NetScaler Application Delivery Management 14.1

Machine translated content

Disclaimer

Contents

Versionshinweise

February 5, 2024

In den Versionshinweisen zu NetScaler Application Delivery Management (ADM) 14.1 werden die neuen Funktionen, Verbesserungen vorhandener Funktionen und die bekannten Probleme in einem Build beschrieben. Das Release Notes Dokument für die Version 14.1 enthält die folgenden Abschnitte:

- **Neuerungen**: Die neuen Funktionen und Verbesserungen bestehender Features, die in einem Build veröffentlicht wurden.
- **Bekannte Probleme**: Die Probleme, die in einem Build bestehen, und deren Problemumgehungen, wo immer zutreffend.
- **Behobene Probleme**: Die in einem Build behandelten Probleme.

> **Hinweis**
>
> Diese Versionshinweise dokumentieren keine sicherheitsrelevanten Korrekturen. Eine Liste sicherheitsbezogener Fixes und Empfehlungen finden Sie im Security Bulletin.

Versionshinweise für NetScaler ADM 14.1-12.34 Build

February 5, 2024

In diesem Dokument mit Versionshinweisen werden die Verbesserungen und Änderungen sowie die behobenen und bekannten Probleme beschrieben, die für die NetScaler ADM-Version Build 14.1-12.34 bestehen.

Hinweise

- Dieses Dokument mit den Versionshinweisen enthält keine sicherheitsrelevanten Fixes. Eine Liste mit sicherheitsrelevanten Fixes und Hinweisen finden Sie im Citrix Security Bulletin.
- Build 14.1-12.34 ersetzt Build 14.1-12.30.
- Build 14.1-12.34 enthält eine neue Funktion NSADM-98483 und ein bekanntes Problem NSADM-106497 sowie alle Verbesserungen und Bugfixes, die in Build 14.1-12.30 verfügbar sind.

Was ist neu

Die Verbesserungen und Änderungen, die in Build 14.1-12.34 verfügbar sind.

Lizenzierung

NetScaler Flexed-Lizenzierung NetScaler Flected Licensing ist das neue Lizenzierungsframework, das darauf abzielt, den Lizenzverwaltungsprozess zu vereinfachen. Ihre Flexed-Lizenz umfasst Softwareinstanzlizenzen (VPX/CPX/BLX, SDX, MPX und VPX FIPS) und Bandbreitenkapazitätslizenzen. Sie müssen die Flexed-Lizenzen im NetScaler Console Service oder NetScaler ADM vor Ort anwenden. Sie müssen auch die MPX Z-Cap- und SDX Z-Cap-Lizenz auf NetScaler MPX-Hardware bzw. NetScaler SDX-Hardware anwenden. Sie können sie dann allen NetScaler-Formfaktoren zuweisen, die in der Cloud oder vor Ort bereitgestellt werden.

Weitere Informationen finden Sie unter
Flexed-Lizenz .

Flexed-Lizenzen werden in den NetScaler ADM On-Prem-Versionen 14.1 und 13.1 offiziell unterstützt. In Version ADM on-prem 14.1-12.x und höher sind gebündelte Berechtigungen für eine unbegrenzte Anzahl von ADM-VIPs für Analysen verfügbar, und Sie können Flexed-Lizenzen über die Flexed-Dashboard-Benutzeroberfläche verwalten (**NetScaler Licensing > Flected Licensing**).

Wenn Sie Flexed-Lizenzen für ADM-Builds der Versionen 13.1 und 14.1 vor 14.1-12.x anwenden, behandelt ADM diese genauso wie gepoolte Lizenzen und zeigt die Details in der Benutzeroberfläche des gepoolten Dashboards an (**Infrastruktur > Pooled Licensing**). Ein gebündelter Anspruch auf eine unbegrenzte Anzahl von ADM-VIPs für Analysen ist in diesen Versionen nicht verfügbar.

Für ein besseres Produkterlebnis mit der Flexed-Benutzeroberfläche und dem Angebot gebündelter Berechtigungen empfehlen wir, dass Sie Ihr ADM vor Ort auf Version 14.1-12.x oder höher aktualisieren.

> **Hinweis:**
>
> Um die aktuellen Flexed-Lizenzanforderungen zu erfüllen , aktivieren Sie bitte den ADM On-Prem Cloud Connector. Diese Funktion verbindet Ihren lokalen ADM mit dem ADM Service für die Telemetrieerfassung. Wir empfehlen, die Telemetrieerfassung zu aktivieren, wenn Sie die Flexed-Lizenzierung verwenden. Informationen zum Aktivieren von ADM On-Prem Cloud Connector finden Sie unter ADM On-Prem Cloud Connector.

[NSADM-98483]

Analytics

Erkennung von Anomalien in wichtigen Anwendungskennzahlen Als Administrator müssen Sie sicherstellen, dass Ihre Anwendungen effizient verwaltet werden, um Erkenntnisse für eine bessere Priorisierung und Problembehebung zu erhalten. In einigen Szenarien möchten Sie möglicherweise auch die ungewöhnliche Abweichung der Anwendungsleistung anzeigen und analysieren, die für einen bestimmten Zeitraum auftreten kann.

Wenn Sie im **App-Dashboard** eine Anwendung auswählen, können Sie auf der Registerkarte **Wichtige Kennzahlen** sehen, wie Ihre Anwendungen genutzt werden. NetScaler ADM überwacht das Verkehrsmuster und analysiert, ob die wichtigsten Metriken im erwarteten Bereich liegen. Sie können jetzt Anomalien für die folgenden wichtigen Kennzahlen anzeigen, wenn Abweichungen vom erwarteten Bereich vorliegen:

- Reaktionszeit
- Durchsatz
- Datenvolume
- Anfragen pro Sekunde

Weitere Informationen finden Sie unter Anwendungsnutzung und Anomalien

[NSADM-97531]

Daten nur von ausgewählten Instanzen nach Splunk und New Relic exportieren Wenn Sie ein Abonnement für den Export von Daten nach Splunk und New Relic erstellen, können Sie jetzt Instanzen auswählen. Wenn Sie ein Abonnement mit bestimmten Instanzen erstellen, werden die Daten nur von den ausgewählten Instanzen nach Splunk und New Relic exportiert.

Weitere Informationen finden Sie unter Integration mit Splunk und Integration mit New Relic.

[NSADM-94371]

Umsetzbare Aufgaben und Empfehlungen Die folgenden Verbesserungen wurden der **Aufgabenfunktion** jetzt hinzugefügt:

- Ein neuer **Aufgaben-Tab** wird eingeführt, auf dem Sie umsetzbare Aufgaben sehen können, die Ihre sofortige Aufmerksamkeit erfordern. Diese Aufgaben werden basierend auf Ihrer aktuellen Auslastung angezeigt. Als Administrator stellen Sie durch die Erledigung dieser umsetzbaren Aufgaben sicher, dass Ihre NetScaler-Bereitstellung sicher, konform und effizient ist. Diese umsetzbaren Aufgaben richten sich nach dem Schweregrad der Probleme (kritisch und mittel).
- Die Registerkarte „ **Aufgaben** “wurde in **Empfehlungen**umbenannt. Unter **Empfehlungen**können Sie die vorhandenen Aufgaben weiterhin überprüfen und auf **Anleitung klicken,** um die Aufgabe abzuschließen.
- Die Registerkarte **Archiv** ist nicht mehr verfügbar. Stattdessen können Sie eine Empfehlung aus der Liste **verwerfen** .

Weitere Informationen finden Sie unter Umsetzbare Aufgaben und Empfehlungen.

[NSADM-91870]

Infrastruktur

Verwenden Sie den Zertifikatsspeicher, um SSL-Zertifikate zu aktualisieren Wenn Sie ein SSL-Zertifikat unter **Infrastruktur > SSL-Dashboard > Aktualisieren aktualisieren,** können Sie das Zertifikat jetzt aus dem Zertifikatsspeicher auswählen. Zuvor mussten Sie die Zertifikatsdatei und die Schlüsseldatei hochladen, um ein SSL-Zertifikat zu aktualisieren.

Weitere Informationen finden Sie unter So aktualisieren Sie ein installiertes Zertifikat.

[NSADM-101303]

Scan-Log-Unterstützung im Security Advisory **In der Sicherheitsempfehlung können Sie jetzt eine neue Option namens **Scan Log** anzeigen. Mithilfe des **Scan-Protokolls** können Sie:

- Sehen Sie sich den Bericht der letzten fünf CVE-Scans an. Der Bericht umfasst sowohl den Standardsystemscan als auch den benutzerinitiierten Scan auf Anforderung.
- Laden Sie den Bericht jedes Scans im CSV- und PDF-Format herunter.
- Zeigen Sie den Status des gerade laufenden Scans auf Anforderung an.

Weitere Informationen finden Sie unter Sicherheitsempfehlung.

[NSADM-101142]

Aktualisierte Liste der SNMP-Traps Die Liste der SNMP-Traps wurde jetzt mit neuen Traps sowie einigen zuvor fehlenden Traps aktualisiert. Um die vollständige Liste anzuzeigen, navigieren Sie zu **Infrastruktur > Ereignisse > Ereigniseinstellungen > NetScaler**.

[NSADM-99798]

Verwaltung benutzerdefinierter Datenbankzertifikate und Chiffren in einer HA-Bereitstellung Mit NetScaler ADM können Sie jetzt die integrierten Standarddatenbankzertifikate durch Ihre eigenen Zertifikate einer vertrauenswürdigen Zertifizierungsstelle ersetzen. Sie können auch Ihre eigenen Cipher Suites für die ADM-Datenbank konfigurieren. Um diese Funktion zu verwenden, navigieren Sie zu **Einstellungen > HA-Bereitstellung > Datenbankzertifikate**.

Weitere Informationen finden Sie unter Verwalten von benutzerdefinierten Datenbankzertifikaten und Verschlüsselungen in einer Hochverfügbarkeitsbereitstellung.

[NSADM-96583]

Austausch von Abonnementlizenzinformationen zwischen ADM on-premises und ADM Service Der on-premises ADM-Server sendet jetzt NetScaler-Abonnementlizenzinformationen über den ADM On-Prem Cloud Connector an den ADM Service.

[NSADM-93820]

Gemeinsame Nutzung von gepoolten Lizenzinformationen zwischen ADM on-premises und ADM Service Der on-premises ADM-Server sendet jetzt die gepoolten NetScaler-Lizenzinformationen über den ADM On-Prem Cloud Connector an den ADM Service.

[NSADM-93812]

Sicherheit

Einheitliches Sicherheitsdashboard In NetScaler ADM können Sie jetzt ein Dashboard mit nur einem Bereich verwenden, um Schutzmaßnahmen zu konfigurieren, Analysen zu aktivieren und sie in Ihren Anwendungen bereitzustellen. Navigieren Sie zu **Sicherheit > Sicherheitsdashboard** und klicken Sie dann auf **Anwendung verwalten**, um:

- Sehen Sie sich alle gesicherten und ungesicherten Anwendungen an.
- Wählen Sie eine ungesicherte Anwendung aus, konfigurieren Sie Schutzmaßnahmen aus verschiedenen Vorlagenoptionen, aktivieren Sie Analysen für die Schutzmaßnahmen und stellen Sie sie in Ihrer Anwendung bereit, um die Anwendung zu sichern.

Zuvor mussten Sie alle Schutzmaßnahmen in den NetScaler-Instanzen konfigurieren und konnten nur Analysen für die konfigurierten Schutzmaßnahmen in NetScaler ADM anzeigen. Als Administrator können Sie mit diesem Dashboard in einem einzigen Bereich Schutzmaßnahmen für die Anwendung in einem einzigen Arbeitsablauf konfigurieren.

Weitere Informationen finden Sie unter Einheitliches Sicherheitsdashboard.

[NSADM-92678]

StyleBooks

Verwenden Sie Zertifikate aus dem NetScaler ADM-Zertifikatsspeicher in StyleBooks Sie können StyleBooks jetzt so definieren, dass Zertifikate aus dem NetScaler ADM-Zertifikatsspeicher verwendet werden. Beim Erstellen von Konfigurationspaketen können Sie Zertifikate auswählen, die bereits im Zertifikatsspeicher vorhanden sind, oder neue Zertifikate zum Zertifikatsspeicher hinzufügen.

Weitere Informationen finden Sie unter Verwalten von SSL-Zertifikaten aus dem Zertifikatsspeicher mit StyleBooks.

[NSADM-101515]

Definieren Sie ein Drop-down-Menü in StyleBooks Mit NetScaler ADM können Sie jetzt ein Dropdownmenü in den ‘Parameterbedingungen’der StyleBook-Definition definieren.

Weitere Informationen finden Sie unter Parameterbedingungen.

[NSADM-99543]

Laden Sie Support-Pakete für StyleBooks und Konfigurationspakete herunter Sie können jetzt ein Support-Paket zur Fehlerbehebung bei Config-Pack- oder StyleBook-Vorgängen herunterladen. Sie können diese Support-Pakete mit dem NetScaler-Team teilen, wenn Sie ein Support-Ticket für StyleBooks öffnen. Um ein Support-Paket herunterzuladen, navigieren Sie zu **Applications > Configuration > Config Packs > Support Bundles**.

Weitere Informationen finden Sie unter Laden Sie das Support-Paketherunter.

[NSADM-97838]

Ändern Sie den Status und den ARP-Status virtueller Server in StyleBooks Unter **Anwendungen > Konfiguration > Config Packs > NetScaler-Konfiguration migrieren**können Sie jetzt den Status (Aktiviert/Deaktiviert) und den ARP-Status aller virtuellen Server anzeigen und bearbeiten, die zu einem neuen NetScaler migriert wurden.

Weitere Informationen finden Sie unter Erstellen eines StyleBook zur Migration der NetScaler-Anwendungskonfiguration.

[NSADM-97827]

Konfigurationen ohne Konfigurationspaket migrieren NetScaler ADM bietet jetzt die Option, Anwendungskonfigurationen zwischen NetScalern zu migrieren, ohne ein Konfigurationspaket in NetScaler ADM zu erstellen. Standardmäßig erstellt die Migration ein Konfigurationspaket auf ADM, das zur weiteren Verwaltung der Konfiguration über StyleBooks verwendet wird. Wenn Sie die Anwendungskonfiguration nur von einem NetScaler zu einem anderen migrieren möchten, ohne sie anschließend über StyleBooks zu verwalten, deaktivieren Sie das Kontrollkästchen **Konfiguration über ADM verwalten während der** Migration unter **Anwendungen > Konfigurationen > Config Packs > NetScaler-Konfiguration migrieren > Migrieren**.

Weitere Informationen finden Sie unter Migrieren der NetScaler-Anwendungskonfiguration mit StyleBooks ConfigurationBuilder.

[NSADM-97802]

Behobene Probleme

Die Probleme, die in Build 14.1-12.34 behoben wurden.

Analytics

- Manchmal stürzt der NetScaler ADM Agent nach einem Upgrade ab und generiert Core-Dump-Dateien.

  [NSHELP-36428]

Infrastruktur

- Unter bestimmten Bedingungen können die auf einige Benutzergruppen angewendeten Regex-Konfigurationen verloren gehen.

  [NSADM-104565]

- Wenn Sie **unter Infrastructure > Instance Advisory > Security Advisory**eine anfällige NetScaler-Instanz mit einem CVE auswählen und auf Proceed **to Upgrade-Workflow**klicken, wird die folgende Fehlermeldung angezeigt:

  „Für die ausgewählte NetScaler-Instanz ist dieser Behebungsworkflow nicht erforderlich“

  [NSADM-103649]

- Unter **Infrastruktur > Ereignisse > Ereignismeldungen**zeigt NetScaler ADM nicht an, ob die NetScaler-CPU-Auslastungs-Traps für die Paket-CPU oder die Management-CPU bestimmt sind.

  [NSADM-103391]

- Wenn NetScaler ADM auf einem Kubernetes-Cluster installiert ist, werden bestimmte Seiten, wie **Infrastructure Analytics**, **Events,**Syslog Events****und **Data Storage Management**, möglicherweise nicht in der NetScaler ADM GUI angezeigt.

  [NSADM-103180]

- Wenn ein Bericht von einer scrollbaren Seite in NetScaler ADM exportiert wird, schneidet der exportierte Bericht möglicherweise Inhalte ab, die über die Höhe des sichtbaren Fensters hinausreichen.

  [NSADM-102765]

- In skalierten Bereitstellungen wird ein Absturz des mas_service-Subsystems beobachtet.

  Dieses Problem tritt auf, wenn Sie über RBAC-Berechtigungen verfügen und einer Gruppe angehören, die unter **Einstellungen > Benutzer und Rollen > Gruppe > Autorisierungseinstellungen**die folgenden Konfigurationen hat:

  - Eine bestimmte Instanz wird in **Instances**ausgewählt
  - **Alle Anwendungen** ist unter **Anwendungen**ausgewählt

  [NSADM-99873]

- Wenn Sie sich als Root-Administrator zum ersten Mal mit Standardanmeldeinformationen bei der NetScaler ADM GUI oder API anmelden, werden Sie aufgefordert, das Standardkennwort zu ändern.

  [NSADM-95328]

Verwaltung und Überwachung

- Wenn ein RBAC-Benutzer eine NITRO-API-Anfrage an NetScaler ADM sendet, um die Liste der NetScaler-Server abzurufen, gibt die Antwort fälschlicherweise keine verfügbaren Server an. Wenn Sie jedoch zur NetScaler ADM GUI navigieren (**Infrastruktur > Netzwerkfunktionen > Load Balancing > Server**), werden alle mit diesem Benutzer verknüpften NetScaler-Server angezeigt.

  [NSHELP-36645]

- Der NetScaler ADM-Wiederherstellungsvorgang **unter Einstellungen > Sicherungsdateien > Wiederherstellen** kann zeitweise nicht abgeschlossen werden.

  [NSHELP-36527]

- NetScaler ADM kann bestimmte Kerndateien nicht komprimieren, was zu einem erhöhten Speicherplatzverbrauch führt.

  [NSHELP-36434]

- Wenn ein Administrator eine Gruppe mit Zugriff auf alle Anwendungen erstellt und ein Benutzer, der zu dieser Gruppe gehört, versucht, auf die Seite **Infrastruktur > Netzwerkfunktionen > Load Balancing > Server** zuzugreifen, kann auf die NetScaler ADM GUI nicht mehr zugegriffen werden.

  [NSHELP-36426]

- Während der Synchronisation von Dateien zwischen primären und sekundären Knoten im NetScaler ADM HA-Setup stürzt das Inventarsubsystem zeitweise ab.

  [NSHELP-36357]

- In den integrierten NetScaler-Agenten werden keine Ereigniswarnungen oder -meldungen generiert, auch wenn das Ereignisalter die unter **Infrastruktur > Ereignisse > Regeln > Hinzufügen**festgelegte Dauer überschreitet.

  [NSHELP-35706]

- Wenn Sie eine VPX-Instanz auf SDX unter **Infrastruktur > Instanzen > NetScaler > SDX > Aktion auswählen > VPX bereitstellen bereitstellen**, wird die Option **Über Netzwerk verwalten** nicht angezeigt.

  [NSHELP-36328]

StyleBooks

- Die NetScaler ADM StyleBook-Protokolldateien werden auch nach Überschreitung der Dateigrößenbeschränkung nicht automatisch komprimiert, was zu einem erhöhten Speicherplatzverbrauch führt.

  [NSHELP-36680]

- Wenn Konfigurationspakete mit Sonderzeichen in ihren Parametern aktualisiert oder gelöscht werden, zeigt NetScaler ADM trotz unvollständiger Aktualisierungs- oder Löschvorgänge auf NetScaler eine Erfolgsmeldung an. Mit diesem Fix zeigt NetScaler ADM jetzt korrekt Fehler für unvollständige Konfigurationen an, die auf Sonderzeichen in der Konfigurationspaket-Definition zurückzuführen sind.

  [NSADM-104423]

Bekannte Probleme

Die Probleme, die in Version 14.1-12.34 bestehen.

Analytics

- Wenn Sie unter **Anwendungen > Dashboard**auf eine Anwendung klicken, die auf dem NetScaler HA-Paar gehostet wird, werden auf der Registerkarte **Leistung** auf der Seite mit den Anwendungsdetails keine Daten unter **Alle**Dienste angezeigt.

  Problemumgehung: Aktualisieren Sie die Seite oder wechseln Sie zu einer anderen Registerkarte auf der Seite mit den Anwendungsdetails und kehren Sie dann zur Registerkarte **Leistung** zurück, um die Dienste anzuzeigen, die dem virtuellen Lastausgleichsserver zugeordnet sind.

  [NSADM-105613]

Infrastruktur

- Das Flexed-Lizenz-Dashboard zeigt NetScaler-Details erst an, nachdem mindestens ein NetScaler aus dem Premium-Bandbreiten-Lizenzpool ausgecheckt wurde.

  [NSADM-106497]

- Wenn Lizenzen aus NetScaler ADM für VMware ESXi gelöscht werden, spiegelt die Lizenzanzahl **unter Einstellungen > Lizenzierungs- und Analysekonfiguration** möglicherweise nicht sofort die aktualisierte Anzahl wider.

  [NSADM-105851]

- Der Differenzbericht wird nicht für einen Upgrade-Job unter **Infrastruktur > Upgrade-Jobs > Vergleichsberichte** generiert.

  [NSADM-106777]

- Nachdem ein neues NetScaler ADM konfiguriert wurde, wird möglicherweise die folgende Fehlermeldung angezeigt: "Fehler im Betrieb —Metriken nicht gefunden".

  Dieses Problem tritt auf, weil der automatische Datenlöschauftrag noch nicht ausgeführt wurde, was dazu führt, dass keine Daten vorhanden sind. Die Ausführung des Jobs ist für 3 Stunden geplant. Nach der Ausführung werden die erforderlichen Daten generiert, und die Fehlermeldung wird nicht mehr angezeigt.

  [NSADM-103157]

- Wenn Sie versuchen, ein Zertifikat auf einer NetScaler BLX-Instanz zu installieren, schlägt die Installation fehl und auf der Seite **Infrastruktur > SSL-Dashboard > SSL-Auditprotokolle** wird die folgende Fehlermeldung angezeigt:

  "SCP: Authentication by password fails on *ip-address*."

  [NSADM-102202]

- Der NetScaler Agent wird nicht bei NetScaler ADM registriert, wenn eines seiner Kennwörter ein #-Symbol hat.

  [NSADM-100613]

Lizenzierung

- Nachdem die Flexing- oder Pooled-Lizenz angewendet wurde, wird die Seite **Analytics-Konfiguration** (**Einstellungen > Analytics-Konfiguration**) nicht mit den richtigen Details aktualisiert.

  Workaround: Aktualisieren Sie die Seite, um die richtigen Details abzurufen.

  [NSADM-106665]

- Das Flexed-Lizenz-Dashboard unter **NetScaler Licensing > Flected Licensing > Dashboard** wird leer angezeigt.

  Workaround: Wenden Sie eine Premium-Bandbreitenlizenz an.

  [NSADM-106561]

Verwaltung und Überwachung

- Der NetScaler ADM Agent generiert SNMP-Traps vom Typ „NetScalerLoginFailure". Dieses Problem tritt auf, weil die Anmeldeinformationen, die der ADM-Agent für die Anmeldung bei

NetScaler verwendet, aufgrund eines Zeilenumbruchs gekürzt werden.

[NSHELP-36804]

- In einem ADM-HA-Paar wurde festgestellt, dass sich der Datenbankstatus im Status Nicht **verfügbar** befindet und nicht synchronisiert wird, selbst nachdem mehrere Versuche mit der Option **Datenbank synchronisieren** in der GUI versucht wurden.

  [NSHELP-29626]

Versionshinweise für NetScaler ADM 14.1—8.50

February 5, 2024

In diesem Dokument mit den Versionshinweisen werden die Erweiterungen und Änderungen sowie die behobenen und bekannten Probleme beschrieben, die für die NetScaler ADM-Version Build 14.1—8.50 bestehen.

Hinweise

- Dieses Dokument mit den Versionshinweisen enthält keine sicherheitsrelevanten Fixes. Eine Liste mit sicherheitsrelevanten Fixes und Hinweisen finden Sie im Citrix Security Bulletin.

Was ist neu

Die Erweiterungen und Änderungen, die in Build 14.1—8.50 verfügbar sind.

Verwaltung und Überwachung

Unterstützung bei der Identifizierung und Behebung von CVE-2023-4966 und CVE-2023-4967

> **Hinweis:**
>
> Sie können die CVE-2023-4966- und CVE-2023-4967-Details nur anzeigen, wenn Sie Security Advisory über ADM On-Prem Cloud Connector aktiviert haben. Weitere Informationen finden Sie unter ADM On-Prem Cloud Connector

NetScaler ADM Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2023-4966 und CVE-2023-4967.

- Die Identifizierung erfordert eine Kombination aus Versions- und Konfigurationsscan.

- Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der das Update enthält.

> **Hinweis:**
>
> Die Sicherheitsempfehlung unterstützt keine NetScaler-Builds, die das Ende des Lebenszyklus (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

Weitere Informationen zur Verwendung von NetScaler ADM zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Jobszum Upgrade von NetScaler-Instanzen.

Weitere Informationen finden Sie im Sicherheitsbulletin.

[NSADM-101092]

Analytics

Unterstützung für die Konfiguration des Exports von Metriken von NetScaler nach Prometheus über StyleBook Um Metriken von NetScaler nach Prometheus zu exportieren, müssen Sie in NetScaler ein Analyseprofil erstellen und die Schemadatei angeben. Weitere Informationen finden Sie unter NetScaler, Anwendungen und Anwendungssicherheit mit Prometheus überwachen.

Unter **Anwendungen > Konfiguration > Stylebooks > Standard-Stylebook** können Sie jetzt das StyleBook **Prometheus TimeSeries Analytics Configuration** verwenden und die Konfiguration für alle verwalteten Instanzen ausführen.

Weitere Informationen finden Sie unter Prometheus Analytics StyleBook.

[NSADM-97698]

Die Hauptursache für Anwendungslatenz anzeigen Anwendungsverlangsamung ist ein wichtiges Anliegen für jede Organisation, da dies zu geschäftlichen Auswirkungen oder Produktivität führt. Unter **Anwendungen > Web Insight**können Sie jetzt eine neue Metrik mit dem Namen **Anwendungen mit Reaktionszeitanomalien**anzeigen. Mithilfe dieser Metrik können Sie als Administrator analysieren, ob die Anwendungslatenz auf die folgenden Ursachen zurückzuführen ist:

- Netzwerklatenz des Clients
- Servernetzwerklatenz
- Verarbeitungszeit des Servers

Weitere Informationen finden Sie unter Anzeigen der Hauptursache für Anwendungslatenz.

[NSADM-97530]

Konfigurationsjob —Unterstützung für die Erstellung eines Jobs für die Konfiguration des Exports von Metriken von NetScaler nach Prometheus Um Metriken von NetScaler nach Prometheus zu exportieren, müssen Sie in NetScaler ein Analyseprofil erstellen und die Schemadatei angeben. Weitere Informationen finden Sie unter NetScaler, Anwendungen und Anwendungssicherheit mit Prometheus überwachen.

In **Configuration Job**können Sie jetzt einen Job mit der **NSConfigurePrometheusAnalyticsProfile-Vorlage** aus der **integrierten Vorlage**erstellen, die erforderlichen Parameter angeben und den Job für alle verwalteten Instanzen ausführen.

Weitere Informationen finden Sie unter Planen von Aufträgen, die mithilfe integrierter Vorlagen erstellt wurden.

[NSADM-97251]

Weisen Sie dem verwalteten NetScaler von NetScaler ADM ein Netzprofil zu Wenn Sie Analysen für die virtuellen Server in NetScaler ADM aktivieren, werden die AppFlow-Daten vom NetScaler über die NetScaler-Subnetz-IP-Adresse (SNIP) nach NetScaler ADM exportiert. In einigen Szenarien kann das SNIP aufgrund der Firewall im Netzwerk blockiert werden. In solchen Szenarien müssen Sie möglicherweise eine andere IP-Adresse als die SNIP verwenden. Weitere Informationen zum Netzprofil finden Sie unter Verwenden einer angegebenen Quell-IP für die Back-End-Kommunikation.

Sie können jetzt über NetScaler ADM Netzprofile einer NetScaler-Instanz zuweisen. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler ADC**, wählen Sie die Instanz aus, und klicken Sie in der Liste **Aktion auswählen** auf **Netzwerkprofile konfigurieren**, um der Instanz ein Netzprofil zuzuweisen.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie die Analyse auf allen virtuellen Servern deaktiviert haben, bevor Sie der Instanz ein Netzprofil zuweisen.

Mit dieser Erweiterung können Sie ein Netzprofil für den Export von AppFlow-Daten von NetScaler nach NetScaler ADM zuweisen.

[NSADM-91836]

Infrastruktur

Verbesserungen des Upgrade-Fehlerszenarios Wenn ein Upgrade-Job (**Infrastruktur > Upgrade-Jobs**) fehlschlägt, führt der fehlgeschlagene Job aufgrund des Vorhandenseins der Build-Dateien und anderer extrahierter Dateien zu Speicherplatzproblemen. Infolgedessen schlägt auch der nächste Upgrade-Job fehl.

Das Fehlschlagszenario für Upgrade-Jobs wurde jetzt verbessert. Wenn ein Upgrade-Job fehlschlägt, entfernt NetScaler ADM die alte Build-Datei aus der NetScaler-Instanz.

[NSADM-97383]

Änderungen beim Rebranding NetScaler ADM wurde jetzt in NetScaler ADM umbenannt. Um dem neuen Branding gerecht zu werden, wurde auch die ADM-GUI aktualisiert.

[NSADM-97365]

Zugriffsrichtlinie für Agenten vor Ort Wenn Sie **unter Einstellungen > Benutzer und Rollen > Zugriffsrichtlinien** eine **Zugriffsrichtlinie** mit **Bearbeitungszugriff**für ADM-Agenten erstellen, können die mit dieser Richtlinie verknüpften Benutzer den Agenten jetzt mit ihren Anmeldeinformationen registrieren.

[NSADM-97337]

Datenspeichermanagement-Dashboard in der NetScaler ADM-GUI verfügbar Unter **Einstellungen > Datenspeicherverwaltung**können Sie jetzt die Datenspeicherinformationen für die verschiedenen Funktionen in Ihrer aktuellen Bereitstellung anzeigen und verwalten. Das Data Storage Management-Dashboard hilft Ihnen zu visualisieren, wie der Speicherplatz in den einzelnen Funktionen genutzt wird, und hilft Ihnen zu überwachen, ob der Speicherverbrauch innerhalb des angegebenen Schwellenwerts liegt.

