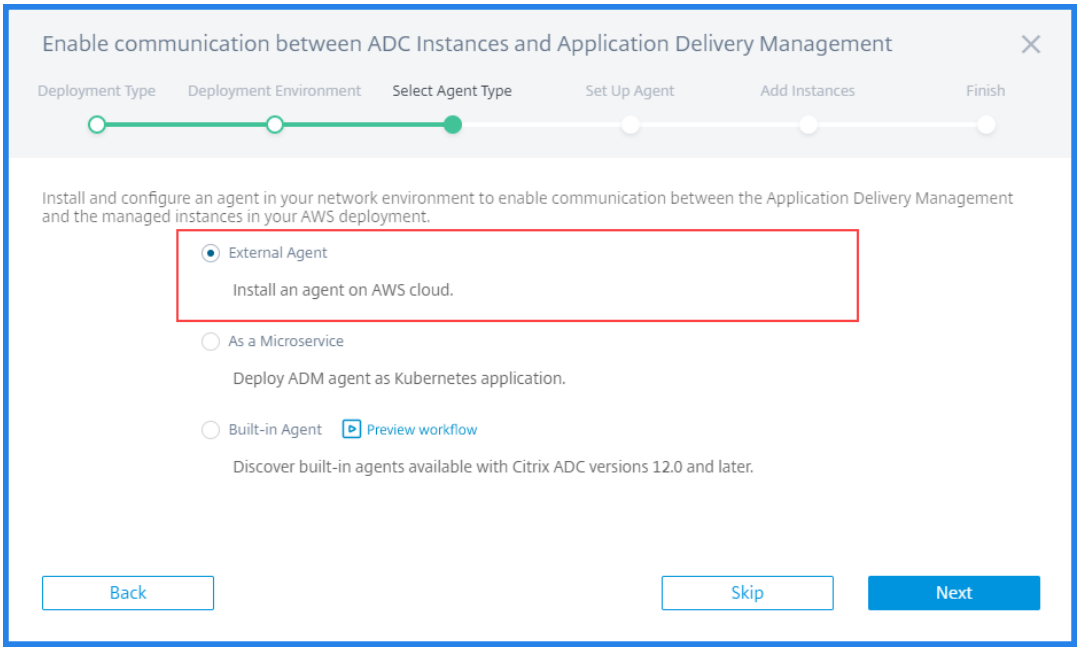
   Der Schritt **Agententyp auswählen** variiert die Agenteninstallationsoptionen je nach ausgewählter Umgebung.

   - **On-Premises** - Wenn Sie **On-Premises** auswählen, können Sie einen Agenten auf den folgenden Hypervisoren installieren:
     - Citrix Hypervisor
     - VMware ESXi
     - Microsoft Hyper-V
     - Linux KVM-Server

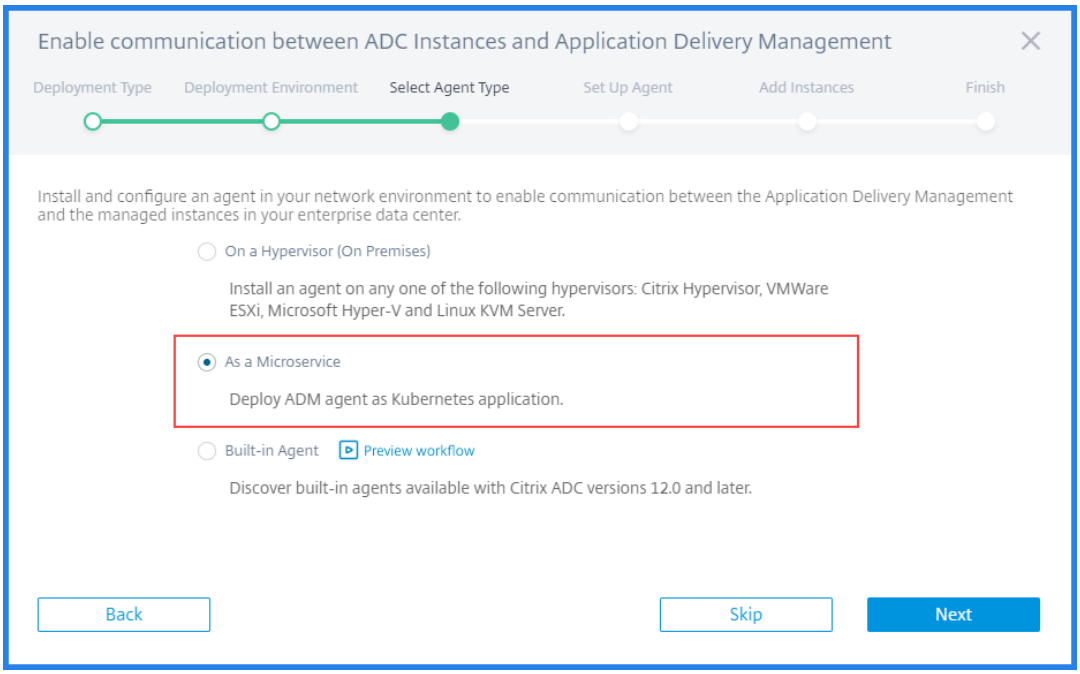


   - **Public Clouds** - Wenn Sie **Amazon Web Services**, **Microsoft Azure** oder **Google Cloud Platform**auswählen, können Sie einen Agenten extern in der ausgewählten Cloud installieren.

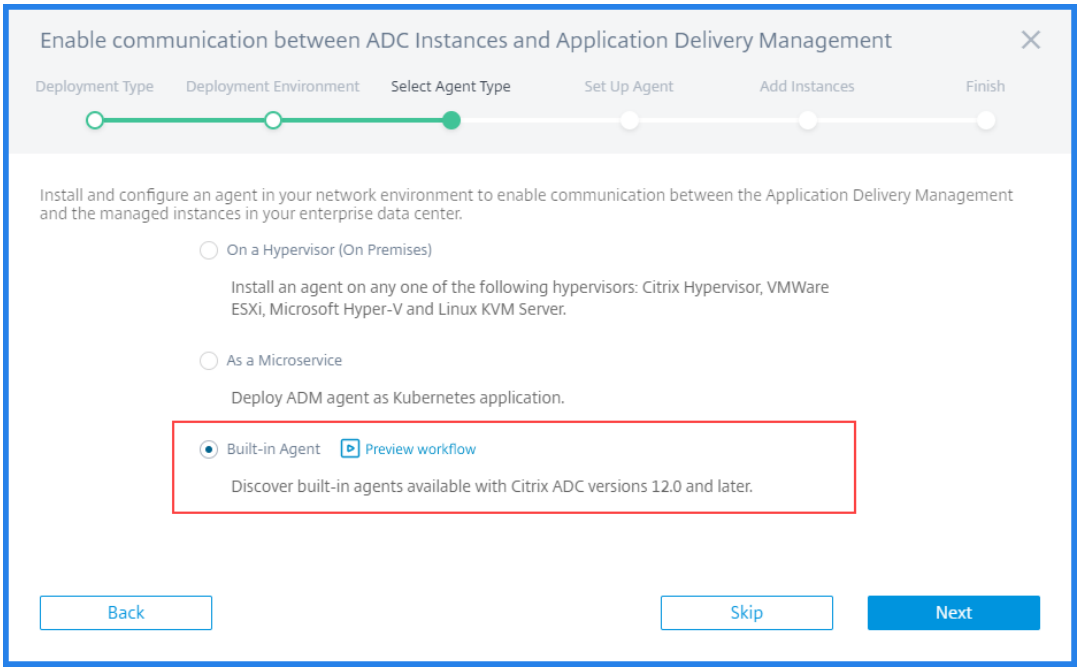
     Es folgt ein Beispiel für die AWS-Umgebung.



- **Als Microservice** - Um einen Agenten als Kubernetes-Anwendung bereitzustellen.



- **Eingebauter Agent** - Um integrierte Agenten zu ermitteln, die mit Citrix ADC Version 12.0 oder höher verfügbar sind.



3. Klicken Sie auf **Weiter**

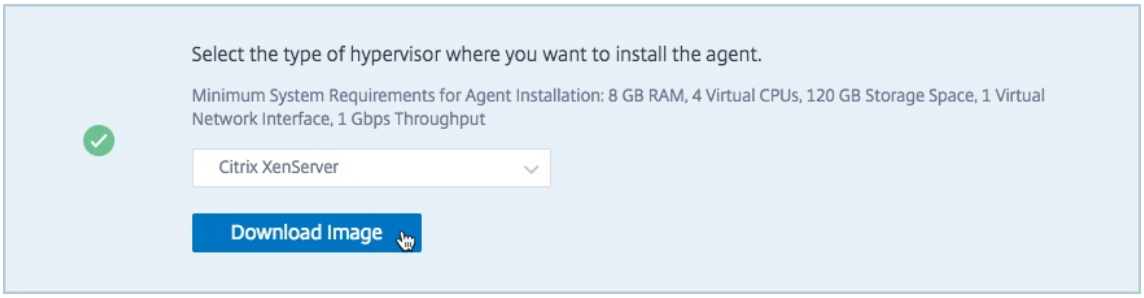
   Die Schritte zur Installation eines Agenten sind bei jeder Option unterschiedlich. Die folgenden Links führen Sie zu den spezifischen Schritten zur Installation eines Agenten:

   - Hypervisor
   - Externer Agent
   - Als Microservice
   - Integrierter Agent

Installieren eines Agenten auf einem Hypervisor

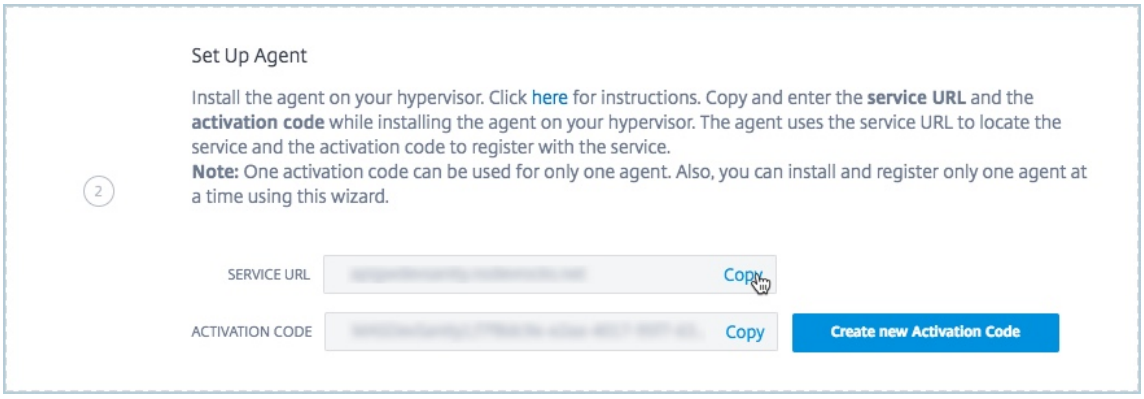
Führen Sie die folgenden Schritte aus, um einen ADM-Agenten auf einem Hypervisor einzurichten:

1. Wählen Sie den Hypervisor aus und klicken Sie auf **Image herunterladen**, um das Agenten-Image auf Ihr lokales System herunterzuladen.



   Eine Service-URL und ein Aktivierungscode werden generiert und auf der GUI angezeigt.

2. Kopieren Sie die Service-URL und einen Aktivierungscode.



3. Geben Sie die kopierte Dienst-URL und den Aktivierungscode an, während Sie den Agenten auf Ihrem Hypervisor installieren.

   Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren. Ausführliche Anweisungen zum Installieren eines Agenten auf dem lokalen Hypervisor finden Sie unterCitrix ADM Agent lokal installieren.

4. Kehren Sie nach erfolgreicher Agenteninstallation zur Seite " **Agenten einrichten** " zurück und klicken Sie auf **Agenten registrieren**.

Der nächste Schritt: Instanzen hinzufügen.

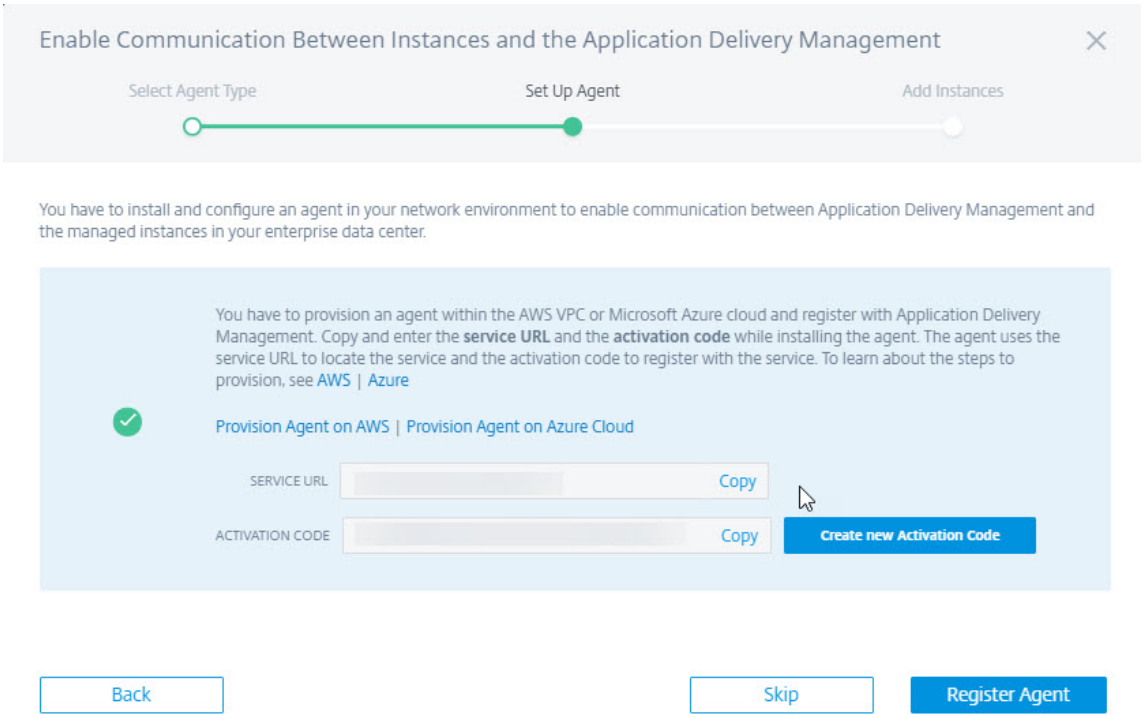
> **Hinweis**
>
> Wenn Sie während der Erstinstallation keine Agenten hinzufügen möchten, klicken Sie auf **Überspringen**, um die von Citrix ADM bereitgestellten Funktionen zu überprüfen. Sie können die Agenten und Instanzen später hinzufügen. Um später Agenten hinzuzufügen, navigieren Sie zu **Einstellungen > Agenten einrichten**. Anweisungen zum späteren Hinzufügen von Instanzen finden Sie unterInstanzen hinzufügen.

Installieren eines Agenten in einer öffentlichen Cloud

Sie müssen das Agent-Image nicht von der Seite **Agent einrichten** herunterladen. Das Agent-Image ist auf dem jeweiligen Cloud-Marktplatz verfügbar.

1. Kopieren und speichern Sie die Service-URL und den Aktivierungscode, der während der Agenteninstallation verwendet werden soll.

   Wenn Sie einen neuen Aktivierungscode wünschen, klicken Sie auf **Neuen Aktivierungscode erstellen**, kopieren und speichern Sie dann den Code, der während der Agenteninstallation verwendet werden soll.



- Ausführliche Anweisungen zum Installieren eines Agenten in der Microsoft Azure-Cloud finden Sie unterInstallieren von Citrix ADM Agent in Microsoft Azure Cloud.
- Ausführliche Anweisungen zum Installieren eines Agenten in AWS finden Sie unterInstallieren von Citrix ADM Agent in AWS.
- Detaillierte Anweisungen zur Installation eines Agenten in Google Cloud finden Sie unter Installieren Sie den Citrix ADM Agenten auf GCP.

2. Kehren Sie nach erfolgreicher Agenteninstallation zur Seite " **Agenten einrichten** " zurück und klicken Sie auf **Agenten registrieren**.

Der nächste Schritt: Instanzen hinzufügen.

Installieren eines Agenten als Microservice

Sie können einen Citrix ADM-Agenten als Microservice im Kubernetes-Cluster bereitstellen, um das **Servicediagramm** in Citrix ADM anzuzeigen.

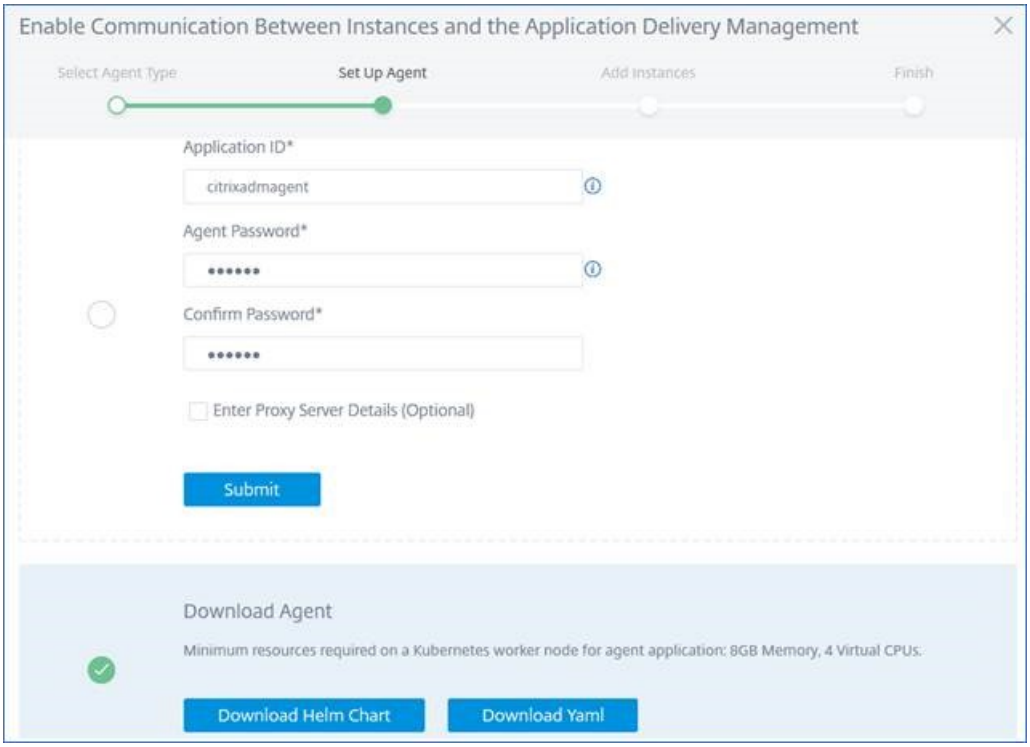
Weitere Informationen zum Einstieg in das Dienstdiagramm finden Sie unter Dienstdiagramm einrichten.

1. Geben Sie die folgenden Parameter an:

   a) **Anwendungs-ID** — Eine String-ID, mit der der Dienst für den Agenten im Kubernetes-Cluster definiert und dieser Agent von anderen Agenten im selben Cluster unterschieden wird.

b) **Agenten-Kennwort** — Geben Sie ein Kennwort an, mit dem CPX dieses Kennwort verwendet werden soll, um den CPX-zu-ADM-Dienst über den Agenten zu ermöglichen.

c) **Kennwort bestätigen** — Geben Sie dasselbe Kennwort zur Bestätigung an.



d) Klicken Sie auf **Senden**.

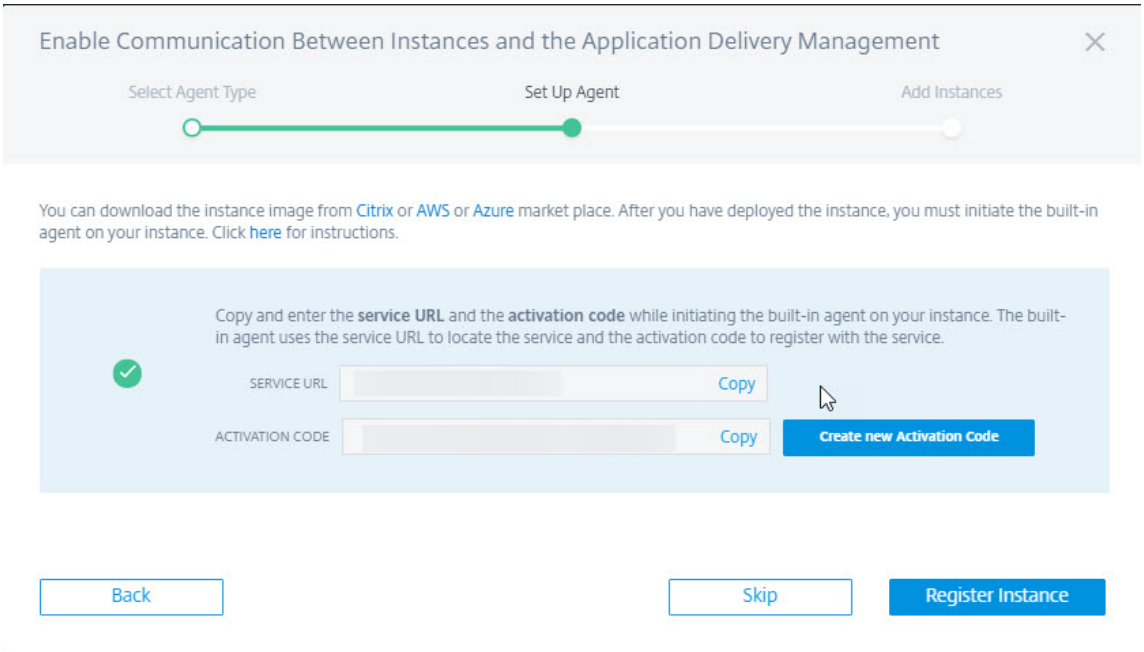
2. Nachdem Sie auf " **Senden**" geklickt haben, können Sie die YAML- oder Helm-Karte herunterladen.
3. Klicken Sie auf **Schließen**.

   Weitere Informationen finden Sie unter Installieren von Citrix ADM Agent im Kubernetes-Cluster.

Verwenden des integrierten Agents in der Citrix ADC-Instanz

Die Citrix ADC-Instanzen in Ihrer Umgebung enthalten einen integrierten Agenten. Sie können den integrierten Agenten initiieren und damit die Kommunikation zwischen der Instanz und Citrix ADM herstellen.

1. Kopieren Sie die generierte **Service-URL** und den **Aktivierungscode**. Speichern Sie sie, um sie beim Initiieren des integrierten Agents auf Ihrer Citrix ADC-Instanz zu verwenden.



Ausführliche Anweisungen zum Initiieren des integrierten Agents in der Citrix ADC-Instanz finden Sie unterInitiieren des integrierten Agents auf der Citrix ADC-Instanz.

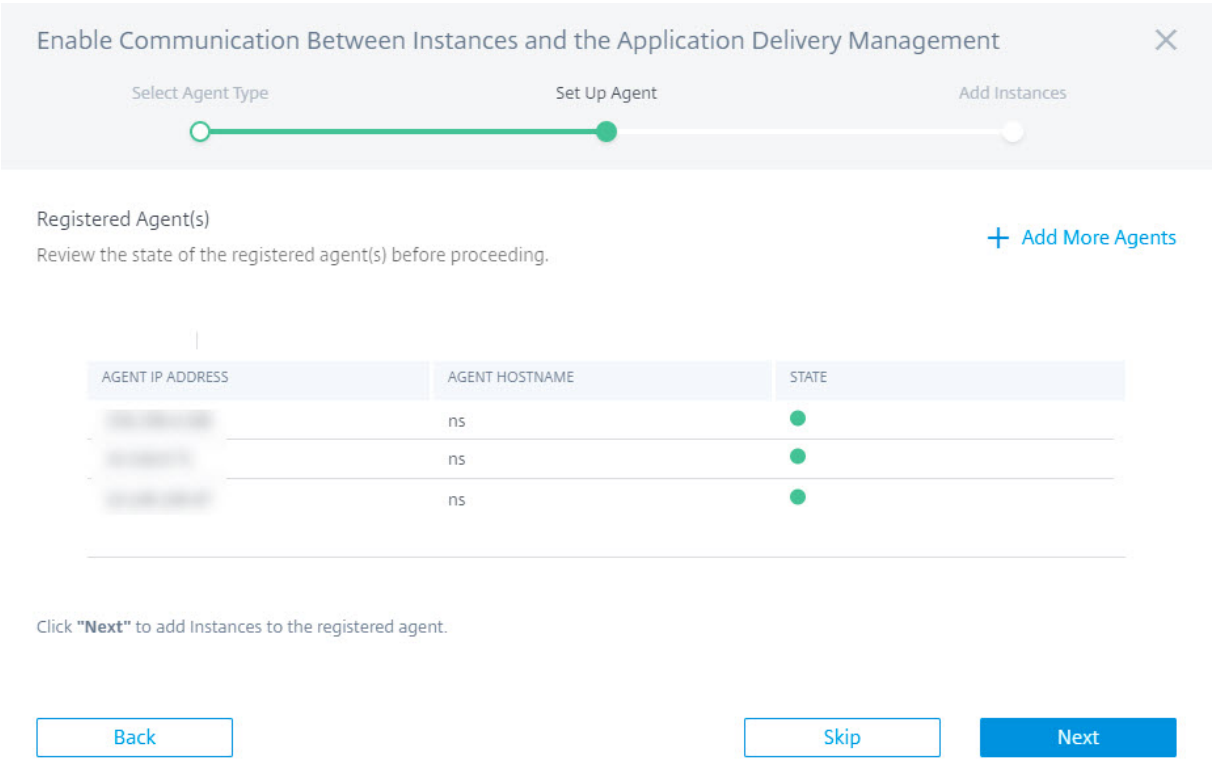
2. Nachdem der integrierte Agent initiiert wurde, kehren Sie zur Seite " **Agenten einrichten** " zurück und klicken Sie auf " **Instanz registrieren**".

Der nächste Schritt: Instanzen hinzufügen.

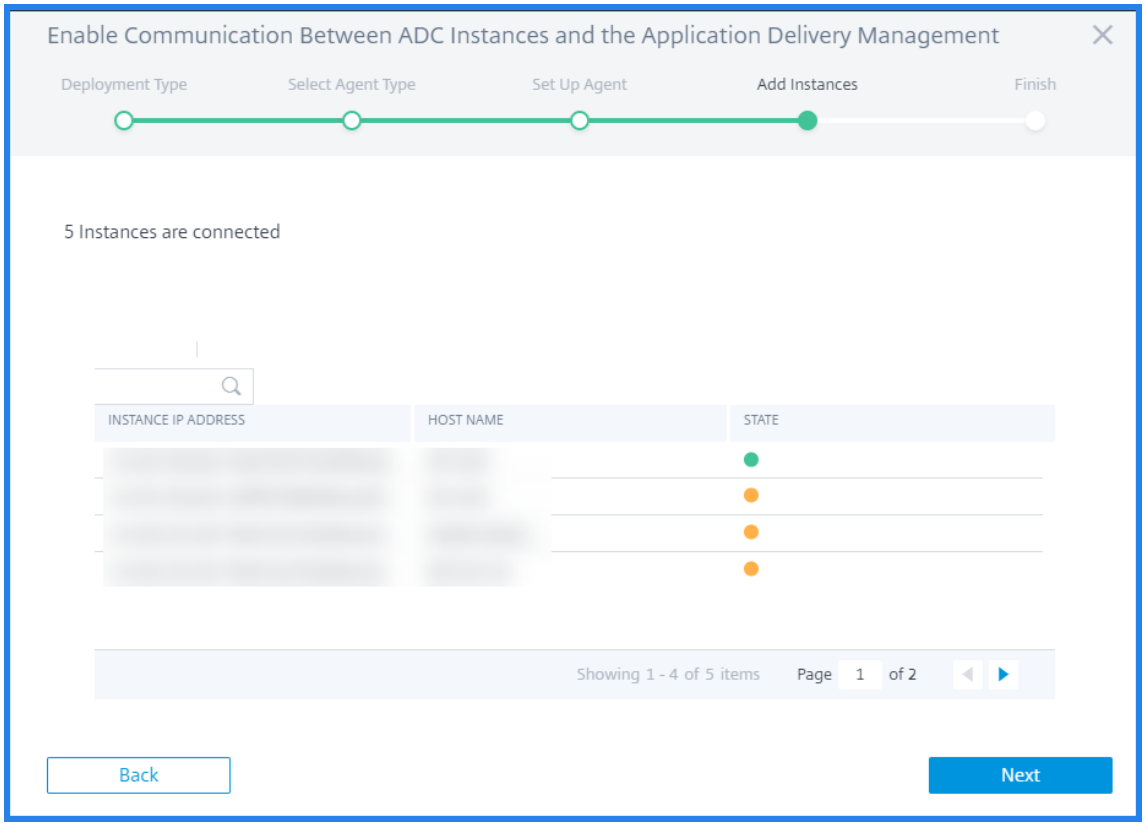
Hinzufügen von Instanzen zu Citrix ADM

Instanzen sind Netzwerk-Appliances oder virtuelle Appliances, die Sie von Citrix ADM aus ermitteln, verwalten und überwachen möchten. Um diese Instanzen zu verwalten und zu überwachen, müssen Sie die Instanzen dem Dienst hinzufügen.

Nach der erfolgreichen Agenteninstallation und -registrierung werden die Agenten auf der Seite " **Agent einrichten** " angezeigt. Wenn sich der Agent-Status im Status UP befindet, der mit einem grünen Punkt daneben gekennzeichnet ist, klicken Sie auf **Weiter**, um Instanzen zum Dienst hinzuzufügen.



1. Zeigen Sie auf der Seite **Add Instanzen** die ADC-Instanzen an, die mit dem registrierten Agenten verbunden sind. Stellen Sie sicher, dass die Instanz den Status “Nach **oben** “ hat, und klicken Sie auf “ **Weiter**”.

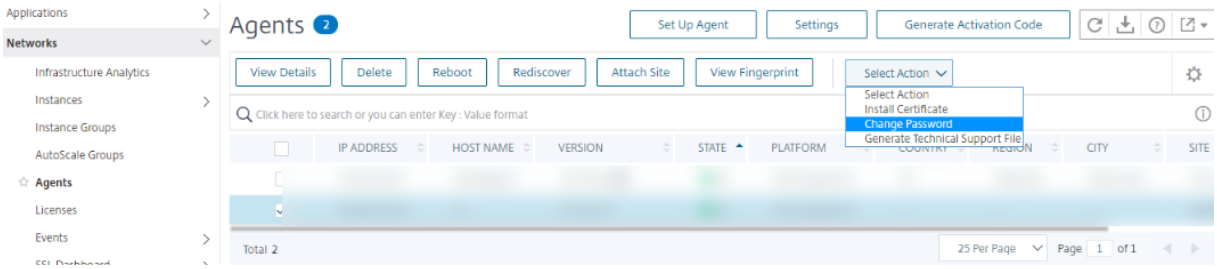


2. Klicken Sie auf **Fertig**, um die Erstinstallation abzuschließen und mit der Verwaltung der Bereitstellung zu beginnen.

> **Hinweis**
>
> Wenn Sie während der Erstinstallation keine Instanzen hinzufügen möchten, können Sie auf **Fertig** klicken, um die Einrichtung abzuschließen und die Instanzen später hinzuzufügen. Anweisungen zum Hinzufügen von Instanzen zu einem späteren Zeitpunkt zu Citrix ADM finden Sie unterInstanzen hinzufügen.

Agent-Aktionen

Nachdem Sie Ihren ADM-Dienst eingerichtet haben, können Sie verschiedene Aktionen auf einen Agenten anwenden. Navigieren Sie zu **Netzwerke > Agents**.



Unter **Aktion auswählen**können Sie die folgenden Funktionen verwenden:

Installieren Sie ein neues Zertifikat: Wenn Sie ein anderes Agentenzertifikat benötigen, um Ihre Sicherheitsanforderungen zu erfüllen, können Sie eines hinzufügen.

Ändern Sie das Standardkennwort: Um die Sicherheit Ihrer Infrastruktur zu gewährleisten, ändern Sie das Standardkennwort eines Agenten.

Erstellen Sie eine Datei für den technischen Support: Generieren Sie eine Datei für den technischen Support für einen ausgewählten Citrix ADM -Agent. Sie können diese Datei herunterladen und an den technischen Support von Citrix zur Untersuchung und Fehlerbehebung senden.

Konfigurieren des integrierten ADC-Agenten zur Verwaltung von Instanzen

April 28, 2021

Ein integrierter Agent ist auf Citrix ADC MPX, VPX, Gateway-Instanzen verfügbar, auf denen die Version ausgeführt wird, `12.1.48.13` und später sowie auf Citrix ADC SDX-Instanzen mit Version 13.0 61.x und höher sowie 12.1 58.x und höher. Sie können diesen Agenten auf der ADC-Instanz initiieren, anstatt einen dedizierten Agenten in Ihrem Rechenzentrum oder in der Public Cloud zu installieren. Der integrierte Agent ermöglicht die Kommunikation zwischen der Instanz und dem Citrix ADM-Dienst.

> **Hinweis**
>
> Der integrierte Agent ist nur für die folgenden Citrix ADC-Instanztypen verfügbar:
>
> - Citrix ADC MPX
> - Citrix ADC VPX
> - Citrix ADC SDX
> - Citrix Gateway

Der integrierte Agent ist ideal für kleinere ADC-Standalone- oder HA-Paar-Bereitstellungen. Wenn Sie über mehrere ADC-Instanzen verfügen, verwenden Sie einen dedizierten Agenten für Bereitstellungen. Dieser Agent stellt sicher, dass Sie über bessere Datenaggregationsfunktionen verfügen als der integrierte Agent. Weitere Informationen finden Sie unter Installieren eines Agenten lokal.

Citrix ADM Dienst unterstützt die Verwaltung und Überwachung von Citrix ADC-Instanzen mit integrierten Agenten. Die folgenden Funktionen werden im integrierten Agent jedoch nicht unterstützt:

- Anwendungs-Dashboard
- Web Insight
- SSL-Einblick
- HDX Insight

- Gateway-Einblick
- Einblicke in die Sicherheit
- Erweiterte Analysen
- Zusammengefasste Lizenzierung

Sie können von einem integrierten Agenten zu einem externen Agenten wechseln. Weitere Informationen finden Sie unter Übergang von einem integrierten Agenten zu einem externen Agenten.

Voraussetzungen

Bevor Sie einen integrierten Agenten in der Citrix ADC-Instanz konfigurieren, stellen Sie Folgendes sicher:

- Die Citrix ADC (MPX, VPX oder Gateway) -Instanz wird auf der Version `12.1.48.13` oder höher ausgeführt. Die SDX-Instanz läuft Version `13.0.61.x` und höher.
- Ein DNS-Namenserver wird auf der Citrix ADC-Instanz hinzugefügt.

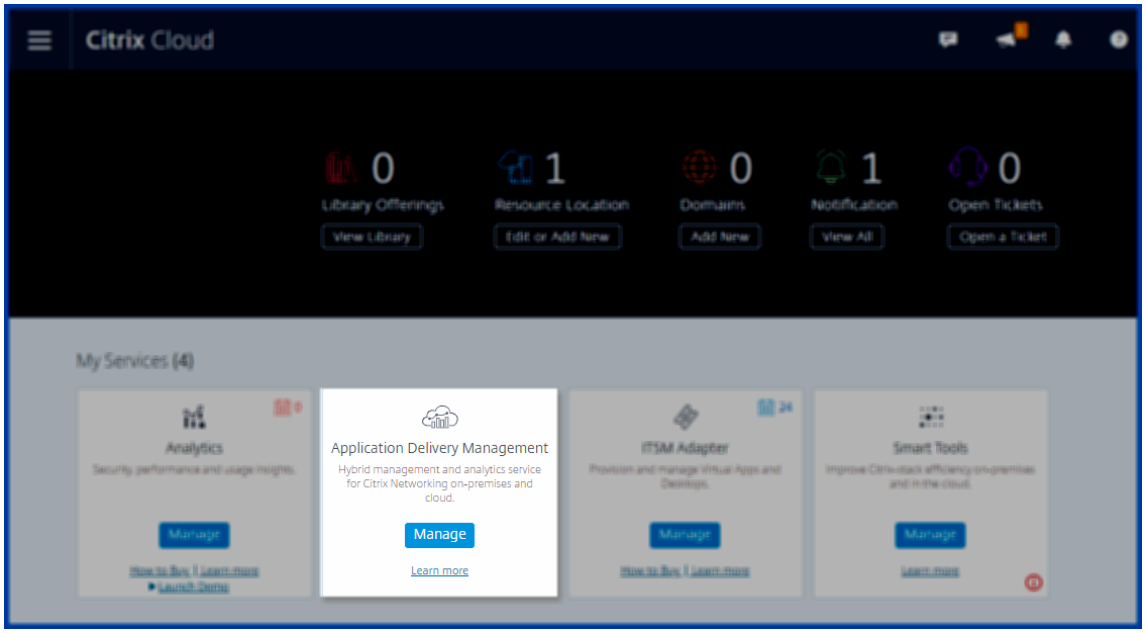
  Weitere Informationen finden Sie unter Hinzufügen eines Nameservers.
- Sie haben ein Citrix Cloud-Konto. Weitere Informationen finden Sie unter Registrierung bei Citrix Cloud.

> **Hinweis**
>
> Alle Informationen zu Ports und anderen Systemanforderungen finden Sie unter Systemanforderungen.

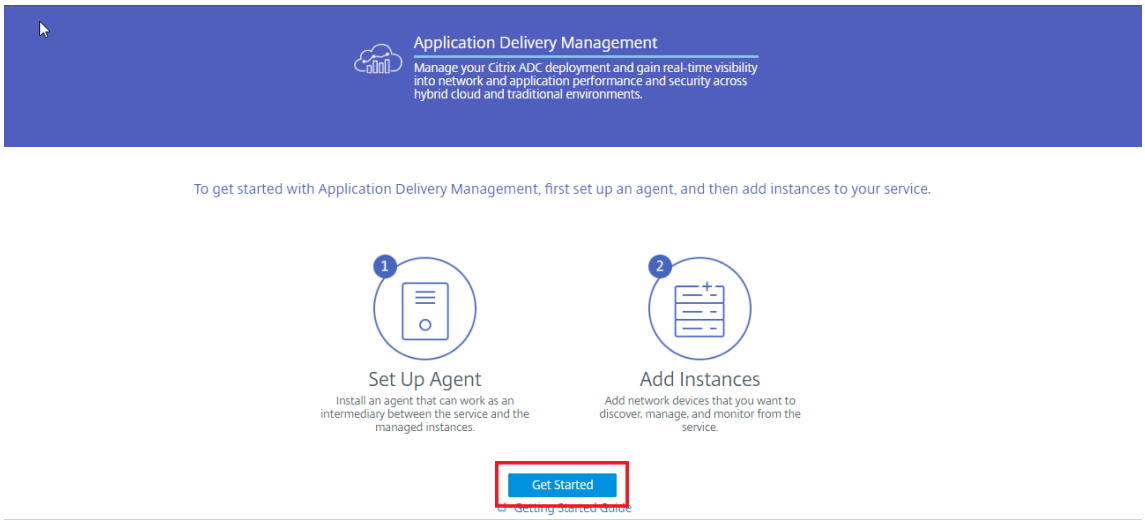
Konfigurieren des integrierten Agenten

Führen Sie die folgenden Aufgaben aus, um den integrierten ADC-Agenten zu konfigurieren:

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf der Kachel **Anwendungsbereitstellungsverwaltung** auf **Verwalten**. Wählen Sie dann die Region aus, die Ihren geschäftlichen Anforderungen entspricht. Weitere Informationen finden Sie unter Verwalten von Citrix ADM mit Express-Konto

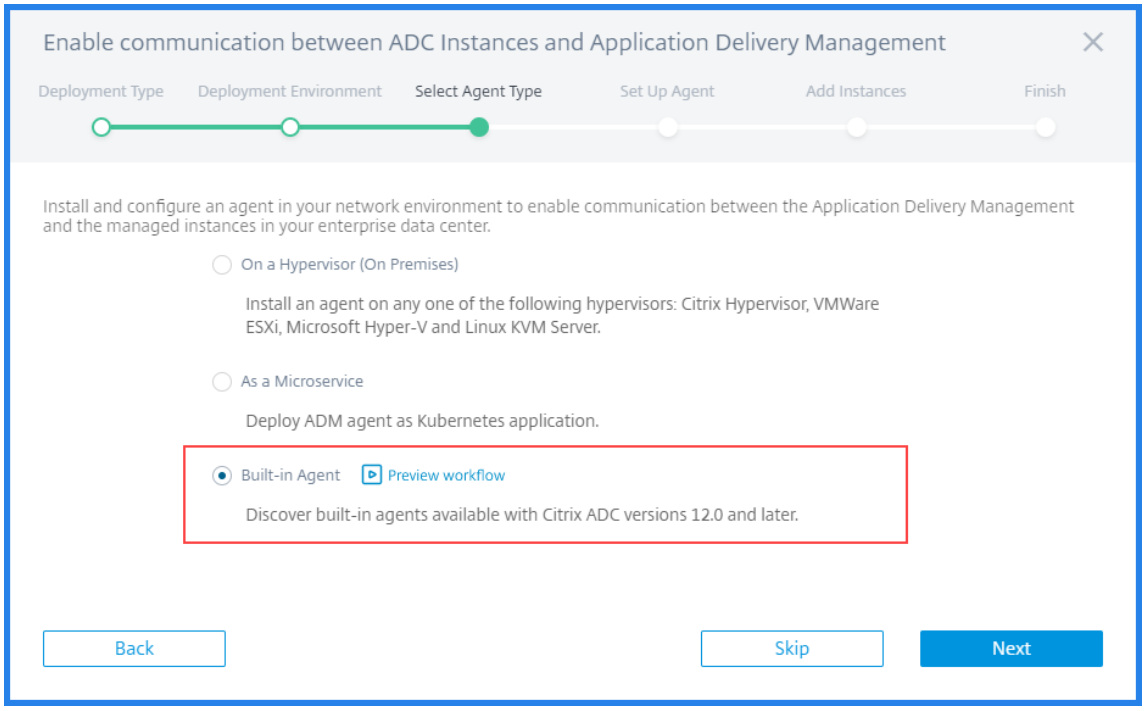


3. Klicken Sie auf **Erste Schritte**.



4. Wählen Sie " **On Premises** " als ADC-Bereitstellungstyp aus.
5. Wählen Sie **Integrierter Agent**aus.

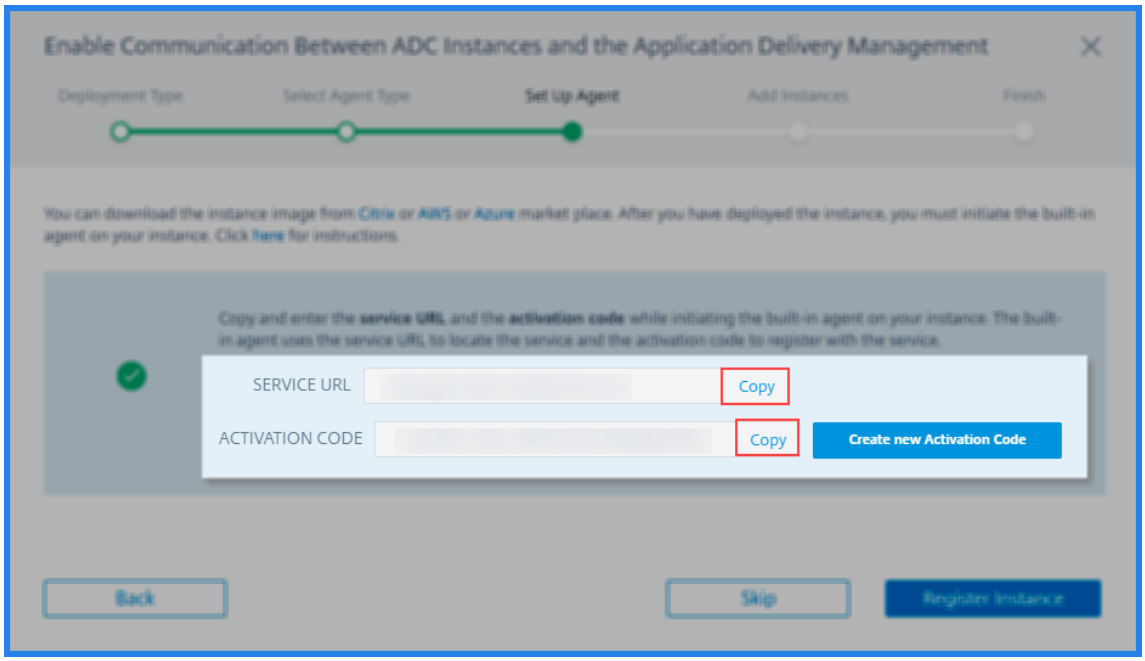
> **Wichtig**
>
> Um den integrierten Agenten verwenden zu können, muss die Citrix ADC-Instanz auf Version `12.1`Build `48.13`und höher installiert sein.



Eine Service-URL und ein Aktivierungscode werden generiert und auf der GUI angezeigt.

6. Kopieren Sie die **Service-URL** und den **Aktivierungscode**.

   Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren. Überspringen Sie Schritt 7, wenn Sie ein MPX- oder Gateway-Kunde sind.



7. Initiieren Sie den integrierten Agenten mit einem SSH-Client. Gateway-Benutzer müssen diesen

Schritt überspringen.

a) Melden Sie sich bei der Citrix ADC-Instanz an. Weitere Informationen finden Sie unter Zugriff auf ein Citrix ADC.

b) Navigieren Sie zum `/var/mastools/scripts`Verzeichnis, und geben Sie den folgenden Befehl ein:

Auf der SDX-Instanz

```
./mastool_int.sh <user-name> <service-url> <activation-code> -sdx
<!--NeedCopy-->
```

oder

```
./mastool_init.sh <device-profile-name> <service-url> <activation-code> -sdx -profile

<!--NeedCopy-->
```

> Hinweis
>
> ADM erkennt alle VPX-Instanzen, die auf diesem SDX ausgeführt werden, und Sie müssen die VPX-Instanzen nicht einzeln registrieren.

Auf VPX-Instanzen, die nicht auf einer SDX-Appliance und MPX- und Gateway-Instanzen ausgeführt werden

Wenn die ADM-Image-Version niedriger als 13.0 61.x oder 12.1 57.x ist, müssen Sie die `mastools` Version überprüfen, indem Sie den Befehl eingeben `cat /var/mastools/version.conf`. Wenn die Ausgabe ist `0.0-0.0`, ist es das erste Mal.

Geben Sie je nach Softwareversion einen der folgenden Befehle ein.

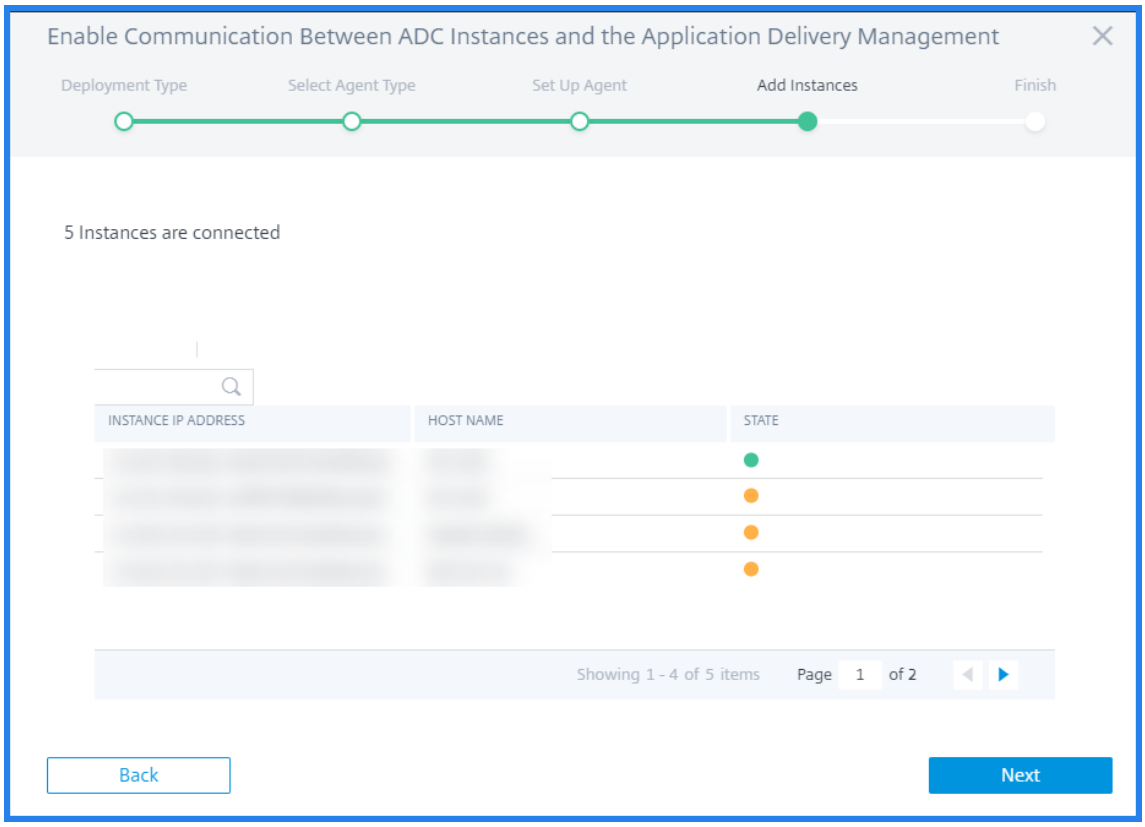
ADC-Image-Version	Ist mastools_version 0.0-0.0?	Befehl zur Registrierung mit Profil	Befehl zur Registrierung ohne Profil
Unter 13,0 61.xx und 12,1 57,xx	Ja	./mastools_init.sh <device_profile_nam> <service_url> ”MAS;<activation_code>”-profile	./mastools_init.sh <user_name> <pwd> <service_url> ”MAS;<activation_code>”
Unter 13,0 61.xx und 12,1 57,xx	Nein	./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile	./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>
Höher als 13,0 61.x und 12.1 57,xx	Nicht zutreffend	./mastools_init.sh <device_profile_nam> <service_url> <activation_code> -profile	./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>

- Geben <username>Sie Citrix ADC Benutzername ein.
- Geben Sie in <password>das ADC-Kennwort ein.
- Fügen Sie in <service_url>die URL ein, die Sie im vorherigen Schritt kopiert haben.
- Fügen Sie in <activation_code>den Aktivierungscode ein, den Sie im vorherigen Schritt kopiert haben.

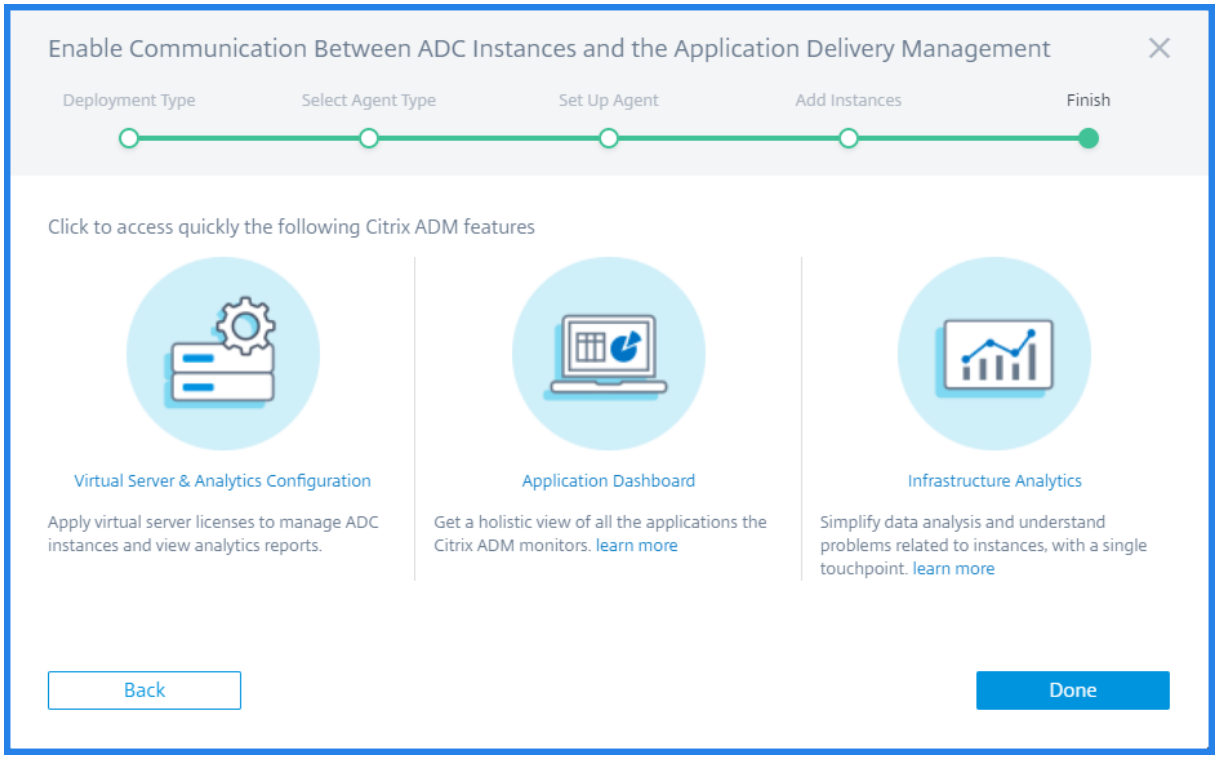
Für MPX-, VPX- und Gateway-Instanzen wird nach Abschluss der Initialisierung mit dem mastools Befehl die Kommunikation zwischen dem Agenten und dem ADM-Dienst hergestellt. Der Agent wird automatisch aktualisiert, wenn eine neueste Softwareversion verfügbar ist. Ab den Versionen ADC 12.1 57,18 und höher und ADC 13.0 61.48 und höher kommuniziert der integrierte Agent jedoch ohne Initialisierung mit dem ADM-Dienst und aktualisiert sich regelmäßig automatisch auf die neueste Softwareversion.
Für SDX-Instanzen verfügt der Agent über die Funktion für das automatische Upgrade in allen unterstützten Versionen, die 13.0 61.x und höher und 12.1 58.x und höher ist.

> Hinweis Schließen Sie
>
> bei einem HA-Paar die Registrierung auf dem primären Knoten ab. Wenn Sie die Registrierung auf dem sekundären Knoten ausführen, wird die folgende Meldung angezeigt:**Führen
>
> Sie den Registrierungsbefehl auf dem primären Knoten aus.**

8. Kehren Sie zur Seite ADM Service zurück, und klicken Sie auf **Instanz registrieren**.
9. Zeigen Sie unter **Instanzen hinzufügen**die Instanz an, in der Sie den integrierten Agent initiiert haben. Stellen Sie sicher, dass die Instanz den Status “Nach **oben** “ hat, und klicken Sie auf “ **Weiter**”.



10. Klicken Sie auf **Fertig**.



Nach erfolgreicher integrierter Agentkonfiguration können Sie auf die ADM-Funktionen zugreifen, z. B.:

- **Virtueller Server und Analysen** — Wenden Sie Lizenzen auf Ihren virtuellen Server an, um ADC-Instanzen zu verwalten. Weitere Informationen finden Sie unter Verwalten von Abonnements.
- **Anwendungs-Dashboard** — Um alle Anwendungen ganzheitlich anzuzeigen. Weitere Informationen finden Sie unter Anwendungsmanagement und Dashboard.
- **Infrastrukturanalyse** — Mit dieser Funktion können Sie die Faktoren visualisieren, die zu einem Problem in den Instanzen geführt haben oder zu einem Problem führen könnten. Weitere Informationen finden Sie unter Infrastrukturanalyse.

> Hinweis
>
> Sie können den integrierten Agenten auch konfigurieren, indem Sie zur Seite **Netzwerke > Agenten > Aktivierungscode generieren** navigieren. Kopieren Sie die URL und den Aktivierungscode in eine ADC-Instanz, und entdecken Sie diese Instanz.

Navigieren Sie nach dem Initiieren des integrierten Agenten zu **Netzwerke > Instanzen > Citrix ADC**. Auf dieser Seite werden die Details zur verwalteten Instanz angezeigt, die mit dem integrierten Agenten ermittelt wurde.

Problembehandlung

Sie können die Protokolle überprüfen, wenn die Registrierung fehlschlägt oder die Registrierung erfolgreich ist, der integrierte Agent jedoch nicht in der ADM-Benutzeroberfläche angezeigt wird.

- Wenn die Registrierung fehlschlägt, checken Sie die Login `/var/mastools/logs/mastools_reg.py.log`
- Wenn die Registrierung erfolgreich ist, der integrierte Agent jedoch nicht in der ADM-Benutzeroberfläche angezeigt wird, überprüfen Sie Folgendes:
  - **mastools_Upgrade** meldet sich an `/var/mastools/logs/mastools_upgrade.log`
  - **Binär meldet** sich an `/var/log/mastoolsd.log`.

Citrix ADM Agent lokal installieren

April 28, 2021

Der Agent arbeitet als Vermittler zwischen Citrix Application Delivery Management (Citrix ADM) und den erkannten Instanzen im Rechenzentrum.

Stellen Sie vor der Installation des Agents sicher, dass Sie über die erforderlichen virtuellen Computerressourcen verfügen, die der Hypervisor für jeden Agenten bereitstellen muss. Im Folgenden sind die Anforderungen für Agenten aufgeführt.

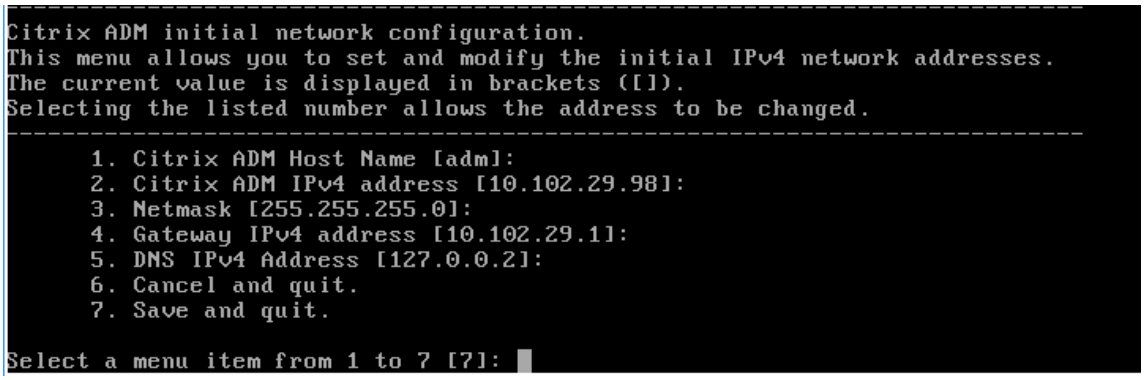
Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8
Speicherplatz	30 GB
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s

> **Hinweis**
>
> Alle Informationen zu Ports und anderen Anforderungen finden Sie unter Systemanforderungen.

So installieren Sie den Citrix ADM Agent:

1. Laden Sie das Agent-Image wie unter angewiesen herunter Erste Schritte.
2. Importieren Sie die Agent-Image-Datei in Ihren Hypervisor.
3. Konfigurieren Sie auf der Registerkarte **Konsole** die anfänglichen Netzwerkkonfigurationsoptio-

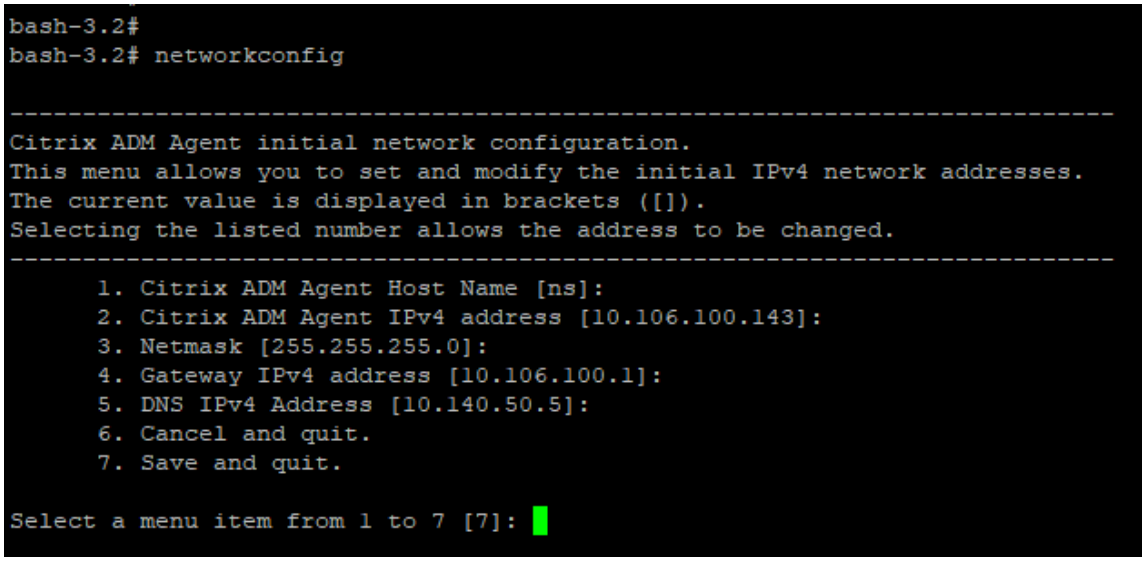
nen wie im folgenden Beispiel dargestellt:



> **Hinweis**
>
> Stellen Sie sicher, dass Sie Ihren DNS so konfigurieren, dass der Internetzugriff auf Ihren Citrix ADM Agent ermöglicht.

4. Nach Abschluss der anfänglichen Netzwerkkonfiguration speichern Sie die Konfigurationseinstellungen. Wenn Sie dazu aufgefordert werden, melden Sie sich mit den Standardanmeldeinformationen()`nsrecover`/`nsroot` an.

   Wenn Sie die konfigurierten Netzwerkeinstellungen auf dem Agenten ändern möchten, geben Sie den `networkconfig` Befehl ein und folgen Sie den Anweisungen in der CLI.



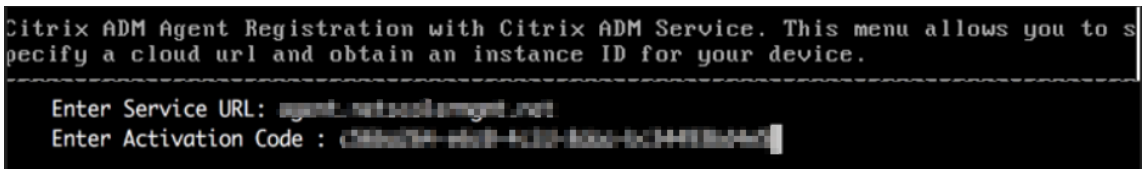
5. Wenn keine Eingabeaufforderung zur Eingabe der Dienst-URL angezeigt wird, navigieren Sie im Citrix ADM -Agent zu /mps, und führen Sie eines der folgenden Skripts aus:

```
deployment_type.py
<!--NeedCopy-->
```



```
register_agent_cloud.py
<!--NeedCopy-->
```

6. Geben Sie die **Service-URL** und den **Aktivierungscode** ein, die Sie beim Herunterladen des Agent-Images gespeichert haben. Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.



7. Nach erfolgreicher Agentenregistrierung wird der Agent neu gestartet, um den Installationsvorgang abzuschließen.

Nachdem der Agent neu gestartet wurde, greifen Sie auf die Citrix ADM GUI zu, und navigieren Sie zu **Netzwerke** > **Agents, um den Status des Agents** zu überprüfen.

Installieren des Citrix ADM-Agenten in der Microsoft Azure-Cloud

April 28, 2021

Der Agent arbeitet als Vermittler zwischen Citrix Application Delivery Management (Citrix ADM) und den verwalteten Instanzen im Rechenzentrum des Unternehmens oder in der Cloud.

Um den Citrix ADM Agent in der Microsoft Azure-Cloud zu installieren, müssen Sie eine Instanz des Agenten im virtuellen Netzwerk erstellen. Rufen Sie das Citrix ADM Agent-Image vom Azure Marketplace ab, und verwenden Sie dann das Azure Resource Manager-Portal, um den Agenten zu erstellen.

Bevor Sie mit dem Erstellen der Citrix ADM Agent-Instanz beginnen, stellen Sie sicher, dass Sie ein virtuelles Netzwerk mit den erforderlichen Subnetzen erstellt haben, in denen sich die Instanz befindet. Sie können während des VM-Provisionings virtuelle Netzwerke erstellen, jedoch ohne die Flexibilität, verschiedene Subnetze einzurichten. Hinweise zum Erstellen virtueller Netzwerke finden Sie unter http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network.

Konfigurieren Sie die DNS-Server- und VPN-Konnektivität, die es einer virtuellen Maschine ermöglicht, auf Internetressourcen zuzugreifen.

Voraussetzungen

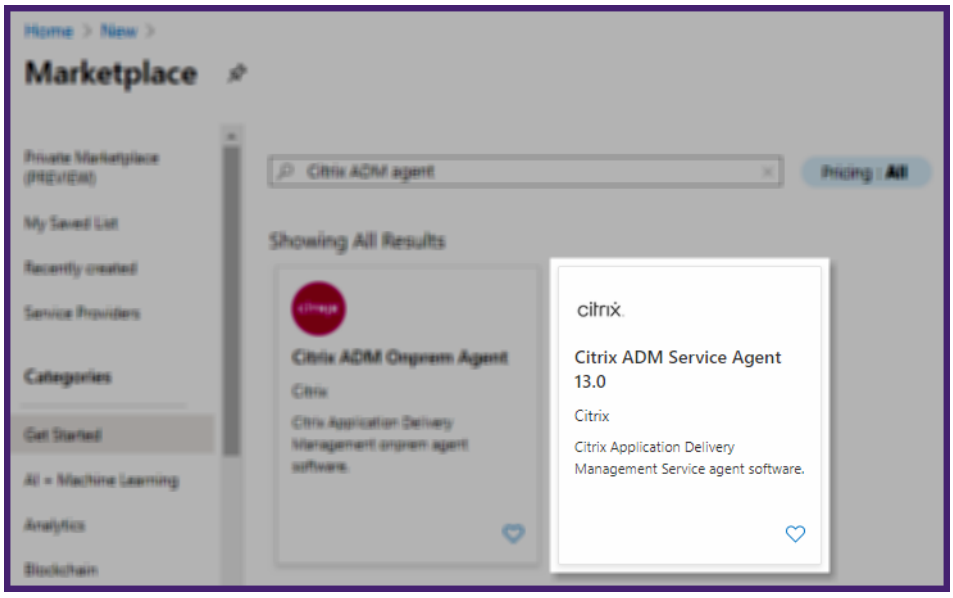
Stellen Sie sicher, dass Sie Folgendes haben:

- Ein Microsoft Azure-Benutzerkonto
- Zugriff auf Microsoft Azure Resource Manager

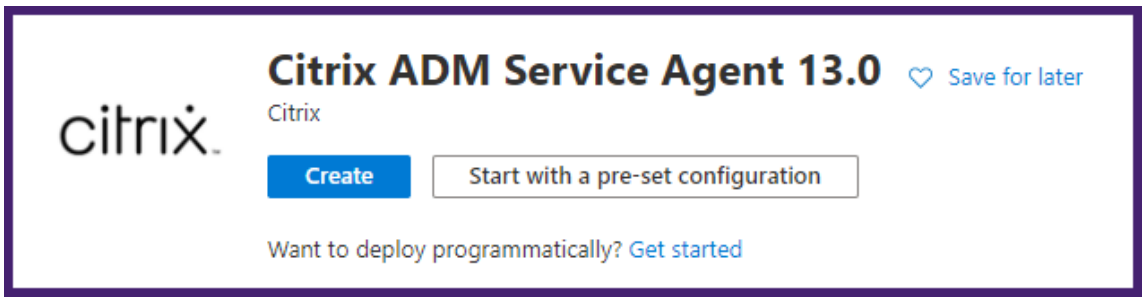
> **Hinweis**
>
> - Citrix empfiehlt, vor der Bereitstellung der virtuellen Citrix ADM Agent-Maschine Ressourcengruppe, Netzwerksicherheitsgruppe, virtuelles Netzwerk und andere Entitäten zu erstellen, damit die Netzwerkinformationen während der Provisioning verfügbar sind.
> - Damit der Citrix ADM-Agent mit Citrix ADM und den Citrix ADC-Instanzen kommunizieren kann, stellen Sie sicher, dass die empfohlenen Ports geöffnet sind. Vollständige Einzelheiten zu den Port-Anforderungen für den Citrix ADM Agent finden Sie unter Ports.

So installieren Sie den Citrix ADM Agent in Microsoft Azure Cloud:

1. Melden Sie sich mit Ihren Microsoft Azure-Anmeldeinformationen am Azure-Portal (https://portal.azure.com) an.
2. Klicken Sie auf **+Eine Ressource erstellen**.
3. Geben `Citrix ADM Agent` Sie die Suchleiste ein und wählen Sie **Citrix ADM Service Agent**aus.



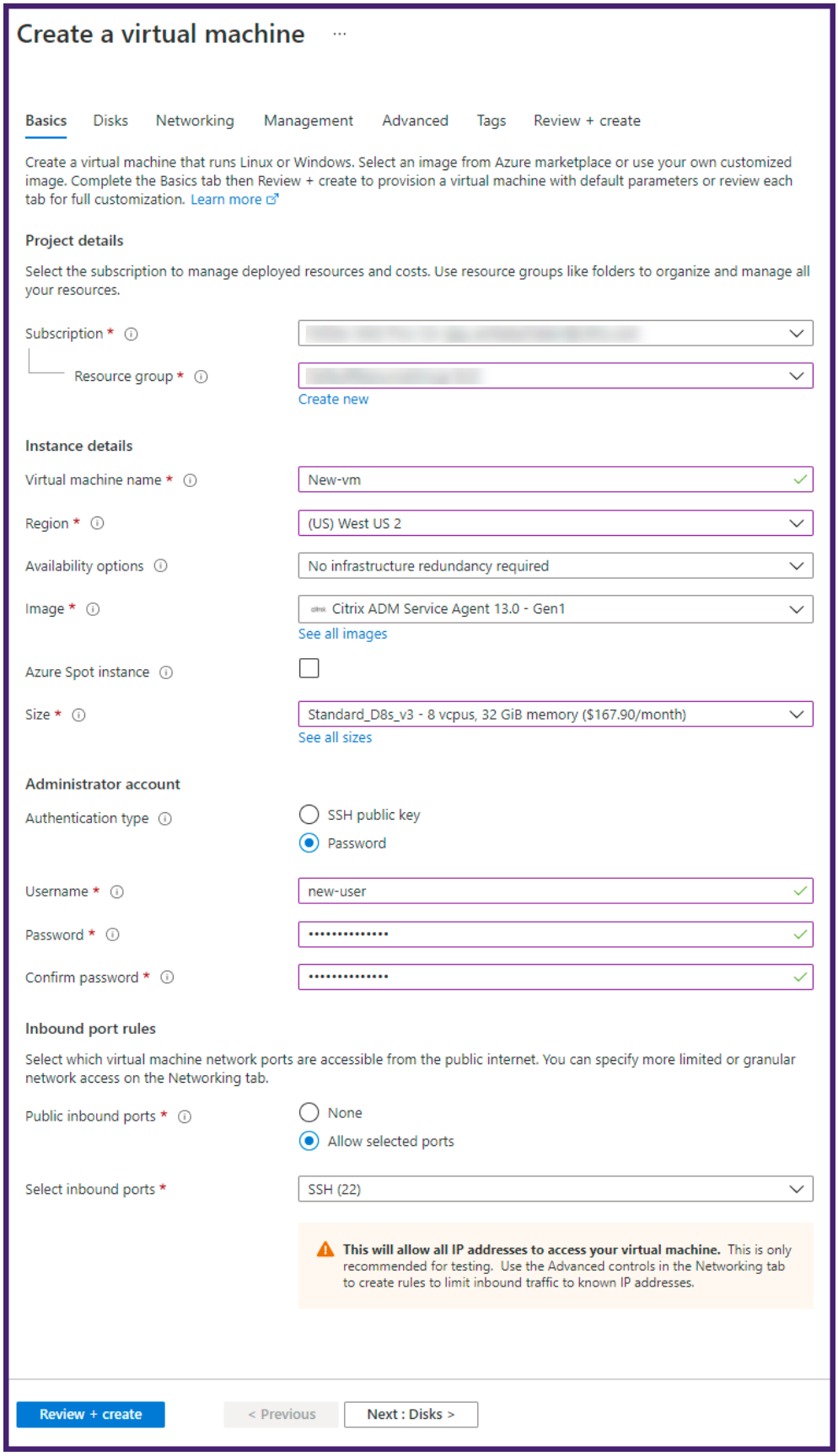
4. Klicken Sie auf **Erstellen**.



5. Geben Sie im Bereich **Virtuelle Maschine erstellen** in jedem Abschnitt die erforderlichen Werte an, um eine virtuelle Maschine zu erstellen.

   Grundlagen:

   Geben Sie auf dieser Registerkarte **Projektdetails**, **Instanzdetails**und **Administratorkonto**an.



- **Ressourcengruppe** — Wählen Sie die von Ihnen erstellte Ressourcengruppe aus der Dropdownliste aus.

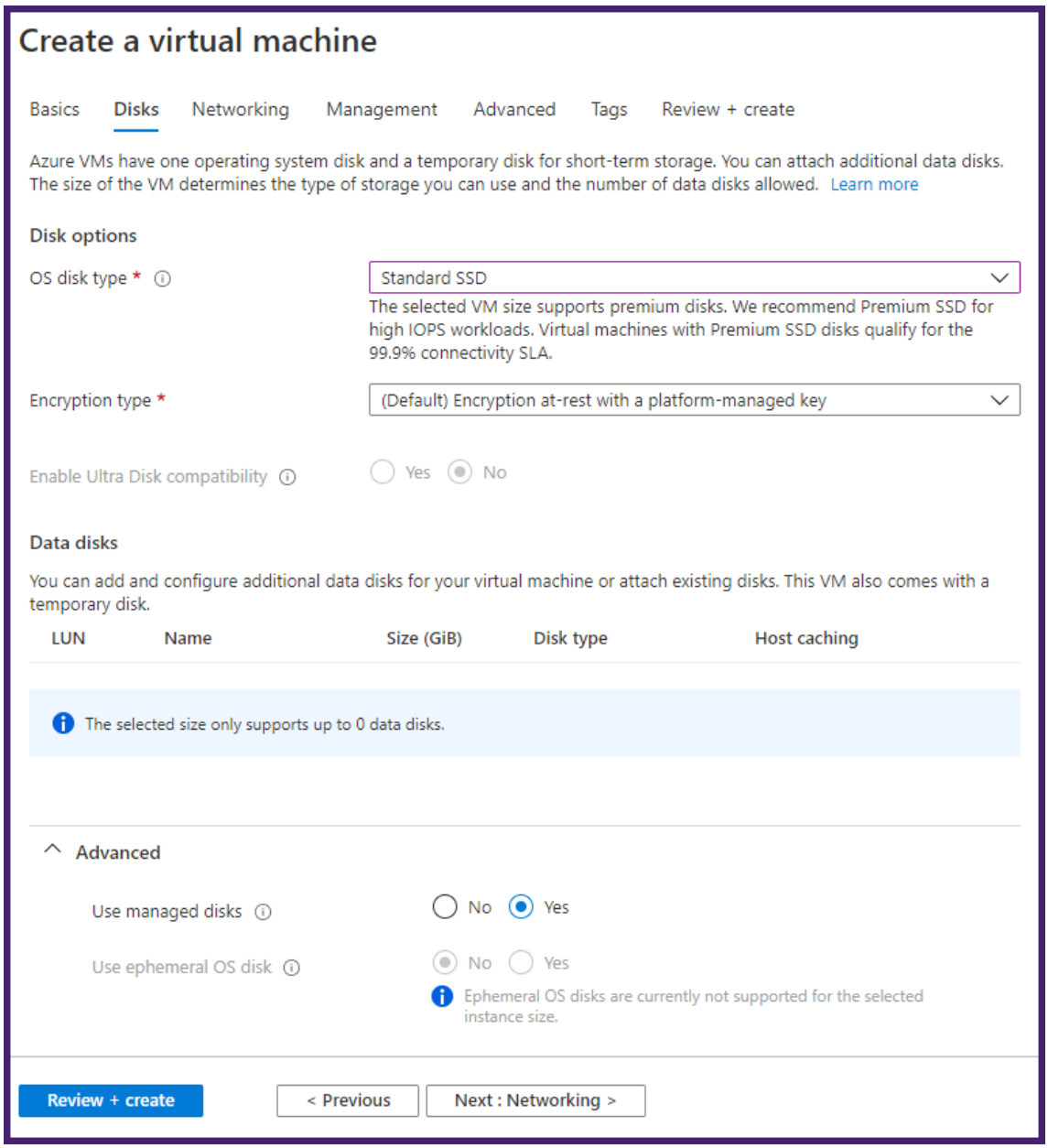
  > **Hinweis**
  >
  > Sie können zu diesem Zeitpunkt eine Ressourcengruppe erstellen, aber Citrix empfiehlt, dass Sie eine Ressourcengruppe aus Ressourcengruppen im Azure Resource Manager erstellen und dann die Gruppe aus der Dropdown-Liste auswählen.

- **Name der virtuellen Maschine** — Geben Sie einen Namen für die Citrix ADM Agent-Instanz an.
- **Region** - Wählen Sie die Region aus, in der Sie einen Agenten ausbringen möchten.
- **Verfügbarkeitsoptionen** — Wählen Sie den Verfügbarkeitssatz aus der Liste aus.
- **Bild** - In diesem Feld wird das bereits ausgewählte Agenten-Image angezeigt. Wenn Sie zu einem anderen Agenten-Image wechseln möchten, wählen Sie das gewünschte Bild aus der Liste aus.
- **Größe** - Geben Sie den Typ und die Größe des virtuellen Laufwerks für die Bereitstellung Ihres Citrix ADM-Agenten an.

  Wählen Sie den Typ Unterstützte virtuelle Laufwerke (**HDD** oder **SSD**) aus der Liste aus.
- **Authentifizierungstyp** — Wählen Sie Kennwort aus.
- **Benutzername und Kennwort** — Geben Sie einen Benutzernamen und ein Kennwort an, um auf die Ressourcen in der von Ihnen erstellten Ressourcengruppe zuzugreifen.

Datenträger:

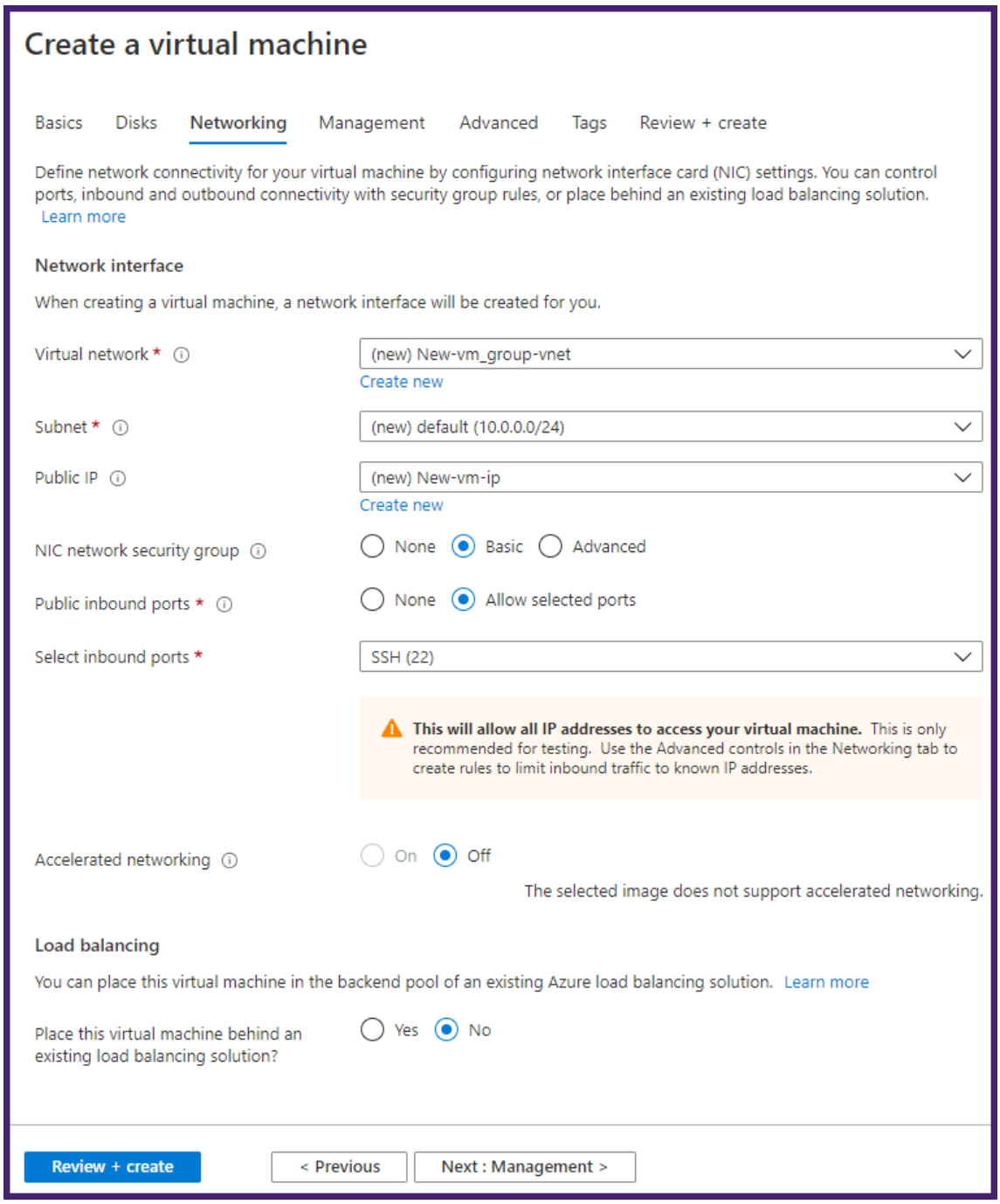
Auf dieser Registerkarte geben Sie **Datenträgeroptionen** und **Datendatenträger**an.



- **Betriebssystemdatenträgertyp** - Wählen Sie den Typ des virtuellen Laufwerks (HDD oder SSD) aus.

Vernetzung:

Geben Sie die erforderlichen Netzwerkdetails an:

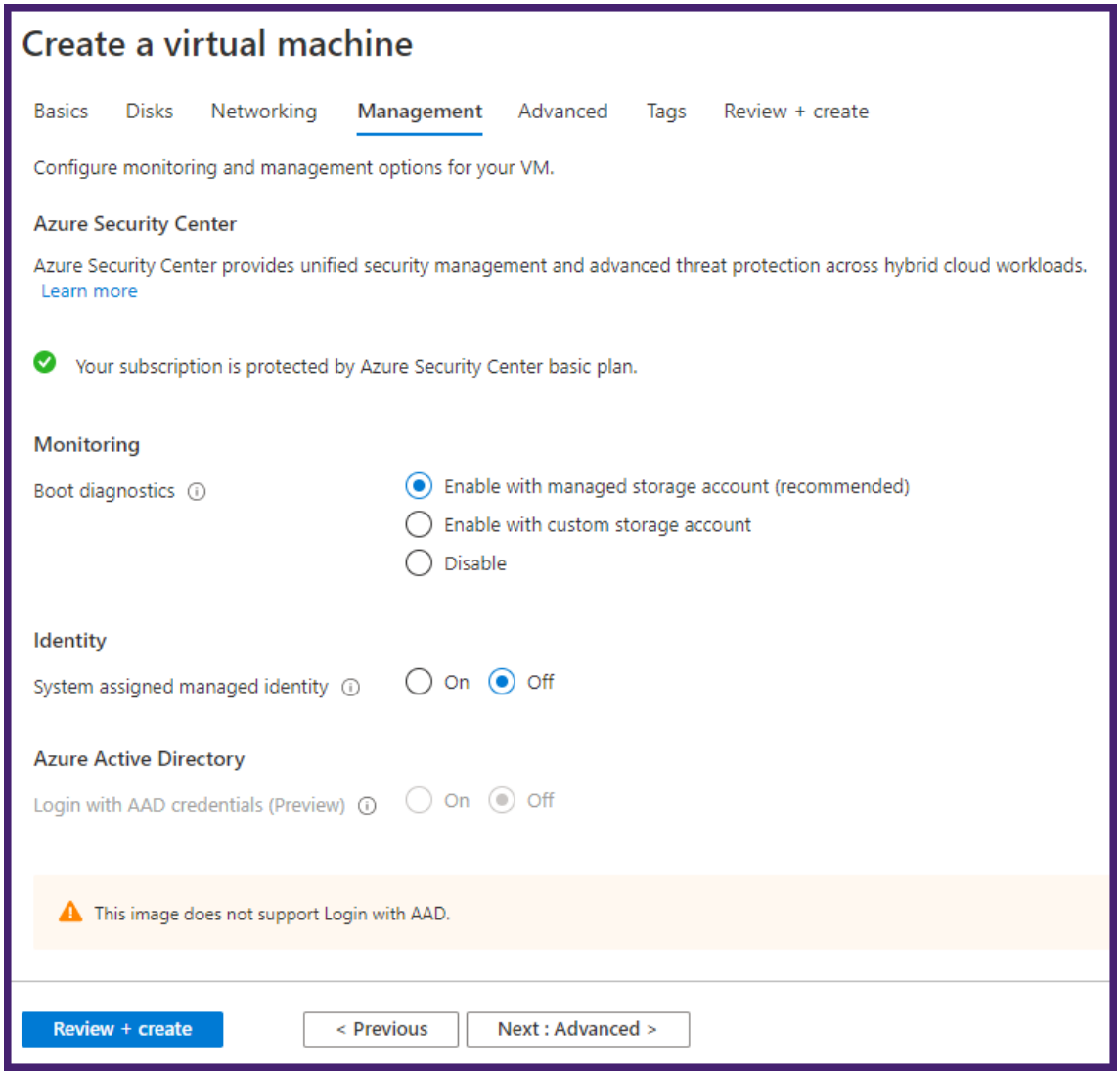


- **Virtuelles Netzwerk** — Wählen Sie das virtuelle Netzwerk aus.
- **Subnet** — Legen Sie die Subnetzadresse fest.
- **Öffentliche IP-Adresse** — Wählen Sie die IP-Adresse aus.
- **Netzwerksicherheitsgruppe** — Wählen Sie die Sicherheitsgruppe aus, die Sie erstellt haben.
- **Eingehende Ports auswählen** - Wenn Sie öffentliche eingehende Ports zulassen, stellen Sie sicher, dass die eingehenden und ausgehenden Regeln in der Sicherheitsgruppe kon-

figuriert sind. Wählen Sie dann die eingehenden Ports aus der Liste aus. Weitere Einzelheiten finden Sie unter Voraussetzungen.

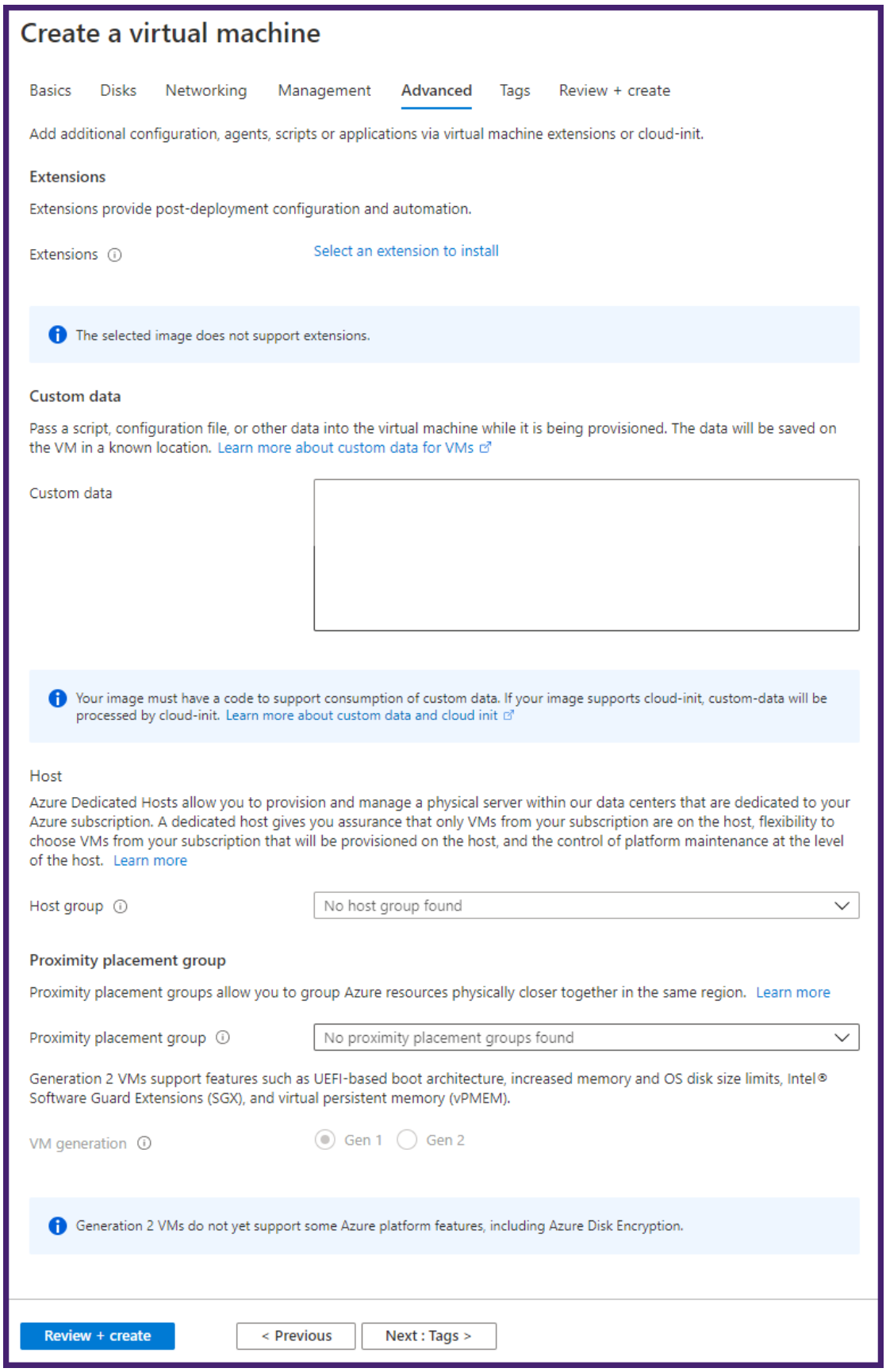
Geschäftsführung:

Geben Sie **Azure Security Center**, **Überwachung**und **Identität**an.



Fortgeschritten:

Optional geben Sie **Erweiterungen**, **benutzerdefinierte Daten**und **Proximity-Platzierungsgruppe**an.



In **Custom Data**können Sie ein Skript zur automatischen Registrierung für Agenten angeben, um den Agenten beim ADM-Dienst zu registrieren. Es folgt ein Beispielskript, das das `deployment.py` Skript ausführt und den Agenten registriert:

```
```python
#!/var/python/bin/python2.7
import os
import requests
import json
import time
import re
import logging
import logging.handlers
import boto3

'''
Das Skript im Überblick:
Das Skript hilft bei der Registrierung eines ADM-Agenten bei ADM. Übergeben Sie es in Benutzerdaten, damit sich der ADM-Agent in AWS beim Booten automatisch registriert. Der Workflow ist wie folgt
1)  Holen Sie sich die ADM-Service-API-Anmeldeinformationen (ID und Secret) aus dem AWS Secret Store (HINWEIS: Sie müssen dem ADM Agent die IAM-Rolle zuweisen, die die Berechtigung zum Abrufen von Secrets aus dem AWS-Geheimspeicher erteilt)
2)  Melden Sie sich bei ADM-Dienst mit Anmeldedaten an, die in Schritt 1 abgerufen wurden
3)  Rufen Sie ADM-Dienst auf, um Anmeldeinformationen (serviceURL und Token) für die Agentenregistrierung abzurufen
4)  Ruft die Registrierung an, indem die in Schritt 3 geholten Anmeldedaten verwendet werden
'''

'''
Dies sind die Platzhalter, die Sie entsprechend Ihren Setup-Konfigurationen ersetzen müssen
aws_secret_id: ID des AWS-Geheimnisses, in dem Sie ADM-Anmeldeinformationen gespeichert haben
Der Secrets-Wert sollte im folgenden JSON-Format vorliegen
{
  ”adm_user_id_key”: ”YOUR_ID”, ” adm_user_secret_key”: ” YOUR_SECRET” }

```


```

```
'''

aws_secret_id = "<AWS_secret_id>"
adm_ip_or_hostname = "<YOUR_ADM_POP>.adm.cloud.com"

'''
Richten Sie einen bestimmten Logger mit Ihrem gewünschten Ausgabe-Level und Log-Dateinamen ein
'''
log_file_name_local = os.path.basename(__file__)
LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'
LOG_MAX_BYTE = 50*1024*1024
LOG_BACKUP_COUNT = 20

logger = logging.getLogger(__name__)
logger.setLevel(logging.DEBUG)
logger_handler = logging.handlers.RotatingFileHandler(LOG_FILENAME, maxBytes=LOG_MAX_BYTE, backupCount=LOG_BACKUP_COUNT)
logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%(funcName)30s:%(lineno)4d: [%(levelname)s] %(message)s', datefmt="%Y-%m-%d %H:%M:%S")
logger_handler.setFormatter(logger_fortmater)
logger.addHandler(logger_handler)

class APIHandlerException(Exception):
    def __init__(self, error_code, message):
        self.error_code = error_code
        self.message = message

    def __str__(self):
        return self.message + ". Error code '" + str(self.error_code) + "'"

def parse_response(response, url, print_response=True):
    if not response.ok:
        if "reboot" in url:
            logger.debug('No response for url: reboot')
            resp = {
 "errorcode": "500", "message": "Error while reading response." }

            return resp

        if print_response:
            logger.debug('Response text for %s is %s' % (url, response.text))
```


```
67
68          response = json.loads(response.text)
69          logger.debug("ErrorCode - " + str(response['errorcode']) +
                ". Message -" + str(response['message']))
70          raise APIHandlerException(response['errorcode'], str(
                response['message']))
71      elif response.text:
72          if print_response:
73              logger.debug('Response text for %s is %s' % (url,
                    response.text))
74
75          result = json.loads(response.text)
76          if 'errorcode' in result and result['errorcode'] > 0:
77              raise APIHandlerException(result['errorcode'], str(
                    result['message']))
78          return result
79
80  def _request(method, url, data=None, headers=None, retry=3,
        print_response=True):
81      try:
82          response = requests.request(method, url, data=data,
                headers=headers)
83          result = parse_response(response, url, print_response=
                print_response)
84          return result
85      except [requests.exceptions.ConnectionError, requests.
            exceptions.ConnectTimeout]:
86          if retry > 0:
87              return _request(method, url, data, headers, retry-1,
                    print_response=print_response)
88          else:
89              raise APIHandlerException(503, 'ConnectionError')
90      except requests.exceptions.RequestException as e:
91          logger.debug(str(e))
92          raise APIHandlerException(500, str(e))
93      except APIHandlerException as e:
94          logger.debug("URL: %s, Error: %s, Message: %s" % (url, e.
                error_code, e.message))
95          raise e
96      except Exception as e:
97          raise APIHandlerException(500, str(e))
98
99  try:
100     '''Get the AWS Region'''
101     client = boto3.client('s3')
```



```
102     my_region = client.meta.region_name
103     logger.debug("The rgion is %s" % (my_region))
104 
105     '''Creating a Boto cleint session'''
106     session = boto3.session.Session()
107     client = session.client(
108         service_name='secretsmanager',
109         region_name=my_region
110     )
111 
112     '''Getting the values stored in the secret with id: <
            aws_secret_id>'''
113     get_id_value_response = client.get_secret_value(
114         SecretId = aws_secret_id
115     )
116     adm_user_id = json.loads(get_id_value_response["SecretString"
            ])["adm_user_id_key"]
117     adm_user_secret = json.loads(get_id_value_response["
            SecretString"])["adm_user_secret_key"]
118 
119 except Exception as e:
120     logger.debug("Fetching of ADM credentials from AWS secret
            failed with error: %s" % (str(e)))
121     raise e
122 
123 '''
124 Initialisieren von gängigen ADM API-Handlern
125 '''
126 mas_common_headers = {
127 
128     'Content-Type': "application/json",
129     'Accept-type': "application/json",
130     'Connection': "keep-alive",
131     'isCloud': "true"
132  }
133 
134 
135 '''
136 API zum Anmelden beim ADM und zum Abrufen der Session-ID und der
        Mandanten-ID
137 '''
138 url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/
        login"
139 payload = 'object={
140  "login":{
```



```
 "ID":"' + adm_user_id + '","Secret":"' + adm_user_secret + '" }
  }
 '
try:
    response = _request("POST", url, data=payload, headers=
        mas_common_headers)
    sessionid = response["login"][0]["sessionid"]
    tenant_id = response["login"][0]["tenant_name"]
except Exception as e:
    logger.debug("Login call to the ADM failed with error: %s" % (
        str(e)))
    raise e

'''
API zum Abrufen der Service-URL und des Token, die für die
   Registrierung des Agenten beim ADM verwendet werden sollen
'''
mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)
url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/
   trust_preauthtoken/" + tenant_id +"?customer="+ tenant_id
logger.debug("Fetching Service URL and Token.")
try:
    response = _request("GET", url, data=None, headers=
        mas_common_headers)
    service_name  = response["trust_preauthtoken"][0]["
        service_name"]
    token = response["trust_preauthtoken"][0]["token"]
    api_gateway_url = response["trust_preauthtoken"][0]["
        api_gateway_url"]
except Exception as e:
    logger.debug("Fetching of the Service URL Passed with error. %
        s" % (str(e)))
    raise e

'''
Ausführen des Befehls register agent mit den Werten, die wir zuvor
    abgerufen haben
'''
try:
    registeragent_command = "registeragent -serviceurl "+
        api_gateway_url+" -activationcode "+service_name+"\;"+token
    file_run_command = "/var/python/bin/python2.7 /mps/
        register_agent_cloud.py "+registeragent_command
    logger.debug("Executing registeragent command: %s" % (
        file_run_command))
```

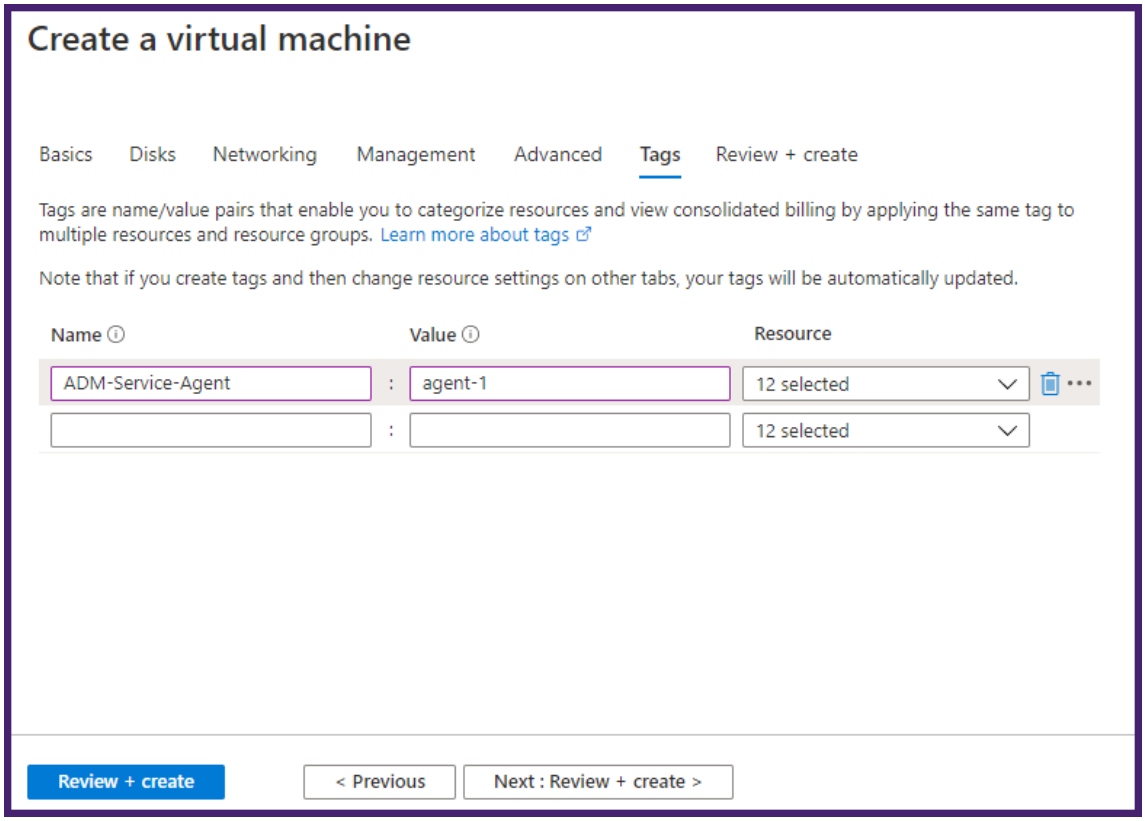


```
174     os.system(file_run_command)
175 except Exception as e:
176     logger.debug("Agent Registeration failed with error: %s" % (
            str(e)))
177         raise e
178 <!--NeedCopy--> ```
```

Wenn Sie dieses Skript für die automatische Registrierung angeben, überspringen Sie Schritt 7 und 8.

Tags:

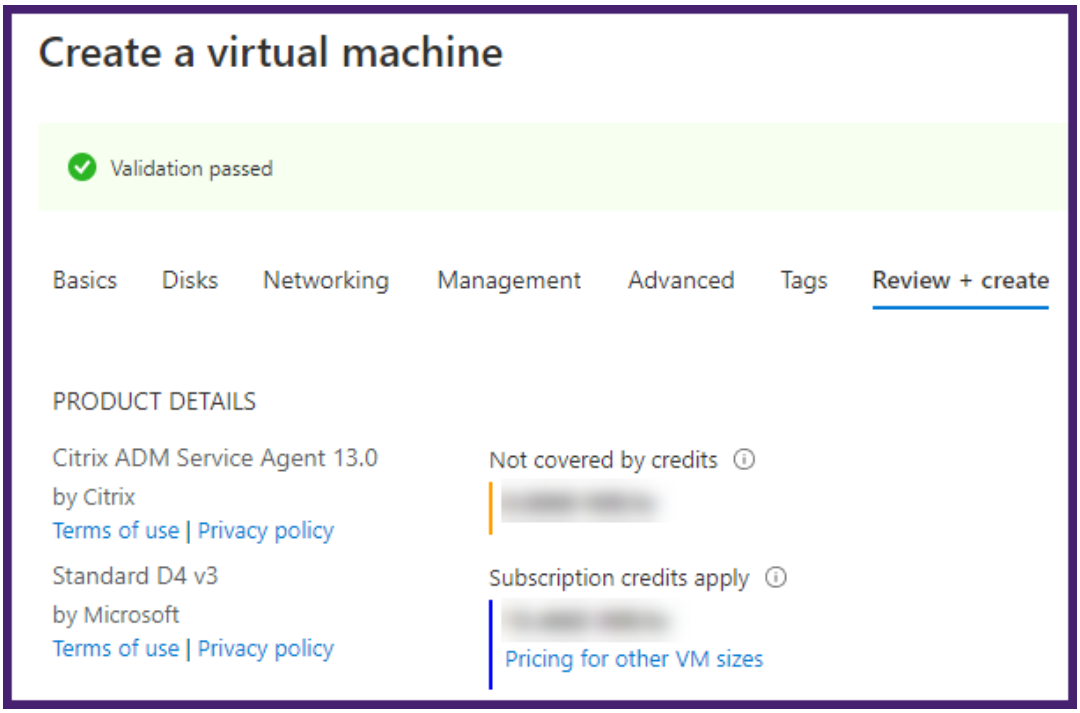
Geben Sie das Schlüssel-Wert-Paar für die ADM-Agent-Tags ein. Ein Tag besteht aus einem Schlüssel-Wert-Paar, das zwischen Groß- und Kleinschreibung unterschieden wird. Mit diesen Tags können Sie den Agenten einfach organisieren und identifizieren. Die Tags werden sowohl für Azure als auch für Citrix ADM angewendet.



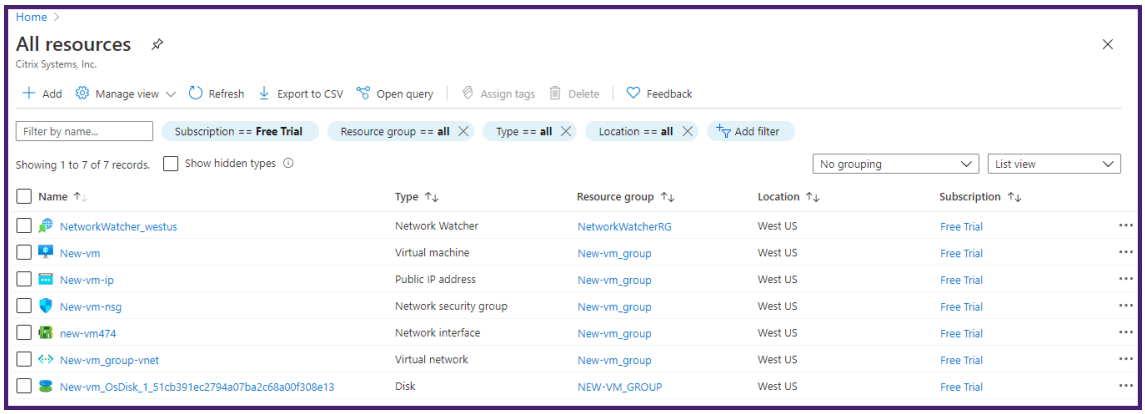
Die Konfigurationseinstellungen werden überprüft, und auf der Registerkarte **Überprüfen und erstellen** wird das Ergebnis der Validierung angezeigt.

- Wenn die Validierung fehlschlägt, zeigt diese Registerkarte den Grund für den Fehler an. Gehen Sie zurück zum jeweiligen Abschnitt und nehmen Sie ggf. Änderungen vor.
- Wenn die Validierung erfolgreich ist, klicken Sie auf **Erstellen**. Der Prozess der Agenten-

bereitstellung beginnt.



Der Bereitstellungsprozess kann etwa 10 bis 15 Minuten dauern. Sobald die Bereitstellung erfolgreich abgeschlossen ist, können Sie Ihre virtuelle Citrix ADM Agent-Maschine in Ihrem Microsoft Azure-Konto anzeigen.



6. Sobald der Agent mit einem SSH-Client einsatzbereit ist, melden Sie sich mit der **öffentlichen IP-Adresse** am Citrix ADM Agent an.

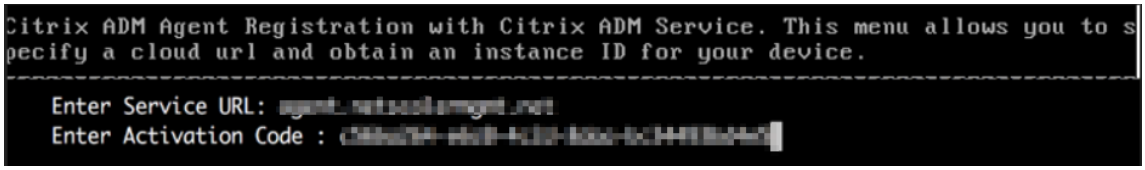
> **Hinweis**
>
> ```
> 1  - Wenn Sie den Benutzernamen als angegeben haben `nsrecover
>      `, verwenden Sie die standardmäßigen Citrix ADM Agent-
> ```



```
        Anmeldeinformationen (**nsrecover/nsroot**), um sich bei
        der virtuellen Maschine anzumelden.
```

- Citrix empfiehlt, das Standardkennwort nach der ersten Anmeldung zu ändern. Um das Kennwort zu ändern, geben Sie bei Shell Folgendes ein: **passwd nsroot**.

7. Geben Sie den folgenden Befehl ein, um den Bereitstellungsbildschirm aufzurufen: **deployment_type.py**
8. Geben Sie die **Service-URL** und den **Aktivierungscode** ein, den Sie kopiert und auf der Seite **Agents einrichten** in Citrix ADM gespeichert haben Erste Schritte. Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.



Nach erfolgreicher Agentenregistrierung wird der Agent neu gestartet, um den Installationsvorgang abzuschließen.

Nachdem der Agent neu gestartet wurde, greifen Sie auf Citrix ADM zu und überprüfen Sie auf der Seite **Agent einrichten** unter **Ermittelte Agents** den Status des Agents.

Installieren Sie den Citrix ADM Agenten auf Amazon Web Services (AWS)

April 28, 2021

Der Citrix Application Delivery Management (Citrix ADM) -Agent arbeitet als Vermittler zwischen Citrix ADM und den erkannten Instanzen im Rechenzentrum oder in der Cloud.

Voraussetzungen

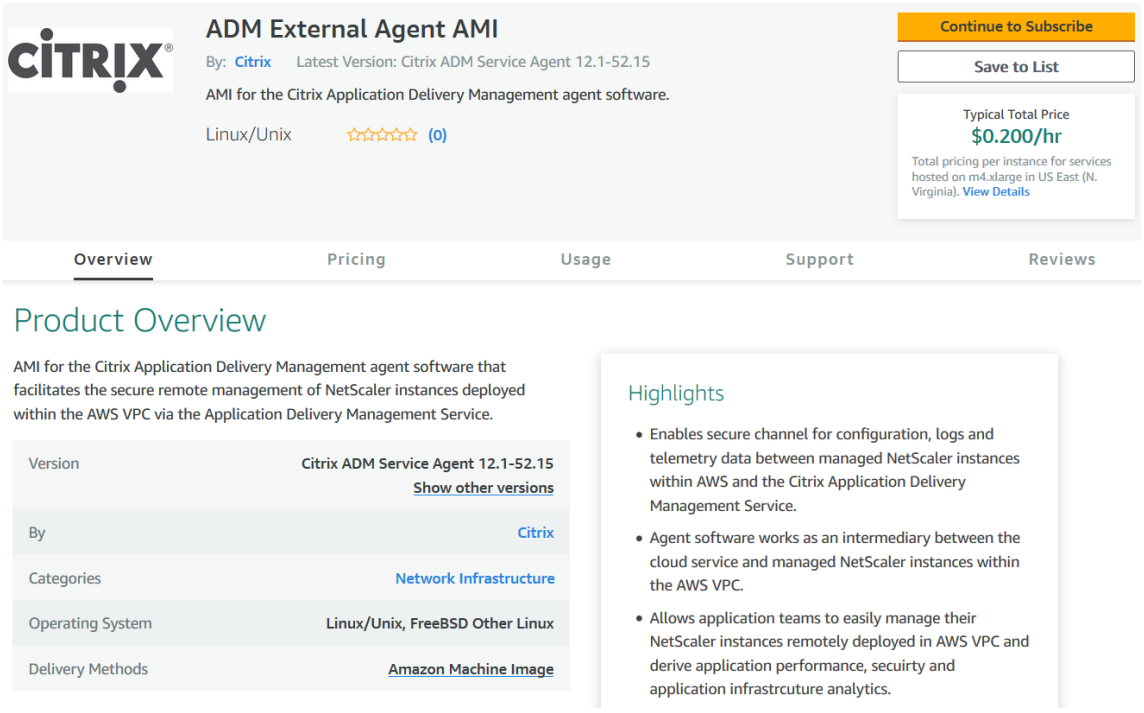
Um ein Citrix ADM Agent-AMI innerhalb einer Amazon Web Services (AWS) Virtual Private Cloud (VPC) über die Amazon GUI zu starten, benötigen Sie:

- Ein AWS-Konto
- Eine virtuelle private AWS-Cloud (VPC)
- Ein IAM-Konto

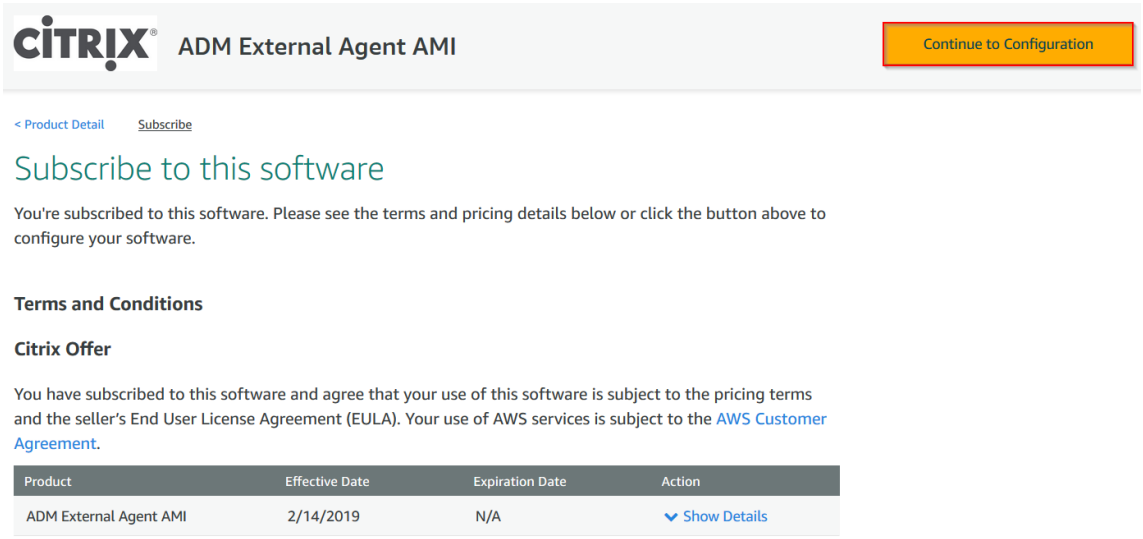
> **Hinweis**
>
> - Bevor Sie eine virtuelle Maschine für ADM-Agenten bereitstellen, empfiehlt Citrix, Sicherheitsgruppe, virtuelles privates Netzwerk, Schlüsselpaar, Subnetz und andere Entitäten zu erstellen. Daher stehen die Netzwerkinformationen während der Provisioning zur Verfügung.
> - Damit ein Citrix ADM-Agent mit dem Citrix ADM und den Citrix ADC-Instanzen kommuniziert, stellen Sie sicher, dass die empfohlenen Ports geöffnet sind. Ausführliche Informationen zu den Portanforderungen für einen Citrix ADM -Agent finden Sie unter Ports.

So installieren Sie den Citrix ADM Agent in AWS:

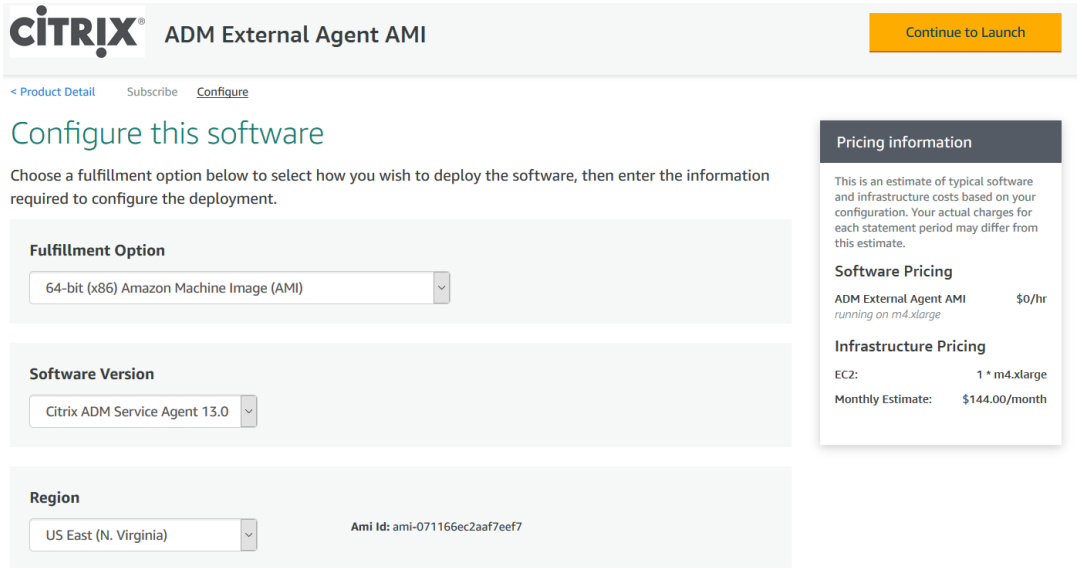
1. MeldenAWS-MarktplatzSie sich mit Ihren AWS-Anmeldeinformationen am an.
2. Geben Sie im Suchfeld **Citrix ADM Agent** ein, um nach dem Citrix ADM-Agent-AMI zu suchen, und klicken Sie auf **Los**.
3. Klicken Sie auf der Suchergebnisseite in der verfügbaren Liste auf das **ADM External Agent AMI**.
4. Klicken Sie auf der Seite **ADM External Agent AMI** auf **Weiter zu Abonnieren**.



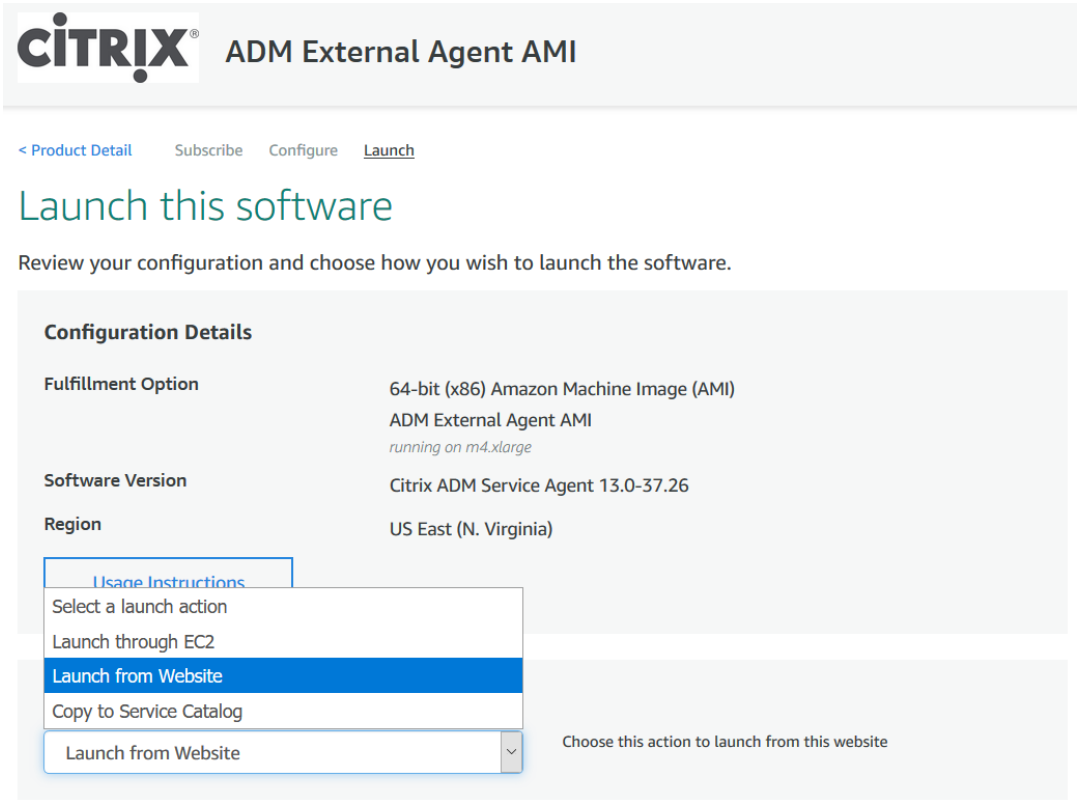
5. Nachdem das Abonnement erfolgreich ist, klicken Sie auf **Weiter zur Konfiguration**.



6. Auf der Seite **Diese Software konfigurieren**:
   a) Wählen Sie das AMI aus der **Fulfillment-Optionsliste** aus.
   b) Wählen Sie die neueste Version des Citrix ADM Agenten aus der Liste **Softwareversion** aus.
   c) Wählen Sie Ihre Region aus der Liste **Region** aus.
   d) Klicken Sie auf **Weiter, um zu starten**



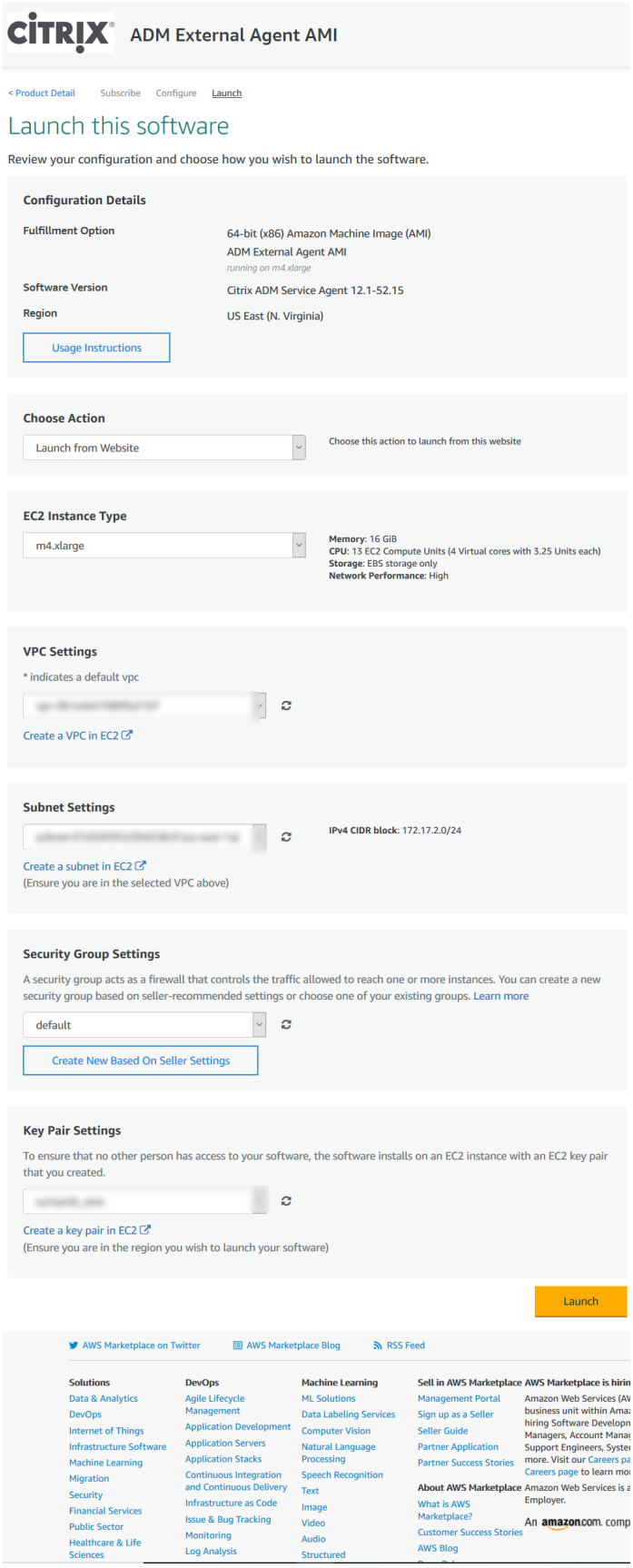
7. Auf der Seite **Diese Software starten** haben Sie zwei Möglichkeiten, den Citrix ADM Agent zu registrieren:
   a) **Start von der Website**
   b) **Start mit EC2**



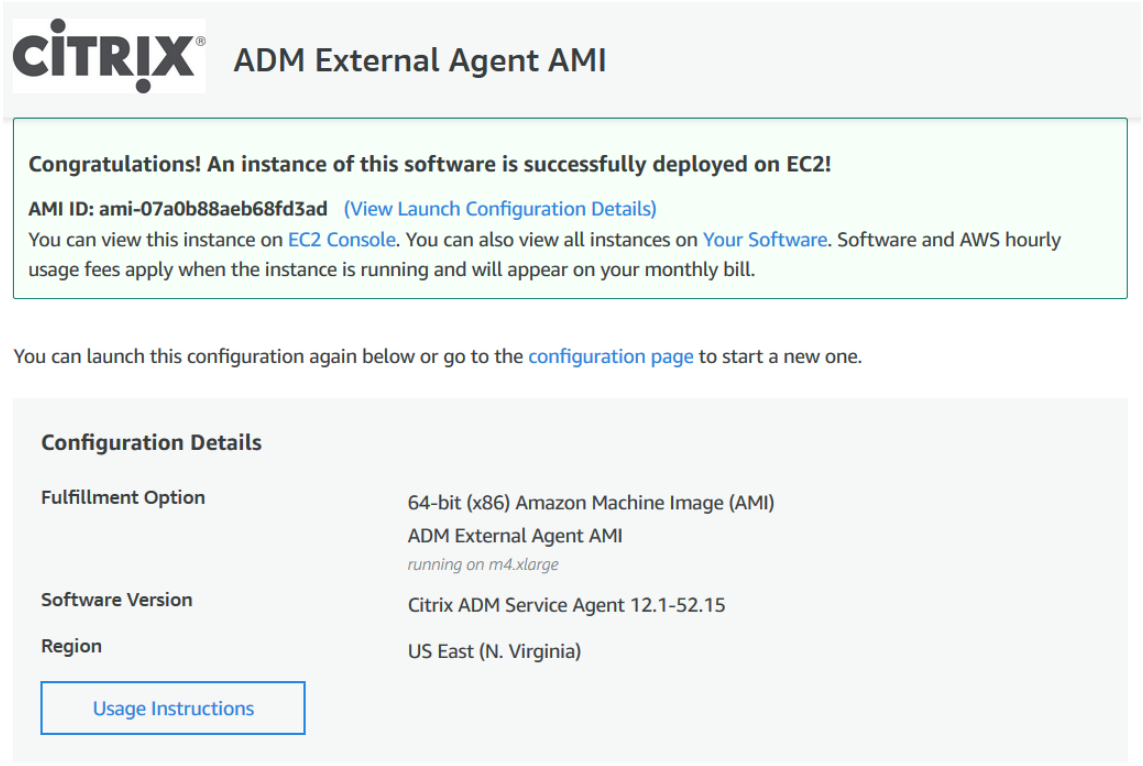
Starten von einer Website

Um von einer Website aus zu starten, wählen Sie:

1. Ein EC2-Instanz-Typ aus der Liste **EC2-Instanz-Typ**
2. Eine VPC aus der Liste **VPC-Einstellungen**. Klicken Sie auf **Erstellen einer VPC in EC2**, um eine VPC für Ihre Software zu erstellen.
3. Ein Subnetz aus der Liste **Subnetzeinstellungen**. Klicken Sie auf **Subnetz in EC2** erstellen, um ein Subnetz zu erstellen, nachdem Sie die VPC ausgewählt haben.
4. Eine Sicherheitsgruppe für die Firewall aus der Liste **Sicherheitsgruppeneinstellungen**. Klicken Sie auf **Neue basierend auf Verkäufereinstellungen** erstellen, um eine Sicherheitsgruppe zu erstellen.
5. Ein Schlüsselpaar, um die Zugriffssicherheit aus der Liste **Schlüsselpaar-Einstellungen** zu gewährleisten. Klicken Sie **in EC2 auf Schlüsselpaar** erstellen, um ein Schlüsselpaar für Ihre Software zu erstellen.
6. Klicken Sie auf **Start**



7. Der Start von einer Website ist erfolgreich.



> **Hinweis**
>
> Der Bereitstellungsprozess kann etwa 10 bis 15 Minuten dauern. Nachdem die Bereitstellung erfolgreich abgeschlossen wurde, können Sie Ihre virtuelle Citrix ADM Agent-Maschine in Ihrem AWS-Konto anzeigen.

8. Nachdem der Agent bereitgestellt wurde, weisen Sie Ihrem Citrix ADM Agent einen Namen zu.
9. Nachdem der Agent ausgeführt wurde, weisen Sie dem Citrix ADM Agent eine elastische IP-Adresse zu.

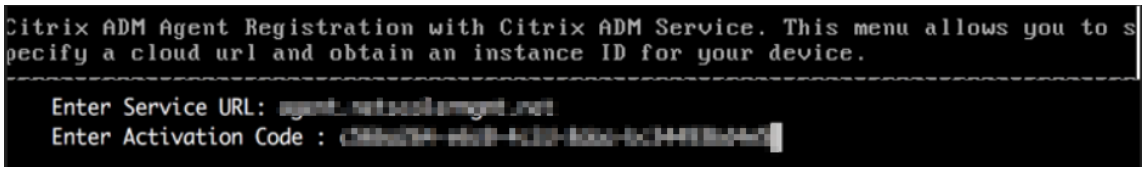
> **Hinweis**
>
> Mit der Elastic IP-Adresse kann Citrix ADM Agent mit Citrix ADM kommunizieren. Eine elastische IP-Adresse ist jedoch möglicherweise nicht erforderlich, wenn Sie NAT-Gateway so konfiguriert haben, dass der Datenverkehr an das Internet weitergeleitet wird.

10. Melden Sie sich mit einem SSH-Client an Ihrem Citrix ADM Agent mit der öffentlichen IP-Adresse an.

> **Hinweis:**
>
> Sie können sich mit einer der folgenden Methoden am Citrix ADM Agent anmelden:
>
> - Verwenden Sie `nsrecover`als Benutzername und AWS-Instanz-ID als Kennwort.

- Verwenden Sie `nsroot`als Benutzername und ein gültiges Schlüsselpaar als Kennwort.

11. Geben Sie den folgenden Befehl ein, um den Bereitstellungsbildschirm aufzurufen: **deployment_type.py**
12. Geben Sie die **Service-URL** und den **Aktivierungscode** ein, den Sie kopiert und auf der Seite **Agents einrichten** in Citrix ADM gespeichert haben Erste Schritte. Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.



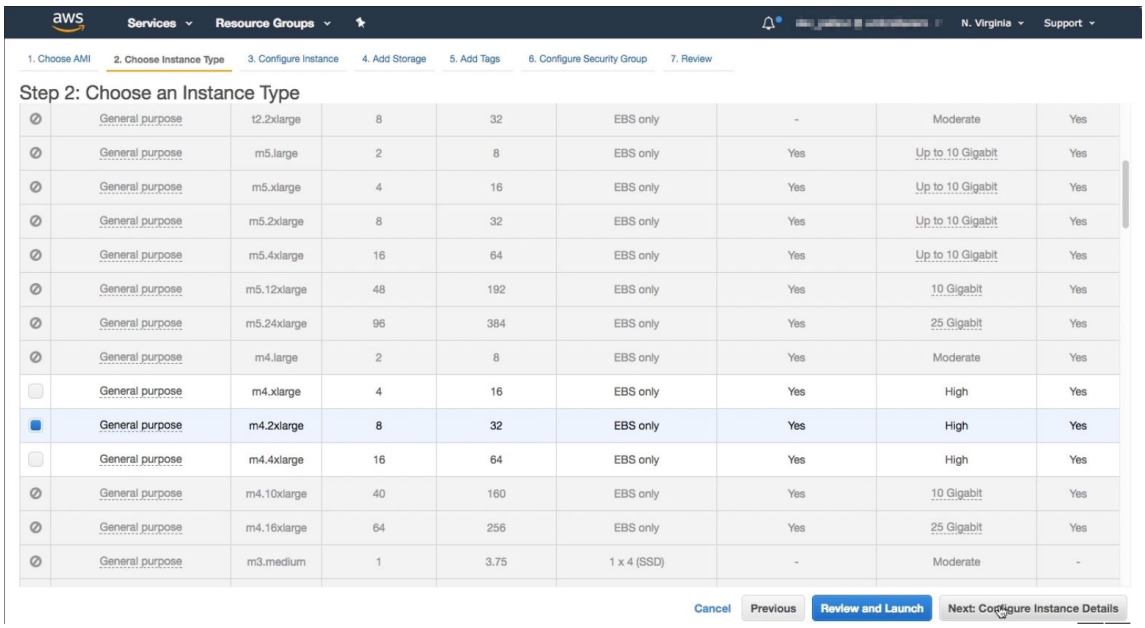
Nach erfolgreicher Agentenregistrierung wird der Agent neu gestartet, um den Installationsvorgang abzuschließen.

Nachdem der Agent neu gestartet wurde, greifen Sie auf Citrix ADM zu und überprüfen Sie auf der Seite **Agent einrichten** unter **Ermittelte Agents** den Status des Agents.

Start mit EC2

Um mit EC2 zu starten, wählen Sie **Start über EC2** aus der Liste **Aktion auswählen** aus, und klicken Sie dann auf **Starten**.

1. **Wählen Sie auf der Seite Choose an Instanz Type** die Instanz aus und klicken Sie auf **Next: Configure Instanz Details**.



2. Geben Sie auf der Seite **Configure Instanz Details** die erforderlichen Parameter an.

   Im Abschnitt **Erweiterte Details** können Sie einen Zero-Touch-Agenten aktivieren, indem Sie Authentifizierungsdetails oder ein Skript im Feld **Benutzerdaten** angeben.

   - **Details zur Authentifizierung** — Geben Sie die **Dienst-URL** und den **Aktivierungscode** an, den Sie von der Seite " **Agenten einrichten** " in Citrix ADM kopiert haben, wie in beschrieben Erste Schritte. Geben Sie die Details im folgenden Format ein.

     ```
     registeragent -serviceurl <apigatewayurl> -activationcode <
        activationcodevalue>
     <!--NeedCopy-->
     ```

     Der Agent verwendet diese Informationen, um sich beim Hochfahren automatisch beim ADM-Dienst zu registrieren.

   - **Skript** - Geben Sie ein Skript zur automatischen Registrierung des Agenten als Benutzerdaten an. Das Folgende ist ein Beispielskript:

     ```
     #!/var/python/bin/python2.7
     import os
     import requests
     import json
     import time
     import re
     import logging
     import logging.handlers
     import boto3

     '''
     Overview of the Script:
     The script helps to register an ADM agent with ADM. Pass it
        in userdata to make ADM agent in AWS to autoregister on
        bootup. The workflow is as follows
     1)  Fetch the ADM service API credentials (ID and secret)
        from AWS secret store (NOTE: you have to assign IAM role
        to the ADM Agent that will give permission to fetch
        secrets from AWS secret store)
     2)  Login to ADM service with credentials fetched in step 1
     3)  Call ADM service to fetch credentials (serviceURL and
        token) for agent registration
     4)  Calls registration by using the credentials fetched in
        step 3
     ```



```
'''

'''
These are the placeholders which you need to replace
   according to your setup configurations
aws_secret_id: Id of the AWS secret where you have stored ADM
    Credentials
The secrets value should be in the following json format
{
 ”adm_user_id_key”: ”YOUR_ID”, ” adm_user_secret_key”: ”
    YOUR_SECRET” }

'''

aws_secret_id = ”<AWS_secret_id>”
adm_ip_or_hostname = ”<YOUR_ADM_POP>.adm.cloud.com”

'''
Set up a specific logger with your desired output level and
   log file name
'''
log_file_name_local = os.path.basename(\_\_file\_\_)
LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'
LOG_MAX_BYTE = 50\*1024\*1024
LOG_BACKUP_COUNT = 20

logger = logging.getLogger(\_\_name\_\_)
logger.setLevel(logging.DEBUG)
logger_handler = logging.handlers.RotatingFileHandler(
   LOG_FILENAME, maxBytes=LOG_MAX_BYTE, backupCount=
   LOG_BACKUP_COUNT)
logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%(
   funcName)30s:%(lineno)4d: [%(levelname)s] %(message)s',
   datefmt=”%Y-%m-%d %H:%M:%S”)
logger_handler.setFormatter(logger_fortmater)
logger.addHandler(logger_handler)

class APIHandlerException(Exception):
    def \_\_init\_\_(self, error_code, message):
        self.error_code = error_code
        self.message = message

    def \_\_str\_\_(self):
        return self.message + ”. Error code '” + str(self.
           error_code) + ”'”
```



```
54
55  def parse_response(response, url, print_response=True):
56      if not response.ok:
57          if ”reboot” in url:
58              logger.debug('No response for url: reboot')
59              resp = {
60  ”errorcode”: ”500”, ”message”: ”Error while reading response.
        ” }
61
62              return resp
63
64          if print_response:
65              logger.debug('Response text for %s is %s' % (url,
                    response.text))
66
67          response = json.loads(response.text)
68          logger.debug(”ErrorCode - ” + str(response['errorcode
                '']) + ”. Message -” + str(response['message']))
69          raise APIHandlerException(response['errorcode'], str(
                response['message']))
70      elif response.text:
71          if print_response:
72              logger.debug('Response text for %s is %s' % (url,
                    response.text))
73
74          result = json.loads(response.text)
75          if 'errorcode' in result and result['errorcode'] > 0:
76              raise APIHandlerException(result['errorcode'],
                    str(result['message']))
77          return result
78
79  def _request(method, url, data=None, headers=None, retry=3,
        print_response=True):
80      try:
81          response = requests.request(method, url, data=data,
                headers=headers)
82          result = parse_response(response, url, print_response
                =print_response)
83          return result
84      except [requests.exceptions.ConnectionError, requests.
            exceptions.ConnectTimeout]:
85          if retry > 0:
86              return _request(method, url, data, headers, retry
                    -1, print_response=print_response)
87          else:
```



```
88                  raise APIHandlerException(503, 'ConnectionError')
89          except requests.exceptions.RequestException as e:
90              logger.debug(str(e))
91              raise APIHandlerException(500, str(e))
92          except APIHandlerException as e:
93              logger.debug("URL: %s, Error: %s, Message: %s" % (url
                    , e.error_code, e.message))
94              raise e
95          except Exception as e:
96              raise APIHandlerException(500, str(e))
97
98      try:
99          '''Get the AWS Region'''
100         client = boto3.client('s3')
101         my_region = client.meta.region_name
102         logger.debug("The rgion is %s" % (my_region))
103
104         '''Creating a Boto cleint session'''
105         session = boto3.session.Session()
106         client = session.client(
107             service_name='secretsmanager',
108             region_name=my_region
109         )
110
111         '''Getting the values stored in the secret with id: <
                aws_secret_id>'''
112         get_id_value_response = client.get_secret_value(
113             SecretId = aws_secret_id
114         )
115         adm_user_id = json.loads(get_id_value_response["
                SecretString"])["adm_user_id_key"]
116         adm_user_secret = json.loads(get_id_value_response["
                SecretString"])["adm_user_secret_key"]
117
118     except Exception as e:
119         logger.debug("Fetching of ADM credentials from AWS secret
                failed with error: %s" % (str(e)))
120         raise e
121
122     '''
123     Initializing common ADM API handlers
124     '''
125     mas_common_headers = {
126
127         'Content-Type': "application/json",
```



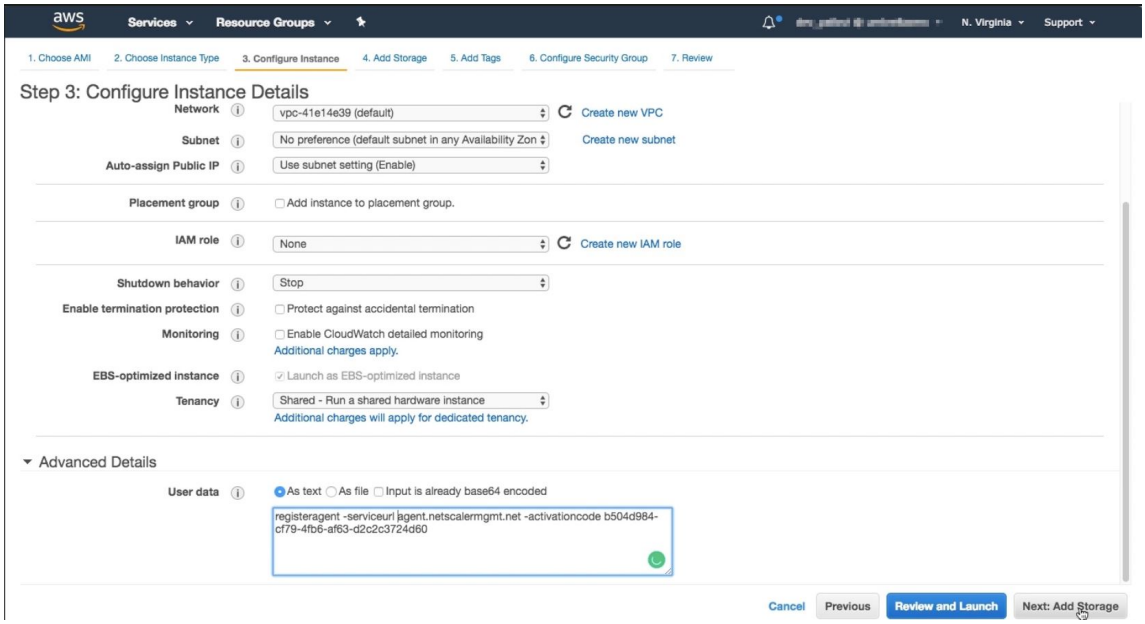
```
128       'Accept-type': ”application/json”,
129       'Connection': ”keep-alive”,
130       'isCloud': ”true”
131    }
132
133
134    '''
135    API to login to the ADM and fetch the Session ID and Tenant
          ID
136    '''
137    url = ”https://” + str(adm_ip_or_hostname) + ”/nitro/v1/
          config/login”
138    payload = 'object={
139    ”login”:{
140    ”ID”:”' + adm_user_id + '”,”Secret”:”' + adm_user_secret + '”
           }
141    }
142    '
143    try:
144        response = _request(”POST”, url, data=payload, headers=
              mas_common_headers)
145        sessionid = response[”login”][0][”sessionid”]
146        tenant_id = response[”login”][0][”tenant_name”]
147    except Exception as e:
148        logger.debug(”Login call to the ADM failed with error: %s
              ” % (str(e)))
149        raise e
150
151    '''
152    API to fetch the service URL and Token to be used for
          registering the agent with the ADM
153    '''
154    mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)
155    url = ”https://” + str(adm_ip_or_hostname) + ”/nitro/v1/
          config/trust_preauthtoken/” + tenant_id +”?customer=”+
          tenant_id
156    logger.debug(”Fetching Service URL and Token.”)
157    try:
158        response = _request(”GET”, url, data=None, headers=
              mas_common_headers)
159        service_name  = response[”trust_preauthtoken”][0][”
              service_name”]
160        token = response[”trust_preauthtoken”][0][”token”]
161        api_gateway_url = response[”trust_preauthtoken”][0][”
              api_gateway_url”]
```



```
except Exception as e:
    logger.debug("Fetching of the Service URL Passed with error. %s" % (str(e)))
    raise e

'''
Running the register agent command using the values we retrieved earlier
'''
try:
    registeragent_command = "registeragent -serviceurl "+api_gateway_url+" -activationcode "+service_name+";"+token
    file_run_command = "/var/python/bin/python2.7 /mps/register_agent_cloud.py "+registeragent_command
    logger.debug("Executing registeragent command: %s" % (file_run_command))
    os.system(file_run_command)
except Exception as e:
    logger.debug("Agent Registeration failed with error: %s" % (str(e)))
     raise e
<!--NeedCopy-->
```

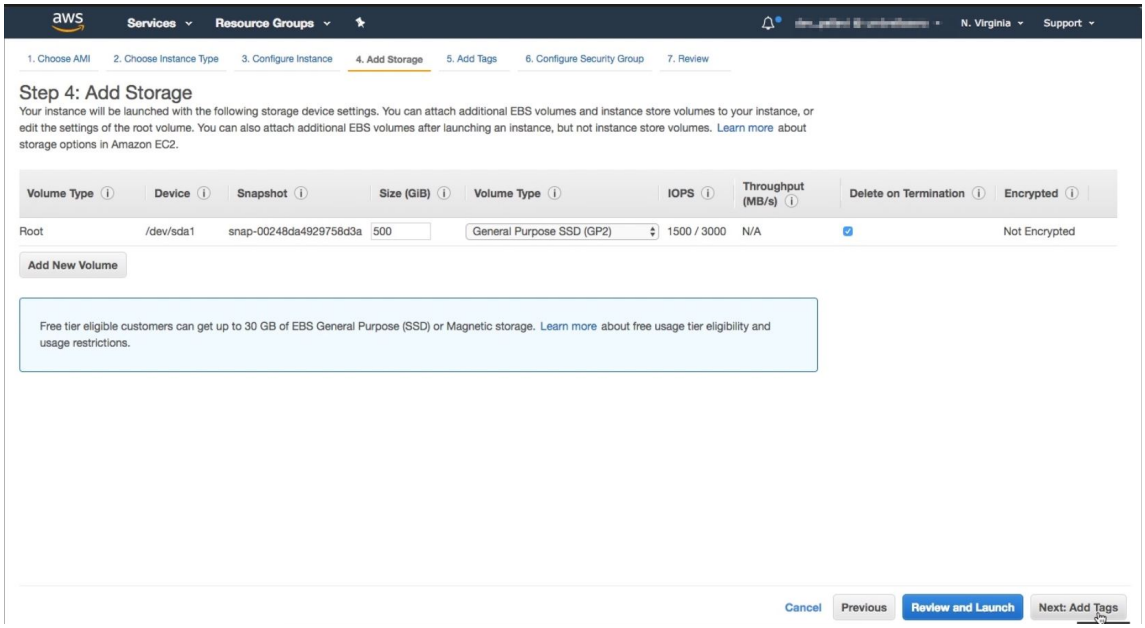
Dieses Skript ruft die Authentifizierungsdetails vom AWS Secrets Manager ab und führt das `deployment.py` Skript aus, um den Agenten beim ADM-Service zu registrieren.



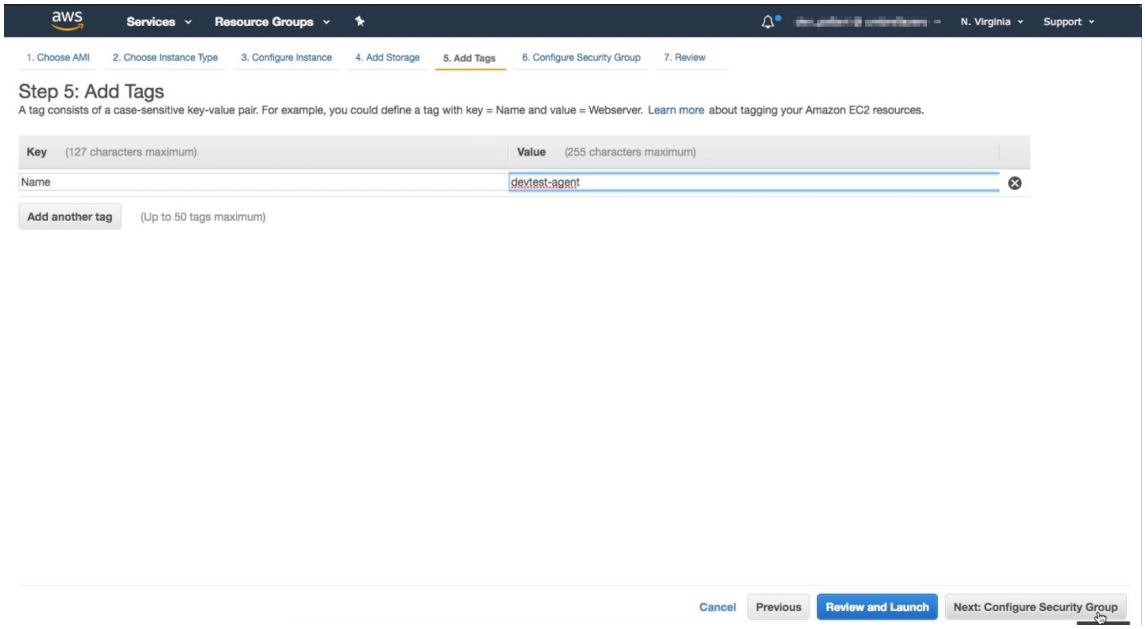
> **Hinweis**
>
> Sie können öffentliche IP-Adresse zwar automatisch zuweisen, aber Sie können auch elastische IP-Adresse zuweisen. Das Zuweisen einer elastischen IP-Adresse ist erforderlich, wenn NAT-Gateway nicht konfiguriert ist.
>
> Wenn die Elastic IP-Adresse in diesem Schritt nicht festgelegt ist, können Sie dies weiterhin auf der EC2-Konsole tun. Sie können eine neue elastische IP-Adresse erstellen und diese mithilfe der Instanz-ID oder ENI-ID dem ADM-Agenten zuordnen.

Klicken Sie auf " **Speicher hinzufügen**"

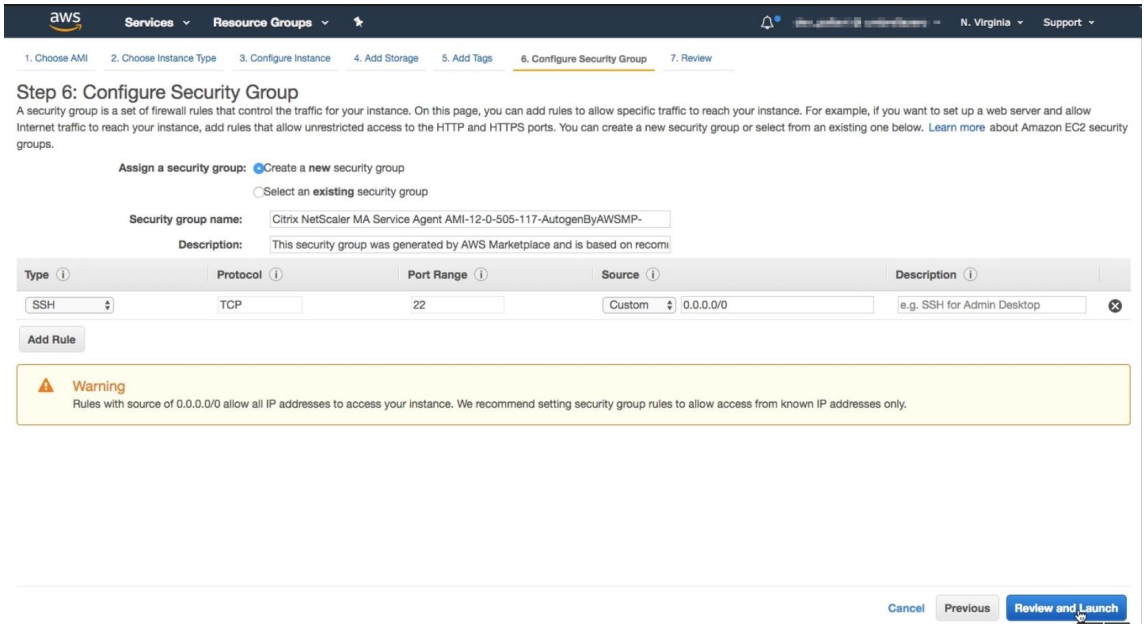
3. Konfigurieren Sie auf der Seite " **Speicher hinzufügen** " die Einstellungen des Speichergeräts für die Instanz und klicken Sie auf **Weiter: Tags hinzufügen**.



4. Definieren Sie auf der Seite **Add Tags** das Tag für die Instanz und klicken Sie auf **Weiter: Security Group konfigurieren**.



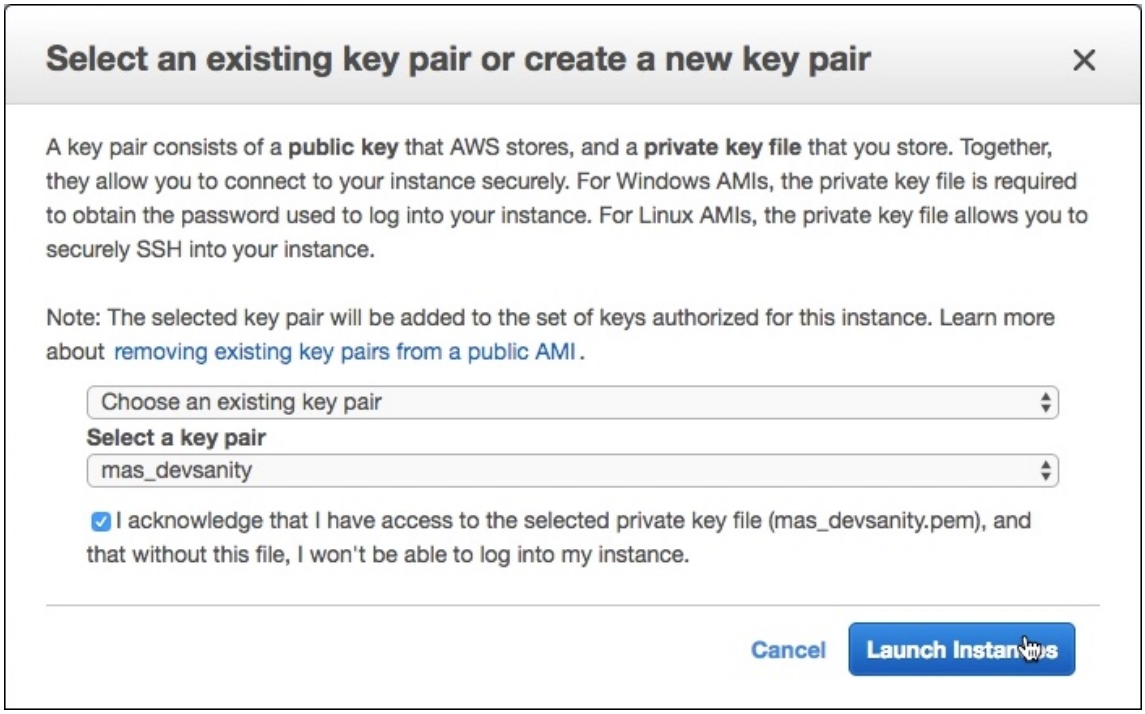
5. Fügen Sie auf der Seite **Configure Security Group** Regeln hinzu, um bestimmten Traffic zu Ihrer Instanz zu erlauben, und klicken Sie auf **Review and Launch**



6. Überprüfen Sie auf der Seite **Review Instanz Launch** die Instanz-Einstellungen und klicken Sie auf **Starten**.

7. Erstellen **Sie im Dialogfeld Wählen Sie ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues** Schlüsselpaar ein Schlüsselpaar. Sie können auch aus den vorhandenen Schlüsselpaaren wählen.

   Akzeptieren Sie die Bestätigung und klicken Sie auf **Launch Instanzen**.



Der Bereitstellungsprozess kann etwa 10 bis 15 Minuten dauern. Nachdem die Bereitstellung erfolgreich abgeschlossen wurde, können Sie Ihre virtuelle Citrix ADM Agent-Maschine in Ihrem AWS-Konto anzeigen.

Installieren Sie den Citrix ADM Agenten auf GCP

April 28, 2021

Der Citrix Application Delivery Management (Citrix ADM) -Agent arbeitet als Vermittler zwischen Citrix ADM und den erkannten Instanzen im Rechenzentrum oder in der Cloud. Sie können den Agenten auf der Google Cloud Platform (GCP) bereitstellen, um die sichere Remote-Verwaltung von Citrix ADC-Instanzen zu erleichtern, die über Citrix ADM im virtuellen Google Cloud-Netzwerk bereitgestellt werden. Weitere Informationen darüber, wie der ADM-Agent auf GCP für IT-Administratoren liefert, finden Sie im Blog Der Citrix ADM Agent ist jetzt auf dem Google Cloud Platform Marketplace verfügbar.

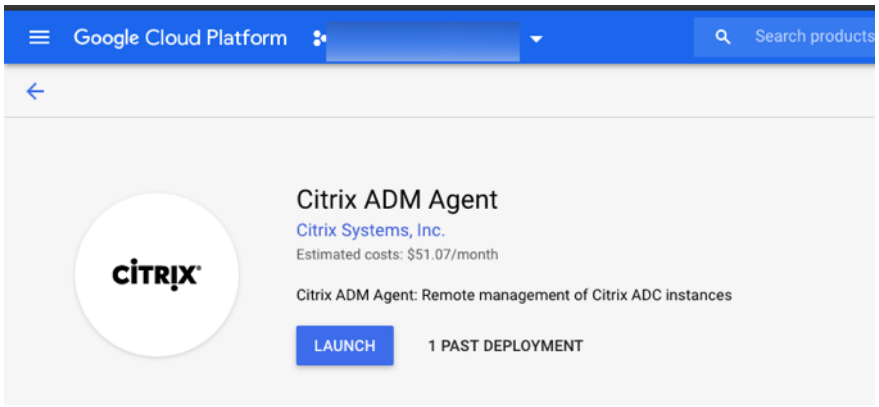
Voraussetzungen

Um einen ADM-Agenten auf GCP zu installieren, benötigen Sie ein GCP-Konto.

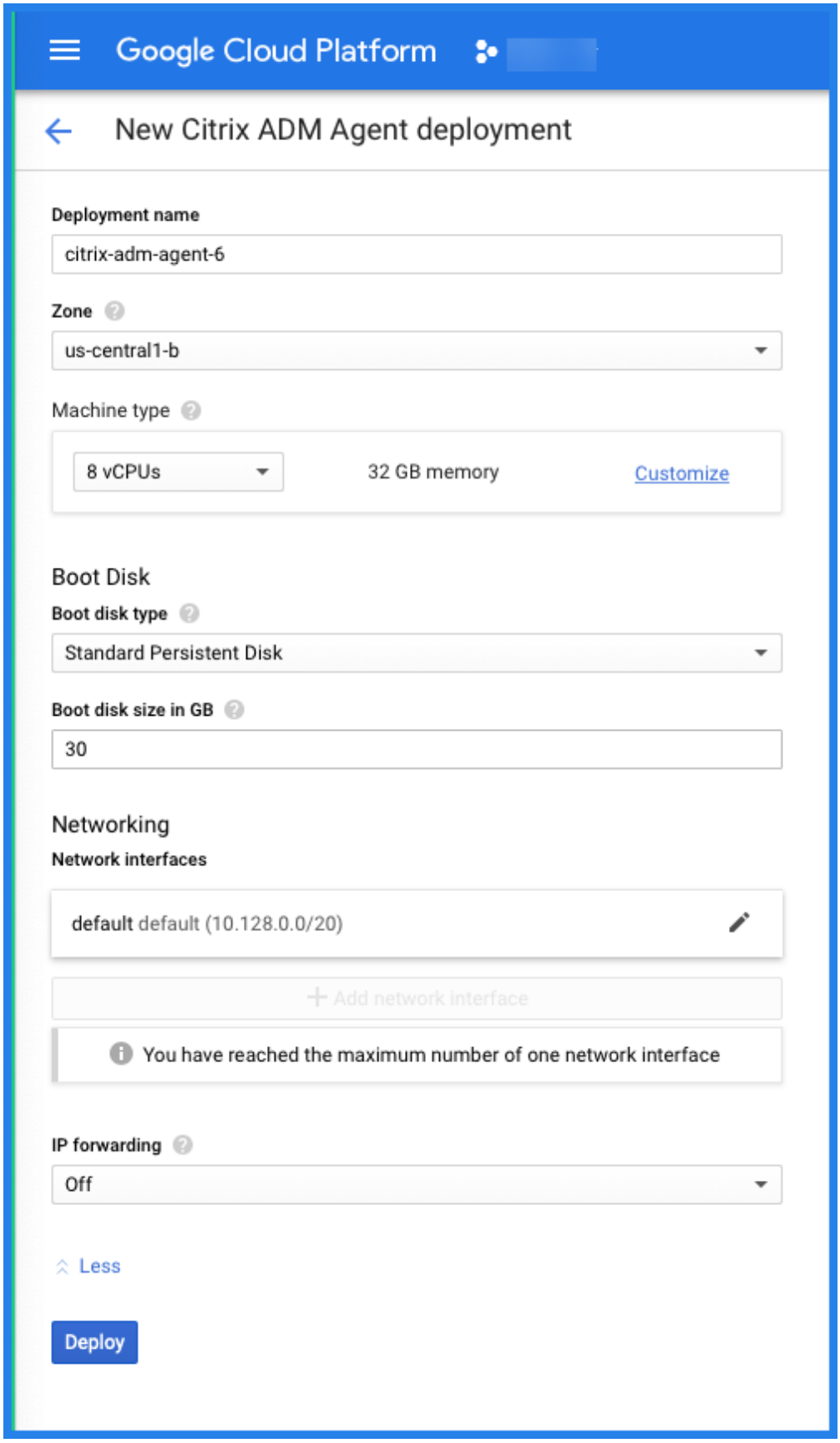
Installieren Sie den Citrix ADM Agent auf GCP

Befolgen Sie diese Schritte, um einen ADM-Agenten auf GCP zu installieren.

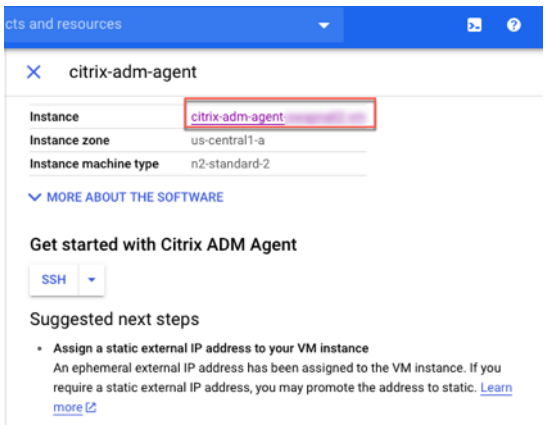
1. Melden Sie sich mit Ihren Anmeldeinformationen bei der GCP-Konsole (console.cloud.google.com) an und gehen Sie zum Marktplatz.
2. Geben Sie im Suchfeld **Citrix ADM Agent**ein.
3. Klicken Sie im Ergebnisfeld auf **Citrix ADM Agen**und dann auf **Launch**.



4. Auf der Seite **Neue Citrix ADM Agent-Bereitstellung** sind die meisten Optionen standardmäßig festgelegt. Sie können die Standardkonfigurationen nach Bedarf ändern und auf **Bereitstellen**klicken.



5. Nachdem der Agent bereitgestellt wurde, klicken Sie auf den Link Instanz und überprüfen Sie die Details auf der **Detailseite der VM-Instanz**.

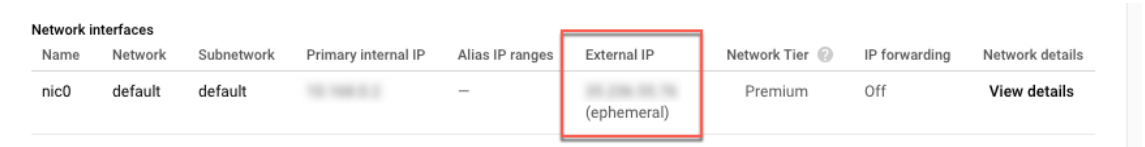


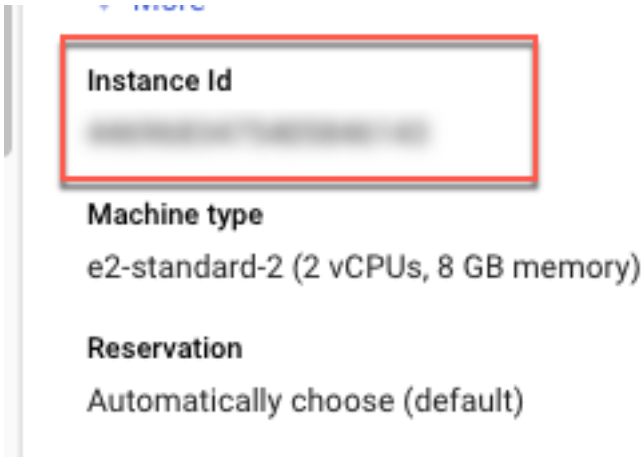
6. Melden Sie sich über einen SSH-Client mit der externen IP-Adresse des Agenten beim Agenten an. Verwenden Sie die folgenden Befehle:

   ```
   ssh nsrecover@<external IP address of the agent>
   ```

   Kennwort: Instanz-ID

   Können Sie die externe IP-Adresse und die Instanz-ID auf der **Detailseite der VM-Instanz finden** ?

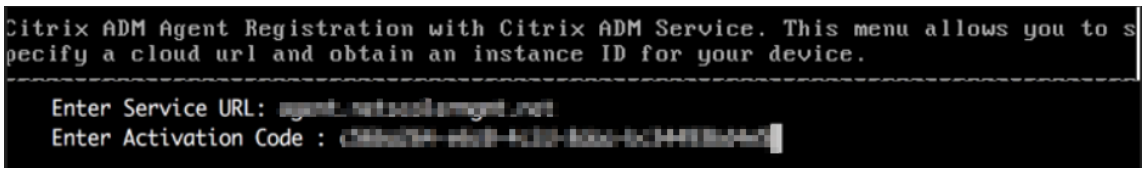




7. Geben Sie den folgenden Befehl ein, um den Bereitstellungsbildschirm aufzurufen: **deployment_type.py**

8. Geben Sie die **Service-URL** und den **Aktivierungscode** ein, den Sie kopiert und auf der Seite **Agents einrichten** in Citrix ADM gespeichert haben Erste Schritte. Der Agent verwendet die

Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.



Nach erfolgreicher Agentenregistrierung wird der Agent neu gestartet, um den Installationsvorgang abzuschließen.

Nachdem der Agent neu gestartet wurde, greifen Sie auf Citrix ADM zu und überprüfen Sie auf der Seite **Agent einrichten** unter **Ermittelte Agents** den Status des Agents.

Installieren von Citrix ADM Agent im Kubernetes-Cluster

April 28, 2021

> **Hinweis**
>
> Die Vorgehensweise zum Installieren eines Agenten als Microservice ist im Erste SchritteAbschnitt verfügbar.

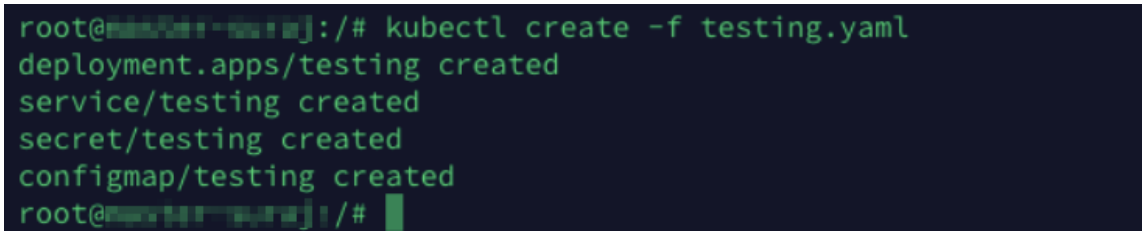
Im Kubernetes-Master-Knoten:

1. Speichern Sie die heruntergeladene YAML-Datei
2. Führen Sie den folgenden Befehl aus:

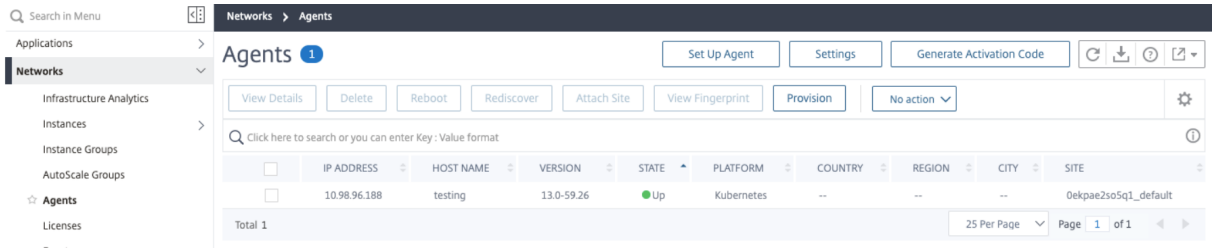
   `kubectl create -f <yaml file>`

   Beispiel: `kubectl create -f testing.yaml`

   Der Agent wurde erfolgreich erstellt.



Navigieren Sie in Citrix ADM zu **Netzwerke** > **Agents**, um den Agentstatus anzuzeigen.



Hilfe und Support

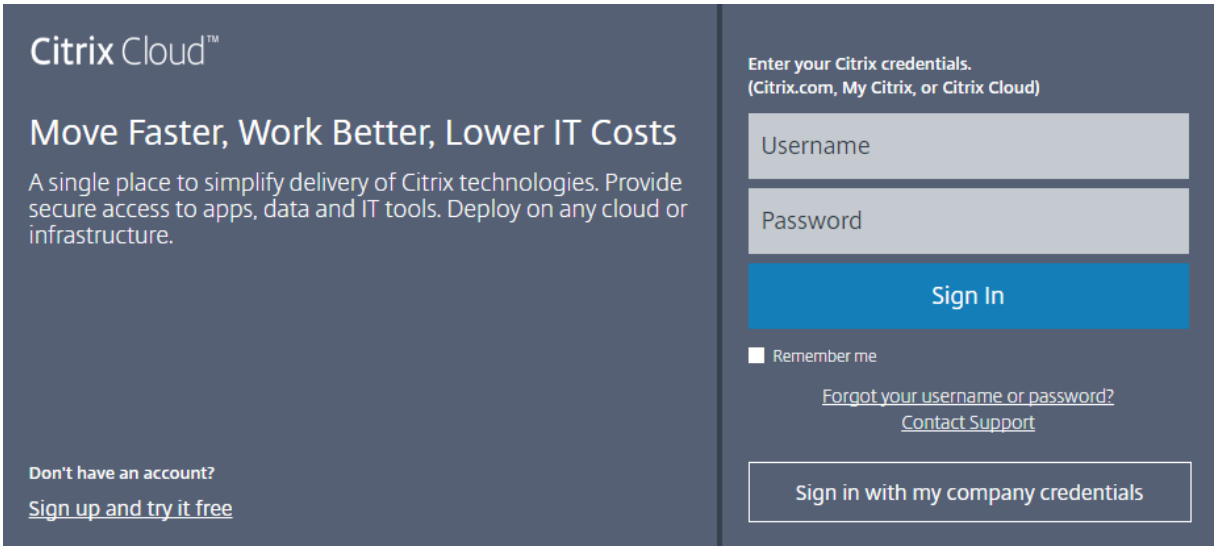
April 28, 2021

Als Citrix Cloud-Benutzer benötigen Sie manchmal Hilfe bei der Sicherstellung eines reibungslosen Funktionierens unserer Infrastruktur. In diesem Thema finden Sie weitere Informationen zu den verschiedenen Hilfe- und Unterstützungsoptionen sowie zum Zugriff auf diese Optionen.

Erstellen eines Citrix Cloud-Kontos

Falls bei der Registrierung für ein Citrix Cloud-Konto ein Fehler auftritt, wenden Sie sich an den Citrix Customer Service.

Melden Sie sich an Ihrem Konto an



Falls beim Anmelden an Ihrem Citrix Cloud-Konto Probleme auftreten:

- Stellen Sie sicher, dass Sie die E-Mail-Adresse und das Kennwort verwenden, die Sie bei der Registrierung angegeben haben.

- Citrix Cloud fordert Sie automatisch auf, Ihr Kennwort zurückzusetzen, bevor Sie sich anmelden können, wenn:
  - Sie haben sich seit einiger Zeit nicht bei Citrix Cloud angemeldet
  - Ihr Kennwort entspricht nicht den Anforderungen von Citrix Cloud
- Weitere Informationen finden Sie unter Ändern Ihres Kennwortsin diesem Artikel.
- Wenn Ihr Unternehmen es Benutzern ermöglicht, sich auch mit den Firmenanmeldeinformationen an Citrix Cloud anzumelden, klicken Sie auf **Mit Firmenanmeldeinformationen anmelden** und geben Sie die Anmelde-URL Ihres Unternehmens ein. Sie können dann Ihre Firmenanmeldeinformationen eingeben, um auf das Citrix Cloud-Konto Ihres Unternehmens zuzugreifen. Wenden Sie sich an Ihren Administrator, wenn Sie die Anmelde-URL Ihres Unternehmens nicht kennen.

Ändern Sie Ihr Kennwort

Wenn Sie Ihr Citrix Cloud-Kontokennwort **vergessen haben, klicken Sie auf Benutzernamen oder Kennwort vergessen?**, und Sie können die E-Mail-Adresse Ihres Kontos eingeben. Sie erhalten eine E-Mail, um Ihr Kennwort zurückzusetzen. Wenn Sie die E-Mail zum Zurücksetzen des Kennwort nicht erhalten oder weitere Unterstützung benötigen, wenden Sie sich bitte an Citrix Customer Service.

Zum Schutz Ihres Kontokennworts fordert Citrix Cloud Sie beim Anmelden möglicherweise auf, Ihr Kennwort zurückzusetzen. Diese Aufforderung wird in folgenden Situationen angezeigt:

- Ihr Kennwort entspricht nicht den Komplexitätsvorgaben von Citrix Cloud. Kennwörter müssen mindestens 8 Zeichen lang sein und Folgendes enthalten:
  - Mindestens eine Zahl
  - Mindestens einen Großbuchstaben
  - Mindestens ein Symbol: `! @ ## $ % ^ * ? + = –`
- Ihr Kennwort enthält im Wörterbuch enthaltene Wörter.
- Ihr Kennwort wird in einer bekannten Datenbank mit gefährdeten Kennwörtern aufgeführt.
- Sie haben sich in den vergangenen sechs Monaten nicht bei Citrix Cloud angemeldet.

Wenn Sie dazu aufgefordert werden, wählen Sie **Kennwort zurücksetzen**, um ein neues sicheres Kennwort für Ihr Konto zu erstellen.

Supportforen für Citrix Cloud

In den Supportforen für Citrix Cloud können Sie Hilfe erhalten, Feedback und Verbesserungsvorschläge hinterlassen, Unterhaltungen anderer Benutzer anzeigen oder selbst ein Thema diskutieren.

Citrix Supportmitarbeiter verfolgen diese Foren und beantworten Ihre Fragen. Andere Citrix Cloud-Community-Mitglieder bieten möglicherweise auch Hilfe an oder nehmen an der Diskussion teil.

Sie müssen sich nicht anmelden, um Forumsbeiträge zu lesen. Um selbst einen Kommentar zu posten oder auf ein Thema zu antworten, müssen Sie jedoch angemeldet sein. Verwenden Sie zur Anmeldung die Anmeldeinformationen für Ihr Citrix Konto oder die E-Mail-Adresse und das Kennwort, die Sie beim Erstellen Ihres Citrix Cloud-Kontos angegeben haben. Um ein Citrix Konto zu erstellen, gehen Sie zu Erstellen oder Anfordern eines Kontos.

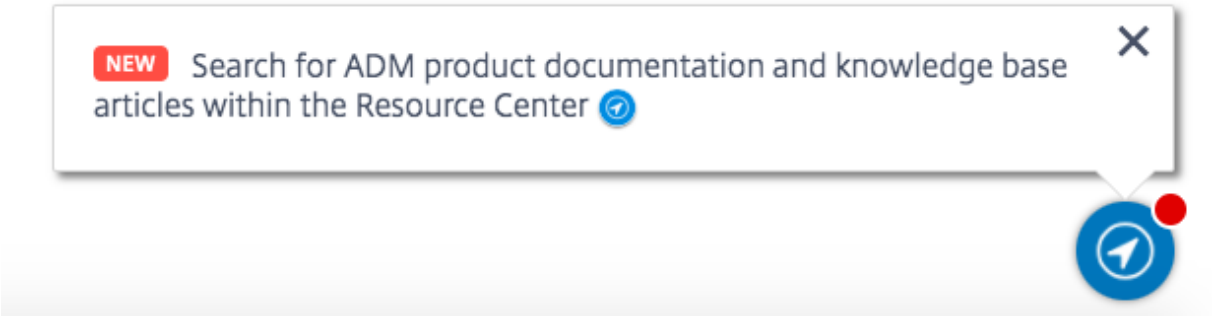
Supportartikel und Dokumentation

Citrix stellt umfangreiche Produkt- und Supportinhalte bereit, die Sie dabei unterstützen, Citrix Cloud optimal zu nutzen und Probleme mit Citrix Produkten zu lösen.

Citrix Cloud-Ressourcencenter

Das Citrix Cloud Resource Center bietet verschiedene Ressourcen, mit denen Sie die ersten Schritte mit den Citrix Cloud-Diensten, weitere Informationen zu Features und Probleme beheben können. Die angezeigten Ressourcen gelten für das Feature oder den Dienst in Citrix Cloud, mit dem Sie gerade arbeiten. Wenn Sie sich beispielsweise in der Verwaltungskonsole für Virtual Apps and Desktops befinden, werden im Ressourcencenter die folgenden Ressourcen angezeigt.

Greifen Sie jederzeit auf das Resource Center zu, indem Sie unten rechts in der Citrix Cloud-Konsole auf das blaue Kompasssymbol klicken.



- **Erste Schritte**: Bietet eine kurze Anleitung zu den wichtigsten Aufgaben speziell für den Service, mit dem Sie gerade arbeiten. Außerdem finden Sie Links zu Schulungs- und Onboarding-Ressourcen, die Ihnen helfen, mehr über Service-Funktionen zu erfahren und Ihre Endbenutzer für Ihren Erfolg einzurichten.
- **Ankündigungen**: Bietet Benachrichtigungen über neu veröffentlichte Funktionen und Links zu wichtigen Citrix Kommunikationen. Klicken Sie auf eine Feature-Benachrichtigung, um eine kurze geführte exemplarische Vorgehensweise des Features zu erhalten.
- **Artikel durchsuchen**: Enthält eine Liste mit Produktdokumentation und Knowledge Center-Artikeln für häufige Aufgaben und hilft Ihnen, weitere Artikel zu finden, ohne Citrix Cloud zu

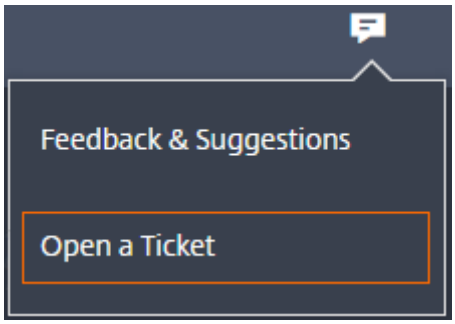
verlassen. Geben Sie eine Suchabfrage in das Feld **How do I ...** ein, um eine gefilterte Liste von Artikeln für den Service anzuzeigen, mit dem Sie arbeiten. Im Allgemeinen werden Supportartikel zuerst in der Liste angezeigt, gefolgt von Artikeln in der Produktdokumentation.

Citrix Tech Zone

Citrix Tech Zone enthält zahlreiche Informationen zu Citrix Cloud und zu anderen Citrix Produkten. Hier finden Sie Referenzarchitekturen, Diagramme, Videos und technische Unterlagen, die Einblicke in das Entwerfen, Erstellen und Bereitstellen von Citrix Technologien bieten.

Technischer Support

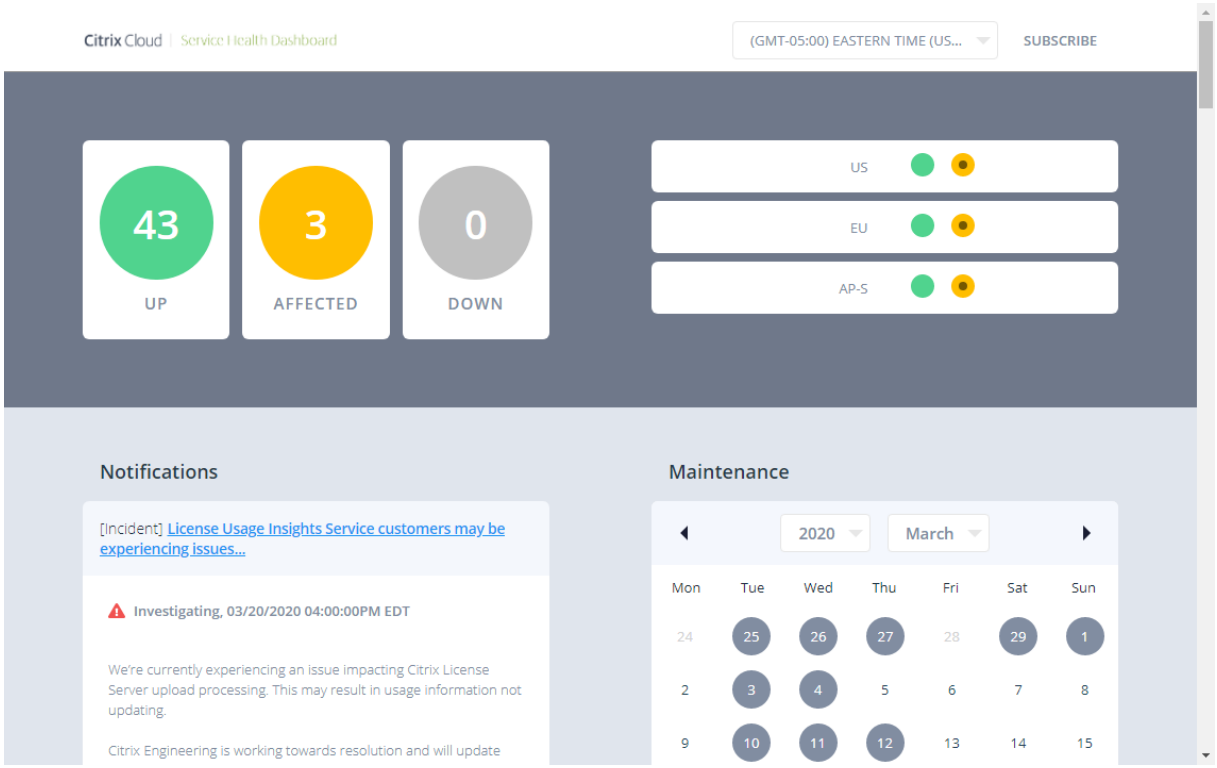
Wenn Sie bei einem Problem technische Hilfe benötigen, klicken Sie rechts oben im Bildschirm auf das Symbol **Feedback und Support**, und wählen Sie **Ticket erstellen**.



Klicken Sie auf **Zu My Support** und dann auf **My Support**, um ein Ticket im My Support-Portal zu erstellen. Im My Support-Portal können Sie außerdem bestehende Tickets verfolgen und aktuelle Produktansprüche anzeigen.

Service Health Dashboard

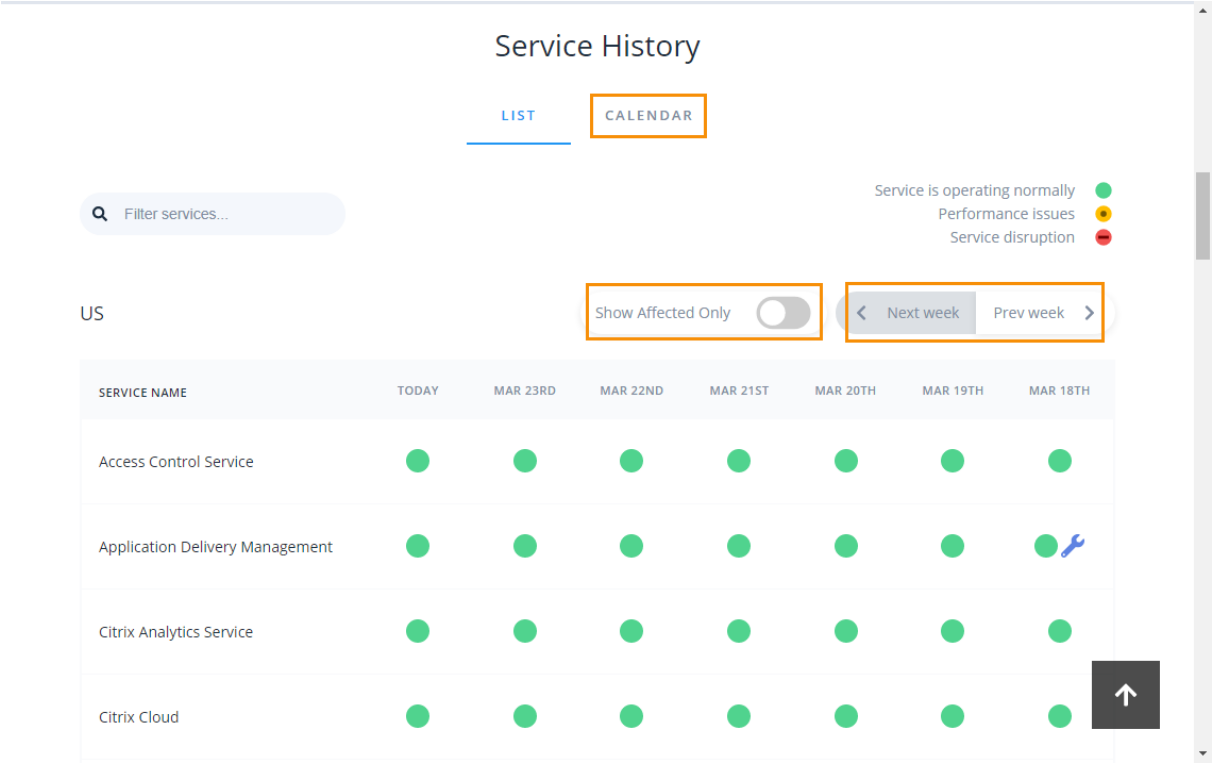
Der Citrix Clouddienst-Integritäts-Dashboardbietet einen Überblick über die Echtzeitverfügbarkeit der Citrix Cloud-Plattform und der Dienste in jeder geografischen Region. Wenn Sie Probleme mit Citrix Cloud haben, überprüfen Sie das Dienstintegritäts-Dashboard, ob Citrix Cloud oder bestimmte Dienste normal funktionieren.



Verwenden Sie das Dashboard, um mehr über die folgenden Bedingungen zu erfahren:

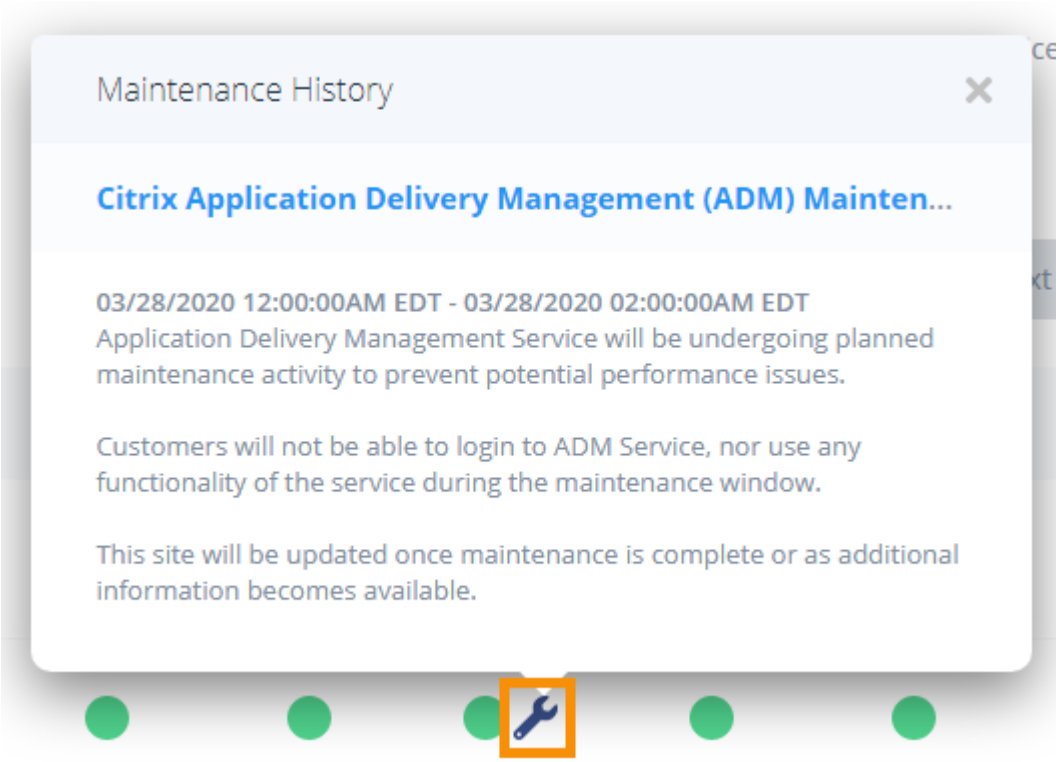
- Der aktuelle Verfügbarkeitsstatus aller Citrix Cloud-Dienste, gruppiert nach geografischer Region
- Der Dienstintegritätsverlauf jedes Dienstes für die letzten sieben Tage (Standard) oder für vorherige Sieben-Tage-Inkremente
- Wartungsfenster für bestimmte Dienste

Standardmäßig wird der Dienstintegritätsstatus als Liste angezeigt, Sie können den Status jedoch auch in einer Kalenderansicht anzeigen. Wählen Sie **Weiter** oder **Zurück** aus, um in Schritten von sieben Tagen durch den Service-Integritätsverlauf zu blättern. Sie können die Liste auch so filtern, dass nur betroffene Dienste angezeigt werden.

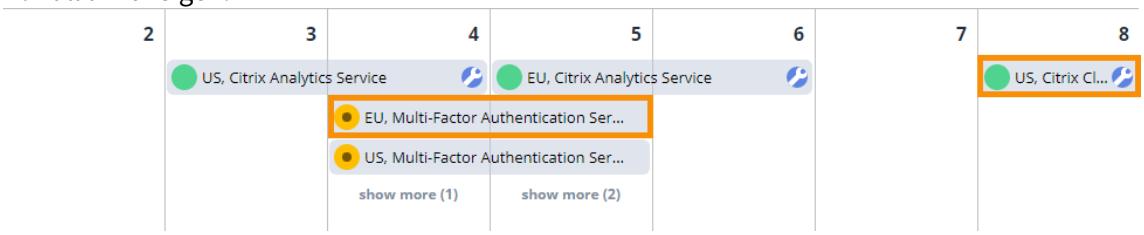


So zeigen Sie detailliertere Informationen zum Service-Integritätsvorfall für einen betroffenen Service an:

- Klicken Sie in der Listenansicht auf das Symbol neben dem Dienstindikator, um detailliertere Informationen zum Service-Integritätsvorfall anzuzeigen.

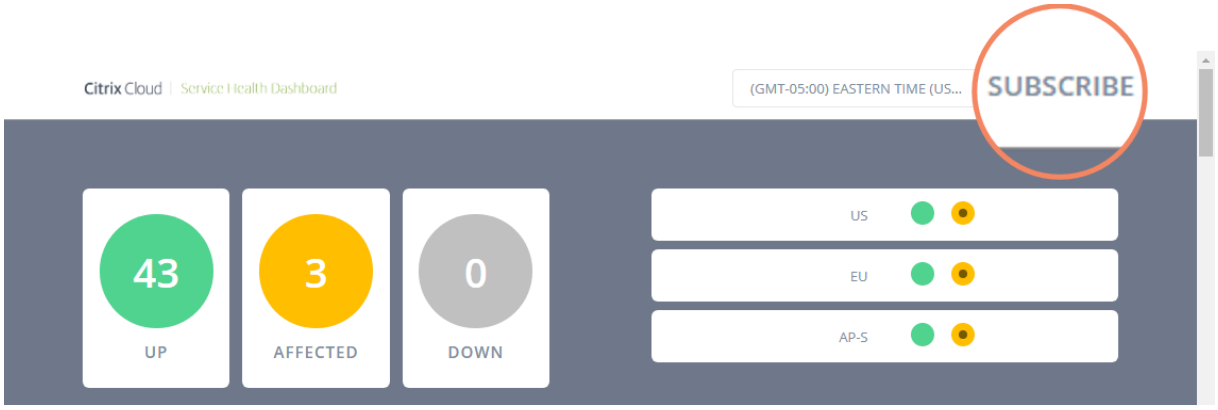


- Klicken Sie in der Kalenderansicht auf den Diensteintrag, um den Status für den Service-Health-Vorfall anzuzeigen.

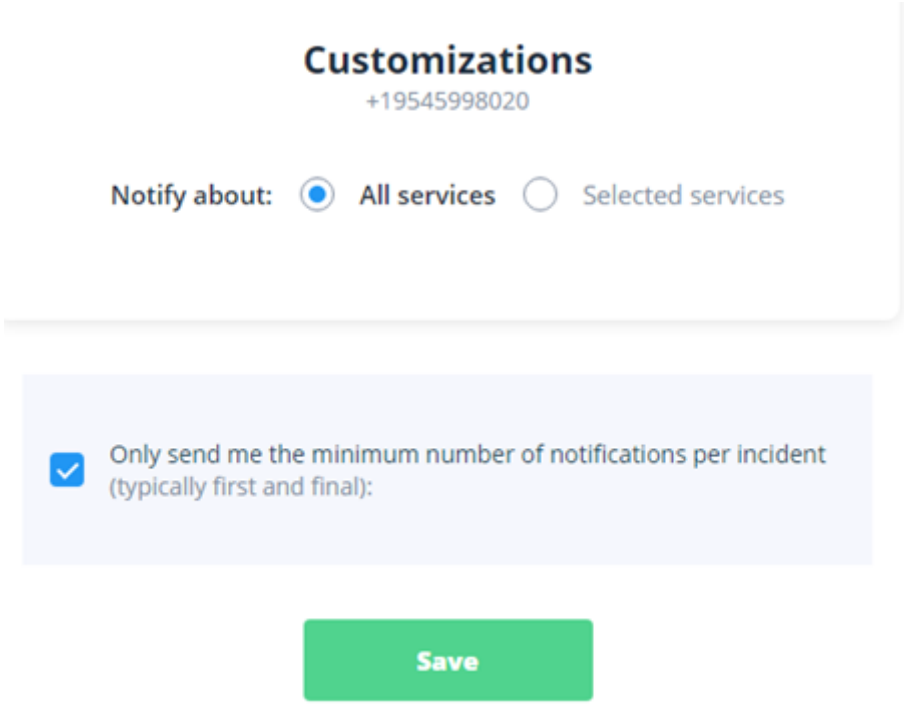


Dienstzustands-Abonnements

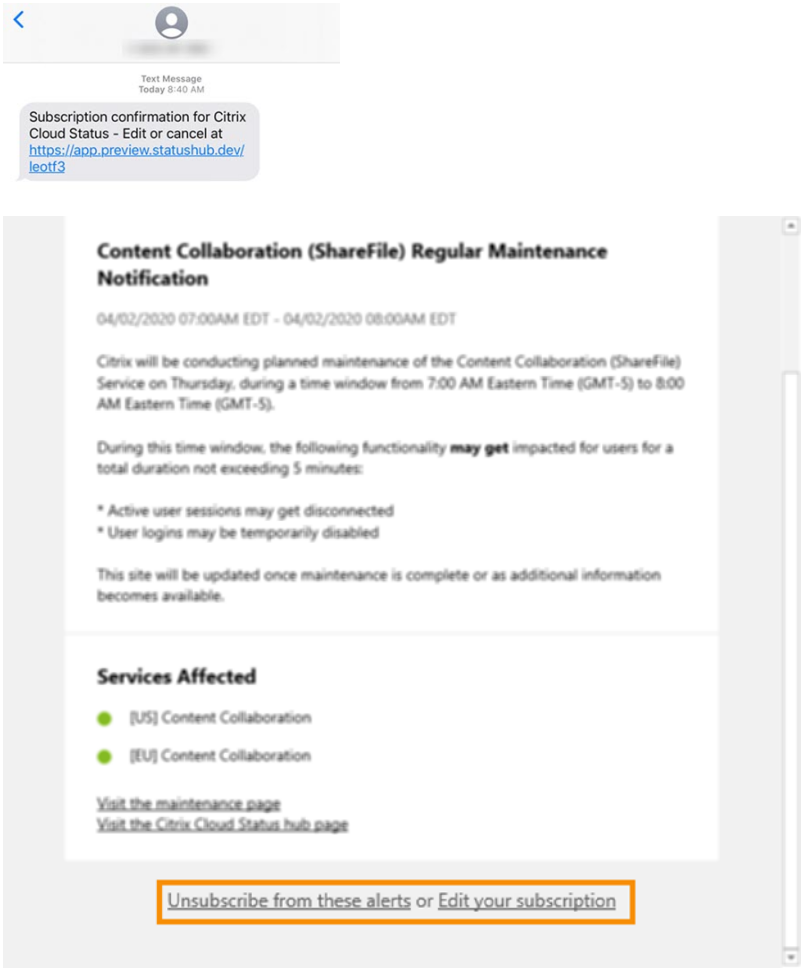
Klicken Sie oben rechts im Dashboard auf **Abonnieren**, und wählen Sie die gewünschte Benachrichtigungsmethode aus, um Benachrichtigungen zu erhalten.



Sie können Benachrichtigungen für alle Dienste oder nur für die ausgewählten Dienste abonnieren. Standardmäßig erhalten Sie alle Benachrichtigungen für einen Service-Integritätsvorfall. Um die Häufigkeit von Benachrichtigungen während eines Vorfalls zu begrenzen, können Sie nur die ersten und letzten Benachrichtigungen empfangen.



Abhängig von der Abonnementmethode sind Links zum Abbestellen und Ändern Ihrer Einstellungen in der Bestätigungsnachricht des Abonnements enthalten, die Sie erhalten (z. B. beim Abonnieren von Telefonbenachrichtigungen) oder in jeder Benachrichtigung (z. B. wenn Sie E-Mail-Benachrichtigungen abonnieren).



So melden Sie sich ab oder ändern Sie Ihre Abonnementeinstellungen:

1. Suchen Sie eine vorhandene Benachrichtigung, und wählen Sie den Link aus, um das Abonnement abzubestellen oder Ihre Benachrichtigungseinstellungen zu ändern.
2. Wenn Sie sich abmelden, wählen Sie **Abmelden** aus, und wählen Sie dann die Benachrichtigungsmethode aus, die Sie stornieren möchten. Wenn Sie alle Benachrichtigungsmethoden abonnieren möchten, wählen Sie **Alle Abonnements entfernen**aus.
3. Wenn Sie die Einstellungen ändern, wählen Sie die Benachrichtigungsmethode aus, nehmen Sie die entsprechenden Änderungen an den Diensten und minimalen Vorfallbenachrichtigungen vor, und wählen Sie dann **Speichern**aus.

Berührungsarmes Onboarding von Citrix ADC-Instanzen mit Citrix ADM Service Connect

April 28, 2021

Wenn Ihre hybride Multi-Cloud (HMC) -Infrastruktur wächst, werden die Herausforderungen bei der Verwaltung, Überwachung, Analyse und Fehlerbehebung von ADC-Instanzen multifacht. Ein zentralisierter Controller, der Einblick in Ihre gesamte Infrastruktur und alle darauf ausgeführten Anwendungen bietet, wird zum Bedarf der Stunde.

In der heutigen Welt muss das Onboarding Ihrer Instanzen auf einen zentralen Controller schnell, einfach und berührungsarm erfolgen. Unter Berücksichtigung dieses Bedarfs startet der Citrix ADM-Service einen neuen Onboarding-Workflow, der Ihnen eine schnellere Möglichkeit bietet, einen vollständigen Überblick über Ihre HMC-Bereitstellung zu erhalten.

Überblick: Komponenten des ADM-Service-Onboarding-Workflows

Die Bausteine dieses Workflows sind zwei ADC-Seiten-Komponenten: ADC-Service connect und Call Home.

- **ADM service connect**: Es ist eine neue Funktion in ADC, die das nahtlose Onboarding von Citrix ADC-Instanzen in den Citrix ADM-Dienst ermöglicht. Mit dieser Funktion kann die Citrix ADC-Instanz automatisch eine Verbindung mit dem Citrix ADM-Dienst herstellen und System-, Nutzungs- und Telemetriedaten an den ADM-Dienst senden. Basierend auf diesen Daten gibt Ihnen der Citrix ADM-Dienst Einblicke und Empfehlungen zu Ihrer Citrix ADC-Infrastruktur. Zum Beispiel die schnelle Identifizierung von Performance-Problemen, eine hohe Ressourcennutzung und kritische Fehler.

  ADM Service Connect ist in den folgenden ADC-Versionen verfügbar:

  - Citrix ADC MPX und VPX Image Version 12.1 57.18 und höher und 13.0 61.48 und höher. Weitere Informationen finden Sie unter Einführung in Citrix ADM Service Connect für Citrix ADC Appliances.
  - Citrix ADC SDX Version Image 12.1 58.14 und höher und 13.0 61.48 und höher. Weitere Informationen finden Sie unter Einführung in Citrix ADM Service Connect für Citrix ADC SDX-Appliances.

- **Call Home**: Es handelt sich um eine vorhandene Funktion in ADC, die die Instanzen regelmäßig überwacht und Daten automatisch auf den Citrix Technical Support Server hochlädt. Weitere Informationen finden Sie unter Call Home. Die von Call Home gesammelten Daten werden ebenfalls an den ADM-Dienst weitergeleitet, um diesen neuen Workflow zu ermöglichen.

Alle ADC-Instanzen mit Internetkonnektivität oder Call Home oder Instanzen, die mit ADM Service Connect aktiviert sind, sind mit dem ADM-Dienst verbunden. Der ADM-Dienst beginnt mit der Erfassung relevanter Metriken aus diesen ADC-Instanzen über die Call Home-Route, die ADM-Dienstverbindungsroute oder beides. Weitere Informationen finden Sie unter Data Governance für MPX- und VPX-Instanzen und Data Governance für SDX-Instanzen.

Mithilfe dieser Daten erstellt der ADM-Dienst ein Inventar von ADC-Instanzen für jeden Kunden (eindeutige Organisations-ID), das Ihnen eine konsolidierte Liste Ihrer ADC-Instanzen anzeigt. Der ADM-Service verwendet diese Daten auch, um Erkenntnisse über Ihre ADC- und Gateway-Instanzen zu gewinnen, die aussagekräftige Einblicke in Ihre HMC-Bereitstellungen geben, Probleme identifizieren und Maßnahmen zur Abschwächung der Probleme empfehlen. Bevor Sie die Probleme abschwächen können, müssen Sie die ADC-Instanzen in den ADM-Dienst einbinden.
Sie können die **Option ADC- und Gateway-Instanzen** auswählen aktivieren und die ADC-Instanzen auswählen, die Sie beim ADM-Service einbinden möchten. Nach dem Start werden Sie zum Onboarding-Prozess geführt.

Der Auto-Onboarding-Prozess verwendet ADM Service Connect, wodurch das Erlebnis automatisiert, nahtlos und schneller wird. Für ADC-Instanzen auf Versionen, die ADM Service Connect und Auto-Onboarding nicht unterstützen, bietet der ADM-Dienst verwendungsskriptbasiertes Onboarding, bei dem es sich um einen halbautomatisierten Prozess handelt.

> **Hinweis**
>
> Das automatische und skriptbasierte Onboarding verwendet einen integrierten Agenten. Dieser Workflow bietet Ihnen jedoch auch die Flexibilität, einen externen Agenten für das Onboarding zu verwenden. Sie können das externe Agenten-basierte Onboarding verwenden, wenn Sie die gepoolte Lizenzierung oder die vollständige Analytics-Suite im ADM-Service verwenden möchten. Oder wenn Sie sowohl die gepoolte Lizenzierung als auch die komplette Analytics-Suite verwenden möchten. Der integrierte Agent unterstützt nur Verwaltung und Überwachung.

Eine kurze Tour durch das Onboarding

Ihr erster Touchpoint auf der Onboarding-Reise ist eine vom Produkt initiierte E-Mail. Hier ist ein kurzer Rundgang durch die Onboarding-Reise:

1. Eine von **Citrix vom Produkt initiierte E-Mail**: Sie erhalten eine E-Mail vom ADM-Service, die einige wichtige Erkenntnisse über Ihre ADC-Infrastruktur zeigt, und laden Sie ein, mit dem ADM-Dienst zu beginnen. Klicken Sie auf den Link in E-Mail.
2. **Citrix Cloud-Anmeldeseite**: Sie müssen sich mit Ihren **My Citrix-Anmeldeinformationen bei Citrix** Cloud anmelden.
3. **Willkommensseite für den Citrix ADM Service**: Sie erhalten einen Überblick über den ADM-Service und seine Vorteile.
4. **Einblicke in Ihre ADC- und Gateway-Instanzen**: Sie erhalten detaillierte Einblicke in Ihre gesamte ADC-Infrastruktur, einschließlich Sicherheitsberatung (Beratung zu aktuellen Citrix CVEs), Upgrade-Beratung (Ratschläge basierend auf EOM/EOL-Zeitplänen), wichtigen Kennzahlen, Trends und Highlights, die die ADC-Leistung betreffen Gesundheit und empfiehlt eine

Möglichkeit, die Probleme zu mildern.

5. **Wählen Sie ADC- und Gateway-Instanzen für Onboard**aus: Sie erhalten eine konsolidierte Ansicht Ihres ADC-Inventars. Sie können auswählen, welche ADC-Instanzen Sie beim ADM-Service einbinden möchten.
6. **Onboarding von ADC-Instanzen an ADM**: Basierend auf den für das Onboarding ausgewählten ADC-Instanzen führt ADM Sie beim Onboarding-Prozess. Standardmäßig ist der integrierte Agent für das automatische Onboarding ausgewählt.
7. **ADM GUI-Dashboard**: Nach Abschluss des Onboardings werden Sie zum ADM-Instanz-Dashboard geführt.

> **Hinweis:**
>
> Dieser Workflow wird stufenweise durch Kanarienfreisetzung eingeführt (GA). Sie erhalten eine E-Mail, wenn diese Funktion in Ihrer ADM-Dienstumgebung verfügbar ist.

Weitere Einzelheiten zu diesen Onboarding-Methoden finden Sie unter Onboard Citrix ADC-Instanzen mit Citrix ADM Service Connect.

Onboard Citrix ADC-Instanzen mit Citrix ADM Service Connect

April 28, 2021

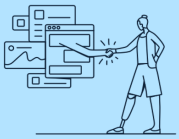
Nachfolgend finden Sie eine Schritt-für-Schritt-Anleitung, die Ihnen den Einstieg in den ADM-Service erleichtert. Bevor Sie beginnen, lesen Sie, wie der Citrix ADM-Dienst einen neuen Onboarding-Workflow startet, der Ihnen eine schnellere Möglichkeit bietet, einen vollständigen Überblick über Ihre hybride Multi-Cloud (HMC) -Bereitstellung zu erhalten. Siehe Berührungsarmes Onboarding von Citrix ADC-Instanzen mit Citrix ADM Service Connect.

Schritt 1: Loslegen

Sie erhalten eine E-Mail vom ADM-Service, die einige wichtige Erkenntnisse über Ihre ADC-Infrastruktur zeigt und Sie dazu auffordert, mit dem ADM-Dienst zu beginnen.

citrix

Onboard to Citrix ADM Service for Security Advisory



Hello [redacted] Org ID - [redacted]

As a valued Citrix customer, your application delivery infrastructure security is our top concern. To help keep your infrastructure secure, we just launched **security advisory and upgrade advisory** for your Citrix ADCs.

These new features can identify outdated software deployed in your ADC fleet, notify you of known vulnerabilities in these releases, and suggest steps you can take to remediate these issues.

Below, you'll see a preview of these advisories and other key insights customized to your infrastructure. More information and recommended actions are available when you onboard to Citrix ADM service. You can get started with Citrix ADM Service Express account at no additional cost.

Insights on your ADC & Gateway infrastructure

These insights are based on data provided via Call Home and/or Citrix ADM Service Connect.

ADC instances by platforms

30	20	5	5
Total	VPX	SDX	MPX

Security Advisory

5 ADC instances are on versions with known common vulnerability exposures (CVEs).
This advisory is based on ADC build version scan only & more conclusive & exhaustive security advisory insights can be seen after onboarding all your ADCs to ADM Svc

Upgrade Advisory

2 ADC instances are on versions that have reached end of life in last 365 days or earlier.

1 ADC instance is on a version that will reach end of life in next 365 days.

3 ADC instances are on versions that have reached end of maintenance in last 365 days or earlier.

4 ADC instances are on versions that will reach end of maintenance in next 365 days.

2 ADC instances are on older builds and releases.

Recent events

4 ADC instances encountered SSL card failure.
2 ADC instances encountered hard disk failure.

Resource utilization

2 ADC instances CPU usage exceeded 50%
3 ADC instances memory usage exceeded 50%

ADC deployment

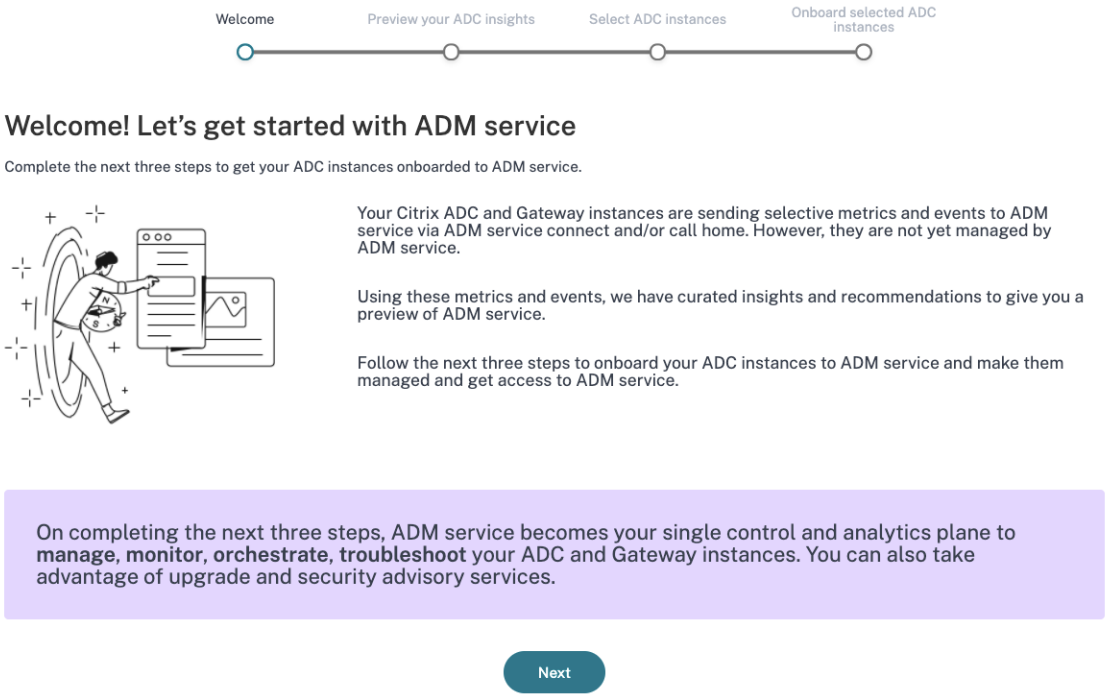
5 ADC instances are not deployed as High Availability (HA) pair. Citrix ADM recommends HA pair for production ADC instances.

To get more details and recommendations on these insights, **onboard your ADC instances to Citrix ADM service, today.**

As a first step, you will need to create Citrix Cloud account by clicking on the button below.

Onboard to ADM Service

1. Klicken Sie in der E-Mail auf **Erste Schritte**, um den Onboarding-Prozess einzuleiten.
2. Melden Sie sich mit Ihren My Citrix/Citrix Cloud-Anmeldedaten bei Citrix Cloud an.
3. Nehmen Sie sich auf der Zielseite des Citrix ADM Service einen Moment Zeit, um zu lesen, warum Sie da sind und welche Vorteile Sie bei der Verwendung von ADM haben.



4. Klicken Sie auf **Weiter**. Die Seite **Insights auf Ihren ADC- und Gateway-Instanzen** wird geöffnet.

Die nächsten Schritte dienen als geführter Workflow, um Ihnen eine Vorschau auf das Angebot von ADM zu geben und Ihnen zu helfen, Ihre ADC-Instanzen nahtlos in den ADM-Dienst einzubinden.

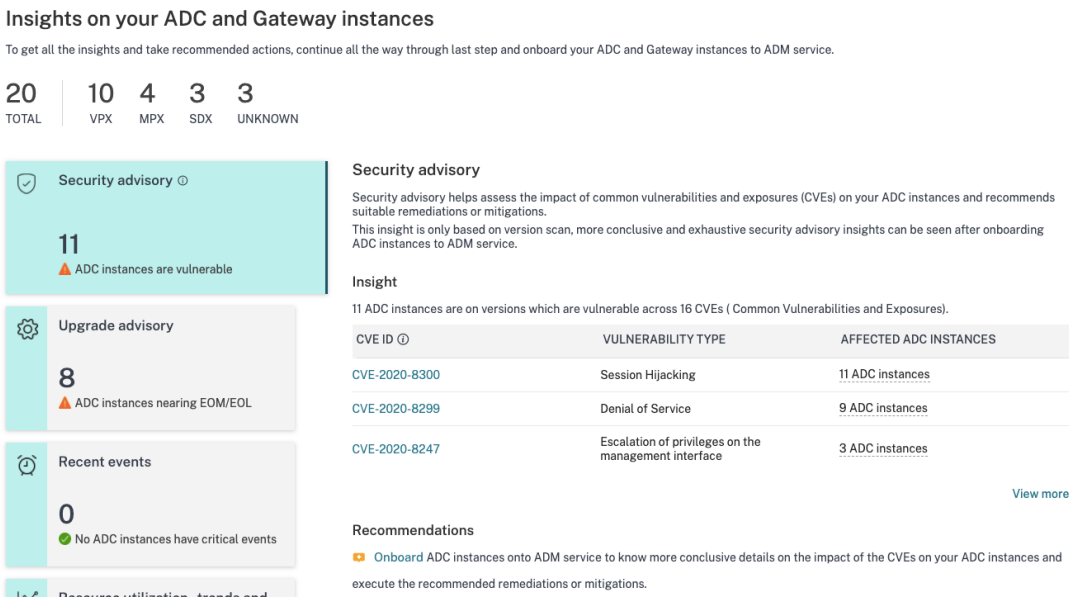
Schritt 2: Einblicke in Ihre ADC- und Gateway-Instanzen

Diese Insights-Seite verwendet die Daten, die über Call Home oder ADM Service connect oder sowohl Call Home als auch ADM Service Connect gesammelt wurden, um Einblicke in Ihre ADC-Instanzen zu erhalten. Diese Seite gibt Ihnen Einblicke in Ihre gesamte ADC-Infrastruktur, einschließlich Sicherheitsberatung (Beratung zu aktuellen Citrix CVEs), Upgrade-Beratung (Ratschläge basierend auf EOM/EOL-Zeitlinien), wichtigen Kennzahlen, Trends und Highlights der Probleme, die sich auf die ADC-Leistung und Gesundheit auswirken, und empfiehlt eine Möglichkeit, die Probleme zu mildern. Diese Erkenntnisse und Empfehlungen sind nur eine kleine Vorschau auf die Fülle von Vorteilen und Mehrwert, die der ADM-Dienst zu bieten hat. Um viele weitere Vorteile, detaillierte Einblicke zu erhalten und die empfohlenen Aktionen ausführen zu können, müssen Sie die ADC-Instanzen in ADM einbinden.

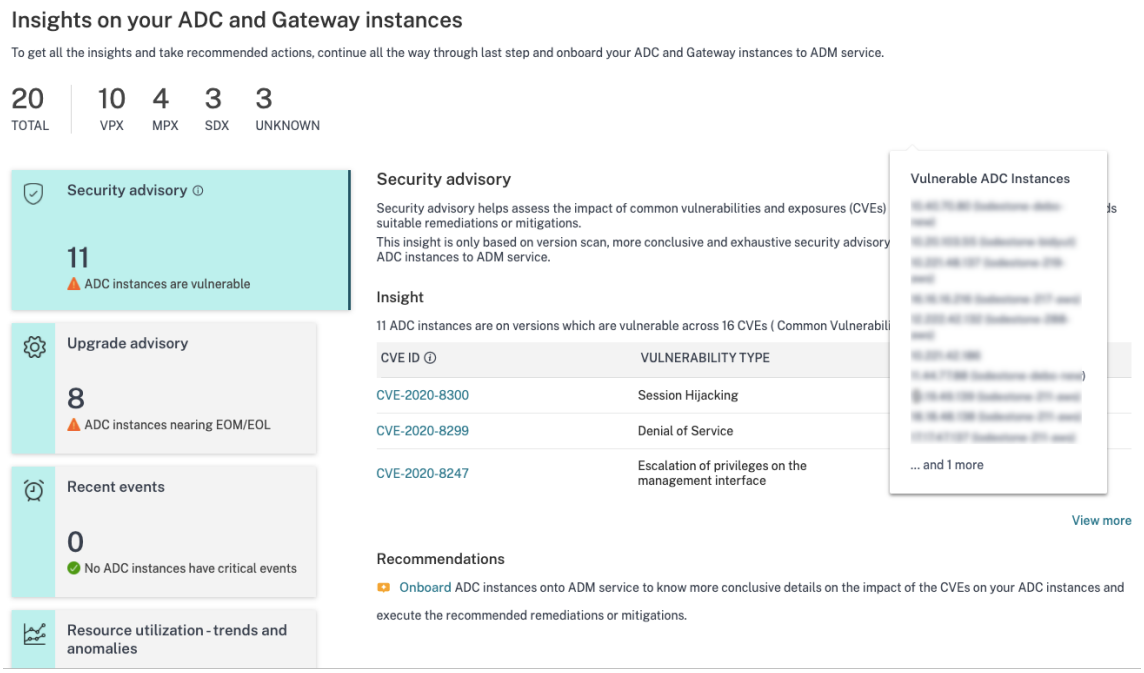
Die Erkenntnisse und Empfehlungen sind in folgende Typen unterteilt:

- **Sicherheitsberatung**: Onboard-ADC-Instanzen, um die CVE-Auswirkungsdetails auf Ihre ADC-Instanzen zu erhalten und die empfohlenen Korrekturen oder Minderungen durchzuführen.
- **Upgrade-Beratung**: Integrieren Sie ADC-Instanzen in ADM und aktualisieren Sie Ihre ADC-Instanzen, die EOM/EOL erreicht haben oder erreichen oder sich auf älteren Releases/Builds befinden.
- **Letzte Ereignisse**: Onboard-ADC-Instanzen an ADM, um mehr als 200 Ereignisse regelmäßig zu überwachen und Regeln zu erstellen, um über E-Mail benachrichtigt zu werden, PagerDuty, Slack, ServiceNow, ergreifen geeignete Maßnahmen.
- **Ressourcennutzung - Trends und Anomalien**: Onboard-ADC-Instanzen an ADM, um einen umfassenden Überblick über den Zustand von ADC-Instanzen, Leistungsprobleme und Empfehlungen zur Abwehr dieser Probleme zu erhalten. Sie können auch die prognostizierte CPU- und Speichernutzung für Ihre ADC-Instanzen bewerten.
- **Leitfaden zur ADC-Bereitstellung**: Onboard-ADC-Instanzen für ADM und Konfiguration als HA-Paar unter Verwendung von Konfigurationsjobs auf ADM.

1. **Sicherheitsberatung**: Citrix ADM Security Advisory informiert Sie über Schwachstellen, die Ihre ADC-Instanzen gefährden, und empfiehlt Abgrenzungen und Behebungen. Sie können die CVE-ID, den Schwachstellentyp und die betroffenen ADC-Instanzen überprüfen. Der CVE-ID-Link geht zum Artikel im Sicherheitsbulletin.



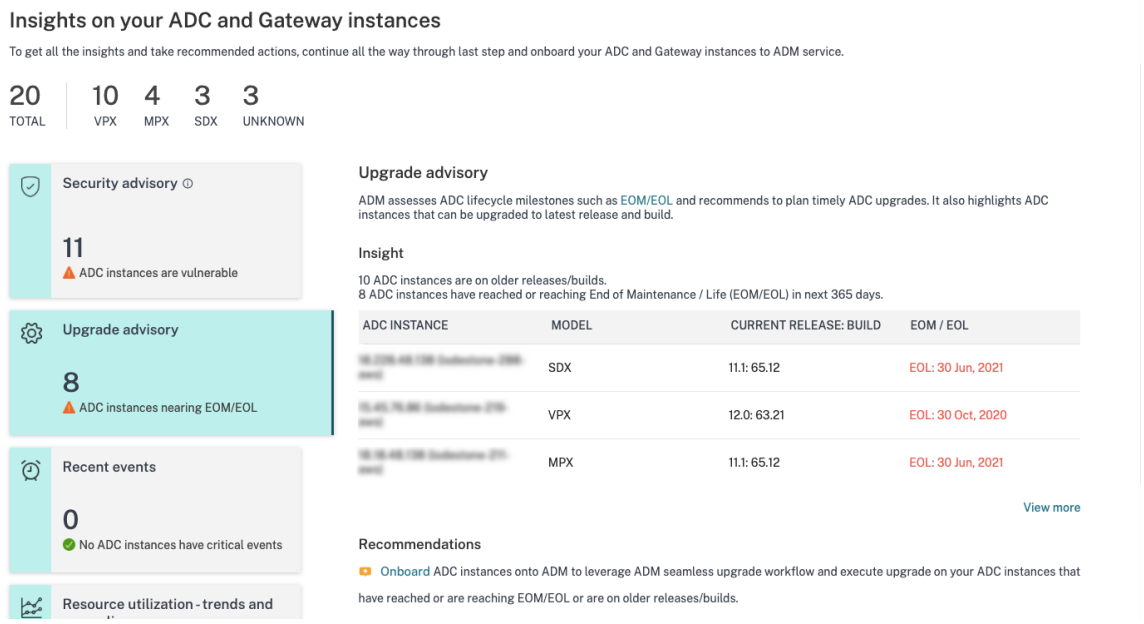
Die Empfehlung führt Sie dazu, Ihre ADC-Instanzen an den ADM Service zu binden, um weitere Informationen zu den Auswirkungen von CVE auf Ihre ADC-Instanzen zu erhalten und die empfohlene Risikominderung oder -behebung durchzuführen. Klicken Sie auf die betroffenen ADC-Instanzen, um die IP-Adressen der betroffenen Instanzen zu sehen.



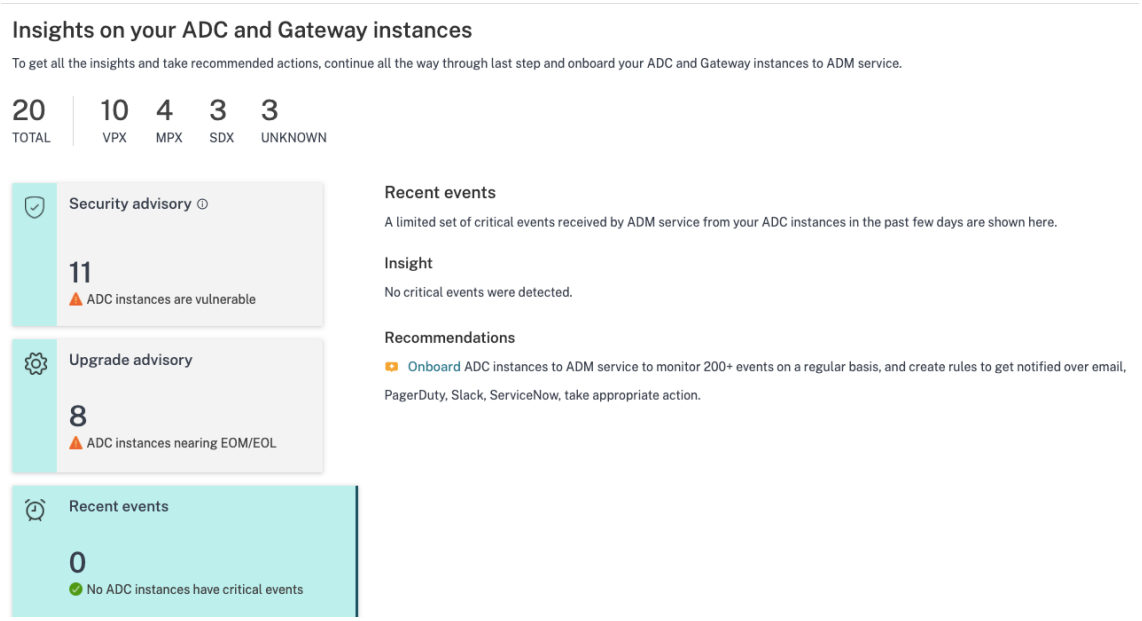
2. **Upgrade-Beratung**: Verwenden Sie diese Empfehlung, um zu überprüfen, welche ADC-Instanzen sich der EOM/EOL nähern oder sich auf älteren Builds befinden.

   Basierend auf diesen Erkenntnissen empfiehlt ADM Ihnen, ein rechtzeitiges Upgrade vor EOM/EOL zu planen oder von den neuesten Funktionen und Korrekturen zu profitieren.

   Um das Upgrade durchzuführen, müssen Sie Ihre ADC-Instanzen im ADM-Service einbinden.

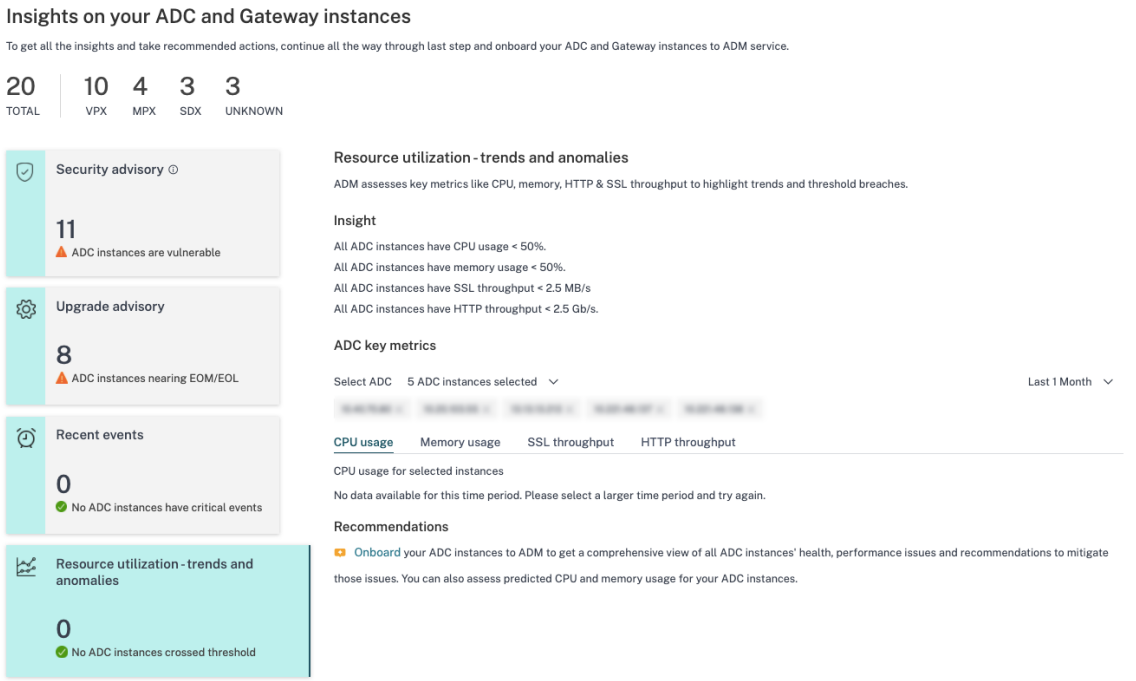


3. **Aktuelle Ereignisse**: Erhalten Sie Details zu einigen kritischen Fehlern, die bei den ADC-Instanzen aufgetreten sind, und eine Liste der ADC-Instanzen, bei denen die Fehler aufgetreten sind.

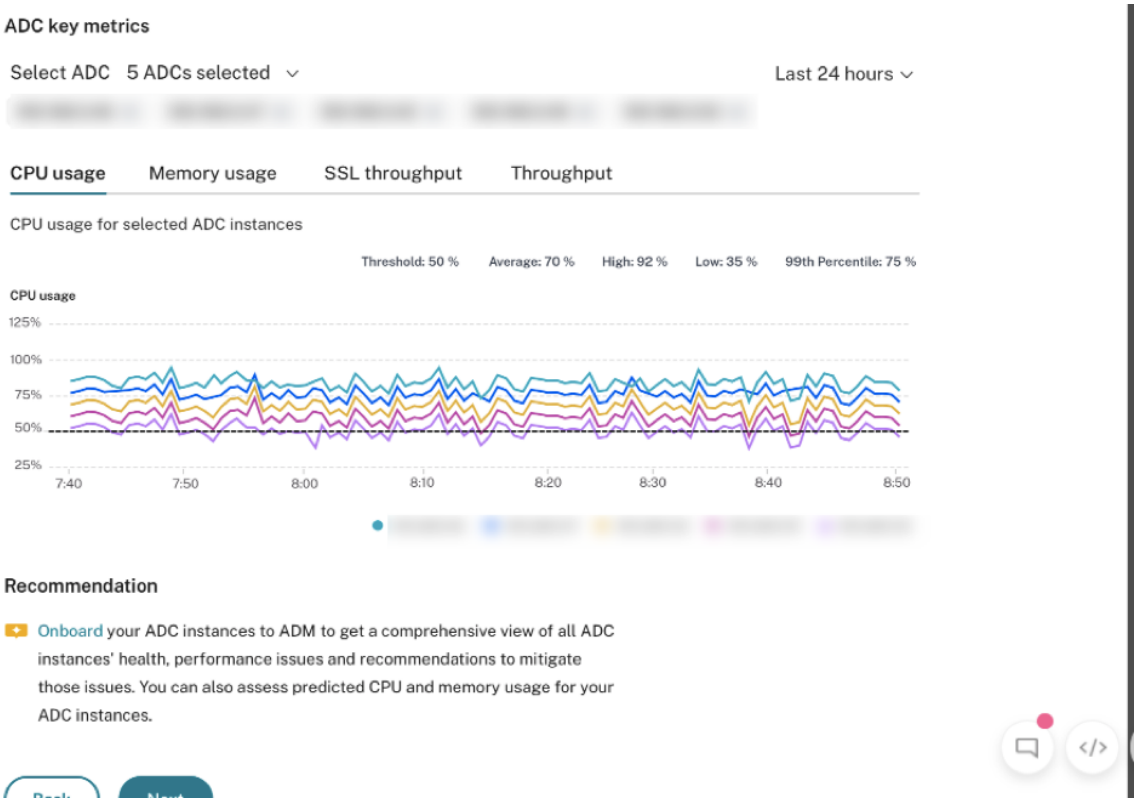


4. **Ressourcennutzung - Trends und Anomalien**: Hier finden Sie Einblicke in eine hohe Ressourcennauslastung für CPU-, Speicher-, HTTP-Durchsatz und SSL-Durchsatz. Für jeden Einblick schlägt ADM empfohlene Maßnahmen vor. Um mehr Einblick in diese Erkenntnisse und Empfehlungen zu erhalten, müssen Sie Ihre ADC-Instanzen in ADM integrieren. Einige Vorteile nach dem Onboarding sind:

    - CPU: Prognostizieren Sie die CPU-Auslastung für die nächsten 24 Stunden auf ADM.
    - Speicher: Prognostizieren Sie die Speicherauslastung für die nächsten 24 Stunden auf ADM.
    - SSL-Durchsatz: Zeigen Sie die SSL-Echtzeitoptimierung mit intelligenten App Analytics auf ADM an.
    - HTTP-Durchsatz: Beheben Sie Probleme mit ADC-Durchsatzkapazität bei Infrastructure Analytics.

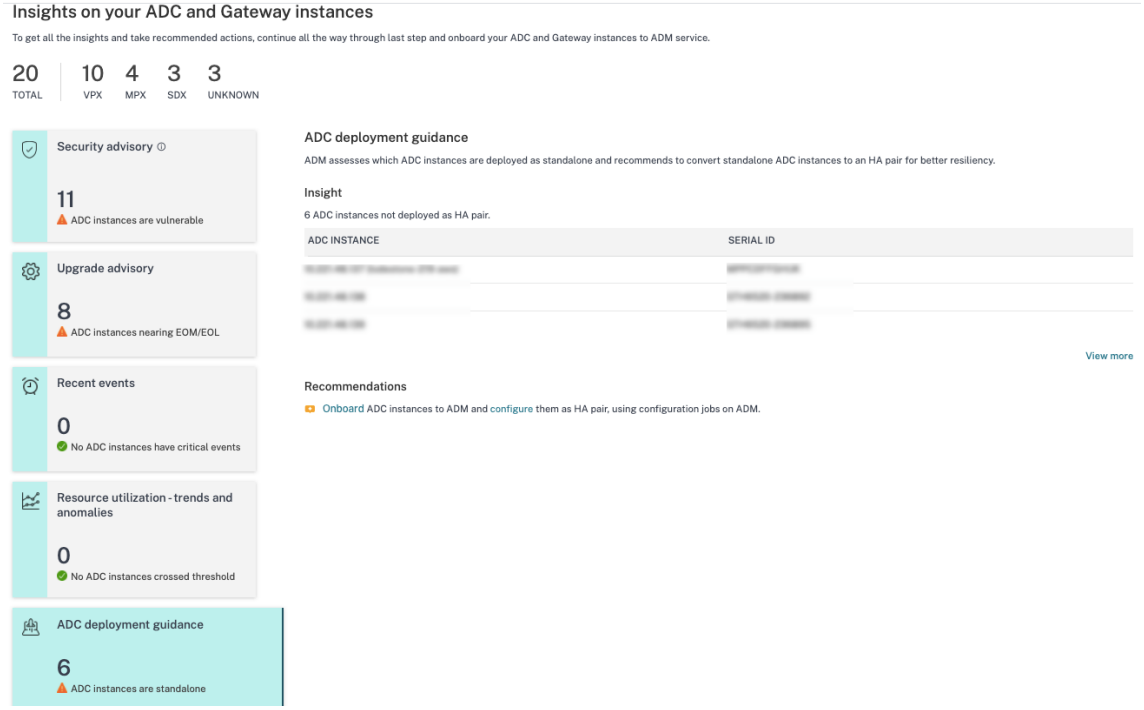


- **Wichtige Metriken**: Erhalten Sie Details zu wichtigen Metriken in Bezug auf CPU, Speicher, HTTP-Durchsatz, SSL-Durchsatz und decken Sie anomale Trends in den Metriken auf.



5. **Bereitstellungshinweise**: Erhalten Sie Einblick in ADC-Instanzen, die als eigenständiger ADC bereitgestellt werden. ADM gibt eine Empfehlung, diese ADC-Instanzen als HA-Paar für eine

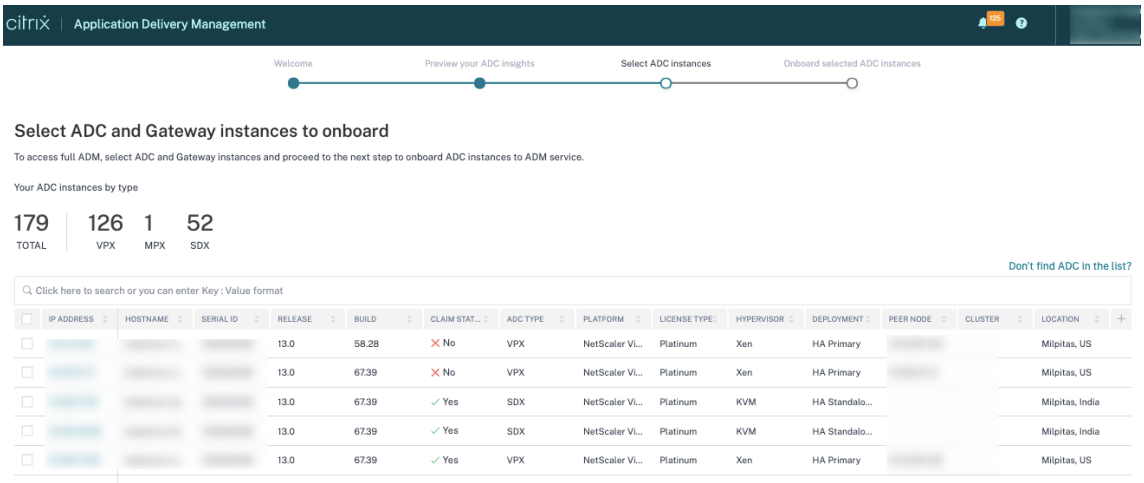
bessere Ausfallsicherheit zu konfigurieren. Dies erfordert, dass Sie Ihre ADC-Instanzen in ADM einbinden und dann Wartungsaufträge verwenden, um die Instanzen als HA-Paar zu konfigurieren.



Schritt 3: Wählen Sie ADC- und Gateway-Instanzen zum Onboard-

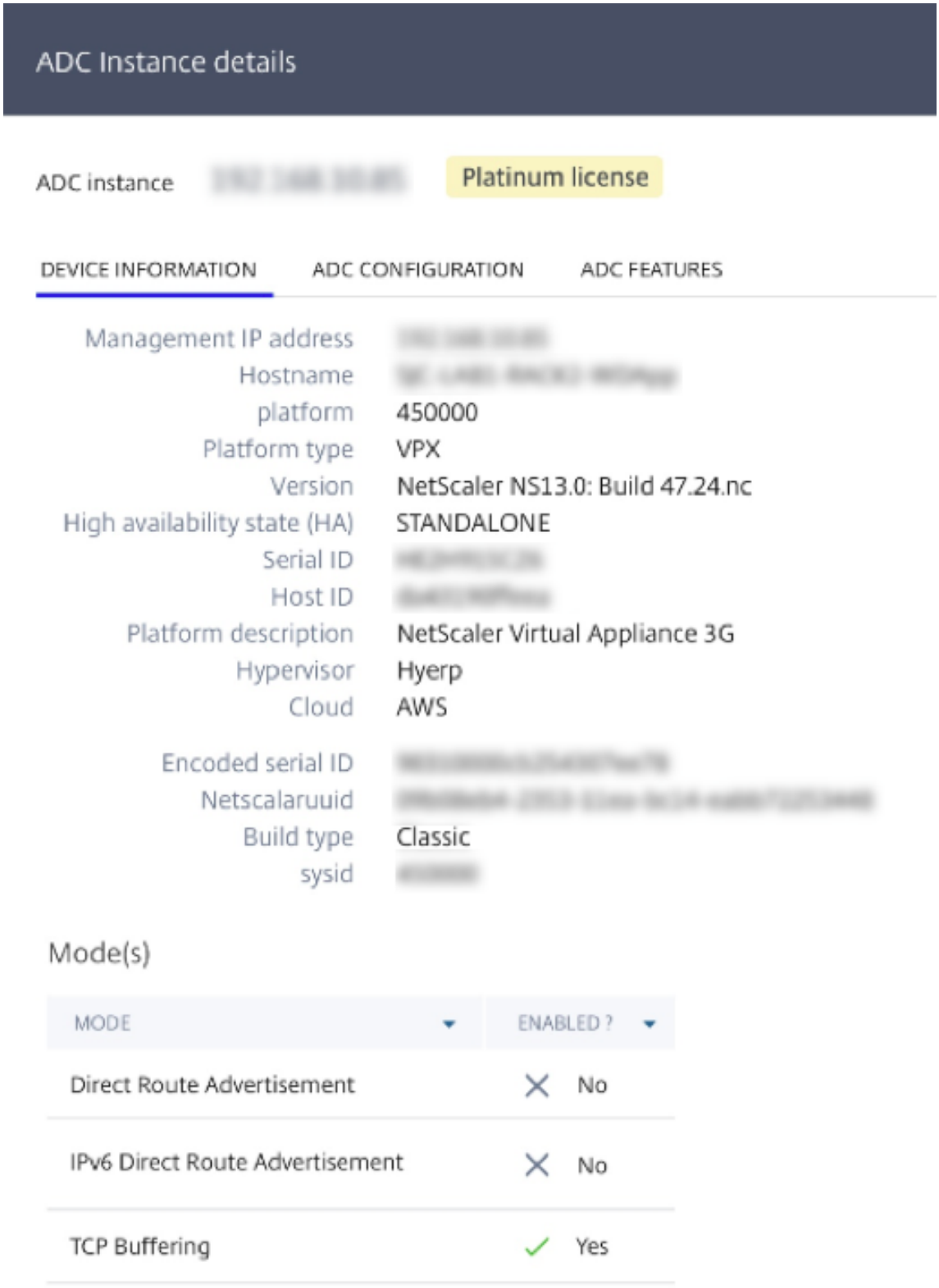
Auf dieser Seite werden alle ADC- und Gateway-Instanzen in Ihrer Umgebung angezeigt. Zeigen Sie die ADC- und Gateway-Instanzen an, wählen Sie sie an, wählen Sie sie aus, und klicken Sie auf **Weiter**.

1. Zeigen Sie die ADC-Instanzen an, die Sie beim ADM-Dienst einbinden möchten, und wählen Sie sie aus.

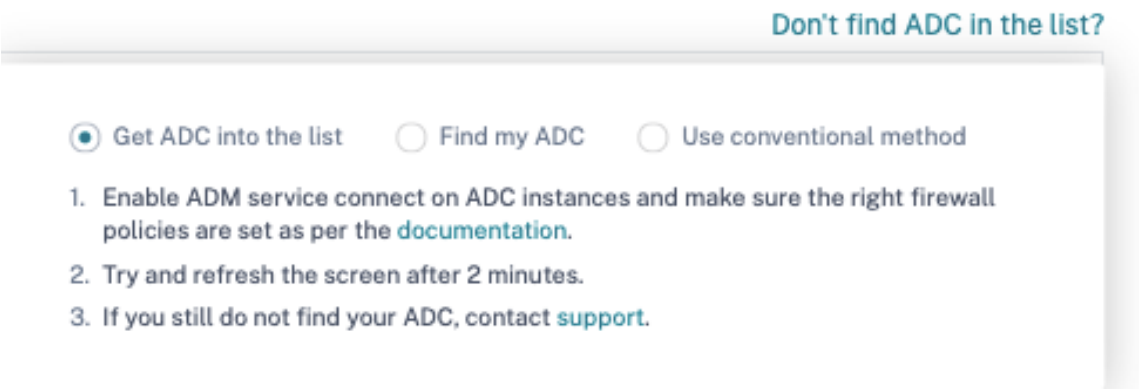


Wenn Sie Details zu einer Instanz wie Geräteinformationen, ADC-Konfiguration, verfügbaren

ADC-Funktionen oder Lizenzinformationen benötigen, klicken Sie unter der ADC-Instanz auf die IP-Adresse der Instanz.

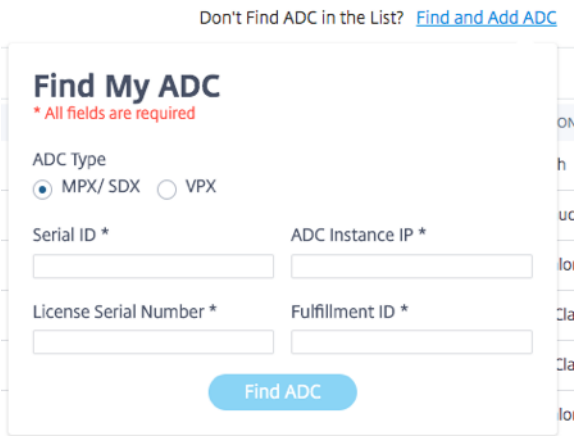


Wenn Ihre Instanz nicht aufgeführt ist, verwenden Sie den **ADC nicht in der Liste oben rechts finden**.



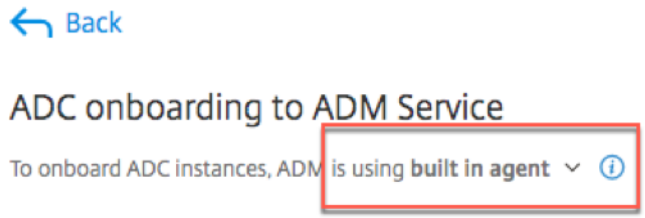
Sie können auf drei Arten vorgehen: Befolgen Sie die unter **ADC abrufen in die Liste** angegebenen Schritte oder verwenden **Sie die Option "Meinen ADC suchen"**. Wenn diese beiden Schritte nicht helfen, klicken Sie auf die Option **Konventionelle Methode verwenden**, die den Workflow überspringt und Sie durch die herkömmliche Art des Onboardings von ADC-Instanzen führt.

Geben Sie für die **Option "Meinen ADC suchen**" die Details in die Pflichtfelder ein (Seriennummer, IP-Adresse der ADC-Instanz, Seriennummer der Lizenz und Fulfillment-ID) und suchen.



Schritt 4: Onboard von ADC-Instanzen an ADM

Sie können Ihre Instanzen mit dem integrierten Agenten (Standardoption) oder einem externen Agenten einbinden.



Integrierte ADC-Instanzen mit einem integrierten Agenten

Auto- und skriptbasiertes Onboarding verwendet den integrierten Agenten, der standardmäßig festgelegt ist.

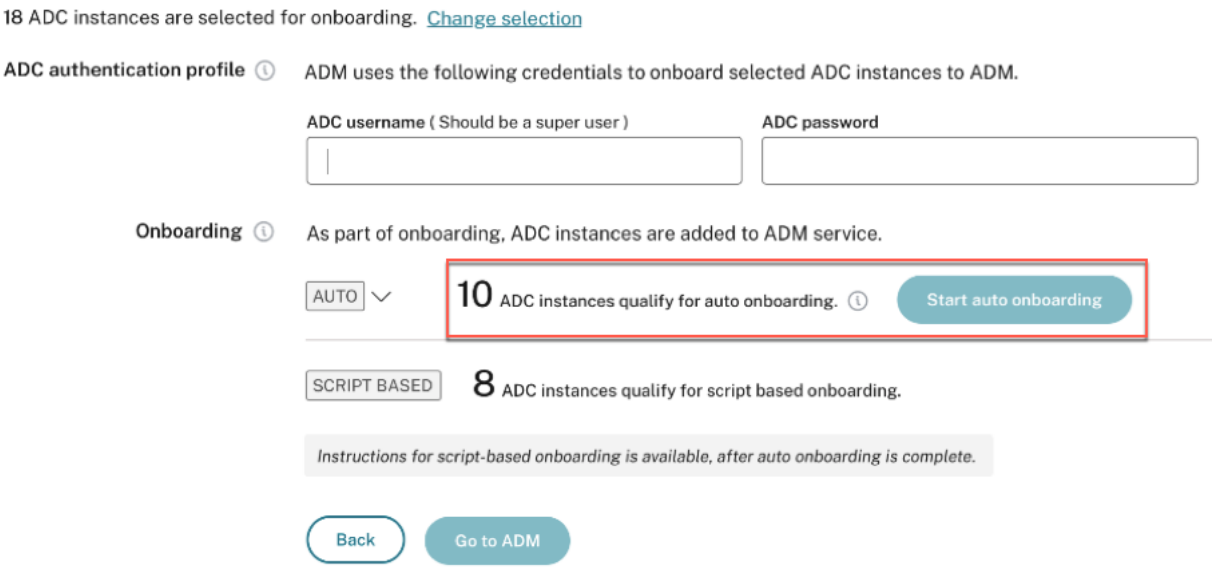
Auto-Onboarding: Es wird nur für die folgenden ADC-Versionen unterstützt:

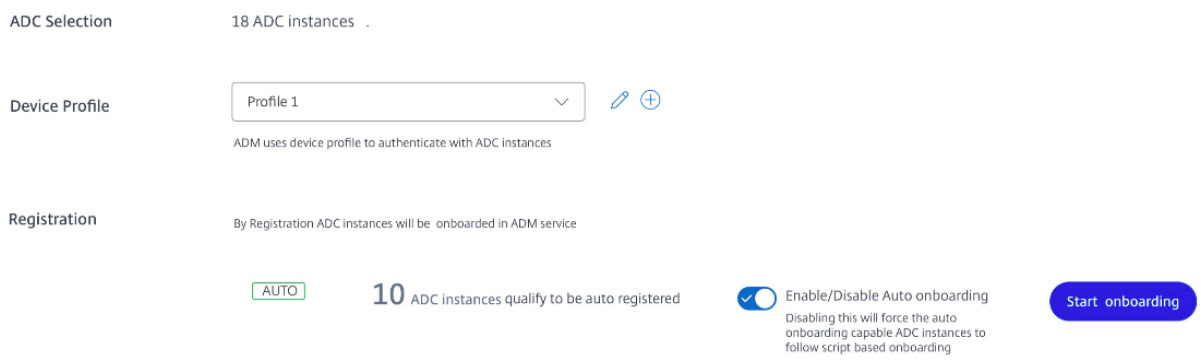
- Citrix ADC MPX und VPX Image-Version 12.1 57.18 und höher sowie 13.0 61.48 und höher
- SDX-Image Version 13.0 61.48 und höher und 12.1 58.14 und höher

Um eine andere ADC-Instanz auszuwählen, klicken Sie auf **Auswahl ändern**.

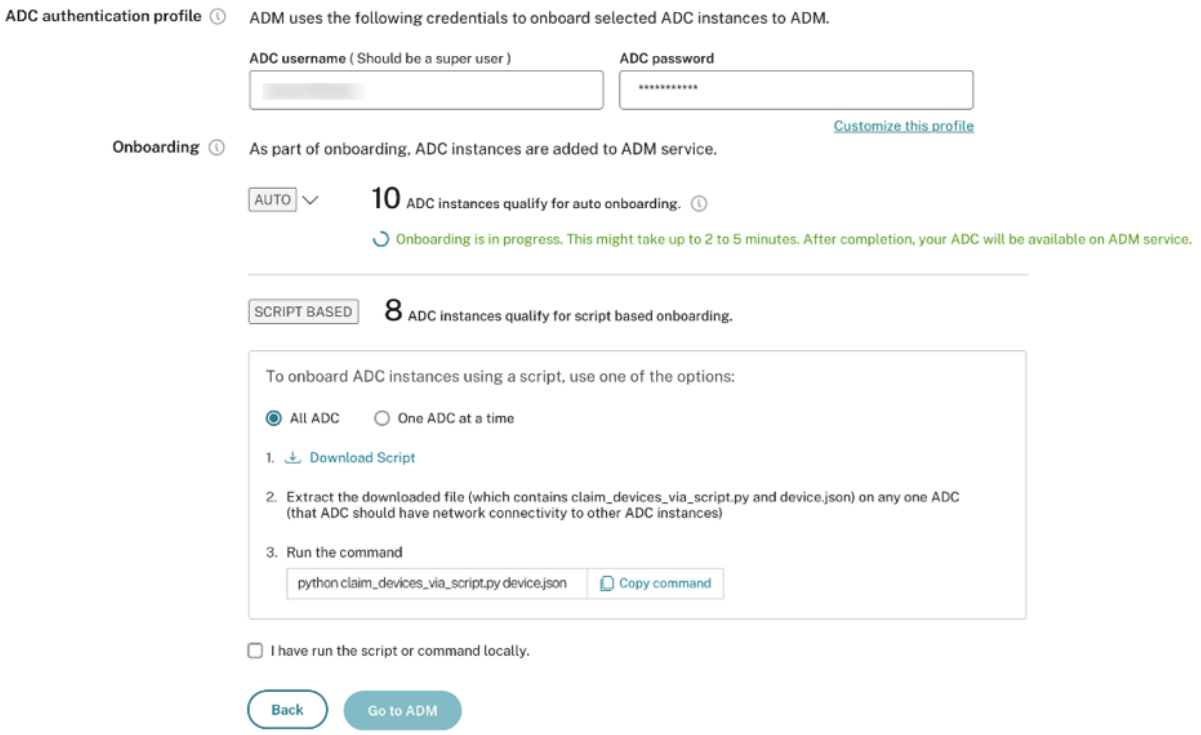
Von den insgesamt ausgewählten ADC-Instanzen qualifizieren sich einige Instanzen möglicherweise für das automatische Onboarding (basierend auf Mindestversionskriterien). Sie können die Instanzen sehen, die sich für das automatische Onboarding qualifizieren.

Geben Sie den ADC-Benutzernamen und das Kennwort ein. Diese Anmeldeinformationen müssen ADC-Benutzeradministratoranmeldeinformationen sein, und ADM verwendet diese Anmeldeinformationen, um ADC zu speichern. Klicken Sie auf **Onboarding starten**, um Ihre ADC-Instanzen in ADM zu onboarden.





Das automatische Onboarding kann bis zu 2-5 Minuten in Anspruch nehmen.



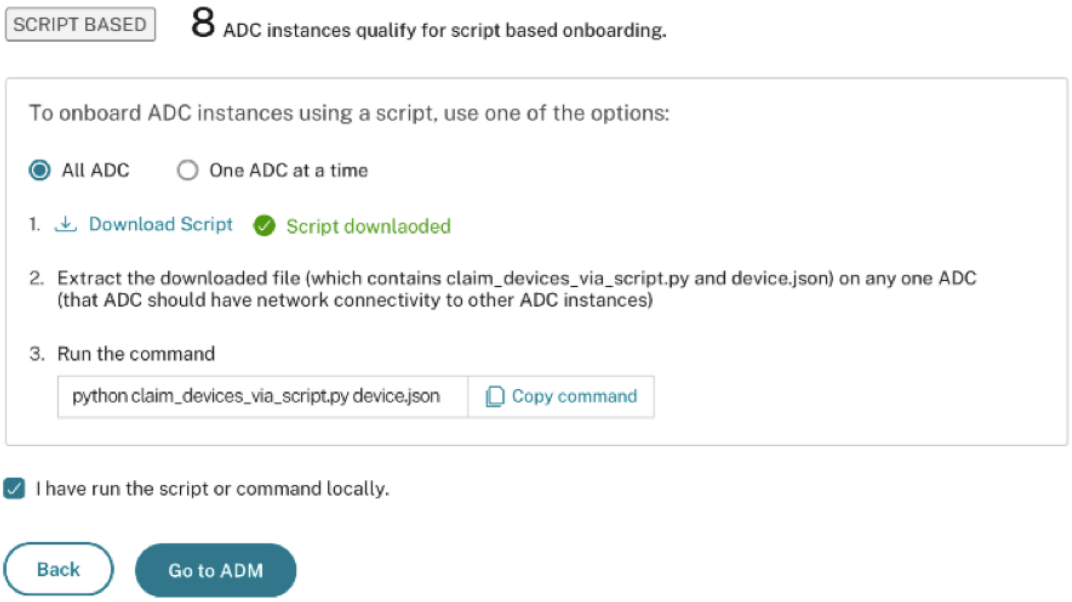
> **Hinweis**
>
> Wenn Sie nicht möchten, dass die ADC-Instanzen automatisch an ADM einbinden, können Sie das automatische Onboarding deaktivieren und die skriptbasierte Option für Onboarding verwenden.

Skriptbasiertes Onboarding: Nachdem das automatische Onboarding abgeschlossen ist, können Sie die restlichen Instanzen mithilfe des skriptbasierten Onboarding einbinden. Verwenden Sie eine der folgenden Optionen:

- **Option 1**: Laden Sie das Skript herunter, extrahieren Sie die Tar-Datei und führen Sie sie mit dem auf der Benutzeroberfläche angegebenen Befehl auf einer der ADC-Instanzen aus. Stellen Sie sicher, dass die ADC-Instanz, auf der Sie dieses Skript ausführen, über Netzwerkkonnektivität

zu allen anderen ausgewählten ADC-Instanzen verfügt.

- **Option 2**: Melden Sie sich bei der CLI-Konsole jeder ADC-Instanz an und führen Sie die auf der Benutzeroberfläche angegebenen Befehle aus. Weitere Einzelheiten finden Sie in Schritt 7 des Dokuments Konfigurieren des integrierten ADC-Agenten zur Verwaltung von Instanzen. Stellen Sie sicher, dass Sie für jede der ADC-Instanzen einen neuen eindeutigen Aktivierungscode generieren.

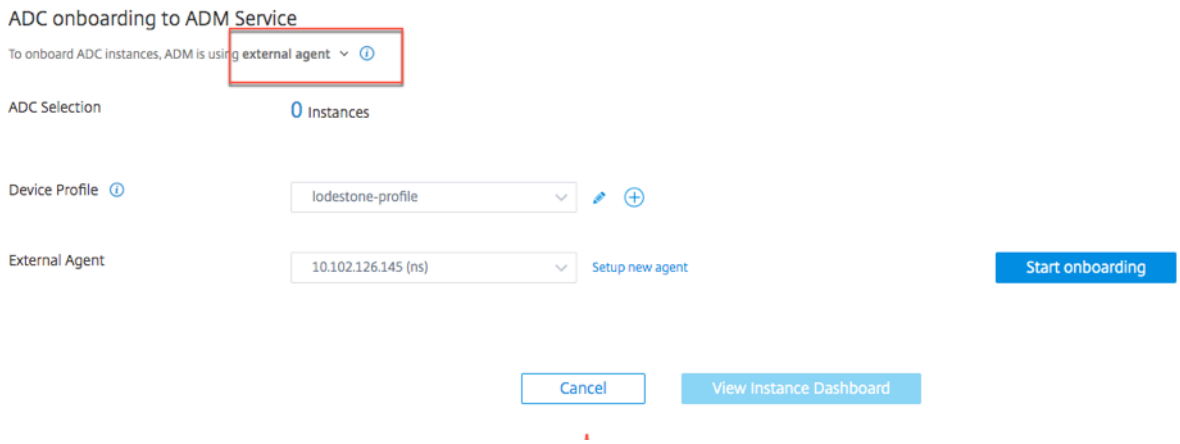


Nachdem Sie alle Ihre Instanzen eingebunden haben, klicken Sie auf **Gehe zu ADM, um** zum Dashboard der ADM-Instanzverwaltungs-Benutzeroberfläche zu gelangen und die verschiedenen Funktionen zu erkunden.

> **Hinweis**
>
> Wenn Sie ein neuer Kunde im ADM-Dienst ohne ADM-Lizenz sind, ist Ihr Citrix Dienstkonto standardmäßig ein Express-Konto. Weitere Informationen zur ADM-Kontoberechtigung finden Sie unter Verwalten von Citrix ADM Ressourcen mit Express-Konto.

Onboard von ADC-Instanzen mit einem externen Agenten

Sie können externes Agenten-basiertes Onboarding verwenden, wenn Sie die gepoolte Lizenzierung oder die vollständige Analytics-Suite im ADM-Dienst verwenden oder beide die gepoolte Lizenzierung und die vollständige Analytics-Suite verwenden möchten.



Führen Sie hierzu die folgenden Schritte aus:

1. Wählen Sie ein Geräteprofil aus.

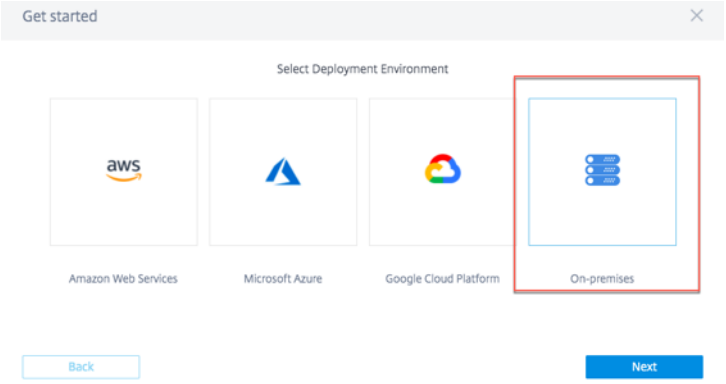
   > **Hinweis**
   >
   > Aus Sicherheitsgründen können Sie die standardmäßigen ADC-Anmeldeinformationen (nsroot/nsroot) nicht für das Onboarding verwenden.

2. Wählen Sie einen externen Agenten aus und klicken Sie auf **Neuen Agenten einrichten**.
3. Wählen Sie eine der folgenden Umgebungen aus:

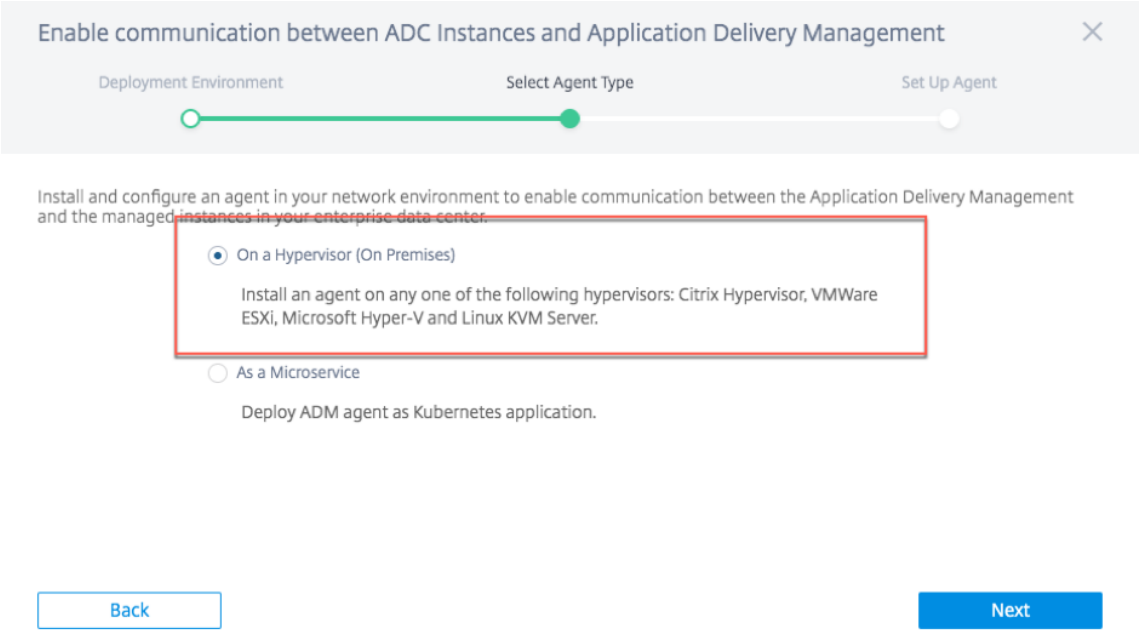
   - Amazon Web Services
   - Microsoft Azure
   - Google Cloud Platform
   - On-Premises

Installieren Sie einen Agenten auf Ihrem on-premises Hypervisor

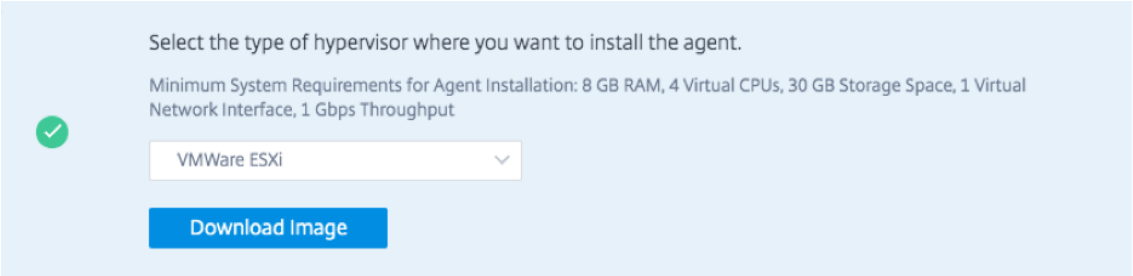
Wenn Sie **On-Premises**auswählen, können Sie den Agenten auf den folgenden Hypervisoren installieren: Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V, Linux KVM Server.



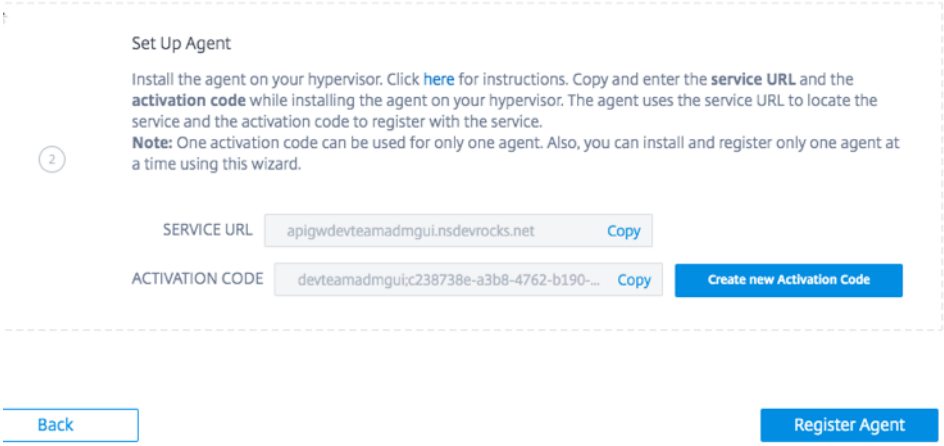
1. Wählen Sie **On a Hypervisor (On Premises)** aus und klicken Sie auf **Weiter**.



2. Wählen Sie den Hypervisortyp aus und laden Sie das Image herunter, zum Beispiel VMware ESXi.



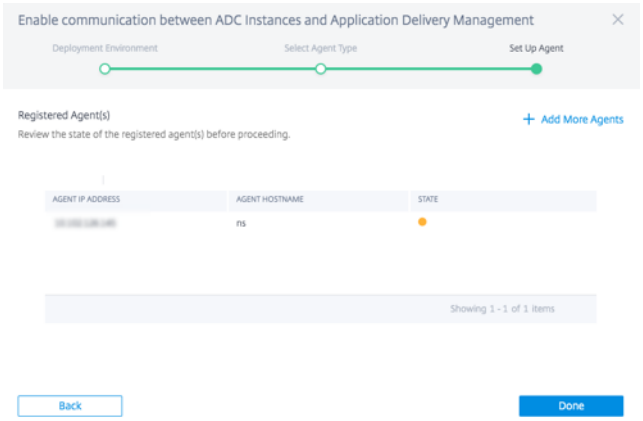
3. Verwenden Sie die Dienst-URL und den Aktivierungscode, um den Agenten zu konfigurieren.



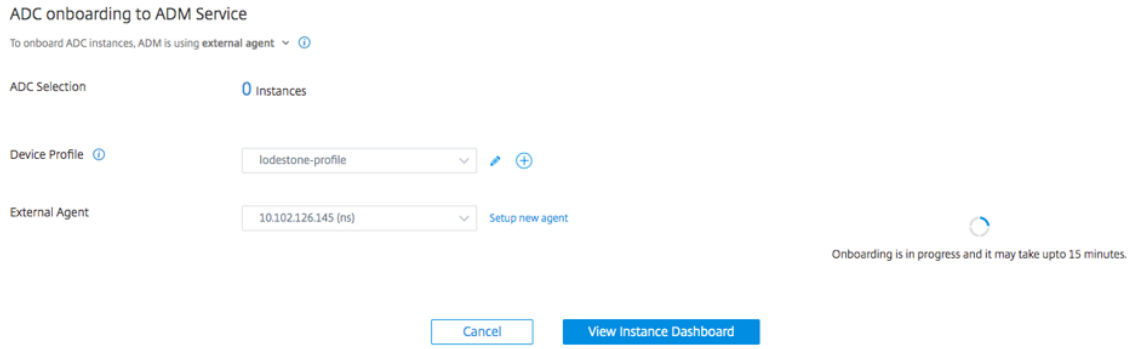
Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren. Ausführliche Anweisungen zur Installation eines Agenten auf

Ihrem on-premises Hypervisor finden Sie unter Citrix ADM Agent lokal installieren

4. Klicken Sie auf **Agenten registrieren**. Wenn Sie fertig sind, klicken Sie auf **Fertig**, um zur ADC-Onboarding-ADM-Service-Seite zurückzukehren.



5. Klicken Sie auf **Onboarding starten**. Nachdem Sie alle Ihre Instanzen eingebunden haben, klicken Sie auf **Instanz-Dashboard anzeigen, um zum Dashboard** der ADM-Instanzverwaltungs-Benutzeroberfläche zu wechseln und die verschiedenen Funktionen zu erkunden.



Installieren eines Agenten in einer öffentlichen Cloud

Sie können den Agenten in einer der folgenden Cloud-Umgebungen installieren:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

Weitere Informationen finden Sie in den folgenden Dokumenten:

- Installieren des Citrix ADM-Agenten in der Microsoft Azure-Cloud
- Installieren des Citrix ADM Agenten in AWS
- Installieren Sie den Citrix ADM Agenten auf GCP

Übergang von einem integrierten Agenten zu einem externen Agenten

April 28, 2021

Möglicherweise haben Sie damit begonnen, den ADM-Service nur für die Verwaltung und Überwachung zu verwenden, und später möchten Sie möglicherweise andere Funktionen wie gepoolte Lizenzierung und Analyse verwenden. Dazu müssen Sie vom integrierten ADM-Service-Agenten zu einem externen Agenten wechseln.

Der integrierte Agent unterstützt nur ADM-Verwaltungs- und Überwachungsfunktionen. Für andere ADM-Funktionen wie gepoolte Lizenzierung und Analysen benötigen Sie einen externen Agenten. Dieses Dokument behandelt die Schritte für den Übergang von einem vorhandenen integrierten ADM-Agenten zu einem externen Hypervisor-basierten Agenten.

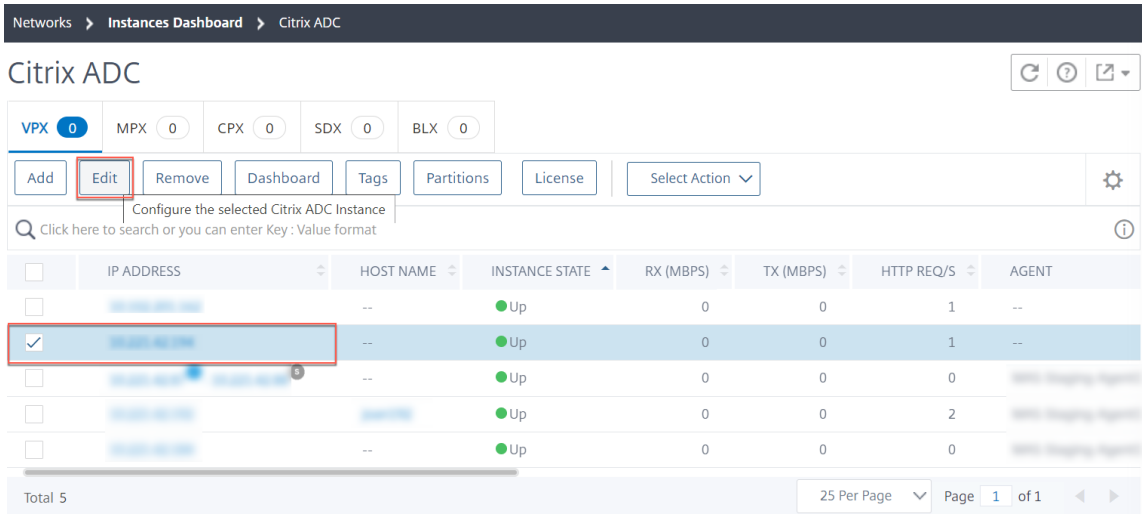
Vorbereitung

Installieren Sie einen externen Agenten, bevor Sie mit dem Umstieg beginnen. Befolgen Sie die im Thema Citrix ADM Agent lokal installierenbeschriebene Vorgehensweise

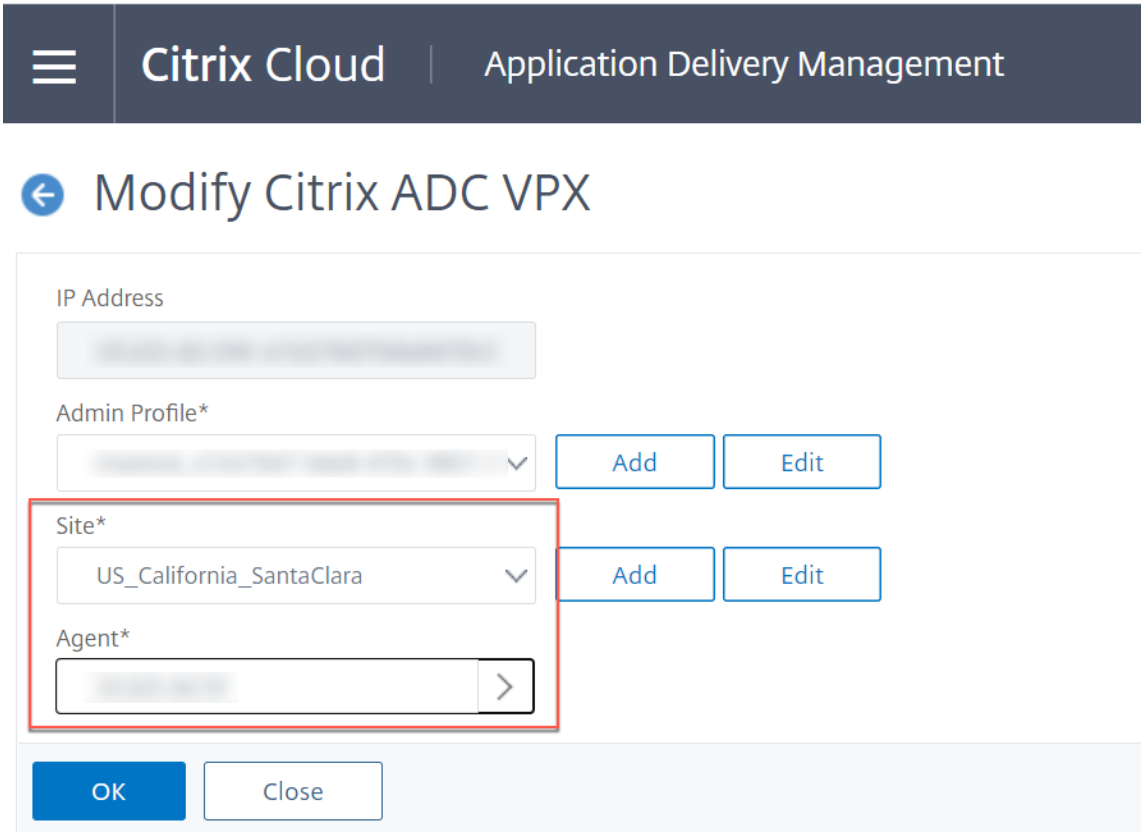
Übergang von einem integrierten Agenten zu einem externen Agenten

Befolgen Sie diese Schritte, um von einem integrierten Agenten zu einem externen Agenten zu wechseln:

1. Wählen Sie in der ADM-Benutzeroberfläche unter **Netzwerke > Instanzen Dashboard > Citrix ADC**die Citrix ADC-Instanz aus und klicken Sie auf **Bearbeiten**.



2. Wählen Sie die Site und den Agenten aus und klicken Sie auf **OK**.



3. Wählen Sie die Instanz erneut aus und klicken **Sie auf Aktion auswählen > Wiederentdecken**.

Funktionen und Lösungen

April 28, 2021

Citrix Application Delivery Management (Citrix ADM) ist mit den meisten Features kompatibel, die mit der lokalen Version von Citrix ADM verfügbar sind. In diesem Dokument werden die Features beschrieben, die vom Dienst unterstützt werden.

Anwendungsanalyse und -management

Die Anwendungsanalyse- und Verwaltungsfunktion von Citrix ADM stärkt den anwendungsorientierten Ansatz, um Ihnen bei der Bewältigung verschiedener Herausforderungen bei der Anwendungsbereitstellung zu helfen. Dieser Ansatz gibt Ihnen Einblick in die Integritätsgrade von Anwendungen, hilft Ihnen bei der Ermittlung der Sicherheitsrisiken und hilft Ihnen, Anomalien im Anwendungsdatenverkehr zu erkennen und Korrekturmaßnahmen zu ergreifen.

- Analyse der Anwendungsleistung: App Score ist das Produkt eines Bewertungssystems, das definiert, wie gut eine Anwendung funktioniert. Es zeigt, ob die Anwendung in Bezug auf die

Reaktionsfähigkeit gut funktioniert, nicht anfällig für Bedrohungen ist und alle Systeme betriebsbereit sind.

- Anwendungssicherheitsanalysen: Das App Security Dashboard bietet einen ganzheitlichen Überblick über den Sicherheitsstatus Ihrer Anwendungen. Beispielsweise werden wichtige Sicherheitsmetriken wie Sicherheitsverletzungen, Signaturverletzungen, Bedrohungsindizes angezeigt. Das App-Security-Dashboard zeigt auch angriffsbezogene Informationen wie SYN-Angriffe, kleine Fensterangriffe und DNS-Flutangriffe für die erkannten Citrix ADC-Instanzen an.
- Intelligente App Analytics:Die Funktion Intelligent App Analytics bietet eine einfache und skalierbare Lösung für die Überwachung und Fehlerbehebung von Anwendungen, die über Citrix ADC Appliances bereitgestellt werden. Intelligent App Analytics überwacht nicht nur alle Ebenen von Anwendungstransaktionen, sondern verwendet auch Machine Learning-Techniken, um normale Verkehrsmuster in Ihrem Netzwerk zu definieren und Anomalien zu erkennen. Diese Funktion reduziert die Gesamtlaufzeit und verbessert die gesamte Anwendungsverfügbarkeit.

StyleBooks

StyleBooks vereinfachen die Verwaltung komplexer Citrix ADC Konfigurationen für Ihre Anwendungen. Ein StyleBook ist eine Vorlage, mit der Sie Citrix ADC Konfigurationen erstellen und verwalten können. Sie können ein StyleBook zum Konfigurieren eines bestimmten Features von Citrix ADC erstellen oder ein StyleBook so entwerfen, dass Konfigurationen für eine Enterprise-Anwendungsbereitstellung wie Microsoft Exchange oder Skype for Business erstellt werden.

Instanzverwaltung

Ermöglicht die Verwaltung der Citrix ADC -, Citrix Gateway -, Citrix Secure Web Gateway - und Citrix SD-WAN Instanzen.

> **Hinweis**
>
> Derzeit unterstützt Citrix ADM nur die WAN-Optimierungsfunktionalität für Citrix SD-WAN Instanzen.

Event-Management

Ereignisse stellen Ereignisse oder Fehler in einer verwalteten Citrix ADC-Instanz dar. Wenn beispielsweise ein Systemfehler oder eine Änderung der Konfiguration vorliegt, wird ein Ereignis auf Citrix ADM generiert und aufgezeichnet. Im Folgenden finden Sie die zugehörigen Funktionen, die Sie mithilfe von Citrix ADM konfigurieren oder anzeigen können:

- Erstellen von Ereignisregeln
- Verwenden von Citrix ADM zum Exportieren von Syslog-Nachrichten

Zertifikatverwaltung

Citrix ADM optimiert alle Aspekte der Zertifikatverwaltung für Sie. Über eine einzige Konsole können Sie automatisierte Richtlinien einrichten, um den richtigen Aussteller, die richtige Schlüsselstärke und korrekte Algorithmen sicherzustellen, während Sie nicht verwendete oder bald ablaufende Zertifikate im Auge behalten.

Konfigurationsverwaltung

Mit Citrix ADM können Sie Konfigurationsaufträge erstellen, mit denen Sie Konfigurationsaufgaben ausführen können, z. B. das Erstellen von Entitäten, das Konfigurieren von Features, die Replikation von Konfigurationsänderungen, Systemaktualisierungen und andere Wartungsaktivitäten auf mehreren Instanzen. Konfigurationsaufträge und Vorlagen vereinfachen die sich wiederholenden Verwaltungsaufgaben zu einer einzigen Aufgabe auf Citrix ADM.

Konfigurations-Audit

Ermöglicht die Überwachung und Identifizierung von Anomalien in den Konfigurationen über Ihre Instanzen hinweg.

- Konfigurationshinweise: Ermöglicht die Identifizierung von Konfigurationsanomalie.
- Prüfvorlage: Ermöglicht es Ihnen, die Änderungen über eine bestimmte Konfiguration hinweg zu überwachen.

Lizenzverwaltung

Ermöglicht die Verwaltung von Citrix ADC -Lizenzen durch Konfigurieren von Citrix ADM als Lizenzmanager.

- Citrix ADC gepoolte Kapazität: Ein gemeinsamer Lizenzpool, von dem aus Ihre Citrix ADC-Instanz eine Instanzlizenz und nur die erforderliche Bandbreite auschecken kann. Wenn die Instanz diese Ressourcen nicht mehr benötigt, werden sie wieder in den gemeinsamen Pool eingecheckt und die Ressourcen anderen Instanzen zur Verfügung gestellt, die sie benötigen.
- Citrix ADC VPX Ein- und Auschecken Lizenzierung: Citrix ADM weist bei Bedarf Lizenzen Citrix ADC VPX Instanzen zu. Eine Citrix ADC VPX Instanz kann die Lizenz vom Citrix ADM auschecken, wenn eine Citrix ADC VPX Instanz bereitgestellt wird, oder ihre Lizenz an Citrix ADM zurückchecken, wenn eine Instanz entfernt oder zerstört wird.

Netzwerkberichterstattung

Sie können die Ressourcennutzung optimieren, indem Sie Ihre Netzwerkberichte auf Citrix ADM überwachen.

Analytics

Bietet eine einfache und skalierbare Möglichkeit, die verschiedenen Erkenntnisse der Daten der Citrix ADC-Instanzen zu untersuchen, zu prognostizieren und die Anwendungsleistung zu verbessern. Sie können eine oder mehrere Analysefunktionen gleichzeitig verwenden.

- HDX Insight: Bietet End-to-End-Sichtbarkeit für ICA-Datenverkehr, der über Citrix ADC geht. Mit HDX Insight können Administratoren Echtzeitmetriken für Client- und Netzwerklatenz, historische Berichte, End-to-End-Performance-Daten anzeigen und Leistungsprobleme beheben.
- Web Insight:Bietet Einblick in Unternehmens-Webanwendungen. Es ermöglicht IT-Administratoren, alle vom Citrix ADC bereitgestellten Webanwendungen zu überwachen, indem sie integrierte und Echtzeitüberwachung von Anwendungen bereitstellen. Web Insight verarbeitet Daten von Citrix ADC unter Verwendung eines Approximationsalgorithmus. Es bietet die 1.000 besten Datensätze der Metriken, die mit den Webanwendungen in Ihrem Unternehmen zusammenhängen.
- Gateway Insight: Bietet Einblick in die Fehler, die Benutzer bei der Anmeldung auftreten, unabhängig vom Zugriffsmodus. Sie können eine Liste der zu einem bestimmten Zeitpunkt angemeldeten Benutzer sowie die Anzahl der aktiven Benutzer, die Anzahl der aktiven Sitzungen sowie Bytes und Lizenzen anzeigen, die von allen Benutzern zu einem bestimmten Zeitpunkt verwendet werden.
- Sicherheitshinweise: Bietet eine Einzelbereichslösung, mit der Sie Ihren Anwendungssicherheitsstatus beurteilen und Korrekturmaßnahmen ergreifen können, um Ihre Anwendungen zu schützen.
- SSL Insight:Bietet Einblick in sichere Transaktionen im Web (HTTPs). Es ermöglicht IT-Administratoren, alle vom Citrix ADC bereitgestellten Webanwendungen zu überwachen, indem sie eine integrierte Echtzeit- und historische Überwachung von Web-Transaktionen bereitstellen. SSL Insight verarbeitet Daten aus Citrix ADC unter Verwendung eines Approximationsalgorithmus. Es bietet die 1.000 besten Datensätze der Metriken, die mit den Web-Transaktionen in Ihrem Unternehmen zusammenhängen.

Rollenbasierte Zugriffssteuerung

Mit der rollenbasierten Zugriffssteuerung (RBAC) können Sie Zugriffsberechtigungen basierend auf den Rollen einzelner Benutzer in Ihrem Unternehmen erteilen. Der erste Benutzer einer Organisation, der sich mit Citrix Cloud-Anmeldeinformationen anmeldet, verfügt über die Superadministratorrolle, die standardmäßig über alle Zugriffsberechtigungen verfügt. Die anderen Benutzer dieser Organisation, die später vom Administrator erstellt werden, erhalten keine Administratorrollen.

Abonnements

Stellt eine Dashboard-Ansicht der Abonnements bereit, die Sie gekauft haben.

Sie sind standardmäßig einem Express-Konto zugewiesen. Mit diesem Konto können Sie begrenzte ADM-Ressourcen verwalten. Weitere Informationen finden Sie unter Verwalten von Citrix ADM Ressourcen mit Express-Konto.

Die folgenden Citrix ADM Funktionen sind derzeit nicht verfügbar:

- Bereitstellung
  - Migration von Citrix Insight Center zu Citrix ADM
  - Integration von Citrix ADM mit Citrix Virtual Desktop Director
- Netzwerke: Unterstützung für Citrix SD-WAN EE
- Analytics: TCP Insight, Video Insight und WAN Insight
- Eingeschränkte Systemeinstellungen
- Orchestrierung
  - Integration mit OpenStack und VMware NSX Manager
  - Citrix ADC Automatisierung im Hybrid-Modus von Cisco ACI
  - Container Orchestration: Integration mit Mesos/Marathon und Kubernetes

Systemanforderungen

April 28, 2021

Bevor Sie Citrix Application Delivery Management (Citrix ADM) verwenden, müssen Sie die Softwareanforderungen, Browseranforderungen, Port-Informationen, Lizenzinformationen und Einschränkungen überprüfen.

Unterstützte Browser

Um auf Citrix ADM zuzugreifen, muss Ihre Workstation über einen unterstützten Webbrowser verfügen.

Die folgenden Browser werden unterstützt.

Webbrowser	Version
Internet Explorer	11.0 und später
Google Chrome	Chrome 19 und höher
Safari	Safari 5.1.1 und höher
Mozilla Firefox	Firefox 3.6.25 und höher

Anforderungen an die Agenteninstallation

Installieren und konfigurieren Sie einen Agenten in der Netzwerkumgebung, um die Kommunikation zwischen Citrix ADM und den verwalteten Instanzen im Rechenzentrum zu ermöglichen. In Ihrem lokalen Rechenzentrum können Sie einen Agenten auf Citrix XenServer, VMware ESXi, Microsoft Hyper-V und Linux KVM-Server installieren.

Die Agentenanforderungen sind die virtuellen Computerressourcen, die der Hypervisor für jeden ADM-Agenten bereitstellen muss. In der folgenden Tabelle sind die Agentenanforderungen aufgeführt, die alle ADM-Funktionen nutzen sollen:

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8
Stauraum	30 GB
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s

Die Agentenanforderungen, um nur die gepoolte Lizenzierungsfunktion zu nutzen, siehe Lightweight Agent für gepoolte Lizenzierung.

Sie können auch einen Agenten in Microsoft Azure oder AWS oder Google Cloud installieren. Citrix empfiehlt, die folgenden Typen virtueller Maschinen der jeweiligen Cloud-Marktplätze zu verwenden, um alle ADM-Funktionen nutzen zu können:

Cloud	Anforderungen an Agenten	Bevorzugter Typ der virtuellen
AWS	8 virtuelle CPUs, 32 GB RAM und 30 GB Speicherplatz	`m4.2xlarge`
Microsoft Azure	8 virtuelle CPUs, 32 GB RAM und 30 GB Speicherplatz	`Standard_D8s_v3`
Google-Wol	8 virtuelle CPUs, 32 GB RAM und 30 GB Speicherplatz	`e2-standard-8`

Anweisungen zur Installation eines Agenten finden Sie unter den folgenden Links:

- Installieren von Citrix ADM Agent in Microsoft Azure Cloud.
- Installieren von Citrix ADM Agent in AWS.
- Installieren von Citrix ADM Agent auf Google Cloud.

Lightweight Agent für gepoolte Lizenzierung

Wenn Sie vorhaben, den ADM-Service nur für gepoolte Lizenzen zu verwenden, können Sie einen Agenten mit niedrigeren Spezifikationen verwenden, wie in der folgenden Tabelle aufgeführt:

Komponente	Voraussetzung
RAM	8 GB
Virtuelle CPU	4
Stauraum	30 GB

Solche Agenten mit niedrigeren Spezifikationen (Lightweight) werden nur im ADM-Service unterstützt.

Citrix empfiehlt, die folgenden Typen virtueller Maschinen der jeweiligen Cloud-Marktplätze zu verwenden, um nur die gepoolte Lizenzierungsfunktion zu nutzen:

Cloud	Anforderungen an Agenten	Bevorzugter Typ der virtuellen
AWS	4 virtuelle CPUs, 8 GB RAM und 30 GB Speicherplatz	`m4.xlarge`. Dieser Instanz-Typ bietet 4 virtuelle CPUs, 16 GB RAM und 30 GB Speicherplatz. Citrix empfiehlt diesen Instanz-Typ, da er den meisten Agentenanforderungen unter vorhandenen Instanz-Typen entspricht.
Microsoft Azure	4 virtuelle CPUs, 8 GB RAM und 30 GB Speicherplatz	`Standard_F4s_v2`
Google-Wol	4 virtuelle CPUs, 8 GB RAM und 30 GB Speicherplatz	`e2-standard-4`

> **Hinweis**
>
> Sie müssen die Standardplanungsaufträge deaktivieren, indem Sie zu **Einstellungen > Systemeinstellungen > Konfigurierbare Funktionen**navigieren.

Ports

Für die Kommunikation zwischen Citrix ADC-Instanzen und Citrix ADM Agenten oder Citrix SD-WAN Instanzen und Citrix ADM Agent müssen die folgenden Ports in einem Citrix ADM Agent geöffnet sein:

Typ	Port	Details	Richtung der Kommunikation
TCP	80/443	Für die NITRO-Kommunikation von Citrix ADM zu Citrix ADC oder Citrix SD-WAN Instanz 443. Für die NITRO-Kommunikation zwischen Citrix ADM-Servern im Hochverfügbarkeitsmodus.	Citrix ADM an Citrix ADC und Citrix ADC an Citrix ADM
TCP	22	Für die SSH-Kommunikation von Citrix ADM zur Citrix ADC - oder Citrix SD-WAN Instanz. Für die Synchronisierung zwischen Citrix ADM-Servern, die im Hochverfügbarkeitsmodus bereitgestellt werden. Und dieser Port ist für die SSH-Kommunikation zwischen dem ADM-Agenten und Citrix ADC erforderlich.	Citrix ADM an Citrix ADC und Citrix ADM Agent an Citrix ADC
UDP	4739	Für die AppFlow Kommunikation von der Citrix ADC - oder Citrix SD-WAN Instanz zu Citrix ADM.	Citrix ADC oder Citrix SD-WAN an Citrix ADM

Typ	Port	Details	Richtung der Kommunikation
ICMP	Kein reservierter Port	Erkennen der Netzwerkerreichbarkeit zwischen Citrix ADM- und Citrix ADC-Instanzen, SD-WAN-Instanzen oder dem sekundären Citrix ADM-Server, der im Hochverfügbarkeitsmodus bereitgestellt wird.	
UDP	161, 162	So empfangen Sie SNMP-Ereignisse von der Citrix ADC-Instanz an Citrix ADM.	**Port 161** - Citrix ADM zu Citrix ADC
			Port 162 - Citrix ADC zu Citrix ADM
UDP	514	So empfangen Sie Syslog-Nachrichten von der Citrix ADC - oder Citrix SD-WAN-Instanz an Citrix ADM.	Citrix ADC oder Citrix SD-WAN an Citrix ADM
TCP	25	So senden Sie SMTP-Benachrichtigungen von Citrix ADM an Benutzer.	
TCP	5563	Um ADC-Metriken (Leistungsindikatoren), Systemereignisse und Überwachungsprotokollmeldungen von der Citrix ADC-Instanz an Citrix ADM zu empfangen.	Citrix ADC zu Citrix ADM

Typ	Port	Details	Richtung der Kommunikation
TCP	5557/5558	Für die **Logstream-Kommunikation** (für Security Insight, Web Insight und HDX Insight) von Citrix ADC zu Citrix ADM.	Citrix ADC zu Citrix ADM
TCP	5454	Standardport für die Kommunikation und Datenbanksynchronisierung zwischen Citrix ADM Knoten im Hochverfügbarkeitsmodus.	Primärer Citrix ADM-Knoten zum sekundären Citrix ADM-Knoten
TCP	27000 und 7279	Lizenzports für die Kommunikation zwischen Citrix ADM Lizenzserver und ADC-Instanz. Diese Ports werden auch für gepoolte ADC-Lizenzen verwendet.	Citrix ADC zu Citrix ADM
TCP	443/8443/7443	Port für die Kommunikation zwischen Citrix ADM Agent und Citrix ADM. Der ADM-Agent initiiert die Kommunikation mit Citrix ADM.	Citrix ADM Agent an Citrix ADM

Stellen Sie für die Kommunikation zwischen Citrix ADM Agent und Citrix ADM sicher, dass der folgende Port im Citrix ADM Agent geöffnet ist:

Typ	Port	Details
HTTPS	443	Für die Kommunikation von Citrix ADM Agent zu Citrix ADM.

> **Hinweis:**
>
> Der Endpunkt des Citrix ADM entspricht der Service-URL, die beim Versuch, den Agenten zu registrieren, generiert wird. Der Agent verwendet die Dienst-URL, um den Citrix ADM zu finden.

Stellen Sie sicher, dass die folgenden Endpunkte auf der Positivliste sind:

- Download-Service:

```
https://download.citrixnetworkapi.net
<!--NeedCopy-->
```

- Treuhand-Service:

```
*.citrixnetworkapi.net
<!--NeedCopy-->
```

- Service-URLs:

```
*.agent.adm.cloud.com
*.adm.cloud.com
adm.cloud.com
<!--NeedCopy-->
```

- ADC-Backup-Dienst:

```
adm-prod-backup-\*.s3.amazonaws.com
adm-prod-backup-\*.s3.*amazonaws.com
<!--NeedCopy-->
```

Stellen Sie für die Kommunikation zwischen Citrix ADM Agenten und Citrix Analytics Service sicher, dass die folgenden Endpunkte auf der Positivliste stehen:

Endpunkt	USA Region	EU-Region
Ereignis-Hub	`https://cas-eh-ns-alias.servicebus.windows.net`	`https://cas-eh-ns-eu-alias.servicebus.windows.net`

Veraltete FQDNs

Einige FQDNs sind für die folgende Verwendung des ADM-Dienstes veraltet. Damit Sie ohne Unterbrechung zu den neuen FQDNs wechseln können, funktionieren die veralteten FQDNs für einige Zeit weiter und werden langsam auslaufen.

ADM Service-Endpunkte	Alter FQDN	Neuer FQDN
Zugriff auf die Benutzeroberfläche des ADM-Dienstes	`netscalermas.cloud.com`	`adm.cloud.com`
Dienst-URL	`agent.netscalermgmt.net`	`*.agent.adm.cloud.com` **Hinweis**: Der Wert von * hängt davon ab, welcher PoP (Point of Presence) Ihre Daten verfügbar sind.
API-Interaktionen	`netscalermas.cloud.com`	`api.adm.cloud.com`

Minimale Citrix ADC-Versionen erforderlich

> Hinweis
>
> Die Citrix ADC-Versionen 10.5, 11.0 und 12.0 haben bereits End Of Life (EOL) erreicht. Weitere Informationen siehe Produktmatrix. Die empfohlene ADC-Version ist 12.1.

Citrix ADM Funktion	Citrix ADC Softwareversion
StyleBooks	10.5 und höher
Überwachen/Reporting und Konfigurieren mit Jobs	10.5 und höher
Analytics	
HDX Insight	10.1 und höher

Citrix ADM Funktion	Citrix ADC Softwareversion
Gateway Insight	11.0.65.31 und höher
Sicherheitshinweise	11.0.65.31 und höher

Anforderungen für die Citrix SD-WAN Instanzverwaltung

Erforderliche Mindestversionen für Citrix SD-WAN WANOP

Citrix ADM Funktion	Citrix CloudBridge / Citrix SD-WAN WO
Überwachung/Berichterstellung und Konfiguration mit Jobs	Citrix CloudBridge 7.4.0 und höher
Analytics	
HDX Insight	Citrix CloudBridge 7.4.0 und höher
WAN Insight	Citrix CloudBridge 7.4.0 und höher

Interoperabilitätsmatrix von Citrix SD-WAN Plattformeditionen und Citrix ADM Funktionen

Plattform-Editionen	Entdeckung	Konfiguration	Überwachen	Berichterstellung	Ereignisverwaltung (SNMP-Traps)	HDX Insight und WAN Insight Analytics	Multi-Hop Einblick
Citrix SD-WAN WANOP	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Thin Clients, die für Citrix SD-WAN Instanzen unterstützt werden

Citrix ADM unterstützt die folgenden Thin Clients zur Überwachung von Citrix SD-WAN Bereitstellungen:

- Dell Wyse WTOS Model R10L Rx0L Thin Client
- NComputing N400
- Dell Wyse WTOS Model CX0 C00X Xenith
- Dell Wyse WTOS Model TXO T00X Xenith2
- Dell Wyse WTOS Model CX0 C10LE

- Dell Wyse WTOS Model R00LX Rx0L HDX Thin Client
- Dell Wyse Enhanced SUSE Linux Enterprise, Model Dx0D, D50D
- Dell Wyse ZX0 Z90D7 (WES7) Thin Client

Anforderungen für die Citrix ADM Analytics-Lösung

Erforderliche Mindestversionen für Citrix Virtual Apps and Desktops

Citrix ADM Funktion	Citrix Virtual Apps and Desktops Version
HDX Insight	Citrix Virtual Apps and Desktops 7.0 und höher

> **Hinweis**
>
> Die Citrix Gateway Funktion (als Access Gateway Enterprise für die Versionen 9.3 und 10.x bezeichnet) muss auf der Citrix ADC-Instanz verfügbar sein. Citrix ADM unterstützt keine eigenständigen Access Gateway Standard-Appliances.

Citrix ADM kann Berichte für Anwendungen erstellen, die auf einer Citrix Virtual App oder einem Desktop veröffentlicht und über Citrix Receiver aufgerufen werden. Diese Funktion hängt jedoch vom Betriebssystem ab, auf dem der Receiver installiert ist. Derzeit analysiert ein Citrix ADC den ICA-Datenverkehr nicht für Anwendungen oder Desktops, auf die über Citrix Receiver unter iOS- oder Android Betriebssystemen zugegriffen wird.

Für HDX Insight unterstützte Thin Clients

Citrix ADM unterstützt die folgenden Thin Clients zur Überwachung von Citrix ADC-Instanzen, die auf Softwareversion 11.0 Build 65.31 und höher ausgeführt werden:

- Dell Wyse Windows based Thin Clients
- Dell Wyse Linux based Thin Clients
- Dell Wyse ThinOS based Thin Clients
- 10ZiG Ubuntu based Thin Clients

Citrix ADC-Instanzlizenz für HDX Insight erforderlich

Die von Citrix ADM für HDX Insight gesammelten Daten hängen von der Version und den installierten Lizenzen der überwachten Citrix ADC-Instanzen ab. HDX Insight Berichte werden nur für Citrix ADC Premium- und Enterprise-Appliances angezeigt, die auf Softwareversion 10.5 und höher ausgeführt werden.

Citrix ADC Lizenz/Dauer	5 Minuten	1 Stunde	1 Tag	1 Woche	> 1 Monat
Standard	Nein	Nein	Nein	Nein	Nein
Erweitert	Ja	Ja	Nein	Nein	Nein
Premium	Ja	Ja	Ja	Ja	Ja

Unterstützte Betriebssysteme und Citrix Receiver-Versionen

In der folgenden Tabelle sind die von Citrix ADM unterstützten Betriebssysteme und die Citrix Receiver-Versionen aufgeführt, die derzeit von jedem System unterstützt werden:

Betriebssystem	Receiver-Version
Windows	4.0 Standard Edition
Linux	13.0.265571 und höher
Mac	11.8, Build 238301 und neuer
HTML5	1.5*
Chrome-App	1.5*

* Anwendbar mit Citrix CloudBridge Release 7.4 und höher.

Lizenzen

April 28, 2021

Citrix Application Delivery Management (ADM) erfordert eine verifizierte Citrix ADM -Lizenz zum Verwalten und Überwachen der Citrix ADC-Instanzen.

Die folgenden Lizenztypen werden für Citrix ADM for Service unterstützt:

Lizenztyp	**Anspruch auf**
Virtueller Server	10 virtuelle Server und 5 GB Speicher pro Lizenz
Speicher	5 GB pro Lizenz

Lizenztyp	Anspruch auf
Express-Lizenz	Citrix ADM Express-Konto ist ein Standardkonto zum Verwalten von ADM-Ressourcen.

Mit einem Express-Konto können Sie begrenzte ADM-Ressourcen verwalten. Weitere Informationen finden Sie unter Verwalten von Citrix ADM Ressourcen mit Express-Konto.

Nachdem die erworbene Lizenz abgelaufen ist, haben Sie 60 Tage Nachfrist. Während der Übergangsfrist können Sie die ADM-Ressourcen auswählen, die mit einem Express-Konto verwaltet werden können.

(Weitere Informationen zu den ersten Schritten mit einem Express-Konto finden Sie unterSchnelleinstieg/en-us/citrix-application-delivery-management-service/getting-started.html[()]und zum Verwalten von Abonnements unterAbonnements verwalten[]/en-us/citrix-application-delivery-management-service/managing-subscriptions.html.)

Lizenz hinzufügen

> Hinweis:
>
> Sie können nur eine Poollizenz für Citrix ADC-Instanzen hinzufügen.

Sie können eine Poollizenz für Citrix ADC-Instanzen in Citrix ADM hinzufügen. Nachdem Sie die Lizenz hinzugefügt haben, können Sie die Lizenzinformationen unter **Konten** > **Abonnements** überprüfen.

So fügen Sie eine Poollizenz hinzu:

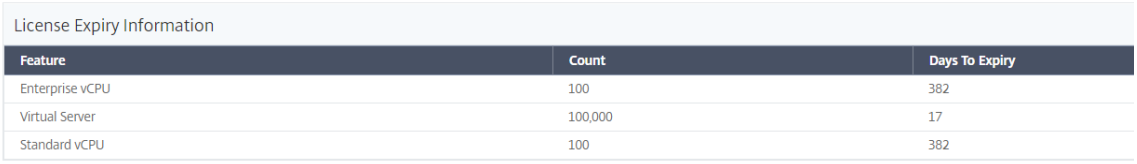
1. Navigieren Sie zu **Netzwerke** > **Lizenzen**.
2. Klicken Sie auf **Lizenzen abrufen**, um die Lizenzdatei auf Ihrem lokalen Computer auszuwählen.
3. Wählen Sie die Lizenzdatei (.lic) aus und klicken Sie auf **OK**.

Ablaufüberprüfungen für virtuelle Serverlizenzen

Sie können nun den Status von Citrix ADM anzeigen und Warnungen für den Ablauf der Lizenz festlegen.

So zeigen Sie den Status der Lizenzen an:

1. Navigieren Sie zu **Netzwerke** > **Lizenzen**.
2. Im Abschnitt **Informationen zum Lizenzablauf** finden Sie die Details der Lizenzen, die ablaufen werden:



License Expiry Information

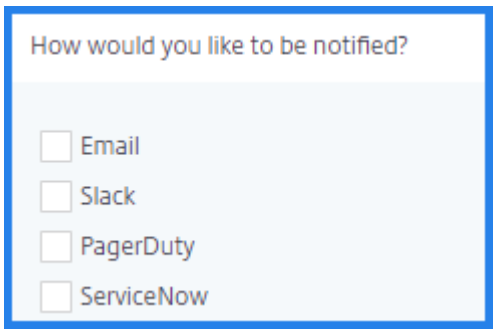
Feature	Count	Days To Expiry
Enterprise vCPU	100	382
Virtual Server	100,000	17
Standard vCPU	100	382

- **Feature**: Art der Lizenz, die ablaufen wird.
- **Count**: Anzahl der Instanzen, die betroffen sind.
- **Tage bis zum Ablauf**: Anzahl der verbleibenden Tage vor Ablauf.

So konfigurieren Sie die Benachrichtigungseinstellungen für Lizenzen:

1. Navigieren Sie zu **Netzwerke**> **Lizenzen**.
2. Klicken Sie im Abschnitt **Benachrichtigungseinstellungen** auf das Stiftsymbol und bearbeiten Sie die Parameter.
   a) **Worüber möchten Sie benachrichtigt werden?** - Geben Sie den Prozentsatz der Kapazität an.
   b) **Wie möchten Sie benachrichtigt werden?** - Wählen Sie die folgenden Benachrichtigungsoptionen aus:
      - **E-Mail** — Geben Sie einen E-Mail-Server und Profildetails an. Eine E-Mail wird ausgelöst, wenn Ihre Lizenzen ablaufen.
      - **Slack** - Geben Sie ein Pufferprofil an. Eine Benachrichtigung wird gesendet, wenn Ihre Lizenzen ablaufen.
      - **PagerDuty** - Geben Sie ein PagerDuty-Profil an. Basierend auf den in Ihrem PagerDuty-Portal konfigurierten Benachrichtigungseinstellungen wird eine Benachrichtigung gesendet, sobald Ihre Lizenzen ablaufen.
      - **ServiceNow** - Eine Benachrichtigung wird an das standardmäßige ServiceNow-Profil gesendet, wenn Ihre Lizenzen ablaufen.

        > **Wichtig**
        >
        > Stellen Sie sicher, dass der Citrix Cloud ITSM-Adapter für ServiceNow konfiguriert und in den Citrix ADM Dienst integriert ist. Weitere Informationen finden Sie unter Integrieren von Citrix ADM Service mit ServiceNow-Instanz.



c) **Ablauf der Lizenzen** - Geben Sie die Tage vor Ablauf der Lizenz an, an denen Sie benachrichtigt werden möchten.

Verwalten von Citrix ADM Ressourcen mit Express-Konto

April 28, 2021

Citrix ADM Express-Konto ist ein Standardkonto zum Verwalten von ADM-Ressourcen. Dieses Konto ist in Citrix Cloud problemlos verfügbar.

Dieses Konto bietet die Optionen zum Verwalten der folgenden ADM-Ressourcen Ihrer Wahl:

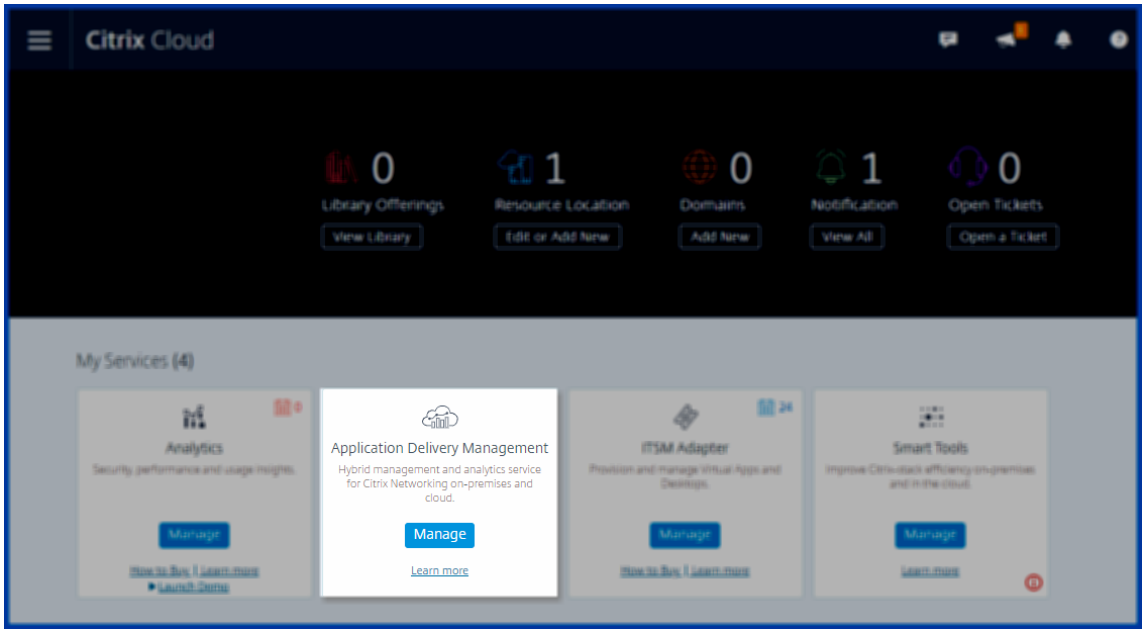
- Bis zu zwei virtuelle Server
- Bis zu zwei Konfigurationsaufträge
- Bis zu zwei StyleBooks Konfigurationspakete

Um die spezifischen Ressourcen mit einem Express-Konto zu verwalten, müssen Sie die erforderlichen Ressourcen während der Kulanzfrist auswählen. Wenn Sie die Ressourcen nicht auswählen, wählt der ADM-Dienst automatisch die Ressourcen aus, die Sie mit dem Express-Konto verwalten können.

> **Wichtig**
>
> - Wenn Ihr Konto in ein Express-Konto konvertiert wird, behält der ADM-Dienst die Speicherdaten bis zu 500 MB oder einen Tag, je nachdem, was der kleinere ist.
> - Wenn Ihr Citrix ADM Express-Konto 90 Tage lang inaktiv bleibt, wird das Konto gelöscht. Das Citrix ADM-Team sendet nach 60 Tagen Inaktivität eine Erinnerung.

So verwalten Sie die ADM-Ressourcen:

1. Melden Sie sich mit Ihren Anmeldeinformationen bei Citrix Cloud an.
2. Klicken Sie auf der Kachel **Citrix Application Delivery Management** auf **Verwalten**.



Nach Ablauf der Citrix ADM Abonnementlizenz und der Kulanzfrist wird Ihr Konto in ein Express-Konto umgewandelt, es sei denn, Sie erneuern Ihre Lizenz. Mit dem Express-Konto können Sie Ihr Geschäft mit dem Citrix ADM Dienst fortsetzen. Um Ihre Citrix ADM -Lizenz zu verlängern, besuchen SieCitrix Cloudoder wenden Sie sich an den technischen Support.

Verwalten von Abonnements

April 28, 2021

Citrix Application Delivery Management (Citrix ADM) erfordert eine verifizierte Lizenz zur Verwaltung und Überwachung von Citrix ADC-Instanzen, Citrix Gateway Instanzen und Lastausgleichsdiensten von Drittanbietern.

Sie können eine beliebige Anzahl von Instanzen verwalten und überwachen, wenn Sie ein Express-Konto verwenden oder eine gültige Lizenz abonniert haben. Sie können jedoch die erkannten Anwendungen im App Dashboard verwalten, Analysedaten anzeigen und Netzwerkfunktionen und Netzwerkberichte nur für die Anzahl der virtuellen Server überwachen, für die Sie Lizenzen erworben haben. Weitere Informationen zu den ADM-Ressourcen, die Sie mit dem Express-Konto verwalten können, finden Sie unterDas Citrix ADM Express-Konto.

Mit jeder installierten Lizenz erhalten Sie eine begrenzte Menge an Daten und Kapazität für die Verwaltung bestimmter virtueller Server. Sie können aber auch reine Datenlizenzen erwerben und anwenden, um Ihre Datenspeicherung aufladen zu können.

Informationen und Anweisungen zum Kauf und Upgrade Ihrer Citrix ADM -Lizenzen finden Sie unterCitrix Application Delivery Management.

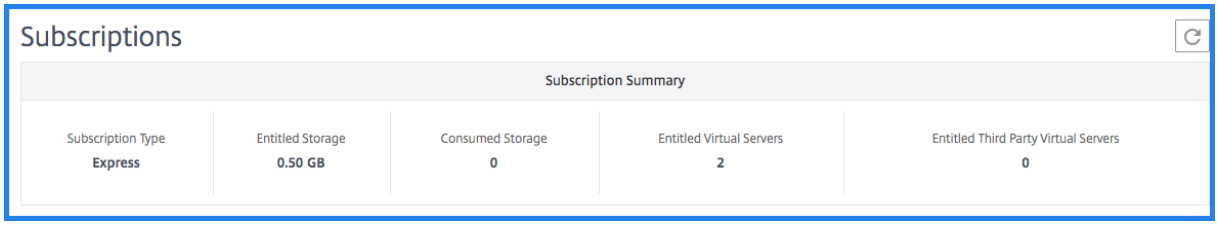
In der folgenden Tabelle sind die Citrix Lizenzen aufgeführt, die für die Verwendung einiger Citrix ADM Features erforderlich sind.

Citrix ADM Feature-Gruppe	Citrix ADM Funktionen	Citrix ADC - und Gateway-Lizenzanforderung
Analytics	HDX Insight	Advanced (Reporting < 1 Stunde) Premium (Reporting = Unbegrenzt)
Analytics	Sicherheitshinweise	Premium (oder) Advanced mit App Firewall-Lizenz
Analytics	Gateway Insight	Advanced (Reporting < 1 Stunde) Premium (Reporting = Unbegrenzt)
Anwendungen	Anwendungsstatistiken (App-Dashboard, App-Sicherheits-Dashboard)	Informationen zu Citrix Web App Firewall im App-Dashboard und App-Sicherheits-Dashboard benötigen Premium (oder) Advanced with App Firewall Lizenz
Anwendungen	API-Gateway	Premium (oder) Advanced-Lizenz
Anwendungen	StyleBooks	Nicht zutreffend
Anwendungen	Bestandsverwaltung — Infrastruktur-Dashboard, Instanzgruppen, Instanz-Dashboards und Sites	Nicht zutreffend
Anwendungen	Ereignisverwaltung & Syslog	Nicht zutreffend
Anwendungen	Konfigurationsaufträge, Konfigurationsüberwachung und Konfigurationshinweise	Nicht zutreffend
Anwendungen	Netzwerkberichterstattung (Instanzebene)	Nicht zutreffend
Anwendungen	Netzwerkberichterstattung (virtuelle Serverebene)	Nicht zutreffend

Citrix ADM Feature-Gruppe	Citrix ADM Funktionen	Citrix ADC - und Gateway-Lizenzanforderung
Anwendungen	Netzwerkfunktionen (Einfache Sichtbarkeit und Verwaltung virtueller Server, Dienste, Servicegruppen, Server)	Nicht zutreffend
Anwendungen	SSL-Zertifikatsverwaltung (Instanzebene)	Nicht zutreffend
Anwendungen	SSL-Zertifikatsverwaltung (virtuelle Serverebene)	Nicht zutreffend
System	RBAC und externe Authentifizierung (Instanzebene)	Nicht zutreffend
System	RBAC und externe Authentifizierung (virtuelle Serverebene)	Nicht zutreffend

Abonnementdetails anzeigen

Sie können die auf Ihrem Citrix ADM installierten Lizenzen anzeigen, indem Sie zu **Konto** > **Abonnements** navigieren. Sie können auch die Lizenzübersicht anzeigen, z. B. den Typ der abonnierten Lizenz, das berechtigte Datenabonnement und das verbrauchte Datenabonnement sowie die zulässigen und verwalteten virtuellen Server und virtuellen Server von Drittanbietern im Abschnitt **Abonnementübersicht**.



Verwalten von Abonnements für virtuelle Server von Drittanbietern

Sie können beliebig viele HAProxy-Hosts verwalten und überwachen, wenn Sie sich in der Testphase befinden oder eine gültige Lizenz abonniert haben. Sie können jedoch die erkannten Anwendungen im HAProxy App Dashboard verwalten, Analysedaten anzeigen und Netzwerkfunktionen nur für die Anzahl der virtuellen Server von Drittanbietern überwachen, für die Sie Lizenzen erworben haben.

Während des Testzeitraums können Sie nur 10 virtuelle Server oder Anwendungen von Drittanbietern überwachen.

> **Hinweis**
>
> In diesem Dokument bezieht sich der virtuelle Server eines Drittanbieters auf das HAProxy-Frontend.

Verwalten virtueller Server

Sie können die virtuellen Server oder virtuellen Server von Drittanbietern auswählen, die Sie über Citrix ADM verwalten und überwachen möchten.

Zu beachtenswerte Punkte:

- Standardmäßig lizenziert Citrix ADM die virtuellen Server nach jedem virtuellen Serverabfragungszyklus automatisch nach dem Zufallsprinzip.
- Wenn die Gesamtzahl der in Ihrem Citrix ADM erkannten virtuellen Server niedriger ist als die Anzahl der installierten virtuellen Serverlizenzen, lizenziert Citrix ADM standardmäßig alle virtuellen Server.

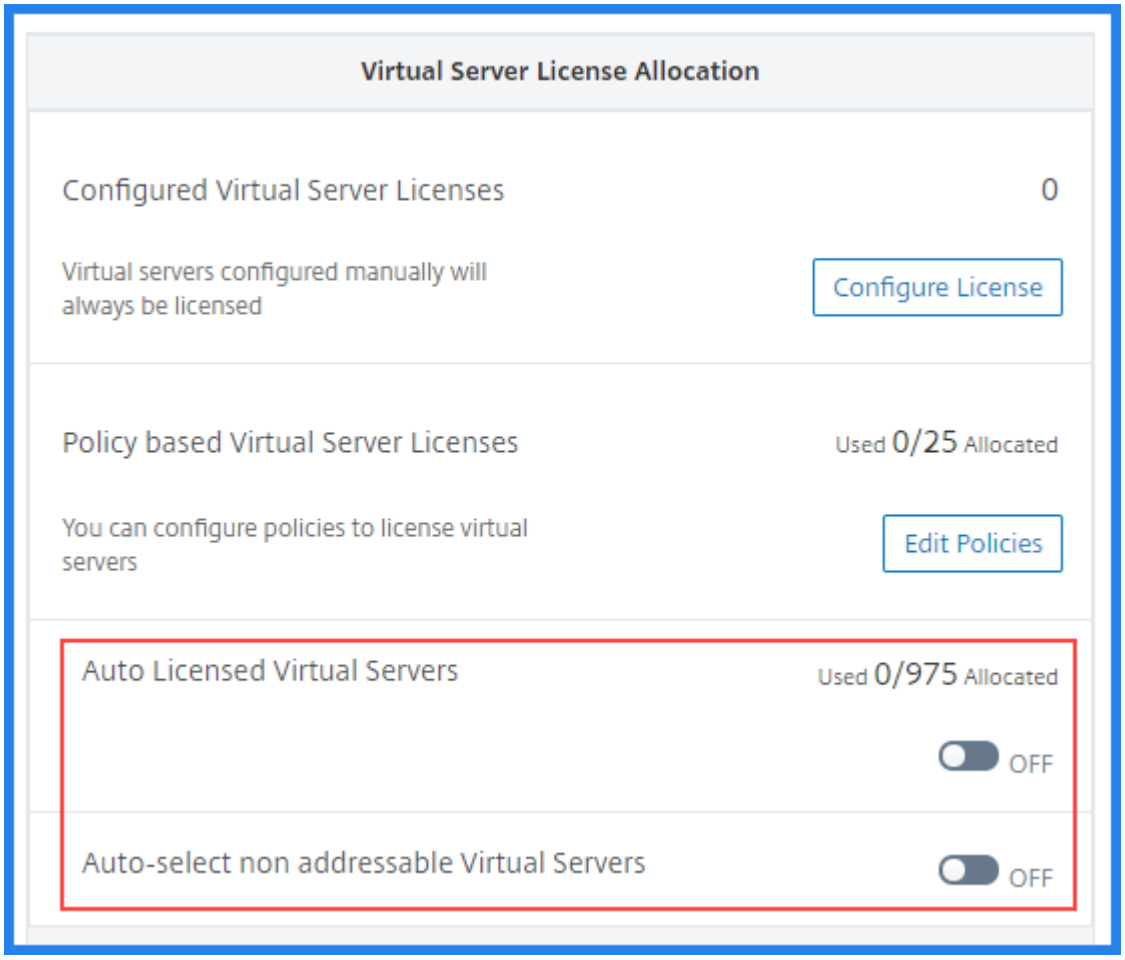
Um die virtuellen Server manuell auszuwählen oder die Lizenzierung auf eingeschränkte virtuelle Server zu beschränken, müssen Sie zuerst die automatische Lizenzierung der virtuellen Server deaktivieren und dann die virtuellen Server auswählen, die Sie verwalten möchten.

So deaktivieren Sie die automatische Lizenzierung virtueller Server:

1. Navigieren Sie zu **Konto > Abonnements**.

   Das Dashboard zeigt die verfügbaren virtuellen Serverlizenzen, die verwalteten virtuellen Server zusammen mit dem virtuellen Servertyp und Informationen zum Ablauf der Lizenz an.

2. Deaktivieren Sie **unter Virtueller Server-Lizenzzuweisung**die Option **Automatisch lizenzierte virtuelle Server, und wählen Sie nicht adressierbare virtuelle Server**automatisch aus.

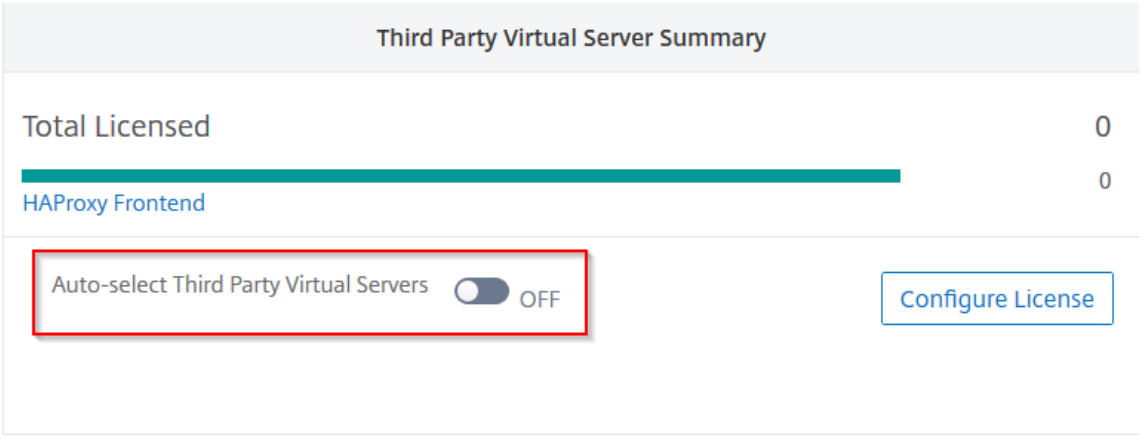


So wählen Sie virtuelle Server von Drittanbietern für die Lizenzierung aus:

1. Navigieren Sie zu **Konto** > **Abonnements**.

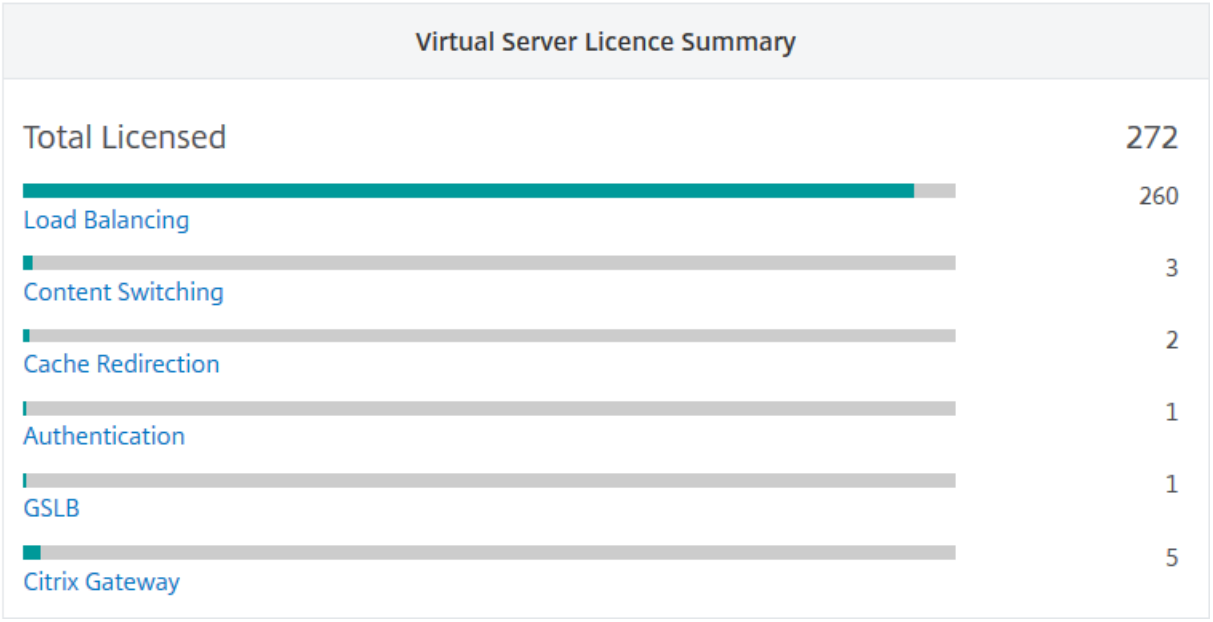
   Das Dashboard zeigt die verfügbaren virtuellen Serverlizenzen, die verwalteten virtuellen Server zusammen mit dem virtuellen Servertyp und Informationen zum Ablauf der Lizenz an.

2. Deaktivieren Sie in der **Zusammenfassung des virtuellen Servers von Drittanbietern**die **automatische Auswahl virtueller Server von Drittanbietern**.



Anzeigen der lizenzierten virtuellen Server

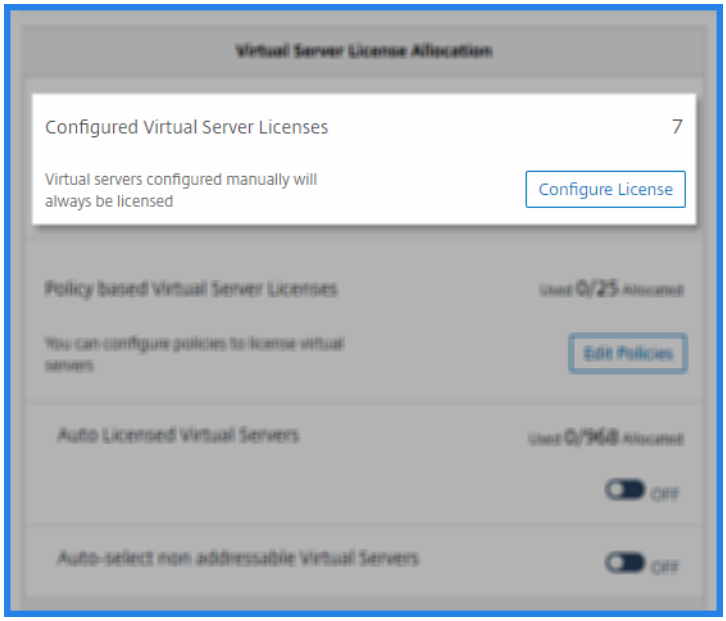
Nachdem die Lizenzen auf die virtuellen Server angewendet wurden, können Sie die lizenzierten virtuellen Server oder virtuellen Server von Drittanbietern auf der Seite **Abonnements** anzeigen. Um die lizenzierten virtuellen Server anzuzeigen, navigieren Sie zu **Konten > Abonnements**, und klicken Sie im Abschnitt **Gesamtlizenzierung** in der **Lizenzübersicht für virtuelle Server auf den virtuellen** Servertyp.



Manuelles Anwenden virtueller Serverlizenzen

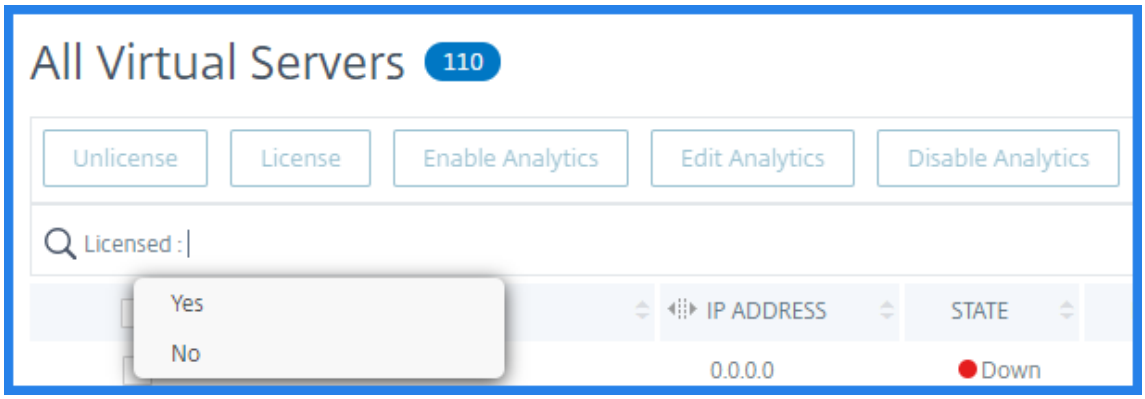
Sie können manuell Lizenzen auf einen einzelnen virtuellen Server anwenden.

1. Wählen Sie unter **Virtueller Server-Lizenzzuweisungdie Option Lizenzen konfigurieren**aus.



Die Seite " **Alle virtuellen Server** " wird angezeigt.

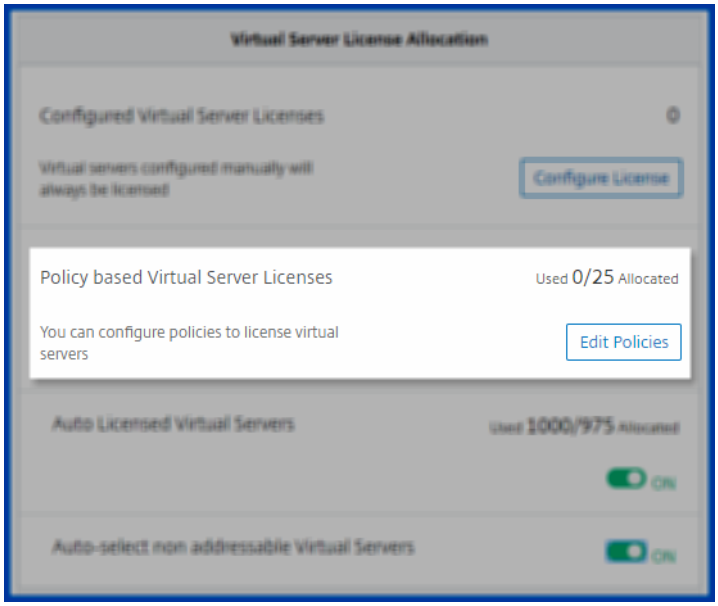
2. Filtern Sie nicht lizenzierte virtuelle Server mithilfe der Eigenschaft: `Licensed: No`.



3. Wählen Sie den virtuellen Server aus, den Sie lizenzieren möchten.
4. Klicken Sie auf **Lizenz**.

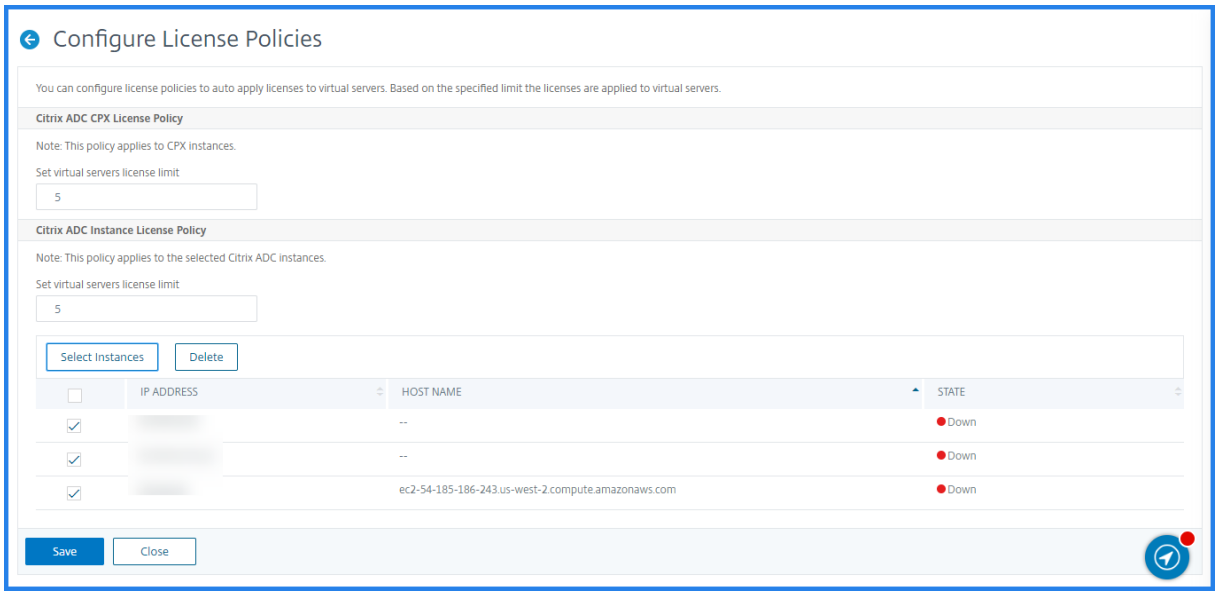
Konfigurieren der richtlinienbasierten Lizenzierung virtueller Server

Sie können eine Richtlinie so konfigurieren, dass eine Lizenz auf virtuelle Server angewendet wird. Diese Richtlinie steuert die Anzahl der virtuellen Server, die Sie automatisch lizenzieren möchten. Außerdem werden Lizenzen nur auf die virtuellen Server ausgewählter Instanzen angewendet.



Klicken Sie auf **Richtlinien bearbeiten**, und Sie können Folgendes angeben:

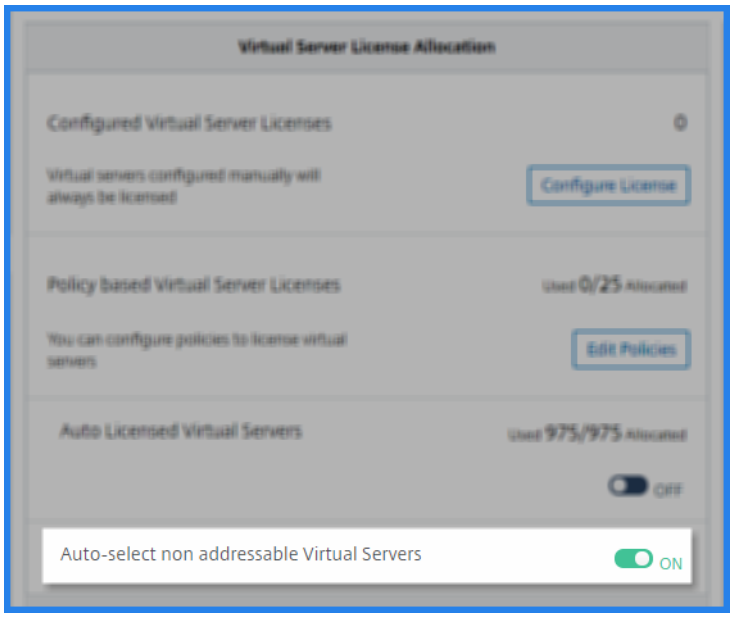
- Legen Sie die Begrenzung virtueller Server für CPX-Instanzen separat fest, um Lizenzen anzuwenden. Der ADM wendet eine Lizenz auf virtuelle Server auf CPX-Instanzen bis zu einem festgelegten Limit an.
- Legen Sie das Limit für virtuelle Server für ausgewählte ADC-Instanzen (MPX/VPX/BLX) fest, um Lizenzen anzuwenden. Der ADM wendet Lizenzen auf virtuelle Server auf ADC-Instanzen bis zu einem festgelegten Limit an.
- Wählen Sie die prioritären ADC-Instanzen aus, die virtuelle Serverlizenzen angewendet werden sollen. Daher kann der ADM eine Lizenz nur auf die virtuellen Server der ausgewählten Instanzen anwenden.



Konfigurieren der automatischen Lizenzunterstützung für nicht adressierbare virtuelle Server

Citrix ADM wendet standardmäßig keine Lizenzen auf nicht adressierbare virtuelle Server an. Für die Lizenzierung nicht adressierbarer virtueller Server müssen Sie die Option für die automatische Lizenzierung deaktivieren und die nicht adressierbaren virtuellen Server manuell auswählen. Dies erhöht den Aufwand, die nicht adressierbaren Server beim Anwenden der Lizenzen anfänglich manuell auszuwählen. Sie müssen auch die neuen nicht adressierbaren virtuellen Server manuell auswählen, wenn sie Ihrem Netzwerk hinzugefügt werden.

Citrix ADM bietet eine Option in Citrix ADM unter **Virtual Server License Allocation**. Wenn Sie die Option **Nicht adressierbare virtuelle Server automatisch auswählen** aktivieren, wenden Sie Lizenzen nicht adressierbare virtuelle Server automatisch an.



Hinweis

- Citrix ADM wählt nicht adressierbare virtuelle Server standardmäßig immer noch nicht automatisch für die Lizenzierung aus.
- Anwendungsanalysen (App Dashboard) sind die einzige Analyse, die derzeit auf lizenzierten, nicht adressierbaren virtuellen Servern unterstützt wird.

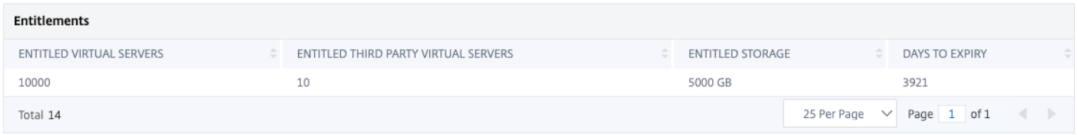
Ablaufüberprüfungen für virtuelle Serverabonnements anzeigen

Sie können den Status der installierten Lizenzen mit dem Ablaufdatum und dem zulässigen Speicherlimit für die Lizenzen in Citrix ADM anzeigen.

So zeigen Sie den Status der Lizenzen an:

1. Navigieren Sie zu **Konto** > **Abonnements**.

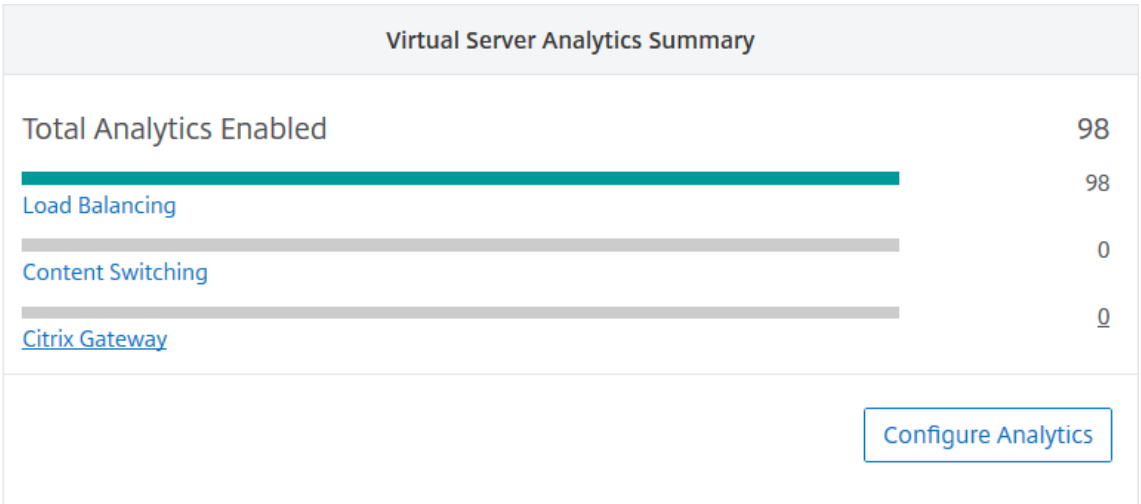
2. Im Abschnitt **Berechtigungen** können Sie die Details der lizenzierten virtuellen Server und die Tage für den Ablauf anzeigen:
    - **Berechtigte virtuelle Server:** Anzahl der virtuellen Server, die lizenziert werden können.
    - **Virtuelle Server von Drittanbietern:** Anzahl der virtuellen Server von Drittanbietern, die Sie mit der Lizenz verwalten können.
    - **Berechtigter Speicher:** Speicherlimit der Lizenz.
    - **Tage bis zum Ablauf:** Anzahl der Tage, die vor Ablauf der Lizenz verbleiben.



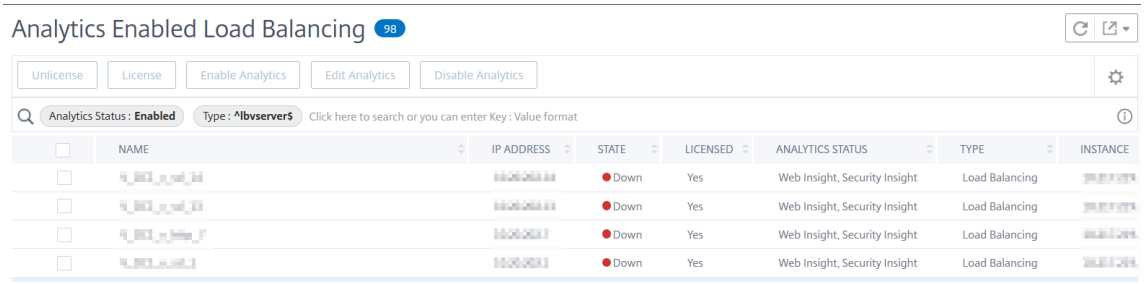
Anzeigen des auf den virtuellen Servern aktivierten Analysetyps

Nachdem Sie AppFlow auf den ausgewählten virtuellen Servern aktiviert haben, können Sie den auf den lizenzierten virtuellen Servern oder virtuellen Servern von Drittanbietern aktivierten Analysetyp auf der Seite **Abonnements** anzeigen.

1. Navigieren Sie zu **Konto** > **Abonnements**.
2. Wählen Sie im Abschnitt **Virtual Server Analytics Summary** den Typ der lizenzierten virtuellen Server aus.



3. Auf der Seite Lizenzierte virtuelle Server wird die Liste der lizenzierten virtuellen Server angezeigt. Auf dieser Seite wird in der Spalte **Analytics-Status** der Analysetyp angezeigt, der auf den virtuellen Servern aktiviert ist.



Einrichten

April 28, 2021

Nachdem die erste Einrichtung abgeschlossen ist, müssen Sie bestimmte Einstellungen konfigurieren, um mit der vollständigen Verwaltung der Bereitstellung zu beginnen.

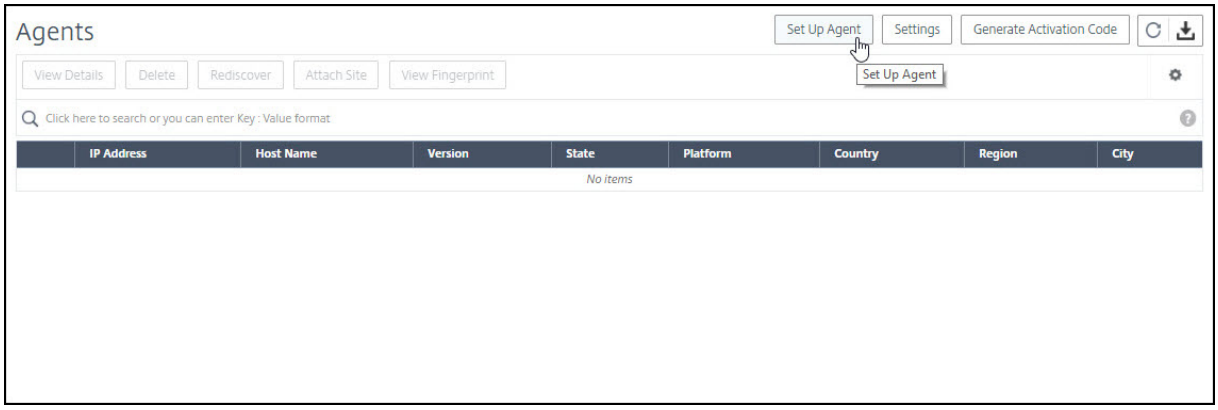
- Hinzufügen mehrerer Agents. Die Anzahl der zu installierenden Agents hängt von der Anzahl der verwalteten Instanzen in einem Rechenzentrum oder einer Cloud und dem Gesamtdurchsatz ab. Citrix empfiehlt, mindestens einen Agenten für jedes Rechenzentrum zu installieren.
- Instanzen hinzufügen. Sie können Instanzen entweder beim Einrichten des Citrix ADM fürzum ersten Maloder zu einem späteren Zeitpunkt hinzufügen. Sie müssen Instanzen zum Dienst hinzufügen, um sie zu verwalten und zu überwachen. Nachdem Sie mehrere Agents installiert haben, müssen Sie Instanzen hinzufügen und sie den Agents zuordnen.
- Analytics aktivieren. Um Analysedaten für den Anwendungsdatenverkehr anzuzeigen, müssen Sie die Analytics-Funktion auf den virtuellen Servern aktivieren, die Datenverkehr für die spezifischen Anwendungen empfangen.
- Konfigurieren von Syslog für Instanzen. Sie können die Syslog-Ereignisse überwachen, die auf Ihren Citrix ADC-Instanzen generiert werden, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Nachrichten an Citrix ADM umgeleitet werden. Um Syslog-Ereignisse zu überwachen, müssen Sie zuerst Citrix ADM als Syslog-Server für Ihre Citrix ADC-Instanz konfigurieren.
- Konfigurieren der rollenbasierten Zugriffssteuerung. Citrix ADM bietet eine fein abgestimmte, rollenbasierte Zugriffssteuerung (RBAC), mit der Sie Zugriffsberechtigungen basierend auf den Rollen einzelner Benutzer in Ihrem Unternehmen erteilen können.
- Analytics-Einstellungen konfigurieren. Sie können bestimmte Einstellungen konfigurieren, um eine optimale Erfahrung mit der Analytics-Funktion zu gewährleisten. Sie können beispielsweise die Dauer angeben, in der historische Analytics-Daten gespeichert werden sollen, und Sie können auch Schwellenwerte und Warnungen festlegen, um die gewünschten Analytics-Metriken zu überwachen.

Hinzufügen mehrerer Agents

April 28, 2021

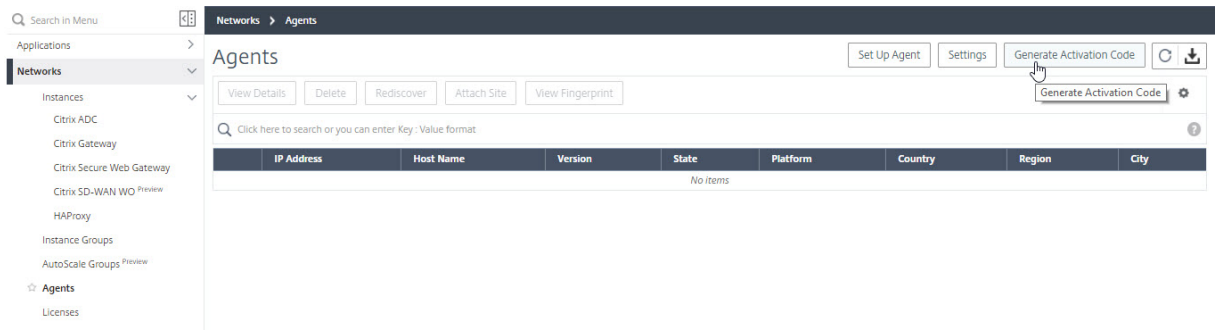
Die Anzahl der zu installierenden Agents hängt von der Anzahl der verwalteten Instanzen in einem Rechenzentrum und dem Gesamtdurchsatz ab. Citrix empfiehlt, mindestens einen Agenten für jedes Rechenzentrum zu installieren.

Sie können nur einen Agenten installieren, wenn Sie sich zum ersten Mal beim Dienst anmelden. Um mehrere Agents hinzuzufügen, schließen Sie zuerst die Erstinstallation ab, navigieren Sie zu **Netzwerke > Agents**, und klicken Sie auf **Agent einrichten**.



Laden Sie das Image für den erforderlichen Hypervisor herunter, und installieren Sie den Agenten, indem Sie die Anweisungen unter Erste Schritte. Vergewissern Sie sich, dass Sie die Service-URL und den Aktivierungscode auf dem Bildschirm kopieren, da Sie während der Installation des Agents auf Ihrem Hypervisor die Service-URL und den Aktivierungscode eingeben müssen. Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.

Sie können dasselbe Image verwenden, um mehrere Agents in Ihrem Hypervisor zu installieren. Sie können den gleichen Aktivierungscode jedoch nicht auf mehreren Agents verwenden. Nachdem Sie einen Agenten installiert haben, generieren Sie den Aktivierungscode erneut für den nächsten Agenten. Sie können einen neuen Aktivierungscode generieren, indem Sie zu **Netzwerke > Agents**navigieren und auf **Aktivierungscode generieren**klicken.



Nachdem der Agent erfolgreich installiert und registriert wurde, überprüfen Sie den Agent-Status auf der Dienst-GUI und fügen Sie Instanzen hinzu.

> **Hinweis**
>
> Sie können auch einen Citrix ADM-Agenten in der Microsoft Azure Cloud oder AWS Cloud installieren. Das Agent-Image ist auf dem jeweiligen Cloud-Marktplatz verfügbar.
>
> - Anweisungen zum Installieren eines Agenten in der Microsoft Azure-Cloud finden Sie unter Installieren von Citrix ADM Agent in Microsoft Azure Cloud.
> - Anweisungen zum Installieren eines Agenten in AWS finden Sie unter Installieren von Citrix ADM Agent in AWS.

Konfigurieren von Citrix ADM -Agenten für die Bereitstellung mehrerer Sites

April 28, 2021

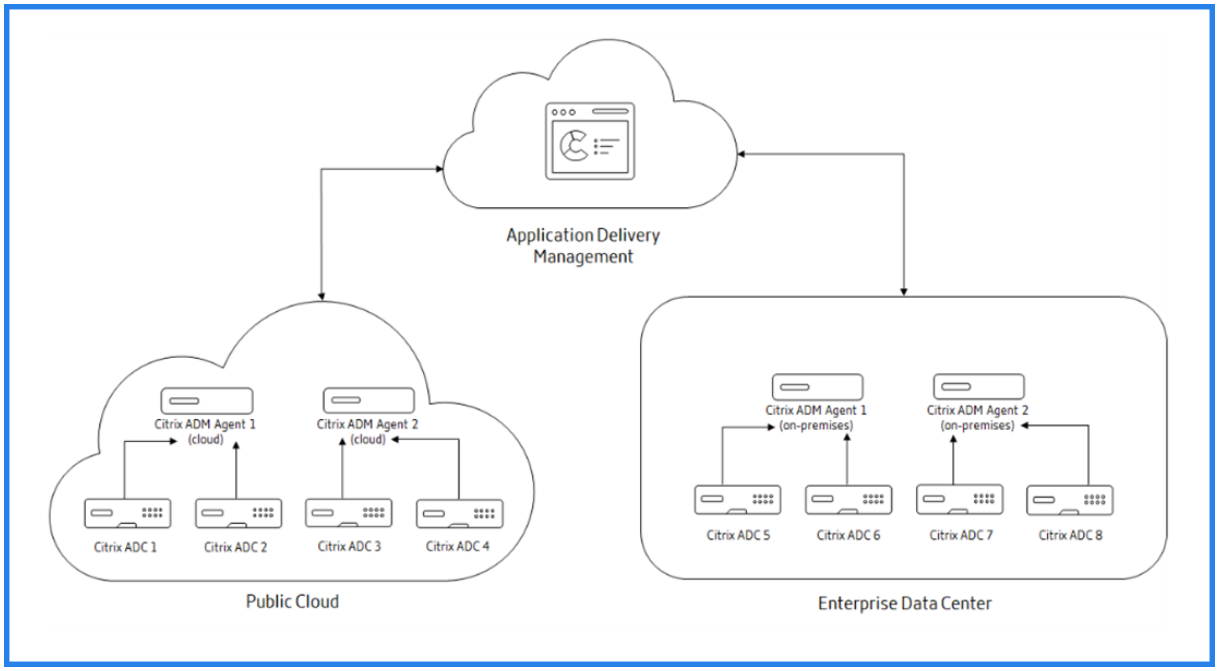
Agents arbeiten als Vermittler zwischen dem Citrix ADM Dienst und den erkannten Instanzen in verschiedenen Rechenzentren und Public Clouds. Citrix ADM unterstützt Agent-Failover in einem Rechenzentrum oder einer Public Cloud.

Die folgenden Vorteile der Installation von Agenten:

- Die konfigurierten Instanzen an einen Agenten senden die unverarbeiteten Daten direkt an den Agent anstelle des Citrix ADM Dienstes. Der Agent führt die erste Ebene der Datenverarbeitung durch und sendet die verarbeiteten Daten in komprimiertem Format zur Speicherung an das Citrix ADM.
- Agenten und Instanzen befinden sich in demselben Rechenzentrum oder derselben Cloud, sodass die Datenverarbeitung schneller erfolgt.
- Das Clustering der Agents ermöglicht die Neuverteilung von Citrix ADC-Instanzen beim Agent-Failover. Wenn ein Agent in einer Site ausfällt, wechselt der Datenverkehr von Citrix ADC-Instanzen zu einem anderen verfügbaren Agenten an derselben Site.

Architektur

Die folgende Abbildung zeigt Citrix ADC-Instanzen, die auf mehreren Agenten in einem Rechenzentrum und einer Public Cloud konfiguriert sind, um ein Agent-Failover zu erzielen:



Die Public Cloud verfügt über vier ADC-Instanzen und zwei ADM-Agenten. Das Rechenzentrum des Unternehmens verfügt außerdem über vier ADC-Instanzen und zwei ADM-Agenten. Jeder Agent ist mit zwei ADC-Instanzen konfiguriert.

Die Agenten empfangen Daten direkt von den konfigurierten Instanzen. Nachdem der Agent die Daten empfängt, verarbeitet der Agent die Daten und sendet ihn in einem komprimierten Format an den Citrix ADM Dienst. Agents kommunizieren mit dem Citrix ADM -Server über einen sicheren Kanal.

Wenn **Citrix ADM Agent 1** in Public Cloud inaktiv wird (DOWN Status), tritt ein Agent-Failover auf. Der Citrix ADM-Dienst verteilt die ADC-Instanzen von **Citrix ADM Agent 1** mit **Citrix ADM Agent 2.** Die Umverteilung der Instanzen erfolgt in einem Unternehmensrechenzentrum, wenn einer der Agenten im Rechenzentrum ausfällt.

Informationen zur Installation eines Citrix ADM -Agents finden Sie unter Installieren des Citrix ADM Agenten.

Citrix ADM Agent-Failover

Das Agenten-Failover kann an einem Standort mit zwei oder mehr registrierten Agenten auftreten. Wenn ein Agent in der Site inaktiv wird (DOWN Status), verteilt der Citrix ADM Dienst die ADC-Instanzen des inaktiven Agents mit anderen aktiven Agenten neu.

> **Wichtig**
>
> - Citrix ADM Agentenfailover berücksichtigt keine CPX-Instanzen.
> - Stellen Sie sicher, dass die Agenten-Failover-Funktion für Ihr Konto aktiviert ist. Informa-

> tionen zum Aktivieren dieser Funktion finden Sie unter Aktivieren oder Deaktivieren von ADM-Funktionen.
>
> - Wenn ein Agent ein Skript ausführt, stellen Sie sicher, dass das Skript auf allen Agenten in der Site vorhanden ist. Daher kann der geänderte Agent das Skript nach dem Agent-Failover ausführen.

So hängen Sie eine Site an einen Agenten in der Citrix ADM-Benutzeroberfläche an:

1. Navigieren Sie zu **Netzwerke > Agents**.
2. Wählen Sie einen Agenten aus, den Sie an eine Site anhängen möchten.
3. Geben Sie die Site aus der Liste an. Wenn Sie eine neue Website hinzufügen möchten, klicken Sie auf **Hinzufügen**.
4. Klicken Sie auf **Save**.

Um ein Agent-Failover zu erzielen, wählen Sie Citrix ADM -Agents nacheinander aus, und fügen Sie sie an dieselbe Site an.

Beispielsweise sind zwei Agenten 10.106.1xx.2x und 10.106.1xx.7x am Standort Bangalore angeschlossen und betriebsbereit. Wenn ein Agent inaktiv wird, erkennt Citrix ADM ihn und zeigt den Status als heruntergefahren an.

Wenn ein Citrix ADM-Agent an einem Standort inaktiv wird (Down-Status), wartet Citrix ADM einige Minuten darauf, dass der Agent aktiv wird (Status “Aufwärts”). Wenn der Agent inaktiv bleibt, verteilt Citrix ADM die Instanzen automatisch auf die verfügbaren Agents an derselben Site neu. Diese Umverteilung kann etwa 10 bis 15 Minuten dauern.

Citrix ADM löst die Instanzumverteilung alle 30 Minuten aus, um die Last zwischen den aktiven Agenten in der Site auszugleichen.

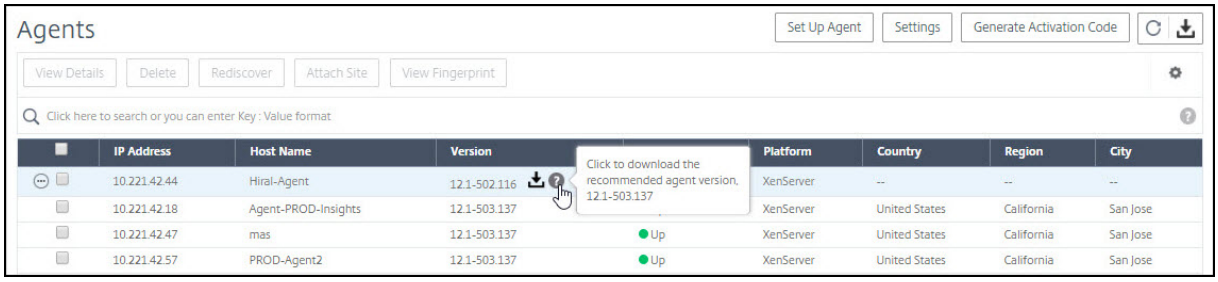
Die Instanzen, die Agenten an derselben Site für Trap-Destination, Syslog-Server und Analysen angefügt und automatisch neu konfiguriert wurden.

Konfigurieren der Agent-Upgradeeinstellungen

April 28, 2021

In Citrix ADM werden Agents, die auf Softwareversion 12.0 Build 507.110 und höher ausgeführt werden, automatisch von Citrix ADM auf neuere und empfohlene Versionen aktualisiert. Der Agent wird entweder aktualisiert, wenn eine neue Version verfügbar ist oder zu einem von Ihnen angegebenen Zeitpunkt.

Sie können die aktuelle Version und die empfohlene Version Ihrer Agenten anzeigen, indem Sie zu **Netzwerke** > **Agents** navigieren.



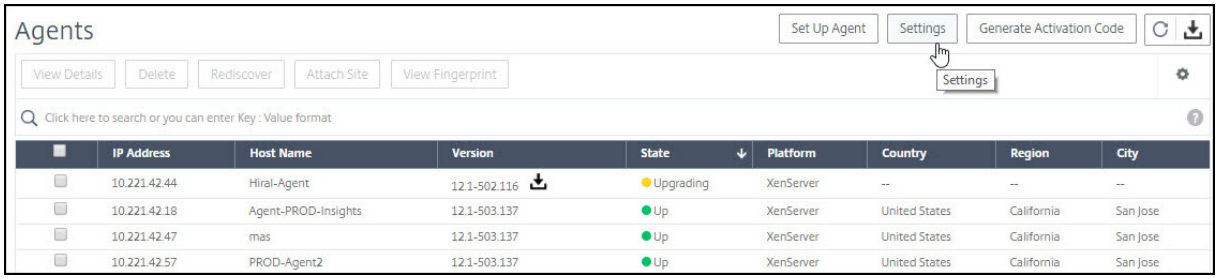
Standardmäßig wird ein Agent automatisch aktualisiert, wenn eine neuere Version verfügbar ist. Sie können jedoch angeben, wann das Agent-Upgrade durchgeführt werden soll.

Wenn Sie eine bestimmte Zeit auswählen, werden die Agents zu dem angegebenen Zeitpunkt aktualisiert, jedoch in der Zeitzone, in der Ihre Agents bereitgestellt werden.

Während des Upgrades kann es zu einer Ausfallzeit von etwa 30 Minuten kommen.

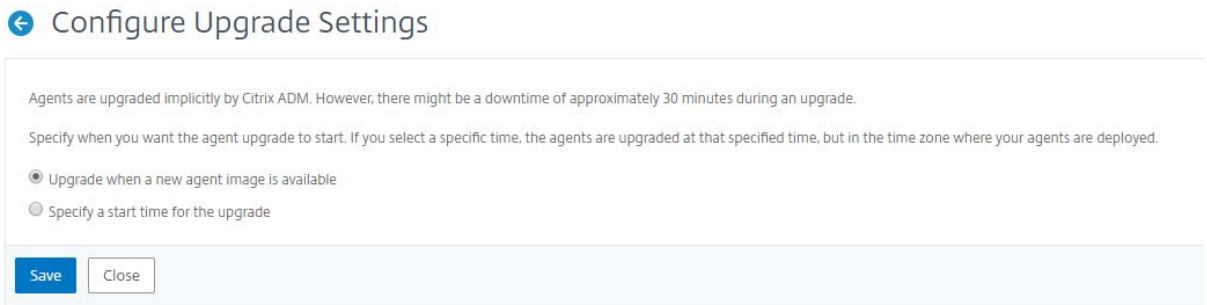
So konfigurieren Sie Agent-Upgradeeinstellungen:

Navigieren Sie zu **Netzwerke** > **Agents**, und klicken Sie auf **Einstellungen**.



Geben Sie an, wann das Agent-Upgrade gestartet werden soll. Sie können ein Upgrade auswählen, wenn ein neuer Agent verfügbar ist, oder Sie können einen bestimmten Zeitpunkt festlegen, zu dem Citrix ADM den Agenten implizit aktualisieren soll. Die von Ihnen festgelegte Zeit ist spezifisch für die Agent-Zeitzone.

Klicken Sie auf **Speichern**, um Ihre Einstellungen zu speichern. Diese Einstellungen bleiben für zukünftige Agent-Upgrades bestehen, bis Sie die Einstellungen ändern.



Instanzen hinzufügen

April 28, 2021

Sie können Instanzen entweder beim Einrichten von Citrix Application Delivery Management (Citrix ADM) fürzum ersten Maloder höher hinzufügen.

Instanzen sind Citrix Appliances oder virtuelle Appliances, die Sie von Citrix ADM aus ermitteln, verwalten und überwachen möchten. Sie können Citrix ADM die folgenden Citrix Appliances und virtuellen Appliances hinzufügen:

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix ADC BLX
- Citrix Gateway
- Citrix Secure Web Gateway
- Citrix SD-WAN WANOP

Um Instanzen hinzuzufügen, müssen Sie entweder den Hostnamen oder die IP-Adresse jeder Citrix ADC-Instanz oder einen Bereich von IP-Adressen angeben. Geben Sie für SD-WAN-Instanzen die IP-Adresse jeder Instanz oder einen Bereich von IP-Adressen an.

> **Hinweis**
>
> Citrix ADM unterstützt nur Citrix SD-WAN WANOP.

Geben Sie ein Instanzprofil an, mit dem Citrix ADM auf die Instanz zugreifen kann. Dieses Instanzprofil enthält den Benutzernamen und das Kennwort der Instanzen, die Sie dem Dienst hinzufügen möchten. Für jeden Instanztyp ist ein Standardprofil verfügbar. Beispielsweise ist das ns-root-Profil das Standardprofil für Citrix ADC-Instanzen. Die standardmäßigen Citrix ADC-Administratoranmeldeinformationen definieren dieses Profil. Wenn Sie die standardmäßigen Administratoranmeldeinformationen Ihrer Instanzen geändert haben, können Sie benutzerdefinierte Instanzprofile für diese Instanzen definieren. Wenn Sie die Anmeldeinformationen einer Instanz ändern, nachdem die Instanz erkannt wurde, müssen Sie das Instanzprofil bearbeiten oder ein Profil erstellen und dann die Instanz neu ermitteln.

Sie können vom Citrix ADM aus auf die GUIs von Citrix ADC-Instanzen zugreifen, nachdem Sie die Instanzen im Citrix ADM hinzugefügt haben. Um vom Citrix ADM aus auf die Citrix ADC-Instanzen zuzugreifen, müssen Sie mit dem Citrix Netzwerk verbunden sein.

> **Hinweis**
>
> - Um Citrix ADC-Instanzen hinzuzufügen, die in einem Cluster konfiguriert sind, müssen

> Sie entweder die Cluster-IP-Adresse oder einen der einzelnen Knoten im Cluster-Setup angeben. Unter Citrix ADM repräsentiert die Cluster-IP-Adresse jedoch den Cluster.
>
> - Für die Citrix ADC-Instanzen, die als HA-Paar eingerichtet sind, wird beim Hinzufügen einer Instanz automatisch die andere Instanz im Paar hinzugefügt.

So fügen Sie Citrix ADC-Instanz zu Citrix ADM hinzu

> **Hinweis**
>
> Führen Sie diese Aufgabe aus, um alle anderen ADC-Instanzen mit Ausnahme der ADC CPX-Instanz hinzuzufügen.

1. Navigieren Sie zu **Netzwerke** > **Dashboard**, und klicken Sie auf **Alle Instanzen**. Klicken Sie auf der Seite **Instanzen** oben rechts auf der Seite auf **Neu**. Wählen Sie auf der Seite **Instanz hinzufügen** unter **Instanztyp** den Instanztyp aus, den Sie hinzufügen möchten.

   Alternativ können Sie zu **Netzwerke**> **Instanzen** navigieren. Wählen Sie unter Instanzen den Instanztyp aus, den Sie hinzufügen möchten (z. B. Citrix ADC VPX), und klicken Sie auf **Hinzufügen**.

2. Wählen Sie eine der folgenden Optionen:

   - **IP-Adresse des Geräts eingeben** - Geben Sie bei Citrix ADC-Instanzen entweder den Hostnamen oder die IP-Adresse jeder Instanz oder einen Bereich von IP-Adressen an. Geben Sie für SD-WAN-Instanzen die IP-Adresse jeder Instanz oder einen Bereich von IP-Adressen an.
   - **Aus Datei importieren** - Laden Sie aus Ihrem lokalen System eine Textdatei hoch, die die IP-Adressen aller Instanzen enthält, die Sie hinzufügen möchten.

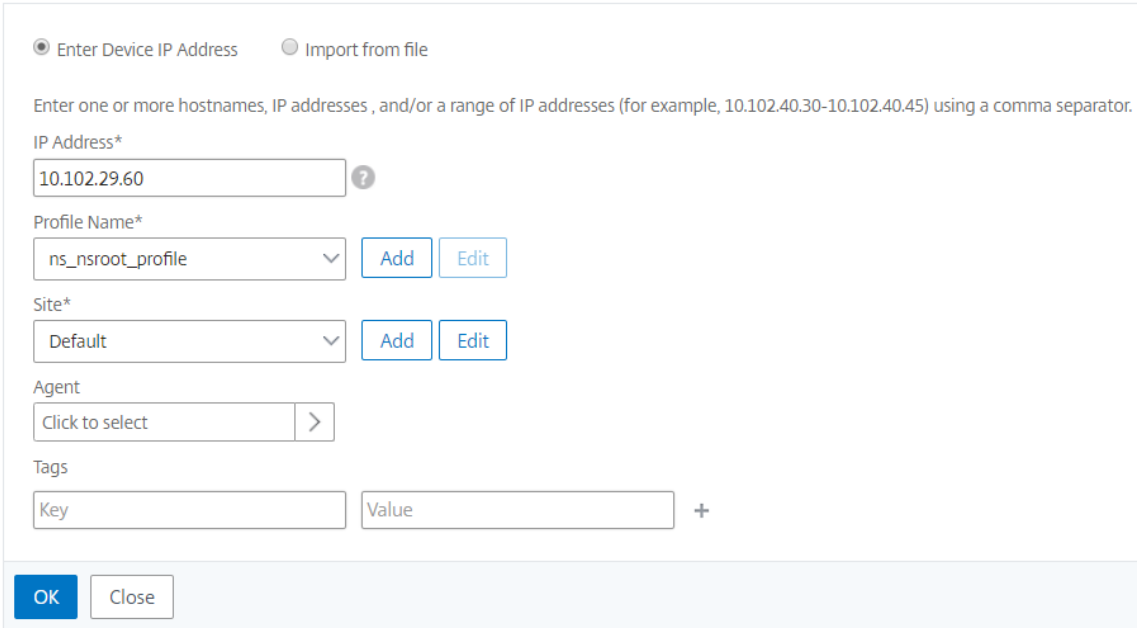
3. (Optional) Wählen Sie **Gerätezusatz beim ersten Anmeldefehler aktivieren**aus. Mit dieser Option können Sie die Instanz auch ohne gültige Anmeldeinformationen hinzufügen.

4. Wählen Sie unter **Profilname** das entsprechende Instanzprofil aus, oder erstellen Sie ein Profil, indem Sie auf das Symbol **+** klicken.

5. Wählen Sie unter **Site** die Site aus, an der die Instanz hinzugefügt werden soll.

6. Wählen Sie unter **Agent** den Agenten aus, dem Sie die Instanzen zuordnen möchten, und klicken Sie dann auf **OK**.

   Wenn auf Ihrem Citrix ADM nur ein Agent konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.



So fügen Sie Citrix ADC CPX-Instanz in ADM hinzu

1. Navigieren Sie zu **Netzwerke** > **Instanzen**. Wählen Sie unter **Instanzen** die Option **Citrix ADC** aus, und wählen Sie die Registerkarte CPX aus.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie eine der folgenden Optionen:
   - **Geben Sie die IP-Adresse des Geräts ein**. Geben Sie entweder den Hostnamen oder die IP-Adresse jeder Instanz oder einen Bereich von IP-Adressen an.
   - **Aus Datei importieren**. Laden Sie von Ihrem lokalen System eine Textdatei hoch, die die IP-Adressen aller Instanzen enthält, die Sie hinzufügen möchten.
4. (Optional) Wählen Sie **Gerätezusatz beim ersten Anmeldefehler aktivieren**aus. Mit dieser Option können Sie die Instanz auch ohne gültige Anmeldeinformationen hinzufügen.
5. Geben Sie im Feld **Routable IP/Docker IP** die IP-Adresse ein. Die IP-Adresse kann entweder die Citrix ADC CPX-Instanz (falls erreichbar) oder der Docker Host sein.
6. Wählen Sie im Feld **Profilname** das entsprechende Instanzprofil aus, oder erstellen Sie ein Profil, indem Sie auf das Symbol + klicken.

   > **Hinweis:**
   >
   > Stellen Sie beim Erstellen eines Profils sicher, dass Sie die HTTP-, HTTPS-, SSH- und SNMP-Port-Details des Hosts angeben. Sie können auch den Bereich der Ports angeben, die vom Host veröffentlicht werden, im Feld Startport und Anzahl der Ports angeben.

7. Wählen Sie optional den Standort aus, an dem die CPX-Instanz bereitgestellt werden soll. Sie können eine Website auch erstellen, indem Sie auf **Hinzufügen** klicken.
8. Wählen Sie, falls verfügbar, den Citrix ADM Dienst-Agent aus der Agentenliste aus.
9. Klicken Sie auf **OK**, um das Hinzufügen von Instanzen zu Citrix ADM zu initiieren.

> **Hinweis**
>
> Wenn Sie eine Instanz wiederfinden möchten, führen Sie die folgenden Schritte aus:
>
> a) Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC** > **CPX**.
> b) Wählen Sie die Instanz aus, die Sie erneut ermitteln möchten.
> c) Klicken Sie in der Liste **Aktion auswählen** auf **Wiederermitteln**.

So fügen Sie eine eigenständige Citrix ADC BLX-Instanz in Citrix ADM hinzu

Eine eigenständige Citrix ADC BLX-Instanz ist eine einzelne Instanz, die auf dem dedizierten Host-Linux-Server ausgeführt wird.

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Klicken Sie auf der Registerkarte **BLX** auf **Hinzufügen**.
3. (Optional) Wählen Sie **Gerätezusatz beim ersten Anmeldefehler aktivieren**aus. Mit dieser Option können Sie die Instanz auch ohne gültige Anmeldeinformationen hinzufügen.
4. Wählen Sie in der Liste **Instanztyp** die Option **Standalone** aus.
5. Geben Sie im Feld **IP-Adresse** die IP-Adresse der BLX-Instanz an.
6. Geben Sie im Feld **Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die BLX-Instanz gehostet wird.
7. Wählen Sie in der Liste **Profilname** das entsprechende Profil für eine BLX-Instanz aus, oder erstellen Sie ein Profil.

   Um ein Profil zu erstellen, klicken Sie auf **Hinzufügen**.

   > **Wichtig**
   >
   > Stellen Sie sicher, dass Sie den richtigen Hostbenutzernamen und das korrekte Kennwort des Linux-Servers im Profil angegeben haben.

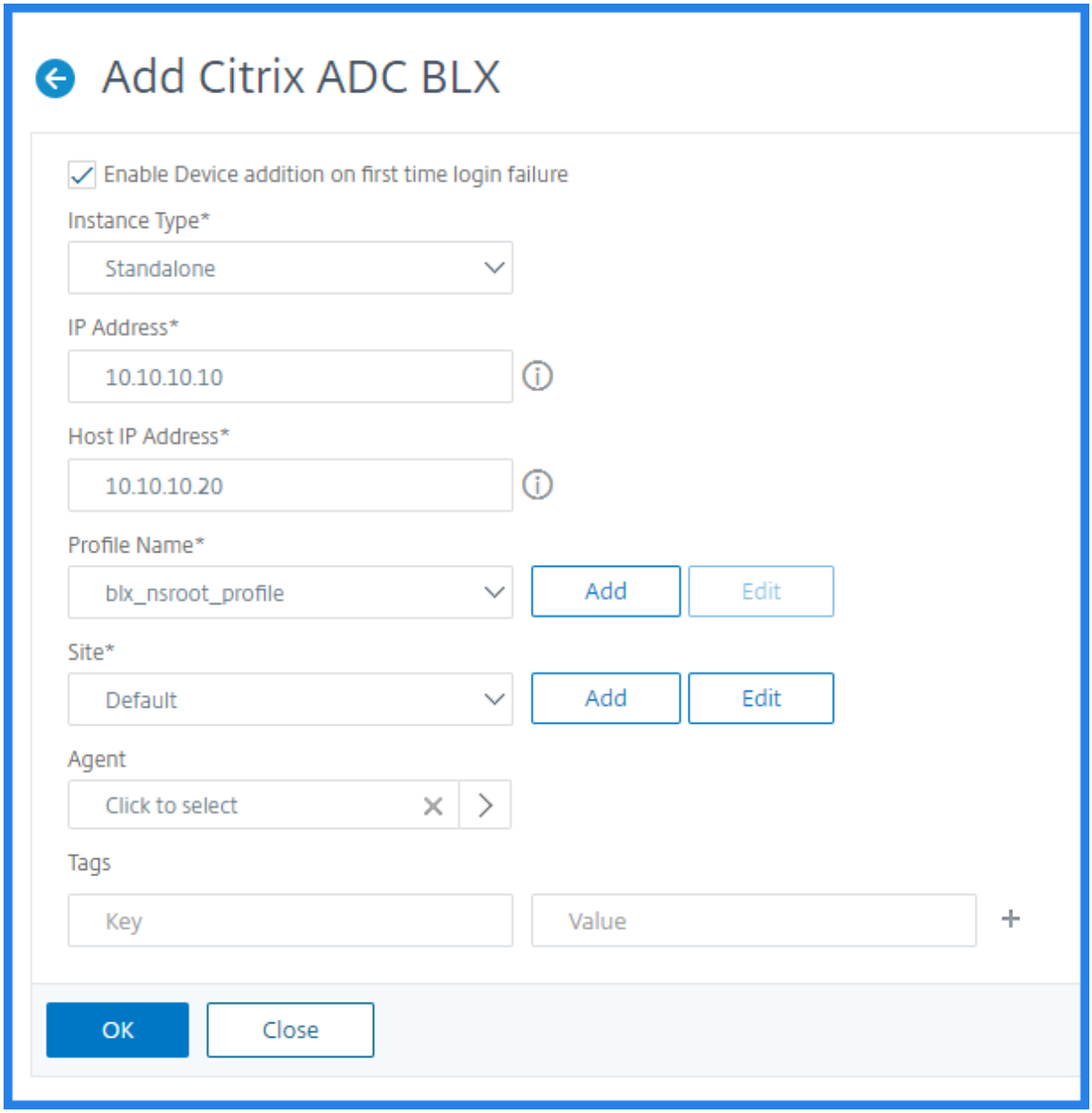
8. Wählen Sie in der Liste **Site** die Site aus, an der Sie eine Instanz hinzufügen möchten.

   Wenn Sie eine Website hinzufügen möchten, klicken Sie auf **Hinzufügen**.

9. Wählen Sie in der Liste **Agent** den Citrix ADM Agent aus, dem Sie die Instanz zuordnen möchten.

   Wenn auf Ihrem Citrix ADM nur ein Agent konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.

10. Klicken Sie auf **OK**.



So fügen Sie Citrix ADC BLX-Instanzen mit hoher Verfügbarkeit in Citrix ADM hinzu

Die hochverfügbaren Citrix ADC BLX-Instanzen, die auf verschiedenen Host-Linux-Servern ausgeführt werden. Ein Linux-Server kann nicht mehr als eine BLX-Instanzen hosten.

1. Klicken Sie auf der Registerkarte **BLX** auf **Hinzufügen**.
2. (Optional) Wählen Sie **Gerätezusatz beim ersten Anmeldefehler aktivieren**aus. Mit dieser Option können Sie die Instanz auch ohne gültige Anmeldeinformationen hinzufügen.
3. Wählen Sie die Option **Hochverfügbarkeit** aus der Liste **Instanztyp** aus.

4. Geben Sie im Feld **IP-Adresse** die IP-Adresse der BLX-Instanz an.
5. Geben Sie im Feld **Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die BLX-Instanz gehostet wird.
6. Geben Sie im Feld **Peer-IP-Adresse** die IP-Adresse der Peer-BLX-Instanz an.
7. Geben Sie im Feld **Peer-Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die Peer-BLX-Instanz gehostet wird.
8. Wählen Sie in der Liste **Profilname** das entsprechende Profil für eine BLX-Instanz aus, oder erstellen Sie ein Profil.

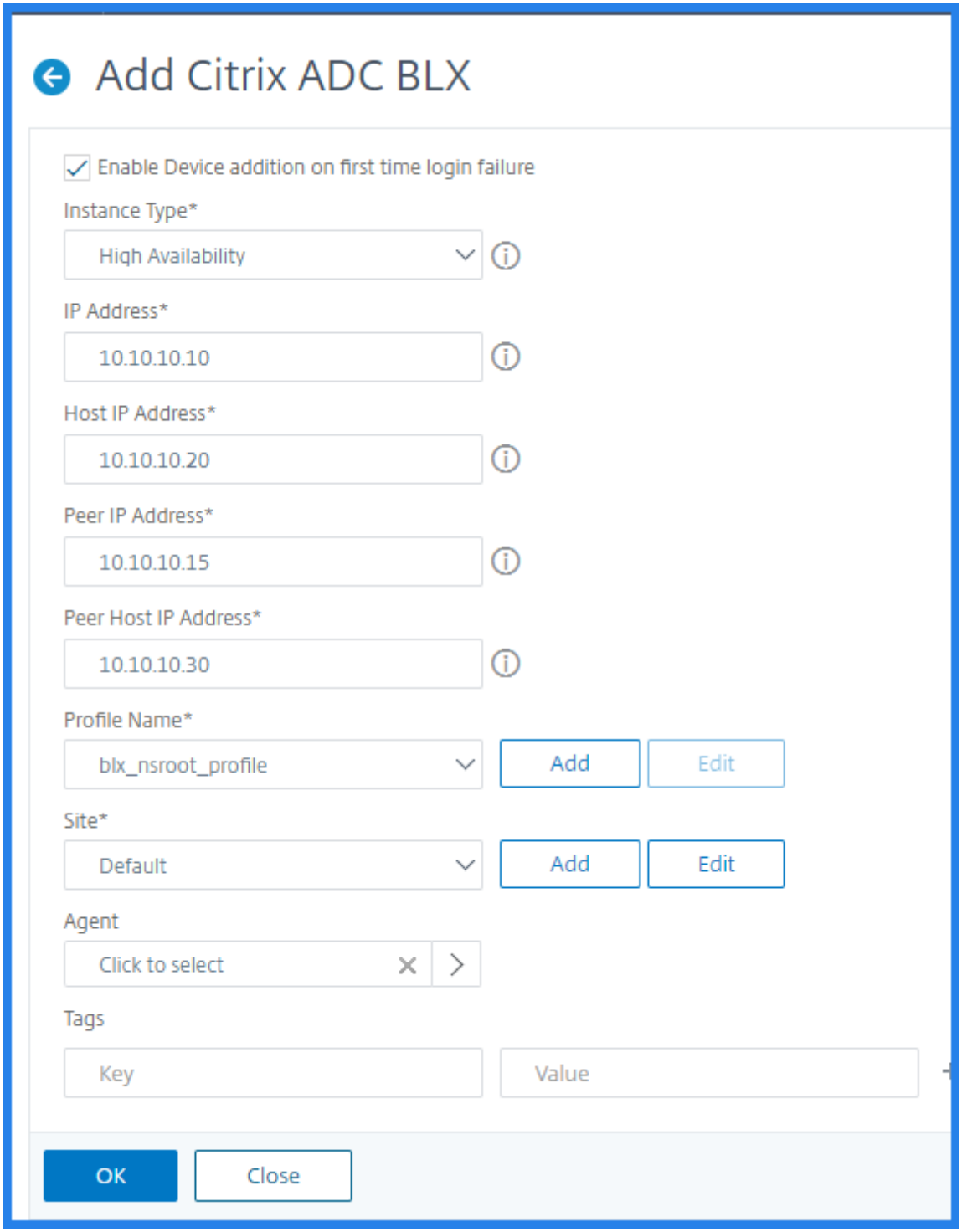
   Um ein Profil zu erstellen, klicken Sie auf **Hinzufügen**.

   > **Wichtig**
   >
   > Stellen Sie sicher, dass Sie den richtigen Hostbenutzernamen und das korrekte Kennwort des Linux-Servers im Profil angegeben haben.

9. Wählen Sie in der Liste **Site** die Site aus, an der Sie eine Instanz hinzufügen möchten.

   Wenn Sie eine Website hinzufügen möchten, klicken Sie auf **Hinzufügen**.
10. Wählen Sie in der Liste **Agent** den Citrix ADM Agent aus, dem Sie die Instanz zuordnen möchten.

    Wenn auf Ihrem Citrix ADM nur ein Agent konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.
11. Klicken Sie auf **OK**.

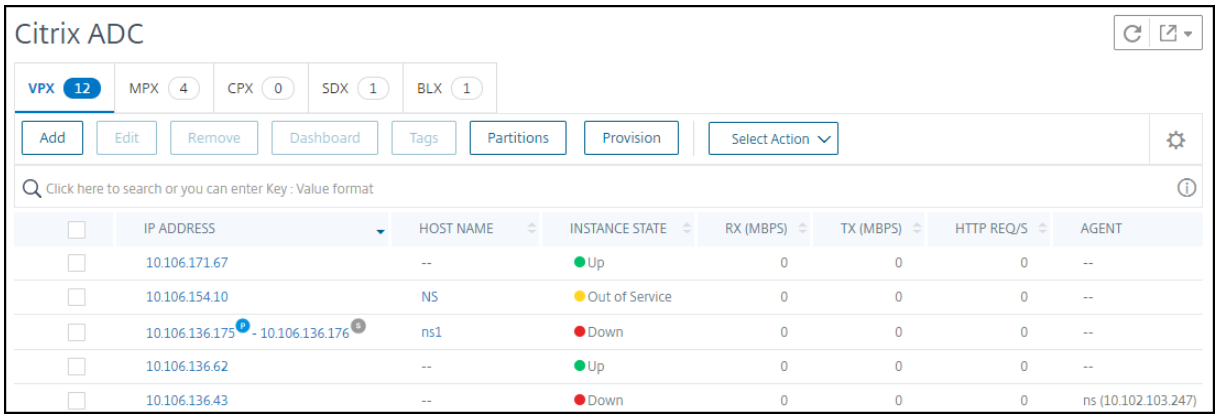


So greifen Sie über das Citrix ADM auf eine Instanz-GUI zu

1. Navigieren Sie zu **Netzwerke > Instanzen** > **Citrix ADC**.
2. Wählen Sie den Instanztyp aus, auf den Sie zugreifen möchten (z. B. VPX, MPX, CPX, SDX oder

BLX).

3. Klicken Sie auf die erforderliche Citrix ADC IP-Adresse oder den Hostnamen.



Die GUI der ausgewählten Instanz wird in einem Popup-Fenster angezeigt.

Lösen Sie Instanzwarnungen

Ein Warnzeichen wird aus folgenden Gründen auf der Instanz angezeigt:

- **Anmeldung fehlgeschlagen** - Wenn Sie eine Instanz ohne gültige Anmeldeinformationen hinzufügen, wird sie im Status DOWN mit einer Warnung bei Anmeldung fehlgeschlagen angezeigt. Geben Sie die richtigen Anmeldeinformationen für die Verwaltung der Instanz in ADM an.

  Wenn die Instanz nicht lizenziert ist, wird die Option **Lizenz** angezeigt, wenn Sie die Instanz auswählen. Klicken Sie auf **Lizenz**, um die Lizenz auf eine Instanz aus dem Lizenzpool anzuwenden.

- **Nicht lizenzierte Instanz mit HTTPS-Profil** - Wenn eine nicht lizenzierte Instanz nur eine HTTPS-Verbindung verwendet, wenden Sie die Lizenz auf eine Instanz über die ADC-GUI an.

Hinzufügen von HAProxy-Instanzen

April 28, 2021

Sie können eine auf einem Host bereitgestellte HAProxy-Instanz hinzufügen, indem Sie die Details des Hosts angeben, während Sie das Citrix Application Delivery Management (Citrix ADM) für den zum ersten Mal oder höher einrichten.

Citrix ADM unterstützt HAProxy Version 1.6.3 oder höher, und Sie können auf den folgenden Hosts bereitgestellte HAProxy-Instanzen zu Citrix ADM hinzufügen:

- Ubuntu 14.0 oder höher

- Red Hat Enterprise Linux (RHEL) 6.0 oder höher
- SUSE 11.0 oder höher
- CentOS 6.0 oder höher
- Amazon Linux AMI

> **Hinweis**
>
> Stellen Sie sicher, dass der Host nicht mit einer benutzerdefinierten Eingabeaufforderungszeichenfolge für die Shell konfiguriert ist. Die Shell muss entweder **$** oder **#** als Eingabeaufforderungszeichenfolge haben.

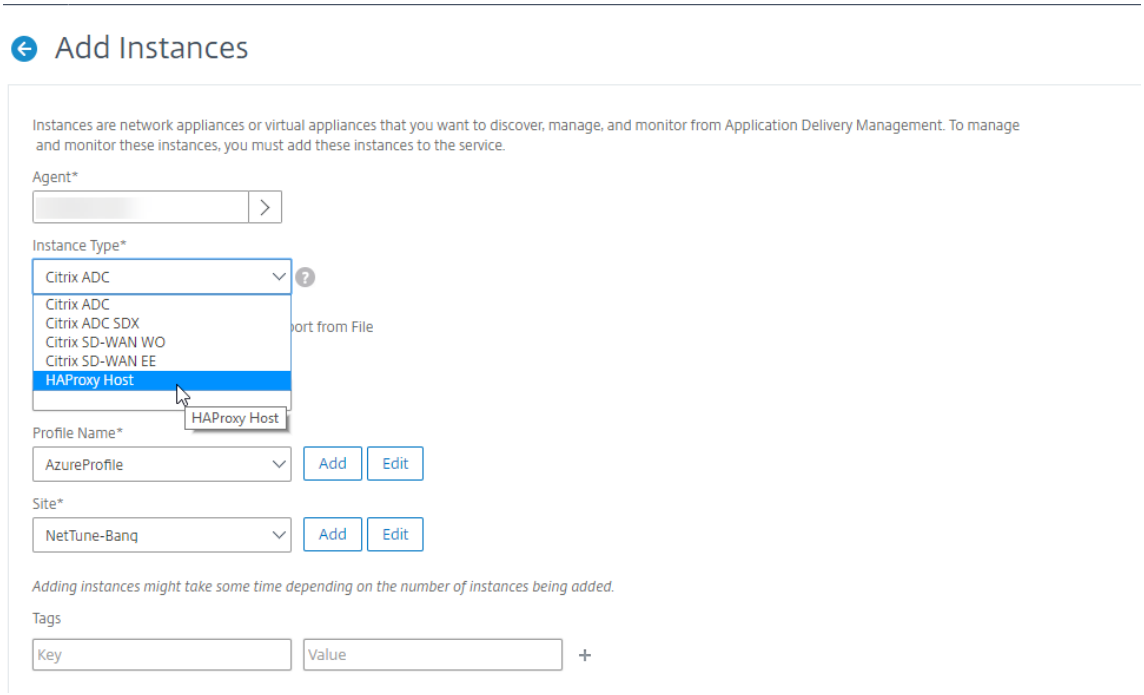
Um HAProxy-Instanzen hinzuzufügen, müssen Sie die IP-Adresse des Hosts angeben, auf dem Sie die HAProxy-Instanzen bereitgestellt haben. Anschließend müssen Sie ein HAProxy-Profil angeben, das Citrix ADM für den Zugriff auf den Host verwenden kann. Dieses HAProxy-Profil enthält den Benutzernamen und das Kennwort des Hosts, den Sie dem Dienst hinzufügen möchten.

> **Hinweis**
> **Stellen Sie**sicher, dass das Benutzerkonto, das dem Benutzernamen zugeordnet ist, Folgendes hat:
>
> - Berechtigungen zum Ausführen des Befehls ps, um alle HAProxy-Instanzen auf dem Host aufzulisten.
> - Berechtigung zum Neustart der HAProxy-Instanz auf dem Host.

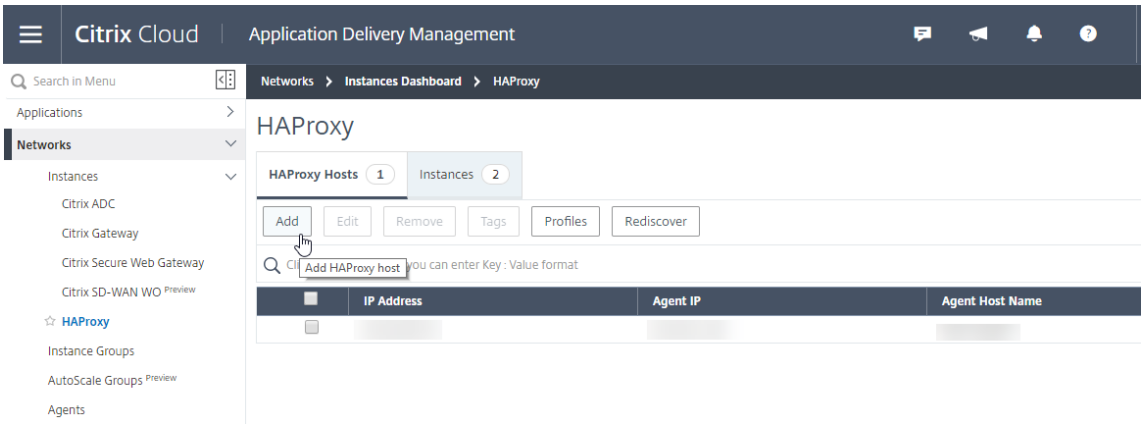
Nachdem Sie Citrix ADM den Host hinzugefügt haben, auf dem Sie die HAProxy-Instanzen bereitgestellt haben, greift Citrix ADM mithilfe des SSH-Protokolls auf den Host zu. Es erkennt automatisch die auf dem Host bereitgestellten HAProxy-Instanzen und fügt sie der Citrix ADM Bestandsliste hinzu. Es erkennt auch alle Frontends, Backends und Server, die auf den HAProxy-Instanzen konfiguriert sind, und behandelt die Frontends als erkannte Anwendungen.

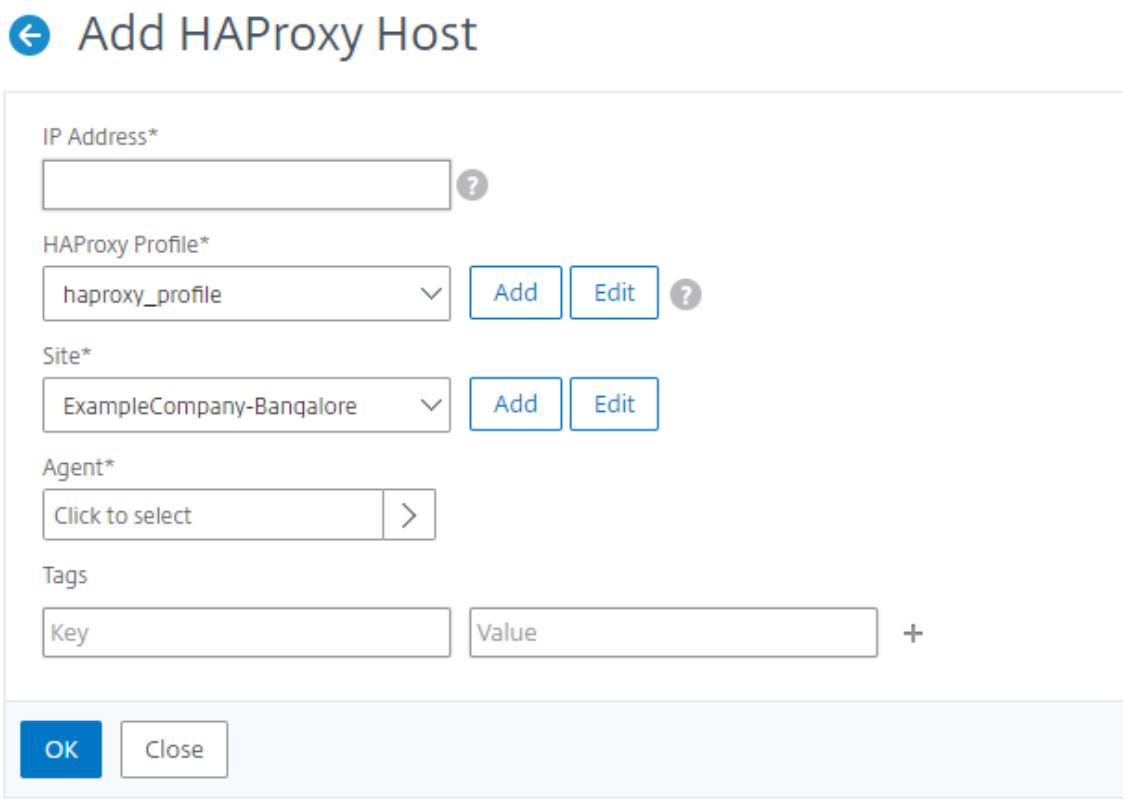
So fügen Sie Citrix ADM HAProxy-Instanzen hinzu:

1. Navigieren Sie zu **Netzwerke > Instanzen**, und klicken Sie auf Instanzen gesamt. Klicken Sie im Abschnitt Instanzen oben rechts auf der Seite auf **Hinzufügen**. Wählen Sie auf der Seite Instanzen hinzufügen aus der Dropdownliste **Instanztyp** die Option **HAProxy-Host** aus.



Alternativ können Sie zu **Netzwerke > Instanzen**navigieren. Wählen Sie unter Instanzen **HAProxy** aus, und klicken Sie auf **Hinzufügen**.





2. Geben Sie im Feld **IP-Adresse** die IP-Adresse des Hosts ein, auf dem Sie die HAProxy-Instanzen bereitgestellt haben.
3. Wählen Sie in der Dropdownliste **HAProxy-Profil** ein vorhandenes HAProxy-Profil aus oder erstellen Sie ein neues HAProxy-Profil. Um ein HAProxy-Profil zu erstellen, klicken Sie auf das Symbol **+**.
4. Gehen **Sie im Dialogfeld HAProxy-Profil hinzufügen** folgendermaßen vor:
   a) Geben Sie im Feld **Profilname** einen eindeutigen Namen für das HAProxy-Profil ein.
   b) Geben Sie im Feld **Benutzername** den Benutzernamen ein, der für den Zugriff auf den Host mithilfe des SSH-Protokolls verwendet wird.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass das mit dem Benutzernamen verknüpfte Benutzerkonto Folgendes hat:

```
1     - Berechtigungen zum Ausführen des Befehls ps, um
        alle HAProxy-Instanzen auf dem Host aufzulisten.
```

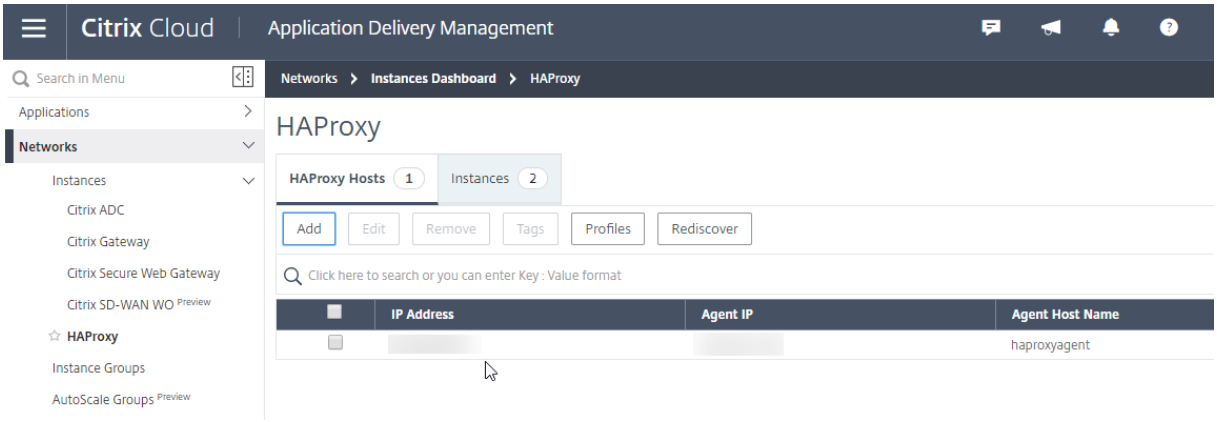

> • Berechtigung zum Neustart der HAProxy-Instanz auf dem Host.

c) Geben Sie im Feld **Kennwort** das Kennwort des Hosts ein.

d) Klicken Sie auf **Erstellen**.

5. Geben Sie eine Site für die Instanz an.
6. **Wählen Sie in der Dropdownliste Agent den Agenten aus, dem Sie die Instanzen zuordnen möchten.**
7. Geben Sie im Feld Tags einen Schlüssel und zugehörige Werte für die HAProxy-Instanz an. Tags helfen Ihnen, die Instanzen zu klassifizieren und zu identifizieren. Geben Sie beispielsweise Location als Schlüssel und Bangalore als Wert an. Sie können auch mehrere Werte für einen Schlüssel hinzufügen. Trennen Sie die Mehrfachwerte durch Kommas.
8. Wählen Sie **OK**.

Citrix ADM erkennt die auf dem Host bereitgestellten HAProxy-Instanzen, und Sie können alle HAProxy-Instanzen auf der Registerkarte **Instanzen** auf der Seite **Netzwerke > Instanzen > HAProxy** anzeigen.



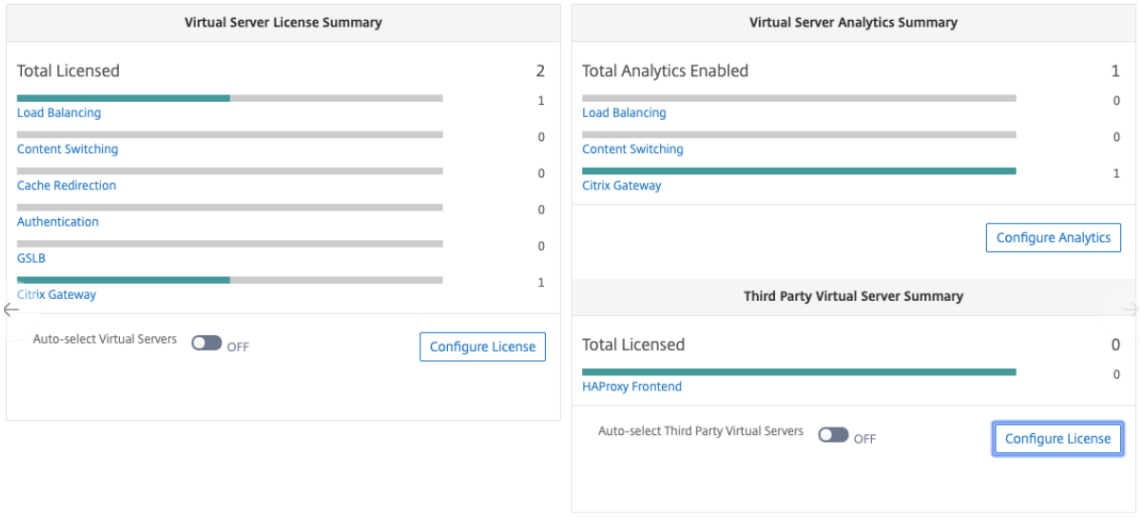
Verwalten der Lizenzierung und Aktivieren von Analysen auf virtuellen Servern

April 28, 2021

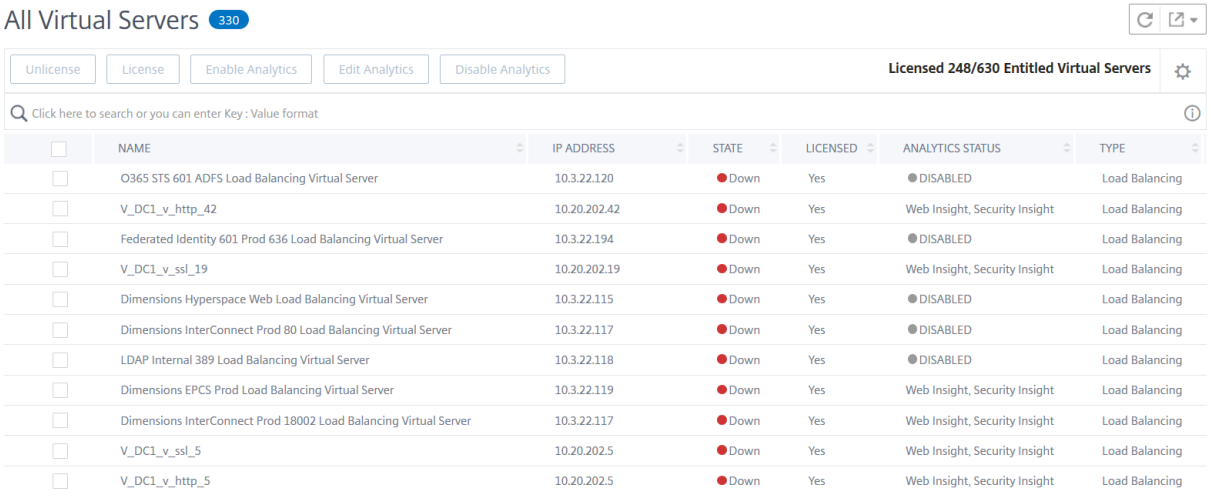
Der Prozess der Aktivierung von Analysen wird vereinfacht. Sie können jetzt den virtuellen Server lizenzieren und Analysen in einem einzigen Workflow aktivieren.

Navigieren Sie zu **Konto** > **Abonnements** zu:

- Übersicht über **virtuelle Server-Lizenzen anzeigen**
- Übersicht über **Virtual Server Analytics anzeigen**



Wenn Sie auf **Lizenz konfigurieren** oder **Analytics konfigurieren**klicken, wird die Seite **Alle virtuellen Server**angezeigt.



Auf der Seite **Alle virtuellen Server** können Sie:

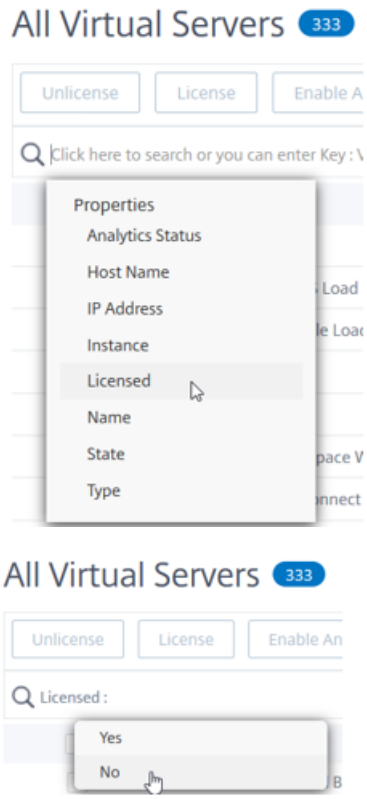
- Lizenz für nicht lizenzierte virtuelle Server anwenden
- Lizenz für lizenzierte virtuelle Server entfernen
- Analytics auf lizenzierten virtuellen Servern aktivieren
- Analytics bearbeiten
- Analytics deaktivieren

> **Hinweis**
>
> Die unterstützten virtuellen Server zur Aktivierung von Analysen sind Load Balancing, Content Switching und Citrix Gateway.

Verwalten der Lizenzierung auf virtuellen Servern

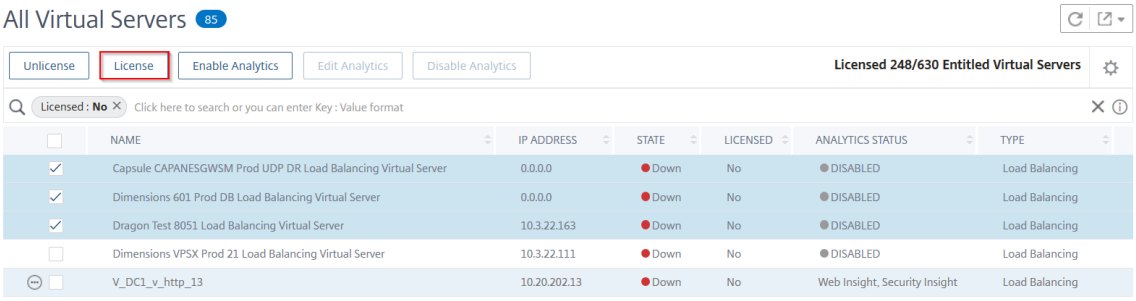
So lizenzieren Sie die virtuellen Server auf der Seite **Alle virtuellen Server**:

1. Klicken Sie auf die Suchleiste, wählen Sie **Lizenziert**und wählen Sie **Nein**aus.



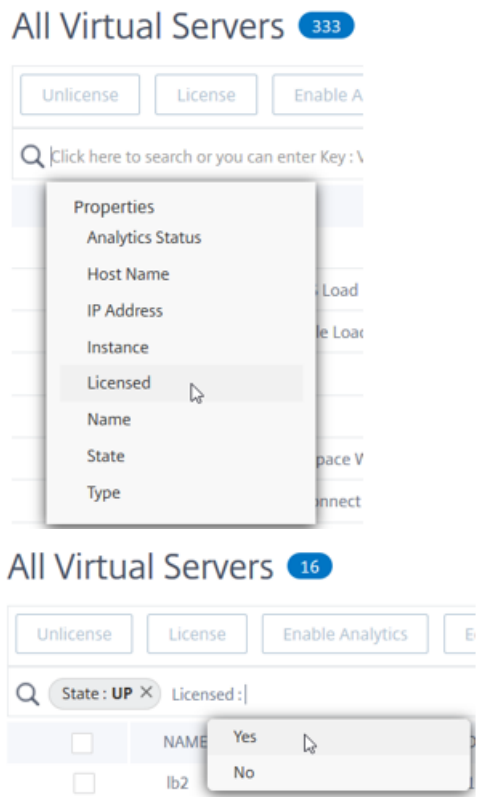
   Der Filter wird nun angewendet und nur die nicht lizenzierten virtuellen Server werden angezeigt.

2. Wählen Sie die virtuellen Server aus, und klicken Sie dann auf **Lizenz**.

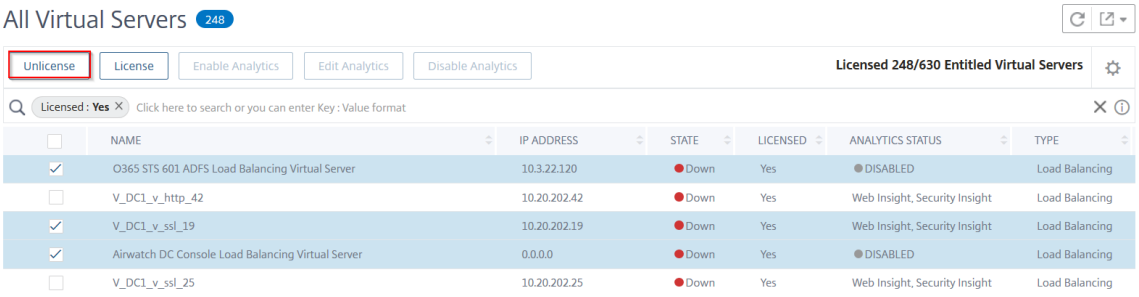


So heben Sie die Lizenzierung der virtuellen Server auf der Seite **Alle virtuellen Server** auf:

1. Klicken Sie auf die Suchleiste, wählen Sie **Lizenziert**und wählen Sie **Ja**aus.



2. Wählen Sie die virtuellen Server aus, und klicken Sie auf **Lizenz aufheben**.



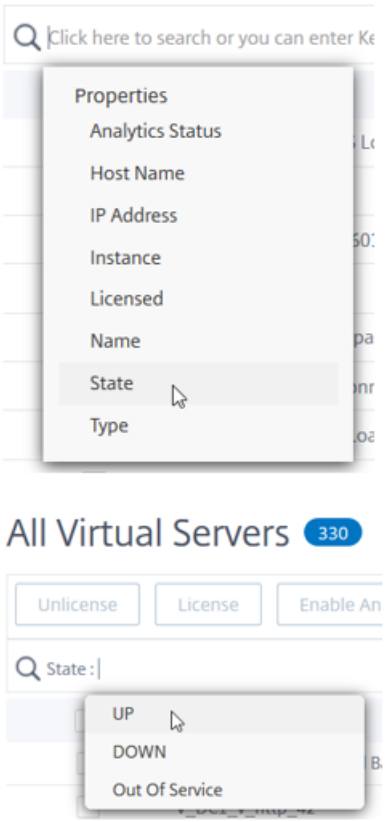
Analytics aktivieren

Folgende Voraussetzungen sind für die Aktivierung von Analysen für virtuelle Server:

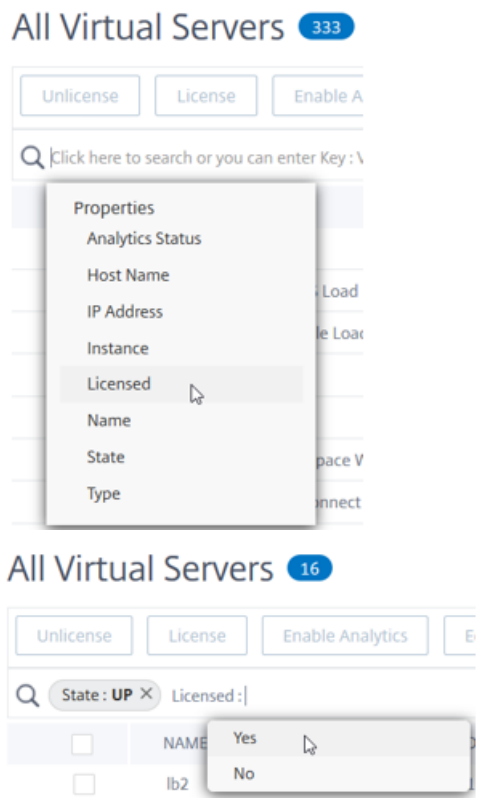
- Sicherstellen, dass virtuelle Server **lizenziert** sind
- Stellen Sie sicher, dass der Analytics-Status **deaktiviert** ist
- Stellen Sie sicher, dass virtuelle Server im Status **UP** sind

Sie können die Ergebnisse filtern, um die virtuellen Server zu identifizieren, die in den Voraussetzungen erwähnt werden.

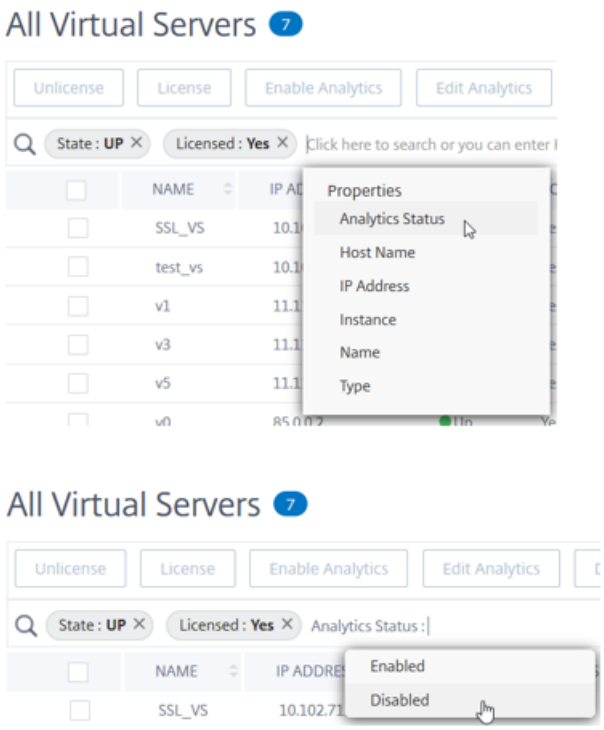
1. Klicken Sie auf die Suchleiste, wählen Sie **Status** und dann **UP** aus.



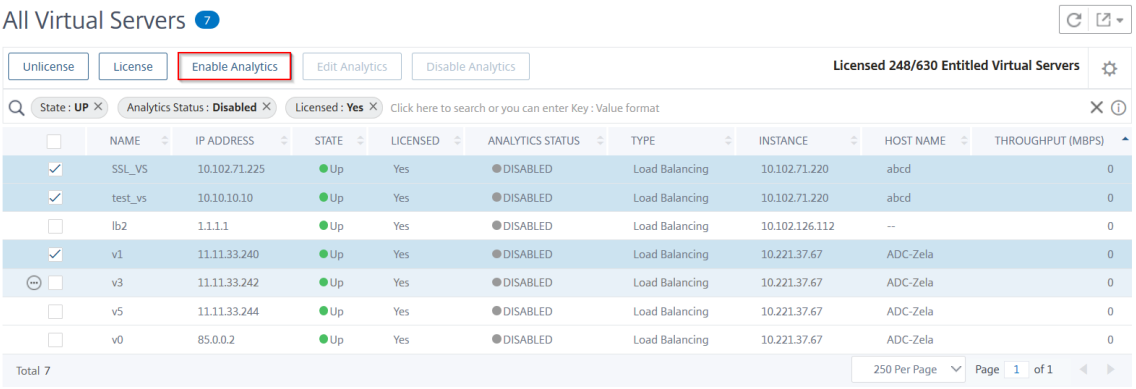
2. Klicken Sie auf die Suchleiste, wählen Sie **Lizenziert** aus, und wählen Sie dann **Ja** aus.



3. Klicken Sie auf die Suchleiste, wählen Sie **Analytics-Status** aus, und wählen Sie dann **Deaktiviert** aus.



4. Wählen Sie nach dem Anwenden der Filter die virtuellen Server aus, und klicken Sie dann auf **Analytics aktivieren**.



5. Im Fenster **Analytics aktivieren**:

   a) Auswählen der Einsichtstypen (Web Insight oder Security Insight)

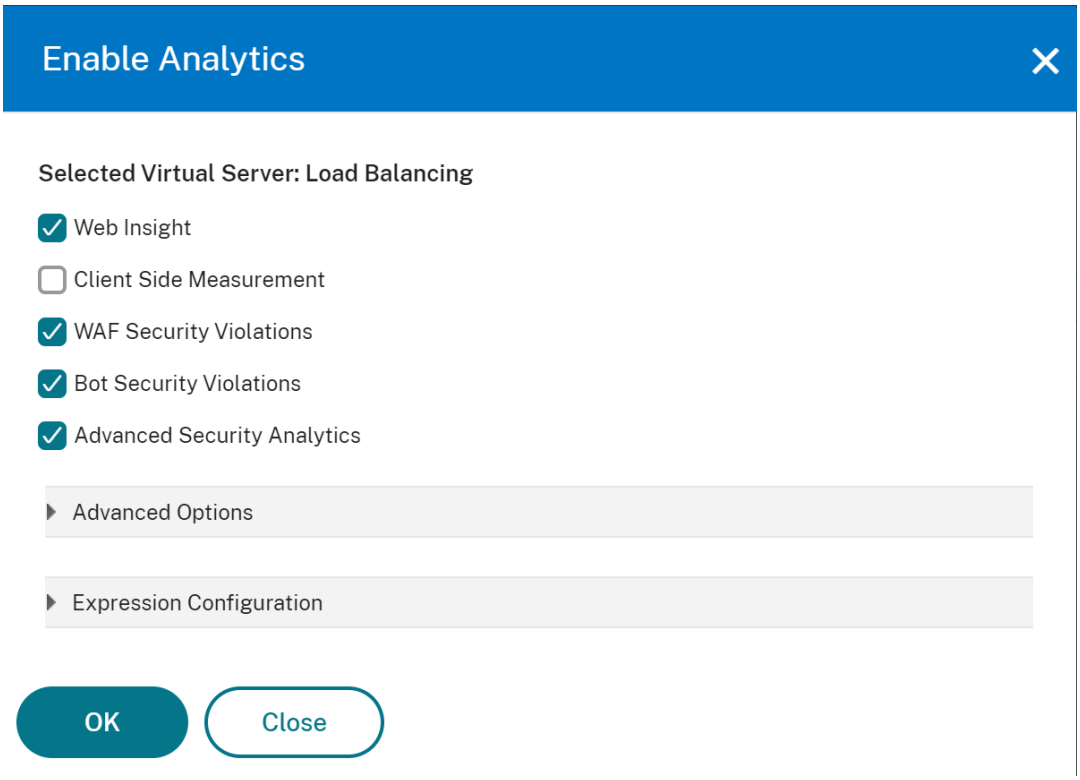
   b) Wählen Sie **Logstream** oder **IPFIX** als Transportmodus

> **Hinweis**
>
> Für Citrix ADC 12.0 oder früher ist **IPFIX** die Standardoption für den Transportmodus. Für Citrix ADC 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Trans-

> portmodus auswählen.
>
> Weitere Informationen zu **IPFIX** und **Logstream** finden Sie unter **Übersicht über den Logstream**.

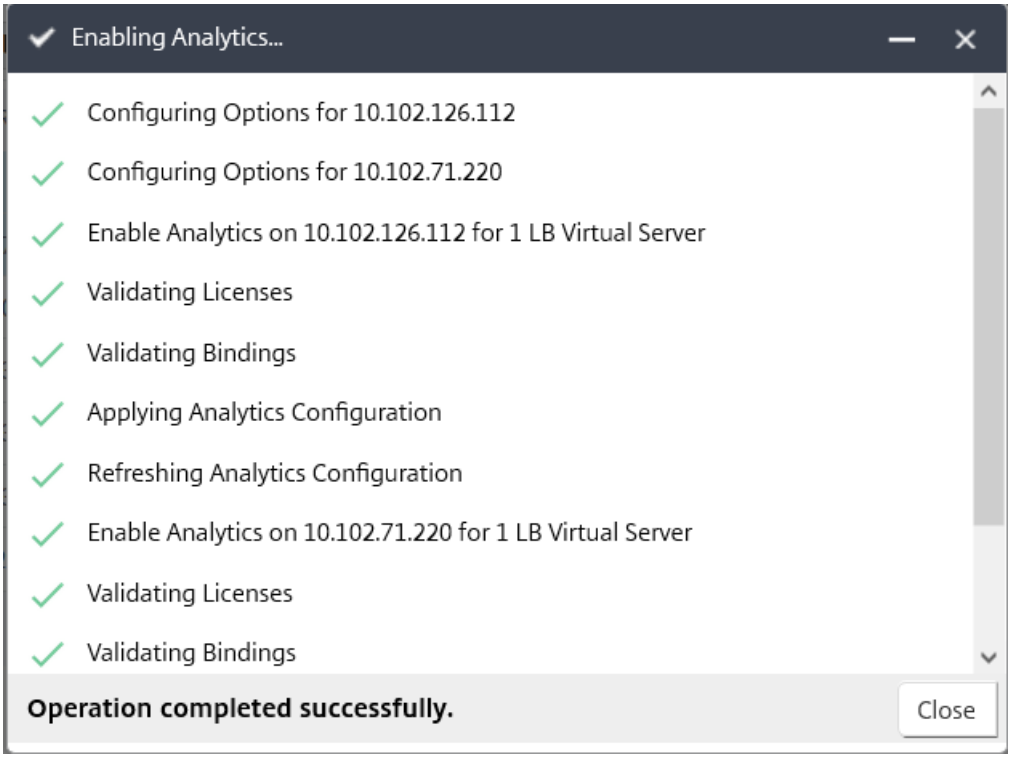
c) Der Ausdruck ist standardmäßig true

d) Klicken Sie auf **OK**



> **Hinweis**
>
> ```
> - Wenn Sie virtuelle Server auswählen, die nicht lizenziert sind, lizenziert Citrix ADM zuerst diese virtuellen Server und aktiviert dann Analysen.
>
> - Für Administratorpartitionen wird nur **Web Insight ** unterstützt
> ```
>
> - Für virtuelle Server wie **Cache-Umleitung**, **Authentifizierung**und **GSLB**können Sie keine Analysen aktivieren. Es wird eine Fehlermeldung angezeigt.

Nachdem Sie auf **OK** geklickt haben, verarbeitet Citrix ADM Analysen auf den ausgewählten virtuellen Servern zu aktivieren.

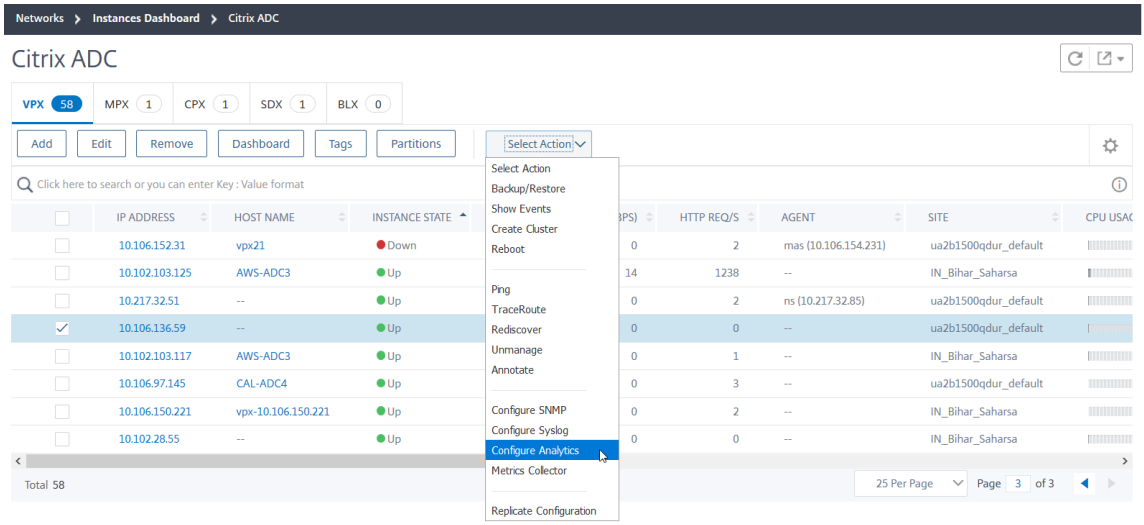


> **Hinweis**
>
> Citrix ADM verwendet Citrix ADC SNIP für **Logstream** und NSIP für **IPFIX**. Wenn zwischen Citrix ADM-Agent und Citrix ADC-Instanz eine Firewall aktiviert ist, stellen Sie sicher, dass Sie den folgenden Port öffnen, damit Citrix ADM Agent AppFlow Datenverkehr erfassen kann:
>
> | Transportmodus | Quell-IP | Typ | Port|
> |—|
> —|—|—| | **IPFIX** | NSIP | UDP |
> **4739**| | SNIP | TCP | 5557|

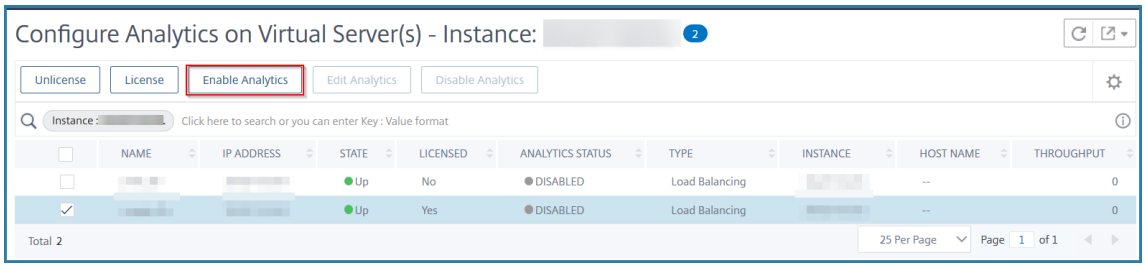
Analytics für eine Instanz aktivieren

Alternativ können Sie auch Analysen für eine bestimmte Instanz aktivieren:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC** und wählen Sie dann den Instanz-Typ aus. Zum Beispiel VPX.
2. Wählen Sie die Instanz aus, und wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.



3. Wählen Sie auf der Seite **Analytics auf virtuellen Servern konfigurieren** den virtuellen Server aus, und klicken Sie auf **Analytics aktivieren**.



4. Im Fenster **Analytics aktivieren**:

   a) Wählen Sie den Einsichtstyp aus (Web Insight, Security Insight, Bot Insight)

   b) Wählen Sie **Logstream** oder **IPFIX** als Transportmodus

   > **Hinweis**
   >
   > Für Citrix ADC 12.0 oder früher ist **IPFIX** die Standardoption für den Transportmodus. Für Citrix ADC 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.
   >
   > Weitere Informationen zu **IPFIX** und **Logstream** finden Sie unter **Übersicht über den Logstream**.

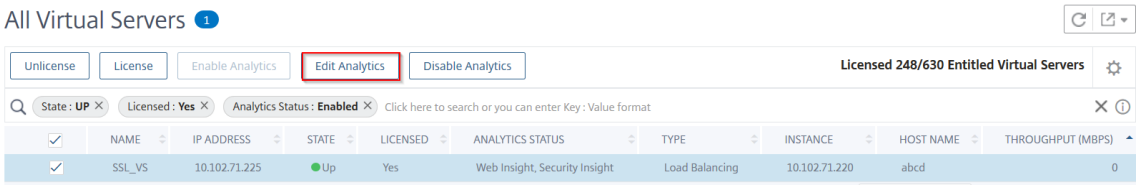
   c) Der Ausdruck ist standardmäßig true

   d) Klicken Sie auf **OK**

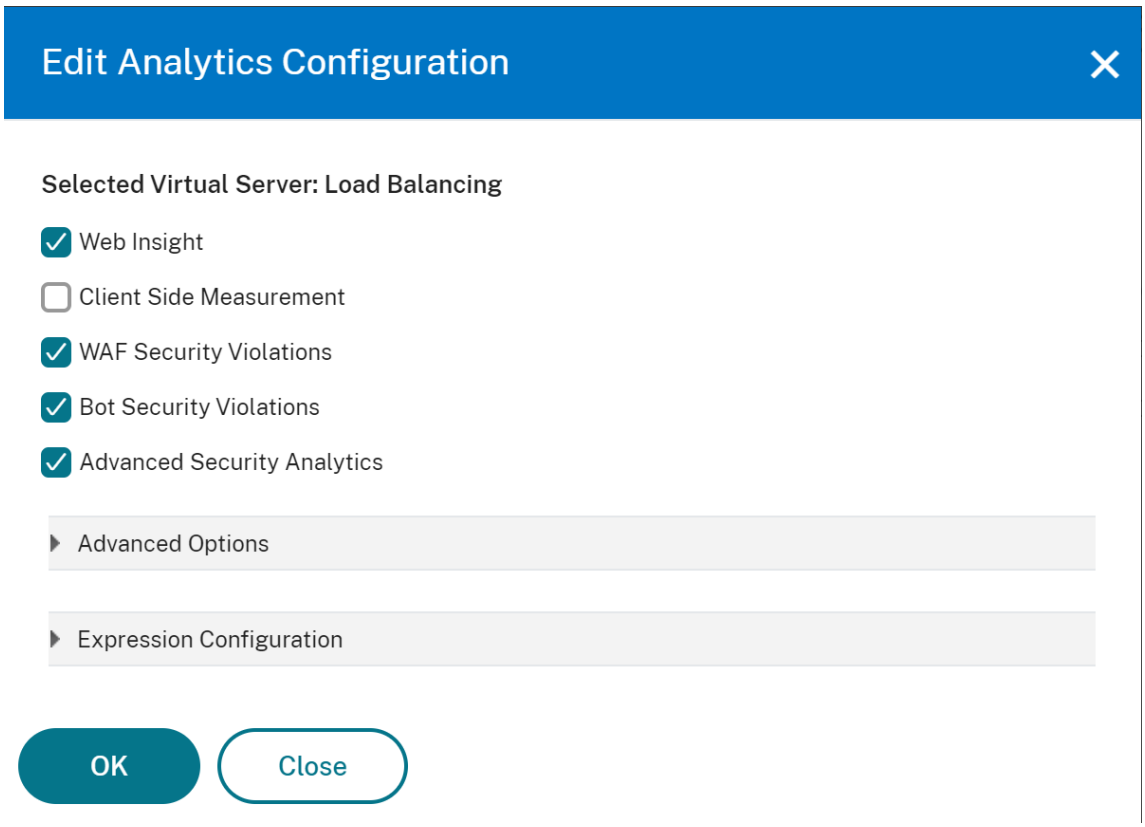
Analytics bearbeiten

So bearbeiten Sie Analysen auf den virtuellen Servern:

1. Wählen Sie die virtuellen Server aus
2. Klicken Sie auf **Analytics bearbeiten**



3. Bearbeiten Sie die Parameter, die Sie im Fenster **Analytics-Konfiguration bearbeiten** anwenden möchten
4. Klicken Sie auf **OK**.



Bearbeiten von Analysen für eine Instanz

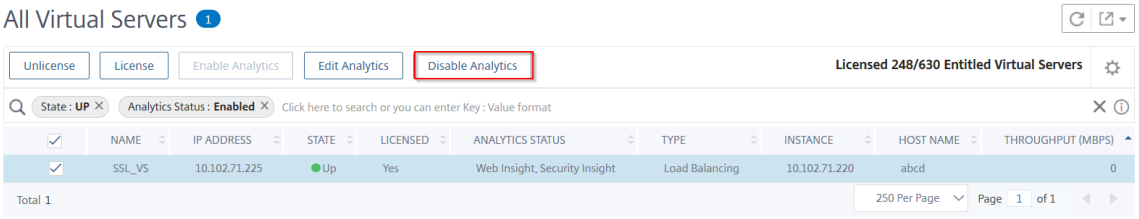
Alternativ können Sie Analysen auch für eine bestimmte Instanz deaktivieren:

1. Navigieren Sie zu **Netzwerk > Instanz > Citrix ADC**, und wählen Sie den Instanztyp aus. Zum Beispiel VPX.
2. Wählen Sie die Instanz aus, und klicken Sie auf **Analytics bearbeiten**

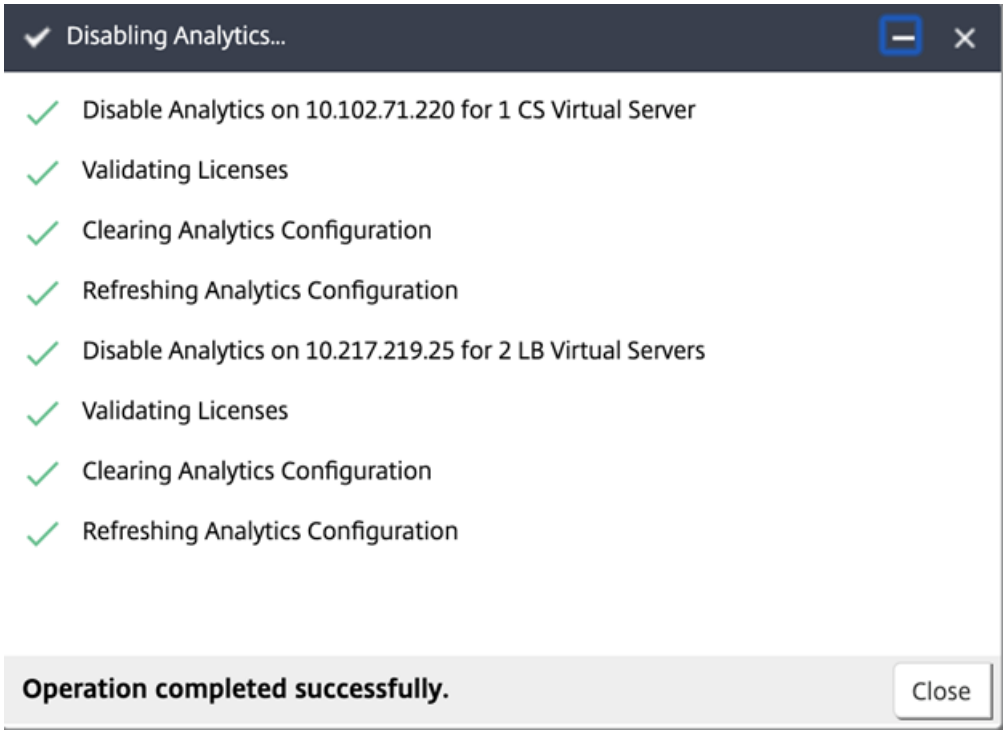
Analytics deaktivieren

So deaktivieren Sie die Analyse auf den ausgewählten virtuellen Servern:

1. Wählen Sie die virtuellen Server aus
2. Klicken Sie auf **Analytics deaktivieren**



Citrix ADM deaktiviert die Analyse auf den ausgewählten virtuellen Servern



Konfigurieren von Syslog für Instanzen

April 28, 2021

Das Syslog-Protokoll stellt einen Transport bereit, mit dem die Citrix ADC-Instanzen Ereignisbenachrichtigungsmeldungen an Citrix Application Delivery Management (Citrix ADM) senden können, das als Collector oder Syslog-Server für diese Nachrichten konfiguriert ist.

Sie können die Syslog-Ereignisse überwachen, die auf Ihren Citrix ADC-Instanzen generiert werden, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Nachrichten an Citrix ADM umgeleitet werden. Um Syslog-Ereignisse zu überwachen, müssen Sie zuerst Citrix ADM als Syslog-Server für Ihre Citrix ADC-Instanz konfigurieren. Nach der Konfiguration der Instanz werden alle Syslog-Nachrichten an Citrix ADM umgeleitet, sodass diese Protokolle dem Benutzer strukturiert angezeigt werden können.

Syslog verwendet das User Datagram Protocol (UDP), Port 514, für die Kommunikation, und da UDP ein verbindungsloses Protokoll ist, stellt es keine Bestätigung zurück zu den Instanzen bereit. Die Syslog-Paketgröße ist auf 1024 Byte begrenzt und enthält folgende Informationen:

- Raum
- Schweregrad
- Hostname
- Zeitstempel
- Meldung

In Citrix ADM müssen Sie den Schweregrad der Einrichtung und des Protokolls für die Instanzen konfigurieren.

- **Facility** - Syslog-Nachrichten werden auf der Grundlage der Quellen, die sie generieren, breit kategorisiert. Diese Quellen können das Betriebssystem, der Prozess oder eine Anwendung sein. Diese Kategorien werden Einrichtungen genannt und werden durch ganze Zahlen dargestellt. Beispielsweise wird 0 von Kernelmeldungen verwendet, 1 wird von Nachrichten auf Benutzerebene verwendet, 2 wird vom Mailsystem verwendet usw. Die lokalen Nutzungsmöglichkeiten (von local0 bis local7) sind nicht reserviert und stehen zur allgemeinen Nutzung zur Verfügung. Daher können die Prozesse und Anwendungen, die keine vorab zugewiesenen Anlagenwerte haben, an eine der acht lokalen Nutzungseinrichtungen gerichtet werden.
- **Schweregrad** - Die Quelle oder Einrichtung, die die Syslog-Nachricht generiert, gibt auch den Schweregrad der Nachricht mit einer einstelligen Ganzzahl an, wie unten dargestellt:

```
1 - Notfall: System ist unbrauchbar.

2 - Warnung: Maßnahmen müssen sofort ergriffen werden.

3 - Kritisch: Kritische Bedingungen.

4 - Fehler: Fehlerbedingungen.

5 - Warnung: Warnbedingungen.

```



```
6 - Hinweis: Normaler, aber signifikanter Zustand.

7 - Informativ: Informationsbotschaften.

8 - Debug: Meldungen auf Debug-Ebene.
```

So konfigurieren Sie Syslog auf Citrix ADC-Instanzen:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen**.
2. Wählen Sie die Citrix ADC-Instanz aus, aus der die Syslog-Nachrichten gesammelt und in Citrix ADM angezeigt werden sollen.
3. Wählen Sie in der Dropdownliste **Aktion** die Option **Syslog konfigurieren** aus.
4. Klicken Sie auf **Aktivieren**.
5. Wählen Sie in der Dropdownliste **Einrichtung** eine lokale Einrichtung oder auf Benutzerebene aus.
6. Wählen Sie die erforderliche Protokollstufe für die Syslog-Meldungen aus.
7. Klicken Sie auf **OK**.

Dadurch werden alle Syslog-Befehle in der Citrix ADC-Instanz konfiguriert, und Citrix ADM beginnt, die Syslog-Nachrichten zu empfangen. Sie können die Nachrichten anzeigen, indem Sie zu “ **Netzwerke** “ > “ **Ereignisse** “ > “ **Syslog-Nachrichten**” navigieren.

Konfigurieren der rollenbasierten Zugriffssteuerung

April 28, 2021

Citrix Application Delivery Management (Citrix ADM) bietet eine fein abgestimmte, rollenbasierte Zugriffssteuerung (RBAC), mit der Sie Zugriffsberechtigungen basierend auf den Rollen einzelner Benutzer in Ihrem Unternehmen erteilen können.

In Citrix ADM werden alle Benutzer in Citrix Cloud hinzugefügt. Als erster Benutzer Ihrer Organisation müssen Sie zunächst ein Konto in Citrix Cloud erstellen und sich dann mit den Citrix Cloud-Anmeldeinformationen an der Citrix ADM GUI anmelden. Sie erhalten die Superadministratorrolle, und standardmäßig verfügen Sie über alle Zugriffsberechtigungen in Citrix ADM. Später können Sie weitere Benutzer in Ihrer Organisation in Citrix Cloud erstellen.

Benutzer, die später erstellt werden und sich als reguläre Benutzer bei Citrix ADM anmelden, werden als delegierte Administratoren bezeichnet. Diese Benutzer verfügen standardmäßig über alle Berechtigungen mit Ausnahme der Benutzerverwaltungsberechtigungen. Sie können diesen delegierten Administratorbenutzern jedoch bestimmte Benutzerverwaltungsberechtigungen erteilen. Sie können dies tun, indem Sie entsprechende Richtlinien erstellen und diese diesen delegierten Benutzern

zuweisen. Die Benutzerverwaltungsberechtigungen befinden sich unter **Konto** > **Benutzerverwaltung**. Weitere Informationen zum Zuweisen bestimmter Berechtigungen finden Sie unterZuweisen zusätzlicher Berechtigungen für delegierte Administratorbenutzer.

Weitere Informationen zum Erstellen von Richtlinien, Rollen, Gruppen und zum Binden der Benutzer an Gruppen finden Sie in den folgenden Abschnitten.

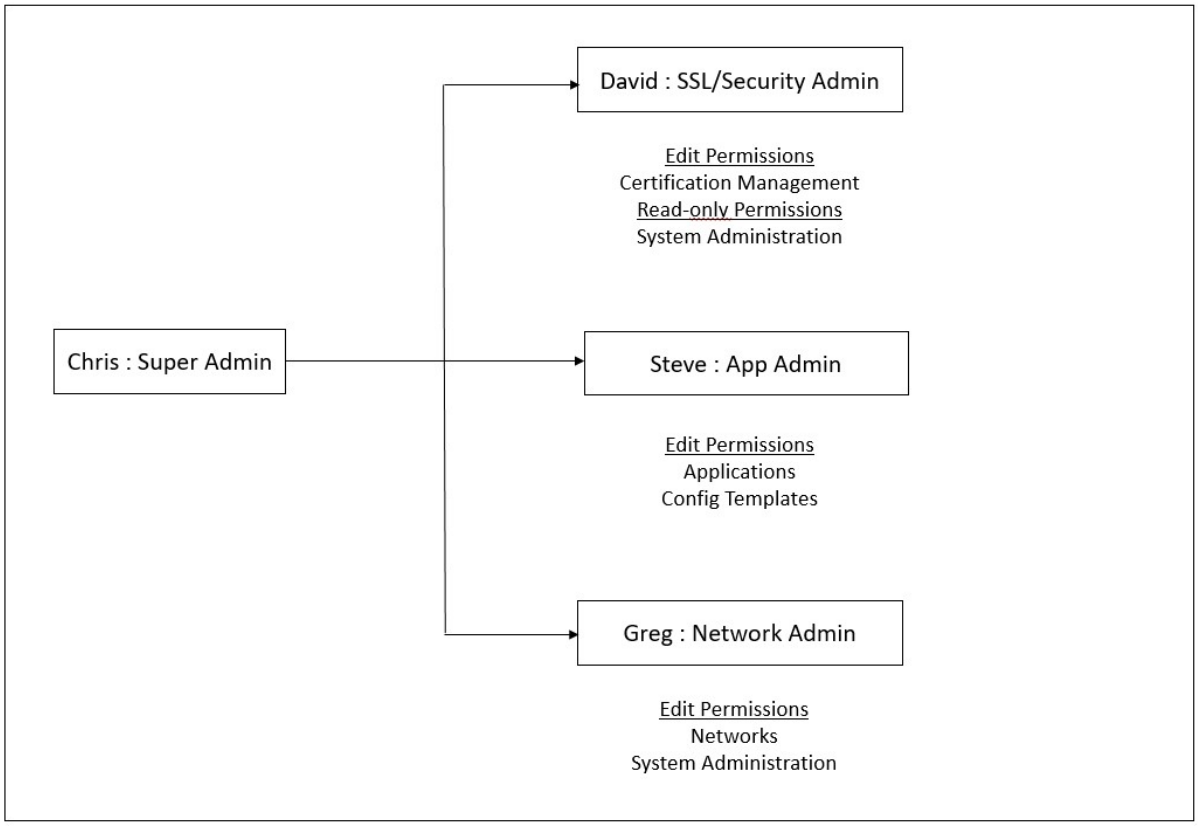
Beispiel:

Das folgende Beispiel veranschaulicht, wie RBAC in Citrix ADM erreicht werden kann.

Chris, der Leiter der ADC-Gruppe, ist der Superadministrator von Citrix ADM in seiner Organisation. Er erstellt drei Administratorrollen: Sicherheitsadministrator, Anwendungsadministrator und Netzwerkadministrator.

- David, der Sicherheitsadministrator, muss über vollständigen Zugriff auf die Verwaltung und Überwachung von SSL-Zertifikaten verfügen, muss jedoch über schreibgeschützten Zugriff für den Systemverwaltungsbetrieb verfügen.
- Steve, ein Anwendungsadministrator, benötigt nur Zugriff auf bestimmte Anwendungen und nur bestimmte Konfigurationsvorlagen.
- Greg, ein Netzwerkadministrator, benötigt Zugriff auf System- und Netzwerkadministration.
- Chris muss auch RBAC für alle Benutzer bereitstellen, unabhängig davon, dass sie lokal oder extern sind.

Das folgende Bild zeigt die Berechtigungen, die Administratoren und andere Benutzer haben und ihre Rollen in der Organisation.



Um seinen Benutzern eine rollenbasierte Zugriffssteuerung bereitzustellen, muss Chris zuerst Benutzer in Citrix Cloud hinzufügen und erst danach können die Benutzer in Citrix ADM angezeigt werden. Chris muss je nach Rolle Zugriffsrichtlinien für jeden Benutzer erstellen. Zugriffsrichtlinien sind eng an Rollen gebunden. Chris muss also auch Rollen erstellen, und dann muss er Gruppen erstellen, da Rollen nur Gruppen zugewiesen werden können und nicht einzelnen Benutzern.

Access ist die Möglichkeit, eine bestimmte Aufgabe auszuführen, wie zum Beispiel Anzeigen, Erstellen, Ändern oder Löschen einer Datei. Rollen werden entsprechend der Autorität und Verantwortung der Benutzer innerhalb des Unternehmens definiert. Beispielsweise kann ein Benutzer alle Netzwerkvorgänge ausführen, während ein anderer Benutzer den Verkehrsfluss in Anwendungen beobachten und beim Erstellen von Konfigurationsvorlagen helfen kann.

Rollen werden durch Richtlinien bestimmt. Nach dem Erstellen von Richtlinien können Sie Rollen erstellen, jede Rolle an eine oder mehrere Richtlinien binden und Benutzern Rollen zuweisen. Sie können auch Benutzergruppen Rollen zuweisen. Eine Gruppe ist eine Sammlung von Benutzern, die gemeinsam über Berechtigungen verfügen. Beispielsweise können Benutzer, die ein bestimmtes Rechenzentrum verwalten, einer Gruppe zugewiesen werden. Eine Rolle ist eine Identität, die Benutzern gewährt wird, indem sie basierend auf bestimmten Bedingungen zu bestimmten Gruppen hinzugefügt werden. In Citrix ADM sind die Erstellung von Rollen und Richtlinien spezifisch für das RBAC-Feature in Citrix ADC. Rollen und Richtlinien können einfach erstellt, geändert oder eingestellt werden, wenn sich die Anforderungen des Unternehmens entwickeln, ohne dass die Berechtigungen

für jeden Benutzer individuell aktualisiert werden müssen.

Rollen können Feature- oder ressourcenbasiert sein. Betrachten Sie beispielsweise einen SSL/Sicherheitsadministrator und einen Anwendungsadministrator. Ein SSL/Security-Administrator muss über vollständigen Zugriff auf die Verwaltungs- und Überwachungsfunktionen von SSL-Zertifikaten verfügen, muss jedoch über schreibgeschützten Zugriff für Systemadministrationsvorgänge verfügen. Anwendungsadministratoren können nur auf die Ressourcen in ihrem Geltungsbereich zugreifen.

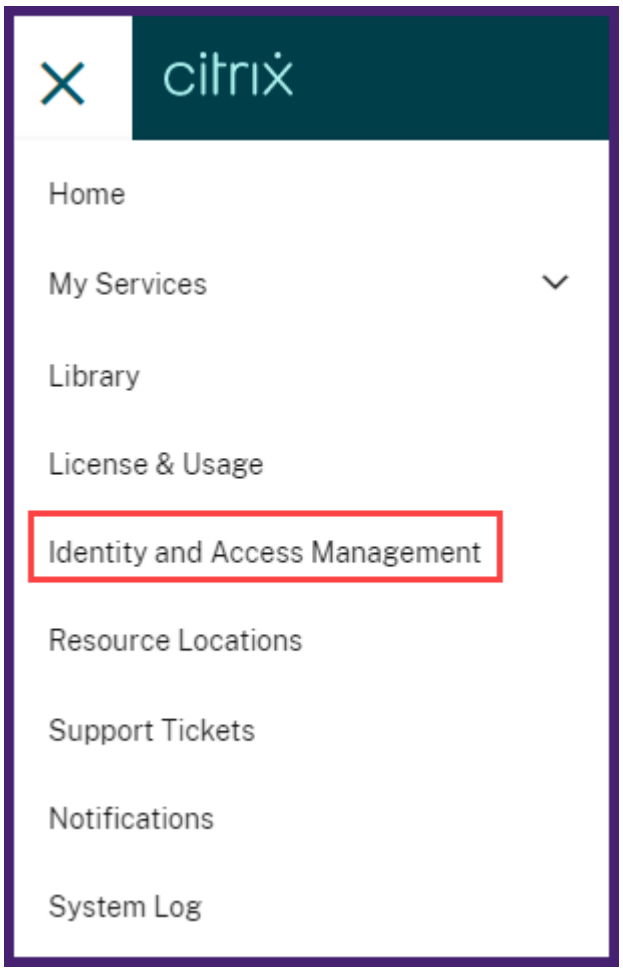
Führen Sie daher in Ihrer Rolle als Superadministrator Chris die folgenden Beispielaufgaben in Citrix ADM aus, um Zugriffsrichtlinien, Rollen und Benutzergruppen für David zu konfigurieren, der der Sicherheitsadministrator in Ihrer Organisation ist.

Konfigurieren von Benutzern auf Citrix ADM

Als Superadministrator können Sie mehr Benutzer erstellen, indem Sie Konten für sie in Citrix Cloud und nicht in Citrix ADM konfigurieren. Wenn die neuen Benutzer Citrix ADM hinzugefügt werden, können Sie ihre Berechtigungen nur definieren, indem Sie dem Benutzer die entsprechenden Gruppen zuweisen.

So fügen Sie neue Benutzer in Citrix Cloud hinzu:

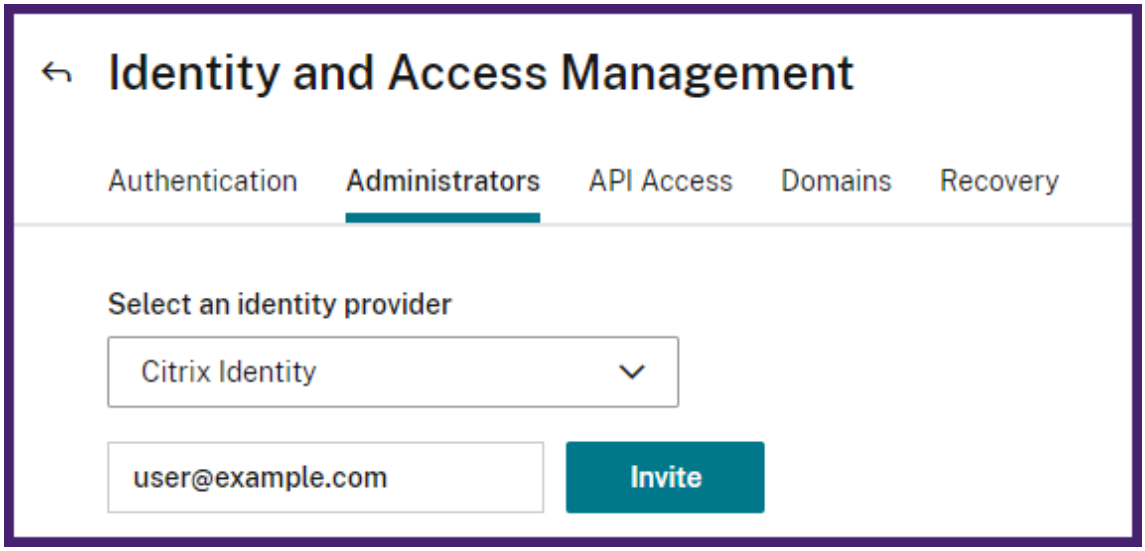
1. Klicken Sie in der Citrix ADM-Benutzeroberfläche oben links auf das Hamburger-Symbol und wählen Sie **Identity and Access Management**aus.



2. Wählen Sie auf der Seite Identitäts- und Zugriffsverwaltung die Registerkarte **Administratoren** aus.

   Auf dieser Registerkarte werden die Benutzer aufgeführt, die in Citrix Cloud erstellt wurden.

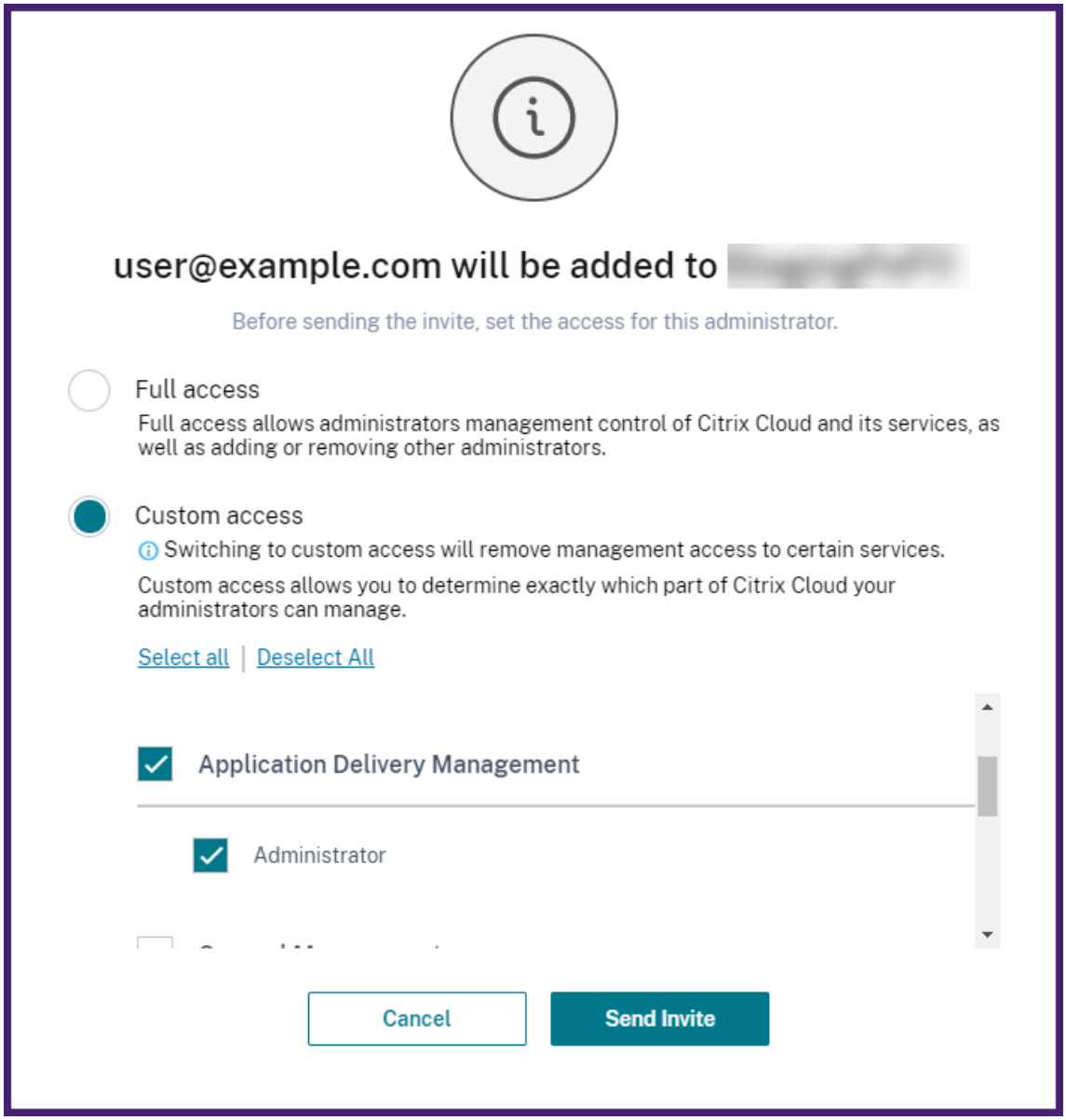
3. Wählen Sie **Citrix Identity** als Identitätsanbieter aus.
4. Geben Sie die E-Mail-Adresse des Benutzers ein, den Sie in Citrix ADM hinzufügen möchten, und klicken Sie auf **Einladen**.



> **Hinweis**
>
> Der Benutzer erhält eine E-Mail-Einladung von Citrix Cloud. Der Benutzer muss auf den in der E-Mail bereitgestellten Link klicken, um den Registrierungsvorgang abzuschließen, indem er seinen vollständigen Namen und sein Kennwort angeben und sich später mit seinen Anmeldeinformationen bei Citrix ADM anmelden.

5. Wählen Sie **Benutzerdefinierter Zugriff** für den angegebenen Benutzer aus.
6. Wählen Sie **Management für die Anwendungsbereitstellung**aus.

   Diese Option wählt standardmäßig die Rolle “ **Administrator** “ aus.



7. Klicken Sie auf **Einladung senden**.

Als Administrator sehen Sie den neuen Benutzer erst in der Liste der Citrix ADM-Benutzer, nachdem sich der Benutzer bei Citrix ADM angemeldet hat.

So konfigurieren Sie Benutzer in Citrix ADM:

1. Navigieren Sie in der Citrix ADM-Benutzeroberfläche zu **Konto** > **Benutzerverwaltung** > **Benutzer**.
2. Der Benutzer wird auf der Seite **Benutzer** angezeigt.

3. Sie können die Berechtigungen bearbeiten, die dem Benutzer zur Verfügung gestellt werden, indem Sie den Benutzer auswählen und auf **Bearbeiten**klicken. Sie können Gruppenberechtigungen auch auf der Seite **Gruppen** unter dem Knoten **Einstellungen** bearbeiten.

> **Hinweis**
>
> ```
> - Die Benutzer werden in Citrix ADM nur aus der Citrix Cloud hinzugefügt. Obwohl Sie über Administratorberechtigungen verfügen, können Sie daher keine Benutzer in der Citrix ADM -Benutzeroberfläche hinzufügen oder löschen. Sie können nur die Gruppenberechtigungen bearbeiten. Benutzer können aus Citrix Cloud hinzugefügt oder gelöscht werden.
>
> - Die Benutzerdetails werden auf der Dienst-GUI erst angezeigt, nachdem sich der Benutzer mindestens einmal am Citrix ADM angemeldet hat.
> ```

Konfigurieren von Zugriffsrichtlinien auf Citrix ADM

Zugriffsrichtlinien definieren Berechtigungen. Eine Richtlinie kann auf eine Benutzergruppe oder auf mehrere Gruppen angewendet werden, indem Rollen erstellt werden. Rollen werden durch Richtlinien bestimmt. Nach dem Erstellen von Richtlinien müssen Sie Rollen erstellen, jede Rolle an eine oder mehrere Richtlinien binden und Benutzergruppen Rollen zuweisen. Citrix ADM bietet fünf vordefinierte Zugriffsrichtlinien:

- **admin_policy**. Gewährt Zugriff auf alle Citrix ADM -Knoten. Der Benutzer verfügt sowohl über Anzeige- als auch Bearbeitungsberechtigungen, kann alle Citrix ADM Inhalte anzeigen und alle Bearbeitungsvorgänge ausführen. Das heißt, der Benutzer kann Vorgänge für die Ressourcen hinzufügen, ändern und löschen.
- **adminExceptSystem_policy**. Gewährt Benutzern Zugriff auf alle Knoten in der Citrix ADM GUI, mit Ausnahme des Zugriffs auf den Knoten Einstellungen.
- **readonly_policy**. Gewährt schreibgeschützte Berechtigungen. Der Benutzer kann den gesamten Inhalt auf Citrix ADM anzeigen, ist jedoch nicht berechtigt, Vorgänge auszuführen.

- **appadmin_policy**. Gewährt Administratorberechtigungen für den Zugriff auf die Anwendungsfeatures in Citrix ADM. Ein Benutzer, der an diese Richtlinie gebunden ist, kann benutzerdefinierte Anwendungen hinzufügen, ändern und löschen und die Dienste, Dienstgruppen und die verschiedenen virtuellen Server für Content Switching, Cache-Umleitung und virtuelle HAProxy-Server aktivieren oder deaktivieren.
- **appreadonly_policy**. Gewährt schreibgeschützte Berechtigung für Anwendungsfeatures. Ein Benutzer, der an diese Richtlinie gebunden ist, kann die Anwendungen anzeigen, kann jedoch keine Vorgänge zum Hinzufügen, Ändern oder Löschen, Aktivieren oder Deaktivieren ausführen.

Obwohl Sie diese vordefinierten Richtlinien nicht bearbeiten können, können Sie eigene (benutzerdefinierte) Richtlinien erstellen.

Früher, wenn Sie Rollen Richtlinien zugewiesen und die Rollen an Benutzergruppen gebunden haben, können Sie in der Citrix ADM-GUI Berechtigungen für die Benutzergruppen auf Knotenebene bereitstellen. Beispielsweise können Sie nur Zugriffsberechtigungen für den gesamten Load Balancing-Knoten bereitstellen. Ihre Benutzer hatten die Berechtigung, auf alle entitätsspezifischen Unterknoten unter dem Load Balancing-Knoten (z. B. virtuelle Server, Dienste und andere) zuzugreifen, oder sie hatten keine Berechtigung, auf einen Knoten unter **Load Balancing**zuzugreifen.

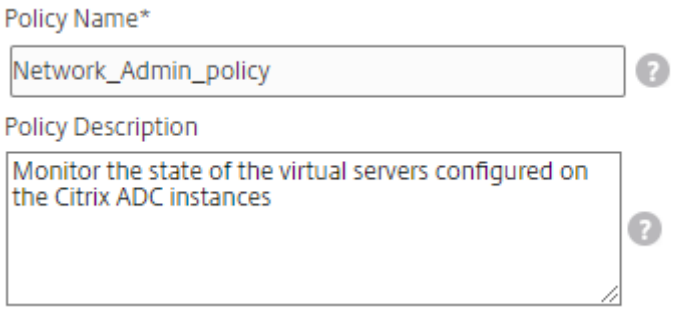
In Citrix ADM 507.x Build und höheren Versionen wird die Zugriffsrichtlinienverwaltung erweitert, um auch Berechtigungen für Unterknoten bereitzustellen. Zugriffsrichtlinieneinstellungen können für alle Unterknoten wie virtuelle Server, Dienste, Dienstgruppen und Server konfiguriert werden.

Derzeit können Sie eine solche Zugriffsberechtigung auf granularer Ebene nur für Unterknoten unter einem Load Balancing-Knoten und auch für Unterknoten unter dem GSLB-Knoten erteilen.

Beispielsweise möchten Sie als Administrator dem Benutzer eine Zugriffsberechtigung erteilen, um nur virtuelle Server anzuzeigen, jedoch nicht die Back-End-Dienste, Dienstgruppen und Anwendungsserver im Knoten Lastenausgleich. Die Benutzer, denen eine solche Richtlinie zugewiesen ist, können nur auf die virtuellen Server zugreifen.

So erstellen Sie benutzerdefinierte Zugriffsrichtlinien:

1. Navigieren Sie in der Citrix ADM-Benutzeroberfläche zu **Konto** > **Benutzerverwaltung** > **Zugriffsrichtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **Zugriffsrichtlinien erstellen** im Feld **Richtlinienname** den Namen der Richtlinie ein, und geben Sie die Beschreibung in das Feld **Richtlinienbeschreibung** ein.



Im Abschnitt **Berechtigungen** werden alle Citrix ADM Funktionen aufgelistet, mit Optionen zum Festlegen von Schreibschutz, Aktivieren und Bearbeiten des Zugriffs.

a) Klicken Sie auf das Symbol (+), um jede Feature-Gruppe in mehrere Features zu erweitern.

b) Aktivieren Sie das Kontrollkästchen Berechtigung neben dem Feature-Namen, um den Benutzern Berechtigungen zu erteilen.

- **Ansicht:** Mit dieser Option kann der Benutzer das Feature in Citrix ADM anzeigen.
- **Aktivieren-Deaktivieren:** Diese Option ist nur für die **Netzwerkfunktions-Features** verfügbar, mit denen Aktionen für Citrix ADM aktiviert oder deaktiviert werden können. Benutzer können die Funktion aktivieren oder deaktivieren. Und Benutzer können auch die Aktion **Jetzt abfragen** ausführen.

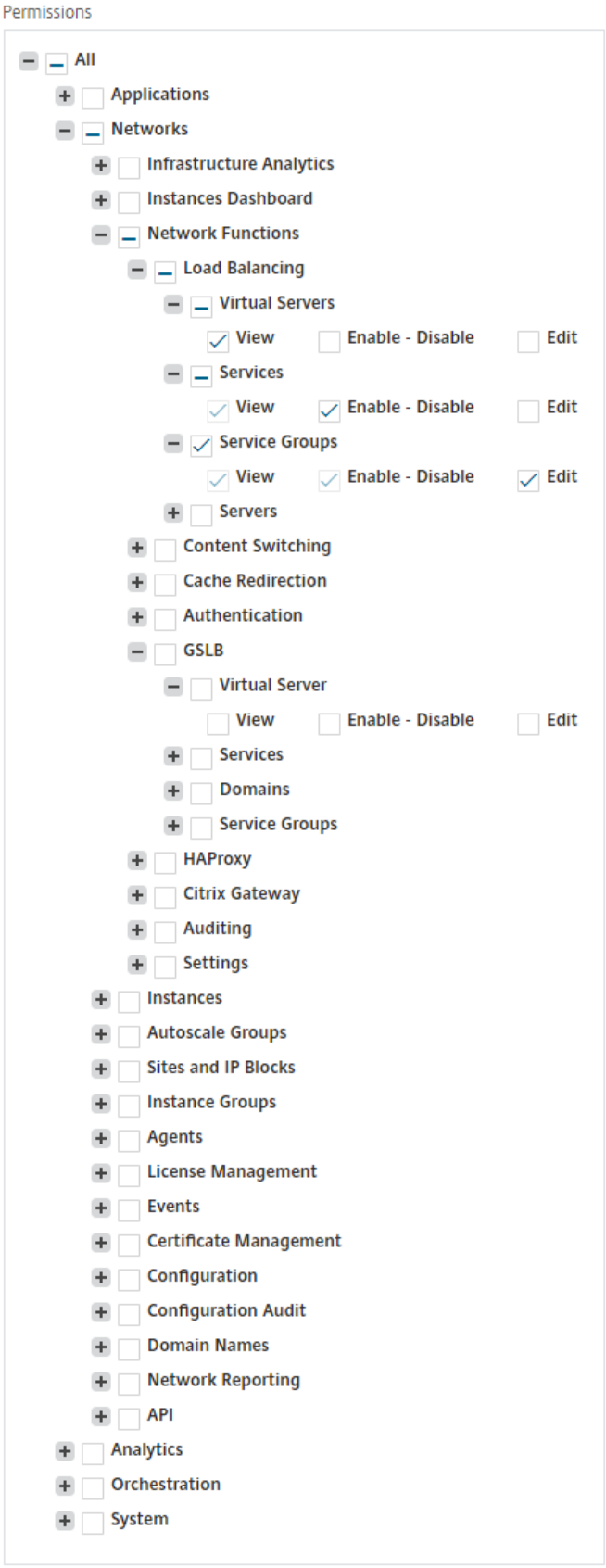
  Wenn Sie einem Benutzer die Berechtigung zum Aktivieren und **Deaktivieren** erteilen, wird auch die Berechtigung **Anzeigen** erteilt. Sie können diese Option nicht aufheben.
- **Bearbeiten:** Diese Option gewährt dem Benutzer den vollen Zugriff. Der Benutzer kann das Feature und seine Funktionen ändern.

  Wenn Sie die Berechtigung **Bearbeiten** erteilen, werden sowohl die Berechtigungen **Ansicht** als auch **Aktivieren-Deaktivieren** erteilt. Sie können die Auswahl der automatisch ausgewählten Optionen nicht aufheben.

Wenn Sie das Kontrollkästchen Feature aktivieren, werden alle Berechtigungen für das Feature ausgewählt.

> **Hinweis**
>
> Erweitern Sie Lastenausgleich und GSLB, um weitere Konfigurationsoptionen anzuzeigen.

In der folgenden Abbildung haben die Konfigurationsoptionen des Lastenausgleichs unterschiedliche Berechtigungen:



Die Berechtigung **Anzeigen** wird einem Benutzer für das Feature **Virtuelle Server** gewährt. Benutzer können die virtuellen Lastausgleichsserver in Citrix ADM anzeigen. Um virtuelle Server anzuzeigen, navigieren Sie zu **Netzwerke** > **Netzwerkfunktionen** > **Lastenausgleich** und wählen Sie die Registerkarte **Virtuelle Server**.

Die Berechtigung **Aktivieren-Deaktivieren** wird einem Benutzer für die Funktion **Dienste** gewährt. Diese Berechtigung erteilt auch die Berechtigung **Anzeigen**. Benutzer können die Dienste aktivieren oder deaktivieren, die an einen virtuellen Lastausgleichsserver gebunden sind. Außerdem kann der Benutzer eine **Jetzt abfragen**-Aktion für Dienste ausführen. Um Dienste zu aktivieren oder zu deaktivieren, navigieren Sie zu **Netzwerke** > **Netzwerkfunktionen** > **Lastenausgleich** und wählen Sie die Registerkarte **Dienste**.

> **Hinweis**
>
> Wenn ein Benutzer über die Berechtigung **Enable-Disable**verfügt, ist die Aktion zum Aktivieren oder Deaktivieren für einen Dienst auf der folgenden Seite eingeschränkt:
>
> a) Navigieren Sie zu **Netzwerke** > **Netzwerkfunktionen**.
>
> b) Wählen Sie einen virtuellen Server aus, und klicken Sie auf **Konfigurieren**.
>
> c) Wählen Sie die Seite **Load Balancing Virtual Server Service Bindung**.
> Auf dieser Seite wird eine Fehlermeldung angezeigt, wenn Sie **Aktivieren** oder **Deaktivieren** auswählen.

Die Berechtigung **Bearbeiten** wird einem Benutzer für das Feature **Dienstgruppen** erteilt. Diese Berechtigung gewährt den vollen Zugriff, auf den Berechtigungen **Anzeigen** und **Enable-Deaktivieren** erteilt werden. Benutzer können die Dienstgruppen ändern, die an einen virtuellen Lastausgleichsserver gebunden sind. Um Dienstgruppen zu bearbeiten, navigieren Sie zu **Netzwerke** > **Netzwerkfunktionen** > **Lastenausgleich** und wählen Sie die Registerkarte **Dienstgruppen**.

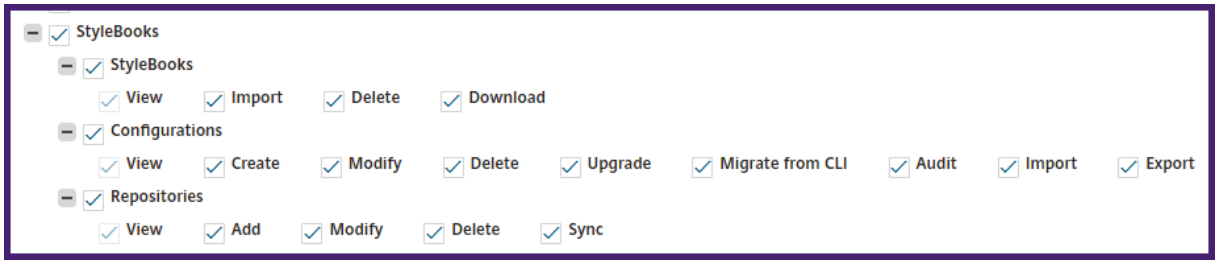
4. Klicken Sie auf **Erstellen**.

> **Hinweis**
>
> Wenn Sie **Bearbeiten** auswählen, weisen Sie möglicherweise intern abhängige Berechtigungen zu, die im Abschnitt Berechtigungen nicht als aktiviert angezeigt werden. Wenn Sie beispielsweise Bearbeitungsberechtigungen für die Fehlerverwaltung aktivieren, stellt Citrix ADM intern die Berechtigung zum Konfigurieren eines E-Mail-Profils oder zum Erstellen von SMTP-Serverkonfigurationen bereit, damit der Benutzer den Bericht als E-Mail senden kann.

Erteilen von StyleBook-Berechtigungen für Benutzer

Sie können eine Zugriffsrichtlinie erstellen, um StyleBook-Berechtigungen wie Importieren, Löschen, Herunterladen und mehr zu erteilen.

> **Hinweis**
>
> Die Anzeigeberechtigung wird automatisch aktiviert, wenn Sie andere StyleBook-Berechtigungen erteilen.



Konfigurieren von Rollen auf Citrix ADM

In Citrix ADM ist jede Rolle an eine oder mehrere Zugriffsrichtlinien gebunden. Sie können Eins-zu-Eins-, Eins-zu-Viele- und Viele-zu-Viele-Beziehungen zwischen Richtlinien und Rollen definieren. Sie können eine Rolle an mehrere Richtlinien binden und mehrere Rollen an eine Richtlinie binden.

Beispielsweise kann eine Rolle an zwei Richtlinien gebunden sein, wobei eine Richtlinie Zugriffsberechtigungen für ein Feature und die andere Richtlinie Zugriffsberechtigungen für ein anderes Feature definiert. Eine Richtlinie kann die Berechtigung zum Hinzufügen von Citrix ADC-Instanzen in Citrix ADM erteilen, und die andere Richtlinie kann die Berechtigung zum Erstellen und Bereitstellen eines StyleBook und zum Konfigurieren von Citrix ADC-Instanzen erteilen.

Wenn mehrere Richtlinien die Bearbeitungs- und Schreibschutzberechtigungen für ein einzelnes Feature definieren, haben die Bearbeitungsberechtigungen Priorität gegenüber schreibgeschützten Berechtigungen.

Citrix ADM bietet fünf vordefinierte Rollen:

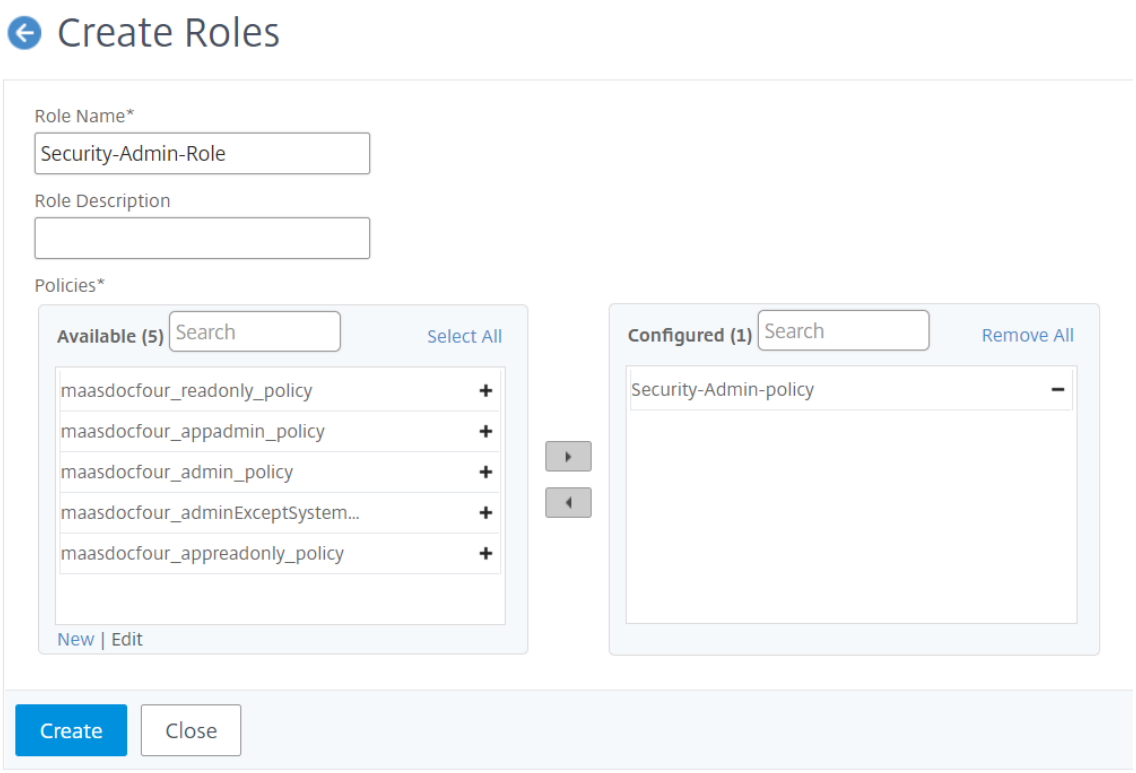
- **admin_role**. Hat Zugriff auf alle Citrix ADM Funktionen. (Diese Rolle ist gebunden an `adminpolicy`.)
- **adminExceptSystem_role**. Hat Zugriff auf die Citrix ADM GUI mit Ausnahme der Einstellungen Berechtigungen. (Diese Rolle ist an AdminExceptSystem_Policy gebunden)
- **readonly_role**. Schreibgeschützter Zugriff. (Diese Rolle ist gebunden an `readonlypolicy`.)
- **appAdmin_role**. Hat Administratorzugriff nur auf die Anwendungsfeatures in Citrix ADM. (Diese Rolle ist an appAdminPolicy gebunden).
- **appReadonly_role**. Hat schreibgeschützten Zugriff auf die Anwendungsfunktionen. (Diese Rolle ist an appReadOnlyPolicy gebunden.)

Obwohl Sie die vordefinierten Rollen nicht bearbeiten können, können Sie eigene (benutzerdefinierte) Rollen erstellen.

So erstellen Sie Rollen und weisen ihnen Richtlinien zu:

1. Navigieren Sie in der Citrix ADM-Benutzeroberfläche zu **Konto** > **Benutzerverwaltung** > **Rollen**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben **Sie auf der Seite Rollen erstellen** im Feld **Rollenname** den Namen der Rolle ein, und geben Sie die Beschreibung in das Feld **Rollenbeschreibung** ein (optional).
4. Fügen Sie im Abschnitt **Richtlinien** eine oder mehrere Richtlinien zur Liste **Konfiguriert** hinzu.

> **Hinweis**
>
> Die Richtlinien sind vorab mit einer Mandanten-ID (z. B. `maasdocfour`) versehen, die für alle Mandanten eindeutig ist.



> **Hinweis**
>
> Sie können eine Zugriffsrichtlinie erstellen, indem Sie auf **Neu**klicken, oder Sie können zu **Konto**> **Benutzerverwaltung**> **Zugriffsrichtlinien**navigieren und Richtlinien erstellen.

5. Klicken Sie auf **Erstellen**.

Konfigurieren von Gruppen auf Citrix ADM

In Citrix ADM kann eine Gruppe sowohl auf Featureebene als auch auf Ressourcenebene zugreifen. Beispielsweise kann eine Benutzergruppe nur auf ausgewählte Citrix ADC-Instanzen zugreifen, eine andere Gruppe mit nur wenigen ausgewählten Anwendungen usw.

Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, Zugriff auf Anwendungsebene für die Gruppe gewähren und der Gruppe Benutzer zuweisen. Allen Benutzern in dieser Gruppe werden in Citrix ADM dieselben Zugriffsrechte zugewiesen.

Sie können einen Benutzerzugriff in Citrix ADM auf der Ebene der Netzwerkfunktionsobjekte verwalten. Sie können dem Benutzer oder der Gruppe dynamisch bestimmte Berechtigungen auf Entitätenebene zuweisen.

Citrix ADM behandelt virtuelle Server, Dienste, Dienstgruppen und Server als Netzwerkfunktions-Entitäten.

- **Virtueller Server (Anwendungen)** - Load Balancing (`lb`), GSLB, Context Switching (`CS`), Cache-Umleitung (`CR`), Authentifizierung (`Auth`) und Citrix Gateway (`vpn`)
- **Services** - Lastenausgleich und GSLB-Dienste
- **Servicegruppe** - Lastenausgleich und GSLB-Servicegruppen
- **Server** - Lastausgleichsserver

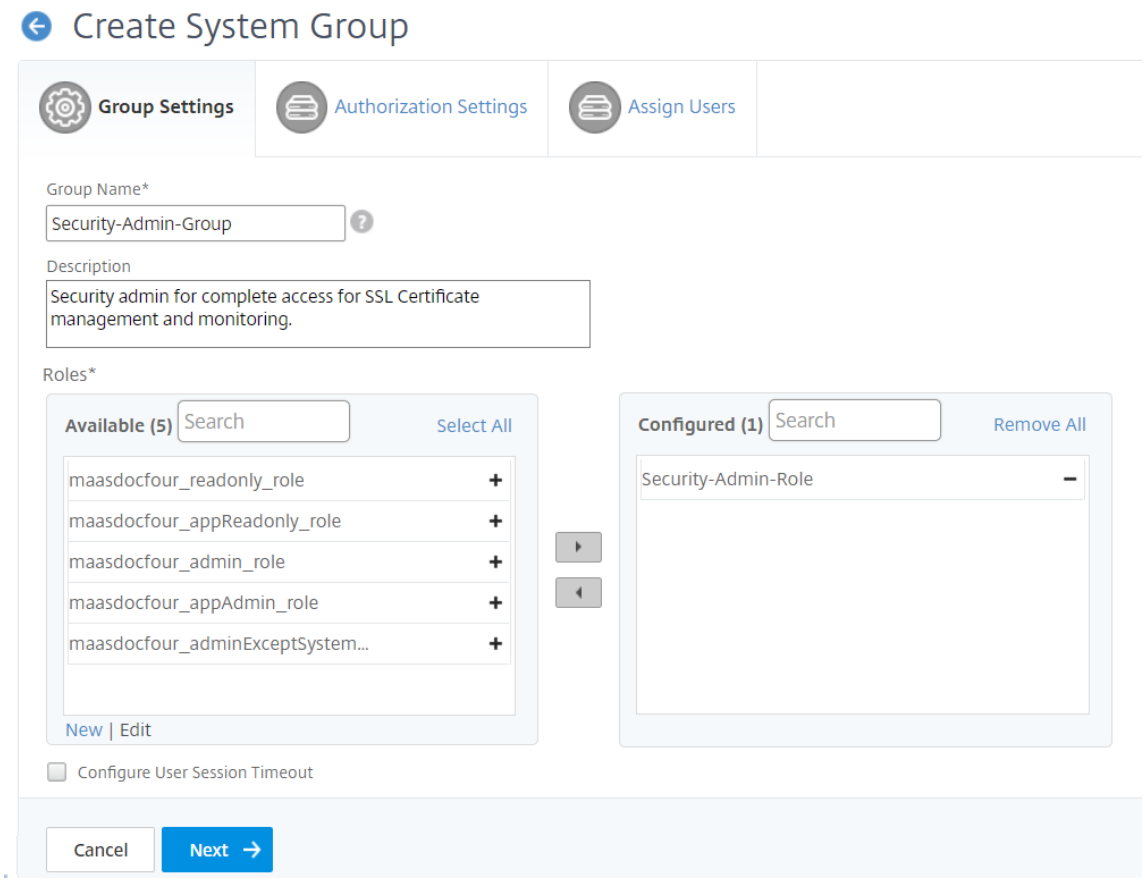
So erstellen Sie eine Gruppe:

1. Navigieren Sie in Citrix ADM zu **Konto** > **Benutzerverwaltung** > **Gruppen**.
2. Klicken Sie auf **Hinzufügen**.

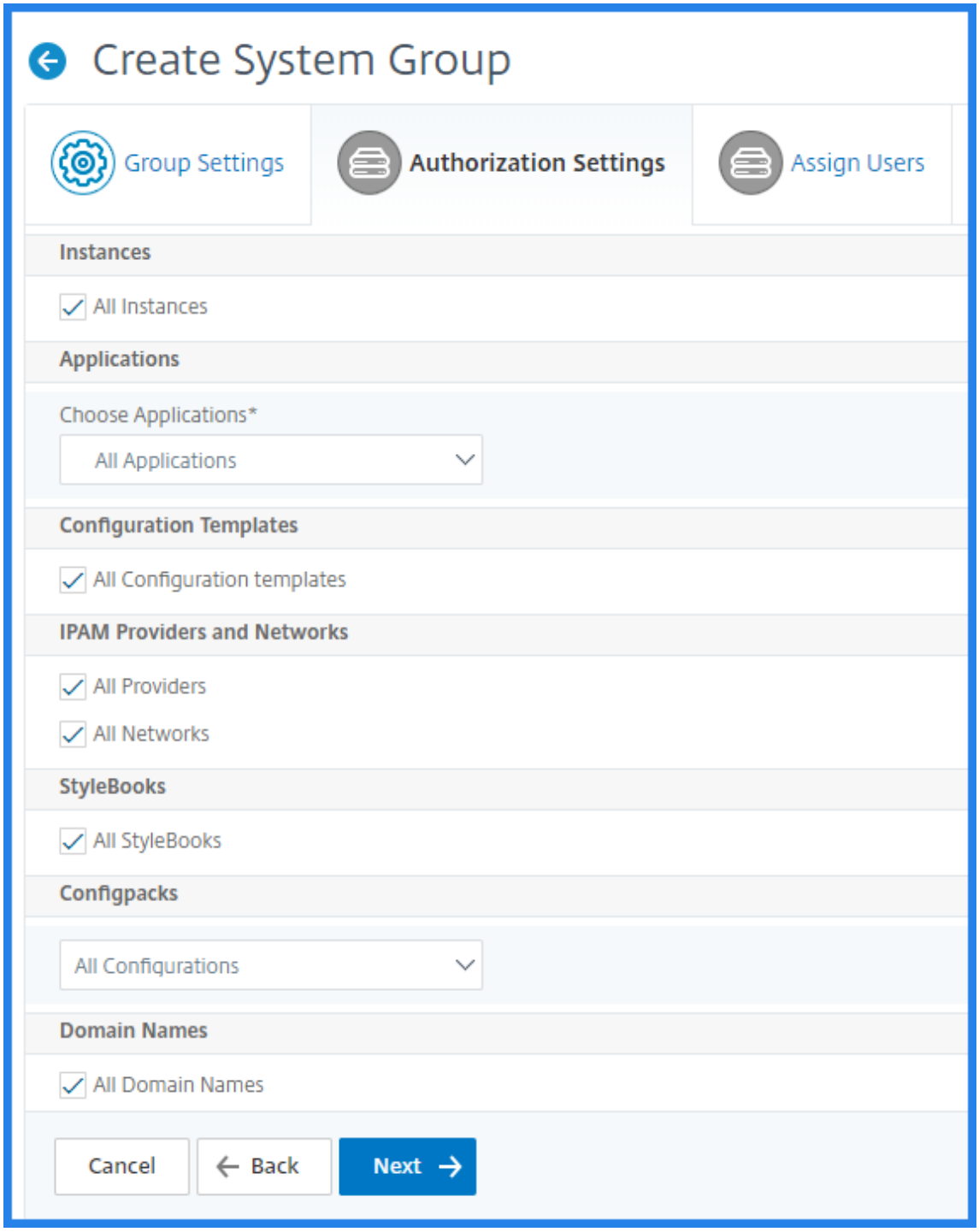
   Die Seite **Systemgruppe erstellen** wird angezeigt.
3. Geben Sie im Feld **Gruppenname** den Namen der Gruppe ein.
4. Geben Sie im Feld **Gruppenbeschreibung** eine Beschreibung Ihrer Gruppe ein. Eine gute Beschreibung hilft Ihnen, die Rolle und Funktion der Gruppe zu verstehen.
5. Verschieben Sie im Abschnitt **Rollen** eine oder mehrere Rollen in die Liste **Konfiguriert**.

   > **Hinweis**
   >
   > Den Rollen wird eine Mandanten-ID (z. B. `maasdocfour`) vorangestellt, die für alle Mandanten eindeutig ist.
6. In der Liste **Verfügbar** können Sie auf **Neu** oder **Bearbeiten** klicken und Rollen erstellen oder ändern.

   Alternativ können Sie zu **Konten** > **Benutzerverwaltung** > **Benutzer** navigieren und Benutzer erstellen oder ändern.



7. Klicken Sie auf **Weiter**.
8. Auf der Registerkarte **Autorisierungseinstellungen** können Sie Ressourcen aus den folgenden Kategorien auswählen:
   - **Gruppen automatisch skalieren**
   - **Instanzen**
   - **Anwendungen**
   - **Konfigurationsvorlagen**
   - **IPAM-Anbieter und Netzwerke**
   - **StyleBooks**
   - **Konfigurationspakete**
   - **Domänennamen**



Sie können bestimmte Ressourcen aus den Kategorien auswählen, auf die Benutzer Zugriff haben können.

Gruppen automatisch skalieren:

Wenn Sie die spezifischen Gruppen für die automatische Skalierung auswählen möchten, die Benutzer anzeigen oder verwalten können, führen Sie die folgenden Schritte aus:

a) Deaktivieren Sie das Kontrollkästchen **Alle AutoScale-Gruppen**, und klicken Sie auf **AutoScale-Gruppen hinzufügen**.

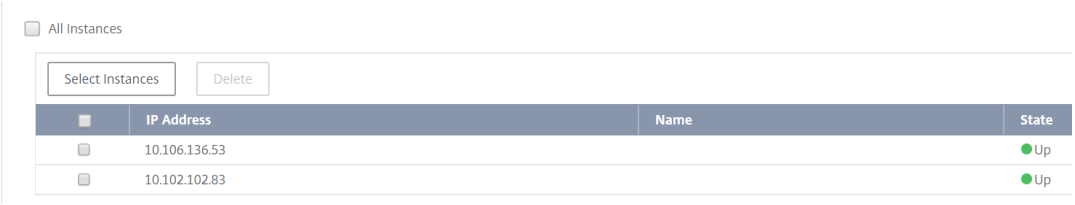
b) Wählen Sie die erforderlichen Autoscale-Gruppen aus der Liste aus, und klicken Sie auf **OK**.

Instanzen:

Wenn Sie die spezifischen Instanzen auswählen möchten, die ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

a) Deaktivieren Sie das Kontrollkästchen **Alle Instanzen**, und klicken Sie auf **Instanzen auswählen**.

b) Wählen Sie die erforderlichen Instanzen aus der Liste aus, und klicken Sie auf **OK**.



Anwendungen:

Mit der Liste **Anwendungen auswählen** können Sie einem Benutzer Zugriff auf die erforderlichen Anwendungen gewähren.

Sie können den Zugriff auf Anwendungen gewähren, ohne deren Instanzen auszuwählen. Da Anwendungen unabhängig von ihren Instanzen sind, um Benutzerzugriff zu gewähren.

Wenn Sie einem Benutzer Zugriff auf eine Anwendung gewähren, ist der Benutzer berechtigt, unabhängig von der Instanzauswahl nur auf diese Anwendung zuzugreifen.

Diese Liste enthält die folgenden Optionen:

- **Alle Anwendungen:** Diese Option ist standardmäßig ausgewählt. Es fügt alle Anwendungen hinzu, die im Citrix ADM vorhanden sind.
- **Alle Anwendungen ausgewählter Instanzen:** Diese Option wird nur angezeigt, wenn Sie Instanzen aus der Kategorie **Alle Instanzen** auswählen. Es fügt alle Anwendungen, die auf der ausgewählten Instanz vorhanden sind.
- **Bestimmte Anwendungen:** Mit dieser Option können Sie die erforderlichen Anwendungen hinzufügen, auf die Benutzer zugreifen sollen. Klicken Sie auf **Anwendungen hinzufügen**, und wählen Sie die erforderlichen Anwendungen aus der Liste aus.
- **Einzelner Entitätstyp auswählen:** Mit dieser Option können Sie den spezifischen Typ der Netzwerkfunktionsentität und die entsprechenden Entitäten auswählen.

  Sie können entweder einzelne Entitäten hinzufügen oder alle Entitäten unter dem erforderlichen Entitätstyp auswählen, um einem Benutzer den Zugriff zu gewähren.

Die Option **Auf gebundene Entitäten auch anwenden**autorisiert die Entitäten, die an den ausgewählten Entitätstyp gebunden sind. Wenn Sie beispielsweise eine Anwendung auswählen und **auch auf gebundene Entitäten anwenden** auswählen, autorisiert Citrix ADM alle Entitäten, die an die ausgewählte Anwendung gebunden sind.

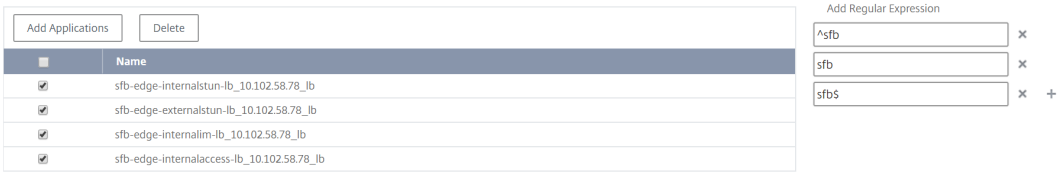
> **Hinweis**
>
> Stellen Sie sicher, dass Sie nur einen Entitätstyp ausgewählt haben, wenn Sie gebundene Entitäten autorisieren möchten.

Sie können reguläre Ausdrücke verwenden, um die Netzwerkfunktionsobjekte zu suchen und hinzuzufügen, die die Regex-Kriterien für die Gruppen erfüllen. Der angegebene Regex-Ausdruck wird in Citrix ADM beibehalten. So fügen Sie regulären Ausdruck hinzu:

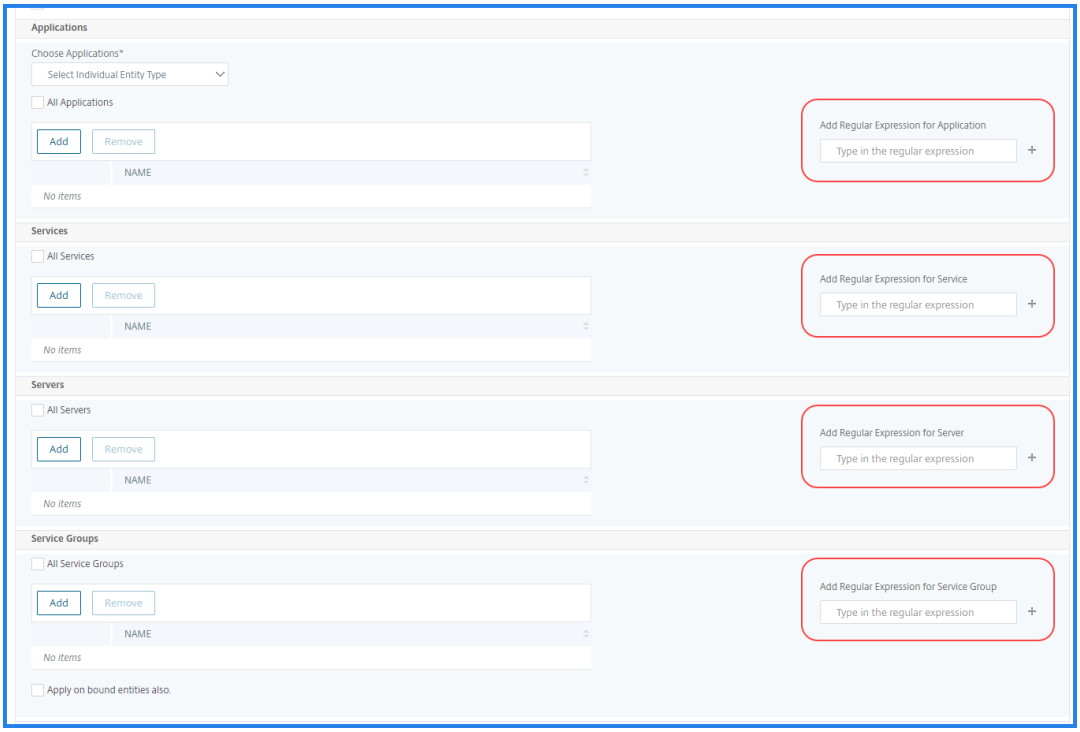
a) Klicken Sie auf **Regulären Ausdruck hinzufügen**.

b) Geben Sie den regulären Ausdruck im Textfeld an.

In der folgenden Abbildung wird erläutert, wie Sie einen regulären Ausdruck verwenden, um eine Anwendung hinzuzufügen, wenn Sie die Option **Spezifische Anwendungen** auswählen:



In der folgenden Abbildung wird erläutert, wie Sie regulären Ausdruck verwenden, um Netzwerkfunktionsobjekte hinzuzufügen, wenn Sie die Option **Individuelle Entitätstyp auswählen** auswählen:



Wenn Sie weitere reguläre Ausdrücke hinzufügen möchten, klicken Sie auf das Symbol **+**.

> **Hinweis:**
>
> Der reguläre Ausdruck stimmt nur mit dem Servernamen für den Entitätstyp **Servers** und nicht mit der Server-IP-Adresse überein.

Wenn Sie die Option **Auch auf gebundene Entitäten anwenden** für eine erkannte Entität auswählen, kann ein Benutzer automatisch auf die Entitäten zugreifen, die an die erkannte Entität gebunden sind.