Das Dashboard bietet die folgenden Funktionen:

- Kacheln für**Datenaufnahme, Speicherverbrauch**und **Aktionen** : Die Kacheln bieten Ihnen:
  - Status der Datenaufnahmeaktivität
  - Informationen über Ihre verbrauchten Daten und den gesamten verfügbaren Festplattenspeicher
  - Optionen zur Überprüfung der Datenaufbewahrungsrichtlinie, zur Datenbereinigung und zur Überprüfung Ihrer Systembenachrichtigungen
- **Trend zum Speicherverbrauch**: Hilft Ihnen zu visualisieren, wie die Daten in den verschiedenen Funktionen über einen bestimmten Zeitraum gespeichert werden
- **Speicherverbrauch nach Funktionen**:
  - Zeigt die Verteilung des Datenspeichers nach verschiedenen Funktionen an
  - Ermöglicht das Ausführen von Datenlöschungen, das Anzeigen des Verlaufs von Datenlöschungen und das Anzeigen der Funktionen, die in den einzelnen Datenlöschungen entfernt wurden

Weitere Informationen finden Sie unter Verwenden des Datenspeicher-Dashboards.

[NSADM-97320]

Unterstützung für den SSL-Zertifikatsspeicher in NetScaler ADM Sie können Ihre SSL-Zertifikate jetzt unter **Infrastruktur > SSL-Dashboard > Zertifikatsspeicher**verwalten.

Verwenden Sie den **Zertifikatsspeicher** für:

- Zertifikate hinzufügen, aktualisieren und löschen
- Zertifikate auf NetScaler-Instanzen installieren
- Zertifikate aus NetScaler-Instanzen importieren

Weitere Informationen finden Sie unter So verwenden Sie den Zertifikatsspeicher.

[NSADM-97257]

Das Limit für Benutzersitzungen wurde auf 40 geändert Unter **Einstellungen > Benutzer und Rollen > Gruppen**können Sie bis zu 40 Benutzersitzungen konfigurieren. Standardmäßig sind Ihnen 20 Benutzersitzungen zugewiesen. Wenn Sie jedoch zu den Benutzergruppen Admin und Read-Only gehören, werden Ihnen standardmäßig 40 Benutzersitzungen zugewiesen, und dieser Wert kann nicht geändert werden.

[NSADM-95314]

Fehlgeschlagene Upgrade-Jobs erneut versuchen Unter **Infrastruktur > Upgrade-Jobs** können Sie jetzt den fehlgeschlagenen Upgrade-Job auswählen und eine der folgenden Aktionen ausführen:

- Klicken Sie neben dem fehlgeschlagenen Upgrade-Job auf **Erneut versuchen**.
- Gehen Sie zu **Aktion auswählen > Upgrade-Job erneut versuchen**.

Weitere Informationen finden Sie unter Fehlgeschlagene Upgrade-Jobs erneut versuchen.

[NSADM-93439]

ADM On-Prem Cloud Connector Sie können die Cloud Connector-Funktion verwenden, um eine Verbindung zwischen ADM On-Prem und dem ADM Service herzustellen. Diese Konnektivität ermöglicht es Ihnen, die Security Advisory-Funktion in ADM On-Prem zu nutzen. Mit Security Advisory können Sie alle neuen Common Vulnerabilities and Exposures (CVEs) verfolgen, die Auswirkungen von CVEs bewerten, die Behebung nachvollziehen und die Sicherheitslücken beheben. Als Administrator können Sie die NetScaler-Instanzen durch den regelmäßigen Scan oder durch manuelles Scannen auf neue CVEs überwachen und die erforderlichen Maßnahmen für die Behebung ergreifen.

Weitere Informationen finden Sie unter ADM On-Prem Cloud Connector.

[NSADM-92204]

Sicherheitsempfehlung für NetScaler ADM Sie können ADM On-Prem Cloud Connector konfigurieren und Security Advisory aktivieren, um die Vollversion der Security Advisory-Funktion in ADM On-Prem zu verwenden. Zuvor war die Sicherheitsempfehlung nur in der Vorschauversion verfügbar.

Weitere Informationen finden Sie unter Sicherheitsempfehlung.

> **Hinweis:**
>
> Wenn Sie den ADM On-Prem Cloud Connector nicht konfiguriert oder deaktiviert haben, können Sie die Sicherheitsempfehlung nur als Vorschauversion verwenden.

Weitere Informationen zu ADM On-Prem Cloud Connector finden Sie unter ADM On-PremCloud Connector.

[NSADM-91726]

Verwaltung und Überwachung

Für StyleBook-Operationen ist eine Authentifizierung erforderlich, um auf NetScaler-Instanzen zuzugreifen Als Administrator können Sie Benutzer jetzt auffordern, Anmeldeinformationen für alle StyleBook- und Config Pack-Operationen anzugeben, die auf NetScaler-Instanzen ausgeführt werden. Gehen Sie wie folgt vor, um diese Funktion zu aktivieren:

- Navigieren Sie zu **Einstellungen > Administration > System, Zeitzone, zulässige URLs und Agenteneinstellungen > Grundeinstellungen**
- Wählen Sie **Prompt Credentials für die Instance-Anmeldung**
- Wählen Sie **Prompt Credentials for Stylebook Operations**

Wenn Sie alternativ **Prompt Credentials for Instance Login** auswählen und **Prompt Credentials for Stylebook Operations**deaktivieren, werden StyleBook- und Config-Pack-Operationen, die auf NetScaler-Instanzen ausgeführt werden, nicht zur Eingabe eines Benutzernamens und Kennworts aufgefordert.

Weitere Informationen finden Sie unter So aktivieren Sie den Shell-Zugriff für nicht standardmäßige Benutzer.

[NSHELP-35432]

Schreibgeschützter Zugriff auf NetScaler ADM-Backupdateien und Benutzersitzungen Benutzer mit schreibgeschütztem Zugriff können jetzt die folgenden Seiten aufrufen:
Einstellungen > Benutzer und Rollen > Sessions*
**Einstellungen **Backup-Dateien

[NSHELP-35431]

Schwellenwert für die Datenaufnahme konfigurieren Sie können jetzt einen Schwellenwert für die Datenaufnahme **unter Einstellungen > Datenspeicherverwaltung > Datenaufbewahrungsrichtlinie > System > Datenaufnahmeeinstellung**konfigurieren. Mit dieser Einstellung können Sie den Prozess auf Systemebene so konfigurieren, dass er beendet wird, wenn der Datenspeicher den Schwellenwert erreicht. Die akzeptierten Schwellenwerte liegen zwischen 50 und 80%

Weitere Informationen finden Sie unter Richtlinie zur Datenaufbewahrung.

[NSHELP-35237]

ADM-Version und IP-Adresse sind im Filer für den technischen Support verfügbar Die ADM-Version und die IP-Adresse sind jetzt in der Datei für den technischen Support unter **Einstellungen > Diagnose > Datei für technischen Support generieren**verfügbar.

[NSHELP-33551]

StyleBooks

Die folgenden Funktionen sind jetzt in StyleBooks verfügbar:

- Datenquellen: Verwenden Sie NetScaler ADC-Instanzen als Datenquellen oder erstellen Sie benutzerdefinierte Datenquellen.
- GitHub Enterprise: Importiere und synchronisiere StyleBooks und Config Packs von deinem GitHub Enterprise Server.
- Integrierte Funktionen: Die folgenden integrierten Funktionen wurden hinzugefügt:
  - `match()`
  - `contains()`
  - `select()`
  - `hash_sha256()`
  - `relate()`
  - `splat()`
- StyleBook-Definitionen: Aktualisieren Sie benutzerdefinierte StyleBook-Definitionen direkt über die NetScaler ADM-GUI.
- Konfigurationspakete aus dem GitHub-Repository: Importiere und synchronisiere Konfigurationspakete aus einem GitHub-Repository. Bisher waren nur StyleBooks erlaubt.
- `botinsight` Attribut: Konfigurieren Sie den `botinsight` Typ im `insights` Abschnitt von StyleBooks.

[NSADM-97841]

Unterstützung für zusätzliche Attribute in StyleBooks Analytics Der StyleBooks-Analysebereich wurde jetzt erweitert um:
- Parameter zur Konfiguration des Transportmodus akzeptieren (`transport-mode`)
- HDX Insight für verschiedene Verkehrsarten konfigurieren (`enable-hdxinsight-for`)
- HTTP X-Forwarded-For-Option aktivieren (`http-x-forwarded-for`)
- Clientseitige Messungen aktivieren ()`client-side-measurements`

Weitere Informationen finden Sie unter StyleBooks-Grammatik.

[NSADM-97839]

Behobene Probleme

Die Probleme, die in Build 14.1—8.50 behoben wurden.

Analytics

- Das regelmäßige Bereinigen der App-Dashboard-Daten funktionierte nicht wie erwartet. Infolgedessen verbrauchte NetScaler ADM mehr Speicherplatz.

  [NSHELP-36184]

- Wenn NetScaler ADM die virtuellen Serverlizenzen verliert, wird der Analysestatus für die virtuellen Server, die diese Lizenzen verwenden, voraussichtlich deaktiviert. Dieses Szenario funktionierte für die virtuellen VPN-Server nicht wie erwartet.

  [NSHELP-36183]

Infrastruktur

- In **Gateway > HDX Insight** und **Gateway > Gateway Insight**werden auf der X-Achse der Diagramme Datumsangaben statt Uhrzeit angezeigt.

  [NSHELP-36043]

- Das NetScaler ADM HA-Paar kann das Split-Brain-Szenario aufgrund eines Synchronisierungsfehlers bei der Heartbeat-Kommunikation nicht überwinden.

  [NSHELP-35934]

- Die Funktion des Programms zur Verbesserung der Benutzerfreundlichkeit (CUXIP) ist für Benutzer aktiviert und ihre Nutzungsdaten werden auch dann erfasst, wenn der Administrator CUXIP **unter Einstellungen > Administration > CUXIP-Einstellungen**deaktiviert hat.

  [NSADM-101771]

- Wenn Sie sich als Root-Administrator zum ersten Mal mit Standardanmeldeinformationen an der NetScaler ADM GUI oder API anmelden, wurden Sie nicht aufgefordert, das Standardkennwort zu ändern. Mit diesem Fix sind Sie gezwungen, das Standardkennwort zu ändern.

  [NSADM-95328]

- Wenn mehrere SNMP-Benutzer gleichzeitig mit einem Skript erstellt werden, schlagen die SNMP-Anforderungen an ADM fehl.

  [NSADM-83924]

Verwaltung und Überwachung

- Ordner, die im NetScaler ADM-Backup-Verzeichnis erstellt wurden, werden während des Backup-Löschvorgangs, der alle 2 Stunden geplant ist, nicht entfernt.

  [NSHELP-35911]

- Die Authentifizierung mit externem LDAP schlägt in NetScaler ADM zeitweise fehl und wird nur durch einen Neustart von NetScaler ADM behoben.

  [NSHELP-35733]

- Das ADM mas_perf-Subsystem stürzt ab und eine Ereignismeldung wird **unter Einstellungen**> ADM-Systemereignisse angezeigt.

  [NSHELP-35711]

- Benutzer können ihre autorisierten Anwendungen nicht unter **Anwendungen > App-Dashboard**anzeigen. Dieses Problem tritt auf, wenn Benutzer vielen Gruppen angehören und jede Gruppe viele Anwendungen hat.

  [NSHELP-35165]

- Ein auf NetScaler ADM durchgeführter Qualys-Scan meldete eine schwache Sicherheitslücke beim aktiven SSL/TLS-Schlüsselaustausch auf PostgreSQL-Ports.

  [NSHELP-34487]

- Wenn NetScaler die Verbindung zum Lizenzserver trennt und innerhalb von 10 Minuten wieder eine Verbindung herstellt, wird die vom NetScaler ausgecheckte Lizenz möglicherweise zweimal auf dem Lizenzserver angezeigt. Starten Sie den Lizenzserver neu, um diesen veralteten Eintrag freizugeben.

  [NSHELP-35420]

Provisioning

- Wenn Sie NetScaler VPX in der Cloud (**Infrastruktur > Instanzen > NetScaler > VPX > Provision) mit ESXi oder VMware vCenter bereitstellen**, wird die Lizenzkonfiguration ignoriert.

  [NSHELP-35984]

- Die NetScaler VPX-Bereitstellung auf VMware vCenter (**Infrastruktur > Instanz > NetScaler > VPX > Bereitstellung**) schlägt fehl, weil derselbe Name verwendet wurde, der in der zuvor gelöschten VPX-Instanz verwendet wurde.

  [NSHELP-35983]

StyleBooks

- Wenn Sie ein Konfigurationspaket aus einer StyleBook-Definition erstellen, die über einen virtuellen Authentifizierungsserver und integrierte Cache-Richtlinienbindungen verfügt, und dann das Konfigurationspaket löschen, ist das Löschen erfolgreich. Wenn Sie jedoch versuchen, das Config Pack erneut mit denselben Parametern zu erstellen, wird die folgende Fehlermeldung angezeigt:
  `Resource already exists`.

  [NSHELP-35646]

- Wenn Sie versuchen, eine ADC-Konfiguration von einer Quell-ADC-Instanz auf eine Zielinstanz unter **Anwendungen > Konfiguration > Config Packs > Migrieren Sie ADC > Erste Schritte > Konfiguration angeben** zu migrieren und auf **Weiter** klicken, wird zeitweise die folgende Fehlermeldung angezeigt:

  `No Job found`.

  [NSADM-97948]

Bekannte Probleme

Die Probleme, die in Version 14.1—8.50 bestehen.

Infrastruktur

- Wenn Sie **unter Infrastructure > Instance Advisory > Security Advisory**eine anfällige NetScaler-Instanz mit einem CVE auswählen und auf Proceed **to Upgrade-Workflow**klicken, wird die folgende Fehlermeldung angezeigt:

  „Für die ausgewählte NetScaler-Instanz ist dieser Behebungsworkflow nicht erforderlich“

Problemumgehung: Aktualisieren Sie die NetScaler-Instanz manuell über **Infrastruktur**Upgrade-Jobs.

[NSADM-103649]

- Nach der Konfiguration eines neuen NetScaler ADM wird möglicherweise die folgende Fehlermeldung angezeigt: `Error in operation - Metrics not found.`

  Dieses Problem tritt auf, weil der automatische Datenlöschauftrag noch nicht ausgeführt wurde, was dazu führt, dass keine Daten vorhanden sind. Die Ausführung des Jobs ist für 3 Stunden geplant. Nach der Ausführung werden die erforderlichen Daten generiert, und die Fehlermeldung wird nicht mehr angezeigt.

  [NSADM-103157]

- Wenn ein Bericht von einer scrollbaren Seite in NetScaler ADM exportiert wird, schneidet der exportierte Bericht möglicherweise Inhalte ab, die über die Höhe des sichtbaren Fensters hinausreichen.

  [NSADM-102765]

- Wenn Sie versuchen, ein Zertifikat auf einer NetScaler BLX-Instanz zu installieren, schlägt die Installation fehl und auf der Seite **Infrastruktur > SSL-Dashboard > SSL-Auditprotokolle** wird die folgende Fehlermeldung angezeigt:

  `SCP: Authentication by password fails on _<ip-address>_.`

  [NSADM-102202]

- Der NetScaler Agent wird nicht bei NetScaler ADM registriert, wenn eines seiner Passwörter ein %23-Symbol hat.

  [NSADM-100613]

Verwaltung und Überwachung

- In einem ADM-HA-Paar wurde festgestellt, dass sich der Datenbankstatus im Status Nicht **verfügbar** befindet und nicht synchronisiert wird, selbst nachdem mehrere Versuche mit der Option **Datenbank synchronisieren** in der GUI versucht wurden.

  [NSHELP-29626]

Versionshinweise für NetScaler ADM 14.1-4.42

February 5, 2024

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

Hinweise

- Dieses Dokument mit den Versionshinweisen enthält keine sicherheitsrelevanten Fixes. Eine Liste mit sicherheitsrelevanten Fixes und Hinweisen finden Sie im Citrix Security Bulletin.

Was ist neu

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

Analytics

Web Insight —Unterstützung für die Anzeige der prozentualen Verteilung auf der Grundlage von Anfragen In **Web Insight**können Sie jetzt die **prozentuale Verteilung nach Anfragen** unter den folgenden Metriken anzeigen:

- Kunden
- Server
- Geo Standorte
- URLs

Als Administrator können Sie anhand dieser Erweiterung die prozentuale Verteilung der eingegangenen Anfragen anhand der Gesamtzahl der Anfragen für den ausgewählten Zeitraum nachvollziehen. Sie können beispielsweise vergleichen, wie die Server Anfragen für die gewählte Dauer empfangen.

Weitere Informationen finden Sie unter Web Insight.

[NSADM-96158]

Unterstützung für den Export aus jedem Widget in Web Insight In **Web Insight** ist die Exportoption jetzt in allen Widgets eingeführt und ermöglicht es Ihnen, Daten im tabellarischen Format zu exportieren. Mit dieser Erweiterung können Sie:

- Exportieren Sie die erforderlichen Daten einzeln aus einem beliebigen Widget.
- Führen Sie eine detaillierte Analyse aller Metriken durch und exportieren Sie die erforderlichen Daten aus einem beliebigen Widget.

Bisher lieferten die Exportdaten nur den konsolidierten Bericht.

> **Hinweis:**
>
> Sie können auch weiterhin die bestehende Exportoption verwenden, um den konsolidierten Bericht zu generieren.

[NSADM-94140]

Ein einheitliches Dashboard zum Anzeigen der wichtigsten Metrikdetails für die Instanz Als Administrator können Sie jetzt ein Dashboard visualisieren, das einen Überblick über wichtige Metrikdetails bietet, basierend auf:

- Anwendungen
- ADC-Infrastruktur
- Anwendungssicherheit
- Gateway

Mit diesem Einbereichs-Dashboard können Sie Details anzeigen, um die Instanz-Nutzung und -Leistung besser überwachen zu können.

Weitere Informationen finden Sie unter Vereinheitlichtes Dashboard

[NSADM-94137]

Exportieren Sie ADM-Ereignisse und Metrikdaten nach Splunk und New Relic Wenn Sie unter **Einstellungen > Ökosystemintegration** ein neues Abonnement für die Integration von NetScaler ADM mit Splunk und New Relic erstellen, können Sie jetzt die Option **ADM-Ereignisse** und **ADM-Metriken** auswählen. Nachdem Sie das Abonnement mit einer oder beiden Optionen konfiguriert haben, können Sie die entsprechenden Daten im Splunk- und New Relic-Dashboard anzeigen.

Weitere Informationen finden Sie unter Integration mit Splunk und Integration mit New Relic.

[NSADM-93765]

SSL-Bewertung einer Anwendung anzeigen Unter **Anwendungen > Dashboard**können Sie jetzt die SSL-Bewertung einer Anwendung einsehen. Sie können SSL-Probleme überprüfen und die Anwendung aktualisieren, um eine A+-Bewertung zu erhalten. Wenn Sie jedoch aufgrund dieses Upgrades einen gewissen Rückgang des Datenverkehrs feststellen, können Sie das in Ihrer Anwendung konfigurierte sichere Front-End-Profil zurücksetzen. Diese Aktion setzt die A+-Bewertung auf eine frühere Bewertung zurück.

Weitere Informationen finden Sie unter A+ SSL-Bewertungsanalyse.

[NSADM-92025]

Web Insight - Unterstützung für die Anzeige von Nullwerten in Diagrammen Wenn Sie in **Web Insight** eine Metrik unter **Applications**, Clients, URLs oder Instances aufschlüsseln, zeigt die Analytics-Ansicht jetzt die Sichtbarkeit von Nullwerten (z. B. 0 ms und 0 Anfragen) im Diagramm für die gewählte Dauer an.

Wenn früher für die gewählte Dauer kein Traffic oder keine Transaktionen eingingen, zeigte Web Insight die Diagramme an, indem diese Nullwerte übersprungen wurden. Als Administrator können Sie sich jetzt das komplette Diagramm mit diesen Nullwerten ansehen.

[NSADM-88686]

Infrastruktur

Unterstützung für RPC-Knotenkennwörter für die NetScaler-Bereitstellung mit hoher Verfügbarkeit Sie können jetzt das RPC-Knotenkennwort festlegen, wenn Sie die primären und sekundären Knoten in einer HA-Bereitstellung erstellen. Navigieren Sie zu **Infrastruktur > Upgrade-Jobs > Job erstellen > HA-Paar von NetScaler-Instanzen konfigurieren**, um die RPC-Knotenkennwörter für die Hochverfügbarkeitsknoten einzugeben.

Weitere Informationen finden Sie unter Planung der Konfiguration eines HA-Paares von NetScaler-Instanzen.

[NSADM-93912]

NetScaler ADM Agent speichert NetScaler-Images im Cache Der Zeitaufwand für das NetScaler-Upgrade ist jetzt erheblich reduziert, da die NetScaler-Images nach dem Herunterladen im NetScaler ADM Agent zwischengespeichert werden. Daher müssen die Images für nachfolgende Upgrade-Jobs nicht heruntergeladen werden.

> **Hinweis:**
>
> Dies gilt nur für ADCs, die mit dem NetScaler ADM Agent hinzugefügt werden.

Weitere Informationen finden Sie unter Erstellen eines ADC-Upgrade-Jobs.

[NSADM-76343]

Sehen Sie sich die komplette Zertifikatskette an Sie können jetzt die gesamte Linkkette für ein Zertifikat einschließlich der Zwischenzertifikate bis hin zum Root-CA-Zertifikat anzeigen.

Um die Zertifikatskette einzusehen, navigieren Sie zu **Infrastruktur > SSL-Dashboard**, wählen Sie ein SSL-Zertifikat aus und klicken Sie auf **Details**.

Weitere Informationen finden Sie unter SSL-Zertifikatskette anzeigen.

[NSADM-52467]

StyleBooks

Unterstützung für zusätzliche Argumenttypen in der Funktion replace () Die eingebaute Funktion „replace ()“kann auch eine Liste der folgenden eingebauten Typen akzeptieren:

- `string`
- `ipaddress`
- `tcp-port`
- `number`
- **`boolean`**

Weitere Informationen finden Sie unter Integrierte Funktionen.

[NSADM-96802]

Unterstützung für die Funktion multiple () Die integrierten StyleBooks-Funktionen unterstützen jetzt die Funktion multiple (). Die Funktion multiple (argument1, argument2) verwendet zwei Argumente und gibt eine Liste mit vielen Kopien von Argument 1 zurück. Die Anzahl der Kopien entspricht der Anzahl, die an Argument 2 übergeben wurde.

Weitere Informationen finden Sie unter Integrierte Funktionen.

[NSADM-95973]

Unterstützung für optionale Abschnitte in StyleBook-Konfigurationspaketen Die Abschnitte `targets` und `stylebook` sind jetzt in der Nutzlast des Konfigurationspakets optional. Wenn Sie diese Abschnitte nicht angeben, um ein Config Pack zu aktualisieren, werden die zuletzt verwendeten Abschnitte `targets` und `stylebook` aus der NetScaler ADM-Datenbank abgerufen und das Config Pack wird aktualisiert.

[NSADM-92377]

Geben Sie den Zugriff von Benutzergruppen auf Konfigurationspakete an Als Administrator können Sie nun Benutzergruppen daran hindern, auf Konfigurationspakete zuzugreifen, die von anderen Benutzergruppen erstellt wurden. Um diese Option auszuwählen, navigieren Sie zu **Einstellungen > Benutzer und Rollen > Gruppen > Autorisierungseinstellungen > Config Packs > Alle von der Benutzergruppe erstellten Konfigurationen** .

Weitere Informationen finden Sie im Abschnitt **Konfigurationspakete** unter Erstellen einer Benutzergruppe.

[NSADM-92374]

Behobene Probleme

Die Probleme, die in Build 14.1-4.42 behoben werden.

Analytics

- Das NetScaler ADM HA-Paar kann zeitweise zu einem Split-Brain-Szenario führen.

  [NSHELP-35430]

- HTTP-Webtransaktionen, die keinen Abfrageparameterwert in der URL haben, werden im NetScaler ADM Web Insight-Dashboard (**Anwendungen > Web**Insight) nicht angezeigt.

  Wenn die URL `https://www.google.com/search?q=abstract%20api` beispielsweise nicht den Abfrageparameterwert hat und als `https://www.google.com/search?q=` verfügbar ist, werden HTTP-Transaktionen gelöscht und sind im Dashboard nicht verfügbar.

  [NSADM-99448]

- Wenn Sie in **Web Insight**eine Metrik aufschlüsseln, um Details anzuzeigen, und dann eine Metrik weiter aufschlüsseln, bleibt das Diagramm immer noch in der vorherigen Ansicht, aber alle anderen Details werden wie erwartet angezeigt.

  Dies führt zu der Annahme, dass der weitere Drilldown nicht wie erwartet funktioniert.

  [NSADM-98995]

Infrastruktur

- MPX-Instanzen fehlen auf der Seite **Infrastruktur > NetScaler Inventory > NetScaler** (MPX/VPX/CPX/BLX).

  [NSHELP-35593]

- Wenn Sie sich mit LDAP-Benutzerauthentifizierung an der NetScaler ADM GUI anmelden und „domain\ username“verwenden, werden die Benutzereinstellungen nicht gespeichert.

  [NSADM-100995]

- Wenn Sie Befehle auf einer Partition für einen Konfigurationsauftrag ausführen, wird die folgende Fehlermeldung angezeigt: „Befehl für Admin-Partitionsgerät blockiert“.

  Dieses Problem tritt bei NetScaler 13.1-42.47 und späteren Builds auf.

  [NSADM-100416]

- Nachdem Sie unter **Einstellungen > Bereitstellung > Failover erzwingen** ein Failover für ein ADM-HA-Paar durchgeführt haben, werden die Details zum sekundären Knoten auf der Seite **Einstellungen > Bereitstellung** nicht angezeigt.

  [NSADM-98674]

- Wenn du versuchst, ein Slack-Profil **unter Einstellungen > Benachrichtigungen > Slack > Hinzufügen hinzuzufügen**, wird das Profil nicht hinzugefügt und du erhältst die folgende Fehlermeldung:

  `Please check internet connectivity`.

  [NSADM-98633]

- Wenn Sie sich als Root-Administrator zum ersten Mal mit Standardanmeldeinformationen an der NetScaler ADM GUI oder API anmelden, wurden Sie nicht aufgefordert, das Standardkennwort zu ändern. Mit diesem Fix sind Sie gezwungen, das Standardkennwort zu ändern.

  [NSADM-95328]

Verwaltung und Überwachung

- Wenn Sie eine NetScaler-Instanz sichern oder wiederherstellen, wird das Verzeichnis /var/metrics_conf nicht gesichert.

  [NSHELP-35724]

- Wenn Sie die SSL-Ablaufberichte für wöchentlich, 30 Tage oder 90 Tage unter **Infrastruktur > SSL-Dashboard > SSL-Zertifikate > Berichte exportieren** und **Tabellarisch**auswählen, zeigt der resultierende Bericht eine leere Domain-Spalte an.

  [NSHELP-35592]

- Unter **Infrastruktur > SSL-Dashboard > SSL-Zertifikate**zeigt das NetScaler-Hochverfügbarkeitspaar nicht die hochgestellten Buchstaben „P“und „S“für das primäre und das sekundäre Gerät an.

  [NSHELP-35523]

- Der NetScaler ADM-Status wird zeitweise als **Nicht verfügbar** angezeigt, auch wenn alle Prozesse aktiv sind.

  [NSHELP-35408]

- Wenn Sie für mehrere Cluster-IP-Adressen (CLIPs) in einem Cluster einen CLIP in Klammern unter **Infrastruktur > Instanzen > NetScaler > Hinzufügen hinzufügen**, schlägt die Konfiguration fehl und der CLIP wird nicht zu NetScaler ADM hinzugefügt.

  [NSHELP-35323]

- Wenn Sie unter **Infrastruktur > Konfiguration > Konfigurationsjobs > Job erstellen > Konfiguration auswählen** eine Kennwortvariable (`$password$`) eingeben und den **Typ** als **Textfeld** anstelle von **Kennwortfeld** beibehalten und auf **Weiter** klicken, wird die Seite nicht geladen.

  [NSHELP-35266]

- Der NetScaler ADM-Inventarisierungsprozess stürzt zeitweise ab, wenn Anfragen an andere ADM-Prozesse gesendet werden.

  [NSHELP-35048]

- NetScaler ADM reagiert aufgrund mehrerer Subsystemabstürze nicht.

  [NSHELP-34633]

- Der primäre Standort (NetScaler ADM HA-Paar) versucht immer wieder, die Daten mit dem NetScaler ADM Disaster Recovery-Knoten zu synchronisieren, und schlägt fehl.
  Dieses Problem tritt auf, wenn der primäre Standort über große Datenmengen (>1 GB) verfügt.

  [NSHELP-32750]

Provisioning

- Die Bereitstellung von NetScaler VPX auf SDX (**Infrastruktur > Instanzen > NetScaler ADC > VPX) schlägt in NetScaler ADM fehl**.

  [NSHELP-35347]

StyleBooks

- Die Bereitstellung von Konfigurationspaketen schlägt möglicherweise fehl, wenn die StyleBook-Definition den Abschnitt `operations` enthält.

  [NSHELP-35588]

- Wenn Sie einige Versionen von Infoblox als IPAM-Anbieter **unter Einstellungen > IPAM > Hinzufügen hinzufügen**, wird die folgende Fehlermeldung angezeigt:

  ```
  Invalid provider information: Invalid attributes for registering provider.
  ```

  [NSHELP-35302]

Bekannte Probleme

Die Probleme, die in Version 14.1-4.42 bestehen.

Infrastruktur

- Der NetScaler Agent wird nicht bei NetScaler ADM registriert, wenn eines seiner Kennwörter ein Symbol # enthält.

  [NSADM-100613]

- Wenn unter **Einstellungen > Administration > SSL-Zertifikate installieren**der Name der Zertifikatsdatei, die Sie hochladen, Klammern enthält, schlägt die Installation des SSL-Zertifikats in NetScaler fehl. Die folgende Fehlermeldung wird angezeigt:

  „Ungültige POST-Anfrage, Nutzlast sollte mit object= beginnen“.

  [NSADM-99531]

Verwaltung und Überwachung

- In einem ADM-HA-Paar wurde festgestellt, dass sich der Datenbankstatus im Status Nicht **verfügbar** befindet und nicht synchronisiert wird, selbst nachdem mehrere Versuche mit der Option **Datenbank synchronisieren** in der GUI versucht wurden.

  [NSHELP-29626]

On-premises NetScaler ADM auf Citrix Cloud migrieren

February 5, 2024

Sie können on-premises **NetScaler ADM 13.0 64.35 oder eine neuere Version** auf Citrix Cloud migrieren. Wenn Ihr ADM 12.1 oder eine frühere Version hat, müssen Sie zuerst auf **13.0 64.35 oder eine neuere Version** upgraden und dann auf Citrix Cloud migrieren. Weitere Informationen finden Sie im Abschnitt Upgrade.

> **Hinweis:**
>
> Der NetScaler ADM Service wurde jetzt in NetScaler Console Service umbenannt. Unsere Produktuberfläche und Dokumentation werden derzeit aktualisiert, um diesen Änderungen Rechnung zu tragen. Während dieser Zeit stoßen Sie möglicherweise auf die älteren und neueren Namen, auf die synonym verwiesen wird. Wir danken Ihnen für Ihr Verständnis während dieses Übergangs.

Mit dem NetScaler Console-Dienst über Citrix Cloud erhalten Sie:

- Schnellere Releases, ungefähr alle zwei Wochen mit den neuesten Feature-Updates.

- Auf maschinellem Lernen basierende Analysen für Anwendungssicherheit und Bot, Performance und Nutzung.
- Verschiedene andere Funktionen, die derzeit nur im NetScaler Console-Dienst unterstützt werden, wie z. B. Peak- und Lean-Period-Analysen, auf maschinellem Lernen basierende Analysen für Anwendungssicherheit und Bot, CPU-Analysen für Anwendungen und viele mehr.

Für eine erfolgreiche Migration müssen Sie:

- Stellen Sie sicher, dass Sie eine Internetverbindung im on-premises ADM haben, um die Barrierefreiheit von Citrix Cloud zu
- Den NetScaler Agent konfigurieren
- Holen Sie sich die Client- und geheime CSV-Datei von Citrix Cloud
- Überprüfen Sie die NetScaler Console-Lizenzierung
- Migrieren mit einem Skript

Wenn Sie nach der Migration vom on-premises ADM zum NetScaler Console-Dienst erneut mit dem on-premises ADM fortfahren möchten, können Sie das Rollback-Skript verwenden. Weitere Informationen finden Sie unter Rollback zu lokalem ADM.

Den NetScaler Agent konfigurieren

Um die Kommunikation zwischen NetScaler-Instanzen und NetScaler ADM zu aktivieren, müssen Sie einen Agent konfigurieren. NetScaler ADM-Agents werden standardmäßig automatisch auf den neuesten Build aktualisiert. Sie können auch einen bestimmten Zeitpunkt für das Agentupgrade auswählen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgrade-Einstellungen.

- Wenn für Ihr vorhandenes lokales ADM (Standalone oder HA-Paar) keine on-premises Agenten konfiguriert sind, müssen Sie mindestens einen Agenten für den NetScaler Console-Dienst konfigurieren.
- Wenn Ihr vorhandenes lokales ADM (eigenständig oder HA-Paar) mit on-premises Agenten für Bereitstellungen an mehreren Standorten konfiguriert wurde, müssen Sie dieselbe Anzahl von Agenten für den NetScaler Console-Dienst konfigurieren.

Weitere Informationen zum Konfigurieren eines Agents finden Sie im Abschnitt Erste Schritte.

Holen Sie sich die Client- und geheime CSV-Datei von Citrix Cloud

Nachdem Sie den Agent konfiguriert haben, rufen Sie die Client- und geheime CSV-Datei von der Citrix Cloud-Seite ab:

1. Melden Sie sich bei citrix.cloud.com an
2. Klicken Sie auf das **Home-Symbol** und wählen Sie **Identity and Access Management**
3. Geben Sie auf der Registerkarte **API-Zugriff** einen sicheren Client-Namen ein und klicken Sie auf **Client erstellen**.
4. ID und Secret wird generiert. Klicken Sie auf **Herunterladen** und speichern Sie die CSV-Datei im on-premises ADM.

   Speichern Sie beispielsweise die CSV-Datei im Verzeichnis /var.

Überprüfen Sie die NetScaler Console-Dienstlizenzen

Sie müssen Lizenzen für den NetScaler Service erwerben.

- Die VIP-Lizenzen im NetScaler Console-Dienst müssen mindestens den on-premises VIP-Lizenzen entsprechen.

  > **Hinweis** Wenn die VIP-Lizenzen geringer sind, werden virtuelle Server nach dem Zufallsprinzip ausgewählt und die Konfiguration auf VIP-Ebene für den NetScaler Console-Dienst schlägt fehl.

- Wenn Sie die on-premises ADM-Bereitstellung als Lizenzserver verwenden, weisen Sie Ihre Lizenzen vor der Migration dem NetScaler Console-Dienst neu zu. Weitere Informationen finden Sie unter Konfigurieren eines ADM-Servers nur als gepoolten Lizenzserver und Neuzuweisen einer Lizenzdatei.
- Wenn Sie die gepoolten Lizenzen in on-premises ADM verwenden, müssen Sie die gepoolten Lizenzen für den NetScaler Console-Dienst abrufen und dann den ADC-Instanzen Lizenzen zuweisen. Weitere Informationen finden Sie unter Konfigurieren der gepoolten Lizenzierung. Mit den folgenden unterstützten ADC-Versionen können Sie die Lizenzzuweisung von ADM ändern:
  - NetScaler SDX: 13.0 74.11 oder neuere Versionen.
  - NetScaler VPX und MPX: 13.0 47.24 oder neuere Versionen, 12.1 58.14 oder neuere Versionen und 11.1 65.10 oder höhere Versionen.

Migrieren mit einem Skript

- Mit dem ADM 82.x-Build können Sie die Funktion auswählen und dann migrieren.
- Für ADM 76.x oder spätere Builds sind die Migrationsskripte (`servicemigrationtool.py` und `config_collect_onprem.py`) als Teil des Builds verfügbar unter `cd /mps/scripts`.

- Bei ADM vor 76.x-Builds müssen Sie die Migrationsskripte herunterladen und die Skripts im on-premises ADM kopieren.

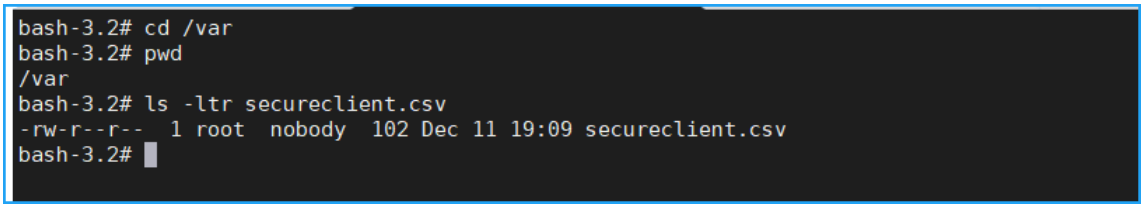
  > Hinweis
  >
  > Stellen Sie sicher, dass der on-premises ADM während der Migration über Internetverbindung verfügt.

1. Melden Sie sich mit einem SSH-Client beim on-premises ADM an.

   > Hinweis
   >
   > Melden Sie sich bei einem ADM HA-Paar bei dem primären Knoten an.

2. Geben Sie **shell** ein und drücken **Sie**die Eingabetaste , um in den Bash-Modus zu wechseln.
3. Kopieren Sie die Client-ID und die geheime CSV-Datei. Kopieren Sie die Datei beispielsweise in das Verzeichnis /var.

   Nachdem Sie die CSV-Datei kopiert haben, können Sie überprüfen, ob die CSV-Datei vorhanden ist.

   > Hinweis
   >
   > Kopieren Sie für ein ADM HA-Paar die CSV-Datei in den primären Knoten.

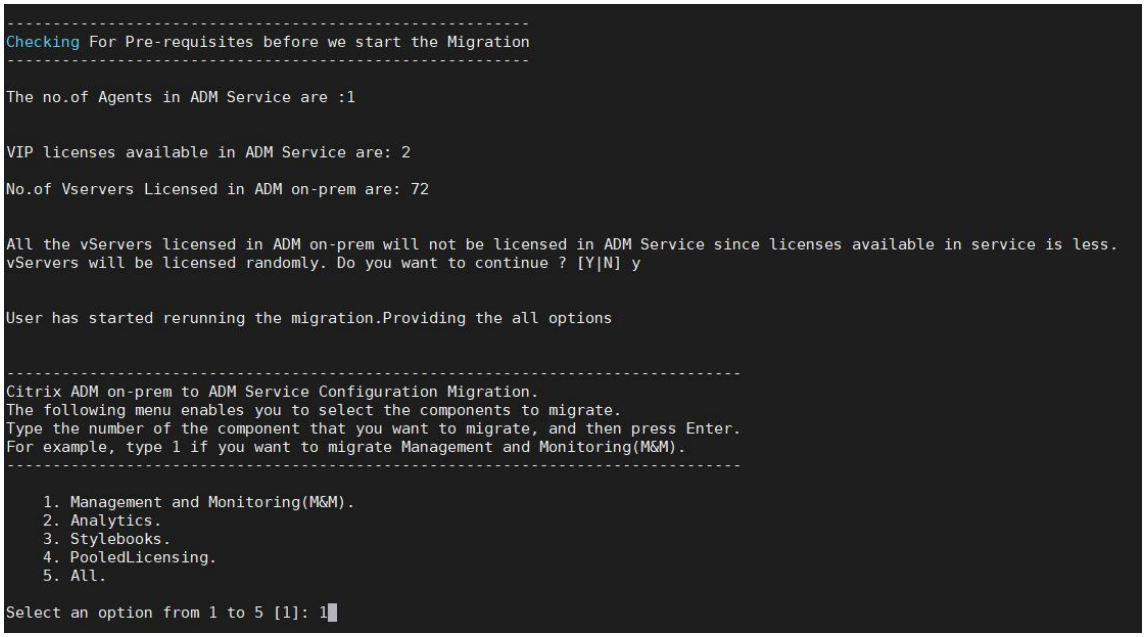
4. Führen Sie für die ADM **13.0 82.xx-Version**die folgenden Befehle aus, um die Migration abzuschließen:

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises NetScaler ADM VM>`

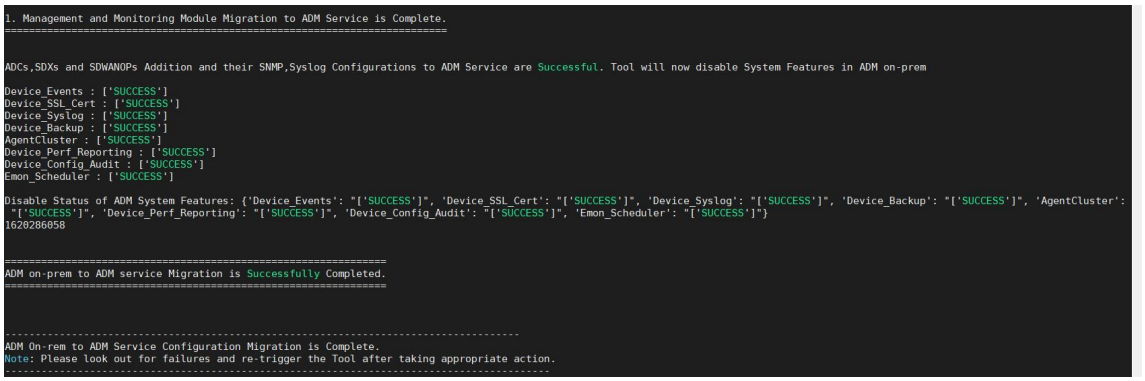
   Beispiel: `python servicemigrationtool.py /var/secureclient.csv`

   Nachdem Sie das Migrationsskript ausgeführt haben, zeigt das Tool die folgenden Optionen an:



Basierend auf der von Ihnen angegebenen Auswahl wird nur diese Funktion zum NetScaler Console-Dienst migriert.

In diesem Beispiel ist Option 1 ausgewählt. Das Tool schließt die Management and Monitoring (M&M)-Migration ab und zeigt die folgende Meldung an:



Management and Monitoring (M&M) umfasst:

- ADC-Instanzen, Tags, Instanzgruppen, Profile, benutzerdefinierte Apps, Konfigurationsaufträge, SNMP, Syslog-Konfigurationen.
- Websites, IP-Blöcke, Netzwerkberichte, Analyse-Schwellenwerte, Benachrichtigungseinstellungen, Einstellungen für das Beschneiden von Daten.
- Konfigurieren Sie Überwachungsvorlagen, Abfrageintervalle, Ereignisregeln und Einstellungen.
- RBAC-Gruppen, Rollen und Richtlinien

Die **Analytics-Funktion** umfasst:

- Appflow-Konfiguration pro vserver aus ADC-Instanzen.
- Appflow-Konfiguration pro SDWAN-Gerät.

> Hinweis:
>
> - Die Management and Monitoring (M&M) -Funktion wird automatisch migriert, auch wenn Sie eine andere Funktion (2, 3 oder 4) auswählen.
> - Sie können jeweils nur ein Feature angeben.
> - Wenn Sie die Migration eines Features abgeschlossen haben und später ein anderes Feature migrieren möchten, wird das bereits migrierte Feature nicht in der Liste angezeigt. Wenn Sie beispielsweise zuerst die Migration der **Analytics-Funktion** abschließen und das Migrationsskript das nächste Mal ausführen, werden nur die Optionen **StyleBooks**, **Pooled Licensing**und **All** angezeigt.
> - Wenn Sie Poollizenzen migrieren, werden alle Typen, einschließlich vServer, migriert.

5. Führen Sie für ADM **13.0 76.xx**die folgenden Befehle aus, um die Migration abzuschließen:

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises NetScaler ADM VM>`

   Beispiel: `python servicemigrationtool.py /var/secureclient.csv`

6. Für ADM früher als 13.0 76.xx-Version:

   a) Laden Sie das Migrationsskript von folgendem Ort herunter: `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigration.tgz`

   The downloaded file comprises two bundle scripts, `servicemigrationtool_27.py` and `config_collect_onprem_27.py`.

   b) Speichern Sie die beiden Skripte im on-premises ADM. Speichern Sie zum Beispiel im /var-Verzeichnis

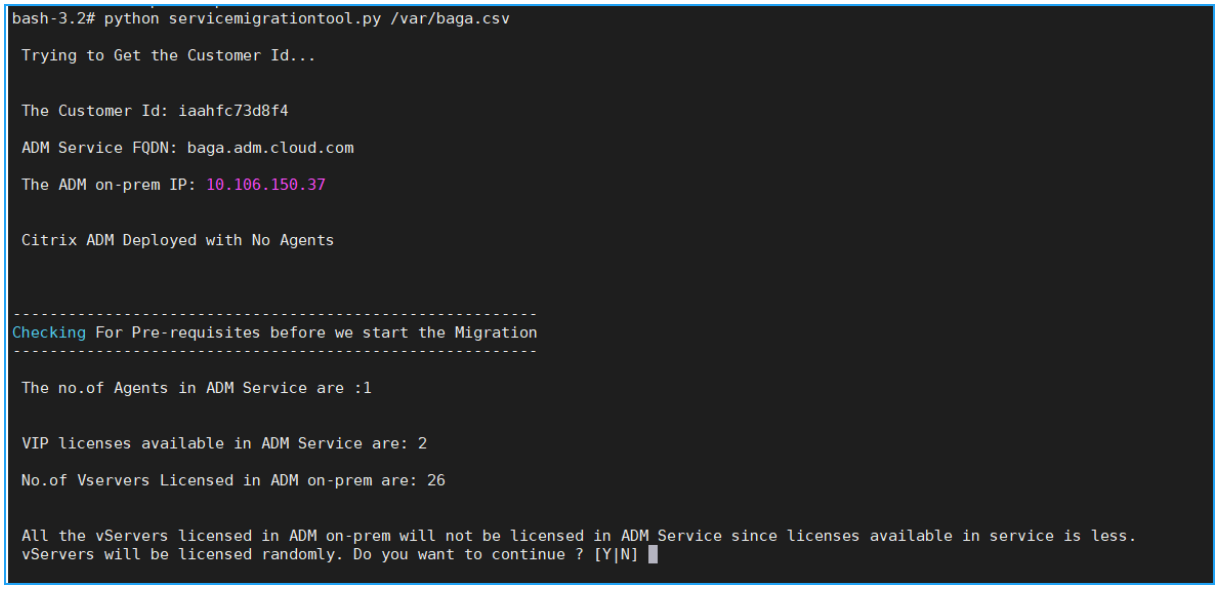
   c) Führen Sie die folgenden Befehle zur Migration aus:

      i. `cd /var`

      ii. `servicemigrationtool_27.py <path of ClientID/Secret File in on-premises ADM VM>`

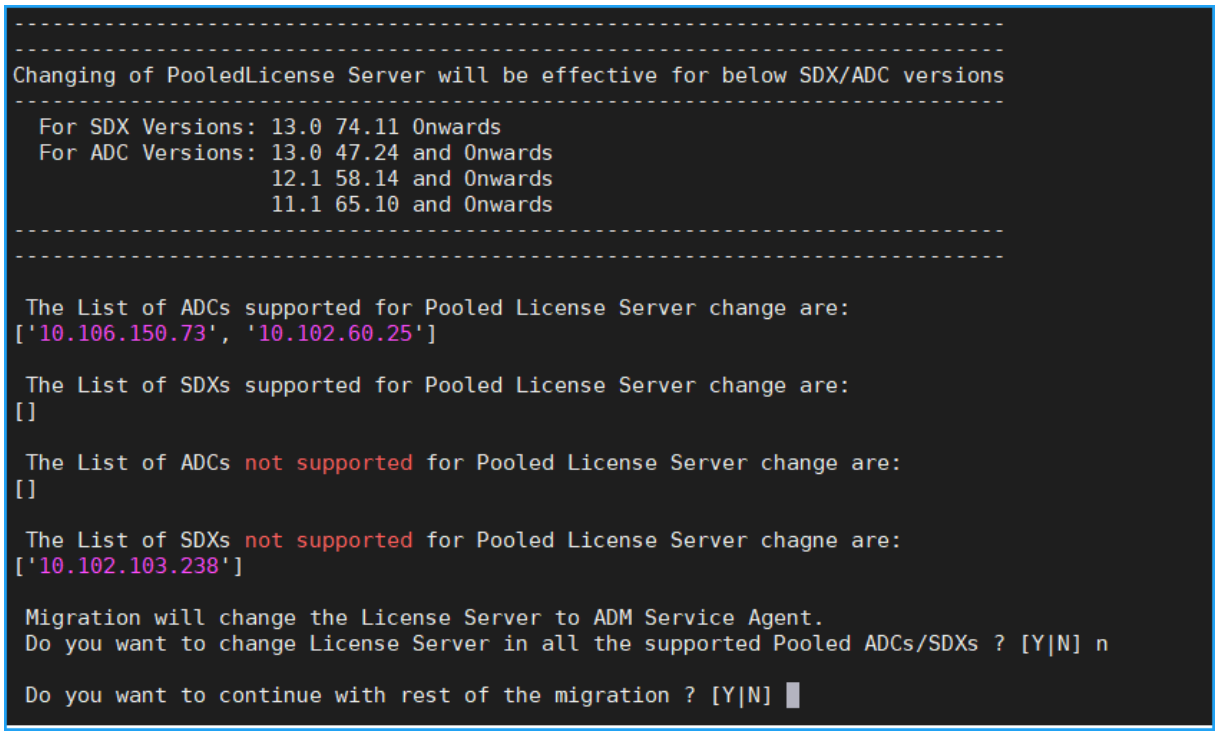
      Beispiel: `python servicemigrationtool_27.py /var/secureclient.csv`

Nachdem Sie das Skript ausgeführt haben, überprüft es die Voraussetzungen und fährt dann mit der Migration fort. Das Skript prüft zuerst die Verfügbarkeit der Lizenz. Die folgende Meldung wird nur angezeigt, wenn Sie eine geringere NetScaler Console-Dienstlizenz als die on-premises Lizenz haben.



Wenn Sie **Y**auswählen, wird die Migration fortgesetzt, indem Sie den VIP nach dem Zufallsprinzip lizenzieren. Wenn Sie **N**wählen, stoppt das Skript die Migration.

Wenn Sie die nicht unterstützte ADC-Instanzversion für den gepoolten Lizenzserver haben, wird die folgende Meldung angezeigt:



Wenn Sie **Y**auswählen, wird der Migrationsprozess fortgesetzt, indem Sie den Lizenzserver ändern. Wenn Sie **N**auswählen, wird das Skript aufgefordert, ob Sie mit dem Rest der Migration fortfahren möchten. Das Skript stoppt die Migration, wenn Sie **N**auswählen.

Abhängig von der on-premises Konfiguration liegt die ungefähre Zeit für den Abschluss der Migration zwischen einigen Minuten und einigen Stunden. Nachdem die Migration abgeschlossen ist, wird die folgende Meldung angezeigt:

```
--------------------------------------------------------------------------------
ADM OnPrem to ADM Service Configuration Migration is Complete.
Note: Please Look out for Failures and re-trigger the Tool after taking appropriate action.
--------------------------------------------------------------------------------
```

Die Migration ist erfolgreich, sobald alle ADC-Instanzen und ihre jeweiligen Konfigurationen erfolgreich in den NetScaler Console-Dienst verschoben wurden. Nach erfolgreicher Migration beendet das on-premises NetScaler ADM die Verarbeitung der folgenden Instanzereignisse:

- SSL-Zertifikate
- Syslog-Nachrichten
- Backup
- Agenten-Cluster
- Performance-Berichte
- Konfigurationsaudit
- Emon Planer

Rollback zu On-Premises ADM

Wenn Sie ein Rollback zu lokalem ADM durchführen möchten, stellen Sie sicher, dass die Voraussetzungen erfüllt sind.

Voraussetzungen

Wenn Ihr lokales ADM (vor der Migration zum NetScaler Console-Dienst) wie folgt lautet:

- Wird als gepoolter Lizenzserver verwendet, stellen Sie sicher, dass Sie über die erforderlichen gepoolten Lizenzen im on-premises ADM verfügen.
- Stellen Sie bei Konfiguration mit on-premises ADM-Agents sicher, dass die Agents im Status “UP” verfügbar sind.

Verwenden Sie das Rollbackskript

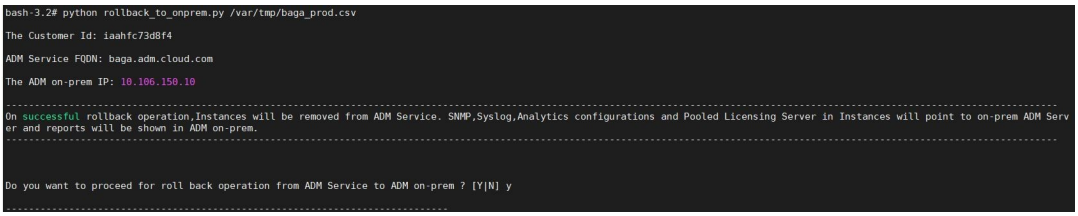
> Hinweis
>
> Nach dem Rollback sind dieselben Konfigurationen (vor der Migration) in Analytics, SNMP und gepoolte Lizenzierung wieder im on-premises ADM verfügbar. Wenn Sie nach der Migration Änderungen an diesen Konfigurationen vorgenommen haben, werden diese Änderungen nicht im on-premises ADM berücksichtigt.

- Für **ADM 82.xx oder neuere** Builds ist das Rollback-Skript als Teil des Builds verfügbar und unter zugänglich `/mps/scripts`.
- Für **ADM vor 79.xx-Builds** können Sie entweder auf 82.x-Build aktualisieren und das Rollback-Skript verwenden, oder Sie können das Rollback-Skript herunterladen und das Skript in lokales ADM kopieren.

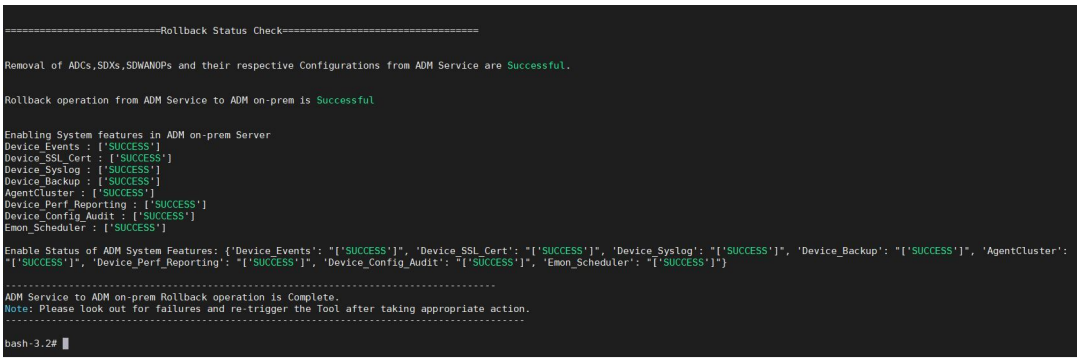
1. Melden Sie sich mit einem SSH-Client beim on-premises ADM an.
2. Geben Sie shell ein und drücken Sie die Eingabetaste, um in den Bash-Modus zu wechseln.
3. Führen Sie für ADM **13.0 82.xx** Build die folgenden Befehle aus, um das Rollback abzuschließen:
   a) cd /mps/scripts
   b) python rollback_to_onprem.py <`path of ClientID/Secret File in ADM on-prem VM`>

      Beispiel: `python rollback_to_onprem.py /var/ secureclient.csv.csv`

      Das Tool leitet den Rollback-Vorgang ein und eine Eingabeaufforderung fragt, ob Sie fortfahren möchten. Geben Sie **Y** ein, um fortzufahren.



Sie können die folgende Meldung sehen, nachdem das Rollback abgeschlossen wurde.



4. Für ADM vor 82.xx Build:

   a) Laden Sie das Rollback-Skript von folgendem Ort herunter:

   ```
   https://download.citrixnetworkapi.net/root/download/v1/public
   /software?product=admonprem&build=migrationtool&model=servicemigration
   .tgz
   ```

   b) Für ADM 79.xx- und 76.xx-Builds speichern Sie das Skript in `/mps/scripts` und führen Sie die folgenden Befehle aus, um ein Rollback durchzuführen:

      i. `cd /mps/scripts`

      ii. `python rollback_to_onprem.py < path of client/secret csv file in ADM on-prem>`

      Beispiel: `python rollback_to_onprem.py /var/ secureclient.csv`

   c) Für ADM-Builds vor 76.xx speichern Sie das Skript im on-premises ADM. Speichern Sie es beispielsweise am Speicherort `/var` und führen Sie die folgenden Befehle aus, um ein Rollback durchzuführen:

      i. `cd /var`

      ii. `python rollback_to_onprem_27.py < path of client/secret csv file in ADM on-prem>`

      Beispiel: `python rollback_to_onprem_27.py /var/secureclient.csv`

   Das Tool leitet den Rollback-Vorgang ein und eine Eingabeaufforderung fragt, ob Sie fortfahren möchten. Geben Sie **Y** ein, um fortzufahren.

Häufig gestellte Fragen

February 5, 2024

ADM Service

Ist der ADM-Servicemitarbeiter optional ähnlich wie ein lokaler NetScaler ADM-Agent?

Nein. Der ADM-Servicemitarbeiter ist für ADM Service obligatorisch und die gesamte Kommunikation zwischen Instanzen und ADM Service erfolgt über den ADM Service-Agent. Der on-premises ADM-Agent ist optional. Sie können den lokalen Agenten jedoch nur konfigurieren, um Bandbreitenverbrauch zu sparen.

Warum ADM Service?

ADM Service über Citrix Cloud bietet die folgenden Vorteile, ohne dass neue periodische Builds erforderlich sind:

- Cloud-basiertes SaaS-Angebot mit einfacherem Onboarding und geringeren Betriebskosten als das on-premises NetScaler ADM.
- Schnellere Releases, ungefähr alle zwei Wochen mit den neuesten Feature-Updates.
- Auf maschinellem Lernen basierende Analysen für Anwendungssicherheit, -leistung und -nutzung.
- Verschiedene andere Funktionen, die derzeit nur im ADM-Service unterstützt werden, wie Peak- und Lean-Periodenanalyse, auf maschinellem Lernen basierende Anwendungssicherheitsanalysen für WAF und Bot, Anwendungs-CPU-Analysen und viele mehr.

Sie können auch am monatlichen Webinar des NetScaler ADM Service teilnehmen, um die neuesten Produktfunktionen und -lösungen zu verstehen. Melden Sie sich über den folgenden Link für das Webinar an:

`https://www.citrix.com/events/2022/whats-new-with-citrix-application-delivery-management.html`

Was passiert nach der Migration, wenn on-premises NetScaler ADM ein HA-Paar ist?

Alle Konfigurationen werden auf Citrix Cloud verschoben. Die Konfiguration eines Disaster Recovery-Knotens ist nicht erforderlich.

Was passiert, wenn der Agent aus irgendeinem Grund ausfällt?

Sie können mit einem potenziellen Datenverlust rechnen, bis der Agent betriebsbereit ist. Sie können jedoch auch ADM-Agenten für Multisite-Bereitstellungen konfigurieren, um die Kontinuität bei einem Agentenfailover zu gewährleisten. Weitere Informationen finden Sie unter Konfigurieren von ADM-Agenten für die Multisite-Bereitstellung.

Wird das Instanzbackup auch migriert?

Das Backup ist nicht in der Migration enthalten.

Sind historische Daten auch migriert?

Historische Daten werden nicht migriert. Sie können die Daten aus dem on-premises ADM exportieren.

Werden on-premises Lizenzen auch migriert?

Nein. Die on-premises Lizenzdatei kann nicht für ADM Service verwendet werden. Sie müssen Lizenzen für ADM Service erwerben. Weitere Informationen finden Sie unter Lizenzierung. Wenn Sie gepoolte Lizenzen im on-premises ADM verwenden, müssen Sie gepoolte Lizenzen für den ADM-Service beziehen und dann Instanzen Lizenzen zuweisen.

Was wird nicht von on-premises NetScaler ADM migriert?

Die folgenden Funktionen können nicht auf ADM Service migriert werden:

- **RBAC** —In ADM Service basiert der Benutzerzugriff auf der Einladung des Administrators. Benutzer von ADM Service müssen ein Konto in Citrix Cloud haben. Infolgedessen werden die on-premises ADM-Benutzer nicht migriert.
- **Exportpläne** —Exportpläne enthalten Details wie Drilldown und Zeitpläne von verschiedenen Seiten. All diese detaillierten Exportpläne werden nicht migriert.
- **SSL-Zertifikate/Schlüssel/CSRs** —ADM Service kann nur die ADC SSL-Zertifikate/Schlüssel/CSRs anzeigen. Infolgedessen werden SSL-Zertifikate/Schlüssel, die auf ein on-premises NetScaler ADM hochgeladen wurden, nicht in ADM Service migriert.

On-Premises NetScaler ADM ist in Citrix Director integriert. Was passiert mit der Integration?

Die Director-Integration mit ADM wird derzeit nur im on-premises ADM unterstützt.

Ist es nach der Migration erneut erforderlich, die Instanz zu lizenzieren oder Analysen zu aktivieren?