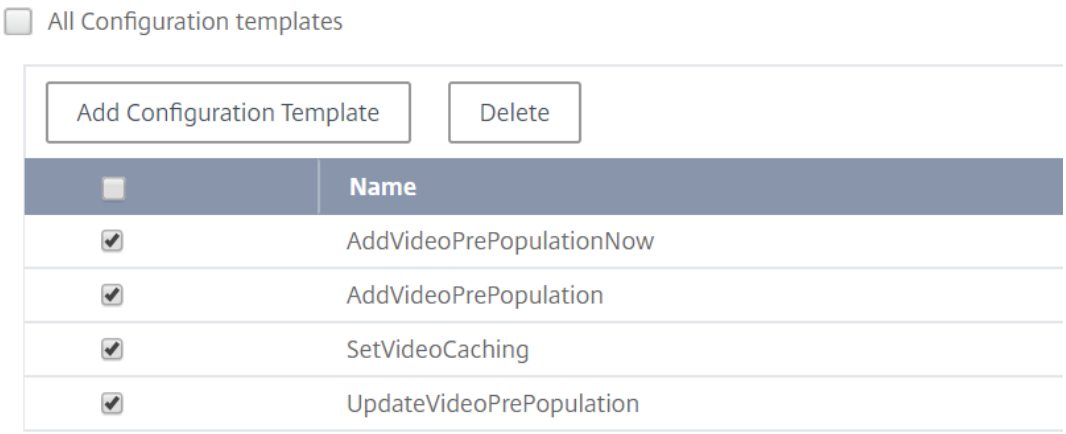
Der reguläre Ausdruck wird im System gespeichert, um den Autorisierungsbereich zu aktualisieren. Wenn die neuen Entitäten mit dem regulären Ausdruck ihres Entitätstyps übereinstimmen, aktualisiert Citrix ADM den Autorisierungsbereich auf die neuen Entitäten.

Konfigurationsvorlagen:

Wenn Sie die bestimmte Konfigurationsvorlage auswählen möchten, die ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

a) Deaktivieren Sie das Kontrollkästchen **Alle Konfigurationsvorlagen**, und klicken Sie auf **Konfigurationsvorlage hinzufügen**.

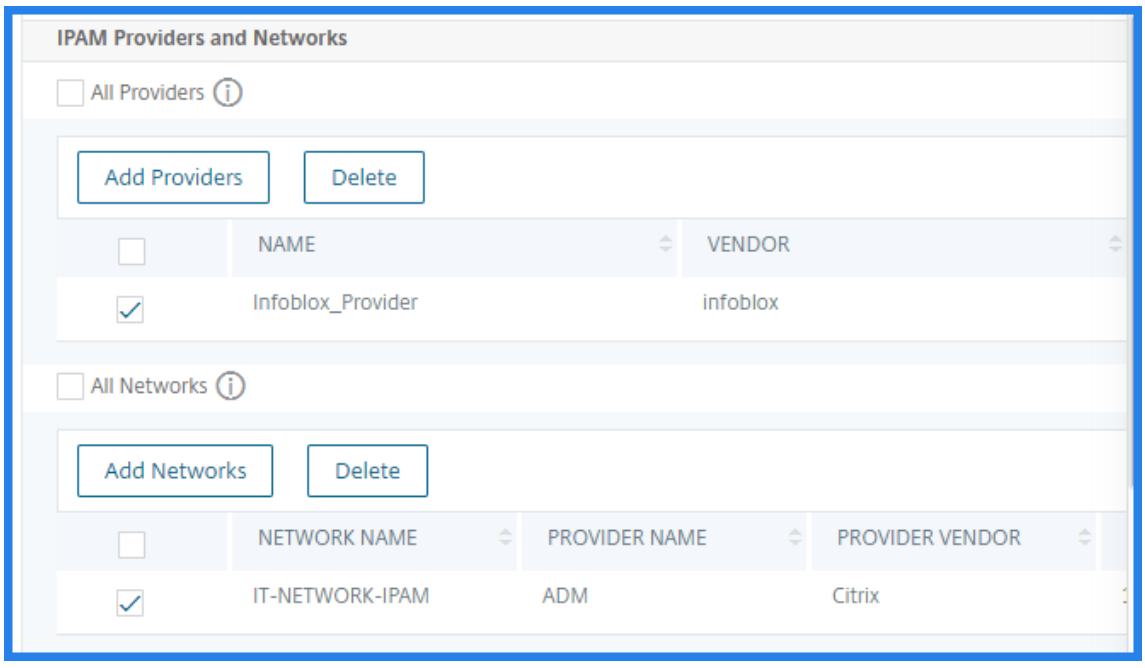
b) Wählen Sie die gewünschte Vorlage aus der Liste aus, und klicken Sie auf **OK**.



IPAM-Anbieter und Netzwerke:

Wenn Sie die spezifischen IPAM-Anbieter und -Netzwerke hinzufügen möchten, die ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

- **Anbieter hinzufügen** - Deaktivieren Sie das Kontrollkästchen **Alle Anbieter** und klicken Sie auf **Anbieter hinzufügen**. Sie können die erforderlichen Anbieter auswählen und auf **OK**klicken.
- **Netzwerke hinzufügen** - Deaktivieren Sie das Kontrollkästchen **Alle Netzwerke** und klicken Sie auf **Netzwerke hinzufügen**. Sie können die erforderlichen Netzwerke auswählen und auf **OK**klicken.



StyleBooks:

Wenn Sie das bestimmte StyleBook auswählen möchten, das ein Benutzer anzeigen oder ver-

walten kann, führen Sie die folgenden Schritte aus:

a) Deaktivieren Sie das Kontrollkästchen **Alle StyleBooks**, und klicken Sie auf **StyleBook zu Gruppe hinzufügen**. Sie können entweder einzelne StyleBooks auswählen oder eine Filterabfrage angeben, um StyleBooks zu autorisieren.

Wenn Sie die einzelnen StyleBooks auswählen möchten, wählen Sie die StyleBooks im Bereich **Einzelne StyleBooks** aus, und klicken Sie auf **Auswahl speichern**.

Wenn Sie eine Abfrage zum Suchen von StyleBooks verwenden möchten, wählen Sie den Bereich **Benutzerdefinierte Filter** aus. Eine Abfrage ist eine Zeichenfolge von Schlüssel-Wert-Paaren, in denen Schlüssel `namenamespace`, und `version`.

Sie können reguläre Ausdrücke auch als Werte verwenden, um StyleBooks zu suchen und hinzuzufügen, die Regex-Kriterien für die Gruppen erfüllen. Eine benutzerdefinierte Filterabfrage zum Durchsuchen von StyleBooks unterstützt `And` sowohl `Or` den Betrieb.

Beispiel:

```
1 name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
     version=1.0
2 <!--NeedCopy-->
```

Diese Query listet die StyleBooks auf, die die folgenden Bedingungen erfüllen:

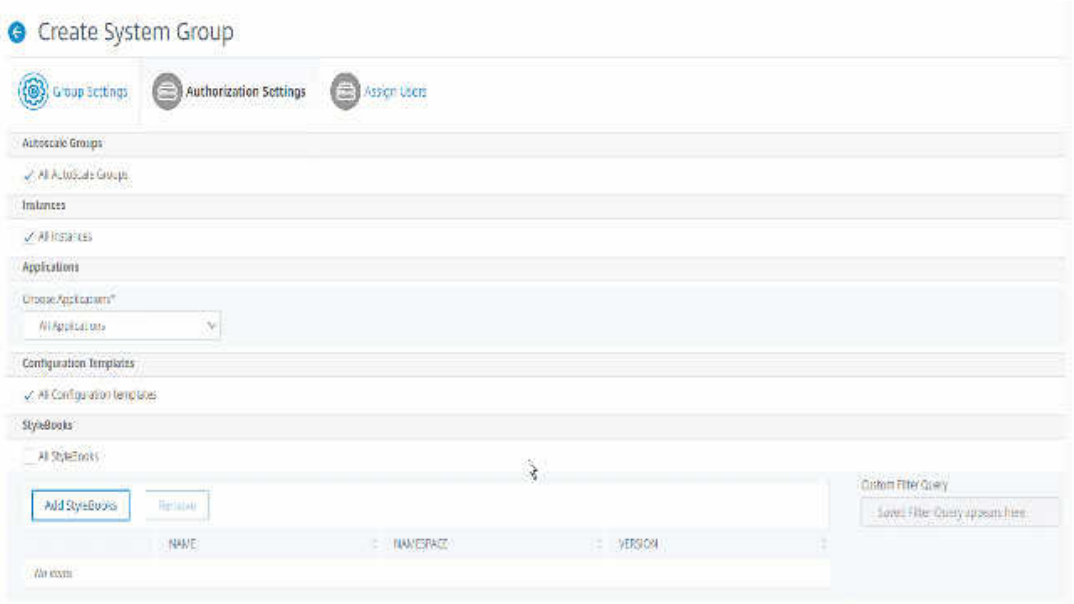
- StyleBook-Name ist entweder `lb-mon` oder `lb`.
- StyleBook Namespace ist `com.citrix.adc.stylebooks`.
- StyleBook-Version ist `1.0`.

Verwenden Sie eine `Or`-Operation zwischen Werteausdrücken, die für den Schlüsselausdruck definiert ist.

Beispiel:

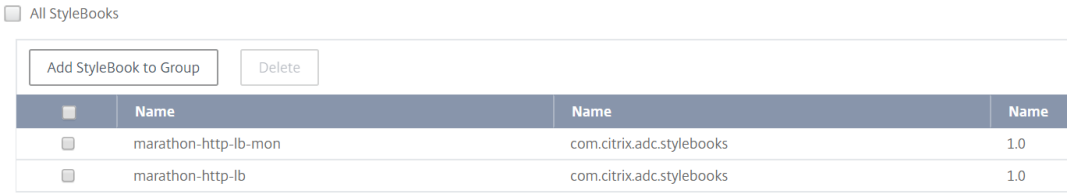
- Die Abfrage `name=lb-mon|lb` ist gültig. Es gibt die StyleBooks zurück, die einen Namen `lb-mon` oder `lb` haben.
- Die Abfrage `name=lb-mon | version=1.0` ist ungültig.

Drücken Sie `Enter`, um die Suchergebnisse anzuzeigen, und klicken Sie auf **Abfrage speichern**.



Die gespeicherte Abfrage wird in der **Abfrage für benutzerdefinierte Filter**angezeigt. Basierend auf der gespeicherten Abfrage bietet das ADM Benutzerzugriff auf diese StyleBooks.

b) Wählen Sie die gewünschten StyleBooks aus der Liste aus und klicken Sie auf **OK**.

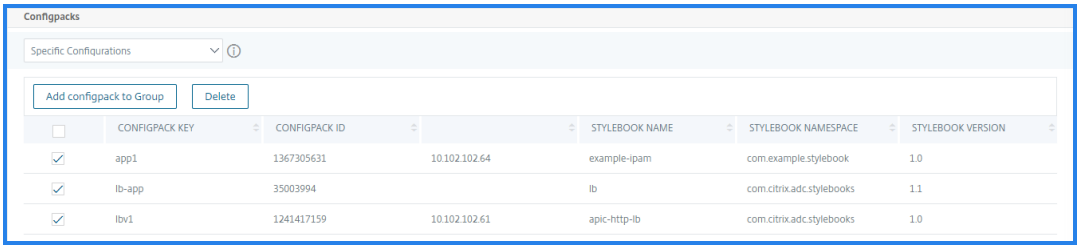


Sie können die erforderlichen StyleBooks auswählen, wenn Sie Gruppen erstellen und Benutzer zu dieser Gruppe hinzufügen. Wenn Ihr Benutzer das erlaubte StyleBook auswählt, werden auch alle abhängigen StyleBooks ausgewählt.

Konfigurationspakete:

Wählen Sie in **Configpacks** eine der folgenden Optionen aus:

- **Alle Konfigurationen**: Diese Option ist standardmäßig ausgewählt. Es fügt alle Konfigurationspakete hinzu, die in ADM enthalten sind.
- **Alle Konfigurationen der ausgewählten StyleBooks**: Diese Option fügt alle Konfigurationspakete des ausgewählten StyleBook hinzu.
- **Spezifische Konfigurationen**: Mit dieser Option können Sie die erforderlichen Konfigurationspakete hinzufügen.



Sie können die erforderlichen Konfigurationspakete auswählen, wenn Sie Gruppen erstellen und Benutzer zu dieser Gruppe hinzufügen.

Domainnamen:

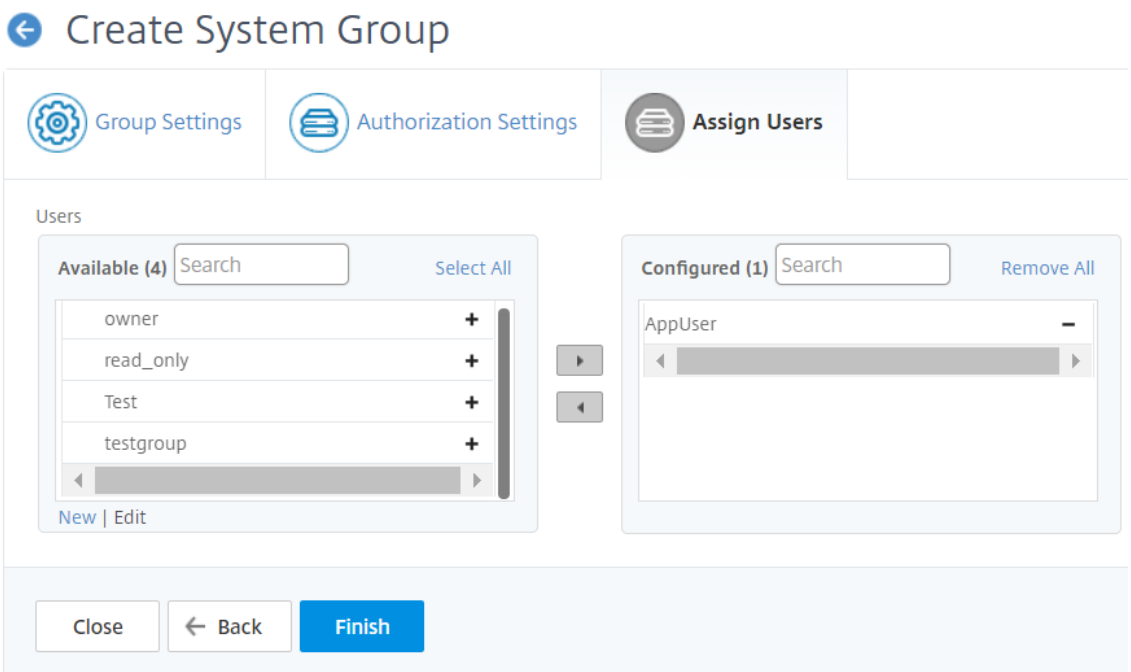
Wenn Sie den bestimmten Domänennamen auswählen möchten, den ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

a) Deaktivieren Sie das Kontrollkästchen **Alle Domänennamen**, und klicken Sie auf **Domänennamen hinzufügen**.

b) Wählen Sie die erforderlichen Domänennamen aus der Liste aus, und klicken Sie auf **OK**.

9. Klicken Sie auf **Gruppe erstellen**.
10. Wählen Sie im Abschnitt **Benutzer zuweisen** den Benutzer in der Liste **Verfügbar** aus, und fügen Sie den Benutzer zur Liste **Konfiguriert** hinzu.

> **Hinweis**
>
> Sie können auch neue Benutzer hinzufügen, indem Sie auf **Neu**klicken.



11. Klicken Sie auf **Fertig stellen**.

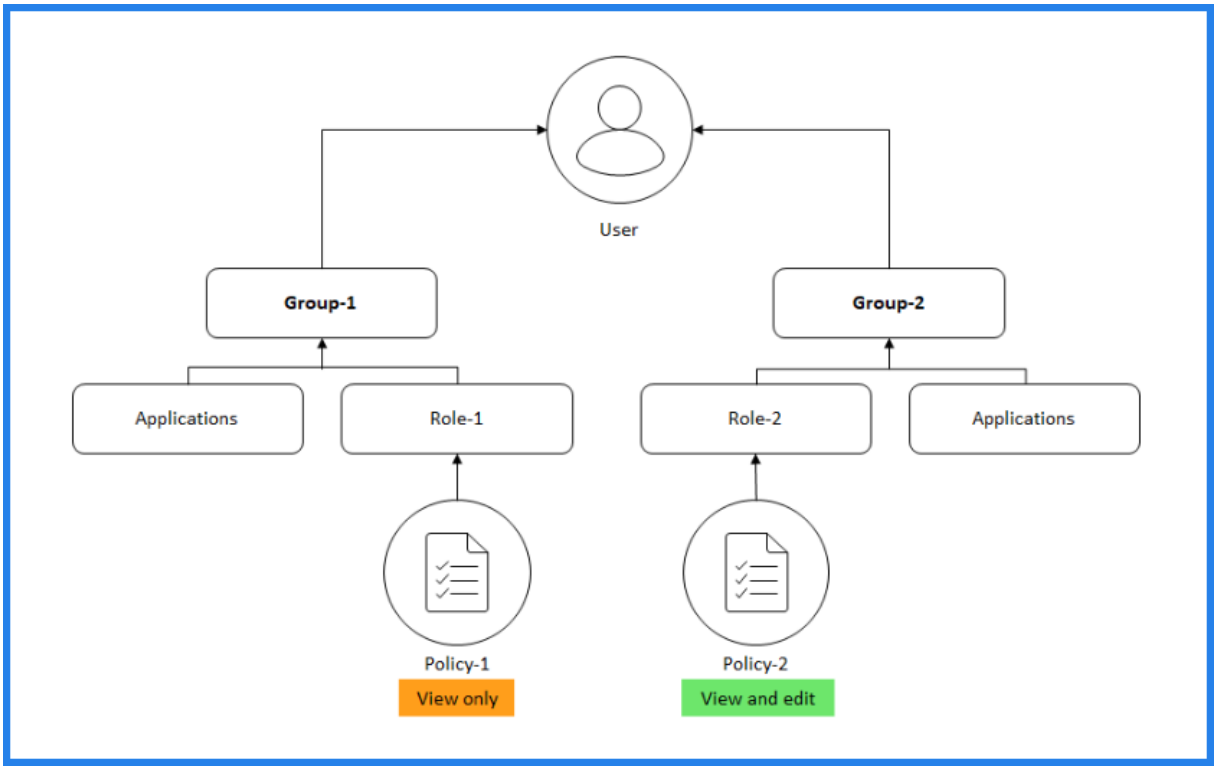
Ändern des Benutzerzugriffs basierend auf dem Berechtigungsbereich

Wenn ein Administrator einer Gruppe mit unterschiedlichen Zugriffsrichtlinieneinstellungen einen Benutzer hinzufügt, wird der Benutzer mehreren Autorisierungsbereichen und Zugriffsrichtlinien zugeordnet.

In diesem Fall gewährt das ADM dem Benutzer je nach Berechtigungsumfang Zugriff auf Anwendungen.

Betrachten Sie einen Benutzer, der einer Gruppe zugewiesen ist, die zwei Richtlinien Policy-1 und Policy-2 hat.

- **Richtlinien-1** — Nur Berechtigung für Anwendungen anzeigen.
- **Policy-2** — Anzeigen und Bearbeiten der Berechtigung für Anwendungen.



Der Benutzer kann die in Policy-1 angegebenen Anwendungen anzeigen. Außerdem kann dieser Benutzer die in Policy-2 angegebenen Anwendungen anzeigen und bearbeiten. Der Bearbeitungszugriff auf Gruppe-1-Anwendungen ist eingeschränkt, da er nicht unter dem Berechtigungsumfang von Gruppe 1 liegt.

Einschränkungen

RBAC wird von den folgenden Citrix ADM Funktionen nicht vollständig unterstützt:

- Analytics - RBAC wird von den Analytics-Modulen nicht vollständig unterstützt. Die RBAC-Unterstützung ist auf Instanzebene beschränkt und gilt nicht auf Anwendungsebene in den Analytics-Modulen Gateway Insight, HDX Insight und Security Insight.
  - Beispiel 1: Instanzbasierter RBAC (unterstützt). Ein Administrator, dem einige Instanzen zugewiesen wurden, kann nur diese Instanzen unter **HDX Insight** > **Geräte** und nur die entsprechenden virtuellen Server unter **HDX Insight** > **Anwendungen** sehen, da RBAC auf Instanz-Ebene unterstützt wird.
  - Beispiel 2: Anwendungsbasierte RBAC (nicht unterstützt). Ein Administrator, dem einige Anwendungen zugewiesen wurden, kann alle virtuellen Server unter **HDX Insight** > **Anwendungen** anzeigen, aber nicht darauf zugreifen, da RBAC auf Anwendungsebene nicht unterstützt wird.
- StyleBooks — RBAC wird für StyleBooks nicht vollständig unterstützt.
  - Stellen Sie sich eine Situation vor, in der mehrere Benutzer Zugriff auf ein einzelnes StyleBook haben, jedoch Zugriffsberechtigungen für verschiedene Citrix ADC-Instanzen haben. Benutzer können Konfigurationspakete auf ihren eigenen Instanzen erstellen und aktualisieren, aber nicht auf anderen Instanzen, da sie keinen Zugriff auf andere Instanzen als ihre eigenen haben. Sie können jedoch weiterhin die Konfigurationspakete und Objekte anzeigen, die auf Citrix ADC-Instanzen erstellt wurden.

Analytics-Einstellungen konfigurieren

April 28, 2021

Bevor Sie mit der Analytics-Funktion in Citrix Application Delivery Management (Citrix ADM) beginnen, um Einblick in Ihre Instanz- und Anwendungsdaten zu erhalten, wird empfohlen, einige Analyseeinstellungen zu konfigurieren, um eine optimale Erfahrung mit dieser Funktion zu gewährleisten.

Datenbankzusammenfassung für Analytics konfigurieren

Mit der Funktion Datenbankzusammenfassung konfigurieren in Citrix ADM können Sie die Dauer anpassen, für die Sie die historischen Analysedaten Ihrer Citrix ADC-Instanzen speichern möchten. Sie können die folgenden Datenbankzusammenfassungstypen auswählen:

- Stunden, die minütlich erfasste Daten erhalten bleiben
- Tage, die stündlich erfasste Daten erhalten bleiben
- Tage, die täglich erfasste Daten erhalten bleiben

So konfigurieren Sie die Datenbankzusammenfassung:

1. Melden Sie sich in einem unterstützten Webbrowser bei Ihrem Citrix ADM an.

2. Navigieren Sie zu **Einstellungen** > **Analytics-Einstellungen** > **Datenbankzusammenfassung**.
3. Klicken Sie auf den Namen des Insight-Typs, für den Sie die Datenbankzusammenfassung konfigurieren möchten. Wenn Sie beispielsweise die Datenbankzusammenfassung für Gateway Insight konfigurieren möchten, klicken Sie auf **GatewayInsight**.
4. Geben Sie die Dauer an, für die Sie Insight-Daten auf Citrix ADM beibehalten möchten, und klicken Sie dann auf **OK**. Für Gateway Insight können Sie beispielsweise die minutenlangen historischen Daten Ihrer Analytiker für 2 Stunden oder stündliche Daten für einen Tag speichern.

Schwellenwerte und Warnungen für Analytics erstellen

Sie können Schwellenwerte und Warnungen festlegen, um die Analytics-Metriken der verwalteten virtuellen Server zu überwachen, die auf den erkannten Instanzen konfiguriert sind. Wenn der Wert einer Metrik den Schwellenwert überschreitet, generiert Citrix ADM ein Ereignis, das eine Schwellenverletzung kennzeichnet.

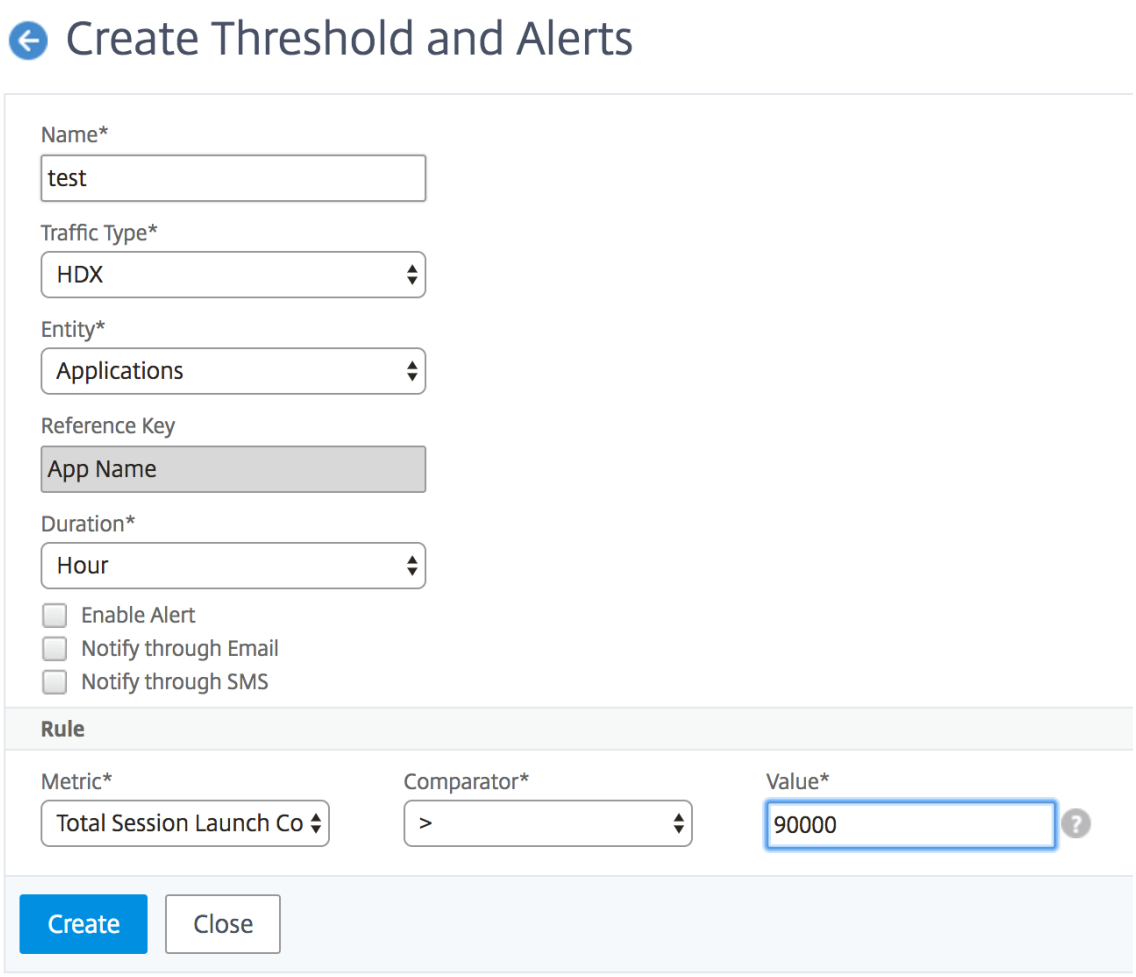
Sie können Aktionen auch den festgelegten Schwellenwerten zuordnen. Zu den Aktionen gehören das Anzeigen einer Warnung auf der GUI und das Senden von E-Mails wie konfiguriert.

Sie können beispielsweise einen Schwellenwert festlegen, um ein Ereignis für HDX-Einblicke zu generieren, wenn der ICA RTT-Wert eines Benutzers 1 Sekunde überschreitet. Sie können auch Warnungen für das generierte Ereignis aktivieren und die Informationen zur Schwellenverletzung an eine konfigurierte E-Mail-Liste senden.

So erstellen Sie Schwellenwerte und Warnungen für Analysen:

1. Melden Sie sich in einem unterstützten Webbrowser bei Ihrem Citrix ADM an.
2. Navigieren Sie zu **Einstellungen** > **Analytics-Einstellungen** > **Schwellenwerte**.
3. Klicken Sie im Fenster **Schwellenwerte** auf **Hinzufügen**, um einen neuen Schwellenwert hinzuzufügen und Alerts für die festgelegten Schwellenwerte zu konfigurieren.
4. Geben Sie auf der Seite **Schwellenwerte und Warnungen erstellen** die folgenden Details an:
    - **Name** — Name für die Konfiguration des Schwellenwerts.
    - **Traffic Type** — Typ des Analytics-Datenverkehrs, für den Sie den Schwellenwert konfigurieren möchten. Zum Beispiel: HDX Insight, Security Insight.
    - **Entity** — Kategorie oder Ressourcentyp, für die Sie den Schwellenwert konfigurieren möchten.
    - **Referenzschlüssel** — Automatisch generierter Wert basierend auf dem ausgewählten Datenverkehrstyp und der ausgewählten Entität.
    - **Dauer** - Intervall, für das Sie den Schwellenwert konfigurieren möchten.

5. Um E-Mail-Benachrichtigungen zu konfigurieren, aktivieren Sie das Kontrollkästchen für die festgelegten Schwellenwerte.
6. Geben Sie im Abschnitt **Regeln** Folgendes an:
   - **Metrik** — Metrik für den ausgewählten Traffic-Typ, um den Schwellenwert zu konfigurieren.
   - **Comparator** — Komparator zur ausgewählten Metrik (z. B.: <, >=).
   - **Wert** — Wert für die Metrik, um den Schwellenwert festzulegen und Alerts aufzurufen.
7. Klicken Sie auf **Erstellen**.



So weisen Sie delegierten Admin-Benutzern weitere Berechtigungen zu

April 28, 2021

Wenn sich der erste Benutzer Ihrer Organisation bei Citrix Application Delivery Management (Citrix ADM) anmeldet, werden diesem Benutzer die Superadministratorrechte zugewiesen. Jedem nachfolgenden Benutzer, der sich anmeldet, wird standardmäßig eine delegierte Administratorrolle zugewiesen. Ein delegierter Administrator verfügt nicht über die Berechtigung zum Anzeigen und Ausführen von Aufgaben im Zusammenhang mit der Benutzerverwaltung oder RBAC-Einstellungen.

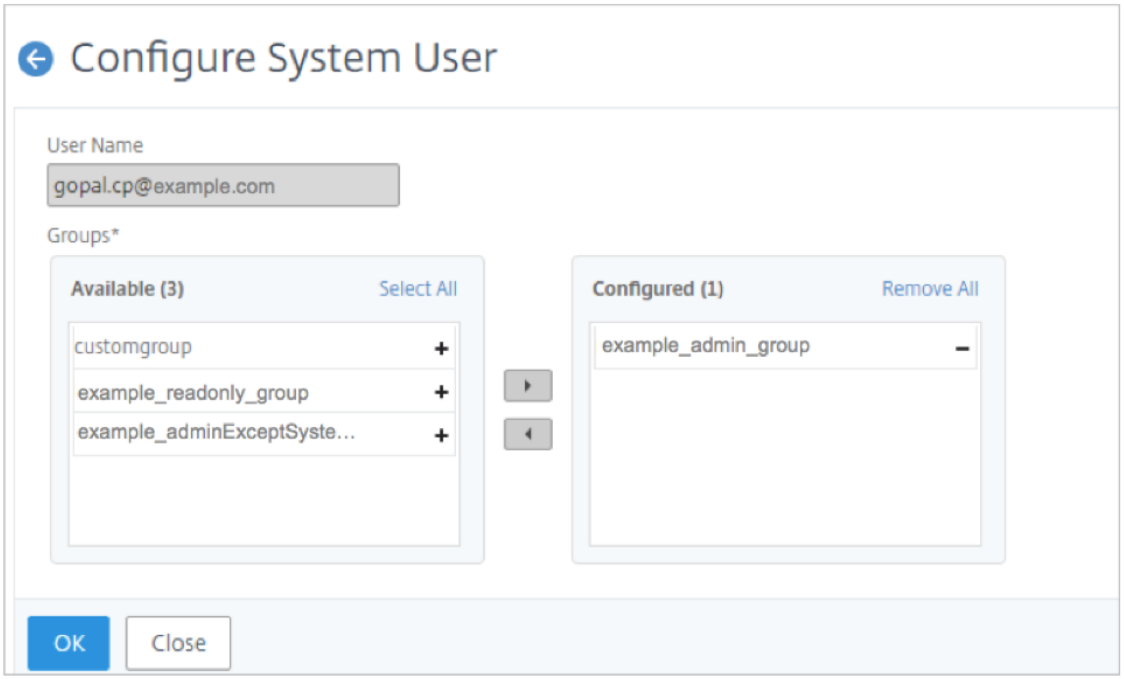
Sie können jedoch einem delegierten Administrator Superadmin-Berechtigungen oder bestimmte Nicht-Super-Admin-Rollen zuweisen, damit der Administrator Aufgaben im Zusammenhang mit der Benutzerverwaltung ausführen kann.

Ausführliche Informationen zur rollenbasierten Zugriffssteuerung finden Sie unterKonfigurieren der rollenbasierten Zugriffssteuerung.

Zuweisen von Superadministratorberechtigungen zu einem delegierten Administrator

Um einem delegierten Administrator Superadministratorberechtigungen zuzuweisen, muss ein Superadministrator die Standard-Admin-Gruppe einem delegierten Admin-Benutzer zuweisen. Führen Sie die folgenden Aufgaben aus:

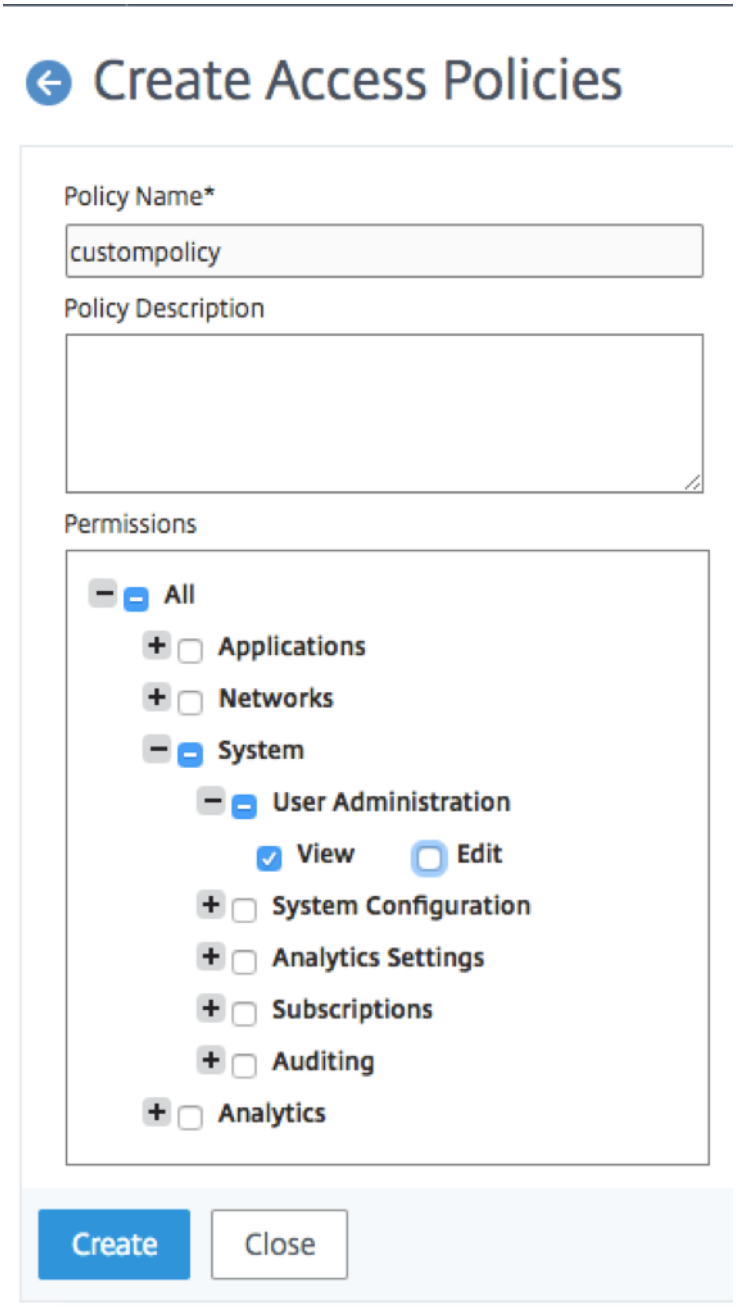
1. Melden Sie sich bei Citrix ADM als Superadministrator an.
2. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Benutzer**.
3. Wählen Sie den Benutzernamen des delegierten Administrators aus, und klicken Sie auf **Bearbeiten**.
4. Assign the group **<*tenant_name*>_admin_group** to the delegated admin and click **OK**. In der folgenden Abbildung wird beispielsweise “example_admin_group” einem delegierten Admin-Benutzer zugewiesen.



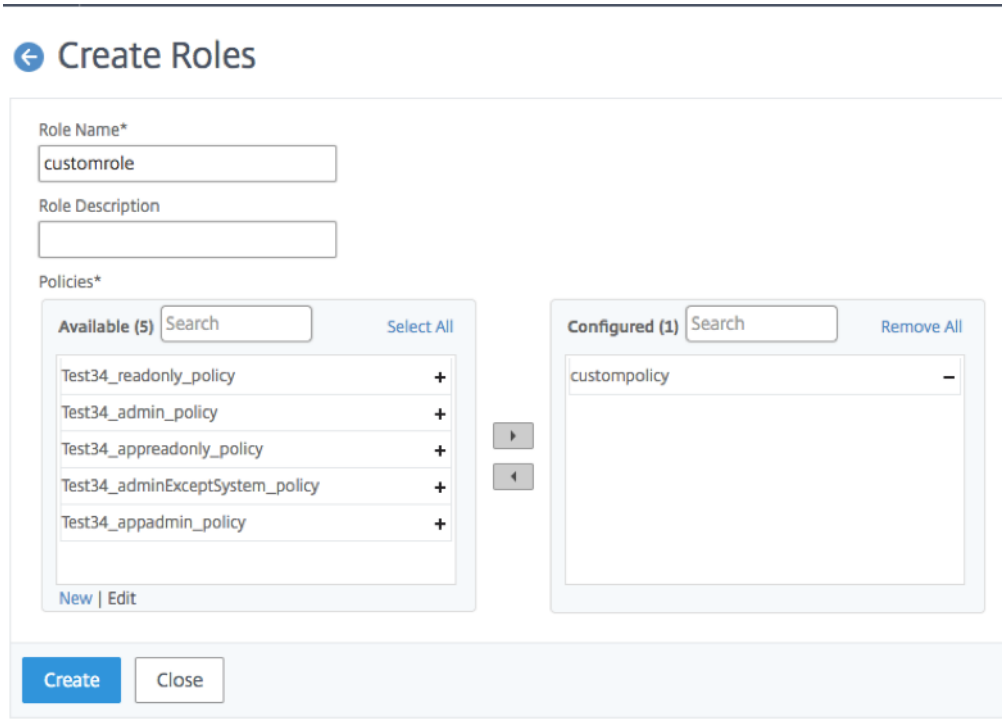
Zuweisen einer benutzerdefinierten Rolle zu einem delegierten Administrator

Um eine beliebige benutzerdefinierte Rolle einem delegierten Administrator zuzuweisen, muss der Superadmin eine Gruppe, Rolle und Richtlinie erstellen und dem delegierten Administratorbenutzer zuweisen. Dadurch wird sichergestellt, dass der delegierte Administrator nur über die erforderlichen Berechtigungen verfügt. Führen Sie die folgenden Aufgaben aus:

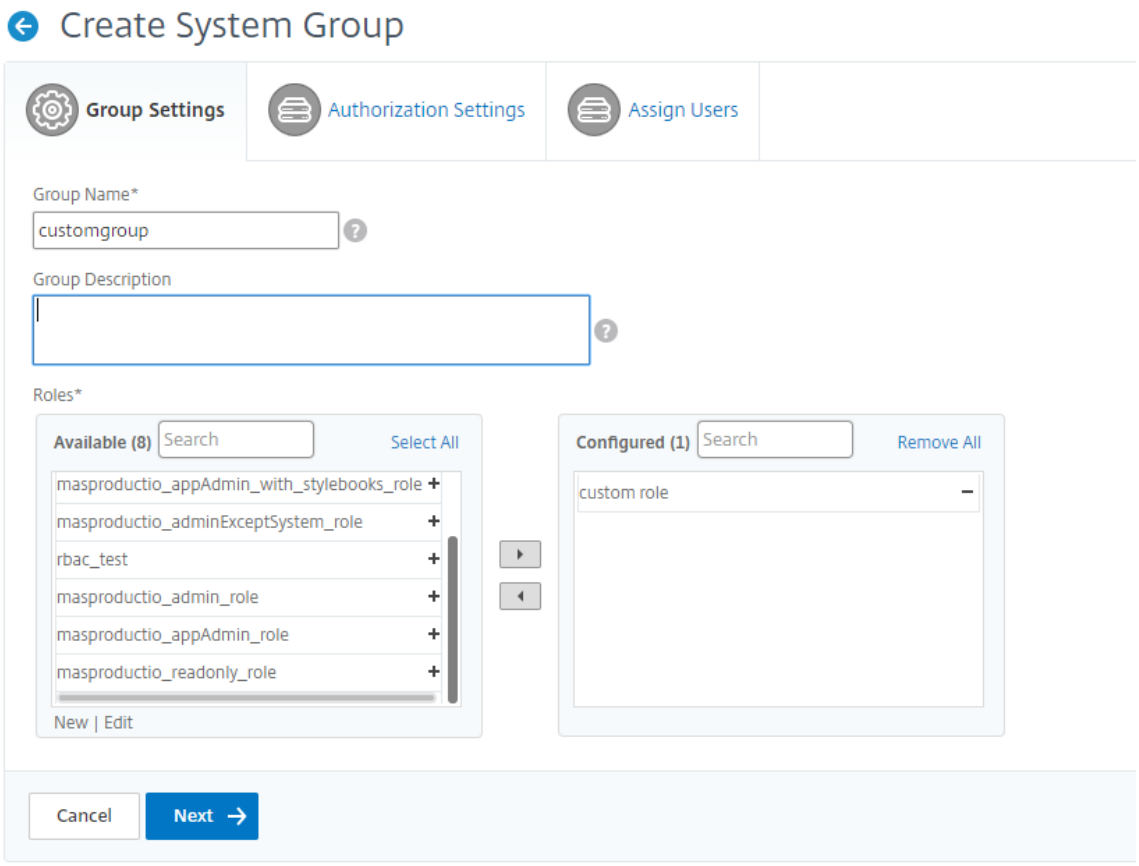
1. Melden Sie sich bei Citrix ADM als Superadministrator an.
2. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Zugriffsrichtlinien**. Wählen Sie **Hinzufügen** aus, um eine Zugriffsrichtlinie mit den erforderlichen Berechtigungen für den delegierten Administrator zu erstellen. In diesem Beispiel `custompolicy` wird eine Zugriffsrichtlinie erstellt, die den Zugriff auf die Einstellungen der Benutzerverwaltung ermöglicht.



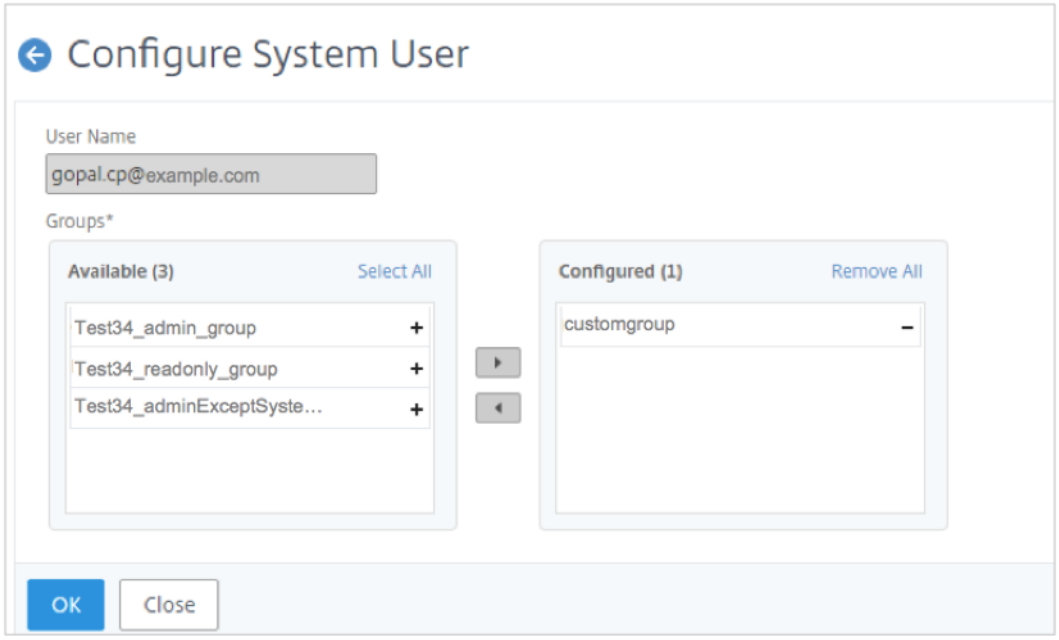
3. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Rollen**. Wählen Sie **Hinzufügen** aus, um eine Rolle zu erstellen und diese Rolle an die im vorherigen Schritt erstellte Zugriffsrichtlinie zu binden. In diesem Beispiel `customrole` wird eine Rolle erstellt und an die `custompolicy` Zugriffsrichtlinie gebunden.



4. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Gruppen**. Wählen Sie **Hinzufügen** aus, um eine Gruppe zu erstellen und diese Gruppe an die Rolle zu binden, die Sie im vorherigen Schritt erstellt haben. In diesem Beispiel wird die Gruppe “benutzerdefinierte Gruppe” erstellt und an die Rolle “benutzerdefinierte Rolle” gebunden.



5. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Benutzer**
6. Wählen Sie den Benutzernamen des delegierten Administrators aus, und klicken Sie auf **Bearbeiten**.
7. Weisen Sie die Gruppe, die Sie im vorherigen Schritt erstellt haben, dem delegierten Admin-Benutzer zu. In diesem Beispiel wird dem delegierten Admin-Benutzer die Gruppe zugewiesen `customgroup`.



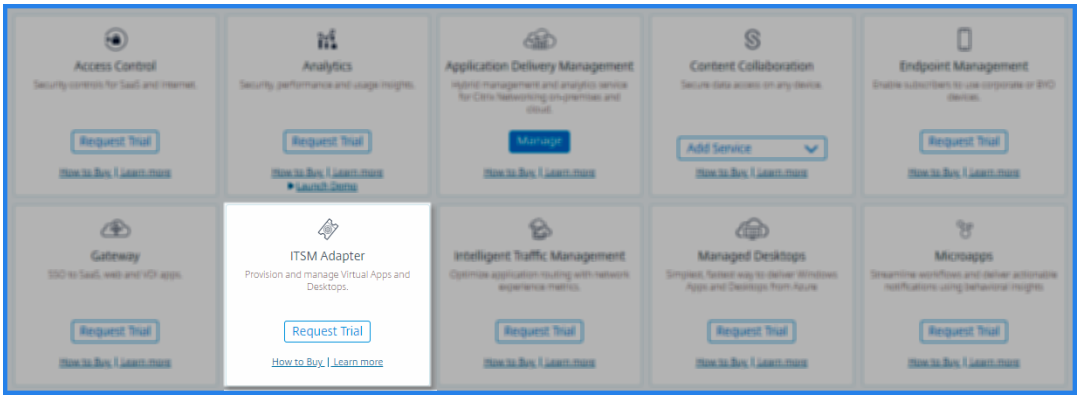
Integration von Citrix ADM in die ServiceNow-Instanz

April 28, 2021

Wenn Sie ServiceNow-Benachrichtigungen für Citrix ADC-Ereignisse und ADM-Ereignisse aktivieren möchten, müssen Sie Citrix ADM in die ServiceNow-Instanz integrieren. Um ADM in die ServiceNow-Instanz zu integrieren, verwenden SieCitrix ITSM-Connector. Der ITSM-Connector stellt die Kommunikation zwischen Citrix ADM und der ServiceNow-Instanz her. Weitere Informationen finden Sie unter Funktionsweise des ITSM-Adapters.

Führen Sie die folgenden Schritte aus, um Citrix ADM mit ServiceNow über den ITSM-Connector zu integrieren:

1. Abonnieren des **ITSM-Adapter-Dienstes** in Citrix Cloud
    a) Klicken Sie auf der Kachel **ITSM-Adapter** auf **Testversion anfordern**.



b) Navigieren Sie zu **Identitätszugriff und Verwaltung** > **API-Zugriff**, und notieren Sie sich die **Client-ID** und **Client-Geheiminformationen**.

2. Melden Sie sich mit einer Administratoranmeldeinformationen bei Ihrer ServiceNow-Instanz an, und führen Sie die folgenden Schritte aus:

   a) Gehen Sie zum ServiceNow Store. Laden Sie den **Citrix ITSM-Connector**herunter und installieren Sie sie.

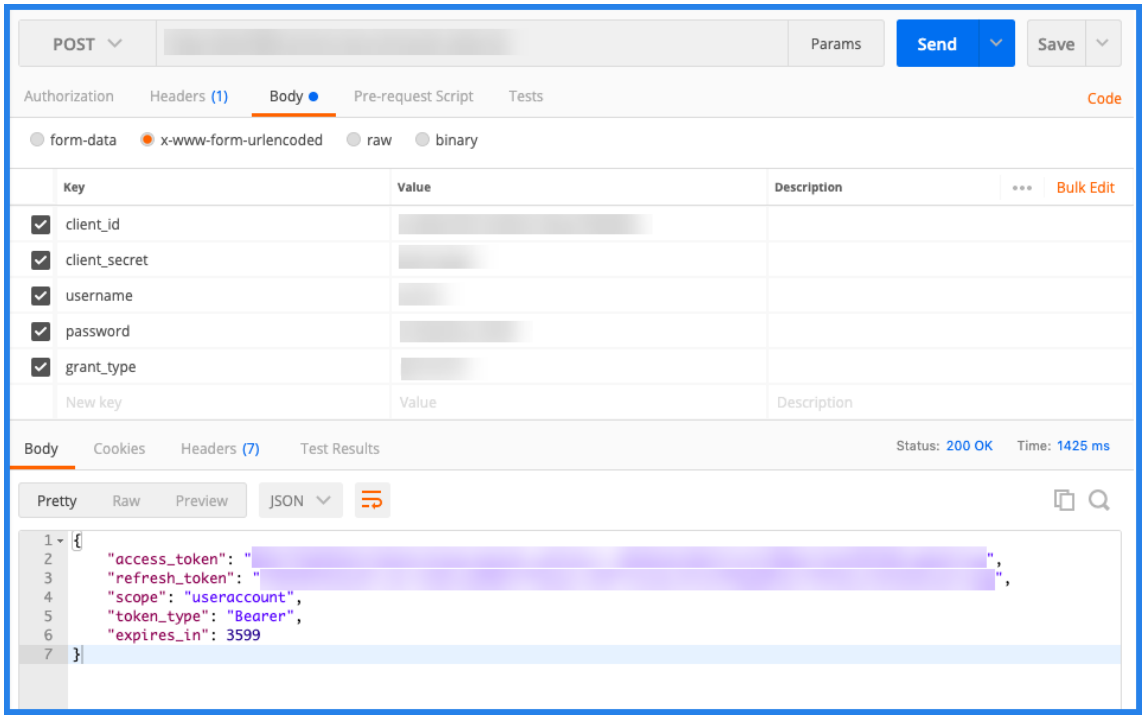
   b) Wählen Sie im Bereich **Citrix ITSM-Connector** die Option **Home** aus, und klicken Sie dann auf **Authentifizieren**. Geben Sie die Client-ID und den geheimen Schlüssel ein, die Sie in Citrix Cloud notiert haben.

   c) Testen Sie die Verbindung.

   d) Speichern Sie die Konfiguration. Eine Bestätigung von ServiceNow wird angezeigt, die darauf hinweist, dass die Verbindung aktiv ist.

3. Erstellen Sie einen Endpunkt für den Zugriff auf eine ServiceNow-Instanz. Siehe Erstellen eines Endpunkts für Clients für den Zugriff auf die Instanz.

4. Rufen Sie die Zugriffs- und Aktualisierungstoken mit der Client-ID und dem Clientgeheimnis ab. Siehe OAuth-Token.

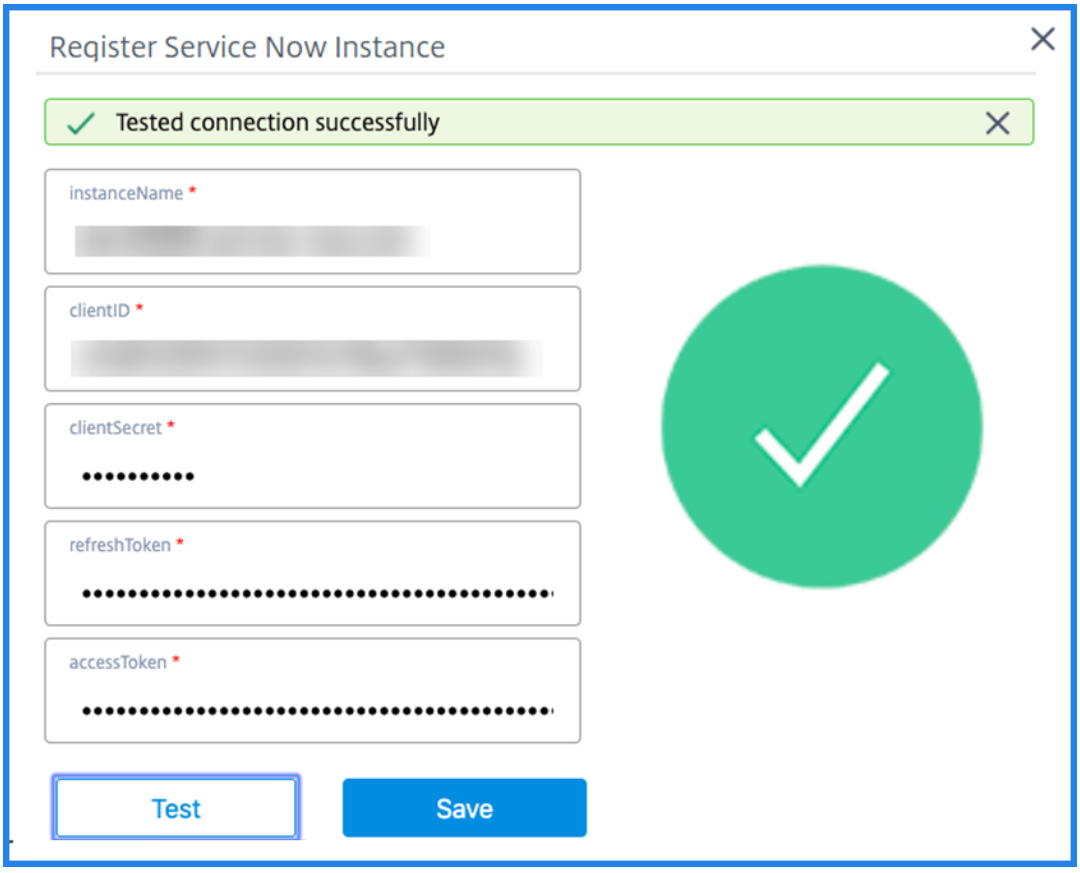


5. Fügen Sie im ITSM-Adapter eine ServiceNow-Instanz hinzu:

   a) Wählen Sie auf der Registerkarte **Verwalten** die Option ServiceNow-Instanz hinzufügen aus.

   b) Geben Sie den **Instanznamen**, die **Client-ID**, den **Client-Schlüssel, dasAktualisierungstoken**und das**Zugriffstoken**an.

   c) Klicken Sie auf **Test**.



Die ServiceNow-Instanz ist nun mit dem ITSM-Adapterdienst verbunden.

d) Nachdem Sie die Verbindung erfolgreich getestet haben, klicken **Sie auf Speichern**, um eine ServiceNow-Instanz hinzuzufügen.

6. Testen Sie die automatische Generierung von ServiceNow-Tickets in Citrix ADM.

   a) Melden Sie sich bei Citrix ADM an.

   b) Navigieren Sie zu **Konto > Benachrichtigungen** und wählen Sie **ServiceNow**.

   c) Wählen Sie das ServiceNow-Profil aus der Liste aus.

   d) Klicken Sie auf **Test**, um ein ServiceNow-Ticket automatisch zu generieren und die Konfiguration zu überprüfen.

      Wenn Sie ServiceNow-Tickets in der Citrix ADM GUI anzeigen möchten, wählen Sie **ServiceNow Tickets**aus.

Nachdem ServiceNow-Instanz auf dem ITSM-Adapter registriert wurde, können Sie ServiceNow-Benachrichtigungen für die folgenden Ereignisse in der Citrix ADM GUI einrichten:

> **Wichtig**
>
> Diese Funktion wird von ServiceNow Cloud unterstützt.

- **Citrix ADC Ereignisse**: Citrix ADM kann ServiceNow-Vorfälle für ausgewählte Citrix ADC Ereignisse aus ausgewählten verwalteten Citrix ADC-Instanzen generieren.

  Um ServiceNow-Benachrichtigungen für Citrix ADC Ereignisse von den verwalteten Instanzen zu senden, müssen Sie eine Ereignisregel konfigurieren und die Regelaktion als **ServiceNow-Benachrichtigungen senden** zuweisen.

  Erstellen Sie eine Ereignisregel für den ADM-Dienst, indem Sie zu **Netzwerke** > **Ereignisse** > **Regeln** navigieren. Weitere Informationen finden Sie unter ServiceNow-Benachrichtigungen senden.

- **Das SSL-Zertifikat und die ADM-Lizenzereignisse**: Citrix ADM kann die ServiceNow-Vorfälle für das Ablaufdatum des SSL-Zertifikats und das Ablaufdatum der ADM-Lizenz generieren.

  Informationen zum Senden von ServiceNow-Benachrichtigungen für ein Ablaufdatum von SSL-Zertifikaten finden Sie unterDas Ablaufdatum des SSL-Zertifikats.

  Informationen zum Senden von ServiceNow-Benachrichtigungen für eine ADM-Lizenzablauf finden Sie unterAblauf der Citrix ADM -Lizenz.

Exportieren oder Planen von Exportberichten

April 28, 2021

In Citrix ADM können Sie einen umfassenden Bericht für das ausgewählte Citrix ADM Feature exportieren. Dieser Bericht bietet Ihnen einen Überblick über die Zuordnung zwischen den Instanzen, Partitionen und entsprechenden Details.

Citrix ADM zeigt funktionsspezifische geplante Exportberichte unter einzelnen ADM-Features an, die Sie anzeigen, bearbeiten oder löschen können. Um beispielsweise die Exportberichte von Citrix ADC-Instanzen anzuzeigen, navigieren Sie zu **Netzwerk > Instanzen > Citrix ADC** und klicken Sie auf das Exportsymbol. Sie können diese Berichte im PDF-, JPEG-, PNG- und CSV-Dateiformat exportieren.

In **Exportieren von Berichten**können Sie die folgenden Aktionen ausführen:

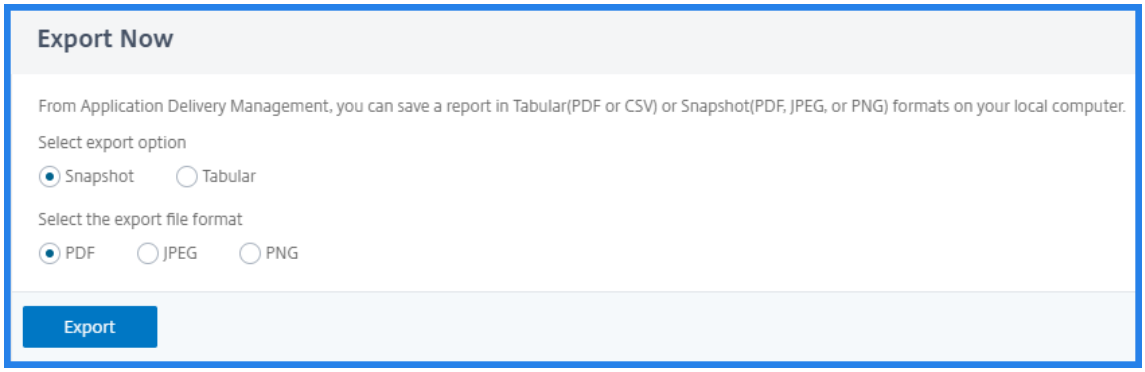
- Exportieren eines Berichts auf einen lokalen Computer
- Exportierungsberichte planen
- Anzeigen, Bearbeiten oder Löschen der geplanten Exportberichte

Exportieren eines Berichts

Um einen Bericht aus dem ADM auf den lokalen Computer zu exportieren, führen Sie die folgenden Schritte aus:

1. Klicken Sie oben rechts auf der Seite auf das Exportsymbol.

2. Wählen Sie **Jetzt exportieren**aus.
3. Wählen Sie eine der folgenden Exportoptionen aus:
    - **Snapshot** - Diese Option exportiert ADM-Berichte als Snapshot.
    - **Tabellarisch** - Diese Option exportiert ADM-Berichte in einem tabellarischen Format. Sie können auch auswählen, wie viele Datensätze in einem Tabellenformat exportiert werden sollen



4. Wählen Sie das Dateiformat aus, das Sie den Bericht auf Ihrem lokalen Computer speichern möchten.
5. Klicken Sie auf **Exportieren**.

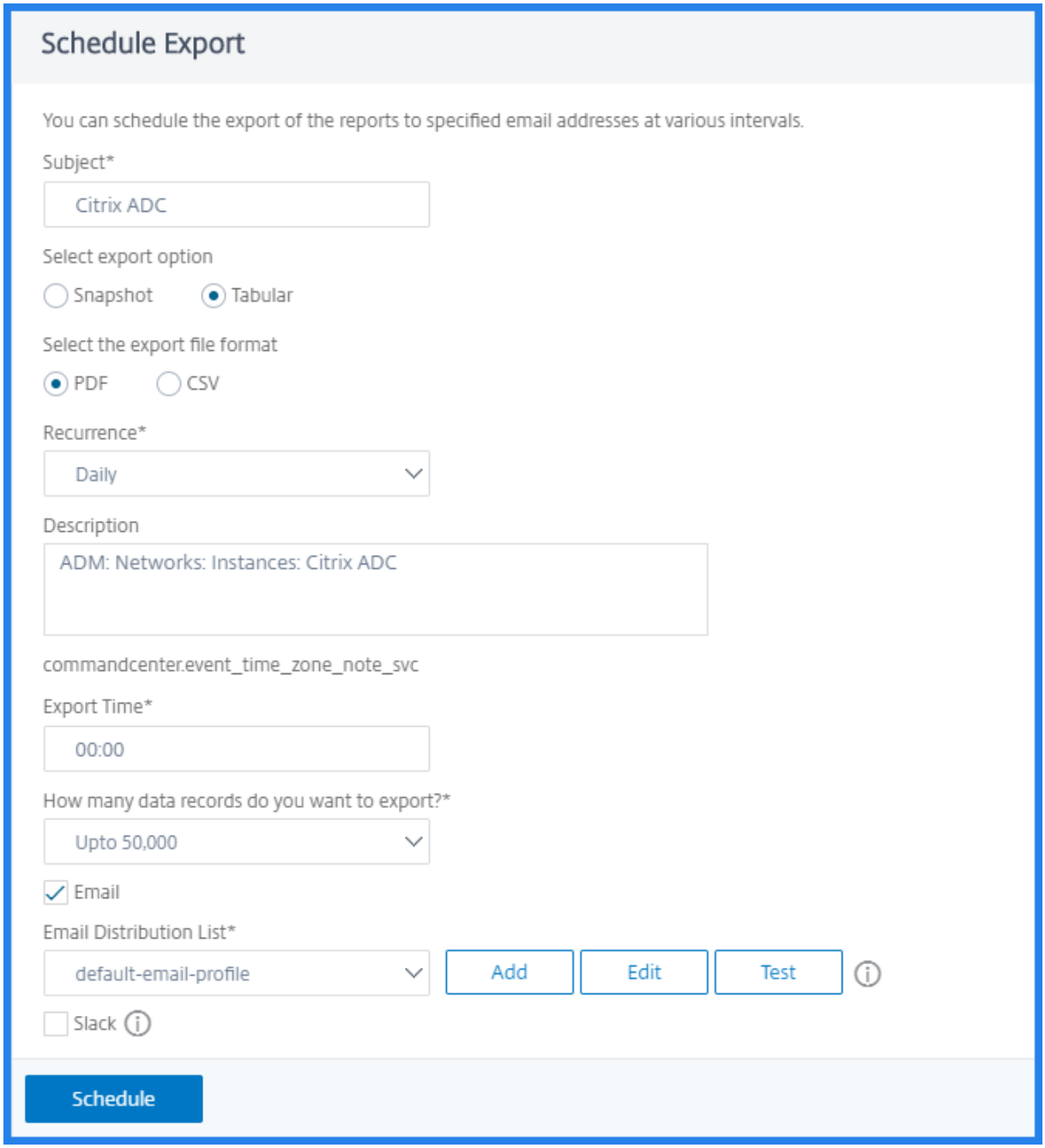
Exportierungsbericht planen

Um den Exportbericht in regelmäßigen Abständen zu planen, geben Sie das Serienintervall an. Citrix ADM sendet den exportierten Bericht an das konfigurierte E-Mail- oder Pufferprofil.

1. Klicken Sie oben rechts auf der Seite auf das Exportsymbol.
2. Wählen Sie **Export planen**, und geben Sie Folgendes an:
    - **Betreff** - Standardmäßig füllt dieses Feld den Namen des ausgewählten Features automatisch aus. Sie können es jedoch mit einem aussagekräftigen Titel umschreiben.
    - **Exportoption** - Exportieren Sie ADM-Berichte in einem Snapshot oder einem Tabellenformat. Sie können auch auswählen, wie viele Datensätze in einem Tabellenformat exportiert werden sollen
    - **Format** - Wählen Sie das Dateiformat aus, das Sie den Bericht für das konfigurierte E-Mail- oder Pufferprofil erhalten möchten.
    - **Wiederholung** - Wählen Sie in der Liste **Täglich**, **Wöchentlich**oder **Monatlich** aus.
    - **Beschreibung** - Geben Sie die aussagekräftige Beschreibung für einen Bericht an.
    - **Exportzeit** - Geben Sie an, zu welchem Zeitpunkt der Bericht exportiert werden soll.

- **E-Mail** - Aktivieren Sie das Kontrollkästchen, und wählen Sie das Profil aus dem Listenfeld aus. Wenn Sie ein Profil hinzufügen möchten, klicken Sie auf **Hinzufügen**.
- **Slack** - Aktivieren Sie das Kontrollkästchen, und wählen Sie das Profil aus dem Listenfeld aus. Wenn Sie ein Profil hinzufügen möchten, klicken Sie auf **Hinzufügen**.

3. Klicken Sie auf **Zeitplan**.



Anzeigen und Bearbeiten der geplanten Exportberichte

Führen Sie folgende Schritte aus, um die Exportberichte anzuzeigen:

1. Klicken Sie oben rechts auf der Seite auf das Exportsymbol.

   Auf der Seite " **Bericht exportieren** " werden alle funktionsspezifischen Exportberichte angezeigt.

2. Wählen Sie den Bericht aus, den Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.

Upgrade-Beratung

April 28, 2021

Als Netzwerkadministrator können Sie viele ADC-Instanzen verwalten, die auf verschiedenen ADC-Versionen in Citrix ADM ausgeführt werden. Die Überwachung des Lebenszyklus jeder ADC-Instanz kann eine umständliche Aufgabe sein. Sie müssen die ADC-Instanzen besuchen Citrix-Produktmatrix, die End of Life (EOL) oder End of Maintenance (EOM) erreichen oder erreicht haben. Planen Sie dann ihr Upgrade.

Um diesen Prozess zu vereinfachen, hilft Ihnen Citrix ADM Upgrade-Beratung dabei, den Lebenszyklus Ihrer ADC-Instanzen auf folgende Weise zu überwachen:

- Identifiziert Instanzen, die EOL oder EOM erreichen oder erreicht haben. Sie können also ADC-Upgrades vor dem EOL- oder EOM-Datum planen.
- Hebt die Instanzen hervor, die nicht auf der neuesten Version oder dem neuesten Build Sie können diese Instanzen auf die neueste Version oder den neuesten Build aktualisieren. Mit diesem Upgrade erhalten Sie Updates zu neuen Funktionen und behobenen Problemen.
- Hebt die Instanzen hervor, die sich nicht auf bevorzugten ADC-Builds befinden. Einige Organisationen haben möglicherweise bevorzugte ADC-Builds für ihre Instanzen. In ADM können Sie setze den bevorzugten Build für Ihr Unternehmen abhängig von Build-Stabilität, Funktionen und anderen Überlegungen sein. Überprüfen und aktualisieren Sie dann die Instanzen, die nicht auf bevorzugten Builds sind. Instanzen, auf denen die bevorzugten Builds ausgeführt werden, sind mit einem Sternsymbol gekennzeichnet.
- Hebt Instanzen hervor, die in den beliebtesten Versionen oder Builds ausgeführt werden. Instanzen, auf denen die beliebten Builds ausgeführt werden, werden durch ein Ribbon-Symbol gekennzeichnet

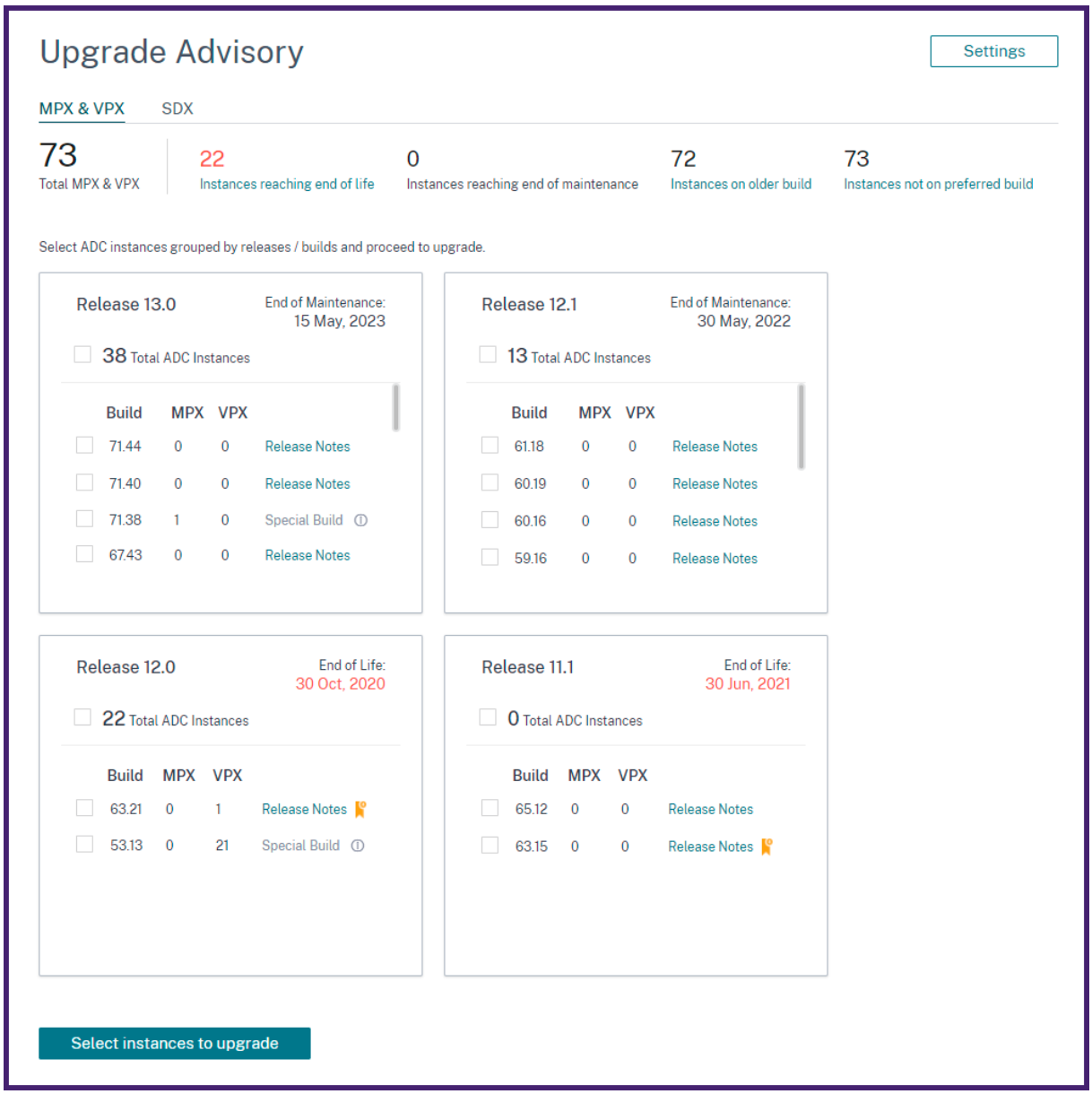
Der Upgrade-Advisory bietet Links zu entsprechenden Versionshinweisen. Mit diesen Informationen können Sie einen ADC-Build für das Upgrade überprüfen und entscheiden. Sie können auf der Seite Upgrade-Advisory einen Wartungsauftrag erstellen, um ADC-Instanzen zu aktualisieren.

> **Wichtig**
>
> Upgrade-Advisory überwacht nur die EOL von ADC-Softwareversionen. Es überprüft nicht die EOL von ADC-Appliances.

Upgrade-Advisory anzeigen

Navigieren Sie in **Netzwerken > Instanz Advisory > Upgrade Advisory** und zeigen Sie die folgenden Informationen an:

- Gesamtzahl der ADC-Instanzen.
- Instanzen, die das Lebensende erreichen.
- Instanzen, die das Ende der Wartung erreichen.
- Instanzen in älteren Builds.
- Instanzen, die sich nicht im bevorzugten Buil
- Termine für Ende der Lebensdauer und Ende der Wartung für die verschiedenen ADC-Versionen.

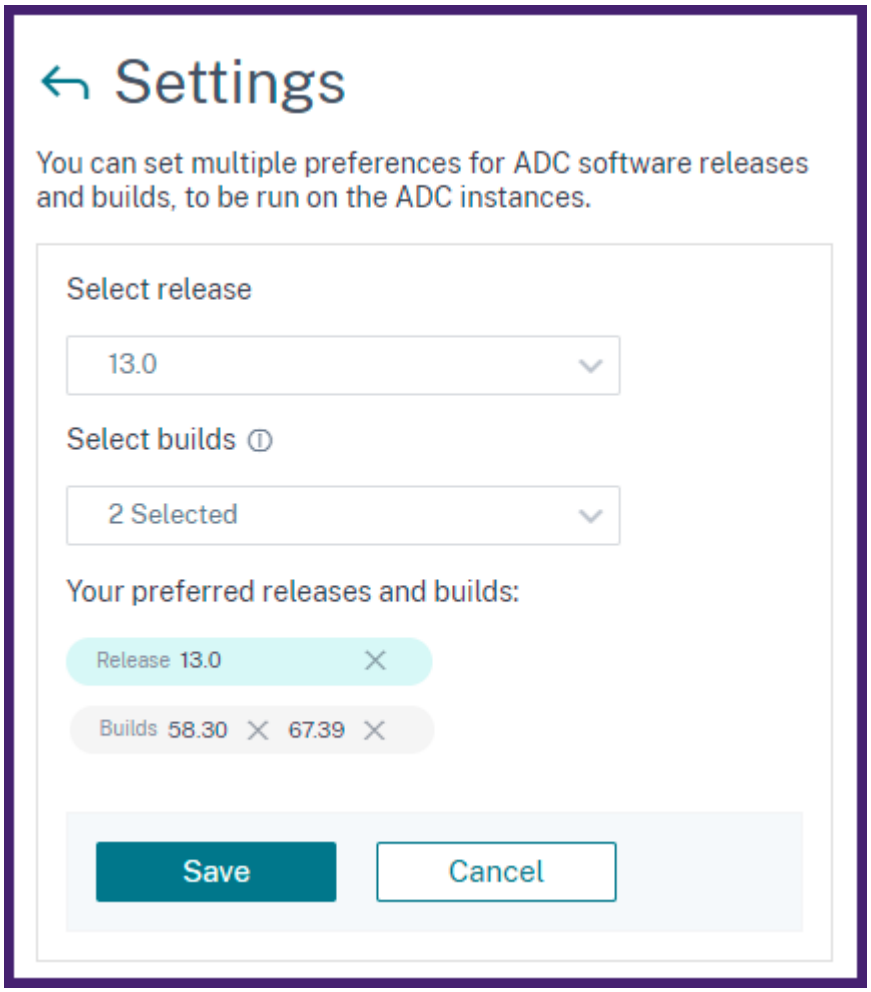


Auf der Seite **Upgrade Advisory** werden die ADC-Instanzen nach ihren Releases gruppiert. Der Link **Versionshinweise** führt Sie zu den spezifischen ADC-Versionshinweisen. Überprüfen Sie neue Funktionen, behobene und bekannte Probleme, bevor Sie sich für ein Upgrade entscheiden. Sie können mehrere ADC-Instanzen in verschiedenen Versionen auswählen, um gleichzeitig ein Upgrade durchzuführen. Wenn Sie mit einem Upgrade fortfahren, wird ein Upgrade-Job erstellt. Siehe Aktualisieren von ADC-Instanzen.

Festlegen der bevorzugten Builds

Als Administrator können Sie einen bevorzugten ADC-Build für die Organisation definieren. Führen Sie folgende Schritte aus, um den bevorzugten Build festzulegen:

1. Klicken Sie unter **Netzwerke > Instanz Advisory > Upgrade Advisory**auf **Einstellungen**.
2. Wählen Sie das bevorzugte Release und Build.

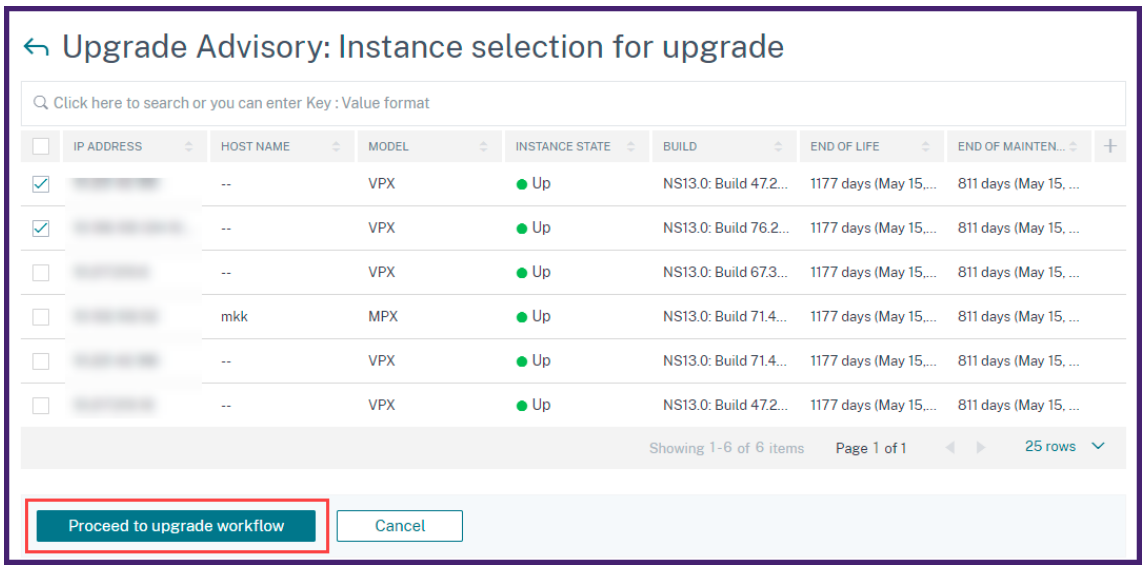


   In diesem Beispiel sind die bevorzugten Builds `13.0-58.30` und `13.0-67.39`.
3. Klicken Sie auf **Save**.

Aktualisieren von ADC-Instanzen

Führen Sie auf der Seite **Upgrade-Advisory** nach Ihrer Überprüfung die folgenden Schritte aus, um die erforderlichen ADC-Instanzen zu aktualisieren:

1. Wählen Sie die Instanz-Builds aus, die Sie aktualisieren möchten, und klicken Sie auf **Instanzen auswählen, um ein Upgrade durchzuführen**
2. Wählen Sie die ADC-Instanz aus, die Sie aktualisieren möchten, und klicken Sie auf **Weiter zum Upgrade-Workflow**.

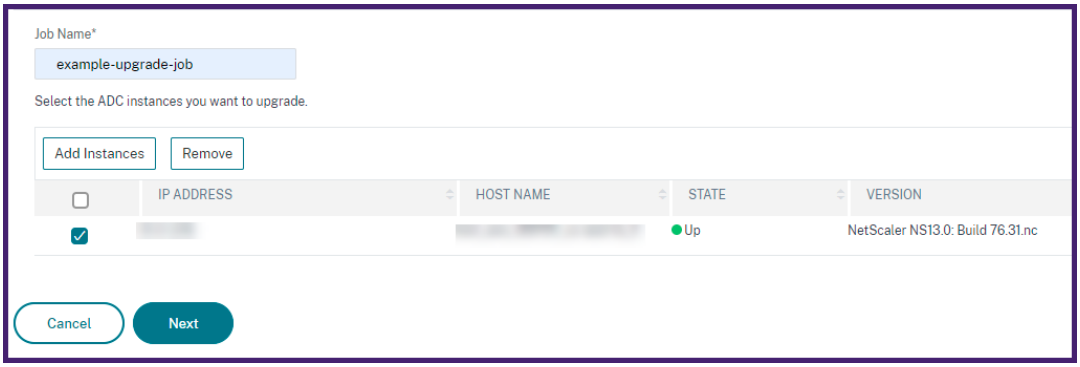


Dieser Workflow erstellt einen Upgrade-Auftrag.

3. Auf der Registerkarte **Select Instanz**

   a) Geben Sie einen Namen für den Upgrade-Auftrag an.

   b) (Optional) wenn Sie weitere Instanzen hinzufügen möchten, klicken Sie auf **Instanzen hinzufügen**.



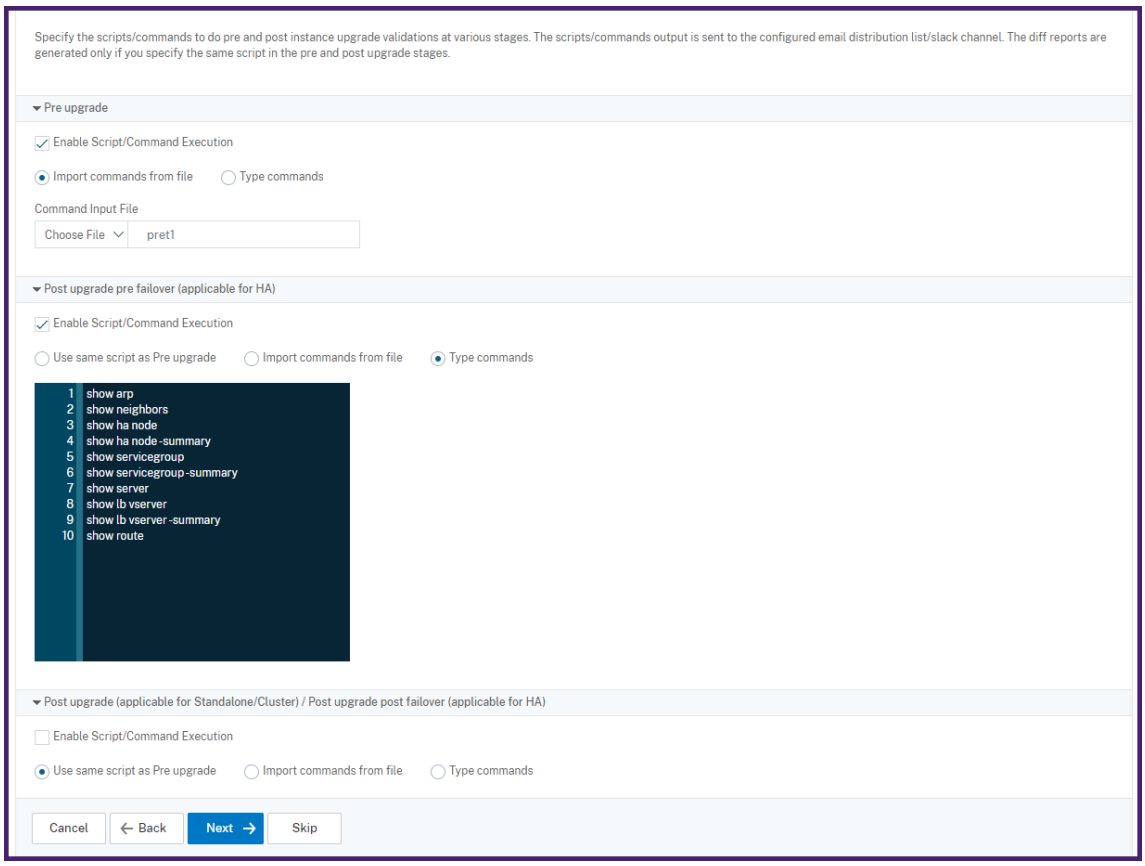
   c) Klicken Sie auf **Weiter**.

   Die Validierung vor dem Upgrade beginnt.

4. Entfernen Sie auf der Registerkarte **Validierung vor dem Upgrade** die fehlerhaften Instanzen und fahren Sie fort.

   Wenn Sie auf einer Instanz nicht genügend Speicherplatz haben, können Sie den Speicherplatz überprüfen und bereinigen. Siehe Bereinigen Sie ADC-Speicherplatz.

5. Optional geben Sie auf der Registerkarte **Benutzerdefinierte Skripts** die Scripts an, die vor und nach einem Instanz-Upgrade ausgeführt werden sollen.

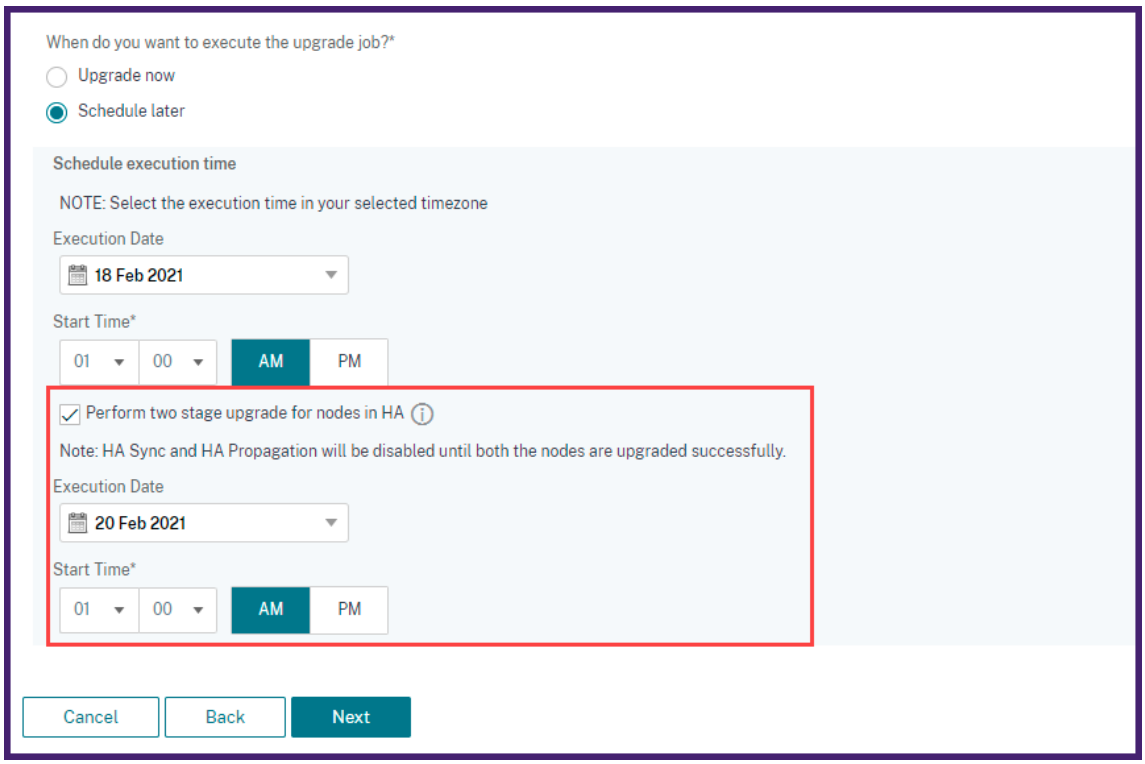


Weitere Informationen finden Sie unter Verwenden von benutzerdefinierten Skripts.

6. Wählen Sie im **Task planen**eine der folgenden Optionen aus:

   - **Jetzt upgraden** - Der Upgrade-Auftrag wird sofort ausgeführt.
   - **Später planen** - Wählen Sie diese Option, um diesen Upgrade-Auftrag später auszuführen. Geben Sie das **Ausführungsdatum** und die **Startzeit** an, wenn Sie die Instanzen aktualisieren möchten.

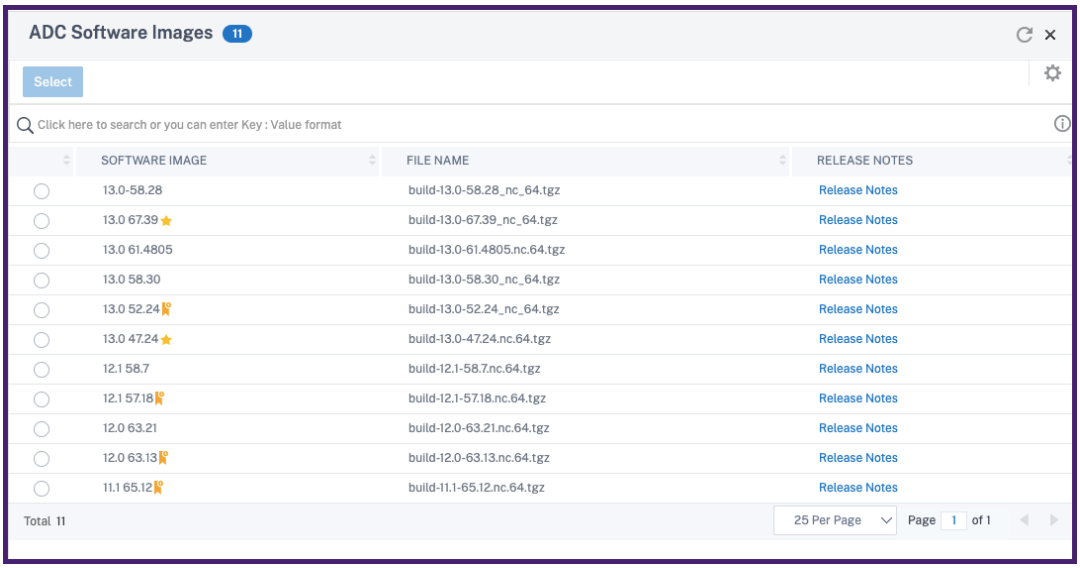
   Wenn Sie ein ADC-Hochverfügbarkeitspaar in zwei Stufen aufrüsten möchten, wählen Sie Zweistufiges Upgrade für Knoten in HA durchführen aus.



Weitere Informationen finden Sie unter Upgrade von ADC-Hochverfügbarkeitspaar.

7. Geben Sie auf der Registerkarte " **Job erstellen** " eine der folgenden Optionen an:

   - **Wählen Sie das ADC-Software-Image**: Wählen Sie ein ADC-Bild aus der Liste aus. Diese Option listet alle ADC-Images auf, die auf der Citrix Downloads-Website verfügbar sind.



   - **ADC-Software-Image**hochladen: Sie können das Bild von Ihrem lokalen Computer oder der ADC-Appliance hochladen. Wenn Sie ADC-Appliance auswählen, zeigt die ADM-GUI die Instanzdateien an, die in vorhanden sind `/var/mps/mps_images`. Wählen Sie das Image

in der ADM-GUI aus

Wenn Sie den Upgrade-Auftrag planen, können Sie angeben, wann Sie das Image in eine Instanz hochladen möchten:

- **Jetzt hochladen**: Wählen Sie diese Option, um das Image sofort hochzuladen. Der Upgrade-Auftrag wird jedoch zum geplanten Zeitpunkt ausgeführt.
- **Zum Zeitpunkt der Ausführung hochladen**: Wählen Sie diese Option, um das Image hochzuladen, wenn der Upgradejob ausgeführt wird.

Weitere Informationen zu den anderen Optionen finden Sie unter ADC-Upgrade-Optionen.

Sicherheits-Advisory

April 28, 2021

Eine sichere und belastbare Infrastruktur ist die Lebensader jeder Organisation. Daher muss die Organisation neue Common Vulnerabilities and Exposures (CVEs) nachverfolgen, die Auswirkungen von CVEs auf ihre Infrastruktur bewerten, die Minderung und Behebung verstehen und die Minderung und Behebung planen, um die Schwachstellen zu lösen.

Citrix ADM Security Advisory hebt Citrix CVes hervor, Ihre ADC-Instanzen einem Risiko auszusetzen, und empfiehlt Abgrenzungen und Korrekturen. Sie können die Empfehlungen überprüfen und geeignete Maßnahmen ergreifen, indem Sie den ADM-Service verwenden, um die Gegenmaßnahmen und Behebungen anzuwenden.

Funktionen zur Sicherheitsberatung

Die folgenden Sicherheitsfunktionen helfen Ihnen beim Schutz Ihrer Infrastruktur.

- Scan: enthält den standardmäßigen Systemscan und den Scannen auf Anforderung.
  - Systemscan: scannt alle verwalteten Instanzen standardmäßig einmal pro Woche. ADM entscheidet über Datum und Uhrzeit von Systemscans, und Sie können diese nicht ändern.
  - Anforderungsscan: ermöglicht es Ihnen, die Instanzen bei Bedarf manuell zu scannen. Wenn die nach dem letzten Systemscan verstrichene Zeit erheblich ist, können Sie den Anforderungs-Scan ausführen, um die aktuelle Sicherheitslage zu beurteilen. Oder scannen Sie, nachdem eine Behebung oder Minderung durchgeführt wurde, um die überarbeitete Haltung zu beurteilen.
- CVE-Wirkungsanalyse: zeigt Ergebnisse aller CVEs, die sich auf Ihre Infrastruktur auswirken, und alle ADC-Instanzen, die betroffen sind, und schlägt eine Abhilfe und Minderung vor. Verwenden

Sie diese Informationen, um Minderung und Abhilfe zu beantragen, um Sicherheitsrisiken zu beheben.

- CVE berichtet: speichert Kopien der letzten fünf Scans. Sie können diese Berichte im CSV-Format herunterladen und analysieren.
- CVE-Repository: Bietet einen detaillierten Überblick über alle ADC-bezogenen CVEs, die Citrix seit Dezember 2019 angekündigt hat und die Auswirkungen auf Ihre ADC-Infrastruktur haben könnten. Sie können diese Ansicht verwenden, um die CVEs im Bereich der Sicherheitsberatung zu verstehen und mehr über den CVE zu erfahren.

Punkte zu beachten

Beachten Sie bei der Verwendung von Security Advisory die folgenden Punkte:

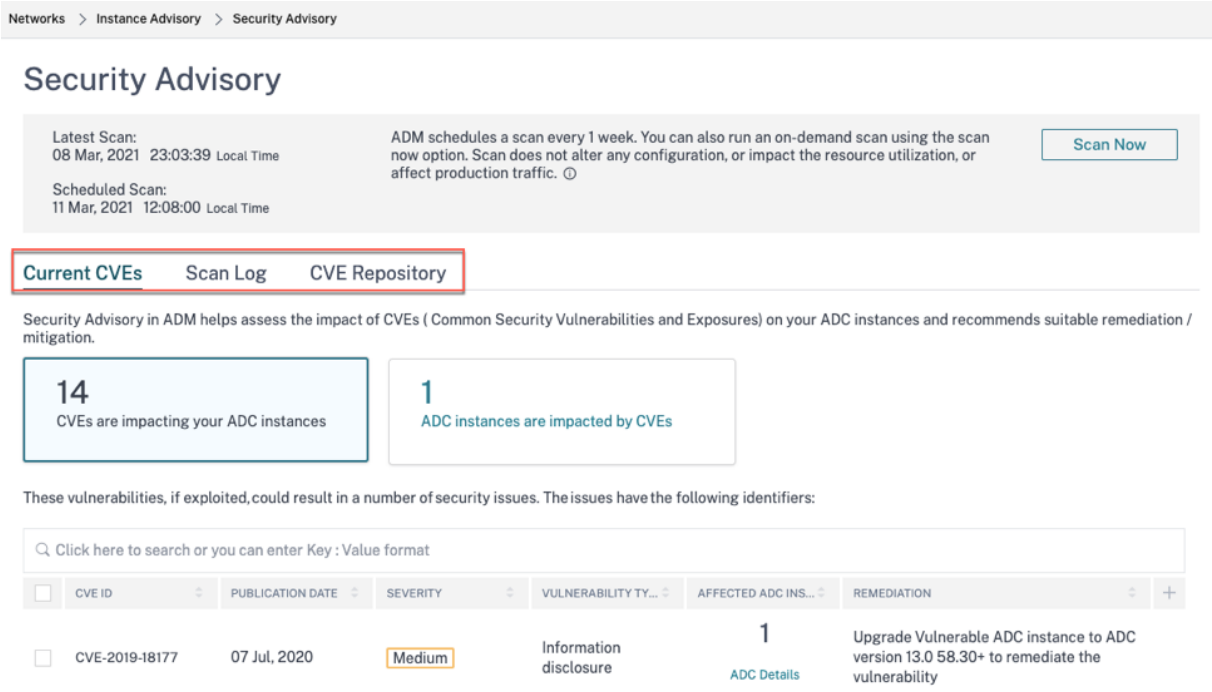
- Instanzen, die für die CVE-Erkennung unterstützt werden: alle ADC (SDX, MPX, VPX, BLX) und Gateway.
- Unterstützte CVEs: alle CVEs nach Dezember 2019.
- Umfang von ADC, Gateway-Versionen: Die Funktion ist auf Hauptgebäude beschränkt. Die Sicherheitsberatung enthält keinen speziellen Build in seinen Anwendungsbereich.
  - Security Advisory wird in ADC-Instanzen unterstützt, in denen Versionen höher als 10.5 ausgeführt werden, und nicht in Instanzen, in denen 10.5 und niedrigere Versionen ausgeführt werden.
  - Die Sicherheitshinweise wird in Admin-Partitions-, SD-WAN-Geräten, HAProxy oder HAProxy-Host-Geräten nicht unterstützt.
- Arten von Scans: Sicherheitshinweise führt Versionsscans und Konfigurationsscans durch
  - Versionsscan: prüft, ob die ADC-Version eine anfällige Version ist. Die verwendete Logik ist, wenn ein CVE auf ADC-Version xx.xx festgelegt ist, werden alle Releases und Builds niedriger als xx.xx Build als anfällig angesehen.
  - Config Scan — Scannen Sie die ADC-Konfiguration, um festzustellen, ob ein bestimmtes Konfigurationsmuster existiert, das sie anfällig macht.
- Scans haben keinen Einfluss auf den Produktionsverkehr auf ADC und verändern keine ADC-Konfiguration unter ADC.

So verwenden Sie das Sicherheits-Advisory-Dashboard

Um über die ADM-GUI auf das **Security Advisory** Dashboard zuzugreifen, navigieren Sie zu **Netzwerke > Instanz Advisory > Security Advisory**. Das Dashboard zeigt den Schwachstellenstatus aller ADC-Instanzen an, die Sie über ADM verwalten. Die Instanzen werden einmal pro Woche gescannt; Sie können sie jedoch jederzeit scannen, indem Sie auf **Jetzt scannen**klicken.

Das Dashboard enthält drei Registerkarten:

- Aktuelle CVEs
- Protokoll scannen
- CVE-Repository



> **Wichtig**
>
> In der **Sicherheits-Advisory-GUI** oder im Bericht werden möglicherweise nicht alle CVEs angezeigt, und Sie sehen möglicherweise nur eine CVE. Klicken Sie als Workaround auf **Jetzt scannen**, um einen Anforderungsscan auszuführen. Nachdem der Scan abgeschlossen ist, werden alle CVEs im Bereich (ungefähr 15) in der Benutzeroberfläche oder im Bericht angezeigt.

Aktuelle CVEs

Diese Registerkarte zeigt die Anzahl der CVEs, die sich auf Ihre Instanzen auswirken (in diesem Bildschirm 14 CVEs), sowie die Instanzen, die von CVEs betroffen sind (in diesem Bildschirm Capture One). Die Registerkarten sind nicht sequenziell, und als Administrator können Sie je nach Anwendungsfall zwischen diesen Registerkarten wechseln.

Die Tabelle mit der Anzahl der CVEs, die sich auf die ADC-Instanzen auswirken, enthält die folgenden Details.

CVE ID: Die ID der CVE, die sich auf die Instanzen auswirkt.

Veröffentlichungsdatum: Das Datum, an dem das Sicherheitsbulletin für diesen CVE veröffentlicht wurde.

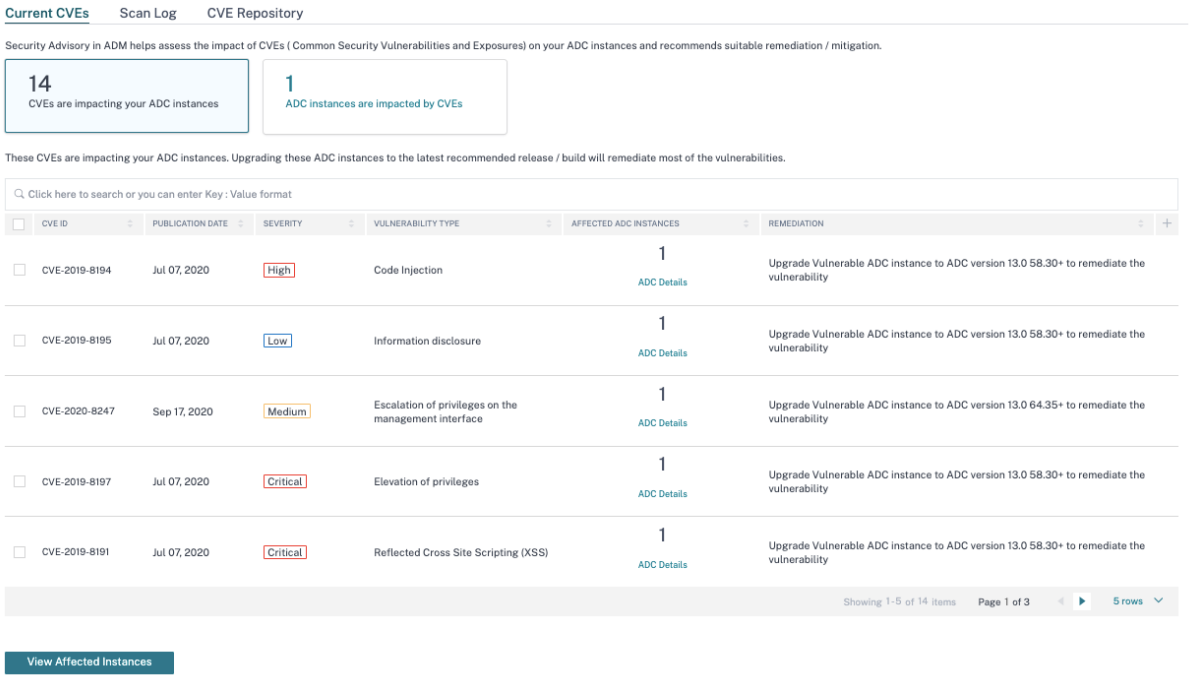
Schweregrad: der Schweregrad (hoch/mittel/kritisch) und Score. Um die Punktzahl zu sehen, bewegen Sie den Mauszeiger über den Schweregrad

Schwachstellentyp: Die Art der Schwachstelle für diese CVE.

Betroffene ADC-Instanzen: Die Instanz, auf die sich die CVE-ID auswirkt. Wenn Sie den Mauszeiger darüber bewegen, wird die Liste der ADC-Instanzen angezeigt.

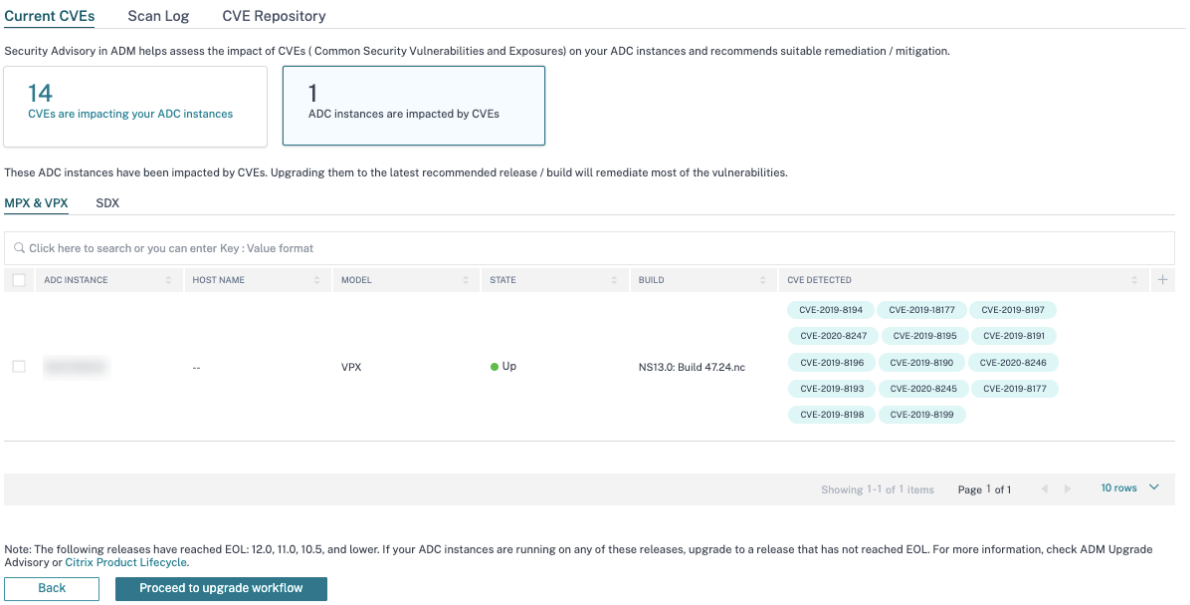
Behebung: Die verfügbaren Behebungen, bei denen die Instanz (normalerweise) aktualisiert oder Konfigurationspakete angewendet werden.

Die gleiche Instanz kann von mehreren CVEs betroffen sein. In dieser Tabelle können Sie sehen, wie viele Instanzen eine bestimmte CVE oder mehrere ausgewählte CVEs Auswirkungen haben. Um die IP-Adresse der betroffenen Instanz zu überprüfen, bewegen Sie den Mauszeiger über ADC-Details unter **Betroffene ADC-Instanzen**. Um die Details der betroffenen Instanz zu überprüfen, klicken Sie unten in der Tabelle auf **Betroffene Instanzen anzeigen**.
Sie können auch Spalten in der Tabelle hinzufügen oder entfernen, indem Sie auf das Pluszeichen klicken.



Die **<number of>ADC-Instanzen werden von der Registerkarte CVEs beeinflusst** und zeigt Ihnen alle betroffenen ADM-verwalteten ADC-Instanzen. Die Tabelle zeigt die ADC-IP-Adresse, den Hostnamen, die ADC-Modellnummer, den Status des ADC, die Softwareversion und den Build sowie die Liste der CVEs, die den ADC beeinflussen.

Bei der folgenden Bildschirmaufnahme ist eine ADC-Instanz betroffen. Sie fügen eine dieser Spalten nach Bedarf hinzu oder entfernen sie, indem Sie auf das Zeichen + klicken.



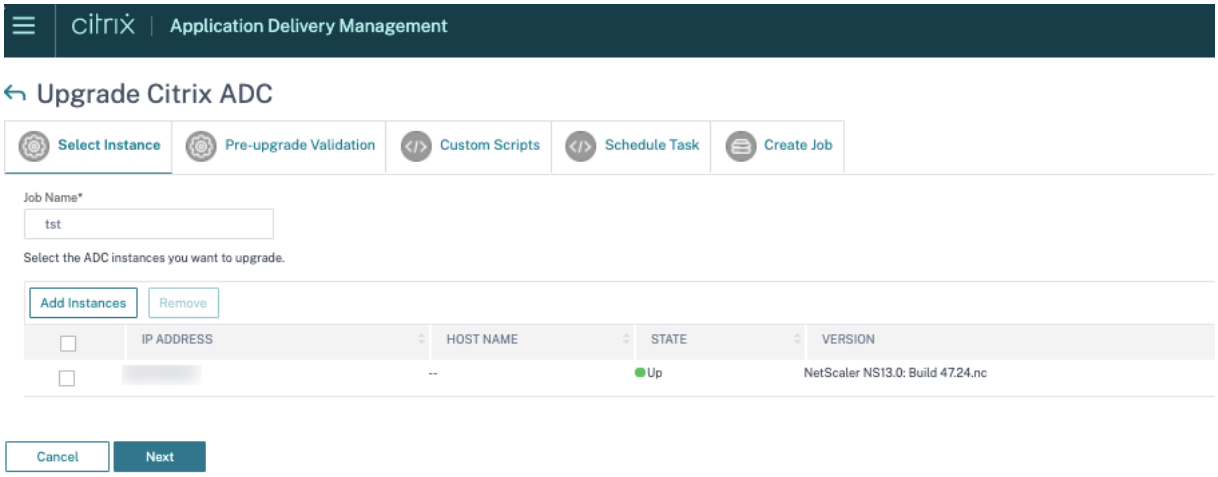
Um das Schwachstellenproblem zu beheben, wählen Sie die ADC-Instanz aus und wenden Sie die Empfehlungsbehebung an, bei der die Instanz aktualisiert wird.

- **Upgrade**: Sie können die anfälligen ADC-Instanzen auf eine Version und einen Build mit dem Fix aktualisieren. Dieses Detail ist in der Behebungsspalte zu sehen. Wählen Sie zum Upgrade die Instanz aus und klicken Sie dann auf **Weiter zum Upgrade-Workflow**. Im Upgrade-Workflow wird der anfällige ADC automatisch als Ziel-ADC ausgefüllt.

> **Hinweis**
>
> Die Releases 12.0, 11.0, 10.5 und niedriger sind bereits Ende des Lebenszyklus (EOL). Wenn Ihre ADC-Instanzen auf einer dieser Versionen ausgeführt werden, führen Sie ein Upgrade auf eine unterstützte Version durch.

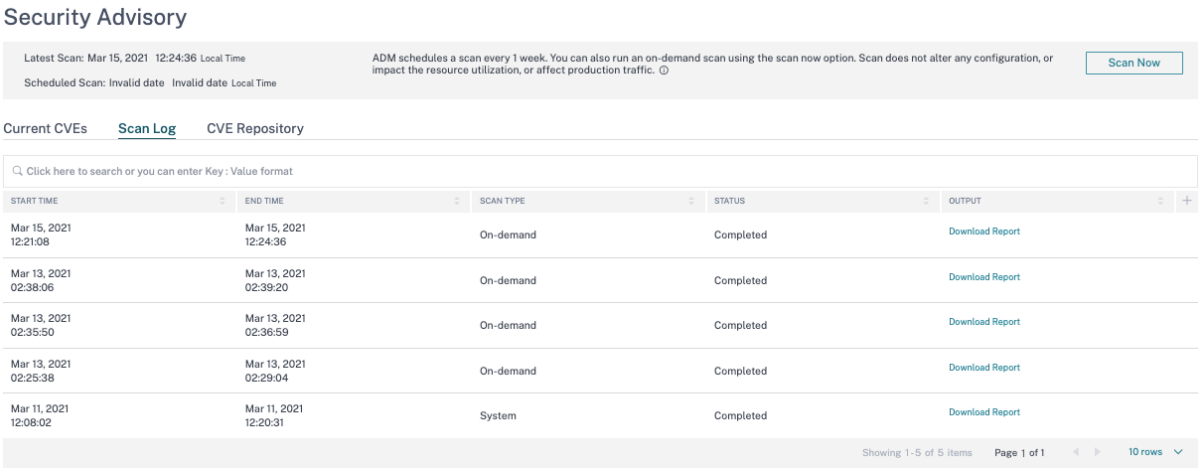
Der Upgrade-Workflow beginnt. Weitere Informationen zur Verwendung von ADM zum Upgrade von ADC-Instanzen finden Sie unter Erstellen eines ADC-Upgrade-Auftrags.

> **Hinweis**
>
> Die Version und der Build, auf die Sie upgraden möchten, liegt in Ihrem Ermessen. Lesen Sie die Ratschläge in der Behebungsspalte, um zu erfahren, welche Releases und Builds den Sicherheit-skorrektur haben, und wählen Sie entsprechend eine unterstützte Version und einen Build aus, der noch nicht das Ende der Lebensdauer erreicht hat.



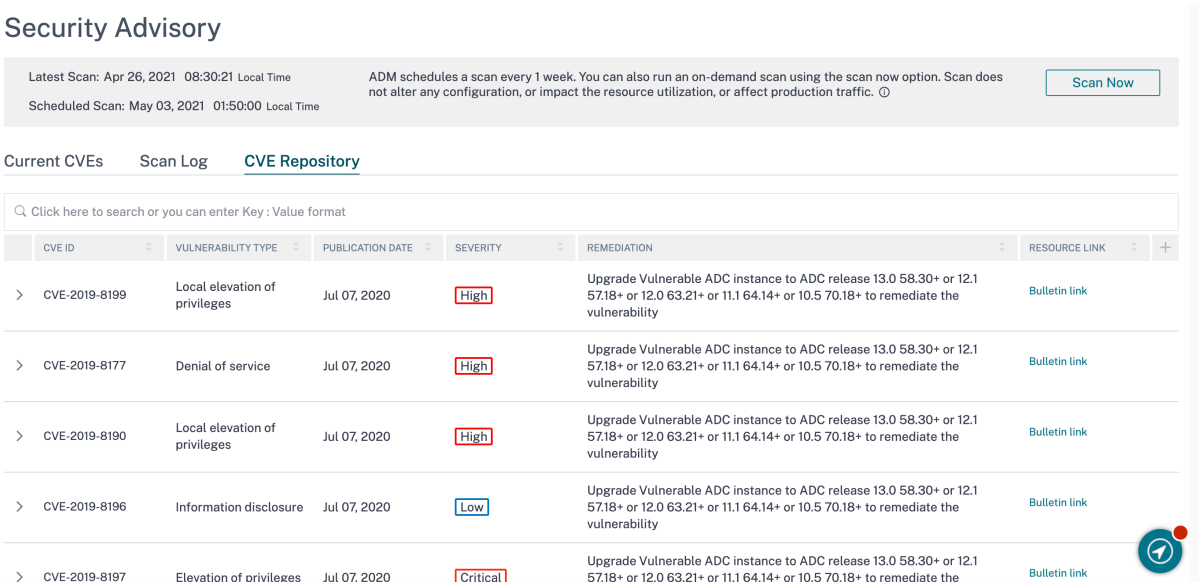
Protokoll scannen

Die Registerkarte zeigt Berichte der letzten fünf Scans, die sowohl Standardsystem-Scans als auch benutzerinitiierte Scans auf Anforderung enthalten. Sie können den Bericht jedes Scans im CSV-Format herunterladen. Wenn ein Anforderungsscan läuft, können Sie den Abschlussstatus hier einsehen. Wenn ein Scan fehlgeschlagen ist, zeigt der Status dies an.



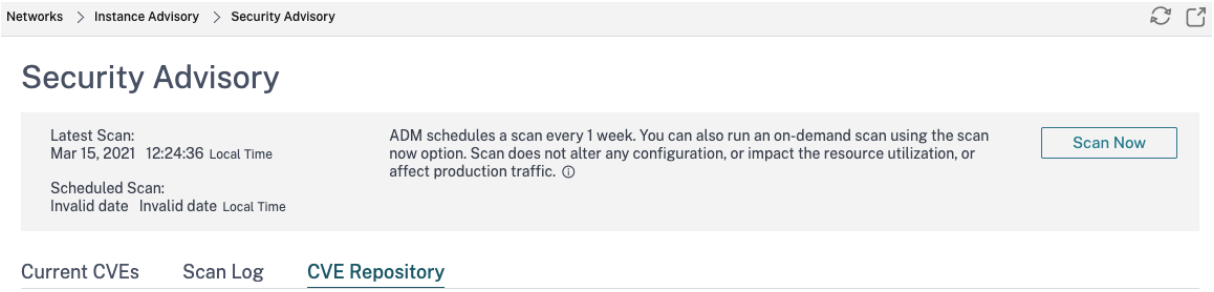
CVE-Repository

Diese Registerkarte enthält die neuesten Informationen aller CVEs ab Dezember 2019 sowie die CVE-IDs, den Schwachstellentyp, das Veröffentlichungsdatum, den Schweregrad, die Behebung und Links zu Sicherheitsbulletins.

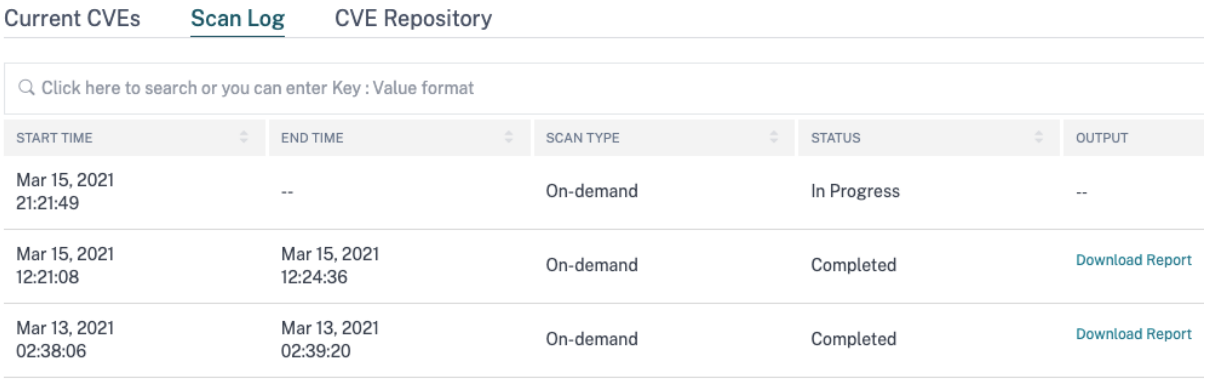


Jetzt durchsuchen

Die Sicherheitsberatung zeigt an, wann die Instanzen zuletzt gescannt wurden und wann der nächste Zeitplan fällig ist. Sie können die Instanzen auch jederzeit scannen, je nach Bedarf. Klicken Sie auf Jetzt scannen, um den neuesten Sicherheitsbericht Ihrer Instanz zu erhalten. ADM benötigt ein paar Minuten, um den Scan abzuschließen.



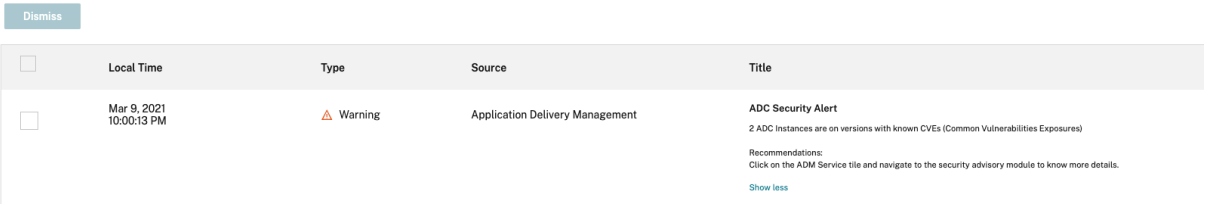
Sobald der Scanvorgang abgeschlossen ist, werden die überarbeiteten Sicherheitsdetails in der Sicherheitsinform-GUI angezeigt. Sie finden den Bericht auch unter Scan Log, den Sie auch herunterladen können.



> **Hinweis**
>
> Das Scan-Log zeigt nur die Protokolle der letzten fünf Scans an, die sowohl geplant als auch bei Bedarf erfolgen können.

Benachrichtigung

Als Administrator erhalten Sie Citrix Cloud-Benachrichtigungen, die zeigen, wie viele ADC-Instanzen anfällig sind. Um die Benachrichtigungen zu sehen, klicken Sie auf das Glockensymbol in der oberen rechten Ecke der ADM-GUI.



Anwendungen

April 28, 2021

Mit der Anwendungsanalyse- und Verwaltungsfunktion von Citrix ADM können Sie die Anwendungen mithilfe eines anwendungsorientierten Ansatzes überwachen. Dieser Ansatz hilft Ihnen:

- Überprüfen Sie die Punktzahl und analysieren Sie die Gesamtleistung der Anwendungen
- Suchen Sie nach Problemen, die mit dem Server oder Client bestehen
- Erkennung von Anomalien im Anwendungsdatenverkehr und Durchführung von Korrekturmaßnahmen

> **Hinweis**
>
> Anwendungen beziehen sich auf einen oder mehrere virtuelle Server, die auf den Instanzen konfiguriert sind (Citrix ADC).

Sie können die Anwendungen für die Zeitdauer wie 1 Stunde, 1 Tag, 1 Woche und 1 Monat überwachen.

Voraussetzungen

- Stellen Sie sicher, dass Sie Citrix ADC-Instanzen in Citrix ADM hinzugefügt haben
- Stellen Sie sicher, dass Sie über eine gültige Lizenz für Ihre Citrix ADC-Instanzen verfügen. Weitere Informationen finden Sie unter Lizenzierung
- Stellen Sie sicher, dass Sie die Lizenz für virtuelle Server angewendet haben. Weitere Informationen finden Sie unter Verwalten der Lizenzierung auf virtuellen Servern

Anwendungsübersicht

Anwendungen können sein:

- Diskrete Anwendungen
- Benutzerdefinierte Anwendungen
- Microservices-Anwendungen (k8s_discrete)

Diskrete Anwendungen

Alle virtuellen Server, die lizenziert sind, werden als diskrete Anwendungen bezeichnet.

Benutzerdefinierte Anwendungen

Die virtuellen Server unter einer Kategorie werden als benutzerdefinierte Anwendungen bezeichnet. Als Administrator müssen Sie benutzerdefinierte Anwendungen basierend auf einer Kategorie hinzufügen. Anschließend können Sie die Anwendungen über das Dashboard verwalten und überwachen. Sie erhalten eine einfache Überwachung bestimmter Anwendungen, die in einer Kategorie gruppiert sind.

Sie können beispielsweise eine Kategorie für Ihr Rechenzentrum1 erstellen und dessen ADC-Instanzen hinzufügen. Nachdem Sie eine Kategorie definiert und die Instanz für Ihr Rechenzentrum1 hinzugefügt haben, wird das Anwendungs-Dashboard mit einer separaten Kategorie angezeigt, die alle Anwendungen umfasst, die sich auf Ihr Rechenzentrum beziehen.

Punkte zu beachten

- Die diskreten Anwendungen, die den benutzerdefinierten Anwendungen hinzugefügt werden, werden aus den diskreten Anwendungen entfernt.
- Alle Anwendungen, die keiner Kategorie hinzugefügt werden, stehen als **Andere** zur Verfügung.
- Standardmäßig können Sie mit Citrix ADM Lizenzen für bis zu zwei Anwendungen hinzufügen. Abhängig von Ihrer Lizenz können Sie Lizenzen für die Anwendungen auswählen und anwenden, die Sie überwachen möchten.

Microservices-Anwendungen

In einem Kubernetes-Cluster stellt Citrix einen Ingress Controller für Citrix ADC MPX (Hardware), Citrix ADC VPX (virtualisiert) und Citrix ADC CPX (containerisiert) bereit. Weitere Informationen finden Sie unter Citrix Ingress Controller.

Die diskreten Anwendungen, die mit den Citrix ADC CPX-Instanzen konfiguriert werden, werden als Microservices-Anwendungen bezeichnet.

Anwendungsmanagement und Anwendungs-Dashboard

April 28, 2021

Mit Citrix ADM können Sie Anwendungen auf der Seite **Anwendungen** verwalten und Anwendungsdetails auf der Seite **Dashboard** anzeigen.

Anwendungen verwalten

Auf der Seite **Anwendungen** können Sie alle benutzerdefinierten und diskreten Anwendungen anzeigen.

Auf der Seite Anwendungen können Sie als Administrator folgende Aufgaben ausführen:

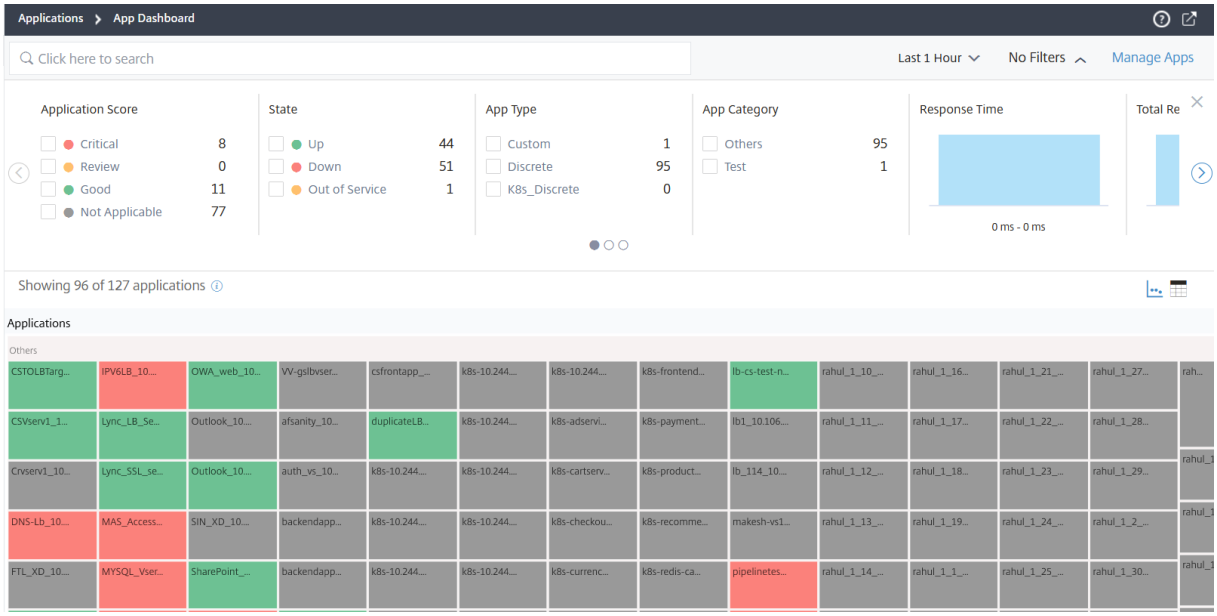
- Hinzufügen von Anwendungen
- Anzeigen von Anwendungsdetails wie App-Name, App-Typ, App-Kategorie, zugeordnete virtuelle Server, zugeordnete Dienste usw.
- Bearbeiten oder Löschen von benutzerdefinierten Anwendungen

Nachdem Sie Anwendungen hinzugefügt, bearbeitet oder gelöscht haben, werden die Details sofort auf der Seite “Anwendungen” angezeigt.

Weitere Informationen finden Sie unter Anwendungen verwalten.

Anwendungs-Dashboard

Navigieren Sie zu **Anwendungen** > **Dashboard**, um die Liste der Anwendungen entweder in der tabellarischen Ansicht oder in der Diagrammansicht anzuzeigen.



Alle Anwendungen werden erst dann im Dashboard angezeigt, wenn die Anwendungen mit dem Auffüllen von Daten beginnen. Klicken Sie im Dashboard auf eine Anwendung, um detaillierte Informationen zur Anwendungsleistung anzuzeigen. Weitere Informationen finden Sie unter Anwendungsdetails.

Wenn die Anwendungsanalyse auch nach etwa 10 bis 15 Minuten Dauer nicht angezeigt wird, führen Sie die Schritte zur Fehlerbehebung unter aus Problembehandlung bei App-Dashboard.

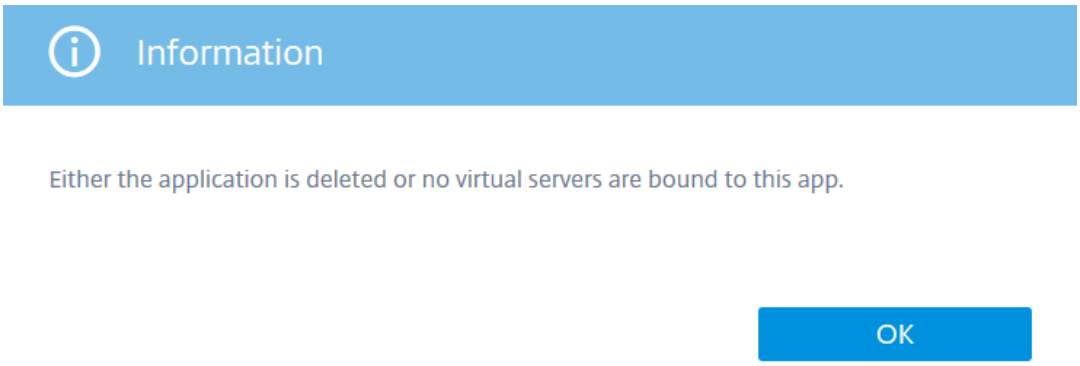
Aktualisierungen im neuen Dashboard-Verhalten im Vergleich zum früheren Dashboard

- Nachdem Sie eine benutzerdefinierte Anwendung hinzugefügt oder bearbeitet haben, kann es einige Minuten dauern, bis die Anwendung im Dashboard wiedergegeben wird.
- Wenn Sie eine benutzerdefinierte Anwendung löschen, zeigt das Dashboard weiterhin die gelöschte Anwendung an, bis ADM über die Analysedaten verfügt (maximal 1-Monats-Dauer).

  Betrachten Sie ein Szenario, dass Sie eine Anwendung am 2. Januar 2020 erstellt haben und Sie die Anwendung am 4. Januar 2020 gelöscht haben. Für dieses Szenario gilt:

  - Das Dashboard kann die gelöschte Anwendung am 4. Januar 2020 weiterhin anzeigen, wenn Sie die Zeitdauer für den letzten Tag, eine Woche und einen Monat auswählen.
  - Das Dashboard kann die gelöschte Anwendung am 5. Januar 2020 weiterhin anzeigen, wenn Sie die Zeitdauer für die letzten 1 Woche und 1 Monat auswählen.

- Wenn die Dauer das Löschdatum der App überschreitet, wird die Anwendung nicht im Dashboard angezeigt. Das heißt, das Dashboard wird nicht mit der gelöschten Anwendung am 6. Januar 2020 (für den letzten 1 Tag), 12. Januar 2020 (für die letzte 1 Woche) und nach dem 5. Februar 2020 (für den letzten 1 Monat) angezeigt.
- Wenn Sie im Dashboard auf die gelöschte Anwendung klicken, wird die folgende Meldung angezeigt.

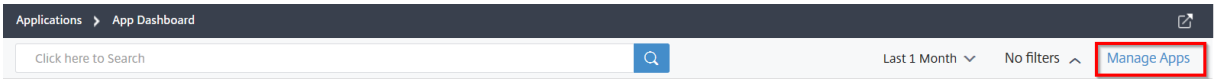


> **Hinweis**
>
> Wenn die zugeordnete Citrix ADC-Instanz nach dem Hinzufügen einer Anwendung “Heruntergefahren”, “außer Betrieb” ist oder aufgrund eines temporären Netzwerkfehlers nicht erreichbar ist:
>
> -Die der ADC-Instanz zugeordneten Anwendungen sind nur auf der Seite **Anwendungen**, jedoch nicht im Dashboard sichtbar.
>
> -Die Anwendungen werden im Dashboard angezeigt, nachdem die ADC-Instanz hochgefahren ist.

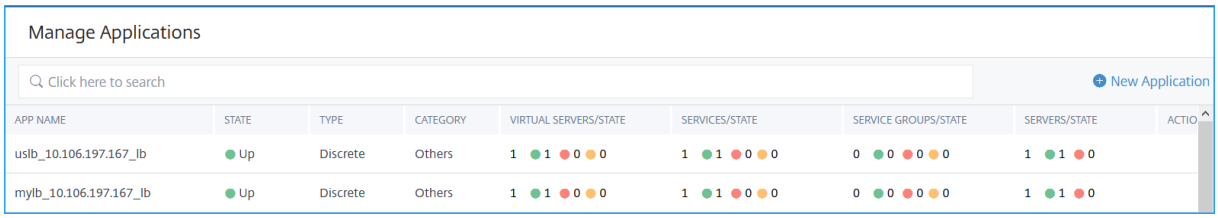
Anwendungen verwalten

April 28, 2021

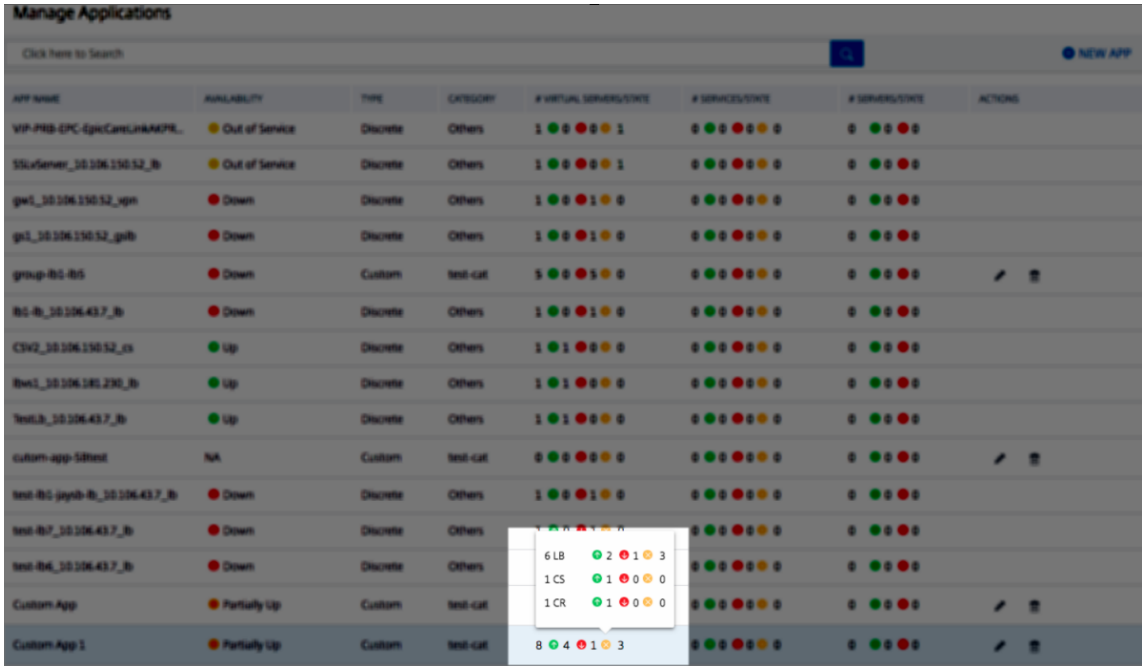
Klicken Sie im Dashboard auf **Apps verwalten**, um Anwendungsdetails anzuzeigen und benutzerdefinierte Anwendungen hinzuzufügen, zu bearbeiten oder zu löschen.



Anwendungsdetails anzeigen



- **App-Name** — Bezeichnet den Anwendungsnamen
- **Status** — Gibt den aktuellen Anwendungsstatus an, z. B. Nach **oben**, **Runter**, **Teilweise nach oben**, **Außerhalb des Dienstes**und **NA**
  - **Up** — Alle virtuellen Server, die der Anwendung zugeordnet sind, sind betriebsbereit.
  - **Heruntergefahren** — Alle virtuellen Server, die der Anwendung zugeordnet sind, sind Down
  - **Teilweise hochgefahren** — Entweder ist eine virtuelle, die der Anwendung zugeordnet ist, heruntergefahren oder außer Betrieb.
  - **Out of Service** — Alle virtuellen Server, die mit den Anwendungen verknüpft sind, sind außer Betrieb
  - **NA** — Es sind keine virtuellen Server für die Anwendung konfiguriert
- **Typ** — Gibt an, ob die Anwendung zu Custom oder Discrete gehört
- **Kategorie** — Bezeichnet die Anwendungskategorie, die gruppiert ist
- **Virtueller Server/Status** — Bezeichnet die gesamte konfigurierte virtuelle Server und den Status aller virtuellen Server. Bewegen Sie den Mauszeiger, um Details anzuzeigen, wie z. B. die Gesamtanzahl der virtuellen Server, der virtuelle Servertyp und der Status des virtuellen Servers.

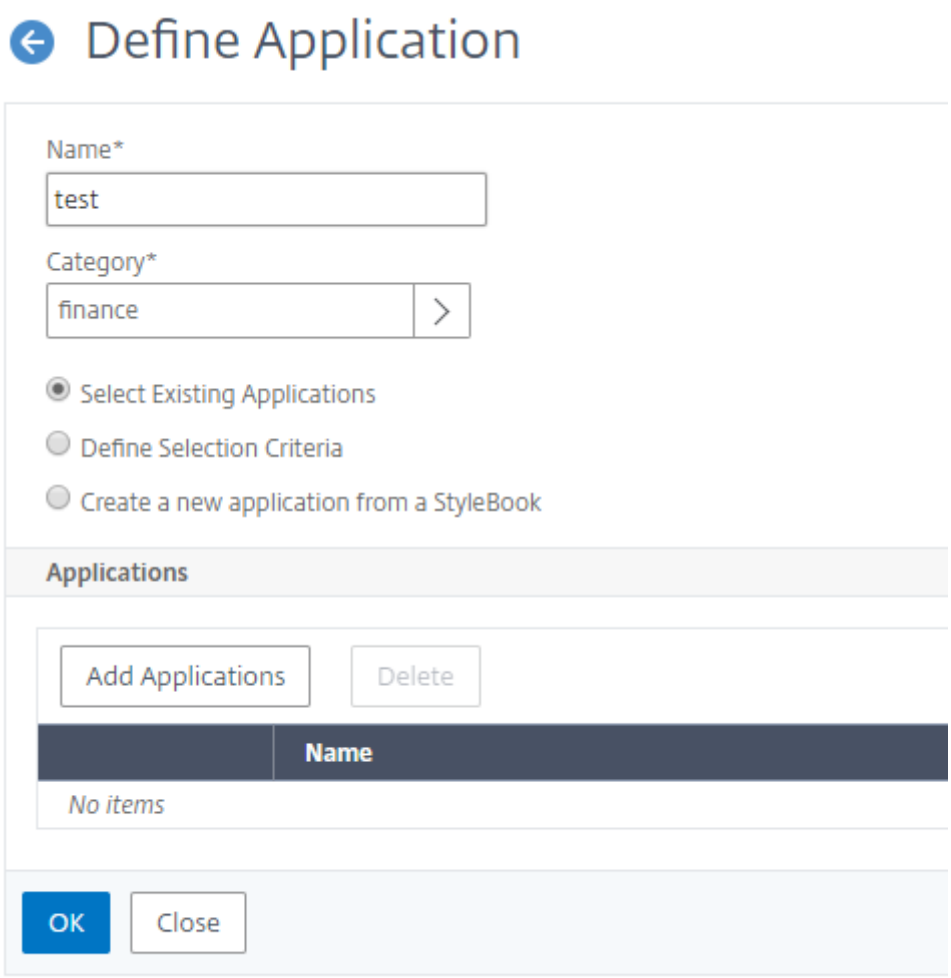


- **Dienstleistungen/Status** — Bezeichnet die Gesamtanzahl der konfigurierten Dienste und den Status aller Dienste
- **Service Goups/State** — Bezeichnet die gesamten konfigurierten Servicegruppen und den Status aller Servicegruppen
- **Server/Status** — Bezeichnet die Gesamtanzahl der für die Anwendung konfigurierten Server und den Status aller Server
- **Aktionen** — Ermöglicht das Bearbeiten oder Löschen von benutzerdefinierten Anwendungen

Hinzufügen einer Anwendung

1. Klicken Sie auf **Neue Anwendung**, um eine Anwendung zu erstellen

Die Seite **“Anwendung definieren** “ wird angezeigt.



> **Hinweis**
>
> Sie können auch auf **Anwendungen** klicken und dann **Neue Anwendung auswählen, um eine Anwendung** zu erstellen.

2. Legen Sie die folgenden Parameter fest:

Feld	Beschreibung
Name	Der Name der benutzerdefinierten Anwendung. Zum Beispiel LB_TEST.

Feld	Beschreibung
Kategorie	Die Kategorie, in der Sie die Anwendungen gruppieren können. Klicken Sie hier, um die Seite Anwendungskategorie zu erhalten. Wählen Sie die Kategorie aus und klicken Sie auf **Auswählen**. So fügen Sie eine Kategorie hinzu:
	1. Klicken Sie auf **Hinzufügen**
	2. Geben Sie einen Namen Ihrer Wahl ein.
	3. Klicken Sie auf **Erstellen**
Vorhandene Anwendungen auswählen	Ermöglicht die Auswahl der vorhandenen Anwendungen, die den Citrix ADC-Instanzen hinzugefügt wurden.
Anwendung hinzufügen	Zeigt alle virtuellen Server an, die auf den Instanzen konfiguriert sind. Wählen Sie die Anwendungen aus der Liste aus, und klicken Sie auf **OK**.
Auswahlkriterien definieren	Option zur Definition der Anwendung nach virtuellem Serverbereich oder nach Ursprungsserver/Dienst-IP-Adressbereich.
	- **Server.** Geben Sie die Server- oder Dienst-IP-Adresse, den Servernamen oder den Port des Back-End-Servers an, auf dem die Anwendungen ausgeführt werden. Sie können eine IP-Adresse, einen Bereich von IP-Adressen oder eine Kombination von beiden durch Kommas getrennt eingeben. Sie können beispielsweise 10.102.29.20, 10.102.43.10-60, 10.216.43.45 eingeben.

Feld	Beschreibung
	- **Virtuelle Server.** Sie können entweder eine der folgenden Optionen angeben: IP-Adresse des virtuellen Servers, Name des virtuellen Servers oder Port des Back-End-Servers, auf dem die Anwendungen ausgeführt werden. Sie können eine IP-Adresse oder einen Bereich von IP-Adressen oder eine Kombination von beiden durch Kommas getrennt eingeben. Sie können beispielsweise 10.102.29.20, 10.102.43.10-60, 10.216.43.45 eingeben.
Erstellen einer Anwendung aus einem StyleBook	Ermöglicht das Erstellen einer Anwendung mit dem StyleBook. Weitere Informationen finden Sie unter Erstellen Sie eine Anwendung mit dem StyleBook.

a) Klicken Sie auf **OK**.

> **Hinweis**
>
> Derzeit unterstützt Application Dashboard nur virtuelle Server für Lastausgleich und Content Switching.

Das Anwendungs-Dashboard wird nun mit der Kategorie angezeigt und alle Anwendungen sind darunter gruppiert.

Wenn Sie eine Anwendung mit StyleBooks erstellen, bestätigen Sie die erforderliche Lizenzverwendung während der Anwendungsbereitstellung.

Klicken Sie auf **Ja**, um die Bestätigungsmeldung anzuzeigen. Der ADM weist einer Anwendung die erforderlichen Lizenzen zu.

Erstellen Sie eine Anwendung mit dem StyleBook

So erstellen Sie eine Anwendung mit dem StyleBook:

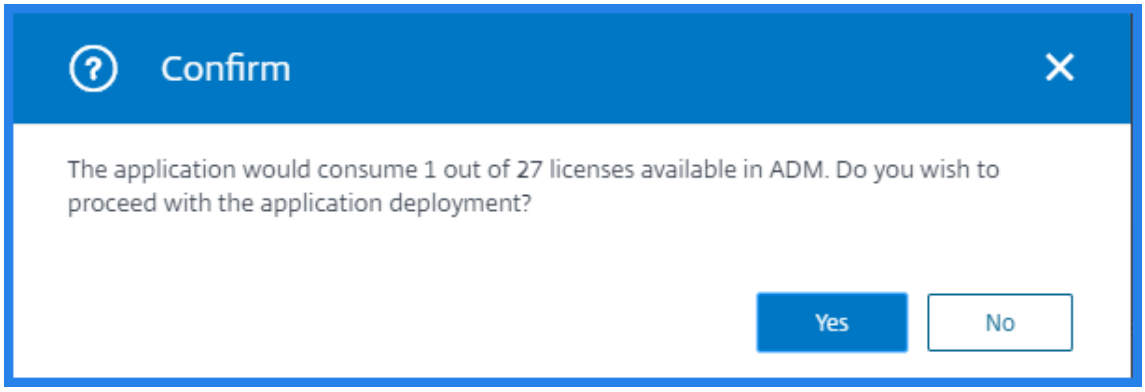
1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Dashboard**, und klicken Sie auf **Benutzerdefinierte App definieren**, um eine benutzerdefinierte Anwendung zu erstellen.
2. Geben Sie auf der Seite **Anwendung definieren** den Namen der Anwendung in das Feld **Name** ein.

3. Wählen Sie im Abschnitt Kategorie die Anwendungskategorie aus. Mit Citrix ADM können Sie Kategorien definieren, um die benutzerdefinierten Anwendungen zu gruppieren. Sie können bei Bedarf auch weitere Kategorien hinzufügen.
4. Klicken Sie auf **Neue Anwendung aus einem StyleBook erstellen**, und klicken Sie auf **OK**.

   Die Seite StyleBook auswählen wird angezeigt. Diese Seite enthält alle standardmäßigen StyleBooks, die in Citrix ADM verfügbar sind.
5. Wählen Sie das StyleBook aus.
   Die Seite **Konfigurationsdetails** wird angezeigt.
6. Geben Sie die Werte für alle Parameter im StyleBook ein. Sie können auch auf View Definition klicken, um das Konstrukt des StyleBook anzuzeigen, bevor Sie es verwenden.

   Weitere Informationen finden Sie unter Standard-StyleBooks verwenden.
7. Klicken Sie auf **Erstellen**.

   Es wird eine Bestätigungsmeldung angezeigt, um erforderliche Lizenzen zu verbrauchen und eine Anwendung bereitzustellen. Im Folgenden finden Sie eine Beispielmeldung:

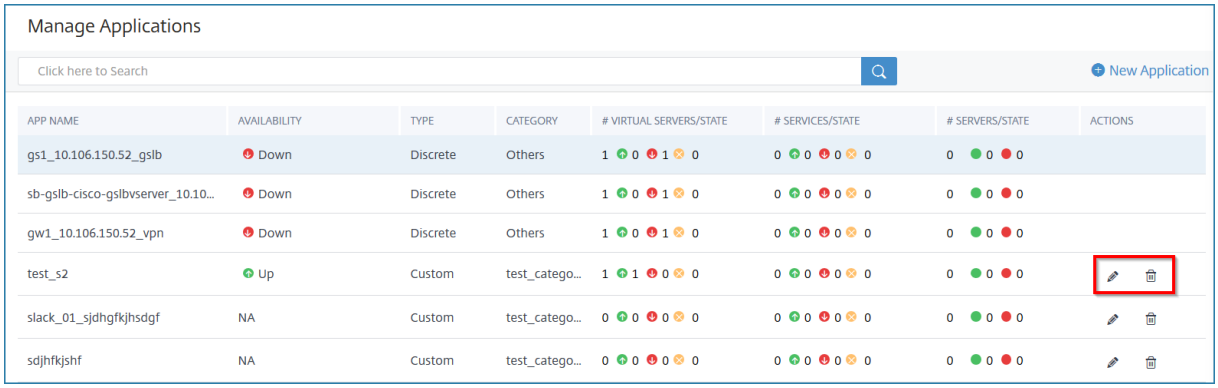


8. Klicken Sie auf **Ja**.

Sie können auch auf **Dry Run** klicken, um die Konfigurationen zu überprüfen, die Citrix ADM auf der ausgewählten Citrix ADC-Instanz zu erstellen versucht. Diese Option ist nur für Ihren Testzweck, um die endgültige Überprüfung der Konfigurationen zu sehen. Selbst wenn die Option Trockenlauf erfolgreich ist, kann die tatsächliche Konfiguration auf dem ausgewählten Citrix ADC aus verschiedenen Gründen weiterhin fehlschlagen (IP-Konflikt, Instanz nicht erreichbar usw.).

Bearbeiten oder Löschen einer Anwendung

Auf der Seite " **Anwendungen** " können Sie die benutzerdefinierten Anwendungen entweder bearbeiten oder löschen. Klicken Sie auf die Schaltfläche "Bearbeiten", um eine Anwendung zu bearbeiten, und klicken Sie auf die Schaltfläche "Löschen", um die Anwendung zu entfernen.



Exportieren von Berichten über App-Dashboard und Sicherheits-Dashboard

Mit Citrix ADM können Sie einen Snapshot des aktuellen App Dashboards erstellen und als Berichte exportieren. In einem häufigen Zeitintervall müssen die App-Administratoren möglicherweise diese Berichte verwenden, um die App-Nutzung und Leistungseinbußen zu aktualisieren.

Mit dieser Funktion können die Administratoren diese Daten als PNG-, JPEG- oder PDF-Berichte extrahieren.

> **Hinweis**
>
> Im Gegensatz zu anderen Berichtsexportoptionen in Citrix ADM können Sie die Berichte App Dashboard und Security Dashboard nur als PDF- oder PNG-Dateien exportieren. Das CSV-Format wird derzeit nicht unterstützt.

Der Bericht wird auf Ihr System heruntergeladen. Auf den Seiten App Dashboard und App Security Dashboard können Sie auch zu Seiten der zweiten Ebene navigieren und als Berichte exportieren. Derzeit können Sie Berichte zu jeweils nur einer Anwendung herunterladen.

Automatisieren Sie die SSL-Zertifikatsverwaltung

April 28, 2021

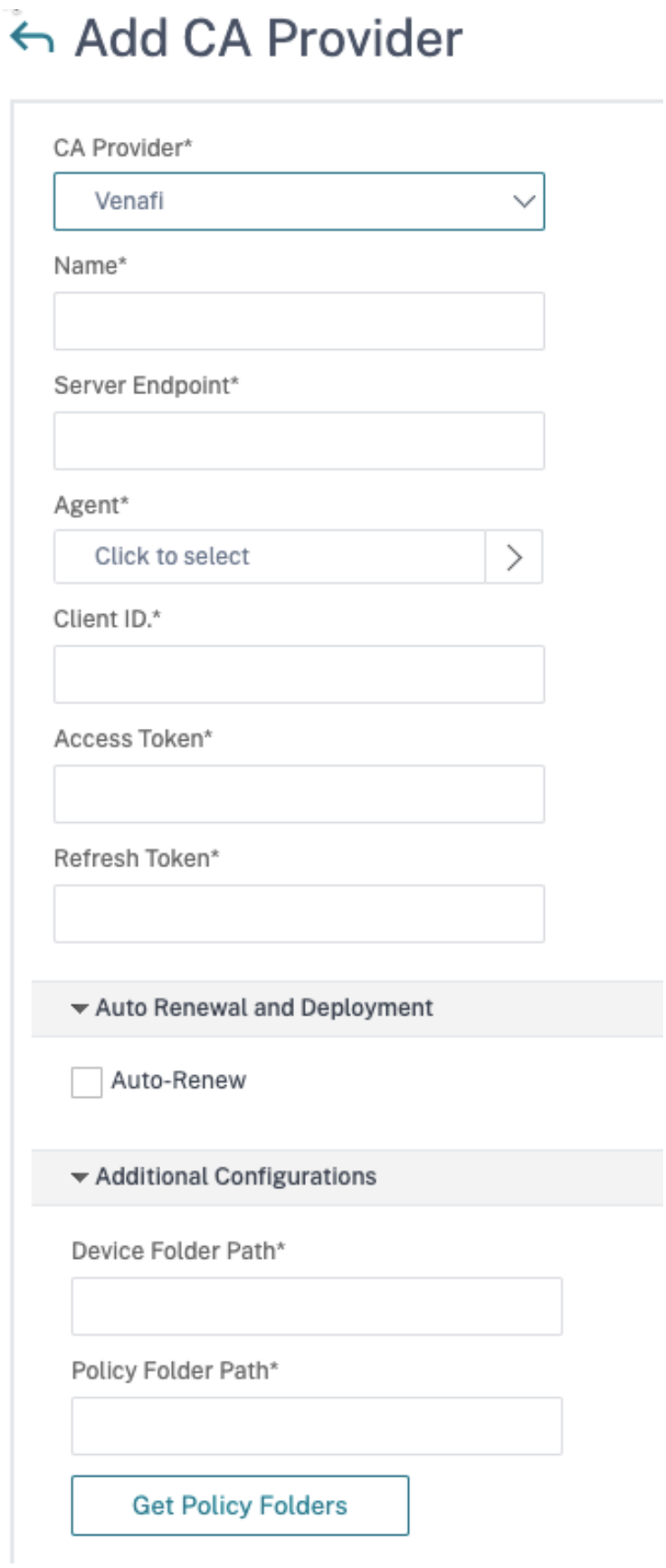
Um die digitale Sicherheit aufrechtzuerhalten, müssen Sie die Verwaltung von SSL-Zertifikaten in Ihrer Umgebung automatisieren. Sie benötigen Möglichkeiten, alle Zertifikate proaktiv zu verwalten und zu überwachen, Sie über die für den Ablauf fälligen Zertifikate zu informieren und die Zertifikate automatisch zu erneuern, bevor sie ablaufen. Abgelaufene SSL-Zertifikate führen zu Sicherheitsrisiken. Sie können Server der Venafi Trust Protection Platform mit ADM konfigurieren, um die Verwaltung von SSL-Zertifikaten zu automatisieren, die auf ADC-Instanzen installiert sind.

Durch die Verwendung von Venafi mit ADM können Sie die SSL-Zertifikate über den gesamten Lebenszyklus verwalten. Sie können die folgenden Aufgaben im **ADM-Anwendungs-Dashboard** ausführen:

- Überprüfen Sie SSL-Probleme und Anwendungsbewertungen.
- Beheben Sie SSL-Probleme und wenden Sie vorgeschlagene Behebungen an.
- Prüfen Sie die an eine Anwendung gebundenen Zertifikate.
- Erstellen, installieren und erneuern Sie schnell Zertifikate.
- Automatisieren Sie die Erneuerung von Zertifikaten.
- Sichern Sie Anwendungen, indem Sie generierte Zertifikate an virtuelle ADC-Server binden.
- Überprüfen Sie alle SSL-Aufgabenprotokolle für eine bestimmte Anwendung.

Konfigurieren eines Venafi-Servers auf ADM

Die Konfiguration eines Venafi-Servers erfolgt in zwei Schritten. Zuerst fügen Sie den Venafi-Server auf ADM hinzu. Als Nächstes konfigurieren Sie die Richtlinien auf dem Venafi-Server. Um den Venafi-Server auf ADM hinzuzufügen, navigieren Sie von der ADM-GUI aus durch **Netzwerk > SSL-Dashboard > Drittanbieter-CA**. Klicken Sie auf **Hinzufügen**.

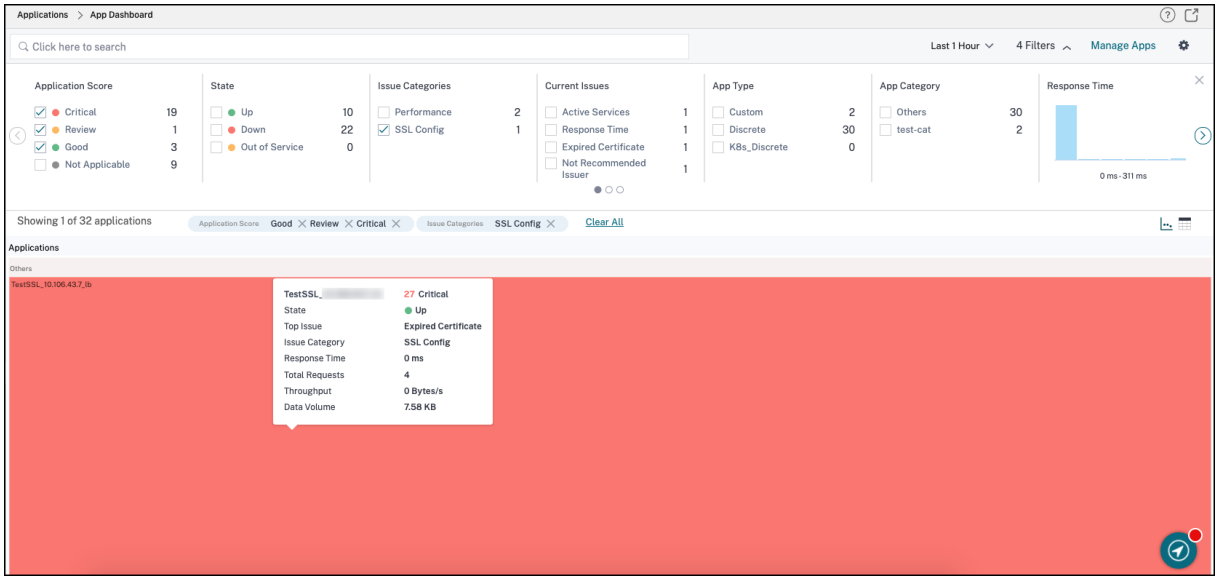


Geben Sie die Details in die dafür vorgesehenen Felder ein. Aktivieren Sie die Option **Automatische Verlängerung**, wenn Sie möchten, dass die Zertifikate automatisch verlängert werden. Um Details zu jedem Feld zu erhalten, bewegen Sie den Mauszeiger über das Feld und klicken Sie auf das i Symbol.

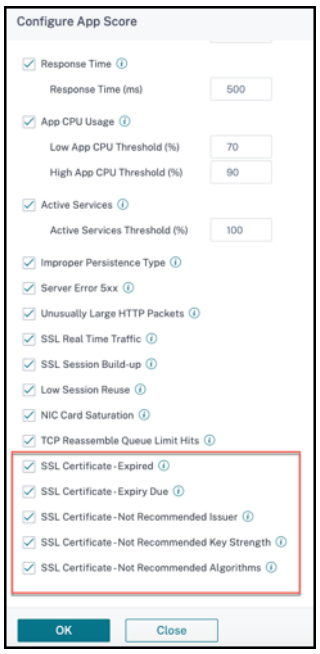
Nachdem Sie den Venafi-Server konfiguriert haben, können Sie das ADM-Dashboard verwenden, um Ihre SSL-Zertifikate zu verwalten.

Verwalten des Lebenszyklus von SSL-Zertifikaten

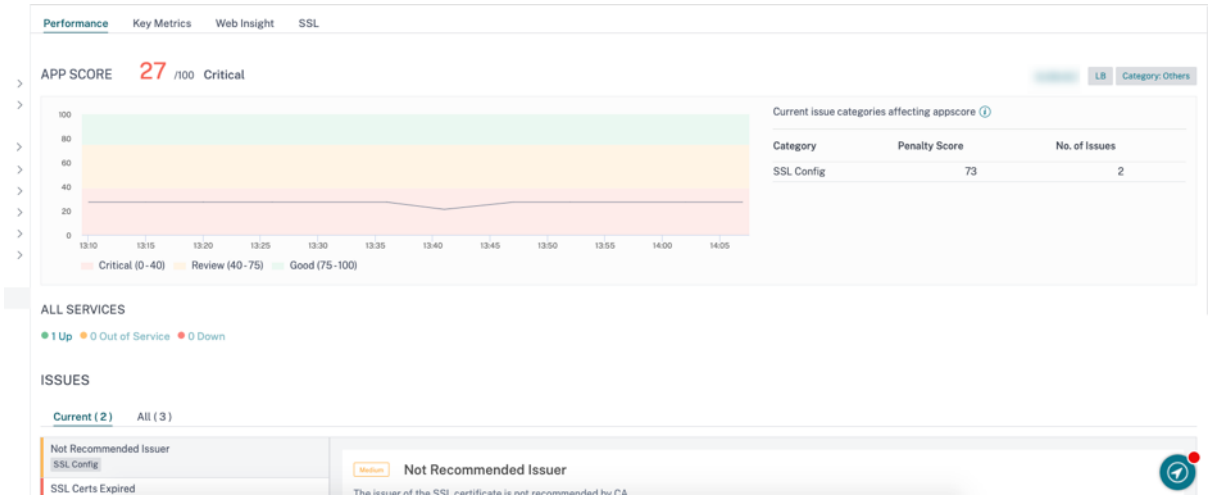
Das Anwendungs-Dashboard ist eine zentrale Anlaufstelle, um Ihre SSL-Zertifikate von Anfang bis Ende zu verwalten. Navigieren Sie von der ADM-GUI zu **Anwendungen > App Dashboard**. Wählen Sie unter **Problemkategorien** die Option **SSL Config**aus. Unter **Aktuelle Probleme**sehen Sie die SSL-bezogenen Probleme Ihrer Anwendungen. Um den SSL-Bericht anzuzeigen, bewegen Sie den Mauszeiger unter **Anwendungen**über die App. Um Details zum Bericht anzuzeigen, klicken Sie auf die App. In diesem Beispiel haben wir eine Anwendung mit einer Punktzahl von 27.



Darüber hinaus können Sie Ihre Probleme mithilfe von **Anwendungsbewertungen** wie kritisch oder überprüfen filtern. Die SSL-Anwendungsbewertungen basieren auf SSL-Parametern, die standardmäßig unter Einstellungen für **Apps verwalten** in der oberen rechten Ecke des Dashboards aktiviert sind.

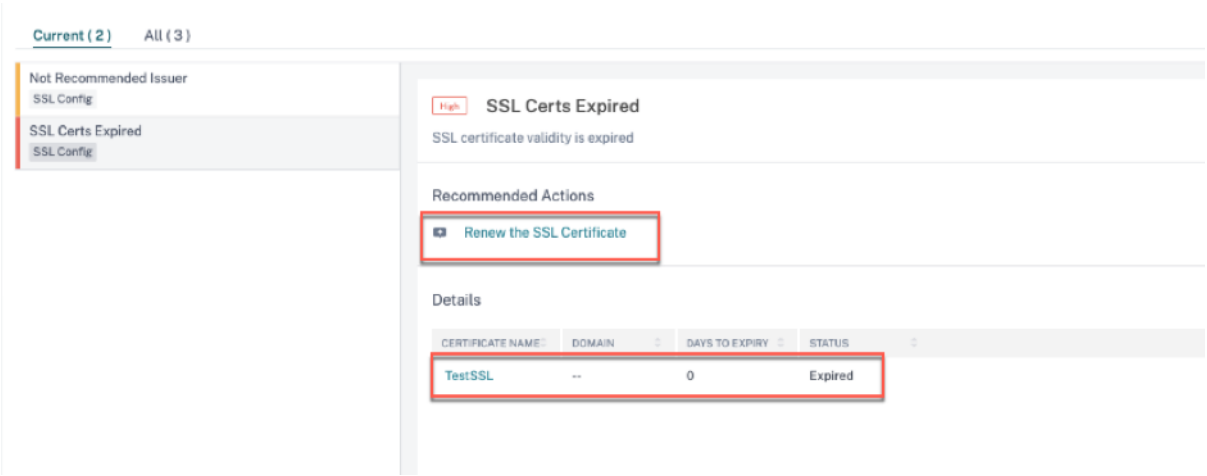


Um einen der SSL-Parameter zu deaktivieren, deaktivieren Sie das Kästchen und klicken Sie auf **OK**. Um die Details des SSL-Berichts anzuzeigen, klicken Sie unter **Anwendungen**auf die App, für die Sie den Bericht sehen möchten.



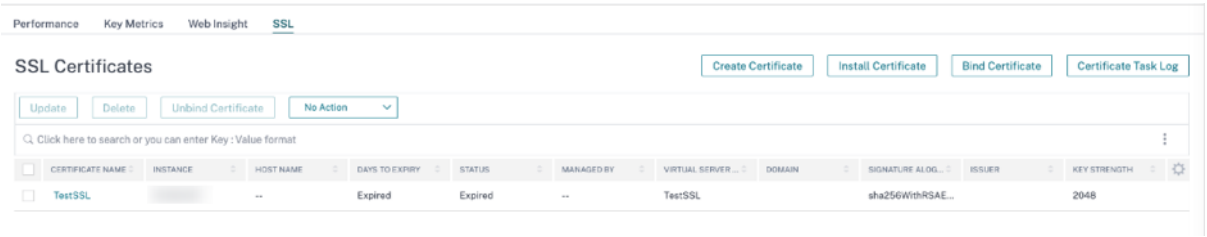
Sie können die Leistungsbewertung überprüfen und die Seite nach unten scrollen, um Details wie die virtuellen Server der App und die an die virtuellen Server gebundenen Zertifikate und die Probleme mit den Zertifikaten anzuzeigen. Um Details zum Zertifikat anzuzeigen, klicken Sie auf den Link unter **Zertifikatsname**. Für ein abgelaufenes Zertifikat können Sie es verlängern.

Die Erneuerung des Zertifikats umfasst das Erstellen des Zertifikats, die Installation und das Binden an den virtuellen Server.

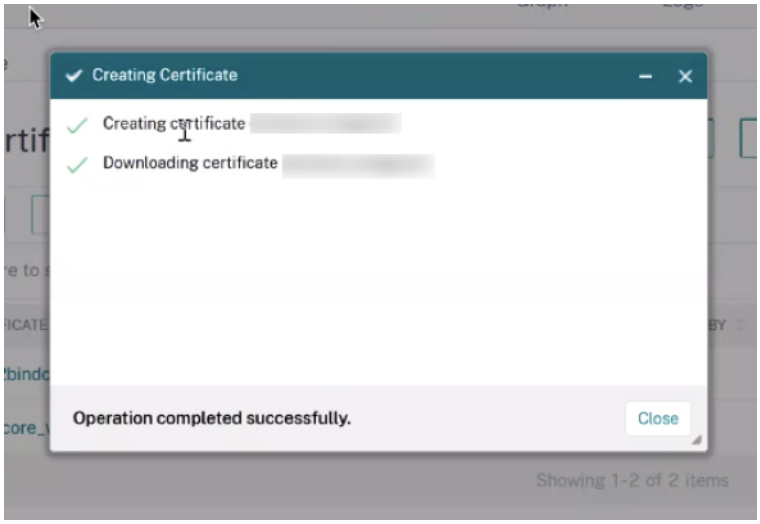


> **Hinweis**
>
> Wenn Sie einen Venafi-Server auf ADM hinzufügen und die Option zur automatischen Verlängerung aktivieren, werden die Zertifikate vor Ablauf automatisch erneuert.

Wenn Sie auf **SSL-Zertifikat verlängern** klicken, gelangen Sie auf die Registerkarte SSL, auf der alle Zertifikate aufgeführt sind, die an die virtuellen Server der Anwendung gebunden sind. Auf dieser Registerkarte können Sie Zertifikate erstellen und installieren und an die virtuellen Server binden. Außerdem können Sie alle SSL-aufgabenbezogenen Protokolle für eine bestimmte Anwendung in den SSL-Aufgabenprotokollen für eine bestimmte Anwendung überprüfen.

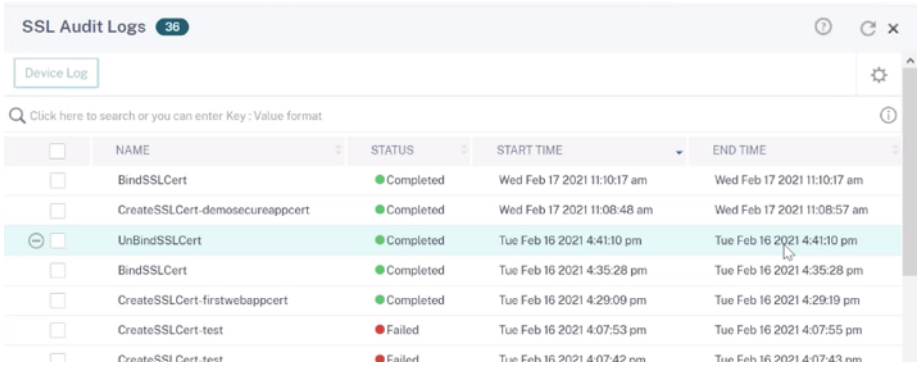


Um ein Zertifikat zu erstellen, klicken Sie auf **Zertifikat erstellen** und geben Sie die Details ein. Geben Sie ein Kennwort ein, da die heruntergeladenen Zertifikate verschlüsselt sind und klicken **Sie** ADM kontaktiert den Venafi-Server, um das Zertifikat zu erstellen. Klicken Sie auf **Schließen**, wenn das Zertifikat heruntergeladen wird.



Klicken Sie anschließend auf der Registerkarte SSL auf **Zertifikat installieren**. Wählen Sie das heruntergeladene Zertifikat aus und klicken Sie auf **Installieren**. Weitere Informationen zum Installieren einer SSL-Zertifikates in ADC über ADM finden Sie im Abschnitt zur Installation eines SSL-Zertifikats von Citrix ADM unter Installieren von SSL-Zertifikaten auf einer Citrix ADC-Instanz.

Klicken Sie als Nächstes auf **Zertifikat binden**. Sie können bei Bedarf auch die Bindung eines Zertifikats aufheben. Nach der nächsten SSL-Abfrage wird das Anwendungs-Dashboard mit den neuen Daten aktualisiert. Wenn Sie alle SSL-Aufgabenprotokolle für eine bestimmte Anwendung überprüfen möchten, klicken Sie auf **Zertifikataufgabenprotokoll**.

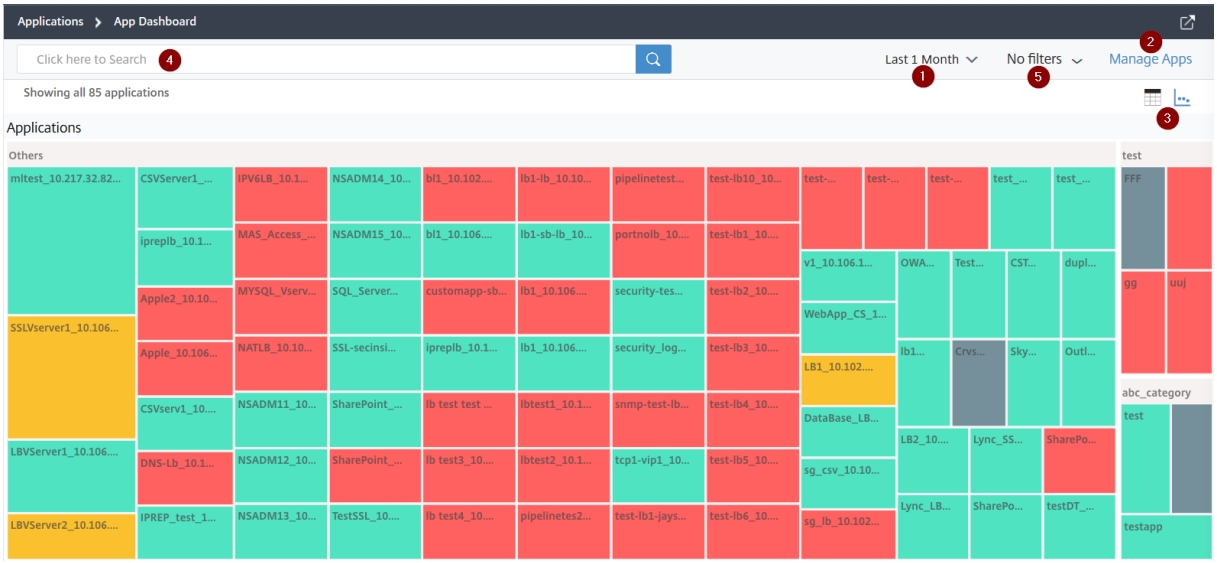


Übersicht über das Anwendungs-Dashboard

April 28, 2021

Das Anwendungs-Dashboard zeigt die diskreten Anwendungen unter **Andere** und die benutzerdefinierten Anwendungen an, die unter den jeweiligen Kategorien gruppiert sind.

Navigieren Sie zu **Anwendung** > **Dashboard**, um das App-Dashboard anzuzeigen.



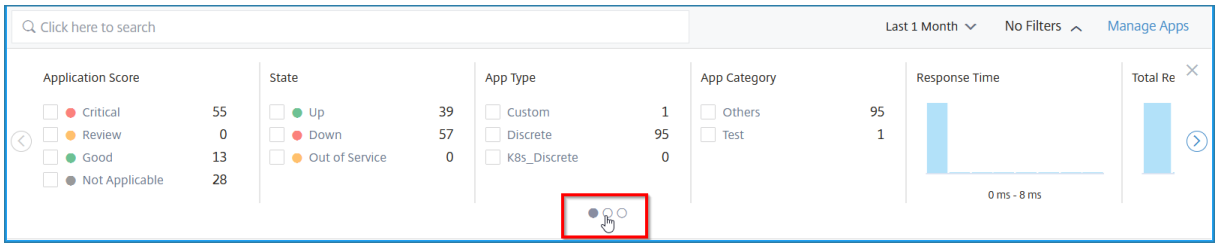
1 — Zeigt die Anwendungsdetails für die ausgewählte Zeitdauer an, z. B. 1 Stunde, 1 Tag, 1 Woche und 1 Monat.

2 — Ermöglicht Ihnen das Verwalten von Anwendungen und das Hinzufügen neuer Anwendungen

3 — Ermöglicht das Anzeigen von Anwendungen entweder in der Tabellenansicht oder in der Diagrammansicht

4 — Ermöglicht es Ihnen, eine Anwendung über die Suchleiste zu suchen

5 — Ermöglicht das Anwenden von Filtern zur Anzeige von Anwendungen. Klicken Sie hier, um Details anzuzeigen.

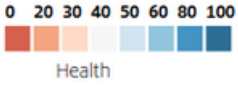


Sie können den Karussell-Schieberegler auswählen, der Ihnen den Zugriff auf alle Optionen erleichtert.

Sie haben folgende Möglichkeiten:

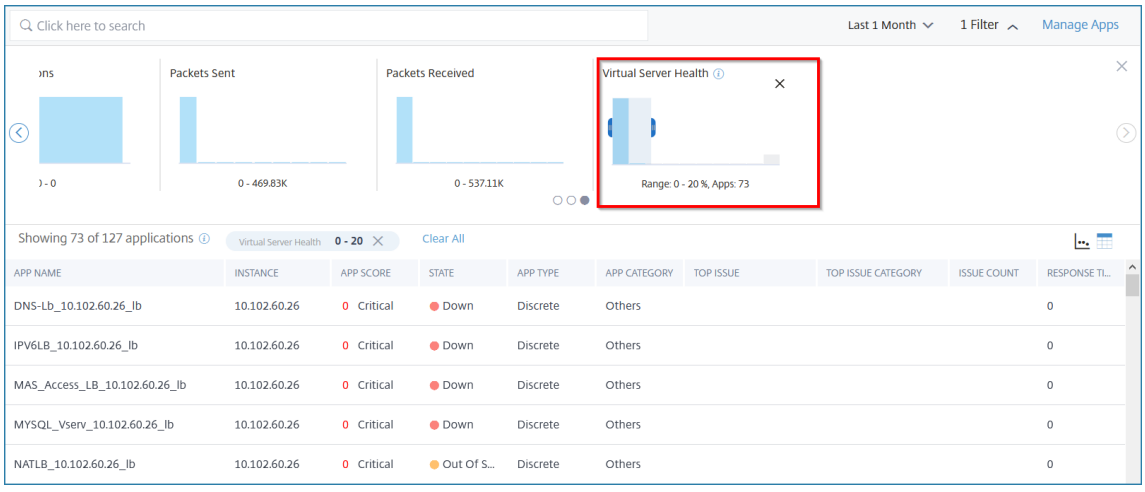
- Wählen Sie diese Option aus, um Anwendungen basierend auf den Ergebnissen anzuzeigen.
  - **Kritisch** — Anwendungsbewertung liegt zwischen 0 und < 40
  - **Fair** — Anwendungsbewertung liegt zwischen 40 und < 75
  - **Gut** — Anwendungsbewertung ist größer als 75
  - **Nicht anwendbar** — Es sind keine virtuellen Server für die Anwendung konfiguriert

In der folgenden Tabelle werden die Unterschiede zwischen der früheren App-Bewertung und der aktuellen App-Bewertung beschrieben.

Bewertungsbewertung (Kritisch, Überprüfung, Gut, Nicht zutreffend)	App-Punktzahl (frühere Ansicht mit Farbenlegenden)
Die Punktzahl wird als **100 minus Strafpunktzahl aller aktuellen Ausgaben der Anwendung**berechnet.	Die Punktzahl wird als **100 berechnet — (App-Serverressource + Citrix ADC -Systemressource)**
Anwendungen werden in den Farben **Rot (kritisch)**, **Orange (prüfen)**, **Grün (gut)** und **Grau (nicht anwendbar)**angezeigt.	Anwendungen werden in Farblegenden angezeigt. 

- Wählen Sie diese Option aus, um Anwendungen basierend auf dem Anwendungsstatus anzuzeigen, z. B. Up-, Down- und Out-of Service
- Wählen Sie diese Option aus, um Anwendungen basierend auf dem Anwendungstyp anzuzeigen, z. B. Diskret oder Benutzerdefiniert
- Wählen Sie diese Option aus, um Anwendungen basierend auf den unten gruppierten Kategorien anzuzeigen.
- Ziehen Sie das Histogramm, um Filter anzuwenden und Anwendungen anzuzeigen.

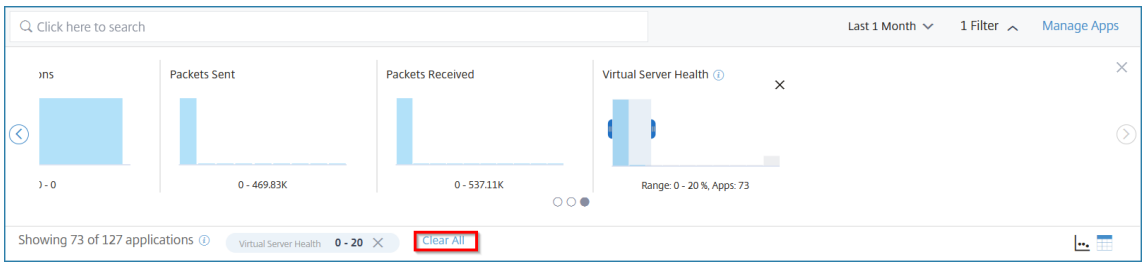
  Wenn Sie beispielsweise Anwendungen anzeigen möchten, die eine virtuelle Serverintegrität zwischen 0 und 20 aufweisen, ziehen Sie das Histogramm für virtuelle Serverintegrität, um die Ergebnisse zu filtern.



> **Hinweis**
>
> Sie können auch auf das Histogramm klicken, um die entsprechenden Anwendungen

> anzuzeigen.

Klicken Sie auf **Alle löschen**, um den angewendeten Filter zu löschen.



Im Folgenden finden Sie die Anwendungsübersicht, für die Sie Filter anwenden können:

- **Anwendungsbewertung** — Ermöglicht es Ihnen, Anwendungen basierend auf **Kritisch**, **Review**, **Good**und **Not Application**anzuzeigen.

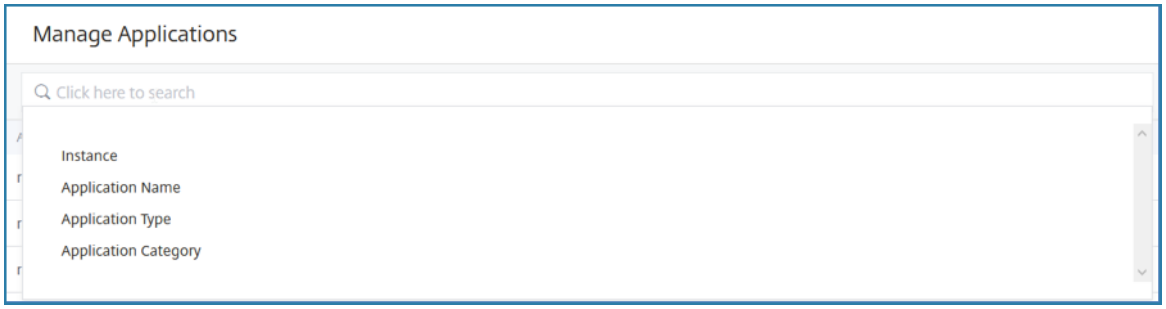
  > Hinweis
  >
  > Standardmäßig können Sie Anwendungen anzeigen, die den Status “Kritisch”, “Überprüfen” und “Gut” aufweisen. Um Anwendungen anzuzeigen, die sich im Status N/A befinden, müssen Sie die Option **Nicht anwendbar** auswählen.

- **Status** — Ermöglicht es Ihnen, die Anwendung basierend auf dem Anwendungsstatus wie Up, **Down**und **Out of Service**anzuzeigen.
- **Aktuelle Probleme** — Ermöglicht es Ihnen, eine Liste der Anwendungen zu erhalten, die mit einem bestimmten Problem betroffen sind, indem Sie den Problemtyp wie **Performance**, **Instanz Health**, **Config**und **Systemressourcen**auswählen.
- **App-Typ** — Ermöglicht es Ihnen, Anwendungen basierend auf dem Anwendungstyp wie **benutzerdefinierten**, **diskreten**und **Kubernetes-Diensten**anzuzeigen.
- **App-Kategorie** — Ermöglicht es Ihnen, die Anwendungen basierend auf der zugewiesenen Kategorie anzuzeigen.
- **Reaktionszeit** — Ein Histogramm, das die durchschnittliche Reaktionszeit der Anwendungen anzeigt.
- **Gesamtzahl der Anforderungen** — Ein Histogramm, das die Gesamtzahl der Anfragen anzeigt, die von den Anwendungen empfangen wurden.
- **Durchsatz** — Ein Histogramm, das den gesamten von den Anwendungen verarbeiteten Netzwerkdurchsatz anzeigt.
- **Datenvolumen** — Ein Histogramm, das die von den Anwendungen verarbeiteten Gesamtdaten anzeigt. Das Datenvolumen wird anhand der gesamten Anforderungsbytes und Antwortbytes für die Anwendungen berechnet.
- **Clientverbindungen** — Ein Histogramm, das die durchschnittlichen Clientverbindungen anzeigt, die von den Anwendungen hergestellt werden.

- **Serververbindungen** — Ein Histogramm, das die durchschnittlichen Serververbindungen anzeigt, die von den Anwendungen hergestellt wurden.
- **Gesendete Pakete** — Ein Histogramm, das die Gesamtzahl der von den Anwendungen gesendeten Pakete anzeigt.
- **Empfangene Pakete** — Ein Histogramm, das die Gesamtzahl der von den Anwendungen empfangenen Pakete anzeigt.
- **Virtueller Serverzustand** — Ein Histogramm, das die gesamten Anwendungen zwischen dem Bewertungsbereich 0% und 100% anzeigt. Eine virtuelle Serverintegrität ist (%) der aktiven Dienste, die der Anwendung zugeordnet sind. Wenn beispielsweise ein virtueller Server mit 2 Diensten konfiguriert ist und einer davon ausgefallen ist, beträgt die Punktzahl 50%.

Suchen und filtern Sie Ergebnisse mit der Suchleiste

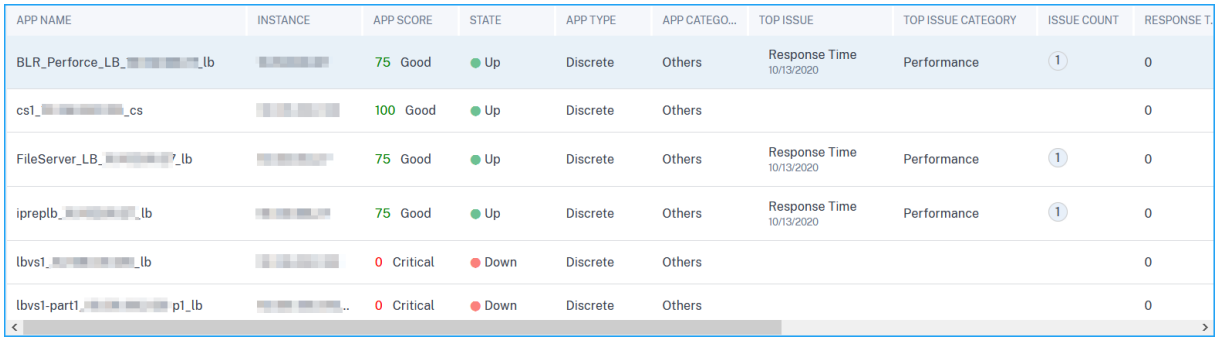
Sie können den Mauszeiger auf die Suchleiste setzen und die Kategorie auswählen, um die Suche zu verfeinern.



Anwendungen anzeigen

April 28, 2021

Standardmäßig werden im Anwendungs-Dashboard alle Anwendungen angezeigt. Je nach Anforderung können Sie die Filteroption verwenden, um Anwendungen anzuzeigen.



APP NAME	INSTANCE	APP SCORE	STATE	APP TYPE	APP CATEGO...	TOP ISSUE	TOP ISSUE CATEGORY	ISSUE COUNT	RESPONSE T...
BLR_Perforce_LB_[redacted]_lb	[redacted]	75 Good	Up	Discrete	Others	Response Time 10/13/2020	Performance	1	0
cs1_[redacted]_cs	[redacted]	100 Good	Up	Discrete	Others				0
FileServer_LB_[redacted]_lb	[redacted]	75 Good	Up	Discrete	Others	Response Time 10/13/2020	Performance	1	0
ipreplb_[redacted]_lb	[redacted]	75 Good	Up	Discrete	Others	Response Time 10/13/2020	Performance	1	0
lbvs1_[redacted]_lb	[redacted]	0 Critical	Down	Discrete	Others				0
lbvs1-part1_[redacted]_p1_lb	[redacted]	0 Critical	Down	Discrete	Others				0

Das Dashboard zeigt die folgenden Anwendungsdetails an:

- **App-Name** — Gibt den Namen der Anwendung an.
- **Instanz** — Bezeichnet die Citrix ADC-Instanz.
- **App-Score** — Gibt die Anwendungsbewertung und den Status wie **Kritisch**, **Gut**, **Fair**und **Nicht zutreffend**an.
- **State** – Bezeichnet die aktuelle Verfügbarkeit der Anwendung, wie **Up**, **Down**, **Partially Up**, **Out of Service** und **NA**.
  - **Up** — Alle virtuellen Server, die der Anwendung zugeordnet sind, sind betriebsbereit.
  - **Heruntergefahren** — Alle virtuellen Server, die der Anwendung zugeordnet sind, sind “Heruntergefahren”.
  - **Teilweise hochgefahren** — Entweder ist eine virtuelle, die der Anwendung zugeordnet ist, heruntergefahren oder außer Betrieb.
  - **Out of Service** — Alle virtuellen Server, die den Anwendungen zugeordnet sind, sind außer Betrieb.
  - **NA** — Für die Anwendung sind keine virtuellen Server konfiguriert.
- **App-Typ** — Bezeichnet den Anwendungstyp wie **benutzerdefiniert**, **diskret** oder **Kubernetes-Dienste**.
- **App-Kategorie** — Gibt die Kategorie an, die der Anwendung zugewiesen ist.
- **Top Issue** — Bezeichnet das Problem, das die maximale Anzahl von Fehlern für die Anwendung hat.
- **Top-Issue-Kategorie** — Kennzeichnet die Kategorie des Problems.
- **Ausgabeanzahl** — Gibt die Gesamtzahl der Emissionswerte für die Anwendung an.
- **Reaktionszeit** — Gibt die durchschnittliche Reaktionszeit an, um von der Anwendung zu antworten.
- **Gesamtzahl der Anfragen** — Kennzeichnet die Gesamtzahl der von der Anwendung eingegangenen Anfragen.

- **Durchsatz** — Bezeichnet den gesamten Netzwerkdurchsatz für die Anwendung. Der Durchsatz wird von den Req Bytes/Sec + Res Bytes/Sec für die virtuellen Server berechnet.
- **Datenvolumen** — Bezeichnet die Gesamtdaten, die von der Anwendung verarbeitet werden.
- **Clientverbindungen** — Bezeichnet die durchschnittlichen Clientverbindungen, die von der Anwendung hergestellt werden.
- **Serververbindungen** — Bezeichnet die durchschnittlichen Serververbindungen, die von der Anwendung hergestellt werden.

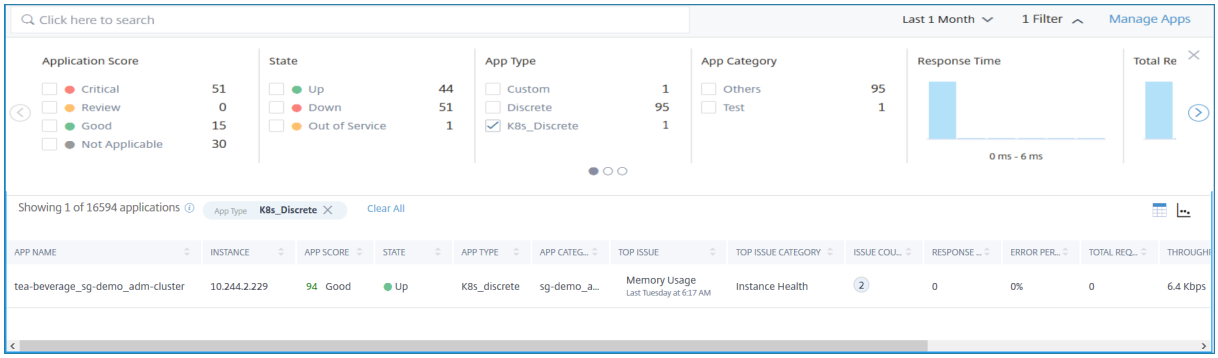
Anzeigen von Microservices-Anwendungen

Um die Microservices-Anwendungen anzuzeigen, wählen Sie die Option **K8S_discrete** unter **App-Typ-Filter**.

Sie können die Microservice-Anwendungen im **App Dashboard** als folgendes Namensformat anzeigen:

`<k8s service>_<k8s namespace>_<k8s cluster_name>`

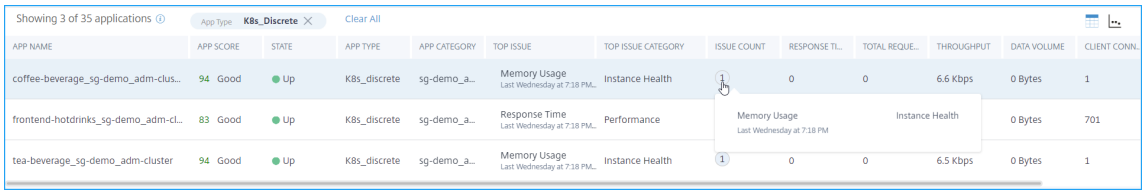
`tea-beverage_sg-demo_adm-cluster` Bezieht sich beispielsweise auf einen Dienst namens “Teegetränk” mit dem Namensraum von `sg-demo` im Cluster `adm-cluster`.



Die folgenden Metriken werden für die ausgewählte Zeitdauer im Dashboard angezeigt:

- **App-Name** — Gibt den Namen der Anwendung an.
- **Instanz** — Bezeichnet die IP-Adresse der Citrix ADC CPX-Instanz.
- **App-Score** — Gibt die Anwendung-Score an.
  - **Kritisch** — App-Punktzahl liegt zwischen 0 und < 40
  - **Bewertung** — App-Punktzahl liegt zwischen 40 und < 75
  - **Gut** — App-Punktzahl ist größer als 75
- **Status** — Gibt den aktuellen Anwendungsstatus an.
- **App-Kategorie** — Gibt den Clusternamen an, in dem die Anwendung gehostet wird.

- **Top Issue** — Bezeichnet die wichtigsten Probleme, die sich auf die aktuelle Anwendungsbewertung auswirken.
- **Top Issue Category** — Kennzeichnet die Problemkategorie, die sich auf die Anwendung auswirkt.
- **Anzahl der Probleme** — Bezeichnet die Gesamtanzahl der Probleme, die sich auf die Anwendung auswirken. Bewegen Sie den Mauszeiger auf die Anzahl der Probleme, um eine Übersicht über die Probleme anzuzeigen.



- **Reaktionszeit** — Gibt die durchschnittliche Antwortzeit an, die die Anwendung erhalten hat.
- **Fehlerprozentsatz** — Gibt den durchschnittlichen Fehlerprozentsatz von 5xx-Fehlern für die Anwendung an.
- **Total Requests** — Gibt die Gesamtzahl der von der Anwendung eingegangenen Anfragen an.
- **Durchsatz** — Bezeichnet den gesamten von der Anwendung verarbeiteten Netzwerkdurchsatz.
- **Datenvolumen** — Bezeichnet die Gesamtdaten, die von der Anwendung verarbeitet werden. Das Datenvolumen wird als Gesamtanforderungsbytes und Antwortbytes für die Anwendung berechnet.
- **Clientverbindungen** — Bezeichnet die durchschnittlichen Clientverbindungen, die von der Anwendung hergestellt werden. Dies kann sich auch auf die zugehörigen ausgehenden Dienste beziehen, die mit dem ausgewählten Dienst verbunden sind.
- **Serververbindungen** — Bezeichnet die durchschnittlichen Serververbindungen, die von der Anwendung hergestellt werden. Dies kann sich auch auf die zugehörigen eingehenden Dienste beziehen, die mit dem ausgewählten Dienst verbunden sind.

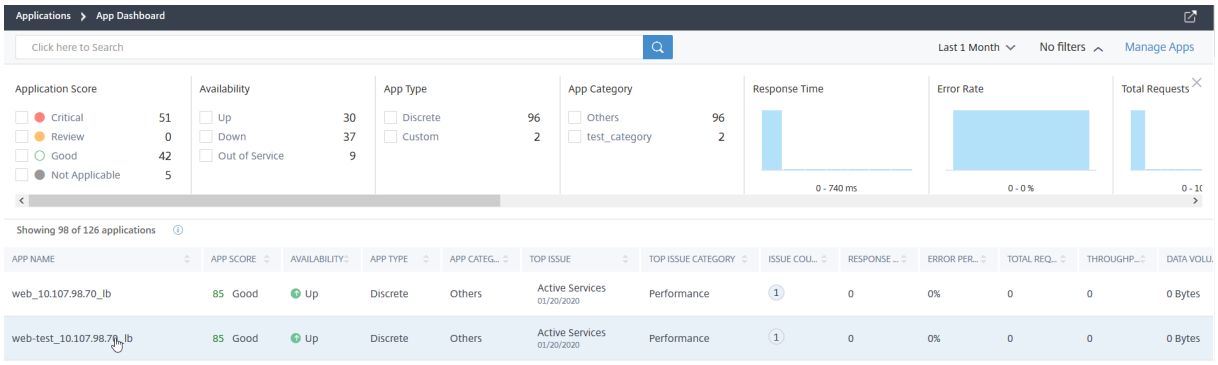
Klicken Sie auf die Option **+**, um die Optionen hinzuzufügen oder zu entfernen, die im Dashboard angezeigt werden sollen.

Klicken Sie auf eine Anwendung, um die Anwendungsdetails anzuzeigen. Weitere Informationen Microservices-Anwendungsdetails

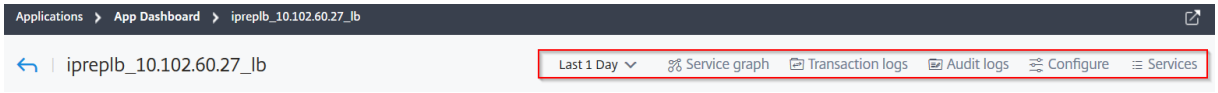
Anwendungsdetails

April 28, 2021

Klicken Sie im Dashboard auf eine Anwendung, um weitere detaillierte Informationen zu erhalten.



Die ausgewählte Anwendungsseite wird angezeigt.

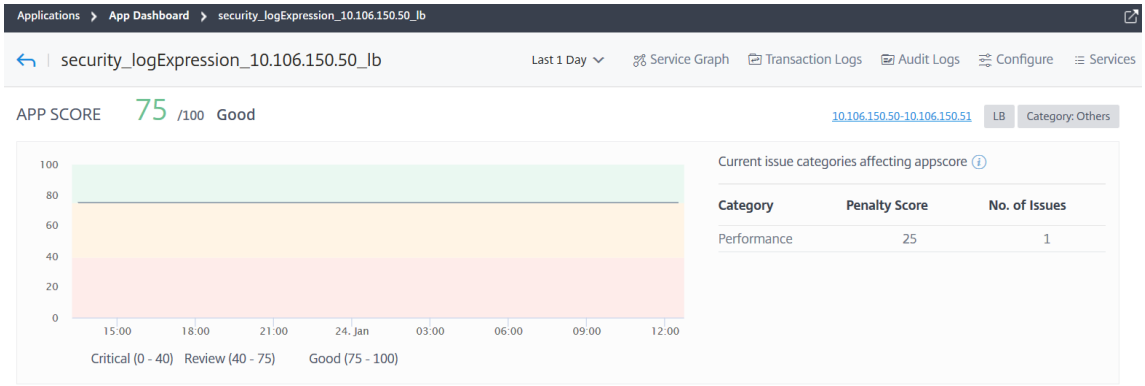


Auf der Seite mit den Anwendungsdetails:

- Wählen Sie die Zeitdauer aus der Liste aus, um Details für die bestimmte Zeitdauer anzuzeigen.
- Klicken Sie auf **Service-Diagramm**, um das Service-Diagramm für die ausgewählte Anwendung anzuzeigen. Weitere Informationen finden Sie unter Service-Diagramm für Anwendungen.
- Klicken Sie hier **Transaktionsprotokolle**, um die detaillierten Transaktionen für die ausgewählte Anwendung anzuzeigen.
- Klicken Sie auf **Überwachungsprotokolle**, um die detaillierten Überwachungsprotokollinformationen anzuzeigen.
- Klicken Sie auf **Konfigurieren**, um die Dienst- und Dienstgruppenkonfiguration für die ausgewählte Anwendung anzuzeigen oder zu bearbeiten.
- Klicken Sie auf **Dienst**, um Dienste anzuzeigen, die an die Anwendung gebunden sind

Nachdem Sie die Zeitdauer ausgewählt haben, werden die folgenden Anwendungsdetails angezeigt:

- **App-Score** — Die Bewertungsbewertung für die ausgewählte Zeitdauer. Die Endpunktzahl wird als **100 minus Gesamtstrafe**berechnet.

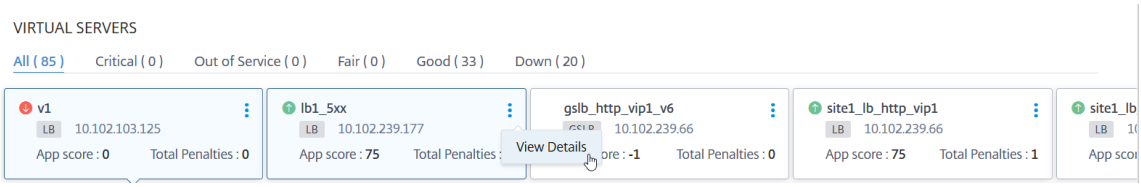


Mit diesem Dashboard können Sie auch die aktuellen Probleme anzeigen, die sich auf die App-Bewertung auswirken. Sie können die Problemdetails unter Probleme anzeigen.

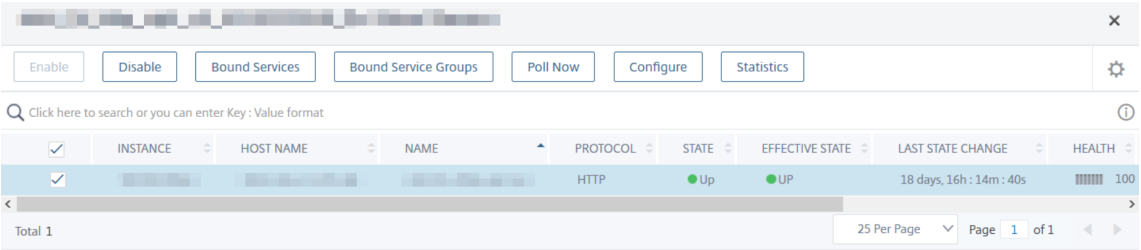
- **Virtuelle Server** —

> **Hinweis**
>
> Der Abschnitt **Virtuelle Server** wird nur für die benutzerdefinierten Anwendungen angezeigt. Klicken Sie bei diskreten Anwendungen auf die **IP-Adresse**, um die Details des virtuellen Servers anzuzeigen.

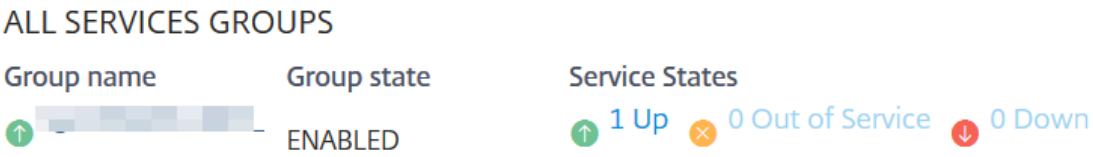
Zeigt alle virtuellen Server an, die der benutzerdefinierten Anwendung zugeordnet sind



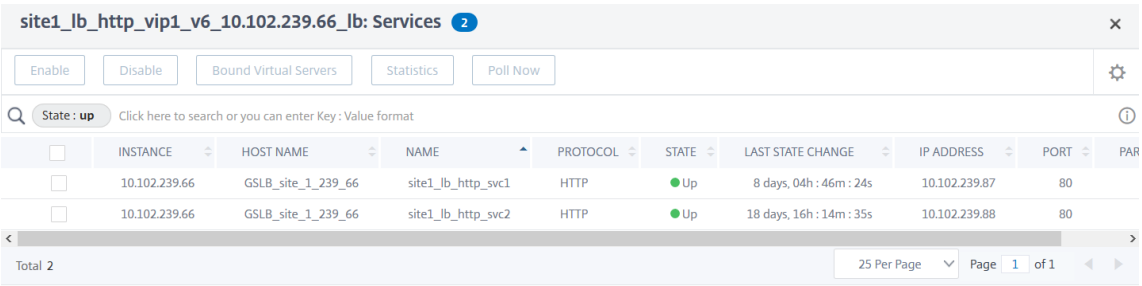
Klicken Sie auf **Details anzeigen**, um die Einstellungen des virtuellen Servers anzuzeigen und zu verwalten.



- **Alle Dienste** — Die Dienste, die an die Anwendung gebunden sind



Klicken Sie hier, um die Service-Details anzuzeigen und die Service-Einstellungen zu verwalten.



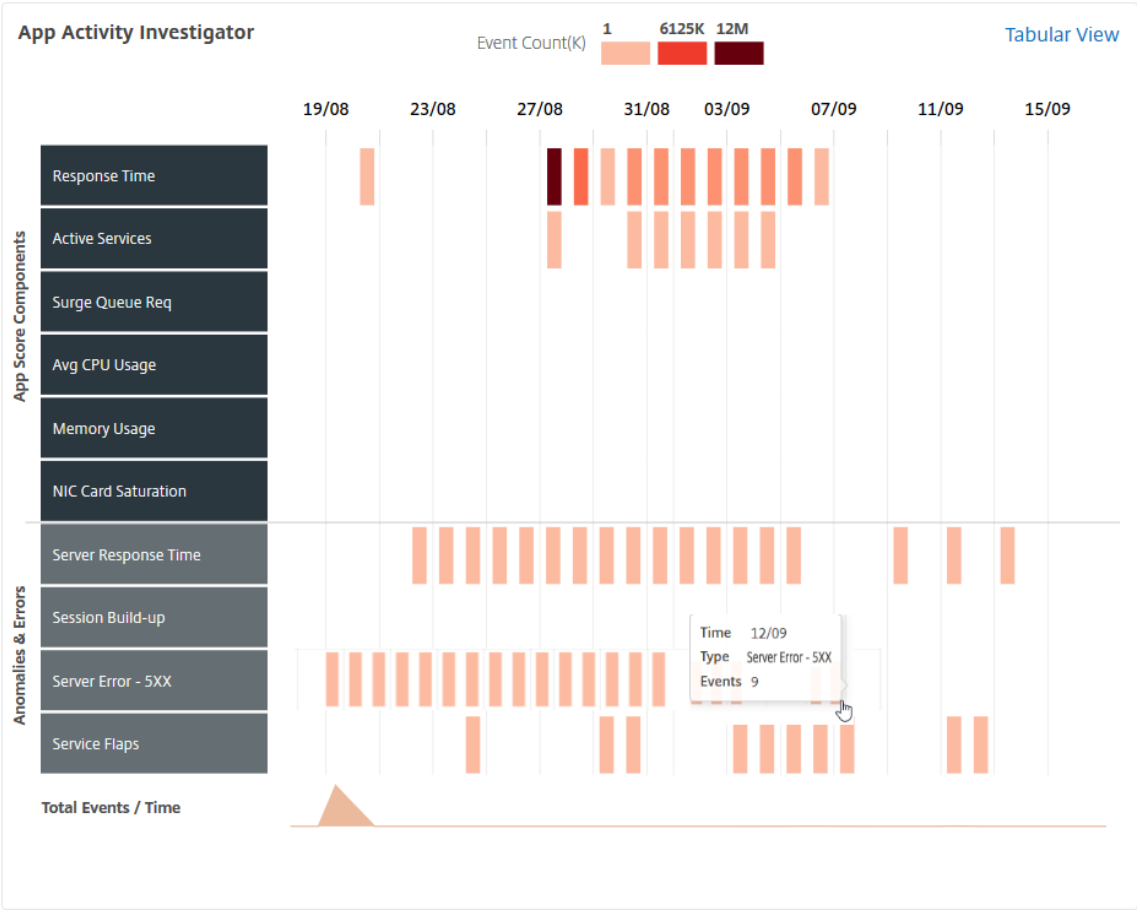
- **Probleme** — Die Probleme, die für die ausgewählte Anwendung gelten. Sie können die folgenden Probleme zusammen mit der Kategorie anzeigen:

Leistung	Instanz-Integrität	Config	Systemressourcen
Reaktionszeit	Durchschnittliche CPU-Auslastung	Instabiler Server	Unsachgemäßer Persistenz-Typ
Aktive Dienste	Speicherauslastung	Ungewöhnlich große HTTP-Pakete	NIC-Kartensättigung
Wiederverwendung der niedrigen Sitzung		TCP-Queue-Limit Treffern neu zusammenbauen	
App-CPU-Nutzung			
SurgeQueue-Aufbau			
SSL-Echtzeit-Datenverkehr			
Sitzungsaufbau			
Server-Reaktionszeit			
Service-Klappen			

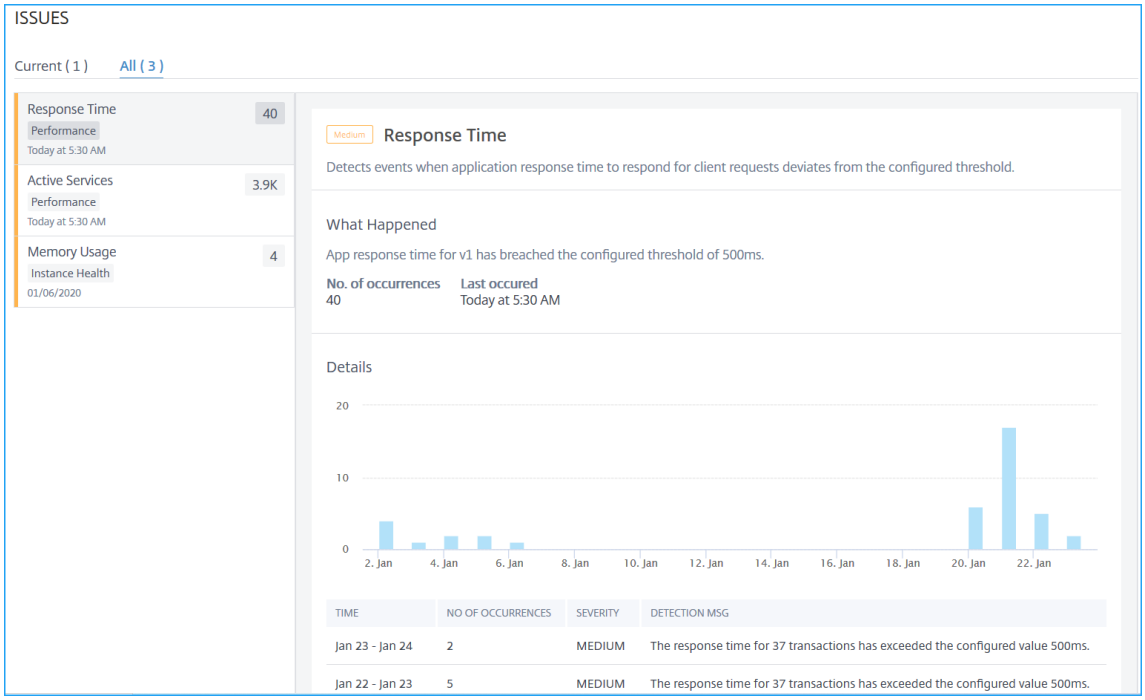
Klicken Sie auf jedes Problem, um Details wie Erkennungsmeldung, wann das Problem aufgetreten ist, Empfohlene Aktionen und Details zu überprüfen.

Weitere Informationen finden Sie unter Leistungsindikatoren für Anwendungsanalysen.

Das folgende Bild zeigt die frühere Ansicht der **App Activity Investigator-Seite** :

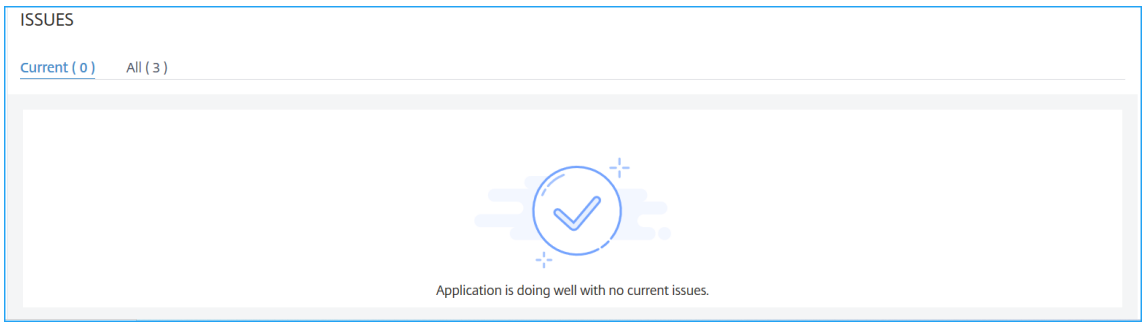


Sie können jetzt alle Probleme im Abschnitt " **Probleme** " zusammen mit der Kategorie anzeigen, die Sie auf der Seite " **App Activity Investigator** " anzeigen können.

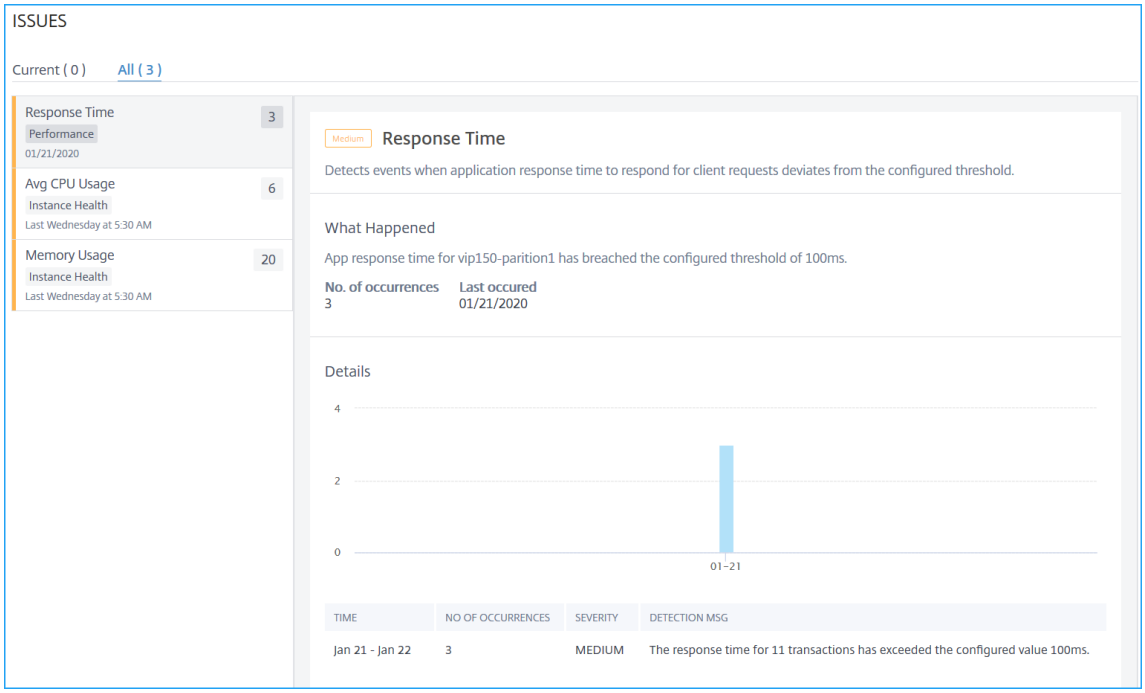


- Die Probleme, die auf der Registerkarte **Aktuell** angezeigt werden, beziehen sich auf die Anwendungsprobleme für die ausgewählte Zeitdauer.
- Die Probleme, die auf der Registerkarte **Alle** angezeigt werden, beziehen sich auf die Gesamtzahl der Anwendungsprobleme.

Das folgende Beispiel zeigt die Anwendungsprobleme für einen Tag. Auf der Registerkarte **Aktuell** werden keine aktuellen Probleme angezeigt, die sich auf die App-Bewertung auswirken.



Auf der Registerkarte **Alle** werden die insgesamt erkannten Probleme für die Dauer eines Tages angezeigt.



Peak- und Lean-Use

April 28, 2021

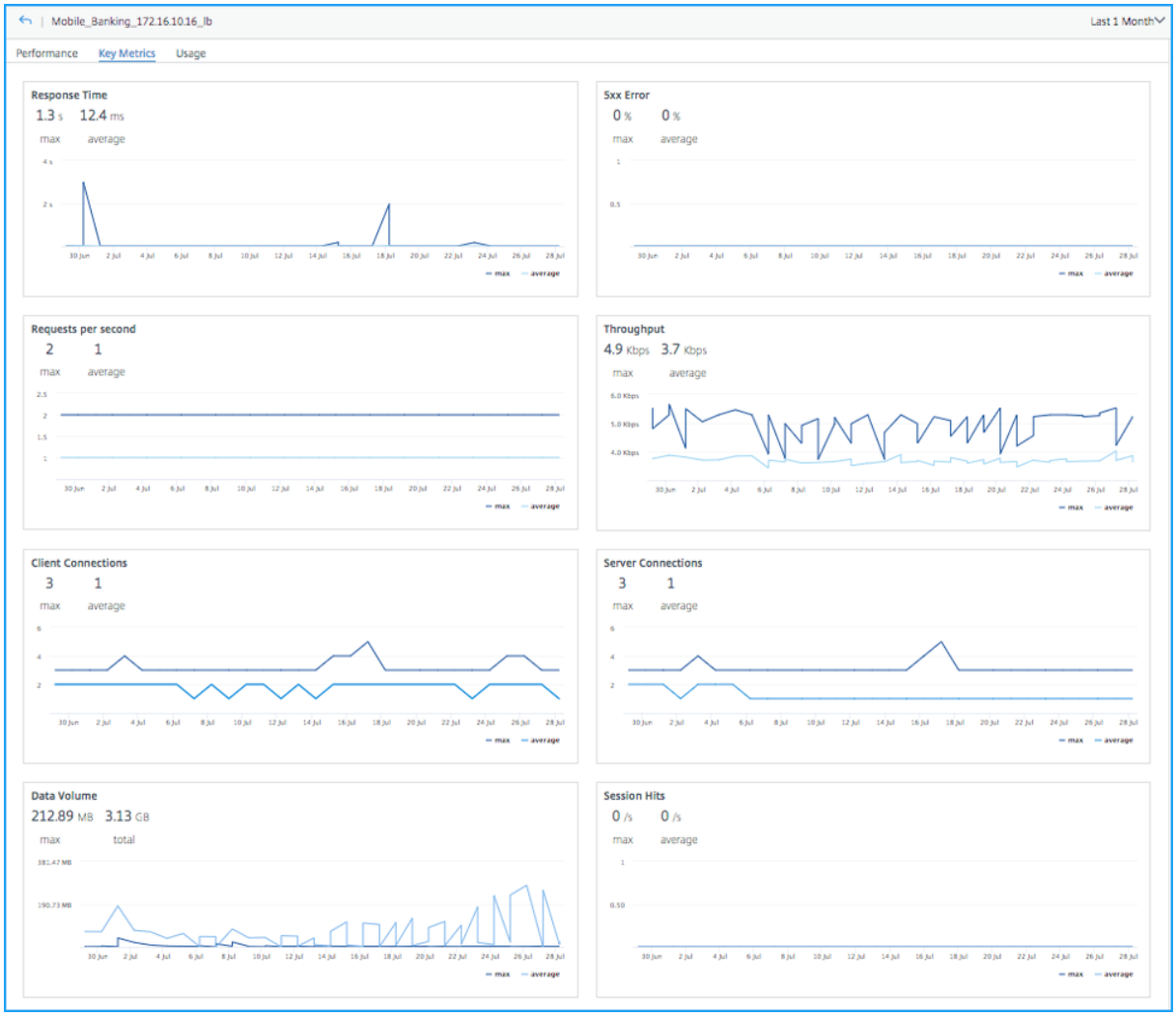
Eine Webanwendung kann entweder hohen Traffic oder geringen Traffic empfangen, und die Verkehrsreichweite für jeden Tag oder jede Stunde ist sicherlich unvorhersehbar. In ähnlicher Weise erfordert eine Webanwendung auch Ausfallzeiten für eine bestimmte Dauer während einer geplanten Wartung oder eines Upgrades. Als Administrator müssen Sie den Datenverkehr analysieren und einen richtigen Zeitpunkt finden, um:

- Skalieren Sie die Webanwendung
- Planen einer Ausfallzeit einer Webanwendung

Die Analysefunktion für Spitzenauslastung und Lean Period in Citrix ADM ermöglicht es Ihnen, die wichtigsten Kennzahlen für eine ausgewählte Zeitdauer zu analysieren. Anhand dieser Metriken können Sie den Datenverkehr analysieren und entscheiden, wann Sie die Webanwendung vergrößern oder eine geplante Ausfallzeit planen möchten.

Bewerten der App-Skalierungslimits

Klicken Sie im **App Dashboard** auf eine Anwendung und wählen Sie die Registerkarte “ **Wichtige Metriken** “ aus, um die konsolidierte Ansicht aller Metriken zu visualisieren. Wählen Sie die Zeitdauer aus der Liste aus, um die Metriken zu analysieren.



Für jede Metrik können Sie Folgendes anzeigen:

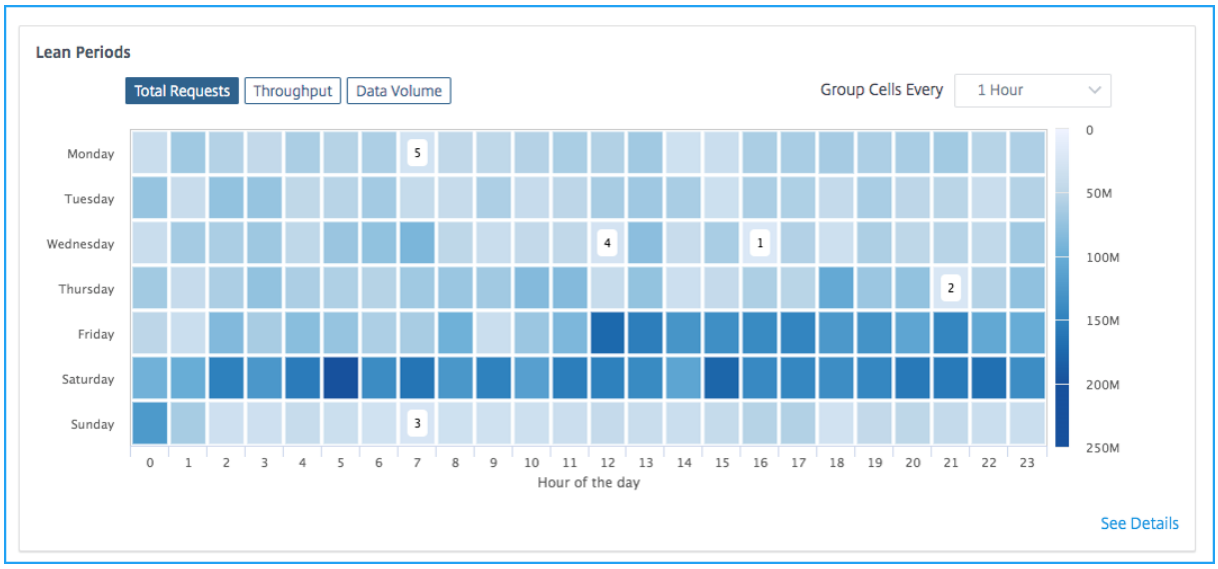
- **Max** — Gibt den Maximalwert für die gewählte Dauer an
- **Durchschnitt** — Gibt den Durchschnittswert für die ausgewählte Dauer

Gemäß dem Beispiel im Bild gibt der Maximalwert für die Reaktionszeit 1,3 s an. Aus dem Diagramm können Sie analysieren, wie oft die hohe Reaktionszeit für die ausgewählte Zeitdauer aufgetreten ist. In ähnlicher Weise können Sie auch Details für andere Metriken anzeigen, analysieren, ob die Anwendung eine Spitzennutzung erhalten hat, und sich für eine Skalierung der Produktionsumgebung entscheiden.

Identifizieren des Top-5-App-Wartungsfenst

Klicken Sie im **App Dashboard** auf eine Anwendung und wählen Sie die Registerkarte “ **Wichtige Metriken** “ aus, um den Schlankzeitraum für die Anwendung anzuzeigen. Eine typische Ausfallzeit für eine Anwendung kann je nach Anforderung 1 Stunde, 2 Stunden oder 4 Stunden betragen. Sie können

die Zeit aus der Liste (1 Stunde, 2 Stunde oder 4 Stunden) auswählen, die Sie für die Ausfallzeit planen möchten. Nachdem Sie die Uhrzeit aus der Liste ausgewählt haben, können Sie den Datenverkehr für Metriken wie Gesamtanforderungen, Durchsatz und Datenvolumen analysieren. Sie können den richtigen Zeitpunkt für die Planung einer Ausfallzeit auswählen, wenn die Anwendungsnutzung geringer ist.
Im folgenden Beispiel wird die Ausfallzeit für die Dauer von 1 Stunde analysiert.



Die Heatmap-Ansicht zeigt die Anwendungsnutzung für die ausgewählte Zeitdauer an. Je dunkler die Farbe (blau) ist, desto höher ist die Anwendungsnutzung.

Die Heatmap-Ansicht schlägt auch die 5 am wenigsten belasteten Zeiträume vor (1, 2, 3, 4 und 5), um die Ausfallzeiten der Anwendung zu planen.

1 — Gibt den ersten Vorschlag für Mittwoch von 16 bis 17 Uhr

2 — Gibt den zweiten Vorschlag für Donnerstag von 21:00 Uhr bis 22:00 Uhr

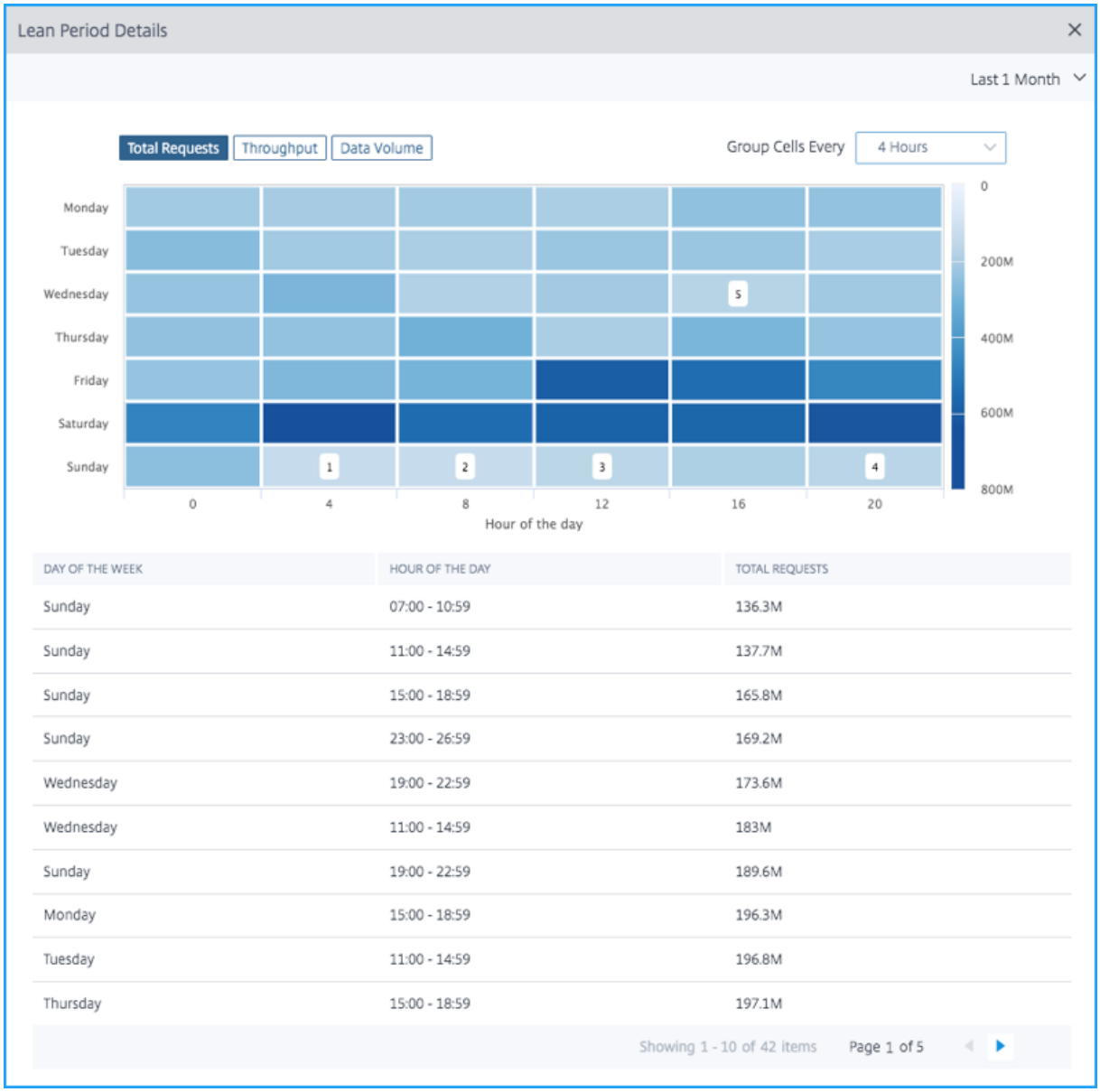
3 — Gibt den dritten Vorschlag für Sonntag von 7.00 bis 20.00 Uhr

4 — Gibt den vierten Vorschlag für Mittwoch von 12 bis 13 Uhr

5 — Gibt den fünften Vorschlag für Montag von 7.00 bis 20.00 Uhr

Sie können auch jeden anderen Tag und jede andere Uhrzeit auswählen, um eine Ausfallzeit zu planen, nachdem Sie den Datenverkehr für alle anderen Tage analysiert haben.

Klicken Sie auf **Details** anzeigen, um weitere detaillierte Informationen anzuzeigen. Klicken Sie auf die Registerkarte **Gesamtzahl der Anforderungen**, des **Durchsatzes**oder des **Datenvolumens**, um Details für den kleinsten Zeitraum der Top 5 und auch für die anderen Tage anzuzeigen.



Anwendungsverwendung und Anomalien

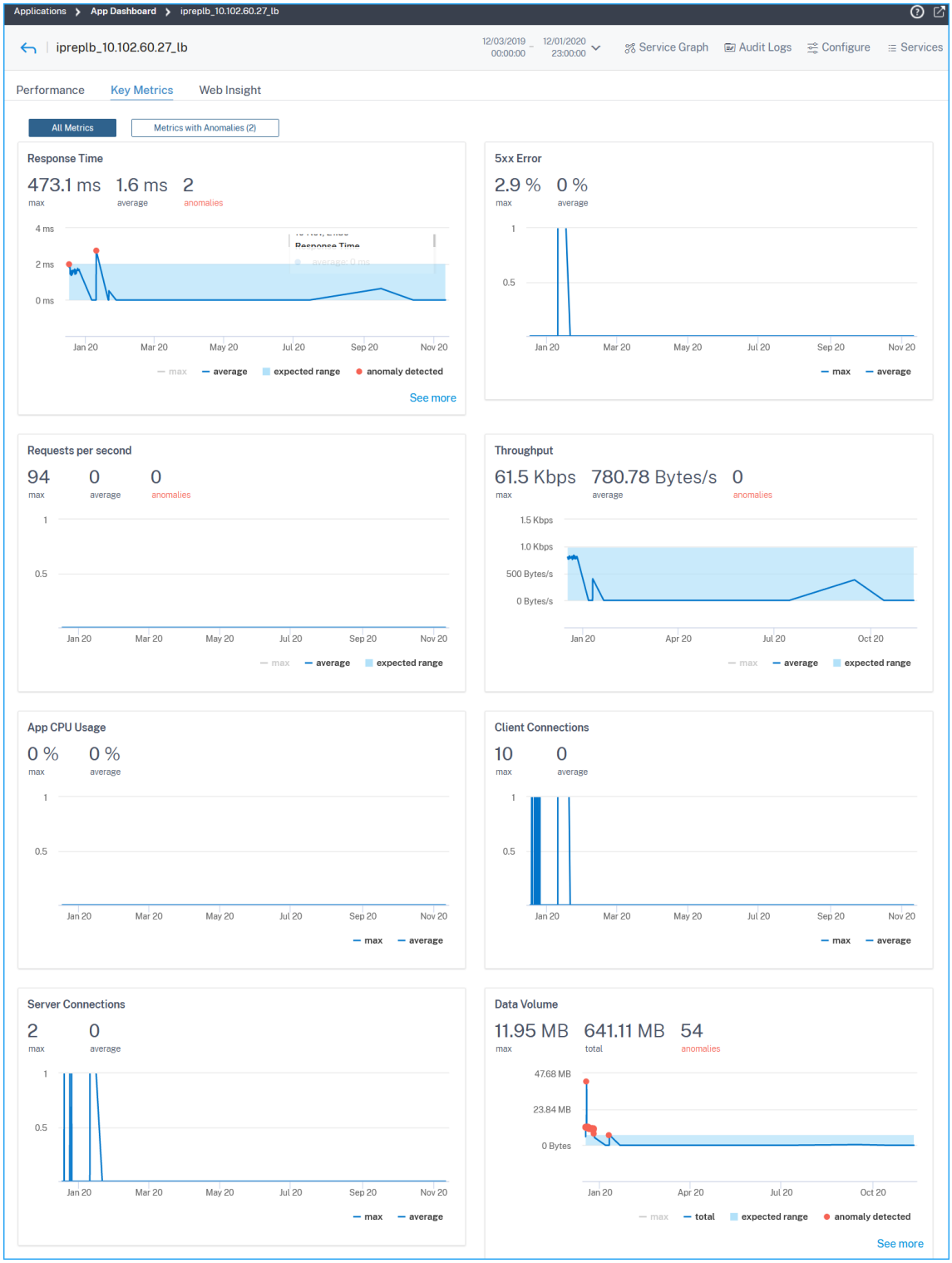
April 28, 2021

Als Administrator müssen Sie sicherstellen, wie die Anwendung genutzt wird. Die Kennzahlen für Anwendungsschlüssel können Ihnen helfen, die Anwendungsnutzung zu identifizieren. Da die Reichweite der Datenverkehrsreichweite für die Anwendung unvorhersehbar ist, können einige ungewöhnliche Abweichungen bei der Anwendungsleistung für eine bestimmte Dauer auftreten. In solchen Szenarien sollten Sie als Administrator solche plötzlichen Anomalien anzeigen und analysieren und sicherstellen, dass eine sofortige Fehlerbehebung erforderlich ist.

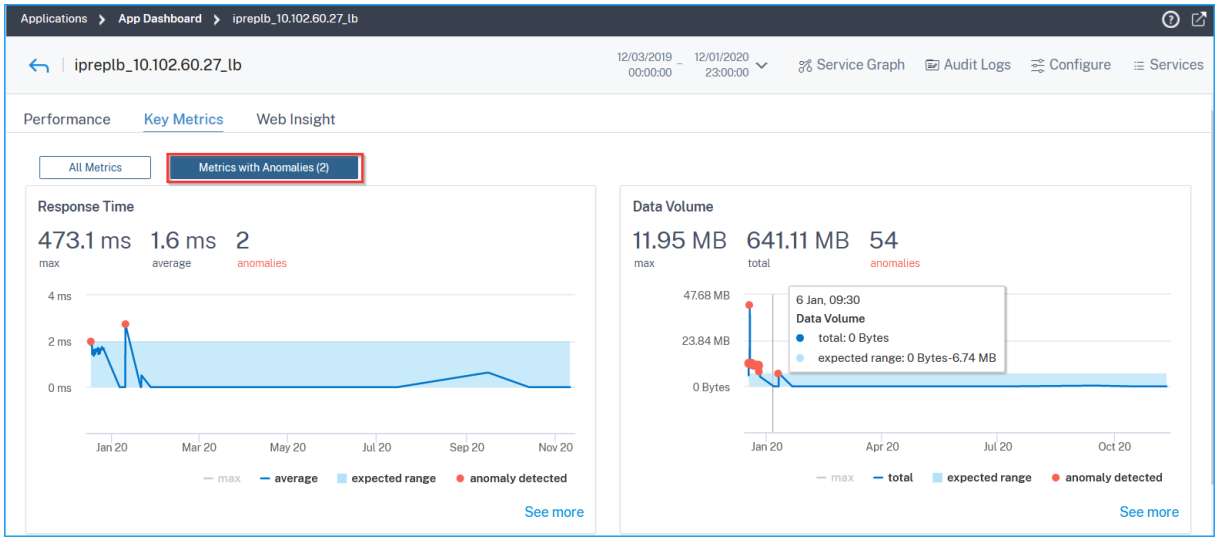
Citrix ADM erkennt solche Anomalien und liefert notwendige Details. Navigieren Sie zu **Anwendungen > Dashboard**, klicken Sie auf eine Anwendung und wählen Sie die Registerkarte " **Wichtige Metriken** " aus. Citrix ADM überwacht das Verkehrsmuster und analysiert, ob die wichtigsten Metriken im erwarteten Bereich liegen. Wenn es eine Abweichung als die erwartete Spanne gibt, meldet Citrix ADM diese Abweichungen als Anomalien.

Sie können Anomalien für die folgenden wichtigen Metriken anzeigen:

- Reaktionszeit
- Durchsatz
- Datenvolume
- Anfragen pro Sekunde



Klicken Sie auf die Registerkarte **Metriken mit Anomalien**, um Details anzuzeigen.



In jeder Metrik können Sie auch auf die Option **Mehr** anzeigen klicken, um Details anzuzeigen. Das folgende Beispiel ist für das Daten-Volume der Anwendung:

Sie können sehen:

- Die Grafik, die den Maximalwert, den Gesamtwert, den erwarteten Bereich und die Anomalien angibt
- Die **empfohlenen Maßnahmen** zur Behebung des Problems

- Die Zeit- und Anomaliedetails unter **Details**

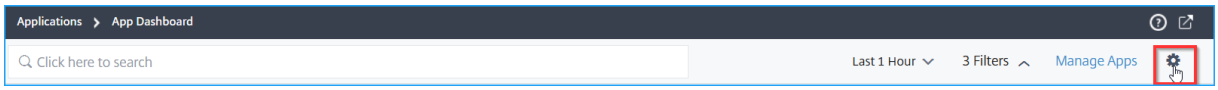
Wählen Sie App-Score-Komponenten und legen Sie Schwellenwerte

April 28, 2021

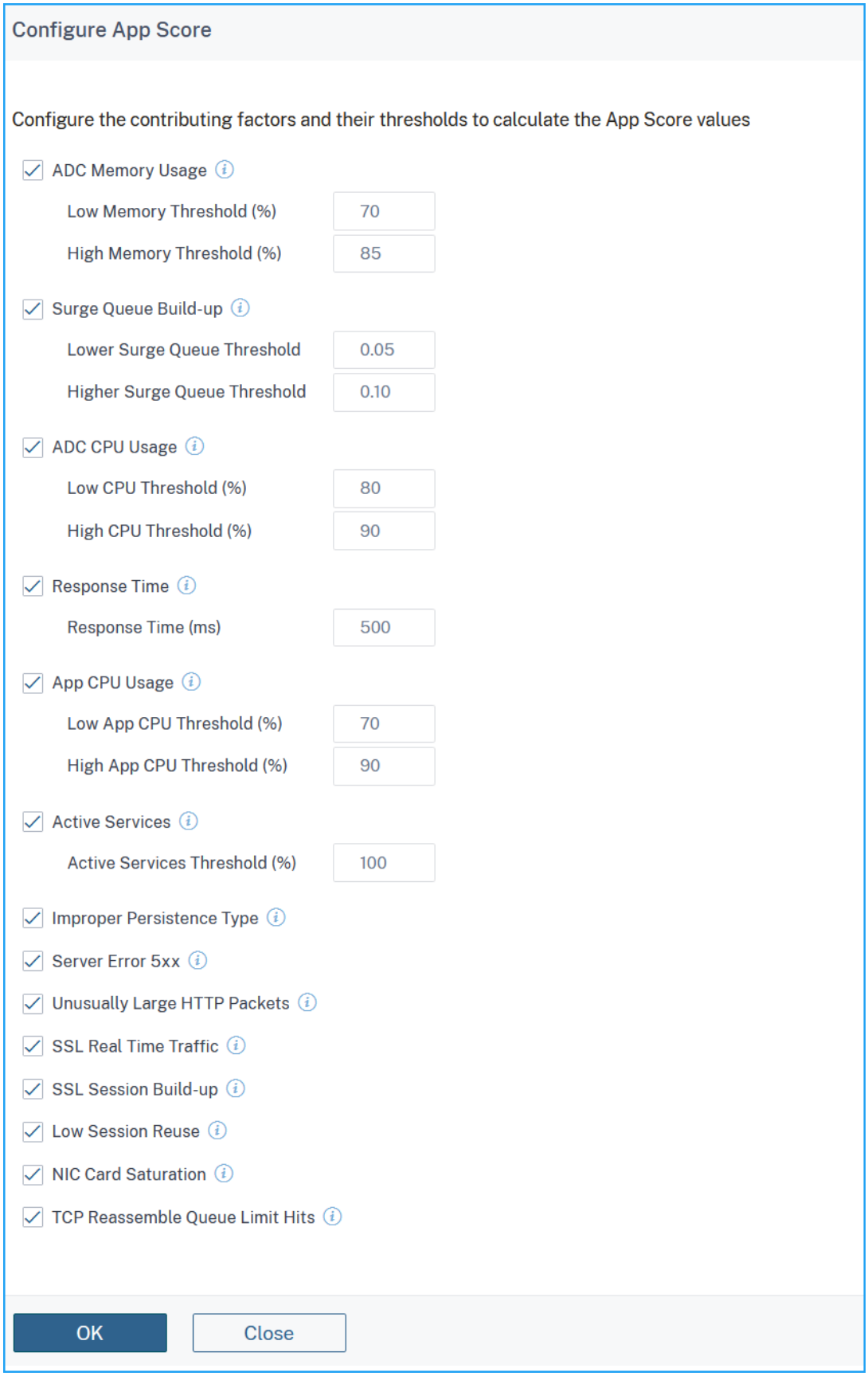
Im **App Dashboard**können Sie als Administrator entscheiden, die Komponenten auszuwählen und Schwellenwerte für die App-Score-Berechnung zu konfigurieren. App Score ist das Punktesystem, das definiert:

- Wie gut funktioniert eine Anwendung
- Ob die Anwendung hinsichtlich der Reaktionsfähigkeit gut funktioniert

Navigieren Sie zu **Anwendungen > Dashboard** und wählen Sie dann das Einstellungssymbol aus.



Auf der Seite **App-Score konfigurieren** können Sie die Komponenten auswählen und Schwellenwerte konfigurieren, um den endgültigen App-Score zu bestimmen.



Die App-Score-Berechnung basiert auf den folgenden Komponenten:

App-Score-Komponenten	Vom Benutzer konfigurierte Schwellenwerte	Beschreibung
ADC-Speichernutzung	Ja	Der niedrige und hohe Schwellenwert für die Gesamtspeicherauslastung in der Citrix ADC-Instanz
Aufbau von Überspannungswarteschlange	Ja	Der niedrige und hohe Schwellenwert für die gesamten Anstiegsanforderungen, die sich in der Warteschlange befinden und eine Antwort benötigen.
ADC-CPU-Auslastung	Ja	Der niedrige und hohe Schwellenwert für die gesamte CPU-Auslastung in der Citrix ADC-Instanz.
Response time	Ja	Das Zeitintervall zwischen dem Senden eines Anforderungspakets und dem Empfangen des ersten Antwortpakets vom Dienst, der auf dem virtuellen Server konfiguriert ist.
App-CPU-Nutzung	Ja	Der niedrige und hohe Schwellenwert für die gesamte CPU-Auslastung durch die Anwendung.
Aktive Dienste	Ja	Der Schwellenwert des Prozentsatzes der Dienste, die aktiv sein müssen, die an den virtuellen Server gebunden sind.
Unsachgemäßer Persistenz-Typ	Nein	Gibt an, ob die Persistenznutzung auf einem virtuellen Server gering ist.

App-Score-Komponenten	Vom Benutzer konfigurierte Schwellenwerte	Beschreibung
Serverfehler (5xx)	Nein	Gibt an, ob der Webserver mit 5xx-Fehlern antwortet.
Ungewöhnlich große HTTP-Pakete	Nein	Gibt das Vorkommen an, wenn die HTTP-Nachrichten mit HTTP-Header-Größe die konfigurierten Werte in der Citrix ADC-Instanz überschreiten.
SSL Echtzeit-Verkehr	Nein	Analysiert den SSL-Verkehr, um den Echtzeitverkehr zu identifizieren, und schlägt optimale Konfigurationseinstellungen zur Verbesserung der Latenz vor.
Aufbau von SSL-Sitzungen	Nein	Gibt den Sitzungsaufbau über einen bestimmten Zeitraum an, der dazu führen kann, dass eine große Menge an Speicher von diesen Sitzungen in der Citrix ADC-Instanz aufgehalten wird.
Geringe Wiederverwendung von Sitz	Nein	Gibt an, ob die tatsächliche Anzahl von Sitzungen, die von der Citrix ADC-Instanz wiederverwendet werden, geringer ist.
Sättigung der NIC	Nein	Gibt die Gesamtzahl der Pakete an, die von den Schnittstellen verworfen werden.

App-Score-Komponenten	Vom Benutzer konfigurierte Schwellenwerte	Beschreibung
TCP-Queue-Limit Treffern neu zusammenbauen	Nein	Gibt an, ob die nicht bestellerischen Pakete einer TCP-Verbindung die konfigurierte Größe der Paketwarteschlange für nicht bestellte Pakete überschreiten.

Standardmäßig sind alle Komponenten aktiviert. Wenn Sie eine Komponente deaktivieren, führt Citrix ADM die endgültige App-Score-Berechnung nur basierend auf den ausgewählten Komponenten durch.

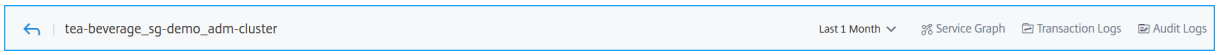
> Hinweis
>
> Sie können auch weiterhin Schwellenwerte konfigurieren, indem Sie zu **Analytics > Einstellungen** navigieren und auf **App-Score konfigurieren**klicken. Weitere Informationen finden Sie unter Erstellen eines Schwellenwerts und einer Warnung für Anwendungsanalysen

Anwendungsdetails für Microservices-Anwendungen

April 28, 2021

Klicken Sie im Dashboard auf eine Microservices-Anwendung, um weitere detaillierte Informationen zu erhalten.

Die ausgewählte Anwendungsseite wird angezeigt.

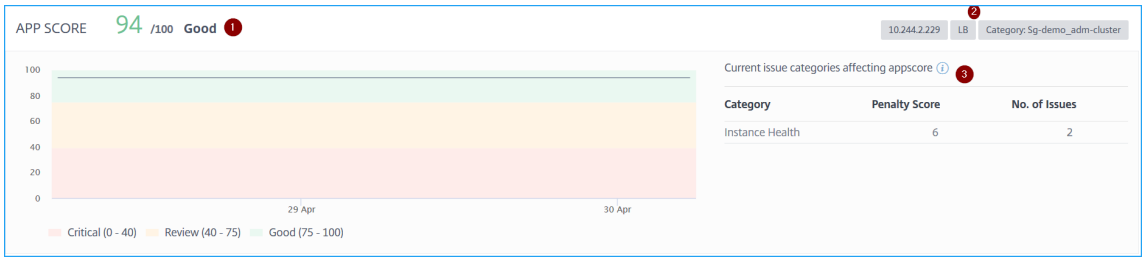


Auf der Seite mit den Anwendungsdetails:

- Wählen Sie die Zeitdauer aus der Liste aus, um Details für die bestimmte Zeitdauer anzuzeigen.
- Klicken Sie auf **Service-Diagramm**, um das Service-Diagramm für die ausgewählte Anwendung anzuzeigen. Weitere Informationen finden Sie unter Service-Diagramm für Anwendungen.
- Klicken Sie hier **Transaktionsprotokolle**, um die detaillierten Transaktionen für die ausgewählte Anwendung anzuzeigen.
- Klicken Sie auf **Überwachungsprotokolle**, um die detaillierten Überwachungsprotokollinformationen anzuzeigen.

Nachdem Sie die Zeitdauer ausgewählt haben, werden die folgenden Anwendungsdetails angezeigt:

- **App-Score** — Die Bewertungsbewertung für die ausgewählte Zeitdauer. Sie können auch die aktuellen Anwendungsprobleme anzeigen, die als Strafwert bezeichnet werden, der basierend auf der Problemkategorie gilt. Die Endpunktzahl wird als **100 minus Gesamtstrafe**berechnet.



1 — Bezeichnet die aktuelle App-Punktzahl

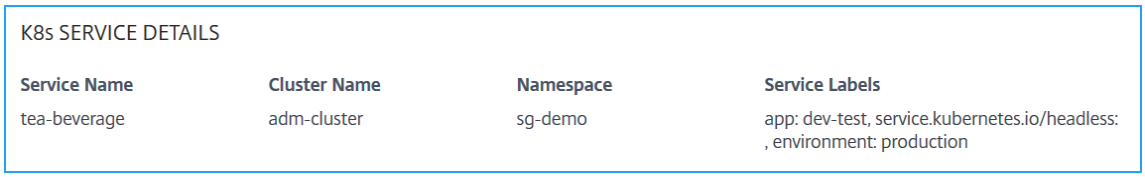
2 — Bezeichnet die CPX-IP-Adresse, den Anwendungstyp wie Lastenausgleich oder Content Switching sowie den Dienstnamespace und den Clusternamen, in dem der Dienst gehostet wird

3 — Bezeichnet die Probleme, die sich auf die aktuelle Bewertungsbewertung auswirken

Mit diesem Dashboard können Sie auch die aktuellen Probleme anzeigen, die sich auf die App-Bewertung auswirken. Sie können die Problemdetails unter Probleme anzeigen.

- **K8s Service-Details**

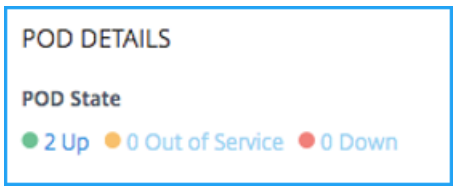
  Sie können die folgenden Details anzeigen:



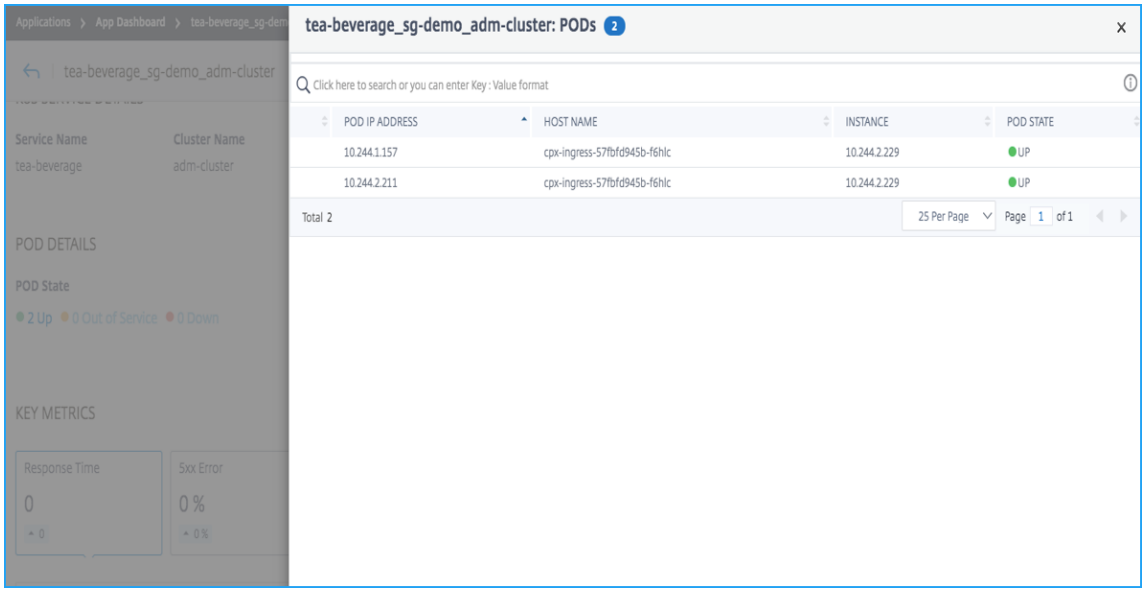
  - **Service-Name** — Der Service-Name
  - **Clustername** — Der Clustername, in dem der Dienst gehostet wird
  - **Namespace** — Der dem Dienst zugewiesene Namespace
  - **Service-Labels** — Die Service-Labels, die dem Service zugewiesen sind

- **Pod Details**

  Ein Pod ist eine Gruppe von Containern, die im Kubernetes-Cluster gehostet werden. In einem Pod können Sie mehrere containerisierte Anwendungen bereitstellen. Jeder Pod ist mit einer IP-Adresse verknüpft.



Klicken Sie auf den Podstatus, um die Details anzuzeigen

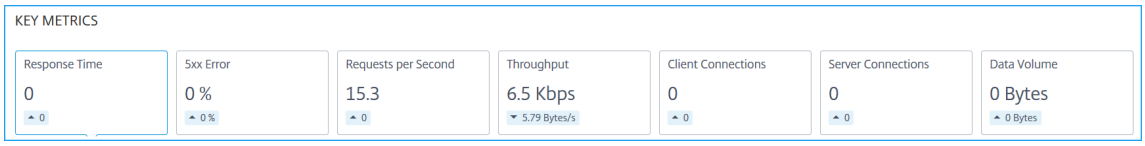


- **Pod-IP-Adresse** — Bezeichnet die Pod-IP-Adresse
- **Hostname** — Kennzeichnet den Hostnamen, der dem Pod zugewiesen ist.
- **Instanz** — Bezeichnet die IP-Adresse von Citrix ADC CPX
- **Podstatus** — Bezeichnet den aktuellen Status des Pods

- **Schlüsselmetriken** — Die wichtigsten Metriken, wie **Antwortzeit**, **5xx Fehler**, **Anforderungen pro Sekunde**, **Durchsatz**, **Clientverbindungen**, **Serververbindungen**und **Datenvolumen** sind angezeigt.

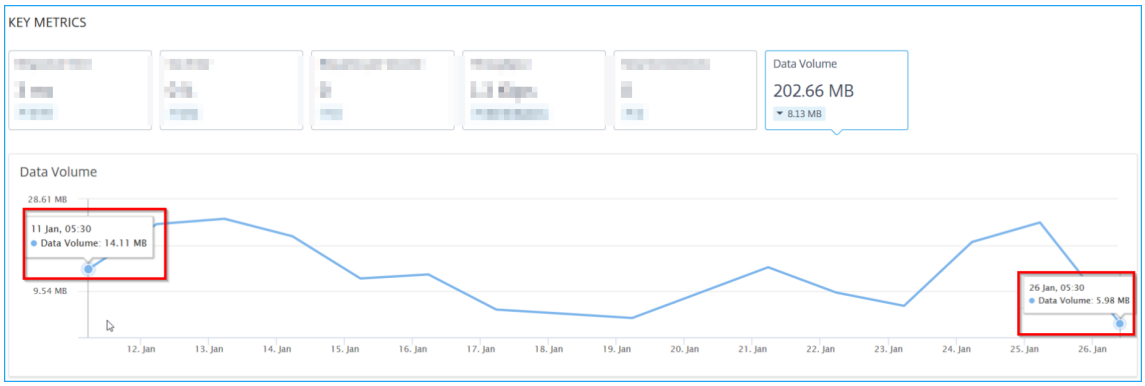
  In jeder Metrik können Sie den Durchschnittswert und den Differenzwert für die ausgewählte Zeitdauer anzeigen. Der Differenzwert wird als **erster Wert minus dem letzten Wert** der ausgewählten Zeitdauer berechnet.

  Sie können die folgenden Instanzmetriken in einem Diagrammformat für die ausgewählte Zeitdauer anzeigen:



  Die folgende Abbildung zeigt ein Beispiel für **Datenvolumen** und die ausgewählte Zeitdauer beträgt 1 Monat. Der Wert 202,66 MB ist das gesamte Datenvolumen für die 1-Monats-Dauer

und der Wert 8,13 MB ist der Differenzwert. In der Grafik ist der erste Wert 14,11 und der letzte Wert 5,98. Der Differenzwert beträgt 14,11 — 5,98 = 8,13 MB.

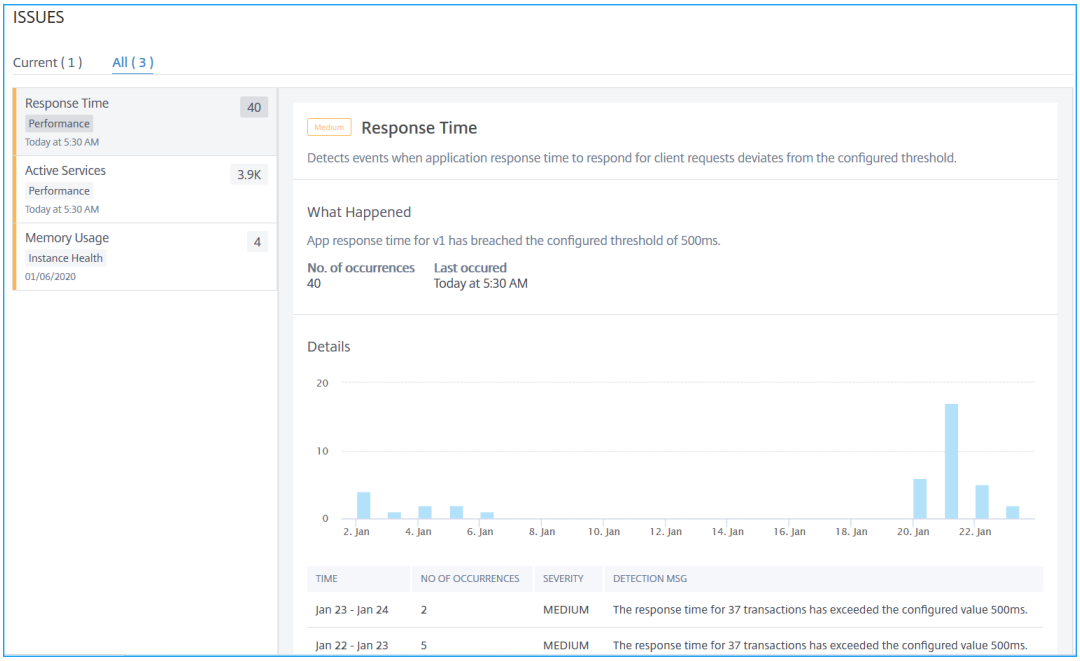


- **Probleme** — Die Probleme, die für die ausgewählte Anwendung gelten. Sie können die folgenden Probleme zusammen mit der Kategorie anzeigen:

Leistung	Instanz-Integrität	Config	Systemressourcen
Reaktionszeit	Durchschnittliche CPU-Auslastung	Hohe 5xx-Antwortvariablen	Unsachgemäßer Persistenz-Typ
Wiederverwendung der niedrigen Sitzung	Speicherauslastung	Ungewöhnlich große HTTP-Pakete	NIC-Kartensättigung
SurgeQueue-Aufbau		TCP-Queue-Limit Treffern neu zusammenbauen	
SSL-Echtzeit-Datenverkehr			

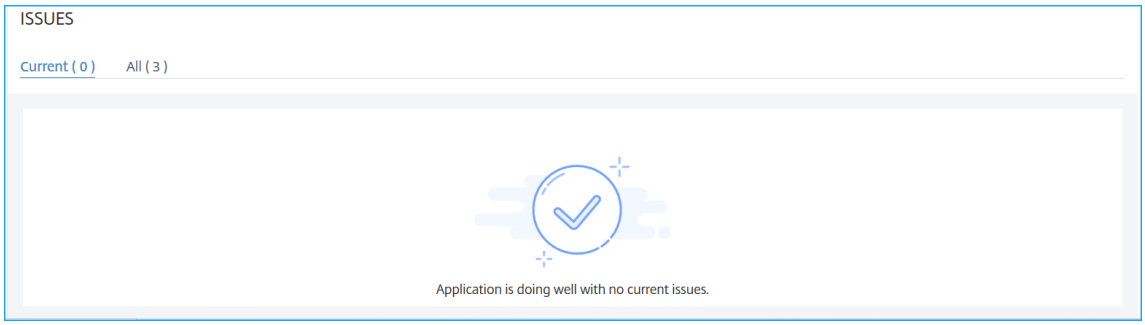
Klicken Sie auf jedes Problem, um die folgenden Informationen anzuzeigen:

- Gesamtvorkommen
- Empfohlene Aktionen zur Behebung des Problems
- Die Problemdetails wie Zeit, Dienstname, Gesamtereignisse, Schweregrad und Erkennungsnachricht

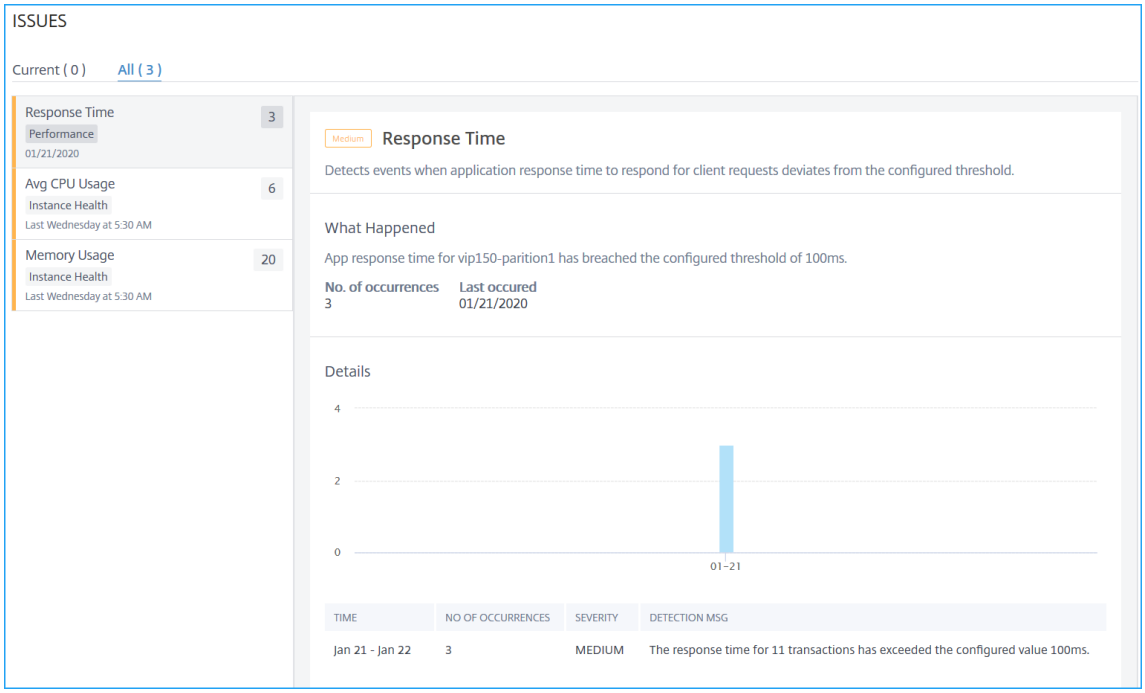


* Die Probleme, die auf der Registerkarte **Aktuell** angezeigt werden, beziehen sich auf die Anwendungsprobleme für die ausgewählte Zeitdauer.
* Die Probleme, die auf der Registerkarte **Alle** angezeigt werden, beziehen sich auf die Gesamtzahl der Anwendungsprobleme.

Das folgende Beispiel zeigt die Anwendungsprobleme für einen Tag. Auf der Registerkarte **Aktuell** werden keine aktuellen Probleme angezeigt, die sich auf die App-Bewertung auswirken.



Auf der Registerkarte **Alle** werden die insgesamt erkannten Probleme für die Dauer eines Tages angezeigt.



Web Insight-Dashboard

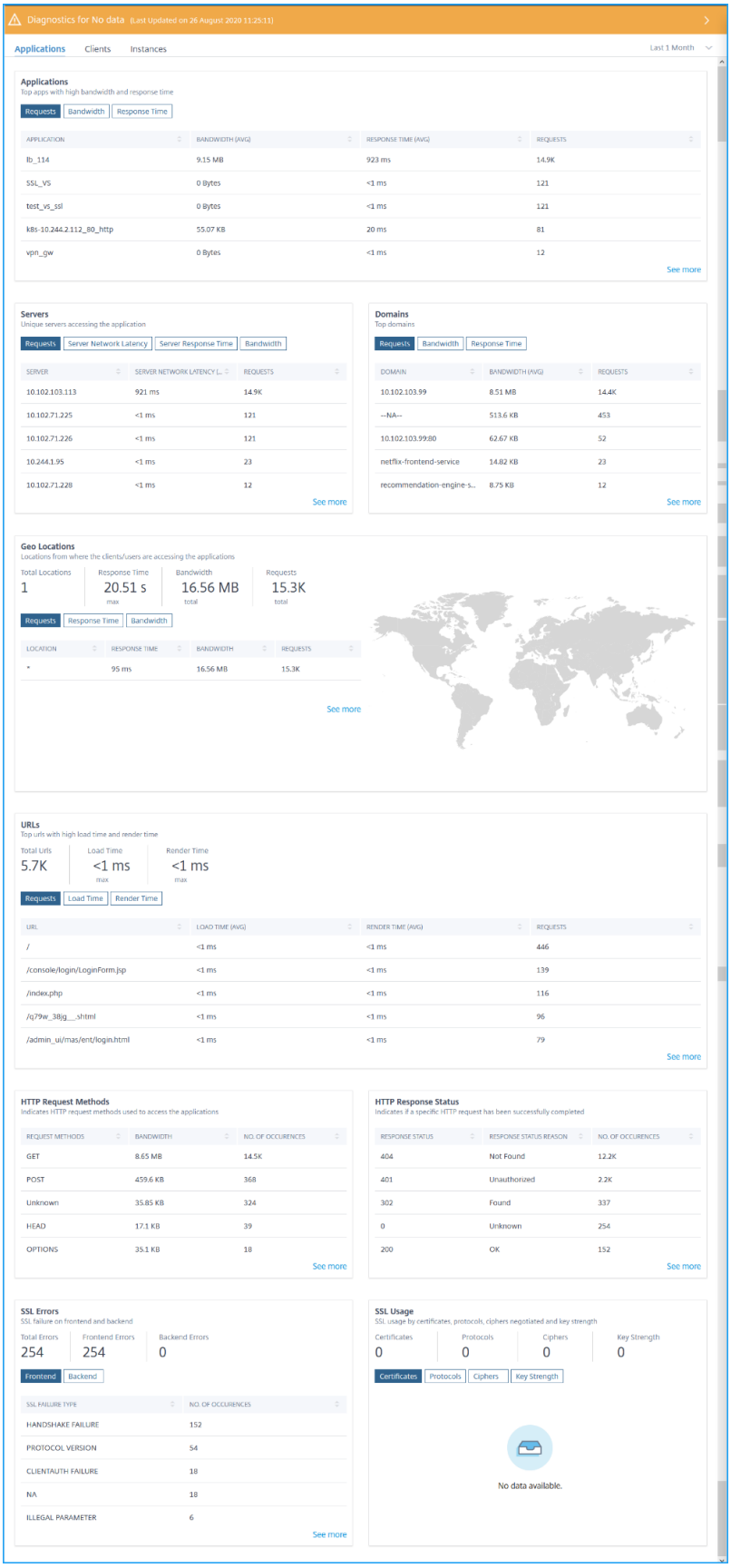
April 28, 2021

Die verbesserte Web Insight-Funktion wurde erweitert und bietet Einblicke in detaillierte Metriken für Webanwendungen, Clients und Citrix ADC-Instanzen. Dieses verbesserte Web Insight ermöglicht es Ihnen, die gesamte Anwendung aus den Perspektiven von Performance und Nutzung gemeinsam zu bewerten und zu visualisieren. Als Administrator können Sie Web Insight anzeigen für:

- Eine Anwendung. Navigieren Sie zu **Anwendungen > Dashboard**, klicken Sie auf eine Anwendung und wählen Sie die Registerkarte **Web Insight** aus, um die detaillierten Metriken anzuzeigen. Weitere Informationen finden Sie unter Analyse der Anwendungsnutzung.
- Alle Anwendungen. Navigieren Sie zu **Applications > Web Insight** und klicken Sie auf die einzelnen Registerkarten (Anwendungen, Clients, Instanz), um die folgenden Metriken anzuzeigen:

Anwendungen	Kunden	Instanzen
Anwendung mit Anomalien der Reaktionszeit	Kunden	Instanzmetriken
Anwendungen	Geo Standorte	Anwendungen
Server	HTTP-Anforderungsmethoden	Domänen

Anwendungen	Kunden	Instanzen
Domänen	HTTP-Antwortstatus	URLs
Geo Standorte	URLs	HTTP-Anforderungsmethoden
URLs	Betriebssystem	HTTP-Antwortstatus
HTTP-Anforderungsmethoden	Browser	Kunden
HTTP-Antwortstatus	SSL-Fehler	Server
SSL-Fehler	SSL-Nutzung	Betriebssystem
SSL-Nutzung		Browser

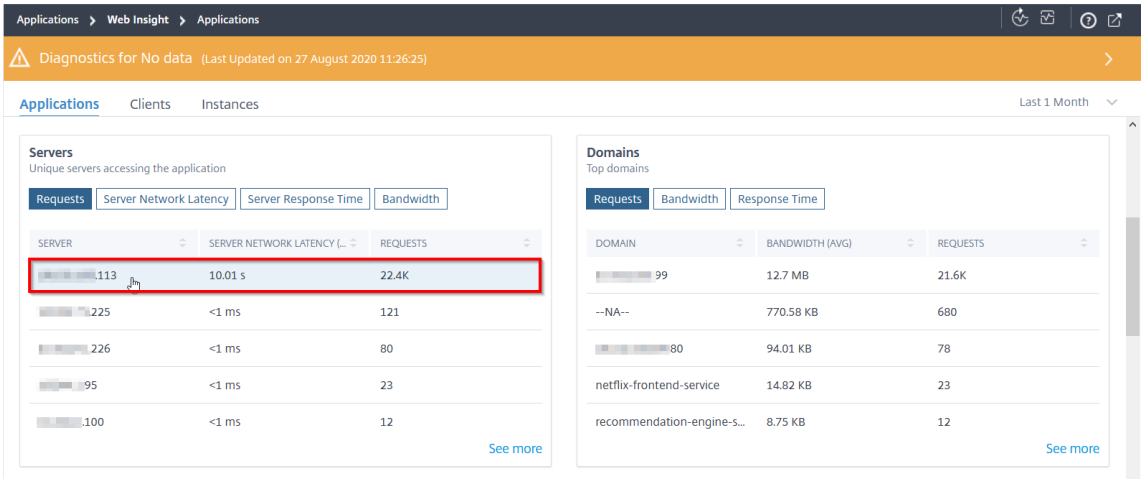


In jeder Metrik können Sie die Top-5-Ergebnisse anzeigen. Sie können klicken, um weitere Drill-downs durchzuführen, um das Problem zu analysieren und schneller Fehlerbehebungsmaßnahmen durchzuführen.

> Hinweis
>
> In einigen Szenarien ist Citrix ADC möglicherweise nicht in der Lage, die RTT-Werte für einige Transaktionen zu berechnen. Für solche Transaktionen sendet Citrix ADC den Wert als Null an Citrix ADM und Citrix ADM zeigt RTT als < 1 ms an.

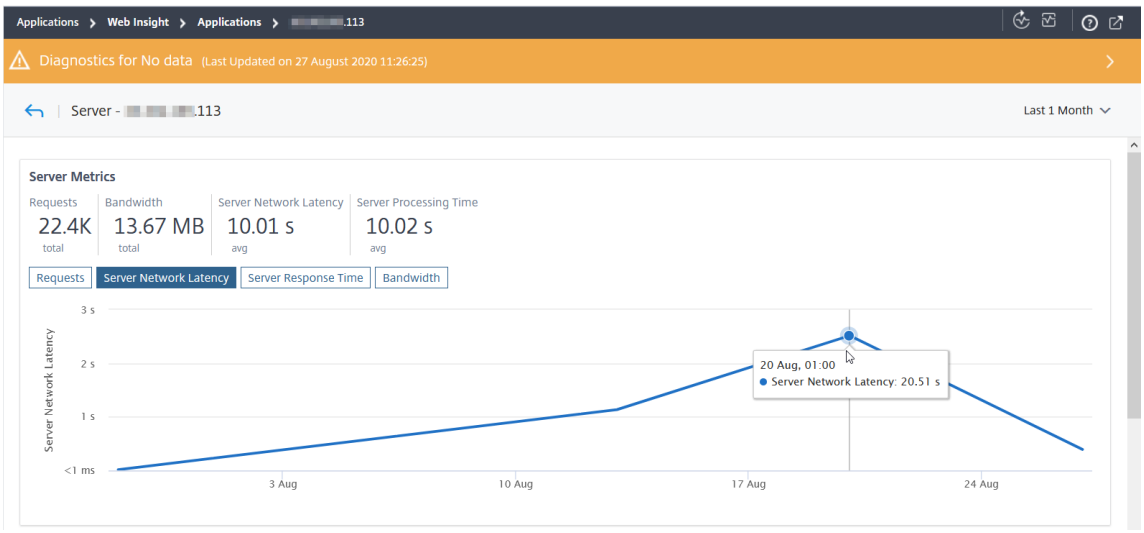
Bedenken Sie beispielsweise, dass Sie die Latenz des Servernetzwerks für eine Dauer von einem Monat analysieren und entscheiden möchten, ob Sie die Produktionsumgebung vergrößern oder verkleinern möchten. Um dies zu analysieren:

1. Wählen Sie Last 1 Month aus der Liste aus, scrollen Sie auf der Registerkarte **Anwendungen** nach unten zu **Servers**und klicken Sie auf einen Server.



   Die Metrikdetails für den ausgewählten Server werden angezeigt.

2. Wählen Sie die Registerkarte **Server Network Latency**, um die Latenz zu analysieren.



Die durchschnittliche Latenz zeigt 10,01s an, und anhand der Grafik können Sie analysieren, dass die Latenz des Servernetzwerks für den letzten Monat hoch zu sein scheint. Als Administrator können Sie sich entscheiden, die Produktionsumgebung zu vergrößern.

Weitere Informationen zum Anwendungsfall von Web Insight finden Sie unter Web Insight.

Analysieren Sie die Ursache für die Langsamkeit der Anwendung

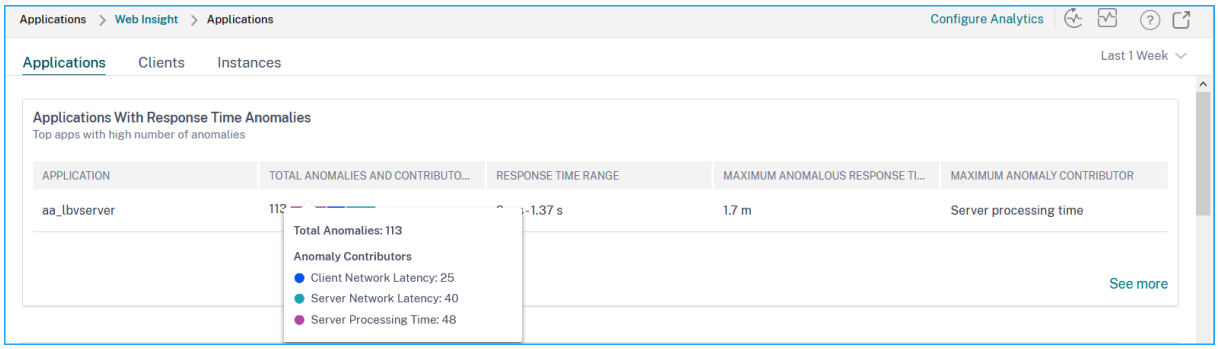
April 28, 2021

Anwendungsverlangsamung ist ein wichtiges Anliegen für jede Organisation, da dies zu geschäftlichen Auswirkungen oder Produktivität führt. Als Administrator müssen Sie sicherstellen, dass alle Anwendungen optimal funktionieren, um geschäftliche Auswirkungen zu vermeiden. Wenn Ihre Benutzer eine langsame Zugriffsart auf die Anwendung haben, müssen Sie sicherstellen, dass das Problem bei folgenden Problemen liegt:

- Latenz des Client-Netzwerks
- Servernetzwerklatenz
- Serververarbeitungszeit

Citrix ADM führt stündlich Anomalieprüfungen durch und meldet Anomalien für den Verkehr in der letzten Stunde, basierend auf bestimmten Voraussetzungen. Um beispielsweise falsch positive Ergebnisse zu vermeiden, werden die Anomalieprüfungen für diese Ergebnisse übersprungen, wenn die Reaktionszeit < 1 ms beträgt.

Auf der Seite " **Anwendungen > Web Insight** " können Sie die Anwendungen mit Anomalien der Reaktionszeit für die ausgewählte Dauer anzeigen. Die Metrik " **Anwendungen mit Antwortanomalien** " zeigt die fünf wichtigsten Anwendungen basierend auf den gesamten Anomalien an. Klicken Sie auf **Mehr** anzeigen, um alle Anwendungen anzuzeigen.



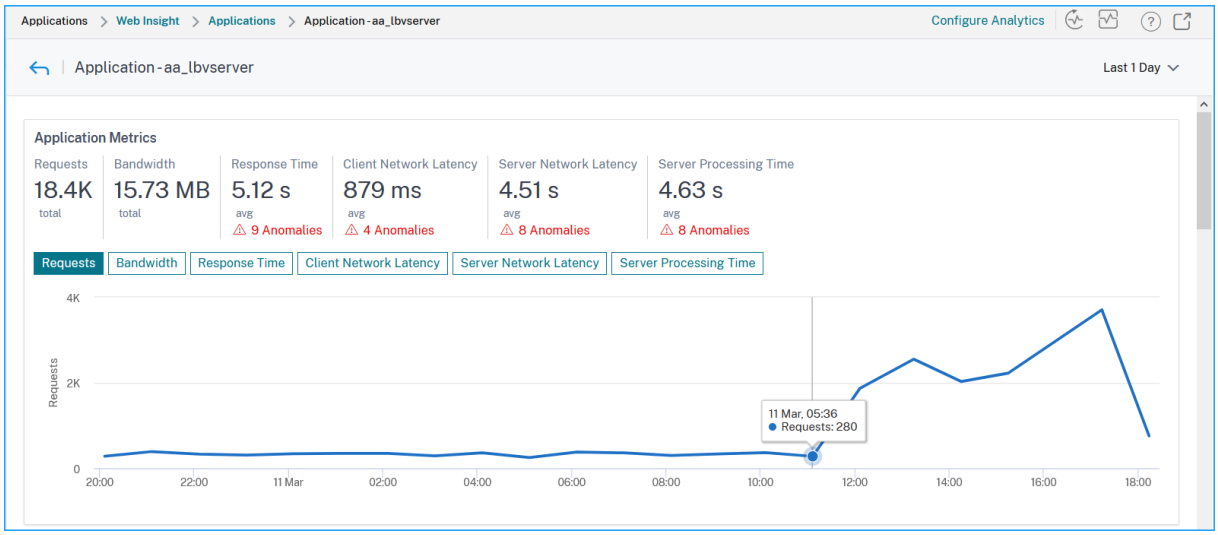
- **Anwendung** — Gibt den Namen der Anwendung an.
- **Total Anomalien und Contributors** - bezeichnet die gesamten Anomalien aus der Anwendung. Wenn Sie den Mauszeiger bewegen, können Sie die Gesamtanomalien anzeigen, die sich aus der

Latenz des Clientnetzwerks, der Latenz des Servernetzwerks und der Serververarbeitungszeit ergibt.

- **Reaktionszeitbereich** — Gibt den erwarteten Antwortzeiten der Anwendung an.
- **Maximale Anomale Reaktionszeit** — Bezeichnet die höchste Reaktionszeit der Anwendung.
- **Maximaler Anomaliebeitrag** — Gibt an, ob die maximale Anzahl von Anomalien für die Anwendung aus Client-Netzwerklatenz, Server-Netzwerklatenz oder Serververarbeitungszeit stammt.

Anwendung drilldown

Klicken Sie auf eine Anwendung, um die Details zu **Anwendungsmetriken** für die ausgewählte Dauer anzuzeigen.



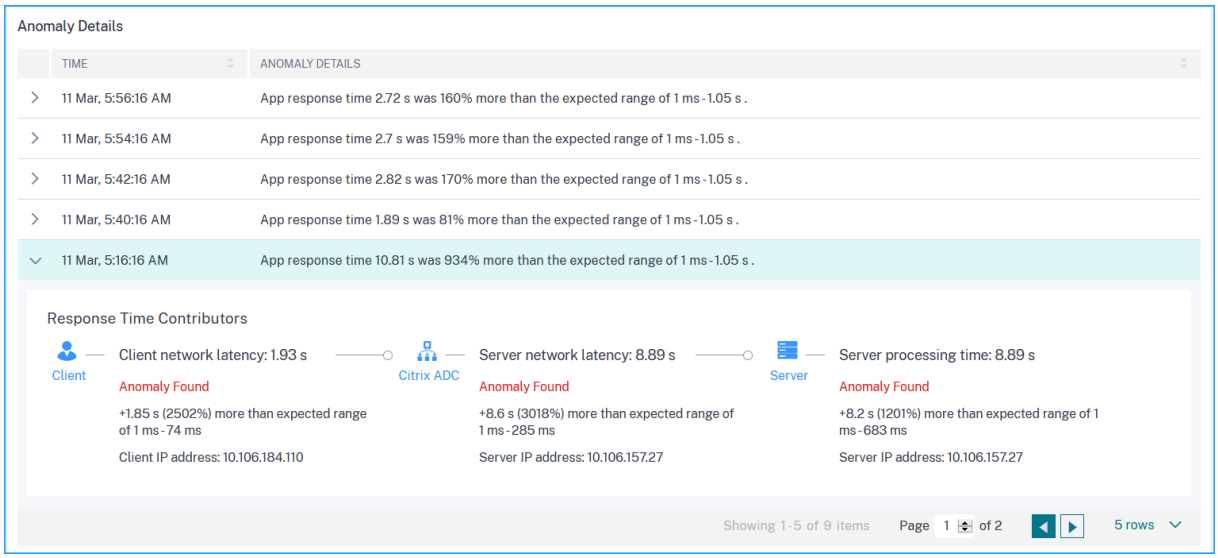
Mit den **Anwendungsmetriken** können Sie Folgendes anzeigen:

- **Anfragen** — Die Gesamtzahl der von der Anwendung eingegangenen Anfragen
- **Bandbreite** — Die Gesamtbandbreite, die von der Anwendung verarbeitet wird
- **Reaktionszeit** — Die durchschnittliche Reaktionszeit der Anwendung
- **Client-Netzwerklatenz** — Die durchschnittliche Client-Netzwerklatenz (vom Client zum ADC)
- **Server-Netzwerklatenz** — Die durchschnittliche Server-Netzwerklatenz (vom ADC zum Server)
- **Server-Verarbeitungszeit** — Die durchschnittliche Server-Verarbeitungszeit (vom Server zum ADC)

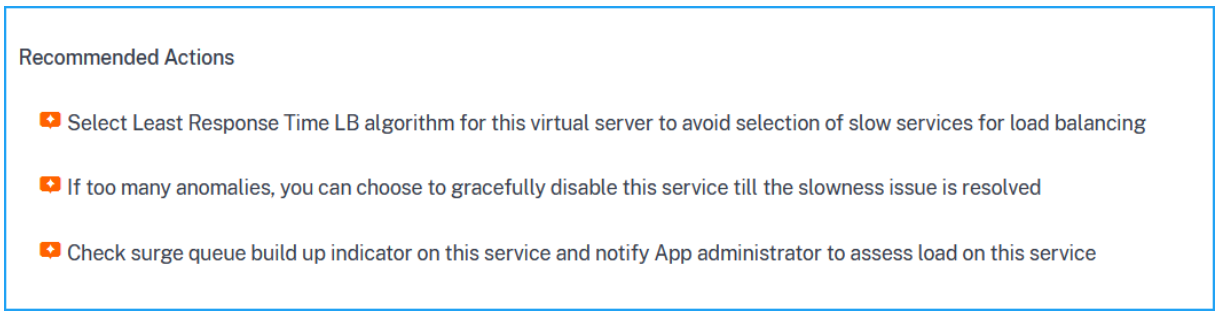
Wenn die Anwendung Anomalien aufweist, können Sie anzeigen, ob die Anomalien aus der Latenz des Client-Netzwerks, der Latenz des Servernetzwerks oder der Serververarbeitungszeit stammen. Klicken Sie auf jede Registerkarte, um Details anzuzeigen.

Reaktionszeit

Klicken Sie unter **Anomaly Details**auf, um Details für die Antwortzeitbeiträge (vom Client zum Server) anzuzeigen. Das folgende Beispiel hat eine Anomalie für Client-Netzwerklatenz, Server-Netzwerklatenz und Server-Verarbeitungszeit. Sie können auch die erwarteten Bereiche und den Verstoß anzeigen, der außerhalb des erwarteten Bereichs stattgefunden hat.



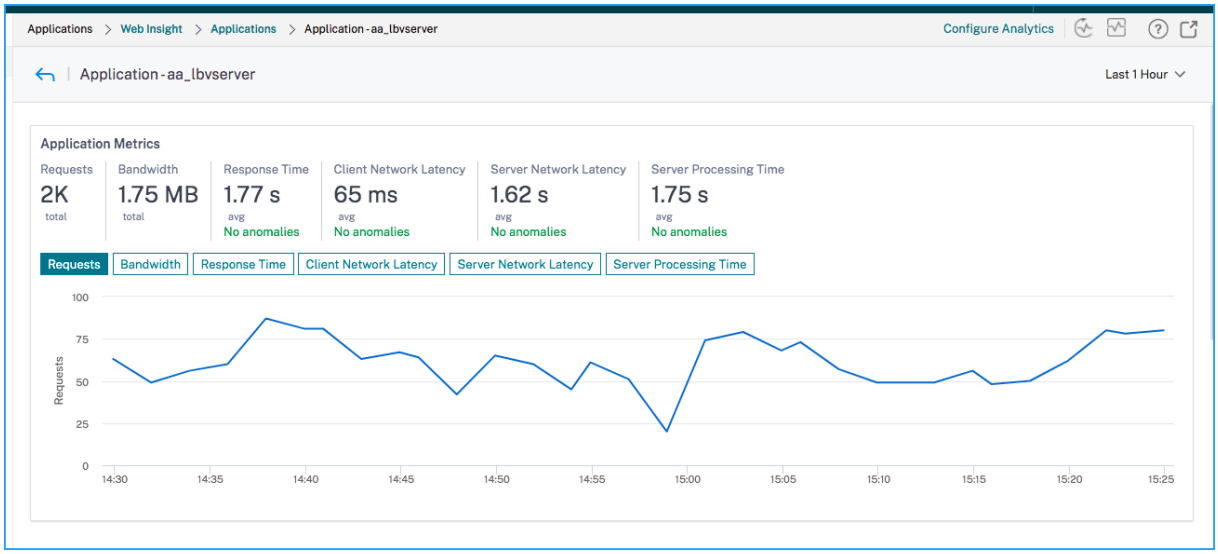
Die **empfohlenen Maßnahmen** schlagen Ihnen die möglichen Lösungen für die Anomalien vor.



In ähnlicher Weise können Sie auf die Registerkarten **Client-Netzwerklatenz**, **Server-Netzwerklatenz**und **Server-Verarbeitungszeit** klicken, um Folgendes anzuzeigen:

- Anomalie, die die erwartete Spanne durchbrochen hat.
- Empfohlene Maßnahmen, die Ihnen die möglichen Lösungen vorschlagen.

Wenn die Anwendung gut funktioniert, können Sie Anwendungsmetriken als keine Anomalien anzeigen.



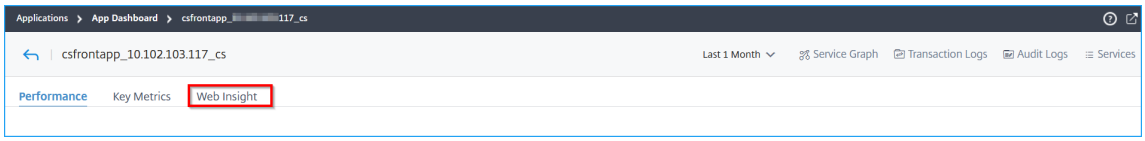
Analyse der Anwendungsverwendung

April 28, 2021

Anwendungseigentümer müssen die Möglichkeit haben, die gesamte Anwendung aus den Perspektiven der Leistung und Nutzung auszuwerten und zu visualisieren.

Das improvisierte **App Dashboard** ermöglicht es Ihnen, alle Anwendungsleistungen und Nutzungsmetriken zusammen anzuzeigen. Wenn Sie auf eine Anwendung klicken, werden neben den vorhandenen Metriken zur Anwendungsleistung auf der Registerkarte **Web Insight** die Metrikdetails angezeigt, die Ihnen helfen:

- Verstehen Sie Ihre Anwendungsnutzung.
- Korrelieren Sie alle Performance-Abweichungen mit den Verwendungsmetriken.



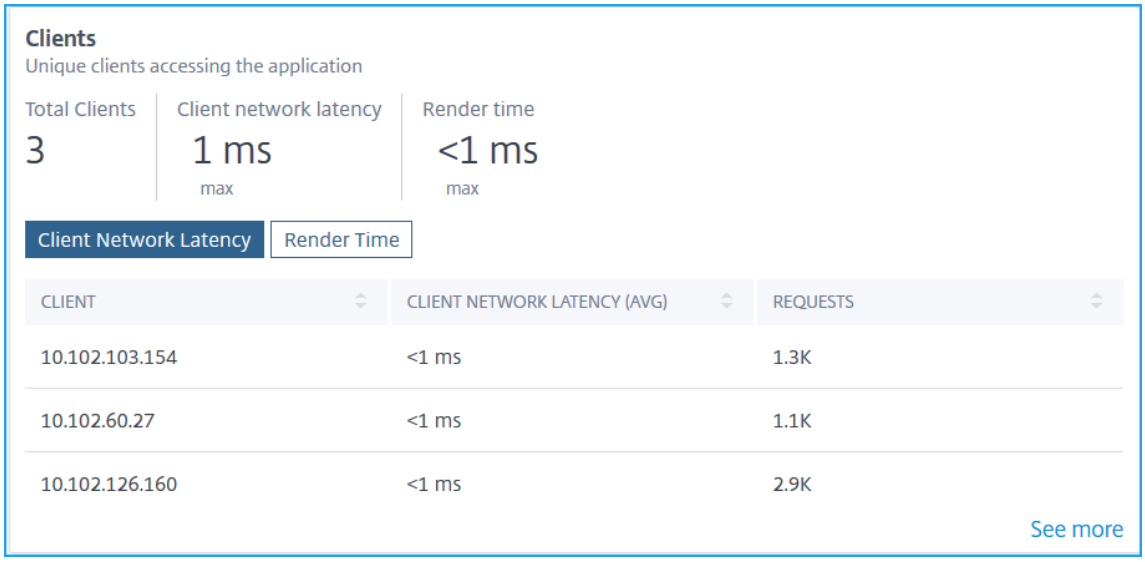
> **Hinweis**
>
> Für jede Metrik können Sie Optionen anzeigen, die den Maximalwert und den Gesamtwert angeben. Beispiel:
>
> Client network latency
> 1 ms
> max
>
> - Die maximale Clientnetzwerk-Latenz für die ausgewählte Dauer. Beachten Sie, dass Sie die Netzwerklatenz für Client 1 = 30 ms, Client 2 = 15 ms und Client 3

= 3 ms haben. In diesem Szenario zeigt die **Clientnetzwerklatenz** 30 ms an.

- - Die Gesamtbandbreite, die für die ausgewählte Dauer über alle verfügbaren Clients/Server verbraucht wird. Beachten Sie, dass Sie den Bandbreitenverbrauch für Client 1 = 30 MB, Client 2 = 45 MB, Client 3 = 40 MB haben. In diesem Szenario wird die Bandbreite angezeigt (30 MB + 45 MB + 40 MB) = 115 MB.

Im Folgenden finden Sie die Web Insight-Metriken, die Sie auf der Registerkarte **Verwendung** anzeigen können:

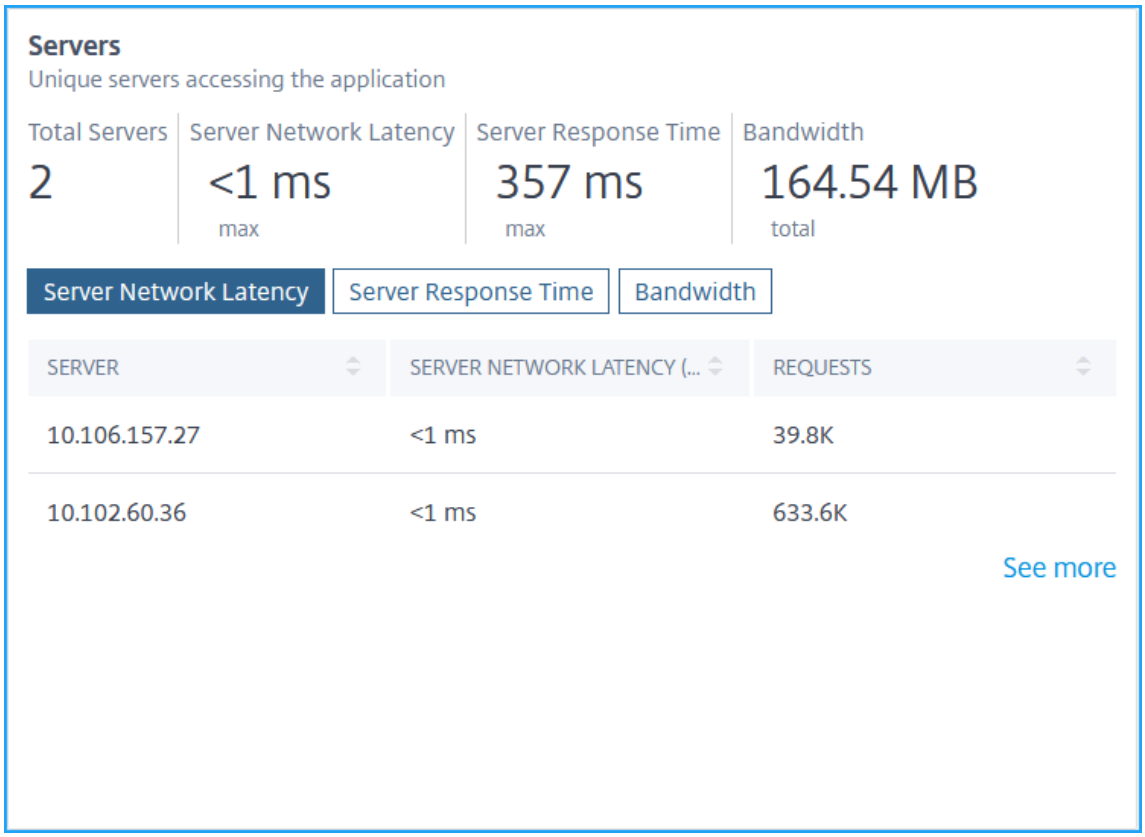
- **Clients** — Zeigt die Erkenntnisse für Clients an, die auf die Anwendung zugreifen:



  - **Clients insgesamt** — Zeigt die Gesamtzahl der Clients an, die auf die Anwendung zugreifen.
  - **Clientnetzwerklatenz** — Zeigt die Netzwerklatenz von Client zu Citrix ADC an. Klicken Sie auf die Registerkarte **Clientnetzwerklatenz**, um Folgendes anzuzeigen:
    - **Client** — Die Client-IP-Adresse.
    - **Client-Netzwerklatenz (Durchschn)** — Die durchschnittliche Netzwerklatenz des Clients.
    - **Anforderungen** — Die Gesamtanzahl der Anforderungen des Clients.
  - **Renderzeit** — Zeigt die Zeit an, die zum Rendern der Serverantwort erforderlich ist. Klicken Sie auf die Registerkarte **Renderzeit**, um Folgendes anzuzeigen:
    - **Client** — Die Client-IP-Adresse.
    - **Renderzeit (Durchschn)** — Die durchschnittliche Renderzeit des Clients.

    * **Anforderungen** — Die Gesamtanzahl der Anforderungen des Clients.

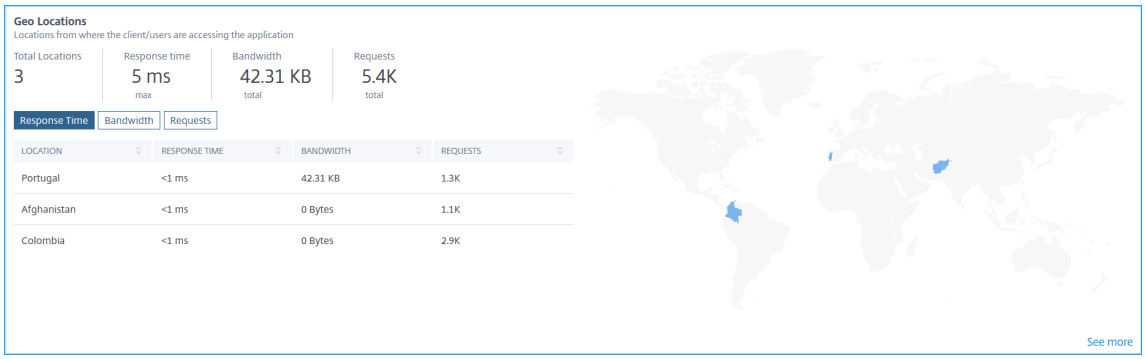
- **Server** — Zeigt die Erkenntnisse für Server an, die auf die Anwendung zugreifen:



  - **Server insgesamt** — Zeigt die Gesamtanzahl der Server an, die auf die Anwendung zugreifen.
  - **Servernetzwerklatenz** — Zeigt die Netzwerklatenz vom Server zu Citrix ADC an. Klicken Sie auf die Registerkarte **Servernetzwerk-Latenz**, um Folgendes anzuzeigen:
    * **Server** — Die IP-Adresse des Servers.
    * **Servernetzwerklatenz (Durchschn)** — Die durchschnittliche Netzwerklatenz vom Server.
    * **Anforderungen** — Die Gesamtanzahl der Anforderungen vom Server.
  - **Server-Antwortzeit** — Zeigt die Zeit an, die der Server für die Beantwortung von Anforderungen verwendet hat. Klicken Sie auf die Registerkarte **Server-Reaktionszeit**, um Folgendes anzuzeigen:
    * **Server** — Die IP-Adresse des Servers.
    * **Antwortzeit (Durchschn)** — Die durchschnittliche Antwortzeit vom Server.
    * **Anforderungen** — Die Gesamtanzahl der Anforderungen vom Server.

  - **Bandbreite** — Zeigt die Gesamtbandbreite an, die von den Servern verbraucht wird. Klicken Sie auf die Registerkarte **Bandbreite**, um Folgendes anzuzeigen:
    * **Server** — Die IP-Adresse des Servers.
    * **Bandbreite** — Die Gesamtbandbreite, die vom Server verbraucht wird.
    * **Anforderungen** — Die Gesamtanzahl der Anforderungen vom Server.

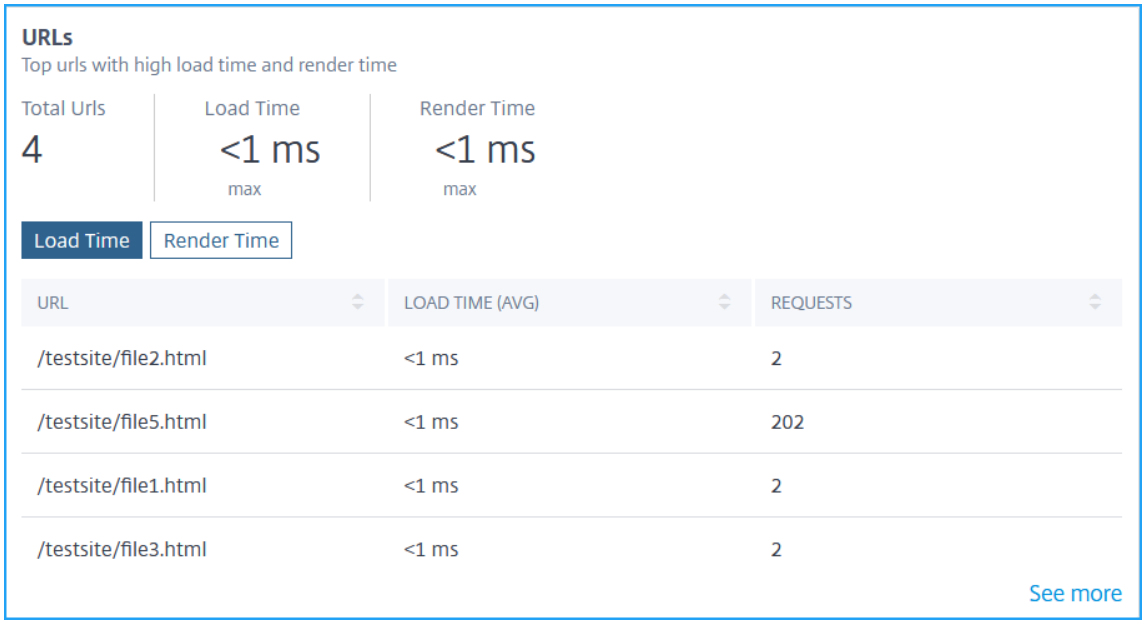
- **Geo-Standorte** — Zeigt die Erkenntnisse für Clients an, die von einem bestimmten Standort aus auf die Anwendung zugreifen:



  - **Gesamtstandorte** — Zeigt die Gesamtanzahl der Clientstandorte an, die auf die Anwendung zugreifen.
  - **Antwortzeit** — Zeigt die Antwortzeit vom Clientstandort an.
  - **Bandbreite** — Zeigt die Gesamtbandbreite an, die von Clients an allen Standorten verbraucht wird.
  - **Anforderungen** — Zeigt die Gesamtanzahl der Anforderungen von allen Clientstandorten an.

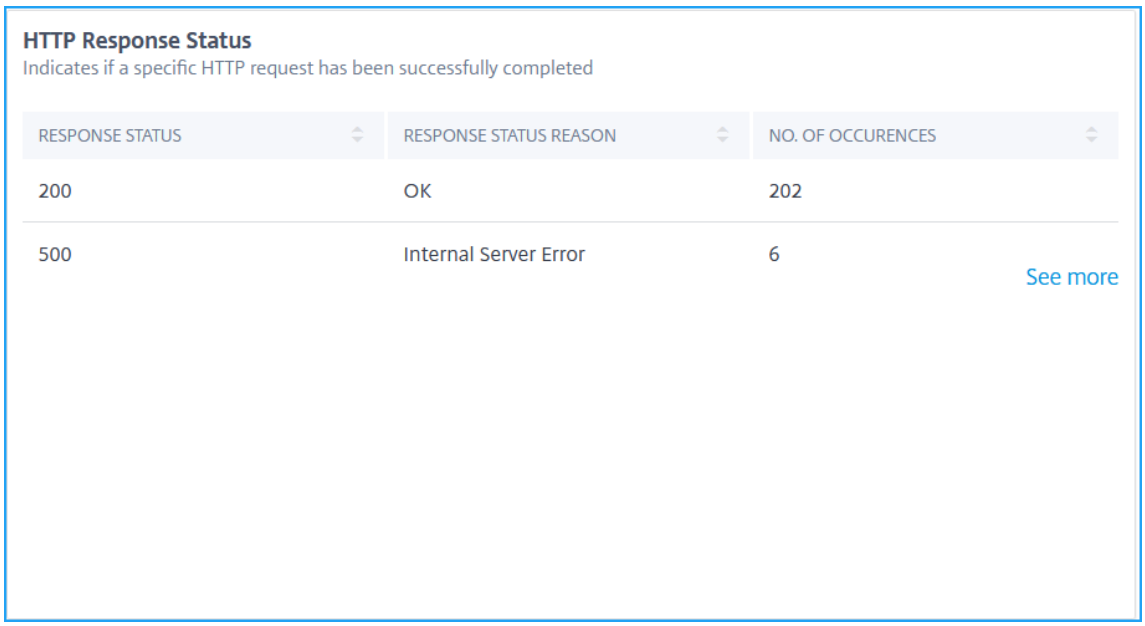
    Klicken Sie auf die einzelnen Registerkarten, um sie anzuzeigen:
    * **Speicherort** — Der Standortname.
    * **Antwortzeit** — Die durchschnittliche Antwortzeit vom Clientstandort.
    * **Bandbreite** — Die Bandbreite, die vom Clientstandort verbraucht wird.
    * **Anforderungen** — Die Gesamtanzahl der Anforderungen vom Clientstandort.

- **URLs** — Zeigt die Erkenntnisse für URLs mit hoher Lade- und Renderzeit an:



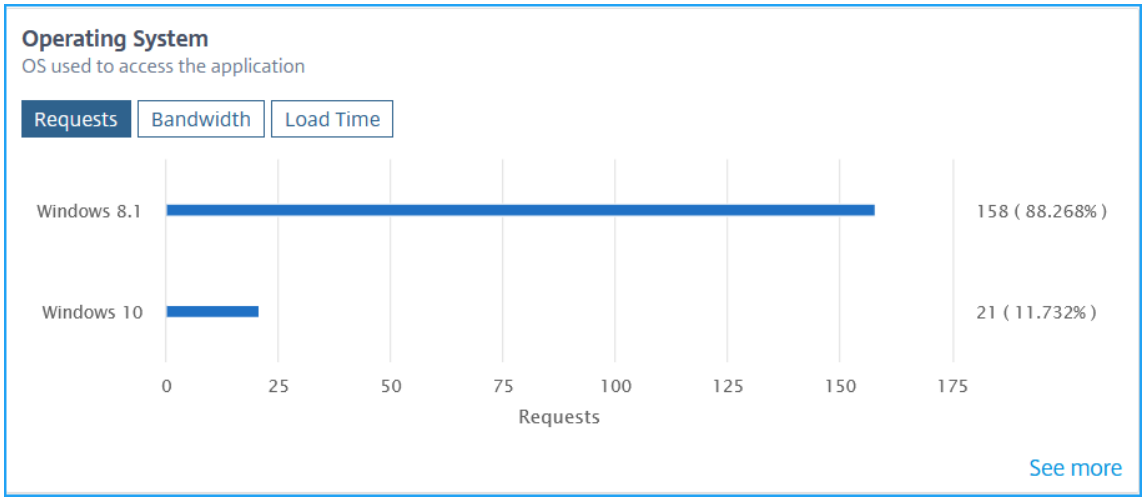
  - **Gesamt URLs** — Zeigt die Gesamtanzahl der URLs an.
  - Ladezeit — Zeigt die Zeit an, die für das Laden der URL gebraucht wurde. Klicken Sie auf die Registerkarte **Ladezeit**, um Folgendes anzuzeigen:
    * **URL** — Der URL-Name.
    * **Ladezeit (Durchschn)** — Die durchschnittliche Zeit, die für das Laden der URL verwendet wurde.
    * **Anforderungen** — Die Gesamtanzahl der Anforderungen von der URL.
  - **Renderzeit** — Zeigt die Zeit an, die für das Rendern und Anzeigen der URL verwendet wird. Klicken Sie auf die Registerkarte **Renderzeit**, um Folgendes anzuzeigen:
    * **URL** — Der URL-Name.
    * **Renderzeit (Durchschn)** — Die durchschnittliche Zeit, die für das Rendern der URL verwendet wurde.
    * **Anforderungen** — Die Gesamtanzahl der Anforderungen von der URL.

- **HTTP-Antwortstatus** — Zeigt die Erkenntnisse für eine bestimmte abgeschlossene HTTP-Anforderung an.



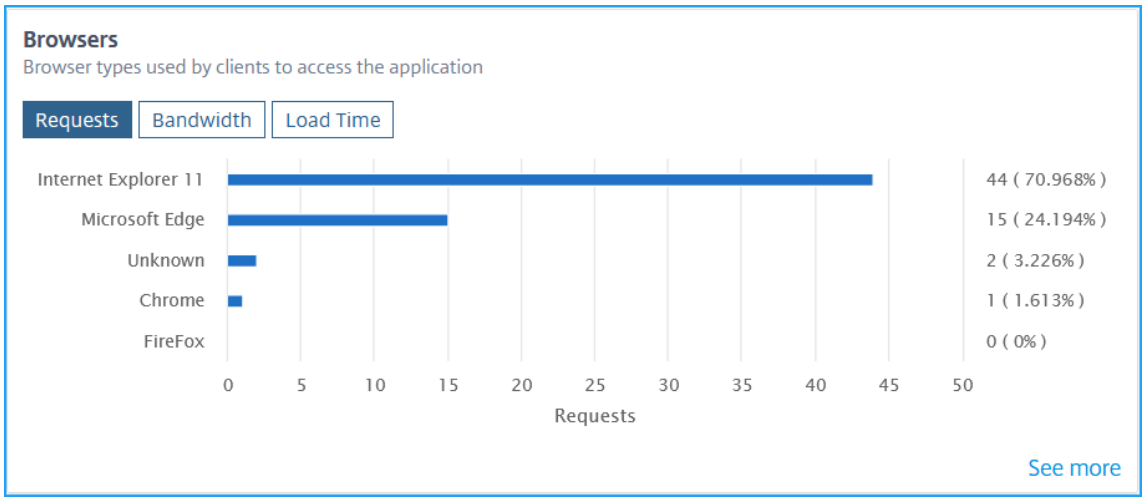
  - **Antwortstatus** — Zeigt den Antwortcode an, z. B. 2xx, 4xx, 5xx usw.
  - **Grund für den Antwortstatus** — Zeigt den Antwortgrund an, z. B. interner Serverfehler, Nicht gefunden usw.
  - **Anzahl von Vorkommen** — Zeigt die Gesamtzahl der Vorkommen an.

- **Betriebssystem** — Zeigt die Erkenntnisse für das Betriebssystem an, das auf die Anwendung zugreift.



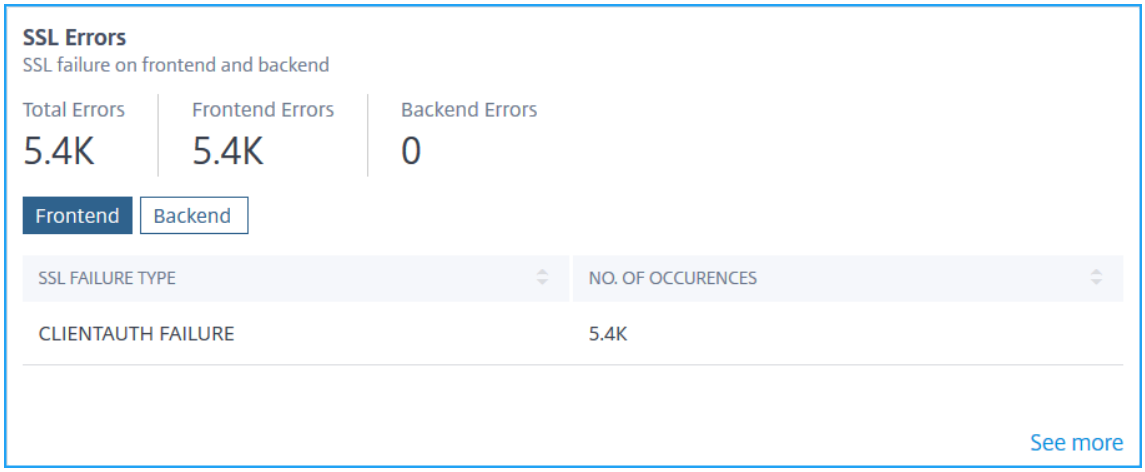
  - **Anforderungen** — Zeigt die Gesamtanzahl der Anforderungen jedes Betriebssystems an.
  - **Bandbreite** — Zeigt die Gesamtbandbreite an, die von den einzelnen Betriebssystemen verbraucht wird.
  - **Ladezeit** — Zeigt die Gesamtzeit an, die jedes Betriebssystem zum Laden vom Server genommen hat.

- **Browser** — Zeigt die Erkenntnisse für die Browsertypen an, die von den Clients für den Zugriff auf die Anwendung verwendet werden.



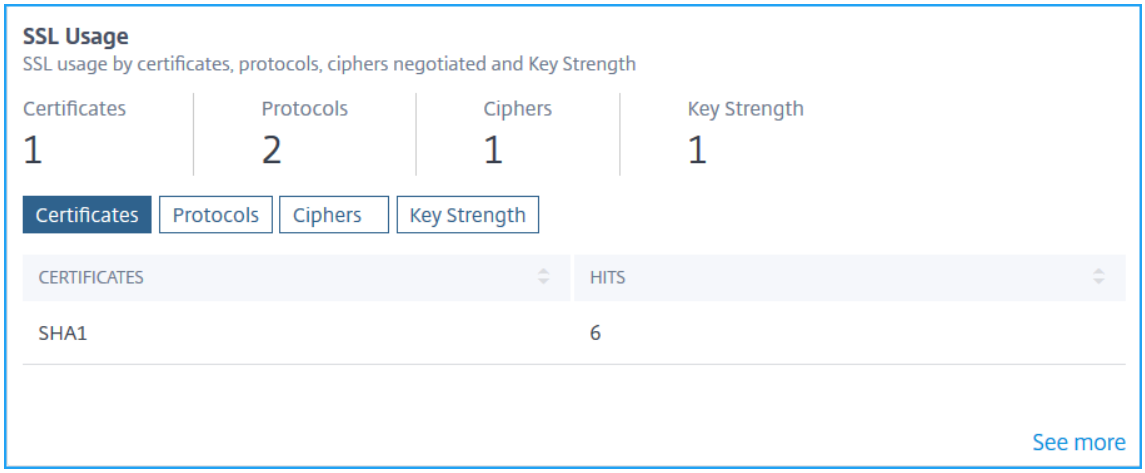
  - **Anforderungen** — Zeigt die Gesamtanzahl der Anforderungen jedes Browsers an.
  - **Bandbreite** — Zeigt die gesamte Bandbreite an, die von jedem Browser verbraucht wird.
  - **Ladezeit** — Zeigt die Gesamtzeit an, die ein Browser vom Server geladen hat.

- **SSL-Fehler** — Zeigt die Erkenntnisse für die SSL-Fehler vom Front-End-Server und Back-End-Server an.



  - **Total Error** — Zeigt die gesamten SSL-Fehlervorkommen an.
  - **Frontend** — zeigt die gesamten SSL-Fehler vom Front-End-Server an. Klicken Sie auf die Registerkarte **Frontend**, um den SSL-Fehlertyp und die Gesamtereignisse anzuzeigen.
  - **Backend** — Zeigt die gesamten SSL-Fehler vom Back-End-Server an. Klicken Sie auf die Registerkarte **Backend**, um den SSL-Fehlertyp und die Gesamtereignisse anzuzeigen.

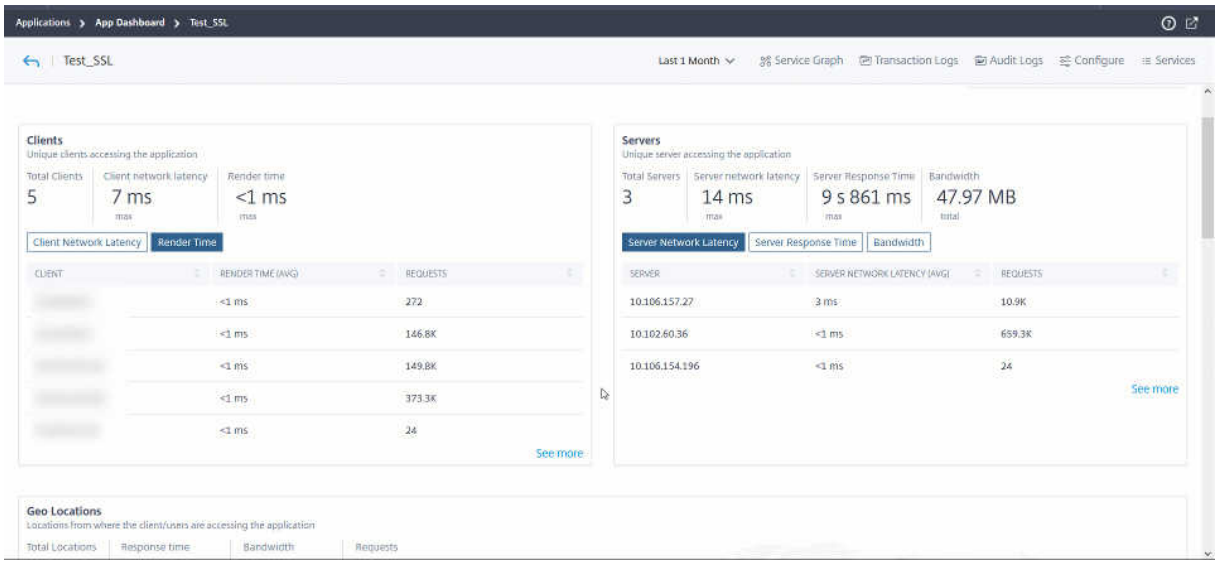
- **SSL-Verwendung** — Zeigt die Erkenntnisse für die SSL-Verwendung an, z. B. SSL-Zertifikate, Protokolle, Verschlüsselungen und Schlüsselstärke.



- **Zertifikate** — Zeigt die gesamten SSL-Zertifikate an. Klicken Sie auf die Registerkarte **Zertifikate**, um den Zertifikatnamen und die Gesamtzahl der Treffer anzuzeigen.
- **Protokolle** — Zeigt die gesamten SSL-Protokolle an. Klicken Sie auf die Registerkarte **Protokolle**, um Details mit SSL/TSL-Protokoll und Gesamtzahl der Treffer anzuzeigen.
- **Chiffre** — Zeigt die gesamte Chiffre an. Klicken Sie auf die Registerkarte **Chiffre**, um Details für jeden Chiffrier-Suite-Namen und die Gesamtzahl der Treffer anzuzeigen.
- **Schlüsselstärke** — Zeigt die Gesamtschlüsselstärke an, die in SSL-Zertifikaten verwendet wird. Klicken Sie auf die Registerkarte " **Key-Stärke** ", um Details für jede Key-Stärke und Gesamt-Treffer anzuzeigen.

Anzeigen von Metriken im grafischen Format

Für jede Metrik können Sie weitere Details in einem grafischen Format anzeigen, indem Sie auf **Mehr anzeigen** klicken. Klicken Sie auf **, um Details in einem grafischen Format anzuzeigen.



Im Folgenden finden Sie die Details, die Sie für jede Metrik anzeigen können, nachdem Sie auf die Option **Weitere anzeigen** klicken:

Name des Einblicks	Metriken	Beschreibung
—-	—-	—-
Kunden	Kunden	Bezeichnet die Client-Liste
	Renderzeit (AVG)	Bezeichnet die durchschnittliche Zeit, die der Client zum Rendern der Serverantwort genommen hat
	Clientnetzwerk-Latenz (AVG)	Kennzeichnet die durchschnittliche Netzwerklatenz vom Client zur Citrix ADC-Instanz
	Anforderungen	Bezeichnet die Gesamtanzahl der Anfragen vom Client
Server	Server	Bezeichnet die Serverliste
	Server-Verarbeitungszeit (AVG)	Bezeichnet die durchschnittliche Zeit, die der Server für die Verarbeitung der Anforderungen verwendet hat.
	Servernetzwerk-Latenz (AVG)	Kennzeichnet die durchschnittliche Netzwerklatenz vom Server zur Citrix ADC-Instanz
	Treffer	Bezeichnet die Gesamtanzahl der vom Server empfangenen Treffer
Geo Standorte	Standorte	Bezeichnet die Clientstandorte
	Reaktionszeit	Bezeichnet die gesamte Antwortzeit vom Clientstandort
	Bandbreite	Bezeichnet die gesamte Bandbreite, die vom Standort verbraucht wird
	Anforderungen	Bezeichnet die Gesamtanzahl der Anfragen vom Standort
URL	Renderzeit (AVG)	Bezeichnet die durchschnittliche Zeit, die zum Laden der Seite vom Server genommen wurde
	Ladezeit (AVG)	Zeigt die durchschnittliche Zeit an, die für die URL zum Rendern und Anzeigen verwendet wird.
	Treffer	Bezeichnet die Gesamtzahl der Treffer von der URL
HTTP-Antwortstatus	Name	Bezeichnet den Namen des Antwortstatus, z. B. “OK”, “Nicht gefunden”, “Interner Serverfehler” usw.
	Antwortstatus	Kennzeichnet den Antwortstatuscode, der vom Server empfangen wurde, z. B. 200, 400, 500 usw.
	Treffer	Kennzeichnet die Gesamtzahl der Treffer aus dem Antwortcode
	Bandbreite	Bezeichnet die gesamte verbrauchte Bandbreite
Betriebssystem	Betriebssystem	Bezeichnet den Namen des Betriebssystems, z. B. Windows, MAC
	Ladezeit	Bezeichnet die Gesamtzeit, die für das Laden des Betriebssystems vom Server erforderlich ist.
	Bandbreite	Bezeichnet die Gesamtbandbreite, die vom Betriebssystem verbraucht wird
	Anforderungen	Bezeichnet die Gesamtanzahl der Anforderungen vom Betriebssystem
Browser	Browser	Bezeichnet den Browsernamen wie Mozilla Firefox, Chrome usw.
	Ladezeit	Bezeichnet die Gesamtzeit, die ein Browser vom Server geladen hat.
	Bandbreite	Bezeichnet die Gesamtbandbreite, die vom Browser verbraucht wird

	Anforderungen	Bezeichnet die Gesamtanzahl der Anfragen aus dem Browser
SSL-Fehler	SSL-Fehlertyp	Bezeichnet den Fehlernamen wie CLIENTAUTH FAILURE
	Vorkommen	Bezeichnet die Gesamtereignisse für den SSL-Fehler
SSL-Verwendung	Bezeichnet den Protokollnamen und die Versionen wie TLS, SSL
	Treffer	Bezeichnet die Gesamtzahl der Treffer aus dem Protokoll

Weitere Informationen zu Web Insight-Anwendungsfällen finden Sie unter Web Insight.

Problembehandlung bei App-Dashboard

April 28, 2021

Nachdem Sie eine Anwendung im App Dashboard hinzugefügt haben, zeigt das Dashboard sofort die grundlegenden Konfigurationsdetails der App an. Die Details der Anwendungsanalyse wie App-Score, wichtige Metriken und Probleme werden innerhalb weniger Minuten (etwa 10 bis 15 Minuten) ausgefüllt. Weitere Informationen finden Sie unter Anwendungen.

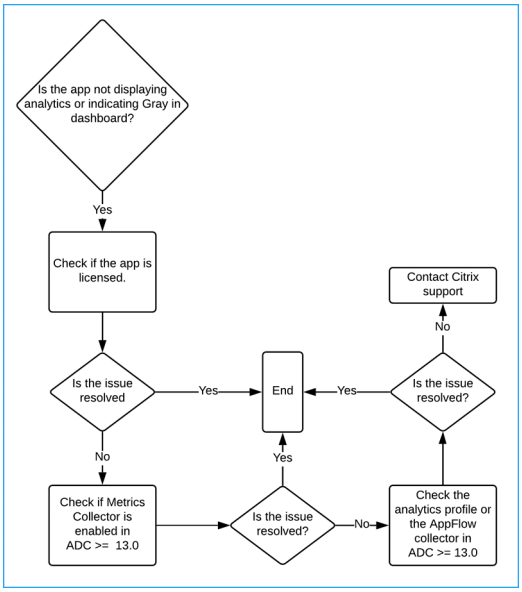
Sie müssen sicherstellen, dass es kein Problem mit dem Datenfluss von Metriken (AppFlow-Collector oder Analytics-Profil) aus der Citrix ADC-Instanz gibt. In diesem Dokument erhalten Sie weitere Informationen zum AppFlow-Collector und zum Analytics-Profil.

In diesem Dokument werden die Schritte zur Fehlerbehebung beschrieben, die Sie ausführen müssen, wenn:

- Sie klicken auf eine Anwendung, die Analysen für die ausgewählte Anwendung zeigen die erforderlichen Daten auch nach der genannten Dauer (10-15 Minuten) nicht an.
- Die CS- oder LB-Anwendung zeigt im App Dashboard immer die graue Farbe (**nicht zutreffender** Status) an.

> **Hinweis**
>
> Die in diesem Dokument erwähnten Fehlerbehebungsverfahren gelten nur für virtuelle **Content Switching** und **Load Balancing**.

Szenario zur Problem



Die Anwendung ist lizenziert

Sie müssen sicherstellen, dass die Anwendung lizenziert ist.

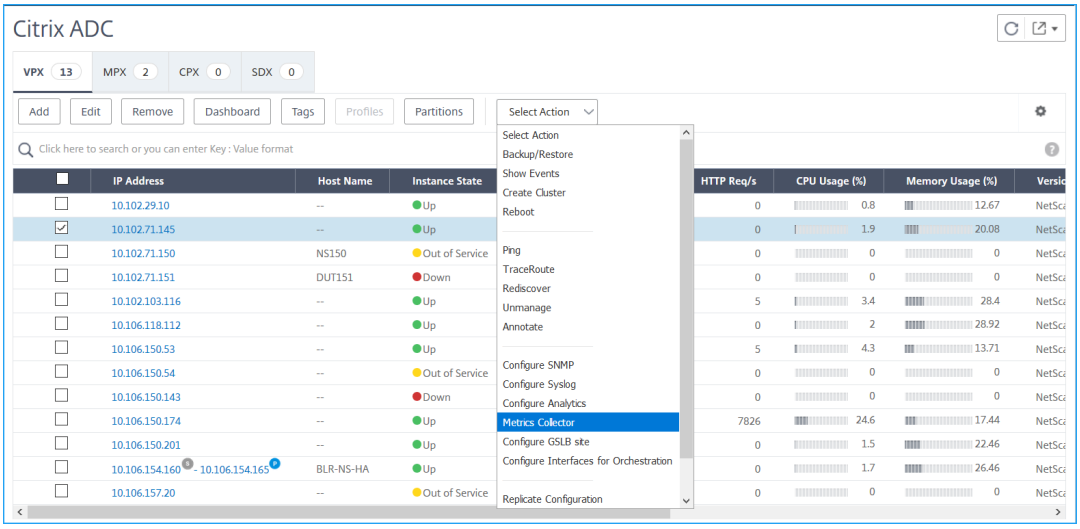
- **ADM-Dienst** - Navigieren Sie zu **Konto > Abonnements** und überprüfen Sie, ob die Anwendung unter **Virtual Server License Summary**lizenziert ist. Wenn die Anwendung nicht lizenziert ist, lesen Sie Verwalten der Lizenzierung und Aktivieren von Analysen auf virtuellen Servern dazu, den virtuellen Server zu lizenzieren.
- **ADM on-prem** — Navigieren Sie zu **System > Licensing & Analytics** und überprüfen Sie, ob die Anwendung unter **Virtual Server License Summary**lizenziert ist. Wenn die Anwendung nicht lizenziert ist, lesen Sie Verwalten der Lizenzierung und Aktivieren von Analysen auf virtuellen Servern dazu, den virtuellen Server zu lizenzieren.

Metrikensammler ist aktiviert

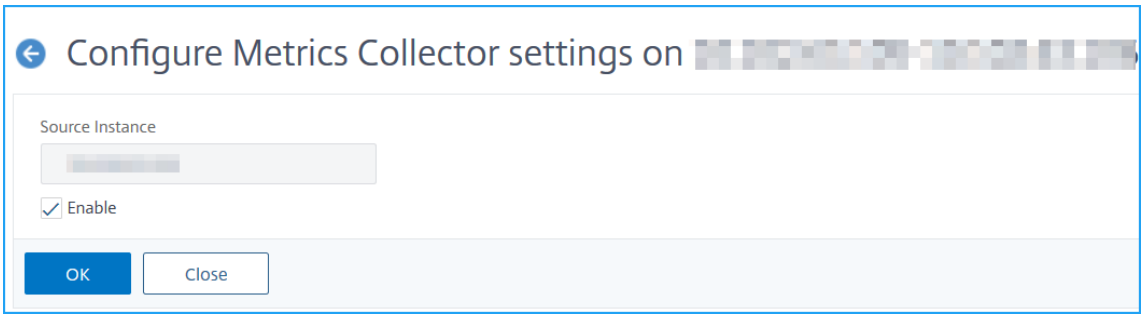
Sie müssen sicherstellen, dass **Metrics Collector** in der Citrix ADC-Instanz aktiviert ist.

Für Citrix ADC Version 13.0 oder höher ist Metrics Collector standardmäßig aktiviert, nachdem die ADC-Instanz erfolgreich in ADM hinzugefügt wurde. So stellen Sie sicher, ob der Metrikensammelpunkt

1. Navigieren Sie zu **Netzwerke > Instanzen**. Wählen Sie unter Instanzen den Instanz-Typ aus (z. B. Citrix ADC VPX).
2. Wählen Sie die Citrix ADC-Instanz aus.
    a) **Wählen Sie in der Liste Aktion auswählen** die Option **Metrikensammler** aus.



3. Stellen Sie sicher, dass auf der Seite **Metriken-Collector-Einstellungen konfigurieren** die Option **Aktivieren** aktiviert ist. Wenn nicht, wählen Sie die Option **Aktivieren** und klicken Sie auf **OK**.



Nachdem Sie den Metrikensammelpunkt aktiviert haben und die Daten immer noch nicht anzeigen können, überprüfen Sie Folgendes:

- Die AppFlow Collector in Citrix ADC-Instanzversion 13.0 **früher als 47.x Build**.
- Die Analytics-Profil in Citrix ADC-Instanz wurde **47.x oder höher**erstellt.

Ältere Builds von Citrix ADC-Instanzen

Bei Citrix ADC:

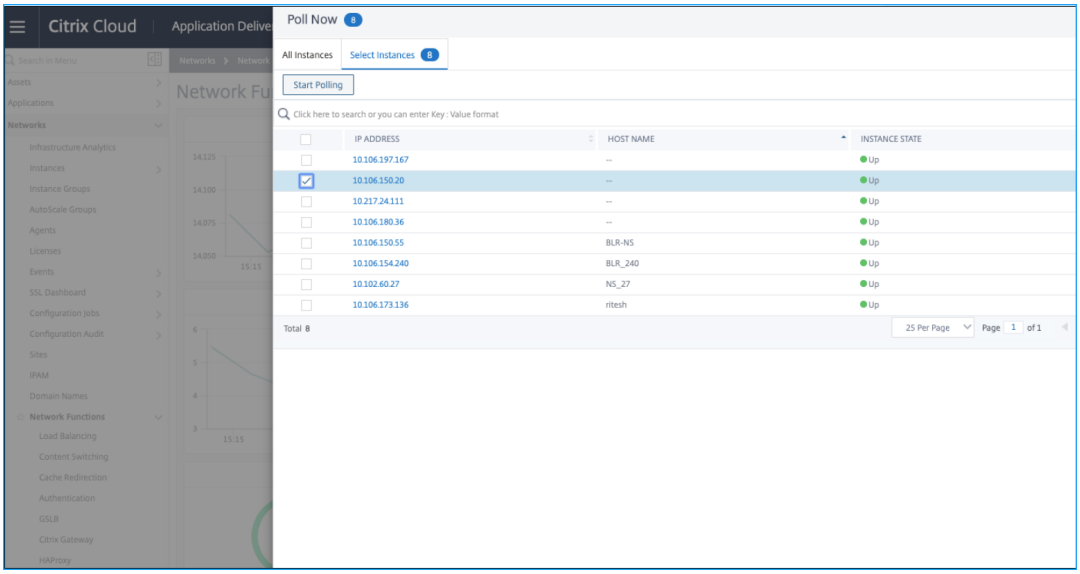
1. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass der Collector an Port 5563 **UP** ist:

```
sh appflow collector af_collector_rest_<adm_receiver_ip>
```



```
> sh appflow collector af_collector_rest_10.102.103.114
1) Name: af_collector_rest_10.102.103.114
IPv4 address: 10.102.103.114
Port: 5563
Netprofile:
Transport: rest
State: UP
Done
```

2. Wenn kein Collector verfügbar ist, führen Sie eine manuelle Instanzabfrage in Citrix ADM durch.
   a) Navigiere zu **Netzwerke > Netzwerkfunktion > Jetzt abfragen**
   b) Wählen Sie die Instanz aus und klicken Sie auf **Polling starten**.



   Wenn das Polling fehlschlägt, entfernen Sie die ADC-Instanz aus ADM und fügen Sie dann die ADC-Instanz erneut hinzu. Wenn Sie die ADC-Instanz hinzufügen, wird der Collector zu ADC hinzugefügt.

Wenn der Kollektor den Status **Down** anzeigt:

1. Stellen Sie sicher, dass die SNIP konfiguriert ist.

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA      Enabled
```

   Wenn SNIP nicht konfiguriert ist, müssen Sie SNIP konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von SNIP.

2. Stellen Sie sicher, dass die ADC-Instanz für ADM erreichbar ist.

Sie können validieren, indem Sie einen Ping-Test durchführen. Führen Sie `ping -S <SNIP> <adm_receiver_ip>` aus.

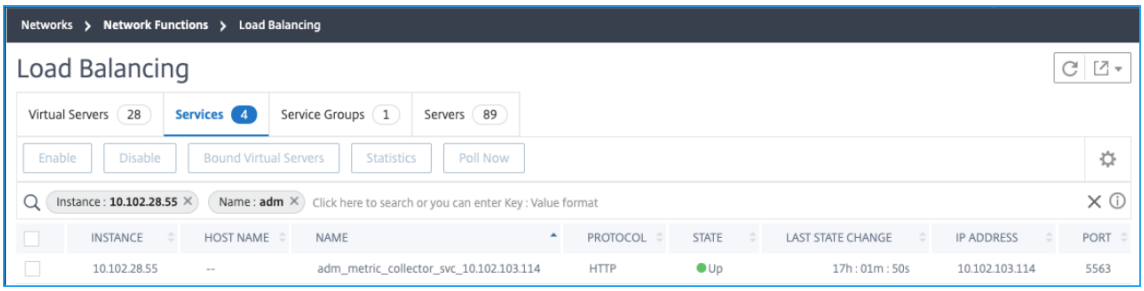
```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

Citrix ADC-Instanz wird später erstellt

Stellen Sie in Citrix ADM sicher, dass der Metrik-Collector-Dienst verfügbar ist:

1. Navigieren Sie zu **Netzwerke > Netzwerkfunktion > Load Balancing > Services**.
2. Filtern Sie in der Suchleiste nach **Instanz: (IP-Adresse)** und **Name: ADM**.
3. Stellen Sie sicher, ob `adm_metric_collector_svc_<adm_receiver ip>` verfügbar ist. Die IP-Adresse kann entweder die ADM-Verwaltungs-IP oder die Agenten-IP sein.

   Stellen Sie sicher, dass sich dieser Dienst im **UP-Status** befindet und auf Port 5563 ausgeführt wird.



Wenn Sie die Daten immer noch nicht anzeigen können, stellen Sie sicher, dass der Collector-Dienst an das Zeitreihenanalyseprofil in Citrix ADC gebunden ist.

1. Melden Sie sich bei Citrix ADC an
2. Führen Sie den folgenden Befehl aus:

   ```
   sh analytics profile ns_analytics_time_series_profile
   ```



```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Wenn der Kollektor den Status **Down** anzeigt:

1. Stellen Sie sicher, dass die SNIP konfiguriert ist.

   ```
   > sh ip | grep SNIP
   2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA       Enabled
   ```

   Wenn SNIP nicht konfiguriert ist, müssen Sie SNIP konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von SNIP.

2. Stellen Sie sicher, dass die ADC-Instanz für ADM erreichbar ist.

   Sie können validieren, indem Sie einen Ping-Test durchführen. Führen Sie `ping -S <SNIP> <adm_receiver_ip>` aus.

   ```
   > ping -S 10.106.150.34 10.102.103.114
   PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
   64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
   64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
   64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
   ```

3. Stellen Sie sicher, dass die Verkehrskonnektivität über Telnet den Dienst verbinden kann.

   ```
   root@ns# telnet 10.102.103.114 5563
   Trying 10.102.103.114...
   Connected to 10.102.103.114.
   Escape character is '^]'.
   ^]
   telnet> q
   Connection closed.
   ```

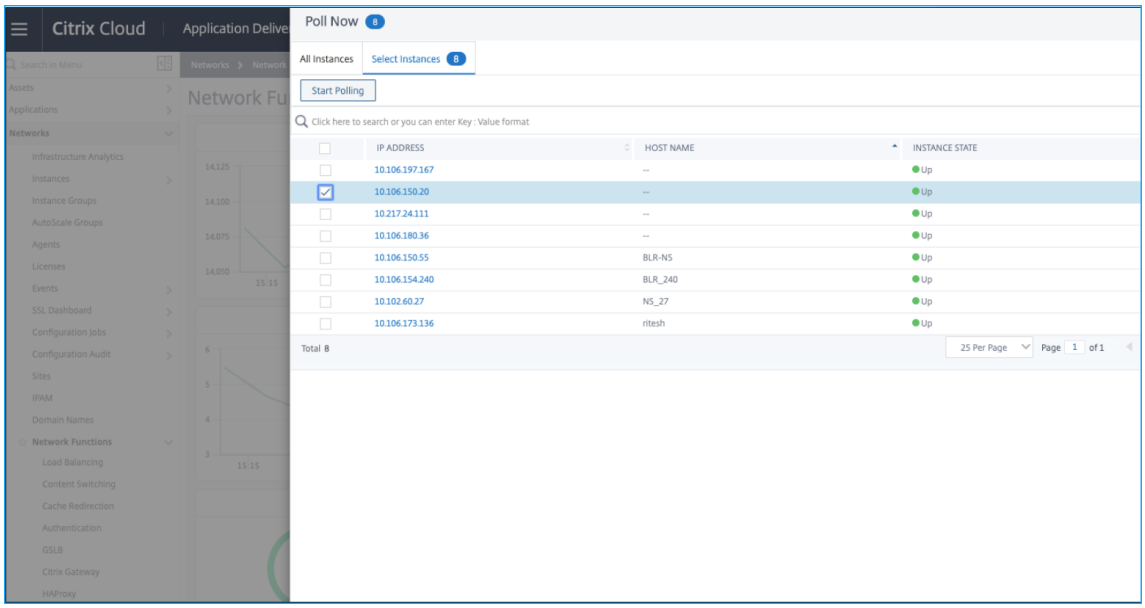
   Wenn Telnet in der Lage ist, den Dienst zu verbinden, existiert eine Firewall, die den Metrikdatenfluss blockiert. Sie müssen das Blockproblem der Firewall lösen.

Wenn kein Collector-Dienst an das Zeitreihenanalyseprofil in Citrix ADC gebunden ist, wird Collector als leer angezeigt.

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector:
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Sie müssen eine manuelle Abfrage für die Instanz in Citrix ADM durchführen.

1. Navigiere zu **Netzwerke > Netzwerkfunktion > Jetzt abfragen**
2. Wählen Sie die Instanz aus und klicken Sie auf **Polling starten**.



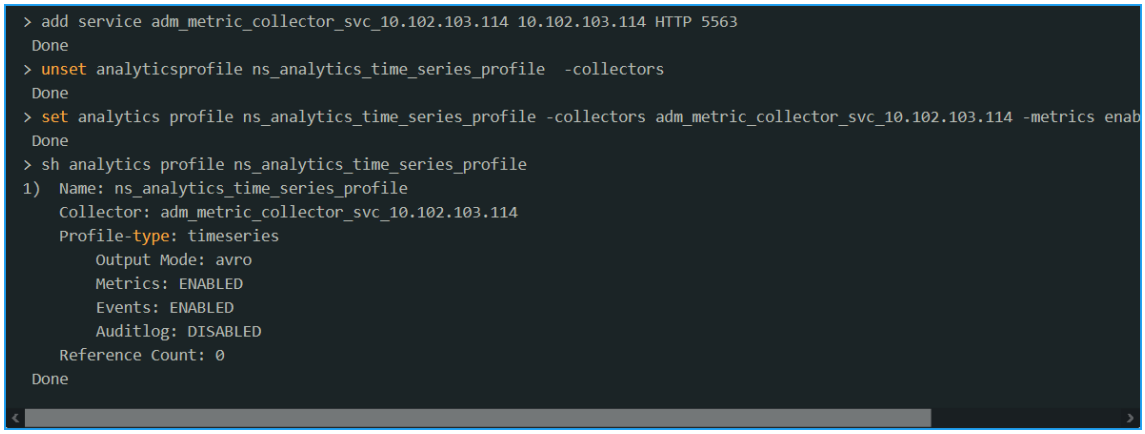
Wenn das Abfragen fehlschlägt, fügen Sie den Collector-Dienst direkt in der Citrix ADC-Instanz mit den folgenden Befehlen hinzu:

```
add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip
> HTTP 5563
```

```
unset analyticsprofile ns_analytics_time_series_profile -collectors
```

```
set analytics profile ns_analytics_time_series_profile -collectors
adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -events
enabled
```


Das Analytics-Zeitreihenprofil wird aktualisiert.



Wenn das Problem auch nach Durchführung aller genannten Schritte zur Fehlerbehebung weiterhin besteht, wenden Sie sich an den **Citrix Support**.

Erstellen eines Schwellenwerts und einer Warnung für Anwendungsanalysen

April 28, 2021

Mit der Anwendungsanalyse in Citrix ADM können Sie die verschiedenen Arten von Datenverkehr überwachen, der durch Citrix ADC-Instanzen fließt. Mit Citrix ADM können Sie Schwellenwerte für die folgenden Leistungsindikatoren festlegen, um den Datenverkehr und die App-Bewertung zu überwachen.

Sie können Schwellenwerte konfigurieren und die App-Bewertung für CPU, Arbeitsspeicher, NIC-Verwertungen und Reaktionszeit überwachen.

So konfigurieren Sie die App-Score in Citrix ADM:

1. Navigieren Sie in Citrix ADM zu **Analytics** > **Einstellungen**.
2. Klicken Sie auf der Seite **Einstellungen** auf **App-Score konfigurieren**.
3. Geben Sie auf der Seite **App-Score konfigurieren** die Werte für die folgenden Parameter ein:
    a) **Niedriger CPU-Schwellenwert**. Der niedrigere Schwellenwert der gesamten CPU-Auslastung in der Citrix ADC-Instanz.
    b) **Hoher CPU-Schwellenwert**. Der höhere Schwellenwert der gesamten CPU-Auslastung in der Citrix ADC-Instanz.
    c) **Niedriger Speicherschwellenwert**. Der niedrigere Schwellenwert der Gesamtspeicher-auslastung in der Citrix ADC-Instanz.

d) **Hoher Speicherschwellenwert**. Der höhere Schwellenwert der Gesamtspeicherauslastung in der Citrix ADC-Instanz.

e) **Niedrige NIC verwirft SLA**. Der niedrigere Schwellenwert von Paketen, die von den Schnittstellen verworfen werden.

f) **Hohe NIC verwirft SLA**. Der höhere Schwellenwert von Paketen, die von den Schnittstellen verworfen werden.

g) **Reaktionszeit**. Das Zeitintervall zwischen dem Senden eines Anforderungspakets und dem Empfangen des ersten Antwortpakets vom Dienst, der auf dem virtuellen Server konfiguriert ist. Der in Citrix ADM konfigurierte Standardwert beträgt 500 ms.

h) **Schwellenwert für aktive Dienste**. Der Schwellenwert des Prozentsatzes der Dienste, die aktiv sein müssen, die an den virtuellen Server gebunden sind.

4. Klicken Sie auf **OK**.

Intelligente App Analytics

April 28, 2021

Intelligent App Analytics ermöglicht es Ihnen, Probleme mit der Anwendungsleistung mithilfe von Machine Learning und Regelalgorithmen zu identifizieren. Die intelligente App Analytics-Funktion von Citrix ADM:

- Bietet eine einfache und skalierbare Lösung für die Überwachung und Fehlerbehebung von Anwendungen, die über Citrix ADC-Instanzen bereitgestellt werden.
- Überwacht alle Anwendungsebenen, um die Bearbeitungszeit für die Fehlerbehebung zu reduzieren und die allgemeine Anwendungsverfügbarkeit zu verbessern.

In einer typischen Bereitstellung erfüllen Tausende von Servern die Datenanforderungen der Benutzer. Der an diese Server gesendete Datenverkehr wird Lastausgleich und von virtuellen Servern überwacht, die auf Citrix ADC Appliances konfiguriert sind. Jeder virtuelle Server ist an mehrere Dienste gebunden, die die Back-End-Server darstellen. In solchen Bereitstellungen unterstützt die Intelligente App Analytics-Funktion folgende Funktionen:

- Überwachung, Verwaltung und Entscheidungsfindung bei Ausfällen und anderen Ereignissen
- Überwachen der für eine Anwendung konfigurierten virtuellen Server und Dienste
- Zeigt kritische Informationen zu virtuellen Servern und Diensten an, sodass Sie die Konfigurationen je nach Bedarf ändern können, um eine optimale Leistung durch die Anwendungen zu erzielen.

Navigieren Sie zu **Anwendung** > **Dashboard**, und wählen Sie eine Anwendung aus, die Leistungsindikatorenim Abschnitt **Probleme** angezeigt werden soll.

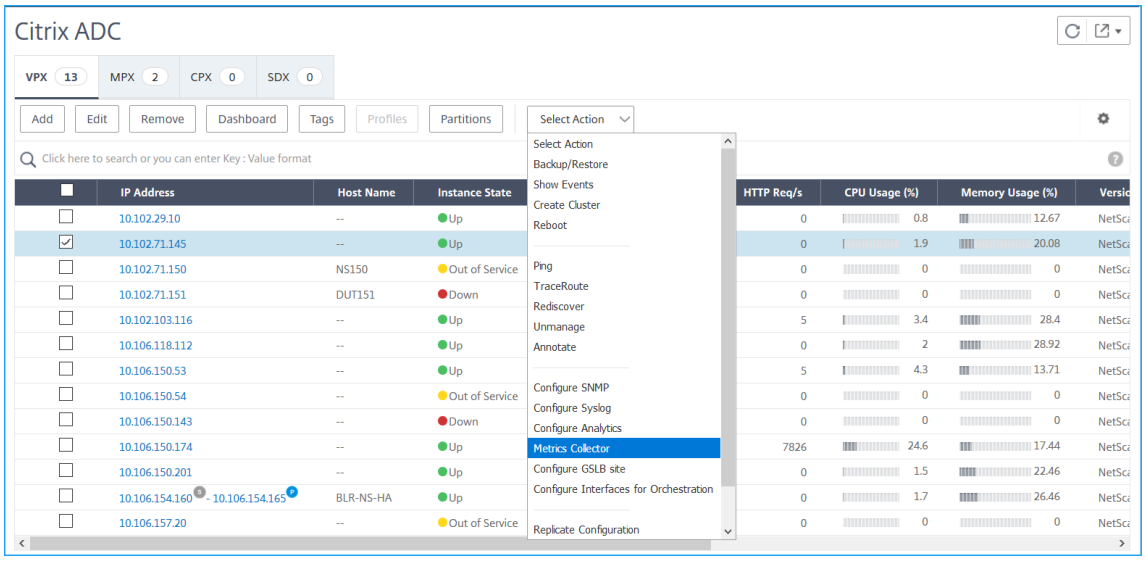
Intelligente App Analytics konfigurieren

April 28, 2021

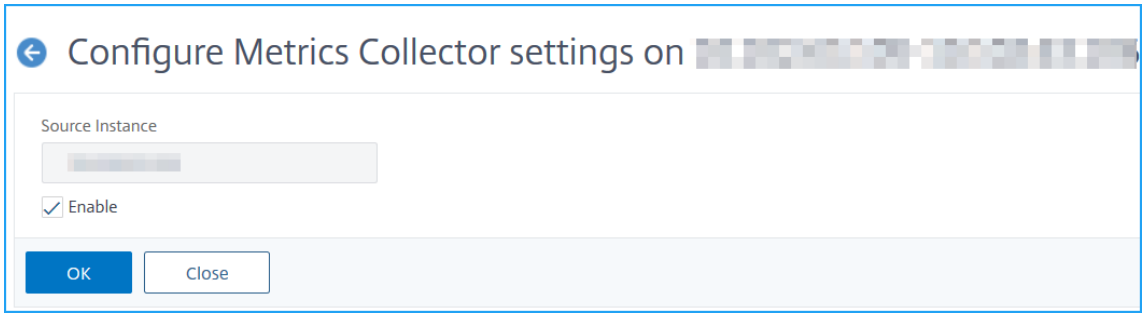
Die Funktion Intelligent App Analytics wird nur in **Citrix ADC 12.1 Build 50.28 oder höher**unterstützt. Metrics Collector verschiebt die Citrix ADC Leistungsindikatordaten an Citrix ADM, das zum Erkennen von Anwendungsproblemen verwendet wird. Um die Funktion Intelligent App Analytics verwenden zu können, muss der **Metrik-Sammler** für jede Citrix ADC-Instanz konfiguriert werden. Standardmäßig ist Metrics Collector in Citrix ADC aktiviert, während Sie die Instanz zu Citrix ADM hinzufügen.

So stellen Sie sicher, ob Metrics Collector aktiviert ist:

1. Navigieren Sie zu **Netzwerke > Instanzen**. Wählen Sie unter **Instanzen**den Instanztyp aus, den Sie überwachen möchten (z. B. Citrix ADC VPX).
2. Wählen Sie die Citrix ADC-Instanz aus.
3. **Wählen Sie in der Liste Aktion auswählen** die Option **Metrikensammler** aus.



4. Stellen Sie sicher, dass auf der Seite **Metriken-Collector-Einstellungen konfigurieren** die Option **Aktivieren** aktiviert ist. Wenn nicht, wählen Sie die Option **Aktivieren** und klicken Sie auf **OK**.



Sobald die Option " **Metrics Collector** " in der Citrix ADC-Instanz aktiviert ist, navigieren Sie zu **Anwendungen** > **Dashboard**. Wählen Sie eine Instanz aus, um Anomalien im Abschnitt " **Probleme** " anzuzeigen.

Es wird empfohlen, Analysen zu aktivieren, um Probleme wie detaillierte Web-Transaktionen für Serverfehler (5xx) zu visualisieren. Weitere Informationen finden Sie unter Analytics aktivieren.

Leistungsindikatoren für Anwendungsanalysen

July 3, 2020

Sie können die Leistungsindikatoren zusammen mit den Kategorien anzeigen, die in Citrix ADC Webanwendungen vorkommen. Um diese Indikatoren anzuzeigen, müssen Sie sicherstellen, dass die Analyse und Metriken (Collector)die ADC-Instanz aktiviert werden:

Nachdem Sie Analytics und Metriken Collector aktiviert haben, können Sie die folgenden Indikatoren anzeigen, indem Sie zu **Anwendungen** > **Dashboard**navigieren, eine Anwendung auswählen und zum Abschnitt **Probleme** nach unten scrollen:

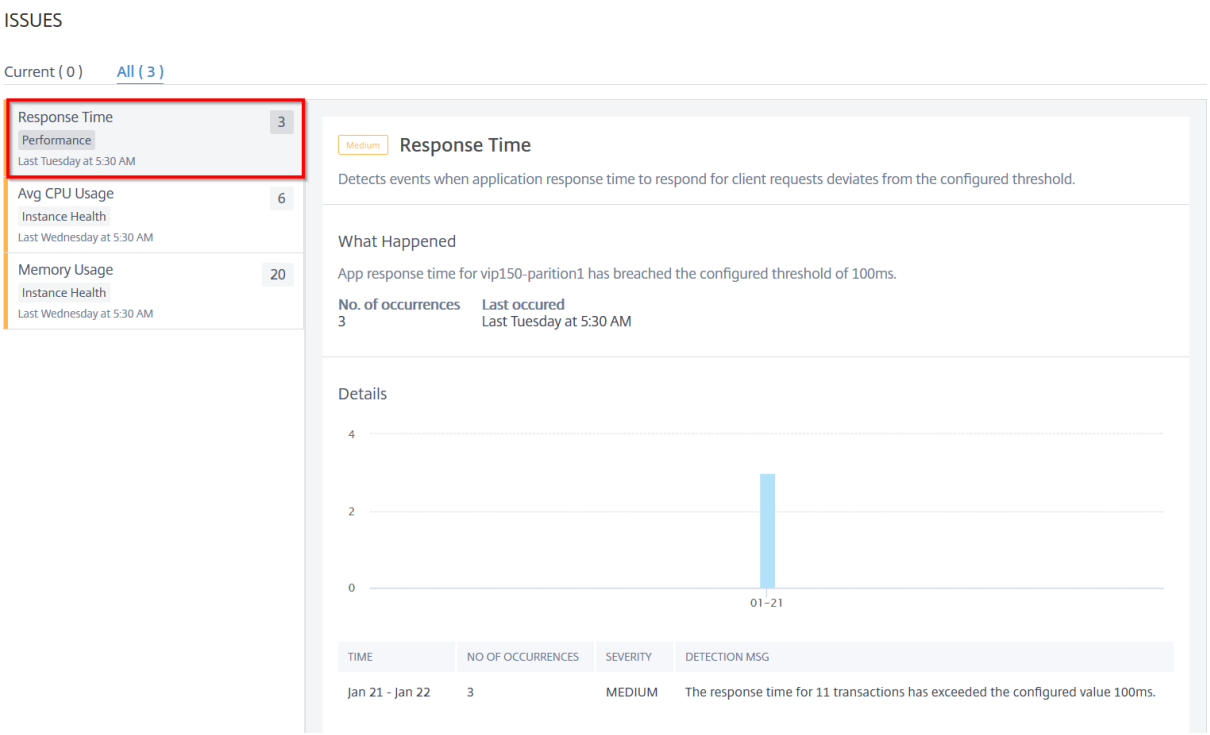
- Reaktionszeit
- Aktive Dienste
- Durchschnittliche CPU-Auslastung
- Speicherauslastung
- NIC-Kartensättigung
- Service-Klappen
- Serverantwortzeit
- Geringe Wiederverwendung von Sitzungen
- Unsachgemäßer Persistenz-Typ
- Instabiler Server (5xx)

- SSL-Echtzeit-Datenverkehr
- Ungewöhnlich große HTTP-Pakete
- TCP-Treffer für die Wiederzusammensetzung der Warteschlange
- Surge Queue Buildup

Reaktionszeit

July 3, 2020

Dieses Problem erkennt, wenn die Antwortzeit der Anwendung für die Beantwortung von Clientanforderungen vom konfigurierten Schwellenwert abweicht. Klicken Sie auf die Registerkarte **Antwortzeit**, um die Problemdetails anzuzeigen.



Unter **Details** können Sie Folgendes anzeigen:

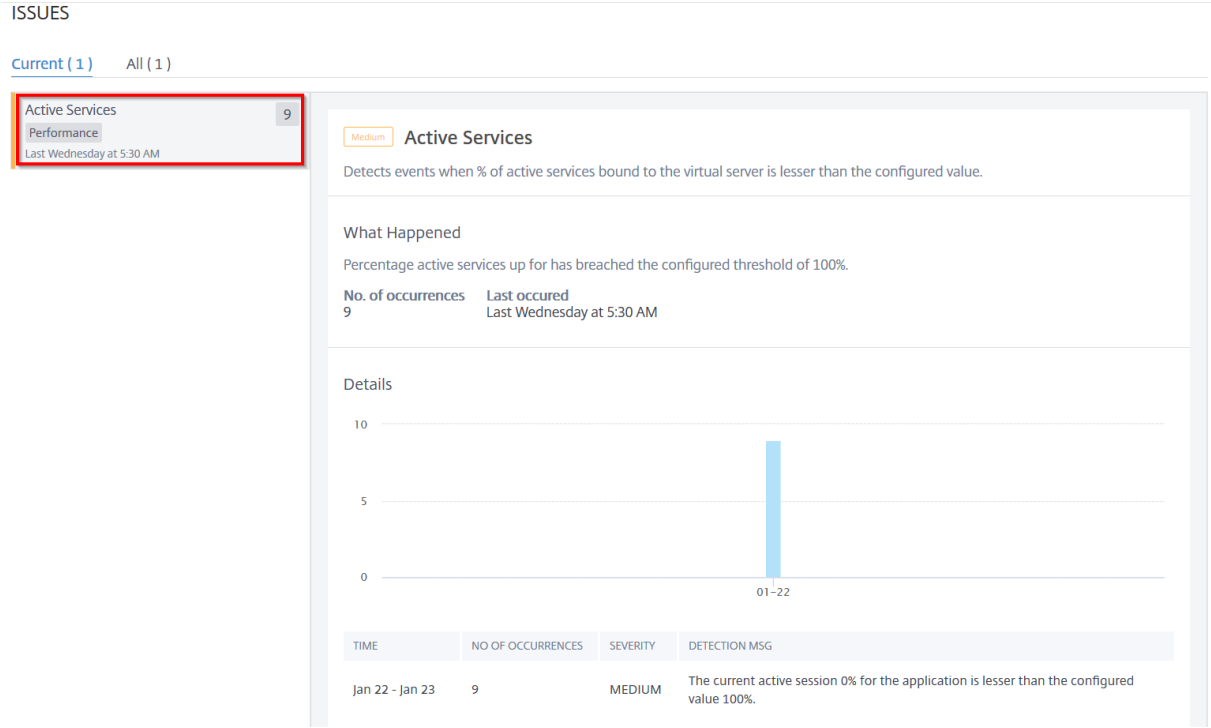
- Das Diagramm, das die Gesamtereignisse für die ausgewählte Zeit angibt. Klicken Sie hier, um Filter anzuwenden und Details anzuzeigen
- Wenn das Problem aufgetreten ist
- Die Gesamtzahl der Vorkommen für die ausgewählte Zeit
- Der Schweregrad des Problems, z. B. niedrig, mittel und hoch

- Die Erkennungsmeldung, die die gesamte Transaktionsantwortzeit angibt, die den konfigurierten Schwellenwert überschreitet

Aktive Dienste

July 3, 2020

Dieses Problem erkennt, wenn der% der aktiven Dienste, die an den virtuellen Server gebunden sind, kleiner als der konfigurierte Schwellenwert ist. Klicken Sie auf die Registerkarte **Aktive Dienste**, um die Problemdetails anzuzeigen.



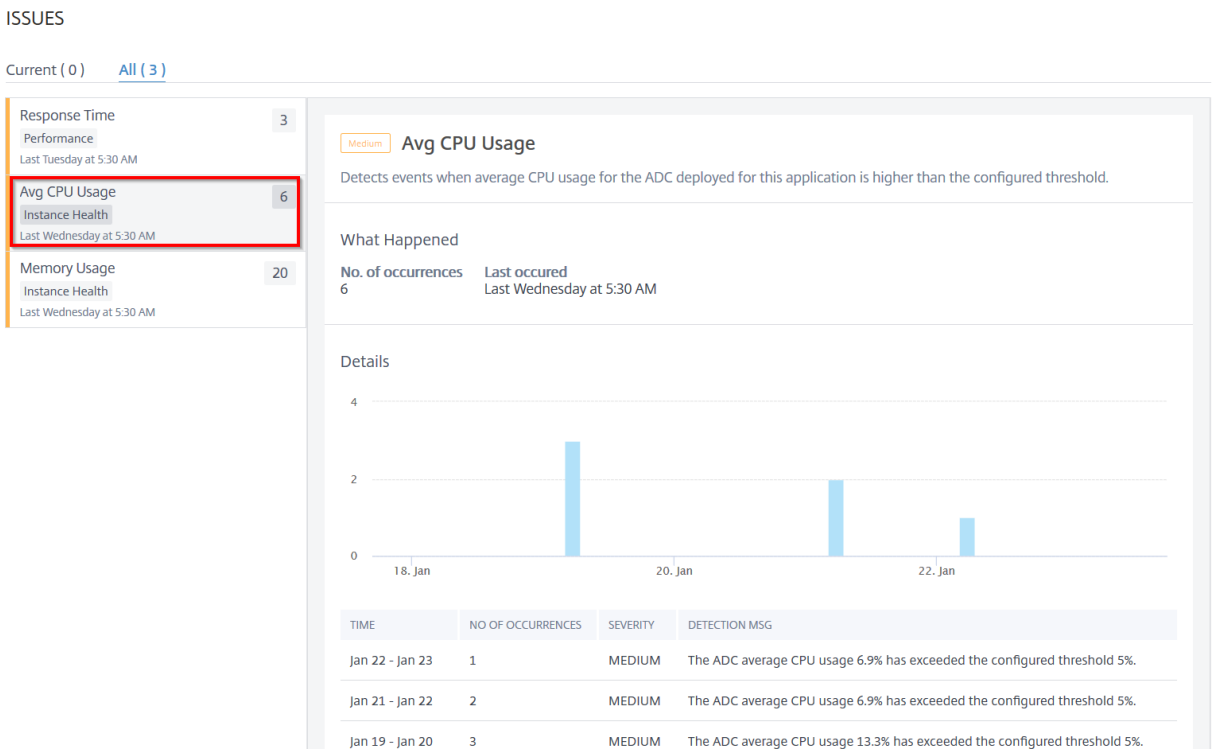
Unter **Details** können Sie Folgendes anzeigen:

- Das Diagramm, das die Gesamtereignisse für die ausgewählte Zeitdauer angibt. Klicken Sie hier, um Filter anzuwenden und Details anzuzeigen
- Wenn das Problem aufgetreten ist
- Die Gesamtereignisse für die ausgewählte Zeitdauer
- Der Schweregrad des Problems, z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die den% der aktiven Dienstsitzungen und den konfigurierten Schwellenwert angibt

Durchschnittliche CPU-Auslastung

July 3, 2020

Dieses Problem erkennt, wenn die ADC-CPU-Auslastung für diese Anwendung den konfigurierten Schwellenwert überschreitet. Klicken Sie auf die Registerkarte **Durchschnittliche CPU-Auslastung**, um die Problemdetails anzuzeigen.



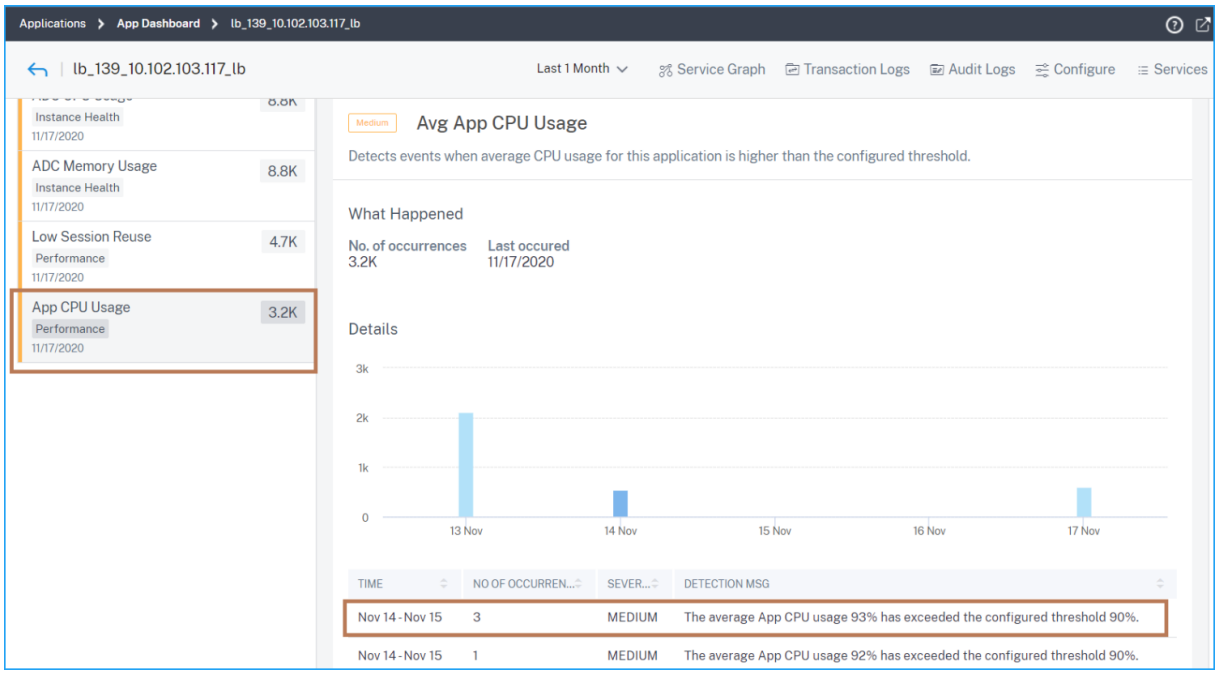
Unter **Details** können Sie Folgendes anzeigen:

- Das Diagramm, das die Gesamtereignisse für die ausgewählte Zeitdauer angibt. Klicken Sie hier, um Filter anzuwenden und Details anzuzeigen
- Wenn das Problem aufgetreten ist
- Die Gesamtereignisse für die ausgewählte Zeitdauer
- Der Schweregrad des Problems, z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die die durchschnittliche CPU-Auslastung% des ADC und den konfigurierten Schwellenwert angibt

Durchschnittliche CPU-Auslastung der

April 28, 2021

Dieses Problem erkennt, wenn die CPU-Auslastung der Anwendung den konfigurierten Schwellenwert überschreitet. Klicken Sie auf die Registerkarte **App-CPU-Auslastung**, um die Problemdetails anzuzeigen.



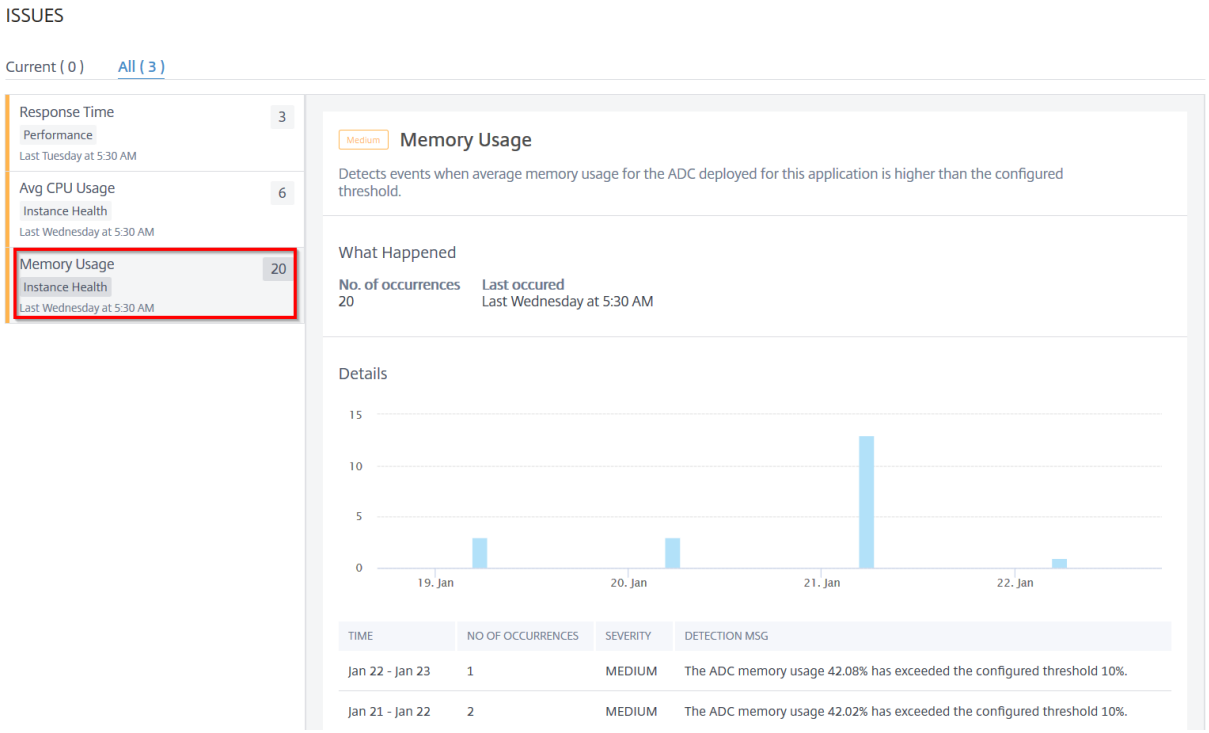
Unter **Details** können Sie Folgendes anzeigen:

- Das Diagramm, das die Gesamtereignisse für die ausgewählte Zeitdauer angibt. Klicken Sie hier, um Filter anzuwenden und Details anzuzeigen
- Wenn das Problem aufgetreten ist
- Die Gesamtereignisse für die ausgewählte Zeitdauer
- Der Schweregrad des Problems, z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die den durchschnittlichen CPU-Auslastung% der Anwendung und den konfigurierten Schwellenwert angibt

Speicherauslastung

April 28, 2021

Dieses Problem erkennt, wenn die ADC-Speicherauslastung für diese Anwendung den konfigurierten Schwellenwert überschreitet. Klicken Sie auf die Registerkarte **Speicherauslastung**, um die Problemdetails anzuzeigen.



Unter **Details** können Sie Folgendes anzeigen:

- Das Diagramm, das die Gesamtereignisse für die ausgewählte Zeitdauer angibt. Klicken Sie hier, um Filter anzuwenden und Details anzuzeigen
- Wenn das Problem aufgetreten ist
- Die Gesamtereignisse für die ausgewählte Zeitdauer
- Der Schweregrad des Problems, z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die die durchschnittliche ADC-Speicherverwendung% und den konfigurierten Schwellenwert angibt

Service-Klappen

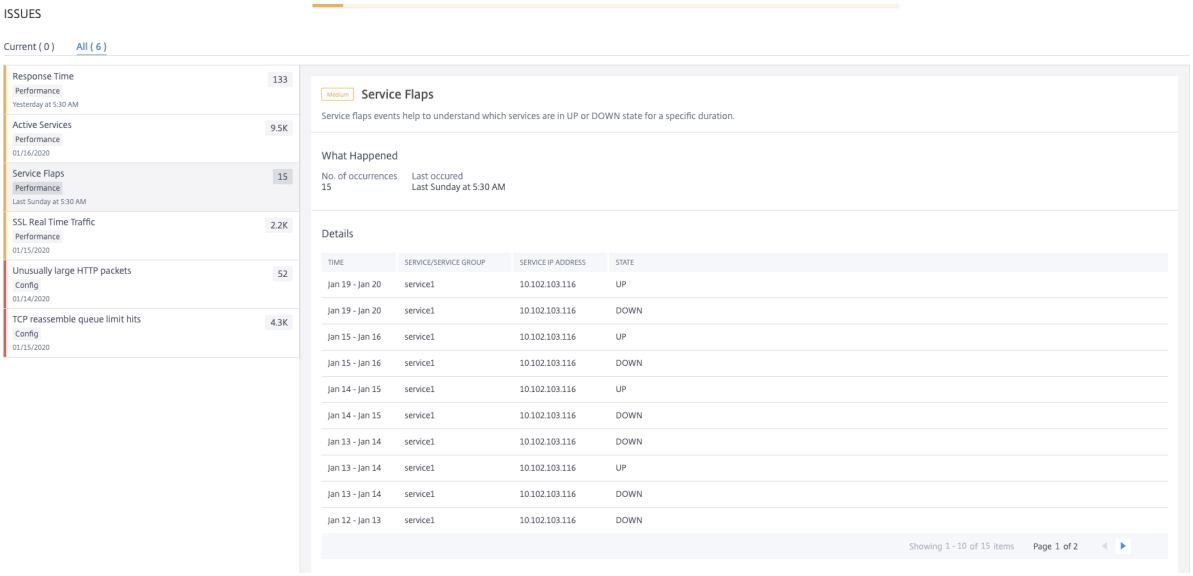
July 3, 2020

Als Netzwerkadministrator müssen Sie sicherstellen, dass die Anwendung optimal verfügbar ist. Bei Netzwerkproblemen oder Konfigurationsproblemen können sich der Status und die Verfügbarkeit eines Anwendungsservers auf die Gesamtleistung auswirken.

Mithilfe der Service-Flapsereignisse können Sie die Anwendung identifizieren, die Probleme aufweist. Service-Klappen Ereignisse helfen Ihnen auch:

- Verstehen, welcher Dienst sich für eine bestimmte Dauer im Status DOWN befindet
- Verstehen, wie viele Dienste sich für eine bestimmte Dauer im Status UP oder DOWN befinden

Klicken Sie auf die Registerkarte **Service-Flaps**, um die Service-Flaps-Details anzuzeigen.



Sie können Details wie die Anzahl der Vorkommen und den Zeitpunkt des letzten Vorkommens anzeigen.

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, die die Service-Klappenanomalie aufgetreten ist
- Name der Service/Servicegruppe
- Die Dienst-IP-Adresse
- Der aktuelle Dienststatus

Instabiler Server

April 28, 2021

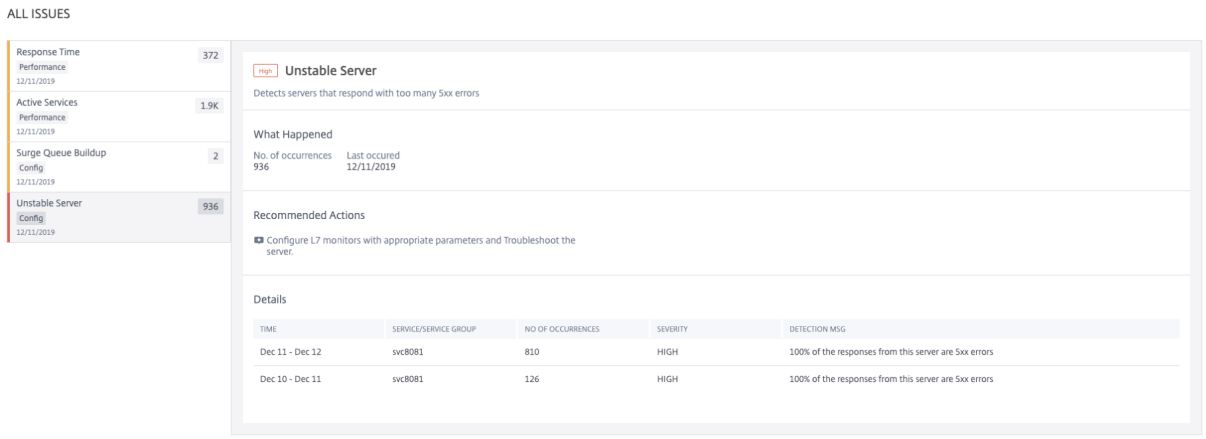
In einigen Szenarien antwortet der Webserver mit Statuscodes, wenn er die Anforderungen aus Gründen wie ungültige Anforderungen, vorübergehende Überlastung oder Serverwartung nicht verarbeiten kann. Diese Fehler werden mit Fehlercodes angezeigt, die verschiedene Szenarien der Fehler definieren. Zum Beispiel:

- **502 Schlechtes Gateway**
  Der Server fungiert als Gateway oder Proxy und erhielt eine ungültige Antwort vom Upstream-Server.
- **503 Dienst nicht verfügbar**
  Der Server ist derzeit nicht verfügbar. Die Server sind möglicherweise zu Wartungszwecken überlastet oder heruntergefahren.
- **504 Gateway-Timeout**
  Der Server fungiert als Gateway oder Proxy und erhielt keine zeitnahe Antwort vom Upstream-Server.

Dies können temporäre Bedingungen sein, aber manchmal müssen Sie eine Korrekturmaßnahme auf den Webservern implementieren, um die Webseiten verfügbar zu machen.

Mit dem Indikator " **Unstable Server** " können Sie diese Fehler anzeigen und Entscheidungen über Korrekturmaßnahmen treffen, um die Probleme zu beheben und sicherzustellen, dass die Clientanforderungen bedient werden und die Webseiten immer verfügbar sind.

Wählen Sie die Registerkarte **Unstable Server** aus, um die Problemdetails anzuzeigen.



Die **empfohlenen Aktionen** zur Behebung des Problems sind:

- Konfigurieren Sie L7-Monitore mit entsprechenden Parametern für den Server, der mit 5xx-Fehlern reagiert. Ein Monitor ist eine Entität, die die Dienstintegrität verfolgt. Die Appliance prüft die Server regelmäßig über den Monitor, der an jeden Dienst gebunden ist. Wenn ein Server nicht innerhalb eines angegebenen Antwortzeitlimits reagiert und die angegebenen Prüfpunkte fehlschlagen, wird der Dienst als DOWN gekennzeichnet. Anschließend führt die Appliance den Lastausgleich unter den verbleibenden Diensten durch. Weitere Informationen zum Konfigurieren eines Monitors finden Sie unter Benutzerdefinierte Monitore
- Problembehandlung beim Server

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, die die instabile Serveranomalie aufgetreten ist
- Name der Service/Servicegruppe
- Gesamtvorkommen
- Der Schweregrad der Anomalie wie hoch, niedrig und mittel
- Die Erkennungsnachricht, die% der Antworten dieses Dienstes angibt, die 5xx-Fehler meldet

Ausführliche Informationen zur Webtransaktion mit Serverfehlern finden Sie unter Web-Transaktionsanalyse für Serverfehler

Server-Reaktionszeit

April 28, 2021

Anwendungsverlangsamung ist ein wichtiges Anliegen für jede Organisation, da dies zu geschäftlichen Auswirkungen oder Produktivität führt. Als Administrator müssen Sie sicherstellen, dass alle Anwendungen optimal funktionieren, um geschäftliche Auswirkungen zu vermeiden.

Jede Anwendung verhält sich anders und hat unterschiedliche Antwortzeiterwartungen. Wenn Sie über eine große Serverfarm verfügen, wird es für Administratoren zeitaufwändig, jede Anwendung zu bewerten und Schwellenwerte für die Reaktionszeit des Servers festzulegen.

Der Indikator **Server-Antwortzeit** hilft Administratoren, jede Anwendung basierend auf dem maschinellen Lernalgorithmus zu bewerten. Dieser Indikator meldet:

- Abnormal hohe Reaktionszeit
- Abnormal niedrige Reaktionszeit

Klicken Sie auf die Registerkarte **Server-Reaktionszeit**, um die Problemdetails anzuzeigen.

Die **empfohlenen Aktionen** empfehlen Ihnen, diese Anomalien zu beheben.

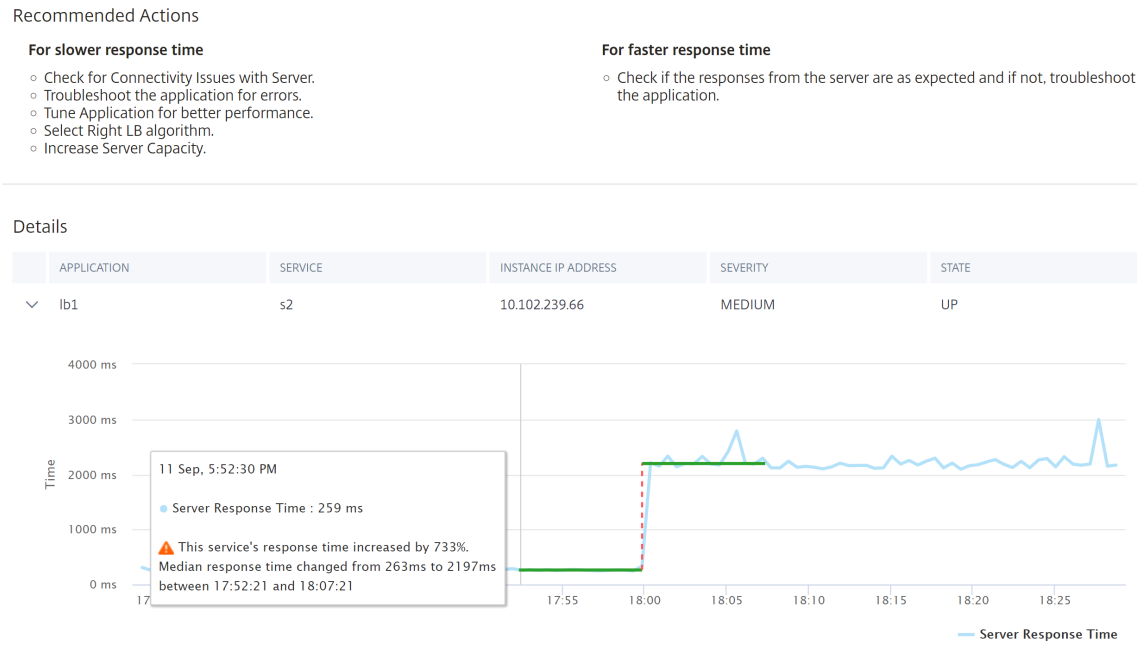
Unter **Details** können Sie Folgendes anzeigen:

- Die Anwendung, die die Anomalie hat
- Der Dienst, der an die Anwendung gebunden ist
- Die IP-Adresse der Citrix ADC-Instanz
- Der Schweregrad der Anomalie
- Der Anwendungsstatus
- Das Reaktionszeitdiagramm des Servers für den ausgewählten Zeitraum
- Rollierendes Mediandiagramm basierend auf der Reaktionszeit des Servers

- Details zu Anomalie

Citrix ADM erkennt Anomalien für abnormal hohe Reaktionszeit und für abnormal niedrige Reaktionszeit.

- **Anomalie für ungewöhnlich hohe Serverreaktionszeit**

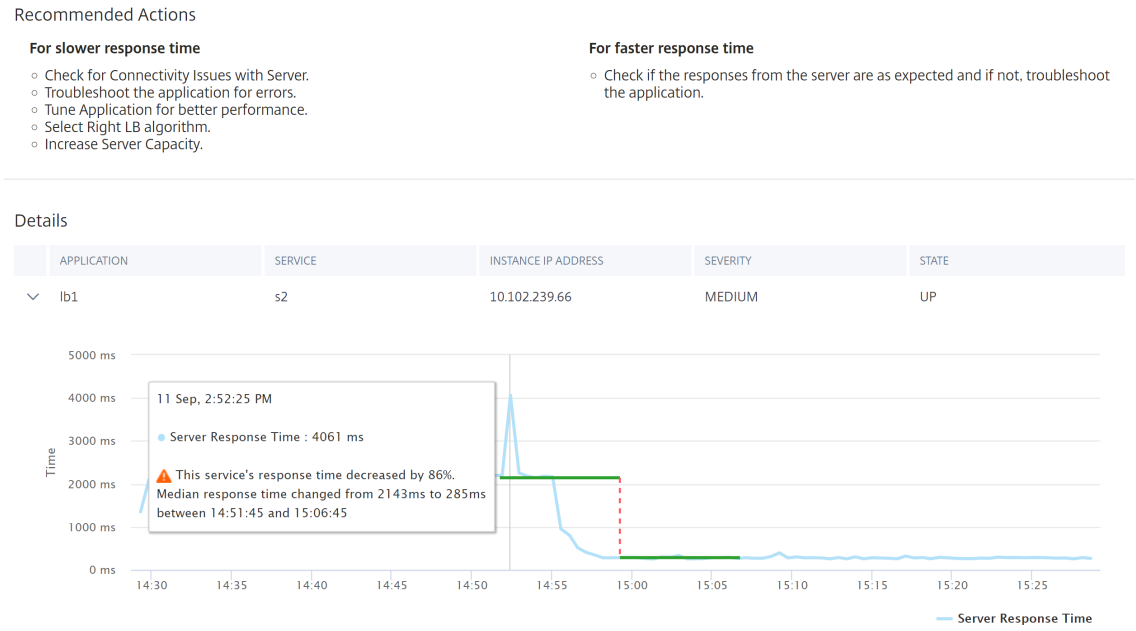


Citrix ADM vergleicht die durchschnittliche Server-Reaktionszeit für eine bestimmte Dauer. Gemäß dem im Bild gezeigten Beispiel vergleicht Citrix ADM die durchschnittliche Server-Reaktionszeit zwischen 17:50 und 18:20.

Wenn die Reaktionszeit des Servers zunimmt, überwacht Citrix ADM die Reaktionszeit des Servers für eine andere bestimmte Dauer und erkennt dann Anomalie für die Zeit, zu der die Reaktionszeit des Servers begonnen hat.

Nach dem Beispiel im Bild sehen Sie, dass eine Anomalie erkannt wurde, wobei erwähnt wird, dass die Reaktionszeit des Servers um 733% erhöht wurde, nachdem die durchschnittliche Reaktionszeit des Servers zwischen 17:52 und 18:07 verglichen wurde.

- **Anomalie für abnormal niedrige Reaktionszeit des Servers**



Citrix ADM vergleicht die durchschnittliche Server-Reaktionszeit für eine bestimmte Dauer. Laut dem in der Abbildung gezeigten Beispiel vergleicht Citrix ADM die durchschnittliche Serverreaktionszeit zwischen 14:51 und 15:06.

Wenn die Reaktionszeit des Servers abnimmt, überwacht Citrix ADM die Reaktionszeit des Servers für eine andere bestimmte Dauer und erkennt dann Anomalie für die Zeit, zu der die Reaktionszeit des Servers beginnt.

Nach dem Beispiel im Bild sehen Sie, dass eine Anomalie erkannt wurde, wobei erwähnt wird, dass die Reaktionszeit des Servers um 86% verringert wurde, nachdem die durchschnittliche Reaktionszeit des Servers zwischen 14:51 und 15:06 verglichen wurde.

Sitzungsaufbau

April 28, 2021

Für alle gesicherten Transaktionen führt Citrix ADC den SSL-Abladungsprozess für die erste Transaktion durch und speichert dann die SSL-Sitzung basierend auf der Konfiguration der **Sitzungswiederverwendung**.

Basierend auf der Datenverkehrsrate besteht die Möglichkeit, Sitzungsaufbau über einen bestimmten Zeitraum hinweg zu erhalten, was dazu führen kann, dass diese Sitzungen in Citrix ADC eine große Menge an Arbeitsspeicher erhalten.

Sitzungsaufbauereignisse warnen die Administratoren und stellen empfohlene Aktionen zur Behebung dieses Ereignisses bereit. Klicken Sie auf die Registerkarte **Sitzungsaufbau**, um die Problemde-

tails anzuzeigen.

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Sitzungsaufbau-Anomalie auftrat
- Der Name des virtuellen Servers
- Der Schweregrad der Anomalie wie hoch, niedrig und mittel
- Die Meldung, die angibt, dass **X-Anzahl** der SSL-Sitzungen auf dem virtuellen Server verfügbar sind und derzeit innerhalb der konfigurierten Timeout-Sitzung **Y-Anzahl** von SSL-Handshakes pro Sekunde vorhanden ist.

Die **empfohlene Aktion** zur Behebung dieser Anomalie besteht darin, entweder das Sitzungszeitlimit zu reduzieren oder die Wiederverwendung der Sitzung zu deaktivieren. Weitere Informationen finden Sie unter Sitzungstimeout.

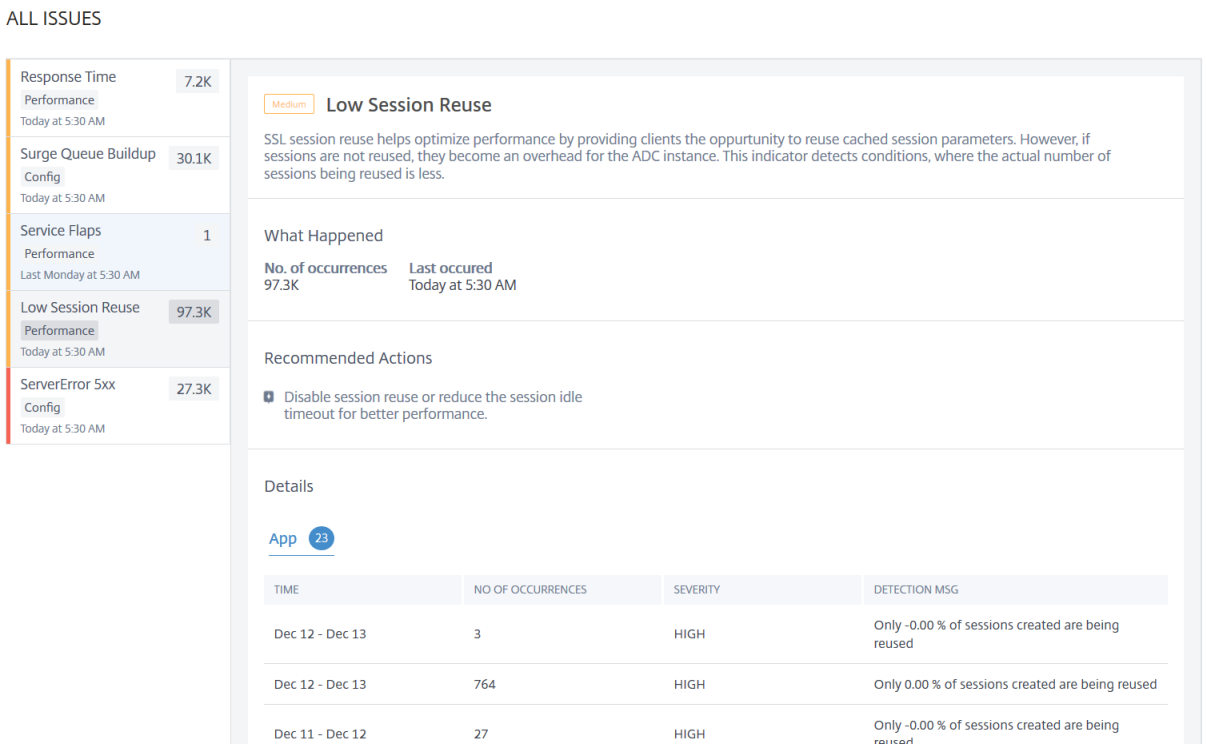
Wiederverwendung der niedrigen Sitzung

April 28, 2021

Citrix ADC-Instanzen verarbeiten SSL-Transaktionen, indem SSL-Handshake-Prozess vom Server abgeladen wird. Nach Erhalt der Antwort vom Server schließt die Citrix ADC-Instanz die sichere Transaktion mit dem Client ab. Mit den zwischengespeicherten Sitzungsparametern schließt die Citrix ADC-Instanz den SSL-Handshake-Prozess für die aufeinanderfolgenden Anforderungen ab.

Wenn diese Sitzungen nicht wiederverwendet werden, werden sie zu einem Overhead für die Citrix ADC-Instanzen. Mit dem Indikator " **Low Session Reuse** " können Sie feststellen, ob die tatsächliche Anzahl der wiederverwendeten Sitzungen geringer ist.

Klicken Sie auf die Registerkarte **Low Session Reuse** (Low Session Reuse), um die Problemdetails anzuzeigen.



Die **empfohlene Aktion** zur Behebung des Problems besteht darin, entweder die Wiederverwendung der Sitzung zu deaktivieren oder das Sitzungstimeout zu reduzieren. Weitere Informationen finden Sie unter Wiederverwendung von Sitzungen.

Unter **Details** können Sie Folgendes anzeigen:

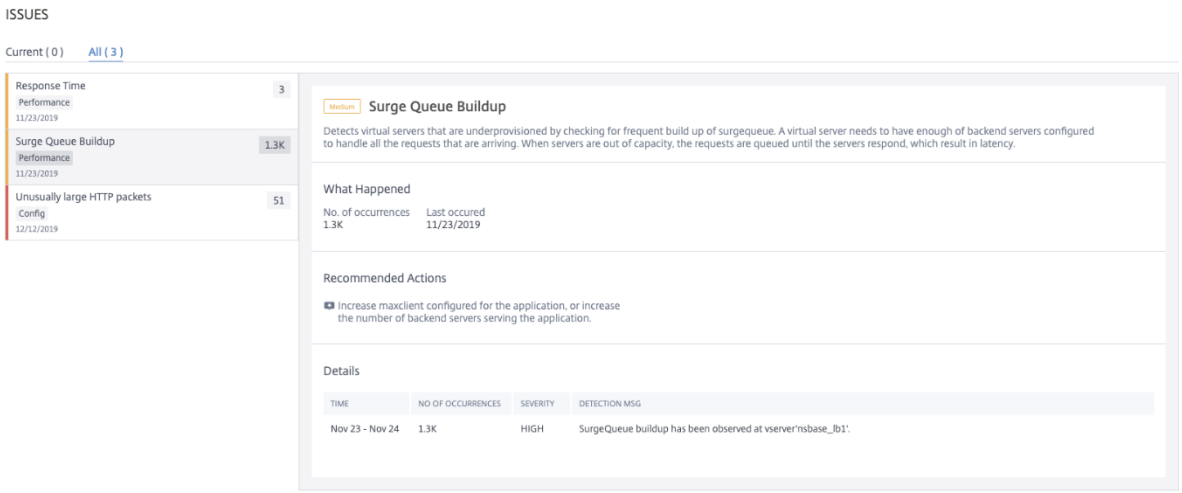
- Gesamtzahl von Anwendungen mit geringer Sitzungswiederverwendung
- Die Zeit, die die niedrige Sitzung Wiederverwendung Anomalie aufgetreten ist
- Gesamtvorkommen
- Der Schweregrad der Anomalie wie hoch, niedrig und mittel
- Die Erkennungsmeldung, die angibt, dass nur% der konfigurierten Sitzungen wiederverwendet werden

Surge Queue Buildup

April 28, 2021

Wenn ein Server eine Welle von Anforderungen empfängt, reagiert der Server langsam auf die Clients. Oft führt die Überlastung auch dazu, dass Clients Fehlerseiten erhalten. Für einen virtuellen Server müssen genügend Backend-Server konfiguriert sein, um die eingehenden Anforderungen zu bearbeiten.

Mit dem Indikator **Surge Queue Buildup** können Sie die virtuellen Server anzeigen, die Surge Queue Buildup haben. Klicken Sie auf die Registerkarte **Surge Queue Buildup**, um die Problemdetails anzuzeigen.



Die **empfohlenen Aktionen** zur Behebung des Problems sind:

- Erhöhen Sie die Anzahl der Clientverbindungen. Weitere Informationen finden Sie unter Festlegen eines Grenzwerts für die Anzahl der Clientverbindungen
- Erhöhen Sie die Back-End-Server, um die Anwendungsanforderungen zu bedienen

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, die die Überspannungswarteschlange Aufbauanomalie aufgetreten ist
- Gesamtvorkommen
- Der Schweregrad der Anomalie wie hoch, niedrig und mittel
- Die Erkennungsmeldung, die den Aufbau einer Überspannungswarteschlange auf dem virtuellen Server angibt

Ungewöhnlich große HTTP-Pakete

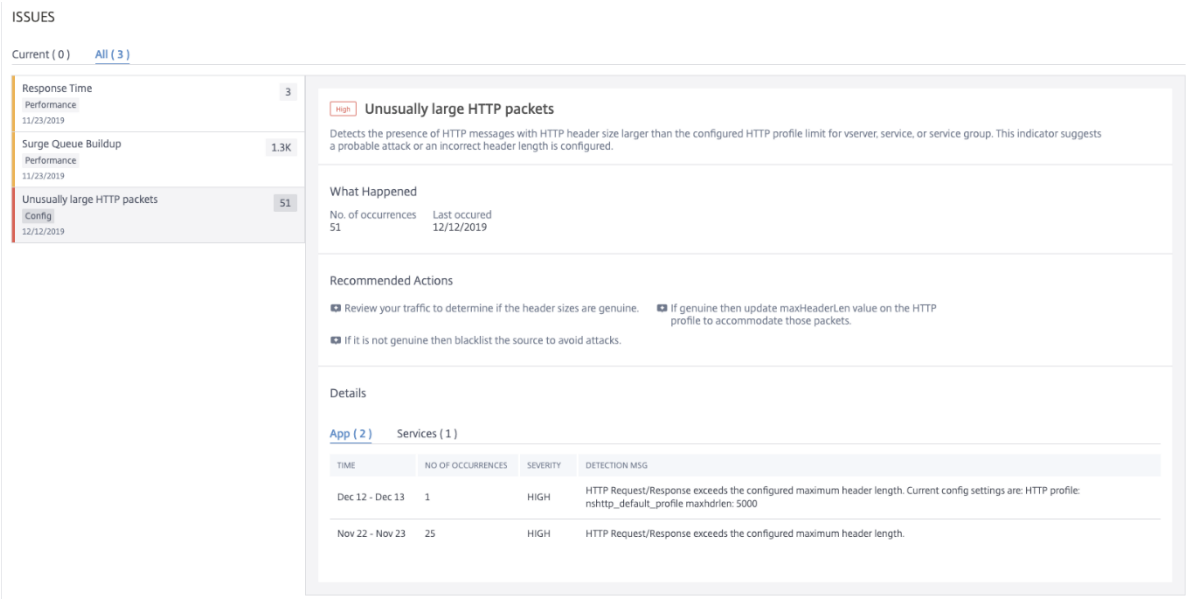
April 28, 2021

Eine HTTP-Transaktion verwendet Anforderungs-Antwort-Nachrichten zwischen dem Client und dem Server. In den Anforderungs- und Antwortmeldungen sind HTTP-Header die Werte, die im HTTP-Protokoll angezeigt werden. Sie können die HTTP-Header-Länge in virtuellen Server-, Dienst- oder Dienstgruppen konfigurieren, um 4xx-Fehler zu vermeiden.

Wenn eine HTTP-Anforderung/Antwort die maximale Header-Länge überschreitet, kann dies ein möglicher Angriff sein. Mit dem Indikator **Ungewöhnlich große HTTP-Pakete** können Sie die

Vorkommen anzeigen, bei denen die HTTP-Nachrichten mit HTTP-Header-Größe die konfigurierten Werte überschreiten.

Klicken Sie auf die Registerkarte **Ungewöhnlich große HTTP-Pakete**, um die Problemdetails anzuzeigen.



Die **empfohlenen Aktionen** zur Behebung des Problems sind:

- Überprüfen Sie den Datenverkehr, um festzustellen, dass die Kopfzeilengröße echt ist. Wenn die Header-Größe echt ist, aktualisieren Sie den Header-Wert im HTTP-Profil. Weitere Informationen finden Sie unter Pufferüberlaufprüfung.
- Wenn die Header-Größe nicht echt ist, fügen Sie die Quelle der Blockierliste hinzu, um Angriffe zu vermeiden.

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Anomalie aufgetreten ist
- Gesamtvorkommen
- Der Schweregrad der Anomalie wie hoch, niedrig und mittel
- Die Erkennungsmeldung, die die aktuelle HTTP-Headerlänge angibt, die auf dem virtuellen Server, Server oder der Dienstgruppe konfiguriert ist.

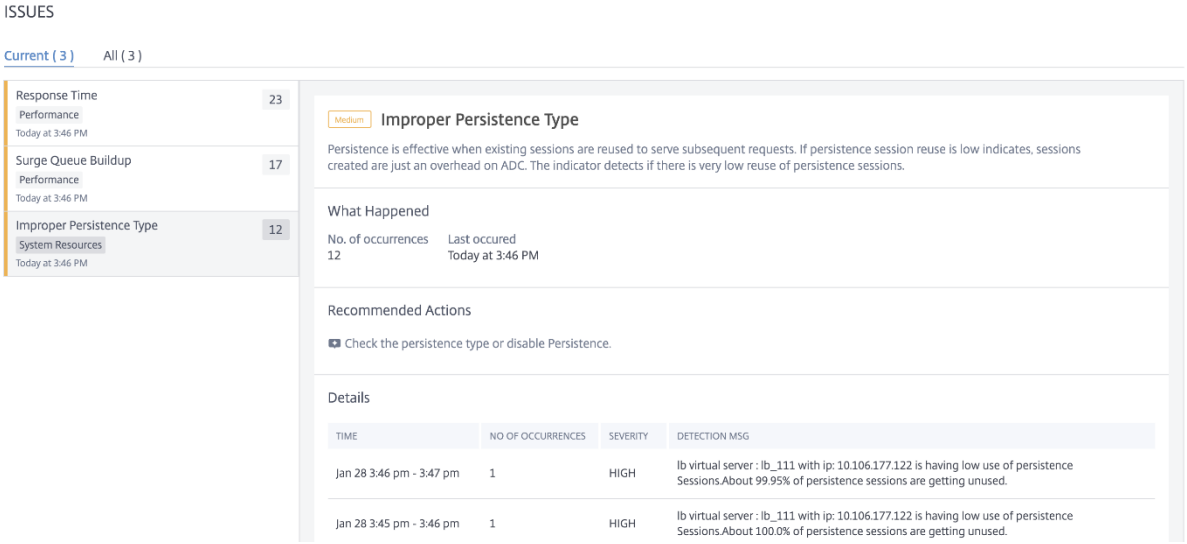
Unsachgemäßer Persistenz-Typ

April 28, 2021

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

Persistenz ist wirksam, wenn vorhandene Sitzungen wiederverwendet werden, um nachfolgende Anforderungen zu bedienen. Wenn die Wiederverwendung von Persistenzsitzungen gering ist, sind Sitzungen, die auf ADC erstellt wurden, nur ein Overhead.

Mithilfe des **Ype-Indikators "Unmissbräuchliche Persistenz** " können Sie feststellen, ob die Persistenznutzung auf einem virtuellen Server gering ist. Klicken Sie auf die Registerkarte **Unsachgemäßer Persistenztyp**, um die Problemdetails anzuzeigen.



Die **empfohlene Aktion** zur Behebung des Problems besteht darin, den Persistenztyp zu überprüfen oder die Persistenz zu deaktivieren. Weitere Informationen finden Sie unter Persistenzeinstellungen.

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Anomalie aufgetreten ist
- Gesamtvorkommen
- Der Schweregrad der Anomalie wie hoch, niedrig und mittel
- Die Erkennungsmeldung, die angibt, in% der Sitzungen, die nicht verwendet werden

TCP-Queue-Limit Treffern neu zusammenbauen

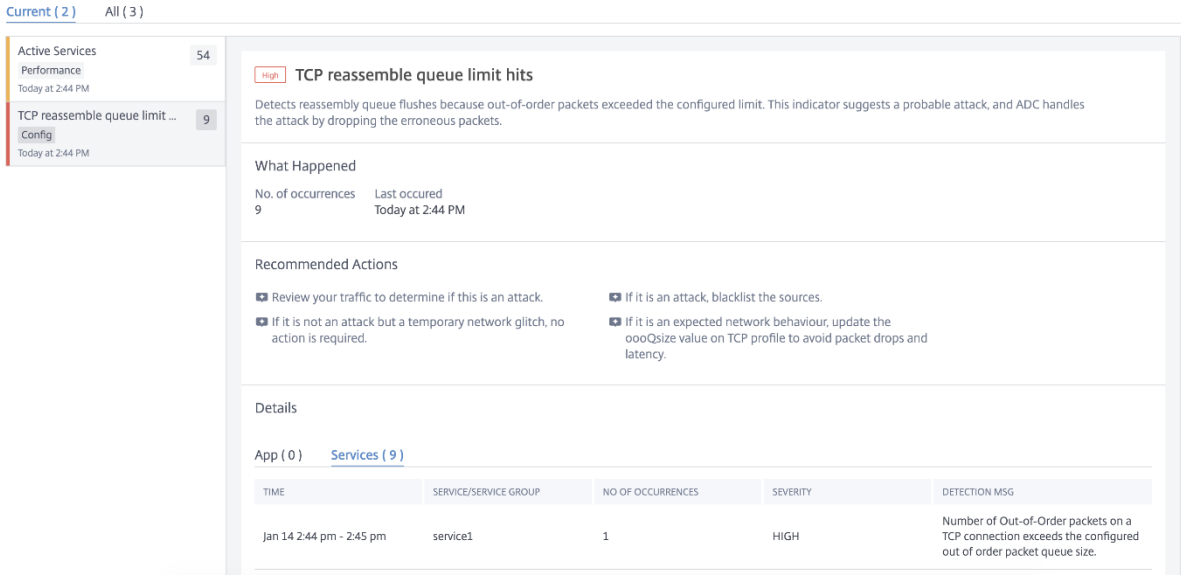
April 28, 2021

TCP unterhält eine Warteschlange außerhalb der Bestellung, um die OOO-Pakete in der TCP-Kommunikation zu halten. Diese Einstellung wirkt sich auf den Citrix ADC Speicher aus, wenn die Warteschlangengröße lang ist, wie die Pakete im Laufzeitspeicher aufbewahrt werden müssen.

Dies muss basierend auf der Art der Netzwerk- und Anwendungseigenschaften auf einem optimierten Niveau gehalten werden.

Mit dem Indikator **TCP reassemble queue limit hits** können Sie anzeigen, ob die Out-of-Order-Pakete auf einer TCP-Verbindung die konfigurierte Paketwarteschlangengröße außerhalb der Reihenfolge überschreiten.

Klicken Sie auf die Registerkarte **TCP reassemble queue limit hits**, um die Problemdetails anzuzeigen.



Die **empfohlenen Aktionen** zur Behebung des Problems sind:

- Überprüfen Sie den Datenverkehr und fügen Sie die zu blockierende Quelle hinzu, wenn es sich um einen Angriff handelt
- Wenn dies ein erwartetes Netzwerkverhalten ist, aktualisieren Sie den Wert der Paketgröße außerhalb der Reihenfolge im TCP-Profil. Weitere Informationen finden Sie unter TCP-Optimierung
- Wenn es sich nur um einen temporären Netzwerk-Fehler handelt, ist keine weitere Aktion erforderlich

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Anomalie aufgetreten ist
- Gesamtvorkommen
- Der Schweregrad der Anomalie wie niedrig, mittel und hoch

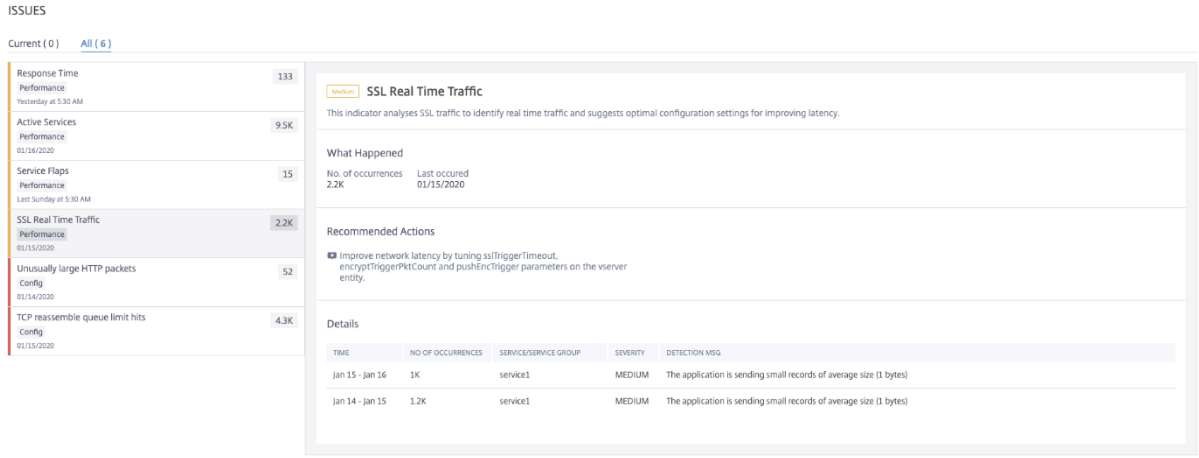
- Die Erkennungsmeldung, die das aktuelle TCP-Profil und die oooQsize-Einstellungen angibt

SSL-Echtzeit-Datenverkehr

April 28, 2021

In der Citrix ADC-Instanz können Sie ein SSL-Profil für die Verarbeitung von SSL-Datenverkehr verwenden. Das SSL-Profil umfasst bestimmte SSL-Parameter für virtuelle Server, Dienste und Dienstgruppen. Der **SSL Real Time Traffic** Indikator analysiert den SSL-Datenverkehr, um Echtzeit-Datenverkehr zu identifizieren und schlägt optimale Konfigurationseinstellungen zur Verbesserung der Latenz vor.

Klicken Sie auf die Registerkarte **SSL-Echtzeitverkehr**, um die Problemdetails anzuzeigen.



Die **empfohlene Aktion** zur Behebung des Problems besteht darin, die Netzwerklatenz durch Aktualisieren von SSL-Parametern zu verbessern. Weitere Informationen finden Sie unter Globale SSL-Parameter.

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Anomalie aufgetreten ist
- Name der Service/Servicegruppe
- Der Schweregrad der Anomalie wie niedrig, mittel und hoch
- Die Erkennungsmeldung mit der aktuellen Einstellung in der Anwendung

Anwendungssicherheits-Dashboard

April 28, 2021

Das **App Security-Dashboard** bietet Ihnen einen Überblick über die Sicherheitsmetriken für die entdeckten/lizenzierten Anwendungen. Dieses Dashboard zeigt die Informationen zum Sicherheitsangriff für die erfunden/lizenzierten Anwendungen an, wie Sync-Angriffe, Angriffe mit kleinen Fenstern und DNS-Überschwemmungsangriffen.

So zeigen Sie die Sicherheitsmetriken im App-Sicherheits-Dashboard an:

1. Navigieren Sie zu **Anwendungen** > **App-Sicherheits-Dashboard**.
2. Wählen Sie die Instanz-IP-Adresse aus der Instanzliste aus.

   Die Berichte enthalten für jede Anwendung die folgenden Informationen:

   - **Bedrohungsindex**. Ein einstelliges Bewertungssystem, das die Kritik von Angriffen auf die Anwendung anzeigt. Je kritischer die Angriffe auf eine Anwendung sind, desto höher ist der Bedrohungsindex für diese Anwendung. Die Werte reichen von 1 bis 7.

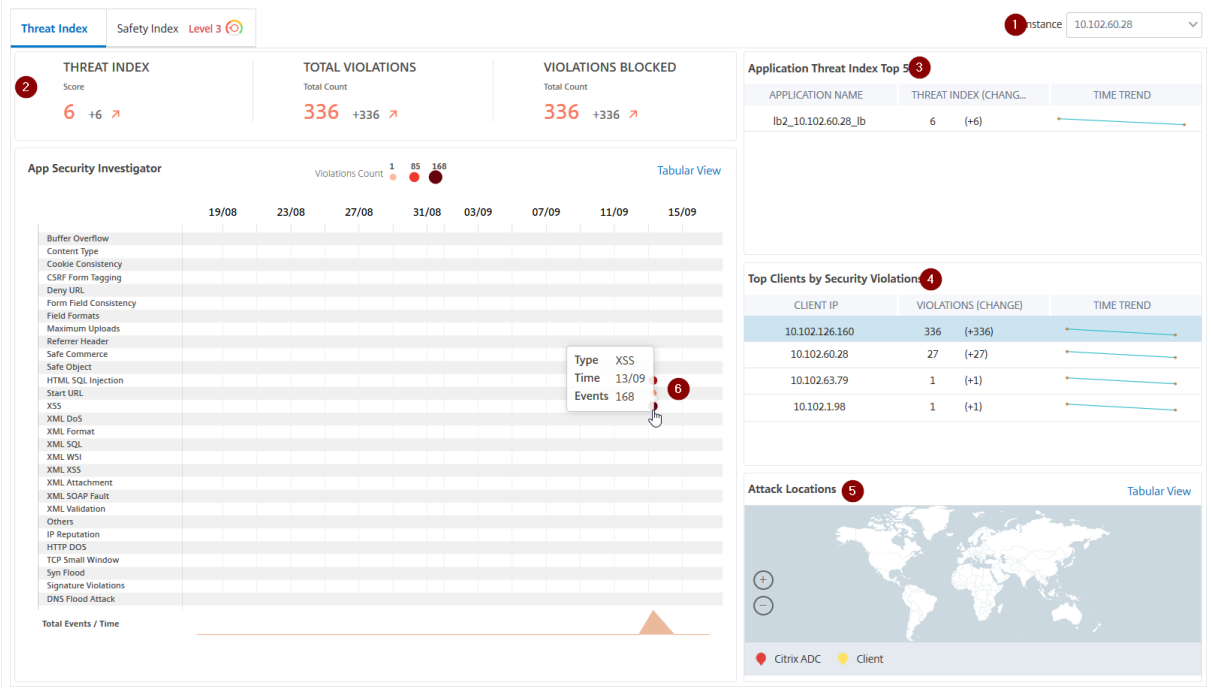
     Der Bedrohungsindex basiert auf Angriffsinformationen. Die angriffsbezogenen Informationen, wie Verletzungstyp, Angriffskategorie, Standort und Client-Details, geben einen Einblick in die Angriffe auf die Anwendung. Verstöße werden nur dann an Citrix ADM gesendet, wenn eine Verletzung oder ein Angriff auftritt. Viele Verstöße und Schwachstellen führen zu einem hohen Bedrohungsindexwert.

   - **Sicherheitsindex**. Ein einstelliges Bewertungssystem, das angibt, wie sicher Sie die Citrix ADC-Instanzen zum Schutz von Anwendungen vor externen Bedrohungen und Sicherheitslücken konfiguriert haben. Je niedriger die Sicherheitsrisiken für eine Anwendung, desto höher der Sicherheitsindex. Die Werte reichen von 1 bis 7.

     Der Sicherheitsindex berücksichtigt sowohl die Konfiguration der Anwendungsfirewall als auch die Sicherheitskonfiguration des Citrix ADC -Systems. Für einen hohen Sicherheitsindex müssen beide Konfigurationen stark sein. Wenn beispielsweise strenge Anwendungsfirewall Prüfungen durchgeführt werden, aber keine Sicherheitsmaßnahmen für das Citrix ADC -System, wie z. B. ein starkes Kennwort für den Benutzer nsroot, bereitgestellt werden, wird den Anwendungen ein niedriger Sicherheitsindex zugewiesen.

Sie können Abweichungen anzeigen, die im **App Security Investigator**gemeldet wurden.

Bedrohungsindizes



1 - Zeigt die IP-Adresse der Citrix ADC-Instanz an, für die Sie Details anzeigen können.

2 - Zeigt Details wie Bedrohungsindizes, Gesamtzahl der aufgetretenen Verletzungen und Gesamtzahl der gesperrten Verletzungen an.

3 - Zeigt den virtuellen Server der ausgewählten Instanz an.

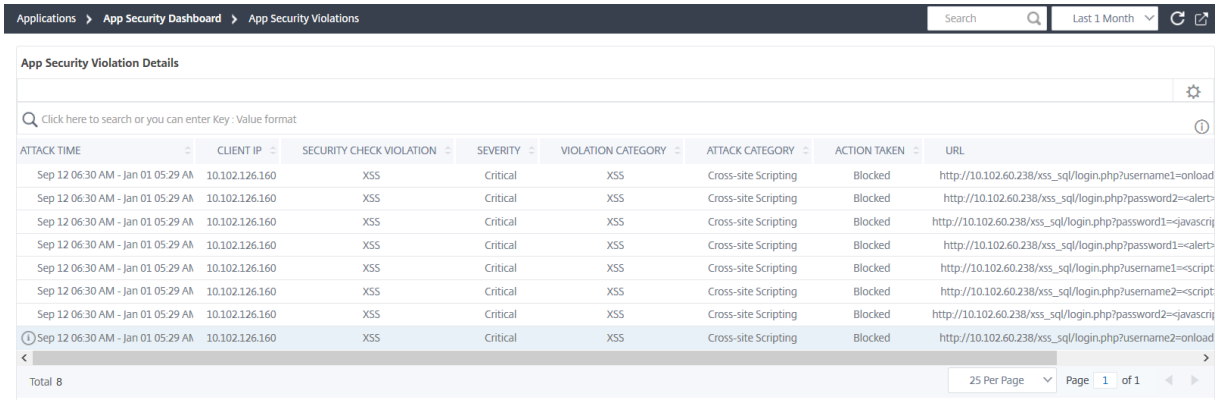
4 - Zeigt die Sicherheitsverletzungen basierend auf Clients an. Das Diagramm App Security Investigator wird für jeden Client angezeigt. Sie können auf jede Client-IP klicken, um Ergebnisse anzuzeigen.

5 - Zeigt die Verstöße in Kartenansicht und Tabellenansicht an.

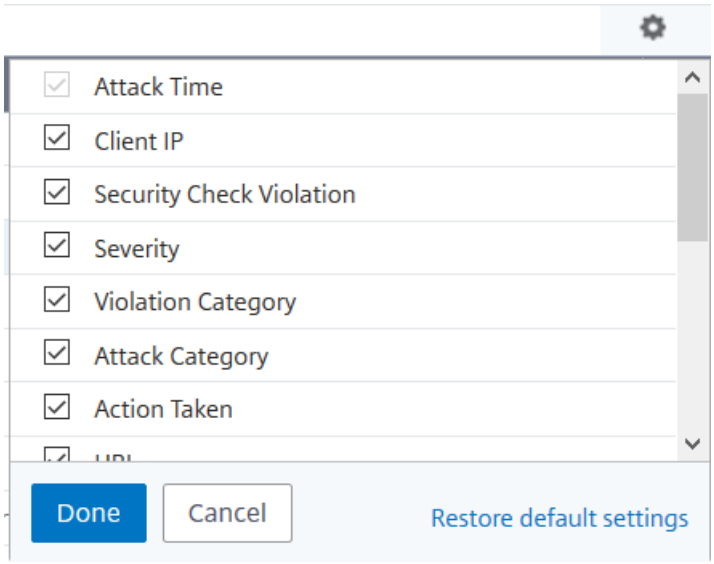
6 - Zeigt die Details der Verletzung an. Wenn Sie den Mauszeiger auf das Diagramm bewegen, werden die Details wie Verletzungstyp, Zeitpunkt des Angriffs und Gesamtereignisse angezeigt.

Wenn Sie auf ein Blasendiagramm klicken, werden die Details auf der Seite **Details zu App-Sicherheitsverletzungen** angezeigt. Wenn Sie beispielsweise weitere Details für eine siteübergreifende Skriptverletzung anzeigen möchten, klicken Sie in **App Security Investigator** auf das Diagramm, das für **XSS**ausgefüllt wurde.

Die **Details zu App-Sicherheitsverletzungen** werden mit Verstoßdetails wie Angriffszeit, Angriffskategorie, Schweregrad, URL usw. angezeigt.



Sie können auch auf die Option **Einstellungen** klicken, um die Optionen auszuwählen, die angezeigt werden sollen.



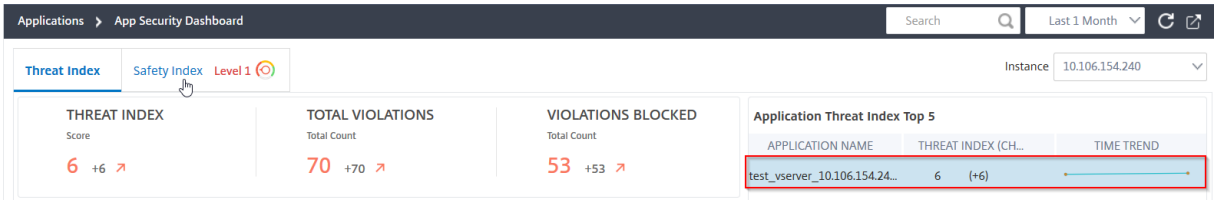
Sicherheitsindex Details

Nachdem Sie die Bedrohungsgefahr einer Anwendung überprüft haben, möchten Sie ermitteln, welche Anwendungssicherheitskonfigurationen vorhanden sind und welche Konfigurationen für diese Anwendung fehlen. Sie können diese Informationen erhalten, indem Sie einen Drilldown in die Zusammenfassung des Anwendungssicherheitsindex anzeigen.

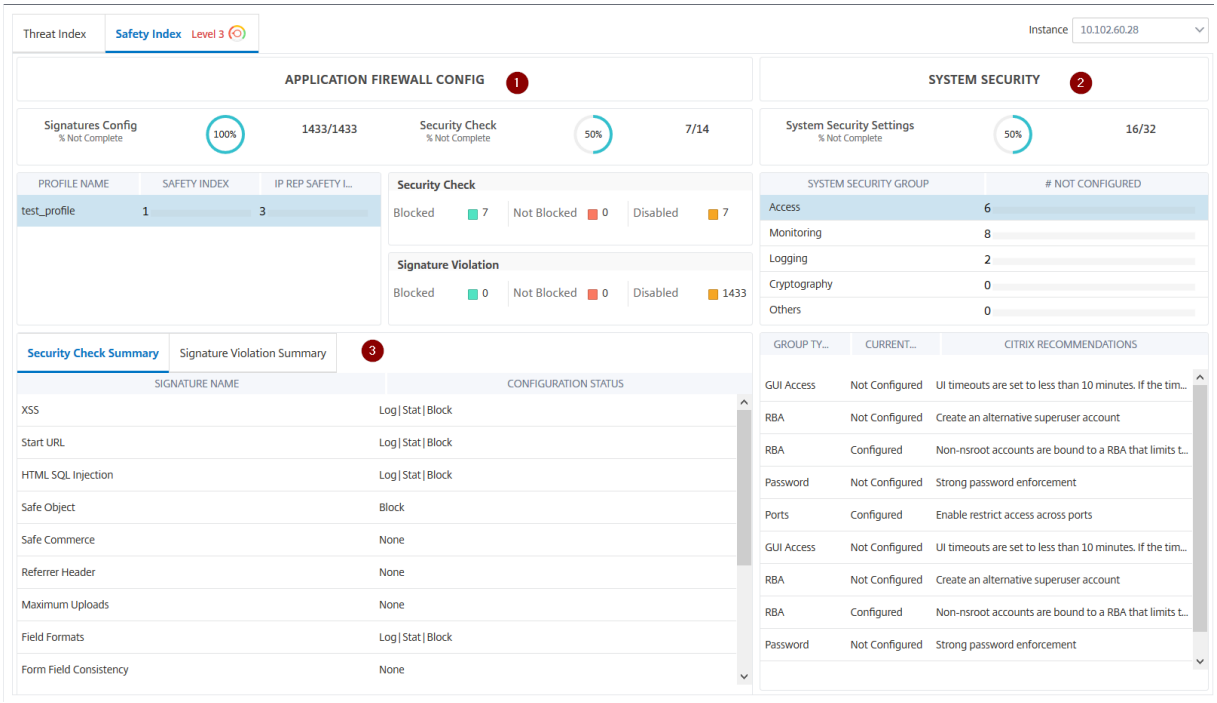
Die Zusammenfassung des Sicherheitsindex enthält Informationen über die Wirksamkeit der folgenden Sicherheitskonfigurationen:

- **Konfiguration der Anwendungs-Firewall**. Zeigt an, wie viele Signatur- und Sicherheitseinheiten nicht konfiguriert sind.
- **Citrix ADM Systemsicherheit**. Zeigt an, wie viele Systemsicherheitseinstellungen nicht konfiguriert sind.

Um die Details des **Sicherheitsindex** anzuzeigen, wählen Sie einen virtuellen Server/eine Anwendung aus, und klicken Sie auf die Registerkarte **Sicherheitsindex**.



Die Details werden angezeigt.



1 - Zeigt die detaillierten Informationen für Anwendungs-Firewall-Konfigurationen an.

2 - Zeigt die detaillierten Informationen für Systemsicherheit an. Klicken Sie auf jede Sicherheitsgruppe, um Details zum Status und zu Citrix Empfehlungen zu erhalten.

3 - Zeigt die Zusammenfassung für Sicherheitsprüfung und Signaturverletzung an.

Sie können auch eine Zusammenfassung der Bedrohungsumgebung anzeigen, indem Sie dieSicherheitseinsichtfür virtuelle Server aktivieren und dann zu **Analytics**> **Security Insight**navigieren. Weitere Informationen zum Anwendungsfall für Sicherheitsindex finden Sie unterSicherheitseinsicht

API-Gateway

April 28, 2021

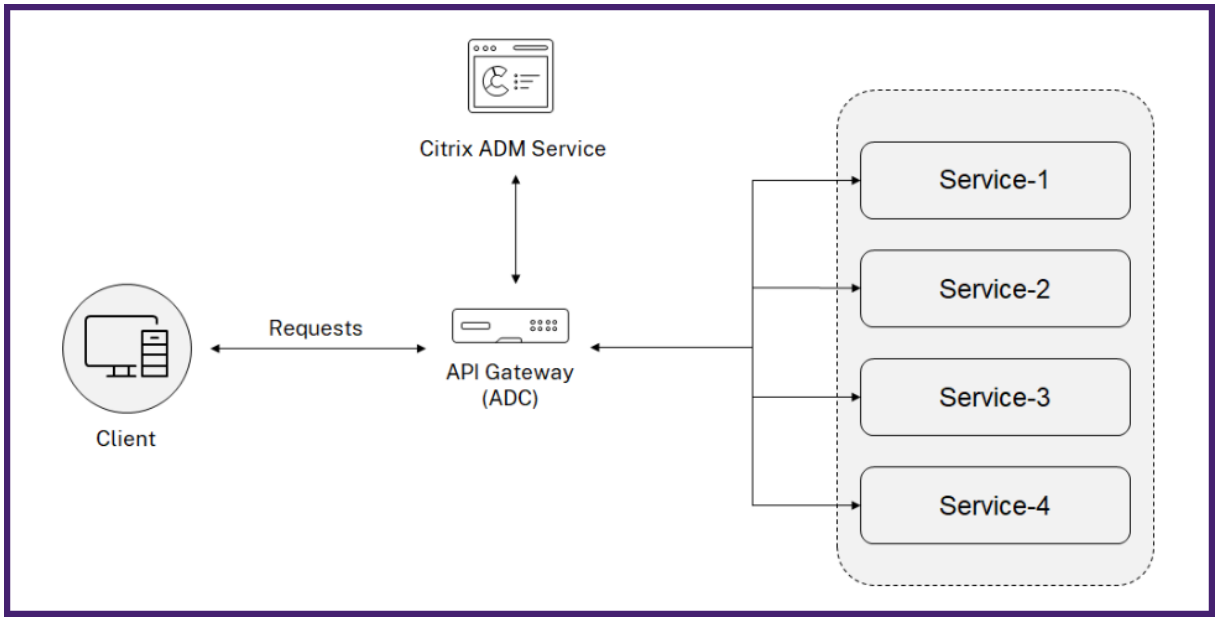
Ein API-Gateway dient als Einstiegspunkt für alle Anfragen an Ihre API-Endpunkte. Und gewährleistet einen sicheren und zuverlässigen Zugriff auf alle API-Endpunkte und Microservices in Ihrem System.

Ein API-Gateway stellt alle Anfragen und Antworten zwischen Ihren API-Clients/Anwendungen und Back-End-API-Services zur Verfügung. Es hilft Ihnen bei der Konfiguration, Verwaltung und Sicherung von API-Endpunkten. Sie können API-Definitionen auch auf eine der folgenden Arten erstellen und verwalten:

- Laden Sie die Swagger OAS-Spezifikationsdatei hoch
- Erstellen Sie Ihre eigene API-Definition

Weitere Informationen finden Sie unter Erstellen oder Hochladen einer API-Definition.

Die folgende Abbildung beschreibt, wie das API-Gateway die Client-Anfrage empfängt und die Antwort von den Back-End-API-Diensten sendet:



> **Hinweis**
>
> In Citrix Application Delivery Management ist diese Funktion für Benutzer verfügbar, die über Premium- oder Advanced-Lizenzen verfügen.

Vorteile des API-Gateways

Das API-Gateway bietet Ihnen die folgenden Vorteile:

- **Schützt Ihre API-Endpunkte**: Das API-Gateway fügt eine Sicherheitsebene hinzu und schützt Ihre API-Endpunkte und Back-End-API-Server vor Angriffen wie:
  - Pufferüberlauf
  - SQL Injection

  - Cross-Site Scripting
  - Denial-of-Service (Dos)

- **Überwacht und verbessert die API-Performance**: Das API-Gateway bietet Dienste wie SSL-Offloading, Authentifizierung, Autorisierung, Ratenbegrenzung und mehr. Diese Dienste erhöhen die API-Performance und ihre Verfügbarkeit.

  Die API-Analytik bietet Ihnen die Einblicke in Ihre API-Performance-Metriken und Bedrohungen für Ihre API-Endpunkte. Weitere Informationen finden Sie unter API-Analysen anzeigen.

- **Verwaltet den API-Verkehr**: Das API-Gateway abstrahiert die Komplexität Ihrer Backend-API-Infrastruktur.

- **Erzeugt API-Endpunkte**: Das API-Gateway erkennt die API-Endpunkte, die sich in Ihrer Organisation befinden, und fügt die Seite **API Discovery** hinzu.

API-Gateway verwalten

Als Administrator können Sie API-Definitionen erstellen und die API-Instanzen auf einem API-Gateway (ADC) in Citrix ADM bereitstellen. Weitere Informationen:

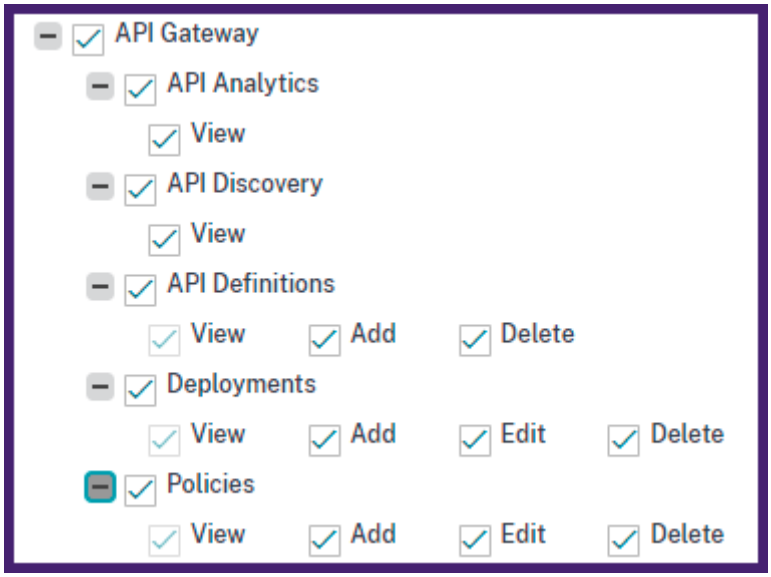
- Hinzufügen einer API-Definition
- Bereitstellen einer API-Instanz

In einem API-Gateway können Sie Sicherheitsrichtlinien anwenden. Informationen zum Erstellen einer API-Richtlinie finden Sie unter Hinzufügen von Richtlinien zu einer API-Bereitstellung.

Erteilen von API-Gateway-Konfigurations- und Verwaltungsberechtigungen

Als Administrator können Sie eine Zugriffsrichtlinie erstellen, um Benutzerberechtigungen für die Konfiguration und Verwaltung des API-Gateways zu erteilen. Die Benutzerberechtigungen können Anzeigen, Hinzufügen, Bearbeiten und Löschen sein. Führen Sie Folgendes aus, um Berechtigungen zu erteilen:

1. Navigieren Sie zu **Konto > Benutzerverwaltung > Zugriffsrichtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie unter **Zugriffsrichtlinien erstellen**einen Richtliniennamen und die Beschreibung an.
4. Erweitern Sie im Feld **Berechtigungen** die Option **Anwendungen** und dann **API Gateway**.
5. Wählen Sie die erforderlichen **API-Gateway-Seiten** aus Wählen Sie dann die Berechtigungen aus, die Sie gewähren möchten.



> **Wichtig**
>
> Stellen Sie sicher, dass Sie Berechtigungen für die Funktionen erteilen, die zur Verwendung eines API-Gateways erforderlich sind. Wenn Sie beispielsweise Benutzern Zugriff auf die Seite " **Bereitstellungen** " gewähren, erfordern die folgenden Funktionen auch Benutzerzugriff:
>
> - StyleBooks
> - IPAM
> - Load Balancing (unter **Netzwerkfunktionen**)
> - Content Switching (unter **Netzwerkfunktionen**)
> - Geräte-API-Proxy (unter **API**)

Weitere Informationen zu Zugriffsrichtlinien finden Sie unter Konfigurieren von Zugriffsrichtlinien für ADM.

API-Analysen anzeigen

April 28, 2021

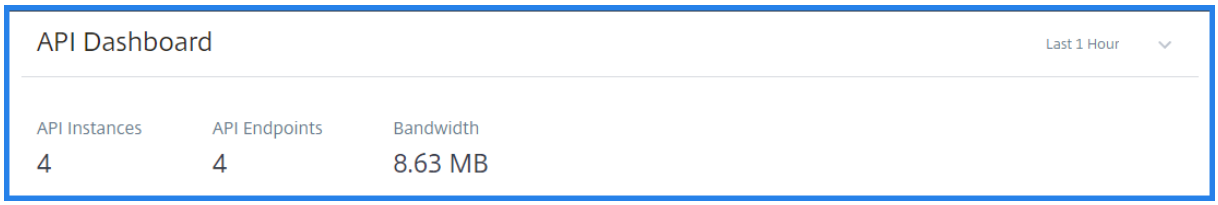
API-Analysen ermöglichen Transparenz im API-Datenverkehr. Diese Analyse ermöglicht es IT-Administratoren, API-Instanzen und Endpunkte zu überwachen, die von einem API-Gateway bereitgestellt werden. Es bietet eine integrierte periodische Überwachung von API-Anfragen.

Bevor Sie API-Analysen überwachen, stellen Sie sicher, dass Sie Folgendes ausführen:

1. Hinzufügen einer API-Definition
2. Bereitstellen einer API-Definition
3. Hinzufügen einer Richtlinie zu einer API-Definition

4. Lizenz auf API-Instanzen anwenden
5. Aktivieren von Web Insight für API-Instanzen

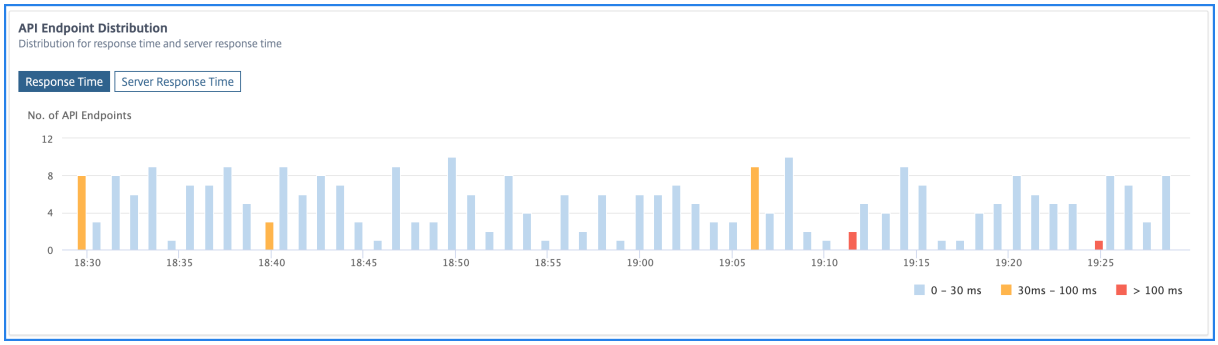
In **API Analytics** können Sie die Antwortzeit von API-Instanzen und Endpunkten überwachen, die als Teil von API-Definitionen hinzugefügt werden. Außerdem wird die verbrauchte Bandbreite von API-Instanzen und Endpunkten angezeigt.



Standardmäßig zeigt das Dashboard API-Analysen für die letzten eine Stunde an. Sie können eine Dauer auswählen, um API-Analysen für dieses Intervall anzuzeigen. Klicken Sie auf **Mehr** anzeigen auf jeder Kachel, um die gesamte Liste anzuzeigen. In dieser Ansicht können Sie API-Instanzen und Endpunkte anhand ihrer Teilnamen mit Ausnahme der Kachel **Geo Locations** durchsuchen.

API-Endpunktverteilung

Dieses Diagramm zeigt die Verteilung der Anwendungs- und Server-Antwortzeit für API-Endpunkte. Sie können einen API-Endpunkt identifizieren, der eine große Reaktionszeit hat, und die erforderlichen Maßnahmen ergreifen.

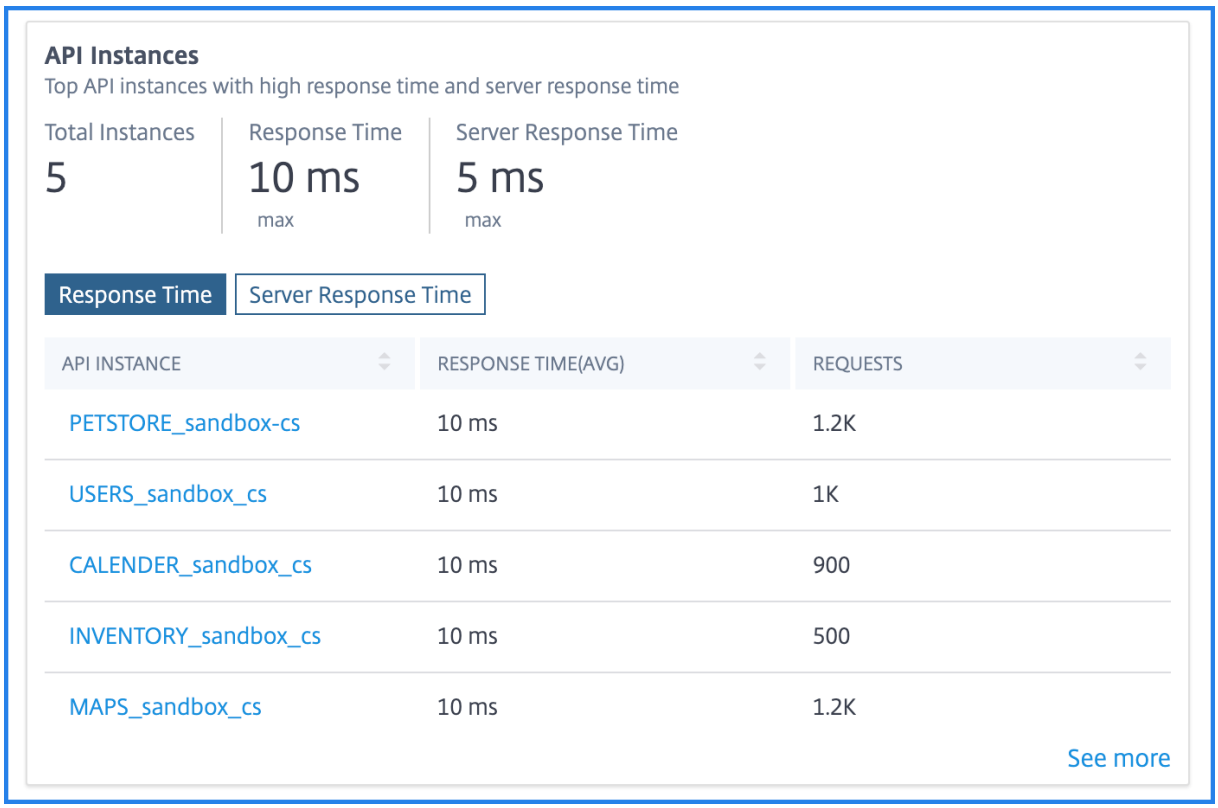


Die API-Endpunkte werden je nach Antwortzeitlimit in einer der folgenden Farben angezeigt:

- **Blau** — Wenn die Antwortzeit weniger als 30 Millisekunden beträgt.
- **Orange** — Wenn die Antwortzeit zwischen 30 und 100 Millisekunden liegt.
- **Rot** — Wenn die Antwortzeit mehr als 100 Millisekunden beträgt.

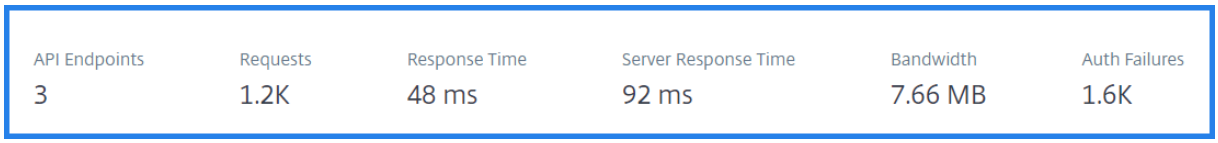
API-Instanzen

Die Kachel **API-Instanzen** zeigt die obersten API-Instanzen mit hoher Reaktionszeit für Anwendungen und Server an.



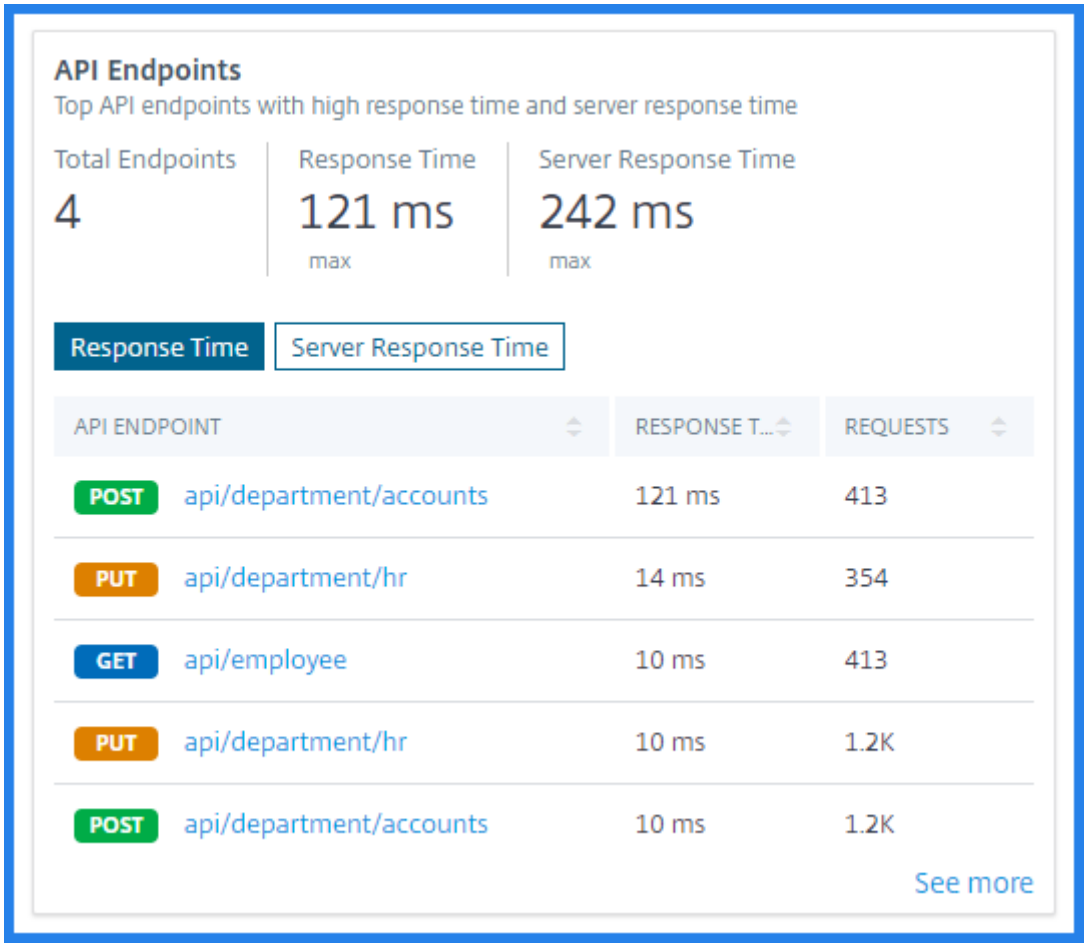
Wählen Sie eine API-Instanz aus, um die Performance-, Verwendungs- und Sicherheitsdetails anzuzeigen. Die ausgewählte API-Instanz zeigt die folgenden Informationen an:

- Anzahl der API-Endpunkte
- Anforderungsanzahl
- Reaktionszeit für Anwendung und Server
- Verbrauchte Bandbreite
- Fehler bei der Authentifizierung



API-Endpunkte

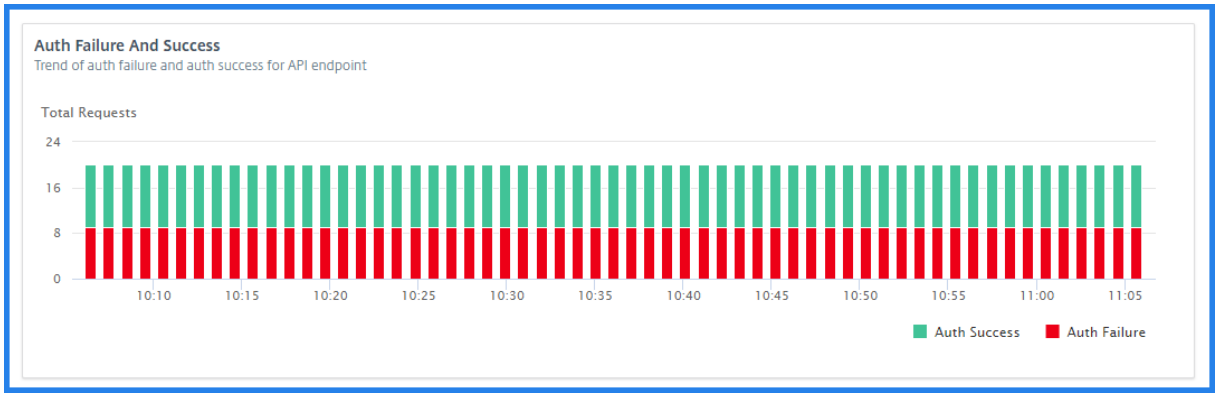
Die Kachel **API-Endpunkte** zeigt die obersten Endpunkte mit hoher Reaktionszeit für Anwendungen und Server an.



Wählen Sie einen API-Endpunkt aus, um Performance-, Verwendungs- und Sicherheitsdetails anzuzeigen.

Fehler bei der Authentifizierung

Die Kachel **Authentifizierungsfehler** zeigt die obersten API-Endpunkte an, die mehr Authentifizierungsfehler aufweisen. Der Authentifizierungsfehler oder der Erfolg erfolgt basierend auf der Richtlinie, die einer API-Definition hinzugefügt wurde.



Wenn Sie Authentifizierungsfehler und Erfolgsrate in einem API-Endpunkt anzeigen möchten, gehen Sie wie folgt vor:

1. Wählen Sie einen Endpunkt von **API-Endpunkten** aus.
2. Klicken Sie auf die Registerkarte **Sicherheit**. Auf dieser Registerkarte werden die Authentifizierungsfehler und -erfolge auf dem ausgewählten Endpunkt angezeigt.

Wenn Sie den Authentifizierungsfehler und die Erfolgsrate in den API-Endpunkten einer Instanz anzeigen möchten, gehen Sie wie folgt vor:

1. Wählen Sie eine Instanz aus der **API-Instanz**aus.
2. Klicken Sie auf die Registerkarte **Sicherheit**. Auf dieser Registerkarte werden die Authentifizierungsfehler und Erfolge in den Endpunkten der ausgewählten Instanz angezeigt.

Unterschiedliche API-Einblicke anzeigen

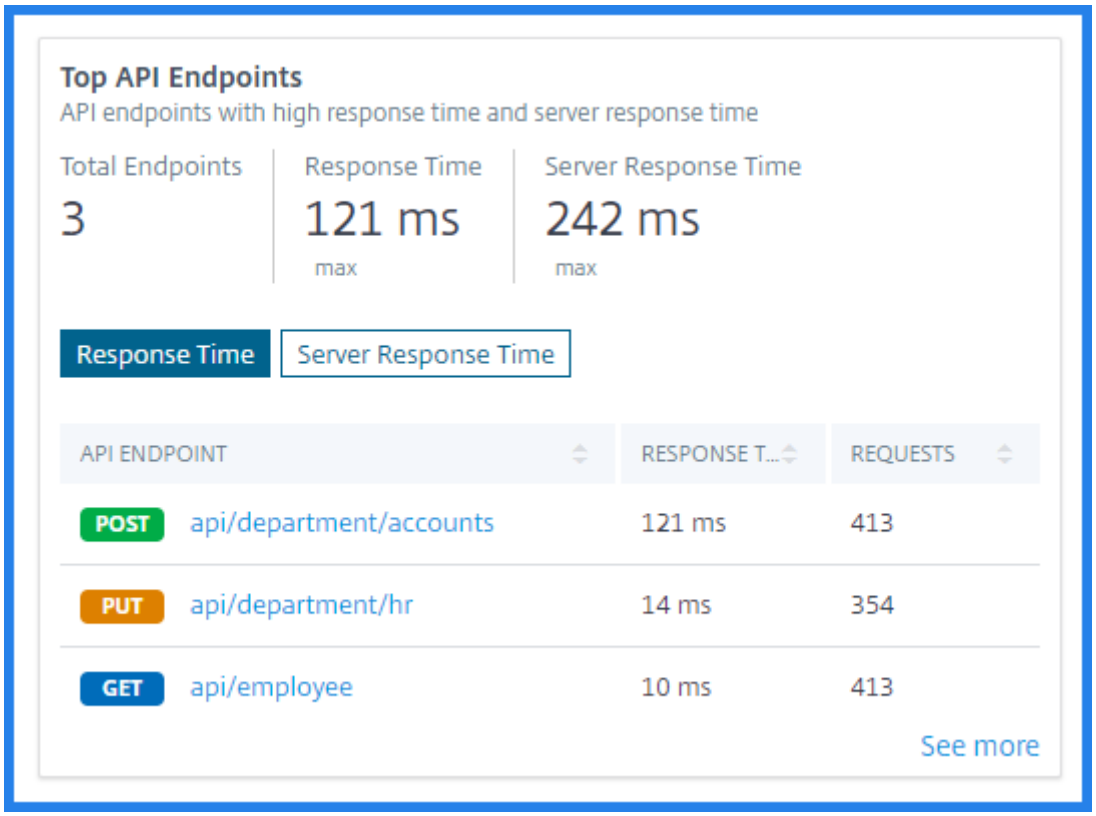
Navigieren Sie durch API Analytics, um bestimmte Informationen zu den folgenden Themen anzuzeigen:

- Top-API-Endpunkte in einer Instanz
- Am häufigsten aufgerufene APIs
- Geolokation eines Endpunkts
- HTTPS-Antwortstatus
- API-Anforderungen Trend
- Bandbreitenverbrauch eines Endpunkts
- SSL-Fehler und Verwendung

Anzeigen der obersten API-Endpunkte in einer Instanz

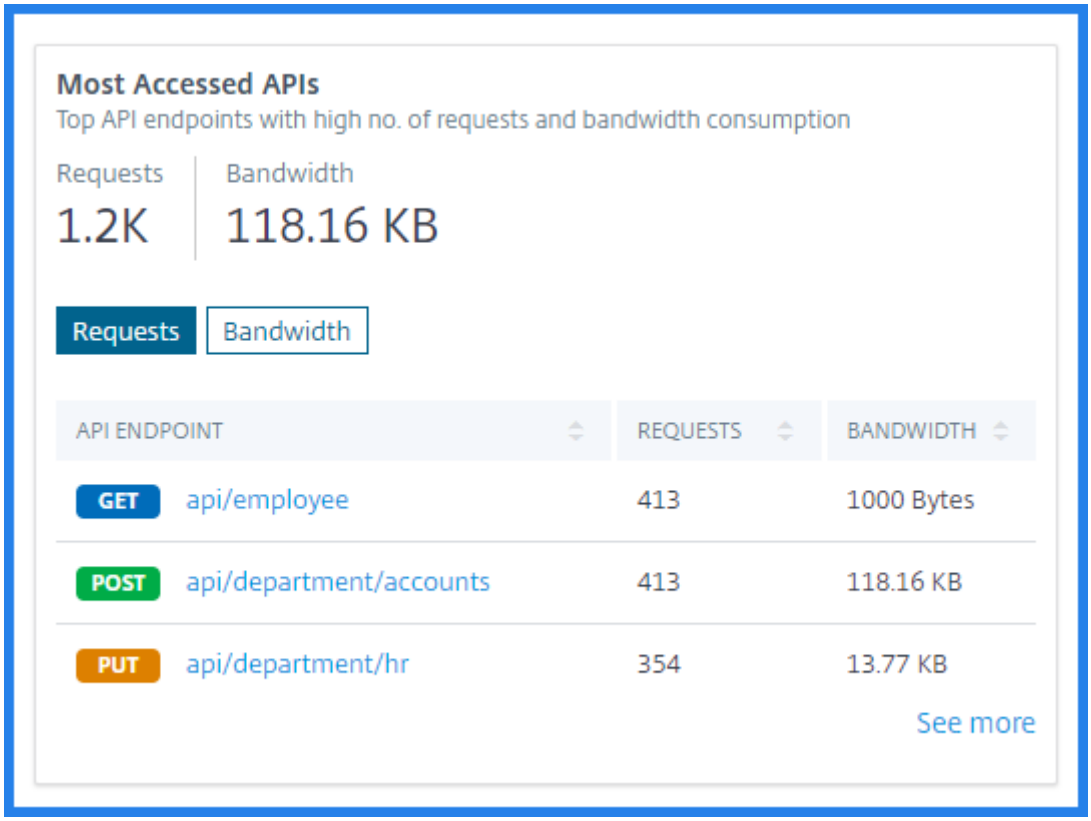
Auf der Seite " **API Analytics** " werden die Top-Endpunkte angezeigt, die eine hohe Reaktionszeit aufweisen. Wenn Sie ähnliche Endpunkte einer Instanz anzeigen möchten, wählen Sie eine Instanz aus **API-Instanzen**aus.

Die Kachel " **Top API-Endpunkte** " zeigt die Endpunkte an, die eine hohe Antwortzeit für Anwendungen und Server aufweisen.



Anzeigen der am meisten aufgerufenen APIs

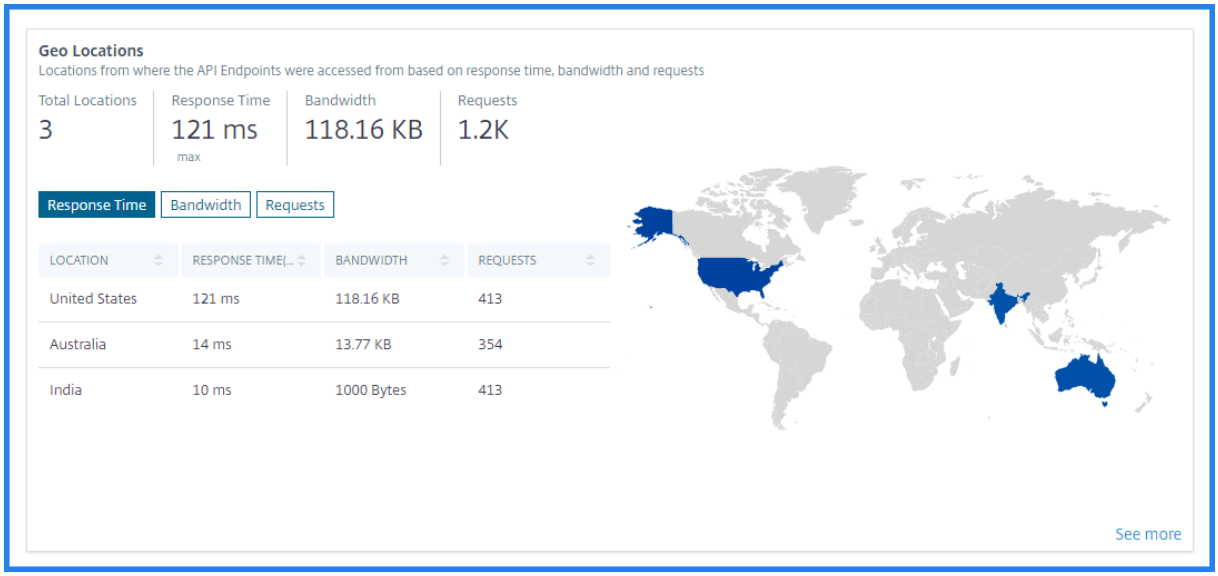
Wählen Sie in **API Analytics**eine API-Instanz aus API-Instanzen aus. Die Kachel **Am meisten Zugriff auf APIs** zeigt die obersten Endpunkte an, die mehr Anforderungen und Bandbreite aufweisen.



Geo-Position eines Endpunkts anzeigen

1. Wählen Sie in **API Analytics**eine der folgenden Optionen aus:
   - Wählen Sie eine Instanz aus **API-Instanzen** aus, um die Speicherorte anzuzeigen, von denen die Endpunkte der ausgewählten Instanz Anforderungen empfangen haben.
   - Wählen Sie einen Endpunkt aus **API-Endpunkten** aus, um Speicherorte anzuzeigen, von denen der Endpunkt Anforderungen empfangen hat.
2. In **Leistung und Nutzung**wird die Kachel **Geostandorte** angezeigt.

   Sie können Standorte basierend auf Antwortzeit, Bandbreite und Anforderungen sortieren.

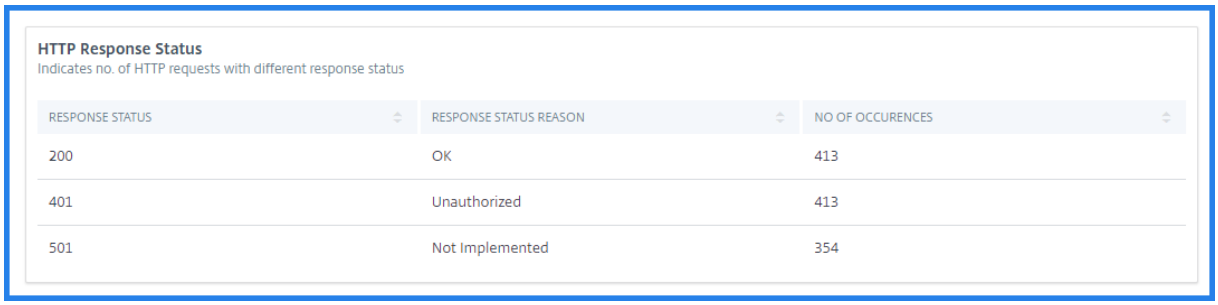


HTTPS-Antwortstatus anzeigen

Die Kachel **HTTPS-Antwortstatus** zeigt den Antwortstatus mit Grund und Vorkommen an. Sie können den HTTPS-Antwortstatus auf eine der folgenden Arten anzeigen:

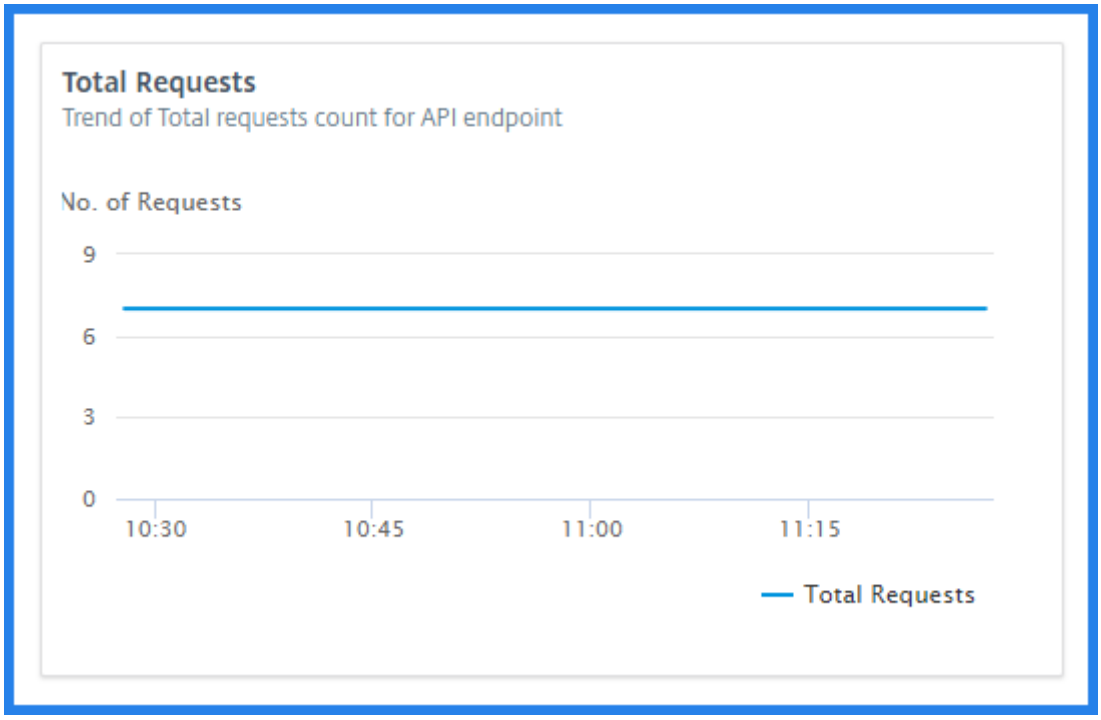
- Wählen Sie eine Instanz aus **API-Instanzen** aus.
- Wählen Sie einen Endpunkt von **API-Endpunkten** aus.

Diese Kachel wird auf der Registerkarte **Leistung und Verwendung** angezeigt.

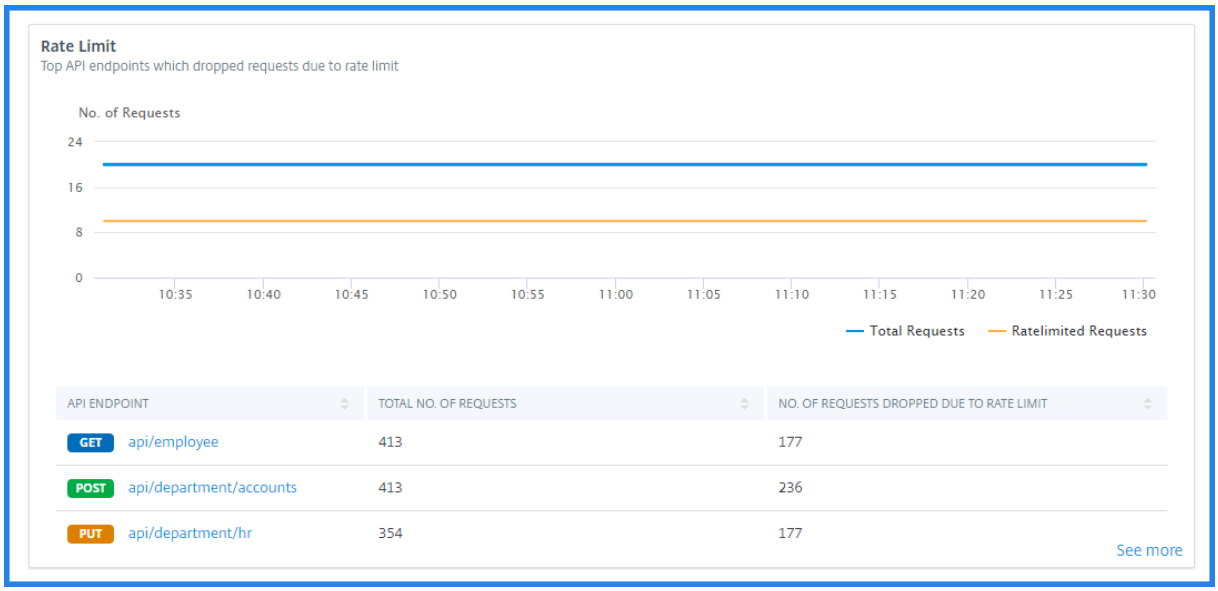


Trend zu API-Anforderungen anzeigen

Wählen Sie einen Endpunkt von **API-Endpunkten** aus. In **Performance und Verwendung**zeigt die Kachel **Gesamtanforderungen** den Trend der Gesamtzahl der von einem Endpunkt empfangenen Anforderungen an.



Wenn Sie den Trend der verfallenen Anforderungen aufgrund eines Tariflimits anzeigen möchten, wählen Sie eine Instanz aus **API-Instanzen**aus. In **Sicherheit**zeigt die Kachel " **Rate Limit** " den Trend der ausgelassenen Anforderungen an. Außerdem wird der Trend der gesamten Anfragen angezeigt, die von einem Endpunkt empfangen wurden.



Mit diesem Vergleich können Sie bestimmen, wie viele Anforderungen aufgrund eines Satzlimits zwischen den Gesamtanforderungen gelöscht werden.

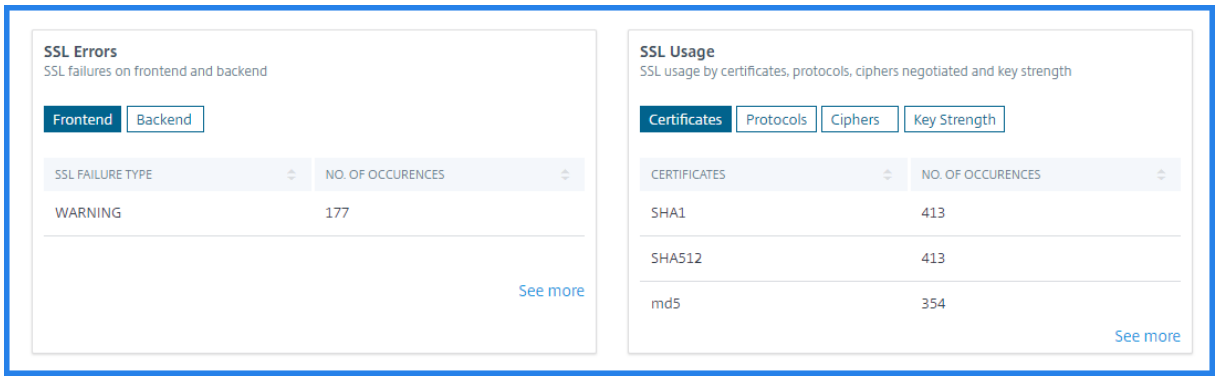
Anzeigen der Bandbreitenverbrauch eines Endpunkts

Um den Trend zum Bandbreitenverbrauch nach einem Endpunkt anzuzeigen, wählen Sie einen Endpunkt aus den API-Endpunkten aus. Die Kachel **Bandbreite** zeigt ein Diagramm für den Bandbreitenverbrauch an.

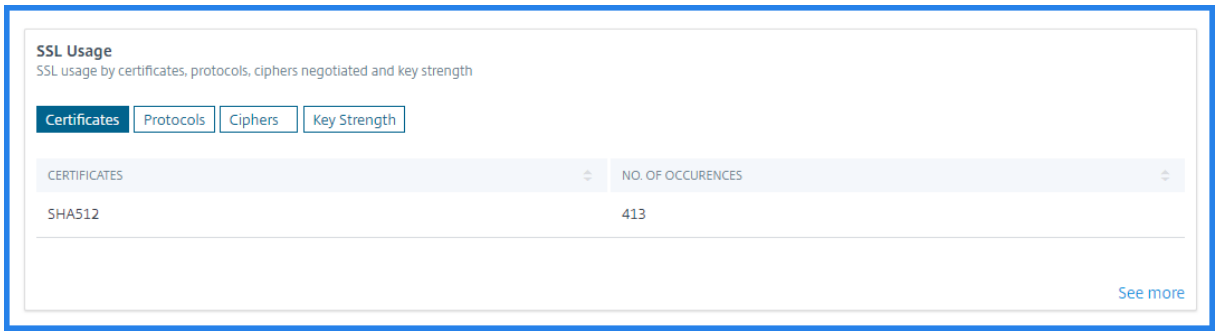
Anzeigen von SSL-Fehlern und -verwendung

Wählen Sie eine Instanz aus **API-Instanzen** aus. In **Sicherheit**werden die folgenden Kacheln angezeigt:

- **SSL-Fehler** — Zeigt SSL-Fehler an, die auf Clients und Anwendungsservern aufgetreten sind.
- **SSL-Verwendung** — Zeigt SSL-Zertifikate, Protokolle, Verschlüsselung und wichtige Stärken mit ihren Vorkommen an.



Um die SSL-Nutzung in einem Endpunkt anzuzeigen, wählen Sie einen Endpunkt aus den API-Endpunkten aus. Die Kachel **SSL-Verwendung** wird auf der Registerkarte **Sicherheit** angezeigt.



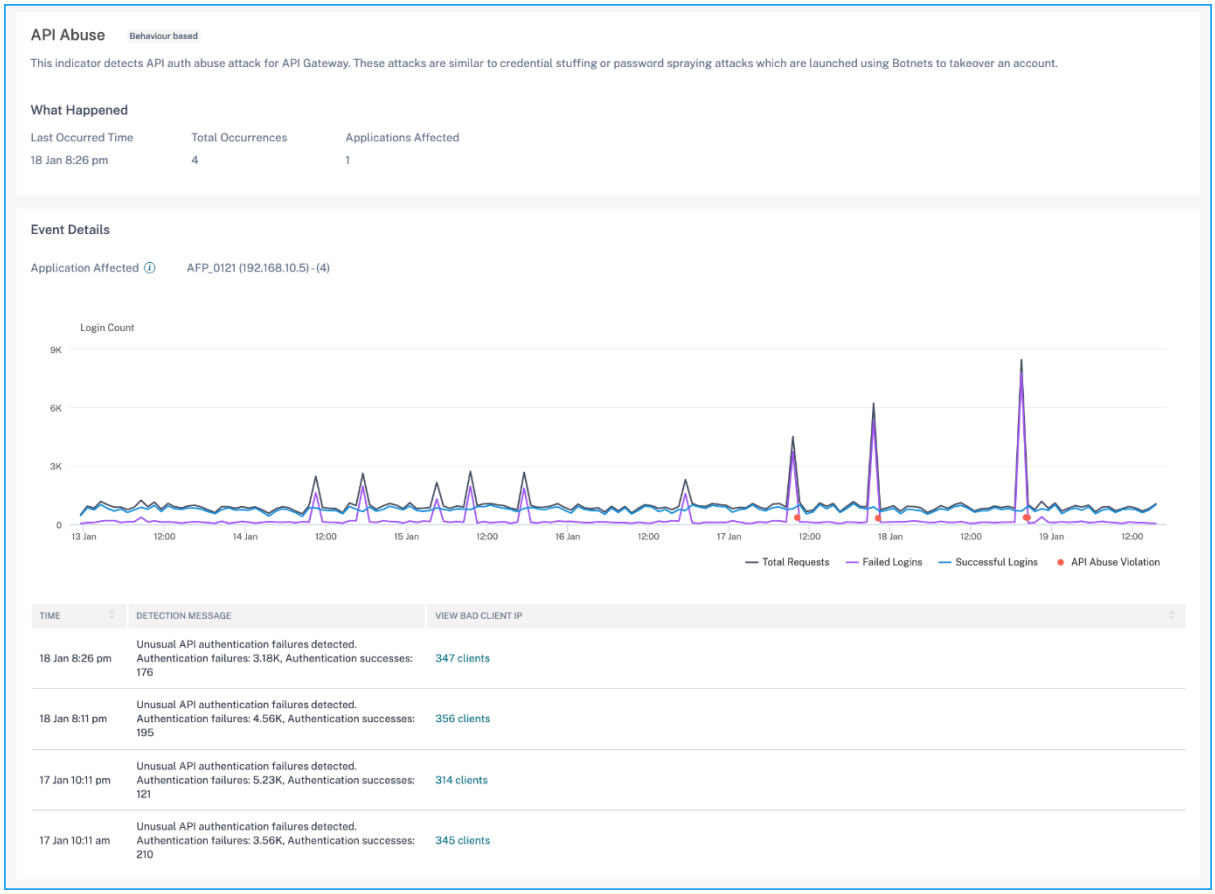
Anzeigen von Sicherheitsverletzungen der API

Citrix ADM zeigt die Sicherheitsverletzungen auf einem API-Gateway an. Die Sicherheitsbedrohung kann von einem Netzwerk, einer WAF oder einem Bot stammen. Mit diesen Informationen können Sie geeignete Maßnahmen ergreifen, um Ihre Instanz zu schützen. Die ADM-GUI zeigt die folgenden API-Sicherheitsverletzungen an:

API-Missbrauch

Schlechte Bots können API-Authentifizierungen verwenden oder stehlen und verschiedene Arten von Cyberangriffen wie Credential Stuffing und Kennwort-Sprühen durchführen. In Citrix ADM können Sie solche ungewöhnlichen Anmeldeaktivitäten für APIs analysieren.

Mithilfe des API-Missbrauchsindikators können Sie als Administrator mithilfe der API-Authentifizierung analysieren, ob schlechte Bots versucht haben, die Zielressource zu übernehmen.

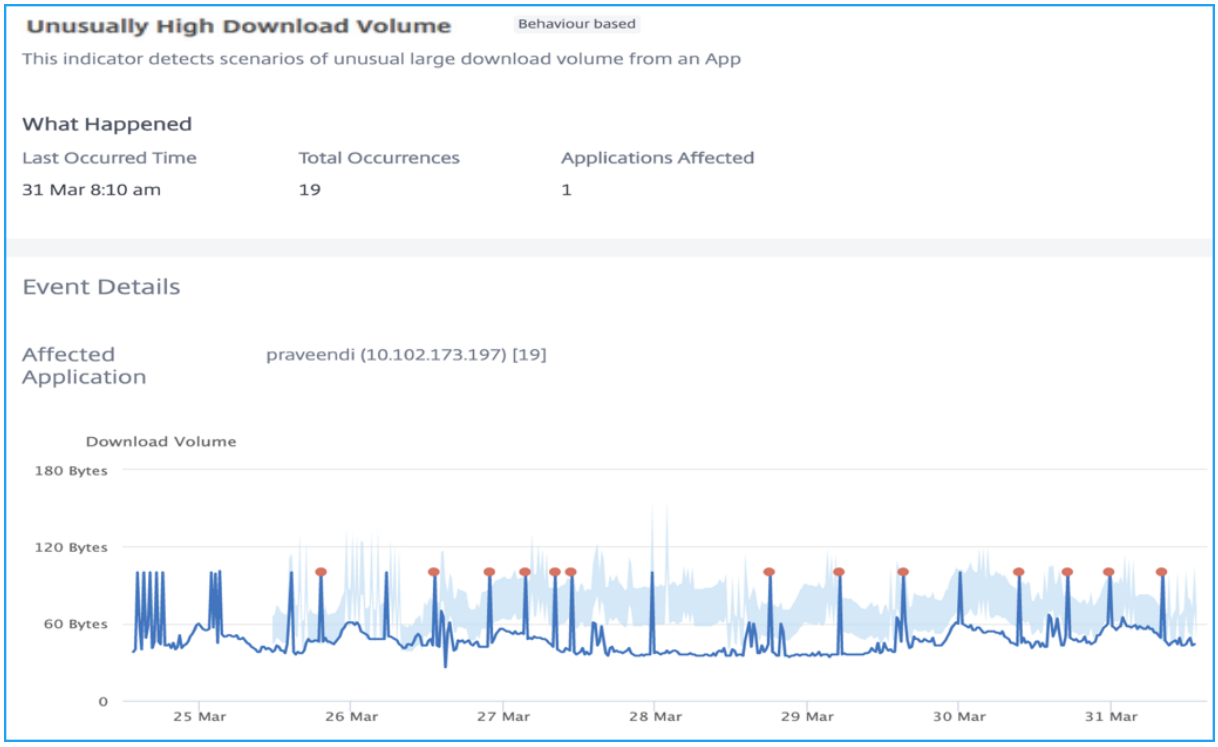


Weitere Informationen finden Sie unter API-Missbrauch.

Übermäßige Datengefährdung

Ein API-Endpunkt kann große Antworten auf Client-Anfragen haben. Diese Bedingung wird als übermäßige Datengefährdung bezeichnet. Ein Angreifer kann solche Schlupflöcher identifizieren, um mehr Informationen vom Endpunkt zu erhalten.

In Citrix ADM können Sie die Antwortgrößen analysieren, die höher als üblich sind. Und Sie können geeignete Maßnahmen ergreifen, um eine übermäßige Datengefährdung zu verhindern. Die ADM-GUI zeigt solche Verstöße unter dem Indikator für **ungewöhnlich hohes Download-Volumen** an. Sie können die übermäßige Datengefährdung vom betroffenen Endpunkt aus analysieren und geeignete Maßnahmen ergreifen.



Weitere Informationen finden Sie unter Ungewöhnlich hohes Downloadvolumen.

Erstellen oder Hochladen einer API-Definition

April 28, 2021

Eine API-Definition ist ein Dokument, das eine API beschreibt, die die OpenAPI-Spezifikationsstandards (Swagger 2.0, OpenAPI 3.0.x) verwendet. Diese Definition kann API-Ressourcenpfade und -methoden enthalten, um sie zu bedienen. Sie können ADM API-Definitionen hinzufügen und sie dann auf einem API-Gateway (Citrix ADC) bereitstellen.

Sie können API-Definitionen auf eine der folgenden Arten erstellen:

- Laden Sie die Swagger OAS-Spezifikationsdatei hoch
- Erstellen Sie Ihre eigene API-Definition

> **Hinweis**
>
> Derzeit unterstützt ADM das Parsen von OAS-Spezifikationsdateien, die **Swagger 2.0** oder **Openapi 3.0.1**verwenden.

Laden Sie die OAS-Spezifikation hoch

Sie können die OAS-Spezifikation auf die ADM-GUI hochladen.

1. Navigieren Sie zu **Anwendungen > API Gateway > API-Definitionen**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie **OAS-Spezifikation hochladen**aus.

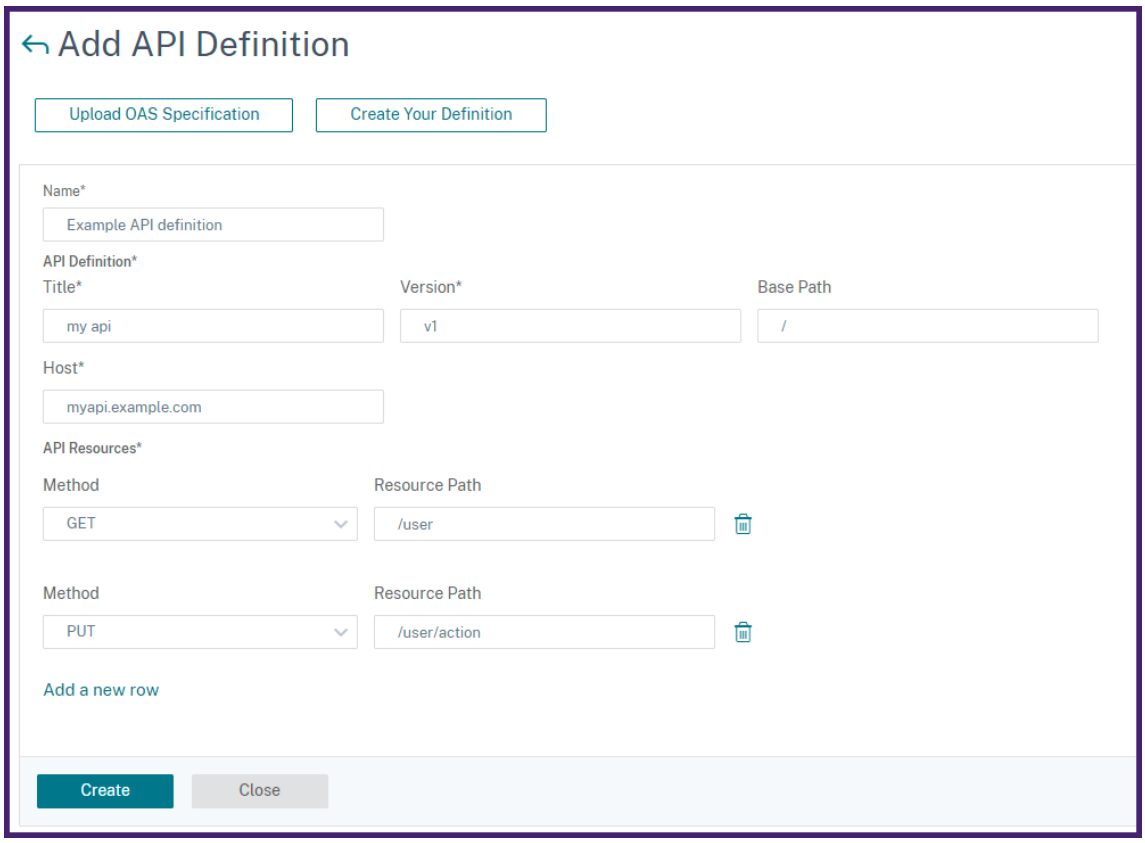
   > **Hinweis:
   >
   > Stellen Sie**sicher, dass die OAS Spezifikationsdatei im YAML- oder JSON-Format vorliegt. Und diese Datei darf keine externen Referenzen enthalten. Derzeit unterstützt ADM Swagger Version 2.0.

4. Durchsuchen Sie eine OAS-Spezifikation von Ihrem lokalen Computer und laden Sie sie zu ADM hoch.

Erstellen einer API-Definition

Sie können Ihre eigene API-Definition in der ADM-GUI erstellen.

1. Navigieren Sie zu **Anwendungen > API Gateway > API-Definitionen**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie **Create Your Definition** und geben Sie Folgendes an:
   - **Name** - Ein Name für die API-Definition.
   - **API-Definition** - Eine Definition muss Titel, Version, Basispfad und Host enthalten. Sie können einen Domainnamen oder eine IP-Adresse im Feld **Host** angeben.
   - **API-Ressourcen** - Fügen Sie Ihrer Definition mehrere API-Ressourcen hinzu. Jede Ressource hat einen Pfad und eine unterstützte Methode.



4. Klicken Sie auf **Erstellen**.

API-Definitionen anzeigen

Auf der Seite " **API-Definitionen** " wird die hochgeladene Definition aufgeführt. Klicken Sie auf **Ansicht**, um die folgenden API-Definitionsdetails anzuzeigen:

- **Name** — Zeigt den Namen einer API-Definition an.
- **API-Definition** — Zeigt Titel, Version, Basispfad und Host einer Definition an.
- **API-Ressourcen** — Listet die API-Ressourcen in einer API-Definition und ihre Methoden zum Betrieb auf.

Als Nächstes stellen Sie diese Definition auf einem API-Gateway bereit.

Bereitstellen einer API-Instanz

April 28, 2021

Führen Sie die folgenden Schritte aus, um eine API-Instanz bereitzustellen:

1. Navigieren Sie zu **Anwendungen > API Gateway > Bereitstellungen**.
2. Klicken Sie auf **Hinzufügen**.
3. In **Deployment Basic** Info
   a) Geben Sie den **Bereitstellungsnamen**an.
   b) Wählen Sie in **Target API Gateway**eine ADC-Instanz als API-Gateway aus.
   c) Wählen Sie unter **API-Definitionen**die erforderliche API-Definition aus.
   d) Fügen Sie in **API Proxy**einen API-Proxy hinzu, um das API-Gateway zu verwenden. Ein API-Proxy ist eine virtuelle Front-End-IP-Adresse, bei der das API-Gateway den API-Verkehr von Clients erhält. Geben Sie die folgenden Details an:
      - **IP-Adresse**
      - **Port**
      - **TLS-Sicherheitsprofil** — Wählen Sie Hoch oder Mittel aus der Liste aus. Wenn Sie Hoch auswählen, wird es dem sicheren SSL-Profil auf einer ADC-Instanz zugeordnet.
      - **TLS-Zertifikat**
      - **TLS-Schlüssel**

      > **Hinweis:
      >
      > Laden Sie**TLS-Zertifikat und -Schlüssel in einem PEM-Format hoch.

      Alternativ können Sie ein IPAM-Netzwerk auswählen, um die IP-Adresse zuzuweisen. Um die zugewiesene IP-Adresse aus dem IPAM-Netzwerk anzuzeigen, navigieren Sie zu **Netzwerke > IPAM**. Weitere Informationen zu IPAM finden Sie unter IPAM konfigurieren.
4. Klicken Sie in **Upstream Services**auf **Hinzufügen**, um Back-End-API-Server hinzuzufügen, an die Sie den API-Datenverkehr übertragen möchten. Sie können einen Upstream-Dienst mit seinem Domänennamen oder seiner IP-Adresse konfigurieren:
   a) Geben Sie einen Namen für einen Upstream-Dienst an.
   b) Geben Sie die Domäne an.
   c) Geben Sie unter **Dienste**eine IP-Adresse und einen Portwert an. Um weitere IP-Adressen hinzuzufügen, klicken Sie auf **Neue Zeile hinzufügen**.
   d) Klicken Sie auf **Hinzufügen**.
5. Geben Sie unter **Routing**die folgenden Details an, um API-Datenverkehr basierend auf dem Ressourcenpfadpräfix zu übertragen:
   a) Geben Sie den Routennamen an.
   b) Wählen Sie eine **API-Ressource** aus, um eine API-Anforderung zu erhalten.

c) Wählen Sie einen **Upstream-Dienst** aus der Liste aus, in den Sie den API-Datenverkehr übertragen möchten.

6. Klicken Sie auf **Speichern**, um die Bereitstellungskonfiguration zu speichern.

   Wenn Sie die Konfiguration für API-Gateway bereitstellen möchten, klicken Sie auf **Save and Deploy**.

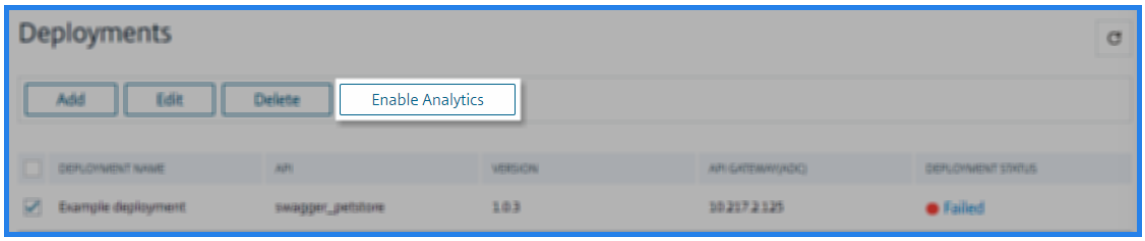
Aktivieren der API-Analytik

Im Folgenden sind die Voraussetzungen aufgeführt, um Analysen für eine Bereitstellung zu ermöglichen:

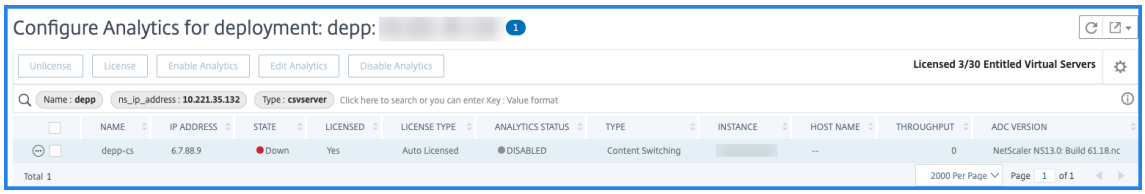
- Sicherstellen, dass virtuelle Server **lizenziert** sind
- Stellen Sie sicher, dass der Analytics-Status **deaktiviert** ist
- Stellen Sie sicher, dass virtuelle Server im Status **UP** sind

Um die API-Analyse für eine Bereitstellung zu aktivieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie die Bereitstellung aus, für die Sie die API-Analyse aktivieren möchten.
2. Klicken Sie auf **Analytics aktivieren**.



3. Wählen Sie auf der Seite **Configure Analytics for deployment** den virtuellen Server aus und klicken Sie auf **Analytics aktivieren**.



4. Im Fenster **Analytics aktivieren**:

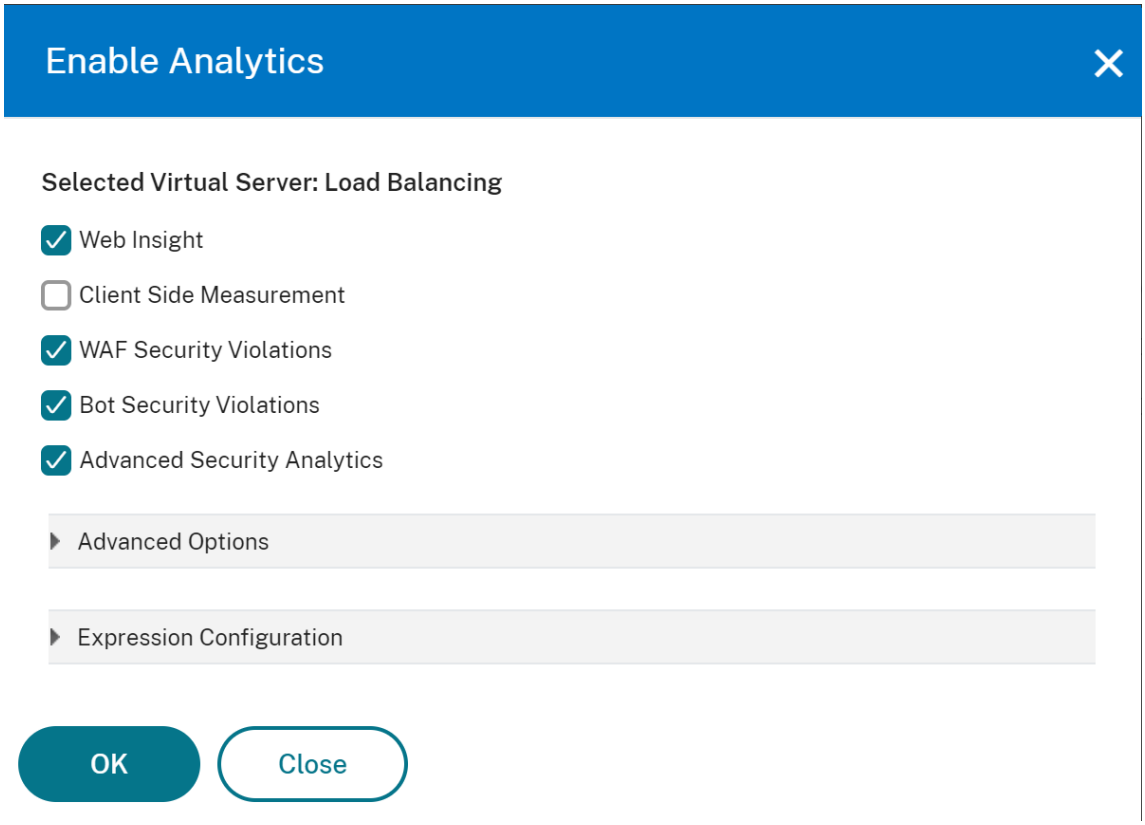
   a) Wählen Sie den Einsichtstyp aus (Web Insight, Security Insight, Bot Insight)

   b) Wählen Sie **Logstream** oder **IPFIX** als Transportmodus aus.

   Weitere Hinweise zu IPFIX und Logstream finden Sie unter Übersicht über den Logstream.

   c) Der Ausdruck ist standardmäßig “true”.

   d) Klicken Sie auf **OK**.



Die Citrix ADM-Prozesse, um Analysen auf den ausgewählten virtuellen Servern zu ermöglichen.

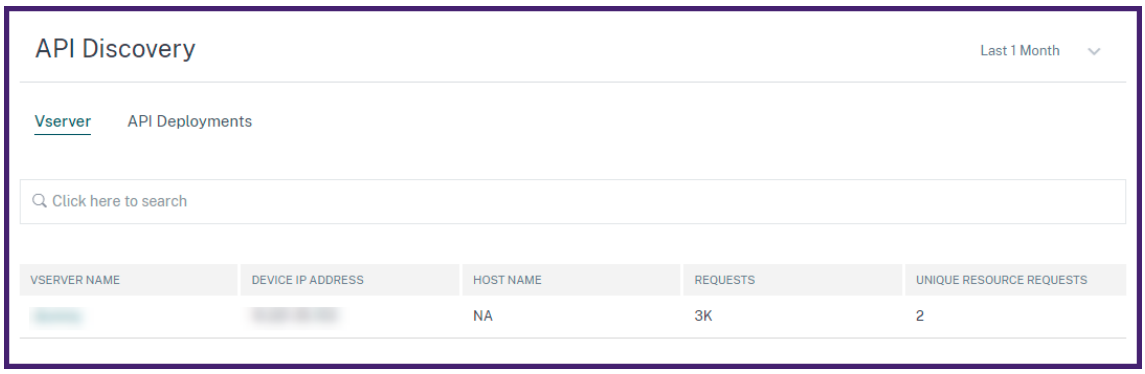
Entdecken Sie API-Endpunkte

April 28, 2021

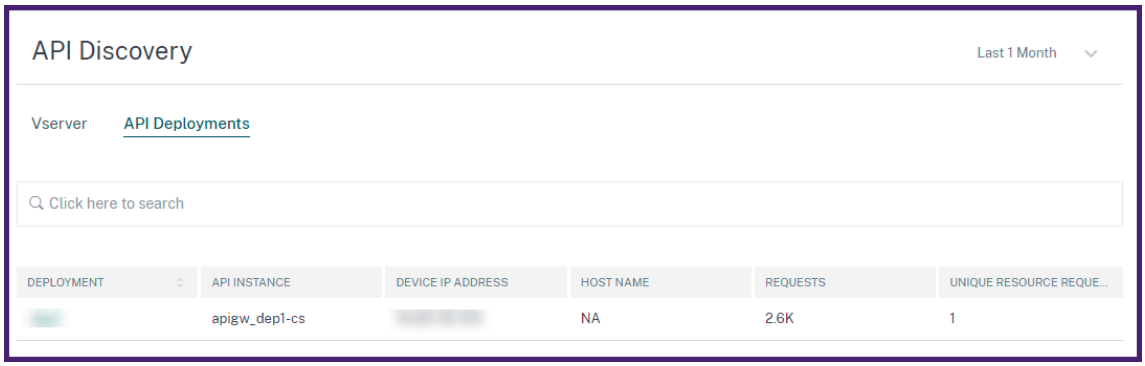
Sie können die erkannten API-Endpunkte, die sich in Ihrer Organisation befinden, mit API-Gateway anzeigen. Citrix ADM erkennt die API-Endpunkte basierend auf dem API-Datenverkehr, der auf ADC-Instanzen und API-Bereitstellungen empfangen wurde.

In Citrix ADM werden auf der Seite **Anwendungen > API Gateway > API Discovery** die erkannten API-Endpunkte angezeigt.

- **Virtuelle Server** — Die Registerkarte " **Vserver** " zeigt die virtuellen Server Ihrer ADC-Instanzen an. Die virtuellen Server werden auf dieser Registerkarte angezeigt, wenn sie die API-Anfragen für den angegebenen Zeitraum erhalten.



- **API-Bereitstellungen** — Auf dieser Registerkarte werden die API-Bereitstellungen angezeigt, die mit einer API-Definition von ADM bereitgestellt werden. Auf dieser Registerkarte werden die API-Endpunkte erkundet, wenn API-Bereitstellungen die API-Anfragen für den angegebenen Zeitraum erhalten. Informationen zum Hinzufügen und Bereitstellen einer API-Definition finden Sie unter Hinzufügen einer API-Definition und Implementieren von API.



> **Hinweis**
>
> - Stellen Sie sicher, dass Sie Analysen konfigurieren und Web Insights auf virtuellen Servern aktivieren. Siehe Aktivieren von Web Insight für API-Instanzen.
> - Sie können nur Richtlinien zu den API-Endpoints hinzufügen, die auf der Registerkarte **API-Bereitstellungen** erkannt werden.

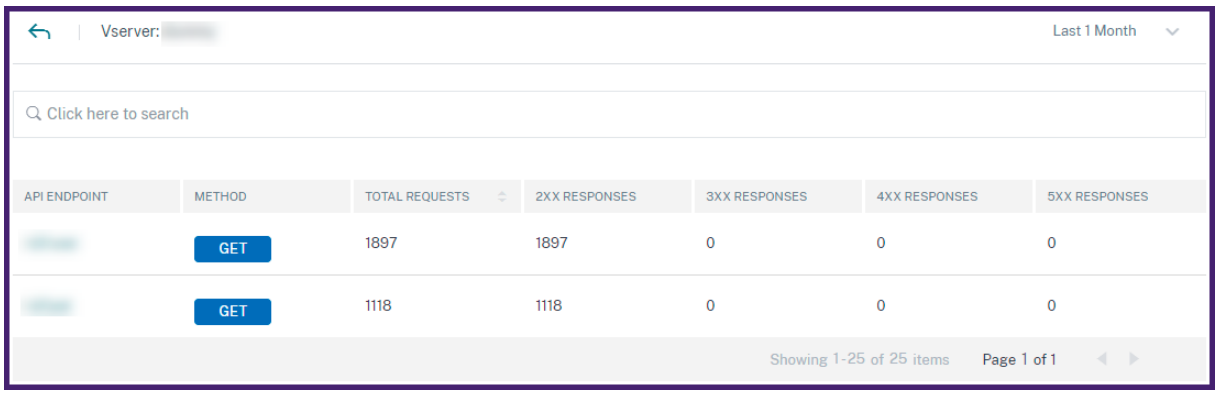
Anzeigen von API-Endpunkten

Wenn Sie in **API Discovery**einen virtuellen Server oder eine API-Bereitstellung auswählen, zeigt die ADM-GUI die API-Endpunkte und ihre Details an, wie zum Beispiel:

- **Methode** - Es zeigt die Methode an, die in einem API-Endpunkt verwendet wird. Zum Beispiel GET und POST Methoden
- **Gesamtzahl der Anforderungen** - Es zeigt die Anzahl der API-Anfragen auf dem API-Endpunkt an.
- **Antwortstatus** - Es zeigt die Anzahl für jeden Antwortstatus an. Zum Beispiel, 2xx3xx, 4xx, und 5xx.

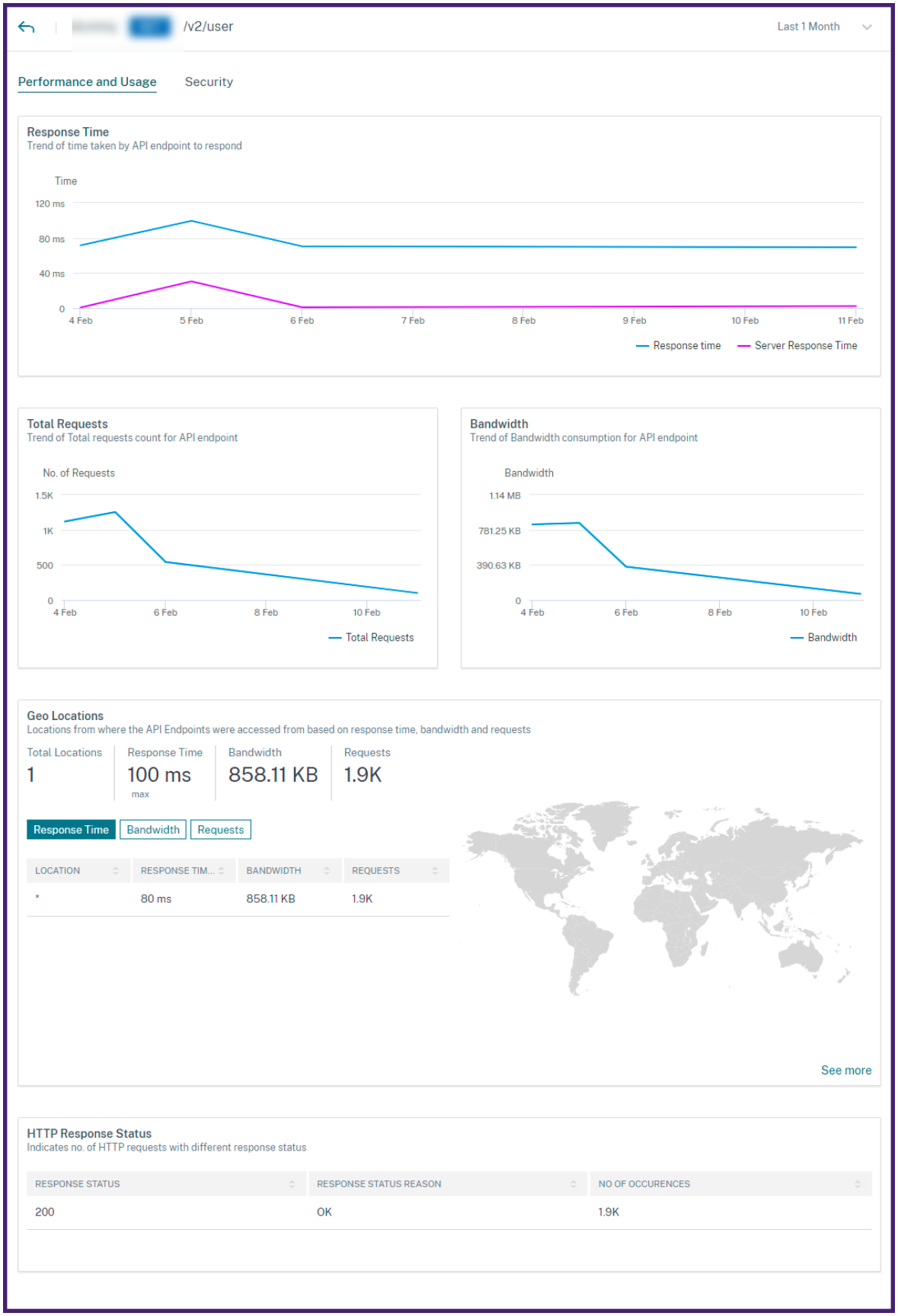
- **In Spec gefunden** - Diese Spalte wird nur für API-Bereitstellungen angezeigt. Manchmal erhalten die internen APIs, die nicht Teil der API-Definition sind, Verkehr von außen. Diese Spalte hilft Ihnen festzustellen, ob der API-Endpunkt und die beobachtete Methode Teil der API-Definition sind.

Virtuelle Server:



API-Bereitstellungen:

Sie können auch den erforderlichen API-Endpunkt auswählen, um den detaillierten Analysebericht anzuzeigen.



Weitere Informationen zu den einzelnen Abschnitten finden Sie unter API-Analysen anzeigen.

Hinzufügen von Richtlinien zu einer API-Bereitstellung

April 28, 2021

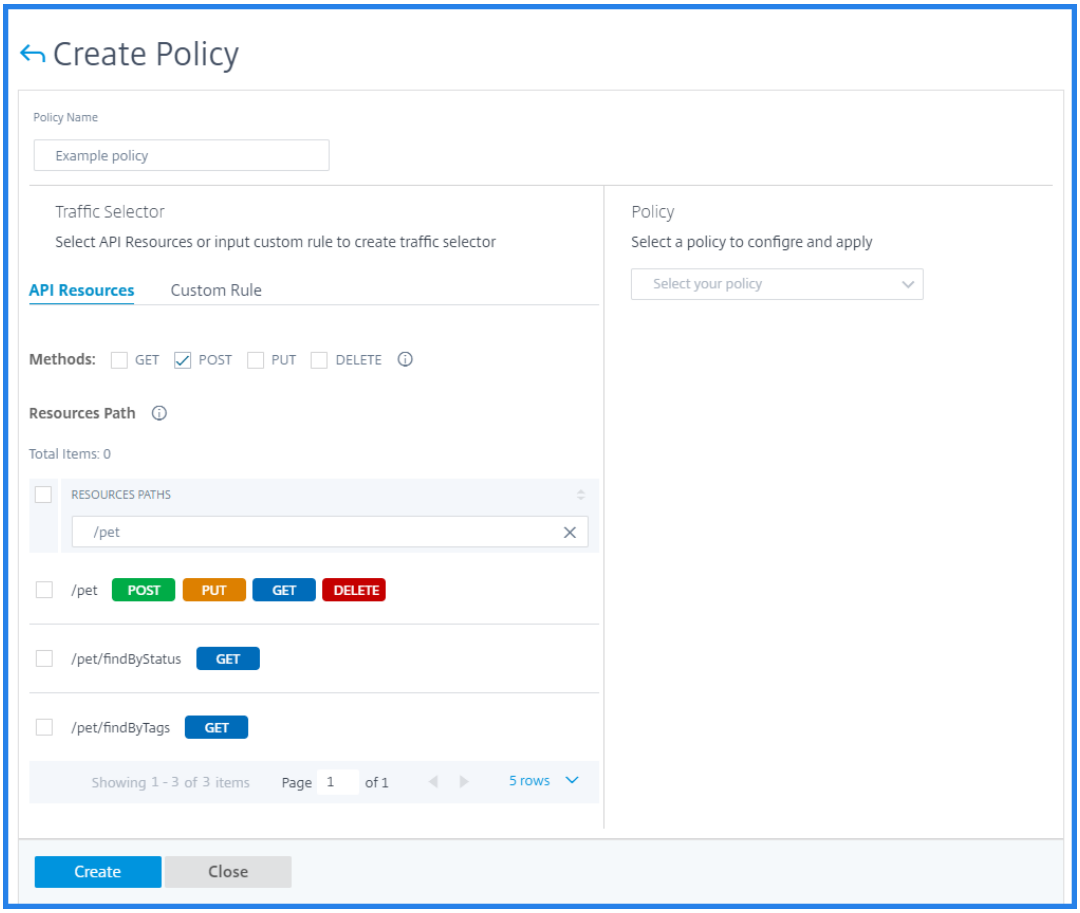
Sie können verschiedene Sicherheitsrichtlinien für Ihren API-Verkehr konfigurieren. Bei dieser Konfiguration müssen Sie die Auswahlkriterien für den Datenverkehr und die für eine Richtlinie erforderlichen Parameter angeben. Führen Sie die folgenden Schritte aus, um einer API-Definition eine Richtlinie hinzuzufügen:

1. Navigieren Sie zu **Anwendungen > API Gateway > Richtlinie**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie den Namen für eine Richtliniengruppe an.
4. Wählen Sie eine **Bereitstellung** aus der Liste aus.
5. Wählen Sie einen **Upstream-Dienst** aus der Liste aus, für den Sie Richtlinien konfigurieren möchten.
6. Klicken Sie auf **Hinzufügen**, um Datenverkehrsmarkierer und einen Richtlinientyp auszuwählen.

   Traffic-Selektor - Die Kriterien zur Auswahl des Datenverkehrs umfassen API-Ressourcenpfade oder Pfadpräfixe, Methoden und Richtlinien.

   Sie können eine der folgenden Optionen verwenden, um Kriterien für die Verkehrsauswahl festzulegen:

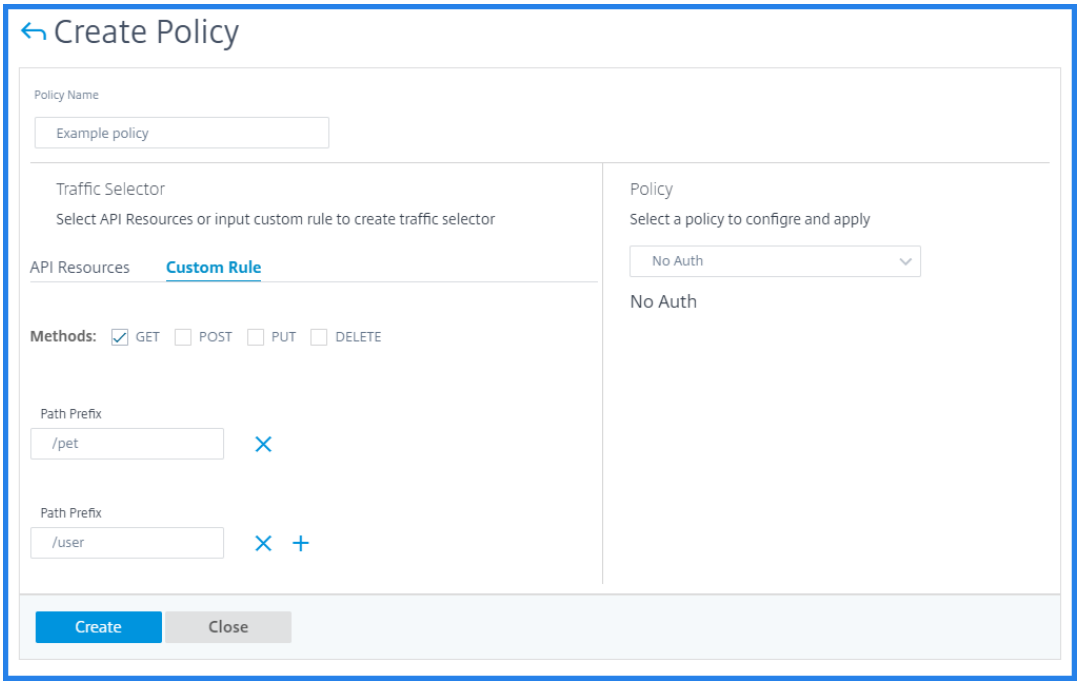
   - **API-Ressourcen** — Wählen Sie eine API-Ressource und ihre Methoden aus, für die Sie eine Richtlinie anwenden möchten. Sie können API-Ressourcen und -Methoden mit einem Schlüsselwort durchsuchen.



In diesem Beispiel werden die API-Ressourcen mit `/user`der `POST`Methode aufgelistet.

- **Benutzerdefinierte Regel** — Auf dieser Registerkarte können Sie benutzerdefinierte Pfadpräfixe und mehrere Methoden angeben.

  Die konfigurierte Richtlinie gilt für eine eingehende API-Anforderung, die der benutzerdefinierten Regel für die Auswahl des API-Datenverkehrs entspricht.



In diesem Beispiel gilt die **No-Auth-Richtlinie** für die API-Ressourcen, die das `/pet` Präfix und die `POST` Methode haben.

Wählen Sie unter **Richtlinie**eine Richtlinie aus der Liste aus, die Sie auf die ausgewählte API-Ressource und -Methode anwenden möchten. Weitere Informationen zu den einzelnen Richtlinien finden Sie unter Arten von Richtlinien.

7. Optional können Sie Richtlinientypen verschieben, um eine Priorität festzulegen. Die Richtlinientypen mit höherer Priorität gelten zuerst.
8. Klicken Sie auf **Speichern**, um eine Richtlinie hinzuzufügen. Wenn Sie die Richtlinie sofort anwenden möchten, klicken Sie auf **Speichern und Anwenden**.

Arten von Richtlinien

Wenn Sie eine API-Richtlinie konfigurieren, können Sie die folgenden Richtlinien auswählen, die Sie auf die API-Ressource und -Methode anwenden möchten:

- **Authentifizierung und Autorisierung**
- **Grenzwert für die Rate**
- **WAF**
- **BOT**
- **Überschrift Rewrite**

Authentifizierung und Autorisierung

API-Ressourcen werden auf einer Anwendung oder einem API-Server gehostet. Wenn Sie Zugriffsbeschränkungen für solche API-Ressourcen durchsetzen möchten, können Sie die Authentifizierungs- und Autorisierungsrichtlinien verwenden. Diese Richtlinien überprüfen, ob die eingehende API-Anfrage über die erforderliche Berechtigung für den Zugriff auf die Ressource verfügt.

Verwenden Sie die folgenden Richtlinien, um die Authentifizierung und Autorisierung für die ausgewählten API-Ressourcen zu definieren:

'No-Auth'

Verwenden Sie diese Richtlinie, um die Authentifizierung für den ausgewählten Datenverkehr zu überspringen.

'Auth-Basic'

Diese Richtlinie legt fest, dass die lokale Authentifizierung mit dem HTTP-Standardauthentifizierungsschema verwendet wird. Um die lokale Authentifizierung zu verwenden, müssen Sie Benutzerkonten auf dem Citrix ADC erstellen.

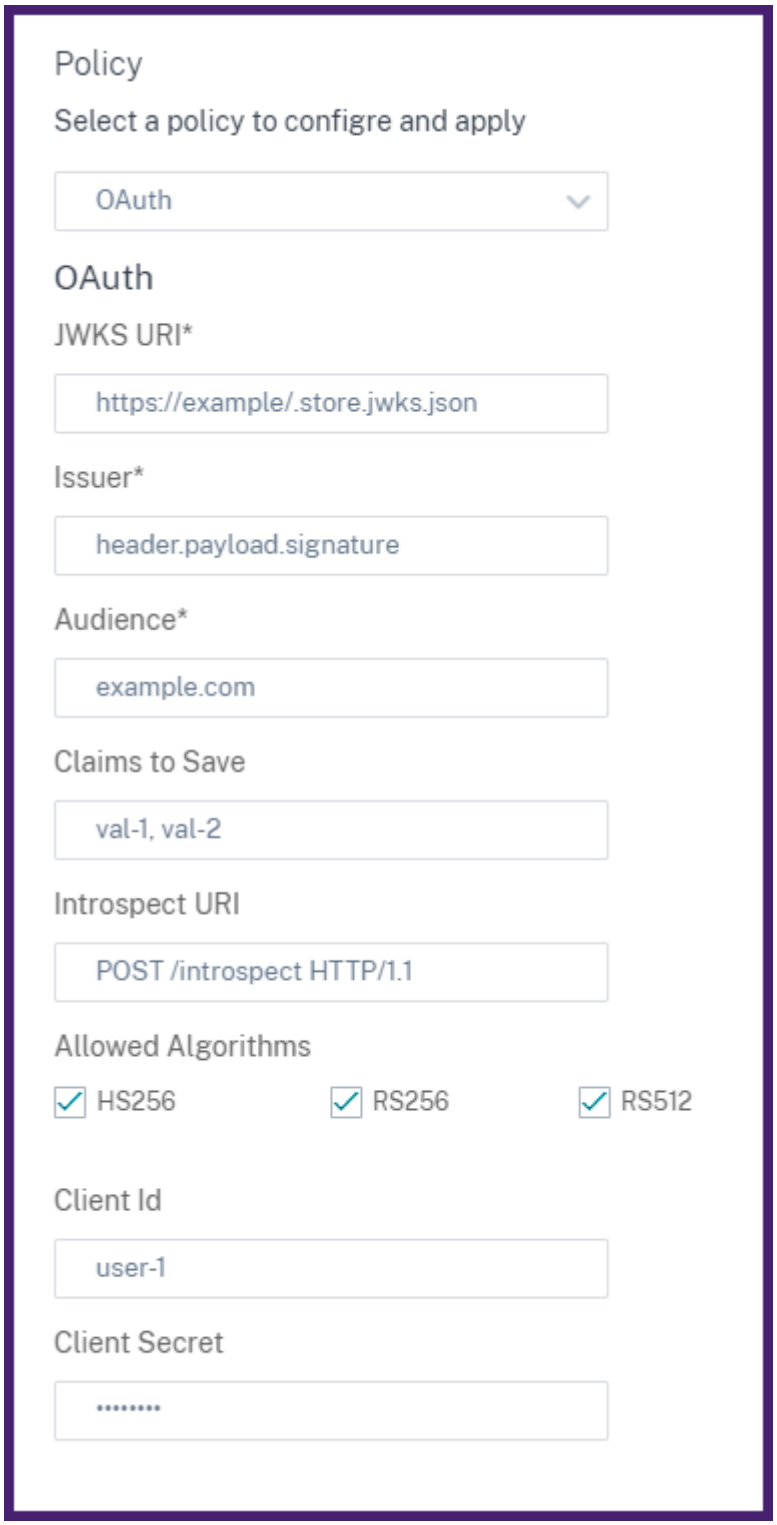
OAuth

OAuth erfordert, dass ein externer Identitätsanbieter einen Client mit OAuth2 authentifiziert und ein Zugriffstoken ausgibt. Wenn der Client dieses Token als Zugriffs-Berechtigung für ein API-Gateway bereitstellt, wird das Token basierend auf den konfigurierten Werten validiert.

- **JWKS URI** - Die URL eines Endpunkts mit JWKs (JSON Web Key) für JWT (JSON Web Token) Verifizierung
- **Aussteller** - Die Identität (normalerweise eine URL) des Authentifizierungsservers.
- **Zielgruppe** : Die Identität des Dienstes oder der Anwendung, für die das Token anwendbar ist.
- **Ansprüche auf Speichern** - Die Zugriffsberechtigungen werden als eine Reihe von Ansprüchen und erwarteten Werten dargestellt. Geben Sie die Anspruchswerte im CSV-Format an.
- **Introspect URI** - Eine Introspektions-Endpunkt-URL des Authentifizierungsservers. Diese URL wird verwendet, um undurchsichtige Zugriffstoken zu überprüfen. Weitere Informationen zu diesen Token finden Sie unter OAuth Konfiguration für undurchsichtige Zugriffstoken.

  Nachdem Sie **Introspect-URI**angegeben haben, geben Sie die **Client-ID** und den **Client Secret** für den Zugriff auf den Authentifizierungsserver an.

- **Zulässige Algorithmen** - Mit dieser Option können Sie bestimmte Algorithmen in den eingehenden Token einschränken. Standardmäßig sind alle unterstützten Methoden zulässig. Sie können jedoch die erforderlichen Algorithmen für den ausgewählten Datenverkehr überprüfen.



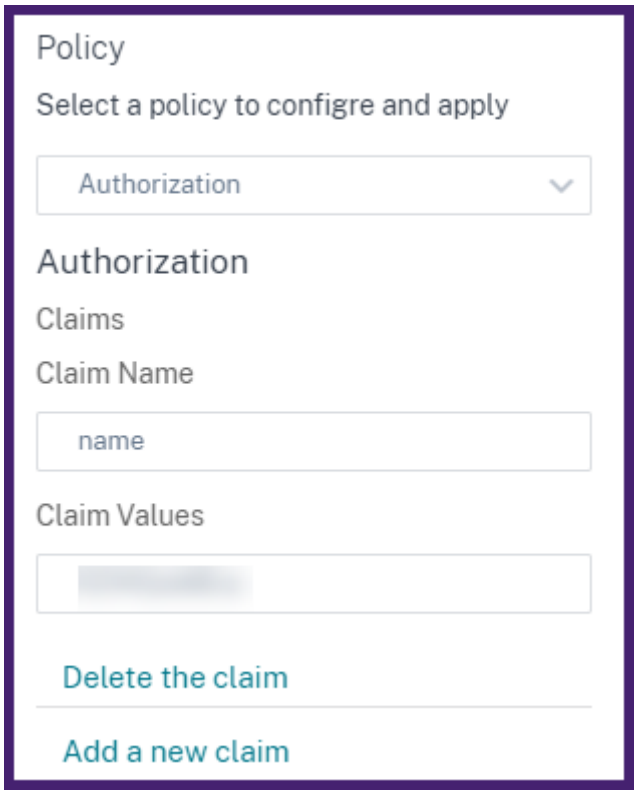
Bei erfolgreicher Validierung gewährt das API-Gateway dem Client Zugriff.

> **Wichtig**
>
> Wenn Sie eine OAuth oder **Auth-Grundlagen** Richtlinie für die ausgewählten API-Ressourcen konfigurieren, konfigurieren Sie die **Nein Auth** Richtlinie für die verbleibenden API-Ressourcen. Diese Konfiguration zeigt explizit an, dass Sie die Authentifizierung für die übrigen Ressourcen überspringen möchten.

Ermächtigung

Diese Richtlinie überprüft die erforderlichen Berechtigungen für den Zugriff auf eine API-Ressource. Die Zugriffsberechtigungen werden als eine Reihe von Ansprüchen und erwarteten Werten dargestellt. Um diese Richtlinie zu konfigurieren, wählen Sie **Neuen Anspruch hinzufügen** aus und geben Sie Folgendes an:

- Bezeichnung des Antrags
- Werte einfordern



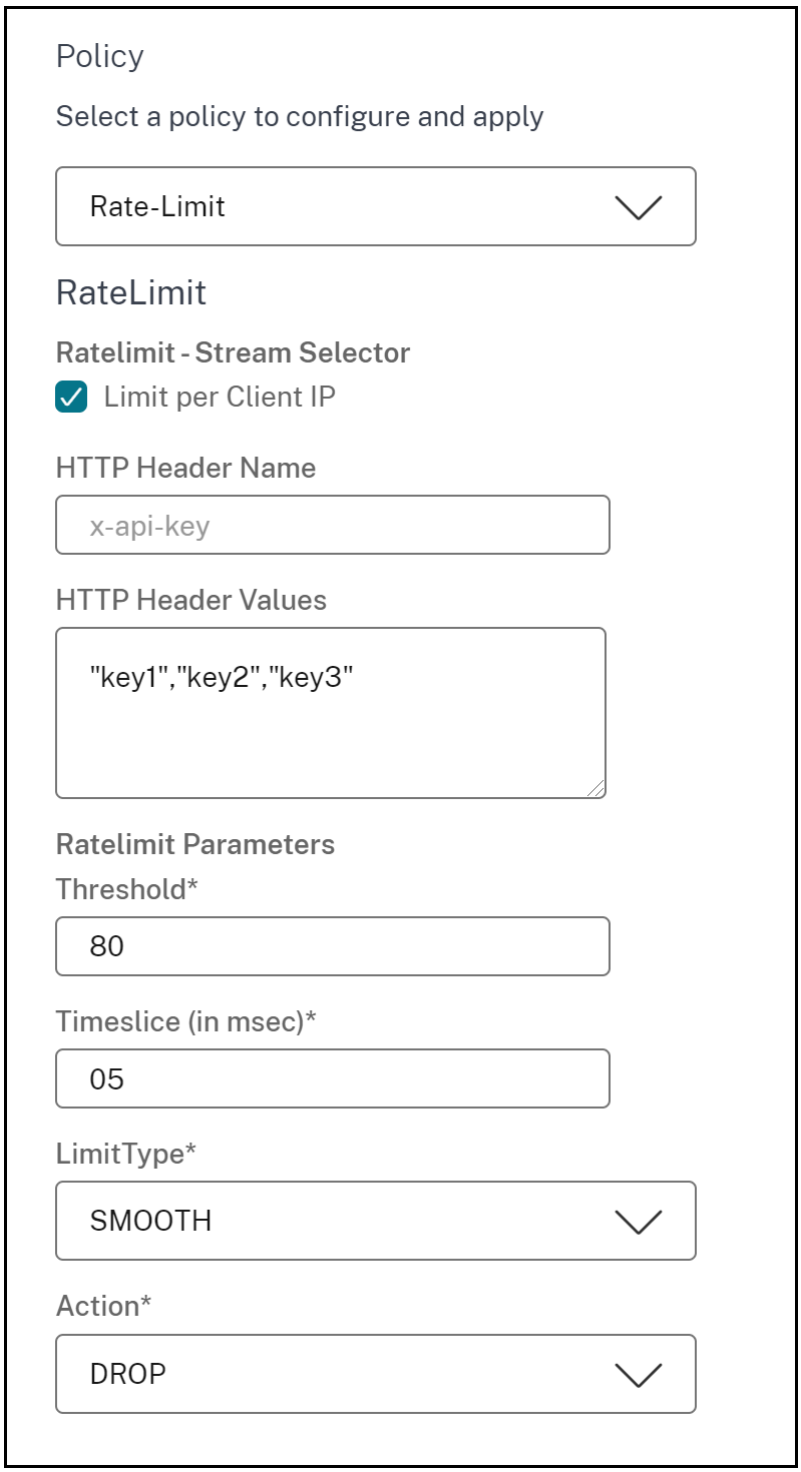
> **Wichtig**
>
> API-Gateway erfordert sowohl Authentifizierungs- als auch Autorisierungsrichtlinien für API-Datenverkehr. Daher müssen Sie eine Autorisierungsrichtlinie mit einer Authentifizierungsrichtlinie konfigurieren. Die Authentifizierungsrichtlinie kann OAuth oder [Auth-Basic](#auth-basic) sein.

> Selbst wenn Sie keine Berechtigungsprüfungen haben, müssen Sie eine Autorisierungsrichtlinie mit leeren Ansprüchen erstellen. Andernfalls wird die Anfrage mit einem 403-Fehler abgelehnt.

Rate Limit Richtlinie

Geben Sie die maximale Belastung an, die der ausgewählten API-Ressource zugewiesen wird. Mit dieser Richtlinie können Sie die API-Datenverkehrsrate überwachen und vorbeugende Maßnahmen ergreifen. Um diese Richtlinie zu konfigurieren, geben Sie Folgendes an:

- **HTTP-Header-Name** - Es ist ein Traffic-Selektorschlüssel, der den Datenverkehr filtert, um die API-Anfragen zu identifizieren. Und die Ratenlimit-Richtlinie gilt und überwacht nur solche API-Anfragen.
- **Schwellenwert** - Die maximale Anzahl von Anfragen, die im angegebenen Intervall zulässig sind.
- **Zeitscheibe** - Das in Mikrosekunden angegebene Intervall. Während dieses Intervalls werden die Anforderungen anhand der konfigurierten Limits überwacht. Standardmäßig ist er auf 1000 Mikrosekunden (1 Millisekunde) eingestellt.
- **Limit-Typ** - Der Modus, in dem Sie die Ratenlimit-Richtlinie anwenden möchten. Sie können den Grenztyp **Burst** oder **Smooth** auswählen.
- **Aktion** - Definiert eine Aktion, die Sie für den Traffic ausführen möchten, der den Schwellenwert überschreitet. Sie können eine der folgenden Aktionen festlegen:
  - **DROP**: Lässt die Anforderungen über die konfigurierten Verkehrsgrenzen hinaus.
  - **RESET**: Setzt die Verbindung für die Anfragen zurück.
  - **REDIRECT**: Leitet den Datenverkehr auf die konfigurierte redirect_url um.
  - **RESPOND**: Reagiert mit der Standardantwort (`429 Too many requests`).

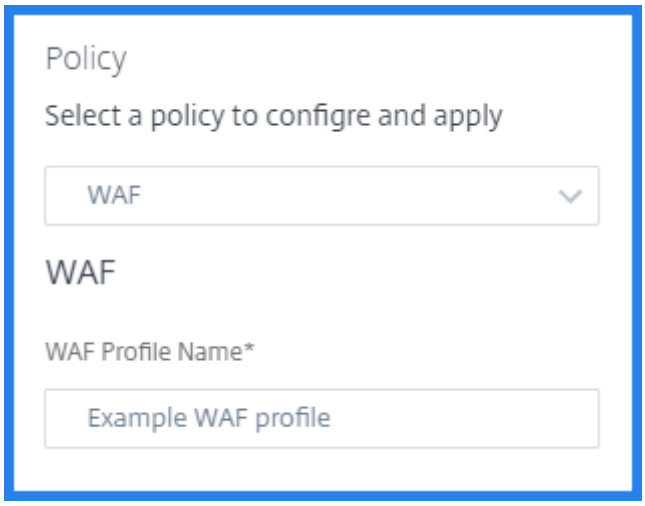


WAF-Richtlinie

Diese Richtlinie verhindert Sicherheitsverletzungen, Datenverlust und mögliche unbefugte Änderungen an Websites, die auf sensible Geschäfts- oder Kundeninformationen zugreifen.

Bevor Sie eine WAF-Richtlinie cofigurieren, erstellen Sie ein WAF-Profil in Citrix ADM verwenden Sie das StyleBook.

Wählen Sie in **WAF-Profilname**das von Ihnen erstellte WAF-Profil aus oder geben Sie es an.

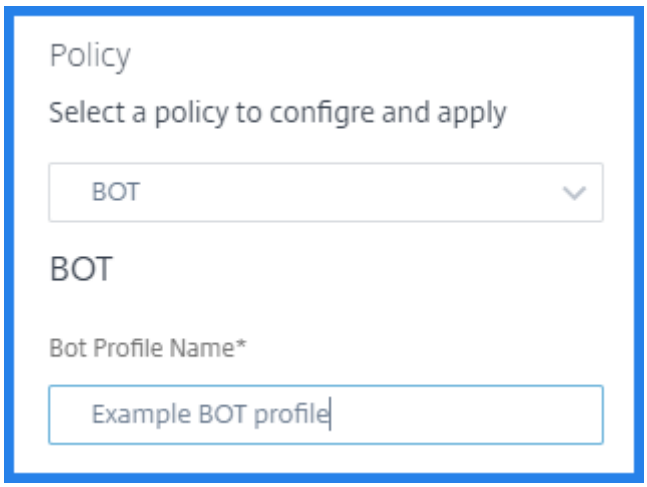


BOT-Richtlinie

Diese Richtlinie identifiziert schlechte Bots und schützt Ihre Appliance vor erweiterten Sicherheitsangriffen.

Bevor Sie eine BOT-Richtlinie konfigurieren, erstellen Sie ein BOT-Profil in Citrix ADM mit dem StyleBook.

Geben Sie unter **Bot-Profilname** das BOT-Profil an, das Sie erstellt haben.



Header Rewrite

Diese Richtlinie hilft Ihnen, den Header von API-Anfragen und -Antworten zu ändern. Wenn Sie den Wert im HTTP-Header ersetzen möchten, geben Sie Folgendes an:

- **HTTP-Header-Name**: Der abgerufene Name, den Sie im Anforderungsheader ändern möchten.

  Beispiel:`Host`

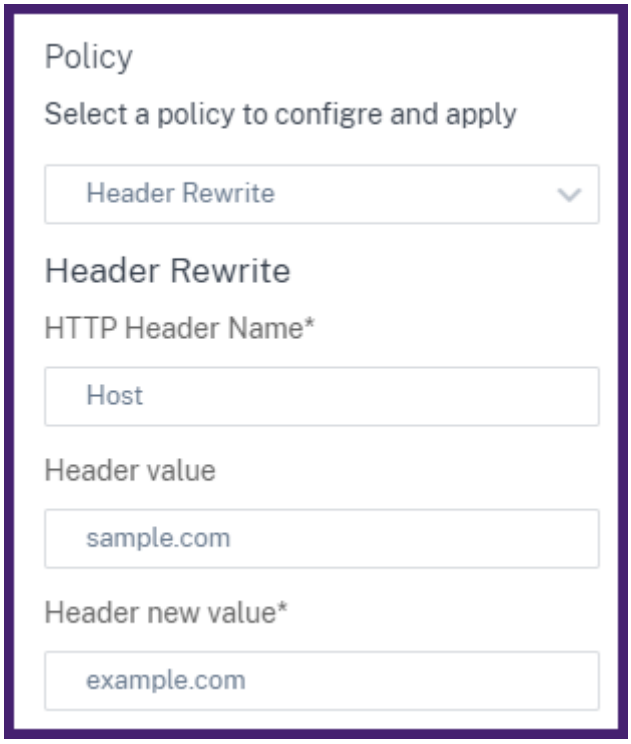
- **Header-Wert**: Optional ist die Wertzeichenfolge, die Sie im angegebenen Header-Namen ändern möchten.

  Beispiel:`sample.com`

- **Header neuer Wert**: Der neue Wert, der den angegebenen Header-Wert ersetzt.

  Wenn kein **Header-Wert** angegeben wird, ersetzt es jeden empfangenen Wert durch den angegebenen Wert für den **HTTP-Header-Namen**.

  Beispiel:`example.com`



In diesem Beispiel wird die Richtlinie `sample.com` zum Umschreiben von Kopfzeilen `example.com` im `Host` Feld einer API-Anforderung ersetzt.

Service-Diagramm

April 28, 2021

Mit der Service-Graph-Funktion in Citrix ADM können Sie alle Dienste in einer grafischen Darstellung überwachen. Mit dieser Funktion können Sie auch eine detaillierte Analyse und umsetzbare Metriken

der Services anzeigen. Navigieren Sie zu **Anwendungen > Servicegrafik**, um das Service-Diagramm anzuzeigen für:

- Für alle Citrix ADC-Instanzen konfigurierte Anwendungen
- Kubernetes Anwendungen
- 3-Tier-Webanwendungen

Dienstdiagramm für Anwendungen über alle Citrix ADC-Instanzen hinweg

Die globale Service-Graph-Funktion ermöglicht es Ihnen, eine ganzheitliche Visualisierung der Ansicht `clients to infrastructure to application`zu erhalten. In dieser Dienstdiagrammansicht mit einem einzigen Fensterbereich können Sie als Administrator folgende Möglichkeiten haben:

- Verstehen, aus welcher Region die Benutzer auf die spezifischen Anwendungen zugreifen (3-Tier-Web-Apps und Microservices-App)
- Visualisieren der Infrastrukturansicht (Citrix ADC-Instanz), dass die Clientanforderung verarbeitet wird
- Verstehen, ob die Probleme vom Client, der Infrastruktur oder der Anwendung auftreten
- Weitere Drilldown zur Behebung des Problems

Navigieren Sie zu **Anwendungen > Service Graph** und klicken Sie auf die Registerkarte **Global**, um Folgendes anzuzeigen:

- End-to-End-Details aller Anwendungen, die vom Client zu Back-End-Servern verbunden sind
- Alle Citrix ADC-Instanzen, die mit den jeweiligen Rechenzentren verbunden sind

  > **Hinweis**
  >
  > Sie können Rechenzentren nur anzeigen, wenn Sie GSLB-Apps haben.

- Informationen zu den Client-Metriken
- Die Citrix ADC Metrikinformationen
- Alle Citrix ADC-Instanzen mit diskreten Anwendungen, benutzerdefinierten Anwendungen und diskreten Microservice-Anwendungen
- Die 4 besten Anwendungen mit niedriger Punktzahl, die zu benutzerdefinierten Apps, diskreten Apps und Microservices-Apps gehören
- Die Metrikinformationen für die 4 besten virtuellen Server mit niedriger Punktzahl
- Der Status von Anwendungen (separate Apps, benutzerdefinierte Apps und Microservices-Apps), z. B. **Kritisch**, **Überprüfen**, **Gut** und **Nicht anwendbar**.

Weitere Informationen finden Sie unter Ganzheitliche Ansicht der Anwendungen im Service-Diagramm.

Service-Diagramm für Kubernetes-Anwendungen

Navigieren Sie zu **Anwendungen > Service Graph** und klicken Sie auf die Registerkarte **Microservices**, um Folgendes anzuzeigen:

- Sicherstellung der Gesamtleistung der Anwendung durch End-to-End-Anwendung
- Identifizieren von Engpässen, die durch die gegenseitige Abhängigkeit verschiedener Komponenten Ihrer Anwendungen entstehen
- Sammeln Sie Einblicke in die Abhängigkeiten verschiedener Komponenten Ihrer Anwendungen
- Überwachung von Diensten innerhalb des Kubernetes-Clusters
- Überwachen, welcher Dienst Probleme hat
- Überprüfen Sie die Faktoren, die zu Leistungsproblemen beitragen
- Detaillierte Sichtbarkeit von Service-HTTP-Transaktionen anzeigen
- Analysieren der HTTP-, TCP- und SSL-Metriken
- Anzeigen von Client-Metriken und zusammenfassenden Kundentransaktionen

Durch die Visualisierung dieser Metriken in Citrix ADM können Sie die Ursache von Problemen analysieren und die erforderlichen Fehlerbehebungsaktionen schneller durchführen. Dienstdiagramm zeigt Ihre Anwendungen in verschiedenen Komponentendiensten an. Diese Dienste, die innerhalb des Kubernetes-Clusters ausgeführt werden, können mit verschiedenen Komponenten innerhalb und außerhalb der Anwendung kommunizieren. Fangen Sie mit den Informationen unter Dienstdiagramm einrichten an.

Service-Diagramm für 3-Tier-Webanwendungen

Navigieren Sie zu **Anwendungen > Service Graph** und klicken Sie auf die Registerkarte **Web-Apps**, um Folgendes anzuzeigen:

- Details zur Konfiguration der Anwendung (mit dem virtueller Content Switching-Server und dem virtuellen Load Balancing-Server)

  Für GSLB-Anwendungen können Sie virtuelle Server für Rechenzentren, ADC-Instanzen, CS- und LB-Server anzeigen.
- End-to-End-Transaktionen vom Client zum Service
- Der Speicherort, von dem aus der Client auf die Anwendung zugreift
- Der Name des Rechenzentrums, in dem die Clientanforderungen verarbeitet werden, und die zugehörigen Citrix ADC Metriken des Rechenzentrums (nur für GSLB-Anwendungen)
- Metrikdetails für Client-, Dienst- und virtuelle Server

- Wenn die Fehler vom Client oder vom Dienst stammen
- Der Dienststatus, z. B. **Kritisch**, **Prüfen**und **Gut**. Citrix ADM zeigt den Dienststatus basierend auf der Reaktionszeit des Dienstes und der Fehleranzahl an.
  - **Kritisch (rot)** - Gibt an, wann durchschnittliche Service-Reaktionszeit > 200 ms UND Fehleranzahl > 0
  - **Überprüfung (orange)** - Gibt an, wann die durchschnittliche Service-Reaktionszeit > 200 ms ODER Fehleranzahl > 0
  - **Gut (grün)** - Zeigt keinen Fehler und durchschnittliche Service-Reaktionszeit < 200 ms
- Der Clientstatus, z. B. **Kritisch**, **Prüfen**und **Gut**. Citrix ADM zeigt den Clientstatus basierend auf Clientnetzwerklatenz und Fehleranzahl an.
  - **Kritisch (rot)**- Gibt an, wann die durchschnittliche Clientnetzwerklatenz > 200 ms UND Fehleranzahl > 0
  - **Überprüfung (orange)** - Gibt an, wann die durchschnittliche Clientnetzwerklatenz > 200 ms ODER Fehleranzahl > 0
  - **Gut (grün)** : Zeigt keinen Fehler und durchschnittliche Clientnetzwerklatenz < 200 ms an.
- Der Status des virtuellen Servers, z. B. **Kritisch**, **Prüfen**und **Gut**. Citrix ADM zeigt den Status des virtuellen Servers basierend auf der App-Bewertung an.
  - **Kritisch (rot)** — Zeigt an, wann die App-Bewertung < 40
  - **Review (orange)** - Zeigt an, wenn die App-Punktzahl zwischen 40 und 75 liegt.
  - **Gut (grün)** - Zeigt an, wenn die App-Punktzahl > 75 ist

Zu beachtenswerte Punkte:

- Nur virtuelle Server für Load Balancing, Content Switching und GSLB werden im Service-Diagramm angezeigt.
- Wenn kein virtueller Server an eine benutzerdefinierte Anwendung gebunden ist, sind die Details im Dienstdiagramm für die Anwendung nicht sichtbar.
- Sie können Metriken für Clients und Services nur dann im Dienstdiagramm anzeigen, wenn aktive Transaktionen zwischen virtuellen Servern und Webanwendung stattfinden.
- Wenn keine aktiven Transaktionen zwischen virtuellen Servern und Webanwendung verfügbar sind, können Sie nur Details im Dienstdiagramm anzeigen, die auf den Konfigurationsdaten wie virtuelle Server für Lastausgleich, Content Switching und GSLB sowie Dienste basieren.
- Wenn Änderungen in der Anwendungskonfiguration vorgenommen werden, kann es 10 Minuten dauern, bis sie im Service-Diagramm angezeigt werden.

Weitere Informationen finden Sie unter Service-Diagramm für Anwendungen.

Dienstdiagramm einrichten

April 28, 2021

Softwareanforderungen

Kubernetes Vertrieb	Kubernetes Version	Container-Netzwerkschnittstellen (CNI)	CPX-Version	CIC-Version	Citrix ADM Agent-Version
Open Source	v1.16.3	Flanell, Kattun oder Kanal	13.0—47.103 oder höher	1.6.1 oder höher	13.0—49.x oder höher

Sie können den Kubernetes-Cluster mit verschiedenen konfigurieren, Deployment-Topologien und die folgende Tabelle enthält die Topologien, die im Service-Graphen unterstützt werden:

Topologie	In Service Graph unterstützt
Single-Tier or Unified ingress	Ja
Zweistufig	Ja
Cloud	Ja, aber der Cloud-Load-Balancer wird im Diagramm nicht angezeigt
Service Mesh lite	Ja
Service-Mesh	Ja
Dienstleistungen des Typs LoadBalancer	Nein
Dienstleistungen des Typs NodePORT	Nein

Um das Setup-Dienstdiagramm in Citrix ADM abzuschließen, klicken Sie auf den Topologie-Typ, den Sie für Ihren Kubernetes-Cluster konfiguriert haben, und führen Sie die genannten Verfahren aus:

- Einstufige oder einheitliche Ingress-Topologie
- Dual-Tier- oder Service Mesh Lite Topologie
- Service-Mesh-Topologie

> **Hinweis**
>
> Das Verfahren zum Einrichten des Servicegraphen für Dual-Tier- und Service-Mesh-Topologien bleibt gleich.

Einstufige oder einheitliche Ingress-Topologie

Stellen Sie sicher, dass Sie die folgenden Schritte ausführen, um die Single-Tier- oder Unified Ingress-Topologie einzurichten. Weitere Informationen finden Sie unter Detaillierte Verfahren zur Einrichtung einer einstufigen oder einheitlichen Ingress-Topologie.

- Kubernetes-Cluster mit Single-Tier- oder einheitlicher Ingress-Topologie konfiguriert.
- VPX, MPX, SDX, BLX-Instanz in Citrix ADM hinzugefügt und **Web Insight**aktiviert.
- Kubernetes-Cluster In Citrix ADM hinzugefügt.

Dual-Tier- oder Service Mesh Lite Topologie

Stellen Sie sicher, dass Sie die folgenden Schritte ausführen, um die Dual-Tier- oder Service-Mesh-Topologie einzurichten. Weitere Informationen finden Sie unter Detaillierte Verfahren zur Einrichtung einer Dual-Tier- oder Service-Mesh-Topologie.

- Der Kubernetes-Cluster wurde mit einem der unterstützten Topologien konfiguriert.
- Installiert Citrix ADM Agent und konfiguriert, um die Kommunikation zwischen Citrix ADM und Kubernetes-Cluster oder verwalteten Instanzen in Ihrem Rechenzentrum oder Ihrer Cloud zu ermöglichen.

  Sie können einen Citrix ADM -Agent auch als Microservice bereitstellen. Weitere Informationen finden Sie im **Abschnitt Installieren von Citrix ADM Agent unter [Erste Schritte()]**.
- [Statische Routen()] Auf dem Citrix ADM Agent konfiguriert, um die Kommunikation zwischen Citrix ADM und Citrix ADC CPX zu aktivieren.

  > **Hinweis**
  >
  > Sie können dieses Verfahren ignorieren, wenn Sie Citrix ADM Agent als Microservice im selben Cluster bereitgestellt haben.
- [Beispiel-Bereitstellungsdateien()] Vom GitHub-Repository heruntergeladen.
- [Erforderliche Parameter()] In CPX YAML-Datei hinzugefügt, um eine erfolgreiche CPX-Registrierung bei Citrix ADM sicherzustellen.
- Ein VPX-, MPX-, SDX- oder BLX-Instanz in Citrix ADM wurde hinzugefügt.
- Das Kubernetes-Cluster in Citrix ADM wurde hinzugefügt.

- Bereitgestellt einer Beispiel-Microservice-Anwendung.
- Bereitgestellt Citrix ADC CPX und registrierte CPX zu ADM (nur für zweistufige Architektur anwendbar).
- Aktiviert Virtuelle Server automatisch auswählen, um die virtuellen CPX-Server zu lizenzieren.
- **In All** for Citrix ADM agent aktiviert Webtransaktions- und TCP-Transaktionseinstellungen, um HTTP- und TCP-Transaktionen abrufen zu können.
- Gesendet Verkehr an Microservices.

Service-Mesh-Topologie

Stellen Sie sicher, dass Sie die folgenden Schritte ausführen, um die Service-Mesh-Topologie einzurichten. Weitere Informationen finden Sie unter Detaillierte Verfahren zum Einrichten der Service-Mesh-Topologie.

- Die Kubernetes-Clusterversion wurde `1.14.0` mit einer der folgenden Service-Mesh-Topologien konfiguriert:
  - Citrix ADC CPX als Sidecar-Proxy für Istio
  - Citrix ADC als Ingress-Gateway für Istio

  Weitere Informationen finden Sie unter Bereitstellungsarchitektur von Citrix ADC Istio Adapter
- `admissionregistration.k8s.io/v1beta1` API aktiviert. Sie können die API überprüfen, indem Sie Folgendes verwenden:

  ```
  kubectl api-versions | grep admissionregistration.k8s.io/v1beta1
  ```

  Die folgende Ausgabe zeigt an, dass die API aktiviert ist:

  ```
  admissionregistration.k8s.io/v1beta1
  ```
- Istio installiert `istio v.1.3.0`.
- Helm Version 3.xInstalliert
- Installiert Citrix ADM Agent und konfiguriert, um die Kommunikation zwischen Citrix ADM und Kubernetes-Cluster oder verwalteten Instanzen in Ihrem Rechenzentrum oder Ihrer Cloud zu ermöglichen.

  Sie können einen Citrix ADM -Agent auch als Microservice bereitstellen. Weitere Informationen finden Sie im **Abschnitt Installieren von Citrix ADM Agent unter [Erste Schritte()]**.
- [Statische Routen()] Auf dem Citrix ADM Agent konfiguriert, um die Kommunikation zwischen Citrix ADM und Citrix ADC CPX zu aktivieren.

> **Hinweis**
>
> Sie können dieses Verfahren ignorieren, wenn Sie Citrix ADM Agent als Microservice im selben Cluster bereitgestellt haben.

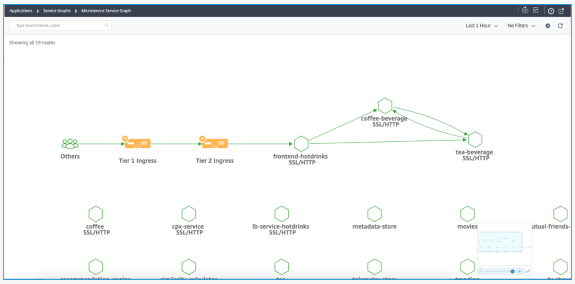
- Der wurde so konfiguriert Erforderliche Parameter, dass die Service-Mesh-Topologiedaten gefüllt werden.
- Bereitgestellt einer Beispiel-Anwendung.
- Das Kubernetes-Cluster in Citrix ADM wurde hinzugefügt.
- Aktiviert Virtuelle Server automatisch auswählen, um die virtuellen Server zu lizenzieren.
- **In All** for Citrix ADM agent aktiviert Webtransaktions- und TCP-Transaktionseinstellungen, um HTTP- und TCP-Transaktionen abrufen zu können.
- Gesendet Verkehr an Microservices.

Nachdem Sie die erforderlichen Einrichtungsverfahren abgeschlossen haben, können Sie das Servicediagramm anzeigen, das unter **Anwendungen** > **Service Graph** und auf der Registerkarte **Microservices** ausgefüllt ist. Weitere Informationen finden Sie unter Details zum Service-Diagramm.

Details im Service-Diagramm anzeigen

April 28, 2021

Nachdem Sie den Kubernetes-Cluster in Citrix ADM hinzugefügt haben, dauert es ungefähr 10 Minuten, bis die Daten im Service-Graphen ausgefüllt werden. Navigieren Sie zu **Anwendung** > **Service Graph**, und klicken Sie auf die Registerkarte **Microservices**, um die Details des Servicediagramms anzuzeigen

Mesh Lite Topologie mit zwei Tieren/Service	Single-Tier-/Unified Ingress-Topologie
	

- **Tier 1-Eintritt** — Citrix Ingress Controller innerhalb des Kubernetes-Clusters konfiguriert eine Citrix ADC-Instanz (VPX/MPX/SDX/BLX) außerhalb des Kubernetes-Clusters.
- **Tier 2 Ingress** — Citrix Ingress Controller läuft zusammen mit der Citrix ADC CPX-Instanz im

Kubernetes-Cluster als Sidecar.

- **Ingress** — Wird für alle anderen Bereitstellungstopologien angezeigt.

Service-Diagramm-Dashboard

1 - End-to-End-Netzwerkkarte Ihrer Anwendung, die zeigt, wie Ihre Komponentendienste kommunizieren

2 — Diagramm, das Treffer und Fehler für eine bestimmte Zeitdauer anzeigt

3 — Suchleiste für die Suche nach Diensten

4 — Zeitliste zur Auswahl der Zeitdauer

5 - Anwenden von Filtern für Anzeigedienste

6 — Einstellungssymbol

7 — Ansicht vergrößern und verkleinern

8 — Diagrammansicht oder tabellarische Ansicht

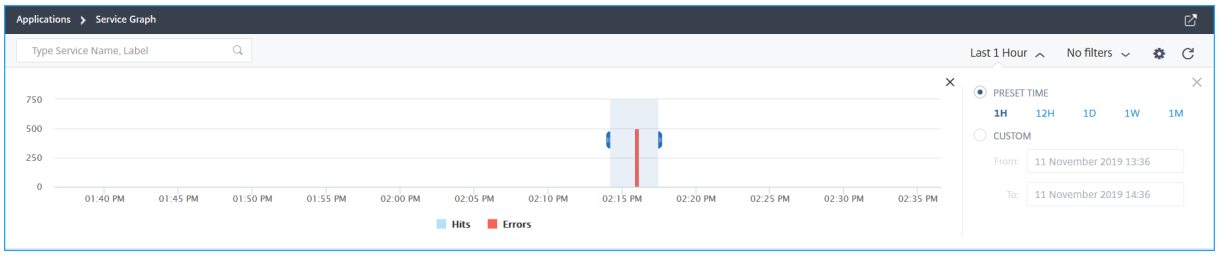
Basierend auf der gewählten Zeitdauer können Sie das Service-Diagramm anzeigen.

Service-Symbol	Beschreibung
	Die Kantenbreite gibt die Anzahl der Treffer an. Je größer oder mehr die Kantenbreite ist, gibt an, dass die Anzahl der Treffer höher ist.

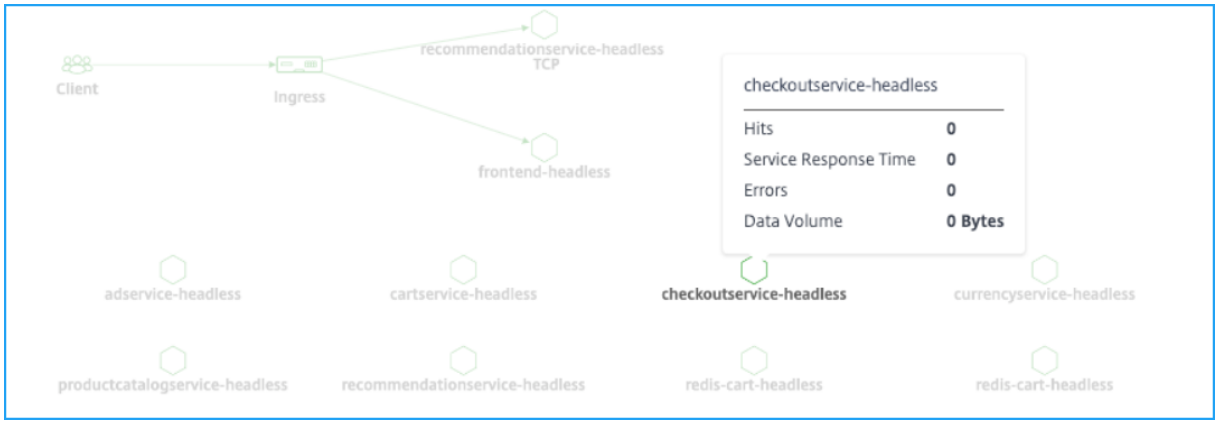
Service-Symbol	Beschreibung
	Der Dienst mit einem Warnsymbol zeigt an, dass der Dienst Fehler enthält.
	Der Dienst mit einem Stoppuhrsymbol zeigt an, dass der Dienst Latenz- oder Reaktionszeitprobleme aufweist.
	Der Dienst mit Stoppuhr- und Warnsymbolen weist darauf hin, dass der Dienst sowohl Fehler als auch Probleme mit Latenz-/Reaktionszeiten hat.

> **Hinweis**
>
> Wenn ein Dienst kein Warn- oder Stoppuhrsymbol hat, zeigt dies an, dass der Dienst Anomalien oder Schwellenwertverletzungen für Hits aufweist.

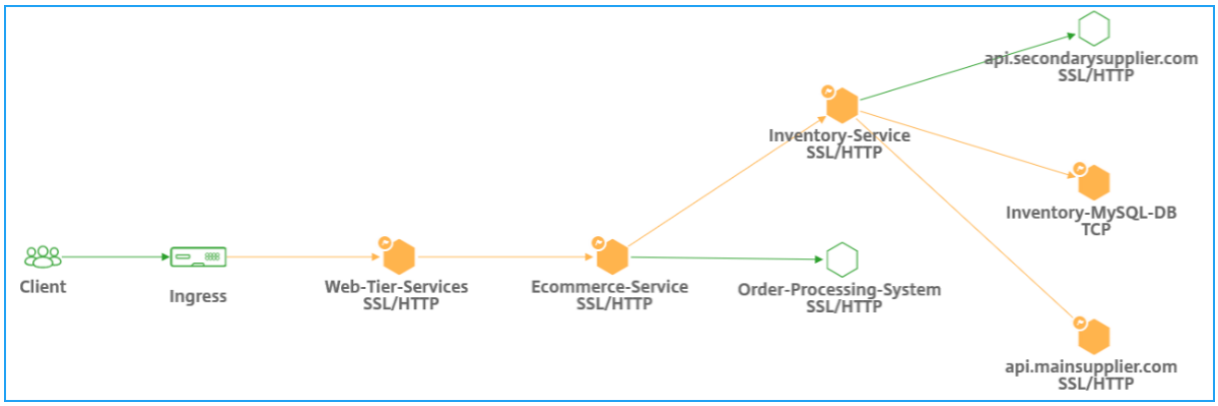
Wählen Sie den Zeitraum aus dem Diagramm aus, der Treffer anzeigt, um weitere Informationen zu erhalten.



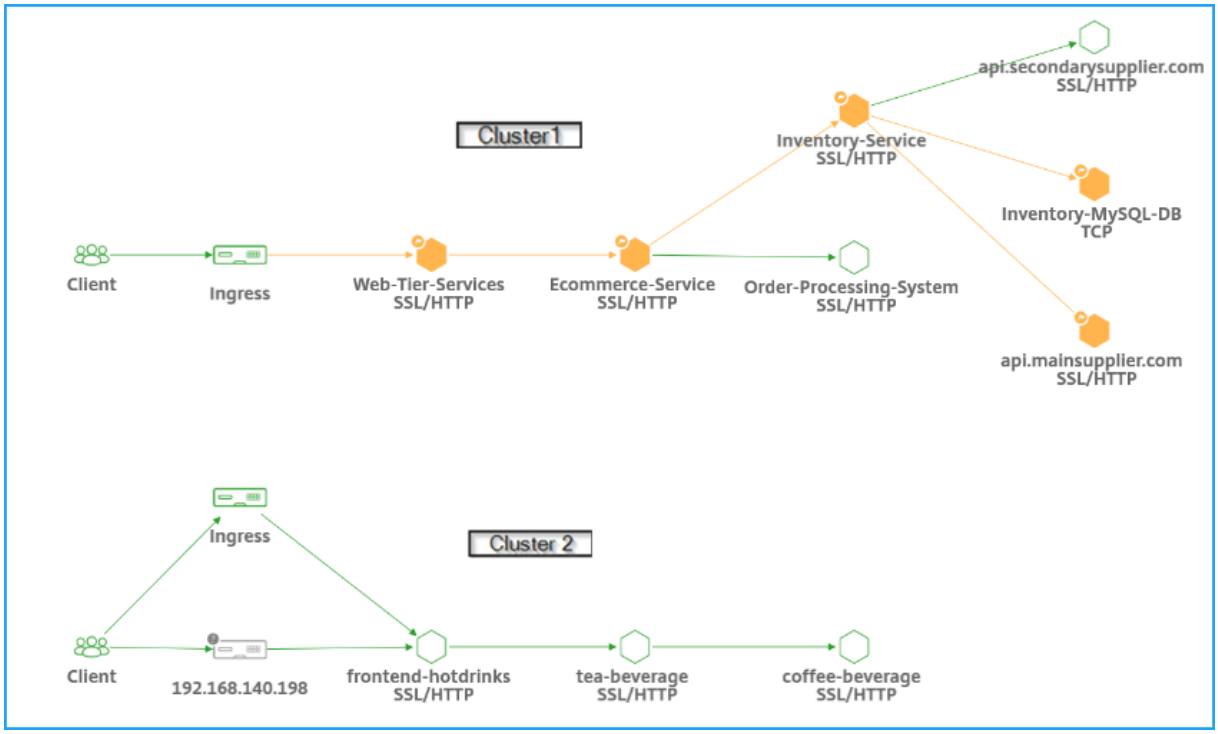
> **Hinweis**
>
> Wenn keine aktiven Transaktionen von Citrix ADM empfangen werden, können Sie nur die Services anzeigen, die von der Citrix ADC-Instanz mit Lastenausgleich ausgeglichen werden. Wenn Sie den Mauszeiger auf einen Dienst bewegen, werden alle Metriken als 0 angezeigt.



Das Dienstdiagramm wird nun mit dem Protokoll angezeigt, das von den Diensten verwendet wird. Beachten Sie, dass in Ihrem Kubernetes-Cluster die folgenden Dienste ausgeführt werden, wie im Bild gezeigt:



> **Hinweis**
>
> Wenn Sie unter “ **Orchestration** “ > “ **Kubernetes** “ > “Cluster” mehrere **Cluster**hinzugefügt haben, können Sie Services anzeigen, die jedem Cluster zugeordnet sind.



Sie können den folgenden Status für Ihre Dienste anzeigen:

- **Kritisch (rot)** - Service hat Anomalien oder Schwellenwertverletzungen in mehreren Metriken. Für die Standardschwellenwerte zeigt der kritische Status die durchschnittliche Serviceantwortzeit > 200 ms UND die Fehleranzahl > 0 an
- **Review (orange)** - Der Dienst hat Anomalien oder Schwellenwertverletzungen in einer der Metriken. Für die Standardschwellenwerte zeigt der Status Überprüfen die durchschnittliche Serviceantwortzeit an > 200 ms ODER Fehleranzahl > 0
- **Gut (grün)** - Service ohne Anomalien oder ohne Schwellenverletzung. Für die Standardschwellenwerte zeigt der Status “Gut” keinen Fehler und keine durchschnittliche Serviceantwortzeit von < 200 ms an

  Weitere Informationen zu Anomalien finden Sie unter Überwachen Sie Dienste mithilfe der Golden Signal-Metriken.

  Weitere Informationen zu Schwellenwerten finden Sie unter Konfigurieren von Schwellenwerten im Dienstdiagramm.

Im Folgenden finden Sie Protokolle, mit denen Sie das Protokoll identifizieren können, das von einem Dienst verwendet wird:

- **TCP** — Gibt an, dass der Dienst das TCP-Protokoll verwendet.
- **SSL, HTTP** — Gibt an, dass der Dienst das SSL-über-HTTP-Protokoll verwendet.
- **SSL, TCP** — Gibt an, dass der Dienst das SSL-über-TCP-Protokoll verwendet.

> **Hinweis**
>
> Der Dienst ohne Protokoll gibt an, dass der Dienst das HTTP-Protokoll verwendet.

Anzeigen wichtiger Metrikentrends mithilfe der tabellarischen Ansicht

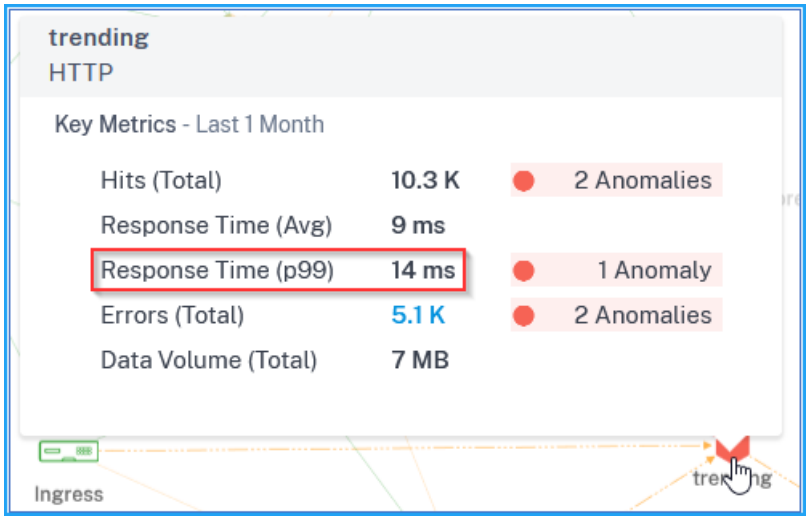
Anhand der tabellarischen Ansicht können Sie Folgendes sehen:

- Die wichtigsten Kennzahlen für den Dienst
- Wichtige Metriken zwischen einem Quelldienst und einem Zieldienst

Als Administrator können Sie mithilfe dieser wichtigen Metriken die Trends der goldenen Signale für die ausgewählte Zeitdauer analysieren. Weitere Informationen finden Sie unter Service-Details anzeigen.

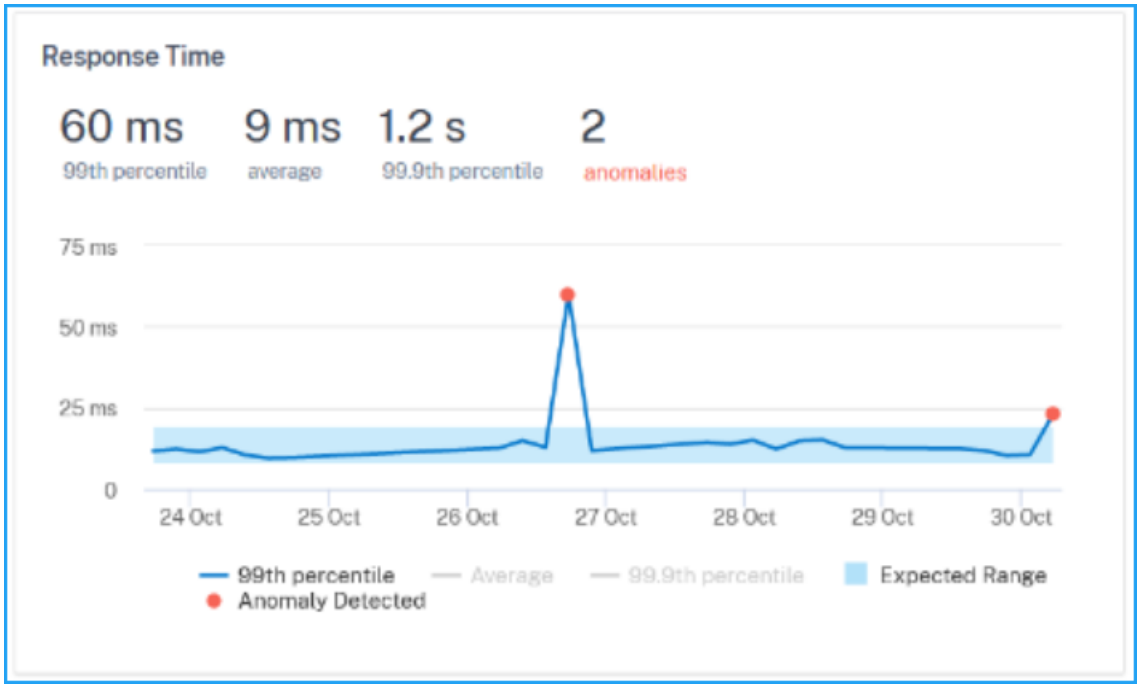
Pxx-Wert für die Reaktionszeit des Dienstes anzeigen

Zeigen Sie mit der Maus auf einen Dienst, um den Pxx-Wert für die Reaktionszeit anzuzeigen.



Reaktionszeit (P99) — Gibt an, dass die 99% der Anforderungen für die ausgewählte Dauer kleiner als der P99-Wert sind.

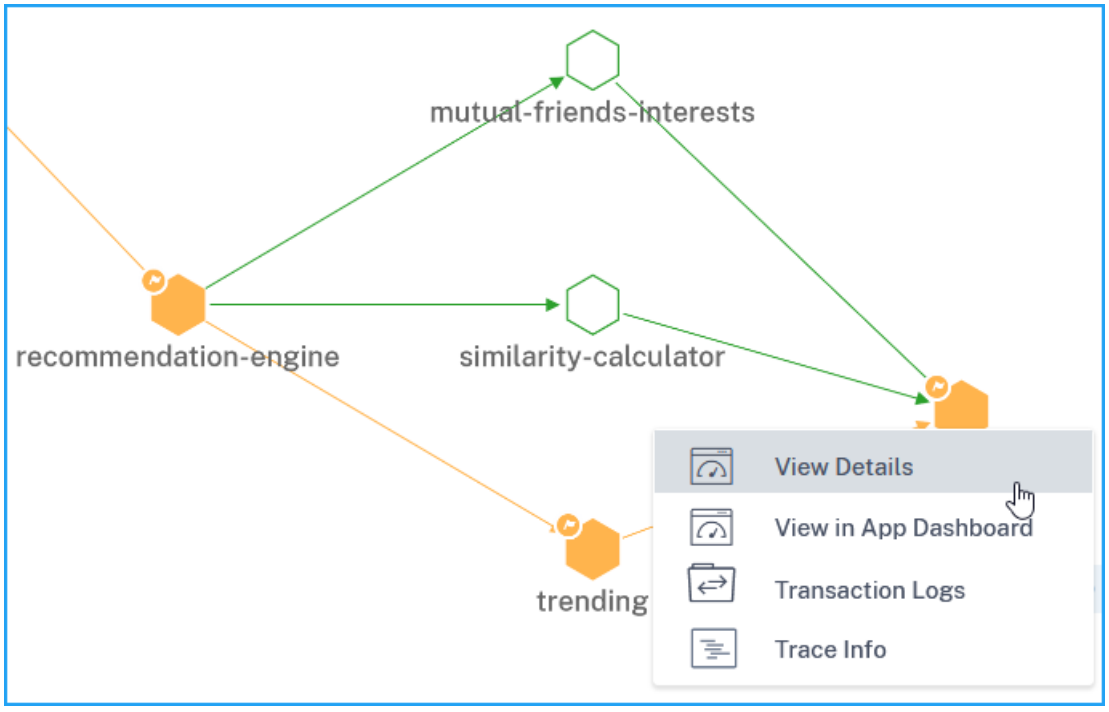
Wenn Sie einen Drilldown zur Anzeige der Servicedetails anzeigen, können Sie auch das 99-te Perzentil und das 99,9. Perzentil der Reaktionszeit für die ausgewählte Dauer anzeigen.



Als Administrator können Sie mithilfe des pxx-Werts die Service-Reaktionszeit besser verstehen. Weitere Informationen finden Sie unter Service-Details anzeigen.

Service-Details anzeigen

Klicken Sie auf einen Dienst, um die folgenden Optionen anzuzeigen:

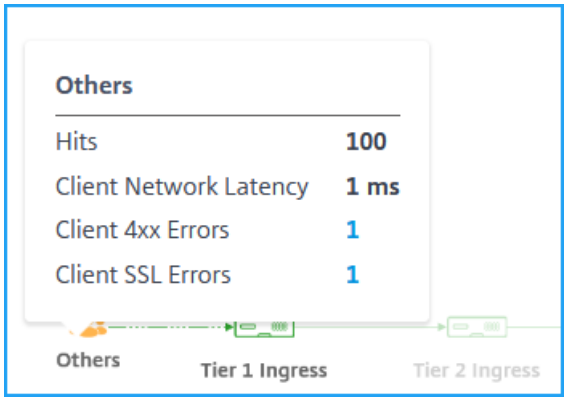


- **Details anzeigen** - Ermöglicht es Ihnen, die Dienstdetails wie Namespace, Labels, Cluster, in dem der Dienst gehostet wird, usw. anzuzeigen. Weitere Informationen finden Sie unter Service-Details anzeigen.
- **Im App-Dashboard** anzeigen - Ermöglicht es Ihnen, die ausgewählten Anwendungsdetails wie App-Score, Kubernetes-Dienstdetails, Pod-Details usw. anzuzeigen. Weitere Informationen finden Sie unter Details zur Kubernetes-Anwendung
- **Transaktionsprotokolle** - Ermöglicht das Anzeigen der HTTP- und SSL-über-HTTP-Transaktionsdetails. Weitere Informationen finden Sie unter Anzeigen von Analysen für Web-Transaktionen.
- **Trace-Info** - Ermöglicht Ihnen, das verteilte Tracing des Service anzuzeigen. Weitere Informationen finden Sie unter Verteilte Ablaufverfolgung.

Client-Metriken anzeigen

Sie können sehen, von welchem Standort der Client auf den Dienst zugreift. Als Administrator können Sie die Client-Metriken visualisieren und die Probleme analysieren, die vom Kunden auftreten.

Bewegen Sie den Mauszeiger auf eine Client-Region, um die Metriken anzuzeigen.



- **Treffer** - Gibt die Gesamtzahl der Treffer an, die der Kunde erhalten hat.
- **Client-Netzwerklatenz** : Gibt die durchschnittliche Clientnetzwerklatenz an.
- **Client 4xx Fehler** - Gibt die Gesamtzahl der 4xx Client-Fehler an.
- **Client-SSL-Fehler** - Gibt die gesamte Client-SSL-Fehler an.

IP-Blöcke in Citrix ADM - Citrix ADM kann den Standort des Clients erkennen, wenn der Client eine öffentliche IP-Adresse verwendet. Citrix ADM verfügt über eine integrierte CSV-Datei, die dem Speicherort basierend auf dem Client-IP-Adressbereich entspricht.

Citrix ADM kann den Clientstandort mit privater IP-Adresse nur erkennen, wenn die IP-Adresse zum Citrix ADM-Server hinzugefügt wird. Wenn die Client-IP-Adresse beispielsweise in einen privaten IP-Adressbereich fällt, der mit Stadt A verknüpft ist, erkennt Citrix ADM, dass der Datenverkehr für diesen Client aus Stadt A stammt.

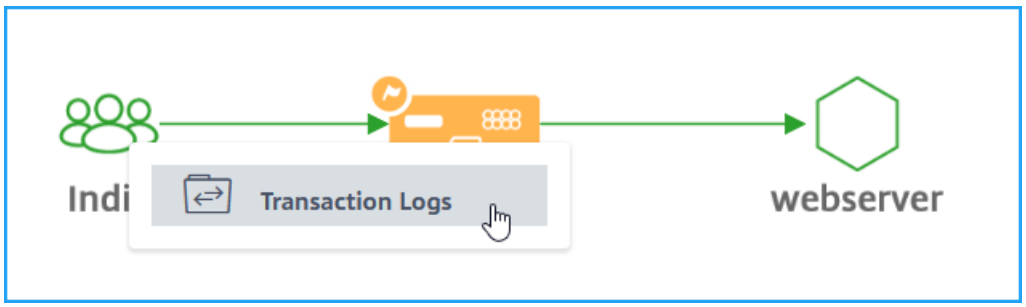
Weitere Informationen finden Sie unter Erstellen eines privaten IP-Blocks.

Zusammenfassung der Client-Transaktion

Die detaillierte Zusammenfassung der Clienttransaktion ermöglicht es Ihnen, Folgendes anzuzeigen:

- Reaktionszeit > 500 ms
- 5xx Fehler

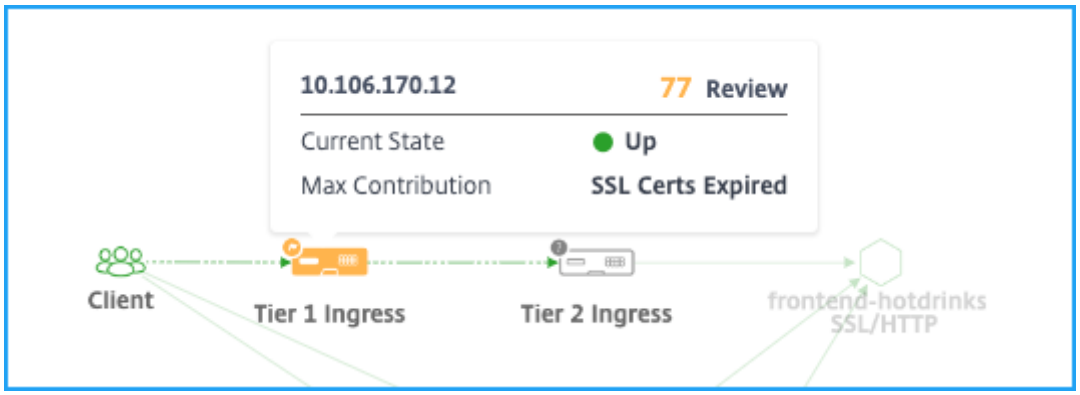
Klicken Sie auf einen Kundenstandort und wählen Sie **Transaktionslogs**.



Weitere Informationen finden Sie unter Web-Transaktionsanalyse.

Anzeigen von Ingress-Metriken

Sie können die Art von Ingress anzeigen, die im Kubernetes-Cluster verwendet wird.



- Citrix ADC IP-Adresse und seine Punktzahl
- **Aktueller Status** — Gibt an, ob die Citrix ADC-Instanz Up, Down oder Out of Status ist
- **Maximaler Beitrag** — Zeigt das Problem an, das den Instanz-Score beeinflusst

Für die einstufige Topologie können Sie nur einen einzelnen **Ingress**anzeigen.

Klicken Sie auf den **Ingress**, um weitere Informationen zu erhalten. Weitere Informationen finden Sie unter Anzeigen von Ingress-Details zur Problembehandlung.

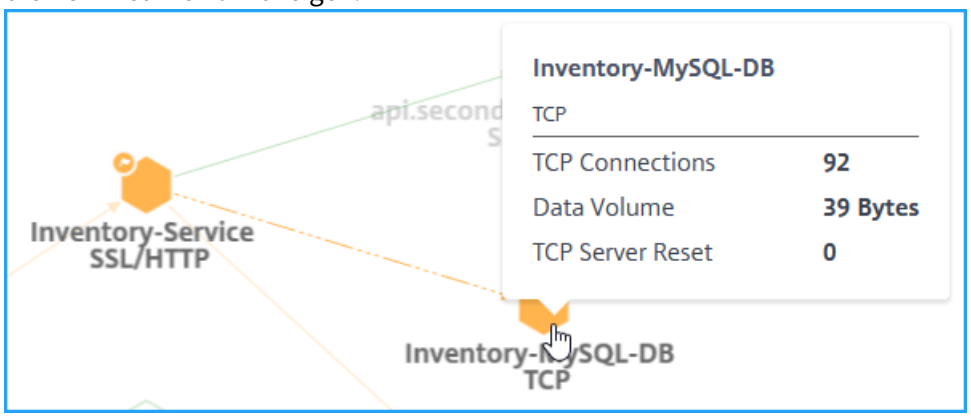
Anzeigen von TCP- und SSL-Metriken

Mit den TCP- und SSL-Metriken können Sie:

- TCP-Verbindungsdetails zwischen Diensten anzeigen
- Bestimmen Sie, ob TCP-bezogene Probleme vom Quell- oder Zieldienst stammen
- Anzeigen, ob der SSL-Fehler vom Quell- oder Zieldienst stammt
- Anzeigen der SSL-Protokollversion, die von SSL-Diensten verwendet wird

TCP-Metriken

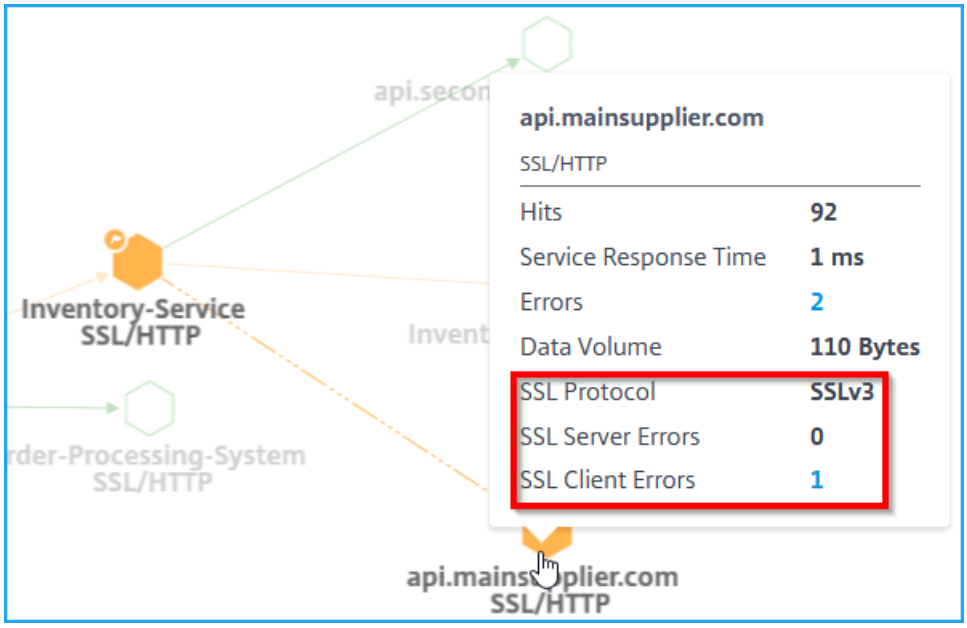
Bewegen Sie den Mauszeiger über einen TCP-Dienst oder den zugehörigen eingehenden Dienst, um die TCP-Metriken anzuzeigen.



- **TCP-Verbindungen** — Gesamtzahl der zwischen den Diensten aufgebauten Verbindungen
- **Datenvolumen** — Gesamtmenge der vom Dienst verarbeiteten Daten
- **TCP-Server-Reset** — Gesamt vom Server initiierte TCP-Resets

SSL-Metriken

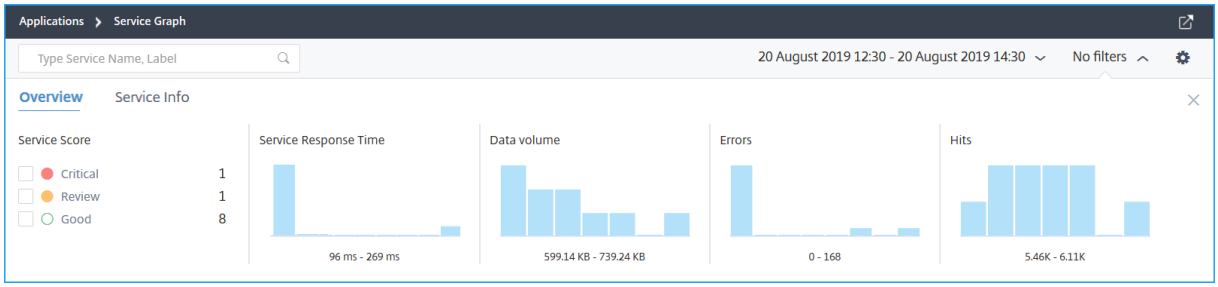
Bewegen Sie den Mauszeiger auf einen Dienst, der SSL-Protokoll verwendet, um die SSL-Metriken anzuzeigen.



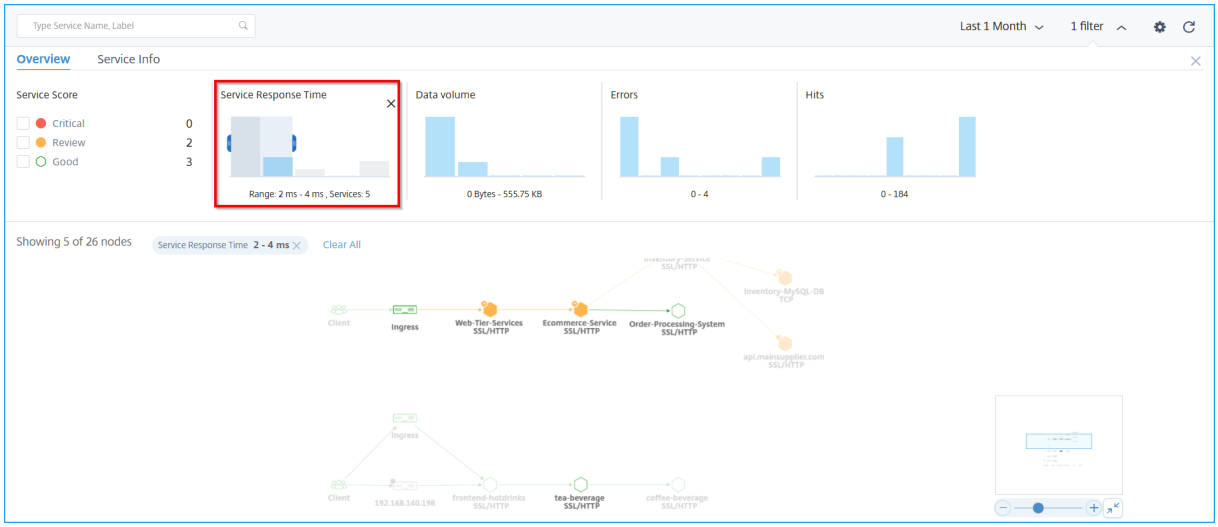
- **SSL-Serverfehler** — Gibt die gesamten SSL-Fehler vom Server an. (Beispiel: SSL-Zertifikat unbekannt)
- **SSL-Protokoll** — Gibt die SSL-Protokollversion an, die vom Dienst verwendet wird.
- **SSL-Client-Fehler** - Geben Sie die gesamten SSL-Fehler vom Client an. (Beispiel: SSL-Clientauthentifizierungsfehler)

Filter anwenden

Sie können Filter anwenden, um bestimmte Dienstinformationen anzuzeigen. Klicken Sie auf **Keine Filter** Liste, um die Filteroptionen abzurufen.

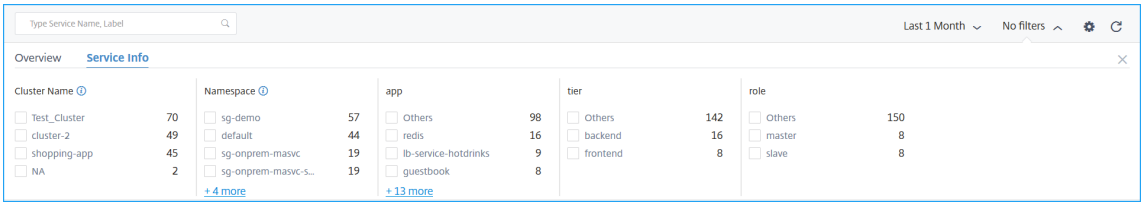


Wenn Sie z. B. Dienste mit einer Latenz von weniger als 150 ms anzeigen möchten, klicken Sie auf das Balkendiagramm unter **Dienstantwortzeit**, um die Ergebnisse anzuzeigen.



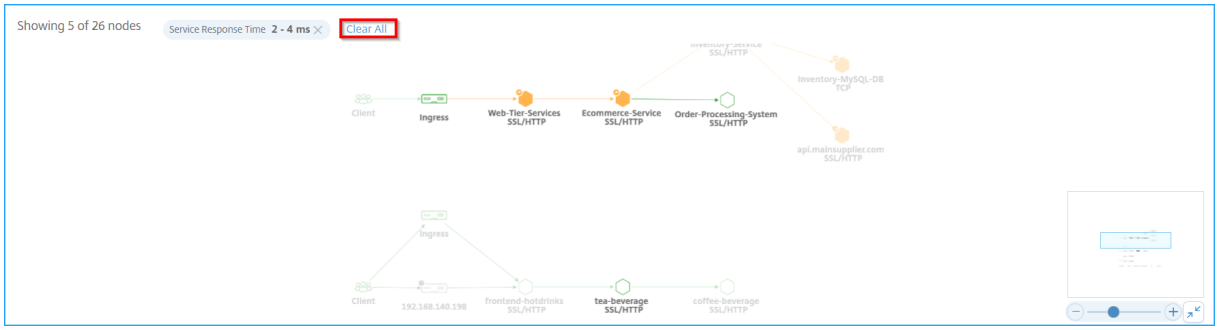
Klicken Sie auf **Service-Info**, um Filter auszuwählen und anzuwenden für:

- **Cluster** — Zeigt alle Dienste an, die für den ausgewählten Cluster oder die ausgewählten Cluster gelten.
- **Namespace** — Zeigt alle Dienste an, die für den ausgewählten Namespace gelten.

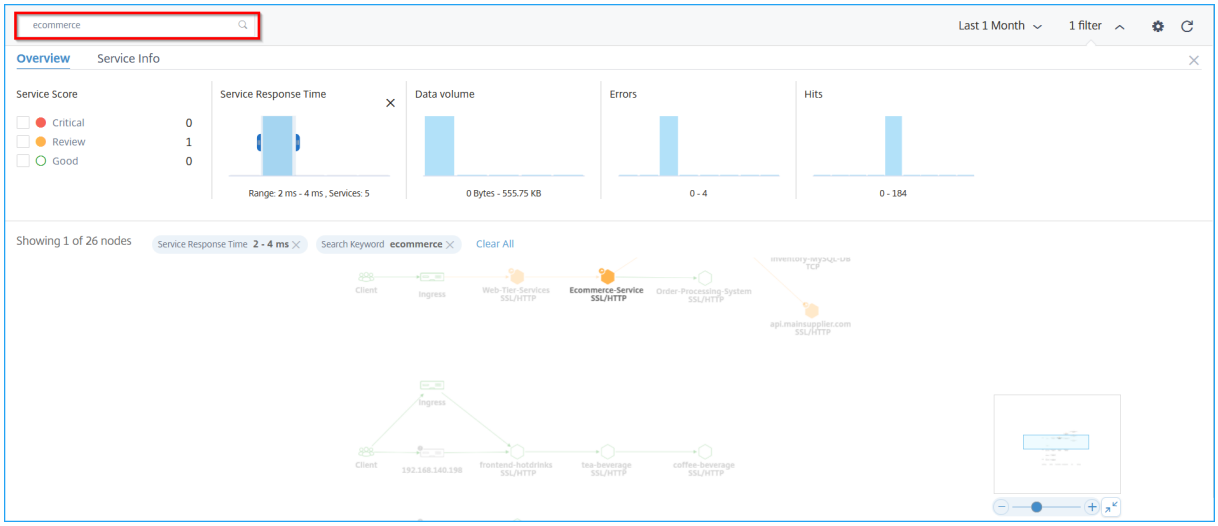


> Hinweis
>
> Abhängig von den in der Kubernetes Service-Definition YAML für den Dienst konfigurierten Labels können Sie auch weitere Filteroptionen anzeigen.

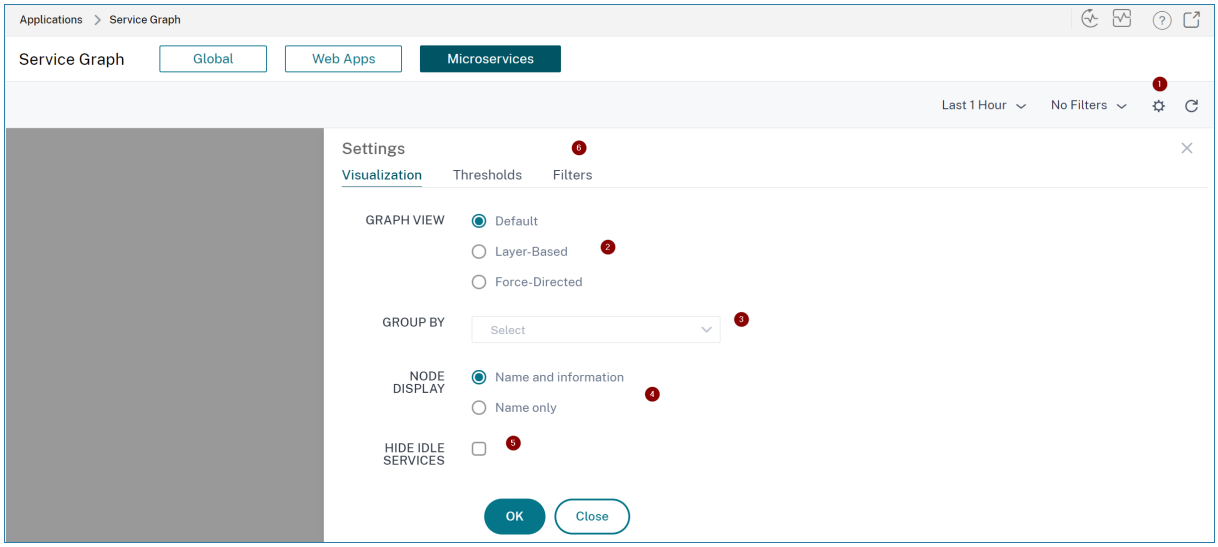
Klicken Sie auf **Alle löschen**, um alle Filter zu löschen.



Alternativ können Sie auch das Suchtextfeld verwenden und einen Dienstnamen eingeben, um die Ergebnisse im Dienstdiagramm anzuzeigen.



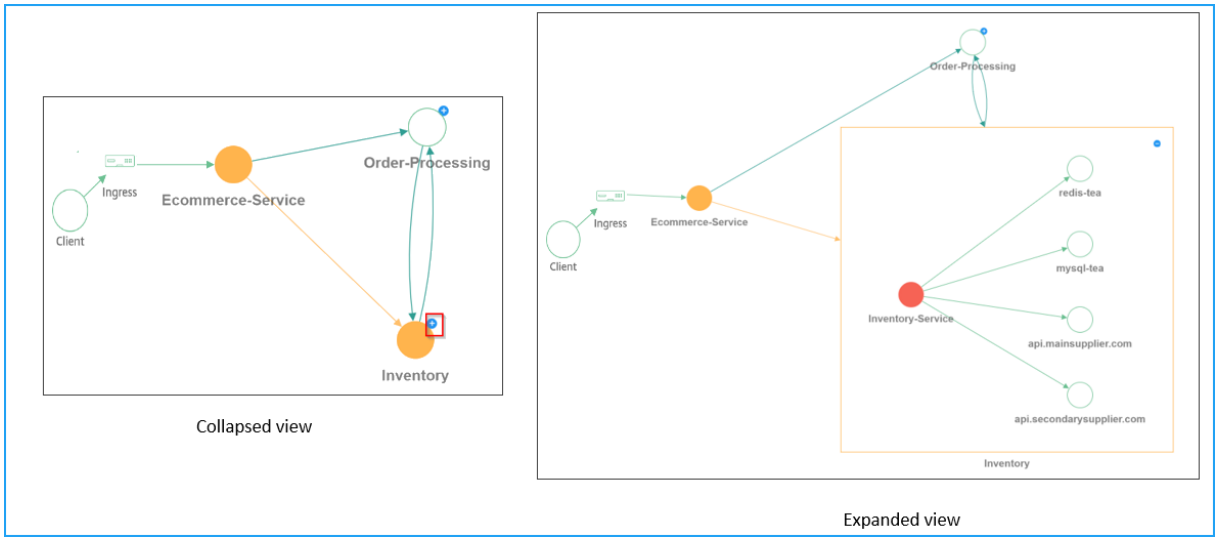
Verwenden der Option “Einstellungen”



1 — Symbol Einstellungen

2 — Optionen zum Anzeigen des Service-Graphen als Standardansicht, ebenenbasierte oder erzwungene Ansichten

3 — Wählen Sie die Optionen aus der Liste aus, um die Services basierend auf Kategorien anzuzeigen. Nachdem Sie eine Kategorie aus der Liste ausgewählt haben, klicken Sie auf **+** in der Grafik, um alle Dienste anzuzeigen.

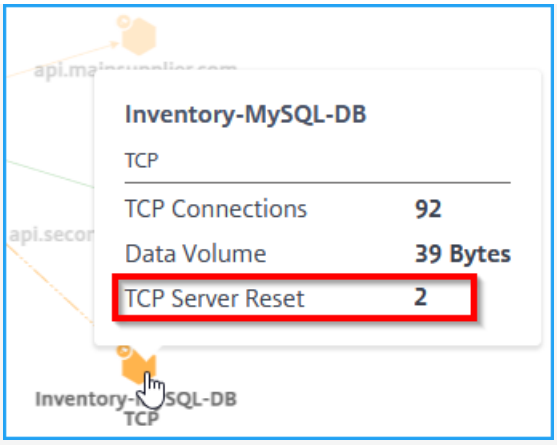


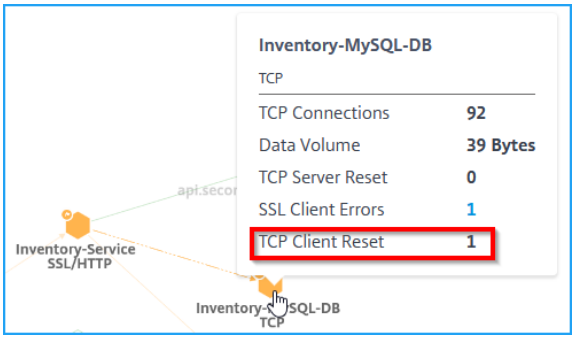
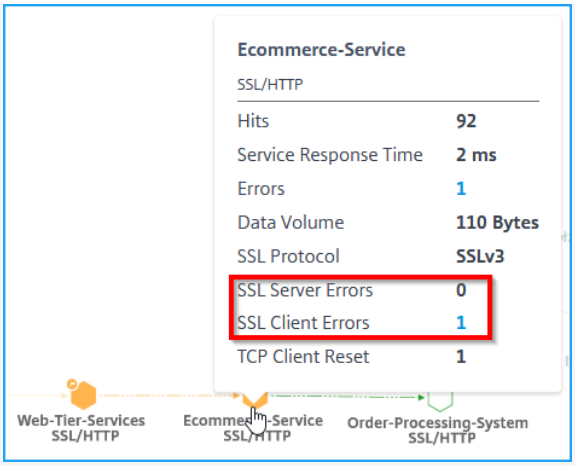
4 — Ermöglicht die Auswahl der Option, wie die Dienste angezeigt werden sollen.

5 - Optionen, um entweder die Einstellungen zu speichern oder auf die Standardeinstellung zurückzusetzen.

Analysieren Sie die Fehler

Bewegen Sie den Mauszeiger auf einen Dienst, der Fehler anzeigt.

Fehler	Beschreibung
	Das **Zurücksetzen des TCP-Servers** gibt die Gesamtanzahl der vom Server initiierten TCP-Resets an.

Fehler	Beschreibung
	Das **Zurücksetzen des TCP-Clients** zeigt die gesamten TCP-Resets an, die vom Client initiiert wurden.
	Die SSL-Client-Fehler geben die gesamten SSL-Fehler des Clients an. (Beispiel: SSL-Clientauthentifizierungsfehler).
	Die SSL-Serverfehler Geben Sie die gesamten SSL-Fehler vom Server an. (Beispiel: SSL-Zertifikat unbekannt)

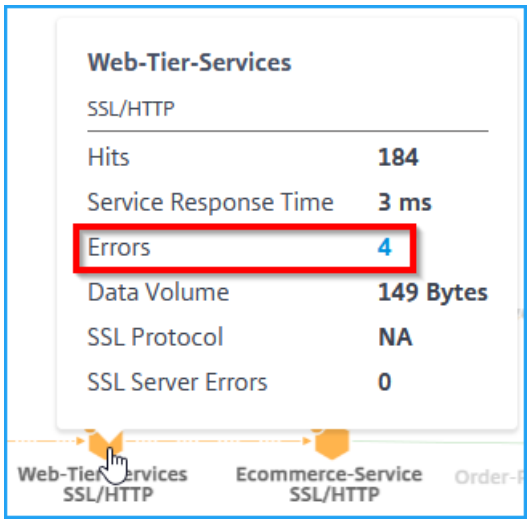
Hinweis

- Client-Fehleranzahl (unabhängig vom Protokolltyp) wird in jedem Dienst angezeigt, wenn die Client-Fehleranzahl **1 oder höher**ist.
- Die Anzahl der Clientfehler, die für jeden Dienst angezeigt wird, zeigt an, dass die Fehler vom Clientende stammen.

HTTP-Transaktionsdetails anzeigen

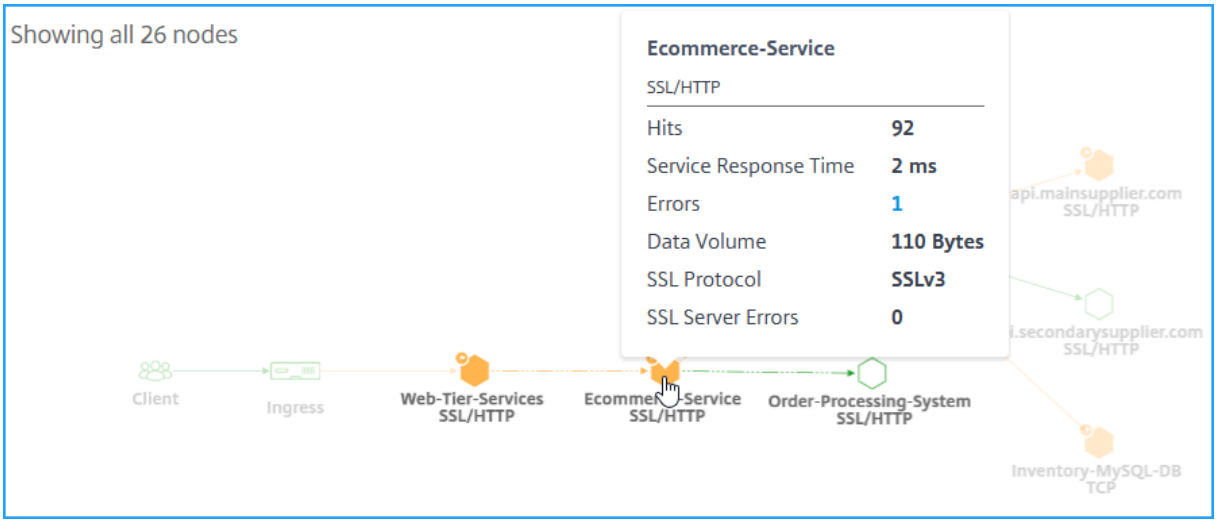
Hinweis

Sie können die Fehler anzeigen, indem Sie den Mauszeiger auf einen fehlerhaften Dienst bewegen und auf die Anzahl der Probleme klicken.

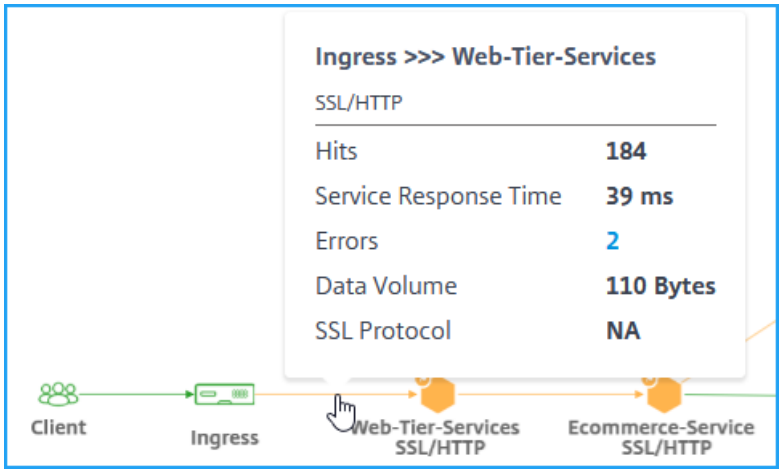


Gemäß dem im Bild gezeigten Beispiel können Sie eine End-to-End-Netzwerkkarte Ihrer Anwendung anzeigen, die zeigt, wie Ihre Komponentendienste kommunizieren.

Wenn Sie den Mauszeiger auf den **Ecommerce-Service**bewegen, können Sie Metrikdetails für **Ecommerce-Service**anzeigen.



Mit Citrix ADM können Sie auch Transaktionsdetails zwischen Ingress und Diensten anzeigen. Zeigen Sie mit der Maus auf den Mauszeiger, um Details wie Gesamtfehler, durchschnittliche Reaktionszeit des Dienstes usw. zwischen dem Ingress und dem Dienst anzuzeigen.



Treffer — Gibt die Gesamtzahl der vom Dienst empfangenen Treffer an.

Service-Antwortzeit — Gibt die durchschnittliche Antwortzeit an, die der Dienst für die Antwort auf Zeit bis erstes Byte (TTFB) verwendet hat.

Fehler — Gibt die Gesamtfehler an, z. B. 4xx, 5xx usw.

Datenvolumen — Gibt das Gesamtvolumen der vom Dienst verarbeiteten Daten an.

SSL-Protokoll — Gibt die Version des SSL-Protokolls an.

Klicken Sie auf den Pfeil zwischen **Ingress** und **Service**, um die detaillierten Transaktionen anzuzeigen.

Weitere Informationen finden Sie unter Anzeigen von Analysen für Web-Transaktionen.

Konfigurieren von Schwellenwerten im Dienstdiagramm

April 28, 2021

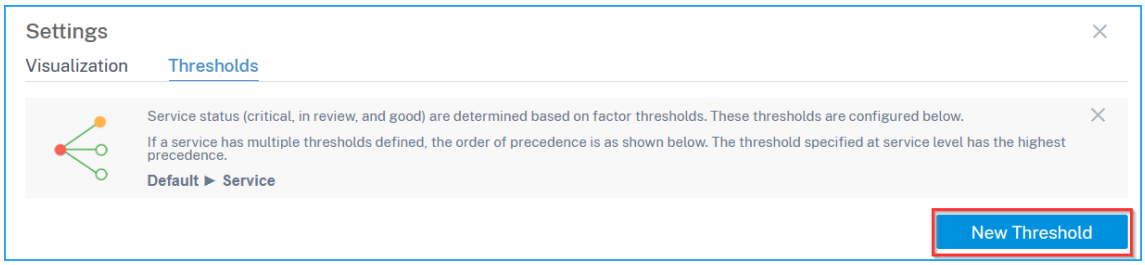
Als Administrator können Sie Schwellenwerte für Kubernetes-Dienste konfigurieren. Citrix ADM zeigt den Dienststatus (Kritisch, Prüfen und Gut) basierend auf der Reaktionszeit des Dienstes und der Fehleranzahl an. Standardmäßig können Sie den **Standardschwellwert** (Service-Reaktionszeit = 200 ms und Fehleranzahl = 0) anzeigen, der auf alle Dienste angewendet wird.

> **Hinweis**
>
> Sie können den Standardschwellenwert nicht löschen.

So konfigurieren Sie einen neuen Schwellenwert:

1. Klicken Sie unter **Applications > Service Graph**auf die Registerkarte **Microservices** :
2. Klicken Sie auf das Symbol “Einstellungen” und wählen Sie die Registerkarte “ **Schwellenwerte** “.

3. Klicken Sie auf **Neuer Schwellenwert**, um einen neuen Schwellenwert zu konfigurieren.



   Die Seite **Neuer Schwellenwert** wird angezeigt.

4. Konfigurieren Sie die folgenden Parameter:

   a) **Name** — Geben Sie einen Namen für den Schwellenwert an.

   b) Wählen Sie unter **Microservices**die Dienste aus, für die Sie den Schwellenwert anwenden möchten.

   c) Wählen Sie unter **SchwellenwerteEinzel-**oder**Doppelschwellenwert** für:

      - Hohe Reaktionszeit (Durchschnitt, P99, P99,9)
      - Hohe Fehler
      - Hohe Treffer

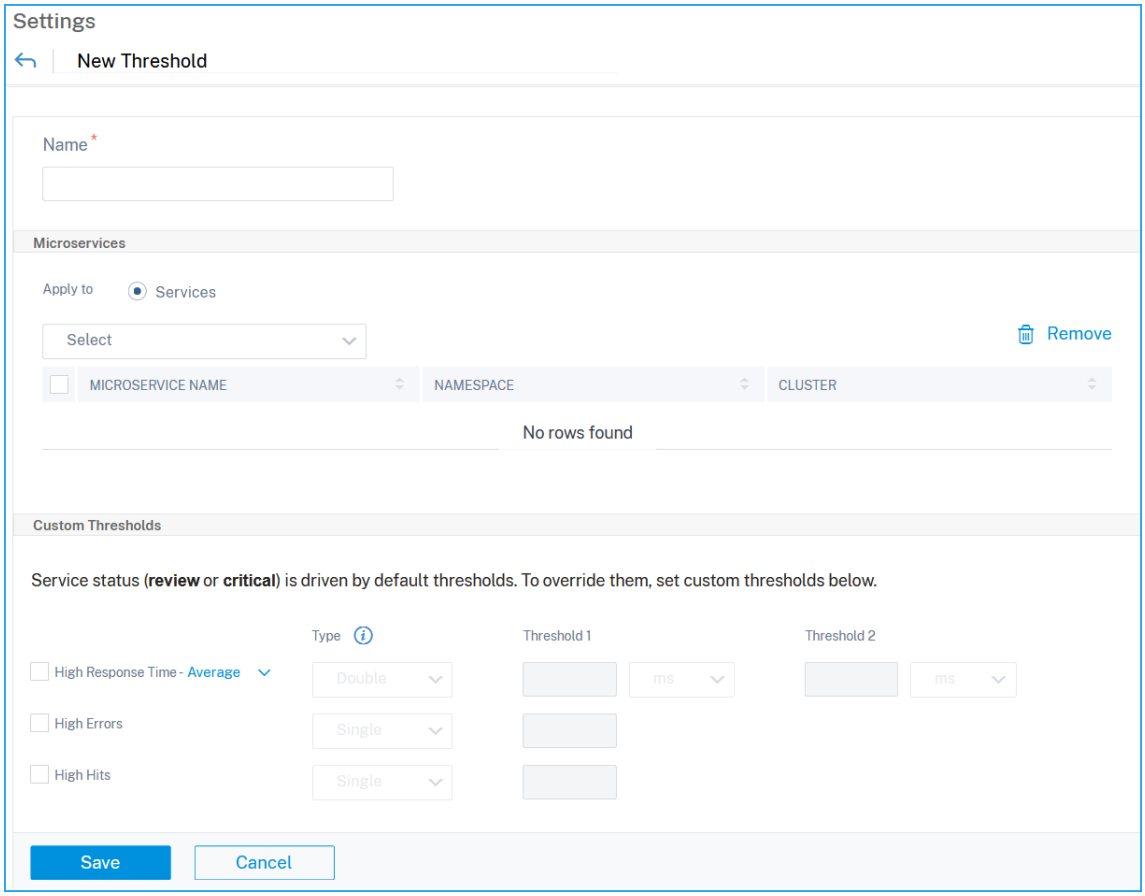
   d) Geben Sie die Schwellenwerte an.

   > **Hinweis**
   >
   > Wenn Sie den doppelten Schwellenwert auswählen, stellen Sie Folgendes sicher:

```
- Der Wert für Schwellenwert 1 ist kleiner als der
  Wert für Schwellenwert 2. Wenn Sie beispielsweise
  Schwellenwert 1 als 250 ms konfigurieren, muss der
  Schwellenwert 2 251 ms oder höher sein.

- Der Wert für Schwellenwert 1 darf nicht mit dem
  Wert für Schwellenwert 2 übereinstimmen.
```

5. Klicken Sie auf **Save**.



Der Schwellenwert wurde erfolgreich erstellt. Sie können die Schwellenwertdetails auf der Seite **Schwellenwerte** anzeigen.

> **Hinweis**
>
> Citrix ADM berechnet den Endstand und den Status des Service basierend auf den ausgewählten Metriken. Wenn Sie beispielsweise nur **High Hits** für die Schwellenwertkonfiguration auswählen, verwendet Citrix ADM den Standardschwellenwert (Reaktionszeit = 200 ms und Fehleranzahl = 0) und hohe Treffer, um den Servicebericht und den Status zu berechnen.

Einzelner Schwellenwert

Wenn Sie einen einzelnen Schwellenwert für alle Metriken oder ausgewählten Metriken konfigurieren, ist Citrix ADM:

- Vergleicht die aktuellen Werte in jeder Metrik mit den konfigurierten Schwellenwerten in jeder Metrik
- Berechnet die Gesamtstrafe basierend auf den überschrittenen Schwellenwerten in jeder Metrik

> Hinweis
>
> Wenn eine Metrik den Schwellenwert nicht verletzt hat, wird die Strafe entsprechend berechnet

- Zeigt die Service-Bewertung und den Service-Status basierend auf der Penalty Berechnung an

Doppelter Schwellenwert

Wenn Sie den doppelten Schwellenwert für alle Metriken oder ausgewählten Metriken konfigurieren, ist Citrix ADM:

- Vergleicht die aktuellen Werte in jeder Metrik mit den konfigurierten Schwellenwerten in jeder Metrik
- Überprüft, ob die aktuellen Werte sind:
  - Weniger als Schwellenwert 1
  - Zwischen Schwelle 1 und Schwellenwert 2
  - Größer als Schwellenwert 2
- Berechnet die Gesamtstrafe basierend auf den überschrittenen Schwellenwerten in jeder Metrik

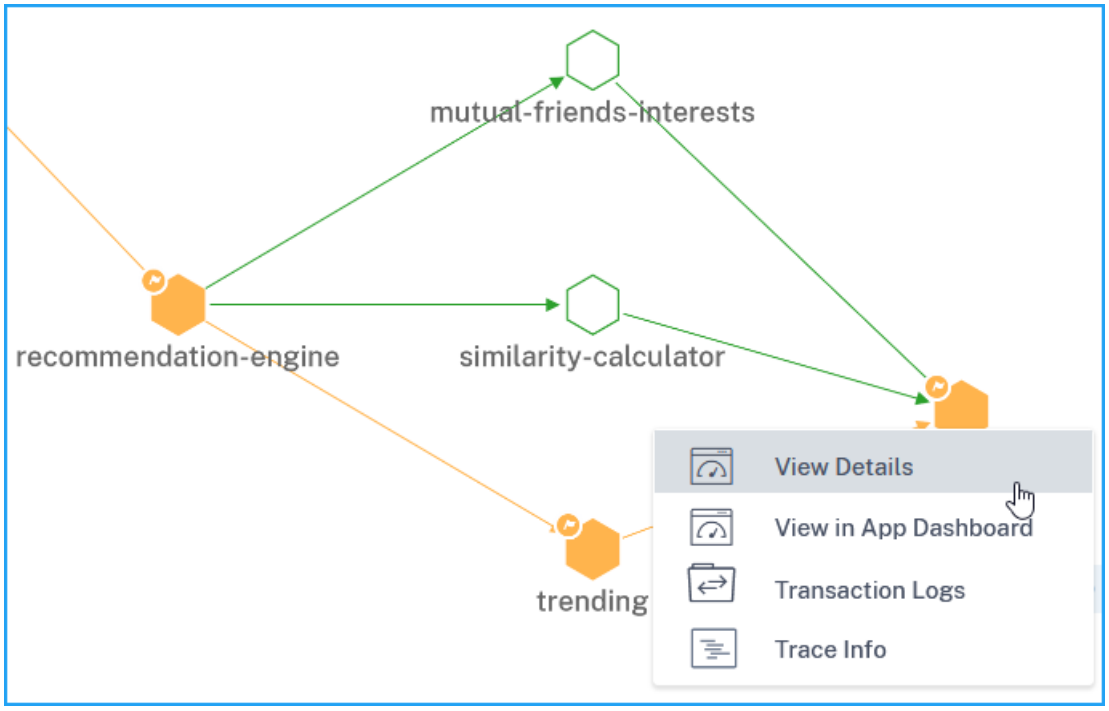
> Hinweis
>
> Wenn eine Metrik den Schwellenwert nicht verletzt hat, wird die Strafe entsprechend berechnet

- Zeigt die Service-Bewertung und den Service-Status basierend auf der Penalty Berechnung an

Service-Details anzeigen

April 28, 2021

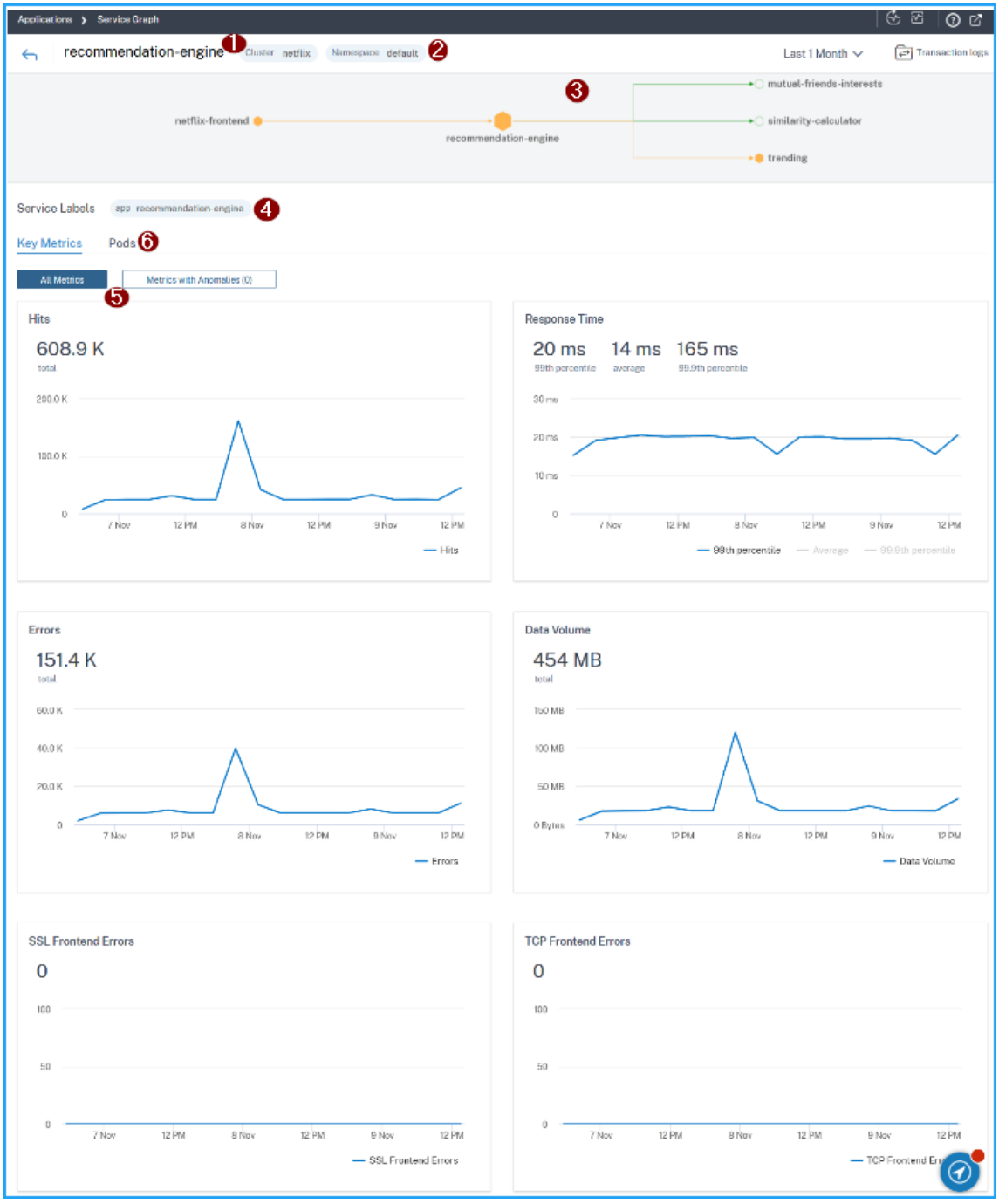
Klicken Sie auf einen Dienst und wählen Sie **Details anzeigen**aus.



Auf der Seite mit den Servicedetails können Sie Folgendes anzeigen:

- Der Clustername, in dem der Dienst gehostet wird (1)
- Der Namespace und die Service-Labels des Dienstes (2) (4)
- Alle zugeordneten eingehenden und ausgehenden Dienste, die mit dem ausgewählten Dienst verbunden sind (3)
- Service-Schlüssel-Metriken in einem Diagrammformat wie Hits, Reaktionszeit, Fehler, Datenvolumen, SSL-Frontend-Fehler und TCP-Frontend-Fehler. Auf der Registerkarte " **Metriken mit Anomalien** " können Sie die Anomalien für eine bestimmte Dauer anzeigen (5).

  Weitere Informationen finden Sie unter Überwachen Sie Dienste mithilfe der Golden Signal-Metriken.
- Die mit dem Dienst verbundenen Backend-Pods (6).



Mithilfe dieser wichtigsten Metrik-Trends können Sie analysieren, wie der Service für eine bestimmte Zeitdauer abläuft.

Betrachten Sie beispielsweise, dass ein Dienst Service-Reaktionszeit > 700 ms für alle Anforderungen angibt. Als Administrator können Sie:

- Analysieren des Metrik-Trends für die Service-Reaktionszeit für eine bestimmte Dauer
- Beheben des Problems

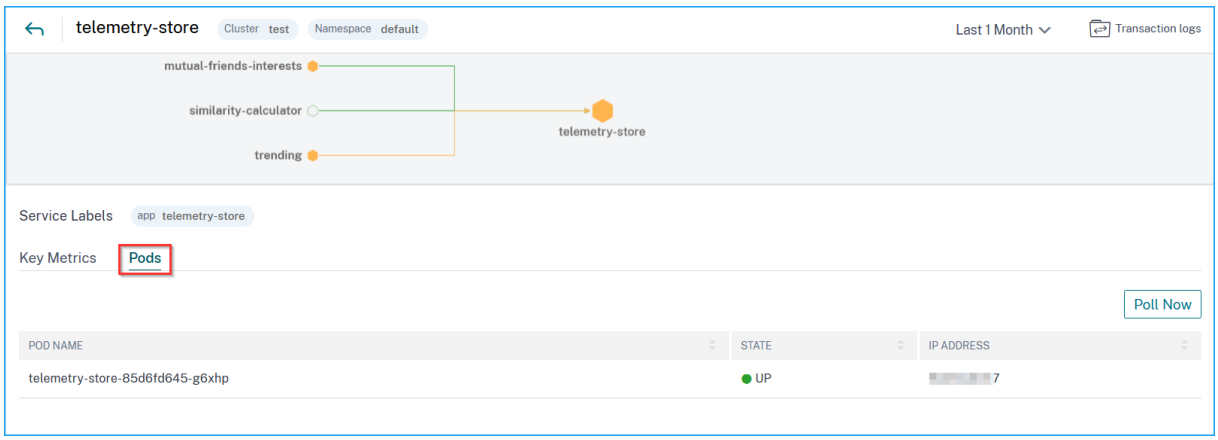
- Überprüfen Sie die Service-Reaktionszeit-Metrik erneut, um zu analysieren, ob sich die Reaktionszeit verbessert hat

Details zu Metriken

Metriken	Beschreibung
Treffer	Die Gesamtzahl der vom Dienst empfangenen Anfragen
Fehler	Die gesamten HTTP-Fehler des Dienstes
Service-Reaktionszeit	Die durchschnittliche Antwortzeit, die der Dienst für die Reaktion auf Time To First Byte (TTFB) verwendet hat.
Datenvolume	Das gesamte Datenvolumen, das vom Dienst verarbeitet wird
SSL Front-End-Fehler	Die gesamten SSL-Front-End-Fehler des Dienstes. Beispiel: SSL CLIENTAUTH FAILURE
SSL-Back-End-Fehler	Die gesamten SSL-Back-End-Fehler des Dienstes. Beispiel: SSL-Client-Fehler
TCP-Backend-Fehler	Die gesamten TCP-Back-End-Fehler vom Dienst. Beispiel: TCP-Server-Reset
TCP-Front-End-Fehler	Die gesamten TCP-Front-End-Fehler vom Dienst. Beispiel: Zurücksetzen des TCP-Clients

Details Back-End Backend-Pod anzeigen

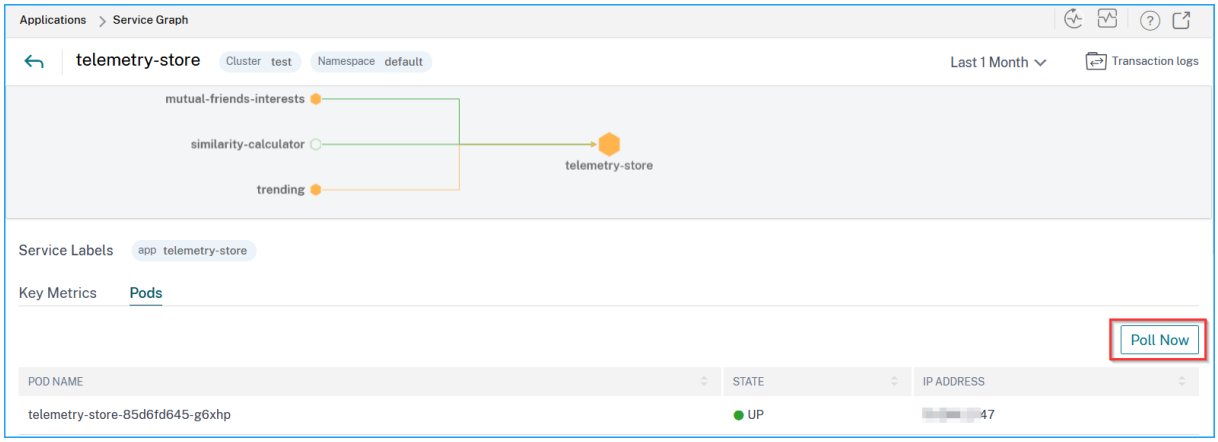
Klicken Sie auf die Registerkarte **Pods**, um die Backend-Pods anzuzeigen, die mit dem Dienst verknüpft sind.



- **Pod-Name** — Bezeichnet den Pod-Namen
- **Status** — Gibt an, ob der Pod läuft (UP) oder nicht (DOWN).
- **IP-Adresse** — Bezeichnet die Pod-IP-Adresse

Verwenden Sie die Option “Jetzt abfragen”, um den Podstatus zu ermitteln

Die Option **Jetzt abfragen** ruft den neuesten Podstatus vom Cluster ab.



Überwachen Sie Dienste mithilfe der Golden Signal-Metriken

Die Metriken des goldenen Signals in Diensten, die im Kubernetes-Cluster ausgeführt werden, beziehen sich auf eine Reihe von Metriken, mit denen Sie potenzielle Anomalien für eine bestimmte Dauer erkennen können. Wenn Sie 100 s Microservices im Kubernetes-Cluster haben, kann es schwierig sein, einen Dienst zu identifizieren, der häufig auftretende Probleme hat. Die folgenden drei wichtigen Metriken sind die Golden Signal-Metriken, mit denen Citrix ADM Service Graph Ihnen helfen kann, potenzielle Anomalien für einen Kubernetes-Service zu identifizieren:

- Treffer

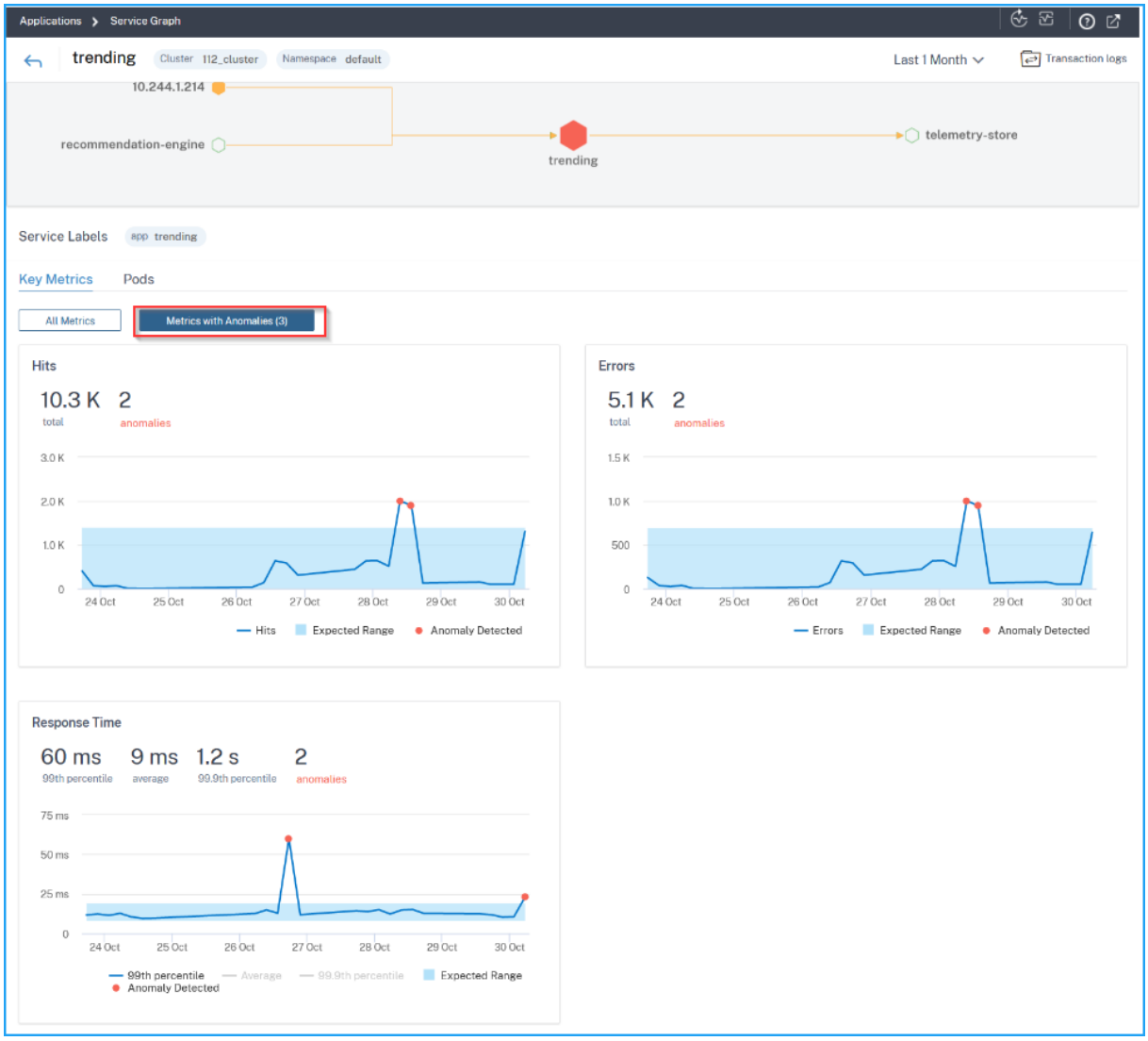
- Reaktionszeit (Durchschn.) und Reaktionszeit (P99)
- Fehler

Als Administrator können Sie mit diesen Metriken:

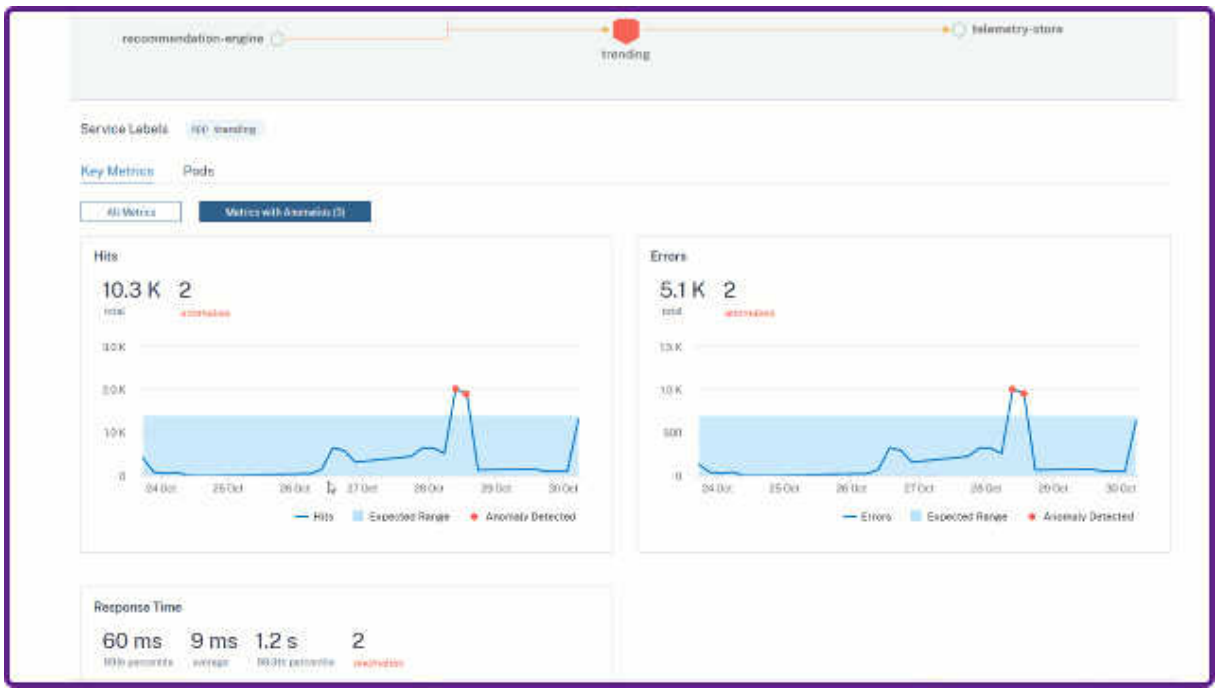
- Identifizieren des Servicestatus
  - **Kritisch** — Dienst hat Anomalien oder Schwellenwertverletzungen in mehreren Metriken
  - **Review** - Der Dienst hat Anomalien oder Schwellenverletzungen in einer der Metriken
  - **Gut** — Service ohne Anomalien oder ohne Schwellenverletzung
- Analysieren Sie, wie viele Anomalien in jeder Metrik identifiziert werden
- Beheben Sie das Problem und vermeiden Sie größere Auswirkungen

Identifizieren von Anomalien

Wenn Sie auf einen Dienst klicken und **Details anzeigen**auswählen, wird auf der Seite “Servicedetails” die Übersicht aller Metriken angezeigt. Klicken Sie auf die Registerkarte **Metriken mit Anomalien**, um die Details der Anomalie anzuzeigen.

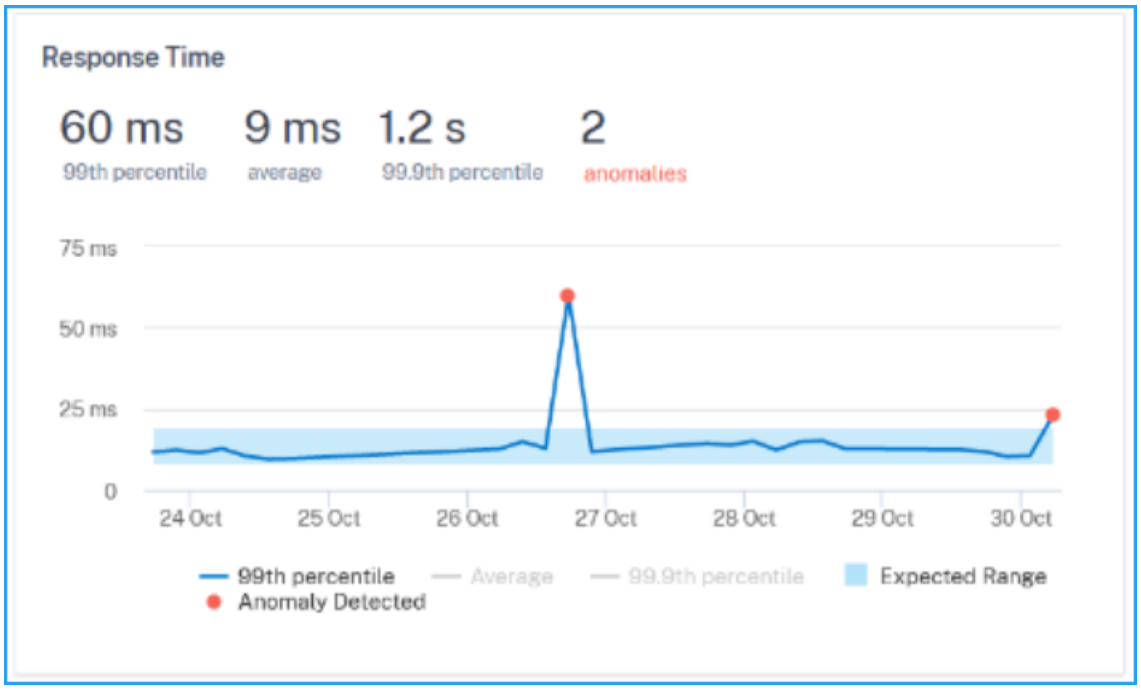


Für jede Metrik können Sie mit dem Diagramm die erkannten Anomalien anzeigen, wenn der erwartete Bereich übersteigt. Sie können auf die Optionen klicken, um die Ansichten im Diagramm zu filtern.



Bedenken Sie, dass Sie die Anomalien für den Service Response Time (P99) analysieren möchten.

Unter **Reaktionszeit**können Sie die folgenden Details für die ausgewählte Zeitdauer anzeigen:



- **99tes Perzentil** — Gibt an, dass die 99% der Anforderungen für die ausgewählte Dauer weniger als 60 ms beträgt
- **Durchschnitt** — Gibt die durchschnittliche Reaktionszeit des Dienstes an
- **99,9. Perzentil** — zeigt die höchste Reaktionszeit des Dienstes

- **Anomalien** — Zeigt die gesamten festgestellten Anomalien an

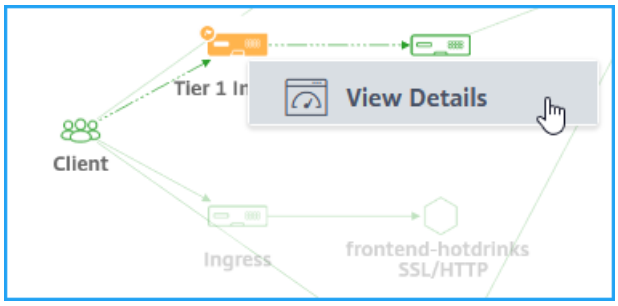
In der Grafik können Sie auch den erwarteten Bereich für die ausgewählte Zeitdauer anzeigen. Laut dem Beispiel können Sie Folgendes anzeigen:

- Die erwartete Reaktionszeit liegt zwischen 1 ms und 9 ms.
- Zwei Anomalien für den Dienst festgestellt (eine für 60 ms und eine für 25 ms), da die Reaktionszeit des Dienstes mehr als die erwartete Spanne überschritten hat (zwischen 1 ms und 9 ms).

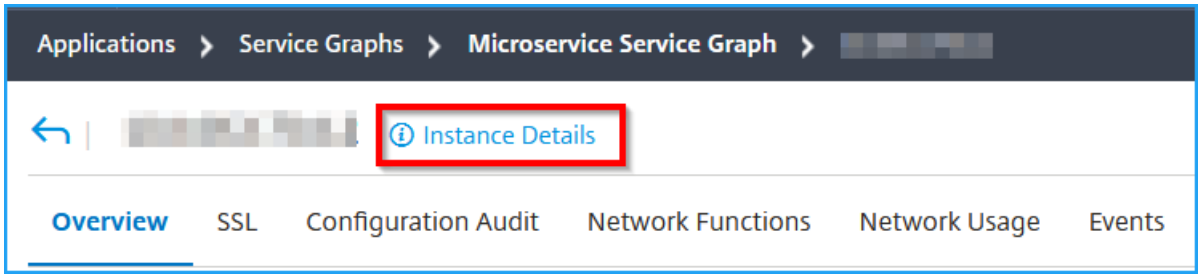
Anzeigen von Ingress-Details zur Problembehandlung

April 28, 2021

Klicken Sie im Service-Diagramm auf den Ingress und wählen Sie **Details anzeigen** aus, um die Details der Citrix ADC-Instanz zu visualisieren, die für den Kubernetes-Cluster konfiguriert ist.

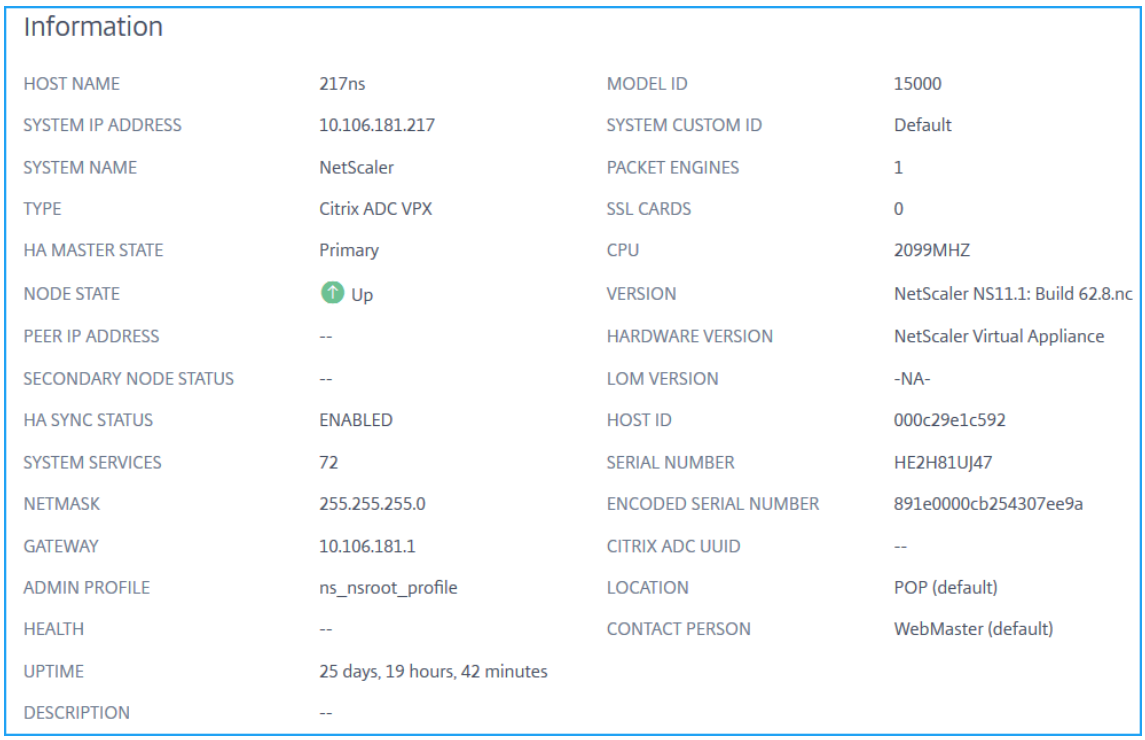


Klicken Sie auf **Instanzdetails**, um die Details anzuzeigen.

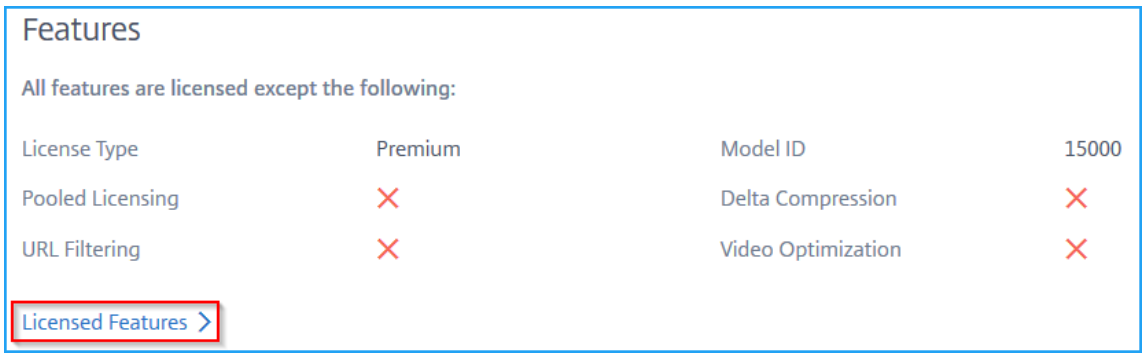


Folgende Details werden angezeigt:

- **Informationen** - Instanzdetails wie Instanztyp, Bereitstellungstyp, Version, Modell usw.



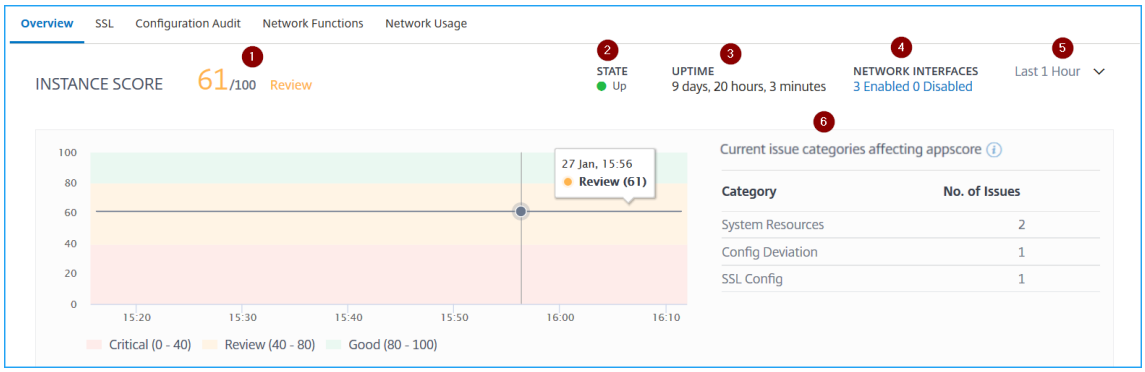
- **Features** — Standardmäßig werden die Features angezeigt, die nicht lizenziert sind. Klicken Sie auf **Lizenzierte Features**, um die lizenzierten Features anzuzeigen.



- **Modi** — Standardmäßig werden alle Modi angezeigt, die für die Instanz deaktiviert sind. Klicken Sie auf **Aktivierte Modi** anzeigen, um die aktivierten Modi auf der Instanz anzuzeigen.

Das Instanz-Dashboard bietet eine Instanzübersicht, in der Sie die folgenden Details sehen können:

- **Instanzbewertung**

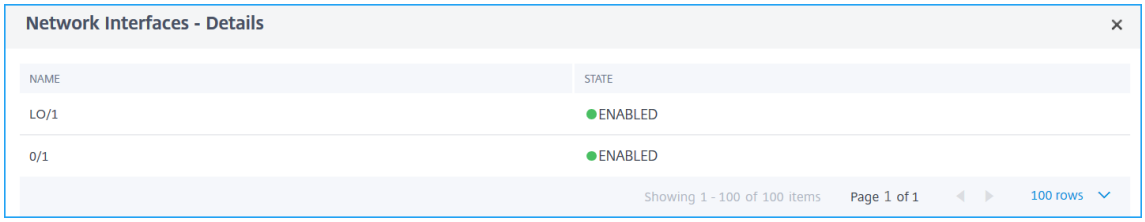


1 — Gibt die aktuelle Citrix ADC-Instanzbewertung für die ausgewählte Zeitdauer an. Die Endpunktzahl wird als **100 minus Gesamtstrafen**berechnet. Das Diagramm zeigt die Bewertungsbereiche für die ausgewählte Zeitdauer an.

2 — Gibt den aktuellen Status der Citrix ADC-Instanz an, z. B. **Up-**, **Down-**und **Out-Out of Service**.

3 — Gibt die Dauer an, die die Citrix ADC-Instanz ausgeführt wird.

4 — Gibt die Gesamtzahl der Netzwerkschnittstellen an, die für die Instanz aktiviert und deaktiviert sind. Klicken Sie hier, um Details wie den Namen der Netzwerkschnittstelle und den Status (aktiviert oder deaktiviert) anzuzeigen.



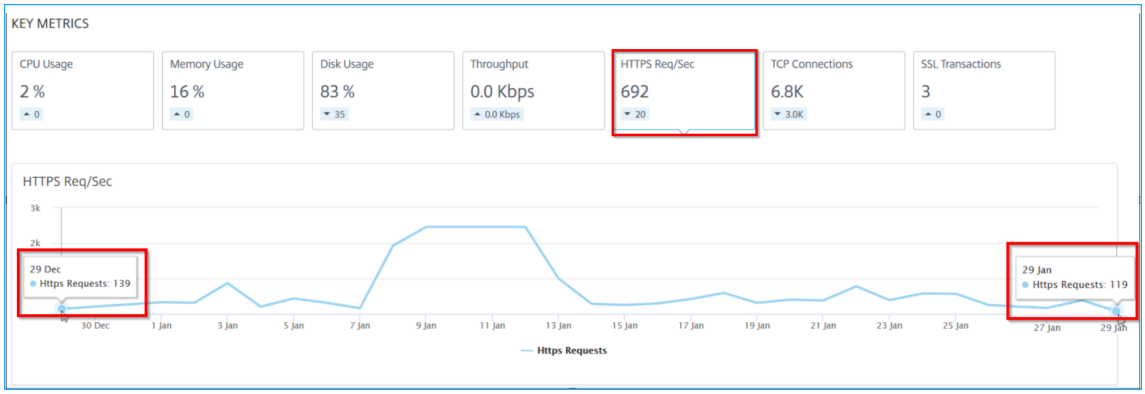
5 — Wählen Sie die Zeitdauer aus der Liste aus, um die Instanzdetails anzuzeigen.

6 — Zeigt die Gesamtzahl der Probleme und die Ausgabekategorie der ADC-Instanz an.

- **Wichtige Metriken**

  Klicken Sie auf die einzelnen Registerkarten, um die Details anzuzeigen. In jeder Metrik können Sie den Durchschnittswert und den Differenzwert für die ausgewählte Zeit anzeigen.

  Das folgende Bild ist ein Beispiel für HTTPS Req/Sec und die ausgewählte Zeitdauer gilt für den letzten Monat. Der Wert **692** ist der durchschnittliche HTTPS Req/Sek für die letzte Dauer von einem Monat und der Wert **20** ist der Differenzwert. In der Grafik ist der erste Wert **139** und der letzte Wert **119**. Der Differenzwert beträgt **139 — 119 = 20.**



  Sie können die folgenden Instanzmetriken in einem Diagrammformat für die ausgewählte Zeitdauer anzeigen:

  - **CPU-Auslastung** — Die durchschnittliche CPU% der Instanz für die ausgewählte Dauer (wird sowohl für Paketprozessoren als auch für Verwaltungs-CPU angezeigt).
  - **Speicherauslastung** — Die durchschnittliche Speicherauslastung% der Instanz für die ausgewählte Dauer.
  - **Datenträgerauslastung** — Der durchschnittliche Speicherplatz% der Instanz für die ausgewählte Dauer.
  - **Durchsatz** — Der durchschnittliche Netzwerkdurchsatz, der von der Instanz für die ausgewählte Dauer verarbeitet wird.
  - **HTTPS-Anforderung/s** — Die durchschnittlichen HTTPS-Anforderungen, die von der Instanz für die ausgewählte Dauer empfangen wurden.

- **TCP-Verbindungen** — Die durchschnittlichen TCP-Verbindungen, die vom Client und Server für die ausgewählte Dauer hergestellt werden.
- **SSL-Transaktionen** — Die durchschnittlichen SSL-Transaktionen, die von der Instanz für die ausgewählte Dauer verarbeitet werden.

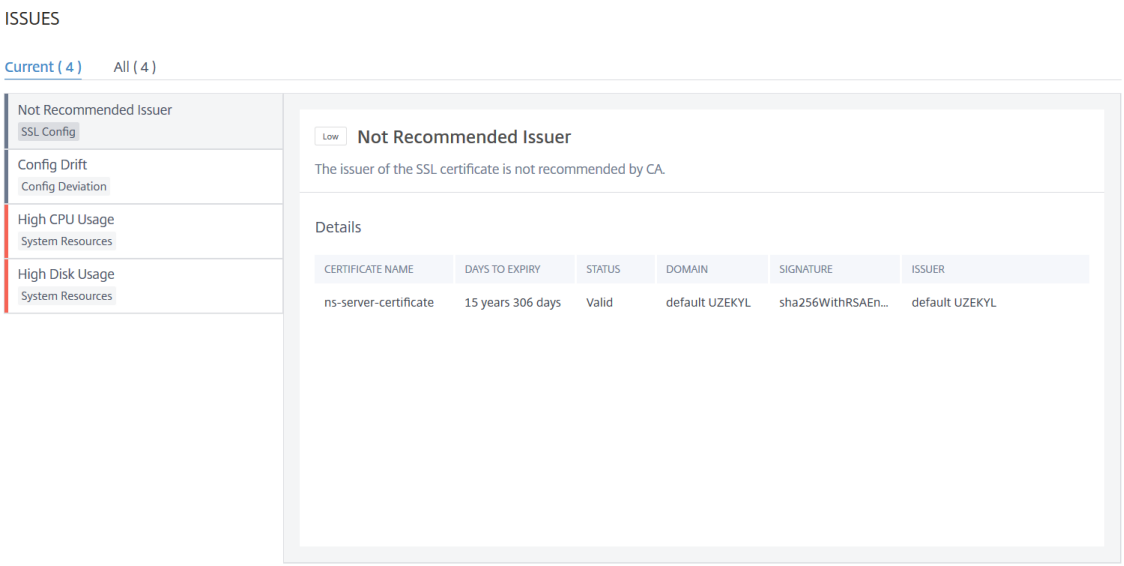
- **Probleme**

  Sie können die folgenden Probleme anzeigen, die in der Citrix ADC-Instanz auftreten:

Issue Kategorie	Beschreibung	Probleme
Systemressourcen	Zeigt alle Probleme im Zusammenhang mit der Citrix ADC -Systemressource an, z. B. CPU, Arbeitsspeicher, Datenträgerauslastung usw.	- Hohe CPU-Auslastung
		- Hohe Speicherauslastung
		- Hohe Datenträgernutzung
		- SSL-Karten-Fehler
		- Stromausfall
		- Datenträgerfehler
		- Blitzfehler
		- NIC verwirft
SSL-Konfiguration	Zeigt alle Probleme im Zusammenhang mit der SSL-Konfiguration auf der Citrix ADC-Instanz an.	- SSL-Zertifikate abgelaufen
		- Nicht empfohlener Aussteller
		- Nicht empfohlen Algo
		- Nicht empfohlene Tastenstärke
Konfigurationsabweichung	Zeigt alle Probleme im Zusammenhang mit den Konfigurationsaufträgen an, die in der Citrix ADC-Instanz angewendet werden.	- Config Drift
		- Laufen vs Vorlage

Issue Kategorie	Beschreibung	Probleme
Kapazitätsprobleme	Zeigt ADC-Kapazitätsprobleme an. Der ADM ruft diese Ereignisse alle fünf Minuten von der ADC-Instanz ab und zeigt die verworfenen Pakete oder Rate-Limit-Zähler-Inkremente an, falls vorhanden. Die Probleme werden nach den folgenden Kapazitätsparametern kategorisiert.	- Durchsatzlimit erreicht
		- PE-CPU-Limit erreicht
		- PPS Limit erreicht
		- SSL-Durchsatzrate Limit
		- SSL TPS Rate Limit
Netzwerke	Zeigt die Betriebsprobleme an, die in den Instanzen auftreten.	Weitere Informationen finden Sie unter Verbesserte Infrastrukturanalyse mit neuen Indikatoren.

Klicken Sie auf die einzelnen Registerkarten, um das Problem zu analysieren und zu beheben. Betrachten Sie beispielsweise, dass eine Instanz die folgenden Fehler für die ausgewählte Zeitdauer aufweist:



- Die Registerkarte **Aktuell** zeigt die aktuellen ADC-Betriebsprobleme an, die sich auf den Instanzscore auswirken.
- Auf der Registerkarte **Alle** werden alle Infrarotprobleme angezeigt, die für die ausgewählte Dauer erkannt wurden.

Verteilte Ablaufverfolgung

April 28, 2021

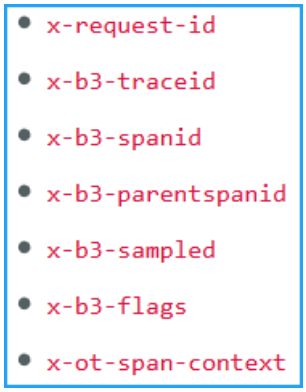
In Service Graph können Sie die verteilte Protokollierungsansicht verwenden, um:

- Analysieren Sie die gesamte Service-Performance.
- Visualisieren Sie den Kommunikationsfluss zwischen dem ausgewählten Dienst und seinen voneinander abhängigen Diensten.
- Identifizieren Sie, welcher Dienst auf Fehler hinweist, und beheben Sie den fehlerhaften Dienst.
- Zeigen Sie Transaktionsdetails zwischen dem ausgewählten Service und dem jeweils voneinander abhängigen Service an.

Voraussetzungen

Um die Ablaufverfolgungsinformationen für den Dienst anzuzeigen, müssen Sie:

- Stellen Sie sicher, dass eine Anwendung beim Senden von Ost-West-Datenverkehr die folgenden Trace-Header aufrechterhält:



- Aktualisieren Sie für **CIC-Builds vor 1.7.23**die CPX YAML-Datei mit `NS_DISTRIBUTED_TRACING` und Wert als `yes`


```
# Add cic as a sidecar
- name: cic
  image: "quay.io/citrix/citrix-k8s-ingress-controller:1.5.6"
  env:
  - name: "EULA"
    value: "yes"
  - name: "NS_IP"
    value: "127.0.0.1"
  - name: "NS_PROTOCOL"
    value: "HTTP"
  - name: "NS_PORT"
    value: "80"
  - name: "NS_DEPLOYMENT_MODE"
    value: "SIDECAR"
  - name: "NS_ENABLE_MONITORING"
    value: "YES"
  - name: "NS_DISTRIBUTED_TRACING"
    value: "yes"
  - name: "NS_LOGPROXY"
    value: "coe-tracing.default.svc.cluster.local"
  - name: POD_NAME
    valueFrom:
      fieldRef:
        apiVersion: v1
        fieldPath: metadata.name
  - name: POD_NAMESPACE
    valueFrom:
      fieldRef:
        apiVersion: v1
        fieldPath: metadata.namespace
  args:
    - --ingress-classes
      watches-ingress
  imagePullPolicy: Always
```

- Für **CIC-Builds, die später als 1.7.23**sind, müssen Sie eine ConfigMap verwenden.

  ConfigMaps ermöglicht es Ihnen, Ihre Konfigurationen von Ihren Pods zu trennen und Ihre Workloads portabel zu machen. Mit ConfigMaps können Sie Ihre Workload-Konfigurationen einfach ändern und verwalten und den Bedarf an Hardcode-Konfigurationsdaten auf Pod-Spezifikationen reduzieren.

  Mit der ConfigMap-Unterstützung können Sie die Konfiguration automatisch aktualisieren,

während der Citrix ingress controller Pod am Laufen gehalten wird. Sie müssen den Pod nach dem Update nicht neu starten. Weitere Informationen finden Sie unter ConfigMap-Unterstützung für den Ingress-Controller.

Mit ConfigMap können Sie verteilte Ablaufverfolgung, Ereignisse, Überwachungsprotokolle usw. aktivieren oder deaktivieren. So verwenden Sie ConfigMap:

1. Erstellen Sie eine YAML-Datei mit den erforderlichen Parametern.

   In der folgenden Beispiel-YAML-Datei ist die verteilte Ablaufverfolgung aktiviert und andere Variablen wie Audit-Logs, Ereignisse und Transaktionen deaktiviert:

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG: |
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'false'
      events:
        enable: 'false'
    transactions:
      enable: 'false'
      port: 5557
<!--NeedCopy-->
```


> Hinweis
>
> Sie können die Werte für 0 `Samplingrate` bis 100 angeben. Citrix ADM zeigt die erwähnte Anzahl von Trace-Transaktionen an.

2. Stellen Sie die ConfigMap bereit, indem Sie Folgendes verwenden:

   `kubectl create -f <configmap-yaml>.yaml`

3. Bearbeiten Sie die CPX YAML-Datei und verwenden Sie entweder `envFrom` oder `args`, um die folgenden Argumente anzugeben:

```
envFrom:
 - configMapRef:
     name: cic-configmap
<!--NeedCopy-->
```

   ODER

```
args:
   - --configmap
     default/cic-configmap
```

   Die ConfigMap YAML-Konfiguration wird in CIC bereitgestellt.

4. Wenn Sie den Wert für eine Variable ändern möchten, bearbeiten Sie die Werte in der ConfigMap. In diesem Beispiel werden alle anderen Variablen von **`false`** in geändert **`true`**.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG: |
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
```



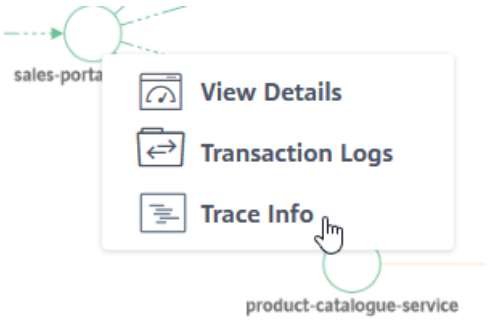
```
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'true'
      events:
        enable: 'true'
    transactions:
      enable: 'true'
      port: 5557
  <!--NeedCopy-->
```

5. Wenden Sie ConfigMap erneut mit dem folgenden Befehl an:

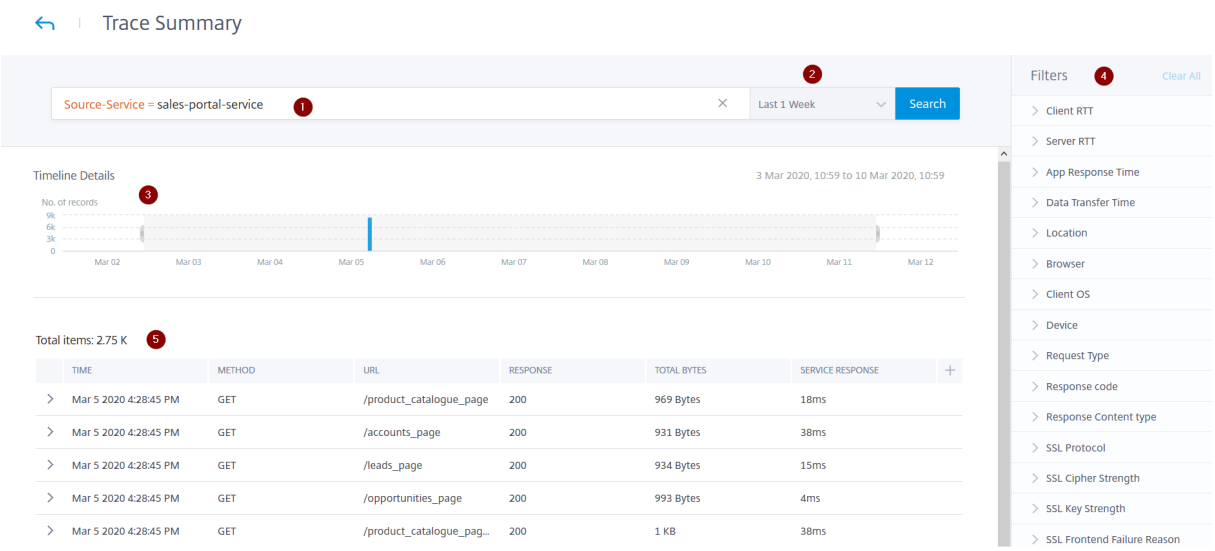
   ```
   kubectl apply -f <yaml-file>.yaml
   ```

Details zur Service-Ablaufverfolgung anzeigen

Klicken Sie im Service-Diagramm auf einen Service, und wählen Sie **Trace-Info**aus.



Die Seite “Trace-Zusammenfassung” wird für den ausgewählten Dienst angezeigt.



Die **Ablaufverfolgungsübersicht** wird angezeigt:

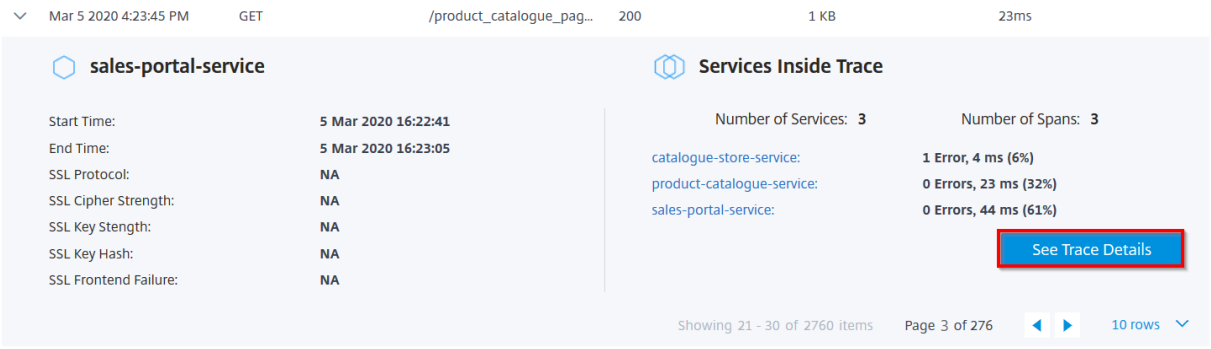
- Eine erweiterte Suche, mit der Sie nach Transaktionen mit Vorschlägen und Operatoren suchen können (1). Weitere Informationen finden Sie unter Erweiterte Suche.
- Die Liste der Zeitdauer, mit der Sie die Zeitdauer auswählen können, z. B. 1 Stunde, 12 Stunden, 1 Tag, 1 Woche, 1 Monat und benutzerdefinierte Zeit (2).
- Das Diagramm “Zeitleistendetails”, mit dem Sie die Ergebnisse für eine bestimmte Zeitdauer ziehen und auswählen können (3).
- Im Bedienfeld “Filter” können Sie Optionen aus jeder Metrik auswählen (4).
- Die Transaktionsdetails für den ausgewählten Service (5).

Transaktionsdetails anzeigen

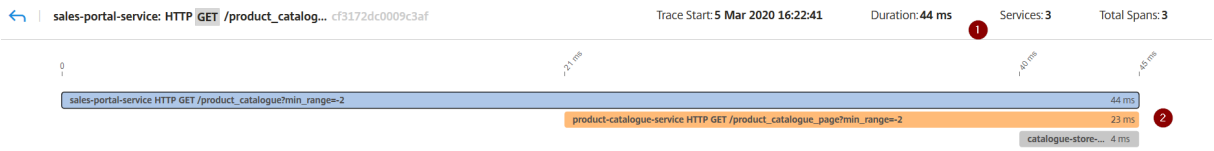
Klicken Sie auf eine Transaktion, um detaillierte Informationen zu erhalten. Sie können Transaktionsdetails für den ausgewählten Service anzeigen, z. B.:

- Startzeit
- Endzeit
- SSL-Metriken
- Kommunikation mit voneinander abhängigen Diensten (zusammen mit Fehlern und Reaktionszeit bei jedem Dienst).

Das folgende Beispiel zeigt einen Fehler von `catalogue-store-service`. Klicken Sie auf **Details zur Verfolgung anzeigen**, um weitere Details zu erhalten.



Die Seite Trace-Details wird angezeigt.

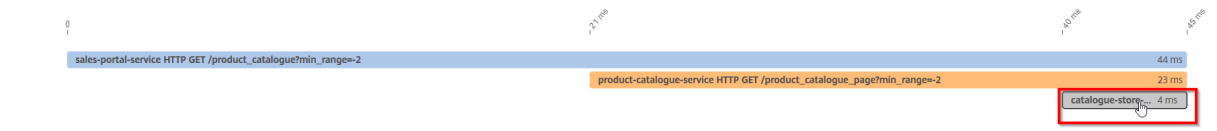


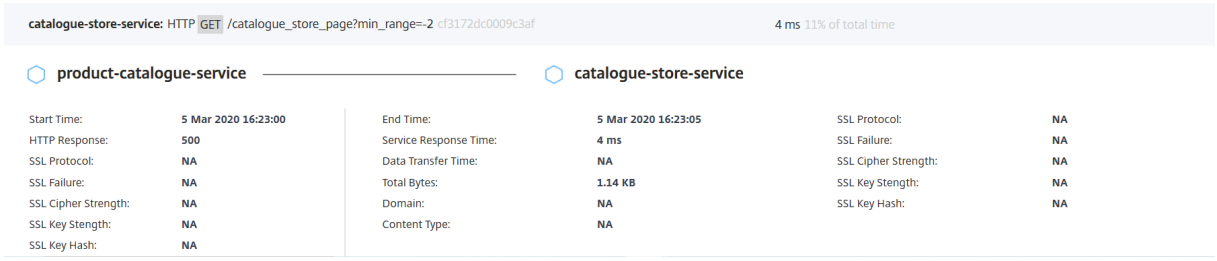
1 — Zeigt die Startzeit, die Antwortzeit, die Summe der Services und die Gesamtspanne für die Transaktion an.

2 — Zeigt die Details für den ausgewählten Dienst an, der mit seinen Abhängigkeitsdiensten kommuniziert hat. Sie können auf jede Transaktion klicken, um Details anzuzeigen.

3 — Zeigt die Transaktionsdetails für jeden Service an.

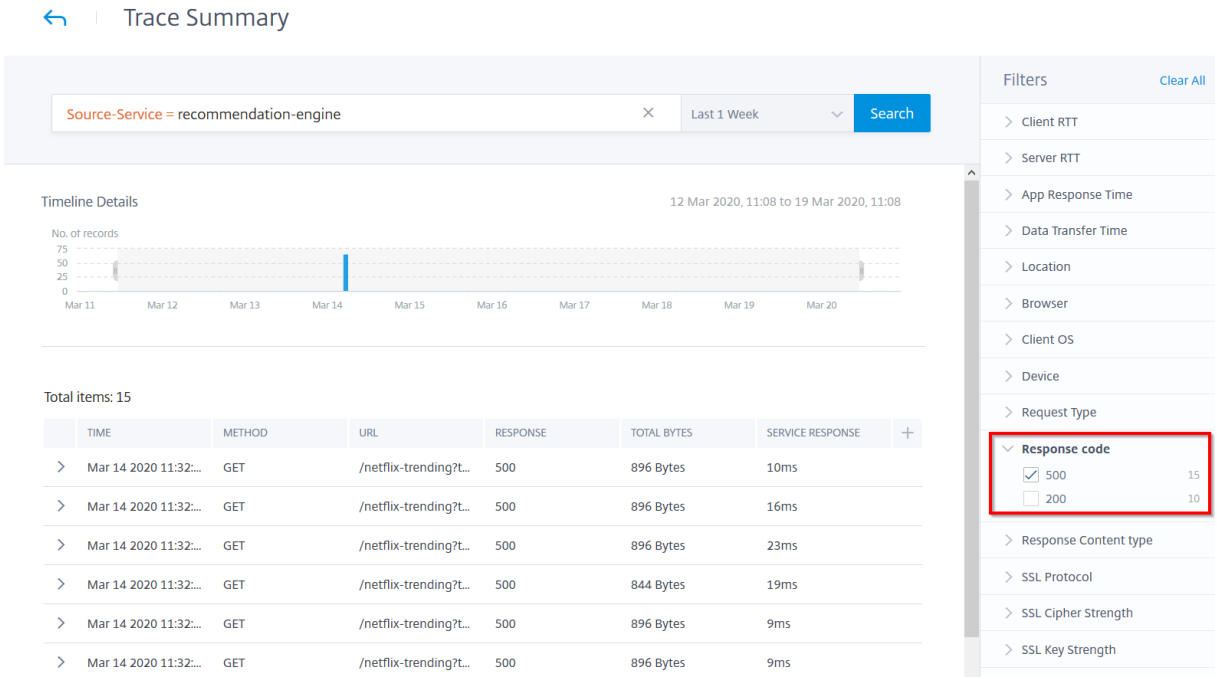
Nach dem Beispielbild, `catalogue-store-service`zeigte einen Fehler. Klicken Sie auf die Transaktion, die für verfügbar ist `catalogue-store-service`.





Die Transaktionsdetails zwischen `product-catalogue-service`und `catalogue-store-service`geben HTTP-Antwort als 500 an. Mit diesen Details können Sie als Administrator den fehlerhaften Service analysieren und die Fehlerbehebung `product-catalogue-service`als Lösung durchführen.

Sie können die Ergebnisse auch filtern, indem Sie Optionen aus den einzelnen Messobjekten im Bedienfeld " **Filter** " auswählen. Wenn Sie beispielsweise alle 5xx-Transaktionen anzeigen möchten, klicken Sie auf **Antwortcode** und wählen Sie **500**aus.



- **Client RTT**: Die Zeitdauer für ein Paket, das vom Client verreist wird.
- **Server RTT**: Die Zeitdauer für ein Paket, das vom Server übertragen werden soll.

- **App-Reaktionszeit**: Die durchschnittliche Reaktionszeit der Anwendung
- **Datentransferzeit**: Die Datentransfergröße und die Rate, mit der die Übertragung von/zu einem Dienst erfolgen kann.
- **Standort**: Der Clientstandort
- **Browser**: Die Browsertypen, die von den Clients verwendet werden. Zum Beispiel: Chrome, Firefox.
- **Client-Betriebssystem**: Das Client-Betriebssystem, das auf den Benutzer-Agent-Details aus dem Browser basiert.
- **Gerät**: Die Geräte, die auf den User-Agent-Details aus dem Browser basieren. Zum Beispiel: Tablet, Mobile.
- **Anforderungsart**: Die Transaktionsanforderungsart. Beispiel: GET.
- **Antwortcode**: Der vom Server empfangene Antwortcode. Zum Beispiel: 501, 404, 200.
- **Inhaltstyp der Antwort**: Der Transaktionsinhaltstyp. Wenn die Clientanforderung für text/html ist, muss die Antwort vom Server text/html sein.
- **SSL-Protokoll**: Die SSL-Protokollversion, die von den Clients verwendet wird. Beispiel: SSLv3.
- **SSL-Verschlüsselungsstärke**: Die Verschlüsselungsstärke basierend auf der Schlüsselgröße des SSL-Zertifikats wie hoch, mittel und niedrig.
- **SSL-Schlüsselstärke**: Die SSL-Verschlüsselungsstärke wird aus der Schlüsselgröße des SSL-Zertifikats berechnet. Die Schlüssellänge definiert die Sicherheit des SSL-Algorithmus. Zum Beispiel: 2048
- **SSL Frontend Failure reason**: Die Fehlermeldung “Front-End-SSL-Handshake”. Beispiel: SSL CLIENTAUTH FAILURE

Anzeigen von Diagnosedetails für partielle oder keine Daten im Service-Diagramm

April 28, 2021

Nachdem Sie das erforderliche Dienstdiagramm abgeschlossen configurationund den Kubernetes-Cluster in Citrix ADM hinzugefügt haben, beginnt das Dienstdiagramm mit dem Auffüllen der Daten. In einigen Szenarien können Sie beobachten, dass Service-Graph entweder Teildaten oder keine Daten anzeigt. Einige der möglichen Gründe für die Teildaten oder keine Daten im Service-Diagramm sind:

- Statische Route ist nicht konfiguriert

- Kubernetes Clusterstatus ist ausgefallen
- CPX-Registrierung ist fehlgeschlagen
- Virtuelle CPX-Server sind nicht lizenziert
- Die erforderliche Analytics-Konfiguration ist nicht festgelegt, die verhindert, dass Service-Graph alle Daten laden kann.

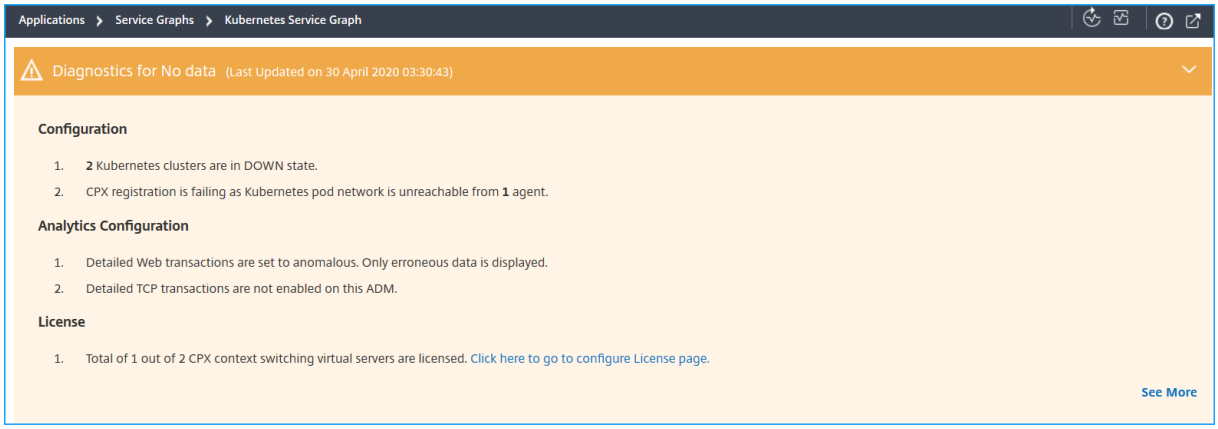
Als Administrator ist es Ihnen möglicherweise schwierig, die Gründe zu analysieren, wenn ein Service-Graph angezeigt wird, das Teildaten oder keine Daten anzeigt. Auf der Seite “Diagnoseinformationen” im Service-Diagramm können Sie die möglichen Gründe und erforderlichen Maßnahmen zur Behebung der Teildaten oder des Datenproblems anzeigen.

Navigieren Sie in Citrix ADM zu **Applications** > **Service Graph** und klicken Sie auf die Registerkarte **Microservices**.

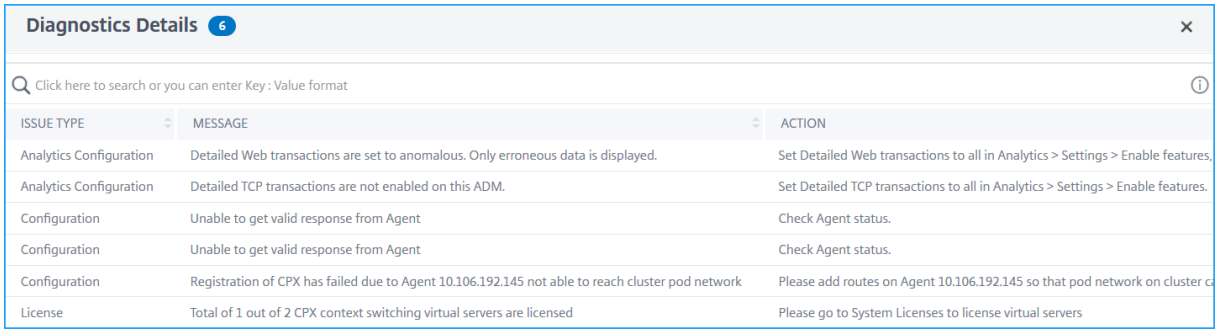
Diagnose für keine Daten

Wenn Service-Graph keine Daten anzeigt, wird die folgende Diagnosemeldung angezeigt.

Klicken Sie auf **, um Details anzuzeigen. Sie können die möglichen Gründe für Service-Graph anzeigen, die keine Daten anzeigen. Die folgende Abbildung ist ein Beispiel für keine Daten im Dienstdiagramm.



Klicken Sie auf **Weitere** Informationen, um Details zu den Problemen anzuzeigen.

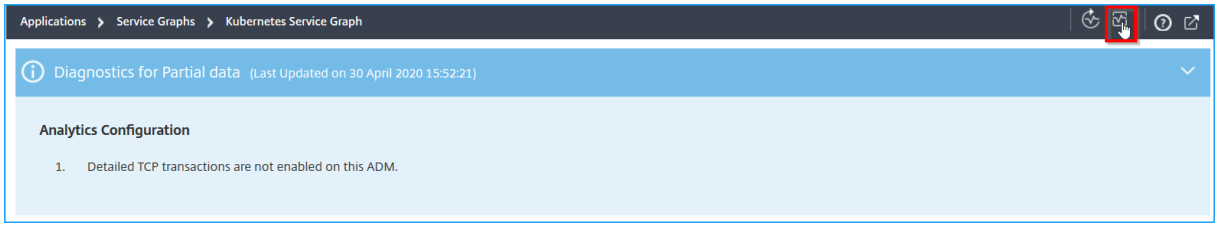


- **Problemtyp** — Gibt an, ob die Probleme bei der Konfiguration, der Analytics-Konfiguration oder der Lizenzierung auftreten.
- **Meldung** — Gibt an, was das Problem verursacht hat.
- **Aktion** — Gibt an, welche Aktion durchgeführt werden muss, um das Problem zu beheben.

Diagnose für Teildaten

Wenn das Service-Diagramm nur mit Teildaten angezeigt wird, klicken Sie auf die Schaltfläche **Diagnose anzeigen**, um die Diagnoseinformationen anzuzeigen.

Das folgende Beispiel zeigt an, dass die TCP-Transaktionen deaktiviert sind.

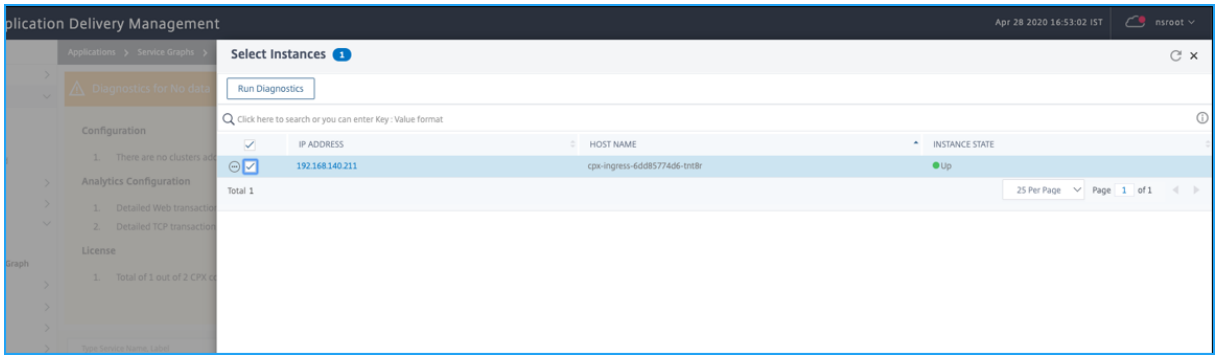


In diesem Beispiel müssen Sie die **TCP-Transaktionseinstellungen** auf **Alle** aktivieren, indem Sie zu **Analytics** > **Einstellungen**navigieren.

Problembehandlung

Als Administrator können Sie diese Probleme mithilfe dieser Diagnosemeldungen überprüfen und versuchen, diese Probleme zu beheben. Nach der Problembehandlung führt Citrix ADM automatisch eine regelmäßige Diagnoseprüfung in einem regelmäßigen Intervall aus. Nachdem die Diagnoseprüfung abgeschlossen ist, werden die Teildaten oder keine Daten im Service-Graph-Problem behoben.

Sie können auch auf **Diagnose ausführen**klicken, die **CPX-Instanzen**auswählen und auf **Diagnose ausführen**klicken.



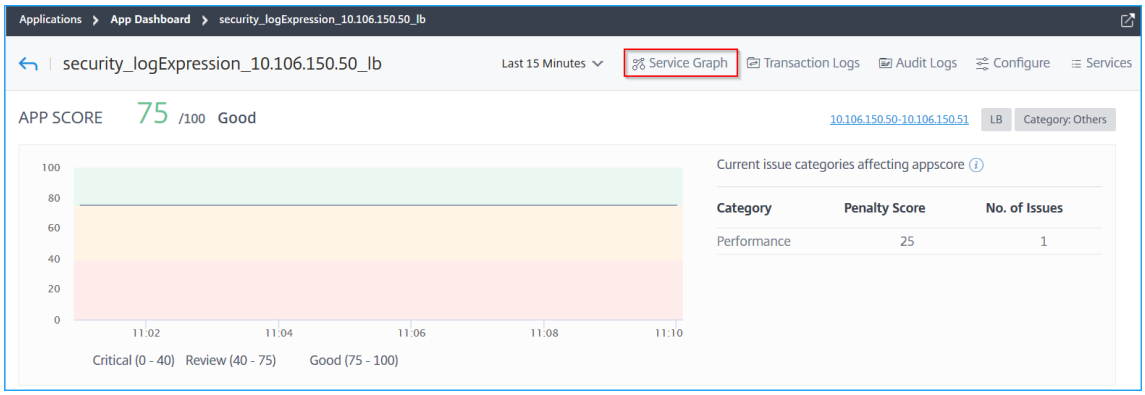
Service-Diagramm für dreistufige Webanwendungen

April 28, 2021

So zeigen Sie Service-Graph für eine Anwendung an:

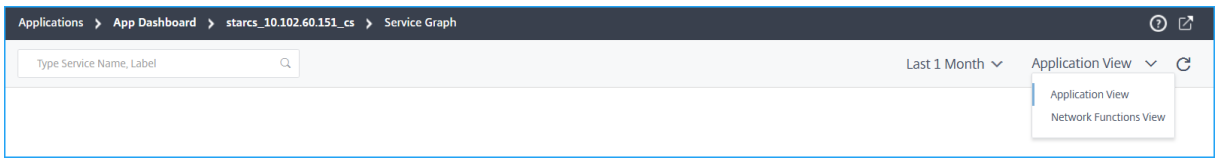
1. Navigieren Sie zu **Anwendungen** > **Dashboard**.
2. Wählen Sie eine Anwendung aus.

   Die Seite mit den Anwendungsdetails wird angezeigt.
3. Wählen Sie die Zeitdauer aus, und klicken Sie auf **Dienstdiagramm**.



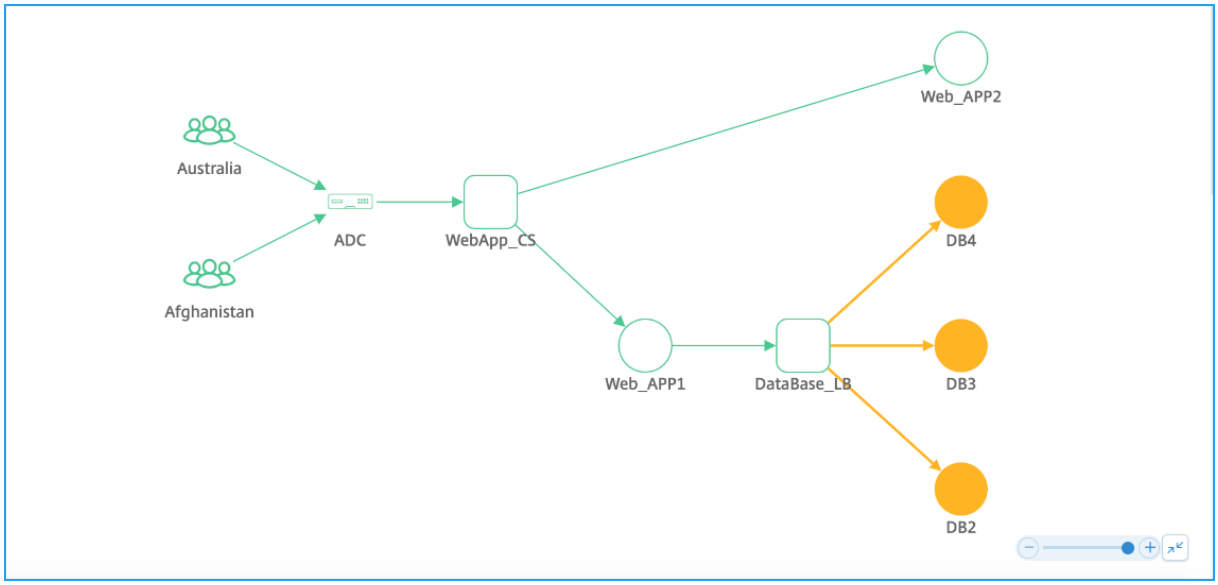
   Die Seite “Service Graphs” wird für die ausgewählte Anwendung angezeigt.

Sie können Service-Graph in der **Anwendungsansicht** oder in der **Netzwerkfunktionsansicht anzeigen**.

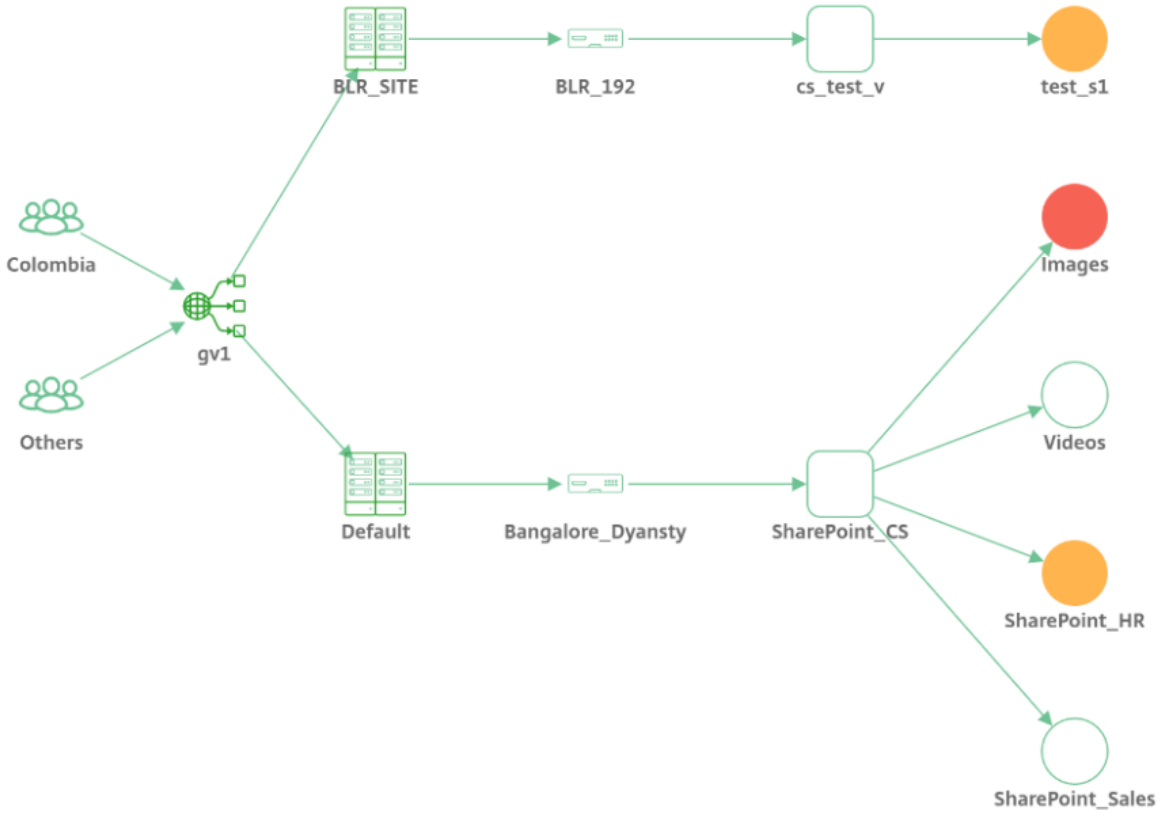


Ansicht der Anwendung

Zeigt die Übersicht über die Anwendungskonfiguration an. In dieser Ansicht können Sie die Kommunikation zwischen Client-, ADC- und Webanwendungen visualisieren.



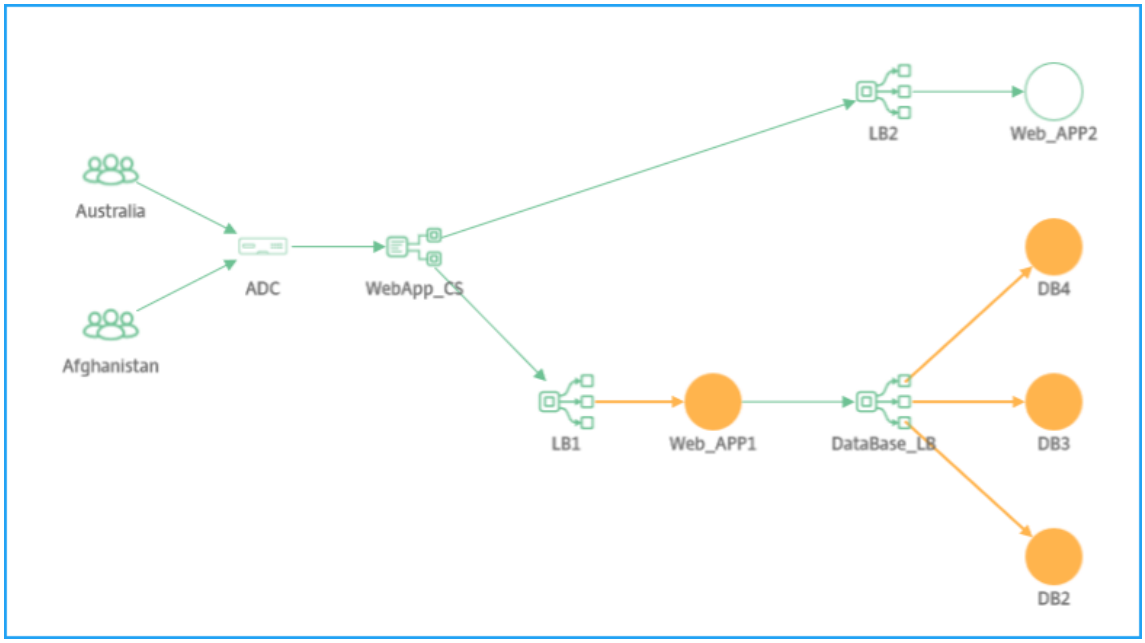
Für eine GSLB-Anwendung können Sie die Kommunikation zwischen Client, Rechenzentrum, ADC und Services visualisieren.



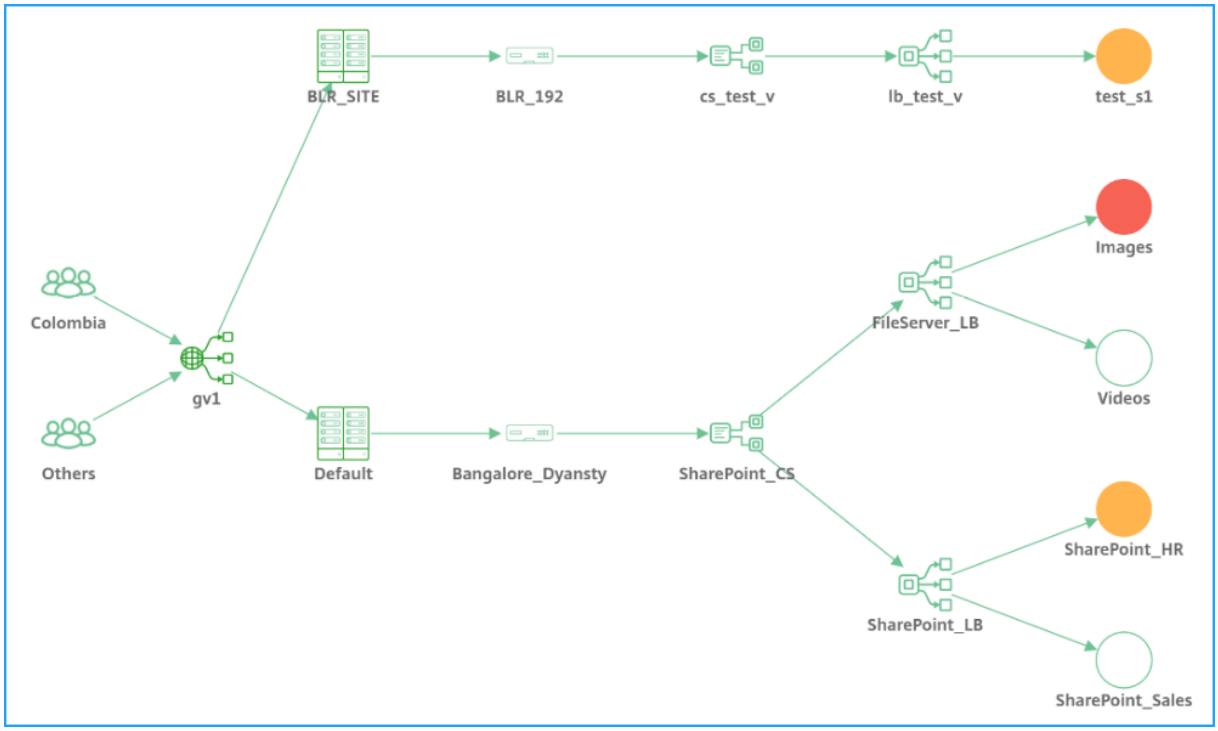
Ansicht “Netzwerkfunktionen”

Zeigt die virtuellen Server an, die der Anwendung zugeordnet sind. In dieser Ansicht können Sie visualisieren, ob der ADC kommuniziert mit:

- Virtueller Content Switching-Server für den Zugriff auf die Anwendung
- Virtueller Lastenausgleich für den Zugriff auf die Anwendung
- Virtuelle Server für Content Switching und Load Balancing für den Zugriff auf die Anwendung

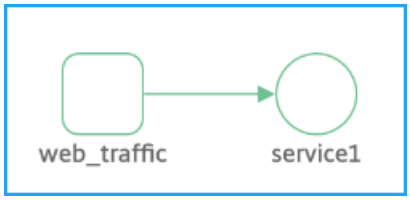


Für die GSLB-Anwendung werden die Details zusammen mit dem Rechenzentrum und dem Citrix ADC angezeigt.

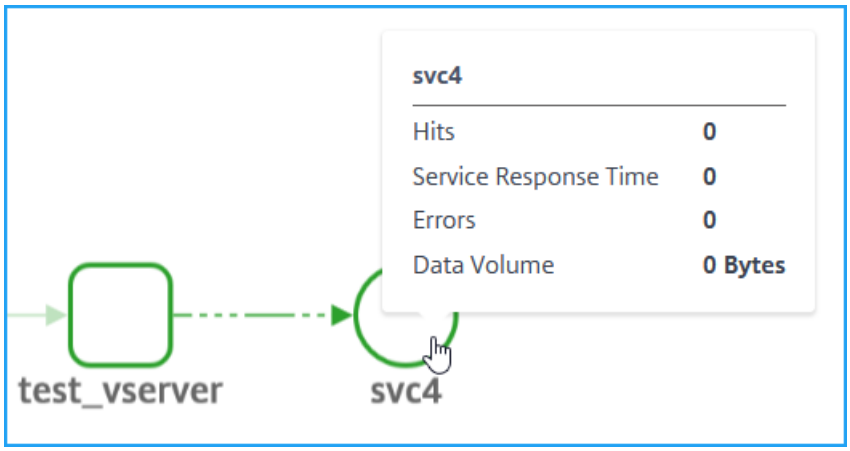


Service-Graph-Ansicht für keine aktiven Transaktionen

Wenn keine aktiven Transaktionen zwischen ADC und Webanwendung auftreten, zeigt das Dienstdiagramm nur die Basiskonfiguration der Anwendung an (ohne Client und ADC).



Wenn Sie den Mauszeiger auf einen Dienst oder einen virtuellen Server bewegen, werden die Details als 0 für alle Metriken angezeigt, da keine Transaktionen vorhanden sind.

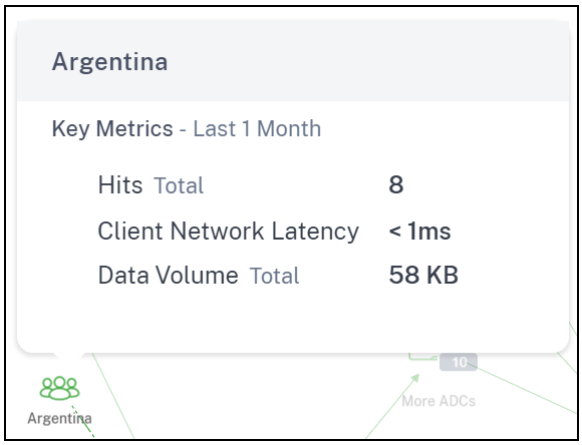


Analysieren von Metriken

Bewegen Sie den Mauszeiger auf jeden Dienst, um Metrikdetails entweder in der **Anwendungsansicht** oder in der **Netzwerkansicht anzuzeigen**.

Client-Metriken

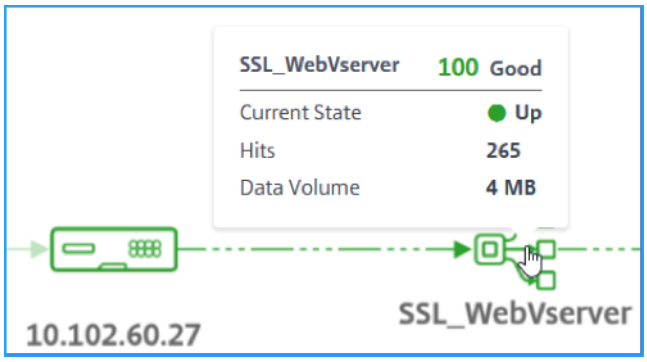
Bewegen Sie den Mauszeiger auf den Client, um Client-Metriken anzuzeigen.



- **Client-Netzwerklatenz** — Gibt die Netzwerklatenz des Clients an.
- **Client 4xx Fehler** — Gibt die Gesamtzahl der 4xx Fehler an, die vom Client aufgetreten sind.
- **Client-SSL-Fehler** — Gibt die Gesamtzahl der SSL-Fehler vom Client an.

Metriken der Netzwerkfunktion

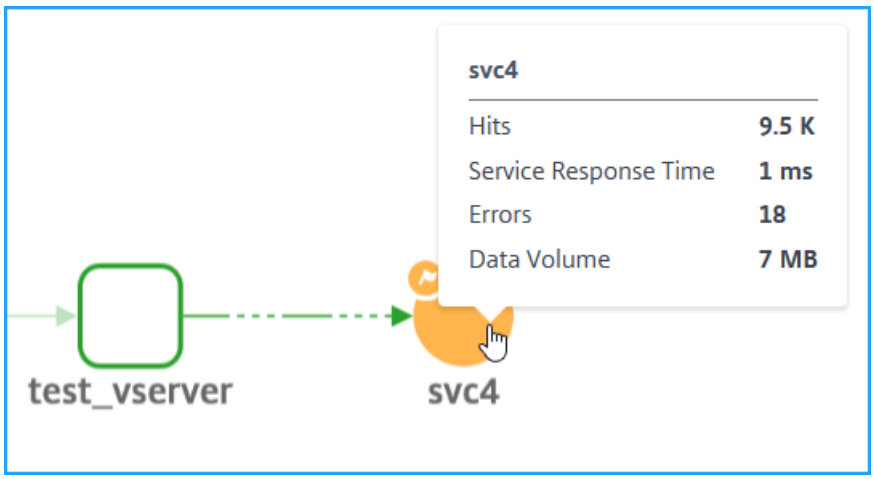
Bewegen Sie den Mauszeiger auf einen Lastausgleichs- oder Content Switching-Dienst, um die Metrikdetails anzuzeigen.



- **Aktueller Status** — Gibt den aktuellen Status des virtuellen Servers an
- **Treffer** — Gibt die Gesamtzahl der vom virtuellen Server empfangenen Treffer an
- **Datenvolumen** — Gibt das gesamte vom virtuellen Server verarbeitete Datenvolumen an.

Service-Metriken

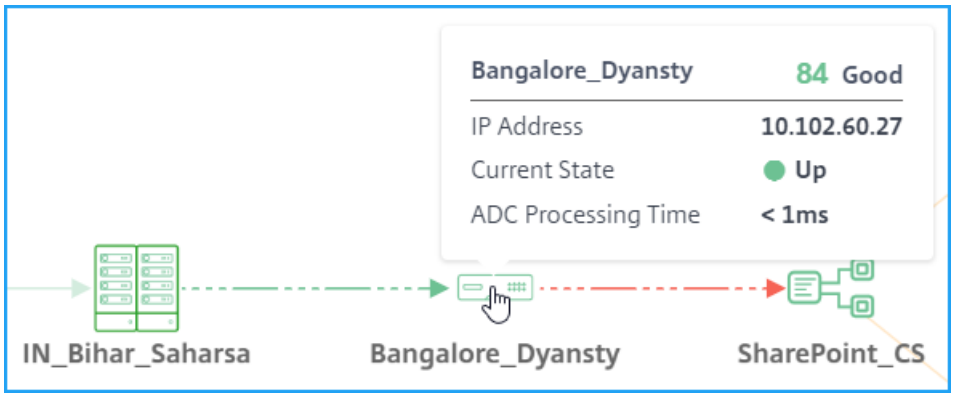
Bewegen Sie den Mauszeiger auf einen Dienst (Webanwendung), um die Metriken anzuzeigen



- **Treffer** — Gibt die Gesamtzahl der vom Dienst empfangenen Treffer an
- **Service-Reaktionszeit** — Gibt die durchschnittliche Reaktionszeit des Service an
- **Fehler** — Gibt die Gesamtzahl der vom Dienst aufgetretenen Fehler an
- **Datenvolumen** — Gibt die Gesamtdaten an, die vom Dienst verarbeitet werden.

Citrix ADC Metriken (nur für GSLB-Anwendungen)

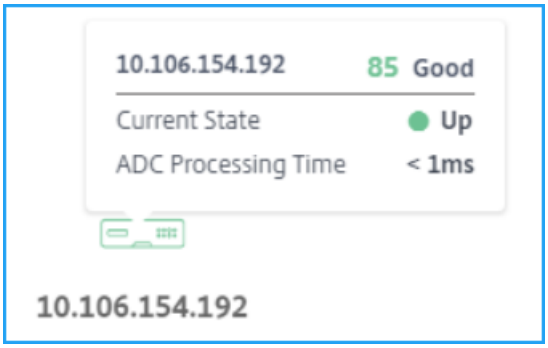
Bewegen Sie den Mauszeiger auf den ADC, um die Metriken anzuzeigen.



- Zeigt den Hostnamen und die aktuelle ADC-Bewertung an. Die Bewertung wird basierend auf den verschiedenen potenziellen Problemen von Citrix ADC berechnet. Weitere Informationen finden Sie unter Instanzbewertung.
- **IP-Adresse** — Bezeichnet die Citrix ADC IP-Adresse
- **Aktueller Status** : Bezeichnet den Citrix ADC Status, z. B. “Aufwärts”, “Heruntergefahren” oder “Abgemeldet”.

- **ADC-Verarbeitungszeit** — Kennzeichnet die durchschnittliche Verarbeitungszeit durch die ADC-Instanz

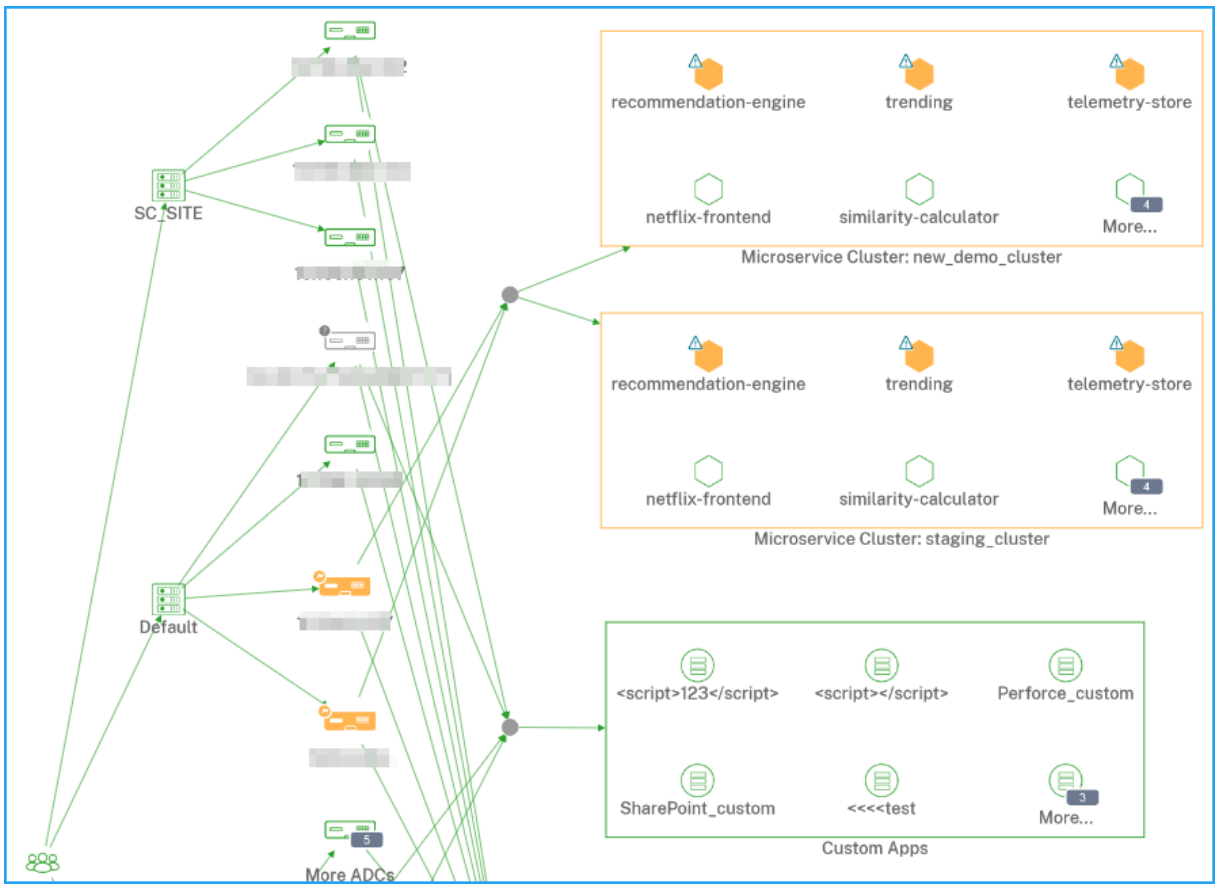
> **Hinweis**
>
> Wenn Citrix ADC kein Hostname zugewiesen ist:
>
> -Die Citrix ADC-IP-Adresse wird anstelle des Hostnamens angezeigt.
>
> -In den Metriken werden die Citrix ADC IP-Adressinformationen nicht angezeigt.



Ganzheitliche Ansicht aller Anwendungen im Service-Graph

April 28, 2021

Navigieren Sie zu **Anwendungen** > **Service Graph** und klicken Sie dann auf **Global**.



Das Service-Diagramm zeigt für die ausgewählte Zeitdauer Folgendes an:

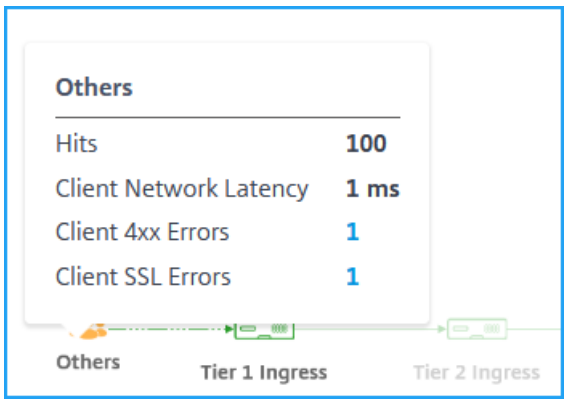
- Die Region, von der aus die Benutzer auf die jeweilige Anwendung zugreifen
- Rechenzentren, in denen die Citrix ADC-Instanzen gehostet werden
- Gesamt diskrete Anwendungen von allen Citrix ADC-Instanzen

> **Hinweis**
>
> Wenn eine Citrix ADC-Instanz keine diskreten Anwendungen hat, ist der Pfeilrand von der Citrix ADC-Instanz in Richtung des diskreten virtuellen Servers nicht sichtbar

- Gesamtanzahl der benutzerdefinierten Anwendungen aus allen Citrix ADC-Instanzen
- Die gesamten Microservice-Anwendungen von der Citrix ADC CPX-Instanz

Client-Metriken anzeigen

Bewegen Sie den Mauszeiger auf eine Client-Region, um die Metriken anzuzeigen.

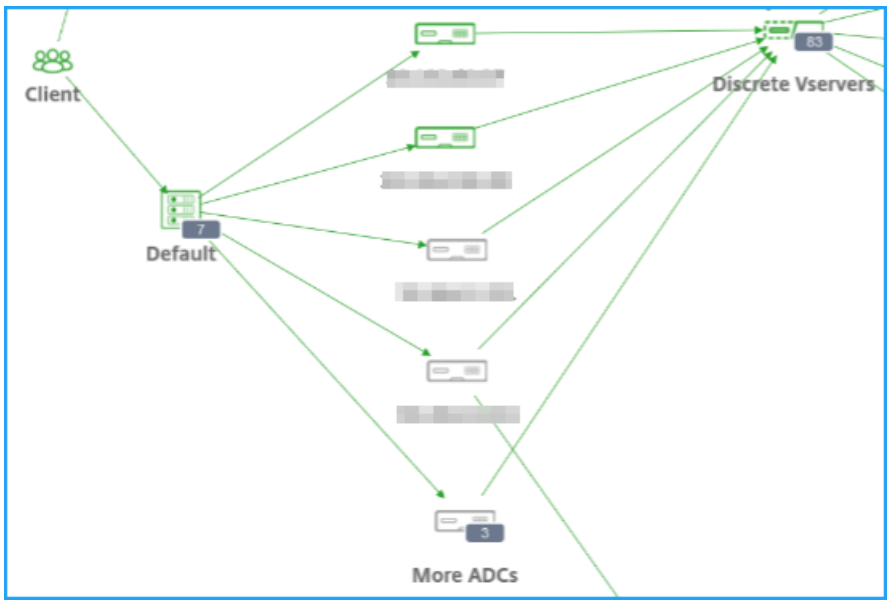


- **Client-Netzwerklatenz** : Gibt die durchschnittliche Clientnetzwerklatenz an.
- **Client 4xx Fehler** - Gibt die Gesamtzahl der 4xx Client-Fehler an.
- **Client-SSL-Fehler** - Gibt die gesamte Client-SSL-Fehler an.

Details zu Citrix ADC anzeigen

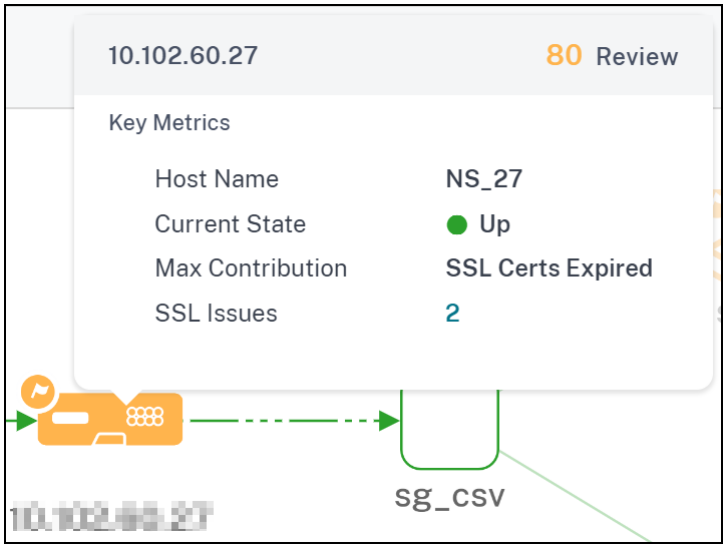
Mit dem Service-Diagramm können Sie Folgendes anzeigen:

- Das Rechenzentrum gruppiert mit den gesamten Citrix ADC-Instanzen
- Nur die 4 besten Citrix ADC-Instanzen mit niedriger Punktzahl aus jedem Rechenzentrum



Klicken Sie auf **Weitere ADCs**, um alle Citrix ADC-Instanzen anzuzeigen, indem Sie die entsprechenden Registerkarten “Kritisch”, “Prüfen”, “Gut” und “Nicht anwendbar” auswählen.

Bewegen Sie den Mauszeiger auf eine Citrix ADC-Instanz, um die Metriken anzuzeigen.



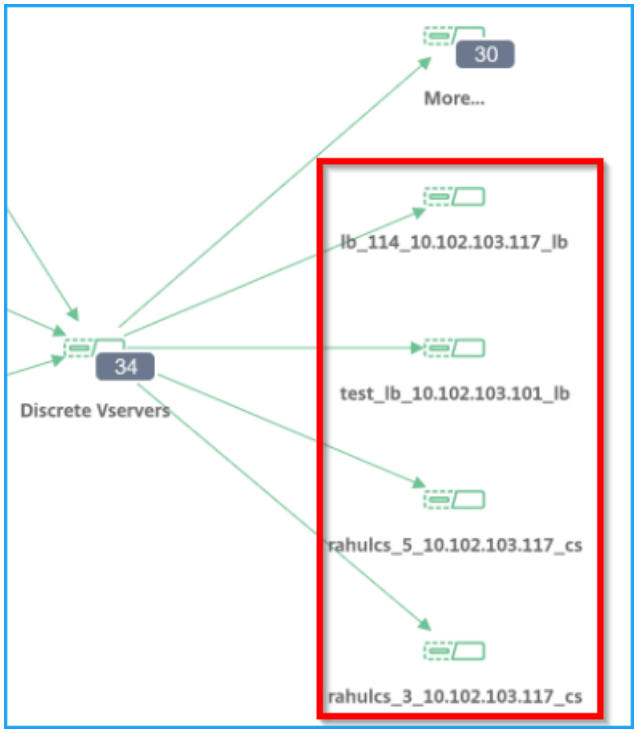
Sie können sehen:

- IP-Adresse und Punktzahl der Citrix ADC-Instanz
- **Hostname** — Gibt den Hostnamen an, der der Citrix ADC-Instanz zugewiesen ist
- **Aktueller Status** — Gibt den aktuellen Status der Citrix ADC-Instanz an, z. B. “Aufwärts”, “Heruntergefahren”, “Out-of-Service”.
- **Top Problem** — Gibt das höchste Problem an, das sich auf die aktuelle Citrix ADC Bewertung auswirkt.

Klicken Sie auf die **Citrix ADC-Instanz**, um Instanzdetails wie Instanzbewertung, Schlüsselmetriken und Probleme im Zusammenhang mit der ADC-Instanz anzuzeigen. Weitere Informationen finden Sie unter Anzeigen von Instanzdetails in Infrastructure Analytics.

Diskrete Anwendungen anzeigen

Das Service-Diagramm zeigt die Top 4 diskreten Anwendungen mit niedriger Punktzahl an.



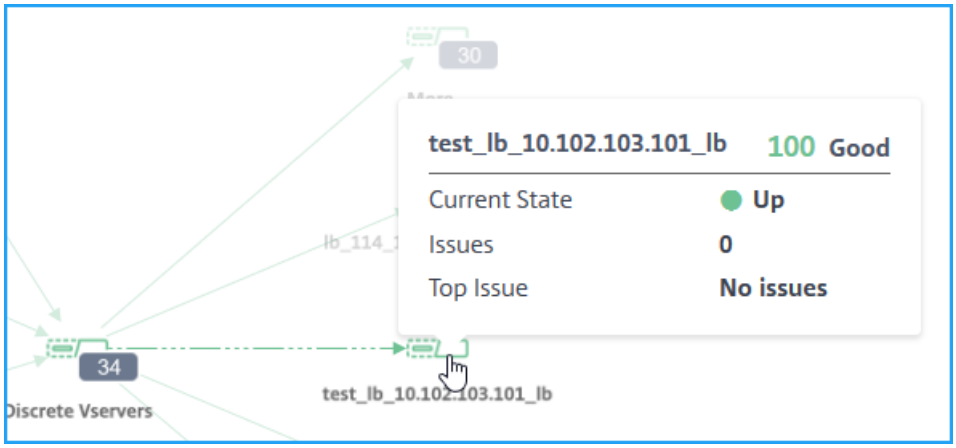
Beachten Sie, dass Sie die folgenden diskreten Anwendungen haben:

App-Name	Citrix ADC	AppScore	App-Status
App1	10.102.29.50	35 (Kritisch)	Bereit
App2	10.102.29.90	100 (Gut)	Nicht bereit
App 3	10.102.32.40	49 (Bewertung)	Bereit
App4	10.102.113.208	92 (Gut)	Nicht bereit
App5	10.102.25.25	86 (Gut)	Bereit
App6	10.102.29.41	77 (Gut)	Bereit
App7	10.102.29.102	41 (Bewertung)	Bereit

In diesem Szenario können Sie App1, App3, App6 und App 7 als die Top 4 Anwendungen mit niedriger Punktzahl im Service-Diagramm anzeigen.

In ähnlicher Weise können Sie auch die Top 4 Anwendungen mit niedriger Punktzahl für **Custom** und **Microservices** anzeigen.

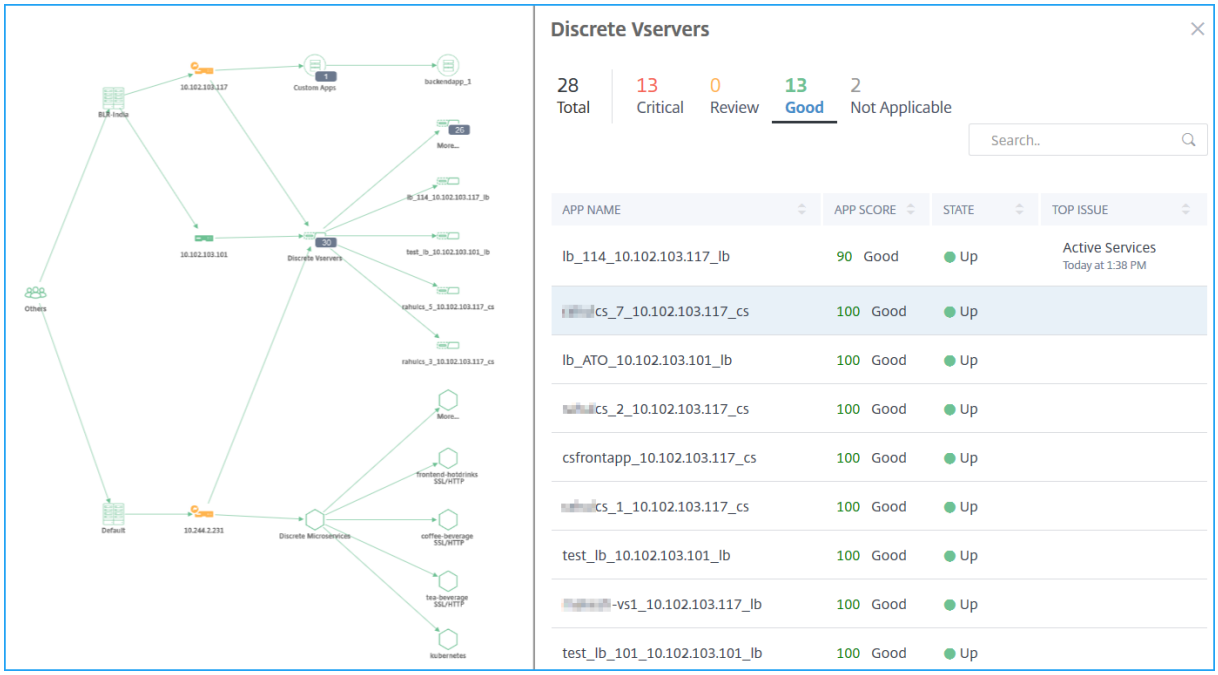
Bewegen Sie den Mauszeiger auf einen Dienst, um die Metrikinformationen anzuzeigen.



Sie können sehen:

- Name und Punktzahl der Anwendung
- **Aktueller Status** — Gibt den aktuellen Status der Anwendung an, z. B. “Nach oben” oder “Nach unten”
- **Probleme** — Gibt die Gesamtanzahl der für die Anwendung geltenden Probleme an
- **Top Problem** — Gibt das höchste Problem an, das sich auf die Gesamtbewertung der Anwendung auswirkt.

Klicken Sie auf **Mehr**, um alle diskreten Anwendungen anzuzeigen. Die Seite Diskreter virtueller Server wird wie in der folgenden Abbildung dargestellt angezeigt:

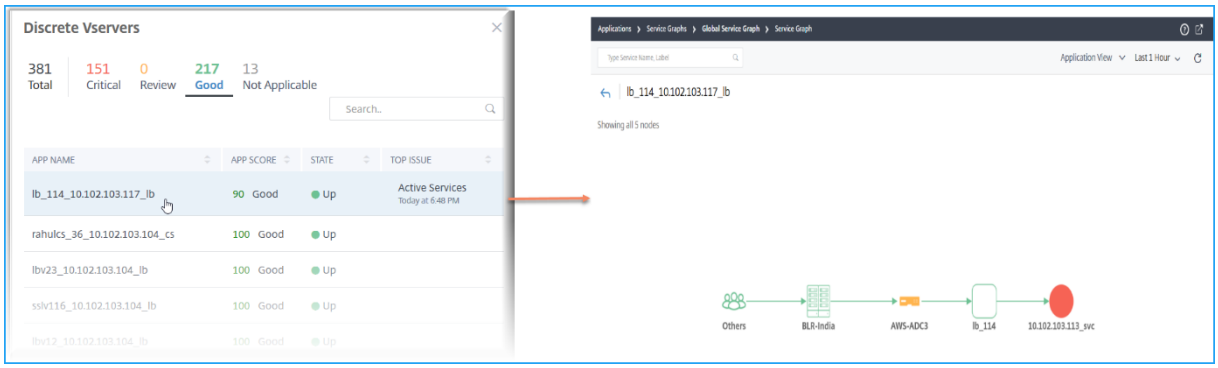


Die virtuellen Server werden entsprechend dem Status angezeigt.

- **Gesamt** — Gesamt diskrete Anwendungen

- **Kritisch** — App-Punktzahl liegt zwischen 0 und < 40
- **Bewertung** — App-Punktzahl liegt zwischen 40 und < 75
- **Gut** — App-Punktzahl ist > 75
- **Nicht anwendbar** — App ist nicht an einen virtuellen Server gebunden

Sie können auf die einzelnen Registerkarten klicken, um die virtuellen Server anzuzeigen. Wenn Sie auf eine Anwendung klicken, wird das Service-Diagramm für die ausgewählte Anwendung angezeigt.



Weitere Informationen finden Sie unter Service Graph für Anwendungen.

Anzeigen von Microservice-Anwendungen

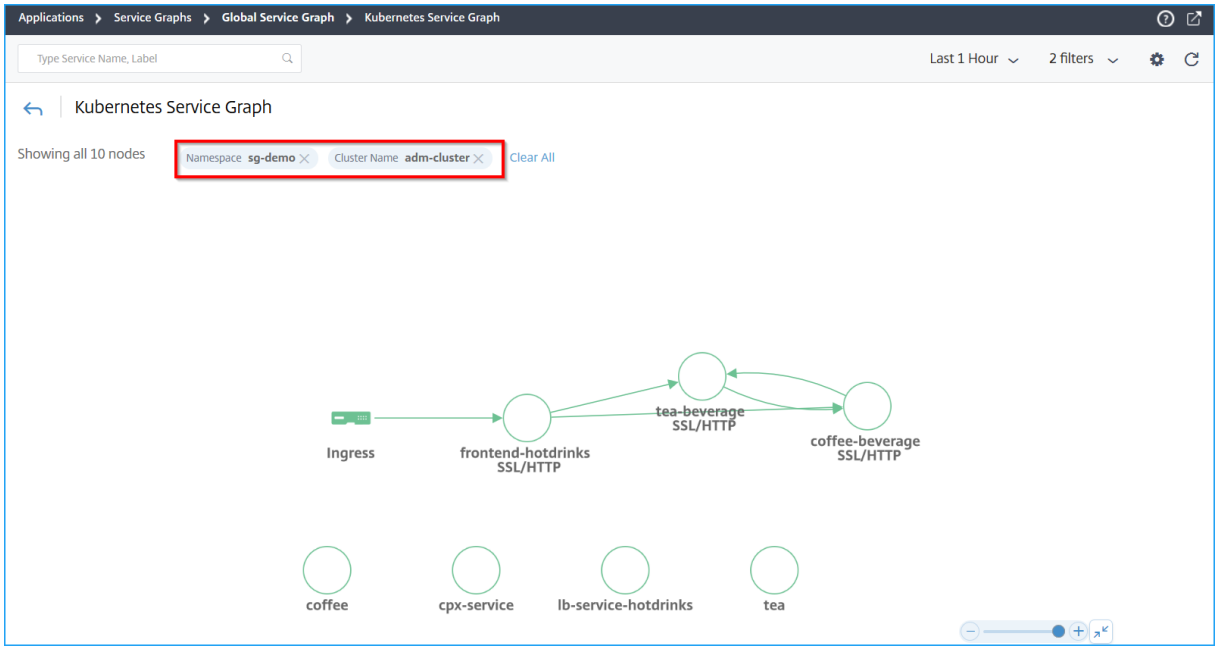
Das Dienstdiagramm zeigt auch alle Microservice-Anwendungen an, die zu den Kubernetes-Clustern gehören. Bewegen Sie den Mauszeiger auf einen Dienst, um die Metrikdetails anzuzeigen.

Sie können sehen:

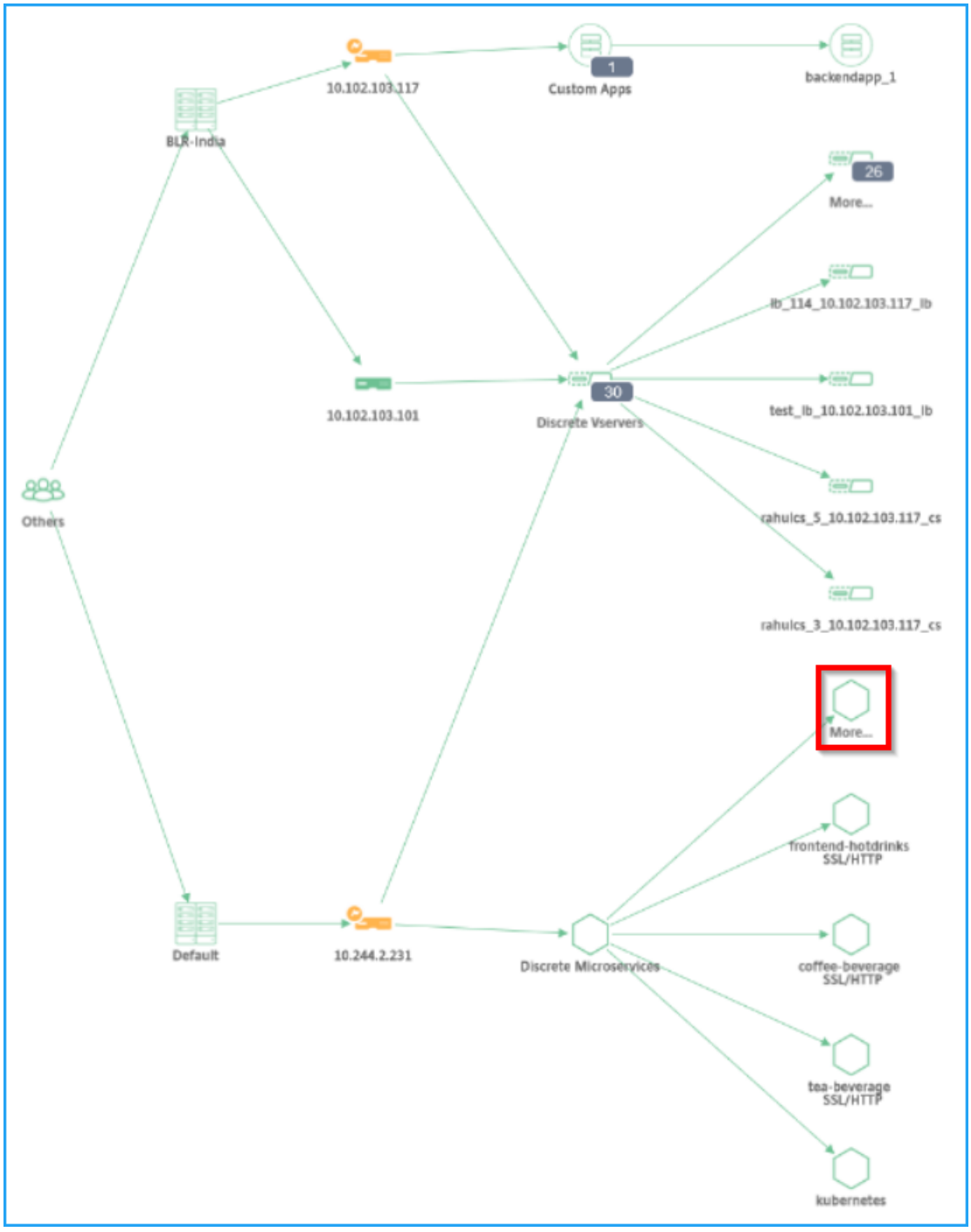
- Der Dienstname
- Das vom Dienst verwendete Protokoll wie SSL, HTTP, TCP, SSL über HTTP
- **Treffer** — Die Gesamtzahl der vom Dienst empfangenen Treffer
- **Service-Reaktionszeit** — Die durchschnittliche Antwortzeit, die vom Dienst genommen wird.

  (Antwortzeit = Client RTT + Anfrage letztes Byte — erstes Byte anfordern)
- **Fehler** — Die Gesamtzahl der Fehler wie 4xx, 5xx usw.
- **Datenvolumen** — Das Gesamtvolumen der vom Dienst verarbeiteten Daten
- **Namespace** — Der Namespace des Dienstes
- **Clustername** — Der Clustername, in dem der Dienst gehostet wird
- **SSL-Serverfehler** — Die gesamten SSL-Fehler des Dienstes

Wenn Sie auf einen Dienst klicken, wird das Kubernetes-Dienstdiagramm für den ausgewählten Dienst zusammen mit den angewendeten Dienstnamespace- und Clusternamenfiltern angezeigt.



Klicken Sie auf **Mehr**, um das Kubernetes-Dienstdiagramm anzuzeigen, das alle Dienste enthält. Weitere Informationen zum Kubernetes-Dienstdiagramm finden Sie unter Service-Diagramm für Cloud-native Anwendungen.



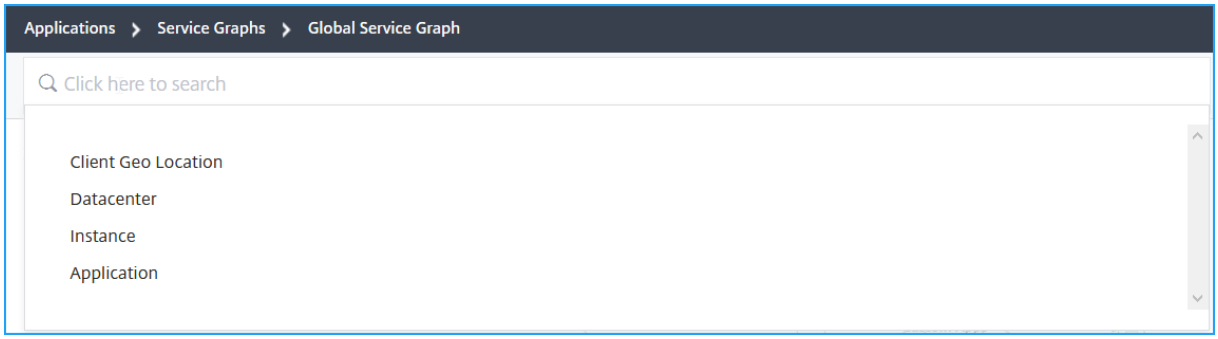
Suchleiste um Ergebnisse zu filtern

Sie können die Suchleiste verwenden, um Ergebnisse zu filtern. Als Administrator können Sie mit dieser Suchleiste schnell auf eine bestimmte Instanz/einen bestimmten Client/eine bestimmte Anwendung/Rechenzentrum eingrenzen, wenn Sie:

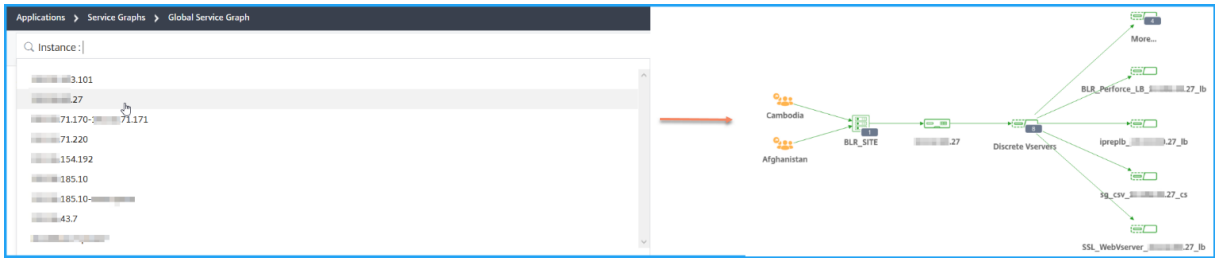
- Ein großes Unternehmen mit vielen Rechenzentren

- Viele Citrix ADC-Instanzen für jedes Rechenzentrum konfiguriert
- Viele Anwendungen konfiguriert, die über jede Citrix ADC-Instanz bereitgestellt oder darauf zugegriffen werden
- Clients, die von verschiedenen Standorten aus auf die Anwendung zugreifen

Platzieren Sie den Mauszeiger auf die Suchleiste und wählen Sie die Kategorie aus, in der Sie den Filter erstellen möchten.



Wenn Sie beispielsweise eine bestimmte ADC-Instanz anzeigen möchten, wählen Sie Instanz in der Suchleiste aus und wählen Sie die IP-Adresse der Instanz aus. Das globale Servicediagramm zeigt die ausgewählte Instanz und die zugehörigen Anwendungen, Rechenzentren und Kundenstandorte an.



StyleBooks

April 28, 2021

StyleBooks vereinfachen die Verwaltung komplexer Citrix ADC Konfigurationen für Ihre Anwendungen. Ein StyleBook ist eine Vorlage, mit der Sie Citrix ADC Konfigurationen erstellen und verwalten können. Sie können ein StyleBook zum Konfigurieren eines bestimmten Features von Citrix ADC erstellen oder ein StyleBook so entwerfen, dass Konfigurationen für eine Enterprise-Anwendungsbereitstellung wie Microsoft Exchange oder Lync erstellt werden.

StyleBooks passen gut zu den Prinzipien von Infrastructure-as-Code, die von DevOps-Teams praktiziert wird, wo Konfigurationen deklarativ und versionsgesteuert sind. Die Konfigurationen werden ebenfalls wiederholt und werden als Ganzes bereitgestellt. StyleBooks bieten folgende Vorteile:

- **Deklarativ**: StyleBooks werden in einer deklarativen statt zwingenden Syntax geschrieben. Mit StyleBooks können Sie sich auf die Beschreibung des Ergebnisses oder des "gewünschten Zustands" der Konfiguration konzentrieren und nicht auf die schrittweisen Anweisungen, wie Sie dies für eine bestimmte ADC-Instanz erreichen können. Citrix ADM berechnet den Unterschied zwischen dem vorhandenen Status auf einem ADC und dem von Ihnen angegebenen Zustand und nimmt die erforderlichen Änderungen an der Infrastruktur vor. Da StyleBooks eine deklarative Syntax verwenden, die in YAML geschrieben wird, können Komponenten eines StyleBook in beliebiger Reihenfolge angegeben werden, und Citrix ADM bestimmt die richtige Reihenfolge basierend auf den berechneten Abhängigkeiten.
- **Atomic**: Wenn Sie StyleBooks zum Bereitstellen von Konfigurationen verwenden, wird die vollständige Konfiguration bereitgestellt oder keine davon bereitgestellt. Dadurch wird sichergestellt, dass die Infrastruktur immer in einem konsistenten Zustand bleibt.
- **Versioniert**: Ein StyleBook hat einen Namen, einen Namensraum und eine Versionsnummer, die es eindeutig von jedem anderen StyleBook im System unterscheidet. Jede Änderung an einem StyleBook erfordert eine Aktualisierung seiner Versionsnummer (oder seines Namens oder Namensraums), um dieses eindeutige Zeichen beizubehalten. Das Versionsupdate ermöglicht es Ihnen auch, mehrere Versionen des gleichen StyleBook zu verwalten.
- **Composable**: Nachdem ein StyleBook definiert wurde, kann das StyleBook als Unit verwendet werden, um andere StyleBooks zu erstellen. Sie können vermeiden, häufige Konfigurationsmuster zu wiederholen. Außerdem können Sie Standardbausteine in Ihrer Organisation einrichten. Da StyleBooks versioniert sind, führen Änderungen an vorhandenen StyleBooks zu neuen StyleBooks, wodurch sichergestellt wird, dass abhängige StyleBooks niemals unbeabsichtigt unterbrochen werden.
- **App-Centric**: StyleBooks können verwendet werden, um die Citrix ADC Konfiguration einer vollständigen Anwendung zu definieren. Die Konfiguration der Anwendung kann mithilfe von Parametern abstrahiert werden. Daher können Benutzer, die Konfigurationen aus einem StyleBook erstellen, mit einer einfachen Schnittstelle interagieren, die darin besteht, einige Parameter zu füllen, um eine komplexe ADC-Konfiguration zu erstellen. Konfigurationen, die aus StyleBooks erstellt werden, sind nicht an die Infrastruktur gebunden. Eine einzelne Konfiguration kann somit auf einer oder mehreren ADC-Instanzen bereitgestellt werden und kann auch zwischen Instanzen verschoben werden.
- **Automatisch generierte Benutzeroberfläche**: Citrix ADM generiert automatisch Benutzeroberflächenformulare, die zum Ausfüllen der Parameter des StyleBook verwendet werden, wenn die Konfiguration mithilfe der Citrix ADM-GUI durchgeführt wird. StyleBook-Autoren müssen keine neue GUI-Sprache erlernen oder UI-Seiten und -Formulare separat erstellen.
- **API-gesteuert**: Alle Konfigurationsvorgänge werden über die Citrix ADM GUI oder über REST-APIs unterstützt. Die APIs können im synchronen oder asynchronen Modus verwendet werden. Zusätzlich zu den Konfigurationsaufgaben können Sie mit den StyleBooks APIs auch das Schema (Parameterbeschreibung) eines beliebigen StyleBook zur Laufzeit ermitteln.

Sie können ein StyleBook verwenden, um mehrere Konfigurationen zu erstellen. Jede Konfiguration wird als Konfigurationspaket gespeichert. Angenommen, Sie haben ein StyleBook, das eine typische HTTP-Load Balancing-Anwendungskonfiguration definiert. Sie können eine Konfiguration mit Werten für die Load Balancing-Entitäten erstellen und sie auf einer Citrix ADC-Instanz ausführen. Diese Konfiguration wird als Konfigurationspaket gespeichert. Sie können dasselbe StyleBook verwenden, um eine andere Konfiguration mit unterschiedlichen Werten zu erstellen und sie auf derselben oder einer anderen Instanz auszuführen. Für diese Konfiguration wird ein neues Konfigurationspaket erstellt. Ein Config Pack wird sowohl in ADM als auch auf der ADC-Instanz gespeichert, auf der die Konfiguration ausgeführt wird.

Sie können entweder Standard-StyleBooks verwenden, die im Lieferumfang von Citrix ADM enthalten sind, um Konfigurationen für Ihre Bereitstellung zu erstellen, oder eigene StyleBooks entwerfen und in Citrix ADM importieren. Sie können die StyleBooks verwenden, um Konfigurationen entweder mithilfe der Citrix ADM GUI oder mithilfe von APIs zu erstellen.

Dieses Dokument enthält die folgenden Informationen:

- So zeigen Sie StyleBooks an
- Standard-StyleBooks
- Für Geschäftsanwendungen entwickelte StyleBooks
- Benutzerdefinierte StyleBooks
- APIs in StyleBooks
- StyleBooks Grammatik

StyleBook-Gruppen

April 28, 2021

Citrix Application Delivery Management (ADM) gibt es zwei StyleBook-Gruppen. Sie sind die standardmäßigen StyleBooks und die benutzerdefinierten StyleBooks. Ob es sich um ein Standard- oder Benutzerdefiniertes StyleBook handelt, ein öffentliches oder ein privates StyleBook. In Citrix ADM können Sie alle StyleBooks anzeigen, die im System vorhanden sind, unabhängig vom Typ oder Sichtbarkeitsstatus. Sie können auch eine grafische Darstellung anzeigen, wie StyleBooks miteinander verbunden sind.

In diesem Dokument werden die verschiedenen Arten von StyleBooks erläutert. Außerdem werden die folgenden Aktionen erläutert, die Sie mit den StyleBooks von Citrix ADM ausführen können:

- Laden Sie ein benutzerdefiniertes StyleBook herunter und nehmen Sie Änderungen vor, oder erstellen Sie ein StyleBook basierend auf einem vorhandenen.
- ADM-StandardstyleBooks ausblenden.
- Löschen Sie ein benutzerdefiniertes StyleBook aus Citrix ADM.

- Fügen Sie den StyleBooks Tags hinzu.

Standard- und benutzerdefinierte StyleBooks

- **StandardstyleBooks** sind die StyleBooks, die mit Citrix ADM ausgeliefert werden, und sie ermöglichen es Ihnen, Konfigurationen zu erstellen, die Sie auf Ihren Citrix ADC-Instanzen bereitstellen können. Sie können Standard-StyleBooks nicht löschen, aber Sie können sie in der ADM-GUI ausblenden.
- **Benutzerdefinierte StyleBooks** sind Ihre eigenen StyleBooks, die Sie in Citrix ADM importiert haben.

Sowohl Standard- als auch benutzerdefinierte StyleBooks können entweder öffentlich oder privat sein.

Öffentliche und private StyleBooks

StyleBooks, aus denen Sie Konfigurationspakete erstellen können, können als **öffentliche** StyleBooks kategorisiert werden. Das heißt, sie stehen alle für Ihre direkte Verwendung zur Verfügung, um Konfigurationen über die Citrix ADM GUI und APIs zu erstellen.

Einige StyleBooks werden jedoch als Bausteine für andere StyleBooks verwendet. Solche StyleBooks sind als **privat**gekennzeichnet. Die privaten StyleBooks können nicht direkt verwendet werden, um Konfigurationspakete aus der Citrix ADM-Benutzeroberfläche zu erstellen. Sie können diese StyleBooks jedoch weiterhin auf Citrix ADM anzeigen und anzeigen. Um Ihre benutzerdefinierten StyleBooks als **privat**zu markieren, setzen Sie das private Attribut im StyleBook auf **true**. Sie können weiterhin private StyleBooks verwenden, um Konfigurationspakete mit den Citrix ADM APIs zu erstellen.

Beispiel für ein StyleBook, das als privat markiert ist

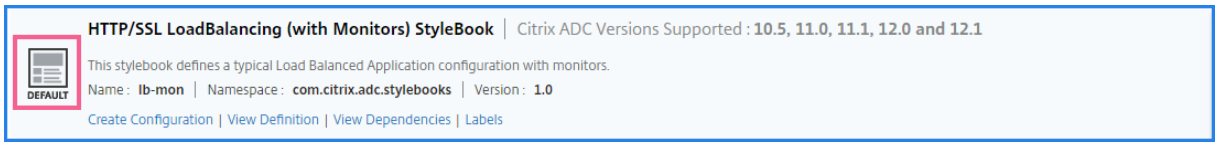
```
name: basic-lb-config
namespace: com.example.stylebooks
version: ”0.1”
display-name: Load Balancing Configuration
description: |
    This StyleBook defines a simple load balancing configuration and is
        a building block to build other load balancing configurations.
schema-version: ”1.0”
private: true
<!--NeedCopy-->
```


StyleBooks anzeigen

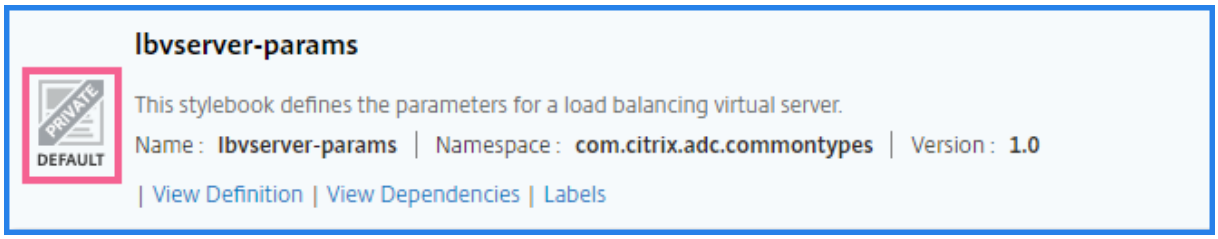
Die Anzahl der StyleBooks - sowohl Standard als auch Privat - nimmt in Citrix ADM zu. Möglicherweise möchten Sie nach dem bestimmten StyleBook suchen, auf das Sie zugreifen möchten. Sie können auch beide Arten von StyleBooks separat anzeigen.

Wenn Sie in Citrix ADM zu **Anwendungen** > **StyleBooks** navigieren, können Sie eine Liste der im System vorhandenen StyleBooks anzeigen.

Ein öffentliches Standard-StyleBook hat das folgende Symbol im Bedienfeld:

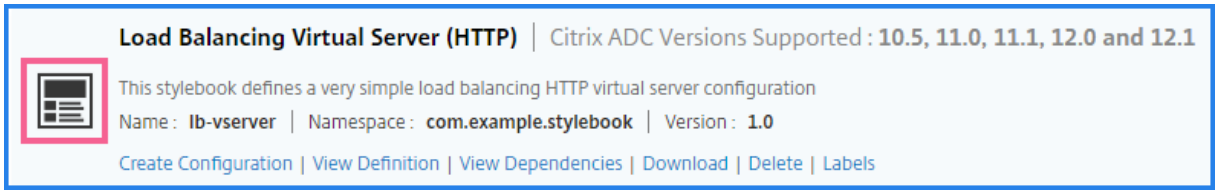


Während ein privates Standard-StyleBook ein Symbol hat, das es als privates StyleBook deklariert:

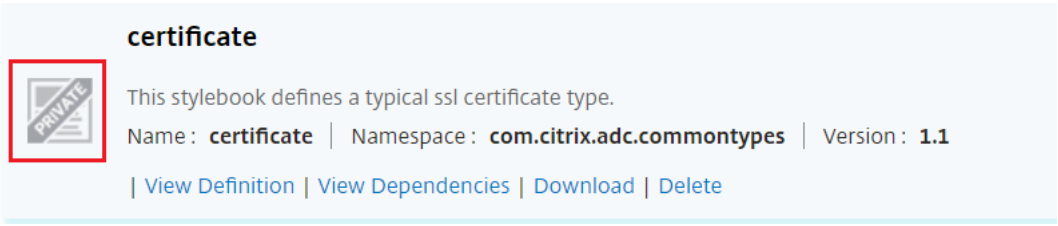


Während Sie die Definition und Abhängigkeiten eines privaten StyleBook anzeigen können, können Sie mit der GUI keine Konfigurationspakete aus einem privaten StyleBook erstellen. Der Hauptzweck eines privaten StyleBook besteht darin, es als Baustein für ein anderes StyleBook zu verwenden. Die Verwendung der Building-Blocks-Stylebooks fördert die Wiederverwendung gängiger Konfigurationsmuster.

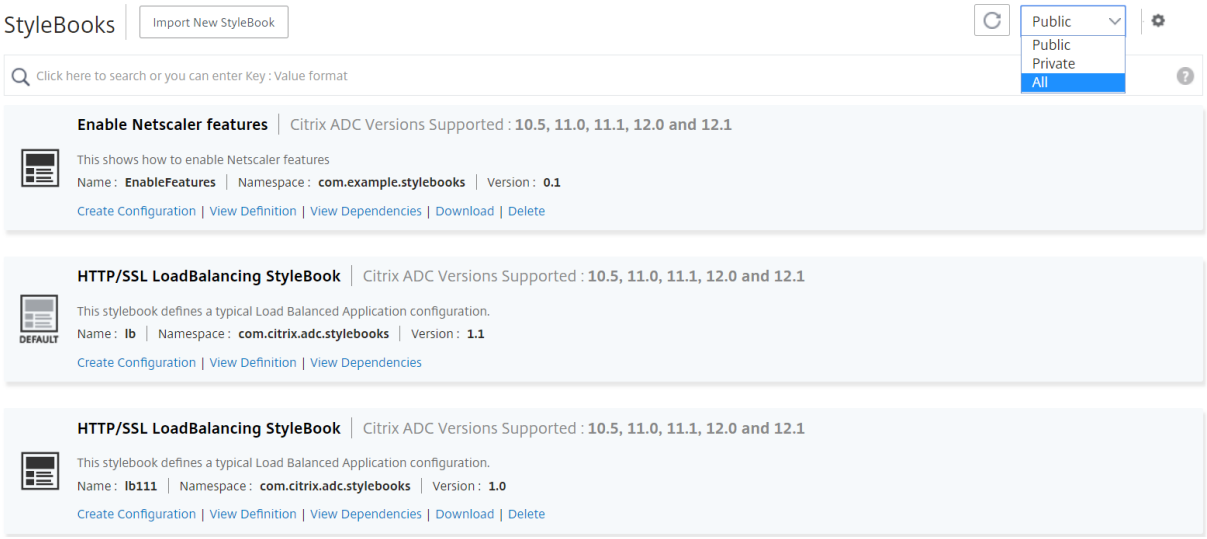
Ein benutzerdefiniertes öffentliches StyleBook hat ein anderes Symbol, wie in der folgenden Abbildung gezeigt:



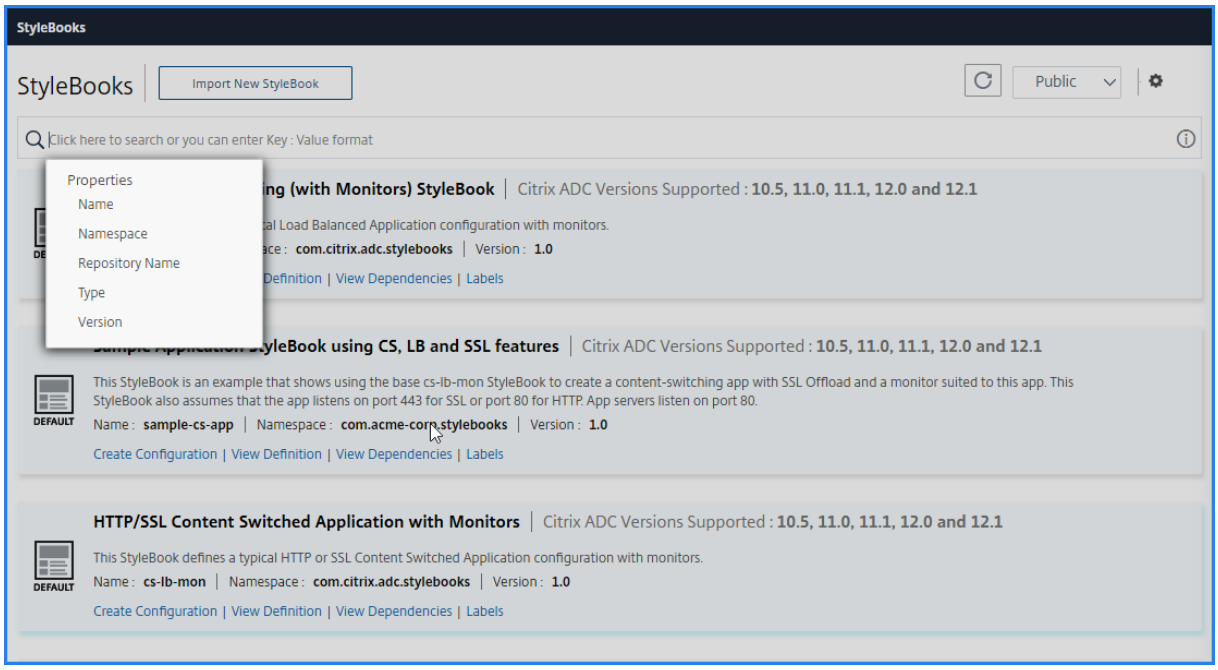
Während ein benutzerdefiniertes privates StyleBook mit diesem Symbol angezeigt wird:



Rechts oben auf der Seite sehen Sie eine Option, um den Typ der anzuzeigenden StyleBooks auszuwählen. Es gibt drei Optionen - alle, öffentliche oder private StyleBooks. Klicken Sie auf eine der Optionen.



Sie können auch nach einem bestimmten StyleBook suchen, indem Sie auf das Suchsymbol klicken. Sie können nach Namens-, Namens- und Versionsattributen oder einer Kombination dieser Optionen suchen. Bei der Suche wird die Groß- und Kleinschreibung nicht berücksichtigt.

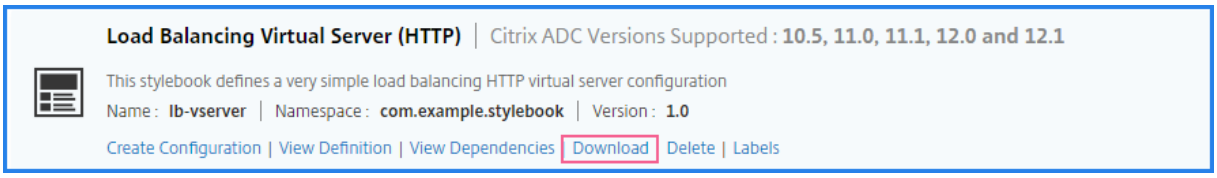


Benutzerdefinierte StyleBooks herunterladen

Um die benutzerdefinierten StyleBooks von Citrix ADM herunterzuladen, navigieren Sie zu **Anwendungen** > **StyleBooks** > **Configurations**. Aktivieren Sie in der Liste der StyleBooks, die auf der rechten

Seite angezeigt werden, die Option zum Herunterladen der benutzerdefinierten StyleBooks. Klicken Sie auf **Download**. Wenn das StyleBook über abhängige benutzerdefinierte StyleBooks verfügt, können Sie die abhängigen StyleBooks in das heruntergeladene Bundle aufnehmen.

> **Hinweis:**
>
> Sie können benutzerdefinierte StyleBooks herunterladen, die als öffentlich oder privat markiert sind.

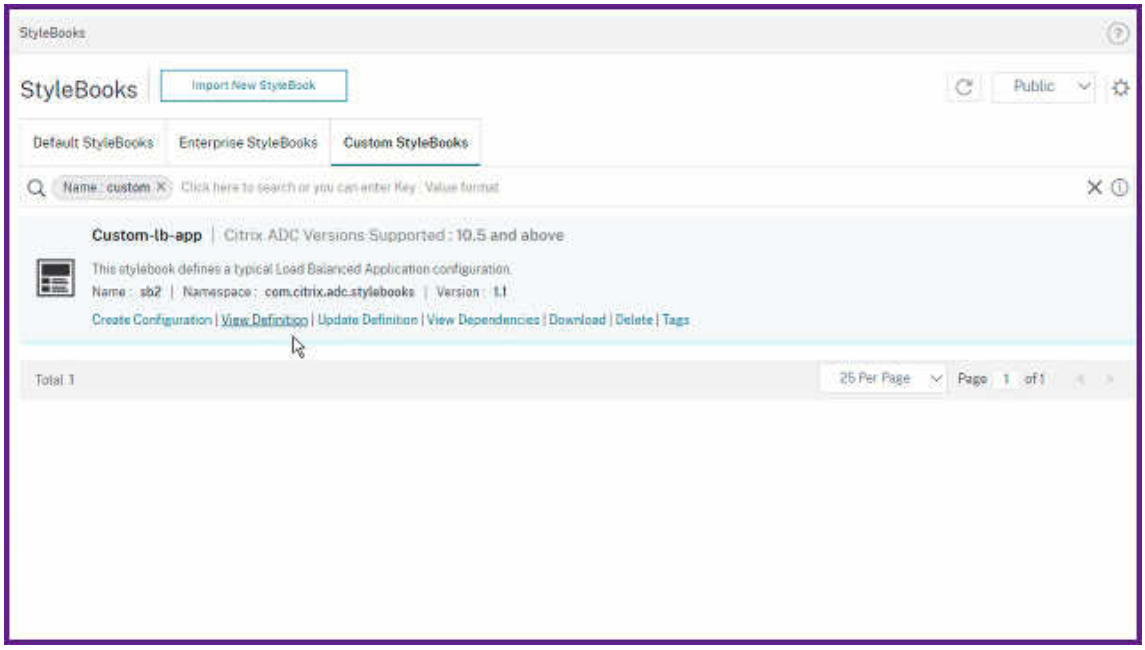


> **Hinweis**
>
> Citrix ADM Standard-StyleBooks können nicht heruntergeladen werden. Sie können ihre Definitionen und Abhängigkeiten einsehen. Klicken Sie dazu im StyleBook-Bedienfeld auf " **Definition anzeigen" und "Abhängigkeiten** anzeigen".

Aktualisieren Sie benutzerdefiniertes StyleBook

Sie können die benutzerdefinierten StyleBook-Definitionen von der ADM-GUI aus aktualisieren.

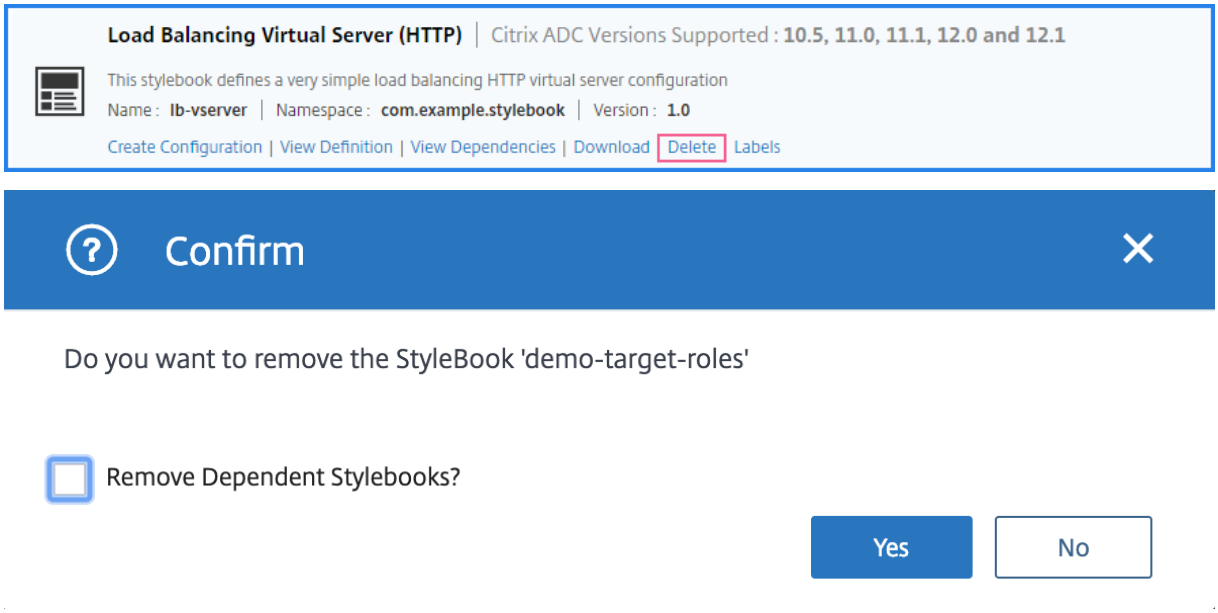
1. Navigieren Sie zu **Anwendungen > StyleBooks**.
2. Wählen Sie die Registerkarte **Benutzerdefinierte StyleBooks** aus.
3. Wählen Sie **Definition aktualisieren** für das StyleBook, das Sie aktualisieren möchten.
4. Aktualisieren Sie die Definition nach Bedarf und klicken Sie auf **Aktualisieren**.



5. Aktualisieren Sie die Seite, um die neuesten Änderungen zu sehen.

Benutzerdefinierte StyleBooks löschen

Sie können ein benutzerdefiniertes StyleBook auch löschen, indem Sie auf die Schaltfläche **Löschen** klicken. In einem Popup-Fenster werden Sie aufgefordert, zu bestätigen, ob Sie das StyleBook aus Citrix ADM entfernen möchten. Wenn das StyleBook andere benutzerdefinierte StyleBooks verwendet, können Sie diese StyleBooks entfernen, indem Sie das Kontrollkästchen aktivieren.



> **Hinweis**
>
> Löschen Sie kein benutzerdefiniertes StyleBook, wenn es abhängige StyleBooks in Citrix ADM hat. Andernfalls würde es die vorhandenen StyleBooks beschädigen.

Anzeigen von StyleBook-Abhängigkeiten

Eine wichtige und leistungsstarke Funktion von StyleBooks ist, dass sie als Bausteine für andere StyleBooks verwendet werden können. Sie können ein StyleBook in ein anderes StyleBook importieren. Ein importiertes StyleBook wird als Typ deklariert und von Komponenten oder Parametern des zweiten StyleBook verwendet. Sie können die vorhandenen Standard-StyleBooks in Citrix ADM untersuchen, um zu erfahren, wie ein StyleBook auf einem anderen StyleBook erstellt werden kann.

Mit Citrix ADM können Sie eine grafische Darstellung der Verbindung von StyleBooks anzeigen. Diese Darstellung ist besonders nützlich für komplexe StyleBooks, die mit anderen StyleBooks als Bausteine erstellt werden. Wenn Sie das Abhängigkeitsdiagramm betrachten, ist es möglich, die Beziehungen und Abhängigkeiten zwischen mehreren StyleBooks zu sehen.

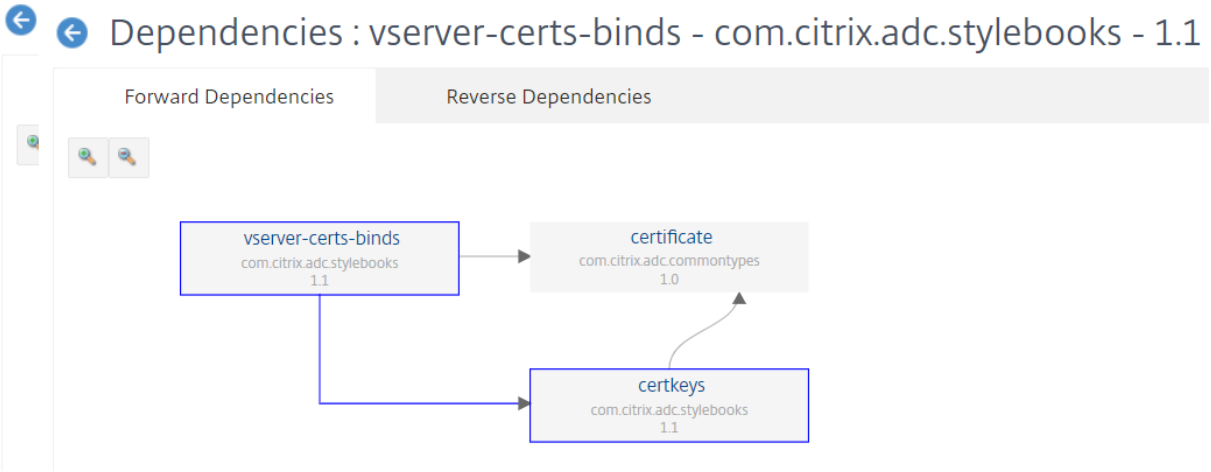
Ein von anderen StyleBooks verwendetes StyleBook kann nicht aus dem System entfernt werden, da es die vorhandenen StyleBooks beschädigen würde. Mithilfe der Abhängigkeitsdiagrammanzeige können Sie ermitteln, welche StyleBooks das Entfernen eines StyleBook verhindern.

So zeigen Sie StyleBook-Abhängigkeiten an

Navigieren Sie in Citrix ADM zu **Anwendungen** > **StyleBooks**. Auf der Seite StyleBooks werden alle StyleBooks angezeigt, die für die Verwendung in Citrix ADM verfügbar sind. Scrollen Sie nach unten und finden Sie Ihr StyleBook. Die **StyleBook-Kachel** zeigt Links zum Erstellen einer Konfiguration, zum Anzeigen der StyleBook-Definition und zum Anzeigen der StyleBook-Abhängigkeiten an. Klicken Sie **auf Abhängigkeiten anzeigen**.

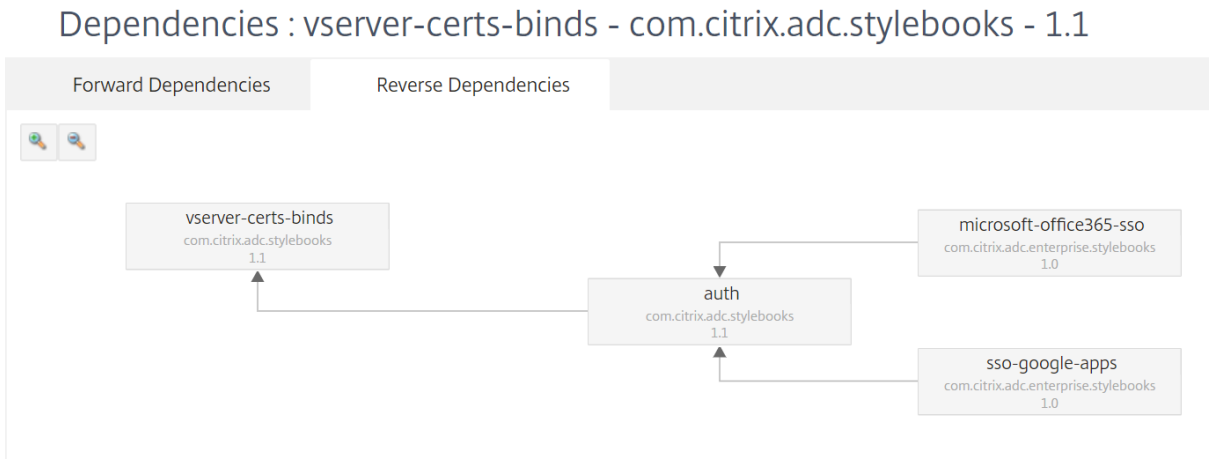
Vorwärtsabhängigkeiten

Auf der Registerkarte **Forward Dependencies** können Sie die verschiedenen Standard-StyleBooks anzeigen, die Ihr StyleBook verwendet. Folgen Sie den Pfeilen, um das StyleBook zu finden, das ein StyleBook verwendet. Wenn Sie mit der Maus auf einen der Pfeile zeigen, werden der Pfeil und die StyleBooks, die miteinander verbunden sind, hervorgehoben. Sie können auch auf die StyleBook-Namen klicken, um die Definition dieses StyleBook anzuzeigen.



Umgekehrte Abhängigkeiten

Auf **der Registerkarte Abhängigkeiten** können Sie die StyleBooks grafisch anzeigen, die Ihr StyleBook verwenden. Wenn Sie den Pfeilen folgen, können Sie sehen, dass alle StyleBooks in der Anzeige auf Ihr StyleBook zeigen. Einige StyleBooks verwenden möglicherweise direkt das StyleBook und einige StyleBooks verwenden das StyleBook möglicherweise über ein anderes StyleBook.



ADC-Konfiguration anhand des Konfigurationspakets überwachen

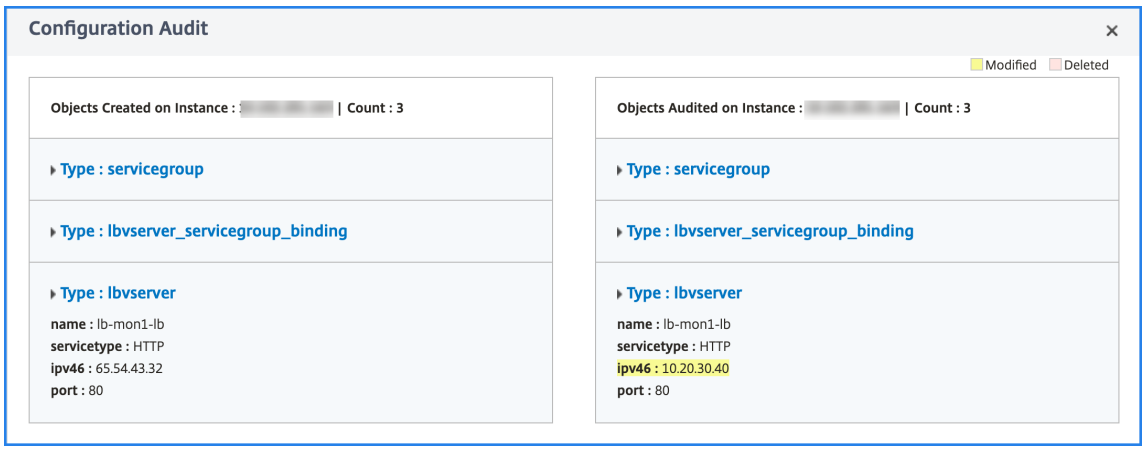
Sie können die von einem StyleBook-Konfigurationspaket vorgenommenen Änderungen mit der aktuellen ADC-Konfiguration vergleichen. Mit diesem Vergleich können Sie Folgendes tun:

- Erkennen Sie die Konfigurationsdrift zwischen StyleBook-Konfigurationspaket und ADC-Konfiguration.
- Identifizieren Sie alle geänderten und gelöschten Objekte im ADC, die die vom Konfigurationspaket vorgenommenen Änderungen nicht widerspiegeln.

Um die Änderungen des Konfigurationspakets mit der ADCs-Konfiguration zu vergleichen, führen Sie die folgenden Schritte aus.

1. Navigieren Sie zu **Anwendungen** > **StyleBooks** > **Konfigurationen**.
2. Klicken Sie auf **Konfigurationsüberwachung**.

   Auf der Seite “Konfigurationsüberwachung” werden die erstellten und überwachten Objekte angezeigt.

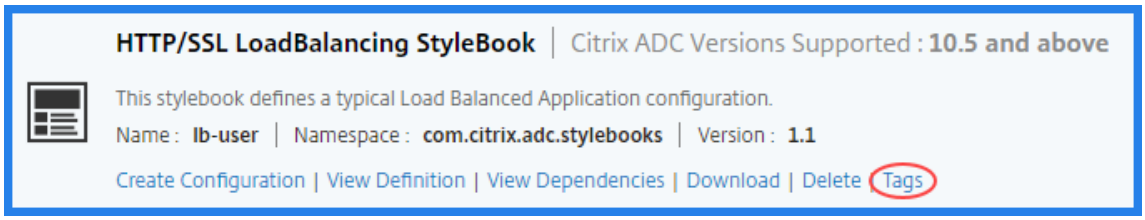


Erstellen Sie ein Tag für das StyleBook

Sie können jedem StyleBook in Citrix ADM Tags hinzufügen. Tags sind Schlüssel-Wert-Paare, mit denen Sie StyleBooks nach verschiedenen Kriterien gruppieren können. Sie können diese Tags verwenden, während Sie in Citrix ADM nach StyleBooks suchen oder filtern.

So fügen Sie dem StyleBook ein Tag hinzu:

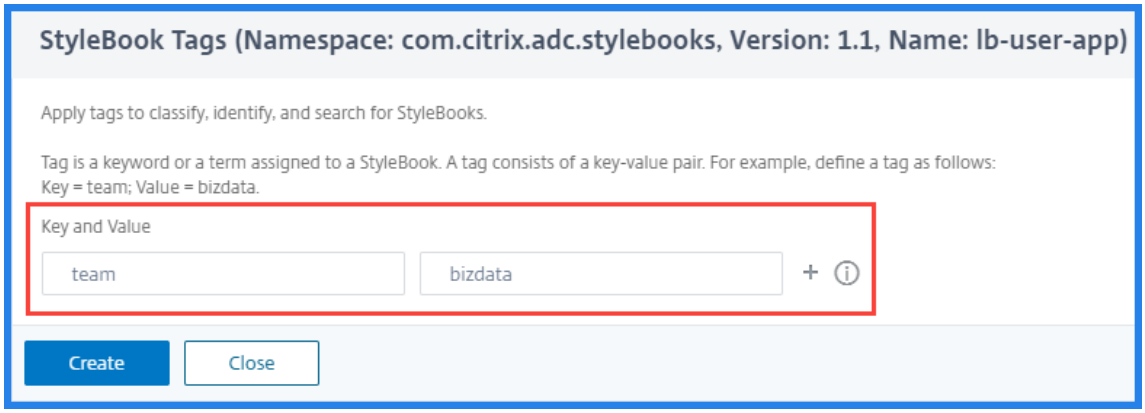
1. Navigieren Sie zu **Anwendungen** > **StyleBooks**.
2. Wählen Sie im StyleBook **Tags** aus, für das Sie Tags hinzufügen möchten.



   Sie können allen Arten von StyleBooks Tags hinzufügen.

3. Geben Sie die erforderlichen **Schlüssel-** und **Wert-Informationen** an, mit denen Sie das StyleBook filtern können.

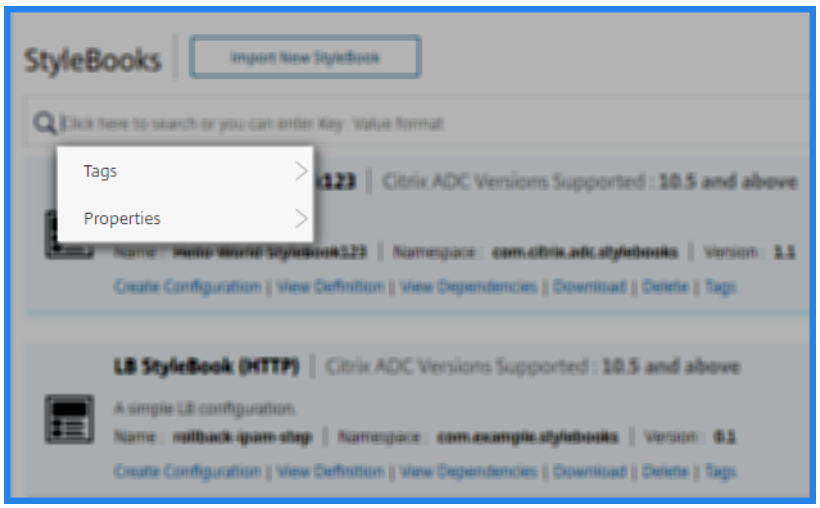
   Beispiel: Schlüssel=Team und Wert=BizData



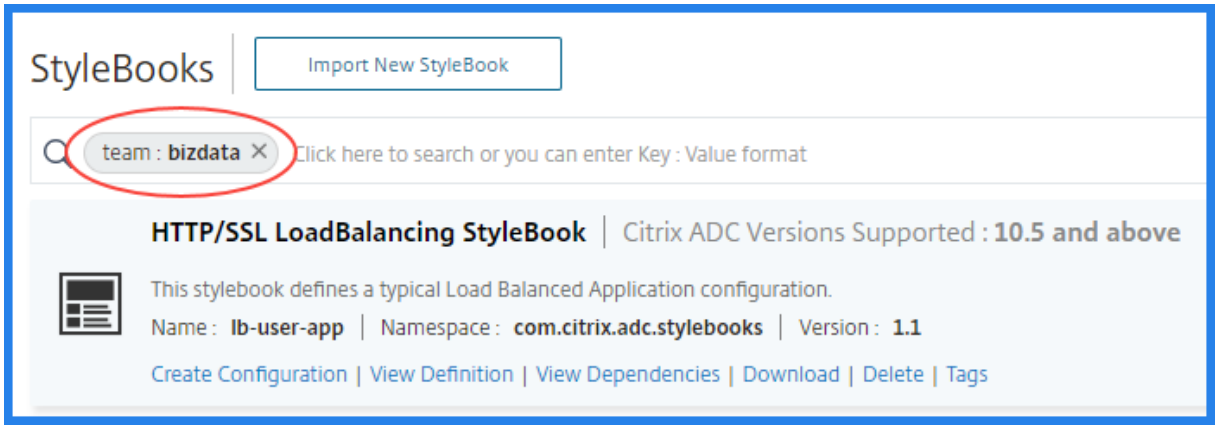
Um weitere Tags hinzuzufügen, klicken Sie auf **+**.

4. Klicken Sie auf **Erstellen**.

Um StyleBooks mithilfe von Tags zu filtern, klicken Sie in der Suchleiste auf **Tags** und wählen Sie Schlüssel und Wert aus der Liste aus. Die StyleBooks, die mit dem angegebenen Tag übereinstimmen, werden angezeigt.



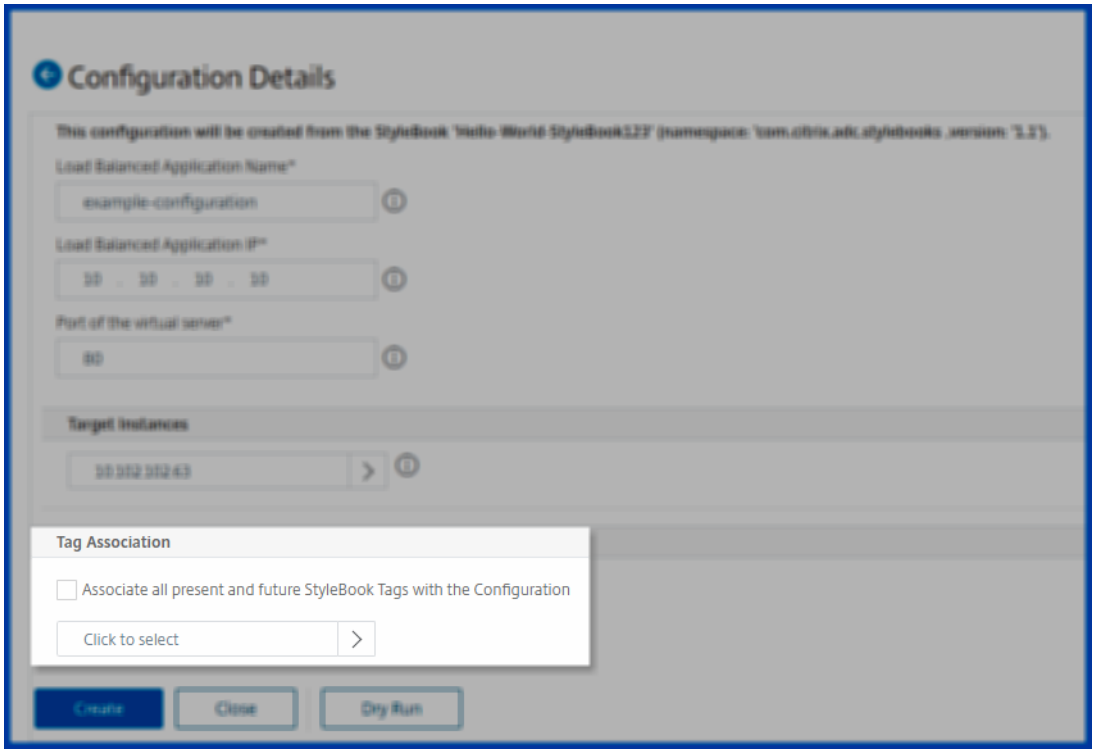
Im Folgenden finden Sie ein Beispiel für die StyleBooks, die ein Tag wo `key=team` und haben `value =bizdata`:



Sie können die StyleBook-Tags seinem Konfigurationspaket zuordnen. Sie können also die Konfigurationspakete mithilfe der StyleBook-Tags selbst durchsuchen.

Wenn Sie ein Konfigurationspaket erstellen, verwenden Sie eine der folgenden Optionen im Abschnitt **Tag-Zuordnung** :

- **Verknüpfen Sie alle gegenwärtigen und zukünftigen StyleBook-Tags mit der Konfiguration** — Diese Option ordnet alle StyleBook-Tags einem Konfigurationspaket zu. Es stellt auch sicher, dass Sie die neuen Tags verknüpfen, die Sie den StyleBooks in Zukunft hinzufügen könnten.
- **Tags auswählen** — Diese Option zeigt die Tags des ausgewählten StyleBook an. Sie können die erforderlichen StyleBook-Tags auswählen und einem Konfigurationspaket zuordnen.



Importieren und Synchronisieren von StyleBooks aus GitHub-Repository

April 28, 2021

Betrachten Sie ein Szenario, in dem Sie CI/CD-Prozesse für Ihre Entwicklung verwenden. Oder ein Szenario, in dem Sie den gesamten Anwendungsquellcode und die Bereitstellungsobjekte in GitHub verwalten.

Im GitHub-Repository haben Sie möglicherweise mehrere StyleBooks für die Bereitstellung der Citrix ADC Konfigurationen und die Verwaltung dieser StyleBooks erstellt. Diese StyleBooks sind auch in Citrix Applications and Delivery Management (ADM) erforderlich. Jetzt können Sie diese StyleBooks direkt in Citrix ADM importieren. Sie müssen sie nicht manuell von GitHub kopieren und dann in Citrix ADM hochladen oder die Dateien in ADM und GitHub manuell synchronisieren.

Sie können nun ein Repository in Citrix ADM definieren, das ein GitHub-Repository darstellt. Geben Sie die GitHub-Repository-URL und Ihren Benutzernamen und/oder Ihr API-Token an, das in GitHub erstellt wurde. Das bedeutet, dass nur autorisierte Benutzer, die ein gültiges Konto in GitHub haben, StyleBooks importieren und synchronisieren können.

Nachdem Sie das Repository erstellt haben, können Sie Citrix ADM mit Ihrem GitHub-Repository synchronisieren. Citrix ADM stellt eine Verbindung mit GitHub her und importiert StyleBooks, die in diesem Repository gefunden wurden. ADM validiert dann die StyleBooks und fügt sie der Liste der StyleBooks in Citrix ADM hinzu. StyleBooks werden Citrix ADM nicht hinzugefügt, wenn die Validierung fehlschlägt. Korrigieren Sie die Fehler und übertragen Sie aktualisierte Versionen in Ihr GitHub-Repository. Später können Sie versuchen, sie zu importieren oder erneut mit Citrix ADM zu synchronisieren.

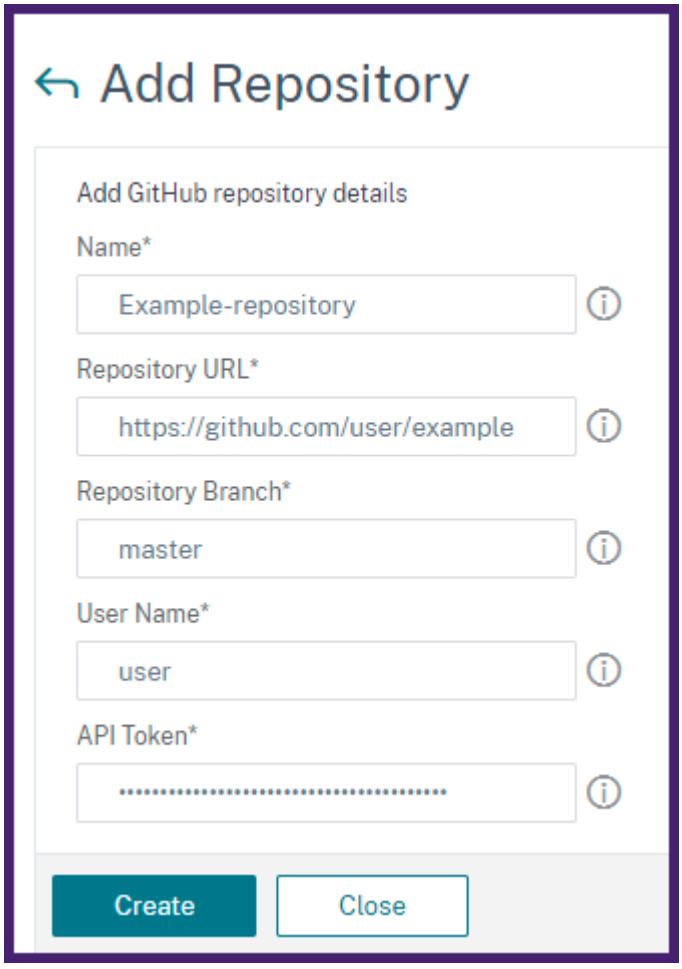
> **Hinweis**
>
> - StyleBooks-Dateien können aus jedem Zweig eines GitHub-Repositorys importiert und synchronisiert werden.
> - Sie können StyleBooks importieren und synchronisieren, denen auch abhängige StyleBooks zugeordnet sind.
> - Die Synchronisierung von StyleBooks aus einem GitHub-Repository muss manuell von der Citrix ADM GUI oder API initiiert werden. Das heißt, derzeit geschieht das Importieren und Synchronisieren von StyleBooks nicht automatisch basierend auf GitHub Commit-Aktivität.

Ein Repository hinzufügen und StyleBooks aus einem GitHub-Repository importieren

Bevor Sie beginnen, stellen Sie sicher, dass Sie über ein gültiges Konto in GitHub verfügen.

Sie können StyleBook-Dateien aus einem beliebigen Ordner im GitHub-Repository in ADM importieren.

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **StyleBooks** > **Repositories**.
2. Klicken Sie auf **Hinzufügen**. Geben **Sie im Fenster Repository hinzufügen** die folgenden Parameter ein:
   - **Name** - Geben Sie den Namen des Repositorys ein. Dieser Name kann mit dem Repository-Namen in GitHub oder einem anderen Namen identisch sein.
   - **Repository-URL** - Geben Sie die URL des GitHub-Reposit
   - **Benutzername** - Geben Sie den Benutzernamen ein, mit dem Sie auf das GitHub-Konto zugreifen.
   - **API-Token** - Dieses Token wird verwendet, um auf Ihr GitHub-Repository zuzugreifen. Informationen zum Erstellen von API-Token für Ihr GitHub-Repository finden Sie in der GitHub-Dokumentation fürErstellen persönlicher Zugriffstoken.
3. Klicken Sie auf **Erstellen**.



Das Repository wird in Citrix ADM erstellt.

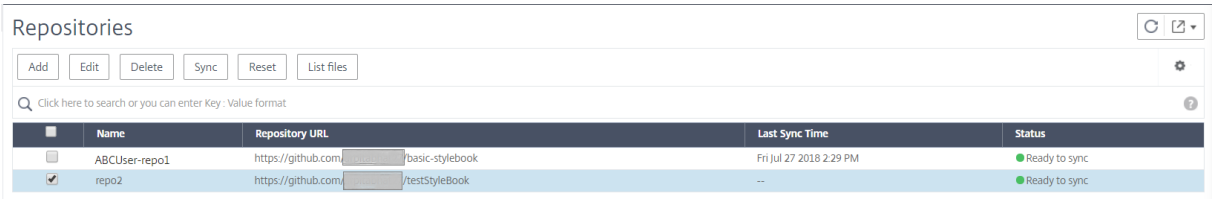
4. Um StyleBooks zu importieren oder zu synchronisieren, wählen Sie das Repository auf der Seite **Repositories** aus, und klicken Sie auf **Synchronisieren**.

Die anderen Aktionen, die Sie hier verwenden können, sind:

- **Bearbeiten:** Sie können die Repository-URL, den Benutzernamen und das API-Token bearbeiten.
- **löschen**. Sie können das Repository zusammen mit allen in Citrix ADM vorhandenen StyleBooks löschen, die zuvor aus diesem GitHub-Repository importiert wurden.

  > **Hinweis:**
  >
  > Sie können ein Repository nicht aus Citrix ADM löschen, wenn StyleBooks mit ConfigPacks verknüpft sind. Löschen Sie zunächst alle Konfigurationspakete dieser StyleBooks. Sie können das Repository später aus Citrix ADM entfernen, um die StyleBooks aus diesem Repository zu bereinigen.

- **Zurücksetzen**. Sie können alle StyleBooks in Citrix ADM synchronisiert aus diesem Repository entfernen, ohne den Repository-Eintrag tatsächlich aus Citrix ADM zu löschen.
- **Dateien auflisten**. Sie können eine Liste aller in Citrix ADM vorhandenen StyleBooks anzeigen, die aus dem GitHub-Repository stammen.



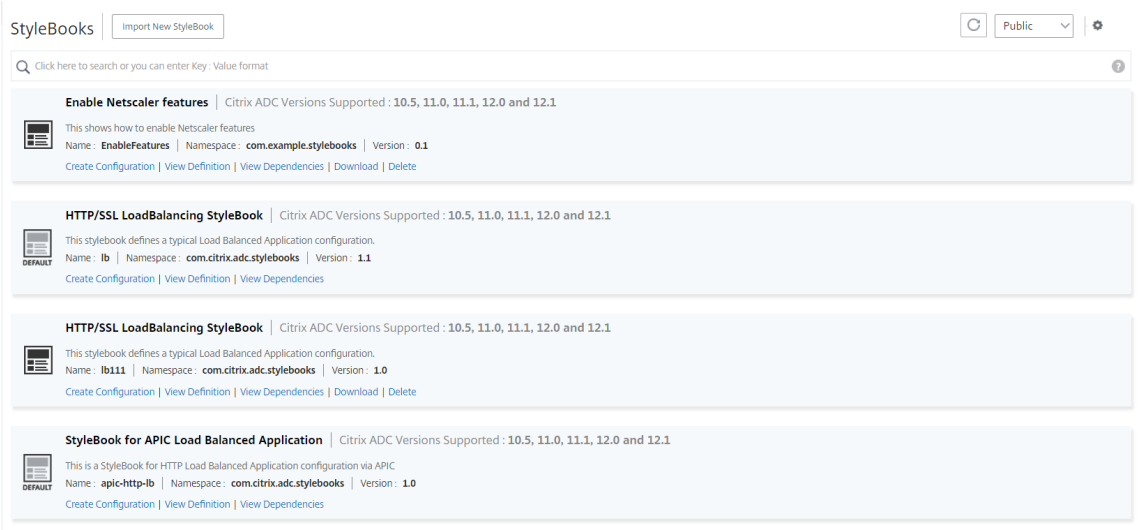
Standard-StyleBooks verwenden

April 28, 2021

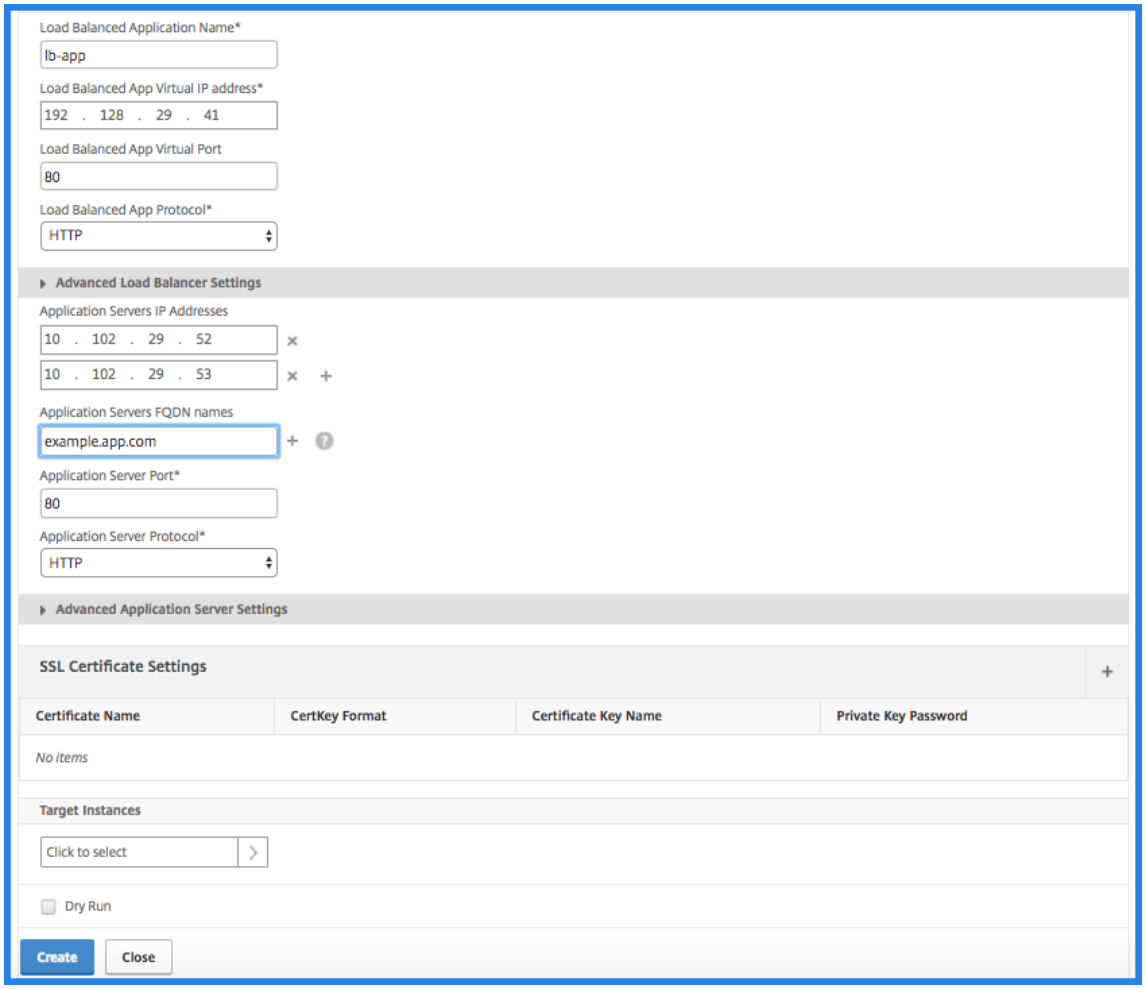
Ein Satz von Standard-StyleBooks wird zusammen mit Citrix Application Delivery Management (ADM) bereitgestellt. Wenn Sie ein standardmäßiges StyleBook verwenden, müssen Sie Werte für die Parameter im StyleBook angeben und die IP-Adressen der Citrix ADC-Instanzen auswählen, in denen Sie die Konfiguration ausführen möchten. Nachdem Sie die Konfiguration übermittelt haben, validiert Citrix ADM die von Ihnen angegebenen Parameterwerte, erstellt ein Diagramm der Konfiguration, stellt eine Verbindung mit den Citrix ADC-Instanzen her und führt die Konfiguration auf den Instanzen aus.

So erstellen Sie eine Konfiguration aus einem Standard-StyleBook

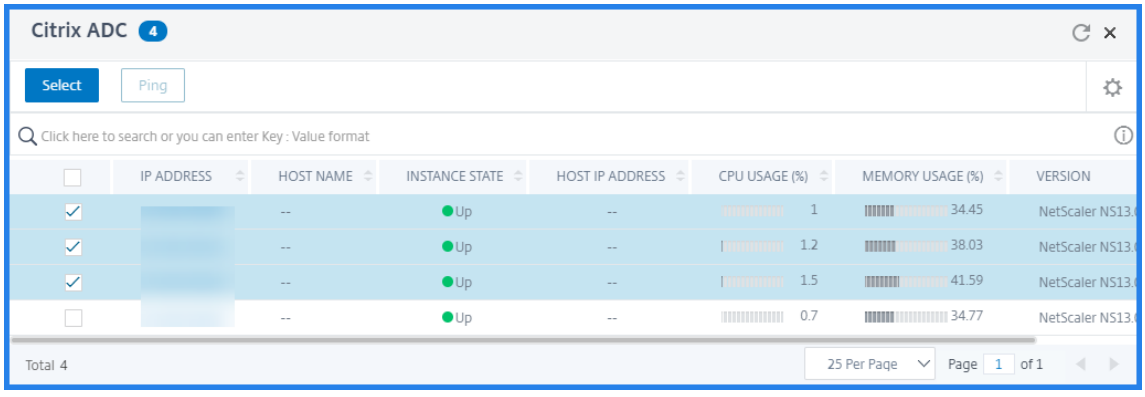
1. Navigieren Sie zu **Anwendungen** > **Konfigurationen > StyleBooks**. Auf der Seite “StyleBooks” werden alle StyleBooks in Citrix ADM angezeigt. Diese Liste enthält sowohl Standard- als auch benutzerdefinierte StyleBooks. Sie können den Namen des StyleBook in das Suchfeld eingeben und die **Eingabetaste** drücken. Andernfalls können Sie in der Liste nach unten scrollen, um das StyleBook zu finden.



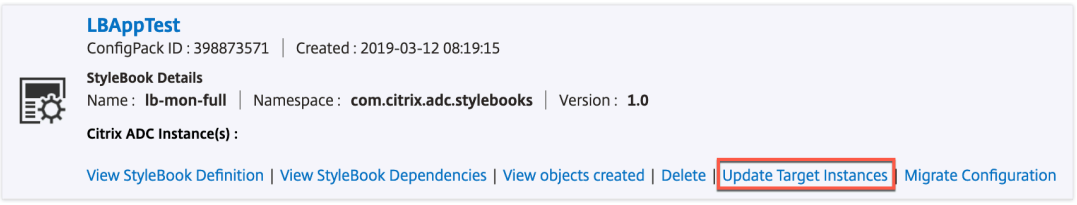
2. Klicken Sie auf **Konfiguration erstellen**. Geben Sie die erforderlichen Werte für die Parameter an.



3. Wählen Sie unter **Target Instanzen**die IP-Adresse der Citrix ADC-Instanz aus, auf der Sie die Konfiguration ausführen möchten. Sie können mehrere Instanzen auswählen, um diese Konfiguration auszuführen.

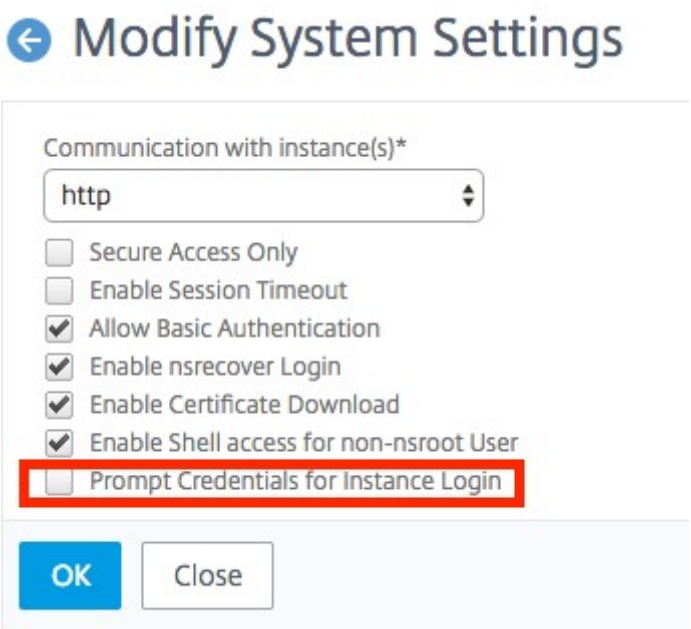


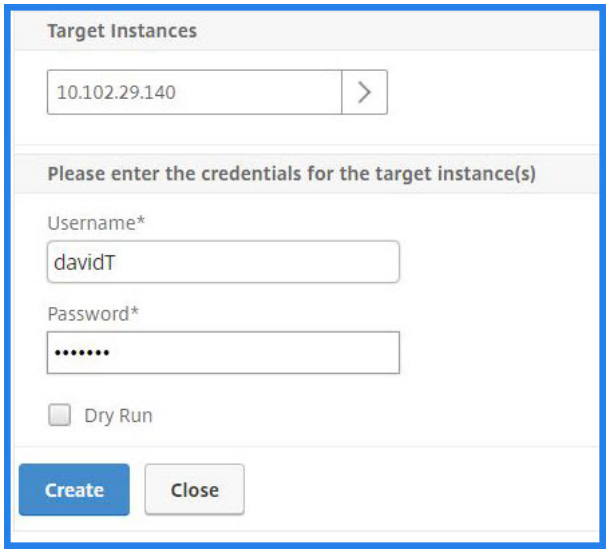
> **Hinweis:**
>
> Sie können auch ein Konfigurationspaket erstellen, ohne die Instanzen auszuwählen. Sie können das Konfigurationspaket später aktualisieren, indem Sie Zielinstanzen auswählen,

> auf denen Sie die Konfiguration bereitstellen möchten. In ähnlicher Weise können Sie alle Zielinstanzen eines Konfigurationspakets entfernen, ohne das Konfigurationspaket selbst zu entfernen.
>
> **Anwendungsfall**: Sie können Konfigurationspakete für Ihre Anwendungen erstellen, auch wenn Sie nicht auf die Instanzen zugreifen können.
>
> Die folgende Abbildung zeigt ein solches Konfigurationspaket, das erstellt wurde, ohne eine bestimmte Instanz auszuwählen. Klicken Sie auf **Zielinstanzen aktualisieren**, und wählen Sie dann Zielinstanzen aus, um diese Konfiguration bereitzustellen.
>
> 
>

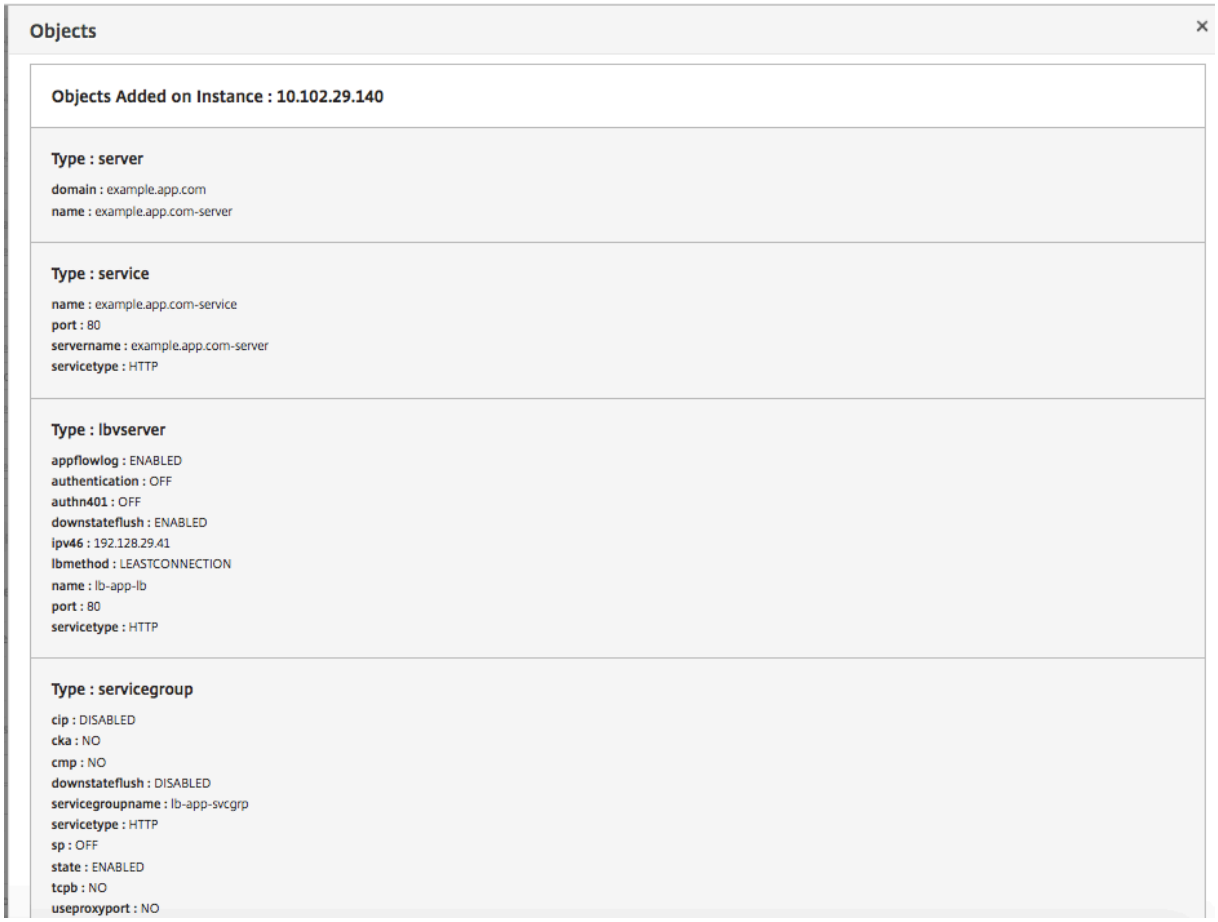
Wenn die Option **Anmeldeinformationen für Instanzanmeldung auffordern** in **Citrix ADM** > **System > Systemeinstellungenändern > Systemeinstellungenändern**aktiviert ist, werden Sie bei der Eingabe Ihrer Citrix ADC-Instanzanmeldeinformationen aufgefordert, wenn Sie die Konfigurationen auf der ausgewählte Citrix ADC-Instanzen. Andernfalls verwendet Citrix ADM die im Instanzprofil gespeicherten Instanzanmeldeinformationen für die Anmeldung bei der Instanz.

Anwendungsfall: Sie können Konfigurationspakete für Ihre Anwendungen erstellen, auch wenn Sie nicht auf die Instanzen zugreifen können.





Wenn Sie Ihre Konfiguration testen oder validieren möchten, bevor Sie sie auf der Citrix ADC-Instanz ausführen, wählen Sie **Dry Run** aus und klicken Sie dann auf **Create**. Wenn Ihre Konfiguration gültig ist, werden die Objekte angezeigt, die anhand der von Ihnen angegebenen Werte erstellt werden.



1. Deaktivieren Sie das Kontrollkästchen **Dry Run** und klicken Sie auf **Erstellen**, um das Konfigu-

rationspaket zu erstellen und die Konfiguration auf der Citrix ADC-Instanz auszuführen. Die von Ihnen erstellte StyleBook-Konfiguration (Konfigurationspaket) wird in der Liste der Konfigurationen angezeigt, wie unten gezeigt.

> **Hinweis**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC-Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

Sie können diese Konfiguration (Konfigurationspaket) jetzt mithilfe von Citrix ADM überprüfen, aktualisieren oder entfernen.

Alle Standard-StyleBooks ausblenden

April 28, 2021

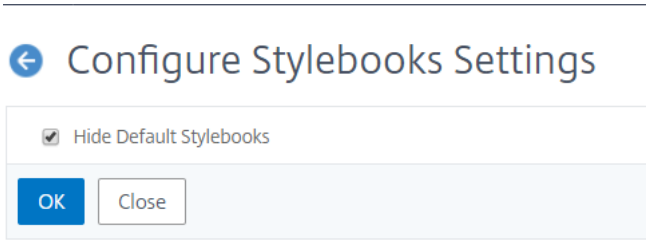
Citrix ADM listet alle im Citrix ADM-Ordnersystem vorhandenen StyleBooks auf. Die Liste der StyleBooks enthält Standard- und benutzerdefinierte StyleBooks, die sowohl privat als auch öffentlich sein können. Als Administrator möchten Sie möglicherweise alle Standard-StyleBooks ausblenden. Sie können Ihren Benutzern erlauben, nur benutzerdefinierte StyleBooks anzuzeigen und darauf zuzugreifen, die von Ihnen oder von den Benutzern erstellt wurden.

Mit Citrix ADM können Sie Ihre benutzerdefinierten StyleBooks anzeigen und alle Standard-StyleBooks ausblenden, die mit Citrix ADM geliefert werden. Eine neue GUI-Option wird zur Verfügung gestellt, in der Sie alle Standard-StyleBooks ausblenden können.

So blenden Sie alle Standard-StyleBooksaus:

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfigurationen > Einstellungen**.
2. Auf der Seite **Einstellungen** werden Informationen angezeigt, ob die Standard-StyleBooks für Benutzer sichtbar sind oder nicht.
3. Um die Standard-StyleBooks auszublenden, klicken Sie oben rechts auf das Bearbeitungssymbol.
4. Wählen Sie auf der Seite **StyleBook-Einstellungen konfigurieren** die Option **Standardstilbücher ausblenden** aus.

5. Klicken Sie auf **OK**.

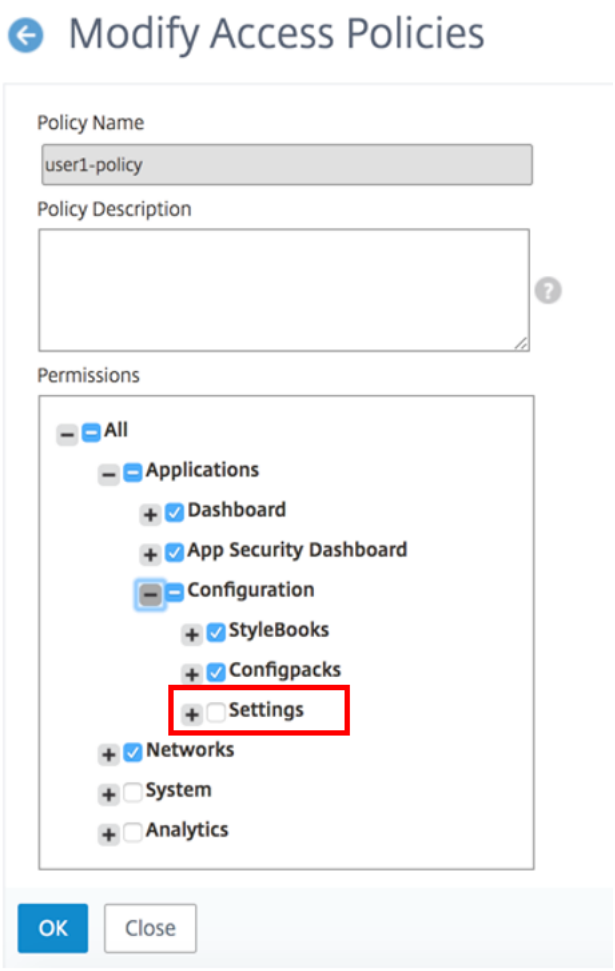


Die Seite **StyleBook-Einstellungen konfigurieren** ist für Benutzer weiterhin sichtbar, wenn Sie sich nicht dafür entschieden haben, die Seite mit der RBAC-Funktion auszublenden. Möglicherweise haben die Benutzer weiterhin die Option, die Standard-StyleBooks einblenden.

Um die Seite **“Configure StyleBook-Einstellungen** “ auszublenden, müssen Sie eine Richtlinie erstellen und diese Richtlinie denjenigen Benutzern zuweisen, die die standardmäßigen StyleBooks nicht sehen dürfen.

So erstellen Sie eine RBAC-Richtlinie:

1. Navigieren Sie in Citrix ADM zu **Konto** > **Benutzerverwaltung** > **Zugriffsrichtlinien**.
2. Klicken Sie auf **Hinzufügen**, um eine Richtlinie zu erstellen.
3. Geben Sie den Richtliniennamen ein.
4. Stellen Sie im Abschnitt **Berechtigungen** sicher, dass unter **Alle** > **Anwendungen** > **Konfiguration** > **Einstellungen** nicht ausgewählt ist, und klicken Sie auf **OK**.



Nach dem Erstellen von Richtlinien müssen Sie Rollen erstellen, jede Rolle an eine oder mehrere Richtlinien binden und Benutzergruppen Rollen zuweisen. Weitere Informationen zum Zuordnen von Richtlinien mit Benutzern finden Sie unterKonfigurieren der rollenbasierten Zugriffssteuerung.

Migrieren der Citrix ADC Anwendungskonfiguration mit dem StyleBooks Configuration Builder

April 28, 2021

Der StyleBooks Configuration Builder wird verwendet, um eine vorhandene ADC-Konfiguration auf StyleBooks zu migrieren. Diese Funktion automatisiert auch die Migration der Anwendungskonfiguration von einer Citrix ADC-Instanz zu einer anderen Instanz oder einer Autoscale-Gruppe.

Der Configuration Builder bietet eine strukturierte Anwendung StyleBook, die für alle Varianten der ADC-Konfiguration verwendet werden kann. Diese Funktion hilft Ihnen, mit StyleBooks zu beginnen, ohne umfassende Kenntnisse der StyleBooks-Grammatik und -Konstrukte zu haben. Andernfalls ist

das Wissen über StyleBooks Grammatik und Konstrukte notwendig, um ein StyleBook zu erstellen.

Der Configuration Builder erstellt auch ein Konfigurationspaket, das dieselbe ADC-Konfiguration für eine neue ADC-Instanz widerspiegelt. Mit diesem Konfigurationspaket kann die anfängliche ADC-Konfiguration von einer ADC-Instanz auf eine andere ADC-Instanz dupliziert werden. Die ursprüngliche Konfigurationsquelle kann eine der folgenden sein:

- **Eine Citrix ADC-Instanz:** Geben Sie die Instanz an, in der die zu duplizierende Anwendungskonfiguration gehostet wird.

  Der Configuration Builder konvertiert die ADC-Konfiguration in StyleBook und das Konfigurationspaket, auch wenn Sie die Zielinstanz nicht angeben. Sie können dieses Konfigurationspaket später verwenden, um die ADC-Konfiguration auf andere ADC-Instanzen zu migrieren.

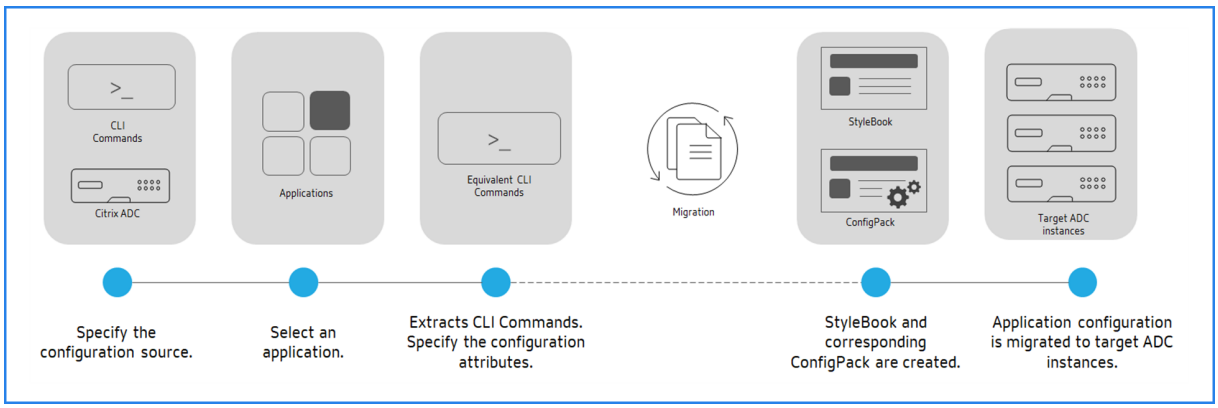
  Wenn es sich bei der Zielinstanz um eine Autoscale-Gruppe handelt, wird das Konfigurationspaket auf der Seite **Netzwerk > AutoScale-Gruppe** angezeigt. Auf der Registerkarte “ **Konfiguration** “.

- **Eine Reihe von CLI-Befehlen:** Fügen Sie die Konfiguration von`ns.conf` oder ein`Application config`.

Der Configuration Builder identifiziert die Liste der verschiedenen Anwendungen, die in die Quellkonfiguration eingebettet sind. Wenn Sie die von Ihnen gewünschte Anwendungskonfiguration auswählen, extrahiert der Configuration Builder den Satz von CLI-Befehlen für die ausgewählte Anwendung. Diese CLI-Befehle werden aus der Quellkonfiguration extrahiert. Außerdem werden die Bereitstellungs- und Konfigurationsattribute identifiziert, die möglicherweise Ihre Eingabe erfordern.

- **IP-Adresse/Ports** - Sie können die IP-Adresse und den Port der virtuellen Server, Dienste und Servicegruppenmitglieder von der ursprünglichen Konfiguration aus anzeigen und bearbeiten.
- **Konfigurationsdateien/Secrets** - Bei diesen Attributen können in der Quellkonfiguration angegebene Kennwörter oder Zertifikate sein.

Nachdem Sie die erforderlichen Informationen angegeben haben, starten Sie mit der Migration oder Duplizierung der Anwendungskonfiguration auf einer ADC-Zielinstanz.



Nach der Erstellung und Migration von Anwendungen wird ein Konfigurationspaket in Citrix ADM mit `adc_nitro_application` StyleBook erstellt. Dieses StyleBook wird basierend auf den ADC NITRO-Ressourcen erstellt. Dieses Konfigurationspaket stellt die Anwendungskonfiguration auf der ADC-Zielinstanz dar. Um das erstellte Konfigurationspaket anzuzeigen, navigieren Sie zu **Anwendungen** > **StyleBooks** > **Configurations**.

Unterstützte Citrix ADC Funktionen

Der StyleBook Configuration Builder erkennt und unterstützt die folgenden Citrix ADC Features in der Quellkonfiguration:

- Content Switching
- Lastausgleich
- Überwachen
- SSL-Offload
- Ratenbegrenzung
- Neuschreiben
- Responder
- Webanwendungs-Firewall (WAF)

Erstellen eines StyleBook zum Migrieren der Citrix ADC Anwendungskonfiguration

Das folgende Verfahren besteht darin, ein StyleBook zu erstellen, das die Citrix ADC Anwendungsmigration in Citrix ADM migriert:

1. Navigieren Sie zu **Anwendungen** > **StyleBooks** > **Konfigurationen**.
2. Klicken Sie auf **ADC-Konfiguration migrieren**.
3. Klicken Sie auf **Erste Schritte**.
4. Wählen **Sie unter Konfiguration angeben**die Konfigurationsquelle aus:
    - **Import aus einem ADC**: Mit dieser Option werden die aktiven Anwendungen auf der ausgewählten ADC-Instanz ermittelt.
    - **Import über CLI-Befehle**: Diese Option analysiert die CLI-Befehle und extrahiert die Anwendungen aus den CLI-Befehlen.
5. Geben Sie die **Quell-ADC-Instanz** an, von der Sie die Anwendungskonfiguration migrieren oder duplizieren möchten.

    Um die Anwendungskonfiguration auf eine Autoscale-Gruppe zu migrieren, stellen Sie sicher, dass die folgenden Informationen nicht in der Quellkonfiguration enthalten sind:

    - `IPset`

- Geräte-Profil
- Protokoll
- Port

6. Geben Sie die **Ziel-ADC-Instanz** an, zu der Sie die Anwendungskonfiguration migrieren oder duplizieren möchten.

   Um eine Anwendungskonfiguration auf eine Autoscale-Gruppe zu migrieren, wählen Sie die Autoscale-Gruppe aus der Liste aus.

7. In **Anwendung definieren,**

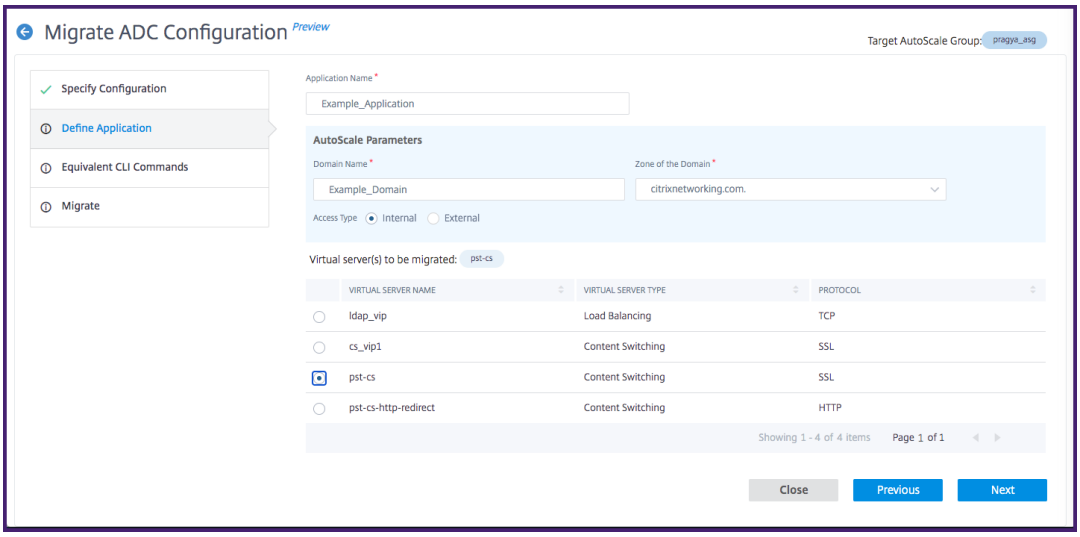
   a) Geben Sie **unter Anwendungsname**den Namen der Anwendung an.

   Wenn es sich bei der Zielinstanz um eine Autoscale-Gruppe handelt, geben Sie die folgenden Autoscale-Parameter an:

   - **Zugriffstyp** - Sie können die ADM-Lösung für die automatische Skalierung sowohl für externe als auch für interne Anwendungen verwenden. Wählen Sie den erforderlichen Anwendungszugriffstyp aus.
   - **Domänenname** - Geben Sie den Domänennamen einer Anwendung an. Diese Option ist nur anwendbar, wenn Sie Benutzerdefinierter FQDN-Typ auswählen.
   - **Zone der Domäne** - Wählen Sie den Zonennamen einer Anwendung aus der Liste aus. Diese Option ist nur anwendbar, wenn Sie Benutzerdefinierter FQDN-Typ auswählen.

     Dieser Domänen- und Zonenname leitet zu den virtuellen Servern in Azure um. Wenn Sie beispielsweise eine Anwendung in `app.example.com`hosten, ist `app`der Domänenname und `example.com`der Zonenname.

   b) Wählen Sie die virtuellen Server aus, die Sie migrieren möchten.



   c) Klicken Sie auf **Weiter**.

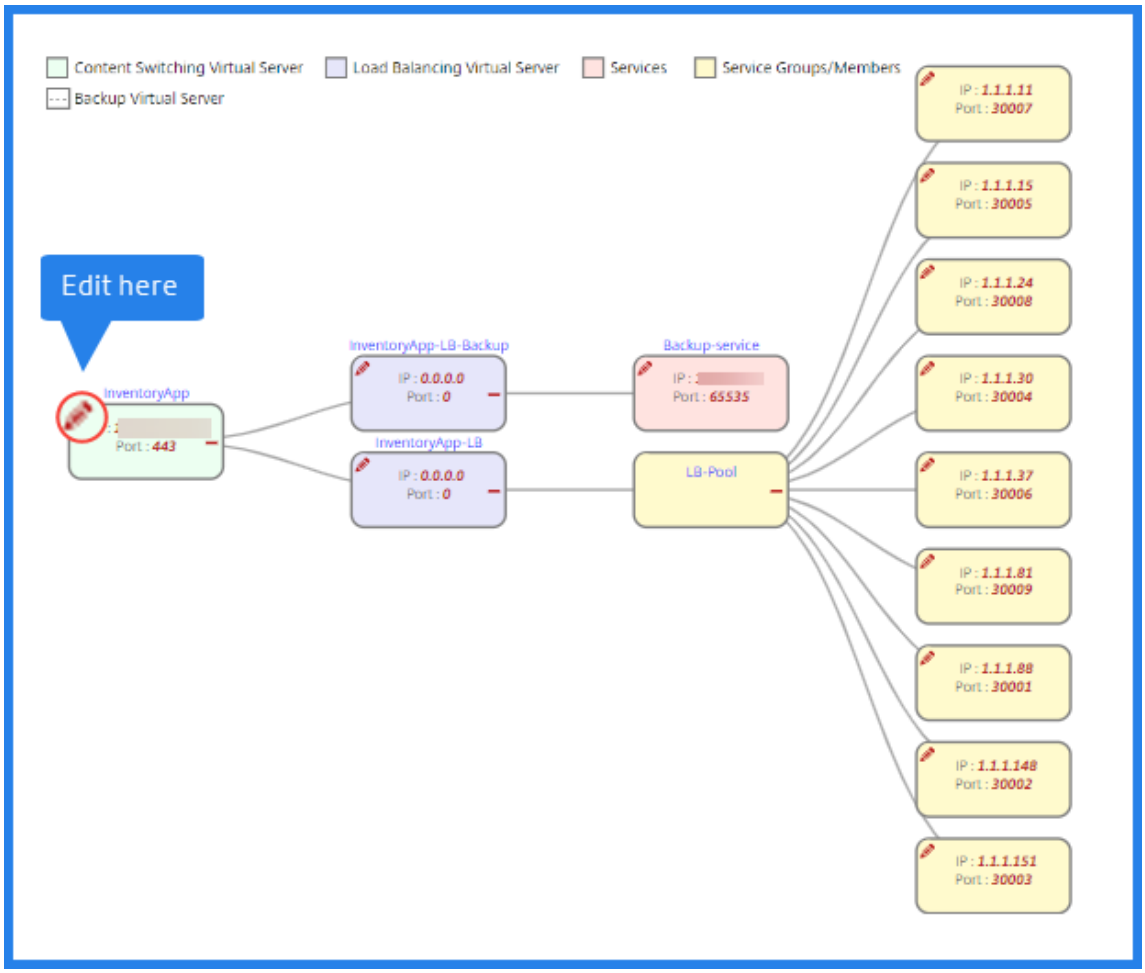
8. Überprüfen Sie unter **Äquivalente CLI-Befehle**die Befehle, und klicken Sie auf **Weiter**.

   Diese Befehle sind spezifisch für die ausgewählte Anwendungskonfiguration.

   > **Hinweis**
   >
   > Sie können die Konfiguration bei Bedarf auch hinzufügen oder bearbeiten.

9. In **Bereitstellungsattribute**können Sie die IP-Adresse und den Port der virtuellen Server, Dienste und Dienstgruppenmitglieder anzeigen und bearbeiten.

   Um die IP-Adresse und den Port zu bearbeiten, klicken Sie im Flussdiagramm auf das Bearbeitungssymbol des virtuellen Servers, Dienstes oder Dienstgruppenmitglieds.



   > **Hinweis**
   >
   > Wenn es sich bei der Zielinstanz um eine Autoscale-Gruppe handelt, ist die Bearbeitung der Front-End-IP-Adresse deaktiviert.

   Diese Registerkarte wird nur in den folgenden Fällen angezeigt:

   - Die Quell- und Zielinstanzen unterscheiden sich.

- Importieren Sie Konfigurationen mit CLI-Befehlen.

10. Geben Sie **unter Konfigurationsattribute**die erforderlichen Details an, und klicken Sie auf **Weiter**.

    Auf dieser Registerkarte werden die Geheimnisse wie Schlüssel zum Entschlüsseln von Kennwörtern und Zertifikaten aufgeführt.

    > **Hinweis**
    >
    > Bevor Sie mit der Migration beginnen, werden die verpassten oder nicht unterstützten Konfigurationen auf einer der folgenden Registerkarten angezeigt:
    >
    > - **Nicht unterstützte Konfigurationen**
    > - **Nicht unterstützte globale Konfigurationen**
    >
    > Um diese Konfigurationen erfolgreich zu migrieren, müssen Sie die fehlenden oder nicht unterstützten Konfigurationen separat auf die Zielinstanz anwenden. Klicken Sie auf **Weiter**.

11. Klicken Sie in **Migrate**auf **Migrate**.

Einschränkungen

- Die benannten Ausdrücke, die in der Quellinstanz `responderhtmlpages`erwähnt werden, werden nicht identifiziert. Stellen Sie sicher, dass Sie die benannten Ausdrücke und `responderhtmlpages`die Zielinstanz vor der Migration konfigurieren.
- Wenn die Quelle eine Konfiguration für die Bindung `servicegroup`und Überwachung wie folgt hat:

  `bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>`

  Der folgende Fehler wird angezeigt:

```
CLI Command conversion failed: 100 - No such command [{
 "errorcode": 1090, "message": "No such argument [XXX]", "
    severity": "ERROR"  }
]
<!--NeedCopy-->
```

  Dieser Fehler tritt auf, weil Citrix ADC die Bindung zwischen Dienstgruppe und Monitor in einem ungültigen Format speichert. Dieses Problem wurde von Citrix ADC 12.1.52.15 Build behoben.

SSO Google Apps StyleBook

April 28, 2021

Google Apps ist eine Sammlung von Cloud-Computing-, Produktivitäts- und Kollaborationstools, Software und Produkten, die von Google entwickelt werden. Mit Single Sign-On (SSO) können Benutzer auf alle ihre Enterprise-Cloud-Anwendungen zugreifen, einschließlich Administratoren, die sich bei der Admin-Konsole anmelden, indem sie sich einmal für alle Dienste mit ihren Enterprise-Anmeldeinformationen anmelden.

Mit dem Citrix Application Delivery Management (ADM) SSO Google Apps StyleBook können Sie SSO für Google Apps über Citrix ADC-Instanzen aktivieren. Das StyleBook konfiguriert die Citrix ADC-Instanz als SAML-Identitätsanbieter für die Authentifizierung von Benutzern für den Zugriff auf Google Apps.

Das Aktivieren von SSO für Google-Apps in einer Citrix ADC-Instanz mit diesem StyleBook führt zu den folgenden Schritten:

1. Konfigurieren des virtuellen Authentifizierungsservers
2. Konfigurieren einer SAML-IdP-Richtlinie und eines Profils
3. Binden der Richtlinie und des Profils an den virtuellen Authentifizierungsserver
4. Konfigurieren eines LDAP-Authentifizierungsservers und einer Richtlinie für die Instanz
5. Binden des LDAP-Authentifizierungsservers und der Richtlinie an den virtuellen Authentifizierungsserver, der auf der Instanz konfiguriert ist

Konfigurationsdetails:

In der folgenden Tabelle sind die minimal erforderlichen Softwareversionen aufgeführt, damit diese Integration erfolgreich funktioniert. Der Integrationsprozess unterstützt auch höhere Versionen derselben.

Produkt	Erforderliche Mindestversion
Citrix ADC	Version 11.0, Advanced/Premium Lizenz

In den folgenden Anweisungen wird davon ausgegangen, dass Sie bereits die entsprechenden externen und internen DNS-Einträge erstellt haben, um Authentifizierungsanfragen an eine von Citrix ADC überwachte IP-Adresse weiterzuleiten.

Bereitstellen von SSO Google Apps StyleBook-Konfigurationen:

Die folgende Aufgabe unterstützt Sie bei der Bereitstellung des Microsoft SSO Google Apps StyleBook in Ihrem Unternehmensnetzwerk.

So stellen Sie SSO Google Apps StyleBook bereit

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfigurationen** > **StyleBooks**. Auf der Seite StyleBooks werden alle StyleBooks angezeigt, die für die Verwendung in Citrix ADM verfügbar sind. Scrollen Sie nach unten und suchen Sie **SSO Google Apps StyleBook**. Klicken Sie auf **Konfiguration erstellen**.
2. Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
3. Geben Sie Werte für die folgenden Parameter ein:
   a) **Anwendungsname**. Name der SSO-Google-Apps-Konfiguration, die in Ihrem Netzwerk bereitgestellt werden soll.
   b) **Authentifizierung Virtuelle IP-Adresse**. Virtuelle IP-Adresse, die vom virtuellen Citrix ADC AAA-Server verwendet wird, an den die SAML-IdP-Richtlinie für Google Apps gebunden ist.
   c) **SAML-Regelausdruck**. Standardmäßig wird der folgende Citrix ADC Richtlinienausdruck (PI) verwendet: HTTP.REQ.HEADER (“Referrer”) .CONTAINS (“Google”). Aktualisieren Sie dieses Feld mit einem anderen Ausdruck, wenn Ihre Anforderung anders ist. Dieser Richtlinienausdruck entspricht dem Datenverkehr, auf den diese SAML-SSO-Einstellungen angewendet werden, und stellt sicher, dass der Referrer-Header von einer Google-Domain stammt.
4. Im Abschnitt SAML IdP-Einstellungen können Sie Ihre Citrix ADC-Instanz als SAML-Identitätsanbieter konfigurieren, indem Sie das SAML-IdP-Profil und die Richtlinie erstellen, die vom in Schritt 3 erstellten Citrix ADC AAA-Server verwendet werden.
   a) **Name des SAML-Ausstellers**. Geben Sie in dieses Feld den öffentlichen FQDN Ihres virtuellen Authentifizierungsservers ein. Beispiel:`https://<Citrix_ADC_VIP>/saml/login`
   b) **SAML-Dienstanbieter-ID (SP)**. (optional) Citrix ADC Identitätsanbieter akzeptiert SAML-Authentifizierungsanforderungen von einem Ausstellernamen, der dieser ID entspricht.
   c) **Assertion Consumer Service-URL**. Geben Sie die URL des Dienstanbieters ein, an die der Citrix ADC Identitätsanbieter die SAML-Assertionen nach erfolgreicher Benutzerauthentifizierung senden muss. Die Assertion Consumer Service-URL kann am Identity Provider Serverstandort oder der Service Provider-Website initiiert werden.
   d) Es gibt weitere optionale Felder, die Sie in diesem Abschnitt eingeben können. Sie können beispielsweise die folgenden Optionen festlegen:
      i. SAML-Bindungsprofil (der Standardwert ist das POST -Profil).

ii. Signaturalgorithmus zum Überprüfen/Signieren von SAML-Anforderungen/Antworten (Standard ist RSA-SHA1).

iii. Methode zum Digest Hash für SAML-Anforderungen/Antworten (Standard ist SHA-1).

iv. Verschlüsselungsalgorithmus (Standard ist AES256) und andere Einstellungen.

> **Hinweis**
>
> Citrix empfiehlt, dass Sie die Standardeinstellungen beibehalten, da diese Einstellungen zur Unterstützung von Google Apps getestet wurden.

e) Sie können auch das Kontrollkästchen Benutzerattribute aktivieren, um die Benutzerdetails einzugeben, z. B.:

i. Name des Benutzerattributs

ii. Citrix ADC PI-Ausdruck, der ausgewertet wird, um den Wert des Attributs zu extrahieren

iii. Benutzerfreundlicher Name des Attributs

iv. Wählen Sie das Format des Benutzerattributs aus.

Diese Werte sind in der ausgegebenen SAML-Assertion enthalten. Sie können bis zu fünf Gruppen von Benutzerattributen in eine Assertion einfügen, die von Citrix ADC mit diesem StyleBook ausgegeben wird.

5. Geben Sie im Abschnitt LDAP-Einstellungen die folgenden Details ein, um Google Apps Benutzer zu authentifizieren. Damit Domänenbenutzer mithilfe ihrer Unternehmens-E-Mail-Adressen bei der Citrix ADC-Instanz anmelden können, müssen Sie Folgendes konfigurieren:

a) **LDAP-Basis (Active Directory)**. Geben Sie den Basisdomänennamen für die Domäne ein, in der sich die Benutzerkonten im Active Directory (AD) befinden, für die Sie die Authentifizierung zulassen möchten. Zum Beispiel: `dc=netscaler,dc=com`

b) **LDAP (Active Directory) Bindet DN**. Fügen Sie ein Domänenkonto hinzu (unter Verwendung einer E-Mail-Adresse zur Vereinfachung der Konfiguration), das über die Rechte zum Durchsuchen der AD-Struktur verfügt. Zum Beispiel: `cn=Manager,dc=netscaler,dc=com`

c) **LDAP (Active Directory) Bindet DN Kennwort**. Geben Sie das Kennwort des Domänenkontos für die Authentifizierung ein.

d) Einige weitere Felder, die Sie in diesem Abschnitt eingeben müssen, sind wie folgt:

i. LDAP-Server-IP-Adresse, mit der Citrix ADC eine Verbindung zur Authentifizierung von Benutzern herstellt

ii. FQDN-Name des LDAP-Servers

> **Hinweis**
>
> Sie müssen mindestens eine der oben genannten beiden angeben - die IP-Adresse des LDAP-Servers oder den FQDN-Namen.

iii. LDAP-Serverport, mit dem Citrix ADC eine Verbindung zur Authentifizierung von Benutzern herstellt (Standard ist 389).

iv. LDAP-Hostname. Dies wird verwendet, um das LDAP-Zertifikat zu validieren, wenn die Validierung aktiviert ist (standardmäßig deaktiviert).

v. LDAP-Anmeldenamen-Attribut. Das Standardattribut zum Extrahieren von Anmeldenamen ist `samAccountname`.

vi. Weitere optionale verschiedene LDAP-Einstellungen

6. Im Abschnitt SAML IdP SSL Certificate können Sie die Details des SSL-Zertifikats angeben:

   a) **Zertifikatname**. Geben Sie den Namen des SSL-Zertifikats ein.

   b) **Zertifikatdatei.**Wählen Sie die SSL-Zertifikatsdatei aus dem Verzeichnis auf Ihrem lokalen System oder Citrix ADM.

   c) **CertKey-Format**. Wählen Sie das Format des Zertifikats und der Dateien mit privatem Schlüssel aus dem Dropdownlistenfeld aus. Die unterstützten Formate sind `.pem`.`der` Erweiterungen.

   d) **Name des Zertifikatsschlüssels**. Geben Sie den Namen des privaten Zertifikatsschlüssels ein.

   e) **Zertifikatsschlüsseldatei**. Wählen Sie die Datei aus, die den privaten Schlüssel des Zertifikats von Ihrem lokalen System oder von Citrix ADM enthält.

   f) **Kennwort für den privaten Schlüssel**. Wenn Ihre private Schlüsseldatei durch eine Passphrase geschützt ist, geben Sie sie in dieses Feld ein.

   g) Sie können auch das Kontrollkästchen Erweiterte Zertifikateinstellungen aktivieren, um Details wie das Ablaufdatum des Zertifikats einzugeben, oder die Ablaufüberwachung des Zertifikats zu aktivieren oder zu deaktivieren.

7. Optional können Sie IdP SSL CA-Zertifikat auswählen, wenn für das oben eingegebene SAML-IdP-Zertifikat ein öffentliches Zertifizierungsstellenzertifikat auf Citrix ADC installiert werden muss. Stellen Sie sicher, dass Sie in den erweiterten Einstellungen Ist ein CA-Zertifikat auswählen.

8. Optional können Sie SAML SP-SSL-Zertifikat auswählen, um das Google SSL-Zertifikat (öffentlicher Schlüssel) anzugeben, das zur Validierung von Authentifizierungsanforderungen von Google Apps (SAML SP) verwendet wird.

9. Klicken Sie auf **Zielinstanzen**, und wählen Sie die Citrix ADC-Instanz (en) aus, für die diese Google Apps SSO-Konfiguration bereitgestellt werden soll. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und die Konfiguration auf den ausgewählten Citrix ADC-Instanzen bereitzustellen.

   > **Hinweis**
   >
   > Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC-Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

auch,

> **Tipp**

```
> Citrix empfiehlt, dass Sie vor dem Ausführen der eigentlichen
  Konfiguration **Dry Run** auswählen, um die Konfigurationsobjekte,
  die auf den Citrix ADC-Zielinstanzen (n) vom StyleBook erstellt
  wurden, visuell zu bestätigen.
```

SSO Office 365 StyleBook

April 28, 2021

Microsoft™ Office 365 ist eine Suite von cloudbasierten Produktivitäts- und Collaboration-Anwendungen, die von Microsoft auf Abonnementbasis bereitgestellt werden. Es umfasst die beliebten serverbasierten Anwendungen von Microsoft wie Exchange, SharePoint, Office und Skype for Business. Mit Single Sign-On (SSO) können Benutzer auf alle ihre Enterprise-Cloud-Anwendungen zugreifen:

- Einschließlich von Administratoren, die sich bei der Administratorkonsole anmelden
- Einmalige Anmeldung für alle Microsoft Office 365-Dienste unter Verwendung ihrer Enterprise-Anmeldeinformationen.

Mit dem SSO Office 365 StyleBook können Sie SSO für Microsoft Office 365 über Citrix ADC-Instanzen aktivieren. Sie können nun die SAML-Authentifizierung mit Citrix ADC als SAML-Identitätsanbieter (IdP) und Microsoft Office 365 als SAML-Dienstanbieter konfigurieren.

Das Aktivieren von SSO für Microsoft Office 365 in einer Citrix ADC-Instanz mit diesem StyleBook umfasst die folgenden Schritte:

1. Konfigurieren des virtuellen Authentifizierungsservers
2. Konfigurieren einer SAML-IdP-Richtlinie und eines Profils

3. Binden der Richtlinie und des Profils an den virtuellen Authentifizierungsserver
4. Konfigurieren eines LDAP-Authentifizierungsservers und einer Richtlinie für die Instanz
5. Binden des LDAP-Authentifizierungsservers und der Richtlinie an den virtuellen Authentifizierungsserver, der auf der Instanz konfiguriert ist.

In der Tabelle sind die erforderlichen Mindestsoftwareversionen aufgeführt, damit diese Integration erfolgreich funktioniert. Der Integrationsprozess unterstützt auch höhere Versionen derselben.

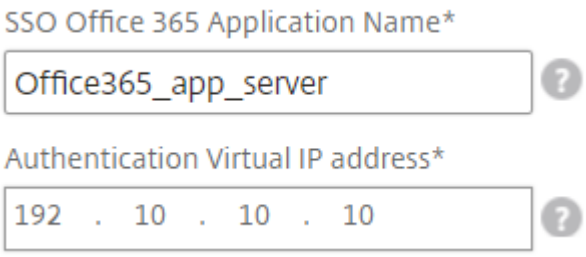
Produkt	Erforderliche Mindestversion
Citrix ADC	11.0, Advanced/Premium Lizenz

In den folgenden Anweisungen wird davon ausgegangen, dass Sie bereits die entsprechenden externen und internen DNS-Einträge erstellt haben. Diese Einträge sind unerlässlich, um Authentifizierungsanforderungen an eine von Citrix ADC überwachte IP-Adresse weiterzuleiten.

Die folgenden Anweisungen helfen Ihnen bei der Implementierung des SSO Office 365 StyleBook in Ihrem Unternehmensnetzwerk.

So stellen Sie SSO Microsoft Office 365 StyleBook bereit

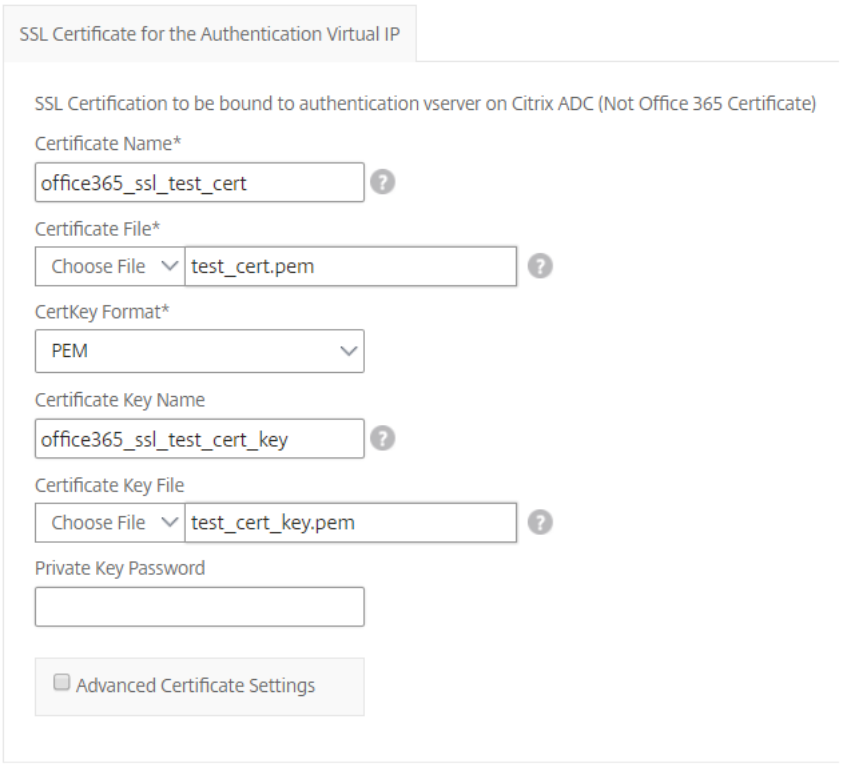
1. Navigieren Sie in Citrix Application Delivery Management (ADM) zu **Anwendungen** > **StyleBooks**. Auf der Seite **StyleBooks** werden alle für Ihre Verwendung in Citrix ADM verfügbaren StyleBooks angezeigt. Scrollen Sie nach unten und suchen Sie **SSO Office 365 StyleBook**. Klicken Sie auf **Konfiguration erstellen**.
2. Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
3. Geben Sie Werte für die folgenden Parameter ein:
    a) **Anwendungsname**. Name der SSO Microsoft Office 365-Konfiguration, die im Netzwerk bereitgestellt werden soll.
    b) **Authentifizierung Virtuelle IP-Adresse**. Virtuelle IP-Adresse, die vom virtuellen Citrix ADC AAA-Server verwendet wird, an den die Microsoft Office 365 SAML-IdP-Richtlinie gebunden ist.



4. Geben Sie im Abschnitt ****SSL-Zertifikateinstellungen**** die Namen des SSL-Zertifikats und des Zertifikatschlüssels ein.

   > **Hinweis**
   >
   > Dies ist nicht das Office 365-Dienstanbieterzertifikat. Dieses SSL-Zertifikat ist an den virtuellen Authentifizierungsserver der Citrix ADC-Instanz gebunden.

5. Wählen Sie die entsprechenden Dateien aus Ihrem lokalen Speicherordner aus. Sie können auch das Kennwort für den privaten Schlüssel eingeben, um verschlüsselte private Schlüssel im PEM-Format zu laden.



6. Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Ablauf der Benachrichtigung des Zertifikats eingeben, den Ablaufmonitor des Zertifikats aktivieren oder deaktivieren.
7. Optional können Sie das Kontrollkästchen **SSL-CA-Zertifikat für die virtuelle Authen-**

tifizierung aktivieren, wenn für das SSL-Zertifikat ein öffentliches Zertifikat der Zertifizierungsstelle auf Citrix ADC installiert werden muss. Stellen Sie sicher, dass Sie Ist ein CA-Zertifikat im obigen Abschnitt **Erweiterte Zertifikateinstellungen auswählen**.

8. Geben Sie im Abschnitt **LDAP-Einstellungen für SSO Office 365** die folgenden Details ein, um Office 365-Benutzer zu authentifizieren. Um Domänenbenutzern die Anmeldung bei der Citrix ADC-Instanz mithilfe ihrer Unternehmens-E-Mail-Adressen zu ermöglichen, konfigurieren Sie Folgendes:

   a) **LDAP-Basis (Active Directory)**. Geben Sie den Basisdomänennamen für die Domäne ein, in der sich die Benutzerkonten im Active Directory (AD) befinden, um die Authentifizierung zu ermöglichen. Zum Beispiel: `dc=netscaler,dc=com`

   b) **LDAP (Active Directory) Bindet DN**. Fügen Sie ein Domänenkonto hinzu (unter Verwendung einer E-Mail-Adresse zur Vereinfachung der Konfiguration), das über die Rechte zum Durchsuchen der AD-Struktur verfügt. Zum Beispiel: `cn=Manager,dc=netscaler,dc=com`

   c) **LDAP (Active Directory) Bindet DN Kennwort**. Geben Sie das Kennwort des Domänenkontos für die Authentifizierung ein.

   d) Einige weitere Felder, die Sie in diesem Abschnitt eingeben müssen, sind wie folgt:

      i. IP-Adresse des LDAP-Servers, mit der Citrix ADC eine Verbindung zur Authentifizierung von Benutzern herstellt.

      ii. Der FQDN-Name des LDAP-Servers.

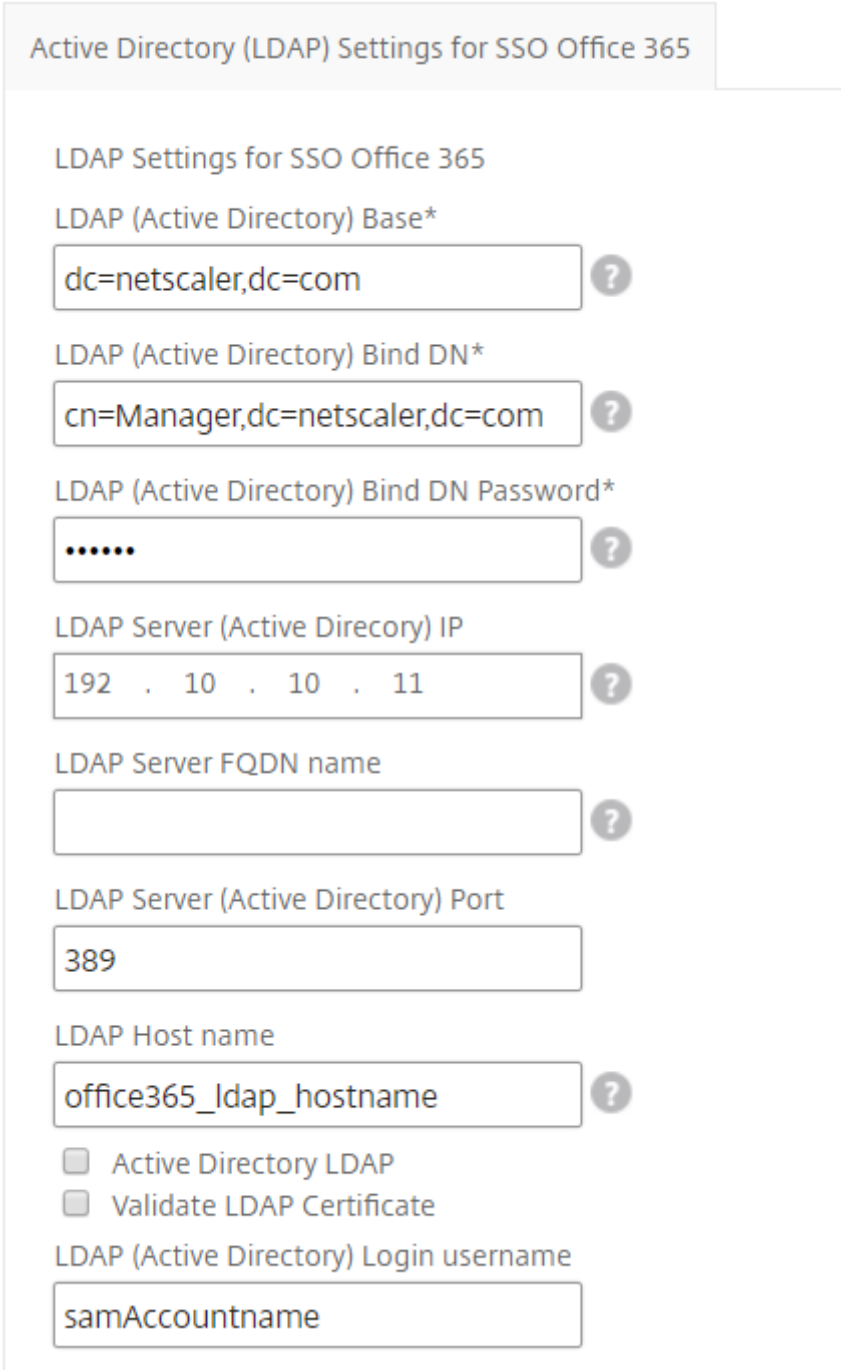
      > **Hinweis**
      >
      > Sie müssen mindestens eine der oben genannten beiden angeben - die IP-Adresse des LDAP-Servers oder den FQDN-Namen.

      iii. LDAP-Serverport, mit dem Citrix ADC eine Verbindung zur Authentifizierung von Benutzern herstellt (Standard ist 389). LDAPS verwendet 636.

      iv. LDAP-Hostname. Der Hostname wird verwendet, um das LDAP-Zertifikat zu validieren, wenn die Validierung aktiviert ist (standardmäßig ist es deaktiviert).

      v. LDAP-Anmeldenamen-Attribut. Das Standardattribut zum Extrahieren von Anmeldenamen ist “sAMAccountName. “

      vi. Andere optionale verschiedene LDAP-Einstellungen.



9. Im Abschnitt **SAML-IdP-Zertifikat** können Sie die Details der SSL-Zertifikate angeben, die für die SAML-Assertion verwendet werden.

   a) **Zertifikatname**. Geben Sie den Namen des SSL-Zertifikats ein.

   b) **Zertifikatdatei**. Wählen Sie die SSL-Zertifikatsdatei aus dem Verzeichnis auf Ihrem lokalen System aus.

   c) **CertKey-Format**. Wählen Sie das Format des Zertifikats und der Dateien mit privatem

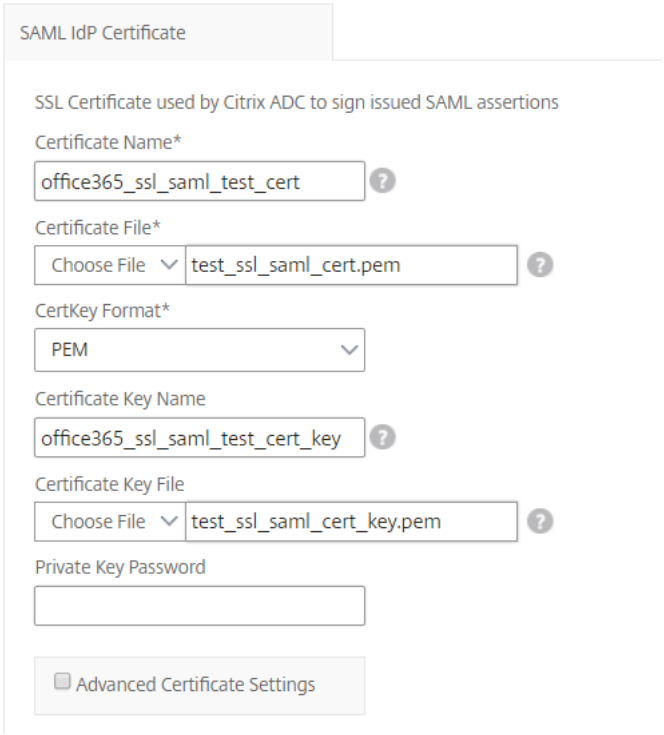
Schlüssel aus dem Dropdownlistenfeld aus. Die unterstützten Formate sind Erweiterungen PEM und .der.

d) **Name des Zertifikatsschlüssels**. Geben Sie den Namen des privaten Zertifikatsschlüssels ein.

e) **Zertifikatsschlüsseldatei**. Wählen Sie die Datei aus, die den privaten Schlüssel des Zertifikats enthält.

f) **Kennwort für den privaten Schlüssel**: Geben Sie die Passphrase ein, die Ihre private Schlüsseldatei schützt.

Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Ablauf der Benachrichtigung des Zertifikats eingeben, den Ablaufmonitor des Zertifikats aktivieren oder deaktivieren.



10. Optional können Sie **SAML-IdP-Zertifizierungsstellenzertifikat** auswählen, wenn für das oben eingegebene SAML-IdP-Zertifikat ein öffentliches Zertifizierungsstellenzertifikat auf Citrix ADC installiert werden muss. Stellen Sie sicher, dass Sie Ist ein Zertifizierungsstellenzertifikat im obigen Abschnitt **Erweiterte Zertifikateinstellungen** auswählen.

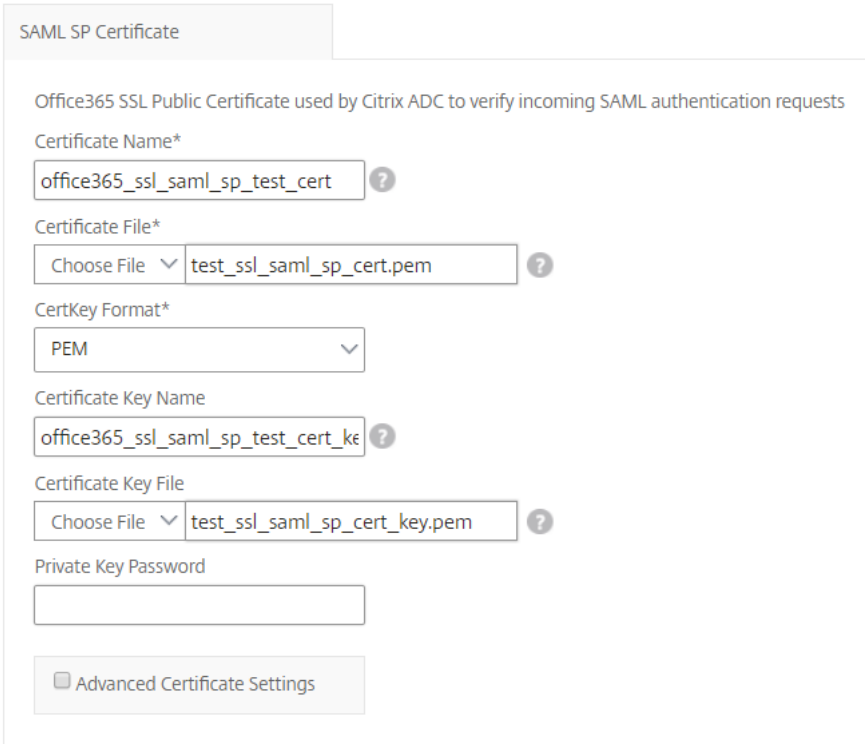
11. Geben Sie im Abschnitt **SAML-SP-Zertifikat** die folgenden Details für das öffentliche Office 365-SSL-Zertifikat ein. Dieses Zertifikat wird von der Citrix ADC-Instanz verwendet, um eingehende SAML-Authentifizierungsanforderungen zu überprüfen.

a) **Zertifikatname**. Geben Sie den Namen des SSL-Zertifikats ein.

b) **Zertifikatdatei**. Wählen Sie die SSL-Zertifikatsdatei aus dem Verzeichnis auf Ihrem lokalen System aus.

c) **CertKey-Format**. Wählen Sie das Format des Zertifikats und der Dateien mit privatem Schlüssel aus dem Dropdownlistenfeld aus. Die unterstützten Formate sind Erweiterungen PEM und .der.

Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Ablauf der Benachrichtigung des Zertifikats eingeben, den Ablaufmonitor des Zertifikats aktivieren oder deaktivieren.



12. Im Abschnitt **SAML Idp-Einstellungen** können Sie Ihre Citrix ADC-Instanz als SAML-Identitätsanbieter konfigurieren, indem Sie das SAML-IdP-Profil und die Richtlinie erstellen, die vom in Schritt 3 erstellten Citrix ADC AAA-Server verwendet werden.

a) **Name des SAML-Ausstellers**. Geben Sie in dieses Feld den öffentlichen FQDN Ihres virtuellen Authentifizierungsservers ein. Beispiel:`https://\<Citrix ADC_VIP_Address \>/saml/login`

b) **Namensbezeichnerausdruck**. Geben Sie den Citrix ADC Ausdruck ein, der ausgewertet wird, um den SAML-NameIdentifier zu extrahieren, der in der SAML-Assertion gesendet wird. Beispiel:`"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`

c) **Signaturalgorithmus**: Wählen Sie den Algorithmus zum Überprüfen/Signieren von SAML-Anforderungen/Antworten (Standard ist RSA-SHA256).

d) **Digest-Methode**. Wählen Sie die Methode aus, um den Hash für SAML-Anforderungen/Antworten zu verdauen (Standard ist SHA256).

e) **Zielgruppenname**. Geben Sie den Entitätsnamen oder die URL ein, die den Dienstanbieter darstellt (Microsoft Office 365).

f) **SAML-Dienstanbieter-ID (SP)**. (optional) Citrix ADC Identitätsanbieter akzeptiert SAML-Authentifizierungsanforderungen von einem Ausstellernamen, der dieser ID entspricht.

g) **Assertion Consumer Service-URL**. Geben Sie die URL des Dienstanbieters ein, an die der Citrix ADC Identitätsanbieter die SAML-Assertionen nach erfolgreicher Benutzerauthentifizierung senden muss. Die Assertion Consumer Service-URL kann am Identity Provider Serverstandort oder der Service Provider-Website initiiert werden.

h) Es gibt weitere optionale Felder, die Sie in diesem Abschnitt eingeben können. Sie können beispielsweise die folgenden Optionen festlegen:

   i. **SAML-Attributname**. Name des in SAML-Assertion gesendeten Benutzerattributs.

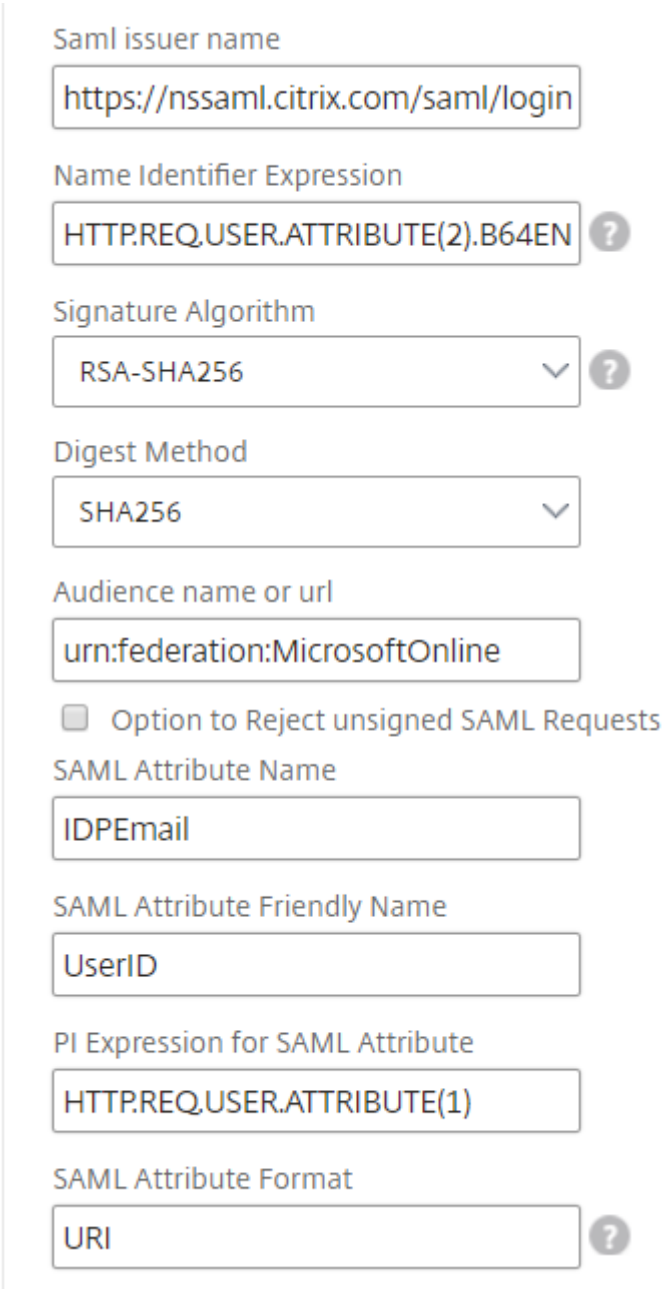
   ii. **Anzeigename des SAML-Attributs**. Anzeigename des in SAML-Assertion gesendeten Benutzerattributs.

   iii. **PI-Ausdruck für SAML-Attribut**. Standardmäßig wird der folgende Ausdruck der Citrix ADC Richtlinie (PI) verwendet: HTTP.REQ.USER.ATTRIBUTE (1). Dieses Feld gibt das erste Benutzerattribut an, das vom LDAP-Server (mail) als SAML-Authentifizierungsattribut gesendet wird.

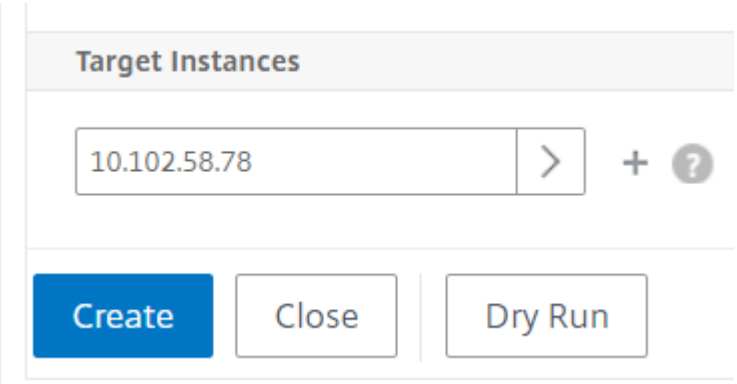
   iv. Wählen Sie das Format des Benutzerattributs aus.

   Diese Werte sind in der ausgegebenen SAML-Assertion enthalten.

> **Tipp**
>
> Citrix empfiehlt, dass Sie die Standardeinstellungen beibehalten, da diese Einstellungen für den Support von Microsoft Office 365-Apps getestet wurden.



13. Klicken Sie auf **Zielinstanzen**, und wählen Sie die Citrix ADC-Instanz (en) aus, für die diese Microsoft Office 365-SSO-Konfiguration bereitgestellt werden soll. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und die Konfiguration auf den ausgewählten Citrix ADC-Instanzen bereitzustellen.



> **Tipp**
>
> Citrix empfiehlt, dass Sie vor dem Ausführen der eigentlichen Konfiguration die Option **Dry Run** auswählen, um die Konfigurationsobjekte anzuzeigen, die vom StyleBook auf den Citrix ADC-Zielinstanzen erstellt werden.

Microsoft Skype for Business StyleBook

April 28, 2021

Die Skype for Business 2015-Anwendung basiert auf mehreren externen Komponenten zu funktionieren. Das Skype for Business Netzwerk besteht aus verschiedenen Systemen, wie Servern und deren Betriebssysteme, Datenbanken, Authentifizierungs- und Autorisierungssysteme, Netzwerksysteme und Infrastruktur sowie Telefonanlagen. Skype for Business Server 2015 ist in zwei Versionen verfügbar, Standard Edition und Advanced Edition. Der Hauptunterschied besteht in der Unterstützung von Hochverfügbarkeitsfunktionen, die nur in der Advanced Edition enthalten sind. Um eine hohe Verfügbarkeit zu implementieren, müssen mehrere Front-End-Server in einem Pool bereitgestellt und SQL-Server gespiegelt werden.

Eine Advanced Edition-Bereitstellung ermöglicht die Erstellung mehrerer Server mit unterschiedlichen Rollen.

Die Hauptkomponenten in Skype for Business 2015-Anwendung sind:

- Front-End-Server
- Edge-Server
- Director-Server
- Datenbankserver (SQL)

Front-End-Server:

In der Skype for Business Anwendung ist der Front-End-Server der Kernserver in Ihrem Netzwerk. Es bietet Links und Dienste für Benutzerauthentifizierung, Registrierung, Präsenz, Adressbuch,

A/V-Konferenzen, Anwendungsfreigabe, Instant Messaging und Webkonferenzen. Wenn Sie Skype for Business 2015 Enterprise Edition bereitstellen, besteht die Topologie in der Regel aus mindestens zwei Front-End-Servern in einem Front-End-Pool mit einem Datenbankserver, der die SQL Server-Instanz hostet, die die Skype for Business-Datenbank enthält.

Edge-Server:

Die Bereitstellung von Edge-Servern für Skype for Business ist erforderlich, wenn externe Benutzer, die nicht bei Ihrem

Das interne Netzwerk der Organisation muss in der Lage sein, mit internen Benutzern zu interagieren. Diese externen Benutzer können authentifizierte und anonyme Remote-Benutzer, Verbundpartner oder andere mobile Clients sein.

Es gibt vier Arten von Rollen in Skype for Business Edge Server:

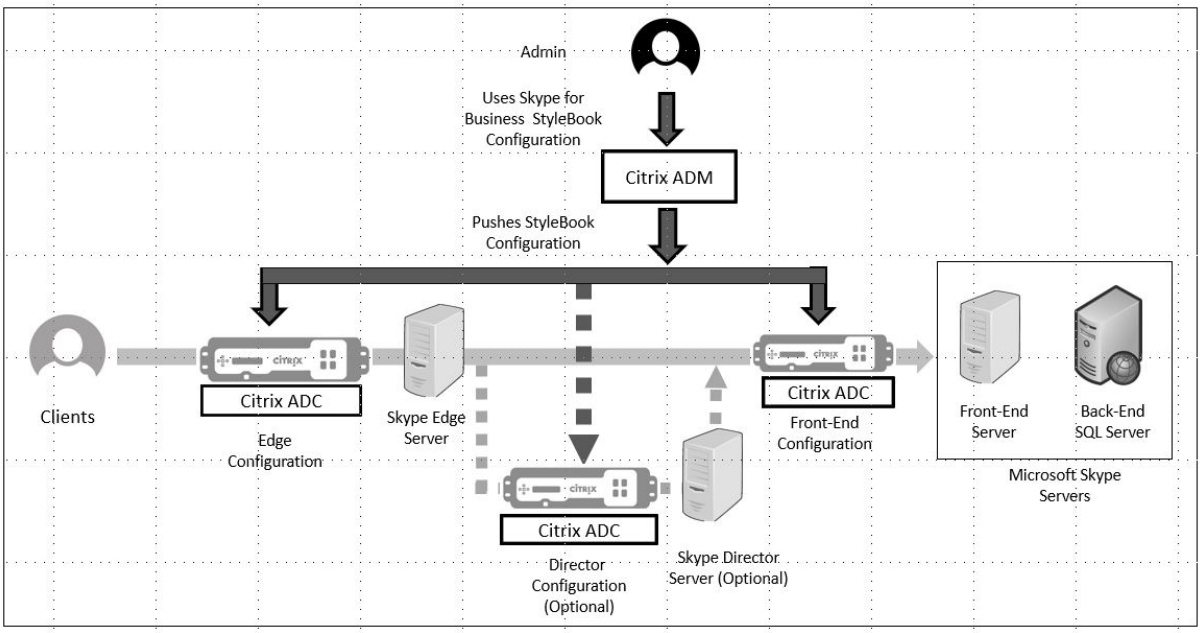
- Access Edge, der SIP-Datenverkehr verarbeitet und externe Verbindungen authentifiziert, Remoteverbindung ermöglicht und Verbundverbindung ermöglicht
- Webkonferenzen, die Datenkonferenzpakete verarbeiten und externen Benutzern den Zugriff auf Skype for Business ermöglichen
- A/V-Konferenzen, die A/V-Konferenzpakete verarbeitet und Audio- und Video-, App-Sharing und Dateiübertragung auf externe Benutzer erweitert
- XMPP-Proxy, der XMPP-Pakete verarbeitet und XMPP-basierte Server oder Clients ermöglicht, eine Verbindung zu Skype for Business herzustellen.

Director-Server:

Die Hauptfunktion des Director-Servers in Skype for Business 2015 besteht darin, Endpunkte zu authentifizieren und die Benutzer an den Pool zu leiten, der ihr Konto enthält. In Skype for Business 2015 ist der Director zwar eine vollständig dedizierte und spezifische Rolle auf einem eigenständigen Server, jedoch ein optionaler Server. Dies erleichtert die Sicherheit, da die Bereitstellung oder das Entfernen der Konfigurationen vereinfacht wird.

Directors sind am nützlichsten, wenn mehrere Pools vorhanden sind, da sie einen einzigen Ansprechpartner für die Authentifizierung von Endpunkten bieten. Außerdem dient ein Director für Remote-Benutzer als zusätzlicher Hop zwischen dem Edge-Pool und dem Front-End-Pool und fügt eine zusätzliche Schutzschicht vor Angriffen hinzu.

Die folgende Abbildung zeigt die Bereitstellung von Skype-Servern im Netzwerk:



Konfigurieren von Citrix ADC-Instanzen in einem Unternehmen

In der folgenden Tabelle sind die IP-Adressen aufgeführt, die in der Beispielkonfiguration verwendet werden, die in den folgenden Anweisungen enthalten sind:

Skype for Business server	Virtuelle IP-Adresse	Server-IP-Adressen	Citrix ADC-Instanz
Edge-Server	Externes VIP - 192.20.20.20	192.20.20.21; 192.20.20.22	10.102.29.141
	Interne VIP - 10.10.10.20	10.10.10.21; 10.10.10.22	
Front-End-Server	10.10.10.10	10.10.10.11; 10.10.10.12	10.102.29.60
Director-Server	10.10.10.30	10.10.10.31; 10.10.10.32	10.102.29.93

So konfigurieren Sie Front-End-Server:

1. Navigieren Sie in Citrix Application Delivery Management (ADM) zu **Anwendungen** > **Konfiguration**, und klicken Sie auf **Neu erstellen**. Auf der Seite **StyleBook auswählen** werden alle StyleBooks angezeigt, die für Ihre Verwendung in Citrix ADM verfügbar sind. Scrollen Sie nach unten und wählen Sie **Microsoft Skype for Business 2015 StyleBook**aus. Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
2. Geben Sie im Abschnitt **Edge-Server** die folgenden virtuellen IP-Adressen (VIP) und IP-Adressen

aller Edge-Server im Netzwerk ein.

a) Externe VIP-Adresse und IP-Adressen für die Edge-Server, die für Access Edge, Webkonferenz-Edge und A/V Edge verwendet werden.
b) Interne VIP-Adresse und IP-Adressen für die Edge-Server, die mit dem internen Netzwerk verbunden werden.
c) Zwei externe und zwei interne Edge-Server in Ihrem Netzwerk.

3. Geben Sie im Abschnitt **Front-End-Server** die IP-Adresse des virtuellen Front-End-Servers (VIP) ein, der für die Skype for Business Front-End-Server erstellt werden soll. Geben Sie außerdem die IP-Adressen aller Skype for Business Front-End-Server im Netzwerk ein.
4. Geben Sie im Abschnitt **Director Server** die virtuelle IP-Adresse (VIP) für die Director-Server ein, die für die Skype for Business Anwendung erstellt werden soll. Geben Sie außerdem die IP-Adressen für alle Skype for Business Director-Server im Netzwerk ein. Erstellen Sie mindestens zwei Director-Server für hohe Verfügbarkeit.
5. Im Abschnitt **Erweiterte Einstellungen** werden alle Standardports aufgeführt, die auf den Citrix ADC-Instanzen für die drei Skype-Server konfiguriert sind.

Die folgende Tabelle enthält eine Liste aller Standardports und -protokolle:

Label	Port	Protokoll	Beschreibung
HTTP Port	80	HTTP	Wird für die Kommunikation von Front-End-Servern zu den FQDNs der Webfarm verwendet, wenn HTTPS nicht verwendet wird.
HTTPS-Port	443	HTTPS	Wird für die Kommunikation von Front-End-Servern zu den FQDNs der Webfarm verwendet.
Internen Port automatisch entdecken	4443	HTTPS	HTTPS (von Reverse Proxy) und HTTPS Front-End-Interpool-Kommunikation für Auto Discover-Anmeldung.

Label	Port	Protokoll	Beschreibung
RPC Port	135	DCOM- und Remoteprozeduraufruf (RPC)	Wird für DCOM-basierte Vorgänge wie das Verschieben von Benutzern, die Synchronisierung von Benutzerreplikatoren und die Synchronisierung von Adressbüchern verwendet.
SIP Port	5061	TCP (TLS)	Wird von Front-End-Servern für die gesamte interne SIP-Kommunikation verwendet.
SIP Focus Port	444	HTTPS, TCP	Wird für die HTTPS-Kommunikation zwischen dem Fokus (der Komponente, die den Skype-Konferenzstatus verwaltet) und den einzelnen Servern verwendet.
SIP Group Port	5071	TCP	Wird für eingehende SIP-Anforderungen für die Antwortgruppenanwendung verwendet.
SIP AppSharing Port	5065	TCP	Wird für eingehende SIP-Listening-Anforderungen für die Anwendungsfreigabe verwendet.

Label	Port	Protokoll	Beschreibung
SIP Attendant Port	5072	TCP	Wird für eingehende SIP-Anfragen für die Telefonzentrale (d. h. für Einwahlkonferenzen) verwendet.
SIP Conf Announcement Port	5073	TCP	Wird für eingehende SIP-Anforderungen für den Skype for Business - Serverkonferenzankündigungsdienst (d. h. für Einwahlkonferenzen) verwendet.
SIP CallPark Port	5075	TCP	Wird für eingehende SIP-Anfragen für die CallPark-Anwendung verwendet.
SIP Call Admission Port	448	TCP	Wird für die Anrufzugangssteuerung durch den Skype for Business - Serverbandbreitenrichtliniendienst verwendet.
SIP Call Admission TURN Port	5080	TCP	Wird für die Anrufzugangskontrolle durch den Bandbreitenrichtliniendienst für Audio/Video Edge TURN-Verkehr verwendet.
SIP Audio Test Port	5076	TCP	Wird für eingehende SIP-Anfragen für den Audiotestdienst verwendet.

Label	Port	Protokoll	Beschreibung
HTTPS External Port	443	HTTPS	Wird für externe Ports für die SIP/TLS-Kommunikation für den Remote-Benutzerzugriff, den Zugriff auf interne Webkonferenzen und die eingehende und ausgehende STUN/TCP-Medienkommunikation für den Zugriff auf interne Medien und A/V-Sitzungen verwendet.
HTTPS Internal Port	443	HTTPS	Wird für interne Ports für die SIP/TLS-Kommunikation für den Remote-Benutzerzugriff, den Zugriff auf interne Webkonferenzen und die eingehende und ausgehende STUN/TCP-Medienkommunikation für den Zugriff auf interne Medien und A/V-Sitzungen verwendet.
SIP External Remote Access Port	5061	TCP	Wird für externe Ports für die SIP/MTLS-Kommunikation für den Remote-Benutzerzugriff oder den Verbund verwendet.

Label	Port	Protokoll	Beschreibung
SIP Internal Remote Access Port	5061	TCP	Wird für interne Ports für die SIP/MTLS-Kommunikation für den Remote-Benutzerzugriff oder den Verbund verwendet.
SIP External STUN UDP Port	3478	UDP	Wird für externe Ports für eingehende und ausgehende STUN/UDP-Medienkommunikation verwendet.
SIP Internal STUN UDP Port	3478	UDP	Wird für interne Ports für eingehende und ausgehende STUN/UDP-Medienkommunikation verwendet.
SIP Internal IM Port	5062		Wird für interne Ports zur SIP/MTLS-Authentifizierung der IM-Kommunikation verwendet, die ausgehend durch die interne Firewall fließt.
HTTP Port	80	TCP	Wird für die erste Kommunikation von Directors zu den FQDNs der Webfarm verwendet.
HTTPS-Port	443	HTTPS	Wird für die Kommunikation von Directors zu den FQDNs der Webfarm verwendet.

Label	Port	Protokoll	Beschreibung
Internen Port automatisch entdecken	4443	HTTPS	Wird für HTTPS (von Reverse Proxy) und HTTPS Director Interpool-Kommunikation für Auto Discover-Anmeldung verwendet.
SIP Internal Port	5061	TCP	Wird für die interne Kommunikation zwischen Servern und für Clientverbindungen verwendet.

1. Wählen Sie im Abschnitt **Zielinstanzen** die drei verschiedenen Citrix ADC-Instanz aus, auf denen die drei Skype for Business -Server bereitgestellt werden sollen.

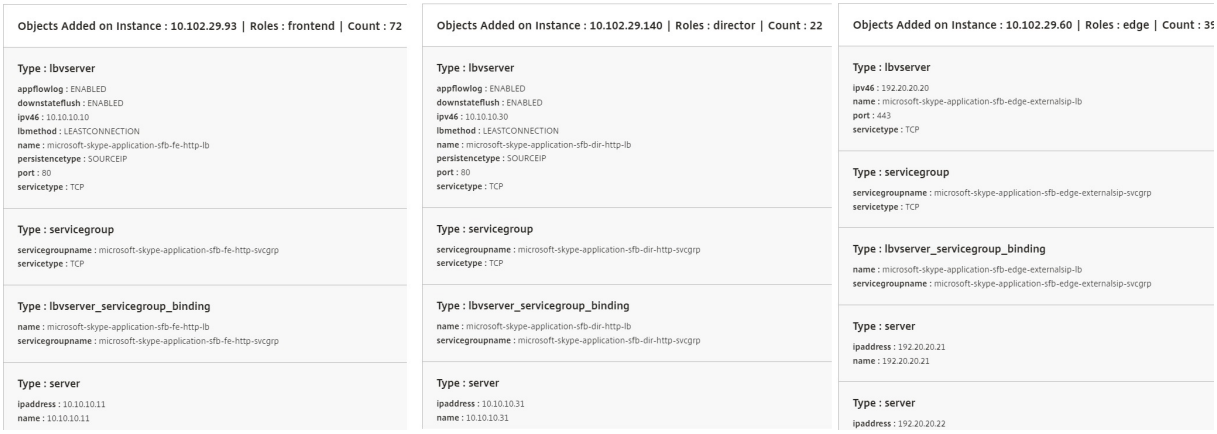
   > **Hinweis**
   >
   > Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC-Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

2. Klicken Sie auf **Erstellen**, um die Konfiguration für die ausgewählten Citrix ADC-Instanzen zu erstellen.

   > **Tipp**
   >
   > Citrix empfiehlt, dass Sie **Dry Run** auswählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt werden müssen, bevor Sie die eigentliche Konfiguration auf der Instanz ausführen.

Wenn die Konfiguration erfolgreich erstellt wurde, erstellt das StyleBook 25 virtuelle Server mit Lastenausgleich. Das heißt, für jeden Port wird ein virtueller Lastausgleichsserver zusammen mit einer Dienstgruppe definiert, und die Dienstgruppe ist an den virtuellen Lastausgleichsserver gebunden. Die Konfiguration fügt auch die Front-End-Server als Dienstgruppenmitglieder hinzu und bindet sie an die Dienstgruppe. Die Anzahl der erstellten Dienstgruppenmitglieder entspricht der Anzahl der erstellten Front-End-Server.

Die folgende Abbildung zeigt die in jedem Server erstellten Objekte:



Microsoft Exchange-StyleBook

April 28, 2021

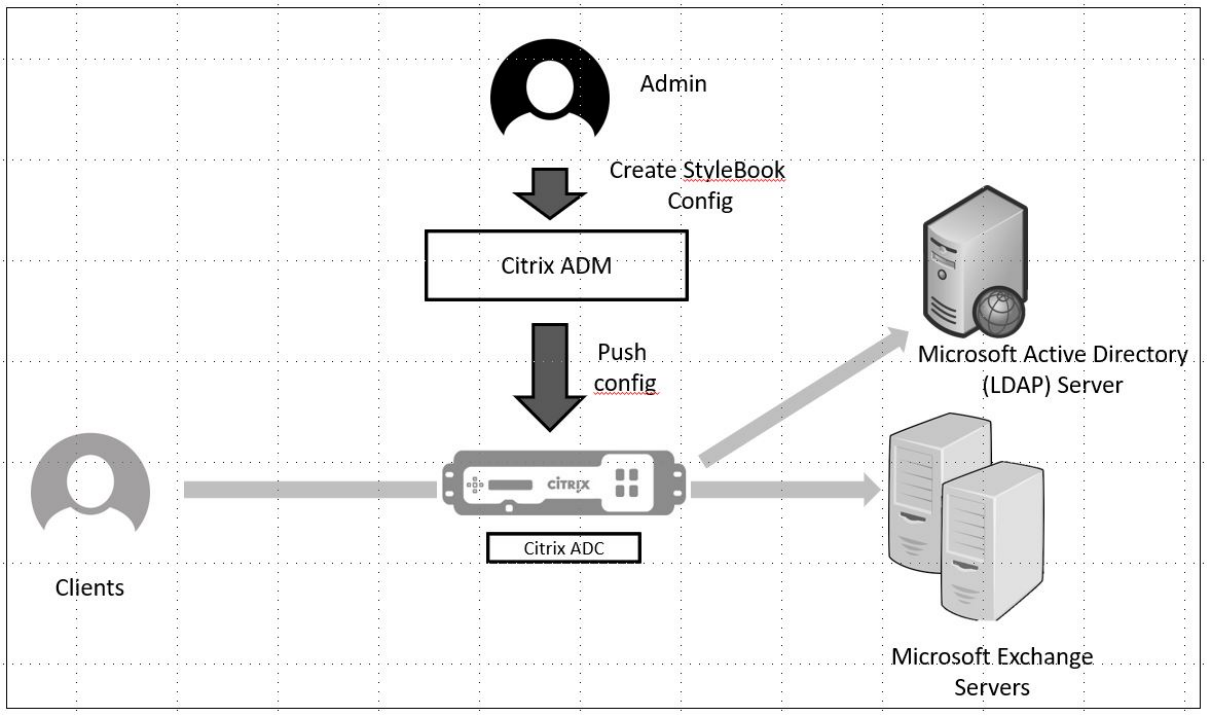
Sie können das Microsoft Exchange 2016-StyleBook verwenden, um eine Citrix ADC Konfiguration bereitzustellen, die eine Microsoft Exchange 2016-Unternehmensanwendung in Ihrem Netzwerk optimiert und schützt. Microsoft Exchange 2016 ist eine wichtige Unternehmensanwendung für die Bereitstellung von E-Mail-, Personalinformations- und Messagingdiensten für Ihre Mitarbeiter und andere Interessengruppen.

Citrix ADC Funktionen, die mithilfe von Microsoft Exchange StyleBook konfiguriert wurden

Das Microsoft Exchange 2016 StyleBook aktiviert und konfiguriert die folgenden Citrix ADC Features für Microsoft Exchange 2016-Server:

- Lastenausgleich — Grundlegender Lastausgleich, der den Lastenausgleich mehrerer Exchange-Server ermöglicht
- Content Switching - Content Switching, dass Einzel-IP-Zugriff und Umleitung von Abfragen an die richtigen virtuellen Server mit Lastenausgleich ermöglicht
- Rewrite - leitet Benutzer auf sichere Seiten um
- SSL-Offload - Verlagert die SSL-Verarbeitung an den Citrix ADC, wodurch die Last auf dem Exchange-Server reduziert wird

Die folgende Abbildung zeigt die Bereitstellung von Exchange-Servern im Netzwerk:



Voraussetzungen

- Für die zertifikatbasierte Authentifizierung müssen alle adressierbaren Hosts, die Teil der Netzwerkeinrichtung sind, auflösbare Domänennamen und nicht nur IP-Adressen haben.
- Stellen Sie sicher, dass auf die SIP-Ports im Microsoft Exchange 2016-Server zugegriffen werden kann.

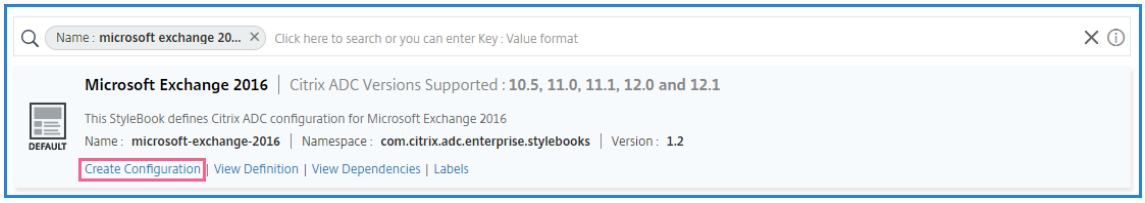
Konfigurieren von Microsoft Exchange StyleBook

Konfigurieren Sie das Microsoft Exchange-StyleBook in Ihrem Unternehmen, um die Citrix ADC Konfiguration bereitzustellen.

So konfigurieren Sie Microsoft Exchange-Anwendung

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **StyleBooks**.
2. Suchen Sie nach **Microsoft Exchange 2016 StyleBook**, und klicken Sie auf **Konfiguration erstellen**.

   Das StyleBook erscheint als Benutzeroberflächenformular, in dem Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.



3. Geben Sie die Details für die folgenden Parameter ein:

   - **Exchange-Anwendungsname** - Name der Microsoft Exchange-Anwendung in Ihrem Netzwerk
   - **Exchange-VIP** - Virtuelle IP-Adresse auf Citrix ADC, die Clientanforderungen für die Microsoft Exchange-Anwendung empfängt
   - **Exchange Server IPs** - IP-Adressen aller Exchange-Server im Netzwerk.

     Wenn Sie weitere IP-Adressen hinzufügen möchten, klicken Sie auf das Plus-Symbol (**+**). Normalerweise werden zwei Exchange-Server im Netzwerk konfiguriert.

4. Laden Sie im Abschnitt **Exchange-Zertifikate** Austauschzertifikate in Citrix ADM hoch. Geben Sie die Namen des Zertifikats und der Schlüsseldateien ein und laden Sie sie aus dem lokalen Speicher hoch. Sie können auch ein Kennwort für den privaten Schlüssel angeben, um die Schlüsseldatei zu verschlüsseln.

   > **Hinweis**
   >
   > Stellen Siesicher, dass die Zertifikatdateien das Format .pem oder .der haben. Citrix ADM lehnt die Dateien anderer Formate ab.

   Wenn Sie Details zum Ablauf des Zertifikats oder erweiterte Einstellungen angeben möchten, wählen Sie **Erweiterte Zertifikateinstellungen** aus.

5. Konfigurieren Sie im Abschnitt **Konfiguration der Exchange Active Directory Authentifizierung** die AD-Einstellungen, indem Sie die Daten eingeben.

   - **Active Directory Authentifizierungs-VIP**: Die virtuelle IP-Adresse, die zum Erstellen und Konfigurieren des virtuellen AD (LDAP)-Servers auf einer Citrix ADC Appliance verwendet wird.
   - **Active Directory Server-IP** - Die IP-Adresse des Active Directory Domänencontroller.
   - **Active Directory-Basiszeichenfolge** - Die LDAP-Basiszeichenfolge in Active Directory. Beispiel: CN=Benutzer, DC=CTXNSSFB, DC=COM.
   - **Active Directory LDAP-Bind Distinguished Name (DN)** - LDAP-Bind Distinguished Name (DN) wird verwendet, um dieses Objekt an den LDAP-Server (AD) zu binden. Beispiel: CN=Administrator, CN=Benutzer, dc=acme, dc=com
   - **Active Directory LDAP-Bind Distinguished Name (DN) Kennwort** - LDAP-Bind Distinguished Name (DN) ist das Kennwort für die AD-Authentifizierung

- **Active Directory Benutzernamenattribut** - AD-Attribut für den Benutzernamen. Citrix ADC verwendet das LDAP-Attribut, um externe Active Directory -Server abzufragen. Beispiel: SamAccountName
- **Active Directory Gruppen-Attributname** - die auf dem LDAP-Server konfigurierten LDAP-Gruppen-Attributnamen. Beispiel: MemberOf für das Gruppenattribut in LDAP.
- **Active Directory Unterattributname** - die LDAP-Unterattributnamen, die auf dem LDAP-Server konfiguriert sind. Beispiel: cn für das Unterattribut in LDAP.
- **Active Directory Authentifizierungsdomäne** - Der AD/LDAP-Domänenname, der für die Authentifizierung verwendet wird. Zum Beispiel ctxnssfb.com.

6. Wählen Sie im Abschnitt **Zielinstanzen** die Citrix ADC-Instanz aus, auf der diese Exchange-Konfiguration bereitgestellt werden soll.

   > **Hinweis**
   >
   > Wenn Sie die kürzlich erkannten Citrix ADC-Instanzen anzeigen möchten, klicken Sie auf das Aktualisierungssymbol.

7. Klicken Sie auf **Erstellen**, um die Konfigurationsdatei zu erstellen und die Konfiguration auf der ausgewählten Citrix ADC-Instanz auszuführen.

   Citrix empfiehlt, dass Sie zuerst **Dry Run** auswählen, um die auf der Zielinstanz erstellten Konfigurationsobjekte zu überprüfen, bevor Sie die tatsächliche Konfiguration auf der Instanz ausführen.

Wenn die Konfiguration erfolgreich erstellt wurde, hat das StyleBook einen virtuellen Content Switching-Server, fünf virtuelle Lastenausgleichsserver und eine LDAP-Richtlinie erstellt, die an einen virtuellen LDAP-Authentifizierungsserver gebunden ist. Außerdem wurden die entsprechenden Dienstgruppen erstellt und an die virtuellen Server mit Lastenausgleich gebunden.

Microsoft SharePoint-StyleBook

April 28, 2021

Microsoft SharePoint 2016 ist eine wichtige Unternehmensanwendung, die in erster Linie ein Dokumentverwaltungs- und Speichersystem bereitstellt, das hochgradig konfigurierbar ist und von allen gängigen Browsern unterstützt wird.

Sie können das Microsoft SharePoint 2016 StyleBook verwenden, um eine Citrix ADC Konfiguration bereitzustellen, die die Microsoft SharePoint 2016 Enterprise-Anwendung in Ihrem Netzwerk optimiert und schützt.

Voraussetzungen

- Microsoft SharePoint 2016
- Citrix Application Delivery Management (ADM), Version 12.0 und höher
- Citrix ADC, Version 10.5 und höher

Citrix ADC Funktionen, die vom Microsoft SharePoint 2016 StyleBook konfiguriert werden

Sie können das Microsoft SharePoint 2016 StyleBook verwenden, um die folgenden Citrix ADC Features für Microsoft SharePoint 2016 zu aktivieren und zu konfigurieren:

- Lastausgleich
- Content Switching
- Responder
- Neuschreiben
- Komprimierung
- Integriertes Caching

Lastausgleich

Citrix ADC Load Balancing verteilt Anfragen gleichmäßig an SharePoint-Server mit Back-End. Die intelligente Überwachung von Back-End-Servern verhindert, dass Anfragen an fehlerhafte Server gesendet werden.

Das SharePoint-StyleBook konfiguriert 12 virtuelle Server mit Lastenausgleich, die jeweils für Lastenausgleichsanforderungen für einen bestimmten Inhaltstyp wie Dokumente, Bilder, Audio-, Video- und andere Dateitypen bestimmt sind.

Citrix ADM unterstützt jetzt den SSL-Modus der SharePoint-Anwendung, indem virtuelle SSL-basierte LB-Server konfiguriert werden. Stellen Sie sicher, dass Sie SSL als Front-End-Protokoll auswählen. Beachten Sie, dass der virtuelle Port standardmäßig auf 443 festgelegt ist.

Content Switching

Content Switching wird verwendet, um Clientanforderungen auf mehrere virtuelle Server mit Lastenausgleich auf der Grundlage bestimmter Arten von angeforderten SharePoint-Inhalten (z. B. Dokumente, Bilder sowie Audio- oder Videodateien) zu verteilen. Das Content Switching-Modul leitet eingehenden Datenverkehr an einen optimal passenden virtuellen Lastausgleichsserver weiter, der diesen Inhaltstyp verarbeiten kann. Sie können daher unterschiedliche Optimierungsrichtlinien auf verschiedene Arten von Datenverkehr anwenden. Beispielsweise können Sie andere Komprimierungs- oder Caching-Richtlinien für Video als für Textdokumente verwenden.

Responder

Die Responder-Funktionalität einer Citrix ADC-Instanz kann verwendet werden, um Benutzer nahtlos von HTTP zu HTTPS umzuleiten. Responder kann auch so konfiguriert werden, dass benutzerdefinierte Fehlerseiten bereitgestellt werden. Die Responder-Richtlinie bestimmt die Anforderungen (Datenverkehr), für die eine Aktion ausgeführt werden muss, und bindet jede Richtlinie an einen virtuellen Lastausgleichsserver. Das SharePoint-StyleBook enthält eine Konfiguration, die Benutzer von HTTP auf HTTPS-URLs umleitet.

Neuschreiben

Das Rewrite-Modul wird verwendet, um Request/Response-Header, URLs oder Inhalte im laufenden Betrieb zu ändern. Dieses Modul arbeitet in Verbindung mit der Datenverarbeitung und kann daher den Verkehrsfluss je nach Anwendungsfall ändern. Beispielsweise kann das Umschreiben Zugriff auf den angeforderten Inhalt bieten, ohne unnötige Details über den Server der Website offenzulegen.

Im SharePoint-StyleBook wird das Rewrite-Feature verwendet, um unnötige Header aus Benutzeranforderungen zu entfernen.

Komprimierung

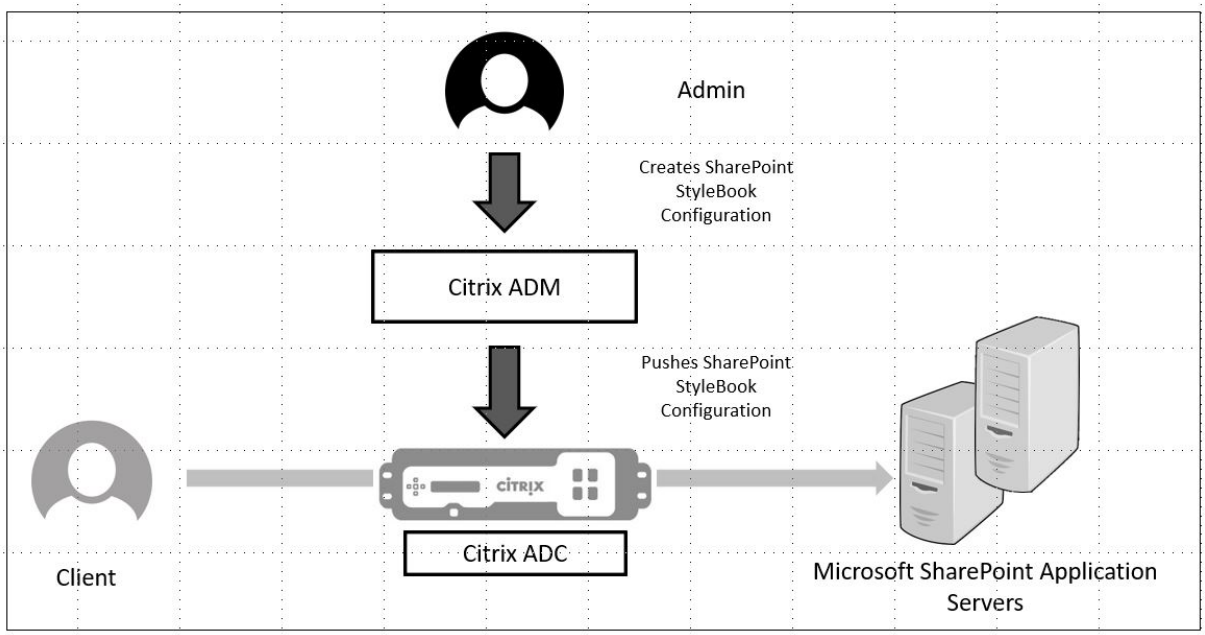
Das Citrix ADC Komprimierungsmodul identifiziert und komprimiert komprimierbare Inhalte. Dieser Prozess verbessert die Datenübertragungszeit und reduziert die Netzwerkbandbreitenanforderungen für die Clients, während CPU-Zyklen auf SharePoint-Inhaltsservern gespart werden. Eine Citrix ADC-Instanz kann sowohl statische als auch dynamisch generierte Daten komprimieren. Es wendet den GZIP- oder den DEFLATE-Komprimierungsalgorithmus an, um fremde und sich wiederholende Informationen aus den Serverantworten zu entfernen und die ursprünglichen Informationen in einem kompakteren und effizienteren Format darzustellen. Die Fähigkeit des Client-Browsers, die Daten zu dekomprimieren, hängt davon ab, welchen Algorithmus oder welche Algorithmen er unterstützt: GZIP, DEFLATE oder beide.

Eine Citrix ADC-Instanz ist so konfiguriert, dass der Text in HTML-, XML-, Nur-Text-, Cascading Stylesheet (CSS) und Microsoft Office-Dokumenten komprimiert wird, aber keine Bilder im GIF- oder JPG-Format komprimiert werden. Zu den Hauptvorteilen des komprimierten Datenverkehrs gehören reduzierte Bandbreitenkosten, WAN-Latenzreduzierung und bessere Serverleistung.

Integriertes Caching

Der Citrix ADC In-Memory-Cache kann SharePoint-Objekte speichern, um häufig angeforderte Inhalte schnell an Benutzer bereitzustellen. Im Cache gespeicherte Inhalte enthalten heruntergeladene Dokumente sowie Audio-, Video- und Bilddateien.

In der folgenden Abbildung wird die Bereitstellung von SharePoint-Servern in einem Netzwerk dargestellt, das von einer Citrix ADC-Instanz auf der Citrix ADM zum Bereitstellen einer SharePoint StyleBook-Konfiguration verwendet wird.



Bereitstellen von SharePoint StyleBook-Konfigurationen

Die folgende Aufgabe unterstützt Sie bei der Bereitstellung des Microsoft SharePoint 2016 StyleBook in Ihrem Unternehmensnetzwerk.

So stellen Sie Microsoft SharePoint 2016 StyleBook bereit:

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Verwaltung** > **Konfiguration**, und klicken Sie auf **Neu erstellen**.

   Auf der Seite **StyleBook auswählen** werden alle StyleBooks angezeigt, die für Ihre Verwendung in Citrix ADM verfügbar sind.

2. Scrollen Sie nach unten und wählen Sie **Microsoft SharePoint 2016 StyleBook** aus.

   > **Hinweis Navigieren Sie**
   >
   > in Citrix ADM zu **Anwendungen**> **Konfigurationen**> **StyleBooks**. Scrollen Sie nach unten, um das **Microsoft SharePoint 2016 StyleBook** zu finden. Klicken Sie im **Microsoft SharePoint 2016 StyleBook-Bedienfeld** auf **Konfiguration erstellen**.

   Das StyleBook öffnet sich als Benutzeroberflächenformular, in dem Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

   Geben Sie Werte für die folgenden Parameter ein:

a) **SharePoint-Anwendungsname**. Name der SharePoint-Konfiguration, die im Netzwerk bereitgestellt werden soll.

b) **Virtuelle SharePoint-IP-Adresse**. Virtuelle IP-Adresse, unter der die Citrix ADC-Instanz Clientanforderungen für die Microsoft SharePoint-Anwendung empfängt.

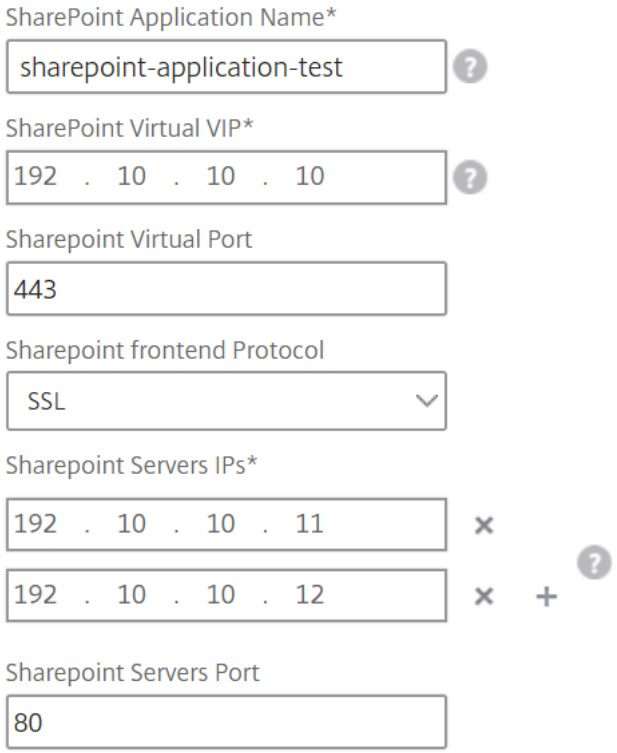
c) **Virtueller SharePoint-Anschluss**. Der TCP-Port, der von den Benutzern beim Zugriff auf die SharePoint-Anwendung verwendet werden soll

d) **SharePoint-Frontend-Protokoll**. Wählen Sie das SharePoint-Frontend-Protokoll aus der Dropdown-Liste aus. Die verfügbaren Optionen sind HTTP oder SSL.

> **Hinweis**
>
> Wenn Sie SSL auswählen, stellen Sie sicher, dass der Parameter Konfiguration umschreiben im Abschnitt Erweiterte SharePoint-Einstellungen in diesem StyleBook aktiviert ist.

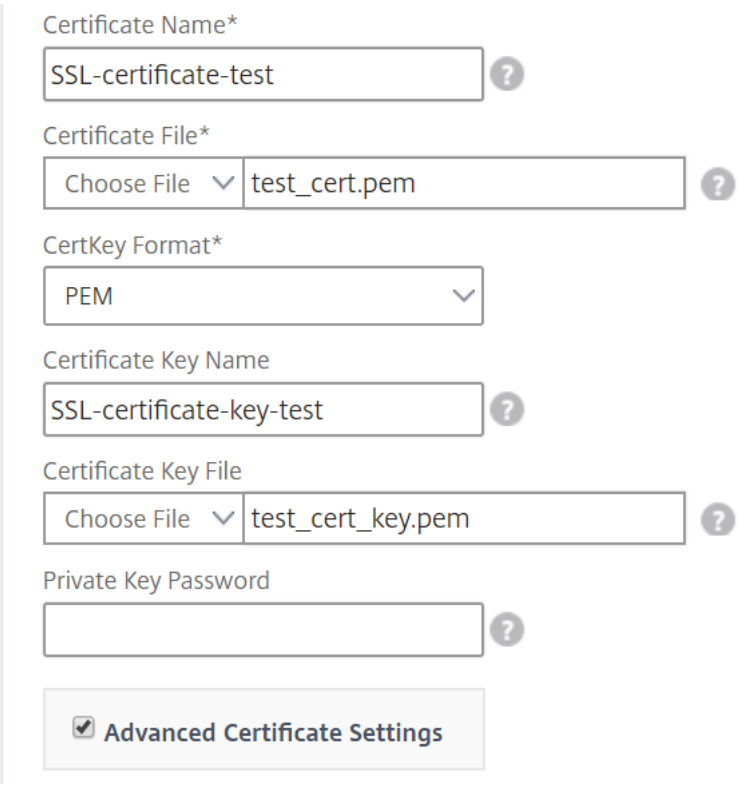
e) **SharePoint Server-IPs**. IP-Adressen aller SharePoint-Server im Netzwerk.

f) **SharePoint-Server-Port**. TCP-Portnummer, die von den SharePoint-Servern verwendet wird. Standardmäßig ist dies 80. Sie können diesen Wert bei Bedarf bearbeiten, stellen Sie jedoch sicher, dass auf diesen Port auf Microsoft SharePoint 2016-Servern zugegriffen werden kann.

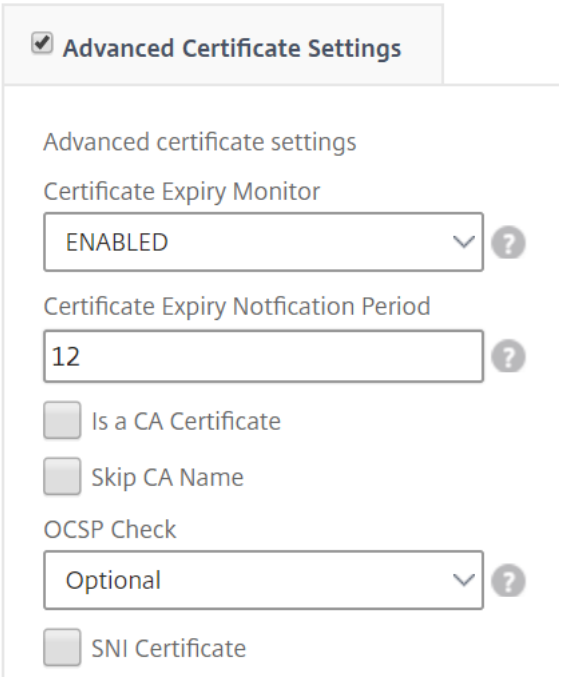


3. Klicken Sie im Abschnitt **Einstellungen für SSL-Zertifikate** auf +, um den Namen des SSL-Zertifikats und den Zertifikatschlüssel einzugeben und die entsprechenden Dateien aus Ihrem

lokalen Speicherordner auszuwählen.

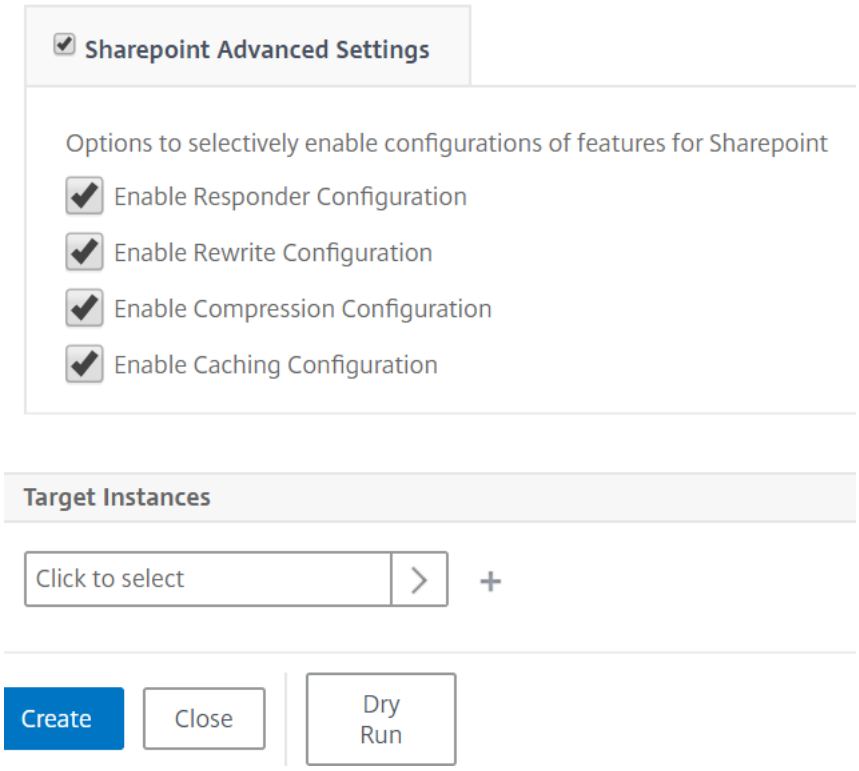


4. Klicken Sie optional auf **Erweiterte Zertifikateinstellungen**, um die Ablaufüberwachung von SSL-Zertifikaten zu aktivieren oder zu deaktivieren. Wenn Sie die Zertifikatablaufüberwachung aktivieren, legen Sie die Anzahl der Tage fest, sodass Citrix ADM nach diesen vielen Tagen, an denen das Zertifikat abläuft, einen Alarm ausgibt. Sie haben auch die Möglichkeit, die OCSP-Prüfung als optionales Feature oder als obligatorisches Feature durchzuführen.



5. Im Abschnitt **Erweiterte SharePoint-Einstellungen** können Sie die Citrix ADC Features aktivieren, die auf den Citrix ADC-Instanzen konfiguriert werden. Während die Load Balancing- und Content Switching-Funktionen standardmäßig auf den Instanzen konfiguriert sind, können Sie die anderen Funktionen auswählen, d. h. die Responderkonfiguration, die Rewrite-Konfiguration, die Komprimierungskonfiguration und die integrierte Caching-Konfiguration, die Sie für die Instanz konfigurieren möchten.
6. Klicken Sie auf **Zielinstanzen**, und wählen Sie die Citrix ADC-Instanz aus, auf der diese SharePoint-Konfiguration bereitgestellt werden soll. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und die Konfiguration auf der ausgewählten Citrix ADC-Instanz bereitzustellen.

> **Hinweis**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC-Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.



> **Hinweis**
>
> Citrix empfiehlt, dass Sie vor dem Ausführen der eigentlichen Konfiguration **Dry Run** auswählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt werden.

Wenn die Konfiguration erstellt und erfolgreich bereitgestellt wird, erstellt das SharePoint-StyleBook einen virtuellen Content Switching-Server und 12 virtuelle Lastenausgleichsserver. Außerdem werden Richtlinien und Dienstgruppen erstellt und an die virtuellen Server mit Lastenausgleich gebunden. Welche Richtlinien erstellt werden, hängt von den Features ab, die im StyleBook während der Erstellung des Konfigurationspakets ausgewählt wurden.

Anzeigen der in der Citrix ADC-Instanz definierten Objekte

Nachdem das Konfigurationspaket auf Citrix ADM erstellt wurde, können Sie alle Objekte anzeigen, die in der Citrix ADC-Instanz für das SharePoint StyleBook erstellt wurden. Navigieren Sie zu **Anwendungen** > **Verwaltung** > **Konfiguration**, und klicken Sie auf **Objekte erstellt anzeigen**. Die folgende Abbildung zeigt einige der erstellten Objekte mit den IP-Adressen, die im Beispiel unter Deploying SharePoint StyleBook Configurations from Citrix ADM angegeben sind.

Type : lbvserver

appflowlog : DISABLED
backuppersistencetimeout : 20
downstateflush : DISABLED
ipv46 : 0.0.0.0
lbmethod : LEASTCONNECTION
name : sharepoint application test frontpage services lb
persistencebackup : SOURCEIP
persistencetype : COOKIEINSERT
port : 0
servicetype : HTTP
timeout : 20

Type : servicegroup

cip : DISABLED
cka : YES
cmp : NO
downstateflush : DISABLED
healthmonitor : NO
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp
servicetype : HTTP
sp : ON
state : ENABLED
tcpb : NO
useproxyport : NO
usip : NO

Type : lbvserver_servicegroup_binding

name : sharepoint-application-test-frontpage-services-lb
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.11
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.12
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : csaction

name : sharepoint-application-test-cs-frontpage-services-csaction
targetlbvserver : sharepoint-application-test-frontpage-services-lb

Type : cspolicy

action : sharepoint-application-test-cs-frontpage-services-csaction
policyname : sharepoint-application-test-cs-frontpage-services-cspol
rule : HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS

Type : csvserver_cspolicy_binding

name : sharepoint-application-test-cs
policyname : sharepoint-application-test-cs-frontpage-services-cspol
priority : 10

Microsoft ADFS-Proxy-StyleBook

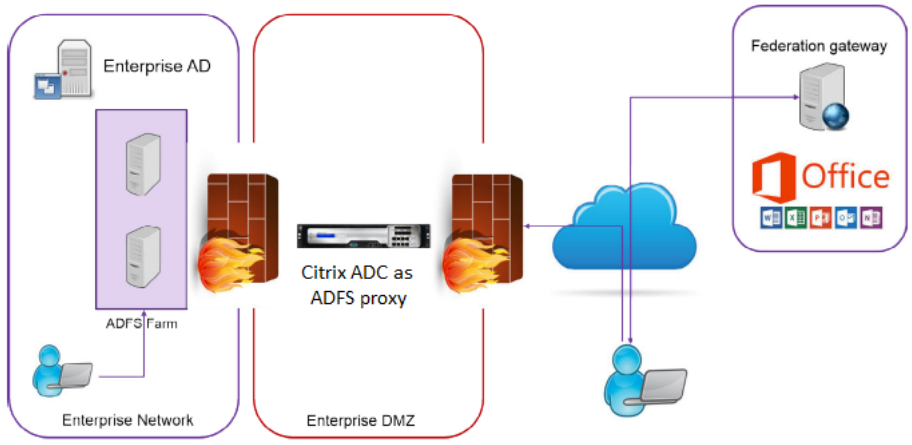
April 28, 2021

Der Microsoft™ ADFS-Proxy spielt eine wichtige Rolle, indem er Single Sign-On-Zugriff sowohl für interne, verbündungsfähige Ressourcen als auch für Cloud-Ressourcen gewährt. Ein Beispiel für Cloud-Ressourcen ist Office 365. Der Zweck des ADFS-Proxyservers besteht darin, Anfragen an ADFS-Server zu empfangen und weiterzuleiten, auf die über das Internet nicht zugegriffen werden kann. Der ADFS-Proxy ist ein Reverse-Proxy und befindet sich normalerweise im Perimeter-Netzwerk (DMZ) Ihrer Organisation. Der ADFS-Proxy spielt eine wichtige Rolle bei der Remotebenutzerkonnektivität und dem Anwendungszugriff.

Citrix ADC verfügt über die präzise Technologie, um sichere Konnektivität, Authentifizierung und Verarbeitung von Verbundidentitäten zu ermöglichen. Die Verwendung von Citrix ADC als ADFS-Proxy vermeidet die Bereitstellung einer zusätzlichen Komponente in der DMZ.

Mit dem Microsoft ADFS Proxy StyleBook in Citrix Application Delivery Management (ADM) können Sie einen ADFS-Proxyserver auf einer Citrix ADC-Instanz konfigurieren.

Die folgende Abbildung veranschaulicht die Bereitstellung einer Citrix ADC-Instanz als ADFS-Proxyserver in der Unternehmens-DMZ.



Vorteile der Verwendung von Citrix ADC als ADFS-Proxy

1. Erfolgt sowohl Lastausgleich als auch ADFS-Proxy-Anforderungen
2. Unterstützt sowohl interne als auch externe Benutzerzugriffsszenarien
3. Unterstützt umfassende Methoden für die Vorauthentifizierung
4. Bietet Benutzern eine einmalige Anmeldung
5. Unterstützt sowohl aktive als auch passive Protokolle
    a) Beispiele für aktive Protokoll-Apps sind — Microsoft Outlook, Microsoft Skype for Business

   b) Beispiele für passive Protokoll-Apps sind: Microsoft Outlook Web App, Webbrowser
6. Gehärtetes Gerät für DMZ-basierte Bereitstellung
7. Mehrwert durch die Verwendung zusätzlicher Citrix ADC Kernfunktionen
   a) Content Switching
   b) SSL-Abladung
   c) Neuschreiben
   d) Sicherheit (Citrix ADC AAA)

Bei aktiven protokollbasierten Szenarien können Sie eine Verbindung zu Office 365 herstellen und Ihre Anmeldeinformationen angeben. Microsoft Federation Gateway kontaktiert den ADFS-Dienst (über ADFS-Proxy) im Auftrag des aktiven Protokollclients. Das Gateway übermittelt die Anmeldeinformationen dann mit der Standardauthentifizierung (401). Citrix ADC behandelt die Clientauthentifizierung vor dem Zugriff auf den ADFS-Dienst. Nach der Authentifizierung stellt der ADFS-Dienst ein SAML-Token für das Federation Gateway bereit. Das Federation Gateway wiederum sendet das Token an Office 365, um Clientzugriff zu ermöglichen.

Für passive Clients erstellt das ADFS-Proxy-StyleBook ein KCD-Benutzerkonto (Kerberos Constrained Delegation). Das KCD-Konto ist für die Kerberos-SSO-Authentifizierung erforderlich, um eine Verbindung mit den ADFS-Servern herzustellen. Das StyleBook generiert auch eine LDAP-Richtlinie und eine Sitzungsrichtlinie. Diese Richtlinien sind später an den virtuellen Citrix ADC AAA-Server gebunden, der die Authentifizierung für passive Clients verarbeitet.

Das StyleBook kann auch sicherstellen, dass die DNS-Server auf dem Citrix ADC für ADFS konfiguriert sind.

Im folgenden Abschnitt zur Konfiguration wird beschrieben, wie Citrix ADC für die Behandlung der aktiven und passiven protokollbasierten Clientauthentifizierung eingerichtet wird.

Konfigurationsdetails

In der folgenden Tabelle sind die Mindestsoftwareversionen aufgeführt, die für die erfolgreiche Bereitstellung dieser Integration erforderlich sind.

Produkt	Erforderliche Mindestversion
Citrix ADC	11.0, Advanced/Premium Lizenz

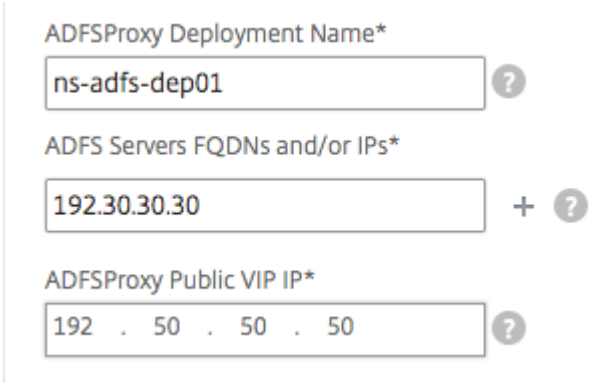
In den folgenden Anweisungen wird davon ausgegangen, dass Sie bereits die entsprechenden externen und internen DNS-Einträge erstellt haben.

Bereitstellen von Microsoft ADFS Proxy StyleBook-Konfigurationen von Citrix ADM

Die folgenden Anweisungen helfen Ihnen bei der Implementierung des Microsoft ADFS Proxy StyleBook in Ihrem Unternehmensnetzwerk.

So stellen Sie Microsoft ADFS-Proxy StyleBook bereit

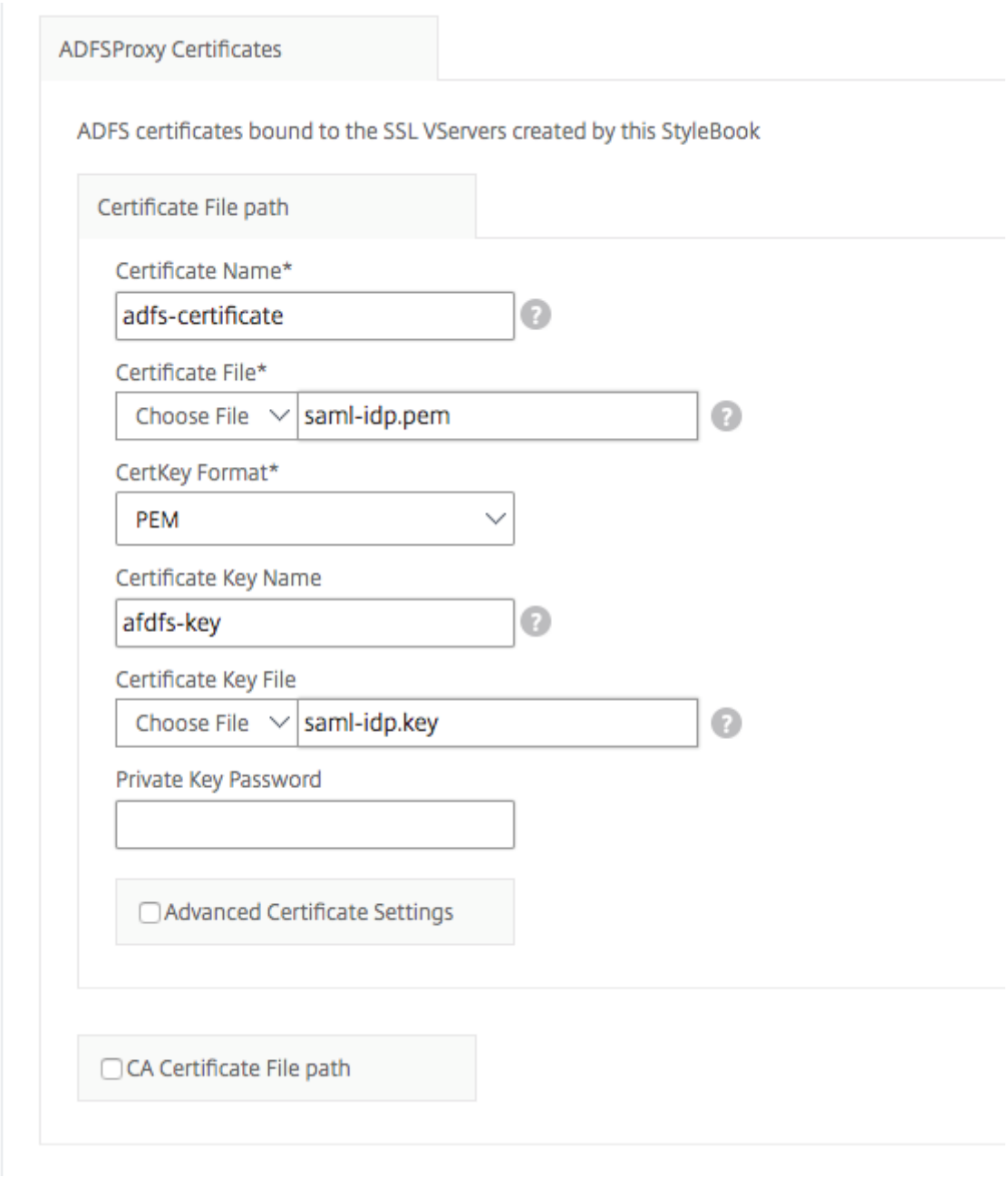
1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **StyleBooks**. Auf der Seite **StyleBooks** werden alle für Ihre Verwendung in Citrix ADM verfügbaren StyleBooks angezeigt.
2. Scrollen Sie nach unten und suchen Sie das **Microsoft ADFS Proxy StyleBook**. Klicken Sie auf **Konfiguration erstellen**.
   Das StyleBook wird als Benutzeroberfläche geöffnet, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
3. Geben Sie Werte für die folgenden Parameter ein:
   a) **ADFS-Proxybereitstellungsname**. Wählen Sie einen Namen für die im Netzwerk bereitgestellte ADFS-Proxy-Konfiguration aus.
   b) **ADFS-Server-FQDNs oder IPs**. Geben Sie die IP-Adressen oder FQDNs (Domänennamen) aller ADFS-Server im Netzwerk ein.
   c) **ADFS Proxy Public VIP IP**. Geben Sie die öffentliche virtuelle IP-Adresse auf dem Citrix ADC ein, der als ADFS-Proxyserver ausgeführt wird.



4. Geben Sie im Abschnitt **ADFS-Proxyzertifikate** die Details des SSL-Zertifikats und des Zertifikatsschlüssels ein.

   Dieses SSL-Zertifikat ist an alle virtuellen Server gebunden, die auf der Citrix ADC-Instanz erstellt wurden.

   Wählen Sie die entsprechenden Dateien aus Ihrem lokalen Speicherordner aus. Sie können auch das Kennwort für den privaten Schlüssel eingeben, um verschlüsselte private Schlüssel im PEM-Format zu laden.



Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie Zertifikatablaufbenachrichtigungszeitraum eingeben, den Zertifikatablaufmonitor aktivieren oder deaktivieren.

5. Optional können Sie das Kontrollkästchen **SSL-CA-Zertifikat** aktivieren, wenn für das SSL-Zertifikat ein öffentliches Zertifizierungsstellenzertifikat auf Citrix ADC installiert werden muss. Stellen Sie sicher, dass Sie Ist ein Zertifizierungsstellenzertifikat im Abschnitt **Erweiterte Zertifikateinstellungen** auswählen.
6. Aktivieren Sie die Authentifizierung für aktive und passive Clients. Geben Sie den DNS-

Domänennamen ein, der in Active Directory für die Benutzerauthentifizierung verwendet wird. Anschließend können Sie die Authentifizierung entweder für aktive oder passive Clients oder für beide konfigurieren.

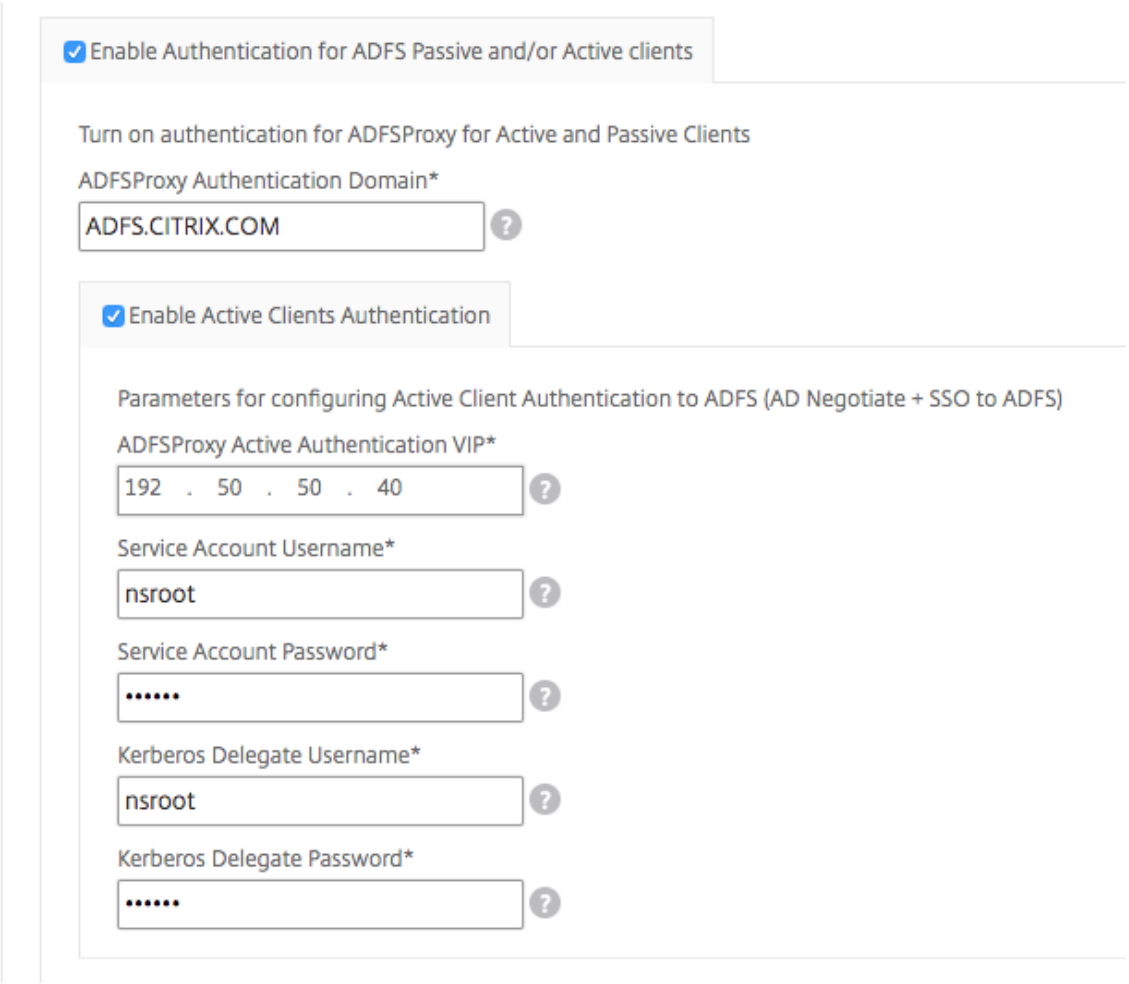
7. Geben Sie die folgenden Details ein, um die Authentifizierung für aktive Clients zu aktivieren:

   > **Hinweis:**
   >
   > Es ist optional, die Unterstützung für aktive Clients zu konfigurieren.

   a) **ADFS Proxy Active Authentication VIP**. Geben Sie die virtuelle IP-Adresse des virtuellen Authentifizierungsservers auf der Citrix ADC-Instanz ein, in der die aktiven Clients zur Authentifizierung umgeleitet werden.

   b) **Benutzername des Dienstkontos**. Geben Sie den Benutzernamen des Dienstkontos ein, der von Citrix ADC verwendet wird, um Ihre Benutzer im Active Directory zu authentifizieren.

   c) **Kennwort des Dienstkontos**. Geben Sie das Kennwort ein, das von Citrix ADC verwendet wird, um Ihre Benutzer beim Active Directory zu authentifizieren.



8. Konfigurieren Sie die Authentifizierung für passive Clients, indem Sie die entsprechende Option aktivieren und die LDAP-Einstellungen konfigurieren.

   > **Hinweis:**
   >
   > Es ist optional, die Unterstützung für passive Clients zu konfigurieren.

   Geben Sie die folgenden Details ein, um die Authentifizierung für passive Clients zu aktivieren:

   a) **LDAP-Basis (Active Directory)**. Geben Sie den Basisdomänennamen für die Domäne ein, in der sich die Benutzerkonten im Active Directory (AD) befinden, um die Authentifizierung zu ermöglichen. Zum Beispiel: `dc=netscaler,dc=com`

   b) **LDAP (Active Directory) Bindet DN**. Fügen Sie ein Domänenkonto hinzu (unter Verwendung einer E-Mail-Adresse zur Vereinfachung der Konfiguration), das über Berechtigungen zum Durchsuchen der AD-Struktur verfügt. Zum Beispiel, cn=Manager,`dc=netscaler,dc=com`

   c) **LDAP (Active Directory) Bindet DN Kennwort**. Geben Sie das Kennwort des Domänenkontos für die Authentifizierung ein.

      Einige andere Felder, die Sie in die Werte in diesem Abschnitt eingeben müssen, sind wie folgt:

   d) **LDAP-Server-IP (Active Directory)**. Geben Sie die IP-Adresse des Active Directory Servers ein, damit die AD-Authentifizierung ordnungsgemäß funktioniert.

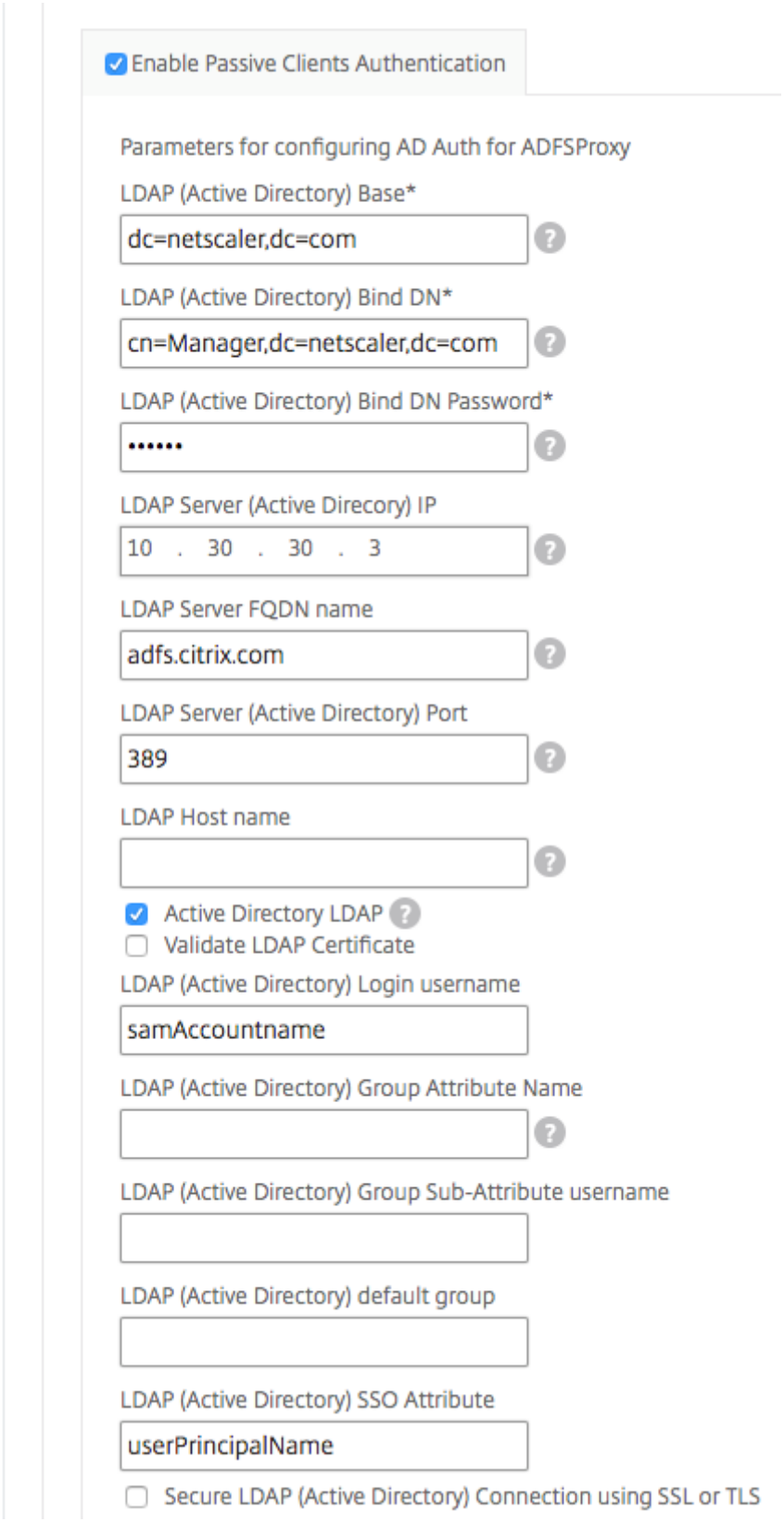
   e) **FQDN-Name des LDAP-Servers**. Geben Sie den FQDN-Namen des Active Directory Servers ein. Der FQDN-Name ist optional. Geben Sie die IP-Adresse wie in Schritt 1 oder den FQDN-Namen an.

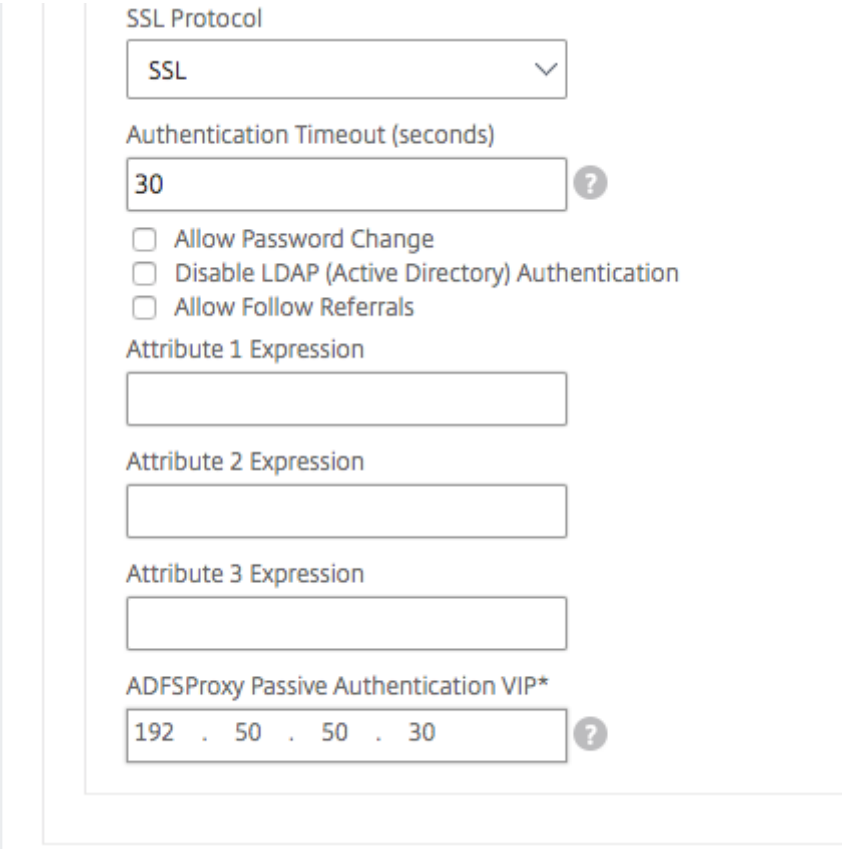
   f) **LDAP-Server-Active Directory Port**. Standardmäßig sind die TCP- und UDP-Ports für das LDAP-Protokoll 389, während der TCP-Port für Secure LDAP 636 ist.

   g) **LDAP-Anmeldebenutzername (Active Directory)**. Geben Sie den Benutzernamen als “sAMAccountName” ein.

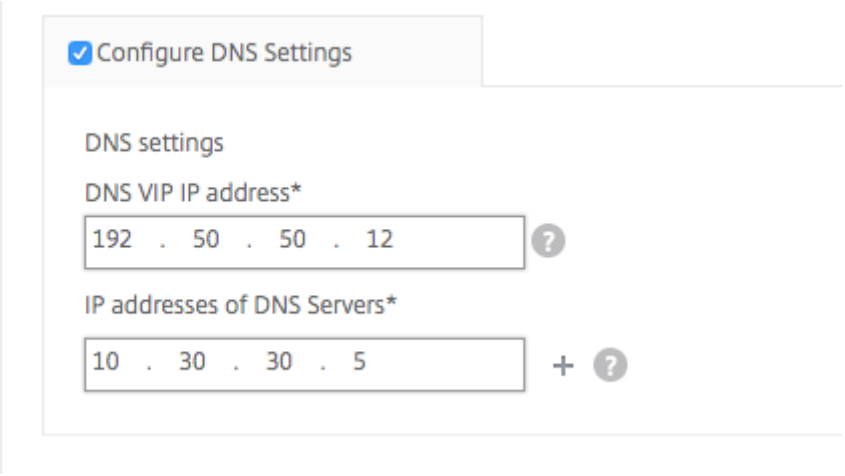
   h) **ADFS Proxy Passive Authentifizierung VIP**. Geben Sie die IP-Adresse des virtuellen ADFS-Proxyservers für passive Clients ein.

      > **Hinweis:**
      >
      > Die mit * gekennzeichneten Felder sind Pflichtfelder.

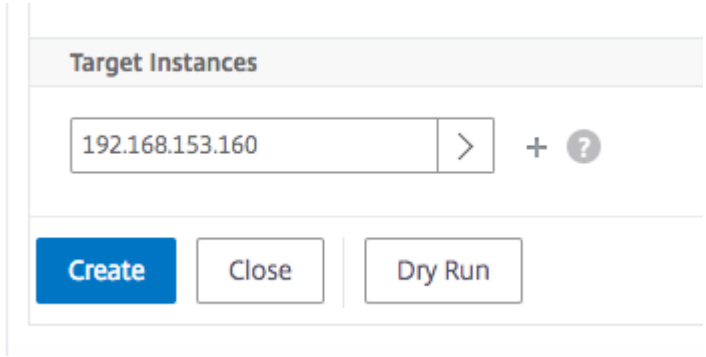




9. Optional können Sie auch eine DNS-VIP für Ihre DNS-Server konfigurieren.



10. Klicken Sie auf **Zielinstanzen**, und wählen Sie die Citrix ADC-Instanzen aus, um diese Microsoft ADFS-Proxykonfiguration bereitzustellen. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und die Konfiguration auf den ausgewählten Citrix ADC-Instanzen bereitzustellen.

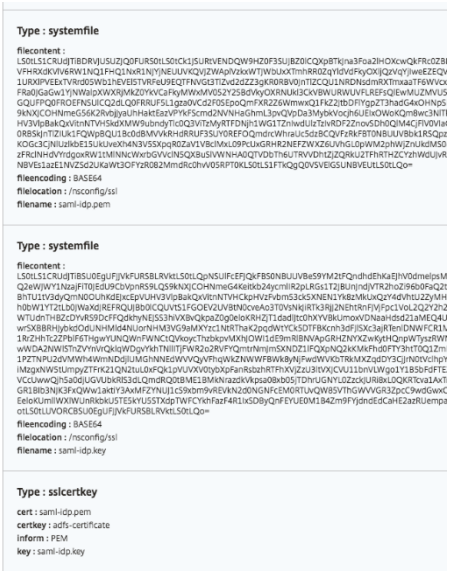


Hinweis

Citrix empfiehlt, dass Sie vor dem Ausführen der eigentlichen Konfiguration die Option **Dry Run auswählen.** Sie können zunächst die Konfigurationsobjekte anzeigen, die vom StyleBook auf den Citrix ADC Zielinstanzen erstellt werden. Sie können dann auf **Erstellen** klicken, um die Konfiguration auf den ausgewählten Instanzen bereitzustellen.

Erstellte Objekte

Mehrere Konfigurationsobjekte werden erstellt, wenn die ADFS-Proxykonfiguration auf der Citrix ADC-Instanz bereitgestellt wird. In der folgenden Abbildung wird die Liste der erstellten Objekte angezeigt.



Objects Added on Instance : 192.168.153.160 | Count : 57

Type : nsfeature

Meta Properties
action : **enable**

feature : cs lb ssl rewrite aaa

Type : lbvserver

ipv46 : 192.50.50.12
name : ns-adfs-dep01-adfs-dns
port : 53
servicetype : DNS

Type : service

ip : 10.30.30.5
name : ns-adfs-dep01-dns-svc-1
port : 53
servicetype : DNS

Type : lbvserver_service_binding

name : ns-adfs-dep01-adfs-dns
servicename : ns-adfs-dep01-dns-svc-1

Type : authenticationnegotiateaction

domain : ADFS.CITRIX.COM
domainuser : nsroot
domainuserpasswd : nsroot
name : ns-adfs-dep01-negotiate-action

Type : authenticationpolicy

action : ns-adfs-dep01-negotiate-action
name : ns-adfs-dep01-negotiate-policy
rule : true

Type : aaakcdaccount

delegateduser : nsroot
kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
kcdpassword : nsroot
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
name : ns-adfs-dep01-adfs-auth401-tmsession-action
persistentcookie : ON
persistentcookievalidity : 3
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-auth401-tmsession-action
name : ns-adfs-dep01-adfs-auth401-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.40
maxloginattempts : 255
name : ns-adfs-dep01-adfs-auth401-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-auth401-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-negotiate-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-adfs-auth401-tmsession-policy
priority : 10

Type : authenticationldapaction

authentication : ENABLED
authtimeout : 30
followreferrals : OFF
ldapbase : dc=netscaler,dc=com
ldapbinddn : cn=Manager,dc=netscaler,dc=com
ldapbinddnpassword : nsroot
ldaploginname : samAccountname
name : ns-adfs-dep01-ldap-action
passwdchange : DISABLED
sectype : PLAINTEXT
serverip : 10.30.30.3
serverport : 389
ssonameattribute : userPrincipalName
svrtype : AD
validateservercert : NO

Type : authenticationpolicy

action : ns-adfs-dep01-ldap-action
name : ns-adfs-dep01-ldap-policy
rule : true

Type : aaakcdaccount

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
name : ns-adfs-dep01-adfs-ldap-tmsession-action
persistentcookie : OFF
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-ldap-tmsession-action
name : ns-adfs-dep01-adfs-ldap-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.30
maxloginattempts : 255
name : ns-adfs-dep01-adfs-ldap-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-ldap-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-ldap-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-adfs-ldap-tmsession-policy
priority : 10

Type : csvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-cs
port : 443
servicetype : SSL

Type : lbvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
port : 445
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : server

ipaddress : 192.30.30.30
name : 192.30.30.30

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
priority : 9800

Type : lbvserver

appflowlog : ENABLED
authentication : ON
authenticationhost : ADFS.CITRIX.COM
authn401 : OFF
authnvsname : ns-adfs-dep01-adfs-ldap-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
port : 446
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
priority : 9900

Type : lbvserver

appflowlog : ENABLED
authentication : OFF
authn401 : ON
authnvsname : ns-adfs-dep01-adfs-auth401-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
port : 444
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
rule : true

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
priority : 10000

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-cs

Type : rewritepolicylabel

labelname : ns-adfs-dep01-request-rewritepolicylabel
transform : HTTP_REQ

Type : rewritepolicylabel

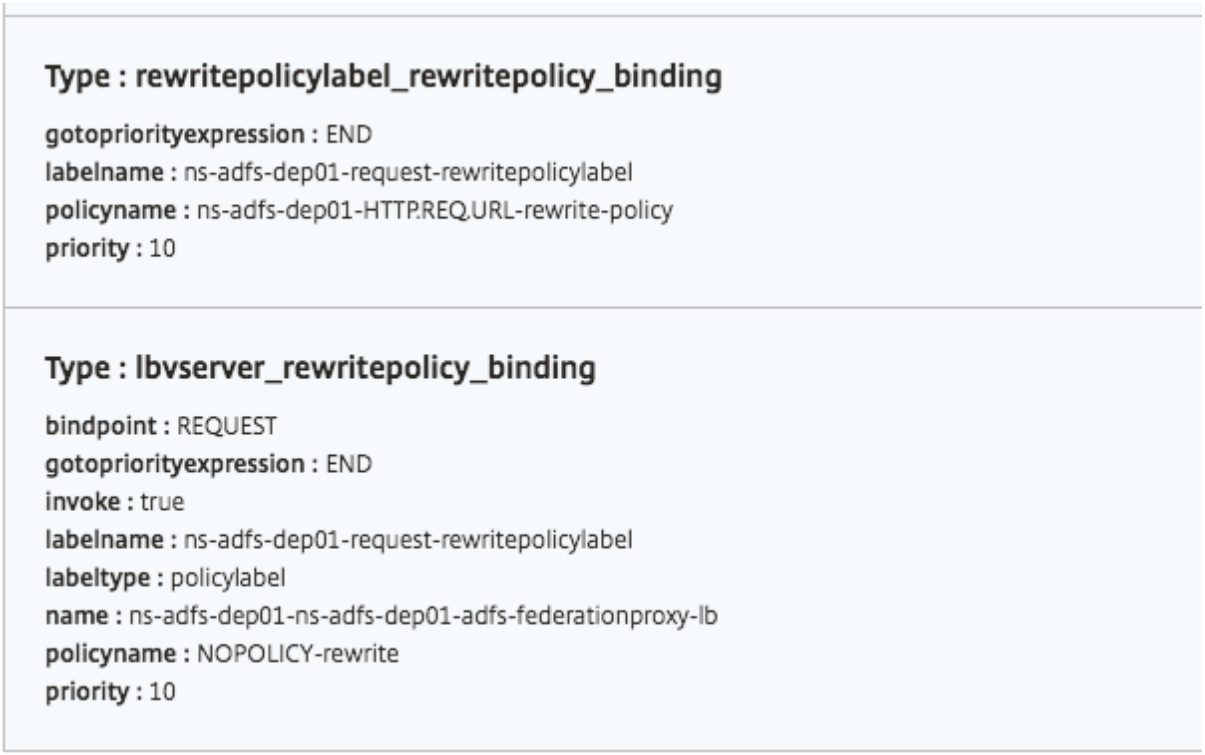
labelname : ns-adfs-dep01-response-rewritepolicylabel
transform : HTTP_RES

Type : rewriteaction

name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
stringbuilderexpr : "/adfs/services/trust/proxymex"
target : HTTP.REQ.URL
type : REPLACE

Type : rewritepolicy

action : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") && (!HTTP.REQ.URL.CONTAINS("/trust/proxymex"))



Oracle e-business StyleBook

April 28, 2021

Oracle E-Business Suite ist die umfassendste Suite integrierter, globaler Geschäftsanwendungen. Diese Suite ermöglicht Unternehmen, bessere Entscheidungen zu treffen, Kosten zu senken und die Leistung zu steigern. Sie besteht aus den folgenden Anwendungen.

- Enterprise Resource Planning (ERP)
- Kundenbeziehungsmanagement (CRM)
- Supply-Chain-Management (SCM)

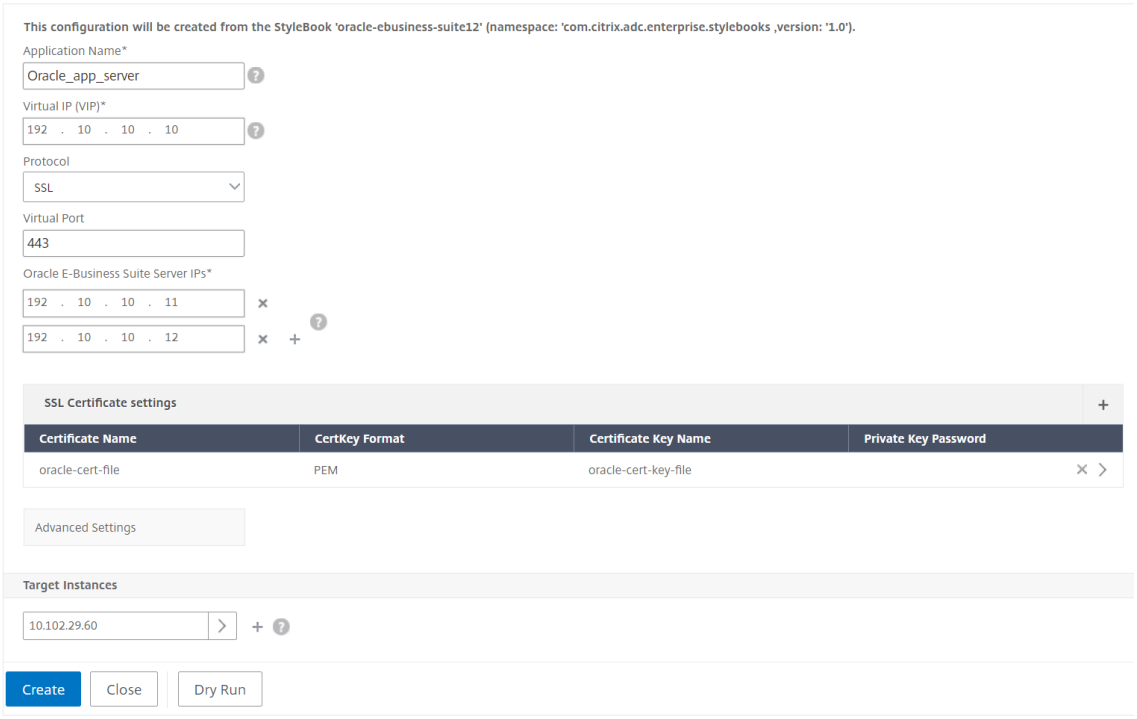
Diese Computeranwendungen werden entweder von Oracle entwickelt oder erworben. Mit dem Oracle E-Business Suite 12.2 StyleBook können Sie die Konfiguration auf den ausgewählten Citrix ADC-Instanzen bereitstellen.

Dieses StyleBook erstellt eine Lastausgleichskonfiguration, die einen virtuellen Lastausgleichsserver, eine Dienstgruppe und eine Liste von Diensten umfasst. Außerdem werden die Dienste an die Dienstgruppe gebunden und die Dienstgruppe an den virtuellen Server gebunden. Sie können die verschlüsselte Kommunikation auswählen, indem Sie SSL auswählen und die SSL-Dateien und Schlüsseldateien Ihres lokalen Systems bereitstellen.

So erstellen Sie eine Konfiguration für Oracle E-Business Suite 12.2

1. Navigieren Sie in Citrix Application Delivery Management (ADM) zu **Anwendungen** > **Konfiguration > StyleBooks**. Auf der Seite **StyleBooks** werden alle StyleBooks angezeigt, die in Ihrem Citrix ADM verfügbar sind. Scrollen Sie nach unten und wählen Sie **Oracle E-Business Suite 12.2**. Sie können auch die Suchoption verwenden, um das StyleBook zu durchsuchen.
2. Klicken Sie im StyleBook-Bedienfeld auf **Konfiguration erstellen**.
3. Geben Sie den Namen der Load Balancer-Anwendung und die virtuelle IP-Adresse im Abschnitt Load Balancer-Einstellungen ein.
4. Wählen Sie das erforderliche Protokoll aus. Sie haben hier zwei Optionen - HTTP und HTTP-S/SSL. Sie können auch die Portnummer eingeben.
5. Geben Sie die IP-Adressen aller Oracle E-Business Suite-Anwendungsserver im Netzwerk ein, die vom Lastausgleich ausgeglichen werden sollen. Klicken Sie auf **+**, um weitere Server-IP-Adressen hinzuzufügen.
6. Wählen Sie im Abschnitt **SSL-Zertifikateinstellungen** die entsprechenden Dateien aus Ihrem lokalen Speicher aus. Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie weitere Details konfigurieren, wie z. B. das Ablaufdatum des Zertifikats. Sie können den Zertifikatablaufmonitor auch aktivieren oder deaktivieren.

   Wählen Sie die Citrix ADC Zielinstanz aus, für die die Konfiguration erstellt werden muss, und klicken Sie auf **Erstellen**.



> **Tipp**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC-Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen. Das Aktualisierungssymbol ist nur auf Citrix ADM verfügbar.

Webanwendungs-Firewall-StyleBook

April 28, 2021

Citrix Web App Firewall ist eine Web Application Firewall (WAF), die Webanwendungen und Websites vor bekannten und unbekannten Angriffen schützt, einschließlich aller Anwendungen und Zero-Day-Bedrohungen.

Citrix ADM bietet jetzt ein Standard-StyleBook, mit dem Sie eine Anwendungs-Firewall-Konfiguration auf Citrix ADC-Instanzen bequemer erstellen können.

Bereitstellen von Anwendungs-Firewall-Konfigurationen

Die folgende Aufgabe unterstützt Sie bei der Bereitstellung einer Lastausgleichskonfiguration zusammen mit der Anwendungsfirewall und der IP-Reputationsrichtlinie auf Citrix ADC-Instanzen in Ihrem Unternehmensnetzwerk.

So erstellen Sie eine LB-Konfiguration mit Applikations-Firewall-Einstellungen:

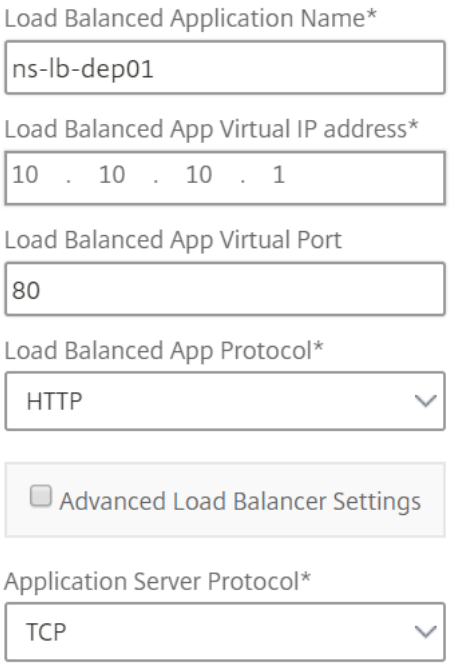
1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfigurationen** > **StyleBooks**. Auf der Seite StyleBooks werden alle StyleBooks angezeigt, die für die Verwendung in Citrix ADM verfügbar sind. Scrollen Sie nach unten und suchen Sie das HTTP/SSL Load Balancing StyleBook mit der Firewall-Richtlinie und der IP-Reputationsrichtlinie. Sie können auch nach dem StyleBook suchen, indem Sie den Namen als eingeben `lb-appfw`. Klicken Sie auf **Konfiguration erstellen**.

   Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

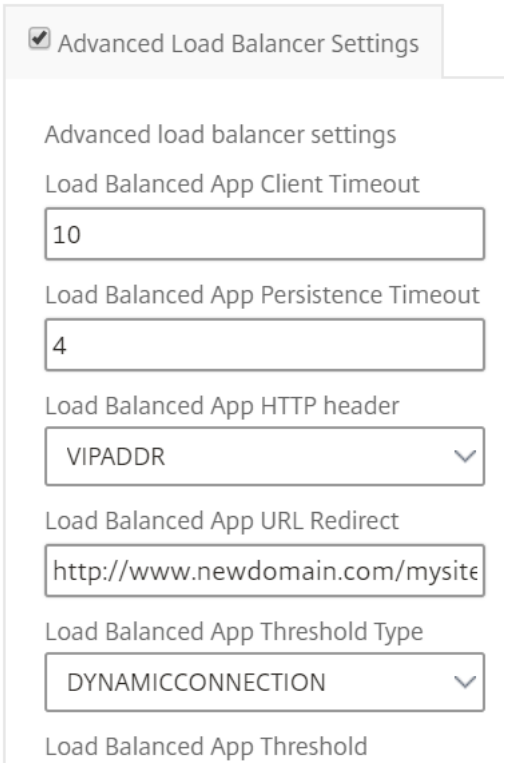
2. Geben Sie Werte für die folgenden Parameter ein:

   - **Anwendungsname für Lastausgleich**. Name der Lastausgleichskonfiguration mit der Anwendungsfirewall, die in Ihrem Netzwerk bereitgestellt werden soll.
   - **Laden Sie ausbalancierte virtuelle IP-Adresse der App**. Virtuelle IP-Adresse, unter der die Citrix ADC-Instanz Clientanforderungen empfängt.
   - **Laden Sie den virtuellen Port für ausbalancierte App**. Der TCP-Port, der von den Benutzern beim Zugriff auf die Lastausgleichsanwendung verwendet wird.

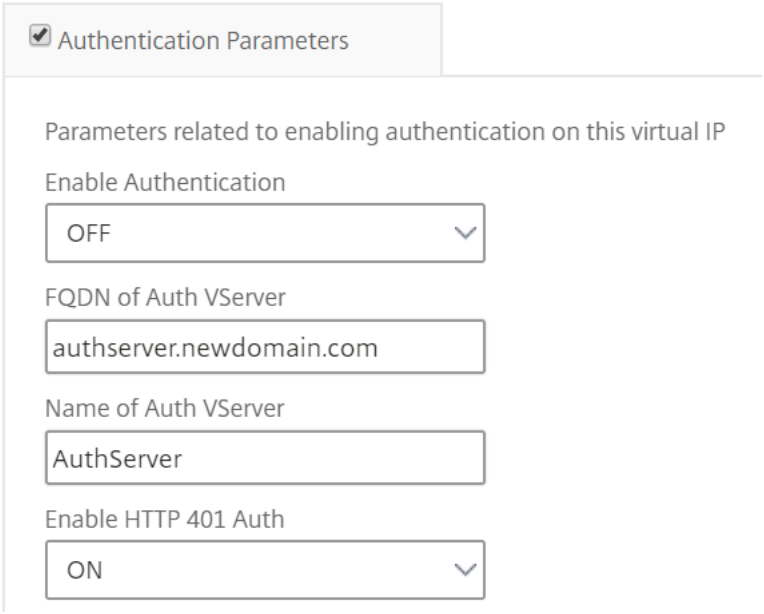
- **Load Balanced App-Protokoll**. Wählen Sie das Front-End-Protokoll aus der Liste aus.
- **Anwendungsserver-Protokoll**. Wählen Sie das Protokoll des Anwendungsservers aus.



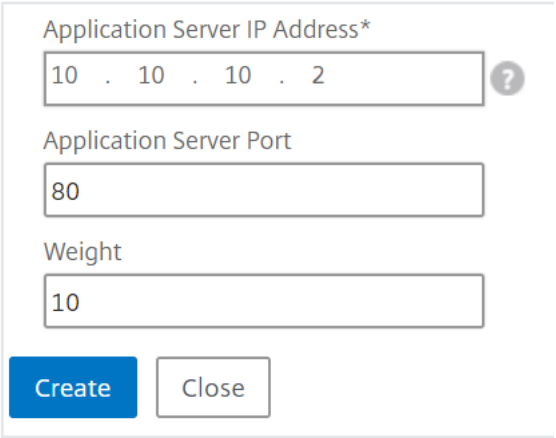
3. Optional können Sie die **erweiterten Lastenausgleichseinstellungen**aktivieren und konfigurieren.



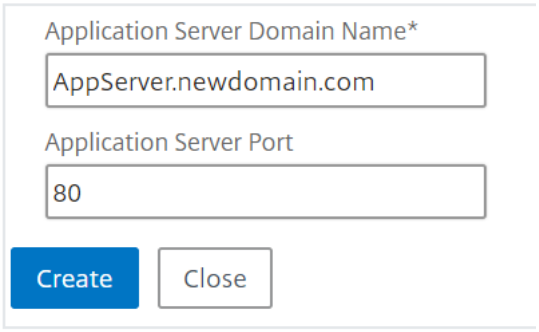
4. Optional können Sie auch einen Authentifizierungsserver für die Authentifizierung des Datenverkehrs für den virtuellen Lastausgleichsserver einrichten.



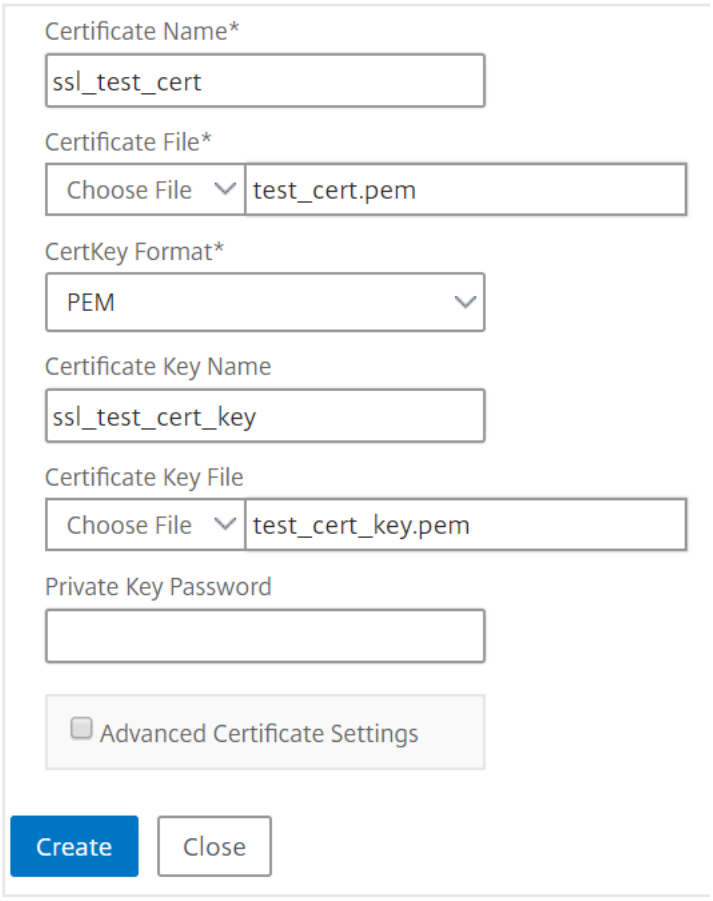
5. Klicken Sie im Abschnitt Server-IPs und -Ports auf +, um Anwendungsserver und die Ports zu erstellen, auf die sie zugegriffen werden können.



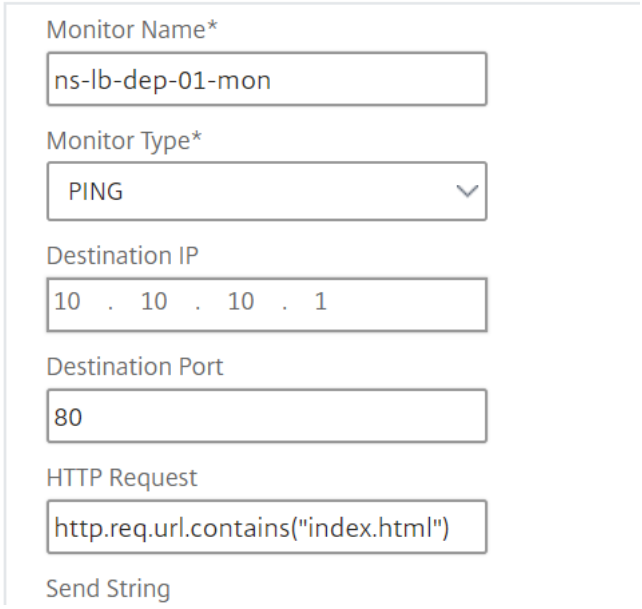
6. Sie können auch FQDN-Namen für Anwendungsserver erstellen.



7. Sie können auch die Details des SSL-Zertifikats angeben.

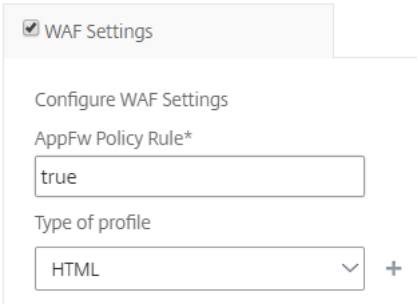


8. Sie können auch Monitore in der Citrix ADC Zielinstanz erstellen.



9. Um eine Anwendungsfirewall auf dem virtuellen Server zu konfigurieren, aktivieren Sie WAF-Einstellungen.

   Stellen Sie sicher, dass die Richtlinienregel für die Anwendungsfirewall wahr ist, wenn Sie die Einstellungen für die Anwendungsfirewall auf den gesamten Datenverkehr in diesem VIP anwenden möchten. Andernfalls geben Sie die Citrix ADC Richtlinienregel an, um eine Teilmenge von Anforderungen auszuwählen, auf die die Firewalleinstellungen der Anwendung angewendet werden sollen. Wählen Sie als Nächstes den Profiltyp aus, der angewendet werden soll - HTML oder XML.

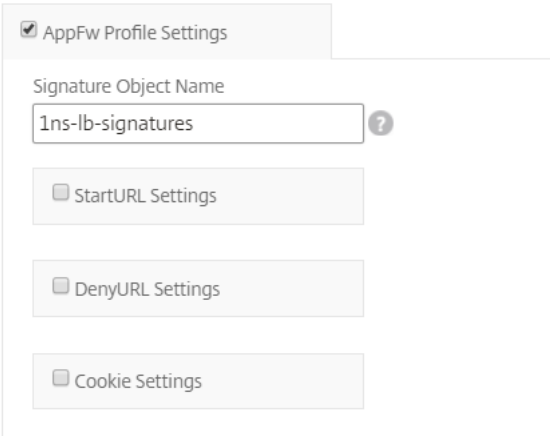


10. Optional können Sie detaillierte Profileinstellungen der Anwendungsfirewall konfigurieren, indem Sie das Kontrollkästchen Profileinstellungen der Anwendungsfirewall aktivieren.

11. Wenn Sie die Anwendungsfirewall Signaturen konfigurieren möchten, geben Sie optional den Namen des Signaturobjekts ein, das auf der Citrix ADC-Instanz erstellt wird, in der der virtuelle Server bereitgestellt werden soll.

> **Hinweis**
>
> Sie können mit diesem StyleBook kein Signature-Objekt erstellen.

12. Als Nächstes können Sie auch andere Anwendungs-Firewall-Profileinstellungen wie StartURL-Einstellungen, DenyURL-Einstellungen und andere konfigurieren.

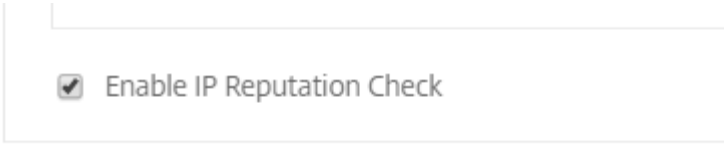


Weitere Informationen zur Anwendungsfirewall und Konfigurationseinstellungen finden Sie unter Anwendungsfirewall.

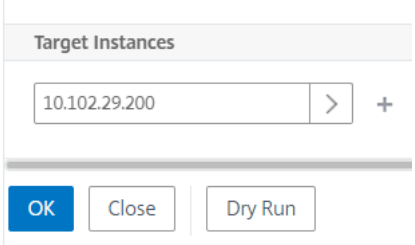
13. Wählen Sie im Abschnitt " **Target Instanzen** " die Citrix ADC-Instanz aus, auf der der virtuelle Lastausgleichsserver mit der Anwendungsfirewall bereitgestellt werden soll.

> **Hinweis**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC-Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

14. Sie können auch die **IP-Reputationsprüfung** aktivieren, um die IP-Adresse zu identifizieren, die unerwünschte Anfragen sendet. Sie können die IP-Reputationsliste verwenden, um Anforderungen vorbeugend abzulehnen, die von der IP mit der schlechten Reputation stammen.



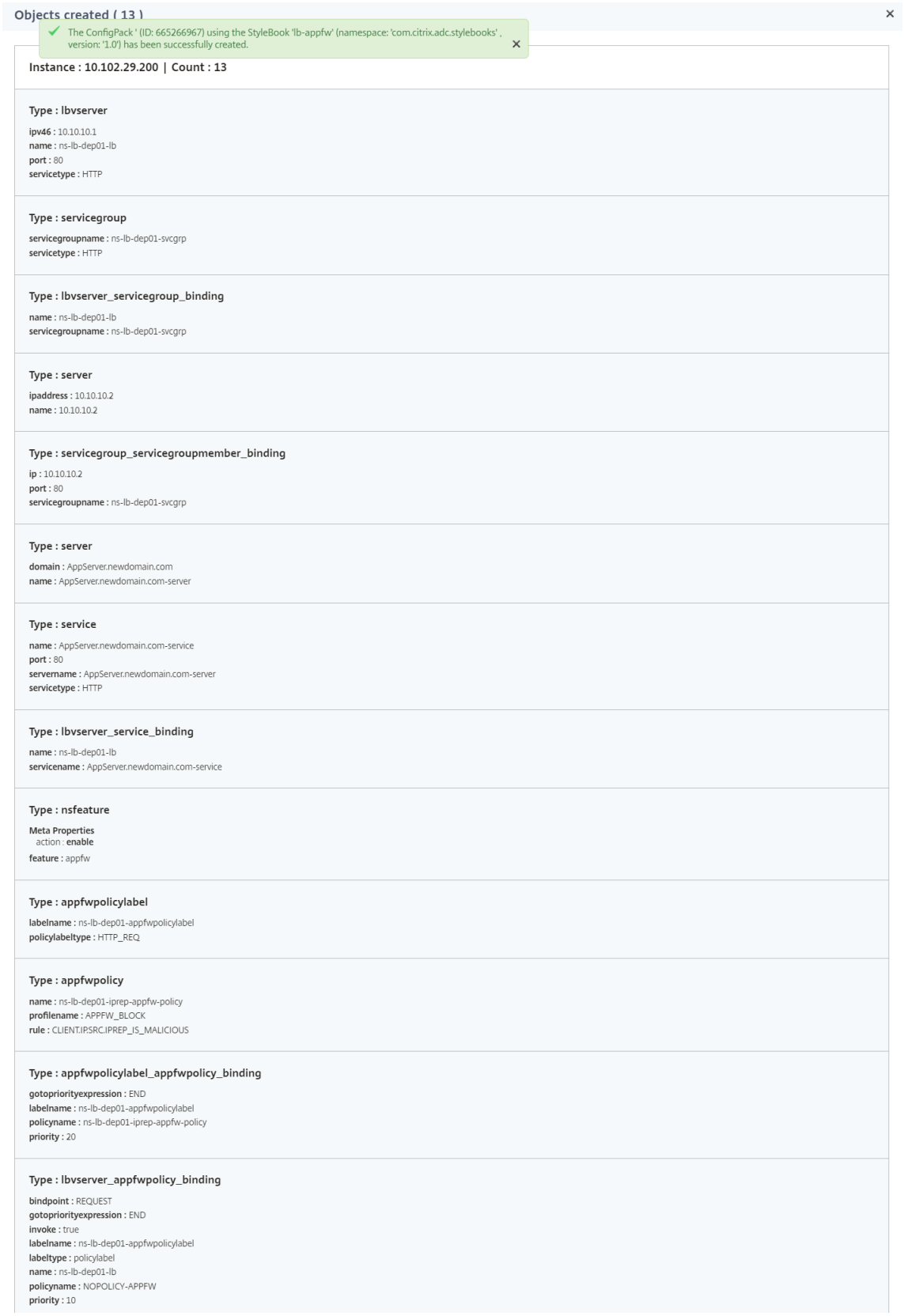
15. Klicken Sie auf **Erstellen**, um die Konfiguration für die ausgewählten Citrix ADC-Instanzen zu erstellen.



> **Tipp**
>
> Citrix empfiehlt, dass Sie Dry Run auswählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt werden müssen, bevor Sie die eigentliche Konfiguration auf der Instanz ausführen.

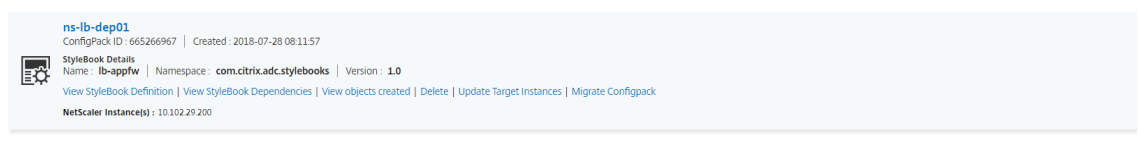
Wenn die Konfiguration erfolgreich erstellt wurde, erstellt das StyleBook den erforderlichen virtuellen Lastenausgleichsserver, Anwendungsserver, Dienste, Dienstgruppen, Anwendungsfirewall Labels, Anwendungsfirewall Richtlinien und bindet sie an den virtuellen Lastausgleichsserver.

Die folgende Abbildung zeigt die in jedem Server erstellten Objekte:



16. Um das ConfigPack anzuzeigen, das auf Citrix ADM erstellt wurde, navigieren Sie zu **Anwendun-**

gen > **Konfigurationen**.



Erstellen von WAF- und BOT-Profilen mit StyleBook

April 28, 2021

Wenn Sie eine Richtlinie für eine API-Ressource in **API Gateway**auswählen können, können Sie die Kriterien zur Verkehrsauswahl definieren, um eine API-Anfrage zu authentifizieren. Außerdem können Sie API-Sicherheitsrichtlinien für den API-Datenverkehr konfigurieren. Weitere Informationen finden Sie unter API-Gateway verwalten.

Sie können WAF- und BOT-Richtlinien für eine API-Ressource konfigurieren. Bevor Sie eine Richtlinie konfigurieren, müssen Sie sicherstellen, dass Sie ihr Profil in Citrix Application Delivery Management (ADM) erstellen. Verwenden Sie die folgenden Standard-StyleBooks, um ein Profil zu erstellen:

- API WAF Erkennung StyleBook
- API BOT Erkennung StyleBook

Erstellen Sie ein WAF-Profil mit dem StyleBook

Führen Sie Folgendes aus, um ein WAF-Profil zu erstellen:

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfigurationen** > **StyleBooks**. Suchen Sie nach dem StyleBook, indem Sie den Namen als eingeben `api-waf-profile`. Klicken Sie auf **Konfiguration erstellen**.

   Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

2. Geben Sie Werte für die folgenden Parameter an:

   - **API WAF-Profilname** - Ein Name zur Identifizierung eines WAF-Profils.
   - **Anwendungstyp** - Fügen Sie dem Profil Anwendungstypen hinzu. Das WAF-Profil unterstützt JSON- und XML-Anwendungstypen.

3. Optional: Aktivieren Sie **Sicherheitseinstellungen**, um HTTP-, JSON- oder XML-Schutzprüfungen anzugeben. Sie können auch eine Fehler-URL für die Citrix Web App Firewall angeben. Weitere Informationen finden Sie unter Erstellen eines Web App Firewall-Profils.

4. Wählen Sie die Citrix ADC-Zielinstanz oder Instanzgruppe aus, auf der Sie diese Konfiguration bereitstellen möchten.
5. Klicken Sie auf **Erstellen**.

Informationen zum Konfigurieren einer WAF-Richtlinie finden Sie unter Hinzufügen von Richtlinien zu einer API-Bereitstellung.

Erstellen Sie ein BOT-Profil mit dem StyleBook

Führen Sie Folgendes aus, um ein BOT-Profil zu erstellen:

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfigurationen** > **StyleBooks**. Suchen Sie nach dem StyleBook, indem Sie den Namen als eingeben `api-bot-profile`. Klicken Sie auf **Konfiguration erstellen**.

   Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
2. Geben Sie in **BOT Profile Name**einen Namen zur Identifizierung eines BOT-Profils an.
3. Optional können Sie die folgenden Optionen basierend auf Ihren Anforderungen aktivieren:
   - **Überprüfung der IP-Reputation aktivieren** - Diese Option identifiziert die IP-Adresse, die unerwünschte Anfragen sendet. Sie können die IP-Reputationsliste verwenden, um Anforderungen vorbeugend abzulehnen, die von der IP mit der schlechten Reputation stammen.
   - **Aktivieren von BOT-Signaturen** - Geben Sie den Namen der BOT-Sig Es blockiert die Anfragen von der angegebenen Signatur.
   - **Liste zulassen** - Geben Sie die IPv4- oder Subnetzadresse (CIDR) an. Diese Option ermöglicht es dem BOT-Profil, Anfragen von der angegebenen IPv4- oder Subnetzadresse zu Bypass.
   - **Liste ablehnen** - Geben Sie die IPv4- oder Subnetzadresse (CIDR) an. Diese Option ermöglicht es dem BOT-Profil, Anfragen von der angegebenen IPv4- oder Subnetzadresse zu blockieren.
4. Wählen Sie die Citrix ADC-Zielinstanz oder Instanzgruppe aus, auf der Sie diese Konfiguration bereitstellen möchten.
5. Klicken Sie auf **Erstellen**.

Informationen zum Konfigurieren einer BOT-Richtlinie finden Sie unter Hinzufügen von Richtlinien zu einer API-Bereitstellung.

Erstellen und Verwenden von benutzerdefinierten StyleBooks

April 28, 2021

Sie können ein eigenes StyleBook für Ihre Bereitstellung schreiben, es in Citrix Application Delivery Management (ADM) importieren und Konfigurationsobjekte erstellen. Sie können auch API verwenden, um Konfigurationen aus Ihren StyleBooks zu erstellen.

Dieses Dokument enthält die folgenden Informationen:

Voraussetzungen

Bevor Sie mit der Erstellung von StyleBooks beginnen, stellen Sie sicher, dass Sie Folgendes kennen:

- NITRO API. Weitere Informationen finden Sie unter NITRO-API-Dokumentation.
- YAML

StyleBook-Dateien verwenden das YAML-Format. Hinweise zum YAML-Format finden Sie unterYAML-Syntax.

Im Folgenden finden Sie eine Liste der YAML-Richtlinien, die Sie beim Erstellen von StyleBooks beachten müssen:

- YAML unterscheidet Groß- und Kleinschreibung.
- YAML erfordert korrekte Einrückung
- Verwenden Sie die<spacebar> Taste, um eine korrekte Einrückung zu erstellen. Verwenden Sie keinen<tab> Schlüssel. Die Verwendung von<tab> Schlüssel erzeugt Kompilierungsfehler beim Importieren Ihres StyleBook in MA Service.
- Verwenden Sie keine Zeichenfolgen in Anführungszeichen. Fügen Sie die Zeichenfolge nur in Anführungszeichen ein, wenn eine Zeichenfolge Satzzeichen (Bindestriche, Doppelpunkte usw.) enthält. Wenn Sie eine Zahl als String interpretieren möchten, fügen Sie entweder die Zahl in Anführungszeichen ein oder verwenden Sie die str() integrierte Funktion von StyleBooks.
- Literals like YES/Yes/yes/Y/y/NO/no/No/n/N, ON/On/on/OFF/Off/off, and TRUE/true/truthy/-FALSE/False/false/falsely are considered Booleans, and are equivalent to true and false respectively. Um sie als Zeichenfolgen zu interpretieren, schließen Sie sie in Anführungszeichen ein. Beispiel:
  - JA
  - Nein
  - Richtig
  - Falsch und so weiter.

> **Hinweis**
>
> Bevor Sie Ihre StyleBook-Datei in Citrix ADM importieren, sollten Sie überprüfen, ob Ihre Datei mit dem YAML-Format kompatibel ist. Citrix empfiehlt, den integrierten YAML-Validator in StyleBooks zu verwenden, um den YAML-Inhalt zu validieren und zu importieren.
>
> Bei der Konfiguration von StyleBooks können Sie nur NITRO-Konfigurationsressourcen verwenden, die die **Erstellen-** und **Löschvorgänge** (HTTP-Methoden POST und DELETE) unterstützen. Weitere Informationen finden Sie unter NITRO-APIs Dokumentation.

Anatomie eines StyleBook

Das Schreiben von StyleBooks erfordert, dass Sie die Grammatik, Syntax und Struktur von StyleBooks verstehen. Ein typisches StyleBook hat folgende Abschnitte:

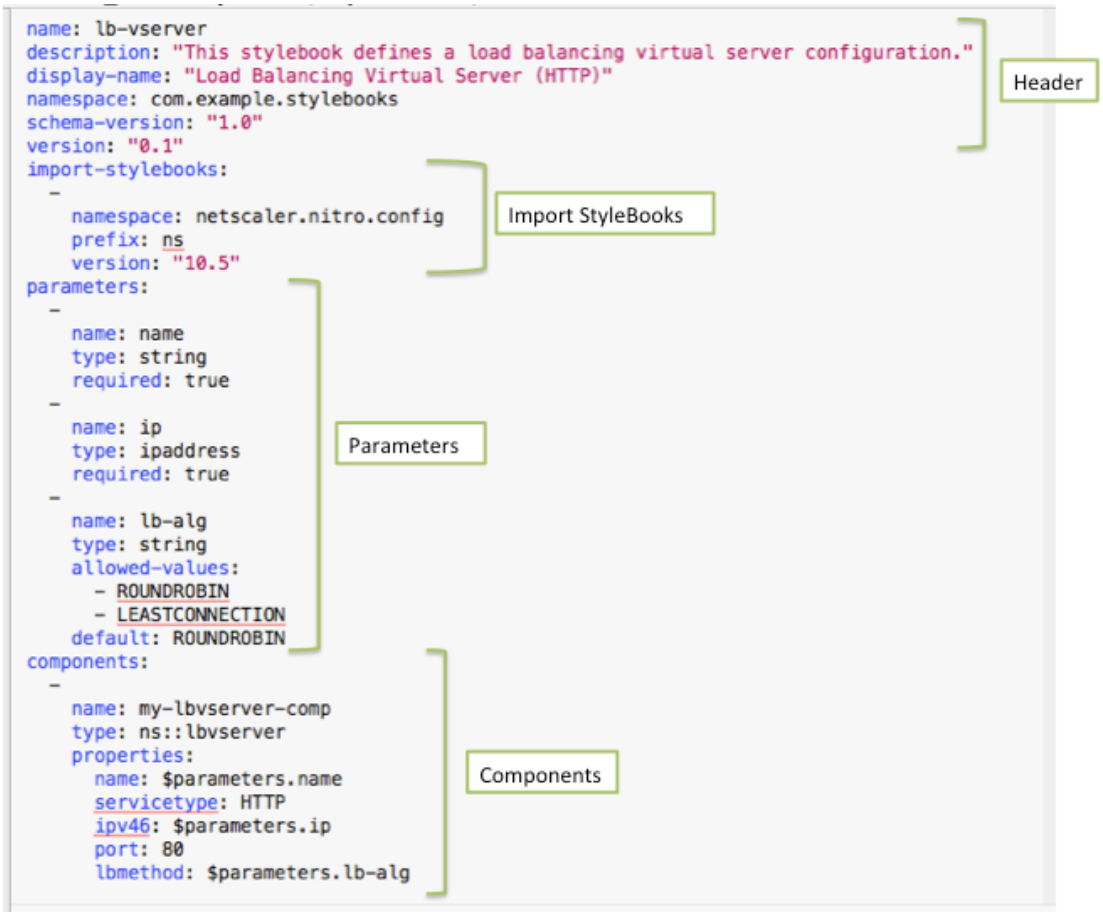
- **Header**: In diesem Abschnitt können Sie die Identität eines StyleBook definieren und beschreiben, was es tut. Dies ist ein obligatorischer Abschnitt.
- **StyleBooks importieren**: In diesem Abschnitt können Sie festlegen, auf welches andere StyleBook Sie aus Ihrem aktuellen StyleBook verweisen möchten. Das Importieren von Citrix ADC NITRO-Konfigurationsstylebooks oder anderen StyleBooks ist erforderlich, um ein StyleBook zu schreiben. Dies ist ein obligatorischer Abschnitt.
- **Parameter**: In diesem Abschnitt können Sie die Parameter definieren, die Sie in Ihrem StyleBook benötigen, um eine Konfiguration zu erstellen. Es beschreibt die Eingabe, die Ihr StyleBook nimmt. Dies ist ein optionaler Abschnitt.
- **Komponenten**: In diesem Abschnitt können Sie die Entitäten (Konfigurationsobjekte) definieren, die vom StyleBook für eine bestimmte Konfiguration erstellt werden. Dieser Abschnitt wird als Kern eines StyleBook betrachtet. Komponenten verwenden in der Regel die Eingabe im Parameterbereich zur Anpassung der vom StyleBook generierten Konfiguration. Dies ist ein optionaler Abschnitt.

  Ein StyleBook kann über einen Parameterabschnitt oder einen Komponentenabschnitt oder beides verfügen. Ein StyleBook mit nur dem Parameterbereich ist nützlich, um eine Liste von Parametern zu definieren, die von anderen StyleBooks verwendet werden können. Dies fördert die Wiederverwendbarkeit von Parametergruppen in einer Reihe von StyleBooks. Ein StyleBook mit nur einem Komponentenabschnitt kann verwendet werden, wenn Sie die Werte für Attribute im StyleBook angeben möchten, anstatt Parameter für Benutzereingaben zu definieren.
- **Ausgaben**: Während der Parameter-Abschnitt die Eingaben des StyleBook definiert, definiert dieser optionale Abschnitt seine Ausgaben. In diesem optionalen Ausgabenabschnitt können Sie die Komponenten angeben, die Benutzern zur Verfügung gestellt werden sollen, die eine Konfiguration aus diesem StyleBook erstellen, und anderen StyleBooks, die dieses StyleBook importieren. Benutzer und das Importieren von StyleBooks können dann auf die Eigenschaften

der exponierten Komponenten verweisen.

- **Vorgänge**: Ein StyleBook kann einen optionalen Abschnitt enthalten, um Analytics in Citrix ADM auf jedem virtuellen Server zu aktivieren, der Teil des StyleBook ist.

Die folgende Abbildung zeigt einen einfachen Überblick über ein StyleBook.



Die folgenden Beispiele helfen Ihnen, die Grammatik und Struktur eines StyleBook zu kennenlernen und StyleBooks mit zunehmender Komplexität zu schreiben.

- StyleBook zum Erstellen eines virtuellen Lastausgleichsservers
- StyleBook, um eine grundlegende Lastausgleichskonfiguration zu erstellen
- Erstellen eines zusammengesetzten StyleBook
- Passen Sie Ihr StyleBook mithilfe von GUI-Attributen an

StyleBook zum Erstellen eines virtuellen Lastausgleichsservers

April 28, 2021

In diesem Beispiel entwerfen Sie ein grundlegendes StyleBook, das einen virtuellen Lastausgle-

ichsserver vom HTTP-Protokolltyp erstellt und Port 80 überwacht. Die Parameter des virtuellen Servers, der IP-Adresse und der Lastausgleichsmethode akzeptieren benutzerdefinierte Werte, d. h. sie sind die Parameter des StyleBook.

Überschrift

Die ersten sechs Zeilen eines StyleBook bilden den Kopfbereich. In diesem Beispiel wird der Kopfzeilenabschnitt wie folgt geschrieben:

```
name: lb-vserver
namespace: com.example.stylebook
version: ”1.0”
display-name: Load Balancing Virtual Server (HTTP)
description: ”This stylebook defines a very simple load balancing HTTP
   virtual server configuration”
schema-version: ”1.0”
<!--NeedCopy-->
```

Der Kopfzeilenabschnitt enthält folgende Details:

- **name**: Ein Name für dieses StyleBook.
- **description**: Eine Beschreibung, die definiert, was dieses StyleBook tut. Diese Beschreibung wird in Citrix Application Delivery Management (ADM) angezeigt.
- **display-name**: Ein beschreibender Name für das StyleBook, das in Citrix ADM angezeigt wird.
- **namespace**: Ein Namespace ist Teil eines eindeutigen Bezeichners für ein StyleBook, um Namenskollisionen zu vermeiden.
- **schema-version**: Nimmt immer den Wert “1.0” in dieser Version.
- **version**: Die Versionsnummer des StyleBook. Sie können die Versionsnummer ändern, wenn Sie das StyleBook aktualisieren.

Die Kombination von **Name**, **Namespace**und **Version** identifiziert ein StyleBook im System eindeutig. Sie können nicht zwei StyleBooks mit derselben Kombination aus Name, Namespace und Version in Citrix ADM verwenden. Sie können jedoch zwei StyleBooks mit demselben Namen und derselben Version, aber unterschiedlichen Namespaces oder mit demselben Namespace und derselben Version, aber unterschiedlichen Namen haben.

> **Hinweis**
>
> Denken Sie daran, dass Sie Ihr StyleBook aktualisiert haben und eine aktualisierte Versionsnummer haben. Wenn Sie nun auf dieses StyleBook in anderen StyleBooks verweisen (dh wenn Sie importieren), stellen Sie sicher, dass Sie die Versionsnummer auch in anderen StyleBooks aktualisieren, damit sie die richtige Version des importierten StyleBook verwenden.

Importieren von Formatvorlagen

Der Abschnitt nach dem Header heißt import-stylebooks. In diesem Abschnitt müssen Sie den Namespace und die Versionsnummer jedes anderen StyleBook deklarieren, auf das Sie in Ihrem aktuellen StyleBook verweisen möchten. Auf diese Weise können Sie andere StyleBooks importieren und wiederverwenden, anstatt dieselbe Konfiguration in Ihrem eigenen StyleBook neu zu erstellen.

In diesem Beispiel wird der Abschnitt Import-StyleBooks wie folgt geschrieben:

```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: ”10.5”
<!--NeedCopy-->
```

Jedes StyleBook muss auf den Namespace netscaler.nitro.config verweisen, wenn es eines der NITRO-Konfigurationsobjekte direkt verwendet. Dieser Namespace enthält alle Citrix ADC NITRO -Typen, z. B. LBVServer.Da Softwareversionen 10.5 und höher unterstützt werden, können Sie mit Ihrem StyleBook Konfigurationen auf jeder Citrix ADC-Instanz erstellen und ausführen, auf der Version 10.5 und höher ausgeführt wird.

Das Präfix, das im Abschnitt Import-StyleBooks verwendet wird, ist eine Abkürzung, um auf die Kombination von Namespace und Version zu verweisen. In diesem Fall bezieht sich ns auf netscaler.nitro.config der Version 10.5. In den späteren Abschnitten Ihres StyleBook können Sie anstelle von Namespace und Version auf das importierte StyleBook die im obigen Beispiel gewählte Präfixzeichenfolge verwenden, z. B. ns.

Die in den StyleBooks verwendete Version ist die Citrix ADC NITRO Version. Ein StyleBook, das auf NITRO-Version X basiert, kann verwendet werden, um jeden Citrix ADC zu konfigurieren, der Version X oder höher ist.

> **Hinweis**
>
> Um sicherzustellen, dass Ihre StyleBooks zur Konfiguration einer beliebigen Citrix ADC-Instanz der Version 10.5 oder höher verwendet werden können, empfiehlt Citrix, den NITRO 10.5-Namespace aus Gründen der maximalen Kompatibilität zu importieren, der direkt die in NITRO integrierten StyleBooks verwendet (Namespace: netscaler.nitro.config, Version: 10.5).

Es ist wichtig, dass ein StyleBook, das andere StyleBooks importiert, auf einer NITRO-Version basieren muss, die dieselbe oder höhere Version als die von ihm importierten StyleBooks hat. Beispielsweise kann ein StyleBook, das auf NITRO Version 10.5 basiert, nicht von einem StyleBook abhängen, das auf 11.1 basiert, nicht verwenden oder es verwenden oder importieren. Ein StyleBook basierend auf

Version 11.1 kann jedoch ein StyleBook importieren, das auf einer beliebigen Version von weniger als 11.1 basiert.

Es ist auch möglich, dass ein StyleBook den NITRO-Namespace überhaupt nicht importiert. Das bedeutet, dass ein StyleBook NITRO-Komponenten nicht direkt definieren muss, sondern StyleBooks importieren kann, die NITRO-Komponenten definieren. Das StyleBook, das andere StyleBooks importiert, erhält immer die höchste NITRO-Version in der Hierarchie seiner Abhängigkeiten. Und es wird verwendet, um Citrix ADCs zu konfigurieren, die von dieser Version oder höher sind.

Parameter

Im Parameterbereich können Sie alle Parameter deklarieren, die Sie in Ihrem StyleBook benötigen. Als StyleBook-Entwickler müssen Sie entscheiden, welche Eingabe die Benutzer Ihres StyleBook angeben sollen. In diesem Beispiel haben Sie Ihr StyleBook so erstellt, dass die Benutzer den Namen des virtuellen Servers, seine IP-Adresse und die Load Balancing-Methode angeben müssen.

Der Parameterabschnitt würde wie folgt aussehen:

```
parameters:
 -
  name: name
  label: "Application Name"
  description: "Give a name to the application configuration."
  type: string
  required: true
 -
  name: vip-ipaddress
  label: "Load Balancer IP Address"
  description: "The Application VIP that clients access"
  type: ipaddress
  required: true
 -
  name: lb-alg
  label: LB Algorithm
  description: Load Balancing Algorithm
  type: string
  default: ROUNDROBIN
  allowed-values:
   - ROUNDROBIN
   - LEAST-CONNECTION
<!--NeedCopy-->
```


> **Hinweis**
>
> Wenn Sie die Bezeichnung eines Parameters nicht angeben, verwendet Citrix ADM bei der Anzeige dieses Parameters das name-Attribut. Sie müssen immer eine Bezeichnung für Ihre Parameter definieren, damit Sie steuern können, wie sie in Citrix ADM angezeigt werden.
>
> Bei Verwendung der APIs wird der Parameter jedoch durch seinen Namen gekennzeichnet.

In diesem Abschnitt haben Sie drei Parameter deklariert, die durch ihre **Name-Attributwerte** angegeben sind: **Name** für den virtuellen Servernamen, **IP** für die IP-Adresse des virtuellen Servers und **lb-alg** für die Load Balancing-Methode.

- **Typ** bezieht sich auf den Typ des Wertes, den diese Parameter annehmen können. Zum Beispiel `lb-alg` kann name und einen String-Wert annehmen, und der IP-Wert muss vom Typ IP-Adresse sein. Parameter in einem StyleBook können von einem der folgenden integrierten Typen sein:
- **string**: Ein Array von Zeichen. Wenn keine Länge angegeben wird, kann der Zeichenfolgenwert beliebig viele Zeichen annehmen. Sie können jedoch die Länge eines String-Typs einschränken, indem Sie die Attribute min-length und max-length verwenden.
- **number**: Eine ganze Zahl. Sie können die minimale und maximale Anzahl angeben, die dieser Typ annehmen kann, indem Sie die Attribute min-value und max-value verwenden.
- **boolean**: Kann entweder wahr oder falsch sein. Beachten Sie auch, dass alle Literale von YAML als Booleans betrachtet werden (zum Beispiel Ja oder Nein).
- **ipaddress**: Eine Zeichenfolge, die eine gültige IPv4- oder IPv6-Adresse darstellt.
- **tcp-port**: Eine Zahl zwischen 0 und 65535, die einen TCP- oder UDP-Port darstellt.
- **password**: Ein undurchsichtiger Zeichenfolgenwert. Wenn Citrix ADM einen Wert für diesen Parameter anzeigt, wird er als Sternchen (*****) angezeigt.
- **certfile**: Eine Zertifikatdatei.
- **keyfile**: Eine private Zertifikatsschlüsseldatei.
- **file**: Ein Parameter dieses Typs erfordert, dass der Benutzer eine Datei hochlädt, z. B. ein Zertifikat oder eine Schlüsseldatei.
- **Objekt**: Besteht aus mehreren Elementen und jedes dieser Elemente ist ein Parameter. Dieser Typ kann verwendet werden, um mehrere verwandte Parameter unter einem übergeordneten Parameter zu gruppieren.
- **required**: Gibt an, ob ein Parameter obligatorisch oder optional ist. Wenn es auf true gesetzt ist, ist der Parameter obligatorisch und der Benutzer muss einen Wert für diesen Parameter angeben, wenn Konfigurationen mit diesem StyleBook erstellt werden. Standardmäßig sind alle Parameter optional. In diesem Beispiel sind **name** und **ip** obligatorische Parameter, während **lb-alg** ein optionaler Parameter ist, dessen Standardwert ROUNDROBIN ist.

Verwenden Sie das **Standardattribut**, um einem optionalen Parameter einen Standardwert zuzuweisen. Wenn ein Benutzer beim Erstellen einer Konfiguration keinen Wert angibt, wird der Standardwert verwendet. Für den Parameter **lb-alg** ist beispielsweise der Standardwert ROUNDROBIN.

Verwenden Sie das **allowed-values** -Attribut, um bestimmte Werte zu definieren, die ein Benutzer beim Erstellen einer Konfiguration auswählen kann. In diesem Beispiel haben Sie zwei Werte für den **lb-alg-Parameter** angegeben: ROUNDROBIN und LEASTCONNECTION.

Wenn Sie Ihr StyleBook importieren und es verwenden, zeigt Citrix ADM ein Formular mit diesen drei Parametern an. Die für Name und IP angezeigten Felder ermöglichen die `ipaddress` Eingabe von Zeichenfolge und Werttyp, und das `lb-alg` Feld wird als Dropdown-Liste angezeigt, wobei ROUNDROBIN als Standardwert ausgewählt ist.

> **Hinweis**
>
> Zusätzlich zu den integrierten Typen kann ein Parameter ein anderes StyleBook als Typ haben. Dies ist eine Möglichkeit, Parameter, die in anderen StyleBooks definiert sind, wiederzuverwenden.

Komponenten

Der letzte Abschnitt in diesem StyleBook wird als Komponentenbereich bezeichnet und gilt als der wichtigste Abschnitt im StyleBook. In diesem Abschnitt definieren Sie die Konfigurationsobjekte, die vom StyleBook erstellt werden müssen.

Für dieses Beispiel müssen Sie den Komponentenabschnitt wie folgt schreiben:

```
components:
 -
  name: lbvserver-comp
  description: This StyleBook component (a Builtin Nitro StyleBook)
     builds a Citrix ADC lbvserver configuration object.
  type: ns::lbvserver
  properties:
   name: $parameters.name
   ipv46: $parameters.vip-ipaddress
   lbmethod: $parameters.lb-alg
   servicetype: HTTP
   port: 80
<!--NeedCopy-->
```

Dieses Beispiel enthält nur eine Komponente. Die wichtigsten Attribute einer Komponente sind Name, Typ und Eigenschaften. Der Typ einer Komponente bestimmt, welche Eigenschaften diese Komponente bietet. Komponenten sind von zwei Arten:

- **Eingebauter Typ**: Dieser Typ wird vom System bereitgestellt und Sie müssen ihn nicht definieren, z. B. die NITRO-Entitätstypen `lbvserver` oder `servicegroup`. In diesem Beispiel verwenden Sie einen integrierten Komponententyp.

- **Composite-Typ**: Dieser Typ ist das StyleBook, das Sie erstellt und in Citrix ADM importiert haben, oder das Standard-StyleBook, das mit Citrix ADM ausgeliefert wird. Weitere Informationen zu Composite StyleBooks finden Sie inErstellen eines zusammengesetzten StyleBook.

In diesem Beispiel haben Sie eine Komponente namens **lbvserver-comp**definiert. Diese Komponente ist vom Typ **ns lbvserver** (ein integrierter NITRO-Typ), wobei "ns" das Präfix ist, das sich auf den Namespace netscaler.nitro.config und Version 10.5 bezieht, den Sie im Abschnitt import-stylebooks angegeben haben, und eine NITRO-Ressource in diesem Namespace `lbvserver` ist.

Die hier definierten **Eigenschaften** sind die Attribute der `lbvserver` Ressource. Weitere Informationen über alle verfügbaren Citrix ADC NITRO-Ressourcen und ihre Attribute finden Sie unter Citrix ADC NITRO REST API-Dokumentation.

Die Eigenschaften in diesem Abschnitt enthalten die obligatorischen Attribute der `lbvserver` Ressource und ermöglichen es Ihnen, Werte für diese Attribute anzugeben. In diesem Beispiel geben Sie statische Werte für `servicetype` und portieren an, während der Name, ipv46 und `lbmethod` Eigenschaften ihre Werte aus den Eingabeparametern erhalten. Im Rest des StyleBook können Sie auf die Parameternamen verweisen, die im Parameterabschnitt definiert sind, indem Sie den Ausdruck **$parameters.<parameter-name>** verwenden, zum Beispiel **$parameters.ip**.

> **Hinweis**
>
> Die Konvention ist, das Präfix "ns" immer zu verwenden, um einen Citrix ADC NITRO-Namespace im Abschnitt "Import-Stylebooks" zu bezeichnen. Obwohl dies nicht obligatorisch ist, empfiehlt Citrix, die gleiche Konvention in Ihren eigenen StyleBooks zur Konsistenz zu verwenden.

Erstellen Sie Ihr StyleBook

Nachdem Sie nun alle erforderlichen Abschnitte dieses StyleBook definiert haben, bringen Sie sie alle zusammen, um Ihr erstes StyleBook zu erstellen. Kopieren Sie den StyleBook-Inhalt und fügen Sie ihn in einen Texteditor ein, und speichern Sie die Datei dann unter **lb-vserver.yaml**. Citrix empfiehlt, den integrierten YAML-Validator in StyleBooks zu verwenden, um den YAML-Inhalt zu validieren und zu importieren.

Der vollständige Inhalt der Datei lb-vserver.yaml wird unten wiedergegeben:

```
1 name: lb-vserver
2 namespace: com.example.stylebook
3 version: "1.0"
4 display-name: Load Balancing Virtual Server (HTTP)
5 description: "This stylebook defines a very simple load balancing HTTP
     virtual server configuration"
6 schema-version: "1.0"
```



```
7
8  import-stylebooks:
9   -
10   namespace: netscaler.nitro.config
11   version: ”10.5”
12   prefix: ns
13  -
14   namespace: com.citrix.adc.stylebooks
15   version: ”1.0”
16   prefix: stlb
17
18 parameters:
19  -
20   name: name
21   label: ”Application Name”
22   description: ”Give a name to the application configuration.”
23   type: string
24   required: true
25  -
26   name: vip-ipaddress
27   label: ”Load Balancer IP Address”
28   description: ”The Application VIP that clients access”
29   type: ipaddress
30   required: true
31  -
32   name: lb-alg
33   label: LB Algorithm
34   description: Load Balancing Algorithm
35   type: string
36   default: ROUNDROBIN
37   allowed-values:
38    - ROUNDROBIN
39    - LEAST-CONNECTION
40
41 components:
42  -
43   name: lbvserver-comp
44   description: This StyleBook component (a Builtin Nitro StyleBook)
        builds a Citrix ADC lbvserver configuration object.
45   type: ns::lbvserver
46   properties:
47    name: $parameters.name
48    ipv46: $parameters.vip-ipaddress
49    lbmethod: $parameters.lb-alg
50    servicetype: HTTP
```



```
    port: 80
<!--NeedCopy-->
```

Um mit dem StyleBook Konfigurationen zu erstellen, müssen Sie es in Citrix ADM importieren und es dann verwenden. Weitere Informationen finden Sie unter So verwenden Sie benutzerdefinierte StyleBooks.

Sie können dieses StyleBook auch in andere StyleBooks importieren (mit dem Import-StyleBooks-Konstrukt). Oder Sie können dieses StyleBook so ändern, dass es weitere Parameter und Komponenten enthält, wie im nächsten Abschnitt beschrieben.

StyleBook, um eine grundlegende Lastausgleichskonfiguration zu erstellen

April 28, 2021

Im vorherigen Beispiel haben Sie ein grundlegendes StyleBook erstellt, um einen virtuellen Lastausgleichsserver zu erstellen. Sie können dieses StyleBook unter einem anderen Namen speichern und es dann aktualisieren, um zusätzliche Parameter und Komponenten für eine grundlegende Lastausgleichskonfiguration aufzunehmen. Speichern Sie diese StyleBook-Datei als **basic-lb-config.yaml**.

In diesem Abschnitt entwerfen Sie ein neues StyleBook, das eine Lastausgleichskonfiguration erstellt, die aus dem virtuellen Lastausgleichsserver, einer Servicegruppe und einer Liste von Diensten besteht. Außerdem werden die Dienste an die Dienstgruppe gebunden und die Dienstgruppe an den virtuellen Server gebunden.

Überschrift

Um dieses StyleBook zu erstellen, müssen Sie mit der Aktualisierung des Kopfzeilenabschnitts beginnen. Dieser Abschnitt ähnelt dem, den Sie für den Lastenausgleich des virtuellen Servers StyleBook erstellt haben. Ändern Sie im Headerbereich den Wert von **name** in basic-lb-config. Aktualisieren Sie außerdem die **Beschreibung** und den **Anzeigenamen**, um dieses StyleBook entsprechend zu beschreiben. Sie müssen die **Namespace-** und **Versionswerte** nicht ändern. Da Sie den Namen geändert haben, erstellt die Kombination aus Name, Namespace und Version einen eindeutigen Bezeichner für dieses StyleBook im System.

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
```



```
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"
<!--NeedCopy-->
```

Importieren von StyleBooks

Der Abschnitt Import-StyleBooks bleibt unverändert. Es bezieht sich auf den Namespace netscaler.nitro.config, um die NITRO-Konfigurationsobjekte zu verwenden.

```
import-stylebooks:
 -
 namespace: netscaler.nitro.config
 prefix: ns
 version: "10.5"
<!--NeedCopy-->
```

Parameter

Sie müssen den Parameterbereich aktualisieren, um zwei zusätzliche Parameter hinzuzufügen, um die Liste der Dienste oder Server und den Port zu definieren, auf dem die Dienste hören. Die ersten drei Parameter `nameip`, und `lb-alg` bleiben gleich.

```
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
  type: string
```



```
17    label: LoadBalancing Algorithm
18    description: Choose the loadbalancing algorithm (method) used for
          loadbalancing client requests between the application servers.
19    allowed-values:
20       - ROUNDROBIN
21       - LEASTCONNECTION
22    default: ROUNDROBIN
23   -
24    name: svc-servers
25    type: ipaddress[]
26    label: Application Server IPs
27    description: The IP addresses of all the servers of this application
28    required: true
29   -
30    name: svc-port
31    type: tcp-port
32    label: Server Port
33    description: The TCP port open on the application servers to receive
          requests.
34    default: 80
35  <!--NeedCopy-->
```

In diesem Beispiel wird der Parameter **svc-Servers** hinzugefügt, um eine Liste von IP-Adressen der Dienste zu akzeptieren, die die Backend-Server der Anwendung darstellen. Dies ist ein obligatorischer Parameter, wie angegeben durch **required: true**. Der zweite Parameter, **svc-port**, gibt die Portnummer an, auf die die Server lauschen. Die Standardportnummer ist 80 für `svc-port` Parameter, wenn sie nicht vom Benutzer angegeben wird.