Sie müssen sicherstellen, dass die Lizenzen im ADM-Service mehr oder gleich den on-premises VIP-Lizenzen sind. Wenn die Lizenzen bereits mehr sind als das on-premises NetScaler ADM VIP, werden die virtuellen Server automatisch lizenziert. Wenn nicht, werden die Lizenzen nach dem Zufallsprinzip vergeben.

Migrations-T

Nach dem Ausführen des Migrationsskripts werden Fehlermeldungen angezeigt. Was kann das Problem sein?

Eine Protokolldatei mit Fehlergründen wird angezeigt. Sie können geeignete Korrekturmaßnahmen ergreifen und das Migrationsskript erneut ausführen. Bevor Sie das Migrationsskript ausführen, müssen Sie im Allgemeinen Folgendes sicherstellen:

- ADM Service Agent konfigurieren
- Beschaffen der ADM-Service-Lizenzen
- Kopieren Sie den richtigen Pfad, in dem Sie den Client gespeichert haben, und sichern Sie die CSV-Datei

Die ADC-Instanzen haben niedrigere Versionen als die genannte Beschränkung für gepoolte Lizenzen. Was passiert, wenn die Option "Y"zum Ändern des Lizenzservers ausgewählt ist?

Die Änderung des Lizenzservers erfolgt nur für die unterstützten Versionen von NetScaler MPX, VPX und SDX.

Was passiert, wenn das Migrationsskript in Bezug auf ADC-Instanzen nicht konfiguriert wurde?

Die ADC-Instanzen arbeiten weiterhin mit dem on-premises ADM-Setup. Sie können die erforderlichen Maßnahmen aus dem vorgeschlagenen fehlgeschlagenen Grund ausführen und das Migrationsskript erneut ausführen.

Was passiert, wenn einige der ADC-Instanzen nicht zum ADM Service wechseln können? Hilft die Wiederverbucht des Migrationsskripts?

Ja. Nachdem Sie das Skript erneut ausgeführt haben, werden nur die fehlgeschlagenen Instanzen migriert. Nehmen wir an, dass sich zwei von fünf Instanzen nicht bewegt haben. Nachdem Sie Korrekturmaßnahmen ergriffen und das Migrationsskript erneut ausgeführt haben, zeigen drei Instanzen, die zuvor erfolgreich verschoben wurden, die Meldung "Gerät ist bereits vorhanden"an. Und die anderen beiden Instanzen, die früher gescheitert sind, werden erfolgreich migriert.

Gibt es eine Protokolldatei, um den Migrationsstatus zu überprüfen?

Ja, eine Protokolldatei wird im `/var/mps/log/` Verzeichnis generiert. ADM mit python3.7 hat die Protokolldatei als `servicemigrationtool.py.log` und ADM mit Python 2.7 hat die Protokoll-

datei als `servicemigrationtool_27.py.log`.

Was passiert, wenn die Sitzung während der Ausführung des Migrationsskripts beendet wird?

Sie können das Migrationsskript erneut ausführen. In der neuen Sitzung werden die bereits hinzugefügten Instanzen aus der letzten Sitzung als "Gerät existiert bereits"angezeigt, und die Migration wird weiter fortgesetzt.

Was passiert, wenn ADM Service weniger Lizenzen hat als das on-premises NetScaler ADM und das Migrationsskript initiiert wird?

Nachdem das Migrationsskript ausgeführt wurde, wird ein Vorschlag angezeigt, in dem erwähnt wird, dass die Lizenzen geringer sind, und fordert Sie auf, fortzufahren oder zu stoppen. Wenn Sie mit geringeren Lizenzen fortfahren möchten, werden die virtuellen Server nach dem Zufallsprinzip aus den verfügbaren Lizenzen lizenziert.

Was passiert, wenn on-premises NetScaler ADM auf das Express-Konto von ADM Service migriert wird?

Das ADM-Dienst-Express-Konto verfügt nur über zwei virtuelle Serverlizenzen, zwei StyleBook-Konfigurationspakete und zwei Konfigurationsaufträge. Wenn Ihr lokales ADM über mehr als diese Konfigurationen verfügt und Sie die Migration mit Express Account initiieren, kann das Skript nur die genannten Konfigurationen migrieren, die für Express Account gelten (zwei virtuelle Serverlizenzen, zwei StyleBook-Konfigurationspakete und zwei Konfigurationsaufträge).

Was passiert, wenn ein von Citrix Cloud eingeladener Benutzer (außer einem Admin-Benutzer, der ein Citrix Cloud-Konto erstellt hat) versucht, das lokale ADM-Setup zu migrieren?

Es wird empfohlen, dass der Administrator das Migrationsskript ausführt. Ein eingeladener Benutzer hat keine Administratorrechte (AdminExceptSystem_Group). Infolgedessen schlägt die Migration von Gruppen, Rollen und Richtlinien fehl und die Meldung "Benutzer hat keine Berechtigung"wird angezeigt.

Als Lösung kann der Administrator (der das Citrix Cloud-Konto erstellt hat) die Gruppe, die mit dem eingeladenen Benutzer verknüpft ist, als "admin_group"ändern.

Rollback-Skript

Was passiert, wenn ein Rollback-Skript in einem on-premises ADM-HA-Paar verwendet wird?

Das on-premises ADM-HA-Paar wird mit allen Konfigurationen wiederhergestellt, die vor der Migration verfügbar waren.

Was passiert mit dem Disaster Recovery-Knoten nach Verwendung des Rollback-Skripts?

Der Disaster Recovery-Knoten wird vor der Migration mit allen Konfigurationen ebenfalls wiederhergestellt.

Problembehandlung

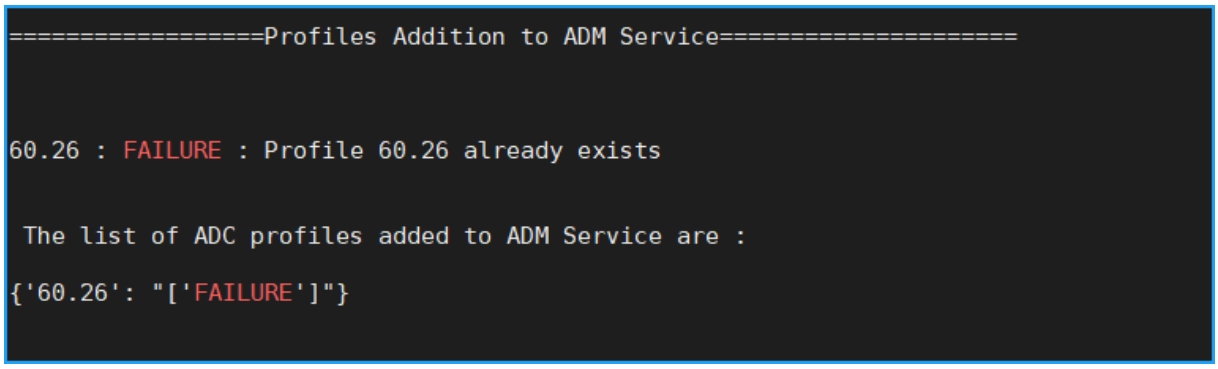
February 5, 2024

Wenn Sie das Migrationsskript zum ersten Mal ausführen, sucht es nach den Voraussetzungen und fährt mit der Migration fort. Wenn alle Voraussetzungen erfüllt sind, wird die Migration ohne Fehler abgeschlossen. Wenn eine Voraussetzung fehlschlägt, zeigt das Skript Fehlermeldungen mit Gründen an. Nachdem Sie die Fehler behoben haben, müssen Sie das Skript erneut ausführen.

> Hinweis
>
> Wenn eine Fehlermeldung angezeigt wird, die “bereits existiert”anzeigt, bedeutet dies Folgendes:
>
> - Möglicherweise haben Sie das Migrationsskript mehr als einmal ausgeführt und einige Konfigurationen sind bereits in ADM Service migriert.
> - Möglicherweise haben Sie die gleiche Konfiguration in ADM Service manuell erstellt, bevor Sie das Migrationsskript ausführen.

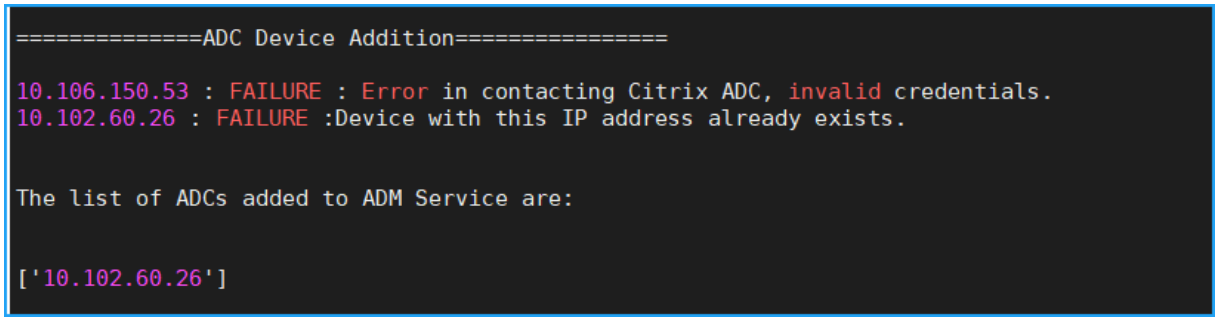
Beziehen Sie sich auf einige der folgenden Fehlermeldungen:

Manuelles Profil zu ADM Service hinzugefügt



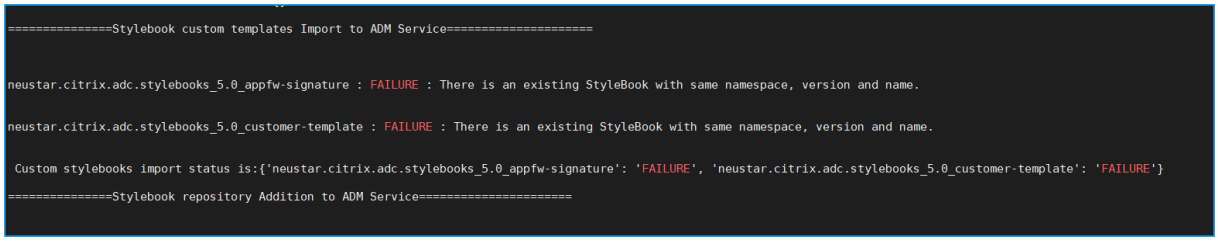
Workaround: Wenn Sie vor dem Ausführen des Migrationsskripts Administratorprofile in NetScaler ADM Service erstellt haben, müssen Sie diese Profile löschen und das Migrationsskript erneut ausführen.

NetScaler-Gerät wurde zu ADM Service hinzugefügt



Workaround: Stellen Sie im on-premises ADM den Instanzstatus sicher und prüfen Sie, ob Sie ohne Probleme auf die Instanz zugreifen können. Wenn ein Problem weiterhin besteht, beheben Sie das Problem und führen Sie das Migrationsskript erneut aus.

Benutzerdefinierte Vorlagen von StyleBook werden in ADM Service importiert



Workaround: Diese Fehlermeldung ist ein Beispiel für das bereits migrierte StyleBook. Sie können diesen Fehler auch sehen, wenn Sie ein StyleBook mit demselben Namen, derselben Version und

demselben Namespace in NetScaler ADM Service erstellt haben, bevor Sie das Migrationsskript ausführen.

Konfigurationsjobs zu ADM Service hinzugefügt

```
==============Config Jobs Addition to ADM Service====================


config_job2_show_ns_ip : FAILURE : Express user can have maximum 2 config jobs

ConfigJob1_show_ha_node : FAILURE : Express user can have maximum 2 config jobs

 The config jobs status is :
{'config_job2_show_ns_ip': 'FAILURE', 'ConfigJob1_show_ha_node': 'FAILURE'}
```

Workaround: Dieser Fehler tritt auf, wenn Sie Express Account abonniert haben und mehr als zwei Konfigurationsaufträge haben. Sie müssen ein gültiges Abonnement erwerben, damit alle Ihre Konfigurationsjobs migriert werden können.

IP-Blöcke zu ADM Service hinzugefügt

```
====================IP Blocks Addition in ADM Service======================


ipblock1 : FAILURE : IP Block Name ipblock1 already exists

ipblock3 : FAILURE : IP Block Name ipblock3 already exists

test : FAILURE : IP Block Name test already exists
```

Workaround: Löschen Sie den IP-Block, der manuell in ADM Service erstellt wurde, und führen Sie das Migrationsskript erneut aus.

Netzwerk-Dashboard Additionsstatus

```
================Network Dashboard Reports Addition to ADM Service================


new456 : FAILURE : Dashboard new456 already exists

new123 : FAILURE : Dashboard new123 already exists

 The network dashoard reports addition status is:
{'new456': "['FAILURE']", 'new123': "['FAILURE']"}
```

Workaround: Löschen Sie das Dashboard, das manuell in ADM Service erstellt wurde, und führen Sie das Migrationsskript erneut aus.

Alle Wie-Macht-Man-Artikel

February 5, 2024

Die „How-to-Artikel“von NetScaler Application Delivery Management (NetScaler ADM) sind einfache, relevante und leicht zu implementierende Artikel zu den Funktionen von NetScaler ADM. Diese Artikel enthalten Informationen zu einigen der beliebtesten NetScaler ADM-Funktionen wie Instanzverwaltung, Anwendungsverwaltung, StyleBooks, Zertifikatsverwaltung und Analytics.

Klicken Sie in der Tabelle unten auf einen Feature-Namen, um die Liste der Artikel mit Anleitungen für diese Funktion anzuzeigen.

Themen				
Instanzverwaltung	Ereignisverwaltung	StyleBooks	Zertifikatverwaltung	NetScaler ADM -System
	Konfigurationsverwaltung	Authentifizierung	Analytics	Netzwerkfunktionen

Instanzverwaltung

So überwachen Sie global verteilte Websites

Verwalten von Adminpartitionen von NetScaler-Instanzen

So fügen Sie Instanzen zu NetScaler ADM hinzu

So erstellen Sie Instanzgruppen auf NetScaler ADM

So konfigurieren Sie Sites für Geomaps in NetScaler ADM

So erzwingen Sie mithilfe von NetScaler ADM ein Failover zur sekundären NetScaler-Instanz

So zwingen Sie eine sekundäre NetScaler-Instanz, mithilfe von NetScaler ADM sekundär zu bleiben

So sichern und stellen Sie eine Instanz mit NetScaler ADM wieder her

So verwenden Sie das NetScaler ADM-Dashboard zur Überwachung einer HAProxy-Instanz

So zeigen Sie die Details der auf HAProxy-Instanzen konfigurierten Frontends an

So zeigen Sie die Details der auf HAProxy-Instanzen konfigurierten Backends an

So zeigen Sie die Details der auf HAProxy-Instanzen konfigurierten Server an

So starten Sie eine HAProxy-Instanz von NetScaler ADM aus neu

So sichern und stellen Sie eine HAProxy-Instanz mithilfe von NetScaler ADM wieder her

So bearbeiten Sie die HAProxy-Konfigurationsdatei mit NetScaler ADM

So entdecken Sie mehrere NetScaler VPX-Instanzen wieder

Abfragen von NetScaler-Instanzen und Entitäten in NetScaler ADM

So heben Sie die Verwaltung einer Instanz auf NetScaler ADM auf

So verfolgen Sie die Route zu einer Instanz von NetScaler ADM

Konfigurationsverwaltung

So erstellen Sie einen Konfigurationsauftrag auf NetScaler ADM

So verwenden Sie den SCP (put) -Befehl in Konfigurationsjobs

So aktualisieren Sie NetScaler SDX-Instanzen mithilfe von NetScaler ADM

So planen Sie Jobs, die mithilfe integrierter Vorlagen in NetScaler ADM erstellt wurden

So verschieben Sie Aufträge, die mithilfe integrierter Vorlagen in NetScaler ADM konfiguriert wurden

So können ausgeführte Konfigurationsjobs wiederverwendet werden

Aktualisieren von NetScaler-Instanzen mithilfe von NetScaler ADM

So verwenden Sie Variablen in Konfigurationsaufträgen auf NetScaler ADM

So verwenden Sie Konfigurationsvorlagen zum Erstellen von Überwachungsvorlagen auf NetScaler ADM

So erstellen Sie Konfigurationsaufträge aus Korrekturbefehlen in NetScaler ADM

So replizieren Sie laufende und gespeicherte Konfigurationsbefehle von einer NetScaler-Instanz auf eine andere auf NetScaler ADM

So verwenden Sie Record and Play, um Konfigurationsaufträge zu erstellen

So verwenden Sie Konfigurationsjobs, um die Konfiguration von einer Instanz auf mehrere Instanzen zu replizieren

So verwenden Sie die Masterkonfigurationsvorlage in NetScaler ADM

So fragen Sie das Konfigurationsaudit von NetScaler-Instanzen ab

So verwenden Sie Vorlagen für Konfigurationsprüfungen in Konfigurationsaufträgen wieder

So importieren und exportieren Sie Konfigurationsvorlagen

So generieren Sie einen Konfigurationsaudit-Diff für ConfigChange-SNMP-Traps

Zertifikatverwaltung

So konfigurieren Sie eine Unternehmensrichtlinie in NetScaler ADM

Installieren von SSL-Zertifikaten auf einer NetScaler-Instanz von NetScaler ADM

So aktualisieren Sie ein installiertes Zertifikat von NetScaler ADM

So verknüpfen und trennen Sie SSL-Zertifikate mithilfe von NetScaler ADM

So erstellen Sie eine Certificate Signing Request (CSR) mithilfe von NetScaler ADM

So richten Sie Benachrichtigungen für den Ablauf des SSL-Zertifikats von NetScaler ADM ein

So verwenden Sie das SSL-Dashboard auf NetScaler ADM

Abfragen von SSL-Zertifikaten von NetScaler Instanzen

StyleBooks

So zeigen Sie verschiedene Gruppen von StyleBooks an

So erstellen Sie Ihre eigenen StyleBooks

So verwenden Sie benutzerdefinierte StyleBooks in NetScaler ADM

So verwenden Sie die API, um Konfigurationen aus StyleBooks zu erstellen

So aktivieren Sie Analysen und konfigurieren Alarme auf einem in einem StyleBook definierten virtuellen Server

So erstellen Sie ein StyleBook zum Hochladen von Dateien auf NetScaler ADM

So verwenden Sie die API, um Konfigurationen zum Hochladen eines beliebigen Dateityps zu erstellen

So erstellen Sie ein StyleBook, um SSL-Zertifikat- und Zertifikatsschlüsseldateien auf NetScaler ADM hochzuladen

So verwenden Sie die API, um Konfigurationen zum Hochladen von Zertifikat- und Schlüsseldateien zu erstellen

So verwenden Sie Microsoft Skype for Business StyleBook in Unternehmen

So verwenden Sie Microsoft Exchange StyleBook in Geschäftsunternehmen

So verwenden Sie Microsoft SharePoint StyleBook in Geschäftsunternehmen

Analytics

So aktivieren Sie Analysen für Instances

So konfigurieren Sie adaptive Schwellenwerte

So konfigurieren Sie das SLA-Management

So konfigurieren Sie die Datenbankzusammenfassung für Analysen

So erstellen Sie Schwellenwerte und Warnungen mit NetScaler ADM

So deaktivieren Sie die URL-Datenerfassung für Analysen von NetScaler ADM

So zeigen Sie die Art der gestreamten Videos und das von Ihrem Netzwerk verbrauchte Datenvolumen an

So zeigen Sie die Spitzendatenrate für einen bestimmten Zeitrahmen an

So sehen Sie die Netzwerkeffizienz

Ereignisverwaltung

So legen Sie das Ereignisalter für Ereignisse in NetScaler ADM fest

So planen Sie einen Ereignisfilter mithilfe von NetScaler ADM

So richten Sie wiederholte E-Mail-Benachrichtigungen für Ereignisse von NetScaler ADM ein

So unterdrücken Sie Ereignisse mithilfe von NetScaler ADM

So verwenden Sie das Ereignis-Dashboard, um Ereignisse zu überwachen

So erstellen Sie Ereignisregeln auf NetScaler ADM

Ändern des gemeldeten Schweregrads von Ereignissen, die auf NetScaler-Instanzen auftreten

Authentifizierung

NetScaler ADM-System

So weisen Sie einem NetScaler ADM Server einen Hostnamen zu

So konfigurieren Sie die System-Prune-Einstellungen für NetScaler ADM

So konfigurieren Sie die Systemsicherungseinstellungen mithilfe von NetScaler ADM

Konfigurieren und Anzeigen von Systemalarmen in NetScaler ADM

Netzwerkfunktionen

So generieren Sie Berichte für Load-Balancing-Entitäten

So exportieren oder planen Sie den Export von Netzwerkfunktionsberichten

Übersicht

February 5, 2024

NetScaler Application Delivery Management (ADM) ist eine zentrale Verwaltungslösung, die den Betrieb vereinfacht, indem sie Administratoren unternehmensweite Transparenz bietet und Verwaltungsaufgaben automatisiert, die auf mehreren Instanzen ausgeführt werden müssen. Sie können NetScaler-Produkte verwalten und überwachen, zu denen NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler CPX und NetScaler Gateway gehören. Sie können ADM verwenden, um die gesamte globale Infrastruktur für die Anwendungsbereitstellung von einer einzigen, einheitlichen Konsole aus zu verwalten, zu überwachen und Fehler zu beheben.

ADM ist eine virtuelle Appliance, die auf Citrix Hypervisor, VMware ESXi und Linux KVM läuft. ADM begegnet der Herausforderung der Anwendungstransparenz, indem es die folgenden detaillierten Informationen über den Traffic von Webanwendungen und virtuellen Desktops sammelt:

- Informationen auf Benutzersitzungsebene
- Leistungsdaten der Webseite
- -Datenbankinformationen, die durch die ADC-Instanzen an Ihrem Standort fließen und umsetzbare Berichte bereitstellen.

ADM ermöglicht es IT-Administratoren, Kundenprobleme innerhalb weniger Minuten zu beheben und proaktiv zu überwachen.

Features und Lösungen

February 5, 2024

NetScaler Application Delivery Management (ADM) bietet die folgenden Funktionen:

Anwendungsanalyse und -verwaltung

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 eine gute Leistung erbringt, nicht anfällig für Bedrohungen ist und alle Systeme in Betrieb hat.

Analysen zur Anwendungssicherheit

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, Angriffe auf kleine Fenster und DNS-Hochwasserangriffe für die entdeckten ADC-Instanzen an.

Netzwerke

Instances

Ermöglicht die Verwaltung der NetScaler- und NetScaler Gateway-Instanzen.

Instanzgruppen

Ermöglicht es Ihnen, Ihre Instances wie folgt zu gruppieren:

- Statische Gruppe: Ermöglicht die Definition einer Gerätegruppe, die Sie für verschiedene Aufgaben wie Konfigurationsaufträge usw. verwenden können.
- Privater IP-Block: Ermöglicht es Ihnen, Ihre Instances nach geografischen Standorten zu gruppieren.

Ereignisverwaltung

Wenn die IP-Adresse einer ADC-Instanz zu ADM hinzugefügt wird, wird ein NITRO -Aufruf von ADM gesendet und implizit selbst als Trap-Ziel für die Instanz hinzugefügt, um ihre Traps oder Ereignisse zu empfangen.

Ereignisse stellen das Auftreten von Ereignissen oder Fehlern in einer verwalteten ADC-Instanz dar.

Zertifikatverwaltung

NetScaler 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 ADM und seine Funktionen zu verwenden, müssen Sie verstehen, was ein SSL-Zertifikat ist und wie Sie ADM verwenden können, um Ihre SSL-Zertifikate zu verfolgen.

Konfigurationsverwaltung

Mit NetScaler ADM können Sie Konfigurationsaufträge erstellen, mit denen Sie Konfigurationsaufgaben wie das Erstellen von Entitäten, das Konfigurieren von Features, die Replikation von Konfigurationsänderungen, Systemaktualisierungen und andere Wartungsaktivitäten auf mehreren Instanzen problemlos ausführen können. Konfigurationsaufträge und Vorlagen vereinfachen die sich wiederholenden Verwaltungsaufgaben zu einer einzigen Aufgabe in ADM.

Konfigurationsaudit

Ermöglicht es Ihnen, Anomalien in den Konfigurationen in Ihren Instanzen zu überwachen und zu identifizieren.

- Konfigurationshinweis: Ermöglicht die Identifizierung von Konfigurationsanomalien.
- Audit-Vorlage: Ermöglicht Ihnen, die Änderungen in einer bestimmten Konfiguration zu überwachen.

Netzwerkberichterstellung

Sie können die Ressourcennutzung optimieren, indem Sie Ihre Netzwerkberichte auf ADM überwachen.

Analytics

Web Insight

Bietet Einblick in Unternehmens-Webanwendungen und ermöglicht IT-Administratoren die Überwachung aller Webanwendungen, die vom NetScaler bereitgestellt werden, indem die Anwendungen integriert und in Echtzeit überwacht werden. Web Insight bietet wichtige Informationen wie die Antwortzeit von Benutzern und Servern, sodass IT-Organisationen die Anwendungsleistung überwachen und verbessern können.

HDX Insight

Bietet umfassende Transparenz für den ICA-Verkehr, der über NetScaler fließt. Mit HDX Insight können Administratoren Client- und Netzwerklatenzmetriken, historische Berichte und End-to-End-Leistungsdaten in Echtzeit anzeigen und Leistungsprobleme beheben.

Gateway Insight

Bietet einen Überblick über die Fehler, auf die Benutzer bei der Anmeldung stoßen, unabhängig vom Zugriffsmodus. Sie können eine Liste der zu einem bestimmten Zeitpunkt angemeldeten Benutzer anzeigen, zusammen mit der Anzahl der aktiven Benutzer, der Anzahl der aktiven Sitzungen sowie Bytes und Lizenzen, die von allen Benutzern zu einem bestimmten Zeitpunkt verwendet werden.

Security Insight

Bietet eine zentrale Lösung, mit der Sie den Sicherheitsstatus Ihrer Anwendung beurteilen und Korrekturmaßnahmen zum Schutz Ihrer Anwendungen ergreifen können.

SSL Insight

SSL Insight bietet Einblick in sichere Webtransaktionen (HTTPS) und ermöglicht IT-Administratoren, alle vom NetScaler bereitgestellten sicheren Webanwendungen zu überwachen, indem sie eine integrierte Echtzeit- und historische Überwachung sicherer Webtransaktionen bereitstellen.

TCP Insight

TCP Insight bietet eine einfache und skalierbare Lösung für die Überwachung der Metriken der Optimierungstechniken und Strategien zur Überlastung (oder Algorithmen), die in ADC-Instanzen verwendet werden, um Netzwerküberlastungen bei der Datenübertragung zu vermeiden.

Video Insight

Die Video Insight-Funktion bietet eine einfache und skalierbare Lösung für die Überwachung der Metriken der Videooptimierungstechniken, die von NetScaler-Instanzen verwendet werden, um das Kundenerlebnis und die betriebliche Effizienz zu verbessern.

WAN Insight

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 auch Einblick in Clients, Anwendungen und Zweigstellen im Netzwerk, um Netzwerkprobleme effektiv zu beheben.

Orchestrierung

Cloud-Orchestrierung

Ermöglicht die Integration von NetScaler-Produkten mit der OpenStack-Cloud-Orchestrierung. NetScaler ADM und OpenStack implementieren einander APIs und ermöglichen die Integration der Load Balancing Feature (LBaaS) der NetScaler Instanz mit OpenStack Cloud Orchestrierung.

Orchestration

NetScaler ADM unterstützt SDN im Unternehmensnetzwerk durch Integration mit SDN-Controllern verschiedener Anbieter. ADM unterstützt sowohl VMware NSX Manager als auch Cisco Application Policy Infrastructure Controller (APIC).

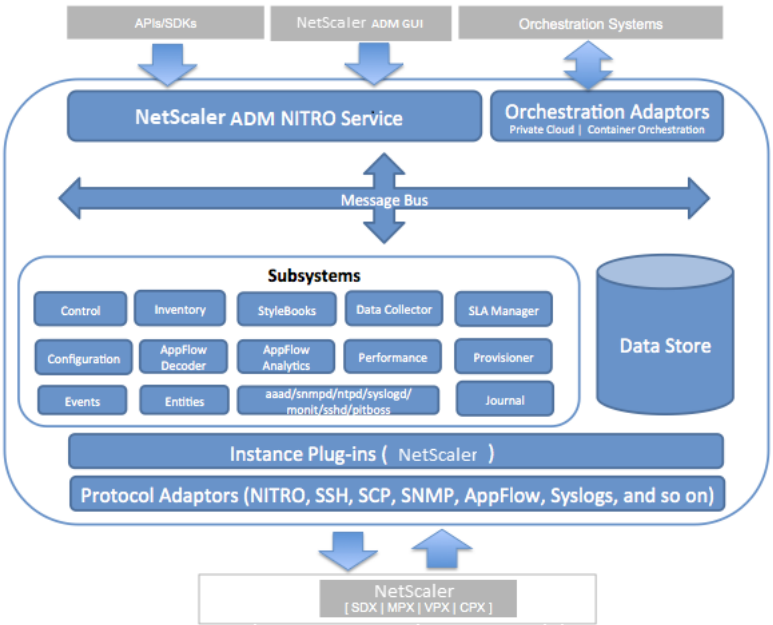
Architektur

February 5, 2024

Die NetScaler Application Delivery Management (ADM) -Datenbank ist in den Server integriert, und der Server verwaltet alle wichtigen Prozesse wie Datenerfassung und NITRO-Aufrufe. In seinem Datenspeicher speichert der Server eine Bestandsaufnahme der Instanzdetails wie Hostname, Softwareversion, laufende und gespeicherte Konfiguration, Zertifikatsdetails und auf der Instance konfigurierte Entitäten. Eine Bereitstellung auf einem einzelnen Server eignet sich, wenn Sie kleine Datenverkehrsmengen verarbeiten oder Daten für eine begrenzte Zeit speichern möchten.

Derzeit unterstützt ADM zwei Arten von Softwarebereitstellungen: Einzelserver und Hochverfügbarkeit.

Die folgende Abbildung zeigt die verschiedenen Subsysteme innerhalb von ADM und wie die Kommunikation zwischen dem ADM-Server und den verwalteten Instanzen erfolgt.



Das Dienst-Subsystem in ADM fungiert als Webserver, der HTTP-Anfragen und -Antworten verarbeitet, die über die Ports 80 und 443 von der GUI oder der API aus an Subsysteme innerhalb von ADM gesendet werden. Diese Anfragen werden über den Message Bus (Message Processing System) an die Subsysteme über den IPC (Inter-Process Communication) -Mechanismus gesendet. Eine Anforderung

wird an das Teilsystem “Control”gesendet, das die Informationen entweder verarbeitet oder an das entsprechende Teilsystem sendet. Jedes der anderen Subsysteme —Inventory, StyleBooks, Data Collector, Konfiguration, AppFlow Decoder, AppFlow Analytics, Performance, Events, Entities, SLA Manager, Provisioner und Journal —hat eine bestimmte Rolle.