Komponenten

Sie müssen auch den Komponentenabschnitt aktualisieren, um zusätzliche Komponenten so zu definieren, dass sie die beiden neuen Parameter verwenden und die komplette Lastausgleichskonfiguration erstellen.

Für dieses Beispiel müssen Sie den Komponentenabschnitt wie folgt schreiben:

```
1  components:
2   -
3    name: lbvserver-comp
4    type: ns::lbvserver
5    properties:
6     name: $parameters.name + "-lb"
7     servicetype: HTTP
```



```
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg

components:
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
   name: $parameters.name + "-svcgrp"
   servicetype: HTTP

components:
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $parent.parent.properties.name
   servicegroupname: $parent.properties.name
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

In diesem Beispiel enthält die ursprüngliche Komponente **lbvserver-comp** (aus dem vorherigen Beispiel) jetzt eine untergeordnete Komponente namens **svcg-comp**. Und die **svcg-comp-Komponente** enthält zwei untergeordnete Komponenten. Durch das Verschachteln einer Komponente in einer anderen Komponente kann die verschachtelte Komponente Konfigurationsobjekte erstellen, indem sie auf Attribute in der übergeordneten Komponente verweist. Die verschachtelte Komponente kann für jedes Objekt, das in der übergeordneten Komponente erstellt wurde, ein oder mehrere Objekte erstellen.

Die Komponente **svcg-comp** wird verwendet, um eine Dienstgruppe auf der Citrix ADC-Instanz zu erstellen, indem die für die Attribute der Ressource angegebenen Werte verwendet werden `servicegroup`. In diesem Beispiel geben Sie einen statischen Wert für an `servicetype`, während name seinen Wert aus dem Eingabeparameter erhält. Sie verweisen auf den **Parameternamen**, der im **Parameterabschnitt definiert ist, indem Sie $parameters.name + -svcgrp** -Notation verwenden, wobei "**-svcgrp** " an den benutzerdefinierten Namen angehängt (verkettet) wird.

Die Komponente **svcg-comp** hat zwei untergeordnete Komponenten, **lbvserver-svg-binding-comp** und **members-svcg-comp**.

Die erste untergeordnete Komponente, **lbvserver-svg-binding-comp**, wird verwendet, um ein Konfigurationsobjekt zwischen der von ihrer übergeordneten Komponente erstellten Servicegruppe und dem virtuellen Lastausgleichsserver (`lbvserver`) zu binden, der von der übergeordneten Komponente des Elternteils erstellt wurde. Die $parent Notation, auch übergeordnete Referenz genannt, wird verwendet, um auf Entitäten in den übergeordneten Komponenten zu verweisen. Beispiel: **servicegroupname: $parent.properties.name** bezieht sich auf die Dienstgruppe, die von der übergeordneten Komponente **svcg-comp** erstellt wurde, und **name: $parent.parent.properties.name** bezieht sich auf den virtuellen Server, der von der übergeordneten Komponente **lbvserver erstellt wurde. - Komp**.

Die **members-svcg-Komponente** wird verwendet, um Konfigurationsobjekte zwischen der Liste der Dienste an die von der übergeordneten Komponente erstellte Dienstgruppe zu binden. Die Erstellung mehrerer Bindungskonfigurationsobjekte wird erreicht, indem das **repeat**-Konstrukt von StyleBook verwendet wird, um über die Liste der Server zu iterieren, die im Parameter **svc-Server** angegeben ist. Während der Iteration erstellt diese StyleBook-Komponente ein NITRO-Konfigurationsobjekt vom Typ **servicegroup_servicegroupmember_binding** für jeden Dienst (wie `srv` im **repeat-Item-Konstrukt** bezeichnet) in der Servicegruppe und legt das **ip-Attribut** in jeder NITRO-Konfigurationsobjekt der IP-Adresse des entsprechenden Servers.

Im Allgemeinen können Sie die Repeat- und Repeat-Item-Konstrukte**in einer Komponente verwenden, um diese Komponente mehrere Konfigurationsobjekte desselben Typs zu erstellen.** Sie können dem **Repeat-Item-Konstrukt** einen Variablennamen zuweisen `srv`, um beispielsweise den aktuellen Wert in der Iteration zu bestimmen. Dieser Variablenname wird in den Eigenschaften derselben Komponente oder in untergeordneten Komponenten wie **$<varname>**, z. B. $srv bezeichnet.

Im obigen Beispiel haben Sie Verschachtelung von Komponenten ineinander verwendet, um diese Konfiguration einfach zu konstruieren. In diesem speziellen Fall war die Verschachtelung von Komponenten nicht die einzige Möglichkeit, die Konfiguration zu erstellen. Sie können das gleiche Ergebnis ohne Verschachtelung erzielen, wie unten gezeigt:

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + ”-lb”
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
```



```
    lbmethod: $parameters.lb-alg
  -
   name: svcg-comp
   type: ns::servicegroup
   properties:
     servicegroupname: $parameters.name + "-svcgrp"
     servicetype: HTTP
  -
   name: lbvserver-svg-binding-comp
   type: ns::lbvserver_servicegroup_binding
   properties:
    name: $components.lbvserver-comp.properties.name
    servicegroupname: $components.svcg-comp.properties.servicegroupname
  -
   name: members-svcg-comp
   type: ns::servicegroup_servicegroupmember_binding
   repeat: $parameters.svc-servers
   repeat-item: srv
   properties:
    ip: $srv
    port: 80
    servicegroupname: $components.svcg-comp.properties.servicegroupname
<!--NeedCopy-->
```

Hier befinden sich alle Komponenten auf der gleichen Ebene (d. h. sie sind nicht verschachtelt), aber das erzielte Ergebnis (die generierte Citrix ADC Konfiguration) entspricht dem der zuvor verwendeten verschachtelten Komponenten. Auch die Reihenfolge, in der die Komponenten im StyleBook deklariert werden, wirkt sich nicht auf die Reihenfolge der Erstellung der Konfigurationsobjekte aus. In diesem Beispiel müssen die Komponenten **svcg-comp** und **lbvserver-comp**, obwohl zuletzt deklariert, vor dem Erstellen der zweiten Komponente **lbvserver-svg-binding-comp** erstellt werden, da in der zweiten Komponente Vorwärtsreferenzen auf diese Komponenten vorhanden sind.

> **Hinweis**
>
> Nach der Konvention sind die Namen von StyleBooks, Parametern, Substitutionen, Komponenten und Ausgaben in Kleinbuchstaben. Wenn sie mehrere Wörter enthalten, werden sie durch ein - -Zeichen getrennt. Zum Beispiel `lb-bindingsapp-namerewrite-config`, und so weiter. Eine andere Konvention besteht darin, Komponentennamen mit einer `-comp` Zeichenfolge zu suffi

Ausgaben

Der letzte Abschnitt, den Sie dem neuen StyleBook hinzufügen können, ist der Ausgabebereich, in dem Sie angeben, was dieses StyleBook seinen Benutzern (oder in anderen StyleBooks) zur Verfügung

stellt, nachdem es zum Erstellen einer Konfiguration verwendet wird. Sie können beispielsweise im Abschnitt Ausgaben angeben, um die Konfigurationsobjekte `lbvserver` und die von diesem StyleBook erstellten `servicegroup` Konfigurationsobjekte verfügbar zu machen.

```
outputs:
-
  name: lbvserver-comp
  value: $components.lbvserver-comp
  description: The component that builds the Nitro lbvserver
     configuration object
-
  name: servicegroup-comp
  value: $components.svcg-comp
  description: The component that builds the Nitro servicegroup
     configuration object
<!--NeedCopy-->
```

Der Ausgabebereich eines StyleBook ist optional. Ein StyleBook muss keine Ausgaben zurückgeben. Durch die Rückgabe einiger interner Komponenten als Ausgaben ermöglicht es jedoch allen StyleBooks, die dieses StyleBook importieren, mehr Flexibilität, wie Sie beim Erstellen eines zusammengesetzten StyleBook sehen können.

> **Hinweis**
>
> Es empfiehlt sich, eine ganze Komponente des StyleBook im Ausgaben-Abschnitt verfügbar zu machen, anstatt nur eine einzelne Eigenschaft einer Komponente (z. B. die gesamte $components.lbvserver-comp und nicht nur den Namen $components.lbvserver-comp.properties.name). Fügen Sie der Ausgabe auch eine Beschreibung hinzu, die erklärt, was die spezifische Ausgabe darstellt.

Erstellen Sie Ihr StyleBook

Nachdem Sie nun alle erforderlichen Abschnitte dieses StyleBook definiert haben, bringen Sie sie alle zusammen, um Ihr zweites StyleBook zu erstellen. Sie haben diese StyleBook-Datei bereits als **basic-lb-config.yaml**gespeichert. Citrix empfiehlt, den integrierten YAML-Validator in StyleBooks zu verwenden, um den YAML-Inhalt zu validieren und zu importieren.

Der vollständige Inhalt der Datei **basic-lb-config.yaml** wird nachfolgend wiedergegeben:

```
name: basic-lb-config
namespace: com.example.stylebooks
```



```
version: "0.1"
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the loadbalancing algorithm (method) used for
     loadbalancing client requests between the application servers.
  allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: svc-servers
  type: ipaddress[]
  label: Application Server IPs
  description: The IP addresses of all the servers of this application
  required: true
 -
  name: svc-port
  type: tcp-port
  label: Server Port
  description: The TCP port open on the application servers to receive
```



```
        requests.
    default: 80

components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
    servicegroupname: $parameters.name + "-svcgrp"
    servicetype: HTTP
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $components.lbvserver-comp.properties.name
   servicegroupname: $components.svcg-comp.properties.servicegroupname
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: 80
   servicegroupname: $components.svcg-comp.properties.servicegroupname

outputs:
-
  name: lbvserver-comp
  value: $components.lbvserver-comp
  description: The component that builds the Nitro lbvserver
      configuration object
-
  name: servicegroup-comp
  value: $components.svcg-comp
  description: The component that builds the Nitro servicegroup
```



```
        configuration object
<!--NeedCopy-->
```

Um mit dem StyleBook Konfigurationen zu erstellen, müssen Sie es in Citrix ADM importieren und es dann verwenden. Weitere Informationen finden Sie unter So verwenden Sie benutzerdefinierte StyleBooks.

Sie können dieses StyleBook auch in andere StyleBooks importieren und seine Eigenschaften wie im nächsten Abschnitt beschrieben verwenden.

Erstellen eines zusammengesetzten StyleBook

April 28, 2021

Eine wichtige und leistungsstarke Funktion von StyleBooks ist, dass sie als Bausteine für andere StyleBooks verwendet werden können. Ein StyleBook kann in ein anderes StyleBook importiert werden und kann als ein **Typ** bezeichnet werden, der von Komponenten des zweiten StyleBook ähnlich einem in NITRO integrierten StyleBook verwendet wird.

Beispielsweise können Sie das **Basic-lb-config** StyleBook verwenden, das Sie im vorherigen Abschnitt erstellt haben, um ein anderes StyleBook namens **composite-example** zu erstellen. Um das StyleBook basic-lb-config zu verwenden, müssen Sie es in das neue StyleBook im Import-StyleBook-Sektion importieren.

Erstellen Sie Ihr StyleBook

Das neue StyleBook würde wie folgt aussehen:

```
name: composite-example
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
description: This StyleBook defines a RoundRobin load balancing
   configuration with a monitor.
schema-version: "1.0"
import-stylebooks:
  -
   namespace: netscaler.nitro.config
   version: "10.5"
   prefix: ns
  -
```



```
    namespace: com.example.stylebooks
    version: ”0.1”
    prefix: stlb
parameters:
  -
    name: name
    type: string
    label: Application Name
    description: Give a name to the application configuration.
    required: true
  -
    name: ip
    type: ipaddress
    label: Application Virtual IP (VIP)
    description: The Application VIP that clients access
    required: true
  -
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this
       application
    required: true

  -
    name: response-code
    type: string[]
    label: List of Response Codes
    description: List of Response Codes - Provide a list of response
       codes in integer.

components:
  -
    name: basic-lb-comp
    type: stlb::basic-lb-config
    description: This component's type is another StyleBook that builds
        the NetScaler lbvserver, servicegroups and services
       configuration objects.
    properties:
     name: $parameters.name
     ip: $parameters.ip
     svc-servers: $parameters.svc-servers
  -
     name: monit-comp
     type: ns::lbmonitor
```



```
54      description: This component is a basic Nitro type (a Builtin
           StyleBook) that builds the NetScaler monitor configuration
           object.
55      properties:
56        monitorname: $parameters.name + "-mon"
57        type: HTTP
58        respcode: $parameters.response-code
59        httprequest: "'GET /'"
60        lrtm: ENABLED
61        secure: "YES"
62
63      components:
64         -
65           name: monit-svcgrp-bind-comp
66           type: ns::servicegroup_lbmonitor_binding
67           properties:
68             servicegroupname: $components.basic-lb-comp.outputs.
                  servicegroup-comp.properties.servicegroupname
69             monitor_name: $parent.properties.monitorname
70  <!--NeedCopy-->
```

Im Abschnitt import-stylebooks importieren Sie das basic-lb-config StyleBook mithilfe seines Namespace und seiner Version, auf die mit dem Präfix verwiesen wird `stlb`.

Im Komponentenabschnitt werden zwei Komponenten definiert. Die erste Komponente ist vom Typ **stlb:: basic-lb-config**, wobei basic-lb-config der Name des StyleBook ist, in dem Sie erstellt habenStyleBook, um eine grundlegende Lastausgleichskonfiguration zu erstellen. Die für diese Komponente definierten Eigenschaften entsprechen den obligatorischen Parametern, die im Basic-lb-config StyleBook deklariert sind. Sie können jedoch jeden Parameter des StyleBook verwenden (sowohl erforderlich als auch optional). Anstatt a `lbvserver`, eine Dienstgruppe sowie Service- und Servicegruppenbindungen neu aufzubauen, importieren Sie das StyleBook, das dies alles als Komponente tut, und verwenden es, um diese Konfigurationsobjekte im neuen StyleBook zu erstellen.

StyleBook fügt eine zweite Komponente hinzu `monit-comp`, die die Attribute der NITRO-Ressource `lbmonitor` (ein integriertes StyleBook) verwendet, um ein Monitor-Konfigurationsobjekt zu erstellen. Es verfügt auch über eine Unterkomponente `monit-svcgrp-bind-comp` zum Erstellen des Bindungskonfigurationsobjekts, das den Monitor an die in der ersten Komponente `servicegroup` erstellte Bindung. Da die im StyleBook "basic-lb-config" erstellte `servicegroup` Komponente als Ausgabe verfügbar gemacht wird, kann dieses StyleBook mit dem Ausdruck **$components.basic-lb-comp.outputs.servicegroup-comp**darauf zugreifen. Dies ist ein Beispiel dafür, wie der Ausgabeabschnitt vom importierenden StyleBooks verwendet werden kann, um Zugriff auf Komponenten in den importierten StyleBooks zu haben, auf die sie sonst nicht zugreifen können.

Kopieren Sie anschließend den StyleBook-Inhalt und fügen Sie ihn in einen Texteditor ein, und speichern Sie die Datei als **composite-example.yaml**. Überprüfen Sie den YAML-Inhalt, bevor Sie die Datei in Citrix ADM importieren. Importieren Sie es dann in Citrix ADM und erstellen Sie eine oder mehrere Konfigurationen mithilfe dieses StyleBook.

Citrix empfiehlt, den integrierten YAML-Validator in StyleBooks zu verwenden, um den YAML-Inhalt zu validieren und zu importieren.

Verwenden von GUI-Attributen in einem benutzerdefinierten StyleBook

April 28, 2021

Sie können GUI-Attribute im Parameterabschnitt Ihres StyleBook hinzufügen, um die Felder intuitiv zu gestalten, wenn sie in Citrix Application Delivery Management (ADM) angezeigt werden.

Beispiel: Sie können einen beschreibenden Namen für den Parameter mithilfe des label-Attributs hinzufügen und eine QuickInfo für diesen Parameter mithilfe des description -Attributs hinzufügen.

```
name: ip
label: Virtual Server IP Address
description: IP address of the virtual server that represents the load
   balanced application.
type: ipaddress
required: true
<!--NeedCopy-->
```

Beispiel: Wenn Sie einen Parameter vom Typ Objekt haben, können Sie das Layout mithilfe des **GUI-Attributs**definieren. In diesem Beispiel ist das Layout ein reduzierbares Objekt, in dem Felder in zwei Spalten angezeigt werden.

```
name: svcg-advanced
label: Advanced Application Server Settings
type: object
required: false
gui:
 collapse_pane: true
 columns: 2
<!--NeedCopy-->
```


Beispiel. Sie können auch eine Zusammenfassungsansicht eines Parameters vom Typ Objekt[] (Liste von Objekten) als Tabelle mit den inneren Parametern anzeigen, die die Spalten darstellen. Um einen inneren Parameter aus der Zusammenfassungsansicht einzuschließen oder auszuschließen, können Sie das `summary_display` Attribut im `gui` Abschnitt wie folgt verwenden:

```
name: settings
label: Settings
type: object[]
parameters:
  -
    name: name
    label: Name
    description: Name of this setting
    type: string
    gui:
      summary_display: true
<!--NeedCopy-->
```

Beispiel: Einige StyleBooks auf Citrix ADM werden nur als Bausteine für andere StyleBooks verwendet. Und Sie möchten möglicherweise nicht, dass Benutzer Konfigurationen direkt aus diesen StyleBooks erstellen. Weil diese StyleBooks als Teil anderer StyleBooks verwendet werden sollen. Markieren Sie das StyleBook als privat, um sicherzustellen, dass das StyleBook nicht direkt zum Erstellen von Konfigurationen in der Citrix ADM GUI verwendet wird.

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"
<!--NeedCopy-->
```

Importieren von benutzerdefinierten StyleBooks

April 28, 2021

Nachdem Sie Ihr StyleBook erstellt haben, müssen Sie es in Citrix Application Delivery Management (ADM) importieren, um es zu verwenden. Mit Citrix ADM können Sie ein einzelnes StyleBook in YAML-

Form oder mehrere StyleBook-YAML-Dateien als Bundle in einem Zip-, TGZ- oder GZ-Formular importieren. Das Citrix ADM -System validiert Ihre StyleBooks beim Import. Das StyleBook kann nun zum Erstellen von Konfigurationen verwendet werden.

Citrix ADM verfügt auch über einen integrierten YAML-Editor, mit dem Sie die StyleBook YAML-Inhalte erstellen können. Der YAML-Editor ermöglicht es Ihnen, Ihre YAML-Konstrukte über die Citrix ADM GUI selbst zu validieren. Sie müssen kein separates Tool für diese Validierungsprüfungen verwenden. Der Inhalt wird nach YAML-Standards validiert und jede Abweichung wird hervorgehoben. Anschließend können Sie den Inhalt korrigieren und versuchen, das StyleBook in Citrix ADM zu importieren. Der integrierte YAML-Editor bietet zwei Vorteile beim Schreiben Ihres eigenen StyleBook.

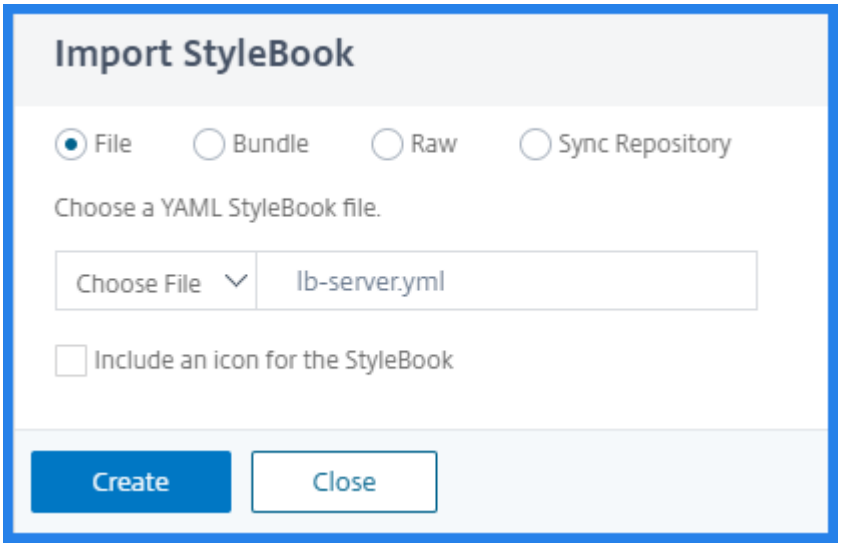
- **Farbcodiert**. Der Editor zeigt den nach YAML-Richtlinien analysierten StyleBook-Inhalt an, und die Farbcodierung hilft Ihnen, einfach zwischen den Schlüsseln und den im YAML-Inhalt definierten Werten zu unterscheiden.
- **YAML-Validierung**. Der Inhalt wird bei der Eingabe auf YAML-Fehler überprüft und jede Abweichung wird sofort hervorgehoben. Mit dieser Validierung können Sie Text schreiben, der den YAML-Richtlinien entspricht, noch bevor Sie das StyleBook in Citrix ADM importieren.

> **Hinweis**
>
> Aktuell überprüft der Editor den Inhalt gemäß den YAML-Richtlinien. Es validiert nicht auf Code Korrektheit und typografische Fehler.

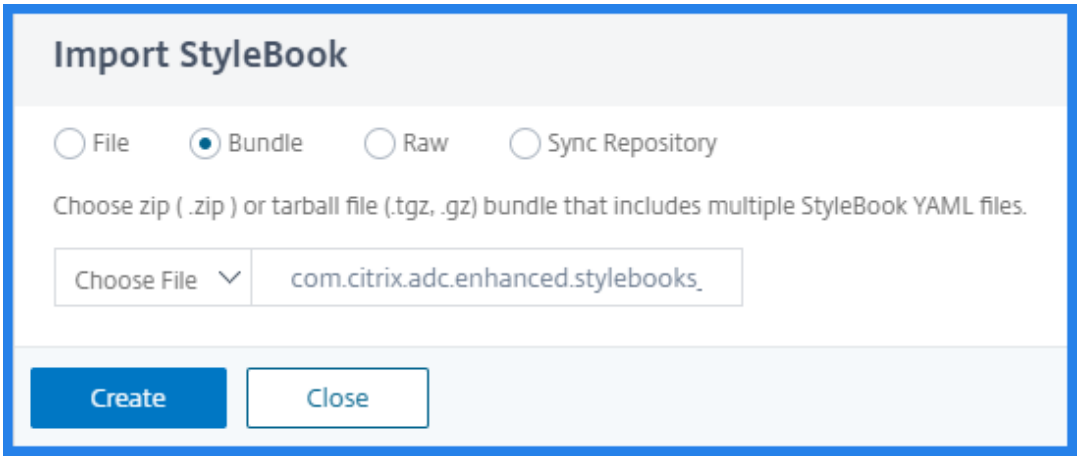
So importieren Sie Ihr StyleBook

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfiguration** > **StyleBooks**, und klicken Sie dann auf **Neues StyleBook importieren**.
2. Klicken Sie auf eine der folgenden Optionen, um ein StyleBook zu importieren.
    - **Datei** - Wählen Sie die gewünschte Datei oder das Bündel von Dateien aus Ihrem lokalen Speicher aus.

      > **Hinweis: Importieren Sie**
      >
      > in diesem Beispiel das `lb-vserver.yml`StyleBook, das Sie in erstellt haben StyleBook zum Erstellen eines virtuellen Load Balancing Servers.



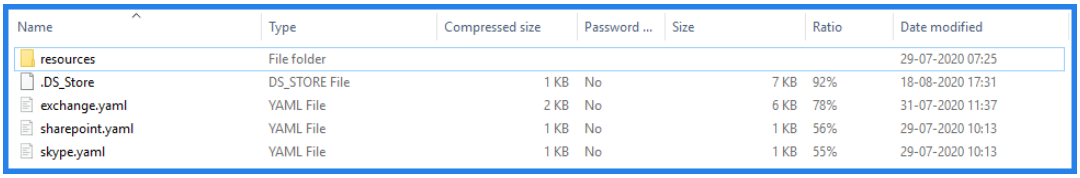
- **Bundle** - Mit Citrix ADM können Sie mehrere StyleBooks im YAML-Format importieren. Sie können mehrere YAML StyleBook-Dateien importieren, die im ZIP-Format (.zip) oder Tarball-Format (.tgz, .gz) komprimiert sind.



Sie können jetzt jedem StyleBook im Bundle Symbole hinzufügen. Laden Sie dazu die Icons und die `icon_mapping.json` Datei in den `resources` Ordner hoch. Wenn der Name der Symboldatei und der Name des StyleBook übereinstimmen, werden die Symbole automatisch den StyleBooks zugeordnet. Andernfalls ordnen Sie StyleBooks und Symbole in der `icon_mapping.json` Datei wie folgt zu:

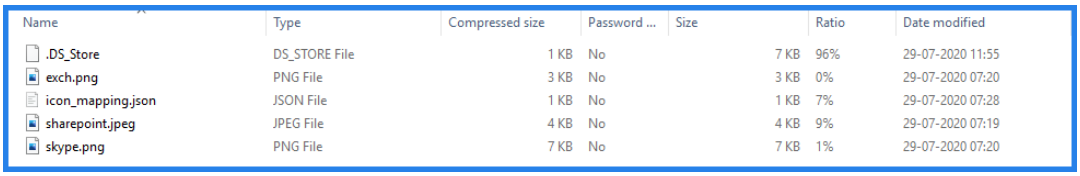
```
<StyleBook file name> : <icon file name>
<!--NeedCopy-->
```

Es folgt ein Beispiel für ein StyleBook-Bundle:



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
resources	File folder					29-07-2020 07:25
.DS_Store	DS_STORE File	1 KB	No	7 KB	92%	18-08-2020 17:31
exchange.yaml	YAML File	2 KB	No	6 KB	78%	31-07-2020 11:37
sharepoint.yaml	YAML File	1 KB	No	1 KB	56%	29-07-2020 10:13
skype.yaml	YAML File	1 KB	No	1 KB	55%	29-07-2020 10:13

Der `resources` Ordner enthält die erforderlichen Symbole.



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
.DS_Store	DS_STORE File	1 KB	No	7 KB	96%	29-07-2020 11:55
exch.png	PNG File	3 KB	No	3 KB	0%	29-07-2020 07:20
icon_mapping.json	JSON File	1 KB	No	1 KB	7%	29-07-2020 07:28
sharepoint.jpeg	JPEG File	4 KB	No	4 KB	9%	29-07-2020 07:19
skype.png	PNG File	7 KB	No	7 KB	1%	29-07-2020 07:20

In diesem Beispiel werden `sharepoint.yaml` und `skype.yaml` Dateien automatisch `sharepoint.jpeg` und `skype.png` zugeordnet.

Um `exchange.yaml` zuzuordnen `exch.png`, geben Sie Folgendes in der `icon_mapping.json` Datei an:

```
{

”exchange.yaml”:”exch.png”
 }

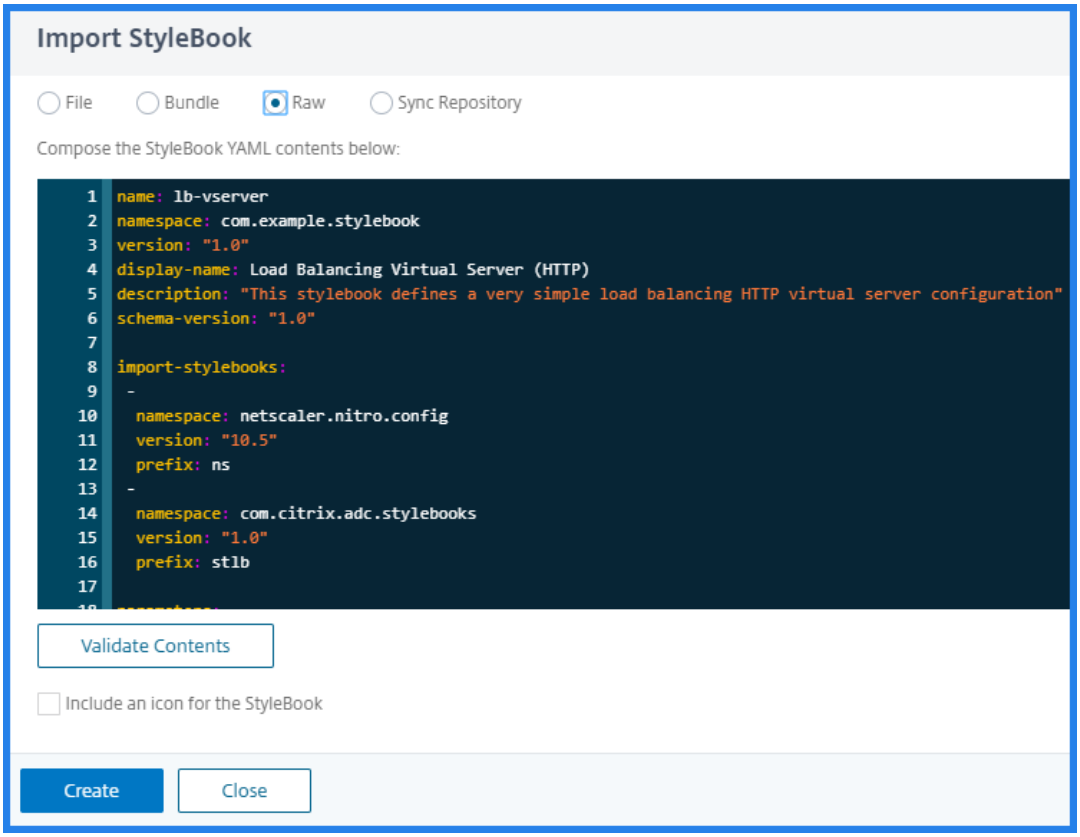
<!--NeedCopy-->
```

- **Raw** - Verfassen Sie den Inhalt Ihres StyleBook im YAML-Editor.

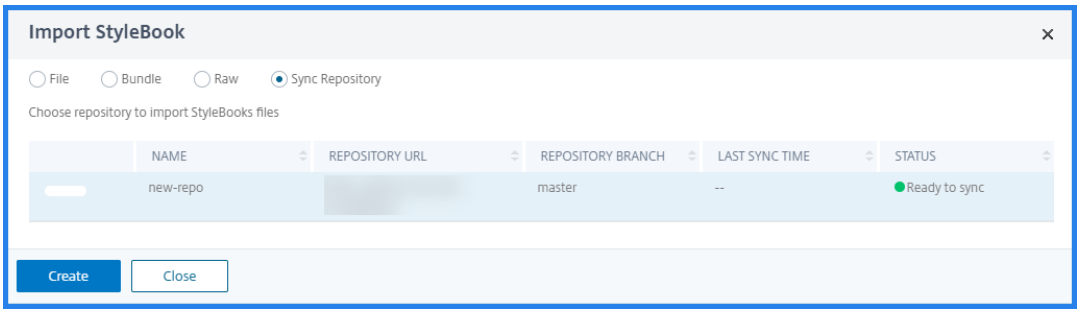
  Sie können den StyleBook-Inhalt überprüfen, um die StyleBook-Grammatikfehler zu überprüfen. Um StyleBook-Inhalte zu überprüfen, klicken Sie auf **Inhalt überprüfen**.

  > **Hinweis Achten Sie**
  >
  > beim Komponieren von StyleBook darauf, die folgenden Konzepte zu kennen:
  >
  > - NITRO API
  > - YAML

  Weitere Informationen zum Schreiben eigener StyleBooks finden Sie unterSo erstellen Sie Ihre eigenen StyleBooks.



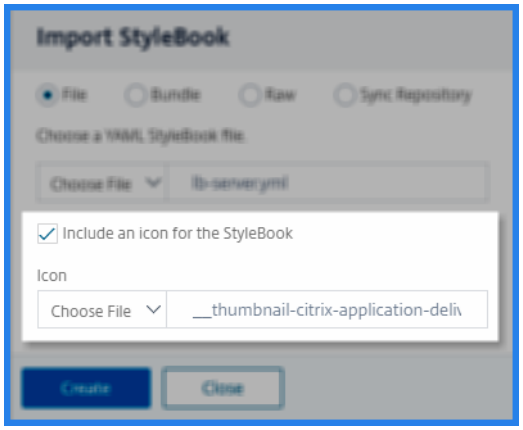
- **Sync Repository** - Diese Option listet die Repositories auf, die ADM hinzugefügt wurden. Wählen Sie das Repository aus, das Sie mit ADM synchronisieren möchten.



> **Hinweis**
>
> Sie können den Inhalt auch aus einer StyleBook YAML-Datei kopieren und in den YAML-Editor einfügen.

3. Optional können Sie ein Symbol für ein StyleBook auswählen.

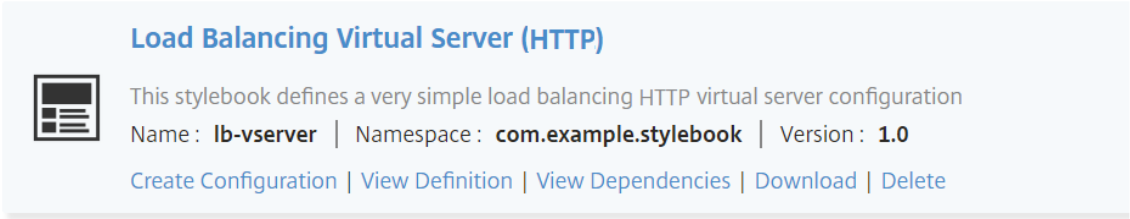
   In **Anwendungen > StyleBook**wird das importierte StyleBook mit diesem Symbol angezeigt.



4. Klicken Sie auf **Erstellen**.

   Citrix ADM überprüft jetzt Ihr StyleBook auf alle syntaktischen und semantischen Fehler gemäß der StyleBook-Grammatik. Ihr StyleBook wird bei Fehlern nicht in Citrix ADM importiert.

   Wenn keine Fehler auftreten, wird das StyleBook erfolgreich importiert und auf der Seite **StyleBooks** aufgeführt. Sie können das StyleBook anhand des Anzeigenamens identifizieren, den Sie im Kopfbereich des StyleBook definiert haben.



> **Hinweis**
>
> Wenn Sie ein Paket von Dateien importieren, dekomprimiert Citrix ADM den gezippten Ordner und validiert alle StyleBooks.
> Das Bundle wird nicht importiert, auch wenn eine StyleBook-Datei den Validierungstest fehlschlägt.

   Weitere Hinweise zur StyleBook-Grammatik und Syntax der verschiedenen Konstrukte und Attribute finden Sie unterStyleBook Grammatik.

5. Klicken Sie auf den Link **Konfiguration erstellen**, um Konfigurationen aus diesem StyleBook zu erstellen.

   Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

6. Geben Sie die erforderlichen Werte für die Parameter an.

   Im folgenden Beispiel wird

a) Geben Sie den **Anwendungsnamen** und die**Pflichtfelder für die IP-Adresse des**Lastausgleichs an.

b) Wählen Sie den **LoadBalancing-Algorithmus** aus der Liste aus. Standardmäßig**ist**ROUNDROBIN ausgewählt.

!![Beispiel-Konfigurationsbereitstellung] (/de-de/citrix-application-delivery-management-service/media/nmas-stylebooks-yaml-editor-4.png)

7. Wählen Sie unter **Zielinstanzen**die IP-Adresse der Citrix ADC-Instanz aus, in der Sie die Konfiguration bereitstellen möchten.

   Sie können die Konfiguration auch auf mehreren Citrix ADC bereitstellen, indem Sie beliebig viele Zielinstanzen angeben.

8. Wenn Sie die Citrix ADC (NITRO) -Konfigurationsobjekte testen möchten, bevor Sie die Konfiguration bereitstellen, klicken Sie auf **Dry Run**.

   Wenn die Konfiguration gültig ist, werden die Konfigurationsobjekte basierend auf den angegebenen Werten erstellt.

   In diesem Beispiel erstellt das StyleBook nur ein Objekt vom Typ `lbvserver`. Dieser Lastenausgleichsserver war die einzige Komponente, die in diesem grundlegenden Beispiel StyleBook definiert wurde.

   Klicken Sie später auf **Erstellen**, um die Konfiguration auf den ausgewählten Citrix ADC-Instanzen bereitzustellen.

Nachdem Sie die Konfiguration erfolgreich bereitgestellt haben, wird auf der Seite “Konfigurationen” ein neues **Konfigurationspaket** angezeigt.

> **Hinweis**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC-Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

Benutzerdefinierte StyleBooks suchen

Mit Citrix ADM können Sie jetzt basierend auf ihrem Typ nach StyleBooks suchen. Das heißt, Sie können jetzt entweder nach Standard-StyleBooks oder benutzerdefinierten StyleBooks suchen. Diese Option ist besonders hilfreich, wenn Sie in vielen Standard-StyleBooks nach Ihren benutzerdefinierten StyleBooks suchen müssen.

So suchen Sie nach benutzerdefinierten StyleBooks

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfigurationen** > **StyleBooks**.
2. Klicken Sie oben rechts auf das Suchsymbol.
3. Wählen Sie in der Suchleiste **Typ** aus, und wählen Sie dann **Benutzerdefiniert** aus der Unterliste aus.
4. Citrix ADM zeigt nur die benutzerdefinierten StyleBooks an.

Importieren eines StyleBook, um eine Anwendung für die Autoscale-Gruppe zu konfigurieren

April 28, 2021

Sie können die standardmäßigen StyleBooks in ADM verwenden, um eine Anwendung in einer ADC Autoscale-Gruppe zu konfigurieren. Weitere Informationen finden Sie unter den folgenden Links:

- AWS
- Microsoft Azure

Alternativ können Sie auch eigene StyleBooks erstellen oder importieren, um eine Anwendung zu erstellen. Die Autoscale-Gruppe StyleBooks ähneln traditionellen StyleBooks. Die StyleBooks zum Konfigurieren von Anwendungen in ADC Autoscale-Gruppen und Instanzen weisen jedoch einige Variationen auf. Dieser Artikel hilft Ihnen, sich mit den StyleBook-Regeln zur Konfiguration einer Autoscale-Anwendung vertraut zu machen.

Bevor Sie beginnen, stellen Sie sicher, dass Sie eine ADC Autoscale-Gruppe haben, die in ADM erstellt wurde.

Um ein benutzerdefiniertes StyleBook zum Konfigurieren einer Autoscale-Anwendung zu importieren, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Netzwerke > AutoScale-Gruppe**.
2. Wählen Sie die Autoscale-Gruppe aus, die Sie konfigurieren möchten.
3. Klicken Sie auf **Konfigurieren**.
4. Geben Sie die folgenden Details an:
    - **Anwendungsname** - Geben Sie den Namen einer Anwendung an.
    - **Zugriffstyp** - Sie können die ADM-Lösung für die automatische Skalierung sowohl für externe als auch für interne Anwendungen verwenden. Wählen Sie den erforderlichen Anwendungszugriffstyp aus.

- **FQDN-Typ** - Wählen Sie einen Modus für die Zuweisung von Domänen- und Zonennamen aus.

  Wenn Sie manuell angeben möchten, wählen Sie **Benutzerdefiniert** aus. Um Domänen- und Zonennamen automatisch zuzuweisen, wählen Sie **Automatisch generiert** aus.

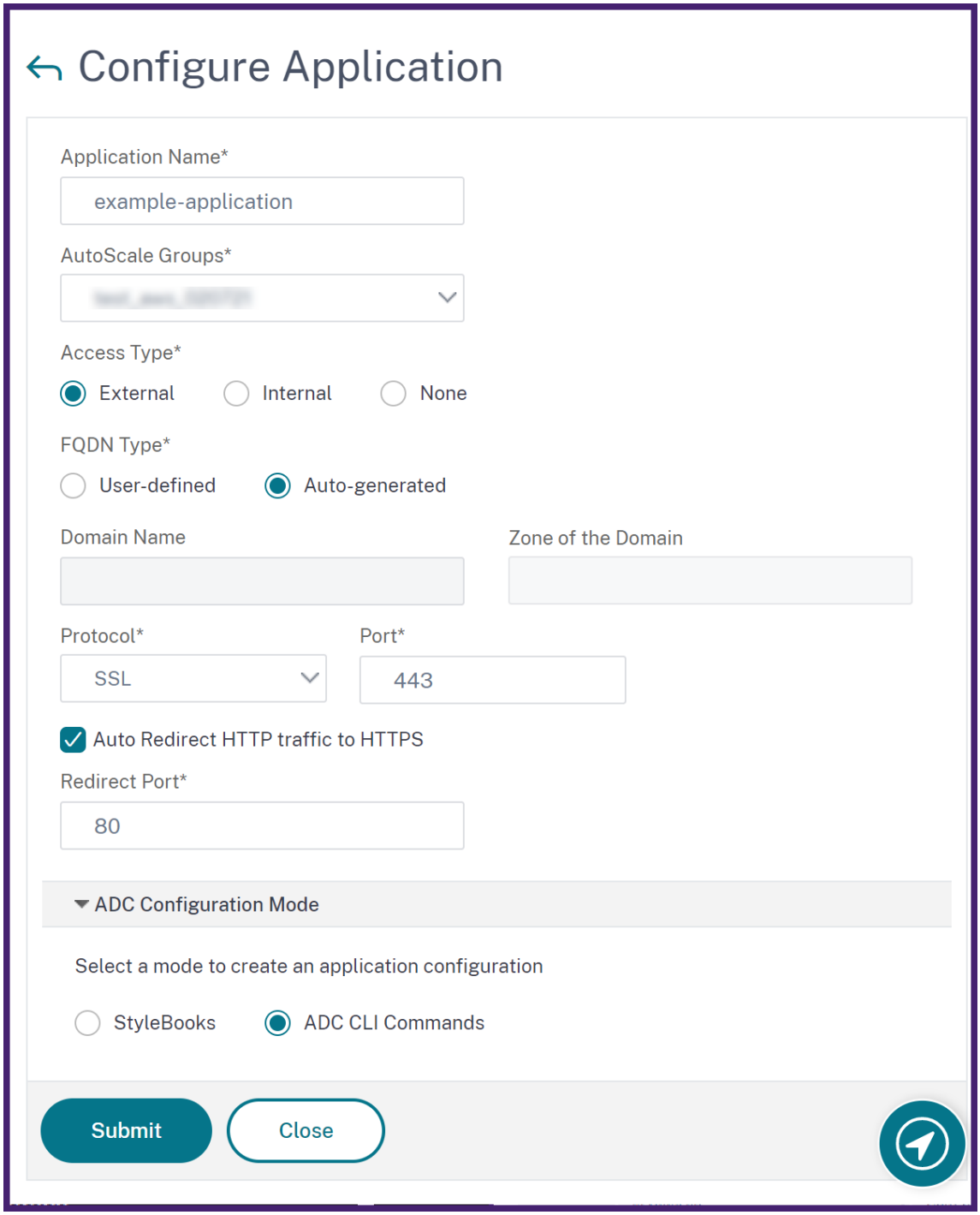
- **Domänenname** - Geben Sie den Domänennamen einer Anwendung an. Diese Option ist nur anwendbar, wenn Sie Benutzerdefinierter FQDN-Typ auswählen.

- **Zone der Domäne** - Wählen Sie den Zonennamen einer Anwendung aus der Liste aus. Diese Option ist nur anwendbar, wenn Sie Benutzerdefinierter FQDN-Typ auswählen.

  Dieser Domänen- und Zonenname leitet zu den virtuellen Servern in Azure um. Wenn Sie beispielsweise eine Anwendung in `app.example.com`hosten, ist `app`der Domänenname und `example.com`der Zonenname.

- **Protokoll** - Wählen Sie den Protokolltyp aus der Liste aus. Die konfigurierte Anwendung empfängt den Datenverkehr abhängig vom ausgewählten Protokolltyp.

- **Port** - Geben Sie den Portwert an. Der angegebene Port wird verwendet, um eine Kommunikation zwischen der Anwendung und der Autoscale-Gruppe herzustellen.



5. Klicken Sie auf **StyleBook wählen**.
6. Klicken Sie auf der Seite **StyleBook auswählen** auf **Neues StyleBook importieren**. Weitere Informationen zu den Importoptionen finden Sie unter Importieren und verwenden StyleBook.

Die Autoscale-Gruppe StyleBooks haben einige obligatorische Parameter. Die folgende Attributliste beschreibt die Variation zwischen der Autoscale-Gruppe und traditionellen StyleBooks:

- **Typ** - Schließen Sie im Abschnitt “Header” das `type` Attribut mit dem Wert ein: `autoscale`.

```
type: autoscale
<!--NeedCopy-->
```

Dieses Attribut stellt sicher, dass das StyleBook nur zur Konfiguration einer Anwendung in der ADC Autoscale-Gruppe verwendet wird. Und es verhindert, dass das StyleBook in der Liste **Anwendungen > StyleBooks** angezeigt wird.

Es folgt ein Beispiel-Header der Autoscale-Gruppe StyleBook:

```
name: autoscale-params
namespace: com.citrix.adc.commontypes
version: ”1.0”
description: ”This StyleBook defines the parameters required for
   Autoscale Deployment”
display-name: ”Autoscale Parmeters StyleBook”
private: true
type: autoscale
schema-version: ”1.0”
<!--NeedCopy-->
```

- **Anwendungsname** : Dieser Parameter beschreibt den Anwendungsnamen und die Beschreibung. Geben Sie das Beschriftungsfeld an, um den Parameter in der ADM-GUI anzuzeigen. Dieses Feld ist ein String-Typ.

```
-
    name: app_name
    label: ”Application Name”
    description: ”Name of the Application”
    type: string
    key: true
    gui:
      updatable: false
      required: true
<!--NeedCopy-->
```

- **Virtuelle IP-Adresse** - Dieser Parameter beschreibt die IP-Adresse eines virtuellen Servers. Die Autoscale-Gruppe aktualisiert diesen Parameter automatisch.


```
1  -
2      name: ip_address
3      label: "IP Address of the LoadBalancer"
4      description: "IP Address of the LoadBalancer"
5      type: ipaddress
6      gui:
7        hidden: true
8  <!--NeedCopy-->
```

- **IPSet** - Wenn Sie eine Anwendung bereitstellen, `IPset` wird eine auf Clustern in jeder Availability Zone erstellt.
  - In AWS sind die Domain und die Instanz-IP-Adressen bei DNS/NLB registriert.
  - In Azure sind die Domäne und die Instanz IP-Adressen beim Azure-Traffic-Manager oder ALB registriert.

  Sie können IP-Adressen oder eine IP angeben, die in der Autoscale-Gruppe StyleBook festgelegt wurde.

```
1  -
2      name: ipset
3      label: "IPSet"
4      description: "Configuration for network ipset resource"
5      type: string
6      gui:
7        hidden: true
8  <!--NeedCopy-->
```

Erstellen eines StyleBook zum Hochladen von Dateien in Citrix ADM

April 28, 2021

Mit Citrix Application Delivery Management (Citrix ADM) -StyleBooks können Sie Citrix ADC Konfigurationen erstellen, die unter anderem beim Hochladen von Dateien beliebiger Art von Ihrem lokalen Dateisystem auf die Citrix ADC-Instanz unter Verwendung der Citrix ADM GUI oder der APIs umfassen können. Diese Dateien können die Beispielzertifikatdateien oder Geolocation-Dateien sein. Sie können auch das Verzeichnis angeben, in dem diese Dateien hochgeladen werden sollen.

StyleBook-Konfiguration

Im Folgenden finden Sie ein Beispiel-StyleBook, das beschreibt, wie eine Geo-Location-Datei auf die Citrix ADC-Instanz hochgeladen wird. Die Geodateien werden in der Regel in GSLB-Konfigurationen verwendet, um die statische Nähe basierend auf dem Geo-Standort zu definieren:

Erstellen Sie Ihr StyleBook - 1

```
name: upload-geolocations
namespace: com.citrix.adc.stylebooks.samples
version: ”1.0”
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: ”1.0”

import-stylebooks:
-
 namespace: netscaler.nitro.config
 version: ”11.1”
 prefix: ns

parameters:
-
 name: locationfile
 label: Location File
 description: The system file path of the geolocation file on Citrix
    ADM
 type: file
 required: true

components:
-
 name: upload-file-comp
 type: ns::systemfile
 properties:
    filename: $parameters.locationfile.filename
    filelocation: ”/var/netscaler/inbuilt_db/”
    filecontent: base64.encode($parameters.locationfile.contents)
<!--NeedCopy-->
```


> **Hinweis:**
>
> Der in diesem Beispiel verwendete Parameter ist vom Typ “Datei”. Sie können dieses StyleBook in Citrix ADM importieren und es zum Hochladen von Geolocationsdateien verwenden.

Für dieses StyleBook muss die Datei bereits in Citrix ADM vorhanden sein (z. B. hätten Sie sie bereits mit einem Dienstprogramm wie SCP auf Citrix ADM kopiert).
Wenn Sie eine Datei über Citrix ADM auf Citrix ADCs hochladen möchten, ohne sie zuerst in das Citrix ADM-Dateisystem zu kopieren, können Sie ein StyleBook erstellen, das über zwei string-Parameter verfügt. Einer ist für die Angabe des Dateinamens, der auf dem Citrix ADC verwendet werden soll, und der andere, um den Inhalt des -Datei und verwenden Sie diese beiden Parameter in den Upload-file-comp-Komponenten. Im Folgenden finden Sie ein alternatives StyleBook, um eine Geo-Location-Datei hochzuladen:

Erstellen Sie Ihr StyleBook - 2

```
name: upload-geolocations-alt
namespace: com.citrix.adc.stylebooks.samples
version: ”1.0”
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: ”1.0”

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: ”11.1”
  prefix: ns

parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the Citrix ADC
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true
```



```
27
28 components:
29  -
30   name: upload-file-comp
31   type: ns::systemfile
32   properties:
33    filename: $parameters.filename
34    filelocation: ”/var/Citrix ADC/inbuilt_db/”
35    filecontent: base64.encode($parameters.filecontents)
36 <!--NeedCopy-->
```

Erstellen von Konfigurationen zum Hochladen von Dateien

Im folgenden Verfahren wird eine Konfiguration für eine ausgewählte Citrix ADC-Instanz erstellt, die eine Geolocationsdatei mithilfe des ersten oben beschriebenen StyleBook hochladen würde.

So erstellen Sie eine Konfiguration zum Hochladen von Dateien:

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfiguration**, und klicken Sie auf **Neu erstellen**. Auf der Seite StyleBook auswählen werden alle StyleBooks angezeigt, die in Ihrem Citrix ADM verfügbar sind. Scrollen Sie nach unten und wählen Sie das StyleBook aus, das Sie importiert haben.

   Die StyleBook-Parameter werden als Benutzeroberflächenseite angezeigt, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

2. Geben Sie den Namen des Load Balancers und die virtuelle IP-Adresse in den Abschnitt Basic Load Balancer Einstellungen ein.

3. Geben Sie im Abschnitt **Speicherortdatei** den Namen oder den Speicherort der Datei ein.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass die Datei in Citrix ADM nur unter dem Ordner des aktuellen Mandanten ist. Kopieren Sie die Datei mit einem beliebigen FTP in das Citrix ADM-Dateisystem.

4. Möglicherweise werden Sie aufgefordert, Ihre Benutzeranmeldeinformationen anzugeben, bevor Sie auf die Zielinstanzen zugreifen.

5. Wählen Sie die Citrix ADC Zielinstanz aus, für die die Konfiguration erstellt werden muss, und klicken Sie auf **Erstellen**.

> **Hinweis**
>
> Citrix empfiehlt, dass Sie **Dry Run** auswählen, um die auf der Zielinstanz erstellten Konfigurationsobjekte zu überprüfen, bevor Sie die eigentliche Konfiguration auf der Instanz ausführen.

Wenn die Erstellung des Konfigurationspakets erfolgreich ist, wird die Datei im Citrix ADC-Instanzdateisystem unter dem Speicherort gespeichert: /var/netscaler/inbuilt_db/

> **Hinweis**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC-Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

Verwenden der Citrix ADM -API zum Erstellen eines Konfigurationspakets

Sie können die Citrix ADM API auch verwenden, um ein Konfigurationspaket zu erstellen, das Dateien in die ausgewählte Citrix ADC-Instanz hochlädt. Weitere Informationen zur Verwendung von APIs finden Sie unter Verwenden von API zum Erstellen von Konfigurationen zum Hochladen beliebiger Dateitypen.

Erstellen eines StyleBook zum Hochladen von SSL-Zertifikats- und Zertifikatsschlüsseldateien in Citrix ADM

April 28, 2021

Wenn Sie eine StyleBook-Konfiguration erstellen, die das SSL-Protokoll verwendet, müssen Sie die SSL-Zertifikatdateien und Zertifikatschlüsseldateien gemäß den StyleBook-Parametern hochladen. Mit StyleBook können Sie die SSL-Dateien und Schlüsseldateien direkt von Ihrem lokalen System hochladen, indem Sie die Citrix Application Delivery Management (ADM) GUI verwenden. Sie können Citrix ADM APIs auch zum Hochladen von Zertifikatsdateien und Schlüsseldateien verwenden, die bereits von Citrix ADM verwaltet werden.

StyleBook-Konfiguration

Dieses Dokument unterstützt Sie beim Erstellen eines eigenen StyleBook - **Load Balancing Virtual Server (SSL)**
mit Komponenten zum Hochladen von SSL-Zertifikaten und Schlüsseldateien. Das hier bereitgestellte StyleBook als Beispiel erstellt eine grundlegende Konfiguration des Lastenausgleichs für die virtuelle Serverkonfiguration auf der ausgewählten Citrix ADC-Instanz. Die Konfiguration verwendet das SSL-Protokoll. Um eine Konfiguration mit diesem StyleBook zu erstellen, müssen Sie den Namen und die IP-Adresse des virtuellen Servers angeben, die Parameter für die Lastausgleichsmethode auswählen und die Zertifikatdatei und die Zertifikatsschlüsseldatei für den virtuellen Server hochladen oder eine Zertifikat- und Zertifikatschlüsseldatei verwenden, die bereits im Citrix ADM vorhanden. Diese werden im Abschnitt Parameter angegeben, wie unten dargestellt:


```
parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: certificate
  label: "SSL Certificate File"
  description: "The file name of the SSL certificate file"
  type: certfile
 -
  name: key
  label: "SSL Certificate Key File"
  description: "The file name of the server certificate's private key
     file"
  type: keyfile
<!--NeedCopy-->
```

Im Komponentenbereich des StyleBook werden dann zwei Komponenten erstellt, wie unten gezeigt. Die `my-lbvserver-comp` Komponente ist vom Typ ns lbvserver, wobei

- ns ist das Präfix, das sich auf den integrierten Namespace netscaler.nitro.config und Version 10.5 bezieht, den Sie im Abschnitt import-stylebooks angegeben hatten.
- `lbvserver` ist ein integriertes StyleBook in diesem Namespace. Es entspricht der gleichnamigen Citrix ADC `lbvserver` NITRO-Ressource.

Die zweite Komponente `lbvserver-certificate-comp` ist vom Typ `stlb::vserver-certs-binds`. Das Präfix `stlb` bezieht sich auf den Namespace "com.citrix.adc.stylebooks" und Version 1.0, der im Abschnitt "Import-Stylebooks" des StyleBooks angegeben ist. Wenn der Namespace "com.citrix.adc.stylebooks" als Ordner betrachtet werden kann, `vserver-certs-binds` befindet sich ein anderes StyleBook (oder eine Datei) in diesem Ordner. StyleBooks, die sich im Namespace com.citrix.adc.stylebooks befinden, werden als Teil von Citrix ADM ausgeliefert.

Mit dem von benutzerdefinierten `vserver-certs-binds` StyleBooks verwendeten StyleBook können Sie die Zertifikate einfach konfigurieren, indem Sie das Zertifikat und die Schlüsseldateien auf die Citrix ADC-Zielinstanz hochladen und die Bindung des Zertifikats und der Schlüsseldateien an die entsprechenden virtuellen Server konfigurieren. Die Eigenschaften für diese Komponente lauten - der Name des virtuellen lb Servers und die Namen der SSL-Zertifikate, die Sie beim Erstellen des Konfigurationspakets angeben.

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: SSL
   ipv46: $parameters.ip
   port: 443
   lbmethod: $parameters.lb-alg
 -
  name: lbvserver-certificate-comp
  type: stlb::vserver-certs-binds
  description: Binds lbvserver with server certificate
  properties:
   vserver-name: $components.my-lbvserver-comp.properties.name
   certificates:
    -
     cert-name: $parameters.name + "-lb-cert"
     cert-file: $parameters.certificate
     ssl-inform: PEM
     key-name: $parameters.name + "-key"
     key-file: $parameters.key
<!--NeedCopy-->
```

Wenn Sie die API verwenden, um eine Konfiguration aus einem solchen StyleBook zu erstellen, verwenden Sie nur die Dateinamen (nicht den vollständigen Dateipfad). Diese Dateien werden voraussichtlich bereits in den Zertifikats- und Schlüsseldateiordnern auf Citrix ADM verfügbar sein. Die hochgeladene SSL-Zertifikatsdatei wird auf Citrix ADM im Verzeichnis /var/mps/tenants/… gespeichert. /ns_ssl_certs Verzeichnis und die SSL-Zertifikatsschlüsseldatei wird in /var/mps/tenants/… gespeichert. Verzeichnis /ns_ssl_keys in Citrix ADM.

Erstellen von Konfigurationen zum Hochladen von SSL-Dateien

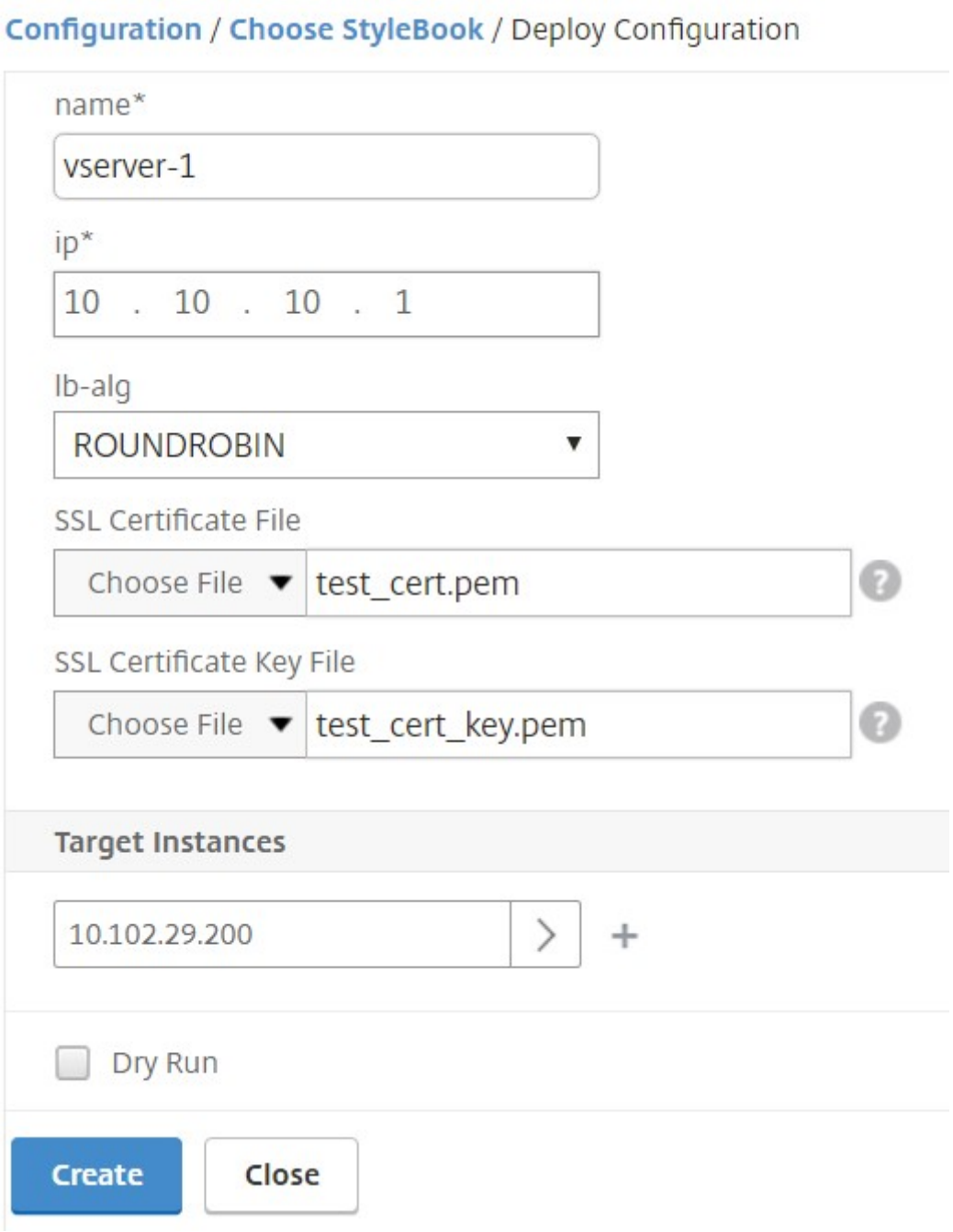
Das folgende Verfahren erstellt eine grundlegende Konfiguration des virtuellen Lastenausgleichs auf einer ausgewählten Citrix ADC-Instanz unter Verwendung des SSL-Protokolls aus dem oben angegebenen StyleBook. Sie können dieses Verfahren verwenden, um die SSL-Zertifikatsdateien und die Zertifikatsschlüsseldateien in Citrix ADM hochzuladen.

So erstellen Sie eine Konfiguration zum Hochladen von Dateien:

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfiguration > StyleBooks**. Auf der Seite **StyleBooks** werden alle StyleBooks angezeigt, die in Ihrem Citrix ADM verfügbar sind.
2. Scrollen Sie nach unten, wählen Sie **Load Balancing Virtual Server (SSL)** oder geben Sie **Load Balancing Virtual Server (SSL)** in das Suchfeld ein und drücken **Sie die Eingabetaste**.
3. Klicken Sie im StyleBook-Bedienfeld auf **Konfiguration erstellen**.

   Die StyleBook-Parameter werden als Benutzeroberflächenseite angezeigt, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
4. Geben Sie den Namen des Load Balancers und die virtuelle IP-Adresse in den Abschnitt Basic Load Balancer Einstellungen ein.
5. Wählen Sie im Abschnitt **SSL-Zertifikateinstellungen** die entsprechenden Dateien aus Ihrem lokalen Speicherordner aus. Alternativ können Sie die Dateien auswählen, die auf dem Citrix ADM selbst vorhanden sind.
6. Wählen Sie die Citrix ADC Zielinstanz aus, für die die Konfiguration erstellt werden muss, und klicken Sie auf **Erstellen**.

> **Hinweis**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC-Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.



Hinweis

In Citrix ADM können Sie mithilfe der folgenden Standard-StyleBooks, die als Teil von Citrix ADM ausgeliefert werden, SSL-Unterstützung durch Hochladen der SSL-Zertifikate und -Schlüssel erstellen.

- HTTP/SSL LoadBalancing StyleBook (lb)
- HTTP/SSL LoadBalancing (mit Monitoren) StyleBook (`lb-mon`)

> - HTTP/SSL Content Switched Anwendung mit Monitoren (`cs-lb-mon`)
> - Beispiel für Application StyleBook mit CS, LB und SSL Funktionen (`sample-cs-app`)
>
> Sie können auch Ihre eigenen StyleBooks erstellen, die SSL-Zertifikate verwenden, wie im obigen StyleBook beschrieben

Erstellen Sie Ihr StyleBook

Der vollständige Inhalt der Datei lb-vserver-ssl.yaml ist unten dargestellt:

```
name: lb-vserver-ssl
description: ”This stylebook defines a load balancing virtual server
   configuration.”
display-name: ”Load Balancing Virtual Server (SSL)”
namespace: com.example.ssl.stylebooks
schema-version: ”1.0”
version: ”0.1”

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: ”10.5”
 -
  namespace: com.citrix.adc.stylebooks
  prefix: stlb
  version: ”1.0”

parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
```



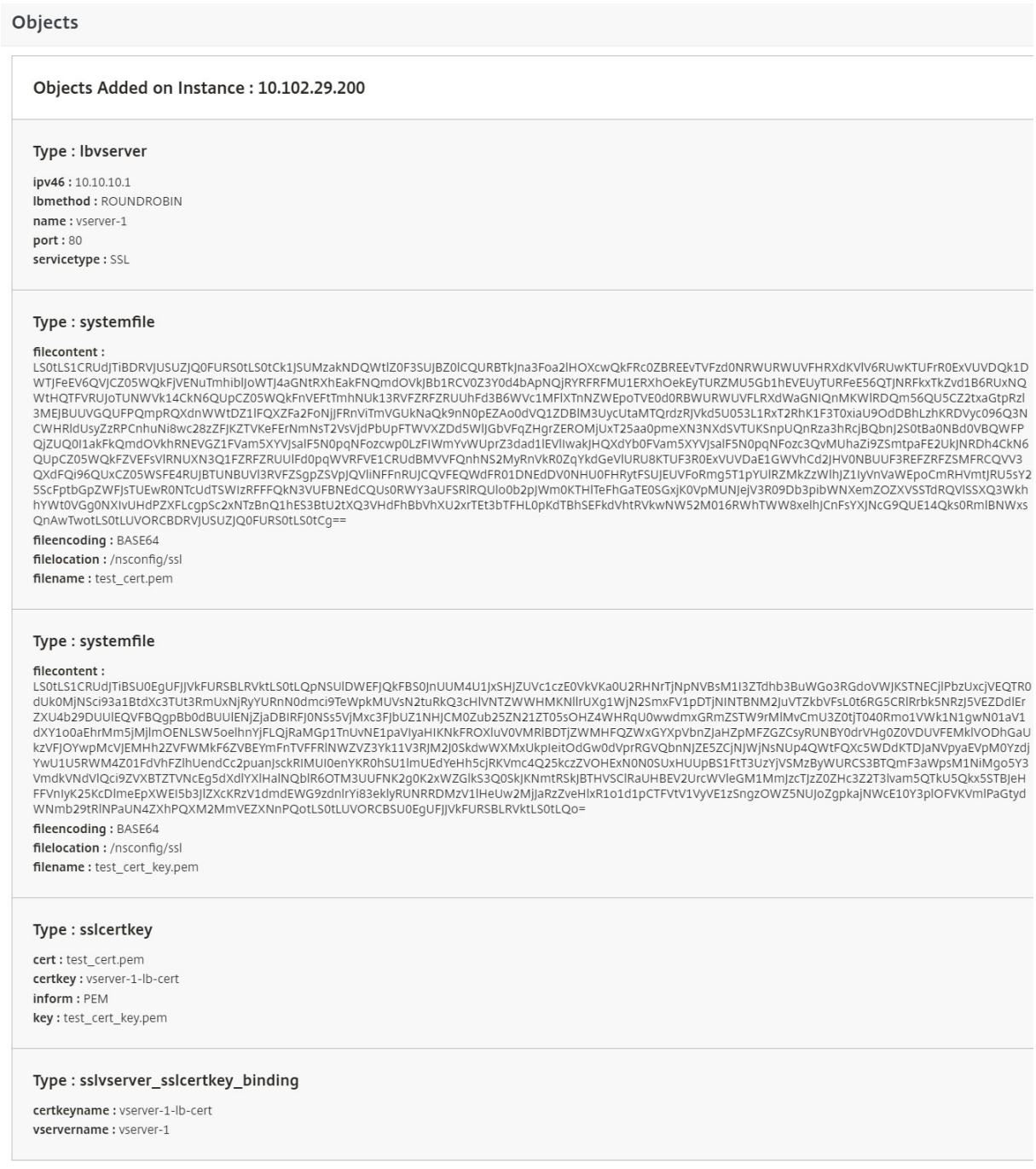
```
33    default: ROUNDROBIN
34   -
35    name: certificate
36    label: "SSL Certificate File"
37    description: "The file name of the SSL certificate file"
38    type: certfile
39   -
40    name: key
41    label: "SSL Certificate Key File"
42    description: "The file name of the server certificate's private key
          file"
43    type: keyfile
44
45  components:
46   -
47    name: my-lbvserver-comp
48    type: ns::lbvserver
49    properties:
50      name: $parameters.name
51      servicetype: SSL
52      ipv46: $parameters.ip
53      port: 443
54      lbmethod: $parameters.lb-alg
55   -
56    name: lbvserver-certificate-comp
57    type: stlb::vserver-certs-binds
58    description: Binds lbvserver with server certificate
59    properties:
60     vserver-name: $ components.my-lbvserver-comp.properties.name
61     certificates:
62      -
63       cert-name: $parameters.name + "-lb-cert"
64       cert-file: $parameters.certificate
65       ssl-inform: PEM
66       key-name: $parameters.name + "-key"
67       key-file: $parameters.key
68  <!--NeedCopy-->
```

Verwenden der Citrix ADM API zum Erstellen eines Konfigurationspakets:

Sie können die Citrix ADM-API auch verwenden, um ein Konfigurationspaket zu erstellen, das Cert- und Key-Dateien auf die ausgewählte Citrix ADC-Instanz hochlädt. Weitere Informationen zur Verwendung von APIs finden Sie unter Verwenden der API zum Erstellen von Konfigurationen zum Hochladen von Zertifikaten und Schlüsseldateien.

Anzeigen der in der Citrix ADC-Instanz definierten Objekte

Nachdem die StyleBook-Konfiguration (Configuration Pack) auf Citrix ADM erstellt wurde, klicken Sie auf **View objects**, um alle Citrix ADC-Objekte anzuzeigen, die auf der Citrix ADC-Zielinstanz erstellt wurden



Analytics aktivieren und Alarme auf einem virtuellen Server konfigurieren, der in einem StyleBook definiert ist

April 28, 2021

Sie können das Konstrukt “Vorgänge” verwenden, um Citrix Application Delivery Management (ADM) -Analysen zu konfigurieren, um AppFlow-Datensätze für alle oder einen Teil der Verkehrstransaktionen zu sammeln, die von einer virtuellen Serverkomponente verarbeitet werden, die Teil eines StyleBook ist. Sie können dieses Konstrukt auch verwenden, um Alarme zu konfigurieren, um Einblicke in den vom virtuellen Server verwalteten Datenverkehr zu erhalten.

Das folgende Beispiel zeigt einen Operationsabschnitt eines StyleBook:

```
operations:
  analytics:
   -
    name: lbvserver-ops
    properties:
      target: $components.basic-lb-comp
      filter: HTTP.REQ.URL.CONTAINS(”catalog”)
  alarms:
   -
    name: lbvserver-alarm
    properties:
      target: $components.basic-lb-comp
      email-profile: $parameters.emailprofile
      sms-profile: ”MyProdSMS”
      rules:
       -
         metric: ”total_requests”
         operator: ”greaterthan”
         value: 25
         period-unit: $parameters.period
       -
         metric: ”total_bytes”
         operator: ”lessthan”
         value: 60
         period-unit: ”day”
<!--NeedCopy-->
```

Die Attribute im Analytics-Abschnitt werden verwendet, um die Citrix ADM-Analytics-Funktion anzuweisen, AppFlow-Datensätze auf einer virtuellen Serverkomponente zu sammeln, die durch die

Zieleigenschaft identifiziert wird. Sie können optional auch eine Filtereigenschaft angeben, die einen Citrix ADM-Richtlinienausdruck akzeptiert, um Anforderungen zu filtern, für die AppFlow-Datensätze auf dem virtuellen Server gesammelt werden.

Wenn ein Konfigurationspaket aus diesem StyleBook erstellt wird, ist die Citrix ADM Analytics-Funktion so konfiguriert, dass es AppFlow-Datensätze auf den virtuellen Servern sammelt, die beim Erstellen eines Konfigurationspakets angegeben wurden.

Die Attribute im Abschnitt Alarme werden verwendet, um Schwellenwerte für die Generierung von Alarmen und das Senden von Benachrichtigungen auf dem virtuellen Server festzulegen, der von der Zieleigenschaft identifiziert wird. Im obigen Beispiel werden die Eigenschaften des E-Mail-Profils und des SMS-Profils verwendet, um anzugeben, wohin die Benachrichtigungen gesendet werden müssen. Der Abschnitt Regeln definiert die Schwellenwerte. Wenn beispielsweise die Gesamtanforderungen, die vom virtuellen Server verarbeitet werden, größer als 25 sind und für einen vom Benutzer definierten Zeitraum ein Alarm gesetzt und eine Benachrichtigung gesendet wird. Period-Unit gibt an, wie häufig ein Alarm ausgelöst wird. Es kann den Wert des Tages, der Stunde oder der Woche nehmen.

Sie können die folgenden Operatoren verwenden, wenn Sie den Metrikwert mit dem Schwellenwert vergleichen:

- `greaterthan` für >
- `lessthan` für <
- `greaterthanequal` für >=
- `lessthanequal` für <=

Beachten Sie, dass StyleBooks API-Namen für die Metriken verwenden und nicht die Namen, die auf der Citrix ADM Analytics-GUI angezeigt werden.

Informationen zum Anzeigen und Analysieren von Daten, die auf virtuellen Servern gesammelt wurden, die als Teil eines Konfigurationspakets erstellt wurden, finden Sie in der Citrix ADM Analytics-Dokumentation.

Instanzrollen

April 28, 2021

In Citrix Application Delivery Management (ADM) kann es ein Szenario geben, in dem Sie mehrere Citrix ADC-Instanzen für eine einzelne Anwendung konfigurieren müssen, aber auch, wenn für jede ADC-Instanz eine andere Konfiguration erforderlich ist. Ein Beispiel für einen solchen Fall ist das standardmäßige Microsoft Skype for Business StyleBook.

StyleBooks unterstützt derzeit die Möglichkeit, ein Konfigurationspaket zu erstellen und dieselbe Konfiguration auf mehrere Citrix ADC-Instanzen anzuwenden. Ein solches Szenario, in dem die Konfiguration auf allen ADC-Instanzen identisch ist, kann als symmetrische Konfiguration bezeichnet werden.

Mit der Funktion “Instanzrollen” von StyleBooks können Sie jetzt eine asymmetrische Konfiguration erstellen, dh ein Konfigurationspaket, das auf mehrere ADC-Instanzen angewendet werden kann, jedoch mit unterschiedlichen Konfigurationen auf verschiedenen ADC-Instanzen.

Wenn ein StyleBook mit Instanzrollen zum Erstellen eines Konfigurationspakets verwendet wird, kann jeder ADC-Instanz in einem Konfigurationspaket eine andere Rolle zugewiesen werden. Diese Rolle bestimmt die Konfigurationsobjekte des Konfigurationspakets, das die ADC-Instanz erhalten wird.

Zu beachtenswerte Punkte:

- Die Gruppe der Instanzrollen in einem StyleBook werden beim Erstellen des StyleBook definiert.
- Die Rollen werden einer bestimmten ADC-Instanz beim Erstellen oder Aktualisieren des Konfigurationspakets zugewiesen.

Abschnitt Zielrollen

Ein neuer Abschnitt in einem StyleBook namens target-roles wird eingeführt, in dem alle vom StyleBook unterstützten Rollen deklariert werden.

Dieser Abschnitt wird normalerweise nach dem Abschnitt Import-StyleBooks eines StyleBook und vor dem Parameterabschnitt platziert.

Im folgenden StyleBook-Beispiel werden im Abschnitt Zielrollen zwei Rollen definiert - A und B

```
target-roles:

  -
   name: A
   name: B
     min-targets: 2
     max-targets: 5
<!--NeedCopy-->
```

Sie können sehen, dass Rolle B auch zwei optionale Untereigenschaften definiert, min-targets und max-targets.

Obwohl diese beiden Untereigenschaften optional sind, geben Min-Ziele die minimale obligatorische Anzahl von ADC-Instanzen an, um diese Rolle zuzuweisen, wenn ein Konfigurationspaket aus diesem StyleBook erstellt wird, und maximale Ziele geben die maximale Anzahl von ADC-Instanzen an, denen diese Rolle beim Erstellen eines Konfigurationspakets zugewiesen werden kann von diesem StyleBook.

Wenn diese Untereigenschaften nicht angegeben sind, gibt es keine Begrenzung für die Anzahl der ADC-Instanzen, die für diese Rolle konfiguriert werden können. Wenn min-targets = 0 ist, ist die dieser Rolle zugeordnete Konfiguration optional, und wenn min-targets = 1 ist, ist diese Konfiguration obligatorisch, und mindestens eine ADC-Instanz muss für diese Rolle konfiguriert werden.

Rolle Standard

Zusätzlich zu explizit definierten Rollen gibt es eine implizite Rolle, die alle StyleBooks besitzen, und diese Rolle wird als Standardrolle aufgerufen. Diese Rolle kann wie jede andere Rolle in einem StyleBook verwendet werden. Wenn beim Erstellen eines Konfigurationspakets eine ADC-Instanz nicht mit einer bestimmten Rolle zugewiesen wird, wird die Instanz implizit der Rolle “Standard” zugewiesen. Die Instanz erhält nun alle Konfigurationsobjekte, die von Komponenten generiert werden, die die Standardrolle haben.

Komponenten mit Rollen

Nachdem die Rollen definiert sind, die ein StyleBook unterstützen kann (einschließlich der Rolle Standard), können die Rollen im Komponentenabschnitt eines StyleBook verwendet werden. Wenn eine Komponente nur auf ADC-Instanzen bereitgestellt werden soll, die eine bestimmte Rolle spielen, können Sie das Attribut roles als Teil der Komponente angeben, wie im folgenden Beispiel einer Komponente dargestellt:

```
1   -
2     name: C1
3     type: ns::lbvserver
4     roles:
5       - A
6     properties:
7       name: lb1
8       servicetype: HTTP
9       ipv46: 1.1.1.1
10      port: 80
11 <!--NeedCopy-->
```

Im obigen Beispiel generiert die Komponente eine `lbvserver`, die für Instanzen bereitgestellt wird, die die Rolle A spielen. Beachten Sie, dass das Rollenattribut einer Komponente eine Liste ist und einer Komponente mehrere Rollen zugewiesen werden kann. Diese Rollen wären im Abschnitt Zielrollen des StyleBook deklariert worden.

Hinweis: Wenn eine Komponente in einem StyleBook kein Rollenattribut angibt, werden Konfigurationsobjekte, die von der Komponente generiert werden, unabhängig von ihrer Rolle auf allen Citrix

ADC-Instanzen erstellt. Sie können diese Funktion effektiv verwenden, um Konfigurationsobjekte zu erstellen, die auf alle Instanzen eines Konfigurationspakets angewendet werden können.

Nehmen wir an, dass es ein StyleBook mit zwei Rollen definiert - A und B, und das vier Komponenten enthält.

- Komponente C1 hat die Rollen A und B
- Komponente C2 hat die Rolle B
- Komponente C3 hat keine Rollen definiert
- Komponente C4 hat die Rolle Standard

Der Komponentenbereich dieses StyleBook wird nachfolgend wiedergegeben:

```
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
```



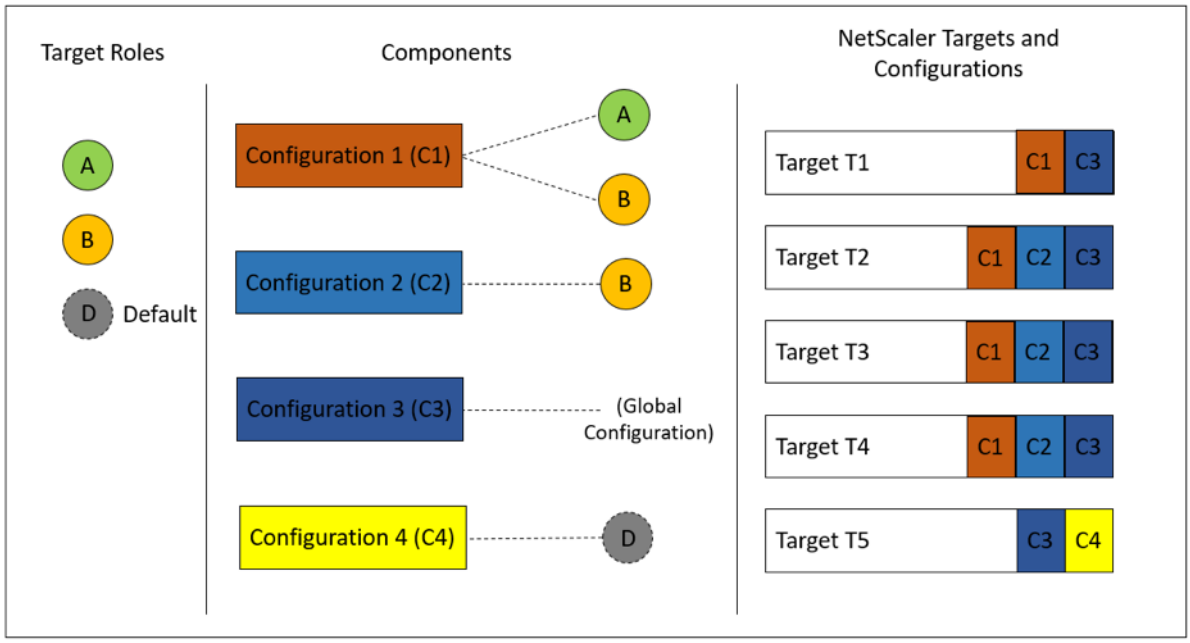
```
32      name: C4
33      type: ns::lbvserver
34      roles:
35        - default
36      properties:
37        name: lb4
38        servicetype: HTTP
39        ipv46: 14.14.14.14
40        port: 80
41  <!--NeedCopy-->
```

Beachten Sie, dass für die Komponente C3 keine Rolle definiert ist, was bedeutet, dass die Komponente unabhängig von ihrer Rolle auf allen Instanzen bereitgestellt wird. Auf der anderen Seite hat die Komponente C4 die Rolle Standard, was bedeutet, dass sie auf jede Instanz angewendet wird, der keine explizite Rolle zugewiesen ist.

Bedenken Sie nun, dass Sie ein Konfigurationspaket mit diesem StyleBook erstellen und es auf fünf ADC-Instanzen bereitstellen möchten. In diesem Stadium können Sie den Instanzen die Rollen folgendermaßen zuweisen:

- Rolle A ist den Instanzen T1, T2, T3 und T4 zugewiesen
- Rolle B wird den Instanzen T2, T3 und T4 zugewiesen
- Instanz T5 ist keine Rolle zugewiesen

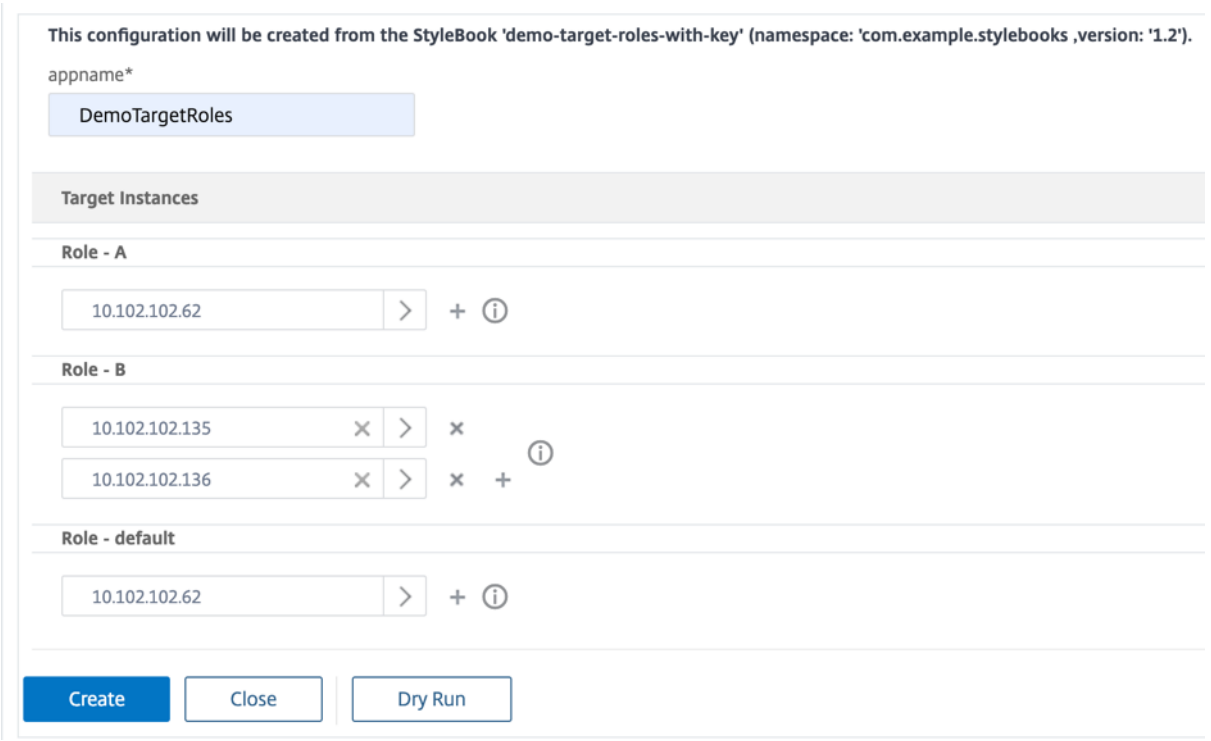
Das folgende Bild fasst die Rollenzuweisungen zusammen und zeigt die resultierende Konfiguration, die jede ADC-Instanz erhält:



Beachten Sie, dass die Komponente C3 unabhängig von der Rolle auf allen Instanzen bereitgestellt

wird, da diese Komponente kein Rollenattribut hatte.

Die folgende Abbildung zeigt die Zuweisung von Rollen beim Erstellen eines Beispielkonfigurationspakets:



Sie können auch die Funktion “Dry Run” verwenden, wenn Sie ein Konfigurationspaket erstellen, um die korrekte Zuweisung von Rollen und die Konfigurationsobjekte anzuzeigen und zu überprüfen, die für jede ADC-Instanz erstellt werden.

Erstellen Sie Ihr StyleBook

Der vollständige Inhalt des StyleBook demo-target-roles finden Sie unten:

```
---
name: demo-target-roles
namespace: com.example.stylebooks
version: ”1.2”
schema-version: ”1.0”
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: ”10.5”
parameters:
```

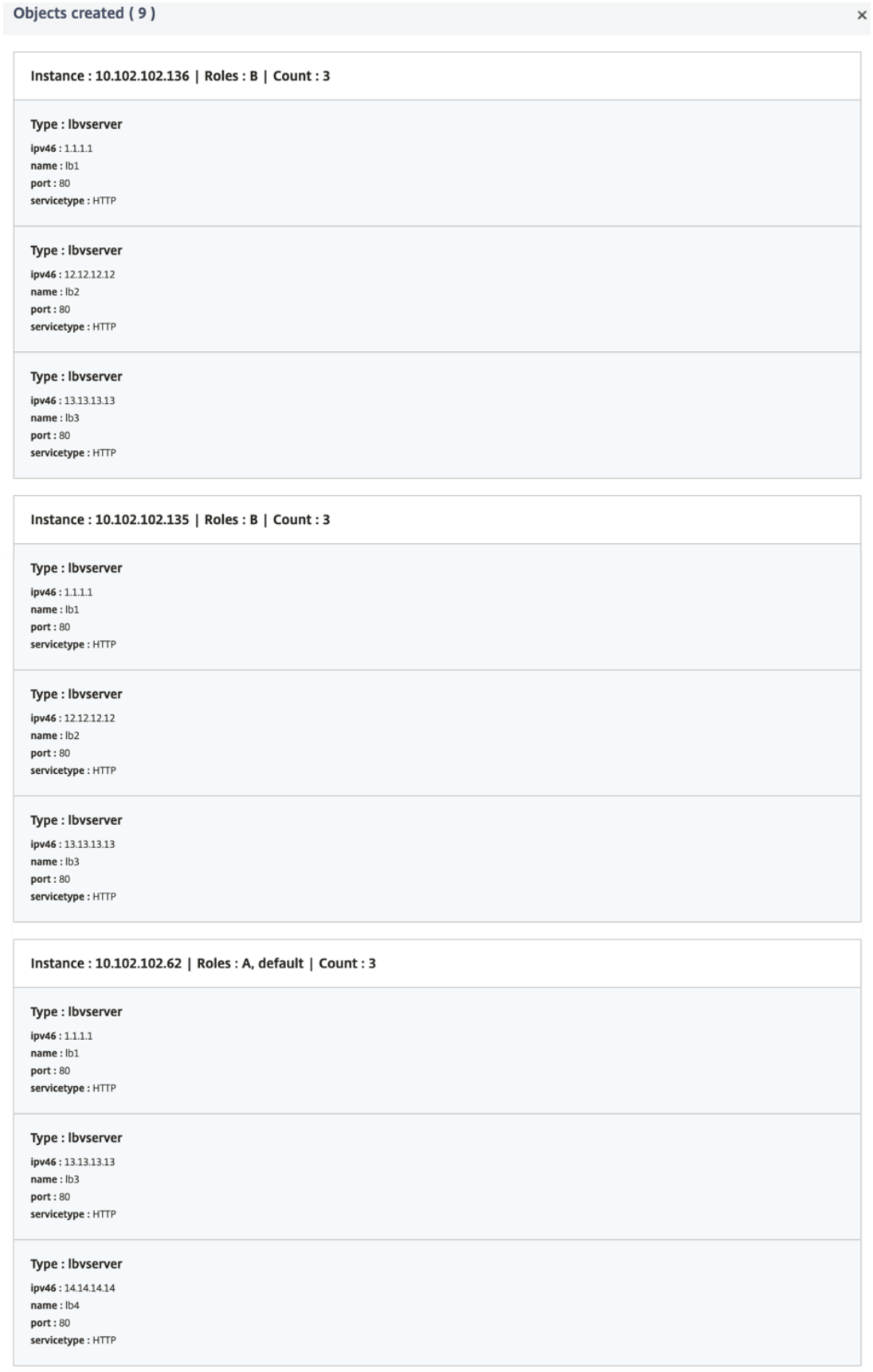


```
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
  -
    name: A
  -
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
```



```
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
<!--NeedCopy-->
```

Die folgende Abbildung zeigt die für ein Beispiel-Konfigurationspaket erstellten Objekte:



Verwenden von APIs

Wenn Sie die REST-API verwenden, können Sie beim Erstellen oder Aktualisieren des Konfigurationspakets Rollen für jede ADC-Instanz wie folgt angeben. Geben Sie im Block Ziele die UUID der spezifischen Citrix ADC-Instanz an, auf der die einzelnen Komponenten bereitgestellt werden sollen.

```
”targets”: [
            {

             ”id”: ”<ADC-UUID>”,
             ”roles”: [”A”]
             }
 ,
          ]
<!--NeedCopy-->
```

Als Referenz wird eine vollständige Beispiel-REST-API bereitgestellt.

POST/<ADM-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  ”configpack”: {

     ”parameters”: {

     ”appname”: ”app1”
     }
 ,
     ”targets”: [
        {

          ”id”: ”f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb”,
        ”roles”: [”A”]
         }
 ,
        {

          ”id”: ”c08caa1c-1011-48aa-b8c7-9aed1cd38ed0”,
          ”roles”: [”A”, ”B”]
         }
 ,
```



```
        {

          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
         }
,
        {

          "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
          "roles": ["A", "B"]
         }
,
        {

          "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
          "roles": ["default"]
         }

       ]
      }

}

<!--NeedCopy-->
```

Erstellen Sie ein StyleBook, um Nicht-CRUD-Operationen durchzuführen

April 28, 2021

StyleBooks verwalten Citrix ADC Konfigurationen, indem die erforderlichen Konfigurationsobjekte auf den Citrix ADC-Instanzen berechnet werden. Diese Objekte werden jedes Mal hinzugefügt, aktualisiert oder aus der Instanz entfernt, wenn Sie ein ConfigPack erstellen oder aktualisieren. Das ist, wenn Sie den gewünschten Zustand angeben.

Einige Citrix ADC-Konfigurationsobjekte unterstützen jedoch einige andere Vorgänge als Erstellen, Aktualisieren oder Löschen (CRUD-Vorgänge). Beispielsweise kann ein Load Balancer-Objekt (`lbvserver`) oder ein Citrix ADC-Funktionsobjekt (`nsfeature`) die Operation “Aktivieren” oder “Deaktivieren” unterstützen. In ähnlicher Weise `certkeys` unterstützt Citrix ADC die Operation “Link” und “Unlink”, um ein Zertifikat mit einem anderen Zertifikat zu verknüpfen oder aufzuheben. Diese Vorgänge für Citrix ADC Objekte werden als Nicht-CRUD-Vorgänge bezeichnet. In diesem Abschnitt wird beschrieben, wie nicht-CRUD-Vorgänge für Konfigurationsobjekte ausgeführt werden, die sie mithilfe von StyleBooks unterstützen.

> **Hinweis**
>
> Die Bindung zwischen Konfigurationsobjekten (z. B. “ `certkey` Binden a an a” `lbvserver`) wird nicht als Nicht-Crud-Operation angesehen. Dies liegt daran, dass NITRO-Bindungen selbst als Konfigurationsobjekte dargestellt werden. Diese Objekte werden wie jedes andere Citrix ADC Konfigurationsobjekt erstellt und gelöscht.

Unterstützung der Nicht-CRUD-Operationen

Ein neues Konstrukt namens meta-properties wird in der Komponente auf der gleichen Ebene wie das Konstrukt properties hinzugefügt. Das einzige Attribut, das in diesem Konstrukt derzeit unterstützt wird, heißt action Dieses Attribut kann Werte wie enable oder disable annehmen, die von diesem Konfigurationsobjekt unterstützt werden.

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  meta-properties
   action: enable
  properties:
    name: $parameters.name
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

In diesem Beispiel ist die `my-lbvserver-comp` Komponente vom Typ `ns::lbvserver`. Das “ns” ist das Präfix, das sich auf den Namespace netscaler.nitro.config und Version **10.5 bezieht, die Sie im Abschnitt import-stylebooks angegeben haben. Die `lbvserver` ist eine NITRO-Ressource in diesem Namensraum. Als implizite Aktion `lbvserver` wird der zuerst vom StyleBook erstellt. Dann wird der “Enable” -Vorgang daran ausgeführt.

Die in den Meta-Eigenschaften angegebene Aktion wird für das Konfigurationsobjekt nur während der Erstellung des ConfigPack ausgeführt. Aktualisierungen des ConfigPack führen keine nicht-CRUD-Aktionen aus.

> **Hinweis:**
>
> Der Wert des action -Attributs kann kein StyleBook-Ausdruck sein, der dynamisch ausgewertet wird.

Erstellen und Bearbeiten eines Konfigurationspakets

April 28, 2021

In Citrix Application Delivery Management (ADM) können Sie ein Konfigurationspaket aus einem StyleBook erstellen. Und das Konfigurationspaket ist an das StyleBook gebunden, aus dem es erstellt wurde. Die Aktualisierungen des Konfigurationspakets werden über das StyleBook vorgenommen, an das es gebunden ist.

Erstellen Sie ein Konfigurationspaket

Führen Sie Folgendes aus, um ein Konfigurationspaket aus einem StyleBook zu erstellen:

1. Navigieren Sie zu **Anwendungen > StyleBooks > Konfigurationen**.
2. Klicken Sie auf **Hinzufügen**.
3. **Wählen Sie in Choose StyleBooks**die erforderlichen StyleBooks aus, aus denen Sie ein Konfigurationspaket erstellen möchten.

   Diese Seite kategorisiert StyleBooks in Standard- und benutzerdefinierte StyleBooks. Wählen Sie die entsprechenden Reiter aus, um die erforderlichen StyleBooks zu finden
4. Geben Sie die erforderlichen Details wie Anwendungsname, IP-Adresse, Port oder Protokolltyp an.

   Die GUI-Felder unterscheiden sich von StyleBook zu StyleBook.
5. Wählen Sie in **Target Instanzen** Instanzen oder Instanzgruppen aus, in denen Sie die Konfiguration ausführen möchten.

   > **Hinweis:**
   >
   > Sie können die Konfiguration auf mehr als einem Citrix ADC bereitstellen, indem Sie beliebig viele Zielinstanzen angeben.
6. Klicken Sie auf **Dry Run**.

   Auf der Seite " **Objekte** " werden die Objekte angezeigt, die erstellt, geändert oder aus den Citrix ADC-Instanzen entfernt werden.
7. Klicken Sie auf **Erstellen**

   Das Konfigurationspaket wird auf der Seite **StyleBook > Konfigurationen** angezeigt.

Wenn Sie die vorhandenen Konfigurationspakete bearbeiten möchten, wählen Sie das Konfigurationspaket aus und klicken Sie auf **Bearbeiten**.

Ändern des StyleBook eines Konfigurationspakets

Manchmal müssen Sie das StyleBook aktualisieren, um Funktionen hinzuzufügen oder ein Problem zu beheben. Wenn Sie bereits Konfigurationspakete mit dem alten StyleBook erstellt haben, möchten Sie diese möglicherweise aktualisieren, um das neue aktualisierte StyleBook zu verwenden. Um ein neues StyleBook zu verwenden, ändern Sie das vorhandene StyleBook des Konfigurationspakets.

Betrachten Sie ein Beispiel für ein **StyleBook-Beispiel-lb**, das eine grundlegende Load Balancer-Konfiguration auf einer ADC-Instanz bereitstellt. Und Sie erstellen ein Konfigurationspaket CP1 aus diesem StyleBook.

Wenn Sie Monitore mit der grundlegenden Load Balancer-Konfiguration konfigurieren möchten, benötigen Sie ein neues StyleBook. Erstellen Sie daher **beispiel-lb-mon** StyleBook, das die Möglichkeit bietet, Monitore zusammen mit der grundlegenden Load Balancer-Konfiguration zu konfigurieren.

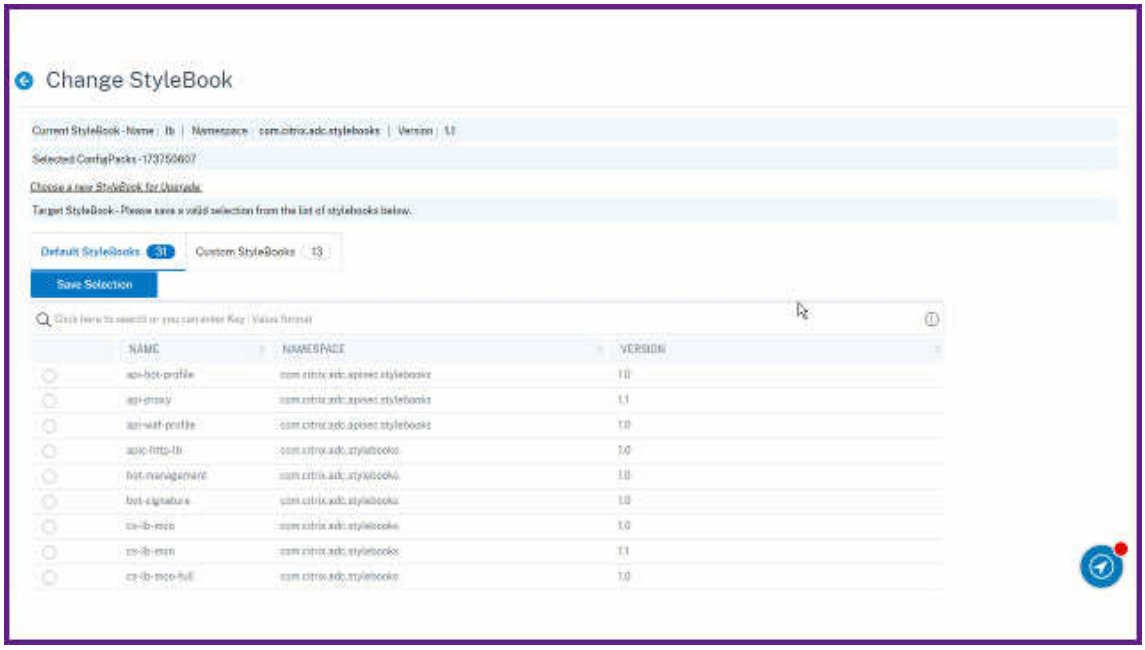
Nachdem Sie ein StyleBook erstellt haben, aktualisieren Sie das vorhandene Konfigurationspaket CP1, um einige Monitore hinzuzufügen. Führen Sie dazu folgende Schritte aus:

1. Navigieren Sie zu **Anwendungen > StyleBooks > Konfigurationen**.
2. Wählen Sie das Konfigurationspaket aus, für das Sie das StyleBook ändern möchten.

   In diesem Beispiel wählen Sie CP1 aus der Liste aus.
3. Klicken Sie auf **StyleBook ändern**.
4. Wählen Sie das gewünschte StyleBook aus der Liste aus. Klicken Sie dann auf " **Auswahl speichern**".
5. Klicken Sie auf **Ändern**.

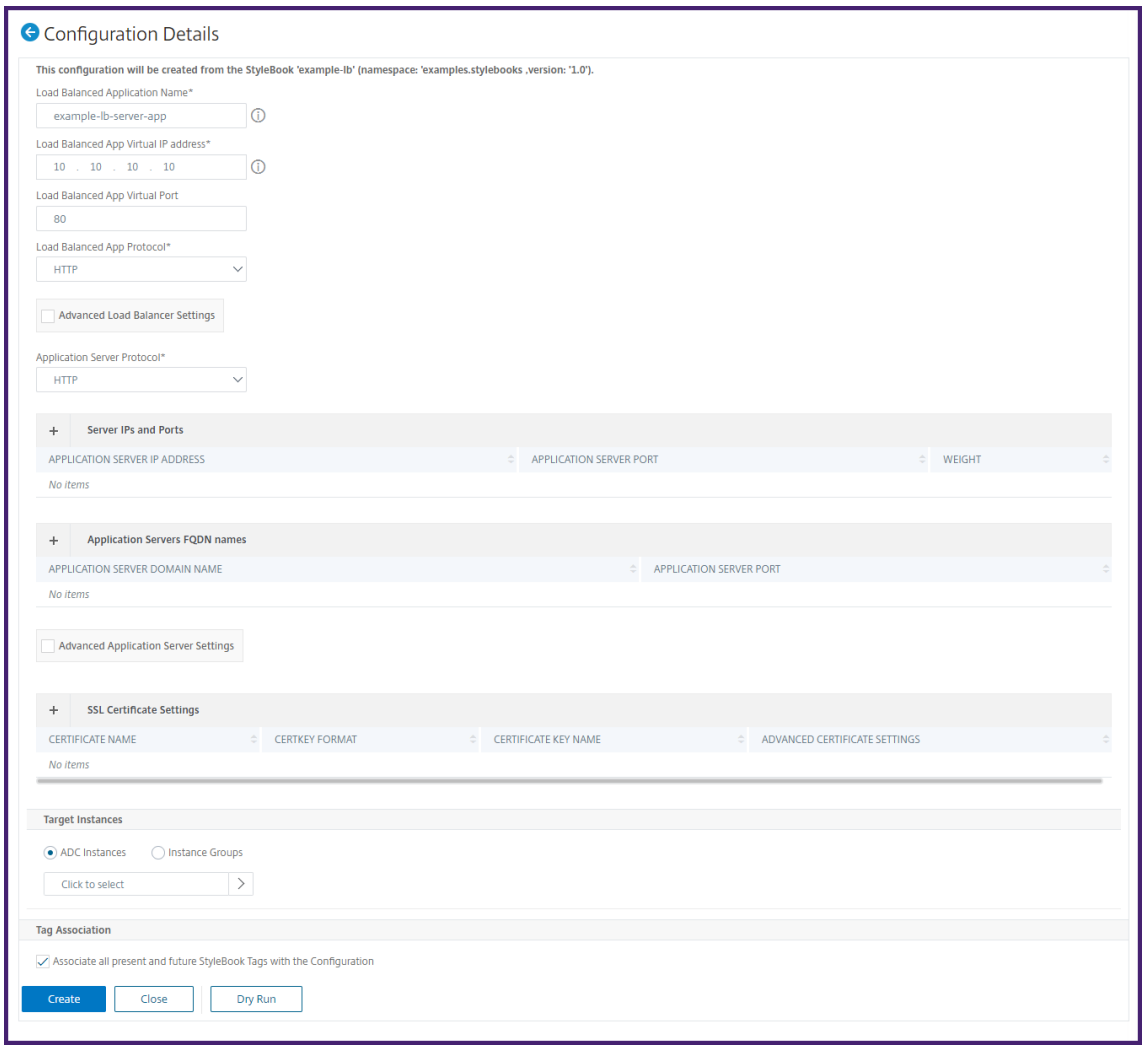
   In diesem Beispiel wählen Sie **example-lb-mon** aus der Liste aus.

   Wenn Sie das StyleBook eines Konfigurationspakets ändern, haben die Parameter im neuen StyleBook möglicherweise eine andere Struktur als das vorhandene StyleBook. Wenn die Parameterstruktur dem vorherigen StyleBook ähnelt, werden die Werte der Parameter automatisch in den jeweiligen Feldern beibehalten. Andernfalls werden nur Parameter übertragen, die die gleiche Struktur zwischen den beiden StyleBooks haben. Zum Beispiel derselbe Parametername, Typ, übergeordnetes Parameterelement und vieles mehr.

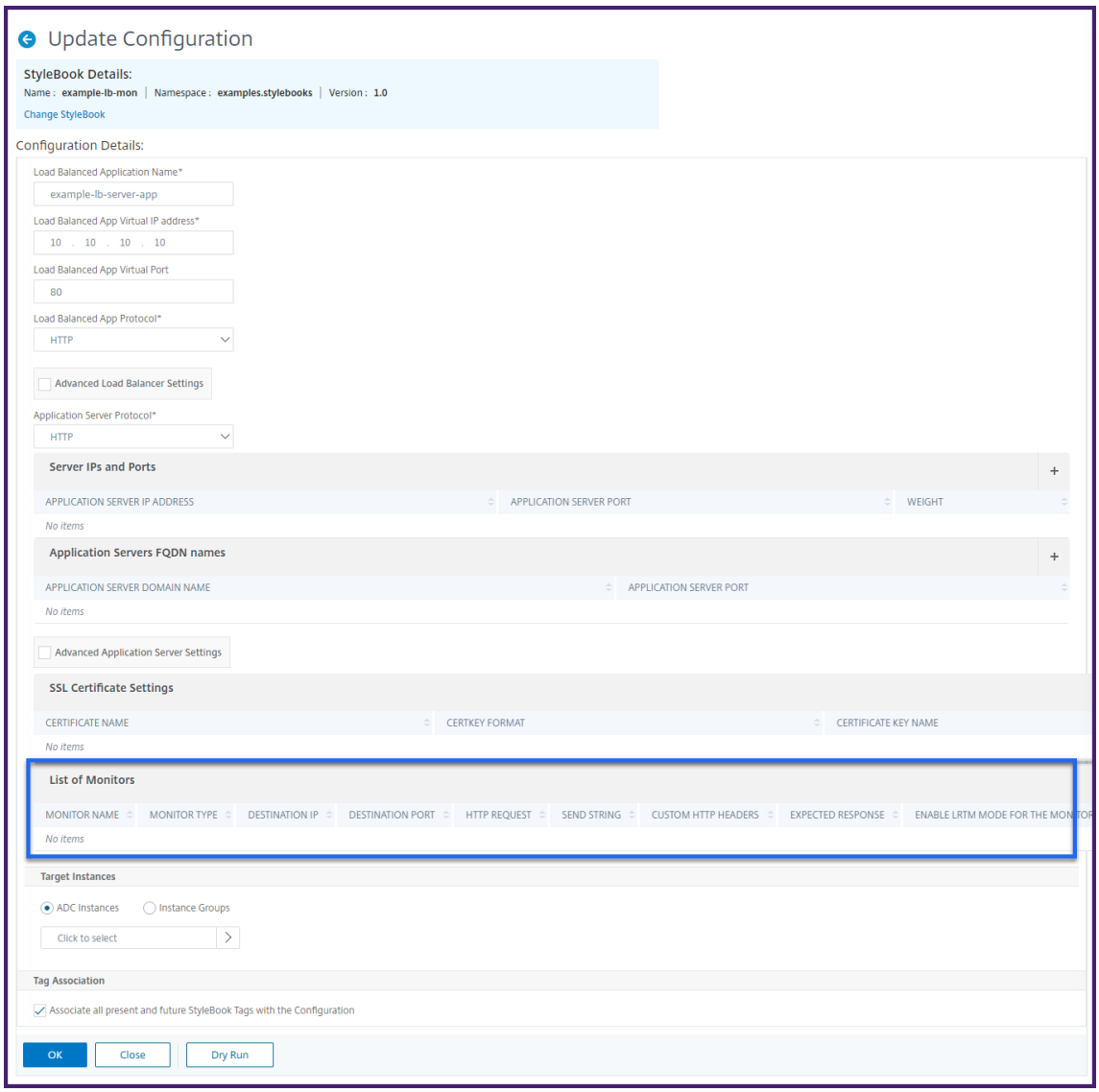


Wenn neue erforderliche Parameter im neuen StyleBook hinzugefügt werden, müssen Sie nach dem Ändern des StyleBook die Werte für solche Parameter manuell angeben.

In diesem Beispiel lauten die Parameter, die auf der Konfigurationsseite für das **Beispiel-lb** StyleBook angezeigt werden:



Die Parameter, die auf der Konfigurationsseite für das neue **Beispiel-LB-Mon StyleBook** angezeigt werden, lauten wie folgt:



In diesem Fall behalten die StyleBooks die älteren Werte für die grundlegende Load Balancer-Konfiguration bei, da das neue StyleBook vorhandene Parameter nicht geändert hat. Und es fügt nur die neuen Parameter hinzu. Geben Sie für Monitorparameter manuell die erforderlichen Werte an.

6. Überprüfen Sie in **Target Instanzen** die ausgewählten Instanzen und aktualisieren Sie die Liste bei Bedarf.
7. Klicken Sie auf **Dry Run**.

   Auf der Seite " **Objekte** " werden die Objekte angezeigt, die erstellt, geändert oder aus den Citrix ADC-Instanzen entfernt werden.
8. Klicken Sie auf **OK**.

   Auf der Seite **StyleBook > Configurations** wird in der Spalte **StyleBook Name** der neue

StyleBook-Name für das ausgewählte Konfigurationspaket angezeigt. In diesem Fall wird **Beispiel-lb-mon**angezeigt.

Ändern des StyleBook mit mehreren Konfigurationspaketen

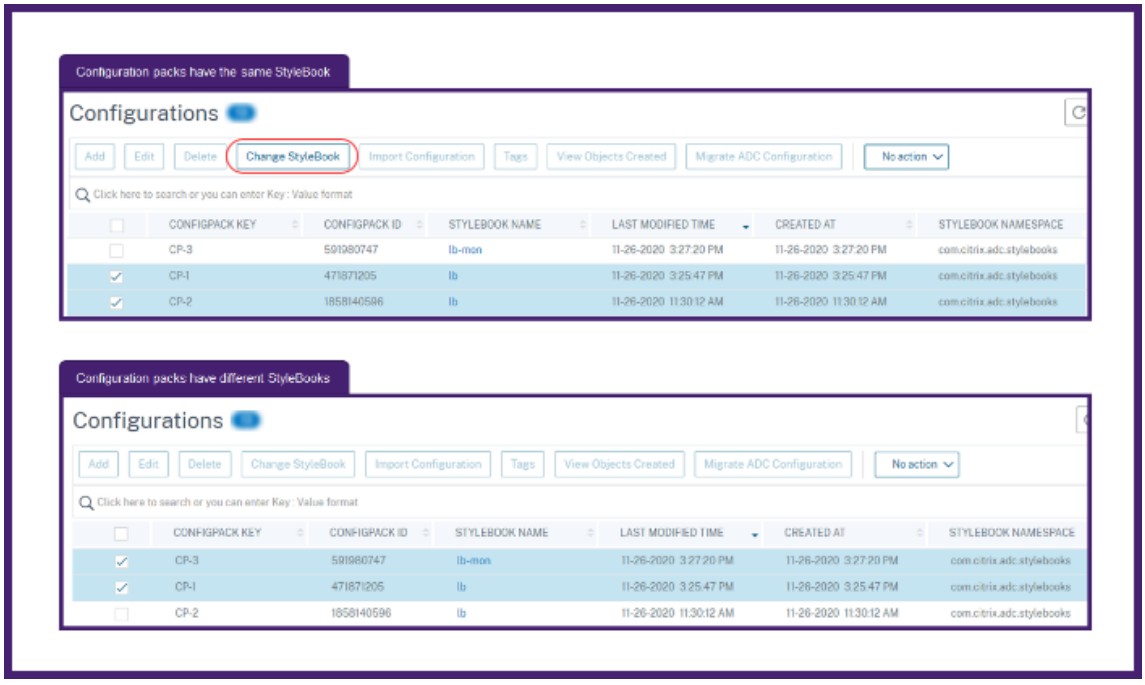
Wenn Sie ein vorhandenes StyleBook mit mehreren Konfigurationspaketen ändern, führen Sie die folgenden Schritte aus:

1. Importieren Sie ein neues StyleBook in ADM.

   In der Regel hat das neue StyleBook den gleichen Namen und den gleichen Namespace mit einer höheren Version als das vorhandene StyleBook. Sie können diesen Schritt jedoch überspringen, wenn der Name, der Namensraum oder die Version unterschiedlich sind.

2. Ändern Sie das StyleBook für die Konfigurationspakete, die mit dem vorhandenen StyleBook verknüpft sind.

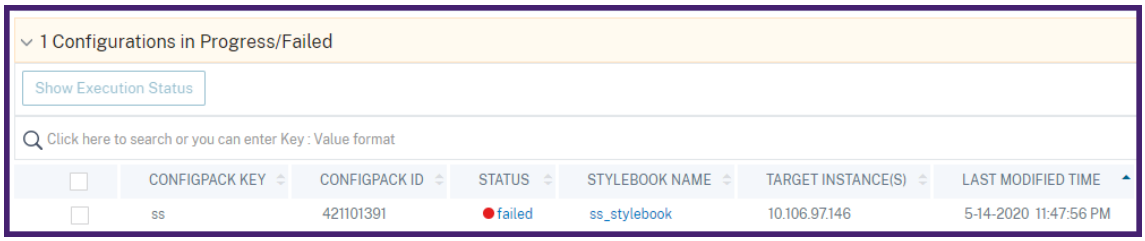
   Sie können **StyleBook ändern** nur auswählen, wenn die ausgewählten Konfigurationspakete mit demselben StyleBook verknüpft sind.



   Für die ausgewählten Konfigurationspakete ändert das ADM erfolgreich das StyleBook, wenn die folgenden Bedingungen erfüllt sind:

   - Alle Konfigurationsparameter des vorhandenen StyleBook müssen im ausgewählten StyleBook enthalten sein.
   - Die neuen Parameter aus dem ausgewählten StyleBook sind optional.

Um den Fortschritt der ausgewählten Konfigurationspakete anzuzeigen, wählen Sie **Konfigurationen in Fortschritt/Fehlgeschlagen** auf der Seite **Konfigurationen** aus.



3. Entfernen Sie das alte StyleBook aus ADM, sobald alle Konfigurationspakete an das neue StyleBook gebunden sind.

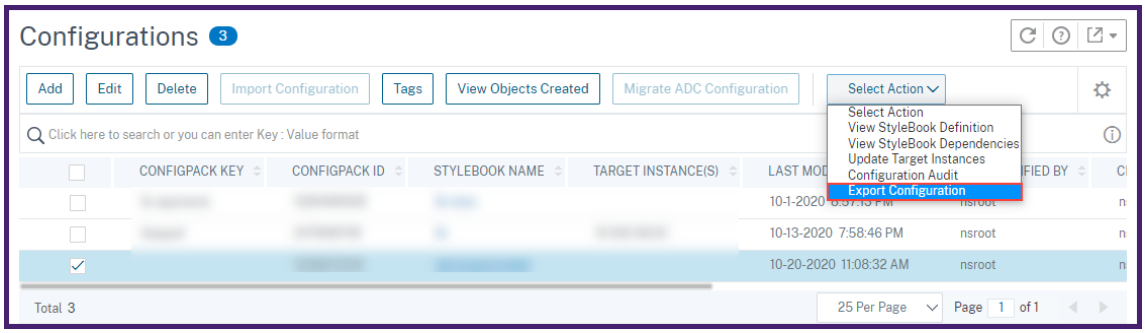
Exportieren oder Importieren von Konfigurations

Sie können ein Konfigurationspaket wie StyleBooks exportieren oder importieren. Mit dieser Funktion können Sie die StyleBook-Konfiguration problemlos mit einem anderen ADM-Server teilen. Wenn Sie ein Konfigurationspaket exportieren, wird ein `tgz` oder `zip` Paket auf Ihren lokalen Computer heruntergeladen. Dieses Bundle enthält eine JSON-Datei mit allen in einem Konfigurationspaket definierten Parameter.

Export-Konfiguration

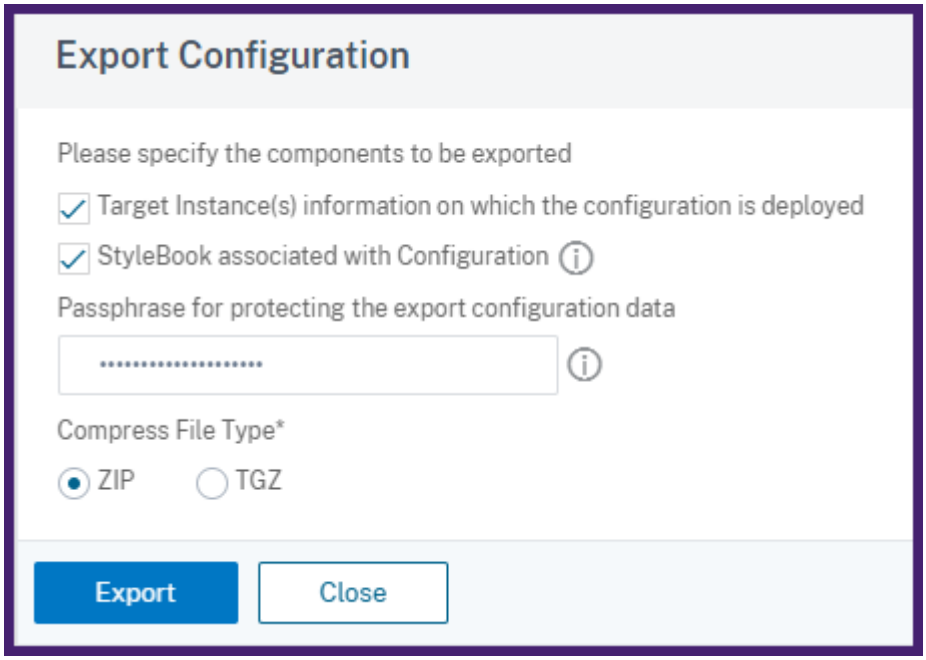
Führen Sie Folgendes aus, um ein Konfigurationspaket zu exportieren:

1. Navigieren Sie zu **Anwendungen > StyleBooks > Konfigurationen**.
2. Wählen Sie ein Konfigurationspaket aus, das Sie exportieren möchten.
3. **Wählen Sie unter Aktion**auswählen die Option **Konfiguration exportieren**aus.



4. Geben Sie im Bereich **Exportkonfiguration** Folgendes an:
   - **Informationen zu Zielinstanzen, für die die Konfiguration bereitgestellt wird**: Wählen Sie diese Option aus, um die Informationen der Zielinstanzen in das Exportpaket aufzunehmen.

- **Mit Konfiguration verknüpftes StyleBook**: Wählen Sie diese Option aus, um das StyleBook in das Export-Bundle aufzunehmen.
- **Passphrase zum Schutz der Exportkonfigurationsdaten**: Geben Sie eine Passphrase an, um das Export-Bundle zu verschlüsseln. Diese Passphrase sichert die sensiblen Daten eines Konfigurationspakets.
- **Dateityp komprimieren**: Wählen Sie entweder **ZIP-** oder **TGZ-Dateityp** aus.



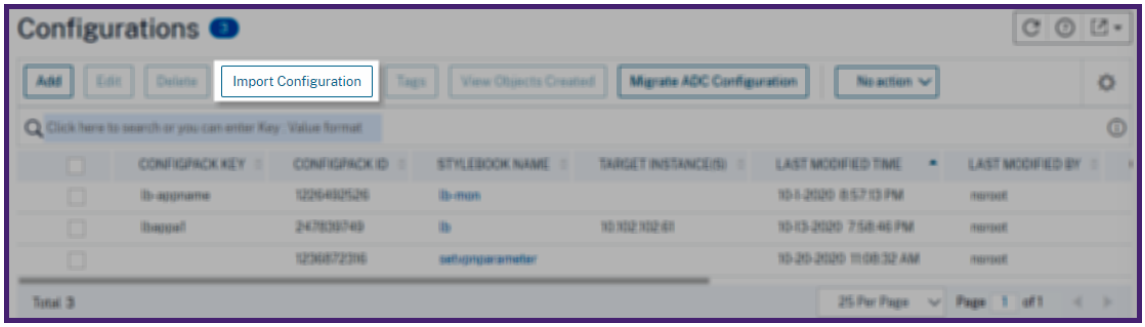
5. Klicken Sie auf **Exportieren**.

   Speichern Sie das Export-Bundle auf Ihrem lokalen Computer.

Konfiguration importieren

Sie können ein Konfigurationspaket von Ihrem lokalen Computer auf einen anderen ADM-Server importieren. Um ein Konfigurationspaket zu importieren, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Anwendungen > StyleBooks > Konfigurationen**.
2. Wählen Sie **Konfiguration importieren**aus.



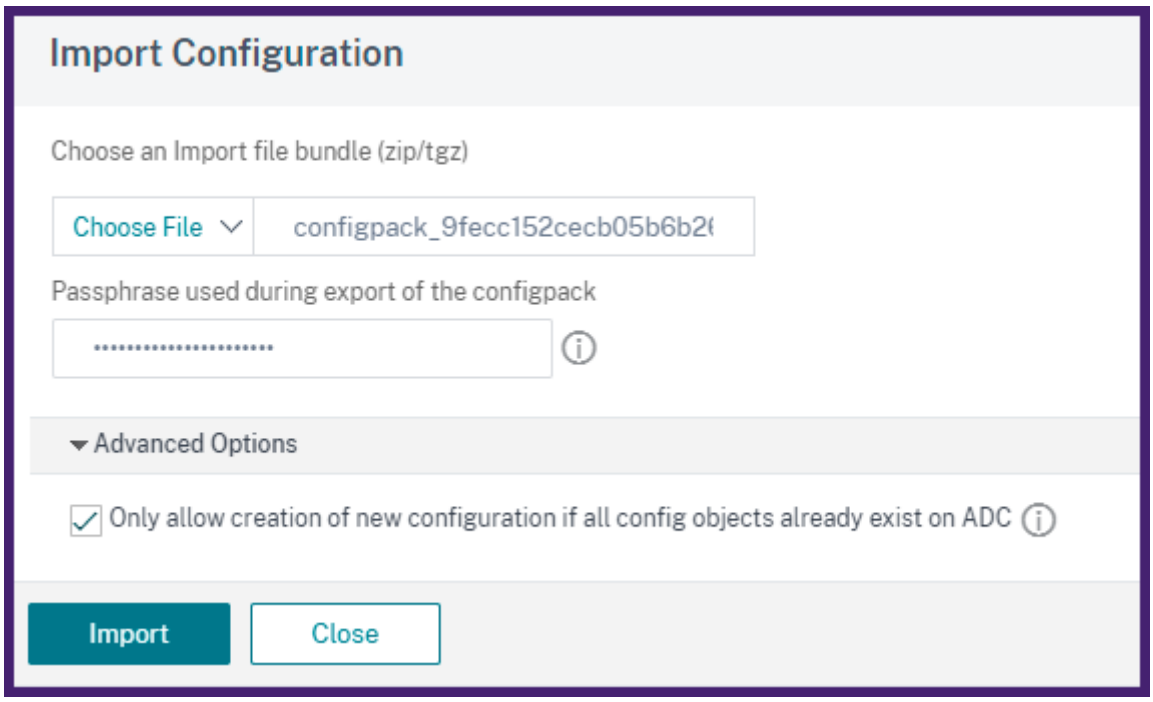
3. Wählen Sie das Importdatei-Paket von Ihrem Computer aus.
4. Verwenden Sie die Passphrase, die Sie beim Export angegeben haben.
5. Optional können Sie in Erweiterte Optionen die Option **Erstellen einer neuen Konfiguration nur zulassen, wenn alle Konfigurationsobjekte bereits auf ADC vorhanden sind**.

   Diese Option ändert nicht die Objekte, die bereits auf der ADC-Instanz erstellt wurden.

   Bedenken Sie, dass Sie dieselbe ADC-Instanz auf zwei ADM-Servern hinzugefügt haben. Und Sie möchten ein Konfigurationspaket von einem ADM-Server auf einen anderen Server migrieren. Verwenden Sie diese Option, um ein Konfigurationspaket zu importieren, ohne seine Konfigurationsobjekte auf einer ADC-Instanz zu ändern.

   > **Wichtig**
   >
   > Um diese Option zu verwenden, stellen Sie sicher, dass das angegebene Konfigurationspaket die Informationen zu Zielinstanzen enthält. Siehe Export-Konfiguration.
   >
   > Diese Option migriert die Konfiguration nur, wenn alle Objekte auf der Zielinstanz vorhanden sind.

6. Klicken Sie auf **Importieren**.



Wenn Sie ein Konfigurationspaket importieren, überprüft der ADM Folgendes:

- **Assoziiertes StyleBook**: Wenn das zugehörige StyleBook nicht im ADM enthalten ist, importiert es das StyleBook zusammen mit dem Konfigurationspaket.
- **Zielinstanzen**: Suchen Sie nach Zielinstanzen und stellt die Konfiguration auf den angegebenen Zielinstanzen bereit. Wenn die genannten ADC-Instanzen im ADM nicht vorhanden sind, wird das Konfigurationspaket ohne Zielinstanzen importiert.
- **Quell-ADM**: Wenn Sie ein Konfigurationspaket auf demselben ADM-Server importieren, aktualisiert das ausgewählte Bundle das vorhandene Konfigurationspaket.

Erstellen Sie Ihre StyleBooks

Der vollständige Inhalt von **Beispiel-lb** StyleBook wird wie folgt als Referenz bereitgestellt:

```
1 name: example-lb
2 namespace: examples.stylebooks
3 version: ”1.0”
4 display-name: Basic Load Balancer App
5 description: This is an example StyleBook that creates a load balancer
     application
6 schema-version: ”1.0”
7 import-stylebooks:
8   -
```



```
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: ”1.0”
parameters-default-sources:
  - stlb::lb
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb
       configuration objects
    properties-default-sources:
      - $parameters
<!--NeedCopy-->
```

Der vollständige Inhalt von **beispiel-lb-mon** StyleBook wird wie folgt als Referenz bereitgestellt:

```
name: example-lb-mon
namespace: examples.stylebooks
version: ”1.0”
description: This is an example StyleBook that creates a load balancer
   application with monitors
display-name: Basic Load Balancer App with Monitors
schema-version: ”1.0”
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: ”10.5”
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: ”1.0”
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: ”1.0”
parameters-default-sources:
  - stlb::lb
parameters:
  -
    name: monitors
    label: ”List of Monitors”
```



```
26      description: "List of Monitors to monitor Application Servers"
27      type: cmtypes::monitor[]
28  substitutions:
29    mon-name(appname, monname): $appname + "-mon-" + $monname
30  components:
31    -
32      name: lb-comp
33      type: stlb::lb
34      description: Uses the default lb StyleBook to build the typical lb
           configuration objects
35      properties-default-sources:
36        - $parameters
37    -
38      name: monitors-comp
39      type: cmtypes::monitor
40      condition: $parameters.monitors
41      repeat: $parameters.monitors
42      repeat-item: mon
43      repeat-index: ndx
44      description: Builds a list of Citrix ADC monitor objects and binds
           them to the servicegroup of this LB config
45      properties-default-sources:
46        - $mon
47      properties:
48          monitorname: $substitutions.mon-name($parameters.lb-appname,
              $mon.monitorname)
49      components:
50        -
51          name: monitor-svcg-binding-comp
52          condition:  $parameters.svc-servers
53          type: ns::servicegroup_lbmonitor_binding
54          properties:
55            servicegroupname: $components.lb-comp.outputs.servicegroup.
                properties.servicegroupname
56            monitor_name: $parent.properties.monitorname
57  <!--NeedCopy-->
```

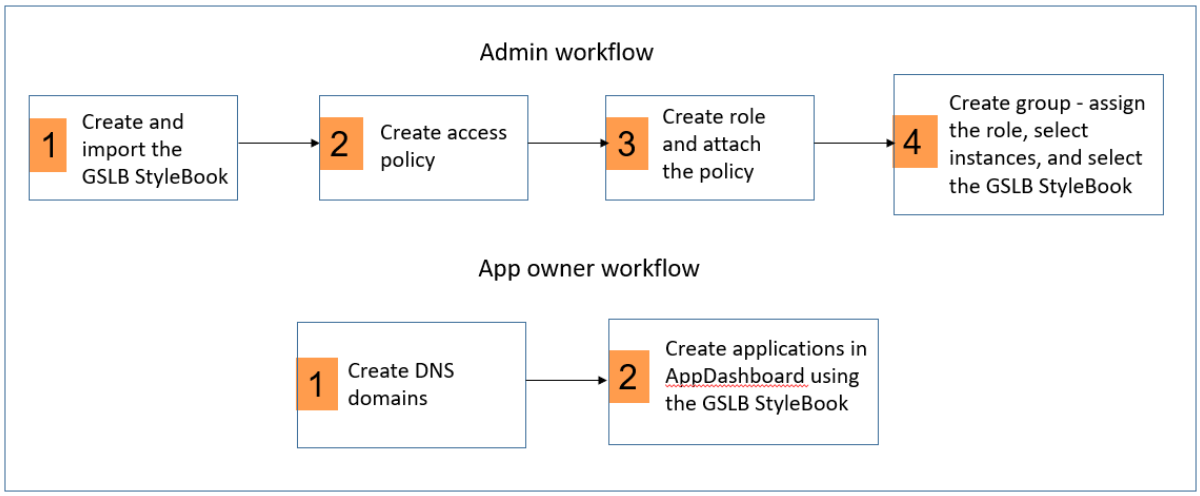
Bereitstellen von GSLB-Konfigurationen mithilfe von DNS-Domänennamen

April 28, 2021

Mit den neuen RBAC-Erweiterungen in Citrix Application Delivery Management (ADM) können nur autorisierte Anwendungsbesitzer eigene DNS-Domänen in Citrix ADM erstellen und verwalten. Sie können nun die App-Besitzer ermächtigen, GSLB-Konfigurationen aus den DNS-Domänen zu erstellen, die sie besitzen, indem Sie bestimmte StyleBooks verwenden. Wenn der ausgewählte DNS-Domänenname dem Benutzer gehört, kann er beim Erstellen von GSLB-Konfigurationen mithilfe von GSLB StyleBooks im Citrix ADM Anwendungs-Dashboard verwendet werden.Citrix ADM gibt es zwei Workflows zum Konfigurieren von GSLB-Konfigurationen.

1. **Workflow für die Administratoren**. Richten Sie die RBAC-Umgebung in Citrix ADM ein. Das heißt, um GSLB StyleBooks zu erstellen und zu importieren, müssen Sie Benutzergruppen, Richtlinien und Rollen erstellen und der Gruppe Benutzer zuweisen. Als Administrator müssen Sie diesen Workflow ausführen.
2. **Workflow für die Anwendungseigentümer**. Anwendungsbesitzer müssen GSLB-Konfigurationen unter Verwendung von Domänennamen erstellen, die ihnen gehören.

Das folgende Flussdiagramm zeigt beide Workflows:



Workflow für die Administratoren

Als Administrator besteht Ihr Workflow zum Erstellen einer RBAC-Umgebung in Citrix ADM aus den folgenden Schritten:

Erstellen Sie zunächst ein StyleBook, um GSLB-Konfigurationen auf den Citrix ADC-Instanzen bereitzustellen. Dieses Dokument enthält eine Beispiel-YAML-Inhalt, um Ihnen zu helfen, Ihr eigenes StyleBook zu erstellen -Erstellen Sie Ihr StyleBook.

Weitere Informationen zum Erstellen benutzerdefinierter StyleBooks finden Sie unterErstellen und Verwenden von benutzerdefinierten StyleBooks.

> **Hinweis**
>
> Citrix ADM unterstützt ein neues Konstrukt in StyleBooks namens allowed-dynamic-values. Mit diesem Konstrukt kann der Benutzer die DNS-Domänenwerte auflisten und auswählen, die in Citrix ADM vorhanden sind, um den Parameter domain-name im StyleBook in Citrix ADM GUI automatisch aufzufüllen.

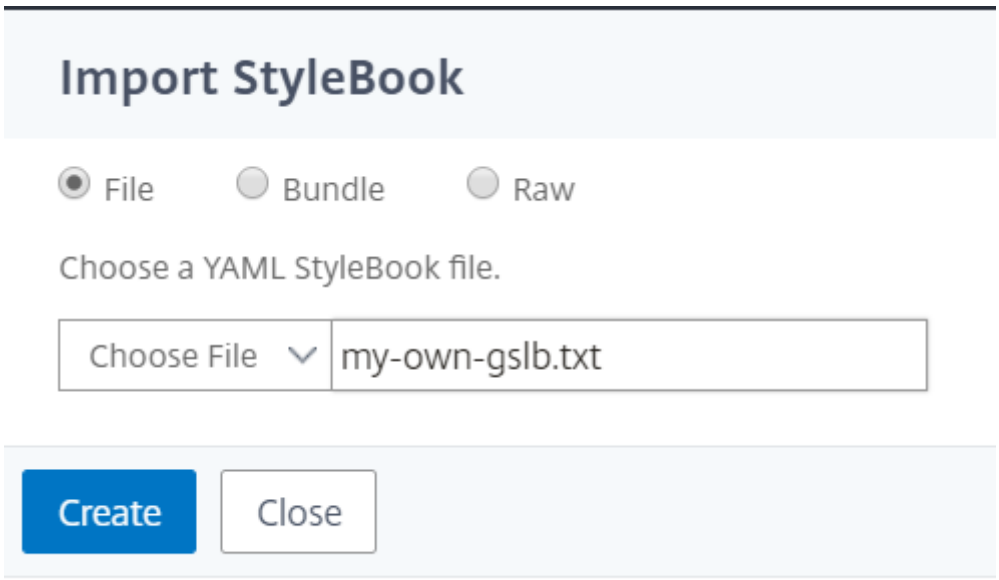
Ein Beispiel-Parameterabschnitt domain-name wird für Ihre Referenz bereitgestellt.

Der hier verwendete Parameter domain-name ist nur ein Beispiel. Der Parameter kann in Ihrem benutzerdefinierten StyleBook unterschiedlich sein.

```
-
  name: domain-name
   label: DNS Domain Name
   description: GSLB DNS Domain Name
   type: string
   required: true
   allowed-dynamic-values:
      source: local
      resource-type: dns_domain_entry
<!--NeedCopy-->
```

> **Hinweis**
>
> Derzeit in Citrix ADM wird das Konstrukt allowed-dynamic values in keinem der Standard-StyleBooks verwendet. Erstellen Sie ein neues benutzerdefiniertes GSLB StyleBook mit dem Standard-GSLB StyleBook. Ersetzen Sie das Teil für den Domänennamen-Parameter durch das oben angegebene Beispiel. Sie können einen beliebigen Texteditor verwenden, um neue StyleBooks zu erstellen.

1. Melden Sie sich bei Citrix ADM als Administrator an.
2. Navigieren Sie zu **Anwendungen** > **Konfigurationen** > **StyleBooks**.
3. Klicken Sie auf **Neues StyleBook importieren**, und laden Sie das neue GSLB StyleBook in Citrix ADM hoch.



Weitere Informationen zum Importieren von StyleBooks in Citrix ADM finden Sie unterBenutzerdefinierte StyleBooks verwenden.

4. Navigieren Sie zu **System** > **Benutzer** > **Richtlinien**, und klicken Sie auf **Hinzufügen**, um eine Zugriffsrichtlinie für die Anwendungseigentümer einzurichten, wie unten dargestellt.

   Citrix empfiehlt, eine Zugriffsrichtlinie zu erstellen, um sicherzustellen, dass die Anwendungseigentümer den von Ihnen festgelegten RBAC-Regeln nicht umgehen.

5. Geben Sie einen Namen für die Richtlinie und eine kurze Beschreibung ein. Stellen Sie im Abschnitt Berechtigungen sicher, dass die folgenden Berechtigungen zum Ansichtsbearbeiten zwingend überprüft werden.

   a) Anwendungen > Dashboard

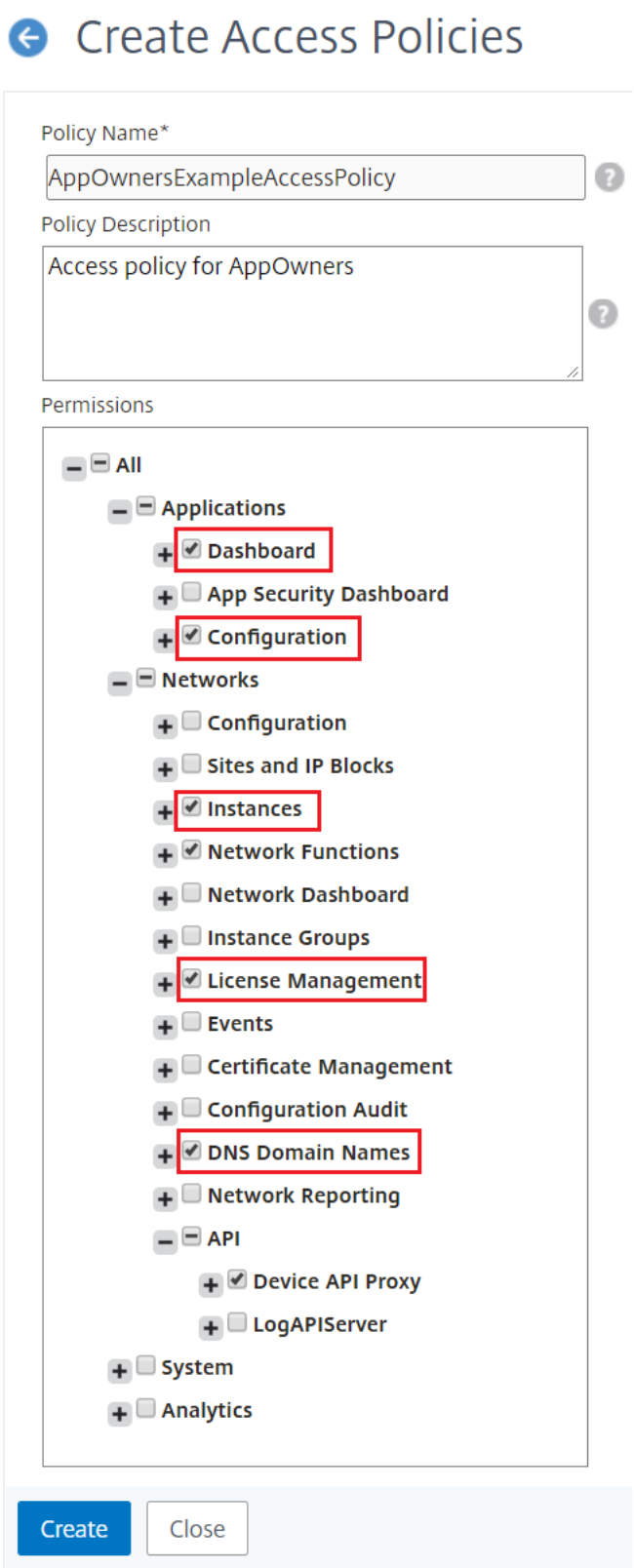
   b) Anwendungen > Konfigurationen

   c) Netzwerke > Instanzen

   d) Netzwerke > Lizenzverwaltung

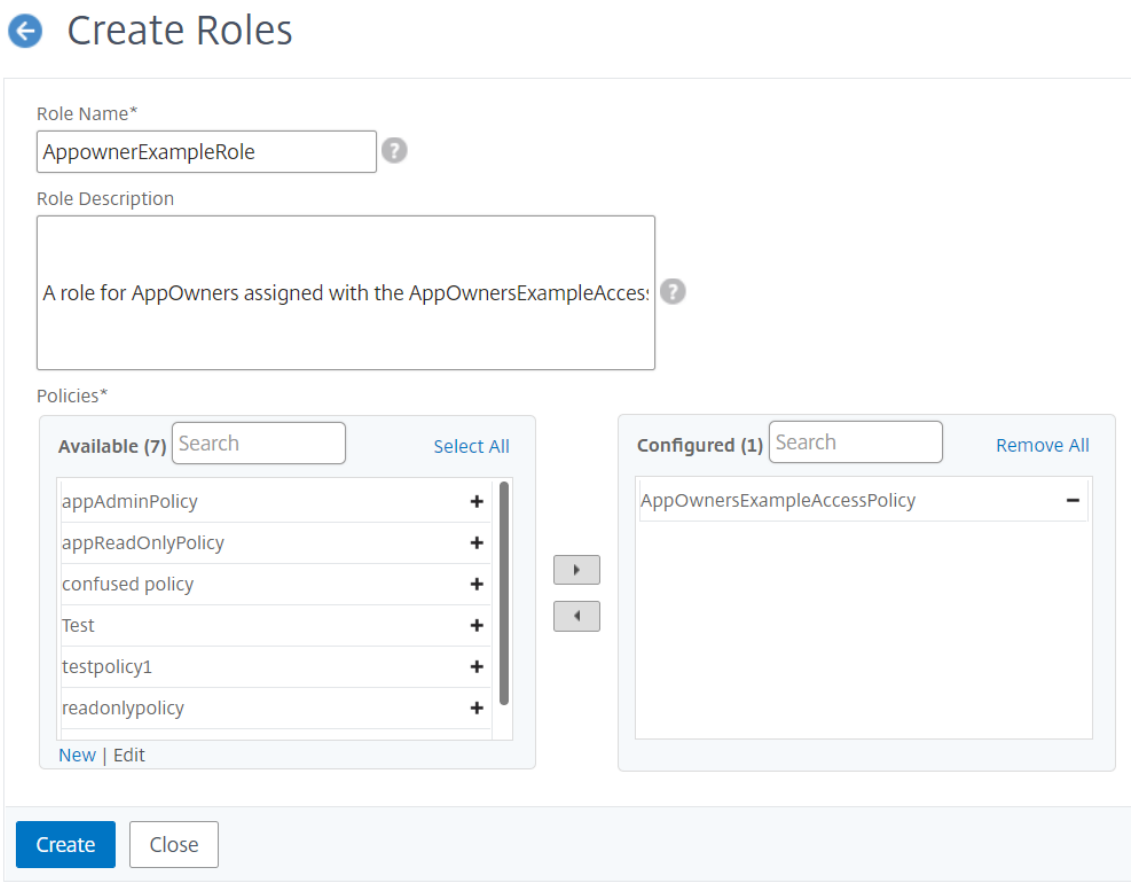
   e) Netzwerke > DNS-Domänennamen

   Sie können ggf. weitere Berechtigungen bereitstellen und auf **Erstellen**klicken.

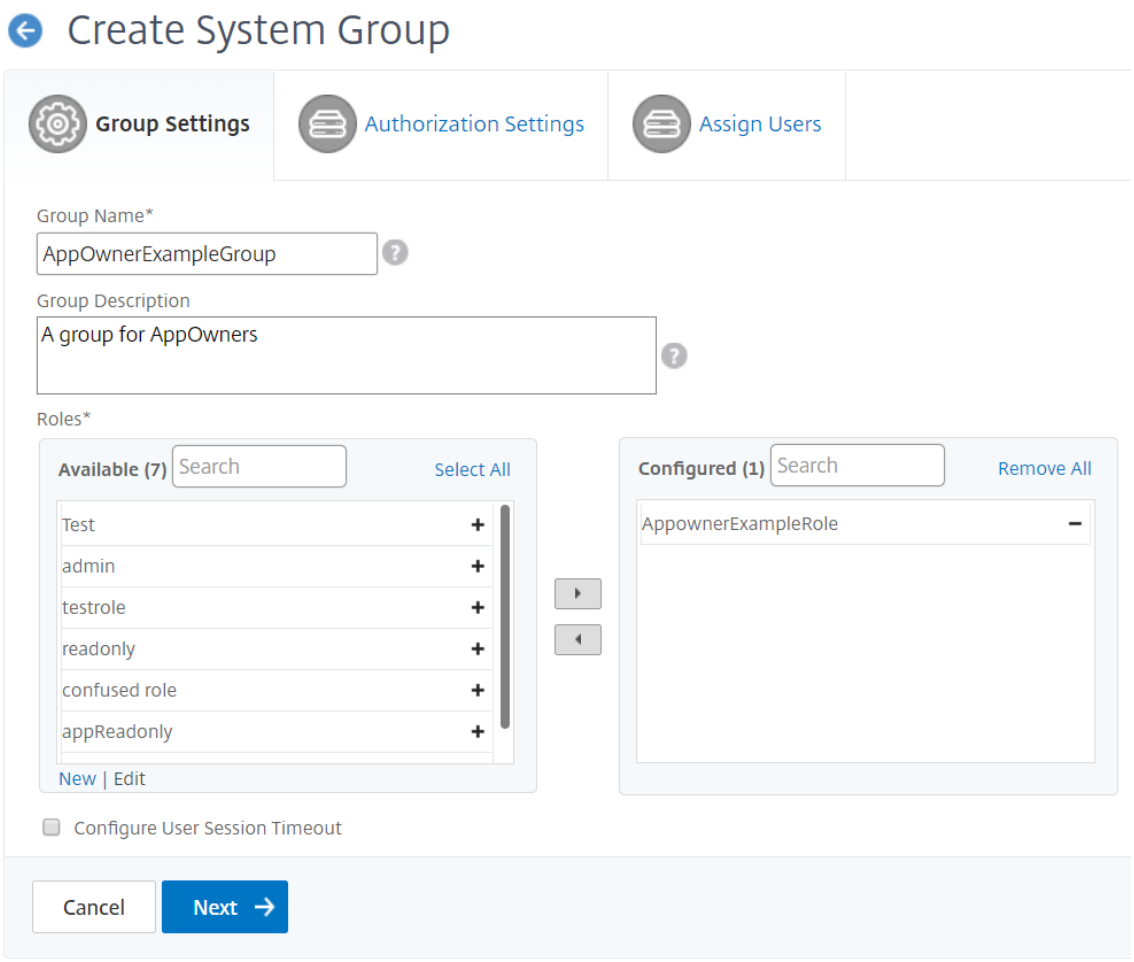


6. Navigieren Sie zu **System** > **Benutzer** > **Rollen**, erstellen Sie eine Rolle und weisen Sie die im vorherigen Schritt erstellte Richtlinie zu.

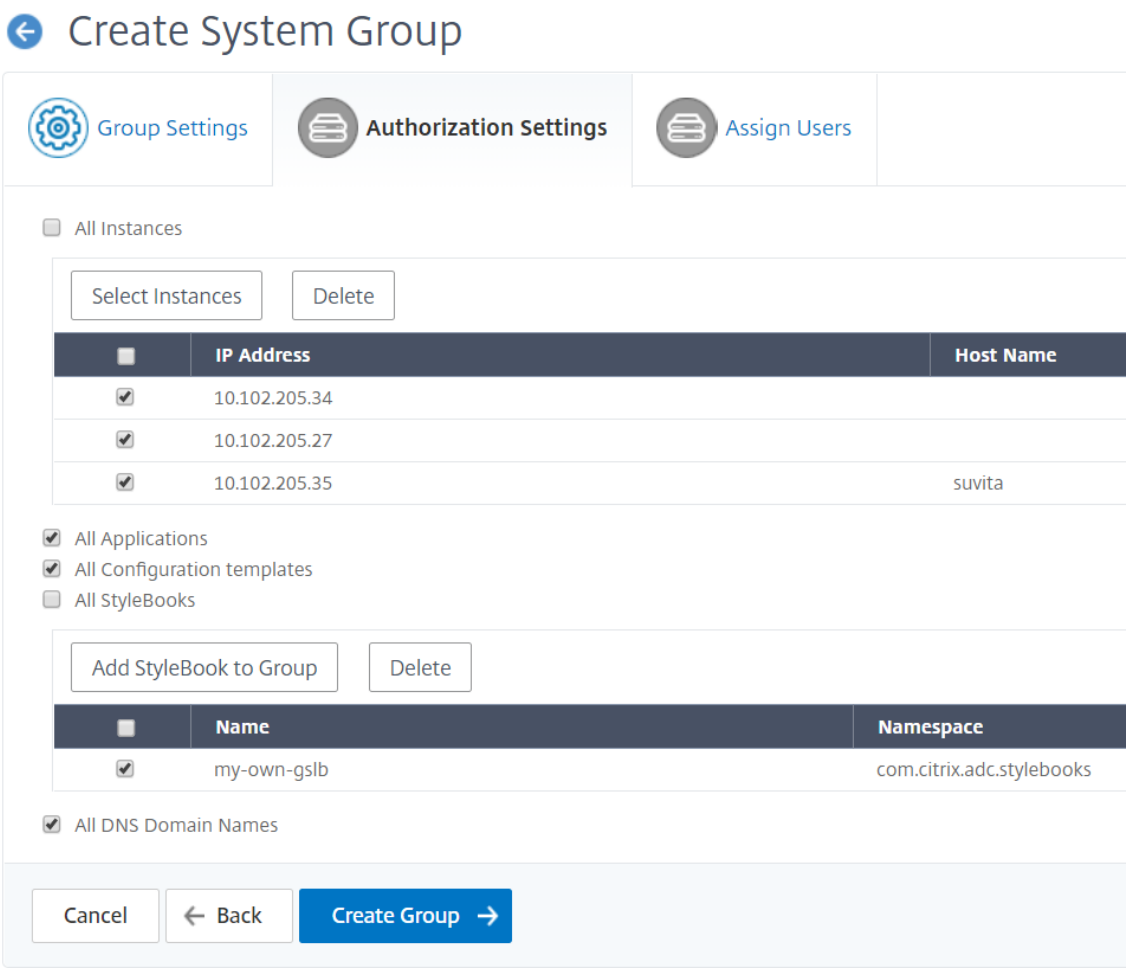
7. Geben Sie einen Namen für die Rolle ein, und geben Sie eine kurze Beschreibung an. Wählen Sie im Abschnitt Richtlinien die Option **AppOwnerExampleAccessPolicy**aus.



8. Navigieren Sie zu **System** > **Benutzer** > **Gruppen**, erstellen Sie eine Gruppe, und ordnen Sie die im vorherigen Schritt erstellte Rolle zu.
9. Geben Sie einen Namen und eine Beschreibung ein, und wählen Sie im Abschnitt Rollen die Option **AppOwnerExamplerole**aus.



10. Klicken Sie auf **Weiter**.
11. Wählen Sie auf der Registerkarte **Autorisierungseinstellungen** die Citrix ADC-Instanzen, auf die der Anwendungseigentümer Zugriff hat, und das neue GSLB-StyleBook aus.

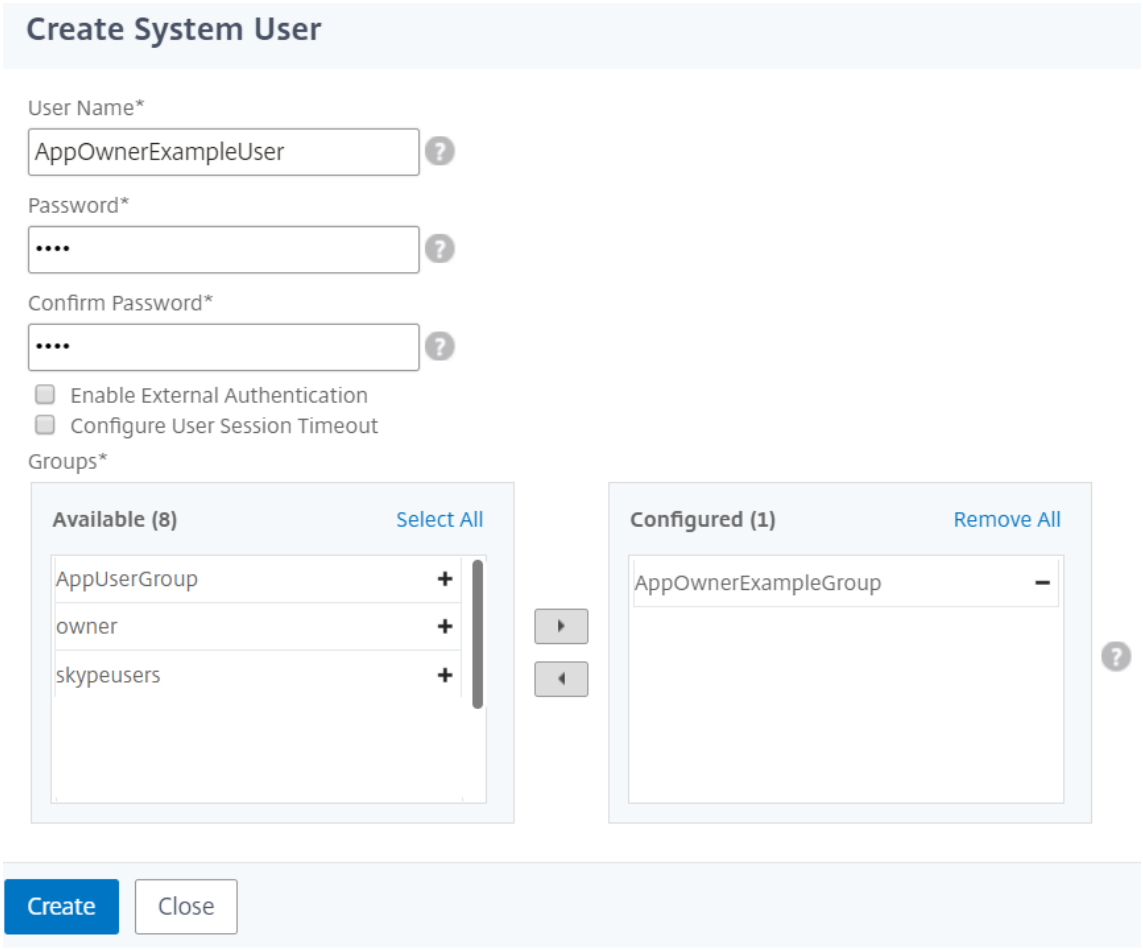


Wiederholen Sie diesen Schritt, um so viele Benutzergruppen zu erstellen, wie Sie in Ihrer Organisation benötigen. Klicken Sie auf **Gruppe erstellen**.

12. Erstellen Sie einen Systembenutzer und weisen Sie den Benutzer einer Benutzergruppe zu. Dieses Dokument bezieht sich nur auf lokal erstellte Benutzer. Sie müssen keine Benutzer in Benutzergruppen erstellen, wenn Citrix ADM für die Verwendung externer Authentifizierung (z. B. LDAP) eingerichtet ist. Die Benutzerzuordnung zu Gruppen wird aus dem externen Authentifizierungsverzeichnis abgerufen.

    a) Navigieren Sie zu **System** > **Benutzer** > **Benutzer**.

    b) Geben Sie einen Benutzernamen und ein Kennwort für den Systembenutzer ein, und weisen Sie den Benutzer der Gruppe zu.



> **Hinweis**
>
> Schritt 12 ist optional und ist nicht erforderlich, wenn externe Authentifizierung wie LDAP verwendet wird.

Citrix ADM REST-API für Admin-Workflow

REST-API für die Anmeldung bei Citrix ADM

```
URL: http: //<MAS_IP>/nitro/v2/config/login
HTTPMETHOD: POST

Body Payload:
{

  ”login”: {

    ”username”: ”<USER_NAME>”,
    ”password”: ”<PASSWORD>”,
```



```
    "session_timeout": 1800
   }

 }


The response results in a session cookie header, that can be sent with
   the rest of the API requests below.

Set-Cookie: SESSID=##
   ED31F7C886E248CCDCA8F0E0AD2AA511ACCC5F46C48D6D2BCAA719A9DE62;path=/;
   secure;HttpOnly
<!--NeedCopy-->
```

REST-API zum Erstellen einer Zugriffsrichtlinie

```
URL: https://<MAS_IP>/nitro/v2/config/rba_policy
HTTP METHOD: POST

{

  "rba_policy": {

    "name": " AppOwnerAccessPolicy",
    "description": " ExampleCompany AppOwner Access Policy",
    "tenant_id": "7c12ec97-1472-4096-97e7-a5acb453cc5c",
    "statement": [
      {

        "access_type": true,
        "resource_type": "application",
        "operation_name": "add",
        "dependent_resources": "mail_profile,slack_profile,smtp_server,
           app_category"
       }
 ,
      {

        "access_type": true,
        "resource_type": "application",
        "operation_name": "get",
        "dependent_resources": "download,smtp_server,ns_vserver_license
           ,app_category,app_summary,app_health_dashboard_details,
```



```
                haproxy_frontend,haproxy_backend,haproxy_frontend_stats"
26          }
27    ,
28          {
29
30            "access_type": true,
31            "resource_type": "si_app_unit",
32            "operation_name": "get",
33            "dependent_resources": "download,smtp_server,app_summary,
                  si_app_summary,si_device,security_app_dashboard_details,
                  si_geo_location,si_safety_app_firewall,si_safety_overview,
                  si_safety_security_check,si_safety_system_security,
                  si_safety_signature"
34          }
35    ,
36          {
37
38            "access_type": true,
39            "resource_type": "stylebooks",
40            "operation_name": "get",
41            "dependent_resources": "download,smtp_server,ns_vserver_license
                  "
42          }
43    ,
44          {
45
46            "access_type": true,
47            "resource_type": "stylebooks",
48            "operation_name": "add",
49            "dependent_resources": "mail_profile,slack_profile,smtp_server"
50          }
51    ,
52          {
53
54            "access_type": true,
55            "resource_type": "configpacks",
56            "operation_name": "get",
57            "dependent_resources": "download,smtp_server,stylebooks,
                  ns_vserver_license"
58          }
59    ,
60          {
61
62            "access_type": true,
63            "resource_type": "configpacks",
```



```
64          "operation_name": "add",
65          "dependent_resources": "mail_profile,slack_profile,smtp_server"
66         }
67  ,
68       {
69
70          "access_type": true,
71          "resource_type": "stylebooks_system_settings",
72          "operation_name": "get",
73          "dependent_resources": "download,smtp_server"
74         }
75  ,
76       {
77
78          "access_type": true,
79          "resource_type": "stylebooks_system_settings",
80          "operation_name": "add",
81          "dependent_resources": "mail_profile,slack_profile,smtp_server"
82         }
83  ,
84       {
85
86          "access_type": true,
87          "resource_type": "ns_crvserver",
88          "operation_name": "get",
89          "dependent_resources": "download,DeviceAPIProxy,smtp_server,
               perf_cache_redirection_report,poll_activity_status,
               ns_emon_poll_policy,lb_export_report"
90         }
91  ,
92       {
93
94          "access_type": true,
95          "resource_type": "ns_crvserver",
96          "operation_name": "add",
97          "dependent_resources": "DeviceAPIProxy,mail_profile,
               slack_profile,smtp_server,poll_activity_status,
               ns_emon_poll_policy,lb_export_report"
98         }
99  ,
100      {
101
102         "access_type": true,
103         "resource_type": "haproxy_frontend",
104         "operation_name": "get",
```



```
105           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  haproxy_backend,haproxy_server"
106         }
107   ,
108         {
109
110           "access_type": true,
111           "resource_type": "haproxy_frontend",
112           "operation_name": "add",
113           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server"
114         }
115   ,
116         {
117
118           "access_type": true,
119           "resource_type": "ns_server",
120           "operation_name": "get",
121           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  ns_emon_poll_policy,poll_activity_status,ns_server,
                  lb_export_report"
122         }
123   ,
124         {
125
126           "access_type": true,
127           "resource_type": "ns_server",
128           "operation_name": "add",
129           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,ns_emon_poll_policy,
                  poll_activity_status,lb_export_report"
130         }
131   ,
132         {
133
134           "access_type": true,
135           "resource_type": "ns_lbvserver",
136           "operation_name": "get",
137           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  perf_lb_vserver_report,ns_emon_poll_policy,
                  poll_activity_status,lb_export_report"
138         }
139   ,
140         {
141
```



```
142           "access_type": true,
143           "resource_type": "ns_lbvserver",
144           "operation_name": "add",
145           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,ns_emon_poll_policy,
                  poll_activity_status,lb_export_report"
146         }
147   ,
148         {
149
150           "access_type": true,
151           "resource_type": "ns_service",
152           "operation_name": "get",
153           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  ns_emon_poll_policy,poll_activity_status,
                  ns_visualizer_lb_bindings,lb_export_report"
154         }
155   ,
156         {
157
158           "access_type": true,
159           "resource_type": "ns_service",
160           "operation_name": "add",
161           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,ns_emon_poll_policy,
                  poll_activity_status,ns_visualizer_lb_bindings,
                  lb_export_report"
162         }
163   ,
164         {
165
166           "access_type": true,
167           "resource_type": "ns_servicegroup",
168           "operation_name": "get",
169           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  ns_emon_poll_policy,poll_activity_status,
                  ns_servicegroupmember_binding,ns_visualizer_lb_bindings,
                  lb_export_report"
170         }
171   ,
172         {
173
174           "access_type": true,
175           "resource_type": "ns_servicegroup",
176           "operation_name": "add",
```



```
177           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,ns_emon_poll_policy,
                  poll_activity_status,ns_servicegroupmember_binding,
                  ns_visualizer_lb_bindings,lb_export_report"
178         }
179   ,
180         {
181
182           "access_type": true,
183           "resource_type": "ns_authenticationvserver",
184           "operation_name": "get",
185           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  perf_authentication_report,poll_activity_status,
                  ns_emon_poll_policy,lb_export_report"
186         }
187   ,
188         {
189
190           "access_type": true,
191           "resource_type": "ns_authenticationvserver",
192           "operation_name": "add",
193           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,poll_activity_status,
                  ns_emon_poll_policy,lb_export_report"
194         }
195   ,
196         {
197
198           "access_type": true,
199           "resource_type": "syslog_messages",
200           "operation_name": "get",
201           "dependent_resources": "download,smtp_server"
202         }
203   ,
204         {
205
206           "access_type": true,
207           "resource_type": "ns_emon_poll_policy",
208           "operation_name": "get",
209           "dependent_resources": "download,poll_activity_status,
                  smtp_server"
210         }
211   ,
212         {
213
```



```
214           "access_type": true,
215           "resource_type": "ns_emon_poll_policy",
216           "operation_name": "add",
217           "dependent_resources": "download,poll_activity_status,
                  mail_profile,slack_profile,smtp_server"
218         }
219   ,
220         {
221
222           "access_type": true,
223           "resource_type": "ns_visualizer_gslb_bindings",
224           "operation_name": "add",
225           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,poll_activity_status,
                  ns_emon_poll_policy,ns_gslbvserver_domain,lb_export_report"
226         }
227   ,
228         {
229
230           "access_type": true,
231           "resource_type": "ns_visualizer_gslb_bindings",
232           "operation_name": "get",
233           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  poll_activity_status,ns_emon_poll_policy,
                  ns_gslbvserver_domain,lb_export_report"
234         }
235   ,
236         {
237
238           "access_type": true,
239           "resource_type": "ns_gslbservice",
240           "operation_name": "add",
241           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,poll_activity_status,
                  ns_emon_poll_policy,lb_export_report"
242         }
243   ,
244         {
245
246           "access_type": true,
247           "resource_type": "ns_gslbservice",
248           "operation_name": "get",
249           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  poll_activity_status,ns_emon_poll_policy,lb_export_report"
250         }
```



```
,
      {

        "access_type": true,
        "resource_type": "ns_gslbvserver",
        "operation_name": "get",
        "dependent_resources": "download,DeviceAPIProxy,smtp_server,
            perf_global_server_load_balancing_report,
            poll_activity_status,ns_emon_poll_policy,lb_export_report"
       }
,
      {

        "access_type": true,
        "resource_type": "ns_gslbvserver",
        "operation_name": "add",
        "dependent_resources": "DeviceAPIProxy,mail_profile,
            slack_profile,smtp_server,poll_activity_status,
            ns_emon_poll_policy,lb_export_report"
      }
,
      {

        "access_type": true,
        "resource_type": "ns_vpnvserver",
        "operation_name": "add",
        "dependent_resources": "DeviceAPIProxy,mail_profile,
            slack_profile,smtp_server,poll_activity_status,
            ns_emon_poll_policy,lb_export_report"
       }
,
      {

        "access_type": true,
        "resource_type": "ns_vpnvserver",
        "operation_name": "get",
        "dependent_resources": "download,DeviceAPIProxy,smtp_server,
            perf_ssl_vpn_report,poll_activity_status,ns_emon_poll_policy
            ,lb_export_report"
       }
,
      {

        "access_type": true,
        "resource_type": "ns_csvserver",
```



```
288           "operation_name": "get",
289           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  perf_content_switching_report,ns_emon_poll_policy,
                  poll_activity_status,ns_visualizer_cs_bindings,
                  lb_export_report"
290         }
291   ,
292         {
293
294           "access_type": true,
295           "resource_type": "ns_csvserver",
296           "operation_name": "add",
297           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,ns_emon_poll_policy,
                  poll_activity_status,ns_visualizer_cs_bindings,
                  lb_export_report"
298         }
299   ,
300         {
301
302           "access_type": true,
303           "resource_type": "dns_domain_entry",
304           "operation_name": "get",
305           "dependent_resources": ""
306         }
307   ,
308         {
309
310           "access_type": true,
311           "resource_type": "dns_domain_entry",
312           "operation_name": "add",
313           "dependent_resources": ""
314         }
315   ,
316         {
317
318           "access_type": true,
319           "resource_type": "devicewise_detail_summary",
320           "operation_name": "get",
321           "dependent_resources": "download,mps_user_heatmap,ns_event,
                  mps_agent,active_event,smtp_server,mps_datacenter,
                  event_severity_report,event_device_report,ns_conf,
                  device_event_summary"
322         }
323   ,
```



```
        {

          "access_type": true,
          "resource_type": "devicewise_detail_summary",
          "operation_name": "add",
          "dependent_resources": "mail_profile,slack_profile,smtp_server"
         }
  ,
        {

          "access_type": true,
          "resource_type": "cbwanopt",
          "operation_name": "get",
          "dependent_resources": "download,device_backup,traceroute,
              inventory,inventory_status,ping,mps_datacenter,
              cbwanopt_device_profile,sdwanvw_device_profile,
              sdwanvw_snmp_config,sdwanvw_appflowconfig,smtp_server,
              cbwanopt_snmp_config,cbwanopt_appflowconfig,sdwanvw,tag"
         }
  ,
        {

          "access_type": true,
          "resource_type": "cbwanopt",
          "operation_name": "add",
          "dependent_resources": "inventory,managed_device,device_backup,
              upload,cbwanopt_device_profile,mps_datacenter,mail_profile,
              slack_profile,smtp_server,sdwanvw_device_profile,
              sdwanvw_snmp_config,sdwanvw_appflowconfig,
              cbwanopt_snmp_config,cbwanopt_appflowconfig,sdwanvw,tag"
         }
  ,
        {

          "access_type": true,
          "resource_type": "device_login",
          "operation_name": "get",
          "dependent_resources": ""
         }
  ,
        {

          "access_type": true,
          "resource_type": "ns",
          "operation_name": "get",
```



```
361           "dependent_resources": "download,ns_config_replicate,ns_conf,
                  ns_ns_runningconfig,ns_ns_savedconfig,active_event,
                  device_backup,traceroute,inventory,inventory_status,ping,
                  ns_device_profile,nssdx_device_profile,sdx_snmp_config,
                  sdx_syslog_config,smtp_server,ns_cluster,ns_snmp_config,
                  ns_syslog_config,ns_l7_latency_config,ica_l7_latency_update,
                  af_vserver_policy,ns_vserver_appflow_config,mps_datacenter,
                  ns_appflow_param_config,ns_ns_license,ns_ns_mode,
                  ns_network_interface,advanced_analytics_config,tag"
362         }
363   ,
364         {
365
366           "access_type": true,
367           "resource_type": "ns",
368           "operation_name": "add",
369           "dependent_resources": "inventory,ns_l7_latency_config,
                  ica_l7_latency_update,af_vserver_policy,ns_config_replicate,
                  managed_device,device_backup,upload,ns_device_profile,
                  nssdx_device_profile,mps_datacenter,sdx_snmp_config,
                  sdx_syslog_config,mail_profile,slack_profile,smtp_server,
                  ns_cluster,ns_snmp_config,ns_syslog_config,
                  ns_vserver_appflow_config,ns_appflow_param_config,
                  advanced_analytics_config,tag"
370         }
371   ,
372         {
373
374           "access_type": true,
375           "resource_type": "haproxyhost",
376           "operation_name": "get",
377           "dependent_resources": "download,traceroute,inventory,
                  inventory_status,ping,mps_datacenter,smtp_server,
                  haproxy_device_profile,device_backup,tag"
378         }
379   ,
380         {
381
382           "access_type": true,
383           "resource_type": "haproxyhost",
384           "operation_name": "add",
385           "dependent_resources": "inventory,managed_device,mail_profile,
                  slack_profile,smtp_server,mps_datacenter,
                  haproxy_device_profile,haproxy,device_backup,tag"
386         }
```



```
,
      {

        "access_type": true,
        "resource_type": "docker_host",
        "operation_name": "add",
        "dependent_resources": "inventory,ns_snmp_config,managed_device
            ,ns,upload,mail_profile,slack_profile,smtp_server,
            mps_datacenter,ns_device_profile,docker_nscpx_image"
       }
,
      {

        "access_type": true,
        "resource_type": "docker_host",
        "operation_name": "get",
        "dependent_resources": "download,ns_snmp_config,ns_conf,
            ns_ns_runningconfig,ns_ns_savedconfig,smtp_server,
            mps_datacenter,ns_device_profile,traceroute,inventory,
            inventory_status,ping,active_event,ns_ns_license,ns_ns_mode,
            ns_network_interface"
       }
,
      {

        "access_type": true,
        "resource_type": "perf_reports",
        "operation_name": "add",
        "dependent_resources": "mail_profile,slack_profile,smtp_server,
            perf_custom_dashboard"
       }
,
      {

        "access_type": true,
        "resource_type": "perf_reports",
        "operation_name": "get",
        "dependent_resources": "download,smtp_server,
            perf_report_counters,perf_res_util_report,
            perf_http_req_tcp_conn_report,perf_lb_ssl_traffic_report,
            perf_ip_bytes_rxtx_report,perf_ip_pkt_rxtx_report,
            perf_icmp_pkt_rxtx_report,perf_icmp_bytes_rxtx_report,
            perf_icmpv6_pkt_rxtx_report,perf_icmpv6_bytes_rxtx_report,
            perf_ipv6_bytes_rxtx_report,perf_ipv6_pkt_rxtx_report,
            perf_udp_bytes_rxtx_report,perf_udp_packets_rxtx_report,
```



```
                perf_cmp_bytes_rxtx_report,perf_cmp_tcp_bytes_rxtx_report,
                perf_cmp_tcp_ratiosaving_report,
                perf_cmp_decmp_bytes_rxtx_report,
                perf_cmp_decmp_ratiosaving_report,
                perf_tcp_server_conn_report,
                perf_tcp_surgelen_spareconn_report,perf_http_bytes_rx_report
                ,perf_http_gets_posts_report,
                perf_ssl_transactions_hits_report,
                perf_ssl_client_auth_report,perf_ssl_rsa_dhkey_report,
                perf_ssl_frontend_ciphers_report,
                perf_ssl_backend_ciphers_report,
                perf_wsdevice_cpu_utilization_report,
                perf_wsdevice_send_compression_ratio_report,
                perf_wsdevice_connected_plugins_report,
                perf_wsdevice_data_reduction_report,
                perf_wsdevice_link_utilization_report,
                perf_wsserviceclassstatstable_pass_through_connection_report
                ,perf_wsserviceclassstatstable_service_class_report,
                perf_wsserviceclassstatstable_acceleration_report,
                perf_wslinkstatstable_throughput_report,
                perf_wslinkstatstable_packet_loss_report,
                perf_wsappstatstable_application_report,
                perf_wsqosstatstable_qos_report,
                perf_ssl_cpu_keyexchange_report,perf_ssl_be_rsa_dhkey_report
                ,perf_custom_dashboard,perf_ns_throughput_report,
                perf_network_interface_report"
418          }
419   ,
420          {
421
422            "access_type": true,
423            "resource_type": "perf_threshold",
424            "operation_name": "get",
425            "dependent_resources": "download,perf_reports,
                   perf_report_counters,smtp_server,sms_server,sms_profile"
426          }
427   ,
428          {
429
430            "access_type": true,
431            "resource_type": "perf_threshold",
432            "operation_name": "add",
433            "dependent_resources": "mail_profile,slack_profile,smtp_server,
                   sms_server,sms_profile"
434          }
```



```
435   ,
436         {
437
438           "access_type": true,
439           "resource_type": "perf_poll_config",
440           "operation_name": "add",
441           "dependent_resources": "mail_profile,slack_profile,smtp_server"
442          }
443   ,
444         {
445
446           "access_type": true,
447           "resource_type": "perf_poll_config",
448           "operation_name": "get",
449           "dependent_resources": "smtp_server,download"
450          }
451   ,
452         {
453
454           "access_type": true,
455           "resource_type": "license_server_info",
456           "operation_name": "get",
457           "dependent_resources": "sms_server,license_proxy_server,
                jazz_license,download,sms_profile,smtp_server,
                user_managed_tp_vserver,managed_vserver,user_managed_vserver
                ,haproxy_frontend,haproxy_backend,license_file,
                device_license_info,license_info,ns_authenticationvserver,
                ns_gslbvserver,ns_vpnvserver,ns_csvserver,ns_crvserver,
                ns_lbvserver,autoselection_preference,license_threshold,
                license_expiry_info"
458          }
459   ,
460         {
461
462           "access_type": true,
463           "resource_type": "license_server_info",
464           "operation_name": "add",
465           "dependent_resources": "sms_server,license_proxy_server,
                jazz_license,sms_profile,mail_profile,slack_profile,
                smtp_server,user_managed_tp_vserver,managed_vserver,upload,
                license_file,license_info,license_threshold,mas_license,
                user_managed_vserver,autoselection_preference,
                license_expiry_info"
466          }
467
```



```
468       ],
469       "ui": [
470         {
471
472           "access_type": true,
473           "name": "ApplicationsDashboard",
474           "display_name": "Dashboard"
475         }
476   ,
477         {
478
479           "access_type": true,
480           "name": "SecurityDashboard",
481           "display_name": "App Security Dashboard"
482         }
483   ,
484         {
485
486           "access_type": true,
487           "name": "Stylebooks",
488           "display_name": "StyleBooks"
489         }
490   ,
491         {
492
493           "access_type": true,
494           "name": "Stylebooks",
495           "display_name": "Configpacks"
496         }
497   ,
498         {
499
500           "access_type": true,
501           "name": "StylebooksSettings",
502           "display_name": "Settings"
503         }
504   ,
505         {
506
507           "access_type": true,
508           "name": "CacheRedirection",
509           "display_name": "Cache Redirection"
510         }
511   ,
512         {
```



```
513
514           "access_type": true,
515           "name": "HAProxy",
516           "display_name": "HAProxy"
517         }
518   ,
519         {
520
521           "access_type": true,
522           "name": "Servers",
523           "display_name": "Servers"
524         }
525   ,
526         {
527
528           "access_type": true,
529           "name": "VirtualServers",
530           "display_name": "Virtual Servers"
531         }
532   ,
533         {
534
535           "access_type": true,
536           "name": "Services",
537           "display_name": "Services"
538         }
539   ,
540         {
541
542           "access_type": true,
543           "name": "ServiceGroups",
544           "display_name": "Service Groups"
545         }
546   ,
547         {
548
549           "access_type": true,
550         "name": "Authentication",
551           "display_name": "Authentication"
552         }
553   ,
554         {
555
556           "access_type": true,
557           "name": "MonitoringAuditing",
```



```
558           "display_name": "Auditing"
559         }
560   ,
561         {
562
563           "access_type": true,
564           "name": "MonitoringSettings",
565           "display_name": "Settings"
566         }
567   ,
568         {
569
570           "access_type": true,
571           "name": "GSLBDomains",
572           "display_name": "Domains"
573         }
574   ,
575         {
576
577           "access_type": true,
578           "name": "GSLBServices",
579           "display_name": "Services"
580         }
581   ,
582         {
583
584           "access_type": true,
585           "name": "GSLBVirtualServer",
586           "display_name": "Virtual Server"
587         }
588   ,
589         {
590
591           "access_type": true,
592           "name": "NetScalerGateway",
593           "display_name": "NetScaler Gateway"
594         }
595   ,
596         {
597
598           "access_type": true,
599           "name": "ContentSwitching",
600           "display_name": "Content Switching"
601         }
602   ,
```



```
603         {
604
605           "access_type": true,
606           "name": "DNSDomainNames",
607           "display_name": "DNS Domain Names"
608          }
609   ,
610         {
611
612           "access_type": true,
613           "name": "NetworkDashboard",
614           "display_name": "Instances Dashboard"
615          }
616   ,
617         {
618
619           "access_type": true,
620           "name": "NetScalerSDWANWOInstances",
621           "display_name": "NetScaler SD-WAN"
622          }
623   ,
624         {
625
626           "access_type": true,
627           "name": "InstanceOperations",
628           "display_name": "Instance Operations"
629          }
630   ,
631         {
632
633           "access_type": true,
634           "name": "NetScalerInstances",
635           "display_name": "NetScaler ADC"
636          }
637   ,
638         {
639
640           "access_type": true,
641           "name": "HAProxyInstances",
642           "display_name": "HAProxy"
643          }
644   ,
645         {
646
647           "access_type": true,
```



```
          "name": "NetScalerCPXDockerHost",
          "display_name": "Docker Hosts"
        }
  ,
       {

          "access_type": true,
          "name": "Reports",
          "display_name": "Reports"
        }
  ,
       {

          "access_type": true,
          "name": "Thresholds",
          "display_name": "Thresholds"
        }
  ,
       {

          "access_type": true,
          "name": "ReportingSettings",
          "display_name": "Settings"
        }
  ,
       {

          "access_type": true,
          "name": "Licenses",
          "display_name": "License Management"
        }

     ]
    }

 }

<!--NeedCopy-->
```

REST-API zum Erstellen einer Zugriffsrolle

```
URL: https://<MAS_IP>/nitro/v2/config/rba_role
HTTPMETHOD: POST
```



```
3
4  Payload:
5  {
6
7    "rba_role": {
8
9      "name": "AppOwnerRole",
10     "description": "ExampleCompany App Owner Role",
11     "policies": [
12       "AppOwnerAccessPolicy"
13     ]
14    }
15
16 <!--NeedCopy-->
```

REST-API zum Hochladen des neuen GSLB StyleBook

```
1  URL: https://<MAS_IP>/stylebook/nitro/v2/config/stylebooks
2  HTTPMETHOD: POST
3
4  Payload:
5  {
6
7      "stylebook": {
8
9        "file_name": "my-own-gslb.yaml",
10       "source": "bmFtZTogZ3NsYi1kbnMtZG9tYW...aXRvcm5hbWU=",
11       "encoding": "base64"
12      }
13
14    }
15
16 <!--NeedCopy-->
```

> **Hinweis:**
>
> Der Name des StyleBook kann sich auf Ihrem System ändern.

REST-API zum Erstellen von Gruppen und Zuweisen ausgewählter Instanzen und StyleBooks

```
1  URL: https://<MAS_IP>/nitro/v2/config/mpsgroup
2  HTTPMETHOD: POST
```



```
3
4  Payload:
5  {
6
7    "mpsgroup": {
8
9      "id": "",
10     "name": "AppOwnerGroup1",
11     "description": "ExampleCompany App Owner Group",
12     "roles": [
13       "AppOwnerRole"
14     ],
15     "enable_session_timeout": false,
16     "assign_all_devices": false,
17     "ass ign_all_apps": false,
18     "application_names_with_regex": [
19
20     ],
21     "standalone_instances_id": [
22       "72c178da-47df-4426-9acc-cd6316f92506",
23       "c948061e-6240-4062-931c-f6988ef36e3b"
24     ],
25     "application_list": [
26
27     ],
28     "permission": "none",
29     "application_names": [
30
31     ],
32     "authscope_props": [
33       {
34
35         "propname": "configuration_template_id",
36         "propvalues": [
37           "NONE"
38         ]
39        }
40 ,
41       {
42
43         "propname": "dns_domain_entry_id",
44         "propvalues": [
45           "cf6631e5-2f56-4bb1-b0a5-90fabfc0e3e2",
46           "b268905c-522d-47e3-a2ca-3f8d8a754373"
47         ]
```



```
        }
 ,
      {

        "propname": "stylebook_id",
        "propvalues": [
          "gslbbb963abe85936913035e1d4dd14b56f7",
          "moni72fad4494466d102b19c18ac329fa9f3"
        ]
       }

    ],
    "tenant_id": "6d024111-6636-4571-a250-d47b31aba7a8"
   }

 }

<!--NeedCopy-->
```

Hinweis

Um die IDs für DNS-Domänennamen und GSLB-StyleBooks zu erhalten, die in der oben genannten API-Nutzlast verwendet werden, können Sie reguläre Citrix ADM APIs zum Abfragen von IDs verwenden, die Entitätsnamen entsprechen. Um beispielsweise die ID für eine DNS-Domäne namens app1.acme.com zu erhalten, können Sie die folgende Citrix ADM REST-API verwenden.

```
URL: https://<MAS_IP>/nitro/v2/config/dns_domain_entry?filter=name:
   app1.acme.com
HTTPMETHOD: GET

The ID of this domain can be extracted from the following response.
{

  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "dns_domain_entry",
  "username": "nsroot",
  "tenant_name": "Owner",
  "tenant_id": "568d8e12-1d88-42b2-8943-cbaa04826fd1",
  "resourceName": "",
  "dns_domain_entry": [
    {
```



```
17
18        "tenant_id": "568d8e12-1d88-42b2-8943-cbaa04826fd1",
19        "name": "app1.acme.com",
20        "id": "3e3d85ea-1c21-49b2-97f4-60fccdbae2e0",
21        "description": "app1 domain name"
22       }
23
24    ]
25   }
26
27  <!--NeedCopy-->
```

Um die StyleBook-ID für ein StyleBook zu erhalten, dessen Namespace com.citrix.adc.stylebook, Version: 1.0, name: ist `my-own-gslb`, können Sie die folgende API verwenden.

```
1 URL: https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks?filter=name:
     my-own-gslb,namespace:com.citrix.adc.stylebooks,version:1.0
2 HTTPMETHOD: GET
3 <!--NeedCopy-->
```

Die Antwort enthält die StyleBook-Details, einschließlich des ID-Attributs.

```
1  {
2
3    "stylebooks": [
4      {
5
6        "author": null,
7        "builtin": "false",
8        "builtins": "{
9   "netscaler.nitro.config": "10.5" }
10   ",
11       "deprecate": "false",
12       "description": " This StyleBook is used to configure one or a
             number of Citrix ADCs in different sites into a GSLB setup. It
              is assumed that the SNIP IP on each Citrix ADC to be used by
             this StyleBook as the Site IP is already configured on the
             appliance.",
13       "display_name": "HTTP/SSL LoadBalancing StyleBook",
14       "filename": "my-own-gslb.yaml",
15       "hide": null,
16       "id": "gslb5a748d8b7684846cf6c409ad7dea8ccf",
```



```
        "imported_by": "",
        "imported_datetime": "2018-05-25 17:20:32.848902",
        "name": "my-own-gslb",
        "namespace": "com.citrix.adc.stylebooks",
        "pkg_id": "gslb5a748d8b7684846cf6c409ad7dea8ccf",
        "primary_keys": "["name"]",
        "private": "false",
        "recompile": "false",
        "schema_version": "1.0",
        "source": "LS0tIApuYW1lOiBsYgpuYW1lc…",
        "system": null,
        "tags": "",
        "tenant_id": null,
        "user_sb": "false",
        "version": "1.0"
      }
  ,
     {

        …
      }

   ]
  }

<!--NeedCopy-->
```

> **Hinweis**
>
> Die obige API gibt eine Liste von StyleBooks zurück, die mit dem Filter übereinstimmen. Stellen Sie sicher, dass Sie das richtige StyleBook aus der Antwort auswählen, um die ID abzurufen.

REST-API zum Erstellen von Systembenutzern

> **Hinweis**
>
> Dieser Schritt ist optional.

```
URL: https://<MAS_IP>/nitro/v2/config/mpsuser
HTTPMETHOD: POST

Payload:
{

```



```
  "mpsuser": {

    "name": "John",
    "password": "welcome",
    "external_authentication": false,
    "enable_session_timeout": false,
    "groups": [
      "AppOwnerGroup1"
    ]
   }

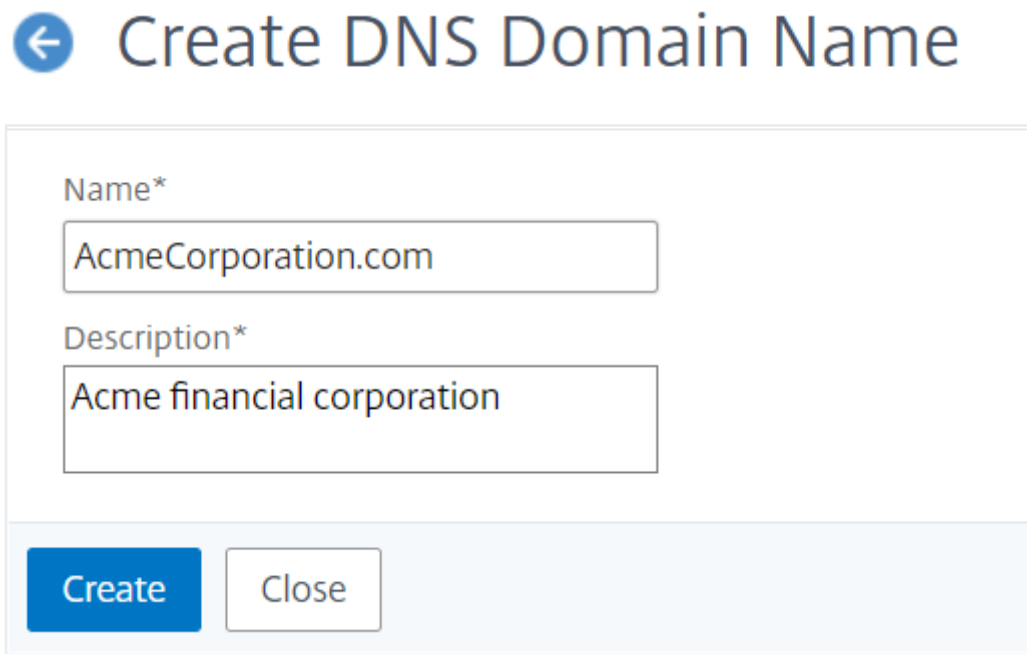
 }

<!--NeedCopy-->
```

Workflow für die Anwendungseigentümer

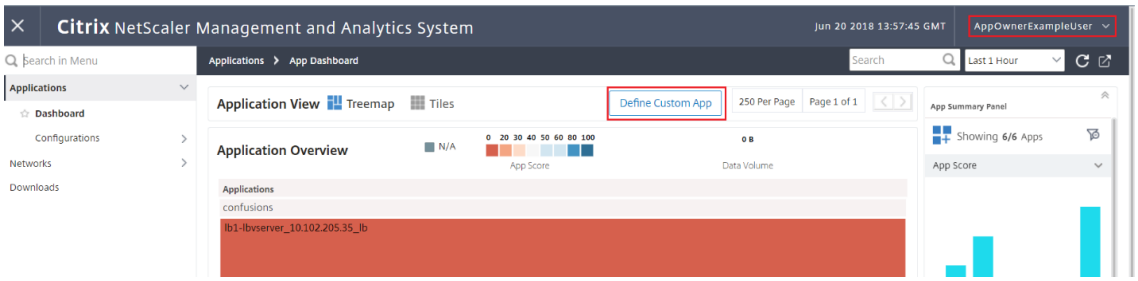
Ihre Benutzer müssen sich mit ihren Anmeldeinformationen als Anwendungsbenutzer anmelden. Die Benutzer müssen diese Aufgabe ausführen, um ihre eigenen DNS-Domänennamen zu erstellen und das neue GSLB-StyleBook zu verwenden.

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **DNS-Domänennamen**.
2. Klicken Sie auf **Hinzufügen**, um eine neue DNS-Domäne zu erstellen. Erstellen Sie die DNS-Domänen in Citrix ADM.

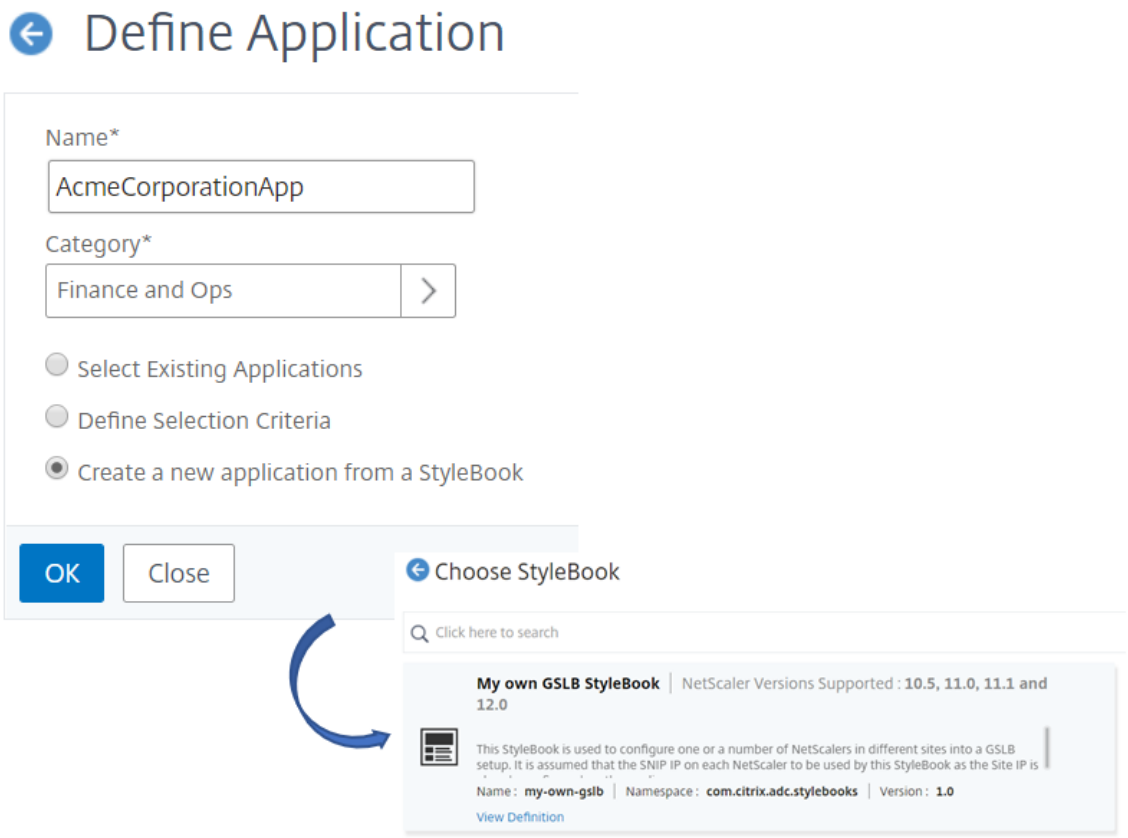


> **Hinweis**
>
> Als Administrator können Sie diese Domänennamen auch erstellen und den Benutzergruppen zuweisen.

3. Navigieren Sie zu **Anwendungen** > **Dashboard**, und klicken Sie auf **Benutzerdefinierte App definieren**.



4. Geben Sie einen Namen für die Anwendung ein, und wählen Sie eine Kategorie aus. Wählen Sie **Neue Anwendung aus einem StyleBook erstellen** aus und klicken Sie auf **OK**. Wählen Sie **Mein eigenes GSLB-StyleBook** aus, um die Konfiguration auf den ausgewählten Instanzen bereitzustellen.



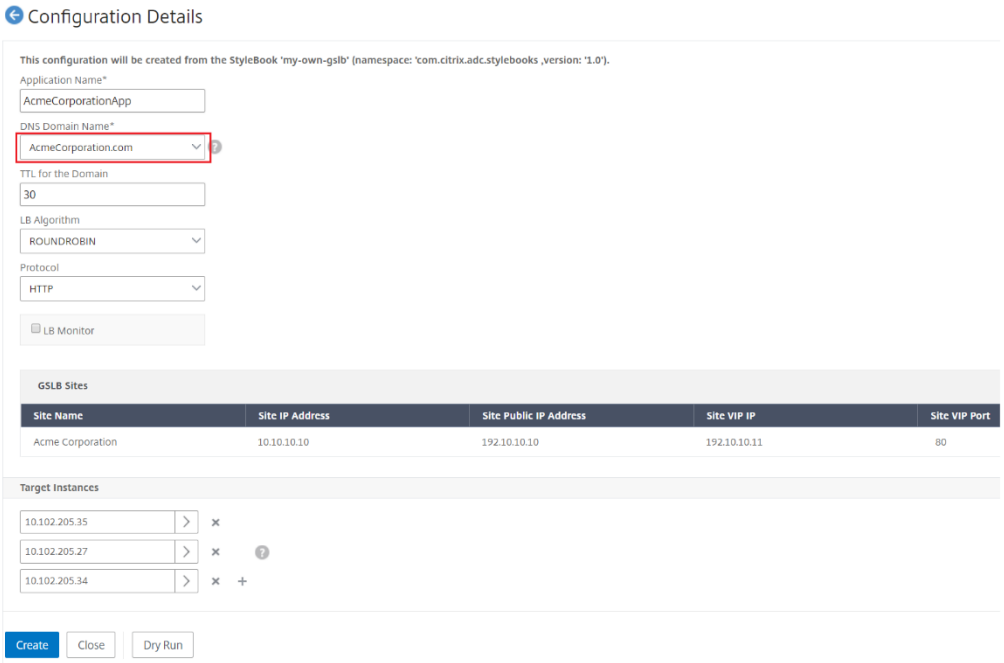
5. Geben Sie die Werte ein, die für alle Parameter im StyleBook erforderlich sind.

   a) Wählen Sie den Domänennamen aus der Liste aus.

b) Fügen Sie die GSLB-Sites Ihrer Anwendung hinzu.

c) Wählen Sie die Citrix ADC Zielinstanzen in allen GSLB-Sites aus.

d) Klicken Sie auf **Erstellen**, um eine GSLB-Konfiguration zu erstellen.



> **Hinweis**
>
> Der StyleBook-Parameter DNS-Domänenname zeigt nur die Liste der DNS-Domänen an, die zum Benutzer in Citrix ADM gehören.

Citrix ADM REST-API für App-Besitzer-Workflow

REST-API für die Anmeldung bei Citrix ADM

```
URL: http: //<MAS_IP>/nitro/v2/config/login
HTTPMETHOD: POST

Payload:
{

  ”login”: {

    ”username”: ”<USER_NAME>”,
    ”password”: ”<PASSWORD>”,
    ”session_timeout”: 1800
   }

```



```
 }

<!--NeedCopy-->
```

REST-API zum Erstellen von DNS-Domänennamen

```
URL: https://<MAS_IP>/nitro/v2/config/dns_domain_entry
HTTP METHOD: POST
PAYLOAD: {
 ”dns_domain_entry”:{
 ”name”:”app1.acme.com”,”description”:”app1 acme domain”
 }

 }

<!--NeedCopy-->
```

REST-API zum Erstellen von Anwendungen mit StyleBook

```
URL: https://<MAS_IP>/nitro/v2/config/application
HTTPMETHOD: POST

Payload:
{

  ”params”: {

    ”action”: ”app_discovery”
   }
 ,
  ”application”: {

    ”id”: ””,
    ”name”: ”app1”,
    ”app_c ategory”: ”ITOps”,
    ”stylebook_params”: ”{
 ”name”:”my-own-gslb”,”namespace”:”com.citrix.adc.stylebooks”,”version”
    :”1.0”,”configpack_payload”:{
 ”parameters”:{
 ”name”:”app1”,”domain-name”:”app1.acme.com”,]”ttl”:”30”,”algorithm”:”
    ROUNDROBIN”,”protocol”:”HTTP”,”sites”:[{
```



```
21  "name":"site1","ipaddress":"6.5.6.77","virtual-ip":"88.6.5.44","
       virtual-port":"80" }
22  ] }
23  ,"targets":[ {
24  "id":"72c178da-47df-4426-9acc-cd6316f92506" }
25  , {
26  "id":"0e4d0789-bffe-4266-ba1c-09adfc61db4e" }
27  , {
28  "id":"b5af4455-3f06-4f56-b0cb-3d9f868c1f94" }
29  ] }
30   }
31  "
32    }
33
34  }
35
36 <!--NeedCopy-->
```

In der obigen Nutzlast:

- Die stylebook_params enthält den Namen, Namespaces und die Version des zu verwendenden StyleBook.
- Die configpack_payload enthält die gefüllten Parameter des StyleBook, wie in der äquivalenten GUI-Form oben gezeigt. Citrix ADM stellt sicher, dass nur DNS-Domänennamen, auf die der Benutzer Zugriff hat, als Werte für den Parameter domain-name verwendet werden können.
- Die "Ziele" enthalten die Liste der NetScaler IDs, auf denen die GSLB-Konfiguration bereitgestellt wird (die ADC-Instanzen auf den GSLB-Sites).

Um die NetScaler-ID unter Angabe der Verwaltungs-IP-Adresse von NetScaler zu erhalten, können Sie die folgende Citrix ADM API verwenden:

```
1 URL: https://<MAS_IP>/nitro/v2/config/ns?filter=ip_address:
     192.168.153.162
2 HTTPMETHOD: GET
3 <!--NeedCopy-->
```

Die Antwort-Nutzlast enthält Informationen zu diesem NetScaler, einschließlich seiner ID:

```
1 {
2
3   "errorcode": 0,
```



```
  "message": "Done",
  ...."tenant_id": "ec0eb868-0d6b-4729-bfbd-3005dd2694c1",
  "resourceName": "",
  "ns": [
    {

      "manufacturedate": "9/30/2009",
      "is_grace": "false",
      "hostname": "youcef-ns",
      "std_bw_config": "0",
      "gateway_deployment": "false",
      "gateway_ipv6": "",
      "ha_master_state": "Primary",
      "instance_available": "0",
      "device_finger_print": "",
      "instance_state": "Down",
      "reason": "Device not reachable",
      "name": "",
      "ent_bw_available": "0",
      "description": "",
      "id": "da9ffff2-c100-45f1-a913-c542718338b2",
      "mgmt_ip_address": "192.168.153.162",
      ....
    }

  ]
 }

<!--NeedCopy-->
```

Erstellen Sie Ihr StyleBook

Der vollständige Inhalt der Datei my-own-gslb.yaml StyleBook ist unten dargestellt:
Sie können dieses benutzerdefinierte StyleBook so verwenden, wie es ist, oder passen Sie es an Ihre Bedürfnisse an, um die erforderliche GSLB-Konfiguration zu generieren. Der wichtige Parameter in diesem StyleBook namens “domänenname” muss in jedem StyleBook vorhanden sein, um die DNS-Namenfunktionalität nutzen zu können.

```
name: my-own-gslb
namespace: com.citrix.adc.stylebooks
version: "1.0"
display-name: My own GSLB StyleBook
```



```
description: This StyleBook is used to configure one or a number of
    NetScalers in different sites into a GSLB setup. It is assumed that
    the SNIP IP on each NetScaler to be used by this StyleBook as the
    Site IP is already configured on the appliance.
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
  -
    namespace: com.citrix.adc.commontypes
    version: "1.0"
    prefix: cmtypes
parameters:
  -
    name: name
    label: Application Name
    type: string
    required: true
    key: true

  -
    name: domain-name
    label: DNS Domain Name
    description: GSLB DNS Domain Name
    type: string
    required: true
    allowed-dynamic-values:
      source: local
      resource-type: dns_domain_entry

  -
    name: ttl
    label: TTL for the Domain
    description: Time-To-Live value (number of seconds) for the Domain
    type: number
    default: 30

  -
    name: algorithm
    label: LB Algorithm
    description: Global Load Balancing Algorithm
    type: string
    default: ROUNDROBIN
```



```
47      allowed-values:
48        - ROUNDROBIN
49        - STATICPROXIMITY
50        - SOURCEIPHASH
51
52    -
53      name: protocol
54      label: Protocol
55      description: The protocol of the GSLB VIP
56      type: string
57      default: HTTP
58      allowed-values:
59        - HTTP
60        - FTP
61        - TCP
62        - UDP
63        - SSL
64        - SSL_BRIDGE
65        - SSL_TCP
66        - NNTP
67        - ANY
68        - SIP_UDP
69        - SIP_TCP
70        - SIP_SSL
71        - RADIUS
72        - RDP
73        - RTSP
74        - MYSQL
75        - MSSQL
76        - ORACLE
77
78    -
79      name: monitor
80      label: LB Monitor
81      description: Monitor to be bound to the GSLB service
82      type: cmtypes::monitor
83
84    -
85      name: sites
86      label: GSLB Sites
87      description: Provide information about the GSLB Sites
88      type: object[]
89      required: true
90      parameters:
91        -
```



```
92          name: name
93          label: Site Name
94          type: string
95          required: true
96        -
97          name: ipaddress
98          label: Site IP Address
99          description: The IP Address of this Site. Use a SNIP IP address
                on the site's appliance.
100         type: ipaddress
101         required: true
102       -
103         name: public-ipaddress
104         label: Site Public IP Address
105         description: The Public IP Address of this Site. It NATs to the
                Site's IP address
106         type: ipaddress
107       -
108         name: virtual-ip
109         label: Site VIP IP
110         description: The IP Address for the GSLB Service on this site (
               The VIP on this Site)
111         type: ipaddress
112         required: true
113       -
114         name: virtual-port
115         label: Site VIP Port
116         description: The port number for the GSLB Service (VIP) on this
                site
117         type: tcp-port
118         default: 80
119
120 components:
121   -
122     name: enable-gslb-comp
123     type: ns::nsfeature
124     description: Enables the GSLB feature
125     meta-properties:
126       action: enable
127     properties:
128       feature: [”GSLB”, ”LB”]
129   -
130     name: gslb-monitor-comp
131     type: cmtypes::monitor
132     condition: $parameters.monitor
```



```
133       properties:
134         monitorname: $parameters.name + "-" + $parameters.monitor.
              monitorname + "-gslbmon"
135         type: $parameters.monitor.type
136         destip?: $parameters.monitor.destip
137         destport?: $parameters.monitor.destport
138         httprequest?: $parameters.monitor.httprequest
139         send?: $parameters.monitor.send
140         customheaders?: $parameters.monitor.customheaders
141         respcodes?: $parameters.monitor.respcodes
142         recv?: $parameters.monitor.recv
143         lrtm?: $parameters.monitor.lrtm
144         secure?: $parameters.monitor.secure
145         interval?: $parameters.monitor.interval
146         interval_units?: $parameters.monitor.interval_units
147         resptimeout?: $parameters.monitor.resptimeout
148         retries?: $parameters.monitor.retries
149         downtime?: $parameters.monitor.downtime
150     -
151       name: gslb-vserver-comp
152       type: ns::gslbvserver
153       description: Creates a GSLB VServer config object
154       properties:
155         name: $parameters.name + "-gslbvserver"
156         servicetype: $parameters.protocol
157         lbmethod: $parameters.algorithm
158       components:
159         -
160           name: gslb-domain-comp
161           type: ns::gslbvserver_domain_binding
162           properties:
163             name: $parent.properties.name
164             domainname: $parameters.domain-name
165             ttl: $parameters.ttl
166     -
167       name: gslb-site-comp
168       type: ns::gslbsite
169       description: Creates a GSLB Site config object
170       repeat: $parameters.sites
171       repeat-item: site
172       properties:
173         sitename: $parameters.name + "-" + $site.name + "-gslbsite"
174         siteipaddress: $site.ipaddress
175         publicip?: $site.public-ipaddress
176       components:
```



```
177         -
178           name: gslb-service-comp
179           type: ns::gslbservice
180           description: Creates a GSLB Service
181           properties:
182             servicename: $parameters.name + "-" + $site.name + "-
                  gslbservice"
183             ip: $site.virtual-ip
184             servicetype: $parameters.protocol
185             port: $site.virtual-port
186             sitename: $parent.properties.sitename
187           components:
188             -
189               name: gslb-vserver-service-binding-comp
190               type: ns::gslbvserver_gslbservice_binding
191               description: Creates a Binding between the GSLB vserver and
                    the GSLB Service
192               properties:
193                 name: $components.gslb-vserver-comp.properties.name
194                 servicename: $parent.properties.servicename
195             -
196               name: gslb-service-monitor-binding-comp
197               type: ns::gslbservice_lbmonitor_binding
198               description: Creates a Binding between the GSLB service and
                    the GSLB monitor
199               condition: $parameters.monitor
200               properties:
201                 servicename: $parent.properties.servicename
202                 monitor_name: $components.gslb-monitor-comp.properties.
                      monitorname
203   <!--NeedCopy-->
```

Verwenden von API zum Erstellen von Konfigurationen aus StyleBooks

April 28, 2021

Nachdem Sie Ihr StyleBook erstellt haben, müssen Sie es in Citrix Application Delivery Management (ADM) importieren, um es entweder mithilfe des Citrix ADM oder mithilfe von Citrix ADM-APIs zu verwenden. Citrix ADM validiert Ihr StyleBook beim Importieren. Wenn die Validierung erfolgreich ist, wird Ihr StyleBook im Citrix ADM -Katalog von StyleBooks angezeigt, der zum Erstellen von Konfigurationen verwendet werden kann.

Sie können jetzt die StyleBook-APIs verwenden, um Konfigurationen basierend auf diesem StyleBook zu erstellen. Sie können ein beliebiges Tool wie das cURL-Befehlszeilentool oder die Chrome-Browsererweiterung von Postman verwenden, um HTTP-Anfragen an Citrix ADM zu senden.

Beispiel 1

Betrachten Sie das in Ihnen erstellte `lb-vserver` StyleBook StyleBook zum Erstellen eines virtuellen Load Balancing Servers. Verwenden Sie REST API, um ein Konfigurationspaket aus diesem StyleBook wie folgt zu erstellen:

HTTP METHOD: POST

URL: `https://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/lb-vserver/configpacks`

REQUEST Headers:

Content-Type: application/json

Accept: application/json

REQUEST BODY PAYLOAD:

```
{

  ”configpack”:
  {

    ”parameters”: {

      ”name”: ”lb1”,
      ”ip”: ”10.102.117.31”
     }
 ,
    ”targets”:
    [
      {

        ”id”: ”deecee30-f478-4446-9741-a85041903410”
       }

    ]
   }

 }
```



```
23
24 <!--NeedCopy-->
```

In dieser HTTP-Anforderung ist die ID (z. B. “deecee30-f478-4446-9741-a85041903410”) die Instanz-ID der Citrix ADC-Instanz, auf der der virtuelle Lastausgleichsserver lb1 mit der IP-Adresse 10.102.117.31 erstellt wird. Die Instanz-ID der Citrix ADC-Instanz wird von Citrix ADM abgerufen.

Um die ID einer Instanz zu erhalten, die von Citrix ADM verwaltet wird, können Sie Citrix ADM-APIs verwenden. Um beispielsweise die Instanz-ID oder eine Citrix ADC-Instanz abzurufen, deren IP-Adresse 192.168.153.160 lautet, können Sie die folgende API verwenden:

HTTP METHOD: GET

URL: `https://<ADM-IP>/nitro/v1/config/ns?filter=ip_address:192.168.153.160`

REQUEST HEADERS:

Accept: application/json

Die Antwort enthält die ID in der json-Nutzlast:

EXPECTED RESPONSE HEADERS (on success):

200 OK

Content-Type: application/json

EXPECTED RESPONSE BODY (on success):


```
1  {
2
3    ”errorcode”: 0,
4    ”message”: ”Done”,
5    ”operation”: ”get”,
6    ”resourceType”: ”ns”,
7    ”username”: ”nsroot”,
8    ”tenant_name”: ”Owner”,
9    ”resourceName”: ””,
10   ”ns”:
11   [
12     {
13
14     ”is_grace”: ”false”,
15     ”hostname”: ””,
16     ”std_bw_config”: ”0”,
17     ”gateway_deployment”: ”false”,
18     ”id”: ”deecee30-f478-4446-9741-a85041903410”,
```



```
    }

 ]
 }

<!--NeedCopy-->
```

Wenn das Configuration (Configuration Pack) erfolgreich erstellt wurde, erhalten Sie die folgende HTTP-Antwort:

EXPECTED RESPONSE HEADERS (on success):

200 OK

Content-Type: application/json

EXPECTED RESPONSE BODY (on success):

```
{

  "configpack":
  {

    "config_id": "1460806080"
   }

 }

<!--NeedCopy-->
```

Sie haben Ihre erste Konfiguration (Configuration Pack) erstellt, die durch die ID 1460806080 eindeutig identifiziert wird. Mit dieser ID können Sie die Konfiguration abfragen, aktualisieren oder löschen.

Beispiel 2

Sie können dasselbe StyleBook verwenden, um ein anderes Konfigurations- oder Konfigurationspaket zu erstellen und es auf denselben oder verschiedenen Citrix ADC-Instanzen auszuführen. Erstellen Sie in diesem Beispiel eine weitere Konfiguration, geben Sie einen anderen Namen und eine andere IP-Adresse für den virtuellen Server an und geben Sie LEASTCONNECTION als Lastausgleichsmethode an. Stellen Sie diese Konfiguration auf zwei Citrix ADC-Instanzen bereit.

Die HTTP-Anforderung lautet wie folgt:

HTTP METHOD: POST

URL: https://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/lb-vserver/configpacks

REQUEST HEADERS:

Content-Type: application/json

Accept: application/json

REQUEST BODY PAYLOAD:

```
{

  ”configpack”:
  {

    ”parameters”:
    {

      ”name”: ”lb2”,
      ”ip”: ”10.102.117.32”,
      ”lb-alg”: ”LEASTCONNECTION”
     }
 ,
    ”targets”
    [
     {
 ”id”: ”deecee30-f478-4446-9741-a85041903410” }
 ,
     {
 ”id”: ”debecc60-d589-4557-8632-a74032802412” }

    ]
   }

 }

<!--NeedCopy-->
```

In dieser HTTP-Anforderung wird der virtuelle Server lb2 mit der IP-Adresse 10.102.117.32 auf den beiden Citrix ADC-Instanzen erstellt, die durch die IDs deecee30-f478-4446-9741-a85041903410” und debecc60-d589-4557-8632-a74032802412” dargestellt werden.

Bei erfolgreicher Erstellung des Konfigurationspakets wird die folgende HTTP-Antwort empfangen:

EXPECTED RESPONSE HEADERS (on success):

200 OK

Content-Type: application/json

EXPECTED RESPONSE BODY (on success):

```
{

   ”configpack”:
  {

     ”config_id”: ”1657696292”
   }

 }

<!--NeedCopy-->
```

Dieses neue Konfigurationspaket hat eine andere ID 165769629. Sie können diese Konfiguration mithilfe dieser ID aktualisieren oder entfernen.

Beispiel 3

Betrachten Sie das StyleBook basic-lb-config, das Sie in erstellt habenStyleBook zum Erstellen einer einfachen Lastausgleichskonfiguration. Verwenden Sie REST API, um ein Konfigurationspaket aus diesem StyleBook wie folgt zu erstellen:

HTTP METHOD: POST

URL: `http://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/basic-lb-config/configpacks`

REQUEST HEADERS:

Content-Type: application/json

Accept: application/json

EXPECTED RESPONSE HEADERS (on success):

200 OK

Content-Type: application/json

EXPECTED RESPONSE BODY (on success):


```
{

  ”configpack”:
  {

    ”parameters”:
    {

      ”name”: ”myapp”,
      ”ip”: ”10.70.122.25”,
      ”svc-servers”: [”192.168.100.11”,”192.168.100.12”],
       ”svc-port”: 8080
     }
 ,
    ”targets”:
    [
     {

      ”id”: ”deecee30-f478-4446-9741-a85041903410”
      }
 ,
     {

      ”id”: ”debecc60-d589-4557-8632-a74032802412”
      }

    ]
   }

 }

<!--NeedCopy-->
```

In dieser HTTP-Anforderung wird die Load Balancing-Konfiguration auf zwei Citrix ADC-Instanzen ausgeführt. Sie können sich bei diesen Citrix ADC-Instanzen anmelden, um zu überprüfen, ob ein virtueller Server und eine Dienstgruppe mit zwei Diensten erstellt werden.

Beispiel 4

Betrachten Sie das zusammengesetzte **StyleBook-Composite-Beispiel**, das Sie in erstellt habenErstellen eines zusammengesetzten StyleBook. Verwenden Sie REST API, um ein Konfigurationspaket aus diesem StyleBook wie folgt zu erstellen:

HTTP METHOD: POST

URL: `http://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks`

REQUEST HEADERS:

Content-Type: application/json

Accept: application/json

REQUEST BODY PAYLOAD:

```
{

  ”configpack”:
  {

    ”parameters”: {

      ”name”: ”myapp”,
      ”ip”: ”2.2.2.2”,
      ”svc-servers”: [”10.102.29.52”,”10.102.29.53”]
     }
 ,
    ”targets”:
    [
     {

      ”id”: ”deecee30-f478-4446-9741-a85041903410”
      }
 ,
     {

      ”id”: ”debecc60-d589-4557-8632-a74032802412”
      }

    ]
   }

 }

<!--NeedCopy-->
```

In dieser HTTP-Anforderung wird die Konfiguration auf zwei Citrix ADC-Instanzen erstellt, die durch ihre IDs dargestellt werden. Wenn Sie sich bei Citrix ADC-Instanzen anmelden, können Sie die Konfigurationsobjekte anzeigen, die mit dem StyleBook basic-lb-config erstellt wurden, das in das StyleBook

Composite-example importiert wurde. Sie können auch einen neuen HTTP-Monitor mit dem Namen sehen `myapp-mon`, der Teil des StyleBook “Composite-Beispiel” war.

Bei erfolgreicher Erstellung des Konfigurationspakets wird die folgende HTTP-Antwort empfangen:

EXPECTED RESPONSE HEADERS (on success):

200 OK

Content-Type: application/json

EXPECTED RESPONSE BODY (on success):

```
{

  ”configpack”: {

    ”config_id”: ”4917276817”
   }

 }

<!--NeedCopy-->
```

Aktualisieren einer Konfiguration

Um diese Konfiguration beispielsweise durch Hinzufügen eines neuen Backendservers mit der IP-Adresse 10.102.29.54 zum virtuellen Lastausgleichsserver zu aktualisieren `myapp`, verwenden Sie die API zum Aktualisieren eines Konfigurationspakets wie folgt:

HTTP METHOD: PUT

URL: `http://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks/4917276817`

REQUEST HEADERS:

Content-Type: application/json

Accept: application/json

REQUEST BODY PAYLOAD:

```
{

  ”configpack”: {
```



```
4
5      "parameters": {
6
7        "name": "myapp",
8        "ip": "2.2.2.2",
9        "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
10     }
11   ,
12    "targets":
13     [
14       {
15
16        "id": "deecee30-f478-4446-9741-a85041903410"
17        }
18   ,
19       {
20
21        "id": "debecc60-d589-4557-8632-a74032802412"
22        }
23
24     ]
25     }
26
27   }
28
29 <!--NeedCopy-->
```

Bei erfolgreichem Update des Konfigurationspakets wird die folgende HTTP-Antwort empfangen:

EXPECTED RESPONSE HEADERS (on success):

200 OK

Content-Type: application/json

EXPECTED RESPONSE BODY (on success):

```
1 {
2
3    "configpack": {
4
5      "config-id": "4917276817"
6    }
7
8  }
```



```
9
10 <!--NeedCopy-->
```

Löschen einer Konfiguration

Um diese Konfiguration (aus allen Citrix ADC-Instanzen) zu löschen, können Sie die API wie folgt zum Löschen eines Konfigurationspakets verwenden:

Bei erfolgreichem Löschen des Konfigurationspakets wird die folgende HTTP-Antwort empfangen:

HTTP METHOD: DELETE

URL: `http://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks/4917276817`

REQUEST HEADERS:

Accept: application/json

EXPECTED RESPONSE HEADERS (on success):

200 OK

Content-Type: application/json

EXPECTED RESPONSE PAYLOAD (on success):

```
1 {
2
3    ”configpack”: {
4
5      ”config_id”: ”4917276817”
6    }
7
8  }
9
10 <!--NeedCopy-->
```

Sie können sich bei der Citrix ADC-Instanz anmelden und sicherstellen, dass alle Konfigurationsobjekte, die Teil dieses Konfigurationspakets sind, entfernt wurden.

Wenn Sie die Konfiguration aus bestimmten Citrix ADC-Instanzen anstelle von allen Instanzen entfernen möchten, verwenden Sie den oben beschriebenen Update-Konfigurationspack-Vorgang und ändern Sie das Attribut “Ziele” in der JSON-Nutzlast, um die spezifischen Citrix ADC-Instanz-IDs zu entfernen.

Verwenden der API zum Erstellen von Konfigurationen zum Hochladen von Zertifikaten und Schlüsseldateien

April 28, 2021

Verwenden Sie die StyleBook-APIs, um Konfigurationen basierend auf diesem StyleBook zu erstellen. Sie können ein beliebiges Tool wie das cURL-Befehlszeilentool oder die Chrome-Browsererweiterung von Postman verwenden, um HTTP-Anfragen an Citrix ADM zu senden.

Betrachten Sie das StyleBook-Beispiel, das Sie erstellt haben, um das Zertifikat und die Schlüsseldateien in hochzuladenErstellen eines StyleBook zum Hochladen von SSL-Zertifikats- und Zertifikatsschlüsseldateien in Citrix ADM. Verwenden Sie die REST API, um ein Konfigurationspaket aus diesem StyleBook wie folgt zu erstellen:

POST

`https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async`

```
Content-Type: application/jsonAccept: application/json {

   ”configpack”: {

       ”parameters”: {

           ”lb-appname”: ”lbmon”,
           ”lb-virtual-ip”: ”13.1.11.10”,
           ”lb-virtual-port”: ”80”,
           ”lb-service-type”: ”HTTP”,
           ”svc-service-type”: ”HTTP”,
           ”svc-servers”: [
               {

                   ”ip”: ”14.1.1.15”,
                   ”port”: ”80” }

      ],
           ”certificates”: [
               {

                   ”cert-name”: ”server_cert”,
                   ”cert-file”: ”server_cert.pem”,
                   ”ssl-inform”: ”PEM”,
```



```
                    "key-name": "server_key",
                    "key-file": "server_key.pem",
                    "cert-password": "secret",
                    "cert-advanced": {

                        "is-ca-cert": false,
                        "skip-ca-name": false
            }

          }

       ],
            "lb-advanced": {

                "flush-on-state-down": "ENABLED",
                "auth-params": {

                    "authentication": "OFF",
                    "authentication-http-401": "OFF"
          }
,
                "appflow-log": "ENABLED",
                "algorithm": "LEASTCONNECTION"
        }
,
            "svcg-advanced": {

                "svc-client-ip": "DISABLED",
                "svc-use-source-ip": "NO",
                "svc-use-proxy-port": "NO",
                "svc-surge-protection": "OFF",
                "svc-client-keepalive": "NO",
                "svc-tcp-buffering": "NO",
                "svc-compression": "NO",
                "svc-state": "ENABLED",
                "svc-downstate-flush": "DISABLED",
                "svc-enable-health-monitor": "NO"
        }

     }
,
       "targets": [
            {

                "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"
```



```
70          }
71
72       ]
73     }
74
75   }
76
77 <!--NeedCopy-->
```

Dieses Konfigurationspaket wird unter Verwendung der ID 8c158e7a-0087-423f-91b0-0ccf16de552a eindeutig identifiziert. Mit dieser ID können Sie die Konfiguration abfragen, aktualisieren oder löschen. Bei erfolgreicher Aktualisierung des Konfigurationspakets werden das Zertifikat und die Schlüsseldateien in das Citrix ADM-Dateisystem hochgeladen.

Verwenden der API zum Erstellen von Konfigurationen zum Hochladen beliebiger Dateitypen

April 28, 2021

Sie können auch die Citrix Application Delivery Management (ADM) -API verwenden, um ein Konfigurationspaket zu erstellen, das Dateien in die ausgewählte Citrix ADC-Instanz hochlädt.

Betrachten Sie das StyleBook-Beispiel, das Sie erstellt haben, um Dateien beliebiger Art in Erstellen eines StyleBook zum Hochladen von Dateien in Citrix ADMhochzuladen. Erstellen Sie in diesem Beispiel ein Konfigurationspaket und geben Sie den Wert des Parameters `locationfile` als Dateipfad der Standortdatei auf Citrix ADM an.
Verwenden Sie die REST API, um ein Konfigurationspaket aus diesem StyleBook wie folgt zu erstellen:

POST
`https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.stylebooks.samples/1.0/upload-geolocations/configpacks`

```
1 Content-Type: application/json
2 Accept: application/json
3 {
4
5    ”configpack”:
6    {
7
8       ”parameters”: {
9
```



```
10          "locationfile": "/var/mps/tenants/root/files/ /
                custom_geolocations.csv"
11       }
12   ,
13        "targets": [
14           {
15
16              "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"
17          }
18
19       ]
20      }
21
22   }
23
24   <!--NeedCopy-->
```

Verwenden der API zum Importieren benutzerdefinierter StyleBooks

April 28, 2021

Mit den StyleBook-APIs können Sie nun benutzerdefinierte StyleBooks in Citrix Application Delivery Management (ADM) importieren. Verwenden Sie die REST API, um ein Konfigurationspaket aus diesem StyleBook wie in einem Tool wie dem cURL-Befehlszeilentool oder der Chrome-Browsererweiterung von Postman zu erstellen. Sie können beispielsweise ein StyleBook mit dem Namen example-lb importieren, das zum Erstellen einer Load Balancer-Konfiguration auf einer Citrix ADC-Instanz verwendet werden kann.

HTTP-Methode: POST

URL: `http://<mas-ip>/stylebook/nitro/v1/config/stylebooks`

Kopfzeilen:

```
1  Content-Type: application/json
2  Accept: application/json
3  <!--NeedCopy-->
```

RequestBody:


```
{

       ”stylebook”:
  {

     ”file_name”: ”example-lb.yaml”,
     ”source”: ”<base64-contents>”,
     ”encoding”: ”base64”
   }

 }

<!--NeedCopy-->
```

Wo ist der Wert des Attributs “source” die Base64-Codierung des Inhalts Ihrer StyleBook-Datei. Sie können den YAML-Inhalt Ihrer StyleBook-Datei in ein Online-Tool einfügen, z. B.https://www.browserling.com/tools/file-to-base64 um die base64-Zeichenfolge zu erhalten, die Sie dann als Wert für das obige Attribut source verwenden können.

Mit diesem API-Aufruf können Sie auch eine komprimierte Tarball-Datei (TGZ-Datei) hochladen, die mehrere StyleBook-Dateien in einem API-Vorgang enthält. Ändern Sie dazu einfach das Dateiname-nattribut in den .tgz-Dateinamen und den Wert für das Quellattribut in die Base64-Codierung des Inhalts Ihrer tgz-Datei.

Nachdem die API erfolgreich im Tool ausgeführt wurde, erhalten Sie die folgende Antwort, die angibt, dass das StyleBook in Citrix ADM importiert wurde.

```
200 OK
<!--NeedCopy-->
```

Antworttext:

```
{


  ”stylebook”:
{


    ”name”: ”example-lb”,

```



```
10      "namespace": "com.example.stylebook",
11
12      "version": "1.0"
13
14    }
15
16
17  }
18
19 <!--NeedCopy-->
```

Verwenden der API zum Herunterladen benutzerdefinierter StyleBooks

April 28, 2021

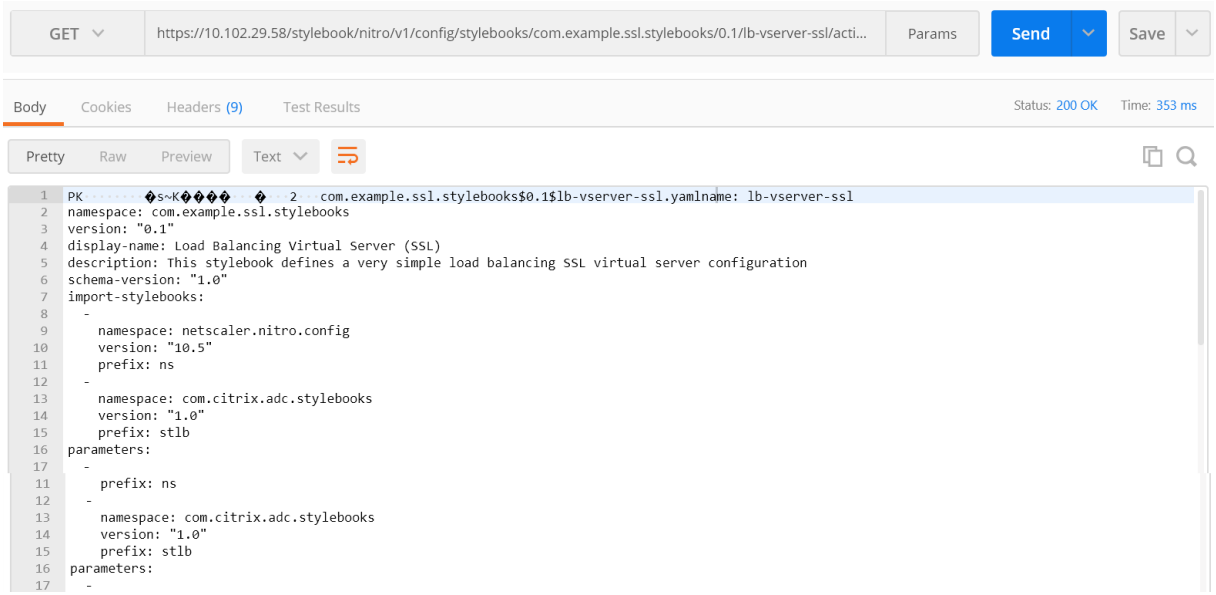
Sie können ein benutzerdefiniertes StyleBook herunterladen, indem Sie die folgende StyleBooks REST-API bereitstellen:

GET https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>/actions/download

Sie können die API in jedem Tool wie dem cURL-Befehlszeilentool ausführen. Oder Sie können die Chrome-Browsererweiterung von Postman verwenden, nachdem Sie die Felder IP-Adresse, Name, Version und Namespace geändert haben.

GEThttps://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-vserver-ssl/actions/download

Das StyleBook im Format.yaml wird heruntergeladen.



Verwenden der API zum Löschen benutzerdefinierter StyleBooks

April 28, 2021

Sie können das benutzerdefinierte StyleBook löschen, indem Sie die folgende StyleBooks REST-API bereitstellen:

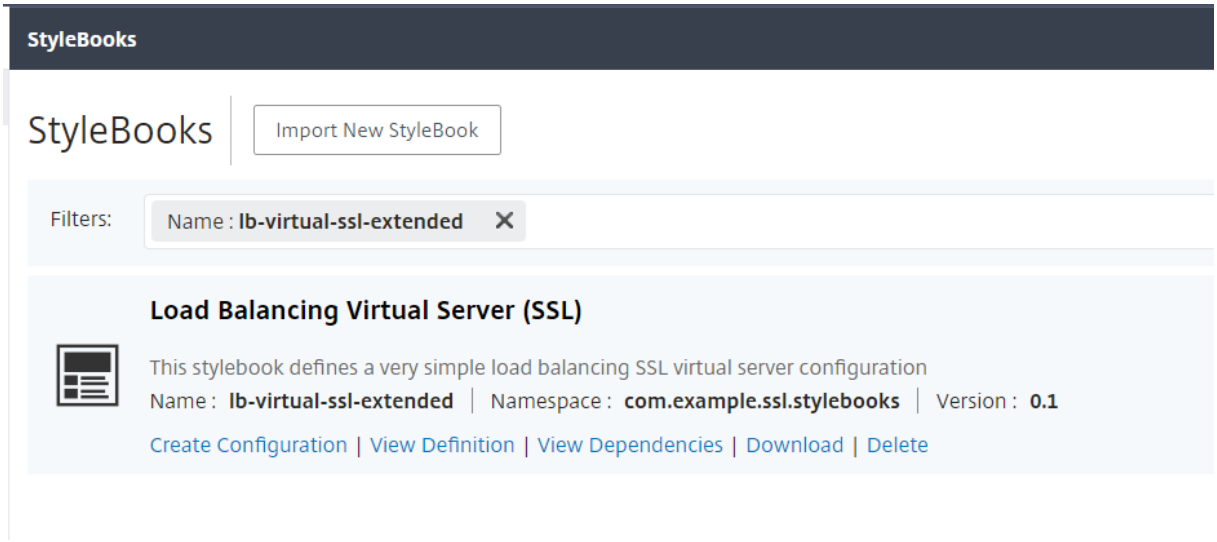
DELETE `https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>?dependencies=true`

Wenn der Abfrageparameter für Abhängigkeiten in der URL nicht angegeben wird oder sein Wert auf false festgelegt ist, werden die StyleBook-Abhängigkeiten nicht gelöscht. Und nur das StyleBook wird gelöscht.

Wenn Sie einen HTTP-Antwortstatuscode von 200 erhalten, bedeutet dies, dass das benutzerdefinierte StyleBook und seine Abhängigkeiten erfolgreich aus Citrix Application Delivery Management (ADM) entfernt wurden.

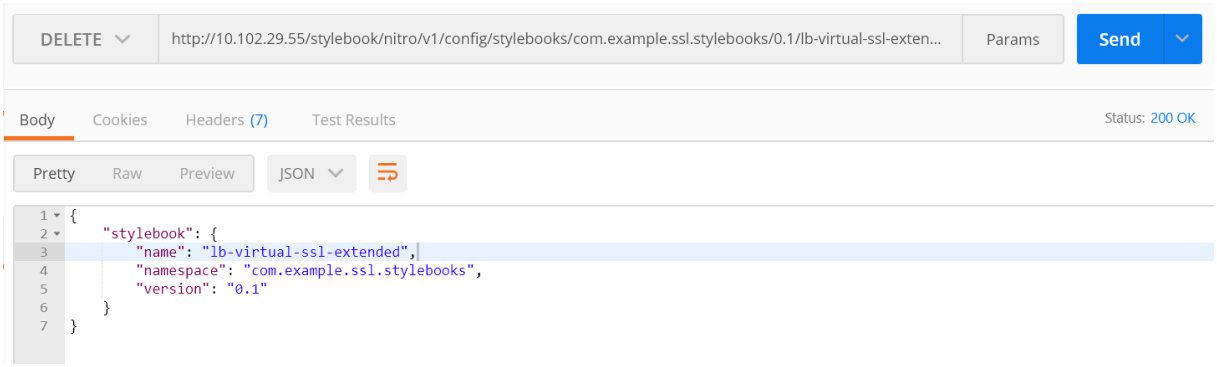
> **Hinweis:**
>
> Sie können kein benutzerdefiniertes StyleBook löschen, das andere StyleBooks in MA Service enthält, die davon abhängen.

Nehmen wir beispielsweise an, Sie haben ein StyleBook mit dem Namen `lb-virtual-ssl-extended` in Citrix ADM erstellt. Sie haben sich später entschieden, dieses StyleBook zu löschen.

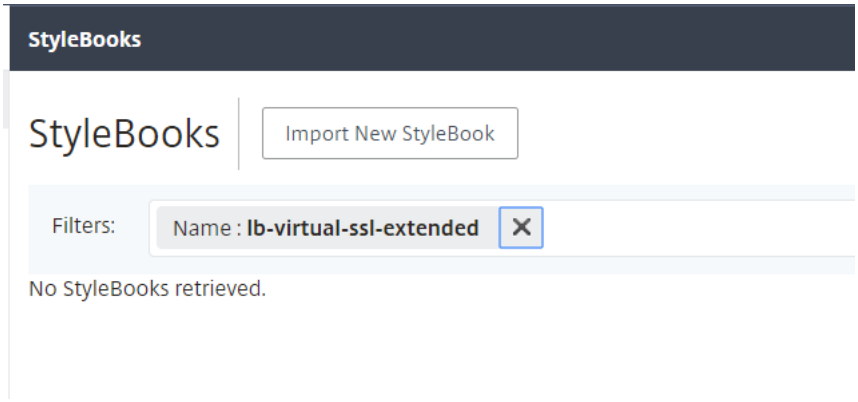


Sie können die API in jedem Tool wie dem cURL-Befehlszeilentool ausführen. Sie können auch die Chrome-Browsererweiterung von Postman verwenden, nachdem Sie die Felder IP-Adresse, Name, Version und Namespace geändert haben.

DELETE https://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=false



Das StyleBook wird aus Citrix ADM gelöscht.



StyleBooks Grammatik

April 28, 2021

Sie können Ihre eigenen StyleBooks entwerfen, in Citrix Application Delivery Management (ADM) importieren und sie dann verwenden, um Konfigurationen entweder mit der Citrix ADM GUI oder mithilfe von APIs zu erstellen. Um eigene StyleBooks erstellen zu können, müssen Sie zunächst die Grammatik und Syntax der verschiedenen Konstrukte und Attribute verstehen, die Sie verwenden können.

Dieses Dokument beschreibt die verschiedenen Konstrukte und Referenzen, die Sie beim Erstellen von StyleBooks verwenden können.

Klicken Sie in der folgenden Tabelle auf einen Abschnitts-, Konstruktions- oder Referenznamen, um die Details anzuzeigen.

Überschrift	Importieren von StyleBooks
Parameter	Parameters-Default-Sources-Konstrukt
Ersetzungen	Komponenten
Optionale Eigenschaften	Hilfskomponenten
Eigenschaftenstandardquellen	Verschachtelte Komponenten
Konditionskonstrukt	Konstrukt wiederholen
Konstrukt für Wiederholungsbedingung	Ausgaben
Verschachtelte Wiederholungen	Übergeordnete Referenz
Parameterreferenz	Substitutionsreferenz
Komponentenreferenz	Vorgänge
Variablenreferenz	Alarme
Analytics	Integrierte Funktionen
Ausdrücke	Abhängigkeitserkennung
In-Place-Interpolationen	

> **Hinweis**
>
> While defining `repeat-item`, `repeat-index`, or arguments to substitution functions, do not use the following reserved words to name a user-defined variable, `$<var-name>`
>
> - StyleBook, Parameter, Substitutionen, Komponenten, Eigenschaften, Ausgaben, Eltern, Selbst, Betrieb, Analytik, Alarme
> - repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
> - repeat-index, repeat-index-0, repeat-index-1, repeat-index-2
> - Standard
> - roles, role, targets, target

- context, parent-context, parent_context

Informationen und Beispiele zum Entwerfen eigener StyleBooks finden Sie unter So erstellen Sie Ihre eigenen StyleBooks.

Überschrift

April 28, 2021

Die ersten sechs Zeilen eines StyleBook bilden den Kopfbereich. In diesem Abschnitt können Sie die Identität eines StyleBook definieren und beschreiben, was es tut. Dies ist ein obligatorischer Abschnitt.

In der folgenden Tabelle werden die Attribute des Kopfzeilenabschnitts beschrieben:

Attribut	Beschreibung
Name	Ein Name zum Identifizieren des StyleBook. Dieses Attribut ist obligatorisch.
Beschreibung	Eine Beschreibung, die definiert, was ein StyleBook tut. Diese Beschreibung wird auf der Benutzeroberfläche von Citrix Application Delivery Management (ADM) angezeigt. Dies ist ein optionales Attribut.
Anzeigename	Ein beschreibender Name für das StyleBook. Dieser Name wird auf der Citrix ADM GUI angezeigt. Dies ist ein optionales Attribut.
Autor	Die Autorenperson oder Organisation, die das StyleBook erstellt. Dies ist ein optionales Attribut.

Attribut	Beschreibung
Namensraum	Ein Namespace ist Teil eines eindeutigen Bezeichners für ein StyleBook, um Namenskollisionen zu vermeiden. Ein Namespace kann eine beliebige Zeichenfolge sein, aber es empfiehlt sich, ihn für die Benennung der Firma, Abteilung oder Einheit zu verwenden, die einen Satz von StyleBooks erstellt oder besitzt. Beispielsweise können Sie das folgende Format verwenden: `<company>.<department>.<unit>.stylebooks`. Dies ist ein obligatorisches Attribut.
version	Die Versionsnummer des StyleBook. Sie können die Versionsnummer ändern, wenn Sie ein StyleBook aktualisieren. StyleBooks verschiedener Versionen können zusammen existieren. Dies ist ein obligatorisches Attribut.
Schema-Version	Die Version des StyleBooks-Schemas. Es nimmt den Wert “1.0” in der aktuellen Version von Citrix ADM. Dies ist ein obligatorisches Attribut.
private	Wenn dieses Attribut auf true gesetzt ist, wird das StyleBook nicht auf der Citrix ADM GUI angezeigt. Dies ist eine nützliche Einstellung für StyleBooks, die Bausteine für andere StyleBooks sind und nicht für die direkte Verwendung von Benutzern bestimmt sind. Dies ist ein optionales Attribut. Der Standardwert ist false.

Beispiel:

```
1     name: lb
2
3     description: ”This stylebook defines a sample load balancing
          configuration.”
4
```



```
    display-name: "Load Balancing StyleBook (HTTP)"

    author: Mike Smith (ACME Infra team)

    namespace: com.example.stylebooks

    schema-version: "1.0"

    version: "0.1"
<!--NeedCopy-->
```

Die Kombination aus Name, Namespace und Version identifiziert ein StyleBook im System eindeutig. Sie können nicht zwei StyleBooks mit derselben Kombination aus Name, Namespace und Version in Citrix ADM verwenden. Sie können jedoch zwei StyleBooks mit demselben Namen und derselben Version, aber unterschiedlichen Namespaces oder mit demselben Namespace und derselben Version, aber unterschiedlichen Namen haben.

Importieren von StyleBooks

April 28, 2021

Dies ist der zweite Abschnitt Ihres StyleBook und können Sie erklären, auf welches andere StyleBook Sie aus Ihrem aktuellen StyleBook verweisen möchten. Auf diese Weise können Sie andere StyleBooks importieren und wiederverwenden, anstatt dieselbe Konfiguration in Ihrem eigenen StyleBook neu zu erstellen. Dies ist ein obligatorischer Abschnitt.

Sie müssen den **Namespace** und die **Versionsnummer** der StyleBook (s) deklarieren, auf die Sie in Ihrem aktuellen StyleBook verweisen möchten. Jedes StyleBook muss auf den Namespace netscaler.nitro.config verweisen, wenn es eines der NITRO-Konfigurationsobjekte direkt verwendet. Dieser Namespace enthält alle Citrix ADC NITRO-Typen, wie `lbvserver` Dienst oder Monitor. StyleBooks für Citrix ADC Versionen 10.5 und höher werden unterstützt. Das bedeutet, dass Sie mit Ihrem StyleBook Konfigurationen auf jeder Citrix ADC-Instanz erstellen und ausführen können, auf der Version 10.5 oder höher ausgeführt wird.

Das **Präfixattribut**, das im Abschnitt import-stylebooks verwendet wird, ist eine Kurzschrift, um auf die Kombination von Namespace und Version zu verweisen. Zum Beispiel kann das Präfix ns verwendet werden, um auf den Namespace netscaler.nitro.config mit Version 10.5 zu verweisen. In den späteren Abschnitten Ihres StyleBook können Sie nicht jedes Mal, wenn Sie auf ein StyleBook mit diesem Namespace und Version verweisen möchten, einfach die Präfixzeichenfolge verwenden, die zusammen mit dem Namen des StyleBook ausgewählt wurde, um sie eindeutig zu identifizieren.

Beispiel:


```
      import-stylebooks:
       -
         namespace: netscaler.nitro.config
         version: ”10.5”
         prefix: ns
      -
         namespace: com.acme.stylebooks
         version: ”0.1”
         prefix: stlb
<!--NeedCopy-->
```

In diesem Beispiel heißt das erste definierte Präfix ns und bezieht sich auf den Namespace netscaler.nitro.config und Version 10.5. Das zweite definierte Präfix heißt `stlb`und bezieht sich auf den Namespace com.acme.stylebooks und Version 0.1.

Nachdem Sie ein Präfix definiert haben, können Sie jedes Mal, wenn Sie auf einen Typ oder ein StyleBook verweisen möchten, das zu einem bestimmten Namespace und einer bestimmten Version gehört, die Notation ⊠<namespace-shorthand> verwenden <type-name>. Zum Beispiel bezieht sich **ns⊠ lbvserver** auf den Typ `lbvserver`, der im Namespace netscaler.nitro.config, Version 10.5, definiert ist.

Wenn Sie im Namespace com.acme.stylebooks auf ein StyleBook mit der Version “0.1” verweisen möchten, können Sie die Notation **stlb::<stylebook-name>** verwenden.

> **Hinweis**
>
> Konventionsgemäß wird das Präfix ns verwendet, um auf den NITRO-Namespace von Citrix ADC zu verweisen.

Parameter

April 28, 2021

In diesem Abschnitt können Sie alle Parameter definieren, die Sie in Ihrem StyleBook benötigen, um eine Konfiguration zu erstellen. Es beschreibt die Eingabe, die Ihr StyleBook nimmt. Obwohl dieser Abschnitt optional ist, benötigen die meisten StyleBook möglicherweise einen. Sie können den Abschnitt Parameter in Betracht ziehen, um die Felder für die Benutzer zu definieren, die das StyleBook zum Erstellen einer Konfiguration auf einer Citrix ADC-Instanz verwenden.

Wenn Sie Ihr StyleBook in Citrix ADM importieren und zum Erstellen einer Konfiguration verwenden, verwendet die GUI diesen Abschnitt des StyleBook, um ein Formular anzuzeigen. Dieses Formular nimmt eine Eingabe für die definierten Parameterwerte an.

Im folgenden Abschnitt werden die Attribute beschrieben, die Sie für jeden Parameter in diesem Abschnitt angeben müssen:

‘name’

Der Name des Parameters, den Sie definieren möchten. Sie können einen alphanumerischen Namen angeben.

Der Name muss mit einem Alphabet beginnen und kann mehr Alphabete, Zahlen, Bindestriche (-) oder Unterstriche (_) enthalten.

Wenn Sie ein StyleBook schreiben, können Sie dieses Attribut “name” verwenden, um mithilfe der Notation $parameters auf den Parameter in anderen Abschnitten zu verweisen. <name>.

Obligatorisch? Ja

‘label’

Eine Zeichenfolge, die in der ADM-GUI als Name dieses Parameters angezeigt wird.

Obligatorisch? Nein

‘description’

Eine Hilfe-Zeichenfolge, die beschreibt, wofür der Parameter verwendet wird. Die ADM-GUI zeigt diesen Text an, wenn der Benutzer auf das Hilfesymbol für diesen Parameter klickt.

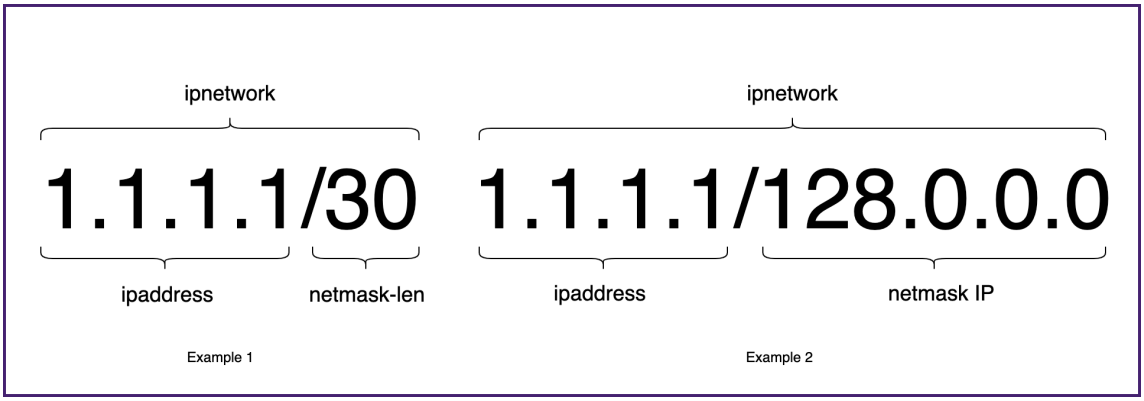
Obligatorisch? Nein

‘type’

Die Art des Wertes, den diese Parameter annehmen können. Parameter können von einem der folgenden integrierten Typen sein:

- `string`: Eine Reihe von Zeichen. Wenn keine Länge angegeben wird, kann der Zeichenfolgenwert beliebig viele Zeichen annehmen. Sie können jedoch die Länge eines String-Typs einschränken, indem Sie die Attribute min-length und max-length verwenden.
- `number`: Eine ganze Zahl. Sie können die minimale und maximale Anzahl angeben, die dieser Typ annehmen kann, indem Sie die Attribute min-value und max-value verwenden.
- **`boolean`**: Kann entweder wahr oder falsch sein. YAML betrachtet alle Literale als Boolesche (zum Beispiel Ja oder Nein).
- `ipaddress`: Eine Zeichenfolge, die eine gültige IPv4- oder IPv6-Adresse darstellt.

- `ipnetwork`: Es besteht aus zwei Teilen. Der erste Teil ist die IP-Adresse und der zweite Teil ist die Netzmaske.



  Die Netzmaske wird durch eine Netzmaske length (`netmask-len`) oder Netmask-IP-Adresse (`netmask_ip`) dargestellt. Die Netzmaskenlänge ist eine Ganzzahl zwischen 0-32 und 0-128 für eine IPv6-Adresse. Es wird verwendet, um die Anzahl der IP-Adressen in einem Netzwerk zu bestimmen.

- `tcp-port`: Eine Zahl zwischen 0 und 65535, die einen TCP- oder UDP-Port repräsentiert.
- `password`: Repräsentiert einen undurchsichtigen/geheimen String-Wert. Wenn die ADM-GUI einen Wert für diesen Parameter anzeigt, wird sie als Sternchen (*****) angezeigt.
- `certfile`: Repräsentiert eine Zertifikatdatei. Mit diesem Wert können Sie die Dateien direkt von Ihrem lokalen System hochladen, wenn Sie eine StyleBook-Konfiguration mit der ADM-GUI erstellen. Die hochgeladene Zertifikatsdatei wird im Verzeichnis `/var/mps/tenants/\<tenant_path>/ns_ssl_certs` in ADM gespeichert.

  Die Zertifikatsdatei wird der Liste der von ADM verwalteten Zertifikate hinzugefügt.

- `keyfile`: Repräsentiert eine Zertifikatschlüsseldatei. Mit diesem Wert können Sie die Datei direkt von Ihrem lokalen System hochladen, wenn Sie eine StyleBook-Konfiguration mit der ADM-GUI erstellen. Die hochgeladene Zertifikatsdatei wird im Verzeichnis `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` in ADM gespeichert.

  Die Zertifikatschlüsseldatei wird zur Liste der von ADM verwalteten Zertifikatschlüssel hinzugefügt.

- `file`: Repräsentiert eine Datei.
- `object`: Dieser Typ wird verwendet, wenn Sie mehrere verwandte Parameter unter einem übergeordneten Element gruppieren möchten. Geben Sie den übergeordneten Parameter den Typ als “Objekt” an. Ein Parameter vom Typ object kann einen verschachtelten Abschnitt parameter haben, um die darin enthaltenen Parameter zu beschreiben.
- `another StyleBook`: Wenn Sie diesen Parametertyp verwenden, erwartet dieser Parameter, dass sein Wert in Form der Parameter vorliegt, die im StyleBook definiert sind und seinen Typ

angibt.

Ein Parameter kann auch eine `type` die Liste der Typen haben. Fügen Sie dazu `[]` am Ende des Typs hinzu. Wenn das `type` Attribut beispielsweise lautet `string[]`, verwendet dieser Parameter eine Liste von Strings als Eingabe. Sie können eine, zwei oder mehrere Strings für diesen Parameter angeben, wenn Sie eine Konfiguration aus diesem StyleBook erstellen.

Obligatorisch? Ja

'network'

Für können Sie das `network` Attribut angeben `type: ipaddress`, um eine IP-Adresse automatisch aus einem ADM IPAM-Netzwerk zuzuweisen.

ADM weist automatisch eine IP-Adresse aus dem `network`Attribut zu, wenn Sie eine StyleBook-Konfiguration erstellen.

Beispiel:

```
        name: virtual-ip
        label: "Load Balancer IP Address"
        type: ipaddress
        network: "network-1"
        required: true
<!--NeedCopy-->
```

In diesem Beispiel weist das `virtual-ip` Feld automatisch eine IP-Adresse von zu `network-1`. Die IP-Adresse wird beim Löschen der Konfiguration wieder an das Netzwerk freigegeben.

'dynamic-allocation'

Das `dynamic-allocation` Attribut wird in der Parameterdefinition von hinzugefügt `type: ipaddress`. Verwenden Sie dieses Attribut, um die ADM IPAM-Netzwerke dynamisch aufzulisten. Dieses Attribut kann entweder **`true`** oder **`false`** als Eingabe verwendet werden. Geben Sie für das `dynamic-allocation: true` Attribut an `type: ipaddress`, um die ADM IPAM-Netzwerke, die sich in ADM befinden, dynamisch aufzulisten. Im Formular zur Erstellung von Konfigurationspakets können Sie Folgendes tun:

1. Wählen Sie das erforderliche IPAM-Netzwerk aus der Liste aus.
2. Geben Sie eine IP-Adresse an, die Sie aus dem ausgewählten IPAM-Netzwerk zuweisen möchten.

   Wenn keine IP-Adresse angegeben ist, weist der ADM automatisch eine IP-Adresse aus dem ausgewählten IPAM-Netzwerk zu.

Beispiel:

```
1   -
2     name: virtual-ip
3     label: "Load Balancer IP Address"
4     type: ipaddress
5     dynamic-allocation: true
6     required: true
7  <!--NeedCopy-->
```

In diesem Beispiel listet das `virtual-ip` Feld die ADM IPAM-Netzwerke auf, die sich in ADM befinden. Wählen Sie ein Netzwerk aus der Liste aus, um eine IP-Adresse automatisch aus dem Netzwerk zuzuweisen. Die IP-Adresse wird beim Löschen der Konfiguration wieder an das Netzwerk freigegeben.

'key'

Geben Sie true oder false an, um anzugeben, ob dieser Parameter ein Schlüsselparameter für das StyleBook ist.

Ein StyleBook kann nur einen Parameter als key -Parameter definiert haben.

Wenn Sie aus demselben StyleBook (auf derselben oder
anderen ADC-Instanzen) unterschiedliche Konfigurationen erstellen, weist jede Konfiguration einen anderen/eindeutigen Wert für diesen
Parameter auf.

Der Standardwert ist false.

Obligatorisch? Nein

'required'

Geben Sie true oder false an, um anzugeben, ob ein Parameter obligatorisch oder optional ist. Wenn es auf true
gesetzt ist, ist der Parameter obligatorisch und der Benutzer muss beim Erstellen von Konfigurationen einen Wert für diesen
Parameter angeben.

Die ADM-GUI zwingt den Benutzer, einen gültigen Wert für diesen Parameter anzugeben.

Der Standardwert ist false.

Obligatorisch? Nein

‘allowed-values’

Verwenden Sie dieses Attribut, um eine Liste gültiger Werte für einen Parameter zu definieren, wenn der Typ auf string gesetzt ist.

Beim Erstellen einer Konfiguration über die ADM-GUI wird der Benutzer aufgefordert, einen Parameterwert aus dieser Liste auszuwählen. Diese Liste ist statisch, der Benutzer kann nur einen Wert aus der Liste auswählen. Wenn Sie dem Benutzer gestatten möchten, Werte zur Liste hinzuzufügen, verwenden Sie das Attribut [allow-**new**-values] (#allow -new-values).

> **Hinweis**
>
> Wenn Sie die Listenwerte als Radio-Optionen anzeigen möchten, legen Sie das Attribut [layout] (#layout) fest.

Beispiel 1:

```
-
      name: ipaddress
      type: string
      allowed-values:
            -  SOURCEIP
            -  DEST IP
            -  NONE
<!--NeedCopy-->
```

Beispiel 2:

```
-
      name: TCP Port
      type: tcp-port
      allowed-values:
            -  80
            -  81
            -  8080
<!--NeedCopy-->
```

Beispiel 3:

Liste von tcp-ports, in der jedes Element der Liste nur Werte in angegeben haben kann allowed-values.


```
-
      name: tcpports
      type: tcp-port[]
      allowed-values:
            -  80
            -  81
            -  8080
            -  8081
<!--NeedCopy-->
```

Obligatorisch? Nein

‘allow-new-Werte’

Verwenden Sie dieses Attribut, um eine dynamische Liste für einen Parameter hinzuzufügen. Beim Erstellen oder Aktualisieren einer Konfiguration über die ADM-GUI kann der Benutzer der Liste Werte hinzufügen.

Geben Sie “true” an, wenn der Benutzer der Parameterliste einen Wert hinzufügen soll. Sie können die `allowed-values` Attribute `allow-new-values` und in einer Kombination verwenden. Diese Kombination ermöglicht es Ihnen, eine Liste von vorgeschlagenen Werten für einen Parameter zu definieren und neue Werte zu akzeptieren.

```
-
      name: port
      type: tcp-port
      allowed-values:
            -  80
            -  81
            -  8080
      allow-new-values: true
<!--NeedCopy-->
```

In diesem Beispiel kann ein Benutzer entweder aus 80, 81, 8080 auswählen oder `port` beim Erstellen oder Aktualisieren eines Konfigurationspakets einen neuen Wert für den Parameter eingeben.

‘default’

Verwenden Sie dieses Attribut, um einem optionalen Parameter einen Standardwert zuzuweisen. Wenn ein Benutzer eine Konfiguration erstellt, ohne einen Wert anzugeben, wird der Standardwert verwendet.

Der Parameter nimmt keinen Wert an, wenn die folgenden Bedingungen erfüllt sind:

- Der Parameter hat keinen Standardwert.
- Ein Benutzer gibt keinen Wert für den Parameter an.

Beispiel 1:

```
-
      name: timeout
      type: number
      default: 20
<!--NeedCopy-->
```

Beispiel 2:

So listen Sie die Standardwerte des Parameters auf:

```
-
      name: protocols
      type: string[]
      default:
            - TCP
            - UDP
            - IP
<!--NeedCopy-->
```

Beispiel 3:

```
-
      name: timeout
      type: number
      default: 20
<!--NeedCopy-->
```

Beispiel 4:

```
-
      name: tcpport
      type: tcp-port
      default: 20
```



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

Obligatorisch? Nein

‘pattern’

Verwenden Sie dieses Attribut, um ein Muster (regulärer Ausdruck) für die gültigen Werte dieses Parameters zu definieren, wenn der Typ des Parameters string ist.

Beispiel:

```
-
      name: appname
      type: string
      pattern: ”[a-z]+”
<!--NeedCopy-->
```

Obligatorisch? Nein

‘min-value’

Verwenden Sie dieses Attribut, um den Mindestwert für Parameter vom Typ `number` oder zu definieren `tcp-port`.

Beispiel:

```
-
      name: audio-port
      type: tcp-port
      min-value: 5000
<!--NeedCopy-->
```

Die `min-value` Zahlen können negativ sein. Das `min-value` Für `tcp-port` muss jedoch positiv sein.

Obligatorisch? Nein

‘max-value’

Verwenden Sie dieses Attribut, um den Höchstwert für Parameter vom Typ `number` oder zu definieren `tcp-port`.

Stellen Sie sicher, dass der Maximalwert größer als der Mindestwert ist, falls definiert.

Beispiel:

```
-
      name: audio-port
      type: tcp-port
      min-value: 5000
      max-value: 15000
<!--NeedCopy-->
```

Obligatorisch? Nein

‘min-length’

Verwenden Sie dieses Attribut, um die Mindestlänge der Werte zu definieren, die für einen Parameter vom
Typ string akzeptiert werden.

Stellen Sie sicher, dass die Mindestlänge der Zeichen definiert ist, die größer oder gleich Null sind.

Beispiel:

```
-
      name: appname
      type: string
      min-length: 3
<!--NeedCopy-->
```

Obligatorisch? Nein

‘max-length’

Verwenden Sie dieses Attribut, um die maximale Länge der Werte zu definieren, die für einen Parameter vom
Typ string akzeptiert werden.

Stellen Sie sicher, dass die maximale Länge der Werte größer oder gleich der Länge der in definierten Zeichen ist `min-length`.

Beispiel:


```
-
      name: appname
      type: string
      max-length: 64
<!--NeedCopy-->
```

Obligatorisch? Nein

‘min-items’

Verwenden Sie dieses Attribut, um die Mindestanzahl von Elementen in einem Parameter zu definieren, der eine Liste ist.

Stellen Sie sicher, dass die Mindestanzahl von Elementen größer oder gleich Null ist.

Beispiel:

```
-
      name: server-ips
      type: ipaddress[]
      min-items: 2
<!--NeedCopy-->
```

Obligatorisch? Nein

‘max-items’

Verwenden Sie dieses Attribut, um die maximale Anzahl von Elementen in einem Parameter zu definieren,
der eine Liste ist.

Stellen Sie sicher, dass die maximale Anzahl von Artikeln größer ist als die Mindestanzahl von Elementen, falls definiert.

Beispiel:

```
-
      name: server-ips
      type: ipaddress[]
      min-items: 2
      max-items: 250
<!--NeedCopy-->
```


Obligatorisch? Nein

‘gui’

Verwenden Sie dieses Attribut, um das Layout des Parameters in der ADM-GUI anzupassen.

Obligatorisch? Nein

‘columns’

Dieses Attribut ist ein Unterattribut des `gui` Attributs. Verwenden Sie dieses Attribut, um die Anzahl der Spalten zu definieren, die die `type: object[]`Parameter in der ADM-GUI anzeigen.

Obligatorisch? Nein

‘updatable’

Dieses Attribut ist ein Unterattribut des `gui` Attributs. Verwenden Sie dieses Attribut, um anzugeben, ob der Parameter nach dem Erstellen der Konfiguration aktualisiert werden kann. Legen Sie dieses Attribut nur für einfache Parametertypen wie String, Boolesch oder Zahl fest.

Wenn der Wert auf festgelegt ist **`false`**, ist das Parameterfeld beim Aktualisieren der Konfiguration abgeblendet.

Obligatorisch? Nein

‘collapse_pane’

Dieses Attribut ist ein Unterattribut des `gui` Attributs. Verwenden Sie dieses Attribut, um anzugeben, ob der Bereich, der das Layout dieses Objektparameters definiert, zusammenlegbar ist.

Wenn der Wert auf true gesetzt ist, kann der Benutzer die untergeordneten Parameter unter diesem übergeordneten Parameter erweitern oder reduzieren.

Beispiel:

```
gui:

 collapse_pane: true

 columns: 2
<!--NeedCopy-->
```


Beispiel für einen vollständigen Parameterabschnitt:

```
parameters:

   -

      name: name

      label: Name

      description: Name of the application

      type: string

      required: true

   -

      name: ip

      label: IP Address

      description: The virtual IP address used for this application

      type: ipaddress

      required: true

   -

      name: svc-servers

      label: Servers

      type: object[]

      required: true

      parameters:

        -

              name: svc-ip
```



```
42
43              label: Server IP
44
45              description: The IP address of the server
46
47              type: ipaddress
48
49              required: true
50
51          -
52
53              name: svc-port
54
55              label: Server Port
56
57              description: The TCP port of the server
58
59              type: tcp-port
60
61              default: 80
62
63          -
64
65              name: lb-alg
66
67              label: LoadBalancing Algorithm
68
69              type: string
70
71              allowed-values:
72
73                 - ROUNDROBIN
74
75                 - LEASTCONNECTION
76
77              default: ROUNDROBIN
78
79          -
80
81              name: enable-healthcheck
82
83              label: Enable HealthCheck?
84
85              type: boolean
86
```



```
                default: true
<!--NeedCopy-->
```

Im Folgenden finden Sie ein Beispiel, das alle Attribute einer Liste und die in früheren Abschnitten erläuterten Werte definiert:

```
        -
                name: features-list

                type: string[]

                min-length: 1

                max-length: 3

                min-items: 1

                max-items: 3

                pattern: "[A-Z]+"

                allowed-values:

                  - SP

                  - LB

                  - CS

                default:

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

‘layout’

Dieses Attribut ist ein Unterattribut des `gui` Attributs. Verwenden Sie dieses Attribut, um die Listenwerte als Optionsfelder anzuzeigen. Legen Sie das `layout` Attribut `radio` im Parameterabschnitt einer StyleBook-Definition fest. Sie gilt für den Parameter, der das [`allowed-values`] (#allowed -values) -Attribut besitzt. Wenn Sie ein Konfigurationspaket erstellen, zeigt die ADM-GUI die Werte in der `allowed-values` Liste als Optionsfelder an.

Beispiel:

```
-
    gui:
        layout: radio
    allowed-values:
        - One
        - Two
        - Three
<!--NeedCopy-->
```

Die Werte Eins, Zwei und Drei werden als Optionsfelder in der ADM-GUI angezeigt.

‘dependent-parameter’

Dieses Attribut ist ein Unterattribut des `gui` Attributs. Es steuert dynamisch das Aussehen des Parameters oder seinen Anfangswert im StyleBook-Konfigurationsformular basierend auf dem in einem anderen Parameter angegebenen Wert.

Geben Sie dieses Attribut für einen Quellparameter an, der das Verhalten des Parameters im Formular steuert. Sie können mehrere Bedingungen einbeziehen, die andere Parameter steuern. Beispielsweise `protocol` kann ein Quellparameter einen dependent-Parameter haben, der nur angezeigt wird `certificate`, wenn der `protocol` Parameterwert lautet `SSL`.

Jede Bedingung kann die folgenden Attribute haben:

- **target-parameter**: Geben Sie den Zielparameter an, für den diese Bedingung gilt.
- **Matching-Werte**: Geben Sie die Liste der Werte des Quellparameters an, der die Aktion auslöst.
- **action**: Geben Sie eine der folgenden Aktionen für den Zielparameter an:
  - `read-only`: Der Parameter wird schreibgeschützt.
  - `show`: Der Parameter wird im Formular angezeigt, wenn er ausgeblendet ist.
  - `hide`: Der Parameter wird aus dem Formular entfernt.
  - `set-value`: Der Parameterwert wird auf den im value-Attribut angegebenen Wert festgelegt.
- **value**: Der Wert des Zielparameters, wenn die Aktion ist `set-value`.

Wenn eine Benutzereingabe den angegebenen Werten für den Quellparameter entspricht, ändert sich das Aussehen oder der Wert des Zielparameters entsprechend der angegebenen Aktion.

Beispiel:


```
-
   name: lb-virtual-port
   label: "Load Balanced App Virtual Port"
   description: "TCP port representing the Load Balanced application"
   type: tcp-port
   gui:
     updatable: false
     dependent-parameters:
           -
             matching-values:
               - 80
             target-parameter: $parameters.lb-service-type
             action: set-value
             allowed-values:
             - HTTP
             - TCP
             - UDP

   default: 80

<!--NeedCopy-->
```

In diesem Beispiel wird der abhängige Parameter unter dem `lb-virtual-port` Parameter (Quellparameter) angegeben.

Wenn der Quellparameterwert auf festgelegt ist `80`, löst der `lb-service-type` Parameter die `set-value` Aktion aus. Infolgedessen kann ein Benutzer eine der folgenden Optionen auswählen:

- HTTP
- TCP
- UDP

Parameters-Default-Sources-Konstrukt

April 28, 2021

Sie können dieses Konstrukt verwenden, um Parameterdefinitionen aus anderen StyleBooks wiederzuverwenden.

Betrachten Sie ein Szenario, in dem ein Parameter oder eine Gruppe von Parametern wiederholt in mehreren StyleBooks verwendet wird. Um diese Parameter nicht neu zu definieren, können Sie sie jedes Mal, wenn Sie ein neues StyleBook erstellen möchten, einmal definieren und dann ihre

Definitionen in die StyleBooks importieren, die diese Parameter benötigen, indem Sie das Konstrukt **parameters-default-sources** verwenden.

Wenn beispielsweise viele Ihrer StyleBooks eine virtuelle IP konfigurieren müssen, müssen Sie möglicherweise dieselben Parameter für virtuelle IPs in jedem neuen StyleBook definieren, das Sie erstellen. Stattdessen können Sie ein separates StyleBook mit dem Namen erstellen, in `vip-params` dem Sie beispielsweise alle damit verbundenen Parameter definieren, wie im folgenden Beispiel gezeigt:

```
1      -
2
3      name: vip-params
4
5      namespace: com.acme.commontypes
6
7      version: ”1.0”
8
9      description: This StyleBook defines a typical virtual IP config.
10
11     private: true
12
13     schema-version: ”1.0”
14
15     parameters:
16
17       -
18
19            name: lb-appname
20
21            label: Load Balanced Application Name
22
23           description: Name of the Load Balanced application
24
25            type: string
26
27            required: true
28
29       -
30
31            name: lb-virtual-ip
32
33            label: Load Balanced App Virtual IP address
34
```



```
35              description: Virtual IP address representing the Load
                    Balanced application
36
37              type: ipaddress
38
39              required: true
40
41          -
42
43              name: lb-virtual-port
44
45              label: Load Balanced App Virtual Port
46
47              description: TCP port representing the Load Balanced
                    application
48
49              type: tcp-port
50
51              default: 80
52
53          -
54
55              name: lb-service-type
56
57              label: Load Balanced App Protocol
58
59              description: Protocol used for the Load Balanced application
                    .
60
61              type: string
62
63              default: HTTP
64
65              required: true
66
67              allowed-values:
68
69                   - HTTP
70
71                   - SSL
72
73                   - TCP
74  <!--NeedCopy-->
```

Dann können Sie andere StyleBooks erstellen, die diese Parameter verwenden. Es folgt ein Beispiel

für ein solches StyleBook.

```
      -

      name: acme-biz-app

      namespace: com.acme.stylebooks

      version: ”1.0”

      description: This stylebook defines the Citrix ADC configuration
         for Biz App

      schema-version: ”1.0”

      import-stylebooks:

        -

           namespace: com.acme.commontypes

           prefix: cmtypes

           version: ”1.0”

      \*\*parameters-default-sources:\*\*

**            - cmtypes::vip-params**

      parameters:

          -

            name: monitorname

            label: Monitor Name

            description: Name of the monitor

            type: string

            required: true

```



```
41          -
42
43            name: type
44
45            label: Monitor Type
46
47            description: Type of the monitor
48
49            type: string
50
51            required: true
52
53            allowed-values:
54
55              - PING
56
57              - TCP
58
59              - HTTP
60
61              - HTTP-ECV
62
63              - TCP-ECV
64
65              - HTTP-INLINE
66  <!--NeedCopy-->
```

Im StyleBook werden zunächst der Namespace und die Version des `vip-params` StyleBook mithilfe des Abschnitts “Import-Stylebooks” importiert. `acme-biz-app` Dann wird das Gebäudemodul **Parameter-Default-sources** hinzugefügt, und der StyleBook-Name `vip-params` wird angegeben. Dieser Parameter hat den gleichen Effekt wie das Definieren der Parameter von `vip-params` StyleBook direkt in diesem StyleBook.

Sie können Parameter aus mehreren StyleBooks einbeziehen, da es sich bei den parameters-default-sources um eine Liste handelt und bei jedem Element in der Liste erwartet wird, dass es sich um ein StyleBook handelt.

Neben der Einbeziehung von Parametern aus anderen StyleBooks können Sie auch eigene Parameter definieren, indem Sie den Parameterbereich verwenden. Die vollständige Liste der Parameter des StyleBook ist die Kombination von Parametern aus anderen StyleBooks und Parametern, die in diesem StyleBook definiert sind. Daher bezieht sich der Ausdruck **$parameters** auf diese Kombination von Parametern.

Wenn ein Parameter sowohl in einem importierten StyleBook als auch im aktuellen StyleBook definiert ist, überschreibt die Definition im aktuellen StyleBook die aus einem anderen StyleBook

importierte Definition. Sie können diesen Ansatz effektiv verwenden, indem Sie bei Bedarf einige der importierten Parameter anpassen und dabei die restlichen importierten Parameter verwenden.

Das Konstrukt parameters-default-sources kann auch in verschachtelten Parametern verwendet werden, wie gezeigt:

```
parameters:

    -

      name: vip-details

      label: Virtual IP details

      description: Details of the Virtual IP

      type: object

      required: true

      parameters-default-sources:

              - cmtypes::vip-params
<!--NeedCopy-->
```

Dieser Ansatz ähnelt dem `vip-params` Hinzufügen der Parameter des StyleBook direkt als untergeordnete Parameter des `vip-details` Parameters in diesem StyleBook.

Ersetzungen

April 28, 2021

Der Substitutionsabschnitt wird verwendet, um Kurzzeichennamen für komplexe Ausdrücke zu definieren, die im Rest des StyleBook verwendet werden können, um das Lesen des StyleBook zu erleichtern. Sie sind auch nützlich, wenn der gleiche Ausdruck oder Wert mehrmals im StyleBook wiederholt wird, z. B. ein konstanter Wert. Wenn Sie einen Ersetzungsnamen für diesen Wert verwenden, können Sie nur den Ersetzungswert aktualisieren, wenn dieser Wert geändert werden muss, anstatt ihn an jedem im StyleBook angezeigten Speicherort zu aktualisieren, was möglicherweise fehleranfällig ist.

Ersetzungen werden auch zum Definieren von Zuordnungen zwischen Werten verwendet, wie in

Beispielen weiter unten in diesem Dokument beschrieben.

Jede Ersetzung in der Liste besteht aus einem Schlüssel und einem Wert. Der Wert kann ein einfacher Wert, ein Ausdruck, eine Funktion oder eine Karte sein.

Im folgenden Beispiel werden zwei Substitutionen definiert. Die erste ist `http-port`, dass sie als Kurzform für 8181 verwendet werden kann. Wenn Sie eine Substitution verwenden, können Sie dies im Rest des StyleBook als **$substitutions.http-port** anstelle von 8181 verweisen.

Substitutionen:

```
http-port: 8181
```

Auf diese Weise können Sie einen mnemonischen Namen für eine Portnummer angeben und diese Portnummer an einer Stelle im StyleBook definieren, unabhängig davon, wie oft sie verwendet wird. Wenn Sie die Portnummer in 8080 ändern möchten, können Sie sie im Substitutionsabschnitt ändern, und die Änderung wird überall wirksam, wo der mnemonische Name verwendet `http-port` wird. Das folgende Beispiel zeigt, wie eine Substitution in einer Komponente verwendet wird.

```
components:

 -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

          name: $parameters.name + "-lb"

          servicetype: HTTP

          ipv46: $parameters.ip

          port: $substitutions.http-port

          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Eine Substitution kann auch ein komplexer Ausdruck sein. Das folgende Beispiel zeigt, wie zwei Substitutionen Ausdrücke verwenden.


```
substitutions:

  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS

  app-name: str("acme-") + $parameters.name + str("-app")
<!--NeedCopy-->
```

Ein Substitutionsausdruck kann auch vorhandene Substitutionsausdrücke verwenden, wie im folgenden Beispiel gezeigt.

```
substitutions:

  http-port: 8181

  app-name: str("acme-") + $parameters.name + str($substitutions.http-
     port) + str("-app")
<!--NeedCopy-->
```

Ein weiteres nützliches Feature von Substitutionen sind Maps, in denen Sie Schlüssel zu Werten zuordnen können. Im Folgenden finden Sie ein Beispiel für eine Kartenersetzung.

```
substitutions:

    secure-port:

        true: int("443")

        false: int("80")

    secure-protocol:

        true: SSL

        false: HTTP
<!--NeedCopy-->
```

Das folgende Beispiel zeigt, wie Sie die Karten Secure-Port und Secure-Protokoll verwenden.

```
components:

```



```
3  -
4
5      name: my-lbvserver-comp
6
7      type: ns::lbvserver
8
9      properties:
10
11          name: $parameters.name + "-lb"
12
13          servicetype: $substitutions.secure-protocol[$parameters.is-
               secure]
14
15          ipv46: $parameters.ip
16
17          port: $substitutions.secure-port[$parameters.is-secure]
18
19          lbmethod: $parameters.lb-alg
20 <!--NeedCopy-->
```

Dies bedeutet, dass, wenn der Benutzer des StyleBook den booleschen Wert "true" für den Parameter ist-sicher angibt oder das diesem Parameter entsprechende Kontrollkästchen in der Citrix ADM-GUI auswählt, der `servicetype` Eigenschaft dieser Komponente der Wert **SSL** zugewiesen wird und die Eigenschaft port ist hat den Wert **443**zugewiesen. Wenn der Benutzer jedoch "false" für diesen Parameter angibt oder das entsprechende Kontrollkästchen in der Citrix ADM GUI deaktiviert, wird der `servicetype` Eigenschaft der Wert **HTTP** zugewiesen, und dem Port wird der Wert **80**zugewiesen.

Das folgende Beispiel zeigt, wie Substitutionen als Funktion verwendet werden. Eine Substitutionsfunktion kann ein oder mehrere Argumente annehmen. Argumente können vom einfachen Typ sein, z. B. string, number `ipaddress`„ boolean und andere Typen.

Substitutionen:

form-lb-name(name): $name + "-lb"

In diesem Beispiel definieren wir eine Substitutionsfunktion form-lb-name, die ein String-Argument namens "name" nimmt und es verwendet, um eine neue Zeichenfolge zu erstellen, die -lb an die Zeichenfolge im Namen Argument. Ein Ausdruck, der diese Substitutionsfunktion verwendet, kann wie folgt geschrieben werden:

```
$substitutions.form-lb-name("my")
```

Es kehrt zurück `my-lb`

Betrachten Sie ein anderes Beispiel:

Substitutionen:

`cspol-priority(priority): 10100 - 100 * $priority`

Die Substitution `cspol-priority` ist eine Funktion, die ein Argument namens Priorität verwendet und es zur Berechnung eines Werts verwendet. Im Rest des StyleBook kann diese Substitution verwendet werden, wie im folgenden Beispiel gezeigt:

```
components:

  -

    name: cspolicy-binding-comp

    type: ns::csvserver_cspolicy_binding

    condition: not $parameters.is-default

    properties:

         name: $parameters.csvserver-name

         policyname: $components.cspolicy-comp.properties.policyname

         priority: $substitutions.cspol-priority($parameters.pool.
            priority)
<!--NeedCopy-->
```

Substitution kann auch aus einem Schlüssel und einem Wert bestehen. Der Wert kann ein einfacher Wert, ein Ausdruck, eine Funktion, eine Karte, eine Liste oder ein Wörterbuch sein.

Das Folgende ist ein Beispiel für eine Substitution namens `slist` deren Wert eine Liste ist:

```
substitutions:

  slist:

    - a

    - b

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


Der Wert einer Substitution kann auch ein Wörterbuch von Schlüssel-Wert-Paaren sein, wie im folgenden Beispiel einer folgenden Substitution `sdict` gezeigt wird:

```
substitutions:

  sdict:

    a: 1

    b: 2

    c: 3
<!--NeedCopy-->
```

Sie können komplexere Attribute erstellen, indem Sie Listen und Wörterbücher kombinieren. Zum Beispiel gibt eine Substitution namens eine Liste von Schlüssel-Wert-Paaren `slistofdict` zurück.

```
  slistofdict:

    -

      a: $parameters.cs1.lb1.port

      b: $parameters.cs1.lb2.port

    -

      a: $parameters.cs2.lb1.port

      b: $parameters.cs2.lb2.port
<!--NeedCopy-->
```

Im folgenden Beispiel gibt eine Substitution jedoch ein Schlüssel-Wert-Paar `sdictoflist` zurück, wobei der Wert selbst eine andere Liste ist.

```
  sdictoflist:

    a:

      - 1
```



```
6
7         - 2
8
9       b:
10
11        - 3
12
13        - 4
14  <!--NeedCopy-->
```

In Komponenten können diese Substitutionen in Condition, Properties, repeat-condition Konstrukten verwendet werden.

Das folgende Beispiel einer Komponente zeigt, wie eine Substitution verwendet werden kann, um die Eigenschaften anzugeben:

```
1       properties:
2
3         a: $substitutions.slist
4
5         b: $substitutions.sdict
6
7         c: $substitutions.slistofdict
8
9         d: $substitutions.sdictoflist
10  <!--NeedCopy-->
```

Ein Anwendungsfall zum Definieren einer Substitution, deren Wert eine Liste oder ein Wörterbuch ist, ist, wenn Sie einen virtuellen Content Switching-Server und mehrere virtuelle Server für den Lastenausgleich konfigurieren. Da alle virtuellen Server von lb, die an denselben virtuellen CS-Server gebunden sind, möglicherweise eine identische Konfiguration haben, können Sie die Ersetzungsliste und das Wörterbuch verwenden, um diese Konfiguration zu erstellen, um zu vermeiden, dass diese Konfiguration für jeden virtuellen lb-Server wiederholt wird.

Das folgende Beispiel zeigt die Ersetzung und die Komponente in den `cs-lb-mon` StyleBooks, um eine virtuelle Content Switching-Serverkonfiguration zu erstellen. Bei der Erstellung der Eigenschaften von `cs-lb-mon` StyleBooks gibt die komplexe Substitution “lb-properties” die Eigenschaften der virtuellen lb-Server an, die mit dem virtuellen Server cs verknüpft sind. Die Substitution lb-properties ist eine Funktion, die den Namen, den Diensttyp, die virtuelle IP-Adresse, den Port und die Server als Parameter annimmt und ein Schlüssel-Wert-Paar als Wert generiert. In der `cs-pools` Komponente weisen wir den Wert dieser Substitution einem lb-pool-Parameter für jeden Pool zu.


```
substitutions:

  cs-port[]:

    true: int("80")

    false: int("443")

  lb-properties(name, servicetype, vip, port, servers):

    lb-appname: $name

    lb-service-type: $servicetype

    lb-virtual-ip: $vip

    lb-virtual-port: $port

    svc-servers: $servers

    svc-service-type: $servicetype

    monitors:

      -

        monitorname: $name

        type: PING

        interval: $parameters.monitor-interval

        interval_units: SEC

        retries: 3

components:

  -

    name: cs-pools

    type: stlb::cs-lb-mon

```



```
45      description: | Updates the cs-lb-mon configuration with the
            different pools provided. Each pool with rule result in a dummy
            LB vserver, cs action, cs policy, and csvserver_cspolicy_binding
             configuration.
46
47      condition: $parameters.server-pools
48
49      repeat: $parameters.server-pools
50
51      repeat-item: pool
52
53      repeat-condition: $pool.rule
54
55      repeat-index: ndx
56
57      properties:
58
59        appname: $parameters.appname + "-cs"
60
61        cs-virtual-ip: $parameters.vip
62
63        cs-virtual-port: $substitutions.cs-port($parameters.protocol == "
              HTTP")
64
65        cs-service-type: $parameters.protocol
66
67        pools:
68
69          -
70
71            lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP"
                  , "0.0.0.0", 0, $pool.servers)
72
73            rule: $pool.rule
74
75            priority: $ndx + 1
76  <!--NeedCopy-->
```

Substitutionszuordnung:

Sie können Substitutionen erstellen, die Schlüssel Werten zuordnen. Betrachten Sie beispielsweise ein Szenario, in dem Sie den Standardport (Wert) definieren möchten, der für jedes Protokoll (Schlüssel) verwendet werden soll. Für diese Aufgabe schreiben Sie eine Substitutionszuordnung wie folgt.


```
substitutions:

     port:

          HTTP: 80

          DNS: 53

          SSL: 443
<!--NeedCopy-->
```

In diesem Beispiel wird HTTP 80 zugeordnet, DNS 53 zugeordnet und SSL 443 zugeordnet. Um den Port eines bestimmten Protokolls abzurufen, das als Parameter angegeben wird, verwenden Sie den Ausdruck

$substitutions.port[$parameters.protocol]

Der Ausdruck gibt einen Wert zurück, der auf dem vom Benutzer angegebenen Protokoll basiert.

- Wenn der Schlüssel HTTP ist, gibt der Ausdruck 80
- Wenn der Schlüssel DNS ist, gibt der Ausdruck 53
- Wenn der Schlüssel SSL ist, gibt der Ausdruck 443 zurück
- Wenn der Schlüssel nicht in der Karte vorhanden ist, gibt der Ausdruck keinen Wert zurück

Komponenten

April 28, 2021

Das Komponentenkonstrukt in einem StyleBook gilt als der wichtigste Abschnitt im StyleBook. In diesem Abschnitt definieren Sie die Konfigurationsobjekte, die erstellt werden müssen. Mit diesem Konstrukt können Sie ein oder mehrere Konfigurationsobjekte desselben Typs erstellen.

Das Komponentenkonstrukt kann die Eingabe im Parameterbereich verwenden, um die vom StyleBook generierte Konfiguration anzupassen. Dies ist ein optionaler Abschnitt, obwohl die meisten StyleBooks einen Komponentenabschnitt haben.

In der folgenden Tabelle werden die wichtigsten Attribute einer Komponente beschrieben.

Attribut	Beschreibung
Name	Der Name der Komponente. Sie können einen alphanumerischen Namen angeben. Der Name muss mit einem Alphabet beginnen und kann zusätzliche Alphabete, Zahlen, Bindestrich (-) oder Unterstrich (_) enthalten.
Beschreibung	Eine Beschreibung der Rolle dieser Komponente im StyleBook.

Attribut	Beschreibung
Typ	Der Typ bestimmt, welche Eigenschaften diese Komponente bietet. Komponenten haben zwei Arten von Typen: **Eingebauter Typ**: Dieser Typ wird vom System bereitgestellt und Sie müssen ihn nicht definieren, z. B. die NITRO-Entitätstypen `lbvserver` oder `servicegroup`. Wenn eine Komponente über ein integriertes Typattribut verfügt, erstellt sie ein Konfigurationsobjekt dieses Typs auf dem Citrix ADC. Wenn sich eine Komponente beispielsweise auf den integrierten Typ `lbvserver` bezieht, erstellt diese Komponente einen virtuellen Lastausgleichsserver auf der Citrix ADC-Instanz, der das Ziel der Konfiguration ist. **Zusammengesetzter Typ**: Dieser Typ bezieht sich auf ein vorhandenes StyleBook, das Sie erstellt und in Citrix Application Delivery Management (ADM) importiert haben. Wenn eine Komponente über ein zusammengesetztes Typattribut verfügt, erstellt sie alle Konfigurationsobjekte, die im referenzierten StyleBook angegeben sind, auf der Citrix ADC-Instanz, die das Ziel der Konfiguration ist. Auf diese Weise können Sie mehrere StyleBooks kombinieren, in denen jedes StyleBook einen Teil der endgültigen Konfiguration erstellt. Weitere Hinweise zu zusammengesetzten StyleBooks finden Sie unter Erstellen eines zusammengesetzten StyleBook.

Attribut	Beschreibung
properties	Die Unterattribute, die für ein Komponententypattribut verwendet werden können. Die Eigenschaften, die für eine Komponente gültig sind, werden durch ihren Typ bestimmt. Bei einem integrierten Typ sind dies die Eigenschaften oder Attribute des entsprechenden NITRO-Objekts. Für eine Komponente, deren Typ ein anderes StyleBook ist, d. h. ein zusammengesetzter Typ, entsprechen die Eigenschaften den in diesem StyleBook definierten Parametern.

Beispiel:

```
components:

   -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

        name: $parameters.name

        servicetype: HTTP

        ipv46: $parameters.ip

        port: 80

        lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

In diesem Beispiel haben Sie eine Komponente mit dem Namen definiert `my-lbvserver-comp`. Diese Komponente ist vom Typ ns lbvserver (ein integrierter Typ), wobei “ns” das Präfix ist, das sich auf den Namespace netscaler.nitro.config und Version 10.5 bezieht, den Sie im Abschnitt

import-stylebooks angegeben haben, und eine NITRO-Ressource in diesem Namespace `lbvserver` ist.

Die Eigenschaften in diesem Abschnitt enthalten vier obligatorische und ein optionales Attribut (`lbmethod`) der `lbvserver` Ressource und ermöglichen es Ihnen, Werte für diese Attribute anzugeben. In diesem Beispiel geben Sie statische Werte für `servicetype` und portieren an, während der Name, ipv46 und `lbmethod` Eigenschaften ihre Werte aus den Eingabeparametern erhalten. Sie verweisen auf die Parameternamen, die im Parameterabschnitt definiert sind, indem Sie $parameters verwenden. <name>Notation, zum Beispiel $parameters.ip.

Weitere Informationen zu allen verfügbaren Citrix ADC NITRO -Ressourcen und deren Attribute/Eigenschaften finden Sie in derCitrix ADC NITRO REST APIDokumentation.

> **Hinweis**
>
> Sie müssen Kleinbuchstaben für die Attributnamen von NITRO-Ressourcentypen (deren Komponenteneigenschaften) verwenden. Andernfalls schlägt der Import eines StyleBook fehl.

Hilfskomponenten

April 28, 2021

Die primäre Verwendung des Komponentenabschnitts in einem StyleBook besteht darin, Konfigurationsobjekte über NITRO-integrierte Typen oder ein anderes StyleBook zu generieren, das die tatsächlichen Konfigurationsobjek Die Hilfskomponenten erstellen Konfigurationsobjekte nicht selbst. Hilfskomponenten nehmen die Eingaben aus anderen Abschnitten wie Parameterobjekte, Eigenschaften anderer Komponenten oder Ausgaben anderer Komponenten und transformieren sie in andere Formen. Dies kann später von anderen Komponenten verwendet werden, um die tatsächlichen Konfigurationsobjekte zu generieren. Eine Hilfskomponente kann von zwei Typen sein: Objekttyp oder ein anderes StyleBook, das keinen Komponentenabschnitt enthält.

Das folgende Beispiel zeigt ein Snippet eines StyleBook, das verwendet wird, um einen Load Balancing-Server mit monitor (`lb-mon-comp`) auf einer Citrix ADC-Instanz zu erstellen.

```
1  parameters:
2
3    -
4
5      name: appname
6
7      type: string
8
```



```
  -

    name: ips

    type: ipaddress[]

  -

    name: vip

    type: ipaddress

components:

  -

    name: help-comp

    type: cmtypes::server-ip-port-params

    repeat:

      repeat-list: $parameters.ips

      repeat-item: server-ip

    properties:

      ip: $server-ip

      port: 80

 -

    name: lb-mon-comp

    type: stlb::lb-mon

    properties:

      lb-appname: $parameters.appname

      lb-virtual-ip: $parameters.vip

      lb-virtual-port: 80
```



```
54
55        lb-service-type: HTTP
56
57        svc-service-type: HTTP
58
59        svc-servers: $components.help-comp.properties
60
61  <!--NeedCopy-->
```

Im Parameterbereich können Sie den Namen der Anwendung und die IP-Adressen der Load Balancing Server eingeben. Im Abschnitt “ `lb-mon-comp` Komponente” erwartet der `svc-servers` Parameter von `lb-mon` StyleBook eine Liste von Objekten, bei denen jedes Element zwei Unterparameter `ip` und einen Port hat.

Der Parameterabschnitt dieses StyleBook akzeptiert jedoch nur die Server-IPs über $parameters.ips. Das StyleBook geht davon aus, dass alle Server auf Port 80 ausgeführt werden. Um die Load Balancing-Konfiguration mit `lb-mon` StyleBook zu erstellen, müssen Sie die $ parameters.ips in eine Liste von Objekten umwandeln. Dies wird mit der Helferkomponente help-comp im obigen Beispiel erreicht. Die help-comp-Komponente ist vom Typ `server-ip-port-params` StyleBook. Dieses StyleBook hat keine Komponenten. Daher werden keine Konfigurationsobjekte erstellt. Der help-comp erstellt eine Wiederholungsliste über $parameters.ips und konstruiert ein Objekt, das aus `ip` und portiert (das auf eine statische 80 festgelegt ist) für jedes Element von $parameters.ips. Daher transformiert help-comp eine Liste von IP-Adressen in eine Liste von Objekten, die später `lb-mon-comp` zum Zuweisen von `svc-servers` Eigenschaften verwendet werden können. Das Ergebnis des Hilfe-Comp wird der `svc-servers` Eigenschaft von zugeordnet `lb-mon-comp`.

Optionale Eigenschaften

April 28, 2021

Manchmal nimmt eine Eigenschaft einer Komponente ihren Wert aus einem Ausdruck, der ein einfacher Ausdruck wie eine Parameterreferenz oder ein komplexerer sein kann. Das Festlegen dieses Eigenschaftswerts ist in der Komponente optional. Sie können den Eigenschaftswert nur festlegen, wenn der Ausdruck einen tatsächlichen Wert zurückgibt, andernfalls können Sie diese Eigenschaft nicht festlegen.

Stellen Sie sich beispielsweise vor, dass eine der Eigenschaften, die Sie festlegen möchten, der `lbmethod` (Load Balancing-Algorithmus) einer Komponente ist, deren Typ ns lbvserver ist. Der Wert der Eigenschaft `lbmethod` wird einem vom Benutzer bereitgestellten Parameterwert entnommen, wie unten dargestellt:


```
components

  -

      name: lbvserver_comp

      type: ns::lbvserver

      properties:

        name: $parameters.lb-appname + ”-lb”

        servicetype: $parameters.lb-service-type

        ipv46: $parameters.lb-virtual-ip

        port: 80

        lbmethod: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```

Betrachten Sie nun, dass der Parameter **lb-advanced.algorithm** ein optionaler Parameter ist. Wenn der Benutzer keinen Wert für diesen Parameter bereitstellt, weil er optional ist, wird der Ausdruck **$parameters.lb-advanced.algorithm** als leerer Wert ausgewertet. Daher wird ein ungültiger Wert für die `lbmethod` Eigenschaft übergeben. Um eine solche Situation zu vermeiden, können Sie die Eigenschaft als optional kommentieren, indem Sie ihren Namen mit ? wie folgt:

```
components

   -

     name: lbvserver_comp

     type: ns::lbvserver

     properties:

       name: $parameters.lb-appname + ”-lb”

       servicetype: $parameters.lb-service-type

       ipv46: $parameters.lb-virtual-ip
```



```
16
17          port: 80
18
19          lbmethod?: $parameters.lb-advanced.algorithm
20  <!--NeedCopy-->
```

Die Verwendung von ? wird die Eigenschaft weggelassen, wenn der Ausdruck rechts zu nichts ausgewertet wird, was in diesem Fall einer Komponente gleichwertig wäre, die wie folgt definiert ist:

```
1   components
2
3     -
4
5       name: lbvserver_comp
6
7       type: ns::lbvserver
8
9       properties:
10
11        name: $parameters.lb-appname + "-lb"
12
13        servicetype: $parameters.lb-service-type
14
15        ipv46: $parameters.lb-virtual-ip
16
17        port: 80
18  <!--NeedCopy-->
```

Da **lbmethod** optional ist, ist das Weglassen immer noch eine gültige Komponente. Beachten Sie, dass `lbmethod` dies möglicherweise seinen Standardwert annehmen kann, wenn einer in seinem Typ “ns lbvserver definiert ist. “

Eigenschaften-Default-Source-Konstrukt

April 28, 2021

Das Eigenschaften-default-sources-Konstrukt ist analog zum Konstrukt parameters-default-sources. Während das parameters-default-sources-Konstrukt die Wiederverwendung vorhandener Parameter (aus anderen StyleBooks) in einem StyleBook ermöglicht, Properties-default-sources-Konstrukt dem Benutzer Eigenschaften einer Komponente basierend auf vorhandenen Quellen angeben.

Die Eigenschaften einer Komponente können über verschiedene Abschnitte des StyleBook verteilt werden. Beispielsweise können die Eigenschaften von Objektparametern, Substitutionen, die ein Objekt zurückgeben, Eigenschaften anderer Komponenten oder Ausgaben anderer Komponenten stammen. In solchen Fällen müssen Sie die Eigenschaften, die in anderen Abschnitten des StyleBook in der Definition der Komponente auftreten, neu definieren. Offensichtlich ist dies redundant und kann zu Fehlern führen. Um dieses Problem zu lösen, können Eigenschaften-default-sources-Konstrukt verwendet werden. Das Eigenschaften-default-sources-Konstrukt ist eine Liste, in der jedes Element eine Quelle für einige Eigenschaften der Komponente identifiziert.

Betrachten Sie zum Beispiel eine Komponente, die eine `lbvserver` Konfiguration erstellt. Diese Komponente definiert die Eigenschaften von `lbvserver` wie folgt.

```
parameters:

  -

    name: lb

    type: ns::lbvserver

components:

  -

    name: lb-comp

    type: ns::lbvserver

    properties:

      name: $parameters.lb.name

      ipv46: $parameters.lb.ipv46

      port: $parameters.lb.port

      servicetype: $parameters.lb.servicetype

      lbmethod: $parameters.lb.lbmethod
<!--NeedCopy-->
```

Beachten Sie im obigen Beispiel, dass die Werte für alle Eigenschaften, die im Komponentenabschnitt definiert sind, aus $parameters.lb Objekt genommen werden. Obwohl sie aus einer einzigen Quelle

stammen, werden die Eigenschaften im StyleBook erneut definiert. Wenn außerdem ein neuer Unterparameter für das Objekt $parameters.lb hinzugefügt wird, der für die Konfiguration des relevant `lbvserver` ist, müssen Sie die lb-comp-Komponente aktualisieren, um die neue Eigenschaft hinzuzufügen, die dem neuen Unterparameter entspricht.

Um eine Neudefinition von Eigenschaften zu vermeiden und alle relevanten Eigenschaften einer Komponente abzurufen, ohne sie explizit im Eigenschaftenabschnitt aufzulisten, kann Eigenschaftendefault-sources-Konstrukt verwendet werden. Das obige Beispiel kann wie folgt geschrieben werden.

```
parameters:

  -

    name: lb

    type: ns::lbvserver

components:

  -

    name: lb-comp

    type: ns::lbvserver

    properties-default-sources:

      - $parameters.lb
<!--NeedCopy-->
```

Im obigen Beispiel führt die Verwendung von Eigenschaften-default-Source-Konstrukt zu einer Verringerung der Größe der Komponentendefinition, und dies ermöglicht es Ihnen, eine Komponente prägnant zu definieren. Darüber hinaus werden jedes Mal, wenn sich die Quelle der Eigenschaften der Komponente ändert, die Änderungen automatisch reflektiert. Wenn beispielsweise eine neue Eigenschaft im $parameters.lb-Objekt hinzugefügt wird `persistencetype`, wird diese Eigenschaft standardmäßig zur Konfiguration von lb-comp hinzugefügt, da sie eine Eigenschaft von `persistencetype` ist `lbvserver`. Somit bietet Eigenschaften-default-sources-Konstrukt eine dynamische Schnittstelle, um die Komponenten zu definieren, ohne sich Gedanken über Änderungen an den Quellen der Eigenschaften der Komponente zu machen.

Berechnung der Eigenschaften der Komponente

In diesem Abschnitt wird erläutert, wie die Eigenschaften abgerufen werden, wenn Eigenschaften-default-sources-Konstrukt in einer Komponente verwendet wird. Zunächst identifiziert der StyleBooks-Compiler die Liste der Eigenschaften für eine Komponente basierend auf ihrem Typ (im obigen Beispiel) `lbvserver`. Als Nächstes ruft der Compiler diese Eigenschaften aus den mehreren Quellen in der Reihenfolge ab, in der sie definiert sind (im Abschnitt Eigenschaften-Standardquellen der Komponente). Wenn eine Eigenschaft in mehreren Quellen vorhanden ist, hat die Eigenschaft, die in der letzten Quelle angezeigt wird, Vorrang vor anderen. Schließlich kann eine Eigenschaft, die mit Eigenschaften-default-sources-Konstrukt abgerufen wird, im Eigenschaftenabschnitt der Komponente außer Kraft gesetzt werden. Es ist wichtig zu beachten, dass die Definition eines Komponentenabschnitts mindestens einen Eigenschaften-Standard-Sources-Abschnitt oder einen Eigenschaftenbereich enthält. Es kann beides haben.

Verschachtelte Komponenten

April 28, 2021

Das Verschachteln einer Komponente in einer anderen Komponente ermöglicht es der verschachtelten Komponente, ihre Konfigurationsobjekte zu erstellen, indem sie auf Konfigurationsobjekte oder den Kontext verweist, der von der übergeordneten Komponente erstellt wird. Die verschachtelte Komponente kann für jedes Objekt, das in der übergeordneten Komponente erstellt wurde, ein oder mehrere Objekte erstellen. Das Verschachteln einer Komponente in einer anderen Komponente zeigt keine Beziehung zwischen den erstellten Konfigurationsobjekten an. Verschachtelung ist eine Möglichkeit, die Aufgabe von Komponenten zu erleichtern, Konfigurationsobjekte in einem vorhandenen Kontext der übergeordneten Komponenten zu konstruieren.

Beispiel:

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

   properties:

      name: $parameters.name + ”-lb”
```



```
12
13        servicetype: HTTP
14
15        ipv46: $parameters.ip
16
17        port: 80
18
19        lbmethod: $parameters.lb-alg
20
21        components:
22
23          -
24
25           name: my-svcg-comp
26
27           type: ns::servicegroup
28
29           properties:
30
31              name: $parameters.name + "-svcgrp"
32
33              servicetype: HTTP
34
35           components:
36
37              -
38
39                name: lbvserver-svg-binding-comp
40
41                type: ns::lbvserver_servicegroup_binding
42
43                properties:
44
45                  name: $parent.parent.properties.name
46
47                  servicegroupname: $parent.properties.name
48
49                    -
50
51                      name: members-svcg-comp
52
53                      type: ns::servicegroup_servicegroupmember_binding
54
55                      repeat:
56
```



```
                        repeat-list: $parameters.svc-servers

                        repeat-item: srv

                      properties:

                        ip: $srv

                        port: str($parameters.svc-port)

                        servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

In diesem Beispiel wird eine mehrstufige Verschachtelung verwendet. Die Komponente `my-lbvserver-comp` hat eine untergeordnete Komponente namens `my-svcg-comp`. Und die `my-svcg-comp` Komponente enthält zwei untergeordnete Komponenten. Die `my-svcg-comp` Komponente wird verwendet, um ein Dienstgruppenkonfigurationsobjekt auf der Citrix ADC-Instanz zu erstellen, indem Werte für die Attribute des integrierten NITRO-Ressourcentyps bereitgestellt werden`servicegroup`. “ “ Die erste untergeordnete Komponente der `my-svcg` Komponente wird verwendet `lbvserver-svg-binding-comp`, um die von ihrer übergeordneten Komponente erstellte Dienstgruppe an den virtuellen Lastausgleichsserver (`lbvserver`) zu binden, der von der übergeordneten Komponente des übergeordneten Elements erstellt wurde. Die $parent Notation, auch übergeordnete Referenz genannt, wird verwendet, um auf Entitäten in den übergeordneten Komponenten zu verweisen. Die zweite untergeordnete Komponente wird verwendet `members-svcg-comp`, um die Liste der Dienste an die von der übergeordneten Komponente erstellte Servicegruppe zu binden. Die Bindung wird erreicht, indem das Wiederholungskonstrukt eines StyleBook verwendet wird, um über die Liste der für den Parameter angegebenen Dienste zu iterieren `svc-servers`. Hinweise zu wiederholten Konstrukten finden Sie unterKonstrukt wiederholen.

Sie können auch dieselben Konfigurationsobjekte erstellen, ohne die Verschachtelung von Komponenten zu verwenden. Weitere Informationen und Beispiele finden Sie unter StyleBook zum Erstellen einer einfachen Lastausgleichskonfiguration.

Konditionskonstrukt

April 28, 2021

Sie können eine Komponente bedingungsabhängig machen, indem Sie ein Bedingungskonstrukt verwenden. Der Wert eines bedingten Konstrukts ist ein boolescher Ausdruck, der als true oder false ausgewertet wird. Wenn die Bedingung wahr ist, wird die Komponente verwendet, um ihre Konfigurationsobjekte zu erstellen. Wenn die Bedingung false ist, wird die Komponente übersprungen, und

es werden keine Konfigurationsobjekte erstellt. Der boolesche Ausdruck basiert häufig auf Parameterwerten.

Beispiel:

```
components:

      -

        name: servicegroup-comp

        type: ns::servicegroup

        condition: $parameters.svc-server-ips

        properties:

              name: $parameters.name + ”-svcgrp”

              servicetype: HTTP
<!--NeedCopy-->
```

Wenn der Benutzer in diesem Beispiel einen Wert `svc-server-ips` für den optionalen Parameter `servicegroup-comp` angibt, wird die Komponente von der StyleBook-Engine verarbeitet. Wenn die Bedingung “false” ist, dh wenn der Benutzer diesem Parameter keinen Wert zur Verfügung stellt, wird diesem Parameter ein Nullwert zugewiesen und als “false” ausgewertet, ignoriert die StyleBook-Engine das Vorhandensein dieser Komponente und es wird keine `servicegroup` erstellt.

Beachten Sie, dass der boolesche Ausdruck auf einem beliebigen gültigen Ausdruck basieren kann, der in StyleBooks unterstützt wird (z. B. ob eine andere Komponente vorhanden ist oder ob ein Parameter einen bestimmten Wert hat).

Im folgenden Beispiel wird das Konfigurationsobjekt vom NITRO-Typ ns::systemfile erstellt, wenn die Bedingung auf true ausgewertet wird.

Beispiel:

```
    components

        -

          name: pem_key_files

```



```
            type: ns::systemfile

            condition: "$components.der-certificate-files-comp or
                $components.pem-certificate-files-comp"

            properties:

                    filecontent: $certificate.keyfile.contents

                    fileencoding: "BASE64"

                    filelocation: "/nsconfig/ssl"

                    filename: $certificate.keyfile.filename
<!--NeedCopy-->
```

In diesem Beispiel ist die Bedingung ein komplexer Ausdruck oder, bei dem dieses Konfigurationsobjekt nur dann vom StyleBook erstellt werden soll, wenn zwei weitere Komponenten im StyleBook verarbeitet wurden (nicht übersprungen), wodurch eine Abhängigkeit zwischen den Komponenten entsteht.

Konstrukt wiederholen

April 28, 2021

Sie können das **Wiederholungskonstrukt** einer Komponente verwenden, um mehrere Konfigurationsobjekte desselben Typs zu erstellen.

Im folgenden Beispiel wird die **members-svcg-comp-Komponente** verwendet, um die Liste der Dienste an die von der übergeordneten Komponente erstellte Dienstgruppe zu binden. Um ein Konfigurationsobjekt zu erstellen, das jeden Server an die Dienstgruppe bindet, verwenden **Sie das repeate-Konstrukt**, um die Liste der Dienste zu durchlaufen, die für den Parameter **svc-Server**angegeben ist. Während der Iteration erstellt die Komponente ein NITRO-Objekt vom Typ **servicegroup_servicegroupmember_binding** für jeden Dienst (im **repeat-Item-Konstrukt** als **srv** bezeichnet) in der Servicegruppe und setzt das **ip-Attribut** in jedem NITRO-Objekt auf die IP-Adresse des entsprechenden Dienstes.

Beispiel:

```
components:
  -
```



```
3       name: my-lbvserver-comp
4       type: ns::lbvserver
5       properties:
6            name: $parameters.name + "-lb"
7            servicetype: HTTP
8            ipv46: $parameters.ip
9            port: 80
10           lbmethod: $parameters.lb-alg
11           components:
12                -
13                   name: my-svcg-comp
14                   type: ns::servicegroup
15                   properties:
16                        name: $parameters.name + "-svcgrp"
17                        servicetype: HTTP
18                   components:
19                         -
20                         name: lbvserver-svg-binding-comp
21                         type: ns::lbvserver\servicegroup\binding
22                         properties:
23                               name: $parent.parent.properties.name
24                               servicegroupname: $parent.properties.
                                     name
25                         -
26                         name: members-svcg-comp
27                         type: ns::servicegroup\servicegroupmember\
                              binding
28                         repeat:
29                           repeat-list: $parameters.svc-servers
30                           repeat-item: srv
31                         properties:
32                                ip: $srv
33                                port: $parameters.svc-port
34                                servicegroupname: $parent.properties.
                                      name
35  <!--NeedCopy-->
```

Die **Wiederholung** ist ein Objekt für sich, und **repeat-list** und **repeat-item** sind Attribute für das Wiederholungsobjekt.

- repeat-list ist ein obligatorisches Attribut, das die Liste identifiziert, auf der die Komponente iteriert.
- repeat-item ist optional und wird verwendet, um dem aktuellen Element in der Iteration einen Anzeigenamen zu geben.

Wenn nicht angegeben, kann auf das aktuelle Element mit dem Ausdruck **$repeat-item**zugegriffen werden. Die letzte Komponente im obigen Beispiel kann auch wie folgt geschrieben werden:

```
            -

            name: members-svcg-comp

            type: ns::servicegroup_servicegroupmember_binding

            repeat:

              repeat-list: $parameters.svc-servers

            properties:

                    ip: $repeat-item

                    port: $parameters.svc-port

                    servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

Neben der Möglichkeit, auf das aktuelle Element während der Iteration über eine Liste zu verweisen, ist es auch möglich, auf den aktuellen Index des Elements in der Liste mit **repeat-index**zu verweisen. Im folgenden Beispiel wird **repeat-index** verwendet, um eine Portnummer basierend auf dem aktuellen Index zu berechnen:

```
              name: services

              type: ns::service

              repeat:

                 repeat-list: $parameters.app-services

                 repeat-item: srv

              properties:

                  ip: $parameters.app-ip

                  port: $parameters.base-port + repeat-index
```



```
16
17                  servicegroupname: $parent.properties.name
18 <!--NeedCopy-->
```

Ähnlich wie beim **Repeat-Item-Konstrukt** können Sie einen anderen Variablennamen zuweisen, der auf den aktuellen Index der Iteration verweist. Das vorherige Beispiel entspricht dem folgenden Beispiel:

```
1       -
2
3               name: services
4
5               type: ns::service
6
7               repeat:
8
9                  repeat-list: $parameters.app-services
10
11                 repeat-item: srv
12
13                 repeat-index: idx
14
15              properties:
16
17                  ip: $parameters.app-ip
18
19                  port: $parameters.base-port + $idx
20
21                  servicegroupname: $parent.properties.name
22 <!--NeedCopy-->
```

Konstrukt für Wiederholungsbedingung

April 28, 2021

Das Repeat-Condition-Konstrukt wird in jeder Iteration eines Wiederholungskonstrukts ausgewertet und das Ergebnis bestimmt, ob das Konfigurationsobjekt in dieser Iteration erstellt oder zur nächsten Iteration verschoben werden soll. Das folgende Beispiel zeigt die Verwendung des Repeat-Condition-Konstrukt:

Beispiel:


```
components

   -

      name: der-key-files-comp

      type: ns::systemfile

      repeat:

      repeat-list: $parameters.certificates

      repeat-item: certificate

        repeat-condition: $certificate.ssl-inform == DER

        properties:

         filecontent: base64($certificate.keyfile.contents)

         fileencoding: BASE64

         filelocation: /nsconfig/ssl

         filename: $certificate.keyfile.file
<!--NeedCopy-->
```

In diesem Beispiel iteriert die `der-key-files-comp` Komponente über alle vom Benutzer angegebenen Zertifikate, erstellt jedoch nur Konfigurationsobjekte, die Zertifikaten mit DER-Kodierung entsprechen. In jeder Iteration wird der Wiederholungsbedingung Ausdruck ausgewertet, um zu testen, ob die Zertifikatkodierung vom Typ DER ist. Wenn es nicht vom Typ DER ist, wird in der aktuellen Iteration kein Konfigurationsobjekt erstellt, und die Iteration wird zum nächsten Zertifikat in der Liste verschoben.

Verschachtelte Wiederholungen

April 28, 2021

Mit dem verschachtelten Wiederholungskonstrukt können Sie je nach Definition der Komponente mehr als ein Wiederholungskonstrukt in jeder Komponente haben. Betrachten Sie eine

verschachtelte Wiederholung von zwei Ebenen. Für jedes Element in der äußeren Liste (erste Wiederholungsliste) können Sie eine Wiederholungsliste für alle Elemente der inneren Liste erstellen (zweite Wiederholungsliste). Der StyleBook-Compiler unterstützt bis zu drei verschachtelte Wiederholungen. Jeder Wiederholungsebene sind mit den Attributen repeat-item und repeat-index verknüpft. Sowohl repeat-item als auch repeat-index Attribute sind optional. Darüber hinaus kann jede Wiederholung auch eine Wiederholungsbedingung angeben.

Beispiel:

```
parameters:

  -

      name: vips

      type: ipaddress[]

  -

      name: vip-ports

      type: tcp-port[]

components:

  -

      name: lbvservers-comp

      type: ns::lbvserver

      repeat:

         repeat-list: $parameters.vips

         repeat-item: ip

         repeat:

              repeat-list: $parameters.vip-ports

              repeat-item: port

```



```
35        properties:
36
37           name: str(”lb-”) + str($ip) + '-' + str($port)
38
39           servicetype: HTTP
40
41           ipv46: $ip
42
43           port: $port
44  <!--NeedCopy-->
```

In diesem Beispiel iterieren wir für jedes Element in `$parameters.vips`alle Elemente von `$parameters.vip-ports`. Daher erstellen wir für jedes in `ipaddress` angegebene in `lbvserver` Konfigurationsobjekte für alle Ports `$parameters.vips`, die in $ parameters.vip-Ports angegeben sind. Der Eigenschaftenabschnitt definiert den Namen des Objekts mit “lb” als Präfix für die Kombination der IP-Adresse und des Ports. `$ip + $port` Definiert daher für jede Iteration eine eindeutige Kombination der IP-Adresse und der Portnummer.

Wenn das `repeat-item` Attribut nicht angegeben wird, generiert der Compiler einen Standardwert dafür. Die Standardwerte für Wiederholungselement sind: `$repeat-item$repeat-item-1`, `$repeat-item-2` bzw. für jede Wiederholungsstufe. Wenn das `repeat-index` Attribut nicht angegeben wird, generiert der Compiler einen Standardwert dafür. Die Standardwerte für repeat-index sind: $repeat-index, $repeat-index-1 und $repeat-index-2 jeweils für jede Wiederholungsebene.

Im folgenden Beispiel wird die Benennungskonvention in Abwesenheit von repeat-item und repeat-index Attributen in einem verschachtelten Wiederholungsobjekt beschrieben.

Beispiel:

```
1  components:
2
3  -
4
5       name: lbvservers-comp
6
7       type: ns::lbvserver
8
9       repeat:
10
11          repeat-list: $parameters.vips
12
13          repeat:
14
15             repeat-list: $parameters.vip-ports
```



```
16
17      properties:
18
19          name: str(”lb-”) + str($repeat-item) + '-' + str($repeat-item
                -1)
20
21          servicetype: HTTP
22
23          ipv46: $repeat-item
24
25          port: $repeat-item-1
26  <!--NeedCopy-->
```

Ausgaben

April 28, 2021

Im Abschnitt Ausgaben geben Sie an, was ein StyleBook seinen Benutzern zur Verfügung stellt, nachdem alle Konfigurationsobjekte erfolgreich erstellt wurden. Der Ausgabebereich eines StyleBook ist optional. Ein StyleBook muss keine Ausgaben zurückgeben. Wenn jedoch einige interne Komponenten als Ausgaben zurückgegeben werden, ermöglicht es allen StyleBooks, die es importieren, mehr Flexibilität, wie Sie beim Erstellen eines zusammengesetzten StyleBook sehen können.

In der folgenden Tabelle werden die Attribute beschrieben, die im Output-Abschnitt verwendet werden.

Attribut	Beschreibung	Mandatory
Name	Der Name der Ausgabe, die dem Konfigurationsobjekt entspricht, das verfügbar gemacht werden soll.	Ja
Beschreibung	Eine Textzeichenfolge, die die Ausgabe beschreibt.	Nein
Wert	Dieses Attribut gibt an, wie der Wert extrahiert wird, der von einem StyleBook zurückgegeben wird.	Ja

Beispiel:

```
outputs:

 -

   name: lbvserver

   description: LBVServer component

   value: $components.my-lbvserver-comp

 -

   name: svc-grp

     description: ServiceGroup name

     value: $components.my-svcg.properties.name
<!--NeedCopy-->
```

In diesem Beispiel legen Sie die **lbvserver-Komponente** und den `servicegroup` **Namen** bekannt, der vom StyleBook erstellt würde. Der Wert der Ausgabe namens **lbvserver** ist die Komponente **my-lbvserver-comp**. In ähnlicher Weise ist der Wert der Ausgabe namens **svc-grp** der Name des von der Komponente **my-svcg** **`servicegroup`**erzeugten.

Parameterreferenz

April 28, 2021

Im Komponentenkonstrukt verweisen Sie mithilfe der`$parameters.<parametername>` Notation auf die im Parameterabschnitt definierten Parameter. Wenn`<parametername>` selbst Parameter enthält (wenn Typ Objekt ist), müssen Sie die Notation`$parameters.<parametername>.<sub-parametername>` verwenden usw.

Beispiel:

```
parameters:

  -
```



```
4
5       name: name
6
7       label: Name
8
9       type: string
10
11      required: true
12
13       -
14
15        name: vip
16
17        label: Virtual IP and Port
18
19        type: object
20
21        required: true
22
23        parameters:
24
25          -
26
27            name: ip
28
29            label: Virtual IP
30
31            description: The Virtual IP Address
32
33            type: ipaddress
34
35            required: true
36
37              -
38
39                name: port
40
41                label: The Virtual Port
42
43                description: The TCP port for the Virtual IP
44
45                type: tcp-port
46
47                default: 80
48
```



```
components:

  -

    name: my-lbvserver-comp

    type: ns::lbvserver

    properties:

       name: $parameters.name

       servicetype: HTTP

       ipv46: $parameters.vip.ip

       port: $parameters.vip.port
<!--NeedCopy-->
```

Übergeordnete Referenz

April 28, 2021

Wenn Sie verwendenVerschachtelte Komponenten, können Sie mit der $parent Notation auf die übergeordnete Komponente verweisen. Wenn die übergeordnete Komponente mehrere Konfigurationsobjekte mit dem Wiederholungskonstrukt erstellt und untergeordnete Komponenten innerhalb jeder Iteration andere Konfigurationsobjekte erstellen, bezieht sich die $parent Notation immer auf die aktuelle Iteration der übergeordneten Komponente. Beispiel: $parent.properties.name bezieht sich auf die name-Eigenschaft des Konfigurationsobjekts, das in der aktuellen Iteration vom übergeordneten Objekt erstellt wurde.

Beispiel:

```
components:

 -

   name: my-lbvserver-comp

   type: ns::lbvserver

```



```
  properties:

    name: $parameters.name + "-lb"

    servicetype: HTTP

    ipv46: $parameters.ip

    port: 80

    lbmethod: $parameters.lb-alg

    components:

      -

        name: my-svcg-comp

        type: ns::servicegroup

        properties:

          name: $parameters.name + "-svcgrp"

          servicetype: HTTP

          components:

           -

             name: lbvserver-svg-binding-comp

             type: ns::lbvserver_servicegroup_binding

             properties:

                name: $parent.parent.properties.name

                servicegroupname: $parent.properties.name

                  -

                    name: members-svcg-comp

                    type: ns::servicegroup_servicegroupmember_binding
```



```
54
55                      repeat: $parameters.svc-servers
56
57                      repeat-item: srv
58
59                      properties:
60
61                        ip: $srv
62
63                        port: str($parameters.svc-port)
64
65                        servicegroupname: $parent.properties.name
66  <!--NeedCopy-->
```

Sie können auch durch die Hierarchie der Komponenten nach oben navigieren, indem Sie auf die Eigenschaften der Eltern der Eltern bis hin zu den Komponenten der obersten Ebene zugreifen. Beispielsweise nimmt der Eigenschaftsname der Komponente **lbvserver-svg-binding-comp** seinen Wert aus dem Eigenschaftsnamen des übergeordneten Elements des übergeordneten Elements, der **my-lbvserver-comp-Komponente**, mithilfe der Schreibweise **$parent.parent**.

Komponentenreferenz

April 28, 2021

Im Komponentenkonstrukt verweisen Sie mithilfe der `$components.<componentname>` Notation auf eine Komponente der obersten Ebene im StyleBook. Wenn sich innerhalb einer Komponente der obersten Ebene verschachtelte Komponenten befinden, wird`$components.<componentname>.components.<component-name>` die verwendete Notation darauf verweisen usw.

Beispiel:

```
1  components:
2
3   -
4
5       name: my-lbvserver-comp
6
7       type: ns::lbvserver
8
9       properties:
10
```



```
11          name: $parameters.name + "-lb"
12
13          servicetype: HTTP
14
15          ipv46: $parameters.ip
16
17          port: 80
18
19          lbmethod: $parameters.lb-alg
20
21    -
22
23      name: my-svcg-comp
24
25      type: ns::servicegroup
26
27      properties:
28
29          name: $parameters.name + "-svcgrp"
30
31          servicetype: HTTP
32
33  -
34
35      name: members-svcg-comp
36
37      type: ns::servicegroup_servicegroupmember_binding
38
39      repeat: $parameters.svc-servers
40
41      repeat-item: srv
42
43      properties:
44
45          ip: $srv
46
47          port: str($parameters.svc-port)
48
49          servicegroupname: $components.my-svcg-comp.properties.name
50
51  -
52
53      name: lbvserver-svg-binding-comp
54
55      type: ns::lbvserver_servicegroup_binding
```



```
56
57      properties:
58
59          name: $components.my-lbvserver-comp.properties.name
60
61          servicegroupname: $components.my-svcg-comp.properties.name
62  <!--NeedCopy-->
```

In diesem Beispiel müssen die Komponenten **my-svcg-comp** und **my-lbvserver-comp** erstellt werden, bevor die letzte Komponente **lbvserver-svg-binding-comp** erstellt wird, da in dieser letzten Komponente Verweise auf diese Komponenten vorhanden sind. Diese Referenzen werden mithilfe der Komponentenreferenzen bereitgestellt, die mit bezeichnet werden`$components.<componentname>`.

Substitutionsreferenz

July 3, 2020

Im Abschnitt Komponenten oder Operationen beziehen Sie sich auf Substitutionen, die im Substitutionsabschnitt definiert sind, indem Sie die**`$substitutions.<substitution-name>`**Notation verwenden. Beispiel: **$substitutions.http-port**.

Wenn eine Substitution eine Karte ist, können Sie auf ein Element in der Karte als verweisen**`$substitutions.<substitutions-name>[<map-key>]`**. Beispiel: **`$substitutions.protocol-map[$parameters.port]`**.

Variablenreferenz

April 28, 2021

Wenn Sie die Repeat- und Repeat-Item-Konstrukte in Komponenten verwenden, um mehrere Konfigurationsobjekte zu erstellen, können Sie dem Repeat-Item-Konstrukt einen Variablennamen zuweisen. Diese Variable kann dann in den Eigenschaften dieser Komponente oder in untergeordneten Komponenten mithilfe der Notation referenziert`$<varname>`werden. Beachten Sie, dass, wenn das Wiederholungskonstrukt ohne das Repeat-Item-Konstrukt in einer Komponente verwendet wird, eine Standardvariable namens $repeat-item verwendet werden kann, um auf die Iterationselemente zuzugreifen.

Beispiel:


```
components:

  -

    name: server-members-comp

    type: ns::server

    condition: $parameters.svc-server-domain-names

    repeat: $parameters.svc-server-domain-names

    repeat-item: server-name

    properties:

      name: $server-name + "-server"

      domain: $server-name

    components:

      -

         name: service-members-comp

         type: ns::service

         properties:

           name: $server-name + "-service"

           servername: $parent.properties.name

           servicetype: $parameters.svc-service-type

           port: $parameters.svc-server-port
<!--NeedCopy-->
```

Im obigen Beispiel wird dem Repeat-Item-Konstrukt ein Variablenname, Servername, zugewiesen. Auf diesen Variablennamen wird in den Eigenschaften der gleichen Komponente und in den untergeordneten Komponenten verwiesen `$<varname>`.

Vorgänge

April 28, 2021

Das `Operations` ist ein optionaler Abschnitt in einem StyleBook. In diesem Abschnitt können Sie Citrix Application Delivery Management (ADM) Analytics so konfigurieren, dass AppFlow Datensätze für alle oder einige der Traffic-Transaktionen erfasst werden. Der virtuelle Server, der auf einer Citrix ADC-Instanz mithilfe des StyleBook erstellt wurde, verarbeitet diese Verkehrstransaktionen. In diesem Abschnitt können Sie Citrix ADM auch so konfigurieren, dass Alarme auslöst, wenn bestimmte Verkehrsbedingungen auf einem virtuellen Server erfüllt sind.

Sie können Citrix ADM über StyleBooks konfigurieren, um Verkehrsstatistiken aus verschiedenen Citrix ADM Insights zu sammeln, die wie folgt aufgeführt sind:

- Web Insight
- Sicherheitshinweise
- HDX Insight
- Citrix ADC Gateway Insight.

Zu den unterstützten virtuellen Servern zählen Lastenausgleich, Content Switching und virtuelle VPN-Server.

Aktivieren Sie Web Insight oder Security Insight oder beide für Analysen auf einem Lastausgleich oder einem virtuellen Content Switching-Server. Für virtuelle VPN-Server müssen Sie jedoch sowohl HDX Insight als auch Citrix ADC Gateway Insight aktivieren.

Jeder Citrix ADM Insight, der auf Citrix ADC-Instanzen über StyleBooks aktiviert ist, verwendet ein IPFIX-Protokoll (AppFlow), um die Daten von den Instanzen an Citrix ADC zu senden.

Wenn Sie Web Insight aktivieren, sind clientseitige Messungen auf dem Lastausgleichs- und den virtuellen Content Switching-Server aktiviert. Wenn diese Funktion aktiviert ist, erfasst ADM über HTML-Injection Ladezeit und Rendering-Zeit-Metriken für HTML-Seiten. Mit diesen Metriken können Administratoren Probleme mit der L7-Latenz identifizieren.

Beispiel 1:

Im folgenden Beispiel wird gezeigt, wie der Abschnitt Vorgänge in einem StyleBook geschrieben wird, um HDX Insight und Citrix ADC Gateway Insight auf einem virtuellen VPN-Server zu aktivieren:

```
1 name: simple-vpn-ops
2
3 namespace: com.example.stylebooks
4
5 schema-version: ”1.0”
```



```
6
7  version: "0.1"
8
9  description: Test StyleBook to enable hdxinsight and gatewayinsight on
       a VPN vserver
10
11 import-stylebooks:
12
13   -
14
15     namespace: netscaler.nitro.config
16
17     version: "10.5"
18
19     prefix: ns
20
21 components:
22
23   -
24
25     name: vpnvserver-comp
26
27     type: ns::vpnvserver
28
29     properties:
30
31       name: str("vpn-") + str($current-target.ip)
32
33       servicetype: SSL
34
35       ipv46: 1.1.21.37
36
37       port: 443
38
39 operations:
40
41     analytics:
42
43       -
44
45         name: comp-ops
46
47         properties:
48
49           target: $components.vpnvserver-comp
```



```
50
51            filter: ”true”
52
53            insights:
54
55              -
56
57                type: hdxinsight
58              -
59                type: gatewayinsight
60
61  outputs:
62
63    -
64
65      name: myvpns
66
67      value: $components.vpnvserver-comp
68  <!--NeedCopy-->
```

Beispiel 2:

Das folgende Beispiel zeigt, wie der Abschnitt Vorgänge in einem StyleBook geschrieben wird, um Web Insight und Security Insight auf einem virtuellen Lastausgleichsserver zu aktivieren:

```
1  name: simple-vpn-ops
2  namespace: com.example.stylebooks
3  schema-version: ”1.0”
4  version: ”0.1”
5  description: Test StyleBook to enable hdxinsight and gatewayinsight on
       a VPN vserver
6  import-stylebooks:
7    -
8      namespace: netscaler.nitro.config
9      version: ”10.5”
10     prefix: ns
11 components:
12     -
13         name: vpnvserver-comp
14         type: ns::vpnvserver
15         properties:
16             name: str(”vpn-”) + str($current-target.ip)
17             servicetype: SSL
18             ipv46: 1.1.21.37
```



```
            port: 443
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.vpnvserver-comp
                filter: "true"
                insights:
                  -
                   type: hdxinsight
                    -
                   type: gatewayinsight
outputs:
  -
    name: myvpns
    value: $components.vpnvserver-comp
<!--NeedCopy-->
```

Analytics

April 28, 2021

Der Analytics-Unterabschnitt des Abschnitts "Vorgänge" hat eine ähnliche Struktur wie der Abschnitt "Komponenten". Jedes Element im Analyseabschnitt wird verwendet, um die Citrix Application Delivery Management (ADM) Analytics -Funktion für einen oder mehrere virtuelle Server zu konfigurieren, die vom StyleBook erstellt wurden.

Ein Element im Analyseabschnitt weist die folgenden Attribute auf:

Attribut	Beschreibung	Mandatory
Name	Name des Analyseelements.	Ja
Beschreibung	Eine Textzeichenfolge, die beschreibt, was dieses Element ist.	Nein
Bedingung	Ein boolescher Ausdruck. Wenn diese Bedingung als false ausgewertet wird, wird das gesamte Analyseelement übersprungen.	Nein

Attribut	Beschreibung	Mandatory
Wiederholen	Iteriert über eine Liste.	Nein
Wiederholungsbedingung	Ein boolescher Ausdruck. Wenn der Ausdruck auf false ausgewertet wird, wird die aktuelle Iteration übersprungen.	Nein
Wiederholungselement	Name des Elements in der aktuellen Iteration.	Nein
Wiederholungsindex	Name des Indexwerts der aktuellen Iteration.	Nein
properties	Die Liste der Eigenschaften von Analytics.	Ja
Ziel	Eine der Eigenschaften in der Liste. Der Zielausdruck ist der Name eines virtuellen Servers, der auf dem Citrix ADC konfiguriert ist, für den Analysen gesammelt werden.	Ja
Filter	Eine der Eigenschaften in der Liste. Der Wert dieses Attributs ist ein erweiterter Citrix ADC Richtlinienausdruck, der verwendet wird, um die Anforderungen auf dem virtuellen Server zu filtern, für die Analysen gesammelt werden. Standardmäßig werden die Analysedaten für den gesamten Datenverkehr gesammelt, der durch den virtuellen Server fließt.	Nein

Beispiel:


```
operations:

  analytics:

    -

    name: lbvserver-ops-comp

    properties:

    target: $components-basic-lb-comp.outputs.lbvserver-name

    filter: HTTP.REQ.URL.CONTAINS(”catalog”)

    insights:
          -
            type: webinsight
<!--NeedCopy-->
```

Jedes Attribut im Analytics-Abschnitt wird verwendet, um die Citrix ADM Analytics-Funktion anzuweisen, die Citrix ADC-Instanzen so zu konfigurieren, dass sie AppFlow-Datensätze auf dem von der Zieleigenschaft identifizierten virtuellen Server sammeln.

Alarme

April 28, 2021

Der Unterabschnitt Alarme des Abschnitts Vorgänge hat eine ähnliche Struktur und dieselben Attribute wie im Analytics-Unterabschnitt. Der einzige Unterschied besteht im Attribut properties. Eine Liste aller Attribute (mit Ausnahme des Attributs Eigenschaften) finden Sie unterAnalytics.

Die folgenden Eigenschaften sind in einem Alarm-Unterabschnitt verfügbar:

Attribut	Beschreibung	Erforderlich
target	Ein Ausdruck, der den Namen eines virtuellen Servers auswertet, der auf dem Citrix ADC konfiguriert ist, für den Alarme konfiguriert sind.	Ja

Attribut	Beschreibung	Erforderlich
email-profile	Name eines E-Mail-Profils, das in der Citrix Application Delivery Management (ADM) Analytics definiert ist und eine Liste der E-Mail-Adressen enthält, die Sie benachrichtigen möchten, wenn der Alarm ausgelöst wird.	Nein (entweder ein email-profile oder ein sms-profile muss definiert werden)
sms-profile	Name eines SMS-Profils, das in der Citrix ADM Analytics-Funktion definiert ist und eine Liste der Telefonnummern enthält, die Sie benachrichtigen möchten, wenn der Alarm ausgelöst wird.	Nein (entweder ein email-profile oder ein sms-profile muss definiert werden)
rules	Eine Liste von Regeln, die die Bedingungen definieren, die einen Alarm für den durch die Zieleigenschaft definierten virtuellen Server auslösen würden.	Ja
metric	Ein Attribut der Regel. Der Name einer Metrik, die Sie im Zusammenhang mit dem virtuellen Citrix ADC -Server verfolgen möchten.	Ja
operator	Ein Attribut der Regel. Der Operator, mit dem die Metrik mit dem Wert verglichen werden soll. Gültige Operatoren sind greaterthan und lessthan.	Ja

Attribut	Beschreibung	Erforderlich
`value`	Ein Attribut der Regel. Der Schwellenwert, mit dem die Metrik mithilfe des Operators verglichen wird. Wenn der Metrikwert diesen Schwellenwert überschreitet, werden die zugehörigen Alarme ausgelöst.	Ja
`period-unit`	Ein Attribut einer Regel. Die Häufigkeit, mit der Benutzer benachrichtigt werden sollen, wenn die Alarmregel erfüllt ist. Dieses Attribut kann den Wert Tag, Stunde oder Woche enthalten. Dies bedeutet, dass bei Einhaltung der Regel einmal pro Zeiteinheit (z. B. einmal täglich) ein Alarm gesendet wird.	Ja

Die folgende Tabelle enthält eine Liste der Metriken, die im Zusammenhang mit dem virtuellen Citrix ADC -Server verfolgt werden.

Zähler	Beschreibung	Ausführliche Beschreibung	Citrix ADM Berechnung
Für einen virtuellen VPN-Server:			
total_requests	Anzahl der VPN-Sitzungen insgesamt	Gesamtzahl der aktiven Sitzungen auf diesem virtuellen VPN-Server, die während eines vom Benutzer angegebenen Zeitintervalls gestartet wurden.	Monoton zunehmender Zähler, erhöht bei jedem neuen Sitzungsstart

Zähler	Beschreibung	Ausführliche Beschreibung	Citrix ADM Berechnung
app_count	Anzahl der VPN-App-Start-Aufrufe	Gesamtzahl der eindeutigen VPN-Anwendungen auf diesem virtuellen VPN-Server, die während eines vom Benutzer angegebenen Zeitintervalls gestartet wurden.	Monoton steigender Zähler bei jedem neuen Anwendungsstart
app_launch_duration	Startdauer der VPN-App	Durchschnittliche Zeit zum Starten einer Anwendung (in Millisekunden)	Durchschnittlicher Wert, der über die Dauer der Startzeit aller auf diesem virtuellen VPN-Server gestarteten VPN-Anwendungen hinweg berechnet wird
Andere virtuelle Server (CS, LB, Auth, GSLB)			
total_requests	Anzahl der Anfragen	Anzahl der Clientanforderungen auf diesem virtuellen Server seit dem letzten Neustart der Appliance oder seit der Erstellung des virtuellen Servers, je nachdem, was aktueller ist.	Monoton steigender Zähler, erhöht auf jede neue Anforderung an diesen virtuellen Server.

Zähler	Beschreibung	Ausführliche Beschreibung	Citrix ADM Berechnung
total_bytes	Byte	Gesamte Bytes, die über das angegebene Zeitintervall vom virtuellen Server an Citrix ADM übertragen wurden.	Monoton steigender Zähler, um die Gesamtzahl der Bytes zu berücksichtigen, die von diesem virtuellen Server bereitgestellt werden.
application_response_time	Reaktionszeit	Durchschnittliche Reaktionszeit des virtuellen Servers.	Der Durchschnittswert der Antwortzeiten aller Anfragen, die von diesem virtuellen Server seit dem letzten Neustart der Appliance (oder seit der Erstellung des virtuellen Servers) empfangen wurden, je nachdem, welcher Wert der letzte ist.

Beispiel für einen Alarmabschnitt in einem StyleBook:

```
operations:
alarms:
 -
  name:lbvserver_alarm
  properties:
  target: $outputs.lbvserver
  email-profile: $parameters.emailprofile
  sms-profile: ”NetScalerSMS”
     rules:
      -
        metric: ”total_requests”
        operator: ”greaterthan”
        value: 25
        period-unit: weekly
```



```
15          -
16            metric: "total_bytes"
17            operator: "lessthan"
18            value: 1024
19            period-unit: day
20
21  <!--NeedCopy-->
```

Ausdrücke

April 28, 2021

Eine der mächtigsten Funktionen eines StyleBook ist die Verwendung von Ausdrücken. Sie können StyleBooks Ausdrücke in verschiedenen Szenarien verwenden, um dynamische Werte zu berechnen. Das folgende Beispiel ist ein Ausdruck, um einen Parameterwert mit einer Literalzeichenfolge zu verketten.

Beispiel:

```
1  $parameters.appname + "-mon"
```

Dieser Ausdruck ruft den Parameter mit dem Namen `appname` ab und verkettet ihn mit der Zeichenfolge `-mon`.

Die folgenden Ausdruckstypen werden unterstützt:

Arithmetische Ausdrücke

- Zusatz (+)
- Subtraktion (-)
- Multiplikation (*)
- Abteilung (/)
- Modulo (%)

Beispiele:

- Hinzufügen von zwei Zahlen: $parameters.a + $parameters.b
- Multiplikation von zwei Zahlen: $parameters.a * 10
- Den Rest nach der Division einer Nummer durch eine andere finden:

`15%10` Ergebnisse in `5`

Zeichenfolgenausdrücke

- Verketten Sie zwei Strings (+)

Beispiel:

Verketten Sie zwei Strings: str (app-) + $parameters.appname

Ausdrücke auflisten

Zusammenführen von zwei Listen (+)

Beispiel:

- Verketten Sie zwei Listen: $parameters.external-servers + $parameters.internal-servers
- Wenn `$parameters.ports-1`[80, 81] ist und `$parameters.port-2`ist [81, 82], wird `$parameters.ports-1 + $parameters.ports-2`als eine Liste [80, 81, 81, 82]angezeigt.

Relationale Ausdrücke

- **==** : Prüft, ob zwei Operanden gleich sind und gibt true zurück, wenn sie gleich sind, sonst gibt false zurück.
- **!!** =: Prüft, ob zwei Operanden unterschiedlich sind und gibt true zurück, wenn sie unterschiedlich sind, sonst gibt false zurück.
- ** : Gibt true zurück, wenn der erste Operand größer als der zweite Operanden ist, sonst gibt false zurück.
- **>=** : Gibt true zurück, wenn der erste Operanden größer oder gleich dem zweiten Operanden ist, sonst gibt false zurück.
- **<** : Gibt true zurück, wenn der erste Operand kleiner als der zweite Operanden ist, sonst wird false zurückgegeben.
- **<=** : Gibt true zurück, wenn der erste Operanden kleiner oder gleich dem zweiten Operanden ist, sonst wird false zurückgegeben.

Beispiel:

- Verwendung des Gleichheitsoperator: `$parameters.name = = ”abcd”`
- Verwendung des Operators “Ungleichheit”: `$parameters.name != ”default”`
- Beispiele für andere relationale Operatoren

```
- 10 > 9
- 10 >= 10
- 0 < 9
```



```
- 10 <= 9
- 10 == 10
- 10 != 1
```

Logische Ausdrücke - boolescher Wert

- **und**: Der logische 'und' Operator. Wenn beide Operanden wahr sind, ist das Ergebnis wahr, sonst ist es falsch.
- **oder**: Der logische 'oder' Operator. Wenn einer der Operanden wahr ist, ist das Ergebnis wahr, sonst ist es falsch.
- **nicht**: Der unäre Operator. Wenn der Operand wahr ist, ist das Ergebnis falsch und umgekehrt.
- **in**: Prüft, ob das erste Argument eine Teilzeichenfolge des zweiten Arguments ist
- **in**: Prüft, ob ein Element Teil einer Liste ist

> **Hinweis**
>
> Sie können Ausdrücke typisieren, bei denen Strings in Zahlen umgewandelt werden (mit der integrierten () integrierten Funktion) und Zahlen in Strings konvertiert werden (mit der eingebauten Funktion str ()). In ähnlicher Weise können Sie `tcp-port` auf eine Zahl umwandeln (mit der integrierten () integrierten Funktion), und eine IP-Adresse kann in eine Zeichenfolge umgewandelt werden (mit der integrierten Funktion str ()).
>
> Verwenden Sie ein Trennzeichen vor und nach einem Operator. Sie können die folgenden Trennzeichen verwenden:
>
> - Vor einem Operator: `space`, `tab`, `comma`, `(`, `)`, `[`, `]`
> - Nach einem Operator: `space`, `tab`, `(`, `[`
>
> Beispiel:
>
> - `abc + def`
> - `100 % 10`
> - `10 > 9`
> - `$item in $parameters.some-list`

Wörtliche Zeichenfolgenausdrücke

Sie können wörtliche Zeichenfolgen verwenden, wenn Sonderzeichen in einer Zeichenfolge ihre literale Form annehmen müssen. Diese Zeichenfolgen können Escape-Zeichen, umgekehrter Schrägstrich, Anführungszeichen, Klammern, Leerzeichen, Klammern usw. enthalten. In wörtlichen

Strings wird die übliche Interpretation der Sonderzeichen übersprungen. Alle Zeichen in der Zeichenfolge werden in ihrer literalen Form beibehalten.

In StyleBooks können Sie Citrix ADC Richtlinienausdrücke mithilfe von wörtlichen Zeichenfolgen in ihre literale Form einschließen. Die Richtlinienausdrücke enthalten in der Regel Sonderzeichen. Ohne wörtliche Strings müssen Sie Sonderzeichen entgehen, indem Sie Strings in Teilzeichenfolgen unterteilen.

Um eine wörtliche Zeichenfolge zu erstellen, kapseln Sie eine Zeichenfolge wie folgt zwischen Sonderzeichen:

```
~{
 string }
 ~
<!--NeedCopy-->
```

Sie können wörtliche Strings in den StyleBook-Ausdrücken verwenden.

> **Hinweis**
>
> Verwenden Sie nicht die Zeichenfolge `} ~` in einer Eingabezeichenfolge, da diese Sequenz das Ende einer wörtlichen Zeichenfolge angibt.

Beispiel:

```
 ~{
 HTTP.REQ.COOKIE.VALUE(”jsessionid”) ALT HTTP.REQ.URL.BEFORE_STR(”=”).
    AFTER_STR(”;jsessionid=”) ALT HTTP.REQ.URL.AFTER_STR(”;jsessionid=”
    ) }
 ~
<!--NeedCopy-->
```

Verketten Sie mehrere wörtliche Strings

Sie können wörtliche Strings mit den regulären Strings oder Strings mit Interpolationen verketten. Wenn Sie dies tun, überspringt das StyleBook die Interpretation nur für die wörtlichen Strings. Verwenden Sie den Plus-Operator (+) zwischen den Strings, um zu verketten.

Beispiel:

```
value: ”~{
```



```
2   "id": " }
3   ~ + %{
4   $atom.key }
5   % + ~{
6   ", "value": " }
7   ~ + %{
8   $atom.value }
9   % + ~{
10  " }
11  ~"
12 <!--NeedCopy-->
```

In diesem Beispiel `%{ $atom.key } %` und `%{ $atom.value } %` werden interpretiert. Und die Interpretation wird für den Rest übersprungen.

Target-Ausdrücke

In einer StyleBook-Definition können Sie den `$current-target` Ausdruck verwenden, um auf die aktuelle ADC-Zielinstanz zu verweisen. Um eine IP-Adresse der Ziel-ADC-Instanz ausdrücklich zu referenzieren, verwenden Sie diesen Ausdruck wie folgt:

```
1 $current-target.ip
2 <!--NeedCopy-->
```

Beispiel:

```
1 components:
2  -
3   name: lb-comp
4   type: ns::lbvserver
5   properties:
6     name: $current-target.ip + "-lbvserver"
7 <!--NeedCopy-->
```

In diesem Beispiel `lbvserver` verwendet der Name der die IP-Adresse der ADC-Zielinstanz.

Ausdruckstypvalidierung

Die StyleBook-Engine ermöglicht jetzt eine stärkere Typprüfung während der Kompilierungszeit, dh die beim Schreiben des StyleBook verwendeten Ausdrücke werden beim Import eines StyleBook selbst validiert, anstatt das Konfigurationspaket zu erstellen.

Alle Verweise auf Parameter, Substitutionen, Komponenten, Eigenschaften von Komponenten, Ausgaben von Komponenten, benutzerdefinierte Variablen (Repeat-Item, Repeat-Index, Argumente auf Substitutionsfunktionen) usw. werden auf ihre Existenz und Typen validiert.

Beispiel für Typprüfungen:

Im folgenden Beispiel ist der erwartete Typ der Porteigenschaft von `lbvserver`StyleBook `tcp-port`. In Citrix Application Delivery Management (ADM) werden die Typvalidierungen zur Kompilierungszeit (Importzeit) durchgeführt. Der Compiler findet diese Zeichenfolge und `tcp-port`sind nicht kompatible Typen. Daher zeigt der StyleBook-Compiler einen Fehler an und kann ein StyleBook nicht importieren oder migrieren.

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str(”80”)
      servicetype: HTTP
<!--NeedCopy-->
```

Um dieses StyleBook erfolgreich zu kompilieren, deklarieren Sie Folgendes als Zahl im Compiler:

```
port: 80
```

Beispiel für das Kennzeichnen ungültiger Ausdrücke:

In früheren Versionen hat der Compiler, wenn einem Eigenschaftsnamen ein ungültiger Ausdruck zugewiesen wurde, keine ungültigen Ausdrücke erkannt und die StyleBooks in Citrix ADM importiert werden können. Wenn dieses StyleBook nun in Citrix ADM importiert wird, identifiziert der Compiler solche ungültigen Ausdrücke und kennzeichnet es. Daher kann das StyleBook nicht in Citrix ADM importiert werden.

In diesem Beispiel lautet der Ausdruck, der der name-Eigenschaft in der `lb-sg-binding-comp` Komponente zugewiesen ist: `$components.lbvserver-comp.properties.lbvservername`. Es gibt jedoch keine Eigenschaft, die `lbvservername`in der Komponente aufgerufen wird `lbvserver-comp` . In früheren Citrix ADM Versionen hätte der Compiler diesen Ausdruck zugelassen und erfolgreich importiert. Der tatsächliche Fehler tritt auf, wenn ein Benutzer ein Konfigurationspaket mit diesem StyleBook erstellen möchte. Diese Art von Fehler wird jedoch beim Import erkannt und das StyleBook wird nicht in Citrix ADM importiert. Korrigieren Sie solche Fehler manuell und importieren Sie die StyleBooks.


```
Components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.lbvservername
      servicegroupname: $components.sg-comp.properties.servicegroupname
<!--NeedCopy-->
```

Indizierungslisten

Auf Elemente einer Liste kann jetzt zugegriffen werden, indem sie direkt indiziert werden:

Ausdruck	Beschreibung
`$components.test-lbs[0]`	Bezieht sich auf das erste Element in der `thetest-lbs` Komponente
`$components.test-lbs[0].properties.p1`	Bezieht sich auf die Eigenschaft p1 des ersten Elements in der Test-lbs Komponente
`$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname`	Bezieht sich auf die Eigenschaft `servicegroupname` des zweiten Elements in der `servicegroups` Komponente, bei der es sich um eine Ausgabe des ersten Elements der `lbcomps` Komponente handelt

In-Place-Interpolationen

April 28, 2021

Es ist jetzt möglich, Teile einer Zeichenfolge durch einen StyleBook-Ausdruck zu ersetzen. Wenn diese String-Ausdrücke vom StyleBook-Compiler ausgewertet werden, wird der Teil der Zeichenfolge, der einen StyleBook-Ausdruck verwendet, durch einen Wert des Ausdrucks ersetzt. Um StyleBook-Ausdrücke in eine Zeichenfolge aufzunehmen, verwenden wir die folgende Notation:

```
1 "...%{
2  ... }
3  %..."
4 <!--NeedCopy-->
```

Wo die zwischen"% {"und "}%" eingeschlossenen Zeichen einen StyleBook-Ausdruck bilden. Diese Ausdrücke werden als In-Place-Interpolationen bezeichnet.

Zum Beispiel `lb-%{ $parameters.appname } %-svc` ist der String ein String-Ausdruck mit einer In-Place-Interpolation eines StyleBook-Ausdrucks. Der Wert des String-Ausdrucks hängt vom Wert des Interpolationsausdrucks ab. Beachten Sie, dass **$parameters.appname** mit "app1" zugewiesen ist. Dann wird der Zeichenfolgenausdruck zu **lb-app1-svc**ausgewertet. Dadurch können die Werte in Zeichenfolgenausdrücken nicht fest codiert werden, sondern anhand der benutzerdefinierten Werte ausgewertet werden.

Ein praktischer Anwendungsfall von In-Place-Interpolationen besteht darin, Richtlinienausdrücke in StyleBooks zu parametrieren. Betrachten Sie ein Szenario, in dem Sie einen Richtlinienausdruck schreiben möchten, der prüft, ob die HTTP-URL ein bestimmtes Wort enthält, beispielsweise "jpeg".

Dazu schreiben Sie einen Richtlinienausdruck wie folgt: "HTTP.REQ.URL.CONTAINS(\"jpeg\")".

Wenn Sie nun das Objekt in der HTTP-URL parametrisieren möchten, können Sie im StyleBook beispielsweise einen String-Parameter hinzufügen `$parameters.url-object`. Der Richtlinienausdruck wird basierend auf diesem Parameter geschrieben. Dazu verwenden Sie String-Verkettung, um das Ergebnis zu erzielen. Der Ausdruck würde wie folgt aussehen:

```
1 str("HTTP.REQ.URL.CONTAINS(\\"" + $parameters.url-object + "\\")")
2 <!--NeedCopy-->
```

Wenn "csv" zugewiesen `$parameter.url-object` wird, wird der obige Ausdruck zu "HTTP.REQ.URL.CONTAINS (\" csv\")" ausgewertet. Dieser Ausdruck ist jedoch nicht leicht zu lesen. Um diese Parametrierung leicht zu lesen und zu verstehen, können Sie direkte Interpolationen verwenden.

Der Ausdruck mit direkter Interpolation lautet nun:

```
str(”HTTP.REQ.URL.CONTAINS(%{
 quotewrap($parameters.url-object) }
 %)”)
<!--NeedCopy-->
```

Im obigen Ausdruck haben Sie einen Interpolationsausdruck verwendet, der die inneren Anführungszeichen um den Wert des $parameters.url-Objekts hinzufügt. Das Ergebnis dieses Ausdrucks ist das gleiche wie oben, aber es sieht intuitiver aus und nähert sich dem tatsächlichen Ergebnis.

Zulässige Typen innerhalb von Interpolationen

Sie können Ausdrücke verwenden, die einen Wert der folgenden Typen in Interpolationen generieren: boolean, number `tcp-portipaddress`, und string. Der generierte Wert wird automatisch in eine Zeichenfolge umgewandelt, wenn die Interpolationen durch das Ergebnis ersetzt werden.

Zeichenfolgenausdrücke können 0, 1 oder mehr Interpolationen aufweisen. In einer sequenziellen Interpolation können verschiedene Teile des Zeichenfolgenausdrucks durch verschiedene StyleBook-Ausdrücke ersetzt werden. Die Zeichenfolge g lb-%{$parameters.appname}%-%{$parameters.vip}% gibt “lb-app1-1.1.1.1” zurück, wenn $parameters.appname “app1” und $parameters.vip “1.1.1.1” ist.

String-Ausdrücke unterstützen auch verschachtelte Interpolationen. Das heißt, ein Interpolationsausdruck kann in einem anderen Interpolationsausdruck verschachtelt werden, so dass der Wert eines Ausdrucks eine Eingabe für den zweiten Ausdruck werden kann.

Betrachten Sie beispielsweise die Zeichenfolge “%{lb-%{$parameters.port + 1}%}%”

Die interne Zeichenfolge “**%{$parameters.port + 1}%**” gibt “lb-81” zurück, wenn $parameters.port 80 ist. Hier ist dieser Ausdruck in einem anderen Interpolationsausdruck verschachtelt.

In der folgenden Tabelle werden die verschiedenen Interpolationstypen mit Beispielen und entsprechenden Ergebnissen beschrieben. Der Wert der in den Beispielen verwendeten Parameter ist:

- $parameters.appname: “lb1”
- $parameters.vip: “1.1.1.1”
- $parameters.n1: 1
- $parameters.n2: 3

Einfache Interpolationen

Ausdruck	Ergebnis
`lb-%{ $parameters.appname } %-def`	`lb-lb1-def`

Automatische Typkonvertierungen

Ausdruck	Ergebnis
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

Sequenzielle Interpolationen

Ausdruck	Ergebnis
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

Verschachtelte Interpolationen

Ausdruck	Ergebnis
`%{ abc-%{ $parameters.n1 + 1 } % } %`	`abc-2`
`str("%{ abc-%{ $parameters.n1 } % } %-%{ $parameters.n2 } %")`	`bc-1-3`

Interpolationen mit `quotewrap`

Ausdruck	Ergebnis
`str("%{ quotewrap(abcd)} %")`	`\"abcd\`
`str("%{ quotewrap(https://)} %+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")`	`<https://"+HTTP.REQ.HOST NAME+HTTP.REQ.URL`

Escape-Zeichen in Interpolationen

Wenn die Zeichen"%{" or "}%" Teil der Zeichenfolge sind, müssen Sie "\" als Escape-Zeichen angeben, damit der StyleBook-Compiler diese nicht als Interpolationstags auswertet.

Beispiel:

```
str("%{ \\%\\{ + str($parameters.vip)+ \ } \\% } %")returns "%{ 1.1.1.1 } %
"if $parameters.vip is 1.1.1.1
```

In der folgenden Tabelle werden einige weitere Ausdrücke und deren Ergebnisse beschrieben:

Kategorie	Ausdruck	Ergebnis
—	—	—
Escape-Interpolationen	`str("%{ str($parameters.n1)+ \ } \\% } %")`	`1 } %`
	`lb-%{ str($parameters.n1)+ \ } \\% } %`	`lb-1 } %`
	`"%{ str($parameters.n1)+ \\"\\ } \\\%\\"} %"`	`1 } %`

Integrierte Funktionen

April 28, 2021

Ausdrücke in StyleBooks können integrierte Funktionen verwenden.

Beispielsweise können Sie die integrierte Funktion verwenden, `str()` um eine Zahl in eine Zeichenfolge umzuwandeln.

```
str($parameters.order)
```

Oder Sie können die integrierte Funktion verwenden, `int()` um eine Zeichenfolge in eine Ganzzahl umzuwandeln.

```
int($parameters.priority)
```

Im Folgenden finden Sie die Liste der integrierten Funktionen, die in StyleBook-Ausdrücken unterstützt werden, mit Beispielen, wie sie verwendet werden können:

str()

Die `str()` Funktion transformiert das Eingabeargument in einen String-Wert.

Zulässige Argumenttypen:

- `string`
- `number`
- `TCP-port`

- **boolean**
- IP address

Beispiele:

- Die Funktion "set-"+ str(10) gibt "set-10" zurück.
- Die Funktion str(10) gibt 10 zurück.
- Die Funktion str(1.1.1.1) gibt 1.1.1.1 zurück.
- Die Funktion str(T rue) gibt "T rue" zurück.
- Die Funktion str(ADM) gibt "mas" zurück.

int()

Die **int**() Funktion verwendet eine Zeichenfolge, eine Zahl, eine IP-Adresse oder tcpport als Argument und gibt eine Ganzzahl zurück.

Beispiele:

- Die Funktion **int**("10") gibt 10 zurück.
- Die Funktion **int**(10) gibt 10 zurück.
- Die Funktion **int**(ip('0.0.4.1')) gibt 1025 zurück.

bool()

Die bool() Funktion verwendet einen beliebigen Typ als Argument. Wenn der Argumentwert leer oder nicht vorhanden ist **false**, wird diese Funktion zurückgegeben **false**.

Ansonsten kehrt es zurück **true**.

Beispiele:

- Die Funktion bool(**true**) gibt **true** zurück.
- Die Funktion bool(**false**) gibt **false** zurück.
- Die bool($parameters.a) Funktion gibt zurück **false**, **false** wenn der leer $parameters.a ist oder nicht vorhanden ist.

len()

Die len() Funktion verwendet eine Zeichenfolge oder eine Liste als Argument und gibt die Anzahl der Zeichen in einer Zeichenfolge oder die Anzahl der Elemente in einer Liste zurück.

Beispiel 1:

Wenn Sie eine Substitution wie folgt definieren:

```
items: ["123", "abc", "xyz"]
```


Die Funktion `len($substitutions.items)` gibt `3` zurück.

Beispiel 2:

Die Funktion `len("Citrix ADM")` gibt `10` zurück.

Beispiel 3:

Wenn `$parameters.vips` Werte vorhanden sind `['1.1.1.1', '1.1.1.2', '1.1.1.3']`, wird die `len($parameters.vips)` Funktion zurückgegeben `3`.

min()

Die `min()` Funktion verwendet entweder eine Liste oder eine Reihe von Zahlen oder `tcp-ports` als Argumente und gibt das kleinste Element zurück.

Beispiele mit einer Reihe von Zahlen/TCP-Ports:

- Die Funktion `min(80, 100, 1000)` gibt `80` zurück.
- Die Funktion `min(-20, 100, 400)` gibt `-20` zurück.
- Die Funktion `min(-80, -20, -10)` gibt `-80` zurück.
- Die Funktion `min(0, 100, -400)` gibt `-400` zurück.

Beispiele mit einer Liste von Zahlen/TCP-Ports:

- Support `$parameters.ports` ist eine Liste von `tcp-ports` und hat Werte: `[80, 81, 8080]`.

  Die Funktion `min($parameters.ports)` gibt `80` zurück.

max()

Die `max()` Funktion verwendet entweder eine Liste oder eine Reihe von Zahlen oder `tcp-ports` als Argumente und gibt das größte Element zurück.

Beispiele mit einer Reihe von Zahlen/TCP-Ports:

- Die Funktion `max(80, 100, 1000)` gibt `1000` zurück.
- Die Funktion `max(-20, 100, 400)` gibt `400` zurück.
- Die Funktion `max(-80, -20, -10)` gibt `-10` zurück.
- Die Funktion `max(0, 100, -400)` gibt `100` zurück.

Beispiele mit einer Liste von Zahlen/TCP-Ports:

- Unterstützung `$parameters.ports` ist Liste von `tcp-ports` und hat Werte: `[80, 81, 8080]`.

  Die Funktion `max($parameters.ports)` gibt `8080` zurück.

bin()

Die `bin()` Funktion verwendet eine Zahl als Argument und gibt eine Zeichenfolge zurück, die die Zahl im Binärformat darstellt.

Beispiele für Ausdrücke:

Die Funktion `bin(100)` gibt `0b1100100` zurück.

oct()

Die `oct()` Funktion verwendet eine Zahl als Argument und gibt eine Zeichenfolge zurück, die die Zahl im Oktalformat darstellt.

Beispiele für Ausdrücke:

Die Funktion `oct(100)` gibt `0144` zurück.

hex()

Die `hex()` Funktion verwendet eine Zahl als Argument und gibt eine Kleinbuchstabenzeichenfolge zurück, die die Zahl im Hexadezimalformat darstellt.

Beispiele für Ausdrücke:

Die Funktion `hex(100)` gibt `0x64` zurück.

lower()

Die `lower()` Funktion verwendet eine Zeichenfolge als Argument und gibt die gleiche Zeichenfolge in Kleinbuchstaben zurück.

Beispiel:

Die Funktion `lower("ADM")` gibt `adm` zurück.

upper()

Die `upper()` Funktion verwendet eine Zeichenfolge als Argument und gibt dieselbe Zeichenfolge in Großbuchstaben zurück.

Beispiel:

Die Funktion `upper("Citrix ADM")` gibt `CITRIX ADM` zurück.

sum()

Die `sum()` Funktion nimmt eine Liste von Zahlen oder `tcpports` als Argumente und gibt die Summe der Zahlen in der Liste zurück.

Beispiel 1:

Wenn Sie eine Substitution wie folgt definieren:
Substitutionen:

```
list-of-numbers = [11, 22, 55]
```

Die Funktion `sum($substitutions.list-of-numbers)` gibt `88` zurück.

Beispiel 2:

Wenn ja `$parameters.ports[80, 81, 82]`, kehrt die `sum($parameters.ports)` Funktion zurück `243`.

pow()

Die `pow()` Funktion nimmt zwei Zahlen als Argumente und gibt eine Zahl zurück, die das erste Argument darstellt, das die Potenz des zweiten darstellt.

Beispiel:

Die Funktion `pow(3,2)` gibt `9` zurück.

ip()

Die `ip()` Funktion verwendet eine Ganzzahl, einen String oder eine IP-Adresse als Argument und gibt die IP-Adresse basierend auf dem Eingabewert zurück.

Beispiele:

- Geben Sie eine IP-Adresse in der `ip` Funktion an:

  Die Funktion `ip(3.1.1.1)` gibt `3.1.1.1` zurück.

- Geben Sie eine Zeichenfolge in der `ip` Funktion an:

  Die Funktion `ip('2.1.1.1')` gibt `2.1.1.1` zurück.

- Geben Sie eine Ganzzahl in der `ip` Funktion an:

  - Die Funktion `ip(12)` gibt `0.0.0.12` zurück.
  - Wenn Sie eine Ganzzahl als String in der `ip` Funktion angeben, wird eine entsprechende IP-Adresse der Eingabe zurückgegeben.

    Die Funktion `ip('1025')` gibt `0.0.4.1` zurück.

Diese Funktion unterstützt auch die Integer-Additions- und Subtraktionsoperationen und gibt eine resultierende IP-Adresse zurück.

- Zusatz: Die `ip(1025)+ ip(12)` Funktion kehrt zurück `0.0.4.13`.
- Subtraktion: Die `ip('1025')- ip(12)` Funktion kehrt zurück `0.0.3.245`.
- Kombinieren Sie Addition und Subtraktion: Die `ip('1.1.1.1')+ ip('1.1.1.1')- ip(2)` Renditen `2.2.2.0`.

ip_network()

Die `ip_network` Funktion verwendet IP-Adresse und Netzmaskenlänge als Argumente und gibt eine IP-Netzwerknotation zurück.

Example-1:

Die Funktion `ip_network(1.1.1.1, 28)` gibt `1.1.1.1/28` zurück.

Example-2:

Betrachte das Netzwerk `1.1.1.1/30`. Die Funktion `ip_network($parameters.ipaddr, 30)` gibt `1.1.1.1` zurück.

Example-3:

Betrachte das Netzwerk `23.1.12.76/24`. Die Funktion `ip_network(23.1.12.76, $parameters.netmask-len)` gibt `24` zurück.

network_ip()

Die `network_ip()` Funktion gibt die erste IP-Adresse des angegebenen IP-Netzwerks zurück.

Beispiel:

Die Funktion `network_ip(1.1.1.1/28)` gibt `1.1.1.0` zurück. In diesem Beispiel `1.1.1.0` ist die erste IP-Adresse im angegebenen Netzwerk.

subnets()

Die `subnets()` Funktion gibt die Liste der Subnetze des angegebenen IP-Netzwerks und der Netzmaskenlänge zurück.

Beispiel:

Die `subnets(1.1.1.1/28, 30)` Funktion gibt die Subnetzliste aus dem angegebenen IP-Netzwerk und der Netzmaskenlänge zurück. Die Ausgabe kann wie folgt sein:

```
[1.1.1.0/30', '1.1.1.4/30', '1.1.1.8/30', '1.1.1.12/30']
```


netmask_ip()

Die `netmask_ip()` Funktion gibt die Netmask-IP-Adresse für das angegebene IP-Netzwerk zurück.

Beispiel:

Die Funktion `netmask_ip(1.1.1.1/28)` gibt `255.255.255.0` zurück. Im angegebenen IP-Netzwerk `255.255.255.0` ist die IP-Adresse der Netzmaske.

broadcast_ip()

Die `broadcast_ip()` Funktion gibt die Broadcast-IP-Adresse für das angegebene IP-Netzwerk zurück.

Beispiel:

Die Funktion `broadcast_ip(1.1.1.1/28)` gibt `1.1.1.15` zurück. Im angegebenen Netzwerk `1.1.1.1` ist die Broadcast-IP-Adresse.

cidr()

Die `cidr()` Funktion gibt die CIDR-Notation für das angegebene IP-Netzwerk zurück.

Beispiel:

Die `cidr(1.1.1.1/28)` Funktion gibt den zurück `1.1.1.0/28`. Im gegebenen Netzwerk `1.1.1.0/28` ist die CIDR-Notation.

is_cidr()

Die `is_cidr()` Funktion akzeptiert einen `ipnetwork` als Eingabe. Und es gibt zurück, `True` ob der angegebene Wert mit der CIDR-Notation des IP-Netzwerks übereinstimmt.

Example-1:

Die `is_cidr(1.1.1.0/24)` Funktion wird zurückgegeben, `True` da der angegebene Wert die CIDR-Notation des angegebenen Netzwerks ist.

Example-2:

Die `is_cidr(1.1.1.1/28)` Funktion wird zurückgegeben, `False` da sich die CIDR-Notation des angegebenen Netzwerks von dem angegebenen Wert unterscheidet.

is_in_network()

Die `is_in_network()` Funktion akzeptiert `ipnetwork` und `ipaddress` wertet. Und es gibt zurück, `True` ob die angegebene IP-Adresse im angegebenen IP-Netzwerk vorhanden ist.

Example-1:

Die `is_in_network(1.1.1.1/24, 1.1.1.121)` Funktion wird zurückgegeben `True`, da die `1.1.1.121` Adresse Teil des `1.1.1.1/24` Netzwerks ist.

Example-2:

Die `is_in_network(1.1.1.1/28, 2.1.1.1)` Funktion wird zurückgegeben `Fasle`, da die `2.1.1.1` Adresse nicht Teil des `1.1.1.1/28` Netzwerks ist.

base64.encode()

Die `base64.encode()` Funktion verwendet ein String-Argument und gibt die Base64-codierte Zeichenfolge zurück.

Beispiel:

Die Funktion `base64.encode("abcd")` gibt `YWJjZA==` zurück.

base64.decode()

Die `base64.decode` Funktion verwendet eine Base64-codierte Zeichenfolge als Argument und gibt die dekodierte Zeichenfolge zurück.

Beispiel:

Die Funktion `base64.decode("YWJjZA==")` gibt `abcd` zurück.

exists()

Die `exists()` Funktion verwendet ein Argument eines beliebigen Typs und gibt einen booleschen Wert zurück. Der Rückgabewert ist `True`, wenn die Eingabe einen Wert hat. Der Rückgabewert ist `False` Wenn das Eingabeargument keinen Wert hat (also keinen Wert).

Bedenken Sie, dass der ein optionaler Parameter `$parameters.monitor` ist. Wenn Sie beim Erstellen eines Konfigurationspakets einen Wert für diesen Parameter angeben, gibt die `($parameters.monitor)` Funktion zurück `True`.

Ansonsten kehrt es zurück `False`.

filter()

Die `filter()` Funktion benötigt zwei Argumente.

Argument 1: eine Substitutionsfunktion, die ein Argument annimmt und einen booleschen Wert zurückgibt.

Argument 2: eine Liste.

Die Funktion gibt eine Teilmenge der ursprünglichen Liste zurück, zu der jedes Element `True` bei der Übergabe an die Substitutionsfunktion im ersten
Argument ausgewertet wird.

Beispiel:

Angenommen, wir haben eine Substitutionsfunktion wie folgt definiert.

Substitutionen:

```
x(a): $a != 81
```

Diese Funktion gibt True zurück, wenn der Eingabewert nicht gleich ist `81`. Ansonsten kehrt es zurück `False`.

Nehmen wir an,`$parameters.ports` ist es `[81, 80, 81, 89]`.

Die `filter($substitutions.x, $parameters.ports)` Rückgabe, `[80, 89]` indem alle Vorkommen von `81` aus der Liste entfernt werden.

if-then-else()

Die Funktion **`if`**`-then-`**`else`**`()` benötigt drei Argumente.

Argument 1: Boolescher Ausdruck

Argument 2: Beliebiger Ausdruck

Argument 3: Beliebiger Ausdruck (optional)

Wenn der Ausdruck in Argument 1 zu ausgewertet wird `True`, gibt die Funktion den Wert des als Argument 2 bereitgestellten Ausdrucks zurück.

Andernfalls, wenn Argument 3 angegeben wird, gibt die Funktion den Wert des Ausdrucks in Argument 3 zurück.

Wenn Argument 3 nicht angegeben wird, kehrt die Funktion zurück `no`.

Beispiel 1:

Die **`if`**`-then-`**`else`**`($parameters.servicetype == HTTP, 80, 443)` Funktion gibt zurück `80` , wenn Wert `$parameters.servicetype` hat `HTTP`. Andernfalls wird die Funktion zurückgegeben `443`.

Beispiel 2:

Die **`if`**`-then-`**`else`**`($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` Funktion gibt den Wert von `$parameters.hport` if `$parameters.servicetype` has value zurück `HTTP`.

Andernfalls gibt die Funktion den Wert von zurück `$parameters.sport`.

Beispiel 3:

Die `if-then-else($parameters.servicetype == HTTP, 80)` gibt zurück `80`, wenn Wert `$parameters.servicetype` hat `HTTP`.

Andernfalls gibt die Funktion keinen Wert zurück.

join()

Die `join()` Funktion hat zwei Argumente:

Argument 1: Liste von Zahlen `tcp-ports`, Strings oder IP-Adressen

Argument 2: Trennzeichenfolge (optional)

Diese Funktion verbindet die Elemente der Liste, die als Argument eins bereitgestellt werden, in einer Zeichenfolge, wobei jedes Element durch die als Argument zweite angegebene Begrenzungszeichenfolge getrennt ist. Wenn Argument zwei nicht angegeben wird, werden die Elemente in der Liste als eine Zeichenfolge verbunden.

Beispiel:

- `$parameters.ports` ist `[81, 82, 83]`.
  - Mit Trennzeichen Argument:

    Die Funktion `join($parameters.ports, '-')` gibt `81-82-83` zurück.
  - Ohne Trennzeichen Argument:

    Die Funktion `join($parameters.ports)` gibt `818283` zurück.

split()

Die `split()` Funktion teilt eine Eingabezeichenfolge in mehrere Listen auf, abhängig von den angegebenen Trennzeichen. Wenn kein oder leeres (`''`) Trennzeichen angegeben wird, betrachtet diese Funktion das Leerzeichen als Trennzeichen und teilt die Zeichenfolge in Listen auf.

Beispiele:

- Die Funktion `split('Example_string_split', 's')` gibt `['Example_','tring_','plit']` zurück.
- Die Funktion `split('Example string split')` gibt `['Example','string','split']` zurück.
- Die Funktion `split('Example string split', '')` gibt `['Example','string','split']` zurück.

- Die Funktion `split('Example string')` gibt `['Example','string']` zurück.

  Diese Funktion betrachtet kontinuierliche Räume als ein Leerzeichen.

map()

Die `map()` Funktion benötigt zwei Argumente;

Argument 1: Jede Funktion

Argument 2: Eine Liste von Elementen.

Die Funktion gibt eine Liste zurück, in der jedes Element in der Liste das Ergebnis der Anwendung der `map()` Funktion (Argument eins) auf das entsprechende Element in Argument zwei ist.

Zulässige Funktionen in Argument 1:

- Integrierte Funktionen, die ein Argument annehmen:

  `base64.encode`, `base64.decode`, `bin`, `bool`, `exists`, `hex`, **`int`**, `ip`, `len`, `lower`, `upper`, `oct`, `quotewrap`, `str`, `trim`, `upper`, `url.encode`, `url.decode`

- Substitutionsfunktionen, die mindestens ein Argument verwenden.

Beispiel:

Suppose $parameters.nums is `[81, 82, 83]`.

- Map using a built-in function, str

  Die Funktion `map(str, $parameters.nums)` gibt `["81", "82", "83"]` zurück.

  Das Ergebnis der Map-Funktion ist die Liste der Strings, in denen jedes Element String ist, wird durch Anwenden der str Funktion auf das entsprechende Element in der Eingabeliste berechnet ($parameters.nums).

- Zuordnung mit einer Substitutionsfunktion

  - Substitutionen:

    `add-10(port): $port + 10`

  - Ausdruck:

    Die `map($substitutions.add-10, $parameters.nums)` Funktion gibt eine Liste von Zahlen zurück: `[ 91, 92, 93 ]`

Das Ergebnis dieser Map-Funktion ist eine Liste von Zahlen, wobei jedes Element durch Anwendung der Substitutionsfunktion `$substitutions.add-10` auf das entsprechende Element in der Eingabeliste berechnet wird `($parameters.nums)`.

quotewrap()

Die `quotewrap()` Funktion verwendet eine Zeichenfolge als Argument und gibt eine Zeichenfolge zurück, nachdem vor und nach dem Eingabewert ein doppeltes Anführungszeichen hinzugefügt wurde.

Beispiel:

Die Funktion `quotewrap("ADM")` gibt `"mas"` zurück.

replace()

Die `replace()` Funktion hat drei Argumente:

Argument 1: Zeichenfolge

Argument 2: String oder Liste

Argument 3: Zeichenfolge (optional)

Die Funktion ersetzt alle Vorkommen von Argument zwei durch Argument drei in Argument eins.

Wenn Argument drei nicht angegeben wird, werden alle Vorkommen von Argument zwei aus dem ersten Argument entfernt (mit anderen Worten, durch eine leere Zeichenfolge ersetzt).

Ersetzen Sie eine Teilzeichenfolge durch eine andere Teilzeichenfolge:

- Die Funktion `replace('abcdef', 'def', 'xyz')` gibt `abcxyz` zurück.

  Alle Vorkommnisse von `def` werden durch ersetzt `xyz`.

- `replace('abcdefabc', 'def')` kehrt zurück `abcabc`.

  Da es kein drittes Argument gibt, `def` wird aus der resultierenden Zeichenfolge entfernt.

Geben Sie die Liste der Zeichen an, die Sie in einer Zeichenfolge ersetzen möchten.

```
$parameters.spl_chars = ['@', '##', '!', '%']
```

Diese Liste enthält die Werte, die in einer Eingabezeichenfolge ersetzt werden müssen.

Die Funktion `replace('An##example@to%replace!characters', $parameters.spl_chars, '_')` gibt `An_example_to_replace_characters` zurück.

Die Ausgabezeichenfolge hat einen unterstreichen (_) anstelle der in der `$parameters.spl_chars` Liste angegebenen Zeichen.

trim()

Die `trim()` Funktion gibt eine Zeichenfolge zurück, in der die führenden und nachfolgenden Leerzeichen aus der Eingabezeichenfolge entfernt werden.

Beispiel:

Die Funktion `trim('abc ')` gibt `abc` zurück.

truncate()

Die `truncate()` Funktion hat zwei Argumente:

Argument 1: Zeichenfolge

Argument 2: Zahl

Die Funktion gibt einen String zurück, wo die Eingabezeichenfolge in Argument 1 auf die Länge durch Argument zwei angegeben abgeschnitten wird.

Beispiel:

Die `truncate('Citrix ADM', 6)` Renditen `Citrix`.

distinct()

Die `distinct()` Funktion extrahiert eindeutige Elemente aus einer Listeneingabe.

Beispiele:
Wenn`$parameters.input_list ['ADM', 'ADC', 'VPX', 'ADC', 'ADM', 'CPX']` ist, gibt die Funktion`distinct($parameters.input_list) ['ADM', 'ADC', 'VPX', 'CPX']`zurück.

url.encode()

Die `url.encode()` Funktion gibt eine Zeichenfolge zurück, in die Zeichen mithilfe des ASCII-Zeichensatzes gemäß RFC 3986 transformiert werden.

Beispiel:

Die Funktion `url.encode("a/b/c")` gibt `a%2Fb%2Fc` zurück.

url.decode()

Die `url.decode()` Funktion gibt eine Zeichenfolge zurück, in der das URL-codierte Argument gemäß RFC 3986 in eine reguläre Zeichenfolge decodiert wird.

Beispiel:

Die Funktion `url.decode("a%2Fb%2Fc")` gibt `a/b/c` zurück.

is-ipv4()

Die `is-ipv4()` Funktion verwendet eine IP-Adresse als Argument und gibt den booleschen Wert zurück, `True` wenn die IP-Adresse im IPv4-Format vorliegt.

Die Funktion `is-ipv4(10.10.10.10)` gibt `True` zurück.

is-ipv6()

Die `is-ipv6()` Funktion nimmt eine IP-Adresse als Argument und gibt den booleschen Wert zurück, `True` wenn die IP-Adresse im IPv6-Format vorliegt.

Die Funktion `is-ipv6(2001:DB8::)` gibt `True` zurück.

startswith()

Die `startswith()`Funktion bestimmt, ob eine Zeichenfolge mit einem gegebenen Präfix beginnt. Diese Funktion erfordert zwei obligatorische Zeichenfolgenargumente.

```
startswith(str, sub_str)
```

Diese Funktion gibt zurück `True`, wenn die Zeichenfolge (`str`) mit der Teilzeichenfolge (`sub_str`) beginnt.

Beispiele:

- Die Funktion `startswith('Citrix', 'Ci')` gibt `True` zurück.
- Die Funktion `startswith('Citrix', 'iC')` gibt `False` zurück.
- Die Funktion `startswith('Citrix', 'Ab')` gibt `False` zurück.

endswith()

Die `endswith()`Funktion bestimmt, ob eine Zeichenfolge mit einem gegebenen Suffix endet. Diese Funktion erfordert zwei obligatorische Zeichenfolgenargumente.

```
endswith(str, sub_str)
```

Diese Funktion gibt zurück `True`, wenn die Zeichenfolge (`str`) mit der Teilzeichenfolge (`sub_str`) endet.

Beispiele:

- Die Funktion `endswith('Citrix', 'ix')` gibt `True` zurück.
- Die Funktion `endswith('Citrix', 'Ix')` gibt `False` zurück.
- Die Funktion `endswith('Citrix', 'ab')` gibt `False` zurück.

contains()

Die `contains()`Funktion bestimmt, ob ein String eine bestimmte Teilzeichenfolge enthält. Diese Funktion erfordert zwei obligatorische Zeichenfolgenargumente.

```
contains(str, sub_str)
```

Diese Funktion gibt zurück `True`, wenn die Teilzeichenfolge (`sub_str`) irgendwo innerhalb der Zeichenfolge (`str`) enthalten ist.

Beispiel:

- Die Funktion `contains('Citrix', 'tri')` gibt `True` zurück.
- Die Funktion `contains('Citrix', 'Ci')` gibt `True` zurück.
- Die Funktion `contains('Citrix', 'ti')` gibt `False` zurück.

substring()

Verwenden Sie die `substring()`Funktion, um eine Teilzeichenfolge aus einer Zeichenfolge zu extrahieren.

```
substring(str, start_index, end_index)
```

Diese Funktion erfordert die beiden obligatorischen Argumente und ein optionales ganzzahliges Argument.

- `str` (Obligatorisch)
- `start_index` (Obligatorisch)
- `end_index` Optional:

Diese Funktion gibt die Teilzeichenfolge aus der Zeichenfolge (`str`), die sich zwischen den angegebenen Indexpositionen befindet. Wenn Sie die Endindexposition nicht angeben, extrahiert die Funktion die Teilzeichenfolge vom Startindex bis zum Ende der Zeichenfolge.

> **Hinweis**
>
> Wenn Sie `end_index` angeben, schließt die Teilzeichenfolge das Zeichen an der Position `end_index` aus.

Beispiel:

- Die Funktion `substring('Citrix', 2)` gibt `trix` zurück.
- Die Funktion `substring('Citrix', 10)` gibt (”) zurück.

  In diesem Beispiel gibt die Funktion eine leere Zeichenfolge zurück, da sie eine ungültige Position `start_index` hat.
- Die Funktion `substring('Citrix', 2, 4)` gibt `tr` zurück.

  In diesem Beispiel extrahiert die Funktion die Zeichen zwischen 2 und 4 Indexpositionen.

- Die Funktion `substring('Citrix', -3)` gibt `rix` zurück.

  Wenn Sie Zeichen extrahieren möchten, die sich am Ende der Zeichenfolge befinden, geben Sie einen negativen Wert für das `start_index`Argument an.

  In diesem Beispiel extrahiert die Funktion die Teilzeichenfolge, die die letzten drei Zeichen in der Zeichenfolge enthält.

Abhängigkeitserkennung

April 28, 2021

Komponenten in einem StyleBook können auf Eigenschaften oder Abschnitte anderer Komponenten im selben StyleBook verweisen. Komponenten sind selbst komplette Blöcke und werden möglicherweise nicht in der gleichen Reihenfolge geschrieben, in der sie ausgeführt werden müssen. Der StyleBook-Compiler überprüft die Reihenfolge, in der die Komponenten geschrieben werden, und führt sie dann in einer logischen Reihenfolge aus.

Beispiel:

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

-
    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding
```



```
23
24      condition: $parameters.create-binding
25
26      properties:
27
28        name: $components.lbvserver-comp.properties.name
29
30        servicegroupname: $components.sg-comp.properties.servicegroupname
31
32  -
33      name: sg-comp
34
35      type: ns::servicegroup
36
37      properties:
38
39        servicegroupname: mysg
40
41        servicetype: HTTP
42  <!--NeedCopy-->
```

Im obigen Beispiel gibt es drei Komponenten definiert - **lbvserver-comp**, **lb-sg-binding-comp**und **sg-comp**. Wenn Sie dieses StyleBook ausführen, `lbvserver-comp` wird das zuerst erstellt. Das `lb-sg-binding-comp` bezieht sich auf `lbvserver-comp` Eigenschaften, kann jedoch nicht als nächstes erstellt werden, obwohl es die zweite im StyleBook definierte Komponente ist. Dies liegt daran, dass der `lb-sg-binding-comp` auch eine Abhängigkeit von dem hat `sg-comp`, das noch nicht geschaffen werden muss. Infolgedessen ordnet der Compiler die Komponenten neu an, sodass die Abhängigkeiten einer Komponente zum Zeitpunkt der Erstellung einer Komponente aufgelöst werden, und führt diese neu geordnete Liste von Komponenten aus. Die Ausführreihenfolge des obigen StyleBook ist: `lbvserver-comp`, `sg-comp` und `lb-sg-binding-comp`.

Daher muss sich der Autor eines StyleBook nicht um die korrekte Reihenfolge der Komponenten kümmern. Die Komponenten können in beliebiger Reihenfolge angezeigt werden. Der Compiler berechnet die korrekte Reihenfolge der Ausführung der Komponenten basierend darauf, wie die Komponenten einander verweisen. Beachten Sie, dass dies auch für Abschnitte zu Substitutionen und Ausgaben gilt.

Zyklische Abhängigkeiten

Da sich eine Komponente möglicherweise auf eine andere Komponente bezieht, ist es möglich, dass der Abhängigkeitskreislauf in die Definition des StyleBook eingeführt wird. Beispiel: Wenn Komponente A auf eine Eigenschaft verweist, die in Komponente B definiert ist, die wiederum auf eine Eigenschaft verweist, die in Komponente A definiert ist. Diese Art von Abhängigkeit wird als

zyklische Abhängigkeiten bezeichnet. Zyklische Abhängigkeiten können nicht automatisch aufgelöst werden. Der Autor des StyleBook korrigiert die StyleBook-Definition manuell, um solche zyklischen Abhängigkeiten zu eliminieren. Der Compiler kann zyklische Abhängigkeiten identifizieren - wenn sie existieren, und melden.

Das folgende Beispiel zeigt eine zyklische Abhängigkeit von Komponenten:

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: $components.lb-sg-binding-comp.properties.name

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

  -

    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    condition: $parameters.create-binding

    properties:

      name: mylb

      servicegroupname: $components.sg-comp.properties.servicegroupname

  -

    name: sg-comp

    type: ns::servicegroup
```



```
38
39     properties:
40
41       servicegroupname: mysg
42
43       servicetype: $components.lbvserver-comp.properties.servicetype
44 <!--NeedCopy-->
```

Im obigen Beispiel gibt es drei Komponenten: **lbvserver-comp**, **lb-sg-binding-comp**und **sg-comp**. Die `lbvserver-comp` Komponente hängt von den Komponenten `lb-sg-binding-comp`, `lb-sg-binding` ab. Und diese Komponenten hängen davon ab `sg-comp`. Die `sg-comp` Komponente hängt davon ab `lbvserver-comp`. Hier wird ein Zyklus von Abhängigkeiten zwischen diesen Komponenten gebildet, der nicht automatisch aufgelöst werden kann. Daher kann dieses StyleBook nicht ausgeführt werden. Der StyleBook-Compiler erkennt dies und verhindert, dass das StyleBook in Citrix ADM importiert wird.

Instanzverwaltung

April 28, 2021

Instanzen sind Citrix Application Delivery Controller (ADC) -Appliances, die Sie mit Citrix Application Delivery Management (ADM) verwalten, überwachen und beheben können. Fügen Sie Instanzen zu Citrix ADM hinzu, um sie zu überwachen. Instanzen können hinzugefügt werden, wenn Sie auch Citrix ADM oder höher einrichten. Nachdem Sie Citrix ADM Instanzen hinzugefügt haben, werden diese kontinuierlich abgefragt, um Informationen zu sammeln, die später zur Behebung von Problemen oder als Berichtsdaten verwendet werden können.

Instanzen können als statische Gruppe oder als privater IP-Block gruppiert werden. Eine statische Gruppe von Instanzen kann nützlich sein, wenn Sie bestimmte Aufgaben wie Konfigurationsaufträge und andere ausführen möchten. Ein privater IP-Block gruppiert Ihre Instanzen basierend auf ihren geografischen Standorten.

Hinzufügen einer Instanz

Sie können Instanzen hinzufügen, wenn Sie den Citrix ADM -Server zum ersten Mal oder später einrichten. Um Instanzen hinzuzufügen, müssen Sie entweder den Hostnamen oder die IP-Adresse jeder Citrix ADC-Instanz oder einen Bereich von IP-Adressen angeben.

Informationen zum Hinzufügen einer Instanz zu Citrix ADM finden Sie unterHinzufügen von Instanzen zu Citrix ADM.

Wenn Sie dem Citrix ADM-Server eine Instanz hinzufügen, fügt sich der Server implizit als Trap-Ziel für die Instanz hinzu und sammelt einen Inventar der Instanz. Weitere Informationen finden Sie unter Wie Citrix ADM Instanzen erkennt.

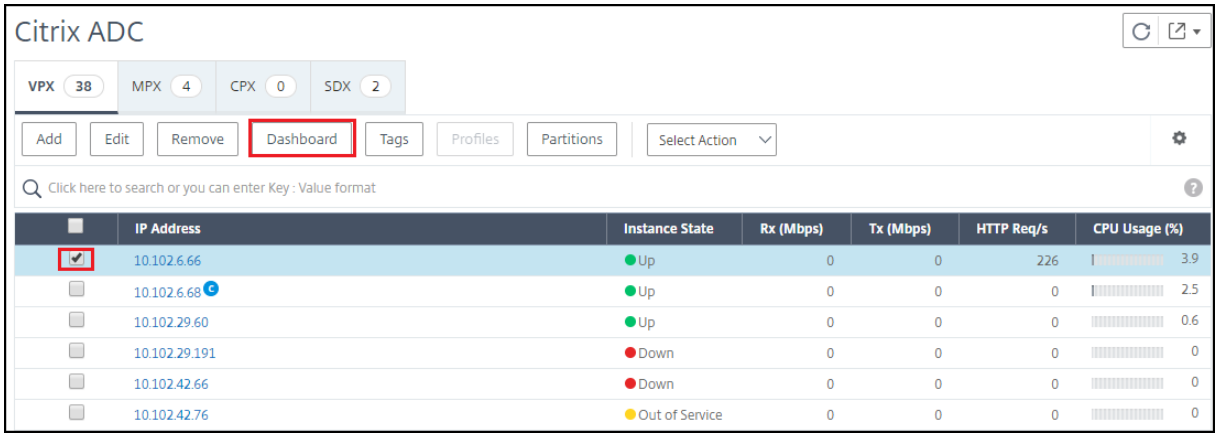
Nachdem Sie eine Instanz hinzugefügt haben, können Sie sie löschen, indem Sie zu **Netzwerke**> **Dashboard**navigieren und auf **Alle Instanzen**klicken. Wählen Sie auf der Seite Instanzen die Instanz aus, die Sie löschen möchten, und klicken Sie auf **Entfernen**.

So verwenden Sie das Instanz-Dashboard

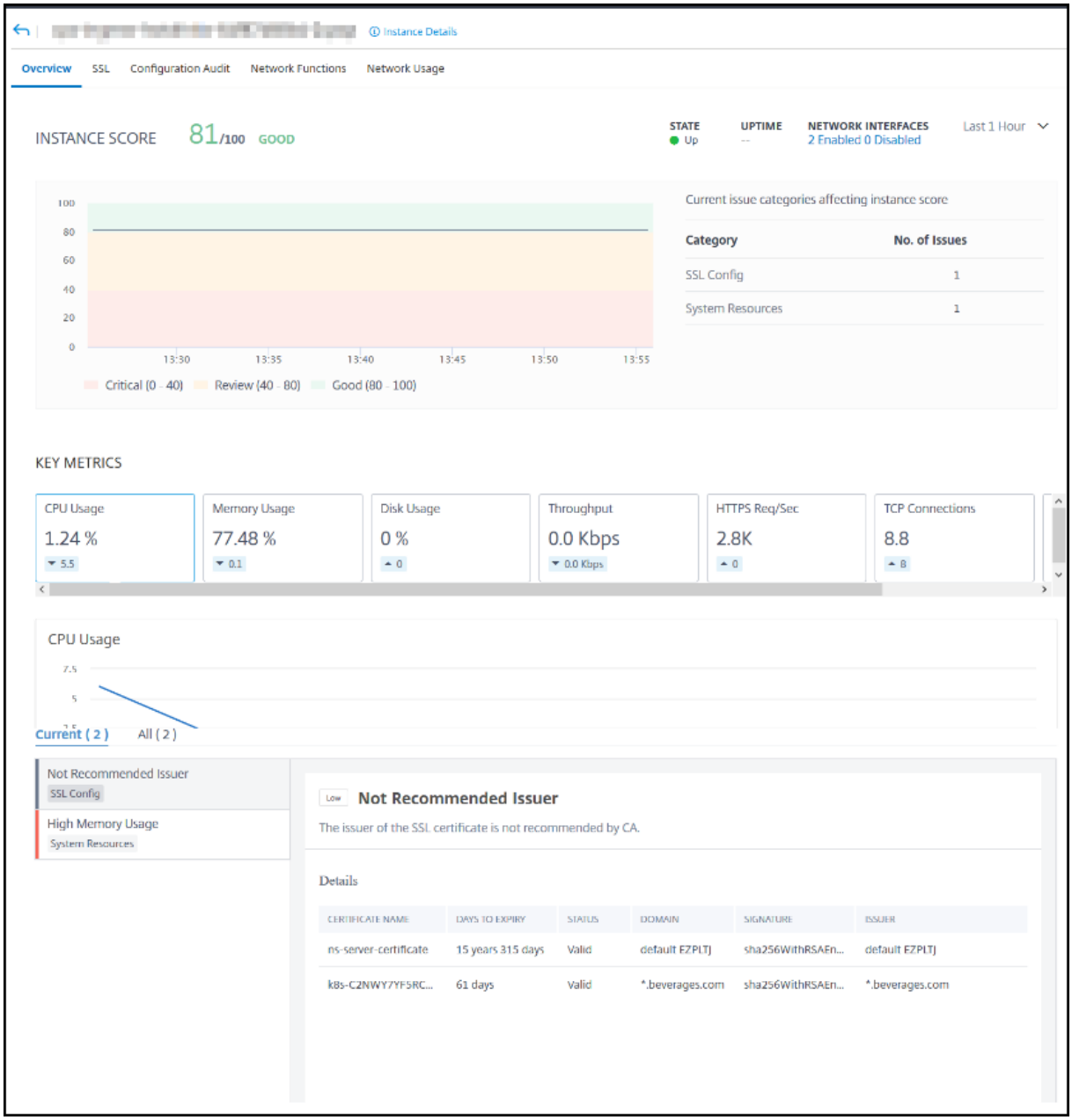
Das Instanz-Dashboard in Citrix ADM zeigt Daten in einem tabellarischen und grafischen Format für die ausgewählte Instanz an. Daten, die während des Polling-Prozesses von Ihrer Instanz gesammelt wurden, werden auf dem Dashboard angezeigt.

Standardmäßig werden verwaltete Instanzen jede Minute zur Datenerfassung abgefragt. Statistische Informationen wie Status, HTTP-Anfragen pro Sekunde, CPU-Auslastung, Speicherauslastung und Durchsatz werden kontinuierlich mit NITRO -Aufrufen erfasst. Als Administrator können Sie all diese gesammelten Daten auf einer einzigen Seite anzeigen, Probleme in der Instanz identifizieren und sofortige Maßnahmen ergreifen, um sie zu beheben.

Um das Dashboard einer bestimmten Instanz anzuzeigen, navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**. Wählen Sie auf der Seite Citrix ADC den Instanztyp aus, wählen Sie dann die Instanz aus, die Sie anzeigen möchten, und klicken Sie auf **Dashboard**.



Die folgende Abbildung bietet einen Überblick über die verschiedenen Daten, die auf dem Instanz-Dashboard angezeigt werden:



- **Übersicht**. Die Registerkarte Übersicht zeigt die CPU- und Speicherauslastung der gewählten Instanz an. Sie können auch Ereignisse anzeigen, die von der Instanz generiert werden und die Durchsatzdaten. Hier werden auch instanzspezifische Informationen wie die IP-Adresse, ihre Hardware- und LOM-Versionen, die Profildetails, die Seriennummer, die Kontaktperson und andere angezeigt. Wenn Sie weiter nach unten scrollen, werden die lizenzierten Funktionen, die für die ausgewählte Instanz verfügbar sind, zusammen mit den darauf konfigurierten Modi. Weitere Informationen finden Sie unter Instanz-Details.
- **SSL-Dashboard**. Sie können die Registerkarte SSL im Dashboard pro Instanz verwenden, um die Details der SSL-Zertifikate, virtuellen SSL-Server und SSL-Protokolle der ausgewählten In-

stanz anzuzeigen oder zu überwachen. Sie können auf die Zahlen in den Graphen klicken, um weitere Details anzuzeigen.

- **Konfigurationsüberwachung**. Sie können die Registerkarte Konfigurationsüberwachung verwenden, um alle Konfigurationsänderungen anzuzeigen, die auf der ausgewählten Instanz aufgetreten sind. Der **gespeicherte Status der Citrix ADC Konfiguration** und die **Driftdiagramme für die Citrix ADC Konfiguration** im Dashboard zeigen Details zu Konfigurationsänderungen in gespeicherten und nicht gespeicherten Konfigurationen auf hoher Ebene an.
- **Netzwerkfunktionen**. Mithilfe des Dashboards für Netzwerkfunktionen können Sie den Status der Entitäten überwachen, die auf der ausgewählten Citrix ADC-Instanz konfiguriert sind. Sie können Diagramme für Ihre virtuellen Server anzeigen, die Daten wie Clientverbindungen, Durchsatz und Serververbindungen anzeigen.
- **Netzwerkauslastung**. Sie können die Netzwerkleistungsdaten für die ausgewählte Instanz auf der Registerkarte Netzwerkauslastung anzeigen. Sie können Berichte für eine Stunde, einen Tag, eine Woche oder einen Monat anzeigen. Die Zeitleisten-Schiebereglerfunktion kann verwendet werden, um die Dauer der zu generierenden Netzwerkberichte anzupassen. Standardmäßig werden nur acht Berichte angezeigt, Sie können jedoch auf das Pluszeichen unten rechts auf dem Bildschirm klicken, um einen weiteren Leistungsbericht hinzuzufügen.

So überwachen Sie global verteilte Standorte

April 28, 2021

Als Netzwerkadministrator müssen Sie möglicherweise Netzwerkinstanzen überwachen und verwalten, die über geografische Standorte verteilt sind. Es ist jedoch nicht einfach, die Anforderungen des Netzwerks bei der Verwaltung von Netzwerkinstanzen in geografisch verteilten Rechenzentren zu beurteilen.

Geomaps in Citrix Application Delivery Management (Citrix ADM) bieten Ihnen eine grafische Darstellung Ihrer Standorte und untergliedern die Netzwerküberwachung nach Geographie. Mit Geomaps können Sie Ihre Netzwerkinstanzverteilung nach Standort visualisieren und Netzwerkprobleme überwachen.

In den folgenden Abschnitten wird erläutert, wie Sie Rechenzentren in Citrix ADM überwachen können.

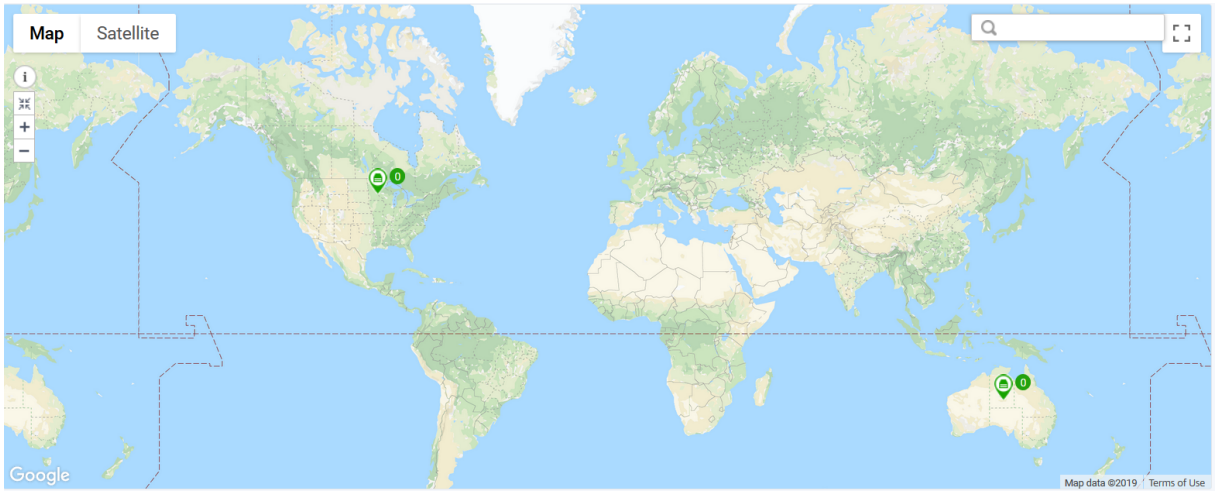
Überwachen global verteilter Standorte in Citrix ADM

Der Citrix ADM Standort ist eine logische Gruppierung von Citrix Application Delivery Controller (Citrix ADC) -Instanzen an einem bestimmten geografischen Standort. Beispielsweise ist eine Website Amazon Web Services (AWS) zugewiesen und eine andere Website Azure™ zugewiesen. Noch eine andere Website wird auf dem Gelände des Mandanten gehostet. Citrix ADM verwaltet und überwacht alle Citrix ADC-Instanzen, die mit allen Standorten verbunden sind. Sie können Citrix ADM verwenden, um Syslog, AppFlow, SNMP und alle von den verwalteten Instanzen stammenden Daten zu überwachen und zu sammeln.

Geomaps in Citrix ADM bietet Ihnen eine grafische Darstellung Ihrer Websites. Geomaps untergliedern auch Ihre Netzwerküberwachungserfahrung nach Geographie. Mit Geomaps können Sie Ihre Netzwerkinstanzverteilung nach Standort visualisieren und alle Netzwerkprobleme überwachen. Sie können im Menü auf **Netzwerke** klicken. Daraufhin wird das **Instanzen Dashboard** für eine visuelle Darstellung der auf der Weltkarte erstellten Sites angezeigt.

Anwendungsfall

Ein führendes Mobilfunkunternehmen, ExampleCompany, stützte sich auf private Dienstleister, um ihre Ressourcen und Anwendungen zu hosten. Das Unternehmen hatte bereits zwei Standorte - einen in Minneapolis in den USA und einen anderen in Alice Springs in Australien. In diesem Bild sehen Sie, dass zwei Marker die beiden vorhandenen Standorte darstellen.



Die Marker zeigen auch die Anzahl der folgenden Komponenten auf der Website an:

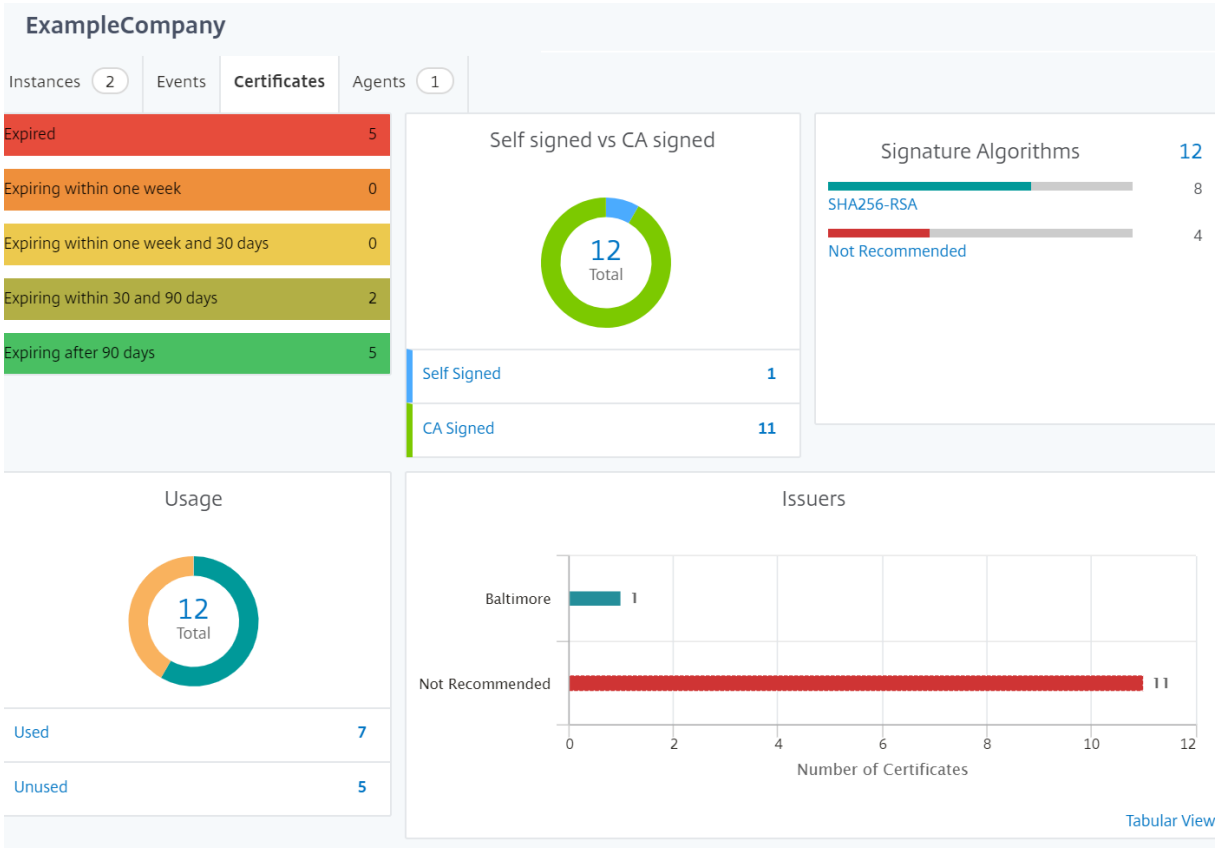
- **Instanzen**: Gibt die Anzahl der verfügbaren Instanzen an.
- **Anwendungen**: Gibt die Anzahl der gehosteten Anwendungen an.
- **Virtuelle Server**: Gibt die Anzahl der verfügbaren virtuellen Server an.
- **Kritische Ereignisse**: Gibt die Anzahl der kritischen Ereignisse an, die auf den Instanzen aufgetreten sind.

- **Wichtige Ereignisse**: Gibt die Anzahl der auf den Instanzen aufgetretenen Hauptereignisse an.

Klicken Sie auf **Anwendungen**, um alle benutzerdefinierten Anwendungen anzuzeigen, die an den einzelnen Standorten erstellt wurden.

Klicken Sie auf **Details**, um eine Liste der Citrix ADC-Instanzen anzuzeigen, die an jedem Standort hinzugefügt wurden. Klicken Sie auf die Registerkarten, um weitere Informationen anzuzeigen:

- Registerkarte **Instanzen**: Auf dieser Registerkarte können Sie Folgendes anzeigen:
  - IP-Adresse jeder Netzwerkinstanz
  - Typ der Citrix ADC-Instanz
  - Anzahl kritischer Ereignisse
  - Bedeutende Ereignisse und alle Ereignisse, die auf einer Citrix ADC-Instanz ausgelöst werden.
- Registerkarte**Ereignisse**: Zeigt eine Liste der kritischen und bedeutenden Ereignisse an, die auf den Instanzen ausgelöst werden.
- Registerkarte**Zertifikate**: Zeigen Sie auf dieser Registerkarte Folgendes an:
  - Liste der Zertifikate aller Instanzen
  - Ablaufstatus
  - Wichtige Informationen und die Top 10 Instanzen durch viele Zertifikate im Einsatz.
- Registerkarte **Agenten**: Zeigt eine Liste der Agenten an, an die die Instanzen gebunden sind.



Geomaps konfigurieren

ExampleCompany entschied sich, eine dritte Website in Bangalore, Indien, zu erstellen. Das Unternehmen wollte die Cloud testen, indem einige ihrer weniger kritischen, internen IT-Anwendungen in das Büro von Bangalore verlagert wurden. Das Unternehmen entschied sich für die Nutzung der AWS-Cloud Computing-Services.

Als Administrator müssen Sie zuerst eine Site erstellen und anschließend die Citrix ADC-Instanzen in Citrix ADM hinzufügen. Sie müssen die Instanz auch der Site hinzufügen, einen Agenten hinzufügen und den Agenten an die Site binden. Citrix ADM erkennt dann den Standort, zu dem die Citrix ADC-Instanz und der Agent gehören.

Weitere Informationen zum Hinzufügen von Citrix ADC-Instanzen finden Sie unterInstanzen hinzufügen.

So erstellen Sie Websites:

Erstellen Sie Sites, bevor Sie Instanzen in Citrix ADM hinzufügen. Die Bereitstellung von Standortinformationen ermöglicht es Ihnen, den Standort genau zu lokalisieren.

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Sites**, und klicken Sie auf **Hinzufügen**.

2. Aktualisieren Sie auf der Seite **Website erstellen** die folgenden Informationen, und klicken Sie auf **Erstellen**.

   a) **Standorttyp**. Wählen Sie **Data Center**aus.

   > **Hinweis:**
   >
   > Der Standort kann als primäres Rechenzentrum oder als Zweig fungieren. Wählen Sie entsprechend.

   a) **Geben Sie ein**. Wählen Sie AWS als Cloud-Anbieter aus der Liste aus.

   > **Hinweis**
   >
   > Aktivieren Sie das Kontrollkästchen **Vorhandene VPC als Site verwenden**entsprechend.

   b) **Standortname**. Geben Sie den Namen der Site ein.

   c) **Suchort**. Geben Sie den Namen der Stadt ein. Klicken Sie auf **Standort abrufen**, um die Site genau an der Position zu platzieren.
   Die Felder Stadt, Postleitzahl, Region, Land, Breitengrad und Längengrad werden automatisch ausgefüllt.

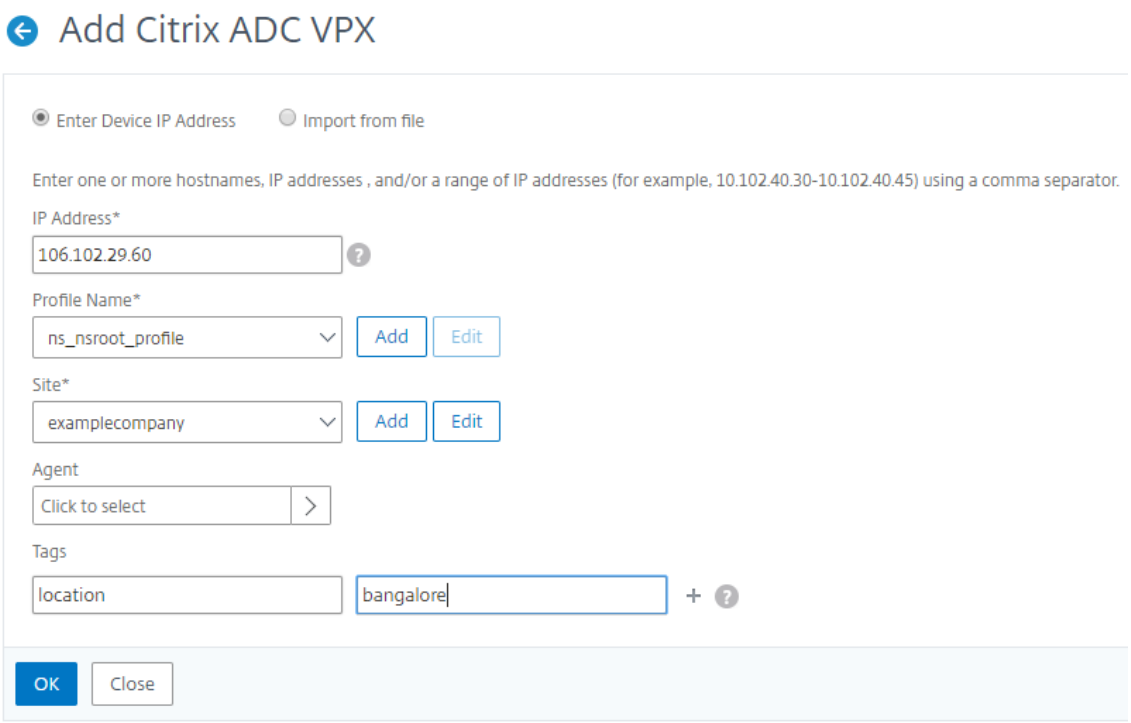
   ! [Sites erstellen] (/en-us/citrix-application-delivery-management-service/media/nmaservice-global-datacenters-4.png)

   d) Klicken Sie auf **Erstellen**, um eine Website in Bangalore zu erstellen.

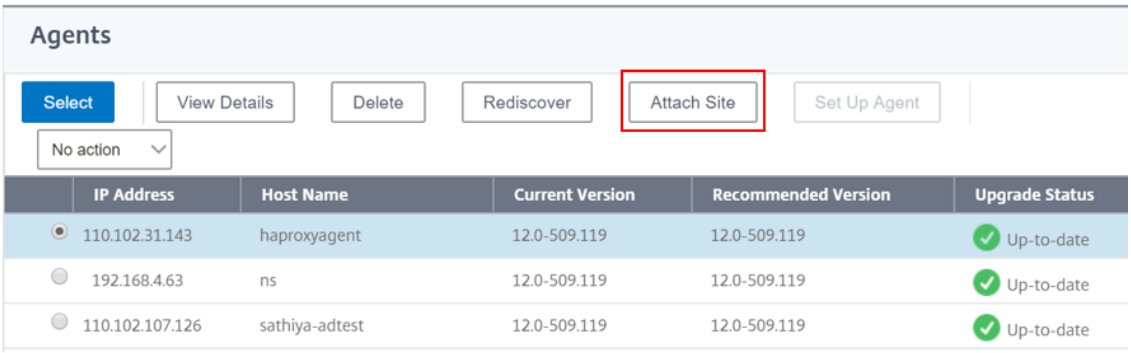
So fügen Sie Instanzen hinzu und wählen Sie Sites aus:

Nach dem Erstellen von Sites müssen Sie Instanzen in Citrix ADM hinzufügen. Sie können die zuvor erstellte Site auswählen, oder Sie können auch eine Site erstellen und die Instanz zuordnen.

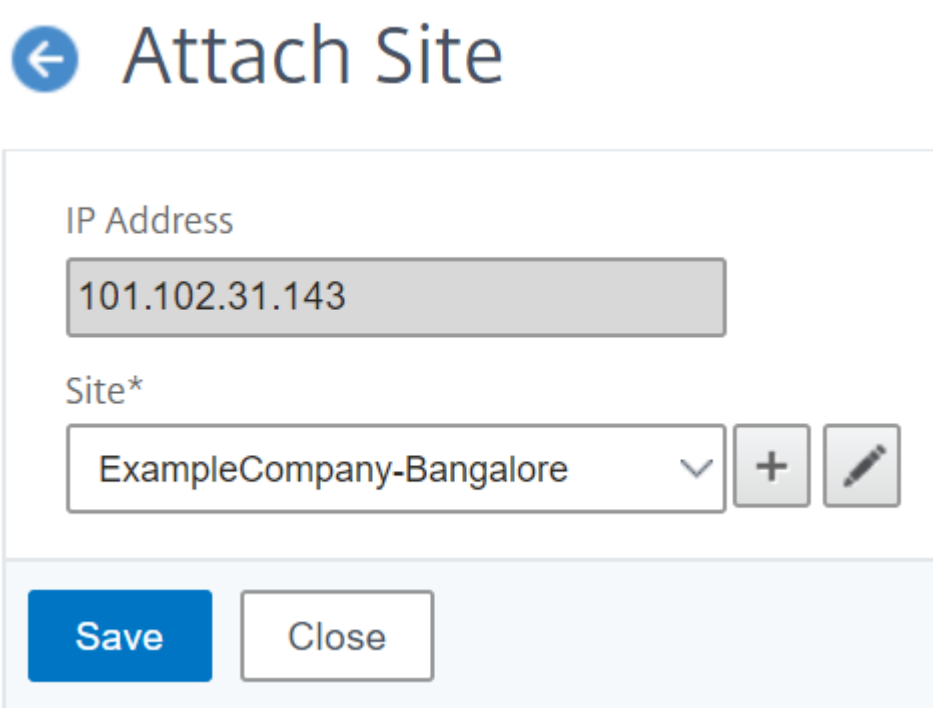
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Wählen Sie die **VPX**aus, und klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **Citrix ADC VPX hinzufügen** die IP-Adresse ein, und wählen Sie das Profil aus der Liste aus.
4. Wählen Sie die Website aus der Liste aus. Sie können auf die Schaltfläche **Hinzufügen** neben dem Feld **Site** klicken, um eine Website zu erstellen, oder auf die Schaltfläche **Bearbeiten** klicken, um die Details der Standardwebsite zu ändern.
5. Klicken Sie auf den Pfeil nach rechts, und wählen Sie den Agenten aus der angezeigten Liste aus.



6. Nachdem Sie den Agenten ausgewählt haben, müssen Sie den Agenten der Site zuordnen. Mit diesem Schritt kann der Agent an die Site gebunden werden. Wählen Sie den Agenten aus, und klicken Sie auf **Site anhängen**.



a) Wählen Sie die Website aus der Liste aus, und klicken Sie auf **Speichern**.



7. Optional können Sie Schlüssel- und Wertfelder für **Tags**eingeben.
8. Klicken Sie auf **OK**.

Sie können einen Agenten auch an eine Site anhängen, indem Sie zu **Netzwerke** > **Agents** navigieren.

So verknüpfen Sie einen Citrix ADM Agent mit der Site:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Agents**.
2. Wählen Sie den Agenten aus, und klicken Sie auf **Site anhängen**.
3. Sie können die Website zuordnen und auf **Speichern**klicken.

Citrix ADM beginnt mit der Überwachung der Citrix ADC-Instanzen, die auf dem Standort in Bangalore hinzugefügt wurden, zusammen mit den Instanzen an den anderen beiden Standorten.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

So erstellen Sie Tags und weisen Sie Instanzen zu

April 28, 2021

Mit Citrix Application Delivery Management (ADM) können Sie Ihre Citrix ADC-Instanzen mit Tags verknüpfen. Ein Tag ist ein Schlüsselwort oder ein Begriff mit einem Wort, das Sie einer Instanz zuweisen können. Die Tags fügen einige zusätzliche Informationen über die Instanz hinzu. Die Tags können als Metadaten betrachtet werden, die eine Instanz beschreiben. Tags ermöglichen es Ihnen, Instanzen basierend auf diesen Schlüsselwörtern zu klassifizieren und zu suchen. Sie können einer einzelnen Instanz auch mehrere Tags zuweisen.

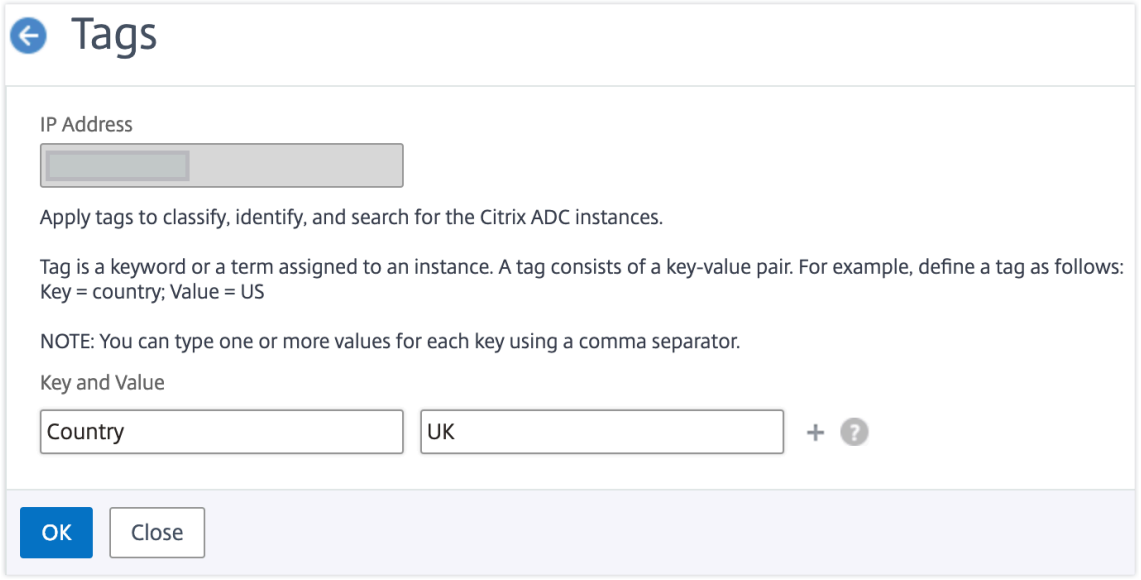
Die folgenden Anwendungsfälle helfen Ihnen zu verstehen, wie die Tagging von Instanzen Ihnen dabei hilft, sie besser zu überwachen.

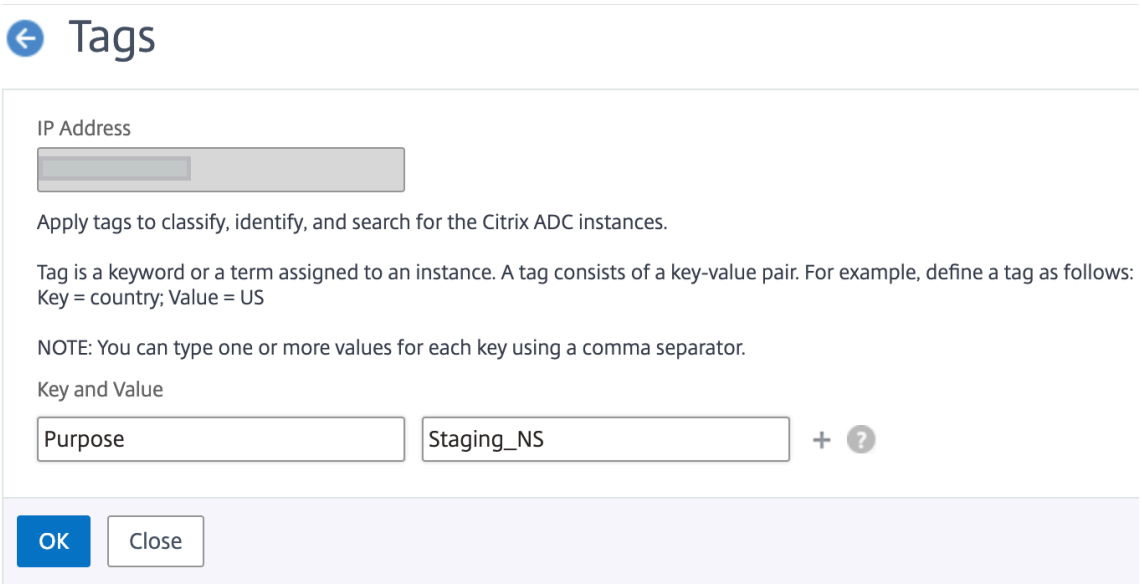
- **Anwendungsfall 1**: Sie können ein Tag erstellen, um alle Instanzen zu identifizieren, die sich im Vereinigten Königreich befinden. Hier können Sie ein Tag mit dem Schlüssel “Country” und dem Wert als “UK” erstellen. Mit diesem Tag können Sie alle Instanzen durchsuchen und überwachen, die sich in Großbritannien befinden.
- **Anwendungsfall 2**: Sie möchten nach Instanzen suchen, die sich in der Stagingumgebung befinden. Hier können Sie ein Tag mit dem Schlüssel “Purpose” und einem Wert als “Staging_NS” erstellen. Mit diesem Tag können Sie alle Instanzen, die in der Stagingumgebung verwendet werden, von den Instanzen trennen, die Clientanforderungen durchlaufen.
- **Anwendungsfall 3**: Betrachten Sie eine Situation, in der Sie die Liste der Citrix ADC-Instanzen herausfinden möchten, die sich im Bereich Swindon in Großbritannien befinden und Ihnen gehören, David T. Sie können Tags für all diese Anforderungen erstellen und diese allen Instanzen zuweisen, die diese Bedingungen erfüllen.

So weisen Sie der Citrix ADC VPX Instanz Tags zu:

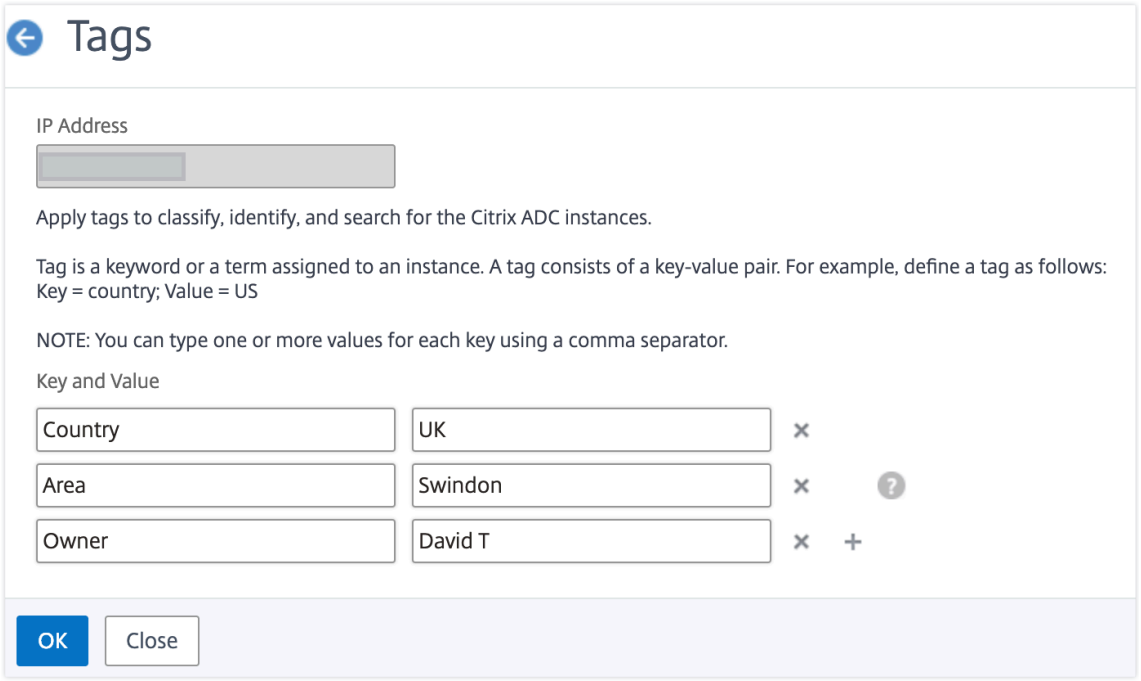
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Wählen Sie die Registerkarte **VPX** aus.
3. Wählen Sie die gewünschte VPX-Instanz aus.
4. Klicken Sie auf **Tags**. Im Fenster **Tags** können Sie eigene Schlüssel-Wert-Paare erstellen, indem Sie jedem erstellten Schlüsselwort Werte zuweisen.

Die folgenden Bilder zeigen beispielsweise einige erstellte Schlüsselwörter und deren Werte. Sie können eigene Schlüsselwörter hinzufügen und für jedes Schlüsselwort einen Wert eingeben.



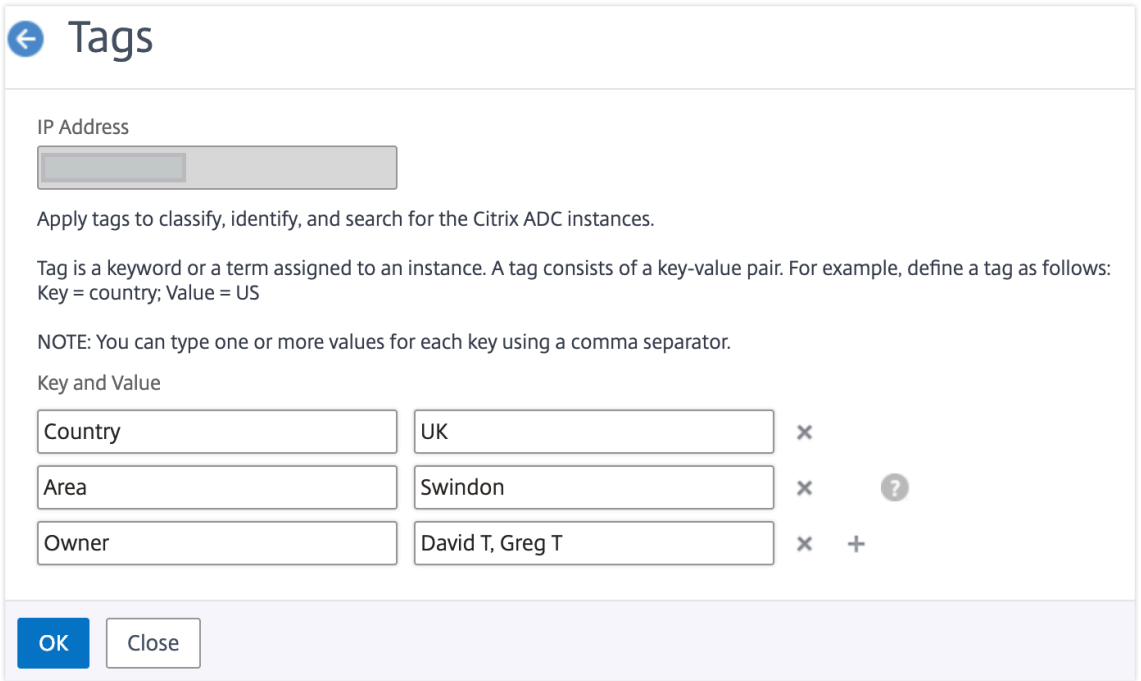


Sie können auch mehrere Tags hinzufügen, indem Sie auf + klicken. Durch das Hinzufügen mehrerer und aussagekräftiger Tags können Sie effizient nach den Instanzen suchen.



Sie können einem Schlüsselwort mehrere Werte hinzufügen, indem Sie sie durch Kommas trennen.

Zum Beispiel weisen Sie die Admin-Rolle einem anderen Mitarbeiter zu, Greg T. Sie können seinen Namen durch ein Komma getrennt hinzufügen. Durch das Hinzufügen mehrerer Namen können Sie entweder nach den Namen oder nach beiden Namen suchen. Citrix ADM erkennt die durch Kommas getrennten Werte in zwei verschiedene Werte.



Weitere Informationen darüber, wie Sie nach auf Tags basierenden Instanzen suchen, finden Sie unter So suchen Sie Instanzen mithilfe von Werten von Tags und Eigenschaften.

5. Klicken Sie auf **OK**.

> **Hinweis**
>
> Sie können später neue Tags hinzufügen oder vorhandene Tags löschen. Es gibt keine Einschränkung für die Anzahl der Tags, die Sie erstellen.

So suchen Sie Instanzen über Werte von Tags und Eigenschaften

April 28, 2021

Es könnte eine Situation geben, in der Citrix Application Delivery Management (ADM) viele Citrix ADC-Instanzen verwaltet. Als Administrator möchten Sie möglicherweise die Flexibilität, die Instanzinventar anhand bestimmter Parameter zu durchsuchen. Citrix ADM bietet jetzt eine verbesserte Suchfunktion, um eine Teilmenge von Citrix ADC-Instanzen basierend auf den Parametern zu durchsuchen, die Sie im Suchfeld definieren. Sie können nach den Instanzen auf der Grundlage von zwei Kriterien suchen - Tags und Eigenschaften.

- **Tags**. Tags sind Begriffe oder Schlüsselwörter, die von Ihnen einer Citrix ADC-Instanz zugewiesen werden können, um zusätzliche Beschreibung zur Citrix ADC-Instanz hinzuzufügen. Sie können Ihre Citrix ADC-Instanzen nun Tags zuordnen. Diese Tags können verwendet werden, um die Citrix ADC-Instanzen besser zu identifizieren und zu suchen.
- **Eigenschaften**. Jede Citrix ADC-Instanz, die in Citrix ADM hinzugefügt wird, verfügt über einige Standardparameter oder Eigenschaften, die dieser Instanz zugeordnet sind. Zum Beispiel hat jede Instanz ihren eigenen Hostnamen, ihre IP-Adresse, ihre Version, ihre Host-ID, ihre Hardwaremodell-ID und so weiter. Sie können nach Instanzen suchen, indem Sie Werte für jede dieser Eigenschaften angeben.

Betrachten Sie beispielsweise eine Situation, in der Sie die Liste der Citrix ADC-Instanzen ermitteln möchten, die sich auf Version 12.0 befinden und sich im UP Status befinden. Hier werden die Version und der Status der Instanz durch die Standardeigenschaften definiert.

Neben der Version 12.0 und dem Status UP der Instanzen können Sie auch diese Instanzen durchsuchen, die Ihnen gehören. Sie können ein Owner -Tag erstellen und diesem Tag einen Wert David T zuweisen. Weitere Informationen zum Erstellen und Zuweisen von Tags finden Sie unter So erstellen Sie Tags und weisen Sie Instanzen zu.

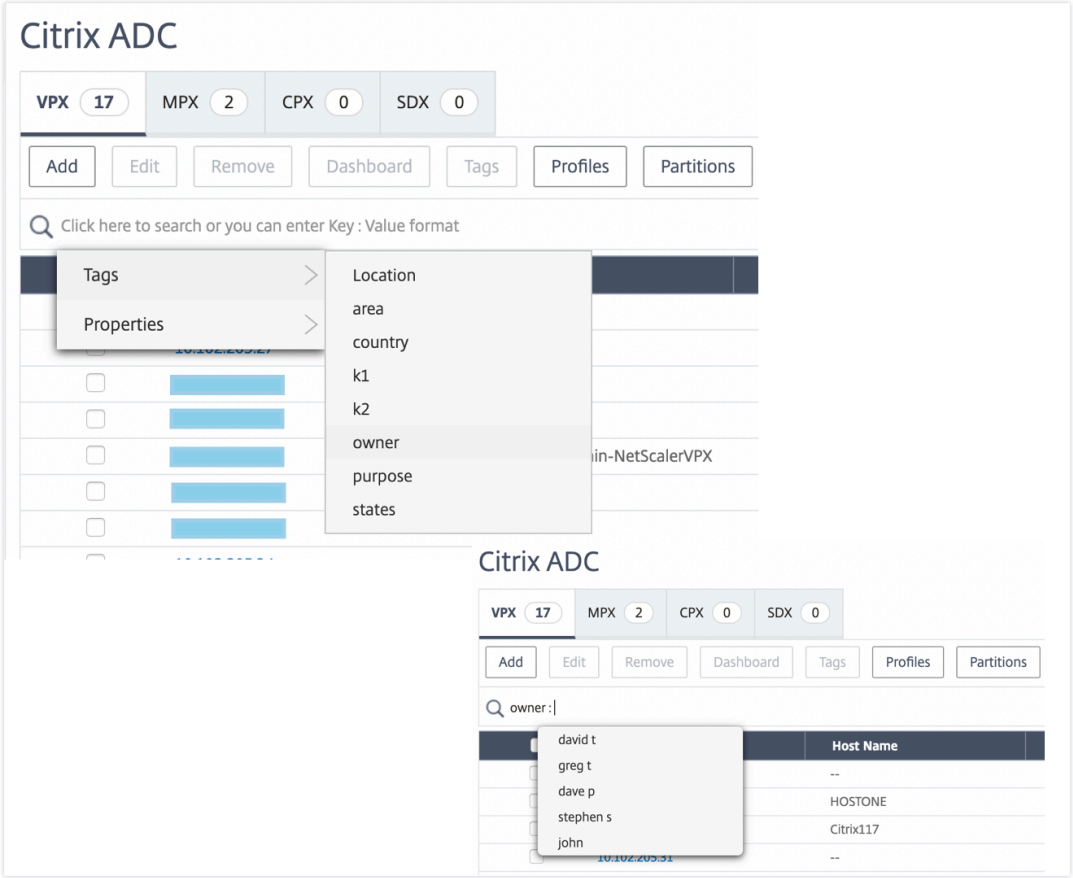
Sie können eine Kombination aus Tags und Eigenschaften verwenden, um eigene Suchkriterien zu erstellen.

So suchen Sie nach Citrix ADC VPX Instanzen

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Wählen Sie die Registerkarte **VPX** aus.
3. Klicken Sie auf das Suchfeld. Sie können einen Suchausdruck erstellen, indem Sie Tags oder Eigenschaften verwenden oder beide kombinieren.

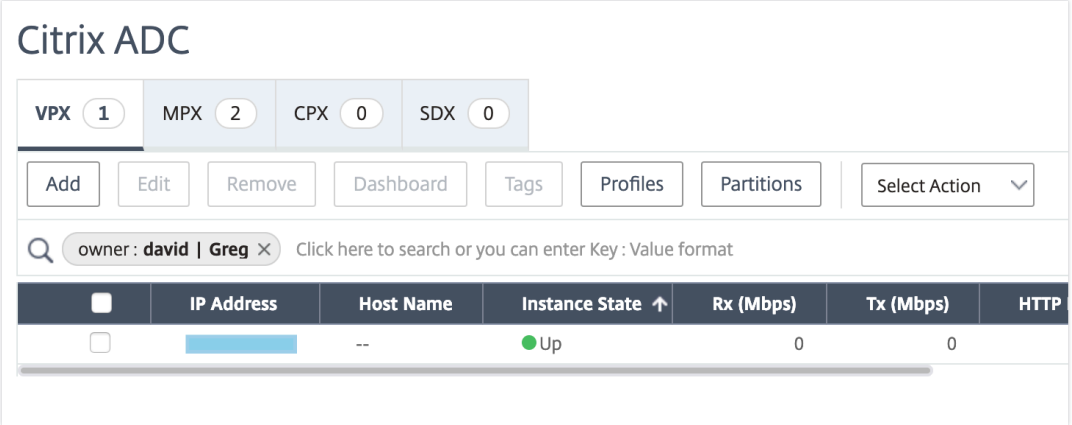
   Die folgenden Beispiele zeigen, wie Sie den Suchausdruck effizient verwenden können, um nach der Instanz zu suchen.

   a) Wählen Sie die Option **Tags** aus und wählen Sie **Besitzer** aus. Wählen Sie David T.

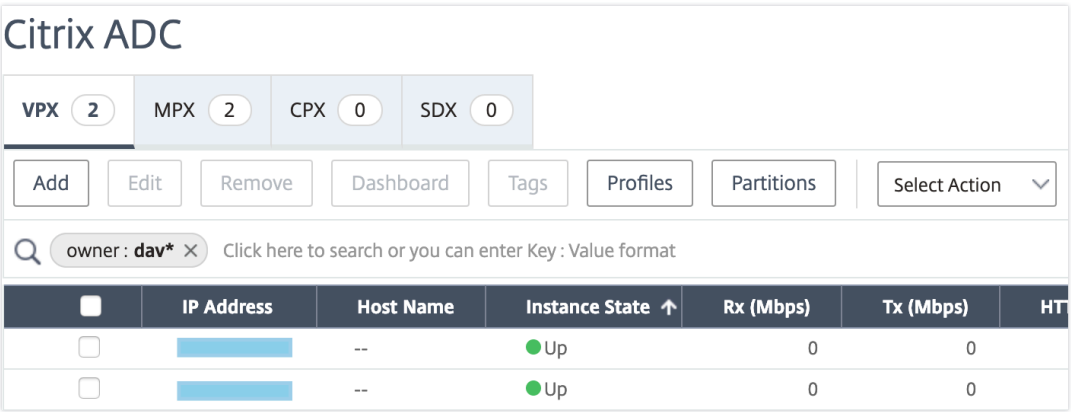


   Citrix ADM unterstützt reguläre Ausdrücke und Platzhalterzeichen in den Suchausdrücken.

   a) Sie können reguläre Ausdrücke verwenden, um die Suchkriterien weiter zu erweitern. Beispielsweise möchten Sie Instanzen durchsuchen, die im Besitz von David oder Stephen sind. In einem solchen Fall können Sie die Werte eingeben, indem Sie die Werte durch einen |-Ausdruck trennen.



b) Sie können auch Platzhalterzeichen verwenden, um ein oder mehrere Zeichen zu ersetzen oder darzustellen. Sie können beispielsweise Dav* nach allen Instanzen suchen, die sich im Besitz von “David” und “Dave P” befinden.



> **Hinweis**
>
> Weitere Informationen zu regulären Ausdrücken und Platzhalterzeichen sowie deren Verwendung finden Sie in der Suchleiste auf das Symbol Informationen.

Verwalten von Adminpartitionen von Citrix ADC-Instanzen

April 28, 2021

Sie können Administratorpartitionen auf Ihren Citrix Application Delivery Controller Instanzen (Citrix ADC) so konfigurieren, dass verschiedenen Gruppen in Ihrer Organisation unterschiedliche Partitionen auf derselben Citrix ADC-Instanz zugewiesen werden. Sie können einen Netzwerkadministrator zuweisen, um mehrere Partitionen auf mehreren Citrix ADC-Instanzen zu verwalten.

Citrix Application Delivery Management (Citrix ADM) bietet eine nahtlose Verwaltung aller Partitionen, die einem Administrator gehören, von einer einzigen Konsole aus. Sie können diese Partitionen verwalten, ohne andere Partitionskonfigurationen zu unterbrechen.

Damit mehrere Benutzer verschiedene Adminpartitionen verwalten können, müssen Sie Gruppen erstellen und diesen Gruppen Benutzer und Partitionen zuweisen. Weitere Informationen zum Erstellen einer Gruppe oder eines Benutzers finden Sie unterErstellen Sie einen BenutzerundErstellen einer Gruppe.

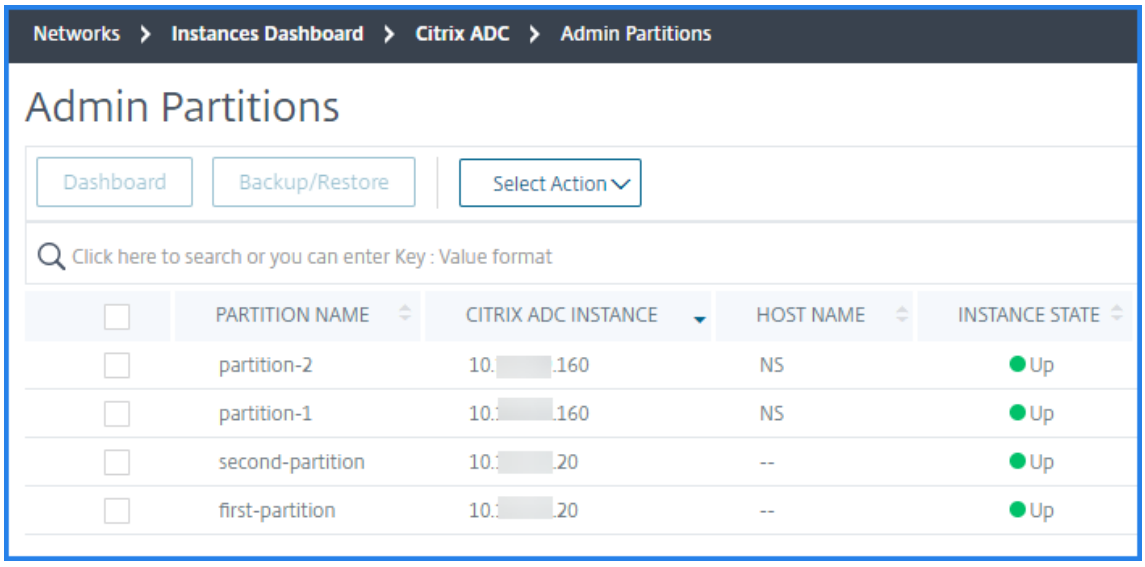
Ein Benutzer kann nur die Partitionen in der Gruppe anzeigen und verwalten, zu der der Benutzer gehört. Wenn Sie eine Citrix ADC-Instanz entdecken, werden die für diese Citrix ADC-Instanz konfigurierten Adminpartitionen automatisch dem System hinzugefügt. Jede Admin-Partition wird in Citrix ADM als Instanz betrachtet.

Anzeigen von Admin-Partitionen

Beachten Sie, dass Sie über zwei Citrix ADC VPX Instanzen verfügen und zwei Administratorpartitionen für jede Instanz konfiguriert sind. Beispielsweise verfügt die Citrix ADC-Instanz 10.xx.xx.160 über Partition-1 und Partition-2 und die 10.xx.xx.20-Instanz über die erste Partition und die zweite Partition.

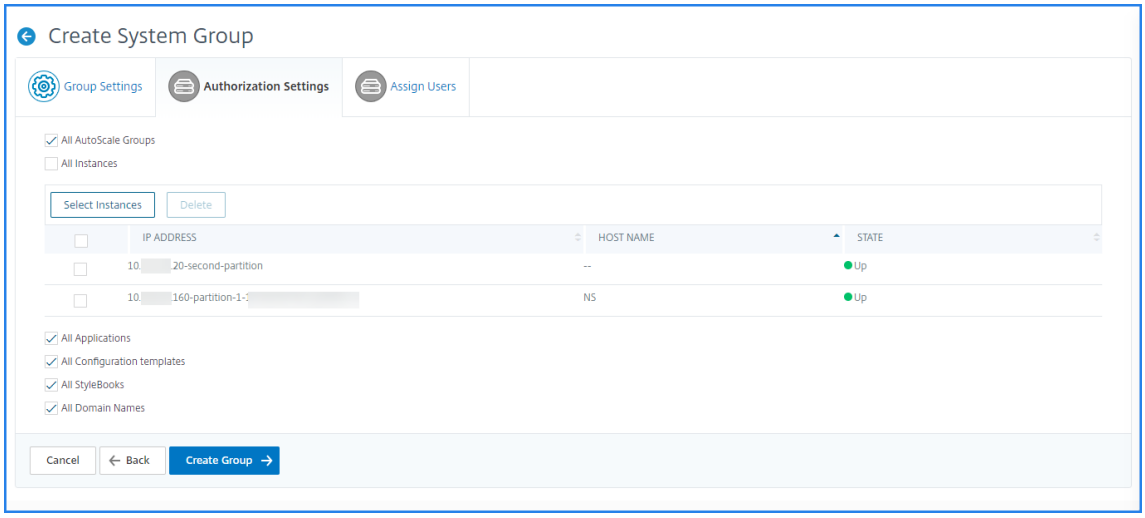
Führen Sie die folgenden Schritte aus, um Administratorpartitionen anzuzeigen:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Klicken Sie auf der Registerkarte **VPX** auf **Partitionen**.

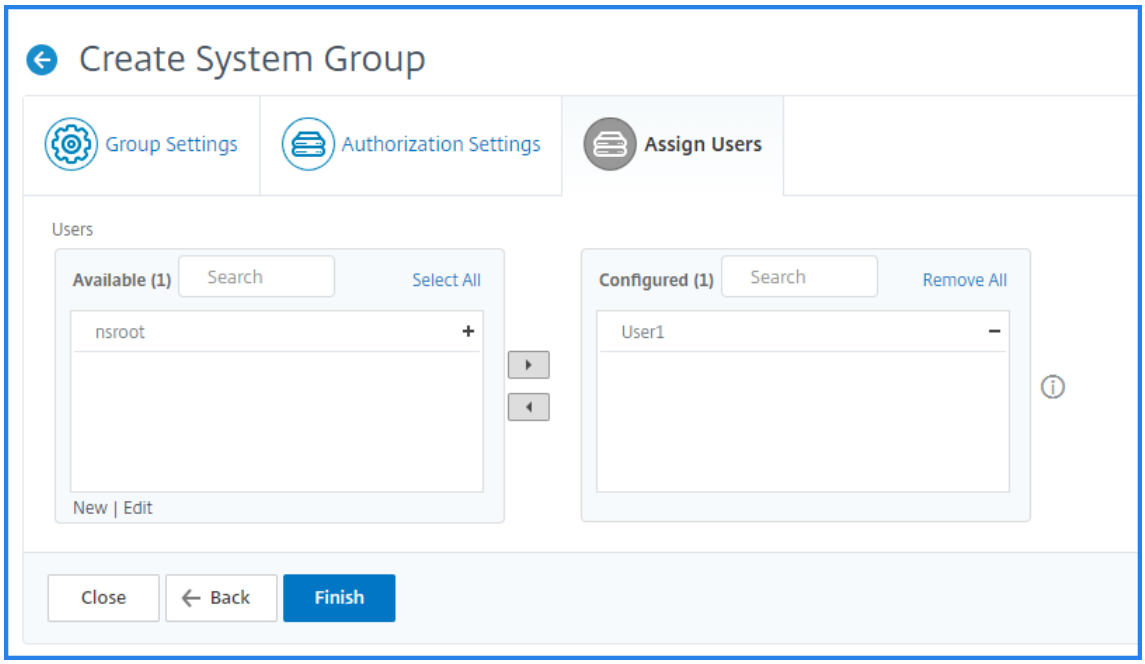


Wenn Sie beispielsweise eine Gruppe mit den folgenden Bedingungen erstellen:

- Auf der Registerkarte **Autorisierungseinstellungen** werden die Instanzen 10.xx.xx.20-second-partition und 10.xx.xx.160-partition-1 ausgewählt.



- Benutzer1 ist der Gruppe zugeordnet.



Benutzer1 kann nur die Partitionen anzeigen und verwalten, die der Gruppe hinzugefügt werden. Die Partitionen, die der Gruppe nicht hinzugefügt werden, sind jedoch auf den Benutzer beschränkt, obwohl sie zu denselben Instanzen gehören.

In diesem Beispiel sind 10.xx.xx.20-first-partition und 10.xx.xx.160-partition-2 eingeschränkt. Da die Instanzen nicht der Gruppe hinzugefügt werden, der der Benutzer zugewiesen ist.

Wenn Sie möchten, dass ein anderer Benutzer die Admin-Partitionen 10.xx.xx.20-first-Partition und 10.xx.x.160-Partition-2 verwaltet, erstellen Sie eine Gruppe mit den folgenden Bedingungen:

- Wählen Sie auf der Registerkarte **Autorisierungseinstellungen** die Instanzen 10.xx.xx.20-first-partition und 10.xx.xx.160-partition-2 aus.

- Weisen Sie der Gruppe den erforderlichen Benutzer zu.

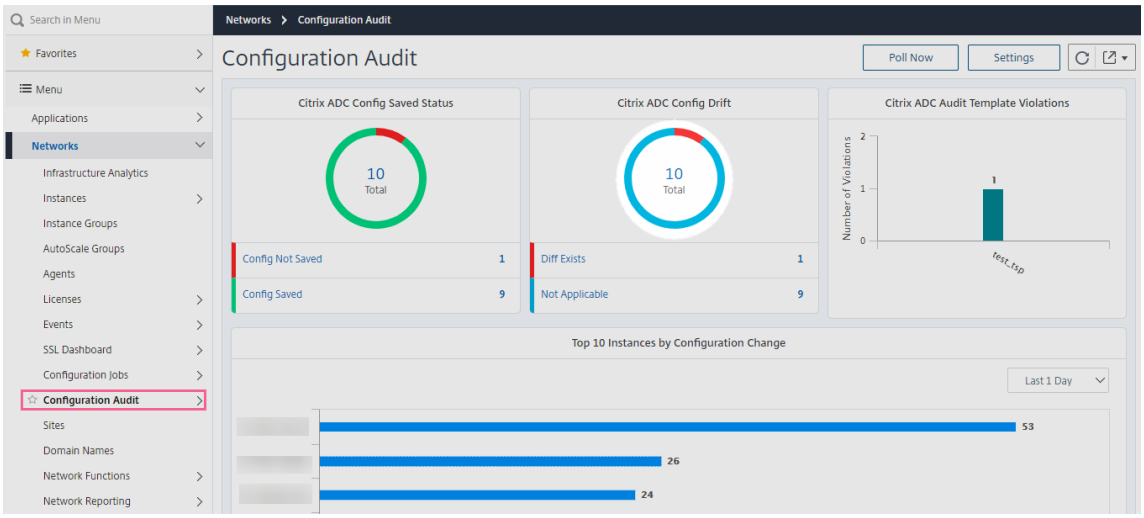
Diese Gruppe ermöglicht es dem zugewiesenen Benutzer, die ausgewählten Adminpartitionen anzuzeigen und zu verwalten.

Versionsverlaufsunterschied anzeigen

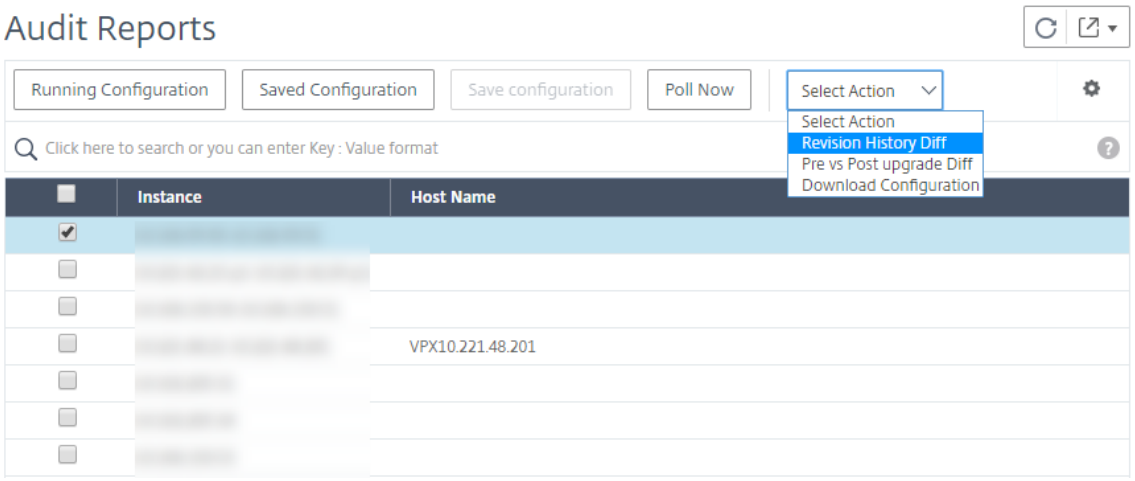
Der Unterschied zum Revisionsverlauf für eine Admin-Partition ermöglicht es Ihnen, den Unterschied zwischen den fünf neuesten Konfigurationsdateien für eine partitionierte Citrix ADC-Instanz zu sehen. Sie können die Konfigurationsdateien miteinander vergleichen (Beispiel: Konfigurationsversion - 1 mit Konfigurationsversion -2) oder mit der aktuellen laufen/gespeicherten Konfiguration mit Konfigurationsversion. Neben den Unterschieden in der Konfiguration werden auch die Korrekturkonfigurationen angezeigt. Sie können alle Korrekturbefehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.

So zeigen Sie die Differenz der Versionshistorie an:

1. Navigieren Sie zu **Netzwerke > Konfigurationsprüfung**. Das Dashboard Configuration Audit zeigt verschiedene Berichte an. Klicken Sie auf die Zahl, die in der Mitte des Donutdiagramms angezeigt wird.

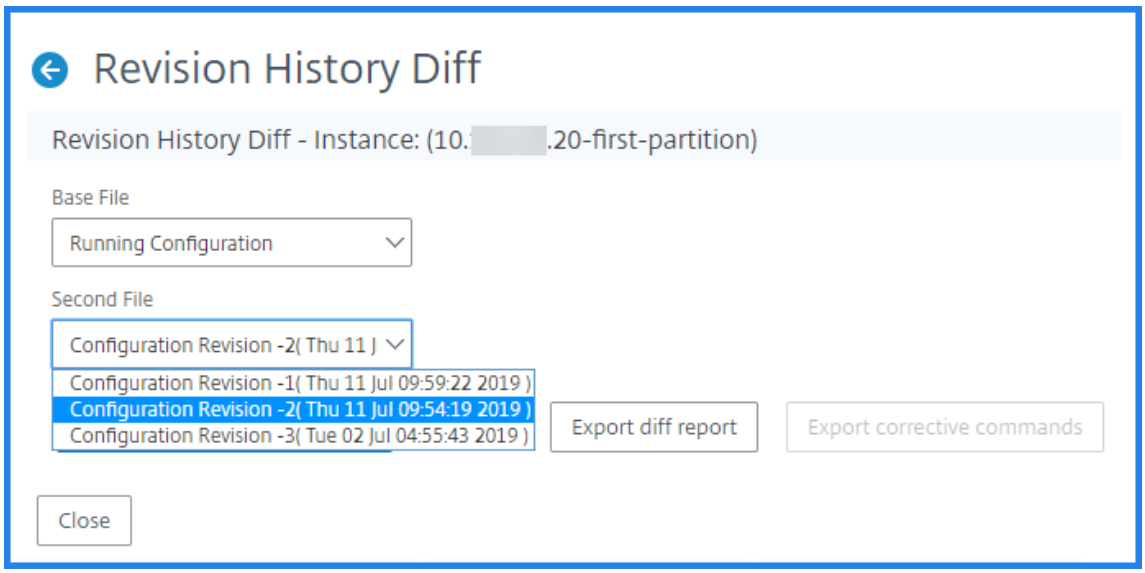


2. Wählen Sie die partitionierte Citrix ADC-Instanz aus.
3. Klicken Sie im Feld “Aktion” auf **Versionsverlauf Diff**.

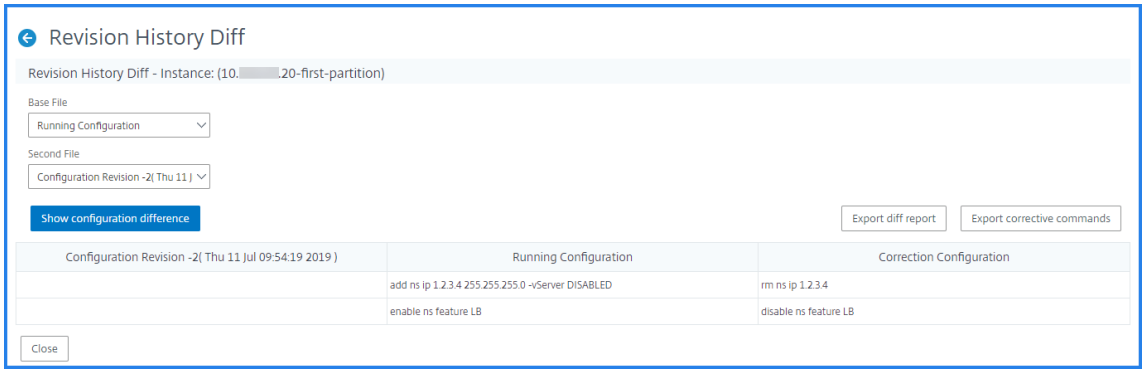


4. Wählen Sie auf der Seite **Versionsverlauf-Diff** die Dateien aus, die Sie vergleichen möchten. Vergleichen Sie beispielsweise die gespeicherte Konfiguration mit Konfigurationsrevision-2, und klicken Sie dann auf **Konfigurationsdifferenz anzeigen**.

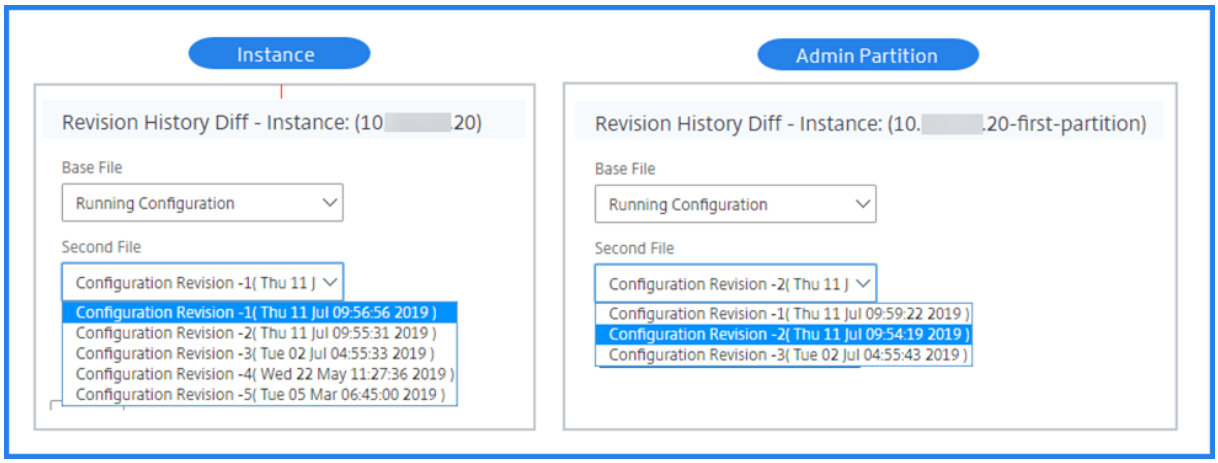
   Anschließend können Sie die Unterschiede zwischen den fünf neuesten Konfigurationsdateien für die ausgewählte partitionierte Citrix ADC-Instanz anzeigen. Im Folgenden finden Sie eine Beispiel-Admin-Partition mit drei gespeicherten Konfigurationen:



   Sie können auch die Korrekturkonfigurationsbefehle anzeigen und diese Korrekturbefehle in Ihren lokalen Ordner exportieren. Diese korrigierenden Befehle sind die Befehle, die für die Basisdatei ausgeführt werden müssen, um die Konfiguration in den gewünschten Zustand zu bringen (Konfigurationsdatei, die zum Vergleich verwendet wird).



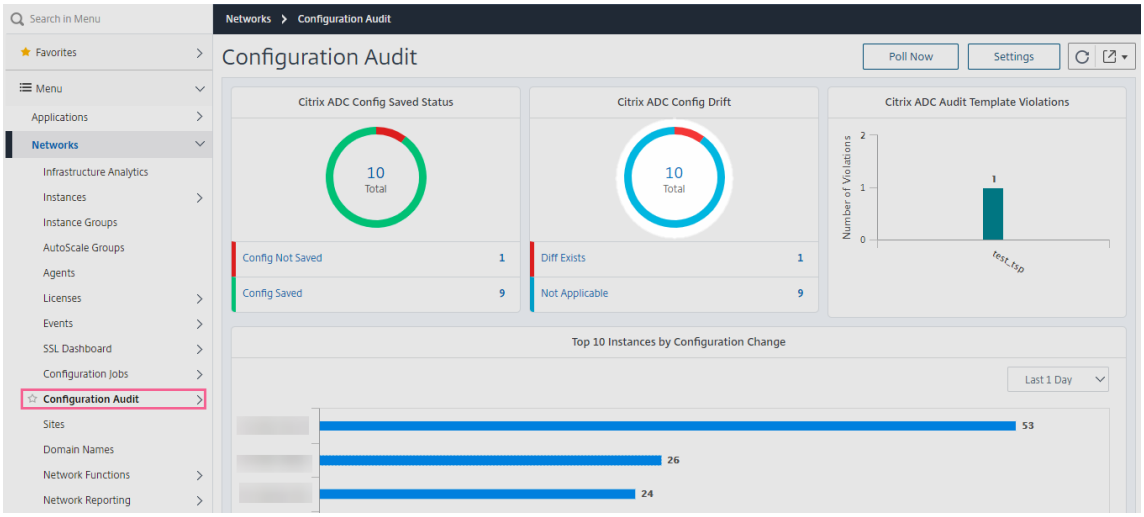
Die gespeicherten Konfigurationen auf einer Admin-Partition und der Instanz sind unterschiedlich. Im folgenden Beispiel verfügt die 10.xx.xx.20-Instanz über fünf gespeicherte Konfigurationen, bei denen die Admin-Partition dieser Instanz drei verschiedene gespeicherte Konfigurationen aufweist:



Anzeigen der Vorlage im Vergleich zu laufenden Differenzen

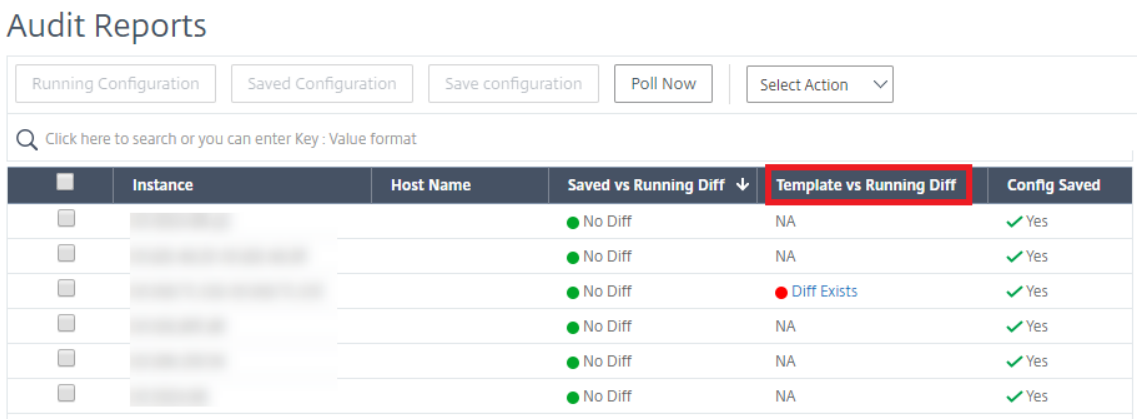
Überwachungsvorlagen für die Partition ermöglichen es Ihnen, eine benutzerdefinierte Konfigurationsvorlage zu erstellen und sie einer Partitionsinstanz zuzuordnen. Jede Variation in der laufenden Konfiguration der Instanz mit der Audit-Vorlage wird in der Spalte “**Vorlage vs Laufendes Diff**” der Seite “ **Auditberichte** “ angezeigt. Neben den Unterschieden in der Konfiguration werden auch die Korrekturkonfigurationen angezeigt. Sie können auch alle Korrekturbefehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.

1. Navigieren Sie zu **Netzwerke > Konfigurationsprüfung**. Das Dashboard Configuration Audit zeigt verschiedene Berichte an. Klicken Sie auf die Zahl, die in der Mitte des Donutdiagramms angezeigt wird.



2. Klicken Sie auf der Seite **Überwachungsberichte** auf den Hyperlink **Diff Existiert** in der Spalte Vorlage vs Laufendes Diff.

   Wenn zwischen der Überwachungsvorlage und der laufenden Konfiguration ein Unterschied besteht, wird der Unterschied als Hyperlink angezeigt. Klicken Sie auf den Hyperlink, um die Unterschiede anzuzeigen, falls vorhanden. Neben den Unterschieden in der Konfiguration werden auch die Korrekturkonfigurationen angezeigt. Sie können auch alle Korrekturbefehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.



So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Sichern und Wiederherstellen von Citrix ADC-Instanzen

April 28, 2021

Sie können den aktuellen Status einer Citrix Application Delivery Controller Instanz (Citrix ADC) sichern und später die gesicherten Dateien verwenden, um die Citrix ADC-Instanz in demselben Zustand wiederherzustellen. Sie müssen eine Instanz immer sichern, bevor Sie sie aktualisieren oder aus vorsorglichen Gründen. Eine Sicherung eines stabilen Systems ermöglicht es Ihnen, es wieder zu einem stabilen Punkt wiederherzustellen, wenn es instabil wird. Es gibt mehrere Möglichkeiten, Sicherungen und Wiederherstellungen auf einer Citrix ADC-Instanz durchzuführen. Sie können Citrix ADC Konfigurationen manuell mithilfe der GUI, CLI sichern und wiederherstellen oder Citrix Application Delivery Management (Citrix ADM) verwenden, um automatische Sicherungen und manuelle Wiederherstellungen durchzuführen. Citrix ADM sichert den aktuellen Status der verwalteten Citrix ADC-Instanzen mithilfe von NITRO -Aufrufen und der Secure Shell (SSH) und Secure Copy (SCP) Protokolle.

Citrix ADM erstellt eine vollständige Sicherung und stellt die folgenden Citrix ADC-Instanztypen wieder her:

- Citrix ADC SDX
- Citrix ADC VPX
- Citrix ADC MPX
- Citrix ADC BLX

Weitere Informationen finden Sie unter Sichern und Wiederherstellen einer ADC-Instanz.

> **Hinweis**
>
> - Von Citrix ADM aus können Sie den Sicherungs- und Wiederherstellungsvorgang auf einem Citrix ADC Cluster nicht ausführen.
> - Sie können die Backupdatei aus einer Instanz nicht verwenden, um eine andere Instanz wiederherzustellen.

Die gesicherten Dateien werden als komprimierte TAR-Datei im folgenden Verzeichnis gespeichert:


```
/var/mps/tenants/root/tenants/<specify-the-tenant-name>/device_backup/

<!--NeedCopy-->
```

Um Probleme aufgrund der Nichtverfügbarkeit von Speicherplatz zu vermeiden, können Sie maximal 50 Backupdateien in diesem Verzeichnis speichern.

Um Citrix ADC-Instanzen zu sichern und wiederherzustellen, müssen Sie zunächst die Sicherungseinstellungen auf Citrix ADM konfigurieren. Nach der Konfiguration der Einstellungen können Sie eine einzelne Citrix ADC-Instanz oder mehrere Instanzen auswählen und eine Backup der Konfigurationsdateien in diesen Fällen erstellen. Bei Bedarf können Sie die Citrix ADC-Instanzen auch mithilfe dieser gesicherten Dateien wiederherstellen.

Erstellen einer Sicherung für eine ausgewählte Citrix ADC-Instanz mithilfe von Citrix ADM

Führen Sie diese Aufgabe aus, wenn Sie eine ausgewählte Citrix ADC-Instanz oder mehrere Instanzen sichern möchten:

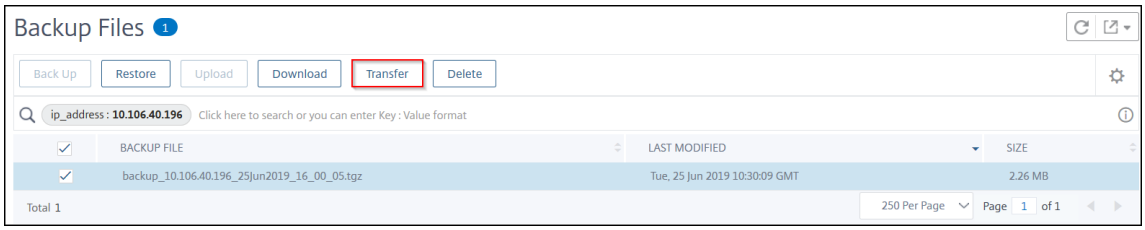
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen**. Wählen Sie unter **Instanzen**den Typ der Instanzen (z. B. VPX) aus, die auf dem Bildschirm angezeigt werden sollen.
2. Wählen Sie die Instanz aus, die Sie sichern möchten.
    - Wählen Sie für MPX-, VPX- und BLX-Instanz aus der Liste **Aktion auswählen die Option-Backup/Restore** aus.
    - Klicken Sie für eine SDX-Instanz auf **Backup/Restore**.
3. Klicken Sie auf der Seite **Sicherungsdateien** auf **Sichern**.
4. Geben Sie an, ob Sie Ihre Backup-Datei für mehr Sicherheit verschlüsseln möchten. Sie können entweder Ihr Kennwort eingeben oder das globale Kennwort verwenden, das Sie zuvor auf der Seite Instanzsicherungseinstellungen angegeben haben.
5. Klicken Sie auf **Weiter**.

Übertragen einer Backupdatei auf ein externes System

Als Vorsichtsmaßnahme können Sie eine Kopie Ihrer Backupdatei auf ein anderes System übertragen. Wenn Sie die Konfiguration wiederherstellen möchten, müssen Sie zuerst die Backupdatei auf den Citrix ADM -Server hochladen und dann den Wiederherstellungsvorgang ausführen.

So übertragen Sie eine Citrix ADM -Sicherungsdatei:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC** und wählen Sie dann den Instanz-Typ aus. Zum Beispiel VPX.
2. Wählen Sie die Instanz aus, und wählen Sie in der Liste **Aktion auswählen** die Option **Sicherung/Wiederherstellung** aus.
3. Wählen Sie die Backupdatei aus, und klicken Sie dann auf **Übertragen**.



Die Seite **Backupdatei übertragen** wird angezeigt. Geben Sie die folgenden Parameter an:

a) **Server** - IP-Adresse des Systems, an das Sie die Backupdatei übertragen möchten.

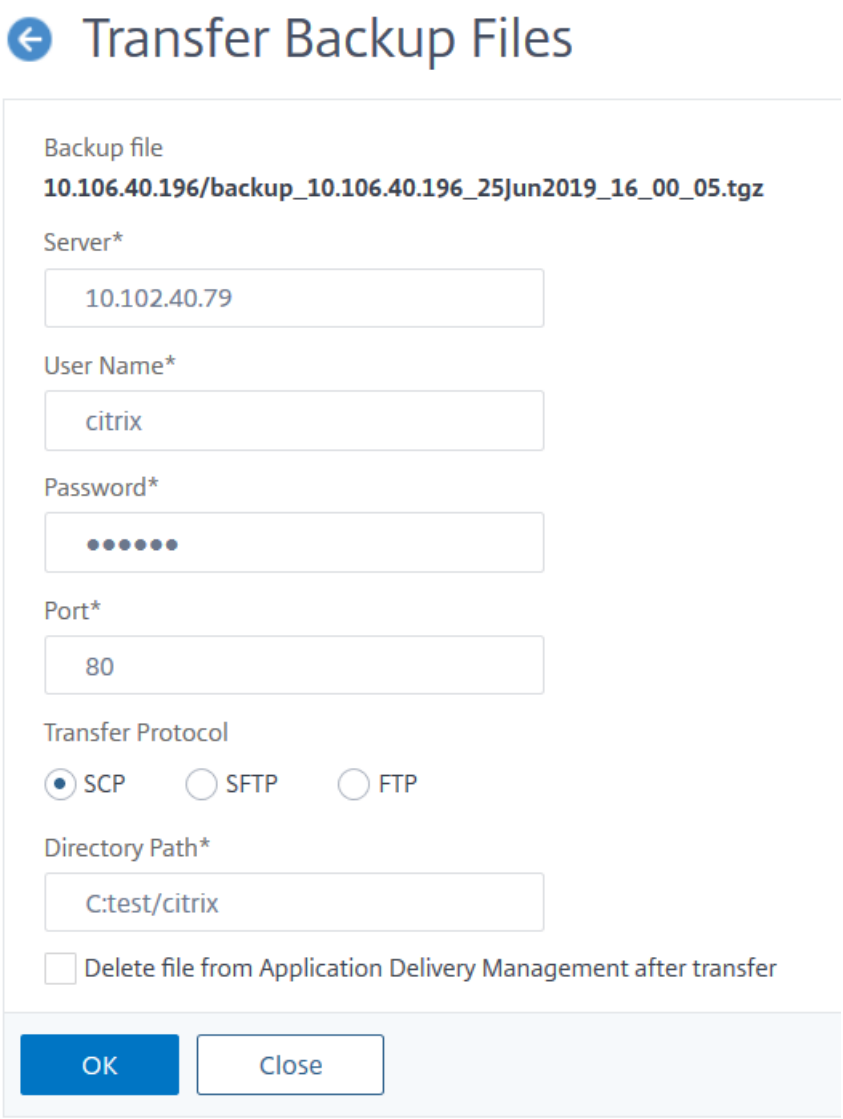
b) **Benutzername** und **Kennwort** — Benutzeranmeldeinformationen des neuen Systems, in das die gesicherten Dateien kopiert werden.

c) **Port** — Portnummer des Systems, in das die Dateien übertragen werden.

d) **Übertragungsprotokoll** — Protokoll, das verwendet wird, um die Backupdateiübertragung durchzuführen. Sie können SCP-, SFTP- oder FTP-Protokolle auswählen, um die Backupdatei zu übertragen.

e) **Verzeichnispfad** — Der Speicherort, an den die gesicherte Datei auf dem neuen System übertragen wird.

f) Klicken Sie auf **OK**.



Wiederherstellen einer Citrix ADC-Instanz mithilfe von Citrix ADM

Hinweis:

Wenn Sie Citrix ADC-Instanzen in einem HA-Paar haben, müssen Sie Folgendes beachten:

- Stellen Sie dieselbe Instanz wieder her, aus der die Backupdatei erstellt wurde. Betrachten wir beispielsweise ein Szenario, dass eine Sicherung von der primären Instanz des HA-Paares genommen wurde. Stellen Sie während des Wiederherstellungsvorgangs sicher, dass Sie dieselbe Instanz wiederherstellen, auch wenn sie nicht mehr die primäre Instanz ist.
- Wenn Sie den Wiederherstellungsprozess für die primäre ADC-Instanz initiieren, können Sie nicht auf die primäre Instanz zugreifen, und die sekundäre Instanz wird in **STAY-**

> **SECONDARY**geändert. Sobald der Wiederherstellungsvorgang für die primäre Instanz abgeschlossen ist, wechselt die sekundäre ADC-Instanz von **STAYSECONDARY** in den **ENABLED** Modus und wird wieder Teil des HA-Paares. Sie können eine mögliche Ausfallzeit für die primäre Instanz erwarten, bis der Wiederherstellungsvorgang abgeschlossen ist.

Führen Sie diese Aufgabe aus, um eine Citrix ADC-Instanz mithilfe der zuvor erstellten Backupdatei wiederherzustellen:

1. Navigieren Sie zu **Netzwerke** > **Instanzen**, wählen Sie die Instanz aus, die Sie wiederherstellen möchten, und klicken Sie dann auf **Sicherung anzeigen**.
2. Wählen Sie auf der Seite **Backupdateien** die Backupdatei aus, die die wiederherzustellenden Einstellungen enthält, und klicken Sie dann auf **Wiederherstellen**.

Wiederherstellen einer Citrix ADC SDX-Appliance mit Citrix ADM

In Citrix ADM umfasst die Sicherung der Citrix ADC SDX-Appliance Folgendes:

- Citrix ADC-Instanzen, die auf der Appliance gehostet werden
- SVM-SSL-Zertifikate und -Schlüssel
- Instanzbeschneidung (im XML-Format)
- Einstellungen für das Instanzbackup (im XML-Format)
- SSL-Zertifikatabfrageeinstellungen (im XML-Format)
- SVM db-Datei
- Citrix ADC Konfigurationsdateien von Geräten, die auf SDX vorhanden sind
- Citrix ADC Build-Images
- Citrix ADC XVA-Images werden diese Images am folgenden Speicherort gespeichert: `/var/mps/sdx_images/`
- SDX Single Bundle Image (SVM+XS)
- Instanzimages von Drittanbietern (falls bereitgestellt)

Sie müssen die Citrix ADC SDX-Appliance auf die in der Backupdatei verfügbare Konfiguration wiederherstellen. Während der Wiederherstellung der Appliance wird die gesamte aktuelle Konfiguration gelöscht.

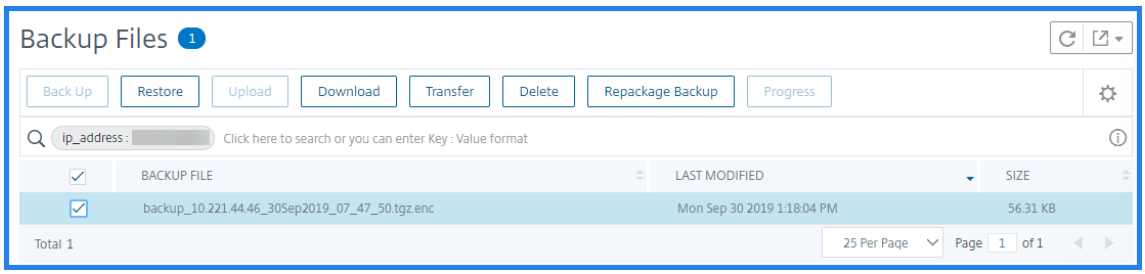
Wenn Sie die Citrix ADC SDX-Appliance mithilfe einer Sicherung einer anderen Citrix ADC SDX-Appliance wiederherstellen, stellen Sie sicher, dass Sie die Lizenzen hinzufügen und die Verwaltungsdienst-Netzwerkeinstellungen der Appliance so konfigurieren, dass sie mit denen in der Sicherungsdatei übereinstimmen, bevor Sie den Wiederherstellungsvorgang starten.

Stellen Sie sicher, dass die gesicherte Citrix ADC SDX-Plattformvariante dieselbe ist wie die, die Sie wiederherstellen möchten. Sie können nicht von einer anderen Plattformvariante wiederherstellen.

> **Hinweis**
>
> Bevor Sie die SDX RMA-Appliance wiederherstellen, stellen Sie sicher, dass die gesicherte Version entweder gleich oder höher als die RMA-Version ist.

So stellen Sie die SDX-Appliance aus der gesicherten Datei wieder her:

1. Navigieren Sie in der Citrix ADM GUI zu **Netzwerke > Instanzen > Citrix ADC**.
2. Klicken Sie auf **Backup/Restore**.
3. Wählen Sie die Backupdatei derselben Instanz aus, die Sie wiederherstellen möchten.
4. Klicken Sie auf **Backup neu verpacken**.



   Wenn die SDX-Appliance gesichert wird, werden die XVA-Dateien und -Images separat gespeichert, um die Netzwerkbandbreite und den Speicherplatz zu sparen. Daher müssen Sie die gesicherte Datei neu verpacken, bevor Sie die SDX-Appliance wiederherstellen.

   Wenn Sie die Backupdatei neu verpacken, enthält sie alle gesicherten Dateien zusammen, um die SDX-Appliance wiederherzustellen. Die neu verpackte Backupdatei stellt die erfolgreiche Wiederherstellung der SDX-Appliance sicher.

5. Wählen Sie die Backupdatei aus, die neu verpackt wird, und klicken Sie auf **Wiederherstellen**.

Exportieren des Berichts dieses Dashboards

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage

> eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Erzwingen eines Failovers auf die sekundäre Citrix ADC-Instanz

April 28, 2021

Sie können ein Failover erzwingen, wenn Sie beispielsweise die primäre Citrix Application Delivery Controller (Citrix ADC) -Instanz ersetzen oder aktualisieren müssen. Sie können ein Failover von der primären Instanz oder der sekundären Instanz erzwingen. Wenn Sie ein Failover für die primäre Instanz erzwingen, wird die primäre Instanz zur sekundären und die sekundäre zur primären Instanz. Ein erzwungenes Failover ist nur möglich, wenn die primäre Instanz feststellen kann, dass die sekundäre Instanz UP ist.

Ein erzwungenes Failover wird nicht propagiert oder synchronisiert. Um den Synchronisationsstatus nach einem erzwungenen Failover anzuzeigen, können Sie den Status der Instanz anzeigen.

Ein erzwungenes Failover schlägt unter folgenden Umständen fehl:

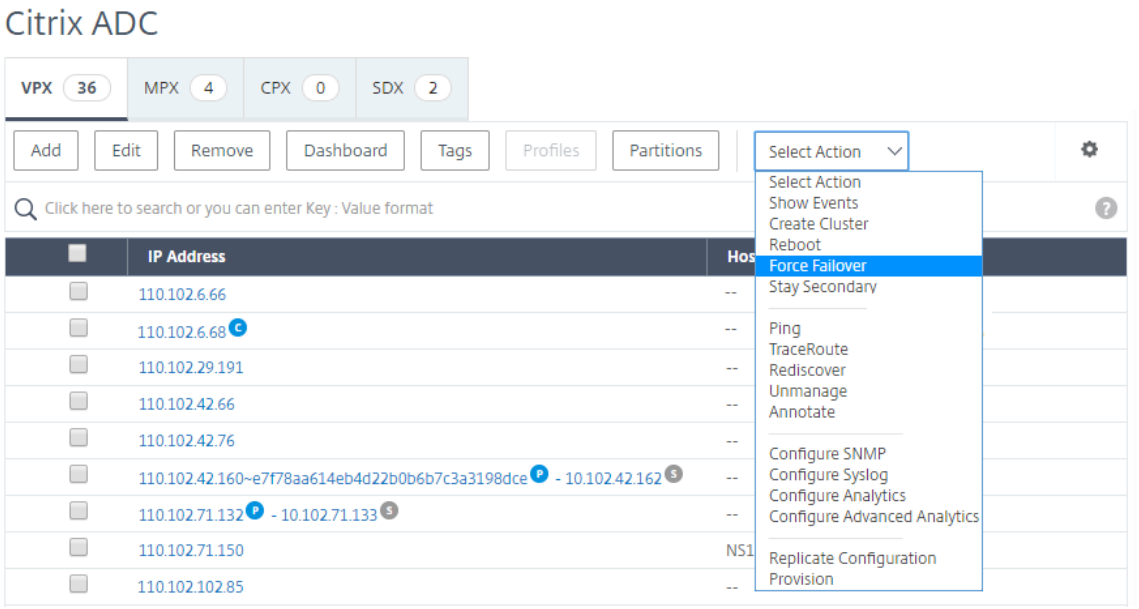
- Sie erzwingen ein Failover auf einem eigenständigen System.
- Die sekundäre Instanz ist deaktiviert oder inaktiv. Wenn sich die sekundäre Instanz in einem inaktiven Zustand befindet, müssen Sie warten, bis der Status UP ist, um ein Failover zu erzwingen.
- Die sekundäre Instanz ist so konfiguriert, dass sie sekundär bleibt.

Die Citrix ADC-Instanz zeigt eine Warnmeldung an, wenn ein potenzielles Problem beim Ausführen des Force-Failoverbefehls erkannt wird. Die Nachricht enthält die Informationen, die die Warnung ausgelöst haben, und fordert eine Bestätigung an, bevor Sie fortfahren.

Sie können ein Failover für eine primäre Instanz oder für eine sekundäre Instanz erzwingen.

So erzwingen Sie ein Failover auf die sekundäre Citrix ADC-Instanz mithilfe von Citrix ADM:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen**. Wechseln Sie zur Registerkarte **VPX** und wählen Sie eine Instanz aus.
2. Wählen Sie Instanzen in einem HA-Setup aus den Instanzen aus, die unter dem ausgewählten Instanztyp aufgeführt sind.
3. Wählen Sie im Feld **Aktion** die Option **Failover erzwingen** aus.
4. Klicken Sie auf **Ja**, um die Aktion “Failover erzwingen” zu bestätigen.



Erzwingen, dass eine sekundäre Citrix ADC-Instanz sekundär bleibt

April 28, 2021

In einem Hochverfügbarkeits-Setup (HA) kann der sekundäre Knoten gezwungen werden, unabhängig vom Status des primären Knotens zweitrangig zu bleiben.

Angenommen, der primäre Knoten muss aktualisiert werden und der Prozess dauert einige Sekunden. Während des Upgrades kann der primäre Knoten für einige Sekunden ausfallen, aber Sie möchten nicht, dass der sekundäre Knoten die Kontrolle übernimmt, und Sie möchten, dass er der sekundäre Knoten bleibt, selbst wenn er einen Fehler im primären Knoten erkennt.

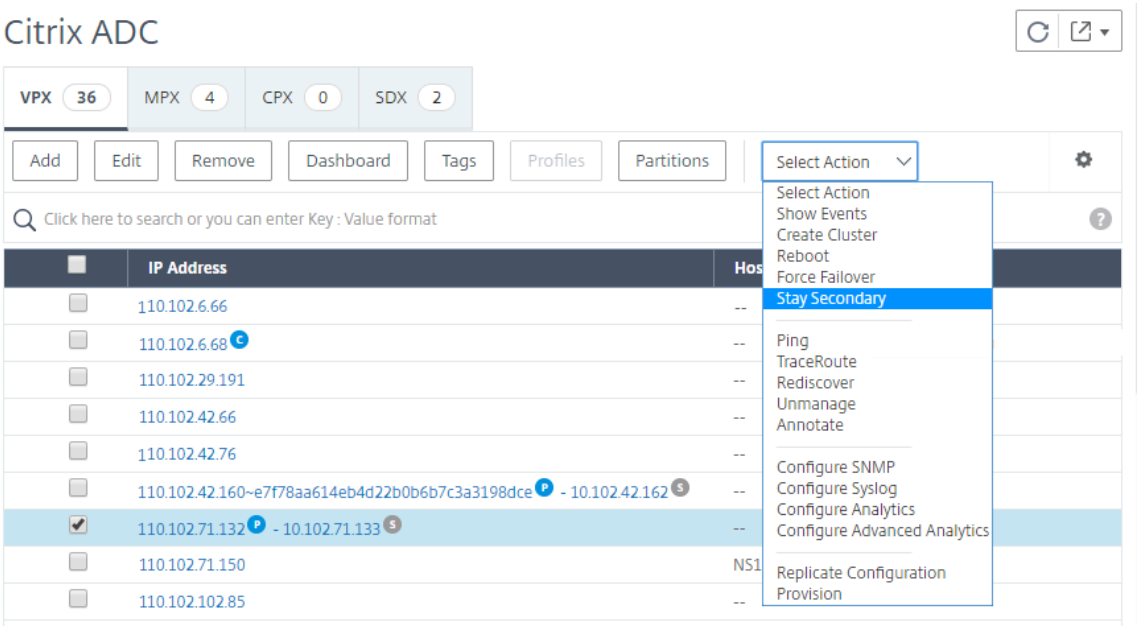
Wenn Sie den sekundären Knoten zwingen, sekundär zu bleiben, bleibt er sekundär, selbst wenn der primäre Knoten ausfällt. Wenn Sie erzwingen, dass der Status eines Knotens in einem HA-Paar sekundär bleibt, nimmt er nicht an Übergängen des HA-Zustands der Maschine teil. Der Status des Knotens wird als STAYSECONDARY angezeigt.

> **Hinweis**
>
> Wenn Sie ein System zwingen, sekundär zu bleiben, wird der erzwungene Prozess weder propagiert noch synchronisiert. Es betrifft nur den Knoten, auf dem Sie den Befehl ausführen.

So konfigurieren Sie mithilfe von Citrix ADM eine sekundäre Citrix ADC-Instanz, um mithilfe von Citrix ADM sekundär zu bleiben:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen**, und wählen Sie dann eine Instanz unter einem Instanztyp (VPX) aus.

2. Wählen Sie Instanzen in einem HA-Setup aus den Instanzen aus, die unter dem ausgewählten Instanztyp aufgeführt sind.
3. Wählen Sie im Feld **Aktion** die Option **Secondary bleiben** aus.
4. Klicken Sie auf **Ja**, um die Ausführung der Aktion Secondary bleiben zu bestätigen.



Instanzgruppen erstellen

April 28, 2021

Um eine Instanzgruppe zu erstellen, müssen Sie zuerst alle Citrix ADC-Instanzen zu Citrix ADM hinzufügen. Nachdem Sie die Instanzen erfolgreich hinzugefügt haben, erstellen Sie Instanzgruppen basierend auf ihrer Instanzfamilie. Das Erstellen einer Gruppe von Instanzen hilft Ihnen dabei, die gruppierten Instanzen gleichzeitig zu aktualisieren, zu sichern oder wiederherzustellen.

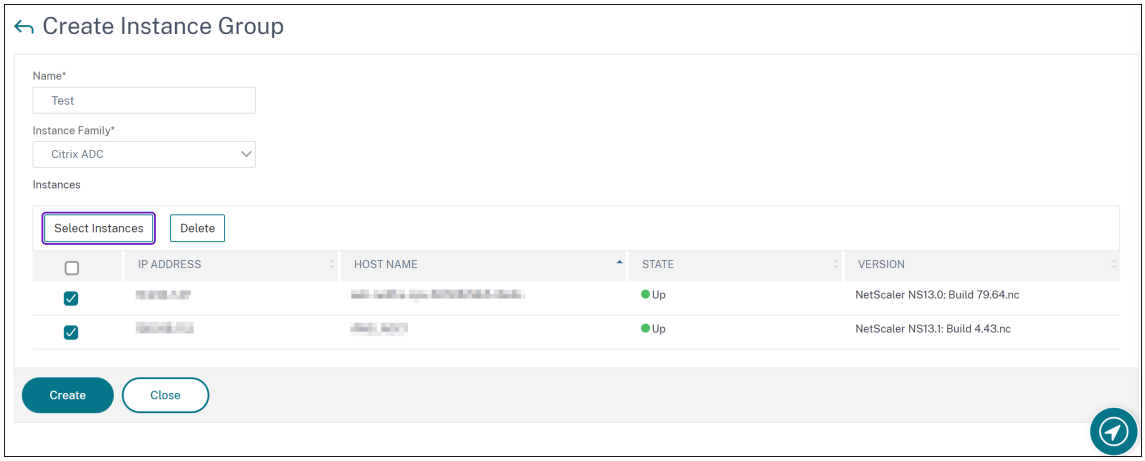
So erstellen Sie eine Instanzgruppe mit Citrix ADM

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzgruppen**, und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie einen Namen für Ihre Instanzgruppe an, und wählen Sie **Citrix ADC** aus der Liste **Instanzfamilie** aus.
3. Wählen Sie unter **Kategorie**die Option **Standard**aus.

4. Klicken Sie auf **Instanzen auswählen**. Wählen Sie auf der Seite **Instanzen auswählen** die Instanzen aus, die Sie gruppieren möchten, und klicken Sie auf **Auswählen**.

   Die Tabelle listet die ausgewählten Instanzen und deren Details auf. Wenn Sie eine Instanz aus der Gruppe entfernen möchten, wählen Sie die Instanz aus der Tabelle aus, und klicken Sie auf **Löschen**.

5. Klicken Sie auf **Erstellen**.



Bereitstellen von ADC VPX-Instanzen auf SDX mithilfe von ADM

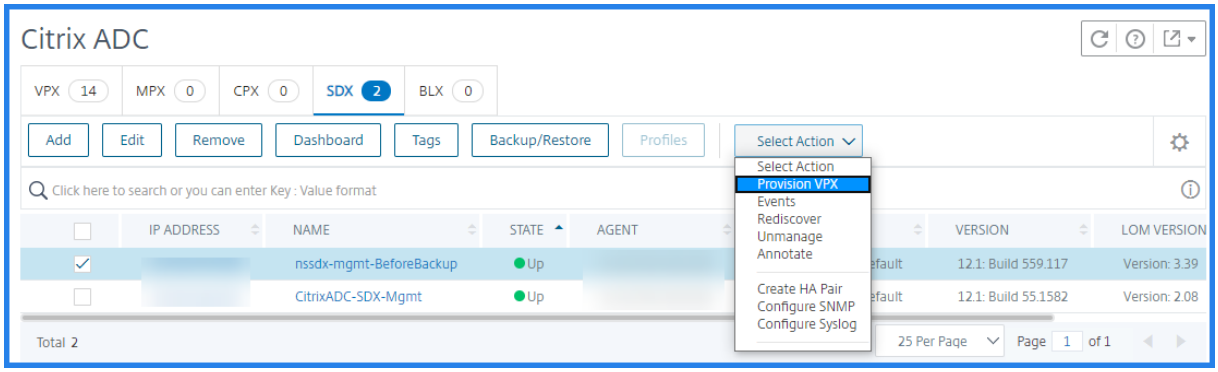
April 28, 2021

Sie können eine oder mehrere ADC VPX-Instanzen auf der SDX-Appliance mit Citrix ADM bereitstellen. Die Anzahl der Instanzen, die Sie bereitstellen können, hängt von der erworbenen Lizenz ab. Wenn die Anzahl der hinzugefügten Instanzen der in der Lizenz angegebenen Anzahl entspricht, können Sie mit dem ADM-Dienst keine weiteren Citrix ADC-Instanzen bereitstellen.

Bevor Sie beginnen, stellen Sie sicher, dass Sie eine SDX-Instanz in ADM hinzufügen, in der Sie VPX-Instanzen bereitstellen möchten.

Führen Sie die folgenden Schritte aus, um eine VPX-Instanz bereitzustellen:

1. Navigieren Sie zu **Netzwerke > Instanzen > Citrix ADC**.
2. Wählen Sie auf der Registerkarte **SDX** eine SDX-Instanz aus, in der Sie eine VPX-Instanz bereitstellen möchten.
3. **Wählen Sie unter Aktion**auswählen die Option **VPX bereitstellen**aus.

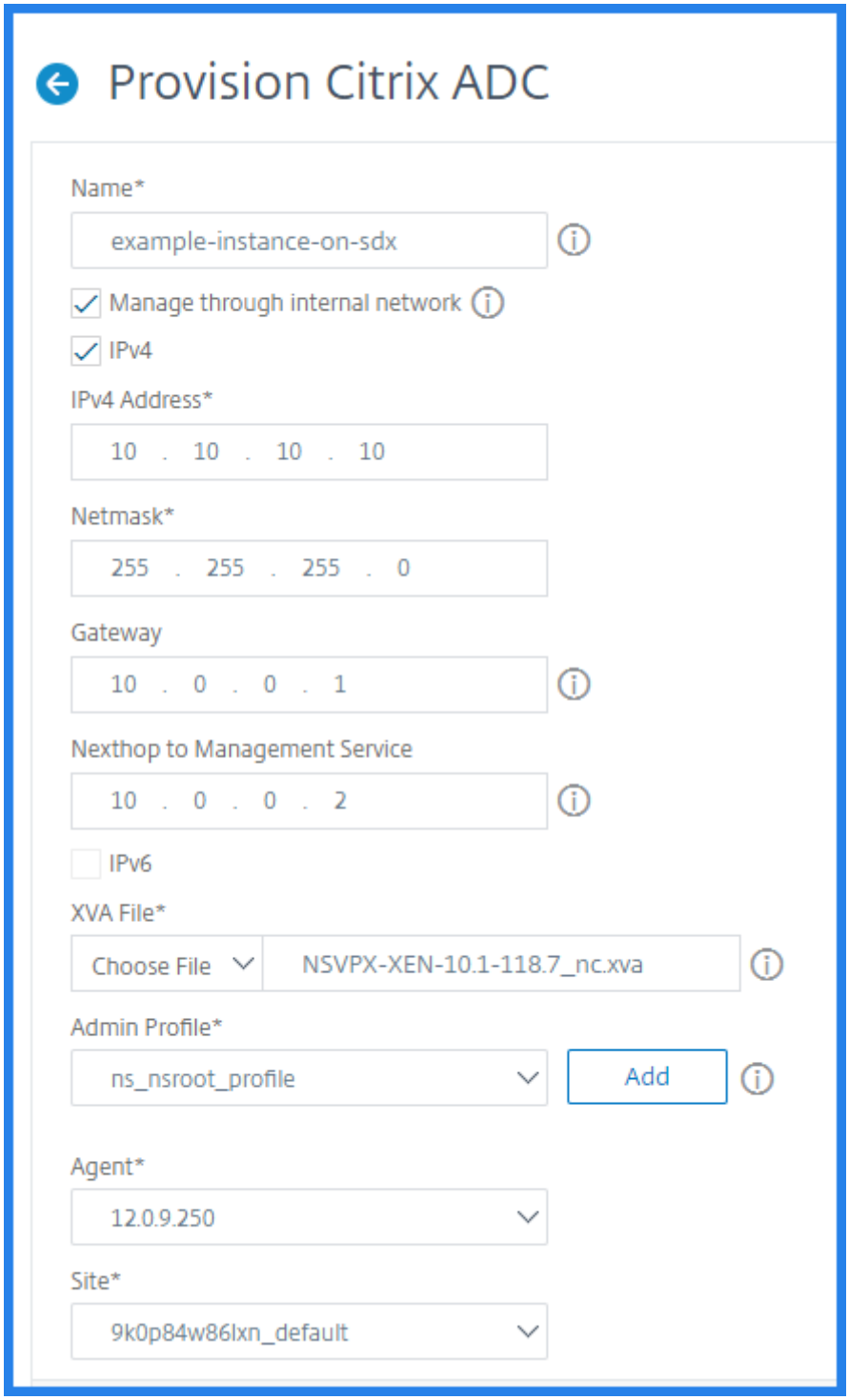


Schritt 1 - Hinzufügen einer VPX-Instanz

Der ADM-Dienst verwendet die folgenden Informationen, um VPX-Instanzen in einer SDX-Appliance zu konfigurieren:

- **Name** - Geben Sie einen Namen für eine ADC-Instanz an.
- Aufbau eines Kommunikationsnetzwerks zwischen SDX und VPX. Wählen Sie dazu die gewünschten Optionen aus der Liste aus:
  - **Über internes Netzwerk verwalten** : Mit dieser Option wird ein internes Netzwerk für eine Kommunikation zwischen dem ADM und einer VPX-Instanz eingerichtet.
  - **IP-Adresse**: Sie können eine **IPv4**- oder **IPv6**-Adresse oder beides auswählen, um die Citrix VPX-Instanz zu verwalten. Eine VPX-Instanz kann nur über eine Verwaltungs-IP verfügen (auch als Citrix ADC IP bezeichnet). Sie können die Citrix ADC IP-Adresse nicht entfernen.

    Weisen Sie für die ausgewählte Option dem ADM-Dienst eine Netzmaske, ein Standardgateway und einen nächsten Hop für die IP-Adresse zu.
- **XVA-Datei** - Wählen Sie die XVA-Datei aus, aus der Sie eine VPX-Instanz bereitstellen möchten. Verwenden Sie eine der folgenden Optionen, um die XVA-Datei auszuwählen.
  - **Lokal** - Wählen Sie die XVA-Datei von Ihrem lokalen Computer aus.
  - **Appliance** : Wählen Sie die XVA-Datei in einem ADM-Dateibrowser aus.
- **Admin-Profil** : Dieses Profil bietet Zugriff auf die Bereitstellung von VPX-Instanzen. Mit diesem Profil ruft ADM die Konfigurationsdaten von einer Instanz ab. Wenn Sie ein Profil hinzufügen müssen, klicken Sie auf **Hinzufügen**.
- **Agent** - Wählen Sie den Agenten aus, dem Sie die Instanzen zuordnen möchten.
- **Site** - Wählen Sie den Standort aus, an dem die Instanz hinzugefügt werden soll.



Schritt 2 - Zuweisen von Lizenzen

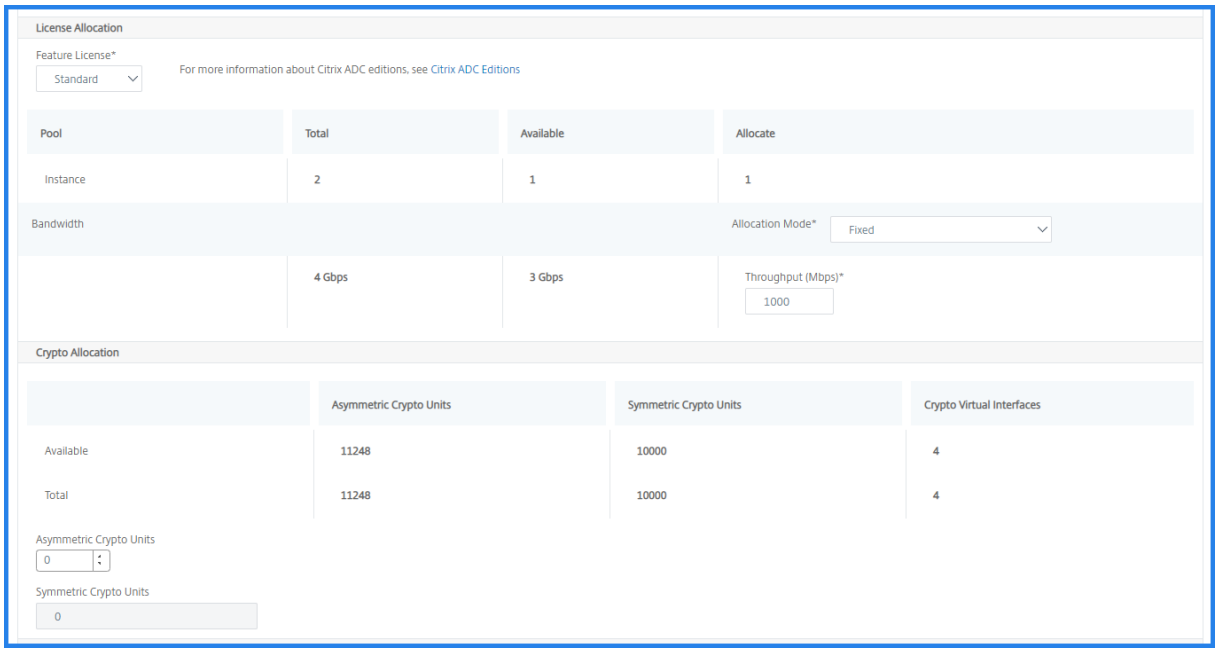
Geben Sie im Abschnitt **Lizenzzuweisung** die VPX-Lizenz an. Sie können Standard-, Advanced- und Premium-Lizenzen verwenden.

- **Zuweisungsmodus** - Sie können **Fest-** oder **Burstable-Modi** für den Bandbreitenpool wählen.

  Wenn Sie den **Burstable-Modus** wählen, können Sie zusätzliche Bandbreite verwenden, wenn die feste Bandbreite erreicht ist.

- **Durchsatz** - Weisen Sie einer Instanz den Gesamtdurchsatz (in Mbit/s) zu.

> **Hinweis
>
> Kaufen Sie**eine separate Lizenz (SDX 2-Instanz Add-On Pack für Secure Web Gateway) für Citrix Secure Web Gateway (SWG) Instanzen auf SDX-Geräten. Dieses Instanz-Pack unterscheidet sich von der SDX-Plattformlizenz oder dem SDX-Instanz-Pack.
>
> Weitere Informationen finden Sie unter Bereitstellen einer Citrix Secure Web Gateway-Instanz auf einer SDX-Appliance.



Ab der SDX 12.0 57.19 Version hat sich die Schnittstelle zur Verwaltung der Krypto-Kapazität geändert. Weitere Informationen finden Sie unter Verwalten der Krypto-Kapazität.

Schritt 3 - Zuweisen von Ressourcen

Weisen Sie im Abschnitt **Ressourcenzuweisung** Ressourcen einer VPX-Instanz zu, um den Datenverkehr aufrechtzuerhalten.

- **Gesamtspeicher (MB)** - Weisen Sie einer Instanz den Gesamtspeicher zu. Der Mindestwert ist `2048`MB.
- **Pakete pro Sekunde** - Geben Sie die Anzahl der Pakete an, die pro Sekunde übertragen werden sollen.

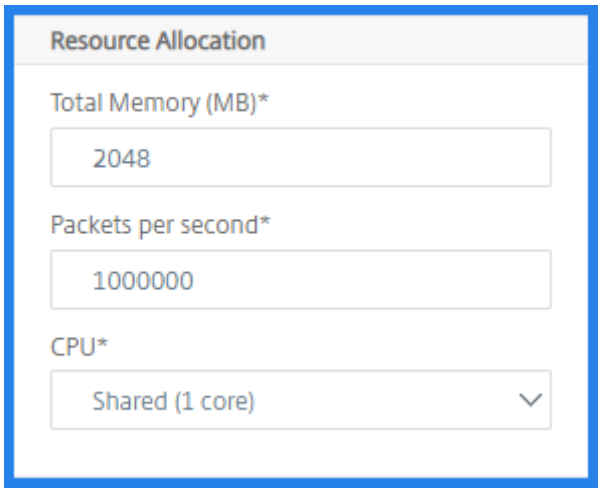
- **CPU** - Geben Sie die Anzahl der CPU-Kerne einer Instanz an. Sie können gemeinsam genutzte oder dedizierte CPU-Kerne verwenden.

  Wenn Sie einen gemeinsam genutzten Kern für eine Instanz auswählen, können die anderen Instanzen den gemeinsam genutzten Kern zum Zeitpunkt des Ressourcenmangels verwenden.

  Starten Sie Instanzen neu, auf denen CPU-Kerne neu zugewiesen werden, um Leistungseinbußen zu vermeiden.

  Wenn Sie die SDX 25000xx-Plattform verwenden, können Sie einer Instanz maximal 16 Kerne zuweisen. Wenn Sie die SDX 2500xxx-Plattform verwenden, können Sie einer Instanz maximal 11 Kerne zuweisen.

  > **Hinweis**
  >
  > Für eine Instanz beträgt der maximale Durchsatz, den Sie konfigurieren, 180 Gbit/s.



In der folgenden Tabelle sind die unterstützten VPX, Single Bungle Image-Version und die Anzahl der Cores aufgeführt, die Sie einer Instanz zuweisen können:

Plattformname	Gesamtkerne	Insgesamt verfügbare Kerne für VPX-Provisioning	Maximale Anzahl der Kerne, die einer einzelnen Instanz zugewiesen werden können
SDX 8015, SDX 8400 und SDX 8600	4	3	3
SDX 8900	8	7	7

Plattformname	Gesamtkerne	Insgesamt verfügbare Kerne für VPX-Provisioning	Maximale Anzahl der Kerne, die einer einzelnen Instanz zugewiesen werden können
SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500 und SDX 20500	12	10	5
SDX 11515, SDX 11520, SDX 11530, SDX 11540 und SDX 11542	12	10	5
SDX 17500, SDX 19500 und SDX 21500	12	10	5
SDX 17550, SDX 19550, SDX 20550 und SDX 21550	12	10	5
SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 und SDX 14100	12	10	5
SDX 22040, SDX 22060, SDX 22080, SDX 22100 und SDX 22120	16	14	7
SDX 24100 und SDX 24150	16	14	7
SDX 14020 40G, SDX 14030 40G, SDX 14040 40G, SDX 14060 40G, SDX 14080 40G und SDX 14100 40G	12	10	10

Plattformname	Gesamtkerne	Insgesamt verfügbare Kerne für VPX-Provisioning	Maximale Anzahl der Kerne, die einer einzelnen Instanz zugewiesen werden können
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS und SDX 14100. FIPS	12	10	5
SDX 14040 40S, SDX 14060 40S, SDX 14080 40S und SDX 14100 40S	12	10	5
SDX 25100A, 25160A, 25200A	20	18	9
SDX 25100-40 G, 25160-40 G, 25200-40 G	20	18	16 (wenn Version 11.1-51.x oder höher ist); 9 (wenn Version 11.1-50.x oder niedriger ist; alle Versionen von 11.0 und 10.5)
SDX 26100, 26160, 26200, 26250	28	26	13
15000-50G	16	14	7

Hinweis

Auf der SDX 26xxx-Plattform können maximal 26 CPU-Kerne einer VPX-Instanz zugewiesen werden. Wenn der Instanz Krypto-Einheiten zugewiesen werden, hängt die maximale Anzahl von Kernen von der Anzahl der Krypto-Einheiten und Datenschnittstellen ab.

Wenn Sie einer Instanz beispielsweise 24000 Krypto-Einheiten zuweisen, können Sie der Instanz 24 CPU-Kerne und maximal zwei Datenschnittstellen zuweisen. Die SDX-Appliance betrachtet Datenschnittstellen und Kryptoeinheiten als PCI-Geräte. Bei 26000 Krypto-Einheiten schlägt die VPX-Instanzprovisioning fehl, da kein Platz zum Hinzufügen von Datenschnittstellen vorhanden

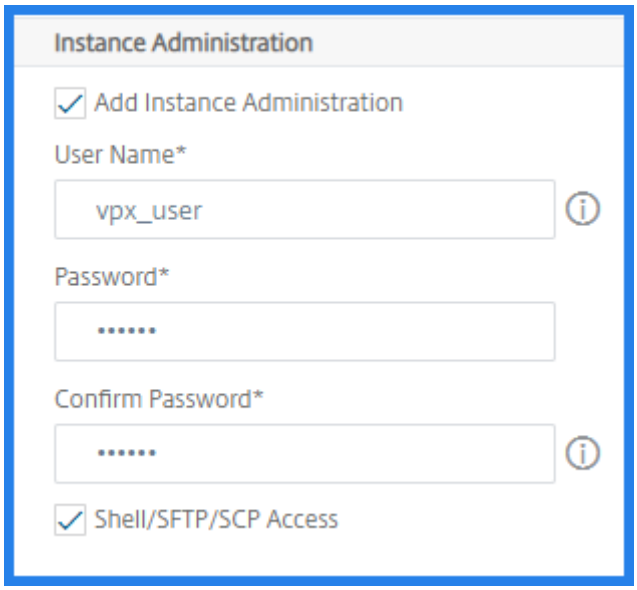
> ist.

Schritt 4 - Instanzverwaltung hinzufügen

Sie können einen Admin-Benutzer für die VPX-Instanz erstellen. Wählen Sie dazu im Abschnitt **Instanzverwaltung die Option**Instanzverwaltung**hinzufügen** aus.

Geben Sie die folgenden Details an:

- **Benutzername**: Der Benutzername für den Citrix ADC-Instanzadministrator. Dieser Benutzer verfügt über Superuser-Zugriff, hat aber keinen Zugriff auf Netzwerkbefehle zum Konfigurieren von VLANs und Schnittstellen.
- **Kennwort**: Geben Sie das Kennwort für den Benutzernamen an.
- **Shell/Sftp/Scp Access**: Der Zugriff, der dem Citrix ADC-Instanzadministrator gewährt wird. Diese Option ist standardmäßig ausgewählt.



Schritt 5 - Angeben von Netzwerkeinstellungen

Wählen Sie die erforderlichen Netzwerkeinstellungen für eine Instanz aus:

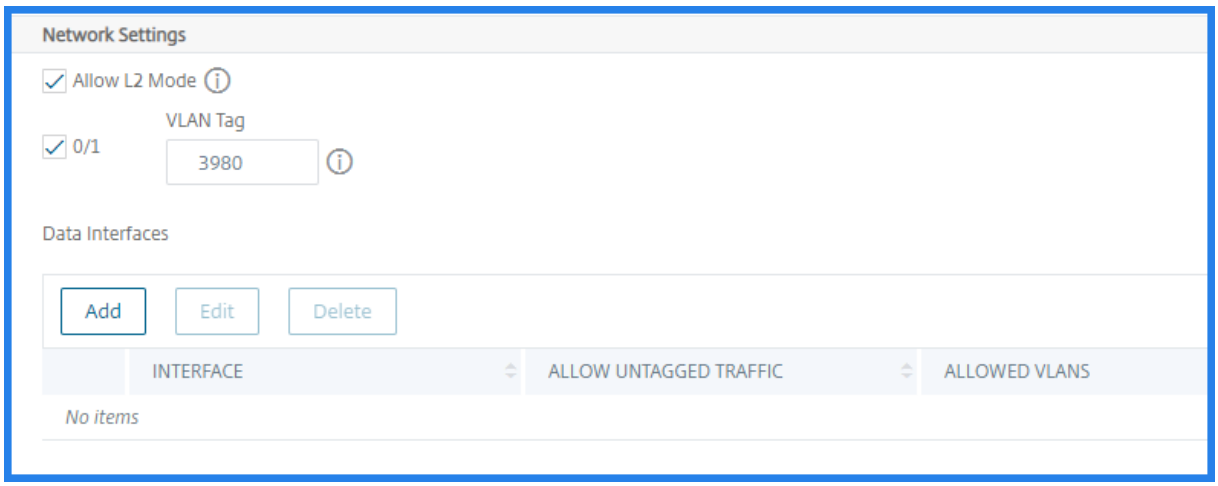
- **L2-Modus unter Netzwerkeinstellungen** zulassen: Sie können den L2-Modus auf der Citrix ADC-Instanz zulassen. Wählen Sie unter Netzwerkeinstellungen die Option L2-Modus zulassen aus. Bevor Sie sich bei der Instanz anmelden und den L2-Modus aktivieren. Weitere Informationen finden Sie unter Zulassen des L2-Modus auf einer Citrix ADC-Instanz.

  > **Hinweis**
  >
  > Wenn Sie den L2-Modus für eine Instanz deaktivieren, müssen Sie sich bei der Instanz an-

> melden und den L2-Modus von dieser Instanz aus deaktivieren. Andernfalls werden alle anderen Citrix ADC Modi nach dem Neustart der Instanz deaktiviert.

- **0/1** - Geben Sie im **VLAN-Tag**eine VLAN-ID für die Verwaltungsschnittstelle an.
- **0/2** - Geben Sie im **VLAN-Tag**eine VLAN-ID für die Verwaltungsschnittstelle an.

Standardmäßig sind die Schnittstellen **0/1** und **0/2** ausgewählt.



Klicken Sie unter **Datenschnittstellen**auf **Hinzufügen**, um Datenschnittstellen hinzuzufügen, und geben Sie Folgendes an:

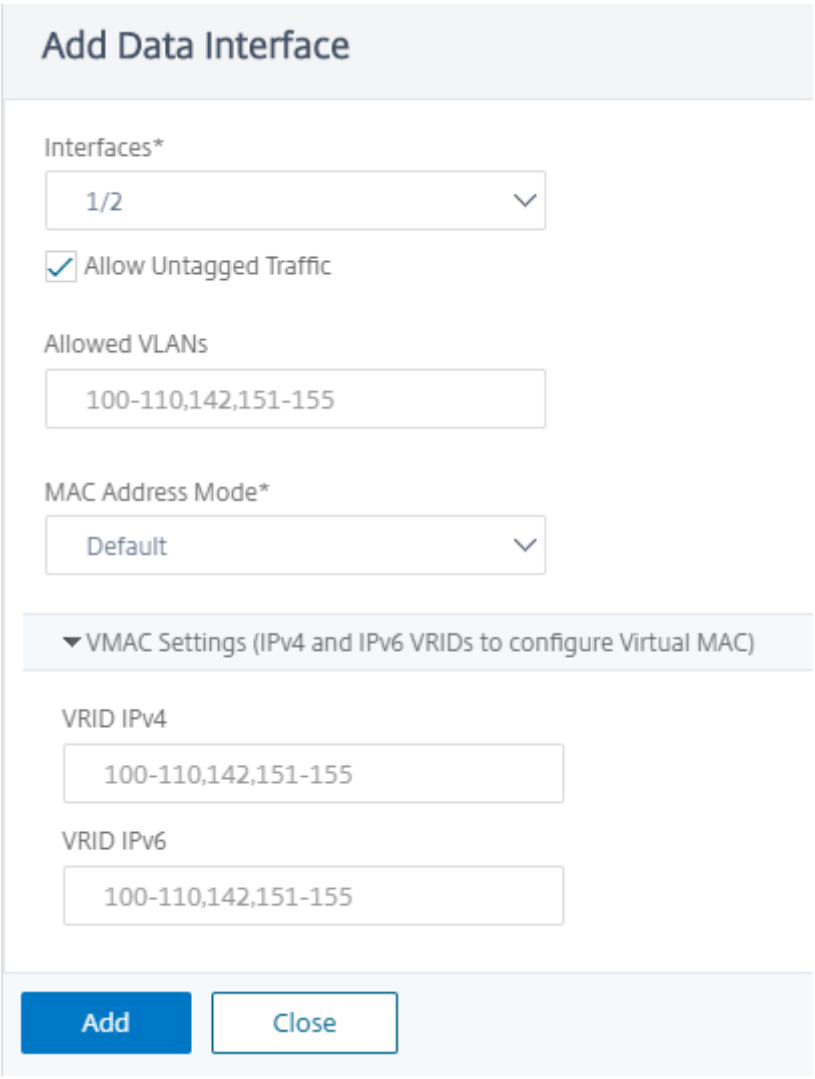
- **Schnittstellen** - Wählen Sie die Schnittstelle aus der Liste aus.

  > **Hinweis**
  >
  > Die Schnittstellen-IDs von Schnittstellen, die Sie einer Instanz hinzufügen, entsprechen nicht unbedingt der physischen Schnittstellennummerierung auf der SDX-Appliance.
  >
  > Beispielsweise ist die erste Schnittstelle, die Sie mit Instanz-1 verknüpfen, die SDX-Schnittstelle 1/4. Sie wird als Schnittstelle 1/1 angezeigt, wenn Sie die Schnittstelleneinstellungen in dieser Instanz anzeigen. Diese Schnittstelle gibt an, dass es sich um die erste Schnittstelle handelt, die Sie mit Instanz-1 verknüpft haben.

- **Zulässige VLANs** : Geben Sie eine Liste von VLAN-IDs an, die einer Citrix ADC-Instanz zugeordnet werden können.
- **MAC-Adressmodus** - Weisen Sie einer Instanz eine MAC-Adresse zu. Wählen Sie eine der folgenden Optionen:
  - **Standard** : Citrix Workspace weist eine MAC-Adresse zu.
  - **Benutzerdefiniert** - Wählen Sie diesen Modus, um eine MAC-Adresse anzugeben, die die generierte MAC-Adresse überschreibt.
  - **Generiert** - Generiert eine MAC-Adresse mithilfe der zuvor festgelegten Basis-MAC-Adresse. Weitere Informationen zum Festlegen einer Basis-MAC-Adresse finden Sie unter

Zuweisen einer MAC-Adresse zu einer Schnittstelle.

- **VMAC-Einstellungen (IPv4- und IPv6-VRIDs zum Konfigurieren von Virtual MAC)**
  - **VRID IPV4** - Die IPv4-VRID, die die VMAC identifiziert. Mögliche Werte: 1 — 255. Weitere Informationen finden Sie unter Konfigurieren von VMACs auf einer Schnittstelle.
  - VRID IPV6 - Die IPv6-VRID, die die VMAC identifiziert. Mögliche Werte: 1 — 255. Weitere Informationen finden Sie unter Konfigurieren von VMACs auf einer Schnittstelle.



Klicken Sie auf **Hinzufügen**.

Schritt 6 - Angeben von Verwaltungs-VLAN-Einstellungen

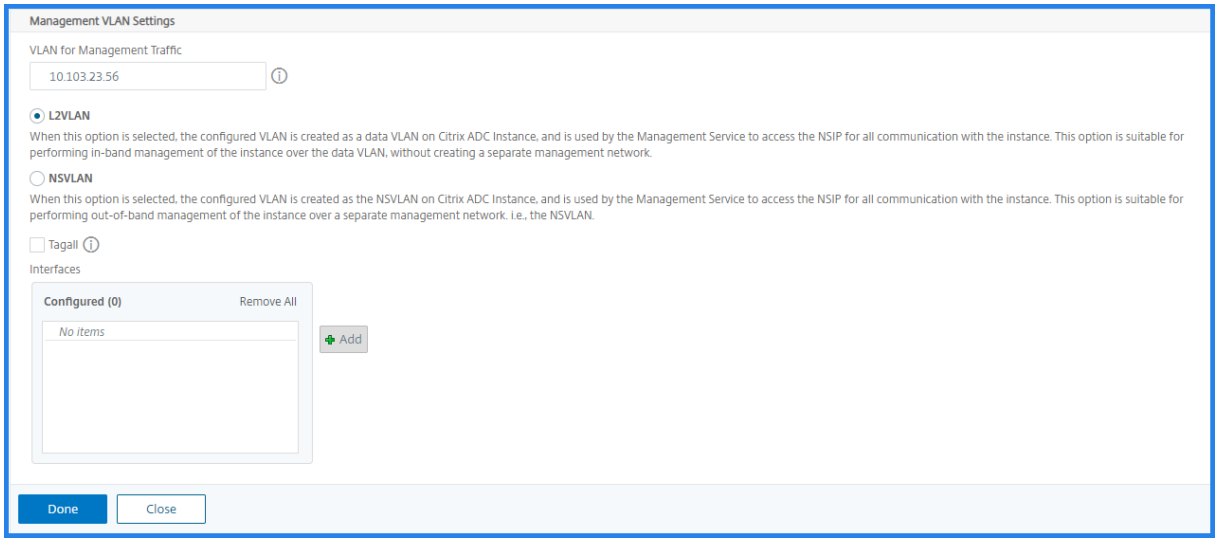
Der Verwaltungsdienst und die Verwaltungsadresse (NSIP) der VPX-Instanz befinden sich im selben Teilnetz, und die Kommunikation erfolgt über eine Verwaltungsschnittstelle.

Wenn sich der Verwaltungsdienst und die Instanz in verschiedenen Teilnetzen befinden, geben Sie eine VLAN-ID an, während Sie eine VPX-Instanz bereitstellen. Daher ist die Instanz über das Netzwerk erreichbar, wenn sie aktiv ist.

Wenn für Ihre Bereitstellung der NSIP nur über die ausgewählte Schnittstelle zugänglich ist, während die VPX-Instanz Provisioning wird, wählen Sie **NSVLAN**aus. Und das NSIP wird über andere Schnittstellen unzugänglich.

- HA-Heartbeats werden nur an den Schnittstellen gesendet, die Teil des NSVLAN sind.
- Sie können ein NSVLAN nur aus dem VPX XVA-Build `9.3-53.4`und höher konfigurieren.

> **Wichtig**
>
> - Sie können diese Einstellung nicht ändern, nachdem Sie die VPX-Instanz bereitgestellt haben.
> - Der `clear config full`Befehl auf der VPX-Instanz löscht die VLAN-Konfiguration, wenn **NSVLAN** nicht ausgewählt ist.

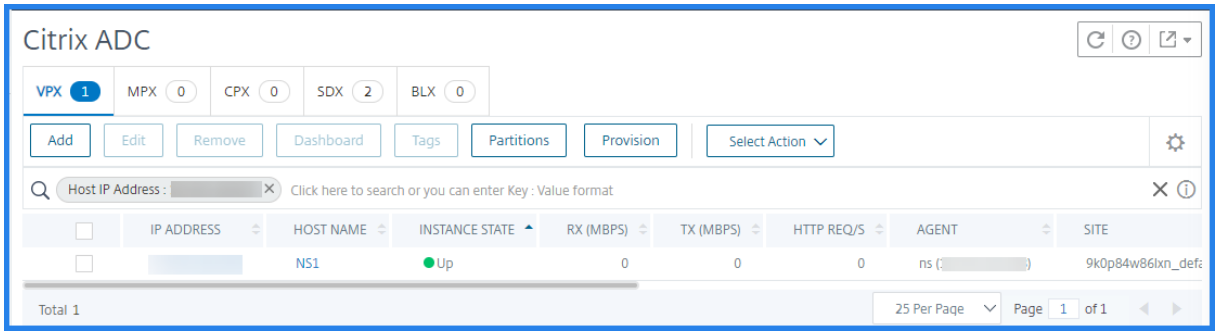


Klicken Sie auf **Fertig**, um eine VPX-Instanz bereitzustellen.

Anzeigen der bereitgestellten VPX-Instanz

Führen Sie die folgenden Schritte aus, um die neu bereitgestellte Instanz anzuzeigen:

1. Navigieren Sie zu **Netzwerke > Instanzen > Citrix ADC**.
2. Suchen Sie auf der Registerkarte **VPX** eine Instanz nach der Eigenschaft **Host-IP-Adresse**, und geben Sie die IP-Adresse der SDX-Instanz an.



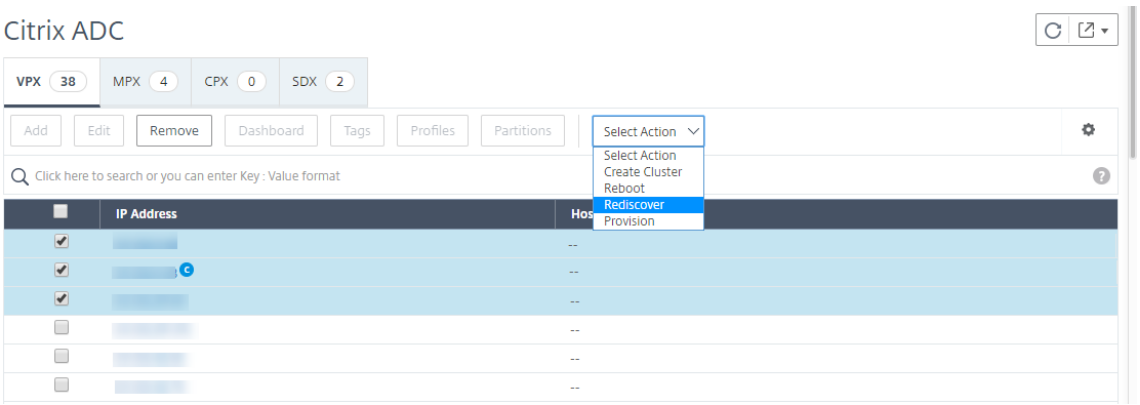
Wiederfinden mehrerer Citrix ADC VPX Instanzen

April 28, 2021

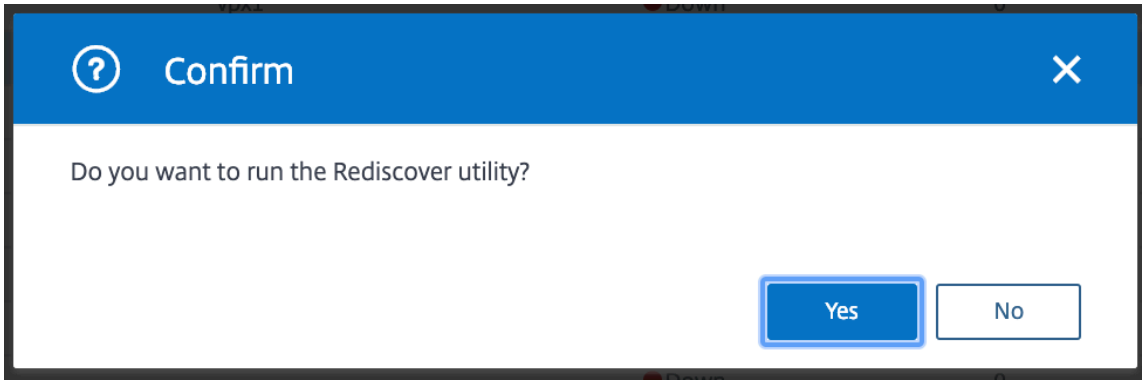
Sie können jetzt mehrere Citrix Application Delivery Controller (Citrix ADC) VPX-Instanzen in Ihrem Citrix Application Delivery Management (Citrix ADM) Setup neu erkennen. Bisher konnten Sie nur einzelne Citrix ADC VPX-Instanzen wiederfinden. Sie können mehrere Citrix ADC VPX Instanzen neu erkennen, wenn Sie die neuesten Status und Konfigurationen dieser Instanzen anzeigen möchten. Der Citrix ADM -Server erkennt alle Citrix ADC VPX Instanzen erneut und überprüft, ob die Citrix ADC-Instanzen erreichbar sind.

So ermitteln Sie mehrere Citrix ADC VPX Instanzen erneut:

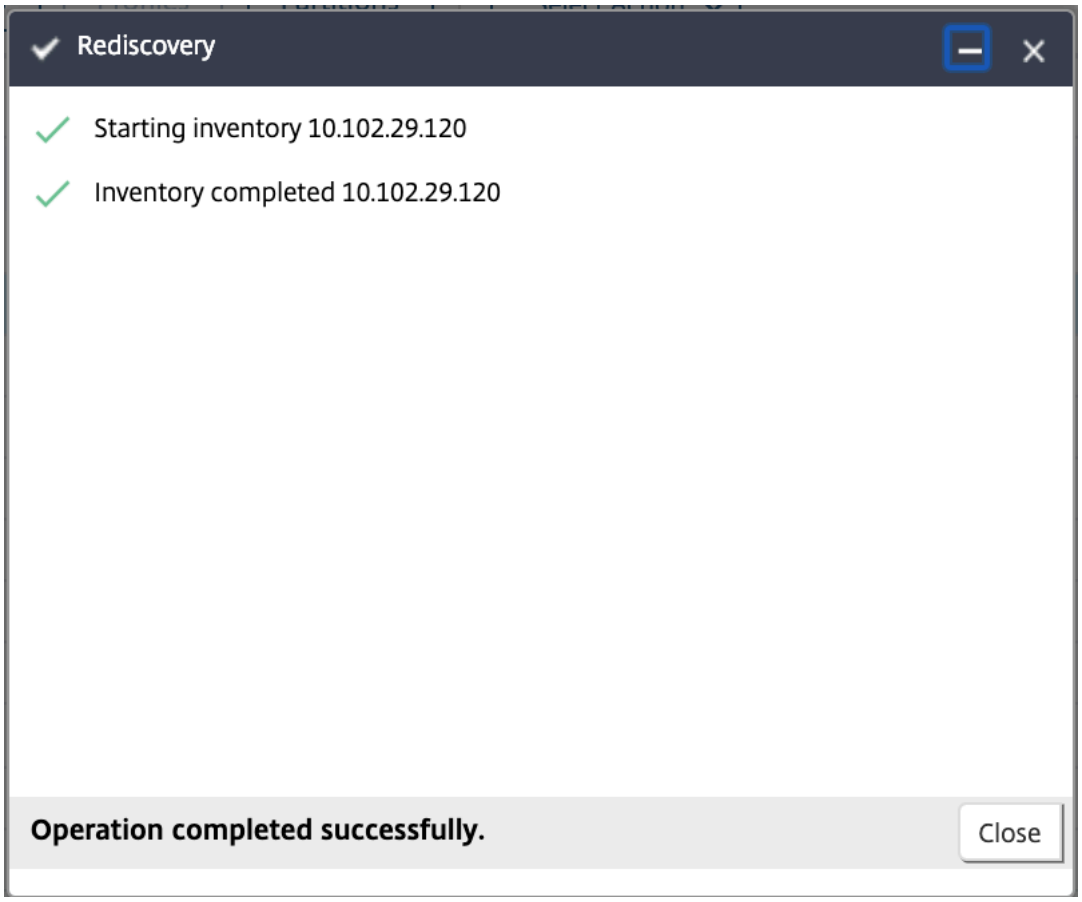
1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC** > **VPX**, und wählen Sie die Instanzen aus, die Sie erneut ermitteln möchten.
2. Klicken Sie im Feld **Aktion** auf **Wiederermitteln**.



3. Wenn die Bestätigungsmeldung für die Ausführung des Dienstprogramms Wiederermittlung angezeigt wird, klicken Sie auf **Ja**.



Auf dem Bildschirm wird der Fortschritt der Wiedererkennung der einzelnen Citrix ADC VPX Instanzen angezeigt.



Übersicht über die Abrufung

April 28, 2021

Polling ist ein Prozess, bei dem Citrix Application Delivery Management (ADM) bestimmte Infor-

mationen von Citrix ADC-Instanzen sammelt. Möglicherweise haben Sie weltweit mehrere Citrix ADC-Instanzen für Ihre Organisation konfiguriert. Um Ihre Instanzen über Citrix ADM zu überwachen, muss Citrix ADM bestimmte Informationen wie CPU-Auslastung, Speichernutzung, SSL-Zertifikate, lizenzierte Funktionen und Lizenztypen aus allen verwalteten ADC-Instanzen sammeln. Im Folgenden werden die verschiedenen Abruftypen aufgeführt, die zwischen ADM und den verwalteten Instanzen auftreten:

- Instanzabfrage
- Lagerbestandsabfrage
- Leistungsdatenerfassung
- Instanz-Backup-Abfrage
- Konfigurationsüberwachungsabfrage
- SSL-Zertifikatabruf
- Entitätsabfrage

Citrix ADM verwendet Protokolle wie NITRO -Aufruf, Secure Shell (SSH) und Secure Copy (SCP), um Informationen von Citrix ADC-Instanzen abzufragen.

Wie Citrix ADM verwaltete Instanzen und Entitäten abfragt

Citrix ADM fragt standardmäßig automatisch in regelmäßigen Abständen ab. Mit Citrix ADM können Sie auch Abrufintervalle für einige Abruftypen konfigurieren und bei Bedarf manuell abfragen.

In der folgenden Tabelle werden die Details der Abrufintervalle, des verwendeten Protokolls usw. beschrieben:

Abruftyp	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufintervalls
Instanzabfrage	Alle 5 Minuten (standardmäßig)	Statistische Informationen wie Status, HTTP-Anforderungen pro Sekunde, CPU-Auslastung, Speicherauslastung und Durchsatz.	NITRO Anruf.	Nein

Abruftyp	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufintervalls
Lagerbestandsabfrage	Alle 60 Minuten (standardmäßig)	Bestandsdetails wie Build-Version, Systeminformationen, lizenzierte Funktionen und Modi.	NITRO -Anrufe und SSH	Nein
Leistungsdatener	Alle 5 Minuten (standardmäßig)	Informationen zur Netzwerkberichterstattung	NITRO Aufruf	Nein
Instanz-Backup-Abfrage	Alle 12 Stunden (standardmäßig)	Die Sicherungsdatei des aktuellen Status der verwalteten ADC-Instanzen	NITRO ruft, SSH und SCP.	Ja. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**. Wählen Sie die Instanz aus, und klicken Sie in der Liste **Aktion auswählen** auf **Backup/Restore**.

Abruftyp	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufintervalls
Konfigurationsüb	Alle 10 Stunden (standardmäßig)	Konfigurationsänd die auf ADC-Instanzen auftreten (z. B. Ausführung im Vergleich zu gespeicherten Konfiguratio-nen)	SSH, SCP und NITRO Anruf	Ja. Navigieren Sie zu **Netzwerke** > **Konfigura-tionsüberwachung**. Klicken Sie auf der Seite Configuration Audit auf **Einstellungen**, und konfigurieren Sie das Abrufintervall für Configuration Audit Polling.

Abruftyp	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufintervalls
				Sie können Konfigurationsaudits manuell abfragen und alle Konfigurationsaudits der Instanzen sofort Citrix ADM hinzufügen. Navigieren Sie dazu zu **Netzwerke** > **Konfigurationsüberwachung**, und klicken Sie auf **Jetzt abfragen**. Auf der Seite **Jetzt abfragen** können Sie alle oder ausgewählte Instanzen im Netzwerk abfragen.

Abruftyp	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufintervalls
Abfrage von SSL-Zertifikaten	Alle 24 Stunden (standardmäßig)	SSL-Zertifikate, die auf Citrix ADC-Instanzen installiert sind.	NITRO -Anrufe und SCP	Ja. Navigieren Sie zu **Netzwerke** > **SSL Dashboard**. Klicken Sie auf der Seite SSL-Dashboard auf **Einstellungen**, um das Abrufintervall zu konfigurieren.
				Sie können SSL-Zertifikate manuell abfragen und alle Zertifikate der Instanzen sofort Citrix ADM hinzufügen. Navigieren Sie dazu zu **Netzwerke** > **SSL-Dashboard** und klicken Sie auf **Jetzt abfragen**. Auf der Seite **Jetzt abfragen** können Sie alle oder ausgewählte Instanzen im Netzwerk abfragen.

Abruftyp	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufintervalls
Entitätsabfrage	Alle 60 Minuten (standardmäßig)	Alle Entitäten, die auf den Instanzen konfiguriert sind. Eine Entität ist entweder eine Richtlinie, ein virtueller Server, ein Dienst oder eine Aktion, die mit einer ADC-Instanz verknüpft ist. Informationen zum Aktivieren der Entitätsabfrage finden Sie unter Aktivieren oder Deaktivieren von ADM-Funktionen.	NITRO ruft an.	Ja, kann aber nicht auf weniger als 10 Minuten eingestellt werden. Navigieren Sie zum Konfigurieren zu **Netzwerke** > **Netzwerkfunktionen**. Klicken Sie auf der Seite Netzwerkfunktion auf **Einstellungen**, um das Abrufintervall zu konfigurieren.

Abruftyp	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufintervalls
				Sie können Entitäten manuell abfragen und alle Entitäten der Instanzen sofort Citrix ADM hinzufügen. Navigieren Sie dazu zu **Netzwerke** > **Netzwerkfunktionen** und klicken Sie auf **Jetzt abfragen**. Auf der Seite **Jetzt abfragen** können Sie alle oder ausgewählte Instanzen im Netzwerk abfragen.

Hinweis

Zusätzlich zum Polling werden von verwalteten ADC-Instanzen generierte Ereignisse von Citrix ADM über SNMP-Traps empfangen, die an die Instanzen gesendet werden. Beispielsweise wird ein Ereignis generiert, wenn ein Systemfehler oder eine Änderung der Konfiguration vorliegt.

Während des Instanzbackups werden SSL-Dateien, CA-Zertifikatdateien, ADC-Vorlagen, Datenbankinformationen usw. in Citrix ADM heruntergeladen. Während einer Konfigurationsüberwachung werden ns.conf-Dateien heruntergeladen und im Dateisystem gespeichert. Alle Informationen, die von verwalteten Citrix ADC-Instanzen erfasst werden, werden intern in der Datenbank gespeichert.

Verschiedene Möglichkeiten zum Abrufen von Instanzen

Im Folgenden werden die verschiedenen Abrufmethoden beschrieben, die Citrix ADM für die verwalteten Instanzen durchführt:

- Globale Abfrage von Instanzen
- Manuelles Abrufen von Instanzen
- Manuelles Abrufen von Entitäten

Globale Abfrage von Instanzen

Citrix ADM fragt automatisch alle verwalteten Instanzen im Netzwerk ab, abhängig vom von dem von Ihnen konfigurierten Intervall. Obwohl das Standardabrufintervall 60 Minuten beträgt, können Sie das Intervall je nach Ihren Anforderungen festlegen, indem Sie zu " **Netzwerke** " > " **Netzwerkfunktionen** " > " **Einstellungen**" navigieren.

Manuelles Abrufen von Instanzen

Wenn Citrix ADM viele Entitäten verwaltet, dauert der Abrufzyklus länger, um den Bericht zu generieren, der zu einem leeren Bildschirm führen kann, oder das System zeigt möglicherweise noch frühere Daten an.

In Citrix ADM gibt es ein minimales Abrufintervall, wenn die automatische Abrufung nicht erfolgt. Wenn Sie eine neue Citrix ADC-Instanz hinzufügen oder eine Entität aktualisiert wird, erkennt Citrix ADM die neue Instanz oder die an einer Entität vorgenommenen Aktualisierungen erst, wenn die nächste Abfrage stattfindet. Und es gibt keine Möglichkeit, sofort eine Liste der virtuellen IP-Adressen für weitere Operationen zu erhalten. Sie müssen warten, bis der minimale Abrufintervall abgelaufen ist. Obwohl Sie eine manuelle Abfrage durchführen können, um neu hinzugefügte Instanzen zu ermitteln, führt dies dazu, dass das gesamte Citrix ADC Netzwerk abgefragt wird, wodurch das Netzwerk stark belastet wird. Anstatt das gesamte Netzwerk abzufragen Citrix ADM Sie jetzt nur ausgewählte Instanzen und Entitäten zu einem bestimmten Zeitpunkt abfragen.

Citrix ADM fragt verwaltete Instanzen automatisch ab, um Informationen zu festgelegten Zeiten an einem Tag zu sammeln. Die ausgewählte Abfrage reduziert die Aktualisierungszeit, die Citrix ADM benötigt, um den neuesten Status der Entitäten anzuzeigen, die an diese ausgewählten Instanzen gebunden sind.

So fragen Sie bestimmte Instanzen in Citrix ADM ab:

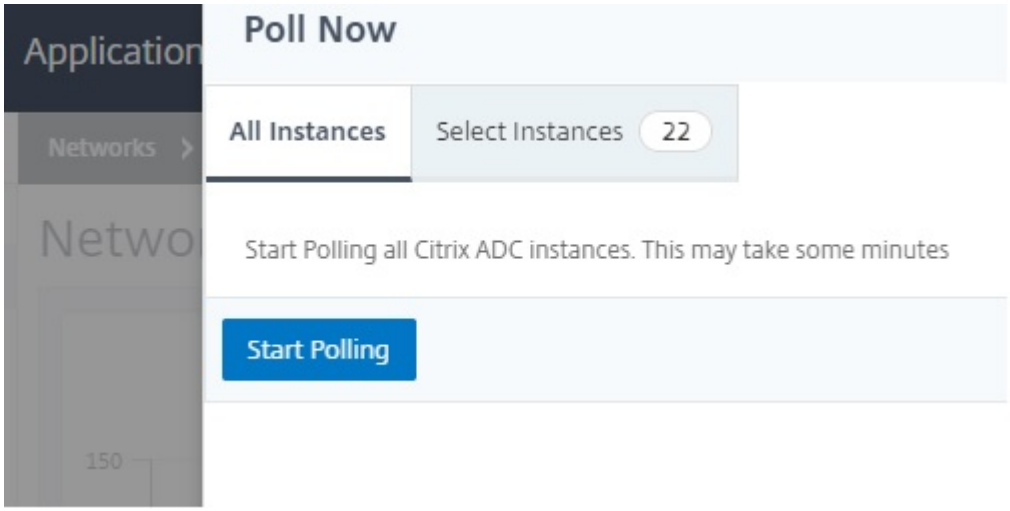
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Netzwerkfunktionen**.
2. Klicken Sie auf der Seite **Netzwerkfunktionen** oben rechts auf **Jetzt abfragen**.

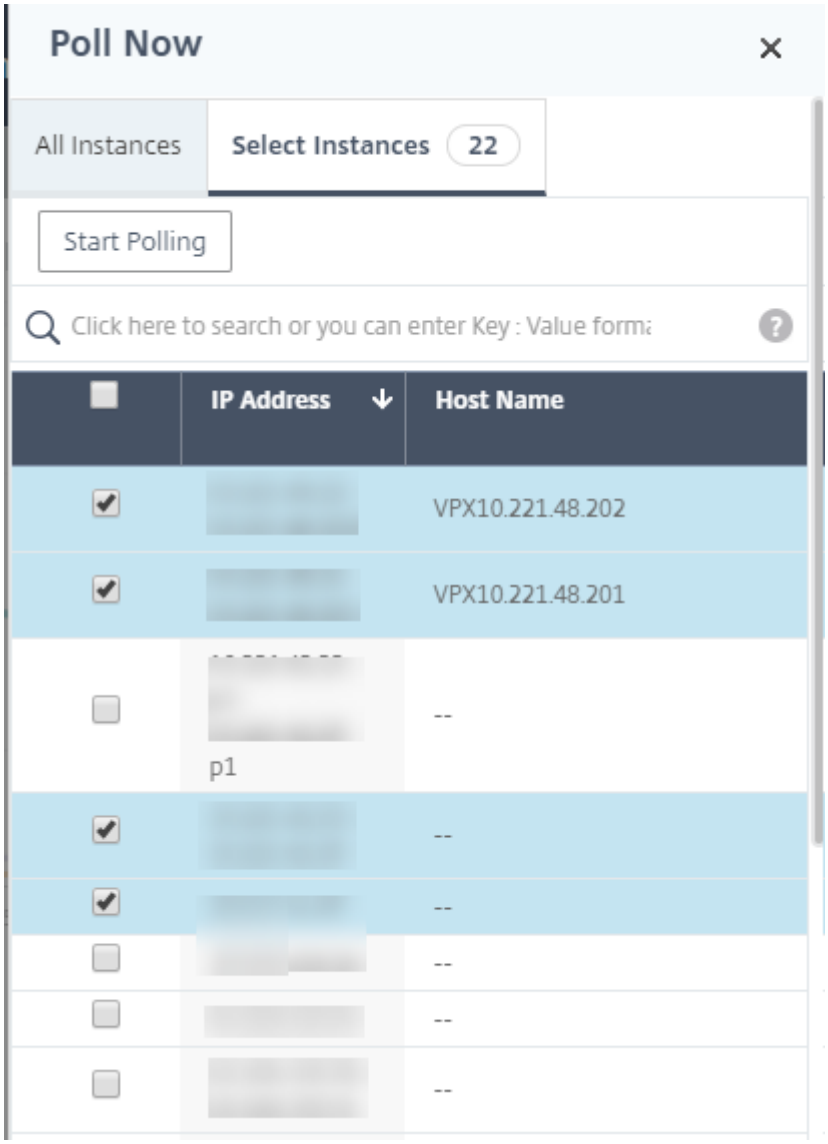
3. Auf der **Popupseite Jetzt** abfragen können Sie alle Citrix ADC-Instanzen im Netzwerk abfragen oder die ausgewählten Instanzen abfragen.

    a) Registerkarte**Alle Instanzen** — Klicken Sie auf **Abruf starten**, um alle Instanzen abzufragen.

    b) Registerkarte **Instanzen auswählen** - wählen Sie die Instanzen aus der Liste aus

4. Klicken Sie auf **Abruf starten**.





Citrix ADM initiiert die manuelle Abfrage und fügt alle Entitäten hinzu.

Manuelles Abrufen von Entitäten

Mit Citrix ADM können Sie auch nur wenige ausgewählte Entitäten abfragen, die an eine Instanz gebunden sind. Sie können diese Option beispielsweise verwenden, um den neuesten Status einer bestimmten Entität in einer Instanz zu kennen. In diesem Fall müssen Sie die Instanz nicht als Ganzes abfragen, um den Status einer aktualisierten Entität zu kennen. Wenn Sie eine Entität auswählen und abfragen, fragt Citrix ADM nur diese Entität ab und aktualisiert den Status in der Citrix ADM-GUI.

Betrachten Sie ein Beispiel dafür, dass ein virtueller Server **DOWN** ist. Der Status dieses virtuellen Servers hat sich möglicherweise in **UP**geändert, bevor die nächste automatische Abrufung stattfindet. Um den geänderten Status des virtuellen Servers anzuzeigen, sollten Sie möglicherweise nur diesen virtuellen Server abfragen, damit sofort der richtige Status auf der GUI angezeigt wird.

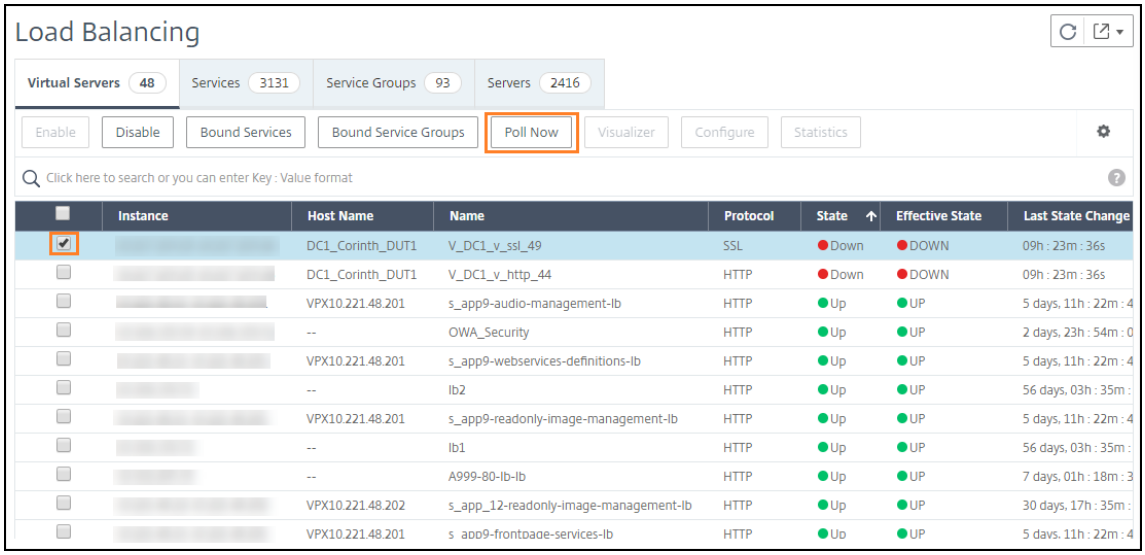
Sie können nun die folgenden Entitäten für alle Aktualisierungen in ihrem Status, Diensten, Dienstgruppen, Lastenausgleichsserver, virtuelle Server zur Cache-Reduzierung, virtuelle Content Switching-Server, virtuelle Authentifizierungsserver, virtuelle VPN-Server, virtuelle GSLB-Server und Anwendungsserver abfragen.

> **Hinweis:**
>
> Wenn Sie einen virtuellen Server abfragen, wird nur dieser virtuelle Server abgefragt. Die zugeordneten Entitäten wie Dienste, Dienstgruppen und Server werden nicht abgefragt. Wenn Sie alle zugeordneten Entitäten abfragen müssen, müssen Sie die Entitäten manuell abfragen oder die Instanz abfragen.

So fragen Sie bestimmte Entitäten in Citrix ADM ab:

Mit dieser Aufgabe können Sie beispielsweise virtuelle Server mit Lastenausgleich abfragen. Ebenso können Sie auch andere Netzwerkfunktions-Entitäten abfragen.

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Netzwerkfunktionen** > **Lastenausgleich** > **Virtuelle Server**.
2. Wählen Sie den virtuellen Server aus, der den Status als **DOWN**anzeigt, und klicken Sie dann auf **Jetzt abfragen**. Der Status des virtuellen Servers ändert sich jetzt in **UP**.



Verwalten einer Instanz aufheben

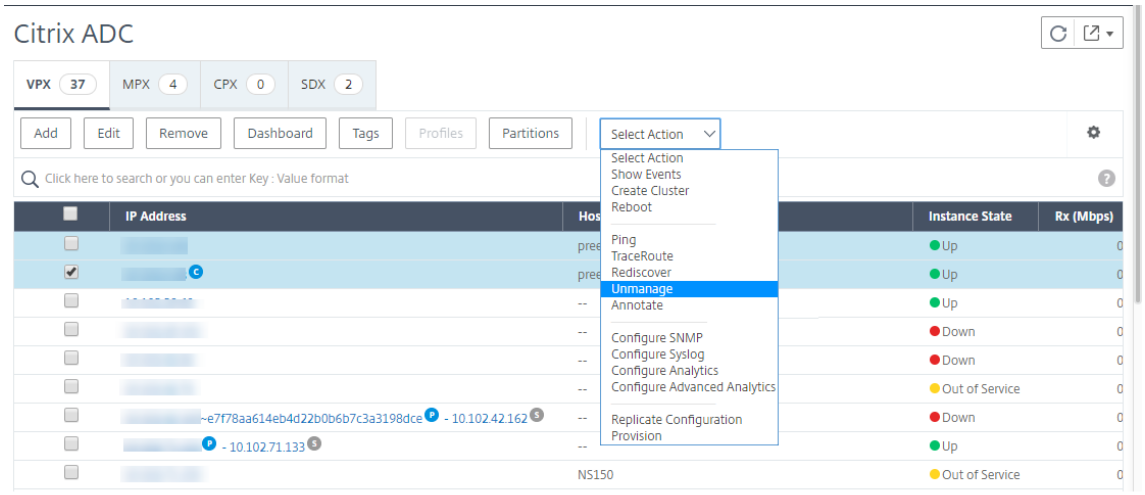
April 28, 2021

Wenn Sie den Informationsaustausch zwischen Citrix Application Delivery Management (Citrix ADM) und den Instanzen in Ihrem Netzwerk stoppen möchten, können Sie die Verwaltung der Instanzen

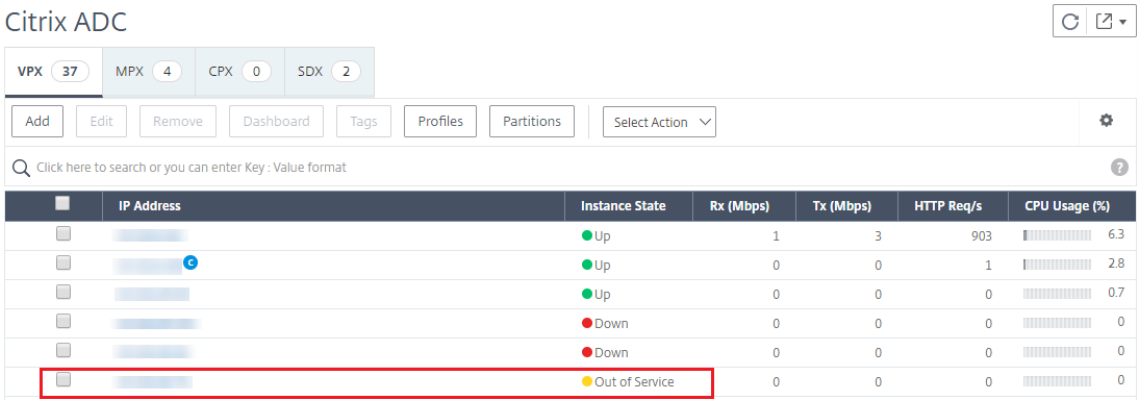
aufheben.

So heben Sie die Verwaltung einer Instanz auf:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Wählen Sie die Registerkarte ADC-Instanz (z. B. VPX).
3. Klicken Sie in der Liste der Instanzen mit der rechten Maustaste auf eine Instanz, und wählen Sie dann **Aufheben** aus, oder wählen Sie Instanz und aus der Liste **Aktion** die Option **Verwalten aufheben** aus.



Der Status der ausgewählten Instanz ändert sich in **Out of Service**.



Die Instanz wird nicht mehr von Citrix ADM verwaltet und tauscht keine Daten mehr mit Citrix ADM aus.

Verfolgen der Route zu einer Instanz

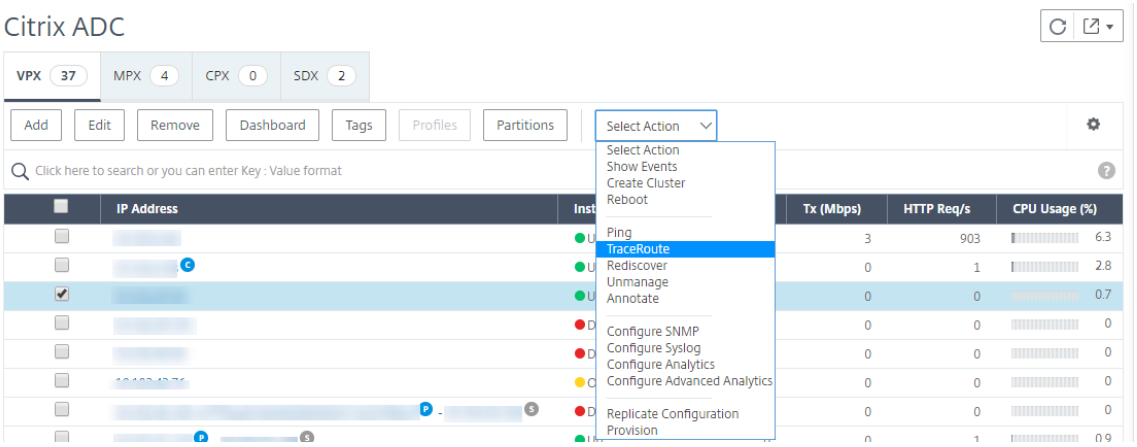
April 28, 2021

Indem Sie die Route eines Pakets von Citrix Application Delivery Management (Citrix ADM) zu einer Instanz verfolgen, finden Sie Informationen wie die Anzahl der Hops, die erforderlich sind, um die Instanz zu erreichen. Die Traceroute verfolgt den Pfad des Pakets von der Quelle zum Ziel. Es zeigt die Liste der Netzwerk-Hops zusammen mit dem Hostnamen und der IP-Adresse der einzelnen Entitäten in der Route an.

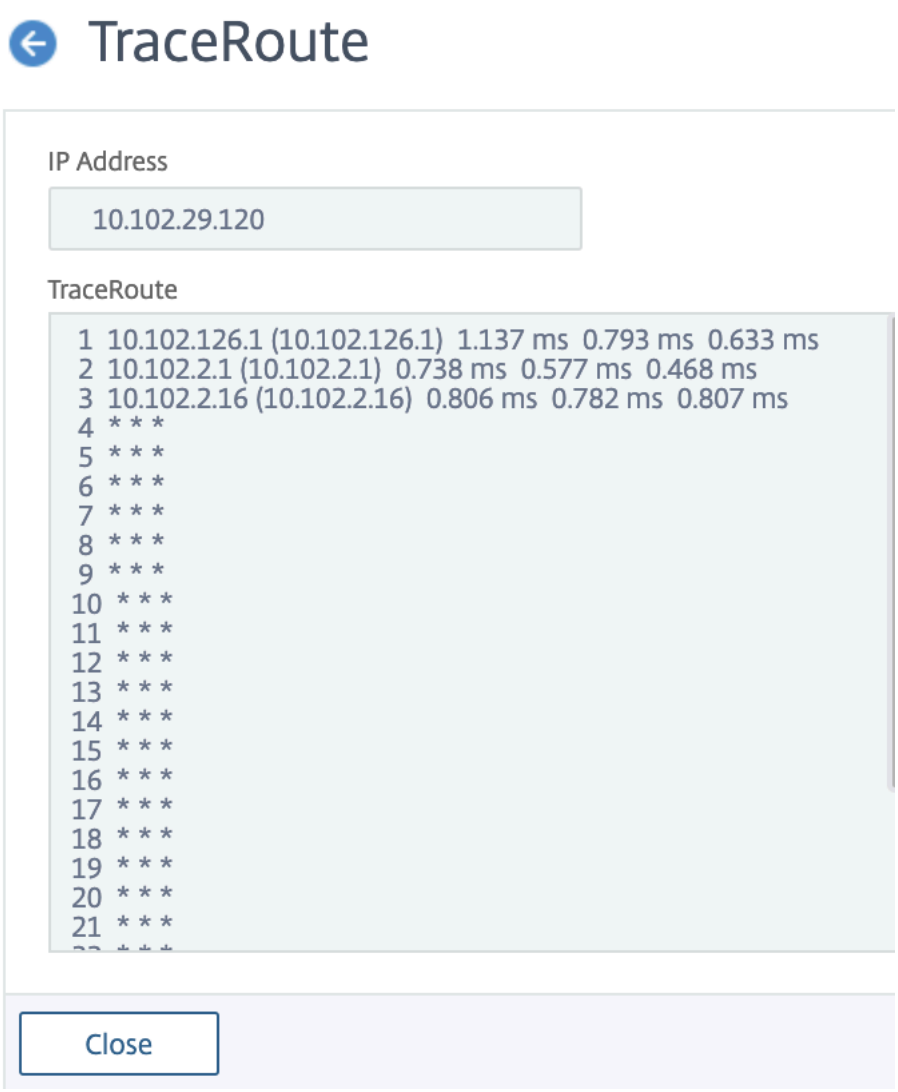
Traceroute erfasst auch die Zeit, die ein Paket für die Reise von einem Hop zum anderen nimmt. Wenn die Übertragung von Paketen unterbrochen wird, zeigt die Traceroute an, wo das Problem besteht.

So verfolgen Sie die Route einer Instanz:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Wählen Sie die Registerkarte ADC-Instanz (z. B. VPX).
3. Klicken Sie in der Liste der Instanzen mit der rechten Maustaste auf eine Instanz, und wählen Sie dann **TraceRoute**aus, oder wählen Sie die Instanz aus, und klicken Sie in der Liste **Aktion**auf **TraceRoute**.



Das Meldungsfeld TraceRoute zeigt die Route zur Instanz und die Zeit in Millisekunden an, die von jedem Hop verbraucht wird.



So ändern Sie das Citrix ADC MPX oder VPX Root-Kennwort

April 28, 2021

Gelegentlich müssen Sie das Stammkennwort der Citrix ADC Appliance aus Sicherheitsgründen oder der Einhaltung der Kennwortrotierungsrichtlinie ändern.

In diesem Dokument werden die Schritte beschrieben, die erforderlich sind, um das Root-Kennwort der Citrix ADC MPX- und VPX-Appliances zu ändern, die über Citrix ADM Cloud verwaltet werden.

Wenn Sie das ADC-Kennwort ändern, müssen Sie das ADM-Administratorprofil ändern, das dem ADC zugeordnet ist. Ein ADM-Administratorprofil verwaltet die ADC-Anmeldeinformationen für die REST-API-, SSH-, SCP- oder SNMP-basierte Kommunikation mit der ADC-Appliance. Über Administratorprofile verwaltet Citrix ADM Citrix ADC MPX- und VPX-Appliances.

Ändern des Kennworts mit der Funktion Konfigurationsaufträge

Mithilfe der Citrix ADM Konfigurationsaufträge können Sie den Prozess der wiederholten Kennwortänderung vereinfachen und die Änderungen auf die Citrix ADC Appliances anwenden, ohne auf die einzelnen Instanzen zuzugreifen.

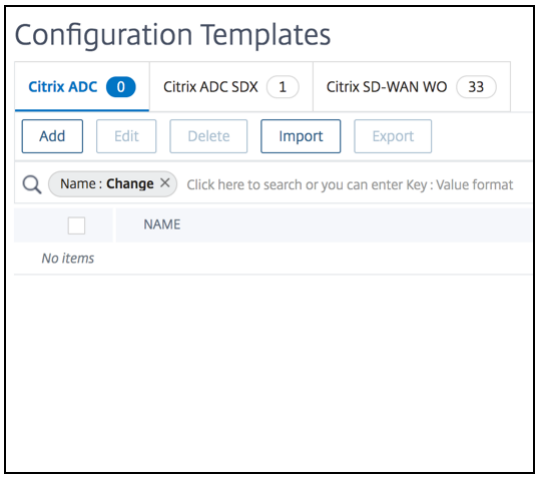
Gehen Sie folgendermaßen vor, um das Kennwort zu ändern:

- Schritt 1. Erstellen Sie eine Konfigurationsvorlage.
- Schritt 2. Erstellen Sie einen Konfigurationsauftrag.
- Schritt 3. Erstellen Sie ein Admin-Profil und ändern Sie es.

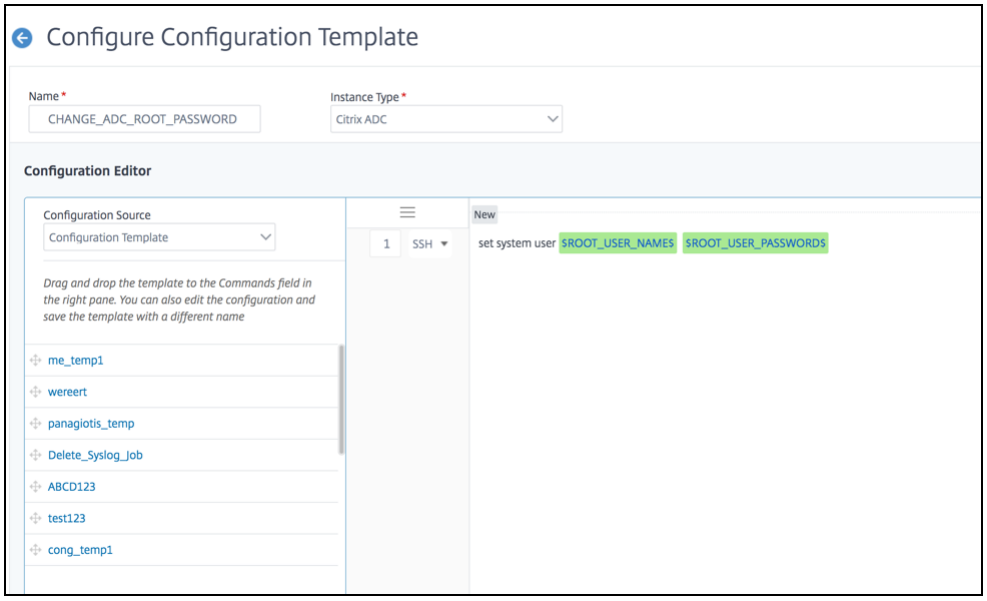
> Hinweis: Wenn die ADC-Appliances auch von anderen Tools verwaltet werden, müssen Sie die Anmeldeinformationen für diese Tools ebenfalls ändern.

Erstellen einer Konfigurationsvorlage

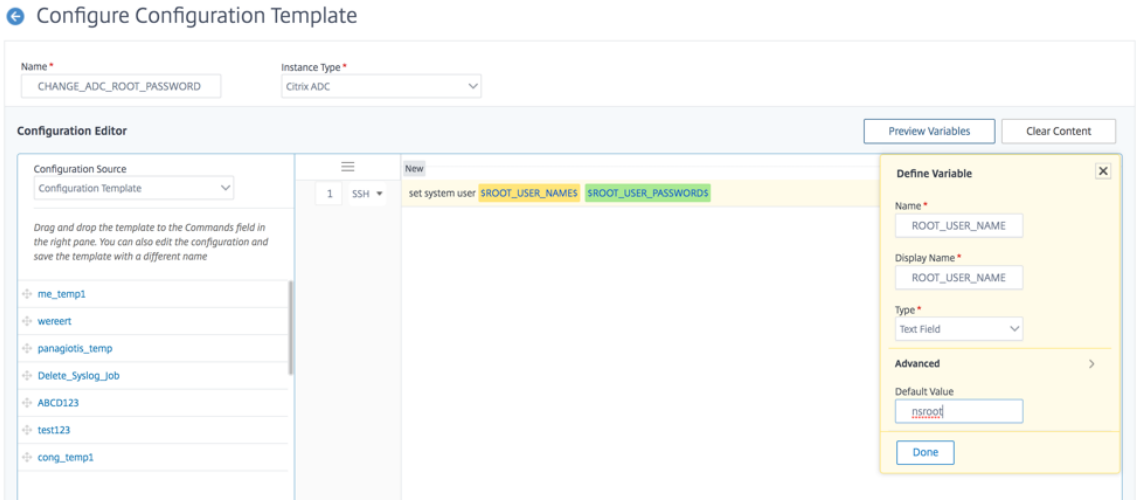
1. Navigieren Sie über die ADM-Benutzeroberfläche zu **Netzwerke > Konfigurationsaufträge > Konfigurationsvorlagen**.



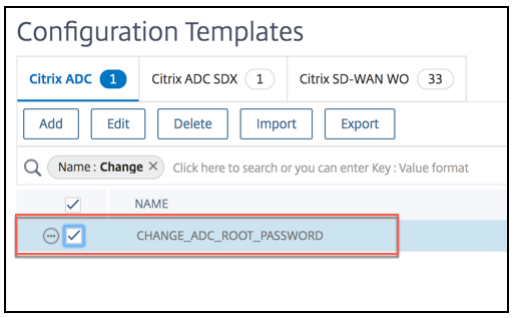
2. Wählen Sie **Hinzufügen**. Erstellen Sie eine Konfigurationsvorlage mit, indem Sie den SSH-Befehl eingeben`set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$`.



3. Wählen Sie die Variable $ROOT_USER_NAME$ aus, und wählen Sie **Textfeld als Typ**aus.
4. Geben Sie optional den Standardwert für den Root-Benutzernamen an. Wählen Sie **Fertig**, um die Variableneinstellungen zu speichern.

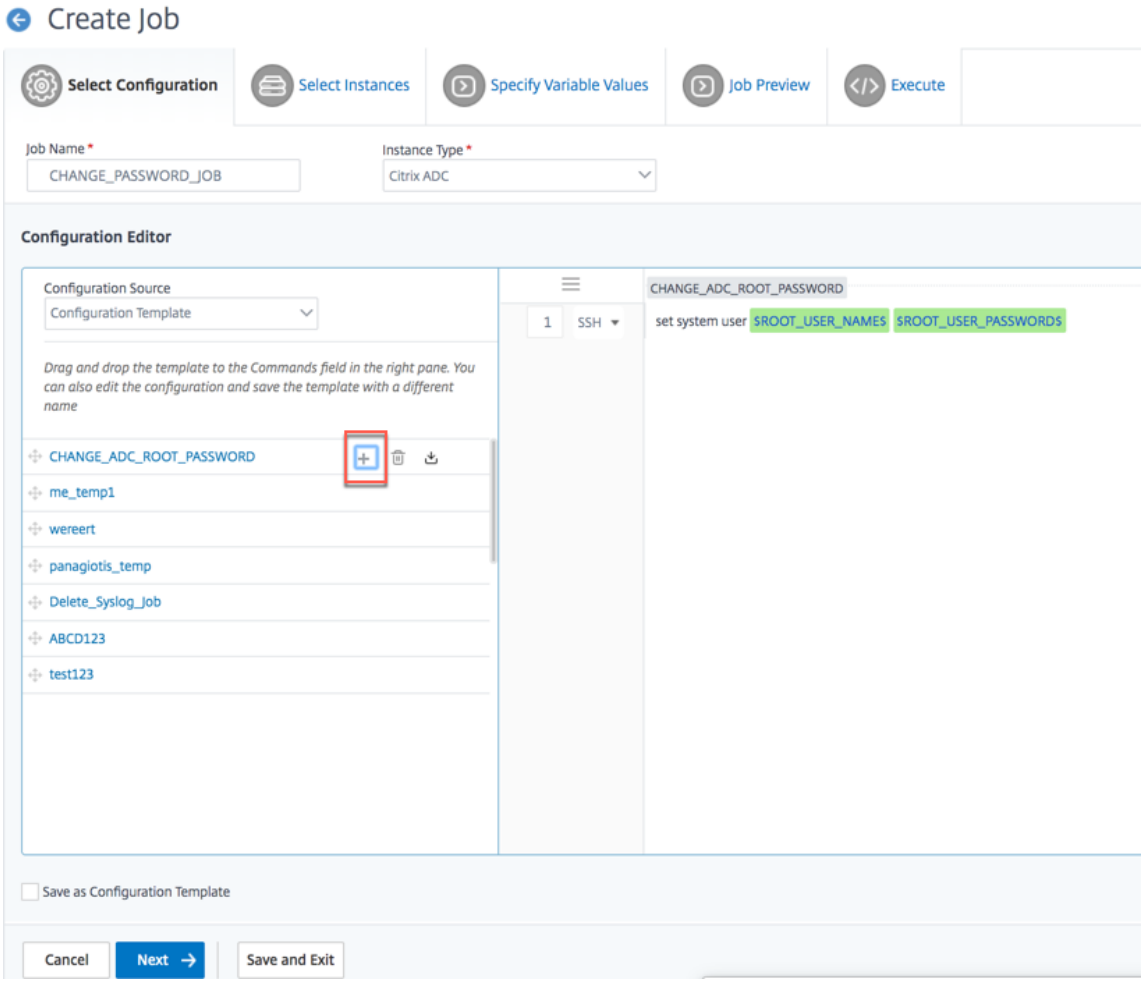


5. Wählen Sie die Variable $ROOT_USER_PASSWORD$ und wählen Sie **Kennwortfeld als Typ**aus. Wählen Sie **Fertig**, um die Variableneinstellungen zu speichern.
6. Wählen Sie **OK**, um die Konfigurationsvorlage zu speichern.
7. Die neue Konfigurationsvorlage wird unter **Konfigurationsvorlagen** angezeigt.

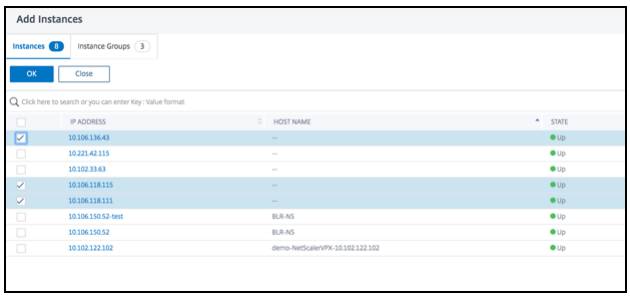


Erstellen eines Konfigurationsauftrags

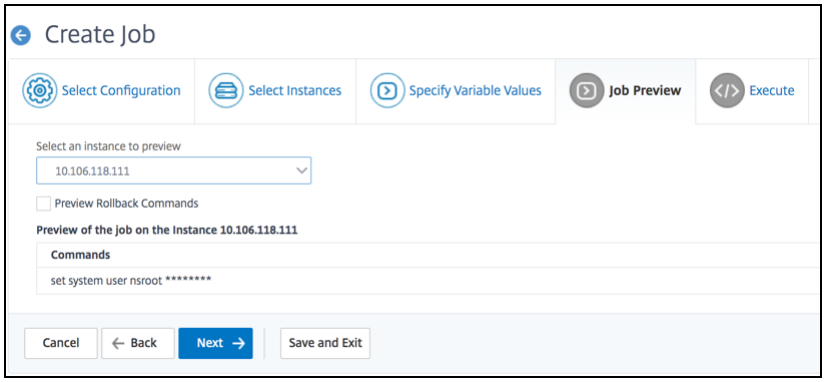
1. Navigieren Sie über die ADM-Benutzeroberfläche zu **Netzwerke > Konfigurationsaufträge**.
2. Wählen Sie **Job erstellen** und klicken Sie auf das Symbol + der neuen Konfigurationsvorlage. Klicken Sie auf **Weiter**.



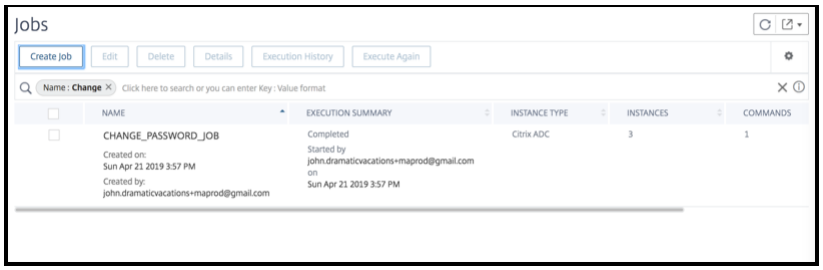
3. Wählen Sie die ADC-Instanz oder Instanzen aus, für die das Kennwort geändert werden muss.



4. Wählen Sie im Bereich **Instanzen auswählen** die Instanzen aus, und klicken Sie auf **Weiter**.
5. Geben Sie im Bereich **Variablenwerte angeben** Werte für Benutzernamen und Kennwort an, und klicken Sie auf **Weiter**.
6. Überprüfen Sie unter **Auftragsvorschau** die tatsächlichen CLI-Befehle, die der ADM auf den ADC-Instanzen ausgeführt wird. Wenn die Vorschau gut aussieht, klicken Sie auf **Weiter**.



7. Im Bereich **Ausführen** haben Sie die Wahl, den Job sofort auszuführen oder ihn für einen späteren Zeitpunkt zu planen. Sie können den Job auch parallel auf allen ausgewählten Instanzen ausführen oder nacheinander ausführen. Wählen Sie Fertig stellen, nachdem Sie die Ausführungsdetails angegeben haben.
8. Konfigurationsauftrag zeigt an, ob die Ausführung erfolgreich war oder fehlgeschlagen ist.

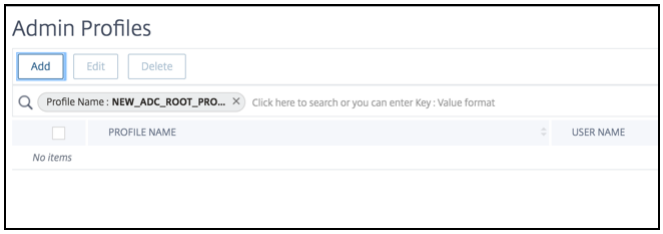


9. Wählen Sie den **Auftrag** aus, und klicken Sie auf **Details**. Die Ausführungsdetails zeigen den Status auf individueller Instanzebene an.

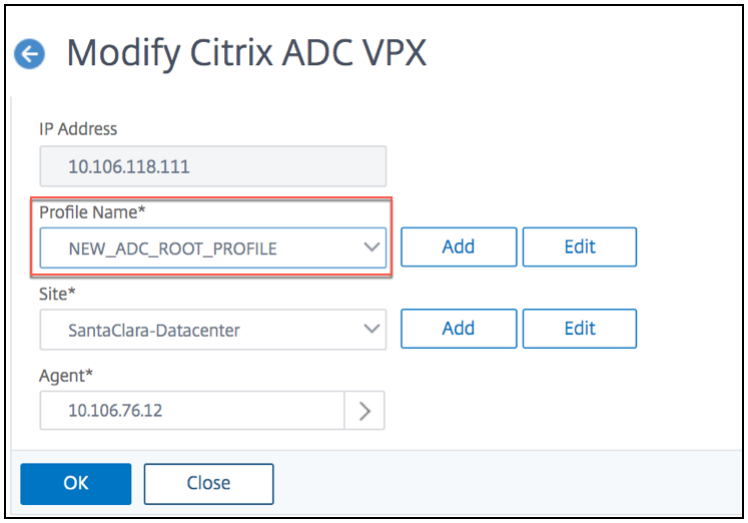
Ändern des Administratorprofils

Nachdem Sie die ADC-Kennwörter geändert haben, müssen Sie die Administratorprofile der Instanzen hinzufügen und ändern. Führen Sie die folgenden Schritte aus:

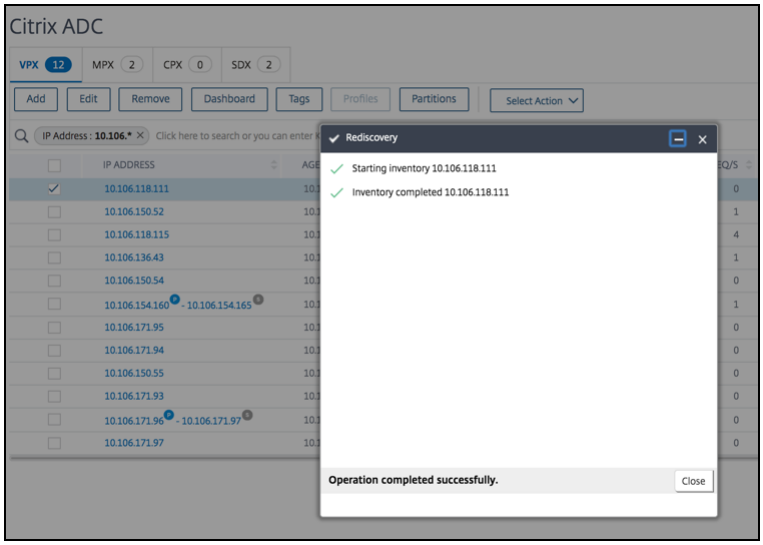
1. Navigieren Sie zu **Netzwerke > Instanzen > Citrix ADC**.
2. Klicken Sie auf **Profile**, um alle Admin-Profile anzuzeigen.
3. Wählen Sie **Hinzufügen** aus, um ein Administratorprofil zu erstellen und neue Citrix ADC Anmeldeinformationen bereitzustellen.



4. Das neu erstellte Profil wird unter **Admin-Profile** angezeigt.
5. Wechseln Sie zu **Netzwerk > Instanzen > Citrix ADC**. Wählen Sie die Citrix ADC-Instanz aus, für die das Kennwort geändert wurde, und wählen Sie **Bearbeiten**aus.
6. Wählen Sie den neu erstellten Profilnamen aus und klicken Sie auf **OK**.



7. Wählen Sie die Instanz erneut aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Wiedererkennen**aus.



Sie haben das Kennwort erfolgreich geändert.

Hinweise zum Ändern des Kennworts einer SDX-Appliance finden Sie unter Ändern eines Citrix ADC SDX-Stammkennworts.

Ändern eines Citrix ADC SDX-Stammkennworts

April 28, 2021

Gelegentlich müssen Sie das Stammkennwort der Citrix ADC Appliance aus Sicherheitsgründen oder der Einhaltung der Kennwortrotierungsrichtlinie ändern.

In diesem Dokument werden die Schritte beschrieben, die erforderlich sind, um das Stammkennwort einer über die Citrix ADM Cloud verwalteten Citrix ADC SDX-Appliance zu ändern.

Wenn Sie das ADC-Kennwort ändern, müssen Sie das ADM-Administratorprofil ändern, das dem ADC zugeordnet ist. Ein ADM-Administratorprofil verwaltet die ADC-Anmeldeinformationen für die REST-API-, SSH-, SCP- oder SNMP-basierte Kommunikation mit der ADC-Appliance. Über Administratorprofile verwaltet Citrix ADM Citrix ADC SDX-Appliances.

Kennwort ändern

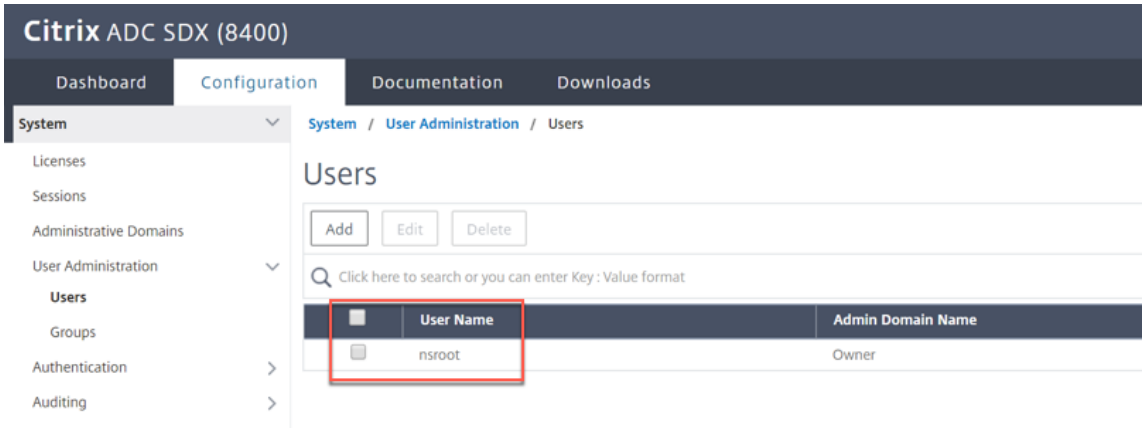
Gehen Sie folgendermaßen vor, um das Kennwort zu ändern:

- Schritt 1. Ändern Sie das SDX-Kennwort über die SDX Management Service-GUI.
- Schritt 2. Ändern Sie das ADM-Administratorprofil, das dem SDX zugeordnet ist.

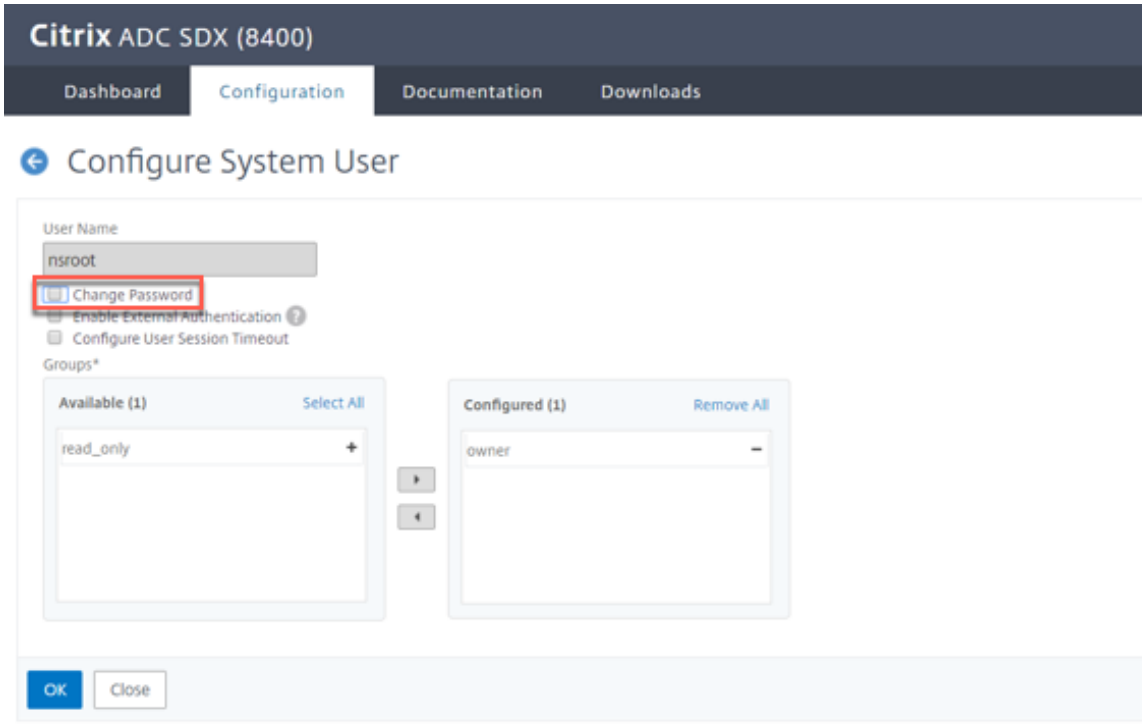
> Hinweis: Wenn die SDX-Appliance auch von anderen Tools verwaltet wird, müssen Sie die Anmeldeinformationen für diese Tools ebenfalls ändern.

Ändern des SDX-Kennworts über die SDX Management Service-GUI

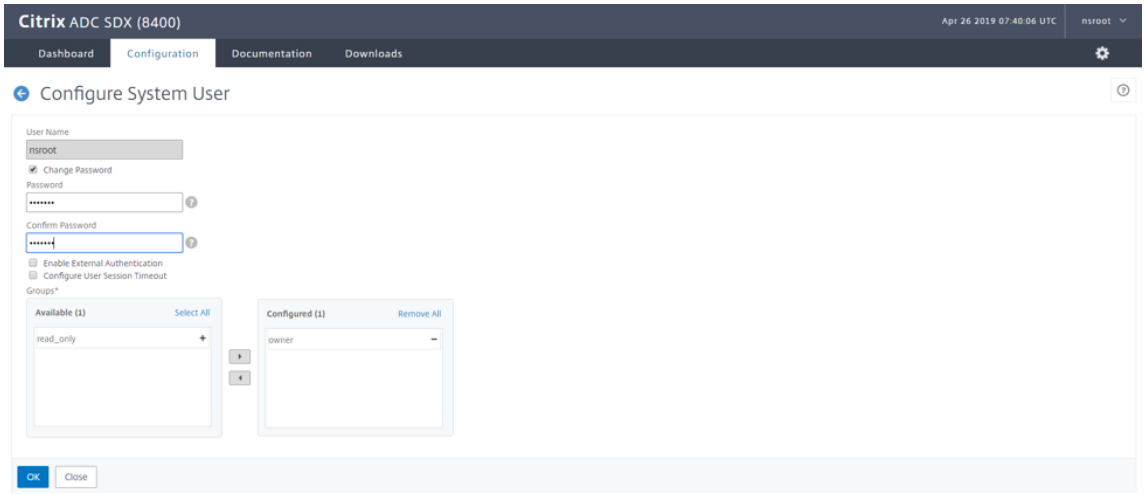
1. Navigieren Sie im SDX Management Service zu **System > Benutzerverwaltung > Benutzer**.
2. Wählen Sie den Benutzernamen aus, für den Sie das Kennwort ändern möchten, und klicken Sie auf **Bearbeiten**.



3. Wählen Sie **Kennwort ändern**aus.



4. Geben Sie ein neues Kennwort ein und klicken Sie auf **OK**.

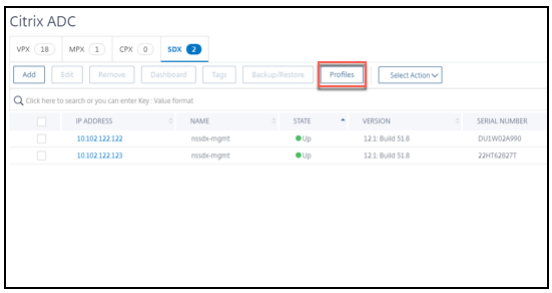


5. Das SDX-Kennwort wurde geändert

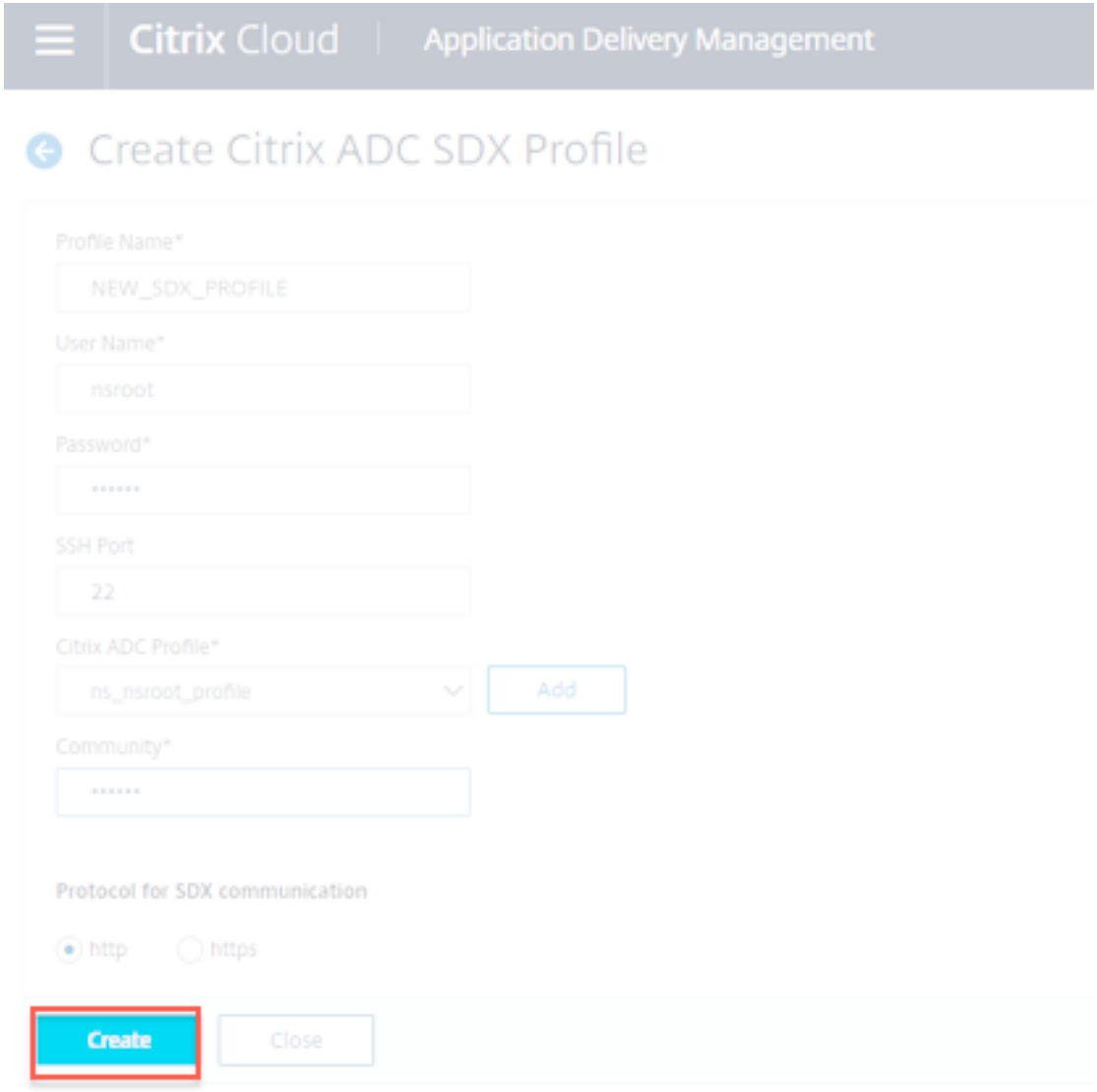
Ändern des ADM-Administratorprofils

Nachdem Sie die SDX-Kennwörter geändert haben, müssen Sie die Administratorprofile der Instanzen ändern. Führen Sie die folgenden Schritte aus:

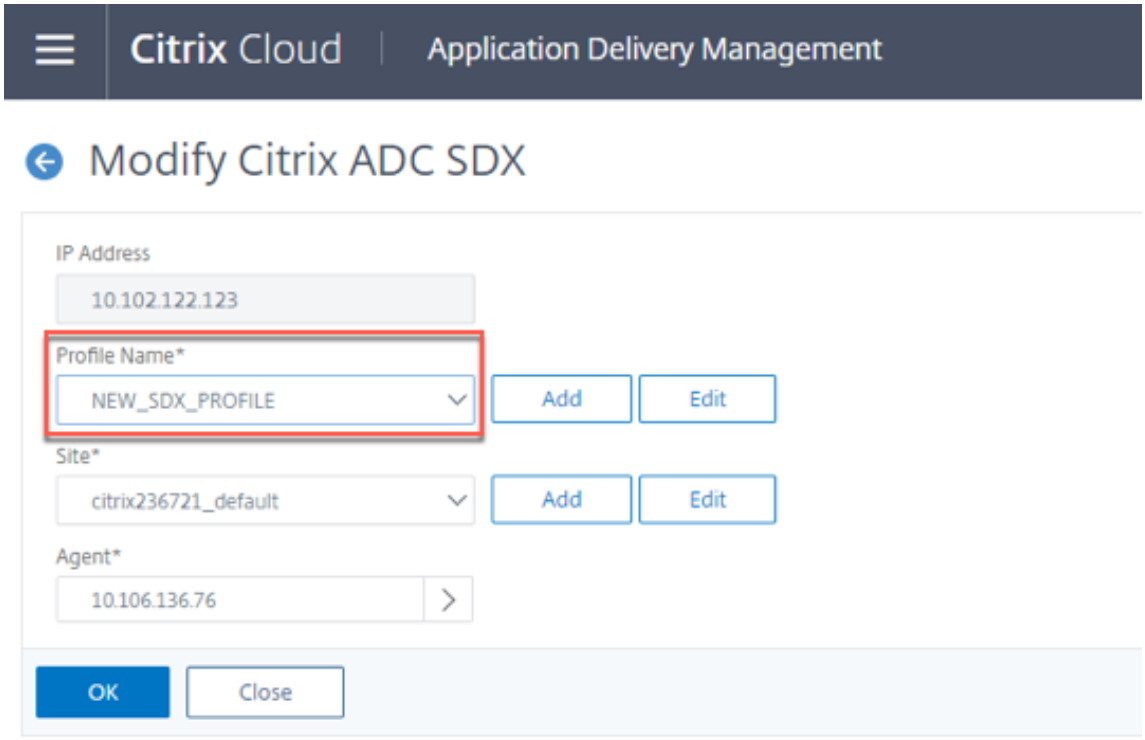
1. Navigieren Sie zu **Netzwerke > Instanzen Dashboard > Citrix ADC > SDX**.
2. Wählen Sie **Profile** aus, um alle Admin-Profile anzuzeigen.



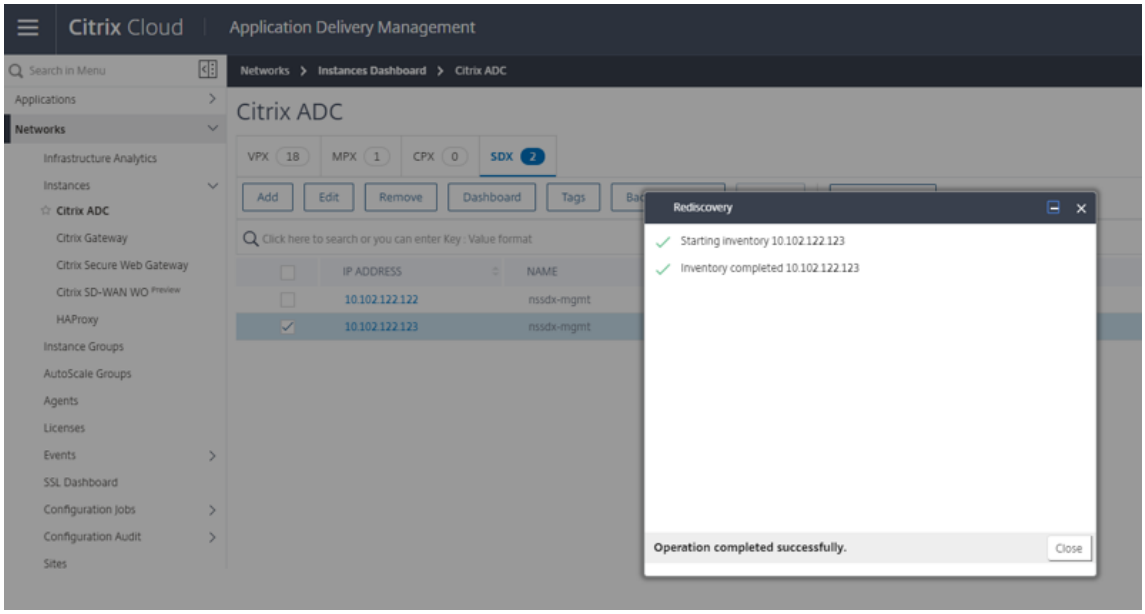
3. Wählen Sie **Hinzufügen** aus, um ein Admin-Profil zu erstellen.
4. Geben Sie neue Citrix ADC Anmeldeinformationen ein, und klicken Sie auf **Erstellen**.



5. Das neu erstellte Profil wird unter **Admin-Profile** angezeigt.
6. Gehen Sie zu **Netzwerk > Instanzen > Citrix ADC > SDX**. Wählen Sie die Instanz aus, für die das Kennwort geändert wurde, und klicken Sie auf **Bearbeiten**.
7. Wählen Sie den neu erstellten Profilnamen aus und klicken Sie auf **OK**.



8. Wählen Sie die Instanz erneut aus, klicken Sie mit der rechten Maustaste und klicken Sie auf **Wiederermitteln**.



Sie haben das Kennwort erfolgreich geändert.

Hinweise zum Ändern des Kennworts einer SDX-Appliance finden Sie unter Ändern eines Citrix ADC MPX- oder VPX-Stammkennworts.

Ereignisse

April 28, 2021

Wenn die IP-Adresse einer Citrix Application Delivery Controller (Citrix ADC) -Instanz zu Citrix Application Delivery Management (Citrix ADM) hinzugefügt wird, sendet Citrix ADM einen NITRO -Aufruf und fügt sich implizit als Trap-Ziel für die Instanz hinzu, um ihre Traps oder Ereignisse zu empfangen.

Ereignisse stellen Ereignisse oder Fehler in einer verwalteten Citrix ADC-Instanz dar. Wenn beispielsweise ein Systemfehler oder eine Änderung der Konfiguration vorliegt, wird ein Ereignis auf dem Citrix ADM -Server generiert und aufgezeichnet. In Citrix ADM empfangene Ereignisse werden auf der Seite “Ereignisübersicht” (**Netzwerke** > **Ereignisse**) angezeigt, und alle aktiven Ereignisse werden auf der Seite “ Ereignismeldungen” (**Netzwerke** > **Ereignisse** > **Ereignismeldungen**) angezeigt.

Citrix ADM überprüft auch die auf Instanzen generierten Ereignisse, um Alarme mit unterschiedlichen Schweregraden zu bilden, und zeigt sie als Nachrichten an, von denen einige möglicherweise sofortige Aufmerksamkeit erfordern. Beispielsweise kann ein Systemausfall als Schweregrad des “kritischen” Ereignisses eingestuft und sofort behoben werden.

Sie können Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Regeln erleichtern die Überwachung verschiedener Ereignisse, die in Ihrer Citrix ADC-Infrastruktur generiert werden.

Sie können eine Reihe von Ereignissen filtern, indem Sie Regeln mit bestimmten Bedingungen konfigurieren und den Regeln Aktionen zuweisen. Wenn die generierten Ereignisse die Filterkriterien in der Regel erfüllen, wird die mit der Regel verknüpfte Aktion ausgeführt. Die Bedingungen für die Erstellung von Filtern sind: Schweregrad, Citrix ADC-Instanzen, Kategorie, Fehlerobjekte, Konfigurationsbefehle und Meldungen.

Sie können auch sicherstellen, dass für ein bestimmtes Zeitintervall für ein Ereignis mehrere Benachrichtigungen ausgelöst werden, bis das Ereignis gelöscht wird. Als zusätzliche Maßnahme möchten Sie Ihre E-Mail möglicherweise mit einer bestimmten Betreffzeile, einer Benutzernachricht und einer Anfügung anpassen.

Ereignis-Dashboard verwenden

April 28, 2021

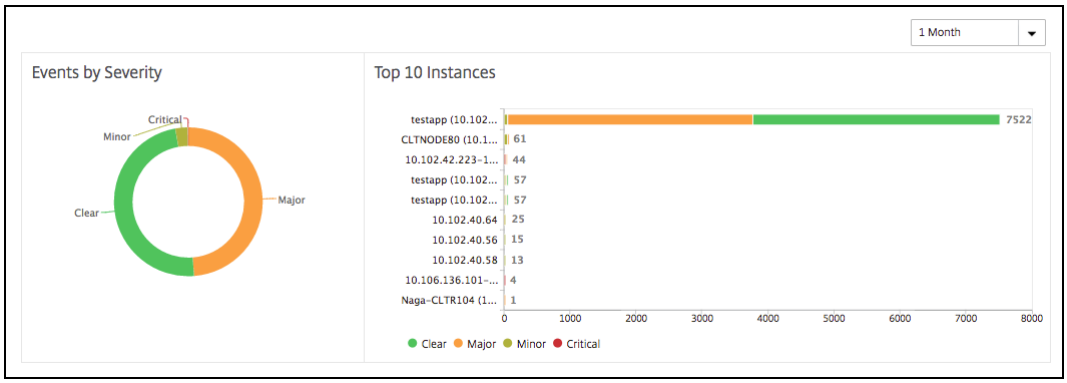
Als Netzwerkadministrator können Sie Details wie Konfigurationsänderungen, Anmeldebedingungen, Hardwarefehler, Schwellenverletzungen und Entitätsstatusänderungen auf Ihren Citrix Application Delivery Controller Instanzen (Citrix ADC) sowie Ereignisse und deren Schweregrad auf bestimmten Instanzen anzeigen. Sie können das Ereignis-Dashboard von Citrix Application Delivery

Management (Citrix ADM) verwenden, um Berichte anzuzeigen, die für Details zum Schweregrad kritischer Ereignisse in allen Citrix ADC-Instanzen generiert wurden.

So zeigen Sie die Details im Ereignis-Dashboard an:

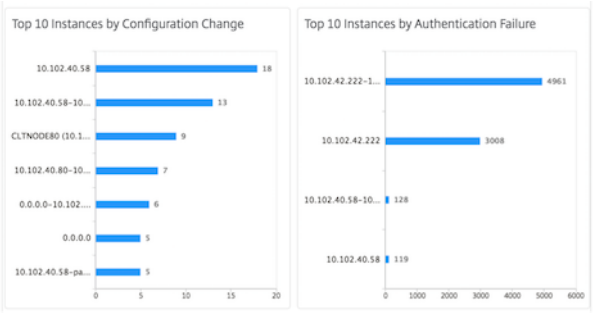
Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Berichte**.

Das Diagramm Top 10 Geräte auf dem Dashboard zeigt einen Bericht der Top 10 Instanzen anhand der Anzahl der auf ihnen erzeugten Ereignisse an. Sie können auf eine Instanz im Diagramm klicken, um weitere Details zum Schweregrad des Ereignisses anzuzeigen.

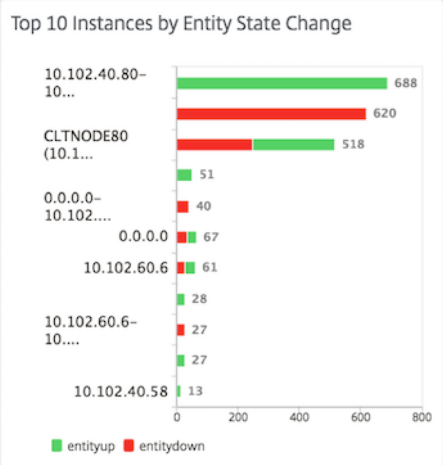


Sie können weitere Details anzeigen, indem Sie zum Citrix ADC-Instanztyp navigieren (**Netzwerke** > **Ereignisse** > **Berichte** > **Citrix ADC/Citrix ADC SDX/Citrix ADC SD-WAN WO**), um Folgendes anzuzeigen:

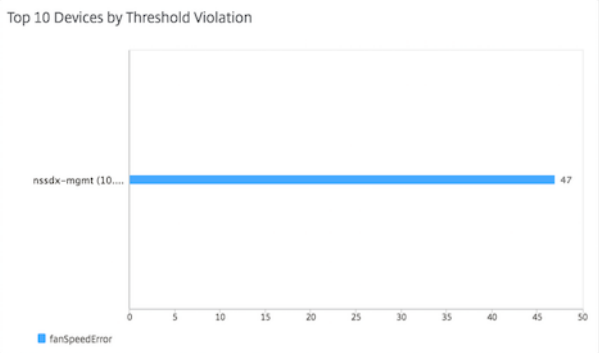
- Top 10 Geräte nach Hardwarefehler
- Top 10 Geräte nach Konfigurationsänderung
- Top 10 Geräte durch Authentifizierungsfehler



- Top 10 Geräte nach Entitätsstatusänderungen



- Top 10 Geräte nach Schwellenverletzung



So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Ereignisalter für Ereignisse festlegen

April 28, 2021

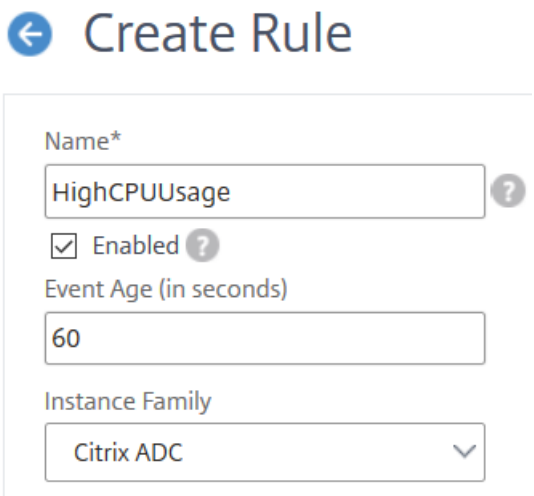
Sie können die Ereignisalteroption einstellen, um das Zeitintervall (in Sekunden) anzugeben. Citrix ADM überwacht die Appliances bis zur festgelegten Dauer und generiert nur dann ein Ereignis, wenn das Ereignisalter die festgelegte Dauer überschreitet.

> Hinweis:
>
> Der Mindestwert für das Ereignisalter beträgt 60 Sekunden. Wenn Sie das Feld **Ereignisalter** leer lassen, wird die Ereignisregel unmittelbar nach dem Auftreten des Ereignisses angewendet.

Angenommen, Sie möchten verschiedene ADC-Appliances verwalten und per E-Mail benachrichtigt werden, wenn ein virtueller Server 60 Sekunden oder länger ausfällt. Sie können eine Ereignisregel mit den erforderlichen Filtern erstellen und das Ereignisalter der Regel auf 60 Sekunden festlegen. Wenn ein virtueller Server dann 60 oder mehr Sekunden lang ausfällt, erhalten Sie eine E-Mail-Benachrichtigung mit Details wie Entitätsname, Statusänderung und Uhrzeit.

So legen Sie das Ereignisalter in Citrix ADM fest:

1. Navigieren Sie im Citrix ADM zu **Netzwerke** > **Ereignisse** > **Regeln**, und klicken Sie auf **Hinzufügen**.
2. Legen Sie auf der Seite **Regel erstellen** die Regelparameter fest.
3. Geben Sie das Ereignisalter in Sekunden an.



Planen eines Ereignisfilters

April 28, 2021

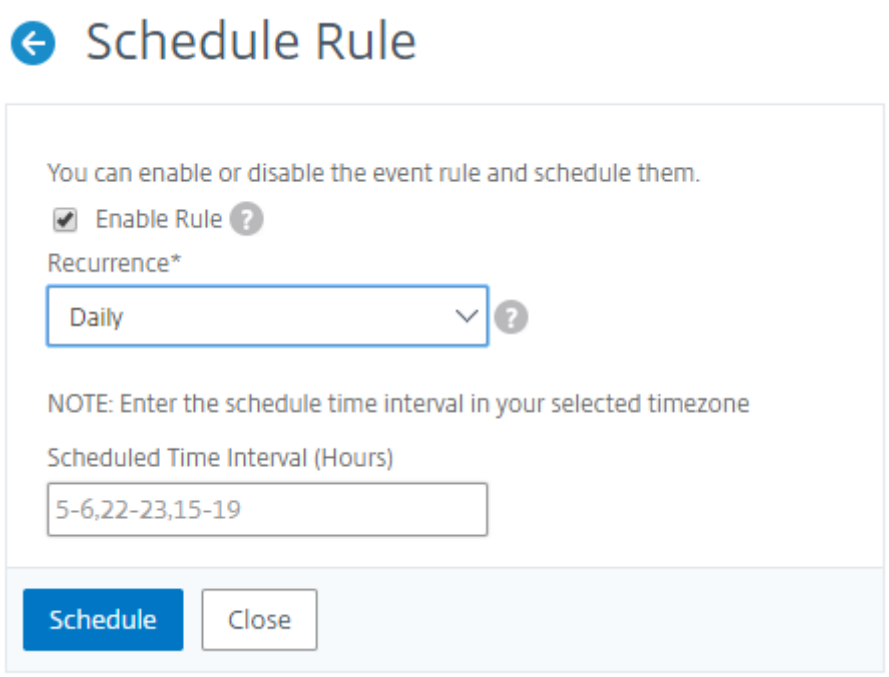
Wenn Sie nach dem Erstellen eines Filters für Ihre Regel nicht möchten, dass Citrix Application Delivery Management (Citrix ADM) jedes Mal eine Benachrichtigung sendet, wenn das generierte Ereignis die Filterkriterien erfüllt, können Sie den Filter so planen, dass er nur in bestimmten Zeitintervallen ausgelöst wird, z. B. täglich, wöchentlich oder monatlich.

Wenn Sie beispielsweise eine Systemwartungsaktivität für verschiedene Anwendungen auf Ihren Instanzen zu unterschiedlichen Zeiten geplant haben, können die Instanzen mehrere Alarme generieren.

Wenn Sie einen Filter für diese Alarme konfiguriert und E-Mail-Benachrichtigungen für diese Filter aktiviert haben, sendet der Server viele E-Mail-Benachrichtigungen, wenn Citrix ADM diese Traps erhält. Wenn Sie möchten, dass der Server diese E-Mail-Benachrichtigungen nur während eines bestimmten Zeitraums sendet, können Sie dies tun, indem Sie einen Filter planen.

So planen Sie einen Filter mit Citrix ADM:

1. Navigieren Sie im Citrix ADM zu **Netzwerke** > **Ereignisse** > **Regeln**.
2. Wählen Sie die Regel aus, für die Sie einen Filter planen möchten, und klicken Sie auf **Zeitplan anzeigen**.
3. Klicken Sie auf der Seite **Geplante Regel** auf **Zeitplan**, und geben Sie die folgenden Parameter an:
    - **Regel aktivieren** — Aktivieren Sie dieses Kontrollkästchen, um die Regel für geplante Ereignisse zu aktivieren.
    - **Wiederholung** - Intervall, in dem die Regel geplant werden soll.
    - **Geplantes Zeitintervall (Stunden)** — Stunden, zu denen die Regel geplant werden soll (verwenden Sie das 24-Stunden-Format).
4. Klicken Sie auf **Zeitplan**.



Festlegen von wiederholten E-Mail-Benachrichtigungen für Ereignisse

April 28, 2021

Um sicherzustellen, dass alle kritischen Ereignisse behoben werden und keine wichtigen E-Mail-Benachrichtigungen übersehen werden, können Sie sich entscheiden, wiederholte E-Mail-Benachrichtigungen für Ereignisregeln zu senden, die die von Ihnen ausgewählten Kriterien erfüllen. Wenn Sie beispielsweise eine Ereignisregel für Instanzen erstellt haben, die Datenträgerfehler verursachen, und Sie benachrichtigt werden möchten, bis das Problem behoben ist, können Sie sich dafür entscheiden, wiederholte E-Mail-Benachrichtigungen zu diesen Ereignissen zu erhalten.

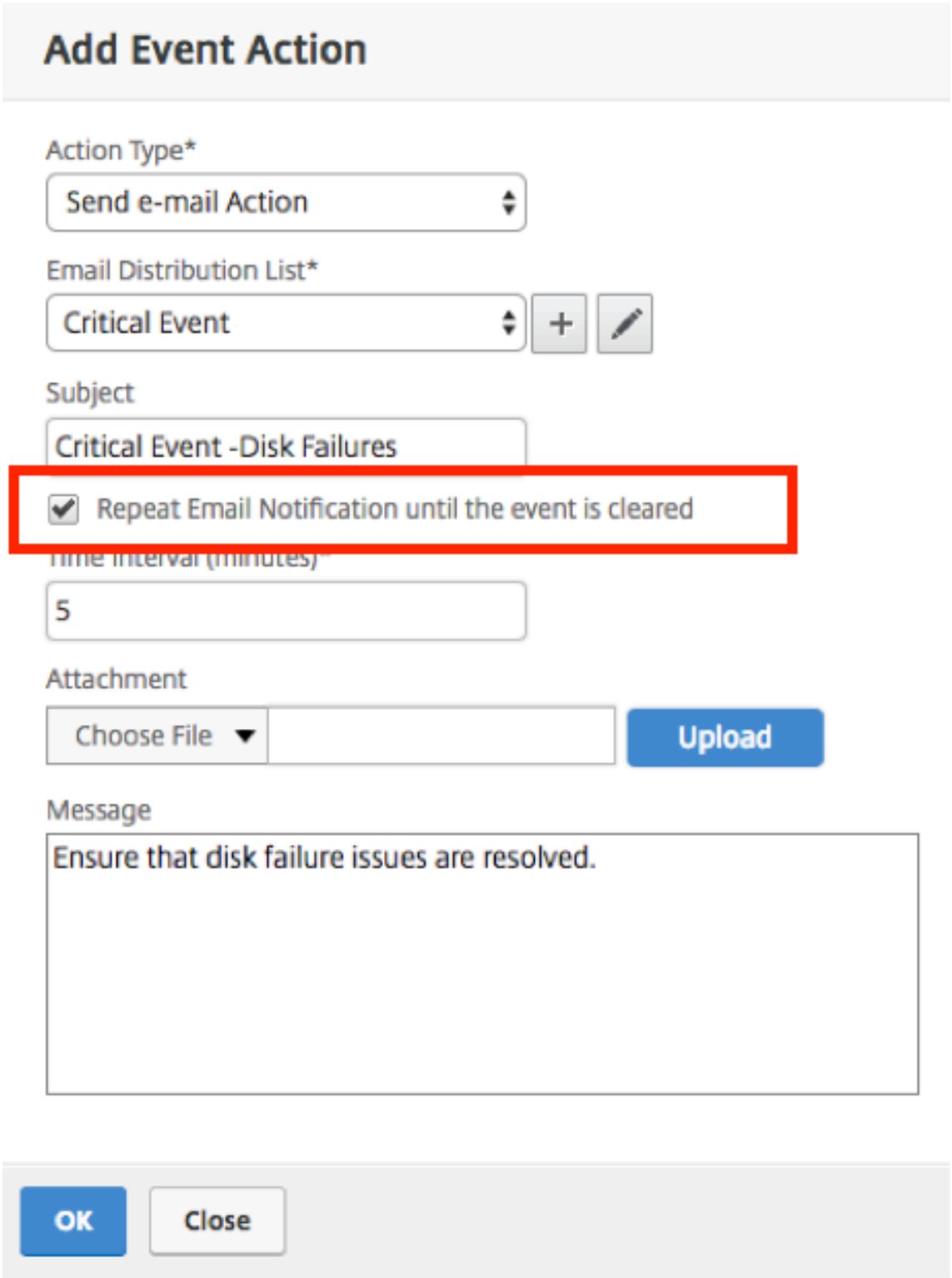
Diese E-Mail-Benachrichtigungen werden wiederholt in vordefinierten Intervallen gesendet, bis der Empfänger bestätigt, dass die Benachrichtigung angezeigt wurde oder die Ereignisregel gelöscht wurde.

> **Hinweis**
>
> Ereignisse können nur automatisch gelöscht werden, wenn ein äquivalenter Clear Trapsatz vorhanden ist und von Ihrer Citrix ADC-Instanz gesendet wird.
>
> Um ein Ereignis manuell zu löschen, können Sie Folgendes tun:
>
> - Navigieren Sie zu **Netzwerke > Ereignisse > Ereignisübersicht**, wählen Sie **Kategorie**aus, wählen Sie eine Veranstaltung in der Kategorie aus und klicken Sie auf **Löschen**.

> • Oder navigieren Sie zu **Netzwerke > Ereignisse > Ereignismeldungen**. Wählen Sie einen Instanztyp aus, wählen Sie dann ein Ereignis aus dem folgenden Raster aus und klicken Sie auf **Löschen**.

So legen Sie wiederholte E-Mail-Benachrichtigungen von Citrix ADM fest:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Ereignisse** > **Regeln**, und klicken Sie auf **Hinzufügen**, um eine Regel zu erstellen.
2. Legen Sie auf der Seite **Regel erstellen** die Regelparameter fest.
3. Klicken Sie unter Aktionen für **Ereignisregeln** auf **Aktion hinzufügen**. Wählen Sie dann in der Dropdownliste **Aktionstyp** die Option **E-Mail-Aktion** senden und wählen Sie eine **E-Mail-Verteilerliste**
4. Sie können auch eine benutzerdefinierte Betreffzeile und eine Benutzernachricht hinzufügen und eine Anlage in Ihre E-Mail hochladen, wenn ein eingehendes Ereignis mit der konfigurierten Regel übereinstimmt.
5. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigung wiederholen, bis das Ereignis deaktiviert ist**.



Ereignisse unterdrücken

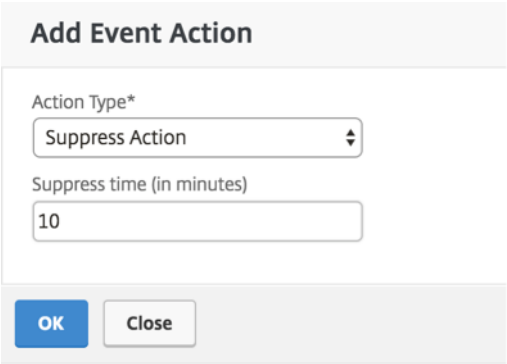
April 28, 2021

Wenn Sie die Ereignisaktion **Aktion unterdrücken** auswählen, können Sie einen Zeitraum in Minuten konfigurieren, für den ein Ereignis unterdrückt oder gelöscht wird. Sie können das Ereignis mindestens 1 Minute unterdrücken.

> Hinweis:
>
> Sie können die Unterdrückungszeit auch als 0 Minuten konfigurieren und das bedeutet unendlich viel Zeit. Wenn Sie keine Zeitdauer angeben, betrachtet Citrix ADM die Unterdrückungszeit als Null und läuft nie ab.

So unterdrücken Sie Ereignisse mithilfe von Citrix ADM:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Ereignisse** > **Regeln**.
2. Wechseln **Sie zur Seite Regel erstellen** oder **Regel konfigurieren**. Geben Sie alle Parameter an, die zum Erstellen einer Regel erforderlich sind.
3. Klicken Sie unter **Ereignisregelaktionen**auf **Aktion hinzufügen**, um Benachrichtigungsaktionen für das Ereignis zuzuweisen.
4. Wählen Sie auf der Seite " **Ereignisaktion hinzufügen** " im Dropdown-Menü " **Aktionstyp** " die Option Aktion **unterdrücken** aus und geben Sie den Zeitraum in Minuten an, für den ein Ereignis unterdrückt werden muss.
5. Klicken Sie auf **OK**.



Ereignisregeln erstellen

April 28, 2021

Sie können Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Regeln erleichtern das Filtern der Ereignisse, die in Ihrer gesamten Infrastruktur generiert wurden.

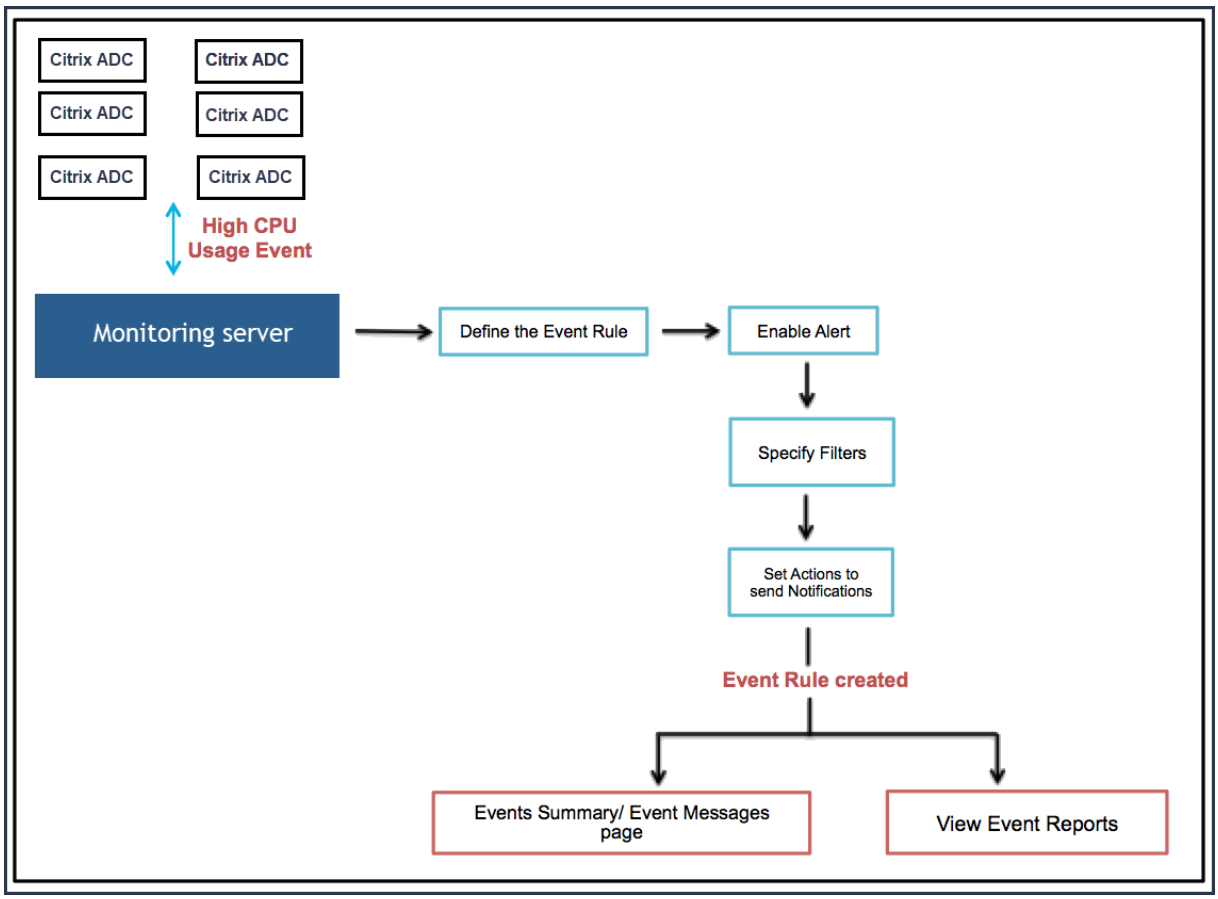
Sie können eine Reihe von Ereignissen filtern, indem Sie Regeln mit bestimmten Bedingungen konfigurieren und den Regeln Aktionen zuweisen. Wenn die generierten Ereignisse die Filterkriterien in der Regel erfüllen, wird die mit der Regel verknüpfte Aktion ausgeführt. Die Bedingungen für die Erstellung von Filtern sind: Schweregrad, Citrix Application Delivery Controller Instanzen (Citrix ADC), Kategorie, Fehlerobjekte, Konfigurationsbefehle und Meldungen.

Den Ereignissen können Sie folgende Aktionen zuweisen:

- **E-Mail senden Aktion**: Senden Sie eine E-Mail für die Ereignisse, die den Filterkriterien entsprechen.
- **Trap-Aktion senden**: SNMP-Traps an ein externes Trap-Ziel senden oder weiterleiten
- **Befehlsaktion ausführen**: Führen Sie einen Befehl aus, wenn ein eingehendes Ereignis die konfigurierte Regel erfüllt.
- **Job-Aktion ausführen**: Die Ausführung eines Jobs ist für Ereignisse vorgesehen, die den von Ihnen angegebenen Filterkriterien entsprechen.
- **Aktion unterdrücken**: Unterdrückt das Löschen eines Ereignisses für einen bestimmten Zeitraum.
- **Send Slack-Benachrichtigungen**: Senden Sie Benachrichtigungen auf dem konfigurierten Slack -Kanal für die Ereignisse, die den Filterkriterien entsprechen.
- **PagerDuty-Benachrichtigungen senden**: Senden Sie Ereignisbenachrichtigungen basierend auf den PagerDuty-Konfigurationen für die Ereignisse, die den Filterkriterien entsprechen.
- **ServiceNow-Benachrichtigungen senden**: Generieren Sie automatisch ServiceNow-Vorfälle für ein Ereignis, das den Filterkriterien entspricht.

Weitere Informationen finden Sie unter Ereignisregelaktionen hinzufügen.

Sie können Benachrichtigungen auch in einem bestimmten Intervall erneut senden lassen, bis ein Ereignis gelöscht wird. Außerdem können Sie die E-Mail mit einer bestimmten Betreffzeile, einer Benutzernachricht und einem Anhang anpassen.



Als Administrator möchten Sie beispielsweise Ereignisse mit hoher CPU-Auslastung auf ADC-Instanzen überwachen, die zu einem Ausfall führen können. Sie können eine der folgenden Aktionen ausführen, um Benachrichtigungen zu erhalten:

- Erstellen Sie eine Regel zum Überwachen von Instanzen. Fügen Sie der Regel eine Aktion hinzu, um Benachrichtigungen zu erhalten, wenn solche Ereignisse auftreten.
- Planen Sie eine Regel, um Instanzen in einem bestimmten Intervall zu überwachen. Sie erhalten also Benachrichtigungen, wenn solche Ereignisse innerhalb dieses Intervalls auftreten.

Das Konfigurieren einer Ereignisregel umfasst die folgenden Aufgaben:

1. Definieren der Regel
2. Wählen Sie den Schweregrad des Ereignisses aus, das von der Regel erkannt wird
3. Geben Sie die Kategorie des Ereignisses an
4. Angeben von Citrix ADC-Instanzen, für die die Regel gilt
5. Auswählen von Fehlerobjekten
6. Angeben von erweiterten Filtern
7. Angeben von Aktionen, die ausgeführt werden sollen, wenn die Regel ein Ereignis erkennt

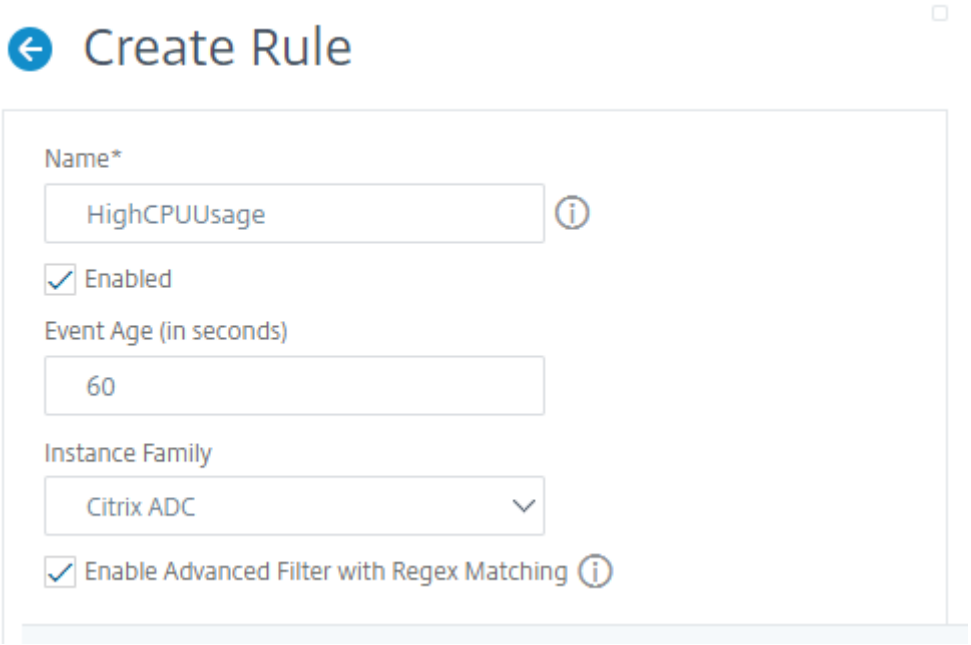
Schritt 1 - Definieren einer Ereignisregel

Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Regeln**, und klicken Sie auf **Hinzufügen**. Wenn Sie die Regel aktivieren möchten, **aktivieren Sie das Kontrollkästchen Regel aktivieren**.

Sie können die Option **Ereignisalter** festlegen, um das Zeitintervall (in Sekunden) anzugeben, nach dem Citrix ADM eine Ereignisregel aktualisiert.

> Hinweis:
>
> Der Mindestwert für das Ereignisalter beträgt 60 Sekunden. Wenn Sie das Feld **Ereignisalter** leer lassen, wird die Ereignisregel unmittelbar nach dem Auftreten des Ereignisses angewendet.

Basierend auf dem obigen Beispiel möchten Sie möglicherweise jedes Mal per E-Mail benachrichtigt werden, wenn Ihre Citrix ADC-Instanz 60 Sekunden lang eine “hohe CPU-Auslastung” hat. Sie können das Ereignisalter auf 60 Sekunden festlegen, sodass Sie jedes Mal, wenn Ihre Citrix ADC-Instanz eine “hohe CPU-Auslastung” für 60 Sekunden oder mehr hat, eine E-Mail-Benachrichtigung mit Details zum Ereignis erhalten.



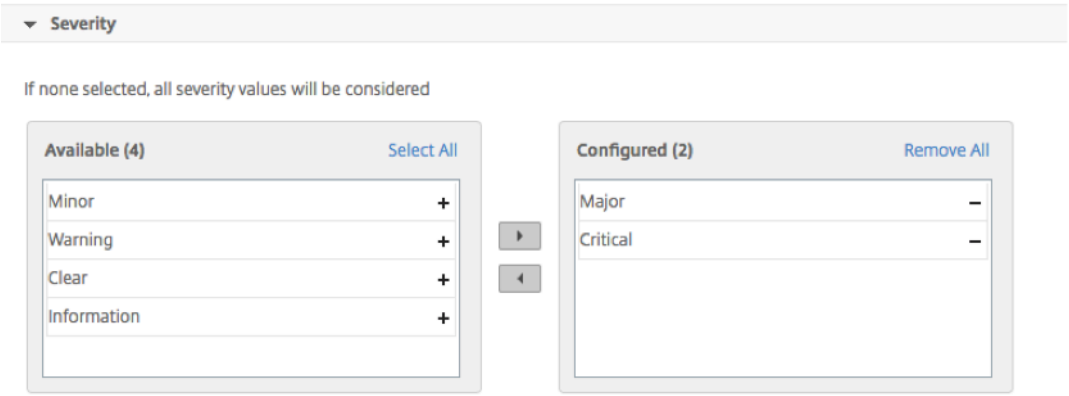
Sie können Ereignisregeln auch nach **Instanzfamilie** filtern, um die Citrix ADC-Instanz zu verfolgen, von der Citrix ADM ein Ereignis empfängt.

Wenn Sie einen anderen regulären Ausdruck als Sternchen (*) -Mustervergleich einschließen möchten, wählen Sie **Erweiterten Filter mit Regex-Matching aktivieren**aus.

Schritt 2 - Wählen Sie den Schweregrad des Ereignisses

Sie können Ereignisregeln erstellen, die die Standardeinstellungen für den Schweregrad verwenden. Schweregrad gibt den aktuellen Schweregrad der Ereignisse an, denen Sie die Ereignisregel hinzufügen möchten.

Sie können die folgenden Schweregrade definieren: Kritisch, Major, Minor, Warnung, Löschen und Information.

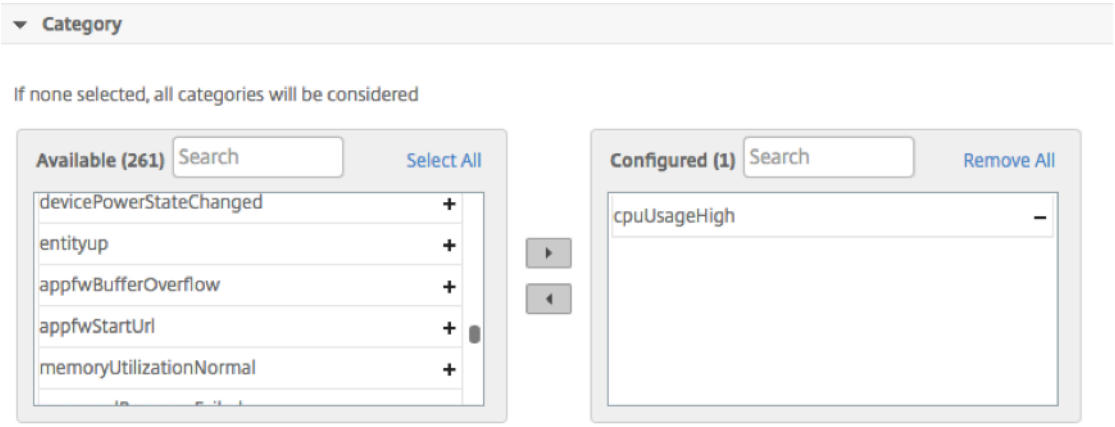


> **Hinweis**
>
> Sie können den Schweregrad sowohl für generische als auch für fortgeschrittene Ereignisse konfigurieren. Um den Schweregrad für Citrix ADC-Instanzen zu ändern, die auf Citrix ADM verwaltet werden, navigieren Sie zu **Netzwerke** > **Ereignisse** > **Ereigniseinstellungen**. Wählen Sie die **Kategorie** aus, für die Sie den Schweregrad des Ereignisses konfigurieren möchten, und klicken Sie auf **Schweregrad konfigurieren**. Weisen Sie einen neuen Schweregrad zu, und klicken Sie auf **OK**.

Schritt 3 - Geben Sie die Ereigniskategorie an

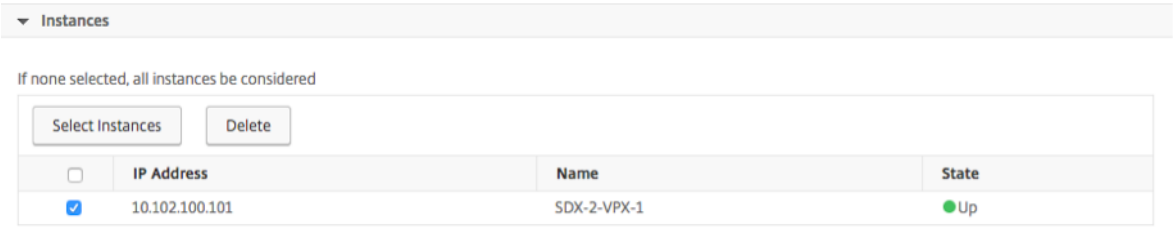
Sie können die Kategorie oder Kategorien der Ereignisse angeben, die von Ihren Citrix ADC-Instanzen generiert werden. Alle Kategorien werden auf Citrix ADC-Instanzen erstellt. Diese Kategorien werden dann dem Citrix ADM zugeordnet, der zur Definition von Ereignisregeln verwendet werden kann. Wählen Sie die Kategorie aus, die Sie berücksichtigen möchten, und verschieben Sie sie aus der Tabelle **Verfügbar** in die Tabelle **Konfiguriert**.

Im obigen Beispiel müssen Sie “cpuUsageHigh” als Ereigniskategorie aus der angezeigten Tabelle auswählen.



Schritt 4 - Angeben von Citrix ADC-Instanzen

Wählen Sie die IP-Adressen der Citrix ADC-Instanzen aus, für die Sie die Ereignisregel definieren möchten. Klicken Sie im Abschnitt **Instanzen** auf **Instanzen auswählen**. Wählen Sie auf der Seite **Instanzen auswählen** Ihre Instanzen aus und klicken Sie auf **Auswählen**.



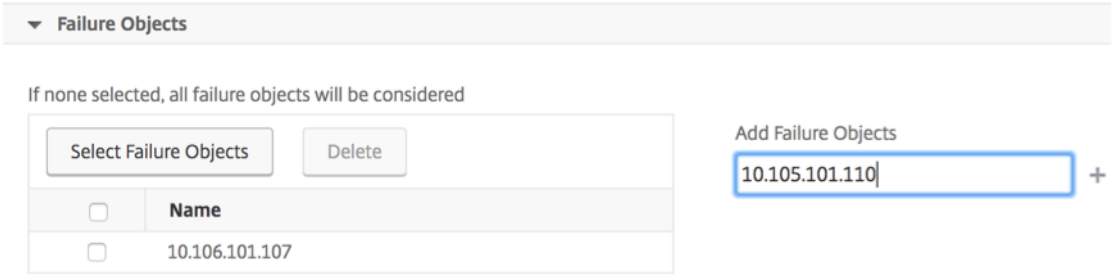
Schritt 5 - Auswählen von Fehlerobjekten

Sie können entweder ein Fehlerobjekt aus der bereitgestellten Liste auswählen oder ein Fehlerobjekt hinzufügen, für das ein Ereignis generiert wurde. Sie können auch einen regulären Ausdruck angeben, um Fehlerobjekte hinzuzufügen. Abhängig vom angegebenen regulären Ausdruck werden die Fehlerobjekte automatisch zur Liste hinzugefügt. Fehlerobjekte sind Entitätsinstanzen oder Leistungsindikatoren, für die ein Ereignis generiert wurde.

> **Wichtig**
>
> Um Fehlerobjekte mithilfe eines regulären Ausdrucks aufzulisten, wählen Sie **Erweiterten Filter mit Regex-Abgleich aktivieren** in Schritt 1.

Das Fehlerobjekt wirkt sich auf die Art und Weise aus, in der ein Ereignis verarbeitet wird, und stellt sicher, dass es genau das Problem wie benachrichtigt widerspiegelt. Mit diesem Filter können Sie Probleme auf den Fehlerobjekten schnell verfolgen und die Ursache für ein Problem identifizieren. Wenn beispielsweise ein Benutzer Anmeldeprobleme hat, ist das Fehlerobjekt hier der Benutzername oder das Kennwort, `nsroot`z. B.

Diese Liste kann Leistungsindikatornamen für alle mit Schwellenwert verbundenen Ereignisse, Entitätsnamen für alle Entity-bezogenen Ereignisse, Zertifikatnamen für zertifikatbezogene Ereignisse usw. enthalten.

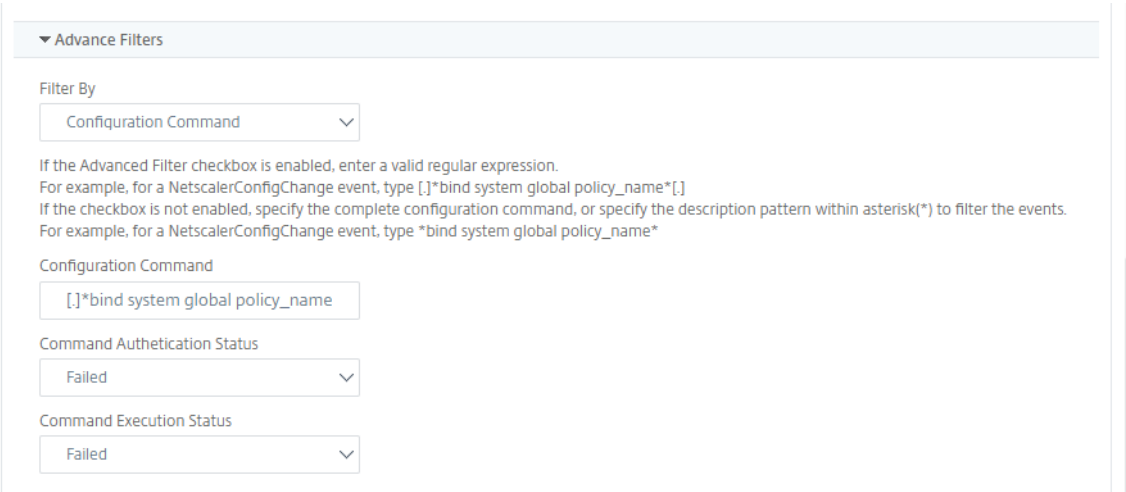


Schritt 6 - Angeben von erweiterten Filtern

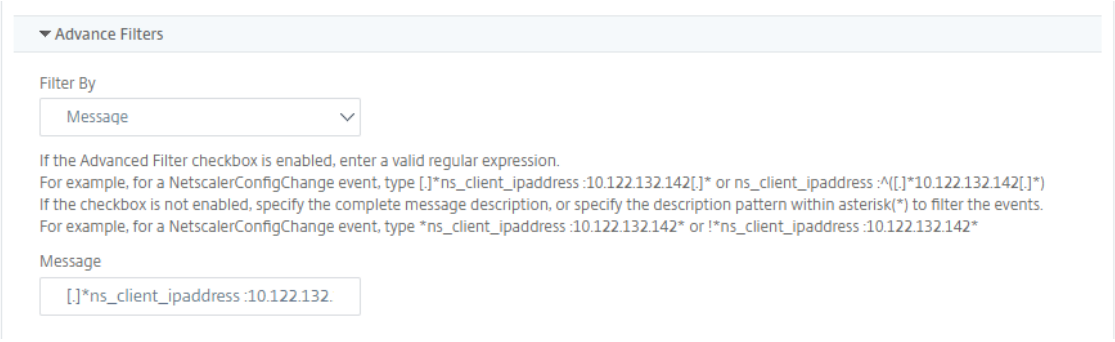
Sie können eine Ereignisregel weiter filtern:

- **Konfigurationsbefehle** - Sie können den vollständigen Konfigurationsbefehl angeben oder einen regulären Ausdruck zum Filtern von Ereignissen angeben.

  Sie können die Ereignisregel weiter nach dem Authentifizierungsstatus und/oder dem Ausführungsstatus des Befehls filtern. Geben Sie beispielsweise für einen `NetscalerConfigChange event`, ein `[.]*bind system global policy_name[.]*`.



- **Meldungen** - Sie können die vollständige Nachrichtenbeschreibung angeben oder einen regulären Ausdruck angeben, um die Ereignisse zu filtern.
  Geben Sie beispielsweise für ein `NetscalerConfigChange`Ereignis ein `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)`.



> **Wichtig**
>
> Um Konfigurationsbefehle und Meldungen mit anderen regulären Ausdrücken als Sternchen (*) -Musterabgleich zu filtern, wählen Sie **Erweiterten Filter mit Regex-Matching aktivieren** in Schritt 1.

Schritt 7 - Ereignisregelaktionen hinzufügen

Sie können Ereignisregelaktionen hinzufügen, um Benachrichtigungsaktionen für ein Ereignis zuzuweisen. Diese Benachrichtigungen werden gesendet oder ausgeführt, wenn ein Ereignis die oben festgelegten Filterkriterien erfüllt. Sie können die folgenden Ereignisaktionen hinzufügen:

- E-Mail senden Aktion
- Trap-Aktion senden
- Befehls-Aktion ausführen
- Job-Aktion ausführen
- Aktion unterdrücken
- Slack Benachrichtigungen senden
- PagerDuty-Benachrichtigungen senden
- ServiceNow-Benachrichtigungen senden

So legen Sie E-Mail-Ereignisregelaktion fest

Wenn Sie **E-Mail-Aktion senden**wählen, wird eine E-Mail ausgelöst, wenn die Ereignisse die definierten Filterkriterien erfüllen. Sie müssen entweder eine E-Mail-Verteilerliste erstellen, indem Sie Details zum Mailserver oder E-Mail-Profil angeben, oder Sie können eine zuvor erstellte E-Mail-Verteilerliste auswählen.

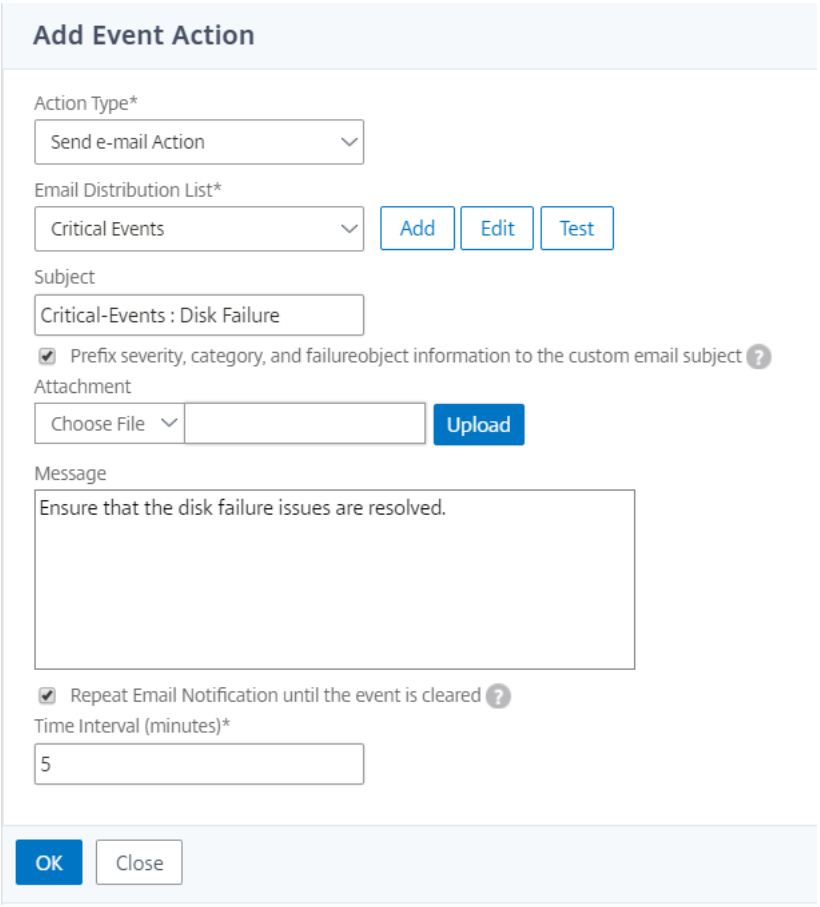
Aufgrund einer hohen Anzahl virtueller Server, die in Citrix ADM konfiguriert werden, erhalten Sie möglicherweise täglich eine hohe Anzahl von E-Mails. Die E-Mails haben eine Standard-Betreffzeile, die Informationen über den Schweregrad des Ereignisses, die Kategorie des Ereignisses und das

Fehlerobjekt bereitstellt. Die Betreffzeile enthält jedoch keine Informationen über den Namen des virtuellen Servers, von dem diese Ereignisse stammen. Sie haben jetzt die Möglichkeit, einige zusätzliche Informationen wie den Namen der betroffenen Entität, also den Namen des Fehlerobjekts, einzubeziehen.

Sie können auch eine benutzerdefinierte Betreffzeile und eine Benutzernachricht hinzufügen und eine Anlage in Ihre E-Mail hochladen, wenn ein eingehendes Ereignis mit der konfigurierten Regel übereinstimmt.

Beim Senden von E-Mails für Ereignisbenachrichtigungen möchten Sie möglicherweise eine Test-E-Mail senden, um die konfigurierten Einstellungen zu testen. Mit der Schaltfläche “Test” können Sie nun eine Test-E-Mail senden, nachdem Sie einen E-Mail-Server, zugeordnete verteilte Listen und andere Einstellungen konfiguriert haben. Diese Funktion stellt sicher, dass die Einstellungen einwandfrei funktionieren.

Sie können auch sicherstellen, dass alle kritischen Ereignisse adressiert werden und keine wichtigen E-Mail-Benachrichtigungen verpasst werden. Aktivieren **Sie das Kontrollkästchen E-Mail-Benachrichtigung wiederholen, bis das Ereignis deaktiviert ist**, um wiederholte E-Mail-Benachrichtigungen für Ereignisregeln zu senden, die den ausgewählten Kriterien entsprechen. Wenn Sie beispielsweise eine Ereignisregel für Instanzen erstellt haben, die Datenträgerfehler verursachen, und Sie benachrichtigt werden möchten, bis das Problem behoben ist, können Sie sich dafür entscheiden, wiederholte E-Mail-Benachrichtigungen zu diesen Ereignissen zu erhalten.



So legen Sie die Aktion Trap-Ereignisregel fest

Wenn Sie den Ereignistyp **Trap-Aktion senden** auswählen, werden SNMP-Traps an ein externes Trap-Ziel gesendet oder weitergeleitet. Durch das Definieren einer Trap-Verteilerliste (oder eines Trap-Ziels und Trap-Profildetails) werden Trap-Nachrichten an einen bestimmten Trap-Listener gesendet, wenn Ereignisse die definierten Filterkriterien erfüllen.

So legen Sie die Aktion Befehl ausführen fest

Wenn Sie die **Ereignisaktion "Befehlsaktion ausführen"** auswählen, können Sie einen Befehl oder ein Skript erstellen, das auf Citrix ADM für Ereignisse ausgeführt werden kann, die einem bestimmten Filterkriterium entsprechen.

Sie können auch die folgenden Parameter für das Skript **Befehlsaktion ausführen** festlegen:

Parameter	Beschreibung

$source	Dieser Parameter entspricht der Quell-IP-Adresse des empfangenen Ereignisses.
$category	Dieser Parameter entspricht der Art der Fallen, die in der Kategorie des Filters definiert sind
$entity	Dieser Parameter entspricht den Entitätsinstanzen oder Leistungsindikatoren, für die ein Ereignis generiert wurde. Es kann die Zählernamen für alle Ereignisse mit Schwellenwert, Entitätsnamen für alle Entitätsbezogenen Ereignisse und Zertifikatnamen für alle zertifikatbezogenen Ereignisse enthalten.
$severity	Dieser Parameter entspricht dem Schweregrad des Ereignisses.
$failureobj	Das Fehlerobjekt wirkt sich auf die Art und Weise aus, wie ein Ereignis verarbeitet wird, und stellt sicher, dass das Fehlerobjekt das genaue Problem wie benachrichtigt wiedergibt. Dies kann verwendet werden, um Probleme schnell aufzuspüren und den Grund für den Fehler zu identifizieren, anstatt einfach rohe Ereignisse zu melden.

> **Hinweis**
>
> Während der Befehlsausführung werden diese Parameter durch tatsächliche Werte ersetzt.

Angenommen, Sie möchten eine Ausführungsbefehl Aktion festlegen, wenn der Status des virtuellen Lastenausgleichs auf **Heruntergefahren festgelegt**wird. Als Administrator möchten Sie möglicherweise eine schnelle Problemumgehung bereitstellen, indem Sie einen anderen virtuellen Server hinzufügen. In Citrix ADM können Sie:

- Schreiben Sie eine Skriptdatei (.sh).

  Im Folgenden finden Sie eine Beispielskriptdatei (.sh):

```
1  #!/bin/sh
```



```
source=$1
failureobj=$2
payload='{
”params”:{
”warning”:”YES” }
,”lbvserver”:{
”name”:”'$failureobj'”,”servicetype”:”HTTP”,”ipv46”:”x.x.x.x”,”
   port”:”80”,”td”:””,”m”:”IP”,”state”:”ENABLED”,”rhistate”:”
   PASSIVE”,”appflowlog”:”ENABLED”,”
bypassaaaa”:”NO”,”retainconnectionsoncluster”:”NO”,”comment”:”” }
 }
'
url=”http://$source/nitro/v1/config/lbvserver”
curl --insecure -basic -u nsroot:nsroot -H ”Content-type:
   application/json” -X POST -d $payload $url

<!--NeedCopy-->
```

- Speichern Sie die SH-Datei an einem beliebigen persistenten Speicherort auf dem Citrix ADM Agent. Beispiel: `/var`.
- Geben Sie den Speicherort der SH-Datei in Citrix ADM an, der ausgeführt werden soll, wenn die Regelkriterien erfüllt sind.

So legen Sie die Aktion **Befehl ausführen** zum Erstellen eines neuen virtuellen Servers fest:

1. Definieren der Regel
2. Wählen Sie den Schweregrad des Ereignisses
3. Wählen Sie die Event-Kategorie **Entitydown**
4. Wählen Sie die Instanz aus, für die der virtuelle Server konfiguriert ist
5. Auswählen oder Erstellen eines Fehlerobjekts für den virtuellen Server
6. Klicken Sie unter **Ereignisregelaktionen** auf **Aktion hinzufügen** und wählen Sie in der Liste **Aktionstyp** die Option **Befehlsaktion ausführen**.
7. Klicken Sie unter **Befehlsausführungsliste** auf **Hinzufügen**.

   Die Seite “Befehlsverteilungsliste erstellen” wird angezeigt.

   a) Geben Sie unter **Profilname**einen Namen Ihrer Wahl an

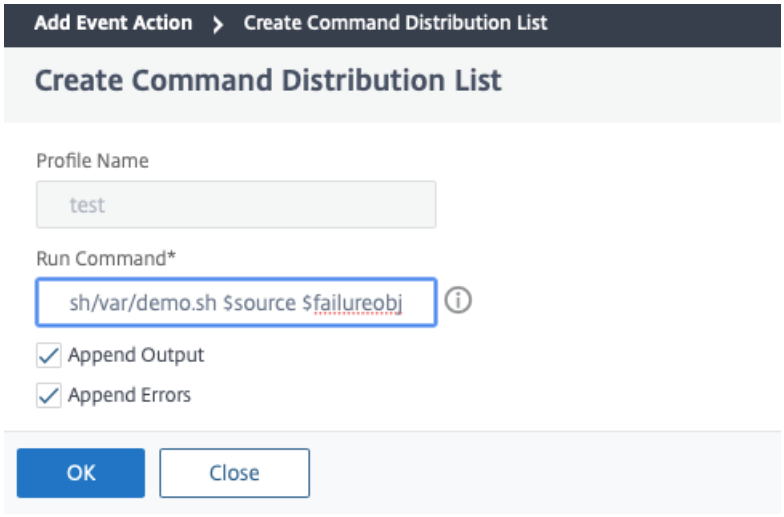
   b) Geben Sie **unter Run Command**den Citrix ADM Agent-Speicherort an, an dem das Skript ausgeführt werden muss. Beispiel: `/sh/var/demo.sh $source $failureobj`.

   c) Wählen Sie **Ausgabe-** und **Anfügefehler anhängen**

> **Hinweis**
>
> Sie können die Optionen **Ausgabe anfügen** und **Fehler anhängen** aktivieren, wenn Sie die Ausgabe und die Fehler speichern möchten, die bei der Ausführung eines Befehlsskripts in den Citrix ADM -Serverprotokolldateien generiert wurden (falls vorhanden). Wenn Sie diese Optionen nicht aktivieren, verwirft Citrix ADM alle Ausgaben und Fehler, die während der Ausführung des Befehlsskripts generiert wurden.

d) Klicken Sie auf **Erstellen**.

8. Klicken Sie auf der Seite **Ereignisaktion hinzufügen** auf **OK**.



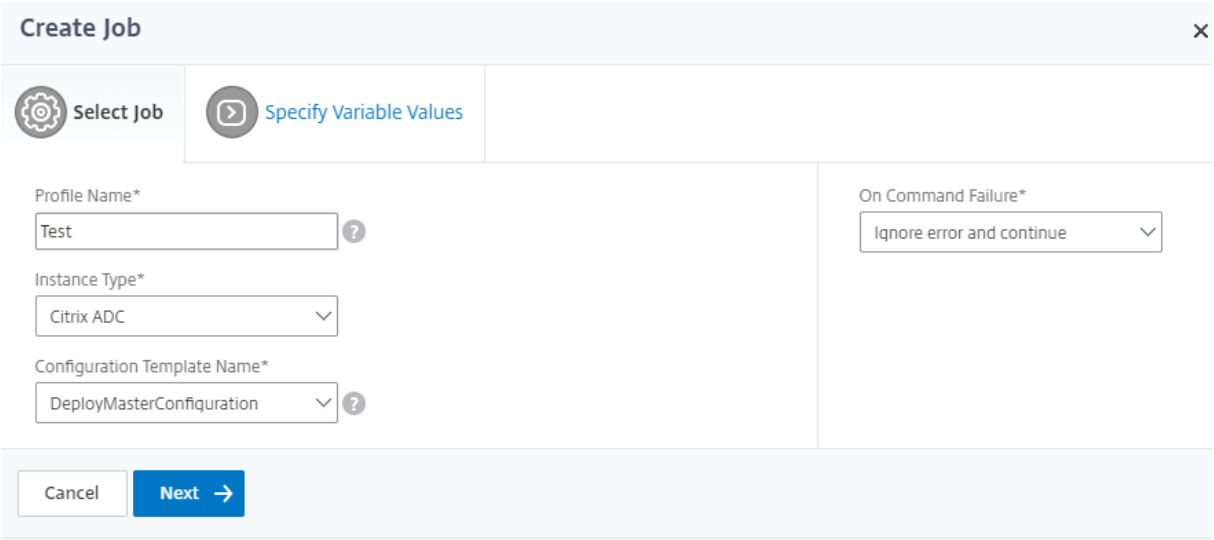
> **Hinweis**
>
> Sie können die Optionen **Ausgabe anfügen** und **Fehler anhängen** aktivieren, wenn Sie die Ausgabe und die Fehler speichern möchten, die bei der Ausführung eines Befehlsskripts in den Citrix ADM -Serverprotokolldateien generiert wurden (falls vorhanden). Wenn Sie diese Optionen nicht aktivieren, verwirft Citrix ADM alle Ausgaben und Fehler, die während der Ausführung des Befehlsskripts generiert wurden.

So legen Sie die Aktion “Job ausführen” fest

Durch das Erstellen eines Profils mit Konfigurationsaufträgen wird ein Job als integrierter Job oder benutzerdefinierter Job für Instanzen Citrix ADC, Citrix ADC SDX und Citrix SD-WAN WO für Ereignisse und Alarme ausgeführt, die den von Ihnen angegebenen Filterkriterien entsprechen.

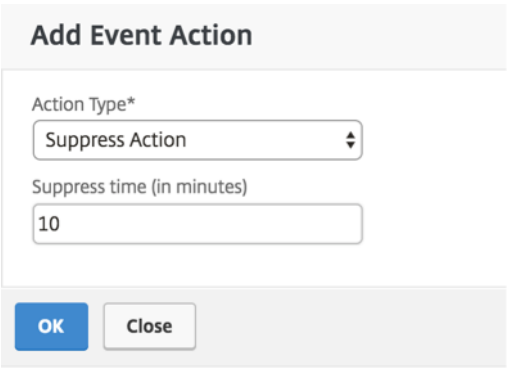
1. Klicken Sie unter **Ereignisregelaktionen**auf **Aktion hinzufügen**, und wählen Sie in der Liste ****Aktionstyp die Option Jobaktion** ausführen** aus.
2. Erstellen Sie ein Profil mit einem Job, den Sie ausführen möchten, wenn die Ereignisse die definierten Filterkriterien erfüllen.

3. Geben Sie beim Erstellen eines Auftrags einen Profilnamen, den Instanztyp, die Konfigurationsvorlage und die Aktion an, die Sie ausführen möchten, wenn die Befehle für den Auftrag fehlschlagen.
4. Geben Sie anhand des ausgewählten Instanztyps und der gewählten Konfigurationsvorlage die Variablenwerte an, und klicken Sie auf **Fertig stellen**, um den Job zu erstellen.



So legen Sie die Aktion Unterdrücken fest

Wenn Sie die Ereignisaktion **Aktion unterdrücken** auswählen, können Sie einen Zeitraum in Minuten konfigurieren, für den ein Ereignis unterdrückt oder gelöscht wird. Sie können das Ereignis mindestens 1 Minute unterdrücken.



So legen Sie Slack -Benachrichtigungen von Citrix ADM fest

Konfigurieren Sie den erforderlichen Slack-Kanal, indem Sie den Profilnamen und die Webhook-URL in der Citrix ADM-Benutzeroberfläche angeben. Die Ereignisbenachrichtigungen werden dann an diesen Kanal gesendet. Sie können mehrere Slack Kanäle konfigurieren, um diese Benachrichtigungen zu erhalten

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Ereignisse** > **Regeln**, und klicken Sie auf **Hinzufügen**, um eine Regel zu erstellen.
2. Legen Sie auf der Seite **Regel erstellen** die Regelparameter wie Schweregrad und Kategorie fest. Wählen Sie Instanzen und auch Fehlerobjekte aus, die Sie überwachen möchten.
3. Klicken Sie unter **Ereignisregelaktionen**auf **Aktion hinzufügen**. Wählen Sie dann aus der Liste **Aktionstyp** die Option **Slack-Benachrichtigungen senden** und dann die Option **Pufferprofilliste** aus.
4. Sie können auch eine Slack-Profilliste hinzufügen, indem Sie neben dem Feld **Pufferprofilliste** auf **Hinzufügen** klicken.
5. Geben Sie die folgenden Parameter ein, um eine Profilliste zu erstellen:
   a) **Profilname** Geben Sie einen Namen für die Profilliste ein, die auf Citrix ADM konfiguriert werden soll.
   b) **Kanalname**. Geben Sie den Namen des Slack Kanals ein, an den die Ereignisbenachrichtigungen gesendet werden sollen.
   c) **Webhook-URL**. Geben Sie die Webhook-URL des Kanals ein, den Sie zuvor eingegeben haben. Eingehende Webhooks sind eine einfache Möglichkeit, Nachrichten aus externen Quellen in Slack zu posten. Die URL ist intern mit dem Kanalnamen verknüpft und alle Ereignisbenachrichtigungen werden an diese URL gesendet, um auf dem angegebenen Slack -Kanal gepostet zu werden. Ein Beispiel für einen Webhook ist wie folgt: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK
6. Klicken Sie auf **Erstellen**, und klicken Sie im Fenster **Ereignisaktion hinzufügen** auf **OK**.

> **Hinweis**
>
> Sie können die Slack profile auch hinzufügen, indem Sie zu **Konto**> **Benachrichtigungen**> **Pufferprofile**navigieren. Klicken Sie auf **Hinzufügen**, und erstellen Sie das Profil wie im vorherigen Abschnitt beschrieben.

Sie können den Status der von Ihnen erstellten Slack -Profile anzeigen.

Ihre Ereignisregel wird jetzt mit geeigneten Filtern und gut definierten Ereignisregelaktionen erstellt.

So richten Sie PagerDuty-Benachrichtigungen von Citrix ADM ein

Sie können in Citrix ADM ein PagerDuty-Profil als Option hinzufügen, um die Vorfallbenachrichtigungen basierend auf Ihren PagerDuty-Konfigurationen zu überwachen. Mit PagerDuty können Sie Benachrichtigungen per E-Mail, SMS, Push-Benachrichtigung und Telefonanruf unter einer registrierten Nummer konfigurieren.

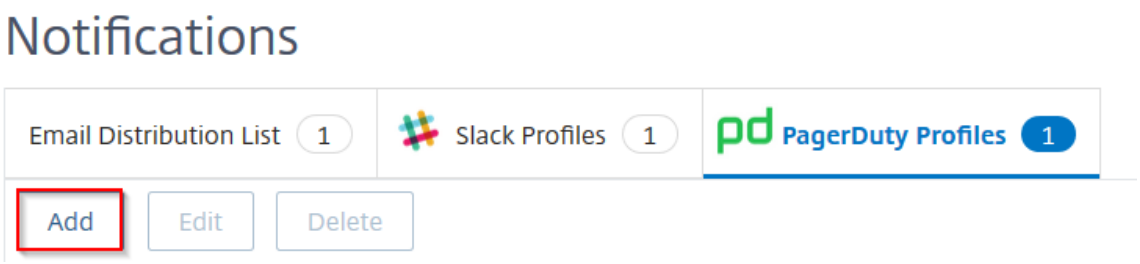
Bevor Sie ein PagerDuty-Profil in Citrix ADM hinzufügen, stellen Sie sicher, dass Sie die erforderlichen Konfigurationen in PagerDuty abgeschlossen haben. Weitere Informationen finden Sie unter PagerDuty-Dokumentation.

Sie können Ihr PagerDuty-Profil als eine der Optionen auswählen, um Benachrichtigungen für die folgenden Funktionen zu erhalten:

- **Ereignisse** — Liste der Ereignisse, die für Citrix ADC-Instanzen generiert werden.
- **Lizenzen** — Liste der Lizenzen, die derzeit aktiv sind, bald ablaufen usw.
- **SSL-Zertifikate** — Liste der SSL-Zertifikate, die Citrix ADC-Instanzen hinzugefügt werden.

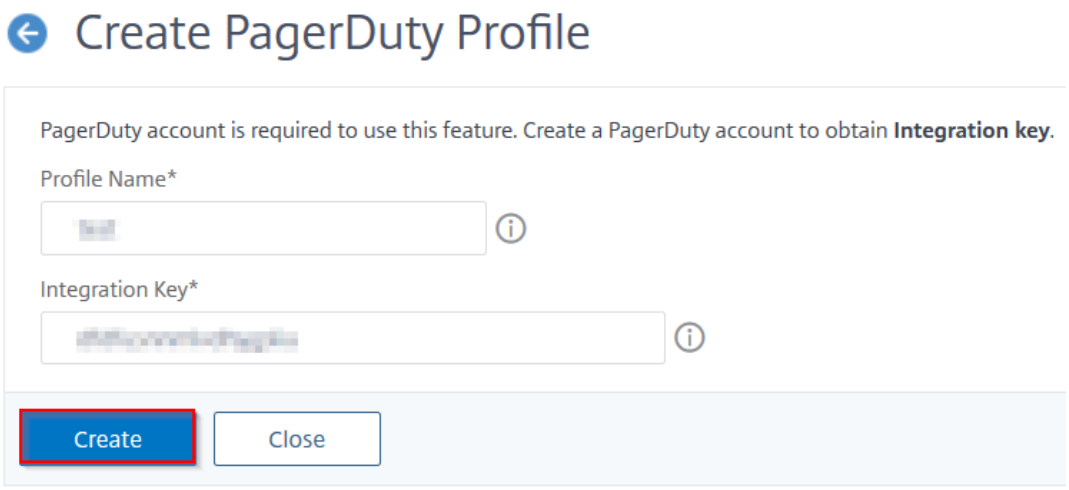
So fügen Sie ein PagerDuty-Profil in ADM hinzu:

1. Melden Sie sich mit Administratoranmeldeinformationen bei Citrix ADM an.
2. Navigieren Sie zu **Konto** > **Benachrichtigungen** > **PagerDuty Profile**.
3. Klicken Sie auf **Hinzufügen**, um ein Profil zu erstellen.



4. Auf der Seite PagerDuty-Profil erstellen:
   a) Geben Sie einen Profilnamen Ihrer Wahl an.
   b) Geben Sie den **Integrationsschlüssel ein**.

      Sie können den Integrationsschlüssel von Ihrem PagerDuty Portal abrufen.
   c) Klicken Sie auf **Erstellen**.



Anwendungsfall:

Betrachten Sie ein Szenario, das Sie:

- möchten Benachrichtigungen an Ihr PagerDuty-Profil senden.
- haben Telefonanruf als Option in PagerDuty konfiguriert, um Benachrichtigungen zu empfangen.
- möchten Anrufwarnungen für Citrix ADC Ereignisse abrufen.

So konfigurieren Sie:

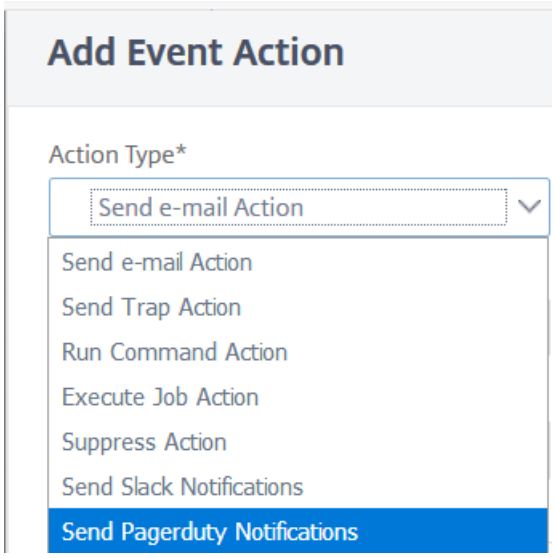
a) Navigieren Sie zu **Ereignissen** > **Regeln**

b) Konfigurieren Sie auf der Seite **Regel erstellen** alle anderen Parameter zum Erstellen einer Regel.

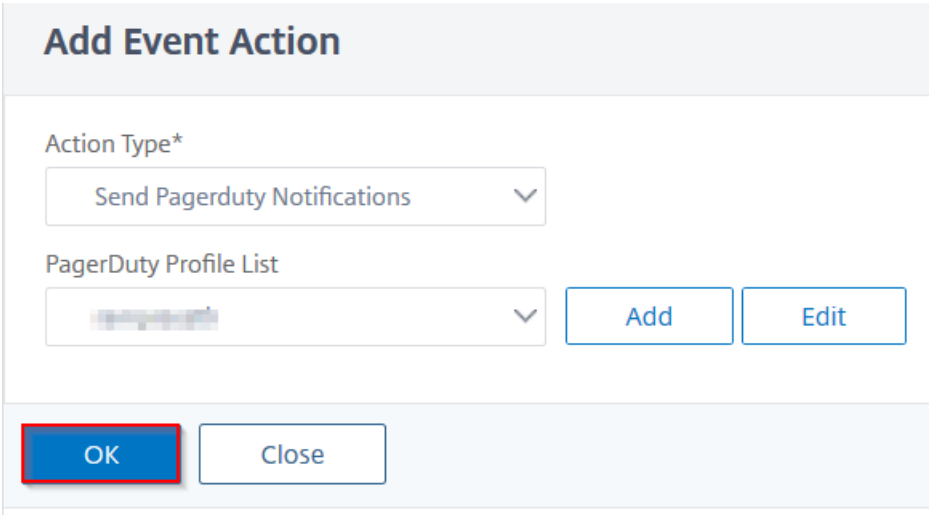
c) Klicken Sie unter **Regelaktionen erstellen** auf **Aktion hinzufügen**.

Die Seite **Ereignisaktion hinzufügen** wird angezeigt.

i. Wählen Sie unter **Aktionstyp**die Option **PagerDuty-Benachrichtigungen senden**aus.



ii. Wählen Sie Ihr PagerDuty-Profil aus und klicken Sie auf **OK**.



Nach Abschluss der Konfiguration erhalten Sie, wenn ein neues Ereignis für die Citrix ADC-Instanz generiert wird, einen Telefonanruf. Aus dem Telefonanruf können Sie entscheiden:

- Bestätigen Sie das Ereignis
- Markieren Sie es als aufgelöst
- Zu einem anderen Teammitglied eskalieren

So generieren Sie ServiceNow-Vorfälle von Citrix ADM automatisch

Sie können ServiceNow-Vorfälle für Citrix ADM Ereignisse automatisch generieren, indem Sie das ServiceNow-Profil auf der Citrix ADM-GUI auswählen. Sie müssen das **ServiceNow-Profil** in Citrix ADM wählen, um eine Ereignisregel zu konfigurieren.

Bevor Sie eine Ereignisregel zum automatischen Generieren von ServiceNow-Vorfällen konfigurieren, integrieren Sie den Citrix ADM-Dienst in die ServiceNow-Instanz. Weitere Informationen finden Sie unter ITSM-Adapter für ServiceNow konfigurieren.

Um eine Ereignisregel zu konfigurieren, navigieren Sie zu **Ereignisse** > **Regeln**.

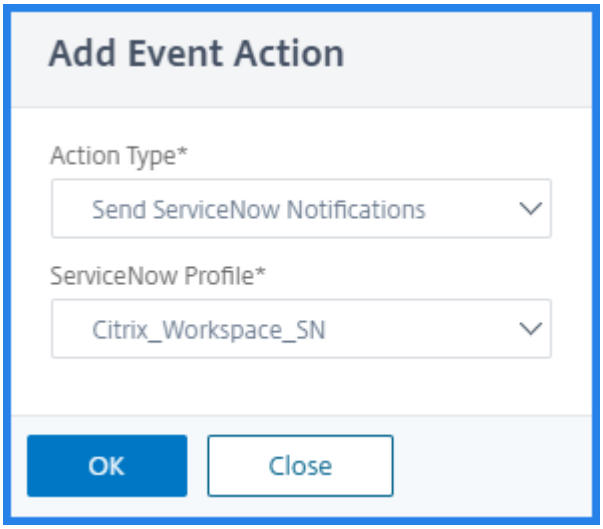
1. Konfigurieren Sie auf der Seite **Regel erstellen** alle anderen Parameter zum Erstellen einer Regel.
2. Klicken Sie unter **Regelaktionen erstellen** auf **Aktion hinzufügen**.

   Die Seite **Ereignisaktion hinzufügen** wird angezeigt.

   a) Wählen Sie unter **Aktionstyp**die Option **ServicNow-Benachrichtigungen senden**aus.

   b) Wählen Sie im **ServiceNow-Profil**das **Citrix_Workspace_SN-Profil**aus der Liste aus.

   c) Klicken Sie auf **OK**.



Ändern des gemeldeten Schweregrads von Ereignissen, die auf Citrix ADC-Instanzen auftreten

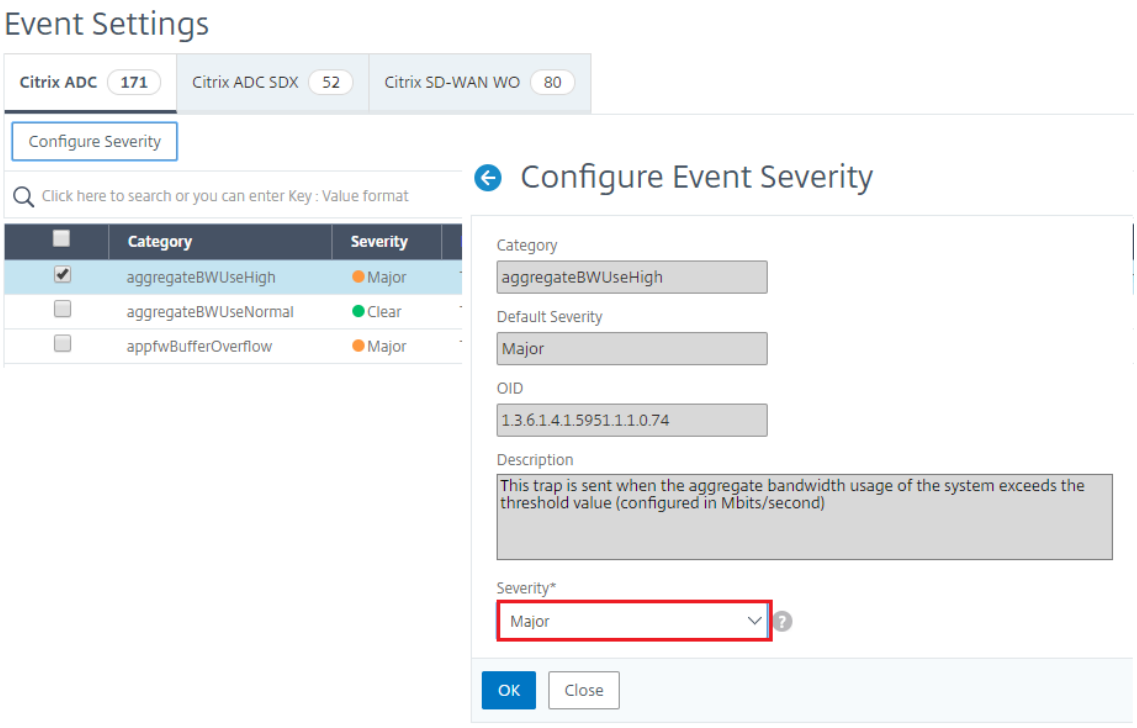
April 28, 2021

Sie können die Berichterstellung über Ereignisse verwalten, die auf allen Ihren Geräten generiert werden, sodass Sie Ereignisdetails zu einem bestimmten Ereignis in einer Instanz anzeigen und Berichte basierend auf dem Schweregrad des Ereignisses anzeigen können. Sie können auch Ereignisregeln erstellen, die die Standardeinstellungen für den Schweregrad verwenden, und Sie können die Einstellungen für den Schweregrad ändern. Sie können den Schweregrad für allgemeine und unternehmensspezifische Ereignisse konfigurieren.

Sie können die folgenden Schweregrade definieren: Kritisch, Major, Minor, Warnung und Löschen.

So ändern Sie den Schweregrad des Ereignisses:

1. Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Ereigniseinstellungen**.
2. Klicken Sie auf die Registerkarte für den Citrix ADC-Instanztyp, den Sie ändern möchten. Wählen Sie dann die Kategorie aus der Liste aus, und klicken Sie auf **Schweregrad konfigurieren**.
3. Wählen Sie unter **Ereignisschweregrad konfigurieren**aus der Dropdownliste den Schweregrad aus.
4. Klicken Sie auf **OK**.

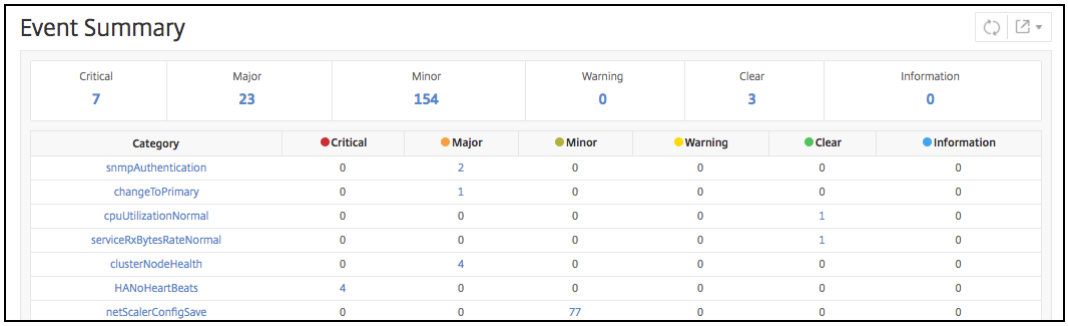


Zusammenfassung der Ereignisse anzeigen

April 28, 2021

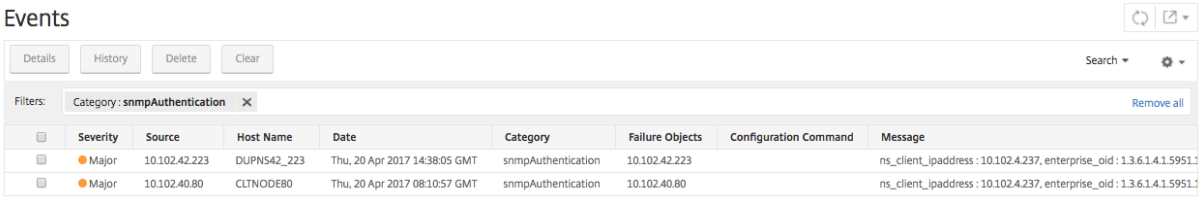
Sie können nun eine Seite Ereigniszusammenfassung anzeigen, um die Ereignisse und Traps zu überwachen, die in Ihrem Citrix Application Delivery Management (Citrix ADM) empfangen wurden. Navigieren Sie zu **Netzwerke** > **Ereignisse**. Auf der Seite Ereignisübersicht werden die folgenden Informationen in einem tabellarischen Format angezeigt:

- **Zusammenfassung aller Ereignisse, die von Citrix ADM empfangen**werden. Die Ereignisse werden nach Kategorie aufgelistet, und die unterschiedlichen Schweregrade werden in verschiedenen Spalten angezeigt: Kritisch, Major, Minor, Warnung, Löschen und Information. Ein kritisches Ereignis tritt beispielsweise auf, wenn eine Citrix Application Delivery Controller (Citrix ADC) -Instanz ausfällt und keine Informationen an das Citrix ADM sendet. Während des Ereignisses wird eine Benachrichtigung an einen Administrator gesendet, in der der Grund für den Ausfall der Instanz, die Zeit, für die sie ausgefallen war, usw. erläutert wird. Das Ereignis wird dann auf der Seite Ereignisübersicht aufgezeichnet, auf der Sie die Zusammenfassung anzeigen und auf die Details des Ereignisses zugreifen können.



- **Anzahl der empfangenen Fallen für jede Kategorie**. Die Anzahl der empfangenen Traps, kategorisiert nach Schweregrad. Standardmäßig hat jeder Trap, der von Citrix ADC-Instanzen an Citrix ADM gesendet wird, einen zugewiesenen Schweregrad, aber als Netzwerkadministrator können Sie den Schweregrad in der Citrix ADM GUI angeben.

Wenn Sie auf einen Kategorietyp oder eine Falle klicken, gelangen Sie zur Seite **Ereignisse**, auf der Filter wie Kategorie und Schweregrad vorausgewählt sind. Auf dieser Seite werden weitere Informationen zum Ereignis angezeigt, z. B. die IP-Adresse und den Hostnamen einer Citrix ADC-Instanz, das Datum, an dem die Trap empfangen wurde, die Kategorie, die Fehlerobjekte, die Ausführung des Konfigurationsbefehls und die Nachrichtenbenachrichtigung.



Sie können die Anzahl der Tage zwischen 1 und 40 konfigurieren, für die Sie die Ereignisse in Citrix ADM anzeigen möchten. Wenn Sie beispielsweise 30 Tage auswählen, zeigt Citrix ADM die Ereignisse für 30 Tage an und nach 30 Tagen werden die Ereignisse gelöscht. Um diese Ereigniseinstellung zu konfigurieren, navigieren Sie zu **Einstellungen > Data Rentention Policy**. Weitere Informationen finden Sie unter Datenaufbewahrungsrichtlinie.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage

> auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Ereignisschweregrade und SNMP-Trap-Details anzeigen

April 28, 2021

Wenn Sie ein Ereignis und seine Einstellungen in Citrix Application Delivery Management (Citrix ADM) erstellen, können Sie das Ereignis sofort auf der Seite Ereigniszusammenfassung anzeigen. Ebenso können Sie den Zustand, die Betriebszeit, die Modelle und die Versionen aller Citrix Application Delivery Controller (Citrix ADC) -Instanzen, die Ihrem Citrix ADM -Server hinzugefügt wurden, im Infrastructure Dashboard detailliert anzeigen und überwachen.

Auf dem Infrastruktur-Dashboard können Sie jetzt irrelevante Werte maskieren, sodass Sie Informationen wie Ereignisse nach Schweregrad, Status, Uptime, Modelle und Version von Citrix ADC-Instanzen einfacher anzeigen und überwachen können.

Beispielsweise können Ereignisse mit einem **kritischen** Schweregrad selten auftreten. Wenn diese kritischen Ereignisse jedoch im Netzwerk auftreten, sollten Sie möglicherweise weiter untersuchen, beheben und überwachen, wo und wann das Ereignis aufgetreten ist. Wenn Sie alle Schweregrade außer Kritisch auswählen, zeigt das Diagramm nur das Vorkommen kritischer Ereignisse an. Wenn Sie auf das Diagramm klicken, gelangen Sie zur Seite **Schweregrade basierende Ereignisse**, auf der Sie alle Details darüber sehen können, wann ein kritisches Ereignis für die von Ihnen ausgewählte Dauer aufgetreten ist: die Instanzquelle, das Datum, die Kategorie und die Benachrichtigung über die Nachricht, die beim Auftreten des kritischen Ereignisses gesendet wurde.

In ähnlicher Weise können Sie den Zustand einer Citrix ADC VPX Instanz auf dem Dashboard anzeigen. Sie können die Zeit maskieren, in der die Instanz gestartet und ausgeführt wurde, und nur die Zeiten anzeigen, in denen die Instanz außer Betrieb war. Wenn Sie auf das Diagramm klicken, gelangen Sie zur Seite dieser Instanz, auf der der Filter *außerhalb des Dienstes* bereits angewendet wurde, und sehen Details wie den Hostnamen, die Anzahl der pro Sekunde empfangenen HTTP-Anforderungen, die CPU-Auslastung und andere. Sie können auch die Instanz auswählen und das Instanz-Dashboard für weitere Details anzeigen.

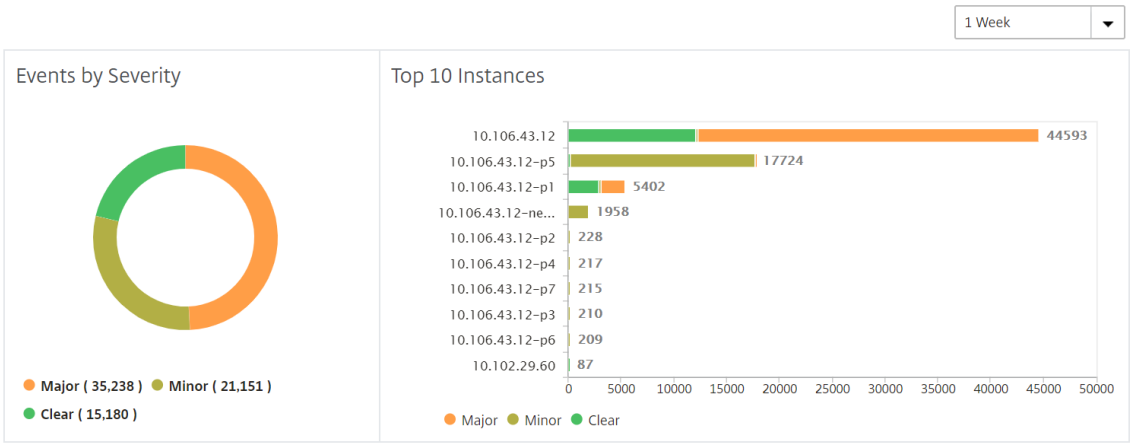
So wählen Sie bestimmte Ereignisse nach Schweregrad in Citrix ADM aus:

1. Melden Sie sich mit Ihren Administratoranmeldeinformationen bei Citrix ADM an.
2. Navigieren Sie zu **Netzwerke** > **Dashboard**.

   ODER

   Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Berichte**.

3. Wählen Sie in der Dropdownliste oben rechts auf der Seite die Dauer aus, für die Ereignisse nach Schweregrad angezeigt werden sollen.

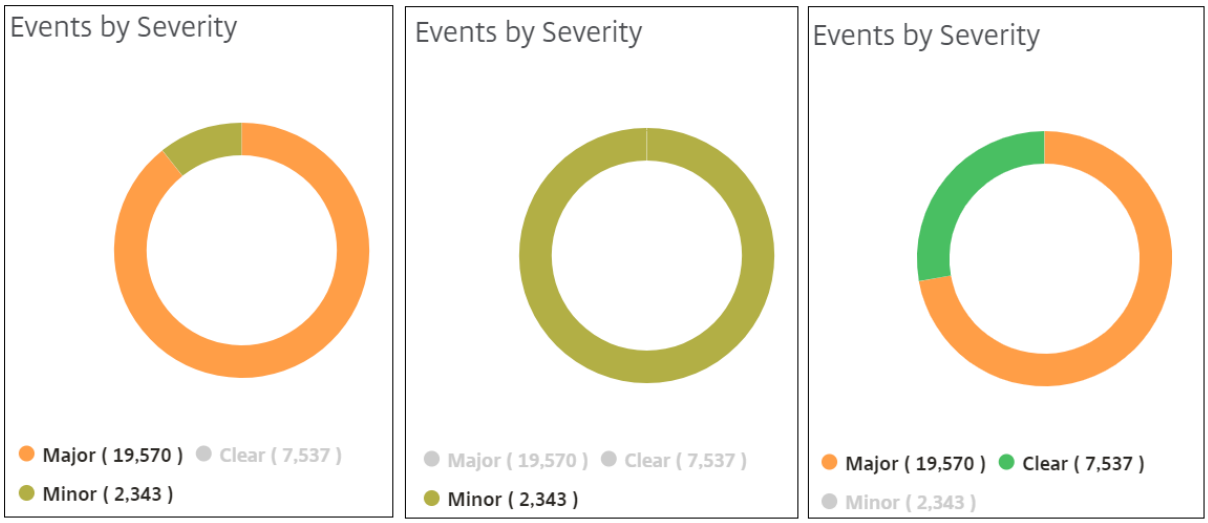


4. Das Donutdiagramm **Ereignisse nach Schweregrad** zeigt eine visuelle Darstellung aller Ereignisse nach ihrem Schweregrad an. Verschiedene Arten von Ereignissen werden als unterschiedliche farbige Abschnitte dargestellt, und die Länge jedes Abschnitts entspricht der Gesamtzahl der Ereignisse dieser Art von Schweregrad.

5. Sie können auf jeden Abschnitt im Donutdiagramm klicken, um die entsprechende Seite auf **Schweregrad basierende Ereignisse** anzuzeigen, auf der die folgenden Details für den ausgewählten Schweregrad für die ausgewählte Dauer angezeigt werden:

   - Instanzquelle
   - Daten der Veranstaltung
   - Kategorie der Ereignisse, die von der Citrix ADC-Instanz generiert werden
   - Nachrichtenbenachrichtigung gesendet

> **Hinweis**
>
> Unterhalb des Donutdiagramms können Sie eine Liste der Schweregrade sehen, die im Diagramm dargestellt werden. Standardmäßig werden in einem Donutdiagramm alle Ereignisse aller Schweregradtypen angezeigt. Daher werden alle Schweregradtypen in der Liste hervorgehoben. Sie können die Schweregradtypen umschalten, um den gewählten Schweregrad leichter anzuzeigen und zu überwachen.

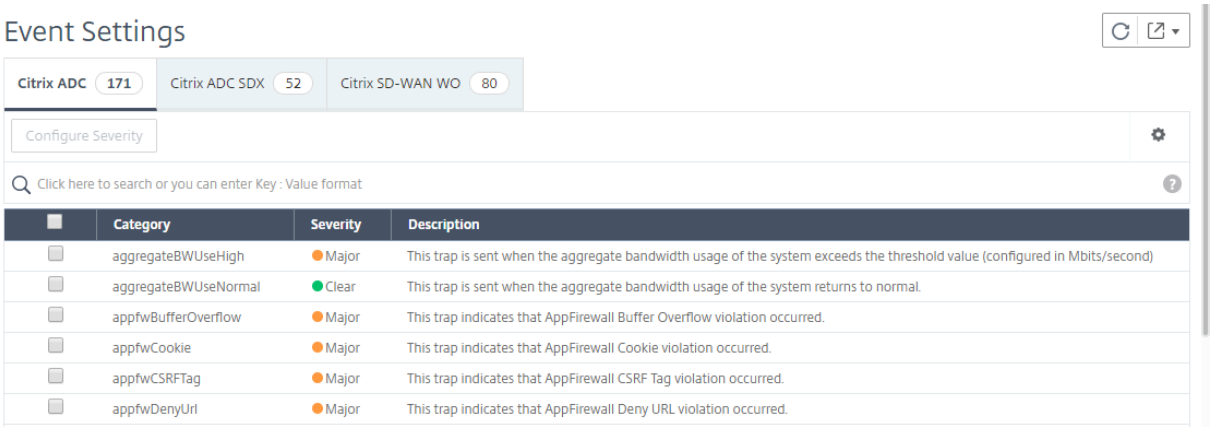


So zeigen Sie Citrix ADC SNMP-Trapdetails auf Citrix ADM an:

Sie können nun die Details der einzelnen SNMP-Traps anzeigen, die von den verwalteten Citrix ADC-Instanzen empfangen wurden, im Citrix ADM auf der Seite **Ereigniseinstellungen**. Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Ereigniseinstellungen**. Für ein bestimmtes Trap, das von Ihrer Instanz empfangen wird, können Sie die folgenden Details im tabellarischen Format anzeigen:

- **Kategorie** - Gibt die Kategorie der Instanz an, zu der das Ereignis gehört.
- **Schweregrad** - Der Schweregrad des Ereignisses wird durch Farben und seinen Schweregrad angezeigt.
- **Beschreibung** - Gibt die Meldungen an, die dem Ereignis zugeordnet sind.

Beispiel: Bei einem Ereignis mit der Trap-Kategorie **monRespTimeoutBelowThresh** wird die Beschreibung des Traps als “Diese Trap wird gesendet, wenn das Antwort-Timeout für einen Monitor-Prüfpunkt wieder normal ist, kleiner als der eingestellte Schwellenwert” angezeigt.



Anzeigen und Exportieren von Syslog-Nachrichten

April 28, 2021

Sie können Syslog-Nachrichten anzeigen, ohne sich bei Citrix Application Delivery Management (Citrix ADM) anzumelden, indem Sie einen Export aller auf dem Server empfangenen Syslog-Nachrichten planen. Sie können Syslog-Nachrichten, die auf Ihren Citrix Application Delivery Controller Instanzen (Citrix ADC) generiert werden, in PDF-, CSV-, PNG- und JPEG-Formaten exportieren. Außerdem können Sie den Export dieser Berichte an bestimmte E-Mail-Adressen in verschiedenen Intervallen planen.

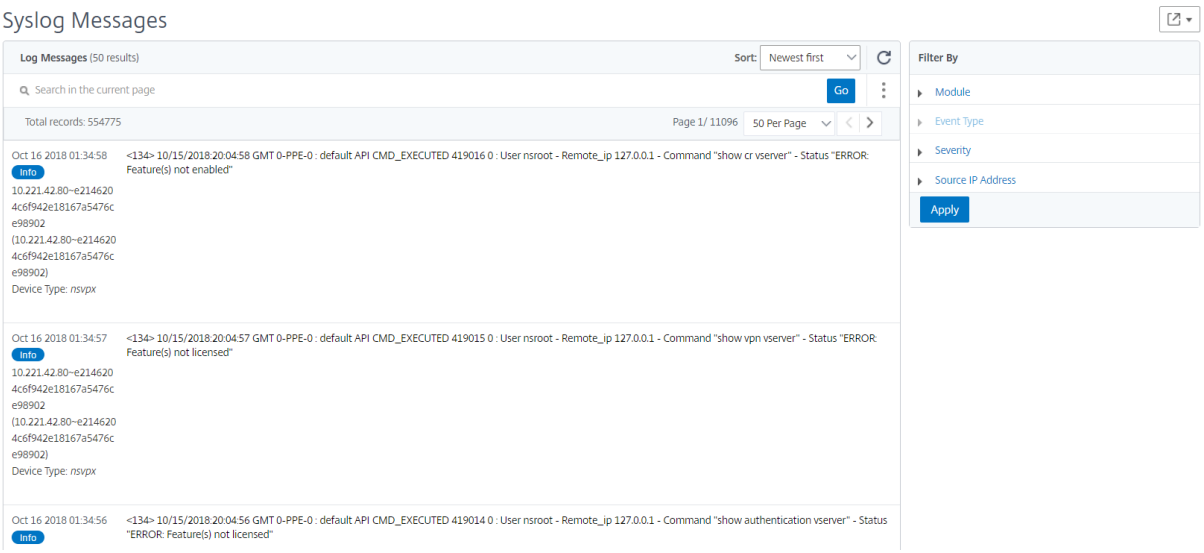
> **Hinweis**
>
> Weitere Informationen zum Konfigurieren eines Syslog-Servers und zum Anzeigen von Syslog-Meldungen auf Citrix ADM finden Sie unterAnzeigen von Überwachungsinformationen von Citrix ADM.

Anzeigen von Syslog-Nachrichten

Sie können alle Syslog-Nachrichten anzeigen, die auf Ihren verwalteten Citrix ADC-Instanzen generiert wurden. Um die Nachrichten anzuzeigen, müssen Sie die Instanzen so konfigurieren, dass die Syslog-Nachrichten an den Citrix ADM -Server umgeleitet werden. Die Syslog-Meldungen werden zentral in der Datenbank gespeichert und stehen im Syslog Viewer für Auditzwecke zur Verfügung. Sie können diese Protokollierungsinformationen kombinieren und Berichte für Analysen aus den gesammelten Daten ableiten.

Sie können syslog auch so konfigurieren, dass verschiedene Arten von Ereignissen protokolliert werden.

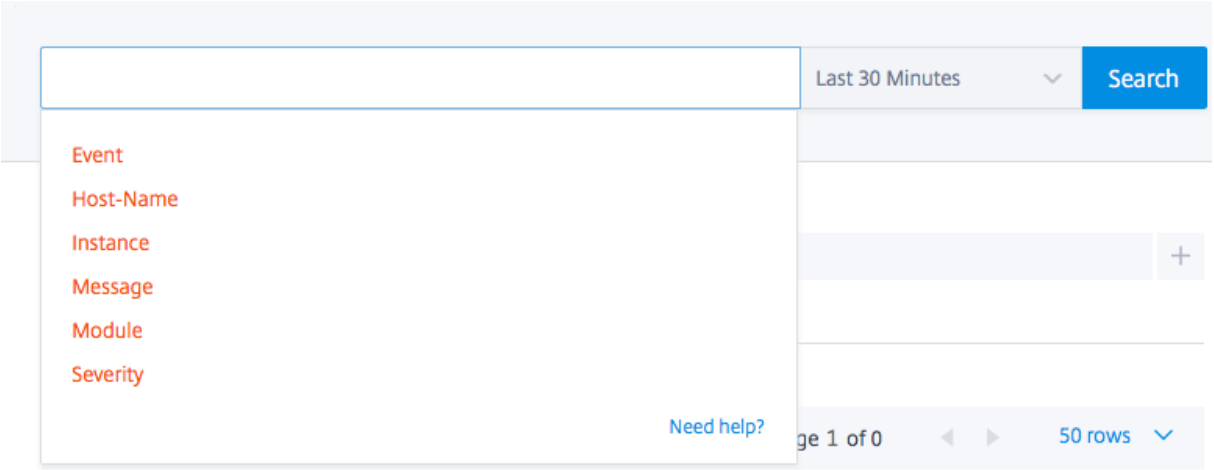
Um den Syslog-Viewer anzuzeigen, navigieren Sie zu **Netzwerke** > **Ereignisse** > **Syslog-Nachrichten**. Wählen Sie die entsprechenden Filter aus, um Ihre Systemprotokollmeldungen anzuzeigen.



Syslog-Nachrichten durchsuchen

Sie können Filter verwenden, um Syslog-Nachrichten und Audit-Protokoll-Nachrichten zu durchsuchen, um Ihre Ergebnisse einzugrenzen und genau das zu finden, wonach Sie suchen und in Echtzeit.

Um Syslog-Nachrichten nach allen ADC-Instanzen in der ADM-Software zu durchsuchen, navigieren Sie über die ADM-GUI zu **Netzwerke > Ereignisse > Syslog-Nachrichten**. Die neuen Filterkategorien sind Instanz, Modul, Ereignis, Schweregrad und Nachricht.



Um alle in der ADM-Software vorhandenen Überwachungsprotokollmeldungen des ADM-Systems zu durchsuchen, navigieren Sie über die ADM-Benutzeroberfläche zu **Konto > Überwachungsprotokollmeldungen**. Die neuen Filterkategorien sind Instanz, Modul, Ereignis, Schweregrad und Nachricht.

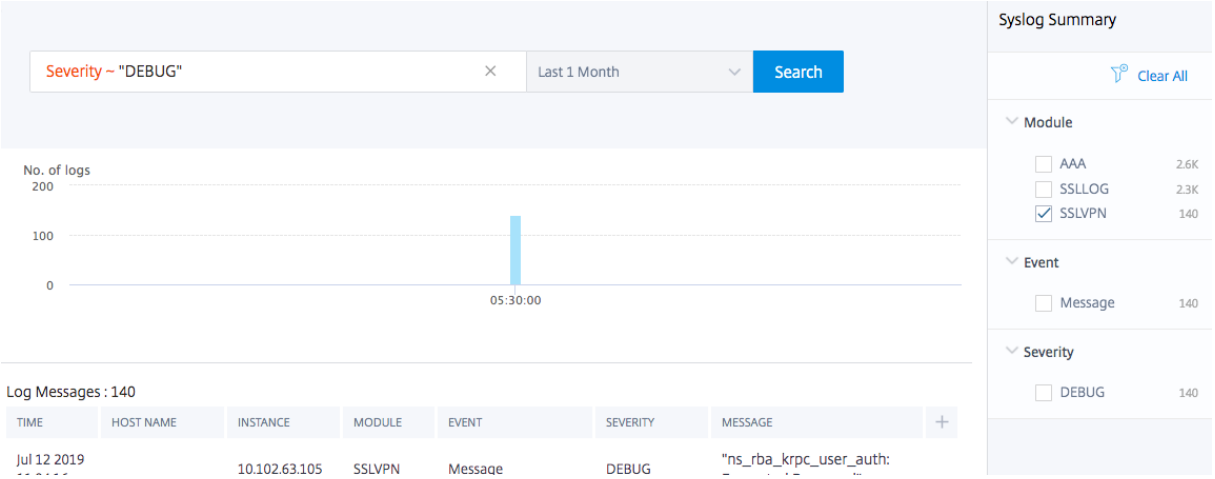
Um Überwachungsprotokollmeldungen nach allen im ADM vorhandenen Anwendungen zu suchen,

navigieren Sie über die ADM-Benutzeroberfläche zu **Netzwerk> Netzwerkfunktionen>Auditing**.

Um die Audit-Logmeldungen nach einer bestimmten Anwendung auf dem ADM zu durchsuchen, navigieren Sie über die ADM-GUI zu **Application>Dashboard** und wählen Sie den virtuellen Server aus, nach dem Sie die Audit-Logmeldungen durchsuchen möchten. Klicken Sie als Nächstes auf die Registerkarte **Überwachungsprotokoll**.

Nachdem Sie eine Filterkategorie ausgewählt haben, geben Sie an, ob sie dem Suchbegriff entspricht oder enthält.

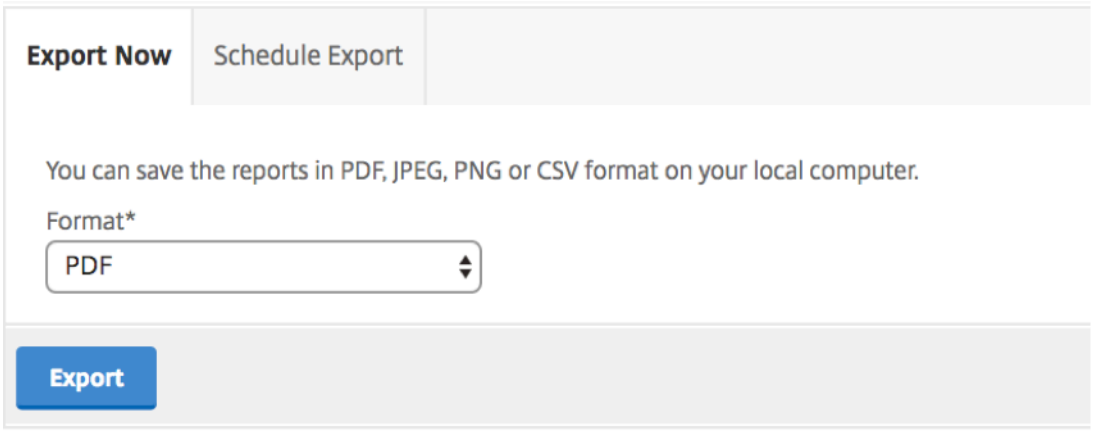
Fügen Sie als Nächstes den Suchbegriff hinzu. Für einige Kategorien wird eine vordefinierte Liste mit Suchbegriffen angezeigt. Standardmäßig beträgt die Suchzeit 1 Tag. Sie können den Zeit- und Datumsbereich ändern, indem Sie auf den Pfeil nach unten klicken. Sie können die Suche weiter einschränken, indem Sie Optionen im Bereich " **Syslog-Zusammenfassung** " oder " **Überwachungsprotokollübersicht** " auswählen.



Exportieren von Syslog-Nachrichten

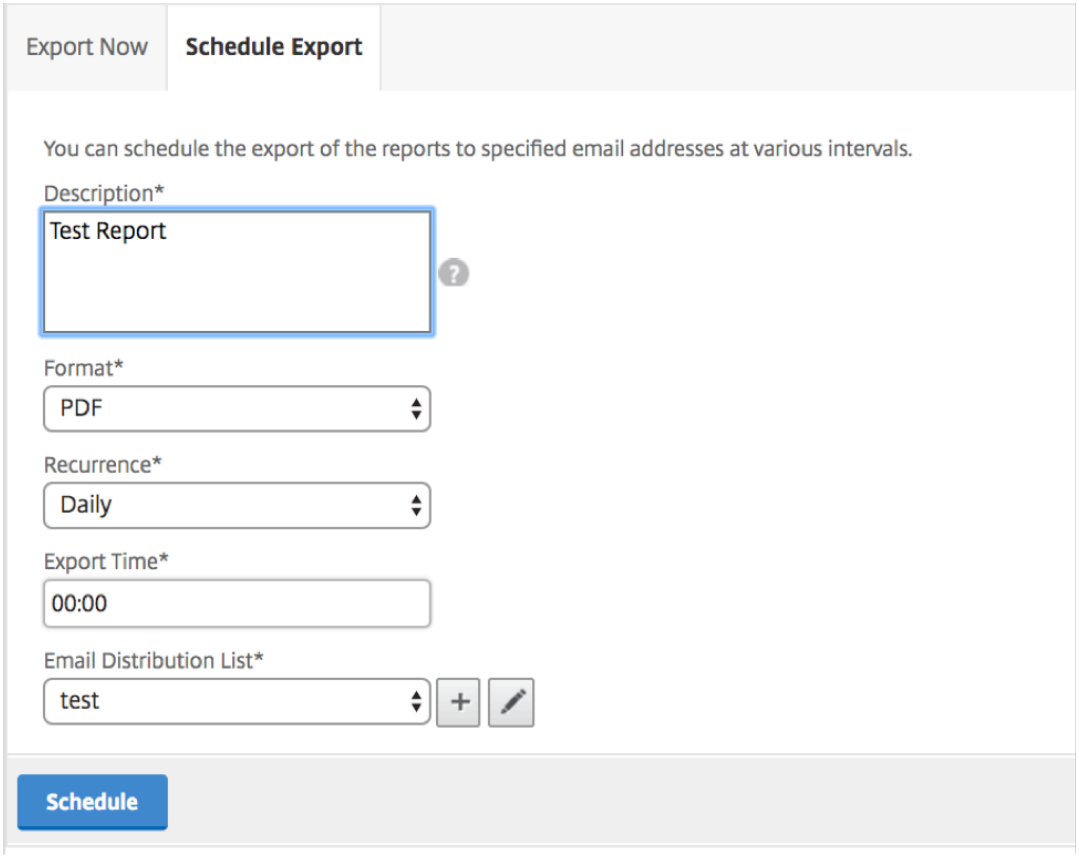
So exportieren Sie einen Syslog-Meldungsbericht mithilfe von Citrix ADM:

1. Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Syslog-Nachrichten**.
2. Klicken Sie im rechten Fensterbereich auf die Schaltfläche Exportieren oben rechts auf der Seite Syslog-Nachrichten.
3. Wählen Sie unter **Jetzt exportieren**das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.



So planen Sie den Export von Syslog-Meldungsberichten mithilfe von Citrix ADM:

1. Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Syslog-Nachrichten**.
2. Klicken Sie auf der Seite **Syslog-Nachrichten** im rechten Fensterbereich auf **Exportieren**.
3. Legen Sie auf der Registerkarte **Bericht planen** die folgenden Parameter fest:
    - **Beschreibung**: Meldung, die den Grund für den Export des Berichts beschreibt.
    - **Format**: Format, in das der Bericht exportiert werden soll.
    - **Wiederholung**: Intervall, in dem der Bericht exportiert werden soll.
    - **Exportzeit**: Der Zeitpunkt, zu dem die Auswertung exportiert werden soll. Geben Sie die Uhrzeit in einem 24-Stunden-Format für Ihre lokale Zeitzone ein.
    - **E-Mail-Verteilerliste**: Liste der Empfänger, die den Bericht per E-Mail erhalten sollen. Wählen Sie eine E-Mail-Verteilerliste aus der bereitgestellten Liste aus. Eine E-Mail wird ausgelöst, wenn der Bericht generiert wird und die geplanten Zeitkriterien erfüllt. Wenn Sie eine E-Mail-Verteilerliste erstellen möchten, klicken Sie auf **+**, und geben Sie Details zum E-Mail-Server und zum E-Mail-Profil an.



Syslog-Nachrichten unterdrücken

April 28, 2021

Wenn Citrix Application Delivery Management (ADM) als Syslog-Server konfiguriert ist, empfängt es alle Syslog-Nachrichten von den konfigurierten Instanzen von Citrix Application Delivery Controller (Citrix ADC). Möglicherweise möchten Sie viele Nachrichten nicht sehen. Zum Beispiel könnten Sie nicht daran interessiert sein, alle Nachrichten auf Informationsebene zu sehen. Sie können nun einige Syslog-Nachrichten verwerfen, die Sie nicht interessieren. Sie können einige der in ADM eingehenden Syslog-Nachrichten unterdrücken, indem Sie einige Filter einrichten. Citrix ADM löscht alle Nachrichten, die mit den Kriterien übereinstimmen. Diese gelöschten Nachrichten werden nicht auf der Citrix ADM GUI angezeigt, und diese Nachrichten werden auch nicht in der Citrix ADM-Datenbank des Kunden gespeichert.

Sie können einige der in ADM eingehenden protokollierten Syslog-Nachrichten unterdrücken, indem Sie einige Filter einrichten. Die beiden Filter, die zum Unterdrücken von Syslog-Nachrichten verwendet werden können, sind Schweregrad und Einrichtung. Sie können auch Nachrichten unterdrücken, die von einer bestimmten Citrix ADC-Instanz oder mehreren Instanzen stammen. Sie können auch ein

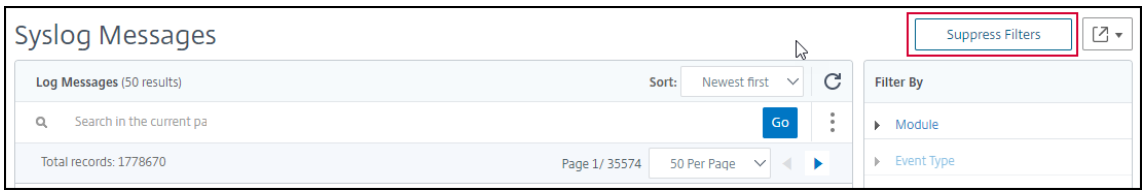
Textmuster für Citrix ADM bereitstellen, um Nachrichten zu suchen und zu unterdrücken. Citrix ADM löscht alle Nachrichten, die mit den Kriterien übereinstimmen. Diese gelöschten Nachrichten werden nicht auf der Citrix ADM GUI angezeigt, und diese Nachrichten werden auch nicht in der Kundendatenbank gespeichert. Daher wird eine gute Menge an Speicherplatz auf dem Speicherserver gespeichert.

Einige Anwendungsfälle zum Unterdrücken von Syslog-Nachrichten sind wie folgt:

- Wenn Sie alle Nachrichten auf Informationsebene ignorieren möchten, unterdrücken Sie Ebene 6 (informativ)
- Wenn Sie nur Firewall-Fehlerbedingungen aufzeichnen möchten, unterdrücken Sie alle Ebenen außer Stufe 3 (Fehler)

Unterdrücken von Syslog-Nachrichten durch Erstellen von Filtern

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Ereignisse** > **Syslog-Nachrichten**.
2. Klicken Sie auf **Filter unterdrücken**.

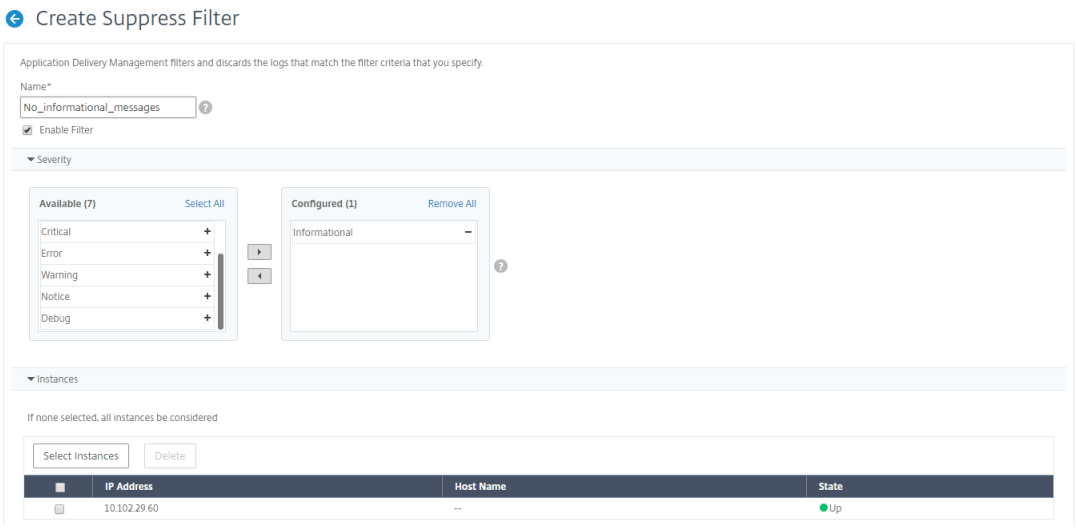


3. Klicken Sie auf der Seite **Filter unterdrücken** auf **Hinzufügen**.
4. Aktualisieren **Sie auf der Seite Unterdrückungsfilter erstellen** die folgenden Informationen:
   a) **Name** - Geben Sie einen Namen für den Filter ein.

   > **Hinweis:**
   >
   > Wenn verschiedene Benutzer unterschiedliche Zugriffsrechte auf mehrere Citrix ADC-Instanzen haben, müssen unterschiedliche Filter für verschiedene Instanzen erstellt werden, da Benutzer nur die Filter sehen können, in denen sie Zugriff auf alle Instanzen haben.

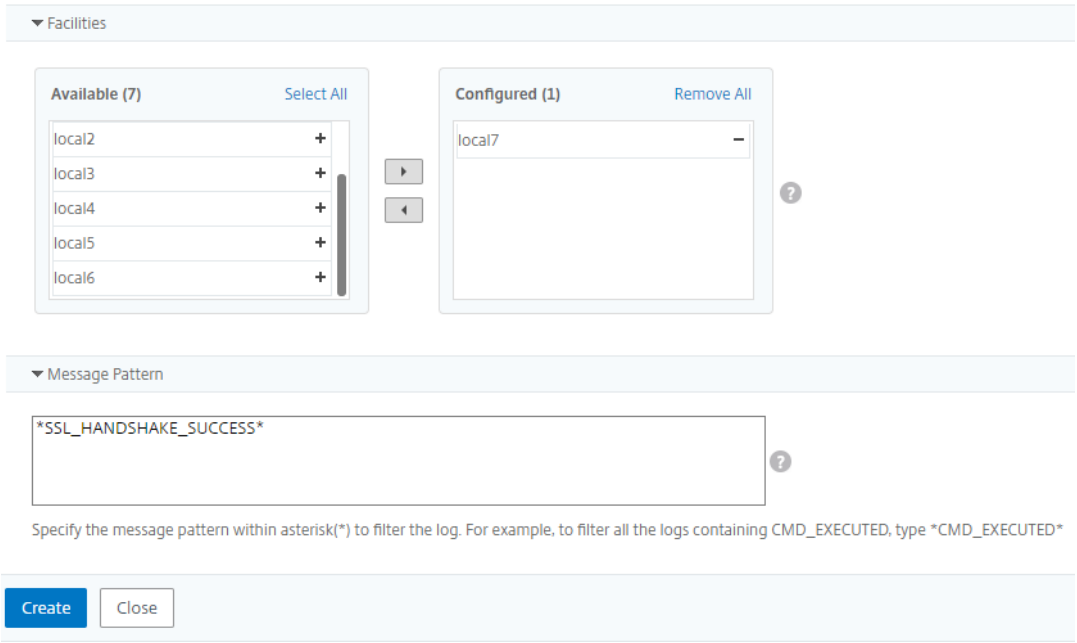
   b) **Schweregrad** - Wählen Sie die Protokollstufen aus, für die Sie die Nachrichten unterdrücken müssen, und fügen Sie sie hinzu.Wenn Sie
   z. B. keine eingehenden Informationsmeldungen anzeigen möchten, können Sie **Informationen** auswählen, um diese Nachrichten zu unterdrücken.

   c) **Instanzen** - Wählen Sie die Citrix ADC-Instanzen aus, für die die Syslog-Meldungen konfiguriert wurden.



d) **Einrichtungen** - Wählen Sie die Möglichkeit aus, um Nachrichten basierend auf der Quelle, die sie generiert, zu unterdrücken.

e) **Nachrichtenmuster** - Sie können auch ein Textmuster eingeben, das von Sternchen (*) umgeben ist, um die Nachrichten zu unterdrücken. Die Nachrichten werden nach der Textmusterzeichenfolge gesucht und die Meldungen, die dieses Muster enthalten, werden unterdrückt.

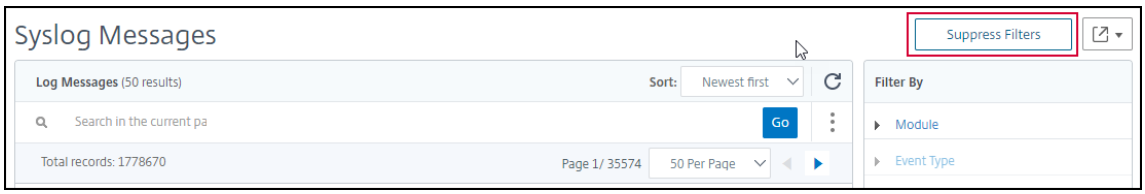


Deaktivieren des Filters

Damit die Nachrichten in Citrix ADM angezeigt werden können, müssen Sie den Filter deaktivieren.

1. Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Syslog-Nachrichten**.

2. Klicken Sie auf **Filter unterdrücken**.



3. Wählen Sie auf der Seite **Filter unterdrücken** den Filter aus, und klicken Sie auf **Bearbeiten**.
4. Deaktivieren Sie auf der Seite **Unterdrückungsfilter konfigurieren** das Kontrollkästchen **Filter aktivieren**, um den Filter zu deaktivieren.

SSL-Dashboard

April 28, 2021

Citrix Application Delivery Management (Citrix ADM) optimiert jetzt alle Aspekte der Zertifikatverwaltung für Sie. Über eine einzige Konsole können Sie automatisierte Richtlinien einrichten, um den richtigen Aussteller, die richtige Schlüsselstärke und korrekte Algorithmen sicherzustellen, während Sie nicht verwendete oder bald ablaufende Zertifikate im Auge behalten. Um das SSL-Dashboard von Citrix ADM und seine Funktionen zu verwenden, müssen Sie wissen, was ein SSL-Zertifikat ist und wie Sie Citrix ADM verwenden können, um Ihre SSL-Zertifikate zu verfolgen.

Ein SSL-Zertifikat (Secure Socket Layer), das Teil einer SSL-Transaktion ist, ist ein digitales Eingabeformular (X509), das ein Unternehmen (Domain) oder eine Person identifiziert. Das Zertifikat verfügt über eine Public-Key-Komponente, die für jeden Client sichtbar ist, der eine sichere Transaktion mit dem Server initiieren möchte. Der entsprechende private Schlüssel, der sich sicher auf der Citrix ADC-Appliance befindet, wird verwendet, um die Verschlüsselung und Entschlüsselung asymmetrischer Schlüssel (oder öffentlicher Schlüssel) abzuschließen.

Sie können ein SSL-Zertifikat und einen Schlüssel auf eine der folgenden Arten beziehen:

- Von einer autorisierten Zertifizierungsstelle (CA)
- Durch Generieren eines neuen SSL-Zertifikats und eines neuen Schlüssels auf der Citrix ADC-Appliance

Citrix ADM bietet eine zentrale Ansicht der in allen verwalteten Citrix ADC-Instanzen installierten SSL-Zertifikate. Auf dem SSL-Dashboard können Sie Diagramme anzeigen, mit denen Sie Zertifikataussteller, wichtige Stärken, Signaturalgorithmen, abgelaufene oder nicht verwendete Zertifikate usw. verfolgen können. Sie können auch die Verteilung der SSL-Protokolle sehen, die auf Ihren virtuellen Servern ausgeführt werden, und die Schlüssel, die auf ihnen aktiviert sind.

Sie können auch Benachrichtigungen einrichten, um Sie darüber zu informieren, wann Zertifikate ablaufen werden, und Informationen darüber enthalten, welche Citrix ADC-Instanzen diese Zertifikate

verwenden.

Sie können ein Citrix ADC-Instanzzertifikat mit einem Zertifizierungsstellenzertifikat verknüpfen. Stellen Sie jedoch sicher, dass die Zertifikate, die Sie mit demselben Zertifizierungsstellenzertifikat verknüpfen, dieselbe Quelle und denselben Aussteller haben. Nachdem Sie ein oder mehrere Zertifikate mit einem Zertifizierungsstellenzertifikat verknüpft haben, können Sie die Verknüpfung aufheben.

> **Hinweis**
>
> Sie können auch einen Server der Venafi Trust Protection Platform mit ADM verwenden, um die Verwaltung des gesamten Lebenszyklus von SSL-Zertifikaten zu automatisieren. Weitere Informationen finden Sie unter Automatisieren Sie die SSL-Zertifikatsverwaltung.

Verwenden des SSL-Dashboards

April 28, 2021

Sie können das SSL-Zertifikat-Dashboard in Citrix Application Delivery Management (Citrix ADM) verwenden, um Diagramme anzuzeigen, die Ihnen helfen, Zertifikataussteller, Schlüsselstärken und Signaturalgorithmen zu verfolgen. Das SSL-Zertifikat-Dashboard zeigt außerdem Diagramme an, die Folgendes angeben:

- Anzahl der Tage, nach denen Zertifikate ablaufen
- Anzahl der verwendeten und nicht verwendeten Zertifikate
- Anzahl selbstsignierter und von der Zertifizierungsstelle signierter Zertifikate
- Zahl der Emittenten
- Signaturalgorithmen
- SSL-Protokolle
- Top 10 Instanzen nach Anzahl der verwendeten Zertifikate

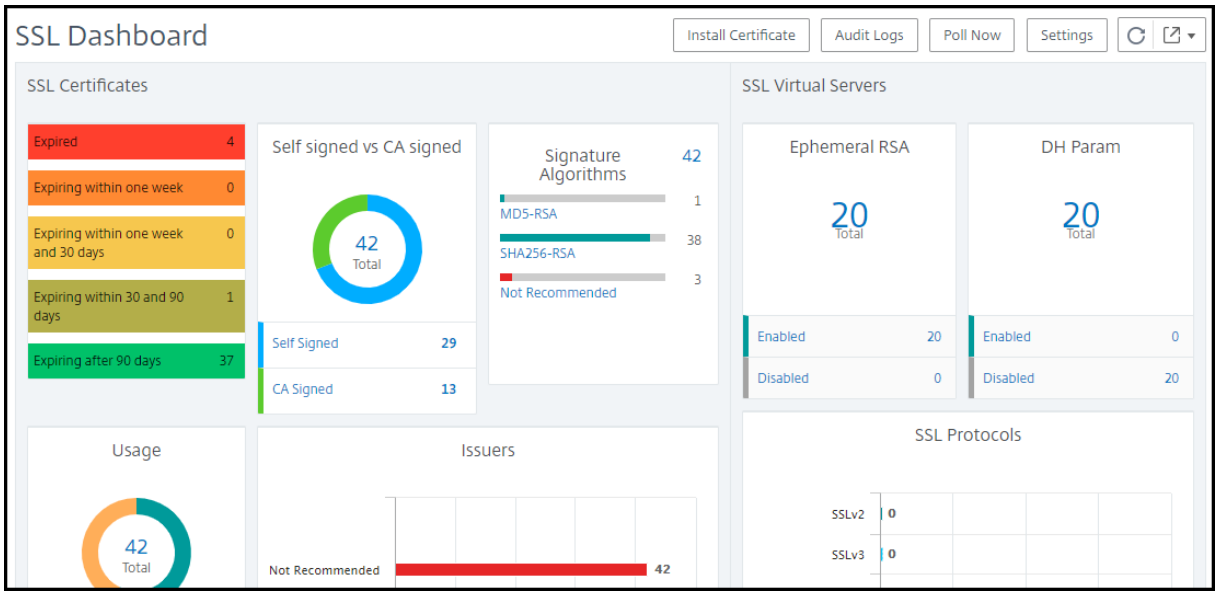
Überwachen von SSL-Zertifikaten

Sie können das SSL-Dashboard in Citrix ADM verwenden, um Ihre Zertifikate zu überwachen, wenn Ihr Unternehmen eine SSL-Richtlinie hat, in der Sie bestimmte SSL-Zertifikatanforderungen definiert haben, z. B. alle Zertifikate müssen Mindestschlüsselstärken von 2048 Bit haben und eine vertrauenswürdige Zertifizierungsstelle sie autorisieren muss.

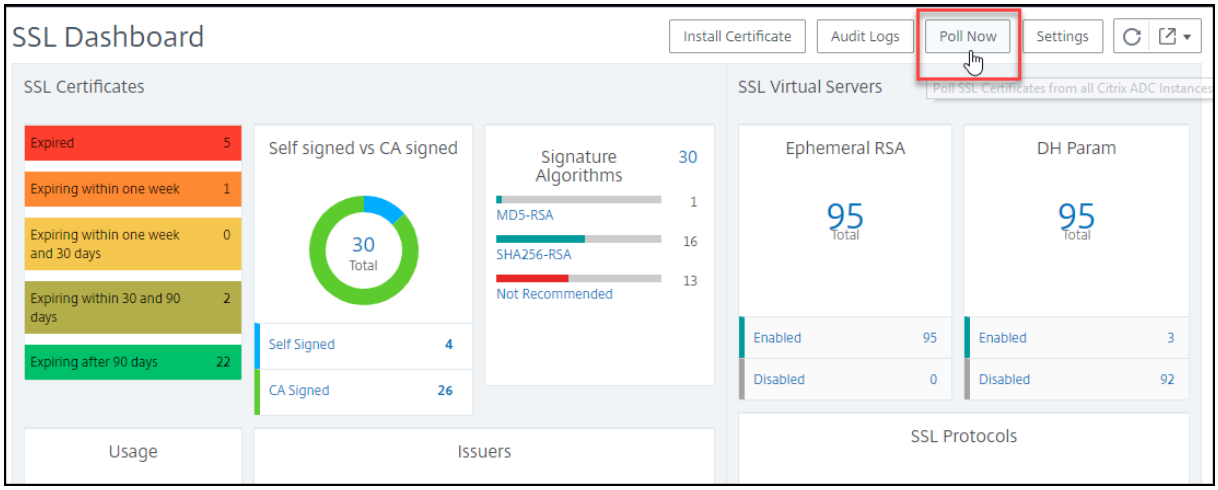
In einem anderen Beispiel haben Sie möglicherweise ein neues Zertifikat hochgeladen, aber vergessen, es an einen virtuellen Server zu binden. Das SSL-Dashboard hebt die verwendeten oder nicht verwendeten SSL-Zertifikate hervor. Im Abschnitt **Verwendung** sehen Sie die Anzahl der installierten Zertifikate und die Anzahl der verwendeten Zertifikate. Sie können weiter auf das Diagramm

klicken, um den Namen der Zertifikate, die Instanz, für die es verwendet wird, ihre Gültigkeit, den Signaturalgorithmus usw. anzuzeigen.

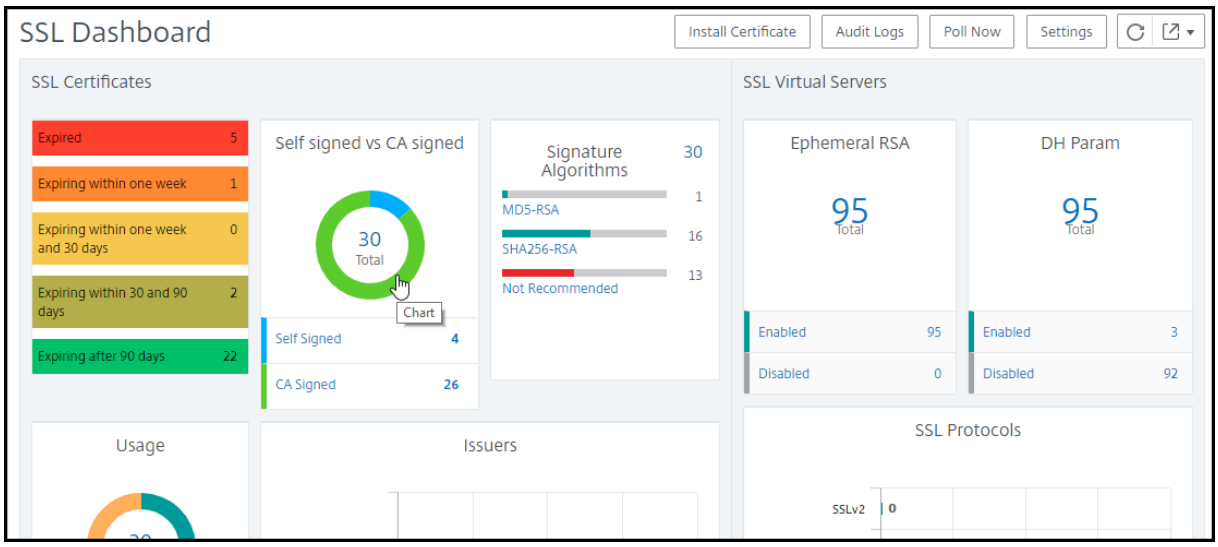
Um SSL-Zertifikate in Citrix ADM zu überwachen, navigieren Sie zu **Netzwerke** > **SSL-Dashboard**.



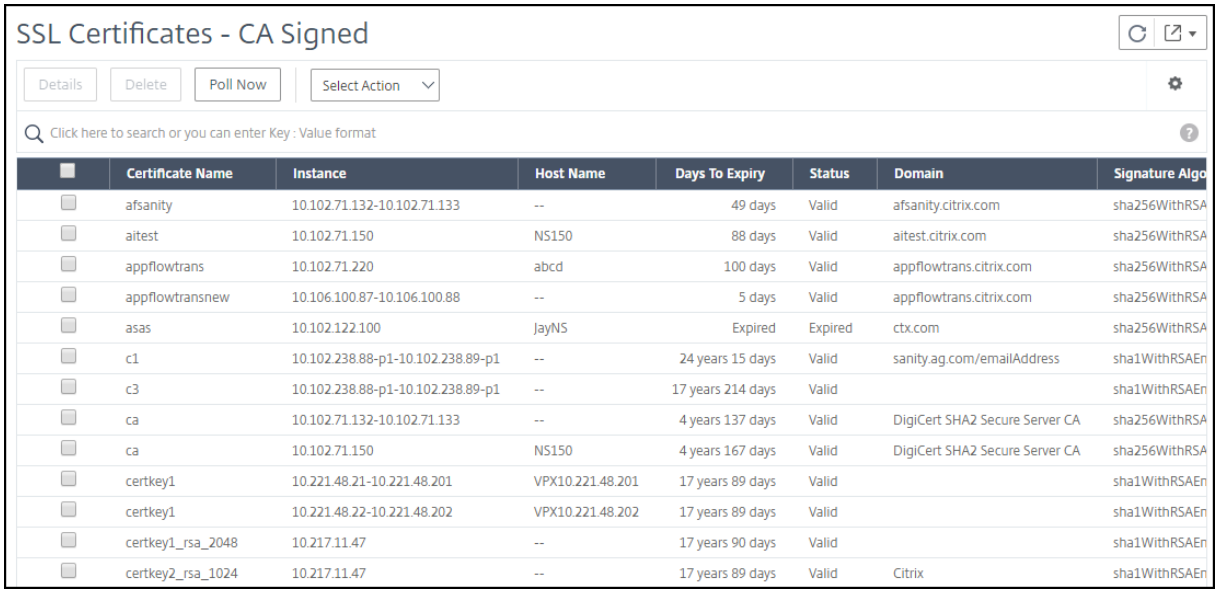
Mit Citrix ADM können Sie SSL-Zertifikate abfragen und alle SSL-Zertifikate der Instanzen sofort Citrix ADM hinzufügen. Navigieren Sie dazu zu **Netzwerke** > **SSL-Dashboard** und klicken Sie auf **Jetzt abfragen**. Die Seite **Jetzt abfragen** wird geöffnet und bietet die Option an, alle Citrix ADC-Instanzen im Netzwerk abzufragen oder ausgewählte Instanzen abzufragen.



Sie können das Citrix ADM SSL-Dashboard verwenden, um die Details von SSL-Zertifikaten, virtuellen SSL-Servern und SSL-Protokollen anzuzeigen oder zu überwachen. Gesamtzahl sind Hyperlinks, auf die Sie klicken können, um Details zu SSL-Zertifikaten, virtuellen SSL-Servern oder SSL-Protokollen anzuzeigen.



Zum Beispiel, wenn ein Benutzer auf die Zahl 30 klickt unter “Selbstsigniert vs. Zertifizierungsstelle signiert” in der obigen Abbildung wird ein neues Fenster mit Details zu den 30 SSL-Zertifikaten auf den Citrix ADC-Instanzen angezeigt.

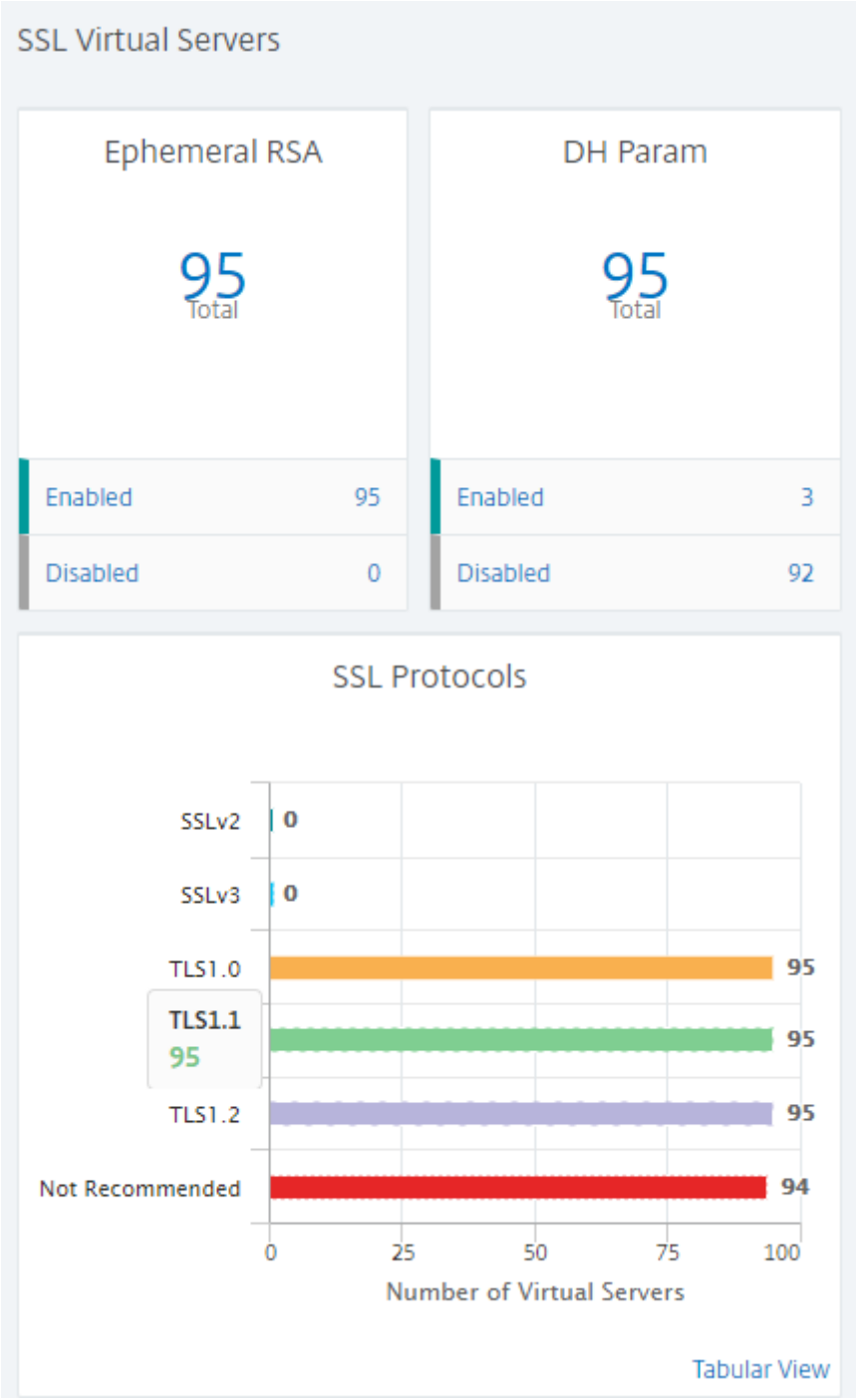


Certificate Name	Instance	Host Name	Days To Expiry	Status	Domain	Signature Algo
afsanity	10.102.71.132-10.102.71.133	--	49 days	Valid	afsanity.citrix.com	sha256WithRSA
aitest	10.102.71.150	NS150	88 days	Valid	aitest.citrix.com	sha256WithRSA
appflowtrans	10.102.71.220	abcd	100 days	Valid	appflowtrans.citrix.com	sha256WithRSA
appflowtransnew	10.106.100.87-10.106.100.88	--	5 days	Valid	appflowtrans.citrix.com	sha256WithRSA
asas	10.102.122.100	JayNS	Expired	Expired	ctx.com	sha256WithRSA
c1	10.102.238.88-p1-10.102.238.89-p1	--	24 years 15 days	Valid	sanity.ag.com/emailAddress	sha1WithRSAEn
c3	10.102.238.88-p1-10.102.238.89-p1	--	17 years 214 days	Valid		sha1WithRSAEn
ca	10.102.71.132-10.102.71.133	--	4 years 137 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
ca	10.102.71.150	NS150	4 years 167 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
certkey1	10.221.48.21-10.221.48.201	VPX10.221.48.201	17 years 89 days	Valid		sha1WithRSAEn
certkey1	10.221.48.22-10.221.48.202	VPX10.221.48.202	17 years 89 days	Valid		sha1WithRSAEn
certkey1_rsa_2048	10.217.11.47	--	17 years 90 days	Valid		sha1WithRSAEn
certkey2_rsa_1024	10.217.11.47	--	17 years 89 days	Valid	Citrix	sha1WithRSAEn

Das Citrix ADM SSL-Dashboard zeigt auch die Verteilung der SSL-Protokolle an, die auf Ihren virtuellen Servern ausgeführt werden. Als Administrator können Sie die Protokolle angeben, die Sie über die SSL-Richtlinie überwachen möchten. Weitere Informationen finden Sie unterKonfigurieren von SSL-Richtlinien. Die unterstützten Protokolle sind SSLv2, SSLv3, TLS1.0, TLS1.1 und TLS1.2. Die auf virtuellen Servern verwendeten SSL-Protokolle werden in einem Balkendiagrammformat angezeigt. Wenn Sie auf ein bestimmtes Protokoll klicken, wird eine Liste der virtuellen Server angezeigt, die dieses Protokoll verwenden.

Ein Donut-Diagramm wird angezeigt, nachdem Diffie-Hellman (DH) oder Ephemere RSA-Schlüssel im SSL-Dashboard aktiviert oder deaktiviert wurden. Diese Schlüssel ermöglichen eine sichere Kommu-

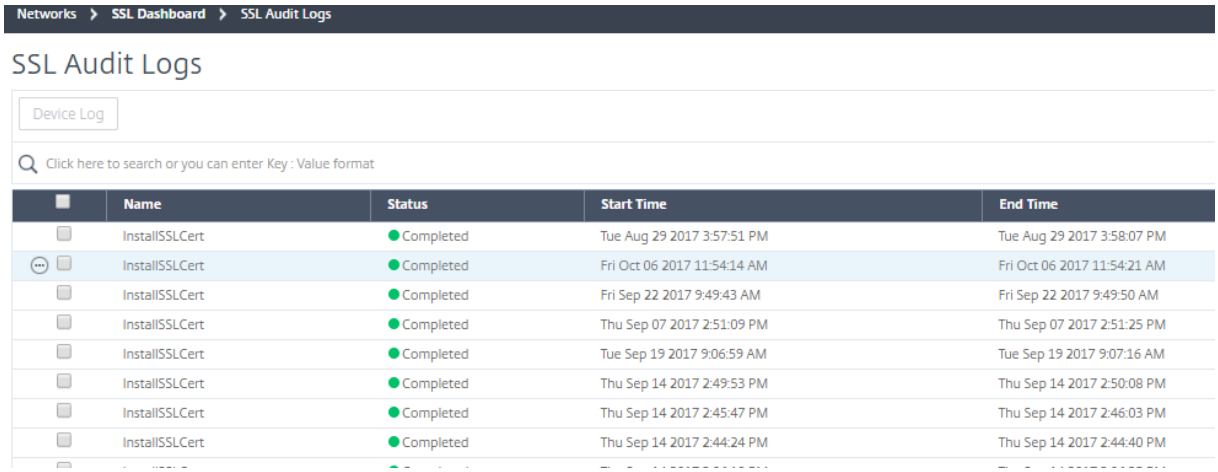
nikation mit Exportclients, selbst wenn das Serverzertifikat keine Exportclients unterstützt, wie bei einem 1024-Bit-Zertifikat. Wenn Sie auf das entsprechende Diagramm klicken, wird eine Liste der virtuellen Server angezeigt, auf denen DH- oder Ephemere RSA-Schlüssel aktiviert sind.



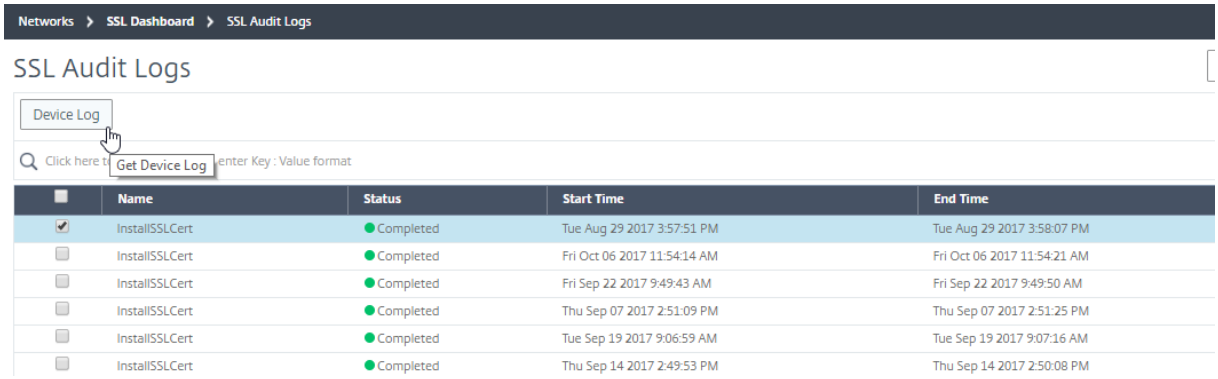
Anzeigen von Überwachungsprotokollen für SSL-Zertifikate

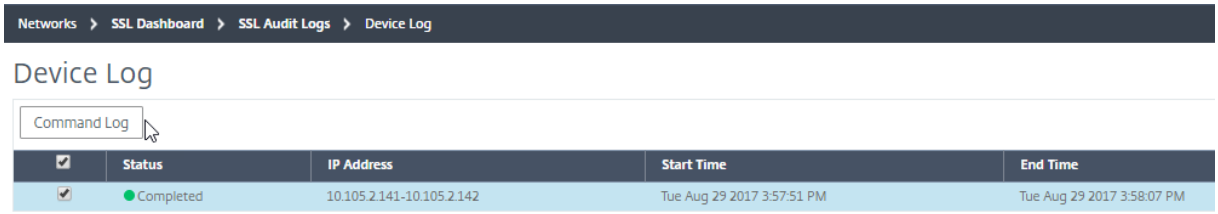
Sie können jetzt Protokolldetails von SSL-Zertifikaten in Citrix ADM anzeigen. In den Protokolldetails werden Vorgänge angezeigt, die mit SSL-Zertifikaten auf Citrix ADM ausgeführt werden, z. B.: Installieren von SSL-Zertifikaten, Verknüpfen und Aufheben der Verknüpfung von SSL-Zertifikaten, Aktualisieren von SSL-Zertifikaten und Löschen von SSL-Zertifikaten. Überwachungsprotokollinformationen sind nützlich, wenn SSL-Zertifikatänderungen überwacht werden, die in einer Anwendung mit mehreren Besitzern durchgeführt werden.

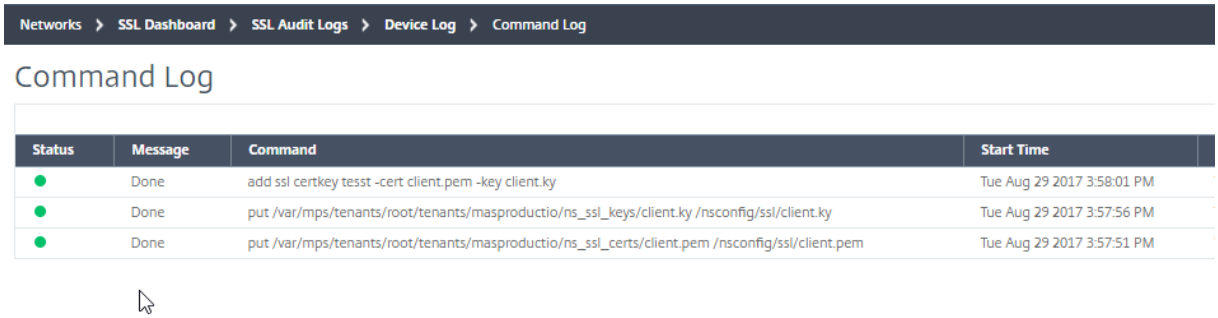
Um ein Überwachungsprotokoll für einen bestimmten Vorgang anzuzeigen, der unter Citrix ADM mithilfe von SSL-Zertifikaten ausgeführt wird, navigieren Sie zu **Netzwerke** > **SSL-Dashboard**, und wählen Sie **Überwachungsprotokolle** aus.



Für einen bestimmten Vorgang, der mit dem SSL-Zertifikat ausgeführt wird, können Sie den Status, die Startzeit und die Endzeit anzeigen. Darüber hinaus können Sie die Instanz anzeigen, für die der Vorgang ausgeführt wurde, und die Befehle, die für diese Instanz ausgeführt werden.





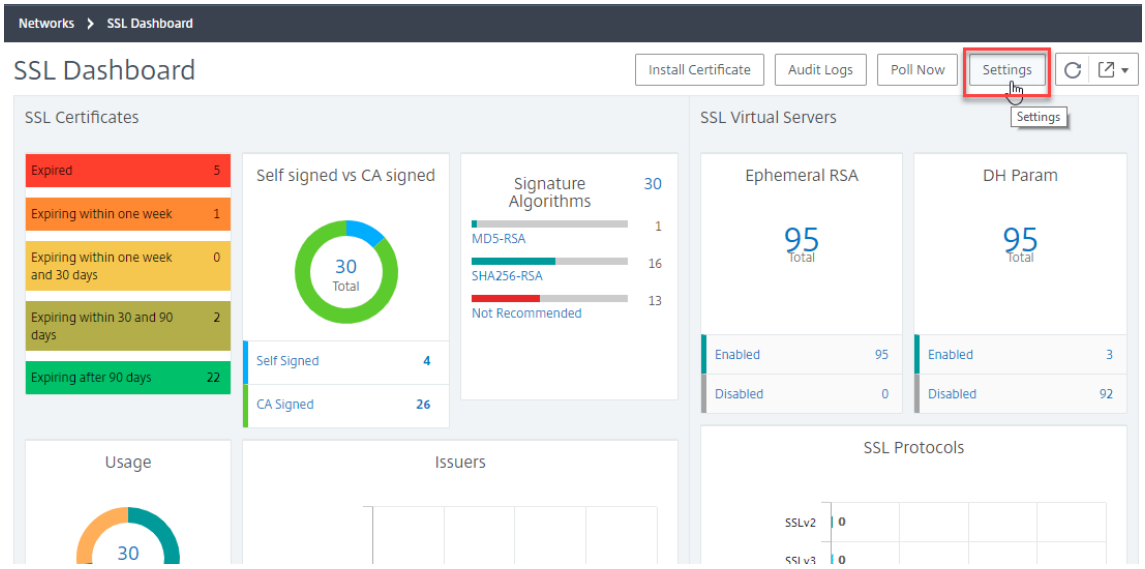


Ausschließen von Citrix ADC Standardzertifikaten auf dem SSL-Dashboard

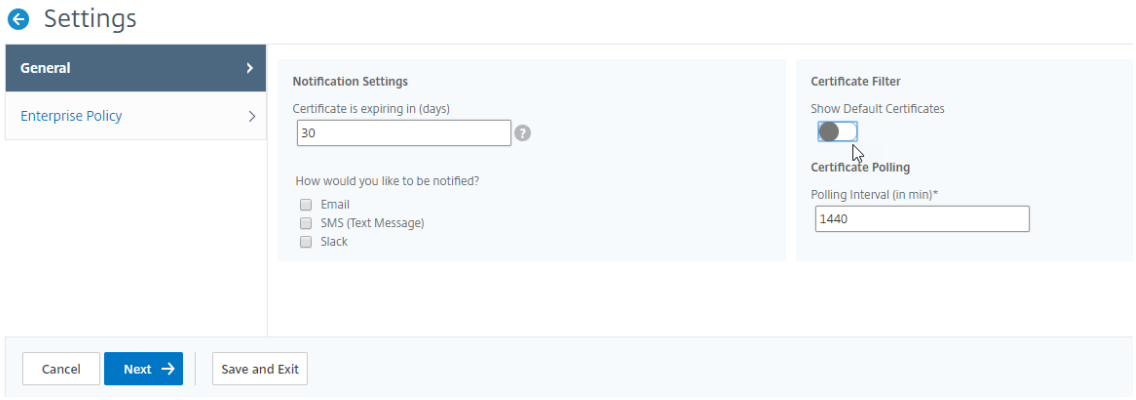
Mit Citrix ADM können Sie Standardzertifikate ein- oder ausblenden, die in den SSL-Dashboard-Diagrammen angezeigt werden, basierend auf Ihren Einstellungen. Standardmäßig werden alle Zertifikate auf dem SSL-Dashboard angezeigt, einschließlich Standardzertifikate.

So blenden Sie Standardzertifikate auf dem SSL-Dashboard ein oder aus:

1. Navigieren Sie zu **Netzwerke** > **SSL-Dashboard** in der Citrix ADM GUI.
2. Klicken Sie auf der Seite **SSL-Dashboard** auf **Einstellungen**.



3. Wählen Sie auf der Seite **Einstellungen** die Option **Allgemein** aus.
4. Deaktivieren Sie im Abschnitt **Zertifikatfilter** die **Standardzertifikate anzeigen**, und wählen Sie **Speichern und Beenden** aus.



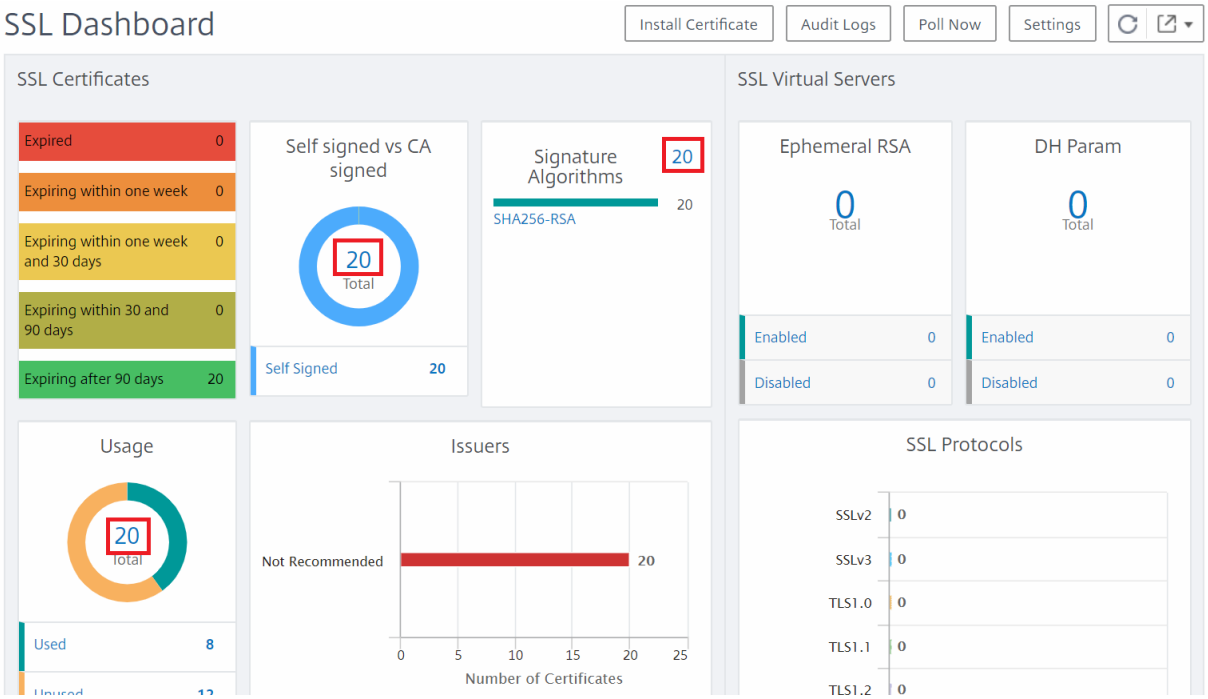
SSL-Zertifikate herunterladen

SSL-Zertifikate müssen pro Instanz einzeln verwaltet werden. Citrix ADM bietet Einblick in alle Zertifikate, die über mehrere Instanzen bereitgestellt werden.

- Sie können auswählen, welche Zertifikate ablaufen und Zertifikatverlängerungen automatisieren.
- Richtlinien können für die zulässigen Arten von Zertifikaten und Unterzeichnerbehörden festgelegt und durchgesetzt werden.
- Sie können die SSL-Zertifikate auch zur Verlängerung herunterladen und später hochladen.

So laden Sie SSL-Zertifikate herunter:

1. Navigieren Sie zu **Netzwerke** > **SSL-Dashboard** in der Citrix ADM GUI.
2. Klicken Sie auf der Seite **SSL Dashboard** auf die Gesamtzahl der SSL-Zertifikate in einem der Diagramme.



1. Klicken Sie auf der Seite **SSL-Zertifikate** auf das Zertifikat, das Sie herunterladen möchten. Zum Beispiel möchten Sie die Datei herunterladen, die in der nächsten Woche abläuft.
2. **Wählen Sie im Listenfeld Aktion** auswählen die Option **Herunterladen** aus.
3. Das Zertifikat wird auf Ihr System heruntergeladen.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Einrichten von Benachrichtigungen für das Ablaufdatum des SSL-Zertifikats

April 28, 2021

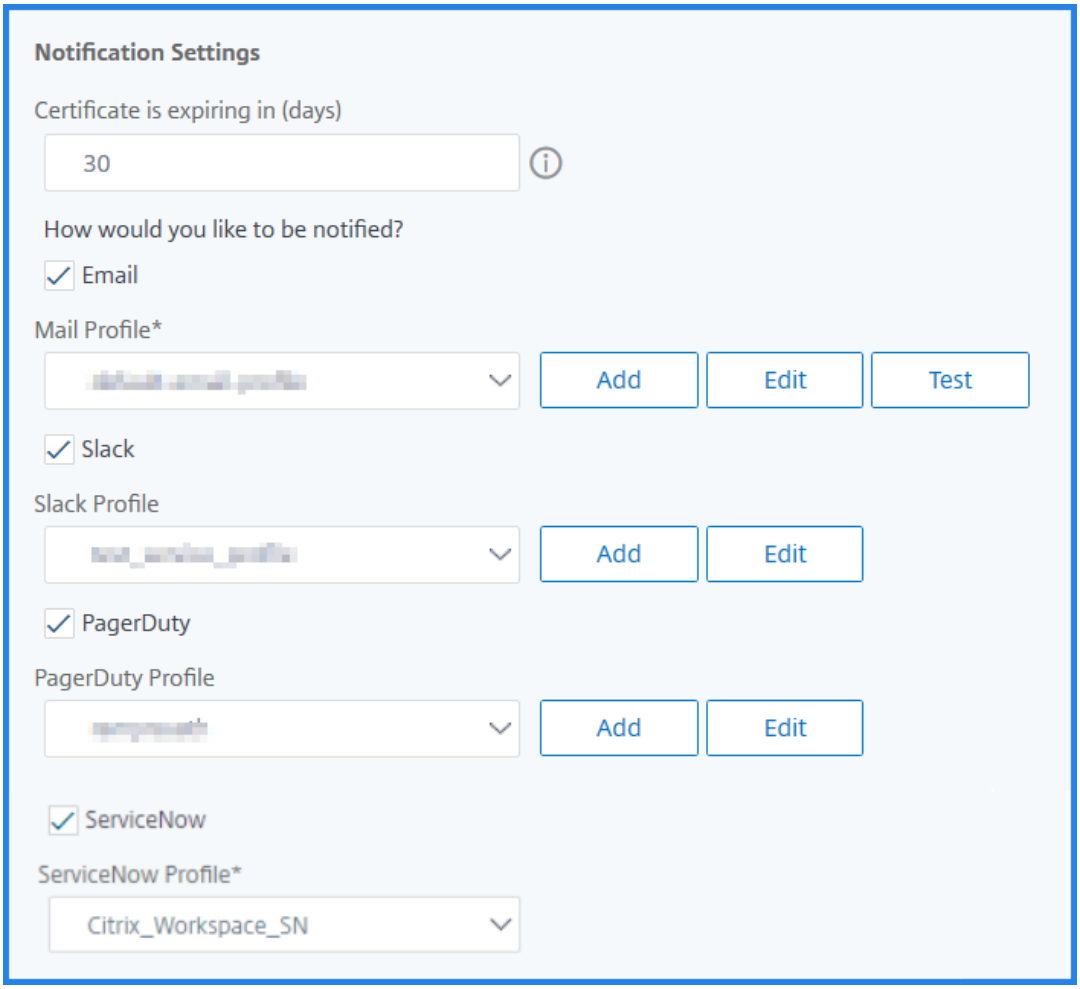
Als Sicherheitsadministrator können Sie Benachrichtigungen konfigurieren, wenn die Zertifikate ablaufen, und Informationen darüber enthalten, welche Citrix ADC-Instanzen diese Zertifikate verwenden. Durch Aktivieren von Benachrichtigungen können Sie Ihre SSL-Zertifikate pünktlich erneuern.

Sie können beispielsweise festlegen, dass eine E-Mail-Benachrichtigung 30 Tage vor Ablauf des Zertifikats eine E-Mail-Verteilerliste gesendet wird.

So richten Sie Benachrichtigungen von Citrix ADM ein:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf der Seite **SSL-Dashboard** auf **Einstellungen**.
3. Klicken Sie auf der Seite **Einstellungen** auf **Allgemein**.
4. Geben Sie im Abschnitt **Benachrichtigungseinstellungen** an, wann die Benachrichtigung in Bezug auf die Anzahl der Tage vor dem Ablaufdatum gesendet werden soll.
5. Wählen Sie die Art der Benachrichtigung, die Sie senden möchten. Wählen Sie im Menü den Benachrichtigungstyp und die Verteilerliste aus. Die Benachrichtigungstypen sind wie folgt:
    - **E-Mail** — Geben Sie einen E-Mail-Server und Profildetails an. Eine E-Mail wird ausgelöst, wenn Ihre Zertifikate ablaufen.
    - **Slack** - Geben Sie ein Pufferprofil an. Eine Benachrichtigung wird gesendet, wenn Ihre Zertifikate ablaufen.
    - **PagerDuty** - Geben Sie ein PagerDuty-Profil an. Basierend auf den in Ihrem PagerDuty-Portal konfigurierten Benachrichtigungseinstellungen wird eine Benachrichtigung gesendet, wenn Ihre Zertifikate ablaufen.
    - **ServiceNow** - Eine Benachrichtigung wird an das standardmäßige ServiceNow-Profil gesendet, wenn Ihre Zertifikate ablaufen.

      > **Wichtig**
      >
      > Stellen Sie sicher, dass der Citrix Cloud ITSM-Adapter für ServiceNow konfiguriert und in den Citrix ADM Dienst integriert ist. Weitere Informationen finden Sie unter Integrieren von Citrix ADM Service mit ServiceNow-Instanz.



6. Klicken Sie auf **Speichern und Beenden**.

Aktualisieren eines installierten Zertifikats

April 28, 2021

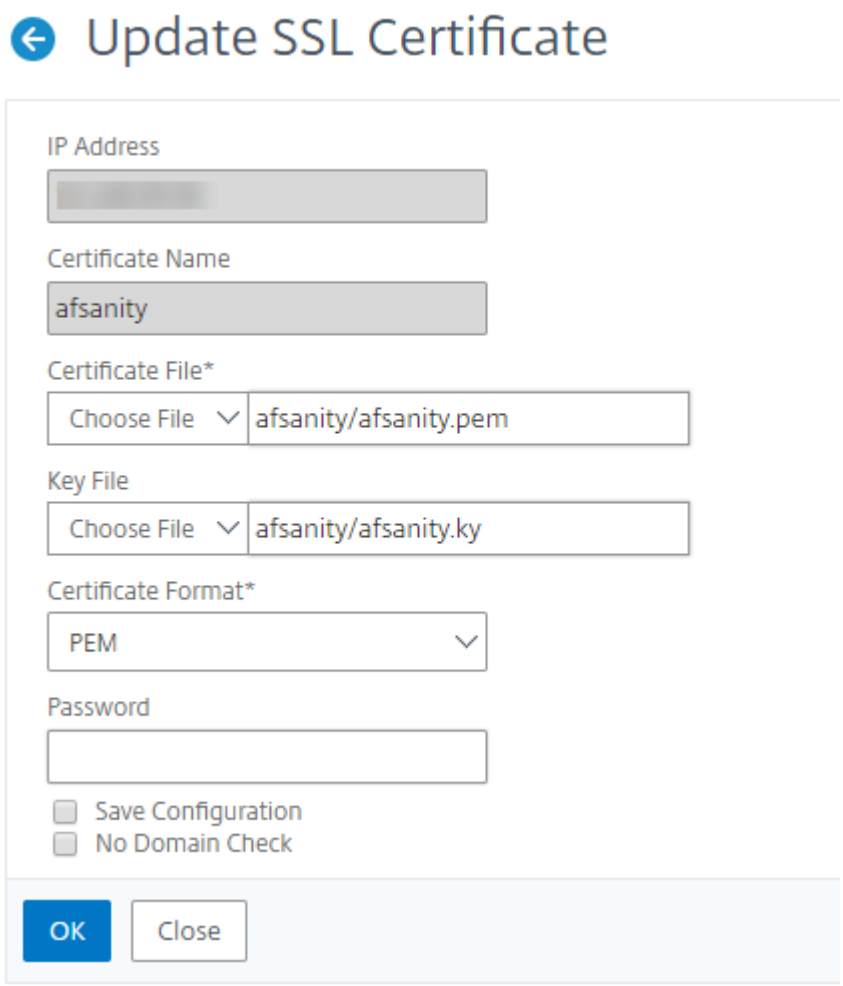
Nachdem Sie ein erneuertes Zertifikat von der Zertifizierungsstelle (Certificate Authority, CA) erhalten haben, können Sie vorhandene Zertifikate aus Citrix Application Delivery Management (Citrix ADM) aktualisieren, ohne sich bei einzelnen Citrix ADC-Instanzen anmelden zu müssen.

So aktualisieren Sie ein SSL-Zertifikat, einen Schlüssel oder beides von Citrix ADM:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf eine der Diagramme, um die Liste der SSL-Zertifikate anzuzeigen.
3. Wählen Sie auf der Seite **SSL-Zertifikate** ein Zertifikat aus und klicken Sie auf **Update**. Alternativ klicken Sie auf das SSL-Zertifikat, um die Details anzuzeigen, und klicken Sie dann oben rechts

auf der Seite **SSL-Zertifikat** auf **Aktualisieren**.

4. Nehmen Sie auf der Seite **SSL-Zertifikat aktualisieren** die erforderlichen Änderungen am Zertifikat, Schlüssel oder beides vor, und klicken Sie auf **OK**.



Installieren von SSL-Zertifikaten auf einer Citrix ADC-Instanz

April 28, 2021

Stellen Sie vor der Installation von SSL-Zertifikaten auf Citrix ADC-Instanzen sicher, dass die Zertifikate von vertrauenswürdigen Zertifizierungsstellen ausgestellt werden. Stellen Sie außerdem sicher, dass die Schlüsselstärke der Zertifikatschlüssel 2.048 Bit oder höher beträgt und dass die Schlüssel mit sicheren Signaturalgorithmen signiert sind.

So installieren Sie ein SSL-Zertifikat von einer anderen Citrix ADC-Instanz:

Sie können ein Zertifikat auch aus einer ausgewählten Citrix ADC-Instanz importieren und es auf andere zielgerichtete Citrix ADC-Instanzen von der Citrix ADM GUI anwenden.

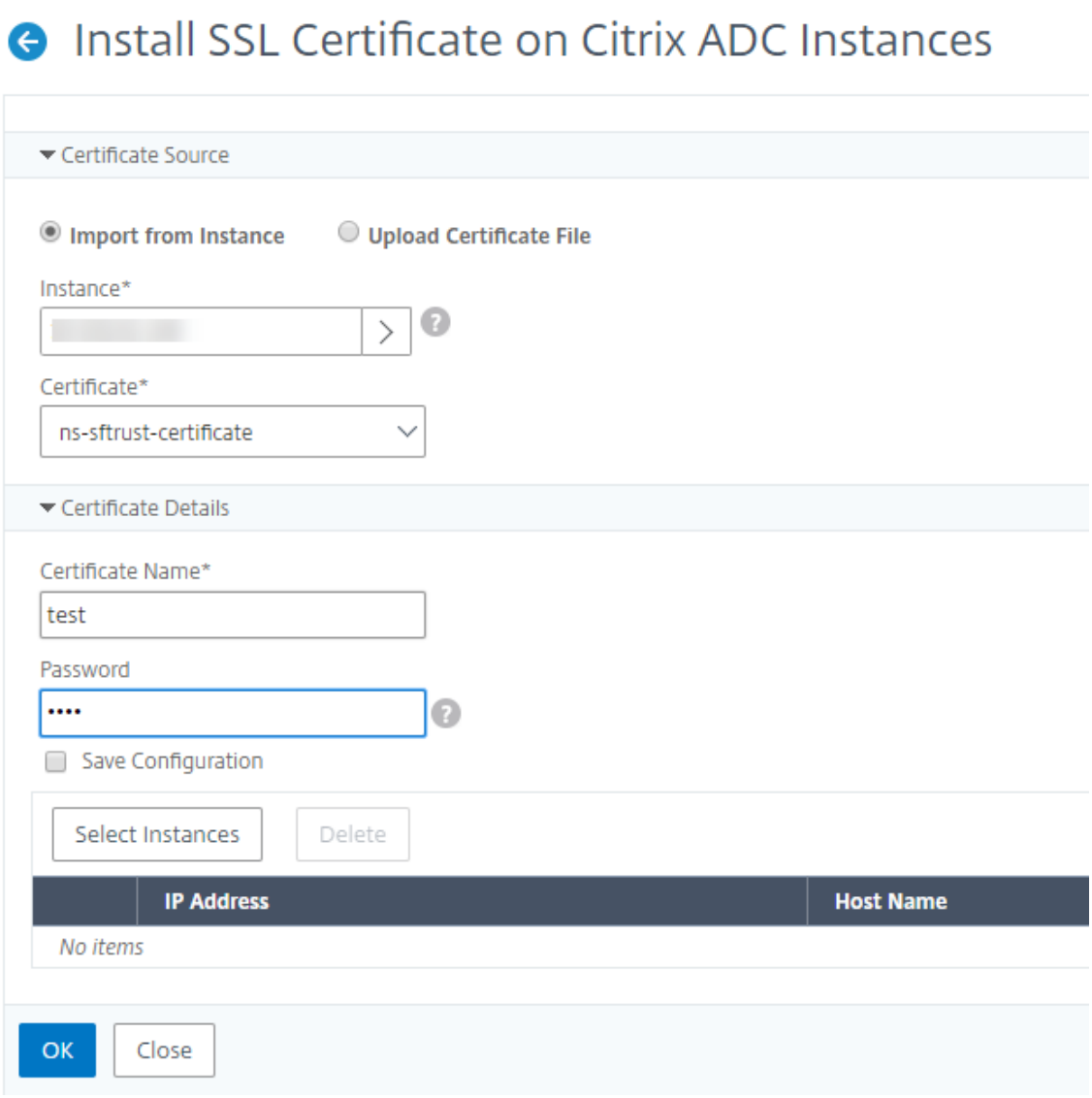
1. Navigieren Sie zu **Netzwerke** > **SSL Dashboard**.
2. Klicken Sie in der rechten oberen Ecke des SSL-Dashboards auf **Zertifikat installieren**.
3. Geben Sie auf der Seite **SSL-Zertifikat auf Citrix ADC-Instanzen installieren** die folgenden Parameter an:
   a) Zertifikatquelle

      Wählen Sie die Option **aus Instanz importieren** aus.

      - Wählen Sie die **Instanz** aus, aus der Sie das Zertifikat importieren möchten.
      - Wählen Sie das **Zertifikat** aus der Liste aller SSL-Zertifikatdateien auf der Instanz.

   b) Zertifikatdetails

      - **Zertifikatname**. Geben Sie einen Namen für den Zertifikatschlüssel an.
      - **Kennwort**. Kennwort zum Verschlüsseln des privaten Schlüssels. Sie können diese Option verwenden, um verschlüsselte private Schlüssel hochzuladen.
4. Klicken Sie auf **Instanzen auswählen**, um die Citrix ADC-Instanzen auszuwählen, auf denen Sie Ihre Zertifikate installieren möchten.
5. Klicken Sie auf **OK**.

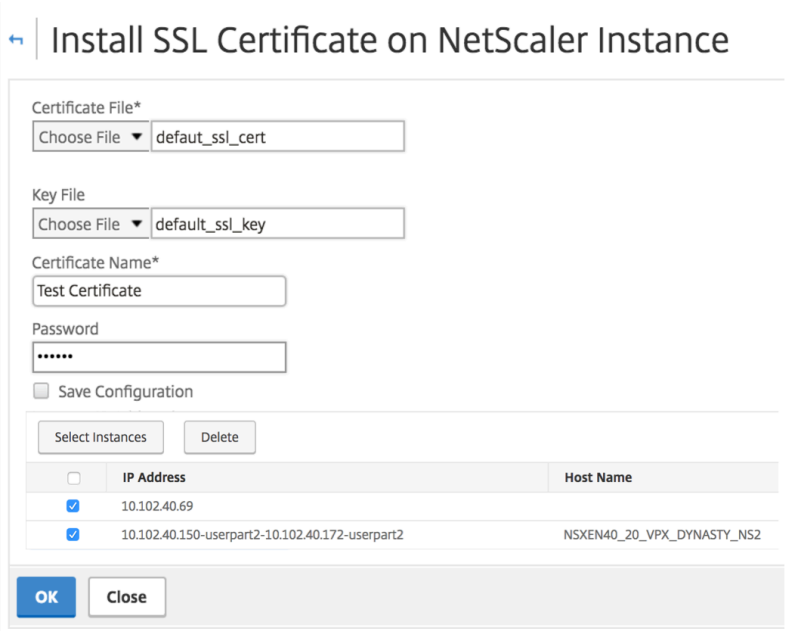


So installieren Sie ein SSL-Zertifikat von Citrix ADM:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie in der rechten oberen Ecke des Dashboards auf **Zertifikat installieren**.
3. Geben Sie auf der Seite **SSL-Zertifikat auf Citrix ADC-Instanz installieren** die folgenden Parameter an:
   - **Zertifikatsdatei** - Laden Sie eine SSL-Zertifikatsdatei hoch, indem Sie entweder **Local** (Ihr lokaler Computer) oder **Appliance** auswählen (die Zertifikatsdatei muss in der virtuellen Citrix ADM-Instanz vorhanden sein).
   - **Schlüsseldatei** - Laden Sie die Schlüsseldatei hoch.
   - **Zertifikatsname** — Geben Sie einen Namen für den Zertifikatschlüssel an.

- **Kennwort** - Kennwort zum Verschlüsseln des privaten Schlüssels. Sie können diese Option verwenden, um verschlüsselte private Schlüssel hochzuladen.
- **Instanzen auswählen** - Wählen Sie die Citrix ADC-Instanzen aus, auf denen Sie Ihre Zertifikate installieren möchten.

4. Um die Konfiguration für die zukünftige Verwendung zu speichern, aktivieren Sie das Kontrollkästchen **Konfiguration speichern**.
5. Klicken Sie auf **OK**.



Erstellen einer Zertifikatsignieranforderung (CSR)

April 28, 2021

Eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) ist ein Block mit verschlüsseltem Text, der auf dem Server generiert wird, auf dem das Zertifikat verwendet wird. Sie enthält Informationen, die im Zertifikat enthalten sind, z. B. den Namen Ihrer Organisation, den allgemeinen Namen (Domänenname), den Ort und das Land.

So erstellen Sie eine CSR mit Citrix ADM:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf eines der Diagramme, um die Liste der installierten SSL-Zertifikate anzuzeigen, und wählen Sie dann das Zertifikat aus, für das Sie eine CSR erstellen möchten, und wählen Sie **CSR erstellen** aus der Dropdown-Liste **Aktion auswählen** aus.

3. Geben Sie auf der Seite **Certificate Signing Request (CSR)** einen Namen für die CSR an.
4. Führen Sie einen der folgenden Schritte aus:
   - **Schlüssel hochladen** - Wählen Sie die Option **Ich habe einen Schlüssel**. Um die Schlüsseldatei hochzuladen, wählen Sie entweder **Lokal** (Ihr lokaler Computer) oder **Appliance** (die Schlüsseldatei muss auf der virtuellen Citrix ADM Instanz vorhanden sein).
   - **Schlüssel erstellen** - Wählen Sie die Option **Ich habe keinen Schlüssel**, und geben Sie dann die folgenden Parameter an:

Verschlüsselungsalgorithmus	Typ des Schlüssels. Zum Beispiel RSA.
Schlüsseldateiname	Name der Datei, in der der RSA-Schlüssel gespeichert ist.
Schlüsselgröße	Schlüsselgröße in Bits.
Öffentlicher Exponentenwert	Wählen Sie entweder **3** oder **F4** aus der Dropdownliste. Dieser Wert ist Teil des Verschlüsselungsalgorithmus, der zum Erstellen Ihres RSA-Schlüssels erforderlich ist.
Schlüsselformat	Be default PEM ist ausgewählt. PEM ist das empfohlene Schlüsselformat für Ihr SSL-Zertifikat.
PEM-Kodierungsalgorithmus	Wählen Sie in der Dropdownliste den Algorithmus (**DES** oder **DES3**) aus, den Sie zum Verschlüsseln des generierten RSA-Schlüssels verwenden möchten. Wenn Sie diesen Algorithmus wählen, müssen Sie eine PEM-Passphrase angeben.
PEM-Passphrase	Wenn Sie den PEM-Kodierungsalgorithmus gewählt haben, geben Sie eine Passphrase ein.
PEM-Passphrase bestätigen	Bestätigen Sie Ihre PEM-Passphrase.

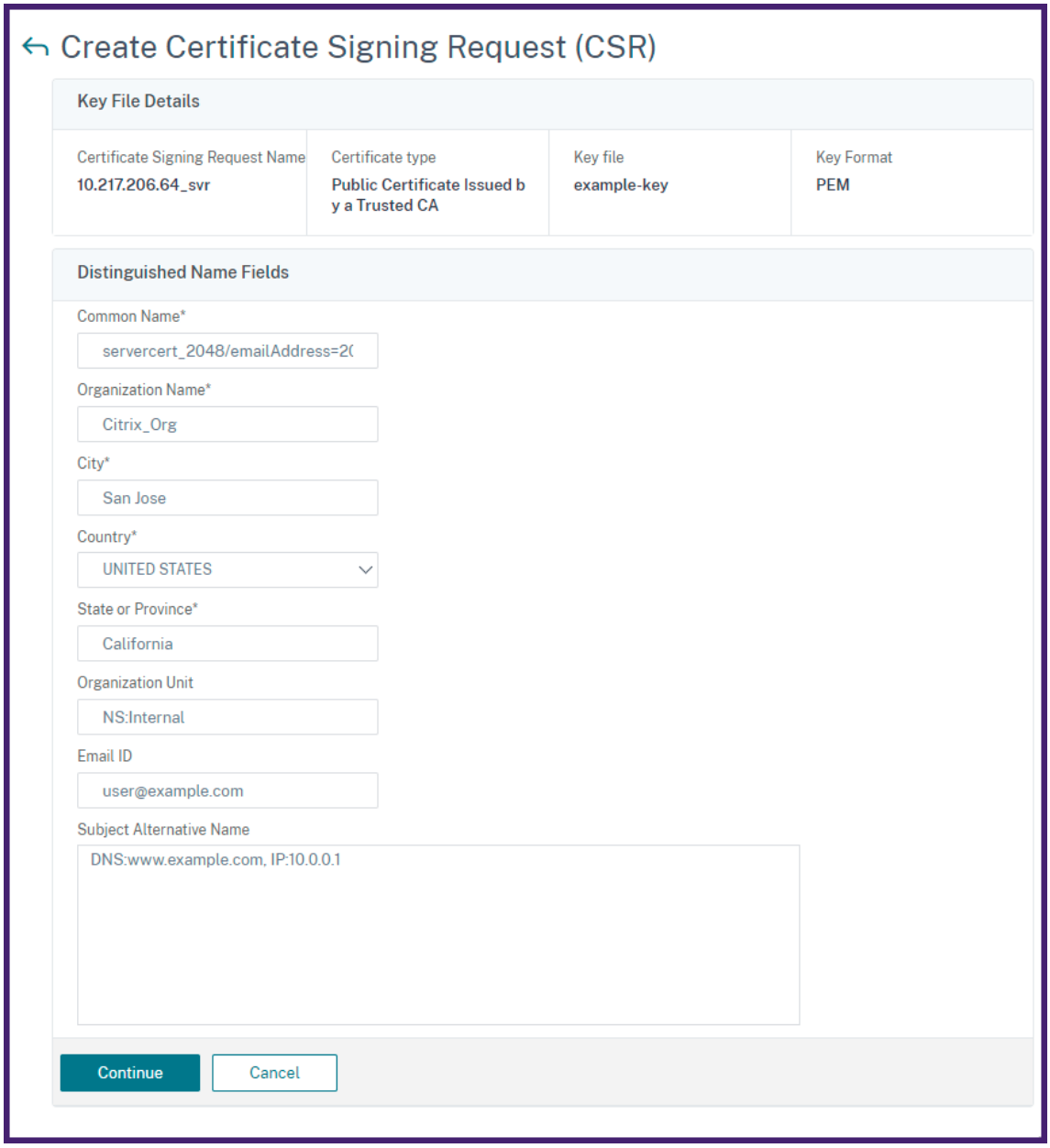
5. Klicken Sie auf **Weiter**.
6. Geben Sie auf der folgenden Seite weitere Details an.

   Die meisten Felder haben Standardwerte, die aus dem Betreff des ausgewählten Zertifikats extrahiert wurden. Der Betreff enthält Details wie den allgemeinen Namen, den Namen der Organisation, den Bundesstaat und das Land.

Im Feld **Subject Alternative Name** können Sie mehrere Werte wie Domänennamen und IP-Adressen mit einem einzigen Zertifikat angeben. Die alternativen Namen des Subjekts helfen Ihnen, mehrere Domänen mit einem einzigen Zertifikat zu sichern.

Geben Sie die Domänennamen und IP-Adressen im folgenden Format an:

```
DNS:<Domain name>, IP:<IP address>
<!--NeedCopy-->
```



In diesem Beispiel sichert es `10.0.0.1` und `www.example.com`.

Überprüfen Sie die Felder und klicken Sie auf **Weiter**.

> **Hinweis**
>
> Die meisten Zertifizierungsstellen akzeptieren Zertifikatsübermittlungen per E-Mail. Die Zertifizierungsstelle gibt ein gültiges Zertifikat an die E-Mail-Adresse zurück, von der Sie die CSR übermitteln.

SSL-Zertifikate verknüpfen und aufheben

April 28, 2021

Sie erstellen ein Zertifikatbündel, indem Sie mehrere Zertifikate miteinander verknüpfen. Um ein Zertifikat mit einem anderen Zertifikat zu verknüpfen, muss der Aussteller des ersten Zertifikats mit der Domäne des zweiten Zertifikats übereinstimmen. Wenn Sie beispielsweise Zertifikat A mit Zertifikat B verknüpfen möchten, muss der Aussteller des Zertifikats A mit der Domäne des Zertifikats B übereinstimmen.

So verknüpfen Sie mithilfe von Citrix ADM ein SSL-Zertifikat mit einem anderen Zertifikat:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf eine der Diagramme, um die Liste der SSL-Zertifikate anzuzeigen.
3. Wählen Sie das Zertifikat aus, das Sie verknüpfen möchten, und klicken Sie dann in der Dropdownliste **Aktion auswählen** auf **Verknüpfung**.
4. Wählen Sie in der Liste der übereinstimmenden Zertifikate das Zertifikat aus, mit dem Sie eine Verknüpfung herstellen möchten, und klicken Sie dann auf **OK**.

   > **Hinweis**
   >
   > Wenn kein übereinstimmendes Zertifikat gefunden wird, wird die folgende Meldung angezeigt: Kein Zertifikat gefunden, um eine Verknüpfung herzustellen.

So heben Sie die Verknüpfung eines SSL-Zertifikats mithilfe von Citrix ADM auf:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf eine der Diagramme, um die Liste der SSL-Zertifikate anzuzeigen.
3. Wählen Sie eines der verknüpften Zertifikate aus, die verknüpft sind, und klicken Sie dann in der Dropdownliste **Aktion auswählen** auf **Verknüpfung aufheben**.
4. Klicken Sie auf **OK**.

> **Hinweis**
>
> Wenn das ausgewählte Zertifikat nicht mit einem anderen Zertifikat verknüpft ist, wird die folgende Meldung angezeigt: Zertifikat verfügt über keine Zertifizierungsstellen-Verknüpfung.

Konfigurieren einer Unternehmensrichtlinie

April 28, 2021

Sie können eine Unternehmensrichtlinie konfigurieren und alle vertrauenswürdigen Zertifizierungsstellen, sichere Signaturalgorithmen hinzufügen und die empfohlene Schlüsselstärke für Ihre Zertifikatschlüssel in Citrix Application Delivery Management (Citrix ADM) auswählen. Wenn eines der auf Ihrer Citrix ADC-Instanz installierten Zertifikate der Unternehmensrichtlinie nicht hinzugefügt wurde, zeigt das SSL-Zertifikat-Dashboard den Aussteller dieser Zertifikate als Nicht empfohlen an.

Wenn die Zertifikatschlüsselstärke nicht mit der empfohlenen Schlüsselstärke in der Unternehmensrichtlinie übereinstimmt, zeigt das SSL-Zertifikat-Dashboard die Stärken dieser Schlüssel als Nicht empfohlen an.

So konfigurieren Sie eine Unternehmensrichtlinie für Citrix ADM:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf der Seite “ **Einstellungen** “ auf das Symbol für **Unternehmensrichtlinien**, um alle vertrauenswürdigen Zertifizierungsalgorithmen und sichere Signaturalgorithmen hinzuzufügen und die empfohlene Schlüsselstärke für Ihre Zertifikate und Schlüssel auszuwählen.
    - **Empfohlene Schlüsselstärken** - Bezeichnet die Algorithmussicherheit und die Anzahl der Bits in einem Schlüssel.
    - **Empfohlene Signaturalgorithmen** - Bezeichnet die signierten Token-Probleme für die Anwendungen.
    - **Empfohlene Trusted CA** - Bezeichnet die vertrauenswürdige Entität, die die digitalen Zertifikate ausstellt. Klicken Sie auf das Symbol **+**, um weitere Entitys hinzuzufügen.
    - **Empfohlene SSL-Protokolle** - Bezeichnet die TLS/SSL-Versionen.
3. Klicken Sie auf **Fertigstellen** oder **Speichern und Beenden**, um Ihre Unternehmensrichtlinie zu speichern.

Abfragen von SSL-Zertifikaten von Citrix ADC-Instanzen

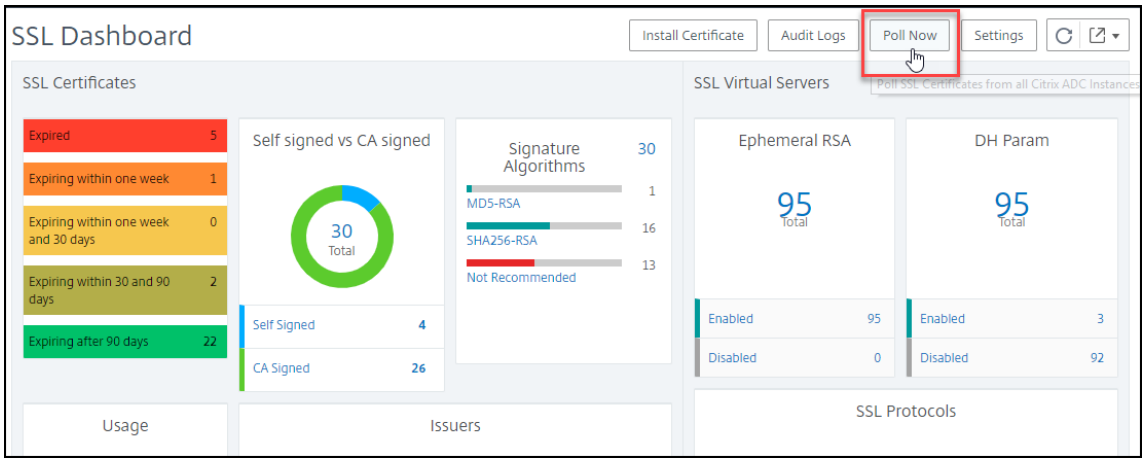
April 28, 2021

Citrix Application Delivery Management (Citrix ADM) fragt automatisch SSL-Zertifikate alle 24 Stunden mithilfe von NITRO -Aufrufen und dem Secure Copy (SCP) -Protokoll ab. Sie können die SSL-Zertifikate auch manuell abfragen, um neu hinzugefügte SSL-Zertifikate auf den Citrix ADC-Instanzen zu ermitteln. Durch das Abrufen aller Citrix ADC-Instanzen SSL-Zertifikate wird das Netzwerk stark belastet.

Anstatt alle SSL-Zertifikate der Citrix ADC-Instanzen abzufragen, können Sie manuell nur die SSL-Zertifikate einer ausgewählten Instanz oder Instanzen abfragen.

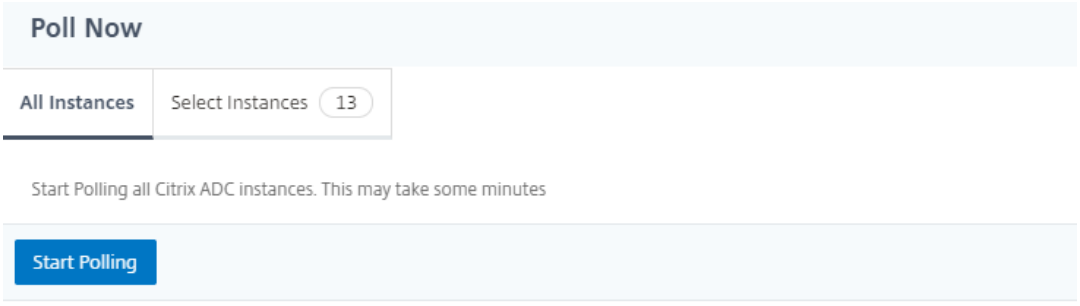
So fragen Sie SSL-Zertifikate auf Citrix ADC-Instanzen ab:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf der Seite **SSL-Dashboard** oben rechts auf **Jetzt abfragen**.

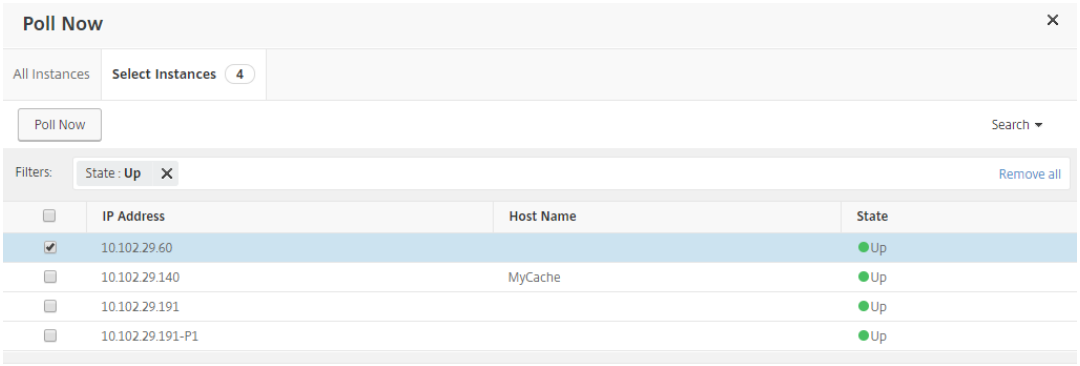


3. Die Seite **Jetzt abfragen** wird geöffnet und bietet Ihnen die Möglichkeit, alle Citrix ADC-Instanzen im Netzwerk abzufragen oder ausgewählte Instanzen abzufragen.

   - Um die SLL-Zertifikate aller Citrix ADC-Instanzen abzufragen, wählen Sie die Registerkarte **Alle Instanzen**, und klicken Sie auf **Abruf starten**.



   - Um bestimmte Instanzen abzufragen, wählen Sie die Registerkarte **Instanzen auswählen** aus, wählen Sie die Instanzen aus der Liste aus und klicken Sie auf **Jetzt abfragen**.



So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Konfigurieren der IP-Adressverwaltung (IPAM)

April 28, 2021

ADM IPAM bietet Ihnen die Möglichkeit, IP-Adressen in ADM-verwalteten Konfigurationen automatisch zuzuweisen und freizugeben. Sie können IP-Adressen aus Netzwerken oder IP-Bereichen zuweisen, die mit den folgenden IP-Anbietern definiert wurden:

- Integrierter IPAM-Anbieter von ADM.
- Infoblox IPAM-Lösung. Weitere Informationen finden Sie unter Infoblox DDI.

Derzeit können Sie ADM IPAM in folgenden Bereichen verwenden:

- **StyleBooks**: Automatische Zuweisung von IPs zu virtuellen Servern, wenn Sie Konfigurationen erstellen.
- **Kubernetes Ingress**: Weisen Sie einer Ingress-Konfiguration in einem Kubernetes-Cluster automatisch eine virtuelle IP-Adresse zu.

- **API-Gateway**: Weisen Sie dem API-Proxy automatisch eine IP-Adresse zu.

Sie können auch die zugewiesenen und verfügbaren IP-Adressen in jedem Netzwerk oder IP-Bereich verfolgen, der von ADM verwaltet wird.

Hinzufügen eines externen IP-Adressanbieters

ADM verfügt über einen integrierten IPAM-Anbieter zur Verwaltung von IPs und IP-Bereichen. Sie können auch einen externen IP-Adressanbieter zu ADM hinzufügen.

> **Wichtig**
>
> Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Berechtigungen im externen IP-Adressanbieter aktiviert sind:
>
> - Möglichkeit zur Abfrage von Netzwerken, die im Anbieter vorhanden sind.
> - Registrieren Sie ein neues Netzwerk.
> - Heben Sie die Registrierung eines bestehenden Netzwerks auf
> - Reservieren Sie eine IP-Adresse im Netzwerk.
> - Geben Sie eine IP-Adresse aus dem Netzwerk frei.
> - Rufen Sie die verwendeten IP-Adressen aus einem Netzwerk ab.
> - Rufen Sie verfügbare IP-Adressen aus einem Netzwerk ab.

Führen Sie die folgenden Schritte durch, um eine externe IP-Provider-Lösung in ADM hinzuzufügen:

1. Navigieren Sie zu **Netzwerke > IPAM**.
2. Klicken Sie unter **Anbieter**auf **Hinzufügen**.
3. Geben Sie die folgenden Details an, um einen IP-Anbieter hinzuzufügen:
   - **Name** - Geben Sie den IP-Providernamen an, der in ADM verwendet werden soll.
   - **Anbieter** - Wählen Sie einen IPAM-Anbieter aus der Liste aus.
   - **URL** - Geben Sie die URL der IPAM-Lösung an, die IP-Adressen in einer ADM-Umgebung zuweist. Stellen Sie sicher, dass Sie die URL im folgenden Format angeben:

     ```
     https://<host name>
     <!--NeedCopy-->
     ```

     Beispiel:`https://myinfoblox.example.com`
   - **Benutzername** - Geben Sie den Benutzernamen für die Anmeldung bei der IPAM-Lösung an.
   - **Kennwort** - Geben Sie das Kennwort für die Anmeldung bei der IPAM-Lösung an.

4. Klicken Sie auf **Hinzufügen**.

Hinzufügen eines Netzwerks

Fügen Sie ein Netzwerk hinzu, um IPAM mit ADM-verwalteten Konfigurationen zu verwenden.

1. Navigieren Sie zu **Netzwerke > IPAM**.
2. Klicken Sie unter **Netzwerke**auf **Hinzufügen**.
3. Geben Sie die folgenden Details an:
   - **Netzwerkname** - Geben Sie den Netzwerknamen an, um das Netzwerk in ADM zu identifizieren.
   - **Anbieter** - Wählen Sie den Anbieter aus der Liste aus.

     In dieser Liste werden die Anbieter angezeigt, die in ADM hinzugefügt wurden.
   - **Netzwerktyp** : Wählen Sie **IP-Bereich** oder **CIDR** aus der Liste basierend auf Ihrer Anforderung aus.
   - **Netzwerkwert** - Geben Sie den Netzwerkwert an.

     > **Hinweis**
     >
     > ADM IPAM unterstützt nur IPv4-Adressen.

     Geben Sie für **IP-Bereich**den Netzwerkwert im folgenden Format an:

     ```
     <first-IP-address>-<last-IP-address>
     <!--NeedCopy-->
     ```

     Beispiel:

     ```
     10.0.0.20-10.0.0.100
     <!--NeedCopy-->
     ```

     Geben Sie für **CIDR**den Netzwerkwert im folgenden Format an:

     ```
     <IP-address>/<subnet-mask>
     <!--NeedCopy-->
     ```

     Beispiel:

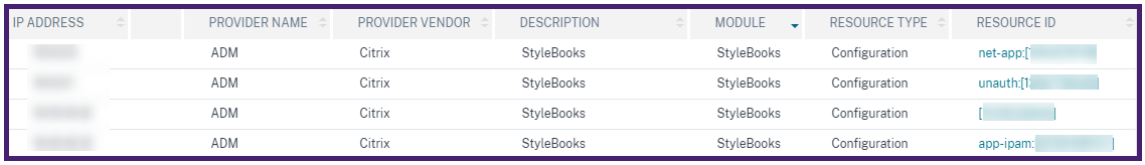

```
10.70.124.0/24
<!--NeedCopy-->
```

4. Klicken Sie auf **Erstellen**.

Anzeigen zugewiesenen IP-Adressen

Um weitere Details zu zugewiesenen IP-Adressen aus dem IPAM-Netzwerk anzuzeigen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Netzwerke > IPAM**.
2. Klicken Sie auf der Registerkarte **Netzwerke** auf **Alle zugewiesenen IPs**anzeigen.



IP ADDRESS	PROVIDER NAME	PROVIDER VENDOR	DESCRIPTION	MODULE	RESOURCE TYPE	RESOURCE ID
[redacted]	ADM	Citrix	StyleBooks	StyleBooks	Configuration	net-app:[
[redacted]	ADM	Citrix	StyleBooks	StyleBooks	Configuration	unauth:[1
[redacted]	ADM	Citrix	StyleBooks	StyleBooks	Configuration	[
[redacted]	ADM	Citrix	StyleBooks	StyleBooks	Configuration	app-ipam:

In diesem Bereich werden IP-Adresse, Anbietername, Anbieter des Anbieters und Beschreibung angezeigt. Außerdem werden die Ressourcendetails angezeigt, die diese IP-Adresse reserviert haben:

- **Modul**: Zeigt das ADM-Modul an, das die IP-Adresse reserviert hat. Wenn StyleBooks beispielsweise die IP-Adresse reserviert hat, zeigt diese Spalte StyleBooks als Modul an.
- **Ressourcentyp**: Zeigt den Ressourcentyp in diesem Modul an. Für das StyleBooks-Modul verwendet nur der Konfigurations-Ressourcentyp das IPAM-Netzwerk. In dieser Spalte werden also Konfigurationen angezeigt.
- **Ressourcen-ID**: Zeigt die genaue Ressourcen-ID mit einem Link an. Klicken Sie auf diesen Link, um auf die Ressource zuzugreifen, die die IP-Adresse verwendet. Für den Konfigurations-Ressourcentyp wird die Konfigurationspack-ID als Ressourcen-ID angezeigt.

> **Hinweis**
>
> Wenn Sie die IP-Adresse freigeben möchten, wählen Sie die IP-Adresse aus, die Sie freigeben möchten, und klicken Sie auf **Zugeteilte IPs freigeben**.

Konfigurationsaufträge

April 28, 2021

Citrix Application Delivery Management (ADM) -Konfigurationsverwaltungsprozess stellt die ordnungsgemäße Replikation von Konfigurationsänderungen, Systemaktualisierungen und anderen Wartungsaktivitäten über mehrere Citrix ADC-Instanzen im Netzwerk sicher.

Citrix ADM ermöglicht es Ihnen, Konfigurationsaufträge zu erstellen, die Ihnen helfen, all diese Aktivitäten problemlos auf mehreren Geräten als eine einzige Aufgabe auszuführen. Konfigurationsaufträge und Vorlagen vereinfachen die sich wiederholenden Verwaltungsaufgaben zu einer einzigen Aufgabe auf Citrix ADM. Ein Konfigurationsauftrag enthält eine Reihe von Konfigurationsbefehlen, die Sie auf einem oder mehreren verwalteten Geräten ausführen können.

Konfigurationsaufträge können entweder SSH-Befehle verwenden, um Konfigurationsbefehle auszuführen oder SCP verwenden, um Dateikopie von entweder lokal oder auf eine andere Appliance zu machen, zum Beispiel können wir ein HA-Failover oder HA-Upgrade planen.

Sie können einen Konfigurationsauftrag erstellen, indem Sie eine der folgenden vier Optionen in Citrix ADM verwenden. Verwenden Sie eine davon, um eine wiederverwendbare Quelle von Befehlen und Anweisungen für das System zur Ausführung eines Konfigurationsauftrags zu erstellen.

1. Konfigurationsvorlage
2. Instanz
3. Datei
4. Aufnehmen und Abspielen

Konfigurationsvorlage:

Sie können Konfigurationsvorlagen erstellen, während Sie einen Auftrag erstellen und eine Reihe von Konfigurationsbefehlen als Vorlage speichern. Wenn Sie diese Vorlagen auf der Seite Jobs erstellen speichern, werden sie automatisch auf der Seite Vorlage erstellen angezeigt.

> **Hinweis**
> Die Option **Umbenennen** ist für die Standardkonfigurationsvorlagen deaktiviert. Sie können jedoch benutzerdefinierte Konfigurationsvorlagen umbenennen.

Sie können eine der folgenden Vorlagen verwenden:

Konfigurationseditor: Sie können den Konfigurationseditor verwenden, um CLI-Befehle einzugeben, die Konfiguration als Vorlage zu speichern und Aufträge zu konfigurieren.

Inbuilt Template: Sie können aus einer Liste von Konfigurationsvorlagen wählen. Diese Vorlagen stellen die Syntaxen der CLI-Befehle bereit und ermöglichen es Ihnen, Werte für die Variablen anzugeben. Die eingebauten Vorlagen sind mit ihren Beschreibungen in der folgenden Tabelle aufgeführt. Sie können einen Job planen, indem Sie die integrierte Vorlagenoption verwenden. Ein Auftrag ist eine Reihe von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Sie können beispielsweise die integrierte Vorlagenoption verwenden, um einen Auftrag zum Konfigurieren von Syslog-Servern zu planen. Sie können den Job auch sofort ausführen oder den Job so planen, dass er zu einem späteren Zeitpunkt ausgeführt wird.

Instanz:

Sie können ein Einzelbündel-Upgrade Ihrer Citrix ADC SDX-Instanzen mit Citrix ADC Version 11.0 und höher durchführen. Um ein Einzelbündel-Upgrade durchzuführen, verwenden Sie einen integrierten Task in Citrix ADM. Sie können eine Citrix ADC-Instanz auch aktualisieren, indem Sie die ausgeführte Konfiguration oder eine gespeicherte Konfiguration extrahieren und die Befehle auf einer anderen Citrix ADC-Instanz desselben Typs ausführen. Dieses Upgrade ermöglicht es Ihnen, die Konfiguration einer Instanz auf der anderen zu replizieren.

Datei:

Sie können eine Konfigurationsdatei von Ihrem lokalen Computer hochladen und Aufträge erstellen.

Vorteile der Verwendung einer Datei

- Sie können eine beliebige Textdatei verwenden, um eine wiederverwendbare Quelle von Konfigurationsbefehlen zu erstellen.
- Jede Art von Formatierung ist nicht erforderlich.
- Die Datei kann auf Ihrem lokalen Computer gespeichert werden.

Sie können entweder eine neue Datei erstellen und speichern oder eine vorhandene Datei importieren und die Befehle ausführen.

Aufnehmen und Abspielen:

Mit Job erstellen können Sie entweder Ihre eigenen CLI-Befehle eingeben oder die Schaltfläche “Aufnehmen und Abspielen” verwenden, um Befehle aus einer Citrix ADC-Sitzung zu erhalten. Wenn Sie den Auftrag ausführen, werden Änderungen in der ns.conf auf der ausgewählten Instanz aufgezeichnet und in Citrix ADM kopiert.

Verwandte Artikel

- Verwenden des SCP-Befehls (put) in Konfigurationsaufträgen
- Verwenden von Variablen in Konfigurationsaufträgen
- Erstellen von Konfigurationsaufträgen aus Korrekturbefehlen
- Verwenden von Konfigurationsvorlagen zum Erstellen von Überwachungsvorlagen
- Erstellen von Konfigurationsaufträgen mit Aufzeichnung und Wiedergabe
- Verwenden der Masterkonfigurationsvorlage unter Citrix ADM

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.

2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Erstellen eines Konfigurationsauftrags

April 28, 2021

Ein Auftrag ist eine Reihe von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen erstellen und ausführen können.

Sie können Aufträge erstellen, um Konfigurationsänderungen über Instanzen hinweg vorzunehmen. Sie können inReplikation von Konfigurationen auf mehreren InstanzenIhrem Netzwerk und Konfigurationsaufgaben aufzeichnen und abspielenüber das Citrix Application Delivery Management (ADM) GUI und konvertieren Sie es in CLI-Befehle.

Mit der Funktion Konfigurationsaufträge von Citrix ADM können Sie einen Konfigurationsauftrag erstellen, E-Mail-Benachrichtigungen senden und Ausführungsprotokolle der erstellten Aufträge überprüfen.

So erstellen Sie einen Konfigurationsauftrag auf Citrix ADM:

1. Navigieren Sie zu “ **Netzwerke** > **Konfigurationsaufträge**”.
2. Klicken Sie auf **Job erstellen**.
3. Geben Sie auf der Seite **Job erstellen** auf der Registerkarte **Konfiguration auswählen** den Auftragsnamen an, und wählen Sie den **Instanztyp** aus der Liste aus.
4. Wählen Sie in der Liste **Konfigurationsquelle** die Konfigurationsauftragsvorlage aus, die Sie erstellen möchten. Fügen Sie die Befehle für die ausgewählte Vorlage hinzu.
    - Sie können entweder die Befehle eingeben oder die vorhandenen Befehle aus den gespeicherten Konfigurationsvorlagen importieren.
    - Sie können auch mehrere Vorlagen verschiedener Typen im Konfigurationseditor hinzufügen, während Sie einen Job in den Konfigurationsaufträgen erstellen.
    - Wählen Sie in der Liste **Konfigurationsquelle** die verschiedenen Vorlagen aus, und ziehen Sie die Vorlagen dann in den Konfigurationseditor. Die Vorlagentypen können **Konfigura-**

tionsvorlage, **In Built Template**, **Master Configuration**, **Record and Play**, **Instanz** und **File** sein.

> **Hinweis**
>
> Wenn Sie die Vorlage Master-Konfigurationsauftrag bereitstellen zum ersten Mal hinzufügen und eine Vorlage eines anderen Typs hinzufügen, wird die gesamte Auftragsvorlage zu einem Master-Konfigurationstyp.

Sie können die Befehle auch im Konfigurationseditor neu anordnen und neu anordnen. Sie können den Befehl von einer Zeile in eine andere verschieben, indem Sie die Befehlszeile ziehen und ablegen. Sie können die Befehlszeile auch von einer Zeile zu einer beliebigen Zielzeile verschieben oder neu anordnen, indem Sie einfach die Befehlszeilennummer im Textfeld ändern. Sie können die Befehlszeile auch beim Bearbeiten des Konfigurationsauftrags neu anordnen und neu anordnen.

Sie können Variablen definieren, mit denen Sie verschiedene Werte für diese Parameter zuweisen oder einen Auftrag über mehrere Instanzen ausführen können. Sie können alle Variablen überprüfen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags in einer einzigen konsolidierten Ansicht definiert haben. Klicken Sie auf die Registerkarte **Variablenvorschau**, um die Variablen in einer einzigen konsolidierten Ansicht anzuzeigen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben.

Sie können Rollback-Befehle für jeden Befehl im Konfigurationseditor anpassen. Um benutzerdefinierte Befehle anzugeben, aktivieren Sie die benutzerdefinierte Rollback-Option.

> **Wichtig**
>
> Damit das benutzerdefinierte Rollback wirksam wird, schließen Sie den Assistenten zum **Erstellen von Jobs**ab. Wählen Sie auf der Registerkarte **Ausführen** die Option **Rollback Successful Commands** aus der Liste **Bei Command Failure**.

5. **Wählen Sie auf der Registerkarte Instanzen** auswählen die Instanzen aus, für die Sie die Konfigurationsüberwachung ausführen möchten.

   a) In einem Citrix ADC Hochverfügbarkeitspaar können Sie einen Konfigurationsauftrag lokal auf einem primären oder sekundären Knoten ausführen. Wählen Sie aus, auf welchem Knoten Sie den Job ausführen möchten.

      - **Auf primären Knoten ausführen** - Wählen Sie diese Option, um den Job nur auf primären Knoten auszuführen.
      - **Auf sekundären Knoten ausführen** - Wählen Sie diese Option, um den Job nur auf sekundären Knoten auszuführen.

      Sie können auch sowohl den primären als auch den sekundären Knoten auswählen, um denselben Konfigurationsauftrag auszuführen. Wenn Sie keinen primären oder

sekundären Knoten auswählen, wird der Konfigurationsauftrag automatisch auf dem primären Knoten ausgeführt.

b) Klicken Sie auf **Instanzen hinzufügen**, und wählen Sie die Instanzen aus der Liste aus. Klicken Sie auf **OK**.

c) Klicken Sie auf **Weiter**.

6. Auf der Registerkarte **Variablenwerte angeben** haben Sie zwei Optionen:

a) Laden Sie die Eingabedatei herunter, um die Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den Citrix ADM -Server hoch.

b) Geben Sie allgemeine Werte für die Variablen ein, die Sie für alle Instanzen definiert haben

c) Klicken Sie auf **Weiter**.

7. Prüfen Sie die Befehle, die für jede Instanz auf der Registerkarte **Auftragsvorschau** ausgeführt werden sollen, und überprüfen Sie sie. Auf dieser Registerkarte werden auch die Rollback-Befehle angezeigt, wenn sie auf der Registerkarte **Konfiguration auswählen** angegeben sind.

8. Wählen Sie auf der Registerkarte **Ausführen**, ob Sie Ihren Job jetzt ausführen möchten, oder planen Sie, den Job später auszuführen.

   Wählen Sie außerdem eine der folgenden Aktionen aus der Liste **On Command Failure** aus, die Citrix ADM ausführen muss, wenn der Befehl fehlschlägt:

   - **Fehler ignorieren und weiter**: Citrix ADM ignoriert den fehlgeschlagenen Befehl und führt die restlichen Befehle für die ausgewählte Instanz aus.

     > **Hinweis:**
     >
     > Mit dieser Aktion können Sie einen Konfigurationsauftrag abbrechen, der gerade ausgeführt wird.

   - **Weitere Ausführung beenden**: Citrix ADM stoppt die verbleibenden Befehle, wenn ein Befehl während der Ausführung fehlschlägt.
   - **Erfolgreiche Befehle zum Zurücksetzen**: Citrix ADM stellt die erfolgreich ausgeführten Befehle wieder her, wenn ein Befehl während der Ausführung fehlschlägt.

     Wenn das benutzerdefinierte Rollback aktiviert ist, führt das Citrix ADM die entsprechenden Rollback-Befehle für die fehlgeschlagenen Befehle aus.

9. Klicken Sie auf **Fertig stellen**.

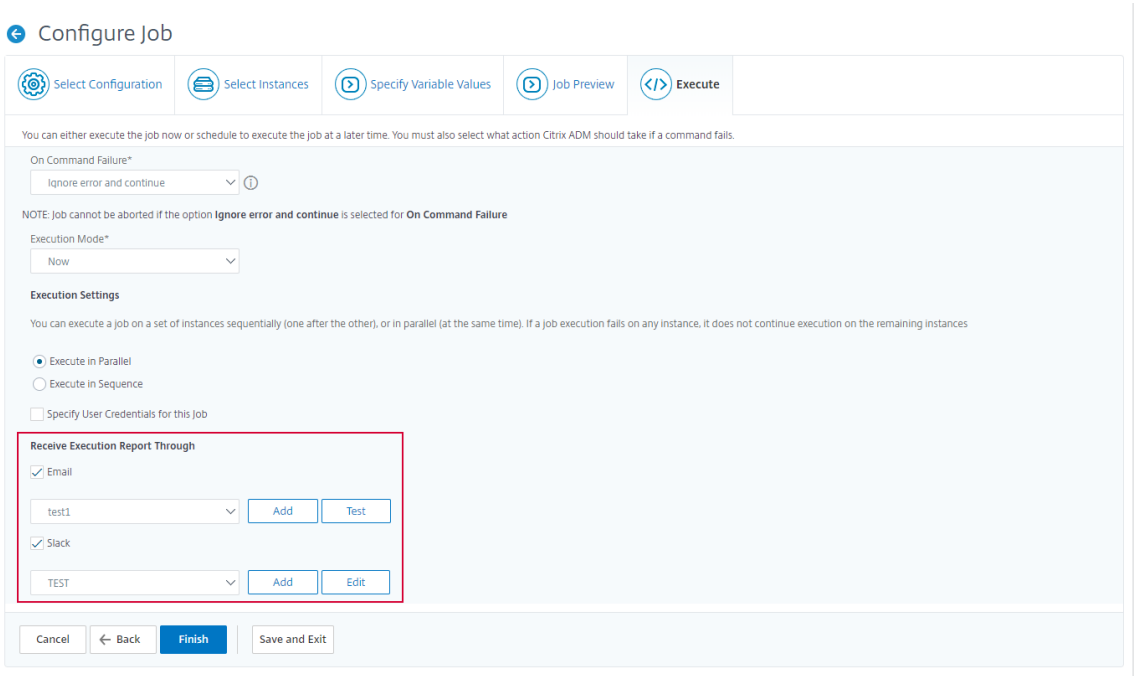
So senden Sie eine E-Mail und eine Slack Benachrichtigung für einen Job:

Eine E-Mail- und Slack-Benachrichtigung wird jetzt jedes Mal gesendet, wenn ein Job ausgeführt oder geplant wird. Die Benachrichtigung enthält Details wie den Erfolg oder Misserfolg des Auftrags sowie die relevanten Details.

1. Navigieren Sie zu **Netzwerke**>**Konfigurationsaufträge**.
2. Wählen Sie den Job aus, den Sie E-Mail- und Slack -Benachrichtigung aktivieren möchten, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Registerkarte **Ausführen** zum Bereich **Empfangsausführungsbericht durch**:
   - Aktivieren Sie das Kontrollkästchen **E-Mail**, und wählen Sie die E-Mail-Verteilerliste, an die Sie den Ausführungsbericht senden möchten.

     Wenn Sie eine E-Mail-Verteilerliste hinzufügen möchten, klicken Sie auf **Hinzufügen**, und geben Sie die Details des E-Mail-Servers an.
   - Aktivieren Sie das Kontrollkästchen **Slack**, und wählen Sie den Pufferkanal, an den Sie den Ausführungsbericht senden möchten.

     Wenn Sie ein Slack -Profil hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie den **Profilnamen**, den **Kanalnamen** und das **Token** des erforderlichen Slack-Kanals an.

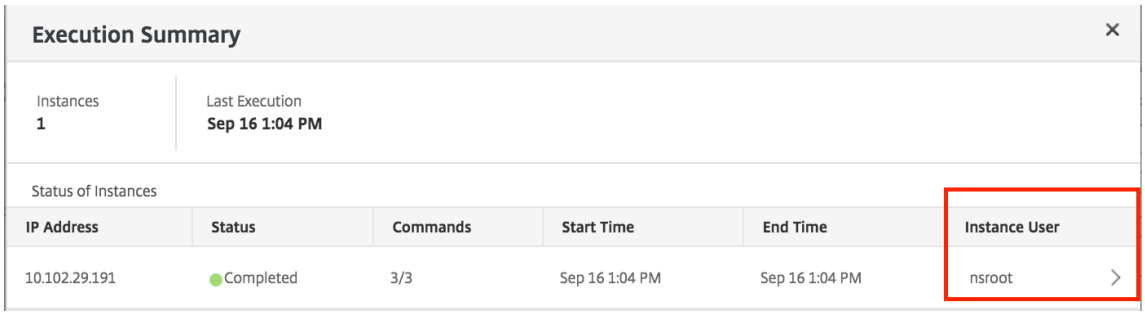


4. Klicken Sie auf **Fertig stellen**.

So zeigen Sie Details zur Ausführungszusammenfassung an:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**.

2. Wählen Sie den Job aus, den Sie die Ausführungszusammenfassung anzeigen möchten, und klicken Sie auf **Details**.
3. Klicken Sie auf **Ausführungsübersicht**, um Folgendes anzuzeigen:
    - Der Status der Instanz des Jobs, der ausgeführt wurde
    - Die Befehle werden für den Auftrag ausgeführt
    - Die Start- und Endzeit des Auftrags und
    - Der Name des Instanzbenutzers



Verwenden von Aufzeichnung und Wiedergabe zum Erstellen von Konfigurationsaufträgen

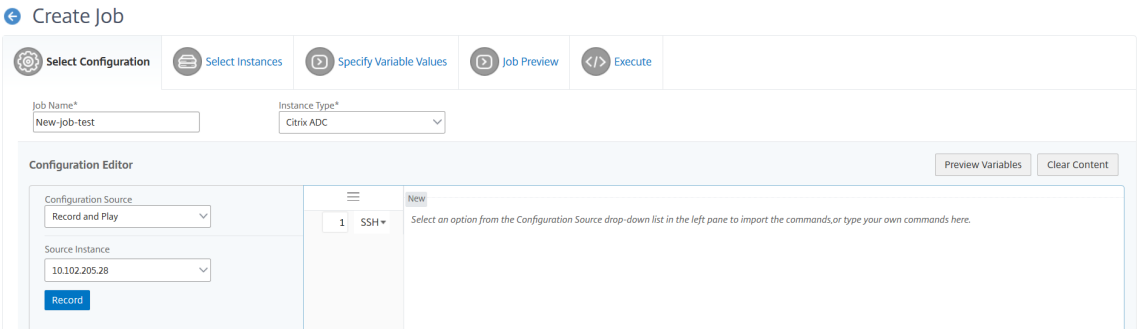
April 28, 2021

Wenn Sie es gewohnt sind, die Citrix ADC GUI zum Konfigurieren einer Citrix ADC-Instanz zu verwenden, fällt es manchmal schwierig, die genauen CLI-Befehle zum Erstellen einer Konfigurationsaufgabe und zum Ausführen auf mehreren Citrix ADC-Instanzen abzurufen.

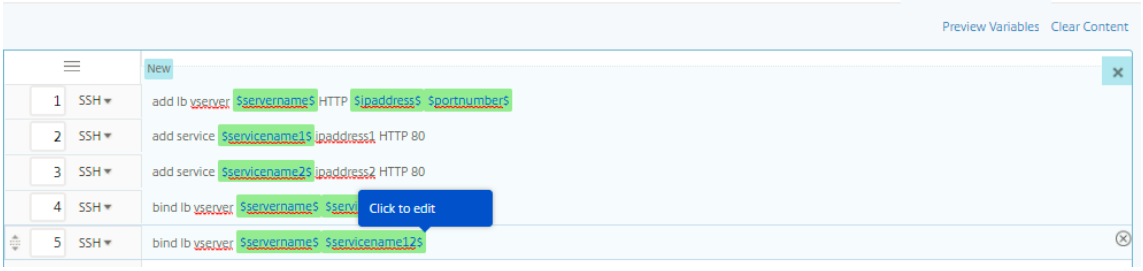
Mit Citrix Application Delivery Management (ADM) können Sie die Konfigurationsaufgaben aufzeichnen, die über die GUI einer Citrix ADC-Instanz ausgeführt werden, und sie in CLI-Befehle konvertieren. Sie können dann aus diesen CLI-Befehlen eine Konfigurationsaufgabe erstellen und diesen Task auf mehreren Instanzen ausführen.

So zeichnen Sie die GUI-Konfiguration auf und wandeln sie in eine Konfigurationsaufgabe um:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**, und klicken Sie dann auf **Job erstellen**.
2. Geben Sie den Jobnamen und den Instanztyp an.
3. Wählen Sie in der Liste **Konfigurationsquelle** die Option **Aufzeichnen und Wiedergeben** aus, und wählen Sie dann die Quellinstanz aus, aus der die Konfiguration aufgezeichnet werden soll. Klicken Sie auf **Aufzeichnen**.



4. Die **Citrix ADC GUI** wird geöffnet. Konfigurieren Sie die Features und Einstellungen, die die Konfigurationsaufgabe enthalten soll. Schließen Sie dann das Citrix ADC GUI-Fenster, und klicken Sie im **Konfigurationseditor** auf **Beenden**. Die Befehle werden im linken Fensterbereich als Link angezeigt. Ziehen Sie die Befehle in den rechten Bereich und klicken Sie dann auf **Weiter**.



Anschließend können Sie die Befehle im Konfigurationseditor neu anordnen und neu anordnen. Sie können den Befehl von einer Zeile in eine andere verschieben, indem Sie die Befehlszeile ziehen und ablegen. Sie können die Befehlszeile auch von einer Zeile zu einer beliebigen Zielzeile verschieben oder neu anordnen, indem Sie einfach die Befehlszeilennummer im Textfeld ändern.

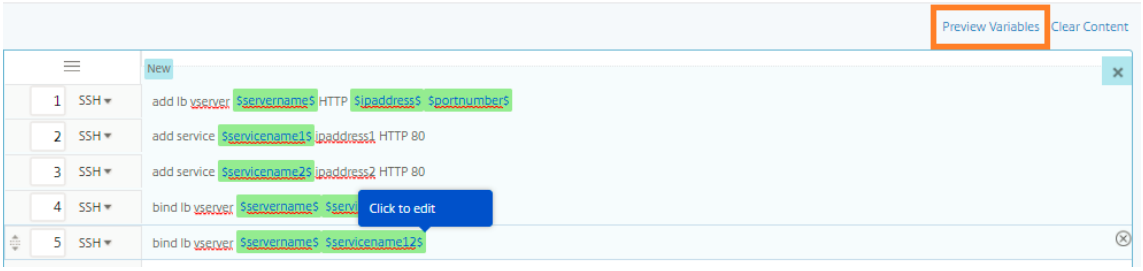
5. Sie können alle Variablen überprüfen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags in einer einzigen konsolidierten Ansicht definiert haben.

6. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:

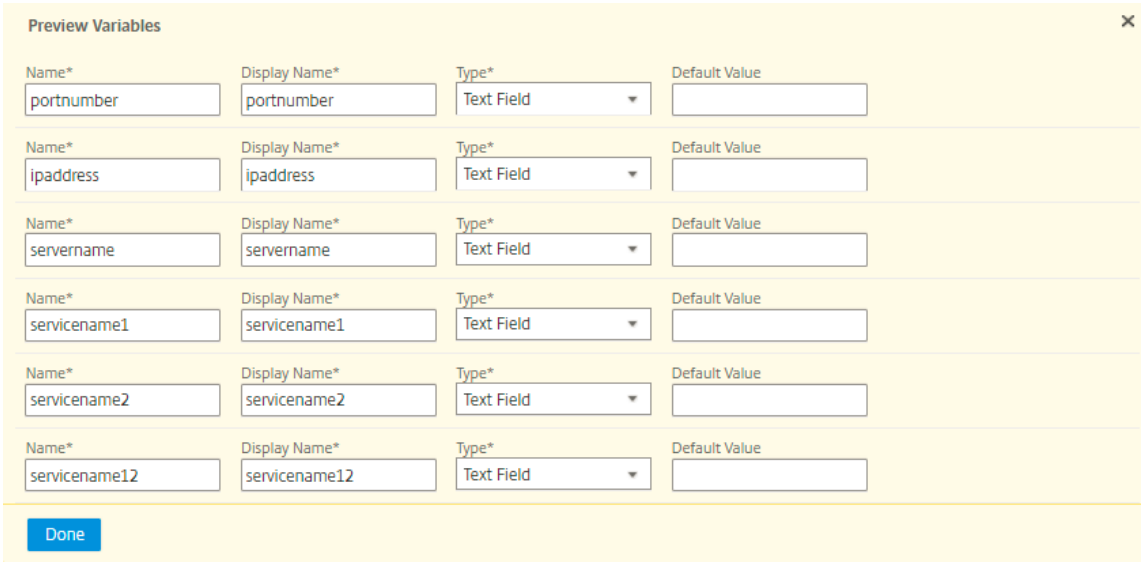
   - Navigieren Sie beim Erstellen eines Konfigurationsauftrags zu **Netzwerke > Konfigurationsaufträge** und wählen Sie **Auftrag erstellen**. Auf der Seite **Job erstellen** können Sie alle Variablen überprüfen, die Sie beim Erstellen des Konfigurationsauftrags hinzugefügt haben.
   - Während Sie einen Konfigurationsauftrag bearbeiten, navigieren Sie zu **Netzwerk > Konfigurationsjobs**, wählen Sie den Job-Namen aus und klicken Sie auf **Bearbeiten**. Auf der Seite **Job konfigurieren** können Sie alle Variablen überprüfen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.

7. Sie können dann auf die Registerkarte **Vorschauvariablen** klicken, um eine Vorschau der Variablen in einer einzelnen konsolidierten Ansicht anzuzeigen, die Sie beim Erstellen oder Bear-

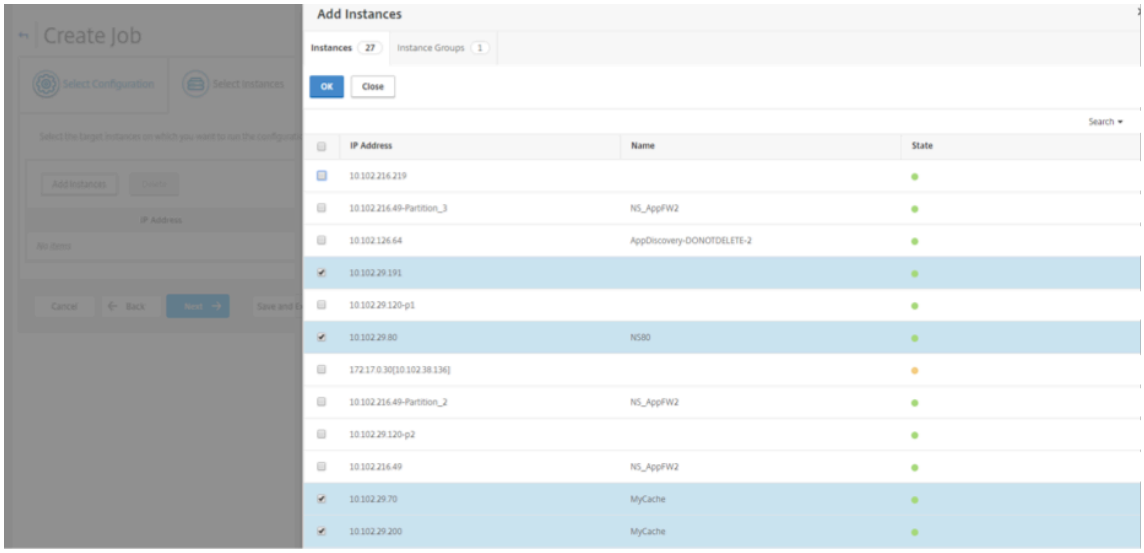
beiten eines Konfigurationsauftrags definiert haben.



8. Ein neues Popup-Fenster wird angezeigt, in dem alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem tabellarischen Format angezeigt werden. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Fertig**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.



9. Klicken Sie auf **Instanzen hinzufügen**, und wählen Sie die Instanzen aus, auf denen Sie den Konfigurationsauftrag ausführen möchten. Klicken Sie auf **OK**, und klicken Sie dann auf **Weiter**.



10. Wenn Sie Variablen in den Befehlen angegeben haben, wählen Sie auf der Registerkarte **Variablenwerte angeben** eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:

    - **Eingabedatei für Variablenwerte hochladen**: Klicken Sie auf **Eingabeschlüsseldatei** herunterladen, um eine Eingabedatei herunterzuladen. Geben Sie in der Eingabedatei Werte für die Variablen ein, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den Citrix ADM -Server hoch.
    - **Allgemeine Variablenwerte für alle Instanzen**: Geben Sie Werte für die Variablen ein. Die Variablen variieren je nach ausgewählter Vorlage.

    Die Eingabedateien, die die Variablenwerte enthalten, werden in den Konfigurationsaufträgen beibehalten (mit demselben Dateinamen). Sie können diese Eingabedateien anzeigen und bearbeiten, die Sie früher beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben.

    Um die Run Configuration Jobs beim Erstellen eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk** > **Konfigurationsjobs**und klicken Sie auf **Job erstellen**. Auf der Seite **Job erstellen**. Wählen Sie auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

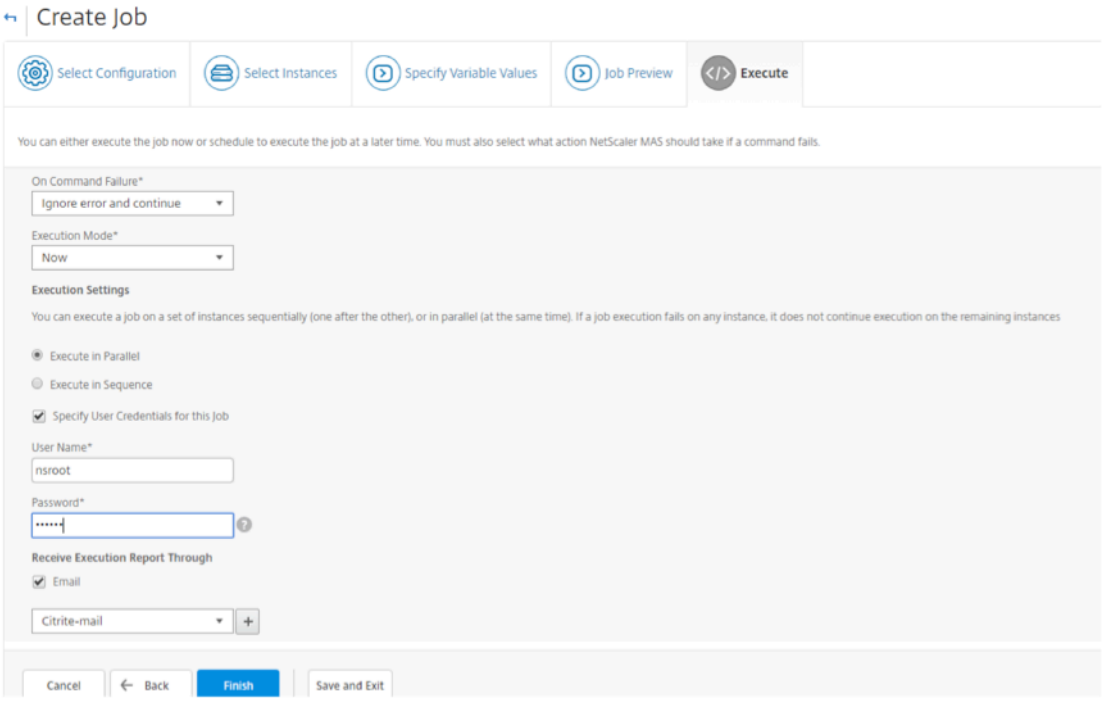
    Um die bereits ausgeführten Konfigurationsaufträge anzuzeigen, während Sie einen Konfigurationsauftrag bearbeiten, navigieren Sie zu **Netzwerk** > **Konfigurationsjobs**, wählen Sie den Job-Namen aus und klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite **Job konfigurieren** auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch

(unter Beibehaltung des gleichen Dateinamens).10. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.

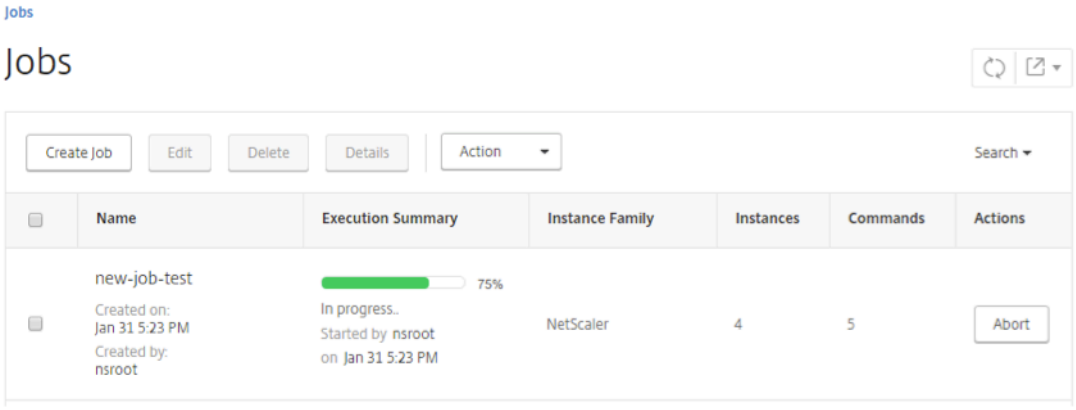
11. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.

12. Auf der Registerkarte**Ausführen**können Sie wählen, ob Sie Ihren Job jetzt ausführen oder planen, dass er später ausgeführt wird. Sie können auch auswählen, welche Aktion Citrix ADM ausführen muss, wenn der Befehl fehlschlägt.

    Sie können auch autorisierten Benutzern erlauben, Aufträge auf Ihren verwalteten Instanzen auszuführen, und Sie können wählen, ob Sie eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Auftrags zusammen mit anderen Details senden möchten.



13. Auf der Seite **Jobs** können Sie dann den Fortschritt der Ausführung der Konfigurationsaufgabe für alle Instanzen anzeigen.



Verwenden von Konfigurationsaufträgen, um die Konfiguration von einer Instanz auf mehrere Instanzen zu replizieren

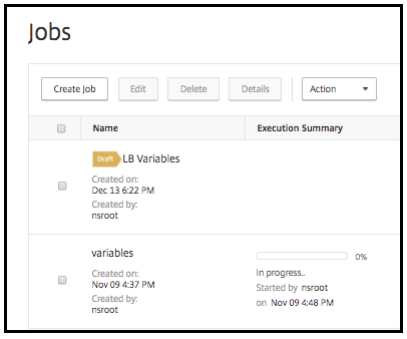
April 28, 2021

Möglicherweise haben Sie sowohl den Lastenausgleich als auch AppFlow auf einer Citrix ADC-Instanz für Ihre Bereitstellung konfiguriert. Jetzt möchten Sie jedoch nur die AppFlow Konfiguration auf andere Citrix ADC-Instanzen replizieren.

Sie können die Funktion Konfigurationsaufträge von Citrix Application Delivery Management (ADM) verwenden, um die AppFlow Konfiguration aus einer Citrix ADC-Instanz zu extrahieren und auf mehreren Instanzen zu replizieren.

So rufen Sie die Konfiguration von einer Instanz auf andere Citrix ADC-Instanzen ab und replizieren sie:

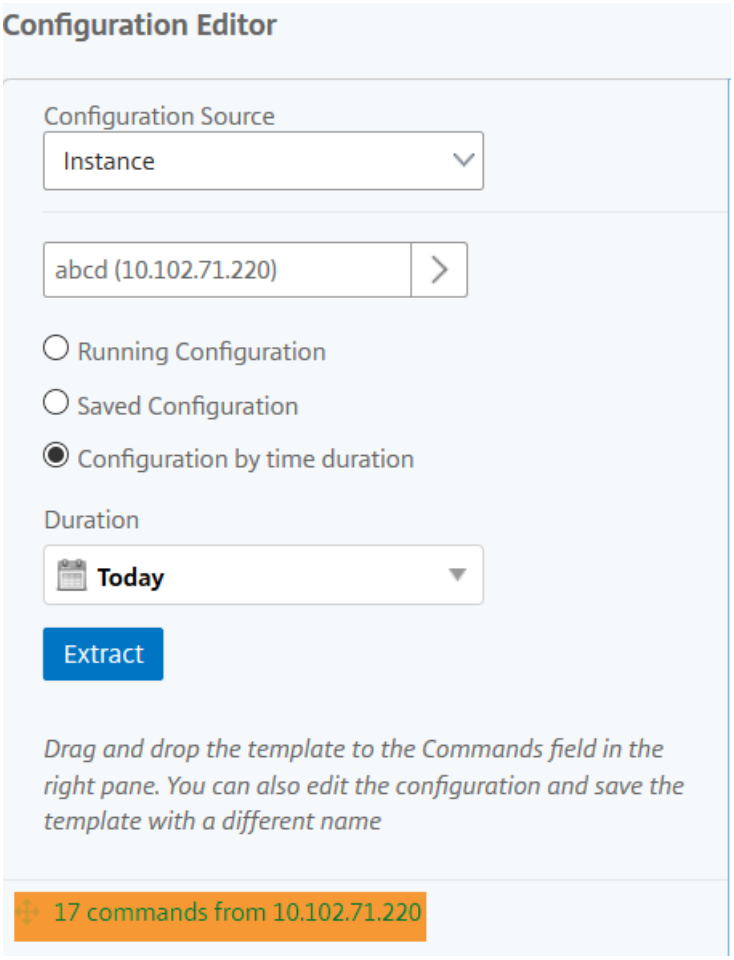
1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**, und klicken Sie dann auf **Job erstellen**.



2. Geben Sie den Jobnamen und den Instanztyp an.
3. Wählen Sie **Instanz** als **Konfigurationsquelle** aus, und wählen Sie die Quellinstanz aus, deren Konfiguration Sie replizieren möchten. Wählen Sie den Konfigurationstyp aus, den Sie

extrahieren möchten. Wenn Sie die Option Konfiguration nach Zeitdauer auswählen, legen Sie den Zeitraum fest, in dem Sie diese Konfiguration ausgeführt haben, und klicken Sie dann auf **Extrahieren**.

Die Anzahl der Befehle, die auf dieser Instanz in der von Ihnen ausgewählten Zeitdauer ausgeführt werden, wird auf dem Bildschirm angezeigt, wie in der Abbildung unten hervorgehoben.



4. Ziehen Sie die Befehle in das Feld **Befehle** im rechten Fensterbereich.

Behalten Sie nur die Befehle im Zusammenhang mit FEO bei und löschen Sie manuell die Befehle für den Lastenausgleich oder Befehle, die sich auf eine andere Konfiguration beziehen, und klicken Sie dann auf **Weiter**.

5. Klicken Sie auf **Instanzen hinzufügen**, und fügen Sie die Instanzen hinzu, auf die Sie die FEO-Konfiguration anwenden möchten. Klicken Sie auf **OK**, und klicken Sie dann auf **Weiter**.

   Wenn Sie in den Befehlen Variablen angegeben haben, klicken Sie auf der Registerkarte Variablenwerte angeben auf **Eingabeschlüsseldatei herunterladen**. Geben Sie in der heruntergeladenen Datei Werte für die Variablen an, und laden Sie die Datei dann in Citrix ADM hoch.

Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.

Klicken Sie auf der Registerkarte **Execute** auf **Finish**, um den Job auf den ausgewählten Citrix ADC-Instanzen auszuführen.

Verwenden von Variablen in Konfigurationsaufträgen

April 28, 2021

Ein Konfigurationsauftrag besteht aus einer Reihe von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Wenn Sie dieselbe Konfiguration auf mehreren Instanzen ausführen, möchten Sie möglicherweise andere Werte für die in Ihrer Konfiguration verwendeten Parameter verwenden. Sie können Variablen definieren, mit denen Sie verschiedene Werte für diese Parameter zuweisen oder einen Auftrag über mehrere Instanzen ausführen können.

Betrachten Sie beispielsweise eine grundlegende Lastausgleichskonfiguration, bei der Sie einen virtuellen Lastausgleichsserver hinzufügen, zwei Dienste hinzufügen und die Dienste an den virtuellen Server binden. Nun möchten Sie möglicherweise dieselbe Konfiguration auf zwei Instanzen haben, aber mit unterschiedlichen Werten für die Namen des virtuellen Servers und der Dienste und IP-Adressen. Sie können die Konfigurationsaufträge Funktion verwenden, um dies zu erreichen, indem

Sie Variablen verwenden, um die Namen und IP-Adressen des virtuellen Servers und der Dienste zu definieren.

In diesem Beispiel werden die folgenden Befehle und Variablen verwendet:

```
add lb vserver \*\*servername\*\* HTTP \*\*ipaddress\*\* \*\*portnumber
    \*\*

add service \*\*servicename1\*\* \*\*ipaddress1\*\* HTTP 80

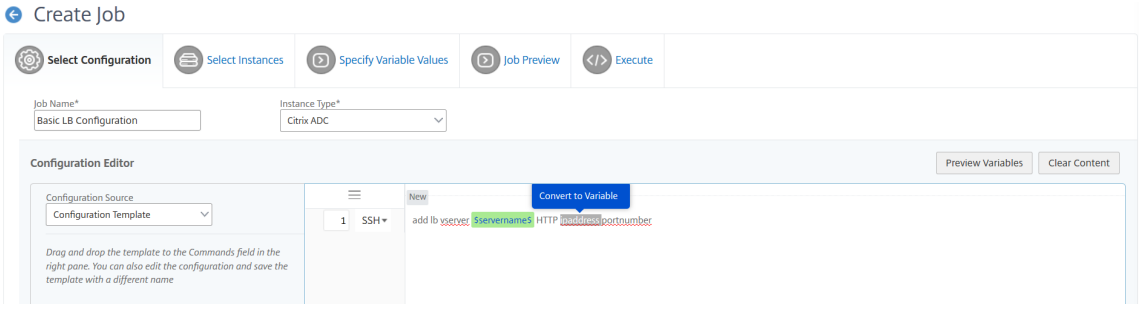
add service \*\*servicename2\*\* \*\*ipaddress2\*\* HTTP 80

bind lb vserver \*\*servername\*\* \*\*servicename1\*\*

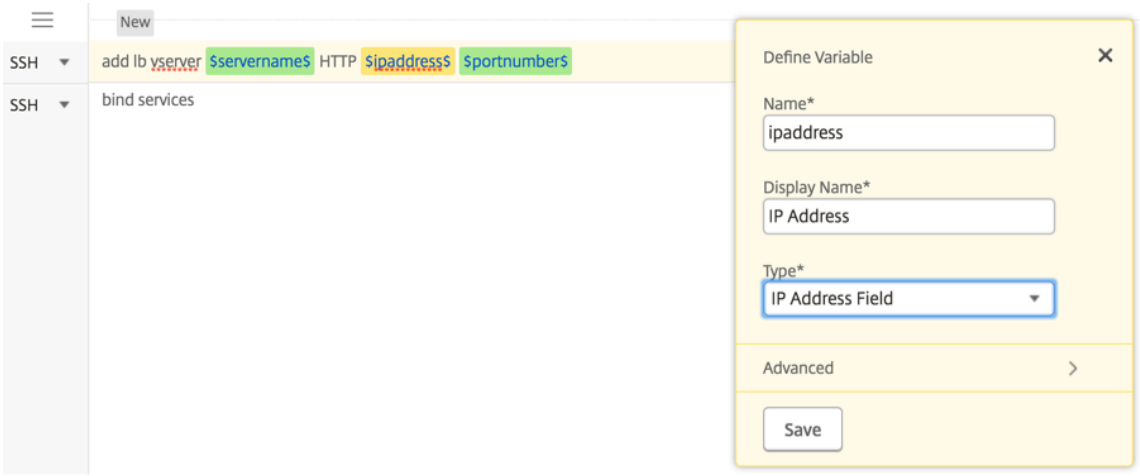
bind lb vserver \*\*servername\*\* \*\*servicename2\*\*
<!--NeedCopy-->
```

So erstellen Sie einen Konfigurationsauftrag durch Definieren von Variablen in Citrix ADM:

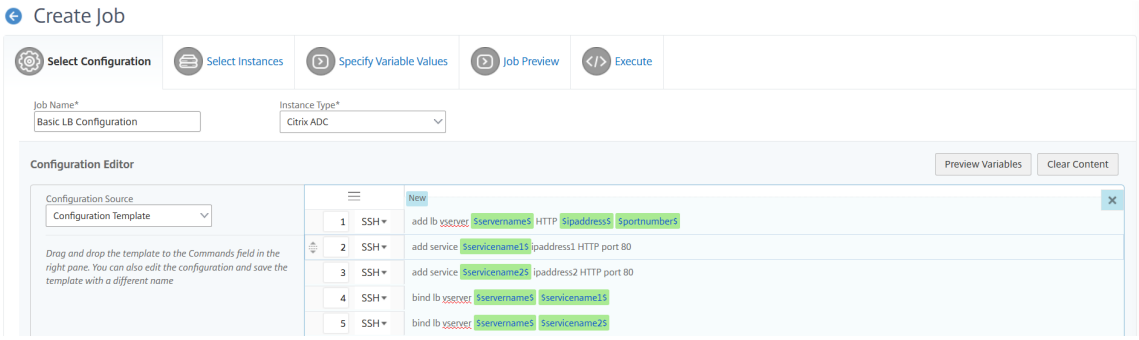
1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**.
2. Klicken Sie auf **Job erstellen**.
3. Wählen Sie auf der Seite **Job erstellen** die benutzerdefinierten Jobparameter aus, z. B. den Namen des Jobs, den Instanztyp und den Konfigurationstyp.
4. Geben Sie im Konfigurationseditor die Befehle ein, um einen virtuellen Lastausgleichsserver, zwei Dienste hinzuzufügen und die Dienste an den virtuellen Server zu binden. Doppelklicken Sie, um die Werte auszuwählen, die Sie in eine Variable konvertieren möchten, und klicken Sie dann **auf In Variable umwandeln**. Wählen Sie beispielsweise die IP-Adresse des Load Balancing-Servers aus und klicken Sie auf In **Variable konvertieren** `ipaddress`, wie in der Abbildung unten gezeigt.



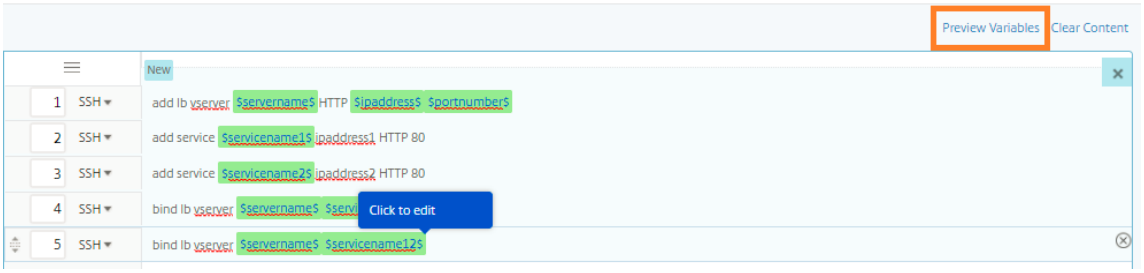
5. Wenn Sie sehen, dass Dollarzeichen den Wert der Variablen einschließen, klicken Sie auf die Variable, um die Details der Variablen wie Name, Anzeigename und Typ anzugeben. Sie können auch auf die Option **Erweitert** klicken, wenn Sie einen Standardwert für Ihre Variable weiter angeben möchten. Klicken Sie auf **Speichern**, und klicken Sie dann auf **Weiter**.



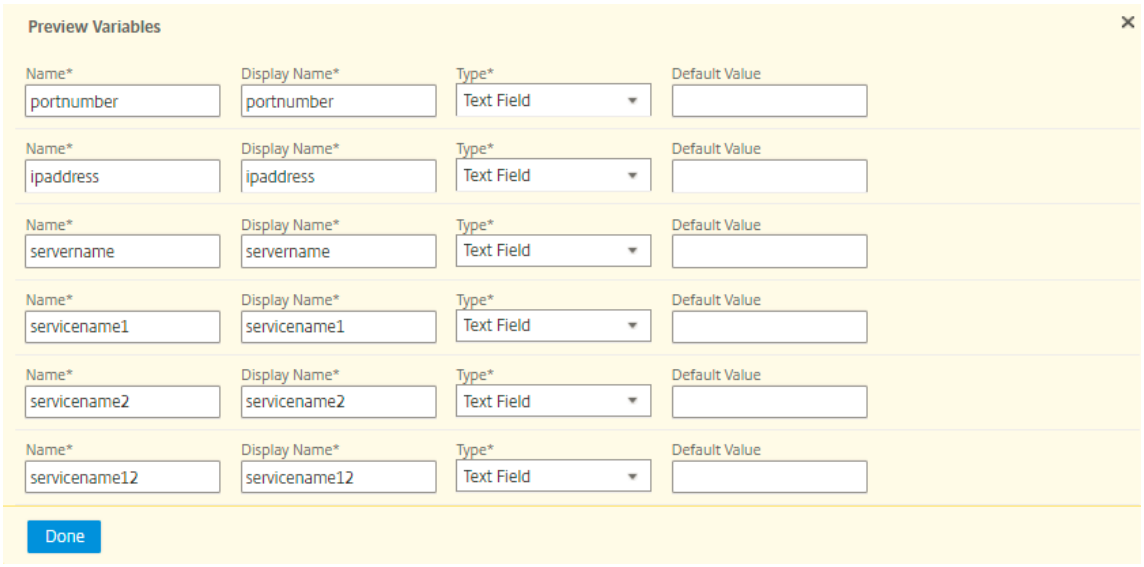
Geben Sie die restlichen Befehle ein und definieren Sie alle Variablen.



6. Sie können alle Variablen überprüfen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags in einer einzigen konsolidierten Ansicht definiert haben.
7. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:
   - Navigieren Sie beim Erstellen eines Konfigurationsauftrags zu **Netzwerke** > **Konfigurationsaufträge**und wählen Sie **Job erstellen**aus. Auf der Seite **Job erstellen** können Sie alle Variablen überprüfen, die Sie beim Erstellen des Konfigurationsauftrags hinzugefügt haben.
   - Navigieren Sie beim Bearbeiten eines Konfigurationsauftrags zu **Netzwerk** > **Konfigurationsaufträge**, wählen Sie den Auftragsnamen aus und klicken Sie auf **Bearbeiten**. Auf der Seite **Job konfigurieren** können Sie alle Variablen überprüfen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.
8. Sie können dann auf die Registerkarte **Vorschauvariablen** klicken, um eine Vorschau der Variablen in einer einzelnen konsolidierten Ansicht anzuzeigen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben.



9. Ein neues Popup-Fenster wird angezeigt, in dem alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem tabellarischen Format angezeigt werden. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Fertig**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.



10. Anschließend können Sie die Befehle im Konfigurationseditor neu anordnen und neu anordnen. Sie können den Befehl von einer Zeile in eine andere verschieben, indem Sie die Befehlszeile ziehen und ablegen. Sie können die Befehlszeile auch von einer Zeile zu einer beliebigen Zielzeile verschieben oder neu anordnen, indem Sie einfach die Befehlszeilennummer im Textfeld ändern.
11. Wählen Sie die Instanzen aus, auf denen Sie den Konfigurationsauftrag ausführen möchten.
12. Wählen **Sie auf der Registerkarte Variablenwerte angeben** die Option **Eingabedatei für Variablenwerte hochladen** aus, und klicken Sie dann auf **Eingabeschlüsseldatei herunterladen**. In unserem Beispiel müssen Sie den Servernamen für jede Instanz, die IP-Adressen des Servers und der Dienste, die Portnummern und die Dienstnamen angeben. Speichern Sie die Datei und laden Sie sie hoch. Wenn Ihre Werte nicht genau definiert sind, kann das System einen Fehler auslösen.
13. Die Eingabeschlüsseldatei wird auf Ihr lokales System heruntergeladen und Sie können sie bearbeiten, indem Sie die Variablenwerte für jede zuvor ausgewählte Citrix ADC-Instanz angeben

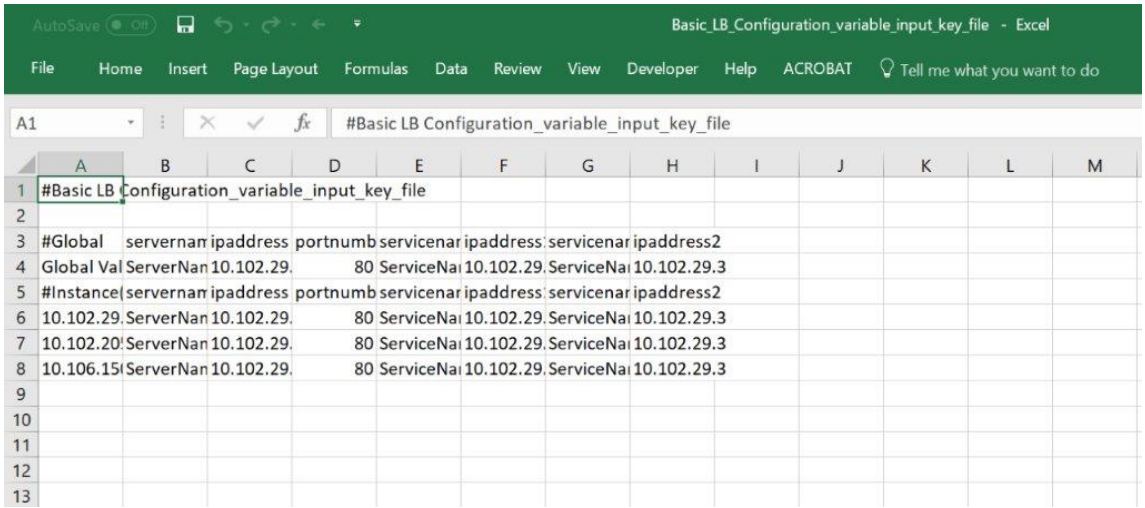
und auf **Hochladen** klicken, um die Eingabeschlüsseldatei in Citrix Application Delivery Management (ADM) hochzuladen. Klicken Sie auf **Weiter**. Die Eingabeschlüsseldatei wird in Ihr lokales System heruntergeladen und Sie können sie bearbeiten, indem Sie die Variablenwerte für jede zuvor ausgewählte Citrix ADC-Instanz angeben.

> **Hinweis**
>
> In der Eingabeschlüsseldatei werden die Variablen auf drei Ebenen definiert:
>
> ```
> 1    -  Globale Ebene
> ```
>
> - Instanzgruppenebene
> - Instanzebene

Globale Variablen sind Variablenwerte, die über alle Instanzen hinweg angewendet werden. Variablenwerte auf Instanzgruppenebene werden auf alle Instanzen angewendet, die in einer Gruppe definiert sind. Variablenwerte auf Instanzebene werden nur auf eine bestimmte Instanz angewendet.

Citrix ADM gibt den Werten der Instanzebene erste Priorität. Wenn den Variablen für einzelne Instanzen keine Werte bereitgestellt werden, verwendet Citrix ADM den auf Gruppenebene bereitgestellten Wert. Wenn auf Gruppenebene keine Werte bereitgestellt werden, verwendet Citrix ADM den auf globaler Ebene bereitgestellten Variablenwert. Wenn Sie eine Eingabe für eine Variable über alle drei Ebenen hinweg bereitstellen, verwendet Citrix ADM den Wert der Instanzebene als Standardwert.

14. Klicken **Sie auf Hochladen**, um die Eingabeschlüsseldatei in Citrix ADM hochzuladen. Klicken Sie auf **Weiter**.



> **Wichtig**
>
> Wenn Sie eine CSV-Datei von einem Mac hochladen, speichert Mac die CSV-Datei mit Semikolons statt Kommas. Dies führt dazu, dass die Konfiguration fehlschlägt, wenn Sie die Eingabedatei hochladen und den Auftrag ausführen. Wenn Sie einen Mac verwenden, verwenden Sie einen Texteditor, um die erforderlichen Änderungen vorzunehmen und dann die Datei hochzuladen.

15. Sie können auch gemeinsame Variablenwerte für alle Instanzen angeben und auf **Hochladen** klicken, um die Eingabeschlüsseldatei in Citrix ADM hochzuladen.

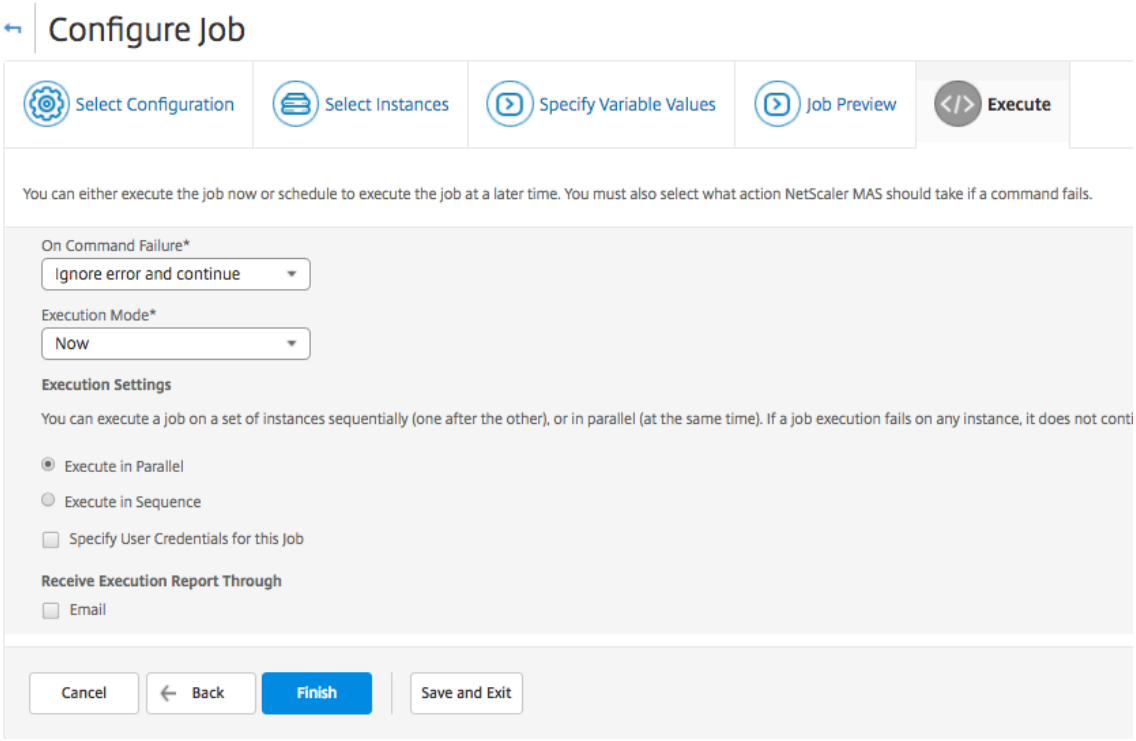
    Die Schlüsseleingabedateien, die die Variablenwerte enthalten, werden in den Konfigurationsaufträgen beibehalten (mit demselben Dateinamen). Sie können diese Eingabedateien anzeigen und bearbeiten, die Sie früher beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben.

    Um die Run Configuration Jobs beim Erstellen eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk** > **Konfigurationsjobs**und klicken Sie auf **Job erstellen**. Auf der Seite **Job erstellen**. Wählen Sie auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

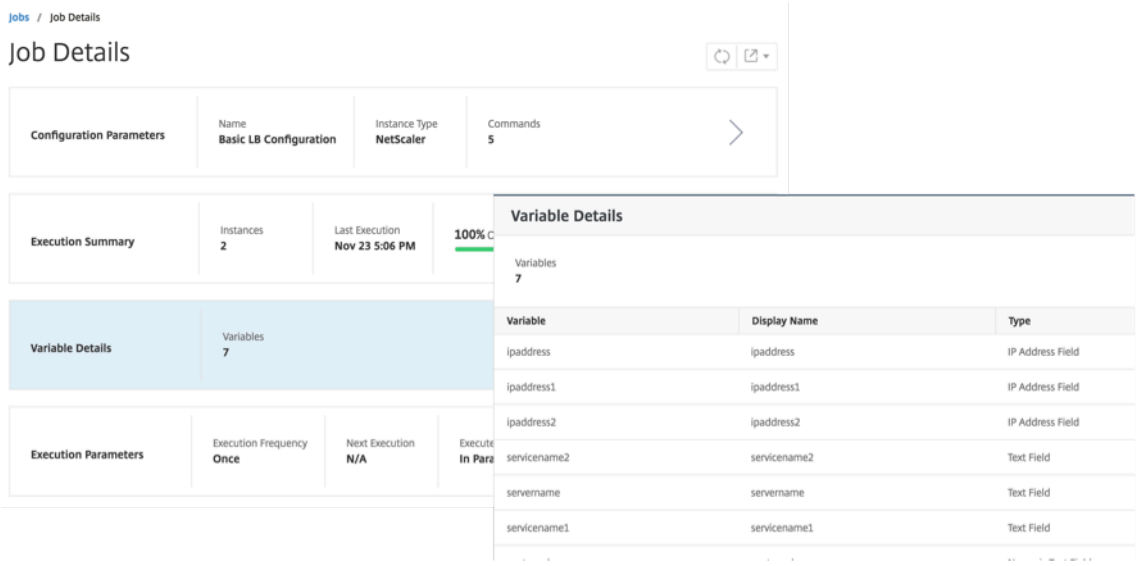
    Um die bereits ausgeführten Konfigurationsaufträge anzuzeigen, während Sie einen Konfigurationsauftrag bearbeiten, navigieren Sie zu **Netzwerk** > **Konfigurationsjobs**, wählen Sie den Job-Namen aus und klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite **Job konfigurieren** auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

16. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.

17. Auf der Registerkarte " **Ausführen** " können Sie Ihren Job jetzt ausführen oder planen, dass er später ausgeführt wird. Sie können auch auswählen, welche Aktion Citrix ADM ausführen muss, wenn der Befehl fehlschlägt und Sie eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Jobs zusammen mit anderen Details senden möchten.



Nachdem Sie Ihre Jobs konfiguriert und ausgeführt haben, können Sie die Auftragsdetails anzeigen, indem Sie zu **Netzwerke** > **Konfigurationsaufträge** navigieren und den von Ihnen konfigurierten Job auswählen. Klicken Sie auf **Details** und dann auf **Variablendetails**, um die Liste der Variablen anzuzeigen, die Ihrem Job hinzugefügt wurden.



> **Hinweis**
>
> Die Werte, die Sie für die Variablen in **Schritt 5** angegeben haben, werden von Citrix ADM beibehalten, wenn Sie den Auftrag speichern und beenden oder wenn Sie planen, dass ein Job

> zu einem späteren Zeitpunkt ausgeführt wird.

Erstellen von Konfigurationsaufträgen aus Korrekturbefehlen

April 28, 2021

Sie können die Überwachungsvorlagenfunktion in Citrix Application Delivery Management (ADM) verwenden, um Konfigurationsänderungen über verwaltete Citrix ADC-Instanzen hinweg zu überwachen und Konfigurationsfehler zu beheben.

Der typische Workflow für das Auditing von Konfigurationsänderungen mithilfe von Audit-Vorlagen besteht aus den folgenden Schritten.

1. Erstellen Sie eine Überwachungsvorlage mit einer Reihe gültiger/erwarteter Citrix ADC-Befehle für die Überwachung von Instanzkonfigurationen.
2. Wählen Sie die Citrix ADC-Instanzen aus, für die Sie die Überwachungsvorlage ausführen möchten, um auf Unterschiede zwischen der laufenden Konfiguration und den erwarteten Konfigurationen zu überprüfen.
3. Verstehen Sie die Differenz-/Korrekturbefehle und nutzen Sie die Funktion Job erstellen, um die Konfigurationen der Instanz in den gewünschten Zustand zu versetzen.

Betrachten Sie ein Szenario, in dem mehrere Administratoren fünf Citrix ADC-Instanzen verwalten. Alle diese Administratoren aktualisieren die vorhandene Instanzkonfiguration, sobald Änderungen erforderlich sind. Der Superadministrator möchte sicherstellen, dass ein bestimmter Satz wichtiger Konfiguration unberührt bleibt, unabhängig von den von anderen Administratoren vorgenommenen Änderungen. Für diesen Anwendungsfall erstellt der Superadministrator eine Vorlage der Konfiguration, die voraussichtlich auf den Citrix ADC-Instanzen vorhanden ist, und führt sie für die Instanzen aus. Citrix ADM vergleicht die Überwachungsvorlagenkonfiguration mit der ausgeführten Konfiguration und meldet eventuelle Abweichungen im Dashboard **Configuration Audit**.

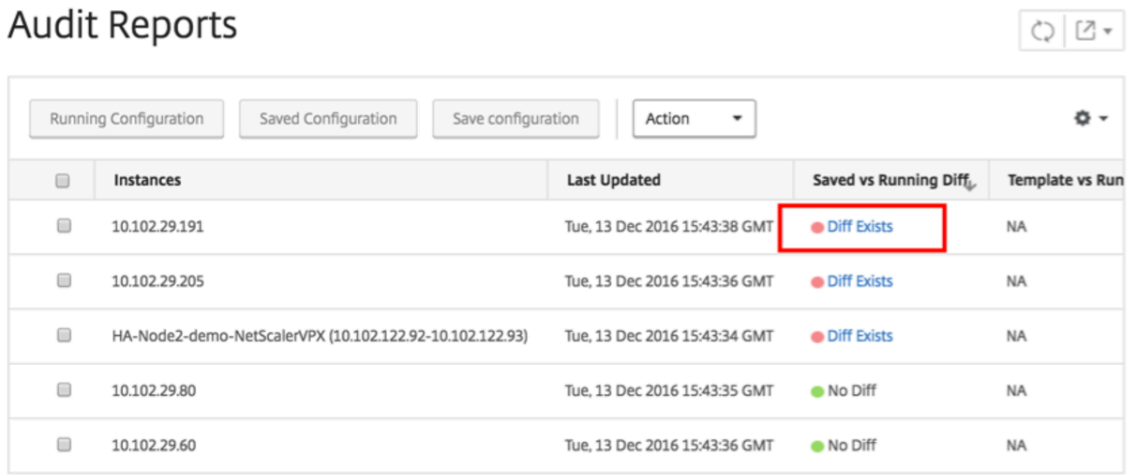
Wenn Sie feststellen, dass sich die Konfiguration einiger Instanzen ändert, können Sie die ADM-Korrekturbefehlsfunktion verwenden, um einen Konfigurationsauftrag mit den geänderten und korrigierten Konfigurationsbefehlen für bestimmte Citrix ADC-Instanzen zu erstellen.

Wenn zwischen der Konfiguration der Überwachungsvorlage und der ausgeführten Konfiguration ein Unterschied besteht, wird auf der Seite " **Audit-Bericht** " eine Statusmeldung " **Diff Exists** " angezeigt. Wenn Sie auf den Link " **Diff beendet** " klicken, gelangen Sie zur Seite " **Konfigurationsdiff** ", auf der Sie den Korrekturbefehl anzeigen können. Sie können diese fehlerbehebenden Befehle auch verwenden, um einen Konfigurationsauftrag zu erstellen und diesen auf den spezifischen Citrix ADC-Instanzen auszuführen, um sie wieder in die gewünschte Konfiguration zu bringen.

So erstellen Sie einen Konfigurationsauftrag aus Korrekturbefehlen in Citrix ADM:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsüberwachung**.

2. Klicken Sie auf der Seite **Konfigurationsüberwachung** in eines der beiden Donutdiagramme, um die Seite **Überwachungsberichte** aufzurufen.
3. Klicken Sie für die Instanz, für die Sie die Konfigurationsbefehle korrigieren möchten, auf den Link **Diff existiert** (unter der Spalte **Gespeichert vs Laufendes Diff** in der Tabelle). Die Seite **Konfigurationsabweichung** wird angezeigt, auf der die Unterschiede zwischen der gespeicherten Konfiguration, der laufenden Konfiguration und der Korrekturkonfiguration für diese Instanz aufgeführt sind.



4. Klicken Sie auf **Job erstellen**, um zur Seite **Job erstellen** zu gehen, auf der die Korrekturbefehle bereits ausgefüllt wurden. Anweisungen zum Erstellen eines Konfigurationsauftrags finden Sie unterErstellen eines Konfigurationsauftrags unter Citrix ADM.

Replizieren der laufenden und gespeicherten Konfiguration von einer Citrix ADC-Instanz auf eine andere

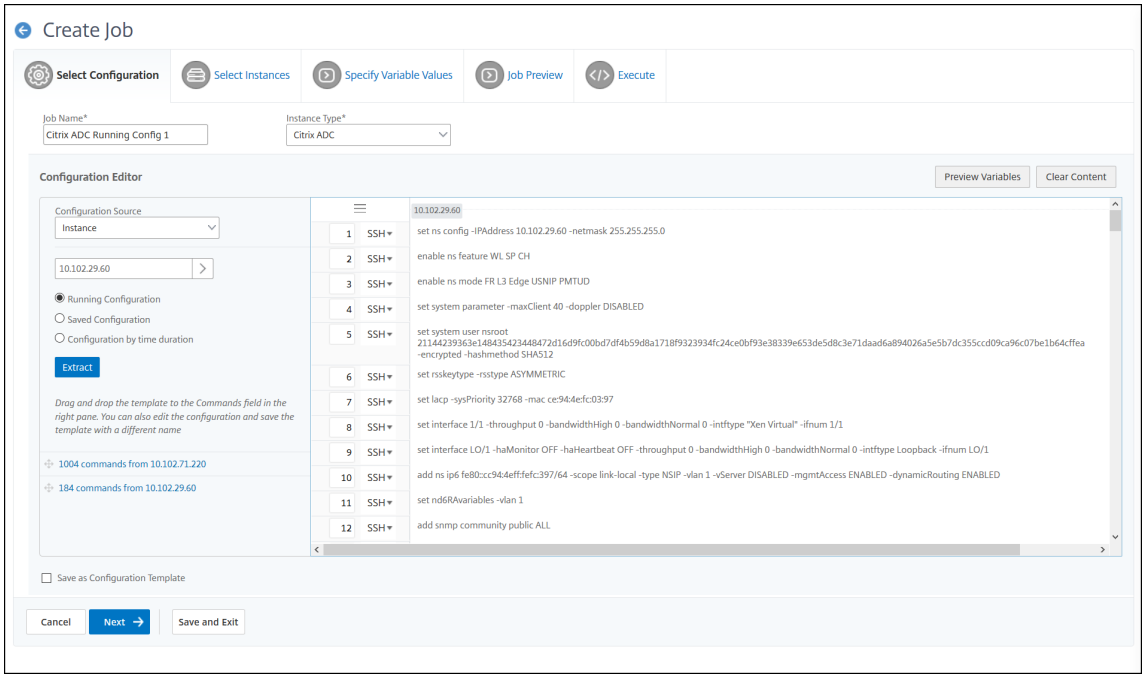
April 28, 2021

Sie können nun die Konfiguration einer Citrix ADC-Instanz auf anderen Instanzen replizieren. Wenn Sie einen Auftrag in Citrix Application Delivery Management (ADM) konfigurieren, wählen Sie eine Instanz als Konfigurationsquelle aus, und wählen Sie die ausgeführte oder gespeicherte Konfiguration der ausgewählten Instanz aus.

Wenn Sie beispielsweise **Laufende Konfiguration** auswählen und auf **Extrahieren** klicken, sendet Citrix ADM eine Anforderung an die ausgewählte Citrix ADC-Instanz, um die ausgeführte Konfiguration zu finden, und zeigt sie als Vorlage an. Sie können die Vorlage in das Feld **Befehle** im rechten Bereich ziehen. Sie können Befehle, Parameter und die Instanzen ändern.

So replizieren Sie laufende und gespeicherte Konfigurationsbefehle einer Instanz auf eine andere Instanz auf Citrix ADM:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**, und klicken Sie auf **Job erstellen**.
2. Geben Sie den Jobnamen und den Instanztyp an. Geben Sie beispielsweise *Citrix ADC Running Config1* als Namen Ihres Auftrags und den Instanztyp als *Citrix ADC an*.
3. Wählen Sie **Instanz** als **Konfigurationsquelle**, und wählen Sie die Quellinstanz aus, deren Konfiguration Sie auf anderen Instanzen replizieren möchten.
4. Sie sehen die folgenden drei Optionen:
   - Laufende Konfiguration
   - Gespeicherte Konfiguration
   - Konfiguration nach Zeitdauer
5. Wählen Sie **Konfiguration ausführen**und klicken Sie auf **Extrahieren**. Die Anzahl der ausgeführten Konfigurationsbefehle, die auf dieser Instanz ausgeführt werden, wird angezeigt.



6. Ziehen Sie die Befehle in das Feld **Befehle** im rechten Fensterbereich.
7. Sie können die Befehle im Feld Befehle bearbeiten. Wenn die extrahierten Befehle beispielsweise eine Citrix ADC-Instanz einrichten sollen. Dies kann das Hinzufügen von Partitionen, das Einrichten des Lastenausgleichs, das Binden des Lastausgleichsservers an Dienste usw. umfassen. Sie können Ihre Befehle bearbeiten, um Ihre neuen Citrix ADC-Instanzen ohne Partitionen einzurichten. Um Partitionen zu entfernen, löschen Sie manuell Befehle im Zusammenhang mit der Erstellung von Partitionen und klicken Sie auf **Weiter**.
8. Klicken Sie auf **Instanzen hinzufügen**, und fügen Sie die Instanzen hinzu, auf die Sie die ausgeführten Konfigurationsbefehle anwenden möchten. Klicken Sie auf **OK**, und klicken Sie dann auf **Weiter**.
9. Wenn Sie Variablen in den Befehlen angegeben haben, klicken Sie auf der Registerkarte **Variablenwerte angeben** auf **Eingabeschlüsseldatei herunterladen**. Geben Sie in der heruntergeladenen Datei Werte für die Variablen an, und laden Sie die Datei dann in Citrix ADM hoch.
10. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.
11. Auf der Registerkarte " **Ausführen** " können Sie Ihren Job jetzt ausführen oder planen, dass er später ausgeführt wird. Sie können auch auswählen, welche Aktion Citrix ADM ausführen muss, wenn der Befehl fehlschlägt und Sie eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Jobs zusammen mit anderen Details senden möchten.

Wiederverwendung von Ausführungsaufträgen

April 28, 2021

Mit Konfigurationsaufträgen können Sie eine Reihe von Konfigurationsbefehlen erstellen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Sie können denselben Satz gespeicherter Konfigurationsaufträge auch ausführen, nachdem Sie die Befehle, Parameter, Konfigurationsquelle und Instanzen im Auftrag geändert haben. Diese Funktion ist nützlich, wenn derselbe Befehlssatz auf einer anderen Instanz ausgeführt werden muss oder wenn der Auftrag auf einen Fehler trifft und die weitere Ausführung stoppt.

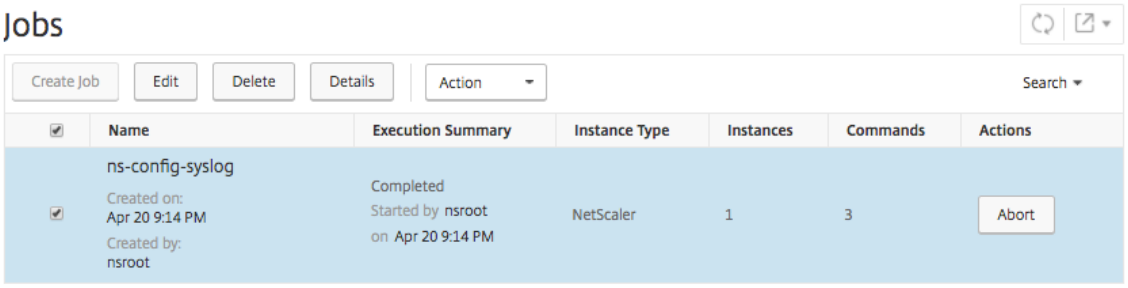
Citrix Application Delivery Management (ADM) bietet eine Funktion zum erneuten Ausführen der abgeschlossenen Aufträge. Mit dieser Funktion können Jobs, die vollständig ausgeführt werden, erneut ausgeführt werden, ohne den Jobnamen zu ändern.

> **Hinweis:**
>
> Sie können nur die Jobs erneut ausführen, die ausgeführt werden, wenn der Ausführungsmodus

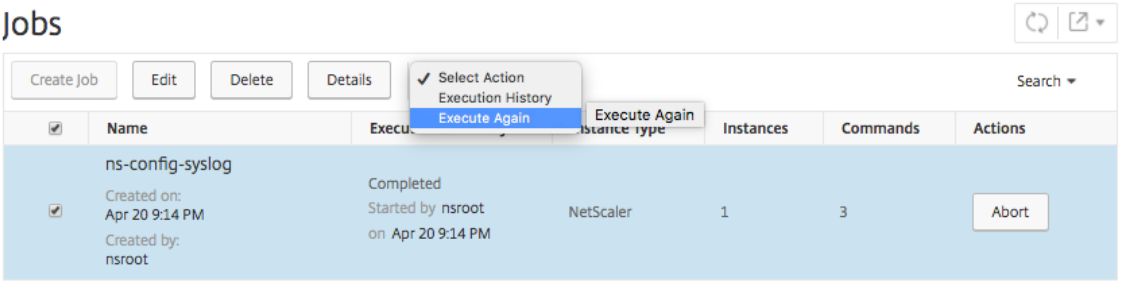
> "Jetzt" ist.

So bearbeiten Sie abgeschlossene Aufträge:

1. Navigieren Sie auf der ADM-Homepage zu **Netzwerke** > **Konfigurationsjobs**.
2. Wählen Sie auf der Seite **Jobs** einen Job aus, der die Ausführungsübersicht als abgeschlossen anzeigt, und klicken Sie auf **Bearbeiten**. Sie können auch einen geplanten Konfigurationsauftrag bearbeiten.
3. Auf der Seite **Job konfigurieren** können Sie sehen, dass der Jobname und der Instanz-Typ nicht editierbar sind. Sie können andere Felder wie die Konfigurationsquelle ändern, Instanzen hinzufügen, Variablenwerte bearbeiten und Ausführungseinstellungen festlegen.
4. Klicken Sie auf **Fertig stellen**, um den Konfigurationsauftrag erneut auszuführen.



> **Hinweis**
>
> Sie können den Job auch auswählen und erneut auf **Ausführen** klicken, um den Job auszuführen, ohne Quelle, Instanz und Befehle zu ändern. Diese Option ist nützlich, wenn Sie dieselben Befehle für dieselben Instanzen ausführen müssen. Manchmal tritt der Auftrag möglicherweise auf einen vorübergehenden Fehler von der Serverseite auf, und Sie müssen den Auftrag möglicherweise erneut ausführen.



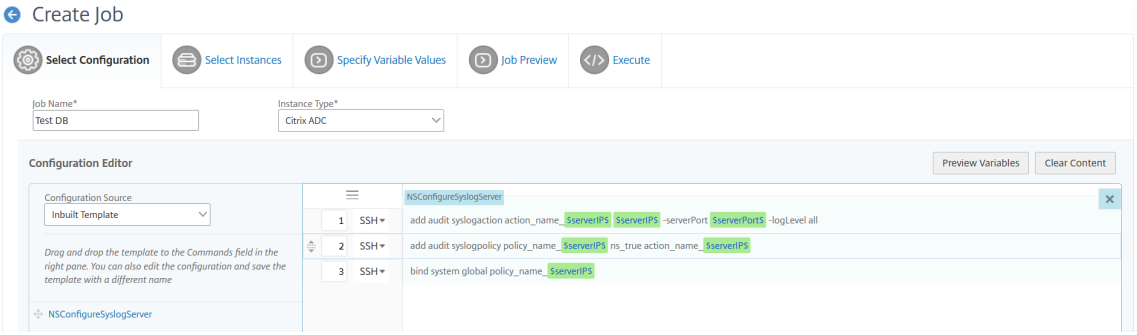
Planen von Jobs, die mit integrierten Vorlagen erstellt wurden

April 28, 2021

Sie können einen Job planen, indem Sie die integrierte Vorlagenoption verwenden. Ein Auftrag ist eine Reihe von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Sie können beispielsweise die integrierte Vorlagenoption verwenden, um einen Auftrag zum Konfigurieren von Syslog-Servern zu planen. Sie können den Job auch sofort ausführen oder den Job planen, der zu einem späteren Zeitpunkt ausgeführt werden soll.

So planen Sie einen Auftrag mithilfe integrierter Vorlagen in Citrix ADM:

1. Navigieren Sie in Citrix Application Delivery Management (ADM) zu **Netzwerke** > **Konfigurationsaufträge**, und klicken Sie dann auf **Job erstellen**.
2. Geben Sie auf der Seite **Job erstellen** auf der Registerkarte **Konfiguration auswählen** den **Auftragsnamen** an, und wählen Sie in der Dropdownliste den **Instanztyp** aus.
3. Wählen Sie in der Dropdownliste **Konfigurationsquelle** die Option **Inbuilt Template** aus. Ziehen Sie den Befehl *NSConfigureResysLogServer* in den rechten Bereich, und klicken Sie dann auf **Weiter**.



4. Klicken Sie auf der Registerkarte **Instanzen auswählen** auf **Instanzen hinzufügen**, wählen Sie die Instanzen aus, für die Sie den Auftrag ausführen möchten, und klicken Sie dann auf **OK**.
5. Klicken Sie auf **Weiter**. Wählen Sie auf der Registerkarte **Variablenwerte angeben** eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:
   - **Variablenwerte aus einer Eingabedatei** : Laden Sie eine Eingabedatei herunter, um Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den Citrix ADM -Server hoch.
   - **Allgemeine Variablenwerte für alle Instanzen** — Geben Sie die IP-Adresse und den Port des Syslog-Servers an.
6. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.
7. Klicken Sie auf **Weiter**.
8. Legen Sie auf der Registerkarte **Ausführen** die folgenden Bedingungen fest:
   - **Bei Befehlsfehler** - Wenn ein Befehl fehlschlägt, können Sie entweder die Fehler ignorieren und den Job weiterhin ausführen oder die weitere Ausführung des Jobs stoppen.

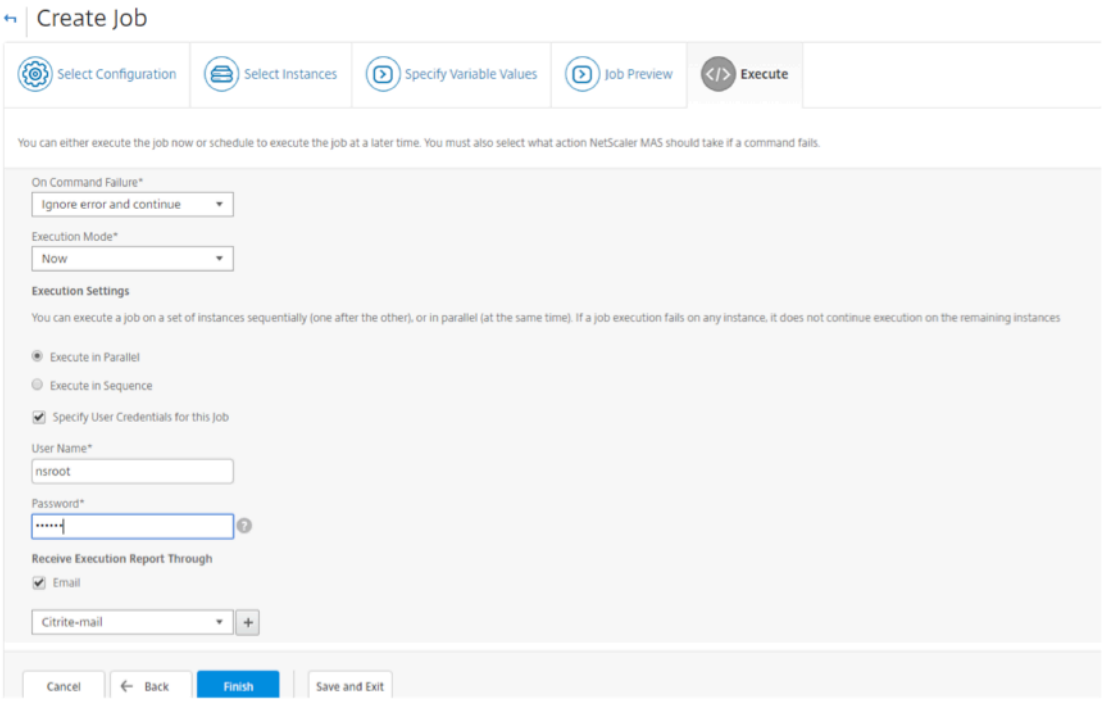
Wählen Sie in der Dropdownliste die Aktion aus, die Sie ausführen möchten.

- **Ausführungsmodus** - Sie können den Job entweder jetzt ausführen oder die spätere Ausführung des Auftrags planen. Wenn Sie den Job später planen möchten, müssen Sie die Ausführungsfrequenzeinstellungen für diesen Job angeben. Wählen Sie aus der Dropdownliste den Zeitplan aus, dem der Auftrag folgen soll.

9. Sie können einen Auftrag auch für eine Reihe von Instanzen sequenziell oder parallel ausführen, indem Sie die erforderliche Methode unter **Ausführungseinstellungen**auswählen. Wenn eine Auftragsausführung auf einer Instanz fehlschlägt, wird sie auf den verbleibenden Instanzen nicht fortgesetzt.

   Sie können auch autorisierten Benutzern erlauben, Aufträge auf Ihren verwalteten Instanzen auszuführen, und Sie können wählen, ob Sie eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Auftrags zusammen mit anderen Details senden möchten.

10. Klicken Sie auf **Fertig stellen**.



Verwenden von Wartungsaufträgen zum Aktualisieren von Citrix ADC SDX-Instanzen

April 28, 2021

Sie können ein Einzelbündel-Upgrade Ihrer Citrix ADC SDX-Instanzen mit Citrix ADC Version 11.0 und höher durchführen. Um ein Single-Bundle-Upgrade durchzuführen, verwenden Sie eine integrierte

Aufgabe in Citrix Application Delivery Management (ADM). Mit dieser integrierten Aufgabe können Sie den Citrix ADC SDX Management Service, den XenServer-Hypervisor sowie die zusätzlichen Packs und Hotfixes für Citrix Hypervisor aktualisieren.

So aktualisieren Sie Citrix ADC SDX-Instanzen mithilfe von Citrix ADM:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsjobs** > **Wartungsaufträge.**
2. Klicken Sie auf **Job erstellen**. Wählen Sie auf der Seite Auftrag erstellen den integrierten Task **Upgrade Citrix ADC SDX** aus, um Ihre Citrix ADC SDX-Instanzen zu aktualisieren. Klicken Sie auf **Weiter**.
3. Geben Sie auf der Seite " **Citrix ADC Appliances aktualisieren** " auf der Registerkarte " **Instanzauswahl** " den **Job-Namen** an und klicken Sie auf **Add Instanzen**.
4. Wählen Sie die Zielinstanzen oder Instanzgruppen aus, die Sie aktualisieren möchten.
5. Nachdem Sie die Citrix ADC-Instanzen oder Instanzgruppen hinzugefügt haben, klicken Sie auf **Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten. Auf dem Bildschirm wird der Fortschritt der Vorvalidierung der einzelnen Citrix ADC-Instanzen angezeigt.
6. Wählen Sie auf der Seite **Upgrade Citrix ADC Appliance (en) ändern** die Registerkarte **Upgrade** aus. Wählen Sie im Dropdownmenü **Software-Image** entweder **Lokal** (Ihr lokaler Computer) oder **Appliance** (die Builddatei muss auf Citrix ADM vorhanden sein).
7. Sie können auch sehen, ob Instanzen Fehler beim Upgrade vor der Validierung aufweisen. Diese Fehler werden in Form einer Nachricht angezeigt. Die Meldungen zeigen die Fehler im Zusammenhang mit Speicherplatz, Festplattenlaufwerk und Benutzeranpassungen an. Wenn Sie nicht mit Instanzen fortfahren möchten, die die Überprüfung vor der Validierung fehlgeschlagen haben, können Sie die Instanzen entfernen. Um die Instanzen zu entfernen, wählen Sie die Instanzen aus, und klicken Sie auf **Löschen**.
8. Auf der Registerkarte **Task planen** können Sie auch Ausführungsdetails festlegen, in denen Sie den Aktualisierungsprozess jetzt durchführen oder ihn für ein späteres Datum planen können. Sie können auch Ihre Citrix ADC SDX-Instanz sichern, einen Ausführungsbericht per E-Mail erhalten oder ein zweistufiges Upgrade für Knoten in HA durchführen.

Das zweistufige Upgrade für Knoten in HA bietet Ihnen die Möglichkeit, das Upgrade sofort durchzuführen oder einen Zeitpunkt für die Aktualisierung der Knoten nacheinander zu planen. Synchronisation und Weitergabe der Knoten werden deaktiviert, bis beide Knoten erfolgreich aktualisiert wurden.

Erstellen von Konfigurationsaufträgen für Citrix SD-WAN WANOP-Instanzen

April 28, 2021

Ein Job ist eine Reihe von Konfigurationsbefehlen, die Sie für eine oder mehrere verwaltete Instanzen erstellen und planen können. Für Citrix SD-WAN WANOP-Instanzen können Sie die folgenden Optionen zum Erstellen von Aufträgen verwenden:

- **Konfigurationsvorlage**: Mit dem Konfigurationseditor können Sie CLI-Befehle eingeben, die Konfiguration als Vorlage speichern und Aufträge konfigurieren.
- **Inbuilt Template**: Sie können aus einer Liste von Konfigurationsvorlagen wählen. Diese Vorlagen stellen die Syntaxen der CLI-Befehle bereit und ermöglichen es Ihnen, Werte für die Variablen anzugeben. Die eingebauten Vorlagen werden mit ihren Beschreibungen in der folgenden Tabelle aufgeführt.
- **Datei**: Sie können eine Konfigurationsdatei von Ihrem lokalen Computer hochladen und Aufträge erstellen.

Sobald ein Job erstellt wurde, können Sie den Job sofort ausführen oder den Job so planen, dass er später ausgeführt wird. Sie können auch die Ausführungsfrequenz

Integrierte Vorlage	Beschreibung
EnableCloudBridgeWANOpt	Aktiviert den Datenverkehr über die Citrix SD-WAN WANOP-Appliance.
DisableCloudBridgeWANOpt	Deaktiviert den Datenverkehr über die Citrix SD-WAN WANOP Appliance.
RestartCloudBridgeWANOpt	Startet die Citrix SD-WAN WANOP Appliance neu.
RestoreConfig	Stellt die Konfiguration der Citrix SD-WAN WANOP Appliance wieder her.
AddLink	Durch das Erstellen oder Definieren von Verknüpfungen kann die SD-WAN WANOP-Appliance Überlastung und Verlust der Verbindungen verhindern und Traffic Shaping durchführen. Sie können die maximale Bandbreite definieren, die über den Link gesendet oder empfangen wird, und auch angeben, dass es sich um einen LAN-seitigen oder WAN-seitigen Datenverkehr handelt.
ConfigureBandwidth	Legt die Bandbreitengrenzen und andere Bandbreitenverwaltungseinstellungen fest.
AddUser	Fügt einen neuen Benutzer hinzu, dem Sie Berechtigungen zuweisen können.

Integrierte Vorlage	Beschreibung
AddUserAdvancedPlatform	Fügt einen neuen Benutzer hinzu, ermöglicht es Ihnen, Berechtigungen zuzuweisen, die in der AddUser-Vorlage nicht verfügbar sind.
AddService-class	Erstellt eine Serviceklasse für die SD-WAN WANOP-Appliance mit einem oder mehreren Serviceklassenfiltern und aktiviert diese.
SetApplication	Legt die Anwendungsklassifizierer-Definition fest.
AddorRemoveVideoCachingPorts	Fügt die Portnummer hinzu, an der die Videoquelle Daten senden oder empfangen kann. Der Standardport ist 80.
RemoveVideoCachingSource	Entfernt eine oder mehrere Video-Caching-Quellen. Geben Sie die IP-Adresse oder den Domänennamen der Videoquelle an.
RemoveAllVideoCaching	Entfernt alle verfügbaren Videozwischenspeicherquellen.
VideoCachingState	Aktiviert oder deaktiviert die Video-Caching-Funktion auf Citrix SD-WAN WANOP-Appliances.
ClearVideoCaching	Löscht entweder den Video-Cache oder die Video-Caching-Statistik.
SetVideoCaching	Legt die maximale Größe für zwischengespeicherte Objekte fest. Ein Objekt, das größer als dieser Grenzwert ist, wird nicht zwischengespeichert. Standardmäßig beträgt die maximale Größe des Caching-Objekts 100 MB.
AddVideoCachingSource	Fügt die IP-Adresse oder den Domänennamen der Videoquelle hinzu. Enthält Optionen zum Aktivieren oder Deaktivieren der Videozwischenspeicherung für diese Quelle.
ConfigureRemoteLicenseServer	Konfiguriert den zentralen Lizenzserver. Geben Sie das Lizenzservermodell, die IP-Adresse und die Portnummer an.

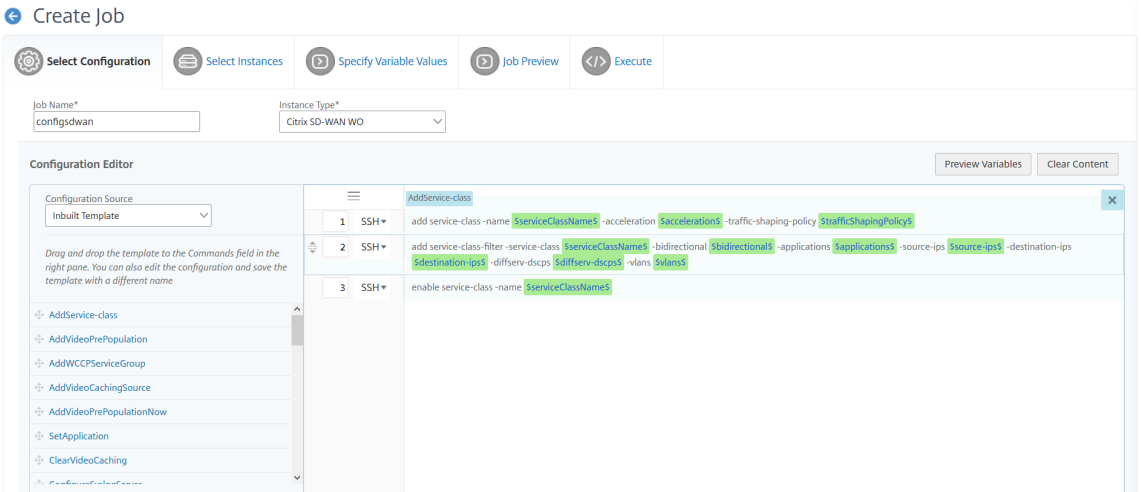
Integrierte Vorlage	Beschreibung
ConfigureLocalLicenseServer	Legt den Speicherort des Lizenzservers als lokal fest.
InstallCACert	Installiert CA-Zertifikate auf der Citrix SD-WAN WANOP Appliance. Geben Sie den Zertifikatsnamen, den Dateinamen und das Schlüsselspeicherkennwort an.
InstallCombinedCerKey	Installiert eine kombinierte SSL-Zertifikatschlüssel-Paardatei.
InstallSeperateCertKey	Installiert SSL-Zertifikat und Schlüssel als separate Dateien.
EnableWCCP	Aktiviert den WCCP-Bereitstellungsmodus.
AddWCCPServiceGroup	Fügt eine neue WCCP-Dienstgruppendefinition für die Citrix SD-WAN WANOP Appliance hinzu.
DisableWCCP	Deaktiviert den WCCP-Bereitstellungsmodus.
AddTrafficShapingPolicy	Erstellt eine Traffic Shaping-Richtlinie für die Citrix SD-WAN Appliance. Die Richtlinie steuert die Netzwerkbandbreite.
SetTrafficShapingPolicy	Ändert die Traffic-Shaping-Richtlinie für die Citrix SD-WAN WANOP Appliance. Die Richtlinie steuert die Netzwerkbandbreite.
AddVideoPrePopulation	Erstellt einen Videoeintrag zur Vorbevölkerung, mit dem Sie ein Video im Voraus herunterladen und zwischenspeichern können. Sie können auch angeben, wann ein Video zwischengespeichert werden soll.
UpdateVideoPrePopulation	Ändert einen Videovorbevölkerungseintrag, der angibt, wann ein Video zwischengespeichert werden soll.
AddVideoPrePopulationNow	Konfiguriert die Videovorbestückung, sodass Sie ein Video sofort herunterladen und zwischenspeichern können. Sie können steuern, wie Sie Videos von einer oder mehreren URLs herunterladen und zwischenspeichern möchten.

Integrierte Vorlage	Beschreibung
VideoPrePopulationState	Ändert, startet, aktualisiert oder entfernt die Video-Vorbestückung.
ConfigureSyslogServer	Legt die IP-Adresse und die Portnummer des Syslog-Servers fest.
ConfigureAlert	Konfiguriert die Warnstufe.

So erstellen Sie einen Konfigurationsauftrag für Citrix SD-WAN WANOP-Instanzen:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge**, und klicken Sie dann auf **Job erstellen**.
2. Geben Sie auf der Seite **Auftrag erstellen** auf der Registerkarte **Konfiguration auswählen** den **Auftragsnamen** an.
3. Wählen Sie im Feld **Instanztyp** die Option **Citrix SD-WAN WO** aus.
4. Wählen Sie in der Dropdownliste **Konfigurationsquelle** eine Option zum Erstellen eines Auftrags aus.

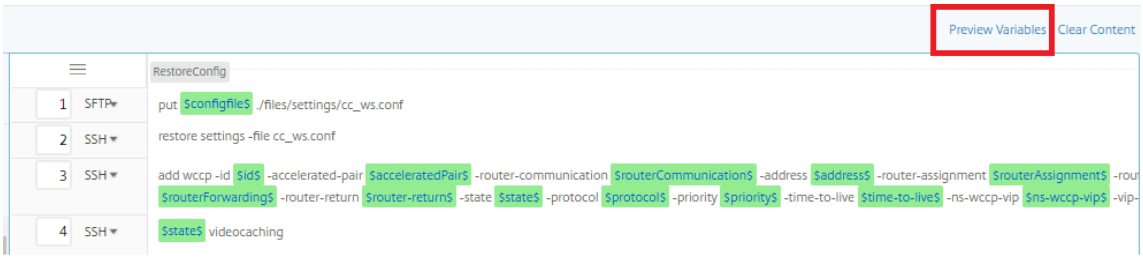
   > **Hinweis**
   >
   > Wählen Sie **Als Konfigurationsvorlage speichern** aus, und geben Sie einen Namen an, um die Konfiguration als Vorlage zu speichern und wiederzuverwenden.



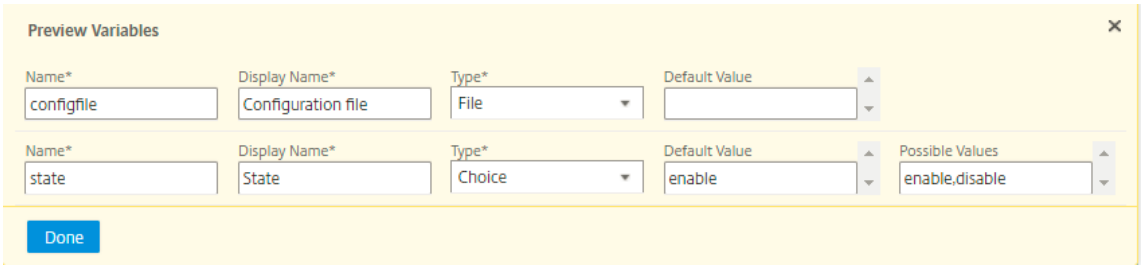
5. Sie können alle Variablen überprüfen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags in einer einzigen konsolidierten Ansicht definiert haben.
6. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:

- Navigieren Sie beim Erstellen eines Konfigurationsauftrags zu **Netzwerke** > **Konfigurationsaufträge**und wählen Sie **Job erstellen**aus. Auf der Seite **Job erstellen** können Sie alle Variablen überprüfen, die Sie beim Erstellen des Konfigurationsauftrags hinzugefügt haben.
- Navigieren Sie beim Bearbeiten eines Konfigurationsauftrags zu **Netzwerk** > **Konfigurationsaufträge**, wählen Sie den Auftragsnamen aus und klicken Sie auf **Bearbeiten**. Auf der Seite **Job konfigurieren** können Sie alle Variablen überprüfen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.

7. Sie können dann auf die Registerkarte **Vorschauvariablen** klicken, um eine Vorschau der Variablen in einer einzelnen konsolidierten Ansicht anzuzeigen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben.



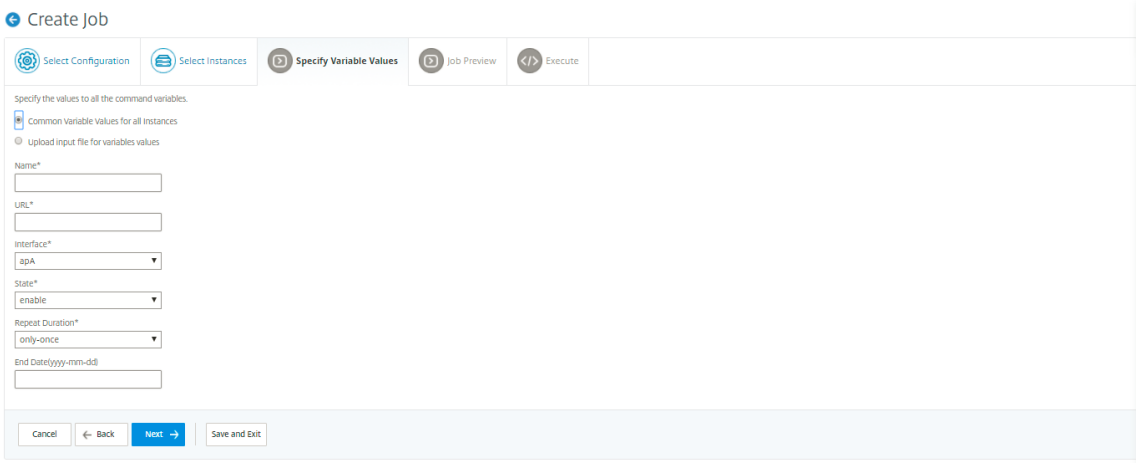
8. Ein neues Popup-Fenster wird angezeigt, in dem alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem tabellarischen Format angezeigt werden. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Fertig**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.



9. Klicken Sie auf **Weiter**, und klicken Sie dann auf der Registerkarte **Instanzen auswählen** auf **Instanzen hinzufügen**. Wählen Sie die Instanzen aus, für die Sie den Auftrag ausführen möchten, und klicken Sie dann auf **OK**.
10. Klicken Sie auf **Weiter**, und wählen Sie dann auf der Registerkarte **Variablenwerte angeben**eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:

    - **Eingabedatei für Variablenwerte hochladen:** Klicken Sie auf **Input Key** File herunterladen, um eine Eingabedatei herunterzuladen. Geben Sie in der Eingabedatei Werte für die Variablen ein, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den Citrix ADM -Server hoch.

- **Allgemeine Variablenwerte für alle Instanzen**: Geben Sie Werte für die Variablen ein. Die Variablen variieren je nach ausgewählter Vorlage.



Die Eingabedateien, die die Variablenwerte enthalten, werden in den Konfigurationsaufträgen beibehalten (mit demselben Dateinamen). Sie können diese Eingabedateien anzeigen und bearbeiten, die Sie früher beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben.

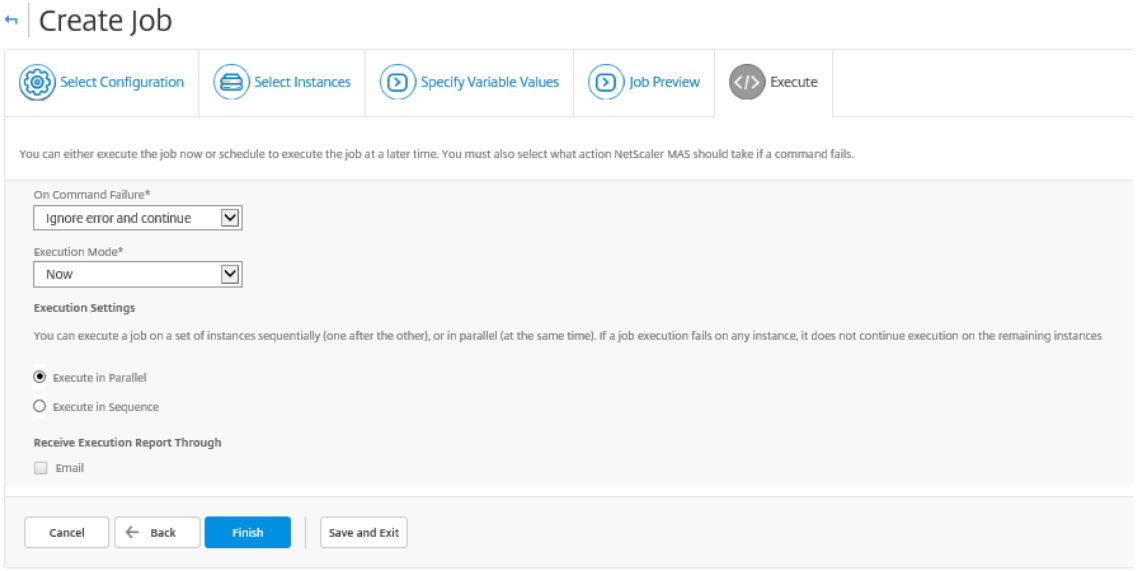
Um die Run Configuration Jobs beim Erstellen eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk** > **Konfigurationsjobs**und klicken Sie auf **Job erstellen**. Auf der Seite **Job erstellen**. Wählen Sie auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

Um die bereits ausgeführten Konfigurationsaufträge anzuzeigen, während Sie einen Konfigurationsauftrag bearbeiten, navigieren Sie zu **Netzwerk** > **Konfigurationsjobs**, wählen Sie den Job-Namen aus und klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite **Job konfigurieren** auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

11. Klicken Sie auf **Weiter**, auf der Registerkarte **Job-Vorschau** können Sie die als Job auszuführenden Befehle bewerten und überprüfen.
12. Klicken Sie auf **Weiter**, legen Sie auf der Registerkarte **Ausführen**die folgenden Bedingungen fest:

    - **Bei Befehlsfehler**: Was ist zu tun, wenn ein Befehl fehlschlägt: Ignorieren Sie die Fehler und setzen Sie den Job fort, oder beenden Sie die weitere Ausführung des Auftrags. Wählen Sie eine Aktion aus der Dropdownliste aus.

- **Ausführungsmodus**: Führen Sie den Auftrag sofort aus oder planen Sie die Ausführung für einen späteren Zeitpunkt ein. Wenn Sie die Ausführung für einen späteren Zeitpunkt planen, müssen Sie die Einstellungen für die Ausführungsfrequenz für den Job angeben. Wählen Sie in der Dropdownliste **Ausführungsfrequenz** den Zeitplan aus, dem der Auftrag folgen soll.



13. Wählen Sie unter **Ausführungseinstellungen**aus, um den Job sequenziell (nacheinander) oder parallel (gleichzeitig) auszuführen.
14. Damit ein Bericht zur Auftragsausführung an eine Liste von Empfängern per E-Mail gesendet wird, aktivieren Sie das Kontrollkästchen **E-Mail** im Abschnitt **Ausführungsbericht erhalten durch**. Wählen Sie in der angezeigten Dropdownliste eine E-Mail-Verteilerliste aus. Um eine E-Mail-Verteilerliste zu erstellen, klicken Sie auf das Symbol **+** und geben Sie die E-Mail-Adressen der Empfänger sowie Details zum E-Mail-Server ein.
15. Klicken Sie auf **Fertig stellen**.

Verwenden der Masterkonfigurationsvorlage

April 28, 2021

Die Verwendung einer Masterkonfigurationsvorlage ist eine flexible Option zum Erstellen und Bereitstellen einer Masterkonfiguration auf mehreren Citrix ADC-Instanzen.

Als Administrator können Sie Konfigurationsänderungen vornehmen und Lizenzen, Zertifikate und andere Dateien auf einer Citrix ADC-Instanz speichern. Sie können die neue Konfiguration als Masterkonfigurationsvorlage (.conf-Datei) speichern.

Um die Masterkonfigurationsvorlage aus einer Citrix ADC-Instanz zu speichern, können Sie einen der folgenden Schritte ausführen:

- Geben Sie an der Eingabeaufforderung **save ns config**ein. Die Konfiguration wird im FLASH-Speicher der Instanz in der Datei /nsconfig/ns.conf gespeichert.
- Navigieren Sie auf der Benutzeroberfläche der Citrix ADC-Instanz zu **Diagnose** > **Konfiguration anzeigen**. Wählen Sie die Art der Konfiguration aus, die Sie speichern möchten. Wenn Sie beispielsweise die gespeicherte Konfiguration Ihrer Citrix ADC-Instanz speichern möchten, wählen Sie **Gespeicherte Konfiguration**aus. Klicken Sie auf den Link **Text in einer Datei** speichern, um die Datei 'ns.conf' auf Ihrem lokalen Computer zu speichern.

Wenn Sie die Master-Konfigurationsvorlage bereitstellen, indem Sie beim Erstellen eines Auftrags die Konfigurationsvorlage "DeployMasterConfiguration" verwenden, können Sie sie für jede bestimmte Citrix ADC-Instanz weiter anpassen, indem Sie weitere Befehle hinzufügen, vorhandene Befehle ändern und unterschiedliche Variablenwerte in der Eingabedatei angeben .

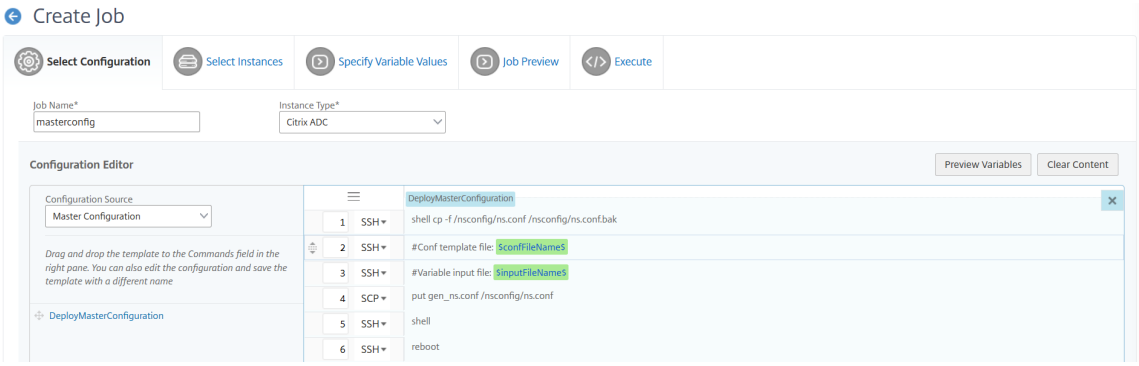
Als Administrator können Sie beispielsweise Zertifikatschlüssel in Ihre Citrix ADC-Instanzen zusätzlich ns.conf-Datei hochladen und die Master-Konfiguration auch auf ihnen bereitstellen.

> **Wichtig**
>
> Sie können einen Konfigurationsauftrag nicht mit der DeployMasterConfiguration-Vorlage auf Citrix ADC CPX-Instanzen, in einem Cluster konfigurierten Citrix ADC-Instanzen oder auf partitionierten Citrix ADC-Instanzen ausführen.

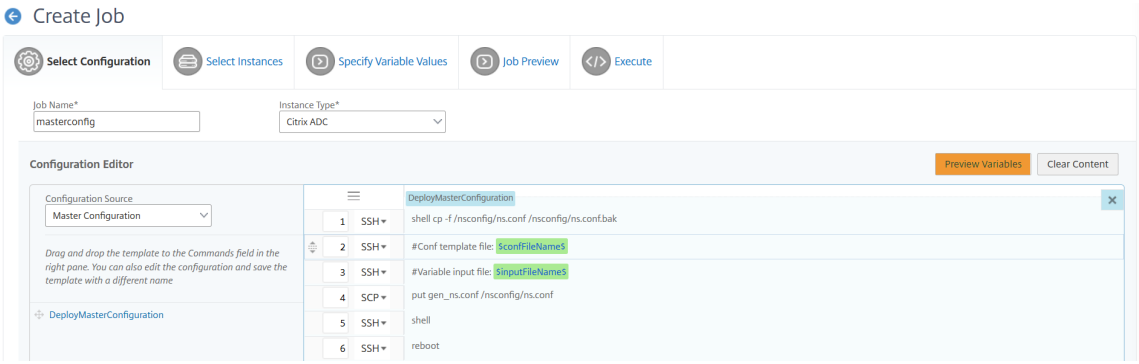
So erstellen Sie einen Konfigurationsauftrag mit der Konfigurationsvorlage Master Config unter Citrix ADM:

1. Navigieren Sie in Citrix Application Delivery Management (ADM) zu **Netzwerke** > **Konfigurationsaufträge**, und klicken Sie dann auf **Job erstellen**.
2. Geben Sie auf der Seite **Job erstellen** auf der Registerkarte **Konfiguration auswählen** den **Auftragsnamen** an, und wählen Sie in der Dropdownliste den **Instanztyp** aus.
3. Wählen Sie in der Dropdownliste **Konfigurationsquelle** die Option **Hauptkonfiguration** aus. Ziehen Sie die Befehle der Vorlage DeployMasterConfiguration in den rechten Bereich. Sie können Befehle auch im rechten Fensterbereich hinzufügen, ändern oder löschen. Klicken Sie auf **Weiter**.

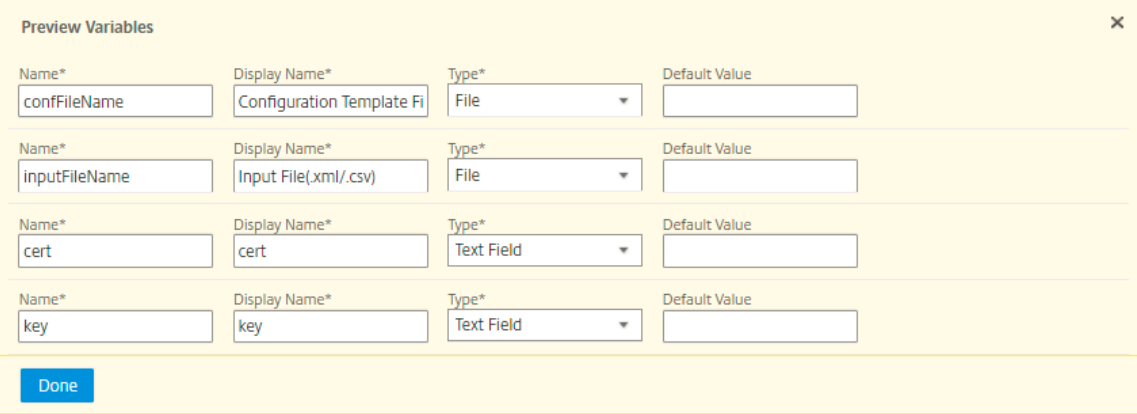
   > **Hinweis**
   >
   > Sie können **Put-Befehle** hinzufügen, um Ihrer Vorlage Eingabedateien hinzuzufügen. In unserem Beispiel müssen wir neben der Konfigurationsvorlagendatei und den variablen Eingabedateien auch Zertifikat- und Schlüsseldateien hochladen.



4. Sie können alle Variablen überprüfen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags in einer einzigen konsolidierten Ansicht definiert haben.
5. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:
    - Navigieren Sie beim Erstellen eines Konfigurationsauftrags zu **Netzwerke > Konfigurationsaufträge** und wählen Sie **Auftrag erstellen**. Auf der Seite **Job erstellen** können Sie alle Variablen überprüfen, die Sie beim Erstellen des Konfigurationsauftrags hinzugefügt haben.
    - Während Sie einen Konfigurationsauftrag bearbeiten, navigieren Sie zu **Netzwerk > Konfigurationsjobs**, wählen Sie den Job-Namen aus und klicken Sie auf **Bearbeiten**. Auf der Seite **Job konfigurieren** können Sie alle Variablen überprüfen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.
6. Sie können dann auf die Registerkarte **Vorschauvariablen** klicken, um eine Vorschau der Variablen in einer einzelnen konsolidierten Ansicht anzuzeigen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben.



7. Ein neues Popup-Fenster wird angezeigt, in dem alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem tabellarischen Format angezeigt werden. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Fertig**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.



8. Wählen Sie die Instanzen aus, auf denen Sie den Konfigurationsauftrag ausführen möchten, und klicken Sie dann auf **Weiter**.
9. Laden Sie auf der Registerkarte **Variablenwerte angeben** Folgendes hoch:
   - **Konfigurationsvorlagendatei (.conf)** - Laden Sie die CONF-Datei hoch, die Sie aus einer Citrix ADC-Instanz extrahiert haben.
   - **Laden Sie die Eingabedatei hoch (.xml/csv)** - Laden Sie die Eingabedatei mit Werten für die Variablen hoch, die Sie in Ihren Befehlen definiert haben.

   Eine XML-Beispieldatei wird hier für Ihre Verwendung bereitgestellt. Stellen Sie sicher, dass die XML-Dateien die Details enthalten, die den verwendeten ADC-Instanzen entsprechen.

```
<?xml version="1.0" encoding="UTF-8" ?>

<properties>

<!--

Provide inputs for all the parameters defined in the master config
    file.

-  global. This tag contains all the common parameters and value.

-  devicegroup. This tag contains all the instance group specific
   parameters and values.

If the same parameters are defined in global and instance tags,
   the instance specific parameters value will take precedence
   over the instance group. The instance group specific parameters
    value will take precedence over global parameters in the
   execution.

```



```
-  name. This attribute represents the name of the instance group.

-  device. This tag contains all the instance specific parameters
   and value.

If the same parameters are defined in global and instance tags,
   the instance specific parameters value will take precedence in
   the execution.

-  name. This attribute represents the IP Address of the instance.
    Host name is not supported for the attibute.

HA pair should be represented as <primaryip>-<secondaryip>.
   Example 10.102.2.1-10.102.2.2

In the template file, the parameter name must be specified within
   the dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters
   names are case sensitive.
-->

<global>

</global>
<devicegroup name="BLR_DEVS">
</devicegroup>
<device name="10.106.101.209">
<param name="IP" value="10.106.101.209"/>
</device>

<!-- HA PAIR-->
<!--<device name="10.102.43.154-10.102.43.155">
<param name="NSIP" value="10.102.43.154"/>
<param name="HostName" value="NS43HA"/>
<param name="LBSERVER" value="haserver43http"/>
<param name="SNMPTrapDest" value="10.102.43.130"/>
</device>-->
</properties>

<!--NeedCopy-->
```

Eine CSV-Datei ist hier für Ihre Verwendung zur Verfügung gestellt.

```
#job-s_variable_input_key_file ,,,,
```

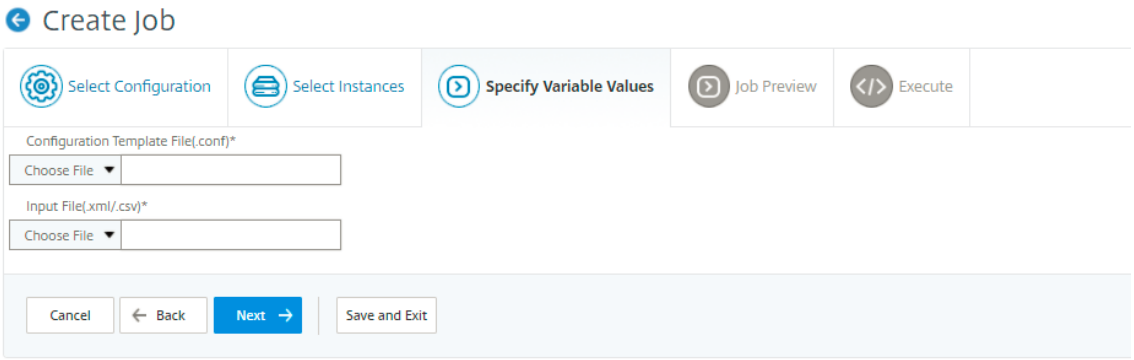


```
,,,,
#Global,NSIP,HostName,LBSERVER,SNMPTrapDest
Global Values,,,,
#InstanceGroup,NSIP,HostName,LBSERVER,SNMPTrapDest
example_doc,,,,
#Instance(s),NSIP,HostName,LBSERVER,SNMPTrapDest
10.xx.xx.xx,,,,
<!--NeedCopy-->
```

Die gleiche Datei wird in Microsoft Excel angezeigt:

#job-s_variable_input_key_file				
#Global	NSIP	HostName	*LBSERVER*	SNMPTrapDest
Global Values				
#InstanceGroup	NSIP	HostName	LBSERVER	SNMPTrapDest
example_doc				
#Instance(s)	NSIP	HostName	LBSERVER	SNMPTrapDest

10. Klicken Sie auf **Weiter**.

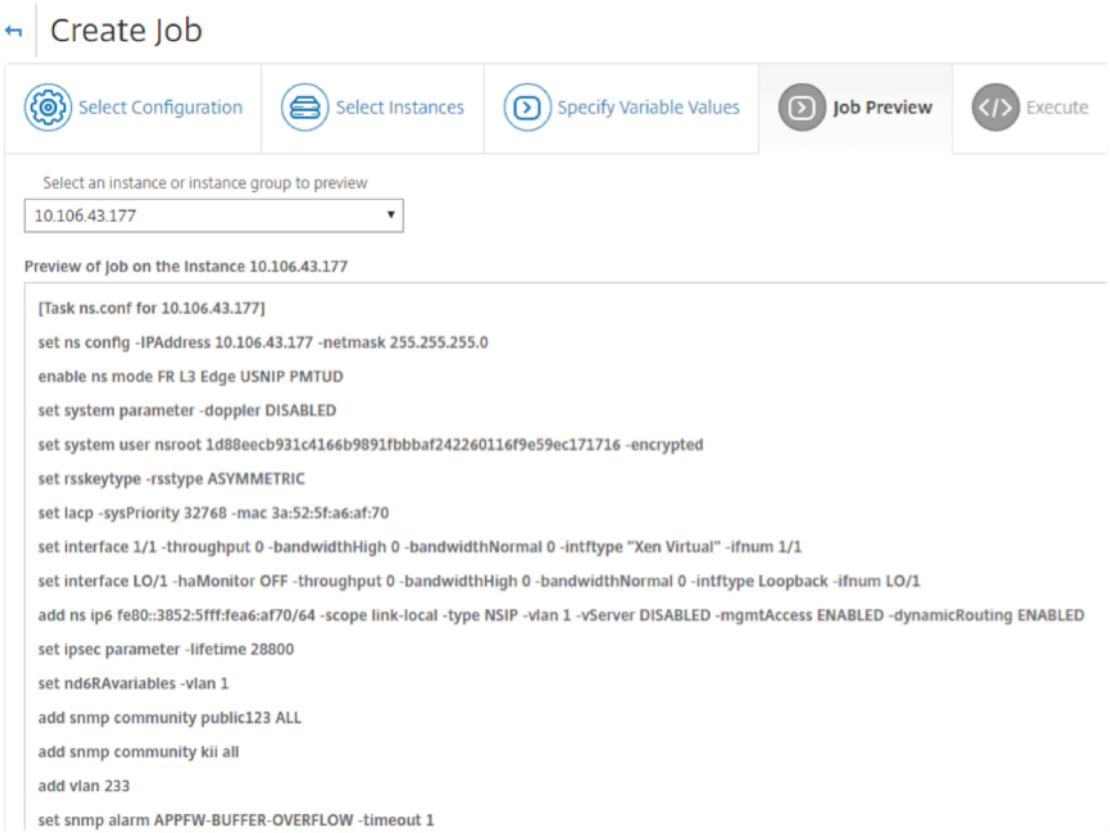


Die Eingabedateien, die die Variablenwerte enthalten, werden in den Konfigurationsaufträgen beibehalten (mit demselben Dateinamen). Sie können diese Eingabedateien anzeigen und bearbeiten, die Sie früher beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben.

Um die Run Configuration Jobs beim Erstellen eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk** > **Konfigurationsjobs**und klicken Sie auf **Job erstellen**. Auf der Seite **Job erstellen**. Wählen Sie auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

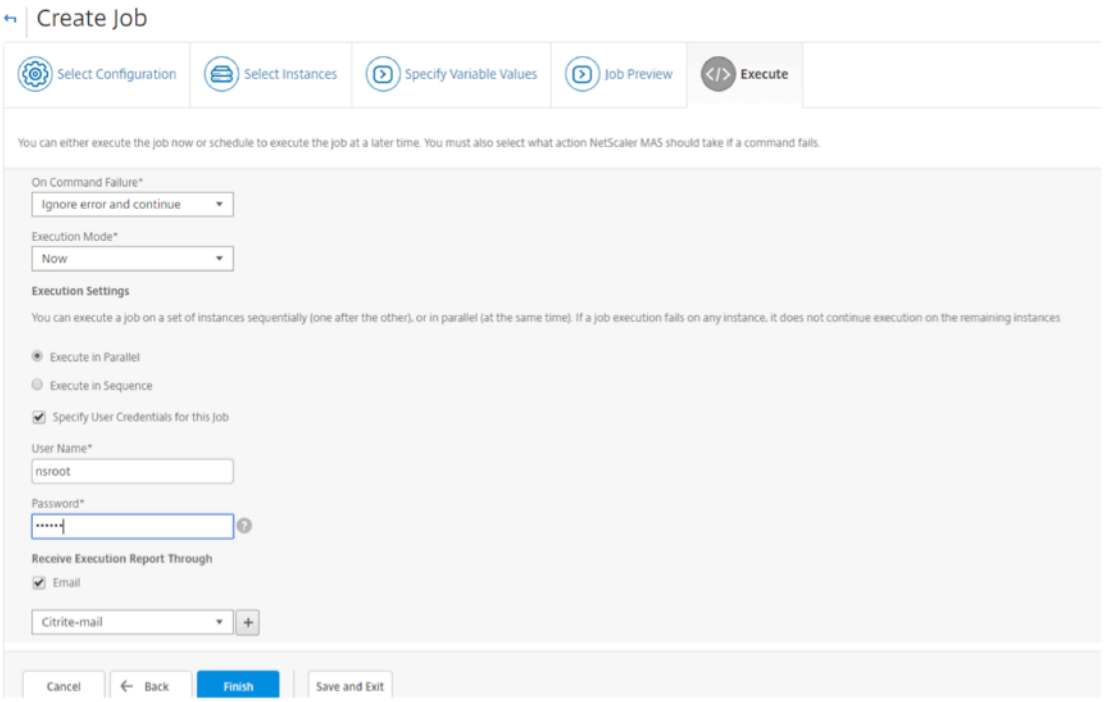
Um die bereits ausgeführten Konfigurationsaufträge anzuzeigen, während Sie einen Konfigurationsauftrag bearbeiten, navigieren Sie zu **Netzwerk** > **Konfigurationsjobs**, wählen Sie den Job-Namen aus und klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite **Job konfigurieren** auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

11. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen, und klicken Sie dann auf **Weiter**.

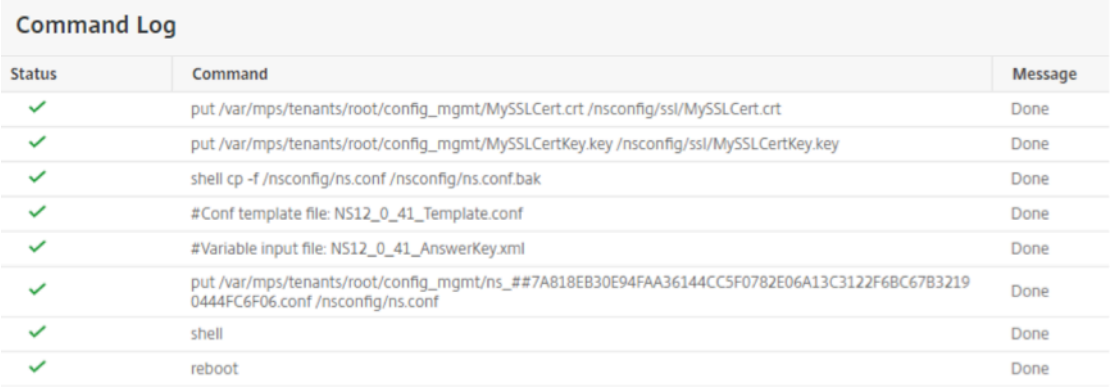


12. Auf der Registerkarte**Ausführen**können Sie wählen, ob Sie Ihren Job jetzt ausführen oder planen, dass er später ausgeführt wird. Sie können auch auswählen, welche Aktion Citrix ADM ausführen muss, wenn der Befehl fehlschlägt.

    Sie können auch autorisierten Benutzern erlauben, Aufträge auf Ihren verwalteten Instanzen auszuführen, und Sie können wählen, ob Sie eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Auftrags zusammen mit anderen Details senden möchten.



Nachdem Sie Ihren Job ausgeführt haben, können Sie die Jobdetails anzeigen, indem Sie zu **Netzwerke** > **Konfigurationsjobs** navigieren und den gerade konfigurierten Job auswählen. Klicken Sie auf **Details** und dann auf **Ausführungszusammenfassung**, um die Details Ihres Jobs anzuzeigen. Klicken Sie auf die Instanz, um die **Befehlsprotokolle** anzuzeigen, damit die Befehle für den Auftrag ausgeführt werden.



Command Log

Status	Command	Message
✓	put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt	Done
✓	put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key	Done
✓	shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak	Done
✓	#Conf template file: NS12_0_41_Template.conf	Done
✓	#Variable input file: NS12_0_41_AnswerKey.xml	Done
✓	put /var/mps/tenants/root/config_mgmt/ns_##7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B32190444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

Verwenden von Aufträgen zum Aktualisieren von Citrix ADC-Instanzen

April 28, 2021

In Citrix Application Delivery Management (ADM) können Sie eine oder mehrere Citrix ADC-Instanzen aktualisieren. Sie müssen das Lizenzierungsframework und die Lizenztypen kennen, bevor Sie eine Instanz aktualisieren.

Voraussetzungen

Bevor Sie eine ADC-Instanz aktualisieren, führen Sie die Vorvalidierungsprüfung für die Instanz durch, die Sie aktualisieren möchten.

1. Auf**Anpassungen prüfen** - Sichern Sie Ihre Anpassungen, und löschen Sie sie aus den Instanzen. Sie können die gesicherten Anpassungen nach dem Instanz-Upgrade erneut anwenden.
2. **Überprüfen Sie auf Datenträger-Hardwareprobleme** - Beheben Sie ggf. die Hardwareprobleme.

ADC-Hochverfügbarkeitspaar

Wenn Sie ein ADC-Hochverfügbarkeitspaar aktualisieren, beachten Sie Folgendes:

- Der sekundäre Knoten wird zuerst aktualisiert.
- Synchronisation und Weitergabe der Knoten werden deaktiviert, bis beide Knoten erfolgreich aktualisiert wurden.
- Nach dem erfolgreichen Hochverfügbarkeitspaar-Upgrade wird eine Fehlermeldung in der Ausführungshistorie angezeigt. Diese Meldung wird angezeigt, wenn sich Ihre Knoten im Hochverfügbarkeitspaar auf verschiedenen Builds oder Versionen befinden. Diese Meldung zeigt an, dass die Synchronisierung zwischen primären und sekundären Knoten deaktiviert ist.

Sie können ein ADC-Hochverfügbarkeitspaar in zwei Phasen aufrüsten:

1. Erstellen Sie einen Upgrade-Auftrag und führen Sie sofort auf einem der Knoten aus oder planen Sie später ein.
2. Planen Sie den Upgrade-Auftrag später auf dem verbleibenden Knoten. Stellen Sie sicher, dass Sie diesen Auftrag nach dem ersten Upgrade des Knotens planen.

ADC-Cluster

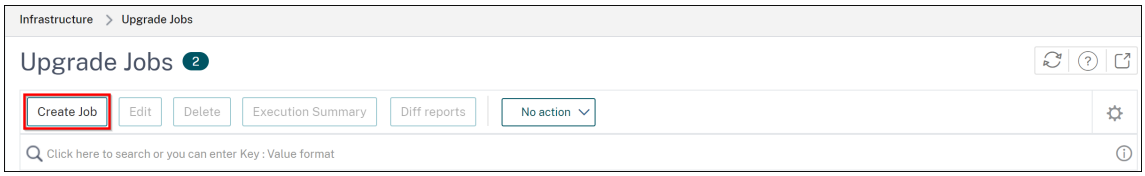
Wenn Sie einen ADC-Cluster aktualisieren, validiert der ADM in der Validierungsphase vor dem Upgrade nur die angegebene Instanz. Überprüfen und beheben Sie daher die folgenden Probleme auf den Clusterknoten:

- Anpassung
- Datenträgernutzung
- Hardware-Probleme

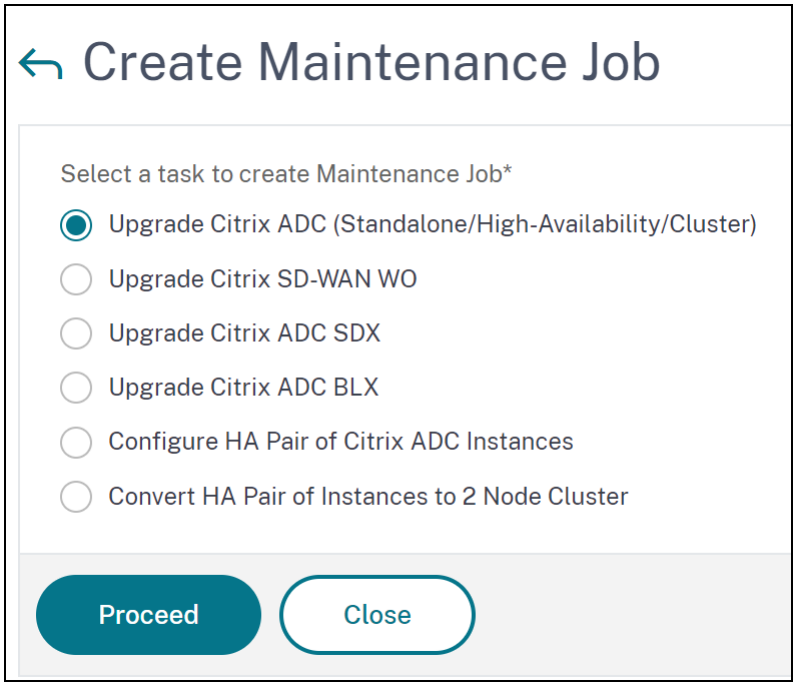
Erstellen eines ADC-Upgrade-Auftrags

Um einen ADC-Upgrade-Job zu erstellen, gehen Sie folgendermaßen vor:

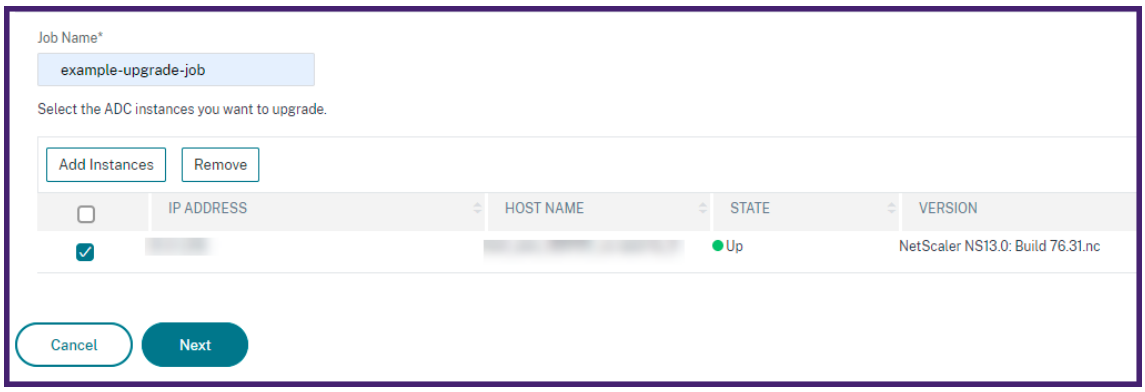
1. Navigieren Sie zu **Netzwerke > Konfigurationsauftrag > Wartungsaufträge**.



2. Wählen Sie unter **Wartungsaufträge erstellen** die Option **Upgrade Citrix ADC (Standalone/High Availability/Cluster)** aus, und klicken Sie auf **Weiter**.



3. Geben Sie unter **Instanz auswählen** einen Namen Ihrer Wahl für **Auftragsname** ein.
4. Klicken Sie auf **Instanzen hinzufügen**, um ADC-Instanzen hinzuzufügen, die Sie aktualisieren möchten.
    - Um ein ADC-Hochverfügbarkeitspaar zu aktualisieren, geben Sie die IP-Adresse des primären oder sekundären Knotens an.
    - Um einen Cluster zu aktualisieren, geben Sie die Cluster-IP-Adresse an.



5. Klicken Sie auf **Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten.

   Auf der Registerkarte **Validierung vor dem Upgrade** werden die fehlgeschlagenen Instanzen angezeigt. Sie können die fehlgeschlagenen Instanzen entfernen und auf **Weiter**klicken.

   > **Wichtig**
   >
   > Wenn Sie die Cluster-IP-Adresse angeben, führt ADM die Validierung vor dem Upgrade nur für die angegebene Instanz und nicht auf den anderen Clusterknoten durch.

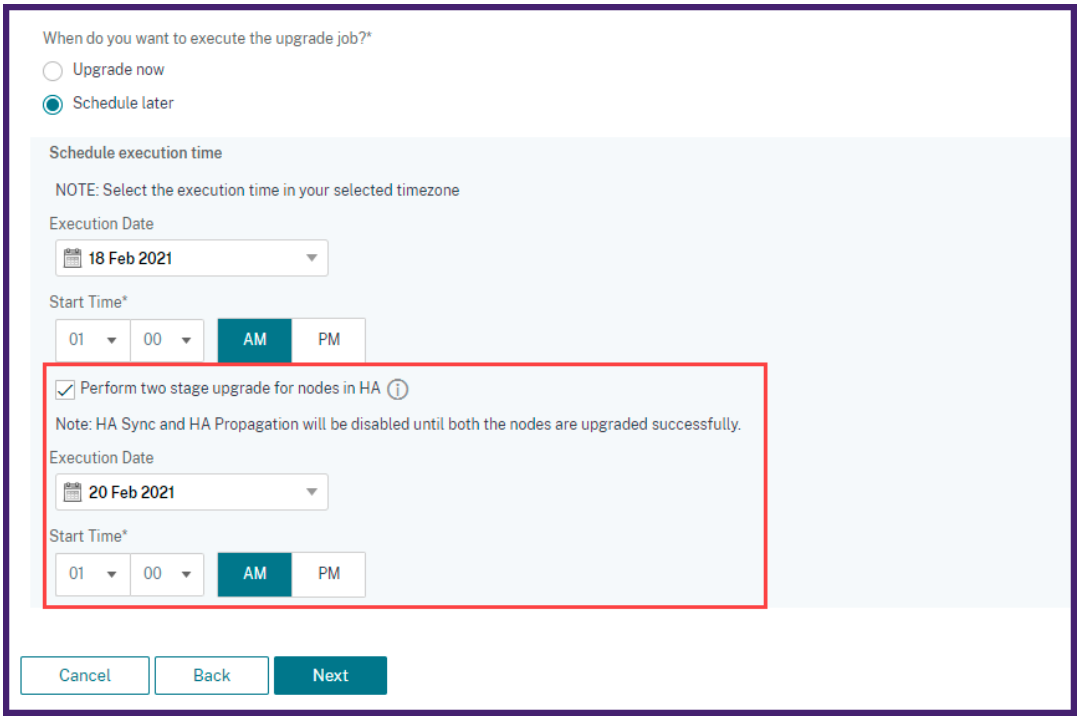
6. Optional geben Sie in **Custom scripts**die Scripts an, die vor und nach einem Instanzupgrade ausgeführt werden sollen. Weitere Informationen finden Sie unter Verwenden von benutzerdefinierten Skripts.

7. Wählen Sie unter **Task planen** eine der folgenden Optionen aus:

   - **Jetzt upgraden**: Der Upgrade-Job wird sofort ausgeführt.
   - **Später planen**: Wählen Sie diese Option, um diesen Upgrade-Auftrag später auszuführen. Geben Sie das **Ausführungsdatum** und die **Startzeit** an, wenn Sie die Instanzen aktualisieren möchten.

     Wenn Sie ein ADC-Hochverfügbarkeitspaar in zwei Stufen aufrüsten möchten, wählen Sie **Zweistufiges Upgrade für Knoten mit hoher Verfügbarkeit durchführen**aus.

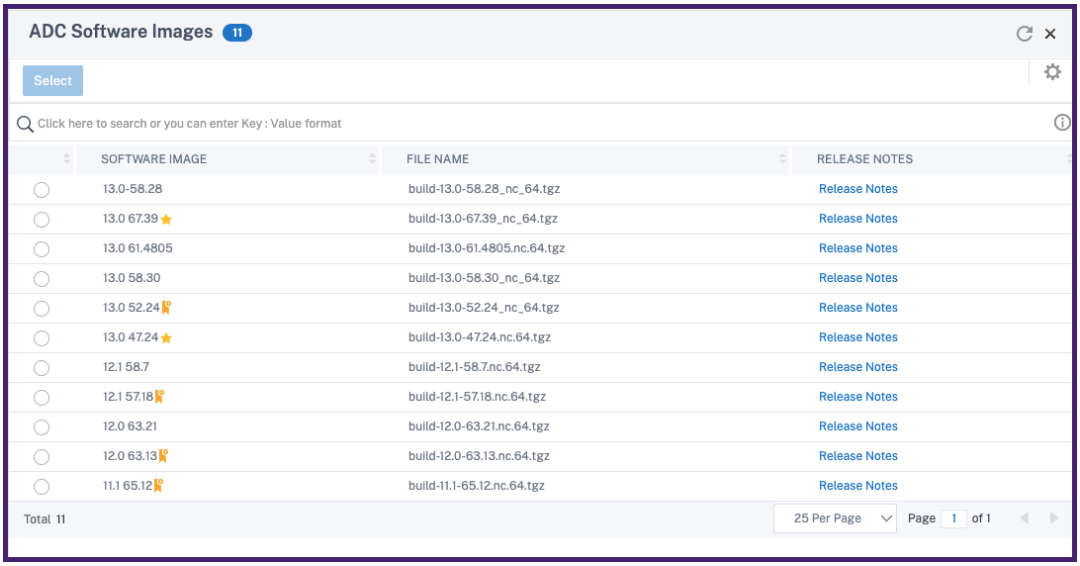
     Geben Sie das **Ausführungsdatum** und die **Startzeit an**, wenn Sie eine andere Instanz im Hochverfügbarkeitspaar upgraden möchten.



Weitere Informationen finden Sie unter ADC-Hochverfügbarkeitspaar.

8. Geben Sie unter **Job erstellen** die folgenden Details an:

   - **Wählen Sie das ADC-Software-Image**: Wählen Sie ein ADC-Bild aus der Liste aus. Diese Option listet alle ADC-Images auf, die auf der Citrix Downloads-Website verfügbar sind.



Die ADC-Software-Images zeigen die bevorzugten Builds mit dem Sternsymbol an. Und die meisten heruntergeladenen Builds mit dem Lesezeichen-Symbol.

   - **ADC-Software-Image**hochladen: Sie können das Bild von Ihrem lokalen Computer oder der ADC-Appliance hochladen. Wenn Sie ADC-Appliance auswählen, zeigt die ADM-GUI die

Instanzdateien an, die in vorhanden sind `/var/mps/mps_images`. Wählen Sie das Image in der ADM-GUI aus.

Wenn Sie den Upgrade-Auftrag planen, können Sie angeben, wann Sie das Image in eine Instanz hochladen möchten:

- **Jetzt hochladen**: Wählen Sie diese Option, um das Image sofort hochzuladen. Der Upgrade-Auftrag wird jedoch zum geplanten Zeitpunkt ausgeführt.
- **Zum Zeitpunkt der Ausführung hochladen**: Wählen Sie diese Option, um das Image hochzuladen, wenn der Upgradejob ausgeführt wird.

Weitere Informationen zu anderen Upgrade-Optionen finden Sie unter ADC-Upgrade-Optionen.

9. Klicken Sie auf **Job erstellen**.

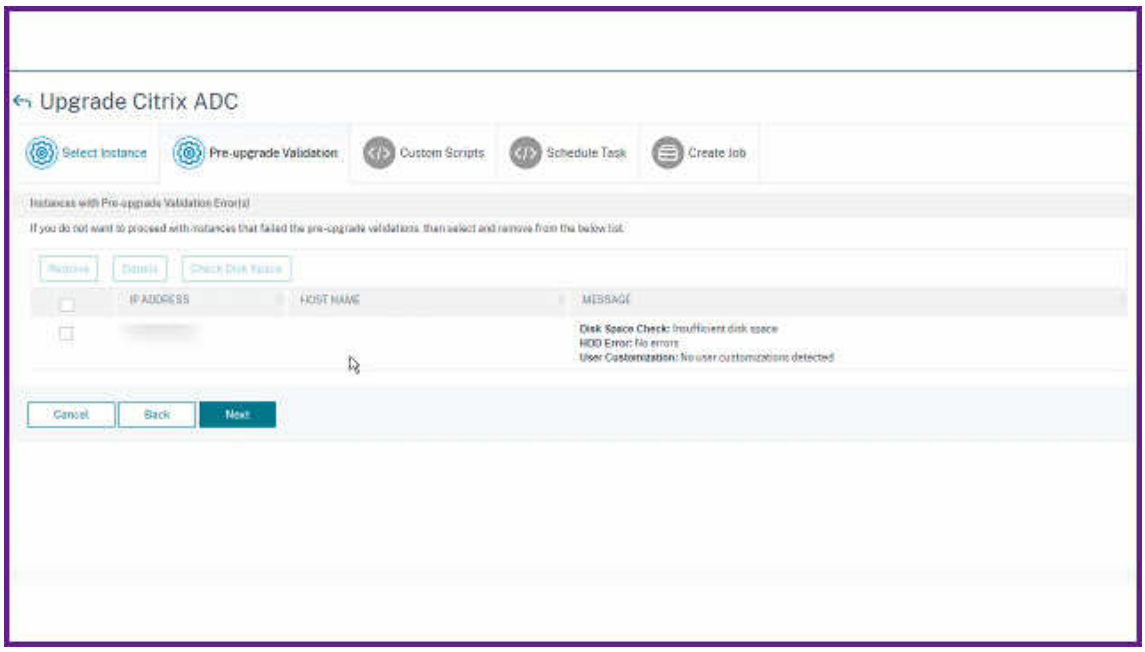
Der Upgrade-Auftrag wird unter **Netzwerke > Konfiguration > Wartungsaufträge** angezeigt. Wenn Sie einen vorhandenen Job bearbeiten, können Sie zu allen Registerkarten wechseln, wenn die erforderlichen Felder bereits ausgefüllt sind. Wenn Sie sich beispielsweise auf der Registerkarte **Konfiguration auswählen** befinden, können Sie auf die Registerkarte **Job-Vorschau** wechseln.

Bereinigen Sie den ADC-Speicherplatz

Wenn Sie beim Upgrade einer ADC-Instanz auf das Problem mit unzureichendem Speicherplatz stoßen, bereinigen Sie den Speicherplatz von der ADM-GUI selbst.

1. Wählen Sie auf der Registerkarte **Validierung vor dem Upgrade** die Instanz aus, die das Problem mit dem Speicherplatz hat.
2. Wählen Sie **Speicherplatz prüfen**aus.

   In diesem Bereich wird der Datenträger der Instanz mit geringem Speicherplatz angezeigt. Es zeigt auch an, wie viel Speicher auf dem Datenträger verwendet und verfügbar ist.
3. Wählen Sie im Bereich **Speicherplatz überprüfen** die Instanz aus, die eine Bereinigung erfordert.
4. Klicken Sie auf **Datenträgerbereinigung**.



5. Wählen Sie die Dateien aus, die Sie löschen möchten.
6. Klicken Sie auf **Löschen**

Verwenden von benutzerdefinierten Skripts

Sie können benutzerdefinierte Skripts angeben, während Sie einen ADC-Upgrade-Job erstellen. Die benutzerdefinierten Skripte werden verwendet, um die Änderungen vor und nach einem ADC-Instanz-Upgrade zu überprüfen. Beispiel:

- Die Instanzversion vor und nach dem Upgrade.
- Der Status von Schnittstellen, Hochverfügbarkeitsknoten, virtuellen Servern und Diensten vor und nach dem Upgrade.
- Die Statistiken der virtuellen Server und Dienste.
- Die dynamischen Routen.

Geben Sie die benutzerdefinierten Skripts an, die in den folgenden Phasen ausgeführt werden sollen:

- **Vor dem Upgrade**: Das angegebene Script wird vor dem Upgrade einer Instanz ausgeführt.
- **Vorab-Failover nach dem Upgrade (gilt für HA)**: Diese Phase gilt nur für die Bereitstellung mit hoher Verfügbarkeit. Das angegebene Skript wird nach dem Upgrade der Knoten, jedoch vor ihrem Failover ausgeführt.
- **Upgrade nach dem Upgrade (gilt für Standalone)/Nach dem Upgrade nach dem Failover (gilt für HA)**: Das angegebene Skript wird nach dem Upgrade einer Instanz in der eigenständigen

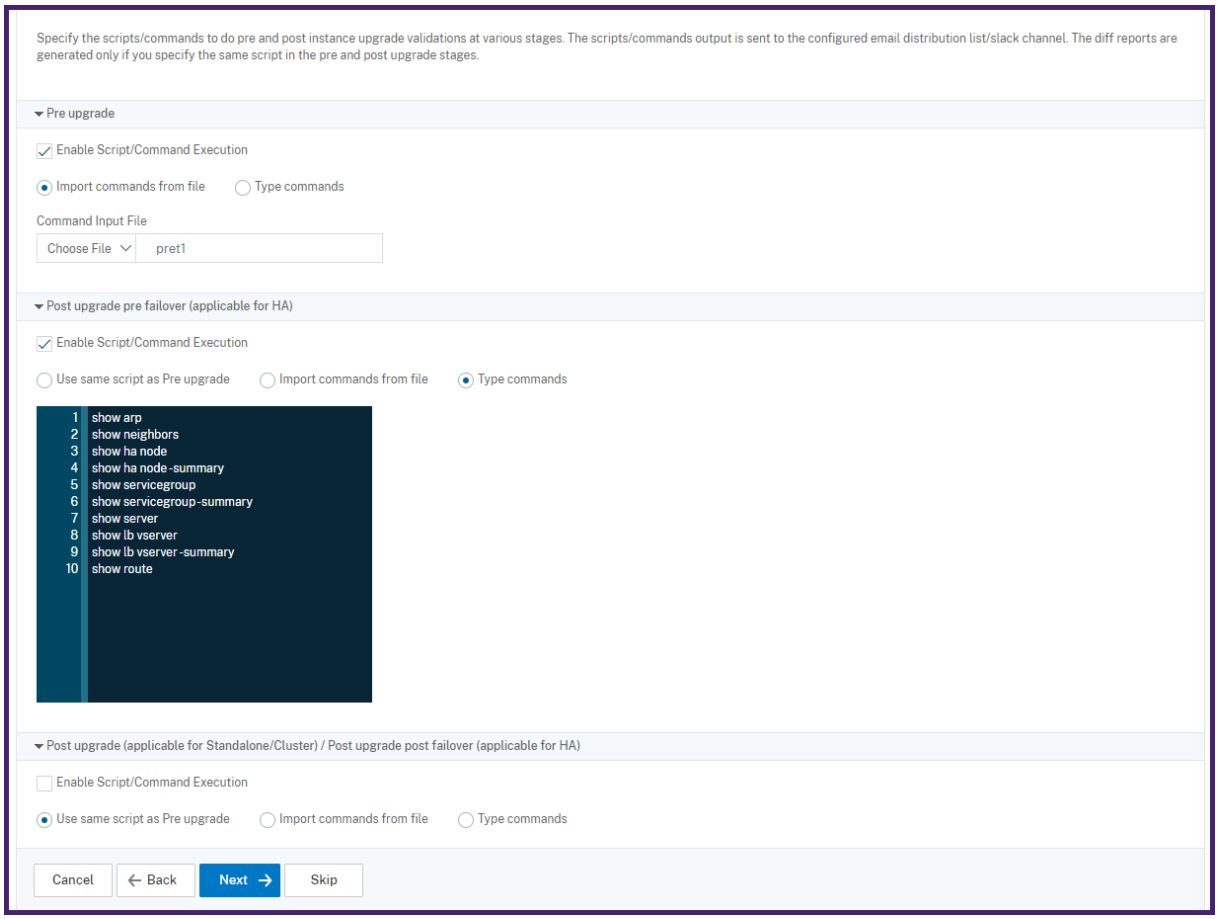
Bereitstellung ausgeführt. Bei der Bereitstellung mit hoher Verfügbarkeit wird das Skript nach dem Upgrade der Knoten und ihres Failovers ausgeführt.

> **Hinweis**
>
> - Stellen Sie sicher, dass Sie die Ausführung von Skripten oder Befehlen in den erforderlichen Phasen aktivieren Andernfalls werden die angegebenen Skripts nicht ausgeführt.
> - Der Diff-Bericht wird nur generiert, wenn Sie dasselbe Skript in den Phasen vor dem Upgrade und nach dem Upgrade angeben. Stellen Sie daher sicher, dass Sie in den Phasen nach dem **Upgrade dasselbe Skript wie Pre-Upgrade verwenden** auswählen. Siehe Laden Sie einen konsolidierten Diff-Bericht über einen ADC-Upgrade-Job.

Sie können eine Skriptdatei importieren oder Befehle direkt in die ADM-GUI eingeben.

- **Befehle aus Datei importieren**: Wählen Sie die Befehlseingabedatei von Ihrem lokalen Computer aus.
- **Type-Befehle**: Geben Sie Befehle direkt auf der GUI ein.

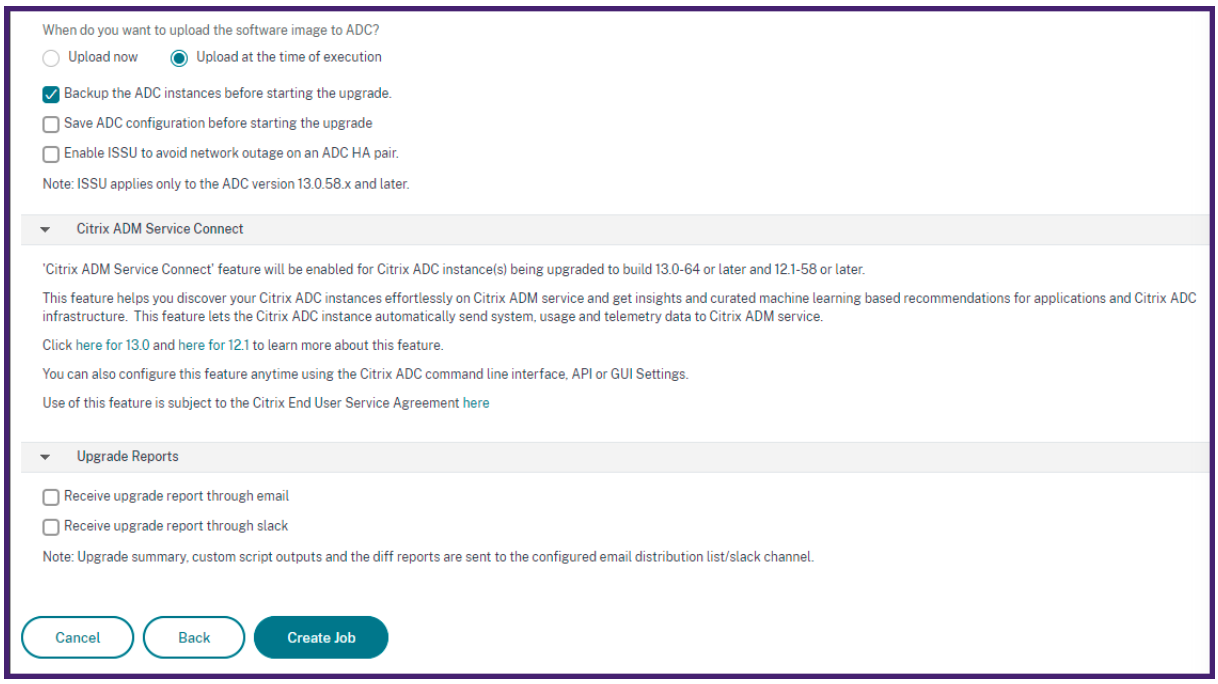
In den Phasen nach dem Upgrade können Sie das gleiche Skript verwenden, das in der Pre-Upgrade-Phase angegeben ist.



ADC-Upgrade-Optionen

Während Sie einen ADC-Upgrade-Job erstellenauf der Registerkarte “ **Job erstellen** “ die folgenden Optionen auswählen können:

- **Software-Image von Citrix ADC bei erfolgreichem Upgrade bereinigen**: Wählen Sie diese Option, um das hochgeladene Image in der ADC-Instanz nach dem Instanz-Upgrade zu löschen.
- **Sichern Sie die ADC-Instanzen, bevor Sie das Upgrade starten.**: Erstellt ein Backup der ausgewählten ADC-Instanzen.
- **Behalten Sie den primären und sekundären Status von hochverfügbaren Knoten nach dem Upgrade**bei: Wählen Sie diese Option, wenn der Upgrade-Auftrag nach dem Upgrade jedes Knotens ein Failover auslösen soll. Auf diese Weise behält der Upgrade-Job den primären und sekundären Status der Knoten bei.
- **Speichern Sie die ADC-Konfiguration vor dem Start des Upgrades** - Speichert die laufende ADC-Konfiguration vor dem Upgrade der ADC-Instanzen.
- **Aktivieren Sie ISSU, um Netzwerkausfälle beim ADC HA-Paar zu vermeiden** - ISSU stellt das Upgrade ohne Ausfallzeiten bei einem ADC-Hochverfügbarkeitspaar sicher. Diese Option bietet eine Migrationsfunktionalität, die die vorhandenen Verbindungen während des Upgrades berücksichtigt. Sie können also ein ADC-Hochverfügbarkeitspaar ohne Ausfallzeiten aktualisieren. Geben Sie das Timeout der ISSU Migration in Minuten an.
- **Ausführungsbericht per E-Mail empfangen** - Sendet den Ausführungsbericht per E-Mail. Informationen zum Hinzufügen einer E-Mail-Verteilerliste finden Sie unter Erstellen einer E-Mail-Verteilerliste.
- **Ausführungsbericht über Pufferzeit empfangen** - Sendet den Ausführungsbericht in Pufferzeit. Informationen zum Hinzufügen eines Slack Profils finden Sie unter Erstellen eines Slack Profils.



Laden Sie einen konsolidierten Diff-Bericht über einen ADC-Upgrade-Job

In Citrix ADM können Sie einen Diff-Bericht über einen ADC-Upgrade-Job herunterladen. Um dies zu tun, muss der Upgrade-Job haben benutzerdefinierte Skripte. Ein Diff-Bericht enthält die Unterschiede zwischen den Ausgaben des Pre-Upgrade- und Post-Upgrade-Skripts. Mit diesem Bericht können Sie bestimmen, welche Änderungen bei der ADC-Instanz nach dem Upgrade aufgetreten sind.

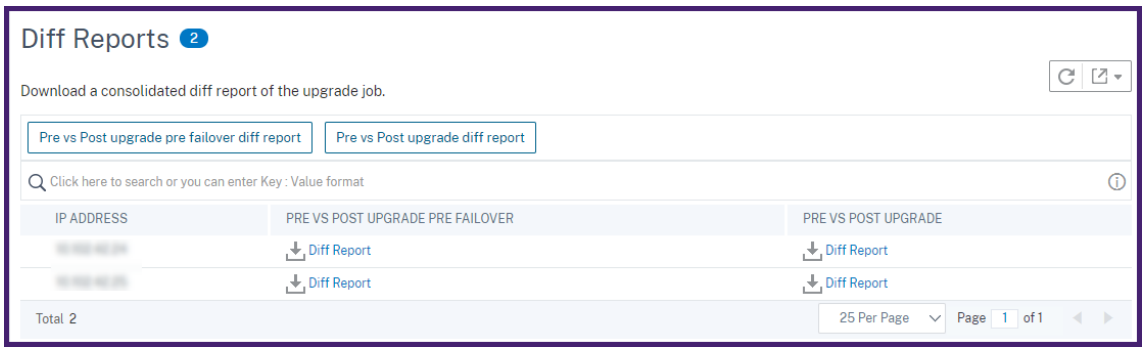
> **Hinweis**
>
> Der Diff-Bericht wird nur generiert, wenn Sie dasselbe Skript in den Phasen vor dem Upgrade und nach dem Upgrade angeben.

Um einen Diff-Bericht über einen Upgrade-Job herunterzuladen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Netzwerke > Konfigurationsjobs > Wartungsaufträge**.
2. Wählen Sie den Upgrade-Job aus, für den Sie einen Diff-Bericht herunterladen möchten.
3. Klicken Sie auf **Diff-Berichte**.
4. Laden Sie in **Diff Reports**einen konsolidierten Diff-Bericht des ausgewählten Upgrade-Jobs herunter.

   Auf dieser Seite können Sie einen der folgenden Arten von Diff-Berichten herunterladen:

   - **Vor und nach dem Upgrade vor dem Failover-Diff-Bericht**
   - **Diff-Bericht vor und nach dem Upgrade**



Verwenden von Konfigurationsvorlagen zum Erstellen von Überwachungsvorlagen

April 28, 2021

Sie können jetzt Konfigurationsbefehle verwenden, die zuvor als Konfigurationsvorlagen gespeichert wurden, um Überwachungsvorlagen zu erstellen, die auf bestimmte Citrix ADC-Instanzen angewendet werden können. Beim Erstellen einer Prüfungsvorlage können Sie zuvor gespeicherte Konfigurationsvorlagen in das Feld **Befehle** ziehen und die Vorlage entsprechend Ihren Anforderungen bearbeiten. Anschließend können Sie die Überwachungsvorlage auf bestimmte Citrix ADC-Instanzen anwenden. Citrix Application Delivery Management (ADM) vergleicht diese Instanzen mit der Überwachungsvorlage und meldet eventuelle Unstimmigkeit. Dieser Prozess hilft Ihnen, Fehler zu erkennen und rechtzeitig zu beheben.

Sie können Konfigurationsvorlagen erstellen, während Sie einen Auftrag erstellen und eine Reihe von Konfigurationsbefehlen als Vorlage speichern. Wenn Sie diese Vorlagen auf der Seite **Jobs erstellen** speichern, werden sie automatisch auf der Seite **Vorlage erstellen** angezeigt.

Betrachten Sie beispielsweise eine grundlegende Lastausgleichskonfiguration, für die Sie einen virtuellen Lastausgleichsserver hinzufügen, zwei Dienste hinzufügen und die Dienste an den virtuellen Server binden.

In diesem Beispiel werden die folgenden Befehle verwendet:

```
add lb vserver **servername** HTTP **ipaddress portnumber**

add service **servicename1 ipaddress1** HTTP 80

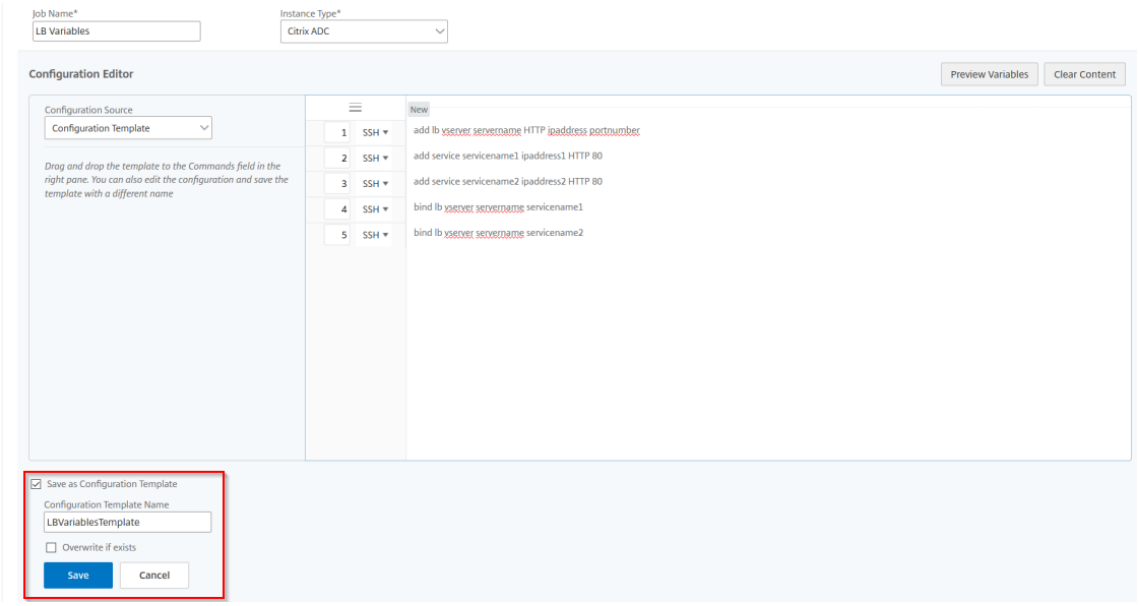
add service **servicename2 ipaddress2** HTTP 80

bind lb vserver **servername servicename1**

bind lb vserver **servername servicename2**
```

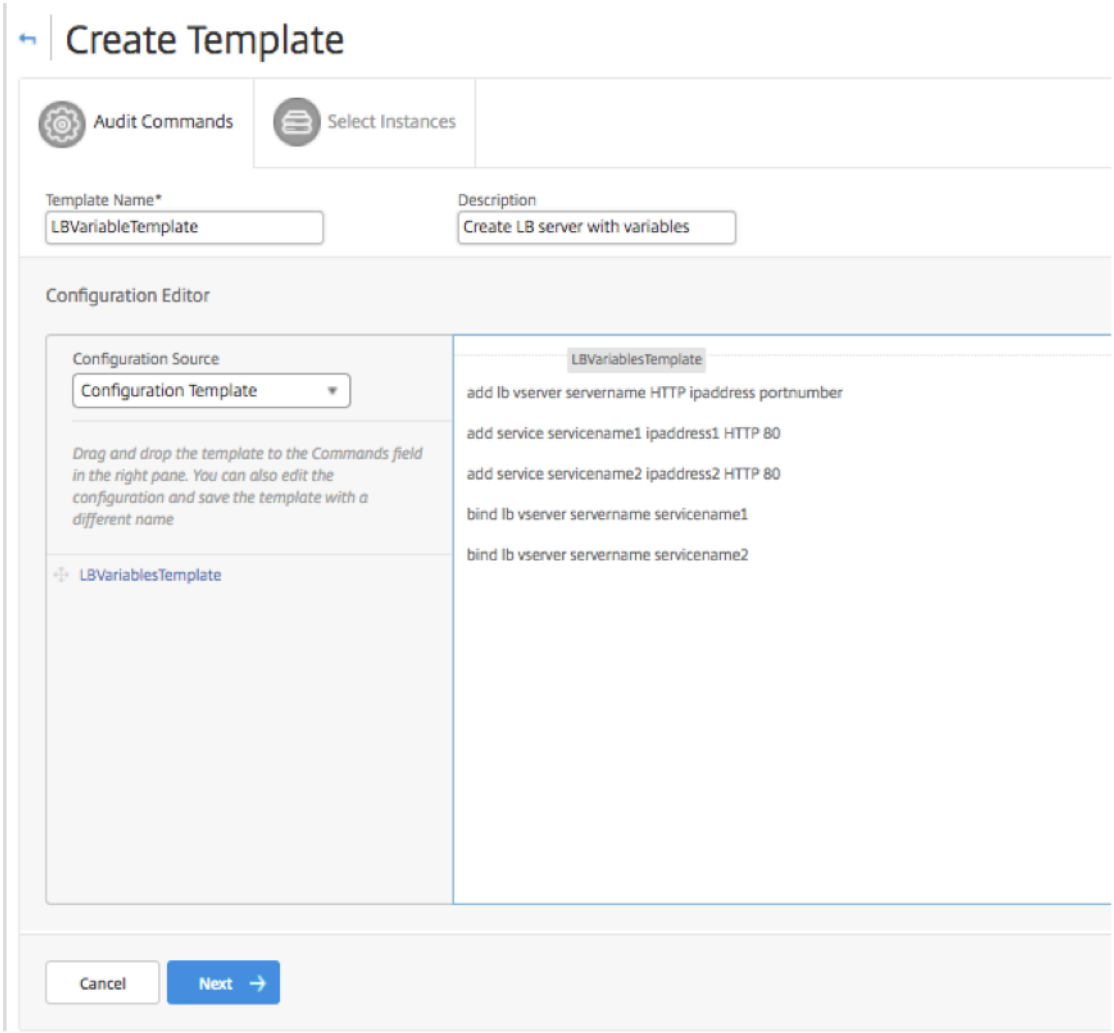
So speichern Sie eine Konfigurationsvorlage in Citrix ADM:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**, und klicken Sie auf **Job erstellen**.
2. Geben Sie auf der Seite **Job erstellen** den Jobnamen und den Instanztyp an.
3. Wählen Sie “ **Konfigurationsvorlage** “ als “Konfigurationsquelle” und geben Sie im Feld “ **Befehle** “ Befehle wie die im vorherigen Beispiel ein.
4. Aktivieren Sie das Kontrollkästchen **Als Konfigurationsvorlage speichern** und geben Sie einen Namen für Ihre Vorlage an. Sie können andere Vorlagen mit demselben Namen überschreiben.
5. Klicken Sie auf **Save**.



So erstellen Sie eine Überwachungsvorlage in Citrix ADM mithilfe einer Konfigurationsvorlage:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsüberwachung** > **Überwachungsvorlagen**, und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Vorlage erstellen** einen Namen für den Vorlagennamen an, und geben Sie eine Beschreibung ein.
3. Wählen Sie in der Liste **Konfigurationsquelle** die Option **Konfigurationsvorlage**aus, und ziehen Sie die Vorlage dann in das Feld Befehle im rechten Fensterbereich. Sie können die Konfiguration auch bearbeiten und die Vorlage unter einem anderen Namen speichern. Klicken Sie auf **Weiter**.
4. Klicken Sie auf der Registerkarte **Instanzen auswählen** auf **Instanzen hinzufügen**, und fügen Sie die Instanzen hinzu, auf denen Sie die Konfiguration ausführen möchten. Klicken Sie auf **OK**.
5. Klicken Sie auf **Fertig stellen**.



Die Überwachungsvorlage wird in der Liste Überwachungsvorlagen angezeigt und wird alle 12 Stunden für die Konfigurationen der angegebenen Instanzen ausgeführt.

Verwenden des SCP-Befehls (put) in Konfigurationsaufträgen

April 28, 2021

Sie können die Funktion " **Konfigurationsaufträge** " von Citrix Application Delivery Management (ADM) verwenden, um Konfigurationsjobs zu erstellen, E-Mail-Benachrichtigungen zu senden und Ausführungsprotokolle der erstellten Jobs zu überprüfen. Ein Auftrag ist eine Reihe von Konfigurationsbefehlen, die Sie auf einer einzelnen verwalteten Instanz oder auf mehreren verwalteten Instanzen erstellen und ausführen können. Beispielsweise können Sie Konfigurationsaufträge für Geräte-Upgrades verwenden.

Konfigurationsaufträge in Citrix ADM verwenden Secure Shell (SSH) -Befehle, um Instanzen zu konfig-

urieren, und Sie können einen Konfigurationsauftrag so konfigurieren, dass Secure Copy (SCP) verwendet wird, um Dateien sicher zu übertragen. SCP basiert auf dem SSH-Protokoll. Einer der SCP-Befehle, die Sie in einen Konfigurationsauftrag aufnehmen können, ist der Befehl put. Sie können den Befehl put in Konfigurationsaufträgen verwenden, um eine oder mehrere Dateien, die in einem lokalen Verzeichnis auf Ihrem System gespeichert sind, in Citrix ADM und dann in ein Verzeichnis auf der Citrix ADC-Instanz oder -Instanzen hochzuladen oder zu übertragen.

> **Hinweis**
>
> Die Datei wird in Citrix ADM hochgeladen und später in die ausgewählten Citrix ADC-Instanzen kopiert (abgelegt). Die hochgeladene Datei wird in Citrix ADM gespeichert und nur gelöscht, wenn der Auftrag gelöscht wird. Dies ist notwendig für Jobs, die später laufen sollen.

Der Befehl hat die folgende Syntax:

```
put <local_filename> <remote_path/remote_filename>
<!--NeedCopy-->
```

Hierbei gilt:

<local_filename> ist der Name der lokalen Datei, die hochgeladen werden soll.

<remote_path/ remote_filename> ist der Pfad zu einem entfernten Verzeichnis und der Name, der der Datei zugewiesen werden soll, wenn sie in dieses Verzeichnis kopiert wird.

Beim Erstellen des Konfigurationsauftrags können Sie die Parameter für lokale und remote Dateinamen in Variablen konvertieren. Auf diese Weise können Sie diesen Parametern bei jeder Ausführung des Auftrags verschiedene Dateien für denselben Satz von Citrix ADC-Instanzen zuweisen. Wenn Sie eine Datei an mehreren Stellen in einem Auftrag verwenden und die Datei umbenennen möchten, können Sie die Variable umdefinieren, anstatt den Dateinamen an allen Stellen zu ändern.

So verwenden Sie den Befehl put zum Hochladen von Dateien in einem Konfigurationsauftrag:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge**.
2. Klicken Sie auf der Seite **Jobs** auf **Job erstellen**.
3. Geben Sie auf der Seite **Job erstellen** den Namen des Jobs in das Feld Jobname ein, und geben Sie im **Konfigurationseditor** den Befehl put ein.

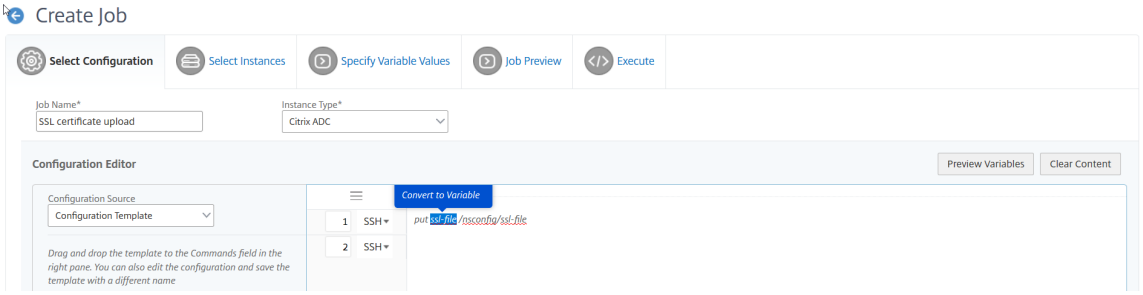
   Wenn Sie beispielsweise einen Konfigurationsauftrag erstellen möchten, der eine auf Ihrem lokalen System gespeicherte SSL-Zertifikatsdatei auf mehrere Citrix ADC-Instanzen kopiert, können Sie einen “put” -Befehl hinzufügen, der eine Variable anstelle des Namens einer bestimmten Datei verwendet, und den Variablentyp als “Datei” definieren.


```
put ssl-file /nsconfig/ssl-file
<!--NeedCopy-->
```

In diesem Beispiel wird

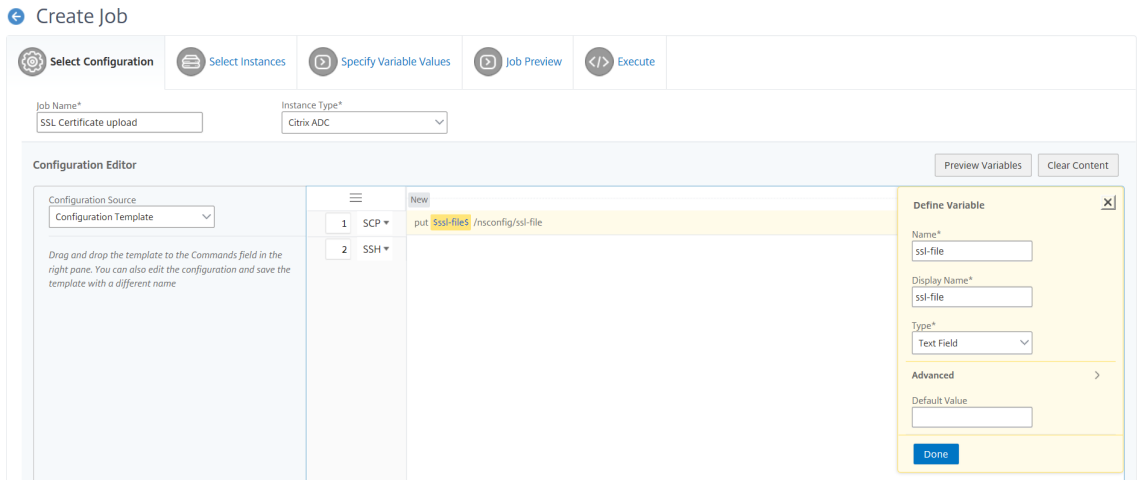
- `ssl-file` - Dies ist der Name der Datei, die in die Citrix ADC-Instanz hochgeladen werden muss.
- `/nsconfig/ssl-file` - es ist der Zielordner in der Instanz, in den der nach der Ausführung der Aufgabe abgelegt `ssl-file` wird.

4. Wählen Sie in dem eingegebenen Befehl den Dateinamen aus, den Sie in eine Variable konvertieren möchten, und klicken Sie dann auf In **Variable umwandeln**, wie in der folgenden Abbildung dargestellt.



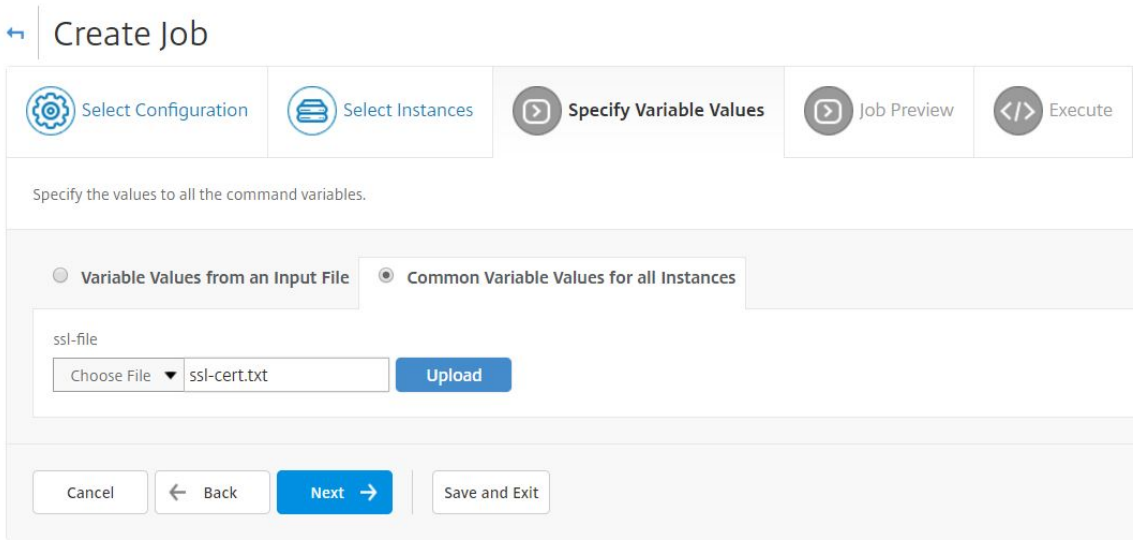
5. Stellen Sie sicher, dass der Dateiname von Dollarzeichen eingeschlossen wurde (was darauf hinweist, dass es sich jetzt um eine Variable handelt), und klicken Sie dann auf die Variable.
6. Geben Sie die Details der Variablen an, wie Name, Anzeigename und Typ.
7. Wählen **Sie in der Dropdownliste Typ** die Option **Datei** aus. Klicken Sie auf **Save**.

   Wenn Sie die Variable als Dateityp deklarieren, können Sie Dateien in Citrix ADM hochladen.



8. Klicken Sie auf **Weiter**, und wählen Sie die Citrix ADC-Instanzen aus, in die die Dateien kopiert werden sollen.

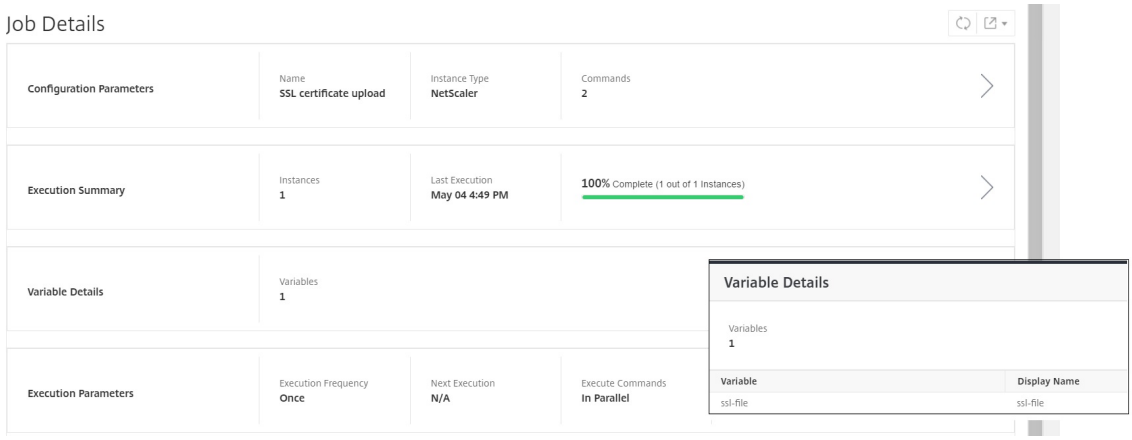
9. Wählen Sie auf der Registerkarte **Variablenwerte angeben** den Abschnitt **Allgemeine Variablenwerte für alle Instanzen** aus, wählen Sie die Datei aus dem lokalen Speicher auf Ihrem System aus, klicken Sie auf **Hochladen**, um die Datei in Citrix ADM hochzuladen, und klicken Sie auf **Weiter**.



10. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.

11. Auf der Registerkarte **Ausführen** können Sie den Job jetzt ausführen oder planen, dass er später ausgeführt wird. Sie können auch auswählen, welche Aktion Citrix ADM ausführen muss, wenn der Befehl fehlschlägt. Sie können auch eine E-Mail-Benachrichtigung erstellen, um Benachrichtigungen über den Erfolg oder Misserfolg des Auftrags und andere Details zu erhalten. Klicken Sie auf **Fertig stellen**.

12. Sie können die Auftragsdetails anzeigen, indem Sie zu **Netzwerke** > **Konfigurationsaufträge**navigieren und den von Ihnen konfigurierten Job auswählen. Klicken Sie auf **Details**, und klicken Sie dann auf **Variablendetails**, um die Variablen aufzulisten, die Ihrem Auftrag hinzugefügt wurden.



Neuplanen von Jobs, die mithilfe integrierter Vorlagen konfiguriert wurden

April 28, 2021

Sie können einen geplanten Auftrag mithilfe integrierter Vorlagen in Citrix Application Delivery Management (ADM) neu planen. Sie können beispielsweise die Aktion ändern, die Citrix ADM ausführen muss, wenn ein Befehl fehlschlägt. Wenn Sie sich zuvor dafür entschieden hatten, einen Fehler zu ignorieren und fortzufahren, können Sie ihn so ändern, dass alle erfolgreichen Befehle zurückgesetzt werden, wenn ein Befehl fehlschlägt.

So planen Sie einen Auftrag neu, der mithilfe integrierter Vorlagen in Citrix ADM konfiguriert wurde:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge**.
2. Wählen Sie den Job aus, den Sie bearbeiten, hinzufügen oder entfernen möchten, geben Sie Variablenwerte an und ändern Sie dann Ausführungsaktionen und -einstellungen.
3. Klicken Sie auf **Fertig stellen**, um den Auftrag neu zu planen.

> **Hinweis**
>
> Sie können den Job auch auswählen und erneut auf **Ausführen** klicken, um den Job auszuführen, ohne Quelle, Instanz und Befehle zu ändern. Dies ist nützlich, wenn Sie dieselben Befehle für dieselben Instanzen ausführen müssen. Manchmal tritt der Auftrag möglicherweise auf einen vorübergehenden Fehler von der Serverseite auf, und Sie müssen den Auftrag möglicherweise erneut ausführen.

Wiederverwenden von Konfigurationsüberwachungsvorlagen in Konfigurationsaufträgen

April 28, 2021

Als Administrator können Sie jetzt Konfigurationsbefehle als eine Reihe von wiederverwendbaren Konfigurationsvorlagen speichern, wenn Sie einen Auftrag erstellen und auch wenn Sie ein Konfigurations-Audit ausführen. Die im Modul Configuration **Jobs erstellte und gespeicherte Konfigurationsvorlage** ist in Configuration Audit verfügbar, um eine Überwachungsvorlage zu erstellen, die auf bestimmte Citrix ADC-Instanzen angewendet werden kann. In ähnlicher Weise ist die im Modul **Konfigurationsprüfung erstellte Audit-Vorlage** in Konfigurationsaufträgen verfügbar, sodass Sie die Vorlage als Konfigurationsauftrag ausführen können. Jede in der Vorlage vorgenommene Änderung ist jetzt sowohl in Konfigurations-Jobs als auch in **Konfigurations-Audi**t-Modulen sichtbar.

Früher mussten die Konfigurationsauftrags- und Konfigurationsüberwachungsvorlagen separat für dieselbe Konfiguration erstellt und als verschiedene Dateien gespeichert werden. Dies führte zu einer doppelten Anstrengung beim Erstellen und Verwalten der Vorlagen.

Mit Citrix Application Delivery Management (ADM) können Sie diese Vorlage im System speichern, sodass die Audit-Vorlage auch in **Konfigurationsjobs** verfügbar ist. Jetzt können die Überwachungsvorlagen zum Erstellen von Konfigurationsaufträgen verwendet werden. Auf diese Weise können die Vorlagen austauschbar zwischen den Konfigurationsjobs und Konfigurationsaudits verwendet werden.

Betrachten Sie beispielsweise eine grundlegende Lastausgleichskonfiguration, für die Sie einen virtuellen Lastausgleichsserver hinzufügen, zwei Dienste hinzufügen und die Dienste an den virtuellen Server binden.