Instanz-Plug-Ins sind freigegebene Bibliotheken, die für jeden Instanztyp, der von ADM unterstützt wird, eindeutig sind. Informationen werden zwischen ADM und verwalteten Instanzen mithilfe von NITRO-Aufrufen oder über das SNMP-, Secure Shell- (SSH) oder Secure Copy (SCP) -Protokoll übertragen. Diese Informationen werden dann verarbeitet und in der internen Datenbank (Datenspeicher) gespeichert.

Instanzdiscovery in NetScaler ADM

February 5, 2024

Instanzen sind NetScaler ADC-Appliances oder virtuelle Appliances, die Sie von NetScaler Application Delivery Management (ADM) aus erkennen, verwalten und überwachen möchten. Um diese Instanzen zu verwalten und zu überwachen, müssen Sie sie dem NetScaler ADM-Server hinzufügen. Sie können die folgenden NetScaler ADC-Appliances und virtuellen Appliances zu ADM hinzufügen:

- NetScaler-Instanzen
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
- NetScaler Gateway Instanzen

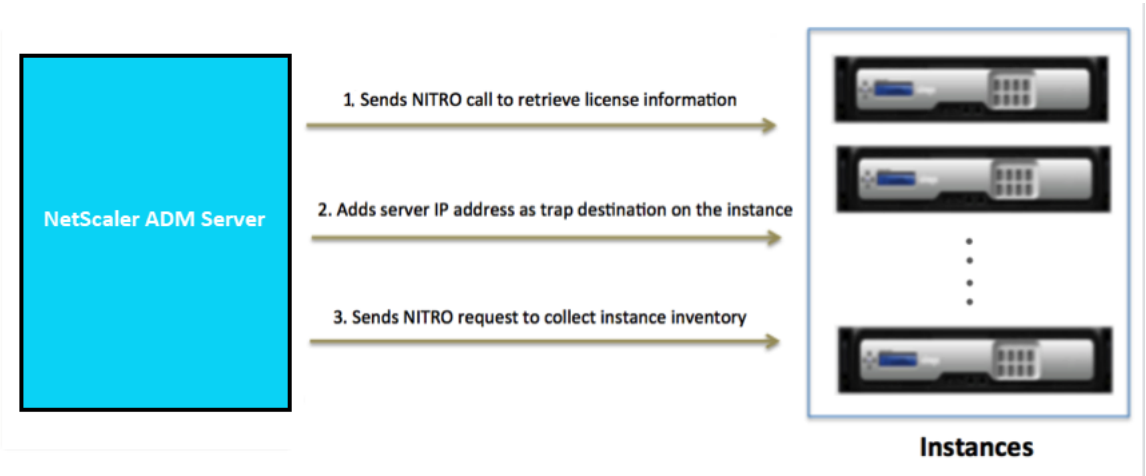
Sie können Instanzen hinzufügen, wenn Sie den NetScaler ADM-Server zum ersten Mal oder später einrichten.

> **Hinweis**
>
> NetScaler ADM verwendet die NetScaler IP (NSIP) -Adresse der ADC-Instanzen für die Kommunikation. ADM kann auch ADC-Instanzen mit einer Subnetz-IP-Adresse (SNIP) erkennen, für die Verwaltungszugriff aktiviert ist. Informationen zu den Ports, die zwischen den ADC-Instanzen und ADM geöffnet sein müssen, finden Sie unter Ports.
>
> Wenn Sie ein ADC-HA-Paar mit SNIP hinzufügen möchten, stellen Sie sicher, dass der Indepen-

> dent Network Configuration (INC) -Modus für das ADC-HA-Paar aktiviert ist. Weitere Informationen zum Hinzufügen von Instanzen finden Sie unter Instanzen hinzufügen.

Wenn Sie dem ADM-Server eine Instanz hinzufügen, fügt sich der Server implizit selbst als Trap-Ziel für die Instanz hinzu und sammelt Inventar der Instanz.

Das folgende Diagramm beschreibt, wie ADM Instanzen implizit erkennt und hinzufügt.



Wie im Diagramm gezeigt, werden die folgenden Schritte implizit von NetScaler ADM durchgeführt.

1. NetScaler ADM verwendet die Details des Instanzprofils, um sich bei der Instanz anzumelden. Mithilfe eines ADC-NITRO-Aufrufs ruft ADM die Lizenzinformationen der Instanz ab. Basierend auf den Lizenzinformationen bestimmt es, ob es sich bei der Instanz um eine ADC-Instanz handelt und um welche Art von ADC-Plattform es sich handelt (z. B. NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler BLX oder NetScaler Gateway). Bei erfolgreicher Erkennung der Instanz wird sie der ADM-Datenbank hinzugefügt.

   Dieser Schritt schlägt möglicherweise fehl, wenn das Instanzprofil nicht die richtigen Anmeldeinformationen enthält. Bei NetScaler MPX-, NetScaler VPX-, NetScaler SDX-, NetScaler BLX- und NetScaler Gateway-Instanzen kann dieser Schritt auch fehlschlagen, wenn die Lizenzen nicht auf die Instanz angewendet werden.

   > **Hinweis**
   >
   > Mithilfe von HTTP können Sie alle Instanzen zu ADM hinzufügen, auch wenn die Lizenzen für die Instanzen nicht konfiguriert sind.

2. ADM fügt seine IP-Adresse der Liste der Trap-Ziele auf der Instance hinzu. Dadurch kann ADM Traps empfangen, die auf der ADC-Instanz generiert wurden.

   Dieser Schritt schlägt möglicherweise fehl, wenn die Anzahl der Trap-Ziele auf der Instance die maximale Anzahl von Trap-Zielen überschreitet. Die Höchstgrenze für Instanzen liegt bei 20.

3. ADM sammelt Inventar von der Instanz, indem eine NITRO -Anfrage gesendet wird. Es sammelt Instanzdetails wie Hostname, Softwareversion, laufende und gespeicherte Konfiguration, Zertifikatsdetails, auf der Instanz konfigurierte Entitäten.

   Dieser Schritt kann aufgrund von Netzwerk- oder Firewallproblemen fehlschlagen.

   Informationen zum Hinzufügen von Instanzen zu ADM finden Sie unter Instanzen hinzufügen.

Übersicht über die Abrufung

February 5, 2024

Polling ist ein Prozess, bei dem NetScaler Application Delivery Management (ADM) bestimmte Informationen von NetScaler-Instances sammelt. Möglicherweise haben Sie weltweit mehrere NetScaler-Instanzen für Ihre Organisation konfiguriert. Um Ihre Instances über NetScaler ADM zu überwachen, muss NetScaler ADM bestimmte Informationen wie CPU-Auslastung, Speichernutzung, SSL-Zertifikate, lizenzierte Funktionen, Lizenztypen usw. von allen verwalteten ADC-Instances sammeln. Im Folgenden werden die verschiedenen Abruftypen aufgeführt, die zwischen ADM und den verwalteten Instanzen auftreten:

- Instanz-Abfrage
- Lagerbestandsabfrage
- Leistungsdatenerfassung
- Instanz-Backup-Abfrage
- Konfigurationsüberwachungsabfrage
- Abfrage von SSL-Zertifikaten
- Entitätsabfrage

NetScaler ADM verwendet Protokolle wie NITRO -Aufruf, Secure Shell (SSH) und Secure Copy (SCP), um Informationen von NetScaler-Instanzen abzufragen.

Wie NetScaler ADM verwaltete Instanzen und Entitäten abfragt

NetScaler ADM fragt standardmäßig automatisch in regelmäßigen Abständen ab. Mit NetScaler ADM können Sie auch Abfrageintervalle für einige Abfragetypen konfigurieren und bei Bedarf manuell abfragen.

In der folgenden Tabelle werden die Details der Abfragetypen, des Abfrageintervalls, des verwendeten Protokolls usw. beschrieben:

Abfrage-Typ	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufin
Instanz-Abfrage	Alle 5 Minuten (standardmäßig)	Statistische Informationen wie Status, HTTP-Anforderungen pro Sekunde, CPU-Auslastung, Speicherauslastung und Durchsatz.	NITRO-Anruf.	Nein
Lagerbestandsabfrage	Alle 60 Minuten (standardmäßig)	Inventardetails wie Build-Version, Systeminformationen, lizenzierte Funktionen und Modi.	NITRO-Anrufe und SSH	Nein
Erfassung von Leistungsdaten	Alle 5 Minuten (standardmäßig)	Informationen zur Netzwerkberichterstattung	NITRO-Anruf	Nein
Instanzbackupabruf	Alle 12 Stunden (standardmäßig)	Sicherungsdatei des aktuellen Status der verwalteten ADC-Instanzen	NITRO ruft, SSH und SCP.	Ja. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** . Wählen Sie die Instanz aus, und klicken Sie in der Liste **Aktion auswählen** auf **Backup/Restore**.

Abfrage-Typ	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufin
Abfragen der Konfigurationsüberprüfung	Alle 10 Stunden (standardmäßig)	Konfigurationsänderungen, die auf ADC-Instanzen auftreten (z. B. laufende oder gespeicherte Konfiguration)	SSH, SCP- und NITRO-Anruf	Ja. Navigieren Sie zu **Infrastruktur > Konfigurationsprüfung**. Klicken Sie auf der Seite Configuration Audit auf **Einstellungen**, und konfigurieren Sie das Abrufintervall für Configuration Audit Polling. Sie können Konfigurationsaudits manuell abfragen und alle Konfigurationsaudits der Instanzen sofort NetScaler ADM hinzufügen. Navigieren Sie dazu zu **Infrastruktur > Konfigurationsprüfung** und klicken Sie auf **Jetzt abfragen**. Auf der **Seite Jetzt** abfragen können Sie alle oder ausgewählte Instanzen im Netzwerk abfragen.

Abfrage-Typ	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufin
Abfrage von SSL-Zertifikaten	Alle 24 Stunden (standardmäßig)	SSL-Zertifikate, die auf NetScaler-Instanzen installiert sind.	NITRO-Anrufe und SCP	Ja. Navigieren Sie zu **Infrastruktur > 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 NetScaler ADM hinzufügen. Navigieren Sie dazu zu **Infrastruktur > SSL Dashboard** und klicken Sie auf **Jetzt abfragen**. Auf der **Seite Jetzt** abfragen können Sie alle oder ausgewählte Instanzen im Netzwerk abfragen.

Abfrage-Typ	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufin
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 ADM-Funktionen aktivieren oder deaktivieren.	NITRO ruft an.	Ja, kann aber nicht auf weniger als 10 Minuten eingestellt werden. Navigieren Sie zur Konfiguration zu **Infrastruktur > Netzwerkfunktionen**. Klicken Sie auf der Seite Netzwerkfunktion auf **Einstellungen**, um das Abrufintervall zu konfigurieren.

Abfrage-Typ	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufin
				Sie können Entitäten manuell abfragen und alle Entitäten der Instanzen sofort NetScaler ADM hinzufügen. Navigieren Sie dazu zu **Infrastruktur > 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 NetScaler 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 NetScaler ADM heruntergeladen. Während einer Konfigurationsüberprüfung werden ns.conf-Dateien heruntergeladen und im Dateisystem gespeichert. Alle Informationen, die von verwalteten NetScaler-Instanzen erfasst werden, werden intern in der Datenbank gespeichert.

Verschiedene Arten der Abfrage von Instanzen

Im Folgenden sind die verschiedenen Abfragemethoden aufgeführt, die NetScaler ADM auf den verwalteten Instanzen durchführt:

- Globale Abfrage von Instanzen
- Manuelles Abrufen von Instanzen
- Manuelles Abrufen von Entitäten

Globale Abfrage von Instanzen

NetScaler ADM fragt automatisch alle verwalteten Instanzen im Netzwerk ab, abhängig vom von dem von Ihnen konfigurierten Intervall. Obwohl das standardmäßige Abrufintervall 30 Minuten beträgt, können Sie das Intervall je nach Ihren Anforderungen festlegen, indem Sie zu **Infrastruktur > Netzwerkfunktionen** > **Einstellungen**navigieren.

Manuelles Abrufen von Instanzen

Wenn NetScaler ADM viele Entitäten verwaltet, dauert der Abfragezyklus länger, um den Bericht zu generieren, was zu einem leeren Bildschirm führen kann, oder das System zeigt möglicherweise immer noch frühere Daten an.

In NetScaler ADM gibt es ein Mindestabfrageintervall, in dem keine automatische Abfrage stattfindet. Wenn Sie eine neue NetScaler-Instanz hinzufügen oder eine Entität aktualisiert wird, erkennt NetScaler 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 virtueller IP-Adressen für weitere Operationen zu erhalten. Sie müssen warten, bis der minimale Abrufintervall abgelaufen ist. Sie können zwar eine manuelle Abfrage durchführen, um neu hinzugefügte Instanzen zu ermitteln, dies führt jedoch dazu, dass das gesamte NetScaler-Netzwerk abgefragt wird, was zu einer starken Belastung des Netzwerks führt. Anstatt das gesamte Netzwerk abzufragen NetScaler ADM Sie jetzt nur ausgewählte Instanzen und Entitäten zu einem bestimmten Zeitpunkt abfragen.

NetScaler ADM fragt verwaltete Instanzen automatisch ab, um Informationen zu festgelegten Zeiten an einem Tag zu sammeln. Ausgewählte Abfragen reduzieren die Aktualisierungszeit, die NetScaler ADM benötigt, um den neuesten Status der an diese ausgewählten Instanzen gebundenen Entitäten anzuzeigen.

So fragen Sie bestimmte Instanzen in NetScaler ADM ab:

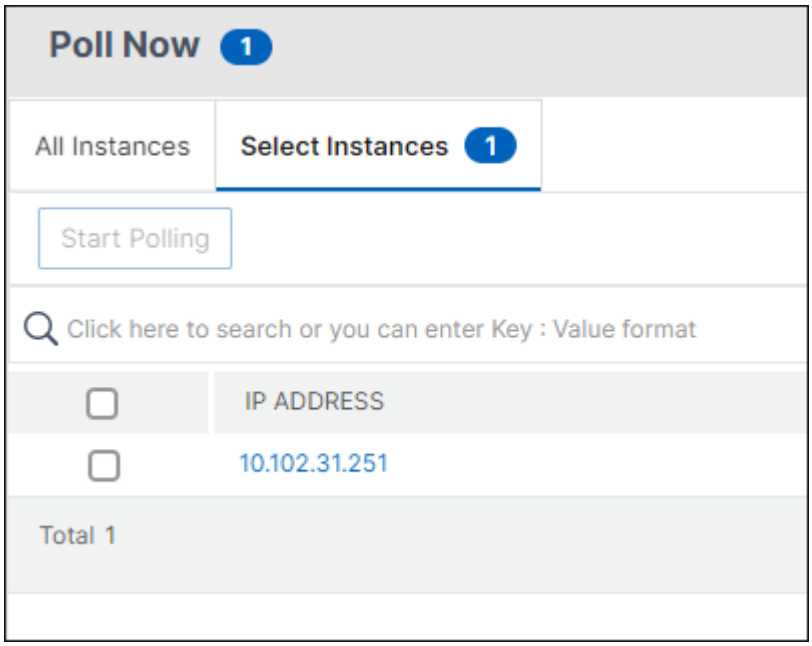
1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Netzwerkfunktionen**.
2. Klicken Sie auf der Seite **Netzwerkfunktionen** oben rechts auf **Jetzt abfragen**.

3. Auf der **Popupseite Jetzt** abfragen können Sie alle NetScaler-Instanzen im Netzwerk abfragen oder die ausgewählten Instanzen abfragen.

    a) Registerkarte**Alle Instanzen** —Klicken Sie auf **Abfrage starten**, um alle Instanzen abzufragen.

    b) Registerkarte "**Instanzen auswählen** "—wählen Sie die Instanzen aus der Liste

4. Klicken Sie auf **Polling starten**.



NetScaler ADM initiiert die manuelle Abfrage und fügt alle Entitäten hinzu.

Manuelles Abrufen von Entitäten

Mit NetScaler ADM können Sie auch nur einige ausgewählte Entitäten abfragen, die an eine bestimmte Instanz gebunden sind. Sie können diese Option beispielsweise verwenden, um den neuesten Status einer bestimmten Entität in einer Instanz zu kennen. In einem solchen 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 NetScaler ADM nur diese Entität ab und aktualisiert den Status in der NetScaler ADM-GUI.

Stellen Sie sich ein Beispiel für einen virtuellen Server vor, der DOWN ist. Der Status dieses virtuellen Servers hat sich möglicherweise auf UP geändert, bevor die nächste automatische Abfrage stattfindet. Um den geänderten Status des virtuellen Servers einzusehen, sollten Sie möglicherweise nur diesen virtuellen Server abfragen, sodass der richtige Status sofort auf der GUI angezeigt wird.

Sie können nun die folgenden Entitäten nach jedem Update in ihrem Status abfragen: Dienste, Dienstgruppen, virtuelle Server für den Lastausgleich, virtuelle Server zur Cachereduzierung, virtuelle Con-

tent Switching-Server, virtuelle Authentifizierungsserver, virtuelle VPN-Server, virtuelle GSLB-Server und Anwendungsserver.

> **Hinweis**
>
> Wenn Sie einen virtuellen Server abfragen, wird nur dieser virtuelle Server abgefragt. Die zugehörigen Entitäten wie Dienste, Dienstgruppen und Server werden nicht abgefragt. Wenn Sie alle verknüpften Entitäten abfragen müssen, müssen Sie die Entitäten manuell abfragen, oder Sie müssen die Instanz abfragen.

So fragen Sie bestimmte Entitäten in NetScaler ADM ab:

Diese Aufgabe unterstützt Sie beispielsweise bei der Abfrage von virtuellen Lastausgleichsservern. Ebenso können Sie auch andere Netzwerkfunktions-Entitäten abfragen.

1. Navigieren Sie in NetScaler ADM zu**Infrastruktur > Netzwerkfunktionen > Load Balancing > Virtuelle Server**.
2. Wählen Sie den virtuellen Server aus, der den Status als DOWN anzeigt, und klicken Sie auf **Jetzt abfragen**. Der Status des virtuellen Servers ändert sich jetzt in UP.

Data Governance

February 5, 2024

ADM On-Prem Cloud Connector ermöglicht es Citrix Cloud, Lizenz-, Konfiguration- und Nutzungsdaten zur Einhaltung der Lizenzbestimmungen zu sammeln und den Service zu verwalten, zu messen und zu verbessern. Ab 14.1 8.x oder einer späteren Version können Sie Cloud Connector so konfigurieren, dass eine Verbindung zwischen dem ADM Service und ADM On-Prem hergestellt wird. Durch die Aktivierung von ADM On-Prem Cloud Connector:

- Die obligatorischen Lizenz- und Nutzungsdaten für die Einhaltung der Flexed-Lizenzbestimmungen werden erfasst.
- Sie können die **Security Advisory**-Funktion in ADM On-Prem abrufen. Weitere Informationen finden Sie unter ADM On-Prem Cloud Connector.

Nach der Aktivierung von Cloud Connector ist die Erfassung von Datenmetriken aktiviert.

Datenkategorien

Die folgenden Tabellen enthalten die Parameterdetails, die nach der Aktivierung von Cloud Connector erfasst werden:

Kategorien	Beschreibung	Wofür verwenden wir es?
Bereitstellung und Nutzung von NetScaler Funktionen	Informationen zur Bereitstellung und Nutzung von NetScaler wie Kundenname, Kunden-ID, Gesamtzahl der verwalteten Geräte und Gesamtzahl der aktiven verwalteten Geräte.	Um den Service zu verwalten, zu messen und zu verbessern.
NetScaler ADM-Bereitstellung	Informationen über NetScaler	Um den Service zu verwalten, zu messen und zu verbessern.
Lizenzierung, Berechtigung und Nutzung von NetScaler und NetScaler ADM	Rechte, Lizenzierung	Einhaltung der Lizenzbestimmungen sowie zur Verwaltung, Messung und Verbesserung des Dienstes.

NetScaler und NetScaler ADM —Parameter für Bereitstellung und Funktionsnutzung

Parameter	Beschreibung
onprem_ip	Die IP-Adresse des ADM
t_zehn	Die Gesamtzahl der Mandanten, die mit ADM verbunden sind
bereitstellen	Prüft, ob der ADM-Bereitstellungstyp eigenständig oder HA-Paar ist
ist_dr	Prüft, ob der Disaster Recovery-Knoten konfiguriert ist oder nicht
ist_agt	Prüft, ob der ADM-On-Prem-Agent konfiguriert ist oder nicht
ist_cloud	Überprüft, ob es sich bei der ADM-Bereitstellung um einen ADM Service oder um ADM-On-Prem handelt
is_cntr	Prüft, ob sich die ADM-Bereitstellung im Kubernetes-Cluster befindet
platform	Die Plattform, auf der das ADM gehostet wird. Zum Beispiel Citrix Hypervisor
Gesamtzahl der Benutzer	Die Gesamtzahl der lokalen ADM-Benutzer

Parameter	Beschreibung
Gesamtzahl der GUI-Anfragen	Gesamtzahl der Benutzer, die sich in den letzten 24 Stunden bei der ADM-GUI angemeldet haben
Gesamtzahl der API-Anfragen	Die Gesamtzahl der Anfragen über die API an ADM in den letzten 24 Stunden. Dazu gehören auch Remote-Proxybenutzer (Anfragen vom Agenten).
total_api_externale_Anfragen	Die Gesamtzahl der Anfragen über die API an ADM, die die Anfragen des Agenten ausschließen
Gesamtzahl der benutzerdefinierten Apps	Die Gesamtzahl der benutzerdefinierten Anwendungen in ADM
insgesamt verwaltete_Apps	Die Gesamtzahl der verwalteten Anwendungen in ADM
Apps insgesamt	Die Gesamtheit der Anwendungen in ADM
Benutzerdefinierte_Websites insgesamt	Die Gesamtzahl der in ADM konfigurierten benutzerdefinierten Websites
insgesamt verwaltete_Geräte	Die Gesamtzahl der verwalteten NetScaler-Instanzen in ADM
Gesamtzahl der aktiven_verwalteten_Geräte	Die Gesamtzahl der NetScaler-Instanzen, die sich im UP-Status befinden
total_ns_device	Die Gesamtzahl der verwalteten MPX-Instanzen in ADM
total_ngvpx_device	Die Gesamtzahl der verwalteten Gateway VPX-Instanzen in ADM
total_nswg_device	Die Gesamtzahl der verwalteten Web Gateway-Instanzen in ADM
total_nswgvpx_device	Die Gesamtzahl der verwalteten Web Gateway VPX-Instanzen in ADM
total_nsvpx_device	Die Gesamtzahl der verwalteten VPX-Instanzen in ADM
total_cpx_device	Die Gesamtzahl der verwalteten CPX-Instanzen in ADM
total_nsap_device	Die Gesamtzahl der Admin-Partitionsinstanzen in ADM
total_nssdx_device	Die Gesamtzahl der verwalteten SDX-Instanzen in ADM
Gesamtzahl der Agenten	Die Gesamtzahl der konfigurierten ADM-On-Prem-Agenten

Parameter	Beschreibung
Gesamtzahl der aktiven Agenten	Die Gesamtzahl der lokalen ADM-Agenten, die sich im Status UP befinden
total_custom_event_rules	Die Gesamtzahl der in ADM erstellten benutzerdefinierten Ereignisregeln
totale_event_rules	Die Gesamtzahl der in ADM erstellten Eventregeln
total_stylebook_config_store_count	Die Gesamtzahl der in ADM erstellten Konfigurationspakete
total_user_sb_stylebook_count	Die Gesamtzahl der in ADM erstellten benutzerdefinierten Konfigurationspakete
WAF-Geräte insgesamt	Die Gesamtzahl der NetScaler-Instanzen, für die WAF-Verstöße aktiviert wurden
total_gw_devices	Die Gesamtzahl der NetScaler-Instanzen, die mit SSL VPN aktiviert sind
total_icaproxy_geräte	Die Gesamtzahl der NetScaler-Instanzen, die mit HDX Insight in ADM aktiviert wurden
Total_Bot-Geräte	Die Gesamtzahl der NetScaler-Instanzen, für die Bot-Verstöße aktiviert wurden
Gesamtzahl der gepoolten Geräte	Die Gesamtzahl der NetScaler-Instanzen (sowohl verwaltet als auch nicht verwaltet) mit gepoolten Lizenzen
total_config_audit	Die gesamte in ADM konfigurierte Config Audit-Vorlage
total_config_job	Die Gesamtzahl der in ADM erstellten Config-Jobs
total_ssl_certs	Die gesamte SSL-Zertifizierung, die aus ADM erstellt/geändert/gelöscht wurde
total_network_report	Der gesamte Netzwerkbericht, der in ADM erstellt wurde
insgesamt_k8s	Das NetScaler ADM wird auf dem Kubernetes-Cluster gehostet. Die gesamten Kubernetes-Cluster.
total_ipam	Die Gesamtzahl der in ADM hinzugefügten IPAM-Anbieter
total_rbac_groups	Die Gesamtzahl der in ADM konfigurierten RBAC-Gruppen
total_ingress_deployed	Die Gesamtzahl der Ingress-Controller in Kubernetes.

Parameter	Beschreibung
total_ipam_configured	Die Gesamtzahl der in ADM hinzugefügten IPAM-Netzwerke
Total_Webtransaktionsanalyse_	Die Gesamtzahl der NetScaler-Instanzen, für die Web-Transaktionsanalyse aktiviert wurde
total_pager_duty_profile	Die Gesamtzahl der in ADM hinzugefügten PagerDuty-Profile
total_slack_profile	Die Gesamtzahl der in ADM hinzugefügten Slack-Profile
total_api_discovery	Die Gesamtzahl der NetScaler-Instanzen, die API-Anfragen erhalten
total_lb_devices	Die Gesamtzahl der NetScaler-Instanzen, die mit virtuellen Lastenausgleichsservern konfiguriert sind
total_lb_devices_http	Die Gesamtzahl der NetScaler-Instanzen, die mit Lastenausgleich für virtuelle HTTP-Server konfiguriert sind
total_lb_devices_ssl	Die Gesamtzahl der NetScaler-Instanzen, die mit Load Balancing für virtuelle SSL-Server konfiguriert sind
total_cs_devices	Die Gesamtzahl der NetScaler-Instanzen, die mit virtuellen Content Switching Switching-Servern konfiguriert sind
total_gslb_geräte	Die Gesamtzahl der NetScaler-Instanzen, die mit virtuellen Servern mit globalem Serverlastenausgleich konfiguriert sind
insgesamte_aaa_geräte	Die Gesamtzahl der NetScaler-Instanzen, die mit virtuellen AAA-Servern konfiguriert sind
t_radius_svr	Die gesamten in ADM konfigurierten RADIUS-Authentifizierungsserver
t_ldap_svr	Die Gesamtzahl der in ADM konfigurierten LDAP-Authentifizierungsserver
t_tacacs_svr	Die Gesamtzahl der in ADM konfigurierten TACACS-Authentifizierungsserver
Agenten-ID	Die eindeutige ID des eingesetzten Agenten
platform	Die Plattform, auf der der Agent gehostet wird. Zum Beispiel Citrix Hypervisor

Parameter	Beschreibung
version	Die ADM-Agent-Version
Stadt	Die Stadt, in der der ADM-Agent eingesetzt wird
Land	Das Land, in dem der ADM-Agent eingesetzt wird
Region	Die Region, in der der ADM-Agent eingesetzt wird
Geräte-ID	Die eindeutige ID der VPX-Instanz
version	Die Build-Version der VPX-Instanz
Bundesstaat	Der aktuelle Status (UP oder Down) der VPX-Instanz
Geräte_Plattform	Die Plattform, auf der die VPX-Instanz gehostet wird
Wurzel	Die Details zur ADM-Festplattennutzung in den Verzeichnissen /var, /root, /flash, /var/mps
gesamt	Der gesamte ADM-Festplattenspeicher (Einheit: Byte)
gebraucht	Der insgesamt genutzte ADM-Festplattenspeicher
frei	Der gesamte verfügbare ADM-Festplattenspeicher
ADM_AnalT_Dx —Funktion	Der Analysetyp (Bot, WAF, Web Insight, Service Graph usw.), für den die Probleme identifiziert wurden.
ADM_AnalT_DX —Problemtyp	Die Problemkategorie, zu der das identifizierte Problem gehört. Zum Beispiel Lizenzierung, Konfiguration

Parameter	Beschreibung
ADM_AnalT_DX —Unterausgabetyp	Die Unterproblemkategorie für das identifizierte Problem. Das Unterproblem kann NO_VIPS_LICENSED, BOT_INSIGHT_IN_ACTION_DISABLED, NS_FEATURE_DISABLED, VSERVER_WITHOUT_BOT_POLICY_BINDING, NO_COLLECTORS_PRESENT, APPFLOWPARAM_DISABLED, ICA_APPFLOW_POLICY_BINDING, VSERVER_WITHOUT_APPFIREWALL_POLICY_BINDING, SECURITY_INSIGHT_IN_ACTION_DISABLED, NO_CPX_VIPS_SEIN PRÄSENT, COLLECTOR_UNBOUND_IN_VSERVER, VSERVER_WITHOUT_APPFLOW_POLICY_BINDING
Feature	Die Analysefunktion, die auf den virtuellen Servern mit Lastausgleich/Content Switching aktiviert ist
total_lbvserver_ft_aktiviert	Die gesamten virtuellen Lastausgleichsserver, auf denen mindestens eine Analysefunktion aktiviert ist
total_csvserver_ft_enabled	Die Gesamtzahl der virtuellen Content-Switching-Server, auf denen mindestens eine Analysefunktion aktiviert ist
Funktion_aktiviert_on_vpn	Die Analysefunktion, die auf den virtuellen VPN-Servern aktiviert ist
total_vpnvserver_ft_aktiviert	Die Gesamtzahl der virtuellen VPN-Server, auf denen mindestens eine Analysefunktion aktiviert ist

Lizenzierungs-, Berechtigungs- und Nutzungsdatenelemente für NetScaler und NetScaler ADM

Parameter	Beschreibung
pool_instances_entitled	Die Gesamtzahl der berechtigten Pool-Instances
Verwendete Poolinstanzen	Die Gesamtzahl der verwendeten gepoolten Instances

Parameter	Beschreibung
pool_fips_instances_entitled	Die Gesamtzahl der Pool-FIPS-Instanzen, die berechtigt sind
pool_fips_instances_used	Die Gesamtzahl der verwendeten Pool-FIPS-Instanzen
pool_entvcpu_entitled	Der gesamte Pool der Enterprise-vCPUs mit dem Titel
pool_entvcpu_gebraucht	Der gesamte verwendete Pool der verwendeten Enterprise-vCPUs
pool_entbw_berechtigt	Die gesamte verfügbare Enterprise-Pool-Bandbreite [Mbit/s]
pool_entbw_gebraucht	Die gesamte genutzte Pool-Bandbreite des Enterprise-Netzwerks [Mbit/s]
pool_pltbw_entitled	Die gesamte zulässige Platin-Bandbreite des Pools [Mbit/s]
pool_pltbw_gebraucht	Die gesamte verwendete Platin-Bandbreite des Pools [MBps]
pool_pltvcpu_entitled	Der gesamte Pool an Platinum-vCPUs mit Anspruch
pool_pltvcpu_gebraucht	Der gesamte verwendete Pool Platinum-vCPUs
pool_stdbw_entitled	Die gesamte Pool-Standardbandbreite, auf die Anspruch besteht
pool_stdbw_gebraucht	Die gesamte verwendete Pool-Standardbandbreite
pool_stdvcpu_entitled	Der gesamte Pool mit Anspruch auf Standard-vCPUs
pool_stdvcpu_gebraucht	Der gesamte Pool verwendeter Standard-vCPUs
pool_cpxvcpu_entitled	Der gesamte Pool berechtigter CPX-vCPUs
pool_cpxvcpu_gebraucht	Der gesamte Pool der verwendeten CPX-vCPUs
pool_perc_instances_used	Der Prozentsatz der verwendeten Instanzen
pool_perc_vcpu_gebraucht	Der Prozentsatz der verwendeten vCPUs
pool_perc_bw_gebraucht	% der verwendeten Bandbreite
total_entitled_vservers	Die Gesamtzahl der berechtigten virtuellen Server
total_used_vservers	Die Gesamtzahl der verwendeten virtuellen Server

Parameter	Beschreibung
total_discovered_vservers	Die Gesamtzahl der erkannten virtuellen Server
perc_used_servers	Der Prozentsatz der verwendeten/berechtigten virtuellen Server
perc_discovered_vservers	Der Prozentsatz der erkannten/berechtigten virtuellen Server
is_local_license	Prüft, ob die Lizenz in NetScaler ADM gehostet wird
Lizenz-Edition	Der Lizenztyp (Platinum/Standard/Enterprise)
is_pooled_license	Prüft, ob es sich bei der Lizenz um eine gepoolte Lizenz handelt
Modell-ID	Die Modell-ID der Instanz
plt_license_allocation	Die Platin-Lizenzzuteilung
ent_license_allocation	Die Zuteilung von Unternehmenslizenzen
std_license_allocation	Die Standard-Lizenzzuweisung
Enddatum der Lizenz	Gesamtzahl der Tage, an denen die Lizenz abläuft
platform	Der Gerätetyp
instanz_id	Die eindeutige Kennung der Instanz
instanzenmodus	Prüft, ob es sich bei der Instanz um ein eigenständiges oder ein HA-Paar handelt
instanz_status	Der Instanzstatus (Hoch/Heruntergefahren)
flex_vpx_inst_entitled	Die Gesamtzahl der berechtigten VPX-Instanzen
flex_vpx_inst_allocated	Die Gesamtzahl der zugewiesenen VPX-Instanzen
flex_sdx_inst_entitled	Die Gesamtzahl der berechtigten SDX-Instanzen
flex_sdx_inst_allocated	Die Gesamtzahl der zugewiesenen SDX-Instanzen
flex_mpx_inst_entitled	Die Gesamtzahl der berechtigten MPX-Instanzen
flex_mpx_inst_allocated	Die Gesamtzahl der zugewiesenen MPX-Instanzen
flex_plt_bw_entitled	Die Titan-Bandbreite
flex_plt_bw_allocated	Die zugewiesene Platin-Bandbreite
flex_ent_bw_entitled	Die berechtigte Unternehmensbandbreite
flex_ent_bw_allocated	Die zugewiesene Unternehmensbandbreite

Parameter	Beschreibung
flex_std_bw_entitled	Die betitelte Standardbandbreite
flex_std_bw_allocated	Die zugewiesene Standardbandbreite
flex_vpx_fips_inst_entitled	Die Gesamtzahl der berechtigten FIPS-Instanzen
flex_vpx_fips_inst_allocated	Die Gesamtzahl der zugewiesenen FIPS-Instanzen

Wenn Ihr NetScaler ADM 14.1 4.x oder eine niedrigere Version ist, können Sie eine Kundenidentität in Citrix Cloud erstellen, um wichtige Statistiken über ADM-Zustand, Status und andere Metriken aus der ADM-On-Prem-Bereitstellung an das Citrix Cloud Cloud-Konto zu senden. Citrix sammelt Statistiken, um die Verwendung von NetScaler ADM zu verstehen. Weitere Informationen finden Sie unter Data Governance für Customer Identity.

Lizenzierung

February 5, 2024

NetScaler Application Delivery Management (ADM) erfordert eine verifizierte NetScaler-Lizenz zur Verwaltung und Überwachung der NetScaler-Instanzen, wenn die Instanzen über das Protokoll erkannt werden. `https`

NetScaler ADM unterstützt die folgenden Lizenzeditionen. Wenden Sie sich an Ihren NetScaler-Vertriebsmitarbeiter oder Partner, um eine ADM-Lizenz zu erwerben.

Express Edition —Mit der Express Edition-Lizenz können Sie beliebig viele Instanzen verwalten und überwachen. Standardmäßig wird die Express-Edition-Lizenz angewendet.

Advanced Edition - Ermöglicht die Verwaltung der erkannten Anwendungen und das Anzeigen von Analysen für die gekauften virtuellen Server zusammen mit den kostenlosen virtuellen Servern.

Zu beachtende Punkte:

- Für Build **13.1-9.x oder früher**können Sie bis zu 30 erkannte Anwendungen oder virtuelle Server verwalten und Analysen anzeigen. Neben den 30 erkannten Anwendungen oder den 30 virtuellen Servern müssen Sie eine Advanced-Lizenz kaufen und anwenden. Wenn Sie beispielsweise 100 virtuelle Serverlizenzen kaufen, sind Sie berechtigt, bis zu 130 virtuelle Serverlizenzen zu verwenden.
- Für Build **13.1-12.x oder höher**können Sie bis zu zwei erkannte Anwendungen oder virtuelle Server verwalten und Analysen anzeigen. Neben den beiden erkannten Anwendungen oder

den beiden virtuellen Servern müssen Sie eine Advanced-Lizenz kaufen und anwenden. Wenn Sie beispielsweise 100 virtuelle Serverlizenzen kaufen, sind Sie berechtigt, bis zu 102 virtuelle Serverlizenzen zu verwenden.

Nach dem Upgrade auf 13.1-12.x erstellen:

- Alle kostenlosen Standardserver von Express bleiben 30 Tage lang funktionsfähig. Sie können die 2 virtuellen Server auswählen und die 2 Standardlizenzen innerhalb der 30-tägigen Kulanzfrist anwenden. Wenn 30 Tage nach dem Upgrade keine Benutzeraktion durchgeführt wird, wendet ADM die Lizenz nach dem Zufallsprinzip auf 2 virtuelle Server an und lizenziert die verbleibenden virtuellen Server. Sie müssen neue Advanced-Lizenzen kaufen und anwenden, um diese virtuellen Server zu aktivieren.
- Nach dem Upgrade sind die folgenden Änderungen im ADM-Verhalten aufgeführt:
  - ADM setzt eine 30-tägige Nachfrist durch.
  - Innerhalb der 30-tägigen Kulanzfrist ist die Zuweisung neuer virtueller Server für die 30 kostenlosen Express-Server gesperrt.
    - Wenn die Anzahl der verfügbaren virtuellen Serverlizenzen vor dem Upgrade auf 12.x beispielsweise 30 betrug und nur 20 lizenzierte virtuelle Server verwendet wurden, dürfen Sie innerhalb des 30-tägigen Kulanzzeitraums nur die 20 virtuellen Server verwenden und die verbleibenden 10 virtuellen Server nicht lizenzieren.
  - Innerhalb der 30-tägigen Kulanzfrist können Sie als Administrator jedoch weiterhin Advanced ADM-Lizenzen anwenden und neue virtuelle Server zuweisen.

Features	Optionen	Express-Ausgabe	Fortgeschrittene Ausgabe	NetScaler Lizenz
Anwendungen	Anwendungs-Dashboard	Bis zu zwei virtuelle Server.	Berechtigt für alle erworbenen virtuellen Serverlizenzen und zwei zusätzliche virtuelle Server.	Für Informationen zur NetScaler Web App Firewall im App Dashboard ist eine Premium- (oder) Advanced-Lizenz mit App Firewall erforderlich.

Features	Optionen	Express-Ausgabe	Fortgeschrittene Ausgabe	NetScaler Lizenz
		Web Insight	Bis zu zwei virtuelle Server.	Berechtigt für alle erworbenen virtuellen Serverlizenzen und zwei zusätzliche virtuelle Server.
		Service-Diagramm	Bis zu zwei virtuelle Server.	Berechtigt für alle erworbenen virtuellen Serverlizenzen und zwei zusätzliche virtuelle Server.
		Konfiguration > StyleBooks	Unbegrenzt	Unbegrenzt
Sicherheit	Sicherheits-Dashboard	Bis zu zwei virtuelle Server.	Berechtigt für alle erworbenen virtuellen Serverlizenzen und zwei zusätzliche virtuelle Server.	Für Informationen zur NetScaler Web App Firewall im Security Dashboard ist eine Premium- (oder) Advanced-Lizenz mit App Firewall erforderlich.
		Sicherheitsverletzungen	Bis zu zwei virtuelle Server.	Berechtigt für alle erworbenen virtuellen Serverlizenzen und zwei zusätzliche virtuelle Server.

Features	Optionen	Express-Ausgabe	Fortgeschrittene Ausgabe	NetScaler Lizenz
		Benutzer und Endpunkte	Bis zu zwei virtuelle Server.	Berechtigt für alle erworbenen virtuellen Serverlizenzen und zwei zusätzliche virtuelle Server.
Gateway	HDX Insight	Bis zu zwei virtuelle Server.	Berechtigt für alle erworbenen virtuellen Serverlizenzen und zwei zusätzliche virtuelle Server.	Advanced (Reporting < 1 Stunde) Premium (Reporting = Unbegrenzt)
		Gateway Insight	Bis zu zwei virtuelle Server.	Berechtigt für alle erworbenen virtuellen Serverlizenzen und zwei zusätzliche virtuelle Server.
Infrastruktur	Infrastruktur-Analytik	Unbegrenzt	Unbegrenzt	Nicht verfügbar
		Instanzen	Unbegrenzt	Unbegrenzt
		SSL-Dashboard	Unbegrenzt	Unbegrenzt
		Ereignisse	Unbegrenzt	Unbegrenzt
		Netzwerk-Funktionen	Unbegrenzt	Unbegrenzt
		Netzwerkberichterstattung	Unbegrenzt	Unbegrenzt
		Gebündelte Lizenzen	Unbegrenzt	Unbegrenzt

Features	Optionen	Express-Ausgabe	Fortgeschrittene Ausgabe	NetScaler Lizenz
		Konfiguration > Konfigurationsaufträge, Konfigurationsvorlagen und Konfigurationsempfehlungen	Unbegrenzt	Unbegrenzt
		Jobs aktualisieren	Unbegrenzt	Unbegrenzt
		Orchestrierung	Unbegrenzt	Unbegrenzt
		WAN-Einblick	Unbegrenzt	Unbegrenzt
Einstellungen	RBAC & externe Authentifizierung (Instanzebene)	Unbegrenzt	Unbegrenzt	Nicht verfügbar
		RBAC & externe Authentifizierung	Unbegrenzt	Unbegrenzt

*Für die Integration von Citrix Director mit NetScaler ADM-Unterstützung muss Citrix Director über eine Premium-Lizenz verfügen.

Lizenzen für weitere virtuelle Server sind in virtuellen Serverpaketen von 10 verfügbar. Sie können eine gültige Lizenz erhalten und die Lizenzen auf den NetScaler ADM-Servern über die NetScaler ADM-GUI hinzufügen.

Hohe Verfügbarkeit

Der NetScaler ADM Server kann VIP-, CICO- und gepoolte Kapazitätslizenzen enthalten. Wenn die Lizenzen an einen ADM-Server ausgestellt werden, sind die Lizenzen an die Host-ID des Servers gebunden. Die Zuweisung von Lizenzen zu einem anderen ADM-Server ist eingeschränkt.

Wenn Sie ein ADM-Hochverfügbarkeitspaar als Lizenzserver konfigurieren, müssen die primären und sekundären Server dieselben Lizenzdateien haben. Daher unterstützt NetScaler ADM in der Bereitstellung mit hoher Verfügbarkeit von ADM, dass Sie beiden Servern dieselben Lizenzdateien zuweisen.

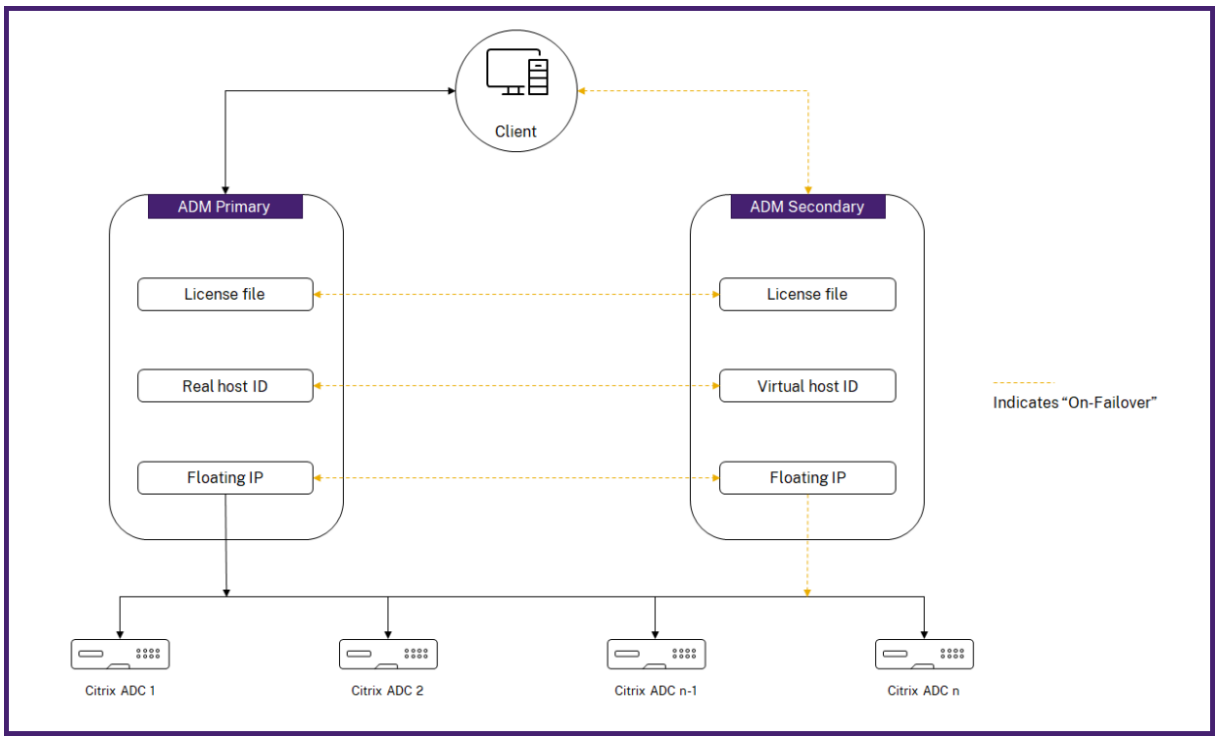
Hinweis

- Wenn Sie NetScaler ADM 12.1.49.x oder frühere Versionen installiert haben, erhalten Sie eine Übergangsfrist von 30 Tagen, um die Lizenzierung auf dem sekundären Knoten aufrechtzuerhalten. Nach Ablauf der Übergangsfrist müssen Sie sich an Citrix wenden, um die ursprüngliche Lizenz erneut zu hosten.
- Bei Versionen 12.1.50.x oder höher wird die NetScaler ADM-Lizenz automatisch mit dem sekundären Knoten synchronisiert.
- Die gepoolten Lizenzen werden ab Version 12.1.50.x oder höher automatisch mit dem sekundären Knoten synchronisiert.

Wie werden Lizenzen zwischen ADM-Hochverfügbarkeitsknoten synchronisiert?

Immer wenn ein Failover auftritt, übernimmt der sekundäre Server die Rolle des Primärservers. Die echte Host-ID des primären Servers wird als virtuelle Host-ID des neuen Primärservers konfiguriert. Die Lizenzdateien erkennen den neuen Primärserver anhand der virtuellen Host-ID.

- **Real Host ID** - Diese ID wird aus einer MAC-Adresse des ADM-Servers generiert. Jede eigenständige ADM-Bereitstellung verfügt über eine eindeutige Host-ID.
- **Virtuelle Host-ID** - Diese ID wird während der HA-Bereitstellung automatisch generiert. Die tatsächliche Host-ID eines ADM-Primärservers wird als virtuelle Host-ID eines sekundären Servers verwendet. Diese ID wird in der ADM-Datenbank in einem verschlüsselten Format gespeichert und Änderungen an dieser ID sind eingeschränkt. Die virtuelle Host-ID wird gegenüber der echten Host-ID bevorzugt.



Angenommen, Node-1 ist der primäre Server und Node-2 ist der sekundäre Server. Die virtuelle Host-ID von Node-1 ist mit Node-2 synchronisiert.

1. In Node-1 verfügbare Lizenzdateien werden mit Node-2 synchronisiert.
2. Alle neuen Lizenzdateien auf Node-1 werden regelmäßig mit Node-2 synchronisiert.
3. ADM stellt sicher, dass der Lizenzserver nur auf Node-1 ausgeführt wird, um eine Verdoppelung der Lizenzkapazität zu vermeiden.
4. NetScaler-Instanzen checken Lizenzen von Node-1 unter Verwendung der Floating-IP-Adresse aus.

Die Lizenzen sind an ADC-Instanzen gebunden. Um Lizenzen von einem NetScaler ADM HA auszuchecken, benötigen Instanzen die IP-Adresse der jeweiligen Appliance. Wenn Sie Lizenzen auf einem Primärserver anwenden, der für die Lizenzierung zuständig ist und er alle zukünftigen Lizenzen auf dieser Instanz anwendet. Sie können Lizenzen nur von dem Server löschen, auf dem Sie die Lizenzen installiert haben.

Orchestrierung

Das Orchestration-Modul ist unabhängig von der Lizenzierung und immer verfügbar.

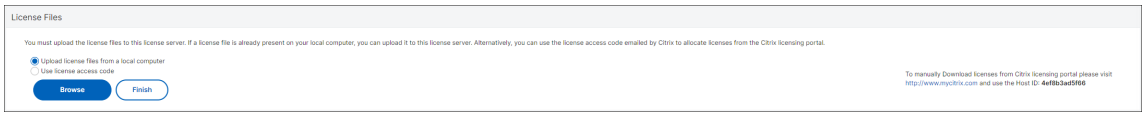
Aktualisieren Sie die virtuellen Serverlizenzen

Sie können die Lizenzierung auf NetScaler ADM aktualisieren, um mehr virtuelle Server zu überwachen und zu verwalten, die auf den NetScaler Appliances gehostet werden.

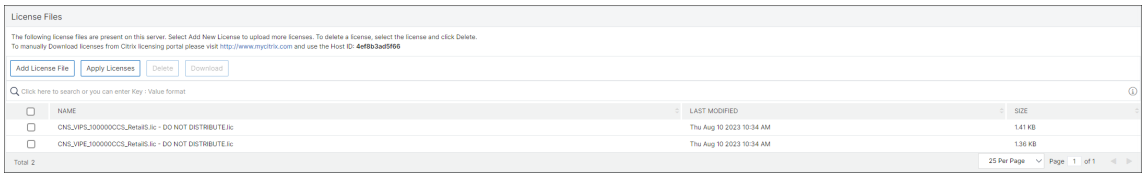
So aktualisieren Sie Ihre Appliance-Lizenzen:

1. Melden Sie sich mit den Administratoranmeldeinformationen bei NetScaler ADM an.
2. Navigieren Sie zu**Infrastruktur > Gepoolte Lizenzierung**.
3. Gehen Sie zu **Lizenzdateien**und wählen Sie eine der folgenden Optionen aus:
   - **Laden Sie Lizenzdateien von einem lokalen Computer**hoch. Wenn auf Ihrem lokalen Computer bereits eine Lizenz vorhanden ist, klicken Sie auf **Durchsuchen** und wählen Sie die Lizenzdatei (.lic) aus, die Sie für die Zuweisung Ihrer Lizenzen verwenden möchten. Klicken Sie auf **Fertig stellen**.
   - **Verwenden Sie den Lizenzaktivierungscode**. Citrix sendet den Lizenzzugangscode für die Lizenz, die Sie gekauft haben, per E-Mail. Geben Sie den Lizenzzugriffscode in das Textfeld ein und klicken Sie dann auf **Lizenzen abrufen**.

   > **Hinweis**
   >
   > Wenn Sie diese Option auswählen, muss NetScaler ADM mit dem Internet verbunden sein, oder es muss ein Proxyserver verfügbar sein.



4. Auf der Seite Lizenzeinstellungen können Sie jederzeit weitere Lizenzen hinzufügen.



Verifizierung

Sie können die auf Ihrem NetScaler ADM installierten Lizenzen überprüfen, indem Sie zu **Einstellungen> Lizenzierung und Analytics-Konfiguration**navigieren.

Virtuelle Server verwalten

Sie können die virtuellen Server oder virtuellen Server von Drittanbietern auswählen, die Sie über NetScaler ADM verwalten und überwachen möchten.

> **Wichtige Hinweise**
>
> - Standardmäßig lizenziert NetScaler ADM die virtuellen Server nach jedem virtuellen Serverabfragungszyklus automatisch nach dem Zufallsprinzip.
> - Wenn die Gesamtzahl der in Ihrem NetScaler ADM erkannten virtuellen Server niedriger ist als die Anzahl der installierten virtuellen Serverlizenzen, lizenziert NetScaler ADM standardmäßig alle virtuellen Server.

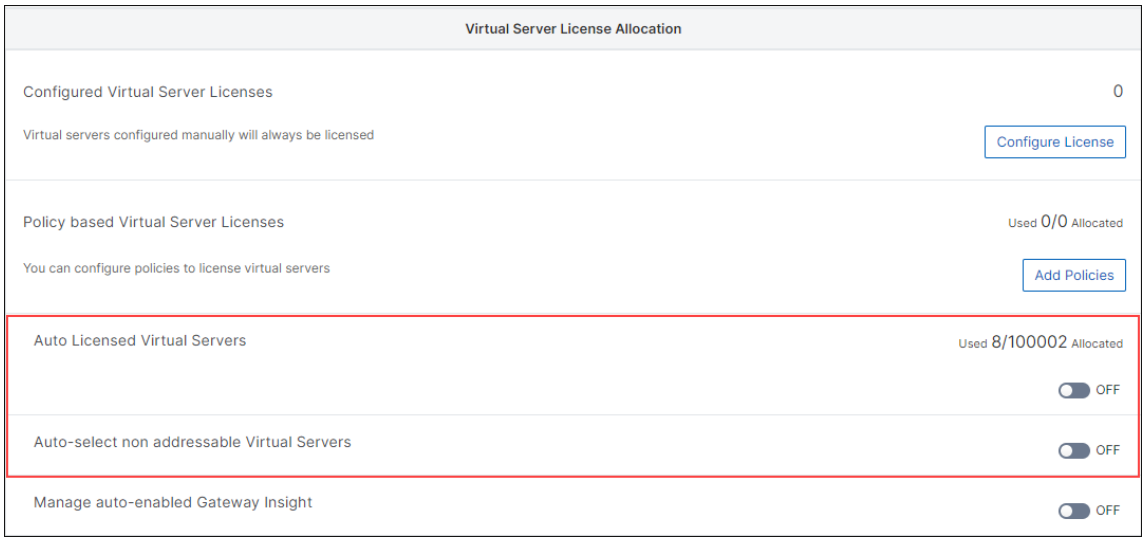
Um die virtuellen Server manuell auszuwählen oder die Lizenzierung auf eingeschränkte virtuelle Server zu beschränken, müssen Sie zuerst die automatische Lizenzierung der virtuellen Server deaktivieren und dann die virtuellen Server auswählen, die Sie verwalten möchten.

Deaktivieren der automatischen Lizenzierung virtueller Server

1. Navigieren Sie zu **Einstellungen > Lizenz- und Analytics-Konfiguration**.

   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 **Lizenzzuweisung für virtuelle Server** die Option **Automatisch lizenzierte virtuelle Server** und wählen Sie **Nicht adressierbare virtuelle Server automatisch auswählen**.

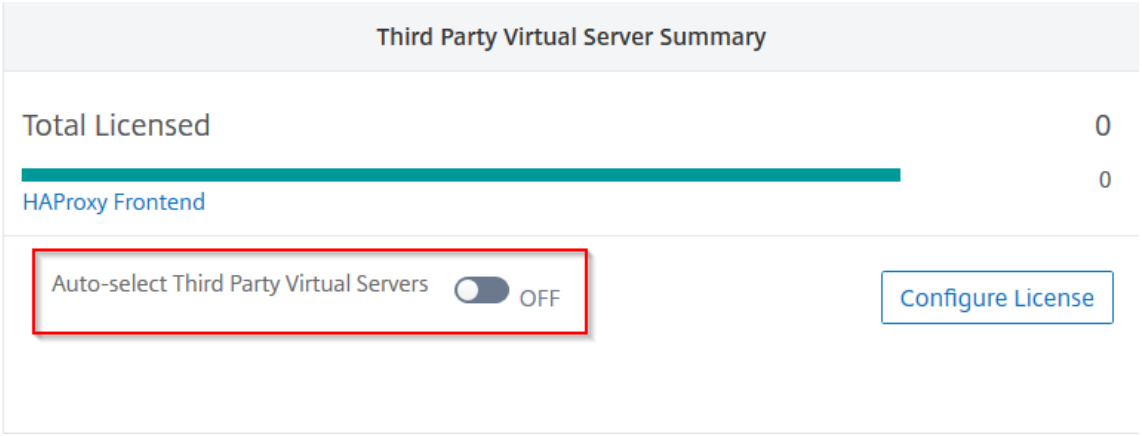


Virtuelle Server von Drittanbietern zur Lizenzierung auswählen

1. Navigieren Sie zu **Einstellungen > Lizenz- und Analytics-Konfiguration**.

   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 **Übersicht über virtuelle Server**von **Drittanbietern die automatische Auswahl virtueller Server von Drittanbietern**.



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**.

Richtlinienbasierte Lizenzierung für virtuelle Server konfigurieren

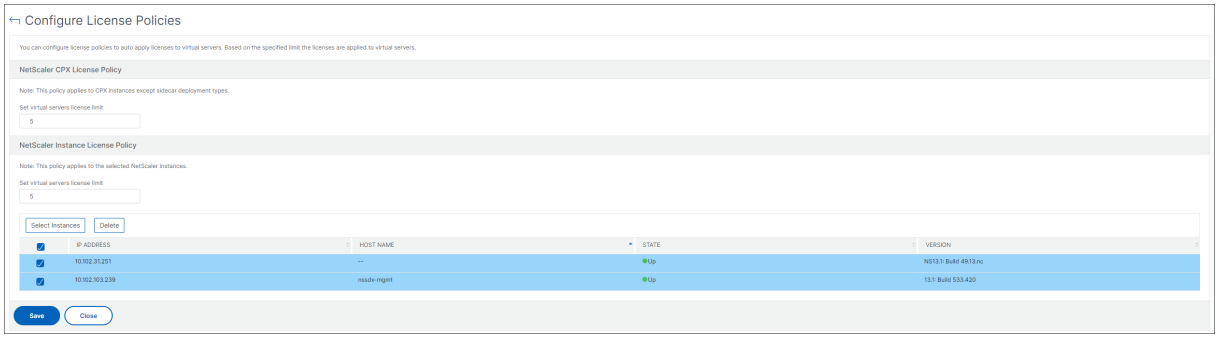
Sie können eine Richtlinie konfigurieren, um die Lizenz auf virtuelle Server anzuwenden. Diese Richtlinie steuert die Anzahl der virtuellen Server, die Sie automatisch lizenzieren möchten. Außerdem werden Lizenzen nur auf die virtuellen Server ausgewählter Instanzen angewendet.

Klicken Sie auf **Richtlinien bearbeiten**, und Sie können Folgendes angeben:

- Legen Sie das Limit virtueller Server für CPX-Instanzen separat fest, um Lizenzen anzuwenden. Der ADM wendet Lizenzen für virtuelle Server auf CPX-Instanzen bis zu einem bestimmten Limit an.

> **Wichtig**
>
> Dieses Limit gilt für CPX-Instanzen mit Ausnahme der Bereitstellungstypen von Sidecar.
>
> Um CPX-Instanzen von Sidecar-Bereitstellungstypen anzuzeigen, filtern Sie die virtuellen Server mithilfe der Eigenschaft: `License Type: Freely Managed`.

- Legen Sie das Limit für virtuelle Server auf ausgewählten ADC-Instanzen (MPX/VPX/BLX) fest, um Lizenzen anzuwenden. Der ADM wendet Lizenzen auf virtuelle Server auf ADC-Instanzen bis zu einem bestimmten Limit an.
- Wählen Sie die vorrangigen ADC-Instanzen für die Anwendung virtueller Serverlizenzen Daher kann der ADM die Lizenz nur auf die virtuellen Server ausgewählter Instanzen anwenden.



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 anzeigen.

1. Navigieren Sie zu **Einstellungen > Lizenz- und Analytics-Konfiguration**.
2. Klicken Sie in der **Lizenzübersicht für virtuelle Server im Abschnitt**Gesamtlizenzierung**auf den virtuellen Servertyp**.

Konfigurieren der automatischen Lizenzunterstützung für nicht adressierbare virtuelle Server

NetScaler ADM wendet standardmäßig nicht automatisch Lizenzen auf nicht adressierbare virtuelle Server an. Für die Lizenzierung nicht adressierbarer virtueller Server müssen Sie die automatische Lizenzierungsoption deaktivieren und die nicht adressierbaren virtuellen Server manuell auswählen. Dies erhöht Ihren Aufwand, die nicht adressierbaren Server zunächst manuell auszuwählen, wenn Sie die Lizenzen anwenden. Sie müssen auch die neuen nicht adressierbaren virtuellen Server manuell auswählen, wenn sie Ihrem Netzwerk hinzugefügt werden.