In diesem Beispiel werden die folgenden Befehle verwendet:

```
1  add lb vserver servername HTTP ipaddress portnumber
2
3  add service servicename1 ipaddress1 HTTP 80
4
5  add service servicename2 ipaddress2 HTTP 80
6
7  bind lb vserver servername servicename1
8
9  bind lb vserver servername servicename2
10 <!--NeedCopy-->
```

Erstellen einer Vorlage in Konfigurationsprüfungen und Wiederverwenden in Konfigurationsaufträgen

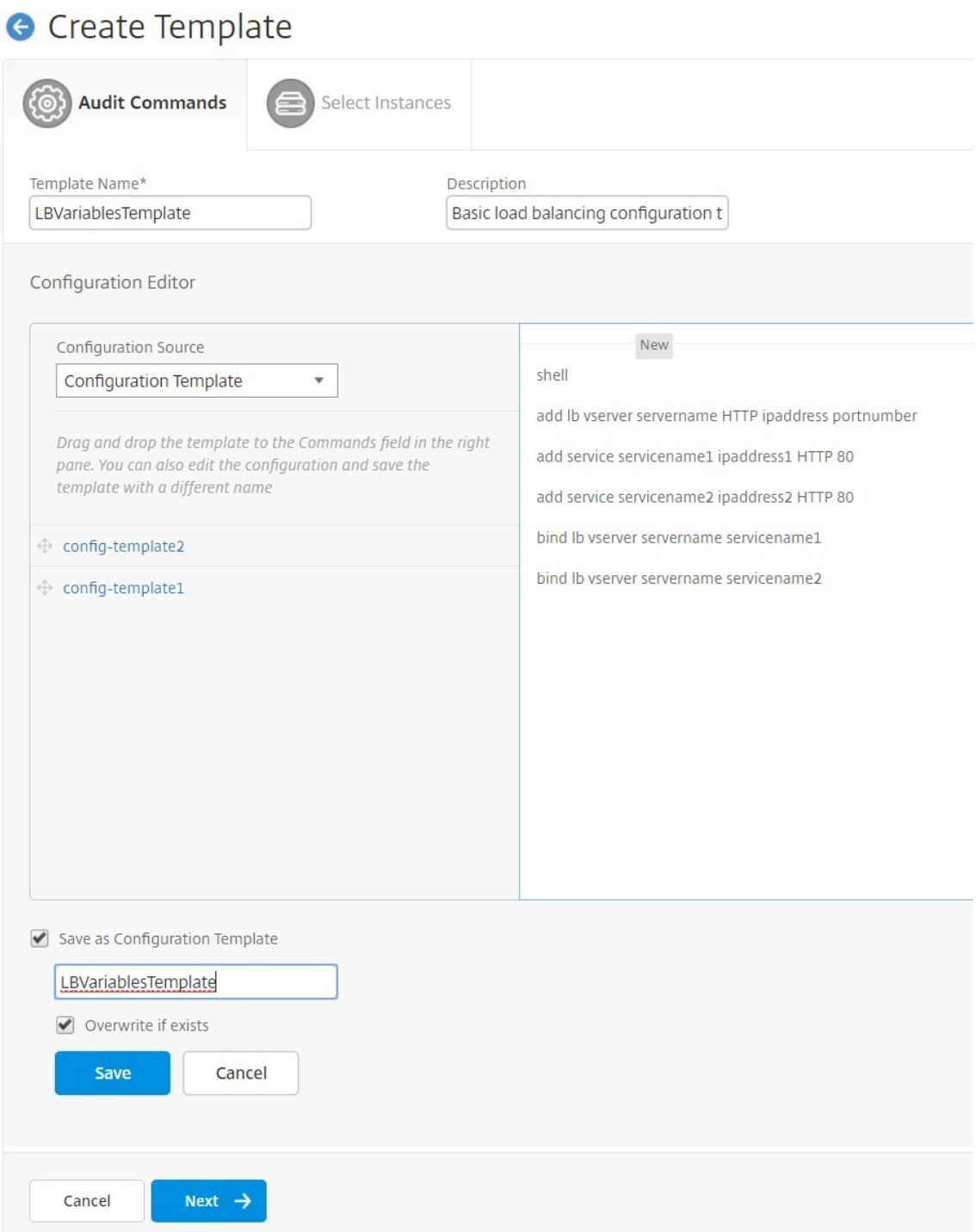
Führen Sie die folgende Aufgabe aus, um eine Vorlage im Konfigurations-Audit-Modul zu erstellen und diese im Modul Konfigurationsjobs wiederzuverwenden.

So erstellen Sie eine Überwachungsvorlage:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsüberwachung** > **Überwachungsvorlage**, und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Vorlage erstellen** den Namen der Vorlage an. Sie können auch weitere Informationen zur Vorlage im Feld **Beschreibung** hinzufügen.
3. Geben Sie im Bereich **Befehle** Befehle wie die im vorherigen Beispiel ein.
4. Aktivieren Sie das Kontrollkästchen **Als Konfigurationsvorlage speichern** und geben Sie einen Namen für Ihre Vorlage an, z. B. können Sie diese Vorlage “LBVariablesTemplate” nennen. Sie können andere Vorlagen mit demselben Namen überschreiben.

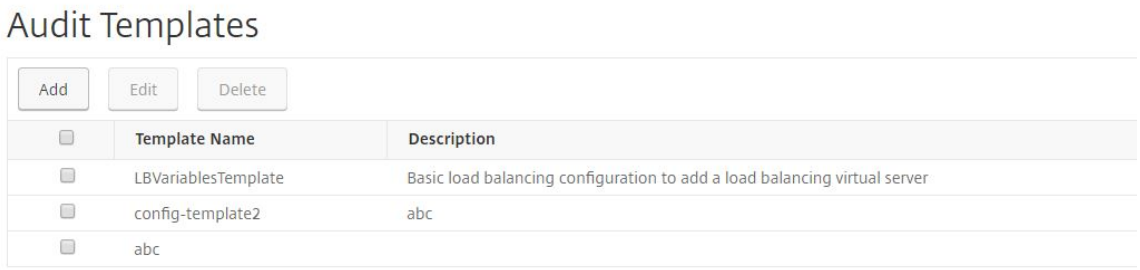
> **Hinweis**
>
> Der Name der Prüfungsvorlage kann mit dem Namen der Konfigurationsvorlage identisch sein.

5. Klicken Sie auf **Speichern** und dann auf **Weiter**.

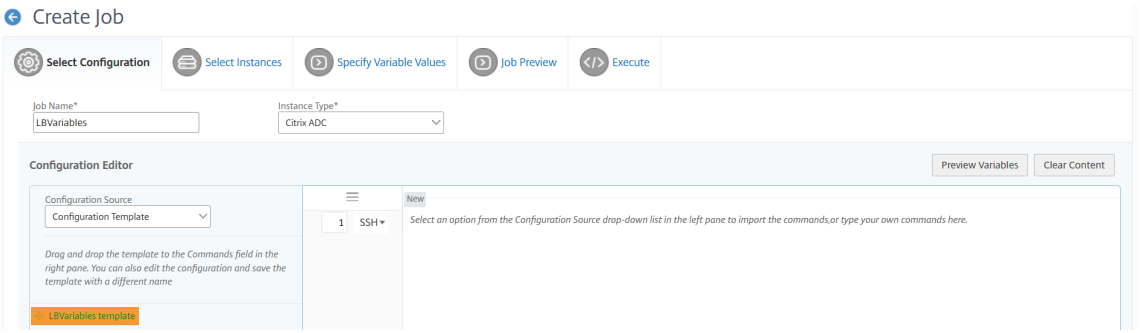


6. Klicken Sie auf **Weiter**.

7. **Wählen Sie auf der Registerkarte Instanzen** auswählen die Citrix ADC-Instanzen aus, auf denen Sie diese Konfigurationsbefehle ausführen möchten, und klicken Sie auf **Fertig stellen**. Die neue Vorlage ist nun in der Liste der Überwachungsvorlagen sichtbar.

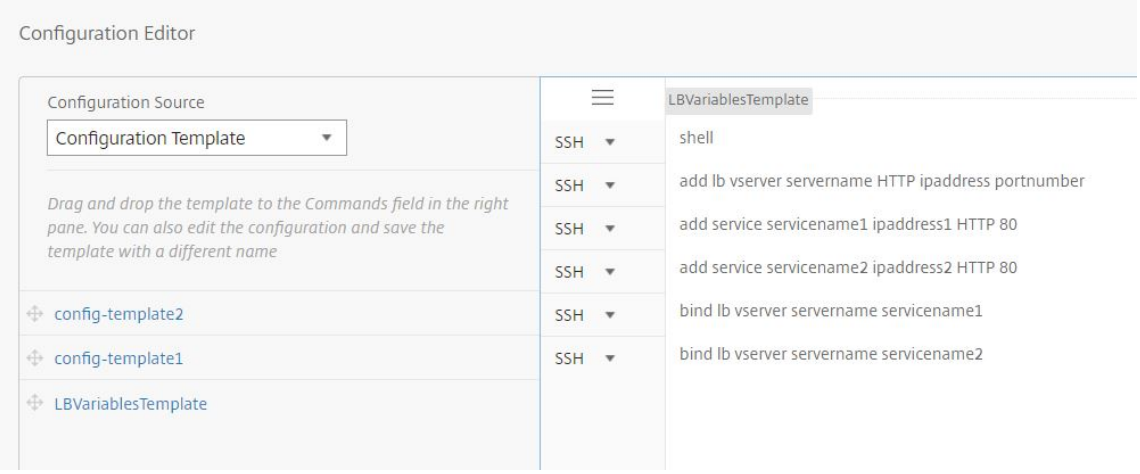


8. Wenn Sie diese Konfigurationsbefehle ausführen möchten, navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge,** und klicken Sie auf **Job erstellen**. Die zuvor erstellte Überwachungsvorlage wird als Konfigurationsvorlage aufgeführt.



So verwenden Sie die Überwachungsvorlage in Konfigurationsaufträgen erneut:

1. Geben Sie einen Namen für den Auftrag ein, wählen Sie den Instanztyp aus und ziehen Sie die Vorlage in den Bereich “Befehle”.

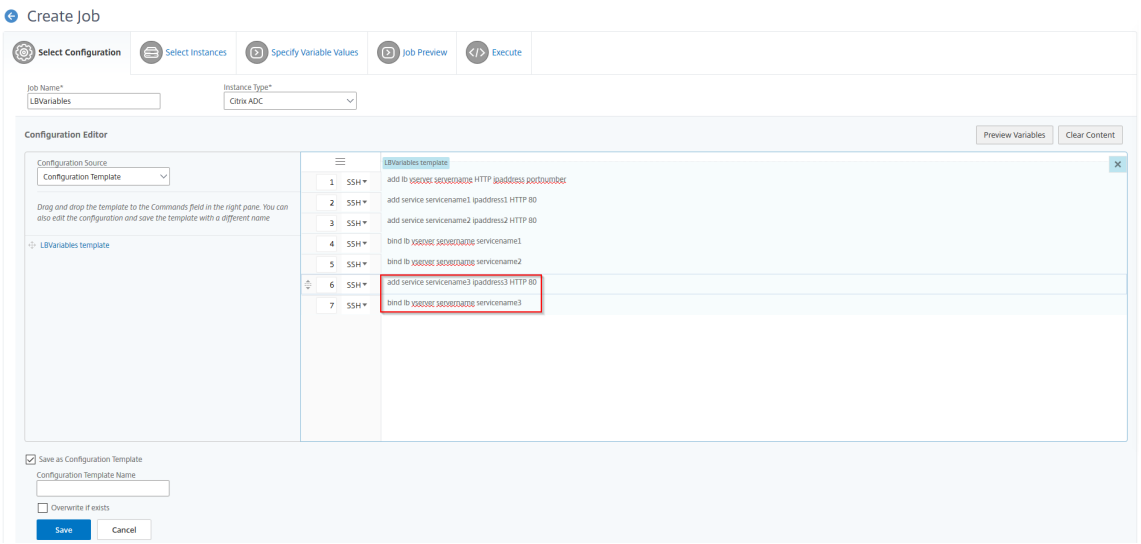


Beim Erstellen des Konfigurationsauftrags können Sie die Parameter für lokale und remote

Dateinamen in Variablen konvertieren. Auf diese Weise können Sie diesen Parametern bei jeder Ausführung des Auftrags verschiedene Dateien für denselben Satz von Citrix ADC-Instanzen zuweisen.

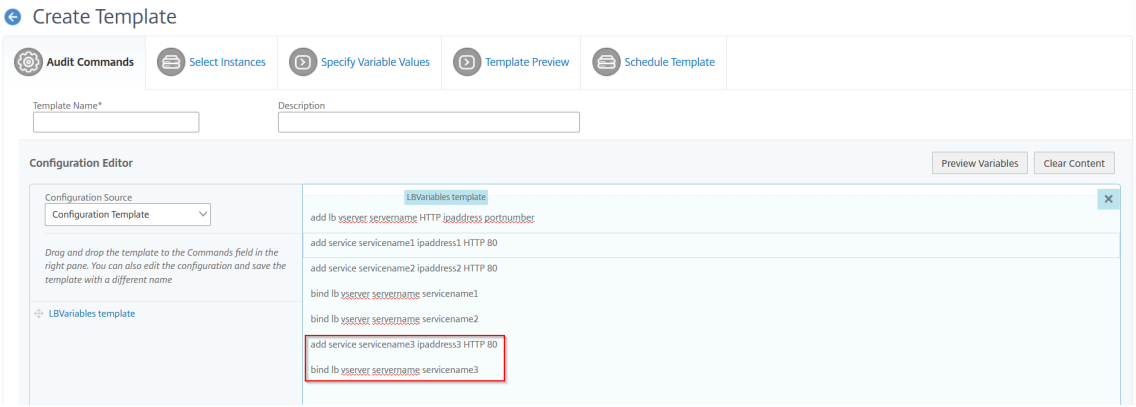
2. Wählen Sie in dem eingegebenen Befehl den Dateinamen aus, den Sie in eine Variable konvertieren möchten, und klicken Sie dann **auf In Variable umwandeln.**
3. Wählen Sie auf der Registerkarte **Instanzen auswählen** die Instanzen aus, auf denen Sie diese Befehle ausführen möchten.
4. Wenn Sie in den Befehlen Variablen angegeben haben, wählen Sie auf der Registerkarte **Variablenwerte angeben** eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:
   - Variablenwerte aus einer Eingabedatei : Laden Sie eine Eingabedatei herunter, um Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den Citrix ADM -Server hoch.
   - Allgemeine Variablenwerte für alle Instanzen — Geben Sie die IP-Adresse und den Port des Syslog-Servers an.
5. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen, und klicken Sie auf **Weiter**.
6. Klicken Sie auf der Registerkarte **Ausführen** auf **Fertig stellen**, um den Konfigurationsauftrag auszuführen.

   Wenn Sie nun einen anderen Dienst zu diesem Lastausgleichsserver hinzufügen und den Dienst an den Server binden möchten, können Sie die Befehle auf der Befehlsseite bearbeiten und speichern.



7. Navigieren Sie zu **Überwachungsvorlagen**, und klicken Sie auf **Hinzufügen**.

8. Ziehen Sie die Vorlage “LBVariablesTemplate” in den Bereich “Befehle”. Sie können sehen, dass die Vorlage mit den neuen Befehlen aktualisiert wurde.



Die Überwachungsvorlage wird in der Liste Überwachungsvorlagen angezeigt und wird alle 12 Stunden für die Konfigurationen der angegebenen Instanzen ausgeführt. Sie können jetzt Vorlagen erstellen und sie zwischen Konfigurationsaufträgen und Konfigurationsüberwachungsmodulen wiederverwenden.

Importieren und Exportieren von Konfigurationsvorlagen

April 28, 2021

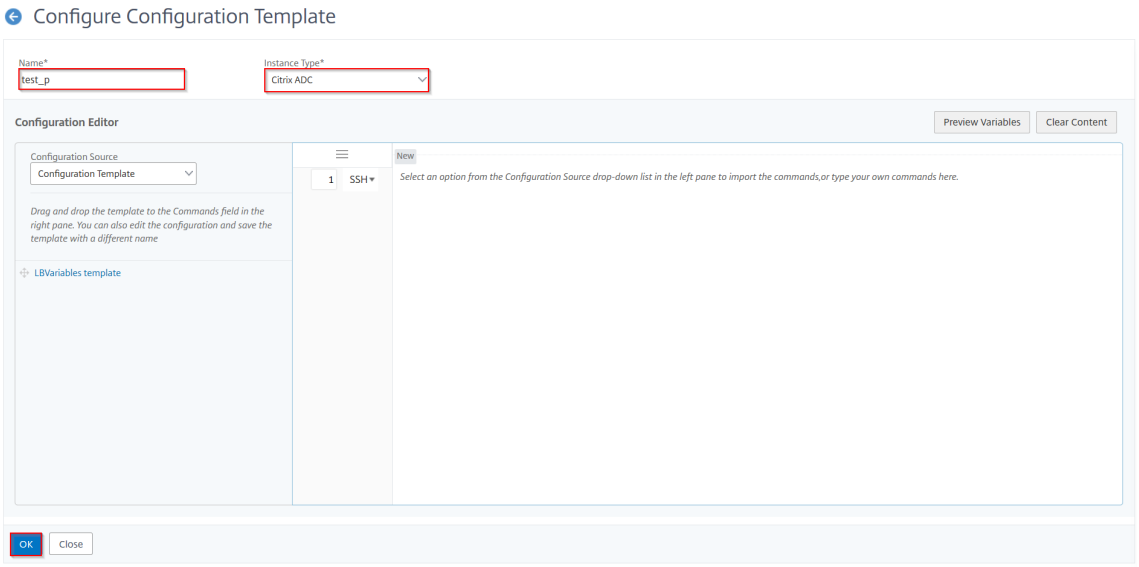
Sie können die Konfigurationsvorlagen von jeder Citrix Application Delivery Management (ADM) -Appliance exportieren und die Datei jederzeit in dieselbe oder eine andere Citrix ADM Appliance importieren. Die Daten der Konfigurationsvorlagen (wie Konfigurationsbefehle, Variablendefinitionen und Parameter) gehen nicht verloren.

Sie können die Konfigurationsvorlagen in ein **JSON-Dateiformat** exportieren und im lokalen Ordner speichern. Sie können eine Konfigurationsvorlage importieren.**json-Dateien** in Citrix ADM-Appliances, die Sie möglicherweise von derselben oder einer anderen Citrix ADM-Appliance exportiert oder manuell erstellt haben.

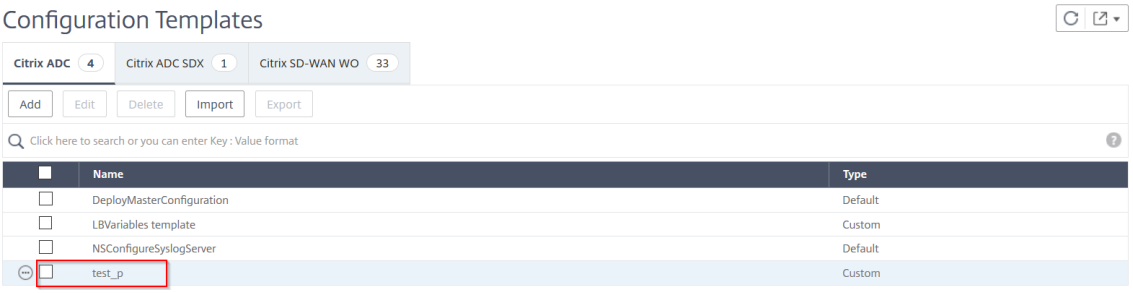
So exportieren Sie die Konfigurationsvorlagen:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge** > **Konfigurationsvorlagen**.
2. Klicken Sie auf **Hinzufügen**, um die Konfigurationsvorlage zu erstellen.

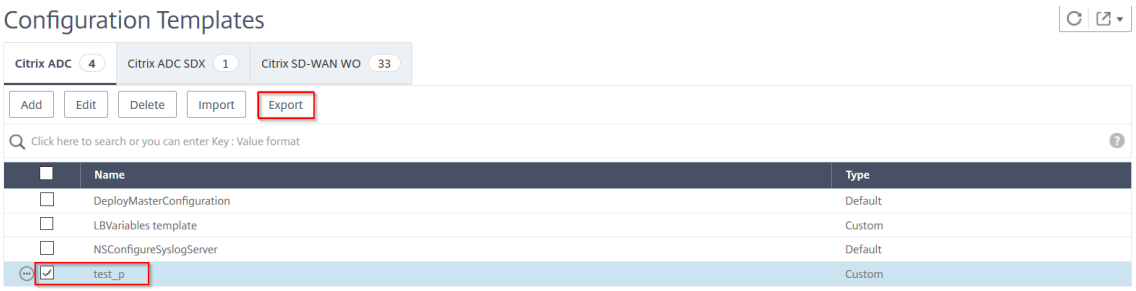
3. Geben Sie auf der Seite **Konfigurationsvorlage erstellen** den Namen der Konfigurationsvorlage an, und wählen Sie den Instanztyp aus. Wählen Sie unter **Konfigurationseditor**Konfigurationsquelle als Konfigurationsvorlage aus dem Dropdownmenü aus. Sie können die vorhandenen Konfigurationsvorlagen in den Konfigurationseditor ziehen. Klicken Sie auf **OK**.



4. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge** > **Konfigurationsvorlagen**, um die Vorlagen anzuzeigen, die in der Liste der Konfigurationsvorlagen erstellt wurden.



5. Wählen Sie die neu erstellte Konfigurationsvorlage aus, und klicken Sie auf die Schaltfläche **Exportieren**.

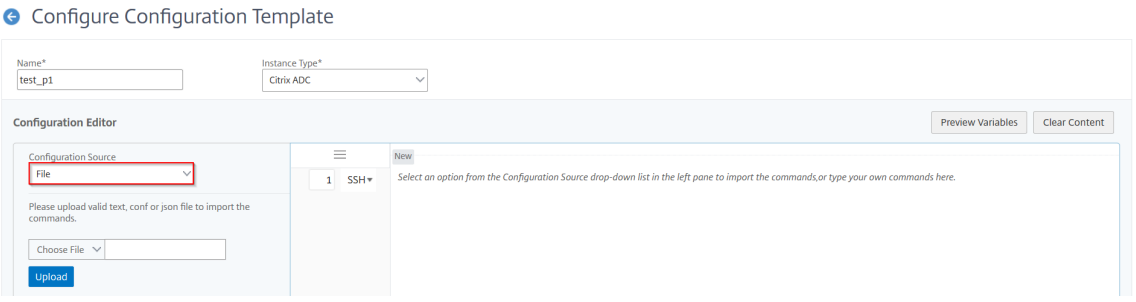


Die entsprechende Konfigurationsvorlage wird im **JSON-Format** auf Ihrem lokalen System heruntergeladen.

So importieren Sie die Konfigurationsvorlagen:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge** > **Konfigurationsvorlagen** und klicken Sie auf die Schaltfläche **Importieren**. Wählen Sie den Pfad aus, in dem die **JSON-Dateien** der Konfigurationsvorlage sind und laden Sie die **JSON-Dateien** hoch. Es wird empfohlen, die **JSON-Dateien** hochzuladen, die Sie bereits exportiert haben.

2. Sie können die Konfigurationsvorlage auch mit der Option **Datei** im **Konfigurationsedi-tor**importieren. **Wählen Sie im Dropdown-Menü im**Konfigurations-Editor**die Option**Datei aus und wählen Sie Datei**(.json-Dateien**) von Ihrem lokalen System und laden Sie die Konfigurationsvorlage hoch.**json-Dateien**.



> **Hinweis**
>
> Sie können die Konfigurationsvorlagen nur importieren, wenn die Datei im **JSON-Format** gespeichert ist. Wenn Sie andere Konfigurationsvorlagen als **JSON-Dateien** aus Ihrem lokalen System importieren, wird ein Fehler angezeigt und der Import der Dateien schlägt fehl.

Wartungsaufträge

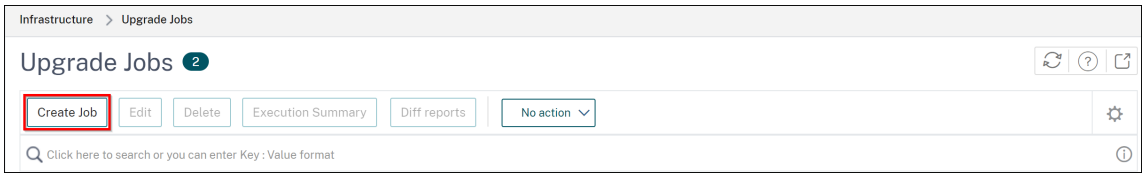
April 28, 2021

Sie können die folgenden Wartungsaufgaben mithilfe von Citrix Application Delivery Management (ADM) erstellen. Anschließend können Sie die Wartungsaufgaben zu einem bestimmten Datum und einer bestimmten Uhrzeit planen.

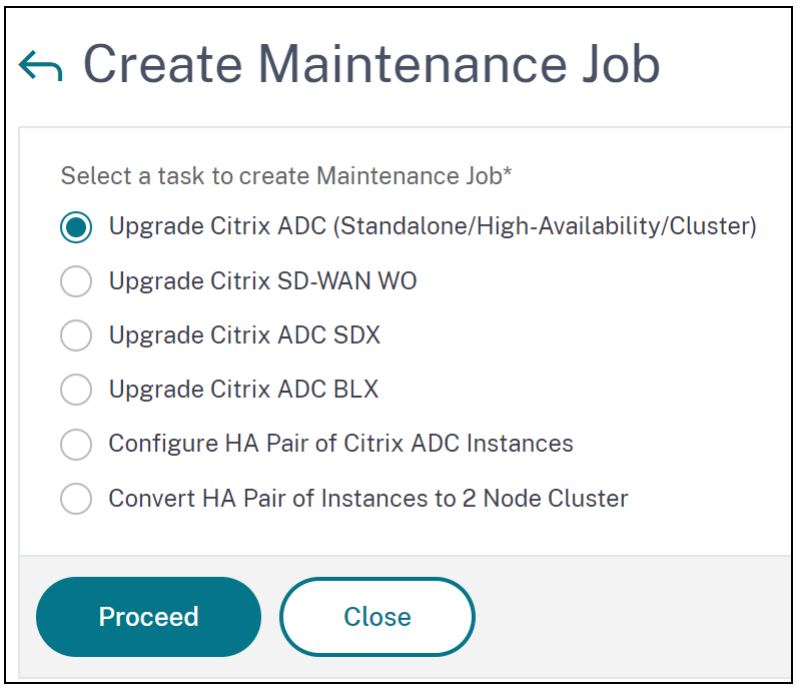
- Upgrade von Citrix ADC-Instanzen
- Upgrade von Citrix SD WAN-WO-Instanzen
- Upgrade von Citrix ADC SDX-Instanzen
- Aktualisieren von Citrix ADC-Instanzen in der Autoscale-Gruppe
- Konfigurieren des HA-Paares von Citrix ADC-Instanzen
- Konvertieren von HA-Instanzen in Cluster

Planen des Upgrades von Citrix ADC-Instanzen

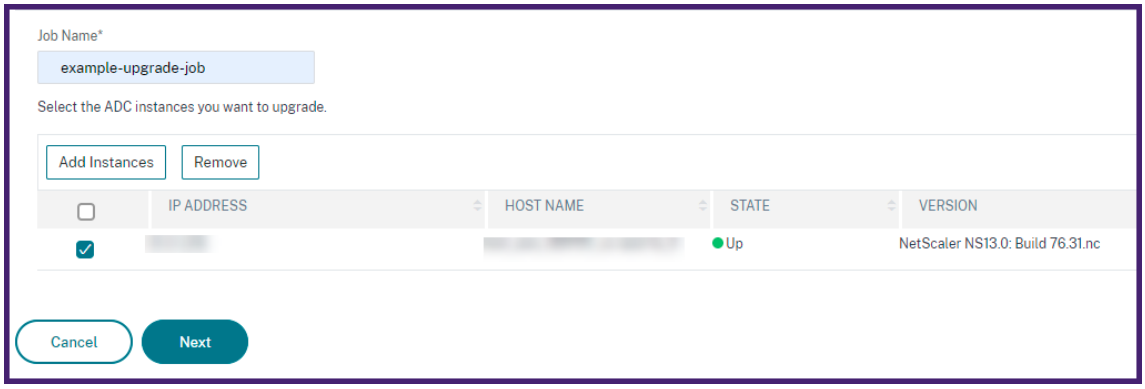
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsjobs** > **Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Job erstellen**.



2. Wählen Sie unter **Wartungsaufträge erstellen** die Option **Upgrade Citrix ADC (Standalone/High Availability/Cluster)** aus, und klicken Sie auf **Weiter**.



3. Geben Sie unter **Instanz auswählen** einen Namen Ihrer Wahl für **Auftragsname** ein.
4. Klicken Sie auf **Instanzen hinzufügen**, um ADC-Instanzen hinzuzufügen, die Sie aktualisieren möchten.
   - Um ein HA-Paar zu aktualisieren, geben Sie die IP-Adresse eines primären oder sekundären Knotens an. Es wird jedoch empfohlen, die primäre Instanz zum Upgrade des HA-Paares zu verwenden.
   - Um einen Cluster zu aktualisieren, geben Sie die Cluster-IP-Adresse an.



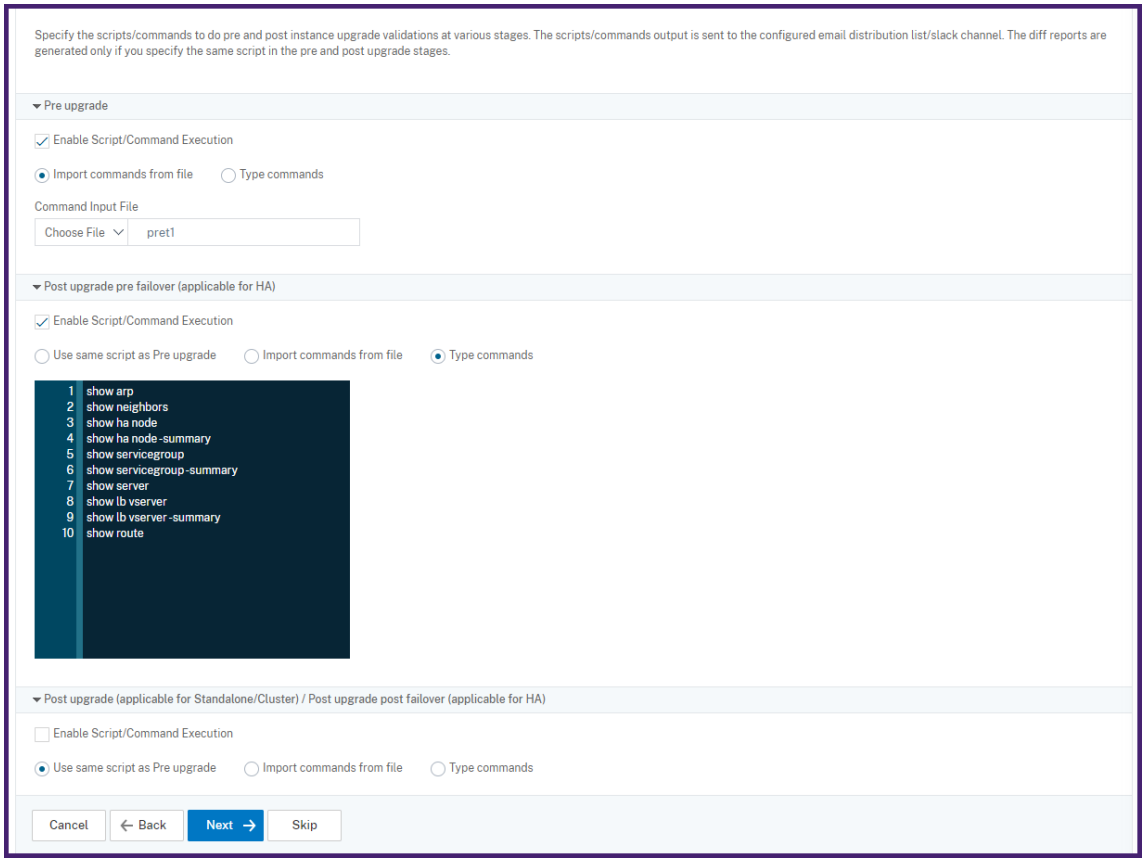
5. Klicken Sie auf **Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten.

   Auf der Registerkarte " **Validierung vor dem Upgrade** " werden die fehlgeschlagenen Instanzen angezeigt. Entfernen Sie die fehlgeschlagenen Instanzen, und klicken Sie auf **Weiter**.

> **Wichtig**
>
> Wenn Sie die Cluster-IP-Adresse angeben, führt ADM die Validierung vor dem Upgrade nur für die angegebene Instanz und nicht auf den anderen Clusterknoten durch.

6. Optional geben Sie in **Custom scripts**die Scripts an, die vor und nach einem Instanzupgrade ausgeführt werden sollen. Verwenden Sie eine der folgenden Möglichkeiten, um die Befehle auszuführen:

   - **Befehle aus Datei importieren** - Wählen Sie die Befehlseingabedatei von Ihrem lokalen Computer aus.
   - **Befehle eingeben** - Geben Sie Befehle direkt auf der GUI ein.



   Sie können benutzerdefinierte Skripte verwenden, um die Änderungen vor und nach einem Instanz-Upgrade zu überprüfen. Beispiel:

   - Die Instanzversion vor und nach dem Upgrade.
   - Der Status von Schnittstellen, Hochverfügbarkeitsknoten, virtuellen Servern und Diensten vor und nach dem Upgrade.
   - Die Statistiken der virtuellen Server und Dienste.
   - Die dynamischen Routen.

7. Wählen Sie unter **Task planen** eine der folgenden Optionen aus:

- **Jetzt upgraden** - Der Upgrade-Auftrag wird sofort ausgeführt.
- **Später planen** - Wählen Sie diese Option, um diesen Upgrade-Auftrag später auszuführen. Geben Sie das **Ausführungsdatum** und die **Startzeit** an, wenn Sie die Instanzen aktualisieren möchten.

  Wenn Sie ein ADC-HA-Paar in zwei Stufen aktualisieren möchten, wählen Sie **Zweistufige Aktualisierung für Knoten in HA durchführen** aus.

  Geben Sie das **Ausführungsdatum** und die **Startzeit** an, wenn Sie eine andere Instanz im HA-Paar aktualisieren möchten.

8. Geben Sie unter **Job erstellen** die folgenden Details an:

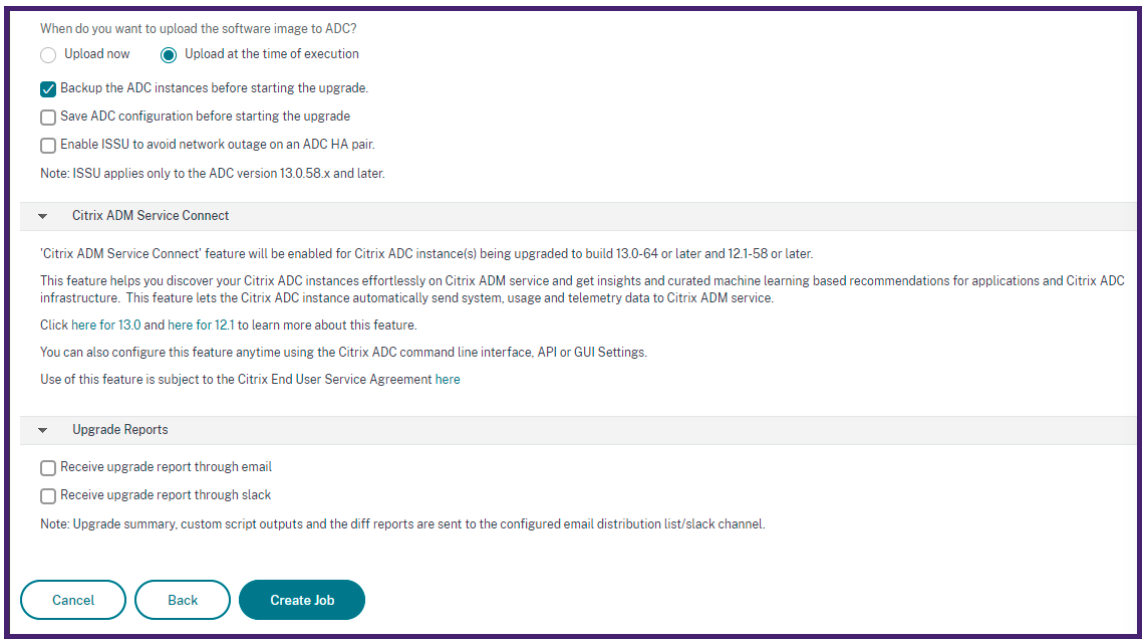
   a) Wählen Sie in der Liste **Softwareimage** eine der folgenden Optionen aus:

   - **Lokal** - Wählen Sie die Instanz-Upgradedatei von Ihrem lokalen Computer aus.
   - **Appliance** : Wählen Sie die Instanz-Upgradedatei aus einem ADM-Dateibrowser aus. Die ADM-GUI zeigt die Instanzdateien an, die in vorhanden sind `/var/mps/mps_images`.

   b) Geben Sie an, wann Sie das Image in eine Instanz hochladen möchten:

   - **Jetzt hochladen** - Wählen Sie diese Option, um das Image sofort hochzuladen. Der Upgrade-Auftrag wird jedoch zum geplanten Zeitpunkt ausgeführt.
   - **Upload zum Zeitpunkt der Ausführung** - Wählen Sie diese Option, um das Image zum Zeitpunkt der Ausführung des Upgrade-Auftrags hochzuladen.

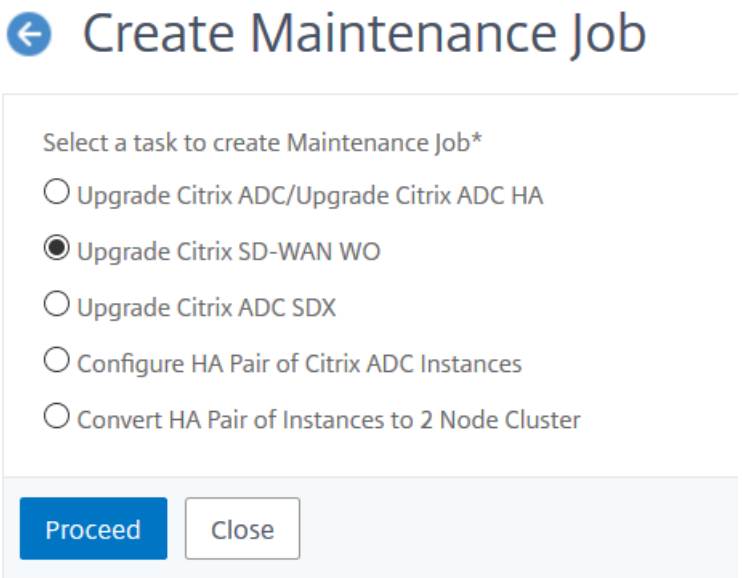
   - **Software-Image von Citrix ADC bei erfolgreichem Upgrade bereinigen**: Wählen Sie diese Option, um das hochgeladene Image in der ADC-Instanz nach dem Instanz-Upgrade zu löschen.
   - **Sichern Sie die ADC-Instanzen, bevor Sie das Upgrade starten.** - Erstellt ein Backup der ausgewählten ADC-Instanzen.
   - **Aktivieren Sie ISSU, um Netzwerkausfälle beim ADC HA-Paar zu vermeiden** - ISSU stellt das Upgrade ohne Ausfallzeiten bei einem ADC-Hochverfügbarkeitspaar sicher. Diese Option bietet eine Migrationsfunktionalität, die die vorhandenen Verbindungen während des Upgrades berücksichtigt. Sie können also ein ADC HA-Paar ohne Ausfallzeiten aktualisieren. Geben Sie das Timeout der ISSU Migration in Minuten an.
   - **Ausführungsbericht per E-Mail empfangen** - Sendet den Ausführungsbericht per E-Mail. Informationen zum Hinzufügen einer E-Mail-Verteilerliste finden Sie unter Erstellen einer E-Mail-Verteilerliste.
   - **Ausführungsbericht über Pufferzeit empfangen** - Sendet den Ausführungsbericht in Pufferzeit. Informationen zum Hinzufügen eines Slack Profils finden Sie unter Erstellen eines Slack Profils.



9. Klicken Sie auf **Job erstellen**.

Planen der Aktualisierung von Citrix SD-WAN WO-Instanzen

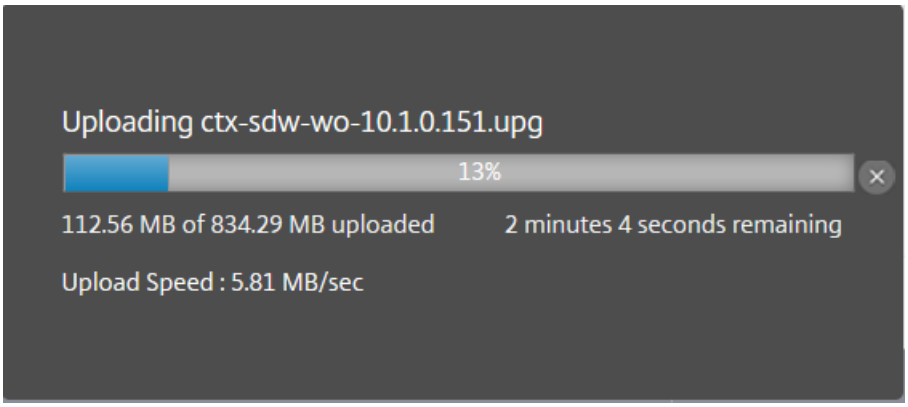
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsjobs** > **Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Job erstellen**.
2. Wählen Sie **Upgrade Citrix SD-WAN WO** und klicken Sie auf **Proceed**.



3. Klicken Sie auf der Seite **Upgrade Citrix SD-WAN WO** auf der Registerkarte **Instanzauswahl**:
   a) Fügen Sie einen **Vorgangsnamen** hinzu.

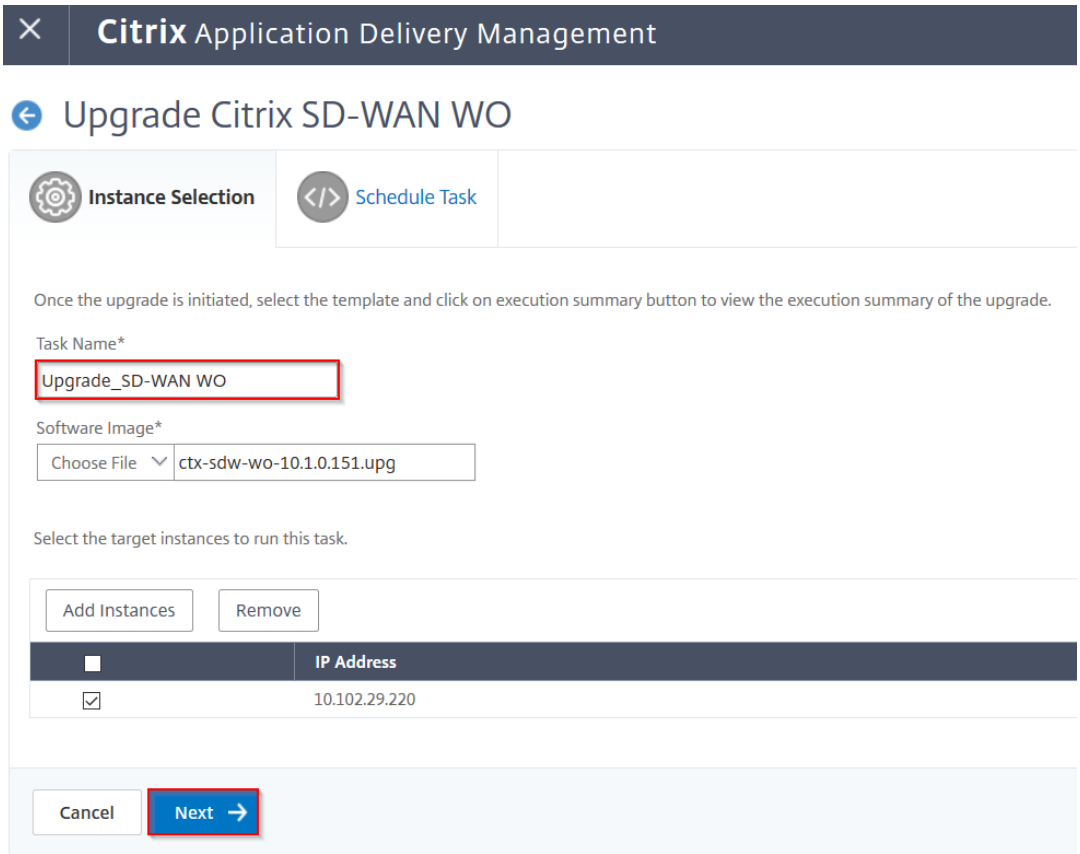
b) Klicken Sie im Dropdownmenü Software-Image auf Lokal (Ihr lokaler Computer) oder Appliance (die Builddatei muss auf der virtuellen Citrix ADM Appliance vorhanden sein).

Der Upload-Prozess beginnt.



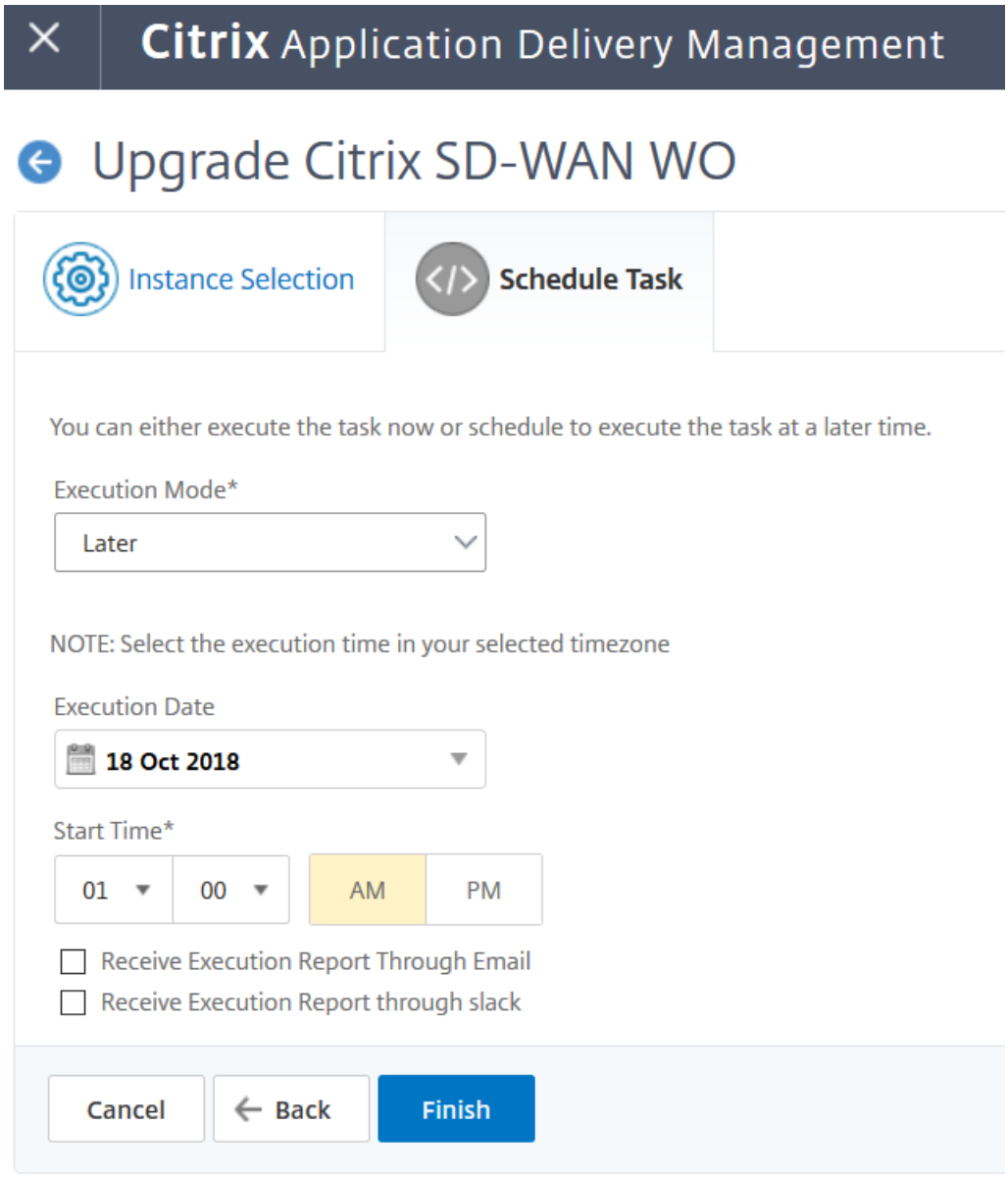
c) Klicken Sie auf **Instanzen hinzufügen**, um die Citrix SD-WAN WO-Instanzen hinzuzufügen, für die Sie den Upgradevorgang ausführen möchten.

d) Klicken Sie auf **Weiter**.



4. Wählen Sie auf der Registerkarte **Task planen** in der Liste **Ausführungsmodus** die Option **Jetzt** aus, um eine Citrix SD-WAN WO-Instanz jetzt zu aktualisieren, und klicken Sie auf **Fertig stellen**.

5. Um eine Citrix ADC SD-WAN WO-Instanz später zu aktualisieren, wählen Sie **Später** aus der Liste **Ausführungsmodus** aus. Sie können dann das Ausführungsdatum und die Startzeit für das Upgrade der Citrix ADC SD-WAN WO-Instanz auswählen und auf **Fertig stellen** klicken.

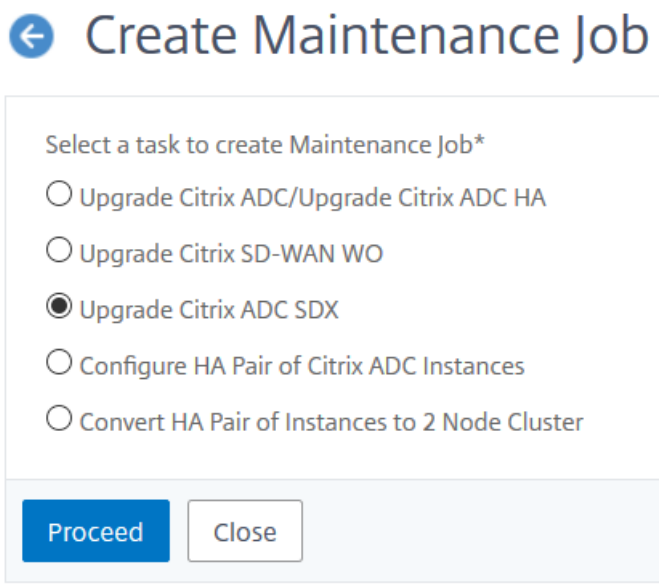


6. Sie können auch E-Mail- und Slack-Benachrichtigungen aktivieren, um den Ausführungsbericht für das Upgrade einer Citrix SD-WAN WO-Instanz zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail** empfangen und **Ausführungsbericht über Pufferzeit** empfangen, um die Benachrichtigungen zu aktivieren.

   Weitere Informationen zum Konfigurieren der E-Mail-Verteilerliste und des Pufferkanals finden Sie in **Schritt 8** in Planen des Upgrades von Citrix ADC-Instanzen

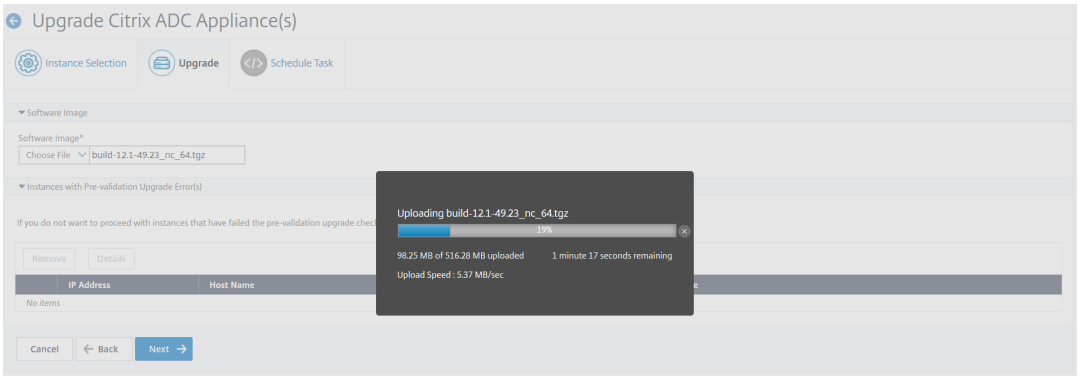
Planen des Upgrades von Citrix ADC SDX-Instanzen

1. Navigieren Sie in Citrix ADM zu **Netzwerke > Konfigurationsaufträge > Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Job erstellen**.
2. Wählen Sie **Citrix ADC SDX aktualisieren** und klicken Sie auf **Weiter**.

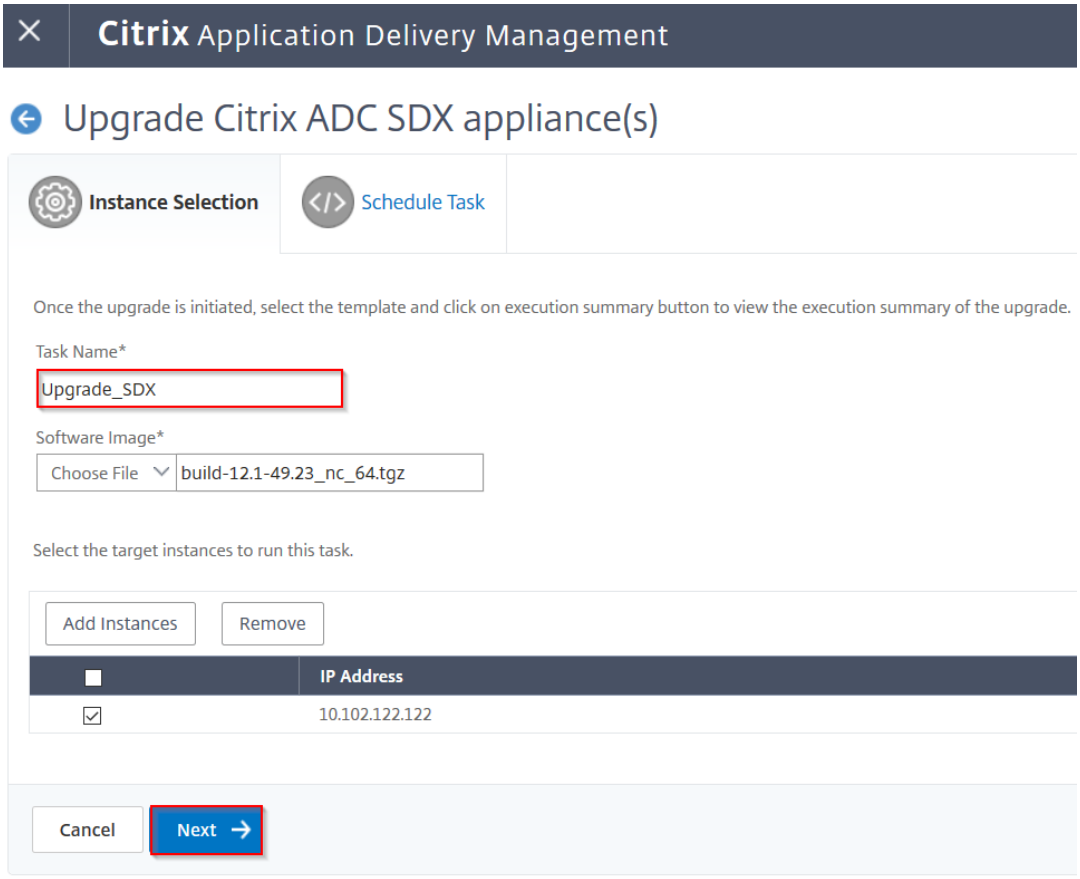


3. Klicken Sie auf der Seite **Upgrade von Citrix ADC SDX** auf der Registerkarte **Instanzauswahl**:
   a) Fügen Sie einen **Vorgangsnamen** hinzu.
   b) Wählen Sie im Dropdownmenü Software-Image entweder Lokal (Ihr lokaler Computer) oder Appliance (die Builddatei muss auf der virtuellen Citrix ADM Appliance vorhanden sein).

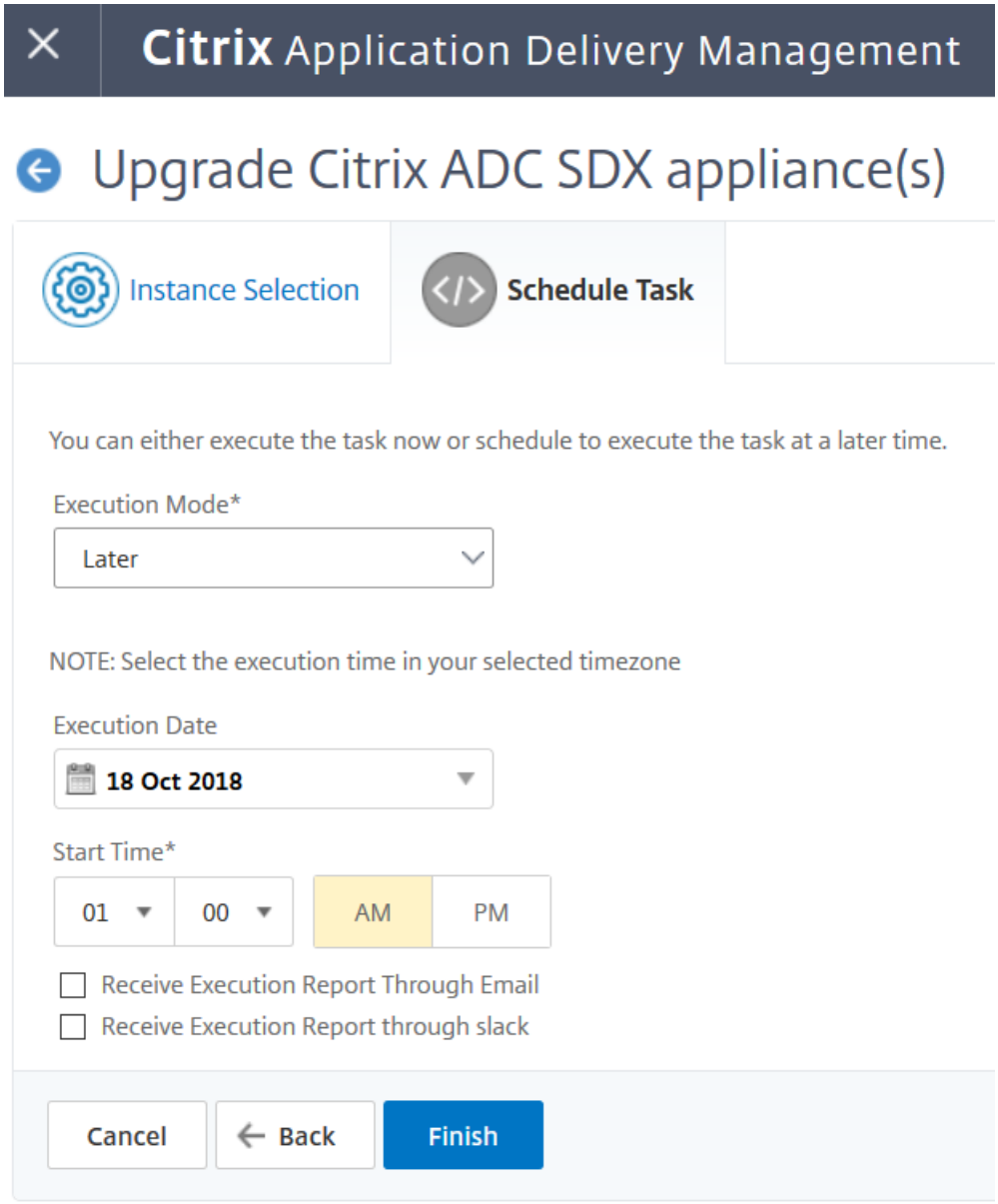
      Der Upload-Prozess beginnt.



   c) Fügen Sie die Citrix ADC SDX-Instanzen hinzu, auf denen Sie den Upgradevorgang ausführen möchten.
   d) Klicken Sie auf **Weiter**.



4. Wählen Sie auf der Registerkarte **Task planen** in der Liste **Ausführungsmodus** die Option **Jetzt** aus, um eine Citrix SD-WAN WO-Instanz jetzt zu aktualisieren, und klicken Sie auf **Fertig stellen**.
5. Um eine Citrix ADC SDX-Instanz später zu aktualisieren, wählen Sie **Später** aus der Liste **Ausführungsmodus** aus. Sie können dann das Ausführungsdatum und die Startzeit für das Upgrade der Citrix ADC SD-WAN WO-Instanz auswählen und auf **Fertig stellen** klicken.



6. Sie können auch E-Mail- und Slack-Benachrichtigungen aktivieren, um den Ausführungsbericht der aktualisierten Citrix ADC SDX-Instanz zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail** empfangen und **Ausführungsbericht über Pufferzeit** empfangen, um die Benachrichtigungen zu aktivieren.

   Weitere Informationen zum Konfigurieren der E-Mail-Verteilerliste und des Pufferkanals finden Sie in **Schritt 8** in Planen des Upgrades von Citrix ADC-Instanzen

Planen der Aktualisierung der Autoskalierungsgruppe

Führen Sie die folgenden Schritte aus, um alle Instanzen in den Clouddiensten zu aktualisieren, die Teil der Autoscale-Gruppe sind:

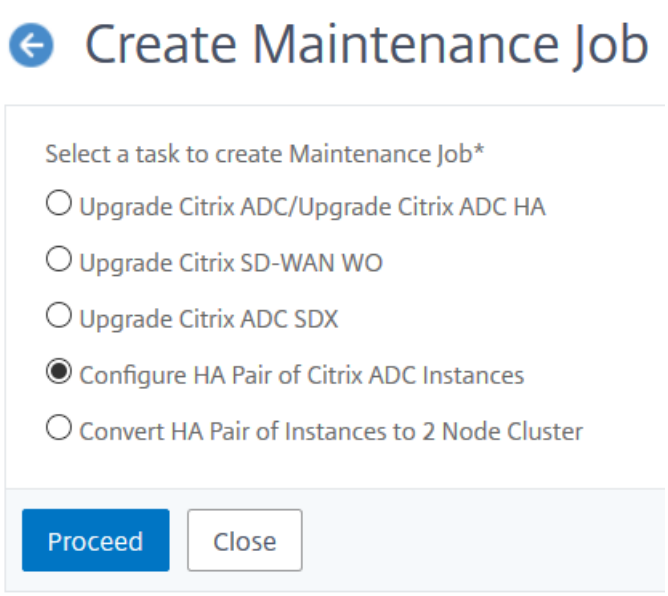
1. Navigieren Sie in Citrix ADM zu **Netzwerke > Konfigurationsaufträge > Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Job erstellen**.
2. Wählen Sie **Autoscale-Gruppe aktualisieren** aus und klicken Sie auf **Weiter**.
3. Auf der Registerkarte **Upgradeeinstellungen**:
   a) Wählen Sie die **Autoskalierungsgruppe** aus, die Sie aktualisieren möchten.
   b) Wählen Sie unter **Image**die Citrix ADC Version aus. Dieses Bild ist die vorhandene Version von Citrix ADC-Instanzen in der Autoscale-Gruppe.
   c) Suchen Sie in **Citrix ADC Image**die Citrix ADC Versionsdatei, auf die Sie ein Upgrade durchführen möchten.

      Wenn Sie die Option **Graceful Upgrade**aktivieren, wartet der Upgrade-Task bis der angegebene Ablaufverbindungszeitraum abläuft.
   d) Klicken Sie auf **Weiter**.
4. Auf der Registerkarte **Task planen**:
   a) Wählen Sie in der Liste Ausführungsmodus eine der folgenden Optionen aus:
      - **Jetzt:**Um das Upgrade der Citrix ADC-Instanzen sofort zu starten.
      - **Später:** Um das Upgrade der Citrix ADC-Instanzen zu einem späteren Zeitpunkt zu starten.
   b) Wenn Sie die Option **Später** auswählen, wählen Sie das Ausführungsdatum und die Startzeit, wenn Sie den Upgrade-Task starten möchten.

   Du kannst auch E-Mail- und Slack-Benachrichtigungen aktivieren, um den Ausführungsbericht der Upgrade-Autoscale-Gruppe zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail** empfangen und **Ausführungsbericht über Pufferzeit** empfangen, um die Benachrichtigungen zu aktivieren.
5. Klicken Sie auf **Fertig stellen**.

Planen der Konfiguration des HA-Paares von Citrix ADC-Instanzen

1. Navigieren Sie in Citrix ADM zu **Netzwerke > Konfigurationsaufträge > Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Job erstellen**.
2. Wählen Sie **HA Pair of Citrix ADC-Instanzen konfigurieren** und klicken Sie auf **Proceed**.



3. Klicken Sie auf der Seite **Citrix ADC HA-Paar** auf der Registerkarte **Instanzauswahl**:

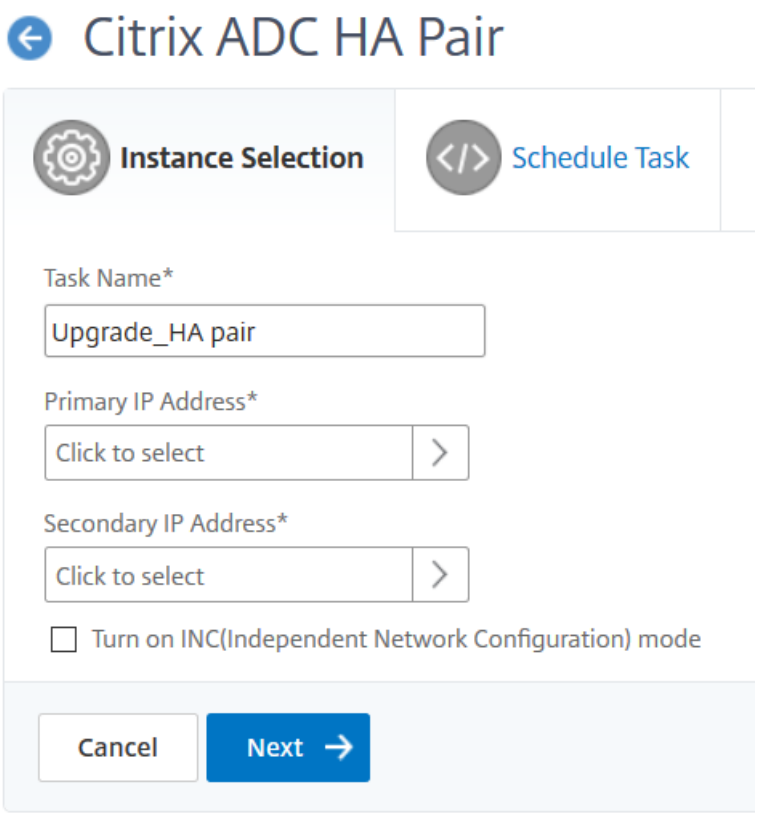
   a) Fügen Sie einen **Vorgangsnamen** hinzu.

   b) Geben Sie die primäre IP-Adresse ein.

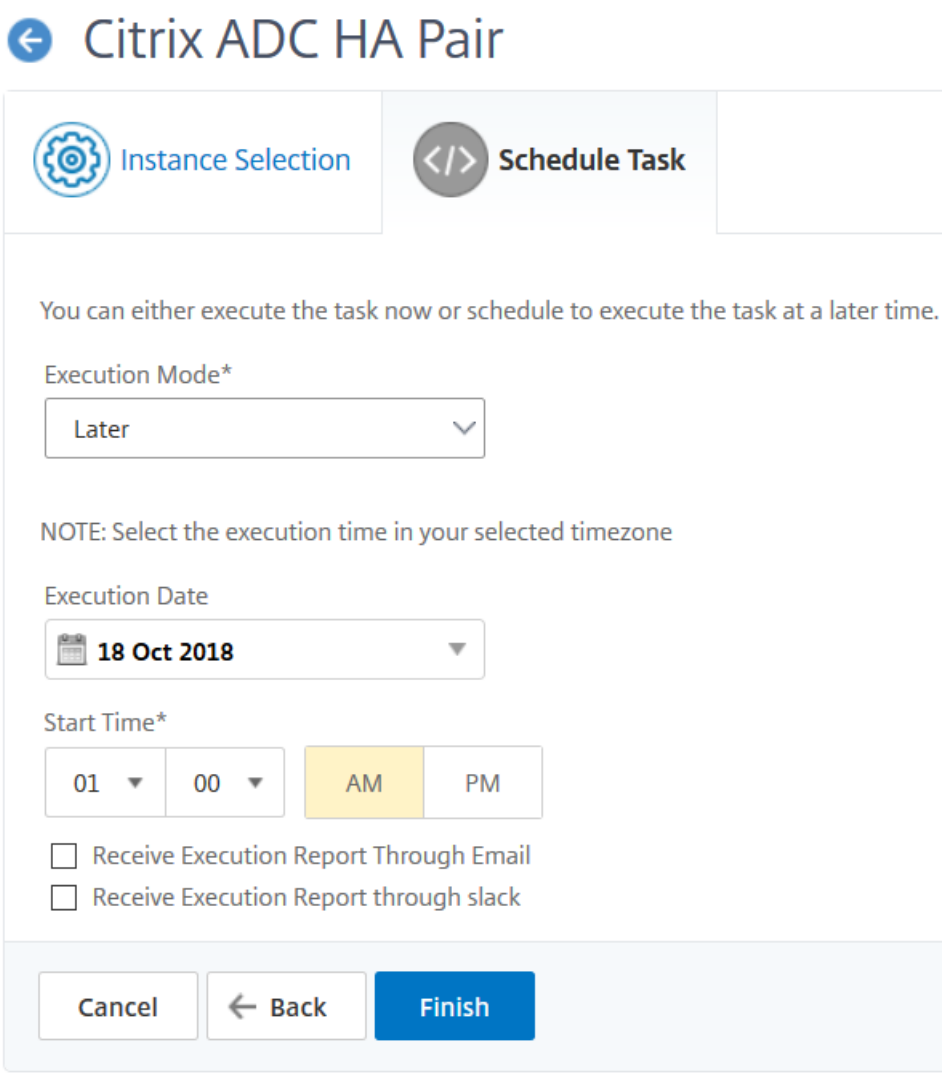
   c) Geben Sie die sekundäre IP-Adresse ein.

   d) Klicken Sie auf **Weiter**.

   e) Klicken Sie hier, um **den INC-Modus (Independent Network Configuration)** zu aktivieren, wenn die HA-Paarinstanzen in zwei Subnetzen vorhanden sind.



4. Wählen Sie auf der Registerkarte **Task planen** in der Liste **Ausführungsmodus** die Option **Jetzt** aus, um eine Citrix SD-WAN WO-Instanz jetzt zu aktualisieren, und klicken Sie auf **Fertig stellen**.
5. Um später ein Citrix ADC HA-Paar zu aktualisieren, wählen Sie **Später** aus der Liste **Ausführungsmodus** aus. Sie können dann das Ausführungsdatum und die Startzeit für das Upgrade der Citrix ADC SD-WAN WO-Instanz auswählen und auf **Fertig stellen** klicken.

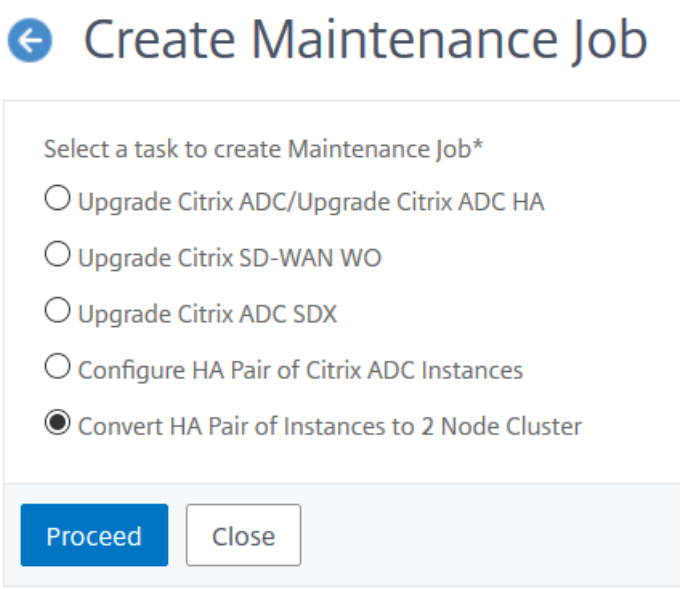


6. Du kannst auch E-Mail- und Slack-Benachrichtigungen aktivieren, um den Ausführungsbericht zum Erstellen des ADC HA-Paares zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail** empfangen und **Ausführungsbericht über Pufferzeit** empfangen, um die Benachrichtigungen zu aktivieren.

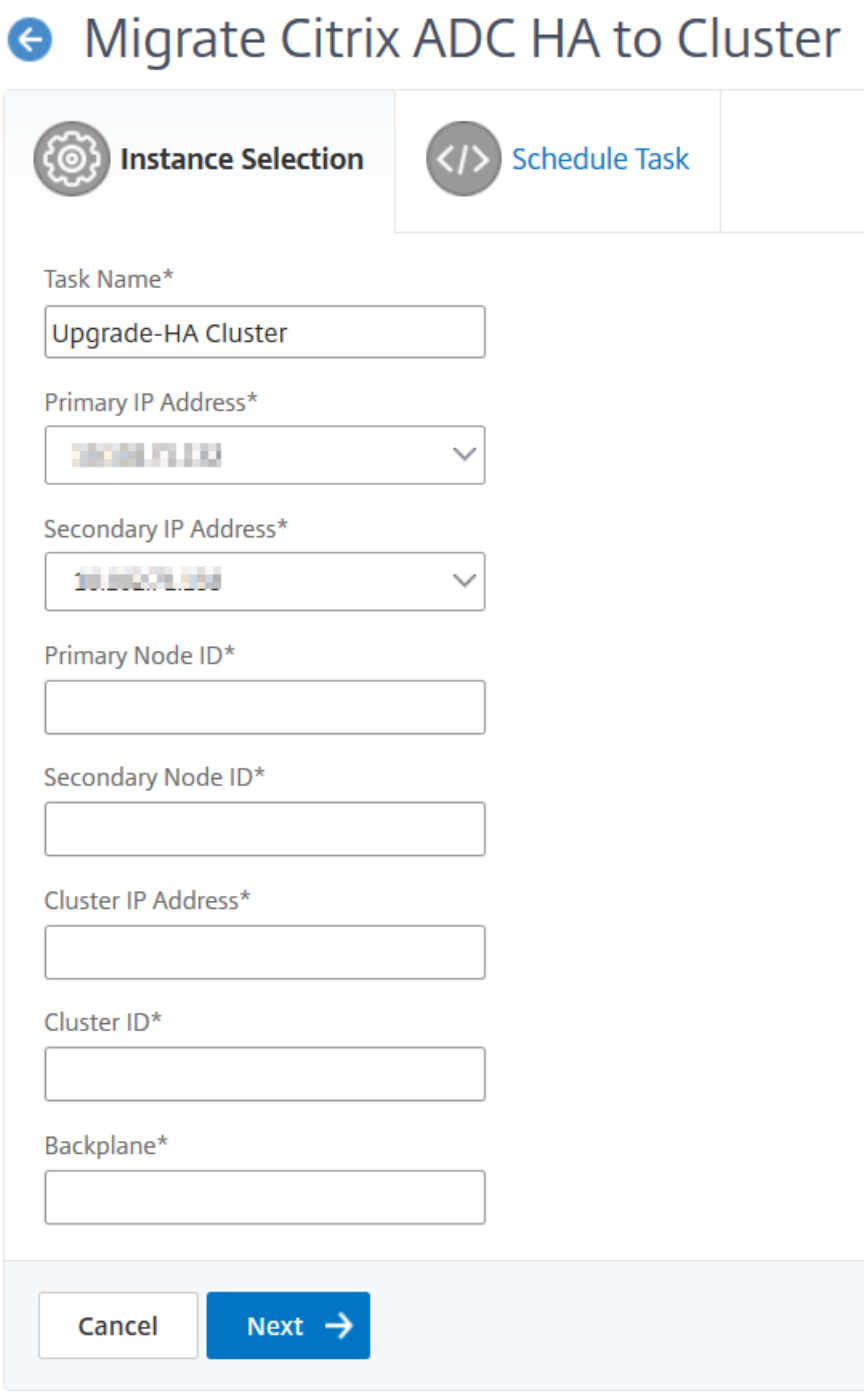
   Weitere Informationen zum Konfigurieren der E-Mail-Verteilerliste und des Pufferkanals finden Sie in **Schritt 8** in Planen des Upgrades von Citrix ADC-Instanzen

Planen der Konvertierung von HA-Instanzen in Cluster

1. Navigieren Sie in Citrix ADM zu **Netzwerke > Konfigurationsaufträge > Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Job erstellen**.
2. Wählen Sie **HA-Paar von Instanzen in 2-Knoten-Cluster konvertieren** und klicken Sie auf **Proceed**.



3. Fügen Sie auf der Seite **NetScaler HA zu Cluster migrieren** auf der Registerkarte **Instanzauswahl** einen **Tasknamen** hinzu. Geben Sie die primäre IP-Adresse, die sekundäre IP-Adresse, die primäre Node-ID, die sekundäre Node-ID, die Cluster-IP-Adresse, die Cluster-ID und die Rückwandplatine an, und klicken Sie dann auf **Weiter**.



4. Wählen Sie auf der Registerkarte **Task planen** in der Liste **Ausführungsmodus** die Option **Jetzt** aus, um eine Citrix SD-WAN WO-Instanz jetzt zu aktualisieren, und klicken Sie auf **Fertig stellen**.
5. Um später zu aktualisieren, wählen Sie **Später** aus der Liste **Ausführungsmodus** aus. Sie können dann das **Ausführungsdatum** und die **Startzeit** für das Upgrade der Citrix ADC SD-WAN WO-Instanz auswählen und auf **Fertig stellen**klicken.
6. Sie können auch E-Mail- und Slack-Benachrichtigungen aktivieren, um den Ausführungsbericht

für das Upgrade einer Citrix ADC SDX-Instanz zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail** empfangen und **Ausführungsbericht über Pufferzeit** empfangen, um die Benachrichtigungen zu aktivieren.

Weitere Informationen zum Konfigurieren der E-Mail-Verteilerliste und des Pufferkanals finden Sie in **Schritt 8** in Planen des Upgrades von Citrix ADC-Instanzen

Konfigurations-Audit

January 3, 2020

Dieses Dokument enthält:

- Erstellen von Überwachungsvorlagen
- Anzeigen von Überwachungsberichten
- Überwachen von Konfigurationsänderungen über alle Instanzen hinweg
- Erhalten Sie Konfigurationshinweise zur Netzwerkkonfiguration
- Abfragen der Konfigurationsüberwachung von Citrix ADM Instanzen
- Konfigurations-Audit-Diff für ConfigChange SNMP-Traps generieren

Erstellen von Überwachungsvorlagen

April 28, 2021

Sie möchten sicherstellen, dass bestimmte Konfigurationen auf bestimmten Instanzen ausgeführt werden, um die optimale Leistung Ihres Netzwerks zu gewährleisten. Außerdem möchten Sie Konfigurationsänderungen über verwaltete Citrix ADC-Instanzen hinweg überwachen, Konfigurationsfehler beheben und nicht gespeicherte Konfigurationen nach einem plötzlichen Herunterfahren des Systems wiederherstellen. Sie können Überwachungsvorlagen mit bestimmten Konfigurationen erstellen, die Sie für bestimmte Instanzen überwachen möchten. Citrix Application Delivery Management (ADM) vergleicht diese Instanzen mit der Prüfungsvorlage und meldet, ob die Konfiguration nicht übereinstimmt. Wenn eine Konfiguration nicht übereinstimmt, generiert Citrix ADM einen Konfigurationsabgrenzungsbericht, mit dem Sie Probleme beheben und unerwünschte Konfigurationsänderungen korrigieren können.

Sie können die Ausführung der Prüfvorlage automatisieren, indem Sie

- Planen der Zeit, zu der die Vorlage ausgeführt werden muss
- Festlegen der Häufigkeit, mit der Citrix ADM die Vorlage ausführen muss. Sie können die Vorlage täglich, an einem bestimmten Tag in einer Woche oder an einem bestimmten Datum in einem

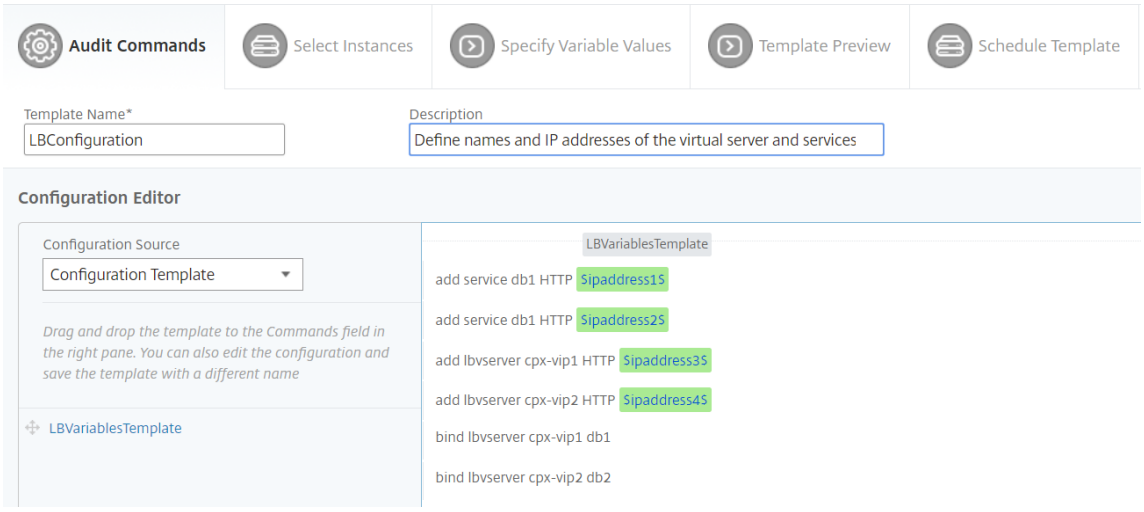
Monat ausführen.

Außerdem haben Sie die Möglichkeit, den von Citrix ADM generierten Diff-Bericht an bestimmte E-Mail-Adressen zu senden, die Sie konfigurieren können. Mit dieser Option kann der Benutzer den Bericht als E-Mail-Anhang empfangen, und der Benutzer muss sich nicht bei Citrix ADM anmelden, um die Berichte manuell zu exportieren.

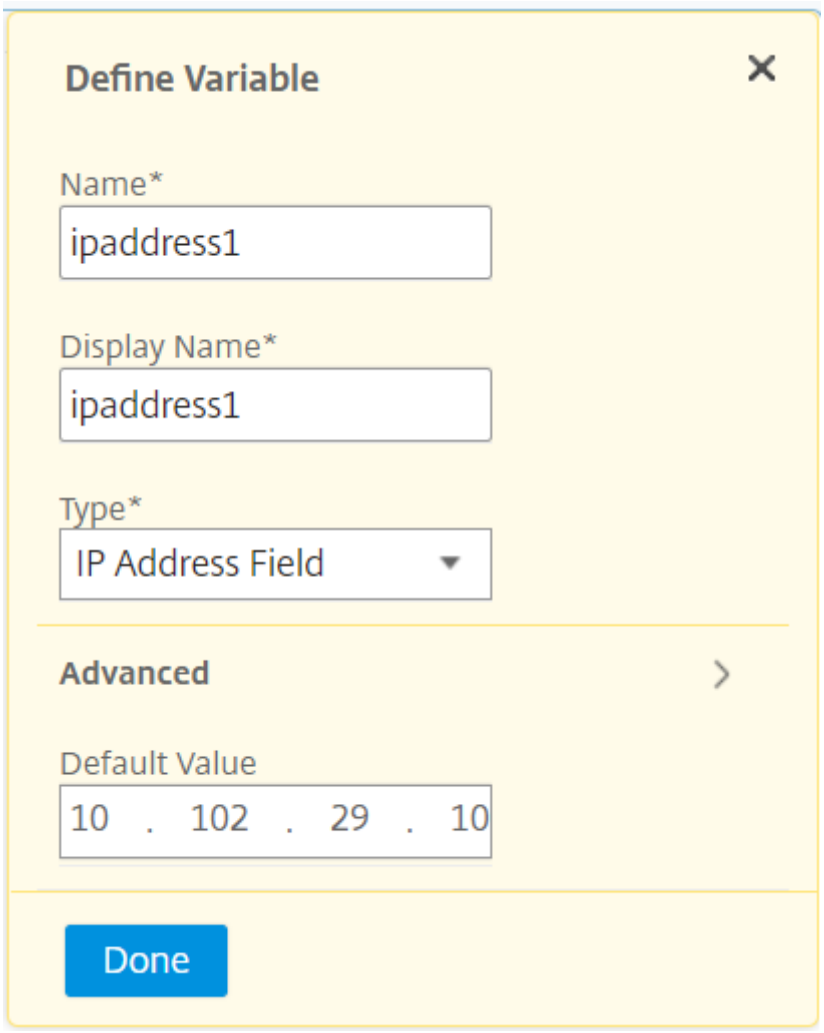
> **Hinweis**
> Die Option **Umbenennen** ist für die Standardkonfigurationsvorlagen deaktiviert. Sie können jedoch benutzerdefinierte Konfigurationsvorlagen umbenennen.

So erstellen Sie Überwachungsvorlagen:

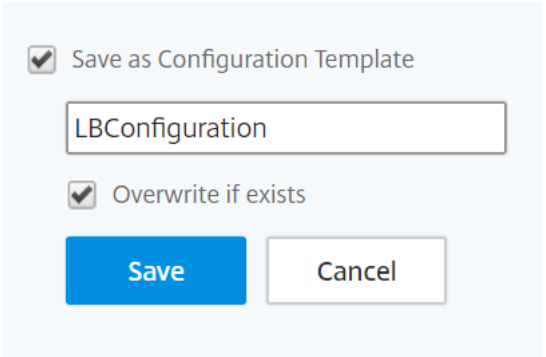
1. Navigieren Sie zu **Netzwerke** > **Konfigurationsüberwachung** > **Überwachungsvorlagen**, und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Vorlage erstellen** und auf der Registerkarte **Überwachungsbefehle** den Vorlagennamen und die Beschreibung an.
3. Geben Sie auf der Seite **Konfigurationseditor** Ihre Befehle ein, und speichern Sie die Befehle als Konfigurationsvorlage. Sie können auch eine vorhandene Vorlage aus dem linken Fensterbereich in den Editor ziehen.
4. Wählen Sie die Werte aus, die Sie in eine Variable konvertieren möchten, und klicken Sie dann auf **In Variable konvertieren**. Wählen Sie beispielsweise die IP-Adresse des Load Balancing-Servers ipaddress1 aus, und klicken Sie auf **In Variable konvertieren**. Die Variable ist nun mit “$” eingeschlossen, wie in der Abbildung unten gezeigt.



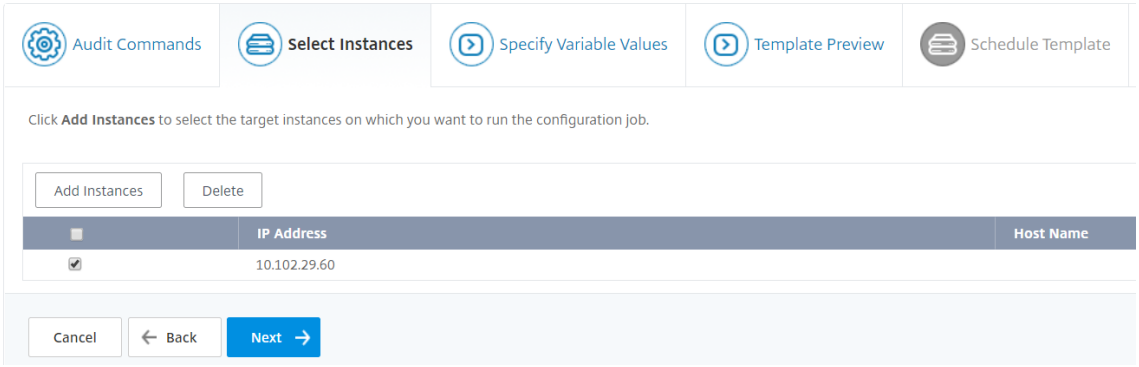
Legen Sie im Fenster **Variable definieren** die Eigenschaften für diese Variable fest: Name, Anzeigename und Typ der Variablen. Klicken Sie auf die Option **Erweitert**, wenn Sie einen Standardwert für Ihre Variable weiter angeben möchten.



Sie können die Befehle auch als Konfigurationsvorlage speichern.



5. Klicken Sie auf **Speichern**, und klicken Sie dann auf **Weiter**.
6. Wählen Sie auf der Registerkarte **Instanzen auswählen** die Instanzen aus, auf denen die Konfigurationsüberwachung ausgeführt werden soll, und klicken Sie auf **Weiter**.

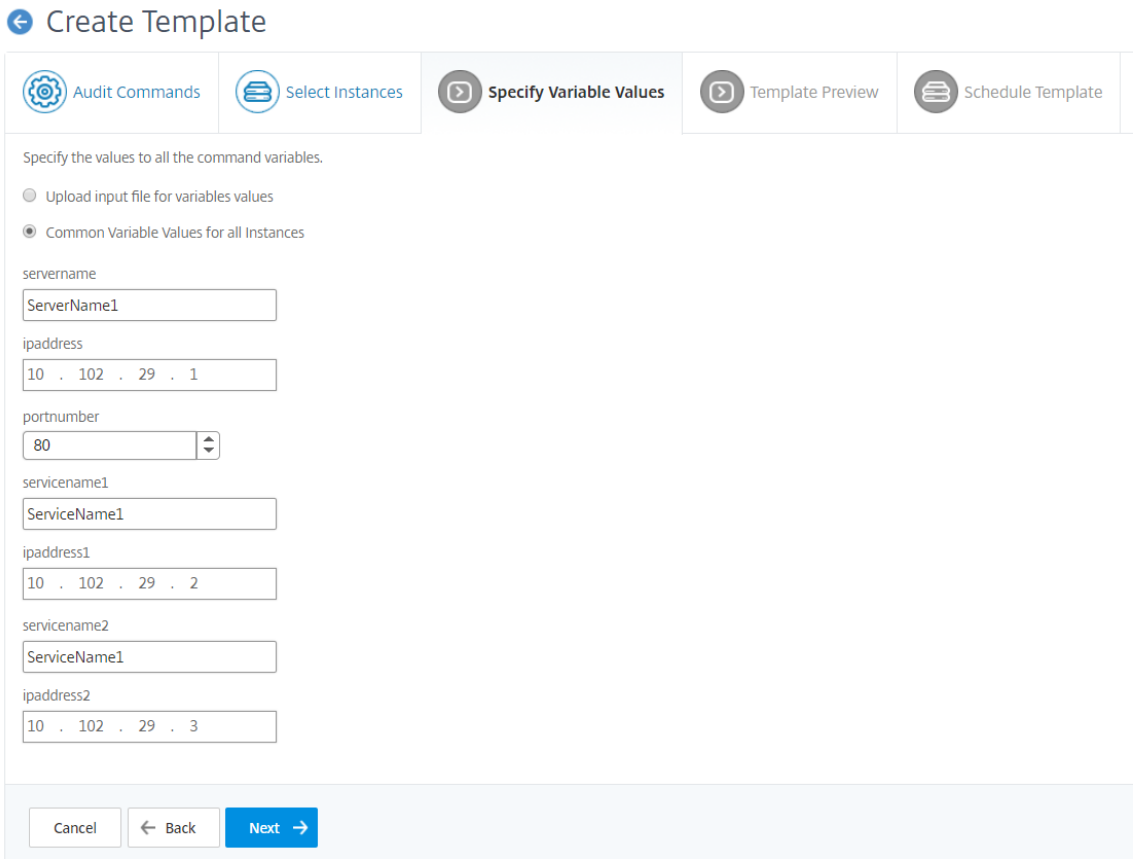


7. Auf der Registerkarte **Variablenwerte angeben** haben Sie zwei Optionen:

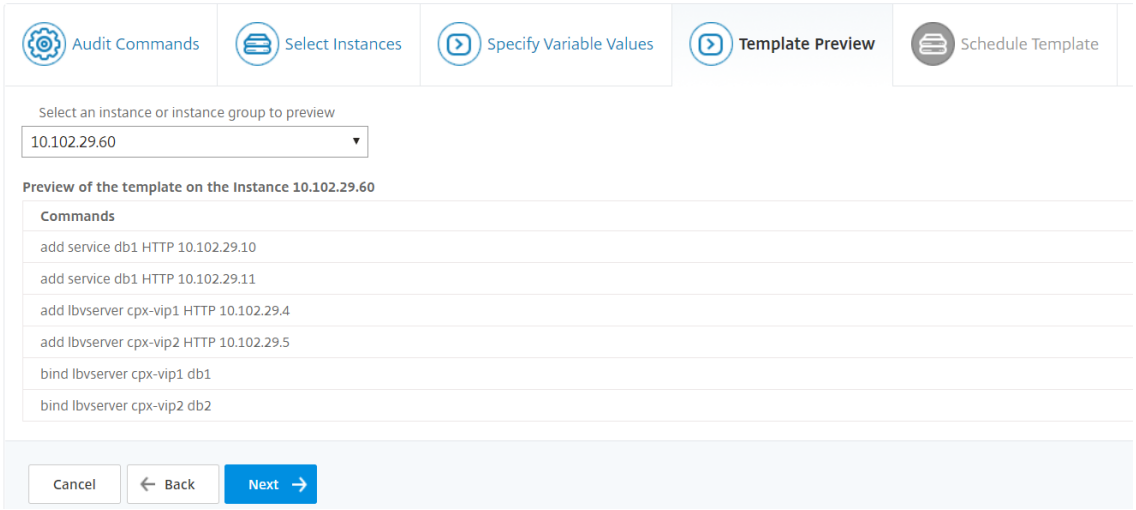
   a) Laden Sie die Eingabedatei herunter, um die Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den Citrix ADM -Server hoch.

   b) Geben Sie allgemeine Werte für die Variablen ein, die Sie für alle Instanzen definiert haben

8. Klicken Sie auf **Weiter**.



9. Auf der Registerkarte **Vorlagenvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen. Klicken Sie auf **Weiter**.



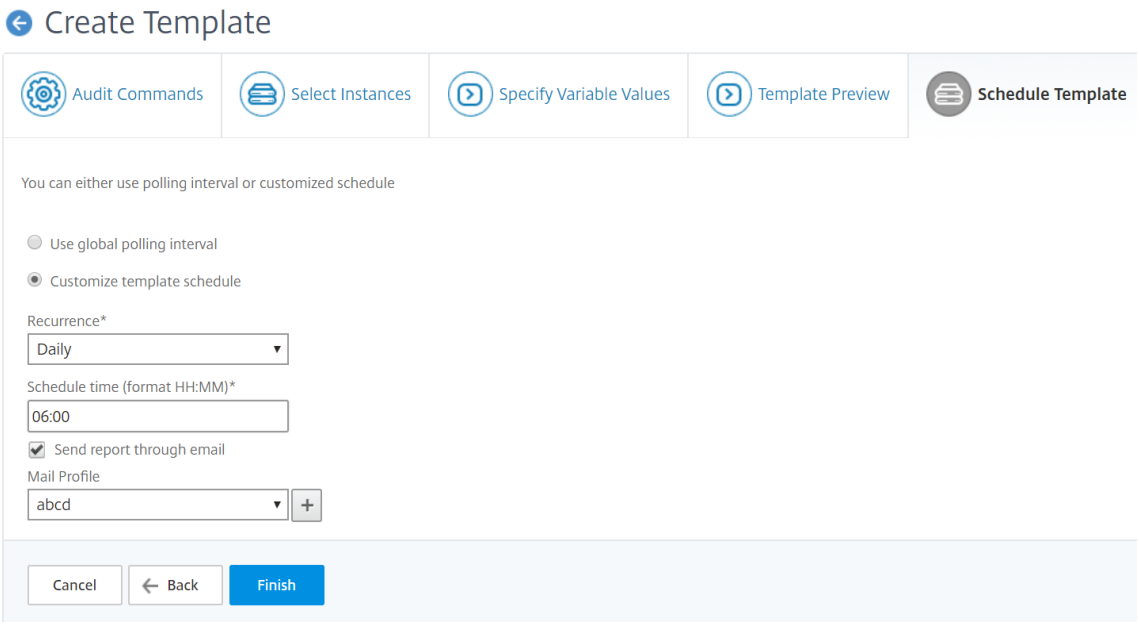
10. Auf der Registerkarte **Vorlage planen** haben Sie die folgenden Optionen, um die Ausführung der Vorlage zu planen und die E-Mail-Adresse so zu konfigurieren, dass der Diff-Bericht gesendet wird.

    - **Verwenden Sie das globale Abrufintervall**. Wählen Sie diese Option aus, um die Vorlage auf den Instanzen zu einem Zeitpunkt auszuführen, der global auf Citrix ADM konfiguriert ist.

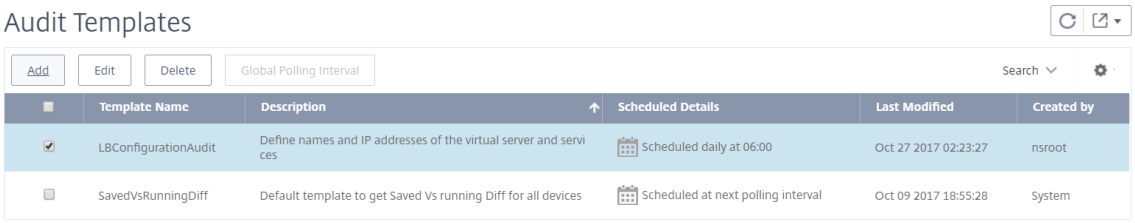
      > **Hinweis:**
      >
      > Um das globale Abrufintervall in Citrix ADM zu konfigurieren, navigieren Sie zu **Netzwerke**> **Konfigurationsüberwachung** > **Überwachungsvorlagen** und klicken Sie auf **Globales Abrufintervall**. Geben Sie im Feld **Abfrageintervall** die Minuten ein, in denen Citrix ADM die Instanzen global abfragen muss.

    - **Anpassen des Vorlagenzeitplans**. Verwenden Sie diese Option, um die Zeit und die Häufigkeit zu konfigurieren, mit der die Vorlagen ausgeführt werden müssen
    - **Bericht per E-Mail senden**. Verwenden Sie diese Option, um das E-Mail-Profil zu konfigurieren, an das der Diff-Bericht als E-Mail-Anhang gesendet werden muss.

11. Klicken Sie auf **Fertig stellen**.



Die Überwachungsvorlage wird in der Liste **Überwachungsvorlagen** angezeigt und zum geplanten Zeitpunkt für die Konfigurationen in den angegebenen Instanzen ausgeführt.



Konfigurationsprüfung von Citrix ADC-Instanzen abfragen

April 28, 2021

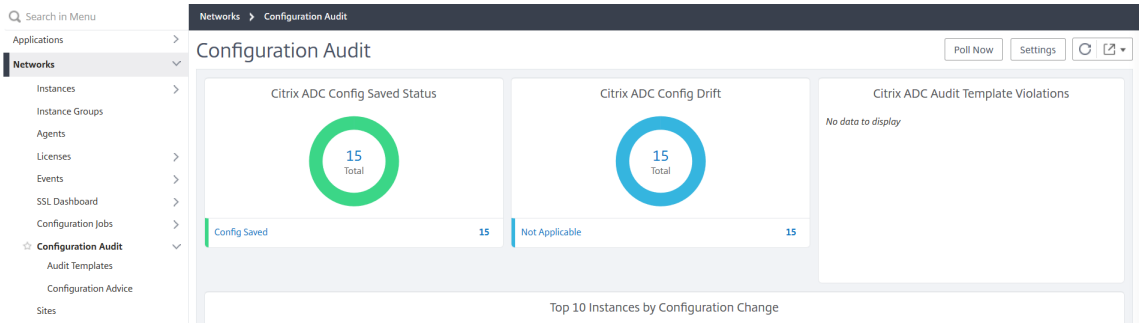
Citrix Application Delivery Management (ADM) fragt die Konfigurationsaudits automatisch alle 10 Stunden ab, um nach Konfigurationsänderungen zu suchen, die auf Citrix ADC-Instanzen auftreten. Sie können die Konfigurationsprüfungen auch manuell abfragen, um die letzten Änderungen zu erkennen. Das Abrufen aller Citrix ADC-Instanzen führt jedoch zu einer hohen Belastung des Netzwerks.

Anstatt die gesamte Konfigurationsüberwachung der Citrix ADC-Instanzen abzufragen, können Sie nur die Konfigurationsaudits einer ausgewählten Instanz oder Instanzen manuell abfragen.

So fragen Sie Konfigurationsaudits von Citrix ADC-Instanzen ab:

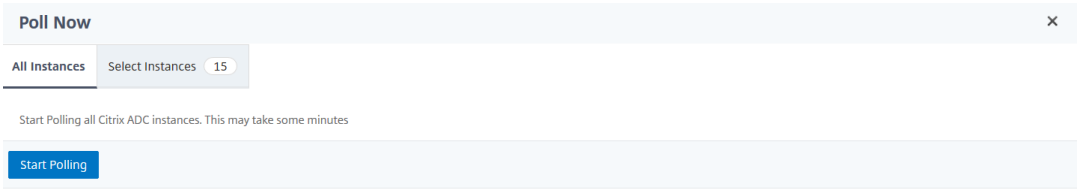
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsüberwachung**.

2. Klicken Sie auf der Seite **Konfigurationsüberwachung** oben rechts auf **Jetzt abfragen**.

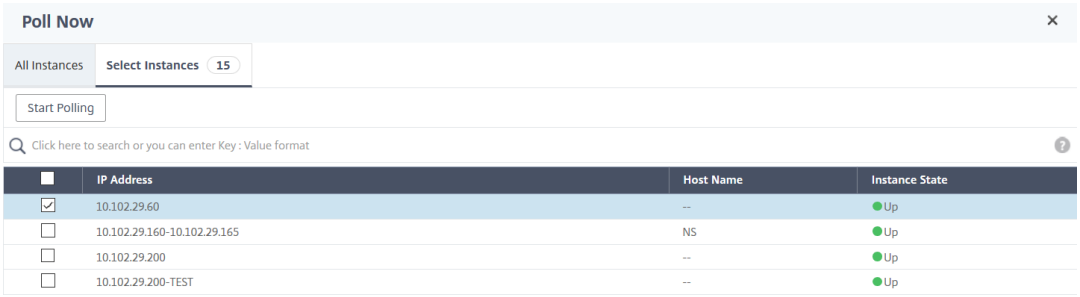


3. Die Seite **Jetzt abfragen** wird geöffnet und bietet Ihnen die Möglichkeit, alle Citrix ADC-Instanzen im Netzwerk abzufragen oder ausgewählte Instanzen abzufragen.

   a) Um alle Citrix ADC-Instanzen abzufragen, wählen Sie die Registerkarte **Alle Instanzen**, und klicken Sie auf **Polling starten**.



   b) Um bestimmte Instanzen abzufragen, wählen Sie die Registerkarte **Instanzen auswählen**, wählen Sie die Instanzen aus der Liste aus und klicken Sie auf **Polling starten**.



Auditberichte anzeigen

April 28, 2021

Mit Citrix Application Delivery Management (ADM) können Sie den Konfigurations-Audit-Diff-Bericht im Abschnitt Konfigurationsprüfung anzeigen und herunterladen. Im Konfigurationsüberwachungsabschnitt können Sie den zusammenfassenden Bericht über alle Instanzen und pro Instanz exportieren. Außerdem können Sie für jedes Instanzvorlagenpaar granulare Diff-Berichte exportieren.

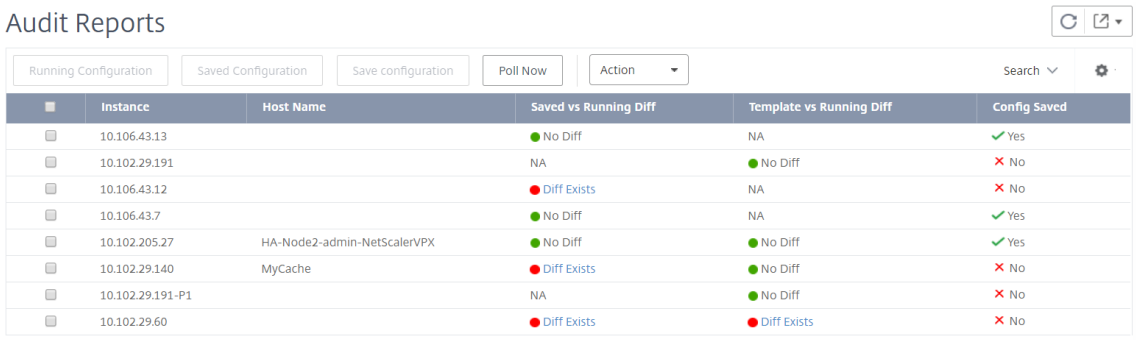
Die Überwachungsvorlagen, die in der Liste Überwachungsvorlagen angezeigt werden, werden zum geplanten Zeitpunkt für die Konfigurationen in den angegebenen Instanzen ausgeführt. Das

Diagramm **Citrix ADC Config Drift** im Dashboard **Configuration Audit** zeigt Details zu Konfigurationsänderungen in gespeicherten Konfigurationen auf hoher Ebene an. Wenn Sie auf das Diagramm **Citrix ADC Config Drift** klicken, zeigt die folgende Seite **Audit Reports** ein Liste der Instanzen, die sowohl “Diff Exists” als auch No Diff” anzeigt. Sie können die von Citrix ADM angezeigten Diff-Berichte herunterladen.

Citrix ADM bietet auch die Option, den automatischen Export von Diff-Bericht als E-Mail-Anlage zu planen. Weitere Informationen zum Planen des Exports von Berichten finden Sie unter Überwachungsvorlagen erstellen.

Exportieren von Konfigurationsüberwachungsberichten

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsüberwachung**.
2. Klicken Sie auf der Seite **Configuration Audit** auf das Diagramm **Citrix ADC Config Drift**.
3. Auf der Seite **Überwachungsberichte** werden Instanzen aufgeführt, die einen Unterschied aufweisen. Auf der Seite wird auch eine Liste der Instanzen angezeigt, die in ihren ausgeführten Konfigurationen keinen Unterschied aufweisen.



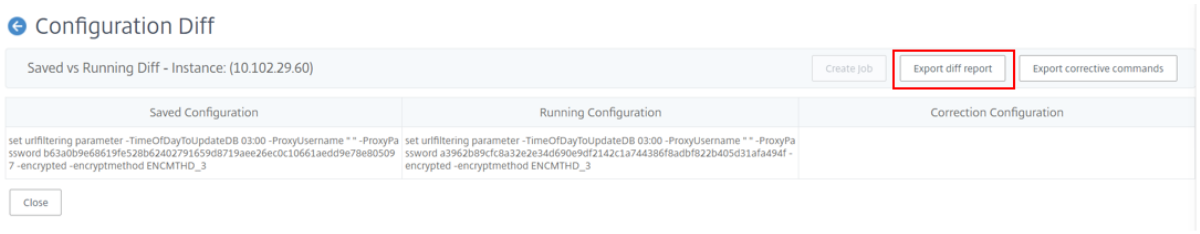
   Im Bild sehen Sie, dass für einige Instanzen ein Diff nur in **Saved Vs Running Diff** vorhanden ist und für einige Instanzen ein Diff nur in **Template vs Running Diff** vorhanden ist. In einigen Fällen gibt es Unterschiede sowohl in **Gespeicherte Vs Running Diff** als auch in **Template vs Running Diff**.

Gespeichert im Vergleich zum Ausführen von Diff:

Sie können einen Bericht über den Unterschied zwischen der auf der Instanz gespeicherten Konfiguration und der derzeit auf dieser Instanz ausgeführten Konfiguration anzeigen. Klicken Sie z. B. für eine Instanz unter **Gespeicherte Vs laufende Diff** auf **Diff existiert**.

Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		No Diff	NA	Yes
10.102.29.191		NA	No Diff	No
10.106.43.12		Diff Exists	NA	No
10.106.43.7		No Diff	NA	Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
10.102.29.140	MyCache	Diff Exists	No Diff	No
10.102.29.191-P1		NA	No Diff	No
10.102.29.60		Diff Exists	Diff Exists	No

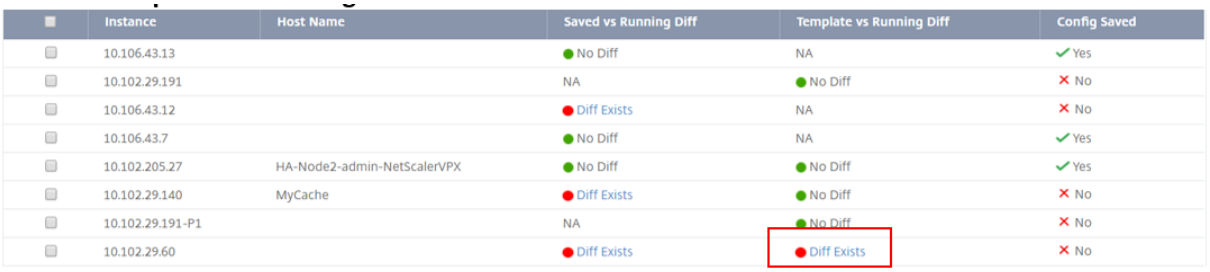
Hier sehen Sie einen Bericht für die gespeicherte Konfiguration gegen den laufenden Konfigurations-diff für diese Instanz.



Klicken Sie auf **Diff-Bericht exportieren**, um eine CSV-Datei des Diff-Berichts herunterzuladen. Sie können auch auf **Korrekturbefehle exportieren** klicken, um die Befehle in eine TXT-Datei zu exportieren. Anschließend können Sie die Befehle für die zugeordnete Citrix ADC-Instanz aus Konfigurationsaufträgen ausführen, um die Konfiguration in dieser Instanz zu korrigieren.

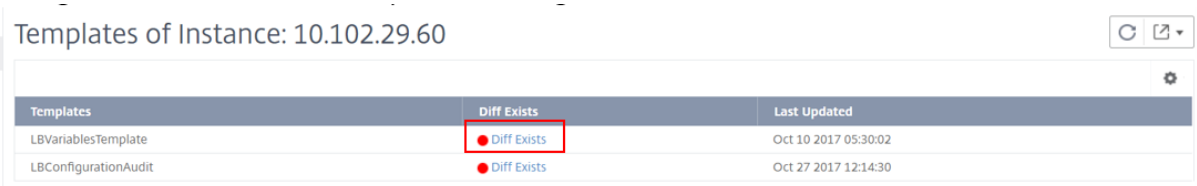
Vorlage vs Ausführen von Diff:

Die **Vorlage vs Running Diff** enthält alle Vorlagen außer **Saved Vs Running Diff**, die die Standardvorlage ist. Sie können den Unterschied zwischen der Vorlage und der laufenden Konfiguration anzeigen. Klicken Sie z. B. auf **Diff Existiert** für eine der Instanzen unter **Vorlage vs Laufendes Diff**.



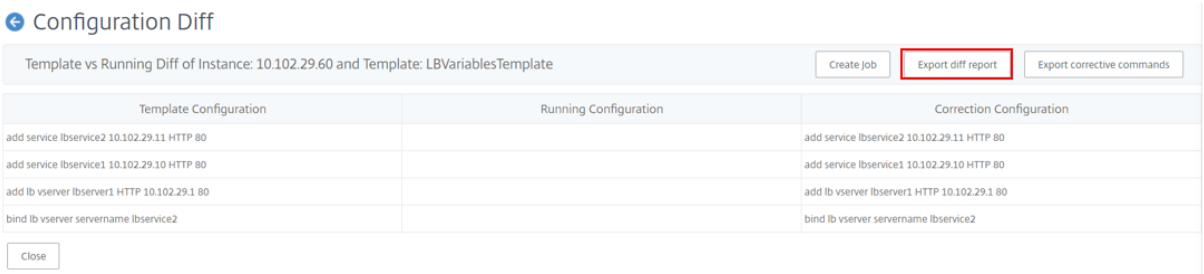
Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		No Diff	NA	Yes
10.102.29.191		NA	No Diff	No
10.106.43.12		Diff Exists	NA	No
10.106.43.7		No Diff	NA	Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
10.102.29.140	MyCache	Diff Exists	No Diff	No
10.102.29.191-P1		NA	No Diff	No
10.102.29.60		Diff Exists	Diff Exists	No

Jetzt können Sie sehen, dass zwei Vorlagen Diff anzeigen und die Citrix ADC-Instanz eine andere Konfiguration hat als die von der Vorlage gesucht wird.



Klicken Sie erneut auf **Diff Existiert**. Das folgende Bild zeigt die Konfiguration, nach der die Vorlage

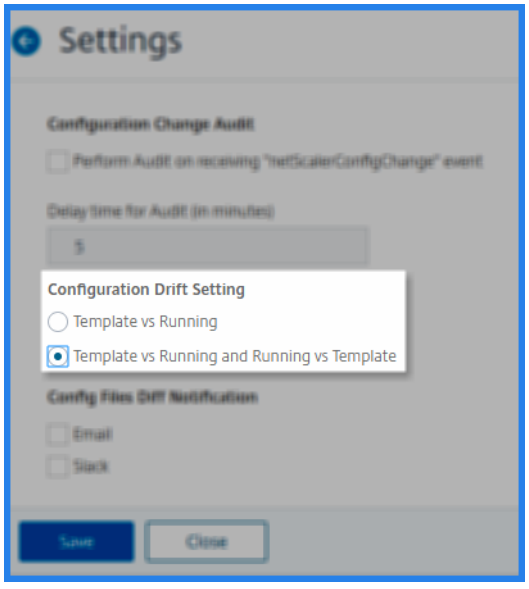
sucht, und die ausgeführte Konfiguration, die leer ist, da keine derartigen Befehle konfiguriert wurden oder entfernt wurden. Sie können auch die Korrekturkonfigurationen oder die Befehle sehen, die ausgeführt werden sollen, um die Konfiguration zu korrigieren.



Sie können auch die Einstellung Template vs Running und Running vs Template Drift verwenden, um die Konfiguration auf beiden Arten zu vergleichen:

- Vergleicht die Konfiguration der Überwachungsvorlagen mit der laufenden Konfiguration auf der Instanz.
- Vergleicht die laufende Konfiguration auf der Instanz mit der Überwachungsvorlage.

Standardmäßig ist die Einstellung “Template vs. running drift” ausgewählt. Um die Drift-Einstellung zu ändern, wählen Sie in der ADM-GUI **Einstellungen** auf der Seite **Configuration Audit (Konfigurationsüberwachung**).



Klicken Sie auf **Diff-Bericht exportieren**, um eine CSV-Datei des Diff-Berichts herunterzuladen. Sie können auch auf **Korrekturbefehle exportieren** klicken, um die Befehle in eine TXT-Datei zu exportieren. Anschließend können Sie die Befehle in CLI ausführen, um die Konfiguration in dieser Instanz zu korrigieren.

Das folgende Bild zeigt eine CSV-Beispieldatei, die auf Ihr System heruntergeladen wird:

#Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate		
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lbserver1 HTTP 10.102.29.1 80		add lb vserver lbserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

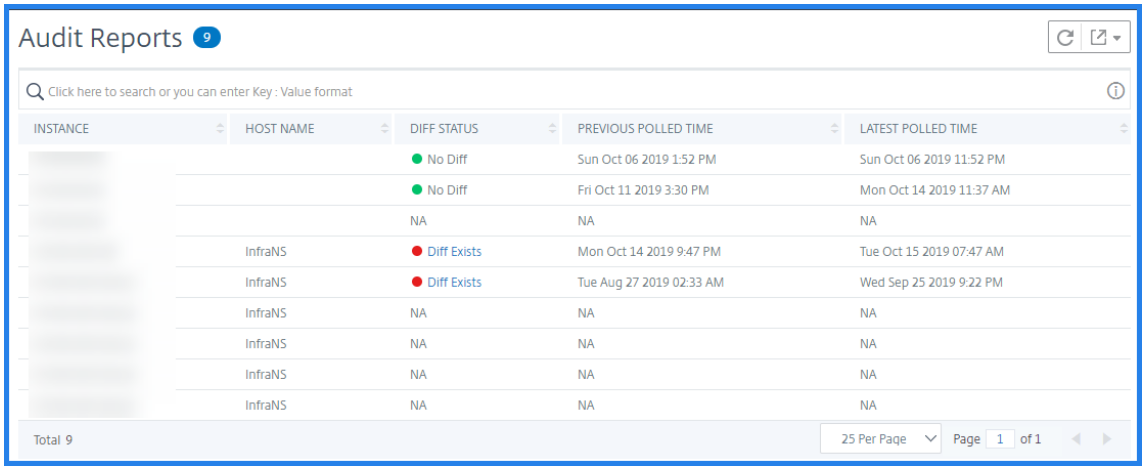
Anzeigen der Dateistatus-Überwachungsberichte

Mit dem **Citrix ADC File Statusdiagramm** können Sie überwachen, ob Dateien im `nsconfig` Ordner hinzugefügt, geändert oder entfernt werden. Beispiel: Wenn die Lizenzdatei auf einer ADC-Instanz aktualisiert wird, können Sie überprüfen, wann diese Datei zuletzt aktualisiert wurde, und entsprechende Maßnahmen ergreifen.

So exportieren Sie die Dateistatus-Überwachungsberichte für die Citrix ADC-Instanzen:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsüberwachung**.
2. Klicken Sie auf der Seite **Konfigurationsüberwachung** auf das Diagramm **Citrix ADC Dateistatus**.

   Auf der Seite **Überwachungsberichte** werden Instanzen mit dem Status Diff aufgelistet.



   Der **Diff-Status** wird für das Intervall zwischen der **vorherigen Abrufzeit** und der **letzten Abrufzeit** berechnet. Der **Diff-Status** kann einer der folgenden sein:

   - **Diff existiert** - Dieser Status gibt an, dass sich die Dateien im`nsconfig` Ordner einer Instanz seit der **vorherigen Abrufzeit geändert** haben. Um die Änderungen an der Datei anzuzeigen, klicken Sie auf **Diff Existiert**.

     ! [Diff existiert im `nsconfig` Ordner] (/en-us/citrix-application-delivery-management-service/media/config-audit-file-status-diff.png)

   - **Kein Diff** - Dieser Status zeigt an, dass sich die Dateien im`nsconfig` Ordner seit der vorherigen Abfragezeit nicht geändert haben.

- **NA** - Dieser Status zeigt an, dass die Überwachung des Dateistatus nicht anwendbar ist. Dieser Status wird angezeigt, wenn Citrix ADM die Instanz nicht abfragen. Wenn beispielsweise eine Instanz neu hinzugefügt wird oder der Instanzstatus inaktiv ist, findet die Abfrage der Instanz nicht statt.

Exportieren des Berichts dieses Dashboards

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. So planen Sie den Bericht täglich, wöchentlich oder monatlich und senden Sie den Bericht per E-Mail oder Puffernachricht.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Konfigurations-Audit-Diff für ConfigChange SNMP-Traps generieren

April 28, 2021

Wenn eine Konfigurationsänderung in einer Citrix ADC-Instanz im Netzwerk erfolgt, wird die Konfigurationsdatei aktualisiert. Die Instanz sendet ein ConfigChange SNMP-Trap an Citrix Application Delivery Management (ADM). Sie können Citrix ADM aktivieren, um eine Konfigurationsüberwachung für diese Instanz durchzuführen, wenn die Instanz ein ConfigChange-SNMP-Trap sendet.

Wenn ein Unterschied zwischen der Konfiguration der Überwachungsvorlage und der laufenden Konfiguration besteht, wird auf der Seite Überwachungsbericht eine Statusmeldung “Diff Existiert “ angezeigt. Wenn Sie auf den Link “ Diff beendet “ klicken, gelangen Sie zur Seite “ Konfigurationsdiff “, auf der Sie den Korrekturbefehl anzeigen können. Sie können diese fehlerbehebenden Befehle verwenden, um einen Konfigurationsauftrag zu erstellen und diesen auf den spezifischen Citrix ADC-Instanzen auszuführen. Wenn Sie den Konfigurationsauftrag ausführen, werden die Instanzen zur gewünschten Konfiguration zurückgesetzt. Weitere Informationen zum Erstellen von Konfigurationsaufträgen aus Korrekturbefehlen finden Sie unter Erstellen von Konfigurationsaufträgen aus Korrekturbefehlen in Citrix ADM.

So führen Sie Konfigurationsüberwachungsvorlagen beim Empfang von ConfigChange SNMP-Trap aus:

Mit Citrix ADM können Sie die Option zum Ausführen der Konfigurationsüberwachungsvorlage in Citrix ADM aktivieren.

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsüberwachung**.
2. Klicken Sie auf der Seite **Konfigurationsüberwachung** auf **Einstellungen**.
3. Klicken Sie im Abschnitt **Überwachungseinstellungen für Konfigurationsänderungen** auf das Symbol Bearbeiten.
4. Aktivieren **Sie das Kontrollkästchen Konfiguration überwachen, wenn NetScalerConfigChange-Ereignis empfangen wird**.

   > **Hinweis**
   >
   > Dies ist eine globale Einstellung für alle Instanzen. Citrix ADM führt eine Konfigurationsüberwachung für jede Instanz durch, die NetScalerConfigChange SNMP-Traps in Zukunft empfängt.

5. Geben Sie im Feld **Zeitverzögerung für die Ausführung der Überwachungsvorlage (in Minuten)** die Minuten ein. Citrix ADM führt die Konfigurationsüberwachungsvorlage auf der Citrix ADC-Instanz nach dieser Zeitverzögerung aus, wenn sie das ConfigChange-SNMP-Trap von dieser Instanz empfängt.

Überwachen von Konfigurationsänderungen über alle Instanzen hinweg

April 28, 2021

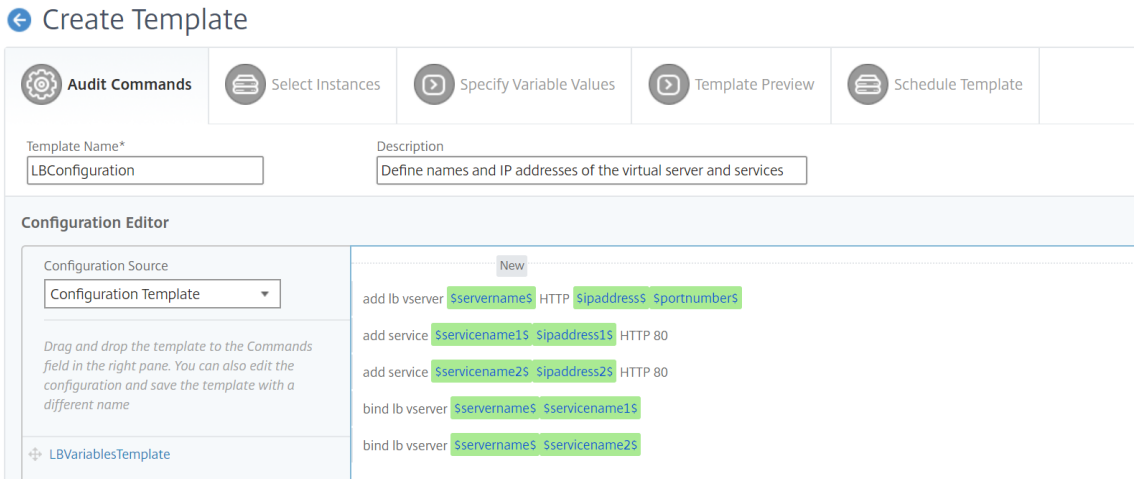
Sie möchten sicherstellen, dass bestimmte Konfigurationen auf bestimmten Instanzen ausgeführt werden, um die optimale Leistung Ihres Netzwerks zu gewährleisten. Außerdem möchten Sie Konfigurationsänderungen über verwaltete Citrix ADC-Instanzen hinweg überwachen, Konfigurationsfehler beheben und nicht gespeicherte Konfigurationen nach einem plötzlichen Herunterfahren des Systems wiederherstellen. Sie können Überwachungsvorlagen mit bestimmten Konfigurationen erstellen, die Sie auf bestimmten Instanzen ausführen möchten. Das Citrix Application Delivery Management (ADM) vergleicht diese Instanzen mit der Überwachungsvorlage und den Berichten, wenn die Konfiguration nicht übereinstimmt. Dieser Vergleich ermöglicht es Ihnen, die Fehler zu beheben und zu beheben.

Sie können die Ausführung der Prüfungsvorlage automatisieren, indem Sie den Zeitpunkt planen, zu dem die Vorlage ausgeführt werden muss. Sie können auch festlegen, mit welcher Häufigkeit Citrix ADM die Vorlage ausführen muss. Sie können die Vorlage täglich, an einem bestimmten Tag in einer

Woche oder an einem bestimmten Datum in einem Monat ausführen. Sie können den von Citrix ADM erstellten Diff-Bericht auch an die angegebenen E-Mail-Adressen senden, die Sie konfigurieren können. Mit dieser Option erhält der Benutzer den Bericht als E-Mail-Anlage, und der Benutzer muss sich nicht bei Citrix ADM anmelden, um die Berichte manuell zu überprüfen.

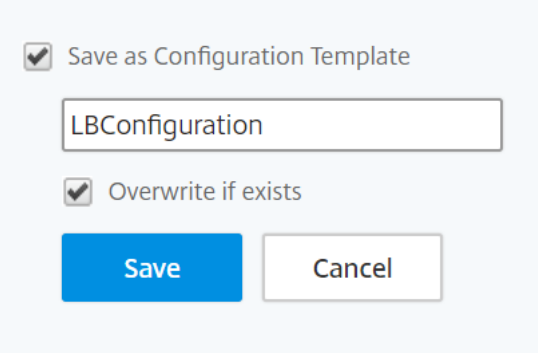
So erstellen Sie Überwachungsvorlagen:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsüberwachung** > **Überwachungsvorlagen**, und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Vorlage erstellen** und auf der Registerkarte **Überwachungsbefehle** den Vorlagennamen und die Beschreibung an.
3. Geben Sie im **Konfigurationseditor**Ihre Befehle ein, und speichern Sie die Befehle als Konfigurationsvorlage. Sie können auch eine vorhandene Vorlage aus dem linken Bereich des Editors ziehen.
4. Wählen Sie die Werte aus, die Sie in eine Variable konvertieren möchten, und klicken Sie dann auf **In Variable konvertieren**. Wählen Sie beispielsweise die IP-Adresse des Load Balancing-Servers aus `ipaddress` und klicken Sie auf In **Variable umwandeln**, wie in der folgenden Abbildung gezeigt.

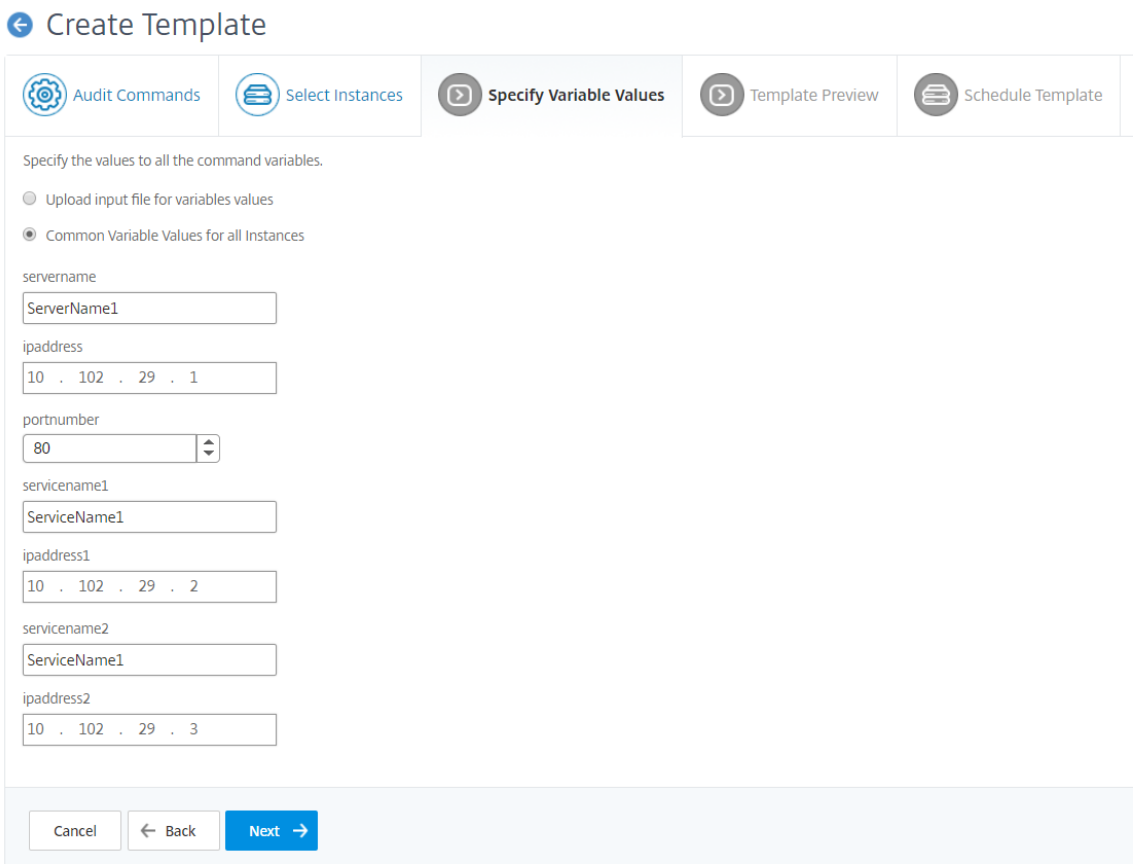


Klicken Sie auf die Option **Erweitert**, wenn Sie einen Standardwert für Ihre Variable weiter angeben möchten.

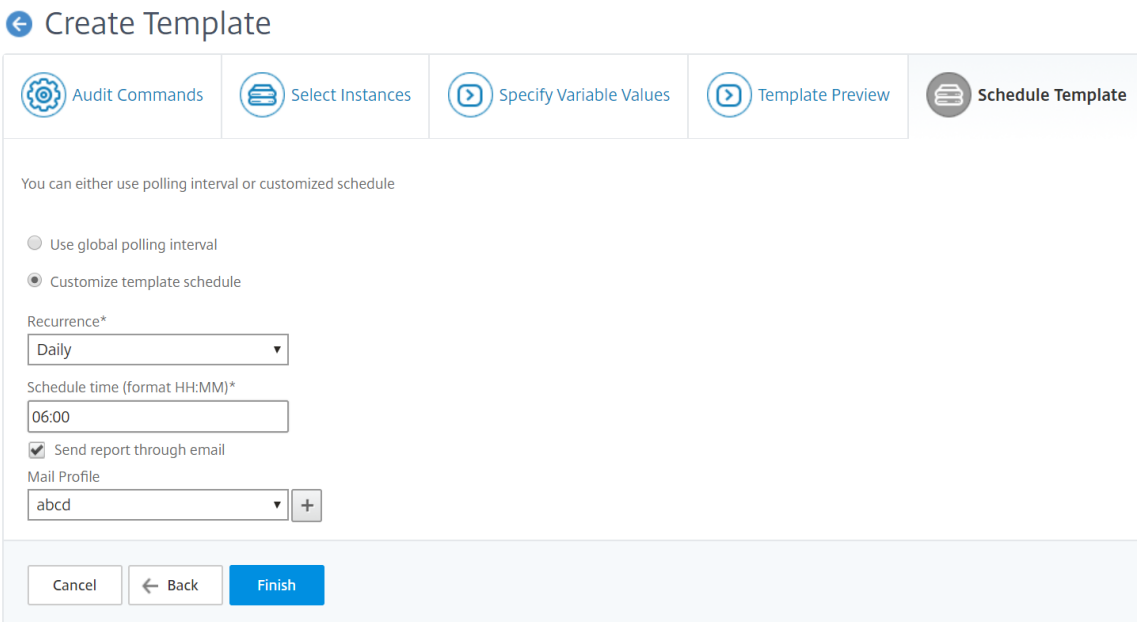
Sie können die Befehle auch als Konfigurationsvorlage speichern.



5. Klicken Sie auf **Speichern**, und klicken Sie dann auf **Weiter**.
6. **Wählen Sie auf der Registerkarte Instanzen auswählen** die Instanzen aus, für die die Konfigurationsüberwachung ausgeführt werden soll.
7. Auf der Registerkarte **Variablenwerte angeben** haben Sie zwei Optionen:
   a) Laden Sie die Eingabedatei herunter, um die Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den Citrix ADM -Server hoch.
   b) Geben Sie allgemeine Werte für die Variablen ein, die Sie für alle Instanzen definiert haben
8. Klicken Sie auf **Weiter**.



9. Auf der Registerkarte **Vorlagenvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen. Klicken Sie auf **Weiter**.
10. Auf der Registerkarte **Vorlage planen** haben Sie drei Optionen, um die Ausführung der Vorlage zu automatisieren und die E-Mail-Adresse, um den Diff-Bericht zu senden.
    - **Verwenden Sie das globale Abrufintervall**. Wählen Sie diese Option aus, um die Vorlage auf den Instanzen zu einem Zeitpunkt auszuführen, der global auf Citrix ADM konfiguriert ist.
    - **Anpassen des Vorlagenzeitplans**. Verwenden Sie diese Option, um die Zeit und die Häufigkeit zu konfigurieren, mit der die Vorlagen ausgeführt werden müssen
    - **Senden Sie den Bericht per E-Mail**. Verwenden Sie diese Option, um das E-Mail-Profil zu konfigurieren, an das der Diff-Bericht als E-Mail-Anhang gesendet werden muss.
11. Klicken Sie auf **Fertig stellen**.



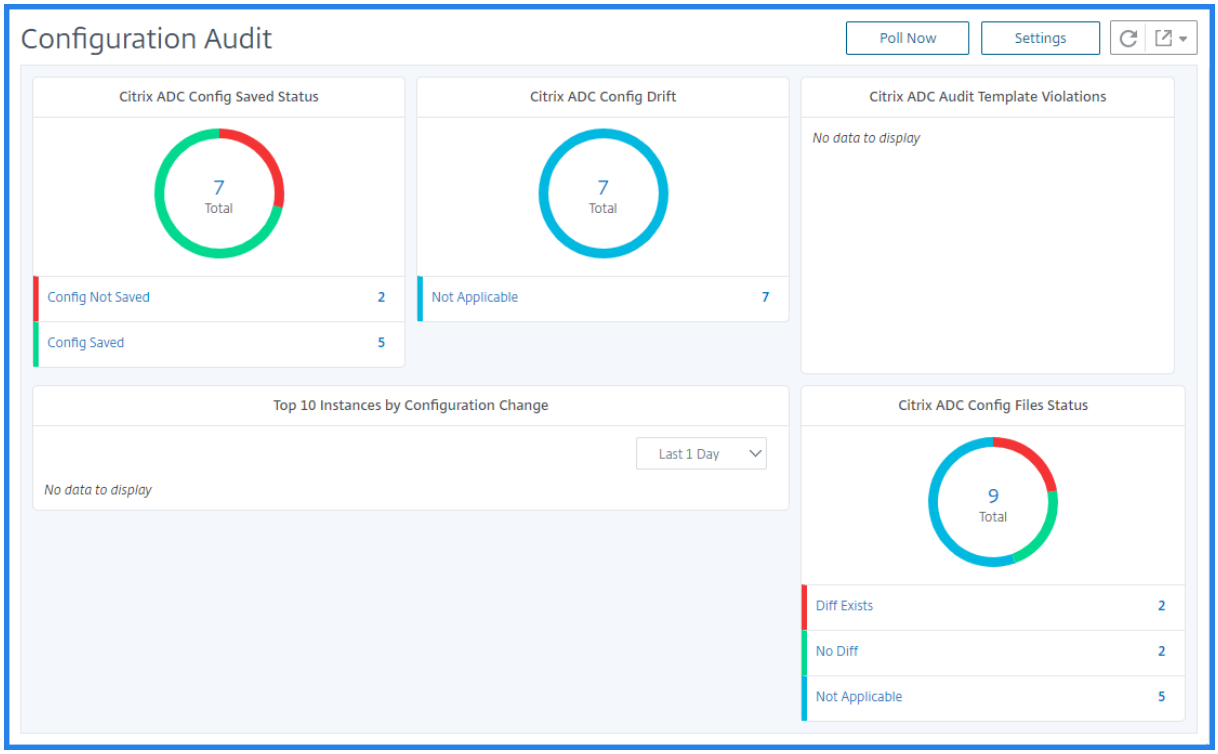
Die Überwachungsvorlage wird in der Liste Überwachungsvorlagen angezeigt und zum geplanten Zeitpunkt für die Konfigurationen in den angegebenen Instanzen ausgeführt.

Details zu Konfigurationsänderungen anzeigen

Sie können das Dashboard Configuration Audit auch verwenden, um Details zu Konfigurationsänderungen auf hoher Ebene anzuzeigen, z. B.:

- Die 10 besten Instanzen durch Konfigurationsänderung
- Die Anzahl der gespeicherten und nicht gespeicherten Konfigurationen

- Die im`nsconfig` Ordner hinzugefügte, entfernte oder geänderte Datei

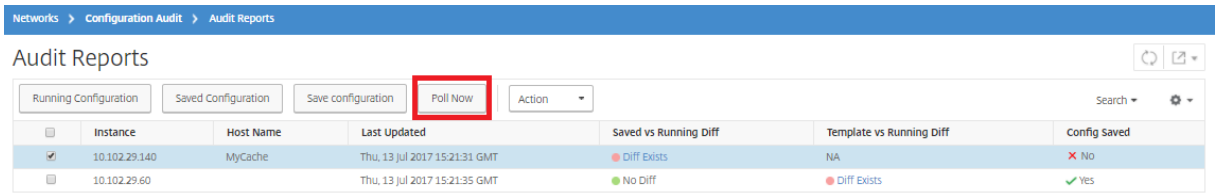


Mit Citrix ADM können Sie Konfigurationsaudits manuell abfragen und alle Konfigurationsaudits der Instanzen sofort dem Citrix ADM hinzufügen. Navigieren Sie dazu zu **Netzwerke** > **Konfigurationsüberwachung,** klicken Sie auf **Jetzt abfragen**. Auf der **Popupseite Jetzt** abfragen können Sie alle Citrix ADC-Instanzen im Netzwerk abfragen oder die ausgewählten Instanzen abfragen.

Sie können auch eine Prüfung für eine Instanz erzwingen. Klicken Sie dazu auf eines der folgenden Diagramme:

- **Status der gespeicherten Citrix ADC Konfiguration**
- **Citrix ADC Konfigurationsdrift**

Wählen Sie auf der Seite **Überwachungsberichte** die Instanz aus, und wählen Sie in der Liste **Aktion** die Option **Jetzt abfragen** aus.

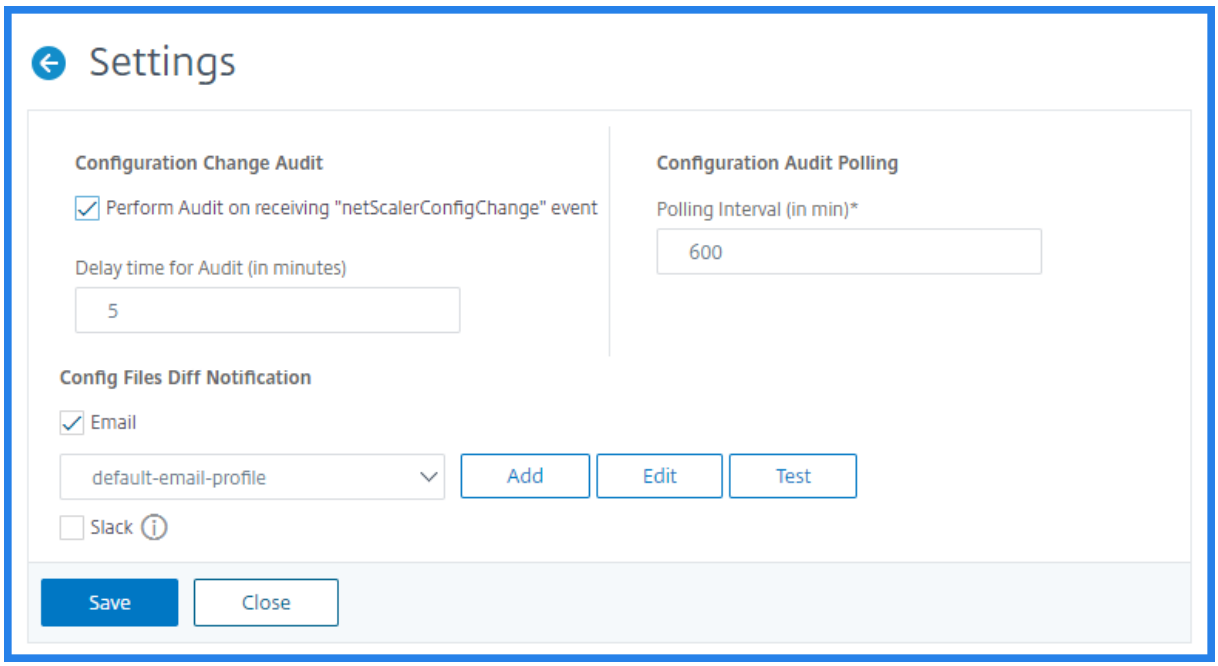


Das Diagramm **Status der Citrix ADC Konfigurationsdatei** enthält den Status der Citrix ADC Dateien, die im`nsconfig` Ordner vorhanden sind. Citrix ADM zeichnet Änderungen in Dateien innerhalb des Ordners `nsconfig`auf und vergleicht diese und zeigt die Unterschiede an. Siehe Anzeigen der Dateistatus-Überwachungsberichte.

Konfigurationsüberwachungsbenachrichtigungen festlegen

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsüberwachung**.
2. Klicken Sie auf der Seite **Konfigurationsüberwachung** auf **Einstellungen**.
3. Auf der Seite **Einstellungen**:
   a) Aktivieren Sie das Kontrollkästchen **Prüfung beim Empfang des Ereignisses NetScaler-ConfigChange durchführen**, um die Benachrichtigungseinstellungen zu aktivieren.
   b) Legen Sie die Verzögerungszeit für Überwachung fest.
4. Legen Sie unter **Configuration Audit Polling**das **Abrufintervall fest**.

   Citrix ADM fragt die Konfigurationsprüfungsereignisse für das angegebene Abrufintervall ab.
5. Wählen Sie unter **Konfigurationsdatei-Diff-Benachrichtigung**die Plattform aus, auf der Sie die Benachrichtigungen erhalten möchten:
   - **E-Mail** - Wählen Sie die E-Mail-Verteilerliste aus. Klicken Sie auf Hinzufügen, um eine E-Mail-Verteilerliste hinzuzufügen, um Benachrichtigungen zu erhalten.
   - **Slack** - Wählen Sie den Slack Kanal aus der Liste aus. Klicken Sie auf Hinzufügen, um einen Kanal für Benachrichtigungen hinzuzufügen.



Erhalten Sie Konfigurationshinweise zur Netzwerkkonfiguration

April 28, 2021

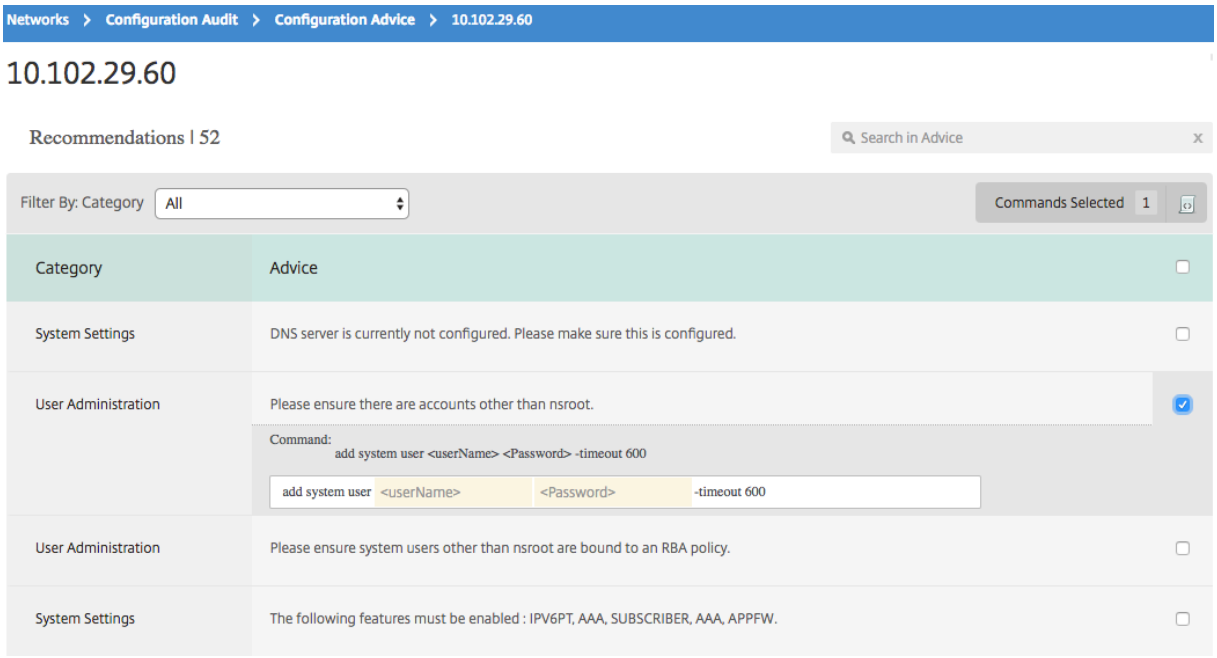
Sie richten Ihre Citrix ADC-Instanzen mit optimalen Konfigurationen ein, damit Sie eine optimale Leistung für Ihre Anwendungen erzielen können. Es ist jedoch möglich, dass es sich bei einigen Konfigurationen möglicherweise nicht um Standardkonfigurationen handelt, die sich auf die Leistung Ihrer Anwendungen auswirken.

Um die Anwendungsleistung zu optimieren, analysiert Citrix Application Delivery Management (ADM) die Citrix ADC-Instanzkonfiguration und gibt Empfehlungen. Sie können die empfohlenen Konfigurationen von Citrix ADM anwenden.

So analysieren Sie die Citrix ADC-Instanz:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsüberwachung** > **Konfigurationshinweise**.
2. Führen Sie einen der folgenden Schritte aus:
    - Klicken Sie auf **Konfigurationsdatei hochladen**, und laden Sie die Konfigurationsdatei Ihrer Netzwerkinstanz hoch.
    - Klicken **Sie auf Gerät** auswählen, und wählen Sie die Citrix ADC-Instanz aus, die Sie analysieren möchten.

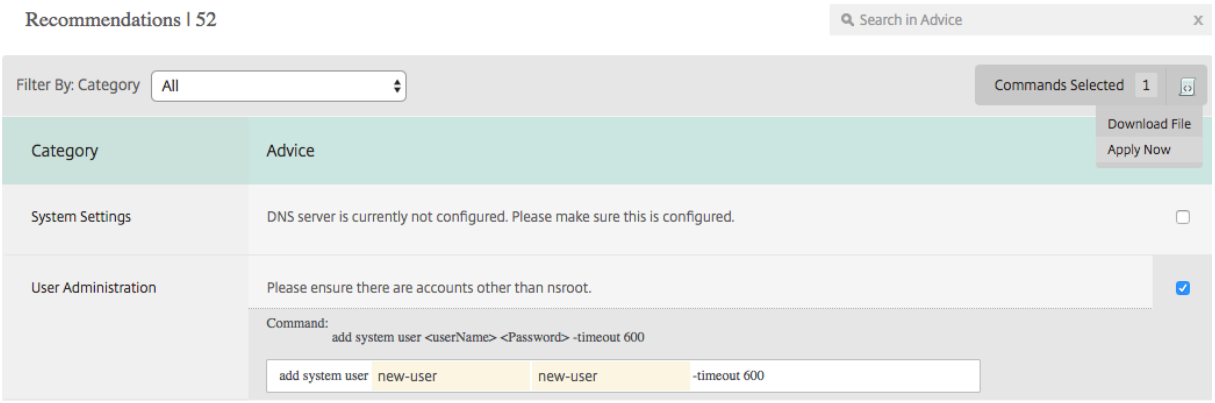
Citrix ADM analysiert die Konfiguration auf Ihrer Instanz und stellt eine Liste von Konfigurationsempfehlungen bereit, wie in der folgenden Abbildung dargestellt. Aktivieren Sie das Kontrollkästchen neben einer Konfigurationsempfehlung, um die Korrekturbefehle anzuzeigen.



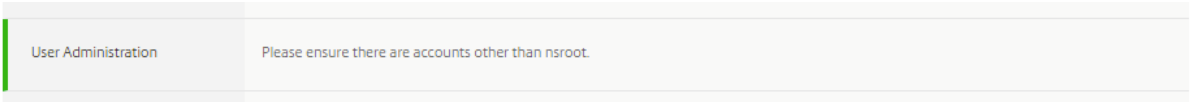
Wenn Sie Ihre Konfiguration aktualisieren möchten, geben Sie die Werte für die Variablen in den Korrekturbefehlen an und klicken Sie auf **Jetzt anwenden**, wie in der folgenden Abbildung gezeigt.

> **Hinweis:**
>
> Die hier aufgeführten Befehle sind nur Empfehlungen. Ein Benutzer mit Lese- und Schreibzugriff kann unter Umständen beliebige Befehle mit dieser Funktion bearbeiten. Stellen Sie sicher, dass Sie Benutzern einen eingeschränkten privilegierten Zugriff gewähren, von denen Sie glauben, dass sie die Befehle nicht bearbeiten dürfen.

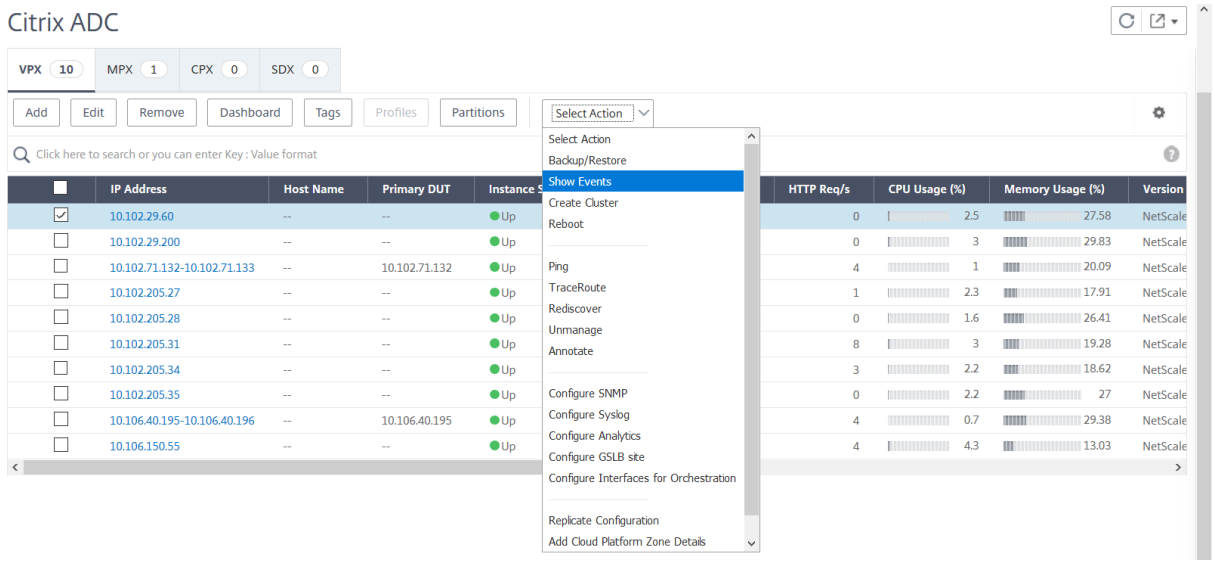
10.102.29.60



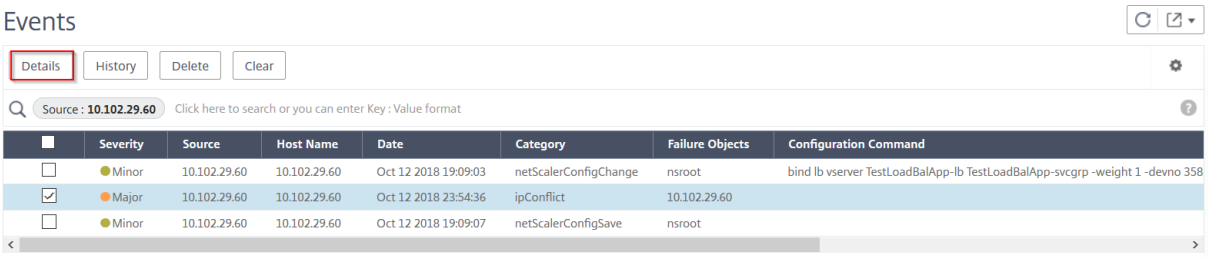
Wenn der Befehl auf der Netzwerkinstanz erfolgreich ausgeführt wird, wird das Kontrollkästchen neben dem Hinweis ausgeblendet.



Wenn Sie die Details der Befehle anzeigen möchten, die auf Ihrer Netzwerkinstanz ausgeführt werden, navigieren Sie zu **Netzwerke** > **Instanzen** > **<Instanztyp>**, wählen Sie die IP-Adresse der Instanz aus, und klicken Sie dann in der Dropdownliste **Aktionen auswählen** auf **Ereignisse anzeigen**.



Auf der Seite **Ereignisse** können Sie die Details der Konfigurationsänderung anzeigen.



Netzwerkfunktionen

April 28, 2021

Mithilfe der Funktion Netzwerkfunktionen können Sie den Status der Entitäten überwachen, die auf Ihren verwalteten Citrix Application Delivery Controller (Citrix ADC) -Instanzen konfiguriert sind. Sie können Statistiken wie Transaktionsdetails, Verbindungsdetails und Durchsatz eines virtuellen Lastausgleichsservers anzeigen. Sie können die Entitäten auch aktivieren oder deaktivieren, wenn Sie eine Wartung planen.

Das Dashboard Netzwerkfunktionen stellt Ihnen folgende Diagramme zur Verfügung:

- Top 5 virtuelle Server mit höchsten Clientverbindungen
- Top 5 virtuelle Server mit höchsten Serververbindungen
- Top 5 virtuelle Server mit maximalem Durchsatz (MB/s)
- Die unteren 5 virtuellen Server mit niedrigem Durchsatz (MB/s)
- Top 5 Instanzen mit den meisten virtuellen Servern
- Status der virtuellen Server
- Zustand der virtuellen Server mit Lastenausgleich
- Protokolle
- Load Balancing-Methode
- Load Balancing-Persistenz
- Top 5 HAProxy-Instanzen mit den meisten Frontends
- Top 5 HAProxy-Instanzen mit den meisten Servern

Erstellen von Berichten für Lastausgleichseinheiten

April 28, 2021

Mit Citrix Application Delivery Management (Citrix ADM) können Sie die Berichte von Citrix Application Delivery Controller (Citrix ADC) Instanzentitäten auf allen Ebenen anzeigen. Es gibt zwei Arten von Berichten, die Sie **unter Citrix ADM > Netzwerkfunktionen** herunterladen können: konsolidierte Berichte und einzelne Berichte.

Konsolidierte Berichte: Sie können einen konsolidierten oder zusammenfassenden Bericht für alle Entitäten herunterladen und anzeigen, die auf Citrix ADC-Instanzen verwaltet werden.

Mit diesem Bericht erhalten Sie einen Überblick über die Zuordnung zwischen den Citrix ADC-Instanzen, Partitionen und den entsprechenden Lastausgleichseinheiten (virtuelle Server, Dienstgruppen und Dienste), die im Netzwerk vorhanden sind.

Die folgende Abbildung zeigt ein Beispiel für einen zusammengefassten Bericht.

Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	cs_lb1#0.0.0.0:0		cs_svc1#192.168.4.56:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	cs_lb2#0.0.0.0:0		cs_svc2#192.168.4.57:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s1#192.168.4.51:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s3#192.168.4.53:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s5#192.168.4.55:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s4#192.168.4.54:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s2#192.168.4.52:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	cs_lb3#0.0.0.0:0		cs_svc3#192.168.2.58:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s4#192.168.2.54:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s1#192.168.2.51:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s2#192.168.2.52:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s3#192.168.2.53:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s5#192.168.2.55:80	

Der konsolidierte Bericht hat ein CSV-Format. Die Einträge in jeder Spalte werden wie folgt beschrieben:

- **Citrix ADC IP-Adresse**: IP-Adresse der Citrix ADC-Instanz wird im Bericht angezeigt
- **Citrix ADC Hostname**: Hostname wird im Bericht angezeigt.
- **Partition**: IP-Adresse der administrativen Partition wird angezeigt
- **Virtueller Server**: <name_of_the_virtual_server> #virtual_IP_address:port_number
- **Dienstleistungen**: <name_of_the_service> #service -IP_Adresse:Port_Number
- **Dienstgruppen**: <name_of_service_group> #Server_Member1_IP_Adresse:Port, Server_Member2_IP_Adre
  Server_Member3_IP_Adresse:Port,……..., Server_Membern_IP_Adresse:Port

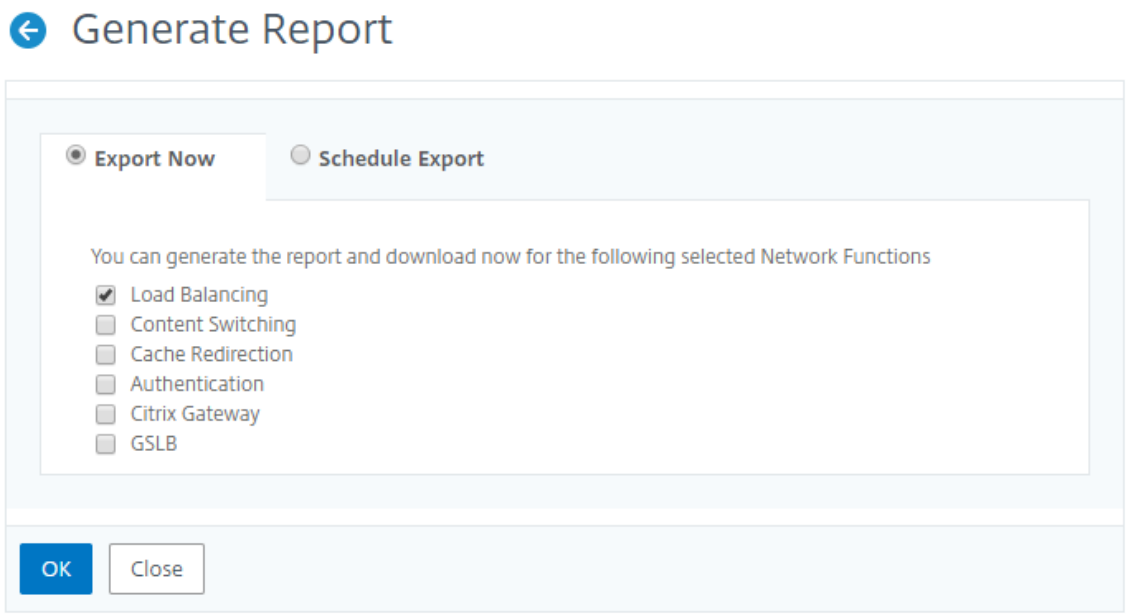
> **Hinweis**
>
> - Ist kein Hostname verfügbar, wird die entsprechende IP-Adresse angezeigt.
> - Leere Spalten geben an, dass die entsprechenden Entitäten für diese Citrix ADC-Instanz nicht konfiguriert sind.

Einzelne Berichte: Sie können auch unabhängige Berichte aller Instanzen und Entitäten herunterladen und anzeigen. Beispielsweise können Sie einen Bericht nur für virtuelle Lastausgleichsserver oder Lastausgleichsdienste oder Lastausgleichsdienstgruppen herunterladen.

Mit Citrix ADM können Sie den Bericht sofort herunterladen. Sie können den Bericht auch einmal am Tag, einmal pro Woche oder einmal im Monat zu einem festen Zeitpunkt erstellen.

Erstellen eines kombinierten Lastausgleichsberichts

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Netzwerkfunktionen**.
2. Klicken Sie auf **Bericht erstellen**.

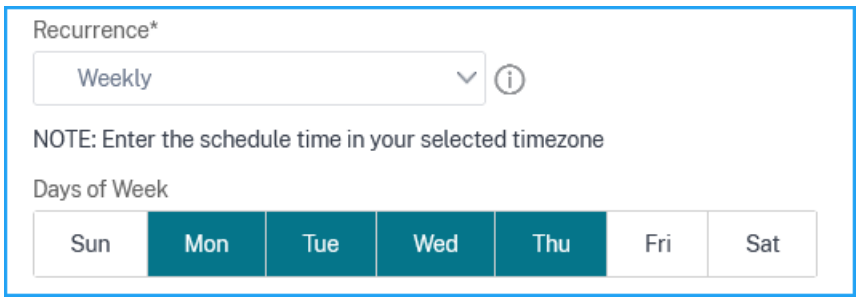


3. Auf der Seite **Bericht generieren**, die geöffnet wird, haben Sie zwei Optionen, um den Bericht anzuzeigen:
   a) Wählen Sie auf der Registerkarte **Jetzt exportieren** die Option **Lastenausgleich** aus, und klicken Sie auf **OK**.

      Der konsolidierte Bericht wird auf Ihr System heruntergeladen.

   b) Wählen Sie **Bericht planen**, um einen Zeitplan für die Erstellung und den Export von Berichten in regelmäßigen Abständen zu erstellen. Geben Sie die Einstellungen für die Berichtsgenerierung an, und erstellen Sie ein E-Mail-Profil, in das der Bericht exportiert wird.
      i. Wählen Sie **Zeitplan aktivieren**aus.
      ii. **Wiederholung** - wählen Sie **Täglich**, **Wöchentlich**oder **Monatlich** aus der Liste aus.

> **Hinweis**
>
> Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.



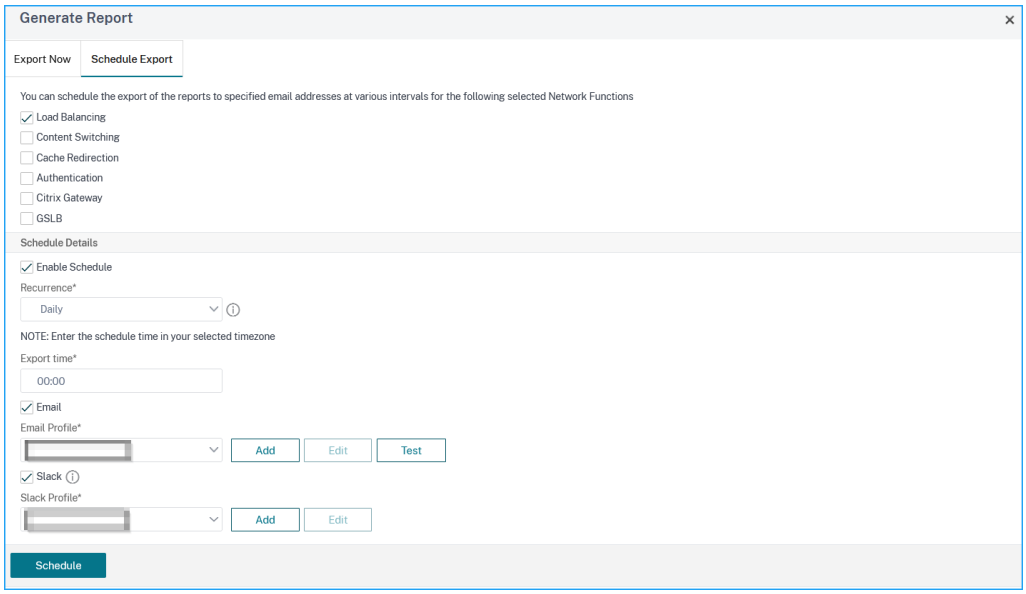
> **Hinweis**
>
> Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie Monatstage mit den Werten zwischen 1 und 31 eingeben.

iii. **Exportzeit** - Geben Sie die Zeit in der Stunde: Minute im 24-Stunden-Format ein.

iv. **E-Mail** - markieren Sie das Kontrollkästchen und wählen Sie dann ein Profil aus der Liste aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

v. **Slack** - Aktivieren Sie das Kontrollkästchen Slack und wählen Sie dann ein Profil aus dem Listenfeld aus oder klicken Sie auf **Hinzufügen**, um ein Slack-Profil zu erstellen.

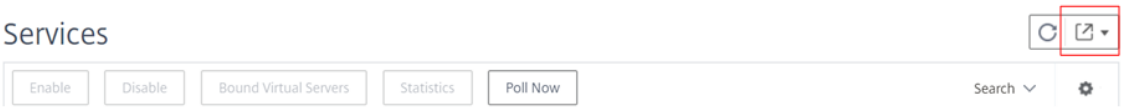
vi. Klicken Sie auf **Zeitplan**, um den Vorgang abzuschließen.



Erstellen eines individuellen Lastausgleichsentitätsberichts

Sie können einen einzelnen Bericht für einen bestimmten Entitätstyp generieren und exportieren, der den Instanzen zugeordnet ist. Betrachten Sie beispielsweise ein Szenario, in dem Sie eine Liste aller Lastausgleichsdienste im Netzwerk anzeigen möchten.

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Netzwerkfunktionen** > **Lastenausgleich** > **Dienste**.
2. Klicken Sie auf der Seite **Dienste** oben rechts auf die Schaltfläche **Exportieren**.



Wählen Sie die Registerkarte **Jetzt exportieren**, wenn Sie den Bericht in diesem Moment generieren und anzeigen möchten.

> **Hinweis**
>
> Sie können die Berichte nur herunterladen oder die Berichte als E-Mail-Anlagen exportieren. Sie können die Berichte auf der Citrix ADM GUI nicht anzeigen.

Exportieren oder Planen des Exports von Netzwerkfunktionenberichten

April 28, 2021

Sie können einen umfassenden Bericht für ausgewählte Netzwerkfunktionen wie Load Balancing, Content Switching, Cache-Umleitung, Global Server Load Balancing (GSLB), Authentication und Citrix Gateway in Citrix Application Delivery Management (Citrix ADM) erstellen. Dieser Bericht ermöglicht Ihnen einen allgemeinen Überblick über die Zuordnung zwischen den Instanzen, Partitionen und den entsprechenden gebundenen Entitäten (virtuelle Server, Dienstgruppen und Dienste), die im Netzwerk vorhanden sind. Sie können diese Berichte im CSV-Dateiformat exportieren.

Der Bericht zeigt die folgenden virtuellen Serverdaten an:

- Citrix ADC IP-Adresse
- Hostname
- Partitionsdaten
- Name des virtuellen Servers
- Typ des virtuellen Servers
- Virtueller Server
- Virtueller Zielserver für LB

> **Hinweis:**
>
> Für virtuelle Server mit Content Switching und Cache-Umleitung werden in der Spalte

> Virtueller Ziel-LB-Server alle LB-Server aufgelistet, d. h. sowohl Standardserver als auch richtlinienbasierte Server.

- Dienstname
- Name der Dienstgruppe

Sie können planen, dass diese Berichte in verschiedenen Intervallen an bestimmte E-Mail-Adressen exportiert werden.

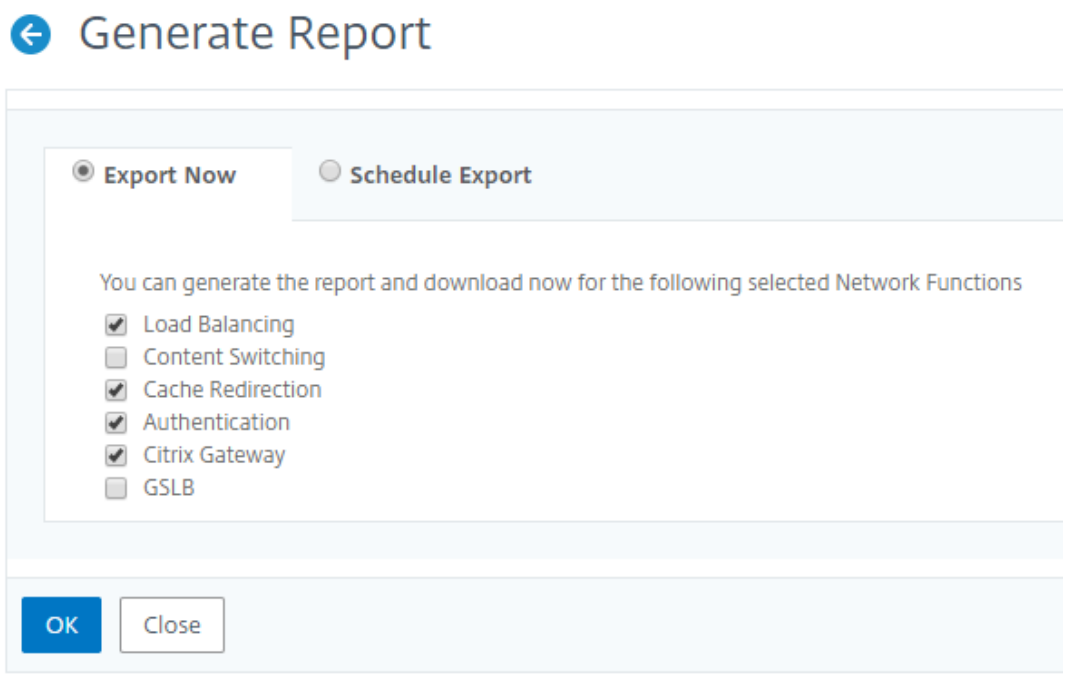
> **Hinweis**
>
> - Bei virtuellen GSLB-Servern werden im Netzwerkfunktionsbericht nur virtuelle GSLB-Server und zugehörige Dienste angezeigt.
> - Für virtuelle Server für Content Switching und Cache-Umleitung zeigt der Bericht nur die Bindungen an die zugeordneten LB-Server an.
> - Virtuelle SSL-Server werden in diesem Bericht nicht aufgeführt, da eine separate Liste virtueller SSL-Server auf Citrix ADM nicht verwaltet wird.
> - Wenn ein neuer Bericht generiert wird, werden die älteren Berichte automatisch aus Ihrem Konto gelöscht.
> - Sie können keinen Netzwerkfunktionsbericht für HAProxy generieren.

So exportieren und planen Sie Berichte über Netzwerkfunktionen:

1. Navigieren Sie zu **Netzwerke** > **Netzwerkfunktionen**.
2. Klicken Sie auf der Seite **Netzwerkfunktionen** im rechten Bereich auf **Bericht generieren** oben rechts auf der Seite.

3. Auf der Seite **Bericht generieren** haben Sie die folgenden 2 Optionen:
   a) Wählen Sie die Registerkarte **Jetzt exportieren** aus und klicken Sie auf **OK**.

Der Bericht wird auf Ihr System heruntergeladen.



Die folgende Abbildung zeigt ein Beispiel für einen Bericht über Netzwerkfunktionen.

Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
121.123.020.85	121.123.020.85		Load Balancing				
121.123.020.100	NS		Load Balancing				
121.123.020.101	admin-NetScalerVPX-10.102.122.101		Load Balancing				
121.123.020.111	PartitionsHost-sp-final-NetScalerVPX	121.123.020.111-partition_	Load Balancing				
121.123.020.115	121.123.020.115	121.123.020.115-partition-	Load Balancing				
121.123.020.139	NS1		Load Balancing				
121.123.020.49	NS1		Load Balancing				

b) Wählen Sie Registerkarte **Bericht planen**, um einen Zeitplan zum Erstellen und Exportieren von Berichten in regelmäßigen Abständen zu erstellen. Geben Sie die Einstellungen für die Berichtsgenerierung an, und erstellen Sie ein E-Mail-Profil, in das der Bericht exportiert wird.

   i. **Wiederholung** - Wählen Sie **Täglich**, **Wöchentlich** oder **Monatlich** aus dem Dropdownlistenfeld aus.

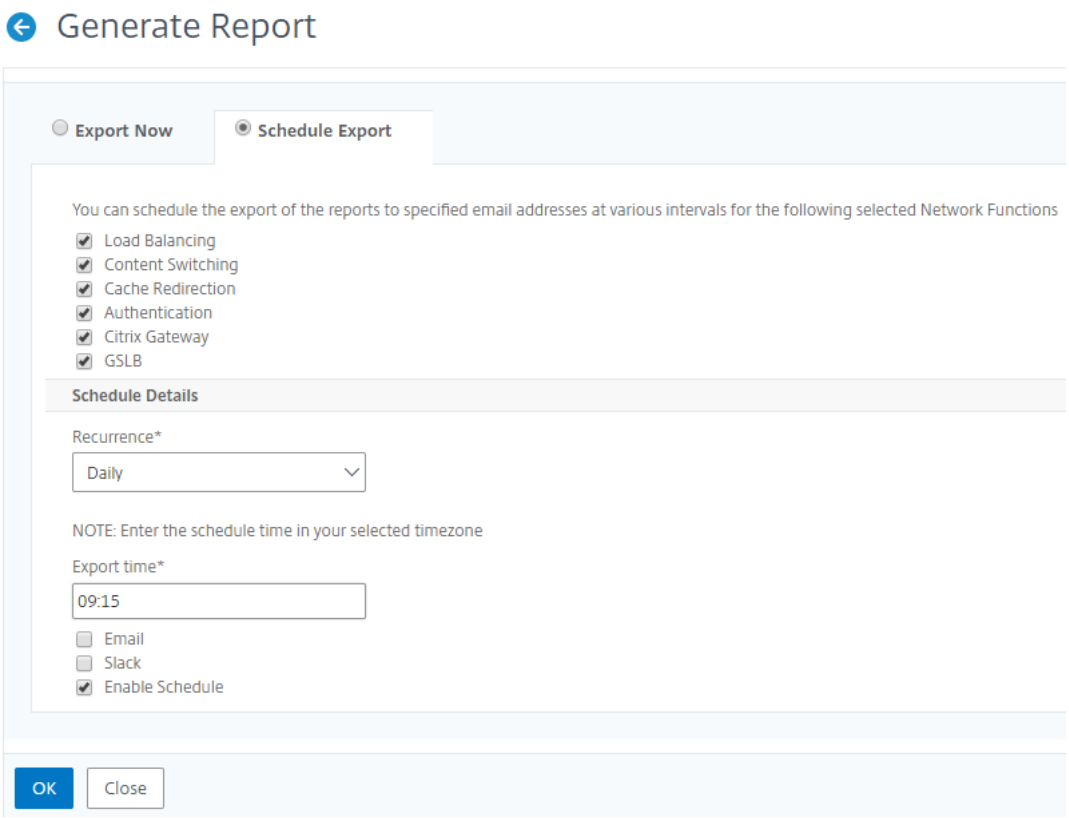
   ii. **Wiederholzeit** - Geben Sie die Zeit in der Stunde: Minute im 24-Stunden-Format ein.

   iii. **E-Mail** - Aktivieren Sie das Kontrollkästchen, und wählen Sie dann das Profil aus dem Dropdownlistenfeld aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

   iv. **Slack** - Aktivieren Sie das Kontrollkästchen, und wählen Sie dann das Profil aus dem Dropdownlistenfeld aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

Klicken Sie auf **Zeitplan aktivieren**, um den Bericht zu planen, und klicken Sie dann auf

OK. Wenn Sie auf das Kontrollkästchen **Zeitplan aktivieren** klicken, können Sie die ausgewählten Berichte erstellen.



Netzwerkberichterstattung

April 28, 2021

Sie können die Ressourcennutzung optimieren, indem Sie Ihre Netzwerkberichte über Citrix Application Delivery Management (Citrix ADM) überwachen. Möglicherweise verfügen Sie über eine verteilte Bereitstellung mit vielen Anwendungen, die an mehreren Standorten bereitgestellt werden. Um eine optimale Leistung Ihrer Anwendungen zu gewährleisten, haben Sie auch mehrere Citrix Application Delivery Controller (Citrix ADC) -Instanzen bereitgestellt, um den Lastausgleich, Content-Switch oder den Datenverkehr zu komprimieren. Die Netzwerkleistung kann sich auf die Anwendungsleistung auswirken. Um die Leistung Ihrer Anwendungen weiterhin aufrechtzuerhalten, müssen Sie Ihre Netzwerkleistung regelmäßig überwachen und sicherstellen, dass alle Ressourcen optimal genutzt werden.

Mit Citrix ADM können Sie Berichte nicht nur für Instanzen auf globaler Ebene erstellen, sondern auch für Entitäten wie virtuelle Server und Netzwerkschnittstellen. Die Instanzfamilie umfasst sowohl Citrix ADC - als auch SD-WAN-Instanzen. Die virtuellen Server, für die Sie Berichte erstellen können, sind wie

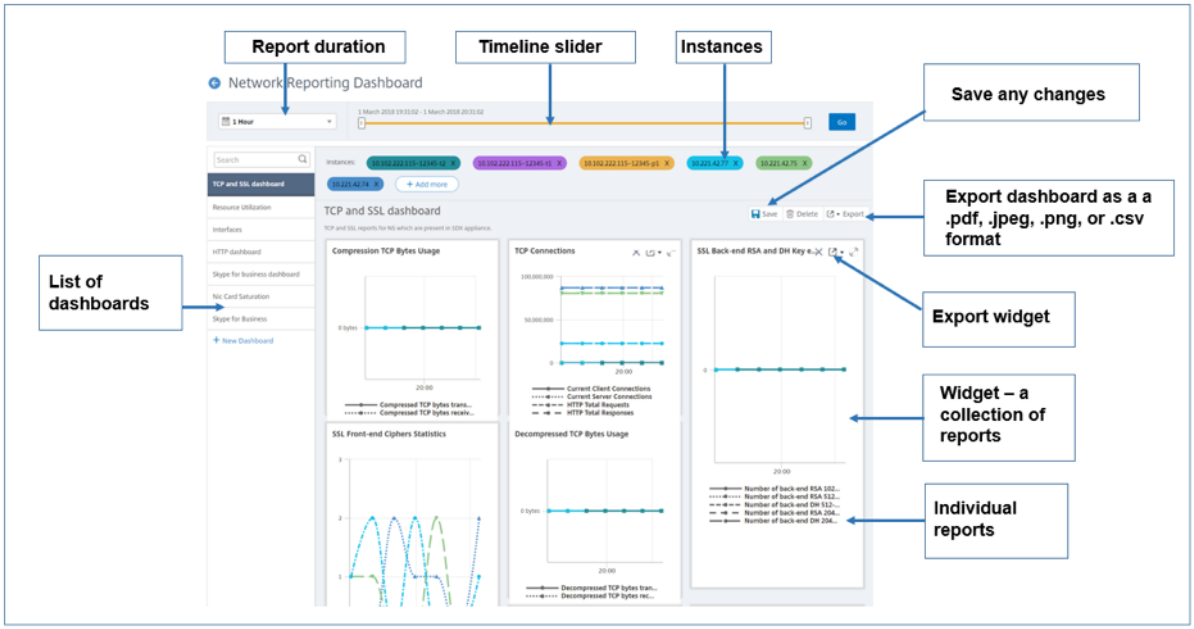
folgt:

- Load Balancing-Server, Dienste und Dienstgruppen
- Content Switching-Server
- Cache-Umleitungsserver
- Globaler Service Load Balancing (GSLB)
- Authentifizierung
- Citrix Gateway

Das Netzwerkberichterstattungs-Dashboard in ADM ist hochgradig anpassbar. Sie können mehrere Dashboards für verschiedene Instanzen, virtuelle Server und andere Entitäten erstellen.

Netzwerkberichterstattungs-Dashboard

Das folgende Bild ruft die verschiedenen Funktionen im Dashboard auf:



- Im linken Bereich werden alle benutzerdefinierten Dashboards aufgelistet, die in Citrix ADM erstellt werden. Sie können auf einen von ihnen klicken, um die verschiedenen Berichte anzuzeigen, aus denen das Dashboard besteht. Beispielsweise enthält ein TCP- und SSL-Dashboard verschiedene Berichte, die sich auf TCP und SSL-Protokolle beziehen.
- Sie können jedes Dashboard mit mehreren Widgets anpassen, um verschiedene Berichte anzuzeigen. Ein Widget stellt einen Bericht auf dem Dashboard dar, d. h. eine Sammlung von verwandten Berichten. Beispielsweise enthält ein Bericht über die Verwendung von komprimierten TCP-Bytes, die pro Sekunde übertragen und empfangen werden.
- Sie können Berichte für eine Stunde, einen Tag, eine Woche oder einen Monat anzeigen. Darüber hinaus können Sie nun die Zeitleistenschiebereglerоption verwenden, um die Dauer

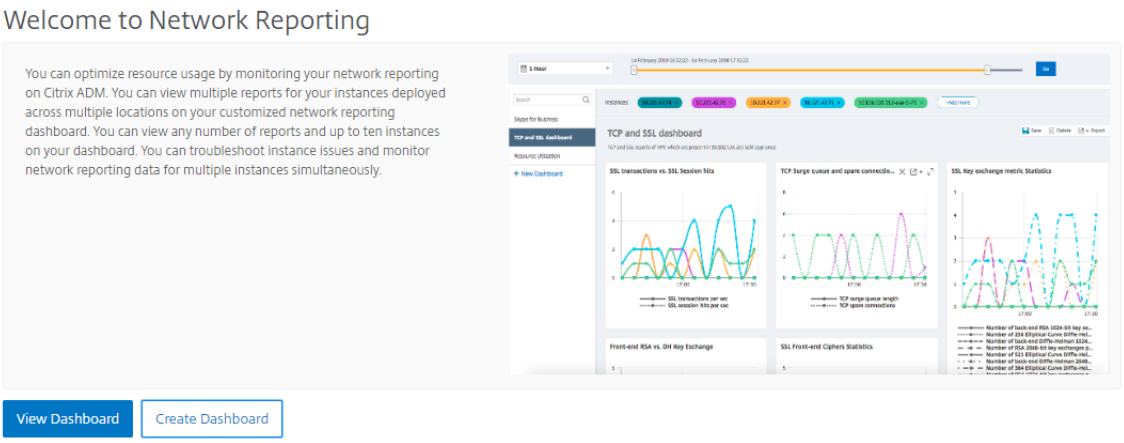
der Berichte anzupassen, die im Citrix ADM generiert werden.

- Sie können einen Bericht entfernen, indem Sie auf X klicken. Sie können den Bericht auch als PDF-, JPEG-, PNG- oder CSV-Format in Ihr System exportieren. Sie können auch einen Zeitpunkt und eine Wiederholung festlegen, wann der Bericht erstellt werden soll. Sie können auch eine E-Mail-Verteilerliste konfigurieren, an die Sie die Berichte senden möchten.
- Im Abschnitt Instanzen oben im Dashboard werden die IP-Adressen aller Instanzen aufgeführt, für die der Bericht generiert wird.
- Sie können Instanzen entweder entfernen, indem Sie auf X klicken oder weitere Instanzen zu den Berichten hinzufügen. Derzeit ermöglicht Ihnen Citrix ADM jedoch, Berichte für 10 Instanzen anzuzeigen.
- Sie können das gesamte Dashboard auch als PDF-, JPEG-, PNG- oder CSV-Format in Ihr System exportieren. Alle am Dashboard vorgenommenen Änderungen müssen gespeichert werden. Klicken Sie auf Speichern, um die Änderungen zu speichern.

Im folgenden Abschnitt werden ausführlich die Aufgaben zum Erstellen eines Dashboards, zum Generieren von Berichten und zum Exportieren von Berichten erläutert.

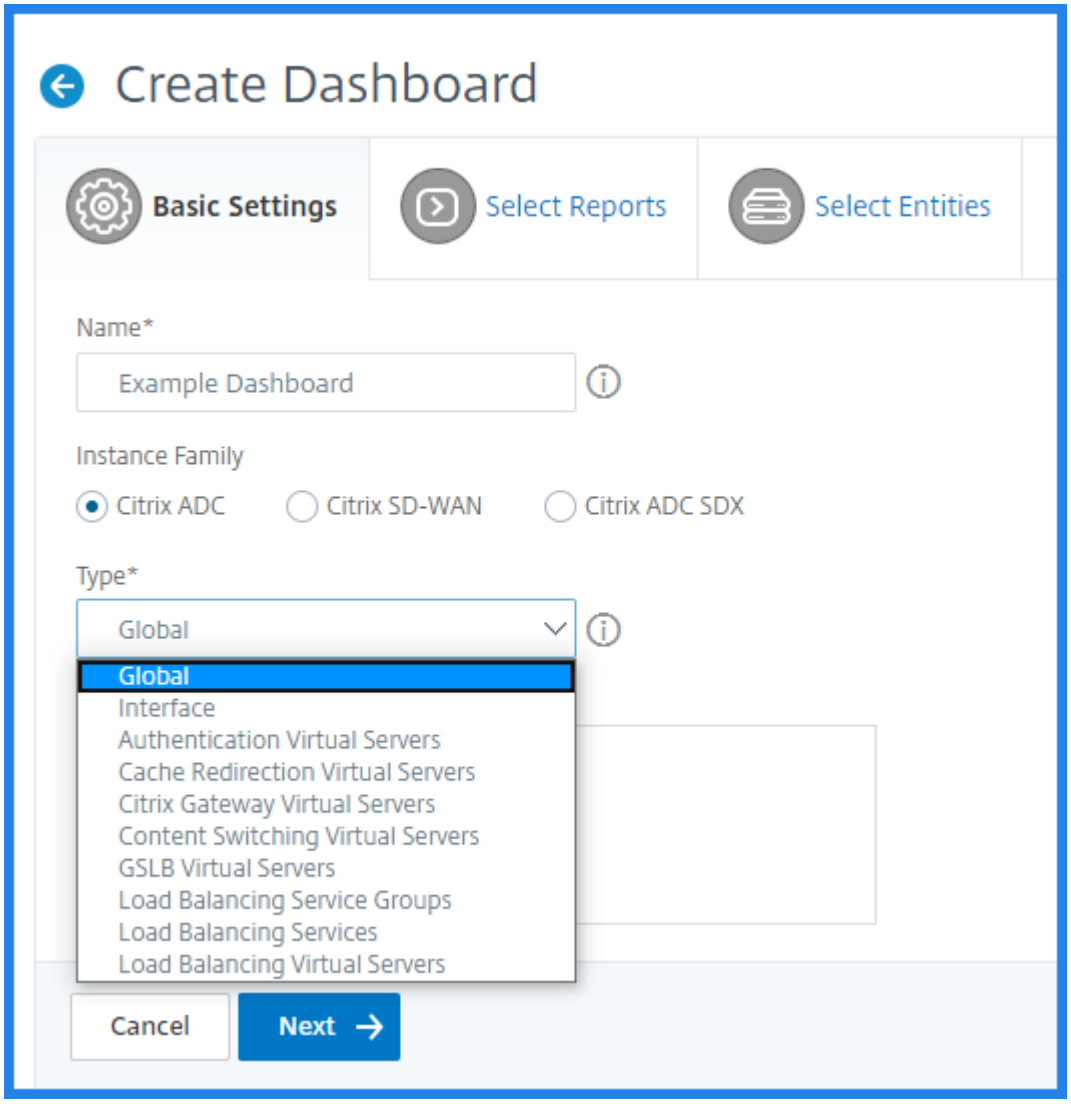
So zeigen Sie ein Dashboard an oder erstellen Sie es:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Netzwerkberichterstattung**.



2. Klicken Sie auf Dashboard anzeigen, um die vorhandenen **Dashboards anzuzeigen**. Die Seite Network Reporting **Dashboard** wird geöffnet, auf der Sie alle Dashboards und Berichtwidgets anzeigen können.
3. Um ein Dashboard zu erstellen, klicken Sie auf **Dashboard erstellen**.

   Die Seite **“Dashboard erstellen** “ wird geöffnet



4. Geben Sie auf der Registerkarte **Grundeinstellungen** die folgenden Details ein:

   a) **Name**. Geben Sie den Namen des Dashboards ein.

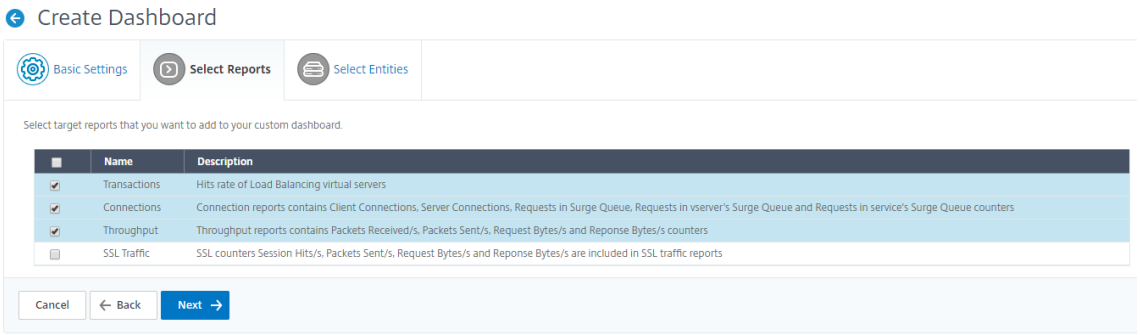
   b) **Instanzfamilie**. Wählen Sie den Instanz-Typ aus - Citrix ADC, Citrix SD-WAN oder Citrix ADC SDX.

   c) **Geben Sie ein**. Wählen Sie den Entitätstyp aus, für den Sie Berichte generieren möchten. Wählen Sie in diesem Beispiel virtuelle Server mit Lastenausgleich aus.

   d) **Beschreibung**. Geben Sie eine aussagekräftige Beschreibung für das Dashboard ein.

5. Klicken Sie auf **Weiter**.

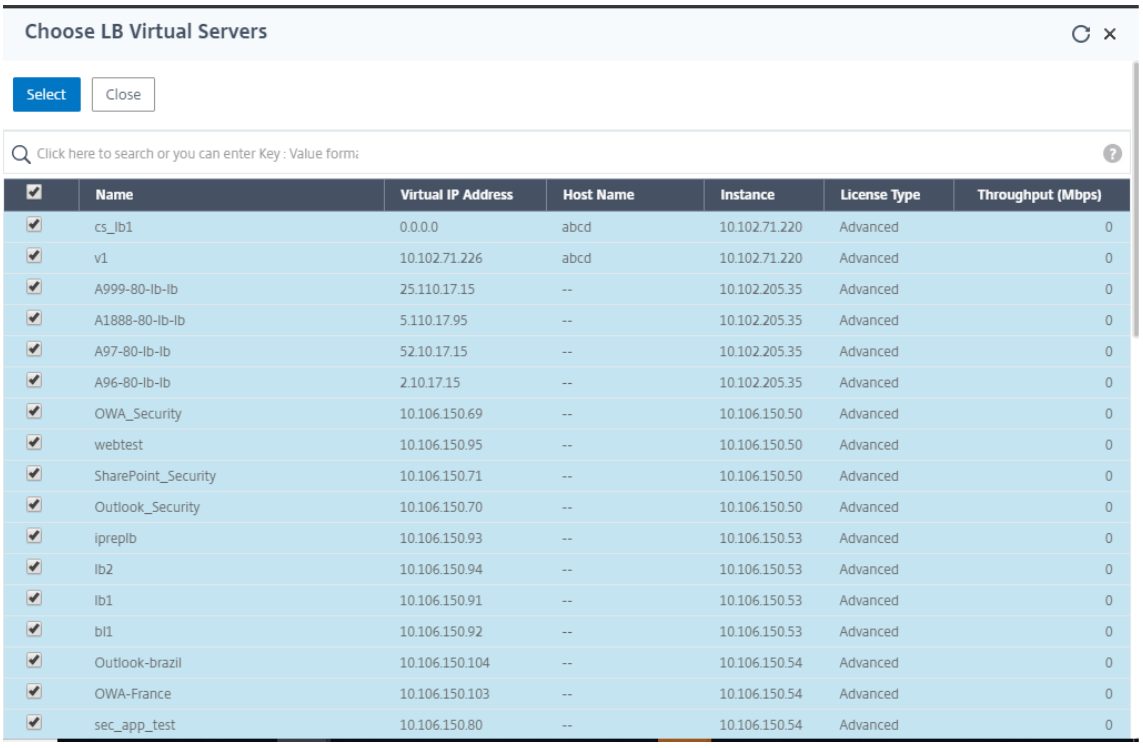
6. **Wählen Sie auf der Registerkarte Berichte** auswählen die erforderlichen Berichte aus. In diesem Beispiel können Sie Transaktionen, Verbindungen und Durchsatz auswählen. Klicken Sie auf **Weiter**.



7. Klicken **Sie auf der Registerkarte Entitäten auswählen** auf **Hinzufügen**.

   Je nach ausgewähltem Entitätstyp auf der Registerkarte **Grundeinstellungen** wird ein Fenster mit der Entitätsliste angezeigt. In diesem Beispiel wird das Fenster **Choose LB Virtual Servers** angezeigt.

8. Wählen Sie die Entitäten aus, die Sie überwachen möchten.



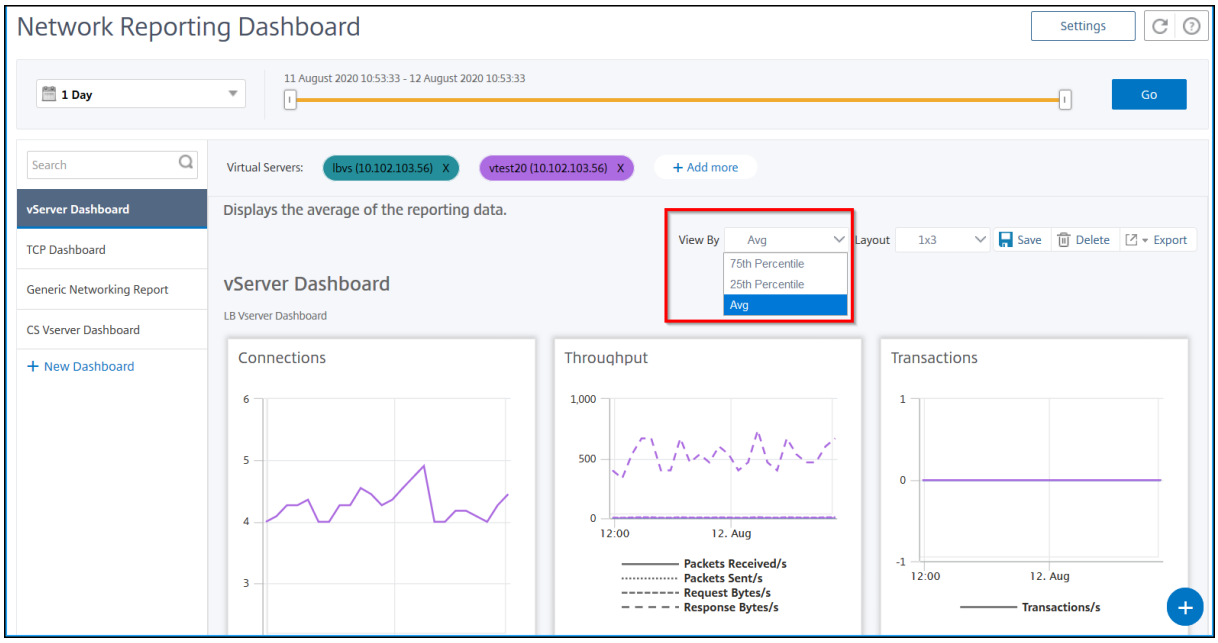
9. Klicken Sie auf **Erstellen**.

Das Dashboard wird erstellt und zeigt alle ausgewählten Berichte an.

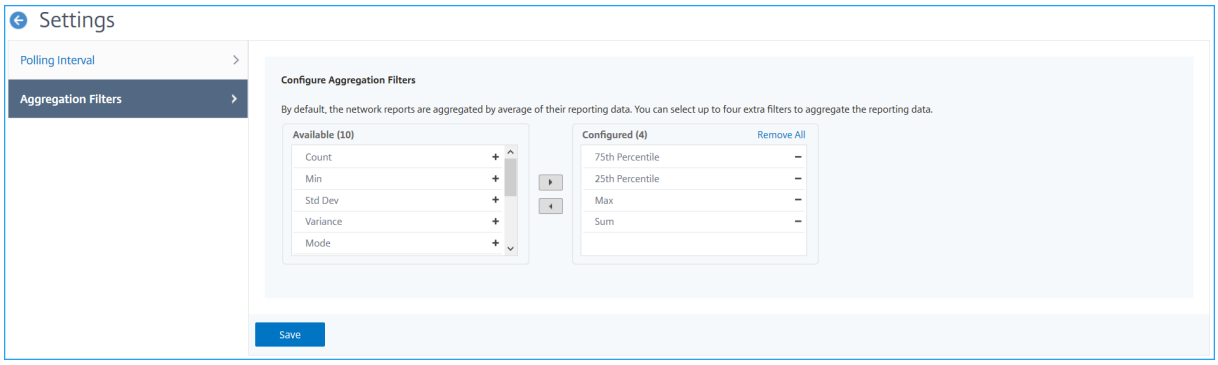
> **Hinweis**
>
> Derzeit können Änderungen, die Sie an Legenden oder Filtern vornehmen, nicht gespeichert werden.

Anzeigen von Netzwerkberichtsdaten durch Anwendung von Aggregationen

Sie können Aggregationen auf die Netzwerkleistungsdaten anwenden und die Anwendungsleistung im Dashboard anzeigen. Sie können die Ergebnisse auch basierend auf Ihren Anforderungen exportieren. Mithilfe dieser Aggregationen, die auf die Daten angewendet werden, können Sie analysieren und sicherstellen, ob alle Ressourcen optimal genutzt werden. Navigieren Sie zu **Netzwerk > Network Reporting** und wählen Sie die Zeitdauer 1 Tag oder später aus, um die Option **Anzeigen nach** zu erhalten.



In den vorhandenen Durchschnittsdaten können Sie Aggregationen anwenden, indem Sie die Option aus der Liste **Anzeigen nach** auswählen. Wenn Sie Aggregation anwenden, werden die Daten für jede Metrik im Dashboard aktualisiert. Klicken Sie auf **Einstellungen** und wählen Sie **Aggregationsfilter**aus.



Im Folgenden finden Sie die Aggregationen, die Sie hinzufügen können:

- Anzahl
- Max.

- Min
- Summe
- Std Dev
- Varianz
- Modus
- Median
- 25. Perzentil
- 75. Perzentil
- 95. Perzentil
- 99. Perzentil
- Vorname
- Nachname

Sie können dem Dashboard bis zu 4 Aggregationsoptionen hinzufügen. Nachdem Sie die Aggregationsoptionen hinzugefügt haben, benötigt Citrix ADM ungefähr eine Stunde, um Berichte für die ausgewählten Aggregationsoptionen zu erstellen.

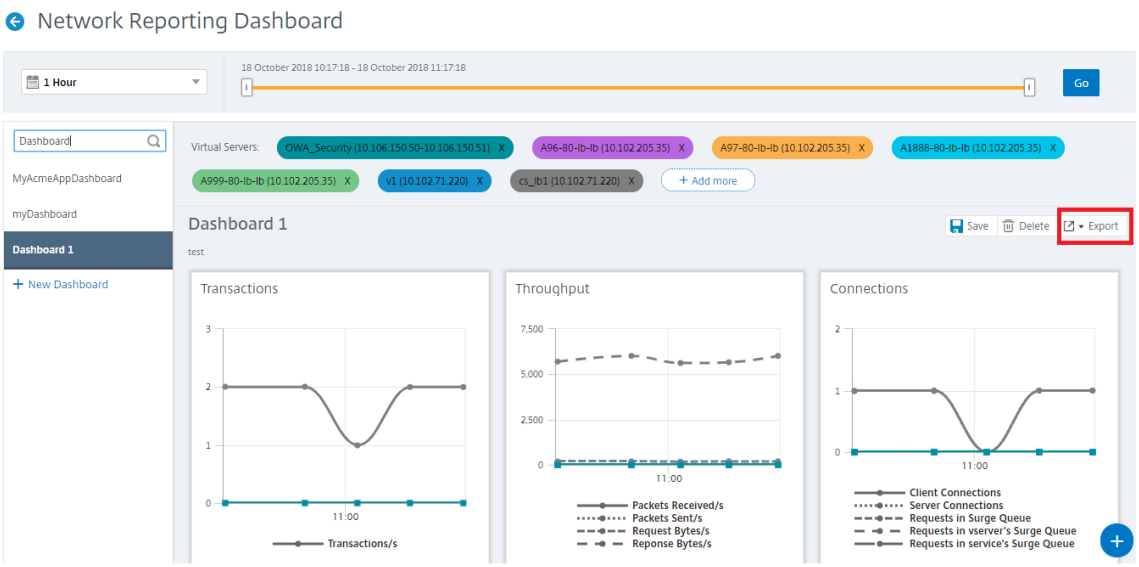
Exportieren von Netzwerkberichten

Sie können Widget-Berichte in den Formaten PDF-, PNG-, JPEG- oder CSV-Format exportieren, aber Sie können die gesamten Dashboards nur in den Formaten PDF-, JPEG- oder PNG-Format exportieren.

> **Hinweis**
>
> Berichte können nicht in Citrix ADM exportiert werden, wenn Sie über schreibgeschützte Berechtigungen verfügen. Sie benötigen eine Bearbeitungsberechtigung, um eine Datei in Citrix ADM erstellen zu können und die Datei exportieren zu können.

So exportieren Sie Dashboard-Berichte:

1. Navigieren Sie zu **Netzwerke** > **Netzwerkberichterstattung**
2. Klicken Sie auf **Dashboards** anzeigen, um alle von Ihnen erstellten Dashboards anzuzeigen.
3. Klicken Sie im linken Bereich auf ein Dashboard. Klicken Sie in diesem Beispiel auf **Dashboard 1.**
4. Klicken Sie oben rechts auf der Seite auf die Schaltfläche Exportieren.
5. Wählen Sie auf der Registerkarte **Jetzt exportieren** das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.



Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

6. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
7. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder Slack-Nachricht zu senden.

   Sie können einen Export der Seite **Network Reporting Dashboard** auf wiederkehrender Basis planen. Sie können beispielsweise eine Option festlegen, um wöchentlich einen Dashboard-Bericht für die vorherige Stunde zu einem bestimmten Zeitpunkt zu generieren. Der Bericht wird dann wöchentlich generiert und zeigt den Status des Dashboards an. Der Bericht überschreibt den Zeit- und Datumsstempel, wenn er vom Benutzer festgelegt wird.

> **Hinweis**
>
> - Wenn Sie Wöchentliche Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie Monatliche Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

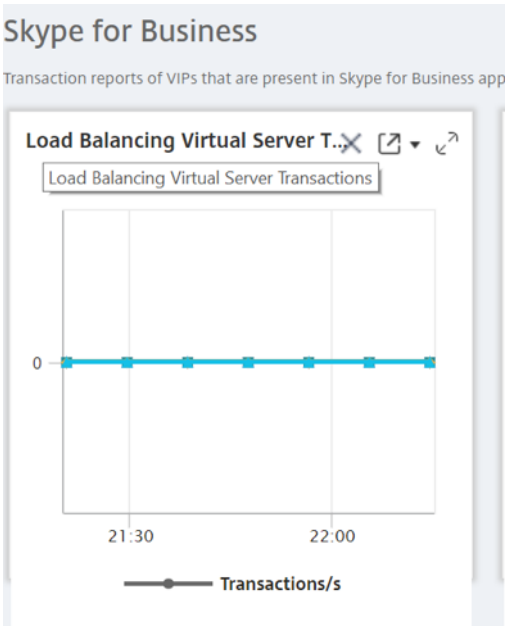
Beim Planen von Netzwerkberichten können Sie die Überschrift des Berichts anpassen, indem Sie eine Textzeichenfolge in das Feld **Betreff** eingeben. Der zum geplanten Zeitpunkt erstellte Bericht hat diese Zeichenfolge als Namen.

Beispielsweise können Sie für Netzwerkberichte, die von einem bestimmten virtuellen Server stammen, den Betreff als authentication-reports-10.106.118.120 eingeben, wobei 10.106.118.120 die IP-Adresse des überwachten virtuellen Servers ist.

> **Hinweis**
>
> Derzeit ist diese Option nur verfügbar, wenn Sie den Export von Berichten planen. Sie können dem Bericht keine Überschrift hinzufügen, wenn Sie sie sofort exportieren.

So exportieren Sie Widget-Berichte:

1. Navigieren Sie zu **Netzwerke** > **Netzwerkberichterstattung**.
2. Klicken Sie auf **Dashboards** anzeigen, um alle von Ihnen erstellten Dashboards anzuzeigen.
3. Klicken Sie im linken Bereich auf ein Dashboard. In diesem Beispiel klicken Sie auch auf **Skype for Business**.
4. Wählen Sie ein Widget aus. Wählen Sie beispielsweise **Lastenausgleichs-Transaktionen**aus.
5. Klicken Sie auf die Schaltfläche Exportieren in der oberen rechten Ecke der Seite
6. Wählen Sie auf der Registerkarte **Jetzt exportieren** das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.



Verwalten von Schwellenwerten für Netzwerkberichte in Citrix ADM

Um den Status einer Citrix ADC-Instanz zu überwachen, können Sie Schwellenwerte für Leistungsindikatoren festlegen und Benachrichtigungen erhalten, wenn ein Schwellenwert überschritten wird. In Citrix ADM können Sie Schwellenwerte konfigurieren und diese anzeigen, bearbeiten und löschen.

Sie können beispielsweise eine E-Mail-Benachrichtigung erhalten, wenn der Leistungsindikator Verbindungen für einen virtuellen Content Switching-Server einen angegebenen Wert erreicht. Sie

können einen Schwellenwert für einen bestimmten Instanztyp definieren. Sie können auch die Berichte auswählen, die Sie für bestimmte Zählermetriken aus der gewählten Instanz generieren möchten.

Wenn der Wert eines Zählers den Schwellenwert überschreitet oder unterschreitet (wie in der Regel angegeben), wird ein Ereignis des angegebenen Schweregrads generiert, das ein leistungsbezogenes Problem darstellt. Wenn der Zählerwert zu einem Wert zurückkehrt, den Sie als normal betrachten, wird das Ereignis gelöscht. Diese Ereignisse können angezeigt werden, indem Sie zu **Netzwerke** > **Ereignisse** > **Berichte** navigieren. Auf der Seite **Berichte** können Sie auf den Donut " **Ereignisse nach Schweregrad** " klicken, um Ereignisse nach ihrem Schweregrad anzuzeigen.

Sie können eine Aktion auch einem Schwellenwert zuordnen, z. B. beim Versenden einer E-Mail- oder SMS-Nachricht, wenn der Schwellenwert überschritten wird.

So erstellen Sie einen Schwellenwert:

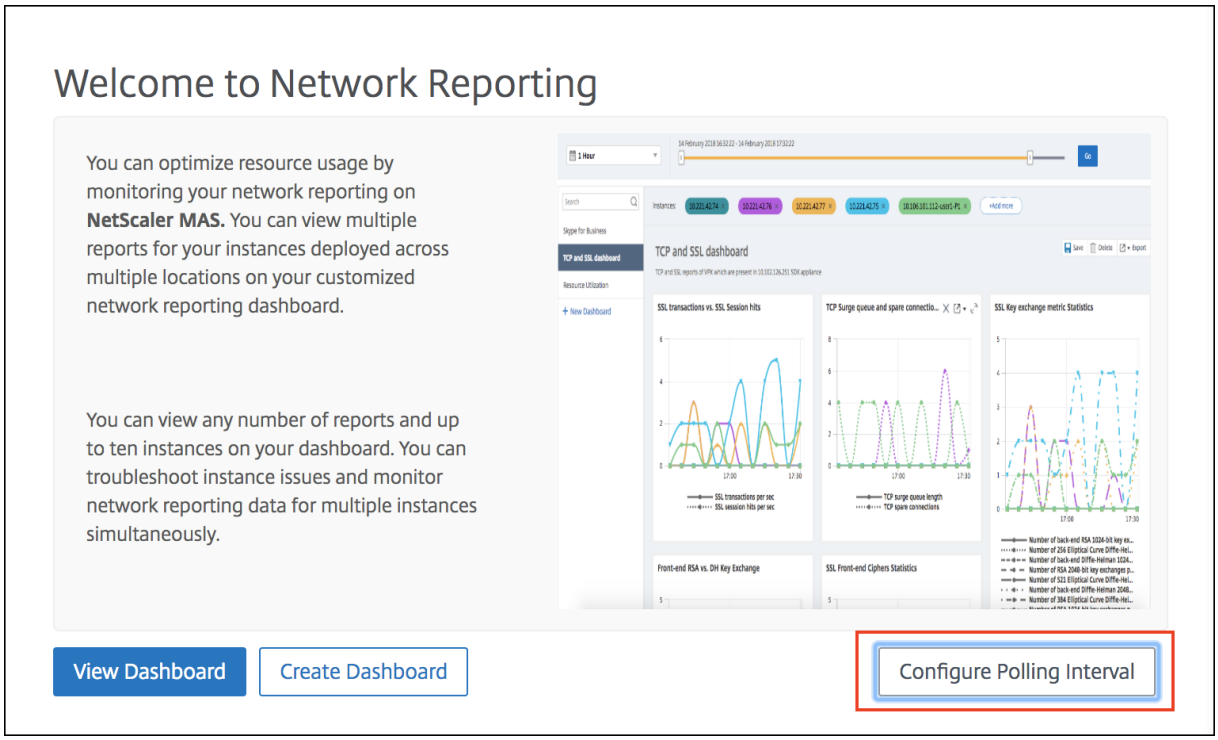
1. Navigieren Sie in Citrix ADM zu **Netzwerke > Network Reporting > Schwellenwerte**. Klicken Sie unter **Schwellenwerte**auf **Hinzufügen**.
2. Geben Sie auf der Seite **Schwellenwert erstellen** die folgenden Details an:
    - **Name**. Name des Schwellenwerts.
    - **Instanztyp**. Wählen Sie Citrix ADC oder Citrix SD-WAN WO.
    - **Berichtsname**. Name des Leistungsberichts, der Informationen zu diesem Schwellenwert enthält.
3. Sie können auch Regeln festlegen, um festzulegen, wann ein Ereignis generiert oder gelöscht werden soll. Sie können die folgenden Details im Abschnitt **Regel konfigurieren** angeben:
    - **Metrisch**. Wählen Sie die Metrik aus, für die Sie einen Schwellenwert festlegen möchten.
    - **Komparator**. Wählen Sie einen Komparator aus, um zu prüfen, ob der überwachte Wert größer oder gleich oder kleiner oder gleich dem Schwellenwert ist.
    - **Schwellenwert**. Geben Sie den Wert ein, für den der Schweregrad des Ereignisses berechnet wird. Beispielsweise können Sie ein Ereignis mit Schweregrad kritischer Ereignisse generieren, wenn der überwachte Wert für aktuelle Clientverbindungen 80 Prozent erreicht. Geben Sie in diesem Fall 80 als Schwellenwert ein. Sie können Ereignisse mit "kritischem Schweregrad" anzeigen, indem Sie zu **Netzwerke > Ereignisse** > **Berichte**navigieren. Auf der Seite **Berichte** können Sie auf den Donut " **Ereignisse nach Schweregrad** " klicken, um Ereignisse nach ihrem Schweregrad anzuzeigen.
    - **Klarer Wert**. Geben Sie den Wert ein, der angibt, wann der Wert gelöscht werden soll. Beispielsweise können Sie den Schwellenwert für aktuelle Clientverbindungen löschen, wenn der überwachte Wert 50 Prozent erreicht. Geben Sie in diesem Fall 50 als Klarwert ein.
    - **Ereignisschweregrad**. Wählen Sie die Sicherheitsstufe aus, die Sie für den Schwellenwert festlegen möchten.

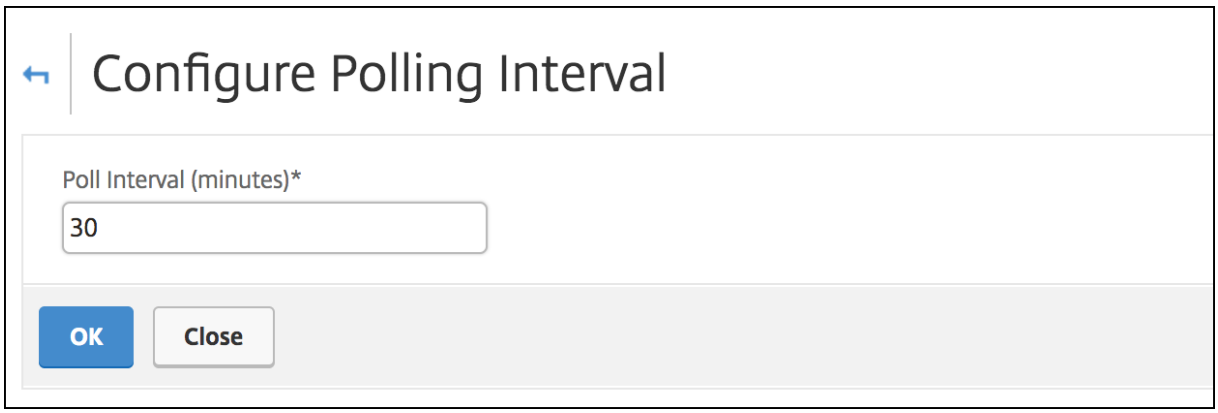
4. Wählen Sie die IP-Adresse der Instanz oder der Instanzen, für die Sie den Schwellenwert festlegen möchten.
5. Sie können auch eine **Ereignisnachricht**hinzufügen. Geben Sie eine Nachricht ein, die angezeigt werden soll, wenn der Schwellenwert erreicht ist. Citrix ADM fügt dieser Nachricht den überwachten Wert und den Schwellenwert an.
6. Wählen Sie **Aktivieren**, um den Schwellenwert zum Generieren von Alarmen zu aktivieren.
7. Optional kannst du **Aktionen** wie E-Mail oder Slack-Benachrichtigungen konfigurieren.
8. Klicken Sie auf **Erstellen**.

Festlegen des Leistungsabrufintervalls für Netzwerkberichte

Standardmäßig erfassen NITRO -Aufrufe alle 5 Minuten Leistungsdaten für das Netzwerk-Reporting. Der ADM ruft Instanzstatistiken wie Zählerinformationen ab und aggregiert sie basierend auf pro Minute, pro Stunde, pro Tag oder pro Woche. Sie können diese aggregierten Daten in vordefinierten Berichten anzeigen.

Um das Leistungsabrufintervall festzulegen, navigieren Sie zu **Netzwerke** > **Netzwerkberichterstattung, und** klicken Sie auf **Abrufintervall konfigurieren**. Das Abrufintervall darf nicht weniger als 5 Minuten oder mehr als 60 Minuten betragen.





Konfigurieren von Netzwerkberichterstattungseinstellungen

Sie können das Löschintervall von Netzwerkberichtsdaten in Citrix ADM konfigurieren. Dieses Intervall begrenzt die Menge der Netzwerkberichtsdaten, die in der Datenbank des Citrix ADM-Servers gespeichert werden. Standardmäßig erfolgt die Beschneidung alle 24 Stunden (um 01.00 Uhr) für das Netzwerk, das historische Daten meldet.

> **Hinweis**
>
> Der Wert, den Sie angeben können, darf 90 Tage oder weniger als 1 Tag betragen.

Orchestrierung

November 15, 2019

Verwalten der Kubernetes Ingress-Konfiguration in Citrix ADM

April 28, 2021

Kubernetes (K8s) ist eine Open-Source-Container-Orchestrierungsplattform, die die Bereitstellung, Skalierung und Verwaltung cloudnativer Anwendungen automatisiert.

Kubernetes bietet die Ingress-Funktion, mit der Clientverkehr außerhalb des Clusters auf Microservices einer Anwendung zugreifen kann, die innerhalb des Kubernetes-Clusters ausgeführt wird. ADC-Instanzen können als Ingress für Anwendungen fungieren, die in einem Kubernetes-Cluster ausgeführt werden. ADC-Instanzen können Lastenausgleich und Content den Nord-Süd-Datenverkehr von den Clients an alle Microservices innerhalb des Kubernetes-Clusters weiterleiten.

> **Hinweis**
>
> - Citrix ADM unterstützt die Ingress-Funktion auf den Clustern mit Kubernetes Version 1.14 und höher.
> - Citrix ADM unterstützt Citrix ADC VPX- und MPX-Appliances als Ingress-Geräte.
> - In einer Kubernetes-Umgebung gleicht die Citrix ADC-Instanzlast nur den Diensttyp "NodePort" aus.

Sie können mehrere ADC-Instanzen so konfigurieren, dass sie als Ingress-Geräte auf demselben Cluster oder auf verschiedenen Clustern oder Namespaces fungieren. Nachdem Sie die Instanzen konfiguriert haben, können Sie jede Instanz auf der Grundlage der Ingress-Richtlinie verschiedenen Anwendungen zuweisen.

Sie können eine Ingress-Konfiguration mit Kubernetes `kubectl`oder APIs erstellen und bereitstellen. Sie können auch ein Ingress von Citrix ADM konfigurieren und bereitstellen.

Sie können die folgenden Aspekte der Kubernetes-Integration in ADM festlegen:

- **Cluster** — Sie können Kubernetes-Cluster registrieren oder die Registrierung aufheben, für die ADM Ingress-Konfigurationen bereitstellen kann. Wenn Sie einen Cluster in Citrix ADM registrieren, geben Sie die Informationen zum Kubernetes API-Server an. Wählen Sie dann einen ADM-Agent aus, der den Kubernetes-Cluster erreichen und Ingress-Konfigurationen bereitstellen kann.
- **Richtlinien** — Ingress-Richtlinien werden verwendet, um die ADC-Instanz basierend auf Cluster oder Namespace auszuwählen, um eine Ingress-Konfiguration bereitzustellen. Geben Sie beim Hinzufügen einer Richtlinie die Cluster-, Standort- und Instanzinformationen an.
- **Ingress-Konfiguration** — Diese Konfiguration ist die Kubernetes-Ingress-Konfiguration, die die Content Switching-Regeln und die entsprechenden URL-Pfade der Microservices und ihrer Ports enthält. Sie können auch die SSL/TLS-Zertifikate (um die SSL-Verarbeitung auf der ADC-Instanz auszulagern) mit den geheimen Ressourcen von Kubernetes angeben.

Citrix ADM ordnet die Ingress-Konfigurationen mithilfe von Ingress-Richtlinien automatisch ADC-Instanzen zu.

Für jede erfolgreiche Ingress-Konfiguration generiert Citrix ADM ein StyleBook ConfigPack. Das ConfigPack stellt die ADC-Konfiguration dar, die auf die ADC-Instanz angewendet wird, die der Ingress-Konfiguration entspricht. Um das ConfigPack anzuzeigen, navigieren Sie zu **Anwendungen > StyleBooks > Configurations**.

Voraussetzungen

Um Citrix ADC-Instanzen als Ingress-Geräte in Kubernetes-Clustern zu verwenden, stellen Sie sicher, dass Sie Folgendes haben:

- Kubernetes Cluster an Ort und Stelle.
- Der Citrix ADM -Agent wurde installiert und konfiguriert, um die Kommunikation zwischen ADM und Kubernetes-Cluster oder verwalteten Instanzen zu ermöglichen. Sie können die verwalteten Instanzen verwenden, die in Ihrem Rechenzentrum oder in der Cloud vorhanden sind.
- Kubernetes-Cluster in Citrix ADM registriert.

Konfigurieren des Citrix ADM Agenten für die Registrierung beim Kubernetes-Cluster

Um die Kommunikation zwischen Kubernetes-Cluster und Citrix ADM zu aktivieren, müssen Sie einen Citrix ADM-Agent installieren und konfigurieren. Sie können einen Agenten auf den folgenden Plattformen bereitstellen:

- Hypervisor (ESX, XenServer, KVM, Hyper-V)
- Öffentliche Cloud-Services (z. B. Microsoft Azure, AWS)

Befolgen Sie die Prozedur, um einen Agenten zu konfigurieren.

> **Hinweis**
>
> Sie können auch einen vorhandenen ADM-Agent verwenden, wenn bereits ein ADM-Agent bereitgestellt wurde.

Konfigurieren Sie Citrix ADM mit einem geheimen Token für die Verwaltung eines Kubernetes-Clusters

Damit Citrix ADM Ereignisse von Kubernetes empfangen kann, müssen Sie ein Dienstkonto in Kubernetes für Citrix ADM erstellen. Konfigurieren Sie das Dienstkonto mit den erforderlichen RBAC-Berechtigungen im Cluster.

1. Erstellen Sie ein Dienstkonto für Citrix ADM. Beispielsweise kann der Name des Dienstkontos sein`citrixadm-sa`. Informationen zum Erstellen eines Dienstkontos finden Sie unterMehrere Dienstkonten verwenden.
2. Verwenden Sie die`cluster-admin` Rolle, um das Citrix ADM Dienstkonto zu binden. Durch diese Bindung wird einem Dienstkonto ein`ClusterRole` über den Cluster hinweg gewährt. Im Folgenden finden Sie einen Beispielbefehl zum Binden einer`cluster-admin` Rolle an das Dienstkonto.

```
kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
   =cluster-admin --serviceaccount=default:citrixadm-sa
<!--NeedCopy-->
```


Nachdem das Citrix ADM Dienstkonto an die`cluster-admin` Rolle gebunden wurde, verfügt das Dienstkonto über den clusterweiten Zugriff. Weitere Informationen finden Sie unter [`kubectl` erstellen `clusterrolebinding`] (https://kubernetes.io/docs/reference/access-authn-authz/rbac/#kubectl-create-clusterrolebinding).

3. Beziehen Sie das Token aus dem erstellten Dienstkonto.

   Führen Sie beispielsweise den folgenden Befehl aus, um das Token für das`citrixadm-sa` Dienstkonto anzuzeigen:

```
kubectl describe sa citrixadm-sa
<!--NeedCopy-->
```

4. Führen Sie den folgenden Befehl aus, um die geheime Zeichenfolge des Tokens zu erhalten:

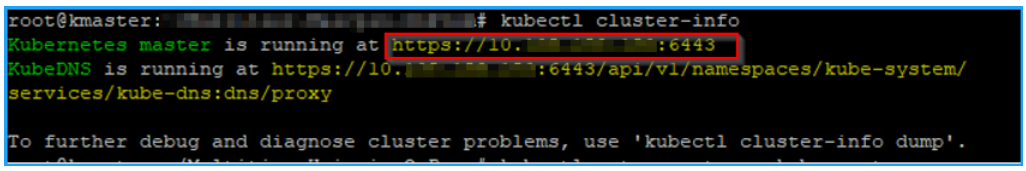
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

Hinzufügen des Kubernetes-Clusters in Citrix ADM

Nachdem Sie einen Citrix ADM -Agent konfiguriert und statische Routen konfiguriert haben, müssen Sie den Kubernetes-Cluster in Citrix ADM registrieren.

So registrieren Sie den Kubernetes-Cluster:

1. Melden Sie sich mit Administratoranmeldeinformationen bei Citrix ADM an.
2. Navigieren Sie zu **Orchestration** > **Kubernetes** > **Cluster**.
   Die Seite “Cluster” wird angezeigt.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie auf der Seite **Cluster hinzufügen** die folgenden Parameter an:
   a) **Name** - Geben Sie einen Namen Ihrer Wahl an.
   b) **API-Server-URL** - Sie können die API-Server-URL-Details vom Kubernetes-Master-Knoten abrufen.
      i. Führen Sie den Befehl auf dem Kubernetes-Master-Knoten aus `kubectl cluster-info`.



ii. Geben Sie die URL ein, die für **Kubernetes master is running at** angezeigt wird.

c) **Authentifizierungstoken** - Geben Sie die Authentifizierungstoken an, die Sie erhalten haben Konfigurieren von Citrix ADM für die Verwaltung eines Kubernetes-Clusters. Das Authentifizierungstoken ist erforderlich, um den Zugriff für die Kommunikation zwischen dem Kubernetes-Cluster und Citrix ADM zu validieren. So generieren Sie ein Authentifizierungstoken:

i. Führen Sie auf dem Kubernetes-Master-Knoten die folgenden Befehle aus:

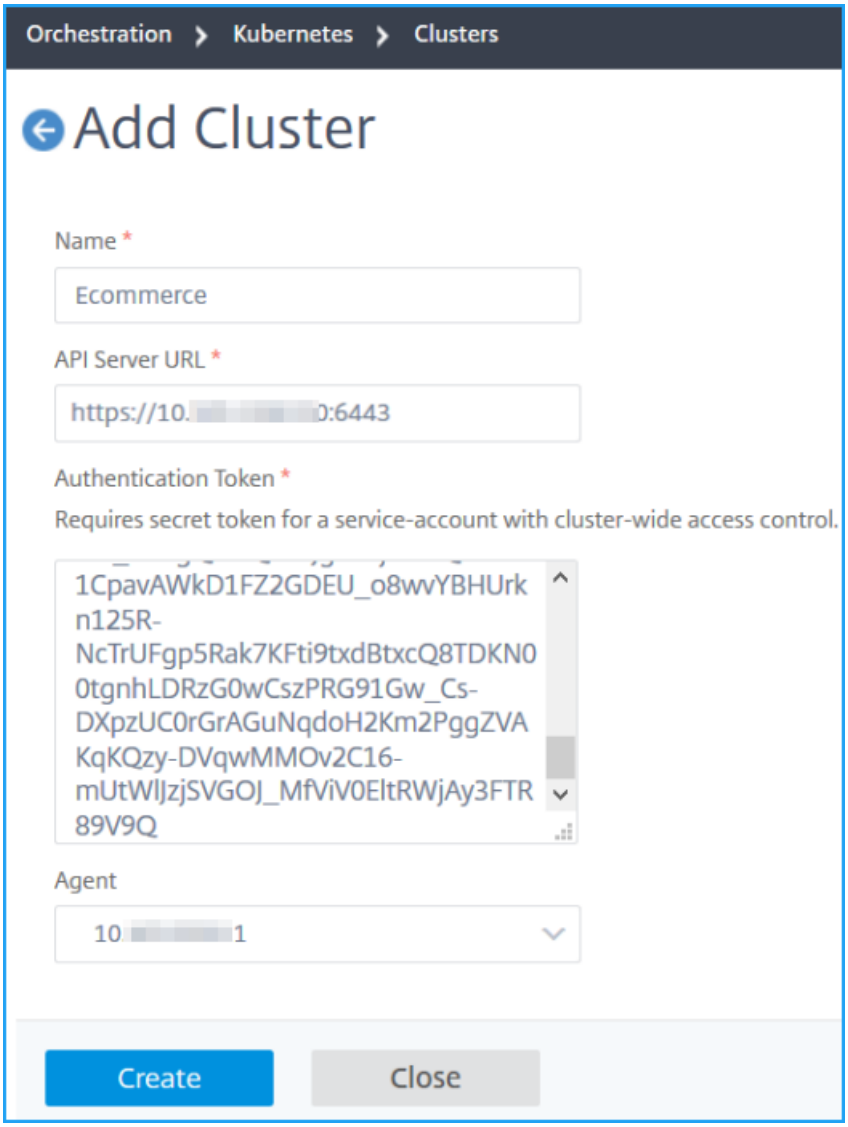
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

ii. Kopieren Sie das generierte Token und fügen Sie es als Authentifizierungstoken ein

Weitere Informationen finden Sie in der Dokumentation unter Kubernetes.

d) Wählen Sie den Agenten aus der Liste aus.

e) Klicken Sie auf **Erstellen**.



Definieren einer Ingress-Richtlinie

Die Ingress-Richtlinie entscheidet, welcher Citrix ADC zur Bereitstellung einer Ingress-Konfiguration verwendet wird, basierend auf dem Ingress Cluster oder Namespace oder beidem.

1. Navigieren Sie zu **Orchestrierung > Kubernetes > Richtlinie**.
2. Klicken Sie auf **Hinzufügen**, um eine Richtlinie zu erstellen.
    a) Geben Sie den Richtliniennamen an.
    b) Definieren Sie **Bedingungen**, um die Ingress-Konfiguration auf einem Kubernetes-Cluster bereitzustellen. Diese Bedingungen basieren in der Regel auf Ingress Cluster und Namespace.
    c) In der Infrastruktur-Panel,

- **Site** - Wählen Sie eine Website aus der Liste aus.
- **Instanz** - Wählen Sie die ADC-Instanz aus der Liste aus.

In den Listen **Site** und **Instanz** werden die Optionen basierend auf der Clusterauswahl im Bedienfeld **Bedingungen** aufgefüllt.

In diesen Listen werden die Sites oder Instanzen angezeigt, die mit dem Citrix ADM Agent verknüpft sind, der mit dem Kubernetes-Cluster konfiguriert ist.

d) **Wählen Sie unter Netzwerk**auswählen das Netzwerk aus, von dem ADM die virtuellen IP-Adressen automatisch einer Ingress-Konfiguration zuweist.

In dieser Liste werden die Netzwerke angezeigt, die unter **Netzwerke > IPAM**erstellt wurden.

e) Klicken Sie auf **Erstellen**.

Bereitstellen der Ingress-Konfiguration

Sie können die Ingress-Konfiguration von Kubernetes mithilfe von Kubernetes `kubectl`, Kubernetes API oder anderen Tools bereitstellen. Sie können die Ingress-Konfiguration auch direkt von Citrix ADM aus bereitstellen.

1. Navigieren Sie zu **Orchestrierung > Kubernetes > Ingresses**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben **Sie im Feld Ingress erstellen** die folgenden Details an:
   a) Geben Sie den Namen des Ingress an.
   b) Wählen Sie unter **Cluster**den Kubernetes-Cluster aus, auf dem Sie einen Ingress bereitstellen möchten.
   c) Wählen Sie den **Cluster-Namespace** aus der Liste aus. Dieses Feld listet die Namespaces auf, die im angegebenen Kubernetes-Cluster vorhanden sind.
   d) Optional: Wählen Sie **Frontend-IP-Adresse automatisch zuweisen**.
   e) Wählen Sie in der Liste die Option **Eindringprotokoll** aus. Wenn Sie **HTTPS**auswählen, geben Sie **TLS-Schlüssel**an.

      Dieses Geheimnis bettet die geheime Kubernetes-Ressource ein, die das HTTPS-Zertifikat und den privaten Schlüssel einbettet.

      Ein HTTPS-Ingress erfordert einen TLS-basierten Schlüssel, der auf dem Kubernetes-Cluster konfiguriert ist. Geben Sie die`tls.crt` Felder`tls.key` und an, die das Serverzertifikat bzw. den Zertifikatschlüssel enthalten sollen.

   f) Geben Sie für das Content-Routing die folgenden Details an:

- **URL-Pfade** - Geben Sie den Pfad an, der dem Kubernetes-Dienst und Port zugeordnet ist.
- **Kubernetes Service** - Geben Sie den gewünschten Service an.
- **Port** - Geben Sie den Dienstport an.
- **LB-Methode** - Wählen Sie die bevorzugte Lastausgleichsmethode für den ausgewählten Kubernetes-Dienst aus.

  Die ausgewählte Methode aktualisiert die Ingress-Spezifikation mit einer entsprechenden Anmerkung. Wenn Sie beispielsweise **ROUNDROBIN** -Methode auswählen, wird die Citrix Annotation wie folgt angezeigt:

```
1  ”lbmethod”:”ROUNDROBIN”
2  <!--NeedCopy-->
```

- **Persistenz-Typ** - Wählen Sie den bevorzugten Load-Balancing-Persistenztyp für den ausgewählten Kubernetes-Dienst aus.

  Der ausgewählte Persistenztyp aktualisiert die Ingress-Spezifikation mit einer entsprechenden Anmerkung. Wenn Sie beispielsweise **COOKIEINSERT**auswählen, wird die Citrix Annotation wie folgt angezeigt:

```
1  ”persistenceType”:”COOKIEINSERT”
2  <!--NeedCopy-->
```

Klicken Sie auf **Hinzufügen**, um weitere URL-Pfade und -Ports zur Ingress-Konfiguration hinzuzufügen.

Nach der Bereitstellung leitet die Ingress-Konfiguration den Clientverkehr auf einen bestimmten Dienst basierend auf den folgenden Informationen um:

- Der angeforderte URL-Pfad und Port.
- Die definierte LB-Methode und der Persistenztyp.

> **Hinweis:**
>
> Kubernetes Services, die in einer Ingress-Konfiguration verwendet werden, müssen vom Typ NodePort sein.

g) Optional, geben Sie eine **Ingress-Beschreibung**an.

h) Klicken Sie auf **Bereitstellen**.

Wenn Sie die Konfiguration vor der Bereitstellung überprüfen möchten, klicken Sie auf **Einspeisung generieren**. Die angegebene Ingress-Konfiguration wird im YAML-Format angezeigt. Klicken Sie nach der Überprüfung der Konfiguration auf **Bereitstellen**.

> **Hinweis**
> Anwenden von Lizenzen auf die virtuellen Server, die mit Ingress-Konfigurationen erstellt werden. Führen Sie die folgenden Schritte aus, um die Lizenz anzuwenden:
>
> 1. Wechseln Sie zu **System > Lizenzierung und Analyse**.
> 2. Aktivieren Sie unter **Virtueller Server-Lizenzübersicht**die **Option Virtuelle Server automatisch auswählen**.

Verwenden von ADM-Audit-Protokollen zur Verwaltung und Überwachung Ihrer Infrastruktur

April 28, 2021

Sie können den Citrix ADM Dienst verwenden, um alle Ereignisse auf ADM- und Syslog-Ereignissen zu verfolgen, die auf ADM-verwalteten ADC-Instanzen generiert wurden. Diese Meldungen können Sie bei der Verwaltung und Überwachung Ihrer Infrastruktur unterstützen. Protokollmeldungen sind jedoch nur dann eine großartige Informationsquelle, wenn Sie sie überprüfen, und ADM vereinfacht die Überprüfung von Protokollmeldungen.

Sie können Filter verwenden, um ADM-Syslog- und Überwachungsprotokollmeldungen zu durchsuchen. Die Filter helfen, Ihre Ergebnisse einzugrenzen und genau das zu finden, wonach Sie suchen und in Echtzeit. Die integrierte Suchhilfe führt Sie zum Filtern der Protokolle. Eine weitere Möglichkeit, Protokollmeldungen anzuzeigen, besteht darin, sie in PDF-, CSV-, PNG- und JPEG-Formaten zu exportieren. Sie können den Export dieser Berichte an bestimmte E-Mail-Adressen in verschiedenen Intervallen planen.

Sie können die folgenden Arten von Protokollnachrichten von der ADM-GUI überprüfen:

- ADC-Instanz bezogene Überwachungsprotokolle
- ADM-bezogene Überwachungsprotokolle
- Anwendungsüberwachungsprotokolle

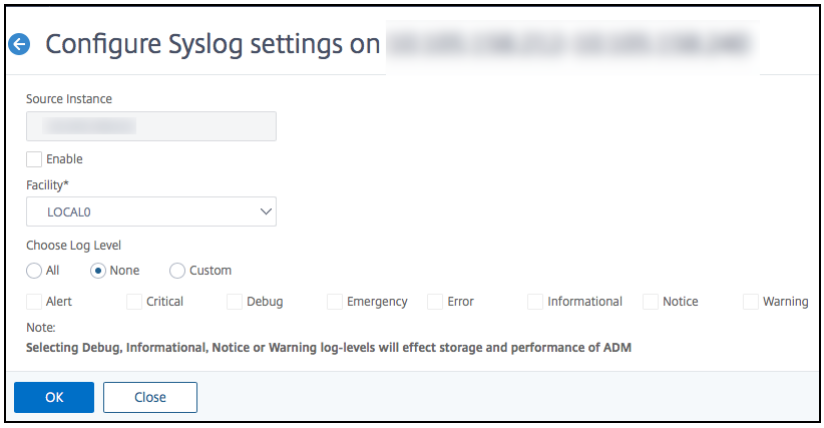
ADC-Instanz bezogene Überwachungsprotokolle

Bevor Sie ADC-Instanz-bezogene Syslog-Nachrichten von ADM anzeigen können, konfigurieren Sie den Citrix ADM Dienst als Syslog-Server für die Citrix ADC-Instanz. Nachdem die Konfiguration abgeschlossen ist, werden alle Syslog-Nachrichten von der Instanz an ADM umgeleitet.

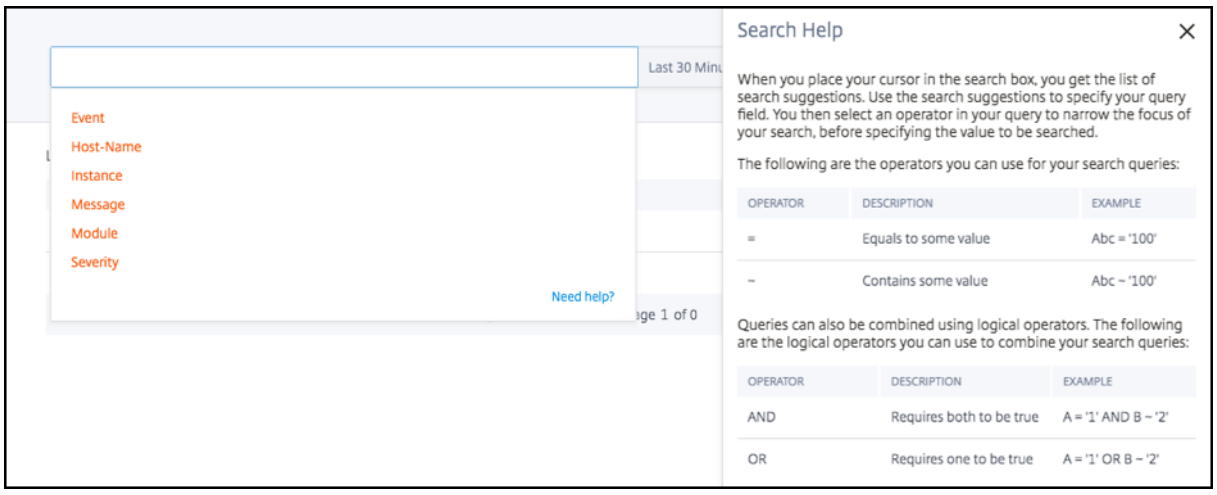
Konfigurieren von ADM als Syslog-Server

Gehen Sie folgendermaßen vor, um ADM als Syslog-Server zu konfigurieren:

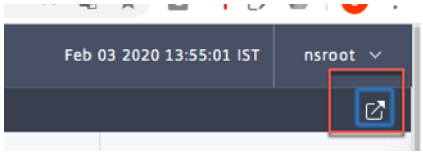
1. Navigieren Sie von der ADM-Benutzeroberfläche zu **Netzwerke > Instanzen**.
2. Wählen Sie die Citrix ADC-Instanz aus, aus der die Syslog-Nachrichten gesammelt und in Citrix ADM angezeigt werden sollen.
3. Wählen Sie in der Liste **Aktion auswählen** die Option **Syslog konfigurieren**aus.
4. Klicken Sie auf **Aktivieren**.
5. Wählen Sie in der Dropdownliste **Einrichtung** eine lokale Einrichtung oder auf Benutzerebene aus.
6. Wählen Sie die erforderliche Protokollstufe für die Syslog-Meldungen aus.
7. Klicken Sie auf **OK**.



Mit diesen Schritten werden alle Syslog-Befehle in der Citrix ADC-Instanz konfiguriert, und Citrix ADM beginnt mit dem Empfang der Syslog-Nachrichten. Sie können die Nachrichten anzeigen, indem Sie zu **Netzwerke > Ereignisse > Syslog-Nachrichten** navigieren. Klicken Sie auf **Hilfe benötigen?**, um die integrierte Suchhilfe zu öffnen. Weitere Informationen finden Sie unter Anzeigen und Exportieren von Syslog-Nachrichten.



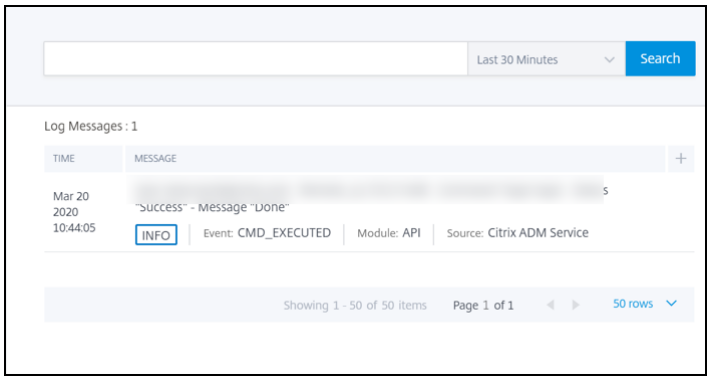
Um die Protokollmeldungen zu exportieren, klicken Sie auf das Pfeilsymbol in der oberen rechten Ecke.



Klicken Sie als Nächstes auf **Jetzt exportieren** oder **Export planen**. Weitere Informationen finden Sie unter Exportieren von Syslog-Nachrichten.

ADM-bezogene Überwachungsprotokolle

Basierend auf vorkonfigurierten Regeln generiert ADM Überwachungsprotokollmeldungen für alle Ereignisse auf und hilft Ihnen dabei, den Zustand Ihrer Infrastruktur zu überwachen. Um alle Audit-Protokollmeldungen anzuzeigen, die im ADM vorhanden sind, navigieren Sie zu **Accounts->Audit-Log Meldungen**.

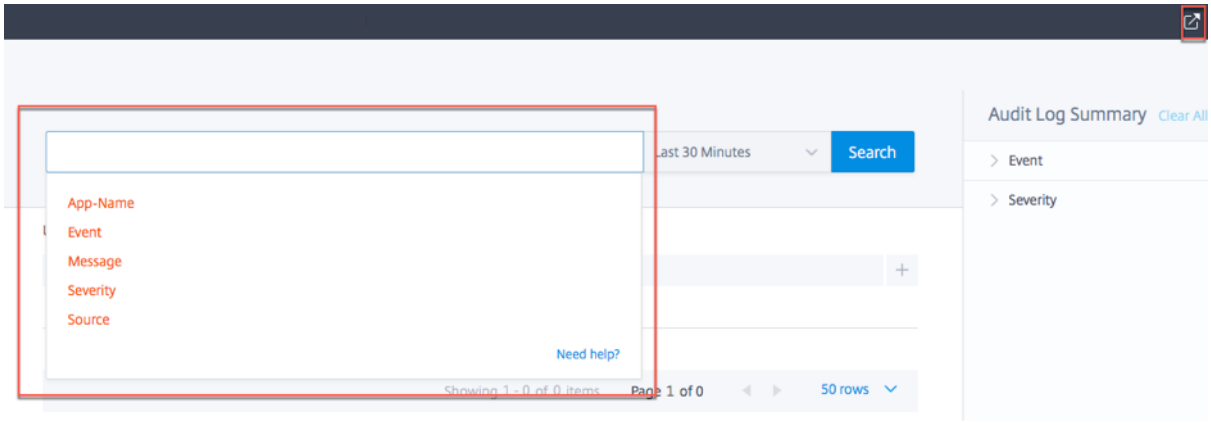


Um die Protokollmeldungen zu exportieren, klicken Sie auf das Pfeilsymbol in der oberen rechten Ecke.

Anwendungsbezogene Überwachungsprotokolle

Sie können die Überwachungsprotokollmeldungen für alle ADM-Anwendungen oder für eine bestimmte Anwendung anzeigen.

- Um alle Überwachungsprotokollmeldungen für alle Anwendungen anzuzeigen, die im ADM vorhanden sind, navigieren Sie zu **Netzwerk->Netzwerkfunktionen >Überwachung**.



- Um Überwachungsprotokollmeldungen für eine bestimmte Anwendung im ADM anzuzeigen, navigieren Sie zu **Anwendung > Dashboard > doppelklicken Sie auf den virtuellen Server > Überwachungsprotokoll**.

> Hinweis:
>
> Sie können ADM-Überwachungsprotokollmeldungen an einen externen Server weiterleiten. Einzelheiten finden Sie unter Auditing-Informationen anzeigen.

Analytics

April 28, 2021

Citrix Application and Delivery Management (ADM) -Analysen bieten eine einfache und skalierbare Möglichkeit, die verschiedenen Erkenntnisse der Daten der Citrix ADC-Instanzen zu beschreiben, vorherzusagen und die Performance der Anwendung zu verbessern. Sie können eine oder mehrere Analysefunktionen gleichzeitig auf Citrix ADM verwenden. Die folgende Tabelle beschreibt verschiedene Analysefunktionen, die von Citrix ADM unterstützt werden:

Analytics-Funktionen	Beschreibungen
Web Insight	Web Insight ermöglicht Einblick in Unternehmens-Webanwendungen und ermöglicht IT-Administratoren die Überwachung aller Webanwendungen, die vom Citrix ADC bedient werden, durch integrierte und Echtzeitüberwachung von Anwendungen.

Analytics-Funktionen	Beschreibungen
HDX Insight	HDX Insight bietet End-to-End-Sichtbarkeit für ICA-Datenverkehr, der über Citrix ADC fließt. Mit HDX Insight können Administratoren Echtzeitmetriken für Client- und Netzwerklatenz, historische Berichte, End-to-End-Performance-Daten anzeigen und Leistungsprobleme beheben.
Gateway Insight	Gateway Insight bietet Einblick in die Fehler, die bei der Anmeldung bei Citrix Gateway auftreten, unabhängig vom Zugriffsmodus.
Sicherheitshinweise	Security Insight bietet eine Lösung aus einem Bereich, mit der Sie Ihren Anwendungssicherheitsstatus beurteilen und Korrekturmaßnahmen ergreifen können, um Ihre Anwendungen zu schützen.
SSL Insight	SSL Insight bietet Einblick in sichere Webtransaktionen (HTTPS) und ermöglicht IT-Administratoren, alle vom Citrix ADC bereitgestellten sicheren Webanwendungen zu überwachen, indem sie eine integrierte Echtzeit- und historische Überwachung sicherer Webtransaktionen bereitstellen.

Lizenzanforderungen

July 3, 2020

Die Lizenzanforderungen, die für die ADC-Instanzen erforderlich sind, um die verschiedenen Analyseberichte zu Citrix Application Delivery Management (ADM) anzuzeigen, sind in der folgenden Tabelle beschrieben:

Citrix ADM Analytics-Funktionen	ADC-Lizenzanforderung
Web Insight	Web Insight-Bericht auf Citrix ADM wird in allen ADC-Lizenzversionen (Standard/Advanced/Premium) unterstützt.

Citrix ADM Analytics-Funktionen	ADC-Lizenzanforderung
HDX Insight	HDX Insight Bericht auf Citrix ADM wird auf einer der folgenden ADC-Lizenzen unterstützt: Advanced Edition (für Berichte < 1 Stunde) oder Premium Edition (für unbegrenzte Berichterstattung). **Hinweis:** Standardlizenz Edition wird nicht unterstützt.
Sicherheitshinweise	Der Security Insight-Bericht für Citrix ADM wird für die Premium Edition oder Advanced Edition mit App Firewall-Lizenz unterstützt. **Hinweis:** Standardlizenz und Standalone App Firewall-Lizenz werden nicht unterstützt.
SSL Insight	SSL Insight-Bericht auf Citrix ADM wird in allen ADC-Lizenzversionen (Standard/Advanced/Premium) unterstützt.
Gateway Insight	Der Gateway Insight-Bericht auf Citrix ADM wird auf einer der folgenden ADC-Lizenzen unterstützt: Advanced Edition (für Berichte < 1 Stunde) oder Premium Edition (für unbegrenzte Berichterstellung). **Hinweis:** Standardlizenz Edition wird nicht unterstützt.
TCP Insight	TCP Insight-Bericht wird für alle ADC-Lizenz-Editionen (Standard/Advanced/Premium) unterstützt.
Video Insight	Video Insight-Bericht auf Citrix ADM wird in der ADC Premium Edition (ADC-T 1000-Serie, VPX-T) unterstützt.
WAN-Einblick	WAN Insight-Bericht auf Citrix ADM wird unter ADC SD-WAN WO Edition (WAN Optimization Edition) unterstützt.

Übersicht über den Logstream

April 28, 2021

Citrix ADC-Instanzen generieren AppFlow Datensätze und stellen einen zentralen Kontrollpunkt für

den gesamten Anwendungsdatenverkehr im Rechenzentrum dar. **IPFIX** und **Logstream** sind die Protokolle, die diese AppFlow-Datensätze von Citrix ADC-Instanzen an Citrix ADM transportieren. Weitere Informationen finden Sie unter AppFlow.

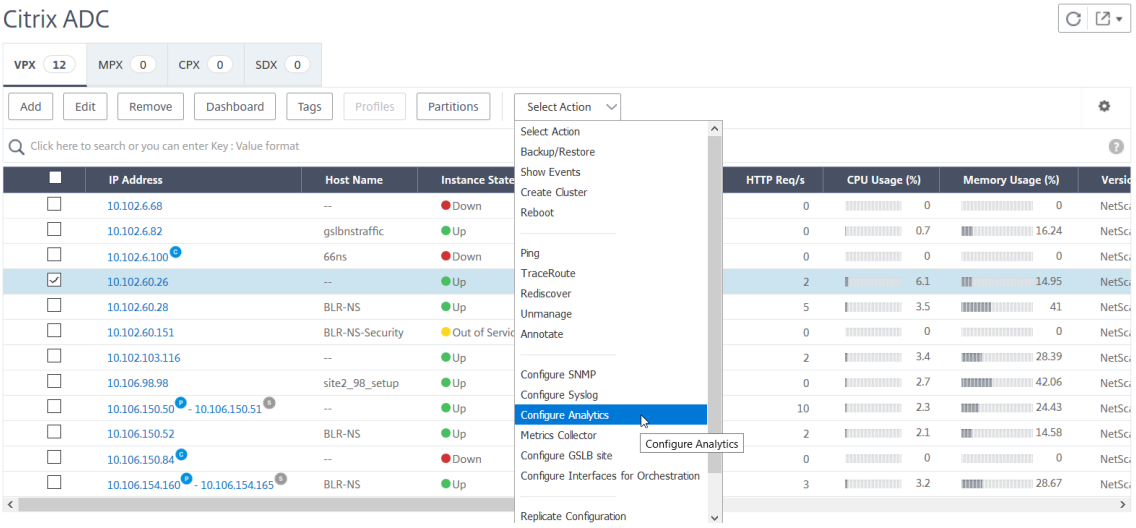
- **IPFIX** ist ein offener Internet Engineering Task Force (IETF) -Standard, der in RFC 5101 definiert ist. **IPFIX** verwendet ein UDP-Protokoll, ein unzuverlässiges Transportprotokoll, das für den Datenfluss in eine Richtung verwendet wird. Da IPFIX UDP-Protokoll verwendet, führt die Einhaltung des IPFIX-Standards zur Verarbeitung von mehr Ressourcen in Citrix ADM.
- **Logstream** ist ein Citrix-eigenes Protokoll, das als einer der Transportmodi verwendet wird, um die Analytics-Protokolldaten von Citrix ADC-Instanzen effizient auf Citrix ADM zu übertragen. **Logstream** verwendet ein zuverlässiges TCP-Protokoll und benötigt weniger Ressourcen für die Verarbeitung der Daten.

Für Citrix ADC zwischen **11.1 Build 47.14 und 11.1 Build 62.8**ist **Logstream** der Standard-Transportmodus zum Aktivieren von Web Insight (HTTP) und IPFIX ist der einzige Transportmodus, um andere Erkenntnisse zu ermöglichen. Für Citrix ADC Version ab **12.0 bis zur neuesten Version** können Sie entweder **Logstream**oder **IPFIX** als Transportmodus auswählen.

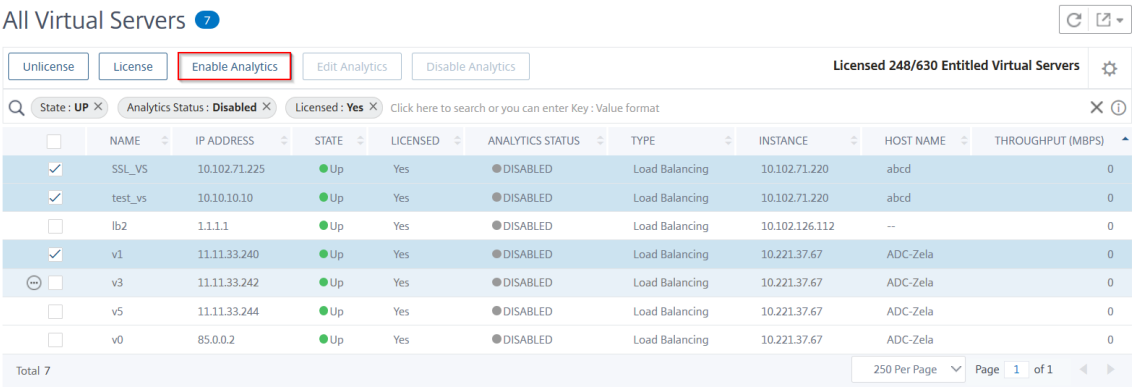
> **Hinweis**
>
> Die Citrix ADM-Version und der Build müssen Ihrer Citrix ADC-Version und Ihrem Build **entsprechen oder höher** sein. Wenn Sie beispielsweise Citrix ADC 12.1 Build 50.28/50.31 installiert haben, stellen Sie sicher, dass Sie Citrix ADM 12.1 Build 50.39 oder höher installiert haben.

Logstream als Transportmodus aktivieren

1. Navigieren Sie zu **Netzwerke** > **Instanzen**, und wählen Sie die ADC-Instanz aus, die Sie Analysen aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.



3. Wählen Sie die virtuellen Server aus, und klicken Sie dann auf **Analytics aktivieren**.



4. Im Fenster **Analytics aktivieren**:

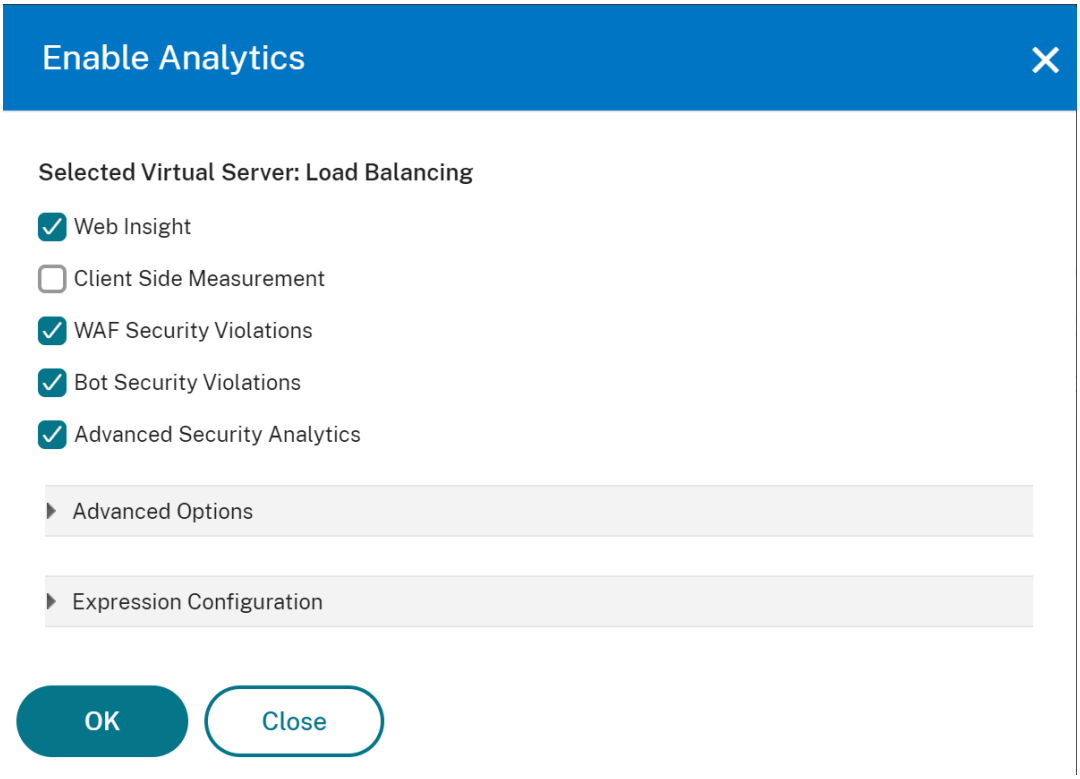
   a) Auswählen der Einsichtstypen (Web Insight oder Security Insight)

   b) **Logstream** als Transportmodus auswählen

   > **Hinweis**
   >
   > Für Citrix ADC zwischen **11.1 Build 47.14 und 11.1 Build 62.8**ist **Logstream** der Standard-Transportmodus zum Aktivieren von Web Insight (HTTP) und IPFIX ist der einzige Transportmodus, um andere Erkenntnisse zu ermöglichen. Für Citrix ADC Version ab **12.0 bis zur neuesten Version** können Sie entweder **Logstream**oder **IPFIX** als Transportmodus auswählen.

   c) Der Ausdruck ist standardmäßig true

   d) Klicken Sie auf **OK**



Hinweis

```
- Wenn Sie virtuelle Server auswählen, die nicht lizenziert sind, lizenziert Citrix ADM zuerst diese virtuellen Server und aktiviert dann die Analyse

- Für Admin-Partitionen wird nur **Web Insight** unterstützt

- Für virtuelle Server wie Cacheumleitung, Authentifizierung und GSLB können Sie keine Analysen aktivieren. Es wird eine Fehlermeldung angezeigt.
```

In der folgenden Tabelle werden die Funktionen von Citrix ADM beschrieben, die **Logstream** als Transportmodus unterstützt:

Feature	**IPFIX**	**Logstream**
Web Insight	•	•
Sicherheitshinweise	•	•

Feature	**IPFIX**	**Logstream**
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Nicht unterstützt	•
CR Einblick	•	•
IP-Reputation	•	•
AppFirewall	•	•
Clientseitige Messung	•	•
Syslog/Auditlog	•	•

Self-Service-Diagnose für Analysen

April 28, 2021

Citrix ADM führt eine Self-Service-Diagnose durch, um die Lizenz- und Konfigurationsprobleme auf den verwalteten Instanzen für die folgenden Analysefunktionen zu identifizieren:

- Web Insight
- HDX Insight
- Gateway Insight
- Sicherheitshinweise
- Bot Einblick
- SSL-Forward-Proxyanalyse

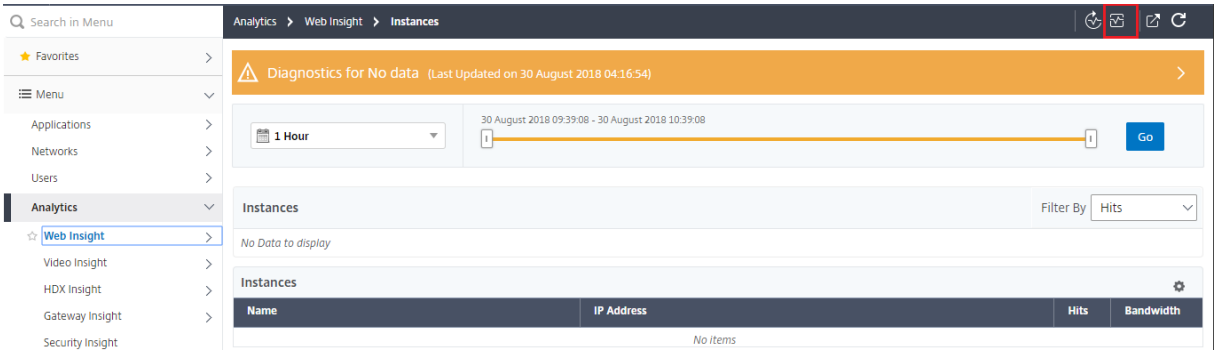
Die Self-Service-Diagnose wird alle 12 Stunden ausgeführt und generiert einen Diagnosebericht, wenn Probleme für jedes der angegebenen Analysefunktionen gefunden werden. Der Diagnosebericht enthält die Ursachen der Probleme, die Arten der Probleme und die Korrekturmaßnahmen zur Behebung der Probleme. Die Self-Service-Diagnose hilft Ihnen, Probleme schneller zu erkennen und zu beheben.

Wenn die AppFlow Richtlinie beispielsweise nicht an einen virtuellen Server gebunden ist oder ein virtueller Server nicht lizenziert ist, erhält Citrix ADM nicht die gewünschten Daten für die Web Insight-Überwachung. Die Self-Service-Diagnose identifiziert die Probleme und generiert einen Diagnosebericht. Sie können den Diagnosebericht anzeigen, um die Probleme zu überprüfen und die Korrekturmaßnahmen durchzuführen.

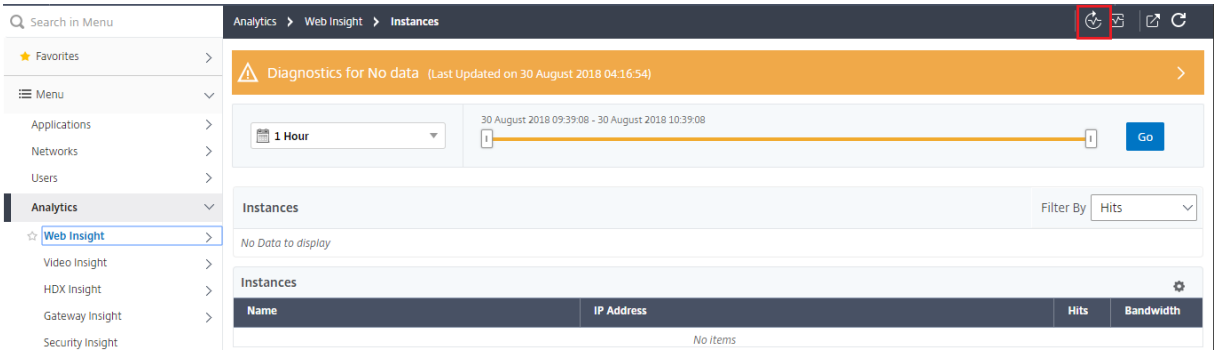
Anzeigen des Diagnoseberichts

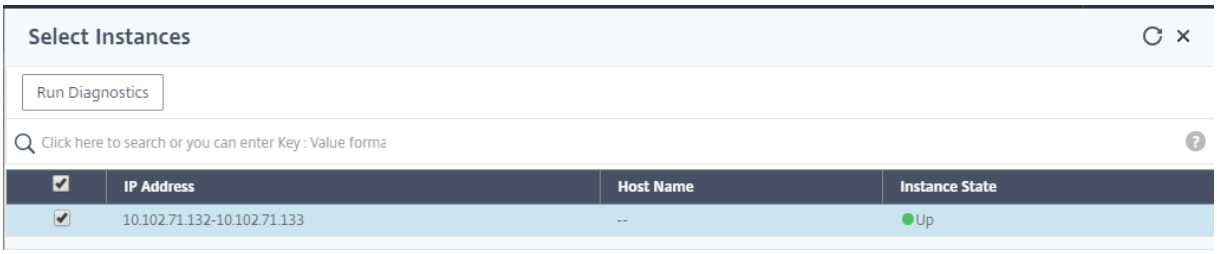
Um die Diagnoseberichte für die angegebenen Analytics-Features anzuzeigen, navigieren Sie im Citrix ADM Dashboard zum jeweiligen Analysemodus.

Um beispielsweise den Diagnosebericht für Web Insight anzuzeigen, navigieren Sie zu **Analytics > Web Insight**. Wählen Sie auf der Seite Web Insight das Symbol **Diagnose anzeigen** aus.



Sie können auch eine sofortige Diagnose ausführen, wenn Sie nach Problemen suchen möchten. Klicken Sie auf **Diagnose ausführen**. Wählen Sie die Instanzen aus, und wählen Sie " **Diagnose ausführen**".





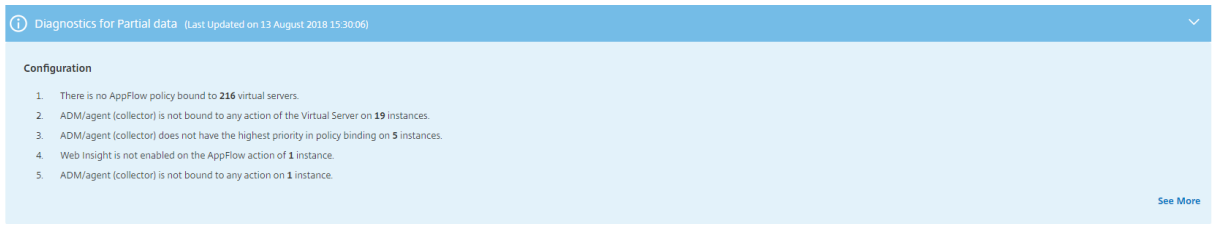
Analysieren des Diagnoseberichts

Die Self-Service-Diagnose zeigt den Diagnosebericht entweder in orangefarbenem oder blauem Hintergrund je nach Problemkritik an.

Diagnosebericht im orangefarbenen Hintergrund bedeutet eine höhere Kritikalität als der blaue Hintergrund.

Beispielsweise sind auf der Citrix ADC-Instanz fünf virtuelle Server konfiguriert. Wenn Sie die AppFlow Parameter auf virtuellen Servern nicht aktiviert haben, erhält Citrix ADM den Web Insight- und Security Insight-Datenverkehr nicht zur Analyse. Die Self-Service-Diagnose identifiziert die Konfigurationsprobleme als kritisch. Sie sehen die Diagnoseberichte in orangefarbenem Hintergrund in Web Insight und Security Insight Funktion.

Wenn Sie AppFlow auf einem der virtuellen Server aktiviert haben, empfängt Citrix ADM Daten für Analysen. Der Diagnosebericht wird in blauem Hintergrund angezeigt, da mindestens ein virtueller Server Datenverkehr zur Analyse sendet.

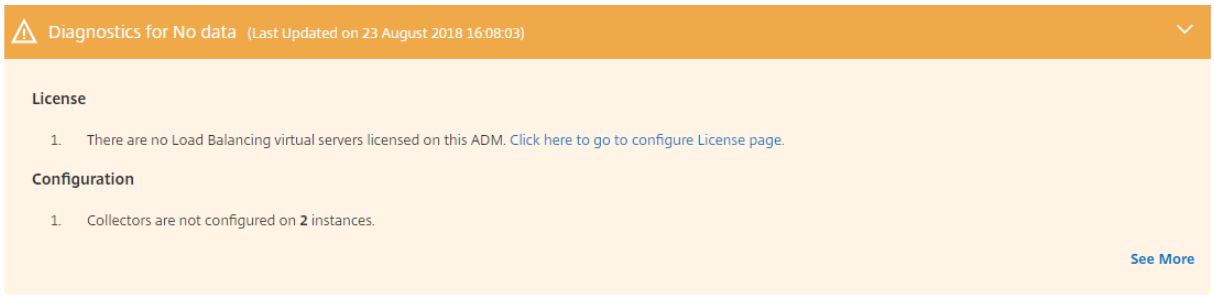


> **WICHTIG**
>
> Die Self-Service-Diagnose überprüft nicht den Datenfluss. Es prüft nur auf Lizenz- oder Konfigurationsprobleme, die mit den angegebenen Analysefunktionen in den verwalteten Instanzen verknüpft sind. Manchmal werden keine Analysedaten angezeigt, da kein aktiver Datenverkehr über virtuelle Server fließt.

Der Diagnosebericht enthält eine Übersichtsseite und eine Detailinformationsseite.

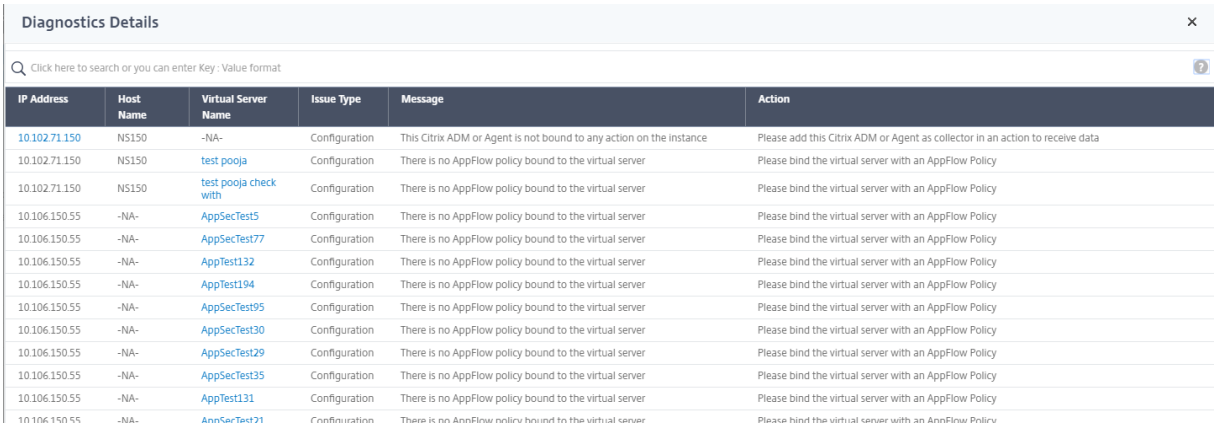
Die Übersichtsseite bietet einen Überblick über die Arten von Problemen - Lizenz oder Konfiguration. Die Seite kann Hyperlinks enthalten, die Sie zu den entsprechenden Konfigurationsseiten führen.

Wenn z. B. keine virtuellen Lastausgleichsserver lizenziert sind, enthält die Übersichtsseite einen Hyperlink, der Sie zur Seite **Systemlizenzen** weiterleitet.

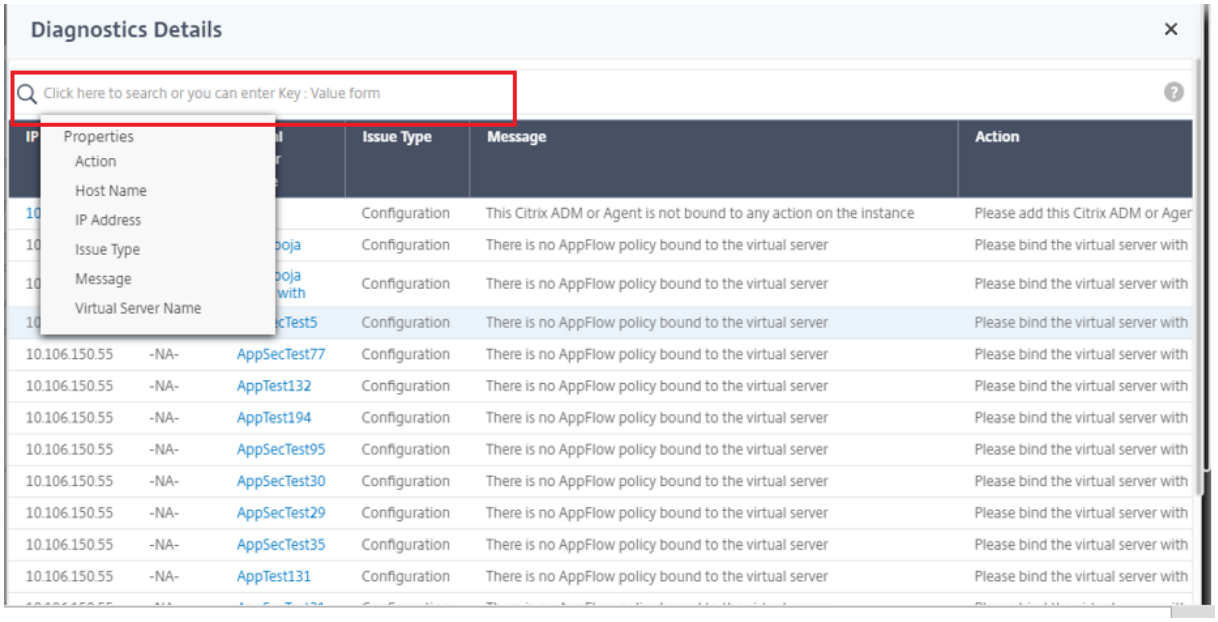


Um detaillierte Informationen zu den Problemen anzuzeigen, klicken Sie auf der Übersichtsseite auf **Mehr** anzeigen.

Die Detailinformationsseite enthält die vollständigen Informationen zu den Problemen und empfiehlt Maßnahmen, die Sie ausführen müssen. Sie können auf den Hyperlink für jedes Problem klicken, um die verwaltete Instanz oder den virtuellen Server zu konfigurieren.



Sie können die Probleme auch basierend auf der Aktion, dem Hostnamen, der IP-Adresse und dem Problemtyp usw. durchsuchen.



Nachdem Sie die Probleme behoben haben, müssen Sie eine sofortige Diagnose ausführen, um den neuesten Diagnosebericht zu generieren.

Web Insight

April 28, 2021

Mit Web Insight können Administratoren alle Webanwendungen überwachen, die von Citrix ADC-

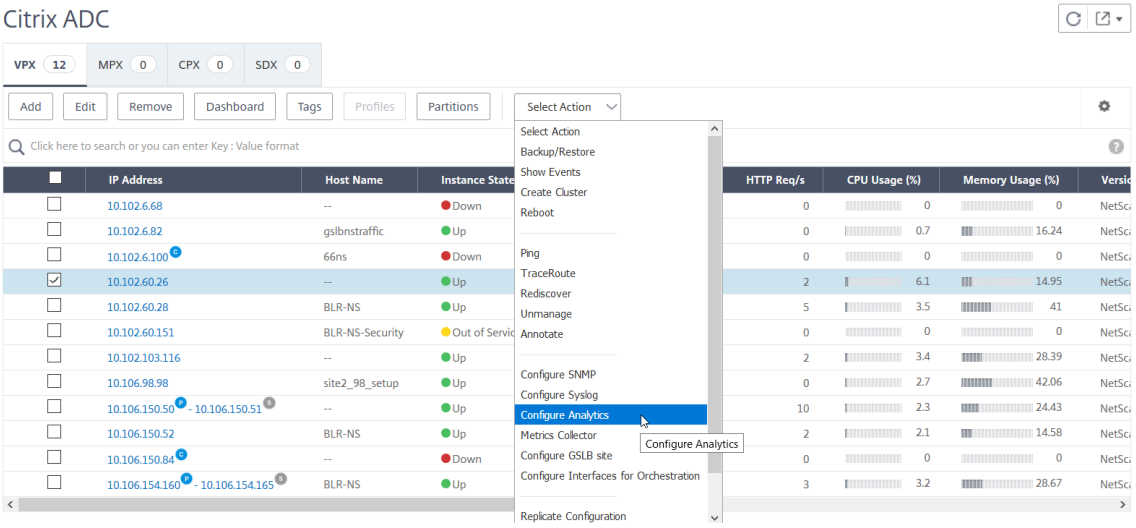
Instanzen bedient werden. Als Administrator erhalten Sie eine integrierte Echtzeitüberwachung der Anwendungen von Citrix ADC-Instanzen. Web Insight stellt wichtige Informationen wie Clientnetzwerklatenz und Server-Reaktionszeit bereit, um die Anwendungsleistung zu überwachen und zu verbessern. Die für die Analyse verwendeten Daten werden aus jeder HTTP-, HTTPS-Transaktion erfasst, die von der Citrix ADC-Instanz verarbeitet werden. Mit den Analysedaten können Sie die Leistung von Citrix ADC-Instanzen, Anwendungen, URL, Client und Server in Ihrer Umgebung analysieren.

Im Folgenden finden Sie einige der Anwendungsfälle, die Sie mit Web Insight anzeigen können:

- Die Liste der Clients mit hoher Latenz beim Zugriff auf eine Anwendung wie SharePoint
- Die Top-Anwendung, die die meisten Treffer innerhalb einer Stunde hatte
- Die Liste der Anwendungen und URLs, auf die von Clients zugegriffen wird
- Betriebssystem und Browser, die von einem bestimmten Client verwendet werden
- Die Anwendungen oder Server, die die meisten fehlerbezogenen Antworten senden
- Barrierefreiheitsprobleme mit einem bestimmten Client
- Probleme mit der Barrierefreiheit über wenige oder alle Anwendungen eines bestimmten Clients hinweg
- Einige Seiten einer Anwendung sind von einem bestimmten Client und vom Back-End-Server langsam
- Die Anwendung ist langsam, wenn Sie von einem bestimmten Client und von einem Back-End-Server aus aufgerufen werden

Sie können Web Insight für einen bestimmten virtuellen Server auf einer ausgewählten Instanz aktivieren, um den Datenverkehr in Ihrer Webanwendung zu überwachen. Das Web Insight-Feature stellt dann Statistiken für den virtuellen Server in Citrix ADM bereit. So aktivieren Sie Web Insight:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**, und wählen Sie die Citrix ADC-Instanz aus, für die Sie die Analyse aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.



3. Auf der Seite **Analytics auf virtuellen Servern konfigurieren**:

   a) Wählen Sie die virtuellen Server aus, die Sie Web Insight aktivieren möchten, und klicken Sie auf **Analytics aktivieren**

   Das Fenster **Analytics aktivieren** wird angezeigt.

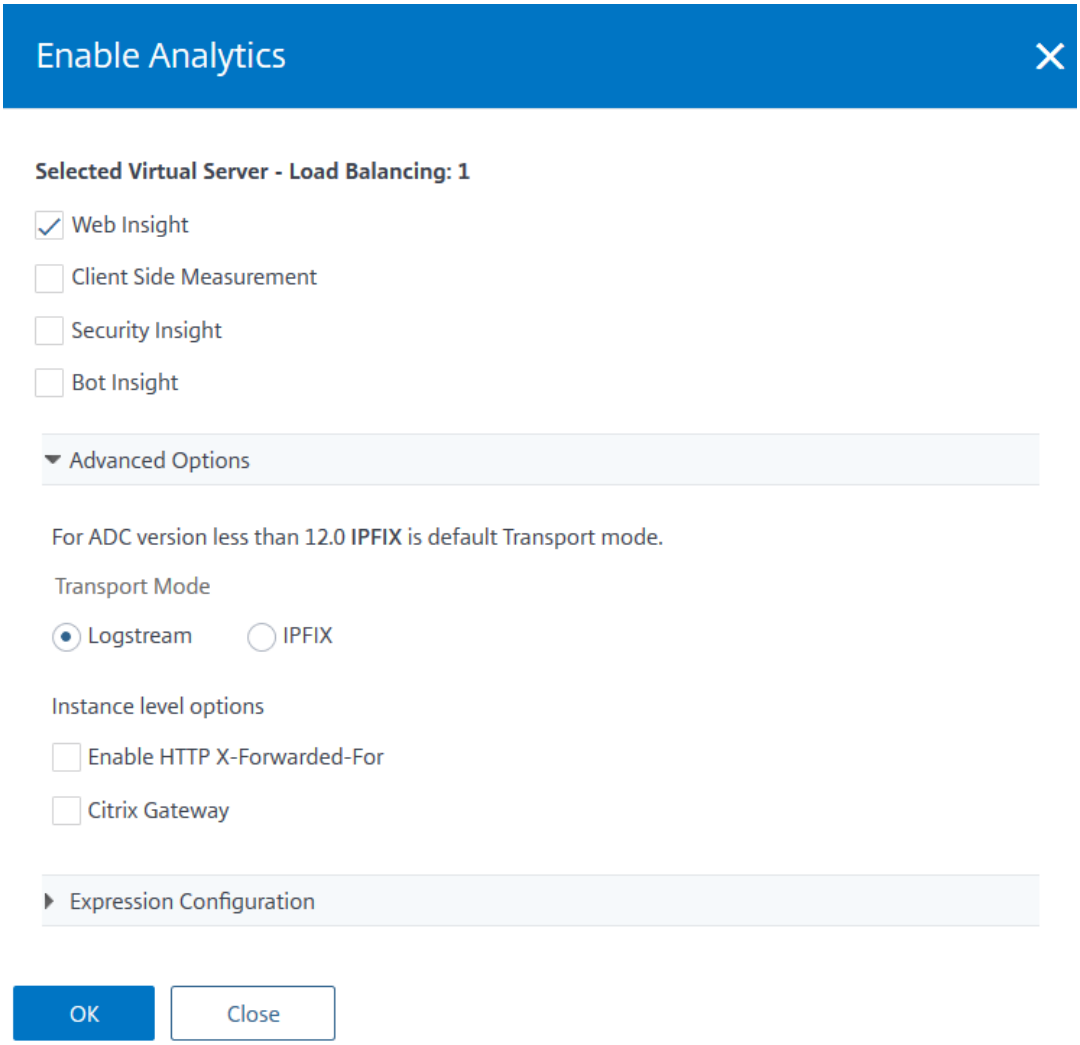
   b) **Web Insight** auswählen

   c) Wählen Sie unter **Erweiterte Optionen** die Option **Logstream** oder **IPFIX** als Transportmodus aus.

   > **Hinweis**
   >
   > Für Citrix ADC 12.0 oder früher ist **IPFIX** die Standardoption für den Transportmodus. Für Citrix ADC 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.
   >
   > Weitere Informationen zu **IPFIX** und **Logstream** finden Sie unter **Übersicht über den Logstream**.

   d) Der Ausdruck ist standardmäßig true

   e) Klicken Sie auf **OK**



Analysieren von Problemen mit Webanwendungen

Eines der häufigsten Probleme, die ein Administrator identifizieren muss, sind die Latenzprobleme. Als Administrator müssen Sie herausfinden, ob das Latenzproblem vom Servernetzwerk, dem Clientnetzwerk oder dem Server-Antwortzeit stammt. Mithilfe von Citrix ADM können Sie diese Informationen identifizieren, indem Sie zu **Analytics** > **Web Insight** navigieren.

Wenn Sie zu **Analytics** > **Web Insight** navigieren, werden die Citrix ADC-Instanzen angezeigt, die mit Web Insight aktiviert sind. Sie können die detaillierten Informationen für die Instanzen wie IP-Adresse, Hostname, Gesamtzahl der Treffer und Bandbreite anzeigen.

In der Liste können Sie die Zeitdauer auswählen, um die Einblicke für die Instanzen anzuzeigen.

Sie können den Schieberegler auch verwenden, um die Zeitdauer anzupassen, und klicken Sie auf **Los**, um die Ergebnisse anzuzeigen.

Wenn Sie auf das Diagramm oder die IP-Adresse der Instanz klicken, werden die detaillierten Informationen über die Instanz angezeigt. Sie können Einblicke für Folgendes anzeigen:

- **Gesamtzahl der Treffer**
- **Bandbreite**
- **Anwendungen**
- **Domänen**
- **URLs**
- **HTTP-Anforderungsmethoden**
- **HTTP-Antwortstatus**
- **Kunden**
- **Server**
- **Betriebssysteme**
- **Benutzeragents**

Sie können auch **Web Insight-Entitäten** auswählen, für die Sie Berichte auf der GUI anzeigen möchten.

1. Navigieren Sie zu **Analytics** > **Web Insight** > **Einstellungen**.
2. Klicken Sie auf **Analytics-Datensatzprotokolle konfigurieren**.
3. Wählen Sie unter **Web Insight-Berichtseinstellungen**die Entitäten aus, die Sie Berichte auf der GUI anzeigen möchten.
4. Klicken Sie auf **OK**.

Um eine Aufgliederung für weitere Analysen durchzuführen, können Sie auf jede Insight-Kategorie unter Web Insight in der GUI klicken. Wenn Sie beispielsweise Probleme für die konfigurierten Server überprüfen möchten:

1. Navigieren Sie zu **Analytics** > **Web Insight** > **Server**.
2. Die Seite Server wird mit allen konfigurierten Servern angezeigt.
3. Klicken Sie im Diagramm auf die IP-Adresse. Sie können auch in der Tabelle auf die IP-Adresse klicken.

   Die Detailansicht für den ausgewählten Server wird angezeigt. In dieser Ansicht können Sie nach mehreren Erkenntnissen suchen, z. B.:

   - Gesamtzahl der vom Server empfangenen Treffer
   - Bandbreite

- Serververarbeitungszeit
- Servernetzwerklatenz
- Virtuelle Server, die für den Server konfiguriert sind
- Gesamtzahl der Clients, die auf den Server zugreifen
- Gesamtzahl der vom Server bereitgestellten Antwortcodes

Anwendungsfall 1 - Interner Serverfehler

Betrachten Sie ein Szenario, dass Ihre Benutzer Unzugänglichkeit Fehler 500 für Ihre Webanwendung haben. Der Fehler 500 (Not Found) ist HTTP-Antwortstatusfehler, der auf ein Problem auf dem Webserver hinweist, aber der Server gibt das Problem nicht explizit an. Um das eigentliche Problem zu identifizieren und einen Drilldown durchzuführen:

1. Navigieren Sie zu **Analytics** > **Web Insight** > **Antwortstatus**.

   Die Dashboard-Seite wird angezeigt. Das Dashboard stellt Ihnen die Metriken zur Verfügung, mit denen Sie den Erfolg und Fehler der verarbeiteten HTTP-Transaktionen analysieren können.

2. Klicken Sie im Diagramm auf **Nicht gefunden**.
3. Führen Sie einen Bildlauf nach unten aus, um das **Serverdiagramm**anzuzeigen, und wählen Sie in der Liste **Filtern nach**die Option **Servernetzwerklatenz**aus.

   Das Diagramm zeigt an, dass jeder Anwendungsserver ein Problem beim Abrufen der Webanwendung hatte und daher die Antwortzeit für Webserver erhöht wird. Das Problem kann auftreten, dass der Webserver nicht auf Anfragen von einem Server reagiert.

Anwendungsfall 2 - Benutzer mit langsamem Zugriff auf die Webanwendung

Betrachten Sie ein Szenario, dass Ihre Webanwendung über 10 verschiedene Webserver gehostet wird. Wenn mehrere Benutzer gleichzeitig auf die Anwendung zugreifen, kann es bei einem oder mehreren Benutzern zu einer langsamen Anwendung kommen. Als Administrator müssen Sie die folgenden Szenarien analysieren, um die Ursache des Problems zu verstehen:

Szenario 1 - Serververarbeitungszeit:

Wenn mehrere Anfragen gleichzeitig auf die 10 verschiedenen Webserver treffen, unterscheidet sich die zum Laden der Anfrage aufgeforderte Zeit basierend auf:

- Anzahl der Anforderungen in der Warteschlange.
- Die Bandbreite, die von jeder Anforderung zur Verarbeitung der HTTP-Transaktion belegt wird.

  Das Serverdiagramm kann Ihnen helfen, die Verarbeitungszeit jedes Servers für die von den Servern verarbeitete Anforderung zu verstehen. Ebenso zeigt das Anwendungsdiagramm die Treffer, die Antwortzeit und die Bandbreite an, die von jeder HTTP-Transaktion belegt wird.

1. Navigieren Sie zu **Analytics** > **Web Insight** > **Server**.
2. Wählen Sie den Server aus dem Diagramm aus.
3. Klicken Sie auf **Serververarbeitungszeit**, um die Verarbeitungszeit des Servers zu analysieren.

Szenario 2 - Client-Latenz:

Die Antwortzeit und die Gesamtzahl der Treffer für die Anwendung können der Grund für die Langsamkeit des Anwendungszugriffs sein. Sie können die Latenz des Client-Netzwerks überprüfen und die Metriken für die Latenz des Client-Netzwerks analysieren. So analysieren Sie die Ursache:

1. Navigieren Sie zu **Analytics** > **Web Insight** > **Clients**.
2. Wählen Sie den Client aus dem Diagramm aus.
3. Klicken Sie auf **Clientnetzwerklatenz**, um die hohe Latenz zu analysieren.

   In diesem Beispiel können Sie als Administrator sehen, dass die Ursache des Problems aus dem Clientnetzwerk stammt, da die Clientnetzwerklatenz eine hohe Latenz anzeigt.

Anwendungsfall 3 - Langsamkeit beim Zugriff auf die Webanwendung

Betrachten Sie ein Szenario, dass Sie Webserver für Windows-Benutzer und Webserver für Mac-Benutzer haben, und Ihre Benutzer melden Langsamkeit beim Zugriff auf die Webanwendung. Als Administrator wissen Sie, dass Sie Folgendes haben:

- Konfiguriert einen virtuellen Content Switching-Server für Windows-Benutzer.
- Konfiguriert einen virtuellen Content Switching-Server für Mac-Benutzer.
- Konfigurierte zugeordnete Dienste, die an die virtuellen Server gebunden sind, um Anforderungen basierend auf Windows- und Mac-Benutzern umzuleiten.

So analysieren Sie die Ursache des Problems mit der Langsamkeit der Webanwendung:

1. Navigieren Sie zu **Analytics** > **Web Insight** > **Anwendungen**
2. Wählen Sie den virtuellen Content Switching-Server aus.
   Beispielsweise ist die `CSTOLBTarget` Anwendung im Image ein virtueller Content Switching-Server, der an andere virtuelle Lastausgleichsserver gebunden ist
3. Klicken Sie auf den virtuellen Content Switching-Server, um den anderen virtuellen Lastausgleichsserver anzuzeigen. Sie können auch auf den Anwendungsnamen in der Tabelle klicken.

Sie können weiter auf die gebundenen Lastausgleichsserver klicken, um die Web Insight-Details dieser Anwendungen anzuzeigen.

Analysieren von Erkenntnissen für Browser und Betriebssysteme

Mithilfe von Web Insight können Sie L7-Latenzprobleme trennen und die Nutzung mobiler Geräte verstehen. Als Administrator können Sie die Erkenntnisse dazu beitragen, unterschiedliche Betriebssystemzugaben in Ihrer Benutzerbasis zu verstehen.

Navigieren Sie zu **Analytics** > **Web Insight** > **Betriebssystem**, um zu sehen, warum der Benutzerzugriff langsam ist und ob dies auf Inkompatibilität in bestimmten Browsern zurückzuführen ist. Sie können auch sehen, welche Betriebssysteme auf bestimmten Clients verwendet werden und welche Browser aufgerufen werden. Sie können die gerenderte Zeit in den verschiedenen Browsern vergleichen und einen weiteren Drilldown zu einem bestimmten Browser erstellen, um zu ermitteln, welche Anwendungsseiten mit der höchsten Rendering-Zeit für diesen Browser verknüpft sind.

Sie können beispielsweise **Google Chrome** auswählen und die entsprechenden Rendering-Zeiten für die verschiedenen URL-Seiten für eine bestimmte Anwendung anzeigen.

Citrix ADC-Instanzen, die im Hochverfügbarkeitsmodus bereitgestellt werden

Citrix ADM stellt Berichte für ADC-Instanzen bereit, die im Hochverfügbarkeitsmodus bereitgestellt werden. Aggregierte Berichte für Instanzen im Hochverfügbarkeitsmodus werden in allen Analysen unterstützt.

Sie können auf den Namen der Instanzen klicken, die hochverfügbar sind, um weitere Details anzuzeigen.

Citrix ADC-Instanzen, die im Clustermodus bereitgestellt werden

Citrix ADM stellt Berichte für ADC-Instanzen bereit, die im Clustermodus bereitgestellt werden. Aggregierte Berichte für Instanzen im Clustermodus werden in allen Analysen unterstützt.

Sie können auch auf den **CLIP-Hostnamen** klicken, um alle Details zu den ADC-Instanzen anzuzeigen, die in einem Clustermodus bereitgestellt werden.

> **Hinweis**
>
> - Alle Daten, die zuvor vor dem Upgrade auf Citrix ADM 12.1 Build 503.x gesammelt wurden, werden weiterhin als unabhängige Berichte für den Zeitraum angezeigt, bis die Daten weiterhin bestehen.
> - Bei ADC-Instanzen, die im Clustermodus bereitgestellt werden, werden Observation Domain ID/Observation Domain Names durch CLIP Hostname und CLIP ersetzt. Alle zuvor gesammelten Daten melden weiterhin Observation Domain ID/Observation Domain Name.

Web Insight-Geokarten-Konfiguration

Die Geomaps-Funktion in Citrix ADM zeigt die Verwendung von Webanwendungen an verschiedenen geografischen Standorten auf einer Karte an. Administratoren können diese Informationen verwenden, um die Trends bei der Anwendungsnutzung und bei der Kapazitätsplanung zu verstehen.

Die Geo-Map bietet Informationen zu den folgenden Kennzahlen, die für ein Land, einen Bundesstaat und eine Stadt spezifisch sind:

- Treffer insgesamt: Gesamtzahl der Zugriffe auf eine Anwendung.
- Bandbreite: Gesamtbandbreite, die während der Bearbeitung von Clientanforderungen verbraucht wird
- Antwortzeit: Durchschnittliche Zeit für das Senden von Antworten auf Clientanforderungen.

Geomaps liefern Informationen, die verwendet werden können, um verschiedene Anwendungsfälle wie die folgenden:

- Region mit der maximalen Anzahl von Clients, die auf eine Anwendung zugreifen
- Region mit der höchsten Reaktionszeit
- Region, die die größte Bandbreite verbraucht

Citrix ADM **aktiviert automatisch** Geomaps für private IP-Adressen oder öffentliche IP-Adressen, wenn Sie **Web Insight**aktivieren.

Erstellen eines privaten IP-Blocks

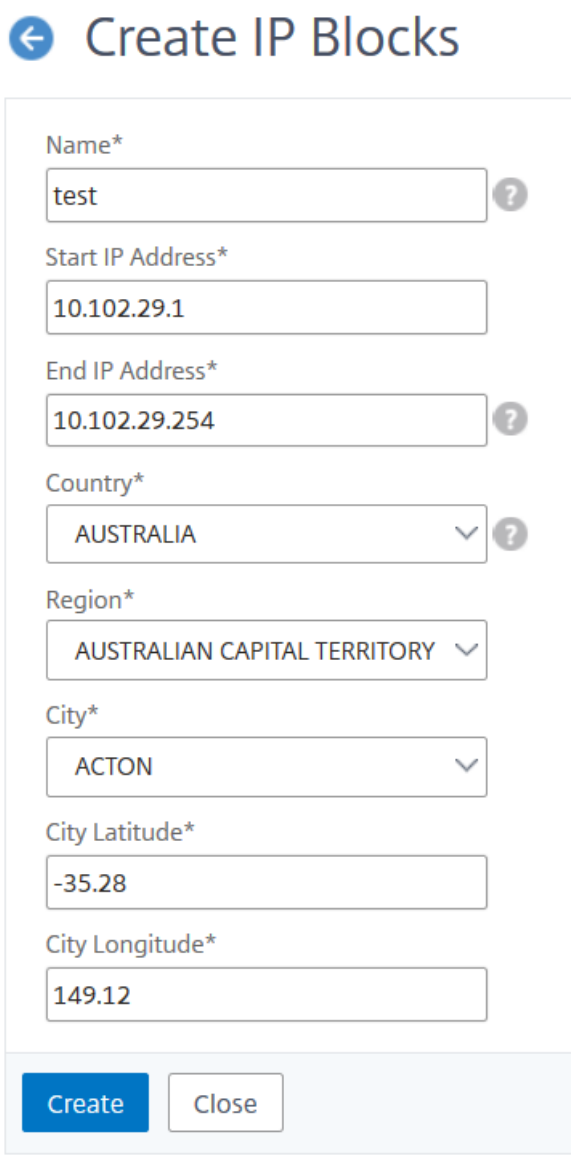
Citrix ADM kann den Clientstandort erkennen, wenn die private IP-Adresse des Clients zum Citrix ADM Server hinzugefügt wird. Wenn beispielsweise die IP-Adresse eines Clients in den Bereich eines privaten IP-Adressblocks fällt, der mit Stadt A verknüpft ist, erkennt Citrix ADM, dass der Datenverkehr von Stadt A für diesen Client stammt.

So erstellen Sie einen IP-Block:

1. Navigieren Sie in Citrix ADM zu **Analytics** > **Einstellungen** > **IP-Blöcke**, und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie auf der Seite **IP-Blöcke erstellen** die folgenden Parameter an:
    - **Name**. Geben Sie einen Namen für den privaten IP-Block an
    - **IP-Adresse starten**. Geben Sie den niedrigsten IP-Adressbereich für den IP-Block an.
    - **IP-Adresse beenden**. Geben Sie den höchsten IP-Adressbereich für den IP-Block an.
    - **Land**. Wählen Sie das Land aus der Liste aus.
    - **Region**. Basierend auf dem Land wird die Region automatisch ausgefüllt, aber Sie können Ihre Region auswählen.

- **Stadt**. Basierend auf der Region wird die Stadt automatisch ausgefüllt, aber Sie können Ihre Stadt auswählen.
- **Stadt Breitengrad** und **Stadt Längengrad**. Je nach ausgewählter Stadt werden Breiten- und Längengrad automatisch ausgefüllt.

3. Klicken Sie zum Abschluss auf **Erstellen**.

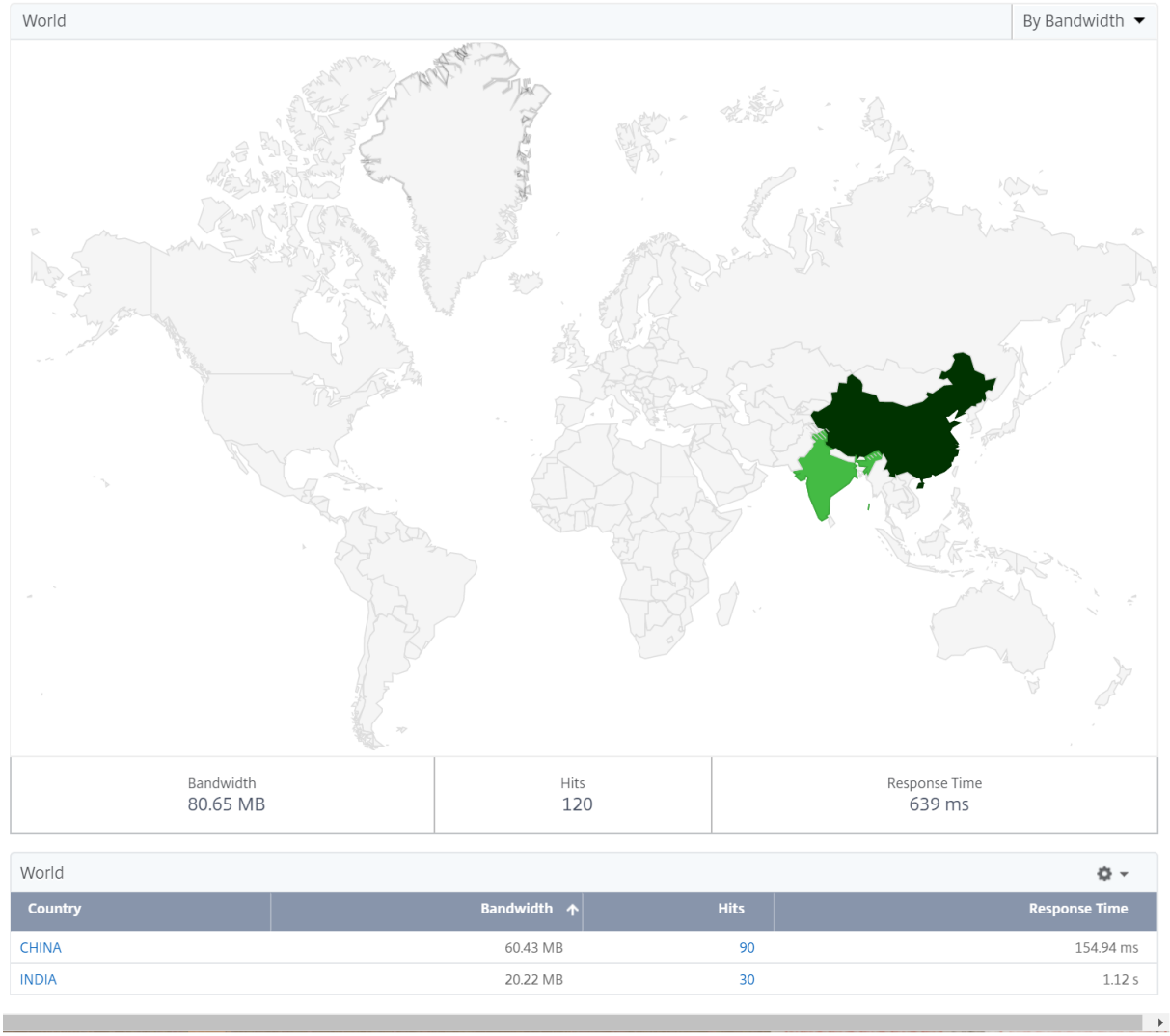


Öffentliche IP-Blöcke

Citrix ADM kann den Standort des Clients auch erkennen, wenn der Client eine öffentliche IP-Adresse verwendet. Citrix ADM verfügt über eine integrierte CSV-Datei, die dem Speicherort basierend auf dem Client-IP-Adressbereich entspricht. Für die Verwendung des öffentlichen IP-Blocks besteht die einzige Anforderung darin, dass Sie die Erfassung von **Geodaten aktivieren** auf der Seite “Configure Insight”

aktivieren müssen.

> Hinweis
>
> Citrix ADM benötigt eine Internetverbindung, um die Geomaps für einen bestimmten geografischen Standort anzuzeigen. Eine Internetverbindung ist auch erforderlich, um die GeoMap in den Formaten PDF-, PNG- oder JPG-Format zu exportieren.



So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. So planen Sie den Bericht täglich, wöchentlich oder monatlich und senden Sie den Bericht per E-Mail oder Puffernachricht.

Hinweis

- Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Schwellenwerte konfigurieren

Sie können Schwellenwerte erstellen und benachrichtigt werden, wenn der Schwellenwert verletzt wird. In einer typischen Bereitstellung können Sie Schwellenwerte auf Folgendes festlegen:

- Verfolgen verschiedener Anwendungsmetriken
- Erleichterung der Planung
- Werden Sie benachrichtigt, wenn der Anwendungsmetrikwert den eingestellten Schwellenwert überschreitet

So konfigurieren Sie den Schwellenwert:

1. Navigieren Sie zu **Analytics** > **Einstellungen** > **Schwellenwerte**.
2. Klicken Sie auf der Seite **Schwellenwerte** auf **Hinzufügen**.

   Die Seite **Schwellenwert erstellen** wird angezeigt.
3. Geben Sie die folgenden Details an:
   a) **Name** - Geben Sie einen Namen zum Erstellen eines Ereignisses an.
   b) **Traffic Type** - Wählen Sie in der Liste WEB aus.
   c) **Entity** - Wählen Sie in der Liste die Kategorie oder den Ressourcentyp aus. Standardmäßig wird Anwendungen als Entität ausgewählt.
   d) **Referenzschlüssel** - Ein Referenzschlüssel wird automatisch basierend auf dem ausgewählten Datenverkehrstyp und der ausgewählten Entität generiert.
   e) **Dauer** - Wählen Sie in der Liste das Zeitintervall aus, für das Sie die Entität überwachen möchten. Sie können die Entitäten für eine Stunde, für einen Tag oder für eine Woche überwachen.
   f) Erstellen **Sie im Abschnitt Regel konfigurieren** eine Regel, indem Sie die Metrik, einen erforderlichen Komparator auswählen und einen Schwellenwert angeben.
   g) Wählen Sie im Abschnitt **Benachrichtigungseinstellungen** die Option **Schwellenwert aktivieren** und den Warnmodus, für den Sie die Warnungen abrufen möchten.
4. Klicken Sie auf **Erstellen**.

SSL Insight

April 28, 2021

SSL Insight bietet Einblick in sichere Webtransaktionen (HTTPS) und ermöglicht IT-Administratoren, alle vom Citrix ADC bereitgestellten sicheren Webanwendungen zu überwachen, indem sie eine integrierte Echtzeit- und historische Überwachung sicherer Webtransaktionen bereitstellen. Mit dieser Sichtbarkeit kann der Administrator Folgendes beurteilen:

- **Bestimmen Sie die Auswirkungen der Konfigurationsänderung auf die Kundennutzung**. Der Administrator kann die Auswirkungen auf Clients verstehen, wenn er eine Konfigurationsänderung wie das Deaktivieren von SSLv3 oder das Entfernen einer Verschlüsselung wie RC4-MD5 vornimmt. Dies kann durch Bewertung der historischen Transaktionsdaten auf diesem Protokoll und Chiffre erfolgen.
- **Quantifizieren der Client-Leistung**. Der Administrator kann die Auswirkungen auf die Antwortzeit der Anwendung basierend auf den verwendeten SSL-Verschlüsselungen/-Protokollen oder den ausgehandelten Zertifikaten verstehen.
- **Anwendungssicherheit**. Prüfen Sie, ob eine der Anwendungen Transaktionen mit niedrigen Sicherheitsprotokollen, Verschlüsselungen oder einer schwachen Schlüsselstärke ausgeführt wird.

Wenn SSL Analytics auf einer ADC-Instanz aktiviert ist, werden SSL-Statistiken für jede SSL-Transaktion aufgezeichnet und protokolliert. Die Statistiken zeigen die Details des SSL-Flows. Außerdem wird jede erfolgreiche Verbindung von Citrix Application Delivery Management (ADM) protokolliert und angezeigt.

SSL Insight stellt die folgenden wichtigen Informationen bereit, die von Citrix ADM Analytics angezeigt werden:

- SSL-Protokollversion ausgehandelt
- Chiffre ausgehandelt, und die Verschlüsselungsstärke
- Signatur-Hash-Algorithmus des verwendeten Zertifikats
- Typ und Größe des Zertifikats
- SSL Frontend- und Backend-Fehler

> **Hinweis**
>
> Bei erfolgreichen SSL-Verbindungen erfolgt die SSL-AppFlow Protokollierung am Ende jeder Transaktion.

Voraussetzungen

- Auf der Citrix ADC-Instanz, auf der Sie SSL Insight konfigurieren möchten, muss die Citrix ADC -Softwareversion 11.1 51.21 und höher ausgeführt werden. Führen Sie die folgenden Befehle auf

der ADC-Instanz aus, auf der 11.1 51.21 ausgeführt wird, um **Logstream** als Transporttyp für SSL Insight zu aktivieren.

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the ADM>`

   Wählen Sie für ADC-Instanzen mit Version 12.0 und höher als Transportart **Logstream** aus, während Sie AppFlow von ADM aktivieren.

- Citrix ADM Version und -Build müssen gleich oder höher sein als die Citrix ADC Version und -Build. Wenn Sie beispielsweise Citrix ADM 11.1 Build 61.7 installiert haben, stellen Sie sicher, dass Sie Citrix ADC 11.1 Build 60.14 oder früher installiert haben.

Konfigurieren von SSL Insight

SSL Insight Metriken sind in Web Insight-Berichten enthalten, wenn Sie die folgenden Elemente aktivieren:

- Aktivieren Sie AppFlow for Web Insight für jede ADC-Instanz.
- Aktivieren Sie den ULFD-Modus für jede ADC-Instanz.
- Aktivieren Sie die erforderlichen AppFlow Parameter für jede ADC-Instanz.

Ermöglichen der Einsicht

> **Hinweis**
>
> Sie können die AppFlow Funktion entweder von Citrix ADM oder von jeder ADC-Instanz aus aktivieren.

Aktivieren der AppFlow Funktion von Citrix ADM

1. Navigieren Sie zu **Netzwerke** > **Instanzen**, und wählen Sie die ADC-Instanz aus, für die Sie die Analyse aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
3. Auf der Seite **Analytics auf virtuellen Servern konfigurieren**:
   a) Wählen Sie die virtuellen Server aus, die Sie Web Insight aktivieren möchten, und klicken Sie auf **Analytics aktivieren**

      Das Fenster **Analytics aktivieren** wird angezeigt.

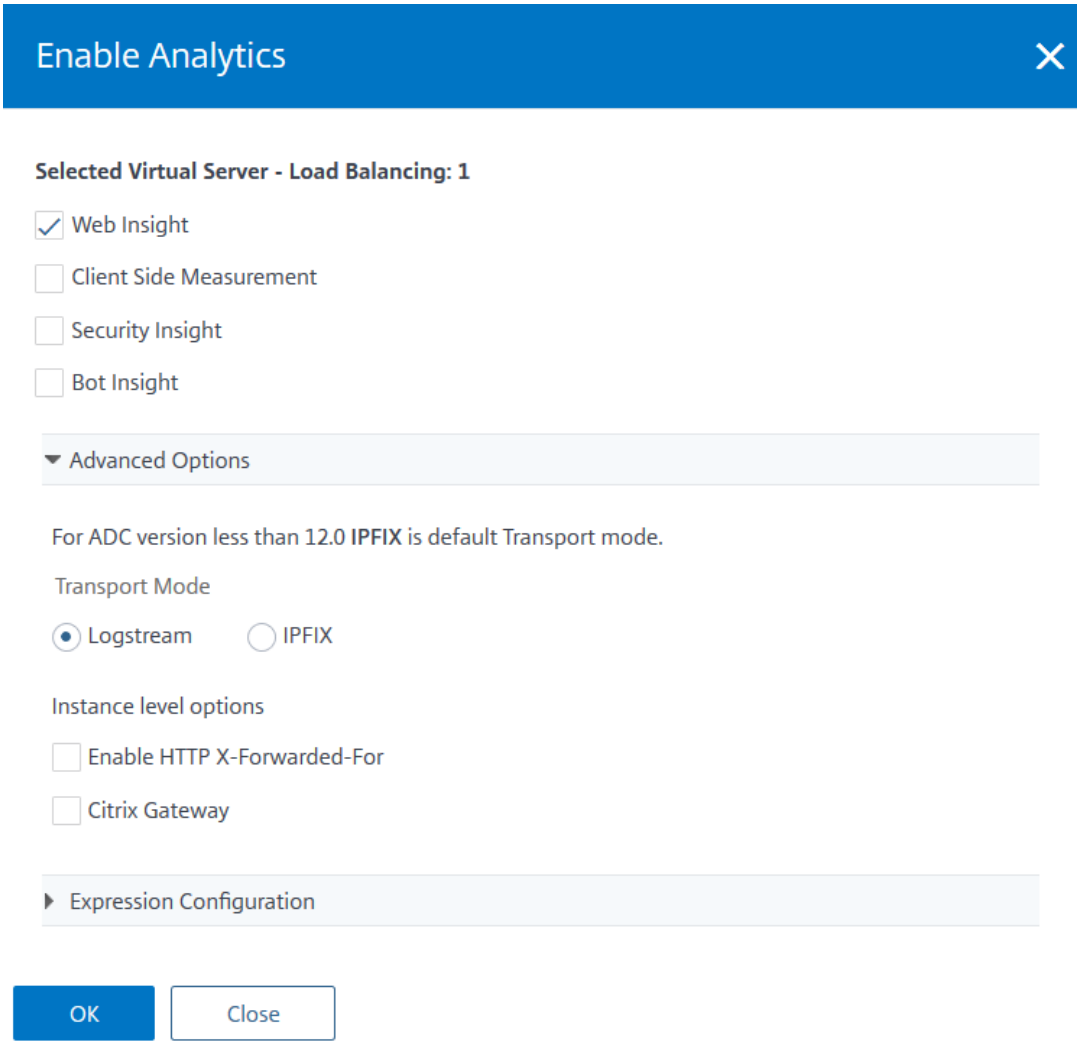
   b) **Web Insight** auswählen

   c) Wählen Sie unter **Erweiterte Optionen** die Option **Logstream** oder **IPFIX** als Transportmodus aus.

> **Hinweis**
>
> Für Citrix ADC 12.0 oder früher ist **IPFIX** die Standardoption für den Transportmodus. Für Citrix ADC 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.
>
> Weitere Informationen zu **IPFIX** und **Logstream** finden Sie unter **Übersicht über den Logstream**.

d) Der Ausdruck ist standardmäßig true

e) Klicken Sie auf **OK**



> **Hinweis**
>
> Sie können die Datenerfassung auf einem virtuellen Server nicht aktivieren, wenn der Betriebszustand des virtuellen Servers nicht UP ist.

Aktivieren der AppFlow Funktion mithilfe der ADC-GUI

Navigieren Sie in der GUI einer ADC-Instanz zu **Konfiguration** > **System** > **Einstellungen**, klicken Sie auf **Erweiterte Funktionen konfigurieren** und wählen Sie **AppFlow** aus.

Aktivieren des ULFD-Modus

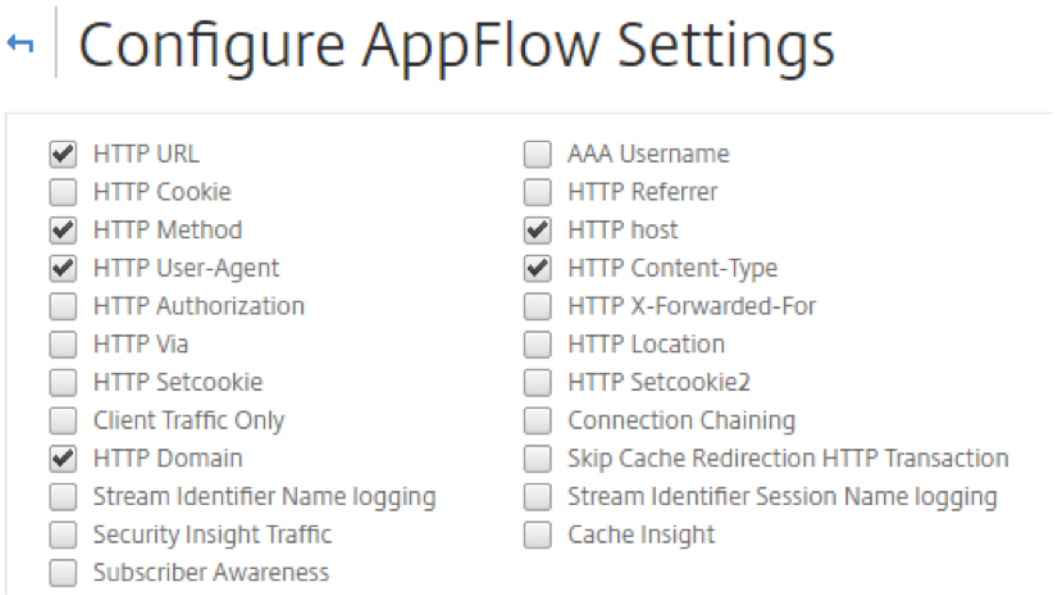
Nachdem Sie den ULFD-Modus für die ADC-Instanzen aktiviert haben, auf denen die virtuellen Server konfiguriert sind, streamt der ULFD-Server die Analysedaten von den ADC-Instanzen an Citrix ADM.

SSL Insight-Parameter aktivieren

Auf jeder ADC-Instanz müssen Sie einige HTTP-Parameter aktivieren, um SSL Insight-Datensätze in Citrix ADM anzuzeigen.

Aktivieren von SSL Insight-Parametern über das ADC-Konfigurationsdienstprogramm

1. Navigieren Sie zu **Konfiguration** > **System** > **AppFlow**, und klicken Sie auf **AppFlowSettings ändern**.
2. Aktivieren Sie die folgenden Kontrollkästchen: **HTTP-Domäne**, **HTTP-Host**, **HTTP-Methode**, **HTTP-URL**, **HTTP-User-Agent**, **HTTP-Inhaltstyp**.
3. Klicken Sie auf **OK**.



Anzeigen der SSL Insight-Metriken

SSL Insight-Metriken in Citrix ADM bieten einen detaillierten Überblick über die Performance der SSL-Transaktionen, die von den ADC-Instanzen bedient werden. Sie können die SSL Insight-Metriken auf Client-, Server- oder Anwendungsebene sowie die Kennzahlen der SSL-Erfolgs- und Fehlertransaktionen anzeigen. Mithilfe dieser Metriken können Sie Ihre ADC-HTTPS-Einstellungen und SSL-Zertifikateinstellungen analysieren und optimieren und Leistungsprobleme nachverfolgen.

> **Hinweis**
>
> Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, Zugriff auf Anwendungsebene für die Gruppe gewähren und Benutzer der Gruppe zuweisen. Citrix ADM Analytics unterstützt jetzt virtuelle IP-Adressen basierte Autorisierung. Ihre Benutzer können jetzt Berichte für alle Insights nur für die Anwendungen (virtuelle Server) anzeigen, für die sie autorisiert sind. Weitere Informationen zu Gruppen und dem Zuweisen von Benutzern zur Gruppe finden Sie unterKonfigurieren von Gruppen auf Citrix ADM.

Überwachung von SSL Insight-Metriken in Citrix ADM

1. Navigieren Sie auf der Registerkarte **Analytics** zu Web Insight, und klicken Sie auf den Knoten **Client**, **Server**oder **Anwendung**, um die Metriken zu Clients, dem Server bzw. den Anwendungen anzuzeigen.
2. Wählen Sie im linken oberen Bereich im Menü den Zeitrahmen aus, dessen Metriken Sie anzeigen möchten. Sie können den Zeitrahmen mithilfe des Zeitrahmen-Schiebereglers anpassen. Klicken Sie auf **Go**.
3. Die SSL Insight-Metriken werden als Kreisdiagramme angezeigt, auf die Sie klicken können, um weitere Details zu erhalten.

   > **Hinweis**
   >
   > Die Kreisdiagramme zeigen die Metriken aller Anwendungen, Clients oder Server an.

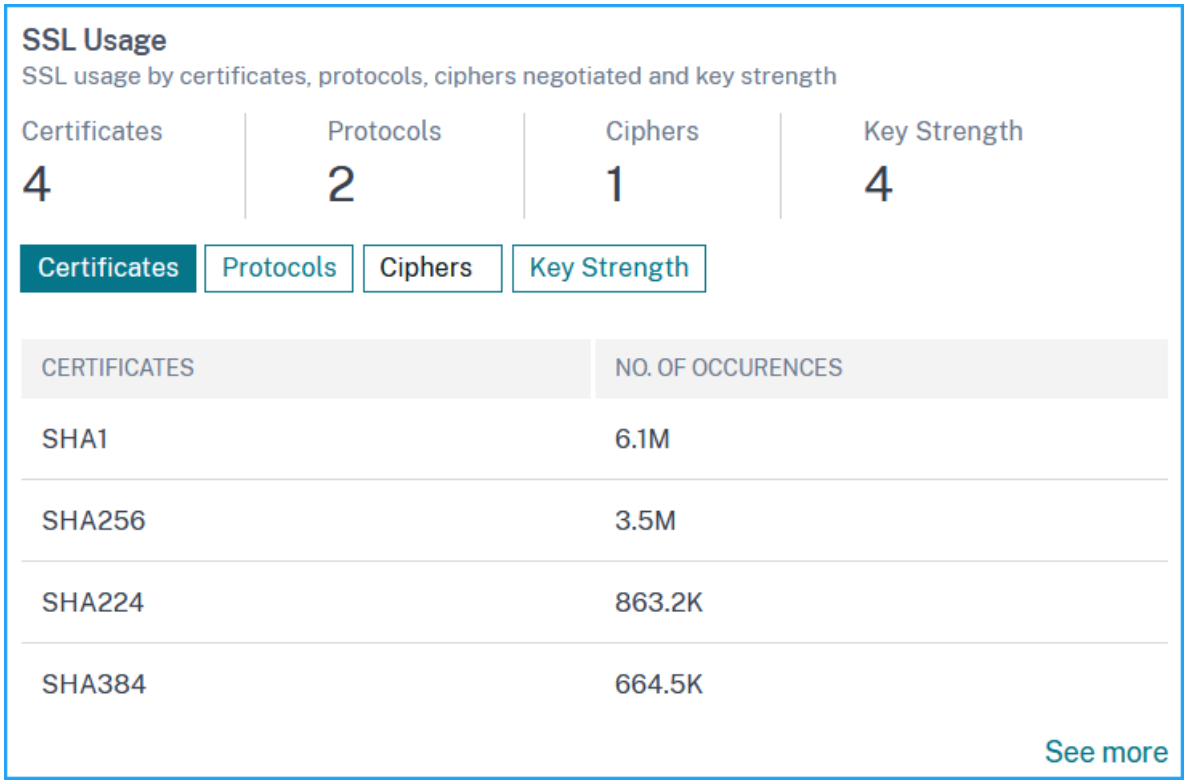
4. Um Details für eine bestimmte Anwendung, einen bestimmten Client oder einen bestimmten Server anzuzeigen, klicken Sie auf den entsprechenden Wert im Balkendiagramm.
5. Um die fehlgeschlagenen SSL-Transaktionen anzuzeigen, wählen Sie im Abschnitt SSL das Optionsfeld im Abschnitt SSL aus.

Anwendungsfall: Erhalten Sie einen Überblick über die SSL-Transaktionen von Anwendungen, Clients oder Servern

Im folgenden Anwendungsfall wird beschrieben, wie Sie SSL Insight verwenden können, um die Verwendung verschiedener SSL-Parameter in Anwendungen, Clients und Servern zu bewerten und Sicherheitsmaßnahmen zu verbessern.

Beachten Sie, dass Sie über eine Reihe von Anwendungen verfügen, die SSL-Transaktionen (HTTPS) für die Kommunikation verwenden, und Sie Citrix ADM konfiguriert haben, um die SSL-Komponenten zu überwachen. Möglicherweise müssen Sie die Anwendungen häufig überprüfen, damit Sie sich zuerst auf die Anwendungen konzentrieren können, die die größte Aufmerksamkeit benötigen. Das SSL-Insight-Dashboard bietet eine Zusammenfassung der verschiedenen SSL-Parameter, die von Ihren Anwendungen über einen bestimmten Zeitraum Ihrer Wahl und für ein ausgewähltes ADC-Gerät verwendet werden. Sie werden folgendermaßen aufgelistet:

- SSL-Zertifikate
- SSL-Protokolle
- SSL-Verschlüsselung ausgehandelt
- SSL-Schlüsselstärke
- SSL-Fehler — Frontend
- SSL-Fehler — Back-End



Im folgenden Beispiel sehen Sie eine Liste der Clients (identifiziert durch ihre IP-Adressen) und die SSL-Zugriffe pro Client. Rechts können Sie auch die SSL-Parameter für alle Clients anzeigen.

Um SSL-Details für einen Client anzuzeigen, wählen Sie den Client im Balkendiagramm oder in der Tabelle unterhalb des Diagramms aus. Im folgenden Beispiel verwenden die Transaktionen des ausgewählten Clients ein SHA1-SSL-Zertifikat und vier Hauptprotokolle: TSLv1.2, TSLv1.1, TSLv1 und SSLv3. Sie können auch sehen, dass Chiffre verschiedener Stärken ausgehandelt wurden. Der Farbcode gibt die Stärke des SSL-Protokolls an, das Ihnen Informationen über schwache Chiffre und

starke Chiffre gibt.

Um die Informationen über die fehlgeschlagenen SSL-Transaktionen anzuzeigen, wählen Sie das Optionsfeld im Abschnitt **SSL**. SSL-Front-End- und Back-End-Fehler werden separat in zwei Kreisdiagrammen angezeigt. Im folgenden Beispiel können Sie anzeigen, dass die wichtigsten Back-End-SSL-Fehler Handshake-Fehler sind und die wichtigsten Front-End-SSL-Fehler Unzulässige Parameter sind.

HDX Insight

April 28, 2021

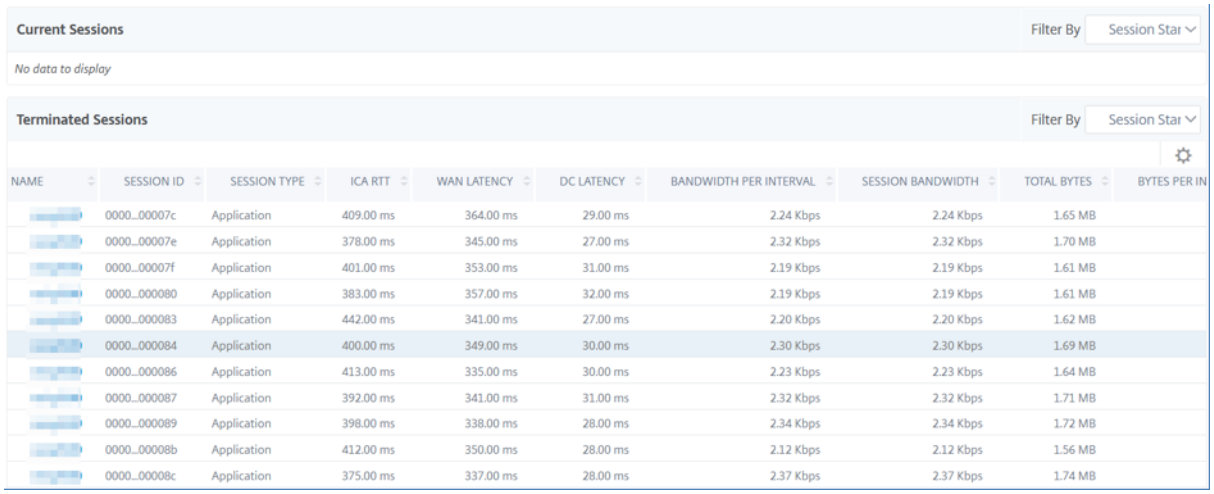
HDX Insight bietet End-to-End-Transparenz für HDX-Datenverkehr zu Citrix Virtual Apps and Desktops, die über Citrix ADC geleitet werden. Darüber hinaus können Administratoren Echtzeitmetriken für Client- und Netzwerklatenz, historische Berichte, End-to-End-Performance-Daten anzeigen und Leistungsprobleme beheben. Die Verfügbarkeit von Echtzeit- und historischen Sichtbarkeitsdaten ermöglicht es Citrix Application Delivery Management (ADM), eine Vielzahl von Anwendungsfällen zu unterstützen.

Damit alle Daten angezeigt werden, müssen Sie AppFlow auf Ihren virtuellen ADC Gateway-Servern aktivieren. AppFlow kann über das **IPFIX-Protokoll** oder die **Logstream-Methode** bereitgestellt werden.

> **Hinweis**
>
> Aktivieren Sie die folgenden Richtlinieneinstellungen, damit ICA Roundtrip Zeitberechnungen protokolliert werden können:
>
> - ICA Roundtrip Berechnung
> - ICA Roundtrip Berechnungsintervall
> - ICA Roundtrip Berechnung für Leerlaufverbindungen

Wenn Sie auf einen einzelnen Benutzer klicken, können Sie jede aktive oder beendete HDX-Sitzung sehen, die der Benutzer innerhalb des ausgewählten Zeitraums erstellt hat. Weitere Informationen umfassen mehrere Latenzstatistiken und während der Sitzung verbrauchte Bandbreite. Sie können auch Bandbreiteninformationen von einzelnen virtuellen Kanälen wie Audio, Druckerzuordnung und Clientlaufwerkzuordnung abrufen.

Sie können auch eine konsolidierte Ansicht aller aktiven und beendeten Sitzungen des Benutzers visualisieren.



Als Administrator ermöglicht Ihnen diese Ansicht Folgendes:

- Zeigen Sie alle Benutzerdetails in einer Einzelbereichs-Visualisierung an
- Eliminieren Sie die Komplexität bei der Auswahl der einzelnen Benutzer und beim Anzeigen der aktiven und beendeten Sitzungen

> **Hinweis**
>
> Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, Zugriff auf Anwendungsebene für die Gruppe gewähren und der Gruppe Benutzer zuweisen. Citrix ADM Analytics unterstützt jetzt virtuelle IP-Adressen basierte Autorisierung. Ihre Benutzer können jetzt Berichte für alle Insights nur für die Anwendungen (virtuelle Server) anzeigen, für die sie autorisiert sind. Weitere Informationen zu Gruppen und dem Zuweisen von Benutzern zur Gruppe finden Sie unterKonfigurieren von Gruppen auf Citrix ADM.

Sie können auch zu **HDX Insight** > **Anwendungen** navigieren und auf **Startdauer** klicken, um die Zeit für den Start der Anwendung anzuzeigen. Sie können auch den User Agent aller verbundenen Benutzer anzeigen, indem Sie zu **HDX Insight > Benutzer**navigieren.

> **Hinweis**
>
> HDX Insight unterstützt Admin-Partitionen, die in ADC-Instanzen konfiguriert sind, die auf Softwareversion 12.0 ausgeführt werden.

Die folgenden Thin Clients unterstützen HDX Insight:

- WYSE Windows-basierte Thin Clients
- WYSE Linux-basierte Thin Clients
- WYSE ThinOS-basierte Thin Clients
- 10ZiG Ubuntu-basierte Thin Clients

Identifizieren der Hauptursache für Probleme mit der langsamen Leistung

Szenario 1

Benutzer hat Verzögerungen beim Zugriff auf Citrix Virtual Apps and Desktops

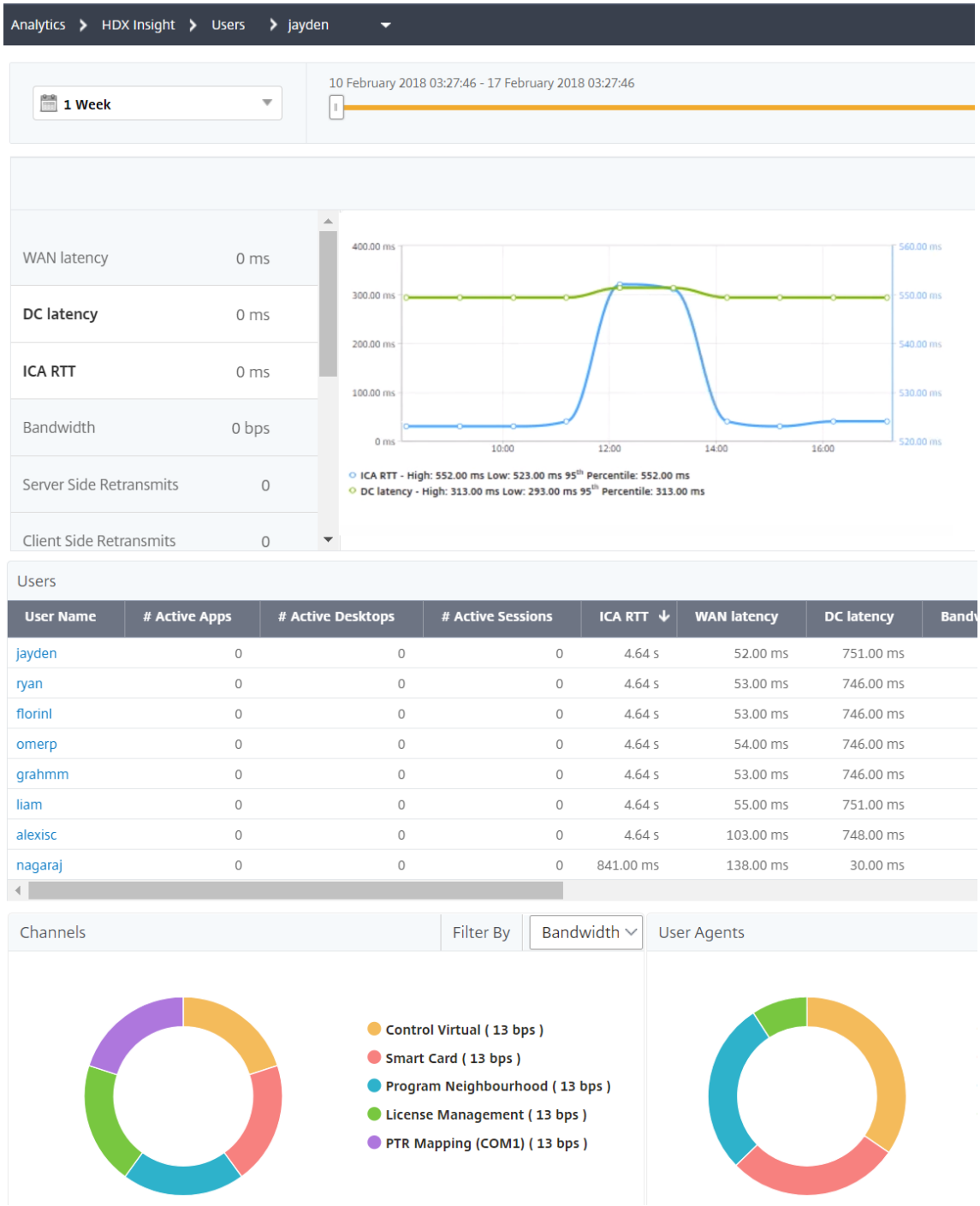
Die Verzögerungen können auf Latenz im Servernetzwerk, ICA-Verzögerungen aufgrund des Servernetzwerks oder Latenz im Clientnetzwerk zurückzuführen sein.

Um die Ursache des Problems zu identifizieren, analysieren Sie die folgenden Metriken:

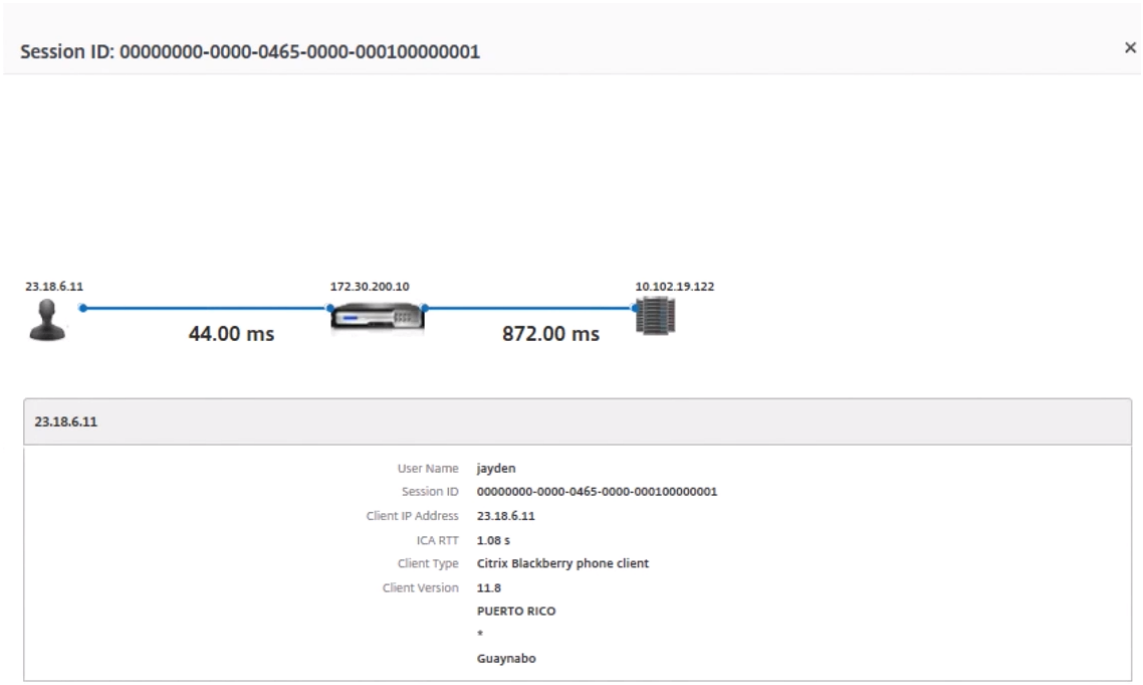
- WAN-Latenz
- DC-Latenz
- Hostverzögerung

So zeigen Sie die Client-Metriken an:

1. Navigieren Sie auf der Registerkarte **Analytics** zu **HDX Insight** > **Benutzer**.
2. Scrollen Sie nach unten, wählen Sie den Benutzernamen aus, und wählen Sie den Zeitraum aus der Liste aus. Der Zeitraum kann ein Tag, eine Woche, einen Monat sein, oder Sie können sogar den Zeitraum anpassen, für den Sie die Daten anzeigen möchten.
3. Das Diagramm zeigt die ICA-RTT- und DC-Latenzwerte des Benutzers für den angegebenen Zeitraum als Diagramm an.



4. Bewegen Sie in der Tabelle **Aktuelle Anwendungssitzungen** den Mauszeiger über den **RTT-Wert**, und notieren Sie sich die Hostverzögerung, die DC-Latenz und die WAN-Latenzwerte.
5. Klicken Sie in der Tabelle **Aktuelle Anwendungssitzungen** auf das Hopdiagrammsymbol, um Informationen über die Verbindung zwischen dem Client und dem Server anzuzeigen, einschließlich Latenzwerte.



Zusammenfassung:

In diesem Beispiel beträgt die **DC-Latenz** 751 Millisekunden, die **WAN-Latenz** 52 Millisekunden und **Hostverzögerungen** 6 Sekunden. Dies zeigt an, dass der Benutzer aufgrund der durchschnittlichen Latenz, die durch das Servernetzwerk verursacht wird, Verzögerung auftritt.

Szenario 2

Benutzer verzögert sich beim Starten einer Anwendung auf Citrix Virtual Apps oder Desktops

Die Verzögerung kann auf Latenz im Servernetzwerk, ICA-Verkehrsverzögerungen durch das Servernetzwerk, Latenz im Client-Netzwerk oder Zeit zurückzuführen sein, die zum Starten einer Anwendung erforderlich ist.

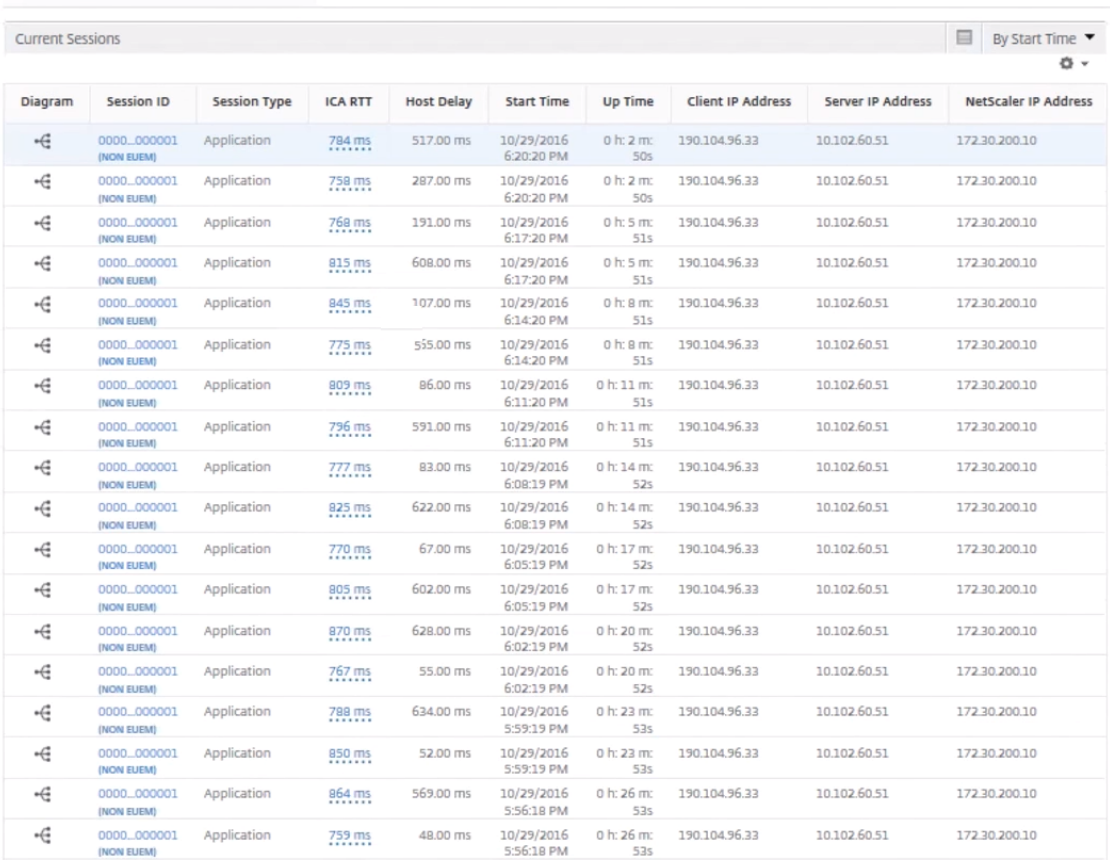
Um die Ursache des Problems zu identifizieren, analysieren Sie die folgenden Metriken:

- WAN-Latenz
- DC-Latenz
- Host-Verzögerung

So zeigen Sie die Benutzermetriken an:

1. Navigieren Sie auf der Registerkarte **Analytics** zu **HDX Insight** > **Benutzer**.
2. Scrollen Sie nach unten und klicken Sie auf den Benutzernamen
3. Notieren Sie sich in der grafischen Darstellung die WAN-Latenz-, DC-Latenz- und RTT-Werte für die jeweilige Sitzung.

4. Beachten Sie in der Tabelle **Aktuelle Anwendungssitzungen**, dass die Hostverzögerung hoch ist.



Current Sessions — By Start Time

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001 (NON EUEM)	Application	784 ms	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	758 ms	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	768 ms	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	815 ms	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	845 ms	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	775 ms	555.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	809 ms	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	796 ms	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	777 ms	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	825 ms	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	770 ms	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	805 ms	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	870 ms	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	767 ms	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	788 ms	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	850 ms	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	864 ms	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	759 ms	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

Zusammenfassung:

In diesem Beispiel beträgt die **DC-Latenz** 1 Millisekunde, die **WAN-Latenz** 12 Millisekunden, die **Hostverzögerung** beträgt jedoch 517 Millisekunden. Ein hoher RTT mit niedrigen DC- und WAN-Latenzen weist auf einen Anwendungsfehler auf dem Hostserver hin.

> **Hinweis:**
>
> HDX Insight zeigt auch mehr Benutzermetriken wie WAN-Jitter und serverseitige Retransmits an, wenn Sie Citrix ADM verwenden, auf dem Software 11.1 Build 51.21 oder höher ausgeführt wird. Um diese Metriken anzuzeigen, navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**, und wählen Sie einen Benutzernamen aus. Die Benutzermetriken werden in der Tabelle neben dem Diagramm angezeigt.

Geo-Map für HDX Insight

Die Geokarten-Funktion in Citrix ADM zeigt die Verwendung von Webanwendungen an verschiedenen geografischen Standorten auf einer Karte an. Als Administrator können Sie diese Informationen verwenden, um die Trends bei der Anwendungsnutzung und für die Kapazitätsplanung zu verstehen.

Die Geo-Map bietet Informationen zu den folgenden Kennzahlen, die für ein Land, einen Bundesstaat und eine Stadt spezifisch sind:

- Treffer insgesamt: Gesamtzahl der Zugriffe auf eine Anwendung.
- Bandbreite: Gesamtbandbreite, die während der Bearbeitung von Clientanforderungen verbraucht wird
- Antwortzeit: Durchschnittliche Zeit für das Senden von Antworten auf Clientanforderungen.

Geo-Map enthält Informationen, die verwendet werden können, um verschiedene Anwendungsfälle wie die folgenden zu behandeln:

- Region mit der maximalen Anzahl von Clients, die auf eine Anwendung zugreifen
- Region mit der höchsten Reaktionszeit
- Region, die die größte Bandbreite verbraucht

Citrix ADM **aktiviert automatisch** Geomaps für private IP-Adressen oder öffentliche IP-Adressen, wenn Sie **Web Insight**aktivieren.

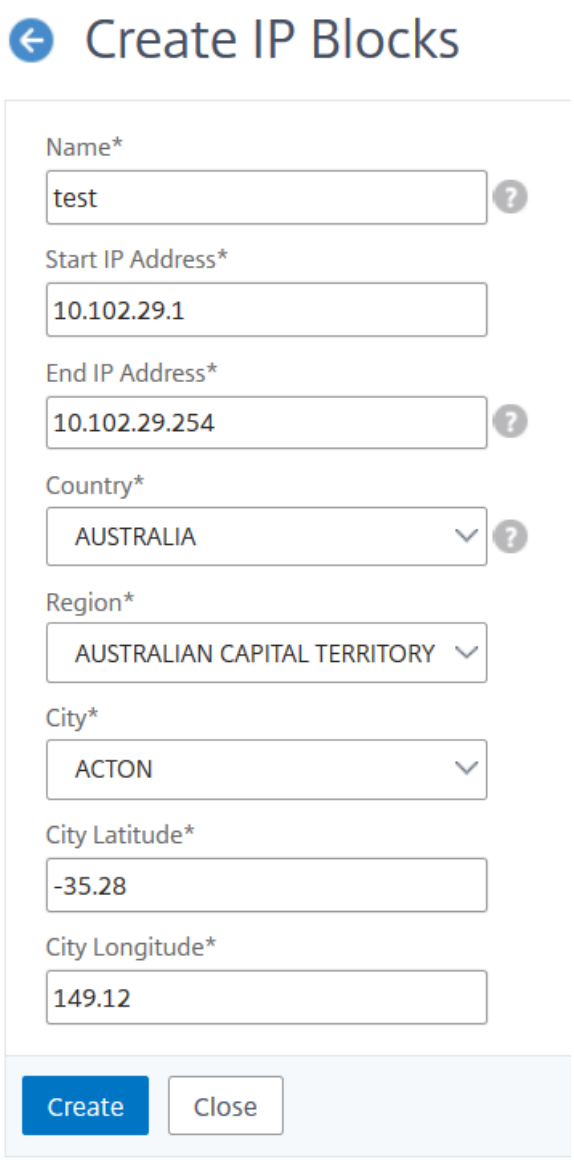
Erstellen eines privaten IP-Blocks

Citrix ADM erkennt den Speicherort eines Clients, wenn die private IP-Adresse des Clients zum Citrix ADM -Server hinzugefügt wird. Wenn beispielsweise die IP-Adresse eines Clients in den Bereich eines

privaten IP-Adressblocks fällt, der mit Stadt A verknüpft ist, erkennt Citrix ADM, dass der Datenverkehr von Stadt A für diesen Client stammt.

So erstellen Sie einen IP-Block:

1. Navigieren Sie in Citrix ADM zu **Analytics** > **Einstellungen** > **IP-Blöcke**, und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie auf der Seite **IP-Blöcke erstellen** die folgenden Parameter an:
   - **Name**. Geben Sie einen Namen für den privaten IP-Block an
   - **IP-Adresse starten**. Geben Sie den niedrigsten IP-Adressbereich für den IP-Block an.
   - **IP-Adresse beenden**. Geben Sie den höchsten IP-Adressbereich für den IP-Block an.
   - **Land**. Wählen Sie das Land aus der Liste aus.
   - **Region**. Basierend auf dem Land wird die Region automatisch ausgefüllt, aber Sie können Ihre Region auswählen.
   - **Stadt**. Basierend auf der Region wird die Stadt automatisch ausgefüllt, aber Sie können Ihre Stadt auswählen.
   - **Stadt Breitengrad** und **Stadt Längengrad**. Je nach ausgewählter Stadt werden Breiten- und Längengrad automatisch ausgefüllt.
3. Klicken Sie zum Abschluss auf **Erstellen**.

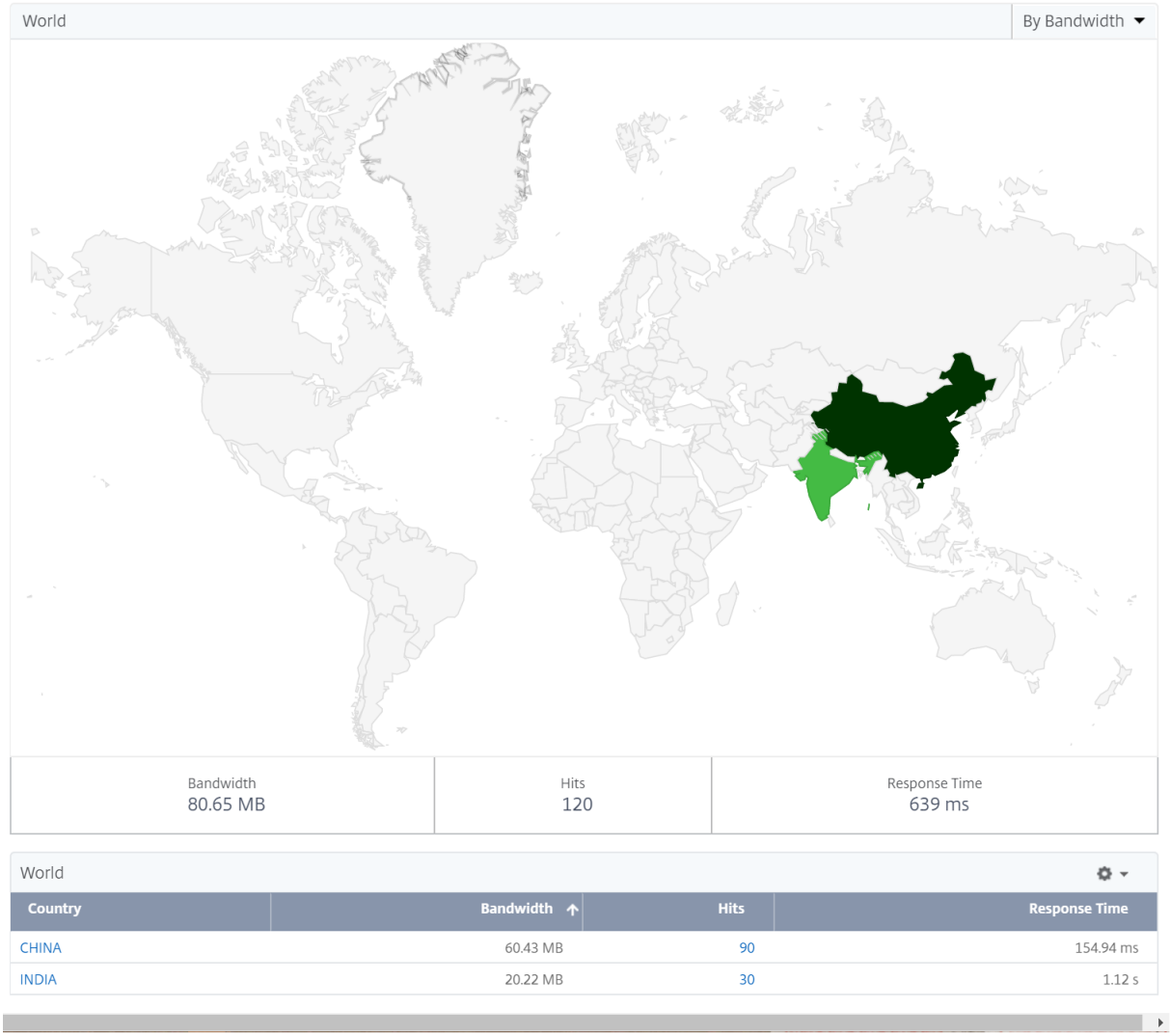


Öffentliche IP-Blöcke

Citrix ADM kann den Standort des Clients auch erkennen, wenn der Client eine öffentliche IP-Adresse verwendet. Citrix ADM verfügt über eine integrierte CSV-Datei, die dem Speicherort basierend auf dem Client-IP-Adressbereich entspricht. Für die Verwendung eines öffentlichen IP-Blocks besteht die einzige Voraussetzung darin, dass Sie die Erfassung von **Geo-Daten aktivieren** auf der Seite Configure Insight aktivieren müssen.

> Hinweis
>
> Citrix ADM benötigt eine Internetverbindung, um die Geomaps für einen bestimmten geografischen Standort anzuzeigen. Eine Internetverbindung ist auch erforderlich, um die GeoMap in den

> Formaten PDF-, PNG- oder JPG-Format zu exportieren.



So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

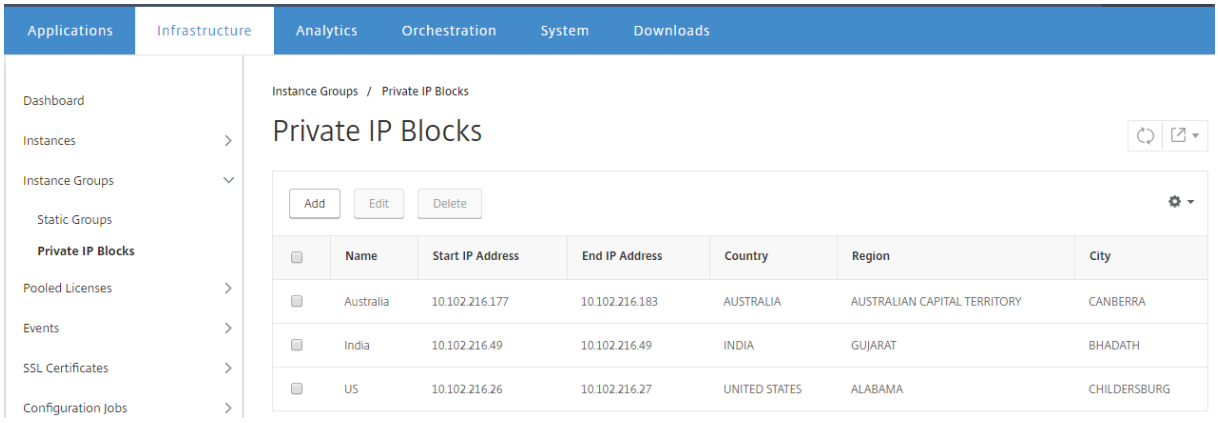
1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. So planen Sie den Bericht täglich, wöchentlich oder monatlich und senden Sie den Bericht per E-Mail oder Puffernachricht.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.

> • Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

So konfigurieren Sie eine Geomap für Rechenzentren:

Navigieren Sie auf der Registerkarte **Netzwerke** zu **Sites** > **Private IP-Blöcke**, um Geomaps für einen bestimmten Standort zu konfigurieren.



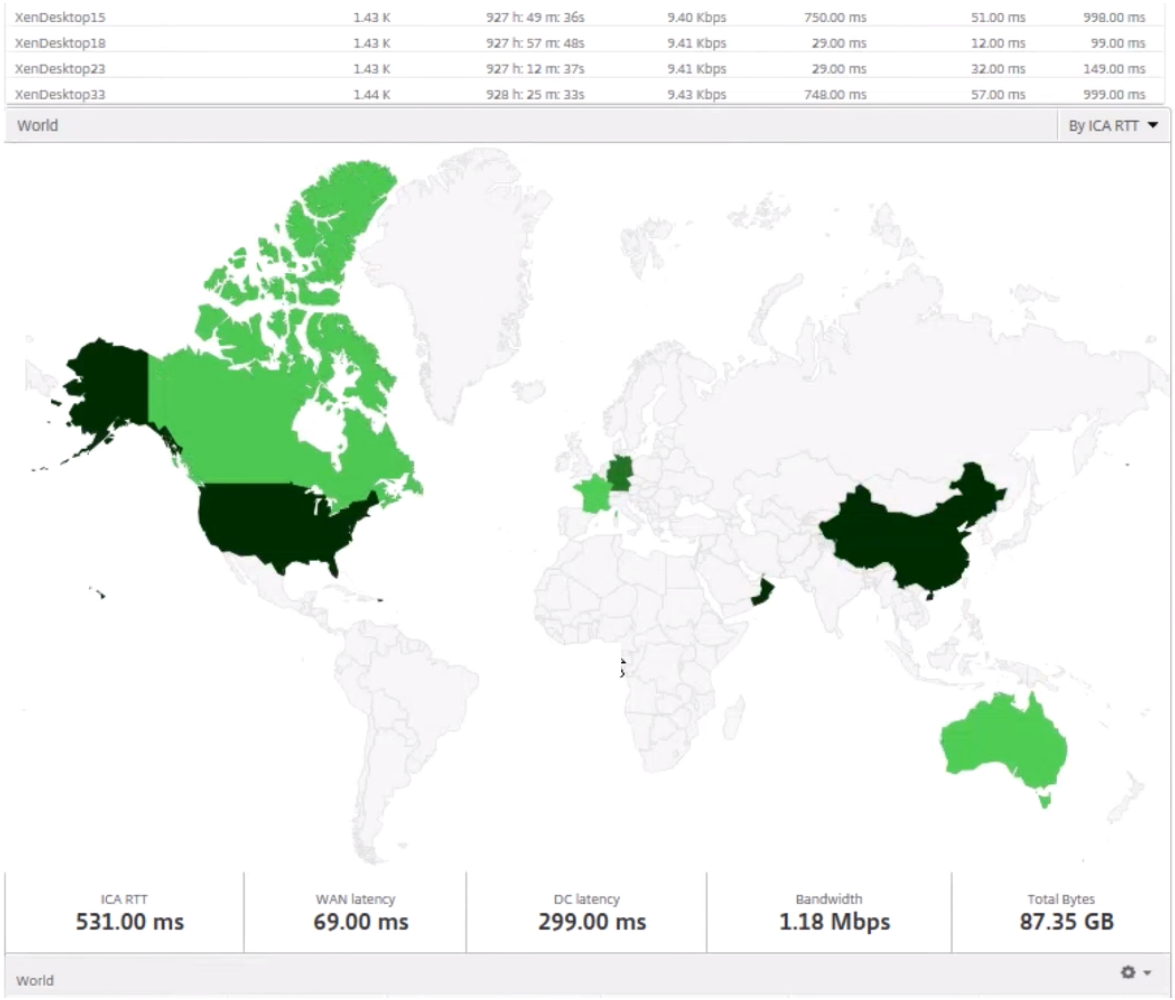
Anwendungsfall

Betrachten Sie ein Szenario, in dem Organisation ABC 2 Niederlassungen hat, eine in Santa Clara und die andere in Indien.

Die Santa Clara Benutzer verwenden die ADC Gateway-Appliance bei Sclara.x.com, um auf VPN-Datenverkehr zuzugreifen. Die indischen Benutzer verwenden die ADC Gateway-Appliance unter India.x.com, um auf VPN-Datenverkehr zuzugreifen.

Während eines bestimmten Zeitintervalls, sagen wir 10 Uhr bis 17 Uhr, verbinden sich die Benutzer in Santa Clara mit Sclara.x.com, um auf VPN-Datenverkehr zuzugreifen. Die meisten Benutzer greifen auf dasselbe ADC-Gateway zu, was zu einer Verzögerung bei der Verbindung mit dem VPN führt, so dass einige Benutzer eine Verbindung zu India.x.com anstelle von Sclara.x.com herstellen.

Ein ADC-Administrator, der den Datenverkehr analysiert, kann die Geokarten-Funktionalität verwenden, um den Verkehr im Büro von Santa Clara anzuzeigen. Die Karte zeigt, dass die Reaktionszeit im Büro von Santa Clara hoch ist, da das Büro von Santa Clara nur über ein ADC Gateway-Appliance verfügt, über das Benutzer auf VPN-Verkehr zugreifen können. Der Administrator kann daher entscheiden, ein anderes ADC-Gateway zu installieren, sodass Benutzer über zwei lokale ADC-Gateway-Appliances auf das VPN zugreifen können.



Einschränkungen

Wenn ADC-Instanzen eine Advanced-Lizenz haben, werden für Citrix ADM für HDX Insight festgelegte Schwellenwerte nicht ausgelöst, da Analysedaten nur für eine Stunde erfasst werden.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. So planen Sie den Bericht täglich, wöchentlich oder monatlich und senden Sie den Bericht per E-Mail oder Puffernachricht.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage

> auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

HDX Insight Datenerfassung aktivieren

April 28, 2021

HDX Insight ermöglicht es dem Administrator, ein außergewöhnliches Benutzererlebnis zu bieten, indem er einen End-to-End-Transick in den ICA-Datenverkehr bietet, der die Citrix ADC oder Citrix SD-WAN Appliances durchläuft.

HDX Insight bietet überzeugende und leistungsstarke Business Intelligence- und Fehleranalysefunktionen für Netzwerk, virtuelle Desktops, Anwendungen und Anwendungs-Fabric. HDX Insight kann Benutzerprobleme sofort erfassen, Daten über virtuelle Desktopverbindungen sammeln, AppFlow Datensätze generieren und als visuelle Berichte präsentieren.

Die Konfiguration zur Aktivierung der Datenerfassung in den ADC-Instanzen unterscheidet sich von der Position der Appliance in der Bereitstellungstopologie. Dieses Thema enthält die folgenden Details:

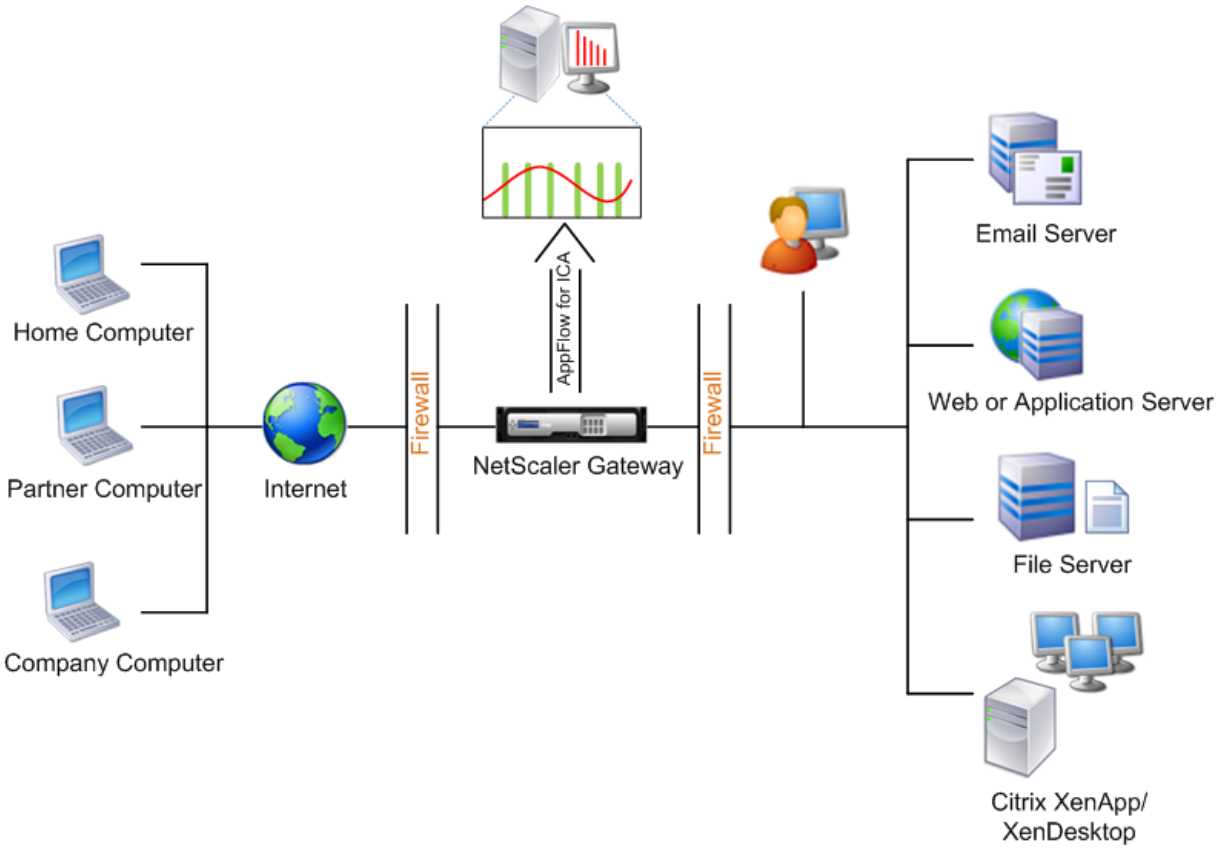
- Aktivieren der Datenerfassung für die Überwachung der im transparenten Modus bereitgestellten Citrix ADCs
- Aktivieren der Datenerfassung für Citrix ADC Gateway-Appliances, die im Einzelhop-Modus bereitgestellt werden
- Aktivieren der Datenerfassung für Citrix ADC Gateway-Appliances, die im Double-Hop-Modus bereitgestellt werden
- Aktivieren der Datenerfassung für die Überwachung der im LAN-Benutzermodus bereitgestellten Citrix ADCs

Aktivieren der Datenerfassung für Citrix ADC Gateway-Appliances, die im Einzelhop-Modus bereitgestellt werden

April 28, 2021

Wenn Citrix ADC Gateway im Einzelhop-Modus bereitgestellt wird, befindet sich das ADC-Gateway am Rand des Netzwerks und stellt ICA-Verbindungen zur Desktopbereitstellungsinfrastruktur her. Diese Bereitstellung ist die einfachste und gebräuchlichste Bereitstellung. Dieser Modus bietet Sicherheit, wenn ein externer Benutzer versucht, auf das interne Netzwerk in einer Organisation zuzugreifen. Im Single-Hop-Modus greifen Benutzer über ein virtuelles privates Netzwerk (VPN) auf die ADC-Appliances zu.

Um mit dem Sammeln der Berichte zu beginnen, müssen Sie die ADC Gateway-Appliance zur Citrix Application Delivery Management (ADM) -Bestandsliste hinzufügen und AppFlow auf ADM aktivieren. Das folgende Bild veranschaulicht einen Citrix ADM, der im Einzelhop-Modus bereitgestellt wird.



Aktivieren der AppFlow Funktion von Citrix ADM

1. Navigieren Sie zu **Infrastruktur** > **Instanzen**, und wählen Sie die ADC-Instanz aus, die Sie Analysen aktivieren möchten.
2. Wählen Sie in der Liste **Aktion** die Option **Insight aktivieren/deaktivieren**aus.
3. Wählen Sie die virtuellen VPN-Server aus, und klicken Sie auf **AppFlow aktivieren**.
4. Geben Sie im Feld **AppFlow aktivieren** den **Wert true** ein, und wählen Sie **ICA** aus.
5. Klicken Sie auf **OK**.

> **Hinweis**
>
> Die folgenden Befehle werden im Hintergrund ausgeführt, wenn Sie AppFlow im Single-Hop-Modus aktivieren. Diese Befehle werden hier explizit zur Fehlerbehebung angegeben.
>
> - `add appflow collector \<name\> -IPAddress \<ip\\_addr\>`
> - `add appflow action \<name\> -collectors \<string\>`

- `set appflow param -flowRecordInterval \<secs\>`
- `disable ns feature AppFlow`
- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >- priority \<positive\\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

Aktivieren der Datenerfassung zur Überwachung der im transparenten Modus bereitgestellten Citrix ADCs

April 28, 2021

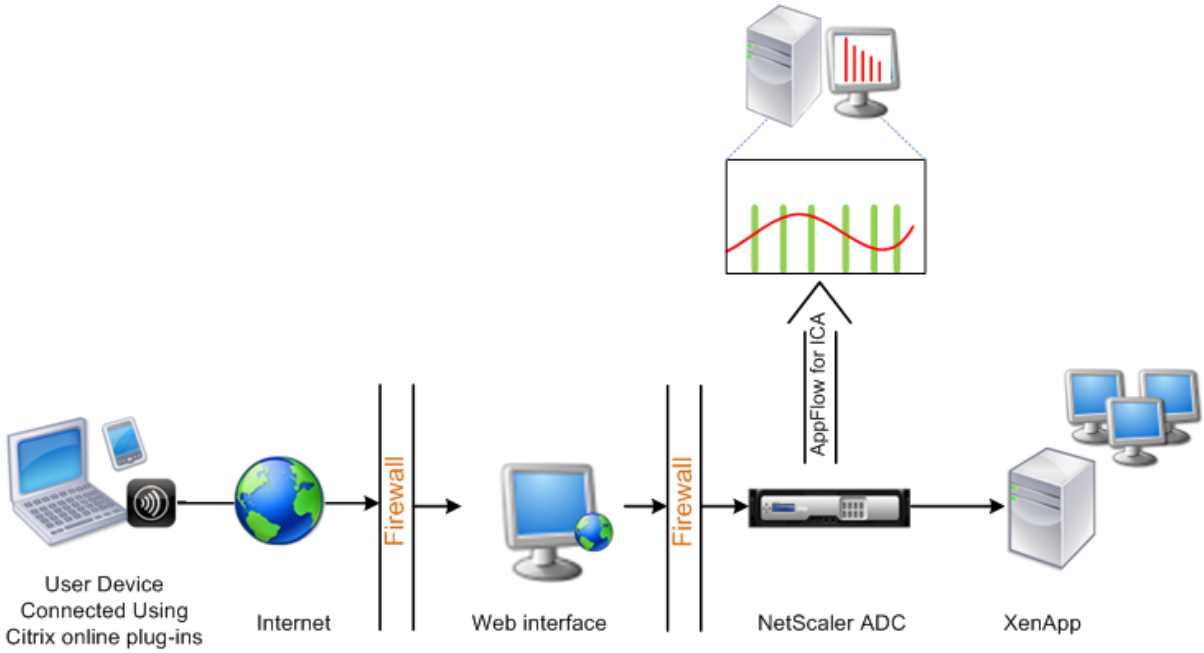
Wenn ein Citrix ADC im transparenten Modus bereitgestellt wird, können die Clients direkt auf die Server zugreifen, ohne dass ein virtueller Server vorhanden ist. Wenn eine Citrix ADC Appliance im transparenten Modus in einer Citrix Virtual Apps and Desktops Umgebung bereitgestellt wird, wird der ICA-Datenverkehr nicht über ein VPN übertragen.

Nachdem Sie Citrix ADC zur Citrix Application Delivery Management (ADM) -Bestandsliste hinzugefügt haben, müssen Sie AppFlow für die Datenerfassung aktivieren. Die Aktivierung der Datenerfassung hängt vom Gerät und vom Modus ab. In diesem Fall müssen Sie Citrix ADM als AppFlow-Collector auf jeder Citrix ADC Appliance hinzufügen, und Sie müssen eine AppFlow-Richtlinie konfigurieren, um den gesamten oder spezifischen ICA-Datenverkehr zu erfassen, der durch die Appliance fließt.

Hinweis

- Sie können die Datenerfassung auf einem Citrix ADC, der im transparenten Modus bereitgestellt wird, nicht mithilfe des Citrix ADM Konfigurationsdienstprogramms aktivieren.
- Ausführliche Informationen zu den Befehlen und deren Verwendung finden Sie unterBefehlsreferenz.
- Hinweise zu Richtlinienausdrücken finden Sie unterRichtlinien und Ausdrücke.

Die folgende Abbildung zeigt die Netzwerkbereitstellung eines Citrix ADM, wenn ein Citrix ADC in einem transparenten Modus bereitgestellt wird:



So konfigurieren Sie die Datenerfassung auf einer Citrix ADC Appliance mithilfe der Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

1. Melden Sie sich bei einer Appliance an.
2. Geben Sie die ICA-Ports an, an denen die Citrix ADC Appliance auf Datenverkehr wartet.

```
set ns param --icaPorts <port>...
<!--NeedCopy-->
```

Beispiel:

```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```

> **Hinweis**
>
> - Mit diesem Befehl können Sie bis zu 10 Ports angeben.
> - Die Standardportnummer ist 2598. Sie können die Portnummer nach Bedarf ändern.

3. Fügen Sie NetScaler Insight Center als AppFlow-Collector auf der Citrix ADC Appliance hinzu.

```
add appflow collector <name> -IPAddress <ip_addr>
```



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

Beispiel:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> **Hinweis**
>
> Um die auf der Citrix ADC Appliance konfigurierten AppFlow-Collector anzuzeigen, verwenden Sie den Befehl **show appflow collector** .

4. Erstellen Sie eine AppFlow Aktion, und ordnen Sie den Kollektor der Aktion zu.

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

Beispiel:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Erstellen Sie eine AppFlow Richtlinie, um die Regel zum Generieren des Datenverkehrs anzugeben.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Beispiel:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Binden Sie die AppFlow Richtlinie an einen globalen Bindungspunkt.

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```


Beispiel:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Hinweis**
>
> Der Wert des **Typs** muss ICA_REQ_OVERRIDE oder ICA_REQ_DEFAULT sein, damit er auf ICA-Verkehr angewendet wird.

7. Legen Sie den Wert des Parameters FlowRecordInterval für AppFlow auf 60 Sekunden fest.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. Speichern Sie die Konfiguration.

```
save ns config
<!--NeedCopy-->
```

Aktivieren der Datenerfassung für Citrix ADC Gateway-Appliances, die im Double-Hop-Modus bereitgestellt werden

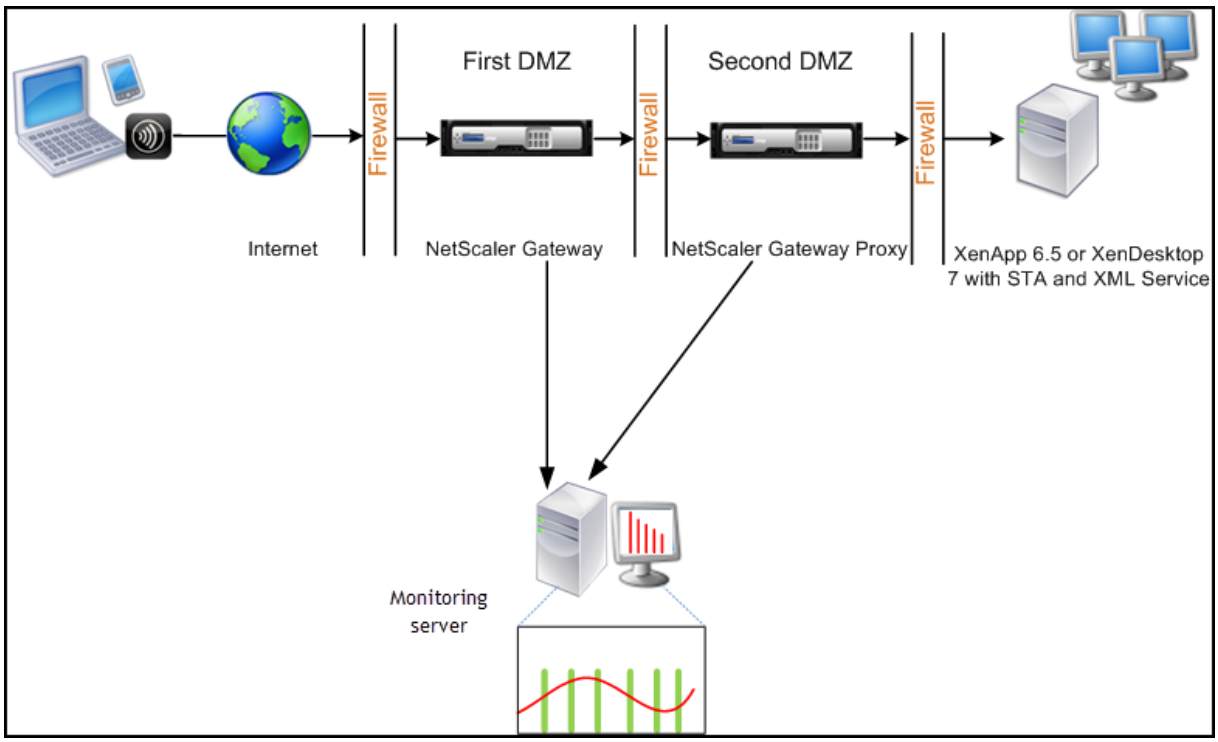
April 28, 2021

Der Doppel-Hop-Modus von Citrix ADC Gateway bietet zusätzlichen Schutz für ein internes Organisationsnetzwerk, da ein Angreifer mehrere Sicherheitszonen oder Demilitarisierte Zonen (DMZ) durchdringen muss, um die Server im sicheren Netzwerk zu erreichen.

Als Administrator können Sie mit Citrix ADM Folgendes analysieren:

- Die Anzahl der Hops (Citrix ADC Gateway-Appliances), über die die ICA-Verbindungen laufen
- Die Details über die Latenz bei jeder TCP-Verbindung und wie sie sich gegen die vom Client wahrgenommene Gesamt-ICA-Latenz auswirkt

Die folgende Abbildung zeigt, dass Citrix ADM und Citrix ADC Gateway in der ersten DMZ im selben Subnetz bereitgestellt werden.



Das Citrix ADC Gateway in der ersten DMZ verarbeitet Benutzerverbindungen und führt die Sicherheitsfunktionen eines SSL-VPN aus. Dieses Citrix ADC Gateway verschlüsselt Benutzerverbindungen, bestimmt, wie die Benutzer authentifiziert werden, und steuert den Zugriff auf die Server im internen Netzwerk.

Das Citrix ADC Gateway in der zweiten DMZ dient als Citrix ADC Gateway-Proxygerät. Mit diesem Citrix ADC Gateway kann der ICA-Datenverkehr die zweite DMZ durchlaufen, um Benutzerverbindungen mit der Serverfarm abzuschließen.

Das Citrix ADM kann entweder im Subnetz bereitgestellt werden, das zur Citrix ADC Gateway-Appliance in der ersten DMZ gehört, oder im Subnetz, das zur zweiten DMZ der Citrix ADC Gateway-Appliance gehört.

Im Double-Hop-Modus sammelt Citrix ADM TCP-Datensätze von einer Appliance und ICA-Einträge von der anderen Appliance. Nachdem Sie die Citrix ADC Gateway-Appliances zum Citrix ADM-Bestand hinzugefügt und die Datenerfassung aktiviert haben, exportiert jede Appliance die Berichte, indem sie die Hop-Anzahl und die Verbindungsketten-ID verfolgt.

Damit Citrix ADM identifiziert, welche Appliance Datensätze exportiert, wird jede Appliance mit einer Hop-Anzahl angegeben, und jede Verbindung wird mit einer Verbindungsketten-ID angegeben. Die Anzahl der Hop stellt die Anzahl der Citrix ADC Gateway-Appliances dar, über die der Datenverkehr von einem Client zu den Servern fließt. Die Verbindungsketten-ID stellt die End- zu-Endverbindungen zwischen Client und Server dar.

Citrix ADM verwendet die Hop-Anzahl und die Verbindungsketten-ID, um die Daten der Citrix ADC

Gateway-Appliances miteinander zu verknüpfen und die Berichte zu generieren.

Um Citrix ADC Gateway-Appliances zu überwachen, die in diesem Modus bereitgestellt werden, müssen Sie zuerst das Citrix ADC Gateway dem Citrix ADM-Bestand hinzufügen, AppFlow auf Citrix ADM aktivieren und dann die Berichte auf dem Citrix ADM Dashboard anzeigen.

Aktivieren der Datenerfassung auf Citrix ADM

Wenn Sie Citrix ADM aktivieren, um die ICA-Details von beiden Appliances zu erfassen, sind die erfassten Details redundant. Um diese Situation zu überwinden, müssen Sie AppFlow für ICA auf der ersten Citrix ADC Gateway-Appliance aktivieren und dann AppFlow für TCP auf der zweiten Appliance aktivieren. Auf diese Weise exportiert eine der Appliances ICA-AppFlow Datensätze, und die andere Appliance exportiert TCP-AppFlow-Datensätze. Dies spart auch die Verarbeitungszeit beim Analysieren des ICA-Datenverkehrs.

So aktivieren Sie die AppFlow Funktion von Citrix ADM:

1. Navigieren Sie zu **Infrastruktur** > **Instanzen**, und wählen Sie die Citrix ADC-Instanz aus, die Sie die Analyse aktivieren möchten.
2. Wählen Sie in der Liste **Aktion** die Option **Insight aktivieren/deaktivieren**aus.
3. Wählen Sie die virtuellen VPN-Server aus, und klicken Sie auf **AppFlow aktivieren**.
4. Geben Sie im Feld **AppFlow aktivieren** den Wert **true** ein, und wählen Sie **ICA/TCP** für ICA-Datenverkehr bzw. TCP-Datenverkehr aus.

   > **Hinweis:**
   >
   > Wenn die AppFlow Protokollierung für die entsprechenden Dienste oder Dienstgruppen auf der Citrix ADC Appliance nicht aktiviert ist, werden die Datensätze im Citrix ADM Dashboard nicht angezeigt, selbst wenn in der Spalte Insight Aktiviert angezeigt wird.

5. Klicken Sie auf **OK**.

Konfigurieren von Citrix ADC Gateway-Geräten zum Exportieren von Daten

Nachdem Sie die Citrix ADC Gateway Appliances installiert haben, müssen Sie die folgenden Einstellungen auf den Citrix ADC-Gateway-Appliances konfigurieren, um die Berichte in Citrix ADM zu exportieren:

- Konfigurieren Sie virtuelle Server der Citrix ADC Gateway-Appliances in der ersten und zweiten DMZ für die Kommunikation miteinander.
- Binden Sie den virtuellen Citrix ADC Gateway-Server in der zweiten DMZ an den virtuellen Citrix ADC Gateway-Server in der ersten DMZ.

- Aktivieren Sie den Doppel-Hop auf dem Citrix ADC Gateway in der zweiten DMZ.
- Deaktivieren Sie die Authentifizierung auf dem virtuellen Citrix ADC Gateway-Server in der zweiten DMZ.
- Aktivieren einer der Citrix ADC Gateway-Appliances zum Exportieren von ICA-Datensätzen
- Aktivieren Sie die andere Citrix ADC Gateway-Appliance zum Exportieren von TCP-Datensätzen:
- Aktivieren Sie die Verbindungsverkettung auf beiden Citrix ADC Gateway-Appliances.

Konfigurieren Sie Citrix ADC Gateway mit der Befehlszeilenschnittstelle:

1. Konfigurieren Sie den virtuellen Citrix ADC Gateway-Server in der ersten DMZ für die Kommunikation mit dem virtuellen Citrix ADC Gateway-Server in der zweiten DMZ.

   add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [**-secure** (ON|OFF)] [**-imgGifToPng**] …

   ```
   add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
   <!--NeedCopy-->
   ```

2. Binden Sie den virtuellen Citrix ADC Gateway-Server in der zweiten DMZ an den virtuellen Citrix ADC Gateway-Server in der ersten DMZ. Führen Sie den folgenden Befehl auf dem Citrix ADC Gateway in der ersten DMZ aus:

   bind vpn vserver <name> **-nextHopServer** <name>

   ```
   bind vpn vserver vs1 -nextHopServer nh1
   <!--NeedCopy-->
   ```

3. Aktivieren Sie Double Hop und AppFlow auf dem Citrix ADC Gateway in der zweiten DMZ.

   set vpn vserver <name> [**- doubleHop** (ENABLED |DISABLED)] [**- appflowLog** (ENABLED |DISABLED)]

   ```
   set vpn vserver vpnhop2 -doubleHop ENABLED -appFlowLog ENABLED
   <!--NeedCopy-->
   ```

4. Deaktivieren Sie die Authentifizierung auf dem virtuellen Citrix ADC Gateway-Server in der zweiten DMZ.

   set vpn vserver<name> [**-authentication** (ON|OFF)]


```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. Aktivieren Sie eine der Citrix ADC Gateway-Appliances zum Exportieren von TCP-Datensätzen.

   bind vpn vserver<name> [**-policy **<string> **-priority **<positive_integer>] [**-type **<type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101  - type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```

6. Aktivieren Sie die andere Citrix ADC Gateway-Appliance zum Exportieren von ICA-Datensätzen:

   bind vpn vserver<name> [**-policy **<string> **-priority **<positive_integer>] [**-type **<type>]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA_REQUEST
<!--NeedCopy-->
```

7. Aktivieren Sie die Verbindungsverkettung auf beiden Citrix ADC Gateway-Appliances:

set appFlow param [**-connectionChaining** (ENABLED DISABLED)]

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

Konfigurieren von Citrix ADC Gateway mithilfe des Konfigurationsdienstprogramms:

1. Konfigurieren Sie das Citrix ADC Gateway in der ersten DMZ für die Kommunikation mit dem Citrix ADC Gateway in der zweiten DMZ und binden Sie das Citrix ADC-Gateway in der zweiten DMZ an das Citrix ADC-Gateway in der ersten DMZ.

   a) Erweitern Sie auf der Registerkarte **Konfiguration** die Option **Citrix ADC Gateway**, und klicken Sie auf **Virtuelle Server**.

   b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der

Gruppe Erweitert die Option **Published Applications**.

c) Klicken Sie auf **Next Hop Server** und binden Sie einen nächsten Hop-Server an das zweite Citrix ADC Gateway-Gerät.

2. Aktivieren Sie den Doppel-Hop auf dem Citrix ADC Gateway in der zweiten DMZ.

a) Erweitern Sie auf der Registerkarte **Konfiguration** die Option **Citrix ADC Gateway**, und klicken Sie auf **Virtuelle Server**.

b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server und klicken Sie in der Gruppe **Grundeinstellungen** auf das Symbol “Bearbeiten”.

c) Erweitern Sie **Mehr**, wählen Sie **Double Hop** und klicken Sie auf **OK**.

3. Deaktivieren Sie die Authentifizierung auf dem virtuellen Server auf dem Citrix ADC Gateway in der zweiten DMZ.

a) Erweitern Sie auf der Registerkarte **Konfiguration** die Option **Citrix ADC Gateway**, und klicken Sie auf **Virtuelle Server**.

b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server und klicken Sie in der Gruppe **Grundeinstellungen** auf das Symbol “Bearbeiten”.

c) Erweitern Sie **Mehr**und deaktivieren **Sie Authentifizierung aktivieren**.

4. Aktivieren Sie eine der Citrix ADC Gateway-Appliances zum Exportieren von TCP-Datensätzen.

a) Erweitern Sie auf der Registerkarte **Konfiguration** die Option **Citrix ADC Gateway**, und klicken Sie auf **Virtuelle Server**.

b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe Erweitert die Option Richtlinien.

c) Klicken Sie auf das Symbol + und **wählen Sie in der Liste Choose policy** die Option **AppFlow** aus und **wählen Sie in der Liste Typ** auswählen die Option **Andere TCP-Anforderung**aus.

d) Klicken Sie auf **Weiter**.

e) Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Schließen**.

5. Aktivieren Sie die andere Citrix ADC Gateway-Appliance zum Exportieren von ICA-Datensätzen:

a) Erweitern Sie auf der Registerkarte **Konfiguration** die Option **Citrix ADC Gateway**, und klicken Sie auf **Virtuelle Server**.

b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe **Erweitert** die Option **Richtlinien**.

c) Klicken Sie auf das Symbol + und **wählen Sie in der Liste Choose policy** die Option **AppFlow** aus und **wählen Sie in der Liste Typ** auswählen die Option **Andere TCP-Anforderung**aus.

d) Klicken Sie auf **Weiter**.

e) Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Schließen**.

6. Aktivieren Sie die Verbindungsverkettung auf beiden Citrix ADC Gateway-Appliances.

a) Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **Appflow**.

b) Klicken Sie im rechten Bereich in der Gruppe **Einstellungen** auf **Appflow-Einstellungen ändern**.

c) Wählen Sie **Verbindungsverkettung** aus, und klicken Sie auf **OK**.

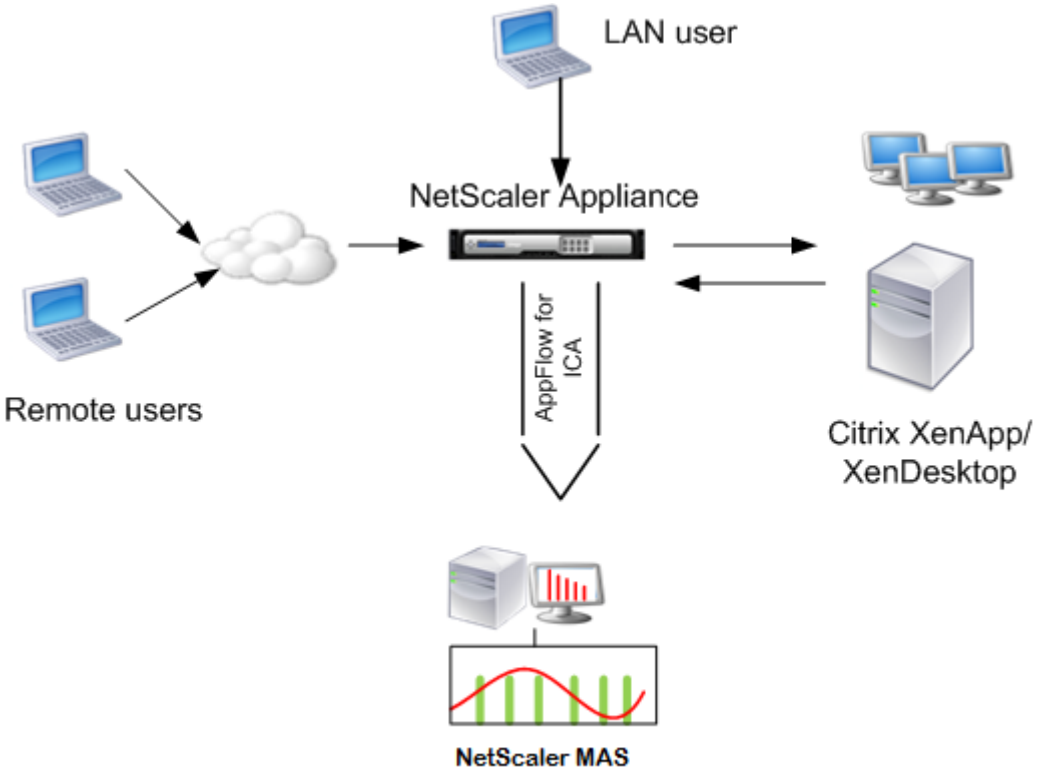
Aktivieren der Datenerfassung zur Überwachung der im LAN-Benutzermodus bereitgestellten Citrix ADCs

April 28, 2021

Externe Benutzer, die auf Citrix Virtual App oder Desktop-Anwendungen zugreifen, müssen sich am Citrix ADC Gateway authentifizieren. Interne Benutzer müssen jedoch möglicherweise nicht an das ADC-Gateway weitergeleitet werden. Außerdem muss der Administrator in einer Bereitstellung im transparenten Modus die Routingrichtlinien manuell anwenden, damit die Anforderungen an die Citrix ADC Appliance umgeleitet werden.

Um diese Herausforderungen zu meistern und LAN-Benutzer direkt mit Citrix Virtual App- und Desktop-Anwendungen zu verbinden, können Sie die ADC-Appliance in einem LAN-Benutzermodus bereitstellen, indem Sie einen virtuellen Cacheumleitungsserver konfigurieren. Der virtuelle Server für die Cacheumleitung fungiert als SOCKS-Proxy auf dem ADC Gateway-Gerät.

Die folgende Abbildung zeigt Citrix Application Delivery Management (ADM), die im **LAN-Benutzermodus bereitgestellt wird**.



> **Hinweis**
>
> Das Citrix ADC Gateway-Gerät muss in der Lage sein, den Citrix ADM -Agent zu erreichen.

Um die in diesem Modus bereitgestellten Citrix ADC-Appliances zu überwachen, fügen Sie zuerst die Citrix ADC Appliance zur Citrix ADC Insight-Bestandsliste hinzu, aktivieren Sie AppFlow und zeigen die Berichte dann auf dem Dashboard an.

Nachdem Sie die Citrix ADC Appliance zur Citrix ADM Bestandsliste hinzugefügt haben, müssen Sie AppFlow für die Datenerfassung aktivieren.

> **Hinweis**
>
> - Sie können die Datenerfassung auf einem Citrix ADC, der im LAN-Benutzermodus bereitgestellt wird, nicht mithilfe des Citrix ADM Konfigurationsdienstprogramms aktivieren.
> - Ausführliche Informationen zu den Befehlen und deren Verwendung finden Sie unter Befehlsreferenz.
> - Weitere Informationen zu Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.

So konfigurieren Sie die Datenerfassung auf einer Citrix ADC Appliance mithilfe der Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

1. Melden Sie sich bei der Citrix ADC Appliance an.
2. Fügen Sie einen virtuellen Forward-Proxy-Cache-Umleitungsserver mit Proxy-IP und Port hinzu, und geben Sie den Diensttyp als HDX an.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

Beispiel:

```
add cr vserver cr1 HDX 10.12.2.2 443 - cacheType FORWARD -
   cltTimeout 180
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie mit einem Citrix ADC Gateway-Gerät auf das LAN-Netzwerk zugreifen, fügen Sie eine Aktion hinzu, um eine Richtlinie anzuwenden, die dem VPN-Datenverkehr entspricht.

```
add vpn trafficAction** <name> <qual> [-HDX ( ON | OFF )]

add vpn trafficPolicy** <name> <rule> <action>
<!--NeedCopy-->
```

Beispiel:

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 ”REQ.IP.DESTIP == 10.102.69.17” act1
<!--NeedCopy-->
```

3. Fügen Sie Citrix ADM als AppFlow Collector auf der Citrix ADC Appliance hinzu.

```
add appflow collector** <name> \*\*-IPAddress\*\* <ip_addr>
<!--NeedCopy-->
```

Beispiel:


```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. Erstellen Sie eine AppFlow Aktion, und ordnen Sie den Kollektor der Aktion zu.

```
add appflow action** <name> \*\*-collectors\*\* <string> ...
<!--NeedCopy-->
```

Beispiel:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Erstellen Sie eine AppFlow Richtlinie, um die Regel zum Generieren des Datenverkehrs anzugeben.

```
add appflow policy** <policyname> <rule> <action>
<!--NeedCopy-->
```

Beispiel:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Binden Sie die AppFlow Richtlinie an einen globalen Bindungspunkt.

```
bind appflow global** <policyname> <priority> \*\*-type\*\* <type>
<!--NeedCopy-->
```

Beispiel:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```


> **Hinweis**
>
> Der Wert vom Typ muss ICA_REQ_OVERRIDE oder ICA_REQ_DEFAULT sein, um auf ICA-Datenverkehr anzuwenden.

7. Legen Sie den Wert des Parameters FlowRecordInterval für AppFlow auf 60 Sekunden fest.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

Beispiel:

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. Speichern Sie die Konfiguration.

```
save ns config
<!--NeedCopy-->
```

Erstellen von Schwellenwerten und Konfigurieren von Warnungen für HDX Insight

April 28, 2021

Mit HDX Insight on Citrix Application Delivery Management (ADM) können Sie den HDX-Datenverkehr überwachen, der durch die Citrix ADC-Instanzen fließt. Mit Citrix ADM können Sie Schwellenwerte für verschiedene Leistungsindikatoren festlegen, die zur Überwachung des Insight-Datenverkehrs verwendet werden. Sie können auch Regeln konfigurieren und Warnungen in ADM erstellen.

Der HDX-Datenverkehrstyp ist verschiedenen Entitäten wie Anwendungen, Desktops, Gateways, Lizenzen und Benutzern zugeordnet. Jede Entität kann verschiedene Metriken enthalten, die ihnen zugeordnet sind. Beispielsweise ist die Anwendungseinheit mehreren Treffern, der von der Anwendung verbrauchten Bandbreite und der Reaktionszeit des Servers zugeordnet. Eine Benutzerentität kann WAN-Latenz, DC-Latenz, ICA RTT und Bandbreite zugeordnet werden, die von einem Benutzer belegt wird.

Mit der Schwellenwertverwaltung für HDX Insight in Citrix ADM können Sie proaktiv Regeln erstellen und Warnungen konfigurieren, wenn die festgelegten Schwellenwerte überschritten werden. Diese Schwellenwertverwaltung wird nun erweitert, um eine Gruppe von Schwellenregeln zu konfigurieren. Sie können nun die Gruppe anstelle einzelner Regeln überwachen. Eine Schwellenregelgruppe besteht aus einer oder mehreren benutzerdefinierten Schwellenwertregeln für Metriken, die aus Entitäten wie Benutzern, Anwendungen und Desktops ausgewählt wurden. Jede Regel wird mit einem erwarteten Wert überwacht, den Sie beim Erstellen der Regel eingeben. In der Entität des Benutzers kann die Schwellenwertgruppe auch mit einer Geolokalisierung verknüpft sein.

Eine Warnung wird nur dann auf Citrix ADM generiert, wenn alle Regeln in der konfigurierten Schwellenwertgruppe verletzt werden. Beispielsweise können Sie eine Anwendung bei der Gesamtzahl des Sitzungsstarts und auch bei der Anzahl des Anwendungsstarts als eine Schwellenwertgruppe überwachen. Eine Warnung wird nur generiert, wenn beide Regeln verletzt werden. Auf diese Weise können Sie realistischere Schwellenwerte für eine Entität festlegen.

Einige Beispiele sind wie folgt aufgeführt:

- Schwellenwertregel1: ICA RTT (Metrik) für Benutzer (Entität) muss <= 100 ms sein
- Schwellenwertregel2: WAN-Latenz (Metrik) für Benutzer (Entität) muss <= 100 ms sein

Ein Beispiel für eine Schwellenwertgruppe kann sein: {Schwellenwertregel 1 + Schwellenwertregel 2}

Um eine Regel zu erstellen, müssen Sie zuerst die Entität auswählen, die Sie überwachen möchten. Wählen Sie dann beim Erstellen einer Regel eine Metrik aus. Sie können beispielsweise die Entität der Anwendung auswählen und dann **Gesamtzahl für den Sitzungsstart oder Anzahl der App-Launch**auswählen. Sie können für jede Kombination einer Entität und einer Metrik eine Regel erstellen. Verwenden Sie die angegebenen Komparatoren (>, <, >= und <=), und geben Sie für jede Metrik einen Schwellenwert ein.

> **Hinweis**
>
> Wenn Sie nicht mehrere Entitäten in einer einzelnen Gruppe überwachen möchten, müssen Sie für jede Entität eine separate Schwellenregelgruppe erstellen.

Wenn der Wert eines Zählers den Wert eines Schwellenwerts überschreitet, generiert Citrix ADM ein Ereignis, das eine Schwellwertverletzung darstellt, und für jedes Ereignis wird eine Warnung erstellt.

Sie müssen konfigurieren, wie Sie die Warnung erhalten. Sie können aktivieren, dass die Warnung auf Citrix ADM angezeigt wird, die Warnung als E-Mail oder beides oder als SMS auf Ihrem Mobilgerät erhalten wird. Für die letzten beiden Aktionen müssen Sie den E-Mail-Server oder den SMS-Server auf Citrix ADM konfigurieren.

Schwellenwert-Gruppen können auch an Geolocations gebunden werden, um die geospezifische Überwachung für Benutzer-Entität zu überwachen.

Anwendungsbeispiele

ABC Inc. ist ein globales Unternehmen und verfügt über Niederlassungen in über 50 Ländern. Das Unternehmen verfügt über zwei Rechenzentren, eines in Singapur und eines in Kalifornien, in denen Citrix Virtual Apps and Desktops gehostet werden. Mitarbeiter des Unternehmens greifen mit dem Citrix ADC Gateway und der GSLB-basierten Umleitung auf die Citrix Virtual Apps and Desktops auf der ganzen Welt zu. Eric, der Citrix Virtual Apps and Desktops Admin für ABC Inc. möchte die Benutzererfahrung für alle ihre Büros verfolgen, um die Apps und die Desktop-Bereitstellung für den Zugriff von überall und jederzeit zu optimieren. Eric möchte auch die Nutzererfahrungsmetriken wie ICA RTTs, Latenzen überprüfen und Abweichungen proaktiv auslösen.

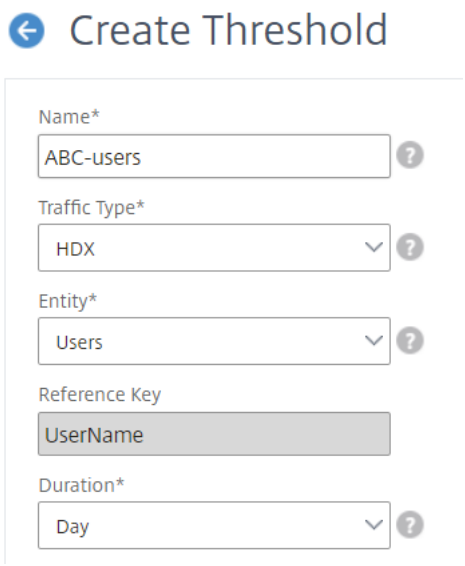
Die Anwender von ABC Inc. haben eine verteilte Präsenz. Einige Benutzer befinden sich in der Nähe des Rechenzentrums, während sich einige wenige weiter vom Rechenzentrum entfernt befinden. Da die Benutzerbasis breit verteilt ist, variieren auch die Metriken und die entsprechenden Schwellenwerte zwischen diesen Standorten. Beispielsweise kann die ICA-RTT für einen Standort in der Nähe des Rechenzentrums 5 bis 10 ms betragen, während das gleiche für einen Remotestandort etwa 100 ms betragen kann.

Mit der Verwaltung von Schwellenwertregelgruppen für HDX Insight kann Eric geospezifische Schwellenwertregelgruppen für jeden Standort festlegen und per E-Mail oder SMS für Verstöße pro Bereich benachrichtigt werden. Eric ist auch in der Lage, die Verfolgung von mehr als einer Metrik innerhalb einer Schwellenregelgruppe zu kombinieren und die Ursache auf Kapazitätsprobleme einzuschränken, falls vorhanden. Eric kann jetzt jede Abweichung proaktiv verfolgen, ohne sich um die Komplexität der manuellen Suche aller Portfoliometriken von Citrix Virtual Apps and Desktops kümmern zu müssen.

Erstellen einer Schwellenregelgruppe und Konfigurieren von Warnungen für HDX Insight mit Citrix ADM

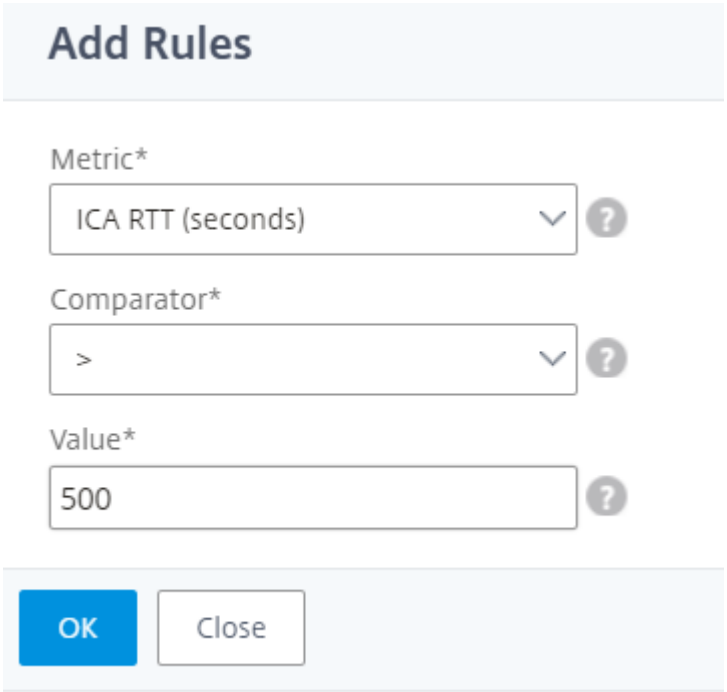
1. Navigieren Sie in Citrix ADM zu **Analytics** > **Einstellungen** > **Schwellenwerte**. Klicken Sie auf der Seite **Schwellenwerte**, die geöffnet wird, auf **Hinzufügen**.
2. Geben Sie auf der Seite **Schwellenwerte und Warnungen erstellen** die folgenden Details an:
    a) **Name**. Geben Sie einen Namen ein, um ein Ereignis zu erstellen, für das Citrix ADM eine Warnung generiert.
    b) **Typ des Verkehrs**. Wählen Sie im Dropdownlistenfeld HDX aus.
    c) **Entität**. Wählen Sie im Dropdownlistenfeld die Kategorie oder den Ressourcentyp aus. Die Entitäten unterscheiden sich für jeden Datenverkehrstyp, den Sie zuvor ausgewählt haben.
    d) **Referenz-Schlüssel**. Ein Referenzschlüssel wird automatisch basierend auf dem ausgewählten Datenverkehrstyp und der ausgewählten Entität generiert.

e) **Dauer**. Wählen Sie im Dropdownlistenfeld das Zeitintervall aus, für das Sie die Entität überwachen möchten. Sie können die Entitäten für eine Stunde, für einen Tag oder für eine Woche überwachen.



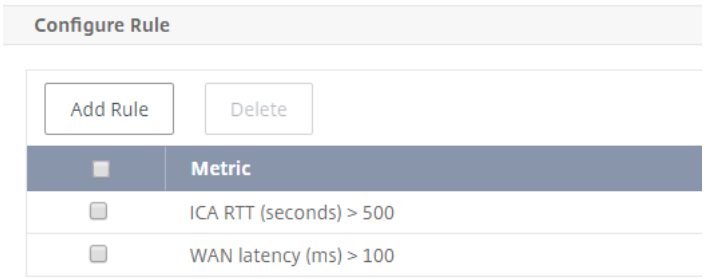
3. **Erstellen von Schwellenwertregelgruppen für alle Entitäten:**

   Für HDX-Datenverkehr müssen Sie eine Regel erstellen, indem Sie auf **Regel hinzufügen** klicken. Geben Sie die Werte im Popupfenster **Regeln hinzufügen** ein, das geöffnet wird.



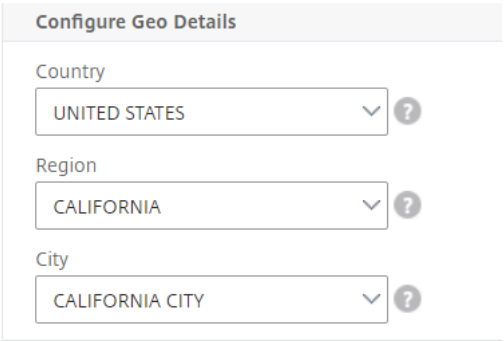
   Sie können mehrere Regeln erstellen, um jede Entität zu überwachen. Durch das Erstellen mehrerer Regeln in einer einzigen Gruppe können Sie die Entitäten als Gruppe von Schwellen-

regeln anstelle von einzelnen Regeln überwachen. Klicken Sie auf **OK**, um das Fenster zu schließen.

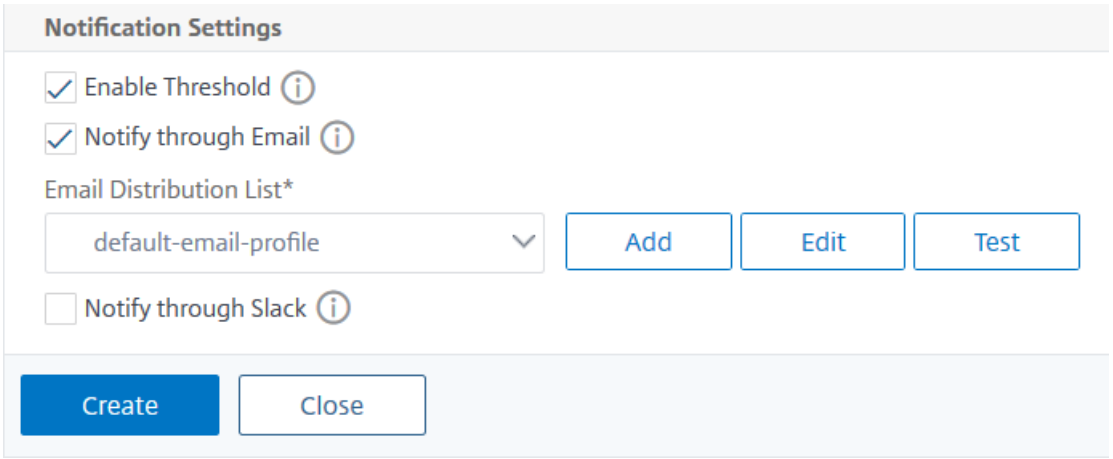


4. **Konfigurieren von Geolocation-Tagging für Benutzer-Entität:**

   Optional können Sie eine standortbasierte Warnung für die Benutzerentität im Abschnitt **Geo-Details konfigurieren** erstellen. Die folgende Abbildung zeigt ein Beispiel für die Erstellung eines Geolocation-basierten Tagging zur Überwachung der WAN-Latenzleistung für Benutzer an der Westküste der Vereinigten Staaten.



5. Klicken Sie auf **Schwellenwerte aktivieren**, damit Citrix ADM mit der Überwachung der Entitäten beginnen kann.
6. Optional können Sie Aktionen wie E-Mail- und Slack -Benachrichtigungen konfigurieren.



7. Klicken Sie auf **Erstellen**, um eine Schwellenregelgruppe zu erstellen.

Anzeigen von HDX Insight Berichten und Metriken

April 28, 2021

HDX Insight bietet vollständige Transparenz der Berichte und Metriken im Zusammenhang mit HDX-Datenverkehr auf Ihren Citrix ADC-Instanzen.

Sie können die HDX-Metriken für jede ausgewählte Entität anzeigen. Die Ansichten umfassen die folgenden Kategorien von Entitäten:

- **Benutzer**: Zeigt die Berichte für alle Benutzer an, die innerhalb des ausgewählten Zeitintervalls auf die Citrix Virtual Apps and Desktops zugreifen.
- **Anwendungen:** Zeigt die Berichte für die Gesamtzahl der Anwendungen und alle zugehörigen relevanten Informationen wie die Gesamtzahl der Startzeiten der Anwendungen innerhalb des angegebenen Zeitintervalls an.
- **Instanzen**: Zeigt die Berichte zu den ADC-Instanzen an, die als Gateways für eingehenden Datenverkehr fungieren.
- **Desktops**: Zeigt die Berichte für die Desktops an, die im ausgewählten Zeitraum verwendet werden.
- **Lizenzen**: Zeigt die Berichte für die gesamten SSL-VPN-Lizenzen an, die innerhalb des angegebenen Zeitfensters verwendet werden.

> **Hinweis**
>
> Der Lizenzwert gilt nicht für ADC SD-WAN-Appliances.

Dieses Dokument enthält Folgendes:

Berichte und Metriken der Anwendungsansicht

April 28, 2021

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf Citrix Virtual Apps. Navigieren Sie zu **Analytics** > **HDX Insight** > **Anwendungen**

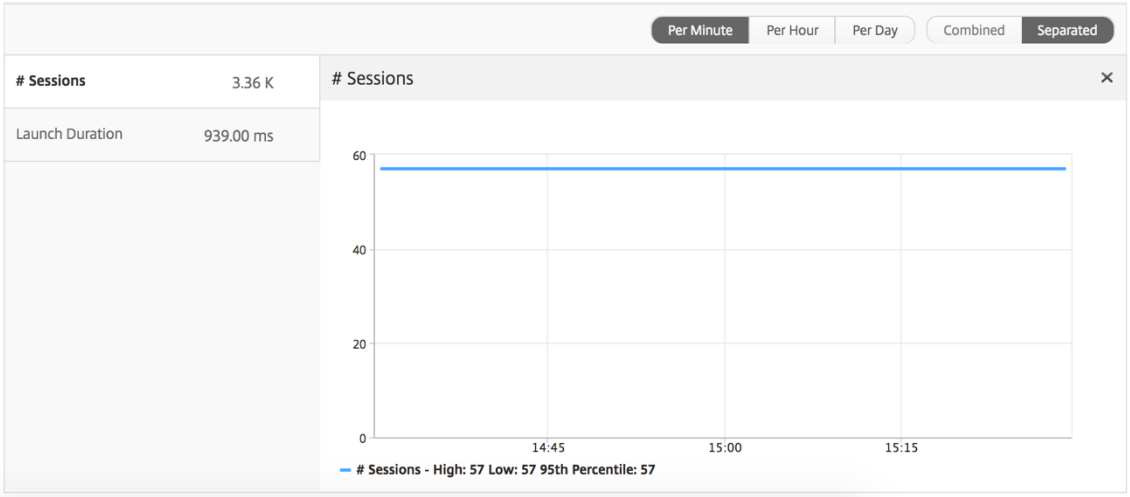
Zusammenfassende Ansicht

In der Zusammenfassungsansicht werden die Berichte für alle Anwendungen angezeigt, die während der ausgewählten Zeitachse angemeldet sind.

Alle Metriken/Berichte, sofern nicht ausdrücklich erwähnt, haben die Werte, die ihnen für den ausgewählten Zeitraum entsprechen.

Liniendiagramm

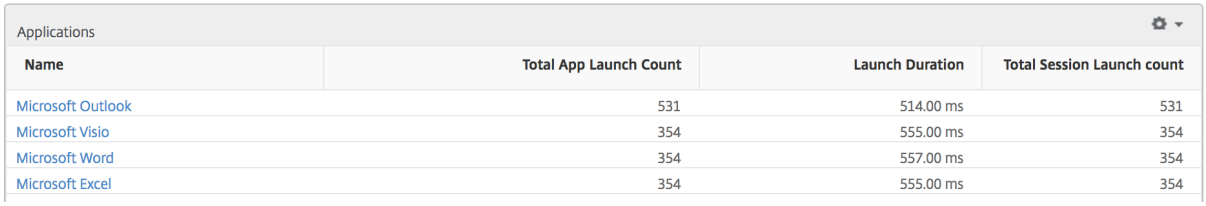
Metriken	Beschreibung
Anz. Sitzungen	Gesamtzahl der Sitzungen in einem bestimmten Zeitintervall.
Startdauer	Durchschnittliche Zeit zum Starten einer Anwendung.



Anwendungsübersichtsbericht

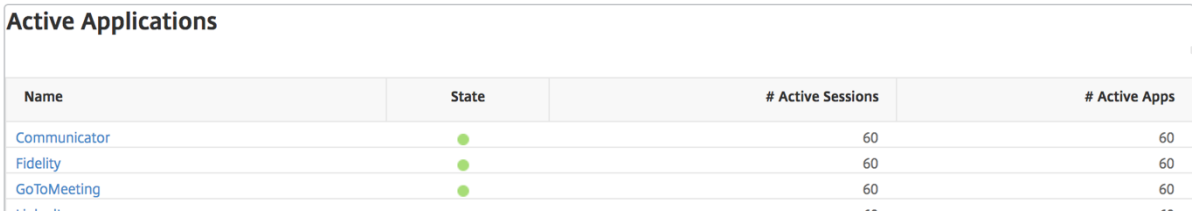
Metriken	Beschreibung
Name	Name der virtuellen Citrix App.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual App-Sitzungen während des angegebenen Zeitintervalls.

Metriken	Beschreibung
App-Starts insgesamt	Gesamtzahl der Citrix Virtual App-Anwendungen, die während des angegebenen Zeitintervalls gestartet wurden.
Startdauer	Durchschnittliche Zeit für den Start der Citrix Virtual App.



Bericht Aktive Anwendung

Metriken	Beschreibung
Name	Name der virtuellen Citrix App.
Status	Zeigt den Status der Anwendung an: Grün-Aktiv, Rot-Inaktiv
#Active Sitzungen	Anzahl der aktiven Benutzersitzungen, die diese App während eines bestimmten Zeitintervalls verwenden.
# Aktive Apps	Anzahl der aktiven Sitzungen für diese Anwendung.

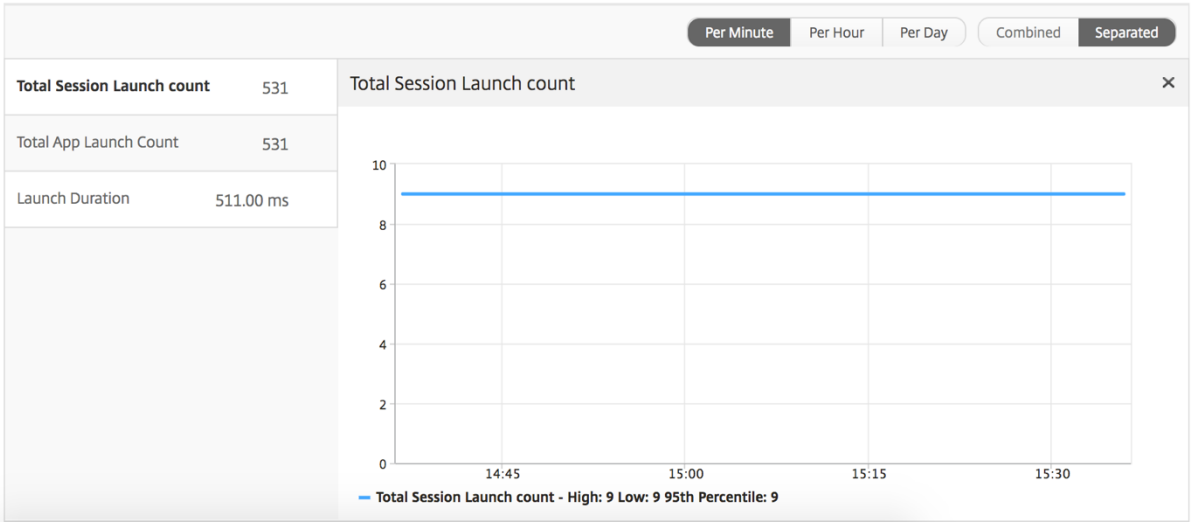


Schwellenwertbericht

Der Schwellenwertbericht stellt die Anzahl der Grenzwerte dar, die überschritten wurden, wenn die *Entität* im ausgewählten Zeitraum als Anwendung ausgewählt wurde.

Liniendiagramm

Metriken	Beschreibung
Anz. aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App- und Desktop-Sitzungen an.
Startdauer	Durchschnittliche Zeit zum Starten einer Anwendung.



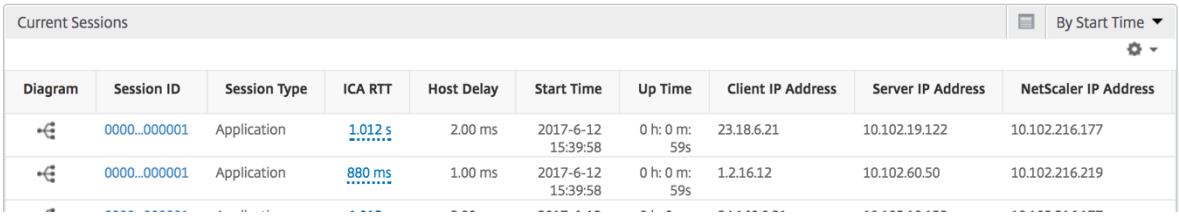
Bericht Aktuelle Sitzungen

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der die Citrix ADCs durchläuft, die durch das Servernetzwerk verursacht werden.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls belegt wird.
Sitzungsbandbreite	Die Bandbreite, die von der Sitzung verbraucht wird, unabhängig vom Zeitintervall.

Metriken	Beschreibung
Bytes pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls belegt werden.
Startzeit	Sitzungsstartzeit.
Betriebszeit	Sitzungsdauer.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management IP (NSIP).
Clienttyp	Empfängertyp: Citrix Windows Client.
Clientversion	Empfängerversion.
MSI	Boolean (Ja/Nein). Gibt an, ob die Sitzung Multi-Stream-ICA ist.
Sitzungswiederverbindungen	Anzahl der Wiederverbindung der Sitzung.
ACR-Anzahl	Gesamtzahl der Wiederanschlüsse, die ein Client Benutzer automatisch mit getrennten Sitzungen verbindet.
Benutzerzugriffstyp	Zeigt den Zugriffsmodus der ICA-Sitzung an. Beispiel: Citrix ADC Gateway-Benutzer/transparenter Modus.
Land	Land, aus dem die Sitzung gegründet wurde.
Region	Region, aus der die Sitzung gegründet wurde.
Stadt	Stadt, von der die Sitzung gegründet wurde.
USB-Status	Aktiv/Inaktiv - Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der angehaltenen USB-Instanzen	Die Anzahl der angehaltenen USB-Instanzen.
Clienthostname	Der Hostname des Clients.
HA-Failover-Anzahl	Anzahl der Fälle, in denen HA-Failover aufgetreten ist.

Metriken	Beschreibung
Grund für Abbruch	Zeigt den Grund für eine Sitzungsbeendigung an. Beispiel: ICA-Sitzungszeitüberschreitung, Sitzung vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen Citrix ADC und Back-End-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der für die Verbindung zwischen Citrix ADC und dem Endbenutzer neu übertragenen Pakete. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Anzahl, wie oft die Zeitüberschreitung der Verbindung zwischen Citrix ADC und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.

Metriken	Beschreibung
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen Citrix ADC und dem Backend-Server aufgetreten ist.
Benutzername	Der Benutzername des Benutzers, der auf diese bestimmte Citrix Virtual App zugreift.
Sitzungs-ID	Eindeutiger Bezeichner für die Citrix Virtual App-Sitzung.
Sitzungstyp	Wird Anwendung sein.
Status	Sitzungsstatus: Grün für aktiv, Rot für In-aktiv.
Maximale Verletzungslatenz	Der höchste Wert der L7-Latenz, wenn ein Verstoß gegen einen definierten Schwellenwert für ein eingestelltes Zeitintervall auftritt.
Durchschnittliche Verletzungslatenz	Der durchschnittliche Wert der L7-Latenz, wenn sich das System im Status L7-Latenz durchbrochen befindet.
L7-Schwellenwertverletzungsanzahl	Gibt an, wie oft eine L7-Schwellenverletzung aufgetreten ist.
L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der Citrix ADC-Instanz beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.
L7 Serverseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem Citrix ADC Gerät und der Citrix Virtual App beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.



Session-Ansicht pro Anwendung

Die Session-Ansicht pro Anwendung zeigt Berichte für eine bestimmte ausgewählte Anwendungssitzung an.

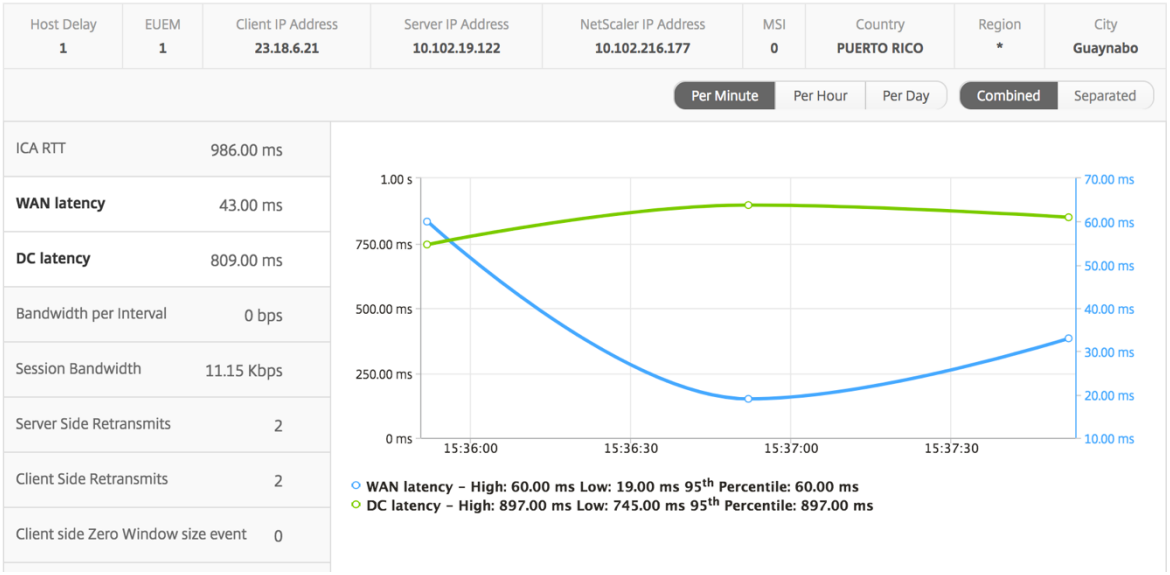
So zeigen Sie die Sitzungsberichte an:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Anwendungen**.
2. Wählen Sie im Anwendungsübersichtsbericht einen bestimmten Benutzer aus.
3. Eine Sitzung aus dem aktuellen Sitzungsbericht ausgewählt.

Liniendiagramm

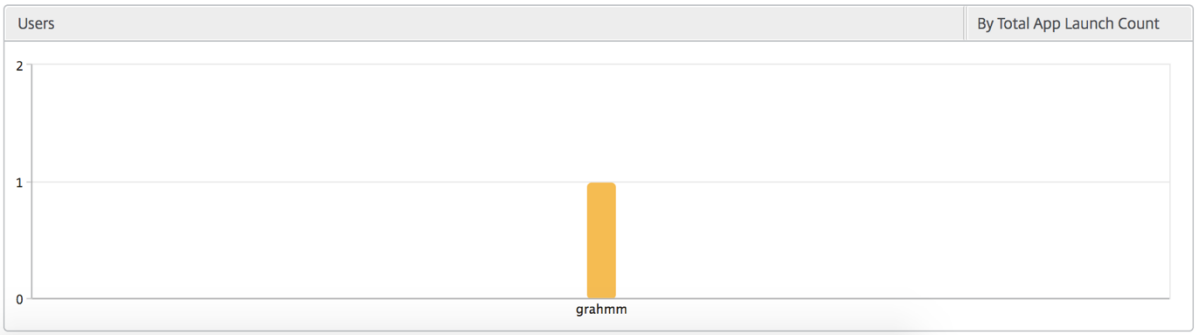
Metriken	Beschreibung
Sitzungswiederverbindungen	Anzahl der Wiederverbindung der Sitzung.
ACR-Anzahl	Gesamtzahl der Wiederanschlüsse, die ein Client Benutzer automatisch mit getrennten Sitzungen verbindet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
Serverseitiges Ereignis mit Zero Window-Größe	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls belegt wird.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen Citrix ADC und Back-End-Server übertragenen Pakete.

Metriken	Beschreibung
Clientseitige Neuübertragungen	Die Anzahl der für die Verbindung zwischen Citrix ADC und dem Endbenutzer neu übertragenen Pakete. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Sitzungsbandbreite	Die Bandbreite, die von der Sitzung verbraucht wird, unabhängig vom Zeitintervall.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Anzahl, wie oft die Zeitüberschreitung der Verbindung zwischen Citrix ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen Citrix ADC und dem Backend-Server aufgetreten ist.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.



Benutzerleistendiagramm

Das Balkendiagramm des **Benutzers** stellt die bei dieser bestimmten App angemeldeten Benutzer dar.



Desktop-View-Berichte und Metriken

April 28, 2021

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf den Citrix Virtual Desktop. Navigieren Sie zu **Analytics** > **HDX Insight** > **Desktop**

Zusammenfassende Ansicht

In der Zusammenfassungsansicht werden die Berichte für alle Citrix Virtual Desktops angezeigt, die während der ausgewählten Zeitachse angemeldet sind.

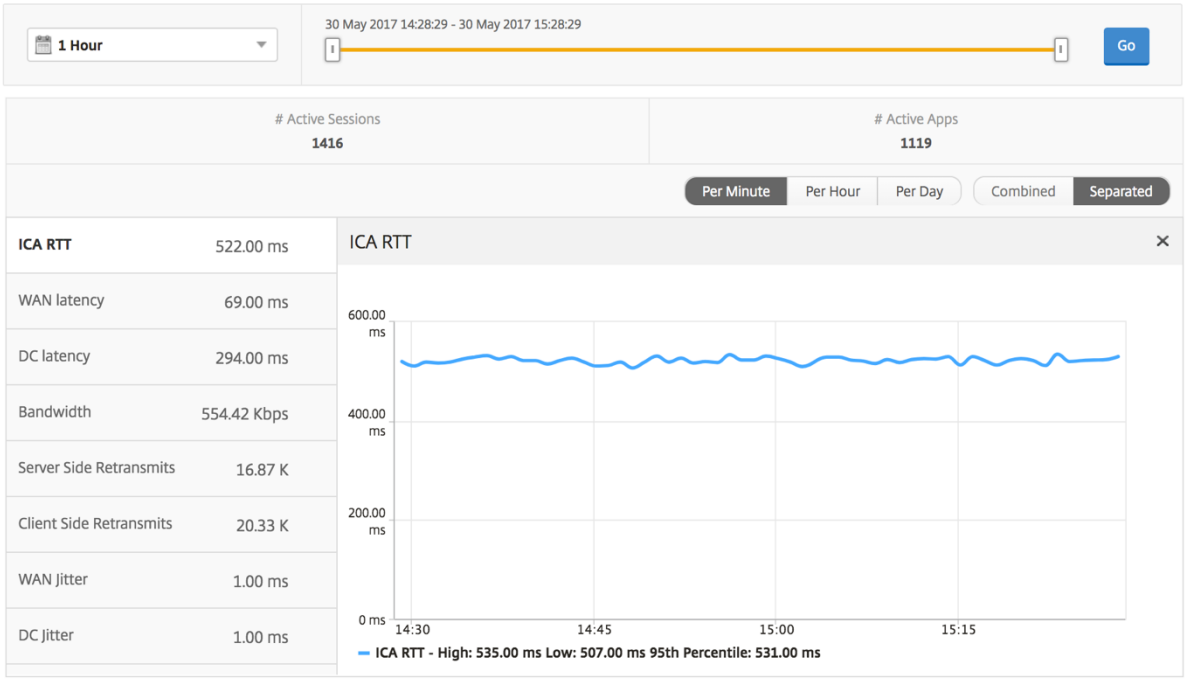
Alle unten aufgeführten Metriken/Berichte, sofern nicht explizit erwähnt, haben die Werte, die ihnen für den ausgewählten Zeitraum entsprechen.

Liniendiagramm

Metriken	Beschreibung
Anz. aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops -Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.

Metriken	Beschreibung
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.
Bandbreite	Gesamtzahl der Bytes pro Sekunde für die Kommunikation zwischen Ende und Ende während des ausgewählten Zeitintervalls.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen Citrix ADC und Back-End-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der für die Verbindung zwischen Citrix ADC und dem Endbenutzer neu übertragenen Pakete. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Anzahl, wie oft die Zeitüberschreitung der Verbindung zwischen Citrix ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen Citrix ADC und dem Backend-Server aufgetreten ist.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.

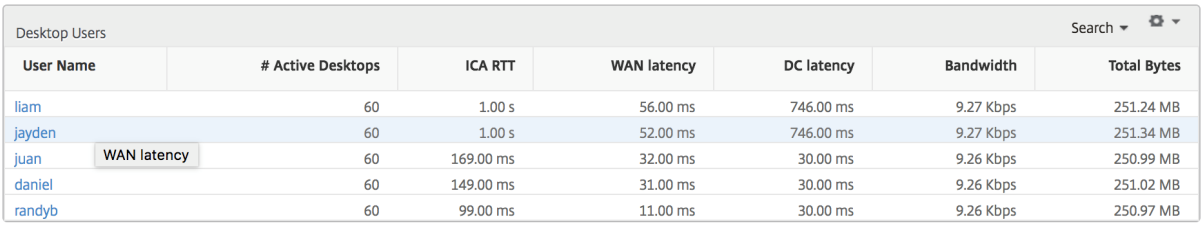
Metriken	Beschreibung
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.



Desktopübersichtsbericht

Metriken	Beschreibung
Aktive Sitzungen	Gesamtzahl der aktiven Citrix Virtual Desktop-Sitzungen in einem bestimmten Zeitintervall.
Aktive Desktops	Gesamtzahl der aktiven Citrix Virtual Desktops in einem bestimmten Zeitintervall.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.

Metriken	Beschreibung
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.
Bandbreite	Gesamtzahl der Bytes pro Sekunde für die Kommunikation zwischen Ende und Ende während des ausgewählten Zeitintervalls.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.



Schwellenwertbericht

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* in der ausgewählten Periode als Desktop ausgewählt wurde.

Pro Desktop-Ansicht

Pro Desktop-Ansicht bietet detaillierte Berichte über die Benutzerfreundlichkeit für einen ausgewählten Citrix Virtual Desktop.

So navigieren Sie zur bestimmten Desktopansicht:

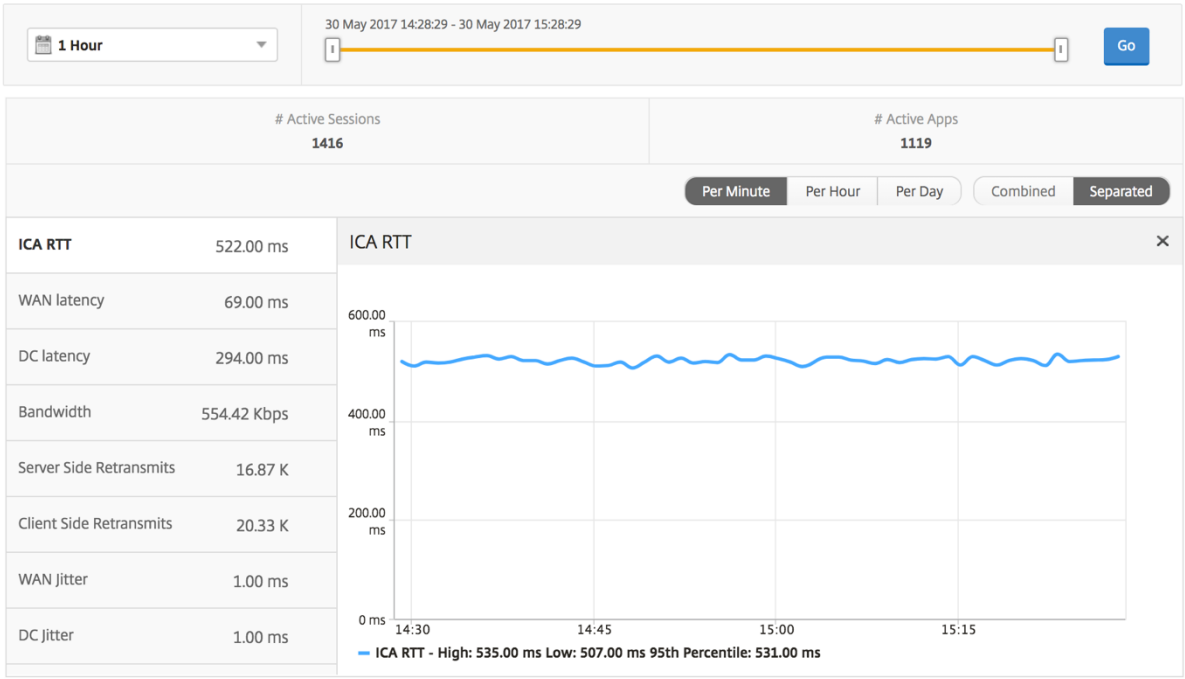
1. Navigieren Sie zu **Analytics > HDX Insight > Desktop**.
2. Wählen Sie im **Desktopübersichtsberichteinen bestimmten Desktop** aus.

Liniendiagramm

Metriken	Beschreibung
Anz. aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops -Sitzungen an.

Metriken	Beschreibung
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.
Bandbreite	Gesamtzahl der Bytes pro Sekunde für die Kommunikation zwischen Ende und Ende während des ausgewählten Zeitintervalls.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen Citrix ADC und Back-End-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der für die Verbindung zwischen Citrix ADC und dem Endbenutzer neu übertragenen Pakete. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Anzahl, wie oft die Zeitüberschreitung der Verbindung zwischen Citrix ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen Citrix ADC und dem Backend-Server aufgetreten ist.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.

Metriken	Beschreibung
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.

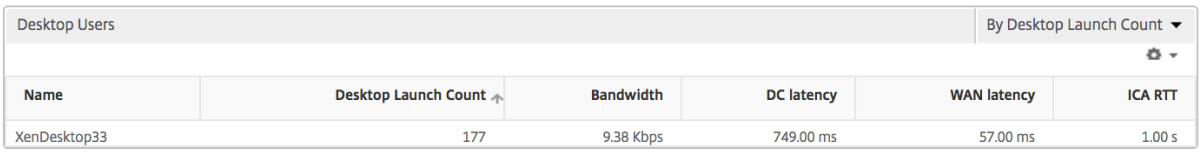


Desktopbenutzer-Bericht

Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Desktop-Launch-Anzahl und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des virtuellen Citrix Desktops.
Anzahl Desktopstarts	Anzahl, wie oft der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Bytes pro Sekunde für die Kommunikation zwischen Ende und Ende während des ausgewählten Zeitintervalls.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.

Metriken	Beschreibung
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.



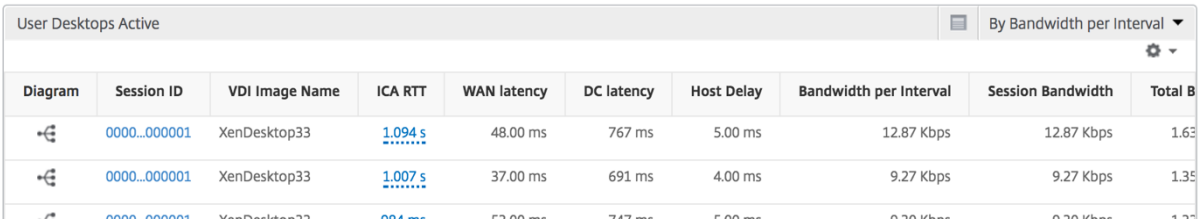
Benutzerdesktops Aktiv/Inaktiv Bericht

Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der die Citrix ADCs durchläuft, die durch das Servernetzwerk verursacht werden.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls belegt wird.
Sitzungsbandbreite	Die Bandbreite, die von der Sitzung verbraucht wird, unabhängig vom Zeitintervall.
Bytes pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls belegt werden.
Startzeit	Sitzungsstartzeit.

Metriken	Beschreibung
Betriebszeit	Sitzungsdauer.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management IP (NSIP).
Clienttyp	Empfängertyp: Citrix Windows Client
Clientversion	Empfängerversion.
MSI	Boolean (Ja/Nein). Gibt an, ob die Sitzung Multi-Stream-ICA ist.
Sitzungswiederverbindungen	Anzahl der Wiederverbindung der Sitzung.
ACR-Anzahl	Gesamtzahl der Wiederanschlüsse, die ein Client Benutzer automatisch mit getrennten Sitzungen verbindet.
Benutzerzugriffstyp	Zeigt den Zugriffsmodus der ICA-Sitzung an. Beispiel: Citrix ADC Gateway-Benutzer/transparenter Modus.
Land	Land, aus dem die Sitzung gegründet wurde.
Region	Region, aus der die Sitzung gegründet wurde.
Stadt	Stadt, von der die Sitzung gegründet wurde.
USB-Status	Aktiv/Inaktiv - Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der angehaltenen USB-Instanzen	Die Anzahl der angehaltenen USB-Instanzen.
Clienthostname	Der Hostname des Clients.
HA-Failover-Anzahl	Anzahl der Fälle, in denen HA-Failover aufgetreten ist.
Grund für Abbruch	Zeigt den Grund für eine Sitzungsbeendigung an. Beispiel: ICA-Sitzungszeitüberschreitung, Sitzung vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.

Metriken	Beschreibung
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen Citrix ADC und Back-End-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der für die Verbindung zwischen Citrix ADC und dem Endbenutzer neu übertragenen Pakete. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Anzahl, wie oft die Zeitüberschreitung der Verbindung zwischen Citrix ADC und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen Citrix ADC und dem Backend-Server aufgetreten ist.
VDI-Imagename	Name des Citrix Virtual Desktop, mit dem der Benutzer verbunden ist
Diagramm	



Ansicht pro Desktop-Sitzung

Pro Desktop-Sitzungsansicht stellt Berichte für eine bestimmte ausgewählte Citrix Virtual Desktop-Sitzung bereit.

So navigieren Sie zur Desktop-Sitzungsansicht:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Desktop**.
2. Wählen Sie im **Desktopübersichtsbericht einen bestimmten Desktop**aus.
3. Wählen Sie eine Sitzung aus dem aktuellen Sitzungsbericht aus.

Zeitleistendiagramm

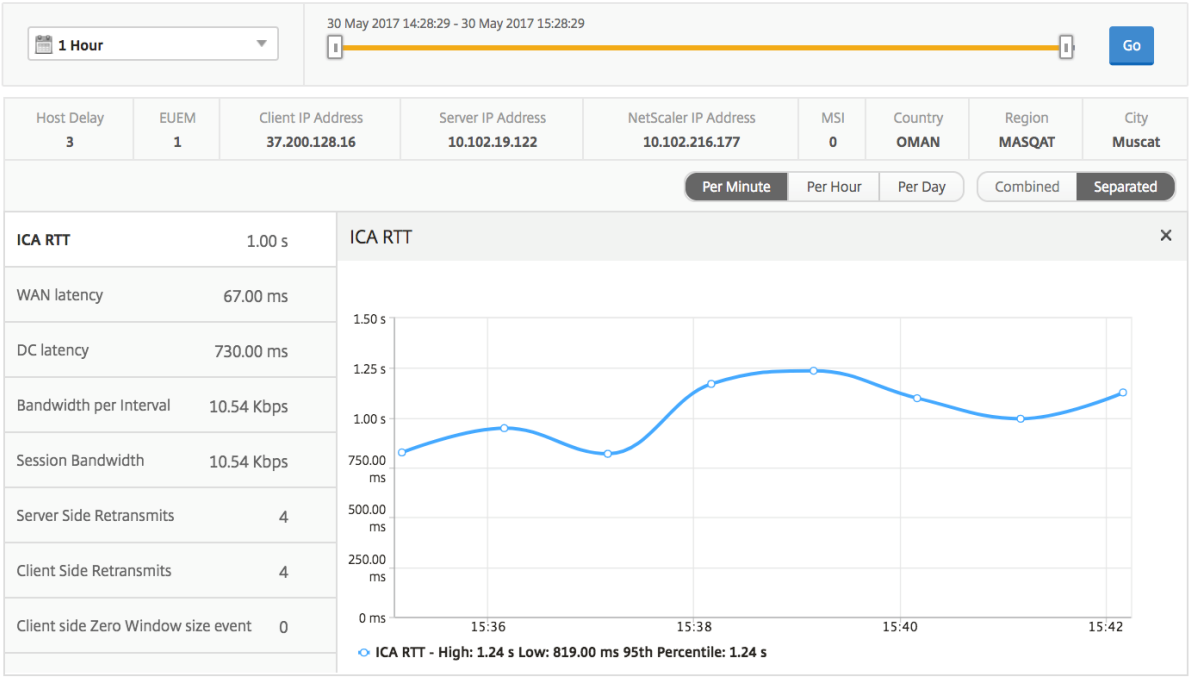
Die Sitzungsansicht pro Benutzer stellt Berichte für die Sitzung eines bestimmten ausgewählten Benutzers bereit.

So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**.
2. Wählen Sie im Abschnitt **Benutzerübersichtsbericht** einen bestimmten Benutzer aus.
3. Wählen Sie eine Sitzung in der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** aus.

Metriken	Beschreibung
Sitzungswiederverbindungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops -Sitzungen an.
ACR-Anzahl	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.

Metriken	Beschreibung
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.
Sitzungsbandbreite	Die Bandbreite, die von der Sitzung verbraucht wird, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen Citrix ADC und Back-End-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der für die Verbindung zwischen Citrix ADC und dem Endbenutzer neu übertragenen Pakete. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Anzahl, wie oft die Zeitüberschreitung der Verbindung zwischen Citrix ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen Citrix ADC und dem Backend-Server aufgetreten ist.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls belegt wird.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.



Bericht zu verwandten Desktop-Sitzungen

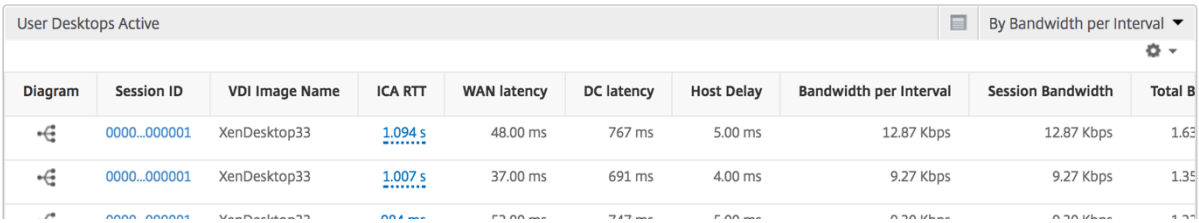
Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der die Citrix ADCs durchläuft, die durch das Servernetzwerk verursacht werden.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls belegt wird.
Sitzungsbandbreite	Die Bandbreite, die von der Sitzung verbraucht wird, unabhängig vom Zeitintervall.
Bytes pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls belegt werden.

Metriken	Beschreibung
Startzeit	Sitzungsstartzeit.
Betriebszeit	Sitzungsdauer.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management IP (NSIP).
Clienttyp	Empfängertyp: Citrix Windows Client
Clientversion	Empfängerversion.
MSI	Boolean (Ja/Nein). Gibt an, ob die Sitzung Multi-Stream-ICA ist.
Sitzungswiederverbindungen	Anzahl der Wiederverbindung der Sitzung.
ACR-Anzahl	Gesamtzahl der Wiederanschlüsse, die ein Client Benutzer automatisch mit getrennten Sitzungen verbindet.
Benutzerzugriffstyp	Zeigt den Zugriffsmodus der ICA-Sitzung an. Beispiel: Citrix ADC Gateway-Benutzer/transparenter Modus.
Land	Land, aus dem die Sitzung gegründet wurde.
Region	Region, aus der die Sitzung gegründet wurde.
Stadt	Stadt, von der die Sitzung gegründet wurde.
USB-Status	Aktiv/Inaktiv - Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der angehaltenen USB-Instanzen	Die Anzahl der angehaltenen USB-Instanzen.
Clienthostname	Der Hostname des Clients.
HA-Failover-Anzahl	Anzahl der Fälle, in denen HA-Failover aufgetreten ist.
Grund für Abbruch	Zeigt den Grund für eine Sitzungsbeendigung an. Beispiel: ICA-Sitzungszeitüberschreitung, Sitzung vom Benutzer beendet.

Metriken	Beschreibung
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen Citrix ADC und Back-End-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der für die Verbindung zwischen Citrix ADC und dem Endbenutzer neu übertragenen Pakete. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Anzahl, wie oft die Zeitüberschreitung der Verbindung zwischen Citrix ADC und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.

Metriken	Beschreibung
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen Citrix ADC und dem Backend-Server aufgetreten ist.
VDI-Imagename	Name des Citrix Virtual Desktop, mit dem der Benutzer verbunden ist

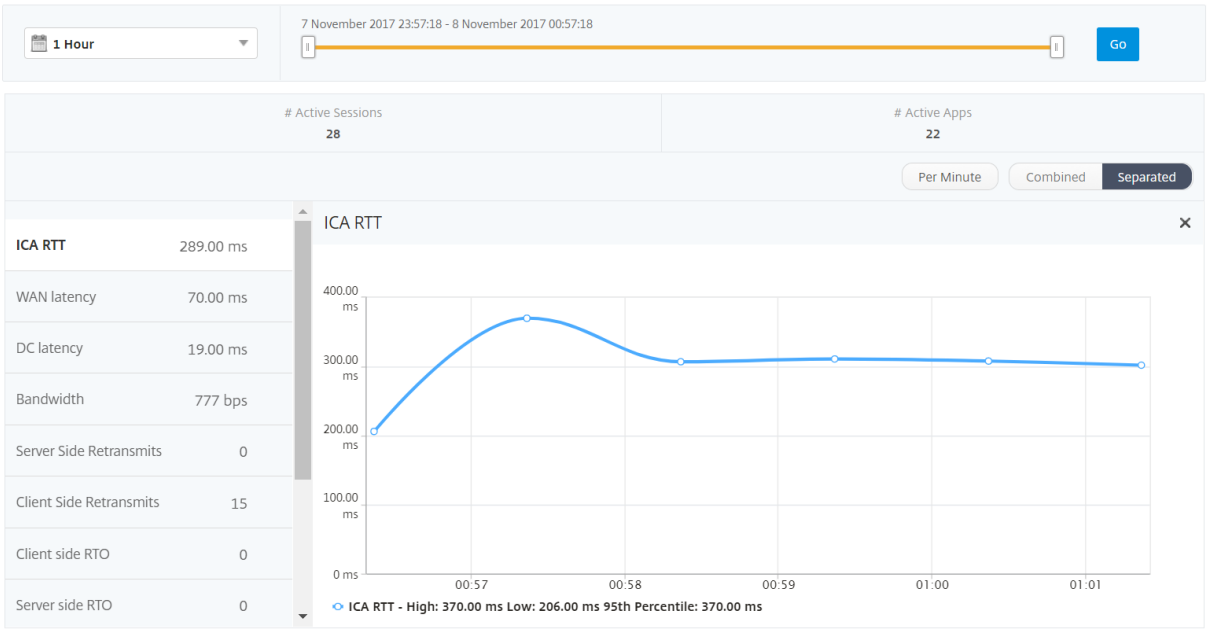


Berichte und Metriken der Benutzeransicht

April 28, 2021

Die Berichte und Metriken in dieser Ansicht werden pro Citrix Virtual App- oder Desktop-Benutzer angezeigt.

Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**



Übersichtsansicht

In der Zusammenfassungsansicht werden die Berichte für alle Benutzer angezeigt, die sich während der ausgewählten Zeitachse angemeldet haben. Alle Metriken/Berichte in dieser Ansicht zeigen, sofern nicht anders angegeben, die ihnen entsprechenden Werte für den ausgewählten Zeitraum an.

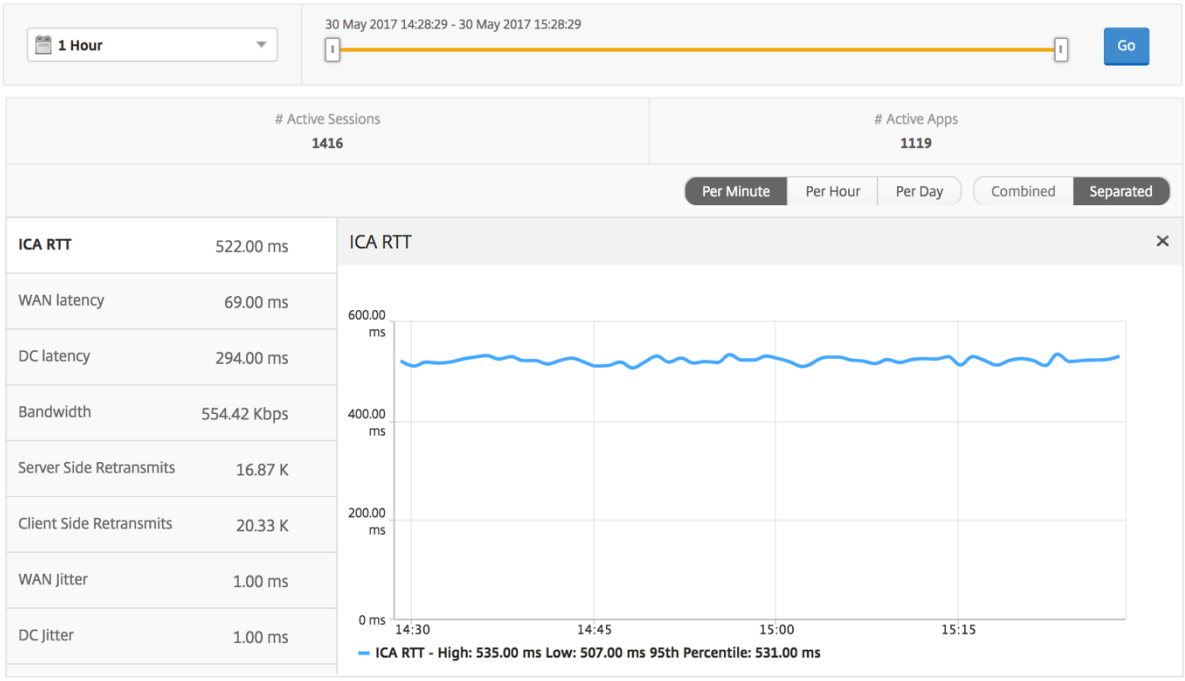
So ändern Sie den ausgewählten Zeitraum:

1. Verwenden Sie die Zeitperiodenliste oder den Zeitschieberegler, um das gewünschte Zeitintervall festzulegen.
2. Klicken Sie auf **Go**.

Liniendiagramm

Metriken	Beschreibung
Anz. aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops -Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.
Bandbreite	Gesamtbits pro Sekunde, die während des ausgewählten Zeitintervalls für die End-zu-Ende-Kommunikation verwendet werden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen Citrix ADC und Back-End-Server übertragenen Pakete.

Metriken	Beschreibung
Clientseitige Neuübertragungen	Die Anzahl der für die Verbindung zwischen Citrix ADC und dem Endbenutzer neu übertragenen Pakete. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Anzahl, wie oft die Zeitüberschreitung der Verbindung zwischen Citrix ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen Citrix ADC und dem Backend-Server aufgetreten ist.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.



Benutzerübersichtsbericht

Im Folgenden finden Sie die Metriken, die für diesen Bericht spezifisch sind.

Metriken	Beschreibung
Anz. aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops -Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.

Metriken	Beschreibung
Bandbreite	Gesamtbits pro Sekunde, die während des ausgewählten Zeitintervalls für die End-zu-Ende-Kommunikation verwendet werden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen Citrix ADC und Back-End-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der für die Verbindung zwischen Citrix ADC und dem Endbenutzer neu übertragenen Pakete. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Anzahl, wie oft die Zeitüberschreitung der Verbindung zwischen Citrix ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen Citrix ADC und dem Backend-Server aufgetreten ist.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
App-Starts insgesamt	Gesamtzahl der Apps, die vom Benutzer während des ausgewählten Zeitraums gestartet wurden.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Aktive Desktops	Gesamtzahl der aktiven Citrix Virtual Desktops in einem bestimmten Zeitintervall.

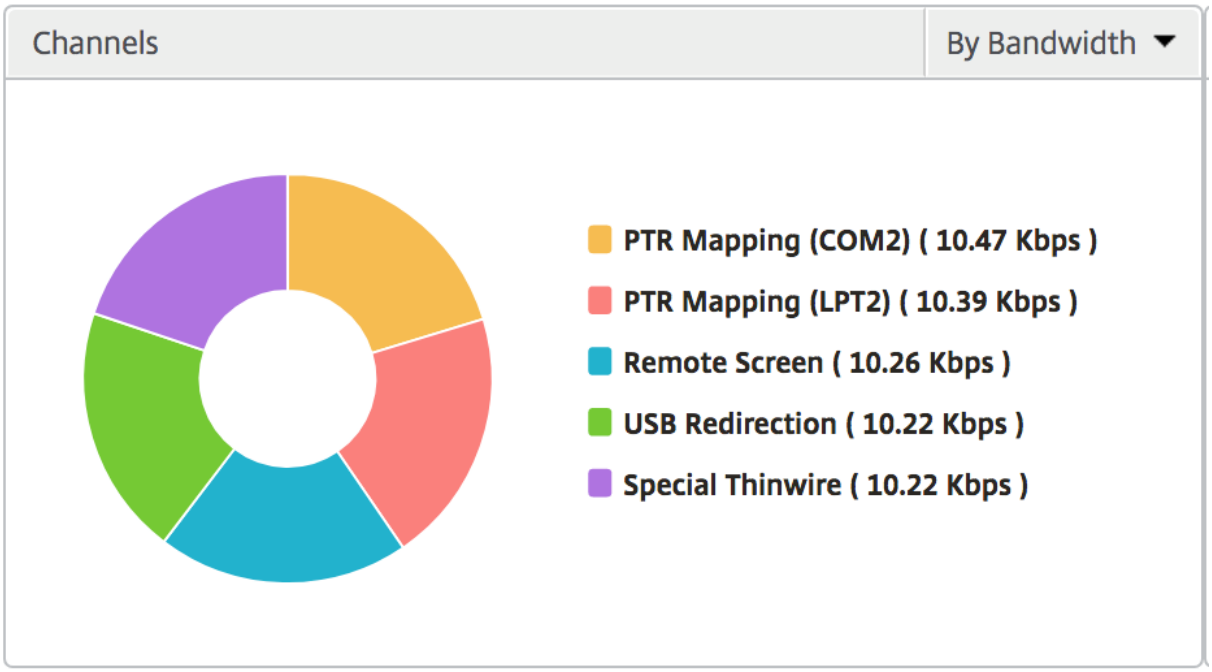
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

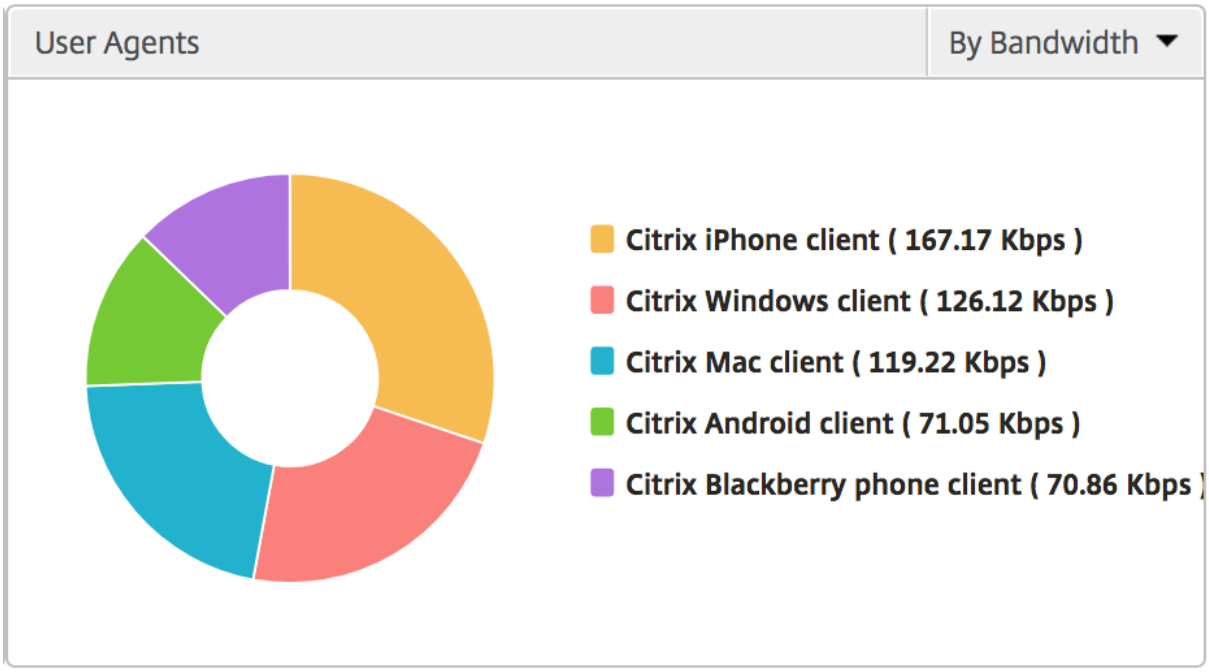
Kanäle

Kanäle stellen die Gesamtbandbreite oder die Gesamtbytes dar, die von jedem virtuellen ICA-Kanal in Form eines Donutdiagramms belegt werden. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Benutzeragents

User Agents stellen die Gesamtbandbreite/Gesamtsumme Bits dar, die von jedem Endpunkt in Form eines Donut-Diagramms verbraucht werden. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Anzahl der Schwellenwerte für Verstöße

Die Metriken für die Anzahl der Schwellenwerte für Verstöße stellen die Anzahl der Schwellenwerte dar, die im ausgewählten Zeitraum überschritten wurden.

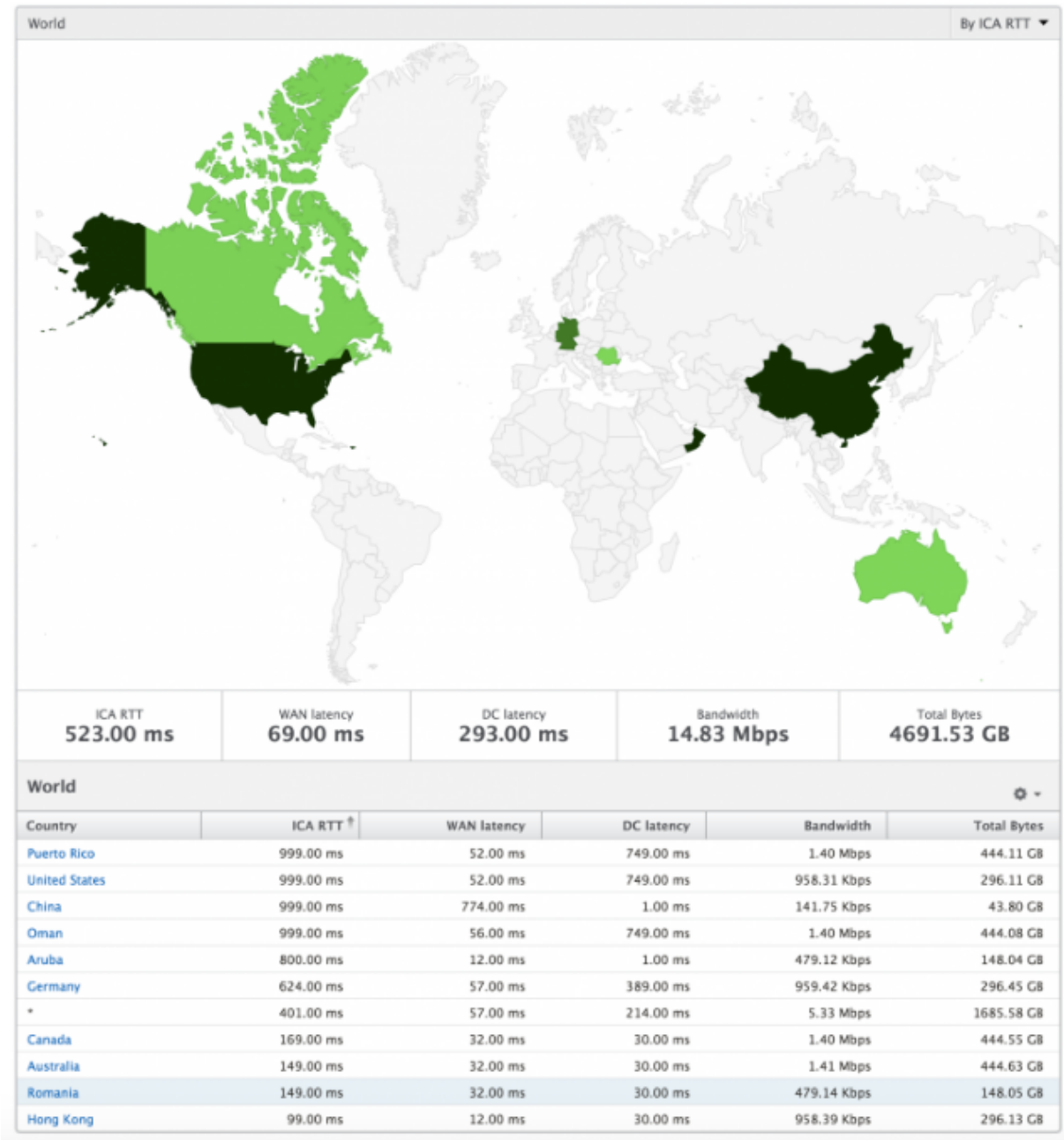
Weltkarte

Mit der Weltkartenansicht in HDX Insight können Administratoren die historischen und aktiven Benutzerdetails aus geografischer Sicht anzeigen. Die Administratoren können durch einfaches Klicken auf die Region einen Überblick über das System haben, einen Drilldown zu einem bestimmten Land und weiter in die Städte einsehen. Die Administratoren können weitere Informationen nach Stadt und Bundesstaat anzeigen. Ab Citrix ADM Version 12.0 und höher können Sie einen Drilldown für Benutzer durchführen, die von einem Geostandort aus verbunden sind.

Die folgenden Details können auf der Weltkarte in HDX Insight angezeigt werden, und die Dichte jeder Metrik wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz

- Bandbreite
- Bytes insgesamt



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Ansicht pro Benutzer

Die Ansicht pro Benutzer bietet detaillierte Berichte über die Endbenutzererfahrung für einen bestimmten ausgewählten Benutzer.

So navigieren Sie zu den Metriken bestimmter Benutzer:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**.

2. Wählen Sie im Übersichtsbericht Benutzer einen bestimmten Benutzer aus.

Liniendiagramm

Liniendiagramm zeigt die Zusammenfassung aller Metriken für den ausgewählten Benutzer während des ausgewählten Zeitraums.

Bericht Aktuelle und abgebrochene Sitzungen

Dieser Bericht ist relevant für alle aktuellen/beendeten Benutzersitzungen für den ausgewählten Benutzer. Diese Metriken können nach Startzeit, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der die Citrix ADCs durchläuft, die durch das Servernetzwerk verursacht werden.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls belegt wird.
Sitzungsbandbreite	Die Bandbreite, die von der Sitzung verbraucht wird, unabhängig vom Zeitintervall.
Bytes pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls belegt werden.
Startzeit	Sitzungsstartzeit.
Betriebszeit	Sitzungsdauer.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/ IP des Citrix Virtual App-Servers.
NetScaler IP-Adresse	NetScaler Management IP (NSIP).
Clienttyp	Empfängertyp: Citrix Windows Client
Clientversion	Empfängerversion.

Metriken	Beschreibung
MSI	Boolean (Ja/Nein). Gibt an, ob die Sitzung Multi-Stream-ICA ist.
Sitzungswiederverbindungen	Anzahl der Wiederverbindung der Sitzung.
ACR-Anzahl	Gesamtzahl der Wiederanschlüsse, die ein Client Benutzer automatisch mit getrennten Sitzungen verbindet.
Benutzerzugriffstyp	Zeigt den Zugriffsmodus der ICA-Sitzung an. Beispiel: Citrix ADC Gateway-Benutzer/transparenter Modus.
Land	Land, aus dem die Sitzung gegründet wurde.
Region	Region, aus der die Sitzung gegründet wurde.
Stadt	Stadt, von der die Sitzung gegründet wurde.
USB-Status	Aktiv/Inaktiv - Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der angehaltenen USB-Instanzen	Die Anzahl der angehaltenen USB-Instanzen.
Clienthostname	Der Hostname des Clients.
HA-Failover-Anzahl	Anzahl der Fälle, in denen HA-Failover aufgetreten ist.
Grund für Abbruch	Zeigt den Grund für eine Sitzungsbeendigung an. Beispiel: ICA-Sitzungszeitüberschreitung, Sitzung vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.

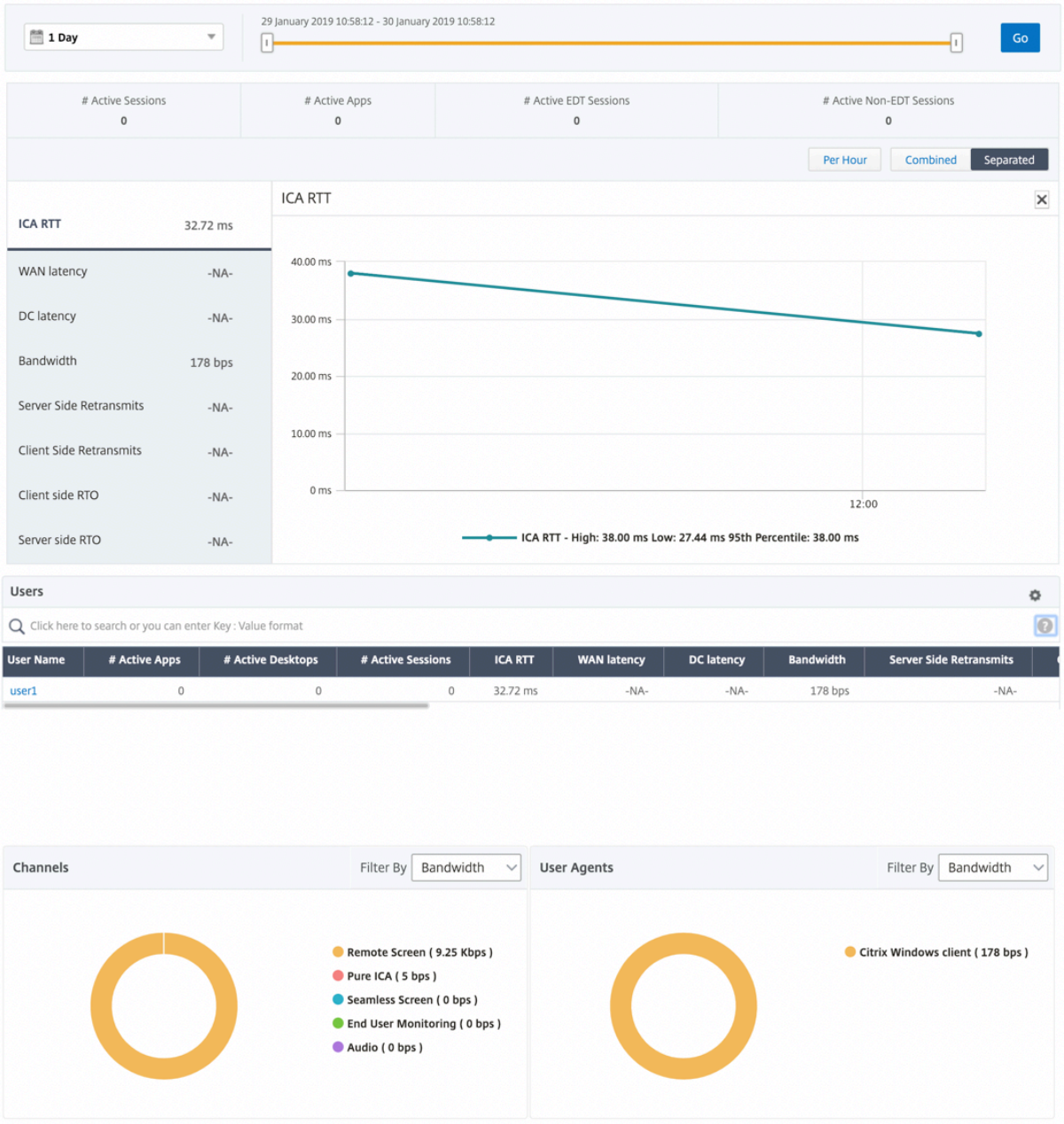
Metriken	Beschreibung
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen Citrix ADC und Back-End-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der für die Verbindung zwischen Citrix ADC und dem Endbenutzer neu übertragenen Pakete. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Anzahl, wie oft die Zeitüberschreitung der Verbindung zwischen Citrix ADC und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen dem Citrix ADC und dem Backend-Server aufgetreten ist.

Unterstützung für EDT in HDX Insight

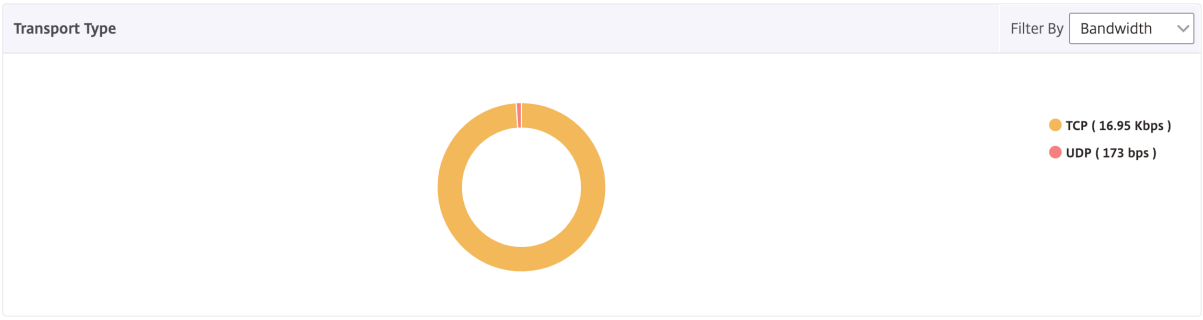
Citrix Application Delivery Management (ADM) unterstützt jetzt EDT (Enlightened Data Transport) für die Anzeige von Analysen für HDX Insight. Das heißt, ADM unterstützt jetzt sowohl das UDP- als auch das TCP-Protokoll. Die EDT-Unterstützung für Citrix Gateway stellt für Benutzer, die Citrix Receiver ausführen, eine High-Definition-Benutzererfahrung virtueller Desktops sicher.

HDX Insight zeigt nun die Anzahl der EDT-Sitzungen und Nicht-EDT-Sitzungen als Teil des Berichts für aktive Sitzungen an. In der Tabelle Benutzer wird ein detaillierter Bericht aller Benutzer im System

angezeigt. Die Tabelle zeigt Metriken wie WAN-Latenz, DC-Latenz, Retransmits, RTOs und einige dieser Metriken sind nicht für Benutzer verfügbar, die über EDT-Sitzungen verfügen, da sie derzeit aus dem TCP-Stack berechnet werden. Daher erscheinen sie als “NA”.

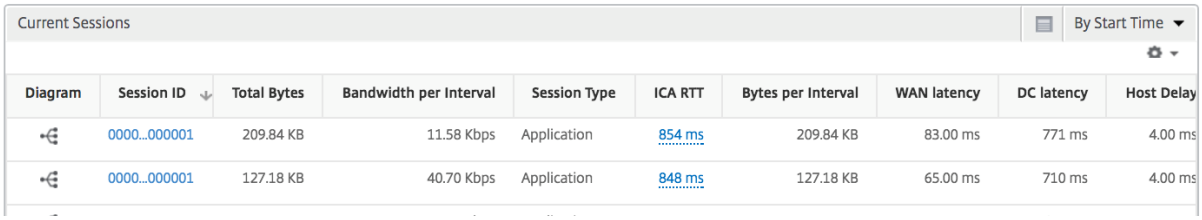


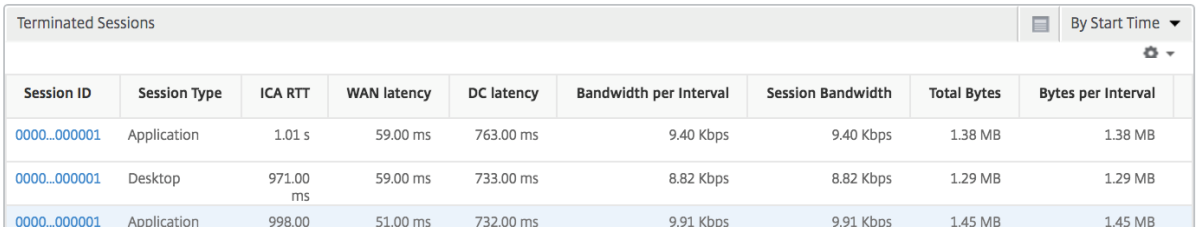
Es wurde ein neues Donutdiagramm eingeführt, mit dem Sie die vom Benutzer verbrauchte Bandbreite und die Gesamtzahl der Bytes basierend auf dem von den Benutzern verwendeten Protokolltyp sehen können.



HDX Insight Metriken ab Citrix ADM 12.0 verfügbar

L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der Citrix ADC-Instanz beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.
L7 Serverseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem Citrix ADC Gerät und der Citrix Virtual App beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.
Maximale Verletzungslatenz	Der höchste Wert der L7-Latenz, wenn ein Verstoß gegen einen definierten Schwellenwert für ein eingestelltes Zeitintervall auftritt.
Durchschnittliche Verletzungslatenz	Der durchschnittliche Wert der L7-Latenz, wenn sich das System im Status L7-Latenz durchbrochen befindet.
L7-Schwellenwertverletzungsanzahl	Gibt an, wie oft eine L7-Schwellenverletzung aufgetreten ist.

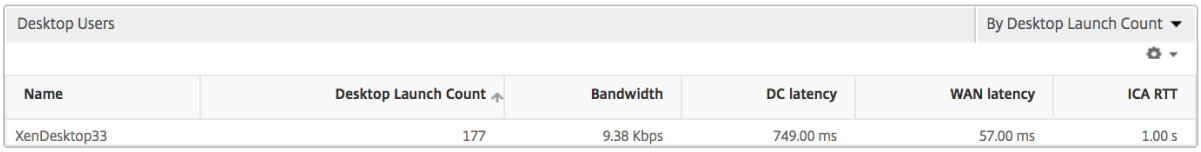




Desktopbenutzer

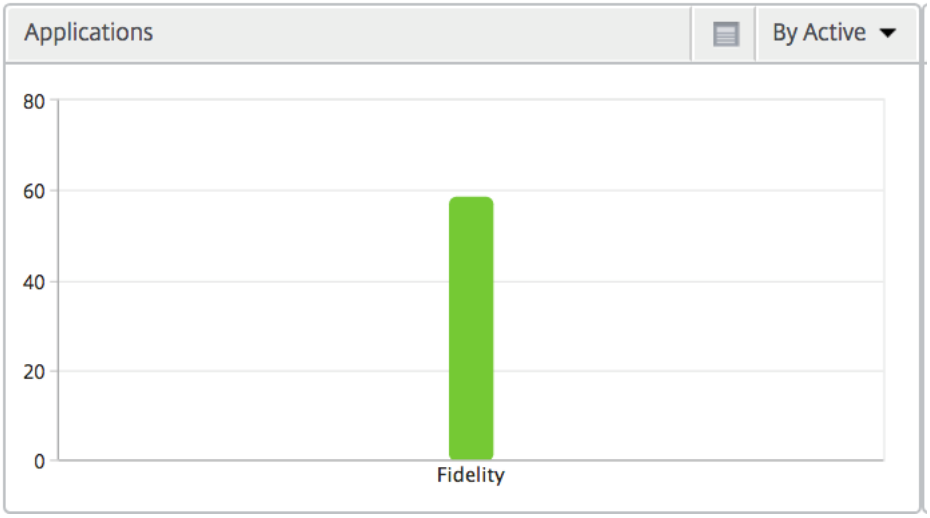
Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Desktop-Launch-Anzahl und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des virtuellen Citrix Desktops.
Anzahl Desktopstarts	Anzahl, wie oft der Desktop gestartet wurde.
Bandbreite	Gesamtbits pro Sekunde, die während des ausgewählten Zeitintervalls für die End-zu-Ende-Kommunikation verwendet werden.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.



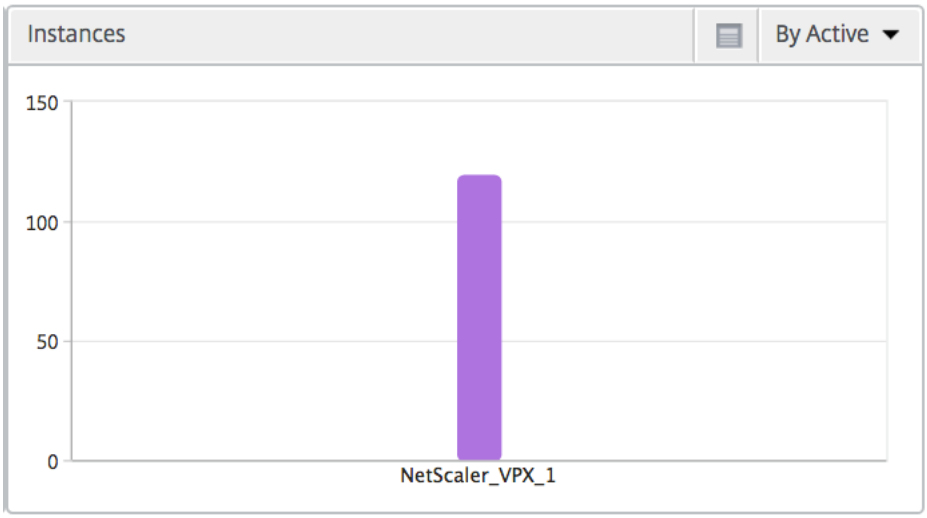
Anwendungen

Ein Balkendiagramm, das Apps sortiert nach Aktiv, Gesamtzahl der Sitzungsstarts, Gesamtanzahl des App-Starts und Startdauer darstellt.



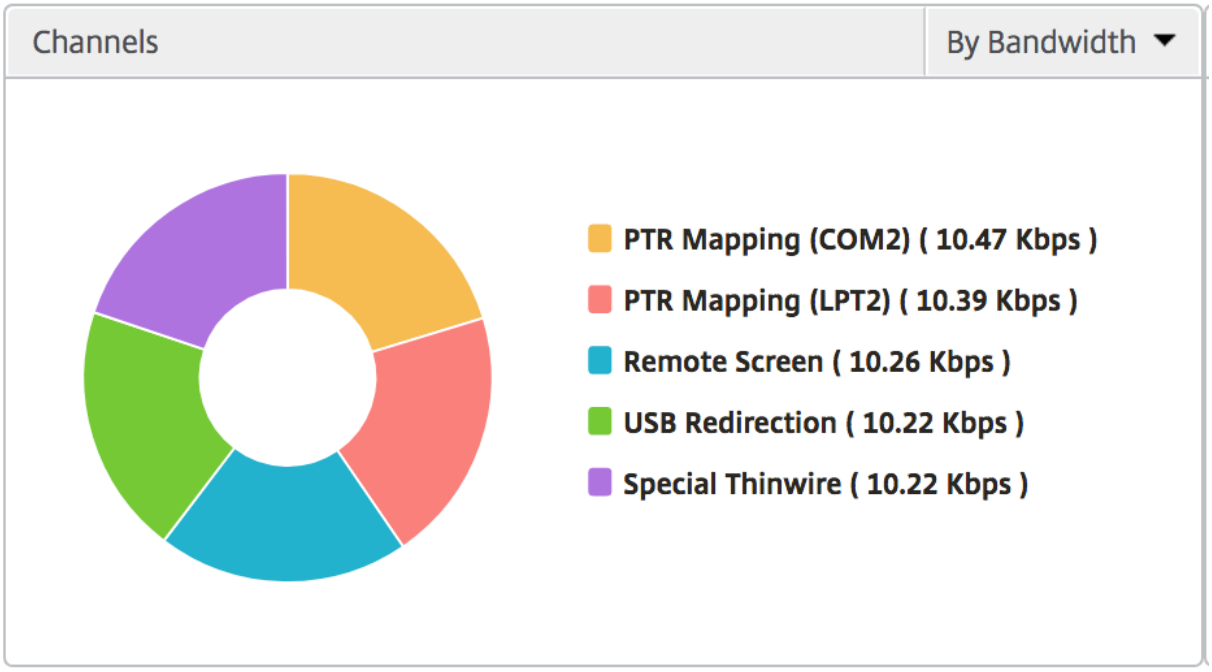
Instanzen

Ein Balkendiagramm, das ADC-Instanzen darstellt, sortiert nach aktiven und insgesamt Apps



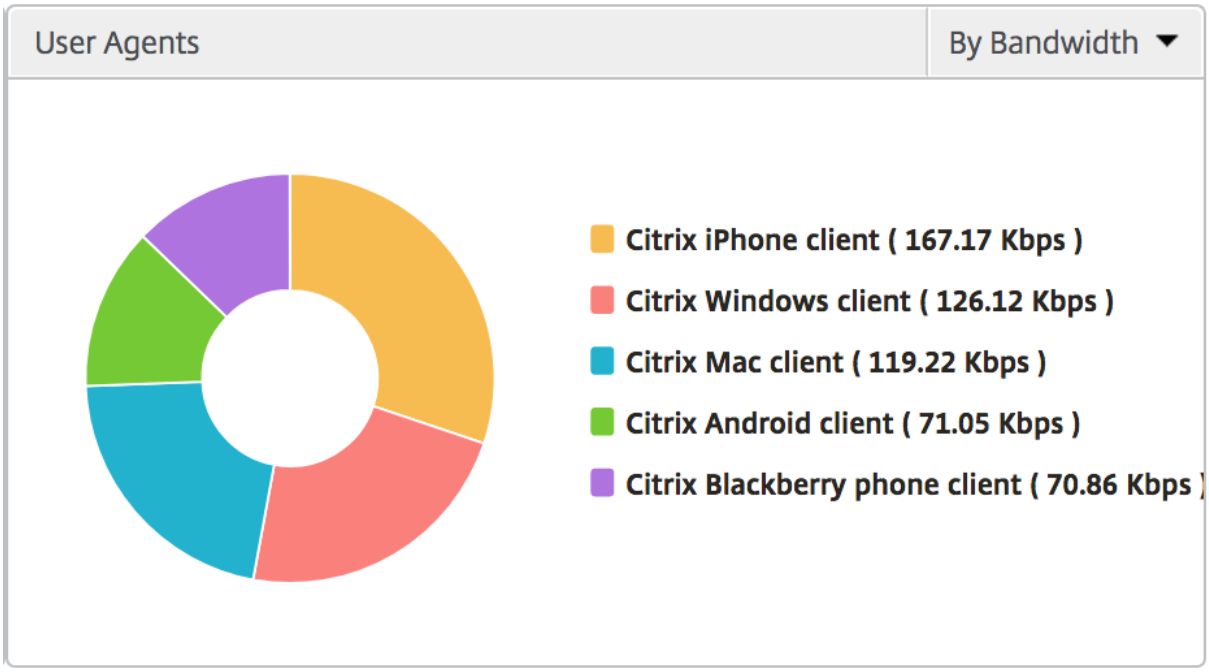
Kanäle

Kanäle stellen die Gesamtbandbreite oder die Gesamtmenge der von jedem virtuellen ICA-Kanal verbrauchten Bits in Form eines Donut-Charts dar. Sie können die Metriken auch nach Bandbreite oder Gesamtbits sortieren.



Benutzeragents

User Agents stellen die Gesamtbandbreite/Gesamtsumme Bits dar, die von jedem Endpunkt in Form eines Donut-Diagramms verbraucht werden. Sie können die Metriken auch nach Bandbreite oder Gesamtbits sortieren.



Session-Ansicht pro Benutzer

Die Sitzungsansicht pro Benutzer stellt Berichte für die Sitzung eines bestimmten ausgewählten Benutzers bereit.

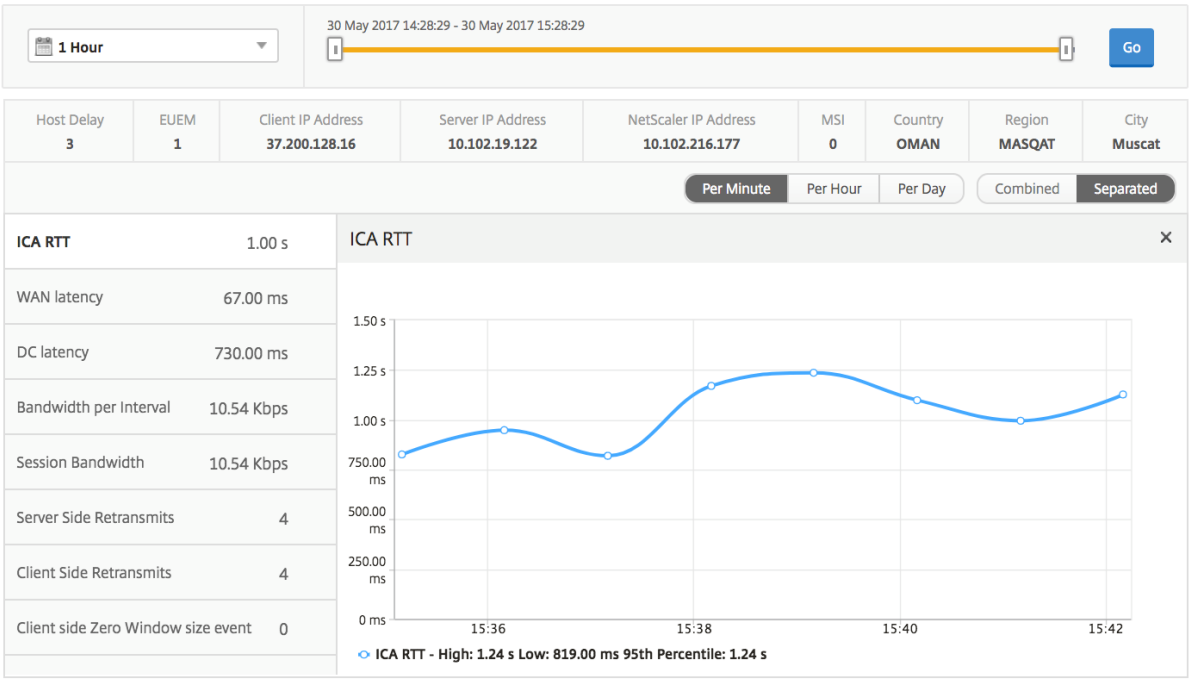
So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**.
2. Wählen Sie im Abschnitt **Benutzerübersichtsbericht** einen bestimmten Benutzer aus.
3. Wählen Sie eine Sitzung in der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** aus.

Zeitleistendiagramm

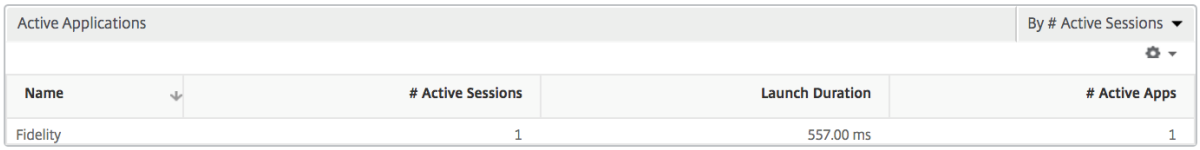
Metriken	Beschreibung
Sitzungswiederverbindungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops -Sitzungen an.
ACR-Anzahl	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.
Sitzungsbandbreite	Die Bandbreite, die von der Sitzung verbraucht wird, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen Citrix ADC und Back-End-Server übertragenen Pakete.

Metriken	Beschreibung
Clientseitige Neuübertragungen	Die Anzahl der für die Verbindung zwischen Citrix ADC und dem Endbenutzer neu übertragenen Pakete. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Anzahl, wie oft die Zeitüberschreitung der Verbindung zwischen Citrix ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen Citrix ADC und dem Backend-Server aufgetreten ist.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls belegt wird.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.



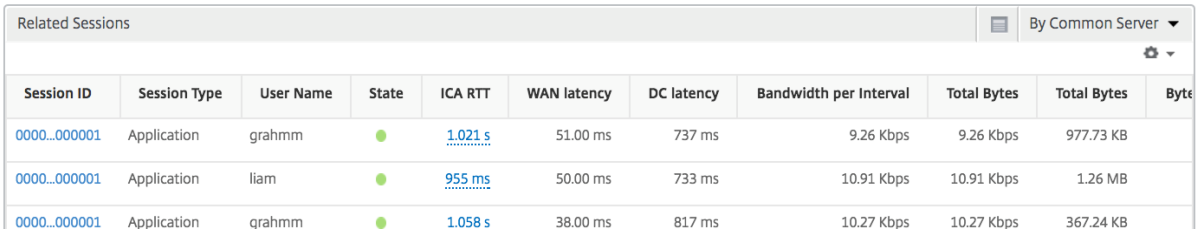
Aktive Anwendung

Im Abschnitt **Aktive Anwendungen** werden die aktiven Anwendungen des ausgewählten Benutzers angezeigt. Diese Anwendungen können auch nach Anzahl der aktiven Sitzungen und Startdauer sortiert werden.



Verbundene Sitzungen

Im Abschnitt Zugehörige Sitzungen werden die zugehörigen Sitzungen der Sitzungen des ausgewählten Benutzers angezeigt. Die Beziehung kann als gemeinsame Server oder gemeinsames Citrix ADC ausgewählt werden.



Instanzansichtsberichte und -metriken

April 28, 2021

Die Berichte und Metriken in der Instanzansicht konzentrieren sich auf eine oder mehrere Citrix ADC-Instanzen.

So navigieren Sie zur Instanzansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem Citrix ADM an.
2. Navigieren Sie zu **Analytics** > **HDX Insight** > **Instanzen**.

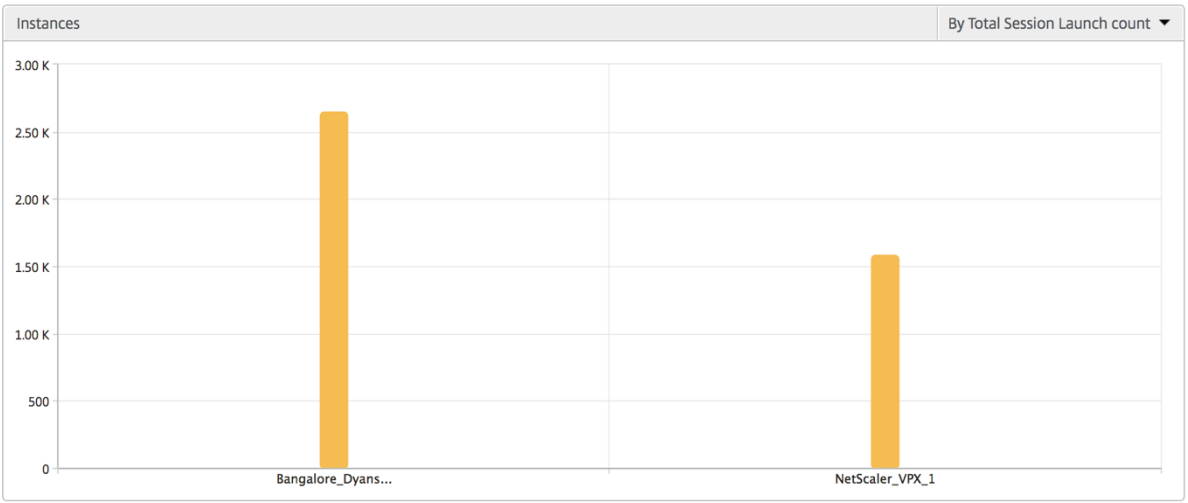
Instanzzusammenfassungsansicht

Diese Ansicht wird als Sammelansicht bezeichnet, da sie die Berichte für alle ADC-Instanzen anzeigt, die Citrix ADM hinzugefügt werden.

Alle diese Metriken/Berichte, sofern nicht ausdrücklich erwähnt, haben die Werte, die ihnen für den ausgewählten Zeitraum entsprechen.

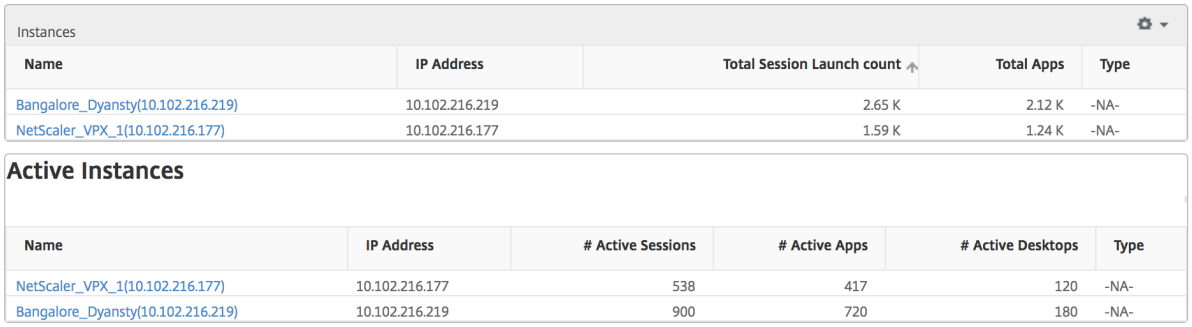
Instanzbalkendiagramm

Dieses Diagramm zeigt die Instanz im Vergleich zur Gesamtzahl der Sitzungsstarts und der Gesamtzahl der Apps aus der Liste oben rechts auf der Diagrammfläche an.



Instanz-/Aktive Instanzen - Übersicht

Metriken	Beschreibung
Name	Hostname der ADC-Instanz.
IP-Adresse	NetScaler IP-Adresse.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der eindeutigen Benutzersitzungen, die während eines bestimmten Zeitintervalls erstellt wurden.
Apps insgesamt	Gesamtzahl der eindeutigen Anwendungen, die während eines bestimmten Zeitintervalls gestartet wurden.
Typ	Nicht zutreffend



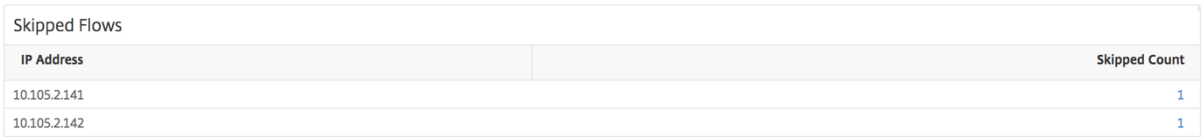
Schwellenwertbericht

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* in der ausgewählten Periode als Instanz ausgewählt wurde. Weitere Informationen finden Sie unter wie Schwellenwerte und Warnungen erstellt werden.

Übersprungene Flüsse

Ein übersprungener Flow ist ein Datensatz, der die Parsing ICA-Verbindung übersprungen hat. Dieser Ablauf kann aus mehreren Gründen auftreten, wie z. B. die Verwendung nicht unterstützter Citrix Virtual App- oder Desktop-Versionen, nicht unterstützter Version des Empfänger- oder Empfängertyps usw. Diese Tabelle zeigt die IP-Adresse und die Anzahl der übersprungenen Flows. Diese Empfänger sind möglicherweise nicht Teil der Zulassungslistenempfänger. Daher werden diese Sitzungen von der Überwachung übersprungen.