NetScaler ADM bietet eine Option in NetScaler ADM unter **Virtual Server License Allocation**. Wenn Sie die Option **Nicht adressierbare virtuelle Server automatisch auswählen** aktivieren, wenden Sie automatisch Lizenzen für nicht adressierbare virtuelle Server an.

> **Hinweis**
>
> - NetScaler ADM wählt standardmäßig immer 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.

Ablaufprüfungen für virtuelle Serverlizenzen

Sie können nun den Status von Warnungen für den Ablauf der Lizenz für virtuelle Server in NetScaler ADM anzeigen und festlegen.

So zeigen Sie den Status der Lizenzen an:

1. Navigieren Sie zu **Infrastruktur > Gepoolte Lizenzierung > Systemlizenzen.**
2. Im Abschnitt **Informationen zum Lizenzablauf** finden Sie die Details der Lizenzen, die ablaufen werden:
    - **Merkmal:**Art der Lizenz, die abläuft.
    - **Anzahl:** Anzahl der betroffenen virtuellen Server oder Instanzen.
    - **Tage bis zum Ablauf:**Anzahl der verbleibenden Tage bis zum Ablauf.

So konfigurieren Sie die Benachrichtigungseinstellungen für Lizenzen:

1. Navigieren Sie zu **Infrastruktur > Gepoolte Lizenzierung > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungseinstellungen** auf das Stiftsymbol und bearbeiten Sie die Parameter.
    - **E-Mail-Profil:** E-Mail-Profil oder Verteilerliste zum Senden von Benachrichtigungen, wenn Lizenzen den Schwellenwert erreichen oder ablaufen.
    - **SMS (Textnachricht):** SMS-Profil oder Verteilerliste zum Senden von Benachrichtigungen, wenn Lizenzen den Schwellenwert erreichen oder ablaufen.
    - **Slack** - Geben Sie die Details des Slack Profils an.
    - **PagerDuty-Warnungen** - Geben Sie ein PagerDuty-Profil an Basierend auf den in Ihrem PagerDuty-Portal konfigurierten Benachrichtigungseinstellungen wird eine Benachrichtigung gesendet, wenn Ihre Zertifikate bald ablaufen.

- **Benachrichtigen:** Legen Sie den Prozentsatz der gepoolten Lizenzen fest, um Administratoren per E-Mail oder SMS zu benachrichtigen.
- **Schwellenwert für den Lizenzablauf:** Anzahl der Tage, bevor die durch den Alert-Schwellenwert ermittelte Anzahl der Lizenzen abläuft.
- **Ablauf der Lizenzen:** Anzahl der verbleibenden Tage vor Ablauf.

Systemanforderungen

February 5, 2024

Bevor Sie NetScaler ADM installieren, müssen Sie die Softwareanforderungen, Browseranforderungen, Portinformationen, Lizenzinformationen und Einschränkungen verstehen.

Anforderungen für NetScaler ADM

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8 CPUs **Hinweis:**Wir empfehlen die Verwendung der Solid-State-Drive-Technologie (SSD) für NetScaler ADM-Bereitstellungen.
Speicherplatz	Der Standardspeicherplatz beträgt 120 GB. Der tatsächliche Speicherbedarf hängt von der Schätzung der NetScaler ADM-Größe ab. Verwenden Sie den Größenrechner , um die Speicherschätzungen zu berechnen. Wenden Sie sich an Ihren NetScaler-Vertreter, um auf den Größenrechner zuzugreifen. Wenn Ihre NetScaler ADM Speicheranforderung 120 GB überschreitet, müssen Sie einen zusätzlichen Datenträger bereitstellen. Sie können nur einen zusätzlichen Datenträger hinzufügen.

Komponente	Voraussetzung
	Es wird empfohlen, bei der ersten Bereitstellung eine Schätzung des Speicherplatzes vorzunehmen und zusätzliche Festplatten anzuschließen. Weitere Informationen finden Sie unter Bereitstellen eines zusätzlichen Datenträgers in NetScaler ADM.
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s oder 100 Mbit/s

Anforderungen für NetScaler ADM On-Prem Agent

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8 CPUs
Speicherplatz	30 GB
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s

> **Hinweis**
>
> AMD-Prozessor wird unterstützt in:
>
> - **NetScaler ADM 13.1 Build 4.43 oder höher**.
> - **NetScaler ADM Agent 13.1 Build 17.42 oder höher**.

Mindestens erforderliche NetScaler Version für NetScaler ADM Funktionen

> **Wichtig!**
>
> Die NetScaler ADM-Version und der Build müssen Ihrer NetScaler-Version und Ihrem Build entsprechen oder **höher** sein. Wenn Sie beispielsweise NetScaler ADM 12.1 Build 50.39 installiert haben, stellen Sie sicher, dass Sie NetScaler 12.1 Build 50.28/50.31 oder früher installiert haben.

NetScaler ADM-Feature	NetScaler-Softwareversion
StyleBooks	10.5 und höher
OpenStack/CloudStack-Unterstützung	11.0 und höher, falls eine Partition erforderlich ist 11.1 und höher, wenn eine Partition in einem gemeinsam genutzten virtuellen LAN erforderlich ist
NSX-Unterstützung	11.1 Build 47.14 und höher (VPX)
Mesos/Marathon-Unterstützung	10.5 und höher
Backups/Wiederherstellung	Für NetScaler 10.1 und höher Für NetScaler SDX, 11.0 und höher
Überwachung/Berichterstellung und Konfiguration mit Jobs	10.1 und höher
Analytics-Funktionen	
Web Insight	10.5 und höher
HDX Insight	10.1 und höher
Sicherheitsverletzungen der WAF	11.0.65.31 und höher
Gateway Insight	11.0.65.31 und höher
Cache Insight	10.5 und neuer*
SSL Insight	12.0 und höher

* Integrierte Cache-Metriken werden in NetScaler ADM mit NetScaler-Instanzen, auf denen Version 11.0 Build 66.x ausgeführt wird, nicht unterstützt.

Anforderungen für NetScaler ADM Analytics

Mindestversionen von Citrix Virtual Apps and Desktops, die für NetScaler ADM-Funktionen erforderlich sind

NetScaler ADM-Feature	Citrix Virtual Apps and Desktops Version
HDX Insight	Citrix Virtual Apps and Desktops 7.0 und höher

> **Hinweis**
>
> Das NetScaler Gateway-Feature (als Access Gateway Enterprise für die Versionen 9.3 und 10.x bezeichnet) muss auf der NetScaler-Instanz verfügbar sein. NetScaler ADM unterstützt keine eigenständigen Access Gateway Standard-Appliances.

NetScaler ADM kann Berichte für Anwendungen generieren, die auf Citrix Virtual Apps oder Citrix Virtual Desktops veröffentlicht sind und auf die über Citrix Workspace zugegriffen wird. Diese Funktion hängt jedoch vom Betriebssystem ab, auf dem Workspace installiert ist. Derzeit analysiert ein NetScaler den ICA-Datenverkehr nicht für Anwendungen oder Desktops, auf die über Citrix Workspace unter iOS- oder Android-Betriebssystemen zugegriffen wird.

Für HDX Insight unterstützte Thin Clients

- Dell Wyse Windows basierte Thin Clients
- Dell Wyse Linux-basierte Thin Clients
- Dell Wyse ThinOS-basierte Thin Clients
- 10ZiG Ubuntu-basierte Thin Clients
- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

NetScaler-Instanzlizenz für HDX Insight erforderlich

Die von NetScaler ADM for HDX Insight erfassten Daten hängen von der Version und den Lizenzen der überwachten NetScaler-Instanzen ab. HDX Insight-Berichte werden nur für NetScaler Premium- und Advanced-Appliances mit Version 10.5 und höher angezeigt.

NetScaler-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 Hypervisoren

In der folgenden Tabelle sind die von NetScaler ADM unterstützten Hypervisoren aufgeführt.

Hypervisor	Versionen
Citrix Hypervisor	7.1 und 7.4
VMware ESX	6,0, 6,5, 6,7 und 7,0
Microsoft Hyper-V	2012 R2 und 2016
Generisches KVM	RHEL 7.4, RHEL 8.0, Ubuntu 16.04 und Ubuntu 18.04

Unterstützte Betriebssysteme und Workspace-Versionen

In der folgenden Tabelle sind die von NetScaler ADM unterstützten Betriebssysteme und die derzeit für jedes System unterstützten Citrix Workspace-Versionen aufgeführt:

Betriebssystem	Workspace-Version
Windows	4.0 Standardausgabe
Linux	13.0.265571 und später
Mac	11.8, Build 238301 und später
HTML5	1.5
Chrome-App	1.5

Unterstützte Browser

In der folgenden Tabelle sind die von NetScaler ADM unterstützten Webbrowser aufgeführt:

Webbrowser	Version
Microsoft Edge	79 und höher
Google Chrome	51 und höher
Safari	10 und höher
Mozilla Firefox	52 und höher

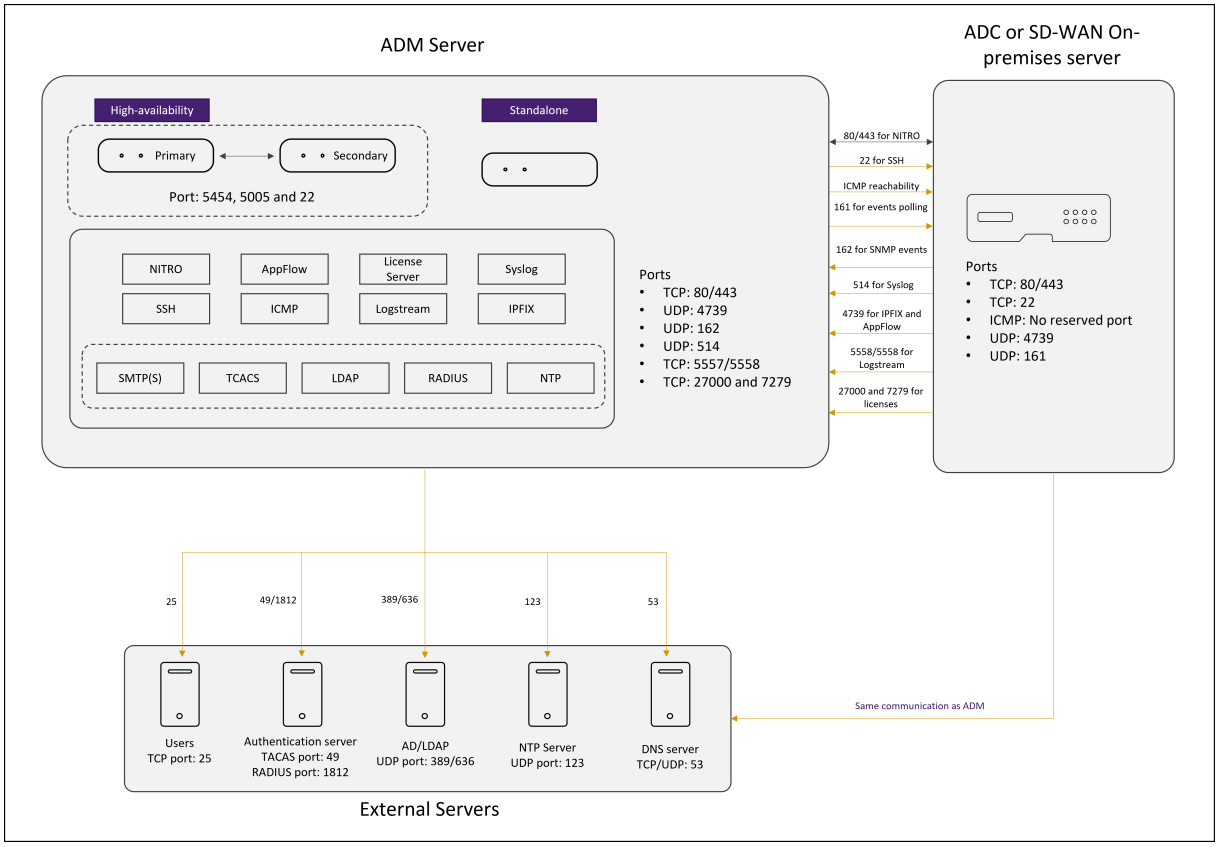
Unterstützte Ports

NetScaler ADM verwendet die NetScaler-IP-Adresse (NSIP), um mit NetScaler zu kommunizieren. Sie können einen Agenten als Vermittler zwischen der ADC-Instanz und ADM verwenden. Um eine Kom-

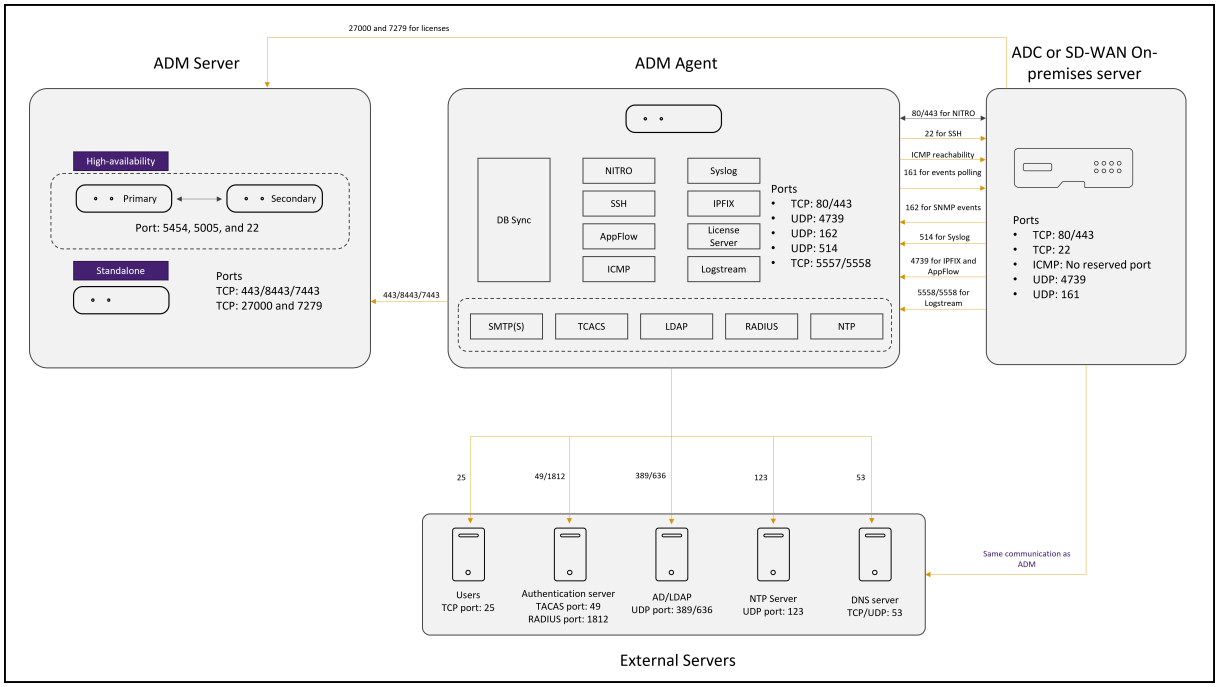
munikation mit diesen Servern herzustellen, öffnen Sie die erforderlichen Ports.

> **Hinweis**
>
> Wenn Sie NetScaler im Hochverfügbarkeitsmodus konfiguriert haben, verwendet NetScaler ADM NSIP, um mit NetScaler zu kommunizieren, und die erforderlichen Ports bleiben dieselben.

Netzwerk-Port-Diagramm für agentlose Bereitstellung:



Netzwerkportdiagramm für die Bereitstellung mit ADM Agent:



Netzwerkportdiagramm für die NetScaler ADM High Availability-Bereitstellung:

Wenn zwei NetScaler ADM Server im Hochverfügbarkeitsmodus eingerichtet sind, gehen Sie beim Hinzufügen einer Instanz wie folgt vor:

- NetScaler ADM kommuniziert mit NetScaler über die primäre IP-Adresse.
- NetScaler stellt die Konnektivität mit NetScaler ADM über die Floating-IP von ADM her. Dies bedeutet, dass NetScaler den gesamten SNMP-, Syslog- und Analytics-Verkehr an die Floating-IP von ADM weiterleitet.

In den folgenden Abschnitten werden die erforderlichen Ports und deren Zweck erläutert:

- ADM-Server
- ADM-Agents
- ADC-Instanz
- Externe Server

Ports für den ADM-Server

In der folgenden Tabelle werden die erforderlichen Ports erläutert, die auf dem ADM-Server geöffnet sein müssen.

Port	Typ	Details	Richtung der Kommunikation
80/443/5454/22	TCP	Standardport für die Kommunikation und Datenbanksynchronisierung zwischen NetScaler ADM Knoten im Hochverfügbarkeitsmodus.	Primärer NetScaler ADM-Knoten zum sekundären NetScaler ADM-Knoten
443/8443/7443	TCP	Port für die Kommunikation zwischen NetScaler ADM Agent und NetScaler ADM.	Der NetScaler ADM-Agent initiiert die Kommunikation mit NetScaler ADM. Anschließend interagieren NetScaler ADM und Agent miteinander.
27000 und 7279	TCP	Lizenzports für die Kommunikation zwischen NetScaler ADM Lizenzserver und ADC-Instanz. Diese Ports werden auch für gepoolte ADC-Lizenzen verwendet.	NetScaler zu NetScaler ADM
5005	UDP	Port zum Austausch von Heartbeats zwischen HA-Knoten.	NetScaler ADM primärer Knoten zum sekundären Knoten. Sekundärer NetScaler ADM-Knoten zum primären Knoten.

Wenn die NetScaler ADM- und NetScaler-Instanzen keinen Agenten für die Kommunikation verwenden, öffnen Sie die folgenden Ports auf dem NetScaler ADM-Server:

Port	Typ	Details	Richtung der Kommunikation
80/443	TCP	Für die NITRO-Kommunikation von NetScaler ADM zur NetScaler-Instanz.	NetScaler ADM Agent an NetScaler und NetScaler an NetScaler ADM Agent
4739	UDP	Für die AppFlow-Kommunikation von der NetScaler-Instanz zu NetScaler ADM.	NetScaler an NetScaler ADM Agent
162	UDP	So empfangen Sie SNMP-Ereignisse von der NetScaler-Instanz an NetScaler ADM.	NetScaler an NetScaler ADM Agent
514	UDP	Um Syslog-Meldungen von der NetScaler-Instanz an NetScaler ADM zu empfangen.	NetScaler an NetScaler ADM Agent
5557/5558	TCP	Für die Logstream-Kommunikation (für WAF-Sicherheitsverletzungen, Web Insight und HDX Insight) von NetScaler zu NetScaler ADM.	NetScaler zu NetScaler ADM
5563	TCP	So empfangen Sie ADC-Metriken (Zähler), Systemereignisse und Audit-Log-Nachrichten von NetScaler-Instanz an NetScaler ADM	NetScaler zu NetScaler ADM

Ports für den ADM Agent

In der folgenden Tabelle werden die erforderlichen Ports erläutert, die auf dem ADM Agent geöffnet sein müssen.

Port	Typ	Details	Richtung der Kommunikation
80/443	TCP	Für die NITRO-Kommunikation von NetScaler ADM zur NetScaler-Instanz.	NetScaler ADM Agent an NetScaler und NetScaler an NetScaler ADM Agent
4739	UDP	Für die AppFlow-Kommunikation von der NetScaler-Instanz zu NetScaler ADM.	NetScaler an NetScaler ADM Agent
162	UDP	So empfangen Sie SNMP-Ereignisse von der NetScaler-Instanz an NetScaler ADM.	NetScaler an NetScaler ADM Agent
514	UDP	Um Syslog-Meldungen von der NetScaler-Instanz an NetScaler ADM zu empfangen.	NetScaler an NetScaler ADM Agent
5557/5558	TCP	Für die Logstream-Kommunikation (für WAF-Sicherheitsverletzungen, Web Insight und HDX Insight) von NetScaler zu NetScaler ADM.	NetScaler zu NetScaler ADM

Ports für ADC-Instanzen

In der folgenden Tabelle werden die erforderlichen Ports erläutert, die auf NetScaler-Instanzen geöffnet sein müssen.

Port	Typ	Details	Richtung der Kommunikation
80/443	TCP	Für die NITRO-Kommunikation von NetScaler ADM zur NetScaler-Instanz. Für die NITRO -Kommunikation zwischen NetScaler ADM-Servern im Hochverfügbarkeitsmodus.	NetScaler ADM an NetScaler und NetScaler an NetScaler ADM
22	TCP	Für die SSH-Kommunikation von NetScaler ADM zur NetScaler-Instanz. Für die Synchronisierung zwischen NetScaler ADM-Servern, die im Hochverfügbarkeitsmodus bereitgestellt werden. Und dieser Port ist für die SSH-Kommunikation zwischen dem ADM-Agent und NetScaler erforderlich.	NetScaler ADM an NetScaler. Oder NetScaler ADM Agent an NetScaler.
Kein reservierter Port	ICMP	Um die Netzwerkerreichbarkeit zwischen NetScaler ADM- und NetScaler-Instanzen oder dem sekundären NetScaler ADM-Server zu erkennen, der im Hochverfügbarkeitsmodus bereitgestellt wird.	NetScaler ADM an NetScaler

Port	Typ	Details	Richtung der Kommunikation
161	UDP	Ereignisse aus ADC-Instanzen abfragen.	NetScaler ADM an NetScaler

Anschlüsse für den integrierten ADC-Agenten

In der folgenden Tabelle werden die erforderlichen Ports erläutert, die für einen integrierten NetScaler-Agenten geöffnet sein müssen.

Port	Typ	Details	Richtung der Kommunikation
443	TCP	Für die gesamte Kommunikation von NetScaler ADM zum integrierten NetScaler-Agenten	Integrierter NetScaler ADM zu NetScaler integrierter Agent und integrierter NetScaler Agent zu NetScaler ADM

> **Hinweis:**
>
> Bei der ADM-Hochverfügbarkeitsbereitstellung verwendet die gesamte Kommunikation von ADM die IP-Adresse des primären Knotens.

Ports für externe Server

In der folgenden Tabelle werden die erforderlichen Ports erläutert, die auf externen Servern geöffnet sein müssen:

Port	Typ	Details	Richtung der Kommunikation
25	TCP	So senden Sie SMTP-Benachrichtigungen von NetScaler ADM an Benutzer.	NetScaler ADM an Benutzer.

Port	Typ	Details	Richtung der Kommunikation
389/636	TCP	Standardport für Authentifizierungsprotokoll. Für die Kommunikation zwischen NetScaler ADM und dem externen LDAP-Authentifizierungsserver.	Externer Authentifizierungsserver von NetScaler ADM zu LDAP
123	UDP	Standard-NTP-Serverport zur Synchronisierung mit mehreren Zeitquellen.	NetScaler ADM zu NTP-Server
1812	RADIUS	Standardport für Authentifizierungsprotokoll. Für die Kommunikation zwischen NetScaler ADM und dem externen RADIUS-Authentifizierungsserver.	NetScaler ADM zu RADIUS externer Authentifizierungsserver
49	TACACS	Standardport für Authentifizierungsprotokoll. Für die Kommunikation zwischen NetScaler ADM und dem externen TACACS Authentifizierungsserver.	Externer Authentifizierungsserver von NetScaler ADM zu TACACS

Einschränkungen

Ab NetScaler ADM 12.1 oder höher unterstützen die folgenden Funktionen das IPv6-Format von IP-Adressen:

1. Verwaltungszugriff für NetScaler ADM GUI
2. Verwaltungszugriff für NetScaler

3. Registrierung und Inventar
4. Netzwerk-Dashboard
5. SSL Dashboard
6. Config-Jobs
7. Prüfung der Konfiguration
8. Netzwerkfunktionen
9. Netzwerkberichterstellung
10. Backup und Wiederherstellung von ADC-Instanzen
11. SNMP-Ereignisse von NetScaler

Die folgenden Funktionen unterstützen IPv6 nicht:

1. Floating-IP mit hoher Verfügbarkeit
2. Syslogs von ADCs erhalten, die IPv6 unterstützen
3. StyleBooks auf ADCs, die IPv6 unterstützen
4. Analytics
5. Zusammengefasste Lizenzierung

Erste Schritte

February 5, 2024

In diesem Dokument erfahren Sie, wie Sie mit der ersten Bereitstellung und Einrichtung von NetScaler Application Delivery Management (ADM) beginnen. Dieses Dokument richtet sich an Netzwerk- und Anwendungsadministratoren, die Citrix-Netzwerkgeräte verwalten (NetScaler und NetScaler Gateway). Folgen Sie den Schritten in diesem Dokument, unabhängig vom dem Gerätetyp, den Sie mit NetScaler ADM verwalten möchten.

Wenn Sie bereits NetScaler ADM verwenden, sollten Sie die Versionshinweise, Systemanforderungen und Lizenzdetails lesen, bevor Sie Ihren Server auf die neueste Version von NetScaler ADM aktualisieren .

Schritt 1 - Überprüfen der Systemanforderungen

Bevor Sie mit der Bereitstellung von NetScaler ADM in Ihrem Rechenzentrum beginnen, überprüfen Sie die Softwareanforderungen, Browseranforderungen, Portinformationen, Lizenzinformationen und Einschränkungen.

- **Informationen zur Lizenz**. Sie können eine beliebige Anzahl von Instanzen und Entitäten ohne Lizenz hinzufügen. Sie können jedoch Analyseinformationen für nur zwei virtuelle Server anzeigen, ohne eine Lizenz zu beantragen. Um Analysen für mehr als zwei virtuelle Server anzuzeigen, müssen Sie die entsprechenden Lizenzen erwerben. Erfahren Sie mehr.
- **Betriebssystem- und Empfängeranforderungen**. Überprüfen Sie diese Informationen, um sicherzustellen, dass Sie die richtige Empfängerversion für die unterstützten Betriebssysteme haben. Erfahren Sie mehr.
- **Anforderungen für den Browser**. Um auf NetScaler ADM GUI zugreifen zu können, müssen Sie sicherstellen, dass Sie über den erforderlichen Browser und die richtige Version verfügen. Erfahren Sie mehr.
- **Ports**. Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind, damit NetScaler ADM mit NetScaler-Instanzen kommunizieren kann. Erfahren Sie mehr.
- **Anforderungen an die NetScaler Instanz**. Verschiedene NetScaler ADM-Funktionen werden in verschiedenen NetScaler-Softwareversionen unterstützt. Überprüfen Sie diese Informationen, um sicherzustellen, dass Sie die NetScaler Instanzen auf die richtige Version aktualisiert haben. Erfahren Sie mehr.

Schritt 2: Bereitstellen von NetScaler ADM

Um die Anwendungen und die Netzwerkinfrastruktur zu verwalten und zu überwachen, müssen Sie zuerst NetScaler ADM auf einem der Hypervisoren installieren. Sie können NetScaler ADM entweder als einzelner Server oder im Hochverfügbarkeitsmodus bereitstellen. Wenn Sie NetScaler Insight Center verwenden, können Sie zu NetScaler ADM migrieren und zusätzlich zu den Analysefunktionen die Funktionen für Verwaltung, Überwachung, Orchestrierung und Anwendungsmanagement nutzen.

- **Bereitstellung auf einem Server**.In einer NetScaler ADM Einzelserverbereitstellung ist die Datenbank in den Server integriert, und ein einzelner Server verarbeitet den gesamten Datenverkehr. Sie können NetScaler ADM mit Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V und Linux KVM bereitstellen. Siehe:
  - NetScaler ADM mit Citrix Hypervisor
  - NetScaler ADM mit Microsoft Hyper-V
  - NetScaler ADM mit VMware ESXi

  - NetScaler ADM mit Linux KVM-Server

- **Bereitstellung mit hoher Verfügbarkeit.** Eine Hochverfügbarkeitsbereitstellung (HA) von zwei NetScaler ADM -Servern ermöglicht einen unterbrechungsfreien Betrieb. In einem Hochverfügbarkeits-Setup müssen beide NetScaler ADM-Knoten im aktiv-Passiv-Modus im selben Subnetz mit derselben Softwareversion und demselben Build bereitgestellt werden und dieselben Konfigurationen aufweisen. Bei der HA-Bereitstellung entfällt durch die Möglichkeit, die Floating-IP auf dem primären NetScaler ADM-Knoten zu konfigurieren, kein separater NetScaler Load Balancer erforderlich.Weitere Informationen finden Sie unter Konfigurieren in einer Hochverfügbarkeitsbereitstellung.

Schritt 3: Hinzufügen von Instanzen zu NetScaler ADM

In NetScaler ADM können Sie alle NetScaler-Instanzen erkennen, verwalten und überwachen, die on-premises oder in der Cloud bereitgestellt werden. Sie müssen dem NetScaler ADM-Server Instanzen hinzufügen, wenn Sie diese Instanzen verwalten und überwachen möchten. Sie können NetScaler ADM folgende Instanzen hinzufügen:

- NetScaler
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
  - NetScaler Gateway

Wenn Sie dem NetScaler ADM-Server eine Instanz hinzufügen, kommuniziert der Server implizit mit den Instanzen und sammelt eine Bestandsaufnahme dieser Instanzen.

Weitere Infos

Schritt 4 —Analytik auf virtuellen Servern aktivieren

Um Analysedaten für den Datenverkehr Ihrer Anwendung anzuzeigen, müssen Sie die Analytics-Funktion auf den virtuellen Servern aktivieren, die Datenverkehr für die jeweiligen Anwendungen empfangen.

Weitere Infos

Schritt 5: Konfigurieren des NTP-Servers auf NetScaler ADM

Sie müssen einen NTP-Server (Network Time Protocol) in NetScaler ADM konfigurieren, um seine Uhr mit dem NTP-Server zu synchronisieren. Durch die Konfiguration eines NTP-Servers wird sichergestellt, dass die NetScaler ADM Uhr dieselben Datums- und Uhrzeiteinstellungen wie die anderen Server im Netzwerk aufweist.

Weitere Infos

Schritt 6 - Konfigurieren von Systemeinstellungen für optimale NetScaler ADM Leistung

Bevor Sie NetScaler ADM zum Verwalten und Überwachen Ihrer Instanzen und Anwendungen verwenden, sollten Sie einige Systemeinstellungen konfigurieren, die eine optimale Leistung Ihres NetScaler ADM-Servers gewährleisten.