Weitere Informationen zu Problemen im Zusammenhang mit der ICA-Analyse finden Sie unter Problem bei der Datensatzgenerierung für HDX/ICA-Datenverkehr in der Citrix ADC Checkliste

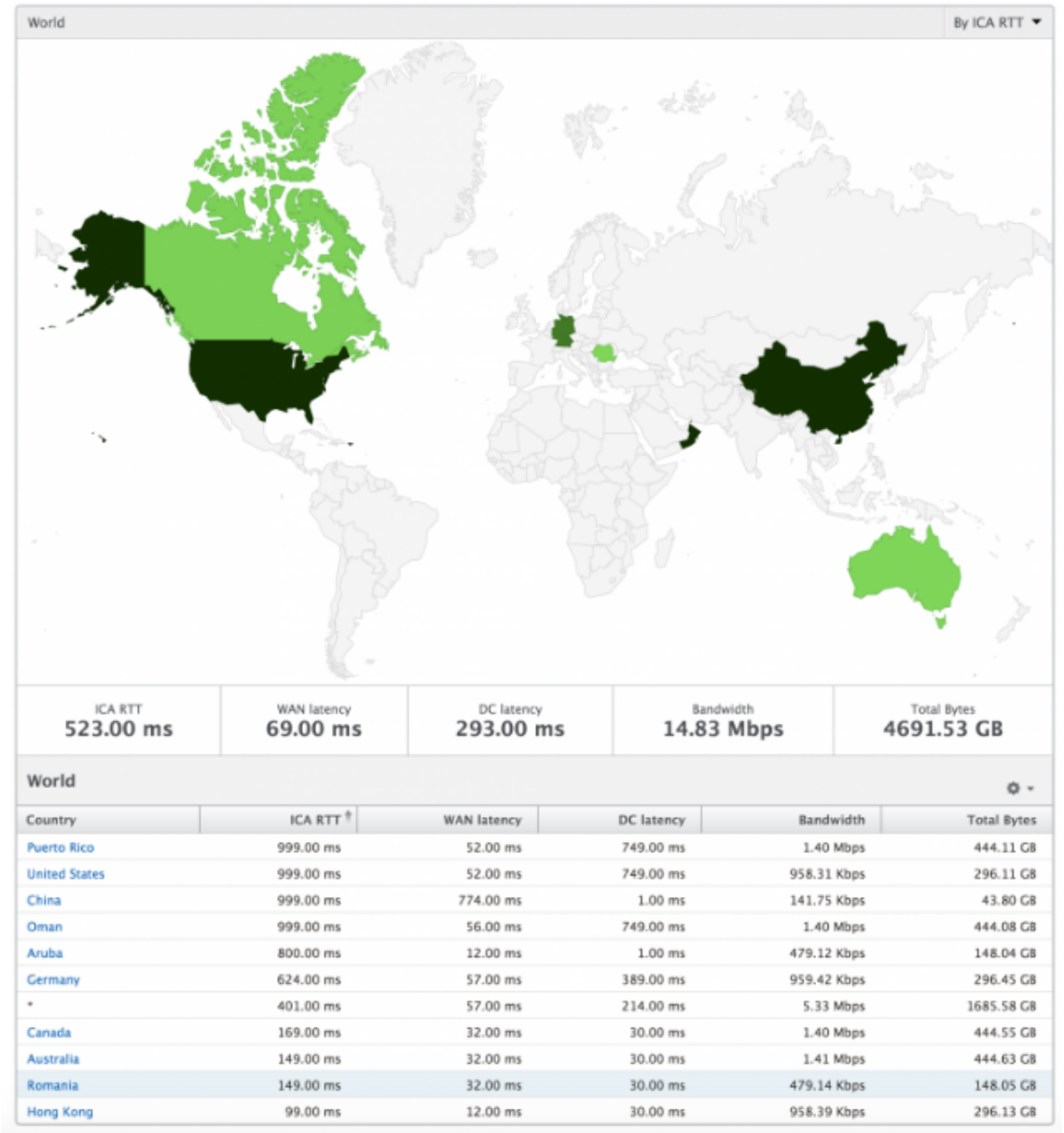


Weltansicht

Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die historischen und aktiven Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltanschauung des Systems, Drilldown zu einem bestimmten Land und weiter in die Städte als auch durch Klicken auf die Region. Die Administratoren können weitere Informationen nach Stadt und Bundesstaat anzeigen. Ab Citrix ADM Version 12.0 und höher können Sie einen Drilldown für Benutzer durchführen, die von einem Geostandort aus verbunden sind.

Die folgenden Details können auf der Weltkarte in HDX Insight angezeigt werden, und die Dichte jeder Metrik wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Bytes insgesamt



Ansicht pro Instanz

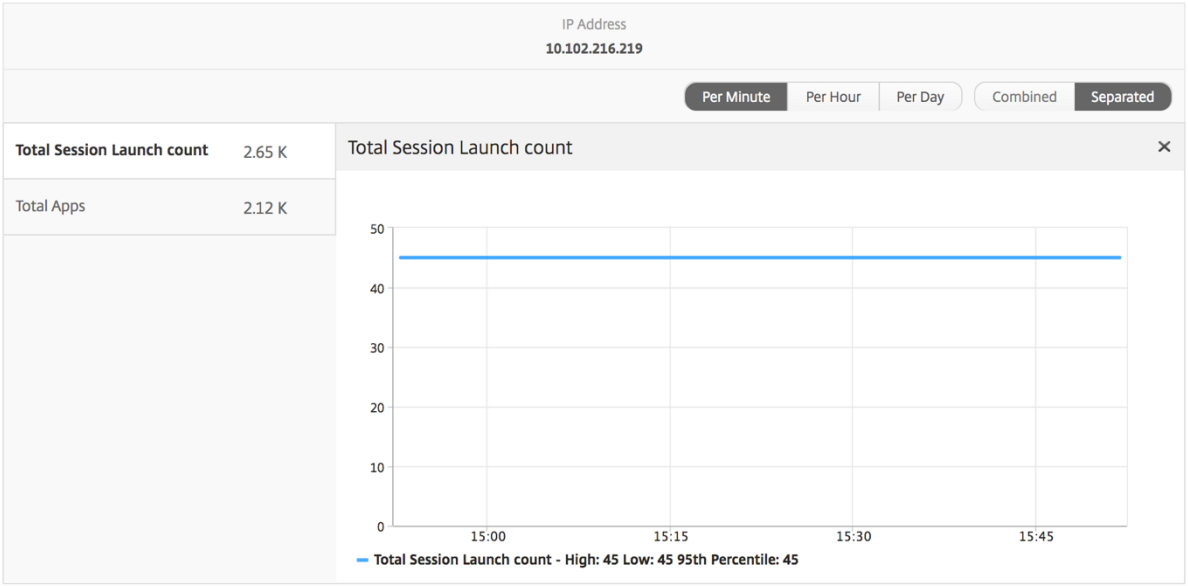
Die Pro-Instanz-Ansicht bietet detaillierte Berichte über die Endbenutzererfahrung für eine bestimmte ausgewählte ADC-Instanz.

So navigieren Sie zur Instanzansicht:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Instanzen**.
2. Wählen Sie im **Bericht Instanzzusammenfassung eine bestimmte Instanz** aus.

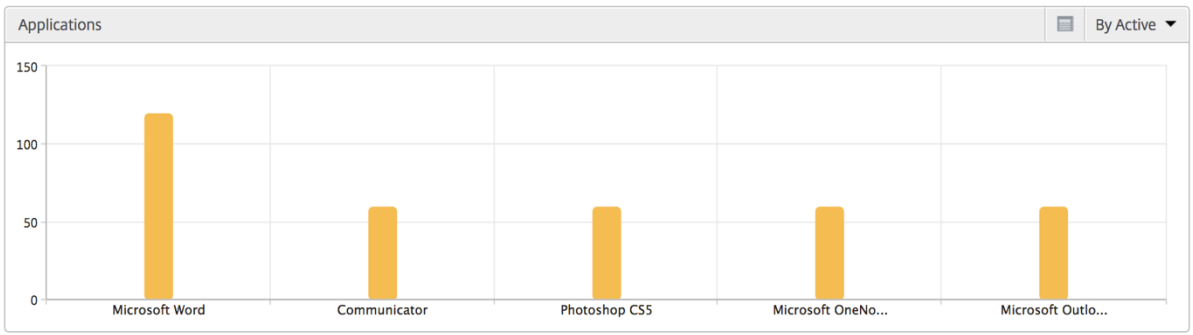
Liniendiagramm

Metriken	Beschreibung
IP-Adresse	Dies stellt die NetScaler IP-Adresse der ausgewählten Instanz dar.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual App-Sitzungen während des angegebenen Zeitintervalls.
Apps insgesamt	Gesamtzahl der eindeutigen Anwendungen, die während eines bestimmten Zeitintervalls gestartet wurden.



Anwendungsleistendiagramm

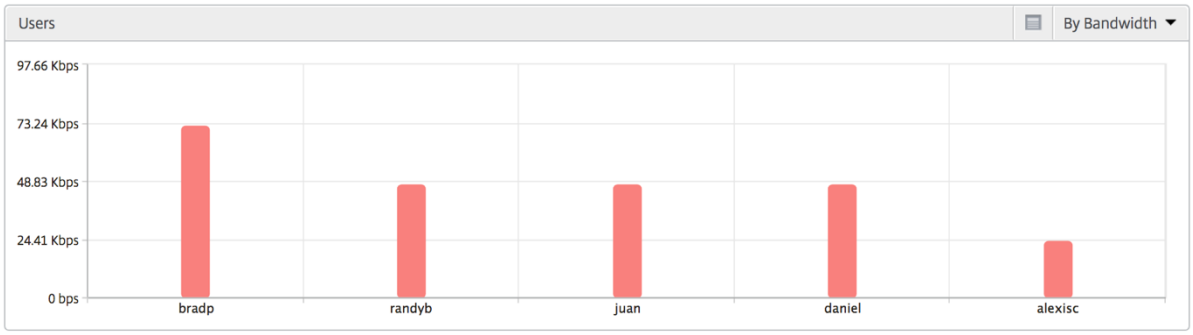
Zeigt die 5 wichtigsten Anwendungen basierend auf aktiven Apps, der Gesamtzahl der Sitzungsstarts, der Gesamtzahl der App-Startzeiten oder der Startdauer an.



Benutzer Balkendiagramm

Das Balkendiagramm Benutzer zeigt die 5 besten Benutzer basierend auf den folgenden Kriterien an.

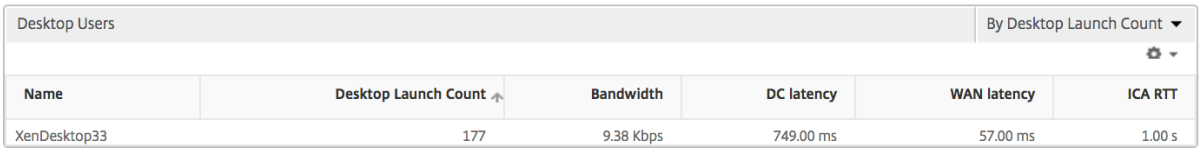
- Bandbreite
- WAN-Latenz
- DC-Latenz
- ICA RTT



Desktopbenutzer-Bericht

Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Desktop-Launch-Anzahl und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Der Name des Citrix Virtual Desktops.
Anzahl Desktopstarts	Anzahl, wie oft der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Bytes pro Sekunde für die Kommunikation zwischen Ende und Ende während des ausgewählten Zeitintervalls.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zu Back-End-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von Citrix ADC bis zum Endbenutzer.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.

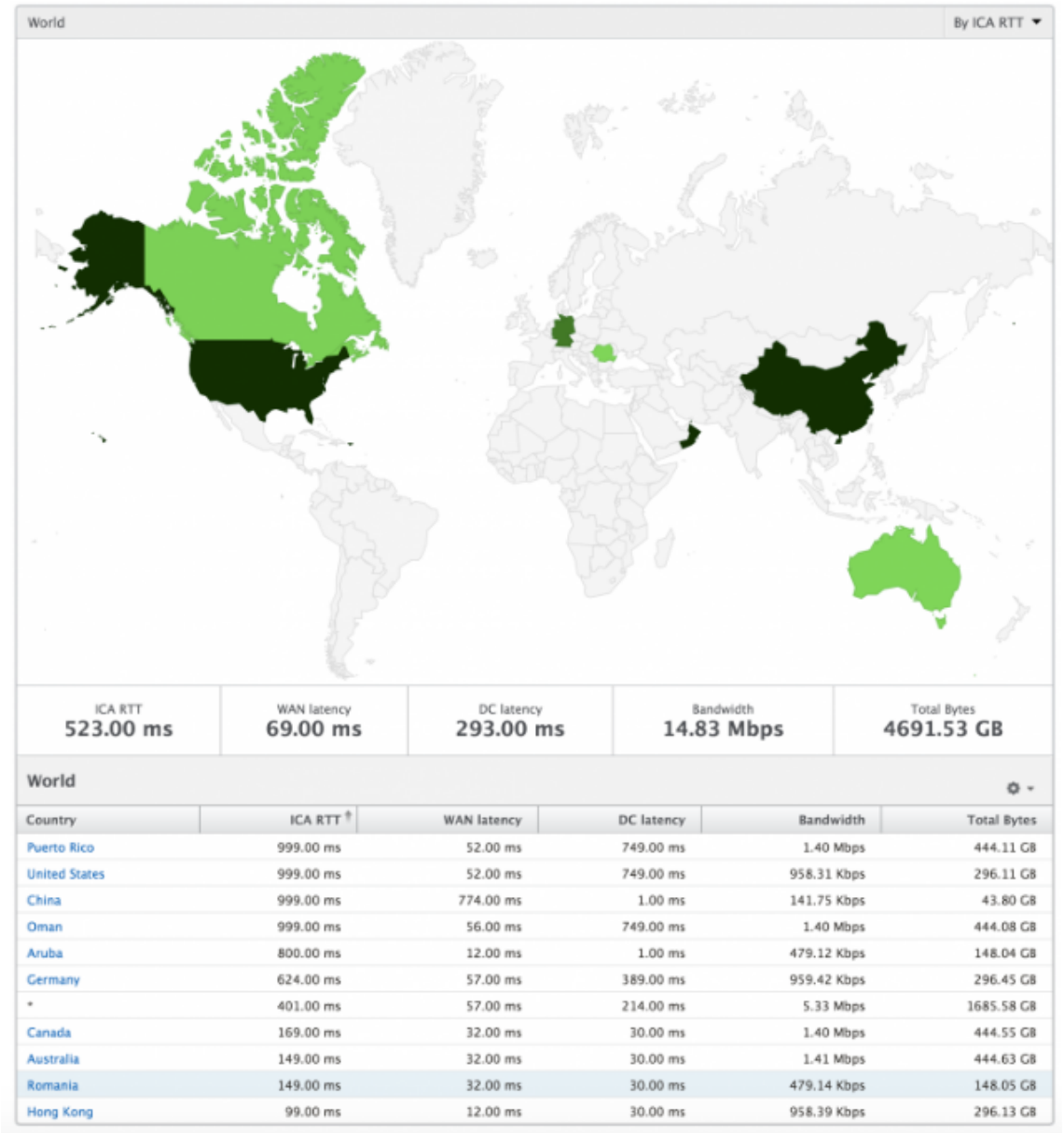


Weltansicht

Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die historischen und aktiven Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltanschauung des Systems, Drilldown zu einem bestimmten Land und weiter in die Städte als auch durch Klicken auf die Region. Die Administratoren können weitere Informationen nach Stadt und Bundesstaat anzeigen. Ab Citrix ADM Version 12.0 und höher können Sie einen Drilldown für Benutzer durchführen, die von einem Geostandort aus verbunden sind.

Die folgenden Details können auf der Weltkarte in HDX Insight angezeigt werden, und die Dichte jeder Metrik wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Bytes insgesamt



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

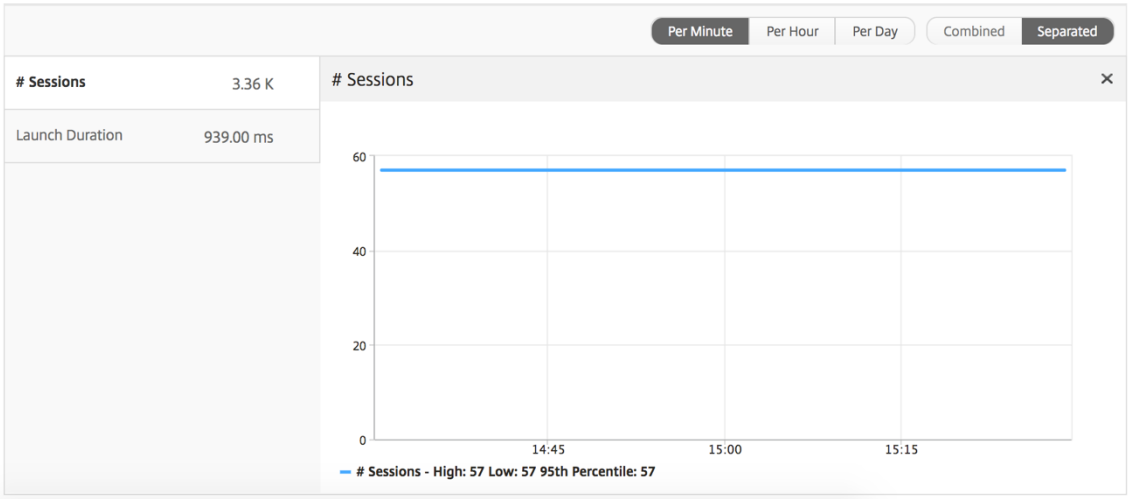
Berichte und Metriken zur Lizenzansicht

April 28, 2021

Die Lizenzansicht enthält Details zu den Citrix ADC Gateway-Lizenzinformationen. Navigieren Sie zu **Analytics** > **HDX Insight** > **Lizenzen**.

Liniendiagramm

Metriken	Beschreibung
Verwendete Lizenzen	Die Citrix ADC Gateway-CCU-Lizenzen, die während der ausgewählten Zeitachse verwendet werden. Jede Anzahl stellt die Anzahl der Benutzersitzungen dar. Dies ist unabhängig von den Anwendungs- und Desktopsitzungen, die von diesem Benutzer gestartet werden.
Gesamtzahl der Lizenzen	Gesamtzahl der Citrix ADC Gateway CCU-Lizenzen, die der Kunde nutzen kann.



Schwellenwertbericht

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* im ausgewählten Zeitraum als Lizenz ausgewählt wurde.

Beheben von Problemen mit HDX Insight

April 28, 2021

Wenn die HDX Insight Lösung nicht wie erwartet funktioniert, liegt das Problem möglicherweise mit einem der folgenden Probleme vor. Informationen zur Fehlerbehebung finden Sie in den Checklisten in den entsprechenden Abschnitten.

- HDX Insight Konfiguration.

- Konnektivität zwischen Citrix ADC und Citrix ADM.
- Datensatzgenerierung für HDX/ICA-Datenverkehr in Citrix ADC.
- Grundgesamtheit von Datensätzen in Citrix ADM.

Checkliste zur Konfiguration von HDX Insight

- Stellen Sie sicher, dass die AppFlow-Funktion in Citrix ADC aktiviert ist. Einzelheiten finden Sie unter AppFlow aktivieren.
- Überprüfen Sie die HDX Insight Konfiguration in der Citrix ADC Konfiguration.

  Führen Sie den Befehl `show running | grep -i <appflow_policy>` aus, um die HDX Insight-Konfiguration zu überprüfen. Stellen Sie sicher, dass der Bindungstyp ICA Request ist. Zum Beispiel;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  Für den transparenten Modus muss der Bindungstyp ICA_REQ_DEFAULT sein. Zum Beispiel;

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- Stellen Sie bei Single-Hop/Access Gateway- oder Double-Hop-Bereitstellung sicher, dass die HDX Insight AppFlow Richtlinie an den virtuellen VPN-Server gebunden ist, auf dem HDX/ICA-Datenverkehr fließt.
- Stellen Sie für den transparenten Modus oder den LAN-Benutzermodus sicher, dass die ICA-Ports 1494 und 2598 eingestellt sind.
- Prüfen Sie, dass der Parameter `appflowlog` in Citrix Gateway oder dem virtuellem VPN-Server für die Access Gateway- oder Double-Hop-Bereitstellung aktiviert ist. Einzelheiten finden Sie unter Aktivieren von AppFlow für virtuelle Server.
- Aktivieren Sie “Connection Chaining” in Double-Hop-Citrix ADC. Einzelheiten finden Sie unter Konfigurieren von Citrix Gateway Geräten zum Exportieren von Daten.
- Wenn die HDX Insight Details nach HA-Failover analysiert werden, überprüfen Sie den ICA-Parameter “enableSRonHAFailover” aktiviert ist. Einzelheiten finden Sie unter Sitzungszuverlässigkeit auf Citrix ADC Hochverfügbarkeitspaar.

Konnektivität zwischen Citrix ADC und Citrix ADM Checkliste

- Überprüfen Sie den AppFlow Collector-Status in Citrix ADC. Einzelheiten finden Sie unter Überprüfen des Status der Verbindung zwischen Citrix ADC und AppFlow Collector.
- Überprüfen Sie die HDX Insight AppFlow Richtlinientreffer.

Führen Sie den Befehl `show appflow policy <policy_name>` aus, um die Treffer der AppFlow-Richtlinie zu überprüfen.

Sie können auch in der GUI zu **System > AppFlow > Richtlinien** navigieren, um die AppFlow-Richtlinientreffer zu überprüfen.

- Überprüfen Sie jede Firewall, die AppFlow Ports 4739 oder 5557 blockiert.

Datensatzgenerierung für HDX/ICA-Datenverkehr in der Citrix ADC Checkliste

Führen Sie den Befehl `tail -f /var/log/ns.log | grep -i "default ICA Message"` zur Log-Validierung aus. Basierend auf den generierten Protokollen können Sie diese Informationen für die Fehlerbehebung verwenden.

- Protokoll: **Parsing ICA-Verbindung übersprungen - HDX Insight wird für diesen Host nicht unterstützt**

  Ursache: Nicht unterstützte Citrix Virtual Apps and Desktops s-Versionen

  Workaround: Aktualisieren Sie die Citrix Virtual Apps and Desktops s-Server auf eine unterstützte Version.

- Protokoll: **Client type received 0x53, NOT SUPPORTED**

  Ursache: Nicht unterstützte Version der Citrix Workspace-App

  Lösung: Aktualisieren Sie die Citrix Workspace App auf eine unterstützte Version. Einzelheiten finden Sie unter Citrix Workspace-App.

- Log: **Fehler von Expand Packet - Überspringen der gesamten hdx-Verarbeitung für diesen Flow**

  Ursache: Problem beim Dekomprimieren des ICA-Datenverkehrs

  Lösung: Für diese ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet ist.

- Log: **Ungültiger Übergang: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT"**

  Ursache: Problem beim Analysieren des ICA-Handshakes

  Lösung: Für diese bestimmte ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wurde.

- Protokoll: **Fehlende EUEM ICA RTT**

  Ursache: Die Kanaldaten für die Überwachung der Endbenutzer-Benutzererfahrung konnten nicht analysiert werden.

Lösung: Stellen Sie sicher, dass der Endbenutzerüberwachungsdienst auf den Citrix Virtual Apps and Desktops s-Servern gestartet wurde. Stellen Sie sicher, dass Sie die unterstützten Versionen von Citrix Workspace App verwenden.

- Log: **Ungültiger Kanal-Header**

  Ursache: Kanal-Header konnte nicht identifiziert werden

  Lösung: Für diese bestimmte ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wurde.

- Log: **Code überspringen**

  Wenn Sie einen der folgenden Werte für Skip-Code sehen, werden die Insight-Details übersprungen analysiert.

  > Überspringen des Codes 0 gibt an, dass der Datensatz erfolgreich aus Citrix ADC exportiert wurde.

Code überspringen	Fehlermeldung	Fehlerursache
100	NS_ICA_ERR_NULL_FRAG	Fehler bei der Verarbeitung von ICA-Fragmenten, wahrscheinlich aufgrund von Speicherbedingungen
101	NS_ICA_ERR_INVALID_HS_CMD	Ungültiger Handshake-Befehl empfangen
102	NS_ICA_ERR_REDUC_PARAM_C	Ungültiger Parameter für die Initialisierung des V3 Expanders angegeben
103	NS_ICA_ERR_REDUC_INIT	Der V3 Expander konnte nicht korrekt initialisiert werden
104	NS_ICA_ERR_REDUC_PARAM_B	Unzureichende Bytes, um einem Kanal einen Coder zuzuweisen
105	NS_ICA_ERR_INVALID_CHANNEL	Ungültige ICA-Kanalnummer
106	NS_ICA_ERR_INVALID_DECODE	Ungültiger Decoder für einen Kanal angegeben
107	NS_ICA_ERR_INVALID_TW_PARAM	Ungültige Parameteranzahl auf Thinwire-Kanal angegeben

Code überspringen	Fehlermeldung	Fehlerursache
108	NS_ICA_ERR_INVALID_TW_DEC	Ungültiger Decoder für Thinwire-Kanal
109	NS_ICA_ERR_REDUC_NO_DECODER	Kein Decoder für Kanal definiert
110	NS_ICA_ERR_REDUC_V3_EXPAN	Fehler beim Erweitern der Kanaldaten
111	NS_ICA_ERR_REDUC_BYTES_V3_EXPA	Expander-Fehler: Bytes, die mehr als Bytes verbraucht wurden, verfügbar
112	NS_ICA_ERR_REDUC_BYTES_O	Fehler: Unkomprimierte Datenüberlauf
113	NS_ICA_ERR_REDUC_INVALID_CMD	Undefinierter Expander (Befehl)
114	NS_ICA_ERR_CGP_FILL_HOLE	Fehler beim Umgang mit geteilten CGP-Frames
115	NS_ICA_ERR_MEM_NSB_ALLOC	NSB-Zuweisungsfehler — aufgrund von geringen Speicherbedingungen
116	NS_ICA_ERR_MEM_REDUC_CTX	Speicherzuordnungsfehler für Expander-Kontext
117	NS_ICA_ERR_ICA_OLD_SERVER	Alter Server, Capability Blöcke werden nicht unterstützt
118	NS_ICA_ERR_PIR_MANY_FRAG	Paketinit-Anforderung ist fragmentiert, kann nicht verarbeitet werden
119	NS_ICA_ERR_INIT_ICA_CAPS	Initialisierungsfehler der ICA-Fähigkeit
120	NS_ICA_ERR_NO_MSI_SUPPOR	Host unterstützt keine MSI-Funktion. Gibt für XenApp Version kleiner als 6.5 oder XenDesktop Versionen kleiner als 5.0 an
121	NS_ICA_ERR_CGP_INVALID_CMD	Ungültiger CGP-Befehl gefunden

Code überspringen	Fehlermeldung	Fehlerursache
122	NS_ICA_ERR_INSUFFICENT_CH	Unzureichende Bytes über Kanal
123	NS_ICA_ERR_CHANNEL_DATA	Falsche Daten auf dem EUEM-, CONTROL- oder SEAMLESS-Kanal
124	NS_ICA_ERR_INVALID_PURE_C	Ungültiger Befehl beim Verarbeiten reinen ICA-Kanaldaten empfangen
125	NS_ICA_ERR_INVALID_PURE_LEN	Ungültige Länge beim Verarbeiten von reinen ICA-Kanaldaten
126	NS_ICA_ERR_INVALID_PURE_LI	Ungültige Länge beim Verarbeiten von PURE ICA-Kanaldaten
127	NS_ICA_ERR_INVALID_CLNT_DATA	Ungültige Datenlänge vom Client empfangen
128	NS_ICA_ERR_MSI_GUID_SZ	Fehler in der MSI-GUID-Größe
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	Ungültiger Kanal-Header erkannt
130	NS_ICA_ERR_CGP_PARSE_REC	Abruf der wiederverbundenen Sitzung fehlgeschlagen
131	NS_ICA_ERR_DISABLE_SR_NON_RELIABLE_RECONNECT	Fehler beim Deaktivieren von SR
132	NS_ICA_ERR_REDUC_NOT_V3	Nicht unterstützte ICA-Reduzierversion
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Komprimierung deaktiviert, nicht vom Host berücksichtigt
134	NS_ICA_ERR_IDENT_PROTO	ICA- oder CGP-Protokoll konnte nicht identifiziert werden, wenn falsche Empfänger angezeigt werden
135	NS_ICA_ERR_INVALID_SIGNATURE	Falsche ICA-Signatur oder magische Zeichenfolge

Code überspringen	Fehlermeldung	Fehlerursache
136	NS_ICA_ERR_PARSE_RAW	Fehler beim Analysieren des ICA-Handshake-Pakets
137	NS_ICA_ERR_INCOMPLETE_PKT	Unvollständiges Paket im Handshake empfangen
138	NS_ICA_ERR_ICAFRAME_TOO_L	ICA-Frame ist zu groß und übersteigt 1.460 Byte
139	NS_ICA_ERR_FORWARD	Fehler beim Weiterleiten der ICA-Daten
140	NS_ICA_ERR_MAX_HOLES	CGP-Befehl kann nicht verarbeitet werden, da er über das unterstützte Limit gespalten wird
141	NS_ICA_ERR_ASSEMBLE_FRAME	ICA-Frame konnte nicht korrekt wieder zusammengesetzt werden
142	NS_ICA_ERR_UNSUPPORTED_F	ICA-Parsing für diesen Receiver (Client) übersprungen, da es nicht in der Zulassungsliste enthalten ist
143	NS_ICA_ERR_LOOKUP_RECONNECT_D	Der Parsing-Status für das Wiederverbindungs-Cookie des Clients konnte nicht erkannt werden
144	NS_ICA_ERR_SYNCUP_RECONN	Ungültige Wiederverbindungs-Cookie-Länge nach der Wiederverbindung des Clients erkannt
145	NS_ICA_ERR_INVALID_RECONNECT_ID	Client reconnects Cookie hat die erforderliche Einschränkung verpasst
146	NS_ICA_ERR_INVALID_CLIENT_	Ungültige Empfängerversion-szeichenfolge, die vom Client empfangen wurde

Code überspringen	Fehlermeldung	Fehlerursache
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	Ungültige Produkt-ID, die vom Client empfangen wurde
148	NS_ICA_ERR_V3_HDR_CORRUP	Ungültige Kanallänge nach Erweiterung
149	NS_ICA_ERR_SPECIAL_THINWIRE	Dekomprimierungsfehler
150	NS_ICA_ERR_SEAMLESS_INSUF	Unzureichende Bytes für Seamless-Befehl gefunden
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Unzureichende Bytes für den EUEM-Befehl
152	NS_ICA_ERR_SEAMLESS_INVAL	Ungültiges Ereignis für Seamless-Channel-Parsing
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Ungültiges Ereignis für die Analyse des Strg-Kanals
154	NS_ICA_ERR_EUEM_INVALID_E	Ungültiges Ereignis für die Analyse des EUEM-Kanals
155	NS_ICA_ERR_USB_INVALID_EVENT	Ungültiges Ereignis für die Analyse von USB-Kanälen
156	NS_ICA_ERR_PURE_INVALID_E	Ungültiges Ereignis für reine Kanalanalyse
157	NS_ICA_ERR_VCP_INVALID_EVENT	Ungültiges Ereignis für die Analyse virtueller Kanäle
158	NS_ICA_ERR_ICAP_INVALID_EV	Ungültiges Ereignis für die Analyse von ICA-Daten
159	NS_ICA_ERR_CGPP_INVALID_EVENT	Ungültiges Ereignis für die Analyse von CGP-Daten
160	NS_ICA_ERR_BASICCRYPT_INV	Ungültiger Status für einen crypt-Befehl in der grundlegenden Verschlüsselung
161	NS_ICA_ERR_BASICCRYPT_INVALID_CRYPTCMD	Ungültiger Crypt-Befehl in der grundlegenden Verschlüsselung

Code überspringen	Fehlermeldung	Fehlerursache
162	NS_ICA_ERR_ADVCRYPT_INVAL	Ungültiger Status für einen crypt-Befehl in RC5-Verschlüsselung
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	Ungültiger Krypt-Befehl in RC5-Verschlüsselung
164	NS_ICA_ERR_ADVCRYPT_ENC	Fehler bei der RC5-Verschlüsselung/Entschlüsselung
165	NS_ICA_ERR_ADVCRYPT_DEC	Fehler bei der RC5-Verschlüsselung/Entschlüsselung
166	NS_ICA_ERR_SERVER_NOT_REI	VDA unterstützt Reducer Version 3 nicht
167	NS_ICA_ERR_CLIENT_NOT_REDUCEDV3	Receiver unterstützt Reducer Version 3 nicht
168	NS_ICA_ERR_ICAP_INSUFFBYTI	Unerwartete Anzahl von Bytes im ICA-Handshake
169	NS_ICA_ERR_HIGHER_RECONSEQ	Höhere CGP-Wiederaufnahme-Sequenznummer aus Peer-Post-Wiederverbindungen
170	NS_ICA_ERR_DESCSRINFO_ABS	ICA-Parsing-Status kann nach der Wiederverbindung nicht wiederhergestellt werden
171	NS_ICA_ERR_NSAP_PARSING	Fehler beim Analysieren von Insight-Kanaldaten
172	NS_ICA_ERR_NSAP_APP	Fehler beim Analysieren von App-Details aus Insight-Kanaldaten
173	NS_ICA_ERR_NSAP_ACR	Fehler beim Analysieren von ACR-Details aus Insight-Kanaldaten
174	NS_ICA_ERR_NSAP_SESSION_E	Fehler beim Analysieren von Sitzungsenddetails aus Insight-Kanaldaten

Code überspringen	Fehlermeldung	Fehlerursache
175	NS_ICA_ERR_NON_NSAP_SN	ICA-Analyse auf dem Dienstknoten übersprungen, da keine Insight-Kanalunterstützung vorhanden ist
176	NS_ICA_ERR_NON_NSAP_CLIEI	NSAP wird vom Client nicht unterstützt
177	NS_ICA_ERR_NON_NSAP_SERVER	NSAP wird vom VDA nicht unterstützt
178	NS_ICA_ERR_NSAP_NEG_FAIL	Fehler bei der NSAP-Datenaushandlung
179	NS_ICA_ERR_SN_RECONNECT_TICKET_FETCH	Fehler beim Abrufen des Dienstes verbindet das Ticket im Serviceknoten
180	NS_ICA_ERR_SN_HIGHER_REC(	Fehler beim Empfangen einer höheren Wiederverbindungssequen-znummer im Serviceknoten
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP	Fehler beim Deaktivieren von HDX Insight für Nicht-NSAP-Verbindungen

Beispielprotokolle:

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT ns-223
 0-PPE-2 : default ICA Message 1234 0 : ”Session setup data send: Session
GUID [57af35043e624abab409f5e6af7fd22c], Client IP/Port [10.105.232.40/52314],
 Server IP/Port [10.106.40.215/2598], MSI Client Cookie [Non-MSI], Session
 setup time [01/09/2020:22:56:49 GMT], Client Type [0x0052], Receiver
Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [WIN2K12
-215], Ctx Flags [0x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]
”
```

```
Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41 GMT ns-223
 0-PPE-0 : default ICA Message 156 0 : ”Skipping ICA flow: Session GUID
[4e3a91175ebcbe686baf175eec7e0200], Client IP/Port [10.105.232.40/60059],
```



```
Server IP/Port [10.106.40.219/2598], MSI Client Cookie [Non-MSI], Session
 setup time [01/09/2020:22:55:39 GMT], Client Type [0x0052], Receiver
Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [10.106.40.219],
 Ctx Flags [0x8820220008], Track Flags [0x1600010c040], Skip Code [171]”
```

Fehlerindikatoren

Verschiedene Zähler werden ICA-Parsing erfasst. In der folgenden Tabelle sind die verschiedenen Leistungsindikatoren für die ICA-Analyse aufgeführt.
Führen Sie den Befehl `nsconmsg -g hdx -d statswt0`zum Anzeigen der Leistungsindikatordetails aus.

Name des HDX-Zählers	Zweck	Kategorie (Stats/Fehler/Diagnose)
hdx_tot_ica_conn	Gibt die Gesamtanzahl der von NS erkannten Pure ICA-Verbindungen an.Inkrementiert, wenn eine ICA-Verbindung auf der ICA-Signatur auf einer Client-PCB erkannt wird.	Statistiken
hdx_tot_cgp_conn	Gibt die Gesamtanzahl der von NS erkannten CGP-Verbindungen an (Sitzungszuverlässigkeit ON). Inkrementiert, wenn eine CGP-Verbindung, die auf der CGP-Signatur auf einer Client-PCB basiert, erkannt wird.	Statistiken
hdx_dbg_tot_udt_conn	Gibt die Gesamtanzahl der von NS erkannten UDP-ICA-Verbindungen an	Statistiken
hdx_dbg_tot_nsap_conn	Gibt die Gesamtzahl der NSAP-unterstützten Verbindungen an, die von NS erkannt wurden.	Statistiken

Name des HDX-Zählers	Zweck	Kategorie (Stats/Fehler/Diagnose)
hdx_tot_skip_conn	Gibt an, wie viele ICA-Verbindungen aufgrund einer ungültigen ICA- oder CGP-Signatur vom Parser übersprungen wurden.	Statistiken
hdx_dbg_active_conn	Aktive EDT/CGP/ICA-Verbindungen zu diesem Zeitpunkt.	Statistiken
hdx_dbg_active_nsap_conn	Aktive EDT/CGP/ICA-NSAP-Verbindungen zu diesem Zeitpunkt.	Statistiken
hdx_dbg_skip_appflow_disabled	Gesamtzahl der Instanzen, in denen AppFlow aufgrund der Deaktivierung von AppFlow von einer Sitzung getrennt wurde	Stats/Diagnostik
hdx_dbg_transparent_user	Gesamtzahl des transparenten Benutzerzugriffs	Stats/Diagnostik
hdx_dbg_ag_user	Gesamtanzahl des Access Gateway-Benutzerzugriffs	Stats/Diagnostik
hdx_dbg_lan_user	Gesamtanzahl des LAN-Benutzermodus-Zugriffs	Stats/Diagnostik
hdx_basic_enc	Gibt die Anzahl der ICA-Verbindungen mit Basisverschlüsselung an	Stats/Diagnostik
hdx_advanced_enc	Gibt die Anzahl der ICA-Verbindungen mit erweiterter RC5-basierter Verschlüsselung an	Stats/Diagnostik
dx_dbg_wanscaler_on_clientside	Gesamtzahl der CGP/ICA-Verbindungen mit Citrix SD-WAN auf Clientseite	Stats/Diagnostik

Name des HDX-Zählers	Zweck	Kategorie (Stats/Fehler/Diagnose)
hdx_dbg_wanscaler_on_server	Gesamtzahl der CGP/ICA-Verbindungen mit Citrix SD-WAN -Serverseite	Stats/Diagnostik
hdx_dbg_reconnected_session	Gesamtzahl der Wiederverbindungsanforderungen vom Client ohne Citrix ADC Fehler	Stats/Diagnostik
hdx_dbg_host_rejected_ns_rec	Gesamtzahl der von Hosts abgelehnten Wiederverbindungsanfragen nach Client	Stats/Diagnostik
hdx_euem_available	Gibt die Anzahl der Verbindungen an, für die der Kanal zur Überwachung der Endbenutzererfahrung verfügbar ist.Der Kanal zur Überwachung der Benutzererfahrung ist erforderlich, um Statistiken wie ICA-RTT zu sammeln.	Stats/Diagnostik
hdx_err_disabled_sr	Die Sitzungszuverlässigkeit ist mit dem `nsapimgr`Drehknopf deaktiviertDie Sitzung funktioniert für diese Sitzung nicht.	Fehler
hdx_err_skip_no_msi	XA/XD-Server fehlt die MSI-Fähigkeit. Dies zeigt eine ältere Serverversion an, HDX Insight überspringt diese Verbindung.	Fehler
hdx_err_skip_old_server	Alte nicht unterstützte Serverversion	Fehler
hdx_err_clnt_not_whitelist	Clientempfänger nicht in der Zulassungsliste, HDX Insight überspringt diese Verbindung	Fehler

Name des HDX-Zählers	Zweck	Kategorie (Stats/Fehler/Diagnose)
hdx_sm_ica_cam_channel_disa	Gesamtzahl der über SmartAccess Richtlinie deaktivierten NS_ICA_CAM_CHANNEL	Diagnose
hdx_sm_ica_usb_channel_disabled	Gesamtzahl der über SmartAccess Richtlinie deaktivierten NS_ICA_USB_CHANNEL	Diagnose
hdx_sm_ica_clip_channel_disa	Gesamtzahl der über SmartAccess Richtlinie deaktivierten NS_ICA_CLIP_CHANNEL	Diagnose
hdx_sm_ica_ccm_channel_disabled	Gesamtzahl der über SmartAccess Richtlinie deaktivierten NS_ICA_CCM_CHANNEL	Diagnose
hdx_sm_ica_cdm_channel_disa	Gesamtzahl der über SmartAccess Richtlinie deaktivierten NS_ICA_CDM_CHANNEL	Diagnose
hdx_sm_ica_com1_channel_disabled	Gesamtzahl der über SmartAccess Richtlinie deaktivierten NS_ICA_COM1_CHANNEL	Diagnose
hdx_sm_ica_com2_channel_di	Gesamtzahl der über SmartAccess Richtlinie deaktivierten NS_ICA_COM2_CHANNEL	Diagnose
hdx_sm_ica_cpm_channel_disabled	Gesamtanzahl der über SmartAccess Richtlinie deaktivierten NS_ICA_CPM_CHANNEL	Diagnose

Name des HDX-Zählers	Zweck	Kategorie (Stats/Fehler/Diagnose)
hdx_sm_ica_lpt1_channel_disa	Gesamtanzahl der über SmartAccess Richtlinie deaktivierten NS_ICA_LPT1_CHANNEL	Diagnose
hdx_sm_ica_lpt2_channel_disabled	Gesamtzahl der über SmartAccess Richtlinie deaktivierten NS_ICA_LPT2_CHANNEL	Diagnose
dx_dbg_sm_ica_msi_disabled	Gesamtzahl der Fälle, in denen MSI über SmartAccess Richtlinie deaktiviert ist	Diagnose
hdx_sm_ica_file_channel_disabled	Gesamtanzahl von NS_ICA_FILE_CHANNEL ist über die SmartAccess Richtlinie deaktiviert	Diagnose
hdx_dbg_usb_accept_device	Gesamtzahl der akzeptierten USB-Geräte	Diagnose
hdx_dbg_usb_reject_device	Gesamtzahl abgelehnter USB-Geräte	Diagnose
hdx_dbg_usb_reset_endpoint	Gesamtzahl der zurückgesetzten USB-Endpunkte	Diagnose
hdx_dbg_usb_reset_device	Gesamtzahl der zurückgesetzten USB-Geräte	Diagnose
hdx_dbg_usb_stop_device	Gesamtzahl der gestoppten USB-Geräte	Diagnose
hdx_dbg_usb_stop_device_response	Gesamtzahl der Antworten von gestoppten USB-Geräten	Diagnose
hdx_dbg_usb_device_gone	Gesamtzahl der USB-Geräte verschwunden	Diagnose
hdx_dbg_usb_device_stopped	Gesamtzahl der gestoppten USB-Geräte	Diagnose

nstrace Validierung

Überprüfen Sie das CFLOW-Protokoll, um alle AppFlow Datensätze aus Citrix ADC zu sehen.

Grundgesamtheit der Datensätze in der Citrix ADM Checkliste

- Führen Sie den Befehl aus `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"`und überprüfen Sie die Protokolle, um zu bestätigen, dass Citrix ADM AppFlow-Einträge erhält.
- Bestätigen Sie, dass Citrix ADC-Instanz zu Citrix ADM hinzugefügt wird.
- Überprüfen Sie, ob der virtuelle Citrix Gateway/VPN-Server in Citrix ADM lizenziert ist.
- Stellen Sie sicher, dass die Multihop-Parametereinstellung für Double-Hop aktiviert ist.
- Stellen Sie sicher, dass Citrix Gateway für den zweiten Hop-Einsatz in der Double-Hop-Bereitstellung freigegeben ist.

Bevor Sie sich an den technischen Support von Citrix wenden

Um eine schnelle Lösung zu erhalten, stellen Sie sicher, dass Sie die folgenden Informationen haben, bevor Sie sich an den technischen Support von Citrix wenden:

- Details zur Bereitstellung und Netzwerktopologie.
- Citrix ADC und Citrix ADM Versionen.
- Citrix Virtual Apps and Desktops -Serverversionen.
- Client-Receiver-Versionen.
- Anzahl der aktiven ICA-Sitzungen, bei denen das Problem aufgetreten ist.
- Das technische Supportpaket wird durch Ausführen des `show techsupport` Befehls an der Citrix ADC-Eingabeaufforderung erfasst.
- Technischer Support Paket für Citrix ADM erfasst.
- Paketverfolgungen, die auf allen Citrix ADC erfasst wurden.
  Um eine Paketablaufverfolgung zu starten, geben Sie Folgendes ein: Um eine Paketablaufverfolgung `start nstrace -size 0'`
  zu stoppen: `stop nstrace`
- Sammeln Sie Einträge in der ARP-Tabelle des Systems, indem Sie den `show arp` Befehl ausführen.

Bekannte Probleme

Weitere Informationen zu bekannten Problemen in HDX Insight finden Sie in den Citrix ADC Versionshinweisen.

Metrikinformationen für Schwellenwerte

April 28, 2021

Web-Site

Metriken	Entität	Beschreibung
Anwendungen	Treffer	Gesamtzahl der Treffer, die von einem virtuellen Server (Anwendung) empfangen werden
	Bandbreite (MB)	Gesamtbandbreite, die vom virtuellen Server (Anwendung) verbraucht wird
	Reaktionszeit (ms)	Die Zeit, die für die Reaktion des virtuellen Servers erforderlich ist
Kunden	Anforderungen	Die Gesamtanforderung, die von einem Client empfangen wird
	Renderzeit (ms)	Die Zeit, die zum Rendern der Serverantwort durch den Client erforderlich ist
	Clientnetzwerklatenz	Die Zeit, die für Anforderungen aus dem Clientnetzwerk gebraucht wird
Geräte	Treffer	Gesamtzahl der von einem Gerät empfangenen Treffer. Zum Beispiel: Laptop, Handy

Metriken	Entität	Beschreibung
	Bandbreite (MB)	Gesamtbandbreite, die von einem Gerät verbraucht wird
Domänen	Treffer	Gesamtzahl der von einer Netzwerkdomäne empfangenen Treffer
	Bandbreite (MB)	Gesamtbandbreite, die von einer Netzwerkdomäne belegt wird
	Reaktionszeit (ms)	Die Zeit, die für die Beantwortung von Anfragen einer Netzwerkdomäne benötigt wird
Betriebssystem	Treffer	Gesamtzahl der von einem Betriebssystem empfangenen Treffer
	Bandbreite (MB)	Gesamtbandbreite, die von einem Betriebssystem belegt wird
	Renderzeit (ms)	Die Zeit, die zum Rendern der Serverantwort durch ein Betriebssystem erforderlich ist
Anforderungsmethoden	Treffer	Gesamtzahl der von einer Anforderungsmethode empfangenen Anforderungen. Zum Beispiel: GET, POST
	Bandbreite (MB)	Gesamtbandbreite, die von einer Anforderungsmethode belegt wird
Antwortstatus	Treffer	Gesamtzahl der mit Antwortcodes empfangenen Treffer
	Bandbreite (MB)	Gesamtbandbreite, die vom Antwortcode belegt wird

Metriken	Entität	Beschreibung
Server	Treffer	Gesamtzahl der von einem Server empfangenen Anforderungen/Treffer
	Bandbreite (MB)	Gesamtbandbreite, die von einem Server verbraucht wird
	Servernetzwerklatenz (ms)	Die Zeit, die für Anforderungen aus dem Servernetzwerk erforderlich ist
	Serververarbeitungszeit (ms)	Die Zeit, die ein Server für die Beantwortung von Anfragen in Anspruch nimmt
URLs	Treffer	Gesamtzahl der Treffer, die von einer URL empfangen wurden. Zum Beispiel: www.citrix.com
	Ladezeit (ms)	Die Zeit, die für das Laden einer URL vom Server erforderlich ist
	Renderzeit (ms)	Die Zeit, die die URL zum Rendern und Anzeigen verwendet
Benutzeragents	Treffer	Gesamtzahl der von einem User-Agent empfangenen Anforderungen. Zum Beispiel: Chrome-Webbrowser
	Bandbreite (MB)	Gesamtbandbreite, die vom User-Agent verbraucht wird
	Renderzeit (ms)	Die Zeit, die benötigt wird, um die Serverantwort durch den Benutzeragenten zu geben

Sicherheit

Metrik	Entität	Beschreibung
Anwendungen	Bedrohungsindex	Ein einstelliges Bewertungssystem, das die Kritik von Angriffen auf die Anwendung anzeigt. Je kritischer die Angriffe auf eine Anwendung sind, desto höher ist der Bedrohungsindex für diese Anwendung. Die Werte reichen von 1 bis 7.
	Sicherheitsindex	Ein einstelliges Bewertungssystem, das angibt, wie sicher Sie die Citrix ADC-Instanzen zum Schutz von Anwendungen vor externen Bedrohungen und Sicherheitslücken konfiguriert haben. Je niedriger die Sicherheitsrisiken für eine Anwendung, desto höher der Sicherheitsindex. Die Werte reichen von 1 bis 7.

APPANALYTICS

Metrik	Entität	Beschreibung
Anwendungen	AppScore	App Score definiert, wie gut eine Anwendung funktioniert, und zeigt an, ob die Anwendung in Bezug auf die Reaktionsfähigkeit gut funktioniert. Die Werte liegen zwischen 0 und 80.

HDX

Informationen zu HDX-Schwellenwerten finden Sie unterErstellen von Schwellenwerten und Konfigurieren von Warnungen für HDX Insight

Gateway Insight

April 28, 2021

In einer Citrix Gateway-Bereitstellung ist der Einblick in die Details zum Benutzerzugriff für die Behebung von Zugriffsfehlern unerlässlich Als Netzwerkadministrator möchten Sie wissen, wann ein Benutzer nicht in der Lage ist, sich bei Citrix Gateway anzumelden, und Sie möchten die Benutzeraktivität und die Gründe für den Anmeldefehler kennen, diese Informationen sind jedoch in der Regel nur verfügbar, wenn der Benutzer eine Anforderung zur Lösung sendet.

Gateway Insight bietet Einblick in die Fehler, die bei der Anmeldung bei Citrix Gateway auftreten, unabhängig vom Zugriffsmodus. Sie können eine Liste aller verfügbaren Benutzer, die Anzahl der aktiven Benutzer, die Anzahl der aktiven Sitzungen sowie die von allen Benutzern verwendeten Bytes und Lizenzen anzeigen. Sie können die Endpunktanalyse (EPA), Authentifizierung, Single Sign-On (SSO) und Anwendungsstartfehler für einen Benutzer anzeigen. Sie können auch die Details der aktiven und beendeten Sitzungen für einen Benutzer anzeigen.

Gateway Insight bietet auch Einblick in die Gründe für den Anwendungsstart für virtuelle Anwendungen. Dadurch können Sie Probleme bei der Anmeldung oder beim Starten von Anwendungen beheben. Sie können die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen, die Anzahl der Gesamtbytes und die Bandbreite der Anwendungen anzeigen. Sie können Details der Benutzer, Sitzungen, Bandbreite und Startfehler für eine Anwendung anzeigen.

Sie können die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die Gesamtbytes und die Bandbreite, die von allen Gateways verwendet wird, die mit einer ADC Gateway-Appliance zu einem bestimmten Zeitpunkt verknüpft sind, anzeigen. Sie können EPA, Authentifizierung, Single Sign-On und Anwendungsstartfehler für ein Gateway anzeigen. Sie können auch die Details aller mit einem Gateway verknüpften Benutzer und deren Anmeldeaktivität anzeigen.

Alle Protokollmeldungen werden in der Citrix Application Delivery Management (ADM) -Datenbank gespeichert, sodass Sie Fehlerdetails für einen beliebigen Zeitraum anzeigen können. Sie können auch eine Zusammenfassung der Anmeldefehler anzeigen und bestimmen, in welcher Phase des Anmeldevorgangs ein Fehler aufgetreten ist.

Punkte zu beachten:

- Gateway Insight wird in den folgenden Bereitstellungen unterstützt:
  - Access Gateway

  - Unified Gateway
- ADM-Version und -Build müssen identisch oder höher sein als die der Citrix Gateway Appliance.
- Eine Stunde Gateway Insight-Berichte können für ADC-Instanzen mit Advanced-Lizenz eingesehen werden. Eine Premium-Lizenz ist erforderlich, um Berichte von Gateway Insight über eine Stunde hinaus anzuzeigen.

Einschränkungen:

- Citrix Gateway unterstützt Gateway Insight nicht, wenn die Authentifizierungsmethode als zertifikatbasierte Authentifizierung konfiguriert ist.
- Erfolgreiche Benutzeranmeldungen, Latenz und Details auf Anwendungsebene für virtuelle ICA-Anwendungen und -Desktops sind nur auf dem HDX Insight User-Dashboard sichtbar.
- In einem Double-Hop-Modus ist die Sichtbarkeit von Fehlern auf der ADC-Gateway-Appliance in der zweiten DMZ nicht verfügbar.
- Remotedesktopprotokoll (RDP) -Desktopzugriffsprobleme werden nicht gemeldet.
- Die Gateway Insight-Datensätze für die SAML-Authentifizierung werden nicht gemeldet.
- Gateway Insight wird für die folgenden Authentifizierungstypen unterstützt. Wenn ein anderer Authentifizierungstyp als diese verwendet wird, werden möglicherweise Abweichungen in Gateway Insight angezeigt.
  - Lokal
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - Natives OTP

Gateway Insight aktivieren

Um Gateway Insight für Ihre Citrix Gateway Appliance zu aktivieren, müssen Sie zuerst die ADC Gateway-Appliance zu ADM hinzufügen. Anschließend müssen Sie AppFlow für den virtuellen Server aktivieren, der die VPN-Anwendung darstellt. Hinweise zum Hinzufügen eines Geräts zu ADM finden Sie unter Instanzen hinzufügen.

> **Hinweis**
>
> Um End-Point Analysis (EPA) -Fehler in Citrix ADM anzuzeigen, müssen Sie aktivieren Sie den Benutzernamen für AppFlow Authentifizierung, Autorisierung und Zugriffskontrolle sich auf dem ADC Gateway-Gerät anmelden.

Aktivieren von AppFlow für einen virtuellen Server in ADM

1. Navigieren Sie zu **Netzwerke > Instanzen > Citrix ADC**und wählen Sie die Instanz aus, für die Sie AppFlow aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
3. Wählen Sie den virtuellen Server aus, und klicken Sie dann auf **Analytics aktivieren**.
4. Wählen Sie unter **Erweiterte OptionenCitrix Gateway**aus.
5. Klicken Sie auf OK.

Aktivieren der AppFlow-Benutzernamenprotokollierung auf einem ADC Gateway-Gerät mithilfe der GUI

1. Navigieren Sie zu **Konfiguration > System > AppFlow > Einstellungen**, und klicken Sie dann auf **AppFlow Einstellungen ändern**.
2. Wählen **Sie im Bildschirm AppFlow Einstellungen konfigurieren** die Option **AAA Benutzername** aus, und klicken Sie dann auf **OK**.

Anzeigen von Gateway Insight-Berichten

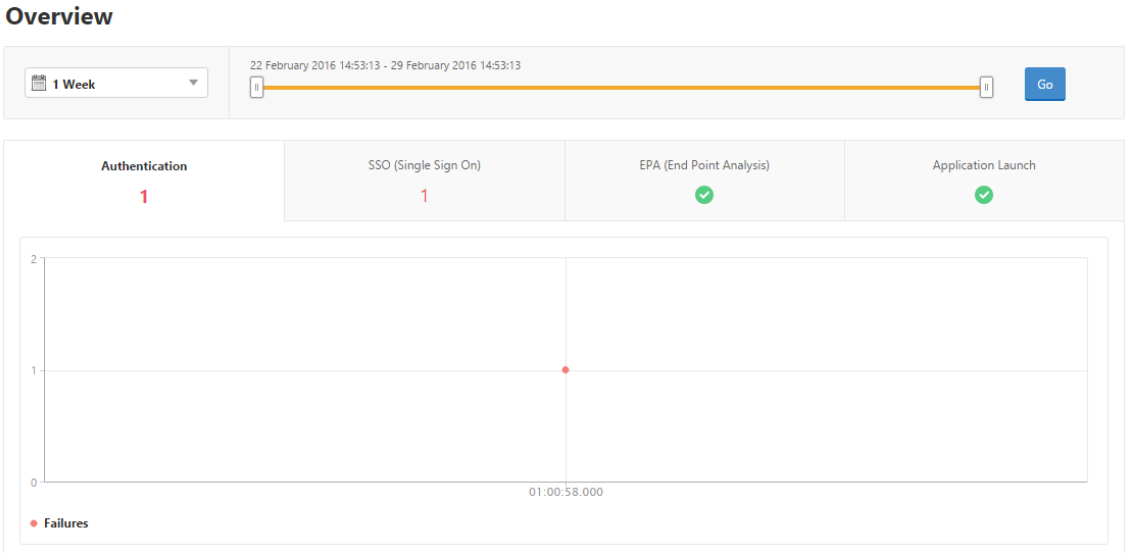
In Citrix ADM können Sie Berichte für alle Benutzer, Anwendungen und Gateways anzeigen, die mit den ADC Gateway-Appliances verknüpft sind, und Sie können Details für einen bestimmten Benutzer, eine bestimmte Anwendung oder ein bestimmtes Gateway anzeigen. Im Abschnitt **Überblick** können Sie die Fehler EPA, SSO, Authentifizierung und Application Launch anzeigen. Sie können auch eine Zusammenfassung der verschiedenen Sitzungsmodi anzeigen, die von Benutzern für die Anmeldung verwendet werden, die Clienttypen und die Anzahl der stündlich angemeldeten Benutzer.

> **Hinweis**
>
> Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, Zugriff auf Anwendungsebene für die Gruppe gewähren und der Gruppe Benutzer zuweisen. Citrix ADM Analytics unterstützt jetzt virtuelle IP-Adressen basierte Autorisierung. Ihre Benutzer können jetzt Berichte für alle Insights nur für die Anwendungen (virtuelle Server) anzeigen, für die sie autorisiert sind. Weitere Informationen zu Gruppen und dem Zuweisen von Benutzern zur Gruppe finden Sie unterKonfigurieren von Gruppen auf Citrix ADM.

Anzeigen von EPA-, SSO, Authentifizierung, Autorisierung und Anwendungsstartfehlern

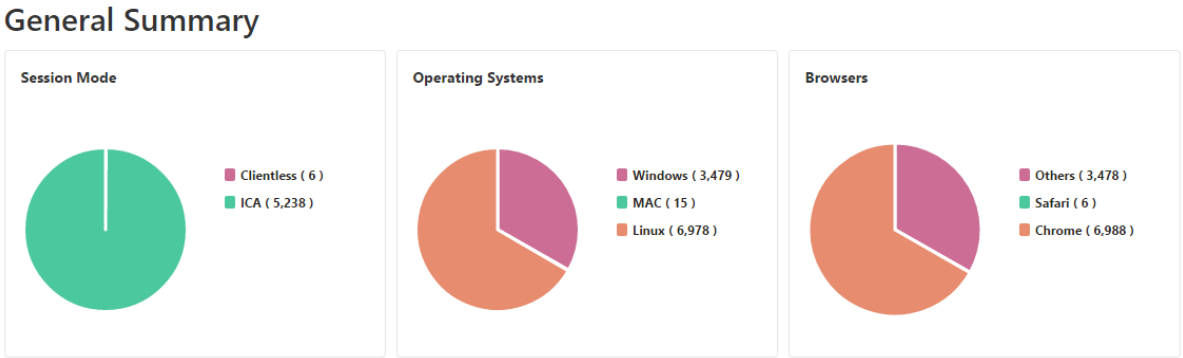
1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.

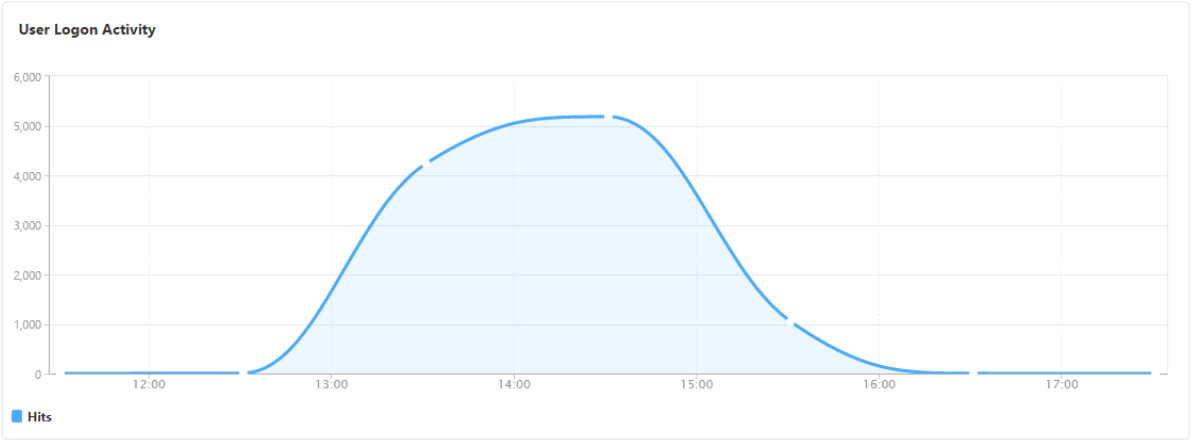
2. Wählen Sie den Zeitraum aus, für den Sie die Benutzerdetails anzeigen möchten. Mit dem Zeitschieberegler können Sie den ausgewählten Zeitraum weiter anpassen. Klicken Sie auf **Go**.
3. Klicken Sie auf die Registerkarten EPA (Endpunktanalyse), Authentifizierung, Autorisierung, SSO (Single Sign On) oder Anwendungsstart, um die Fehlerdetails anzuzeigen.



Zusammenfassung der Sitzungsmodi, Clients und der Anzahl der Benutzer anzeigen

Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**, scrollen Sie nach unten, um die Berichte anzuzeigen.

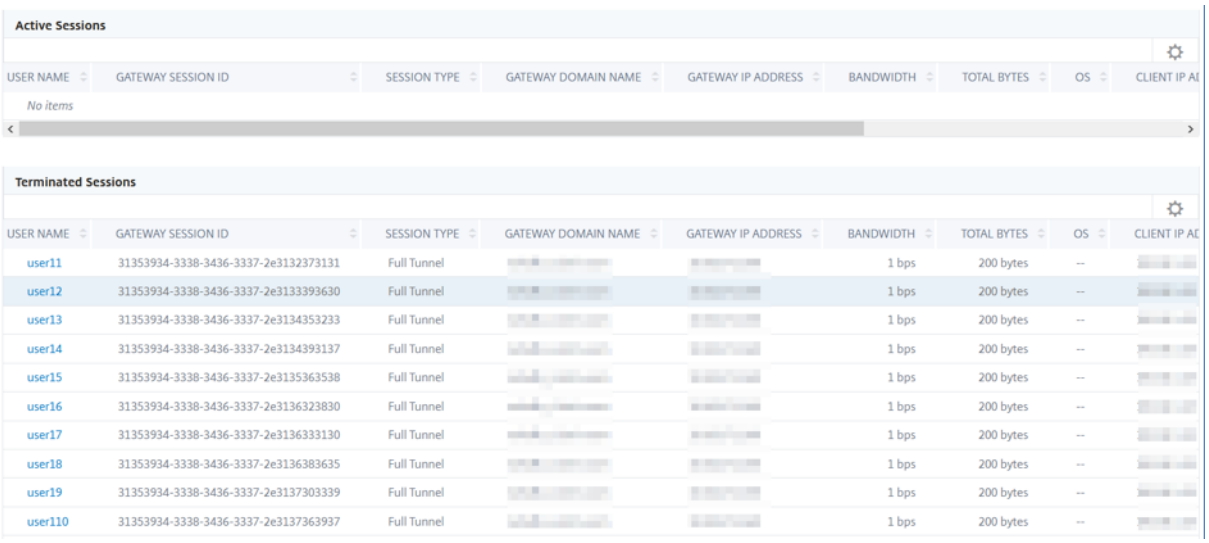




Benutzer

Sie können einen vollständigen Bericht für die Benutzer anzeigen, die mit den ADC Gateway-Appliances verknüpft sind. Sie können die EPA, Authentifizierung, SSO, Fehler beim Start von Anwendungen usw. für einen Benutzer anzeigen.

Sie können auch eine konsolidierte Ansicht aller aktiven und beendeten Sitzungen des Benutzers visualisieren.

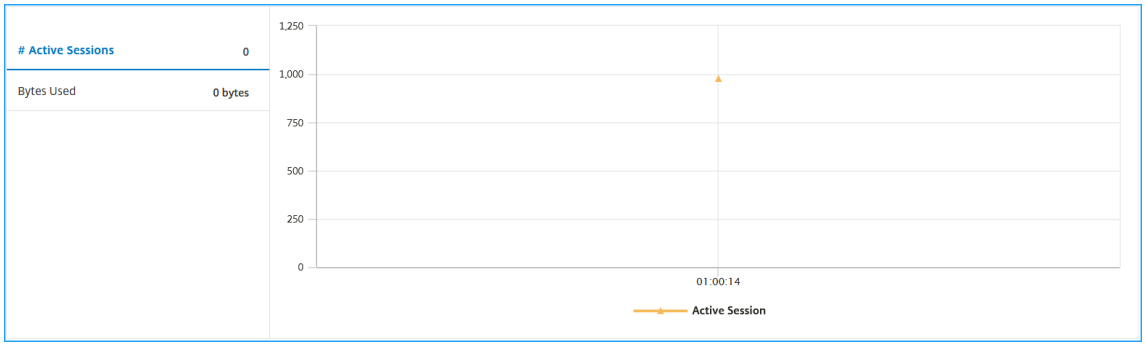


Als Administrator ermöglicht Ihnen diese Ansicht Folgendes:

- Zeigen Sie alle Benutzerdetails in einer Einzelbereichs-Visualisierung an
- Eliminieren Sie die Komplexität bei der Auswahl der einzelnen Benutzer und beim Anzeigen der aktiven und beendeten Sitzungen

Benutzerdetails anzeigen

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight > Benutzer**.
2. Wählen Sie den Zeitraum aus, für den Sie die Benutzerdetails anzeigen möchten. Mit dem Zeitschieberegler können Sie den ausgewählten Zeitraum weiter anpassen. Klicken Sie auf **Go**.
3. Sie können die Anzahl der aktiven Benutzer, die Anzahl der aktiven Sitzungen und Bytes von allen Benutzern während des Zeitraums anzeigen.

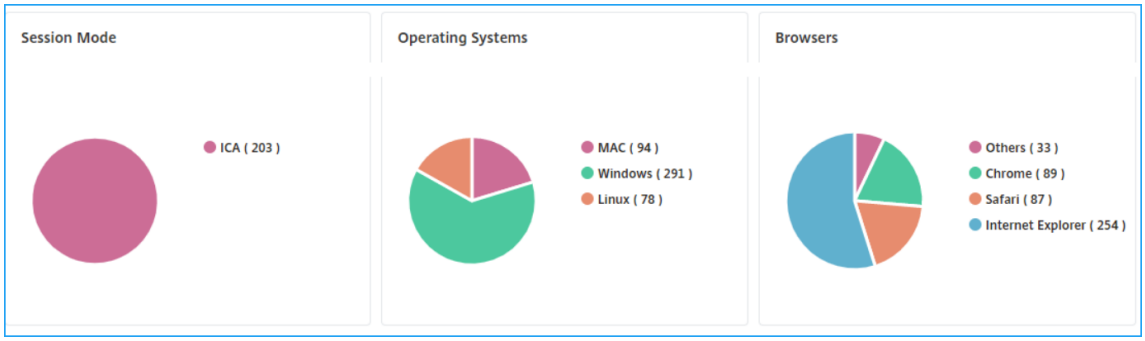


Scrollen Sie nach unten, um eine Liste der verfügbaren Benutzer und aktiven Benutzer anzuzeigen.

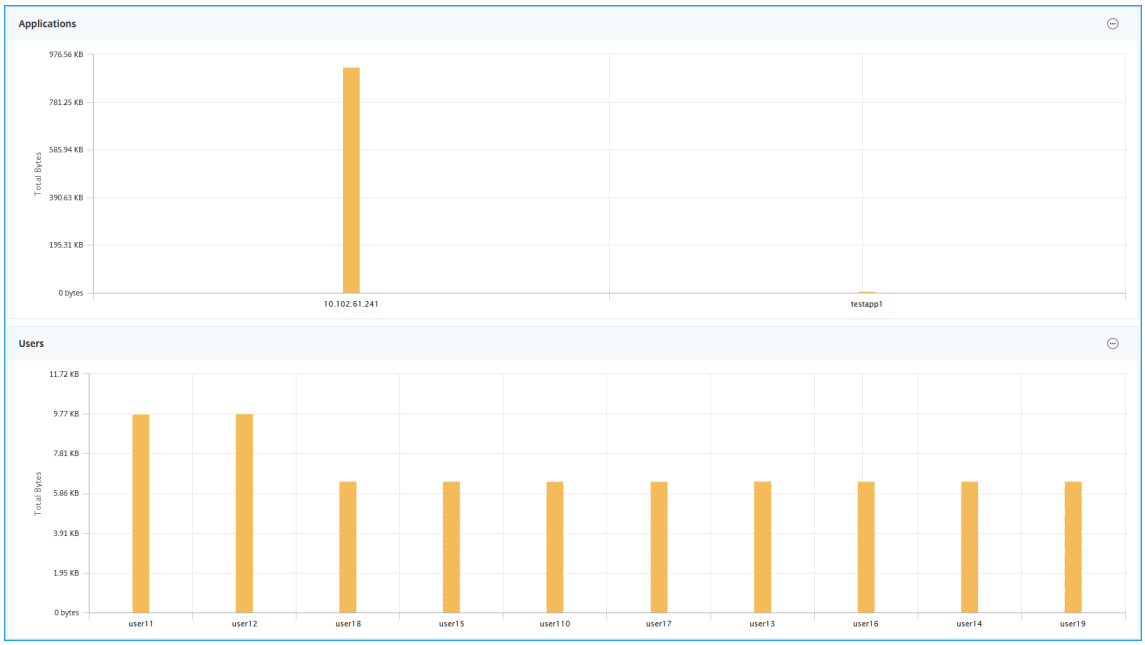
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

Klicken Sie auf der Registerkarte **Benutzer** oder **Aktive Benutzer** auf einen Benutzer, um die folgenden Benutzerdetails anzuzeigen:

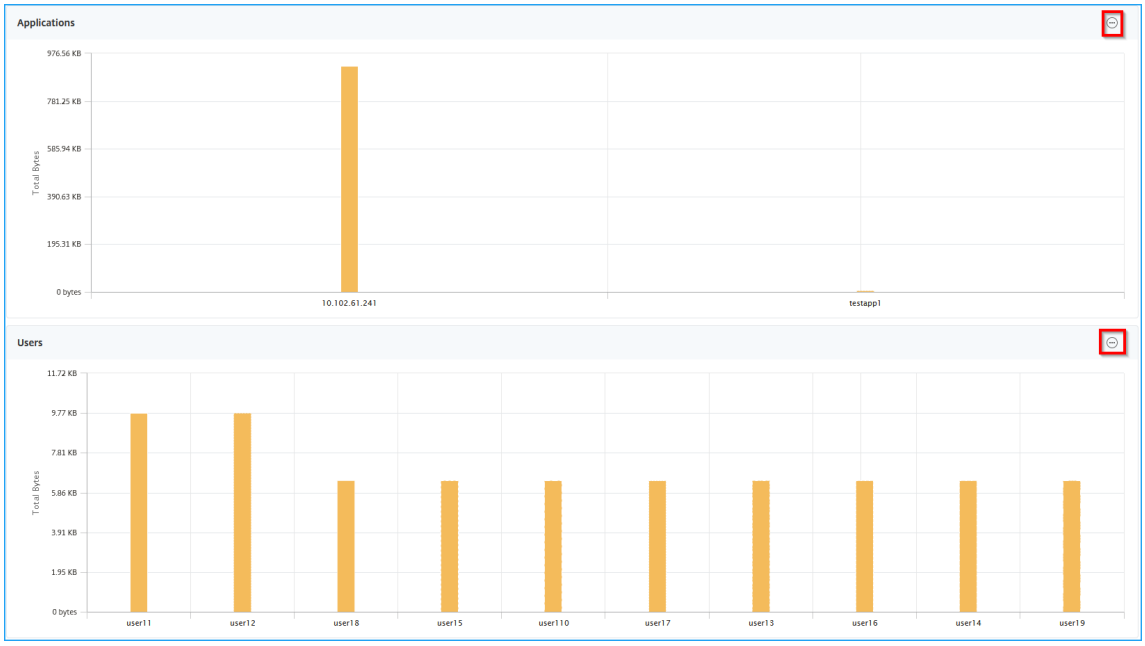
- **Benutzerdetails** - Sie können Erkenntnisse für jeden Benutzer anzeigen, der mit den ADC Gateway-Appliances verknüpft ist. Navigieren Sie zu **Analytics** > **Gateway Insight** > **Benutzer** und klicken Sie auf einen Benutzer, um Erkenntnisse für den ausgewählten Benutzer wie Sitzungsmodus, Betriebssystem und Browser anzuzeigen.



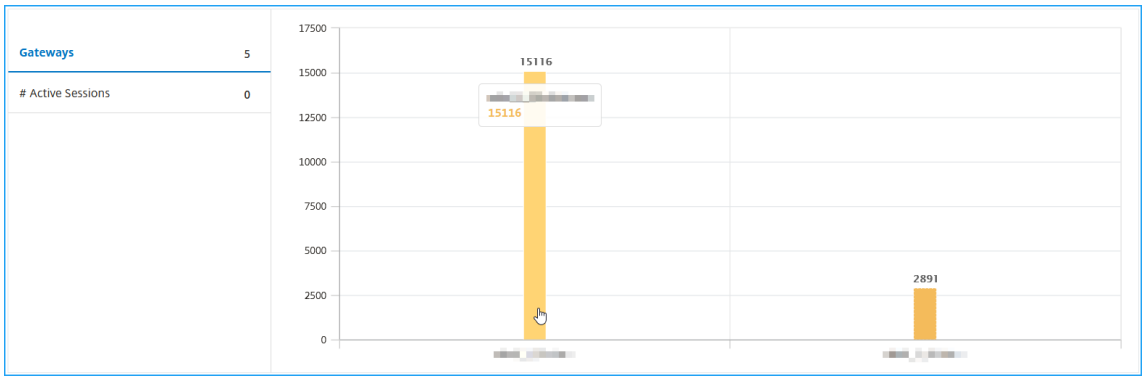
- **Benutzer und Anwendungen für das ausgewählte Gateway** - Navigieren Sie zu **Analytics** > **Gateway Insight** > **Gateway** und klicken Sie auf einen Gateway-Domänennamen, um die 10 wichtigsten Anwendungen und Top-10-Benutzer anzuzeigen, die mit dem ausgewählten Gateway verknüpft sind.



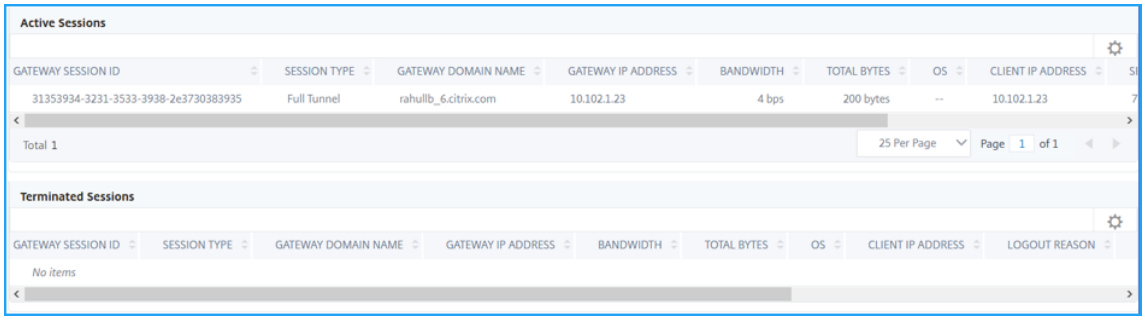
- **Weitere Optionen für Anwendungen und Benutzer anzeigen** — Für mehr als 10 Anwendungen und Benutzer können Sie auf das Mehr-Symbol in Anwendungen und Benutzer klicken, um alle Benutzer- und Anwendungsdetails anzuzeigen, die mit dem ausgewählten Gateway verknüpft sind.



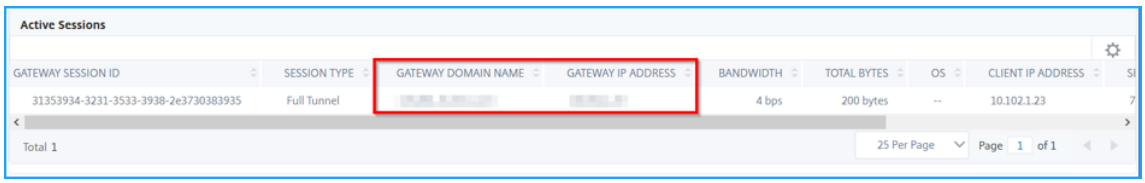
- **Zeigen Sie Details an, indem Sie auf das Balkendiagramm klicken** — Wenn Sie auf ein Balkendiagramm klicken, können Sie die relevanten Details anzeigen. Navigieren Sie beispielsweise zu **Analytics > Gateway Insight > Gateway** und klicken Sie auf das Gateway-Bar-Diagramm, um die Gateway-Details anzuzeigen.



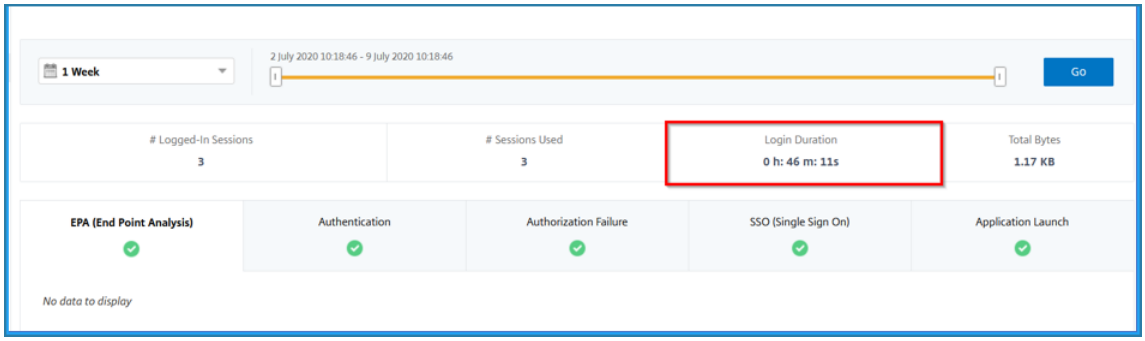
- **Active Sessions** und **Terminated Sessions** der Benutzer.



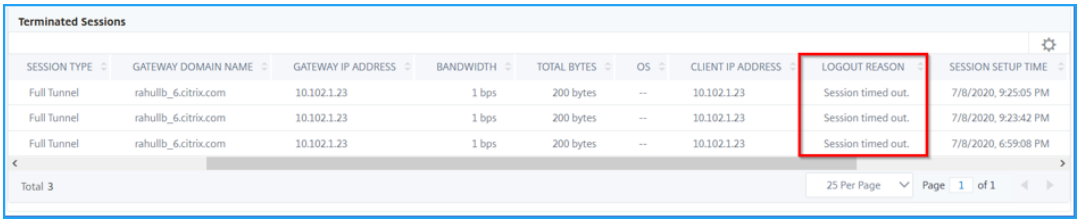
- Der Gateway-Domänenname und die Gateway-IP-Adresse in **Active Sessions**



- Die Dauer der Benutzeranmeldung.



- Der Grund für die Logout-Sitzung des Benutzers. Die Gründe für die Abmeldung können sein:
  - Zeitüberschreitung der Sitzung
  - Ausgeloggt wegen internem Fehler
  - Abgemeldet wegen zeitlich abgelaufenen inaktiven Sitzungen
  - Der Benutzer hat sich abgemeldet
  - Der Administrator hat die Sitzung beendet



Suchleiste und Geokartenansicht

Sie können sehen:

- Eine Suchleiste, mit der Sie Ergebnisse anhand des Benutzernamens filtern können. Navigieren Sie zu **Analytics > Gateway Insight > Benutzer**, um die Suchleiste für **Benutzer** und **Aktive Benutzer** anzuzeigen. Platzieren Sie den Mauszeiger auf die Suchleiste, wählen Sie **Benutzername** und geben Sie einen Benutzernamen ein, um die Ergebnisse zu filtern.

- Eine Geomap, die die Benutzerinformationen basierend auf dem geografischen Standort des Benutzers anzeigt. Als Administrator ermöglicht Ihnen diese Geomap, die Zusammenfassung der gesamten Benutzer, der gesamten Apps und der Gesamtsitzungen für einen bestimmten Standort anzuzeigen.

  1. Navigieren Sie zu **Analytics > Gateway Insight**, um die Geo-Karte anzuzeigen
  2. Klicken Sie auf ein Land. Zum Beispiel United States

     Die Geomap zeigt die Details wie Benutzerliste, aktive Sitzungen, beendete Sitzungen und Anwendungen für das ausgewählte Land an.

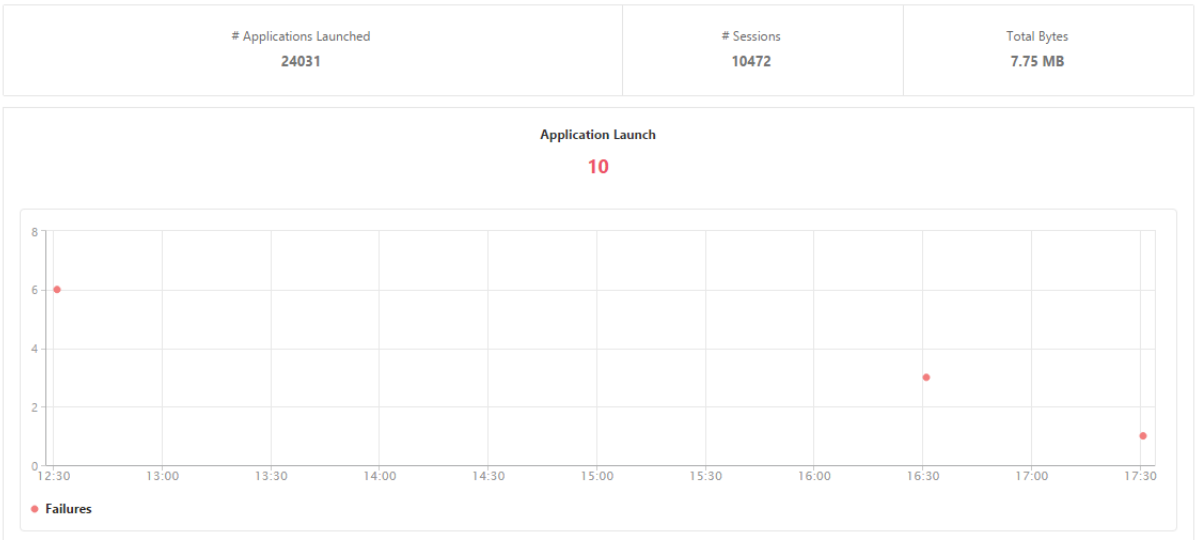
Anwendungen

Sie können die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen, die Anzahl der Gesamtbytes und die Bandbreite der Anwendungen anzeigen. Sie können Details der Benutzer, Sitzungen, Bandbreite und Startfehler für eine Anwendung anzeigen.

Anwendungsdetails anzeigen

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight > Anwendungen**.
2. Wählen Sie den Zeitraum aus, für den Sie die Anwendungsdetails anzeigen möchten. Mit dem Zeitschieberegler können Sie den ausgewählten Zeitraum weiter anpassen. Klicken Sie auf **Go**.

Sie können nun die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen, die Anzahl der Gesamtbytes und die Bandbreite der Anwendungen anzeigen.



Führen Sie einen Bildlauf nach unten durch, um die Anzahl der Sitzungen, Bandbreite und Gesamtbytes anzuzeigen, die von ICA und anderen Anwendungen belegt werden.

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

Auf der Registerkarte **Andere Anwendungen** können Sie in der Spalte **Name** auf eine Anwendung klicken, um Details zu dieser Anwendung anzuzeigen.

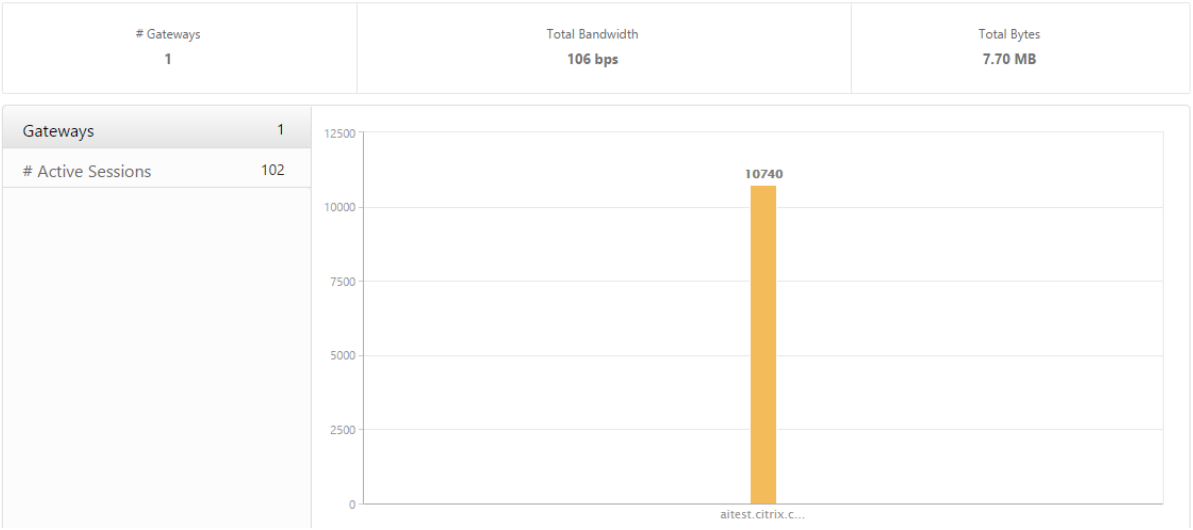
Gateways

Sie können die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die Gesamtbytes und die Bandbreite, die von allen Gateways verwendet werden, die mit einer ADC Gateway-Appliance zu einem bestimmten Zeitpunkt verknüpft sind, anzeigen. Sie können EPA, Authentifizierung, Single Sign-On und Anwendungsstartfehler für ein Gateway anzeigen. Sie können auch die Details aller mit einem Gateway verknüpften Benutzer und deren Anmeldeaktivität anzeigen.

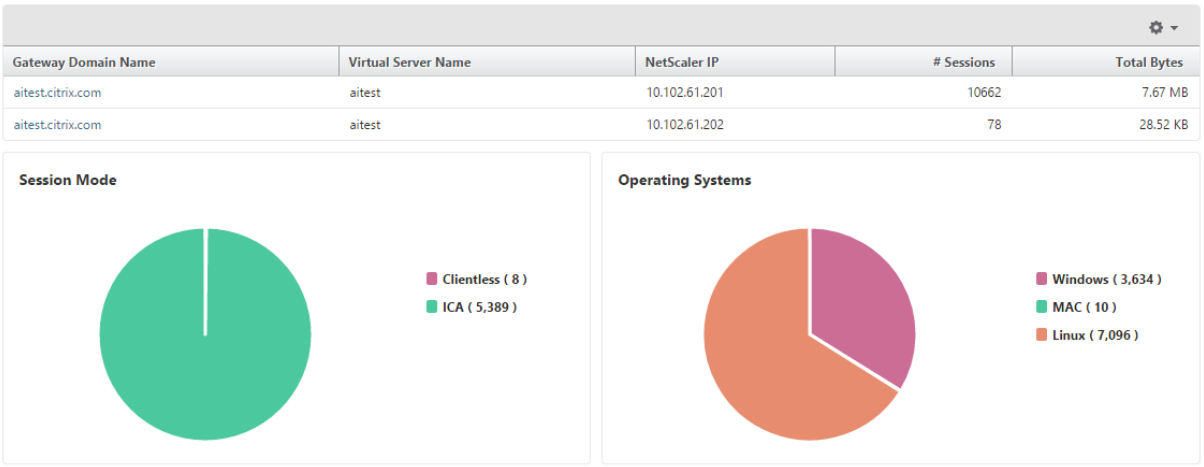
Gateway Details anzeigen

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight > Gateways**.
2. Wählen Sie den Zeitraum aus, für den Sie die Gateway Details anzeigen möchten. Mit dem Zeitschieberegler können Sie den ausgewählten Zeitraum weiter anpassen. Klicken Sie auf **Go**.

Sie können jetzt die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die Gesamtbytes und die Bandbreite anzeigen, die von allen Gateways verwendet werden, die mit einer ADC Gateway-Appliance zu einem bestimmten Zeitpunkt verknüpft sind.



Führen Sie einen Bildlauf nach unten durch, um die Gatewaydetails wie Gatewaydomänenname, Virtual Server Name, ADC-IP-Adresse, Sitzungsmodi und Total Bytes anzuzeigen.



Sie können in der Spalte **Gateway-Domänenname** auf ein Gateway klicken, um EPA, Authentifizierung, Single Sign-On und Anwendungsstart sowie andere Details für ein Gateway anzuzeigen.

Sie können auch eine Geomap für Gateways anzeigen, mit der Sie Benutzer basierend auf einem bestimmten Standort filtern können.

1. Navigieren Sie zu **Analytics > Gateway Insight > Gateways**
2. Wählen Sie einen Gateway-Domainnamen aus, um die Geomap anzuzeigen
3. Klicken Sie auf ein Land. Zum Beispiel United States

Die Geomap zeigt die Details wie Benutzerliste, aktive Sitzungen, beendete Sitzungen und Anwendungen für das ausgewählte Land an.

Exportieren von Berichten

Sie können die Gateway Insight-Berichte mit allen in der GUI angezeigten Details im PDF-, JPEG-, PNG- oder CSV-Format auf Ihrem lokalen Computer speichern. Sie können auch den Export der Berichte an bestimmte E-Mail-Adressen in verschiedenen Intervallen planen.

> **Hinweis**
>
> - Benutzer mit schreibgeschütztem Zugriff können keine Berichte exportieren.
> - Geo-Kartenberichte werden nur exportiert, wenn der ADM über eine Internetverbindung verfügt.

Exportieren eines Berichts

1. Klicken Sie auf der Registerkarte **Dashboard** im rechten Fensterbereich auf die Schaltfläche **Exportieren**.
2. Wählen Sie unter **Jetzt exportieren**das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.

So planen Sie den Export:

1. Klicken Sie auf der Registerkarte **Dashboard** im rechten Fensterbereich auf die Schaltfläche **Exportieren**.
2. Geben Sie unter **Export planen**die Details an, und klicken Sie auf **Zeitplan**.

So bearbeiten Sie den Exportzeitplan:

1. Navigieren Sie auf der Registerkarte Konfiguration zu **Konfiguration** > **NetScaler Insight Center** > **Zeitpläne exportieren**.
2. Wählen Sie einen Bericht aus der verfügbaren Liste aus, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie nach der Bearbeitung auf **Speichern**.

> **Hinweis**
>
> Konfigurieren Sie die E-Mail-Server-Einstellungen, bevor Sie den Bericht planen, indem Sie zu **System**> **Benachrichtigungen**> **E-Mail**navigieren und auf **Hinzufügen**klicken.

So fügen Sie einen E-Mail-Server oder eine E-Mail-Verteilerliste hinzu:

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **Benachrichtigungen** > **E-Mail**.

2. Wählen Sie im rechten Fensterbereich **E-Mail-Server**aus, um einen E-Mail-Server hinzuzufügen, oder wählen Sie **E-Mail-Verteilerliste**aus, um eine E-Mail-Verteilerliste zu erstellen.
3. Geben Sie die Details an, und klicken Sie auf **Erstellen**.

So exportieren Sie das gesamte Gateway Insight-Dashboard:

1. Klicken Sie auf der Registerkarte **Dashboard** im rechten Fensterbereich auf die Schaltfläche **Exportieren**.
2. Wählen Sie unter **Jetzt exportieren**die Option **PDF-Format**aus, und klicken Sie dann auf **Exportieren**.

Gateway Insight Anwendungsfälle

Die folgenden Anwendungsfälle zeigen, wie Sie Gateway Insight verwenden können, um Einblick in die Zugriffsdetails, Anwendungen und Gateways von Benutzern auf ADC Gateway-Appliances zu erhalten.

1. Der Benutzer kann sich nicht an der ADC Gateway-Appliance oder an den internen Webservern anmelden

Sie sind ein ADC-Gateway-Administrator, der ADC Gateway-Geräte über ADM überwacht, und Sie möchten sehen, warum sich ein Benutzer nicht anmelden kann oder in welchem Stadium des Anmeldevorgangs der Fehler aufgetreten ist.

Mit ADM können Sie die Benutzeranmeldefehlerdetails in den folgenden Phasen des Anmeldeprozesses anzeigen:

- Authentifizierung
- Endpunktanalyse (EPA)
- Single Sign-On

In ADM können Sie nach einem bestimmten Benutzer suchen und dann alle Details für diesen Benutzer anzeigen.

So suchen Sie nach einem Benutzer:

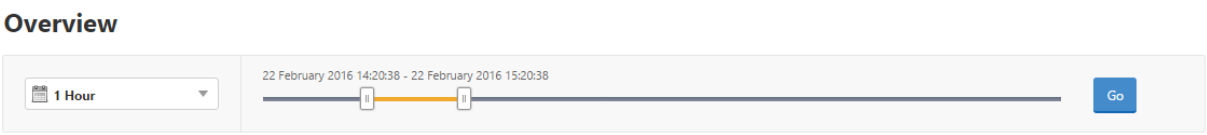
Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**, und geben Sie im Textfeld Nach **Benutzern suchen** den Benutzer an, den Sie suchen möchten.

Authentifizierungsfehler

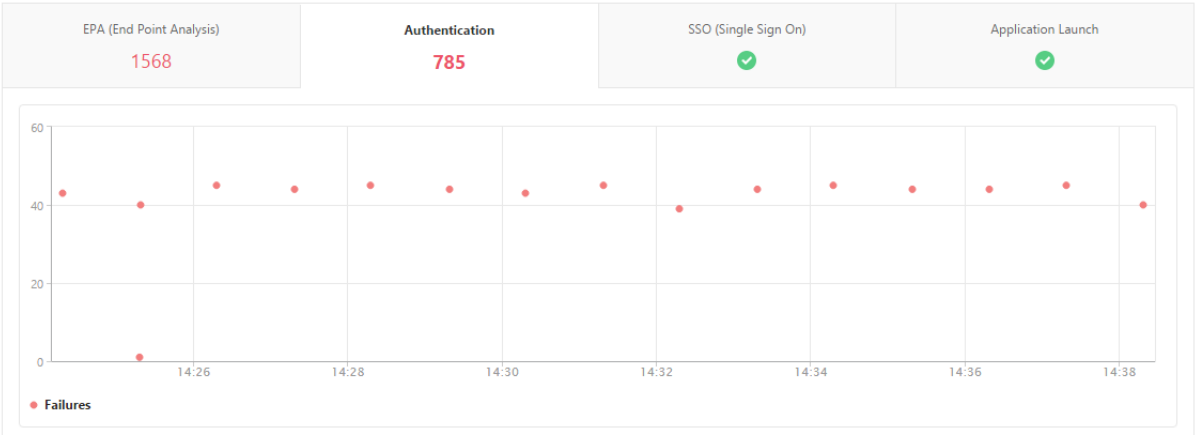
Sie können Authentifizierungsfehler wie falsche Anmeldeinformationen oder keine Antwort vom Authentifizierungsserver anzeigen. Wenn Sie die zweistufige Authentifizierung eingerichtet haben, können Sie sehen, ob die primäre, sekundäre oder beide Phasen der Authentifizierung fehlgeschlagen sind.

Details zum Authentifizierungsfehler anzeigen

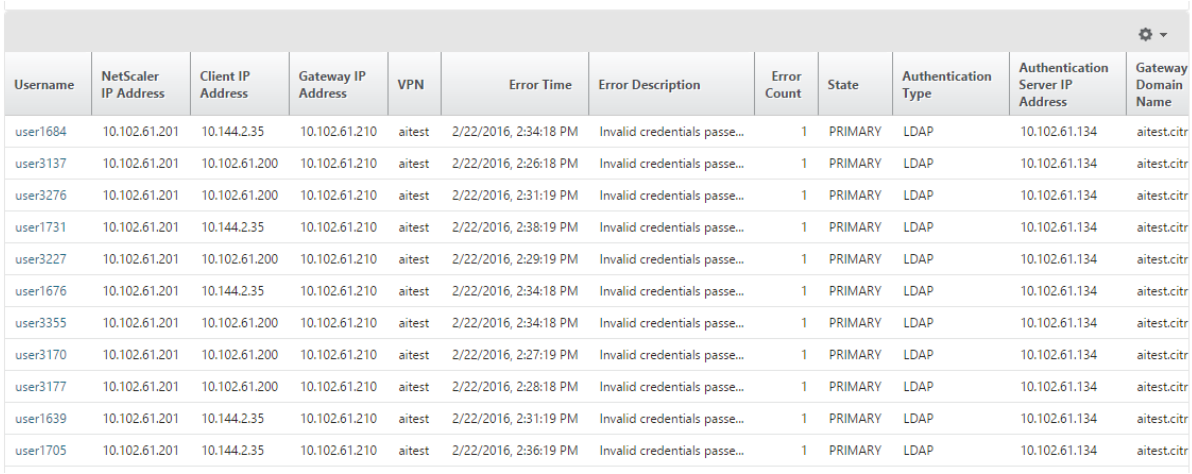
1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Wählen Sie im Abschnitt **Übersicht** den Zeitraum aus, für den Sie die Authentifizierungsfehler anzeigen möchten. Mit dem Zeitschieberegler können Sie den ausgewählten Zeitraum weiter anpassen. Klicken Sie auf **Go**.



1. Klicken Sie auf die Registerkarte **Authentifizierung**. Sie können die Anzahl der Authentifizierungsfehler jederzeit im Diagramm **Fehler** anzeigen.



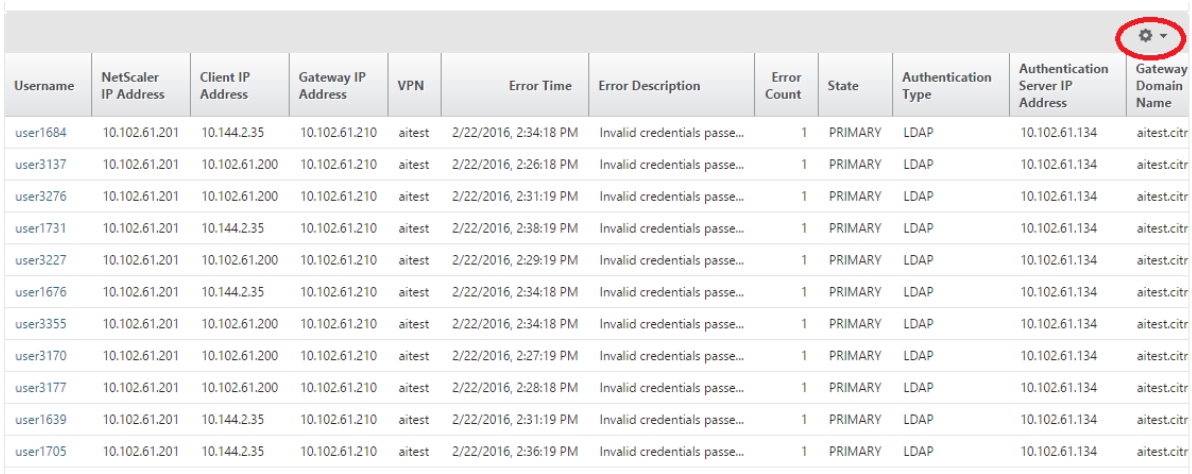
Führen Sie einen Bildlauf nach unten durch, um Details zu jedem Authentifizierungsfehler wie **Benutzername, Client-IP-Adresse, Fehlerzeit, Authentifizierungstyp, IP-Adresse des Authentifizierungsservers**und mehr aus der Tabelle auf derselben Registerkarte anzuzeigen. In der Spalte **Fehlerbeschreibung** in der Tabelle wird der Grund für den Anmeldefehler angezeigt, und in der Spalte **Status** wird angezeigt, in welchem Stadium einer zweistufigen Authentifizierung der Fehler aufgetreten ist.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die Authentifizierungsfehler und andere Details für diesen Benutzer anzuzeigen.

Sie können die Tabelle zum Hinzufügen oder Löschen von Spalten anpassen, indem Sie den in der folgenden Abbildung angegebenen Listenpfeil verwenden.



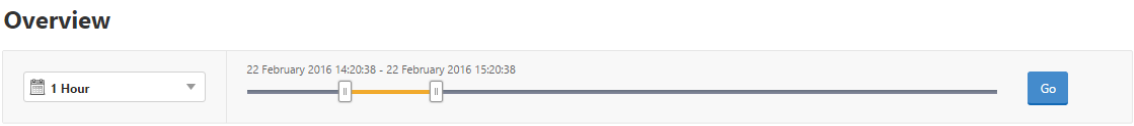
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

EPA-Ausfälle

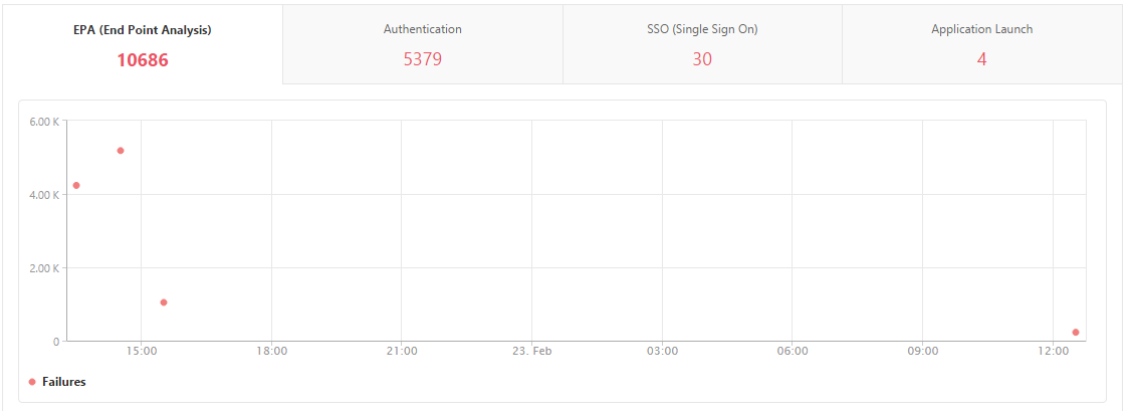
Sie können EPA-Fehler in der Phase vor oder nach der Authentifizierung anzeigen.

EPA-Fehlerdetails anzeigen

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Wählen Sie im Abschnitt Übersicht den Zeitraum aus, für den Sie die EPA-Fehler anzeigen möchten. Mit dem Zeitschieberegler können Sie den ausgewählten Zeitraum weiter anpassen. Klicken Sie auf **Go**.



3. Klicken Sie auf die Registerkarte **EPA (Endpunktanalyse)**. Sie können die Anzahl der EPA-Fehler jederzeit im Diagramm **Fehler** anzeigen.

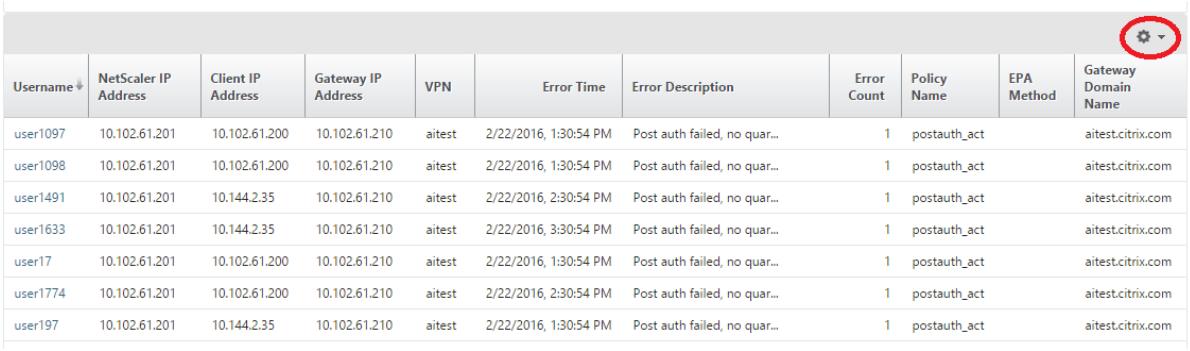


Führen Sie einen Bildlauf nach unten durch, um Details zu jedem EPA-Fehler wie **Benutzername, ADC-IP-Adresse, Gateway-IP-Adresse, VPN, Fehlerzeit, Richtlinienname, Gateway-Domänenname** und mehr aus der Tabelle auf derselben Registerkarte anzuzeigen. In der Spalte **Fehlerbeschreibung** in der Tabelle wird der Grund für den EPA-Fehler angezeigt, und in der Spalte **Richtlinienname** wird die Richtlinie angezeigt, die zum Fehler geführt hat.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die EPA-Fehler und andere Details für diesen Benutzer anzuzeigen.

Sie können die Tabelle zum Hinzufügen oder Löschen von Spalten anpassen, indem Sie den in der folgenden Abbildung angegebenen Listenpfeil verwenden.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

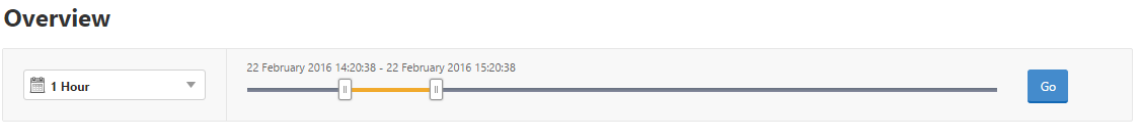
> **Hinweis**
>
> ADC Gateway meldet die EPA-Fehler nicht, wenn der Ausdruck ClientSecurity als VPN-Sitzungsrichtlinienregel konfiguriert ist.

SSO-Fehler

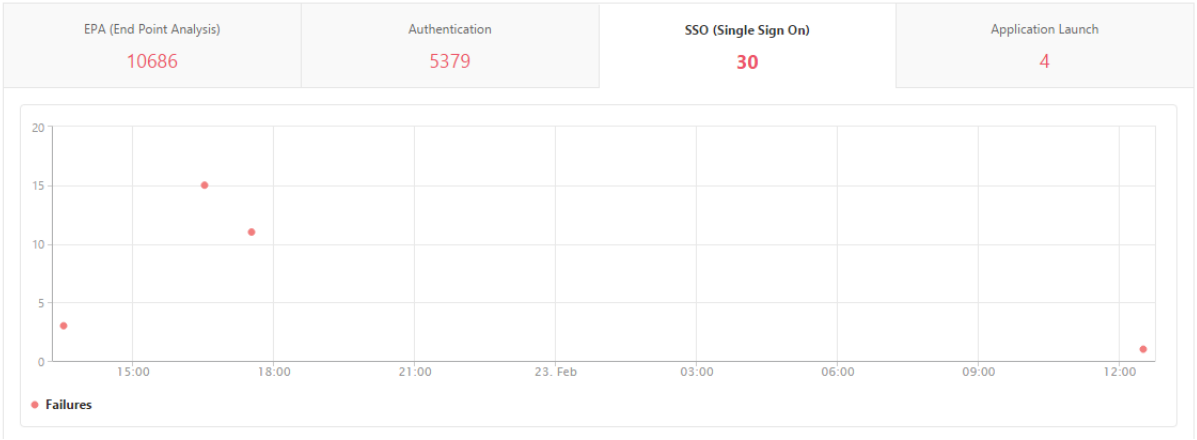
Sie können alle SSO-Fehler in jeder Phase für einen Benutzer anzeigen, der über die ADC-Gateway-Appliance auf Anwendungen zugreift.

Details zum SSO-Ausfall anzeigen

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Wählen Sie im Abschnitt Übersicht den Zeitraum aus, für den Sie die SSO-Fehler anzeigen möchten. Mit dem Zeitschieberegler können Sie den ausgewählten Zeitraum weiter anpassen. Klicken Sie auf **Go**.



3. Klicken Sie auf die Registerkarte **SSO (Single Sign On)**. Sie können die Anzahl der SSO-Fehler jederzeit im Diagramm Fehler anzeigen.



Scrollen Sie nach unten, um Details zu jedem SSO-Fehler wie **Benutzername, ADC-IP-Adresse, Fehlerzeit, Fehlerbeschreibung, Ressourcenname** und mehr aus der Tabelle auf derselben Registerkarte anzuzeigen.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die SSO-Fehler und andere Details für diesen Benutzer anzuzeigen.

Sie können die Tabelle zum Hinzufügen oder Löschen von Spalten anpassen, indem Sie den in der folgenden Abbildung angegebenen Listenpfeil verwenden.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

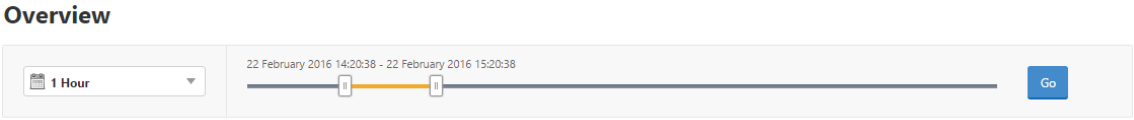
2. Nach erfolgreicher Anmeldung bei ADC Gateway kann ein Benutzer keine virtuelle Anwendung starten

Bei einem Anwendungsstartfehler können Sie Einblick in die Gründe gewinnen, z. B. unzugängliche Secure Ticket Authority (STA) oder Citrix Virtual App Server oder ungültiges STA Ticket. Sie können

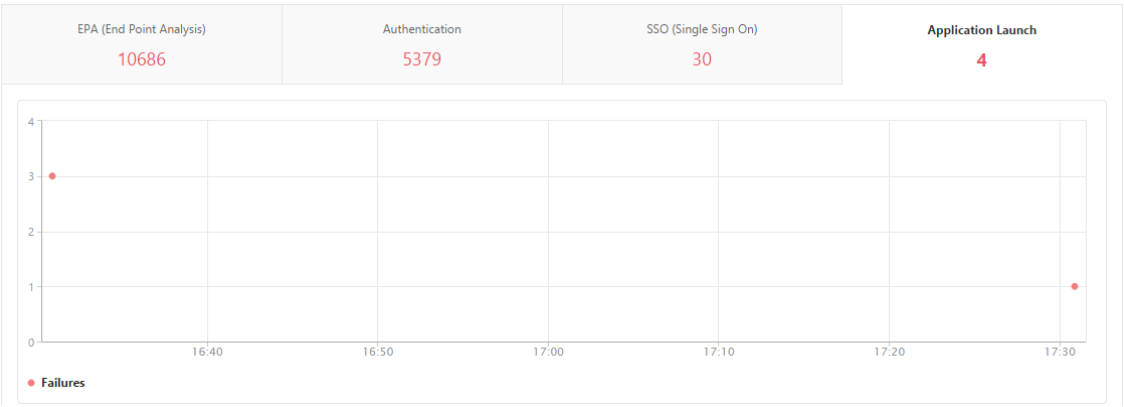
den Zeitpunkt des Auftretens des Fehlers, Details des Fehlers und die Ressource anzeigen, für die die STA-Validierung fehlgeschlagen ist.

Details zum Starten von Anwendungsfehlern anzeigen

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Wählen Sie im Abschnitt **Übersicht** den Zeitraum aus, für den Sie die SSO-Fehler anzeigen möchten. Mit dem Zeitschieberegler können Sie den ausgewählten Zeitraum weiter anpassen. Klicken Sie auf **Go**.



3. Klicken Sie auf die Registerkarte **Anwendungsstart**. Sie können die Anzahl der Anwendungsstartfehler zu einem bestimmten Zeitpunkt im Diagramm **Fehler** anzeigen.

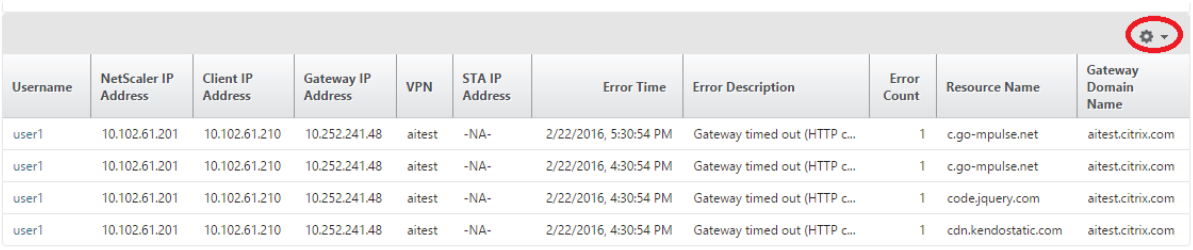


Führen Sie einen Bildlauf nach unten aus, um Details zu jedem Anwendungsstartfehler wie **ADC-IP-Adresse, Fehlerzeit, Fehlerbeschreibung, Ressourcenname, Gateway-Domänenname**usw. aus der Tabelle auf derselben Registerkarte anzuzeigen. In der Spalte **Fehlerbeschreibung** in der Tabelle wird die IP-Adresse des STA-Servers angezeigt, und in der Spalte **Ressourcenname** werden die Details der Ressource angezeigt, für die die STA-Validierung fehlgeschlagen ist.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die Programmstartfehler und andere Details für diesen Benutzer anzuzeigen.

Sie können die Tabelle zum Hinzufügen oder Löschen von Spalten anpassen, indem Sie den in der folgenden Abbildung angegebenen Listenpfeil verwenden.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

3. Nachdem eine neue Anwendung erfolgreich gestartet wurde, möchte ein Benutzer die Gesamtbytes und Bandbreite anzeigen, die von dieser Anwendung belegt wurden

Nachdem Sie eine neue Anwendung erfolgreich gestartet haben, können Sie in Citrix ADM die Gesamtbytes und Bandbreite anzeigen, die von dieser Anwendung belegt werden.

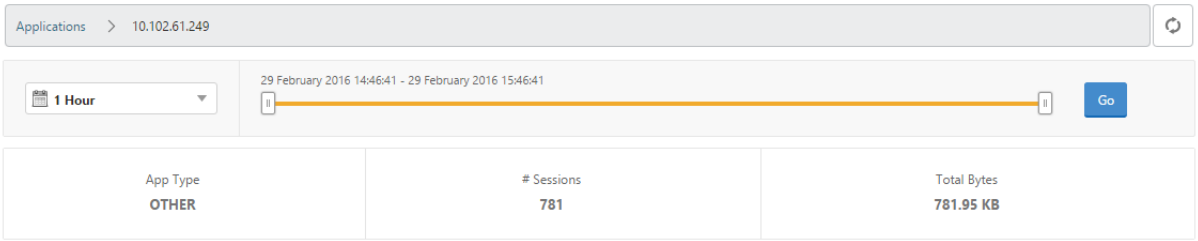
Anzeigen von Gesamtbytes und Bandbreite, die von einer Anwendung belegt werden

Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight > Anwendungen**, scrollen Sie nach unten, und klicken Sie auf der Registerkarte **Andere Anwendungen**auf die Anwendung, für die Sie die Details anzeigen möchten.

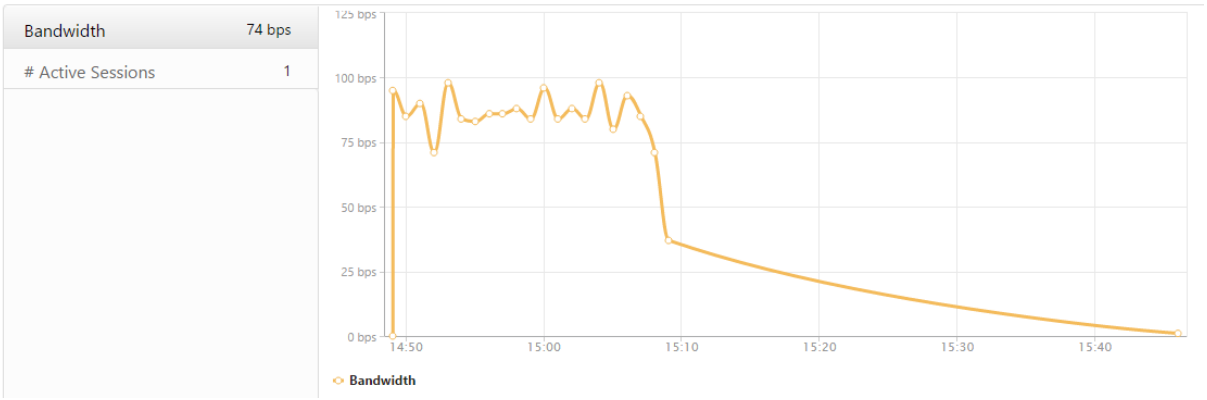
ICA Applications | Other Applications

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.134	1	0 bps	12.19 KB
10.102.61.249	4	0 bps	82.32 KB
alt1-safebrowsing.google.com	1	0 bps	1.04 KB
bcwhwkevnw	1	0 bps	1.98 KB
bcwhwkevnw.citrite.net	1	0 bps	1.01 KB

Sie können die Anzahl der Sitzungen und die Gesamtanzahl der Bytes anzeigen, die von dieser Anwendung belegt werden.



Sie können auch die von dieser Anwendung verbrauchte Bandbreite anzeigen.

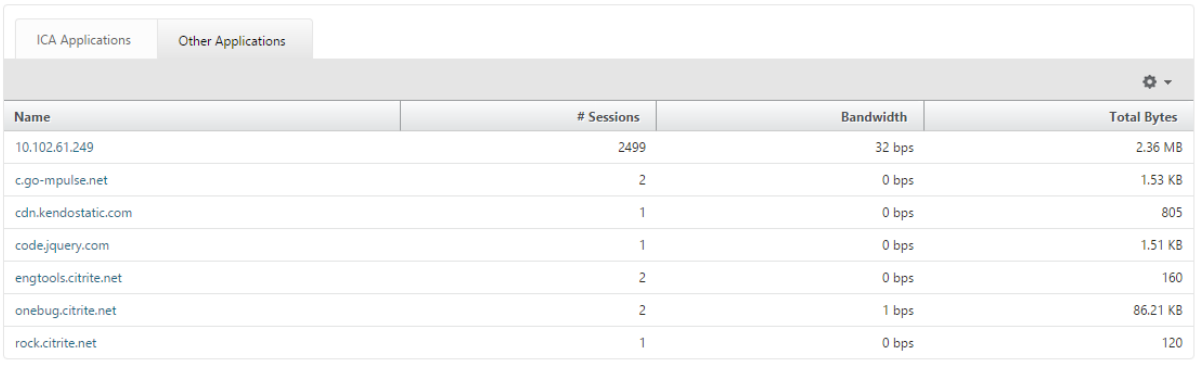


4. Ein Benutzer hat sich erfolgreich bei ADC Gateway angemeldet, kann jedoch nicht auf bestimmte Netzwerkressourcen im internen Netzwerk zugreifen

Mit Gateway Insight können Sie bestimmen, ob der Benutzer Zugriff auf die Netzwerkressourcen hat oder nicht. Sie können auch den Namen der Richtlinie anzeigen, die zum Fehler geführt hat.

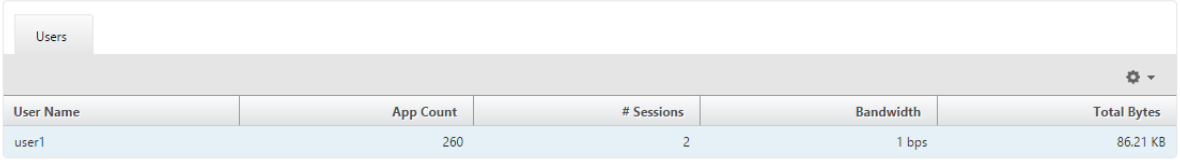
Anzeigen des Benutzerzugriffs für Ressourcen

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight > Anwendungen**.
2. Wählen Sie auf dem angezeigten Bildschirm einen Bildlauf nach unten und auf der Registerkarte **Andere Anwendungen** die Anwendung aus, bei der sich der Benutzer nicht anmelden konnte.



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

Scrollen Sie auf dem angezeigten Bildschirm nach unten und in der Tabelle **Benutzer** alle Benutzer, die Zugriff auf diese Anwendung haben, angezeigt.



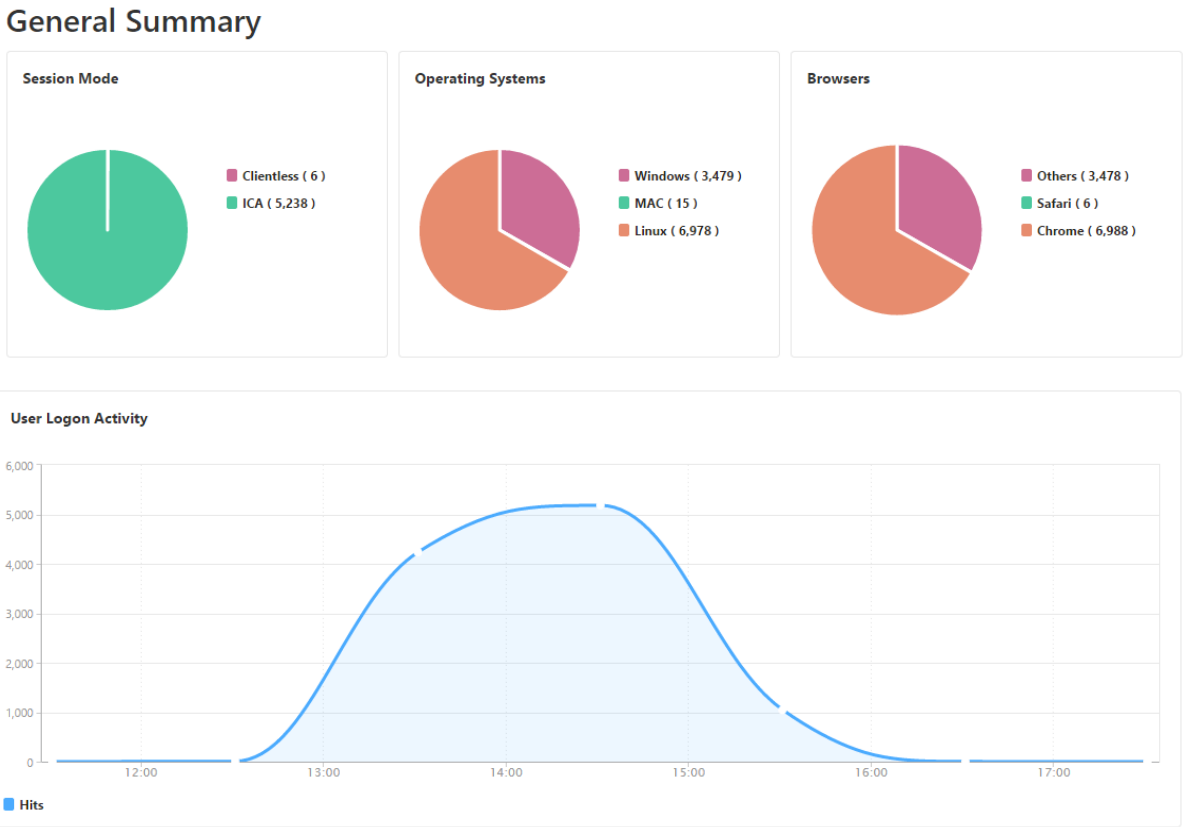
User Name	App Count	# Sessions	Bandwidth	Total Bytes
user1	260	2	1 bps	86.21 KB

5. Verschiedene Benutzer verwenden möglicherweise unterschiedliche ADC Gateway-Bereitstellungen oder melden sich bei ADC Gateway über verschiedene Zugriffsmodi an. Der Administrator muss in der Lage sein, Details zu den Bereitstellungstypen und Zugriffsmodi anzuzeigen

Mit Gateway Insight können Sie eine Zusammenfassung der verschiedenen Sitzungsmodi anzeigen, die von Benutzern für die Anmeldung verwendet werden, die Clienttypen und die Anzahl der stündlich angemeldeten Benutzer. Sie können auch bestimmen, ob es sich bei der Bereitstellung eines Benutzers um ein einheitliches Gateway oder eine klassische ADC-Gateway-Bereitstellung handelt. Bei Unified Gateway Bereitstellungen können Sie den Namen und die IP-Adresse des virtuellen Servers mit Content Switching sowie den Namen des virtuellen VPN-Servers anzeigen.

Zusammenfassung der Sitzungsmodi, des Clienttyps und der Anzahl der angemeldeten Benutzer anzeigen

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Führen Sie im Abschnitt **Übersicht einen** Bildlauf nach unten durch, um die Diagramme **Sitzungsmodus, Betriebssysteme, Browser** und **Benutzeranmeldeaktivitätsdiagramme** anzuzeigen, die von Benutzern zur Anmeldung verwendeten Sitzungsmodi, die Clienttypen und die Anzahl der stündlich angemeldeten Benutzer.



Beheben von Gateway-Insight-Problemen

April 28, 2021

Wenn die Gateway Insight-Lösung nicht wie erwartet funktioniert, liegt das Problem möglicherweise mit einem der folgenden Probleme vor. Informationen zur Fehlerbehebung finden Sie in den Checklisten in den entsprechenden Abschnitten.

- Gateway Insight-Konfiguration.
- Verbindungsproblem zwischen Citrix ADC und Citrix ADM.
- Datensatzgenerierung in Citrix ADC.
- Validierungen in Citrix ADM.

Checkliste für die Konfiguration von Gateway Insight

- Stellen Sie sicher, dass die AppFlow Funktion in Citrix ADC aktiviert ist. Einzelheiten finden Sie unter AppFlow aktivieren.
- Überprüfen Sie die Gateway Insight-Konfiguration in der Citrix ADC Konfiguration.

  Führen Sie den `show running | grep -i <appflow_policy>` Befehl aus, um die Gateway Insight Konfiguration zu überprüfen. Stellen Sie sicher, dass der Bindungstyp REQUEST ist. Zum Beispiel;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

- Stellen Sie bei der Bereitstellung von Single-Hop-, Access Gateway- oder Unified Gateway-Bereitstellung sicher, dass die Gateway Insight AppFlow Richtlinie an den virtuellen VPN-Server gebunden ist, auf dem der VPN-Datenverkehr fließt. Einzelheiten finden Sie unter Aktivieren der HDX Insight Datenerfassung.
- Überprüfen Sie die Parameter `appflowlog` auf dem virtuellen Citrix Gateway/VPN-Server. Einzelheiten finden Sie unter Aktivieren von AppFlow für virtuelle Server.

Konnektivität zwischen Citrix ADC und Citrix ADM Checkliste

- Überprüfen Sie den AppFlow Collector-Status in Citrix ADC. Einzelheiten finden Sie unter Überprüfen des Status der Verbindung zwischen Citrix ADC und AppFlow Collector.
- Überprüfen Sie Gateway Insight AppFlow Richtlinientreffer.

  Führen Sie den Befehl `show appflow policy <policy_name>` aus, um die Treffer der AppFlow-Richtlinie zu überprüfen.

  Sie können auch in der GUI zu **System > AppFlow > Richtlinien** navigieren, um die AppFlow-Richtlinientreffer zu überprüfen.

- Überprüfen Sie jede Firewall, die AppFlow Ports 4739 oder 5557 blockiert.

Datensatzgenerierung in Citrix ADC Checkliste

- Führen Sie den Befehl `nsconmsg -d stats -g ai_tot` aus und suchen Sie nach den Statistik-Inkrementen in Citrix ADC.
- Erfassen Sie `nstrace` Protokolle und suchen Sie nach CFLOW-Paketen, um zu bestätigen, dass Citrix ADC AppFlow-Datensätze exportiert

Validierungen in Citrix ADM

- Führen Sie den Befehl `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` aus, um die Protokolle zu überprüfen, um zu bestätigen, dass Citrix ADM AppFlow-Einträge erhält.
- Stellen Sie sicher, dass die Citrix ADC-Instanz zu Citrix ADM hinzugefügt wird.
- Stellen Sie sicher, dass der virtuelle Citrix Gateway/VPN-Server in Citrix ADM lizenziert ist.

Gateway Insight Statistiken

Die folgenden Gateway Insight-Statistiken sind verfügbar.

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled

Wenden Sie sich an den technischen Support von Citrix

Um eine schnelle Lösung zu erhalten, stellen Sie sicher, dass Sie die folgenden Informationen haben, bevor Sie sich an den technischen Support von Citrix wenden:

- Details zur Bereitstellung und Netzwerktopologie.
- Citrix ADC und Citrix ADM Versionen.
- Technisches Support-Paket für Citrix ADC und Citrix ADM.
- `nstrace` während der Ausgabe erfassen.

Bekannte Probleme

Weitere Informationen zu bekannten Problemen in Gateway Insight finden Sie in den Citrix ADC Versionshinweisen.

Details zu Anwendungssicherheitsverletzungen anzeigen

April 28, 2021

Webanwendungen, die dem Internet ausgesetzt sind, sind drastisch anfällig für Angriffe geworden. Mit Citrix ADM können Sie ausführbare Verstöße visualisieren, um Anwendungen vor Angriffen zu schützen. Navigieren Sie zu **Analytics** > **Sicherheit** > **Sicherheitsverletzungen** für eine Single-Pane-Lösung, um:

- Visualisieren Sie Anwendungen mit umfassendem Einblick in die Bedrohungsdetails, die sowohl mit Sicherheits-Einblicken als auch mit Bot-Erkennt
- Greifen Sie auf die Anwendungssicherheitsverletzungen basierend auf den Kategorien **Netzwerk**, **Bot**und **WAF**zu.
- Ergreifen Sie Korrekturmaßnahmen, um die Anwendungen zu sichern

Die Seite “ **Sicherheitsverletzungen** “ enthält die folgenden Optionen:

- **Anwendungsübersicht** — Zeigt eine Übersicht mit Anwendungen an, die totale Verstöße, totale WAF- und Bot-Verstöße, Verstöße nach Ländern usw. aufweisen. Weitere Informationen finden Sie unter Anwendungsübersicht.
- **Alle Verstöße** — Zeigt die Details zur Verletzung der Anwendungssicherheit an. Weitere Informationen finden Sie unter Alle Verstöße.

Einrichten

Sie müssen **Advanced Security Analytics** aktivieren und **Web-Transaktionseinstellungen fürAlle** auswählen, um die folgenden Verstöße in Citrix ADM anzuzeigen:

- Ungewöhnlich hohe Upload-Transaktionen (WAF)
- Ungewöhnlich hohe Download-Transaktionen (WAF)

- Übermäßige eindeutige IPs (WAF)
- Kontoübernahme (BOT)
- Webseite Scanner (BOT)
- Inhalt Scrapers (BOT)

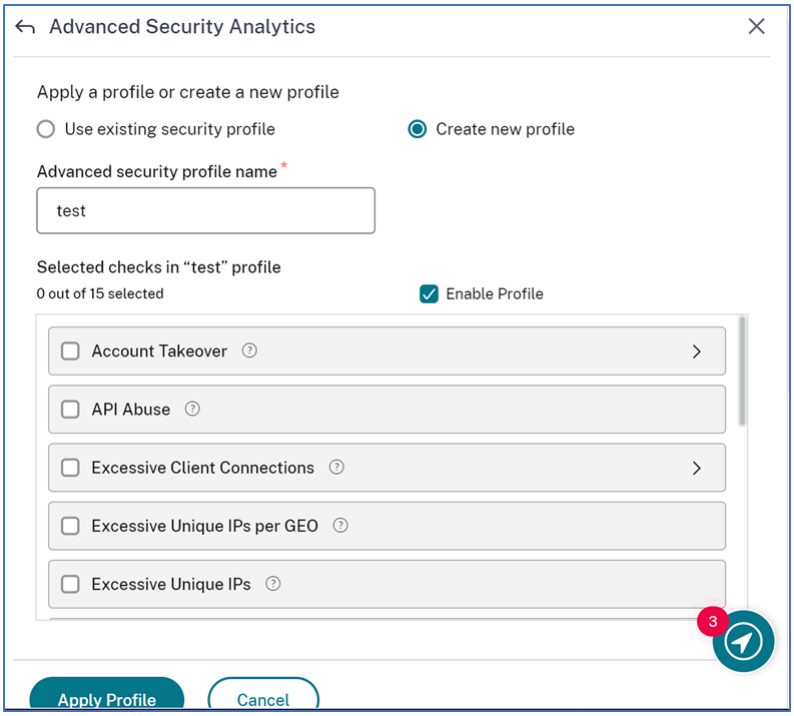
Stellen Sie bei anderen Verstößen sicher, ob **Metrics Collector** aktiviert ist. Standardmäßig ist **Metrics Collector** auf der Citrix ADC-Instanz aktiviert. Weitere Informationen finden Sie unter Intelligente App Analytics konfigurieren.

Erweiterte Sicherheitsanalysen aktivieren

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**, und wählen Sie den Instanztyp aus. Zum Beispiel MPX.
2. Wählen Sie die Citrix ADC-Instanz aus und klicken Sie in der Liste **Aktion auswählen** auf **Analytics konfigurieren**.
3. Wählen Sie den virtuellen Server aus, und klicken Sie auf **Analytics aktivieren**.
4. Im Fenster **Analytics aktivieren**:
   a) Wählen Sie **Web Insight**aus. Nachdem Sie Web Insight ausgewählt haben, wird die schreibgeschützte **Advanced Security Analytics-Option** automatisch aktiviert.

      > **Hinweis**
      >
      > Die Option **Advanced Security Analytics** wird nur für Premium lizenzierte ADC-Instanzen angezeigt.

   b) **Logstream** als Transportmodus auswählen
   c) Der Ausdruck ist standardmäßig true
   d) Klicken Sie auf **OK**



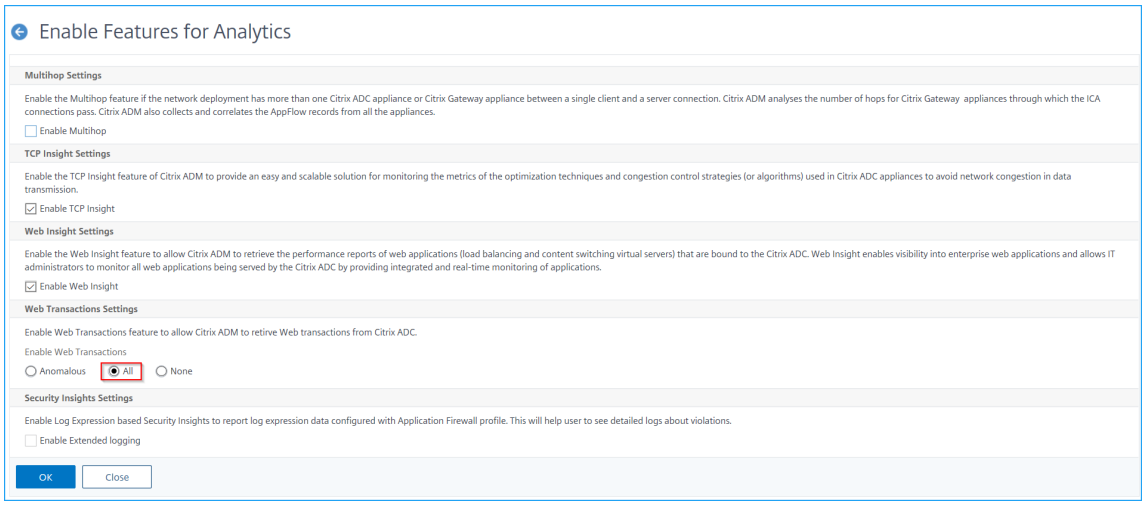
Web-Transaktionseinstellungen aktivieren

1. Navigieren Sie zu **Analytics** > **Einstellungen**.

   Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie auf **Features für Analytics aktivieren**.

3. Wählen Sie unter **Webtransaktionseinstellungen** die Option **Alle** aus.



4. Klicken Sie auf **OK**.

Konfigurieren von Verhaltensüberprüfungs

Citrix ADM ermöglicht es Ihnen, die verhaltensbasierten Verstöße auszuwählen. Bei **übermäßigen Kundenverbindungen**, **Website-Scanning**, **ungewöhnlich hohen Upload-Transaktionen**und Verstößen gegen **ungewöhnlich hohe Downloadtransaktionen** können Sie die Empfindlichkeitsstufe als **Niedrig**, **Mittel**und **Hoch**wählen. Durch das Erstellen eines Profils können Sie entscheiden, wie Citrix ADM die Gesamtzahl der Anomalien für diese Verstöße melden soll.

So konfigurieren Sie diese Einstellung:

1. Navigieren Sie zu **Analytics > Sicherheit > Sicherheitsverletzungen**.
2. Klicken Sie auf das Einstellungssymbol, das neben der Liste der Zeitdauer verfügbar ist.
3. Klicken Sie unter **Verhaltensbasierte Prüfungen**auf **Hinzufügen**.
4. Geben Sie die folgenden Parameter an:
    a) **Verhaltensbasierter Prüfprofilname** — Geben Sie einen Profilnamen Ihrer Wahl an.
    b) Wählen Sie die Option **Aktivieren** aus. Die Standardeinstellung ist 'Auf Remotesitzung nur im Vollbildmodus zugreifen'.
    c) **Wählen Sie unter "Anwendung**auswählen" die Anwendungen aus, für die Sie das Profil anwenden möchten.
    d) **Wählen Sie unter Verhaltensbasierte Prüfungen**auswählen die Option **Niedrig**, **Mittel**oder **Hoch** aus, um die Sensitivitätsstufe für die genannten Verstöße zu definieren.

    > **Hinweis**
    >
    > Standardmäßig sind alle anderen verhaltensbasierten Verletzungen ebenfalls aktiviert. Wenn Sie einen Verstoß deaktivieren, erkennt Citrix ADM Anomalien für diese Verstöße nur basierend auf einer normalen Vorhersage.

    e) Klicken Sie auf **Erstellen**.

WAF Lern-Engine

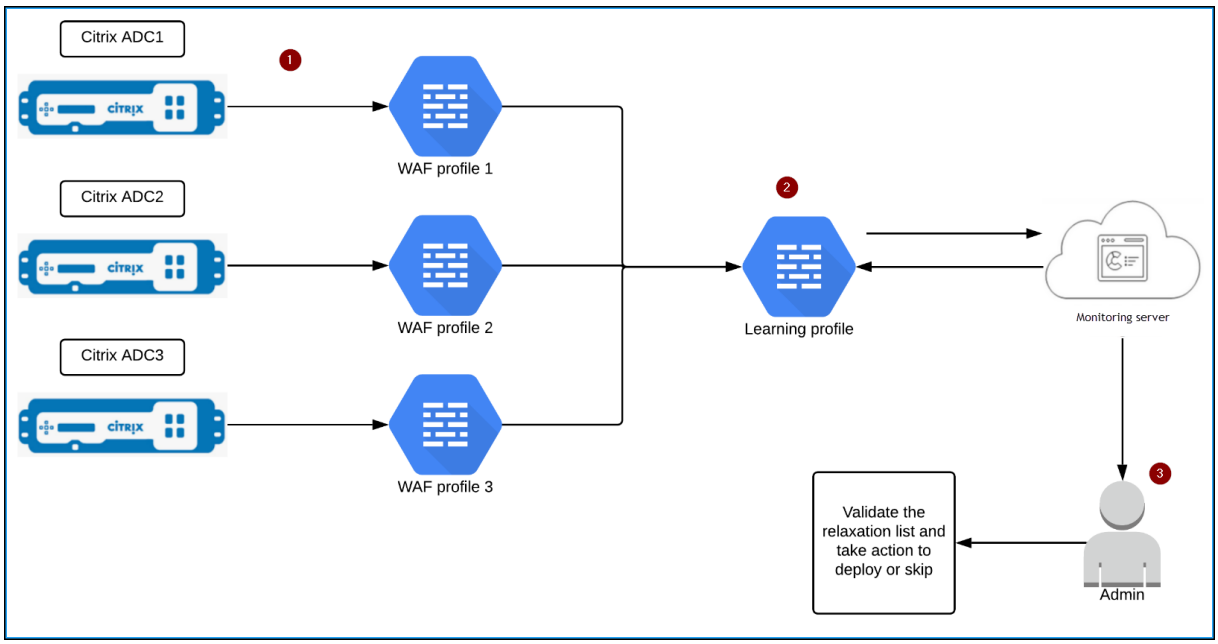
April 28, 2021

Citrix Web App Firewall (WAF) schützt Ihre Webanwendungen vor böswilligen Angriffen wie SQL-Injection und Cross-Site Scripting. Um Datenschutzverletzungen vorzubeugen und den richtigen Sicherheitsschutz zu bieten, müssen Sie Ihren Datenverkehr auf Bedrohungen und umsetzbare Echtzeitdaten bei Angriffen überwachen. Manchmal sind die gemeldeten Angriffe möglicherweise falsch positiv, und diese müssen als Ausnahme bereitgestellt werden.

Die Learning Engine in Citrix ADM ist ein sich wiederholender Pattern-Filter, mit dem WAF das Verhalten (die normalen Aktivitäten) Ihrer Webanwendungen erlernen kann. Basierend auf der Überwachung generiert die Engine eine Liste der vorgeschlagenen Regeln oder Ausnahmen für jede Sicherheitsprüfung, die auf den HTTP-Datenverkehr angewendet wird.

Es ist viel einfacher, Relaxationsregeln mit der Learning-Engine bereitzustellen, als sie manuell bei Bedarf Relaxationen bereitzustellen.

In der folgenden Abbildung werden die allgemeinen Informationen zur Funktionsweise des WAF-Lernens in Citrix ADM erläutert:



1 — Citrix ADC-Instanzen mit seinen WAF-Profilen

2 : Konfigurieren Sie ein Lernprofil in Citrix ADM, fügen Sie die WAF-Profile hinzu und wählen Sie, ob die Relaxationsregeln automatisch bereitgestellt oder manuell bereitgestellt werden sollen.

3 — Der Administrator kann die Relaxationsregeln in Citrix ADM validieren und beschließen, die Bereitstellung oder

Erste Schritte

Um die Lernfunktion bereitzustellen, müssen Sie zunächst ein Web App Firewall Profil (Satz von Sicherheitseinstellungen) auf der Citrix ADC Appliance konfigurieren. Weitere Informationen finden Sie unter Erstellen von Web App Firewall Profilen.

Citrix ADM generiert eine Liste von Ausnahmen (Relaxationen) für jede Sicherheitsprüfung. Als Administrator können Sie die Liste der Ausnahmen in Citrix ADM überprüfen und entscheiden, ob Sie sie bereitstellen oder überspringen möchten.

Mit der WAF-Lernfunktion in Citrix ADM können Sie:

- Konfigurieren Sie ein Lernprofil mit den folgenden Sicherheitsprüfungen
  - Start-URL
  - Konsistenz von Cookies
  - Kreditkarte

    > **Hinweis**
    >
    > Für die Kreditkartensicherheitsprüfung müssen Sie die `doSecureCreditCardLogging` in der Citrix ADC-Instanz konfigurieren und sicherstellen, dass die Einstellung **OFF**ist.

  - Inhaltstyp
  - Konsistenz von Formularfeldern
  - Feld-Formate
  - CSRF-Formular-Tagging
  - HTML Cross-Site-Scripting

    > **Hinweis**
    >
    > Die Standortbeschränkung für Cross-Site-Skripte ist nur FormField.

  - HTML SQL Injection

    > **Hinweis**
    >
    > Für die HTML-SQL-Injection-Prüfung müssen Sie `set -sqlinjectionTransformSpecialChars ON`und `set -sqlinjectiontype sqlspclcharorkeywords`in der Citrix ADC-Instanz konfigurieren.

- Überprüfen Sie die Relaxationsregeln in Citrix ADM und entscheiden Sie, die erforderlichen Maßnahmen zu ergreifen (Bereitstellen oder Überspringen)
- Erhalten Sie die Benachrichtigungen per E-Mail, Slack und ServiceNow
- Verwenden Sie die Seite **Aktionsübersicht**, um Details zur Entspannung anzuzeigen

So verwenden Sie das WAF-Lernen in Citrix ADM:

1. Konfigurieren des Lernprofils
2. Siehe die Entspannungsregeln
3. Verwenden Sie die Seite Zusammenfassung der WAF-Lernaktion

TCP Insight

April 28, 2021

Die TCP Insight-Funktion von Citrix Application Delivery Management (ADM) bietet eine einfache und skalierbare Lösung zur Überwachung der Metriken der Optimierungstechniken und der Engpasskontrollstrategien (oder Algorithmen), die in Citrix ADC Appliances verwendet werden, um Netzwerküberlastung bei der Datenübertragung zu vermeiden. Diese Funktion verwendet die Funktion TCP Speed Report, die die Leistung des Downloads oder Uploads von TCP-Dateien mit und ohne TCP-Optimierung misst.

Sie können die wichtigsten Transport-Layer-Metriken anzeigen, wie Datenvolumen, Durchsatz und Geschwindigkeit, und diese Informationen verwenden, um das von den Citrix ADC-Instanzen bereitete Verkehrsvolumen zu messen und die Vorteile der TCP-Optimierung zu überprüfen. Für die oben genannten Metriken werden Aufschlüsselungen nach Stream-Richtung (von Client zu Citrix ADC und Citrix ADC zum Ursprungsserver), TCP-Port und virtuellem LAN bereitgestellt.

Voraussetzungen

Bevor Sie mit der Konfiguration des TCP Insight-Features beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Die Citrix ADC-Instanzen werden auf Softwareversion 11.1 Build 51.21 oder höher ausgeführt.
- Sie haben Citrix ADM installiert, die auf Softwareversion 11.1 Build 51.21 oder höher ausgeführt wird.
- Alle für eine Anwendung konfigurierten virtuellen Server sind für die Verwaltung und Überwachung auf Citrix ADM lizenziert. Hinweise zur Citrix ADM -Lizenzierung finden Sie unterLizenzierung.

Hardwareanforderungen für Citrix ADM:

Komponente	Voraussetzung
RAM	8 GB
Virtuelle CPU	4
	Hinweis Citrix empfiehlt, 8 CPUs für eine bessere Leistung zu verwenden.
Stauraum	120 GB
	Hinweis Citrix empfiehlt, 500 GB für eine bessere Leistung zu verwenden.

TCP Insight aktivieren

Bevor Sie die TCP Insight-Metriken anzeigen können, müssen Sie die Funktion in Citrix ADM aktivieren.

So aktivieren Sie TCP Insight:

1. Geben Sie in einem Webbrowser die IP-Adresse der virtuellen Citrix ADM Appliance ein (z. B.`http://192.168.100.1`).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **Analytics** > **Einstellungen**, und klicken Sie auf **Features für Analytics aktivieren**.
4. Wählen Sie auf der Seite **Features für Analysen aktivieren** die Option **TCP Insight aktivieren** aus.
5. Klicken Sie im Bestätigungsfenster auf **OK**.

Anzeigen der TCP Insight-Metriken in Citrix ADM

Nachdem Sie TCP Insight in Citrix ADM aktiviert haben, können Sie wichtige Transportschichtinformationen wie Verkehrsmodus (Internet- oder Mobildaten), Datenvolumen, Durchsatz, Schnittstellen, Ports, durchschnittliche Upload-Geschwindigkeit und durchschnittliche Download-Geschwindigkeit anzeigen.

So zeigen Sie TCP Insight-Metriken in Citrix ADM an:

Navigieren Sie zu **Analytics** > **TCP Insight**.

Sie können den Mauszeiger auf die Balkendiagramme bewegen, um das Datenvolumen der entsprechenden Transporttechniken anzuzeigen. Sie können auch das Datenvolumen und andere Metriken in der Tabelle unterhalb des Diagramms anzeigen.

> **Hinweis** Sie können die im Diagramm angezeigten Metriken mithilfe des Einstellungssymbols in der Tabelle anpassen. Sie können auch den Zeitraum auswählen, auf den sich die Metriken beziehen, und den Zeitschieberegler verwenden, um den Zeitraum anzupassen.

Sie können Metriken für Schnittstellen, Ports und Bitraten auch anzeigen, indem Sie in der **TCP-Insight-Liste** auswählen.

Anwendungsfälle

Die folgenden Anwendungsfälle veranschaulichen einige der Möglichkeiten zur Verwendung von TCP Insight auf Citrix ADC Appliances:

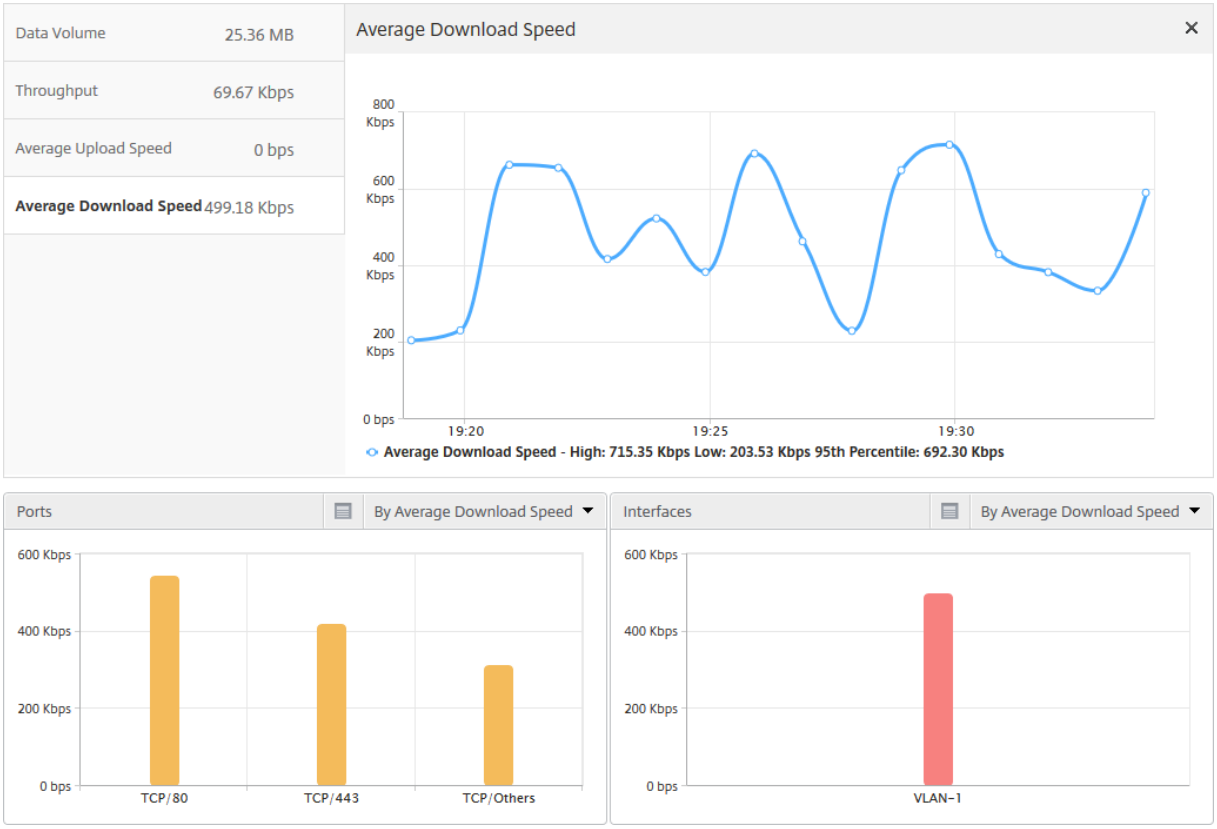
- Bewertung der Vorteile der TCP-Optimierung

- TCP-Parameter optimieren
- Messung der Auswirkungen der TCP-Optimierung auf das Verkehrsvolumen

Bewertung der Vorteile der TCP-Optimierung

Wie viel nützt Citrix ADC TCP-Optimierung tatsächlich einem mobilen (Radio) oder Unternehmensnetzwerk (Internet)? Sie können die Geschwindigkeit der Datenübertragungen über TCP anzeigen und unoptimierte und optimierte Leistung vergleichen. Diese Messungen werden separat für die Download- und Upload-Richtungen (immer auf der Radio/Client-Seite) und für verschiedene Zielports HTTP (80) und HTTPS (443) angezeigt.
Indem Sie die TCP Insight-Metriken untersuchen, können Sie die Geschwindigkeitsverbesserung quantifizieren, die durch die Optimierung von TCP-Flows erzielt wird.

Um eine Zusammenfassung dieser Parameter anzuzeigen, melden Sie sich bei Citrix ADM an, und klicken Sie auf die Registerkarte **TCP Insight**. Klicken Sie dann auf **Seiten**, und wählen Sie **Internet** oder **Radio** aus dem Balkendiagramm oder der Tabelle unterhalb des Diagramms aus.

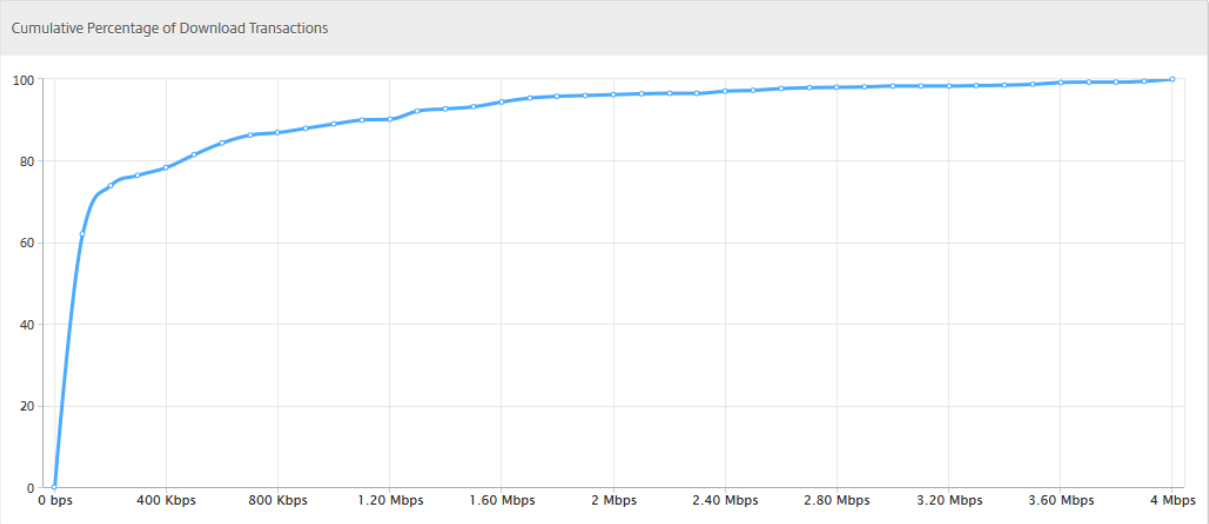


TCP-Parameter optimieren

Die Verwendung verschiedener TCP-Profile kann zu unterschiedlichen Ausgängen für denselben Datenverkehr führen. In solchen Situationen können Sie die Geschwindigkeitsmessungen von

Perioden anzeigen und vergleichen, in denen Citrix ADC verschiedene TCP-Optimierungsprofile ausführt. Sie können die Ergebnisse verwenden, um TCP-Parameter für eine schnellere Übertragung zu optimieren und ein TCP-Profil zu entwickeln, das die Benutzererfahrung in einem bestimmten Kundennetzwerk maximiert.

Melden Sie sich bei Citrix ADM an, um die Berichte anzuzeigen. Klicken Sie dann auf der Registerkarte **TCP Insight** auf **Bitrate**, und wählen Sie die gewünschte Bitrate aus dem Balkendiagramm oder der Tabelle unterhalb des Diagramms aus.

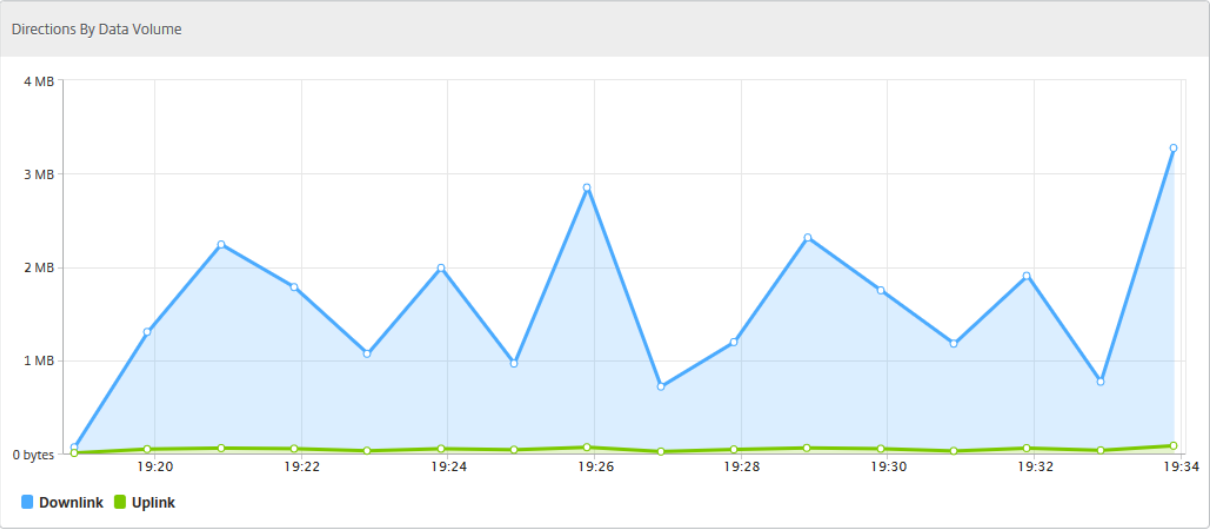


Messung der Auswirkungen der TCP-Optimierung auf das Verkehrsvolumen

Messungen von IP-Layer Data Volume/Durchsatz, die von einer Citrix ADC-Instanz verarbeitet werden, können zwischen verschiedenen Zeiträumen verglichen werden, um die Auswirkungen der TCP-Optimierung auf den Verbrauch von Teilnehmerdaten zu bewerten. Die Messungen können separat für jede Seite des Netzwerks (Radio-Seite vs. Internet-Seite), für verschiedene Verkehrssegmente (durch unterschiedliche Schnittstellen oder VLANs abgegrenzt), für jede Richtung (Downlink vs. Uplink) und für verschiedene Zielports (HTTP und HTTPS) angewendet werden. Der Vergleich kann verwendet werden, um zu bestätigen, dass die TCP-Optimierung Abonnenten dazu ermutigt, mehr Daten zu verbrauchen.

Um eine Zusammenfassung der Messwerte zu erhalten, melden Sie sich bei Citrix ADM an, klicken Sie auf der Registerkarte **TCP Insight** auf **Seiten**, und wählen Sie dann **Internet** oder **Radio** aus dem Balkendiagramm oder der Tabelle unterhalb des Diagramms aus.

Sie können auch einen anderen Zeitrahmen aus der Zeitliste auswählen. Sie können den Zeitrahmen mithilfe des Zeitrahmen-Schiebereglers anpassen.



WAN Insight

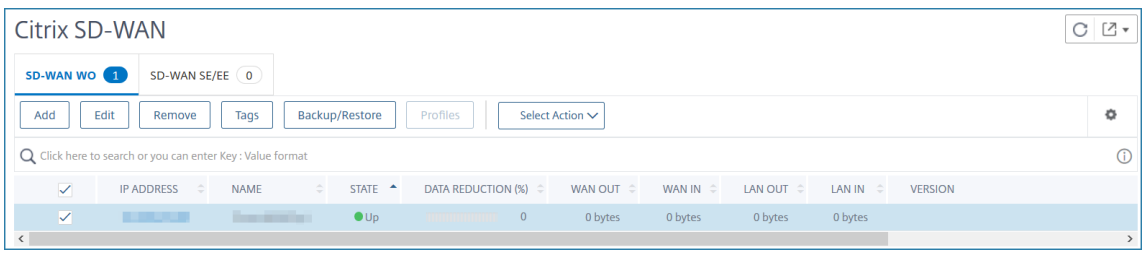
April 28, 2021

Die Citrix SD-WAN WAN Optimization (WO) Appliances optimieren die Bereitstellung einer großen Anzahl von Anwendungen über das WAN, indem sie die Effizienz des Datenflusses über das Netzwerk zwischen dem Rechenzentrum und den Zweigstellen verbessern. WAN Insight Analytics ermöglichen es Administratoren, den beschleunigten und nicht beschleunigten WAN-Datenverkehr, der zwischen dem Rechenzentrum und den WAN-Optimierungsgeräten des Zweigs fließt, einfach zu überwachen WAN Insight bietet Einblick in Clients, Anwendungen und Zweigstellen im Netzwerk, um Netzwerkprobleme effektiv zu beheben. Live-Berichte und historische Berichte ermöglichen es Ihnen, Probleme proaktiv zu lösen, falls vorhanden

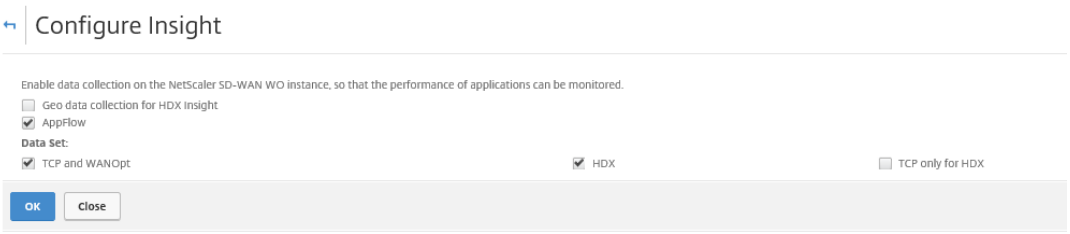
Durch die Aktivierung von Analysen auf der WAN-Optimierungs-Appliance für Rechenzentren kann Citrix Application Delivery Management (ADM) Daten sammeln und Berichte und Statistiken für das Rechenzentrum und die WAN-Optimierungs-Appliances der Zweigstelle bereitstellen.

So aktivieren Sie Analysen auf der WAN-Optimierungs-Appliance:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix SD-WAN**, und wählen Sie die SD-WAN-WO-Instanz aus.



2. **Wählen Sie in der Liste Aktion** auswählen die Option **Insight aktivieren** aus.
3. Wählen Sie die folgenden Parameter nach Bedarf aus:
    - **Geo-Datenerfassung für HDX Insight**: Freigabe der Client-IP-Adresse mit der Google Geo API.
    - **AppFlow**: Beginnt das Sammeln von Daten aus WAN-Optimierungsinstanzen.
    - **TCP und WanOpt**: Bietet TCP- und **WanOpt Insight-Berichte** .
    - **HDX**: Bietet HDX Insight Berichte.
    - **TCP nur für HDX**: Bietet TCP nur für HDX Insight Berichte.



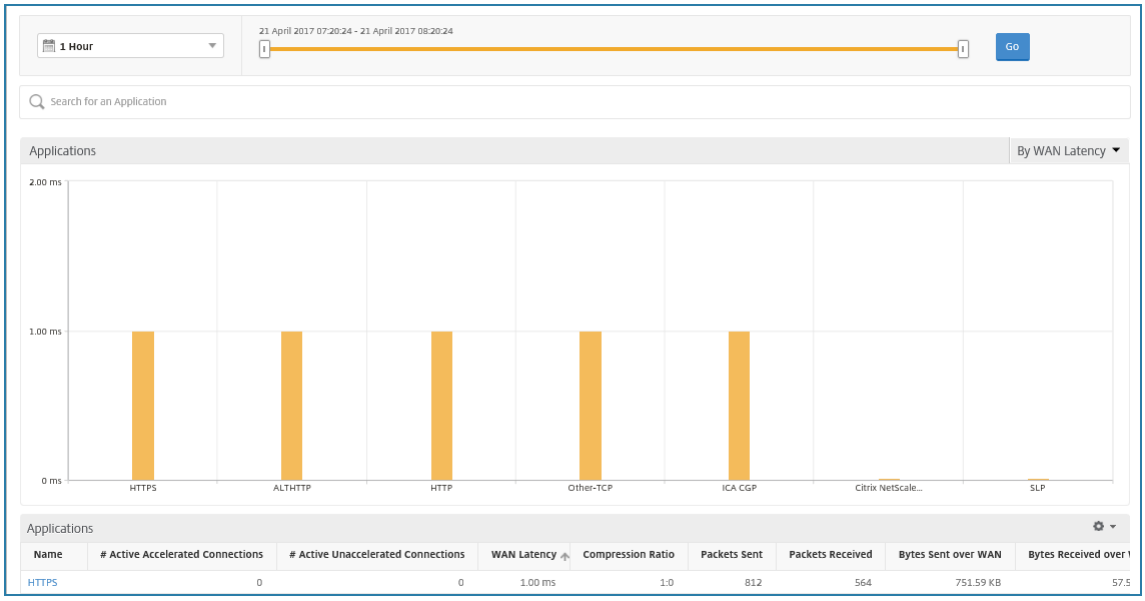
4. Klicken Sie auf **OK**.

Um WAN-Insight-Berichte anzuzeigen, navigieren Sie zu **Analytics** > **WAN Insight**.

> **Hinweis**
>
> Die Option WAN Insight ist erst sichtbar, nachdem Sie Citrix ADM eine SD-WAN-WO-Instanz hinzugefügt haben.

Sie können die folgenden Berichte anzeigen:

- **Anwendungen** - Zeigt die Nutzungs- und Leistungsstatistiken aller Anwendungen für die ausgewählte Dauer an.
- **Zweige** - Zeigt die Nutzungs- und Leistungsstatistiken aller Geräte für WAN-Optimierungszweige an.
- **Clients** - Zeigt die Nutzungs- und Leistungsstatistiken aller Clients an, die auf die WAN-Optimierungs-Appliances in jedem Zweig zugreifen.



Die folgenden Metriken werden angezeigt:

Metrik	Beschreibung
Aktive beschleunigte Verbindungen	Anzahl der aktiven WAN-Verbindungen, die beschleunigt werden.
Aktive nicht beschleunigte Verbindungen	Anzahl der aktiven WAN-Verbindungen, die nicht beschleunigt werden.
WAN-Latenz	Verzögerung in Millisekunden, die der Benutzer während der Interaktion mit einer Anwendung auftritt.
Komprimierungsverhältnis	Verhältnis der Datenkomprimierung zwischen der Zweigstelle und den Appliances des Rechenzentrums für die ausgewählte Dauer.
Gesendete Pakete	Anzahl der Pakete, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer über das Netzwerk gesendet hat.
Empfangene Pakete	Anzahl der Pakete, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer vom Netzwerk empfangen hat.

Metrik	Beschreibung
Über WAN gesendete Bytes	Anzahl der Bytes, die die Citrix WAN-Optimierungs-Appliance für die ausgewählte Dauer über das WAN gesendet hat.
Über WAN empfangene Bytes	Anzahl der Bytes, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer vom WAN empfangen hat.
LAN RTO	Anzahl der Zeitüberschreitungen für die WAN-Optimierungs-Appliance bei der erneuten Übertragung an das LAN für die ausgewählte Dauer.
WAN RTO	Anzahl der Zeitüberschreitungen für die WAN-Optimierungs-Appliance bei der erneuten Übertragung an das WAN für die ausgewählte Dauer.
Neu übertragene Pakete (LAN)	Anzahl der Pakete, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer erneut an das LAN-Netzwerk übertragen hat.
Neu übertragene Pakete (WAN)	Anzahl der Pakete, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer erneut an das WAN-Netzwerk übertragen hat.

Video Insight

April 28, 2021

Die Video Insight-Funktion bietet eine einfache und skalierbare Lösung zur Überwachung der Metriken der Videooptimierungstechniken, die von Citrix ADC Appliances verwendet werden, um die Kundenerfahrung und die betriebliche Effizienz zu verbessern, und bietet folgende Vorteile:

- Verwalten Sie das Netzwerk während der Überlastung in Spitzenzeiten.
- Verbessern Sie die Konsistenz der Videowiedergabe und reduzieren Sie die Videoabspielung.
- Aktivieren Sie neue Videodienstangebote (z. B. Binge-on-Videodienste).

- Ermöglichen Sie Kunden, die beste nachhaltige Videoqualität auszuwählen.
- Bieten Sie eine konsistente Benutzererfahrung für den Abonnenten.

Bei der Optimierung des Videoverkehrs verwendet die Citrix ADC Appliance einen speziellen Mechanismus, um die Videobitrate dynamisch zu beschleunigen, und eine Zufallsabtastung, um die Einsparungen durch die Optimierungstechnik abzuschätzen. Weitere Informationen zur Citrix ADC Videooptimierungsfunktion finden Sie unterVideooptimierung. Wenn Sie die Citrix ADC Appliance in Citrix Application Delivery Management (ADM) integrieren, werden wichtige Informationen aus den Videodaten gesammelt, die durch die Citrix ADC Appliance fließt. Sie können diese Informationen verwenden, um die optimierte und nicht optimierte Leistung des ABR-Videoverkehrs zu vergleichen, die Einsparungen durch Optimierung zu ermitteln und so weiter.

> **Hinweis**
>
> Die Statistiken der nicht optimierten Sitzungen in Citrix ADM entsprechen den Sitzungen, die Sie in der Citrix ADC Appliance ausgewählt haben. Weitere Hinweise zur Random Sampling finden Sie unterVideooptimierung.

Video Insight in Citrix ADM stellt Metriken für die folgenden Arten von Videoverkehr bereit:

- Progressive Download (PD) Videos über HTTP
- ABR-Videos über HTTP
- ABR-Videos über HTTPS
- YouTube ABR Videos über QUIC

Konfigurieren von Video Insight

> **Hinweis**
>
> Video Insight wird auf Citrix ADC-Instanzen mit Citrix ADC Premium-Lizenz unterstützt. Die Citrix ADC Premium-Lizenz wird für Citrix ADC Telco-Plattformen (VPX T1000 und VPX-T) unterstützt.

Um Video Insight auf einer Citrix ADC-Instanz zu konfigurieren, aktivieren Sie zunächst die AppFlow Funktion, konfigurieren Sie einen AppFlow-Collector, eine Aktion und eine Richtlinie und binden Sie die Richtlinie global. Wenn Sie den Collector konfigurieren, müssen Sie die IP-Adresse des Citrix ADM -Servers angeben, auf dem die Berichte überwacht werden sollen.

Um Videoinformationen für eine Citrix ADC-Instanz zu konfigurieren, führen Sie die folgenden Befehle aus, um ein AppFlow Profil und eine Richtlinie zu konfigurieren und die AppFlow-Richtlinie global zu binden.

add appflow collector <name> **-IPAddress** <ipaddress> **-port** <port_number> **-Transport** logstream

set appflow param -**videoInsight** ENABLED

add appflow action <name> **-collectors** <string> **-videoAnalytics** ENABLED

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

enable ns mode ulfd

aktiviere Funktion AppFlow

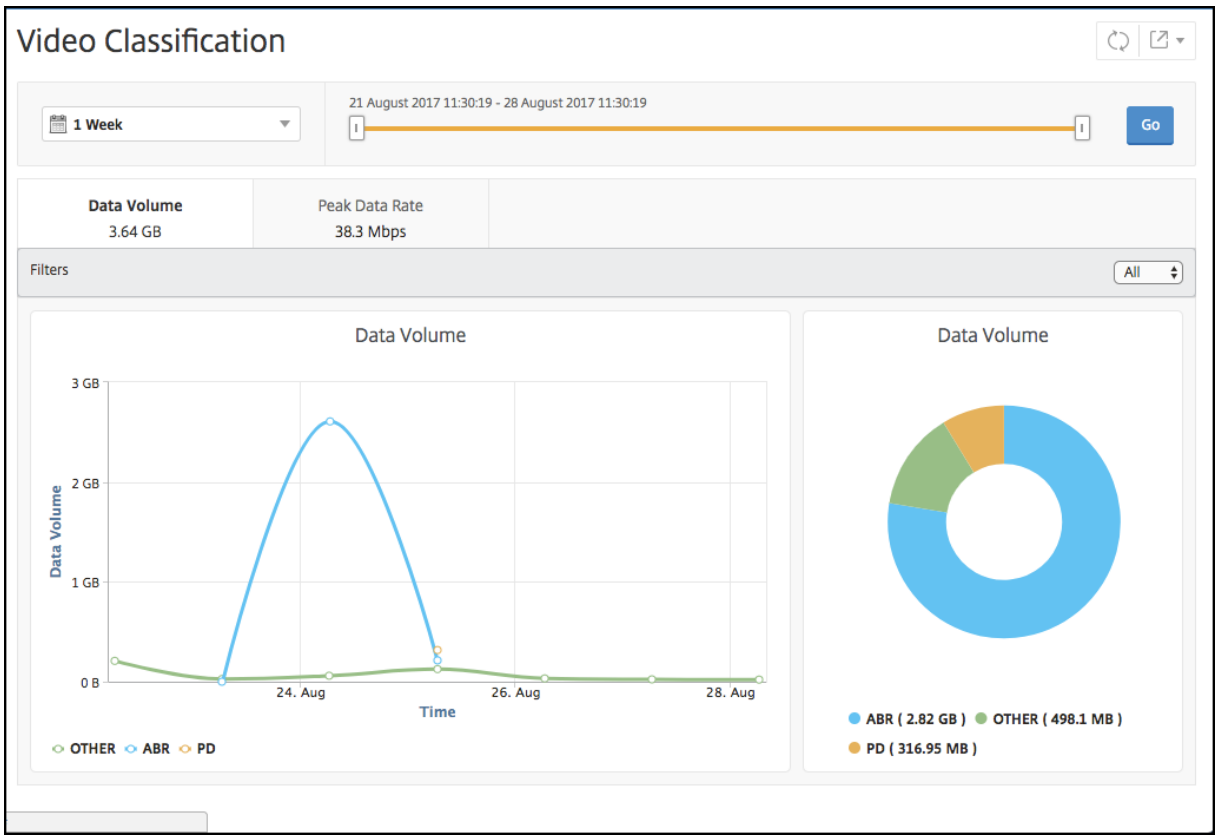
Beispiel

```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
   Transport logstream
set appflow param -videoInsight ENABLED
add appflow action act1 -collectors col1 -videoAnalytics ENABLED
add appflow policy appol true act1
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
<!--NeedCopy-->
```

Anzeigen der Video Insight-Metriken in Citrix ADM

Nachdem Sie Video Insight in Citrix ADM aktiviert haben, können Sie Video-Optimierungsmetriken wie Videoklassifizierung, Datenvolumen, Spitzendatenrate und ABR-Videowiedergabe anzeigen. Diese Metriken helfen Ihnen dabei, Ihr Netzwerk zu analysieren und die Videos zu optimieren, um die Nutzererfahrung, die betriebliche Effizienz und andere Leistungskriterien zu verbessern.

Um die Video Insight-Metriken in Citrix ADM anzuzeigen, navigieren Sie zu **Analytics > Video Insight**.



Hinweis

Die Werte, die von der Legende **OTHER** in den Diagrammen bereitgestellt werden, stellen die Nicht-ABR- und Nicht-PD-Daten im Videoverkehr dar, abhängig vom ausgewählten Filter:

- **Alle** — Summe der Nicht-ABR-Daten (HTTP, HTTPS und QUIC) und Nicht-PD (HTTP) im Videoverkehr.
- **HTTP** — Summe der Nicht-ABR- und Nicht-PD-Daten im Videoverkehr.
- **HTTPS** — Summe der Nicht-ABR-Videodaten im Videoverkehr.
- **QUIC** — Summe der Nicht-ABR-Videodaten im Videoverkehr.

Anzeigen der Netzwerkeffizienz

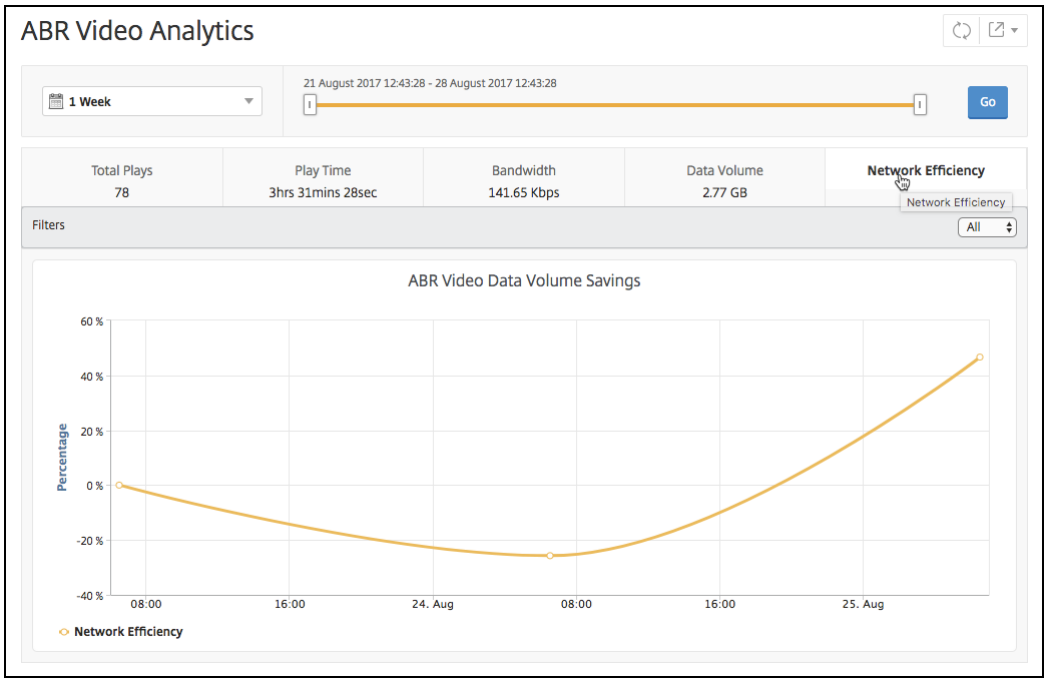
April 28, 2021

Für einen bestimmten Zeitraum stellt Citrix Application Delivery Management (ADM) ein Diagramm bereit, das das Verhältnis von optimierten zu nicht optimierten Videositzungen im Zeitrahmen anzeigt. Es zeigt auch den Prozentsatz der Bandbreite an, die durch die Optimierung gespeichert wurde. Der prozentuale Anteil der gespeicherten Bandbreite wird mit der folgenden Formel berechnet:

Prozentsatz der gesparten Bandbreite = **Durchschnittliches optimiertes ABR-Videodatenvolumen/Durchschn des nicht optimierten ABR-Videodatenvolumens**.

So sehen Sie den Prozentsatz der durch die Optimierung gespeicherten Bandbreite an:

1. Navigieren Sie zu **Analytics > Video Insight**, und klicken Sie auf **ABR Video**.
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.
3. Klicken Sie auf **Los**, und wählen Sie die Registerkarte **Netzwerkeffizienz**.



Vergleichen Sie das Datenvolumen, das von optimierten und nicht optimierten ABR-Videos verwendet wird

April 28, 2021

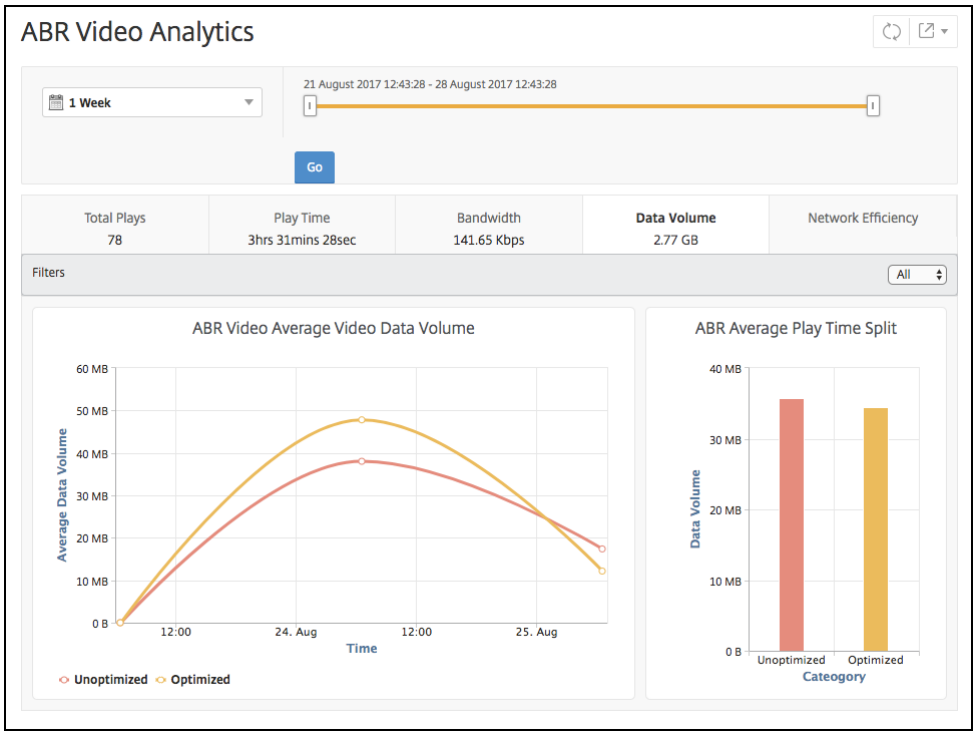
Für einen bestimmten Zeitraum zeigt Citrix Application Delivery Management (ADM) das Datenvolumen an, das von optimierten und nicht optimierten ABR-Videos verwendet wird, sodass Sie die beiden Volumes vergleichen können.

So sehen Sie das Datenvolumen, das von ABR-Videos verwendet wird:

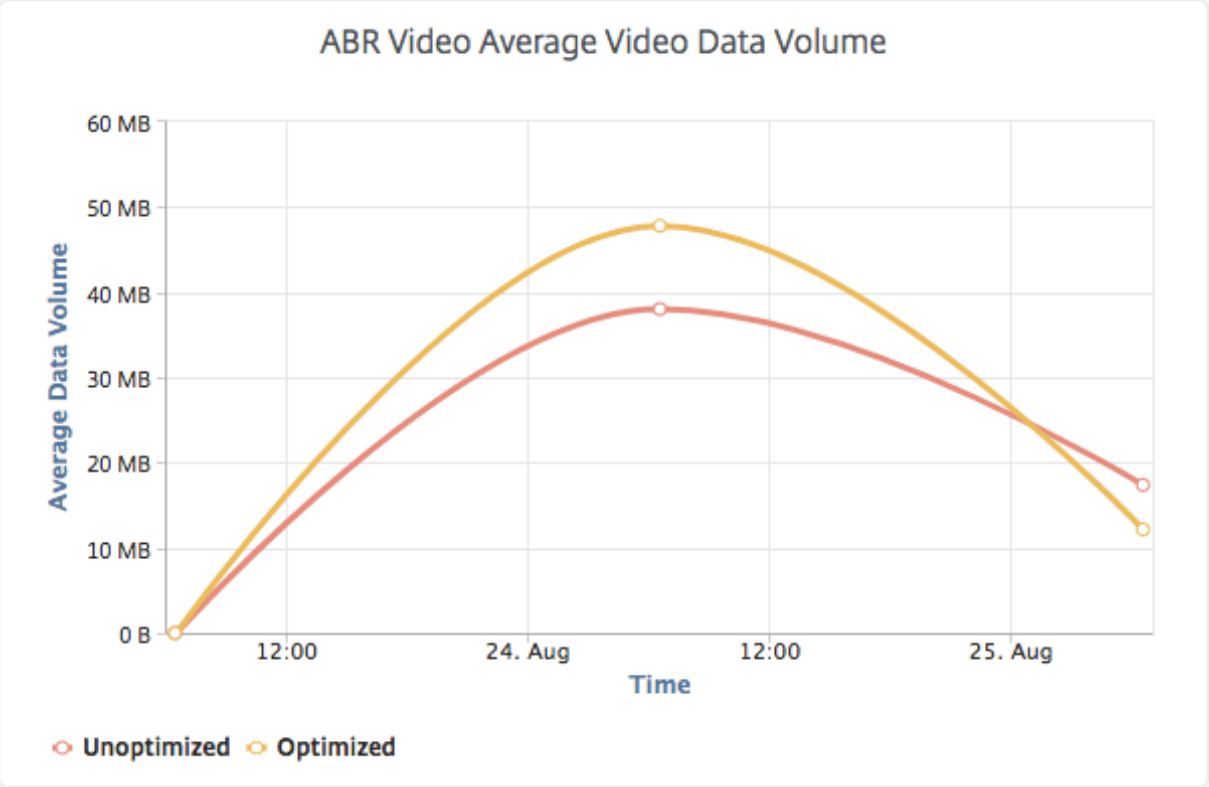
1. Navigieren Sie zu **Analytics > Video Insight**, und klicken Sie auf **ABR Video**.
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.

3. Klicken Sie auf **Los**, und wählen Sie die Registerkarte **Datenvolumen** aus.

Sie können die Liste **Filter** verwenden, um die HTTP-, HTTPS- oder QUIC-ABR-Videos auszuwählen.



Die Registerkarte **Datenvolumen** enthält ein Liniendiagramm und ein Kreisdiagramm, das das durchschnittliche Datenvolumen, das von ABR-Videos verwendet wird, sowie das Datenvolumen, das von optimierten und nicht optimierten ABR-Videos aus Ihrem Netzwerk für den ausgewählten Zeitraum verbraucht wird. Sie können den Mauszeiger auf das Liniendiagramm bewegen, um das durchschnittliche Datenvolumen anzuzeigen, das während eines bestimmten Zeitrahmens verwendet wird:



Zeigen Sie den Typ der gestreamten Videos und das von Ihrem Netzwerk verbrauchte Datenvolumen an

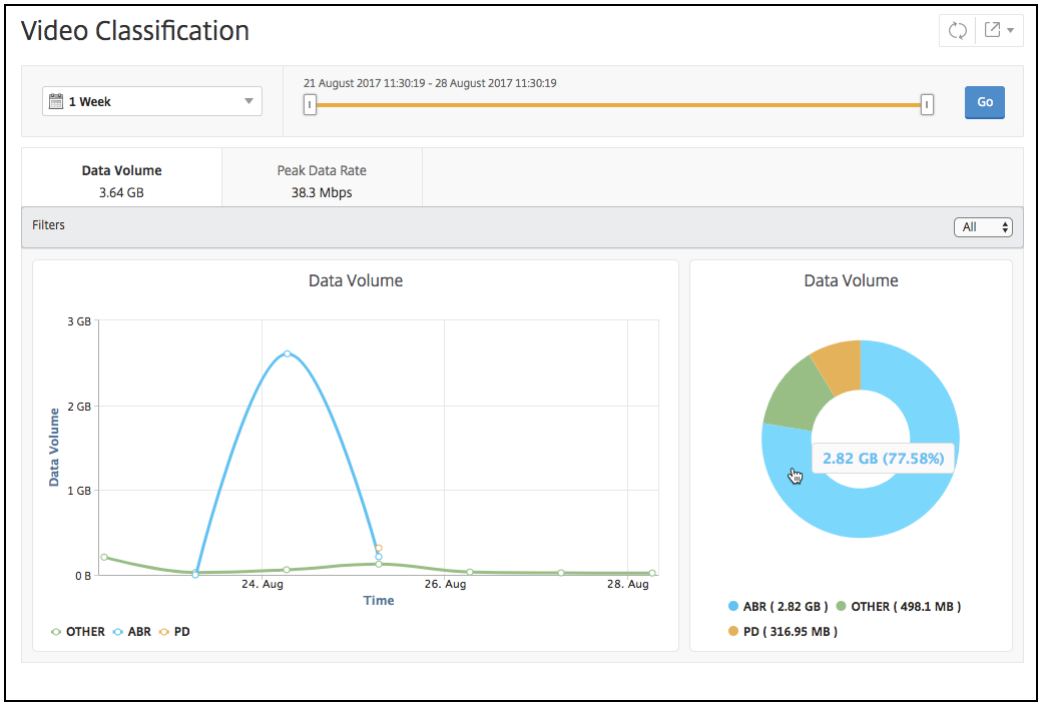
April 28, 2021

Die Citrix ADC Appliance erkennt den verschlüsselten oder unverschlüsselten Videoverkehr in Ihrem Netzwerk und die Art des Video-Streaming (PD oder ABR). Citrix Application Delivery Management (ADM) zeigt diese Metriken und das Datenvolumen an, das vom Videoverkehr für einen definierten Zeitraum belegt wird.

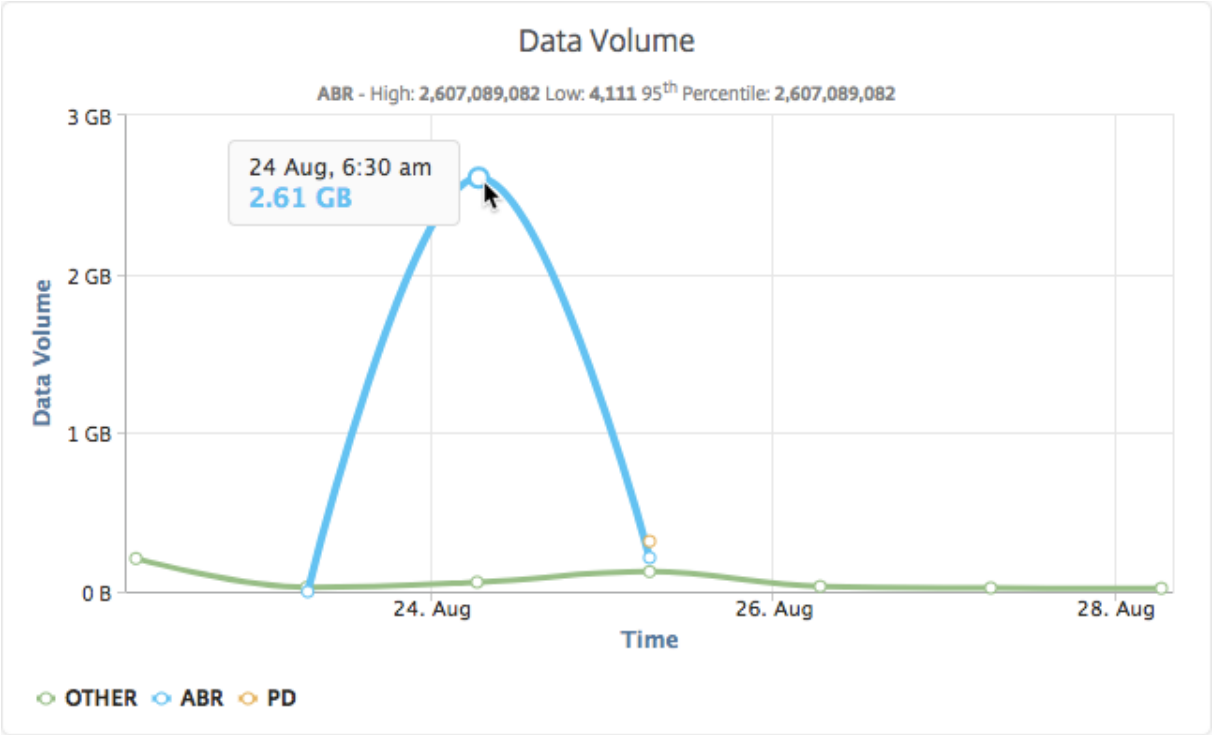
So zeigen Sie die Arten von Videos und das verbrauchte Datenvolumen an:

1. Navigieren Sie zu **Analytics > Video Insight**, und klicken Sie auf **Videoklassifizierung**.
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.
3. Klicken Sie auf **Go**.

Sie können die Liste **Filter** verwenden, um den HTTP-, HTTPS- oder QUIC-Datenverkehr auszuwählen.

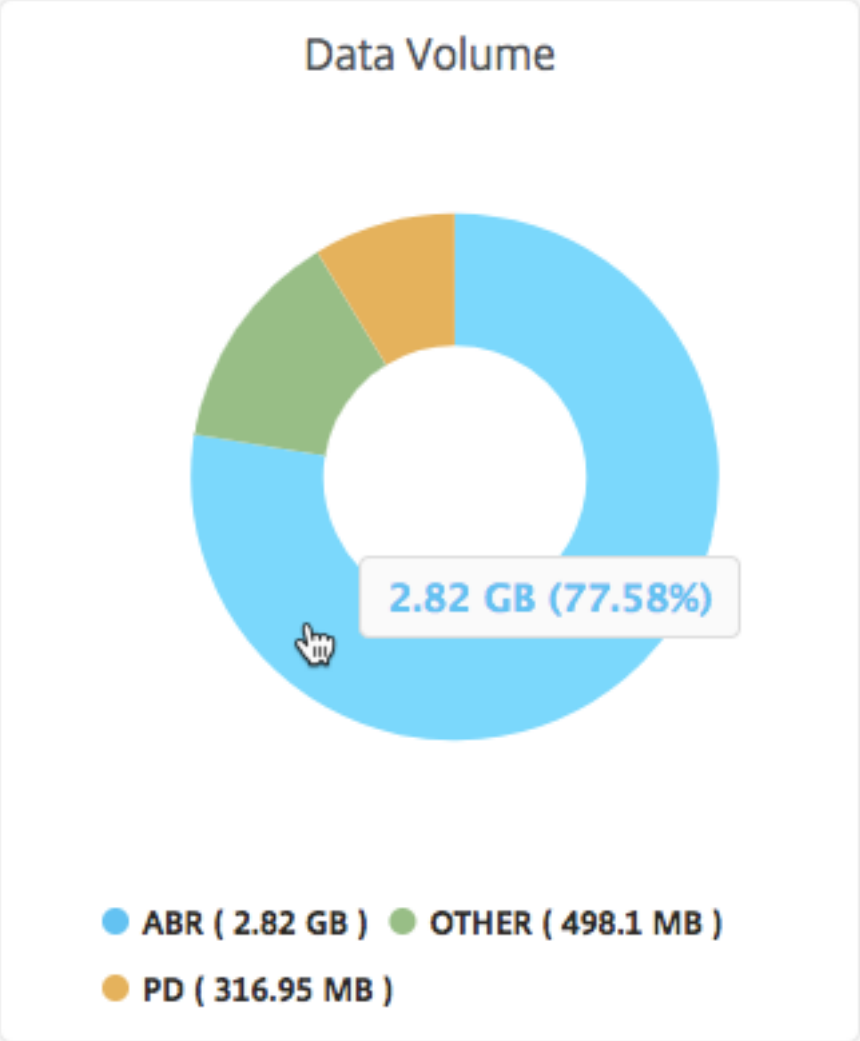


Die Registerkarte **Datenvolumen** enthält ein Liniendiagramm und ein Kreisdiagramm, in dem die Arten des Streamings von Videoverkehr aus Ihrem Netzwerk und das Datenvolumen angezeigt werden, das von Ihrem Netzwerk verbraucht wird. Sie können den Mauszeiger auf das Liniendiagramm bewegen, um die während eines bestimmten Zeitrahmens verbrauchten Daten anzuzeigen:



Außerdem können Sie den Mauszeiger auf das Kreisdiagramm bewegen, um den Prozentsatz des

Datenvolumens anzuzeigen, der von einem bestimmten Typ von Videoverkehr verbraucht wird.



Vergleichen Sie optimierte und unoptimierte Wiedergabezeit von ABR-Videos

April 28, 2021

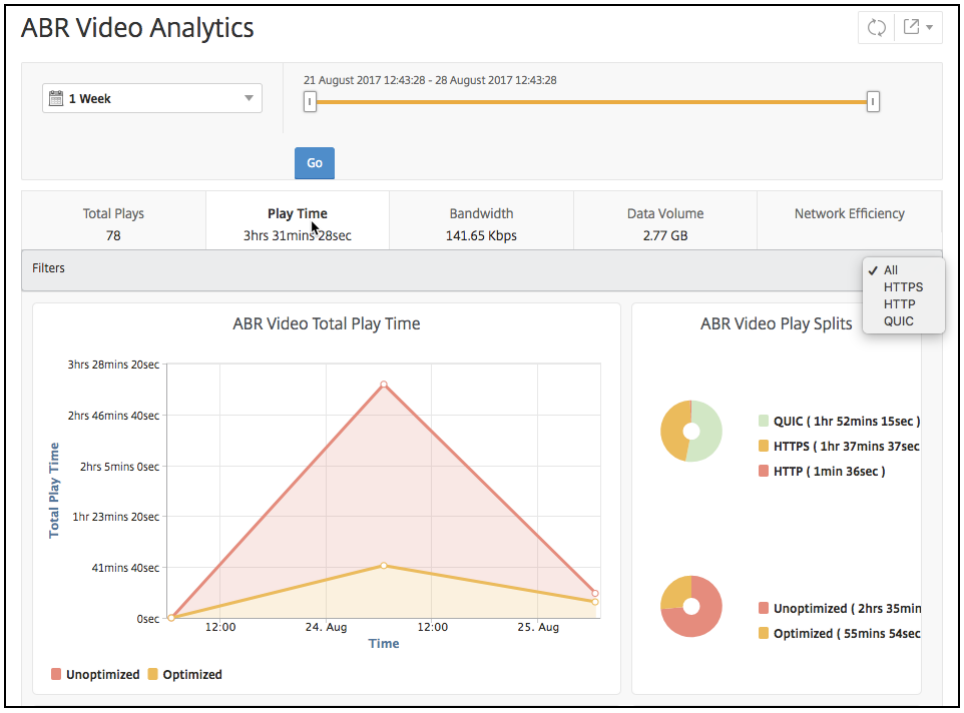
Für einen bestimmten Zeitraum bietet Citrix Application Delivery Management (ADM) die Wiedergabezeit von ABR-Videos und ermöglicht Ihnen außerdem, die Wiedergabezeit optimierter und nicht optimierter ABR-Videos in Ihrem Netzwerk zu vergleichen.

So zeigen Sie die Spielzeit an:

1. Navigieren Sie zu **Analytics > Video Insight**, und klicken Sie auf **ABR Video**.

2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.
3. Klicken Sie auf **Los** und wählen Sie die Registerkarte **Wiedergabezeit** aus.

   Sie können die Liste **Filter** verwenden, um die HTTP-, HTTPS- oder QUIC-ABR-Videos auszuwählen.



Für den ausgewählten Zeitraum enthält die Registerkarte **Wiedergabezeit** ein Liniendiagramm und ein Kreisdiagramm, in dem Folgendes beschrieben wird:

- Gesamte Wiedergabezeit von ABR-Videos aus Ihrem Netzwerk
- Gesamtspielzeit optimierter und unoptimierter Abspielzeiten von ABR-Videos aus Ihrem Netzwerk für den ausgewählten Zeitraum
- Gesamtspielzeit verschlüsselter und unverschlüsselter ABR-Videos
- Durchschnittliche Wiedergabezeit von ABR-Videos
- Durchschnittliche Wiedergabezeit optimierter und nicht optimierter Abspielzeiten von ABR-Videos
- Durchschnittliche Wiedergabezeit verschlüsselter und unverschlüsselter ABR-Videos
- Wiedergabe der Zeitverteilung zwischen optimierten und nicht optimierten ABR-Videos

Vergleich des Bandbreitenverbrauchs optimierter und nicht optimierter ABR-Videos

April 28, 2021

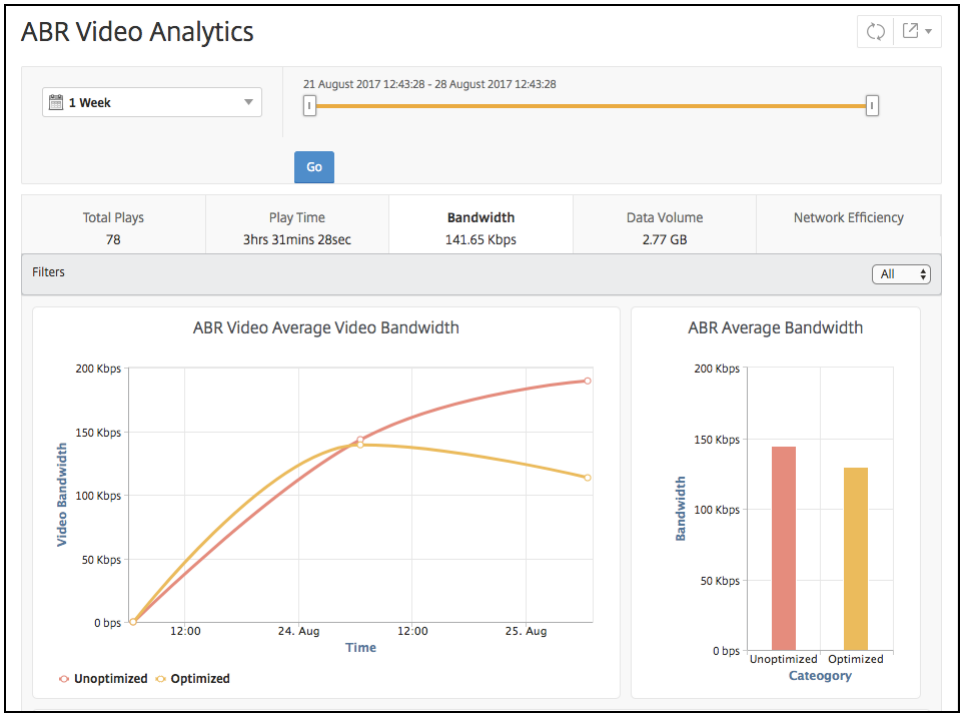
Für einen bestimmten Zeitraum bietet Citrix Application Delivery Management (ADM) die Bandbreite, die von optimierten und nicht optimierten ABR-Videos verbraucht wird, und ermöglicht es Ihnen auch, die Bandbreite zu vergleichen, die von optimierten und nicht optimierten ABR-Videos in Ihrem Netzwerk verbraucht wird, basierend auf:

- Spielzeit
- Datenvolume

So zeigen Sie den Bandbreitenverbrauch an:

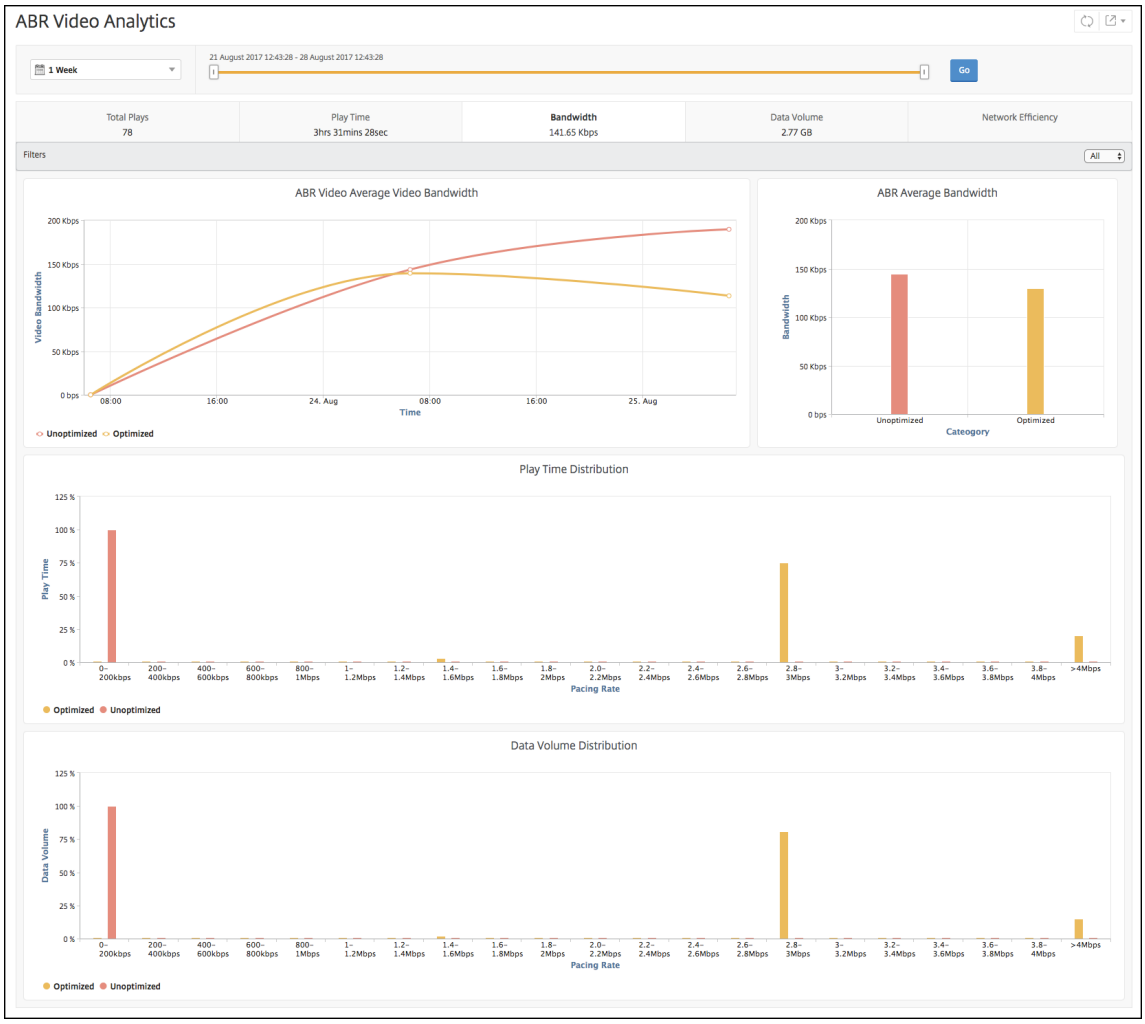
1. Navigieren Sie zu **Analytics > Video Insight**, und klicken Sie auf **ABR Video Analytics**.
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.
3. Klicken Sie auf **Los** und wählen Sie die Registerkarte **Bandbreite** aus.

   Sie können die Liste **Filter** verwenden, um die HTTP-, HTTPS- oder QUIC-ABR-Videos auszuwählen.



Für den ausgewählten Zeitraum enthält die Registerkarte **Bandbreite** ein Liniendiagramm und ein Kreisdiagramm, in dem Folgendes beschrieben wird:

- Durchschnittliche Bandbreite, die von optimierten und nicht optimierten ABR-Videos verbraucht wird.
- Bandbreitenverbrauch basierend auf der Wiedergabezeitverteilung zwischen optimierten und nicht optimierten ABR-Videos.
- Bandbreitenverbrauch basierend auf dem Datenvolumen, das zwischen optimierten und nicht optimierten ABR-Videos verteilt wird.



Vergleichen Sie die optimierte und nicht optimierte Anzahl von Abspielen von ABR-Videos

April 28, 2021

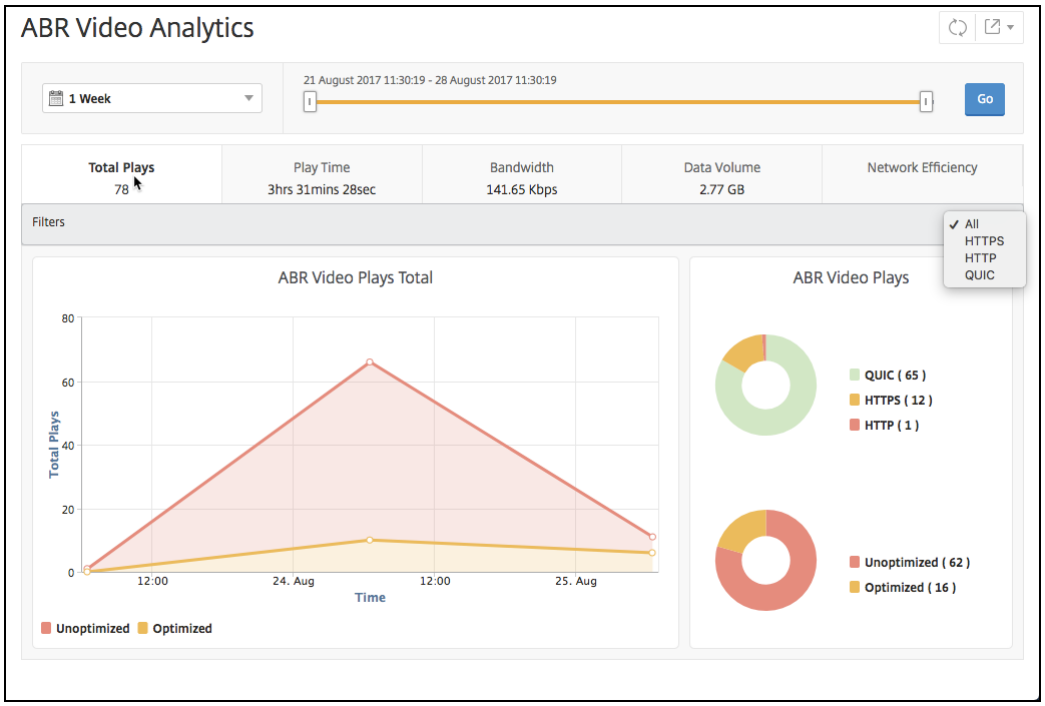
Für einen bestimmten Zeitraum zeigt Citrix Application Delivery Management (ADM) die Anzahl der

Abspielungen von ABR-Videos an und ermöglicht es Ihnen, die Anzahl der optimierten und nicht optimierten Wiedergaben in Ihrem Netzwerk zu vergleichen.

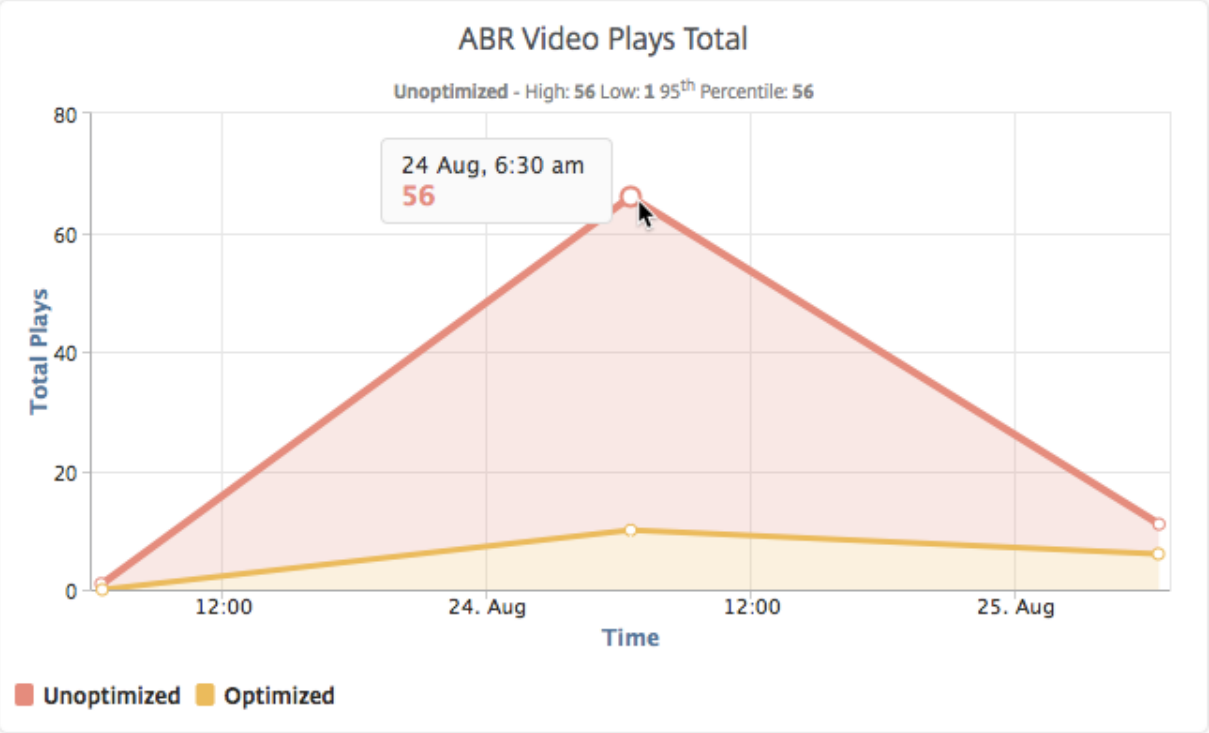
So sehen Sie die Anzahl der Stücke:

1. Navigieren Sie zu **Analytics > Video Insight**, und klicken Sie auf **ABR Video Analytics**.
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.
3. Klicken Sie auf **Los** und wählen Sie die Registerkarte **Anzahl der Wiedergaben**.

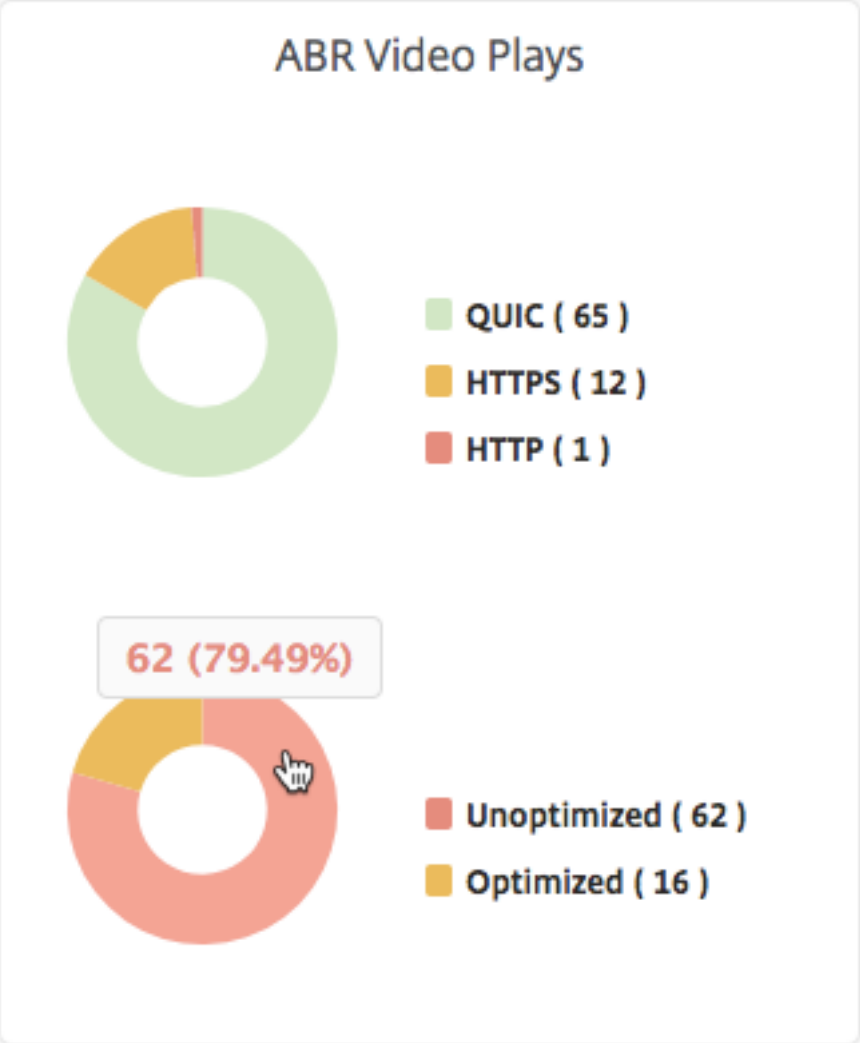
   Sie können die Liste **Filter** verwenden, um die HTTP-, HTTPS- oder QUIC-ABR-Videos auszuwählen.



Die Registerkarte **Anzahl der Wiedergaben** enthält ein Liniendiagramm und ein Kreisdiagramm, das die Anzahl der Wiedergaben von ABR-Videos aus Ihrem Netzwerk sowie die Anzahl der optimierten und nicht optimierten Wiedergaben von ABR-Videos aus Ihrem Netzwerk für den ausgewählten Zeitraum beschreibt. Sie können den Mauszeiger auf das Liniendiagramm bewegen, um die Anzahl der Wiedergaben während eines bestimmten Zeitrahmens anzuzeigen:



Außerdem können Sie den Mauszeiger auf das Kreisdiagramm bewegen, um den Prozentsatz der optimierten und nicht optimierten Wiedergaben und den Prozentsatz der verschlüsselten und unverschlüsselten ABR-Videos für den ausgewählten Zeitraum anzuzeigen.



Anzeige der Spitzendatenrate für einen bestimmten Zeitraum

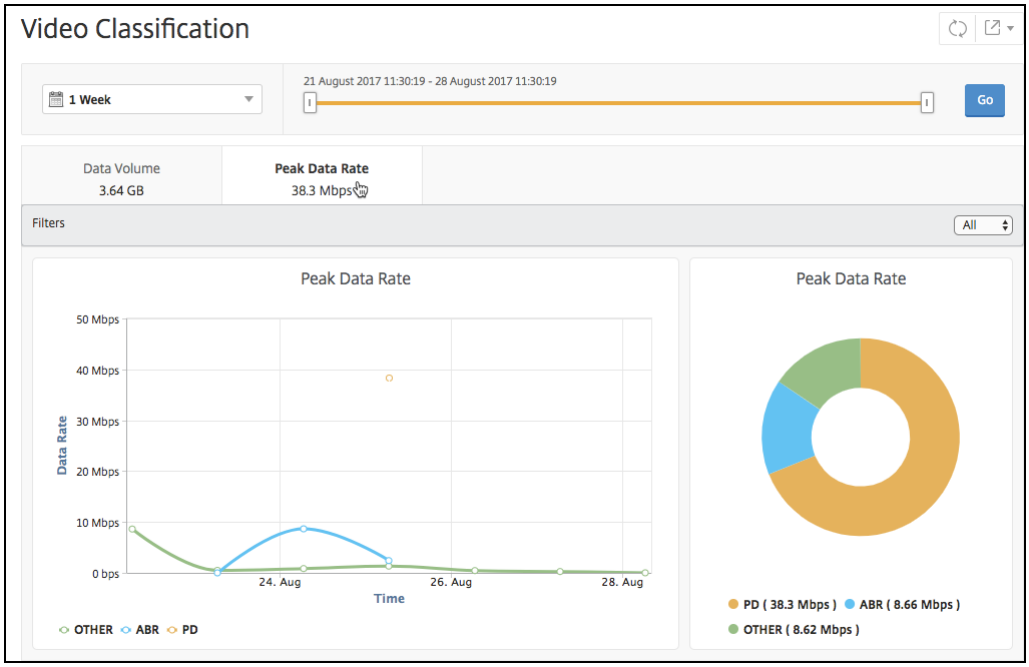
April 28, 2021

Citrix Application Delivery Management (ADM) zeigt den Spitzendurchsatz oder die Datenrate des Videodatenverkehrs in Ihrem Netzwerk an.

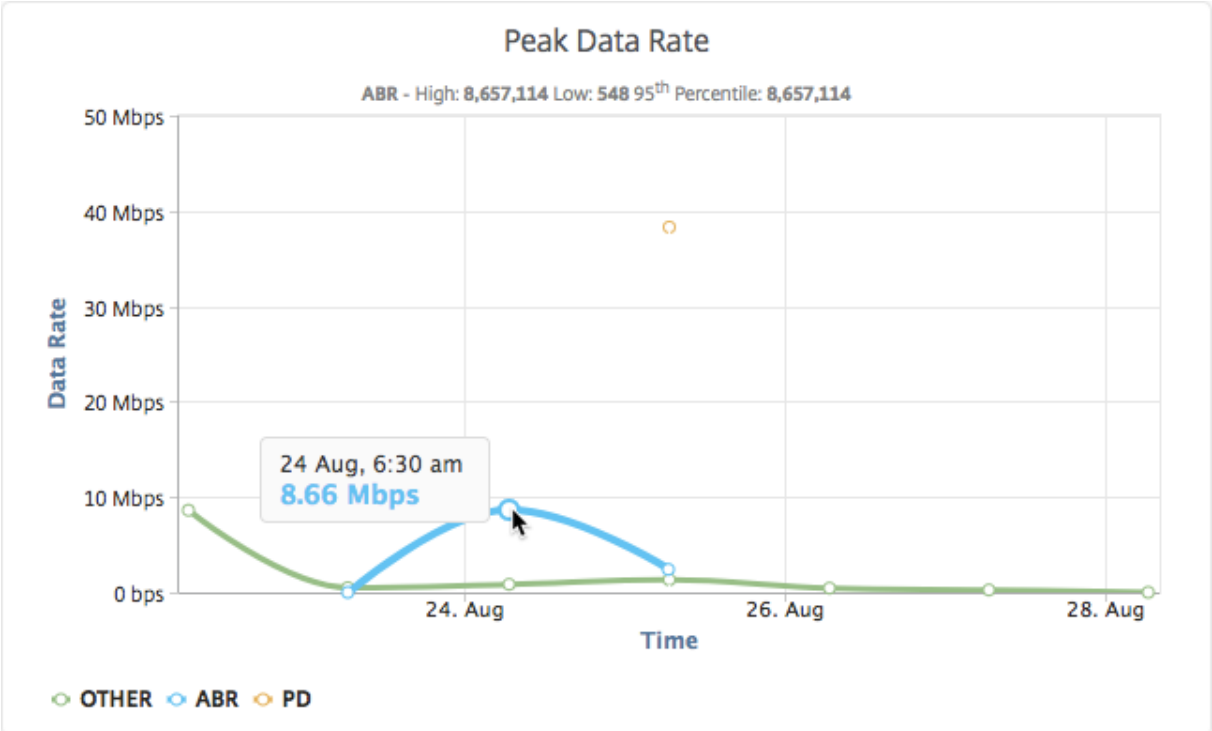
So zeigen Sie die Spitzendatenrate des Videoverkehrs an:

1. Navigieren Sie zu **Analytics > Video Insight**, und klicken Sie auf **Videoklassifizierung**.
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.
3. Klicken Sie auf **Los**, und wählen Sie die Registerkarte **Spitzendatenrate** aus.

Sie können die Liste **Filter** verwenden, um den HTTP-, HTTPS- oder QUIC-Datenverkehr auszuwählen.

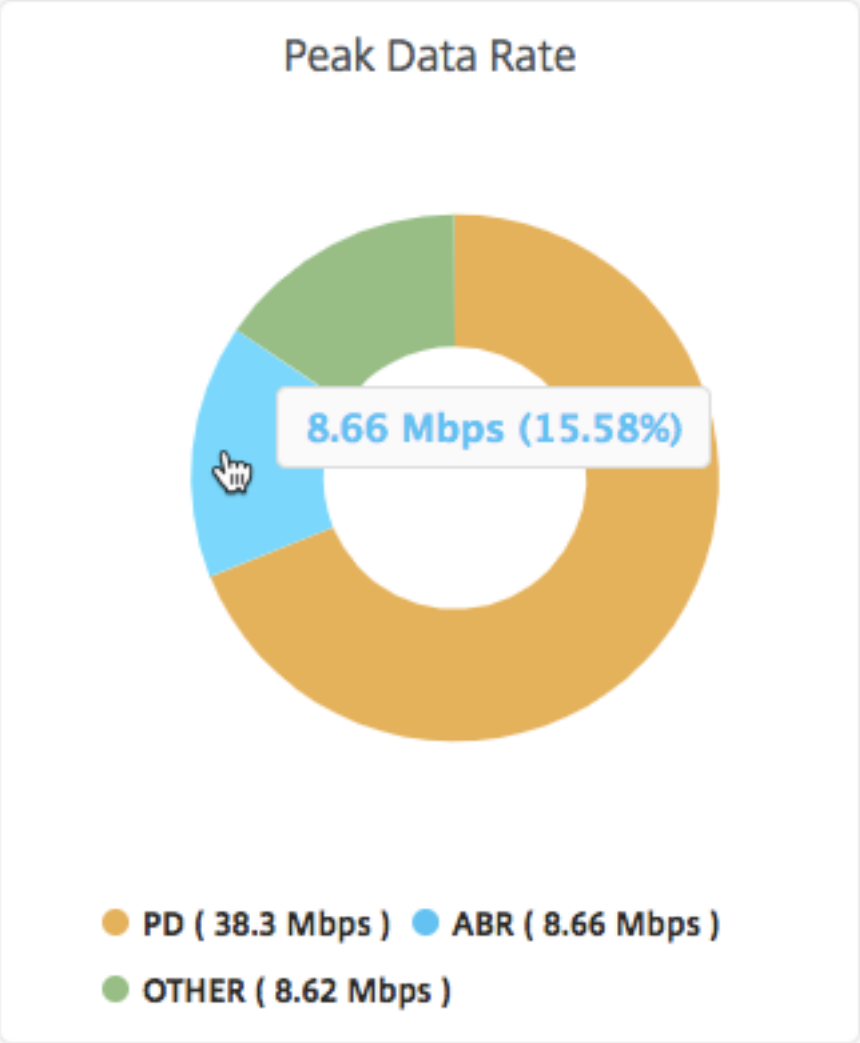


Die Registerkarte **Spitzendatenrate** enthält ein Liniendiagramm und ein Kreisdiagramm, das die Spitzendatenrate des vom Netzwerk ausgehenden Videodatenverkehrs und die Spitzendatenrate des Videodatenverkehrs im Netzwerk während des ausgewählten Zeitrahmens beschreibt. Sie können den Mauszeiger auf das Liniendiagramm bewegen, um die Spitzendatenrate während eines bestimmten Zeitrahmens anzuzeigen.



Außerdem können Sie den Mauszeiger auf das Kreisdiagramm bewegen, um den Prozentsatz der

Spitzendatenrate anzuzeigen, die vom Typ des während des ausgewählten Zeitrahmens gestreamten Videoverkehrs verbraucht wird.



SSL-Forward-Proxyanalyse

April 28, 2021

Eine Citrix ADC Appliance am Rande des Unternehmensnetzwerks fungiert als Internet-Proxy. Die Appliance kann im transparenten Proxy-Modus oder im expliziten Proxymodus betrieben werden und bietet Steuerelemente zum Abfangen des Internetverkehrs, einschließlich HTTPS. Die Entscheidung, Anfragen abzufangen, zu umgehen oder zu blockieren, wird basierend auf den auf der Appliance konfigurierten Richtlinien getroffen. Ein Benutzer wird authentifiziert, bevor er sich am Unternehmensnetzwerk anmeldet. Alle Anfragen und Antworten werden mit dem Benutzer gekennzeichnet, und die Benutzeraktivitäten werden in der Appliance protokolliert. Weitere Informationen finden Sie unter

Citrix SSL-Forward-Proxy.

Wenn Sie Citrix Application Delivery Management (ADM) in eine Citrix ADC Appliance integrieren, werden die protokollierten Benutzeraktivitäten und die nachfolgenden Datensätze auf der Appliance mithilfe von **Logstream**nach Citrix ADM exportiert. Citrix ADM stellt Informationen über die Aktivitäten der Nutzer zusammen, z. B. besuchte Websites und die verbrauchte Bandbreite. Außerdem werden Bandbreitennutzung und erkannte Bedrohungen wie Malware und Phishing-Sites gemeldet. Sie können diese Schlüsselmetriken verwenden, um Ihr Netzwerk zu überwachen und Korrekturmaßnahmen mit der Citrix ADC Appliance durchzuführen.

So integrieren Sie eine Citrix ADC Appliance in Citrix ADM:

1. Aktivieren Sie auf der Citrix ADC Appliance während der Konfiguration des SSL-Forward Proxy **Analytics** und geben Sie die Details der Citrix ADM Instanz an, die Sie für die Analyse verwenden möchten.
2. Fügen Sie in Citrix ADM die Citrix ADC Appliance als Instanz zu Citrix ADM hinzu. Weitere Informationen, siehe Hinzufügen von Instanzen zu Citrix ADM.

Dashboards

April 28, 2021

Citrix Application Delivery Management (ADM) bietet zwei Dashboards, das **Dashboard für ausgehenden Datenverkehr** und das **Benutzerdashboard**. Diese Dashboards zeigen mehrere Diagramme an, in denen die Websites oder Anwendungen zusammengefasst werden, auf die aus dem Unternehmensnetzwerk zugegriffen wird, sowie die Aktivitäten, die von den Benutzern im Netzwerk ausgeführt werden.

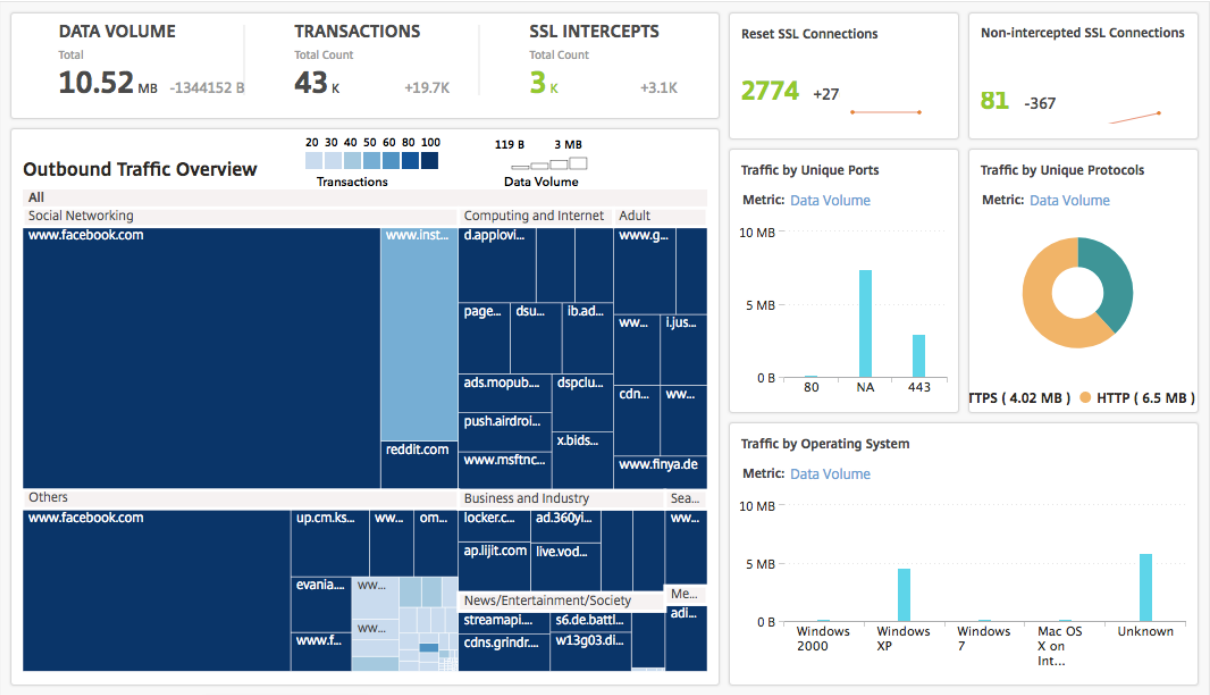
Dashboard für ausgehenden Datenverkehr

Das **Dashboard für ausgehenden Datenverkehr** enthält eine Zusammenfassung der URLs oder Domänen, auf die von Ihrem Netzwerk zugegriffen wird. Es bietet eine ganzheitliche Ansicht aller URLs oder Domains nach Anzahl der Transaktionen oder Datenvolumen, die von den URLs oder Domains verbraucht werden.
Es enthält auch Details wie die folgenden:

1. Menge der Bandbreite, die von den URLs oder Domänen belegt wird, auf die über das Netzwerk zugegriffen wird.
2. Anzahl der Transaktionen, die beim Zugriff auf die URLs und Domänen aus Ihrem Netzwerk aufgetreten sind.

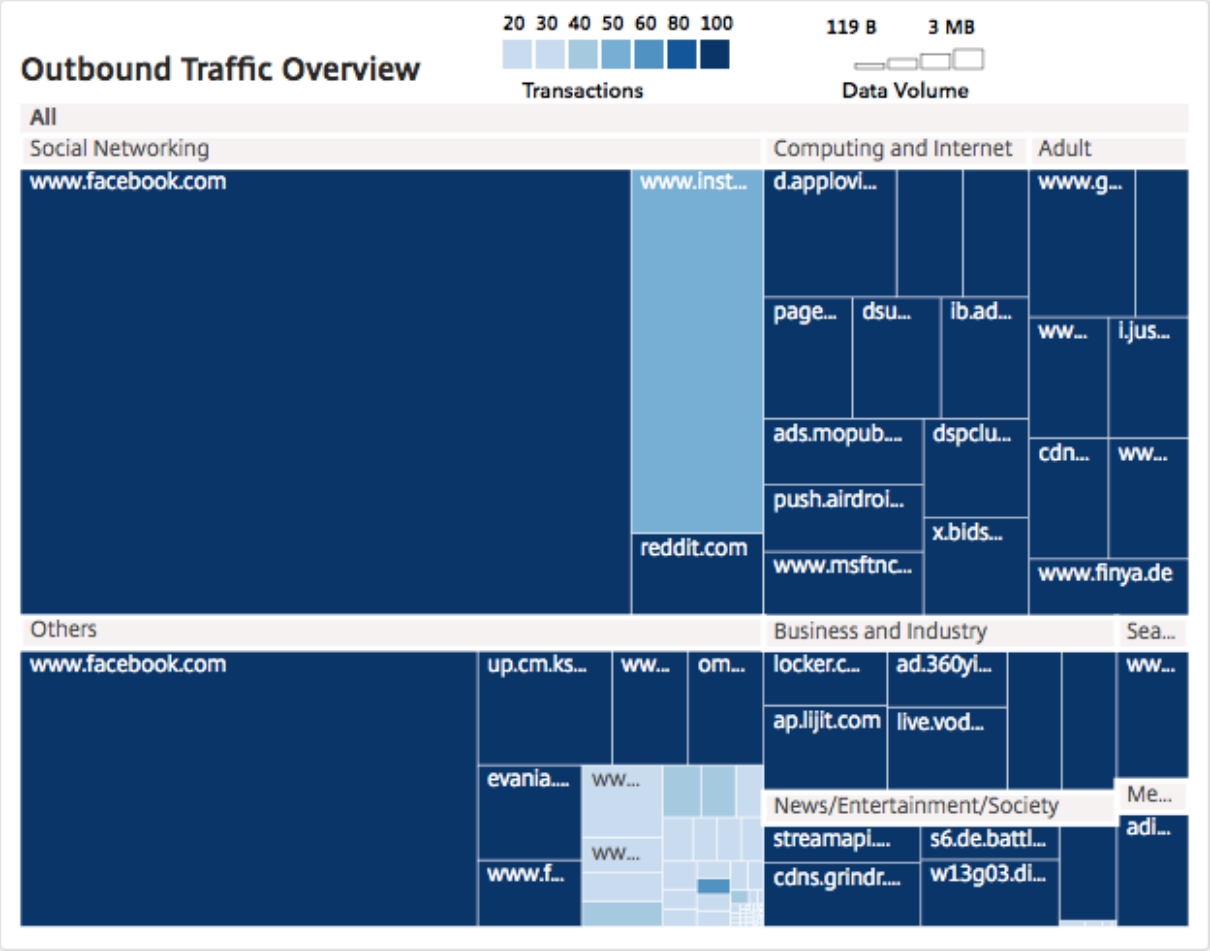
3. Anzahl der SSL-Verbindungen, die von der Citrix ADC Appliance während der Transaktionen abgefangen werden.
4. Anzahl der SSL-Verbindungen, die von der Citrix ADC Appliance während der Transaktionen nicht abgefangen werden.
5. Anzahl der SSL-Verbindungen, die von der Citrix ADC Appliance während der Transaktionen zurückgesetzt werden.
6. Umfang des übertragenen Webverkehrs, basierend auf dem für die Übertragung des Datenverkehrs verwendeten Port, dem Protokoll, das vom Webdatenverkehr verwendet wird, und den Client-Betriebssystemen, die für die Übertragung des Datenverkehrs verwendet werden.

Um auf das Dashboard für ausgehenden Datenverkehr zuzugreifen, navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**.



Anzeigen des ausgehenden Datenverkehrs aus dem Netzwerk

Das **Dashboard für ausgehenden Datenverkehr** enthält einen Bereich **Übersicht über den ausgehenden Datenverkehr**. Im Bereich **Übersicht über den ausgehenden Datenverkehr** gruppiert Citrix ADM die zugegriffenen URLs oder Domänen in Kategorien wie Shopping, Nachrichten, soziale Netzwerke usw. Im Bereich **Übersicht über ausgehenden Datenverkehr** werden die URLs oder Domänen angezeigt, auf die aus dem Netzwerk zugegriffen wird, als Knoten in den URL-Kategorien. Die Größe der Knoten richtet sich nach dem Datenvolumen, das durch den Zugriff auf die URL oder Domäne verbraucht wird. Die Farbe des Knotens gibt die Anzahl der Transaktionen an, die beim Zugriff auf die URL oder Domäne aufgetreten sind.



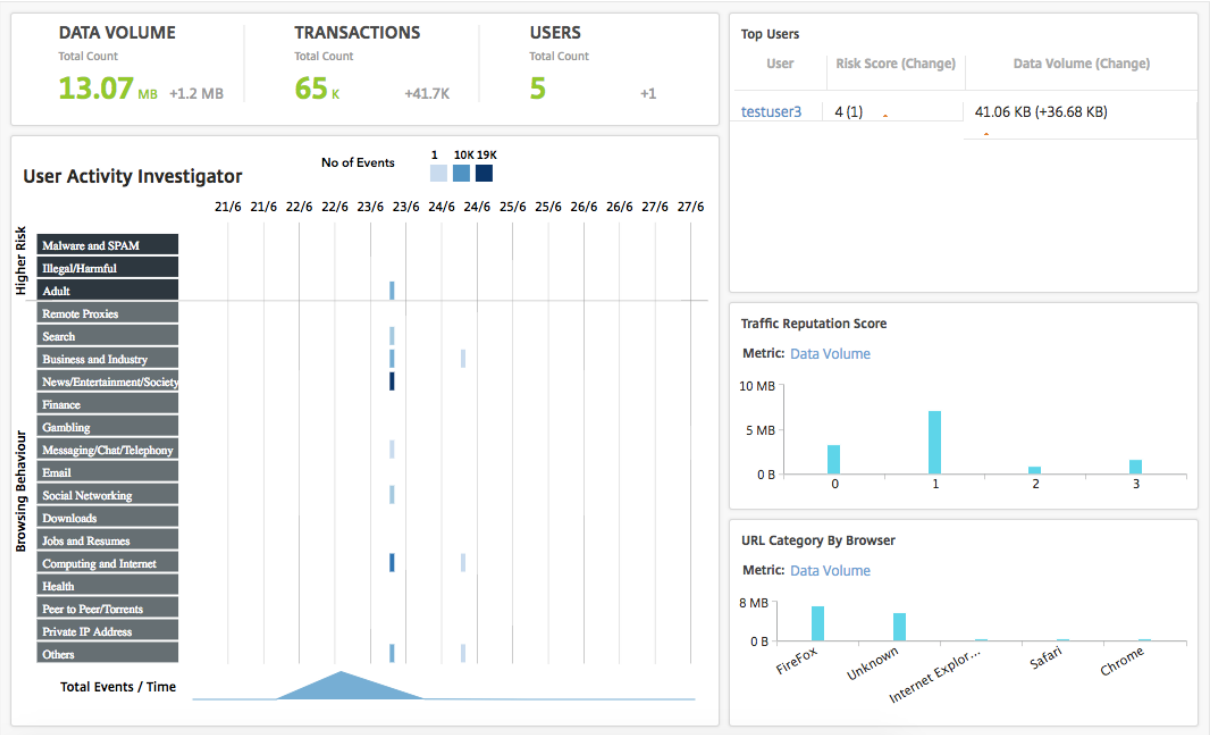
Sie können auf eine Kategorie klicken, um die Diagramme zu filtern, um Details zu der Kategorie für den angegebenen Zeitraum anzuzeigen.

Benutzerdashboard

Das **Benutzerdashboard** zeigt eine Zusammenfassung der Aktivitäten an, die von den Benutzern in Ihrem Unternehmen ausgeführt werden. Sie stellt wichtige Metriken bereit, mit denen Sie Folgendes ermitteln können:

1. Browserverhalten von Benutzern in Ihrem Unternehmen.
2. URL-Kategorien, auf die die Benutzer in Ihrem Unternehmen zugreifen.
3. Die fünf besten Benutzer, basierend auf ihren Risikobewertungen und der Bandbreite, die sie verbrauchen. Weitere Informationen zur Risikobewertung finden Sie unter Risikobewertung.
4. Browser, die für den Zugriff auf die URLs oder Domänen verwendet werden.
5. Menge des von den Benutzern erzeugten Web-Traffic basierend auf dem Traffic-Reputation Score.

Um auf das **Benutzer-Dashboard**zuzugreifen, navigieren Sie zu **Benutzer > Dashboard**.

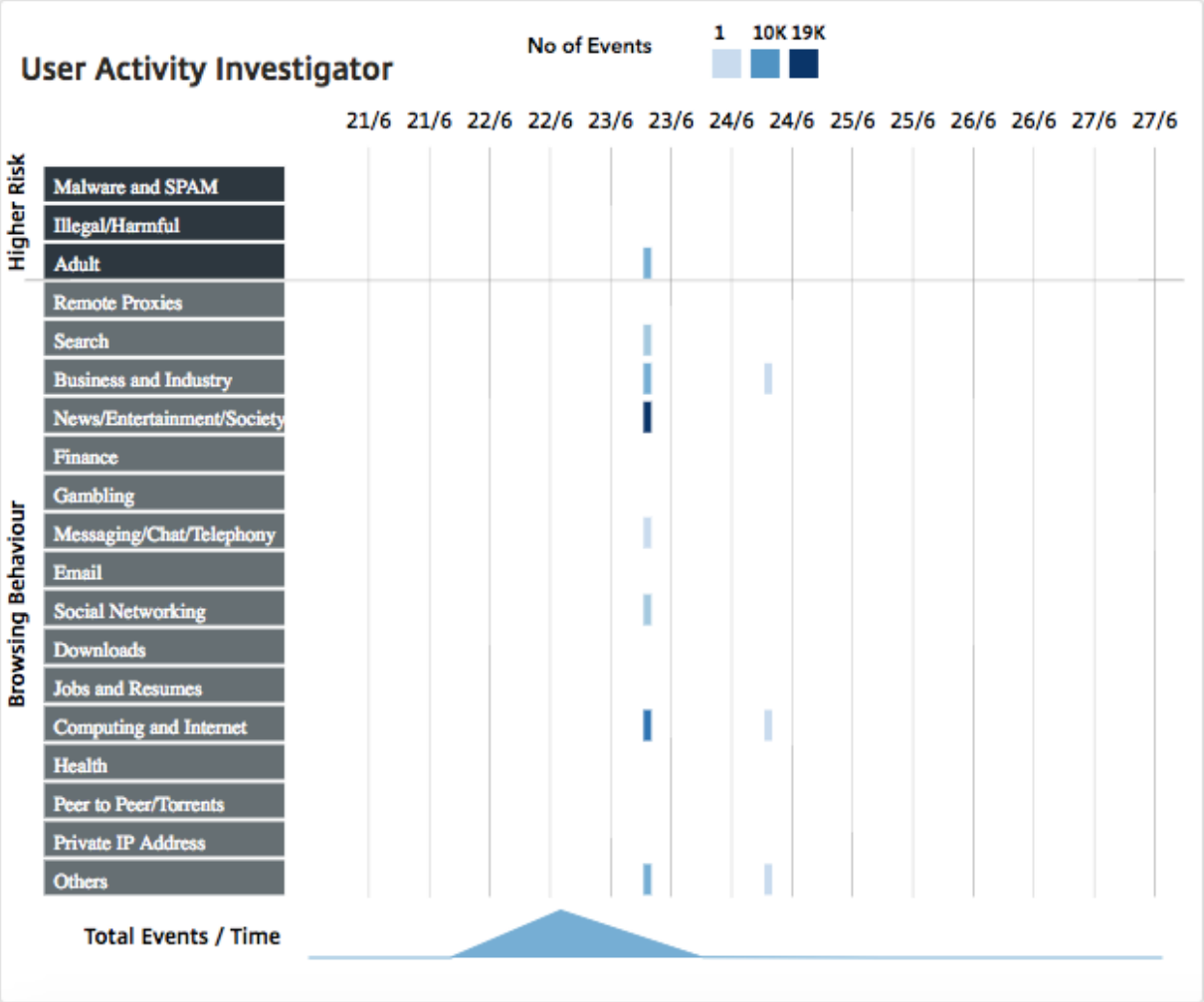


Sie können im Bereich **Top Benutzer auf einen Benutzer** klicken, um die Diagramme zu filtern, um Details der Webaktivität anzuzeigen, die der Benutzer im angegebenen Zeitraum ausgeführt hat.

Ermittler der Benutzeraktivität

Das **Benutzer-Dashboard** enthält einen Bereich **Ermittlungsprogramm**, in dem verschiedene Webaktivitäten angezeigt werden, die von den Benutzern ausgeführt werden. Es zeigt die URL-Kategorien, auf die die Benutzer während des ausgewählten Zeitrahmens zugreifen, und verschiedene Ereignisse, die pro URL-Kategorie ausgelöst werden. Sie können auf die Ereignisse klicken, um die Details auf Transaktionsebene abzurufen.

Der **User Activity Investigator** zeigt wichtige Informationen wie das Browserverhalten des Benutzers, die Aktivität mit hohem Risiko des Benutzers und die ausgelösten Ereignisse pro URL-Kategorie an. Die Ereignisse werden als rechteckige Legenden auf dem Chart dargestellt. Jede der Legenden wird in Intervallen von einer Minute aggregiert, wenn die gewählte Dauer eine Stunde beträgt, und in 1-Stunden-Intervallen, wenn die ausgewählte Dauer einen Tag beträgt.



Diese Legenden werden aggregiert und werden entsprechend der Anzahl der aufgetretenen Ereignisse farbcodiert. Sie können den Mauszeiger auf eine Legende bewegen, um Details wie die Zeit und die Anzahl der Ereignisse anzuzeigen, die für die ausgewählte Legende aggregiert wurden. Sie können den Zeitraum des Diagramms anpassen, indem Sie eine Zeit aus der Zeitperiodenliste auswählen.

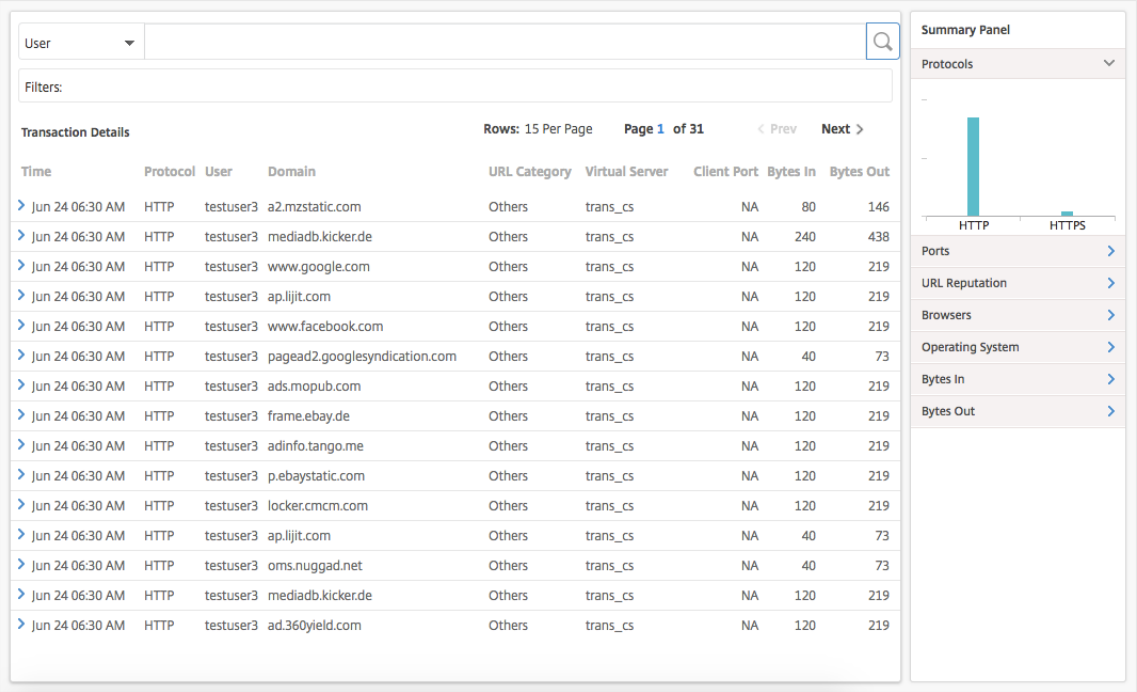
Sie können auf die Ereignisse klicken, um die Details der Transaktionen weiter aufzurufen.

Benutzertransaktionen

Auf der Seite Benutzertransaktionen werden die Details der Benutzertransaktionen in Ihrem Netzwerk angezeigt. Es enthält Details auf Transaktionsebene wie:

1. Zeitpunkt, zu dem die Transaktion stattgefunden hat
2. Protokoll, das für die Transaktion verwendet wird
3. Benutzername
4. Domäne, auf die der Benutzer zugegriffen hat

5. URL-Kategorie
6. Proxyserver, der zum Abfangen der Transaktion verwendet wird
7. Client-Port-Details
8. Bytes In
9. Bytes aus



Übersichtsfenster

Im **Übersichtsfenster** werden alle Metriken der Transaktionen angezeigt, die im Bereich **Transaktionsdetails** angezeigt werden. In diesem Bereich können Sie die Transaktionen im Bereich **Transaktionsdetails** sortieren und anzeigen, indem Sie die Metriken auswählen oder deaktivieren. Im **Übersichtsfenster** werden die folgenden Metriken angezeigt:

Metriken	Beschreibung
Protokolle	Protokolle, die in den Transaktionen verwendet werden
Ports	Ports, die für die Transaktionen verwendet werden
URL-Reputation	URL-Reputationsbewertung
Browser	Browser, die für die Transaktionen verwendet werden

Metriken	Beschreibung
Betriebssystem	Betriebssystem, das für die Transaktionen verwendet wird
Bytes In	Menge der über die Citrix ADC Appliance empfangenen Daten.
Bytes aus	Datenmenge, die über die Citrix ADC Appliance gesendet wird.

Risikobewertung

Risk Score ist ein Bewertungssystem, das in Citrix ADM verwendet wird, um die Risiken zu ermitteln, die mit Benutzern in Ihrem Unternehmen verbunden sind. Citrix ADM weist eine Risikobewertung auf der Grundlage der URL-Reputationsbewertung zu, die von der Citrix ADC Appliance für die URLs zugewiesen wurde, auf die die Benutzer im Netzwerk zugreifen. Hinweise zur URL-Reputationsbewertung finden Sie unterURL-Reputationsbewertung. In der folgenden Tabelle werden die von Citrix ADM zugewiesenen Risikobewertungen beschrieben.

Risikobewertung	Beschreibung
1	Die Web-Aktivität des Benutzers hat keine wahrgenommene Bedrohung oder ist nicht abnormal.
2	Die Web-Aktivität des Benutzers hat keine wahrgenommene Bedrohung oder ist nicht ungewöhnlich, aber der Benutzer greift auf unbekannte Websites zu, die keine URL-Reputationswerte haben.
3	In der Webaktivität des Benutzers wird keine Bedrohung erkannt, aber der Benutzer hat versucht, auf Websites zuzugreifen, die potenziell anfällig sind oder mit Websites verbunden sind, die potenziell anfällig sind.
4	potenziell gefährdete Benutzer.
5	Die Web-Aktivität des Benutzers ist abnormal und der Benutzer hat auf bekannte bösartige Websites zugegriffen.

Anwendungsfälle

April 28, 2021

Überwachung des SSL-Abfanges

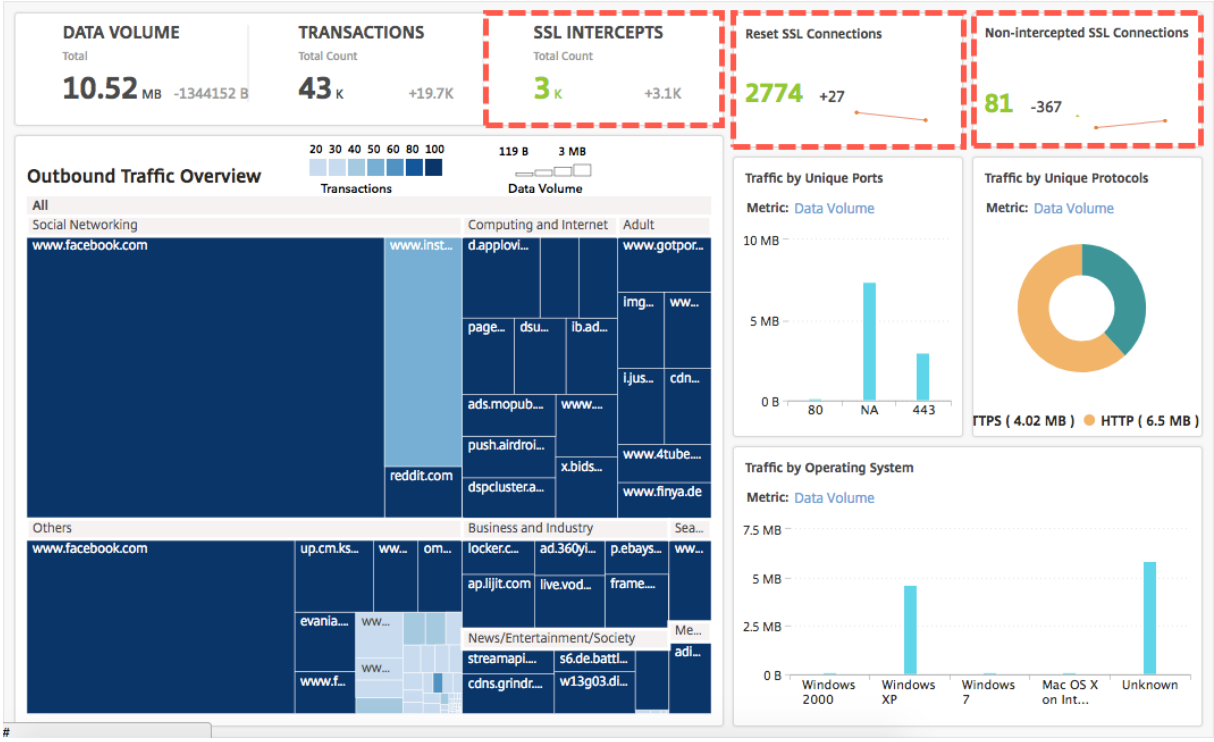
Mit einer Citrix ADC Appliance können Sie Ihren verschlüsselten ausgehenden Datenverkehr überprüfen. Sie können HTTPS-Anforderungen basierend auf Richtlinien abfangen, umgehen oder blockieren, die auf der Appliance konfiguriert sind. Citrix Application Delivery Management (ADM) enthält die folgenden Details zu den SSL-Verbindungen im **Dashboard für ausgehenden Datenverkehr** für einen ausgewählten Zeitraum:

- Anzahl der SSL-Verbindungen, die von der Citrix ADC Appliance abgefangen, nicht abgefangen und zurückgesetzt werden
- Transaktionsdetails der SSL-Verbindungen

Anhand dieser Details können Sie die Richtlinien auf Ihrer Citrix ADC Appliance weiter optimieren, um den verschlüsselten ausgehenden Datenverkehr effizient zu überprüfen. Weitere Informationen finden Sie unter Citrix SSL-Forward-Proxy.

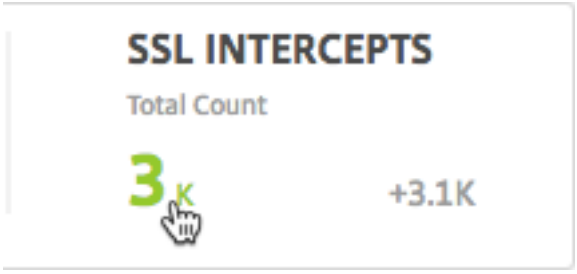
So zeigen Sie die Anzahl der SSL-Verbindungen an, die abgefangen, nicht abgefangen und zurückgesetzt wurden:

Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**. Das Dashboard für Außenbordverkehr zeigt die Anzahl der SSL-Verbindungen an, die abgefangen, nicht abgefangen und zurückgesetzt werden.

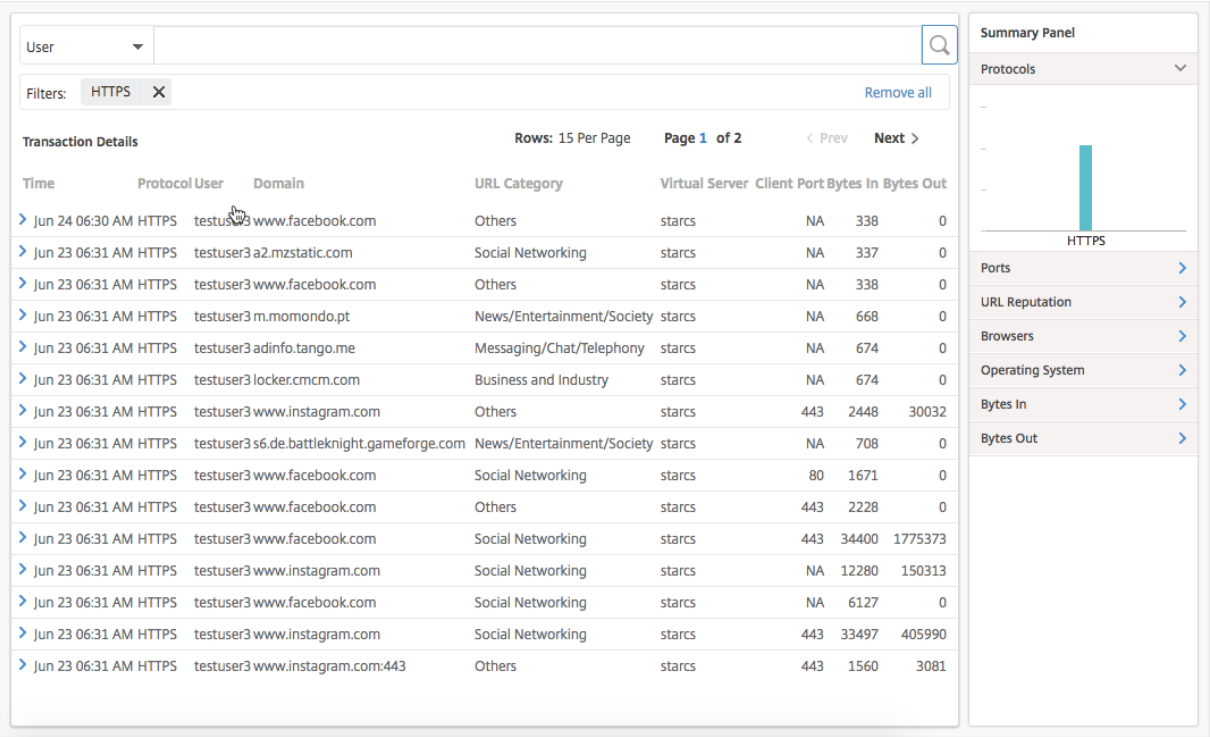


So zeigen Sie die Transaktionsdetails der abgefangenen SSL-Verbindungen an:

1. Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**.
2. Klicken Sie im **Dashboard des Außenbordverkehrs**auf die Gesamtanzahl im Abschnitt **SSL-INTERCEPTS**.



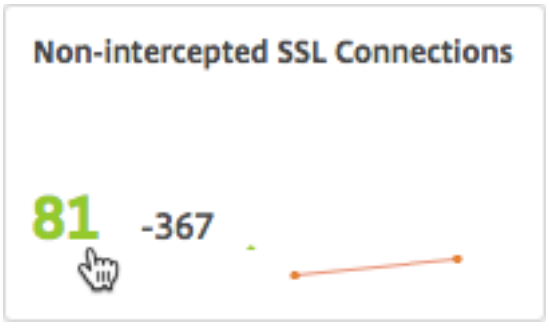
Die Transaktionsdetails der SSL-Verbindungen, die während des ausgewählten Zeitrahmens abgefangen wurden, werden auf der Seite **Transaktionsdetails** angezeigt.



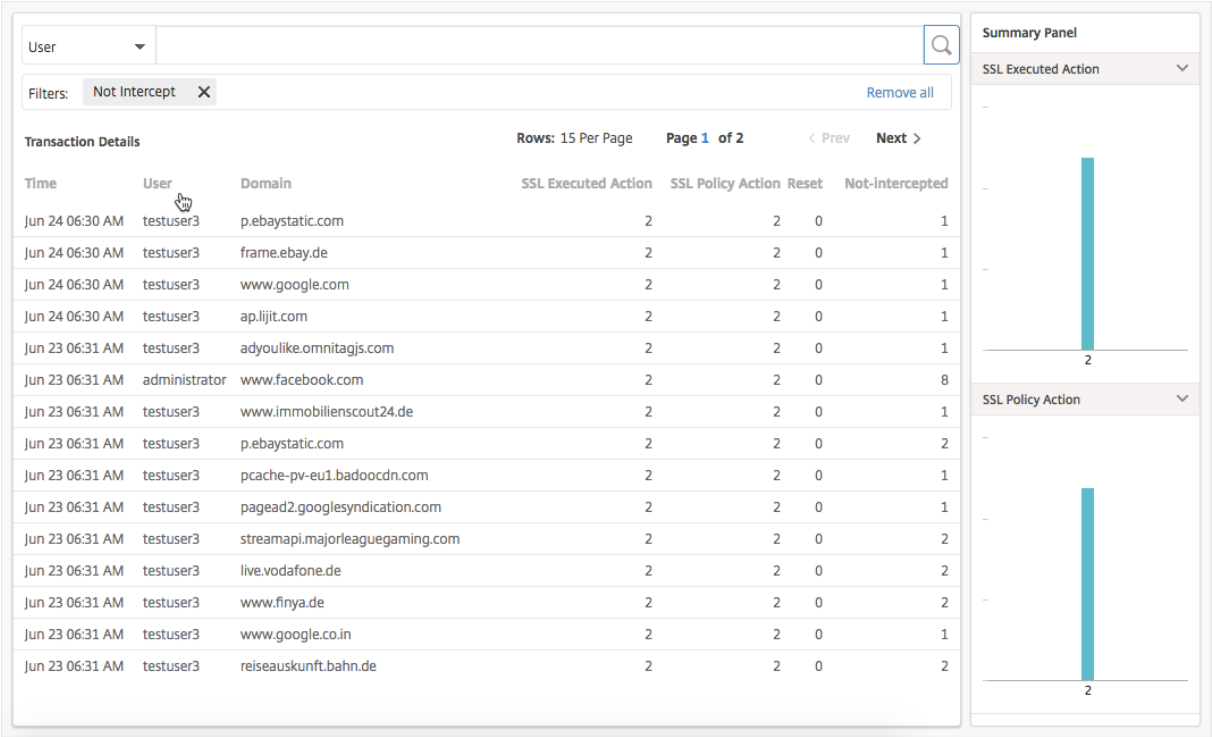
Sie können die Transaktionsdetails weiter nach Benutzer und URL-Kategorie filtern.

So zeigen Sie die Transaktionsdetails der SSL-Verbindungen an, für die kein Datenverkehr abgefangen wurde:

1. Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**.
2. Klicken Sie im **Dashboard für Außenbordverkehr**im Abschnitt **Nicht-abgefangene SSL-Verbindungen** auf die Gesamtanzahl.



Die Transaktionsdetails der SSL-Verbindungen, für die der Datenverkehr während des ausgewählten Zeitraums nicht abgefangen wurde, werden auf der Seite **Transaktionsdetails** angezeigt.

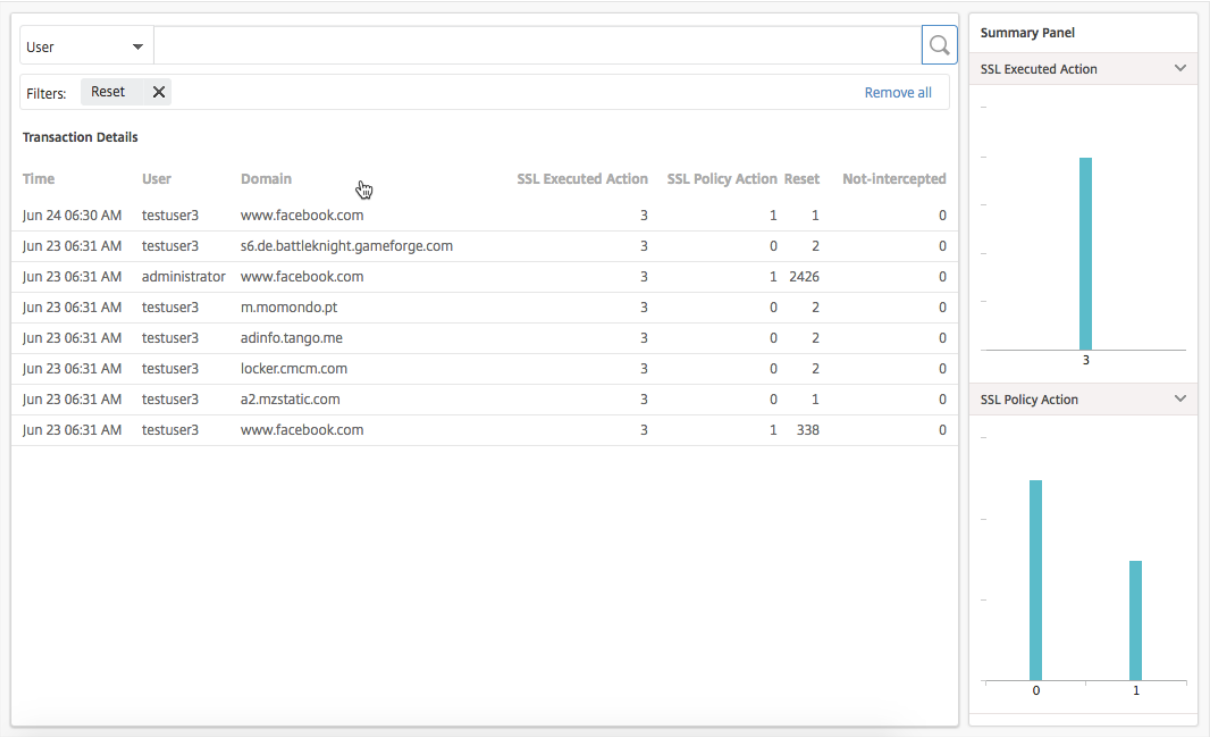


Sie können die Transaktionsdetails weiter nach Benutzer und URL-Kategorie filtern.

So zeigen Sie die Transaktionsdetails der zurückgesetzten SSL-Verbindungen an:

1. Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**.
2. Klicken Sie im **Dashboard für Außenbordverkehr**im Abschnitt **SSL-Verbindungen zurücksetzen**auf die Gesamtanzahl.

Die Transaktionsdetails der SSL-Verbindungen, für die der Datenverkehr während des ausgewählten Zeitraums nicht abgefangen wurde, werden auf der Seite **Transaktionsdetails** angezeigt.



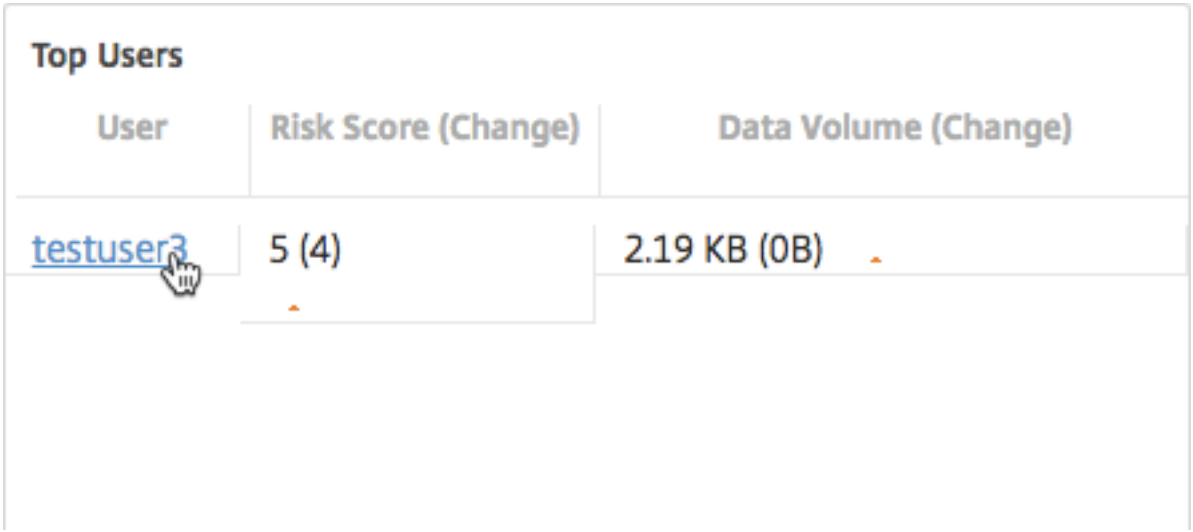
Sie können die Transaktionsdetails weiter nach Benutzer und URL-Kategorie filtern.

Überprüfen von Endpunkten

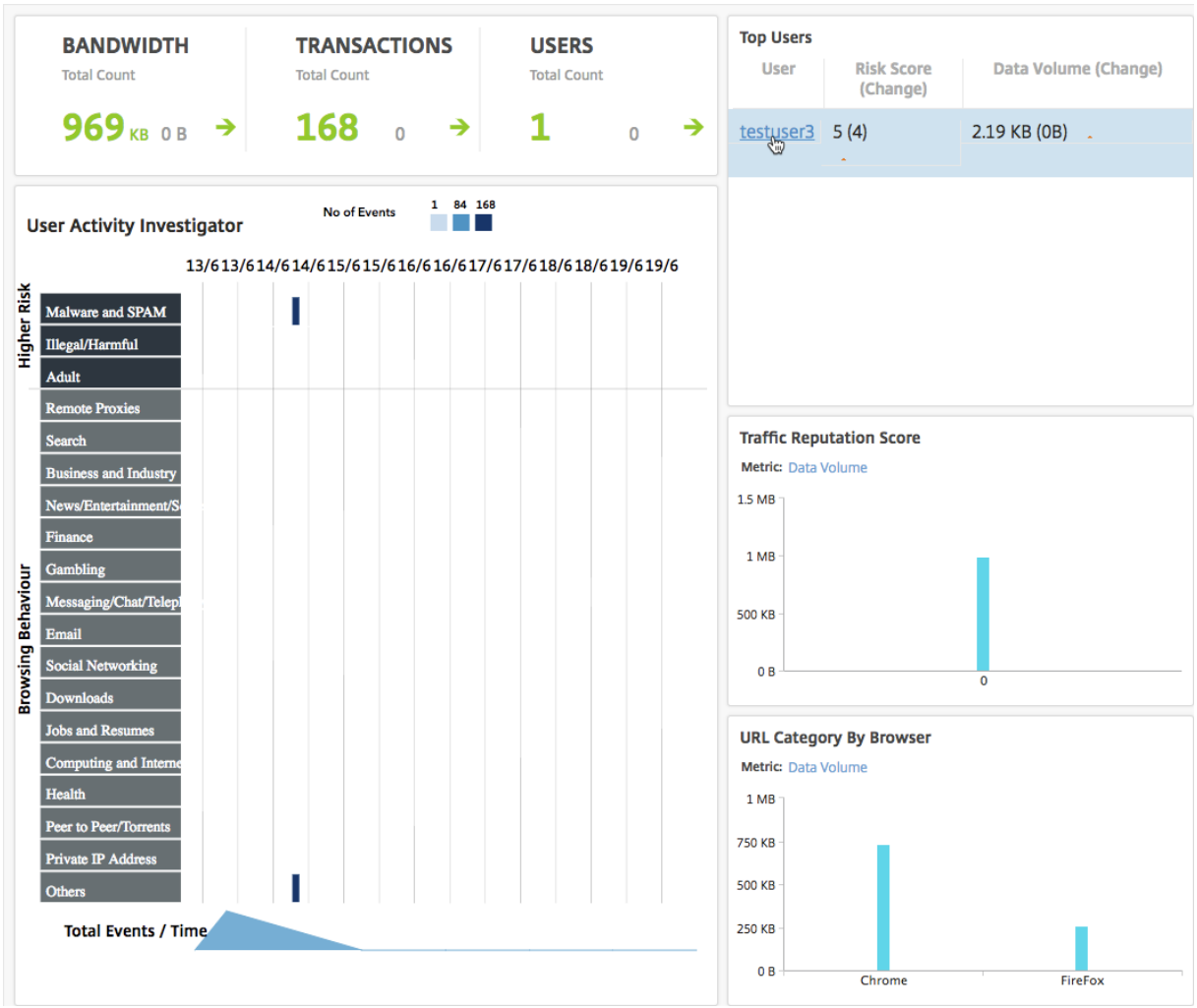
Die Richtlinien, die Sie auf einer Citrix ADC Appliance konfiguriert haben, legen fest, wie die Appliance alle in Ihrem Unternehmen ausgeführten Benutzeraktivitäten protokolliert. Citrix ADM stellt wichtige Metriken zur Verfügung, mit denen Sie Folgendes ermitteln können:

1. Browserverhalten von Benutzern in Ihrem Unternehmen.
2. URL-Kategorien, auf die die Benutzer in Ihrem Unternehmen zugreifen.
3. Die fünf besten Benutzer, basierend auf ihren Risikobewertungen und der Bandbreite, die sie verbrauchen. Weitere Hinweise zu Risikobewertungen finden Sie unterRisikobewertung.
4. Browser, die für den Zugriff auf die URLs oder Domänen verwendet werden.
5. Menge des von den Benutzern erzeugten Web-Traffic basierend auf dem Traffic-Reputation Score.

Wenn beispielsweise ein Benutzer mit der Benutzer-ID testuser3 ständig auf Malware-bezogene Websites in Ihrem Unternehmen zugreift, identifiziert Citrix ADM den Benutzer als Benutzer mit hohem Risiko und weist eine höhere Risikobewertung zu. Die Informationen testuser3 werden im Abschnitt **Top Users** des **User Dashboards** angezeigt.

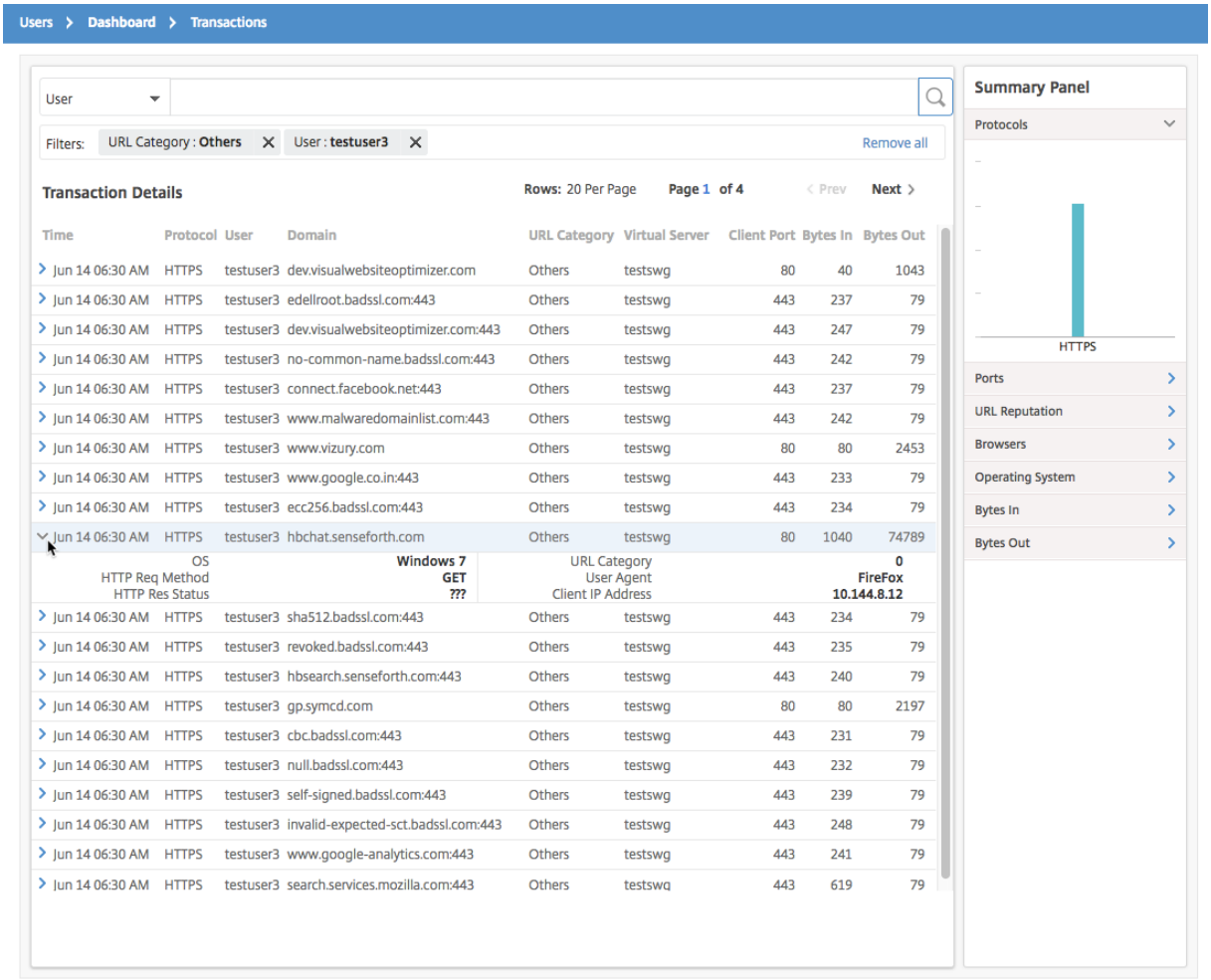


Sie können auf testuser3 klicken, um das **Benutzer-Dashboard** zu filtern, um alle wichtigen Metriken im Zusammenhang mit testuser3 anzuzeigen.



Im Bereich **Benutzeraktivitätsuntersuchung** wird die risikoreiche Aktivität von testuser3 als Ereignisse in den jeweiligen URL-Kategorien angezeigt.

Sie können den Mauszeiger über die Ereignisse bewegen, um die Anzahl der Ereignisse anzuzeigen, und Sie können auf Ereignisse klicken, um die Transaktionen zu untersuchen, die während der Ereignisse aufgetreten sind.

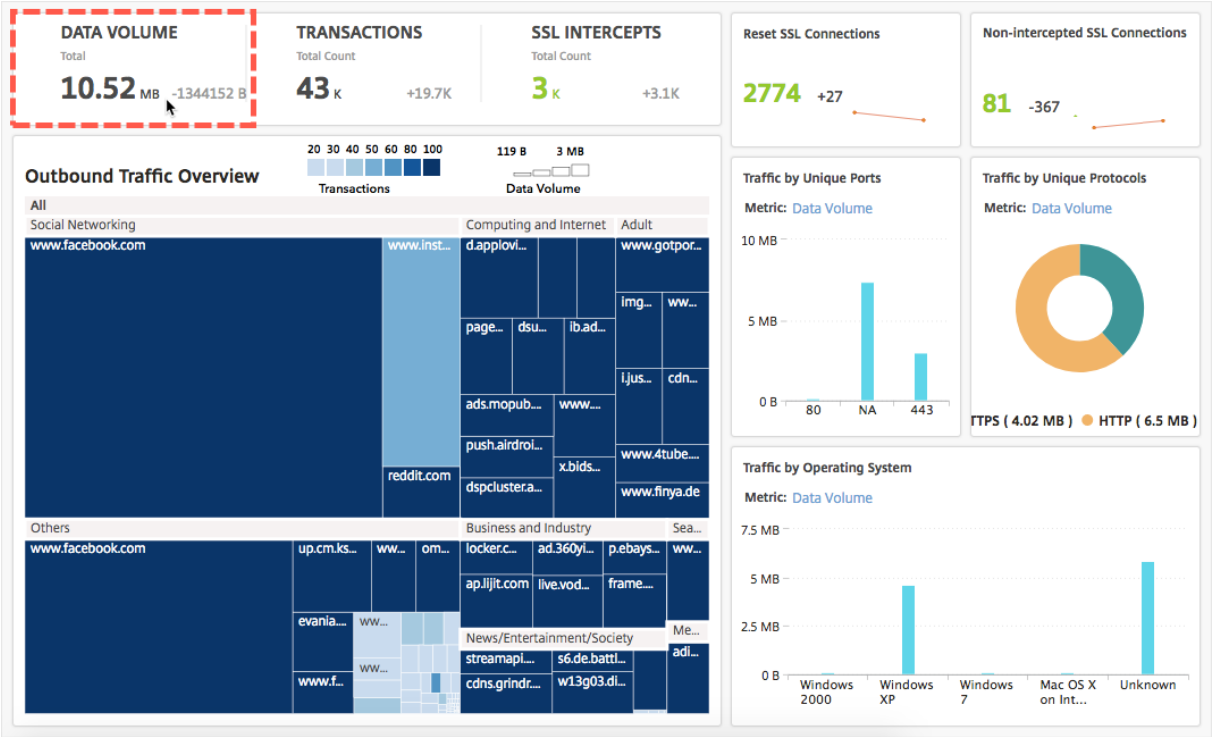


Mit diesen Informationen können Sie feststellen, ob Ihr System durch Malware infiziert ist, oder Sie können das Bandbreitenverbrauchsmuster des Benutzers verstehen und Ihre Citrix ADC Richtlinien optimieren. Weitere Informationen finden Sie unter Citrix SSL-Forward-Proxy-Dokumentation.

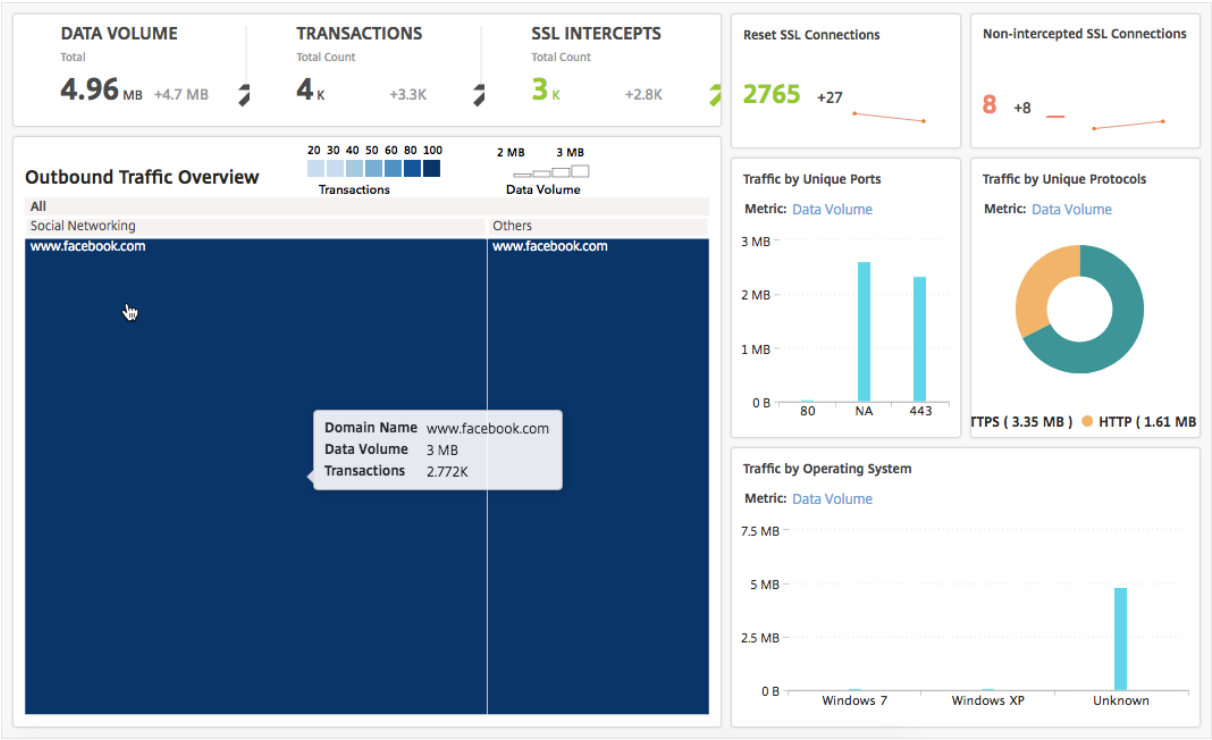
Berichterstattung über Bandbreitenverbrauch

Das **Dashboard für ausgehenden Datenverkehr** und das **Benutzerdashboard** stellen mehrere Diagramme bereit, in denen die Websites oder Anwendungen zusammengefasst werden, auf die vom Unternehmensnetzwerk zugegriffen wird, sowie die Aktivitäten, die von den Benutzern im Netzwerk ausgeführt werden.

Das **Dashboard für ausgehenden Datenverkehr** enthält die Details des Datenvolumens durch die URLs oder Domänen, auf die von Ihrem Netzwerk zugegriffen wurde. Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**, wo die **Daten im Abschnitt Datenvolumen**angezeigt werden.

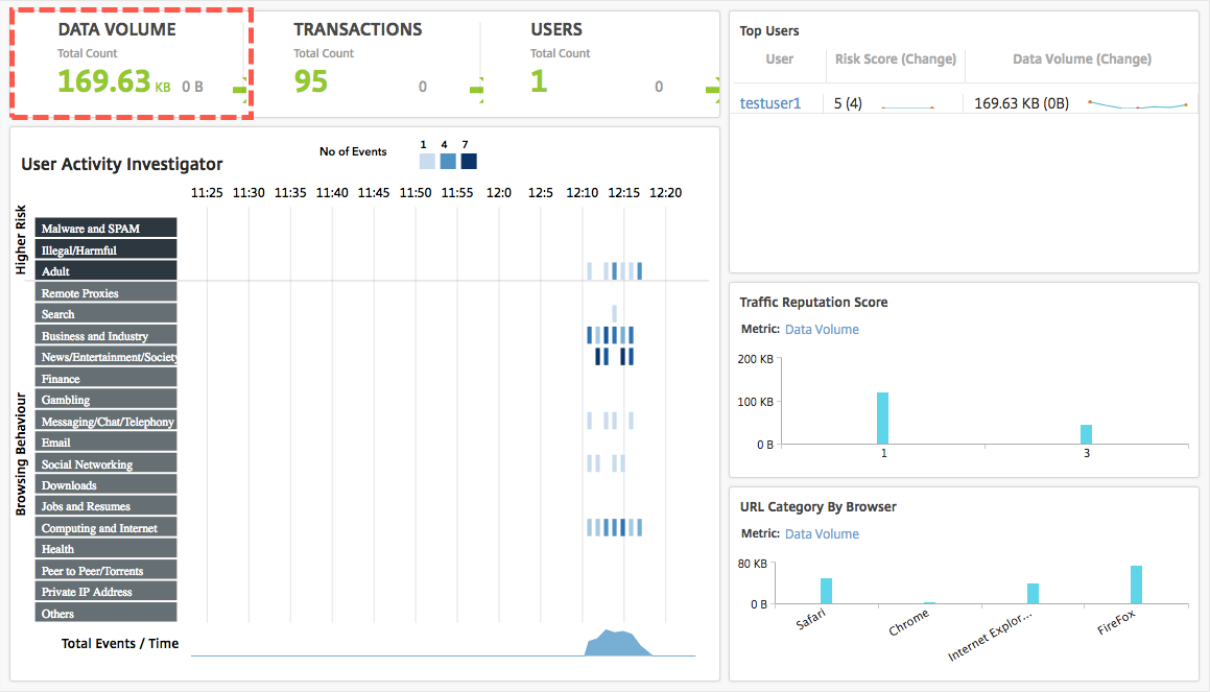


Im Bereich **Übersicht über ausgehenden Datenverkehr** können Sie auf eine Domäne oder URL klicken, um die Details des Datenvolumens anzuzeigen, das von der Domäne oder URL verwendet wird.

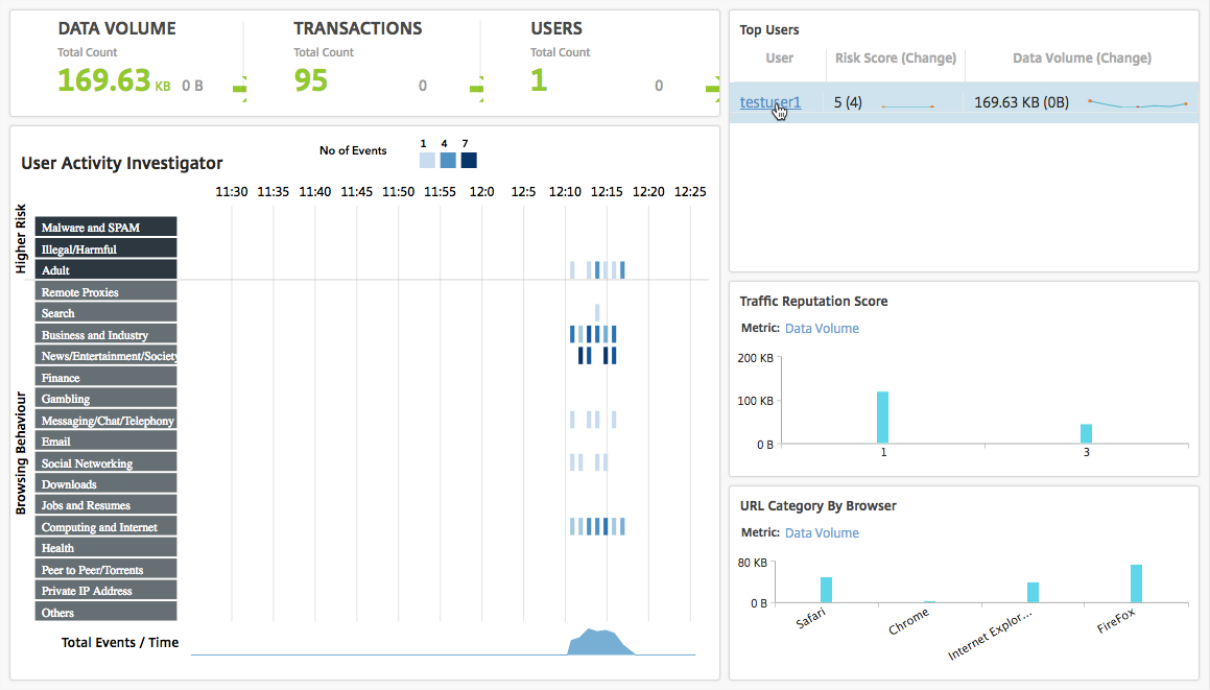


Das **Benutzerdashboard** enthält Details zur Bandbreite, die von den Benutzern in Ihrem Netzwerk

belegt wird. Navigieren Sie zu **Benutzer > Dashboard**, um die Details der von Benutzern verbrauchten Bandbreite im Abschnitt **DATA VOLUME** im **Benutzerdashboard** anzuzeigen.



Sie können die Details der Bandbreite anzeigen, die von einem Benutzer belegt wird, indem Sie den Benutzer im Abschnitt **Top Benutzer** auswählen. Der Abschnitt **DATA VOLUME** und andere Schlüsselmetriken im Diagramm werden für den ausgewählten Benutzer gefiltert.



Anhand dieser Details können Sie den Bandbreitenverbrauch und den Grund für den Verbrauch ver-

stehen. Wenn ein Benutzer beispielsweise auf Websites sozialer Netzwerke zugreift und dies zu einem großen Bandbreitenverbrauch geführt hat, kann der Administrator auf die Citrix ADC Appliance zugreifen und eine URL-Listen-Funktion konfigurieren, um den Zugriff auf die Websites zu steuern. Weitere Informationen finden Sie unter Anwendungsfall: URL-Filterung mit benutzerdefiniertem URL-Set-Thema.

Verteilung des ausgehenden Datenverkehrs anzeigen

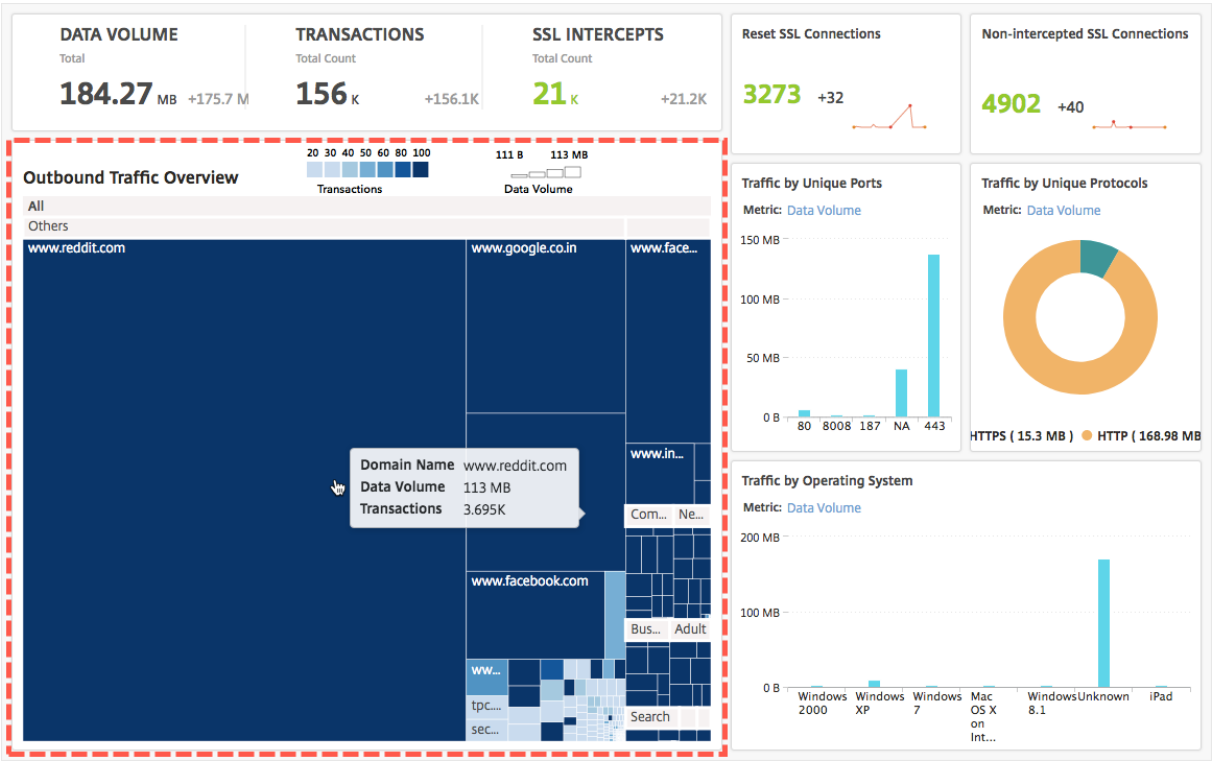
Die Citrix ADC Appliance bietet URL-Kategorisierungs- und Filterfunktionen, mit denen Sie die URLs kategorisieren können, auf die über das Netzwerk zugegriffen wird. In Citrix ADM enthält das **Dashboard für ausgehenden Datenverkehr** einen Bereich **Übersicht über den ausgehenden Datenverkehr**. Im Bereich **Übersicht über den ausgehenden Datenverkehr** gruppiert Citrix ADM die zugegriffenen URLs oder Domänen in Kategorien wie Shopping, News, Mobile usw., um die Verteilung des ausgehenden Datenverkehrs im Netzwerk anzuzeigen. Für einen ausgewählten Zeitraum können Sie auf die URL klicken, um Folgendes zu verstehen:

1. Beim Zugriff auf die URL verbrauchte Bandbreite
2. Transaktionen, die beim Zugriff auf die URL aufgetreten sind
3. Anzahl der SSL-Verbindungen, die beim Zugriff auf die URL abgefangen, nicht abgefangen und zurückgesetzt wurden

Mit diesen Informationen können Sie das Muster des ausgehenden Datenverkehrs verstehen und korrigierende Entscheidungen treffen, z. B. ob bestimmte URLs blockiert werden sollen.

So zeigen Sie die Verteilung des ausgehenden Datenverkehrs an:

Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**. Das **Dashboard für Außenbordverkehr** zeigt die URLs im Bereich **Übersicht über ausgehenden Datenverkehr an**:



Wenn Sie die Details einer bestimmten URL anzeigen möchten, wählen Sie die URL aus.

Mithilfe dieser Informationen können Sie das Muster des ausgehenden Datenverkehrs verstehen und den Netzwerkverkehr mithilfe eines auf der Citrix ADC Appliance konfigurierten URL-Filters steuern. Weitere Informationen finden Sie unter URL-Filterung.

Gepoolte Kapazität

April 28, 2021

Die gepoolte Kapazität in Citrix ADC ist ein Lizenzierungsframework, das einen gemeinsamen Bandbreiten- und Instanzpool umfasst, der auf Citrix Application Delivery Management (ADM) gehostet und bereitgestellt wird. Aus diesem gemeinsamen Pool wird jede ADC-Instanz in Ihrem Rechenzentrum unabhängig von der Plattform oder dem Formfaktor eine Instanzlizenz und nur die erforderliche Bandbreite ausgecheckt. Die Lizenzdatei und damit die Bandbreite sind nicht an die Instanz gebunden. Wenn die Instanz diese Ressourcen nicht mehr benötigt, werden sie wieder in den gemeinsamen Pool eingecheckt und die Ressourcen anderen Instanzen zur Verfügung gestellt, die sie benötigen.

> **Hinweis**
>
> Im ADM-Dienst ist einer der Agenten der Lizenzserver. Im on-premises ADM ist der on-premises

> Server der Lizenzserver (auch wenn Agenten bereitgestellt werden).

Dieses Lizenzierungsframework maximiert die Bandbreitenauslastung, indem sichergestellt wird, dass Instanzen nicht mehr Bandbreite zugewiesen wird als ihre Anforderung. Die Möglichkeit der ADC-Instanzen, Lizenzen und Bandbreite in und aus einem gemeinsamen Pool zu überprüfen, ermöglicht Ihnen auch die Automatisierung des Instanzprovisionings.

Sie können die Bandbreite erhöhen oder verringern, die einer Instanz zur Laufzeit zugewiesen ist, ohne den Datenverkehr zu beeinträchtigen. Sie können die Lizenzen im Pool auch von einer Instanz auf eine andere übertragen.

Konfiguration der gepoolten Kapazität

April 28, 2021

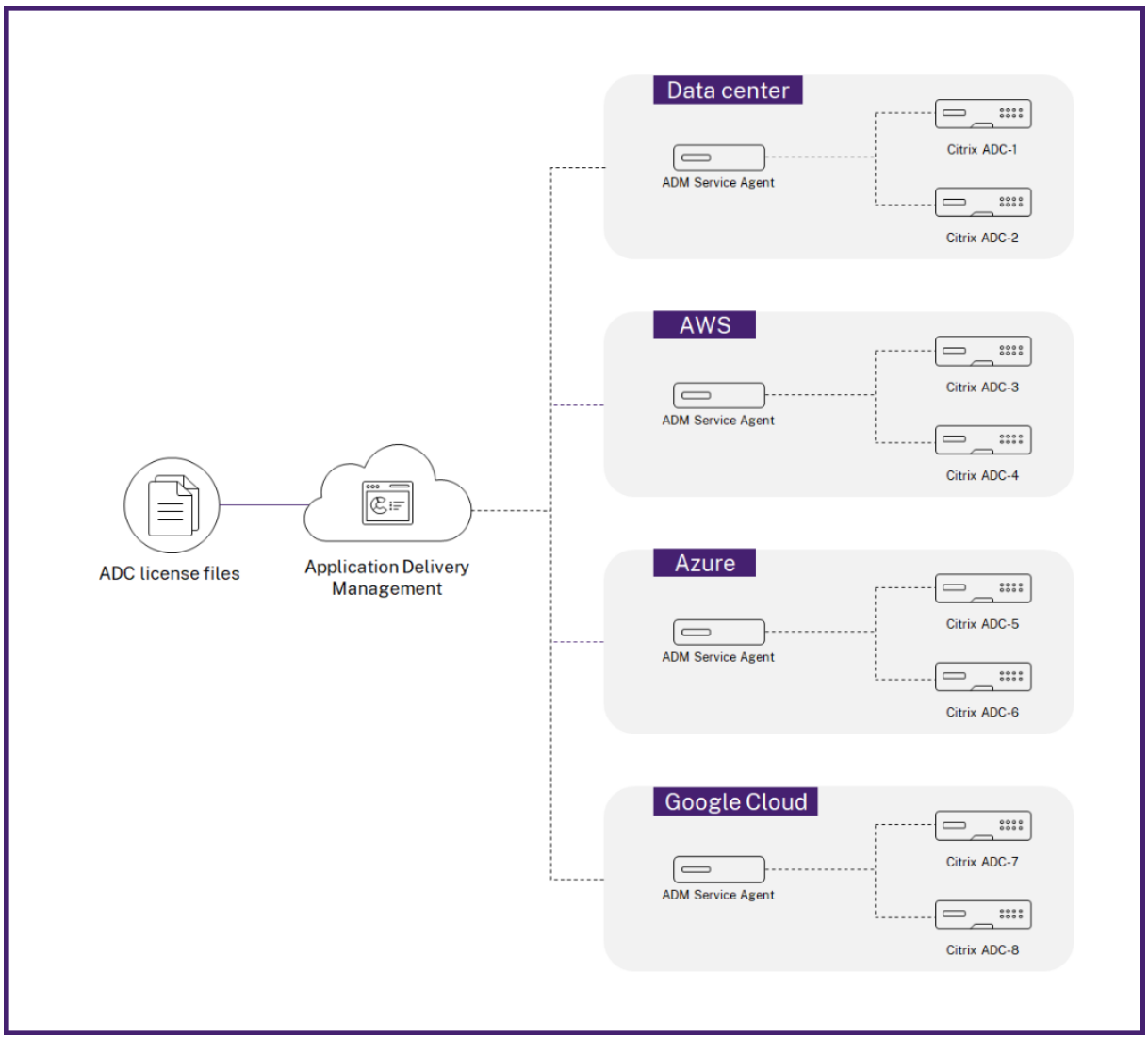
Mit der in Citrix ADC gepoolten Kapazität können Sie Bandbreiten- oder Instanzlizenzen für verschiedene ADC-Formfaktoren freigeben. Für virtuelle CPU-Abonnementinstanzen können Sie virtuelle CPU-Lizenzen für alle Instanzen freigeben. Verwenden Sie diese gepoolte Kapazität für die Instanzen, die sich im Rechenzentrum oder in Public Clouds befinden. Wenn eine Instanz die Ressourcen nicht mehr benötigt, überprüft sie die zugewiesene Kapazität wieder in den gemeinsamen Pool. Verwenden Sie die freigegebene Kapazität für andere ADC-Instanzen, die Ressourcen benötigen.

Sie können die gepoolte Lizenzierung verwenden, um die Bandbreitenauslastung zu maximieren, indem Sie die erforderliche Bandbreitenzuweisung einer Instanz sicherstellen und nicht mehr als deren Bedarf. Erhöhen oder verringern Sie die Bandbreite, die einer Instanz zur Laufzeit zugewiesen wurde, ohne den Datenverkehr zu beeinträchtigen. Mit den gepoolten Kapazitätslizenzen können Sie die Instanz-Provisioning automatisieren.

Um ADC-gepoolte Kapazität zu verwenden, stellen Sie sicher, dass ein ADM-Agent an eine ADC-Instanz angeschlossen wird. ADC-Instanzen checken Lizenzen vom ADM-Dienst über einen Agenten ein und checken sie aus.

Sie können auch gepoolte Kapazitätslizenzen für ADC FIPS-Instanzen verwenden. Sie können die folgenden Aufgaben im ADM-Dienst ausführen:

- Laden Sie die gepoolten Kapazitätslizenzdateien (Bandbreiten-Pool oder Instanz-Pool) auf den Lizenzserver hoch.
- Ordnen Sie ADC-Instanzen nach Bedarf Lizenzen aus dem Lizenzpool zu.
- Überprüfen Sie die Lizenzen von ADC-Instanzen (MPX-Z /SDX-Z/VPX/CPX/BLX) basierend auf der minimalen und maximalen Kapazität der Instanz.



Kapazitätsprobleme mit ADC-Pool-Kapazität

Die gepoolten Kapazitätszustände geben die Lizenzanforderungen für eine ADC-Instanz an. Die ADC-Instanzen, die mit gepoolter Kapazität konfiguriert sind, zeigen einen der folgenden Status an:

- **Optimal**: Die Instanz wird mit der richtigen Lizenzkapazität ausgeführt.
- **Kapazitätskonflikt**: Die Instanz wird mit einer Kapazität ausgeführt, die kleiner ist als der Benutzer konfiguriert.
- **Grace**: Die Instanz wird mit einer Kulanzlizenz ausgeführt.
- **Grace & Mismatch**: Die Instanz wird im Kulanzzeitraum ausgeführt, aber mit einer Kapazität, die geringer ist als der Benutzer konfiguriert.
- **Nicht verfügbar**: Die Instanz ist nicht für die Verwaltung bei ADM registriert, oder die NITRO -Kommunikation von ADM zu den Instanzen funktioniert nicht.

- **Nicht zugewiesen**: Die Lizenz wird in der Instanz nicht zugewiesen.

Voraussetzungen

Stellen Sie vor der Konfiguration der gepoolten Kapazität Folgendes sicher:

- Installieren und registrieren Sie einen Agenten im ADM-Dienst. Informationen zum Installieren und Registrieren eines Agenten finden Sie unter Erste Schritte.
- Die `27000`Ports `7279`und stehen zum Auschecken von Lizenzen von ADM auf eine Instanz zur Verfügung. Siehe,Systemanforderungen

Schritt 1 - Anwenden von Lizenzen in ADM

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Lizenzen**.
2. Wählen Sie im Abschnitt **Lizenzdateien** die Option **Lizenzdatei hinzufügen** aus, und wählen Sie eine der folgenden Optionen aus:
   - **Laden Sie Lizenzdateien von einem lokalen Computer**hoch. Wenn eine Lizenzdatei bereits auf Ihrem lokalen Computer vorhanden ist, können Sie sie auf ADM hochladen.
   - **Lizenzzugriffscode verwenden**. Geben Sie den Lizenzzugriffscode für die Lizenz an, die Sie von Citrix erworben haben. Wählen Sie dann **Lizenzen abrufen**aus. Wählen Sie dann **Fertig stellen**aus.

   > **Hinweis:**Sie können ADM
   >
   > jederzeit über die **Lizenzeinstellungen**weitere Lizenzen hinzufügen.
3. Klicken Sie auf **Fertig stellen**.

   Die Lizenzdateien werden ADM hinzugefügt. Auf der Registerkarte **Lizenzablaufinformationen** werden die im ADM vorhandenen Lizenzen und die verbleibenden Tage bis zum Ablauf aufgeführt.
4. Wählen Sie **unter Lizenzdateien**eine Lizenzdatei aus, die Sie anwenden möchten, und klicken Sie auf **Lizenzen anwenden**.

   Mit dieser Aktion können ADC-Instanzen die ausgewählte Lizenz als gepoolte Kapazität verwenden.

Schritt 2 - Registrieren des ADM-Dienstes als Lizenzserver

Sie können den ADM-Dienst mit einem Agenten als Lizenzserver bei einer Citrix ADC-Instanz registrieren.

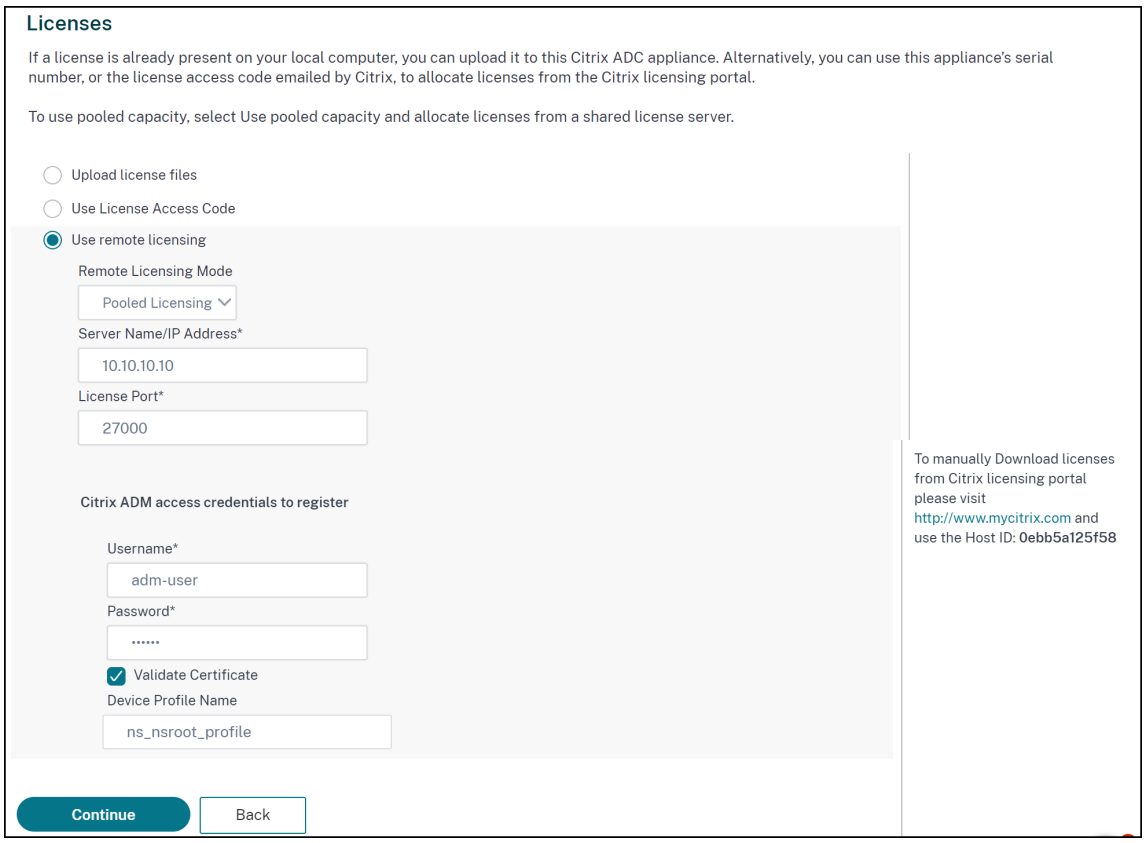
Verwenden Sie eines der folgenden Verfahren, um den ADM-Dienst als Lizenzserver zu registrieren:

- GUI verwenden
- CLI verwenden

Verwenden der GUI zum Registrieren eines ADM-Agenten

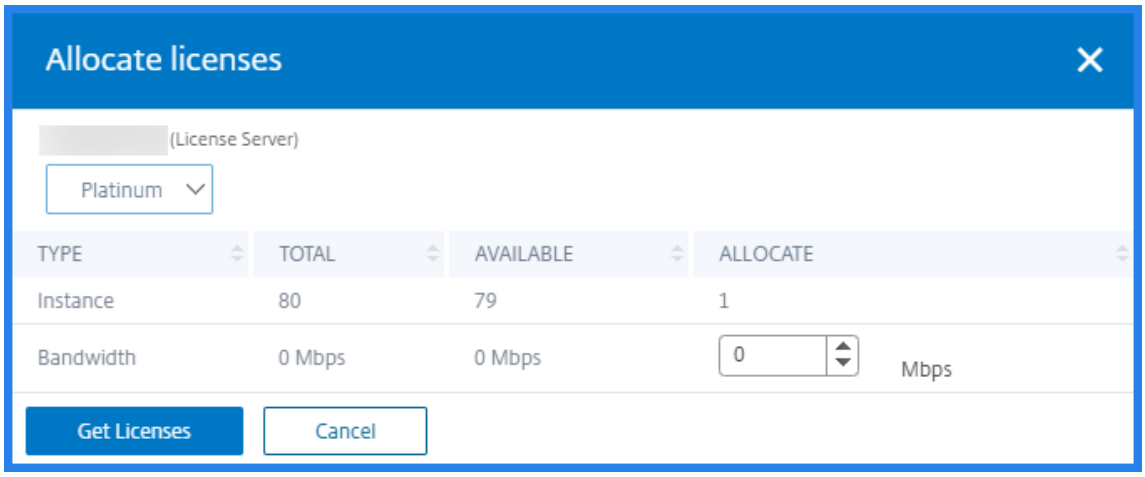
Registrieren Sie in der ADM-GUI den ADM-Agenten, der einer ADC-Instanz zugeordnet ist.

1. Melden Sie sich bei Citrix ADC GUI an.
2. Navigieren Sie zu **System** > **Lizenzen** > **Lizenzen verwalten**.
3. Klicken Sie auf **Neue Lizenz hinzufügen**.
4. Wählen Sie **Remote-Lizenzierung verwenden**, und wählen Sie den Remote-Lizenzierungsmodus aus der Liste aus.
5. Geben Sie im Feld **Servername/IP-Adresse** die IP-Adresse des zugeordneten ADM-Agenten an, der beim ADM-Dienst registriert ist.
6. Wählen Sie **Mit Citrix ADM registrieren**aus.
7. Geben Sie Ihre ADM-Anmeldeinformationen ein, um eine Instanz bei Citrix ADM zu registrieren, und klicken Sie auf **Weiter**.



8. Wählen Sie unter **Lizenzen zuweisen**die Lizenzedition aus, und geben Sie die erforderliche Bandbreite an.

Weisen Sie erstmals Lizenzen in Citrix ADC zu. Sie können die Lizenzzuweisung später von der Citrix ADM GUI ändern oder freigeben.



9. Klicken Sie auf **Get Licenses**.

> **Wichtig**
>
> Starten Sie die Instanz warm neu, wenn Sie die Lizenzversion ändern. Die Konfigurationsänderungen werden erst wirksam, wenn Sie die Instanz neu starten.

Verwenden der CLI zum Hinzufügen eines ADM-Agenten

Wenn eine ADC-Instanz keine GUI hat, verwenden Sie die folgenden CLI-Befehle, um einen ADM-Agent hinzuzufügen, der einer Instanz zugeordnet ist:

1. Melden Sie sich bei der Citrix ADC Konsole an.
2. Fügen Sie die IP-Adresse des zugeordneten ADM-Agenten hinzu, die beim ADM-Dienst registriert ist:

```
1 > add ns licenseserver <adm-agent-IP-address> -port <adm-agent-
    license-port-number>
2 <!--NeedCopy-->
```

3. Zeigen Sie die auf dem Lizenzserver verfügbare Lizenzbandbreite an:

```
1 > sh ns licenseserverpool
2 <!--NeedCopy-->
```

4. Weisen Sie die Lizenzbandbreite aus der erforderlichen Lizenzedition zu:


```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth
    > edition <specify-license-edition>
<!--NeedCopy-->
```

Die Lizenzausgabe kann **Standard** oder **Advanced** oder **Premium**sein.

> **Wichtig**
>
> Warm starten Sie die Instanz neu, wenn Sie die Lizenzversion ändern.
>
> `reboot -w`
>
> Die Konfigurationsänderungen werden erst wirksam, wenn Sie die Instanz neu starten.

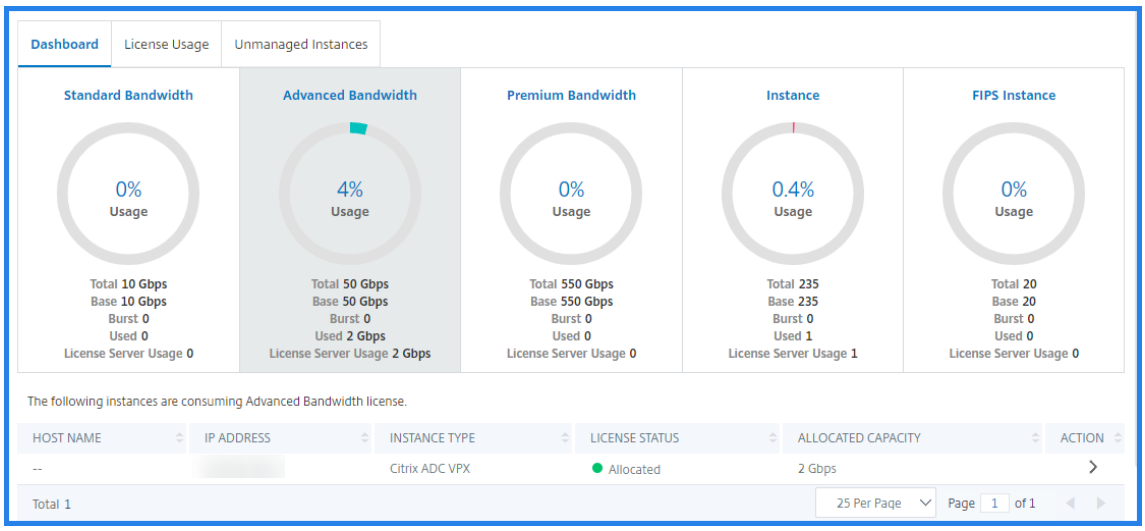
Schritt 3: Zuweisen von gepoolten Lizenzen zu ADC-Instanzen

So weisen Sie gepoolte Kapazitätslizenzen von der ADM-GUI zu:

1. Melden Sie sich bei Citrix ADM an.
2. Navigieren Sie zu **Netzwerke > Lizenzen > Bandbreitenlizenzen > Pooled Capacity**.

   Die Kapazität der FIPS-Instanz wird nur angezeigt, wenn Sie FIPS-Instanzlizenzen in ADM hochladen.
3. Klicken Sie auf den Lizenzpool, den Sie verwalten möchten.

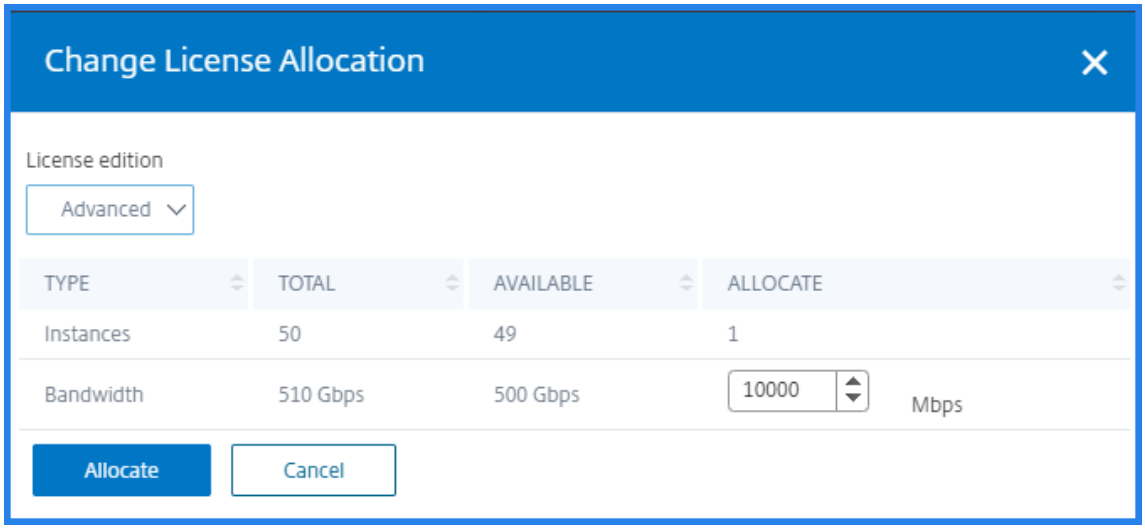
   > **Hinweis:**
   >
   > Das Feld **Zugewiesene Kapazität** spiegelt die geänderte Bandbreite nicht sofort wieder. Die Bandbreitenänderung wird nach dem ADC-Warm-Neustart wirksam.
   >
   > In **Allocation Details**werden die Felder **Angefordert** und **Angewendet** aktualisiert, wenn Sie die Bandbreitenzuweisung der Instanz ändern.
4. Wählen Sie eine ADC-Instanz aus der Liste der verfügbaren Instanzen aus, indem Sie auf die Schaltfläche **klicken.



In der Spalte Lizenzstatus werden entsprechende Lizenzzuordnungsstatusmeldungen angezeigt.

> **Hinweis**
>
> Die Registerkarte **Unmanaged Instanzen** zeigt die Instanzen an, die in Citrix ADM erkannt, aber nicht verwaltet werden.
>
> 
>

5. Klicken Sie auf **Zuweisung ändern** oder **Zuweisung freigeben**, um die Lizenzzuweisung zu ändern.
6. Ein Popup-Fenster mit den verfügbaren Lizenzen im Lizenzserver wird angezeigt.
7. Sie können die Bandbreite oder die Instanzzuweisung für die Instanz auswählen, indem Sie die Optionen für die Liste Zuordnen festlegen. Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie auf **Zuweisen**.
8. Sie können die zugewiesene Lizenzedition auch über die Listenoptionen im **Fenster Lizenzzuweisung ändern** ändern.



> **Hinweis**
>
> Warm starten Sie eine Instanz neu, wenn Sie die Lizenzversion ändern.

Konfigurieren der gepoolten Kapazität auf ADC-Instanzen

Sie können gepoolte Kapazitätslizenzen für die folgenden ADC-Instanzen konfigurieren:

- ADC MPX-Z-Instanzen
- ADC VPX-Instanzen
- ADC-Hochverfügbarkeitspaar

Citrix ADC MPX-Z-Instanzen

MPX-Z ist die aktivierte ADC-MPX-Appliance mit Poolkapazität. MPX-Z unterstützt Bandbreiten-Pooling für Premium-, Advanced- oder Standard Edition-Lizenzen.

MPX-Z erfordert Plattformlizenzen, bevor es eine Verbindung zum Lizenzserver herstellen kann. Sie können die MPX-Z-Plattformlizenz mit einer der folgenden Optionen installieren:

- Hochladen der Lizenzdatei von einem lokalen Computer.
- Verwenden der Hardware-Seriennummer der Instanz.
- Der Lizenzzugriffscode aus dem Abschnitt **System** > **Lizenzen** der Benutzeroberfläche der Instanz.

Wenn Sie die MPX-Z-Plattformlizenz entfernen, ist die Funktion “Pooled Capacity” deaktiviert. Die Instanzlizenzen werden für den Lizenzserver freigegeben.

Sie können die Bandbreite einer MPX-Z-Instanz ohne Neustart dynamisch ändern. Ein Neustart ist nur erforderlich, wenn Sie die Lizenzversion ändern möchten.

> **Hinweis**
>
> Wenn Sie die Instanz neu starten, werden die für die konfigurierte Kapazität erforderlichen Lizenzen automatisch ausgecheckt.

Citrix ADC VPX Instanzen

Eine gepoolte ADC VPX-Instanz mit aktivierter Kapazität kann Lizenzen aus einem Bandbreitenpool auschecken (Premium/Advanced/Standard Editionen). Sie können die ADC-GUI verwenden, um Lizenzen vom Lizenzserver auszuchecken.

Sie können die Bandbreite einer VPX-Instanz ohne Neustart dynamisch ändern. Ein Neustart ist nur erforderlich, wenn Sie die Lizenzversion ändern möchten.

> **Hinweis**
>
> Wenn Sie die Instanz neu starten, werden die konfigurierten Pool-Kapazitätslizenzen automatisch vom ADM-Server ausgecheckt.

Citrix ADC Hochverfügbarkeitspaar

Bevor Sie beginnen, stellen Sie sicher, dass der ADM-Server als Lizenzserver konfiguriert ist. Weitere Informationen finden Sie unter Konfigurieren von ADM als Lizenzserver.

Wenn Sie einem ADC-HA-Paar die Bandbreite zuweisen, checkt Citrix ADM dieselbe Bandbreite für primäre und sekundäre Instanzen aus. Wenn Sie einem ADC-HA-Paar 10 Mbit/s Bandbreite zuweisen, führt ADM die folgenden Schritte aus:

1. Checkt 20 Mbit/s Bandbreite an das HA-Paar aus.
2. weist jeder Instanz im HA-Paar 10 Mbit/s zu.

Informationen zum Zuweisen einer Poollizenz zu einem ADC-HA-Paar finden Sie unter Zuweisen von gepoolten Lizenzen zu ADC-Instanzen.

Auf der Seite " **Pooled Capacity** " werden die Instanzen und ihre zugewiesene Kapazität separat angezeigt. Wenn Sie die Bandbreite der primären Instanz ändern oder freigeben, wird die Bandbreite der sekundären Instanz automatisch mit der primären Instanz synchronisiert. Die Synchronisierung erfolgt jedoch nicht, wenn Sie die Bandbreite der sekundären Instanz ändern oder freigeben.

Konfigurieren Sie den ADM-Dienst nur für die gepoolte Lizenzierungsfunktion

April 28, 2021

Als Administrator können Sie den ADM-Service nur für die gepoolte Lizenzierungsfunktion konfigurieren. Bei dieser Konfiguration erhält der ADM-Dienst nur Lizenzdaten von ADC-Instanzen.

Manchmal haben Sie möglicherweise das regulatorische Mandat, das erfordert, dass die Daten von ADC-Instanzen daran gehindert werden, den regulatorischen Bereich zu verlassen. In solchen Situationen können Sie eine lokale Instanz eines ADM-On-Prem-Servers in Ihrer regulatorischen Zone bereitstellen, um Verwaltungs-, Überwachungs- und Analysefunktionen zu nutzen. Wenn Sie den gleichen Ansatz zur Verwendung der Funktion für gepoolte Lizenzen wählen, müssen Sie gepoolte Lizenzen auf verschiedene ADM-Lizenzserver aufteilen. Dieser Ansatz bietet Ihnen nicht die Flexibilität, gepoolte Lizenzen für Ihre global bereitgestellten ADC-Instanzen zuzuweisen.

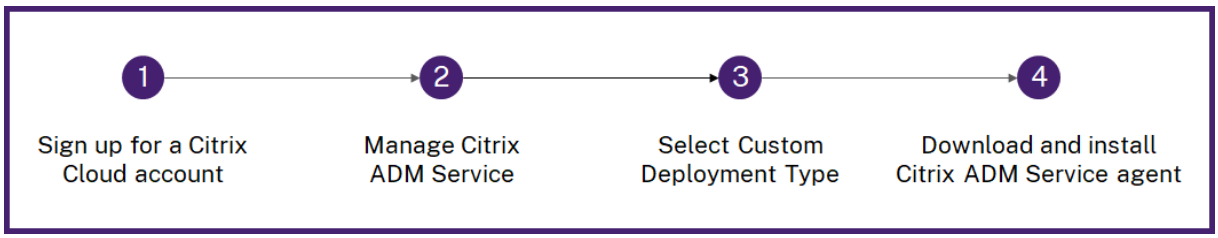
Konfigurieren Sie daher den ADM-Service nur für die gepoolte Lizenzierungsfunktion. Der ADM-Dienst erhält nur Lizenzdaten von allen ADC-Instanzen. So können Sie das regulatorische Mandat einhalten und global bereitgestellte ADC-Instanzen dynamisch gepoolte Kapazitätslizenzen zuweisen.

In diesem Dokument wird erläutert, wie der ADM-Service nur für die gepoolte Lizenzierungsfunktion konfiguriert wird.

Voraussetzungen

Bevor Sie den ADM-Service nur für die gepoolte Lizenzierungsfunktion konfigurieren, schließen Sie das erste Onboarding ab und richten Sie den ADM-Service ein. Stellen Sie sicher, dass Sie die Agentenspezifikationen in Systemanforderungenüberprüfen

> **Wichtig**
>
> Wenn Sie den ADM-Service zum ersten Mal an Bord haben oder einrichten, stellen Sie Folgendes sicher:
>
> - Die Option “Benutzerdefinierte Bereitstellung” ist ausgewählt.
> - ADC-Instanzen, die hinzugefügt werden, nachdem Sie Schritt 4 abgeschlossen haben konfiguration proze.



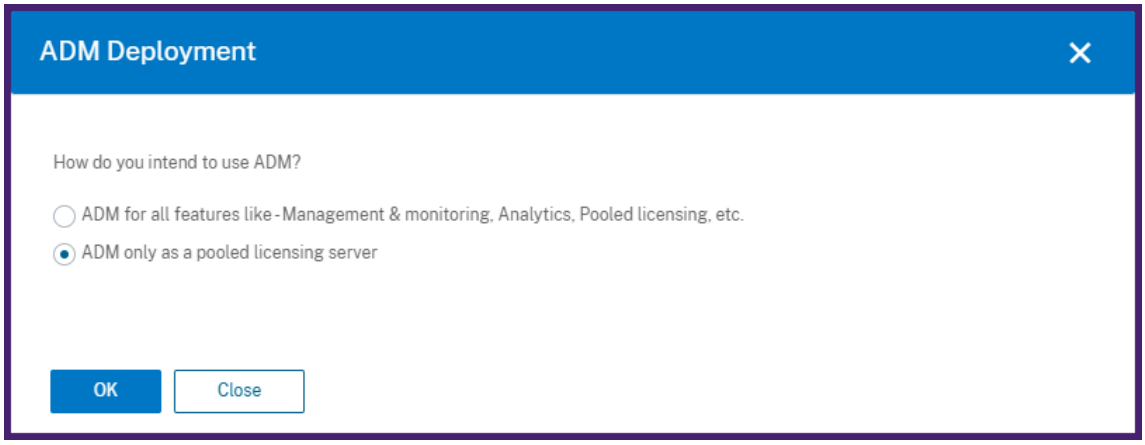
Weitere Informationen zum Onboarding und zur Einrichtung des ADM-Dienstes finden Sie unter Erste Schritte.

Nachdem Sie die Onboarding-Schritte abgeschlossen haben, konfigurieren Sie den ADM-Service nur für die gepoolte Lizenzierungsfunktion.

So konfigurieren Sie den ADM-Service nur für die gepoolte Lizenzierungsfunktion

Gehen Sie folgendermaßen vor, um den ADM-Dienst nur für die Lizenzierungsfunktion zu konfigurieren:

1. Navigieren Sie zu **Konto > Administration**.
2. Wählen Sie im Abschnitt " **Systemkonfigurationen** " die Option **Systembereitstellung**aus.
3. Wählen Sie in **ADM Deploymentnur ADM als gepoolten Lizenzserver**aus.



4. Klicken Sie auf **OK**.

   Diese Aktion behält nur die gepoolte Lizenzierungsfunktion bei und deaktiviert die folgenden ADM-Features:

   - ADM-Backup
   - Event-Management
   - SSL Zertifikatsverwaltung
   - Netzwerkberichterstattung
   - Netzwerkfunktionen
   - Konfigurations-Audit

   > **Hinweis**
   >
   > Standardmäßig ist die ADM-Analytics-Funktion deaktiviert. Stellen Sie sicher, dass Sie diese Funktion deaktivieren, wenn Sie sie aktiviert haben.

   Klicken Sie im Bestätigungsfeld auf **Ja**.

   Die ADM-Benutzeroberfläche zeigt jetzt nur die gepoolte Lizenzierungsfunktion an. Und die übrigen Funktionen werden nicht angezeigt.

5. Nachdem Sie ADM nur für die Lizenzierungsfunktion konfiguriert haben, fügen Sie ADC-Instanzen auf der Seite **Netzwerke > Instanzen** hinzu.

Hinweis

- Sie können eine ADC-Instanz im ADM-Dienst und anderen ADM-Servern hinzufügen. Wenn Sie das Kennwort solcher ADC-Instanzen ändern, müssen Sie das Kennwort auf allen ADM-Servern aktualisieren, auf denen die Instanz erkannt wird. Dieser Hinweis gilt, wenn der ADM-Dienst nur für die Verwendung der gepoolten Lizenzierungsfunktion konfiguriert ist.
- Ein Benutzer kann weiterhin einige Vorgänge der deaktivierten Funktionen in der ADM-Benutzeroberfläche ausführen. Zum Beispiel Ereignisabfrage und ADC-Backup. Wenn Sie solche Vorgänge einschränken möchten, deaktivieren Sie als Superadministrator die Benutzerzugriffe für andere Administratoren mithilfe einer entsprechenden Zugriffsrichtlinie. Weitere Informationen finden Sie unter Konfigurieren von Zugriffsrichtlinien auf Citrix ADM.

Anwenden einer neuen Lizenz auf ADM für ein bestehendes Setup mit gepoolter Kapazität

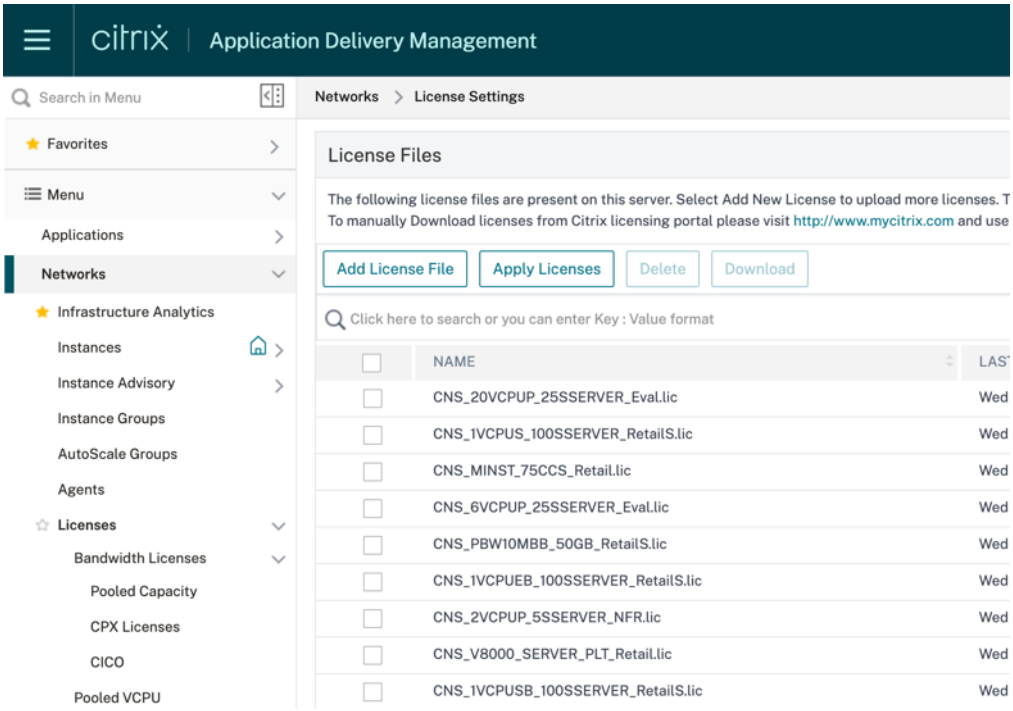
April 28, 2021

In diesem Thema wird beschrieben, wie eine neue Lizenz auf Citrix ADM für ein vorhandenes Setup mit gepoolter Kapazität angewendet wird. Bevor Sie sich bei ADM bewerben können, benötigen Sie eine Lizenzdatei. Wenn eine Lizenzdatei bereits auf Ihrem lokalen Computer vorhanden ist, können Sie sie auf den ADM-Lizenzserver hochladen. Alternativ können Sie den von Citrix per E-Mail gesendete Lizenzzugriffscode verwenden, um Lizenzen aus dem Citrix Lizenzierungsportal zuzuweisen.

Verwenden Sie die GUI **ADM > Networks** Licenses, um alle gepoolten Kapazitätslizenzdateien zu verwalten und bereitzustellen.

Überprüfen Sie den Status bestehender Lizenzen und Pools

Sie können die in ADM verfügbaren Lizenzen überprüfen, indem Sie zu **Netzwerke > Lizenzen**navigieren.

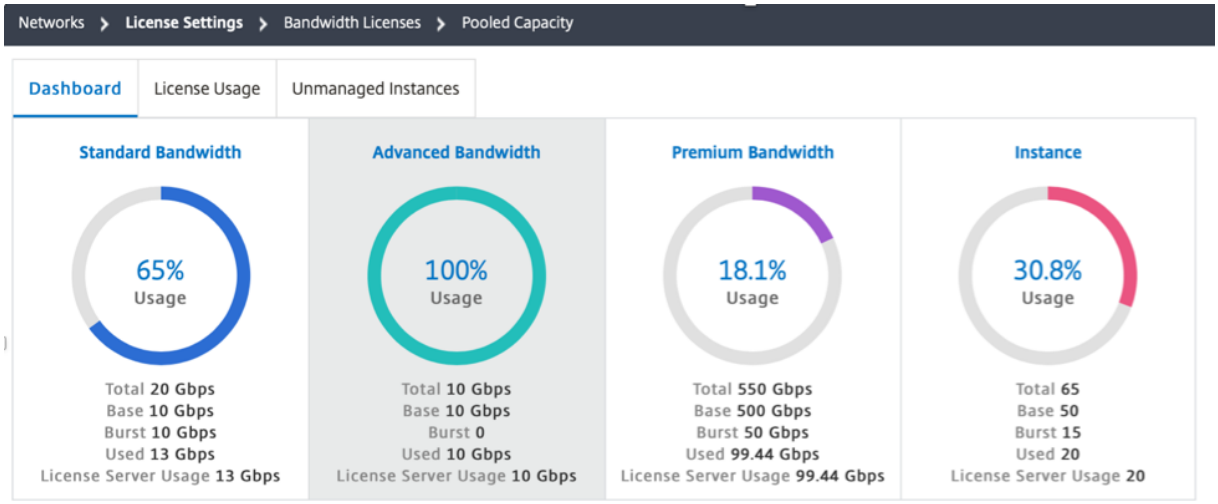


Scrollen Sie nach unten, um zu sehen, die in der Tabelle **Informationen zum Lizenzablauf** mit Ablaufdaten verfügbar sind.

License Expiry Information

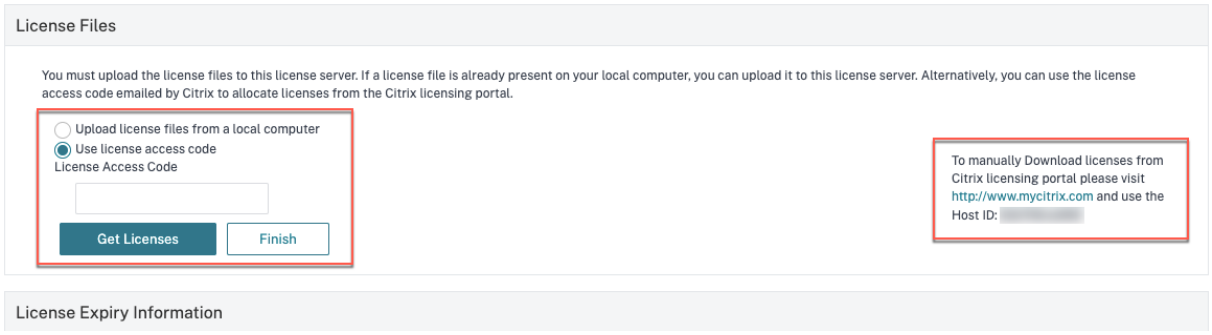
FEATURE	COUNT	DAYS TO EXPIRY
Standard Bandwidth	10,000	71
Platinum vCPU	100	71
VPX 8Gbps Enterprise Edition	1	71
Enterprise vCPU	100	71
Burst Platinum vCPU	100	71
Standard vCPU	100	71
Burst Enterprise vCPU	100	71
Burst Standard Bandwidth	10,000	71
VPX 8Gbps Standard Edition	1	71
Burst Platinum Bandwidth	50,000	71

Um verfügbare Pools für verschiedene Editionen zu überprüfen, navigieren Sie zu **Netzwerke > Lizenzen > Bandbreitenlizenzen > Pool-Kapazität**



Weisen Sie eine neue Lizenz zu

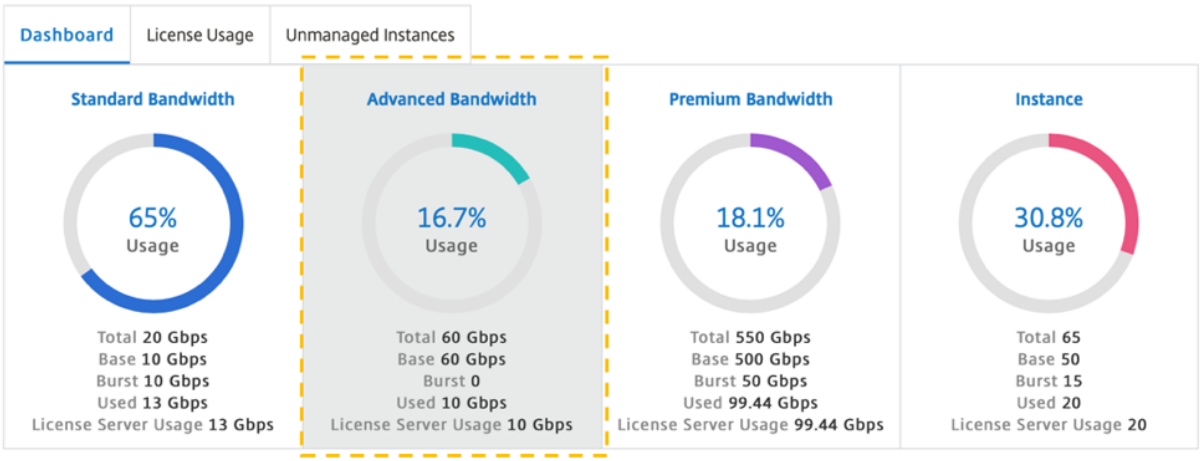
Wenn Sie keine bereits verfügbare Lizenz auf Ihrem lokalen Computer haben, können Sie die Lizenz mit dem von Citrix bereitgestellten Zugangscode zuweisen oder mithilfe der in der GUI angegebenen Host-ID aus dem Citrix Lizenzierungsportal herunterladen. Weitere Informationen zum Herunterladen von Lizenzen aus dem Citrix Lizenzierungsportal finden Sie im Supportartikel Citrix Lizenzierung.



Eine neue Lizenz beantragen

Befolgen Sie diese Schritte, um eine heruntergeladene Lizenzdatei anzuwenden.

1. Navigieren Sie zu **Netzwerke > Lizenzen**und klicken Sie auf **Lizenzdatei hinzufügen**.
2. Klicken Sie auf " **Durchsuchen**" und laden Sie die neue Lizenz hoch.
3. Klicken Sie auf **Fertig stellen**. Auf der Seite Lizenzeinstellungen können Sie jederzeit weitere Lizenzen hinzufügen.
4. Nachdem die Lizenz hinzugefügt wurde, zeigt das Dashboard für gepoolte Kapazität die neue Verfügbarkeitskapazität an.



Eine Lizenz löschen

Gehen Sie folgendermaßen vor, um eine vorhandene Lizenz zu löschen.

1. Navigieren Sie zu **Netzwerke -> Lizenzen**.
2. Wählen Sie die Lizenz aus und klicken Sie auf **Löschen**, um die Lizenz jederzeit zu entfernen.

ADM checkt automatisch die angeforderte Lizenz für ADC aus dem neuen Pool aus.

1. Um für den ausgewählten ADC die Bandbreitenzuweisung zu ändern, klicken Sie auf **Zuweisen**, um den ausgewählten Pool zu ändern.

FAQs und andere Ressourcen

April 28, 2021

In diesem Abschnitt werden die Referenzdokumentationen zur Konfiguration und zum Betrieb von Pool-Lizenzierung aufgeführt. Sie können sich auf diese Dokumente beziehen, um Unterstützung in Bezug auf Konfigurations- und Betriebsprobleme zu erhalten.

Konfiguration

1. Wo finde ich Informationen über den Überblick und die Merkmale der gepoolten Kapazität?

   Antwort: Siehe Citrix ADC-gepoolte Kapazität - Validiertes Referenzdesign.

2. Wie konvertiere oder migriere ich unbefristet zu gepoolten Lizenzen und umgekehrt?

   Antwort: Die Umwandlung von einer unbefristeten Lizenz auf eine gebündelte Kapazitätslizenz ist ein unidirektionaler Lizenzanspruchsprozess. Sie können die gepoolte Kapazitätslizenz nicht auf unbefristet zurücksetzen.

3. Wie stelle ich den ADM-Server bereit?

   Antwort: Folgen Sie dem Erste Schritte Dokument.

4. Wie füge ich einer bestehenden gepoolten Lizenz eine neue Lizenz hinzu und weise sie zu?

   Antwort: Folgen Sie dem Anwenden einer neuen Lizenz auf ADM für ein bestehendes Setup mit gepoolter Kapazität Dokument.

5. Wie ordne ich Kapazität und Bandbreite für Instanzen zu bzw. erhöhen?

   Antwort: Folgen Sie dem Anwenden einer neuen Lizenz auf ADM für ein bestehendes Setup mit gepoolter Kapazität Dokument.

Häufige Probleme

1. Instanzen, die im Gnadenmodus aufgrund von Verbindungsfehlern, Upgrades, Splitbrain und anderen ausgeführt werden.

   Antwort: Siehe das in dokumentierte Verhalten des ADM-Lizenzservers Konfigurieren der gepoolten Citrix ADC-Kapazität.

2. Lizenzen, die keine Instanzen anwenden oder reflektieren.

   Antwort: Siehe Best Practices, Eckfälle und häufig gestellte Fragen.

3. Die Lizenzzuweisung befindet sich im “Sync in Prognose-Bearbeitung”.

   Antwort: Siehe Best Practices, Eckfälle und häufig gestellte Fragen.

4. Fehler aufgrund einer falschen Host-ID in der Lizenzdatei.

   Antwort: Um einen Server mit Citrix Application Delivery Management (ADM) zu identifizieren, können Sie dem Server einen Hostnamen zuweisen. Der Hostname wird in der universellen Lizenz für Citrix ADM angezeigt. Weitere Informationen finden Sie unter Zuweisen eines Hostnamens zu einem Citrix ADM-Server.

5. Probleme aufgrund bekannter oder behobener Fehler

   Antwort: Lesen Sie das VersionshinweiseSystemanforderungen, und Lizenzen.

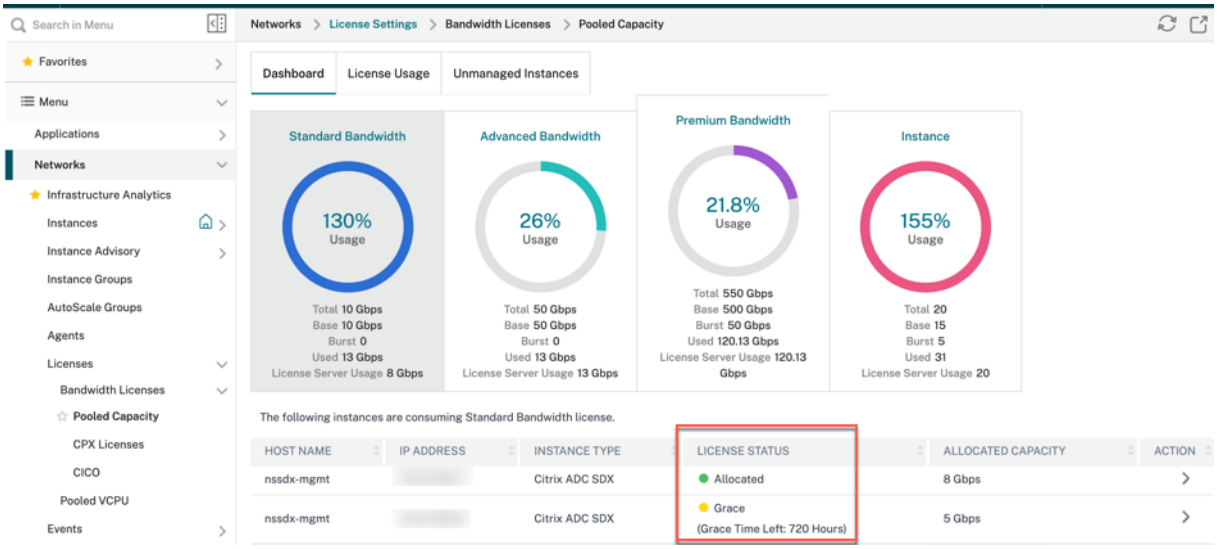
Beheben von Lizenzproblemen mit gepoolter Kapazität

April 28, 2021

In diesem Abschnitt wird beschrieben, wie häufig Probleme mit der gepoolten Kapazität analysiert und behoben werden.

Überprüfen Sie den Lizenzstatus

Der ADM fungiert als Lizenzserver für Ihre ADC-gebündelte Kapazitätslizenz. Sie können die ADM-GUI verwenden, um den Status der Lizenz zu überprüfen. Navigieren Sie zu **Netzwerke > Lizenzen > Gepoolte Kapazität > Lizenznutzung**.



In der folgenden Tabelle sind die Arten des Lizenzstatus aufgeführt und was sie bedeuten

Status	was es bedeutet
Zugeteilt	Der Lizenzstatus ist in Ordnung.
Zugeteilt: nicht auf ADC angewendet	Citrix ADC erfordert möglicherweise einen Neustart, wenn die Lizenz von ADC ausgecheckt oder eingecheckt ist, Citrix ADC jedoch noch nicht neu gestartet wurde.
Nicht zugeteilt	Die Lizenz ist in der ADC-Instanz nicht zugewiesen.
Kulanzzeitraum	Die Citrix ADC-Instanz befindet sich 30 Tage lang in der Kulanzzeit der Lizenz
Synchronisierung wird ausgeführt	Citrix ADM holt Informationen in 2-Minuten-Intervallen von Citrix ADC ab. Die Synchronisierung von Lizenzen zwischen Citrix ADM und Citrix ADC kann bis zu 15 Minuten dauern. Citrix ADM wurde möglicherweise neu gestartet, oder ADM HAS-Failover wird ausgelöst.

Status	was es bedeutet
Teilweise zugeordnet	Citrix ADC kann die zugewiesene Kapazität nicht akzeptieren, da sie möglicherweise mit ihrer maximalen Zuweisung ausgeführt wird. Citrix ADC wird beispielsweise mit einer Kapazität von 10 Gbit/s -Lizenzpools ausgeführt. Beim Neustart von ADC werden die 10 Gbit/s wieder an den ADM-Lizenzserver eingecheckt. Wenn Citrix ADC wieder online kommt, versucht er, die zuvor zugewiesenen 10 Gbit/s automatisch auszuchecken. In der Zwischenzeit könnten andere ADC-Instanzen diese Bandbreite ausgecheckt haben. Teilweise zugewiesen wird angezeigt, wenn der Lizenzpool nicht über genügend Kapazität verfügt, um diesem ADC vollständige 10 Gbit/s oder sogar teilweise Kapazität zuzuweisen.
Nicht verwaltet	Citrix ADC wird ADM aus Verwaltbarkeit nicht hinzugefügt. Dies hat keine Auswirkungen auf die Citrix ADC-Lizenzierung, kann sich jedoch auf die Lizenzüberwachung von ADM auswirken.
Nicht verwaltet	Citrix ADC wird ADM aus Verwaltbarkeit nicht hinzugefügt. Dies hat keine Auswirkungen auf die Citrix ADC-Lizenzierung, kann sich jedoch auf die Lizenzüberwachung von ADM auswirken.
Verbindung unterbrochen	Citrix ADC ist für die Verwaltbarkeit nicht von ADM erreichbar. Beispielsweise gibt es Netzwerkkonnektivitätsprobleme, NITRO funktioniert nicht oder Citrix ADC-Kennwörter nicht übereinstimmen. Wenn NITRO nicht funktioniert oder das Citrix ADC-Kennwort nicht übereinstimmt, hat dies keine Auswirkungen auf die Citrix ADC-Lizenzierung. Es kann sich jedoch auf die Lizenzüberwachung von ADM auswirken.

Überprüfen Sie den Serverstatus

In diesem Abschnitt werden die allgemeinen Probleme mit dem Serverstatus und mögliche Gründe und Korrekturen beschrieben.

Problem: ADC zeigt Lizenzserver als nicht erreichbar an und Änderungen des Lizenzstatus in Gnade.

- Die Verbindung zum Lizenzserver (ADM oder ADM Service Agent) wurde seit mehr als 15 Minuten unterbrochen. Überprüfen Sie, ob der Lizenzserver betriebsbereit und erreichbar ist.
- ADC befindet sich im Gnadenmodus.

Problem: ADC zeigt den Lizenzserverstatus als erreichbar an, aber der Versuch des Benutzers, die Zuweisung zu ändern, hat keine Auswirkungen. Wenn Sie auf **Zuordnung ändern** klicken, wird 0 0 zurückgegeben Dieser Wert könnte den Anschein erwecken, dass die konfigurierte Kapazität verloren gegangen ist.

- Die Verbindung zum Lizenzserver wurde kürzlich unterbrochen, aber der ADC hat den zweiten Takt immer noch nicht verpasst. Daher ist es (noch) nicht in Grace. Überprüfen Sie, ob der Lizenzserver betriebsbereit und erreichbar ist.

Problem: ADC zeigt Kapazitäts- und Instanzanzanzahlen an, aber der Lizenzserver ist **erreichbar/nicht erreichbar**. Wenn Sie auf **Zuordnung ändern** klicken, werden einige Zahlen zurückgegeben, die konfigurierte Kapazität wird jedoch nicht berücksichtigt.

- Die Verbindung zum Lizenzserver wurde wiederhergestellt, aber der ADC soll immer noch den zweiten Heartbeat verpassen oder den Wiederverbindungstest senden.

Problem: ADC sagt, dass keine Verbindung zum Lizenzserver hergestellt werden kann, wenn Pooled Licensing mit ADM-Dienst konfiguriert wird

- Überprüfen Sie die Firewall-Regeln, um sicherzustellen, dass Port 27000 und 7279 offen sind.
- Der Agent ist nicht registriert. Weitere Informationen finden Sie unter Erste Schritte.
- Der ADM-Dienst hat keine Lizenzdateien hochgeladen. Weitere Informationen finden Sie unter Konfigurieren der gepoolten Citrix ADC Kapazität
- ADM hat die falschen Lizenzdateidateien.

Überprüfen Sie den Nutzungsbericht der Lizenz

Unter **Netzwerke > Lizenzen > Pooled Capacity > Lizenznutzung** in der ADM-GUI sehen Sie den monatlichen Höhepunkt Ihrer Lizenznutzung. Sie können diesen Bericht verwenden, um Ihre Lizenznutzung zu erhöhen oder den Kauf einer zusätzlichen Lizenz zu planen.

Im Folgenden finden Sie einige Details, wie der Bericht generiert wird und verwendet werden kann.

Polling: Lizenzdaten werden alle 15 Minuten von den ADC-Instanzen abgefragt.

Aufrechterhaltung der Spitzen pro Stunde: ADM behält nur die maximale Lizenznutzung in einer Stunde pro Gerät bei.

Reporting: Sie können GUI-Berichte für jede Instanz für einen bestimmten Zeitraum erstellen.

Exportieren: Sie können Berichte entweder im CSV-Format oder im XLS-Format exportieren.

Bereinigung: ADM bereinigt Daten am ersten eines jeden Monats um 12:10 Uhr. Der Löschzeitraum ist konfigurierbar (der Standardzeitraum beträgt zwei Monate).

Zähler und Statistiken für gepoolte Kapazitätslizenzierung

Die folgenden Leistungsindikatoren, Protokolle und Befehle legen die gepoolten Lizenzierungsmetriken von Citrix ADC offen, die das Verhalten von ADM- und ADC-Instanzen im gepoolten Lizenzierungsmodus anzeigen.

- **SNMP-Traps**: verfügbar ab ADC-Version 13.xx.
- **NSCONMSG-Zähler für Ratenbegrenzung**: verfügbar ab ADC-Version 12.1 57.xx.
- **ADM-Zähler** ADM-Befehlsaktionen sind in Citrix ADC Cloud Service verfügbar.

SNMP-Fallen

Sie können die folgenden SNMP-Traps konfigurieren v.13 gepoolte Lizenzalarme

- `POOLED-LICENSE-CHECKOUT-FAILURE`
- `POOLED-LICENSE-ONGRACE`
- `Configure POOLED-LICENSE-PARTIAL`

Weitere Informationen zu diesen Alarmen finden Sie unter Citrix ADC SNMP OID Referenz.

NSCONMSG Zähler

Überprüfen Sie die folgenden `NCCONMSG` Leistungsindikatoren und was sie bedeuten:

- `allnic_err_rl_cpu_pkt_drops`: Aggregat (alle NICs) Paket sinkt, nachdem das CPU-Limit erreicht wurde
- `allnic_err_rl_pps_pkt_drops`: Aggregatpaket fällt systemweit nach pps-Limit
- `allnic_err_rl_rate_pkt_drops`: Aggregatrate sinkt systemweit
- `allnic_err_rl_pkt_drops`: Kumulierte ratenbegrenzende Drops aufgrund von Rate, pps und CPU
- `rl_tot_ssl_rl_enforced`: Anzahl der Male, mit der SSL RL angewendet wurde (bei neuen SSL-Verbindungen)
- `rl_tot_ssl_rl_data_limited`: wie oft das SSL-Durchsatzlimit erreicht wurde
- `rl_tot_ssl_rl_sess_limited`: wie oft das SSL TPS-Limit erreicht wurde

ADM-Zähler

Wenn Sie die **Ereignisaktion "Befehlsaktion ausführen"** auswählen, können Sie einen Befehl oder ein Skript erstellen, das auf Citrix ADM für Ereignisse ausgeführt werden kann, die einem bestimmten Filterkriterium entsprechen.
Sie können auch die folgenden Parameter für das Skript **"Befehlsaktion ausführen"** festlegen:

Parameter	Beschreibung
$source	Dieser Parameter entspricht der Quell-IP-Adresse des empfangenen Ereignisses.
$category	Dieser Parameter entspricht der Art der Traps, die in der Kategorie des Filters definiert sind.
$entity	Dieser Parameter entspricht den Entitätsinstanzen oder Leistungsindikatoren, für die ein Ereignis generiert wurde. Es kann die Zählernamen für alle Ereignisse mit Schwellenwert, Entitätsnamen für alle Entitätsbezogenen Ereignisse und Zertifikatnamen für alle zertifikatbezogenen Ereignisse enthalten.
$severity	Dieser Parameter entspricht dem Schweregrad des Ereignisses.
$failureobj	Das Fehlerobjekt wirkt sich auf die Art und Weise aus, wie ein Ereignis verarbeitet wird, und stellt sicher, dass das Fehlerobjekt das genaue Problem wie benachrichtigt wiedergibt. Dies kann verwendet werden, um Probleme schnell aufzuspüren und den Grund für den Fehler zu identifizieren, anstatt einfach rohe Ereignisse zu melden.

> **Hinweis**
>
> Während der Befehlsausführung werden diese Parameter durch tatsächliche Werte ersetzt.

Citrix ADC VPX Ein- und Auschecken Lizenzierung

April 28, 2021

Sie können Citrix ADC VPX-Instanzen bei Bedarf über Citrix Application Delivery Management (ADM) VPX-Lizenzen zuweisen. Die Lizenzen werden von Citrix ADM gespeichert und verwaltet, das über ein Lizenzierungsframework verfügt, das eine skalierbare und automatisierte Provisioning bietet. Eine Citrix ADC VPX Instanz kann die Lizenz vom Citrix ADM auschecken, wenn eine Citrix ADC VPX Instanz bereitgestellt wird, oder ihre Lizenz an Citrix ADM zurückchecken, wenn eine Instanz entfernt oder zerstört wird.

> **Voraussetzungen**: Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:
>
> Sie verwenden ein Citrix ADC VPX Image mit Softwareversion 12.0.
> Beispiel: NSVPX-ESX-12.0-xx.xx_NC.zip.

Installieren von Lizenzen in Citrix ADM

So installieren Sie Lizenzdateien auf dem Citrix ADM:

1. Navigieren Sie zu **Netzwerke** > **Lizenzen**, und klicken Sie auf **Lizenzdatei hinzufügen**.
2. Wählen Sie im Abschnitt Lizenzdateien eine der folgenden Optionen aus:

   - Upload von Lizenzdateien von einem lokalen Computer : Wenn eine Lizenzdatei bereits auf dem lokalen Computer vorhanden ist, können Sie sie in Citrix ADM hochladen.

   Um Lizenzdateien hinzuzufügen, klicken Sie auf Durchsuchen und wählen Sie die Lizenzdatei (.lic) aus, die Sie hinzufügen möchten. Klicken Sie dann auf Fertig stellen.

   - Lizenzzugangscode verwenden - Citrix mailt den Lizenzzugangscode für die Lizenzen, die Sie erwerben.

   Um Lizenzdateien hinzuzufügen, geben Sie den Lizenzzugangscode in das Textfeld ein und klicken Sie dann auf Lizenzen abrufen.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass Sie mit dem Internet verbunden sind, bevor Sie den Lizenzzugangscode für die Installation der Lizenzen verwenden.

Verifizierung

Sie können die verfügbaren und zugewiesenen Lizenzen im Citrix ADM anzeigen.

So zeigen Sie die Lizenzen an

1. Navigieren Sie zu **Netzwerke** > **Lizenz** > **Bandbreitenlizenzen** > **VPX-Lizenzen**.

   Sie können die zugewiesenen Lizenzen in der Tabelle im Abschnitt Verfügbare Lizenzen anzeigen.

Zuweisen von VPX-Lizenzen zu einer Citrix ADC VPX Instanz mithilfe der ADC-GUI

1. Melden Sie sich bei der Citrix ADC VPX Instanz an, navigieren Sie zu **System > Lizenzen > Lizenzen verwalten**, klicken Sie auf **Neue Lizenz hinzufügen**und wählen Sie **Remotelizenzierung verwenden**aus.
2. Geben Sie die Details des Lizenzservers in das Feld **Servername/IP-Adresse** ein.

   > Hinweis
   >
   > Wenn Sie die VPX-Lizenzen Ihrer Instanz über Citrix ADM verwalten möchten, aktivieren Sie das Kontrollkästchen Beim **NetScaler MA Service registrieren**, und geben Sie die Citrix ADM-Anmeldeinformationen ein.

3. Klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster **Lizenzen zuweisen** den Lizenztyp aus. Das Fenster zeigt die Summe und die verfügbaren virtuellen CPUs sowie die zugeordneten CPUs an. Klicken Sie auf **Lizenzen abrufen**.
5. Klicken Sie auf der nächsten Seite auf **Neustart**, um die Lizenzen zu beantragen.

   > **Hinweis**
   >
   > Sie können auch die aktuelle Lizenz freigeben und aus einer anderen Edition auschecken. Beispielsweise führen Sie bereits die Standard Edition-Lizenz für Ihre Instanz aus. Sie können diese Lizenz freigeben und dann in der Advanced Edition auschecken.

6. Sie können die Lizenzzuweisung ändern oder freigeben, indem Sie zu **System** > **Lizenzen > Lizenzenverwalten**navigieren und**Zuordnung ändern oder Zuweisungfreigeben**auswählen.
7. Wenn Sie auf **Zuweisung ändern**klicken, werden in einem Popup-Fenster die auf dem Lizenzserver verfügbaren Lizenzen angezeigt. Wählen Sie die erforderliche Lizenz aus, klicken Sie auf **Lizenzen abrufen**.

Zuweisen von VPX-Lizenz zu einer Citrix ADC VPX Instanz mithilfe von ADC CLI

1. Geben Sie in einem SSH-Client die IP-Adresse der Citrix ADC-Instanz ein, und melden Sie sich mit Administratoranmeldeinformationen an.

2. Geben Sie den folgenden Befehl ein, um einen Lizenzserver hinzuzufügen:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
<!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. Geben Sie den folgenden Befehl ein, um die verfügbaren Lizenzen auf dem Lizenzserver anzuzeigen:

```
sh licenseserverpool
<!--NeedCopy-->
```

```
> sh licenseserverpool
        Instance Total                      : 0
        Instance Available                  : 0
        Standard Bandwidth Total            : 0 Mbps
        Standard Bandwidth Availabe         : 0 Mbps
        Enterprise Bandwidth Total          : 0 Mbps
        Enterprise Bandwidth Available      : 0 Mbps
        Platinum Bandwidth Total            : 0 Mbps
        Platinum Bandwidth Available        : 0 Mbps
        VPX25S Total                        : 1
        VPX25S Available                    : 1
        VPX200E Total                       : 1
        VPX200E Available                   : 1
        VPX1000S Total                      : 1
        VPX1000S Available                  : 1
        VPX8000E Total                      : 2
        VPX8000E Available                  : 1
 Done
```

4. Geben Sie den folgenden Befehl ein, um der VPX-Instanz eine Lizenz zuzuweisen:

```
set capacity  - platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```


Konfigurieren der Ablaufüberprüfungen für Citrix ADC VPX Ein-/Auscheck-Lizenzen

Sie können jetzt den Lizenzablaufschwellenwert für Citrix ADC VPX -Lizenzen konfigurieren. Durch Festlegen von Schwellenwerten sendet Citrix ADM Benachrichtigungen per E-Mail oder SMS, wenn eine Lizenz abläuft. Ein SNMP-Trap und eine Benachrichtigung werden ebenfalls gesendet, wenn die Lizenz auf Citrix ADM abgelaufen ist.

Ein Ereignis wird generiert, wenn eine Lizenzablaufbenachrichtigung gesendet wird und dieses Ereignis in Citrix ADM angezeigt werden kann.

So konfigurieren Sie Lizenzablaufprüfungen

1. Navigieren Sie zu **Netzwerke** > **Lizenzen**.
2. Auf der Seite **Lizenzeinstellungen** finden Sie im Abschnitt **Informationen zum Ablauf der Lizenz** die Details der Lizenzen, die ablaufen werden:
    - Feature: Art der Lizenz, die ablaufen wird.
    - Anzahl: Anzahl der betroffenen virtuellen Server oder Instanzen.
    - Tage bis zum Ablauf: Anzahl der Tage vor Ablauf der Lizenz.
3. Klicken Sie im Abschnitt **Benachrichtigungseinstellungen** auf das Symbol Bearbeiten, und geben Sie den Alarmschwellenwert an. Sie können einen Prozentsatz der Pool-Lizenzkapazität festlegen, der für die Benachrichtigung von Administratoren verwendet wird.
4. Wählen Sie die Art der Benachrichtigung, die Sie senden möchten, indem Sie das entsprechende Kontrollkästchen aktivieren. Die Benachrichtigungstypen sind wie folgt:
    - E-Mail-Profil: Geben Sie einen E-Mail-Server und Profildetails an. Eine E-Mail wird ausgelöst, wenn Ihre Lizenzen ablaufen.
    - SMS-Profil: Geben Sie einen SMS-Server (Short Message Service) und Profildetails an. Eine SMS-Nachricht wird ausgelöst, wenn Ihre Lizenzen ablaufen.
    - Slack profil: Geben Sie einen Pufferkanal an. Eine Benachrichtigung wird gesendet, wenn Ihre Lizenzen ablaufen.
5. Geben Sie dann die Anzahl der Tage bis zum Ablauf der Lizenz an, die Sie mit dem Empfang der Benachrichtigung beginnen möchten.
6. Klicken Sie auf **Save**.

Citrix ADC virtuelle CPU-Lizenzierung

April 28, 2021

Rechenzentrumsadministratoren wie Sie wechseln zu neueren Technologien, die Netzwerkfunktionen vereinfachen und gleichzeitig geringere Kosten und Skalierbarkeit bieten. Eine neuere Rechenzentrumsarchitektur muss mindestens die folgenden Features enthalten:

- Software-Defined Networking (SDN)
- Virtualisierung von Netzwerkfunktionen (NFV)
- Netzwerkvirtualisierung (NV)
- Micro-Services

Eine solche Bewegung muss auch, dass die Softwareanforderungen dynamisch, flexibel und agil sind, um die sich ständig ändernden Geschäftsanforderungen zu erfüllen. Es wird erwartet, dass Lizenzen von einem zentralen Management-Tool verwaltet werden, das volle Einblick in die Nutzung bietet.

Virtuelle CPU-Lizenzierung für Citrix ADC VPX

Zuvor wurden Citrix ADC VPX -Lizenzen basierend auf dem Bandbreitenverbrauch durch die Instanzen zugewiesen. Ein Citrix ADC VPX ist auf die Verwendung einer bestimmten Bandbreite und anderer Performance-Metriken basierend auf der Lizenzedition beschränkt, an die er gebunden ist. Um die verfügbare Bandbreite zu erhöhen, müssen Sie ein Upgrade auf eine Lizenzedition durchführen, die mehr Bandbreite bereitstellt. In bestimmten Szenarien kann die Bandbreitenanforderung geringer sein, aber die Anforderung ist mehr für andere L7-Leistung wie SSL TPS, Komprimierungsdurchsatz usw. Ein Upgrade der Citrix ADC VPX -Lizenz ist in solchen Fällen möglicherweise nicht geeignet. Möglicherweise müssen Sie jedoch noch eine Lizenz mit großer Bandbreite kaufen, um die für die CPU-intensive Verarbeitung erforderlichen Systemressourcen freizuschalten. Citrix Application Delivery Management (ADM) unterstützt jetzt die Zuweisung von Lizenzen zur Citrix ADC-Instanz basierend auf den Anforderungen der virtuellen CPU.

In der virtuellen CPU-Usage-basierten Lizenzierungsfunktion gibt die Lizenz die Anzahl der CPUs an, auf die ein bestimmtes Citrix ADC VPX berechtigt ist. Citrix ADC VPX kann daher Lizenzen nur für die Anzahl der virtuellen CPUs, die auf dem Server ausgeführt werden, vom Lizenzserver auschecken. Citrix ADC VPX checkt Lizenzen je nach Anzahl der im System ausgeführten CPUs aus. Citrix ADC VPX berücksichtigt die Leerlauf-CPUs beim Auschecken der Lizenzen nicht.
Ähnlich wie die gepoolte Lizenzkapazität und die CICO-Lizenzfunktionen verwaltet der Citrix ADM -Lizenzserver einen separaten Satz virtueller CPU-Lizenzen. Auch hier sind die drei Editionen, die für virtuelle CPU-Lizenzen verwaltet werden, Standard, Advanced und Premium. Diese Editionen entsperren dieselben Features wie jene, die von den Editionen für Bandbreitenlizenzen freigeschaltet wurden.

Möglicherweise ändert sich die Anzahl der virtuellen CPUs oder wenn sich die Lizenzversion ändert. In diesem Fall müssen Sie die Instanz immer herunterfahren, bevor Sie eine Anforderung für einen neuen Satz von Lizenzen starten. Starten Sie Citrix ADC VPX nach dem Auschecken der Lizenzen neu.

So konfigurieren Sie den Lizenzserver in Citrix ADC VPX mithilfe der GUI

1. Navigieren Sie in Citrix ADC VPX zu **System** > **Lizenzen**, und klicken Sie auf **Lizenzen verwalten**.
2. Klicken Sie auf der Seite **Lizenz** auf **Neue Lizenz hinzufügen**.
3. Wählen Sie auf der Seite **Lizenzen** die Option **Remote-Lizenzierung verwenden** aus.
4. Wählen Sie in der Liste **Remotelizenzierungsmodus** die Option **CPU-Lizenzierung** aus.
5. Geben Sie die IP-Adresse des Lizenzservers und die Portnummer ein.
6. Klicken Sie auf **Weiter**.

   > **Hinweis**
   >
   > Registrieren Sie Citrix ADC VPX Instanz immer bei Citrix ADM. Aktivieren Sie Registrieren bei Citrix ADM, und geben Sie Citrix ADM-Anmeldeinformationen ein, falls dies noch nicht geschehen ist.

7. Wählen Sie im Fenster **Lizenzen zuweisen** den Lizenztyp aus. Das Fenster zeigt die Summe und die verfügbaren virtuellen CPUs sowie die zugeordneten CPUs an. Klicken Sie auf **Get Licenses**.

   > **Hinweis Weisen Sie**
   >
   > für ein ADC HA-Paar jedem Knoten separat virtuelle CPU-Lizenzen zu.

8. Klicken Sie auf der nächsten Seite auf **Neustart**, um die Lizenzen zu beantragen.

   > **Hinweis**
   >
   > Sie können auch die aktuelle Lizenz freigeben und aus einer anderen Edition auschecken. Beispielsweise führen Sie bereits die Standard Edition-Lizenz für Ihre Instanz aus. Sie können diese Lizenz freigeben und dann aus der Advanced Edition auschecken.

Instanz-Einstellungen

April 28, 2021

Sie können die erkannten Instanzen im Citrix ADM Dienst verwalten und die Einstellungen für die Instanzsicherung konfigurieren.

Verwalten der Instanzkonfiguration

In der **Instanzverwaltung**können Sie die folgenden Instanzkonfigurationen ändern:

- **Kommunikation mit Instanzen** : Sie können HTTP- oder HTTPS-Kommunikationskanal zwischen dem Citrix ADM Dienst und den erkannten Instanzen auswählen.

- **Zertifikatdownload aktivieren** - Ermöglicht das Herunterladen der SSL-Zertifikate von einer erkannten Instanz.
- **Anmeldeinformationen für Instanzanmeldung auffordern** : Wenn Sie über die Citrix ADM GUI auf die Instanz zugreifen, wird die Anmeldeseite für die Instanz angezeigt. Geben Sie Ihre Anmeldeinformationen an, um auf eine Instanz zuzugreifen.

Konfigurieren der Einstellungen für das Instanzbackup

In **Instanz Backup Settings**können Sie die Sicherungseinstellungen für die erkannten ADC-Instanzen in Citrix ADM konfigurieren.

Wählen Sie **unter Einstellungen für die Instanzsicherung konfigurieren**die Option **Instanzsicherungen aktivieren**aus.

- **Sicherungssicherheitseinstellungen** - Verschlüsseln Sie die Sicherungsdatei, um sicherzustellen, dass alle sensiblen Informationen in der Sicherungsdatei sicher sind. Wählen Sie **Kennwortschutzdatei** aus, um die Sicherungsdatei zu verschlüsseln.

  > **Hinweis**
  >
  > Wenn Sie die verschlüsselte Sicherungsdatei herunterladen, wird die Datei nicht in der Citrix ADM GUI oder in einem Texteditor geöffnet. Diese Datei kann nur von Citrix ADM abgerufen und verwendet werden. Sie können jedoch eine unverschlüsselte Sicherungsdatei auf Ihrem System öffnen.
  >
  > Um die verschlüsselte Sicherungsdatei wiederherzustellen, geben Sie das Kennwort an, das Sie zum Verschlüsseln der Sicherungsdatei erwähnt haben.

- **Einstellungen für die Sicherungsplanung**- Sie können eine Instanzsicherung auf zwei Arten planen:
  - **Intervallbasiert** : Nach Ablauf des angegebenen Intervalls wird eine Backupdatei in Citrix ADM erstellt. Das Standardintervall für Backups ist 12 Stunden.
  - **Zeitbasiert** : Geben Sie die Zeit im `hours:minutes`Format an, zu der Citrix ADM die Instanzsicherung übernehmen soll.
- **Citrix ADC Einstellungen** : Mit dieser Option können Sie eine Sicherung basierend auf dem Trap initiieren und GeoDB-Dateien in die Sicherung einbeziehen. Diese Einstellung gilt für MPX-, VPX-, CPX- und BLX-Instanzen.
  - **Führen Sie eine Instanzsicherung durch, wenn NetScalerConfigSave-Trap empfangen wird**. Standardmäßig erstellt Citrix ADM keine Sicherungsdatei, wenn das Trap "NetScalerConfigSave" empfängt. Sie können jedoch die Option zum Erstellen einer Sicherungsdatei aktivieren, wenn eine Citrix ADC-Instanz ein `NetScalerConfigSave`Trap an Citrix ADM sendet.

Eine Citrix ADC-Instanz sendet `NetScalerConfigSave`jedes Mal, wenn die Konfiguration auf der Instanz gespeichert wird.

Geben **Sie die Verzögerung bei Trap** in Minuten an. Wenn der empfangene `NetScalerConfigSave` Trap für die angegebenen Minuten in Citrix ADM beibehalten wird, sichert Citrix ADM die Instanz.

- **GeoDB-Dateien einschließen** - Standardmäßig werden die GeoDatabase-Dateien von Citrix ADM nicht gespeichert. Sie können die Option aktivieren, um ein Backup dieser Dateien auch zu erstellen.

- **Citrix SDX-Einstellungen** : Um SDX-Instanzen zu sichern, geben Sie **Backup-Timeout** in Minuten an. Während einer SDX-Instanzsicherung wird die Verbindung zwischen ADM und SDX für den angegebenen Zeitraum aufrechterhalten.

  Wenn die Größe der Sicherungsdatei der SDX-Instanz groß ist, sollten Sie die Verbindung zwischen ADM und SDX-Instanz für einen längeren Zeitraum aufrechterhalten, um die Sicherung der SDX-Instanz abzuschließen.

  > **Wichtig**
  >
  > Die Sicherung schlägt fehl, wenn die Verbindung ein Zeitabfall hat.

- **Externe Übertragung** : Mit Citrix ADM können Sie die Sicherungsdateien der Citrix ADC-Instanz an einen externen Speicherort übertragen:

  1. Geben Sie die IP-Adresse des Standorts an.
  2. Geben Sie den Benutzernamen und das Kennwort des externen Servers an, auf den Sie die Backupdateien übertragen möchten.
  3. Geben Sie das Übertragungsprotokoll und die Portnummer an.
  4. Geben Sie den Verzeichnispfad an, in dem die Datei gespeichert werden soll.
  5. Wenn Sie die Sicherungsdatei löschen möchten, nachdem Sie die Datei auf einen externen Server übertragen haben, wählen Sie **Datei nach der Übertragung aus Anwendungsbereitstellungsverwaltung löschen**aus.

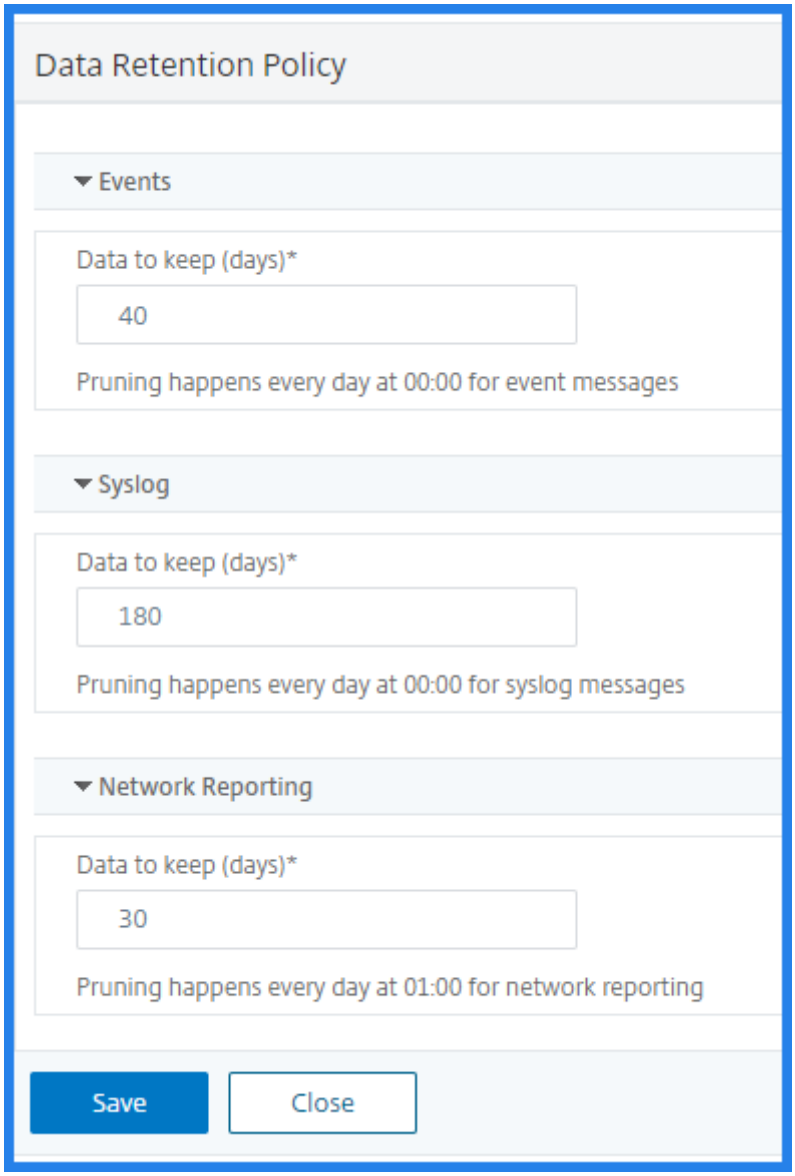
Datenaufbewahrungsrichtlinie

April 28, 2021

Sie können auf Systemereignisse, Syslog-Meldungen und Netzwerk-Berichtsdaten für eine bestimmte Dauer im ADM-Dienst zugreifen.

1. Navigieren Sie zu **Einstellungen > Datenaufbewahrungsrichtlinie**, um die Datenaufbewahrung zu konfigurieren.
2. Klicken Sie auf die Schaltfläche “Bearbeiten”.
3. Geben Sie Tage für die folgenden Optionen an, um Daten im ADM-Dienst beizubehalten:

Optionen	Beschreibung
Ereignisse	Ermöglicht es Ihnen, die im ADM-Dienst gespeicherten Ereignismeldungen auf bis zu 40 Tage zu beschränken. Die Ereignisse werden aus ADM gelöscht, nachdem die Aufbewahrungsrichtlinie abgelaufen ist. Die gelöschten Ereignisse werden nach einem Tag gelöscht. Weitere Informationen finden Sie unter Ereignisse.
Syslog	Ermöglicht es Ihnen, die Anzahl der in der Datenbank gespeicherten Syslog-Daten auf bis zu 180 Tage zu begrenzen. Weitere Informationen finden Sie unter Konfigurieren von Syslog für Instanzen.
Netzwerkberichterstattung	Ermöglicht es Ihnen, die in Citrix ADM gespeicherten Netzwerk-Berichtsdaten auf bis zu 30 Tage zu beschränken. Weitere Informationen finden Sie unter Netzwerkberichterstattung.



Wichtig

Sie können die Datenaufbewahrungsrichtlinie nicht mit einem Express-Konto bearbeiten.

Wenn Ihr Konto in ein Express-Konto konvertiert wird, behält der ADM-Dienst die Speicherdaten bis zu 500 MB oder einen Tag, je nachdem, was der kleinere ist. Weitere Informationen finden Sie unter Verwalten von Citrix ADM Ressourcen mit Express-Konto.

Instanz-Einstellungen

April 28, 2021

Sie können die erkannten Instanzen im Citrix ADM Dienst verwalten und die Einstellungen für die Instanzsicherung konfigurieren.

Verwalten der Instanzkonfiguration

In der **Instanzverwaltung**können Sie die folgenden Instanzkonfigurationen ändern:

- **Kommunikation mit Instanzen** : Sie können HTTP- oder HTTPS-Kommunikationskanal zwischen dem Citrix ADM Dienst und den erkannten Instanzen auswählen.
- **Zertifikatdownload aktivieren** - Ermöglicht das Herunterladen der SSL-Zertifikate von einer erkannten Instanz.
- **Anmeldeinformationen für Instanzanmeldung auffordern** : Wenn Sie über die Citrix ADM GUI auf die Instanz zugreifen, wird die Anmeldeseite für die Instanz angezeigt. Geben Sie Ihre Anmeldeinformationen an, um auf eine Instanz zuzugreifen.

Konfigurieren der Einstellungen für das Instanzbackup

In **Instanz Backup Settings**können Sie die Sicherungseinstellungen für die erkannten ADC-Instanzen in Citrix ADM konfigurieren.

Wählen Sie **unter Einstellungen für die Instanzsicherung konfigurieren**die Option **Instanzsicherungen aktivieren**aus.

- **Sicherungssicherheitseinstellungen** - Verschlüsseln Sie die Sicherungsdatei, um sicherzustellen, dass alle sensiblen Informationen in der Sicherungsdatei sicher sind. Wählen Sie **Kennwortschutzdatei** aus, um die Sicherungsdatei zu verschlüsseln.

  > **Hinweis**
  >
  > Wenn Sie die verschlüsselte Sicherungsdatei herunterladen, wird die Datei nicht in der Citrix ADM GUI oder in einem Texteditor geöffnet. Diese Datei kann nur von Citrix ADM abgerufen und verwendet werden. Sie können jedoch eine unverschlüsselte Sicherungsdatei auf Ihrem System öffnen.
  >
  > Um die verschlüsselte Sicherungsdatei wiederherzustellen, geben Sie das Kennwort an, das Sie zum Verschlüsseln der Sicherungsdatei erwähnt haben.

- **Einstellungen für die Sicherungsplanung**- Sie können eine Instanzsicherung auf zwei Arten planen:
  - **Intervallbasiert** : Nach Ablauf des angegebenen Intervalls wird eine Backupdatei in Citrix ADM erstellt. Das Standardintervall für Backups ist 12 Stunden.
  - **Zeitbasiert** : Geben Sie die Zeit im `hours:minutes`Format an, zu der Citrix ADM die Instanzsicherung übernehmen soll.

- **Citrix ADC Einstellungen** : Mit dieser Option können Sie eine Sicherung basierend auf dem Trap initiieren und GeoDB-Dateien in die Sicherung einbeziehen. Diese Einstellung gilt für MPX-, VPX-, CPX- und BLX-Instanzen.
  - **Führen Sie eine Instanzsicherung durch, wenn NetScalerConfigSave-Trap empfangen wird**. Standardmäßig erstellt Citrix ADM keine Sicherungsdatei, wenn das Trap "NetScalerConfigSave" empfängt. Sie können jedoch die Option zum Erstellen einer Sicherungsdatei aktivieren, wenn eine Citrix ADC-Instanz ein `NetScalerConfigSave`Trap an Citrix ADM sendet.

    Eine Citrix ADC-Instanz sendet `NetScalerConfigSave`jedes Mal, wenn die Konfiguration auf der Instanz gespeichert wird.

    Geben **Sie die Verzögerung bei Trap** in Minuten an. Wenn der empfangene `NetScalerConfigSave` Trap für die angegebenen Minuten in Citrix ADM beibehalten wird, sichert Citrix ADM die Instanz.
  - **GeoDB-Dateien einschließen** - Standardmäßig werden die GeoDatabase-Dateien von Citrix ADM nicht gespeichert. Sie können die Option aktivieren, um ein Backup dieser Dateien auch zu erstellen.
- **Citrix SDX-Einstellungen** : Um SDX-Instanzen zu sichern, geben Sie **Backup-Timeout** in Minuten an. Während einer SDX-Instanzsicherung wird die Verbindung zwischen ADM und SDX für den angegebenen Zeitraum aufrechterhalten.

  Wenn die Größe der Sicherungsdatei der SDX-Instanz groß ist, sollten Sie die Verbindung zwischen ADM und SDX-Instanz für einen längeren Zeitraum aufrechterhalten, um die Sicherung der SDX-Instanz abzuschließen.

  > **Wichtig**
  >
  > Die Sicherung schlägt fehl, wenn die Verbindung ein Zeitabfall hat.

- **Externe Übertragung** : Mit Citrix ADM können Sie die Sicherungsdateien der Citrix ADC-Instanz an einen externen Speicherort übertragen:
  1. Geben Sie die IP-Adresse des Standorts an.
  2. Geben Sie den Benutzernamen und das Kennwort des externen Servers an, auf den Sie die Backupdateien übertragen möchten.
  3. Geben Sie das Übertragungsprotokoll und die Portnummer an.
  4. Geben Sie den Verzeichnispfad an, in dem die Datei gespeichert werden soll.
  5. Wenn Sie die Sicherungsdatei löschen möchten, nachdem Sie die Datei auf einen externen Server übertragen haben, wählen Sie **Datei nach der Übertragung aus Anwendungsbereitstellungsverwaltung löschen**aus.

Systemkonfigurationen

April 28, 2021

Sie können das Keep-Alive-Intervall des ADM-Agenten und die Zeitzone des Citrix ADM -Servers ändern.

Keep-Alive-Intervall des Agenten festlegen

Citrix ADM Server und Agent pflegen dieselbe TCP-Verbindung für das angegebene Keepalive-Intervall. Ein Agent verwendet diese Verbindung, um die Daten der verwalteten Instanzen an den ADM-Server zu senden.

1. Navigieren Sie zu **Einstellungen > Systemeinstellungen**.
2. Wählen Sie unter **Systemkonfigurationen** die Option **Agent und Zeitzone** aus.
3. Geben Sie in **Agent**das Keep-Alive-Intervall zwischen 30 und 120 Sekunden an.
4. Klicken Sie auf **Save**.

Festlegen der Citrix ADM-Zeitzone

Sie können die Zeitzone auswählen, in der Sie die Uhrzeit auf der ADM-Webseite, in Benachrichtigungen und Berichten anzeigen möchten.

1. Navigieren Sie zu **Einstellungen > Systemeinstellungen**.
2. Wählen Sie unter **Systemkonfigurationen** die Option **Agent und Zeitzone** aus.
3. Wählen Sie unter **Zeitzone**die lokale oder GMT-Zeitzone aus, um die Zeit in ADM anzuzeigen.
4. Klicken Sie auf **Save**.

Aktivieren oder Deaktivieren von ADM-Funktionen

April 28, 2021

Als Administrator können Sie die folgenden Funktionen auf der Seite “ **Systemeinstellungen” > “Konfigurierbare Funktionen** “ aktivieren oder deaktivieren:

- **Agentenfailover** : Das Agent-Failover kann auf einem Standort mit zwei oder mehr aktiven Agenten auftreten. Wenn ein Agent in der Site inaktiv wird (DOWN Status), verteilt der Citrix

ADM Dienst die ADC-Instanzen des inaktiven Agents mit anderen aktiven Agenten neu. Weitere Informationen finden Sie unter Konfigurieren von Citrix ADM -Agenten für die Bereitstellung mehrerer Sites.

- **Entity-Polling-Netzwerkfunktion** : Eine Entität ist entweder eine Richtlinie, ein virtueller Server, ein Dienst oder eine Aktion, die an eine ADC-Instanz angehängt ist. Standardmäßig ruft Citrix ADM konfigurierte Netzwerkfunktionsentitäten automatisch alle 60 Minuten ab. Weitere Informationen finden Sie unter Übersicht über die Abrufung.
- **Instanzbackup**: Erstellen Sie ein Backup des aktuellen Status einer Citrix ADC-Instanz und verwenden Sie später die Backupdateien, um die ADC-Instanz in demselben Zustand wiederherzustellen. Weitere Informationen finden Sie unter Sichern und Wiederherstellen von Citrix ADC-Instanzen.
- **Überwachung der Instanzkonfiguration** : Überwachen Sie Konfigurationsänderungen in verwalteten Citrix ADC-Instanzen, beheben Sie Konfigurationsfehler und stellen Sie ungespeicherte Konfigurationen wieder her. Weitere Informationen finden Sie unter Erstellen von Überwachungsvorlagen.
- **Instanzereignisse** : Ereignisse stellen Vorkommen von Ereignissen oder Fehlern in einer verwalteten Citrix ADC-Instanz dar. In Citrix ADM empfangene Ereignisse werden auf der Seite " **Ereignisübersicht** " (**Netzwerke > Ereignisse**) angezeigt. Und alle aktiven Ereignisse werden auf der Seite "Ereignisnachrichten" (**Netzwerke > Ereignisse > Ereignisnachrichten**) angezeigt. Weitere Informationen finden Sie unter Ereignisse.
- **Instanznetzwerk-Reporting** - Sie können Berichte für Instanzen auf globaler Ebene erstellen. Auch für Entitäten wie die virtuellen Server und Netzwerkschnittstellen. Weitere Informationen finden Sie unter Netzwerkberichterstattung.
- **Instanz-SSL-Zertifikate** : Citrix ADM bietet eine zentrale Ansicht der SSL-Zertifikate, die auf allen verwalteten Citrix ADC-Instanzen installiert sind. Weitere Informationen finden Sie unter SSL-Dashboard.
- **Instanzsyslog** : Sie können die Syslog-Ereignisse überwachen, die auf Ihren Citrix ADC-Instanzen generiert werden, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Nachrichten an Citrix ADM umgeleitet werden. Weitere Informationen finden Sie unter Konfigurieren von Syslog für Instanzen.

Führen Sie die folgenden Schritte aus, um ein Feature zu aktivieren:

1. Wählen Sie das Feature aus der Liste aus, die Sie aktivieren möchten.
2. Klicken Sie auf **Aktivieren**.

> **Wichtig**
>
> Wenn eine Funktion deaktiviert ist, kann der Benutzer die mit dieser Funktion verbundenen

> Vorgänge nicht ausführen.

Verwalten und Überwachen von HAProxy-Instanzen

April 28, 2021

Das Citrix Application Delivery Management (ADM) unterstützt HAProxy Version 1.4.24 oder höher. Wenn Sie Citrix ADM einen Host hinzufügen, auf dem Sie die HAProxy-Instanzen bereitgestellt haben, werden die HAProxy-Instanzen auf dem Host ermittelt und Sie können diese verwalten und überwachen. Citrix ADM zeigt Ihnen die folgenden Informationstypen zur HAProxy-Konfiguration auf den Instanzen an:

- Front-End — Definiert, wie Anfragen an das Back-End weitergeleitet werden müssen. Dies sind die entdeckten Entitäten in Citrix ADM, die den Datenverkehr ausgleichen.
- Backend — Die Gruppe von Servern, die die weitergeleiteten Anfragen erhalten.
- Server — Die Server, unter denen HAProxy-Load den Datenverkehr ausgleicht.

Weitere Informationen finden Sie unter http://www.haproxy.org/download/1.7/doc/configuration.txt.

Citrix ADM bietet ein HAProxy App Dashboard, auf dem Sie die Frontends in Echtzeit überwachen können. Weitere Informationen finden Sie unter HAProxy App Dashboard. Außerdem können Sie die Details der Frontends, Backends und Server anzeigen, die auf den HAProxy-Instanzen konfiguriert sind.

Um HAProxy-Instanzen auf einem HAProxy-Host zu verwalten und zu überwachen, müssen Sie den HAProxy-Host zu Citrix ADM hinzufügen. Weitere Informationen finden Sie unter Hinzufügen von HAProxy-Instanzen.

Verwandte Informationen

- HAProxy-App-Dashboard
- HAProxy-Instanzen überwachen
- Zeigen Sie die Details der auf HAProxy-Instanzen konfigurierten Front-Ends an
- Zeigen Sie die Details der auf HAProxy-Instanzen konfigurierten Backends an
- Details der auf HAProxy-Instanzen konfigurierten Server anzeigen
- Anzeigen der HAProxy-Instanzen mit der höchsten Anzahl an Front-Ends oder Servern
- Neustart einer HAProxy-Instanz

Provisioning von Citrix ADC VPX Instanzen in AWS

April 28, 2021

Wenn Sie Ihre Anwendungen in die Cloud verschieben, steigen die Komponenten, die Teil Ihrer Anwendung sind, weiter verteilt und müssen dynamisch verwaltet werden.

Mit Citrix ADC VPX Instanzen in AWS können Sie Ihren L4-L7-Netzwerkstapel nahtlos auf AWS erweitern. Mit Citrix ADC VPX wird AWS zu einer natürlichen Erweiterung Ihrer lokalen IT-Infrastruktur. Sie können Citrix ADC VPX in AWS verwenden, um die Elastizität und Flexibilität der Cloud mit den gleichen Optimierungs-, Sicherheits- und Kontrollfunktionen zu kombinieren, die die anspruchsvollsten Websites und Anwendungen der Welt unterstützen.

Mit Citrix Application Delivery Management (ADM), die Ihre Citrix ADC-Instanzen überwacht, erhalten Sie Einblick in den Zustand, die Leistung und die Sicherheit Ihrer Anwendungen. Sie können die Einrichtung, Bereitstellung und Verwaltung Ihrer Anwendungsbereitstellungsinfrastruktur in hybriden Multi-Cloud-Umgebungen automatisieren.

AWS-Terminologie

Der folgende Abschnitt enthält eine kurze Beschreibung der in diesem Dokument verwendeten AWS-Begriffe:

Begriff	Beschreibung
Amazon Machine Image (AMI)	Ein Maschinenimage, das die Informationen bereitstellt, die zum Starten einer Instanz erforderlich sind, bei der es sich um einen virtuellen Server in der Cloud handelt.
Elastic Compute Cloud (EC2)	Ein Webdienst, der sichere, skalierbare Rechenkapazität in der Cloud bereitstellt. Es wurde entwickelt, um Web-basierte Cloud Computing für Entwickler einfacher zu machen.
Elastische Netzwerkschnittstelle (ENI)	Eine virtuelle Netzwerkschnittstelle, die Sie an eine Instanz in einer VPC anhängen können.

Begriff	Beschreibung
Instanztyp	Amazon EC2 bietet eine große Auswahl an Instanztypen, die für verschiedene Anwendungsfälle optimiert sind. Instanztypen umfassen unterschiedliche Kombinationen von CPU-, Arbeitsspeicher-, Speicher- und Netzwerkkapazität und bieten Ihnen die Flexibilität, den geeigneten Ressourcenmix für Ihre Anwendungen auszuwählen.
Rolle Identity and Access Management (IAM)	Eine AWS-Identität mit Berechtigungsrichtlinien, die bestimmen, was die Identität in AWS tun kann und nicht. Sie können eine IAM-Rolle verwenden, um Anwendungen, die auf einer EC2-Instanz ausgeführt werden, den sicheren Zugriff auf Ihre AWS-Ressourcen zu ermöglichen.
Sicherheitsgruppen	Eine benannte Gruppe zulässiger eingehender Netzwerkverbindungen für eine Instanz.
Subnetze	Ein Segment des IP-Adressbereichs einer VPC, an die EC2-Instanzen angeschlossen werden können. Sie können Subnetze erstellen, um Instanzen entsprechend den Sicherheits- und betrieblichen Anforderungen zu gruppieren.
Virtuelle Private Cloud (VPC)	Ein Webservice zum Provisioning eines logisch isolierten Abschnitts der AWS-Cloud, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können.

Unterstützte Citrix ADC AMI-Instanztypen

Für höhere Bandbreite empfiehlt Citrix die folgenden Instanztypen:

Instanztypen	Bandbreite
M4.X Groß	Premium Edition 10 Mbit/s
M4.X Groß	Premium Edition 200 Mbit/s

Voraussetzungen

Dieses Dokument setzt Folgendes voraus:

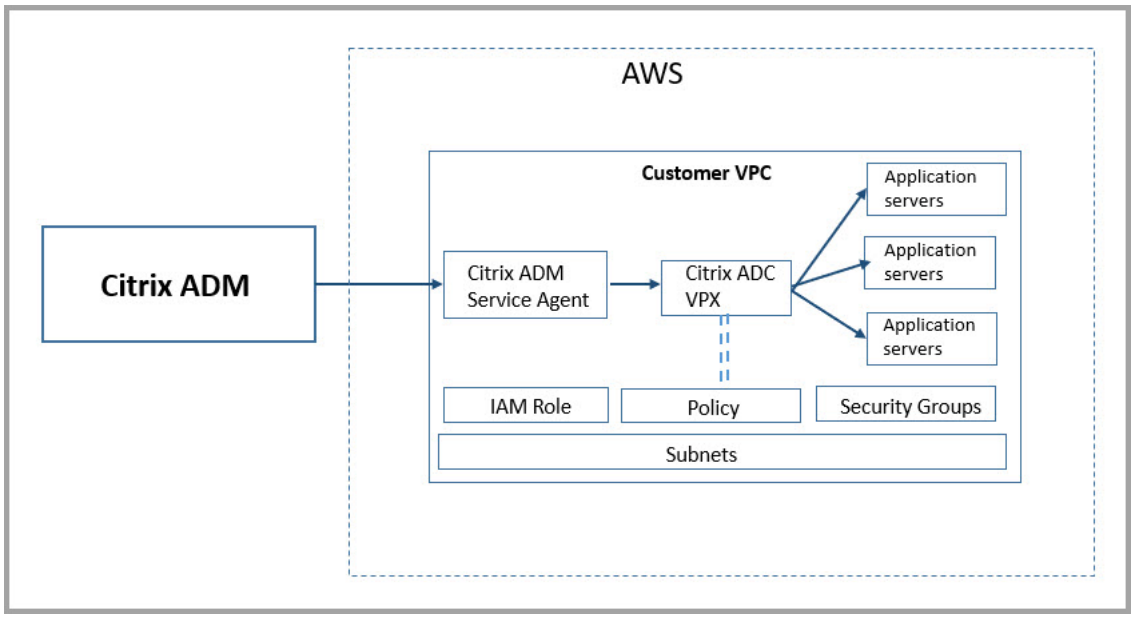
- Sie besitzen ein AWS-Konto.
- Sie haben die erforderliche VPC erstellt und die Availability Zones ausgewählt.
- Sie haben den Citrix ADM Service-Agenten in AWS hinzugefügt.

Weitere Informationen zum Erstellen eines Kontos und anderer Aufgaben finden Sie unter AWS-Dokumentation.

Weitere Informationen zur Installation des Citrix ADM Service-Agents in AWS finden Sie unterInstallieren des Citrix ADM Service Agents auf AWS.

Architekturdiagramm

Das folgende Bild bietet einen Überblick darüber, wie Citrix ADM eine Verbindung mit AWS herstellt, um Citrix ADC VPX Instanzen in AWS bereitzustellen.



Konfigurationsaufgaben

Führen Sie die folgenden Aufgaben in AWS aus, bevor Sie Citrix ADC VPX Instanzen in Citrix ADM bereitstellen:

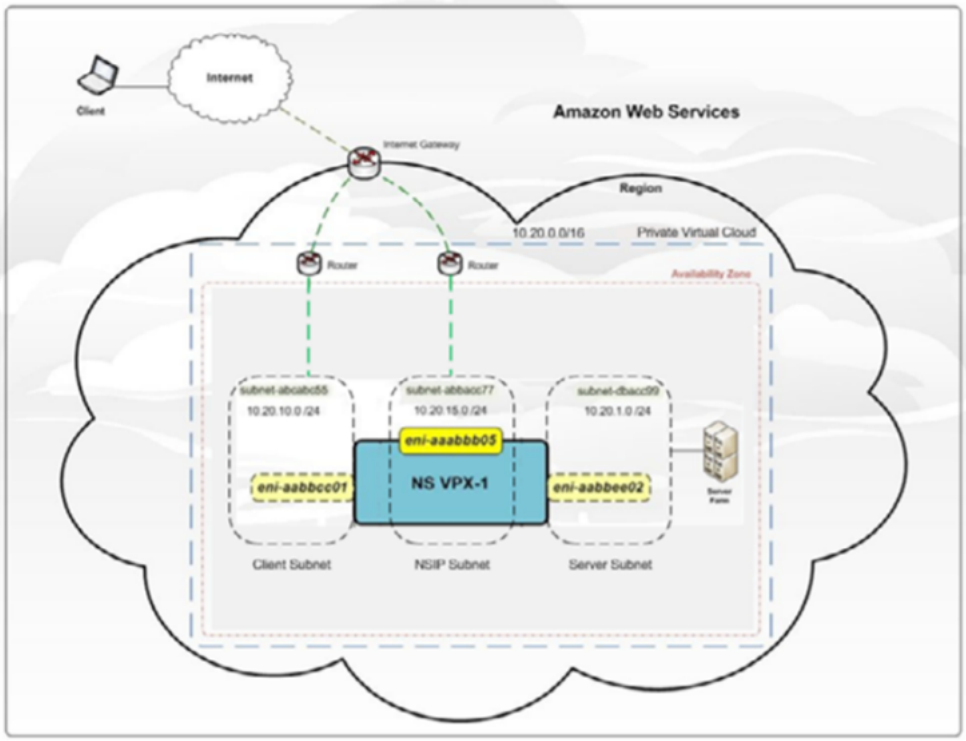
- Subnetze erstellen
- Erstellen von Sicherheitsgruppen
- Erstellen Sie eine IAM-Rolle und definieren Sie eine Richtlinie

Führen Sie die folgenden Aufgaben in Citrix ADM aus, um die Instanzen in AWS bereitzustellen:

- Site erstellen
- Bereitstellen einer Citrix ADC VPX Instanz auf AWS

So erstellen Sie Subnetze

Erstellen Sie drei Subnetze in Ihrer VPC. Die drei Subnetze, die zum Bereitstellen von Citrix ADC VPX Instanzen in Ihrer VPC erforderlich sind, sind Management, Client und Server. Geben Sie einen IPv4-CIDR-Block aus dem Bereich an, der in der VPC für jedes Subnetz definiert ist. Geben Sie die Verfügbarkeitszone an, in der sich das Subnetz befinden soll. Erstellen Sie alle drei Subnetze in derselben Availability Zone. Die folgende Abbildung veranschaulicht die drei in Ihrer Region erstellten Subnetze und deren Konnektivität mit dem Clientsystem.



Weitere Informationen zu VPC und Subnetzen finden Sie unterVPCs und Subnetze.

So erstellen Sie Sicherheitsgruppen

Erstellen Sie eine Sicherheitsgruppe zur Steuerung des eingehenden und ausgehenden Datenverkehrs in der Citrix ADC VPX Instanz. Eine Sicherheitsgruppe fungiert als virtuelle Firewall für Ihre Instanz. Erstellen Sie Sicherheitsgruppen auf Instanzebene und nicht auf Subnetzebene. Es ist möglich, jede Instanz in einem Subnetz in Ihrer VPC einem anderen Satz von Sicherheitsgruppen zuzuweisen. Fügen Sie Regeln für jede Sicherheitsgruppe hinzu, um den eingehenden Datenverkehr

zu steuern, der durch das Clientsubnetz an Instanzen weitergeleitet wird. Sie können auch einen separaten Satz von Regeln hinzufügen, die den ausgehenden Datenverkehr steuern, der das Serversubnetz zu den Anwendungsservern durchläuft. Obwohl Sie die Standardsicherheitsgruppe für Ihre Instanzen verwenden können, sollten Sie Ihre Gruppen erstellen. Erstellen Sie drei Sicherheitsgruppen - eine für jedes Subnetz. Erstellen Sie Regeln für eingehenden und ausgehenden Datenverkehr, die Sie steuern möchten. Sie können beliebig viele Regeln hinzufügen.

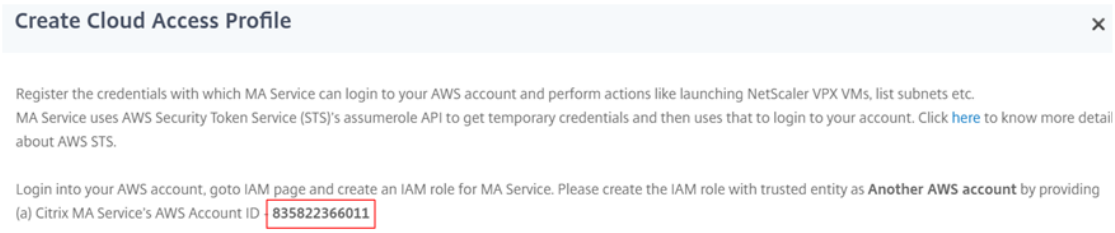
Weitere Informationen zu Sicherheitsgruppen finden Sie unterSicherheitsgruppen für Ihre VPC.

So erstellen Sie eine IAM-Rolle und definieren eine Richtlinie

Erstellen Sie eine IAM-Rolle, damit Sie eine Vertrauensstellung zwischen Ihren Benutzern und dem vertrauenswürdigen Citrix AWS-Konto einrichten und eine Richtlinie mit Citrix Berechtigungen erstellen können.

1. Klicken Sie in AWS auf **Services**. Wählen Sie im linken Navigationsbereich **IAM > Rollen**, und klicken Sie auf **Rolle erstellen**.
2. Sie verbinden Ihr AWS-Konto mit dem AWS-Konto in Citrix ADM. Wählen Sie also **ein weiteres AWS-Konto** aus, damit Citrix ADM Aktionen in Ihrem AWS-Konto ausführen kann.

   Geben Sie die 12-stellige Citrix ADM AWS-Konto-ID ein. Die Citrix ID lautet 835822366011. Sie können die Citrix ID auch in Citrix ADM finden, wenn Sie das Cloud-Zugriffsprofil erstellen.



3. Aktivieren Sie **Externe ID erforderlich**, um eine Verbindung mit einem Drittanbieterkonto herzustellen. Sie können die Sicherheit Ihrer Rolle erhöhen, indem Sie einen optionalen externen Bezeichner benötigen. Geben Sie eine ID ein, die eine Kombination aus beliebigen Zeichen sein kann.
4. Klicken Sie auf **Berechtigungen**.
5. Klicken Sie auf der Seite **Berechtigungsrichtlinien anhängen** auf **Richtlinie erstellen**.
6. Sie können eine Richtlinie im visuellen Editor oder mithilfe von JSON erstellen und bearbeiten.

   Die Liste der Berechtigungen von Citrix finden Sie im folgenden Feld:

```
1 {
```



```
2
3  ”Version”: ”2012-10-17”,
4  ”Statement”:
5  [
6      {
7
8           ”Effect”: ”Allow”,
9          ”Action”: [
10             ”ec2:DescribeInstances”,
11             ”ec2:DescribeImageAttribute”,
12             ”ec2:DescribeInstanceAttribute”,
13             ”ec2:DescribeRegions”,
14             ”ec2:DescribeDhcpOptions”,
15             ”ec2:DescribeSecurityGroups”,
16             ”ec2:DescribeHosts”,
17             ”ec2:DescribeImages”,
18             ”ec2:DescribeVpcs”,
19             ”ec2:DescribeSubnets”,
20             ”ec2:DescribeNetworkInterfaces”,
21             ”ec2:DescribeAvailabilityZones”,
22             ”ec2:DescribeNetworkInterfaceAttribute”,
23             ”ec2:DescribeInstanceStatus”,
24             ”ec2:DescribeAddresses”,
25             ”ec2:DescribeKeyPairs”,
26             ”ec2:DescribeTags”,
27             ”ec2:DescribeVolumeStatus”,
28             ”ec2:DescribeVolumes”,
29             ”ec2:DescribeVolumeAttribute”,
30             ”ec2:CreateTags”,
31             ”ec2:DeleteTags”,
32             ”ec2:CreateKeyPair”,
33             ”ec2:DeleteKeyPair”,
34             ”ec2:ResetInstanceAttribute”,
35             ”ec2:RunScheduledInstances”,
36             ”ec2:ReportInstanceStatus”,
37             ”ec2:StartInstances”,
38             ”ec2:RunInstances”,
39             ”ec2:StopInstances”,
40             ”ec2:UnmonitorInstances”,
41             ”ec2:MonitorInstances”,
42             ”ec2:RebootInstances”,
43             ”ec2:TerminateInstances”,
44             ”ec2:ModifyInstanceAttribute”,
45             ”ec2:AssignPrivateIpAddresses”,
46             ”ec2:UnassignPrivateIpAddresses”,
```



```
47                "ec2:CreateNetworkInterface",
48                "ec2:AttachNetworkInterface",
49                "ec2:DetachNetworkInterface",
50                "ec2:DeleteNetworkInterface",
51                "ec2:ResetNetworkInterfaceAttribute",
52                "ec2:ModifyNetworkInterfaceAttribute",
53                "ec2:AssociateAddress",
54                "ec2:AllocateAddress",
55                "ec2:ReleaseAddress",
56                "ec2:DisassociateAddress",
57                "ec2:GetConsoleOutput"
58            ],
59                "Resource": "*"
60        }
61
62 ]
63  }
64
65 <!--NeedCopy-->
```

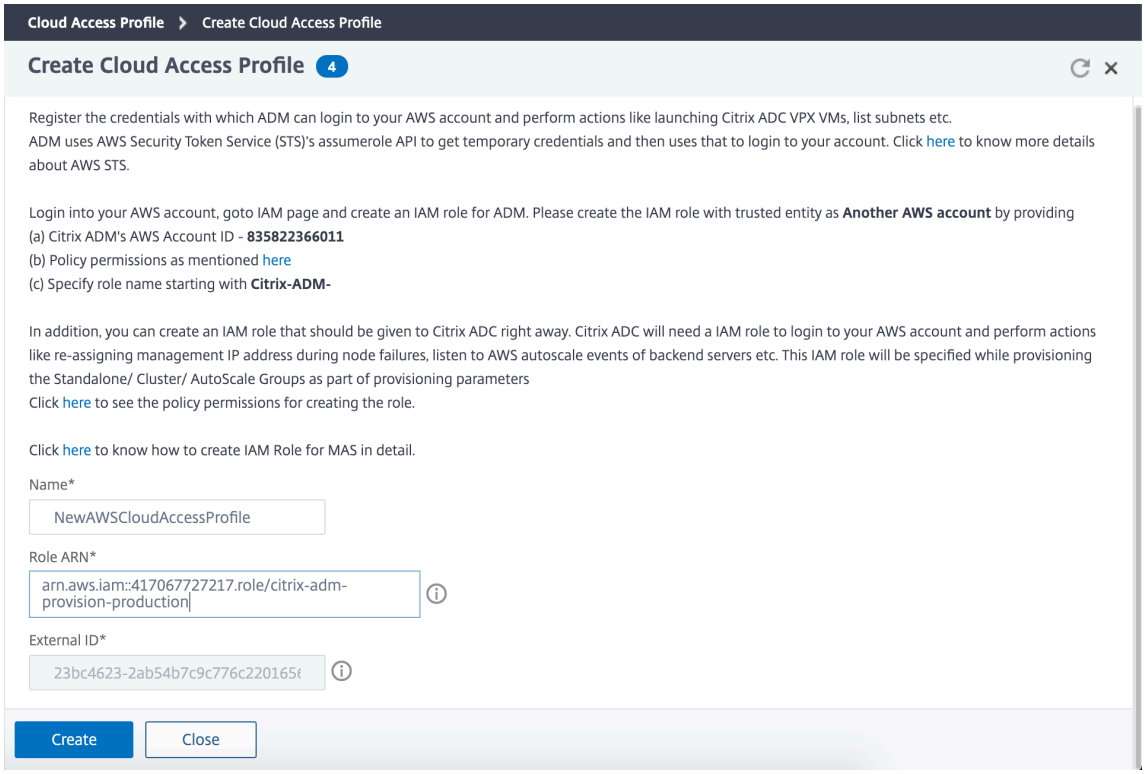
7. Kopieren Sie die Liste der Berechtigungen in der Registerkarte JSON, und fügen Sie sie ein, und klicken Sie auf **Richtlinie überprüfen**.
8. Geben Sie auf der Seite **Richtlinie überprüfen** einen Namen für die Richtlinie ein, geben Sie eine Beschreibung ein, und klicken Sie auf **Richtlinie erstellen**.

So erstellen Sie eine Site in Citrix ADM

Erstellen Sie eine Site in Citrix ADM, und fügen Sie die Details der VPC hinzu, die Ihrer AWS-Rolle zugeordnet ist.

1. Navigieren Sie in Citrix ADM zu **Netzwerke > Sites**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie den Servicetyp als AWS aus, und aktivieren Sie **Vorhandene VPC als Site verwenden**.
4. Wählen Sie das Cloud-Zugriffsprofil aus.
5. Wenn das Cloud-Zugriffsprofil im Feld nicht vorhanden ist, klicken Sie auf **Hinzufügen**, um ein Profil zu erstellen.
    a) Geben Sie auf der Seite **Cloud Access-Profil erstellen** den Namen des Profils ein, mit dem Sie auf AWS zugreifen möchten.
    b) Geben Sie den ARN ein, der der Rolle zugeordnet ist, die Sie in AWS erstellt haben.

c) Geben Sie die externe ID ein, die Sie beim Erstellen einer IAM-Rolle (Identity and Access Management) in AWS angegeben haben. Siehe Schritt 4 in So erstellen Sie eine IAM-Rolle und definieren eine Richtlinienaufgabe. Stellen Sie sicher, dass der in AWS angegebene IAM-Rollenname mit Citrix-ADM- beginnt und im Rollen-ARN korrekt angezeigt wird.



Die Details der VPC, wie Region, VPC-ID, Name und CIDR-Block, die Ihrer IAM-Rolle in AWS zugeordnet sind, werden in Citrix ADM importiert.

6. Geben Sie einen Namen für die Site ein.
7. Klicken Sie auf **Erstellen**.

So stellen Sie Citrix ADC VPX auf AWS bereit

Verwenden Sie die Website, die Sie zuvor erstellt haben, um die Citrix ADC VPX Instanzen in AWS bereitzustellen. Geben Sie Details des Citrix ADM Dienstagenten an, um die Instanzen bereitzustellen, die an diesen Agent gebunden sind.

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Klicken Sie auf der Registerkarte **VPX** auf **Bereitstellung**.

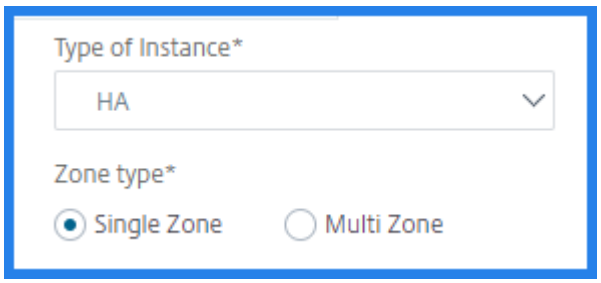
   Mit dieser Option wird die Seite **Citrix ADC VPX in der Cloud bereitstellen** angezeigt.
3. Wählen Sie **Amazon Web Services (AWS)** aus und klicken Sie auf **Weiter**.
4. Auf der Registerkarte " **Grundlegende Parameter** "

a) Wählen Sie in der Liste den **Instanztyp** aus.

- **Standalone:** Diese Option stellt eine eigenständige Citrix ADC VPX Instanz in AWS bereit.
- **HA:** Diese Option stellt die hochverfügbaren Citrix ADC VPX Instanzen in AWS bereit.

  Um die Citrix ADC VPX Instanzen in derselben Zone bereitzustellen, wählen Sie unter **Zonentyp** die Option **Einzelne Zone** aus.

  Um die Citrix ADC VPX Instanzen über mehrere Zonen hinweg bereitzustellen, wählen Sie unter **Zonentyp** die Option **Multi Zone** aus. Stellen Sie sicher, dass Sie auf der Registerkarte **Bereitstellungsparameter** die Netzwerkdetails für jede Zone angeben, die in AWS erstellt wurde.



b) Geben Sie den Namen einer ADC VPX Instanz an.

c) Wählen Sie unter **Site** die Website aus, die Sie zuvor erstellt haben.

d) Wählen Sie unter **Agent**den Agenten aus, der zur Verwaltung der ADC VPX-Instanz erstellt wurde.

e) Wählen Sie im **Cloud Access-Profil** das Cloud-Zugriffsprofil aus, das während der Website-Erstellung erstellt wurde.

f) Wählen Sie unter **Geräteprofil** das Profil für die Authentifizierung aus.

Citrix ADM verwendet das Geräteprofil, wenn es sich bei der Citrix ADC VPX Instanz anmelden muss.

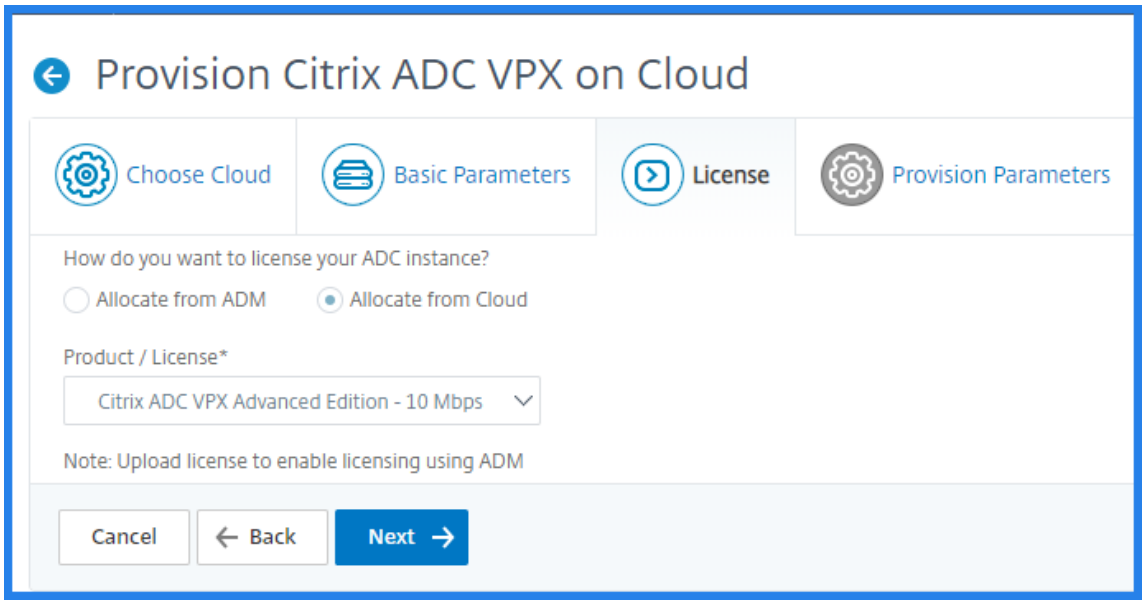
g) Klicken Sie auf **Weiter**.

5. Wählen Sie auf der Registerkarte **Lizenz** einen der folgenden Modi aus, um die Lizenz auf eine ADC-Instanz anzuwenden:

- **Verwendung von Citrix ADM**: Die Instanz, die Sie bereitstellen möchten, checkt die Lizenzen vom Citrix ADM aus.
- **Verwenden der AWS Cloud**: Die Option **Aus Cloud zuweisen** verwendet die auf dem AWS-Marktplatz verfügbaren Citrix Produktlizenzen. Die Instanz, die Sie bereitstellen möchten, verwendet die Lizenzen des Marketplace.

Wenn Sie sich für die Verwendung von Lizenzen aus dem AWS-Marketplace entscheiden, geben Sie das Produkt oder die Lizenz auf der Registerkarte **Bereitstellungsparameter** an.

Weitere Informationen finden Sie unter Lizenzanforderungen.



6. Wenn Sie auf der Registerkarte **Lizenz** die Option **Zuweisen von ADM**auswählen, geben Sie Folgendes an:

   - Lizenztyp - Wählen Sie entweder Bandbreiten- oder virtuelle CPU-Lizenzen aus:

     Bandbreitenlizenzen: Sie können eine der folgenden Optionen aus der Liste **Bandbreitenlizenztypen** auswählen:

     - **Pooled Capacity:** Geben Sie die Kapazität an, die einer Instanz zugewiesen werden soll.

       Aus dem gemeinsamen Pool checkt die ADC-Instanz eine Instanzlizenz aus und nur so viel Bandbreite wird angegeben.

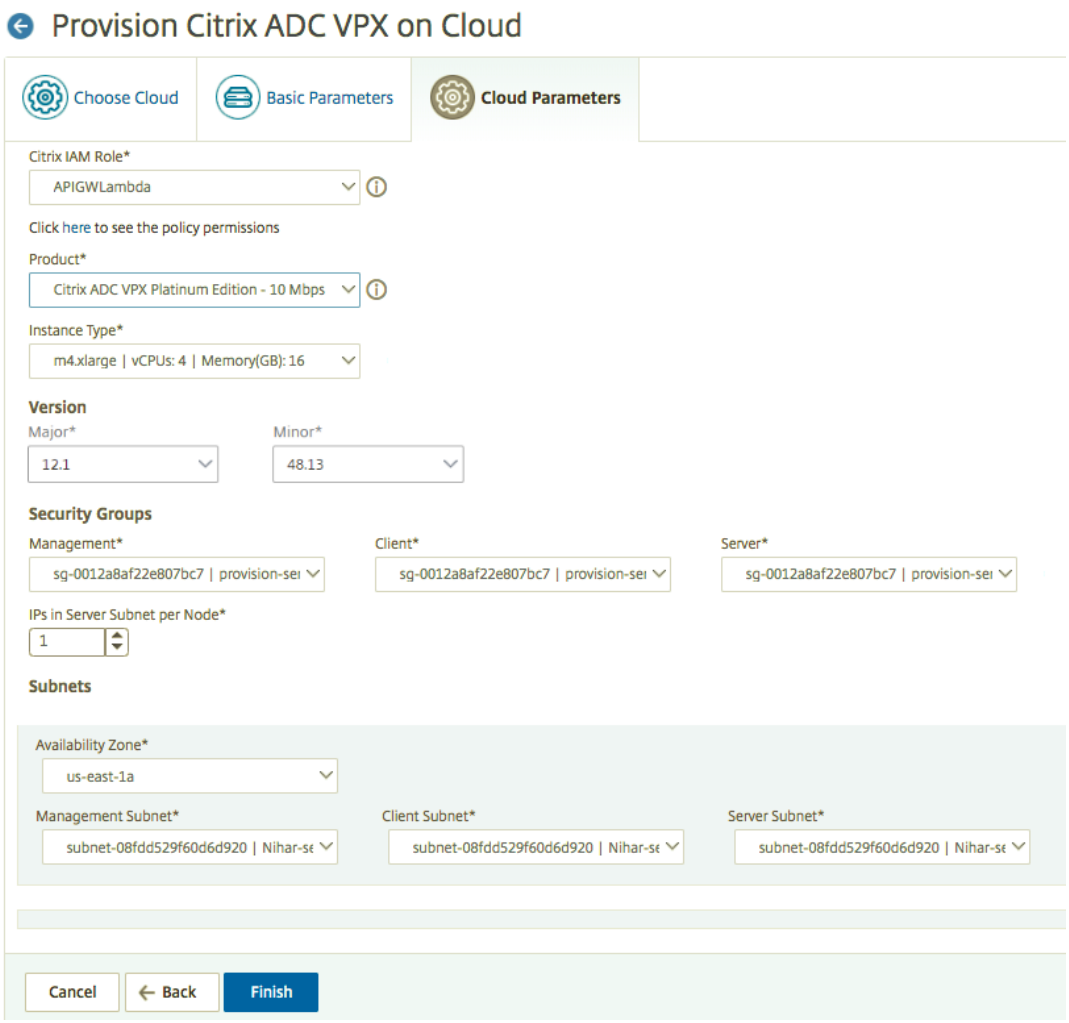
     - **VPX-Lizenzen:** Wenn eine Citrix ADC VPX Instanz bereitgestellt wird, checkt die Instanz die Lizenz vom Citrix ADM aus.

     Virtuelle CPU-Lizenzen: Die bereitgestellte Citrix ADC VPX-Instanz checkt Lizenzen abhängig von der Anzahl der in der Instanz ausgeführten CPUs aus.

     > **Hinweis:**
     >
     > Wenn die bereitgestellten Instanzen entfernt oder gelöscht werden, kehren die angewendeten Lizenzen in den Citrix ADM -Lizenzpool zurück. Diese Lizenzen können wiederverwendet werden, um neue Instanzen bereitzustellen.

a) Wählen Sie in **License Edition** die Lizenzversion aus. Der ADM verwendet die angegebene Edition zur Bereitstellung von Instanzen.

7. Klicken Sie auf **Weiter**.
8. Auf der Registerkarte " **Bereitstellungsparameter** "
   a) Wählen Sie die in AWS erstellte **Citrix IAM-Rolle** aus. Eine IAM-Rolle ist eine AWS-Identität mit Berechtigungsrichtlinien, die bestimmen, was die Identität in AWS tun kann und nicht.
   b) Wählen Sie im Feld **Produkt** die Citrix ADC Produktversion aus, die Sie bereitstellen möchten.
   c) Wählen Sie den EC2-Instanztyp aus der Liste **Instanztyp** aus.
   d) Wählen Sie die **Version** von Citrix ADC aus, die Sie bereitstellen möchten. Wählen Sie sowohl **Haupt-** als auch **Nebenversion** von Citrix ADC aus.
   e) Wählen Sie unter **Sicherheitsgruppen** die Sicherheitsgruppen Management, Client und Server aus, die Sie in Ihrem virtuellen Netzwerk erstellt haben.
   f) Wählen Sie **unter IPs im Serversubnetz pro Knoten**die Anzahl der IP-Adressen im Serversubnetz pro Knoten für die Sicherheitsgruppe aus.
   g) Wählen Sie **unter Subnets**die Verwaltungs-, Client- und Server-Subnetze für jede in AWS erstellte Zone aus. Sie können die Region auch in der Liste **Availability Zone** auswählen.
   h) Klicken Sie auf **Fertig stellen**.



Die Citrix ADC VPX Instanz wird jetzt auf AWS bereitgestellt.

> **Hinweis**
>
> Derzeit unterstützt Citrix ADM die Aufhebung der Bereitstellung von Citrix ADC-Instanzen von AWS nicht.

So zeigen Sie die in AWS bereitgestellte Citrix ADC VPX an

1. Navigieren Sie auf der AWS-Homepage zu **Services** und klicken Sie auf **EC2**.
2. Klicken Sie auf der Seite **Ressourcen** auf **Laufende Instanzen**.
3. Sie können das in AWS bereitgestellte Citrix ADC VPX anzeigen.

Der Name der Citrix ADC VPX-Instanz ist derselbe, den Sie beim Provisioning einer Instanz im Citrix ADM angegeben haben.

So zeigen Sie die in Citrix ADM bereitgestellte Citrix ADC VPX an

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Wählen Sie die Registerkarte **Citrix ADC VPX** aus.
3. Die in AWS bereitgestellte Citrix ADC VPX Instanz wird hier aufgelistet.

Automatische Skalierung von Citrix ADC in AWS mit Citrix ADM

April 28, 2021

Effizientes Hosting von Anwendungen in einer Cloud erfordert eine einfache und kostengünstige Verwaltung der Ressourcen je nach Anwendungsbedarf. Angenommen, Sie verfügen über ein E-Commerce-Webportal, das in AWS ausgeführt wird. Dieses Portal bietet manchmal enorme Rabatte, bei denen es eine Spitze im Anwendungsverkehr gibt. Wenn der Anwendungsdatenverkehr während dieser Angebote zunimmt, müssen die Anwendungen dynamisch skaliert werden, und dementsprechend müssen auch die Netzwerkressourcen erhöht werden.

Die automatische Skalierungsfunktion von Citrix ADM unterstützt die Provisioning und automatische Skalierung von Citrix ADC-Instanzen in AWS. Die automatische Scaling-Funktion von Citrix ADM überwacht ständig die Schwellenwerte wie Speicherauslastung, CPU-Auslastung und Durchsatz. Sie können einen dieser Parameter oder mehrere Parameter für die Überwachung auswählen. Diese Parameterwerte werden dann mit den vom Benutzer konfigurierten Werten verglichen. Wenn die Parameterwerte die Grenzwerte überschreiten, wird das Scale-Out bzw. Scale-In entsprechend ausgelöst.

Die Citrix ADM Autoscale-Feature-Architektur ist so konzipiert, dass Sie die minimale und maximale Anzahl von Instanzen für jede der Autoscale-Gruppen konfigurieren können. Die Voreinstellung dieser Nummern stellt sicher, dass Ihre Anwendung immer betriebsbereit ist.

> **Wichtig**
>
> Autoscaling unterstützt alle Citrix ADC Funktionen mit Ausnahme der folgenden Funktionen, die eine gepunktete Konfiguration auf Clusterknoten erfordern:
>
> - GSLB
> - Citrix Gateway und seine Funktionen
> - Telco-Funktionen
>
> Weitere Informationen zur Spotted-Konfiguration finden Sie unter Striped-, Teil-Striped- und Spotted-Konfigurationen.

Vorteile der automatischen Skalierung

Hohe Verfügbarkeit von Anwendungen. Die automatische Skalierung stellt sicher, dass Ihre Anwendung immer über die richtige Anzahl von Citrix ADC VPX Instanzen verfügt, um die Datenverkehrsanforderungen zu bewältigen. Dadurch wird sichergestellt, dass Ihre Anwendung unabhängig von den Datenverkehrsanforderungen ständig einsatzbereit ist.

Intelligente Skalierungsentscheidungen und Null-Touch-Konfiguration. Die automatische Skalierung überwacht Ihre Anwendung kontinuierlich und fügt Citrix ADC-Instanzen dynamisch hinzu oder entfernt sie je nach Bedarf. Wenn die Bedarfsspitzen nach oben steigen, werden die Instanzen automatisch hinzugefügt. Wenn die Bedarfsspitzen nach unten abwärts gehen, werden die Instanzen automatisch entfernt.
Das Hinzufügen und Entfernen von Citrix ADC-Instanzen erfolgt automatisch und macht es zu einer manuellen Null-Touch-Konfiguration.

Automatische DNS-Verwaltung. Die Citrix ADM Autoscale-Funktion bietet automatisches DNS-Management. Wenn neue Citrix ADC-Instanzen hinzugefügt werden, werden die Domänennamen automatisch aktualisiert.

Ordnungsgemäßer Verbindungsabschluss. Während eines Scale-Ins werden die Citrix ADC-Instanzen ordnungsgemäß entfernt, um den Verlust von Clientverbindungen zu vermeiden.

Besseres Kostenmanagement. Die automatische Skalierung erhöht oder verringert Citrix ADC-Instanzen bei Bedarf dynamisch. So können Sie die damit verbundenen Kosten optimieren. Sie sparen Geld, indem Sie Instanzen nur dann starten, wenn sie benötigt werden, und beenden sie, wenn sie nicht benötigt werden. So zahlen Sie nur für die Ressourcen, die Sie verwenden.

Beobachtbarkeit. Beobachtbarkeit ist der Schlüssel für Anwendungs-Dev-Ops oder IT-Personal, um den Zustand der Anwendung zu überwachen. Das Dashboard “Autoscale” von Citrix ADM ermöglicht Ihnen die Visualisierung der Schwellwert-Parameterwerte, der Autoscale Trigger-Zeitstempel, der Ereignisse und der Instanzen, die an der Autoscale beteiligt sind.

Unterstützungsfähigkeit

Derzeit wird die Autoscale-Funktion nur für Citrix ADC-Instanzen unterstützt, die in AWS bereitgestellt werden.

> **Hinweis**
>
> Die Verwendung von Citrix ADC Release 12.1 Build 50.28 Image zum Erstellen von Autoscale-Gruppen in AWS wird nicht unterstützt.

Lizenzierungsanforderungen

Die Citrix ADC-Instanzen, die für die Citrix Autoscale-Gruppe erstellt werden, verwenden Citrix ADC Advanced- oder Premium ADC-Lizenzen. Citrix ADC Clustering-Funktion ist in Advanced- oder Premium ADC-Lizenzen enthalten.

Sie können eine der folgenden Methoden wählen, um Citrix ADCs zu lizenzieren, die von Citrix ADM bereitgestellt werden:

- **Verwenden von ADC-Lizenzen in Citrix ADM:** Konfigurieren Sie gepoolte Kapazität, VPX-Lizenzen oder virtuelle CPU-Lizenzen beim Erstellen der Autoscale-Gruppe. Wenn also eine neue Instanz für die Autoscale-Gruppe bereitgestellt wird, wird der bereits konfigurierte Lizenztyp automatisch auf die bereitgestellte Instanz angewendet.
  - **Pooled Capacity**: Stellt jeder bereitgestellten Instanz in der Autoscale-Gruppe Bandbreite zu. Stellen Sie sicher, dass in Citrix ADM die erforderliche Bandbreite zur Verfügung steht, um neue Instanzen bereitzustellen. Weitere Informationen finden Sie unter Konfiguration der gepoolten Kapazität.

    Jede ADC-Instanz in der Gruppe Autoscale checkt eine Instanzlizenz und die angegebene Bandbreite aus dem Pool aus.
  - **VPX-Lizenzen:** Wendet die VPX-Lizenzen auf neu bereitgestellte Instanzen an. Stellen Sie sicher, dass Sie über die erforderliche Anzahl von VPX-Lizenzen in Citrix ADM verfügen, um neue Instanzen bereitzustellen.

    Wenn eine Citrix ADC VPX Instanz bereitgestellt wird, checkt die Instanz die Lizenz vom Citrix ADM aus. Weitere Informationen finden Sie unter Citrix ADC VPX Ein- und Auschecken Lizenzierung.
  - **Virtuelle CPU-Lizenzen:** Wendet virtuelle CPU-Lizenzen auf neu bereitgestellte Instanzen an. Diese Lizenz gibt die Anzahl der CPUs an, die für eine Citrix ADC VPX Instanz berechtigt sind. Stellen Sie sicher, dass Sie über die erforderliche Anzahl von virtuellen CPUs in Citrix ADM verfügen, um neue Instanzen bereitzustellen.

    Wenn eine Citrix ADC VPX Instanz bereitgestellt wird, checkt die Instanz die virtuelle CPU-Lizenz vom Citrix ADM aus. Weitere Informationen finden Sie unter Citrix ADC virtuelle CPU-Lizenzierung.

  Wenn die bereitgestellten Instanzen zerstört oder die Bereitstellung aufgehoben werden, werden die angewendeten Lizenzen automatisch an Citrix ADM zurückgegeben.

  Um die verbrauchten Lizenzen zu überwachen, navigieren Sie zur Seite **Netzwerke** > **Lizenzen**.
- **Verwendung von AWS-Abonnementlizenzen:** Konfigurieren Sie Citrix ADC-Lizenzen, die auf dem AWS-Marketplace verfügbar sind, während Sie die Autoscale-Gruppe erstellen. Wenn also eine neue Instanz für die Autoscale-Gruppe bereitgestellt wird, wird die Lizenz vom AWS Marketplace bezogen.

AWS-Terminologie

Die folgende Tabelle enthält eine kurze Beschreibung einiger der in diesem Dokument verwendeten Autoskalierungsbegriffe.

Terminologie	Beschreibung
AWS-Gruppe für automatische Skalierung	AWS Auto Scaling Group ist eine Sammlung von EC2-Instanzen, die ähnliche Merkmale aufweisen und für die Zwecke der Instanzskalierung und -verwaltung als logische Gruppierung behandelt werden.
Amazon Machine Image (AMI)	Ein Maschinenimage, das die Informationen bereitstellt, die zum Starten einer Instanz erforderlich sind, bei der es sich um einen virtuellen Server in der Cloud handelt.
Elastic Compute Cloud (EC2)	Ein Webdienst, der sichere, skalierbare Rechenkapazität in der Cloud bereitstellt. Es wurde entwickelt, um Web-basierte Cloud Computing für Entwickler einfacher zu machen.
Elastic IP (EIP) Adressen	Eine Elastic IP-Adresse ist eine statische, öffentliche IPv4-Adresse, die für das dynamische Cloud-Computing entwickelt wurde. Sie können eine Elastic IP-Adresse einer beliebigen Instanz oder einer Netzwerkschnittstelle für jede VPC in Ihrem Konto zuordnen.
Elastische Netzwerkschnittstelle (ENI)	Eine virtuelle Netzwerkschnittstelle, die Sie an eine Instanz in einer VPC anhängen können.
Instanztyp	Amazon EC2 bietet eine große Auswahl an Instanztypen, die für verschiedene Anwendungsfälle optimiert sind. Instanztypen umfassen unterschiedliche Kombinationen von CPU-, Arbeitsspeicher-, Speicher- und Netzwerkkapazität und bieten Ihnen die Flexibilität, den geeigneten Ressourcenmix für Ihre Anwendungen auszuwählen.

Terminologie	Beschreibung
Rolle Identity and Access Management (IAM)	Eine AWS-Identität mit Berechtigungsrichtlinien, die bestimmen, was die Identität in AWS tun kann und nicht. Sie können eine IAM-Rolle verwenden, um Anwendungen, die auf einer EC2-Instanz ausgeführt werden, den sicheren Zugriff auf Ihre AWS-Ressourcen zu ermöglichen.
IAM-Instanz-Profil	Eine Identität, die den Citrix ADC-Instanzen bereitgestellt wird, die in einem Cluster in AWS bereitgestellt werden. Das Profil ermöglicht es den Instanzen, auf AWS-Services zuzugreifen, wenn es mit dem Lastausgleich der Clientanforderungen beginnt.
Zuhörer	Ein Listener ist ein Prozess, der anhand des von Ihnen konfigurierenden Protokolls und Ports nach Verbindungsanforderungen sucht. Die Regeln, die Sie für einen Listener definieren, bestimmen, wie der Load Balancer Anforderungen an die Ziele in einer oder mehreren Zielgruppen weiterleitet.
NLB	Netzwerklastenausgleichsdienst. NLB ist ein L4-Load Balancer, der in der AWS-Umgebung verfügbar ist.
Route 53	Route 53 ist der hochverfügbare und skalierbare DNS-Webservice (Cloud Domain Name System) von Amazon.
Sicherheitsgruppen	Eine benannte Gruppe zulässiger eingehender Netzwerkverbindungen für eine Instanz.
Subnetze	Ein Segment des IP-Adressbereichs einer VPC, an die EC2-Instanzen angeschlossen werden können. Sie können Subnetze erstellen, um Instanzen entsprechend den Sicherheits- und betrieblichen Anforderungen zu gruppieren.

Terminologie	Beschreibung
Virtuelle Private Cloud (VPC)	Ein Webservice zum Provisioning eines logisch isolierten Abschnitts der AWS-Cloud, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können.

Citrix ADC VPX Autoscale-Terminologie

Die folgende Tabelle enthält eine kurze Beschreibung einiger der in diesem Dokument verwendeten Autoskalierungsbegriffe Citrix ADC VPX.

Terminologie	Beschreibung
Gruppen automatisch skalieren	Autoscale-Gruppe ist eine Gruppe von Citrix ADC-Instanzen, die Anwendungen als einzelne Entität Lastverteilung auslösen und die automatische Skalierung auslösen, wenn die Schwellenwertparameter die Grenzwerte überschreiten. Citrix ADC-Instanzen skalieren oder skalieren dynamisch basierend auf der Konfiguration von Autoscale-Gruppen. **Hinweis:** Die Citrix Autoscale-Gruppe wird in diesem Dokument als Autoscale-Gruppe bezeichnet, während die AWS Autoscale-Gruppe explizit als AWS Autoscale-Gruppe bezeichnet wird.
Citrix ADC Cluster	Ein Citrix ADC-Cluster ist eine Gruppe von Citrix ADC VPX-Instanzen, und jede Instanz wird als Knoten bezeichnet. Der Clientdatenverkehr wird über die Knoten verteilt, um hohe Verfügbarkeit, hohen Durchsatz und Skalierbarkeit zu gewährleisten.

Terminologie	Beschreibung
Zeitüberschreitung für die Entleerung der Verbindung	Während des scale-in entfernt Citrix ADM, sobald eine Instanz für die Aufhebung der Bereitstellung ausgewählt wurde, entfernt Citrix ADM die Instanz von der Verarbeitung neuer Verbindungen zur Autoscale-Gruppe und wartet, bis der angegebene Zeitüberschreitungszeitraum für Drain-Verbindungen vor der Deprovisionierung abläuft. Dadurch können vorhandene Verbindungen zu dieser Instanz entfernt werden, bevor die Bereitstellung aufgehoben wird. Wenn die Verbindungen entleert werden, bevor das Zeitlimit für die Drain-Verbindung abläuft, wartet der Citrix ADM selbst dann, bis die Zeitüberschreitung für die Ablaufverbindung abgelaufen ist, bevor eine neue Auswertung gestartet wird. **Hinweis:** Wenn die Verbindungen auch nach Ablauf des Zeitlimits der Drain-Verbindung nicht entleert werden, entfernt Citrix ADM die Instanzen, die sich auf die Anwendung auswirken könnten. Der Standardwert beträgt 5 Minuten und ist konfigurierbar.

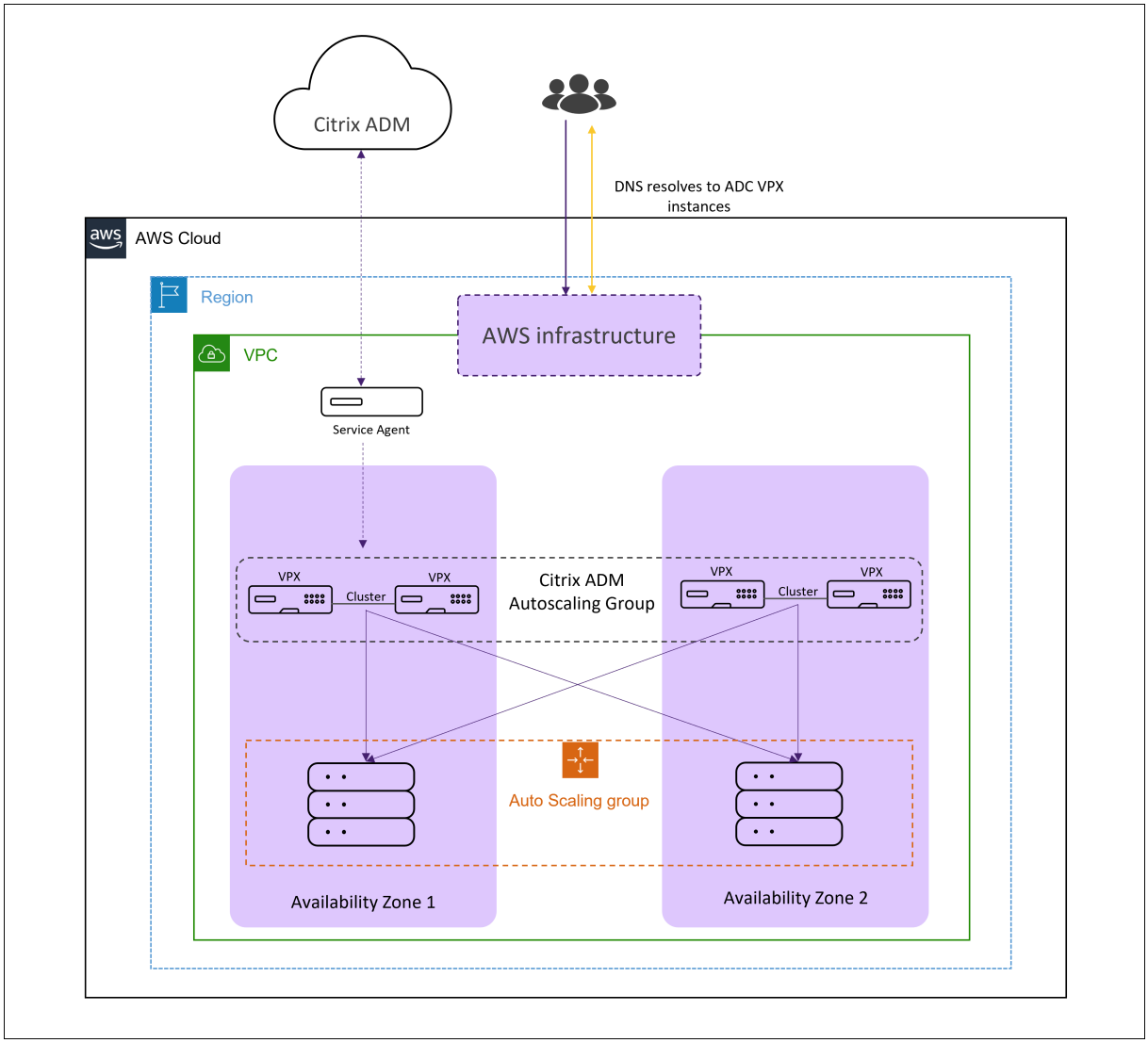
Terminologie	Beschreibung
Abklingzeit	Nach einem Scale-Out ist die Abklingzeit die Zeit, für die die Auswertung der Statistiken gestoppt werden muss. Dies gewährleistet das organische Wachstum einer Autoscale-Gruppe, da sich der aktuelle Datenverkehr stabilisiert und den aktuellen Instanzsatz durchdurchschnittlich ausfällt, bevor die nächste Skalierungsentscheidung getroffen wird. Der Standardwert für die Abklingzeit beträgt 10 Minuten und ist konfigurierbar. **Hinweis:** Der Standardwert wird basierend auf der Zeit ermittelt, die für die Stabilisierung des Systems nach einem Scale-Out (ca. 4 Minuten) sowie der Citrix ADC Konfiguration und der DNS-Ankündigungszeit erforderlich ist.
Tags	Jeder Autoscale-Gruppe wird ein Tag zugewiesen, das ein Schlüssel- und Wertepaar ist. Sie können Tags auf die Ressourcen anwenden, mit denen Sie Ressourcen einfach organisieren und identifizieren können. Die Tags werden sowohl auf AWS als auch auf Citrix ADM angewendet. **Beispiel:** Schlüssel= Name, Wert = Webserver. Es wird empfohlen, einen konsistenten Satz von Tags zu verwenden, um die Autoscale-Gruppen, die verschiedenen Gruppen wie Entwicklung, Produktion und Tests angehören könnten, einfach zu verfolgen.
Schwellenwertparameter	Parameter, die für das Auslösen von Scale-Out oder Scale-In überwacht werden. Die Parameter sind CPU-Auslastung, Speicherauslastung und Durchsatz. Sie können einen Parameter oder mehrere Parameter für die Überwachung auswählen.

Terminologie	Beschreibung
Time to Live (TTL)	Gibt das Zeitintervall an, in dem der DNS-Ressourceneintrag zwischengespeichert werden könnte, bevor die Quelle der Informationen erneut konsultiert werden muss. Der Standard-TTL-Wert ist 30 Sekunden und kann konfiguriert werden.
Wiedergabezeit	Die Zeit, für die der Schwellenwert des Skalierungsparameters überschritten werden muss, damit eine Skalierung erfolgt. Wenn der Schwellenwert für alle Proben, die in dieser angegebenen Zeit gesammelt wurden, überschritten wird, geschieht eine Skalierung. Wenn die Schwellenwertparameter während dieser Dauer auf einem Wert bleiben, der über dem maximalen Schwellenwert liegt, wird ein Scale-Out ausgelöst. Wenn die Schwellenwertparameter mit einem Wert unterhalb des minimalen Schwellenwerts arbeiten, wird ein Scale-In ausgelöst. Der Standardwert beträgt 3 Minuten und ist konfigurierbar.

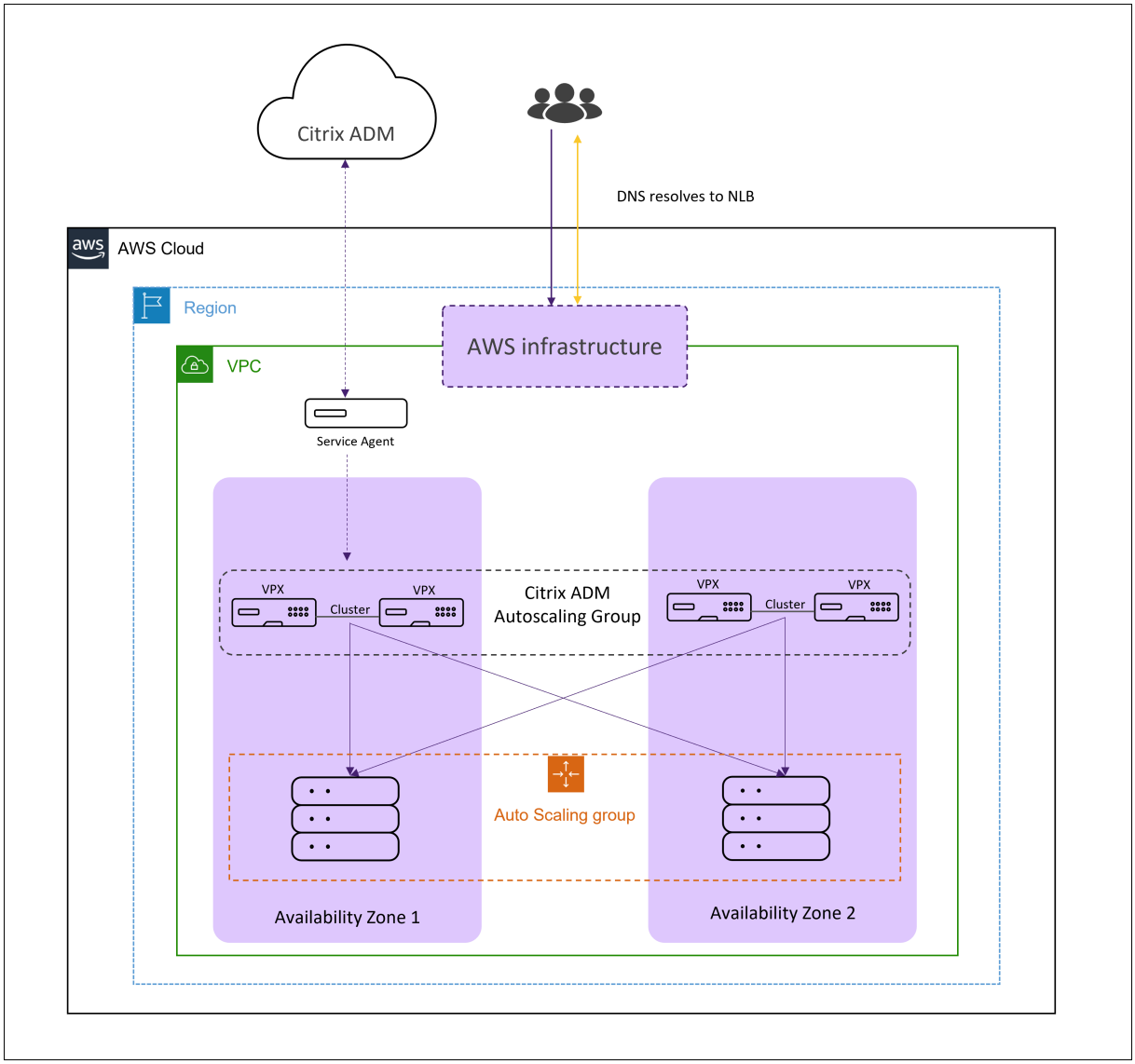
Architektur

April 28, 2021

Das folgende Diagramm veranschaulicht die Architektur des automatischen Skalierungs-Features mit DNS als Traffic-Distributor.



Das folgende Diagramm veranschaulicht die Architektur des automatischen Skalierungs-Features mit NLB als Traffic-Verteiler.



Citrix Application Delivery Management (ADM)

Citrix Application Delivery Management ist eine webbasierte Lösung zur Verwaltung aller Citrix ADC Bereitstellungen, die lokal oder in der Cloud bereitgestellt werden. Mit dieser Cloud-Lösung können Sie die gesamte globale Anwendungsbereitstellungsinfrastruktur über eine einzige, einheitliche und zentrale cloudbasierte Konsole verwalten, überwachen und beheben. Citrix Application Delivery Management (ADM) bietet alle Funktionen, die zum schnellen Einrichten, Bereitstellen und Verwalten der Anwendungsbereitstellung in Citrix ADC Bereitstellungen erforderlich sind, sowie umfassende Analysen zu Anwendungsstatus, Leistung und Sicherheit.

Die Autoscale-Gruppen werden in Citrix ADM erstellt, und die Citrix ADC VPX-Instanzen werden von Citrix ADM bereitgestellt. Die Anwendung wird dann über StyleBooks in Citrix ADM bereitgestellt.

Verkehrsverteiler (NLB oder DNS/Route53)

NLB oder DNS/Route53 wird verwendet, um den Datenverkehr auf alle Knoten in einer Autoscale-Gruppe zu verteilen. Weitere Informationen finden Sie unter Autoscale Traffic-Verteilungsmodi.

Das Citrix ADM kommuniziert mit dem Verkehrsverteiler, um die Anwendungsdomäne und die IP-Adressen der virtuellen Lastausgleichsserver zu aktualisieren, die die Anwendung im Vordergrund stellen.

Citrix ADM Gruppe für automatische Skalierung

Autoscale-Gruppe ist eine Gruppe von Citrix ADC-Instanzen, die Anwendungen als einzelne Entität Lastausgleich auslösen und basierend auf den konfigurierten Schwellenwertparameterwerten die automatische Skalierung auslösen.

Citrix ADC Cluster

Ein Citrix ADC-Cluster ist eine Gruppe von Citrix ADC VPX-Instanzen, und jede Instanz wird als Knoten bezeichnet. Der Clientdatenverkehr wird über die Knoten verteilt, um hohe Verfügbarkeit, hohen Durchsatz und Skalierbarkeit zu gewährleisten.

> **Hinweis**
>
> - Entscheidungen zur automatischen Skalierung werden auf Clusterebene und nicht auf Knotenebene getroffen.
> - Unabhängige Cluster werden in verschiedenen Availability Zones gehostet und daher ist die Unterstützung für einige der Shared State Features begrenzt.
>
>   Persistenzsitzungen wie Quell-IP-Persistenz und andere mit Ausnahme der Cookie-basierten Persistenz können nicht über Cluster gemeinsam genutzt werden. Alle statuslosen Features wie Load Balancing-Methoden funktionieren jedoch in den verschiedenen Availability Zones erwartungsgemäß.

AWS-Gruppen für automatische Skalierung

AWS Auto Scaling Group ist eine Sammlung von EC2-Instanzen, die ähnliche Merkmale aufweisen und für die Zwecke der Instanzskalierung und -verwaltung als logische Gruppierung behandelt werden.

AWS-Verfügbarkeitszonen

AWS Availability Zone ist ein isolierter Standort innerhalb einer Region. Jede Region besteht aus mehreren Availability Zones. Jede Verfügbarkeitszone gehört zu einer einzelnen Region.

Verkehrsverteilungsmodi

Wenn Sie Ihre Anwendungsbereitstellung in die Cloud verschieben, wird die automatische Skalierung Teil der Infrastruktur. Wenn die Anwendungen mithilfe der automatischen Skalierung skalieren oder skalieren, müssen diese Änderungen an den Client weitergegeben werden. Diese Weitergabe wird mittels DNS-basierter oder NLB-basierter Autoskalierung erreicht.

NLB-basierte automatische Skalierung

Im NLB-basierten Bereitstellungsmodus ist die Verteilungsebene für die Clusterknoten der AWS-Netzwerklastenausgleich.

Bei NLB-basierter Autoskalierung wird pro Verfügbarkeitszone nur eine statische IP-Adresse angeboten. Dies ist die öffentliche IP-Adresse, die route53 hinzugefügt wird, und die Backend-IP-Adressen können privat sein. Bei dieser öffentlichen IP-Adresse arbeitet jede neue Citrix ADC-Instanz, die während der automatischen Skalierung bereitgestellt wird, mit privaten IP-Adressen und erfordert keine zusätzlichen öffentlichen IP-Adressen.

Verwenden Sie die NLB-basierte automatische Skalierung, um TCP-Datenverkehr zu verwalten. Verwenden Sie DNS-basierte automatische Skalierung, um UDP-Datenverkehr zu verwalten.

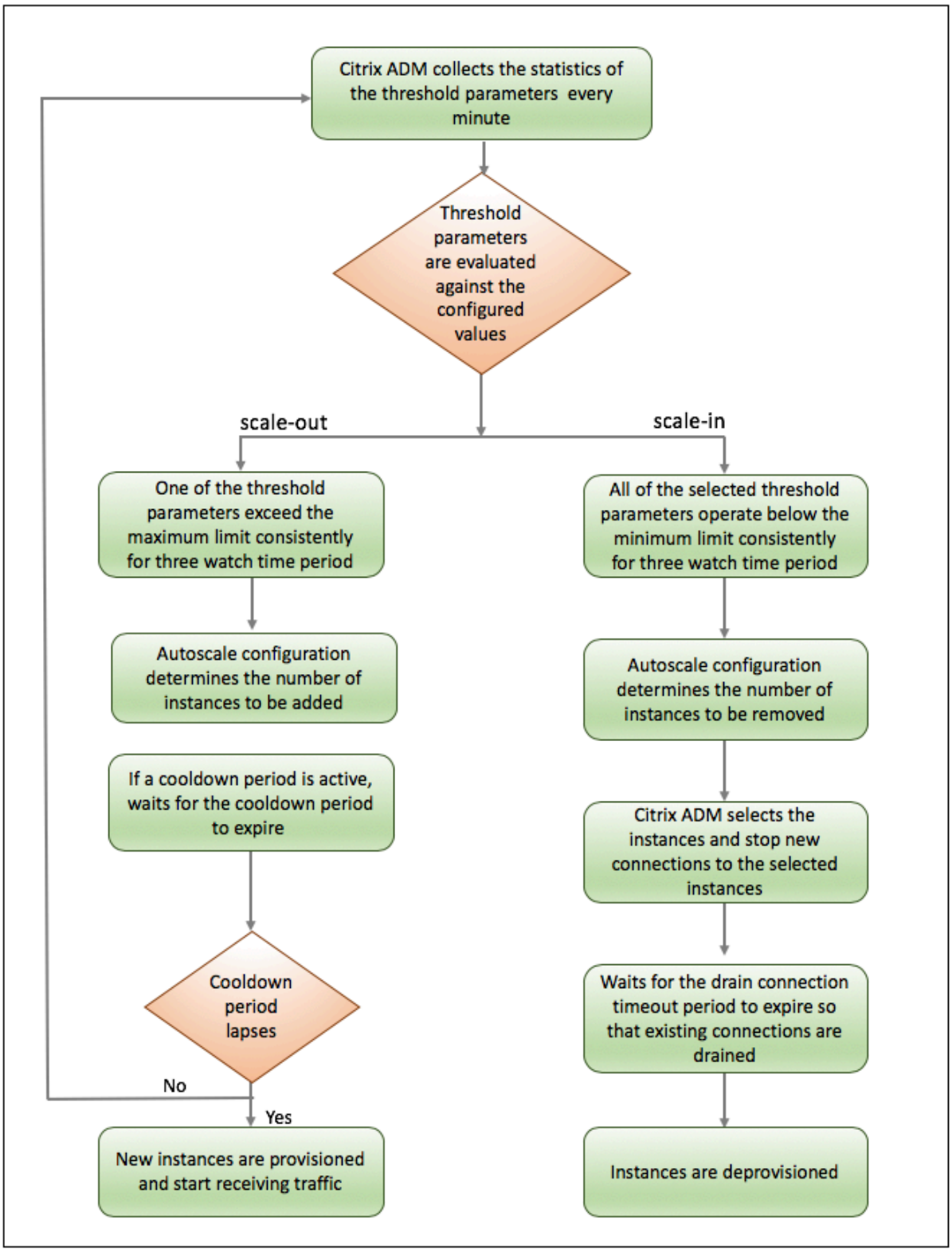
DNS-basierte automatische Skalierung

Bei der DNS-basierten Autoskalierung fungiert DNS als Verteilungsebene für die Citrix ADC Clusterknoten. Die Skalierungsänderungen werden an den Client weitergegeben, indem der Domänenname der Anwendung aktualisiert wird. Derzeit ist der DNS-Anbieter AWS Route53.

> **Hinweis**
>
> Bei DNS-basierter Autoskalierung erfordert jede Citrix ADC-Instanz eine öffentliche IP-Adresse.

So funktioniert die automatische Skalierung

Das folgende Flussdiagramm veranschaulicht den automatischen Skalierungsworkflow.



Der Citrix ADM sammelt Statistiken (CPU-Auslastung, Speichernutzung, Durchsatz) aus den von Autoscale bereitgestellten Clustern in einem Zeitintervall von einer Minute.

Die Statistiken werden anhand der Konfigurationsschwellenwerte ausgewertet. Je nachdem, ob die Statistiken den maximalen Schwellenwert überschreiten oder unter dem Mindestschwellenwert arbeiten, wird Scale-Out bzw. Scale-In ausgelöst.

- Wenn ein Scale-Out ausgelöst wird:
  - Neue Knoten werden bereitgestellt.
  - Die Knoten sind mit dem Cluster verbunden und die Konfiguration wird vom Cluster mit dem neuen Knoten synchronisiert.
  - Die Knoten werden bei Citrix ADM registriert.
  - Die neuen Knoten IP-Adressen werden in DNS/NLB aktualisiert.

Wenn die Anwendung bereitgestellt wird, `IPset` wird auf Clustern in jeder Availability Zone erstellt und die Domäne und die Instanz IP-Adressen werden bei DNS/NLB registriert.

- Wenn ein Scale-In ausgelöst wird:
  - Die IP-Adressen der zum Entfernen identifizierten Knoten werden entfernt.
  - Die Knoten werden vom Cluster getrennt, aufgehoben und dann von Citrix ADM abgemeldet.

Wenn die Anwendung entfernt wird, werden die Domäne und die Instanz IP-Adressen von DNS/NLB abgemeldet und die `IPset` gelöscht.

Beispiel

Beachten Sie, dass Sie eine Autoscale-Gruppe mit dem Namen asg_arn in einer einzelnen Availability Zone mit der folgenden Konfiguration erstellt haben.

- Schwellenwertparameter — Speicherauslastung
- Mindestgrenze: 40
- Höchstgrenze: 85
- Wiedergabezeit: 3 Minuten
- Abklingzeit — 10 Minuten
- Zeitüberschreitung für die Entleerung der Verbindung — 10 Minuten
- TTL-Zeitüberschreitung — 60 Sekunden

Nachdem die Gruppe “Autoscale” erstellt wurde, werden Statistiken aus der Gruppe “Autoscale” gesammelt. Die Autoscale-Richtlinie wertet auch aus, ob ein Autoscale-Ereignis in Bearbeitung ist, und wenn eine Autoskalierung im Gange ist, wartet auf den Abschluss dieses Ereignisses, bevor die Statistiken gesammelt werden.

ASG ID	Availability zone	Cluster IP address	CPU usage	Throughput	Memory usage	Timestamp
asg_arn	eu-west-2	192.0.2.250	55	65	92	T1
asg_arn	eu-west-2	192.0.2.250	60	50	90	T2
asg_arn	eu-west-2	192.0.2.250	59	45	80	T3
asg_arn	eu-west-2	192.0.2.250	49	75	90	T4
asg_arn	eu-west-2	192.0.2.250	63	70	93	T5
asg_arn	eu-west-2	192.0.2.250	65	80	92	T6
asg_arn	eu-west-2	192.0.2.250	65	85	75	T7
asg_arn	eu-west-2	192.0.2.250	35	70	70	.....
asg_arn	eu-west-2	192.0.2.250	55	70	70	T16
asg_arn	eu-west-2	192.0.2.250	58	55	45	T17
asg_arn	eu-west-2	192.0.2.250	59	65	30	T18
asg_arn	eu-west-2	192.0.2.250	75	45	30	T19
asg_arn	eu-west-2	192.0.2.250	46	64	25	T20
asg_arn	eu-west-2	192.0.2.250	64	65	50	T31
asg_arn	eu-west-2	192.0.2.250	64	65	60	T32
asg_arn	eu-west-2	192.0.2.250	64	65	60	T33

Scale-out event is triggered. Nodes are provisioned.

Evaluation of statistics is skipped for this availability zone from T7 –T16 as the cooldown period is in effect.

Scale-in event is triggered. Drain connection timeout in effect.

Ablauf der Ereignisse:

- T1 und T2: Die Speicherbelegung überschreitet den maximalen Schwellenwert.
- T3 - Die Speichernutzung liegt unter den maximalen Schwellenwerten.
- T6, T5, T4: Die Speichernutzung hat die maximale Grenzgrenze für drei Wiedergabezeiten nacheinander überschritten.
  - Ein Scale-Out wird ausgelöst.
  - Das Provisioning von Knoten erfolgt.
  - Die Abklingzeit ist gültig.
- T7 — T16: Die automatische Skalenauswertung wird für diese Verfügbarkeitszone von T7 bis T16 übersprungen, da die Abkühlperiode wirksam ist.
- T18, T19, T20 - Die Speichernutzung hat die Mindestschwellengrenze für drei Wiedergabezeiten nacheinander überschritten.
  - Scale-In wird ausgelöst.
  - Die Zeitüberschreitung für die Ablaufverbindung ist wirksam.
  - IP-Adressen werden vom DNS/NLB entlastet.
- T21 — T30: Die automatische Skalenauswertung wird für diese Verfügbarkeitszone von T21 bis T30 übersprungen, da das Zeitlimit für die Ablaufverbindung wirksam ist.

- T31
  - Bei der DNS-basierten Autoskalierung ist TTL wirksam.
  - Bei NLB-basierter Autoskalierung erfolgt die Aufhebung der Bereitstellung der Instanzen.
- T32
  - Bei der NLB-basierten Autoskalierung beginnt die Auswertung der Statistiken.
  - Bei der DNS-basierten automatischen Skalierung erfolgt die Aufhebung der Bereitstellung der Instanzen.
- T33: Für die DNS-basierte Autoskalierung beginnt die Auswertung der Statistiken.

Autoscale-Konfiguration

April 28, 2021

Um die automatische Skalierung von Citrix ADC VPX Instanzen in AWS zu starten, müssen Sie die folgenden Schritte ausführen:

1. Füllen Sie alle Voraussetzungen in AWS aus
2. Füllen Sie alle Voraussetzungen für Citrix ADM aus
3. Erstellen von Gruppen mit automatischer Skalierung
   a) Konfiguration der automatischen Skalierung initialisieren
   b) Konfigurieren von Parametern für die automatische Skalierung
   c) Lizenzen auschecken
   d) Konfigurieren von Cloud-Parametern
4. Bereitstellen der Anwendung

Voraussetzungen für AWS

Stellen Sie sicher, dass Sie alle Voraussetzungen für die Verwendung der AutoScale-Funktion in AWS erfüllt haben. Dieses Dokument setzt Folgendes voraus:

1. Sie besitzen bereits ein AWS-Konto.
2. Sie haben einen IAM (Identity and Access Management) -Benutzer mit allen Administratorberechtigungen erstellt.

In den nächsten Abschnitten können Sie alle erforderlichen Aufgaben in AWS ausführen, bevor Sie Autoscale-Gruppen in Citrix ADM erstellen. Die Aufgaben, die Sie ausführen müssen, sind wie folgt:

1. Abonnieren Sie die erforderliche Citrix ADC VPX Instanz in AWS.

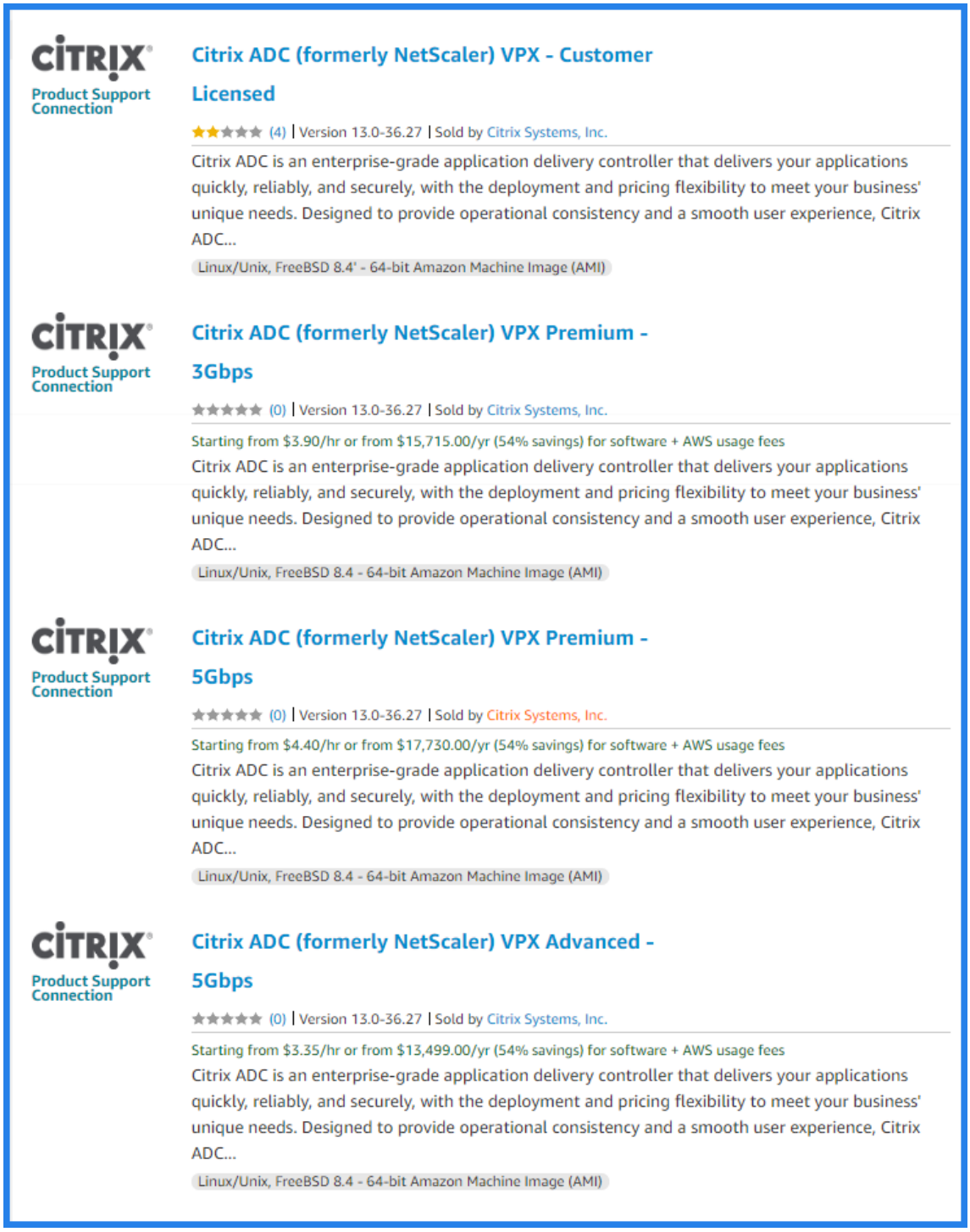
2. Erstellen Sie die erforderliche Virtual Private Cloud (VPC), oder wählen Sie eine vorhandene VPC aus.
3. Definieren Sie die entsprechenden Subnetze und Sicherheitsgruppen.
4. Erstellen Sie zwei IAM-Rollen, eine für Citrix ADM und eine für Citrix ADC VPX Instanz.

> **Tipp**
>
> Mit AWS CloudFormation Vorlagenkönnen Sie die AWS-Voraussetzungen für die automatische Skalierung von Citrix ADC automatisieren.

Weitere Informationen zum Erstellen von VPC-, Subnetz- und Sicherheitsgruppen finden Sie im AWS-Dokumentation.

Abonnieren der Citrix ADC VPX -Lizenz in AWS

1. Rufen Sie die AWS-Marktplatzauf.
2. Melden Sie sich mit Ihren Anmeldeinformationen an.
3. Suchen Sie nach Citrix ADC VPX Customer Licensed, Premium oder Advanced Edition.



4. Abonnieren Sie Citrix ADC VPX Customer Licensed, Premium Edition oder Citrix ADC VPX Advanced Edition-Lizenzen.

> **Hinweis**
>
> Wenn Sie möchten, dass die ADC-Instanzen in der Autoscale-Gruppe die Lizenzen aus dem ADM

> auschecken, stellen Sie Folgendes sicher:
>
> - Die erforderlichen ADC-Lizenzen stehen im ADM zur Verfügung.
> - Das **Citrix ADC VPX Customer Licensed** Produkt ist abonniert.

Subnetze erstellen

Erstellen Sie drei Subnetze in Ihrer VPC - jeweils eines für die Management-, Client- und Serververbindungen. Geben Sie einen IPv4-CIDR-Block aus dem Bereich an, der in der VPC für jedes Subnetz definiert ist. Geben Sie die Verfügbarkeitszone an, in der sich das Subnetz befinden soll. Erstellen Sie alle drei Subnetze in jeder der Availability Zones, in denen Server vorhanden sind.

- **Geschäftsführung**. Vorhandenes Subnetz in Ihrer Virtual Private Cloud (VPC) für die Verwaltung. Citrix ADC muss sich an AWS-Services wenden und erfordert Internetzugang. Konfigurieren Sie ein NAT-Gateway und fügen Sie einen Routentabelleneintrag hinzu, um den Internetzugang von diesem Subnetz zu ermöglichen.

  > **Hinweis: Stellen Sie**
  >
  > sicher, dass Sie öffnen `27000` und `7279` Ports in Citrix ADM. Diese Ports werden verwendet, um Citrix ADC-Lizenzen von Citrix ADM auszuprobieren. Weitere Informationen finden Sie unter Ports.

- **Client**: Vorhandenes Subnetz in Ihrer Virtual Private Cloud (VPC), das für den clientseitigen Datenverkehr bestimmt ist. In der Regel empfängt Citrix ADC Clientdatenverkehr für die Anwendung über ein öffentliches Subnetz aus dem Internet. Ordnen Sie das Clientsubnetz einer Routentabelle zu, die über eine Route zu einem Internet-Gateway verfügt. Mit diesem Subnetz kann Citrix ADC Anwendungsdatenverkehr aus dem Internet empfangen.
- **Server**. Vorhandenes Subnetz in Ihrer Virtual Private Cloud (VPC) für serverseitigen Datenverkehr. ADC sendet über dieses Subnetz Datenverkehr an die Back-End-Anwendungsserver. Alle Ihre Anwendungsserver, die Anwendungsdatenverkehr erhalten, müssen in diesem Subnetz vorhanden sein. Wenn sich die Server außerhalb dieses Subnetzes befinden, wird der Anwendungsdatenverkehr über das Gateway des Subnetzes empfangen.

Erstellen von Sicherheitsgruppen

Erstellen Sie eine Sicherheitsgruppe zur Steuerung des eingehenden und ausgehenden Datenverkehrs in der Citrix ADC VPX Instanz. Erstellen Sie Regeln für eingehenden und ausgehenden Datenverkehr, die Sie in den Citrix Autoscale-Gruppen steuern möchten. Sie können beliebig viele Regeln hinzufügen.

- **Geschäftsführung**. Vorhandene Sicherheitsgruppe in Ihrem Konto für die Verwaltung von Citrix ADC VPX. Eingehende Regeln sind für die folgenden TCP- und UDP-Ports zulässig.

  - TCP: 80, 22, 443, 3008—3011, 4001, 27000, 7279
  - UDP: 67, 123, 161, 500, 3003, 4500, 7000

  Stellen Sie sicher, dass die Sicherheitsgruppe es dem Citrix ADM Agent ermöglicht, auf das VPX zuzugreifen.

- **Client**: Vorhandene Sicherheitsgruppe in Ihrem Konto, die für die clientseitige Kommunikation von Citrix ADC VPX Instanzen bestimmt ist. In der Regel sind eingehende Regeln an den TCP-Ports 80 und 443 zulässig. Und der 60000-Port ist erforderlich, um den Zustand von ADC-Instanzen zu überwachen.
- **Server**. Vorhandene Sicherheitsgruppe in Ihrem Konto, die für die serverseitige Kommunikation von Citrix ADC VPX bestimmt ist. In der Regel blockiert es alle eingehenden Regeln und ermöglicht es ausgehenden Regeln, die gesamte VPC zu erreichen.

IAM-Rollen erstellen

Erstellen Sie IAM-Entitäten, die ADM- und ADC-Instanzen die Berechtigung erteilen, Vorgänge mit Ihrem AWS-Konto durchzuführen. Der ADM erstellt oder löscht Folgendes aus Ihrem AWS-Konto:

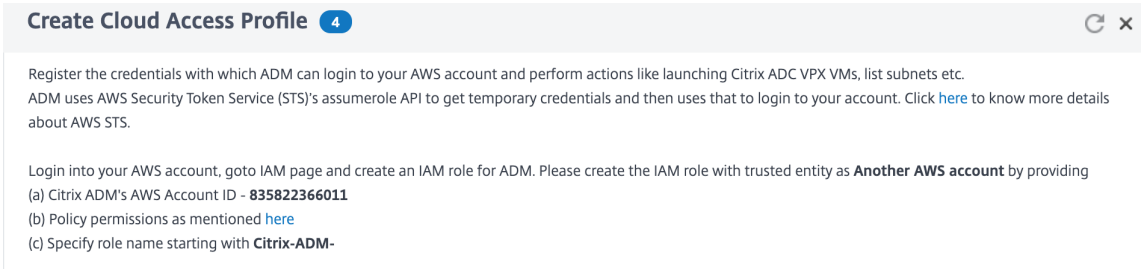
- Citrix ADC EC2-Instanzen
- Cloud LoadBalancers
- Route53

> **Hinweis**
>
> Stellen Sie sicher, dass die Rollennamen mit Citrix-ADM- beginnen und der Name des Instanzprofils mit Citrix-ADC- beginnt.

So erstellen Sie IAM-Entitäten für ADM

Erstellen Sie eine IAM-Rolle, damit Sie eine Vertrauensbeziehung zwischen Ihrem AWS-Konto und dem AWS-Konto von Citrix mit einer IAM-Richtlinie herstellen können, die ADM die Berechtigung zur Durchführung von Vorgängen an Ihrem AWS-Konto bietet.

1. Klicken Sie in **AWS** auf **Services**. Wählen Sie im linken Navigationsbereich **IAM > Rollen**, und klicken Sie auf **Rolle erstellen**.
2. Sie verbinden Ihr AWS-Konto mit dem AWS-Konto in Citrix ADM. Wählen Sie also **ein weiteres AWS-Konto** aus, damit Citrix ADM Aktionen in Ihrem AWS-Konto ausführen kann.
3. Geben Sie die 12-stellige Citrix ADM AWS-Konto-ID ein. Die Citrix ID lautet 835822366011. Sie können die externe ID jetzt leer lassen. Später müssen Sie die IAM-Rolle bearbeiten. Geben Sie die externe ID an, die von ADM während der Erstellung des Cloud-Zugriffsprofils in ADM bereitgestellt wird.



4. Klicken Sie auf **Berechtigungen**.
5. Klicken Sie auf der Seite **Berechtigungsrichtlinien anhängen** auf **Richtlinie erstellen**.
6. Sie können eine Richtlinie im visuellen Editor oder mithilfe von JSON erstellen und bearbeiten.

   Die Liste der Berechtigungen von Citrix für Citrix ADM finden Sie im folgenden Feld:

```
{

”Version”: ”2012-10-17”,
”Statement”: [
    {

        ”Action”: [
            ”tag:GetResources”,
            ”tag:TagResources”,
            ”tag:UntagResources”,
            ”tag:getTagKeys”,
            ”tag:getTagValues”,
            ”ec2:DescribeInstances”,
            ”ec2:UnmonitorInstances”,
            ”ec2:MonitorInstances”,
            ”ec2:CreateKeyPair”,
            ”ec2:ResetInstanceAttribute”,
            ”ec2:ReportInstanceStatus”,
            ”ec2:DescribeVolumeStatus”,
            ”ec2:StartInstances”,
            ”ec2:DescribeVolumes”,
            ”ec2:UnassignPrivateIpAddresses”,
            ”ec2:DescribeKeyPairs”,
            ”ec2:CreateTags”,
            ”ec2:ResetNetworkInterfaceAttribute”,
            ”ec2:ModifyNetworkInterfaceAttribute”,
            ”ec2:DeleteNetworkInterface”,
            ”ec2:RunInstances”,
            ”ec2:StopInstances”,
```



```
30              "ec2:AssignPrivateIpAddresses",
31              "ec2:DescribeVolumeAttribute",
32              "ec2:DescribeInstanceCreditSpecifications",
33              "ec2:CreateNetworkInterface",
34              "ec2:DescribeImageAttribute",
35              "ec2:AssociateAddress",
36              "ec2:DescribeSubnets",
37              "ec2:DeleteKeyPair",
38              "ec2:DisassociateAddress",
39              "ec2:DescribeAddresses",
40              "ec2:DeleteTags",
41              "ec2:RunScheduledInstances",
42              "ec2:DescribeInstanceAttribute",
43              "ec2:DescribeRegions",
44              "ec2:DescribeDhcpOptions",
45              "ec2:GetConsoleOutput",
46              "ec2:DescribeNetworkInterfaces",
47              "ec2:DescribeAvailabilityZones",
48              "ec2:DescribeNetworkInterfaceAttribute",
49              "ec2:ModifyInstanceAttribute",
50              "ec2:DescribeInstanceStatus",
51              "ec2:ReleaseAddress",
52              "ec2:RebootInstances",
53              "ec2:TerminateInstances",
54              "ec2:DetachNetworkInterface",
55              "ec2:DescribeIamInstanceProfileAssociations",
56              "ec2:DescribeTags",
57              "ec2:AllocateAddress",
58              "ec2:DescribeSecurityGroups",
59              "ec2:DescribeHosts",
60              "ec2:DescribeImages",
61              "ec2:DescribeVpcs",
62              "ec2:AttachNetworkInterface",
63              "ec2:AssociateIamInstanceProfile",
64              "ec2:DescribeAccountAttributes",
65              "ec2:DescribeInternetGateways"
66          ],
67          "Resource": "\*",
68          "Effect": "Allow",
69          "Sid": "VisualEditor0"
70      }
71  ,
72      {
73
74          "Action": [
```



```
                "iam:GetRole",
                "iam:PassRole",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "\*",
            "Effect": "Allow",
            "Sid": "VisualEditor1"
        }
    ,
        {

            "Action": [
                "route53:CreateHostedZone",
                "route53:CreateHealthCheck",
                "route53:GetHostedZone",
                "route53:ChangeResourceRecordSets",
                "route53:ChangeTagsForResource",
                "route53:DeleteHostedZone",
                "route53:DeleteHealthCheck",
                "route53:ListHostedZonesByName",
                "route53:GetHealthCheckCount"
                "route53:ListResourceRecordSets",
                "route53.AssociateVPCWithHostedZone",
            ],
            "Resource": "\*",
            "Effect": "Allow",
            "Sid": "VisualEditor2"
        }
    ,
        {

            "Action": [
                "iam:ListInstanceProfiles",
                "iam:ListAttachedRolePolicies",
                "iam:SimulatePrincipalPolicy",
                "iam:SimulatePrincipalPolicy"
            ],
            "Resource": "\*",
            "Effect": "Allow",
            "Sid": "VisualEditor3"
        }
    ,
        {

            "Action": [
```



```
120                 "ec2:ReleaseAddress",
121                 "elasticloadbalancing:DeleteLoadBalancer",
122                 "ec2:DescribeAddresses",
123                 "elasticloadbalancing:CreateListener",
124                 "elasticloadbalancing:CreateLoadBalancer",
125                 "elasticloadbalancing:RegisterTargets",
126                 "elasticloadbalancing:CreateTargetGroup",
127                 "elasticloadbalancing:DeregisterTargets",
128                 "ec2:DescribeSubnets",
129                 "elasticloadbalancing:DeleteTargetGroup",
130                 "elasticloadbalancing:ModifyTargetGroupAttributes",
131                 "elasticloadbalancing:DescribeLoadBalancers",
132                 "ec2:AllocateAddress"
133             ],
134             "Resource": "*",
135             "Effect": "Allow",
136             "Sid": "VisualEditor4"
137         }
138
139     ]
140 }
141
142
143 <!--NeedCopy-->
```

7. Kopieren Sie die Liste der Berechtigungen in der Registerkarte JSON, und fügen Sie sie ein, und klicken Sie auf **Richtlinie überprüfen**.
8. Geben Sie auf der Seite **Richtlinie überprüfen** einen Namen für die Richtlinie ein, geben Sie eine Beschreibung ein, und klicken Sie auf **Richtlinie erstellen**.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass der Name mit “Citrix-ADM-“ beginnt.

9. Geben Sie auf der Seite **Rolle erstellen** den Namen der Rolle ein.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass der Rollenname mit “Citrix-ADM-“ beginnt.

So erstellen Sie IAM-Entitäten für ADCs, die in ADM erstellt wurden

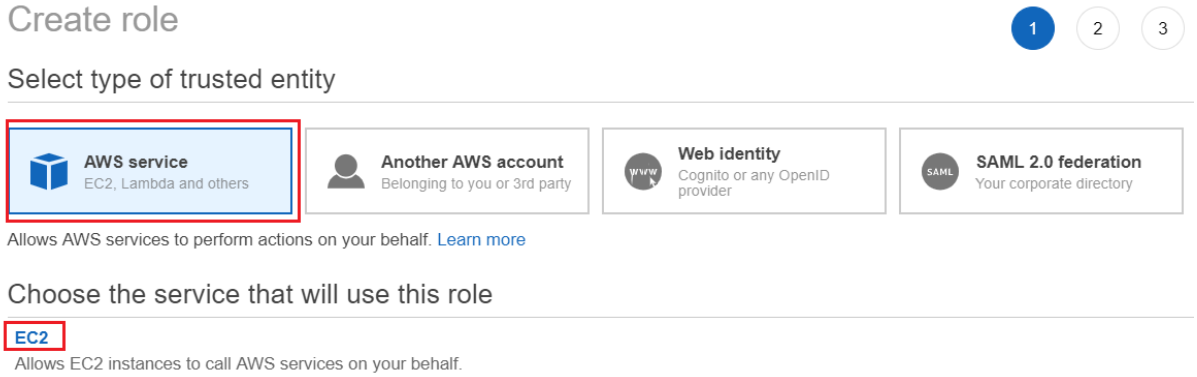
Erstellen Sie eine IAM-Rolle mit einer IAM-Richtlinie, die einem ADC die Berechtigung zur Durchführung von Vorgängen für Ihr AWS-Konto bietet. Diese Rolle ist ADC-Instanzen zugeordnet, die von ADM erstellt werden, wodurch ADCs auf Ihr Konto zugreifen können.

1. Klicken Sie in **AWS** auf **Services**. Wählen Sie im linken Navigationsbereich **IAM > Rollen**, und klicken Sie auf **Rolle erstellen**.

Erstellen Sie in ähnlicher Weise ein Profil für die Citrix ADC-Instanzen, indem Sie einen anderen Namen angeben, der mit Citrix-ADC- beginnt.

Stellen Sie sicher, dass Sie **AWS service > EC2** wählen,

1. Klicken Sie auf der Seite **Berechtigungsrichtlinien anhängen** auf **Richtlinie erstellen**.
2. Sie können eine Richtlinie im visuellen Editor oder mithilfe von JSON erstellen und bearbeiten.



Die Liste der Berechtigungen von Citrix für Citrix ADC-Instanzen finden Sie im folgenden Feld:

```
{

  "Version": "2012-10-17",
  "Statement": [
    {

      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:SimulatePrincipalPolicy",
        "autoscaling:\*",
        "sns:\*",
        "sqs:\*",
        "cloudwatch:\*",
        "ec2:AssignPrivateIpAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:AttachNetworkInterface",
```



```
21          "ec2:StartInstances",
22          "ec2:StopInstances"
23        ],
24        "Resource": "*"
25       }
26
27    ]
28   }
29
30  <!--NeedCopy-->
```

Registrieren Sie die DNS-Domain

Stellen Sie sicher, dass Sie die DNS-Domäne für das Hosten Ihrer Anwendungen registriert haben.

Bewerten Sie die Anzahl der Elastics IPs (EIP), die in Ihrem Netzwerk erforderlich sind.

Die Anzahl der erforderlichen EIPs hängt davon ab, ob Sie DNS-basierte Autoskalierung oder NLB-basierte Autoskalierung bereitstellen. Um die Anzahl der EIPs zu erhöhen, erstellen Sie einen Fall mit AWS.

- Bei der DNS-basierten automatischen Skalierung entspricht die Anzahl der erforderlichen EIPs pro Verfügbarkeitszone der Anzahl der Anwendungen, multipliziert mit der maximalen Anzahl der VPX-Instanzen, die Sie in den Autoscale-Gruppen konfigurieren möchten.
- Bei NLB-basierter Autoskalierung entspricht die Anzahl der erforderlichen EIPs der Anzahl der Anwendungen multipliziert mit der Anzahl der Availability Zones, in denen die Anwendungen bereitgestellt werden.

Bewerten der Instanzgrenzanforderungen

Stellen Sie bei der Bewertung der Instanzgrenzen sicher, dass Sie auch den Platzbedarf für Citrix ADC-Instanzen berücksichtigen.

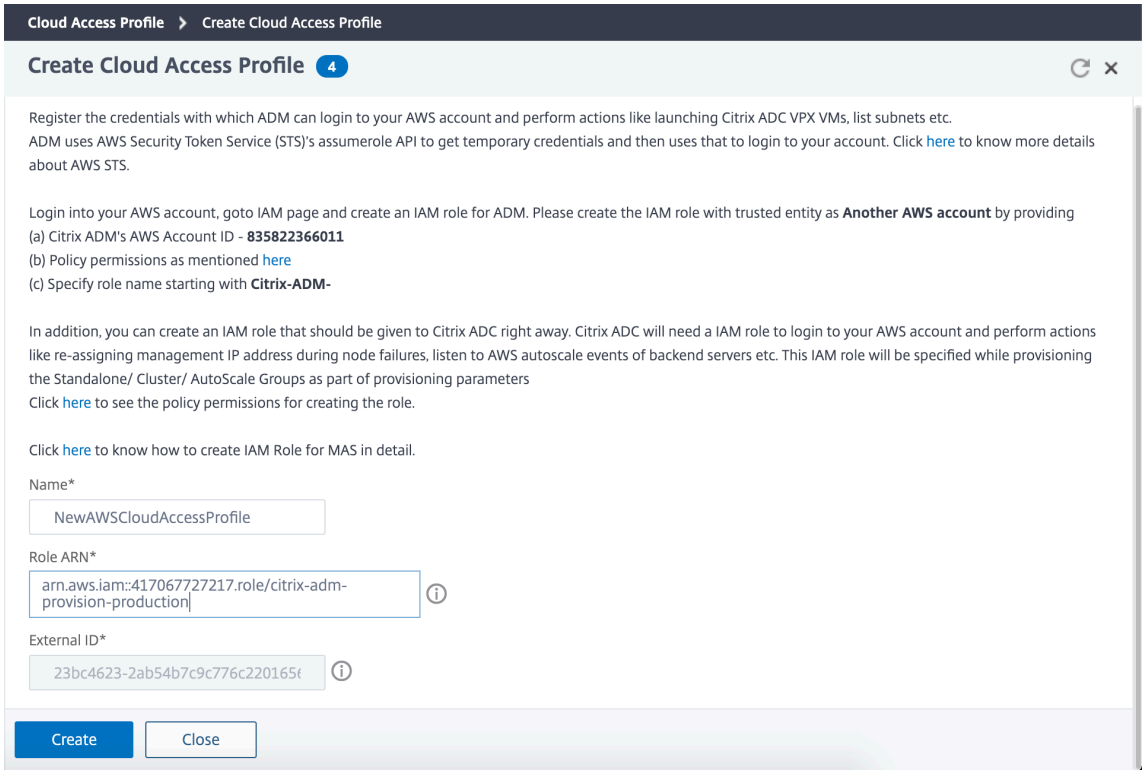
Voraussetzungen für Citrix ADM

Stellen Sie sicher, dass Sie alle Voraussetzungen für die Verwendung der Autoscale-Funktion von Citrix ADM erfüllt haben.

Erstellen einer Site

Erstellen Sie eine Site in Citrix ADM, und fügen Sie die Details der VPC hinzu, die Ihrer AWS-Rolle zugeordnet ist.

1. Navigieren Sie in Citrix ADM zu **Netzwerke > Sites**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie den Servicetyp als AWS aus, und aktivieren Sie **Vorhandene VPC als Site verwenden**.
4. Wählen Sie das Cloud-Zugriffsprofil aus.
5. Wenn das Cloud-Zugriffsprofil im Feld nicht vorhanden ist, klicken Sie auf **Hinzufügen**, um ein Profil zu erstellen.
   a) Geben Sie auf der Seite **Cloud Access-Profil erstellen** den Namen des Profils ein, mit dem Sie auf AWS zugreifen möchten.
   b) Geben Sie den ARN ein, der der Rolle zugeordnet ist, die Sie in AWS erstellt haben.
   c) Kopieren Sie die automatisch generierte **externe ID**, um die IAM-Rolle zu aktualisieren.
6. Klicken Sie auf **Erstellen**.
7. Klicken Sie erneut auf **Erstellen**, um die Website zu erstellen.
8. Aktualisieren Sie die IAM-Rolle in AWS mit der automatisch generierten **externen ID**:



   a) Melden Sie sich bei Ihrem AWS-Konto an, und navigieren Sie zu der Rolle, die Sie aktualisieren möchten.
   b) Klicken Sie auf der Registerkarte **Vertrauensstellungen** auf **Vertrauensstellung bearbeiten**, und fügen Sie die folgende Bedingung innerhalb des`Statement` Blocks an:


```
"Condition": {

  "StringEquals": {

    "sts:ExternalId": "<External-ID>"
   }

 }

<!--NeedCopy-->
```

Wenn Sie externe ID für eine IAM-Rolle in AWS aktivieren, können Sie eine Verbindung mit einem Drittanbieter-Konto herstellen. Die externe ID erhöht die Sicherheit Ihrer Rolle.

Die Details der VPC, wie Region, VPC-ID, Name und CIDR-Block, die Ihrer IAM-Rolle in AWS zugeordnet sind, werden in Citrix ADM importiert.

Bereitstellen des Citrix ADM Agenten in AWS

Der Citrix ADM-Dienst-Agent arbeitet als Vermittler zwischen Citrix ADM und den erkannten Instanzen im Rechenzentrum oder in der Cloud.

1. Navigieren Sie zu **Netzwerke > Agents**.
2. Klicken Sie auf **Bereitstellen**.
3. Wählen Sie **AWS** aus, und klicken Sie auf **Weiter**.
4. Geben Sie auf der Registerkarte **Cloud-Parameter** Folgendes an:
   - **Name**: Geben Sie den Namen des Citrix ADM Agenten an.
   - **Site** - Wählen Sie die Site aus, die Sie für die Bereitstellung eines Agenten und ADC-VPX-Instanzen erstellt haben.
   - **Cloud Access-Profil** - Wählen Sie das Cloud-Zugriffsprofil aus der Liste aus.
   - **Availability Zone** - Wählen Sie die Zonen aus, in denen Sie die Autoscale-Gruppen erstellen möchten. Abhängig von dem ausgewählten Cloud-Zugriffsprofil werden für dieses Profil spezifische Verfügbarkeitszonen aufgefüllt.
   - **Sicherheitsgruppe** — Sicherheitsgruppen steuern den eingehenden und ausgehenden Datenverkehr im Citrix ADC Agent. Sie erstellen Regeln für eingehenden und ausgehenden Datenverkehr, die Sie steuern möchten.
   - **Subnetz** - Wählen Sie das Management-Subnetz aus, in dem Sie einen Agenten bereitstellen möchten.

- **Tags** - Geben Sie das Schlüssel-Wert-Paar für die Autoscale Gruppentags ein. Ein Tag besteht aus einem Schlüssel-Wert-Paar, das zwischen Groß- und Kleinschreibung unterschieden wird. Diese Tags ermöglichen es Ihnen, die Autoskalierungsgruppen einfach zu organisieren und zu identifizieren. Die Tags werden sowohl auf AWS als auch auf Citrix ADM angewendet.

5. Klicken Sie auf **Fertig stellen**.

Alternativ können Sie den Citrix ADM -Agent über die AWS-Marketplace-Site installieren. Weitere Informationen finden Sie unter Installieren des Citrix ADM Agenten in AWS.

Erstellen von Gruppen mit automatischer Skalierung

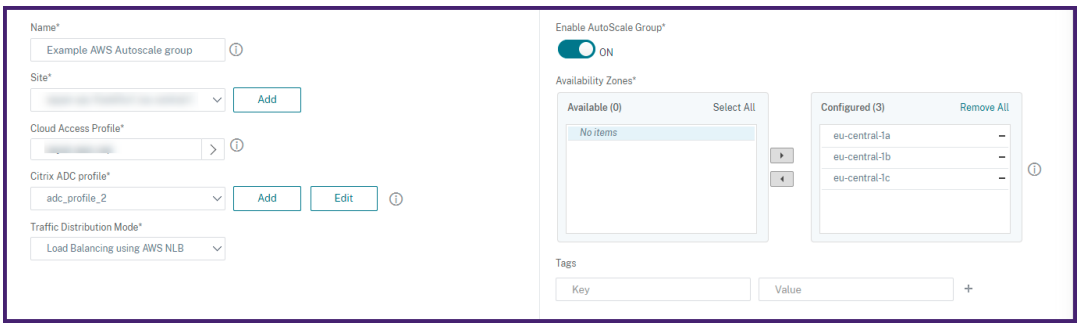
Konfiguration der automatischen Skalierung initialisieren

1. Navigieren Sie in Citrix ADM zu **Netzwerke > AutoScale Groups**.
2. Klicken Sie auf **Hinzufügen**, um Gruppen mit automatischer Skalierung zu erstellen. Die Seite **Create AutoScale Group** wird angezeigt.
3. Geben Sie die folgenden Details ein.

   - **Name**. Geben Sie einen Namen für die Gruppe Autoscale ein.
   - **Site**. Wählen Sie die Site aus, die Sie für die Bereitstellung der Citrix ADC VPX Instanzen in AWS erstellt haben.
   - **Agentin**. Wählen Sie den Citrix ADM Agent aus, der die bereitgestellten Instanzen verwaltet.
   - **Cloud-Zugriffsprofil**. Wählen Sie das Cloud-Zugriffsprofil aus.

     > **Hinweis**. Wenn das Cloud-Zugriffsprofil im Feld nicht vorhanden ist, klicken Sie auf **Hinzufügen**, um ein Profil zu erstellen.
     >
     > - Geben Sie den ARN ein, der der Rolle zugeordnet ist, die Sie in AWS erstellt haben.
     > - Geben Sie die externe ID ein, die Sie beim Erstellen einer IAM-Rolle (Identity and Access Management) in AWS angegeben haben. Abhängig vom ausgewählten Cloud-Zugriffsprofil werden die Availability Zones aufgefüllt.

   - **Geräteprofil**. Wählen Sie das Geräteprofil aus der Liste aus. Das Geräteprofil wird von Citrix ADM immer dann verwendet, wenn die Anmeldung an der Instanz erforderlich ist.
   - **Verkehrsverteilungsmodus**. Die Option **Lastenausgleich mit NLB** ist als Standard-Verteilungsmodus ausgewählt. Wenn Anwendungen UDP-Datenverkehr verwenden, wählen Sie **DNS mit AWS route53**aus.



> **Hinweis:**
>
> Nachdem die Konfiguration für die automatische Skalierung eingerichtet wurde, können keine neuen Availability Zones hinzugefügt werden oder vorhandene Availability Zones können nicht entfernt werden.

- **Enable AutoScale Group**. Aktivieren oder deaktivieren Sie den Status der ASG-Gruppen. Diese Option ist standardmäßig aktiviert. Wenn diese Option deaktiviert ist, wird die automatische Skalierung nicht ausgelöst.
- **Availability Zones**. Wählen Sie die Zonen aus, in denen Sie die Autoskalierungs-Gruppen erstellen möchten. Abhängig von dem ausgewählten Cloud-Zugriffsprofil werden für dieses Profil spezifische Verfügbarkeitszonen aufgefüllt.
- **Tags**. Geben Sie das Schlüssel-Wert-Paar für die Autoscale Gruppentags ein. Ein Tag besteht aus einem Schlüssel-Wert-Paar, das zwischen Groß- und Kleinschreibung unterschieden wird. Diese Tags ermöglichen es Ihnen, die Autoskalierungsgruppen einfach zu organisieren und zu identifizieren. Die Tags werden sowohl auf AWS als auch auf Citrix ADM angewendet.

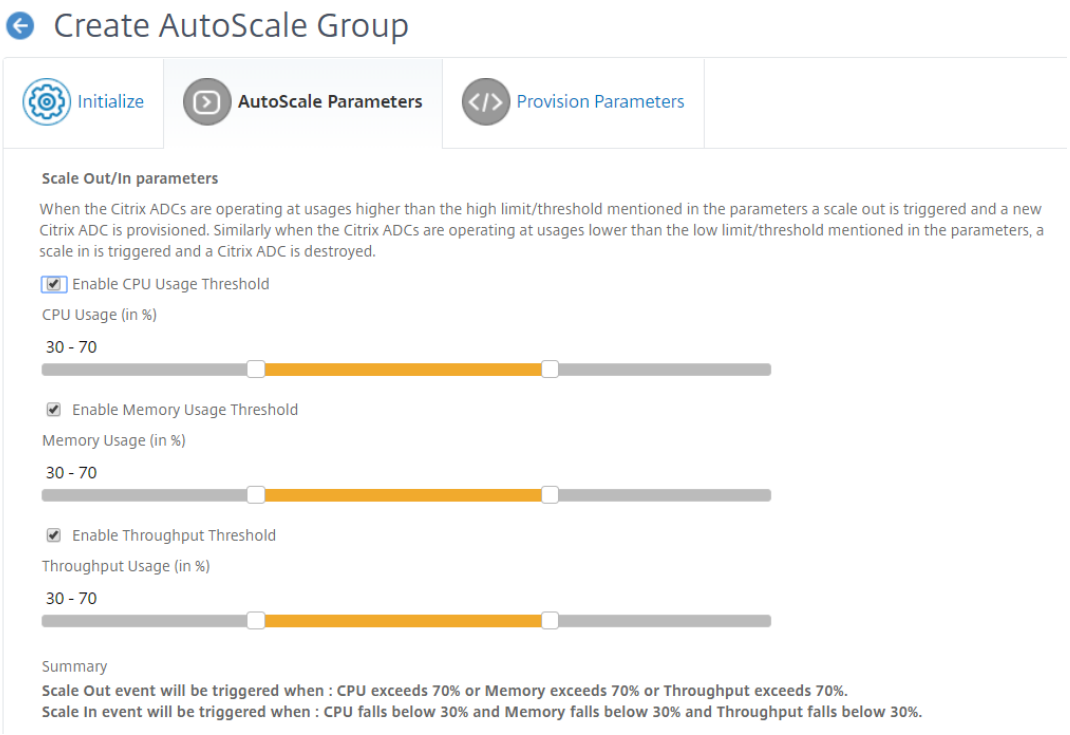
4. Klicken Sie auf **Weiter**.

Konfigurieren von Parametern für die automatische Skalierung

1. Geben Sie auf der Registerkarte **AutoScale-Parameter** die folgenden Details ein.
2. Wählen Sie einen oder mehrere der folgenden Schwellenwertparameter aus, deren Werte überwacht werden müssen, um ein Scale-Out oder ein Scale-In auszulösen.
   - **Schwellenwert für die CPU-Auslastung aktivieren**: Überwachen Sie die Metriken basierend auf der CPU-
   - **Schwellenwert für Speicherauslastung aktivieren**: Überwachen Sie die Metriken basierend auf der Speicherauslastung.
   - **Durchsatzschwellenwert aktivieren**: Überwachen Sie die Metriken basierend auf dem Durchsatz.

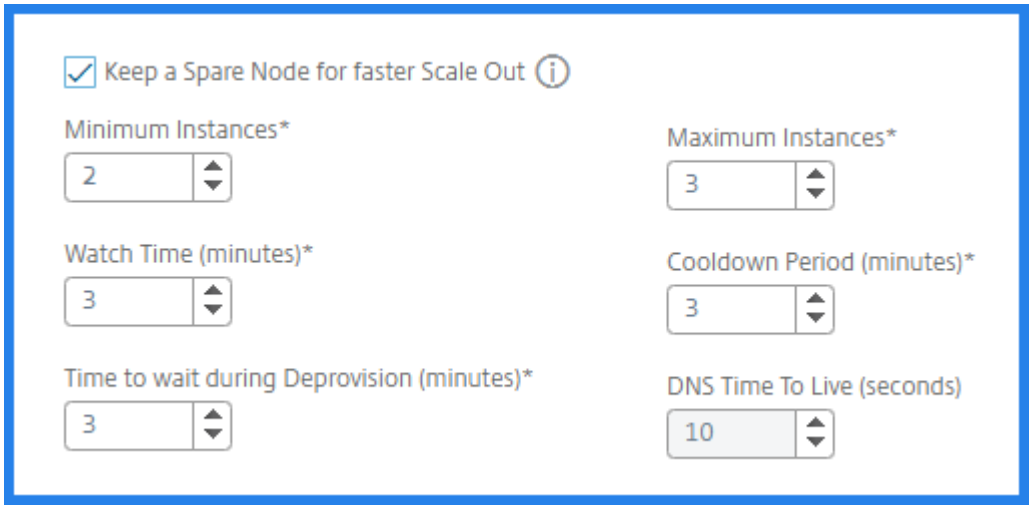
Hinweis

- Der standardmäßige Mindestschwellenwert beträgt 30 und der Höchstschwellenwert 70. Ändern Sie jedoch die Grenzwerte.
- Der Mindestgrenzwert muss gleich oder kleiner als die Hälfte des Höchstgrenzwerts sein.
- Für die Überwachung können mehrere Schwellenwerte ausgewählt werden. In solchen Fällen wird ein Scale-In ausgelöst, wenn mindestens einer der Schwellenwerte über dem maximalen Schwellenwert liegt. Ein Scale-In wird jedoch nur ausgelöst, wenn alle Schwellenwertparameter unterhalb ihrer normalen Schwellenwerte arbeiten.



- **Halten Sie einen Ersatzknoten für eine schnellere Scale-Out:** Diese Option hilft, eine schnellere Scale-Out zu erreichen. ADM stellt einen Reserve-Knoten bereit, bevor die Scale-Out-Aktion ausgeführt wird, und beendet ihn. Wenn die Scale-Out-Aktion für die Autoscale-Gruppe auftritt, startet der ADM den bereits bereitgestellten Ersatzknoten. Infolgedessen reduziert es die Zeit für das Scale-Out.
- **Minimale Instanzen**. Wählen Sie die Mindestanzahl von Instanzen aus, die für diese Gruppe für die automatische Skalierung bereitgestellt werden müssen.
- Standardmäßig ist die Mindestanzahl von Instanzen gleich der Anzahl der ausgewählten Zonen. Sie können die minimalen Instanzen um ein Vielfaches der Anzahl der Zonen erhöhen.

- Wenn beispielsweise die Anzahl der Availability Zones 4 beträgt, beträgt die Mindestinstanz standardmäßig 4. Sie können die minimalen Instanzen um 8, 12, 16 erhöhen.
- **Maximale Instanzen**. Wählen Sie die maximale Anzahl von Instanzen aus, die für diese Gruppe für die automatische Skalierung bereitgestellt werden müssen.
- Die maximale Anzahl von Instanzen muss größer oder gleich dem minimalen Instanzen sein. Die maximale Anzahl der Instanzen, die konfiguriert werden können, entspricht der Anzahl der Availability Zones multipliziert mit 32.
- Maximale Anzahl von Instanzen = Anzahl der Availability Zones * 32
- **Verbindungszeitüberschreitung entleeren (Minuten)**. Wählen Sie den Zeitüberschreitungszeitraum für die Ablaufverbindung aus. Sobald eine Instanz zum Aufheben der Bereitstellung ausgewählt wurde, entfernt Citrix ADM die Instanz während des Scale-Ins von der Verarbeitung neuer Verbindungen mit der Autoscale-Gruppe und wartet, bis die angegebene Zeit abläuft, bevor die Bereitstellung aufgehoben wird. Mit dieser Option können vorhandene Verbindungen zu dieser Instanz entfernt werden, bevor die Bereitstellung aufgehoben wird.
- **Abklingzeit (Minuten)**. Wählen Sie die Abklingzeit aus. Während des Scale-Outs ist die Abklingzeit die Zeit, für die die Auswertung der Statistiken nach einem Scale-Out gestoppt werden muss. Diese Scale-Out gewährleistet das organische Wachstum von Instanzen einer Autoscale-Gruppe, indem der aktuelle Datenverkehr stabilisiert und mit dem aktuellen Satz von Instanzen gemittelt werden kann, bevor die nächste Skalierungsentscheidung getroffen wird.
- **DNS Time To Live (Sekunden)**. Wählen Sie die Zeit (in Sekunden) aus, die ein Paket in einem Netzwerk existiert, bevor es von einem Router verworfen wird. Dieser Parameter ist nur anwendbar, wenn der Verkehrsverteilungsmodus DNS mit AWS route53 ist.
- **Uhrzeit (Minuten)**. Wählen Sie die Dauer der Uhr aus. Die Zeit, für die der Schwellenwert des Skalierungsparameters überschritten werden muss, damit eine Skalierung erfolgt. Wenn der Schwellenwert für alle Proben, die in dieser angegebenen Zeit gesammelt wurden, überschritten wird, geschieht eine Skalierung.



3. Klicken Sie auf **Weiter**.

Konfigurieren von Lizenzen für die Provisioning Citrix ADC-Instanzen

Wählen Sie einen der folgenden Modi aus, um Citrix ADC-Instanzen zu lizenzieren, die Teil der Autoscale Group sind:

- **Verwenden von Citrix ADM**: Beim Provisioning von Citrix ADC-Instanzen checkt die Autoscale-Gruppe die Lizenzen von Citrix ADM aus.
- **Verwenden der AWS Cloud**: Die Option **Aus Cloud zuweisen** verwendet die auf dem AWS-Marktplatz verfügbaren Citrix Produktlizenzen. Bei Provisioning Citrix ADC-Instanzen verwendet die Autoscale-Gruppe die Lizenzen vom Marketplace.

  Wenn Sie sich für die Verwendung von Lizenzen aus dem AWS-Marketplace entscheiden, geben Sie das Produkt oder die Lizenz auf der Registerkarte **Bereitstellungsparameter** an.

Weitere Informationen finden Sie unter Lizenzanforderungen.

Lizenzen von Citrix ADM verwenden

1. Wählen Sie auf der Registerkarte **Lizenz** die Option **Aus ADM zuweisen**.
2. Wählen Sie unter **Lizenztyp**eine der folgenden Optionen aus der Liste:
   - **Bandbreitenlizenzen:** Sie können eine der folgenden Optionen aus der Liste **Bandbreitenlizenztypen** auswählen:
     - **Pooled Capacity:** Geben Sie die Kapazität an, die für jede neue Instanz in der Gruppe Autoscale zugewiesen werden soll.

       Aus dem gemeinsamen Pool checkt jede ADC-Instanz in der Autoscale-Gruppe eine Instanzlizenz aus und es wird nur so viel Bandbreite angegeben.

  - **VPX-Lizenzen:** Wenn eine Citrix ADC VPX Instanz bereitgestellt wird, checkt die Instanz die Lizenz vom Citrix ADM aus.

- **Virtuelle CPU-Lizenzen:** Die bereitgestellte Citrix ADC VPX Instanz checkt Lizenzen in Abhängigkeit von der Anzahl der aktiven CPUs aus, die in der Autoscale-Gruppe ausgeführt werden.

> **Hinweis:**
>
> Wenn die bereitgestellten Instanzen entfernt oder gelöscht werden, kehren die angewendeten Lizenzen in den Citrix ADM -Lizenzpool zurück. Diese Lizenzen können für die Bereitstellung neuer Instanzen während der nächsten Autoscale wiederverwendet werden.

3. Wählen Sie in **License Edition** die Lizenzversion aus. Die Gruppe “Autoscale” verwendet die angegebene Edition zum Bereitstellen von Instanzen.
4. Klicken Sie auf **Weiter**.

Konfigurieren von Cloud-Parametern

1. Geben Sie auf der Registerkarte **Cloud-Parameter** die folgenden Details ein.
   - **IAM-Rolle**: Wählen Sie die IAM-Rolle aus, die Sie in AWS erstellt haben. Eine IAM-Rolle ist eine AWS-Identität mit Berechtigungsrichtlinien, die bestimmen, was die Identität in AWS tun kann und nicht.
   - **Produkt**: Wählen Sie die Citrix ADC Produktversion aus, die Sie bereitstellen möchten.
   - **Version**: Wählen Sie die Version und die Build-Nummer des Citrix ADC Produkts aus. Die Release-Versionen und Build-Nummern werden basierend auf dem ausgewählten Produkt automatisch ausgefüllt.
   - **AWS AMI-ID**: Geben Sie die AMI-ID ein, die für die ausgewählte Region spezifisch ist.
   - **Instanz-Typ**: Wählen Sie den EC2-Instanz-Typ aus.

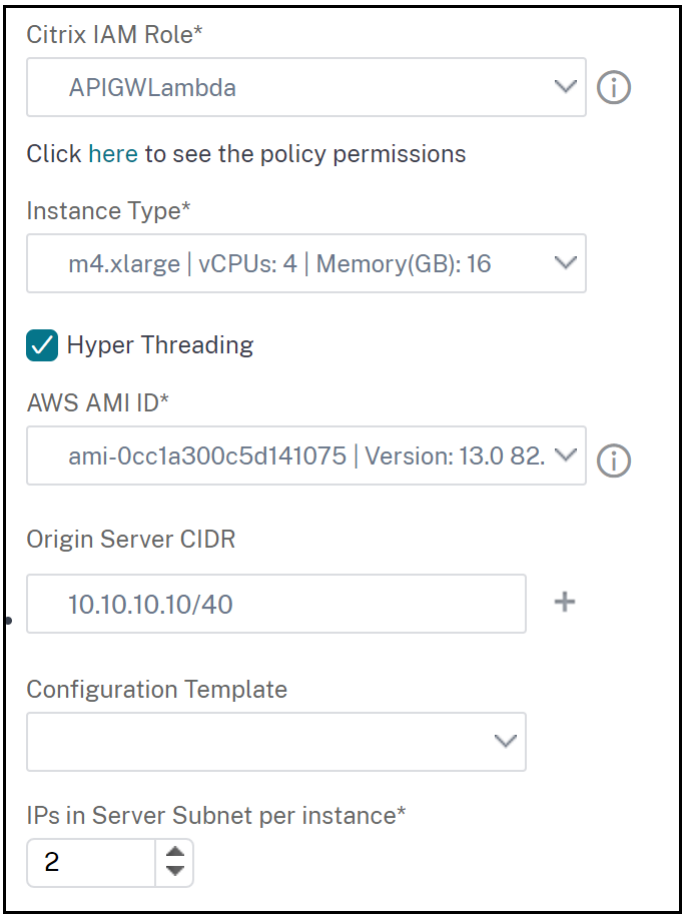
     > **Hinweis:**
     >
     > Der empfohlene Instanztyp für das ausgewählte Produkt wird standardmäßig automatisch ausgefüllt.

   - **Sicherheitsgruppen**: Sicherheitsgruppen steuern den eingehenden und ausgehenden Datenverkehr in der Citrix ADC VPX Instanz. Sie erstellen Regeln für eingehenden und ausgehenden Datenverkehr, die Sie steuern möchten. Wählen Sie die entsprechenden Werte für die folgenden Subnetze aus:
   - **Geschäftsführung**. Vorhandene Sicherheitsgruppe in Ihrem Konto für die Verwaltung von Citrix ADC VPX-Instanzen. Eingehende Regeln sind für die folgenden TCP- und UDP-Ports zulässig.

TCP: 80, 22, 443, 3008—3011, 4001
UDP: 67, 123, 161, 500, 3003, 4500, 7000

Stellen Sie sicher, dass die Sicherheitsgruppe es dem Citrix ADM Agent ermöglicht, auf das VPX zuzugreifen.

- **Client**: Vorhandene Sicherheitsgruppe in Ihrem Konto, die für die clientseitige Kommunikation von Citrix ADC VPX Instanzen bestimmt ist. In der Regel sind eingehende Regeln für die TCP-Ports 80, 22 und 443 zulässig.
- **Server**. Vorhandene Sicherheitsgruppe in Ihrem Konto für die serverseitige Kommunikation von Citrix ADC VPX.
- **IP-Adressen im Server-Subnetz pro Knoten**: Wählen Sie die Anzahl der IP-Adressen im Server-Subnetz pro Knoten für die Sicherheitsgruppe aus.



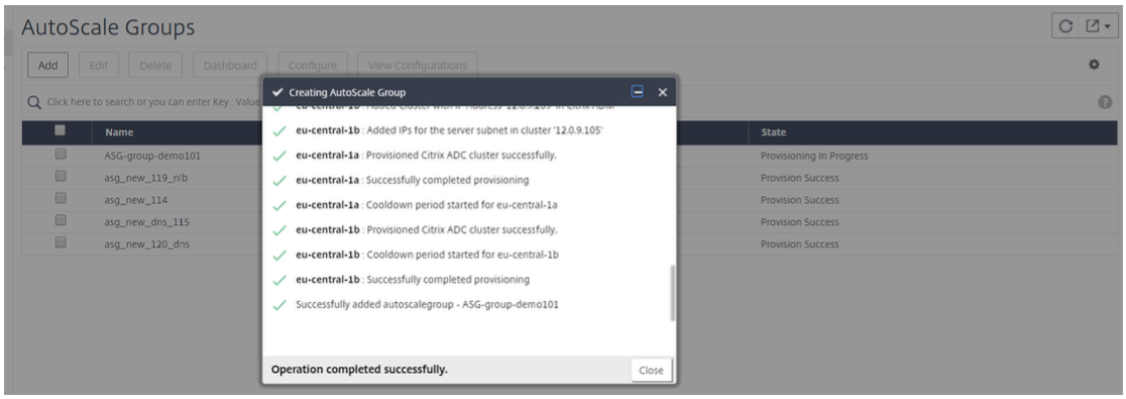
- **Zone**: Die Anzahl der aufgefüllten Zonen entspricht der Anzahl der von Ihnen ausgewählten Availability Zones. Wählen Sie für jede Zone die entsprechenden Werte für die folgenden Subnetze aus:
- **Geschäftsführung**. Vorhandenes Subnetz in Ihrer Virtual Private Cloud (VPC) für die Verwaltung. Citrix ADC muss sich an AWS-Services wenden und erfordert Internetzugang.

Konfigurieren Sie ein NAT-Gateway und fügen Sie einen Routentabelleneintrag hinzu, um den Internetzugang von diesem Subnetz zu ermöglichen.

- **Client**: Vorhandenes Subnetz in Ihrer Virtual Private Cloud (VPC), das für die Clientseite dediziert ist. In der Regel empfängt Citrix ADC Clientdatenverkehr für die Anwendung über ein öffentliches Subnetz aus dem Internet. Ordnen Sie das Clientsubnetz einer Routentabelle zu, die über eine Route zu einem Internet-Gateway verfügt. Mit diesem Subnetz kann Citrix ADC Anwendungsdatenverkehr aus dem Internet empfangen.
- **Server**. Anwendungsserver werden in einem Serversubnetz bereitgestellt. Alle Anwendungsserver befinden sich in diesem Subnetz und empfangen Anwendungsdatenverkehr vom Citrix ADC über dieses Subnetz.

2. Klicken Sie auf **Fertig stellen**.

   Es wird ein Fortschrittsfenster mit dem Status zum Erstellen der Gruppe “Automatische Skalierung” angezeigt. Es kann einige Minuten dauern, bis die Erstellung und Provisioning von Autoscale-Gruppen erstellt und bereitgestellt wird.



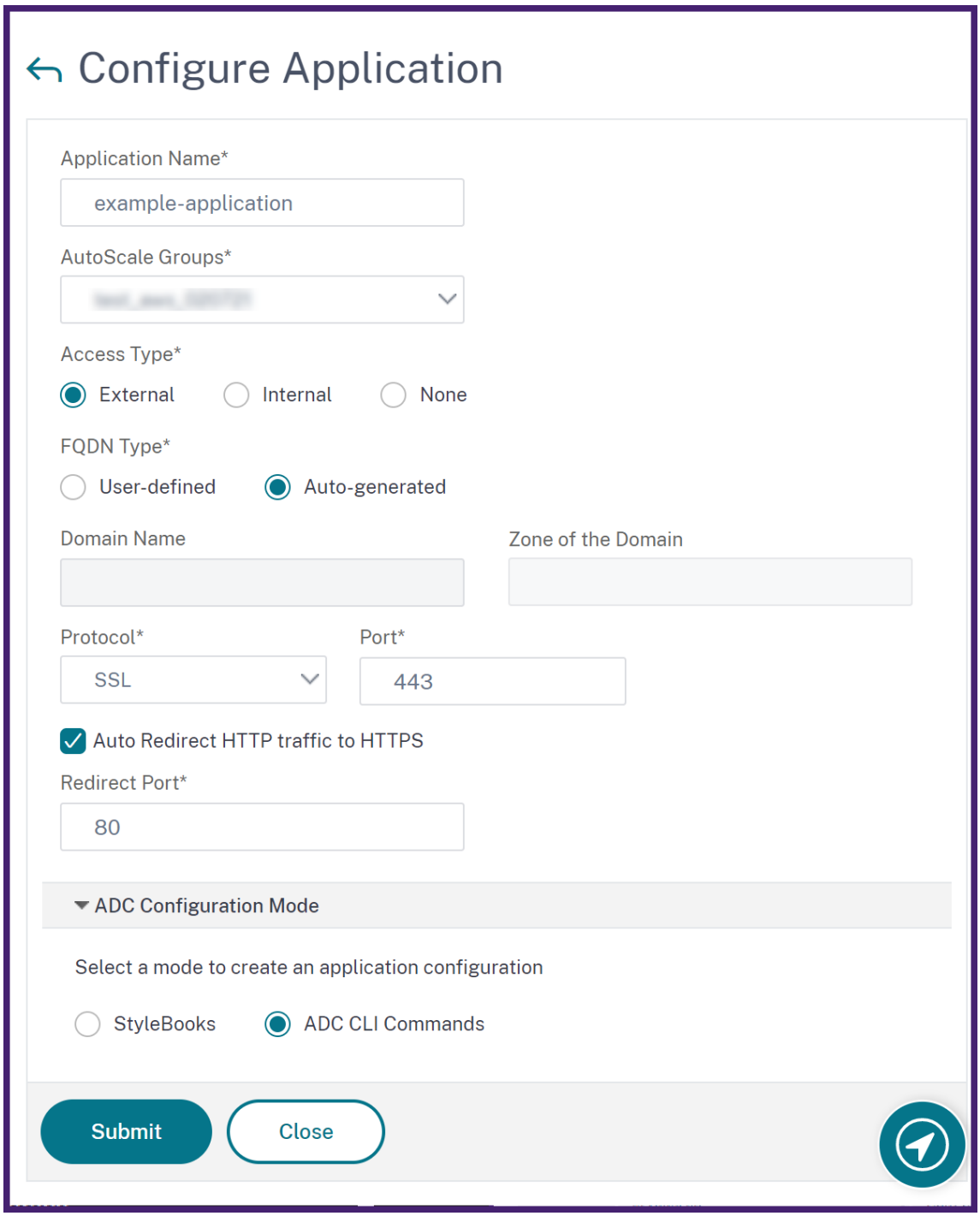
Konfigurieren einer Anwendung für die Autoscale-Gruppe

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Autoscale-Gruppen**.
2. Wählen Sie die von Ihnen erstellte Gruppe “Automatisch skalieren” aus, und klicken Sie auf **Konfigurieren**.
3. Geben Sie unter **Anwendung konfigurieren** die folgenden Details an:
   - **Anwendungsname** - Geben Sie den Namen einer Anwendung an.
   - **Zugriffstyp** - Sie können die ADM-Lösung für die automatische Skalierung sowohl für externe als auch für interne Anwendungen verwenden. Wählen Sie den erforderlichen Anwendungszugriffstyp aus.
   - **FQDN-Typ** - Wählen Sie einen Modus für die Zuweisung von Domänen- und Zonennamen aus.

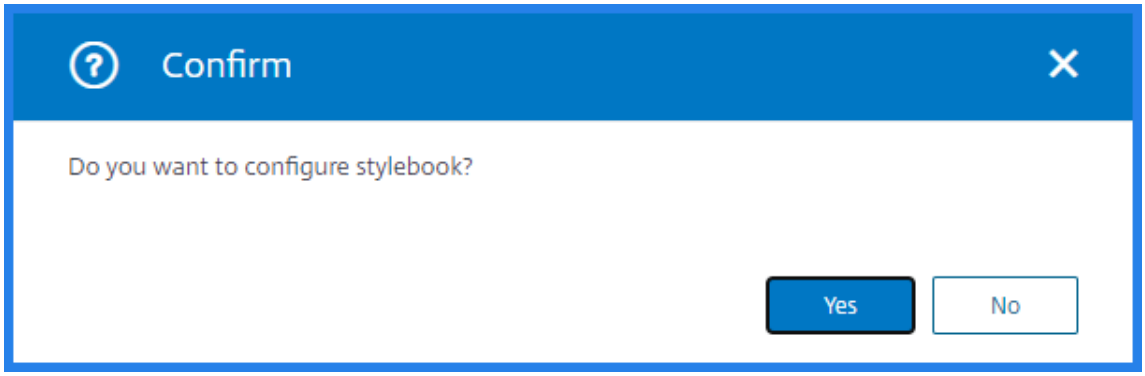
Wenn Sie manuell angeben möchten, wählen Sie **Benutzerdefiniert** aus. Um Domänen- und Zonennamen automatisch zuzuweisen, wählen Sie **Automatisch generiert** aus.

- **Domänenname** - Geben Sie den Domänennamen einer Anwendung an. Diese Option ist nur anwendbar, wenn Sie Benutzerdefinierter FQDN-Typ auswählen.
- **Zone der Domäne** - Wählen Sie den Zonennamen einer Anwendung aus der Liste aus. Diese Option ist nur anwendbar, wenn Sie Benutzerdefinierter FQDN-Typ auswählen.

  Dieser Domänen- und Zonenname leitet zu den virtuellen Servern in AWS um. Wenn Sie beispielsweise eine Anwendung in `app.example.com`hosten, ist `app`der Domänenname und `example.com`der Zonenname.
- **Protokoll** - Wählen Sie den Protokolltyp aus der Liste aus. Die konfigurierte Anwendung empfängt den Datenverkehr abhängig vom ausgewählten Protokolltyp.
- **Port** - Geben Sie den Portwert an. Der angegebene Port wird verwendet, um eine Kommunikation zwischen der Anwendung und der Autoscale-Gruppe herzustellen.



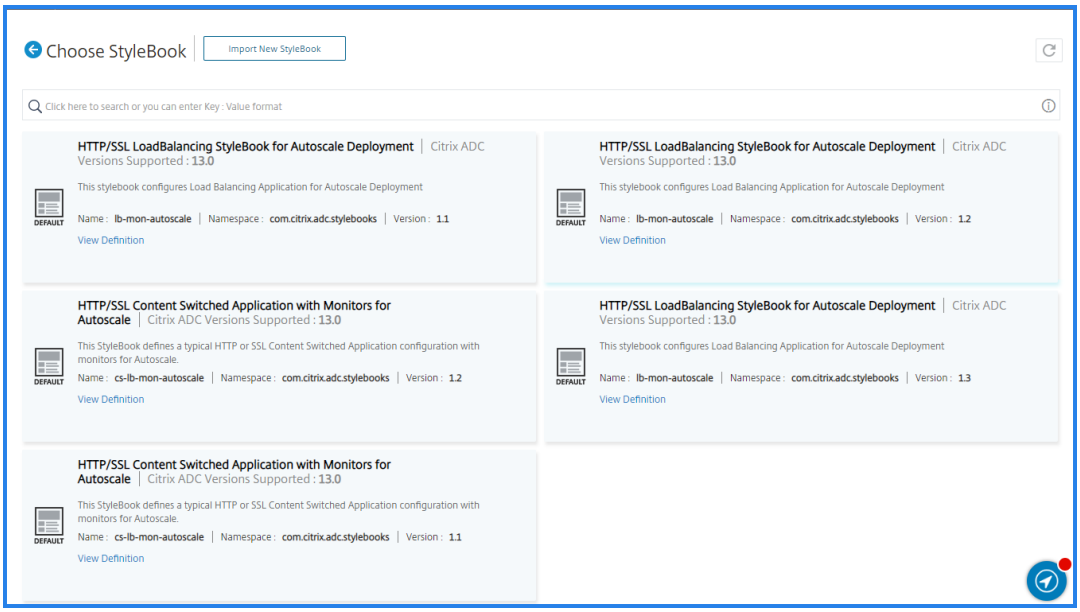
Wenn Sie eine Anwendung mit StyleBooks konfigurieren möchten, wählen Sie im Bestätigungsfenster **Ja** aus.



> **Hinweis Ändern Sie**
>
> den Zugriffstyp einer Anwendung, wenn Sie die folgenden Details in Zukunft ändern möchten:
>
> - FQDN Typ
> - Domänenname
> - Zone der Domäne

4. Auf der Seite **"StyleBook auswählen** " werden alle StyleBooks angezeigt, die für die Bereitstellung von Konfigurationen in den Clustern für die automatische Skalierung verfügbar sind.

   - Wählen Sie das entsprechende StyleBook aus. Sie können beispielsweise das **HTTP/SSL LoadBalancing StyleBook**verwenden. Sie können auch neue StyleBooks importieren.



   - Klicken Sie auf das StyleBook, um die erforderliche Konfiguration zu erstellen.
     Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
   - Geben Sie Werte für alle Parameter ein.

    - Wenn Sie Back-End-Server in AWS erstellen, wählen Sie Back-End-Serverkonfiguration aus. Wählen Sie anschließend **AWS EC2 Autoscaling** > **Cloud** aus und geben Sie die Werte für alle Parameter ein.
    - Je nach StyleBook, das Sie ausgewählt haben, können einige optionale Konfigurationen erforderlich sein. Beispielsweise müssen Sie möglicherweise Monitore erstellen, SSL-Zertifikateinstellungen angeben usw.
    - Klicken Sie auf **Erstellen**, um die Konfiguration im Citrix ADC Cluster bereitzustellen.

- Der FQDN der Anwendung oder des virtuellen Servers kann nicht geändert werden, nachdem er konfiguriert und bereitgestellt wurde.

  Der FQDN der Anwendung wird mithilfe von DNS in die IP-Adresse aufgelöst. Da dieser DNS-Eintrag möglicherweise über verschiedene Namensserver zwischengespeichert wird, kann das Ändern des FQDN dazu führen, dass der Datenverkehr Blackholed wird.

- Die SSL-Sitzungsfreigabe funktioniert wie erwartet innerhalb einer Availability Zone, aber über Availability Zones hinweg, erfordert eine erneute Authentifizierung.

  SSL-Sitzungen werden innerhalb des Clusters synchronisiert. Da die automatische Skalierung von Verfügbarkeitszonen über separate Cluster in jeder Zone verfügt, können SSL-Sitzungen nicht über Zonen hinweg synchronisiert werden.

- Gemeinsame Limits wie max Client und Spill-over werden statisch basierend auf der Anzahl der Availability Zones festgelegt. Legen Sie dieses Limit fest, nachdem Sie es manuell berechnet haben. `Limit = \<Limit required\>/\<number of zones\>`.

  Gemeinsame Grenzwerte werden automatisch auf Knoten innerhalb eines Clusters verteilt. Da die Gruppe “Autoscale”, die über Availability Zones erstreckt, separate Cluster in jeder Zone hat, müssen diese Grenzwerte manuell berechnet werden.

Upgrade von Citrix ADC Clustern

Aktualisieren Sie die Clusterknoten manuell. Sie aktualisieren zuerst das Image vorhandener Knoten und aktualisieren dann AMI vom Citrix ADM.

> **Wichtig**
>
> Stellen Sie während eines Upgrades Folgendes sicher:
>
> - Es wird kein Scale-In oder Scale-Out ausgelöst.
> - Im Cluster in der Gruppe Autoscale dürfen keine Konfigurationsänderungen vorgenommen werden.
> - Sie behalten ein Backup der `ns.conf`Datei der vorherigen Version. Falls ein Upgrade fehlschlägt, können Sie auf die vorherige Version zurückgreifen.

Führen Sie die folgenden Schritte aus, um die Citrix ADC Clusterknoten zu aktualisieren.

1. Deaktivieren Sie die Gruppe “Autoscale” im MAS ASG-Portal.
2. Wählen Sie einen der Cluster in den Gruppen für die automatische Skalierung für das Upgrade aus.
3. Befolgen Sie die im Thema dokumentierten SchritteAktualisieren oder Herabstufen des Citrix ADC Clusters.

   > **Hinweis**
   >
   > - Aktualisieren Sie einen Knoten im Cluster.
   > - Überwachen Sie den Anwendungsdatenverkehr auf Fehler.
   > - Wenn Probleme oder Fehler auftreten, sollten Sie den Knoten herabstufen, der zuvor aktualisiert wurde. Andernfalls fahren Sie mit dem Upgrade aller Knoten fort.

4. Fahren Sie mit dem Upgrade der Knoten in allen Clustern in der Gruppe Autoscale fort.

   > **Hinweis:**
   >
   > Wenn das Upgrade für einen Cluster fehlschlägt, führen Sie ein Downgrade aller Cluster in der Gruppe Autoscale auf die vorherige Version durch. Befolgen Sie die im Thema dokumentierten SchritteAktualisieren oder Herabstufen des Citrix ADC Clusters.

5. Nach erfolgreichem Upgrade aller Cluster aktualisieren Sie AMI auf MAS ASG Portal. AMI muss dieselbe Version haben wie das für das Upgrade verwendete Image.
6. Bearbeiten Sie die Gruppe Autoscale, und geben Sie das AMI ein, das der aktualisierten Version entspricht.
7. Aktivieren Sie die Gruppe “Autoscale” im ADM-Portal.

Ändern der Konfiguration von Gruppen für automatische Skalierung

- Sie können eine Autoscale-Gruppenkonfiguration ändern oder eine Autoscale-Gruppe löschen. Sie können nur die folgenden Gruppenparameter für die automatische Skalierung ändern.
  - Verkehrsverteilungsmodus
  - Maximal- und Minimalgrenzen der Schwellenwerte
  - Minimale und maximale Instanzwerte
  - Wert der Ablaufanschlussperiode
  - Wert der Abklingperiode
  - Time to live value — Wenn der Verkehrsverteilungsmodus DNS ist
  - Wert für die Dauer der Uhr
- Sie können auch die Autoskalier-Gruppen löschen, nachdem sie erstellt wurden.

Wenn Sie eine Autoscale-Gruppe löschen, werden alle Domänen und IP-Adressen von DNS/NLB abgemeldet und die Clusterknoten werden aufgehoben.

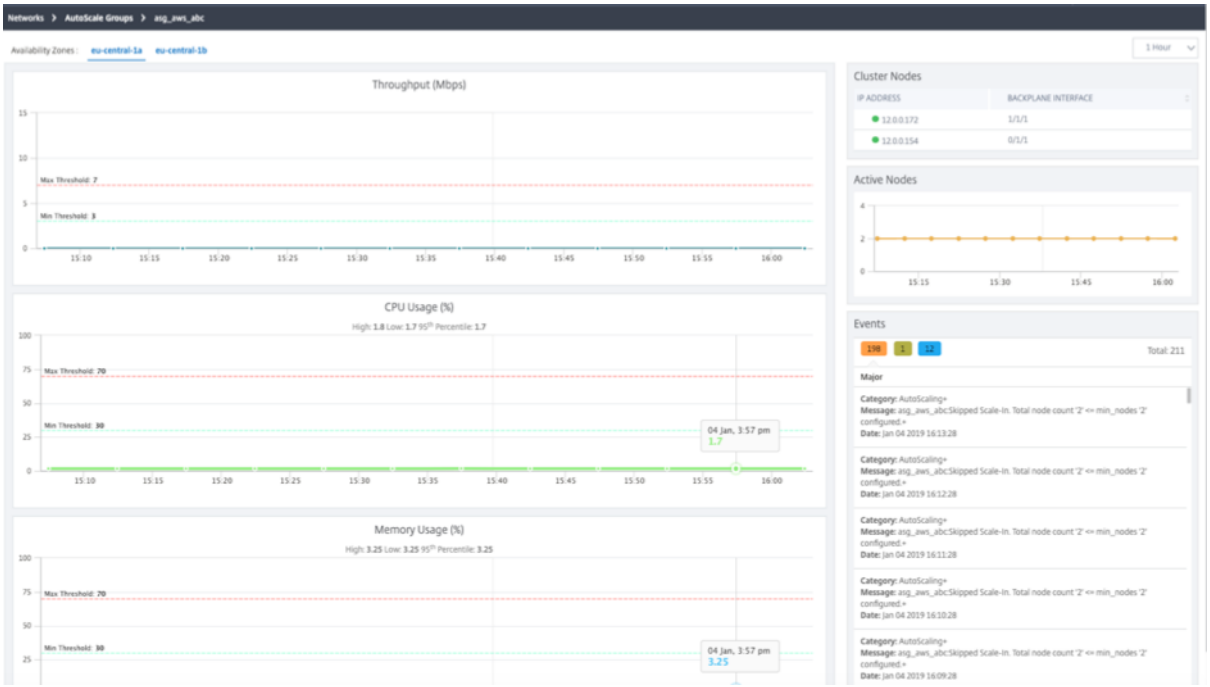
Dashboard

April 28, 2021

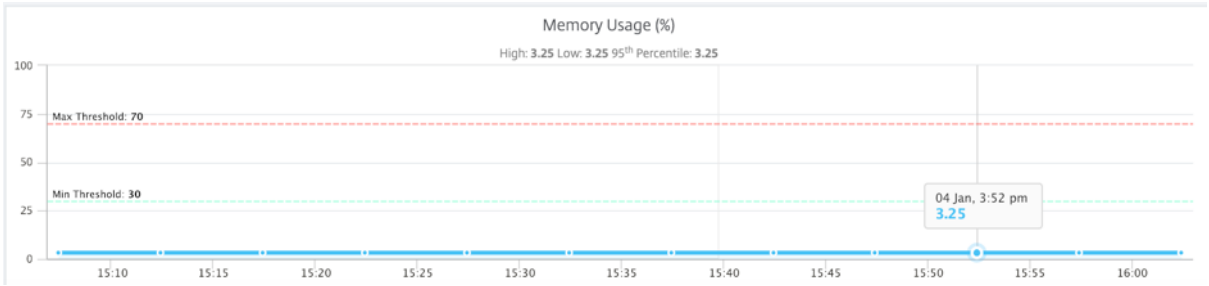
1. Navigieren Sie in Citrix ADM zu **Netzwerke > Gruppen automatisch skalieren**.
2. Wählen Sie die Autoscale-Gruppe und klicken Sie auf **Dashboard**

Sie können das Diagramm für die ausgewählten Überwachungsparameter anzeigen. Im rechten Bereich werden die Ereignisse angezeigt, die die automatische Skalierung auslösen. Im linken Bereich werden die aktiven Knoten im Cluster pro Zone, das Diagramm der aktiven Knoten und die Ereignisse angezeigt.

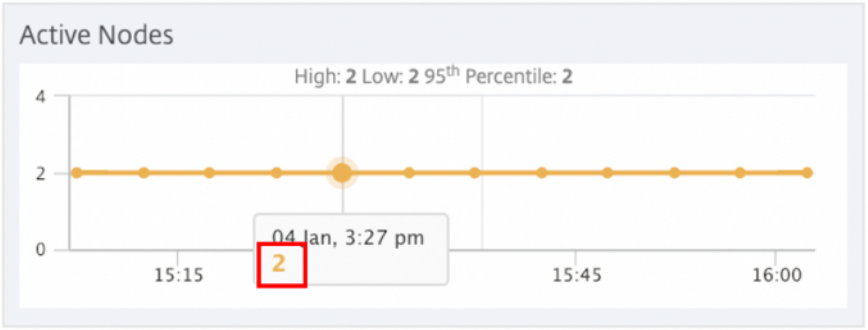
Die folgende Abbildung zeigt ein Beispiel-Dashboard.



Die folgende Abbildung zeigt Ereignisse zur Speichernutzung im Autoscale-Dashboard.



Die folgende Abbildung zeigt das Diagramm der aktiven Knoten. Die Zahl unter dem Zeitstempel zeigt die Anzahl der aktiven Knoten an. Sie können jederzeit die Anzahl der aktiven Knoten anzeigen, die Teil der Availability Zone sind.



Provisioning von Citrix ADC VPX Instanzen unter Microsoft Azure

April 28, 2021

Anwendungen oder Dienste, die in Azure gehostet werden, erfordern ein sicheres Datenverkehrsmanagement und eine effiziente Optimierung von Netzwerkressourcen sowie Cloud-Vorteile. Citrix ADC VPX Instanzen, die in Microsoft Azure bereitgestellt werden, bieten ein sicheres Datenverkehrsmanagement, einen optimierten Ressourcenverbrauch und geringere Kosten für Webanwendungen.

Mit Citrix ADM können Sie die Bereitstellung, Einrichtung und Verwaltung der ADC VPX-Instanzen in Azure automatisieren. Die Provisioning von Citrix ADC VPX Instanzen mit ADM kombiniert die Elastizität und Flexibilität der Cloud mit den Steuerungsfunktionen von Citrix ADC.

Unterstützte Citrix ADC Azure-Images für virtuelle Maschinen für Provisioning

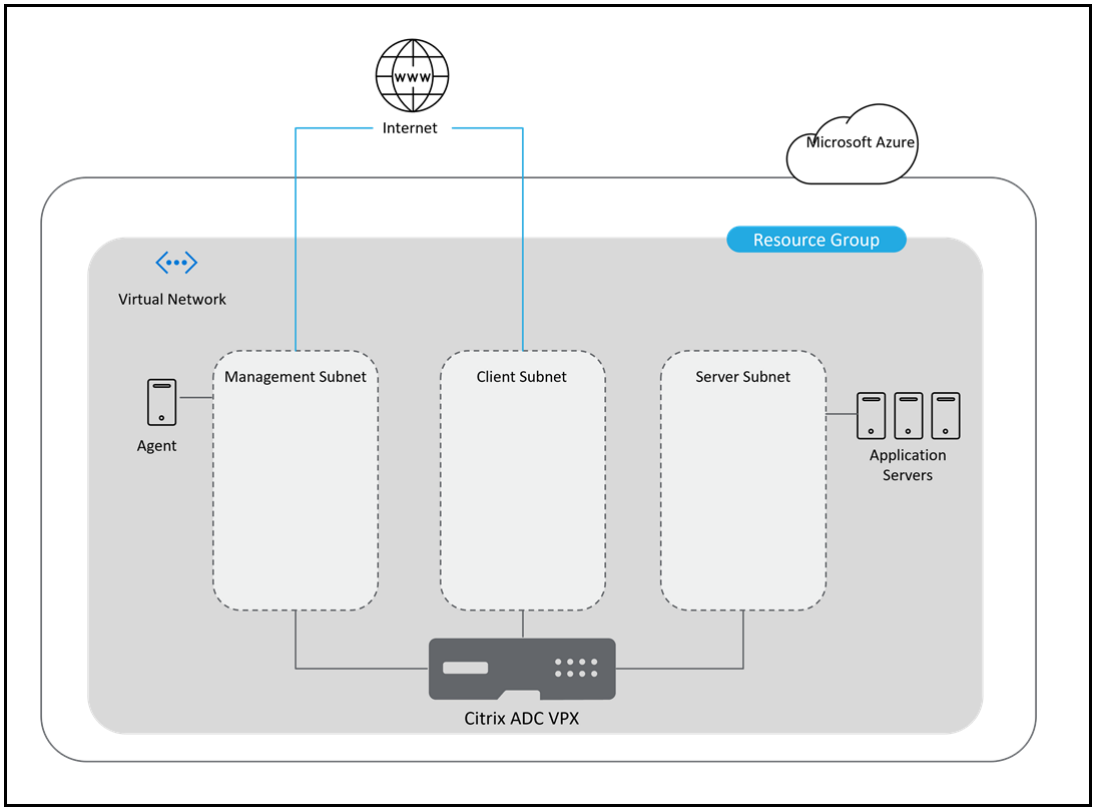
Verwenden Sie das Azure-Image für virtuelle Computer, das mindestens drei Netzwerkkarten unterstützt. Die Provisioning der Citrix ADC VPX Instanz wird nur in der Premium- und Advanced-Edition unterstützt. Weitere Informationen zu Azure-Imagetypen für virtuelle Computer finden Sie unter VM-Typen und -größen in der Microsoft-Dokumentation.

Im Folgenden sind die empfohlenen VM-Größen für die Provisioning:

- Standard_DS3_v2
- Standard_B2ms
- Standard_DS4_v2

Citrix ADM Bereitstellungsarchitektur

Das folgende Bild bietet einen Überblick darüber, wie Citrix ADM eine Verbindung mit Azure herstellt, um Citrix ADC VPX Instanzen in Microsoft Azure bereitzustellen.



Sie benötigen drei Subnetze, um die Citrix ADC VPX-Instanz in Microsoft Azure bereitzustellen und zu verwalten. Für jedes Subnetz muss eine Sicherheitsgruppe erstellt werden. Die im Citrix Gateway festgelegten Regeln regeln die Kommunikation über die Subnetze.

Der Citrix ADM Service Agent hilft Ihnen bei der Bereitstellung und Verwaltung der Citrix ADC VPX Instanz.

Voraussetzungen

In diesem Abschnitt werden die Voraussetzungen beschrieben, die Sie in Microsoft Azure und Citrix ADM ausführen müssen, bevor Sie Citrix ADC VPX Instanzen bereitstellen.

Dieses Dokument setzt Folgendes voraus:

- Sie verfügen über ein Microsoft Azure-Konto, das das Azure Resource Manager Bereitstellungsmodell unterstützt.
- Sie haben eine Ressourcengruppe in Microsoft Azure.

Weitere Informationen zum Erstellen eines Kontos und anderer Aufgaben finden Sie unter Microsoft Azure-Dokumentation.

Einrichten von Microsoft Azure-Komponenten

Führen Sie die folgenden Aufgaben in Azure aus, bevor Sie Citrix ADC VPX Instanzen in Citrix ADM bereitstellen.

1. Erstellen eines virtuellen Netzwerks.
2. Erstellen von Sicherheitsgruppen.
3. Subnetze erstellen.
4. Abonnieren der Citrix ADC VPX -Lizenz in Microsoft Azure.
5. Erstellen und Registrieren einer Anwendung.
6. Einrichten eines Citrix ADM Dienstagenten.

Erstellen eines virtuellen Netzwerks

1. Melden Sie sich bei Ihrem Microsoft Azure-Portal an.
2. Wählen Sie **Ressource erstellen** aus.
3. Wählen Sie **Netzwerk** aus, und klicken Sie auf **Virtuelles Netzwerk**.
4. Geben Sie die erforderlichen Parameter an.
    - In **Ressourcengruppe**müssen Sie die Ressourcengruppe angeben, in der Sie das Citrix ADC VPX-Produkt bereitstellen möchten.
    - In **Standort**müssen Sie die Standorte angeben, die Availability Zones unterstützen, z. B.:
        - USA, Mitte
        - Ost US2
        - Frankreich, Mitte
        - Europa, Norden
        - Südostasien
        - Westeuropa
        - West US2

> **Hinweis**
>
> Die in dieser Ressourcengruppe vorhandenen Anwendungsserver.

5. Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Azure Virtual Network in Microsoft-Dokumentation.

Erstellen von Sicherheitsgruppen

Erstellen Sie drei Sicherheitsgruppen in Ihrem virtuellen Netzwerk (VNet) - jeweils eine für die Verwaltungs-, Client- und Serververbindungen. Erstellen Sie eine Sicherheitsgruppe zur Steuerung des eingehenden und ausgehenden Datenverkehrs in der Citrix ADC VPX Instanz. Sie können beliebig viele Regeln hinzufügen.

- **Management:** Eine Sicherheitsgruppe in Ihrem Konto, die für die Verwaltung von Citrix ADC VPX vorgesehen ist. Citrix ADC muss sich an Azure-Dienste wenden und erfordert Internetzugang. Eingehende Regeln sind für die folgenden TCP- und UDP-Ports zulässig.
  - TCP: 80, 22, 443, 3008—3011, 4001
  - UDP: 67, 123, 161, 500, 3003, 4500, 7000

  > **Hinweis**
  >
  > Stellen Sie sicher, dass die Sicherheitsgruppe es dem Citrix ADM Agent ermöglicht, auf das VPX zuzugreifen.

- **Client:** Eine Sicherheitsgruppe in Ihrem Konto, die für die clientseitige Kommunikation von Citrix ADC VPX Instanzen bestimmt ist. In der Regel sind eingehende Regeln für die TCP-Ports 80, 22 und 443 zulässig.
- **Server:** Eine Sicherheitsgruppe in Ihrem Konto, die für die serverseitige Kommunikation von Citrix ADC VPX bestimmt ist.

Weitere Informationen zum Erstellen einer Sicherheitsgruppe in Microsoft Azure finden Sie unter Erstellen, Ändern oder Löschen einer Netzwerksicherheitsgruppe.

Subnetze erstellen

Erstellen Sie drei Subnetze in Ihrem virtuellen Netzwerk (VNet) - jeweils eines für die Management-, Client- und Serververbindungen. Geben Sie einen Adressbereich an, der in Ihrem VNet für jedes Subnetz definiert ist. Geben Sie die Verfügbarkeitszone an, in der sich das Subnetz befinden soll.

- **Verwaltung:** Ein Subnetz in Ihrem virtuellen Netzwerk (VNet), das für die Verwaltung bestimmt ist. Citrix ADC muss sich an Azure-Dienste wenden und erfordert Internetzugang.
- **Client:** Ein Subnetz in Ihrem virtuellen Netzwerk (VNet), das für die Client-Seite dediziert ist. In der Regel empfängt Citrix ADC Clientdatenverkehr für die Anwendung über ein öffentliches Subnetz aus dem Internet.

- **Server:** Ein Subnetz, in dem die Anwendungsserver bereitgestellt werden. Alle Ihre Anwendungsserver sind in diesem Subnetz vorhanden und empfangen Anwendungsdatenverkehr vom Citrix ADC über dieses Subnetz.

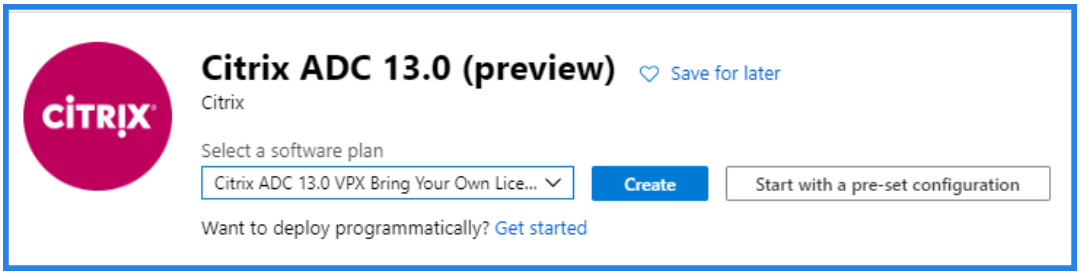
> **Hinweis**
>
> Geben Sie beim Erstellen eines Subnetzes eine geeignete Sicherheitsgruppe für das Subnetz an.

Weitere Informationen zum Erstellen eines Subnetzes in Microsoft Azure finden Sie unter Hinzufügen, Ändern oder Löschen eines virtuellen Netzwerksubnetzes.

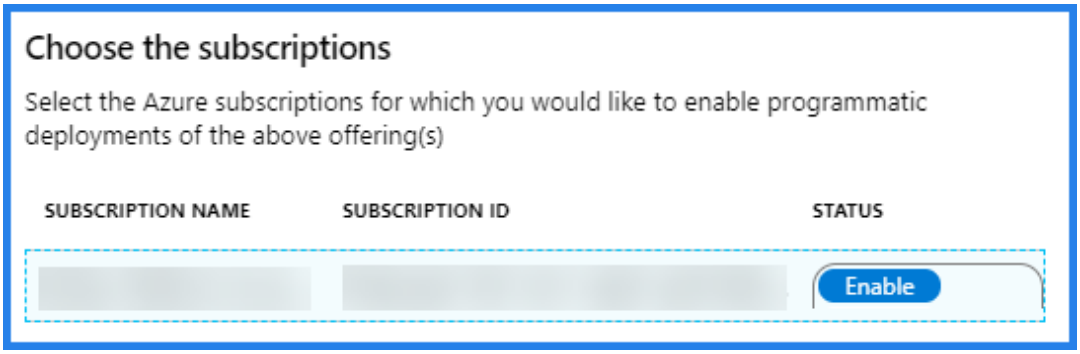
Abonnieren der Citrix ADC VPX -Lizenz in Microsoft Azure

1. Melden Sie sich bei Ihrem Microsoft Azure-Portal an.
2. Wählen Sie **Ressource erstellen** aus.
3. **Suchen Sie in der Leiste Marketplace** durchsuchen die gewünschte Produktversion`Citrix ADC` und wählen Sie sie aus.
4. **Wählen Sie in der Liste Softwareplan** auswählen einen der folgenden Lizenztypen aus:
   - Eigene Lizenz
   - Erweitert
   - Premium

   > **Hinweis**
   >
   > - Wenn Sie die Option **Eigene Lizenz mitbringen** wählen, checkt die Instanz, die Sie bereitstellen möchten, die Lizenzen aus dem Citrix ADM aus, während Sie Citrix ADC-Instanzen bereitstellen.
   > - In Citrix ADM sind **Advanced** und **Premium** die entsprechenden Lizenztypen für **Enterprise** bzw. **Platinum**.
5. Stellen Sie sicher, dass die programmatische Bereitstellung für das ausgewählte Citrix ADC Produkt aktiviert ist.
   a) Klicken Sie neben **Möchten Sie programmgesteuert bereitstellen?** auf **Erste Schritte**.



   b) Wählen Sie unter **Abonnements auswählen** die Option **Aktivieren** aus, um die ausgewählte Citrix ADC VPX Edition programmgesteuert bereitzustellen.



> **Wichtig**
>
> Die Aktivierung der programmatischen Bereitstellung ist erforderlich, um Citrix ADC VPX Instanzen in Azure bereitzustellen.

c) Klicken Sie auf **Save**.

d) Schließen Sie **Programmatische Bereitstellung konfigurieren**.

6. Klicken Sie auf **Erstellen**.

Erstellen und Registrieren einer Anwendung

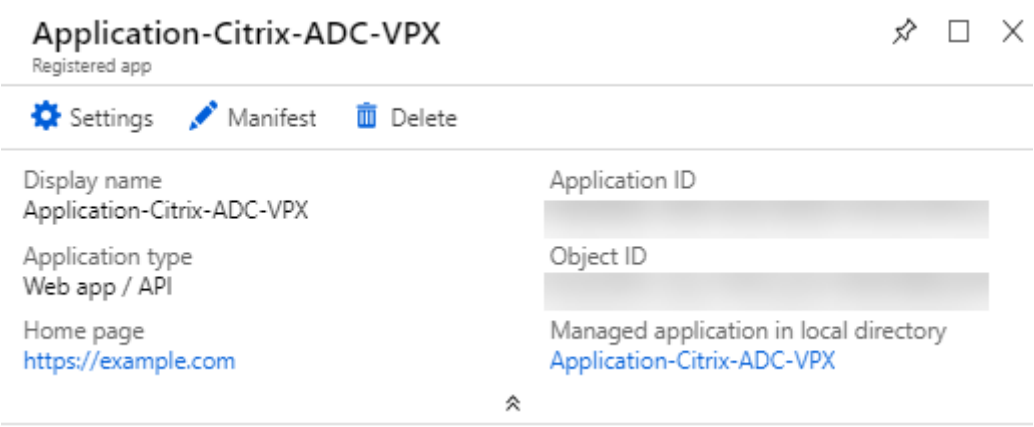
Citrix ADM verwendet diese Anwendung, um Citrix ADC VPX Instanzen in Azure bereitzustellen.

So erstellen und registrieren Sie eine Anwendung in Azure:

1. Wählen Sie im Azure-Portal **Azure Active Directory** aus.
   Diese Option zeigt das Verzeichnis Ihrer Organisation an.
2. Wählen Sie **App-Registrierungen** aus:
   a) Geben Sie unter **Name** den Namen der Anwendung an.
   b) Wählen Sie in der Liste den **Anwendungstyp** aus.
   c) Geben Sie in der **Anmelde-URL die Anwendungs-URL** für den Zugriff auf die Anwendung an.
3. Klicken Sie auf **Erstellen**.

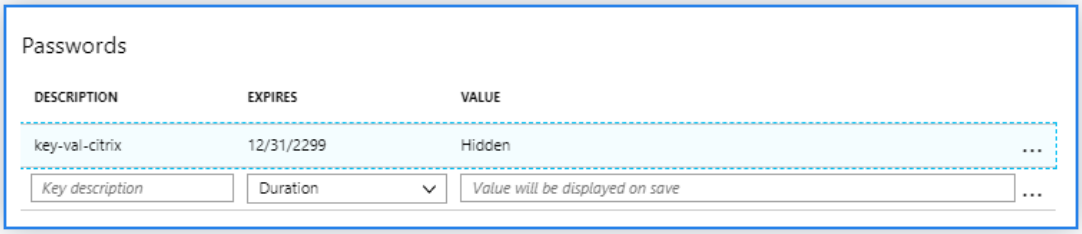
Weitere Informationen zu App-Registrierungen finden Sie unter Microsoft-Dokumentation.

Azure weist der Anwendung eine Anwendungs-ID zu. Im Folgenden finden Sie eine Beispielanwendung, die in Microsoft Azure registriert ist:



Kopieren Sie die folgenden IDs und geben Sie diese IDs an, wenn Sie ein Cloud Access-Profil in Citrix ADM konfigurieren:

- **Anwendungs-ID:** Für Schritte zum Abrufen der Anwendungs- oder Client-ID.
- **Verzeichnis-ID:** Für Schritte zum Abrufen des Verzeichnisses, des Mandanten oder der Objekt-ID.
- **Schlüssel:** Für Schritte zum Abrufen des Schlüsselwerts oder der Clientgeheimnis-ID.



- **Abonnement-ID:** Kopieren Sie die Abonnement-ID aus Ihrem Speicherkonto.

Weitere Informationen finden Sie unter Microsoft-Dokumentation.

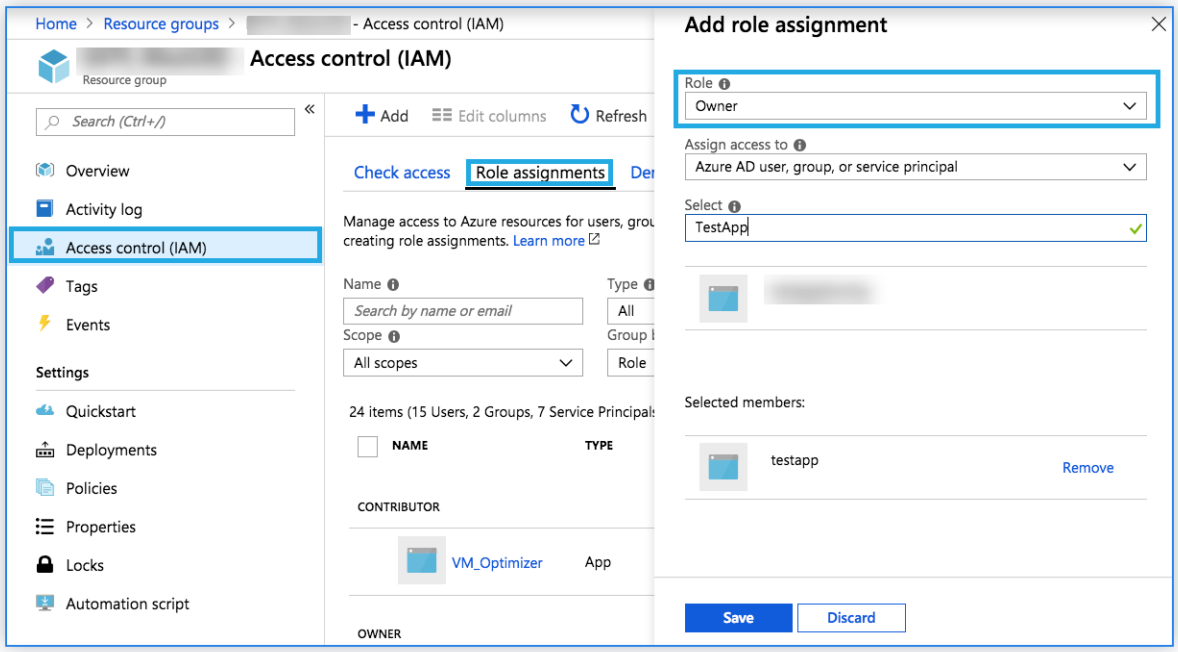
Zuweisen der Rollenberechtigung zu einer Anwendung

Citrix ADM verwendet das Application-as-a-Service-Prinzip, um Citrix ADC-Instanzen in Microsoft Azure bereitzustellen. Diese Berechtigung gilt nur für die ausgewählte Ressourcengruppe.

Um Ihrer registrierten Anwendung eine Rollenberechtigung zuzuweisen, müssen Sie Eigentümer des Microsoft Azure-Abonnements sein.

1. Wählen Sie im Azure-Portal **Ressourcengruppen**aus.
2. Wählen Sie die Ressourcengruppe aus, der Sie die Rollenberechtigung zuweisen möchten.
3. Wählen Sie **Zugriffssteuerung (IAM)** aus.
4. Klicken Sie unter **Rollenzuweisungen** auf **Hinzufügen**.

5. Wählen Sie **Besitzer** aus der Liste **Rolle** aus.
6. Wählen Sie die Anwendung aus, die für die Provisioning Citrix ADC-Instanzen registriert ist. Siehe Erstellen und Registrieren einer Anwendung.
7. Klicken Sie auf **Save**.



Einrichten eines Citrix ADM Dienstagenten

Installieren Sie einen Citrix ADM Dienst-Agent im Verwaltungssubnetz. Dieser Agent arbeitet als Vermittler zwischen Citrix Application Delivery Management (Citrix ADM) und den verwalteten Instanzen in Microsoft Azure. Weitere Informationen zum Installieren des Citrix ADM Dienstagenten in Microsoft Azure finden Sie unter Installieren des Citrix ADM-Agenten in der Microsoft Azure-Cloud.

Einrichten von Citrix ADM Komponenten

Führen Sie die folgenden Aufgaben in Azure aus, bevor Sie Citrix ADC VPX Instanzen in Citrix ADM bereitstellen:

1. Erstellen einer Site.
2. Anfügen der Site an einen Citrix Service-Agent.

Erstellen einer Site in Citrix ADM

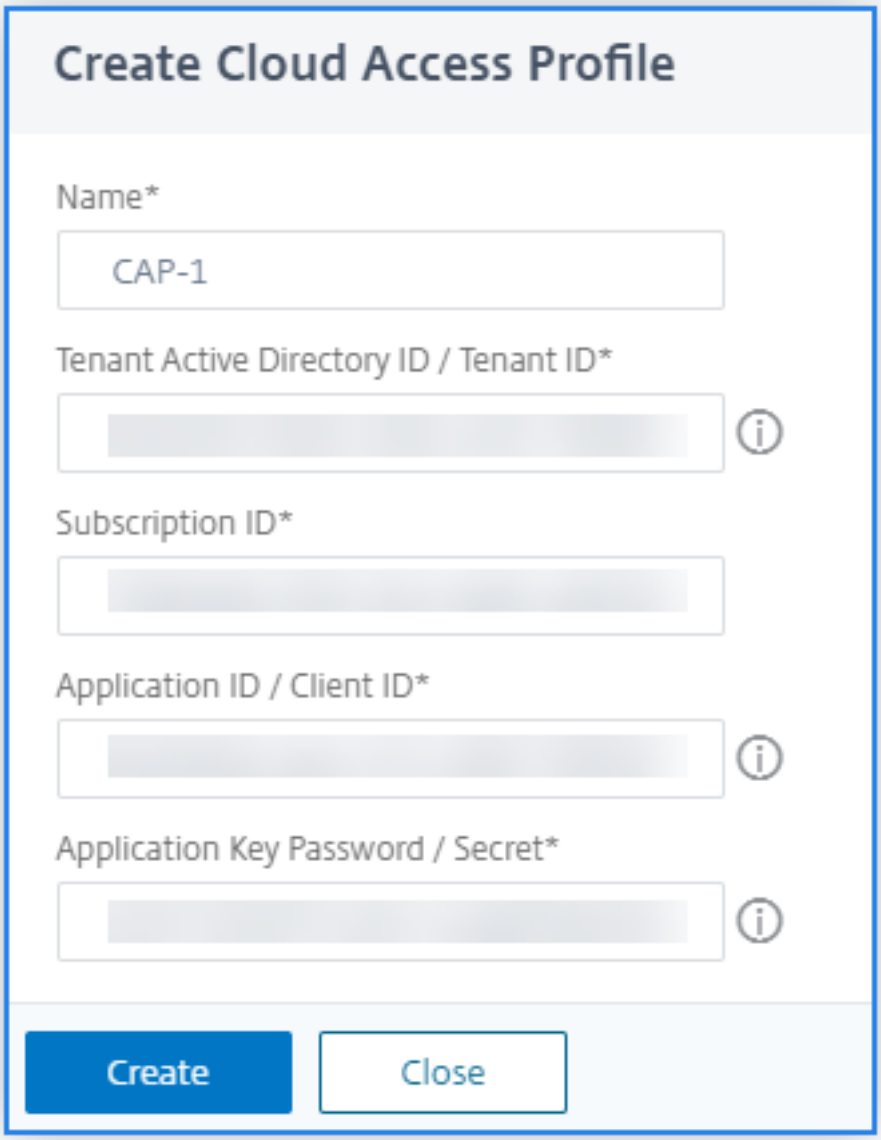
Erstellen Sie eine Site in Citrix ADM, und fügen Sie die VNet-Details hinzu, die Ihrer Microsoft Azure-Ressourcengruppe zugeordnet sind.

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Sites**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie im Bereich **Cloud auswählen**
   a) Wählen Sie **Data Center** als **Standorttyp** aus.
   b) Wählen Sie in der Liste **Typ** die Option **Azure** aus.
   c) Aktivieren Sie das Kontrollkästchen **VNet aus Azure abrufen**.

      Mit dieser Option können Sie die vorhandenen VNet-Informationen aus Ihrem Microsoft Azure-Konto abrufen.

   d) Klicken Sie auf **Weiter**.
4. **Wählen Sie im Bereich Region auswählen**
   a) Wählen Sie im **Cloud Access-Profil** das Profil aus, das für Ihr Microsoft Azure-Konto erstellt wurde. Wenn keine Profile vorhanden sind, erstellen Sie ein Profil.
   b) Klicken Sie auf **Hinzufügen**, um ein Cloud-Zugriffsprofil zu erstellen.
   c) Geben Sie unter **Name** einen Namen an, um Ihr Azure-Konto in Citrix ADM zu identifizieren.
   d) Geben Sie unter **Mandanten-Active Directory ID/Mandanten-ID** die Active Directory-ID des Mandanten oder das Konto in Microsoft Azure an.
   e) Geben Sie die **Abonnement-ID** an.
   f) Geben Sie die **Anwendungs-ID/Client-ID** an.
   g) Geben Sie das **Kennwort für den Anwendungsschlüssel** an.
   h) Klicken Sie auf **Erstellen**.

      Weitere Informationen finden Sie unter Erstellen und Registrieren einer Anwendung und Zuordnung des Cloud-Zugriffsprofils zur Azure-Anwendung.



i) Wählen Sie in **VNet** das virtuelle Netzwerk aus, das Citrix ADC VPX Instanzen enthält, die Sie verwalten möchten.

j) Geben Sie einen **Standortnamen** an.

k) Klicken Sie auf **Fertig stellen**.

Zuordnen von Cloud-Zugriffsprofil zu Azure-Anwendung

Citrix ADM Begriff	Microsoft Azure-Begriff
Mandanten-Active Directory ID/Mandanten-ID	Verzeichnis-ID

Citrix ADM Begriff	Microsoft Azure-Begriff
Abonnement-ID	Abonnement-ID
Anwendungs-ID/Client-ID	Anwendungs-ID
Kennwort des Anwendungsschlüssels/Secret	Schlüssel oder Zertifikate oder Client-Geheimnisse

Anfügen der Site an einen Citrix ADM Dienstagenten

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Agents**.
2. Wählen Sie den Agenten aus, für den Sie eine Site anhängen möchten.
3. Klicken Sie auf **Site anhängen**.
4. Wählen Sie die Website aus der Liste aus, die Sie hinzufügen möchten.
5. Klicken Sie auf **Save**.

Konfigurationsaufgaben

Verwenden Sie die Website, die Sie Ihrer Microsoft Azure-Ressourcengruppe zugeordnet haben, um die Citrix ADC VPX Instanzen bereitzustellen. Geben Sie Details des Citrix ADM Dienstagenten an, um die Instanzen bereitzustellen, die an diesen Agent gebunden sind.

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Klicken Sie auf der Registerkarte **VPX** auf **Bereitstellung**.

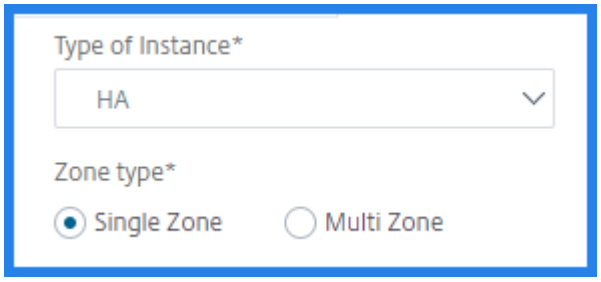
   Mit dieser Option wird die Seite **Citrix ADC VPX in der Cloud bereitstellen** angezeigt.
3. Wählen Sie **Microsoft Azure** aus, und klicken Sie auf **Weiter**. Geben Sie die erforderlichen Parameter für die Bereitstellung einer Instanz an.

Konfigurieren Sie grundlegende Parameter

1. Geben Sie auf der Registerkarte **Grundparameter** Folgendes an:
   - **Instanz**: Wählen Sie eine der folgenden Optionen aus der Liste aus.
     - **Standalone** - Diese Option stellt eine eigenständige Citrix ADC VPX Instanz unter Microsoft Azure bereit.
     - **HA:** Diese Option stellt die hochverfügbaren Citrix ADC VPX Instanzen in Microsoft Azure bereit.

Um die Citrix ADC VPX Instanzen in derselben Zone bereitzustellen, wählen Sie unter **Zonentyp** die Option **Einzelne Zone** aus.

Um die Citrix ADC VPX Instanzen über mehrere Zonen hinweg bereitzustellen, wählen Sie unter **Zonentyp** die Option **Multi Zone** aus. Stellen Sie auf der Registerkarte **Cloud-Parameter** sicher, dass Sie die Netzwerkdetails für jede Zone angeben, die in Microsoft Azure erstellt werden.

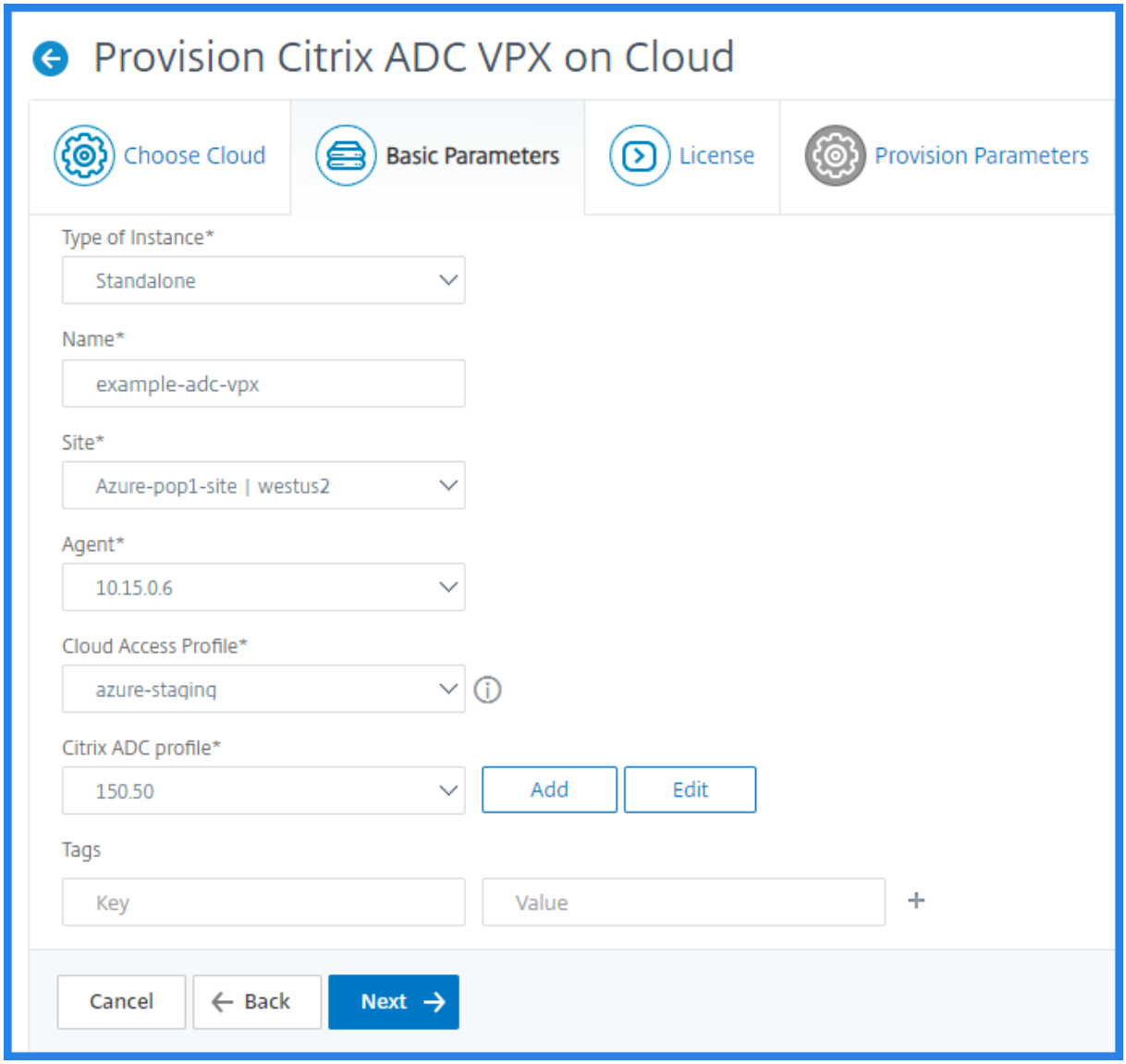


- **Name** - Geben Sie den Namen einer ADC VPX-Instanz an.
- **Site** — Wählen Sie die Website aus, die Sie zuvor erstellt haben.
- **Agent** : Wählen Sie den Agenten aus, der zur Verwaltung der Citrix ADC VPX-Instanz erstellt wurde.
- **Cloud Access-Profil** — Wählen Sie das Cloud-Zugriffsprofil aus, das während der Erstellung der Website erstellt wurde
- **Citrix ADC Profile** - Wählen Sie das Profil aus, das die Authentifizierung bereitstellen soll.

  Citrix ADM verwendet das Geräteprofil, wenn es sich bei der Citrix ADC VPX Instanz anmelden muss.

  > **Hinweis**
  >
  > Stellen Sie sicher, dass das ausgewählte Geräteprofil den Microsoft Azure-Kennwortregelnentspricht.

2. Klicken Sie auf **Weiter**.



Konfigurieren von Lizenzen

Wählen Sie einen der folgenden Modi aus, um die Lizenz auf eine ADC-Instanz anzuwenden:

- **Verwendung von Citrix ADM**: Die Instanz, die Sie bereitstellen möchten, checkt die Lizenzen vom Citrix ADM aus.
- **Verwenden von Microsoft Azure**: Die Option **Aus Cloud zuweisen** verwendet die Citrix Produktlizenzen, die im Azure Marketplace verfügbar sind. Die Instanz, die Sie bereitstellen möchten, verwendet die Lizenzen des Marketplace.

  Wenn Sie Lizenzen von Azure Marketplace verwenden, geben Sie das Produkt oder die Lizenz auf der Registerkarte **Bereitstellungsparameter** an.

Weitere Informationen finden Sie unter Lizenzanforderungen.

Lizenzen von Citrix ADM verwenden

Um diese Option zu verwenden, stellen Sie sicher, dass Sie das Citrix ADC Produkt mit dem Plan **Eigene Lizenzsoftware** in Azure abonniert haben. Siehe Abonnieren der Citrix ADC VPX -Lizenz in Microsoft Azure.

1. Wählen Sie auf der Registerkarte **Lizenz** die Option **Aus ADM zuweisen**.
2. Wählen Sie unter **Lizenztyp**eine der folgenden Optionen aus der Liste:
   - **Bandbreitenlizenzen:** Sie können eine der folgenden Optionen aus der Liste **Bandbreitenlizenztypen** auswählen:
     - **Pooled Capacity:** Geben Sie die Kapazität an, die einer Instanz zugewiesen werden soll.

       Aus dem gemeinsamen Pool checkt die ADC-Instanz eine Instanzlizenz aus und nur so viel Bandbreite wird angegeben.
     - **VPX-Lizenzen:** Wenn eine Citrix ADC VPX Instanz bereitgestellt wird, checkt die Instanz die Lizenz vom Citrix ADM aus.
   - **Virtuelle CPU-Lizenzen:** Die bereitgestellte Citrix ADC VPX-Instanz checkt Lizenzen abhängig von der Anzahl der in der Instanz ausgeführten CPUs aus.

   > **Hinweis:**
   >
   > Wenn die bereitgestellten Instanzen entfernt oder gelöscht werden, kehren die angewendeten Lizenzen in den Citrix ADM -Lizenzpool zurück. Diese Lizenzen können wiederverwendet werden, um neue Instanzen bereitzustellen.
3. Wählen Sie in **License Edition** die Lizenzversion aus. Der ADM verwendet die angegebene Edition zur Bereitstellung von Instanzen.
4. Klicken Sie auf **Weiter**.

Konfigurieren von Bereitstellungsparametern

1. Geben Sie auf der Registerkarte **Bereitstellungsparameter** Folgendes an:
   - **Ressourcengruppe** - Wählen Sie die **Ressourcengruppe** aus, in der Sie die Citrix ADC VPX-Instanz bereitstellen möchten.
   - **Produkt/ Lizenz** - Wählen Sie die gewünschte Option aus der Liste aus.

   a) Wählen Sie die unterstützte **VM-Größe** aus der Liste aus.

   > **Hinweis**
   >
   > Weitere Informationen zu unterstützten Produkten und VM-Größen finden Sie

> unterUnterstützte Citrix ADC Azure-Images für virtuelle Computer.

b) Wählen Sie das Cloud Access-Profil für ADC aus.

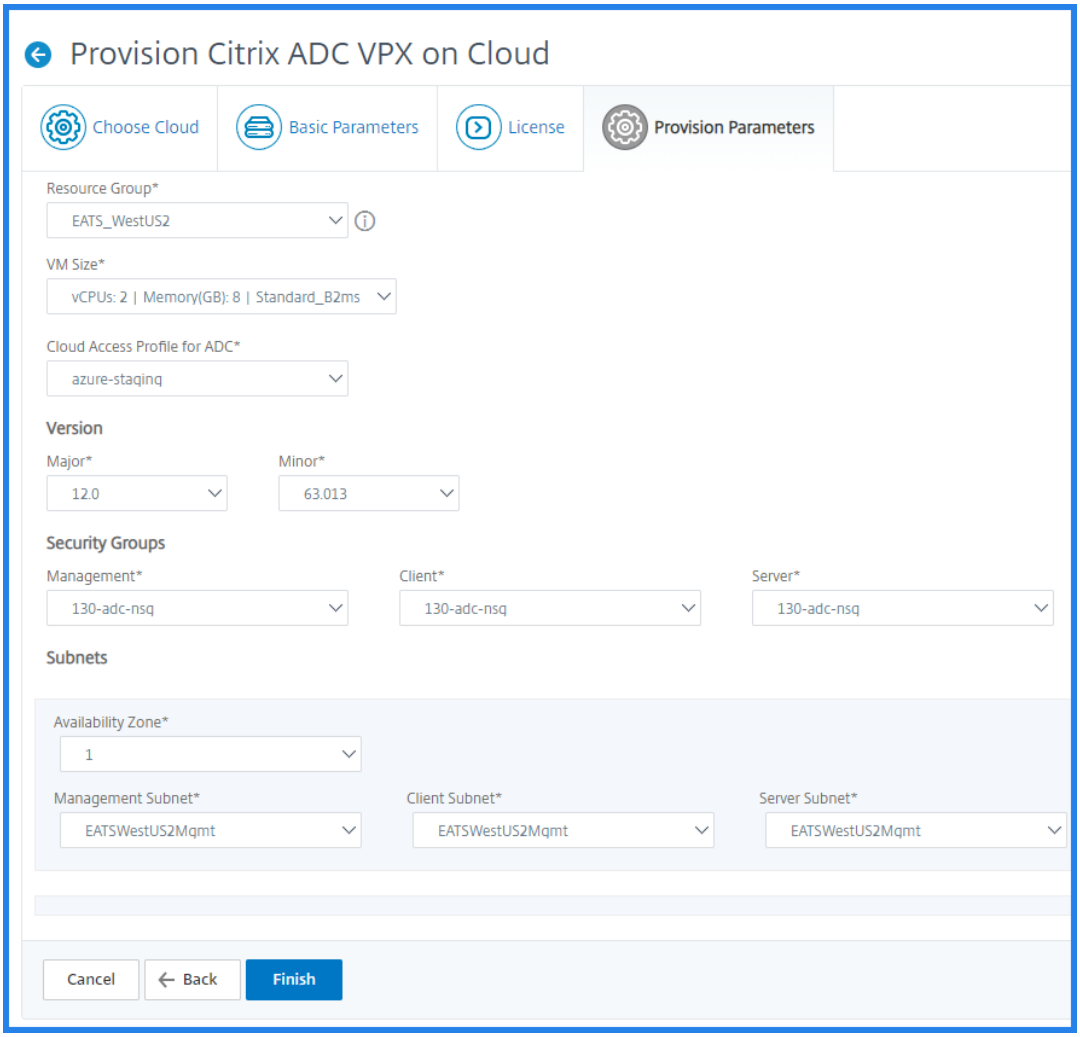
c) Wählen Sie die **Version** von Citrix ADC aus, die Sie bereitstellen möchten. Wählen Sie sowohl **Haupt-** als auch **Nebenversion** von Citrix ADC aus.

d) Wählen Sie unter **Sicherheitsgruppen** die Sicherheitsgruppen Management, Client und Server aus, die Sie in Ihrem virtuellen Netzwerk erstellt haben.

e) Geben Sie **unter Subnets**die erforderliche Anzahl von Availability Zones in Azure an.

f) Wählen Sie **unter Subnets**die Verwaltungs-, Client- und Server-Subnetze aus, die Sie in Ihrem virtuellen Netzwerk erstellt haben.

g) Klicken Sie auf **Fertig stellen**.



Die Citrix ADC VPX Instanz wird jetzt unter Microsoft Azure bereitgestellt.

Anzeigen der bereitgestellten Citrix ADC VPX Instanzen

So zeigen Sie Citrix ADM an:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Wählen Sie die Registerkarte **Citrix ADC VPX** aus.

   Die in Microsoft Azure bereitgestellte Citrix ADC VPX Instanz wird hier aufgelistet.

So zeigen Sie in Microsoft Azure an:

1. Melden Sie sich bei Ihrem Azure-Portal an.
2. Navigieren Sie zu der Ressourcengruppe, die zur Bereitstellung der Citrix ADC VPX-Instanz erstellt wurde.

   Auf dieser Seite wird die bereitgestellte Citrix ADC VPX Instanz angezeigt.

> **Hinweis**
>
> Der Name der Citrix ADC VPX-Instanz ist derselbe, den Sie beim Provisioning einer Instanz im Citrix ADM angegeben haben.

Automatische Skalierung von Citrix ADC VPX in Microsoft Azure mit Citrix ADM

April 28, 2021

Autoscaling ist eine Cloud-Computing-Methode, die automatisch Ressourcen in Abhängigkeit von der tatsächlichen Nutzung hinzufügt oder entfernt. Die automatische Skalierung ist nützlich, wenn Ihre Website oder Anwendung eine Ressourcenzuweisung auf Anforderung benötigt, um die schwankende Anzahl von Clientanforderungen oder Verarbeitungsaufträgen zu erfüllen.

Die Nachfrage nach Webanwendungen oder -diensten kann erheblich variieren. Die korrekte Anzahl von Citrix ADC-Instanzen für die unterschiedlichen Datenverkehrsanforderungen ist wichtig. Je nach Bedarf können Sie die Netzwerkressourcen in Microsoft Azure erhöhen oder verringern. So bietet es Kostenoptimierung, ohne die Leistung zu beeinträchtigen.

Bei der automatischen Skalierung von Citrix Application Delivery Management (ADM) wird die genaue Anzahl von Citrix ADC-Instanzen für den schwankenden Ressourcenverbrauch beibehalten. Citrix ADM bestimmt den Datenfluss basierend auf dem schwankenden Ressourcenverbrauch. Es entscheidet, in Citrix ADC-Instanzen dynamisch zu skalieren oder zu skalieren. Somit bietet es Ihnen die Flexibilität, die korrekte Anzahl von Citrix ADC-Instanzen beizubehalten.

Citrix ADM überwacht die Ressourcennutzung von Citrix ADC-Instanzen und stimmt mit dem konfigurierten Schwellenwert überein. Es löst die Scale-Out-Aktion aus, wenn eine der konfigurierten Ressourcen den angegebenen Schwellenwert überschreitet.

Citrix ADM löst die Aktion Skalieren nur aus, wenn die Verwendung aller konfigurierten Ressourcen unter den normalen Schwellenwert fällt.

> **Wichtig**
>
> Autoscaling unterstützt alle Citrix ADC Funktionen mit Ausnahme der folgenden Funktionen, die eine gepunktete Konfiguration auf Clusterknoten erfordern:
>
> - GSLB
> - Citrix Gateway und seine Funktionen
> - Telco-Funktionen
>
> Weitere Informationen zur Spotted-Konfiguration finden Sie unter Striped-, Teil-Striped- und Spotted-Konfigurationen.

Vorteile

Hohe Verfügbarkeit von Anwendungen: Autoscaling stellt sicher, dass Ihre Anwendung immer über die richtige Anzahl von Citrix ADC VPX Instanzen verfügt, um die Datenverkehrsanforderungen zu bewältigen. Es stellt sicher, dass Ihre Anwendung ständig einsatzbereit ist und ausgeführt wird, unabhängig von den Anforderungen des Datenverkehrs.

Intelligente Skalierungsentscheidungen und Zero-Touch-Konfiguration: Autoscaling überwacht Ihre Anwendung kontinuierlich und fügt Citrix ADC-Instanzen dynamisch je nach Bedarf hinzu oder entfernt sie. Die Instanzen werden automatisch hinzugefügt, wenn der Bedarf für einen bestimmten Zeitraum erhöht wird. Die Instanzen werden automatisch entfernt, wenn der Bedarf für einen bestimmten Zeitraum verringert wird. Das Hinzufügen und Entfernen von Citrix ADC-Instanzen erfolgt automatisch und macht es zu einer manuellen Null-Touch-Konfiguration.

Automatische DNS-Verwaltung: Die Citrix ADM Autoscale-Funktion bietet eine automatische DNS-Verwaltung. Wenn neue Citrix ADC-Instanzen hinzugefügt werden, werden die Domänennamen automatisch aktualisiert.

Ordnungsgemäße Verbindungsbeendigung: Während eines Scale-Ins werden die Citrix ADC-Instanzen ordnungsgemäß entfernt, wodurch der Verlust von Clientverbindungen vermieden wird.

Besseres Kostenmanagement: Die automatische Skalierung erhöht oder verringert Citrix ADC-Instanzen bei Bedarf dynamisch. Mit dieser Methode können Sie die damit verbundenen Kosten optimieren. Wenn Sie Instanzen nur dann starten, wenn sie benötigt werden, und sie beenden, wenn sie nicht benötigt werden, reduziert sich die Betriebskosten. So zahlen Sie nur für die Ressourcen, die Sie verwenden.

Beobachtbarkeit: Beobachtbarkeit ist der Schlüssel für Anwendungsdev-ops oder IT-Personal, um den Zustand der Anwendung zu überwachen. Das Dashboard “Autoscale” von Citrix ADM ermöglicht Ihnen die Visualisierung der Schwellwert-Parameterwerte, der Autoscale Trigger-Zeitstempel, der Ereignisse und der Instanzen, die an der Autoscale beteiligt sind.

Lizenzierungsanforderungen

Die Citrix ADC-Instanzen, die für die Citrix Autoscale-Gruppe erstellt werden, verwenden Citrix ADC Advanced- oder Premium ADC-Lizenzen. Citrix ADC Clustering-Funktion ist in Advanced- oder Premium ADC-Lizenzen enthalten.

> **Hinweis:**
>
> ADC-Cluster werden nur in der automatischen ADM-Skalierung mit ADC Premium- oder Advanced-Lizenzen unterstützt.

Sie können eine der folgenden Methoden wählen, um Citrix ADCs zu lizenzieren, die von Citrix ADM bereitgestellt werden:

- **Verwenden von ADC-Lizenzen in Citrix ADM:** Konfigurieren Sie gepoolte Kapazität, VPX-Lizenzen oder virtuelle CPU-Lizenzen beim Erstellen der Autoscale-Gruppe. Wenn also eine neue Instanz für die Autoscale-Gruppe bereitgestellt wird, wird der bereits konfigurierte Lizenztyp automatisch auf die bereitgestellte Instanz angewendet.
  - **Pooled Capacity**: Stellt jeder bereitgestellten Instanz in der Autoscale-Gruppe Bandbreite zu. Stellen Sie sicher, dass in Citrix ADM die erforderliche Bandbreite zur Verfügung steht, um neue Instanzen bereitzustellen. Weitere Informationen finden Sie unter Konfiguration der gepoolten Kapazität.

    Jede ADC-Instanz in der Gruppe Autoscale checkt eine Instanzlizenz und die angegebene Bandbreite aus dem Pool aus.
  - **VPX-Lizenzen:** Wendet die VPX-Lizenzen auf neu bereitgestellte Instanzen an. Stellen Sie sicher, dass Sie über die erforderliche Anzahl von VPX-Lizenzen in Citrix ADM verfügen, um neue Instanzen bereitzustellen.

    Wenn eine Citrix ADC VPX Instanz bereitgestellt wird, checkt die Instanz die Lizenz vom Citrix ADM aus. Weitere Informationen finden Sie unter Citrix ADC VPX Ein- und Auschecken Lizenzierung.
  - **Virtuelle CPU-Lizenzen:** Wendet virtuelle CPU-Lizenzen auf neu bereitgestellte Instanzen an. Diese Lizenz gibt die Anzahl der CPUs an, die für eine Citrix ADC VPX Instanz berechtigt sind. Stellen Sie sicher, dass Sie über die erforderliche Anzahl von virtuellen CPUs in Citrix ADM verfügen, um neue Instanzen bereitzustellen.

Wenn eine Citrix ADC VPX Instanz bereitgestellt wird, checkt die Instanz die virtuelle CPU-Lizenz vom Citrix ADM aus. Weitere Informationen finden Sie unter Citrix ADC virtuelle CPU-Lizenzierung.

Wenn die bereitgestellten Instanzen zerstört oder die Bereitstellung aufgehoben werden, werden die angewendeten Lizenzen automatisch an Citrix ADM zurückgegeben.

Um die verbrauchten Lizenzen zu überwachen, navigieren Sie zur Seite **Netzwerke** > **Lizenzen**.

- **Verwenden von Microsoft Azure-Abonnementlizenzen:** Konfigurieren Sie Citrix ADC Lizenzen, die im Azure Marketplace verfügbar sind, während Sie die Autoscale-Gruppe erstellen. Wenn also eine neue Instanz für die Autoscale-Gruppe bereitgestellt wird, wird die Lizenz vom Azure Marketplace bezogen.

Unterstützte Citrix ADC Azure-Images für virtuelle Maschinen für die automatische Skalierung

Verwenden Sie das Azure-Image für virtuelle Computer, das mindestens drei Netzwerkkarten unterstützt. Die automatische Skalierung der Citrix ADC VPX Instanz wird nur auf der Premium und Advanced Edition unterstützt. Weitere Informationen zu Azure-Imagetypen für virtuelle Computer finden Sie unter VM-Typen und -größen in der Microsoft-Dokumentation.

Im Folgenden sind die empfohlenen VM-Größen für die automatische Skalierung aufgeführt:

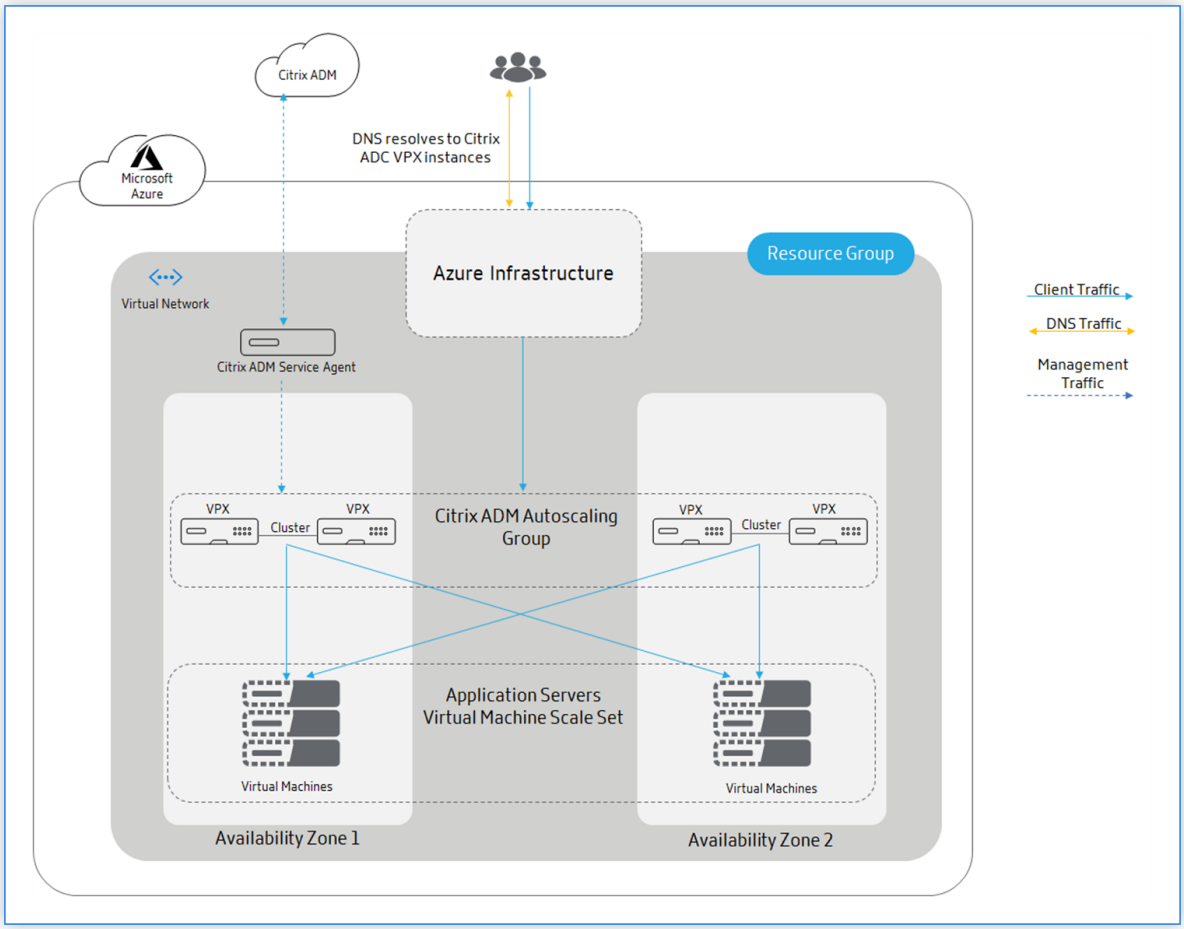
- Standard_DS3_v2
- Standard_B2ms
- Standard_DS4_v2

Architektur

Citrix ADM verarbeitet die Verteilung des Clientdatenverkehrs mithilfe von Azure DNS oder Azure Load Balancer (ALB).

Verkehrsverteilung mit Azure DNS

Das folgende Diagramm veranschaulicht, wie die DNS-basierte automatische Skalierung mit dem Azure-Verkehrs-Manager als Verkehrsverteiler erfolgt:



Bei der DNS-basierten Autoskalierung fungiert DNS als Verteilungsebene. Der Azure Traffic Manager ist der DNS-basierte Load Balancer in Microsoft Azure. Traffic Manager leitet den Clientdatenverkehr an die entsprechende Citrix ADC-Instanz weiter, die in der Autoskalierungsgruppe Citrix ADM verfügbar ist.

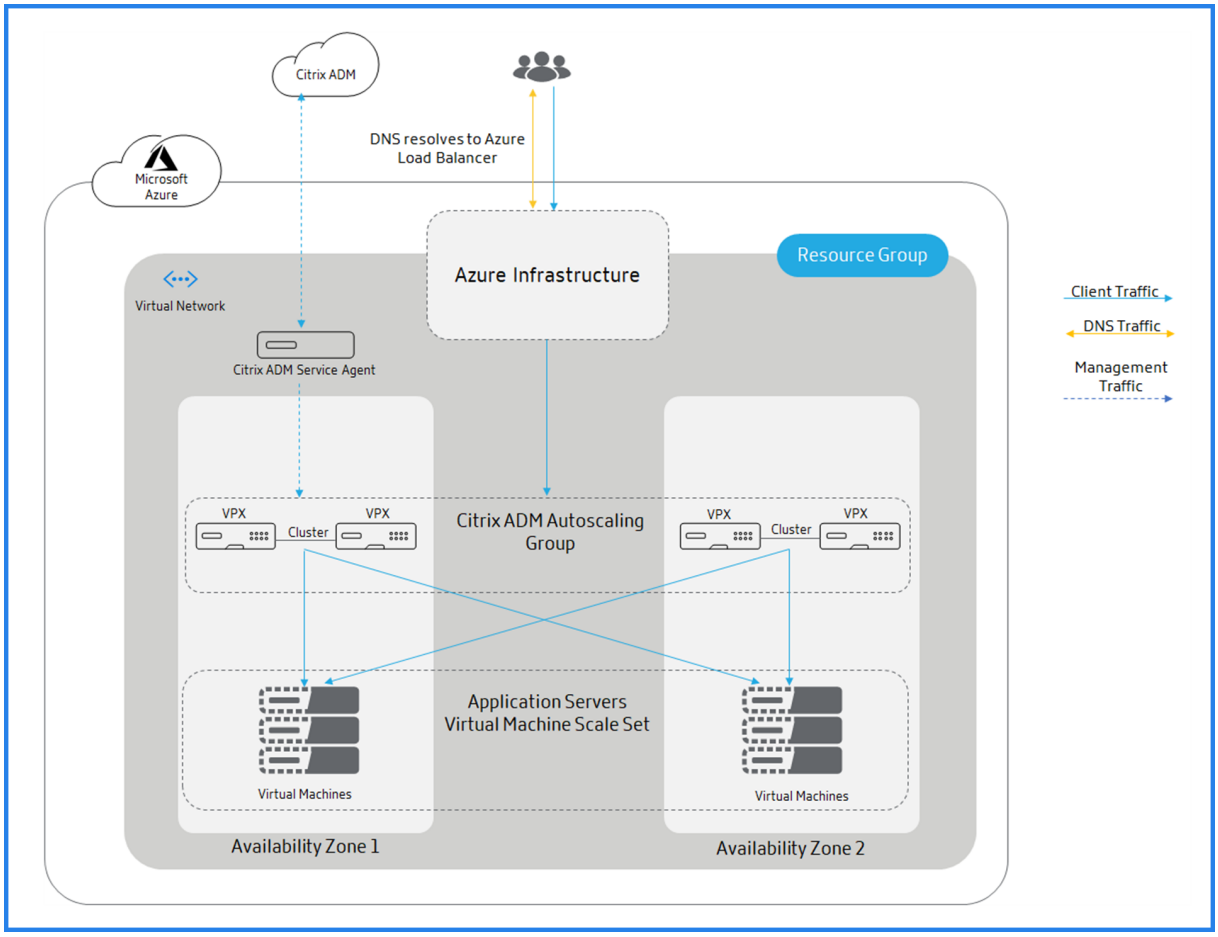
Azure Traffic Manager löst den FQDN in die VIP-Adresse der Citrix ADC-Instanz auf.

> **Hinweis**
>
> Bei der DNS-basierten automatischen Skalierung erfordert jede Citrix ADC-Instanz in der Citrix ADM Autoscale-Gruppe eine öffentliche IP-Adresse.

Citrix ADM löst die Scale-Out- oder Scale-In-Aktion auf Clusterebene aus. Wenn ein Scale-Out ausgelöst wird, werden die registrierten virtuellen Maschinen bereitgestellt und dem Cluster hinzugefügt. Wenn ein Scale-In ausgelöst wird, werden die Knoten entfernt und aus den Citrix ADC VPX Clustern entfernt.

Verkehrsverteilung mit Azure Load Balancer

Das folgende Diagramm veranschaulicht, wie die automatische Skalierung mit dem Azure Load Balancer als Traffic Distributor erfolgt:



Azure Load Balancer ist die Verteilungsebene für die Clusterknoten. ALB verwaltet den Clientdatenverkehr und verteilt ihn an Citrix ADC VPX Cluster. ALB sendet den Clientdatenverkehr an Citrix ADC VPX Clusterknoten, die in der Autoskalierungsgruppe Citrix ADM über Availability Zones verfügbar sind.

> **Hinweis:**
>
> Öffentliche IP-Adresse wird Azure Load Balancer zugewiesen. Citrix ADC VPX Instanzen benötigen keine öffentliche IP-Adresse.

Citrix ADM löst die Scale-Out- oder Scale-In-Aktion auf Clusterebene aus. Wenn ein Scale-Out ausgelöst wird, werden die registrierten virtuellen Maschinen bereitgestellt und dem Cluster hinzugefügt. Wenn ein Scale-In ausgelöst wird, werden die Knoten entfernt und aus den Citrix ADC VPX Clustern entfernt.

Citrix ADM Gruppe für automatische Skalierung

Autoscale-Gruppe ist eine Gruppe von Citrix ADC-Instanzen, die Anwendungen als einzelne Entität Lastausgleich auslösen und basierend auf den konfigurierten Schwellenwertparameterwerten die automatische Skalierung auslösen.

Ressourcengruppe

Ressourcengruppe enthält die Ressourcen, die mit der automatischen Citrix ADC Skalierung zusammenhängen. Diese Ressourcengruppe hilft Ihnen beim Verwalten der Ressourcen, die für die automatische Skalierung erforderlich sind. Weitere Informationen finden Sie unter Verwalten von Ressourcengruppen.

Azure-Back-End-VM-Skalierungssatz

Die Azure-VM-Skalierung ist eine Sammlung identischer VM-Instanzen. Je nach Clientdatenverkehr kann die Anzahl der VM-Instanzen erhöht oder verringert werden. Dieses Set bietet Hochverfügbarkeit für Ihre Anwendungen. Weitere Informationen finden Sie unter Skalierungssätze für virtuelle Maschinen.

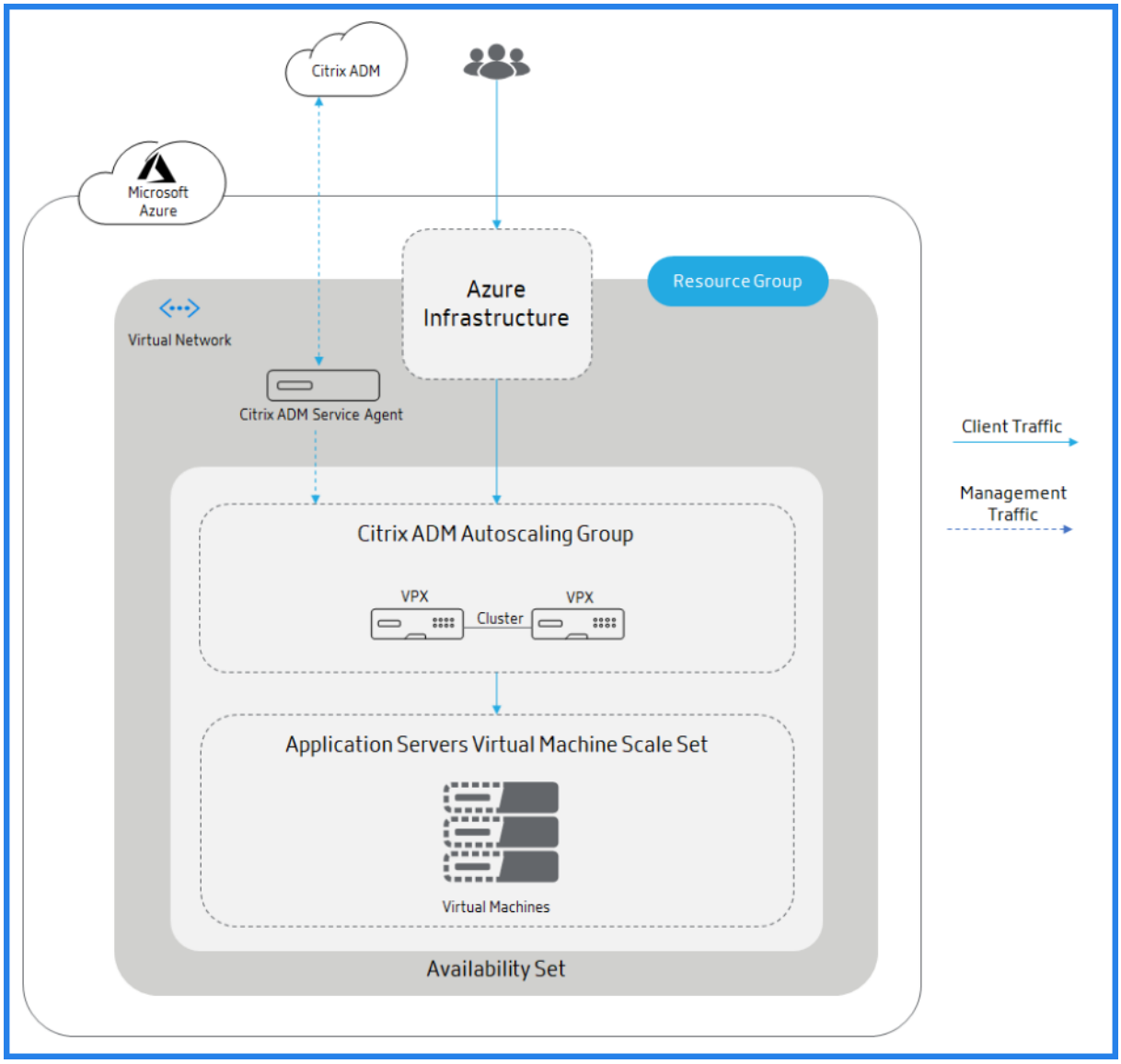
Verfügbarkeitszonen

Availability Zones sind isolierte Standorte in einer Azure-Region. Jede Region besteht aus mehreren Availability Zones. Jede Verfügbarkeitszone gehört zu einer einzelnen Region. Jede Availability Zone verfügt über einen Citrix ADC VPX Cluster. Weitere Informationen finden Sie unter Verfügbarkeitszonen in Azure.

Verfügbarkeitssets

Ein Verfügbarkeitssatz ist eine logische Gruppierung eines Citrix ADC VPX Clusters und Anwendungsservers. Availability Sets sind hilfreich, um ADC-Instanzen über mehrere isolierte Hardwareknoten in einem Cluster bereitzustellen. Mit einem Verfügbarkeitssatz können Sie eine zuverlässige automatische ADM-Skalierung sicherstellen, wenn Hardware- oder Softwarefehler in Azure vorliegen. Weitere Informationen finden Sie unter Verfügbarkeitssets.

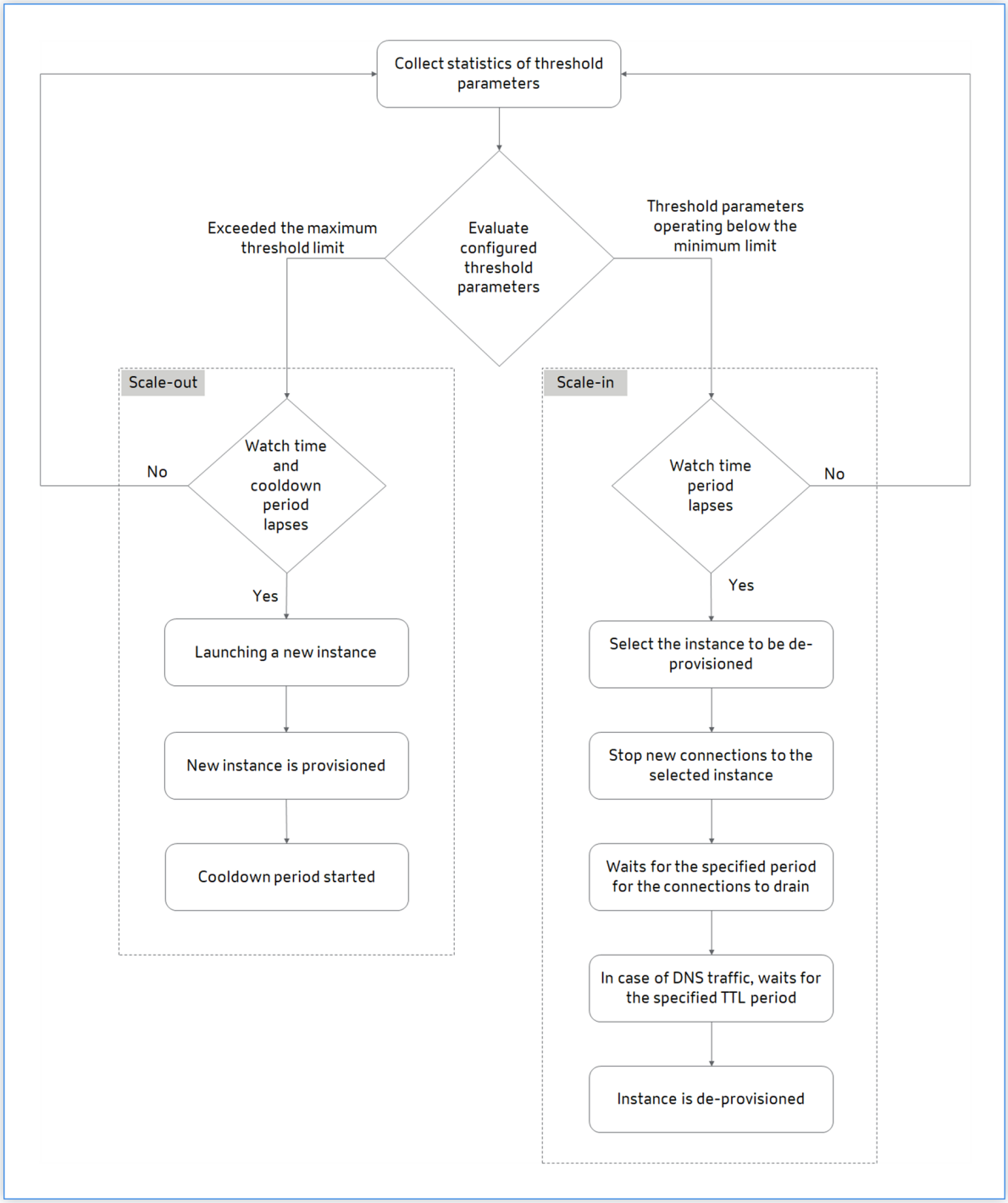
Das folgende Diagramm veranschaulicht die automatische Skalierung in einem Verfügbarkeitssatz:



Die Azure-Infrastruktur (ALB oder Azure Traffic Manager) sendet den Clientverkehr an eine automatische Citrix ADM Gruppe in der Verfügbarkeitsgruppe. Citrix ADM löst die Scale-Out- oder Scale-In-Aktion auf Clusterebene aus.

So funktioniert die automatische Skalierung

Das folgende Flussdiagramm veranschaulicht den automatischen Skalierungsworkflow:



Citrix ADM sammelt die Statistiken (CPU, Arbeitsspeicher und Durchsatz) aus den bereitgestellten Clustern für jede Minute.

Die Statistiken werden anhand der Konfigurationsschwellenwerte ausgewertet. Abhängig von der Statistik wird die Skalierung oder die Skalierung in ausgelöst. Scale-out wird ausgelöst, wenn die Statistik den maximalen Schwellenwert überschreitet. Scale-In wird ausgelöst, wenn die Statistiken

unter dem Mindestschwellenwert arbeiten.

Wenn ein Scale-Out ausgelöst wird:

1. Neuer Knoten wird bereitgestellt.
2. Der Knoten ist mit dem Cluster verbunden und die Konfiguration wird vom Cluster mit dem neuen Knoten synchronisiert.
3. Der Knoten ist bei Citrix ADM registriert.
4. Die neuen Knoten IP-Adressen werden im Azure-Verkehrs-Manager aktualisiert.

Wenn ein Scale-In ausgelöst wird:

1. Der Knoten wird identifiziert, der entfernt werden soll.
2. Stoppen Sie neue Verbindungen zum ausgewählten Knoten.
3. Wartet auf den angegebenen Zeitraum, bis die Verbindungen abgeleitet werden. Im DNS-Datenverkehr wartet er auch auf den angegebenen Zeitraum (Time To-Live, TTL).
4. Der Knoten wird vom Cluster getrennt, von Citrix ADM abgemeldet und dann von Microsoft Azure entfernt.

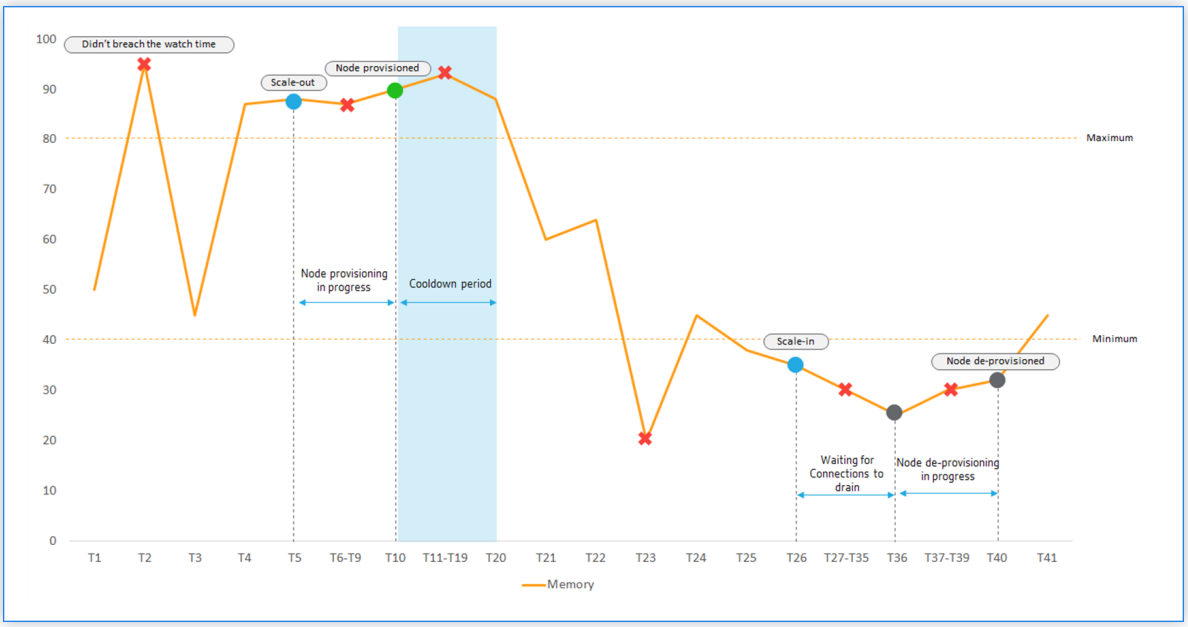
> **Hinweis**
>
> Wenn die Anwendung bereitgestellt wird, wird ein IP-Satz auf Clustern in jeder Availability Zone erstellt. Anschließend werden die Domänen- und Instanz-IP-Adressen beim Azure-Verkehrs-Manager oder ALB registriert. Wenn die Anwendung entfernt wird, werden die Domänen- und Instanz-IP-Adressen vom Azure-Verkehrs-Manager oder ALB abgemeldet. Dann wird der IP-Satz gelöscht.

Beispiel für die automatische Skalierung

Beachten Sie, dass Sie eine Autoscale-Gruppe mit dem Namen asg_arn in einer einzelnen Availability Zone mit der folgenden Konfiguration erstellt haben.

- Ausgewählte Schwellenwertparameter — Speicherbelegung.
- Schwellenwert auf Speicher festgelegt:
  - Mindestgrenze: 40
  - Höchstgrenze: 85
- Wiedergabezeit: 2 Minuten.
- Abklingzeit — 10 Minuten.
- Wartezeit während der De-Bereitstellung — 10 Minuten.
- DNS-Zeit bis zum Leben — 10 Sekunden.

Nachdem die Gruppe “Autoscale” erstellt wurde, werden Statistiken aus der Gruppe “Autoscale” gesammelt. Die Richtlinie “Automatische Skalierung” wertet auch aus, ob ein Ereignis für die automatische Skalierung ausgeführt wird. Wenn die automatische Skalierung ausgeführt wird, warten Sie, bis dieses Ereignis abgeschlossen ist, bevor Sie die Statistiken sammeln.



Die Reihenfolge der Ereignisse

1. Die Speichernutzung überschreitet den Schwellenwert bei **T2**. Das Scale-Out wird jedoch nicht ausgelöst, da es für die angegebene Wiedergabezeit nicht verletzt wurde.
2. Scale-Out wird bei **T5** ausgelöst, nachdem ein Maximalschwellenwert für 2 Minuten (Wiedergabezeit) kontinuierlich überschritten wurde.
3. Für den Verstoß zwischen **T5-T10** wurden keine Maßnahmen ergriffen, da Knotenprovisioning ausgeführt wird.
4. Der Knoten wird bei **T10** bereitgestellt und dem Cluster hinzugefügt. Die Abklingzeit wurde gestartet.
5. Wegen der Abklingzeit wurden keine Maßnahmen für die Verletzung zwischen **T10-T20** ergriffen. Dieser Zeitraum sorgt für den organischen Anbau von Instanzen einer Autoscale-Gruppe. Bevor die nächste Skalierungsentscheidung ausgelöst wird, wird darauf gewartet, dass sich der aktuelle Datenverkehr stabilisiert und auf den aktuellen Satz von Instanzen durchdurchschnittlich wird.
6. Die Speichernutzung unterschreitet den Mindestschwellenwert bei **T23**. Das Scale-In wird jedoch nicht ausgelöst, da es für die angegebene Wiedergabezeit nicht verletzt wurde.

7. Scale-In wird bei **T26** ausgelöst, nachdem der Mindestschwellenwert für 2 Minuten (Wiedergabezeit) kontinuierlich überschritten wurde. Ein Knoten im Cluster wird für die Aufhebung der Bereitstellung identifiziert.
8. Für den Verstoß zwischen **T26-T36** wurden keine Maßnahmen ergriffen, da Citrix ADM darauf wartet, vorhandene Verbindungen zu entleeren. Bei der DNS-basierten Autoskalierung ist TTL wirksam.

   > **Hinweis:**
   >
   > Bei DNS-basierter Autoskalierung wartet Citrix ADM auf den angegebenen Time-To-Live (TTL) -Zeitraum. Anschließend wartet es, bis vorhandene Verbindungen abgeleitet werden, bevor die Node-Bereitstellung initiiert wird.

9. Für den Verstoß zwischen **T37-T39** wurden keine Maßnahmen ergriffen, da die Node-Bereitstellung ausgeführt wird.
10. Der Knoten wird entfernt und bei **T40** aus dem Cluster entfernt.

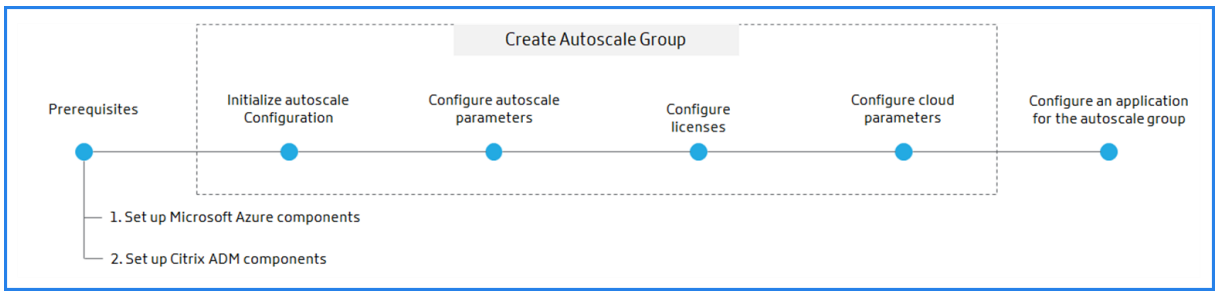
Alle Verbindungen zum ausgewählten Knoten wurden entleert, bevor die Node-Bereitstellung initiiert wurde. Daher wird die Abklingzeit übersprungen, nachdem das Provisioning des Knotens aufgehoben wurde.

Konfiguration

April 28, 2021

Citrix ADM verwaltet alle Citrix ADC VPX Cluster in Microsoft Azure. Citrix ADM greift mithilfe des Cloud Access-Profils auf die Azure-Ressourcen zu.

Das folgende Flussdiagramm erklärt die Schritte beim Erstellen und Konfigurieren einer Autoscale-Gruppe:



Voraussetzungen

In diesem Abschnitt werden die Voraussetzungen beschrieben, die Sie in Microsoft Azure und Citrix ADM erfüllen müssen, bevor Sie die automatische Skalierung von Citrix ADC VPX-Instanzen konfiguri-

eren.

Dieses Dokument setzt Folgendes voraus:

- Sie verfügen über ein Microsoft Azure-Konto, das das Azure Resource Manager Bereitstellungsmodell unterstützt.
- Sie haben eine Ressourcengruppe in Microsoft Azure.

Weitere Informationen zum Erstellen eines Kontos und anderer Aufgaben finden Sie unter Microsoft Azure-Dokumentation.

Einrichten von Microsoft Azure-Komponenten

Führen Sie die folgenden Aufgaben in Azure aus, bevor Sie Citrix ADC VPX Instanzen in Citrix ADM automatisch skalieren.

1. Erstellen eines virtuellen Netzwerks.
2. Erstellen von Sicherheitsgruppen.
3. Subnetze erstellen.
4. Abonnieren der Citrix ADC VPX -Lizenz in Microsoft Azure.
5. Erstellen und Registrieren einer Anwendung.

Erstellen eines virtuellen Netzwerks

1. Melden Sie sich bei Ihrem Microsoft Azure-Portal an.
2. Wählen Sie **Ressource erstellen** aus.
3. Wählen Sie **Netzwerk** aus, und klicken Sie auf **Virtuelles Netzwerk**.
4. Geben Sie die erforderlichen Parameter an.
    - In der **Ressourcengruppe**müssen Sie die Ressourcengruppe angeben, in der Sie ein Citrix ADC VPX Produkt bereitstellen möchten.
    - In **Standort**müssen Sie die Standorte angeben, die Availability Zones unterstützen, z. B.:
        - USA, Mitte
        - Ost US2
        - Frankreich, Mitte
        - Europa, Norden
        - Südostasien
        - Westeuropa

- West US2

> **Hinweis**
>
> Die Anwendungsserver sind in dieser Ressourcengruppe vorhanden.

5. Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Azure Virtual Network in Microsoft-Dokumentation.

Erstellen von Sicherheitsgruppen

Erstellen Sie drei Sicherheitsgruppen in Ihrem virtuellen Netzwerk (VNet) - jeweils eine für die Verwaltungs-, Client- und Serververbindungen. Erstellen Sie eine Sicherheitsgruppe zur Steuerung des eingehenden und ausgehenden Datenverkehrs in der Citrix ADC VPX Instanz. Erstellen Sie Regeln für den eingehenden Datenverkehr, den Sie in den Citrix Autoscale-Gruppen steuern möchten. Sie können beliebig viele Regeln hinzufügen.

- **Management:** Eine Sicherheitsgruppe in Ihrem Konto, die für die Verwaltung von Citrix ADC VPX vorgesehen ist. Citrix ADC muss sich an Azure-Dienste wenden und erfordert Internetzugang. Eingehende Regeln sind für die folgenden TCP- und UDP-Ports zulässig.
  - TCP: 80, 22, 443, 3008—3011, 4001, 27000, 7279
  - UDP: 67, 123, 161, 500, 3003, 4500, 7000

  > **Hinweis Stellen Sie**
  >
  > Folgendes sicher:
  >
  > Die Sicherheitsgruppe hat dem Citrix ADM Agent den Zugriff auf den VPX ermöglicht.
  >
  > Die Ports 27000 und 7279 werden in Citrix ADM geöffnet. Diese Ports werden verwendet, um Citrix ADC-Lizenzen von Citrix ADM auszuprobieren. Weitere Informationen finden Sie unter Ports.

- **Client:** Eine Sicherheitsgruppe in Ihrem Konto, die für eine clientseitige Kommunikation von Citrix ADC VPX Instanzen bestimmt ist. In der Regel sind eingehende Regeln an den TCP-Ports 80 und 443 zulässig. Und der 60000-Port ist erforderlich, um den Zustand von ADC-Instanzen zu überwachen.
- **Server:** Eine Sicherheitsgruppe in Ihrem Konto, die für eine serverseitige Kommunikation von Citrix ADC VPX bestimmt ist.

Weitere Informationen zum Erstellen einer Sicherheitsgruppe in Microsoft Azure finden Sie unter Erstellen, Ändern oder Löschen einer Netzwerksicherheitsgruppe.

Subnetze erstellen

Erstellen Sie drei Subnetze in Ihrem virtuellen Netzwerk (VNet) - jeweils eines für die Management-, Client- und Serververbindungen. Geben Sie einen Adressbereich an, der in Ihrem VNet für jedes Subnetz definiert ist. Geben Sie die Verfügbarkeitszone an, in der sich das Subnetz befinden soll.

- **Verwaltung:** Ein Subnetz in Ihrem virtuellen Netzwerk (VNet), das für die Verwaltung bestimmt ist. Citrix ADC muss sich an Azure-Dienste wenden und erfordert Internetzugang.
- **Client:** Ein Subnetz in Ihrem virtuellen Netzwerk (VNet), das für die Client-Seite dediziert ist. In der Regel empfängt Citrix ADC Clientdatenverkehr für die Anwendung über ein öffentliches Subnetz aus dem Internet.
- **Server:** Ein Subnetz, in dem die Anwendungsserver bereitgestellt werden. Alle Ihre Anwendungsserver sind in diesem Subnetz vorhanden und empfangen Anwendungsdatenverkehr vom Citrix ADC über dieses Subnetz.

> **Hinweis**
>
> Geben Sie beim Erstellen eines Subnetzes eine geeignete Sicherheitsgruppe für das Subnetz an.

Weitere Informationen zum Erstellen eines Subnetzes in Microsoft Azure finden Sie unter Hinzufügen, Ändern oder Löschen eines virtuellen Netzwerksubnetzes.

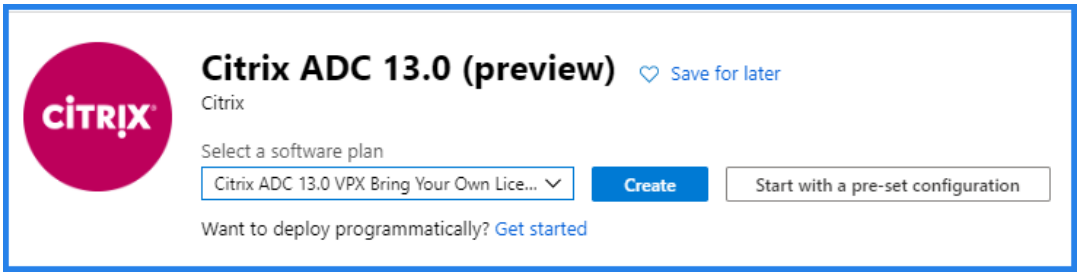
Abonnieren der Citrix ADC VPX -Lizenz in Microsoft Azure

1. Melden Sie sich bei Ihrem Microsoft Azure-Portal an.
2. Wählen Sie **Ressource erstellen** aus.
3. **Suchen Sie in der Leiste Marketplace** durchsuchen die gewünschte Produktversion`Citrix ADC` und wählen Sie sie aus.
4. **Wählen Sie in der Liste Softwareplan** auswählen einen der folgenden Lizenztypen aus:
   - Eigene Lizenz
   - Erweitert
   - Premium

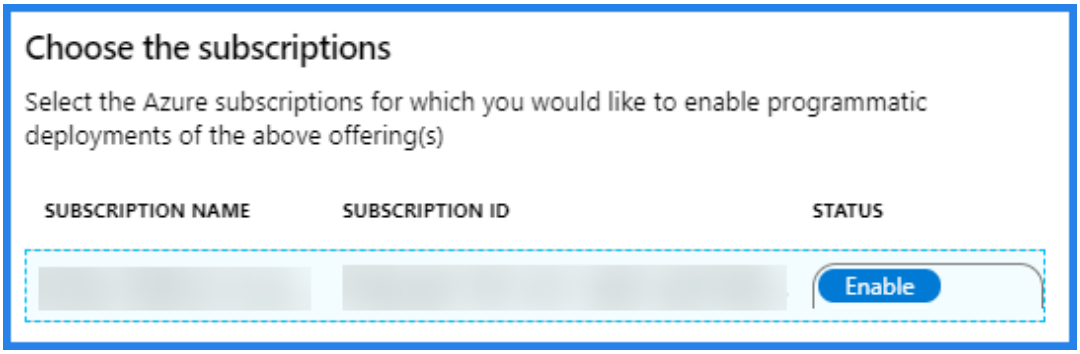
   > **Hinweis**
   >
   > - Wenn Sie die Option **Eigene Lizenz mitbringen** wählen, checkt die Autoscale-Gruppe die Lizenzen vom Citrix ADM aus, während Sie Citrix ADC-Instanzen Provisioning.
   > - In Citrix ADM sind **Advanced** und **Premium** die entsprechenden Lizenztypen für **Enterprise** bzw. **Platinum**.

5. Stellen Sie sicher, dass die programmatische Bereitstellung für das ausgewählte Citrix ADC Produkt aktiviert ist.

   a) Klicken Sie neben **Möchten Sie programmgesteuert bereitstellen?** auf **Erste Schritte**.



b) Wählen Sie unter **Abonnements auswählen** die Option **Aktivieren** aus, um die ausgewählte Citrix ADC VPX Edition programmgesteuert bereitzustellen.



> **Wichtig**
>
> Das Aktivieren der programmgesteuerten Bereitstellung ist für die automatische Skalierung von Citrix ADC VPX Instanzen in Azure erforderlich.

c) Klicken Sie auf **Save**.

d) Schließen Sie **Programmatische Bereitstellung konfigurieren**.

6. Klicken Sie auf **Erstellen**.

Erstellen und Registrieren einer Anwendung

Citrix ADM verwendet diese Anwendung, um Citrix ADC VPX Instanzen in Azure automatisch zu skalieren.

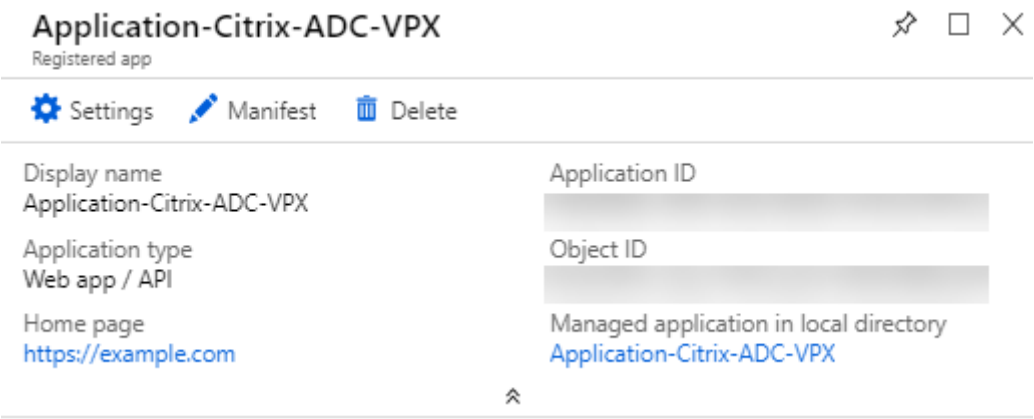
So erstellen und registrieren Sie eine Anwendung in Azure:

1. Wählen Sie im Azure-Portal **Azure Active Directory**aus.
   Diese Option zeigt das Verzeichnis Ihrer Organisation an.
2. Wählen Sie **App-Registrierungen** aus:
   a) Geben Sie unter **Name** den Namen der Anwendung an.
   b) Wählen Sie in der Liste den **Anwendungstyp** aus.
   c) Geben Sie in der **Anmelde-URL die Anwendungs-URL** für den Zugriff auf die Anwendung an.

3. Klicken Sie auf **Erstellen**.

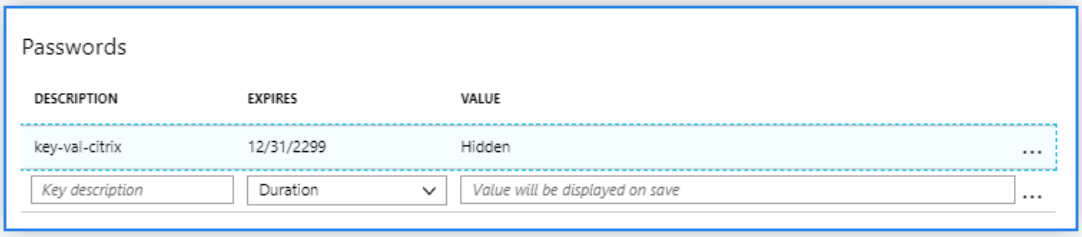
Weitere Informationen zu App-Registrierungen finden Sie unter Microsoft-Dokumentation.

Azure weist der Anwendung eine Anwendungs-ID zu. Im Folgenden finden Sie eine Beispielanwendung, die in Microsoft Azure registriert ist:



Kopieren Sie die folgenden IDs und geben Sie diese IDs an, wenn Sie das Cloud Access-Profil in Citrix ADM konfigurieren. Schritte zum Abrufen der folgenden IDs finden Sie unter Microsoft-Dokumentation:

- Anwendungs-ID
- Verzeichnis-ID
- Key



- Abonnement-ID: Kopieren Sie die Abonnement-ID aus Ihrem Speicherkonto.

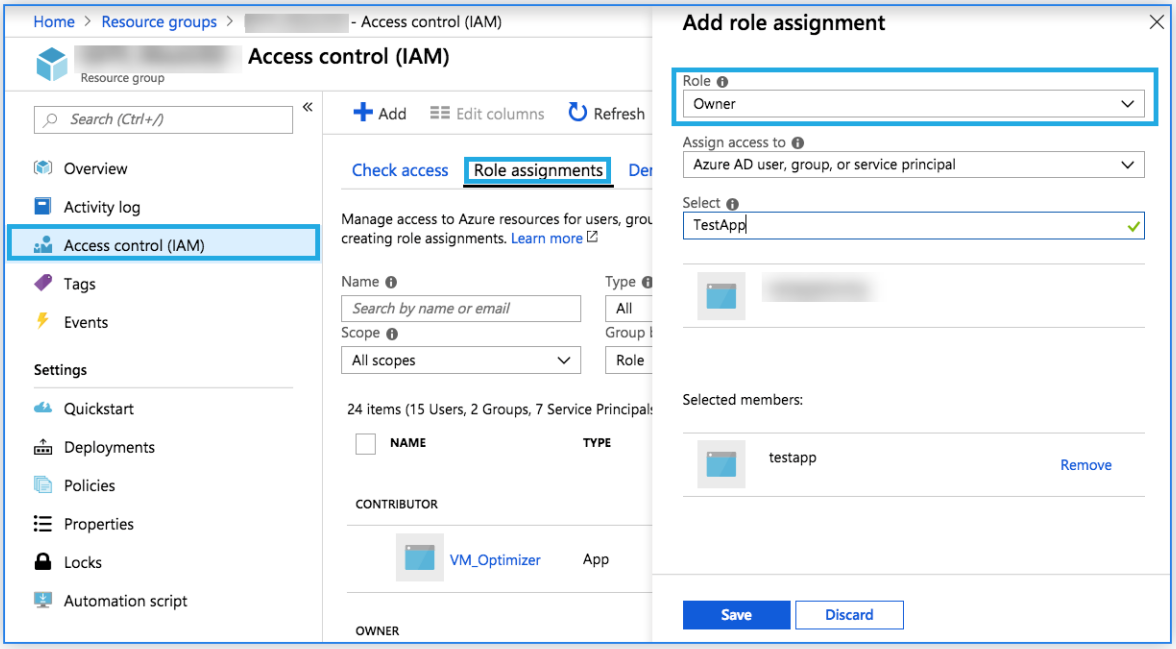
Zuweisen der Rollenberechtigung zu einer Anwendung

Citrix ADM verwendet das Application-as-a-Service-Prinzip, um Citrix ADC-Instanzen in Microsoft Azure automatisch zu skalieren. Diese Berechtigung gilt nur für die ausgewählte Ressourcengruppe.

Um Ihrer registrierten Anwendung eine Rollenberechtigung zuzuweisen, müssen Sie Eigentümer des Microsoft Azure-Abonnements sein.

1. Wählen Sie im Azure-Portal **Ressourcengruppen**aus.

2. Wählen Sie die Ressourcengruppe aus, der Sie eine Rollenberechtigung zuweisen möchten.
3. Wählen Sie **Zugriffssteuerung (IAM)** aus.
4. Klicken Sie unter **Rollenzuweisungen** auf **Hinzufügen**.
5. Wählen Sie **Besitzer** aus der Liste **Rolle** aus.
6. Wählen Sie die Anwendung aus, die für die automatische Skalierung von Citrix ADC-Instanzen registriert ist.
7. Klicken Sie auf **Save**.



Einrichten von Citrix ADM Komponenten

Führen Sie die folgenden Aufgaben in Azure aus, bevor Sie Citrix ADC VPX Instanzen in Citrix ADM automatisch skalieren:

1. Bereitstellen eines Agenten in Azure
2. Erstellen einer Website
3. Anfügen der Site an einen Citrix ADM Dienstagenten

Bereitstellen von Citrix ADM -Agent in Azure

Der Citrix ADM-Dienst-Agent arbeitet als Vermittler zwischen Citrix ADM und den erkannten Instanzen im Rechenzentrum oder in der Cloud.

1. Navigieren Sie zu **Netzwerke > Agents**.

2. Klicken Sie auf **Bereitstellen**.
3. Wählen Sie **Microsoft Azure** aus, und klicken Sie auf **Weiter**.
4. Geben Sie auf der Registerkarte **Bereitstellungsparameter** Folgendes an:
    - **Name**: Geben Sie den Namen des Citrix ADM Agenten an.
    - **Site** - Wählen Sie die Site aus, die Sie für die Bereitstellung eines Agenten und ADC-VPX-Instanzen erstellt haben.
    - **Cloud Access-Profil** - Wählen Sie das Cloud-Zugriffsprofil aus der Liste aus.
    - **Availability Zone** - Wählen Sie die Zonen aus, in denen Sie die Autoscale-Gruppen erstellen möchten. Abhängig von dem ausgewählten Cloud-Zugriffsprofil werden für dieses Profil spezifische Verfügbarkeitszonen aufgefüllt.
    - **Sicherheitsgruppe** — Sicherheitsgruppen steuern den eingehenden und ausgehenden Datenverkehr im Citrix ADC Agent. Sie erstellen Regeln für eingehenden und ausgehenden Datenverkehr, die Sie steuern möchten.
    - **Subnetz** - Wählen Sie das Management-Subnetz aus, in dem Sie einen Agenten bereitstellen möchten.
    - **Tags** - Geben Sie das Schlüssel-Wert-Paar für die Autoscale Gruppentags ein. Ein Tag besteht aus einem Schlüssel-Wert-Paar, das zwischen Groß- und Kleinschreibung unterschieden wird. Diese Tags ermöglichen es Ihnen, die Autoskalierungsgruppen einfach zu organisieren und zu identifizieren. Die Tags werden sowohl für Azure als auch für Citrix ADM angewendet.
5. Klicken Sie auf **Fertig stellen**.

Alternativ können Sie den Citrix ADM -Agent über Azure Marketplace installieren. Weitere Informationen finden Sie unter Installieren eines Citrix ADM -Agents auf Microsoft Azure.

Erstellen einer Website

Erstellen Sie eine Site in Citrix ADM, und fügen Sie die VNet-Details hinzu, die Ihrer Microsoft Azure-Ressourcengruppe zugeordnet sind.

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Sites**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie im Bereich **Cloud auswählen**
    a) Wählen Sie **Data Center** als **Standorttyp** aus.
    b) Wählen Sie in der Liste **Typ** die Option **Azure** aus.

c) Aktivieren Sie das Kontrollkästchen **VNet aus Azure abrufen**.

Mit dieser Option können Sie die vorhandenen VNet-Informationen aus Ihrem Microsoft Azure-Konto abrufen.

d) Klicken Sie auf **Weiter**.

4. **Wählen Sie im Bereich Region auswählen**

a) Wählen Sie im **Cloud Access-Profil** das Profil aus, das für Ihr Microsoft Azure-Konto erstellt wurde. Wenn keine Profile vorhanden sind, erstellen Sie ein Profil.

b) Klicken Sie auf **Hinzufügen**, um ein Cloud-Zugriffsprofil zu erstellen.

c) Geben Sie unter **Name** einen Namen an, um Ihr Azure-Konto in Citrix ADM zu identifizieren.

d) Geben Sie unter **Mandanten-Active Directory ID/Mandanten-ID** die Active Directory-ID des Mandanten oder das Konto in Microsoft Azure an.

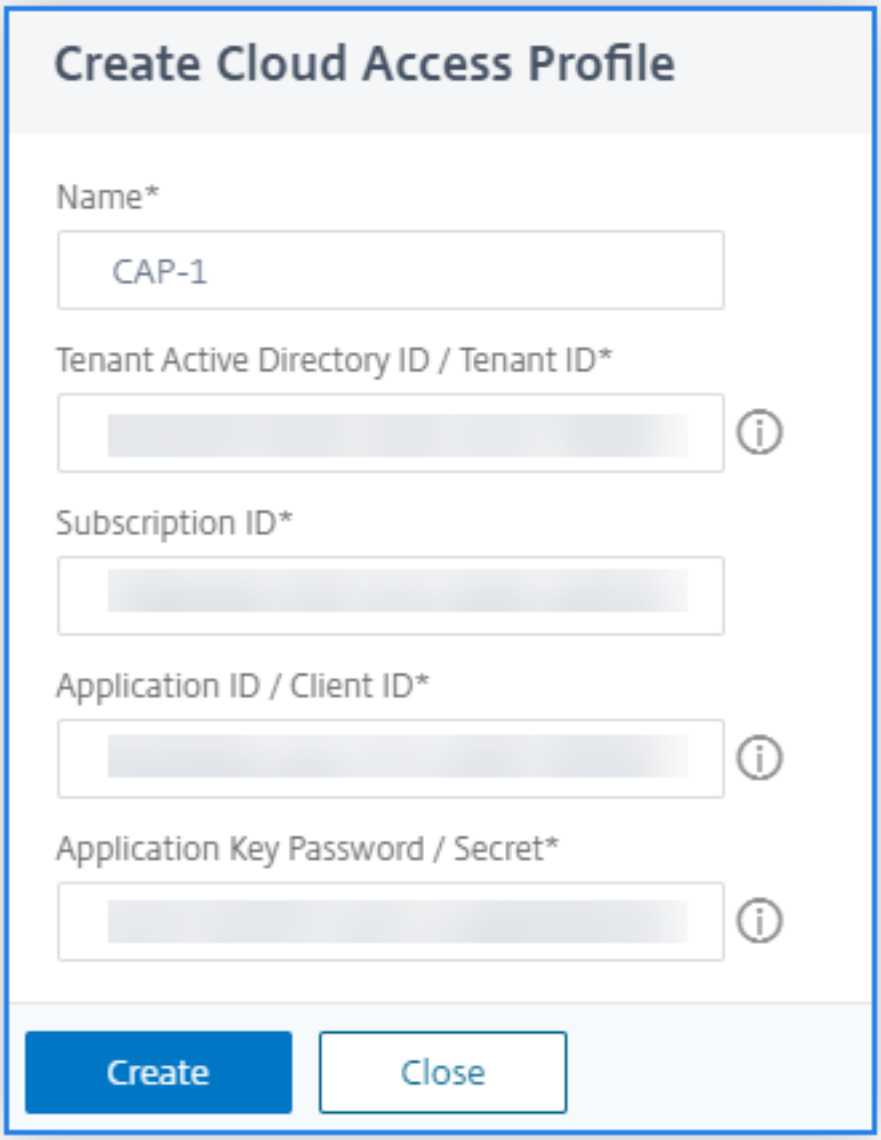
e) Geben Sie die **Abonnement-ID** an.

f) Geben Sie die **Anwendungs-ID/Client-ID** an.

g) Geben Sie das **Kennwort für den Anwendungsschlüssel** an.

h) Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Erstellen und Registrieren einer Anwendung und Zuordnen des Cloud-Zugriffsprofils zur Azure-Anwendung.



i) Wählen Sie in **VNet** das virtuelle Netzwerk aus, das Citrix ADC VPX Instanzen enthält, die Sie verwalten möchten.

j) Geben Sie einen **Standortnamen** an.

k) Klicken Sie auf **Fertig stellen**.

Zuordnen des Cloud Access-Profils zur Azure-Anwendung

Citrix ADM Begriff	Microsoft Azure-Begriff
Mandanten-Active Directory ID/Mandanten-ID	Verzeichnis-ID

Citrix ADM Begriff	Microsoft Azure-Begriff
Abonnement-ID	Abonnement-ID
Anwendungs-ID/Client-ID	Anwendungs-ID
Kennwort des Anwendungsschlüssels/Secret	Schlüssel oder Zertifikate oder Client-Geheimnisse

Anfügen der Site an einen Citrix ADM Dienstagenten

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Agents**.
2. Wählen Sie den Agenten aus, für den Sie eine Site anhängen möchten.
3. Klicken Sie auf **Site anhängen**.
4. Wählen Sie die Website aus der Liste aus, die Sie hinzufügen möchten.
5. Klicken Sie auf **Save**.

Schritt 1: Initialisieren der Konfiguration für die automatische Skalierung in Citrix ADM

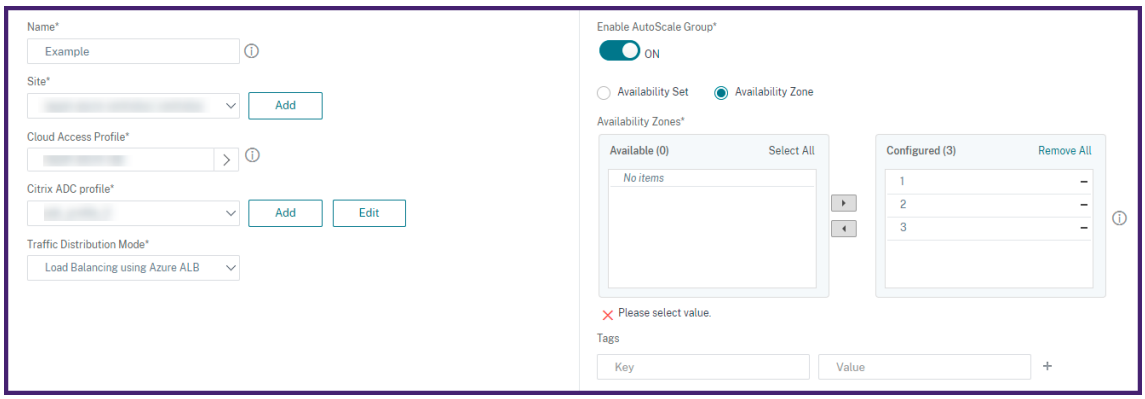
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **AutoScale-Gruppen**.
2. Klicken Sie auf **Hinzufügen**, um Gruppen mit automatischer Skalierung zu erstellen.

   Die Seite **Create AutoScale Group** wird angezeigt.
3. Wählen Sie **Microsoft Azure** aus, und klicken Sie auf **Weiter**.
4. Geben Sie unter **Basisparameter**die folgenden Details ein:
   - **Name:** Geben Sie einen Namen für die Gruppe “Automatisch skalieren” ein.
   - **Site:** Wählen Sie die Site aus, die Sie für die automatische Skalierung der Citrix ADC VPX Instanzen in Microsoft Azure erstellt haben. Wenn Sie keine Website erstellt haben, klicken Sie auf **Hinzufügen**, um eine Website zu erstellen.
   - **Agent:** Wählen Sie den Citrix ADM Agent aus, der die bereitgestellten Instanzen verwaltet.
   - **Cloud-Zugriffsprofil:** Wählen Sie das Cloud-Zugriffsprofil aus. Sie können auch ein Cloud Access-Profil hinzufügen oder bearbeiten.
   - **Geräteprofil:** Wählen Sie das Geräteprofil aus der Liste aus. Citrix ADM verwendet das Geräteprofil, wenn es sich bei der Citrix ADC VPX Instanz anmelden muss.

     > **Hinweis**
     >
     > Stellen Sie sicher, dass das ausgewählte Geräteprofil den Microsoft Azure-

> Kennwortregelnentspricht.

- **Verkehrsverteilungsmodus:** Die Option **Lastenausgleich mit Azure LB** ist als Standardverteilungsmodus für den Datenverkehr ausgewählt. Sie können den **DNS auch im Azure DNS-Modus** für die Verkehrsverteilung auswählen.
- **AutoScale-Gruppen aktivieren:** Aktivieren oder deaktivieren Sie den Status der ASG-Gruppen. Diese Option ist standardmäßig aktiviert. Wenn diese Option deaktiviert ist, wird die automatische Skalierung nicht ausgelöst.
- **Verfügbarkeitsset oder Availability Zone:** Wählen Sie das Verfügbarkeitsset oder die Verfügbarkeitszonen aus, in denen Sie die Autoskalierungs-Gruppen erstellen möchten. Abhängig vom ausgewählten Cloudzugriffsprofil werden Verfügbarkeitszonen in der Liste angezeigt.
- **Tags:** Geben Sie das Schlüssel-Wert-Paar für die Autoscale Gruppentags ein. Ein Tag besteht aus einem Schlüssel-Wert-Paar, das zwischen Groß- und Kleinschreibung unterschieden wird. Diese Tags ermöglichen es Ihnen, die Autoskalierungsgruppen einfach zu organisieren und zu identifizieren. Die Tags werden sowohl für Microsoft Azure als auch für Citrix ADM angewendet.



5. Klicken Sie auf **Weiter**.

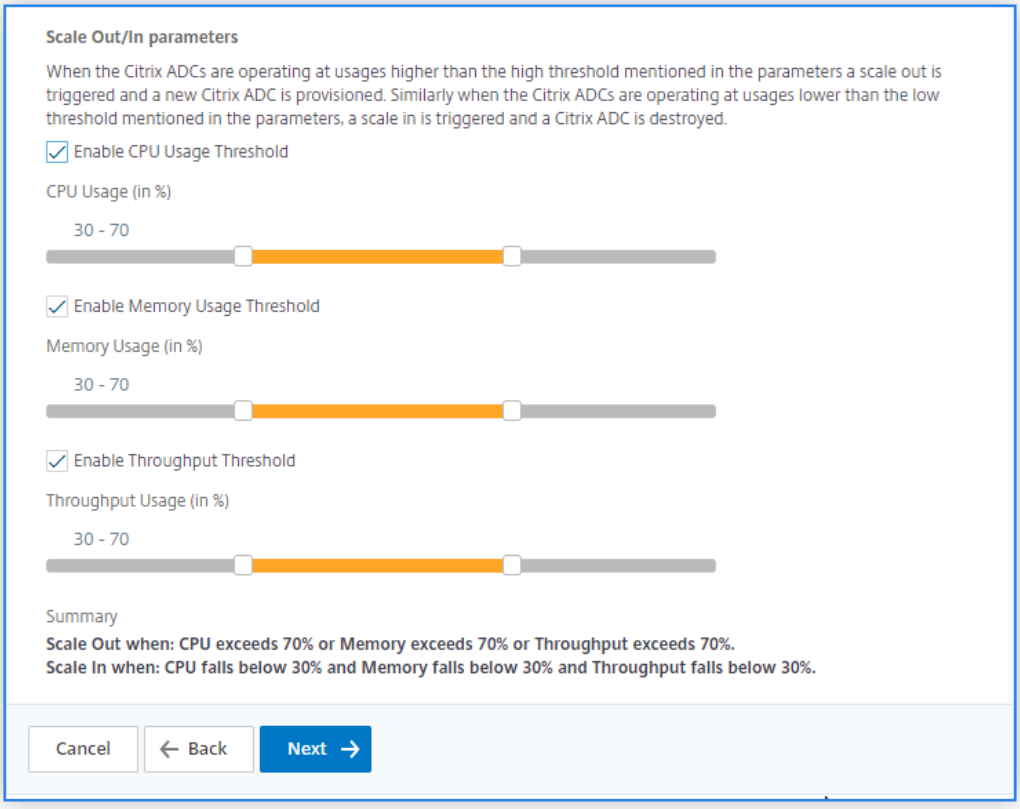
Schritt 2: Konfigurieren der Parameter für die automatische Skalierung

1. Geben Sie auf der Registerkarte **AutoScale-Parameter** die folgenden Details ein.
2. Wählen Sie einen oder mehrere der folgenden Schwellenwertparameter aus, deren Werte überwacht werden müssen, um ein Scale-Out oder ein Scale-In auszulösen.
   - **Schwellenwert für CPU-Auslastung aktivieren:** Überwachen Sie die Metriken basierend auf der CPU-Auslastung.
   - **Schwellenwert für die Speicherauslastung aktivieren:** Überwachen Sie die Metriken basierend auf der Speicherauslastung.

- **Durchsatzschwelle aktivieren:** Überwachen Sie die Metriken basierend auf dem Durchsatz.

  Hinweis

  - Der standardmäßige Mindestgrenzwert beträgt 30 und der Höchstgrenzwert 70. Sie ändern jedoch, um die Limits zu ändern.
  - Der Mindestgrenzwert muss gleich oder kleiner als die Hälfte des Höchstgrenzwerts sein.
  - Sie können mehrere Schwellenwerte für die Überwachung auswählen. Scale-out wird ausgelöst, wenn mindestens einer der Schwellenwertparameter über dem maximalen Schwellenwert liegt. Ein Scale-In wird jedoch nur ausgelöst, wenn alle Schwellenwertparameter unterhalb ihrer normalen Schwellenwerte arbeiten.



- **Halten Sie einen Ersatzknoten für eine schnellere Scale-Out:** Diese Option hilft, eine schnellere Scale-Out zu erreichen. ADM stellt einen Reserve-Knoten bereit, bevor die Scale-Out-Aktion ausgeführt wird, und beendet ihn. Wenn die Scale-Out-Aktion für die Autoscale-Gruppe auftritt, startet der ADM den bereits bereitgestellten Ersatzknoten. Infolgedessen reduziert es die Zeit für das Scale-Out.

- **Mindestinstanzen:** Wählen Sie die Mindestanzahl von Instanzen aus, die für diese Autoscale-Gruppe bereitgestellt werden müssen.

  Die Standardanzahl der Instanzen entspricht der Anzahl der ausgewählten Zonen. Sie können nur die Mindestinstanzen in den Vielfachen der angegebenen Anzahl von Zonen erhöhen.

  Wenn beispielsweise die Anzahl der Availability Zones 4 beträgt, sind die Mindestinstanzen standardmäßig 4. Sie können die minimalen Instanzen um 8, 12, 16 erhöhen.

- **Maximale Instanzen:** Wählen Sie die maximale Anzahl von Instanzen aus, die für diese Autoscale-Gruppe bereitgestellt werden müssen.

  Die maximale Anzahl von Instanzen muss größer oder gleich dem Wert der minimalen Instanzen sein. Die maximale Anzahl von Instanzen darf die Anzahl der Availability Zones multipliziert mit 32 nicht überschreiten.

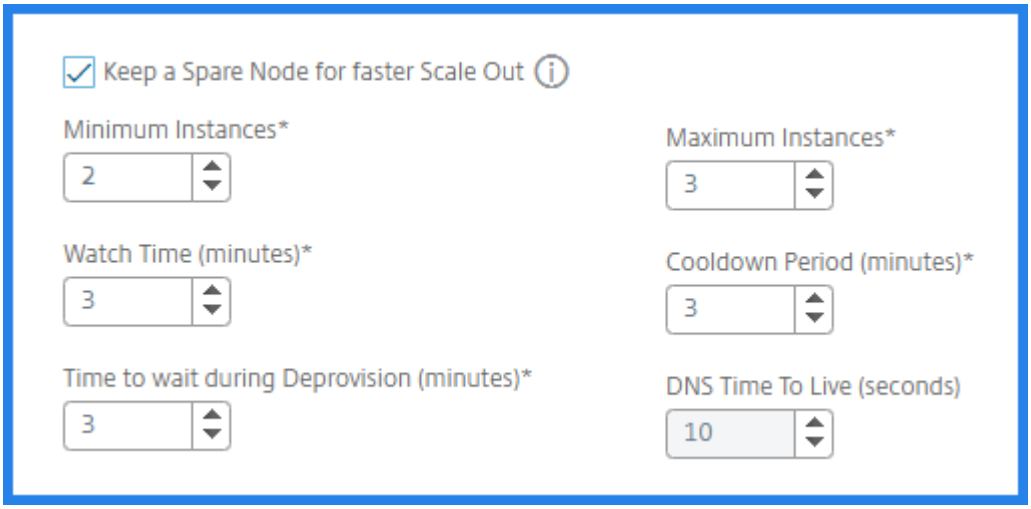
  Maximale Anzahl von Instanzen = Anzahl der Availability Zones * 32

- **Watch-Zeit (Minuten):** Wählen Sie die Dauer der Uhr. Die Zeit, für die der Schwellenwert des Skalierungsparameters überschritten werden muss, damit die Skalierung erfolgt. Wenn der Schwellenwert für alle Proben, die in dieser angegebenen Zeit gesammelt wurden, überschritten wird, geschieht eine Skalierung.

- **Abklingzeit (Minuten):** Wählen Sie die Abklingzeit aus. Während des Scale-Outs ist die Abklingzeit die Zeit, für die die Auswertung der Statistiken nach einem Scale-Out gestoppt werden muss. Dieser Zeitraum sorgt für den organischen Anbau von Instanzen einer Autoscale-Gruppe. Bevor die nächste Skalierungsentscheidung ausgelöst wird, wird darauf gewartet, dass sich der aktuelle Datenverkehr stabilisiert und auf den aktuellen Satz von Instanzen durchdurchschnittlich wird.

- **Wartezeit während der Deprovisierung (Minuten):** Wählen Sie den Zeitüberschreitungszeitraum für die Ablaufverbindung. Während der Scale-In-Aktion wird eine Instanz identifiziert, die die Bereitstellung aufweist. Citrix ADM schränkt die identifizierte Instanz davon ab, neue Verbindungen zu verarbeiten, bis die angegebene Zeit vor der Aufhebung der Bereitstellung abläuft. In diesem Zeitraum können vorhandene Verbindungen zu dieser Instanz entzogen werden, bevor die Bereitstellung aufgehoben wird.

- **DNS Time To Live (Sekunden):** Wählen Sie die Zeit (in Sekunden) aus. In diesem Zeitraum wird ein Paket in einem Netzwerk existieren, bevor der Router das Paket verwirft. Dieser Parameter ist nur anwendbar, wenn der Verkehrsverteilungsmodus DNS ist, der den Microsoft Azure-Traffic-Manager verwendet.



3. Klicken Sie auf **Weiter**.

Schritt 3: Konfigurieren von Lizenzen für die Provisioning Citrix ADC-Instanzen

Wählen Sie einen der folgenden Modi aus, um Citrix ADC-Instanzen zu lizenzieren, die Teil der Autoscale Group sind:

- **Verwenden von Citrix ADM**: Beim Provisioning von Citrix ADC-Instanzen checkt die Autoscale-Gruppe die Lizenzen von Citrix ADM aus.
- **Verwenden von Microsoft Azure**: Die Option **Aus Cloud zuweisen** verwendet die Citrix Produktlizenzen, die im Azure Marketplace verfügbar sind. Bei Provisioning Citrix ADC-Instanzen verwendet die Autoscale-Gruppe die Lizenzen vom Marketplace.

  Wenn Sie Lizenzen von Azure Marketplace verwenden, geben Sie das Produkt oder die Lizenz auf der Registerkarte **Bereitstellungsparameter** an.

Weitere Informationen finden Sie unter Lizenzanforderungen.

Lizenzen von Citrix ADM verwenden

Um diese Option zu verwenden, stellen Sie sicher, dass Sie das Citrix ADC Produkt mit dem Plan **Eigene Lizenzsoftware** in Azure abonniert haben. Siehe Abonnieren der Citrix ADC VPX -Lizenz in Microsoft Azure.

1. Wählen Sie auf der Registerkarte **Lizenz** die Option **Aus ADM zuweisen**.
2. Wählen Sie unter **Lizenztyp**eine der folgenden Optionen aus der Liste:
   - **Bandbreitenlizenzen:** Sie können eine der folgenden Optionen aus der Liste **Bandbreitenlizenztypen** auswählen:

- **Pooled Capacity:** Geben Sie die Kapazität an, die für jede neue Instanz in der Gruppe Autoscale zugewiesen werden soll.

  Aus dem gemeinsamen Pool checkt jede ADC-Instanz in der Autoscale-Gruppe eine Instanzlizenz aus und es wird nur so viel Bandbreite angegeben.

- **VPX-Lizenzen:** Wenn eine Citrix ADC VPX Instanz bereitgestellt wird, checkt die Instanz die Lizenz vom Citrix ADM aus.

- **Virtuelle CPU-Lizenzen:** Die bereitgestellte Citrix ADC VPX Instanz checkt Lizenzen in Abhängigkeit von der Anzahl der CPUs aus, die in der Autoscale-Gruppe ausgeführt werden.

> **Hinweis:**
>
> Wenn die bereitgestellten Instanzen entfernt oder gelöscht werden, kehren die angewendeten Lizenzen in den Citrix ADM -Lizenzpool zurück. Diese Lizenzen können für die Bereitstellung neuer Instanzen während der nächsten Autoscale wiederverwendet werden.

3. Wählen Sie in **License Edition** die Lizenzversion aus. Die Gruppe “Autoscale” verwendet die angegebene Edition zum Bereitstellen von Instanzen.
4. Klicken Sie auf **Weiter**.

Schritt 4: Konfigurieren von Cloud-Parametern

1. Geben Sie auf der Registerkarte **Bereitstellungsparameter** die folgenden Details ein:
   - **Ressourcengruppe:** Wählen Sie die Ressourcengruppe aus, in der Citrix ADC-Instanzen bereitgestellt werden.
   - **Produkt/Lizenz:** Wählen Sie die Citrix ADC Produktversion aus, die Sie bereitstellen möchten. Stellen Sie sicher, dass der programmgesteuerte Zugriff für den ausgewählten Typ aktiviert ist. Weitere Informationen finden Sie unter Abonnieren der Citrix ADC VPX -Lizenz in Microsoft Azure.
   - **Azure-VM-Größe:** Wählen Sie die erforderliche VM-Größe aus der Liste aus.

     > **Hinweis**
     >
     > Stellen Sie sicher, dass die ausgewählte Azure-VM-Größe mindestens drei Netzwerkkarten aufweist. Weitere Informationen finden Sie unter Unterstützte virtuelle Azure-Images für die automatische Skalierung.

   - **Cloud-Zugriffsprofil für ADC:** Citrix ADM meldet sich mit diesem Profil bei Ihrem Azure-Konto an, um ADC-Instanzen bereitzustellen oder aufzuheben. Außerdem wird Azure LB oder Azure DNS konfiguriert.
   - **Image:** Wählen Sie das erforderliche Citrix ADC Versionsimage aus. Klicken Sie auf **Neu hinzufügen**, um ein Citrix ADC Image hinzuzufügen.

- **Sicherheitsgruppen:** Sicherheitsgruppen steuern den eingehenden und ausgehenden Datenverkehr in einer Citrix ADC VPX Instanz. Wählen Sie eine Sicherheitsgruppe für den Datenverkehr Management, Client und Server aus. Weitere Informationen zu Verwaltungs-, Client- und Server-Sicherheitsgruppen finden Sie unterSicherheitsgruppen.
- **Subnetze:** Sie müssen über drei separate Subnetze wie Management, Client und Server-Subnetz verfügen, um Citrix ADC -Subnetze automatisch skalieren zu können. Subnetze enthalten die erforderlichen Entitäten für die automatische Skalierung. Wählen Sie Weitere Informationen finden Sie unterSubnetze.

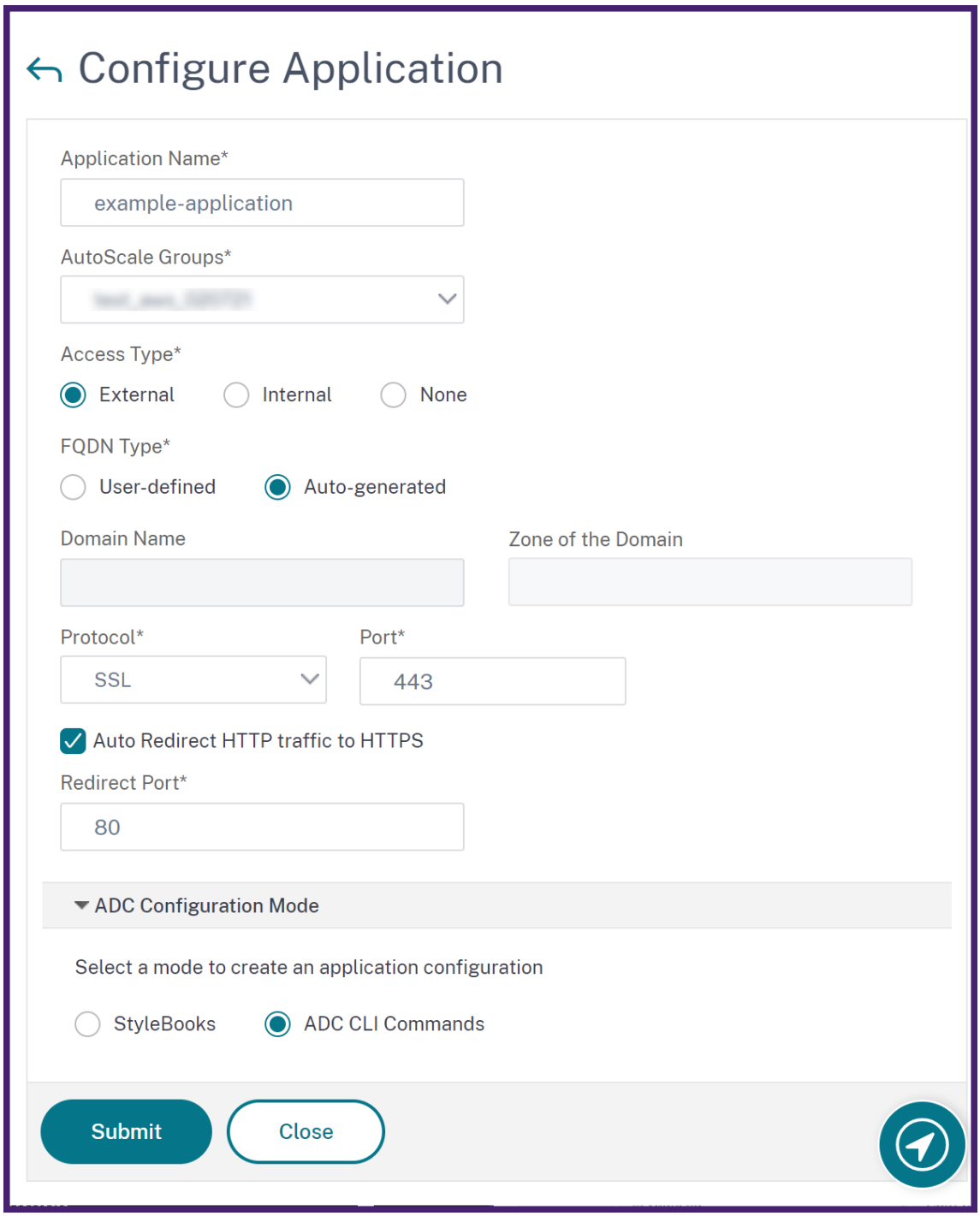
2. Klicken Sie auf **Fertig stellen**.

Schritt 5: Konfigurieren einer Anwendung für die Autoscale-Gruppe

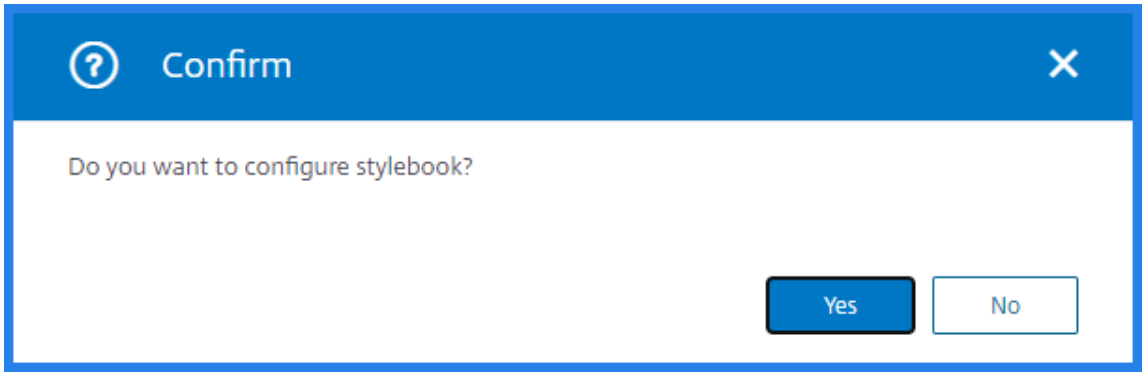
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Autoscale-Gruppen**.
2. Wählen Sie die von Ihnen erstellte Gruppe “Automatisch skalieren” aus, und klicken Sie auf **Konfigurieren**.
3. Geben Sie unter **Anwendung konfigurieren** die folgenden Details an:
   - **Anwendungsname** - Geben Sie den Namen einer Anwendung an.
   - **Zugriffstyp** - Sie können die ADM-Lösung für die automatische Skalierung sowohl für externe als auch für interne Anwendungen verwenden. Wählen Sie den erforderlichen Anwendungszugriffstyp aus.
   - **FQDN-Typ** - Wählen Sie einen Modus für die Zuweisung von Domänen- und Zonennamen aus.

     Wenn Sie manuell angeben möchten, wählen Sie **Benutzerdefiniert** aus. Um Domänen- und Zonennamen automatisch zuzuweisen, wählen Sie **Automatisch generiert** aus.
   - **Domänenname** - Geben Sie den Domänennamen einer Anwendung an. Diese Option ist nur anwendbar, wenn Sie Benutzerdefinierter FQDN-Typ auswählen.
   - **Zone der Domäne** - Wählen Sie den Zonennamen einer Anwendung aus der Liste aus. Diese Option ist nur anwendbar, wenn Sie Benutzerdefinierter FQDN-Typ auswählen.

     Dieser Domänen- und Zonenname leitet zu den virtuellen Servern in Azure um. Wenn Sie beispielsweise eine Anwendung in `app.example.com`hosten, ist `app`der Domänenname und `example.com`der Zonenname.
   - **Protokoll** - Wählen Sie den Protokolltyp aus der Liste aus. Die konfigurierte Anwendung empfängt den Datenverkehr abhängig vom ausgewählten Protokolltyp.
   - **Port** - Geben Sie den Portwert an. Der angegebene Port wird verwendet, um eine Kommunikation zwischen der Anwendung und der Autoscale-Gruppe herzustellen.

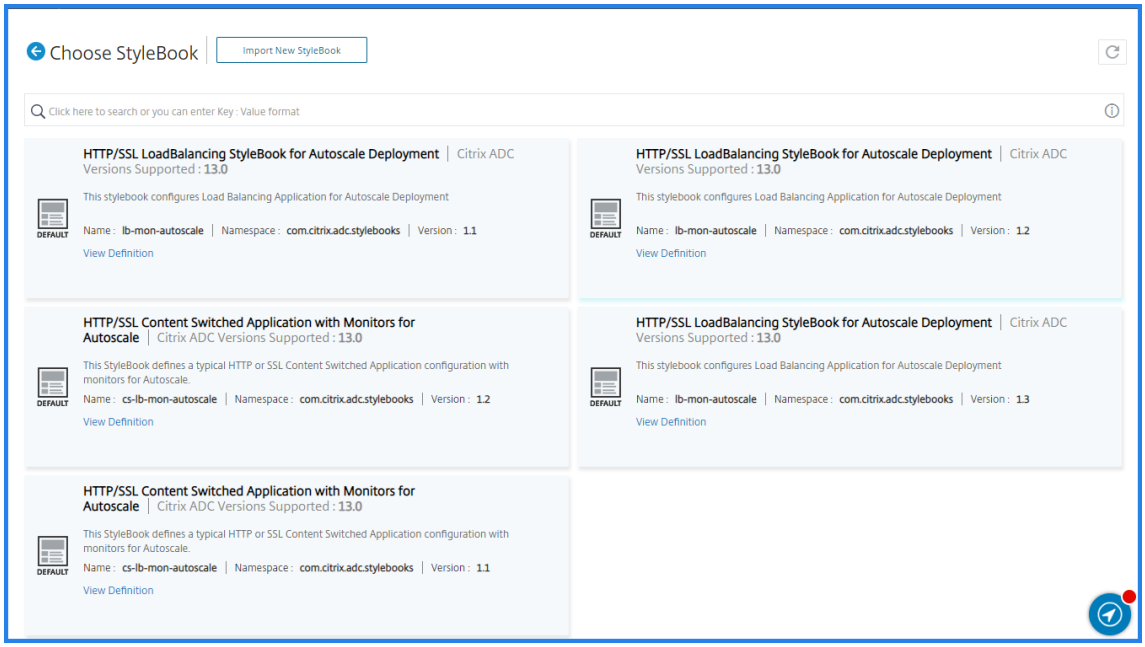


Wenn Sie eine Anwendung mit StyleBooks konfigurieren möchten, wählen Sie im Bestätigungsfenster **Ja** aus.



> **Hinweis Ändern Sie**
>
> den Zugriffstyp einer Anwendung, wenn Sie die folgenden Details in Zukunft ändern möchten:
>
> - FQDN Typ
> - Domänenname
> - Zone der Domäne

4. Wählen Sie das gewünschte StyleBook aus, das Sie Konfigurationen für die ausgewählte Autoscale-Gruppe bereitstellen möchten.



Wenn Sie StyleBooks importieren möchten, klicken Sie auf **Neues StyleBook importieren**.

5. Geben Sie die Werte für alle Parameter an.

   Die Konfigurationsparameter sind im ausgewählten StyleBook vordefiniert.

6. Aktivieren Sie das Kontrollkästchen **Application Server Group Type CLOUD**, um die Anwendungsserver anzugeben, die im Skalierungssatz der virtuellen Maschine verfügbar sind.

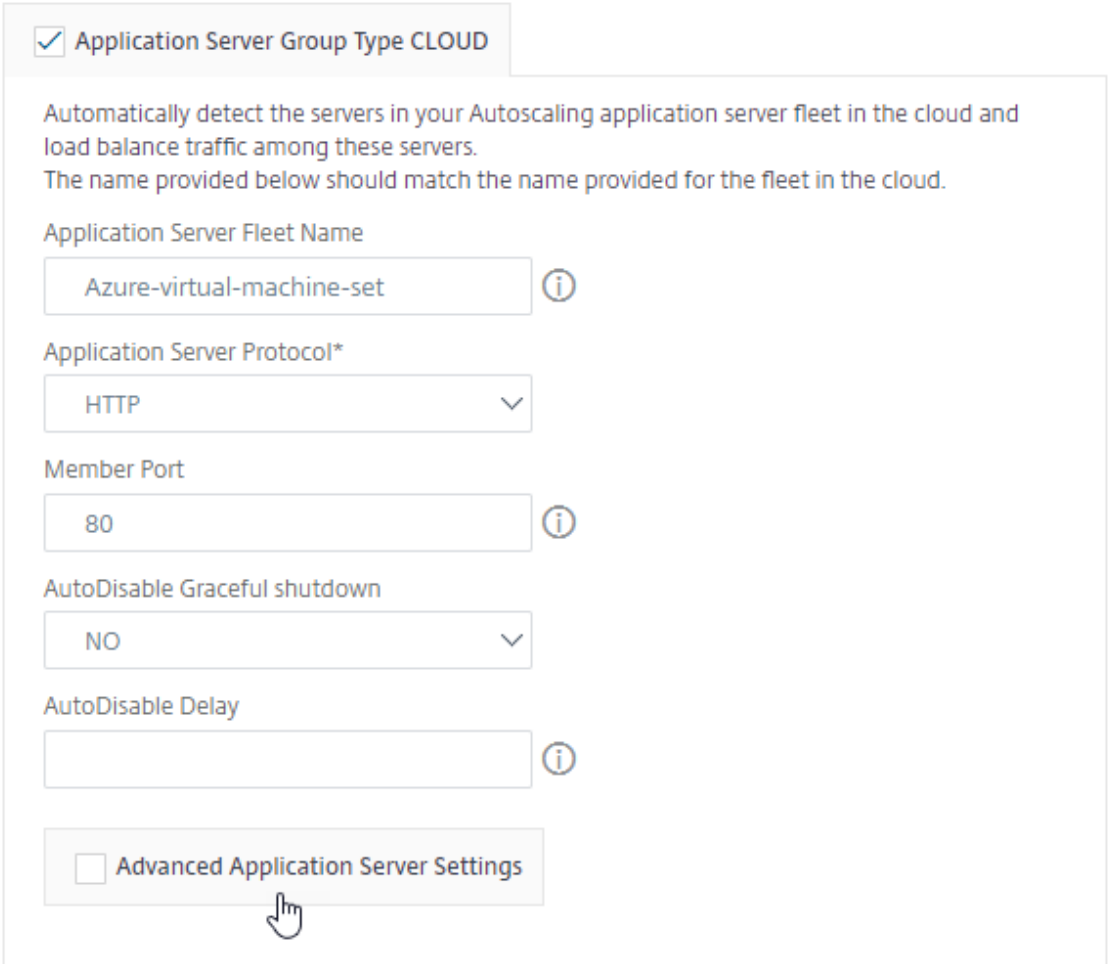
a) Geben Sie unter **Application Server Fleet Name**den **Namen der Autoscale-Einstellung** Ihres Skalierungssatzes für virtuelle Maschinen an.

b) Wählen Sie das **Application Server-Protokoll** aus der Liste aus.

c) Geben Sie unter **Memberport** den Portwert des Anwendungsservers an.

> **Hinweis: Stellen Sie**
>
> sicher, dass **AutoDisable Graceful shutdown** auf **No** festgelegt ist und das Feld **AutoDisable Delay** leer ist.

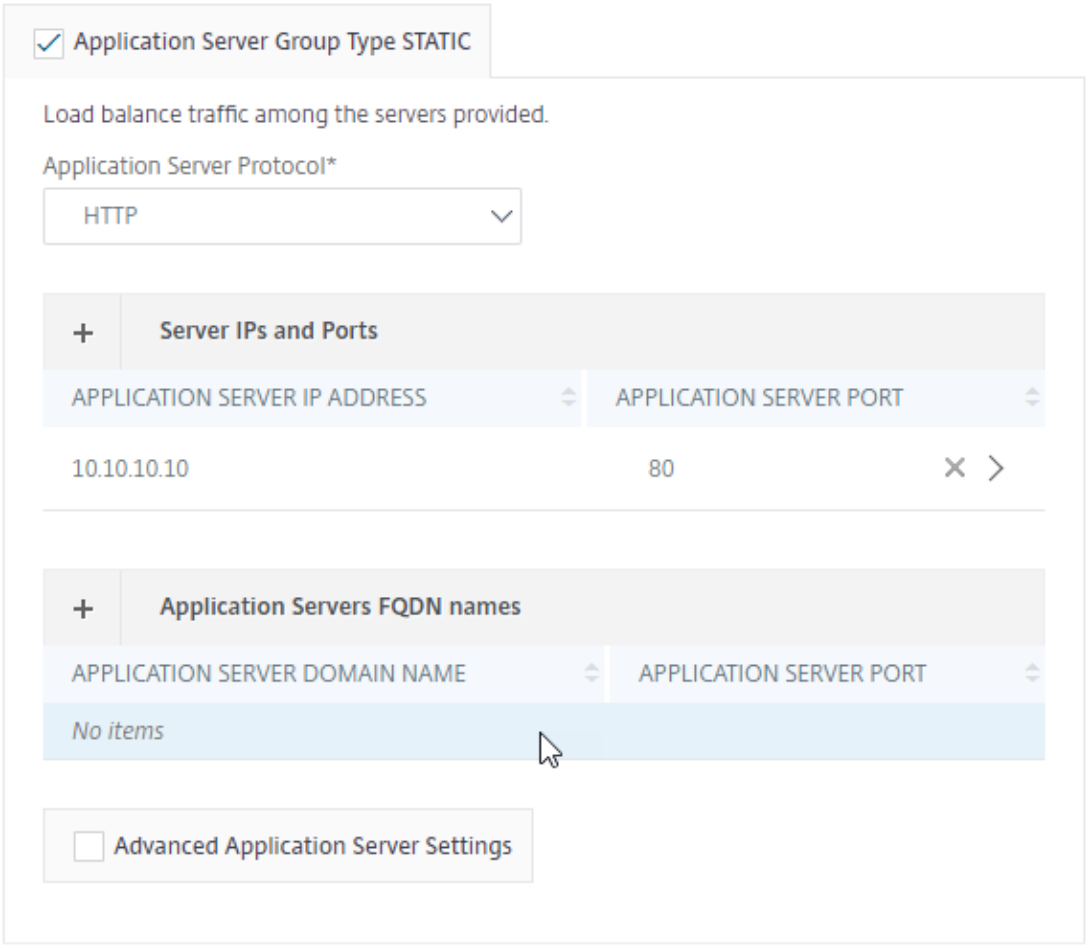
d) Wenn Sie die erweiterten Einstellungen für Ihre Anwendungsserver angeben möchten, aktivieren Sie das Kontrollkästchen **Erweiterte Anwendungsserver-Einstellungen**. Geben Sie dann die erforderlichen Werte an, die unter **Erweiterte Anwendungsservereinstellungen**aufgeführt sind.



7. Wenn Sie eigenständige Anwendungsserver im virtuellen Netzwerk haben, aktivieren Sie das Kontrollkästchen **Anwendungsservergruppentyp STATIC**:

a) Wählen Sie das **Application Server-Protokoll** aus der Liste aus.

b) Klicken Sie **unter Server-IPs und -Ports**auf **+**, um eine IP-Adresse, einen Port und ein Gewicht des Anwendungsservers hinzuzufügen, und klicken Sie dann auf **Erstellen**.



8. Klicken Sie auf **Erstellen**.

Ändern der Konfiguration von Gruppen für automatische Skalierung

Sie können eine Autoscale-Gruppenkonfiguration ändern oder eine Autoscale-Gruppe löschen. Sie können nur die folgenden Gruppenparameter für die automatische Skalierung ändern:

- Maximal- und Minimalgrenzen der Schwellenwerte
- Minimale und maximale Instanzwerte
- Wert der Ablaufanschlussperiode
- Wert der Abklingperiode
- Wert für die Dauer der Uhr

Sie können auch die Autoskalier-Gruppen löschen, nachdem sie erstellt wurden.

Wenn eine Autoscale-Gruppe gelöscht wird, werden alle Domänen und IP-Adressen vom DNS abgemeldet und die Clusterknoten werden aufgehoben.

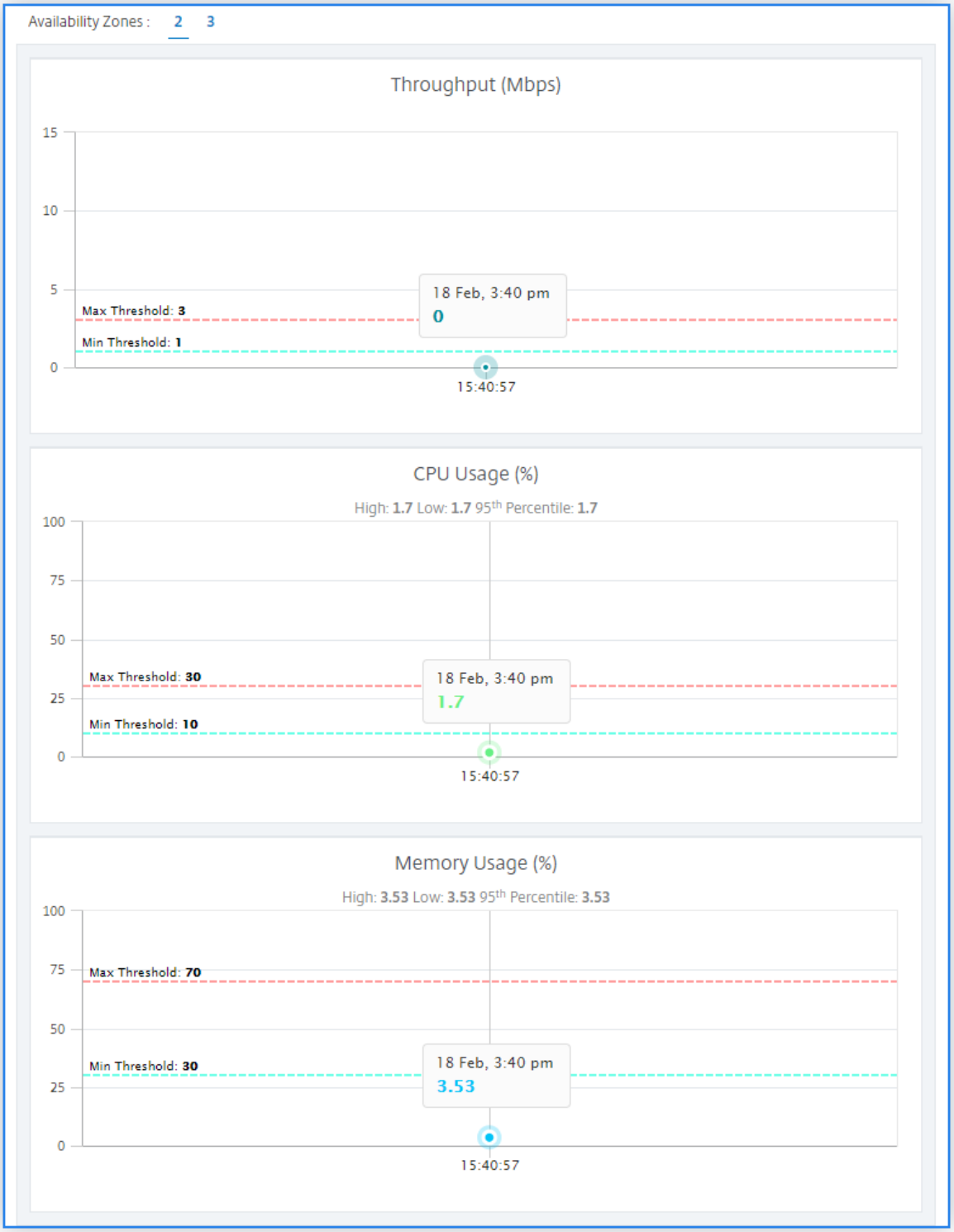
Dashboard

April 28, 2021

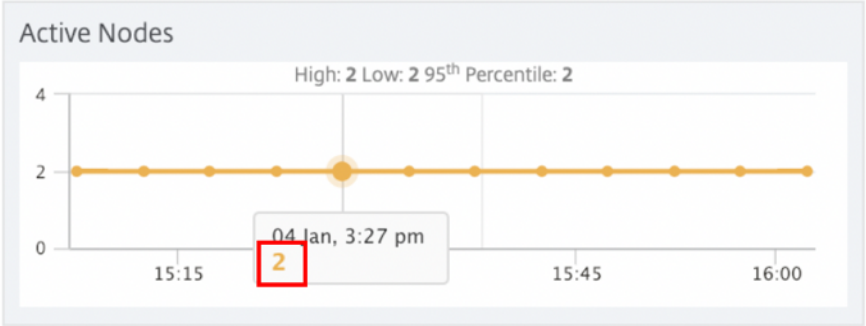
1. Navigieren Sie in Citrix ADM zu **Netzwerke > Gruppen automatisch skalieren**.
2. Wählen Sie die Autoskalierungsgruppe aus, und klicken Sie auf **Dashboard**.

Sie können das Diagramm für die ausgewählten Überwachungsparameter anzeigen. Im rechten Bereich werden die Ereignisse angezeigt, die die automatische Skalierung auslösen. Im linken Bereich werden die aktiven Knoten im Cluster pro Zone, das Diagramm der aktiven Knoten und die Ereignisse angezeigt.

Die folgende Abbildung zeigt ein Beispiel-Dashboard.

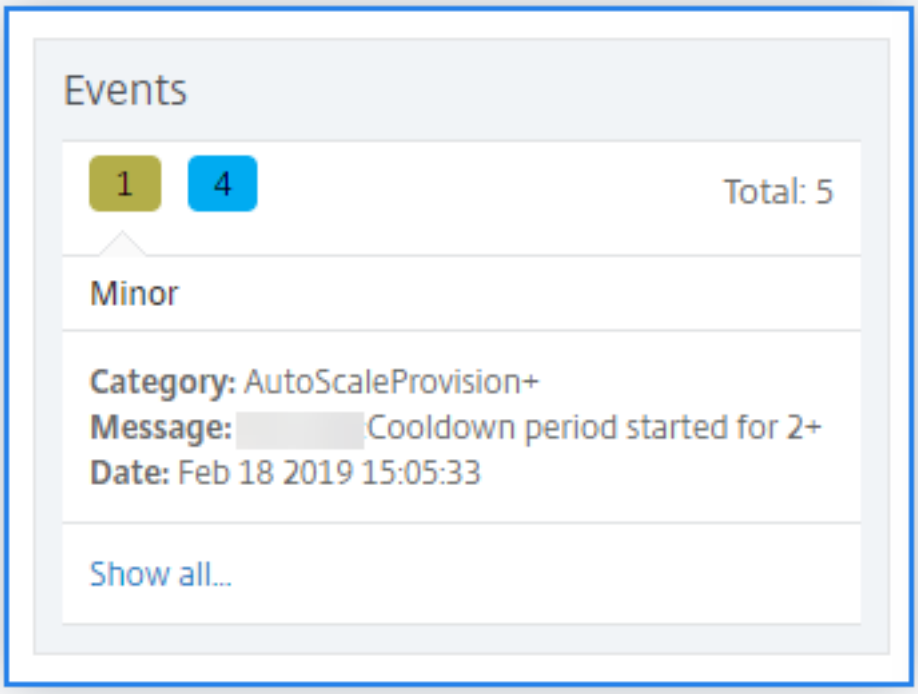


Die folgende Abbildung zeigt das Diagramm der aktiven Knoten. Die Zahl unter dem Zeitstempel zeigt die Anzahl der aktiven Knoten an. Sie können jederzeit die Anzahl der aktiven Knoten anzeigen, die Teil der Availability Zone sind.

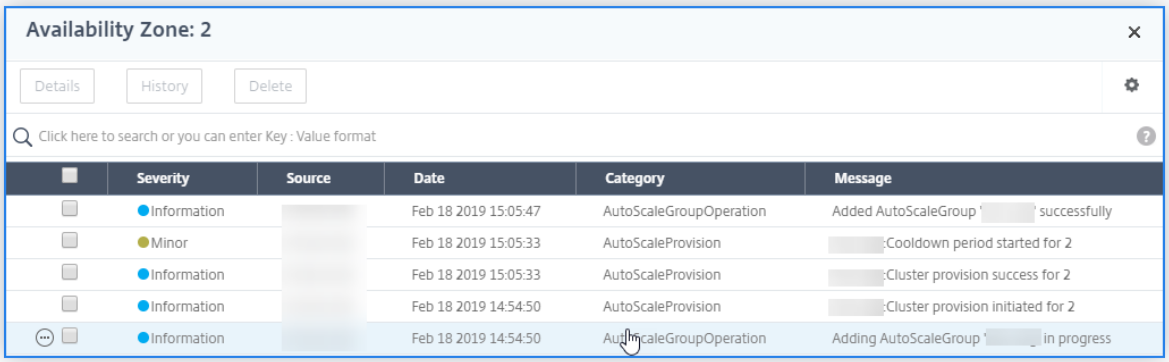


Ereignisse

In **Dashboard**zeigt die Registerkarte **Ereignisse**die Gesamtzahl der Ereignisse für die ausgewählte Autoskalierungsgruppe an. Außerdem wird eine kurze Meldung des letzten Ereignisses angezeigt.



Klicken Sie auf **Alle anzeigen, um die Details der Ereignisse anzuzeigen**.



Azure-Terminologien

April 28, 2021

Im Folgenden finden Sie die Liste der Azure-Terminologien, die in Citrix ADM erforderlich sind:

Begriff	Definition
Azure-Load Balancer	Der Azure-Load Balancer ist eine Ressource, die eingehenden Datenverkehr auf Citrix ADC VPX Instanzen in einem Netzwerk verteilt. Der Datenverkehr wird auf virtuelle Maschinen verteilt, die in einem Lastausgleichssatz definiert sind. Ein Load Balancer kann extern oder mit dem Internet verbunden sein oder intern sein.
Verkehrsleiter	Der Azure Traffic Manager ist der DNS-basierte Load Balancer in Microsoft Azure. Er sendet den eingehenden Datenverkehr an die gewünschte Citrix ADC VPX Instanz in einem Netzwerk.
Azure Resource Manager (ARM)	ARM ist das neue Verwaltungsframework für Dienste in Azure. Azure Load Balancer wird mit ARM-basierten APIs und Tools verwaltet.
Back-End-Adresspool	Diese IP-Adressen sind mit der Netzwerkkarte der virtuellen Maschine verknüpft, auf die die Last verteilt wird.

Begriff	Definition
BLOB	Binary Large Object — Jedes binäre Objekt wie eine Datei oder ein Image, das im Azure-Speicher gespeichert werden kann.
Front-End-IP-Konfiguration	Ein Azure Load Balancer kann eine oder mehrere Front-End-IP-Adressen enthalten, die auch als virtuelle IPs (VIPs) bezeichnet werden. Diese IP-Adressen dienen als Eindringen für den Datenverkehr.
Öffentliche Instanz-IP (ILPIP)	Eine ILPIP ist eine öffentliche IP-Adresse, die Sie direkt Ihrer virtuellen Maschine oder Rolleninstanz anstelle des Clouddiensts zuweisen können. Diese IP tritt nicht an die Stelle der VIP (virtuelle IP), die Ihrem Cloud-Dienst zugewiesen ist. Es handelt sich vielmehr um eine zusätzliche IP-Adresse, mit der Sie direkt eine Verbindung zu Ihrer virtuellen Maschine oder Rolleninstanz herstellen können.
Eingehende NAT-Regeln	Diese Regeln ordnen einen öffentlichen Port auf dem Load Balancer einem Port für die bestimmte virtuelle Maschine im Back-End-Adresspool zu.
IP-Konfiguration	Es handelt sich um ein IP-Adresspaar (öffentliche IP und private IP), das einer einzelnen NIC zugeordnet ist. In einer IP-Konfiguration kann die öffentliche IP-Adresse NULL sein. Jeder NIC kann mehrere IP-Konfigurationen mit bis zu 255 verbunden sein.

Begriff	Definition
Lastenausgleichsregeln	Eine Regeleigenschaft, die eine gegebene Front-End-IP- und Portkombination einer Gruppe von Back-End-IP-Adressen und Portkombinationen zuordnet. Mit einer einzelnen Definition einer Load Balancer-Ressource können Sie mehrere Lastausgleichsregeln definieren. Jede Regel spiegelt eine Kombination aus Front-End-IP und Port sowie Back-End-IP und Port wider, die virtuellen Maschinen zugeordnet sind.
Netzwerksicherheitsgruppe (NSG)	NSG enthält eine Liste von Zugriffssteuerungslisten (Access Control List, ACL) -Regeln, die Netzwerkdatenverkehr zu Ihren virtuellen Maschineninstanzen in einem virtuellen Netzwerk zulassen oder verweigern. NSGs können entweder Subnetzen oder einzelnen Instanzen virtueller Maschinen innerhalb dieses Subnetzes zugeordnet werden.
Private IP-Adresse	Diese Adresse ist eine IP-Adresse, die für die Kommunikation innerhalb eines virtuellen Azure-Netzwerks verwendet wird, und Ihr lokales Netzwerk, wenn ein VPN-Gateway verwendet wird, um Ihr Netzwerk auf Azure zu erweitern. Private IP-Adressen ermöglichen Azure-Ressourcen die Kommunikation mit anderen Ressourcen. Die Kommunikation in einem virtuellen Netzwerk oder einem lokalen Netzwerk erfolgt über ein VPN-Gateway oder eine ExpressRoute-Schaltung. Für diese Kommunikation ist keine internetfähige IP-Adresse erforderlich. Im Azure Resource Manager Bereitstellungsmodell ist eine private IP-Adresse mit den virtuellen Maschinen, dem Internal Load Balancer (ILB) und den Application Gateways von Azure verknüpft.

Begriff	Definition
Sonden	Integritätsprobes, die verwendet werden, um die Verfügbarkeit von Instanzen virtueller Maschinen im Back-End-Adresspool zu überprüfen.
Öffentliche IP-Adressen (PIP)	PIP wird für die Kommunikation mit dem Internet verwendet. Es umfasst öffentliche Azure-Dienste, die mit virtuellen Maschinen, Internal Load Balancer (ILB), VPN-Gateways und Application Gateways von Azure verknüpft sind.
Region	Ein Gebiet innerhalb der Geographie, das keine nationalen Grenzen überschreitet, enthält ein oder mehrere Rechenzentren. Preise, regionale Dienstleistungen und Angebotsarten werden auf regionaler Ebene angezeigt. Eine Region wird in der Regel mit einer anderen Region gekoppelt, die eine große Entfernung von einem regionalen Paar umfasst. Regionale Paare werden auch als Mechanismus für Disaster Recovery und Hochverfügbarkeitsszenarien verwendet. Auch bekannt als Standort.
Ressourcengruppe	Ein Container im Ressourcen-Manager enthält zugehörige Ressourcen für eine Anwendung. Die Ressourcengruppe kann alle Ressourcen für eine Anwendung oder nur die Ressourcen enthalten, die logisch gruppiert sind.
Speicherkonto	Mit einem Azure-Speicherkonto können Sie auf den Azure-BLOB, die Warteschlange, die Tabelle und die Dateidienste in Azure Storage zugreifen. Ihr Speicherkonto stellt den eindeutigen Namespace für Ihre Azure-Speicherdatenobjekte bereit.

Begriff	Definition
Virtuelle Maschine	Die Software-Implementierung eines physischen Computers, auf dem ein Betriebssystem ausgeführt wird. Mehrere virtuelle Maschinen können gleichzeitig auf derselben Hardware ausgeführt werden. In Azure sind virtuelle Maschinen in verschiedenen Größen verfügbar.
Virtuelles Netzwerk	Ein virtuelles Azure-Netzwerk ist eine Darstellung Ihres eigenen Netzwerks in der Cloud. Es ist logisch isoliert und für Ihr Abonnement in der Azure-Cloud dediziert. Sie können die IP-Adressblöcke, DNS-Einstellungen, Sicherheitsrichtlinien und Routingtabellen in diesem Netzwerk steuern.

Provisioning von Citrix ADC VPX Instanzen in Google Cloud

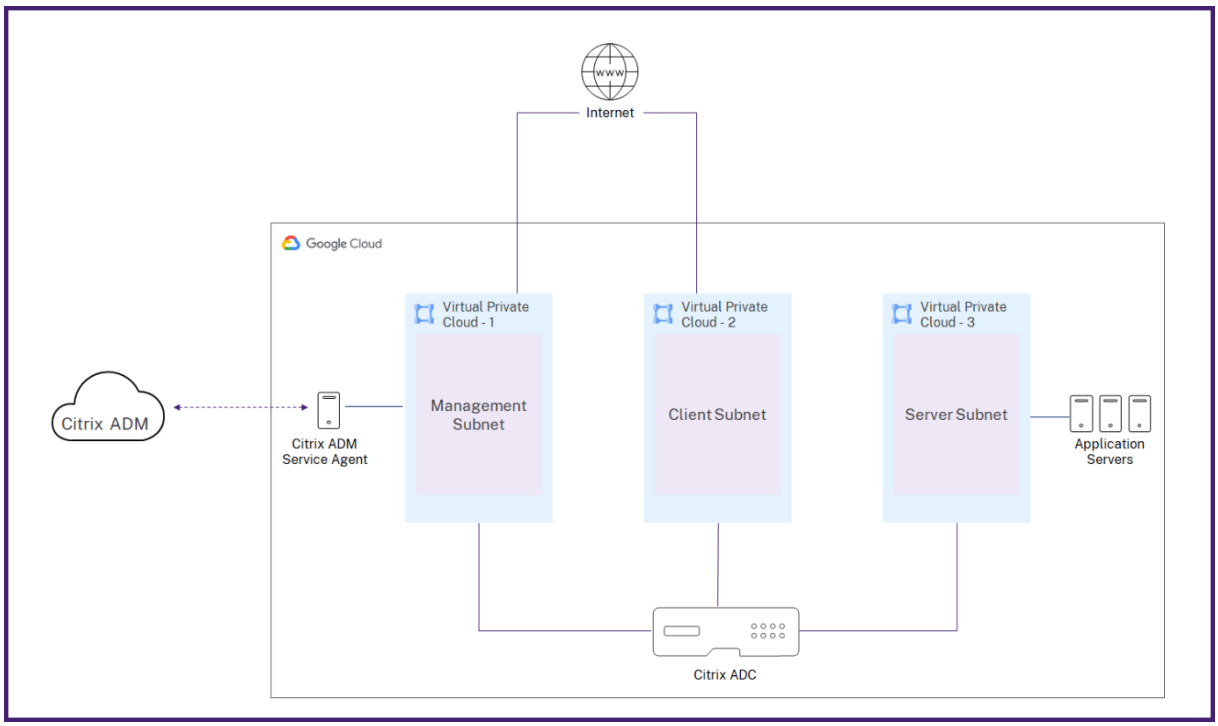
April 28, 2021

Anwendungen oder Dienste, die in Google Cloud gehostet werden, erfordern ein sicheres Verkehrsmanagement und eine effiziente Optimierung der Netzwerkressourcen sowie Cloud-Vorteile. Citrix ADC VPX Instanzen, die in Google Cloud bereitgestellt werden, bieten sicheres Verkehrsmanagement, einen optimierten Ressourcenverbrauch und reduzierte Betriebskosten für Webanwendungen.

Mit Citrix ADM können Sie die Bereitstellung, Einrichtung und Verwaltung der ADC VPX-Instanzen in Google Cloud automatisieren. Die Provisioning von Citrix ADC VPX Instanzen mit ADM kombiniert die Elastizität und Flexibilität der Cloud mit den Steuerungsfunktionen von Citrix ADC.

Citrix ADM Bereitstellungsarchitektur

Das folgende Bild gibt einen Überblick darüber, wie Citrix ADM eine Verbindung mit Google Cloud herstellt, um Citrix ADC VPX-Instanzen in Google Cloud bereitzustellen.



Sie benötigen drei Virtual Private Cloud (VPC) -Netzwerke, um die Citrix ADC VPX Instanz in Google Cloud bereitzustellen und zu verwalten. Ein VPC-Netzwerk enthält ein Subnetz und eine Firewall. Die Firewall verfügt über Regeln, die den ein- und ausgehenden Datenverkehr in ein Subnetz regeln.

Der Citrix ADM Service Agent hilft Ihnen bei der Bereitstellung und Verwaltung der Citrix ADC VPX Instanz.

Voraussetzungen

In diesem Abschnitt werden die Voraussetzungen beschrieben, die Sie in Google Cloud und Citrix ADM erfüllen müssen, bevor Sie Citrix ADC VPX-Instanzen bereitstellen.

In diesem Dokument wird davon ausgegangen, dass Sie ein Google Cloud-Konto besitzen. Weitere Informationen zum Erstellen eines Kontos finden Sie unter Google Cloud-Dokumentation.

Einrichten von Google Cloud-Komponenten

Bevor Sie Citrix ADC VPX-Instanzen in Citrix ADM bereitstellen, führen Sie die folgenden Aufgaben in Google Cloud aus:

1. Aktivieren von APIs
2. Erstellen Sie ein Dienstkonto
3. Erstellen Sie ein VPC-Netzwerk
4. Erstellen Sie eine Firewall
5. Abonnieren Sie die Citrix ADC VPX Lizenz in Google Cloud

Aktivieren von APIs

Citrix ADM benötigt einen programmatischen Zugriff, um die erforderlichen Ressourcen in Google Cloud bereitzustellen und bereitzustellen. Aktivieren Sie daher die folgenden APIs in Ihrem Google Cloud-Projekt:

- Compute Engine-API
- Cloud-DNS-API

Weitere Informationen zum Aktivieren von APIs in Google Cloud finden Sie unter Aktivieren von APIs.

Erstellen Sie ein Dienstkonto

Der ADM verwendet ein Dienstkonto, um auf Ihre Google Cloud-Ressourcen zuzugreifen. Führen Sie die folgenden Schritte aus, um ein Dienstkonto zu erstellen:

1. Melden Sie sich bei Ihrem Google Cloud-Konto an.
2. Gehen Sie zu **IAM & Admin > Dienstkonten**.
3. Klicken Sie auf **+CREATE SERVICE ACCOUNT**

   Erstellen Sie zwei Dienstkonten, ein Dienstkonto wird für ADM verwendet. Und ein anderer wird für ADC-Instanzen verwendet. Führen Sie die folgenden Schritte aus, um ein Dienstkonto zu erstellen.

   a) Geben Sie den Namen, die ID und die Beschreibung an und klicken Sie auf Erstellen.

   b) Weisen Sie die folgenden vordefinierten Rollen zu:

   - Für ADM erforderliche IAM-Rollen

   ```
   roles/iam.serviceAccountUser
   roles/compute.instanceAdmin.v1
   roles/compute.networkAdmin
   roles/dns.admin
   <!--NeedCopy-->
   ```

   - IAM-Rollen, die für die von ADM erstellten ADC-Instanzen erforderlich sind:

   ```
   roles/compute.instanceAdmin.v1
   roles/compute.networkAdmin
   <!--NeedCopy-->
   ```

   Diese Rollen ermöglichen Ihrem Dienstkonto den Zugriff auf Google Cloud-Ressourcen.

   c) Klicken Sie auf **Fertig**.

Erstellen Sie ein VPC-Netzwerk

Erstellen Sie drei Subnetze in Ihrem VPC-Netzwerk - jeweils eines für die Management-, Client- und Serververbindungen. Wählen Sie die benutzerdefinierte Option zum Erstellen eines Subnetzes aus. Geben Sie einen Adressbereich für jedes der Subnetze an. Geben Sie die Region an, in der sich das Subnetz befinden soll.

- **Management**: Ein Subnetz in Ihrem Management-VPC-Netzwerk für die Verwaltung. Citrix ADC muss sich an Google Cloud-Dienste wenden und erfordert einen Internetzugang.
- **Client**: Ein Subnetz in Ihrem Client-VPC-Netzwerk, das für die Clientseite vorgesehen ist. In der Regel empfängt Citrix ADC Clientdatenverkehr für die Anwendung über ein öffentliches Subnetz aus dem Internet.
- **Server**: Ein Subnetz, in dem die Anwendungsserver bereitgestellt werden. Alle Ihre Anwendungsserver sind in diesem Subnetz vorhanden und empfangen Anwendungsdatenverkehr vom Citrix ADC über dieses Subnetz. Weitere Informationen zum Erstellen eines Subnetzes in Google Cloud finden Sie unter VPC-Netzwerkübersicht.

Erstellen Sie eine Firewall

Die Firewall verfügt über Regeln, die den ein- und ausgehenden Datenverkehr in der Citrix ADC VPX-Instanz steuern. Sie können beliebig viele Regeln hinzufügen. Um Citrix ADC-Instanzen automatisch zu skalieren, müssen Sie drei Firewalls erstellen:

- **Management**: Eine Firewall ist für die Verwaltung von Citrix ADC VPX vorgesehen. Citrix ADC muss sich an Google Cloud-Dienste wenden und erfordert einen Internetzugang. Eingehende Regeln sind für die folgenden TCP- und UDP-Ports zulässig.
  - TCP: 80, 22, 443, 3008—3011, 4001, 27000, 7279
  - UDP: 67, 123, 161, 500, 3003, 4500, 7000

  > **Hinweis Stellen Sie**
  >
  > sicher, dass die Firewall dem Citrix ADM-Agenten den Zugriff auf den VPX ermöglicht.

- **Client**: Eine Firewall ist für die clientseitige Kommunikation von Citrix ADC VPX-Instanzen vorgesehen. In der Regel sind eingehende Regeln für die TCP-Ports 80, 22 und 443 zulässig.
- **Server**: Eine Firewall ist für die serverseitige Kommunikation von Citrix ADC VPX vorgesehen. Weitere Informationen zum Erstellen einer Firewall in Google Cloud finden Sie unter VPC-Firewall-Regeln — Überblick.

Abonnieren Sie die Citrix ADC VPX Lizenz in Google Cloud

1. Melden Sie sich bei Ihrem Google Cloud-Portal an

2. Suchen Sie in **Marketplace**nach Citrix ADC und wählen Sie die gewünschte Produktversion aus.
3. Wählen Sie einen der folgenden Lizenztypen aus:
    - Kunde lizenziert
    - Enterprise
    - Platinum

    > **Hinweis**
    >
    > Wenn Sie die Option **Kundenlizenziert** auswählen, checkt die Autoscale-Gruppe die Lizenzen aus dem Citrix ADM aus, während Sie Citrix ADC-Instanzen bereitstellen.

Einrichten von Citrix ADM Komponenten

Bevor Sie Citrix ADC VPX-Instanzen in Citrix ADM bereitstellen, führen Sie die folgenden Aufgaben in Citrix ADM aus:

1. Erstellen einer Site.
2. Bereitstellen eines Citrix ADM-Agenten in Google Cloud.
3. Anfügen der Site an einen Citrix ADM Dienstagenten.

Erstellen einer Site

Erstellen Sie eine Website in Citrix ADM und fügen Sie die mit Ihrer Google Cloud verknüpften VNet-Details hinzu.

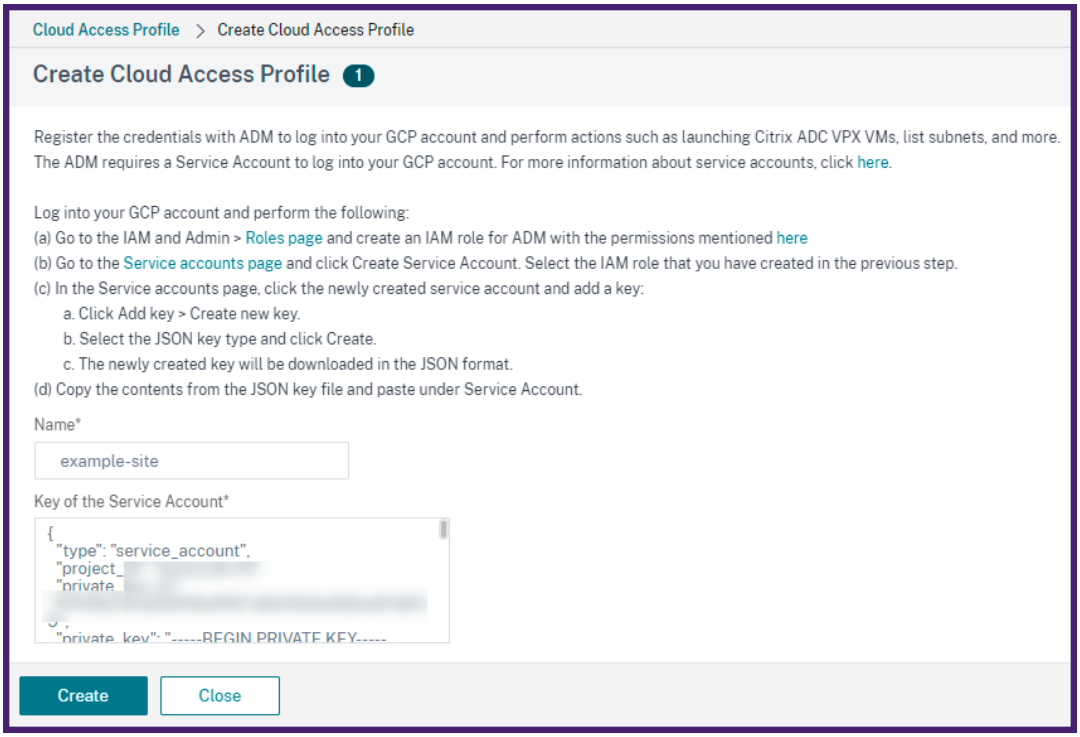
1. Navigieren Sie in Citrix ADM zu **Netzwerke > Sites**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie im Bereich **Cloud auswählen**
    a) Wählen Sie **Datencenter** als Standorttyp aus.
    b) Wählen Sie **Google Cloud** aus der Liste Typ aus.
    c) Aktivieren Sie das Kontrollkästchen **Regionen aus der Google Cloud abrufen**.

    Mit dieser Option können Sie die vorhandenen Regionsinformationen aus Ihrem Google Cloud-Konto abrufen.

    d) Klicken Sie auf **Weiter**.
4. **Wählen Sie im Bereich Region auswählen**
    a) Wählen Sie in **Cloud Access Profile**das für Ihr Google Cloud-Konto erstellte Profil aus. Wenn keine Profile vorhanden sind, erstellen Sie ein Profil.
    b) Klicken Sie auf **Hinzufügen**, um ein Cloud-Zugriffsprofil zu erstellen.

c) Geben Sie **unter Name**einen Namen an, um Ihr Google Cloud-Konto in Citrix ADM zu identifizieren.

d) Geben Sie unter **Schlüssel des Dienstkontos**das in Google Cloud erstellte Dienstkonto an, das JSON erstellt hat.



e) Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Erstellen Sie ein Dienstkonto.

f) Wählen Sie unter **Regionen**die Region aus, die das VPC-Netzwerk enthält, das Citrix ADC VPX-Instanzen enthält, die Sie verwalten möchten.

g) Geben Sie einen **Standortnamen** an.

h) Klicken Sie auf **Fertig stellen**.

Bereitstellen eines Citrix ADM-Agenten in Google Cloud

Der Citrix ADM-Dienst-Agent arbeitet als Vermittler zwischen Citrix ADM und den erkannten Instanzen im Rechenzentrum oder in der Cloud.

1. Navigieren Sie zu **Netzwerke > Agents**.
2. Klicken Sie auf **Bereitstellen**.
3. Wählen Sie **Google Cloud** aus und klicken Sie auf **Weiter**.
4. Geben Sie auf der Registerkarte **Bereitstellungsparameter** Folgendes an:

- **Name**: Geben Sie den Namen des Citrix ADM Agenten an.
- **Site** - Wählen Sie die Site aus, die Sie für die Bereitstellung eines Agenten und ADC-VPX-Instanzen erstellt haben.
- **Cloud Access-Profil** - Wählen Sie das Cloud-Zugriffsprofil aus der Liste aus.
- **Zone** - Wählen Sie die Zonen aus, in denen Sie die Autoscale-Gruppen erstellen möchten. Abhängig von dem Cloud-Zugriffsprofil, das Sie ausgewählt haben, werden die Zonen dieses Profils ausgefüllt.
- **Netzwerk**- Wählen Sie das VPC-Netzwerk aus, in dem Sie Autoscale-Gruppen erstellen möchten.
- **Subnet** - Wählen Sie das Management-Subnetz aus, um einen Agenten bereitzustellen.
- **Tags** - Geben Sie das Schlüssel-Wert-Paar für die Autoscale Gruppentags ein. Ein Tag besteht aus einem Schlüssel-Wert-Paar, das zwischen Groß- und Kleinschreibung unterschieden wird. Diese Tags ermöglichen es Ihnen, die Autoskalierungsgruppen einfach zu organisieren und zu identifizieren. Die Tags werden sowohl auf Google Cloud als auch auf Citrix ADM angewendet.

5. Klicken Sie auf **Fertig stellen**.

Alternativ können Sie den Citrix ADM Agent aus dem Google Cloud Marketplace installieren. Weitere Informationen finden Sie unter Installieren eines Citrix ADM-Agenten in der Google Cloud.

Anfügen der Site an einen Citrix ADM Dienstagenten

1. Navigieren Sie in Citrix ADM zu **Netzwerke > Agenten**.
2. Wählen Sie den Agenten aus, für den Sie eine Site anhängen möchten.
3. Klicken Sie auf **Site anhängen**.
4. Wählen Sie die Website aus der Liste aus, die Sie hinzufügen möchten.
5. Klicken Sie auf **Save**.

Konfigurationsaufgaben

Um eine eigenständige ADC VPX-Instanz in Google Cloud bereitzustellen, führen Sie die folgenden Schritte aus:

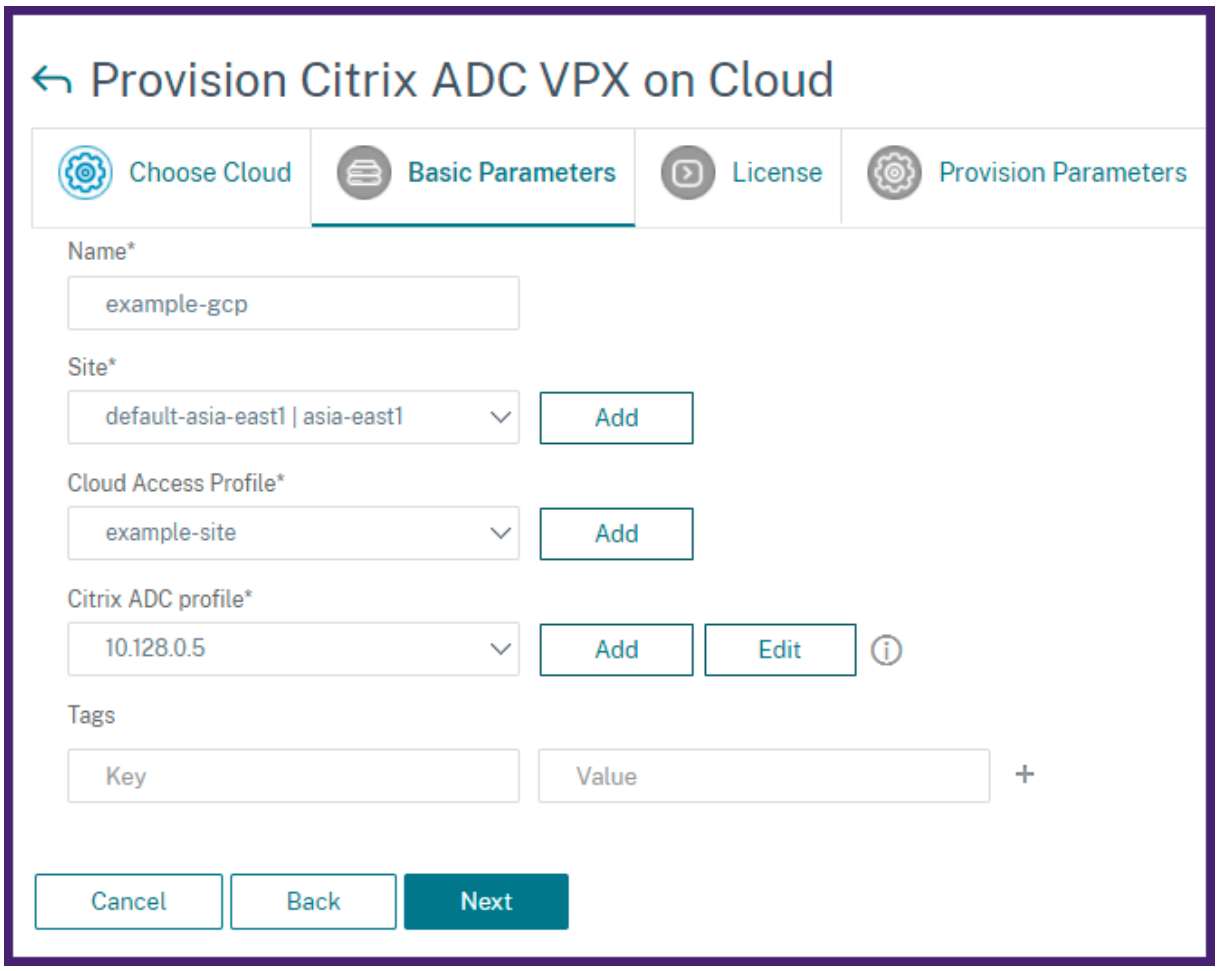
1. Navigieren Sie in Citrix ADM zu **Netzwerke > Instanzen > Citrix ADC**.
2. Klicken Sie auf **Bereitstellen**.
3. Wählen Sie **Google Cloud** aus und klicken Sie auf **Weiter**. Geben Sie die erforderlichen Parameter für die Bereitstellung einer Instanz an.

4. Geben Sie die grundlegende ParameterLizenzen, und an Parameter für die Bereitstellung.

Konfigurieren Sie grundlegende Parameter

1. Geben Sie auf der Registerkarte **Grundparameter** Folgendes an:
   - **Name** - Geben Sie den Namen einer ADC VPX-Instanz an.
   - **Site** — Wählen Sie die Website aus, die Sie zuvor erstellt haben.
   - **Agent** : Wählen Sie den Agenten aus, der zur Verwaltung der Citrix ADC VPX-Instanz erstellt wurde.
   - **Cloud Access-Profil** — Wählen Sie das Cloud-Zugriffsprofil aus, das während der Erstellung der Website erstellt wurde
   - **Citrix ADC Profile** - Wählen Sie das Profil aus, das die Authentifizierung bereitstellen soll.

     Citrix ADM verwendet das Geräteprofil, wenn es sich bei der Citrix ADC VPX Instanz anmelden muss.
2. Klicken Sie auf **Weiter**.



Konfigurieren von Lizenzen

Wählen Sie einen der folgenden Modi aus, um die Lizenz auf eine ADC-Instanz anzuwenden:

- **Verwendung von Citrix ADM**: Die Instanz, die Sie bereitstellen möchten, checkt die Lizenzen vom Citrix ADM aus.
- **Verwendung von Google Cloud**: Die Option " **Aus Cloud zuweisen** " verwendet die im Google Cloud Marketplace verfügbaren Citrix Produktlizenzen. Die Instanz, die Sie bereitstellen möchten, verwendet die Lizenzen des Marketplace.

  Wenn Sie sich für die Verwendung von Lizenzen aus Google Cloud Marketplace entscheiden, geben Sie das Produkt oder die Lizenz auf der Registerkarte **Bereitstellungsparameter** an.

Weitere Informationen finden Sie unter Lizenzanforderungen.

Lizenzen von Citrix ADM verwenden

Um diese Option zu verwenden, stellen Sie sicher, dass Sie das Citrix ADC-Produkt mit dem Plan **Eigene Lizenzsoftware** in Google Cloud abonniert haben. Siehe Abonnieren Sie die Citrix ADC VPX Lizenz in Google Cloud.

1. Wählen Sie auf der Registerkarte **Lizenz** die Option **Aus ADM zuweisen**.
2. Wählen Sie unter **Lizenztyp**eine der folgenden Optionen aus der Liste:
   - **Bandbreitenlizenzen:** Sie können eine der folgenden Optionen aus der Liste **Bandbreitenlizenztypen** auswählen:
     - **Pooled Capacity:** Geben Sie die Kapazität an, die einer Instanz zugewiesen werden soll.

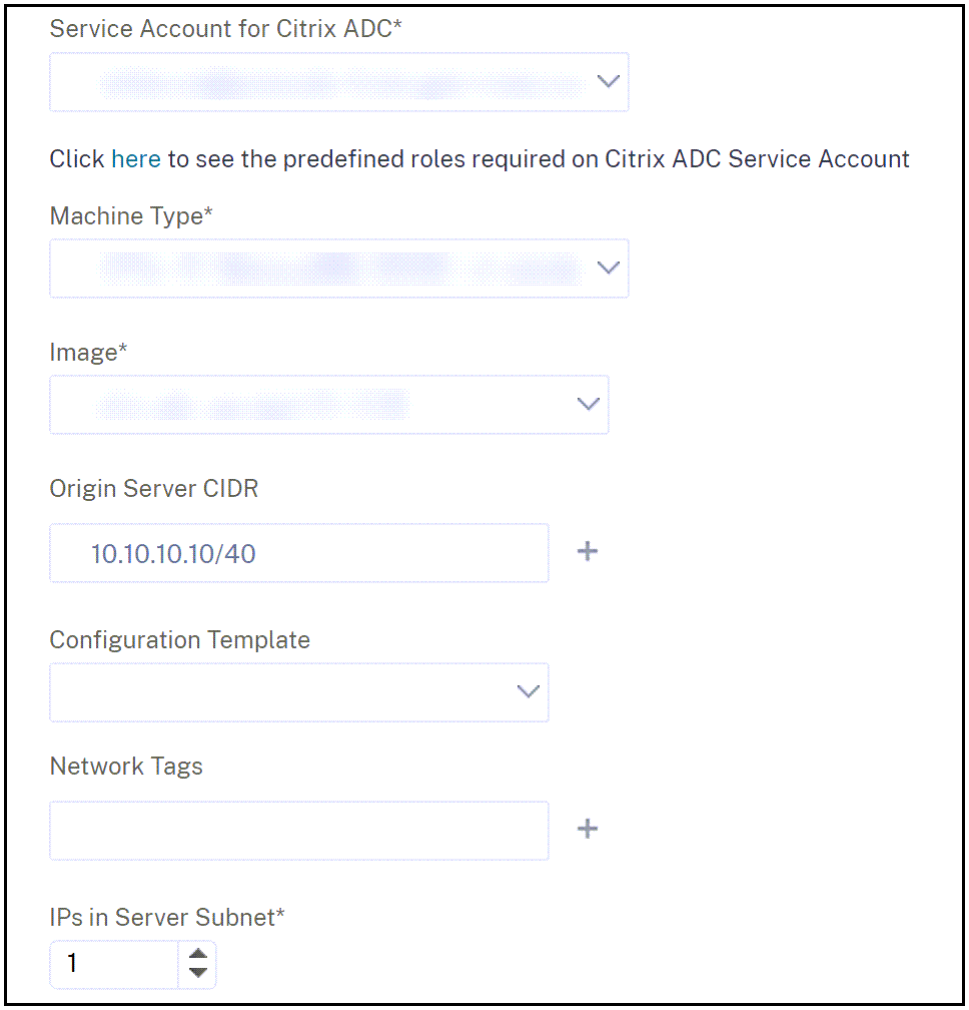
       Aus dem gemeinsamen Pool checkt die ADC-Instanz eine Instanzlizenz aus und nur so viel Bandbreite wird angegeben.
     - **VPX-Lizenzen:** Wenn eine Citrix ADC VPX Instanz bereitgestellt wird, checkt die Instanz die Lizenz vom Citrix ADM aus.
   - **Virtuelle CPU-Lizenzen:** Die bereitgestellte Citrix ADC VPX-Instanz checkt Lizenzen abhängig von der Anzahl der in der Instanz ausgeführten CPUs aus.

   > **Hinweis:**
   >
   > Wenn die bereitgestellten Instanzen entfernt oder gelöscht werden, kehren die angewendeten Lizenzen in den Citrix ADM -Lizenzpool zurück. Diese Lizenzen können wiederverwendet werden, um neue Instanzen bereitzustellen.
3. Wählen Sie in **License Edition** die Lizenzversion aus. Der ADM verwendet die angegebene Edition zur Bereitstellung von Instanzen.
4. Klicken Sie auf **Weiter**.

Konfigurieren von Bereitstellungsparametern

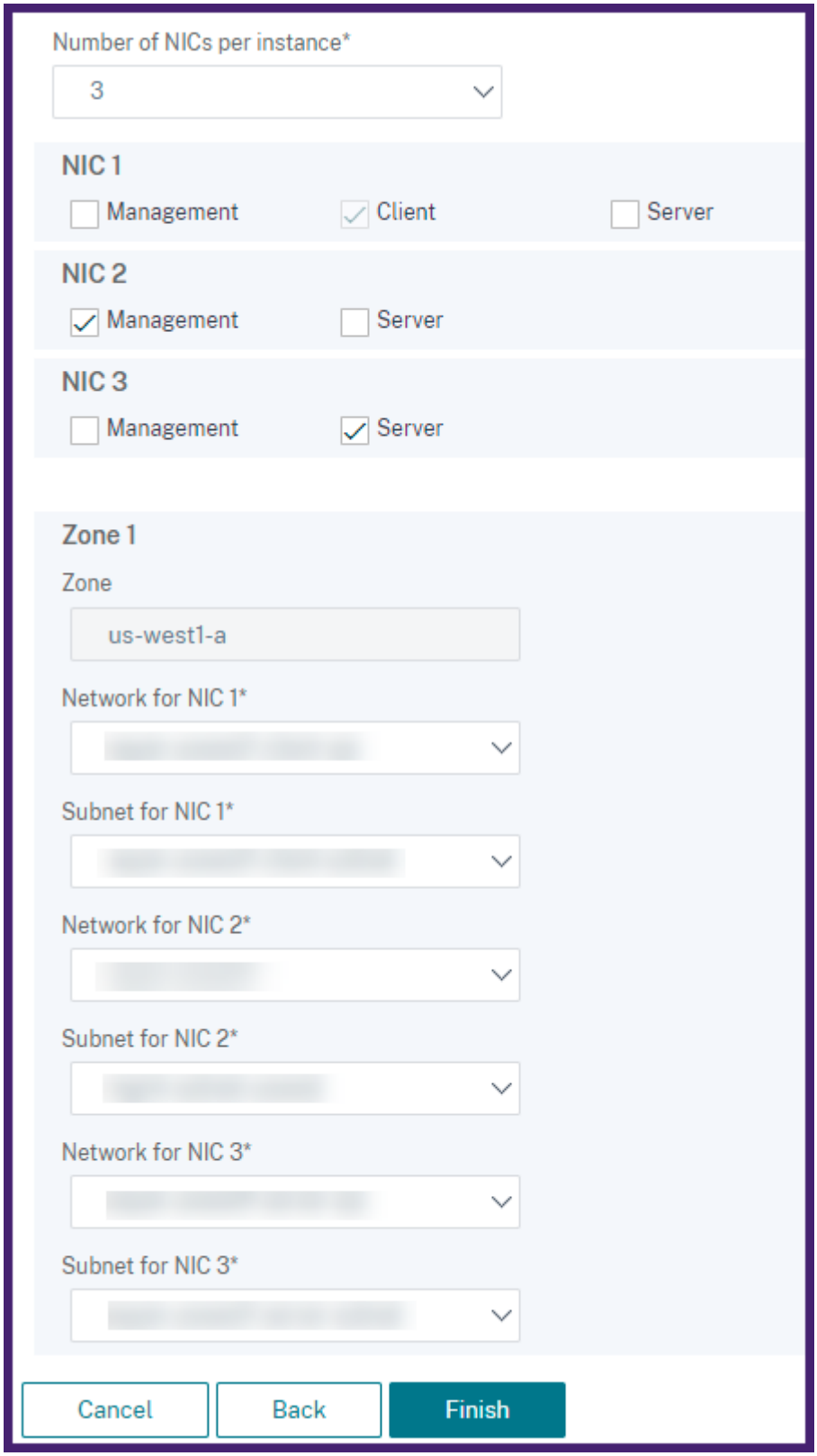
1. Geben Sie auf der Registerkarte **Bereitstellungsparameter** Folgendes an:

   - **ADC-Dienstkonto**: Wählen Sie das Dienstkonto aus, das Sie in Google Cloud erstellt haben. Der ADM verwendet ein Dienstkonto, um auf Ihre Google Cloud-Ressourcen zuzugreifen.
   - **Produkt/ Lizenz**: Wählen Sie die Citrix ADC-Produktversion aus, die Sie bereitstellen möchten. Weitere Informationen finden Sie unter Abonnieren der Citrix ADC VPX-Lizenz in Google Cloud.
   - **Maschinentypen**: Wählen Sie den gewünschten Maschinentyp aus der Liste aus.
   - **Image**: Wählen Sie das erforderliche Citrix ADC-Versionimage aus. Klicken Sie auf Neu hinzufügen, um ein Citrix ADC Image hinzuzufügen.
   - **Konfigurationsvorlage** — Wählen Sie die Konfigurationsvorlage aus, die Sie für die Bereitstellung auf den ADC-Instanzen verwenden möchten.
   - **IPs im Server-Subnetz pro Instanz** — Geben Sie an, wie viele SNIP-Adressen jede Instanz im Serversubnetz haben kann.



Auf dieser Registerkarte können Sie auch die erforderlichen NICs angeben und konfigurieren. Jede NIC enthält eine dedizierte Firewall und ein Subnetz.

Weitere Informationen finden Sie unter Erstellen Sie ein VPC-Netzwerk und Erstellen Sie eine Firewall.



2. Klicken Sie auf **Fertig stellen**.

Anzeigen der bereitgestellten Citrix ADC VPX Instanzen

So zeigen Sie Citrix ADM an:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Wählen Sie die Registerkarte **Citrix ADC VPX** aus.

   Die in Google Cloud bereitgestellte Citrix ADC VPX Instanz ist hier aufgelistet.

So zeigen Sie in Google Cloud an:

1. Melden Sie sich bei Ihrem Google Cloud-Portal an
2. Navigieren Sie zu der Registerkarte **Ressourcen**, auf der die bereitgestellte Citrix ADC VPX-Instanz angezeigt wird.

> **Hinweis**
>
> Der Name der Citrix ADC VPX-Instanz ist derselbe, den Sie beim Provisioning einer Instanz im Citrix ADM angegeben haben.

Autoskalierung von Citrix ADC VPX in Google Cloud mit Citrix ADM

April 28, 2021

Autoscaling ist eine Cloud-Computing-Methode, die automatisch Ressourcen in Abhängigkeit von der tatsächlichen Nutzung hinzufügt oder entfernt. Die automatische Skalierung ist nützlich, wenn Ihre Website oder Anwendung eine Ressourcenzuweisung auf Anforderung benötigt, um die schwankende Anzahl von Clientanforderungen oder Verarbeitungsaufträgen zu erfüllen.

Die Nachfrage nach Webanwendungen oder -diensten kann erheblich variieren. Die korrekte Anzahl von Citrix ADC-Instanzen für die unterschiedlichen Datenverkehrsanforderungen ist wichtig. Je nach Bedarf können Sie die Netzwerkressourcen in Google Cloud erhöhen oder verringern. So bietet es Kostenoptimierung, ohne die Leistung zu beeinträchtigen.
Bei der automatischen Skalierung von Citrix Application Delivery Management (ADM) wird die genaue Anzahl von Citrix ADC-Instanzen für den schwankenden Ressourcenverbrauch beibehalten. Citrix ADM bestimmt den Datenfluss basierend auf dem schwankenden Ressourcenverbrauch. Es entscheidet, in Citrix ADC-Instanzen dynamisch zu skalieren oder zu skalieren. Somit bietet es Ihnen die Flexibilität, die korrekte Anzahl von Citrix ADC-Instanzen beizubehalten.

Citrix ADM überwacht die Ressourcennutzung von Citrix ADC-Instanzen und stimmt mit dem konfigurierten Schwellenwert überein. Es löst die Scale-Out-Aktion aus, wenn eine der konfigurierten Ressourcen den angegebenen Schwellenwert überschreitet.

Citrix ADM löst die Aktion Skalieren nur aus, wenn die Verwendung aller konfigurierten Ressourcen unter den normalen Schwellenwert fällt.

> **Wichtig**
>
> Autoscaling unterstützt alle Citrix ADC Funktionen mit Ausnahme der folgenden Funktionen, die eine gepunktete Konfiguration auf Clusterknoten erfordern:
>
> - GSLB
> - Citrix Gateway und seine Funktionen
> - Telco-Funktionen
>
> Weitere Informationen zur Spotted-Konfiguration finden Sie unter Striped-, Teil-Striped- und Spotted-Konfigurationen.

Vorteile

Hohe Verfügbarkeit von Anwendungen: Autoscaling stellt sicher, dass Ihre Anwendung immer über die richtige Anzahl von Citrix ADC VPX Instanzen verfügt, um die Datenverkehrsanforderungen zu bewältigen. Es stellt sicher, dass Ihre Anwendung ständig einsatzbereit ist und ausgeführt wird, unabhängig von den Anforderungen des Datenverkehrs.

Intelligente Skalierungsentscheidungen und Zero-Touch-Konfiguration: Autoscaling überwacht Ihre Anwendung kontinuierlich und fügt Citrix ADC-Instanzen dynamisch je nach Bedarf hinzu oder entfernt sie. Die Instanzen werden automatisch hinzugefügt, wenn der Bedarf für einen bestimmten Zeitraum erhöht wird. Die Instanzen werden automatisch entfernt, wenn der Bedarf für einen bestimmten Zeitraum verringert wird. Das Hinzufügen und Entfernen von Citrix ADC-Instanzen erfolgt automatisch und macht es zu einer manuellen Null-Touch-Konfiguration.

Automatische DNS-Verwaltung: Die Citrix ADM Autoscale-Funktion bietet eine automatische DNS-Verwaltung. Wenn neue Citrix ADC-Instanzen hinzugefügt werden, werden die Domänennamen automatisch aktualisiert.

Ordnungsgemäße Verbindungsbeendigung: Während eines Scale-Ins werden die Citrix ADC-Instanzen ordnungsgemäß entfernt, wodurch der Verlust von Clientverbindungen vermieden wird.

Besseres Kostenmanagement: Die automatische Skalierung erhöht oder verringert Citrix ADC-Instanzen bei Bedarf dynamisch. Mit dieser Methode können Sie die damit verbundenen Kosten optimieren. Wenn Sie Instanzen nur dann starten, wenn sie benötigt werden, und sie beenden, wenn sie nicht benötigt werden, reduziert sich die Betriebskosten. So zahlen Sie nur für die Ressourcen, die Sie verwenden.

Beobachtbarkeit: Beobachtbarkeit ist der Schlüssel für Anwendungsdev-ops oder IT-Personal, um den Zustand der Anwendung zu überwachen. Das Dashboard “Autoscale” von Citrix ADM ermöglicht Ihnen die Visualisierung der Schwellwert-Parameterwerte, der Autoscale Trigger-Zeitstempel, der Ereignisse und der Instanzen, die an der Autoscale beteiligt sind.

Lizenzierungsanforderungen

Die Citrix ADC-Instanzen, die für die Citrix Autoscale-Gruppe erstellt werden, verwenden Citrix ADC Advanced- oder Premium ADC-Lizenzen. Citrix ADC Clustering-Funktion ist in Advanced- oder Premium ADC-Lizenzen enthalten.

Sie können eine der folgenden Methoden wählen, um Citrix ADCs zu lizenzieren, die von Citrix ADM bereitgestellt werden:

- **Verwenden von ADC-Lizenzen in Citrix ADM**: Konfigurieren Sie gepoolte Kapazität, VPX-Lizenzen oder virtuelle CPU-Lizenzen, während Sie die Autoscale-Gruppe erstellen. Wenn also eine neue Instanz für die Autoscale-Gruppe bereitgestellt wird, wird der bereits konfigurierte Lizenztyp automatisch auf die bereitgestellte Instanz angewendet.
  - **Pooled Capacity**: Stellt jeder bereitgestellten Instanz in der Autoscale-Gruppe Bandbreite zu. Stellen Sie sicher, dass in Citrix ADM die erforderliche Bandbreite zur Verfügung steht, um neue Instanzen bereitzustellen. Weitere Informationen finden Sie unter Konfiguration der gepoolten Kapazität.

    Jede ADC-Instanz in der Gruppe Autoscale checkt eine Instanzlizenz und die angegebene Bandbreite aus dem Pool aus.
  - **VPX-Lizenzen**: Wendet die VPX-Lizenzen auf neu bereitgestellte Instanzen an. Stellen Sie sicher, dass Sie über die erforderliche Anzahl von VPX-Lizenzen in Citrix ADM verfügen, um neue Instanzen bereitzustellen.

    Wenn eine Citrix ADC VPX Instanz bereitgestellt wird, checkt die Instanz die Lizenz vom Citrix ADM aus. Weitere Informationen finden Sie unter Citrix ADC VPX Check-In and Check-out-Lizenzierung.
  - Virtuelle CPU-Lizenzen: Wendet virtuelle CPU-Lizenzen auf neu bereitgestellte Instanzen an. Diese Lizenz gibt die Anzahl der CPUs an, die für eine Citrix ADC VPX Instanz berechtigt sind. Stellen Sie sicher, dass Sie über die erforderliche Anzahl von virtuellen CPUs in Citrix ADM verfügen, um neue Instanzen bereitzustellen.

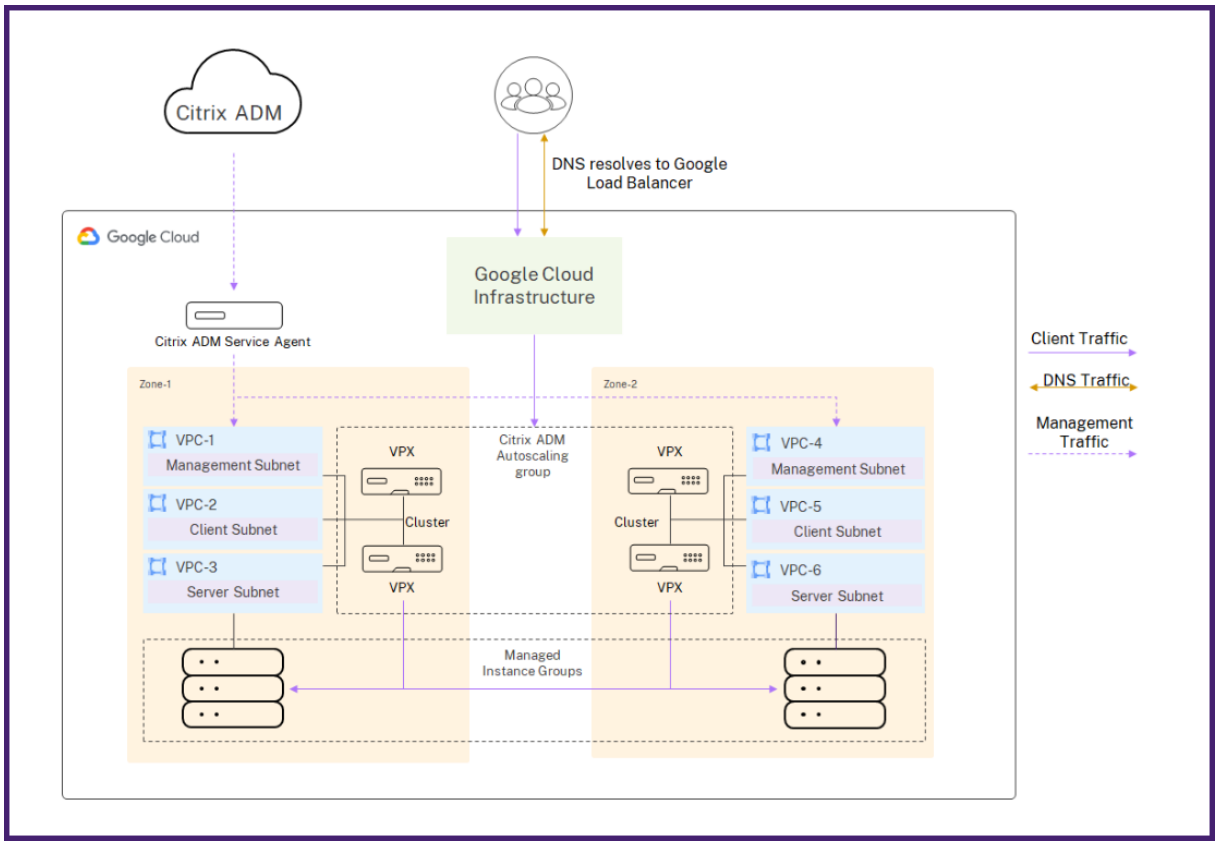
  Wenn eine Citrix ADC VPX Instanz bereitgestellt wird, checkt die Instanz die virtuelle CPU-Lizenz vom Citrix ADM aus. Weitere Informationen finden Sie unter Citrix ADC Virtual CPU-Lizenzierung.

  Wenn die bereitgestellten Instanzen zerstört oder die Bereitstellung aufgehoben werden, werden die angewendeten Lizenzen automatisch an Citrix ADM zurückgegeben.

  Um die verbrauchten Lizenzen zu überwachen, navigieren Sie zur Seite **Netzwerke > Lizenzen**.
- **Verwenden von Google Cloud-Abonnementlizenzen**: Konfigurieren Sie Citrix ADC-Lizenzen, die in Google Marketplace verfügbar sind, während Sie die Autoscale-Gruppe erstellen. Wenn also eine neue Instanz für die Autoscale-Gruppe bereitgestellt wird, wird die Lizenz von Google Marketplace bezogen.

Architektur

Citrix ADM behandelt die Verteilung des Client-Datenverkehrs mit Google Network Load Balancer. Das folgende Diagramm zeigt, wie die Autoskalierung mit dem Google Network Load Balancer als Traffic-Distributor erfolgt:



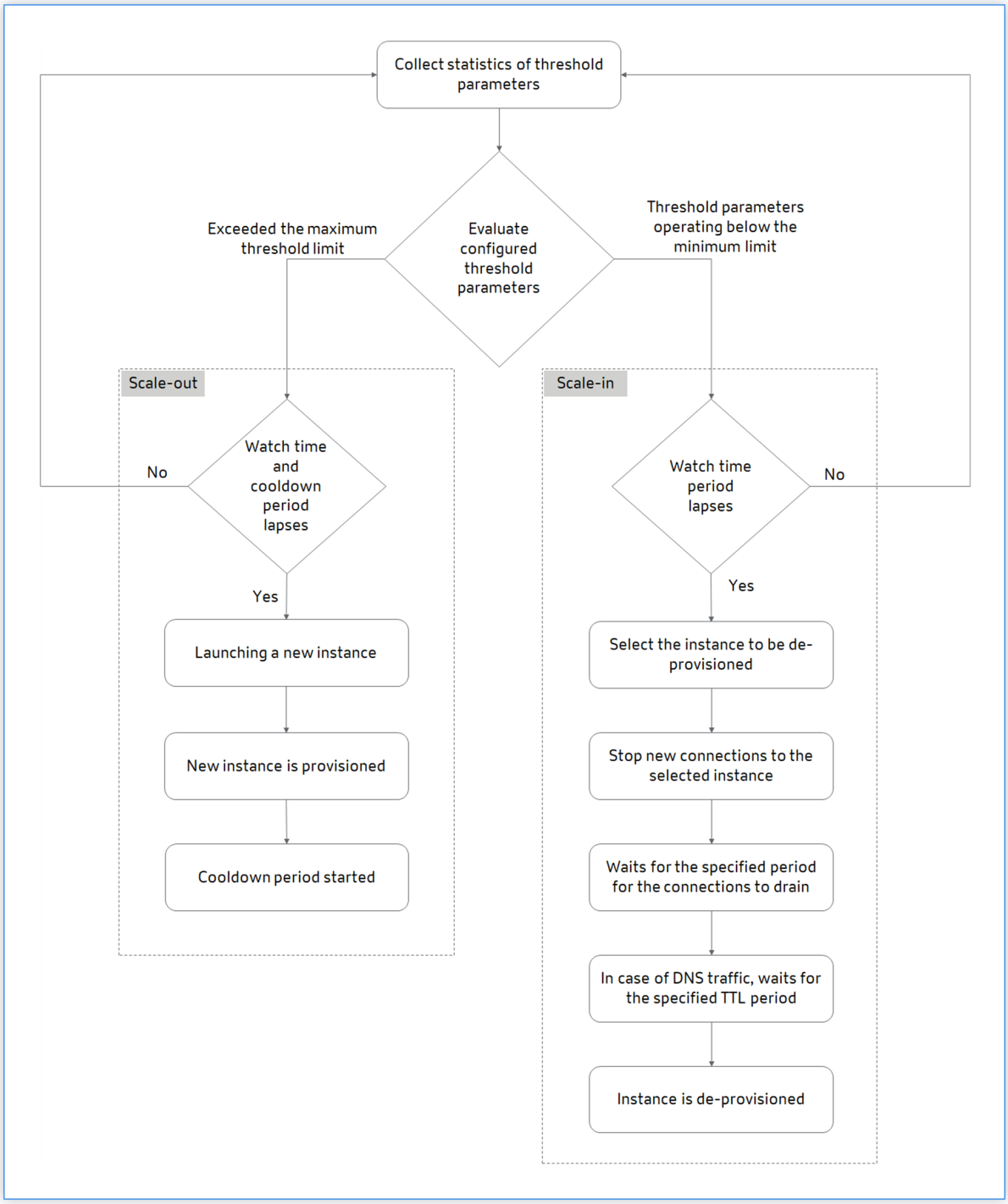
Google Network Load Balancer ist die Verteilungsebene zu den Clusterknoten. Network Load Balancer verwaltet den Clientdatenverkehr und verteilt ihn an Citrix ADC VPX Cluster. Network Load Balancer sendet den Clientdatenverkehr an Citrix ADC VPX Clusterknoten, die in der Citrix ADM Autoscaling Gruppe über Zonen verfügbar sind.

Citrix ADM löst die Scale-Out- oder Scale-In-Aktion auf Clusterebene aus. Wenn ein Scale-Out ausgelöst wird, werden die registrierten virtuellen Maschinen bereitgestellt und dem Cluster hinzugefügt. Wenn ein Scale-In ausgelöst wird, werden die Knoten entfernt und aus den Citrix ADC VPX Clustern entfernt.

Die Citrix ADM Autoscale-Gruppe ist eine Gruppe von Citrix ADC-Instanzen, die Anwendungen als einzelne Entität ausgleichen und basierend auf den konfigurierten Schwellenwert-Parameterwerten Autoscaling auslösen.

So funktioniert die automatische Skalierung

Das folgende Flussdiagramm veranschaulicht den automatischen Skalierungsworkflow:



Citrix ADM sammelt die Statistiken (CPU, Arbeitsspeicher und Durchsatz) aus den bereitgestellten Clustern für jede Minute.

Die Statistiken werden anhand der Konfigurationsschwellenwerte ausgewertet. Abhängig von der

Statistik wird die Skalierung oder die Skalierung in ausgelöst. Scale-out wird ausgelöst, wenn die Statistik den maximalen Schwellenwert überschreitet. Scale-In wird ausgelöst, wenn die Statistiken unter dem Mindestschwellenwert arbeiten.

Wenn ein Scale-Out ausgelöst wird:

1. Neuer Knoten wird bereitgestellt.
2. Der Knoten ist mit dem Cluster verbunden und die Konfiguration wird vom Cluster mit dem neuen Knoten synchronisiert.
3. Der Knoten ist bei Citrix ADM registriert.
4. Die neuen Knoten-IP-Adressen werden im Google Network Load Balancer aktualisiert.

Wenn ein Scale-In ausgelöst wird:

1. Der Knoten wird identifiziert, der entfernt werden soll.
2. Stoppen Sie neue Verbindungen zum ausgewählten Knoten.
3. Der Knoten wird vom Cluster getrennt, von Citrix ADM abgemeldet und dann von Google Cloud nicht bereitgestellt.

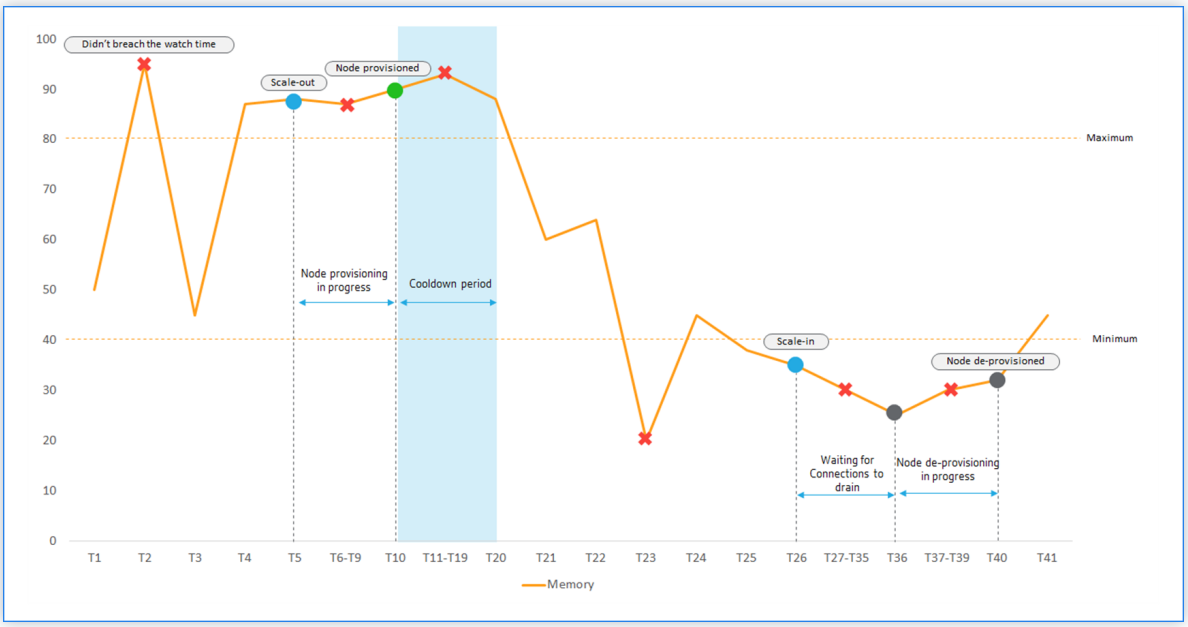
> **Hinweis**
>
> Wenn die Anwendung bereitgestellt wird, wird ein IP-Satz auf Clustern in jeder Availability Zone erstellt. Dann werden die E-Mail-Adressen der Domäne und der Instanz beim Google Network Load Balancer registriert. Wenn die Anwendung entfernt wird, werden die IP-Adresse der Domäne und der Instanz vom Google Network Load Balancer abgemeldet. Dann wird der IP-Satz gelöscht.

Beispiel für die automatische Skalierung

Beachten Sie, dass Sie eine Autoscale-Gruppe mit dem Namen asg_arn in einer einzelnen Availability Zone mit der folgenden Konfiguration erstellt haben.

- Ausgewählte Schwellenwertparameter — Speicherbelegung.
- Schwellenwert auf Speicher festgelegt:
  - Mindestgrenze: 40
  - Höchstgrenze: 85
- Wiedergabezeit: 2 Minuten.
- Abklingzeit — 10 Minuten.
- Wartezeit während der De-Bereitstellung — 10 Minuten.
- DNS-Zeit bis zum Leben — 10 Sekunden.

Nachdem die Gruppe “Autoscale” erstellt wurde, werden Statistiken aus der Gruppe “Autoscale” gesammelt. Die Richtlinie “Automatische Skalierung” wertet auch aus, ob ein Ereignis für die automatische Skalierung ausgeführt wird. Wenn die automatische Skalierung ausgeführt wird, warten Sie, bis dieses Ereignis abgeschlossen ist, bevor Sie die Statistiken sammeln.



Die Reihenfolge der Ereignisse

1. Die Speichernutzung überschreitet den Schwellenwert bei **T2**. Das Scale-Out wird jedoch nicht ausgelöst, da es für die angegebene Wiedergabezeit nicht verletzt wurde.
2. Scale-Out wird bei **T5** ausgelöst, nachdem ein Maximalschwellenwert für 2 Minuten (Wiedergabezeit) kontinuierlich überschritten wurde.
3. Für den Verstoß zwischen **T5-T10** wurden keine Maßnahmen ergriffen, da Knotenprovisioning ausgeführt wird.
4. Der Knoten wird bei **T10** bereitgestellt und dem Cluster hinzugefügt. Die Abklingzeit wurde gestartet.
5. Wegen der Abklingzeit wurden keine Maßnahmen für die Verletzung zwischen **T10-T20** ergriffen. Dieser Zeitraum sorgt für den organischen Anbau von Instanzen einer Autoscale-Gruppe. Bevor die nächste Skalierungsentscheidung ausgelöst wird, wird darauf gewartet, dass sich der aktuelle Datenverkehr stabilisiert und auf den aktuellen Satz von Instanzen durchdurchschnittlich wird.
6. Die Speichernutzung unterschreitet den Mindestschwellenwert bei **T23**. Das Scale-In wird jedoch nicht ausgelöst, da es für die angegebene Wiedergabezeit nicht verletzt wurde.

7. Scale-In wird bei **T26** ausgelöst, nachdem der Mindestschwellenwert für 2 Minuten (Wiedergabezeit) kontinuierlich überschritten wurde. Ein Knoten im Cluster wird für die Aufhebung der Bereitstellung identifiziert.
8. Für den Verstoß zwischen **T26-T36** wurden keine Maßnahmen ergriffen, da Citrix ADM darauf wartet, vorhandene Verbindungen zu entleeren. Bei der DNS-basierten Autoskalierung ist TTL wirksam.

   > **Hinweis:**
   >
   > Bei DNS-basierter Autoskalierung wartet Citrix ADM auf den angegebenen Time-To-Live (TTL) -Zeitraum. Anschließend wartet es, bis vorhandene Verbindungen abgeleitet werden, bevor die Node-Bereitstellung initiiert wird.

9. Für den Verstoß zwischen **T37-T39** wurden keine Maßnahmen ergriffen, da die Node-Bereitstellung ausgeführt wird.
10. Der Knoten wird entfernt und bei **T40** aus dem Cluster entfernt.

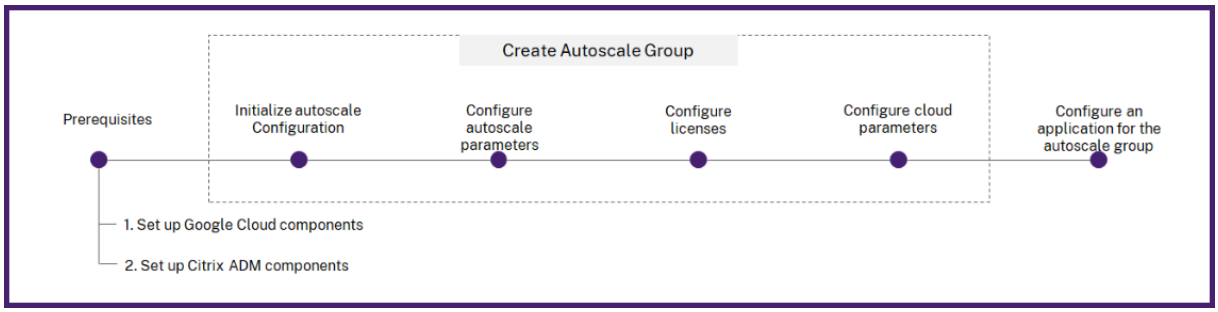
Alle Verbindungen zum ausgewählten Knoten wurden entleert, bevor die Node-Bereitstellung initiiert wurde. Daher wird die Abklingzeit übersprungen, nachdem das Provisioning des Knotens aufgehoben wurde.

Konfiguration

April 28, 2021

Citrix ADM verwaltet alle Citrix ADC VPX-Cluster in Google Cloud. Citrix ADM greift über das Cloud Access-Profil auf die Google Cloud-Ressourcen zu.

Das folgende Flussdiagramm erklärt die Schritte beim Erstellen und Konfigurieren einer Autoscale-Gruppe:



Voraussetzungen

In diesem Abschnitt werden die Voraussetzungen beschrieben, die Sie in Google Cloud und Citrix ADM erfüllen müssen, bevor Sie Citrix ADC VPX-Instanzen von Autoscale erstellen.

In diesem Dokument wird davon ausgegangen, dass Sie ein Google Cloud-Konto besitzen. Weitere Informationen zum Erstellen eines Kontos finden Sie unter Google Cloud-Dokumentation.

Einrichten von Google Cloud-Komponenten

Bevor Sie Citrix ADC VPX-Instanzen in Citrix ADM bereitstellen, führen Sie die folgenden Aufgaben in Google Cloud aus:

1. Aktivieren von APIs
2. Erstellen Sie ein Dienstkonto
3. Erstellen Sie ein VPC-Netzwerk
4. Erstellen Sie eine Firewall

Aktivieren von APIs

Citrix ADM benötigt einen programmatischen Zugriff, um die erforderlichen Ressourcen in Google Cloud bereitzustellen und bereitzustellen. Aktivieren Sie daher die folgenden APIs in Ihrem Google Cloud-Projekt:

- Compute Engine-API
- Cloud-DNS-API

Weitere Informationen zum Aktivieren von APIs in Google Cloud finden Sie unter Aktivieren von APIs.

Erstellen Sie ein Dienstkonto

Der ADM verwendet ein Dienstkonto, um auf Ihre Google Cloud-Ressourcen zuzugreifen. Führen Sie die folgenden Schritte aus, um ein Dienstkonto zu erstellen:

1. Melden Sie sich bei Ihrem Google Cloud-Konto an.
2. Gehen Sie zu **IAM & Admin > Dienstkonten**.
3. Klicken Sie auf **+CREATE SERVICE ACCOUNT**

   Erstellen Sie zwei Dienstkonten, ein Dienstkonto wird für ADM verwendet. Und ein anderer wird für ADC-Instanzen verwendet. Führen Sie die folgenden Schritte aus, um ein Dienstkonto zu erstellen.

   a) Geben Sie den Namen, die ID und die Beschreibung an und klicken Sie auf Erstellen.

   b) Weisen Sie die folgenden vordefinierten Rollen zu:

- Für ADM erforderliche IAM-Rollen

```
roles/iam.serviceAccountUser
roles/compute.instanceAdmin.v1
roles/compute.networkAdmin
roles/dns.admin
<!--NeedCopy-->
```

- IAM-Rollen, die für die von ADM erstellten ADC-Instanzen erforderlich sind:

```
roles/compute.instanceAdmin.v1
roles/compute.networkAdmin
<!--NeedCopy-->
```

Diese Rollen ermöglichen Ihrem Dienstkonto den Zugriff auf Google Cloud-Ressourcen.

c) Klicken Sie auf **Fertig**.

Nachdem Sie ein Dienstkonto erstellt haben, fügen Sie ihm einen Schlüssel hinzu.

1. Wählen Sie das Dienstkonto aus, zu dem Sie einen Schlüssel hinzufügen möchten.
2. Wählen Sie **Schlüssel hinzufügen > Neuen Schlüssel erstellen**aus.
3. Wählen Sie JSON-Schlüsseltyp aus und klicken Sie auf **Erstellen**.

Erstellen Sie ein VPC-Netzwerk

Erstellen Sie drei Subnetze in Ihrem VPC-Netzwerk - jeweils eines für die Management-, Client- und Serververbindungen. Wählen Sie die benutzerdefinierte Option zum Erstellen eines Subnetzes aus. Geben Sie einen Adressbereich für jedes der Subnetze an. Geben Sie die Region an, in der sich das Subnetz befinden soll.

- **Management**: Ein Subnetz in Ihrem Management-VPC-Netzwerk für die Verwaltung. Citrix ADC muss sich an Google Cloud-Dienste wenden und erfordert einen Internetzugang.
- **Client**: Ein Subnetz in Ihrem Client-VPC-Netzwerk, das für die Clientseite vorgesehen ist. In der Regel empfängt Citrix ADC Clientdatenverkehr für die Anwendung über ein öffentliches Subnetz aus dem Internet.
- **Server**: Ein Subnetz, in dem die Anwendungsserver bereitgestellt werden. Alle Ihre Anwendungsserver sind in diesem Subnetz vorhanden und empfangen Anwendungsdatenverkehr vom Citrix ADC über dieses Subnetz. Weitere Informationen zum Erstellen eines Subnetzes in Google Cloud finden Sie unter VPC-Netzwerkübersicht.

Erstellen Sie eine Firewall

Die Firewall verfügt über Regeln, die den ein- und ausgehenden Datenverkehr in der Citrix ADC VPX-Instanz steuern. Sie können beliebig viele Regeln hinzufügen. Um Citrix ADC-Instanzen automatisch zu skalieren, müssen Sie drei Firewalls erstellen:

- **Management**: Eine Firewall ist für die Verwaltung von Citrix ADC VPX vorgesehen. Citrix ADC muss sich an Google Cloud-Dienste wenden und erfordert einen Internetzugang. Eingehende Regeln sind für die folgenden TCP- und UDP-Ports zulässig.
  - TCP: 80, 22, 443, 3008—3011, 4001, 27000, 7279
  - UDP: 67, 123, 161, 500, 3003, 4500, 7000

  Konfigurieren Sie Cloud NAT, um den Internetzugriff von diesem Subnetz aus zu ermöglichen. Weitere Informationen finden Sie unter Verwenden von Cloud NAT.

  > **Hinweis Stellen Sie**
  >
  > sicher, dass die Firewall dem Citrix ADM-Agenten den Zugriff auf den VPX ermöglicht.

- **Client**: Eine Firewall ist für die clientseitige Kommunikation von Citrix ADC VPX-Instanzen vorgesehen. In der Regel sind eingehende Regeln an den TCP-Ports 80 und 443 zulässig. Und der 60000-Port ist erforderlich, um den Zustand von ADC-Instanzen zu überwachen.
- **Server**: Eine Firewall ist für die serverseitige Kommunikation von Citrix ADC VPX vorgesehen. Weitere Informationen zum Erstellen einer Firewall in Google Cloud finden Sie unter VPC-Firewall-Regeln — Überblick.

Einrichten von Citrix ADM Komponenten

Bevor Sie Citrix ADC VPX-Instanzen in Citrix ADM bereitstellen, führen Sie die folgenden Aufgaben in Citrix ADM aus:

1. Erstellen einer Site.
2. Bereitstellen eines Citrix ADM-Agenten in Google Cloud.
3. Anfügen der Site an einen Citrix ADM Dienstagenten.

Erstellen einer Site

Erstellen Sie eine Website in Citrix ADM und fügen Sie die Client-VPC-Details hinzu, die mit Ihrer Google Cloud verknüpft sind.

1. Navigieren Sie in Citrix ADM zu **Netzwerke > Sites**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie im Bereich **Cloud auswählen**

a) Wählen Sie **Datencenter** als Standorttyp aus.

b) Wählen Sie **Google Cloud** aus der Liste Typ aus.

c) Aktivieren Sie das Kontrollkästchen **Regionen aus der Google Cloud abrufen**.

Mit dieser Option können Sie die vorhandenen Regionsinformationen aus Ihrem Google Cloud-Konto abrufen.

d) Klicken Sie auf **Weiter**.

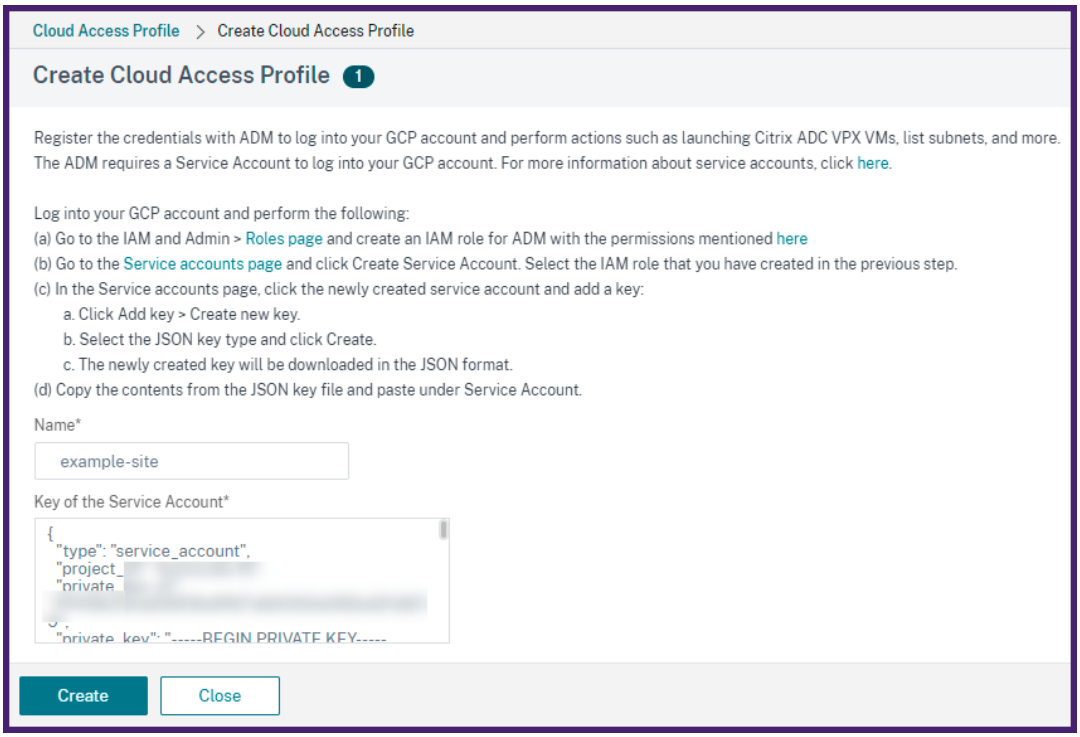
4. **Wählen Sie im Bereich Region auswählen**

a) Wählen Sie in **Cloud Access Profile**das für Ihr Google Cloud-Konto erstellte Profil aus. Wenn keine Profile vorhanden sind, erstellen Sie ein Profil.

b) Klicken Sie auf **Hinzufügen**, um ein Cloud-Zugriffsprofil zu erstellen.

c) Geben Sie **unter Name**einen Namen an, um Ihr Google Cloud-Konto in Citrix ADM zu identifizieren.

d) Geben Sie unter **Schlüssel des Dienstkontos**das in Google Cloud erstellte Dienstkonto an, das JSON erstellt hat.



e) Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Erstellen Sie ein Dienstkonto.

f) Wählen Sie unter **Regionen**die Region aus, die das VPC-Netzwerk enthält, das Citrix ADC VPX-Instanzen enthält, die Sie verwalten möchten.

g) Geben Sie einen **Standortnamen** an.

h) Klicken Sie auf **Fertig stellen**.

Bereitstellen eines Citrix ADM-Agenten in Google Cloud

Der Citrix ADM-Dienst-Agent arbeitet als Vermittler zwischen Citrix ADM und den erkannten Instanzen im Rechenzentrum oder in der Cloud.

1. Navigieren Sie zu **Netzwerke > Agents**.
2. Klicken Sie auf **Bereitstellen**.
3. Wählen Sie **Google Cloud** aus und klicken Sie auf **Weiter**.
4. Geben Sie auf der Registerkarte **Bereitstellungsparameter** Folgendes an:
   - **Name**: Geben Sie den Namen des Citrix ADM Agenten an.
   - **Site** - Wählen Sie die Site aus, die Sie für die Bereitstellung eines Agenten und ADC-VPX-Instanzen erstellt haben.
   - **Cloud Access-Profil** - Wählen Sie das Cloud-Zugriffsprofil aus der Liste aus.
   - **Zone** - Wählen Sie die Zonen aus, in denen Sie die Autoscale-Gruppen erstellen möchten. Abhängig von dem Cloud-Zugriffsprofil, das Sie ausgewählt haben, werden die Zonen dieses Profils ausgefüllt.
   - **Netzwerk**- Wählen Sie das VPC-Netzwerk aus, in dem Sie Autoscale-Gruppen erstellen möchten.
   - **Subnet** - Wählen Sie das Management-Subnetz aus, um einen Agenten bereitzustellen.
   - **Labels** - Geben Sie das Schlüssel-Wert-Paar für die Autoscale-Gruppenbeschriftungen ein. Ein Tag besteht aus einem Schlüssel-Wert-Paar, das zwischen Groß- und Kleinschreibung unterschieden wird. Mit diesen Labels können Sie die Autoscale-Gruppen einfach organisieren und identifizieren. Die Labels werden sowohl auf Google Cloud als auch auf Citrix ADM angewendet.
5. Klicken Sie auf **Fertig stellen**.

Alternativ können Sie den Citrix ADM Agent aus Google Cloud installieren. Weitere Informationen finden Sie unter Installieren eines Citrix ADM-Agenten in der Google Cloud.

Anfügen der Site an einen Citrix ADM Dienstagenten

1. Navigieren Sie in Citrix ADM zu **Netzwerke > Agenten**.
2. Wählen Sie den Agenten aus, für den Sie eine Site anhängen möchten.

3. Klicken Sie auf **Site anhängen**.
4. Wählen Sie die Website aus der Liste aus, die Sie hinzufügen möchten.
5. Klicken Sie auf **Save**.

Schritt 1 - Initialisieren Sie die Autoscale-Konfiguration in Citrix ADM

1. Navigieren Sie in Citrix ADM zu **Netzwerke > AutoScale Groups**.
2. Klicken Sie auf **Hinzufügen**, um Gruppen mit automatischer Skalierung zu erstellen.

   Die Seite **Create AutoScale Group** wird angezeigt.
3. Wählen Sie **Google Cloud** aus und klicken Sie auf Weiter.
4. Geben Sie unter **Basisparameter**die folgenden Details ein:
   - **Name**: Geben Sie einen Namen für die Autoscale-Gruppe ein.
   - **Website**: Wählen Sie die Website aus, die Sie erstellt haben, um die Citrix ADC VPX-Instanzen in Google Cloud automatisch zu skalieren. Wenn Sie keine Website erstellt haben, klicken Sie auf Hinzufügen, um eine Website zu erstellen.
   - **Agent**: Wählen Sie den Citrix ADM-Agenten aus, der die bereitgestellten Instanzen verwaltet.
   - **Cloud Access-Profil**: Wählen Sie das Cloud-Zugriffsprofil aus. Sie können auch ein Cloud Access-Profil hinzufügen oder bearbeiten.
   - **Citrix ADC-Profil**: Wählen Sie das Geräteprofil aus der Liste aus. Citrix ADM verwendet das Geräteprofil, wenn es sich bei der Citrix ADC VPX Instanz anmelden muss.
   - **Traffic-Verteilungsmodus**: Google Cloud unterstützt nur eine Verkehrsverteilung, den Lastenausgleich mit Google Network Load Balancer.
   - **Aktivieren der AutoScale-Gruppe**: Aktivieren oder deaktivieren Sie den Status der ASG-Gruppen. Diese Option ist standardmäßig aktiviert. Wenn diese Option deaktiviert ist, wird die automatische Skalierung nicht ausgelöst.
   - **Zone**: Wählen Sie die Regionen aus, in denen Sie die Autoscale-Gruppen erstellen möchten. Je nach dem von Ihnen ausgewählten Cloud-Zugriffsprofil werden Regionen in der Liste angezeigt.
   - **Labels**: Geben Sie das Schlüssel-Wert-Paar für die Autoscale-Gruppenbeschriftungen ein. Ein Tag besteht aus einem Schlüssel-Wert-Paar, das zwischen Groß- und Kleinschreibung unterschieden wird. Mit diesen Labels können Sie die Autoscale-Gruppen einfach organisieren und identifizieren. Die Labels werden sowohl auf Google Cloud als auch auf Citrix ADM angewendet.
5. Klicken Sie auf **Weiter**.

Schritt 2: Konfigurieren der Parameter für die automatische Skalierung

Geben Sie auf der Registerkarte **AutoScale-Parameter** die folgenden Details ein:

1. Wählen Sie einen oder mehrere der folgenden Schwellenwertparameter aus, deren Werte überwacht werden müssen, um ein Scale-Out oder ein Scale-In auszulösen.

   - **Schwellenwert für die CPU-Auslastung aktivieren**: Überwachen Sie die Metriken basierend auf der CPU-
   - **Schwellenwert für Speicherauslastung aktivieren**: Überwachen Sie die Metriken basierend auf der Speicherauslastung.
   - **Durchsatzschwellenwert aktivieren**: Überwachen Sie die Metriken basierend auf dem Durchsatz.

     > **Hinweis**
     >
     > – Der standardmäßige Mindestgrenzwert beträgt 30 und der Höchstgrenzwert 70. Sie ändern jedoch, um die Limits zu ändern.
     >
     > – Der Mindestgrenzwert muss gleich oder kleiner als die Hälfte des Höchstgrenzwerts sein.
     >
     > – Sie können mehrere Schwellenwerte für die Überwachung auswählen. Scale-out wird ausgelöst, wenn mindestens einer der Schwellenwertparameter über dem maximalen Schwellenwert liegt. Ein Scale-In wird jedoch nur ausgelöst, wenn alle Schwellenwertparameter unterhalb ihrer normalen Schwellenwerte arbeiten.

   - **Mindestinstanzen**: Wählen Sie die Mindestanzahl von Instanzen aus, die für diese Autoscale-Gruppe bereitgestellt werden müssen.

     Die Standardanzahl der Instanzen entspricht der Anzahl der ausgewählten Zonen. Sie können nur die Mindestinstanzen in den Vielfachen der angegebenen Anzahl von Zonen erhöhen.

     Wenn die Anzahl der Zonen beispielsweise 4 beträgt, sind die Mindestinstanzen standardmäßig 4. Sie können die minimalen Instanzen um 8, 12, 16 erhöhen.

   - **Maximale Instanzen**: Wählen Sie die maximale Anzahl von Instanzen aus, die für diese Autoscale-Gruppe bereitgestellt werden müssen.

     Die maximale Anzahl von Instanzen muss größer oder gleich dem Wert der minimalen Instanzen sein. Die maximale Anzahl von Instanzen darf die Anzahl der Zonen multipliziert mit 32 nicht überschreiten.

     Maximale Anzahl von Instanzen = Anzahl der Zonen * 32

- **Watch-Zeit (Minuten)**: Wählen Sie die Dauer der Uhr aus. Die Zeit, für die der Schwellenwert des Skalierungsparameters überschritten werden muss, damit die Skalierung erfolgt. Wenn der Schwellenwert für alle Proben, die in dieser angegebenen Zeit gesammelt wurden, überschritten wird, geschieht eine Skalierung.
- **Abklingzeit (Minuten)**: Wählen Sie die Abklingzeit aus. Während des Scale-Outs ist die Abklingzeit die Zeit, für die die Auswertung der Statistiken nach einem Scale-Out gestoppt werden muss. Dieser Zeitraum sorgt für den organischen Anbau von Instanzen einer Autoscale-Gruppe. Bevor die nächste Skalierungsentscheidung ausgelöst wird, wird darauf gewartet, dass sich der aktuelle Datenverkehr stabilisiert und auf den aktuellen Satz von Instanzen durchdurchschnittlich wird.
- **Wartezeit während der Aufhebung der Bereitstellung (Minuten)**: Wählen Sie den Timeout-Zeitraum für die Drain-Verbindung aus. Während der Scale-In-Aktion wird eine Instanz identifiziert, die die Bereitstellung aufweist. Citrix ADM schränkt die identifizierte Instanz davon ab, neue Verbindungen zu verarbeiten, bis die angegebene Zeit vor der Aufhebung der Bereitstellung abläuft. In diesem Zeitraum können vorhandene Verbindungen zu dieser Instanz entzogen werden, bevor die Bereitstellung aufgehoben wird.

2. Klicken Sie auf **Weiter**.

Schritt 3 - Konfigurieren von Lizenzen

Citrix ADM bietet den ADC-Instanzen die gewünschte Version und Lizenz an. ADC-Images können entweder von Kunden lizenziert (BYOL) oder von Google Cloud lizenziert sein.

Wählen Sie einen der folgenden Modi aus, um die Lizenz auf eine ADC-Instanz anzuwenden:

- **Zuteilung von Citrix ADM**: Die Instanz, die Sie bereitstellen möchten, checkt die Lizenzen aus dem Citrix ADM aus.
- **Aus Google Cloud zuteilen**: Die Option **Aus Cloud zuweisen** verwendet die in Google Cloud verfügbaren Citrix Produktlizenzen. Die Instanz, die Sie bereitstellen möchten, verwendet die Lizenzen aus der Google Cloud.

  Wenn Sie Lizenzen aus Google Cloud verwenden, geben Sie das Produkt oder die Lizenz auf der Registerkarte **Bereitstellungsparameter** an.

Weitere Informationen finden Sie unter Lizenzanforderungen.

Zuteilen von Lizenzen von Citrix ADM

1. Wählen Sie auf der Registerkarte **Lizenz** die Option **Aus ADM zuweisen**.
2. Wählen Sie unter **Lizenztyp**eine der folgenden Optionen aus der Liste:

- **Bandbreitenlizenzen:** Sie können eine der folgenden Optionen aus der Liste **Bandbreitenlizenztypen** auswählen:
  - **Pooled Capacity:** Geben Sie die Kapazität an, die einer Instanz zugewiesen werden soll.

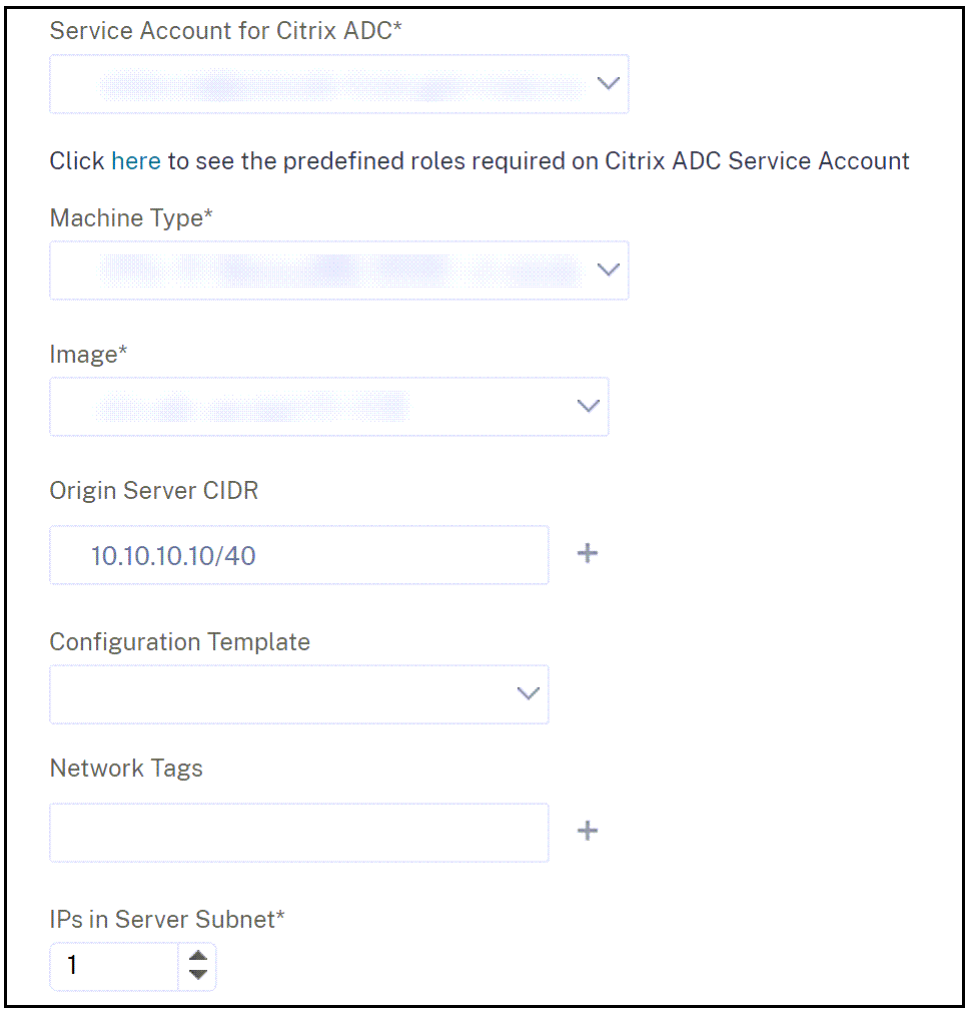
    Aus dem gemeinsamen Pool checkt die ADC-Instanz eine Instanzlizenz aus und nur so viel Bandbreite wird angegeben.
  - **VPX-Lizenzen:** Wenn eine Citrix ADC VPX Instanz bereitgestellt wird, checkt die Instanz die Lizenz vom Citrix ADM aus.
- **Virtuelle CPU-Lizenzen:** Die bereitgestellte Citrix ADC VPX-Instanz checkt Lizenzen abhängig von der Anzahl der in der Instanz ausgeführten CPUs aus.

> **Hinweis:**
>
> Wenn die bereitgestellten Instanzen entfernt oder gelöscht werden, kehren die angewendeten Lizenzen in den Citrix ADM -Lizenzpool zurück. Diese Lizenzen können wiederverwendet werden, um neue Instanzen bereitzustellen.

3. Wählen Sie in **License Edition** die Lizenzversion aus. Der ADM verwendet die angegebene Edition zur Bereitstellung von Instanzen.
4. Klicken Sie auf **Weiter**.

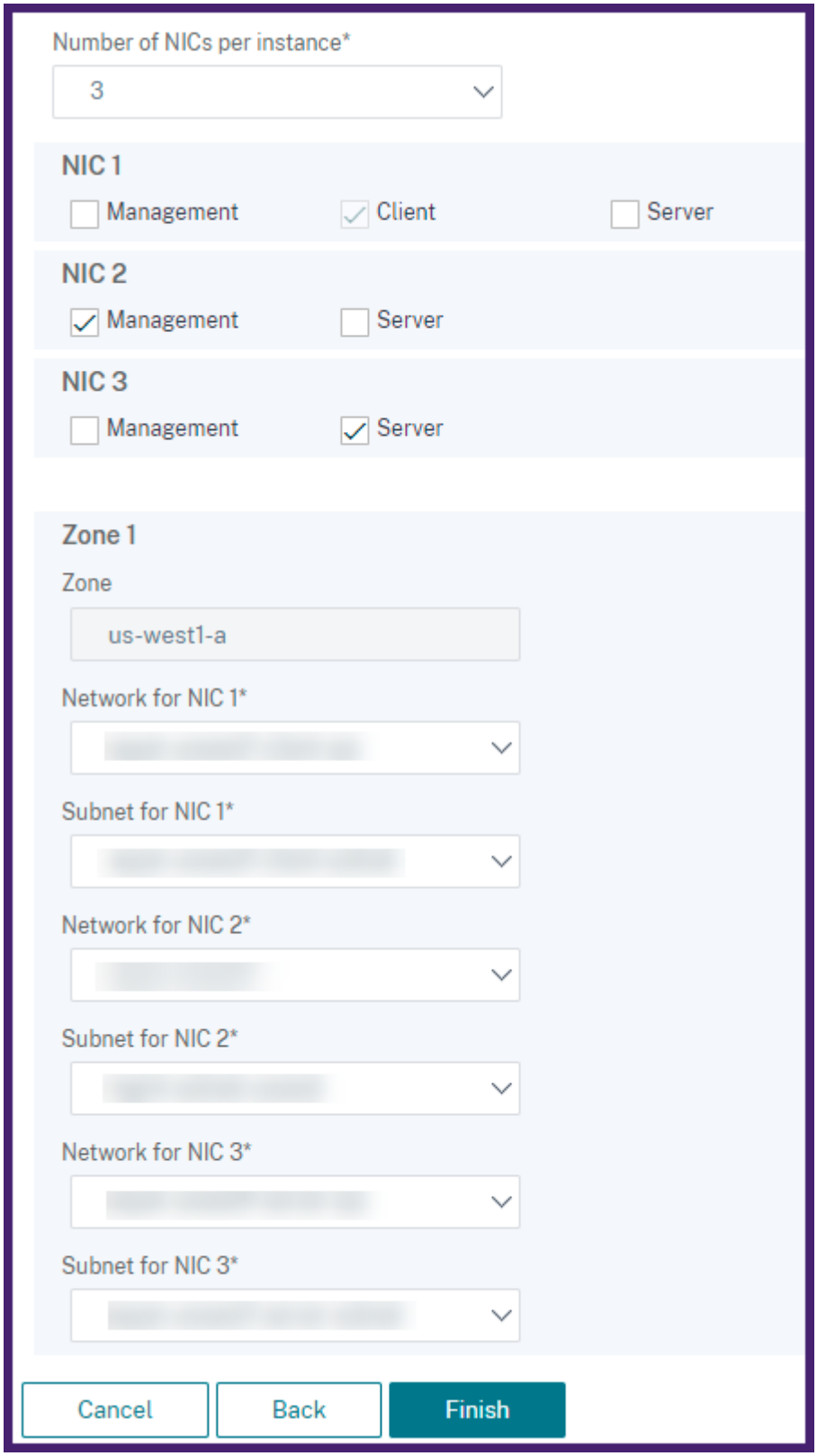
Schritt 4: Konfigurieren Sie die Bereitstellungsparameter

1. Geben Sie auf der Registerkarte **Bereitstellungsparameter** Folgendes an:
   - **ADC-Dienstkonto**: Wählen Sie das Dienstkonto aus, das Sie in Google Cloud erstellt haben. Der ADM verwendet ein Dienstkonto, um auf Ihre Google Cloud-Ressourcen zuzugreifen.
   - **Produkt/ Lizenz**: Wählen Sie die Citrix ADC-Produktversion aus, die Sie bereitstellen möchten. Weitere Informationen finden Sie unter Abonnieren der Citrix ADC VPX-Lizenz in Google Cloud.
   - **Maschinentypen**: Wählen Sie den gewünschten Maschinentyp aus der Liste aus.
   - **Image**: Wählen Sie das erforderliche Citrix ADC-Versionimage aus. Klicken Sie auf Neu hinzufügen, um ein Citrix ADC Image hinzuzufügen.
   - **Konfigurationsvorlage** — Wählen Sie die Konfigurationsvorlage aus, die Sie für die Bereitstellung auf den ADC-Instanzen verwenden möchten.
   - **IPs im Server-Subnetz pro Instanz** — Geben Sie an, wie viele SNIP-Adressen jede Instanz im Serversubnetz haben kann.



Auf dieser Registerkarte können Sie auch die erforderlichen NICs angeben und konfigurieren. Jede NIC enthält eine dedizierte Firewall und ein Subnetz.

Weitere Informationen finden Sie unter Erstellen Sie ein VPC-Netzwerk und Erstellen Sie eine Firewall.



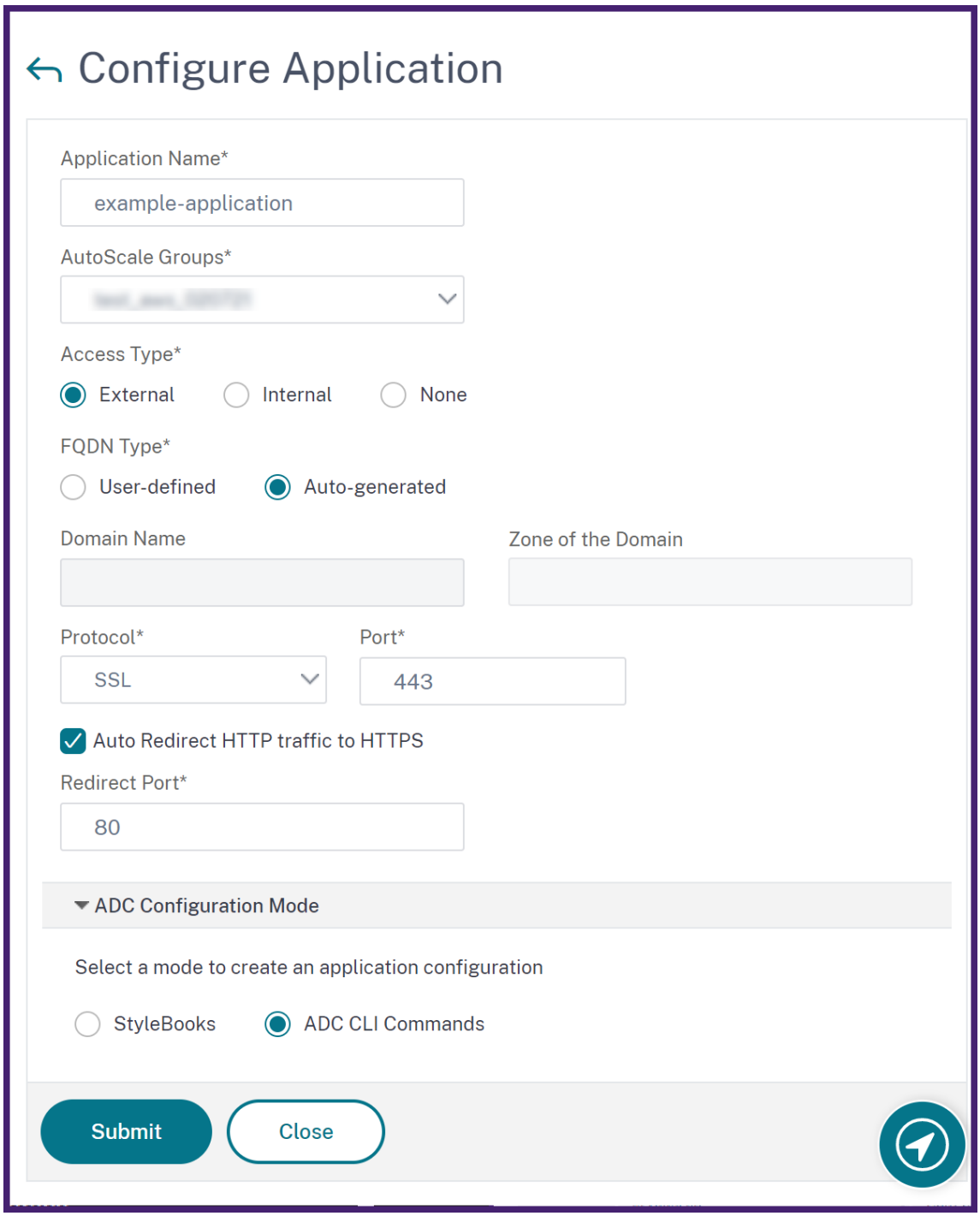
2. Klicken Sie auf **Fertig stellen**.

Schritt 5: Konfigurieren einer Anwendung für die Autoscale-Gruppe

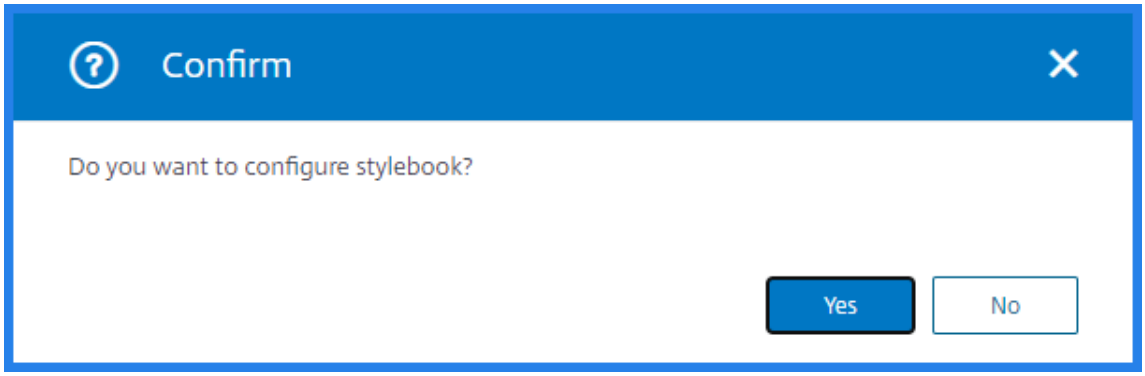
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Autoscale-Gruppen**.
2. Wählen Sie die von Ihnen erstellte Gruppe “Automatisch skalieren” aus, und klicken Sie auf **Konfigurieren**.
3. Geben Sie unter **Anwendung konfigurieren** die folgenden Details an:
    - **Anwendungsname** - Geben Sie den Namen einer Anwendung an.
    - **Zugriffstyp** - Sie können die ADM-Lösung für die automatische Skalierung sowohl für externe als auch für interne Anwendungen verwenden. Wählen Sie den erforderlichen Anwendungszugriffstyp aus.
    - **FQDN-Typ** - Wählen Sie einen Modus für die Zuweisung von Domänen- und Zonennamen aus.

      Wenn Sie manuell angeben möchten, wählen Sie **Benutzerdefiniert** aus. Um Domänen- und Zonennamen automatisch zuzuweisen, wählen Sie **Automatisch generiert** aus.
    - **Domänenname** - Geben Sie den Domänennamen einer Anwendung an. Diese Option ist nur anwendbar, wenn Sie Benutzerdefinierter FQDN-Typ auswählen.
    - **Zone der Domäne** - Wählen Sie den Zonennamen einer Anwendung aus der Liste aus. Diese Option ist nur anwendbar, wenn Sie Benutzerdefinierter FQDN-Typ auswählen.

      Dieser Domain- und Zonenname wird auf die virtuellen Server in Google Cloud weitergeleitet. Wenn Sie beispielsweise eine Anwendung in `app.example.com`hosten, ist `app`der Domänenname und `example.com`der Zonenname.
    - **Protokoll** - Wählen Sie den Protokolltyp aus der Liste aus. Die konfigurierte Anwendung empfängt den Datenverkehr abhängig vom ausgewählten Protokolltyp.
    - **Port** - Geben Sie den Portwert an. Der angegebene Port wird verwendet, um eine Kommunikation zwischen der Anwendung und der Autoscale-Gruppe herzustellen.

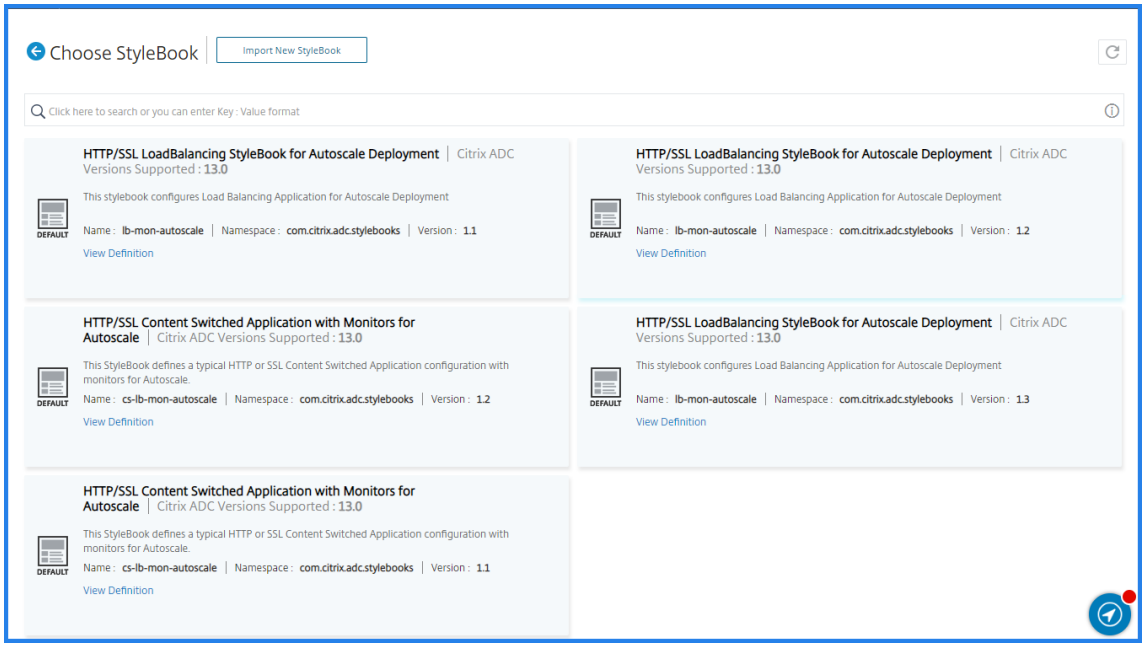


Wenn Sie eine Anwendung mit StyleBooks konfigurieren möchten, wählen Sie im Bestätigungsfenster **Ja** aus.



> **Hinweis Ändern Sie**
>
> den Zugriffstyp einer Anwendung, wenn Sie die folgenden Details in Zukunft ändern möchten:
>
> - FQDN Typ
> - Domänenname
> - Zone der Domäne

4. Wählen Sie das gewünschte StyleBook aus, das Sie Konfigurationen für die ausgewählte Autoscale-Gruppe bereitstellen möchten.



Wenn Sie StyleBooks importieren möchten, klicken Sie auf **Neues StyleBook importieren**.

5. Geben Sie die Werte für alle Parameter an.

   Die Konfigurationsparameter sind im ausgewählten StyleBook vordefiniert.

6. Aktivieren Sie das Kontrollkästchen **Application Server Group Type CLOUD**, um die Anwendungsserver anzugeben, die im Skalierungssatz der virtuellen Maschine verfügbar sind.

a) Geben Sie unter **Application Server Fleet Name**den **Namen der Autoscale-Einstellung** Ihres Skalierungssatzes für virtuelle Maschinen an.

b) Wählen Sie das **Application Server-Protokoll** aus der Liste aus.

c) Geben Sie unter **Memberport** den Portwert des Anwendungsservers an.

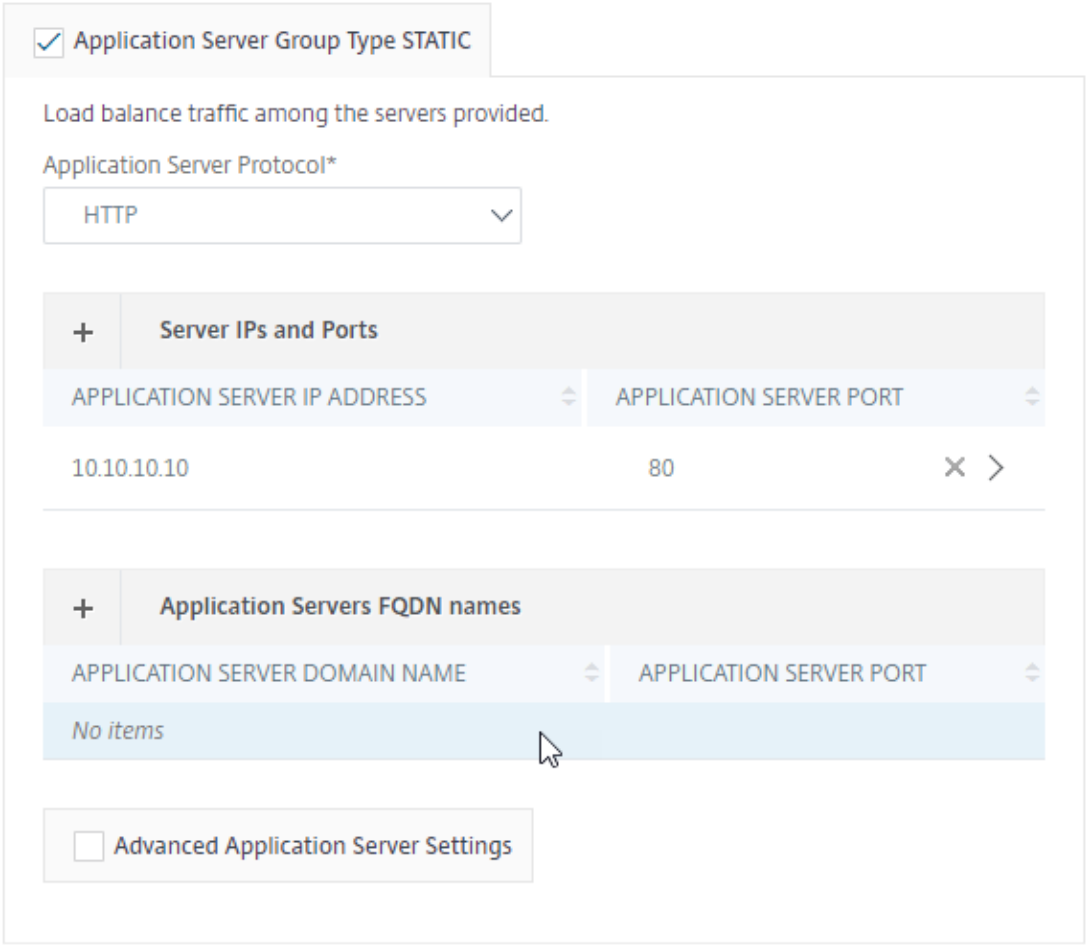
> **Hinweis: Stellen Sie**
>
> sicher, dass **AutoDisable Graceful shutdown** auf **No** festgelegt ist und das Feld **AutoDisable Delay** leer ist.

d) Wenn Sie die erweiterten Einstellungen für Ihre Anwendungsserver angeben möchten, aktivieren Sie das Kontrollkästchen **Erweiterte Anwendungsserver-Einstellungen**. Geben Sie dann die erforderlichen Werte an, die unter **Erweiterte Anwendungsservereinstellungen**aufgeführt sind.

7. Wenn Sie eigenständige Anwendungsserver im virtuellen Netzwerk haben, aktivieren Sie das Kontrollkästchen **Anwendungsservergruppentyp STATIC**:

a) Wählen Sie das **Application Server-Protokoll** aus der Liste aus.

b) Klicken Sie **unter Server-IPs und -Ports**auf **+**, um eine IP-Adresse, einen Port und ein Gewicht des Anwendungsservers hinzuzufügen, und klicken Sie dann auf **Erstellen**.



8. Klicken Sie auf **Erstellen**.

Ändern der Konfiguration von Gruppen für automatische Skalierung

Sie können eine Autoscale-Gruppenkonfiguration ändern oder eine Autoscale-Gruppe löschen. Sie können nur die folgenden Gruppenparameter für die automatische Skalierung ändern:

- Maximal- und Minimalgrenzen der Schwellenwerte
- Minimale und maximale Instanzwerte
- Wert der Ablaufanschlussperiode
- Wert der Abklingperiode
- Wert für die Dauer der Uhr

Sie können auch die Autoskalier-Gruppen löschen, nachdem sie erstellt wurden.

Wenn eine Autoscale-Gruppe gelöscht wird, werden alle Domänen und IP-Adressen vom DNS abgemeldet und die Clusterknoten werden aufgehoben.

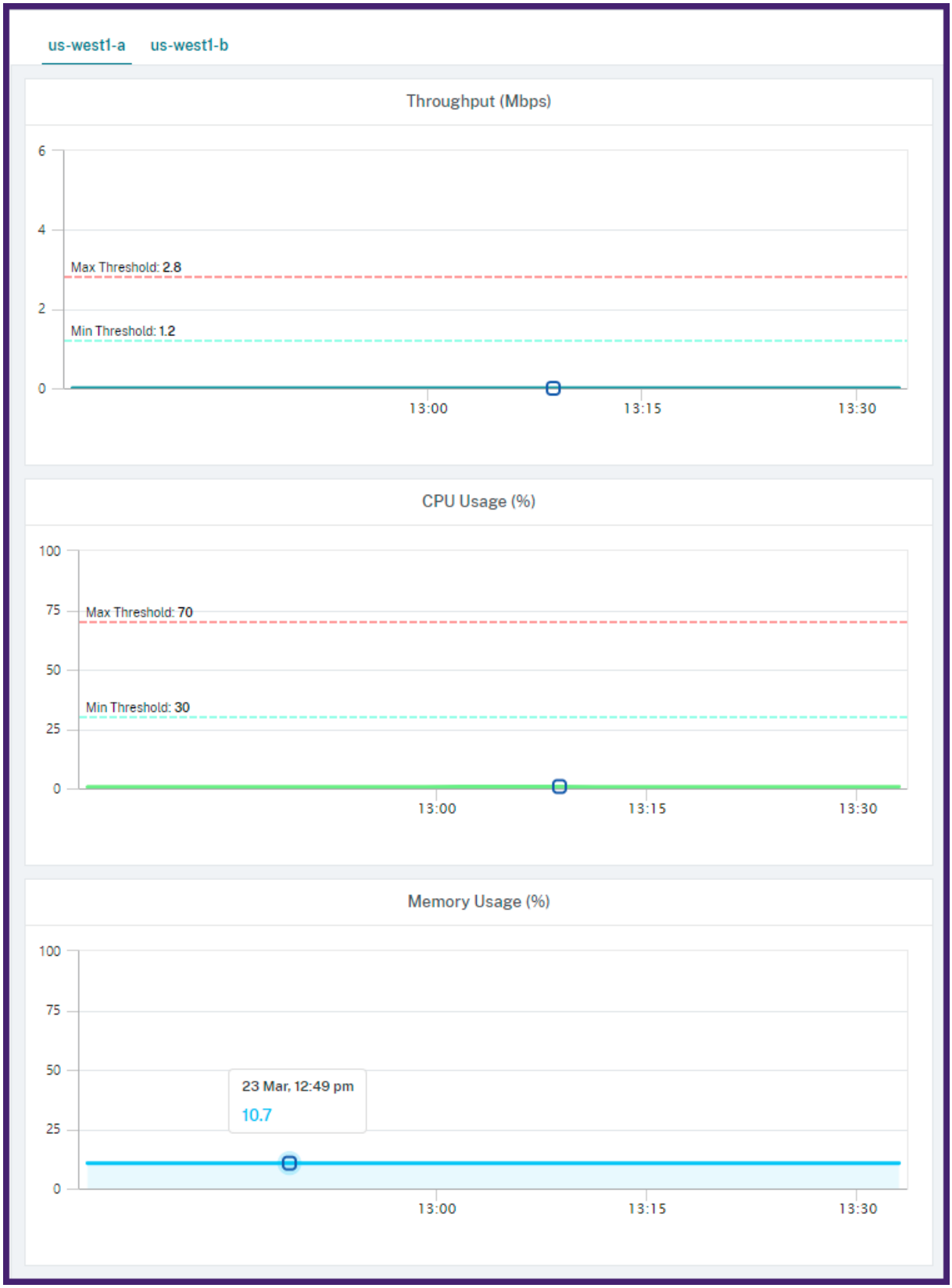
Dashboard

April 28, 2021

Sie können das Diagramm für die ausgewählten Überwachungsparameter anzeigen. Im rechten Bereich werden die Ereignisse angezeigt, die die automatische Skalierung auslösen. Im linken Bereich werden die aktiven Knoten im Cluster pro Zone, das Diagramm der aktiven Knoten und die Ereignisse angezeigt.

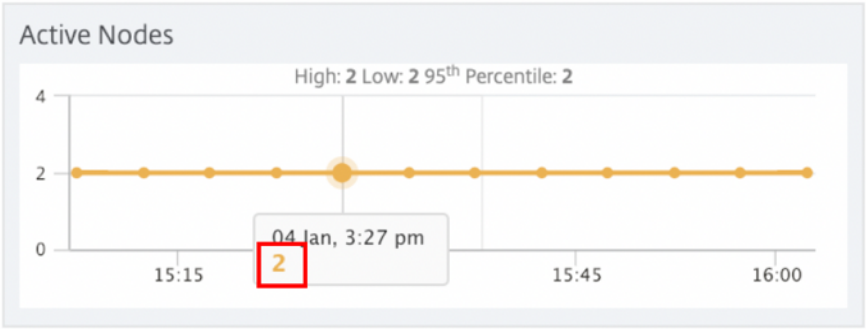
1. Navigieren Sie in Citrix ADM zu **Netzwerke > Gruppen automatisch skalieren**.
2. Wählen Sie die Autoscale-Gruppe und klicken Sie auf **Dashboard**

Die folgende Abbildung zeigt ein Beispiel-Dashboard:



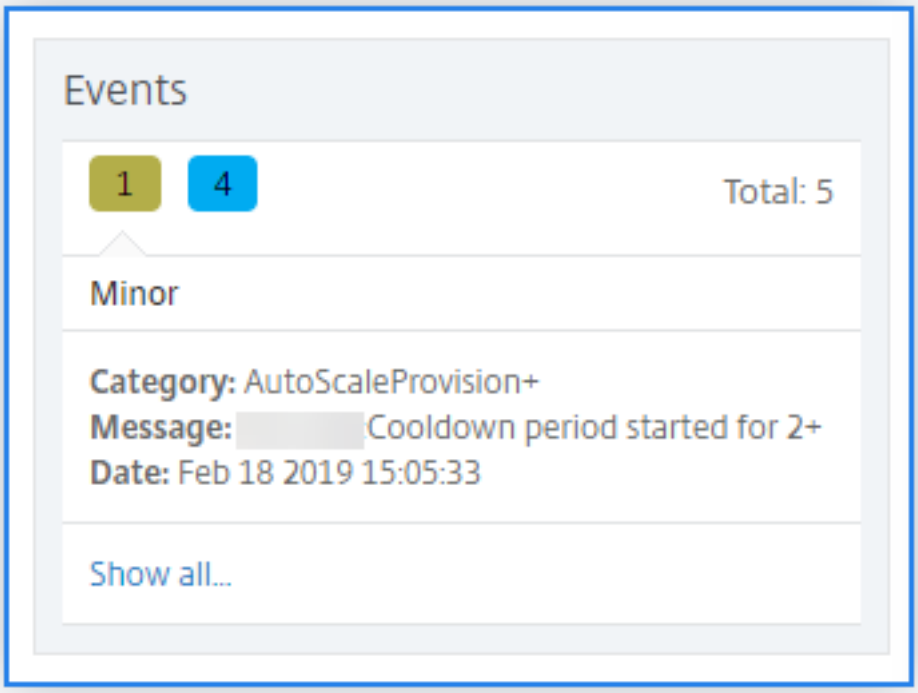
Die folgende Abbildung zeigt das Diagramm der aktiven Knoten. Die Zahl unter dem Zeitstempel zeigt

die Anzahl der aktiven Knoten an. Sie können die Anzahl der aktiven Knoten, die Teil der Zone sind, jederzeit anzeigen.

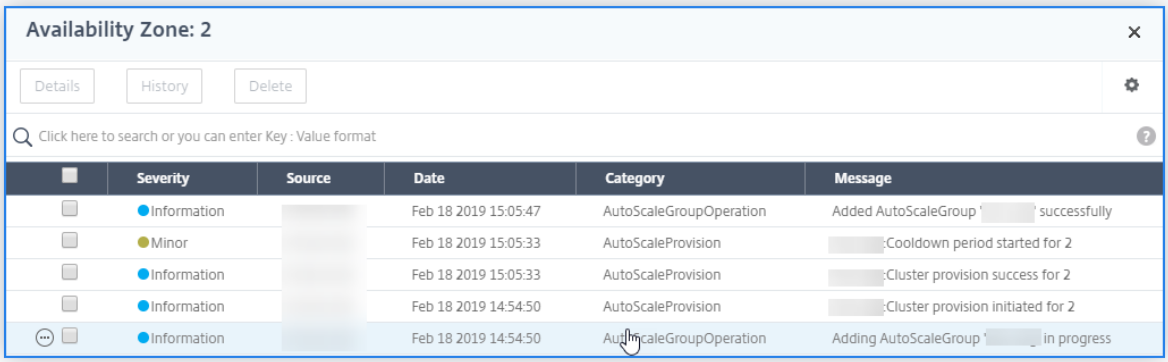


Ereignisse

Im **Dashboard**zeigt die Registerkarte **Ereignisse** die Gesamtzahl der Ereignisse für die ausgewählte Autoscale-Gruppe an. Außerdem wird eine kurze Meldung des letzten Ereignisses angezeigt.



Klicken Sie auf **Alle anzeigen, um die Details der Ereignisse anzuzeigen**.



Globaler Citrix ADC Lastenausgleich für Hybrid- und Multi-Cloud-Bereitstellungen

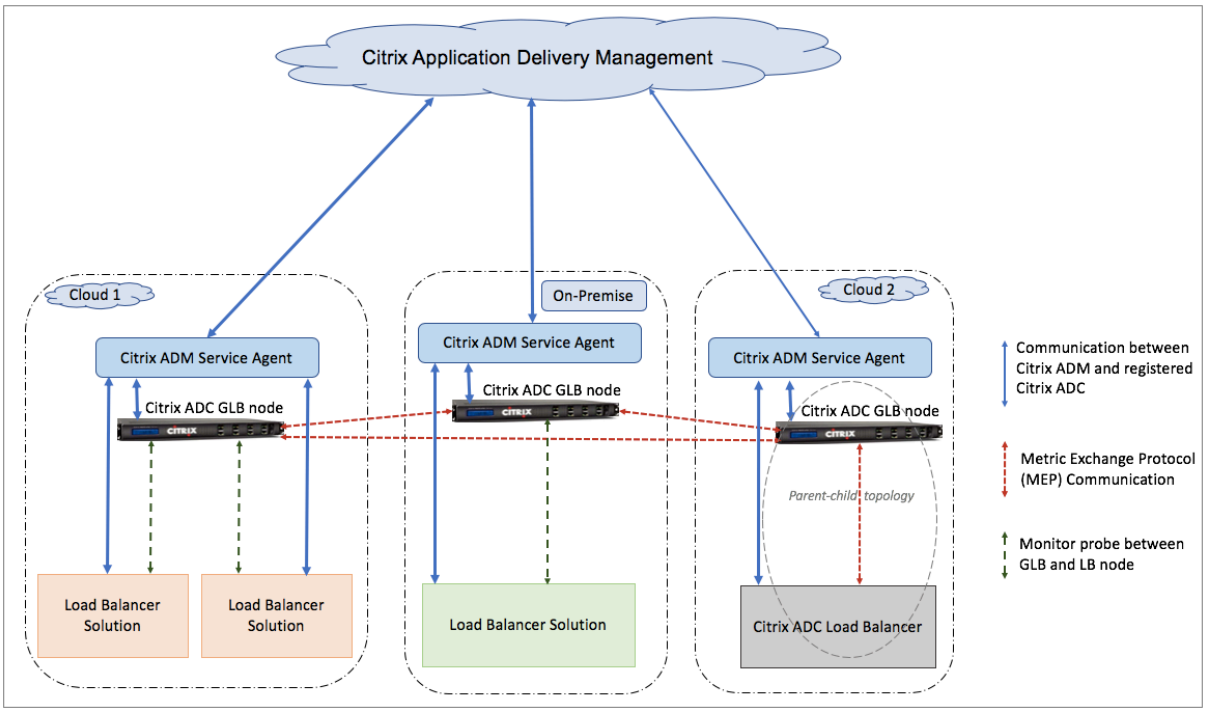
April 28, 2021

Mit der Citrix ADC Hybrid- und Multi-Cloud-Lösung Global Load Balancing (GLB) können Sie den Anwendungsdatenverkehr über mehrere Rechenzentren in Hybrid-Clouds, mehreren Clouds und einer lokalen Bereitstellung verteilen. Die Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung unterstützt Sie bei der Verwaltung Ihrer Load Balancing-Setup in Hybrid- oder Multi-Cloud, ohne das vorhandene Setup zu ändern. Wenn Sie über ein lokales Setup verfügen, können Sie einige Ihrer Dienste in der Cloud testen, indem Sie die Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung verwenden, bevor Sie vollständig in die Cloud migrieren. Beispielsweise können Sie nur einen kleinen Prozentsatz Ihres Datenverkehrs an die Cloud weiterleiten und den größten Teil des Datenverkehrs on-premises abwickeln. Mit der Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung können Sie Citrix ADC-Instanzen über eine einzige einheitliche Konsole hinweg verwalten und überwachen.

Eine Hybrid- und Multi-Cloud-Architektur kann auch die Gesamtleistung des Unternehmens verbessern, indem sie “Anbieterbindung” vermeidet und eine andere Infrastruktur verwendet, um die Anforderungen Ihrer Partner und Kunden zu erfüllen. Mit mehreren Cloud-Architekturen können Sie Ihre Infrastrukturkosten besser verwalten, da Sie jetzt nur für das bezahlen müssen, was Sie nutzen. Skalieren Sie Ihre Anwendungen auch besser, da Sie die Infrastruktur jetzt bei Bedarf nutzen. Es bietet auch die Möglichkeit, schnell von einer Cloud in eine andere zu wechseln, um die Vorteile der besten Angebote jedes Anbieters zu nutzen.

Architektur der Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung

Das folgende Diagramm veranschaulicht die Architektur der Citrix ADC Hybrid- und Multi-Cloud-GLB-Funktion.



Die Citrix ADC GLB-Knoten verarbeiten die DNS-Namensauflösung. Jeder dieser GLB-Knoten kann DNS-Anforderungen von jedem Clientstandort empfangen. Der GLB-Knoten, der die DNS-Anforderung empfängt, gibt die IP-Adresse des virtuellen Load Balancer zurück, wie sie von der konfigurierten Load Balancing-Methode ausgewählt wurde. Metriken (Standort-, Netzwerk- und Persistenzmetriken) werden zwischen den GLB-Knoten mit dem Metrikaustauschprotokoll (MEP) ausgetauscht, bei dem es sich um ein proprietäres Citrix Protokoll handelt. Weitere Informationen zum MEP-Protokoll finden Sie unter Konfigurieren des Metriks-Exchange-Protokolls.

Der im GLB-Knoten konfigurierte Monitor überwacht den Integritätsstatus des virtuellen Lastausgleichsservers im selben Rechenzentrum. In einer übergeordneten und untergeordneten Topologie werden Metriken zwischen den GLB- und Citrix ADC Knoten mithilfe von MEP ausgetauscht. Die Konfiguration von Monitorprobes zwischen einem GLB- und Citrix ADC LB-Knoten ist jedoch in einer übergeordneten und untergeordneten Topologie optional.

Der Citrix Application Delivery Management (ADM) -Dienstagent ermöglicht die Kommunikation zwischen Citrix ADM und den verwalteten Instanzen in Ihrem Rechenzentrum. Weitere Informationen zu Citrix ADM Dienstagenten und deren Installation finden Sie unterSchnelleinstieg.

> **Hinweis**
>
> In diesem Dokument werden die folgenden Annahmen getroffen:

- Wenn Sie ein vorhandenes Load Balancing-Setup haben, ist es in Betrieb.
- Auf jedem Citrix ADC GLB-Knoten wird eine SNIP-Adresse oder eine GLB-Standort-IP-Adresse konfiguriert. Diese IP-Adresse wird als IP-Adresse der Rechenzentrumsquelle beim Austausch von Metriken mit anderen Rechenzentren verwendet.

- Ein ADNS- oder ADNS-TCP-Dienst wird für jede der Citrix ADC GLB-Instanzen konfiguriert, um den DNS-Datenverkehr zu empfangen.
- Die erforderlichen Firewall- und Sicherheitsgruppen werden in den Cloud-Dienstanbietern konfiguriert.

> **Konfiguration von Sicherheitsgruppen**
>
> Sie müssen die erforderliche Firewall-/Sicherheitsgruppenkonfiguration in den Cloud-Dienstanbietern einrichten. Weitere Informationen zu AWS-Sicherheitsfunktionen finden Sie unter AWS-Dokumentation. Weitere Informationen zu Microsoft Azure Network Security Groups finden Sie unter Microsoft Azure-Dokumentation.
>
> Darüber hinaus müssen Sie auf dem GLB-Knoten Port 53 für ADNS Service/DNS-Server-IP-Adresse und Port 3009 für GSLB-Standort-IP-Adresse für den MEP-Datenverkehr öffnen. Auf dem Lastausgleichsknoten müssen Sie die entsprechenden Ports öffnen, um den Anwendungsdatenverkehr zu empfangen. Beispielsweise müssen Sie Port 80 für den Empfang von HTTP-Datenverkehr und Port 443 für den Empfang von HTTPS-Datenverkehr öffnen. Öffnen Sie Port 443 für die NITRO -Kommunikation zwischen dem Citrix ADM Dienst-Agent und Citrix ADM.
>
> Für die dynamische Roundtrip Time GLB-Methode müssen Sie Port 53 öffnen, um UDP- und TCP-Prüfpunkte abhängig vom konfigurierten LDNS-Prüftyp zuzulassen. Die UDP- oder TCP-Prüfpunkte werden mit einem der SNIPs initiiert. Daher muss diese Einstellung für Sicherheitsgruppen erfolgen, die an das serverseitige Subnetz gebunden sind.

Funktionen der Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung

Einige der Funktionen der Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung werden in diesem Abschnitt beschrieben:

Kompatibilität mit anderen Lastausgleichslösungen

Die Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung unterstützt verschiedene Load Balancing-Lösungen, z. B. den Citrix ADC Load Balancer, Nginx, HAProxy und andere Lastausgleichsprogramme von Drittanbietern.

> **Hinweis**
>
> Lastenausgleichslösungen außer Citrix ADC werden nur unterstützt, wenn proximitätsbasierte und nicht-metrische GLB-Methoden verwendet werden und die übergeordnete untergeordnete Topologie nicht konfiguriert ist.

GLB-Methoden

Die Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung unterstützt die folgenden GLB-Methoden.

- Metrikbasierte GLB-Methoden. Metrik-basierte GLB-Methoden erfassen Metriken von den anderen Citrix ADC Knoten über das Metrikaustauschprotokoll.
  - Mindest Connection: Die Client-Anfrage wird an den Load Balancer weitergeleitet, der die wenigsten aktiven Verbindungen hat.
  - Geringste Bandbreite: Die Clientanforderung wird an den Load Balancer weitergeleitet, der derzeit den geringsten Datenverkehr bedient.
  - Kleinste Pakete: Die Clientanforderung wird an den Load Balancer weitergeleitet, der die wenigsten Pakete in den letzten 14 Sekunden empfangen hat.
- Nicht-metrische GLB-Methoden
  - Round Robin: Die Clientanforderung wird an die IP-Adresse des Load Balancers weitergeleitet, der sich oben in der Liste der Load Balancer befindet. Dieser Load Balancer bewegt sich dann an den unteren Rand der Liste.
  - Quell-IP-Hash: Diese Methode verwendet den Hashwert der Client-IP-Adresse, um einen Load Balancer auszuwählen.
- Proximity-basierte GLB-Methoden
  - Statische Nähe: Die Clientanforderung wird an den Load Balancer weitergeleitet, der der Client-IP-Adresse am nächsten ist.
  - Round-Trip-Zeit (RTT): Bei dieser Methode wird der RTT-Wert (die Zeitverzögerung in der Verbindung zwischen dem lokalen DNS-Server des Clients und dem Rechenzentrum) verwendet, um die IP-Adresse des Load Balancer mit der besten Leistung auszuwählen.

Weitere Hinweise zu den Load Balancing-Methoden finden Sie unter Lastausgleichsalgorithmen.

GLB-Topologien

Die Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung unterstützt die aktiv-passive Topologie und die übergeordnete untergeordnete Topologie.

- Aktiv-Passiv-Topologie — Bietet Disaster Recovery und gewährleistet kontinuierliche Verfügbarkeit von Anwendungen durch Schutz vor Ausfallpunkten. Wenn das primäre Rechenzentrum ausfällt, wird das passive Rechenzentrum betriebsbereit. Weitere Hinweise zur aktiven und passiven GSLB-Topologie finden Sie unter Konfigurieren von GSLB für Disaster Recovery.
- Parent-Child-Topologie — Kann verwendet werden, wenn Sie GLB- und LB-Knoten mithilfe der metricbasierten GLB-Methoden konfigurieren und die LB-Knoten auf einer anderen Citrix ADC-Instanz bereitgestellt werden. In einer über-/untergeordneten Topologie muss der LB-Knoten (untergeordneter Standort) eine Citrix ADC Appliance sein, da der Austausch von Metriken zwischen dem übergeordneten und dem untergeordneten Standort über das Metrikaustauschprotokoll (MEP) erfolgt.

Weitere Hinweise zur übergeordneten und untergeordneten Topologie finden Sie unter Bereitstellung der übergeordneten und untergeordneten Topologie mithilfe des MEP-Protokolls.

Unterstützung für IPv6

Die Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung unterstützt auch IPv6.

Überwachen

Die Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung unterstützt integrierte Monitore mit einer Option, um die sichere Verbindung zu ermöglichen. Wenn sich LB- und GLB-Konfigurationen jedoch auf derselben Citrix ADC-Instanz befinden oder die übergeordnete und untergeordnete Topologie verwendet wird, ist die Konfiguration von Monitoren optional.

Persistenz

Die Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung unterstützt Folgendes:

- Quell-IP-basierte Persistenzsitzungen, sodass mehrere Anforderungen desselben Clients an denselben Dienst weitergeleitet werden, wenn sie innerhalb des konfigurierten Zeitüberschreitungsfensters eintreffen. Wenn der Timeout-Wert abläuft, bevor der Client eine andere Anforderung sendet, wird die Sitzung verworfen, und der konfigurierte Lastausgleichsalgorithmus wird verwendet, um einen neuen Server für die nächste Anforderung des Clients auszuwählen.
- Spillover-Persistenz, so dass der virtuelle Backup-Server die empfangenen Anforderungen weiterhin verarbeitet, auch wenn die Last auf dem primären Schwellenwert unterschritten wird. Weitere Informationen finden Sie unter Konfigurieren von Spillover.
- Standortpersistenz, so dass der GLB-Knoten ein Rechenzentrum zur Verarbeitung einer Clientanforderung auswählt und die IP-Adresse des ausgewählten Rechenzentrums für alle nachfolgenden DNS-Anforderungen weiterleitet. Wenn die konfigurierte Persistenz für einen Standort gilt, der DOWN ist, verwendet der GLB-Knoten eine GLB-Methode, um einen neuen Standort auszuwählen, und der neue Standort wird dauerhaft für nachfolgende Anforderungen vom Client.

Konfiguration mithilfe der Citrix ADM StyleBooks

Sie können das Standard-GLB-StyleBook für Multi-Cloud unter Citrix ADM verwenden, um Citrix ADC-Instanzen mit Hybrid- und Multi-Cloud-GLB-Konfiguration zu konfigurieren.

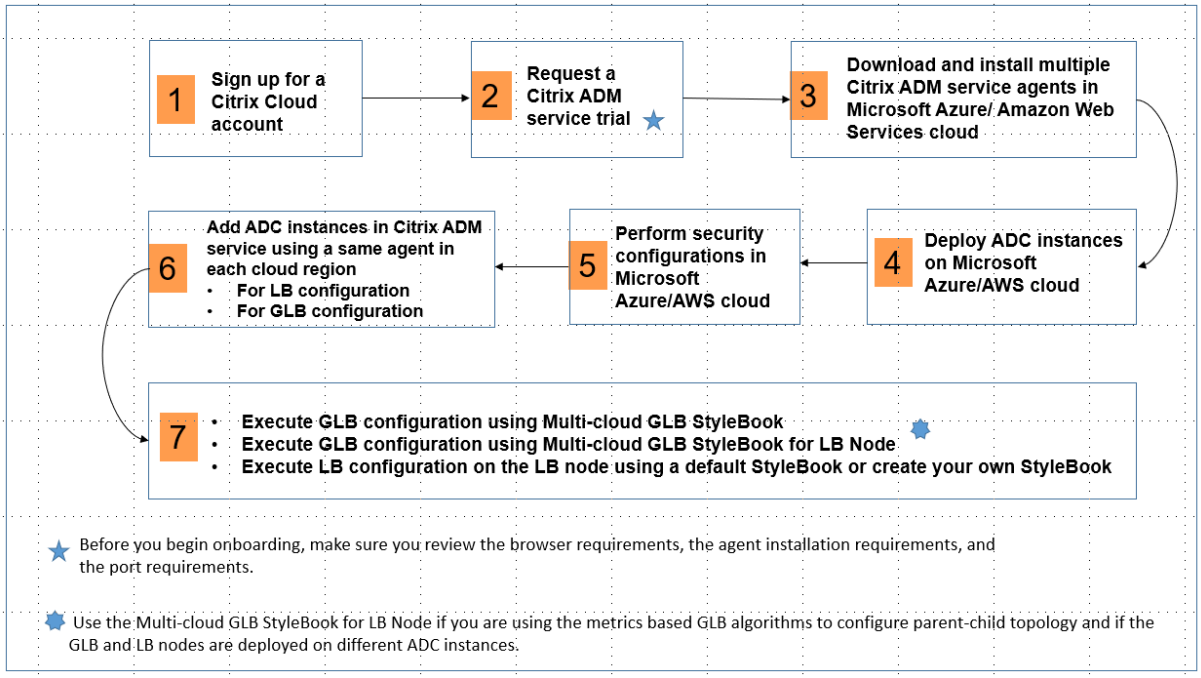
Sie können das standardmäßige GLB-StyleBook für LB Node StyleBook für LB Node verwenden, um die Citrix ADC Lastausgleichsknoten zu konfigurieren, die die untergeordneten Standorte in einer

über-/untergeordneten Topologie sind, die den Anwendungsdatenverkehr verarbeiten. Verwenden Sie dieses StyleBook nur, wenn Sie LB-Knoten im Falle einer übergeordneten und untergeordneten Topologie konfigurieren möchten. Jeder LB-Knoten muss jedoch separat mit diesem StyleBook konfiguriert werden.

Workflow der Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösungskonfiguration

Sie können das mitgelieferte Multi-Cloud-GLB-StyleBook unter Citrix ADM verwenden, um Citrix ADC-Instanzen mit Hybrid- und Multi-Cloud-GLB-Konfiguration zu konfigurieren.

Das folgende Diagramm zeigt den Arbeitsablauf für die Konfiguration der Citrix ADC Hybrid- und Multi-Cloud-GLB-Lösung. Die Schritte im Workflow-Diagramm werden nach dem Diagramm ausführlicher erläutert.



Führen Sie die folgenden Aufgaben als Cloud-Administrator aus:

1. Registrieren Sie sich für ein Citrix Cloud-Konto.

   Um mit der Verwendung von Citrix ADM zu beginnen, erstellen Sie ein Citrix Cloud-Unternehmenskonto oder treten Sie einem bestehenden Konto bei, das von jemandem in Ihrem Unternehmen erstellt wurde.

2. Nachdem Sie sich bei Citrix Cloud angemeldet haben, klicken Sie auf der Kachel **Citrix Application Delivery Management** auf **Verwalten**, um den ADM-Dienst zum ersten Mal einzurichten.

3. Laden Sie mehrere Citrix ADM Dienstagenten herunter und installieren Sie sie.

Sie müssen den Citrix ADM Dienst-Agent in Ihrer Netzwerkumgebung installieren und konfigurieren, um die Kommunikation zwischen Citrix ADM und den verwalteten Instanzen in Ihrem Rechenzentrum oder in der Cloud zu ermöglichen. Installieren Sie in jeder Region einen Agenten, damit Sie LB- und GLB-Konfigurationen auf den verwalteten Instanzen konfigurieren können. Die LB- und GLB-Konfigurationen können einen einzelnen Agenten gemeinsam nutzen. Weitere Informationen zu den oben genannten drei Aufgaben finden Sie unter Erste Schritte.

4. Bereitstellen von Lastausgleichsdiensten in Microsoft Azure/AWS-Cloud/lokalen Rechenzentren.

   Je nach Art der Load Balancer, die Sie in der Cloud und lokal bereitstellen, stellen Sie diese entsprechend bereit. Sie können beispielsweise Citrix ADC VPX-Instanzen in einem Microsoft Azure Resource Manager (ARM) -Portal, in einer virtuellen privaten Cloud von Amazon Web Services (AWS) und in on-premises Rechenzentren bereitstellen. Konfigurieren Sie Citrix ADC-Instanzen für die Funktion als LB- oder GLB-Knoten im eigenständigen Modus, indem Sie die virtuellen Maschinen erstellen und andere Ressourcen konfigurieren. Weitere Informationen zum Bereitstellen von Citrix ADC VPX Instanzen finden Sie in den folgenden Dokumenten:

   - Starten des Citrix ADC VPX für AWS AMI.
   - Konfigurieren von Citrix ADC VPX im eigenständigen Modus in Azure Resource Manager.

5. Führen Sie Sicherheitskonfigurationen durch.

   Konfigurieren Sie Netzwerksicherheitsgruppen und Netzwerk-ACLs in ARM oder AWS, um eingehenden und ausgehenden Datenverkehr für Ihre Instanzen und Subnetze zu steuern.

6. Fügen Sie Citrix ADC-Instanzen in Citrix ADM hinzu.

   Citrix ADC-Instanzen sind Netzwerk-Appliances oder virtuelle Appliances, die Sie von Citrix ADM aus ermitteln, verwalten und überwachen möchten. Um diese Instanzen zu verwalten und zu überwachen, müssen Sie die Instanzen dem Dienst hinzufügen und sowohl LB (wenn Sie Citrix ADC für LB verwenden) als auch GLB-Instanzen registrieren. Weitere Informationen zum Hinzufügen von Citrix ADC-Instanzen im Citrix ADM finden Sie unterSchnelleinstieg.

7. Implementieren Sie die GLB- und LB-Konfigurationen mit standardmäßigen Citrix ADM StyleBooks.

   - Verwenden Sie **Multi-Cloud GLB StyleBook**, um die GLB-Konfiguration auf den ausgewählten GLB Citrix ADC-Instanzen auszuführen.
   - Implementieren Sie die Lastausgleichskonfiguration. (Sie können diesen Schritt überspringen, wenn Sie bereits über LB-Konfigurationen für die verwalteten Instanzen verfügen.)

   Sie können Load Balancer auf Citrix ADC-Instanzen auf zwei Arten konfigurieren:

- Konfigurieren Sie die Instanzen für den Lastenausgleich der Anwendungen manuell. Weitere Informationen zum manuellen Konfigurieren der Instanzen finden Sie unter Grundlegender Lastenausgleich einrichten.
- Verwenden Sie StyleBooks. Sie können eines der Citrix ADM StyleBooks (HTTP/SSL Load-Balancing StyleBook oder HTTP/SSL LoadBalancing (mit Monitoren) StyleBook) verwenden, um die Load Balancer-Konfiguration auf der ausgewählten Citrix ADC-Instanz zu erstellen. Sie können auch Ihre eigenen StyleBooks erstellen. Weitere Informationen zu StyleBooks finden Sie unter StyleBooks.

8. Verwenden Sie **Multi-Cloud GLB StyleBook for LB Node**, um die GLB Parent-Child-Topologie in einem der folgenden Fälle zu konfigurieren:

   - Wenn Sie die metrik-basierten GLB-Algorithmen (Kleinste Pakete, geringste Verbindungen, geringste Bandbreite) verwenden, um GLB- und LB-Knoten zu konfigurieren und wenn die LB-Knoten auf einer anderen Citrix ADC-Instanz bereitgestellt werden.
   - Wenn Site-Persistenz erforderlich ist.

Verwenden von StyleBooks zum Konfigurieren von GLB

April 28, 2021

Mit dem Multi-Cloud-GLB-StyleBook können Sie GLB-Konfigurationen auf Citrix ADC-Instanzen konfigurieren, die in Ihren Rechenzentren bereitgestellt werden. Stellen Sie sicher, dass Sie die Standort-IP-Adresse auf der Citrix ADC GLB-Instanz in jedem Rechenzentrum konfiguriert haben.

Sie können dieses StyleBook auch verwenden, um eine übergeordnete Website zu erstellen, die untergeordnete Websites akzeptiert, die Sie später in den GLB-Knoten hinzufügen können. Konfigurieren der GLB-Multi-Cloud-Konfiguration auf Citrix ADC-Instanzen

1. Navigieren Sie zu **Anwendungen** > **Konfiguration**, und klicken Sie auf **Neu erstellen**.
2. Auf der Seite **StyleBook auswählen** werden alle StyleBooks angezeigt, die Sie im Citrix Application Delivery Management (ADM) verwenden können. Scrollen Sie nach unten und wählen Sie **Multi-Cloud GLB StyleBook**.

   Das Multi-Cloud-GLB-StyleBook wird verwendet, um GLB für eine Anwendung zu konfigurieren, die in mehreren Clouds und lokalen Standorten bereitgestellt wird. Das StyleBook wird als Benutzeroberflächenseite angezeigt, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

   > **Hinweis**
   >
   > Die Begriffe Rechenzentrum und Standorte werden in diesem Dokument austauschbar ver-

> wendet.

3. Legen Sie die folgenden Parameter fest:

    - **Anwendungsname**. Geben Sie den Namen der Anwendung ein, die auf den GLB-Sites bereitgestellt wird.
    - **GLB-Algorithmus**. Wählen Sie den globalen Load Balancing-Algorithmus (Methode), um den Standort auszuwählen, der einem Client dient. The options that are available in the drop-down list box are LEASTCONNECTION, LEASTBANDWIDTH, LEASTPACKETS, ROUNDROBIN, STATICPROXIMITY, SOURCEIPHASH, and RTT.
    - **Geo-Datenbankdatei**. Wenn Sie STATICPROXIMITY als GLB-Algorithmus ausgewählt haben, geben Sie den vollständigen Pfad und den Namen der Datenbankdatei ein, die die statischen Näherungsdaten enthält. Stellen Sie sicher, dass die Datenbankdatei auf allen GLB Citrix ADC-Instanzen am angegebenen Speicherort vorhanden ist. Alternativ können Sie die Standarddatei beibehalten.
    - **-Protokoll**. Wählen Sie das Anwendungsprotokoll der bereitgestellten Anwendung aus dem Dropdownlistenfeld aus.
    - **Persistenzeinstellungen**. Persistenz, die auf einem virtuellen Server konfiguriert ist, verwaltet die Zustände der Verbindungen auf den Servern, die von diesem virtuellen Server dargestellt werden (z. B. Verbindungen, die im E-Commerce verwendet werden). Persistenz überschreibt die Lastausgleichsmethoden, sobald der virtuelle Server ausgewählt ist. Wenn die Persistenzkonfiguration auf einen Dienst angewendet wird, der DOWN ist, verwendet die Instanz die Lastausgleichsmethoden, um einen neuen Dienst auszuwählen, und der neue Dienst wird für nachfolgende Anforderungen vom Client persistent.
    - **Persistenzart**. Wählen Sie den Persistenztyp aus, der für diese Anwendung verwendet werden soll. Wenn Sie z. B. Persistenz als SOURCEIP auswählen, werden nach der ersten Auswahl der Site, auf der die Anwendung gehostet wird, alle nachfolgenden Anforderungen desselben Clients an diese Site gesendet, um Zugriff auf die Dienste der Anwendung zu erhalten.
    - **Persistenz-Timeout**. Wenn Sie SOURCEIP als Persistenztyp ausgewählt haben, geben Sie die Anzahl der Minuten ein, bevor die Persistenzsitzung nach der letzten Clientanforderung abläuft. Die Reichweite beträgt 2 bis 1440 Minuten. Die Minuten werden in Sekunden aufgelöst.

4. **Spillover-Einstellungen**. Konfigurieren Sie die Spillover-Funktion, um die Spillover-Verbindungen an einen sekundären oder virtuellen Backup-Server weiterzuleiten, wenn z. B. das Verbindungslimit oder die Bandbreitengrenze des primären virtuellen Servers den Schwellenwert erreicht hat.

    - **Spillover-Methode**. Wählen Sie im Dropdownlistenfeld die Methode des Spillover-Verfahrens aus. Beispielsweise überwacht die CONNECTION Spillover-Methode die Anzahl der Verbindungen, die auf dem primären Server aktiv sind. Wenn für diese

Methode der Spillover-Schwellenwert erreicht wird, werden neue Verbindungen auf den ersten verfügbaren virtuellen Server in der Sicherungskette umgeleitet. Die HEALTH Spillover-Methode ermöglicht es Ihnen, Spillover, wenn der Schwellenwert unter einen konfigurierten Schwellenwert fällt. Zum Beispiel weniger als 70%.

> **Hinweis**
>
> Mit Ausnahme der Spillover-Methode HEALTH sind andere Methoden nur anwendbar, wenn Citrix ADC als Load Balancer-Instanz verwendet wird.

- **Spilloverschwelle.** Geben Sie einen Schwellenwert für die ausgewählte Spillover-Methode ein.
- **Spillover-Persistenz.** Aktivieren Sie Spillover-Persistence, wenn der virtuelle Backup-Server die empfangenen Anforderungen weiterhin verarbeiten soll, auch wenn die Last auf dem primären Schwellenwert unterschritten wird.
- **Spillover Persistence Timeout**. Konfigurieren Sie den Zeitraum, für den die Spillover-Persistenz wirksam ist. Der Mindestwert beträgt 2 Minuten und der Höchstwert beträgt 1440 Minuten. Die Minuten werden in Sekunden aufgelöst.

5. **Persistenz-/Spillover-Persistenz-ID**. Wenn Sie SOURCEIP als Persistenztyp ausgewählt haben oder wenn die Spillover-Persistenz aktiviert ist, geben Sie eine eindeutige Nummer ein, um dieselbe Domäne auf allen GLB-Appliances zu identifizieren. Der Bereich liegt zwischen 1 und 65535.
    - **Integritätsprüfung von GLB-Service-Endpunkten (optional)**
    - **Typ der Zustandsprüfung**. Wählen Sie im Dropdownlistenfeld den Typ des Prüfpunkts aus, der zum Überprüfen der Integrität der VIP-Adresse des Load Balancer verwendet wird, die die Anwendung auf einer Site darstellt.
    - **Sicherer Modus**. (Optional) Wählen Sie **Ja**, um diesen Parameter zu aktivieren, wenn SSL-basierte Integritätsprüfungen erforderlich sind.
    - **HTTP-Anforderung**. (Optional) Wenn Sie HTTP als Statusprüfungstyp ausgewählt haben, geben Sie die vollständige HTTP-Anforderung ein, die zum Prüfen der VIP-Adresse verwendet wird.
    - **Liste der HTTP-Statusantwortcodes**. (Optional) Wenn Sie HTTP als Integritätsprüfung ausgewählt haben, geben Sie die Liste der HTTP-Statuscodes ein, die in Antworten auf HTTP-Anforderungen erwartet werden, wenn der VIP fehlerfrei ist.
6. **GLB-Domänennamen**. In diesem Abschnitt können Sie die Liste der DNS-Domänennamen konfigurieren, die dieser Anwendung zugeordnet sind. Klicken Sie auf das Plussymbol (**+**), um einen DNS-Domänennamen für die Anwendung zu erstellen.
7. **GLB-Seiten**. In diesem Abschnitt können Sie die Liste der Websites konfigurieren, auf denen diese Anwendung bereitgestellt wird.

Der GLB-Standort ist die oberste Entität für die GLB-Kommunikation. Die beim Konfigurieren des Standorts angegebenen Informationen werden zum Verknüpfen lokaler Standorte mit Remotestandorten und zur Freigabe von Überwachungsdaten mithilfe des Citrix Metrics Exchange-Protokolls (MEP) verwendet. Die IP-Adresse gehört der GLB Citrix ADC-Instanz und verwendet TCP-Port 3009. Im Abschnitt GLB Sites im StyleBook können Sie beliebig viele GLB-Sites angeben.

Klicken Sie auf das Plus-Symbol (**+**), um Websites hinzuzufügen.

- **Standortname**. Geben Sie den Namen der Site ein.
- **IP-Adresse des Standorts**. Geben Sie die IP-Adresse ein, die die Site als Quell-IP-Adresse verwendet, wenn Metriken mit anderen Sites ausgetauscht werden. Es wird davon ausgegangen, dass diese IP-Adresse bereits auf der GLB-Instanz an jedem Standort konfiguriert ist.
- **Öffentliche IP-Adresse des Standorts**. (Optional) Geben Sie die öffentliche IP-Adresse des Standorts ein, der zum Austausch von Metriken verwendet wird, wenn für die IP-Adresse dieses Standorts NAT verwendet wird.

8. **Untergeordnete Websites**. Klicken Sie auf das Plus-Symbol (+), um die erforderlichen untergeordneten Sites zu konfigurieren.

   - **Name der untergeordneten Website**. Geben Sie den Namen der Site ein.
   - **IP-Adresse des untergeordneten Standorts**. Geben Sie die IP-Adresse der untergeordneten Site ein. Verwenden Sie hier die private IP-Adresse oder SNIP des Citrix ADC Knotens, der als untergeordneter Standort konfiguriert wird.
   - **Öffentliche IP-Adresse des Standorts**. (Optional) Geben Sie die öffentliche IP-Adresse des Standorts ein, der zum Austausch von Metriken verwendet wird, wenn für die IP-Adresse dieses Standorts NAT verwendet wird.

9. **Services Site Persistenz**. Wählen Sie den Typ der Persistenz aus dem Dropdownlistenfeld aus, der für die GLB-Dienste auf der Site verwendet werden soll.

   - Wählen Sie ConnectionProxy aus, damit der Standort eine Verbindung mit dem GLB-Site herstellen kann, der das Site-Cookie eingefügt hat, die Clientanforderung an den ursprünglichen Standort versendet, eine Antwort vom ursprünglichen GLB-Site erhalten, die Antwort an den Client weiterleiten und die Verbindung schließen kann.
   - Wählen Sie `HTTPRedirect` diese Option aus, um der Website zu erlauben, die Anfrage an die Website umzuleiten, die das Cookie ursprünglich eingefügt hat. Weitere Hinweise zur Persistenz finden Sie unter Persistente Verbindungen konfigurieren.

10. **Aktive GLB-Dienste**: In diesem Abschnitt können Sie die Liste der aktiven Dienste auf den Sites konfigurieren, auf denen die Anwendung bereitgestellt wird.

    Dienst-IP. Geben Sie die IP-Adresse des GLB-Dienstes auf dieser Website ein.

- **Öffentliche IP-Adresse des Dienstes**. Wenn die virtuelle IP-Adresse privat ist und über eine öffentliche IP-Adresse verfügt, geben Sie die öffentliche IP-Adresse an.
- **Dienstport**. Geben Sie den Port des GLB-Dienstes auf dieser Website ein.
- **Dienstgewicht**. Geben Sie das Gewicht ein, das dem GLB-Dienst zugewiesen ist.

  > **Hinweis**
  >
  > Sie können den Diensten relative Gewichtung zuweisen, abhängig vom Prozentsatz des Datenverkehrs, der an die Cloud gesendet werden muss, und dem Prozentsatz des Datenverkehrs, der on-premises abgewickelt werden muss. Wenn Sie beispielsweise dem Cloud-basierten GLB-Dienst eine Gewichtung von 3 und dem lokalen GLB-Dienst 7 zugewiesen haben, werden 30% des Datenverkehrs an die Cloud geleitet und 70% werden on-premises abgewickelt.

- **Standortname**. Geben Sie den Namen der Site ein, auf der sich der GLB-Dienst befindet.
- **Site-Präfix**. Geben Sie ein Präfix für die Site ein, auf der der GLB-Dienst konfiguriert ist. Dies ist anwendbar, wenn die Standortpersistenz aktiviert ist und die Methode lautet `httpredirect`. Der Standortpräfixwert muss für alle GLB-Dienste einer Anwendung eindeutig sein.
- **Max. Clientverbindungen**. Geben Sie die maximalen Clientverbindungen ein, die im GLB-Dienst konfiguriert sind, wenn Sie in den Einstellungen für die **Spillover-Persistenz** DYNAMICCONNECTION als Spillover-Methode ausgewählt haben. Wenn Sie keinen Wert angeben, weist das System standardmäßig den maximal konfigurierenden Clientverbindungen eine Nummer zu.

11. **Passive GLB-Dienste**: In diesem Abschnitt können Sie die Liste der passiven Dienste auf den Standorten konfigurieren, an denen die Anwendung mit einer aktiv-passiven Topologie bereitgestellt wird. Stellen Sie Informationen für alle GLB-Backup-Dienste bereit, die den Informationen entsprechen, die Sie für aktive GLB-Dienste bereitgestellt haben.
12. Klicken Sie auf **Zielinstanzen**, und wählen Sie die Citrix ADC-Instanzen aus, die als GLB-Instanzen an jedem Standort konfiguriert sind, auf dem die GLB-Konfiguration bereitgestellt werden soll.
13. Klicken Sie auf **Erstellen**, um die GLB-Konfiguration für die ausgewählten Citrix ADC-Instanzen zu erstellen. Sie können auch auf **Dry Run** klicken, um die Objekte zu überprüfen, die in den Zielinstanzen erstellt werden. Die von Ihnen erstellte StyleBook-Konfiguration (Config Pack) wird in der Liste der Konfigurationen auf der Seite Konfigurationen angezeigt. Sie können diese Konfiguration (Config Pack) mit der Citrix ADM GUI überprüfen, aktualisieren oder entfernen.

Verwenden von StyleBooks zum Konfigurieren von GLB auf Citrix ADC LB-Knoten

April 28, 2021

Sie können das **Multi-Cloud GLB StyleBook for LB Node** verwenden, wenn Sie GLB- und LB-Knoten mit metrik-basierten GLB-Algorithmen (Least Packets, Least Connections, Least Bandwidth) konfigurieren und wenn die LB-Knoten auf einer anderen Citrix ADC-Instanz bereitgestellt werden.

Sie können dieses StyleBook auch verwenden, um zusätzliche untergeordnete Websites für eine vorhandene übergeordnete Website zu konfigurieren. Dieses StyleBook konfiguriert jeweils eine untergeordnete Website. Erstellen Sie also so viele Konfigurationen (Konfigurationspakete) aus diesem StyleBook, wie es untergeordnete Websites gibt. Das StyleBook wendet die GLB-Konfiguration auf die untergeordneten Sites an. Sie können maximal 1024 untergeordnete Sites konfigurieren.

> **Hinweis**
>
> Verwenden SieMulti-Cloud GLB StyleBookdiese Option, um die übergeordneten Sites zu konfigurieren.

Dieses StyleBook macht die folgenden Annahmen:

- Eine SNIP-Adresse oder eine GLB-Standort-IP-Adresse wird konfiguriert.
- Die erforderlichen Firewall- und Sicherheitsgruppen werden in den Cloud-Dienstanbietern konfiguriert.

Konfigurieren einer untergeordneten Site in einer über-/untergeordneten Topologie mithilfe von Multi-Cloud GLB StyleBook für LB-Knoten

1. Navigieren Sie zu **Anwendungen** > **Konfiguration**, und klicken Sie auf **Neu erstellen**.
2. Auf der Seite **StyleBook auswählen** werden alle StyleBooks angezeigt, die für Ihre Verwendung in Citrix Application Delivery Management (ADM) verfügbar sind. Scrollen Sie nach unten und wählen Sie **Multi-Cloud GLB StyleBook for LB Node.**

   Das StyleBook wird als Benutzeroberflächenseite angezeigt, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

   > **Hinweis**
   >
   > Die Begriffe Rechenzentrum und Standorte werden in diesem Dokument austauschbar verwendet.

3. Legen Sie die folgenden Parameter fest:

   - **Anwendungsname**. Geben Sie den Namen der GLB-Anwendung ein, die auf den GLB-Sites bereitgestellt wird, für die Sie untergeordnete Sites erstellen möchten.

- **-Protokoll**. Wählen Sie das Anwendungsprotokoll der bereitgestellten Anwendung aus dem Dropdownlistenfeld aus.
- **LB-Zustandsprüfung (optional)**
  - **Typ der Zustandsprüfung**. Wählen Sie im Dropdownlistenfeld den Typ des Prüfpunkts aus, der zum Überprüfen der Integrität der VIP-Adresse des Load Balancer verwendet wird, die die Anwendung auf einer Site darstellt.
  - **Sicherer Modus**. (Optional) Wählen Sie **Ja**, um diesen Parameter zu aktivieren, wenn SSL-basierte Integritätsprüfungen erforderlich sind.
  - **HTTP-Anforderung**. (Optional) Wenn Sie HTTP als Statusprüfungstyp ausgewählt haben, geben Sie die vollständige HTTP-Anforderung ein, die zum Prüfen der VIP-Adresse verwendet wird.
  - **Liste der HTTP-Statusantwortcodes**. (Optional) Wenn Sie HTTP als Integritätsprüfung ausgewählt haben, geben Sie die Liste der HTTP-Statuscodes ein, die in Antworten auf HTTP-Anforderungen erwartet werden, wenn der VIP fehlerfrei ist.

4. Die übergeordnete Site wird konfiguriert.

   Geben Sie die Details des übergeordneten Standorts (GLB-Knoten) an, unter dem Sie den untergeordneten Standort (LB-Knoten) erstellen möchten.

   - **Standortname**. Geben Sie den Namen der übergeordneten Website ein.
   - **IP-Adresse des Standorts**. Geben Sie die IP-Adresse ein, die die übergeordnete Site als SourceIP Adresse verwendet, wenn Metriken mit anderen Sites ausgetauscht werden. Es wird davon ausgegangen, dass diese IP-Adresse bereits auf dem GLB-Knoten an jedem Standort konfiguriert ist.
   - **Öffentliche IP-Adresse des Standorts**. (Optional) Geben Sie die öffentliche IP-Adresse des übergeordneten Standorts ein, der zum Austausch von Metriken verwendet wird, wenn für die IP-Adresse dieses Standorts NAT verwendet wird.

5. Untergeordnete Site wird konfiguriert.

   Geben Sie die Details der untergeordneten Website an.

   - **Standortname**. Geben Sie den Namen der Site ein.
   - **IP-Adresse des Standorts**. Geben Sie die IP-Adresse der untergeordneten Site ein. Verwenden Sie hier die private IP-Adresse oder SNIP des Citrix ADC Knotens, der als untergeordneter Standort konfiguriert wird.
   - **Öffentliche IP-Adresse des Standorts**. (Optional) Geben Sie die öffentliche IP-Adresse des untergeordneten Standorts ein, der zum Austausch von Metriken verwendet wird, wenn für die IP-Adresse dieses Standorts NAT verwendet wird.

6. Konfigurieren aktiver GLB-Dienste (optional)

   Konfigurieren Sie aktive GLB-Dienste nur, wenn die IP-Adresse des virtuellen LB-Servers keine öffentliche IP-Adresse ist. In diesem Abschnitt können Sie die Liste der lokalen GLB-Dienste auf

den Sites konfigurieren, auf denen die Anwendung bereitgestellt wird.

- **Dienst-IP**. Geben Sie die IP-Adresse des virtuellen Lastausgleichsservers auf dieser Site ein.
- **Öffentliche IP-Adresse des Dienstes**. Wenn die virtuelle IP-Adresse privat ist und über eine öffentliche IP-Adresse verfügt, geben Sie die öffentliche IP-Adresse an.
- **Dienstport**. Geben Sie den Port des GLB-Dienstes auf dieser Website ein.
- **Standortname**. Geben Sie den Namen der Site ein, auf der sich der GLB-Dienst befindet.

7. Klicken Sie auf **Zielinstanzen**, und wählen Sie die Citrix ADC-Instanzen aus, die als GLB-Instanzen an jedem Standort konfiguriert sind, auf dem die GLB-Konfiguration bereitgestellt werden soll.
8. Klicken Sie auf **Erstellen**, um die LB-Konfiguration auf der ausgewählten Citrix ADC-Instanz (LB-Knoten) zu erstellen. Sie können auch auf **Dry Run** klicken, um die Objekte zu überprüfen, die in den Zielinstanzen erstellt werden. Die von Ihnen erstellte StyleBook-Konfiguration wird in der Liste der Konfigurationen auf der Seite Konfigurationen angezeigt. Sie können diese Konfiguration mithilfe der Citrix ADM GUI untersuchen, aktualisieren oder entfernen.

Infrastrukturanalyse

April 28, 2021

Ein wichtiges Ziel für Netzwerkadministratoren ist die Überwachung von Citrix ADC-Instanzen. ADC-Instanzen bieten interessante Einblicke in die Nutzung und Leistung von Anwendungen und Desktops, auf die über sie zugegriffen wird. Administratoren müssen die ADC-Instanz überwachen und die von jeder ADC-Instanz verarbeiteten Anwendungsflüsse analysieren. Administratoren müssen auch in der Lage sein, mögliche Probleme bei Konfiguration, Einrichtung, Konnektivität, Zertifikaten und anderen Auswirkungen auf die Anwendungsnutzung oder -leistung zu beheben. Zum Beispiel kann eine plötzliche Änderung des Anwendungsdatenverkehrsmusters auf Änderungen in der SSL-Konfiguration wie die Deaktivierung eines SSL-Protokolls zurückzuführen sein. Administratoren müssen in der Lage sein, die Korrelation zwischen diesen Datenpunkten schnell zu identifizieren, um Folgendes sicherzustellen:

- Anwendungsverfügbarkeit ist in einem optimalen Zustand
- Es gibt keine Probleme mit Ressourcenverbrauch, Hardware, Kapazität oder Konfigurationsänderungen.
- Es gibt keine ungenutzten Lagerbestände
- Es gibt keine abgelaufenen Zertifikate

Infrastructure Analytics Funktion vereinfacht den Prozess der Datenanalyse, indem mehrere Datenquellen korreliert und mit einem messbaren Score quantifiziert werden, der den Zustand einer Instanz definiert. Mit dieser Funktion erhalten Administratoren einen einzigen Berührungspunkt, um das Problem, den Ursprung des Problems und mögliche Korrekturen zu verstehen, die sie durchführen können.

Infrastrukturanalysen in Citrix ADM

Mit der Funktion Infrastructure Analytics werden alle aus den Citrix ADC-Instanzen gesammelten Daten zusammengefasst und in einen **Instanz-Score** quantifiziert, der die Integrität der Instanzen definiert. Die Instanzbewertung wird über Tabellenansicht oder als Circle Pack-Visualisierung zusammengefasst. Mit der Funktion Infrastructure Analytics können Sie die Faktoren visualisieren, die zu einem Problem in den Instanzen geführt haben oder zu einem Problem führen könnten. Diese Visualisierung hilft Ihnen auch, die Aktionen zu bestimmen, die ausgeführt werden müssen, um das Problem und seine Wiederholung zu verhindern.

Instanzbewertung

Instanzbewertung gibt den Zustand einer ADC-Instanz an. Eine Punktzahl von 100 bedeutet eine vollkommen gesunde Instanz ohne Probleme. Die Instanzbewertung erfasst verschiedene Ebenen potenzieller Probleme in der Instanz. Es ist eine quantifizierbare Messung der Instanzgesundheit und mehrere Gesundheitsindikatoren tragen zur Bewertung bei.

Integritätsindikatoren sind die Bausteine der Instanzbewertung, wobei die Bewertung regelmäßig für einen vordefinierten Überwachungszeitraum berechnet wird, basierend auf allen erkannten Indikatoren in diesem Zeitfenster. Derzeit berechnet Infrastructure Analytics die Instanzbewertung einmal stündlich basierend auf den Daten, die von den Instanzen erfasst wurden.
Ein Indikator kann als jede Aktivität (ein Ereignis oder ein Problem) definiert werden, die zu einer der folgenden Kategorien auf den Instanzen gehört.

- Systemressourcenindikatoren
- Indikatoren für kritische Ereignisse
- SSL-Konfigurationsindikatoren
- Konfigurationsabweichungsindikatoren

Gesundheitsindikatoren erläutert

- Systemressourcen-Indikatoren

  Im Folgenden finden Sie die kritischen Systemressourcenprobleme, die auf Citrix ADC-Instanzen auftreten und von Citrix ADM überwacht werden können.

- **Hohe CPU-Auslastung**. Die CPU-Auslastung hat den höheren Schwellenwert in der Citrix ADC-Instanz überschritten.
- **Hohe Speichernutzung**. Die Speicherauslastung hat den höheren Schwellenwert in der Citrix ADC-Instanz überschritten.
- **Hohe Datenträgernutzung**. Die Datenträgerauslastung hat den höheren Schwellenwert in der Citrix ADC-Instanz überschritten.
- **Datenträgerfehler**. Fehler auf Festplatte 0 oder Festplatte 1 auf dem Hypervisor, auf dem die ADC-Instanz installiert ist.
- **Stromausfall**. Die Stromversorgung ist ausgefallen oder von der ADC-Instanz getrennt.
- **SSL-Kartenfehler**. Die auf der Instanz installierte SSL-Karte ist fehlgeschlagen.
- **Flash-Fehler**. Bei der Citrix ADC-Instanz sind Compact Flash Fehler aufgetreten.
- **NIC wird verworfen**. Die von der NIC-Karte verworfenen Pakete haben den höheren Schwellenwert in der Citrix ADC-Instanz überschritten.

Weitere Informationen zu diesen Systemressourcenfehlern finden Sie unterInstanz-Dashboard.

- Indikatoren für kritische Ereignisse

  Die folgenden kritischen Ereignisse werden durch die Ereignisverwaltungsfunktion von ADM identifiziert, die mit kritischem Schweregrad konfiguriert sind.

  - **HA-Synchronisierungsfehler**. Die Konfigurationssynchronisierung zwischen den ADC-Instanzen in hoher Verfügbarkeit ist auf dem sekundären Server fehlgeschlagen.
  - **HA keine Herzschläge**. Der primäre Server in einem Paar von ADC-Instanzen in hoher Verfügbarkeit empfängt keine Herzschläge aus dem sekundären Server.
  - **HA schlechter Sekundärzustand**. Der sekundäre Server in einem Paar von ADC-Instanzen mit hoher Verfügbarkeit befindet sich im Status Heruntergefahren, Unbekannt oder Sekundär bleiben.
  - **HA-Version stimmt nicht überein**. Die Version der ADC-Softwareimages, die auf einem Paar von ADC-Instanzen in hoher Verfügbarkeit installiert sind, stimmt nicht überein.
  - **Fehler bei der Clustersynchronisierung**. Die Konfigurationssynchronisierung zwischen den ADC-Instanzen im Clustermodus ist fehlgeschlagen.
  - **Clusterversion stimmt nicht überein**. Die Version der ADC-Softwareimages, die auf den ADC-Instanzen im Clustermodus installiert sind, stimmt nicht überein.
  - **Clusterausbreitungsfehler**. Die Weitergabe von Konfigurationen an alle Instanzen in einem Cluster ist fehlgeschlagen.

> **Hinweis**
>
> Sie können Ihre Liste der kritischen SNMP-Ereignisse haben, indem Sie den Schweregrad der Ereignisse ändern. Weitere Informationen zum Ändern des Schweregrads finden Sie unterÄndern Sie den gemeldeten Schweregrad der Ereignisse, die auf Citrix ADC-Instanzen auftreten.

Weitere Informationen zu Ereignissen in Citrix ADM finden Sie unterEreignisse.

- SSL-Konfigurationsindikatoren
  - **Nicht empfohlen Schlüsselstärke**. Die Schlüsselstärke der SSL-Zertifikate entspricht nicht den Citrix Standards
  - **Nicht empfohlener Emittent**. Der Aussteller des SSL-Zertifikats wird von Citrix nicht empfohlen.
  - **SSL-Zertifikate sind abgelaufen**. Das in der ADC-Instanz installierte SSL-Zertifikat ist abgelaufen.
  - **SSL-Zertifikate Ablaufdatum fällig**. Das in der ADC-Instanz installierte SSL-Zertifikat läuft in der nächsten Woche ab.
  - **Nicht empfohlene Algorithmen**. Die Signaturalgorithmen von in der ADC-Instanz installierten SSL-Zertifikaten entsprechen nicht den Citrix Standards.

Weitere Informationen zu SSL-Zertifikaten finden Sie unterSSL-Dashboard.

- Konfigurationsabweichungsindikatoren
  - **Config Drift Vorlage**. Es gibt eine Drift (nicht gespeicherte Änderungen) in der Konfiguration aus den Überwachungsvorlagen, die Sie mit bestimmten Konfigurationen erstellt haben, die Sie für bestimmte Instanzen überwachen möchten.
  - **Standardeinstellung für die Konfigurationsdrift**. Es gibt eine Drift (nicht gespeicherte Änderungen) in der Konfiguration aus den Standardkonfigurationsdateien.

Weitere Informationen zu Konfigurationsabweichungen und zum Ausführen von Überwachungsberichten zur Überprüfung der Konfigurationsabweichung finden Sie unterAnzeigen von Überwachungsberichten.

ADC-Kapazitätsprobleme anzeigen

Wenn eine ADC-Instanz die meiste verfügbare Kapazität verbraucht hat, kann ein Paketablegen während der Verarbeitung des Clientdatenverkehrs auftreten. Dieses Problem verursacht eine geringe Leistung in einer ADC-Instanz. Wenn Sie solche ADC-Kapazitätsprobleme verstehen, können Sie zusätzliche Lizenzen proaktiv zuweisen, um die ADC-Leistung zu stabilisieren.

So zeigen Sie ADC-Kapazitätsprobleme an:

1. Navigieren Sie zu **Netzwerke > Infrastructure Analytics**.
2. Erweitern Sie die Instanz, für die Sie Kapazitätsprobleme anzeigen möchten.

Der ADM ruft diese Ereignisse alle fünf Minuten von der ADC-Instanz ab und zeigt die verworfenen Pakete oder Rate-Limit-Zähler-Inkremente an, falls vorhanden. Die Probleme werden nach den folgenden Kapazitätsparametern kategorisiert:

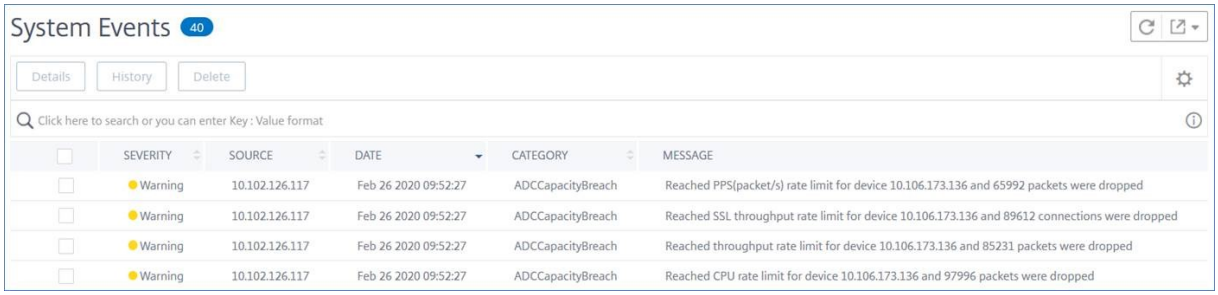
- **Durchsatzlimit erreicht** — Die Anzahl der Pakete, die in der Instanz gelöscht wurden, nachdem das Durchsatzlimit erreicht wurde.
- **PE-CPU-Limit erreicht** - Die Anzahl der Pakete, die auf allen Netzwerkkarten gelöscht wurden, nachdem das PE-CPU-Limit erreicht wurde.
- **PPS Limit erreicht** — Die Anzahl der Pakete, die in der Instanz gelöscht wurden, nachdem das PPS-Limit erreicht wurde.
- **SSL-Durchsatzrate Limit** — Gibt an, wie oft das SSL-Durchsatzlimit erreicht wurde.
- **SSL-TPS Rate Limit** — Gibt an, wie oft das SSL-TPS Limit erreicht wurde.

Der ADM berechnet die Instanzbewertung auf dem definierten Kapazitätsschwellenwert.

- Niedriger Schwellenwert — 1 Schrittweite für Paketabfall oder Ratenbegrenzungszähler
- Hoher Schwellenwert — 10000 Pakete fallen oder Rate-Limit-Zähler-Inkrement

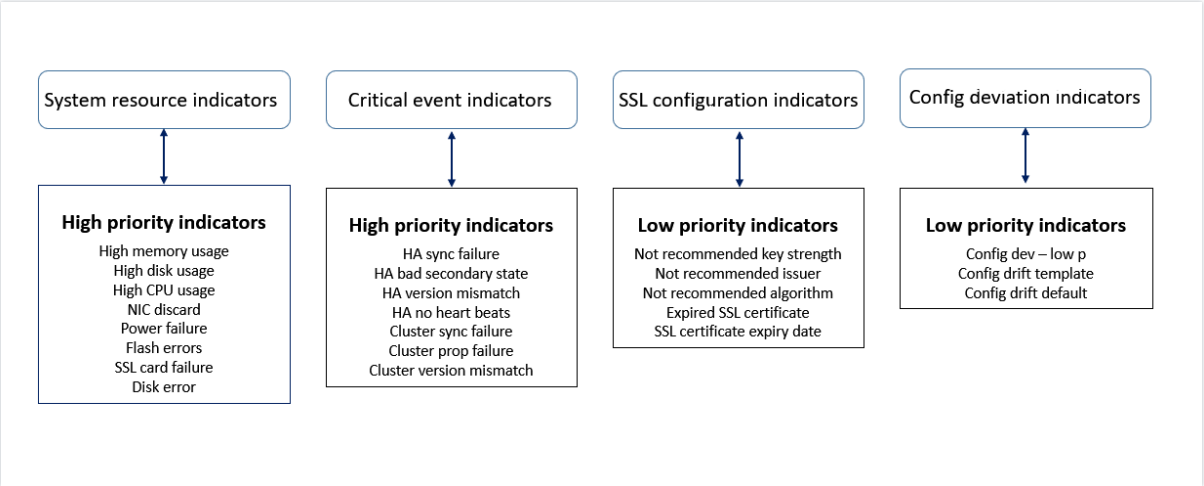
Wenn eine ADC-Instanz den Kapazitätsschwellenwert überschreitet, wird die Instanz-Bewertung beeinträchtigt.

Wenn Pakete fallen oder Rate-Limit Zähler inkrementiert werden, wird ein Ereignis unter der Kategorie `ADCCapacityBreach`generiert. Um diese Ereignisse anzuzeigen, navigieren Sie zu **Konten > Systemereignisse**.



Wert der Gesundheitsindikatoren

Die Indikatoren werden anhand ihrer Werte in Indikatoren mit hoher Priorität und Indikatoren mit niedriger Priorität klassifiziert:



Den Gesundheitsindikatoren innerhalb derselben Gruppe von Indikatoren sind unterschiedliche Gewichte zugewiesen. Ein Indikator kann mehr zur niedrigeren Instanzbewertung beitragen als ein anderer Indikator. Die hohe Speicherauslastung verringert zum Beispiel den Instanzscore mehr als eine hohe Datenträgernutzung, eine hohe CPU-Auslastung und einem NIC-Discard. Wenn eine Instanz eine größere Anzahl von Indikatoren erkannt hat, desto geringer ist die Instanzbewertung.

Der Wert eines Indikators wird anhand der folgenden Regeln berechnet. Der Indikator wird auf eine der folgenden drei Arten erkannt:

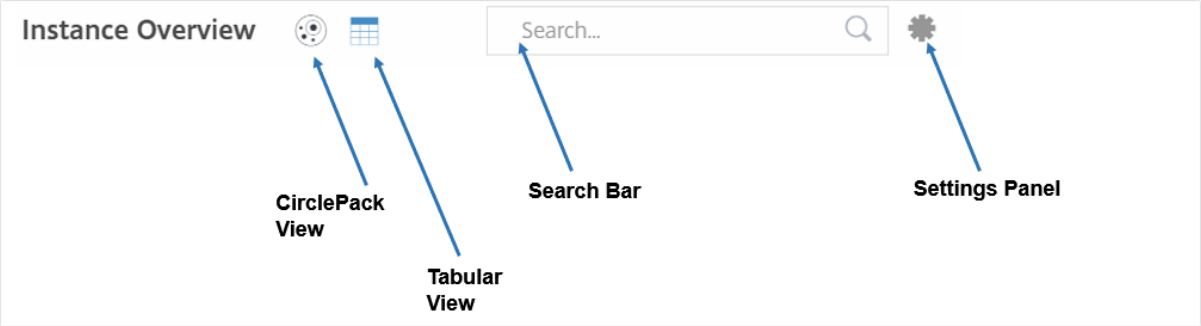
1. **Basierend auf einer Aktivität**. Beispielsweise wird ein Systemressourcenindikator ausgelöst, wenn ein Stromausfall auf der Instanz auftritt, und dieser Indikator reduziert den Wert der Instanzbewertung. Wenn der Indikator gelöscht wird, wird die Strafe gelöscht und die Instanzbewertung erhöht.
2. **Basierend auf der Verletzung des Schwellenwerts**. Beispielsweise wird ein Systemressourcenindikator ausgelöst, wenn die NIC-Karte Pakete verwirft und die Schwellenstufe überschritten wird.
3. **Basierend auf der Verletzung des niedrigen und hohen Schwellenwerts**. Hier kann ein Indikator auf zwei Arten ausgelöst werden:
    - Wenn der Wert des Indikators zwischen niedrigen und hohen Schwellenwerten liegt, wird in diesem Fall eine Teilstrafe für die Instanzbewertung erhoben.
    - Wenn der Wert den hohen Schwellenwert überschreitet, wird in diesem Fall eine volle Strafe für die Instanzbewertung erhoben.
    - Für den Instanzwert wird keine Strafe erhoben, wenn der Wert unter einen niedrigen Schwellenwert fällt.

Beispielsweise ist die CPU-Auslastung ein Systemressourcenindikator, der ausgelöst wird, wenn der Verwendungswert den niedrigen Schwellenwert überschreitet und auch wenn der Wert den hohen Schwellenwert überschreitet.

Dashboard für Infrastrukturanalysen

Navigieren Sie zu **Netzwerke** > **Infrastrukturanalyse**.

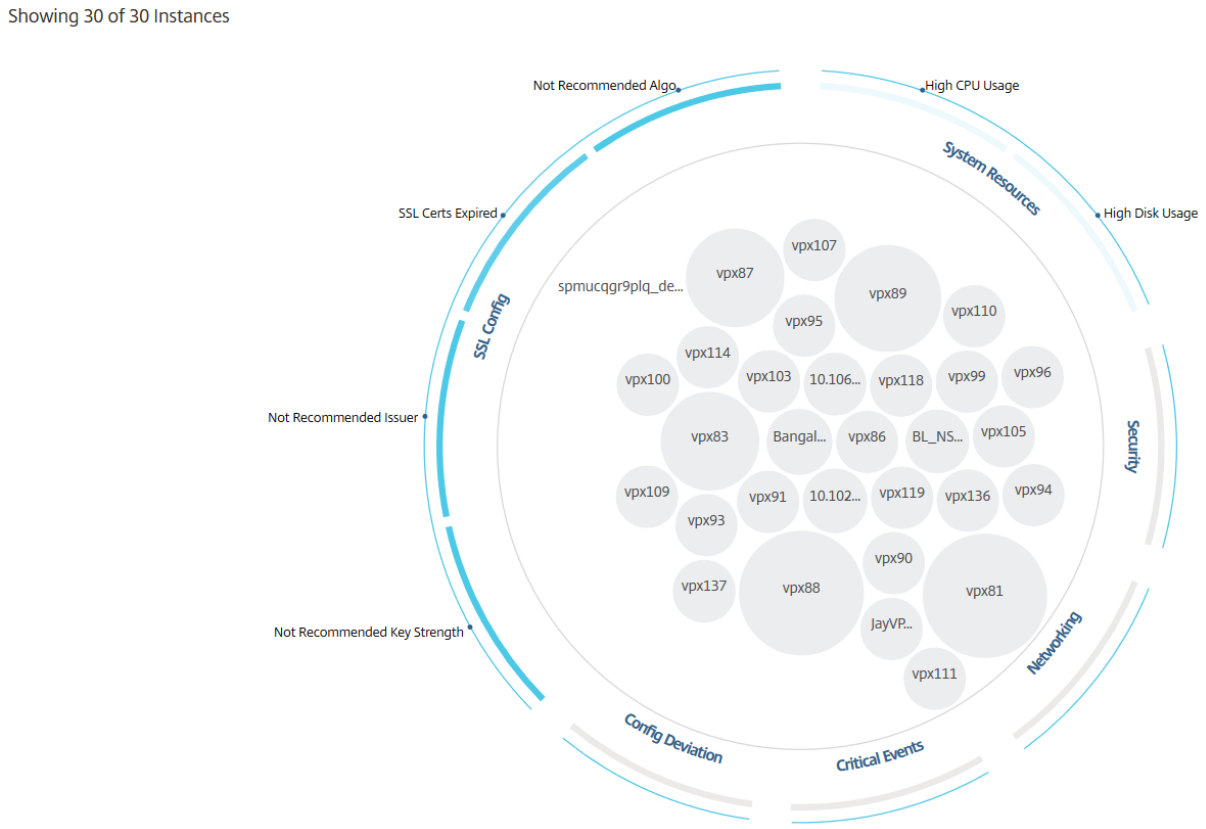
Die Infrastructure Analytics kann im **Circle Pack-** oder **Tabellarformat** angezeigt werden. Sie können zwischen den beiden Formaten wechseln.



- In der tabellarischen Ansicht können Sie nach einer Instanz suchen, indem Sie den Hostnamen oder die IP-Adresse in die Suchleiste eingeben.
- Standardmäßig wird auf der Seite Infrastructure Analytics das Übersichtsfenster auf der rechten Seite der Seite angezeigt.
- Klicken Sie auf das Symbol **Einstellungen**, um das **Einstellungsfenster** anzuzeigen.
- In beiden Ansichtsformaten werden im Zusammenfassungsbereich Details zu allen Instanzen im Netzwerk angezeigt.

Kreispaketansicht

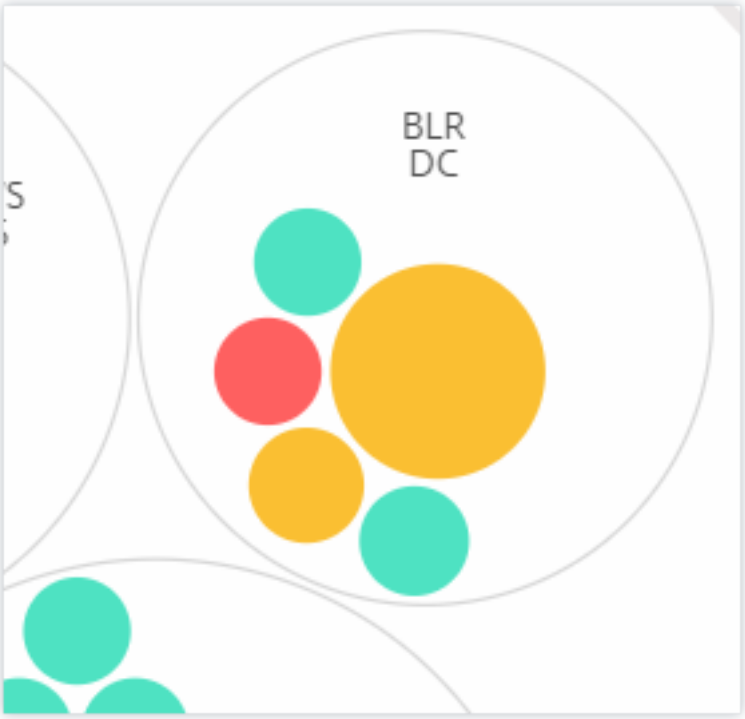
Kreisverpackungsdiagramme zeigen Instanzgruppen als fest organisierte Kreise an. Sie zeigen häufig Hierarchien an, in denen kleinere Instanzgruppen entweder ähnlich wie andere in derselben Kategorie gefärbt sind oder in größeren Gruppen verschachtelt sind. Circle Packs stellen hierarchische Datensätze dar und zeigen verschiedene Ebenen in der Hierarchie und wie sie miteinander interagieren.



Instanzkreise

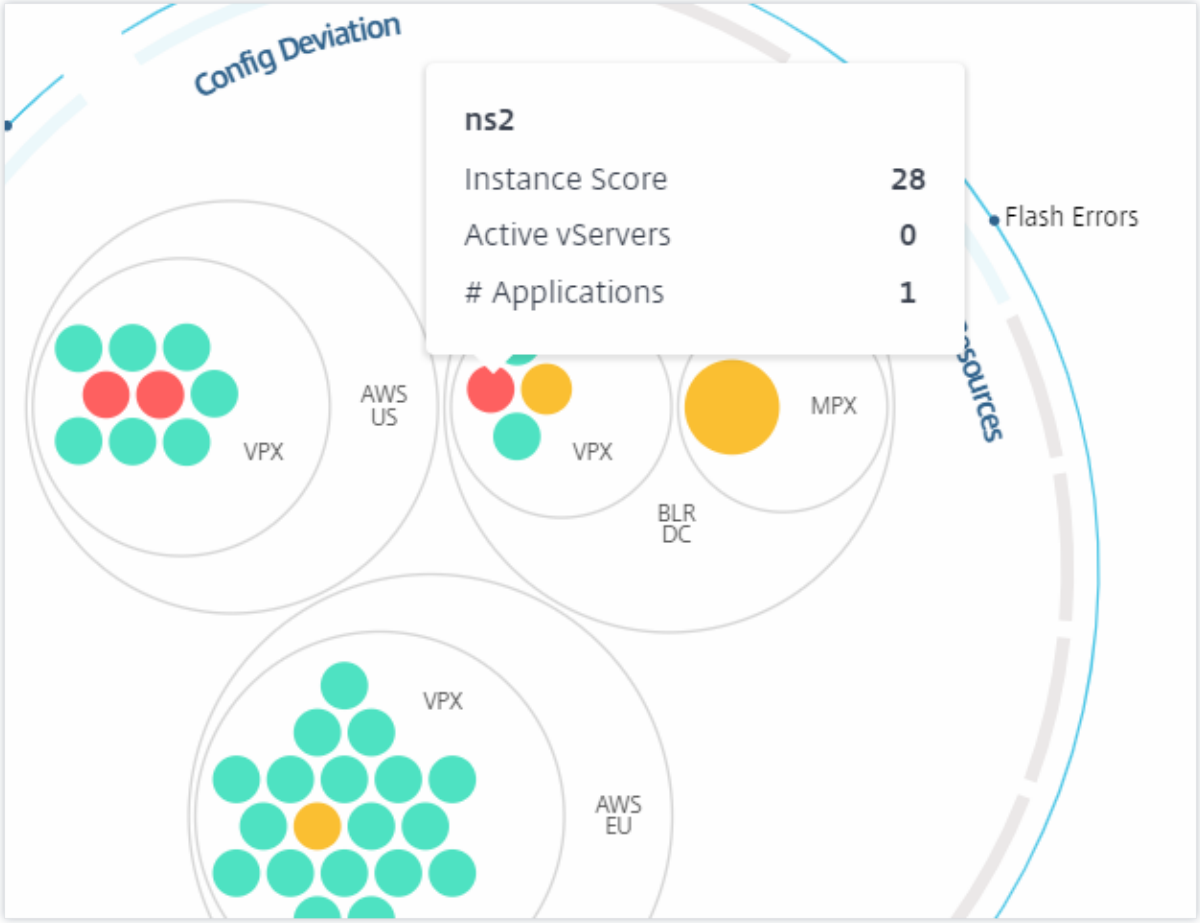
Farbe: Jede Instanz wird im Circle Pack als farbiger Kreis dargestellt. Die Farbe des Kreises zeigt die Integrität dieser Instanz an.

- **Grün** - Instanzwert liegt zwischen 100 und 80. Die Instanz ist fehlerfrei.
- **Gelb** - Instanzbewertung liegt zwischen 80 und 50; einige Probleme wurden bemerkt und müssen überprüft werden.
- **Rot** - Instanzwert liegt unter 50. Die Instanz befindet sich in einem kritischen Stadium, da mehrere Probleme in dieser Instanz auftreten.



Größe: Die Größe dieser farbigen Kreise gibt an, wie viele virtuelle Server auf dieser Instanz konfiguriert sind. Ein größerer Kreis zeigt an, dass eine größere Anzahl virtueller Server vorhanden ist.

Sie können den Mauszeiger auf jeden der Instanzkreise (farbige Kreise) bewegen, um eine Zusammenfassung anzuzeigen. Der Hover-Tooltip zeigt den Hostnamen der Instanz, die Anzahl der aktiven virtuellen Server und die Anzahl der für diese Instanz konfigurierten Anwendungen an.

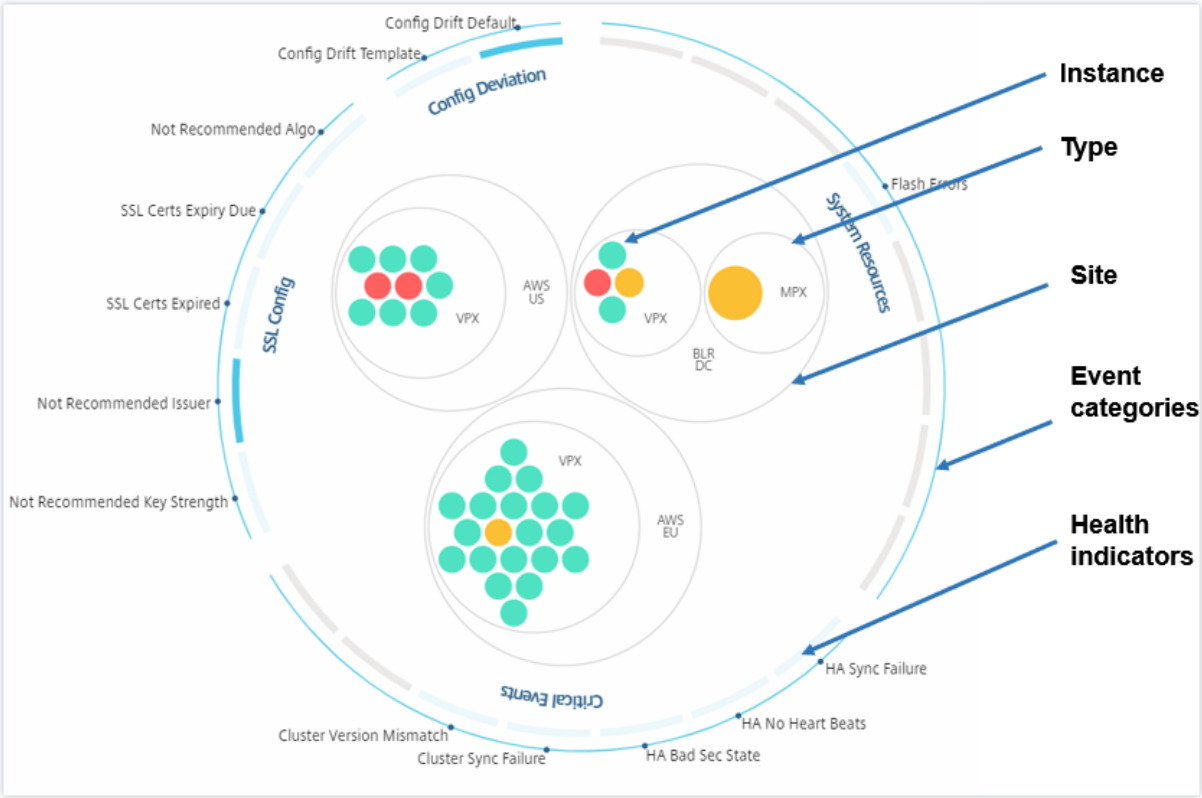


Gruppierte Instanzkreise

Das Circle Pack zu Beginn umfasst Instanzkreise, die nach folgenden Kriterien gruppiert, verschachtelt oder in einen anderen Kreis gepackt werden:

- die Site, auf der sie bereitgestellt werden
- der Typ der bereitgestellten Instanzen - VPX, MPX, SDX und CPX
- das virtuelle oder physische Modell der ADC-Instanz
- die auf den Instanzen installierte ADC-Image-Version

Das folgende Bild zeigt ein Circle Pack, in dem die Instanzen zuerst nach dem Standort oder dem Rechenzentrum gruppiert werden, in dem sie bereitgestellt werden. Anschließend werden sie nach ihrem Typ, VPX und MPX weiter gruppiert.

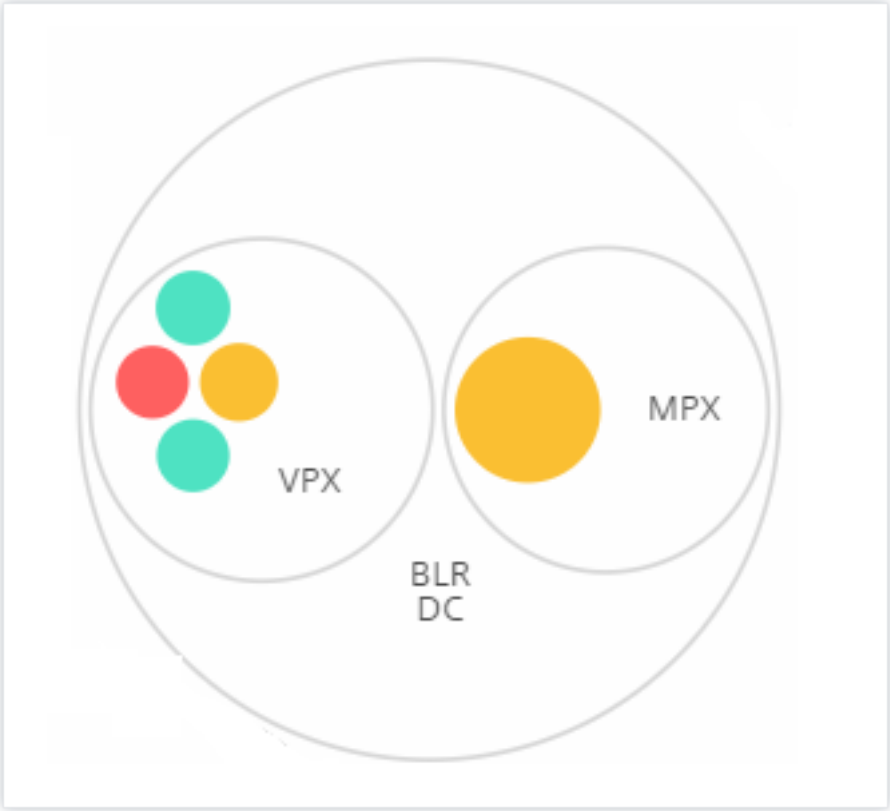


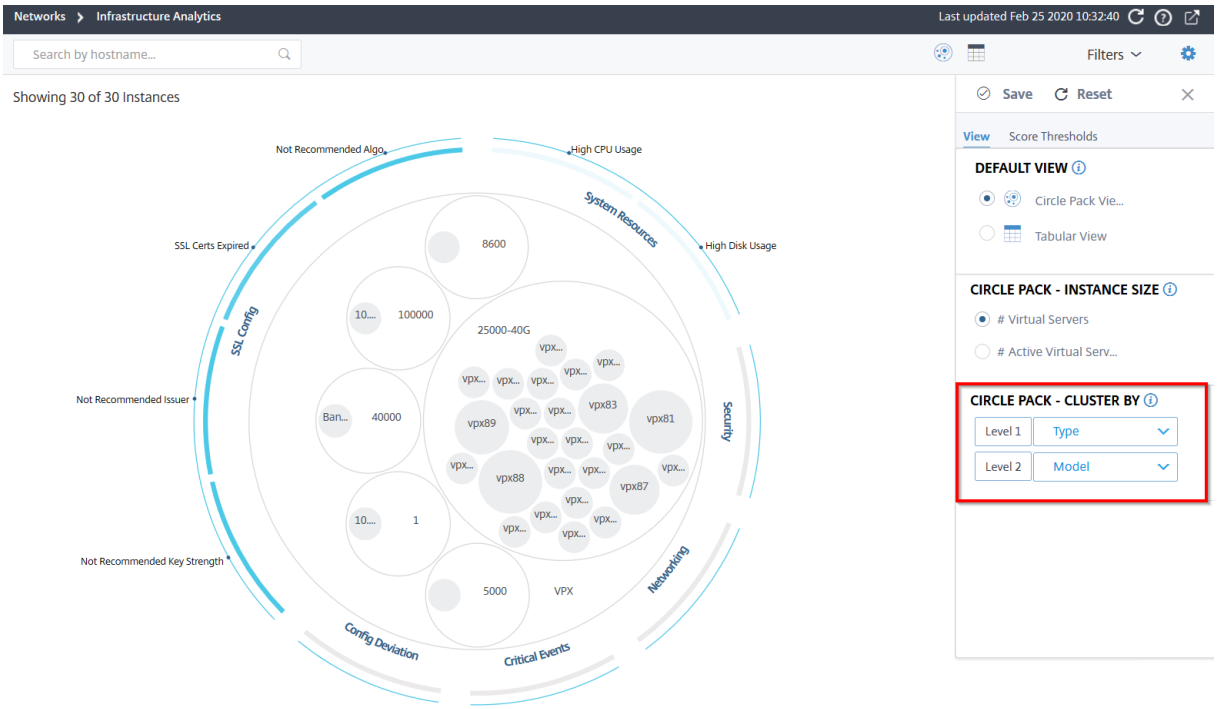
Alle diese verschachtelten Kreise sind durch zwei äußerste Kreise begrenzt. Die beiden äußeren Kreise stellen die vier vom Citrix ADM überwachten Kategorien von Ereignissen dar (Systemressourcen, kritische Ereignisse, SSL-Konfiguration und Konfigurationsabweichung) und die mitwirkenden Integritätsindikatoren.

Cluster-Instanzkreise

Citrix ADM überwacht viele Instanzen. Um die Überwachung und Wartung dieser Instanzen zu vereinfachen, können Sie sie mit Infrastructure Analytics auf zwei Ebenen gruppieren. Das heißt, die Instanzgruppierungen können in einer anderen Gruppierung verschachtelt werden.

Das BLR-Rechenzentrum verfügt beispielsweise über zwei Typen von ADC-Instanzen - VPX und MPX, die darin bereitgestellt werden. Sie können die ADC-Instanzen zuerst nach ihrem Typ gruppieren und dann alle Instanzen nach dem Standort gruppieren, an dem sie gruppiert sind. Sie können nun ganz einfach ermitteln, wie viele Arten von Instanzen in den von Ihnen verwalteten Sites bereitgestellt werden.

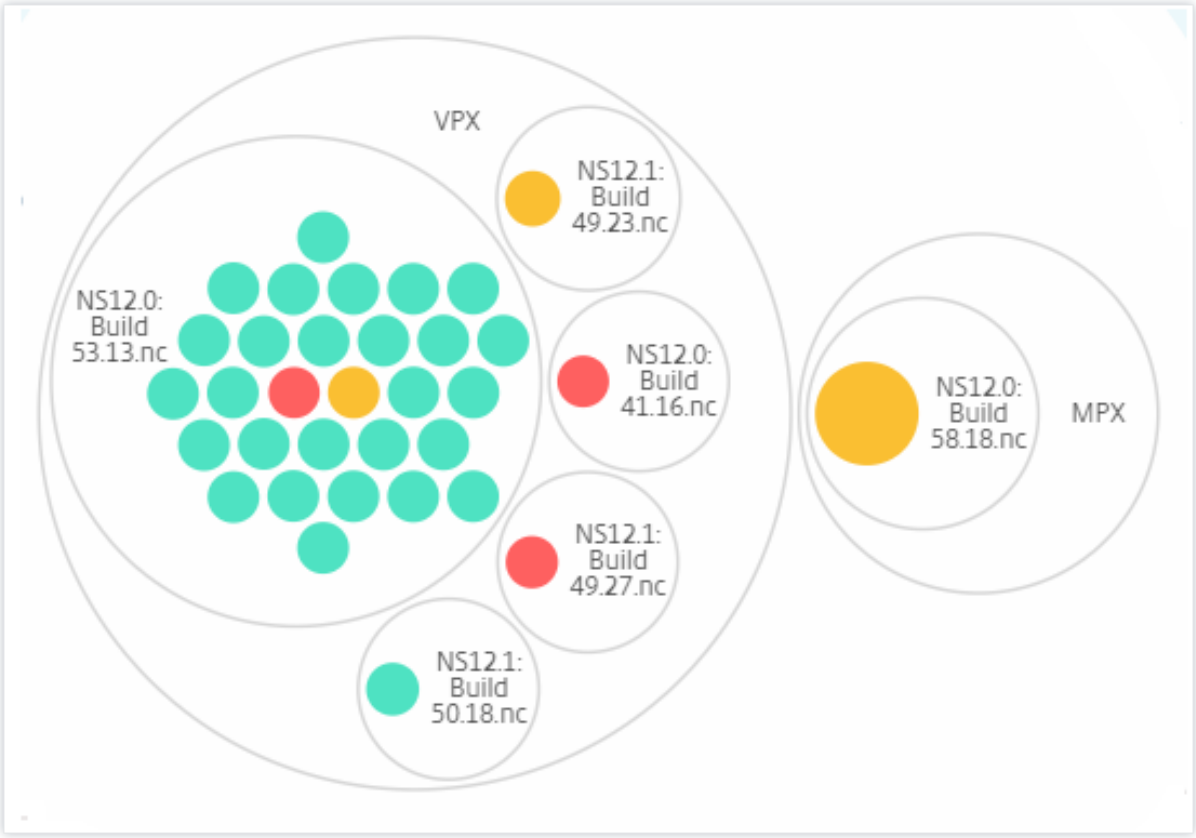




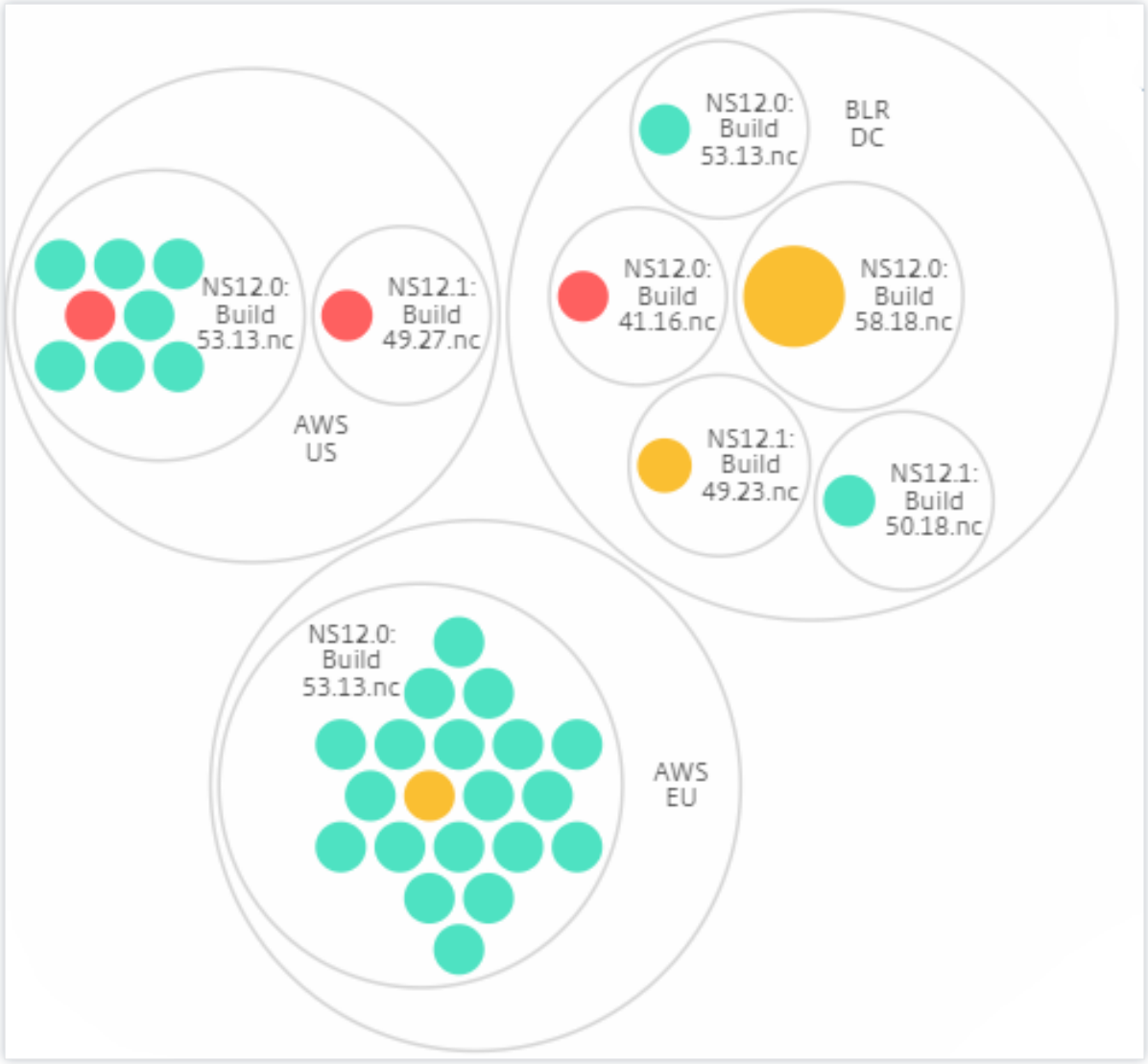
Ein paar weitere Beispiele für zweistufige Clustering sind wie folgt:

Standort und Modell:

Typ und Ausführung:

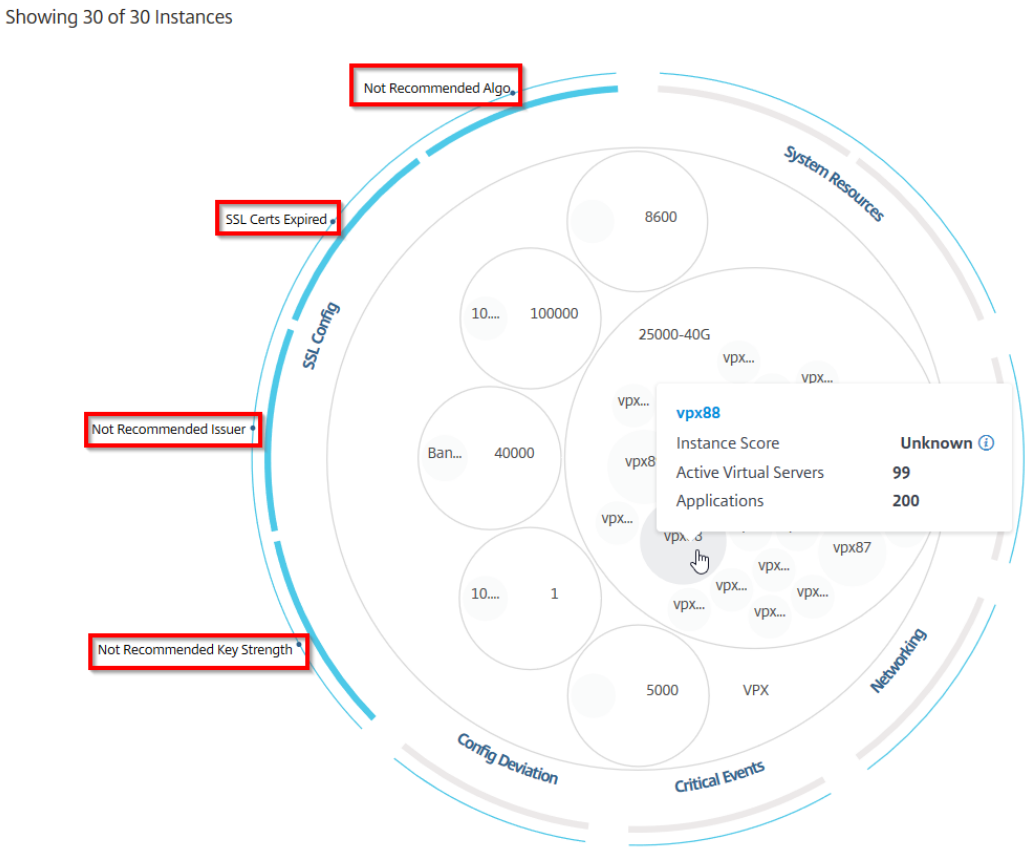


Website und Version:



Wie verwende ich Circle Pack?

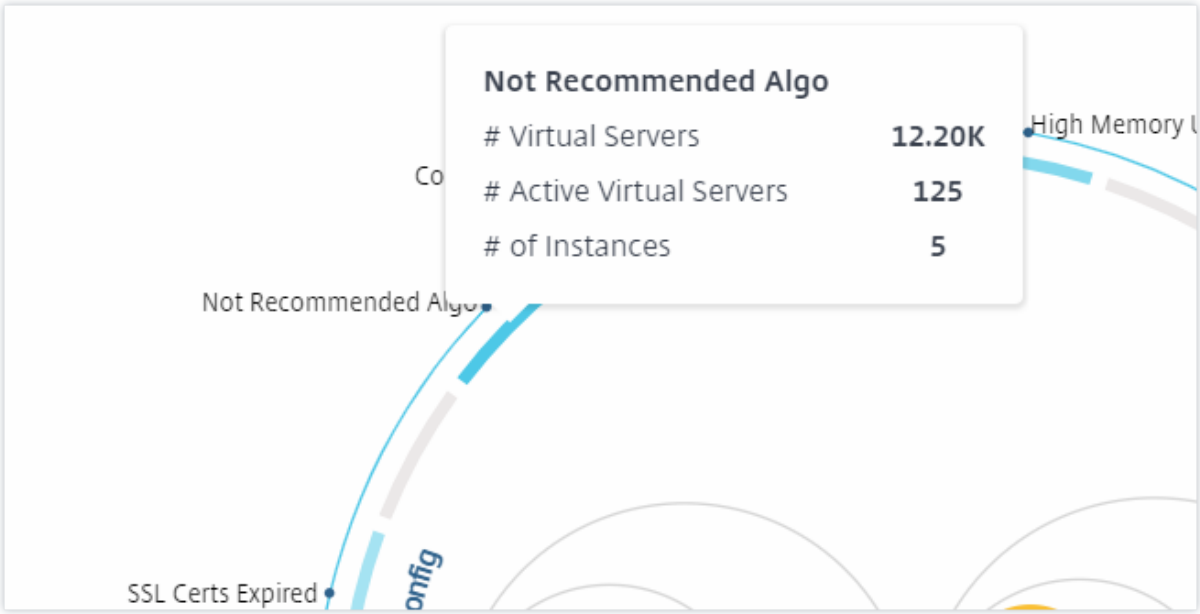
Klicken Sie auf jeden der farbigen Kreise, um diese Instanz hervorzuheben.



Abhängig von den Ereignissen, die in diesem Fall aufgetreten sind, werden nur diese Gesundheitsindikatoren auf den äußeren Kreisen hervorgehoben. Die folgenden beiden Bilder des Circle Pack zeigen beispielsweise verschiedene Gruppen von Risikoindikatoren an, obwohl sich beide Instanzen in einem kritischen Zustand befinden.

Sie können auch auf die Integritätsindikatoren klicken, um weitere Details zur Anzahl der Instanzen zu erhalten, die diesen Risikoindikator gemeldet haben. Klicken Sie beispielsweise auf,

`Not recommended Algo`um den zusammenfassenden Bericht dieses Risikoindikators anzuzeigen.



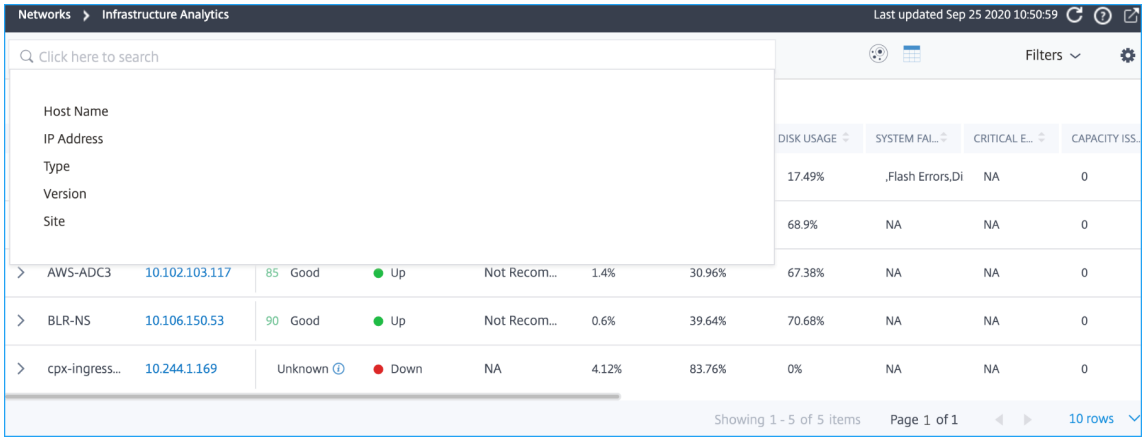
Tabellarische Ansicht

Die tabellarische Ansicht zeigt die Instanzen und die Details dieser Instanzen in einem tabellarischen Format an. Weitere Informationen finden Sie unter Instanz-Details

Suchleiste

Platzieren Sie den Mauszeiger auf die Suchleiste und wählen Sie die folgenden Suchattribute aus, um die Ergebnisse zu filtern:

- Hostname
- IP-Adresse
- Typ
- Version
- Site



Die Suchergebnisse funktionieren sowohl für die Kreis- als auch für die Tabellenansicht.

So verwenden Sie das Übersichtsfenster

Das **Übersichtsfenster** unterstützt Sie dabei, sich effizient und schnell auf die Instanzen zu konzentrieren, die überprüft oder kritisch sind. Das Panel ist in drei Registerkarten unterteilt: Übersicht, Instanzinformationen und Verkehrsprofil. Durch die Änderungen, die Sie in diesem Fenster vornehmen, wird die Anzeige sowohl im Circle Pack- als auch in Tabellaransichtsformaten geändert. In den folgenden Abschnitten werden diese Registerkarten ausführlicher beschrieben. Die Beispiele in den folgenden Abschnitten unterstützen Sie dabei, die verschiedenen Auswahlkriterien effizient zu verwenden, um die von den Instanzen gemeldeten Probleme zu analysieren.

Übersicht:

Auf der Registerkarte **Übersicht** können Sie die Instanzen anhand der Hardwarefehler, der Verwendung, abgelaufenen Zertifikaten und ähnlichen Indikatoren überwachen, die in den Instanzen auftreten können. Die Indikatoren, die Sie hier überwachen können, sind wie folgt:

- CPU-Nutzung
- Speichernutzung
- Datenträgernutzung
- Systemfehler
- Kritische Ereignisse
- Ablaufdatum der SSL-Zertifikate

Weitere Informationen zu diesen Indikatoren finden Sie unter *Integritätsindikatoren in Citrix ADC-Instanzen*.

Die folgenden Beispiele veranschaulichen, wie Sie mit dem Bedienfeld **Übersicht** interagieren können, um die Instanzen zu isolieren, die Fehler melden.

Beispiel 1: Anzeigen von Instanzen, die sich im Überprüfungsstatus befinden:

Aktivieren Sie **das** Kontrollkästchen Überprüfen, um nur die Instanzen anzuzeigen, die keine kritischen Fehler melden, aber dennoch beachtet werden müssen.

Die Histogramme im Bedienfeld **Übersicht** stellen eine aggregierte Anzahl von Instanzen dar, die auf hoher CPU-Auslastung, hoher Speicherauslastung und hoher Datenträgernutzung basieren. Die Histogramme werden mit 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90% und 100% eingestuft. Bewegen Sie den Mauszeiger auf eines der Balkendiagramme. Die Legende am unteren Rand des Diagramms zeigt den Verwendungsbereich und die Anzahl der Instanzen in diesem Bereich an. Sie können auch auf das Balkendiagramm klicken, um alle Instanzen in diesem Bereich anzuzeigen.

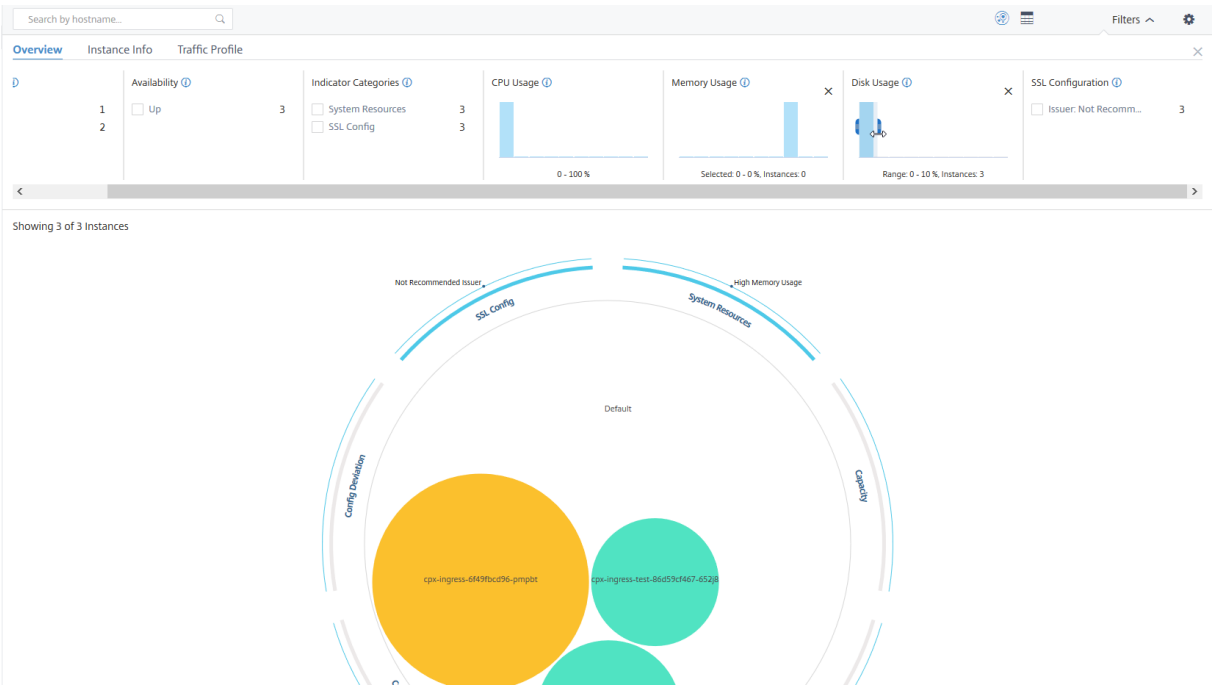
Beispiel 2: Anzeigen von Instanzen, die zwischen 10% und 20% des zugewiesenen Speichers belegen:

Klicken Sie im Bereich Speichernutzung auf das Balkendiagramm. Die Legende zeigt, dass der ausgewählte Bereich 10 bis 20% beträgt und 29 Instanzen in diesem Bereich arbeiten.

Sie können auch mehrere Bereiche in diesen Histogrammen auswählen.

Beispiel 3: Anzeigen von Instanzen, die Speicherplatz in mehreren Bereichen belegen:

Um Instanzen anzuzeigen, die Speicher zwischen 0% und 10% Speicherplatz belegt haben, ziehen Sie den Mauszeiger über die beiden Bereiche, wie in der folgenden Abbildung gezeigt.



> **Hinweis**
>
> Klicken Sie auf X, um die Auswahl zu entfernen. Sie können auch auf **Zurücksetzen** klicken, um mehrere Auswahlen zu entfernen.

Die horizontalen Balkendiagramme im Bedienfeld **Übersicht** geben die Anzahl der Instanzen an, die Systemfehler, kritische Ereignisse und den Ablaufstatus der SSL-Zertifikate melden. Aktivieren Sie das Kontrollkästchen, um diese Instanzen anzuzeigen.

Beispiel 4: Anzeigen von Instanzen für abgelaufene SSL-Zertifikate:

Aktivieren Sie im Abschnitt **Ablaufdatum von SSL-Zertifikaten** das Kontrollkästchen **Abgelaufen**, um die drei Instanzen anzuzeigen.

1 - Klicken Sie auf die **Filterliste**.

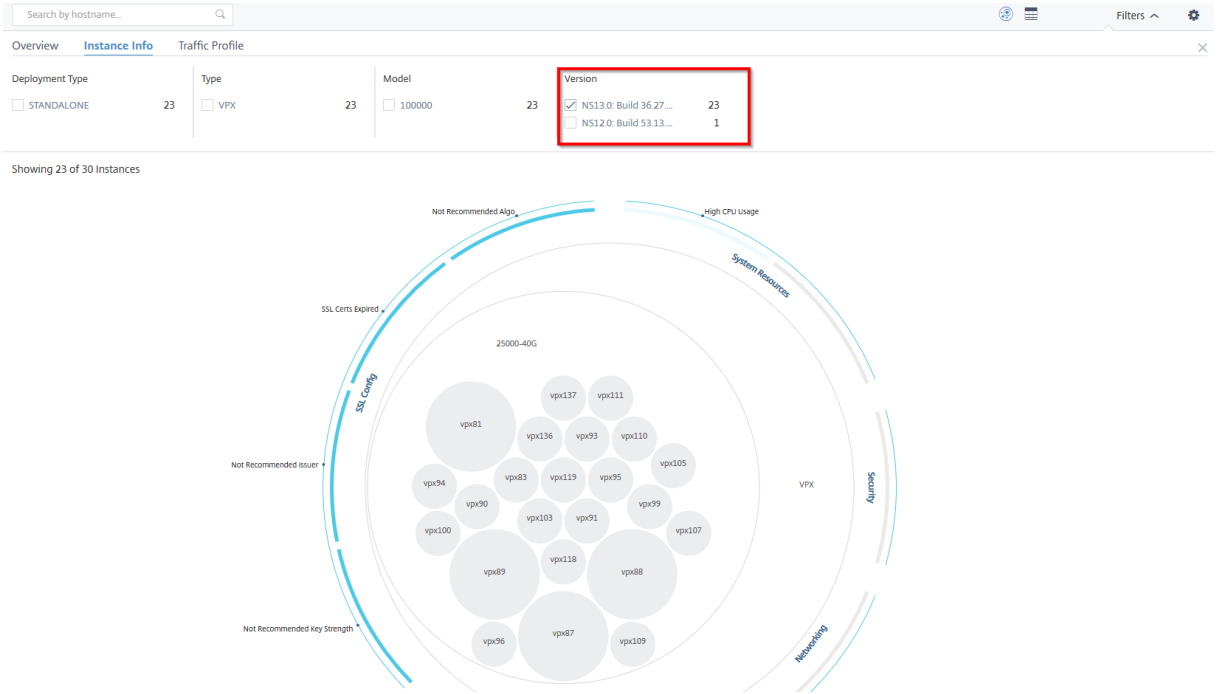
2 - Aktivieren Sie im Abschnitt **Ablaufdatum von SSL-Zertifikaten** das Kontrollkästchen **Abgelaufen**, um die Instanzen anzuzeigen.

Instanzinformationen

Im Fenster **Instanzinfo** können Sie Instanzen basierend auf dem Bereitstellungstyp, dem Instanztyp, dem Modell und der Softwareversion anzeigen. Sie können mehrere Kontrollkästchen aktivieren, um Ihre Auswahl einzuschränken.

Beispiel 5: Anzeigen von ADC VPX-Instanzen mit einer bestimmten Build-Nummer:

Wählen Sie die Version aus, die Sie anzeigen möchten.

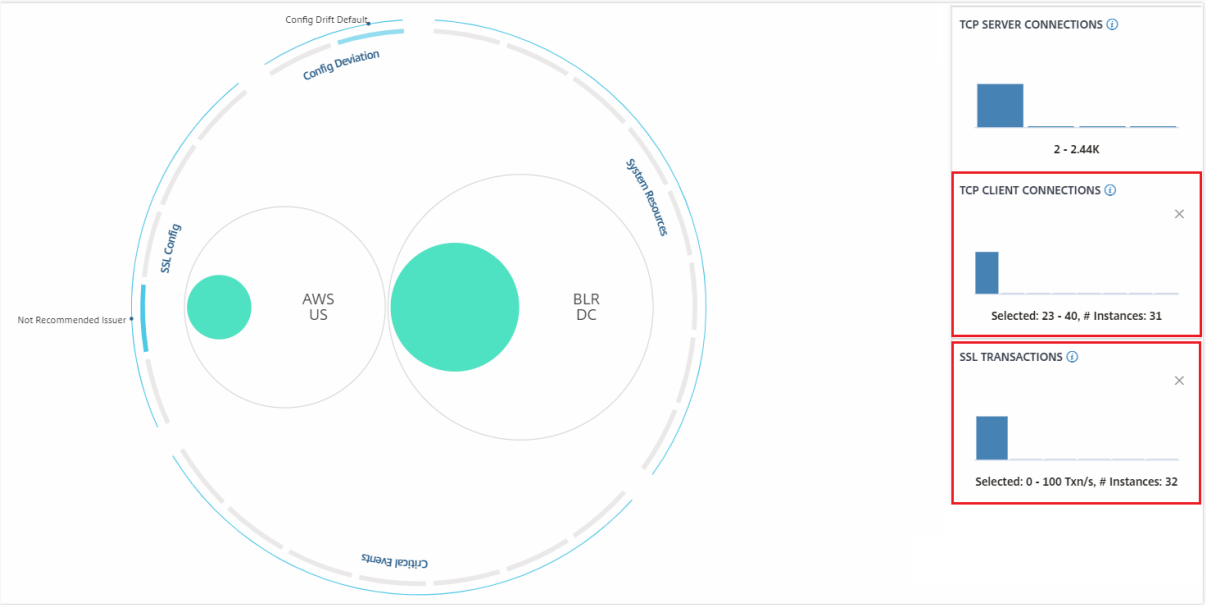


Verkehrsprofil

Die Histogramme im Bedienfeld **Verkehrsprofil** stellen eine aggregierte Anzahl von Instanzen dar, die auf dem lizenzierten Durchsatz der Instanzen, der Anzahl der Anforderungen, Verbindungen und Transaktionen basieren, die von den Instanzen verarbeitet werden. Wählen Sie das Balkendiagramm aus, um Instanzen in diesem Bereich anzuzeigen.

Beispiel 6: View-Instanzen, die TCP-Verbindungen unterstützen:

Das folgende Bild zeigt die Anzahl der Instanzen, die TCP-Verbindungen zwischen 23 und 40 unterstützen und bis zu 100 SSL-Transaktionen pro Sekunde verarbeiten.

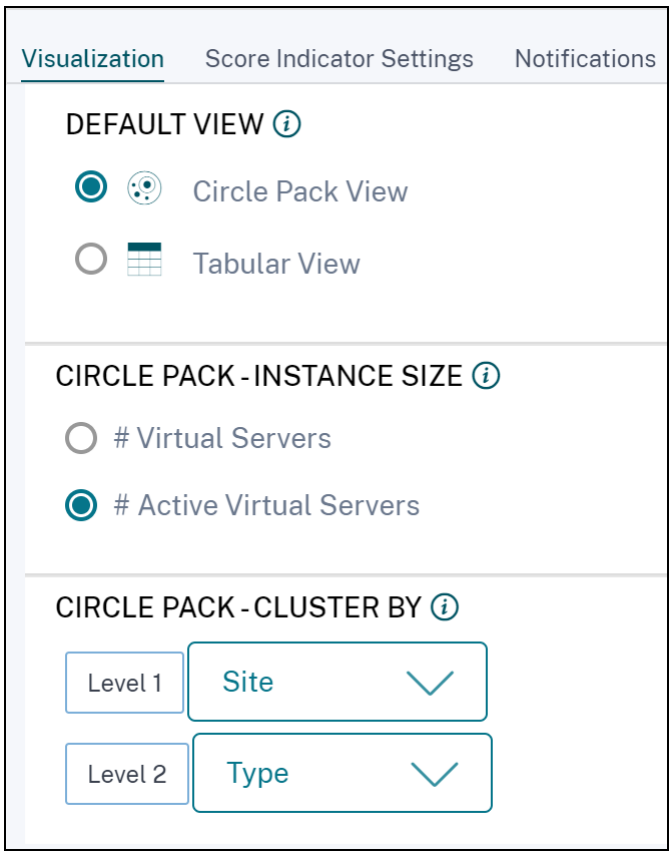


So verwenden Sie das Einstellungsfenster

Im **Einstellungsfenster** können Sie die Standardansicht der Infrastructure Analytics festlegen. Außerdem können Sie die niedrigen und hohen Schwellenwerte für hohe CPU-Auslastung, hohe Datenträgernutzung und hohe Speicherauslastung festlegen. Das Einstellungsfenster ist in zwei Registerkarten unterteilt - Ansichts- und Bewertungsschwellenwerte.

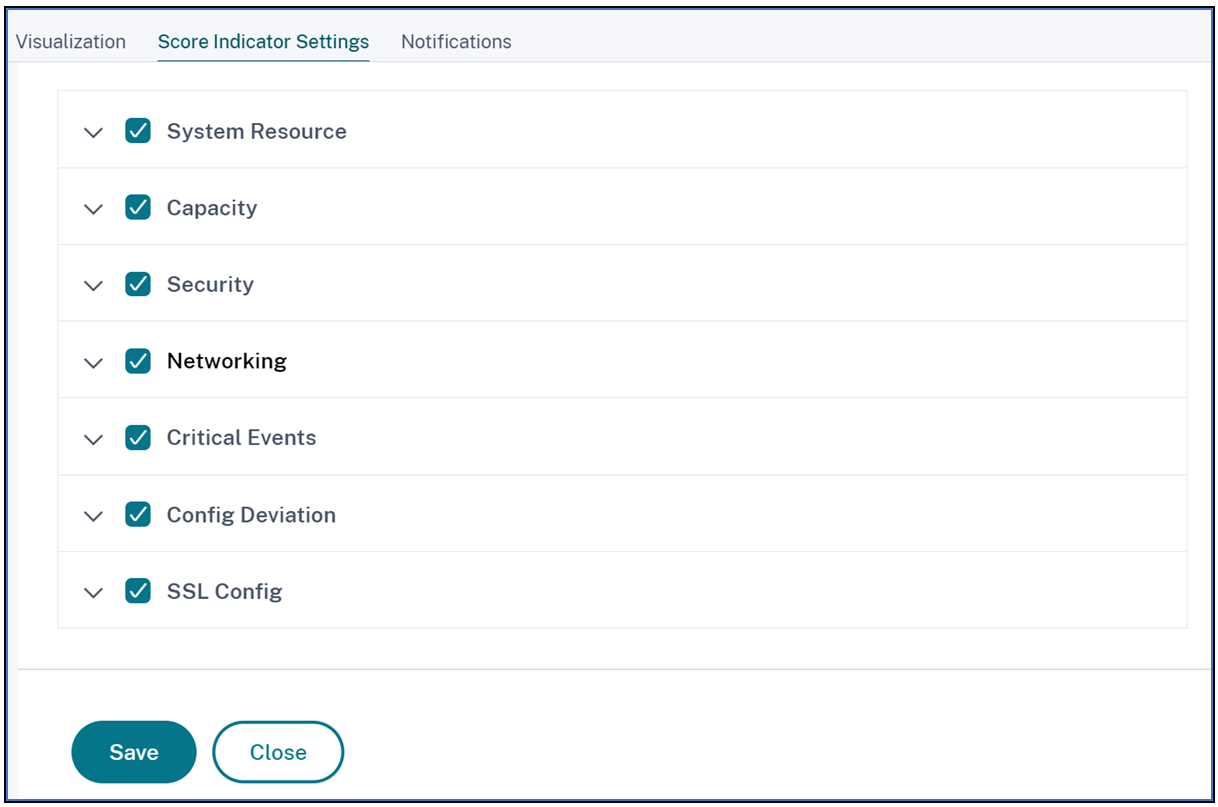
View

- **Standardansicht**. Wählen Sie **Circle Pack** oder Tabellarformat als Standardansicht auf der Analyseseite aus. Das ausgewählte Format wird angezeigt, wenn Sie in Citrix ADM auf die Seite zugreifen.
- **Circle Pack - Instanzgröße**. Lassen Sie die Größe des Instanzkreises durch die Anzahl der virtuellen Server oder die Anzahl der aktiven virtuellen Server zu.
- **Circle Pack - Cluster By**. Entscheiden Sie das zweistufige Clustering der Instanzkreise. Weitere Informationen zum Instanzclustering finden Sie unterCluster-Instanzkreise.



Score-Schwellenwerte

Sie können die niedrigen und hohen Schwellenwerte für hohe CPU-, Arbeitsspeicher- und Datenträgerauslastung in Abhängigkeit von den Datenverkehrsanforderungen in Ihrer Organisation ändern. Ziehen Sie die Ziehpunkte in jedem der Auswahl-Histogramm, um die Werte festzulegen.



> **Hinweis**
>
> Klicken Sie auf **Einstellungen anwenden**, um diese Änderungen anzuwenden, oder klicken Sie auf **Zurücksetzen**, um alle Änderungen zu entfernen.

So visualisieren Sie Daten auf dem Dashboard

Mithilfe von Infrastructure Analytics können Netzwerkadministratoren nun Instanzen identifizieren, die größtmögliche Aufmerksamkeit benötigen. Um dies genauer zu verstehen, betrachten wir den Fall von Chris, einem Netzwerkadministrator von ExampleCompany.

Chris unterhält viele Citrix ADC-Instanzen in seiner Organisation. Einige der Instanzen verarbeiten hohen Datenverkehr, und er muss sie genau überwachen. Er stellt fest, dass einige Instanzen mit hohem Datenverkehr nicht mehr den vollen Datenverkehr verarbeiten, der durch sie fließt. Um diese Reduktion zu analysieren, musste er früher mehrere Datenberichte lesen, die aus verschiedenen Quellen kamen. Chris musste mehr Zeit damit verbringen, die Daten manuell zu korrelieren und festzustellen, welche Instanzen sich nicht im optimalen Zustand befinden und Aufmerksamkeit benötigen. Er verwendet die Funktion Infrastructure Analytics, um die Integrität aller Instanzen visuell zu sehen.

Die folgenden zwei Beispiele veranschaulichen, wie Infrastructure Analytics Chris bei Wartungsaktivitäten unterstützt:

Beispiel 1 - So überwachen Sie den SSL-Datenverkehr:

Chris bemerkt auf dem Circle Pack, dass eine Instanz einen niedrigen Instanzwert hat und sich diese Instanz im Status Kritisch befindet. Er klickt auf die Instanz, um zu sehen, was das Problem ist. Die Instanzzusammenfassung zeigt an, dass ein SSL-Kartenfehler auf dieser Instanz vorliegt und diese Instanz daher nicht in der Lage ist, den SSL-Datenverkehr zu verarbeiten (der SSL-Datenverkehr wurde reduziert). Chris extrahiert diese Informationen und sendet einen Bericht an das Team, um das Problem sofort zu untersuchen.

Beispiel 2 - So überwachen Sie Konfigurationsänderungen:

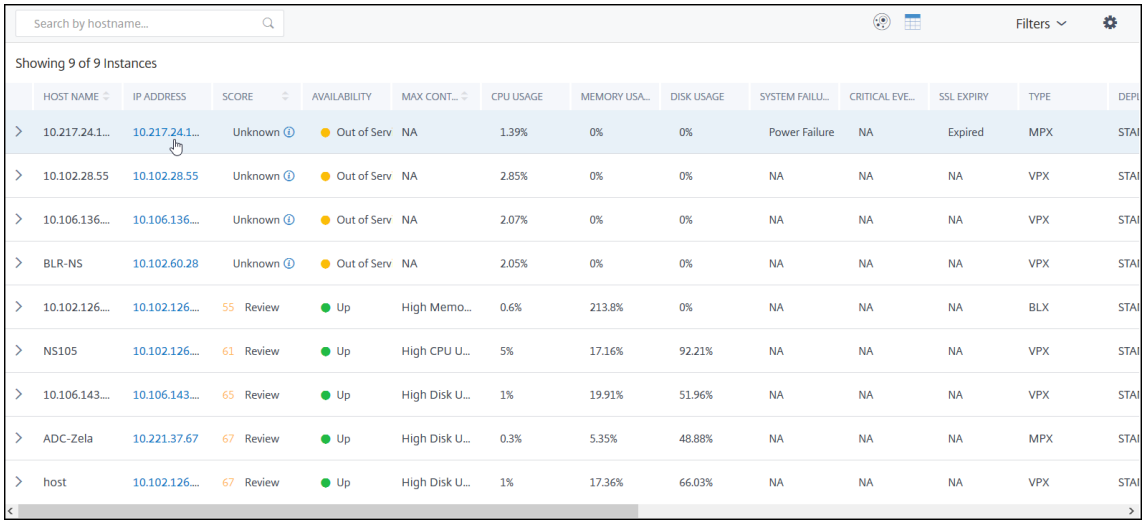
Chris bemerkt auch, dass sich eine andere Instanz im Status Review befindet und dass kürzlich eine Konfigurationsabweichung aufgetreten ist. Wenn er auf den Konfigurationsabweichungsrisikoindikator klickt, stellt er fest, dass Konfigurationsänderungen mit RC4 Cipher, SSL v3, TLS 1.0 und TLS 1.1 vorgenommen wurden, die möglicherweise auf Sicherheitsbedenken zurückzuführen sind. Er bemerkt auch, dass das SSL-Transaktionsprofil für diese Instanz ausgefallen ist. Er exportiert diesen Bericht und sendet ihn an den Administrator, um ihn weiter zu erkundigen.

Anzeigen von Instanzdetails in Infrastructure Analytics

April 28, 2021

1. Navigieren Sie zu **Netzwerke** > **Infrastrukturanalyse**
2. Klicken Sie auf die Circle Pack-Ansicht, und wählen Sie die IP-Adresse aus.

Sie können auch in der Tabellenansicht auf eine IP-Adresse klicken.

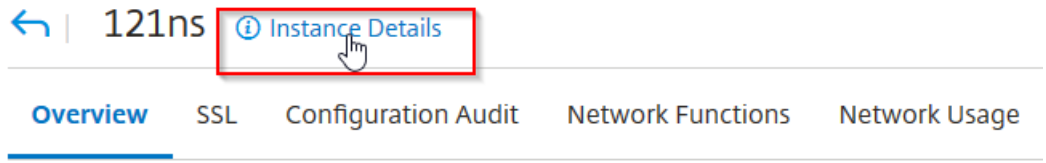


- **Hostname** — Kennzeichnet den Hostnamen, der der ADC-Instanz zugewiesen ist.
- **IP-Adresse** — Bezeichnet die IP-Adresse der ADC-Instanz
- **Punktzahl** — Bezeichnet die ADC-Instanzbewertung und den Status wie Kritisch, Gut und Fair
- **Verfügbarkeit** — gibt den aktuellen Status der ADC-Instanz an, z. B. “ **Aufwärts**”, “ **Heruntergefahren**” oder “ **Abgemeldet”**.
- **Max Contribution** — Gibt die Problemkategorie an, in der die ADC-Instanz die maximale Fehleranzahl aufweist.
- **CPU-Auslastung** — Bezeichnet die aktuelle CPU%, die von der Instanz verwendet wird
- **Speicherauslastung** — Bezeichnet den aktuellen Speicher%, der von der Instanz verwendet wird
- **Datenträgerauslastung** — Kennzeichnet den aktuellen Datenträger%, der von der Instanz verwendet wird
- **Systemfehler** — Gibt die Gesamtzahl der Fehler für das Instanzsystem an
- **Kritische Ereignisse** — Bezeichnet die Ereigniskategorie, in der die Citrix ADC-Instanz die maximalen Ereignisse aufweist.
- **SSL-Ablaufdatum** — gibt den aktuellen Status des SSL-Zertifikats an, das auf der ADC-Instanz installiert ist.
- **Typ** — Bezeichnet den ADC-Instanztyp, z. B. VPX, SDX, MPX oder CPX
- **Bereitstellung** — Gibt an, ob die ADC-Instanz als eigenständige Instanz oder HA-Paar bereitgestellt wird
- **Modell** — Gibt die Modellnummer des ADC-Instanzmodells an
- **Version** — Gibt die ADC-Instanzversion und Build-Nummer an

- **Durchsatz** — Bezeichnet den aktuellen Netzwerkdurchsatz von der ADC-Instanz
- **HTTPS-Anforderung/Sekunde** — Bezeichnet die aktuellen HTTPS-Anforderungen/s, die von der ADC-Instanz empfangen werden
- **TCP-Verbindung** — Bezeichnet die aktuellen TCP-Verbindungen etabliert
- **SSL-Transaktion** — Bezeichnet die aktuellen SSL-Transaktionen, die von der ADC-Instanz verarbeitet werden
- **Site** — Bezeichnet den Namen des Standorts, an dem die ADC-Instanz bereitgestellt wird.

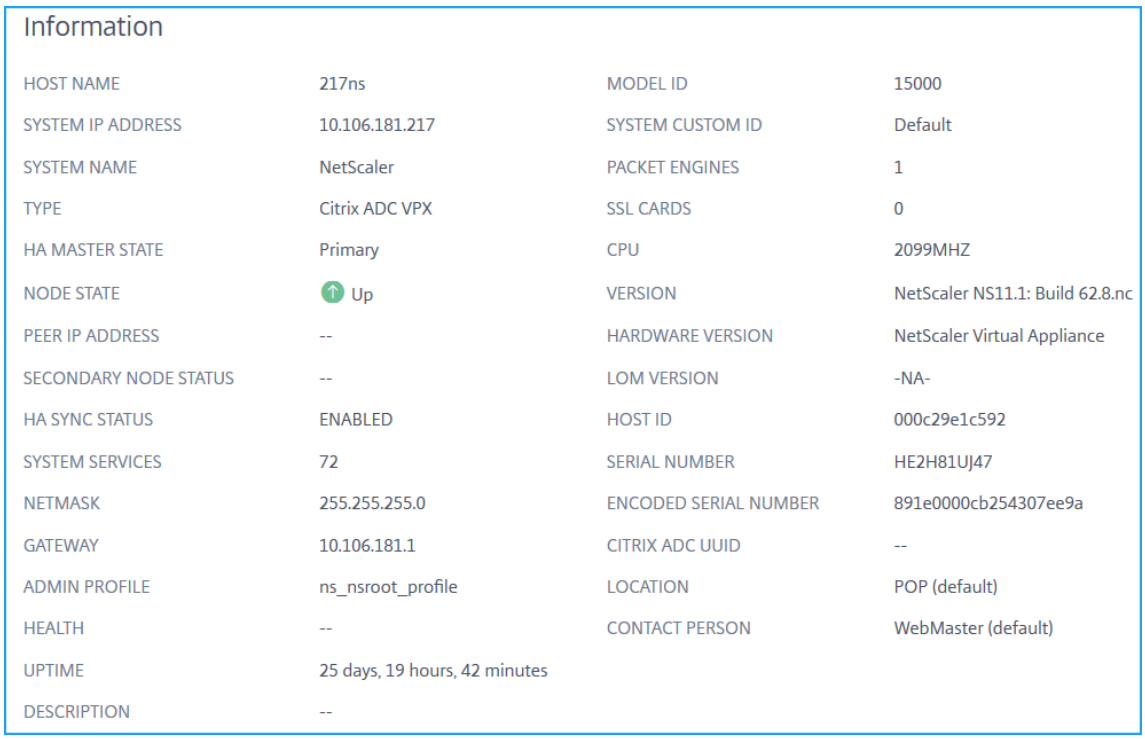
> **Hinweis**
>
> Alle 5 Minuten werden die aktuellen Werte für CPU-Auslastung, Speicherauslastung, Datenträgerauslastung, Durchsatz usw. aktualisiert.

Klicken Sie auf **Instanzdetails**, um die Details anzuzeigen.

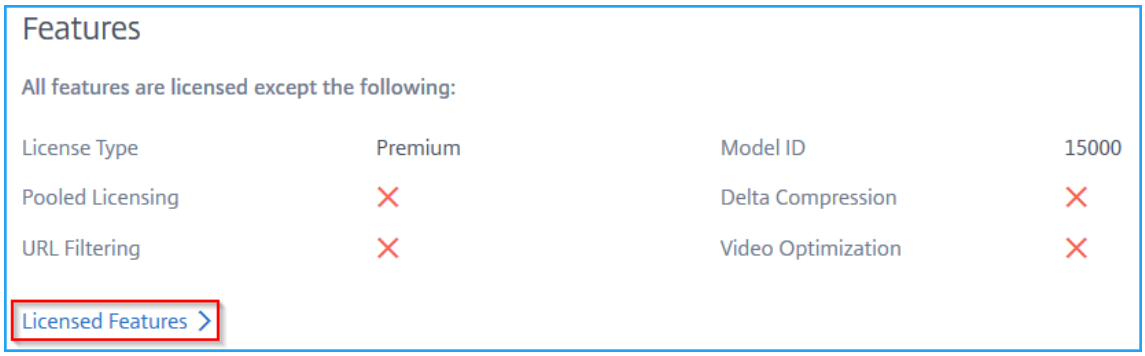


Folgende Details werden angezeigt:

- **Informationen** - Instanzdetails wie Instanztyp, Bereitstellungstyp, Version, Modell usw.



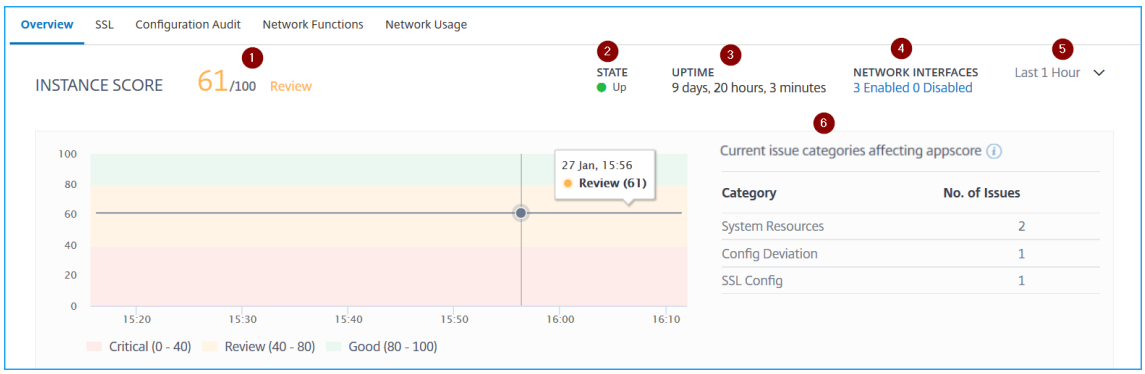
- **Features** — Standardmäßig werden die Features angezeigt, die nicht lizenziert sind. Klicken Sie auf **Lizenzierte Features**, um die lizenzierten Features anzuzeigen.



- **Modi** — Standardmäßig werden alle Modi angezeigt, die für die Instanz deaktiviert sind. Klicken Sie auf **Aktivierte Modi** anzeigen, um die aktivierten Modi auf der Instanz anzuzeigen.

Das Instanz-Dashboard bietet eine Instanzübersicht, in der Sie die folgenden Details sehen können:

- **Instanzbewertung**

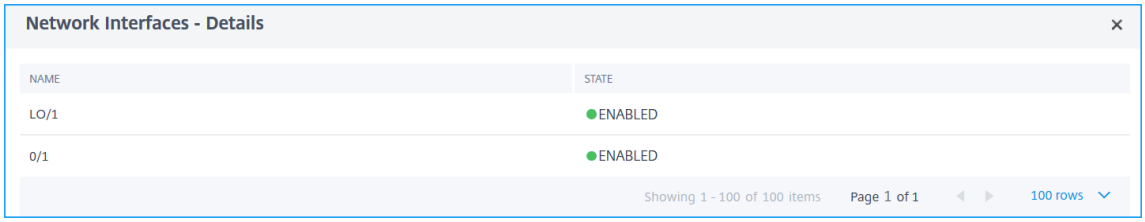


1 — Gibt die aktuelle Citrix ADC-Instanzbewertung für die ausgewählte Zeitdauer an. Die Endpunktzahl wird als **100 minus Gesamtstrafen**berechnet. Das Diagramm zeigt die Bewertungsbereiche für die ausgewählte Zeitdauer an.

2 — Gibt den aktuellen Status der Citrix ADC-Instanz an, z. B. **Up-**, **Down-**und **Out-Out of Service**.

3 — Gibt die Dauer an, die die Citrix ADC-Instanz ausgeführt wird.

4 — Gibt die Gesamtzahl der Netzwerkschnittstellen an, die für die Instanz aktiviert und deaktiviert sind. Klicken Sie hier, um Details wie den Namen der Netzwerkschnittstelle und den Status (aktiviert oder deaktiviert) anzuzeigen.



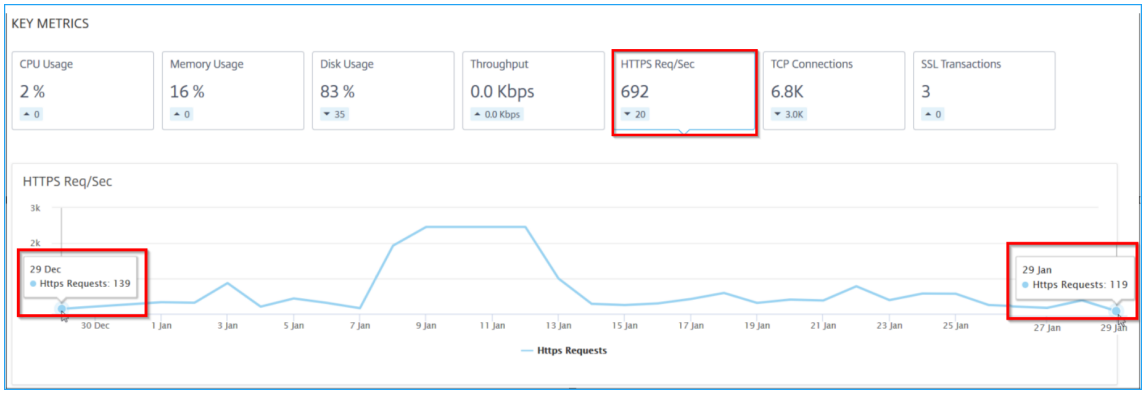
5 — Wählen Sie die Zeitdauer aus der Liste aus, um die Instanzdetails anzuzeigen.

6 — Zeigt die Gesamtzahl der Probleme und die Ausgabekategorie der ADC-Instanz an.

- **Wichtige Metriken**

  Klicken Sie auf die einzelnen Registerkarten, um die Details anzuzeigen. In jeder Metrik können Sie den Durchschnittswert und den Differenzwert für die ausgewählte Zeit anzeigen.

  Die folgende Abbildung ist ein Beispiel für HTTPS Req/Sek. und die ausgewählte Zeitdauer beträgt 1 Stunde. Der Wert **692** ist der durchschnittliche HTTPS-Req/Sek für die 1-Monats-Dauer und der Wert **20** ist der Differenzwert. In der Grafik ist der erste Wert **139** und der letzte Wert **119**. Der Differenzwert beträgt **139 — 119 = 20.**



  Sie können die folgenden Instanzmetriken in einem Diagrammformat für die ausgewählte Zeitdauer anzeigen:

  - **CPU-Auslastung** — Die durchschnittliche CPU% der Instanz für die ausgewählte Dauer (wird sowohl für Paketprozessoren als auch für Verwaltungs-CPU angezeigt).

- **Speicherauslastung** — Die durchschnittliche Speicherauslastung% der Instanz für die ausgewählte Dauer.
- **Datenträgerauslastung** — Der durchschnittliche Speicherplatz% der Instanz für die ausgewählte Dauer.
- **Durchsatz** — Der durchschnittliche Netzwerkdurchsatz, der von der Instanz für die ausgewählte Dauer verarbeitet wird.
- **HTTPS-Anforderung/s** — Die durchschnittlichen HTTPS-Anforderungen, die von der Instanz für die ausgewählte Dauer empfangen wurden.
- **TCP-Verbindungen** — Die durchschnittlichen TCP-Verbindungen, die vom Client und Server für die ausgewählte Dauer hergestellt werden.
- **SSL-Transaktionen** — Die durchschnittlichen SSL-Transaktionen, die von der Instanz für die ausgewählte Dauer verarbeitet werden.

- **Probleme**

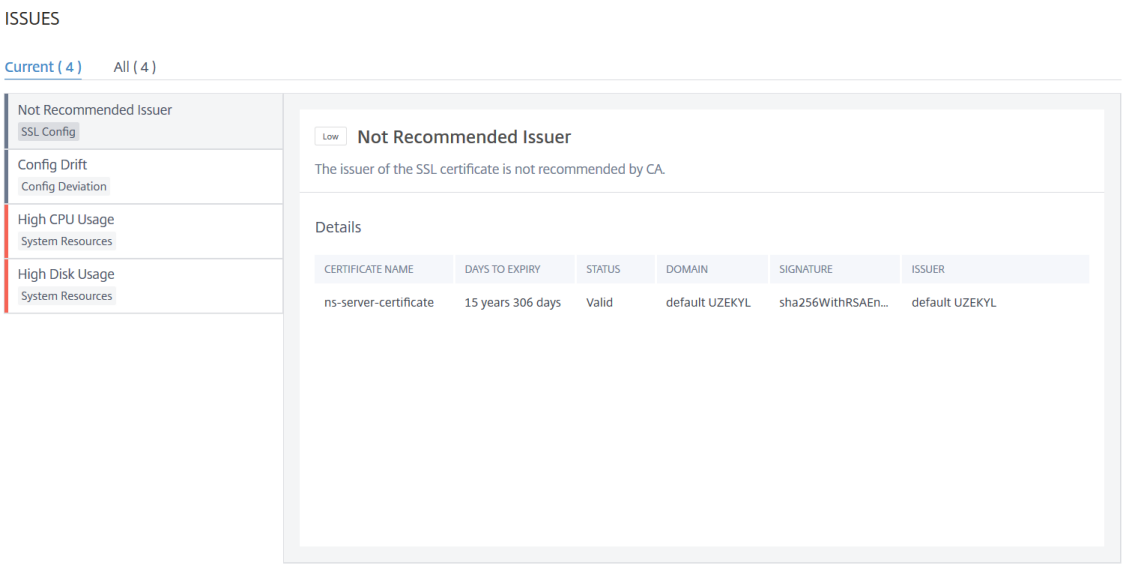
  Sie können die folgenden Probleme anzeigen, die in der Citrix ADC-Instanz auftreten:

Issue Kategorie	Beschreibung	Probleme
Systemressourcen	Zeigt alle Probleme im Zusammenhang mit der Citrix ADC -Systemressource an, z. B. CPU, Arbeitsspeicher, Datenträgerauslastung usw.	- Hohe CPU-Auslastung
		- Hohe Speicherauslastung
		- Hohe Datenträgernutzung
		- SSL-Karten-Fehler
		- Stromausfall
		- Datenträgerfehler
		- Blitzfehler
		- NIC verwirft
SSL-Konfiguration	Zeigt alle Probleme im Zusammenhang mit der SSL-Konfiguration auf der Citrix ADC-Instanz an.	- SSL-Zertifikate abgelaufen
		- Nicht empfohlener Aussteller
		- Nicht empfohlen Algo

Issue Kategorie	Beschreibung	Probleme
		- Nicht empfohlene Tastenstärke
Konfigurationsabweichung	Zeigt alle Probleme im Zusammenhang mit den Konfigurationsaufträgen an, die in der Citrix ADC-Instanz angewendet werden.	- Config Drift
		- Laufen vs Vorlage
Kritische Ereignisse	Zeigt alle kritischen Ereignisse im Zusammenhang mit Citrix ADC-Instanzen an, die im HA-Paar und im Cluster konfiguriert sind.	- Cluster-Prop-Fehler
		- Cluster-Synchronisierungsfehler
		- Clusterversionen stimmen nicht überein
		- HA schlechter Sec Zustand
		- HA keine Heat Beats
		- HA-Synchronisierungsfehler
		- HA Version stimmt nicht überein
Kapazitätsprobleme	Zeigt ADC-Kapazitätsprobleme an. Der ADM ruft diese Ereignisse alle fünf Minuten von der ADC-Instanz ab und zeigt die verworfenen Pakete oder Rate-Limit-Zähler-Inkremente an, falls vorhanden. Die Probleme werden nach den folgenden Kapazitätsparametern kategorisiert.	- Durchsatzlimit erreicht
		- PE-CPU-Limit erreicht

Issue Kategorie	Beschreibung	Probleme
		- PPS Limit erreicht
		- SSL-Durchsatzrate Limit
		- SSL TPS Rate Limit
Netzwerke	Zeigt die Betriebsprobleme an, die in den Instanzen auftreten.	Weitere Informationen finden Sie unter Verbesserte Infrastrukturanalyse mit neuen Indikatoren.

Klicken Sie auf die einzelnen Registerkarten, um das Problem zu analysieren und zu beheben. Betrachten Sie beispielsweise, dass eine Instanz die folgenden Fehler für die ausgewählte Zeitdauer aufweist:



- Auf der Registerkarte **Aktuell** werden die Probleme angezeigt, die sich derzeit auf die Instanzbewertung auswirken.
- Auf der Registerkarte **Alle** werden alle Infrarotprobleme angezeigt, die für die ausgewählte Dauer erkannt wurden.

Anzeigen der Kapazitätsprobleme in einer ADC-Instanz

April 28, 2021

Wenn eine ADC-Instanz die meiste verfügbare Kapazität verbraucht hat, kann ein Paketablegen

während der Verarbeitung des Clientdatenverkehrs auftreten. Dieses Problem verursacht eine geringe Leistung in einer ADC-Instanz. Wenn Sie solche ADC-Kapazitätsprobleme verstehen, können Sie proaktiv zusätzliche Lizenzen zuweisen, um die ADC-Leistung zu stabilisieren.

In der **Circle Pack-Ansicht**können Sie die Kapazitätsprobleme der ADC-Instanz anzeigen, falls vorhanden.

So zeigen Sie ADC-Kapazitätsprobleme an:

1. Navigieren Sie zu **Netzwerke > Infrastructure Analytics**.
2. Wählen Sie die Ansicht des Kreispakets aus.

Die folgende Abbildung legt nahe, dass die Kapazitätsprobleme in der ausgewählten Instanz auftreten:

Die Probleme werden nach den folgenden Kapazitätsparametern kategorisiert:

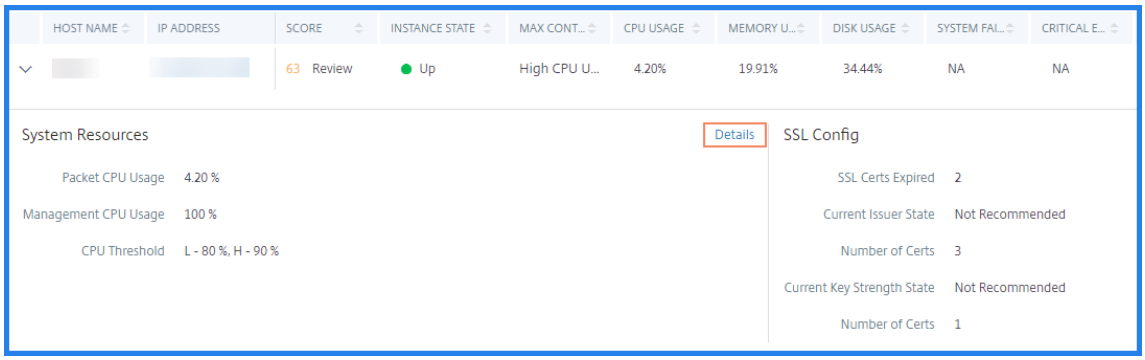
- **Durchsatzlimit erreicht** — Die Anzahl der Pakete, die in der Instanz gelöscht wurden, nachdem das Durchsatzlimit erreicht wurde.
- **PE-CPU-Limit erreicht** - Die Anzahl der Pakete, die auf allen Netzwerkkarten gelöscht wurden, nachdem das PE-CPU-Limit erreicht wurde.
- **PPS Limit erreicht** — Die Anzahl der Pakete, die in der Instanz gelöscht wurden, nachdem das PPS-Limit erreicht wurde.
- **SSL-Durchsatzrate Limit** — Gibt an, wie oft das SSL-Durchsatzlimit erreicht wurde.

- **SSL-TPS Rate Limit** — Gibt an, wie oft das SSL-TPS Limit erreicht wurde.

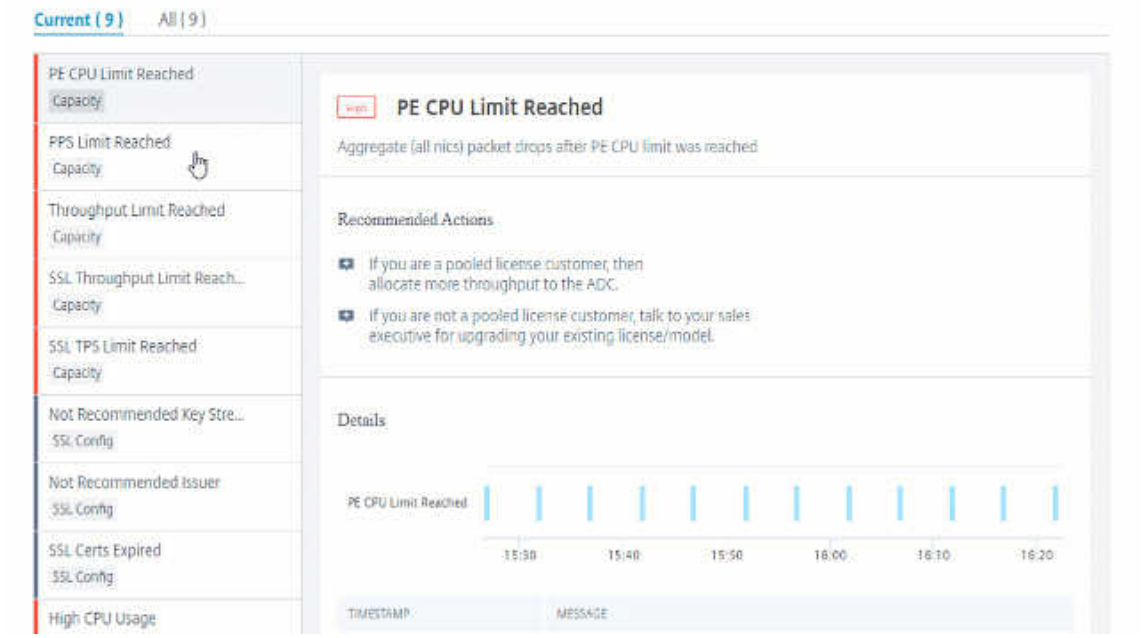
Empfohlene Aktionen zur Behebung von Kapazitätsproblemen anzeigen

ADM empfiehlt Aktionen zur Behebung von Kapazitätsproblemen. Führen Sie die folgenden Schritte aus, um empfohlene Aktionen anzuzeigen:

1. Wählen Sie unter **Netzwerke > Infrastructure Analytics**die tabellarische Ansicht aus.
2. Wählen Sie die Instanz mit Kapazitätsproblemen aus, und klicken Sie auf **Details**.



3. Scrollen Sie auf der Instanzseite nach unten zum Abschnitt " **Probleme** ".
4. Wählen Sie jedes Problem aus, und zeigen Sie die empfohlenen Aktionen an, um Kapazitätsprobleme zu beheben.



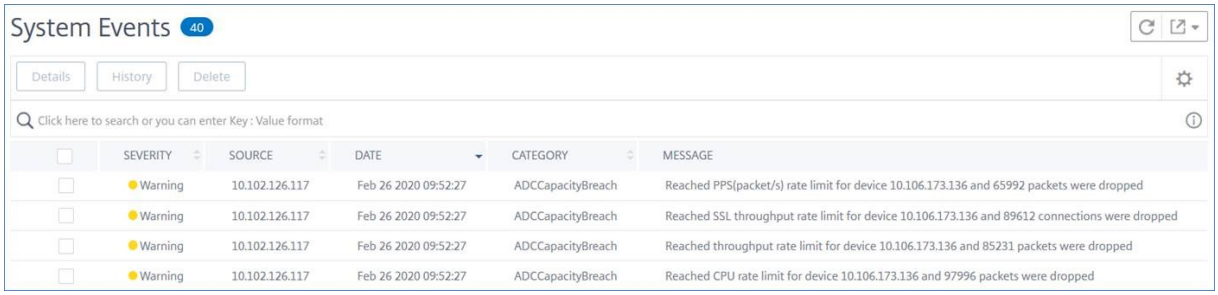
Der ADM ruft diese Ereignisse alle fünf Minuten von der ADC-Instanz ab und zeigt die verworfenen Pakete oder Rate-Limit-Zähler-Inkremente an, falls vorhanden.

Der ADM berechnet die Instanzbewertung auf dem definierten Kapazitätsschwellenwert.

- **Niedriger Schwellenwert** — 1 Schrittweite für Paketabfall oder Ratenbegrenzungszähler
- **Hoher Schwellenwert** — 10000 Pakete fallen oder Rate-Limit-Zähler-Inkrement

Wenn eine ADC-Instanz den Kapazitätsschwellenwert überschreitet, wird die Instanz-Bewertung beeinträchtigt.

Wenn Pakete fallen oder Rate-Limit Zähler inkrementiert werden, wird ein Ereignis unter der Kategorie `ADCCapacityBreach`generiert. Um diese Ereignisse anzuzeigen, navigieren Sie zu **Konten > Systemereignisse**.



Verbesserte Infrastrukturanalyse mit neuen Indikatoren

April 28, 2021

Mit Citrix ADM **Infrastructure Analytics**können Sie:

- Zeigen Sie eine neue Reihe von Betriebsproblemen an, die in Citrix ADC-Instanzen auftreten.
- Zeigen Sie Fehlermeldungen an, und überprüfen Sie Empfehlungen, um die Probleme zu beheben.

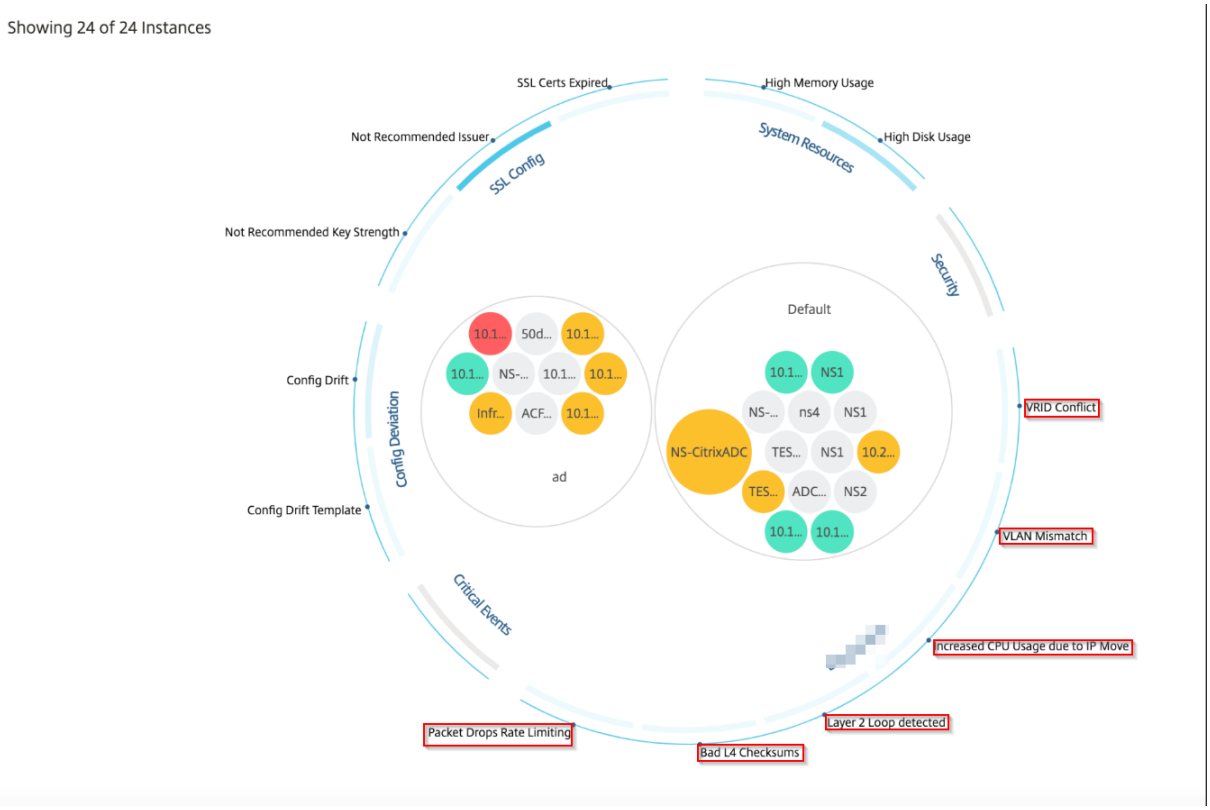
Als Administrator können Sie schnell die Ursachenanalyse von Problemen identifizieren.

> **Hinweis**
>
> Regelindikatoren werden nicht unterstützt für:
>
> - Citrix ADC-Instanzen, die im Clustermodus konfiguriert sind.
> - Citrix ADC-Instanzen, die mit Administratorpartitionen konfiguriert sind.

Navigieren Sie in Citrix ADM zu **Netzwerke** > **Infrastructure Analytics**, um Indikatoren für:

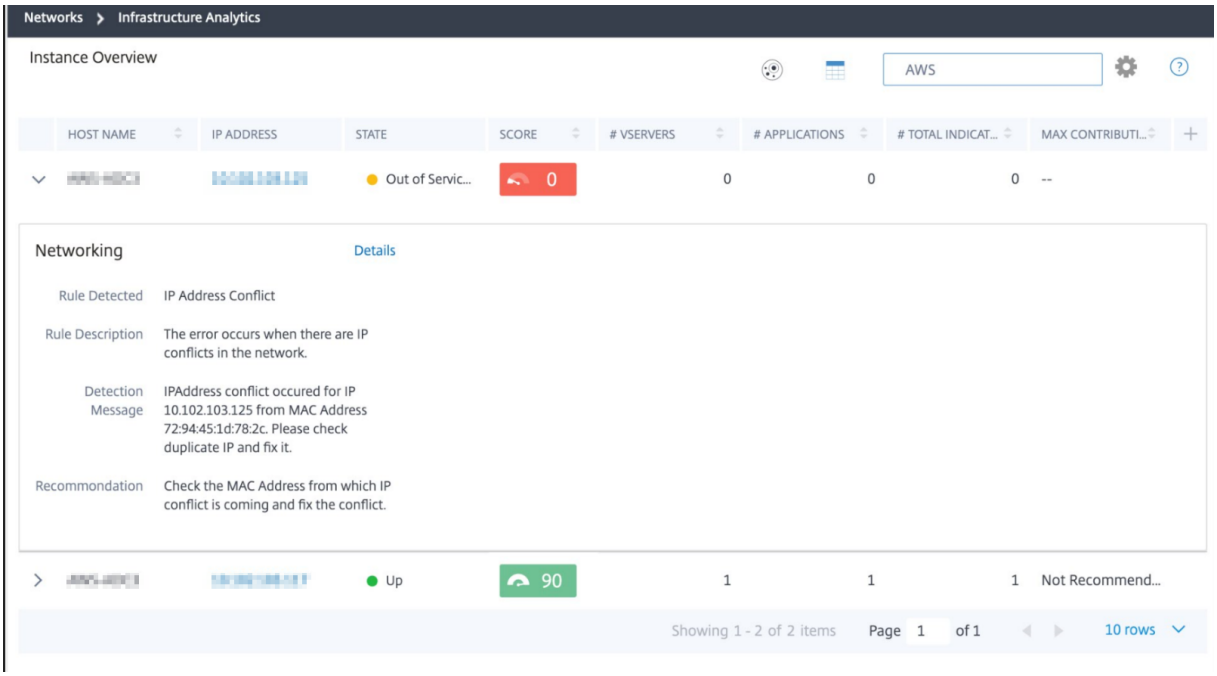
Indikatorname in Infrastructure Analytics	Beschreibung
Fehler bei der Port-Zuweisung	Erkennt, wann Citrix ADC SNIP verwendet, um mit einer neuen Serververbindung zu kommunizieren und die Anzahl der verfügbaren Ports auf diesem SNIP ausgeschöpft sind. Die empfohlene Aktion besteht darin, ein weiteres SNIP im selben Subnetz hinzuzufügen.
Sitzungsaufbau	Erkennt, wenn Citrix ADC Speicher durch SSL-Sitzungen gehalten wird.
Keine Standard-Routenkonfiguration	Erkennt, wenn der Datenverkehr aufgrund der Nichtverfügbarkeit von Routen gelöscht wird.
IP-Konflikt	Erkennt, ob dieselbe IP-Adresse auf zwei oder mehr Instanzen in einem Netzwerk konfiguriert oder angewendet wird.
VRID-Konflikt	Erkennt, wenn intermittierende Zugriffsprobleme für die angegebene VRID auftreten.
VLAN-Unstimmigkeit	Erkennt, ob während der VLAN-Konfiguration, die an IP-Subnetze gebunden ist, Fehler auftreten.
TCP-Angriff mit kleinem Fenster	Erkennt, wenn ein möglicher kleiner Fensterangriff im Gange ist. Diese Warnung dient lediglich der Information, da ADC diesen Angriff bereits mildert.
Schwellenwert für die Regelung der Rate	Erkennt, wann Pakete gelöscht werden, basierend auf dem konfigurierten Schwellenwert für die Ratensteuerung.
Persistenzgrenze	Erkennt, wenn maximale Treffer auf den Citrix ADC Speicher verhängt werden.
GSLB-Sitenname stimmt nicht überein	Erkennt, wenn GSLB-Konfigurationssynchronisationsfehler aufgrund von Nichtübereinstimmungen des Sitename auftreten.
Fehlgebildete IP-Header	Erkennt, wenn die Überprüfung von IPv4-Paketen fehlgeschlagen ist.

Indikatorname in Infrastructure Analytics	Beschreibung
Ungültige L4-Prüfsummen	Erkennt, wenn die Prüfsummenüberprüfung für TCP-Pakete fehlgeschlagen ist.
Erhöhte CPU-Auslastung durch IP-Verschiebung	Erkennt, ob eine große Anzahl von Macs aktualisiert werden muss.
Übermäßige Paketsteuerung	Erkennt hohe Ebenen der Software-Paketsteuerung aufgrund der Verwendung des asymmetrischen RSS-Schlüsseltyps.
Layer-2-Schleife	Erkennt das Vorhandensein von Layer-2-Schleifen im Netzwerk.
Tagged VLAN mismatch	Erkennt, wenn getaggte VLAN-Pakete auf einer nicht markierten Schnittstelle empfangen werden.



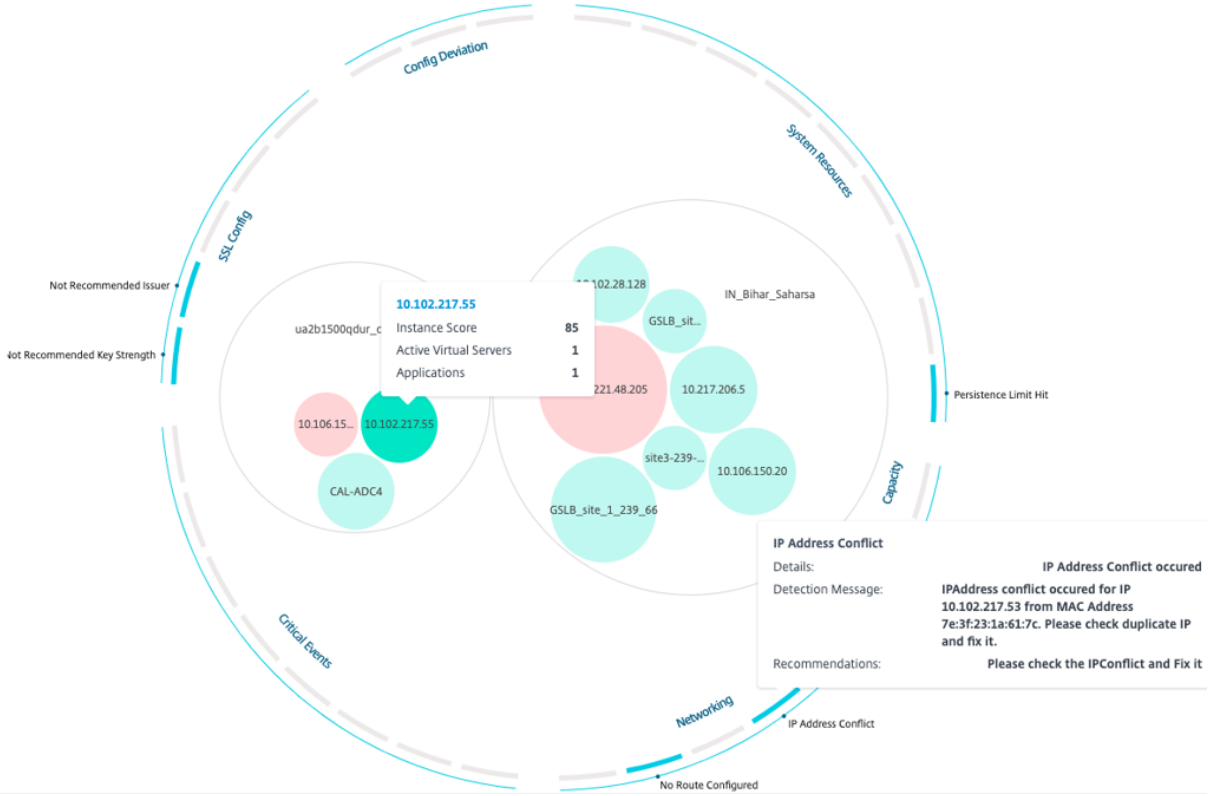
Tabellarische Ansicht

Sie können auch Anomalien anzeigen, indem Sie die Option Tabellenansicht in **Infrastructure Analytics**verwenden. Navigieren Sie zu **Netzwerke** > **Infrastrukturanalyse**, und klicken Sie dann auf , um alle verwalteten Instanzen anzuzeigen. Klicken Sie hier , um Details zu erhalten.



Details einer Anomalie anzeigen

Wenn Sie beispielsweise Details für **IP-Adresskonflikte** im Netzwerk anzeigen möchten, klicken Sie auf die Anomalie, die für IP-Adresskonflikt angezeigt wird.



- **Details** - Gibt an, welche Anomalie erkannt wird
- **Erkennungsnachricht** - Gibt die MAC-Adresse an, für die die IP-Adresse den Konflikt hat
- **Empfehlungen** - Gibt das Verfahren zur Fehlerbehebung an, um diesen IP-Adressenkonflikt zu beheben.

Anleitungsartikel

April 28, 2021

Citrix Application Delivery Management (Citrix ADM) How-to Articles sind einfache, relevante und einfach zu implementierende Artikel zu den Funktionen, die mit dem Service zur Verfügung stehen. Diese Artikel enthalten Informationen zu einigen der beliebten Citrix ADM Funktionen wie Instanzverwaltung, Konfigurationsverwaltung, Ereignisverwaltung, Anwendungsverwaltung, StyleBooks und Zertifikatsverwaltung.

Klicken Sie in der folgenden Tabelle auf einen Feature-Namen, um die Liste der Anleitungsartikel für diese Funktion anzuzeigen.

Artikel		
Instanzverwaltung	Konfigurationsverwaltung	Zertifikatverwaltung
StyleBooks	Event-Management	

Instanzverwaltung

So überwachen Sie global verteilte Standorte

Verwalten von Adminpartitionen von Citrix ADC-Instanzen

Hinzufügen von Instanzen zu Citrix ADM

Erstellen von Instanzgruppen auf Citrix ADM

Abfragen von Citrix ADC-Instanzen und Entitäten in Citrix ADM

Konfigurieren von Sites für Geomaps in Citrix ADM

Erzwingen eines Failovers auf die sekundäre Citrix ADC-Instanz

Wie erzwingen Sie, dass eine sekundäre Citrix ADC-Instanz sekundär bleibt

Ändern eines Citrix ADC MPX- oder VPX-Stammkennworts

Ändern eines Citrix ADC SDX-Stammkennworts

Konfigurationsverwaltung

So verwenden Sie den SCP-Befehl (put) in Konfigurationsaufträgen

Aktualisieren von Citrix ADC SDX-Instanzen mit von Citrix ADM

Planen von Jobs, die mit integrierten Vorlagen in Citrix ADM erstellt wurden

Neuplanung von Jobs, die mit integrierten Vorlagen in Citrix ADM konfiguriert wurden

Wiederverwendung von Ausführungsaufträgen

Aktualisieren von Citrix ADC-Instanzen mithilfe von Citrix ADM

Erstellen eines Konfigurationsauftrags in Citrix ADM

Verwenden von Variablen in Konfigurationsaufträgen auf Citrix ADM

Verwenden von Konfigurationsvorlagen zum Erstellen von Überwachungsvorlagen auf Citrix ADM

Erstellen von Konfigurationsaufträgen aus Korrekturbefehlen in Citrix ADM

Replikation ausgeführter und gespeicherter Konfigurationsbefehle von einer Citrix ADC-Instanz auf eine andere in Citrix ADM

Erstellen von Konfigurationsaufträgen für Citrix SD-WAN WO-Instanzen in Citrix ADM

Verwenden von Konfigurationsaufträgen zur Replikation von Konfiguration von einer Instanz auf mehrere Instanzen

Verwenden der Masterkonfigurationsvorlage in Citrix ADM

Zertifikatverwaltung

Konfigurieren einer Unternehmensrichtlinie auf Citrix ADM

Installieren von SSL-Zertifikaten auf einer Citrix ADC-Instanz von Citrix ADM

Aktualisieren eines installierten Zertifikats von Citrix ADM

Verbinden und Aufheben der Verknüpfung von SSL-Zertifikaten mithilfe von Citrix ADM

Erstellen einer Zertifikatsignieranforderung (CSR) mithilfe von Citrix ADM

Einrichten von Benachrichtigungen für das Ablaufdatum von SSL-Zertifikaten von Citrix ADM

Verwenden des SSL-Dashboards in Citrix ADM

StyleBooks

Verwenden von Standard-StyleBooks in Citrix ADM

So erstellen Sie Ihre eigenen StyleBooks

Verwenden von benutzerdefinierten StyleBooks in Citrix ADM

Verwenden von API zum Erstellen von Konfigurationen aus StyleBooks

Aktivieren von Analysen und Konfigurieren von Alarmen auf einem virtuellen Server, der in einem StyleBook definiert ist

Erstellen eines StyleBook zum Hochladen von SSL-Zertifikats- und Zertifikatsschlüsseldateien in Citrix ADM

Verwenden von Microsoft Skype for Business StyleBook in Unternehmen

Verwenden von Microsoft Exchange StyleBook in Geschäftsunternehmen

Verwenden von Microsoft SharePoint StyleBook in Geschäftsunternehmen

Verwenden von Microsoft ADFS Proxy StyleBook

So verwenden Sie Oracle E-Business StyleBook

Verwenden von SSO Office 365 StyleBook

So verwenden Sie SSO Google Apps StyleBook

Event-Management

Festlegen des Ereignisalters für Ereignisse in Citrix ADM

Planen eines Ereignisfilters mithilfe von Citrix ADM

So legen Sie wiederholte E-Mail-Benachrichtigungen für Ereignisse von Citrix ADM fest

Unterdrücken von Ereignissen mithilfe von Citrix ADM

Verwenden des Ereignis-Dashboards zum Überwachen von Ereignissen

Erstellen von Ereignisregeln in Citrix ADM

Ändern des gemeldeten Schweregrads von Ereignissen, die auf Citrix ADC-Instanzen auftreten

Anzeigen der Ereigniszusammenfassung in Citrix ADM

Anzeigen von Ereignis-Schweregraden und -schiefe von SNMP-Traps auf Citrix ADM

Exportieren von Syslog-Nachrichten mit Citrix ADM

Unterdrücken von Syslog-Nachrichten in Citrix ADM

FAQ

April 28, 2021

Wie viele Agenten muss ich installieren?

Die Anzahl der Agenten hängt von der Anzahl der verwalteten Instanzen in einem Rechenzentrum und vom Gesamtdurchsatz ab. Citrix empfiehlt, mindestens einen Agenten für jedes Rechenzentrum zu installieren.

Wie kann ich mehrere Agenten installieren?

Sie können nur einen Agenten installieren, wenn Sie sich zum ersten Mal beim Dienst anmelden. Um mehrere Agents hinzuzufügen, schließen Sie zuerst die Erstinstallation ab und navigieren Sie zu **Einstellungen** > **Setup-Agents**.

Kann ich von einem integrierten Agenten auf einen externen Agenten umsteigen?

Ja, das kannst du. Weitere Informationen finden Sie unter Übergang von einem integrierten Agenten zu einem externen Agenten.

Wie erhalte ich einen neuen Aktivierungscode, wenn ich ihn verliere?

Wenn Sie zum ersten Mal Onboarding sind, greifen Sie auf die Dienst-GUI zu, navigieren Sie zum Bildschirm **Agent einrichten** und klicken Sie auf **Aktivierungscode generieren**.

Wenn Sie versuchen, einen zweiten Agenten zu installieren, navigieren Sie zum Generieren eines neuen Aktivierungscodes zu **Netzwerke > Agents > Aktivierungscode generieren**.

Wie melde ich mich an der Agent-VM an? Was sind die Standardanmeldeinformationen?

Wenn Ihr Agent auf einem Hypervisor oder Microsoft Azure-Cloud installiert ist, lautet die Standardanmeldeinformationen für den ADM-Dienstagenten `nsrecover`/`nsroot`, der die Shell-Eingabeaufforderung des Agenten öffnet.

Wenn Ihr Agent auf AWS installiert ist, lautet die Standardanmeldeinformationen für die Anmeldung beim Citrix ADM Service Agent`nsrecover`/`instance id`.

Was sind die Ressourcenanforderungen, um einen Agenten on-premises auf einem Hypervisor zu installieren?

32 GB RAM, 8 virtuelle CPU, 500 GB Speicher, 1 virtuelle Netzwerkschnittstellen, 1 Gbit/s Durchsatz

Kann ich zwei Agenten in einem HA-Setup installieren?

Nein, das geht nicht.

Muss ich dem Agenten während der Provisioning einen zusätzlichen Datenträger zuweisen?

Nein, Sie müssen keinen zusätzlichen Datenträger hinzufügen. Der Agent wird nur als Vermittler zwischen Citrix ADM und den Instanzen in Ihrem Unternehmens-Rechenzentrum oder in der Cloud verwendet. Es speichert keine Inventar- oder Analysedaten, für die ein zusätzlicher Datenträger erforderlich wäre.

Kann ich meinen Aktivierungscode mit mehreren Agenten wiederverwenden?

Nein, das geht nicht.

Wie erstelle ich die Netzwerkeinstellungen erneut, wenn ich einen falschen Wert eingegeben habe?

Greifen Sie auf die Agentenkonsole auf Ihrem Hypervisor zu, melden Sie sich mit den Anmeldeinformationen nsrecover/nsroot bei der Shell-Eingabeaufforderung an, und führen Sie dann den Befehl aus `networkconfig`.

Was mache ich, wenn meine Agentenregistrierung fehlschlägt?

- Stellen Sie sicher, dass Ihr Agent Zugriff auf das Internet hat (DNS konfigurieren).
- Stellen Sie sicher, dass Sie den Aktivierungscode korrekt kopiert haben.
- Stellen Sie sicher, dass Sie die Service-URL korrekt eingegeben haben.
- Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind.

Die Registrierung ist erfolgreich, aber woher weiß ich, ob der Agent gut läuft?

Nachdem der Agent erfolgreich registriert wurde, greifen Sie auf Citrix ADM zu, und navigieren Sie zum Bildschirm **Agent einrichten**. Sie können den entdeckten Agenten auf dem Bildschirm sehen. Wenn der Agent einwandfrei läuft, wird ein grünes Symbol angezeigt. Wenn es nicht läuft, erscheint ein rotes Symbol.

Wie kann ich Agents über einen Proxyserver mit Citrix ADM verbinden?

Sie können Agenten über einen Proxy-Server mit dem Citrix ADM-Dienst verbinden. Die Agenten leiten alle ihre Daten an den Proxyserver weiter, der die Daten dann über das Internet an das Citrix ADM sendet.

Um Daten über den Proxyserver weiterzuleiten, geben Sie die Proxy-Serverdetails auf dem Agenten mithilfe des folgenden Skripts ein: proxy_input.py, und folgen Sie den Anweisungen des Skripts, um weitere Informationen einzugeben. Der Agent ruft diese Informationen ab, während er über den Proxyserver eine Verbindung mit Citrix ADM herstellt.

Sie können Ihren Proxy-Server authentifizieren, indem Sie Ihren Benutzernamen und Ihr Kennwort angeben. Wenn der Agent die Daten sendet, authentifiziert der Proxyserver die Anmeldeinformationen des Benutzers, bevor er sie an Citrix ADM weiterleitet.

> **Hinweis**
>
> Proxy-Server unterstützt nur die grundlegende Authentifizierung.

Meine Analytics-Berichte werden nicht angezeigt

Aktivieren Sie Insight auf Ihren virtuellen Servern, um die Analytics-Berichte anzuzeigen. Einzelheiten finden Sie unter Analytics aktivieren.

Welche Versionen von Citrix ADC-Instanzen werden in Citrix ADM unterstützt?

Für Verwaltungs- und Überwachungsfunktionen werden Citrix ADC-Instanzen mit 10.5 und höher unterstützt. Einige Funktionen werden nur bei bestimmten Citrix ADC Versionen unterstützt. Einzelheiten finden Sie unter Systemanforderungen.

Wie exportiere ich Dashboard-Berichte in Citrix ADM?

Um den Bericht eines beliebigen Dashboards in Citrix ADM zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** aus. Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
   Der Bericht wird auf Ihr System heruntergeladen.
2. Wählen Sie **Bericht planen**, um Zeitpläne für das Generieren und Exportieren von Berichten in regelmäßigen Abständen einzurichten. Geben Sie die Einstellungen für die Berichtsgenerierung an, und erstellen Sie ein E-Mail-Profil, in das der Bericht exportiert wird.
   a) **Wiederholung** - Wählen Sie **Täglich**, **Wöchentlich** oder **Monatlich** aus dem Dropdownlistenfeld aus.

      > **Hinweis**
      >
      > - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
      > - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

   b) **Wiederholzeit** - Geben Sie die Zeit wie `Hour : Minute` im 24-Stunden-Format ein.
   c) **E-Mail** - Aktivieren Sie das Kontrollkästchen, und wählen Sie dann das Profil aus dem Dropdownlistenfeld aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.
   d) **Slack** - Aktivieren Sie das Kontrollkästchen, und wählen Sie dann das Profil aus dem Dropdownlistenfeld aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

   Klicken Sie auf **Zeitplan aktivieren**, um den Bericht zu planen, und klicken Sie dann auf **OK**. Wenn Sie auf das Kontrollkästchen **Zeitplan aktivieren** klicken, können Sie die ausgewählten Berichte erstellen.

Was bewirkt die Aktivierung clientseitiger Messungen?

Bei aktivierten clientseitigen Messungen erfasst ADM über HTML-Injection Ladezeit und Rendering-Zeit-Metriken für HTML-Seiten. Mit diesen Metriken können Administratoren Probleme mit der L7-Latenz identifizieren.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States