- **Konfigurieren von Systemalarmen**. Konfigurieren Sie Systemalarme, um sicherzustellen, dass Sie kritische oder größere Systemprobleme kennen. Sie möchten z. B. benachrichtigt werden, wenn die CPU-Auslastung hoch ist oder wenn mehrere Anmeldefehler auf dem Server auftreten.
- **Konfigurieren Sie Systembenachrichtigungen**. Sie können Benachrichtigungen an ausgewählte Benutzergruppen für verschiedene systembezogene Funktionen senden. Sie können einen Benachrichtigungsserver in NetScaler ADM einrichten und E-Mail- und SMS-Gateway server (Short Message Service) so konfigurieren, dass E-Mail- und Textbenachrichtigungen an Benutzer gesendet werden. Dadurch wird sichergestellt, dass Sie über alle Aktivitäten auf Systemebene wie Benutzeranmeldung oder Systemneustart benachrichtigt werden.
- **Konfigurieren Sie die Einstellungen für den Systemausfall**.Um die Menge der Berichtsdaten zu begrenzen, die in der Datenbank Ihres NetScaler ADM-Servers gespeichert werden, können Sie das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle aufbewahren soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00.00 Uhr) bereinigt.
- **Konfigurieren Sie die Einstellungen für das Systembackup**. NetScaler ADM erstellt ein Backup des Systems automatisch jeden Tag um 00:30 Uhr. Standardmäßig werden drei Backupdateien gespeichert. Möglicherweise möchten Sie eine größere Anzahl von Backups des Systems beibehalten.
- **Konfigurieren Sie die Einstellungen für das Instanzbackup**.Wenn Sie den aktuellen Status einer NetScaler-Instanz sichern, können Sie die Backupdateien verwenden, um die Stabilität wiederherzustellen, falls die Instanz instabil wird. Dies ist besonders wichtig, bevor Sie ein Upgrade durchführen. Standardmäßig wird alle 12 Stunden ein Backup erstellt und drei Sicherungsdateien werden im System aufbewahrt.

- **Konfigurieren Sie die Einstellungen für das Ausschneiden von Instanzereignissen**.Um die Anzahl der Ereignismeldungsdaten zu begrenzen, die in der Datenbank Ihres NetScaler ADM-Servers gespeichert werden, können Sie das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle aufbewahren soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00:00 Uhr) beschnitten.
- **Konfigurieren Sie die Syslog-Löscheinstellungen der Instanz**. Um die Menge der in der Datenbank gespeicherten Syslog-Daten zu begrenzen, können Sie das Intervall angeben, in dem Sie Syslog-Daten löschen möchten. Sie können die Anzahl der Tage angeben, nach denen die folgenden Syslog-Daten aus NetScaler ADM gelöscht werden:
  - Generische Syslog-Daten
  - AppFirewall-Daten
  - NetScaler Gateway-Daten.

    Weitere Infos

Nächste Schritte

Nachdem Sie NetScaler ADM bereitgestellt und eingerichtet haben, können Sie mit der Verwaltung und Überwachung Ihrer Instanzen und Anwendungen beginnen.

Verwaltung von NetScaler-Instanzen und -Anwendungen. Alle NetScaler ADM-Funktionen werden auf NetScaler-Instanzen unterstützt. Sie können beginnen, jede der Funktionen zu verwenden.

Bereitstellen

February 5, 2024

Bevor Sie NetScaler ADM zur Verwaltung und Überwachung Ihrer Anwendungen und Netzwerkinfrastruktur verwenden, müssen Sie es zuerst auf einem der Hypervisoren oder auf einem Kubernetes-Cluster installieren. Wenn Sie NetScaler ADM auf einem Hypervisor bereitstellen, können Sie es entweder als Einzelserver oder in einem Hochverfügbarkeitsmodus bereitstellen. Der Hochverfügbarkeitsmodus ist auf einem Kubernetes-Cluster nicht anwendbar. Wenn Sie NetScaler Insight Center verwenden, können Sie zu NetScaler ADM migrieren und zusätzlich zu den Analysefunktionen die Funktionen für Verwaltung, Überwachung, Orchestrierung und Anwendungsmanagement nutzen.

- **Bereitstellung auf einem einzelnen Server**: Bei einem eigenständigen ADM, das auf einem Hypervisor bereitgestellt wird, ist die Datenbank in den Server integriert und ein einziger Server ve-

rarbeitet den gesamten Datenverkehr. Sie können NetScaler ADM mit Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V und Linux KVM bereitstellen. Siehe:

- NetScaler ADM auf Citrix Hypervisor
- NetScaler ADM unter Microsoft Hyper-V
- NetScaler ADM auf VMware ESXi
- NetScaler ADM auf Linux KVM-Server
- NetScaler ADM im Kubernetes-Cluster

- **Bereitstellung mit hoher Verfügbarkeit (HA)**: Eine HA-Bereitstellung von zwei NetScaler ADM-Servern sorgt für einen unterbrechungsfreien Betrieb. In einem HA-Setup müssen beide NetScaler ADM-Knoten im aktiv-Passiven Modus im selben Subnetz mit derselben Softwareversion und demselben Build bereitgestellt werden und müssen dieselben Konfigurationen haben. Mit der HA-Bereitstellung entfällt die Möglichkeit, die schwebende IP-Adresse auf dem primären NetScaler ADM Knoten zu konfigurieren, dass kein separater NetScaler Load Balancer erforderlich ist.Siehe:Konfiguration in Hochverfügbarkeitsbereitstellung.

> Hinweis:
>
> Hochverfügbarkeit gilt nicht für ADM, die auf einem Kubernetes-Cluster bereitgestellt werden.

- **Migrieren Sie von NetScaler Insight Center zu NetScaler ADM**: Sie können Ihre NetScaler Insight Center-Bereitstellung zu NetScaler ADM migrieren, ohne die vorhandene Konfiguration, Einstellungen oder Daten zu verlieren. Mit NetScaler ADM können Sie nicht nur die verschiedenen vom NetScaler generierten Analysen einsehen, sondern auch die gesamte globale Infrastruktur für die Anwendungsbereitstellung von einer einzigen, einheitlichen Konsole aus verwalten, überwachen und Fehler beheben. Siehe:Migration von NetScaler Insight Center zu NetScaler ADM
- **Integration von NetScaler ADM mit Director**: Director integriert sich in NetScaler ADM für Netzwerkanalysen und Performance-Management. Siehe: Integrieren von NetScaler ADM mit Director

Voraussetzungen für die Installation von NetScaler ADM

February 5, 2024

Sie können NetScaler Application Delivery Management (ADM) für die Plattformen Microsoft HyperV, VMware ESXi, Linux KVM und Citrix Hypervisor als virtuelle Appliance herunterladen und installieren. Bevor Sie

NetScaler ADM installieren, müssen Sie die Softwareanforderungen, Browseranforderungen, Portinformationen, Lizenzinformationen und Einschränkungen auf allen diesen Plattformen verstehen.

Spezifische Plattformanforderungen und detaillierte Schritte zur Installation von NetScaler ADM finden Sie in den folgenden Themen:

- NetScaler ADM mit Citrix Hypervisor
- NetScaler ADM mit Microsoft HyperV
- NetScaler ADM mit VMware ESXi
- NetScaler ADM mit Linux KVM-Server

Allgemeine Anforderungen für NetScaler ADM

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8 CPUs
Speicherplatz	Citrix empfiehlt die Verwendung der Solid State Drive-Technologie (SSD) für NetScaler ADM-Bereitstellungen. Der Standardspeicherplatz beträgt 120 GB. Die tatsächliche Speicheranforderung hängt von der Schätzung der NetScaler ADM Größe ab. Verwenden Sie den Größenrechner, der im Abschnitt **Maximale Grenzwerte** (Seitenzahl 7) im NetScaler ADM HA Deployment Guide erwähnt wird. Dieses Handbuch ist auf unserer Download-Siteunter **NetScaler MAS Release 12.1 > Frühere Versionen verfügbar**. **Hinweis**: Sie benötigen ein Citrix Konto, um auf den Bereitstellungsleitfaden und den Größenrechner zuzugreifen Wenn Ihre NetScaler ADM-Speicheranforderungen 120 GB überschreiten, müssen Sie einen zusätzlichen Datenträger anschließen.

Komponente	Voraussetzung
	Citrix empfiehlt, dass Sie den Speicher abschätzen und zum Zeitpunkt der ersten Bereitstellung einen zusätzlichen Datenträger anschließen. Sie können nur einen zusätzlichen Datenträger hinzufügen. Weitere Informationen finden Sie unter Bereitstellen eines zusätzlichen Datenträgers in NetScaler ADM.
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s

> Hinweis:
>
> Citrix empfiehlt, die NetScaler ADM VHD auf einem lokalen Speicher zu hosten. Wenn NetScaler ADM auf Speichergeräten in einem SAN gehostet wird, funktioniert es möglicherweise nicht wie erwartet. Daher wird die ADM-Bereitstellung auf SAN nicht unterstützt.

NetScaler ADM auf Citrix Hypervisor

February 5, 2024

Um NetScaler ADM auf Citrix Hypervisor (ehemals XenServer) zu installieren, müssen Sie zuerst die NetScaler ADM XVA-Imagedatei auf den lokalen Computer herunterladen. Sie müssen Citrix XenCenter verwenden, um die NetScaler ADM-Installation durchzuführen.

> **Hinweis:**
>
> NetScaler ADM unterstützt XenMotion nicht.

Voraussetzungen

Stellen Sie vor der Installation von NetScaler ADM sicher, dass die folgenden Anforderungen erfüllt sind:

- Citrix Hypervisor Version 7.1 oder höher ist auf Hardware installiert, die die Mindestanforderungen erfüllt.

- XenCenter ist auf einer Management-Workstation installiert, die die Mindestanforderungen erfüllt. Sie müssen XenCenter verwenden, um NetScaler ADM auf Citrix Hypervisor zu installieren.
- Sie haben die NetScaler ADM .XVA-Imagedatei heruntergeladen.

XenCenter Systemanforderungen

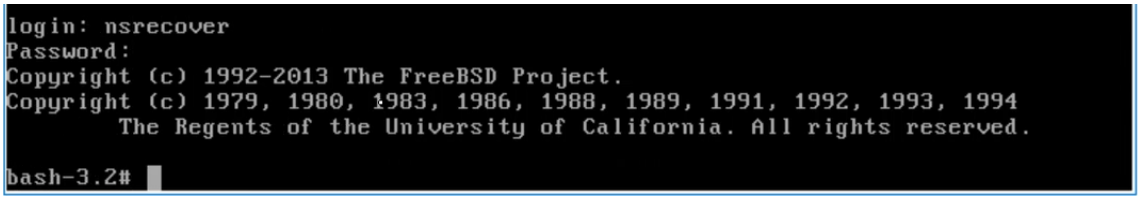
XenCenter ist eine Windows-Clientanwendung. Es kann nicht auf demselben Computer wie der Citrix Hypervisor-Host ausgeführt werden. In der folgenden Tabelle werden die Mindestsystemanforderungen beschrieben.

Komponente	Voraussetzung
Betriebssystem	Windows 7, Windows Server 2003 oder Windows 10
.NET-Framework	Version 2.0 oder höher
CPU	750 MHz (MHz), Empfohlen: 1 Gigahertz (GHz) oder schneller
RAM	1 GB, Empfohlen: 2 GB
Netzwerkkarte	100 Megabit pro Sekunde (Mbit/s) oder schnellere NIC

Installieren Sie NetScaler Application Delivery Management

1. Importieren Sie die XVA-Image-Datei in Ihren Citrix Hypervisor und konfigurieren Sie auf der Registerkarte **Konsole** die anfänglichen Netzwerkkonfigurationsoptionen.

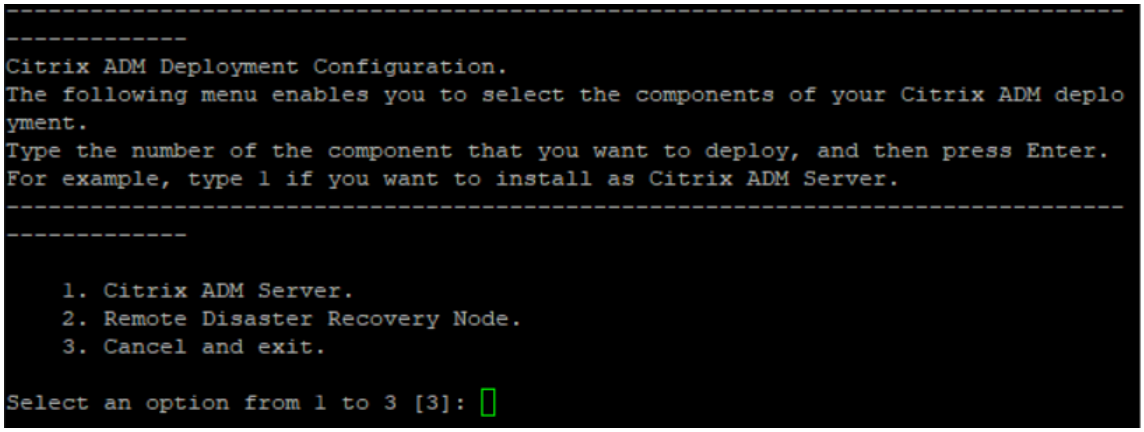
2. Speichern Sie die Konfigurationseinstellungen, nachdem Sie die erforderlichen IP-Adressen angegeben haben.
3. Melden Sie sich bei entsprechender Aufforderung mit den Anmeldeinformationen nsrecover/nsroot an.



> **Hinweis**
>
> Wenn Sie sich nach der Anmeldung die anfängliche Netzwerkkonfiguration aktualisieren möchten, geben Sie die Konfiguration ein `networkconfig`, aktualisieren Sie sie und speichern Sie die Konfiguration.

4. Führen Sie das Bereitstellungsskript aus, indem Sie den Befehl an der Shell-Eingabeaufforderung eingeben: `/mps/deployment_type.py`

5. Wählen Sie den Bereitstellungstyp als **NetScaler ADM Server**aus. Wenn Sie keine Option auswählen, wird diese standardmäßig als Server bereitgestellt.



6. Geben Sie**Ja**ein, um NetScaler ADM als eigenständige Bereitstellung bereitzustellen.
7. Geben Sie**Ja**ein, um den NetScaler ADM Server neu zu starten.

> **Hinweis**
>
> Nach der Installation von NetScaler ADM können Sie die ursprünglichen Konfigurationseinstellungen später aktualisieren.

Verifizierung

Nach der Installation des Servers können Sie auf die GUI zugreifen, indem Sie die IP-Adresse des NetScaler ADM-Servers im Webbrowser eingeben. Die standardmäßigen Administratoranmeldeinfor-

mationen für die Anmeldung am Server lauten nsroot/nsroot.

Der Browser zeigt das NetScaler ADM Konfigurationsprogramm an.

NetScaler ADM unter Microsoft Hyper-V

February 5, 2024

Um NetScaler ADM unter Microsoft Hyper-V zu installieren, müssen Sie zuerst die NetScaler ADM Imagedatei auf Ihren lokalen Computer herunterladen. Stellen Sie außerdem sicher, dass Ihr System über die Hardware-Virtualisierungserweiterungen verfügt, und stellen Sie sicher, dass die CPU-Virtualisierungserweiterungen verfügbar sind.

Voraussetzungen

Stellen Sie vor der Installation der virtuellen NetScaler ADM-Appliance sicher, dass die folgenden Anforderungen erfüllt sind:

- Microsoft Hyper-V Version 6.2 oder höher ist auf Hardware installiert, die die Mindestanforderungen erfüllt.
- Installieren Sie Microsoft Hyper-V Manager auf einer Verwaltungsarbeitsstation, die die Mindestsystemanforderungen erfüllt.
- Sie haben die NetScaler ADM-Image-Datei heruntergeladen.

Microsoft Hyper-V Systemanforderungen

Microsoft Hyper-V ist eine Windows-Client-Anwendung. In der folgenden Tabelle werden die Mindestsystemanforderungen beschrieben.

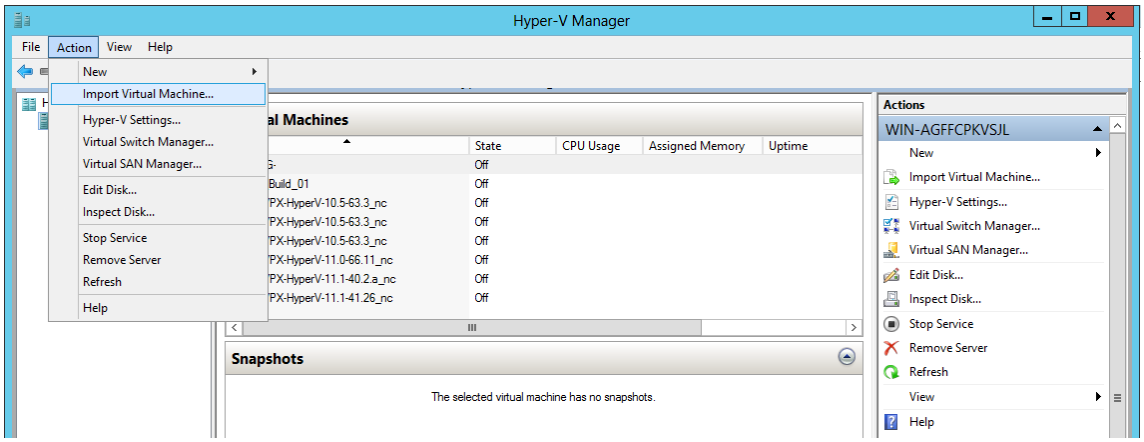
Komponente	Voraussetzung
Betriebssystem	Windows Server 2012 R2
.NET-Framework	Version 2.0 oder höher
CPU	750 MHz (MHz), Empfohlen: 1 Gigahertz (GHz) oder schneller
RAM	1 GB, Empfohlen: 2 GB
Netzwerkkarte	100 Megabit pro Sekunde (Mbit/s) oder schnellere NIC

Installation von NetScaler Application Delivery Management

Die Anzahl der NetScaler ADM Server, die Sie installieren können, hängt vom verfügbaren Arbeitsspeicher auf dem Hyper-V-Server ab.

So installieren Sie NetScaler ADM:

1. Starten Sie den Hyper-V Manager-Client auf Ihrer Workstation.
2. Klicken Sie im Menü **Aktion** auf **Virtuelle Maschine importieren** .



3. Importieren Sie das Hyper-V-Image und gehen Sie wie folgt vor:

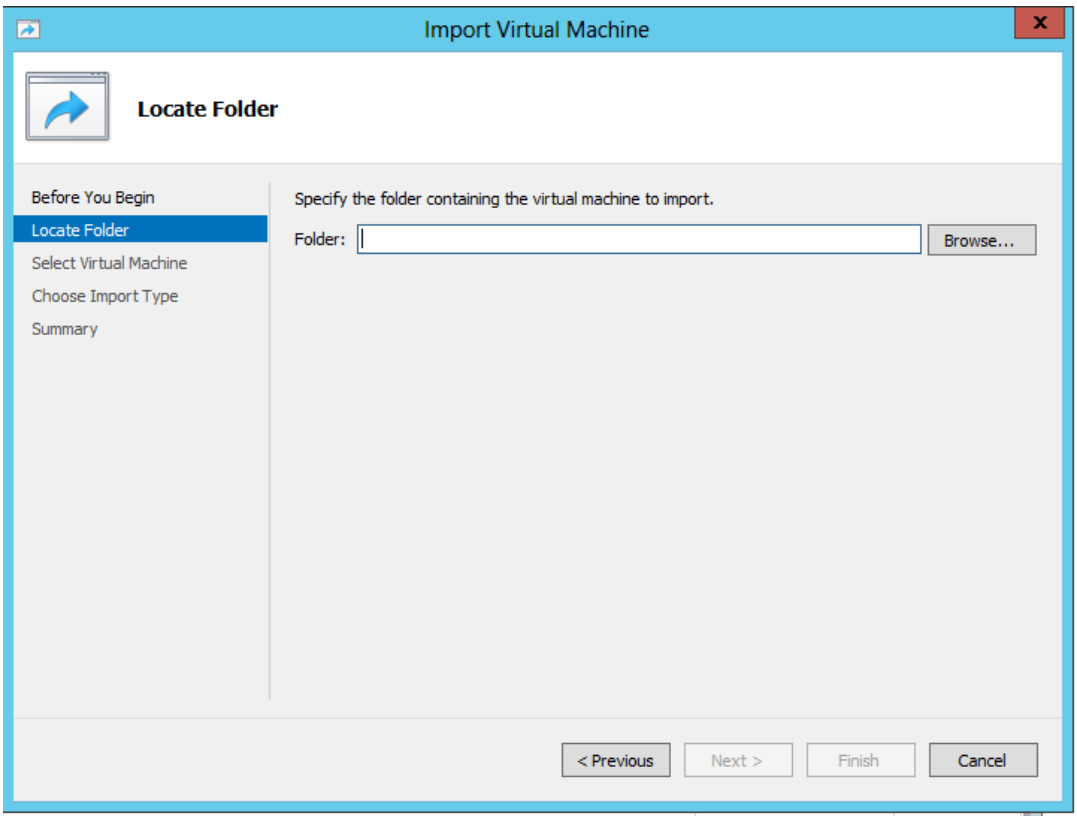
   a) **Navigieren Sie im Dialogfeld Virtuelle Maschine importieren im Abschnitt**Ordner suchen zu dem Ordner**, in dem Sie das NetScaler ADM Hyper-V-Image gespeichert haben, wählen Sie den Ordner aus und klicken Sie auf Weiter.**

   b) Wählen Sie im Abschnitt Virtuelle Maschine auswählen den entsprechenden Namen der virtuellen Maschine aus.

   c) **Wählen Sie im Abschnitt Importtyp** auswählen die Option Virtuelle Maschine kopieren (neue eindeutige ID erstellen) aus und klicken Sie auf Weiter.

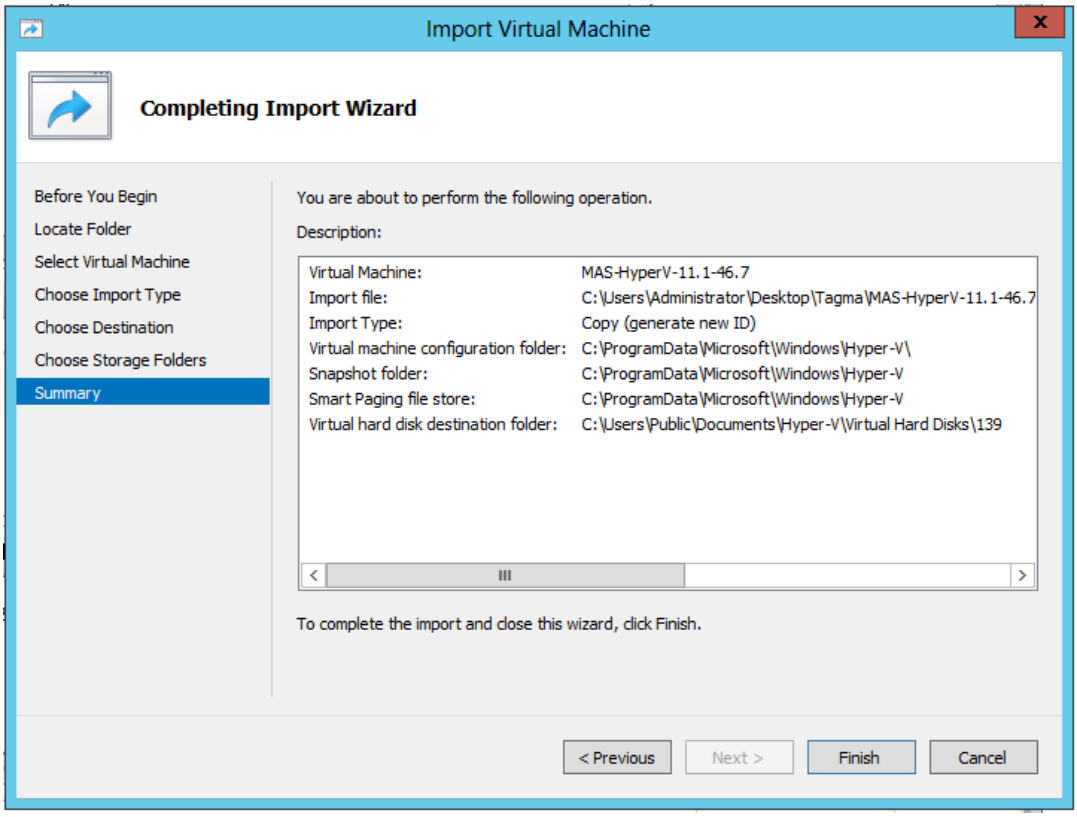
   d) Im Abschnitt **Ziel auswählen** können Sie die Ordner angeben, in denen die Dateien der virtuellen Maschine gespeichert werden sollen.

   > **Hinweis**
   >
   > Standardmäßig importiert der Assistent die Dateien der virtuellen Maschine in Standard-Hyper-V-Ordner auf Ihrem lokalen Host.



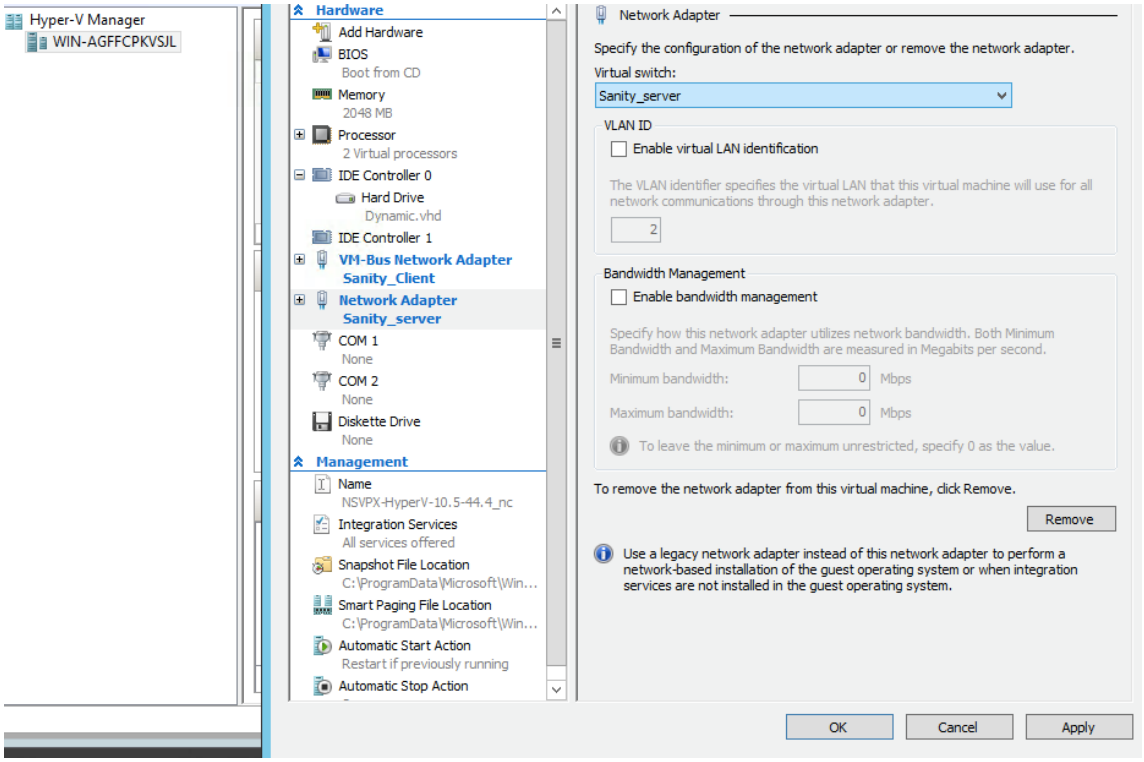
e) Im Abschnitt **Speicherordner auswählen** können Sie den Speicherort auswählen, an dem Sie die virtuellen Festplatten speichern möchten, und dann auf **Weiter**klicken.

f) Sie können die Details der virtuellen Maschine im Übersichtsbereich überprüfen und auf **Fertig stellen**klicken.

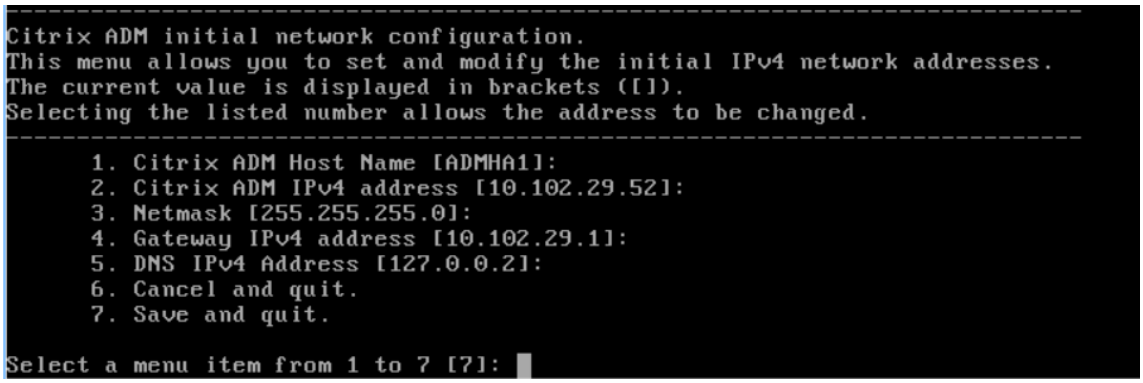


Das NetScaler ADM Hyper-V-Image wird im rechten Bereich angezeigt.

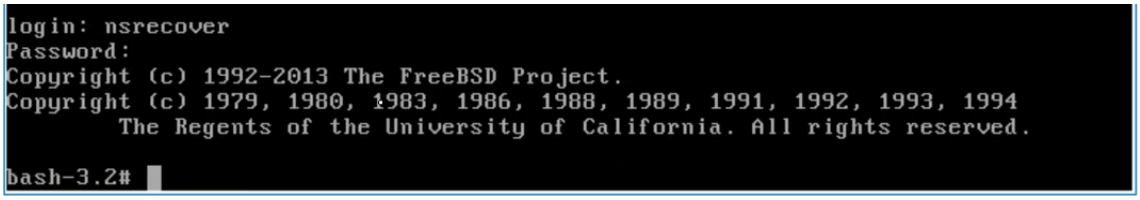
4. Klicken Sie mit der rechten Maustaste auf das NetScaler ADM Hyper-V-Image, und klicken Sie dann auf **Einstellungen**.
5. Navigieren Sie im linken Bereich des angezeigten Dialogfelds zu **Hardware** > **VM_Bus Network Adaptor**und wählen Sie im rechten Bereich aus der Netzwerkliste das entsprechende Netzwerk aus.



6. Klicken Sie auf **Übernehmen** und dann auf **OK**.
7. **Klicken Sie mit der rechten Maustaste auf das NetScaler ADM Hyper-V-Image und klicken Sie auf Verbinden.**
8. Klicken Sie im Konsolenfenster auf die Schaltfläche **Start** .
9. Konfigurieren Sie die anfänglichen Netzwerkkonfigurationsoptionen.



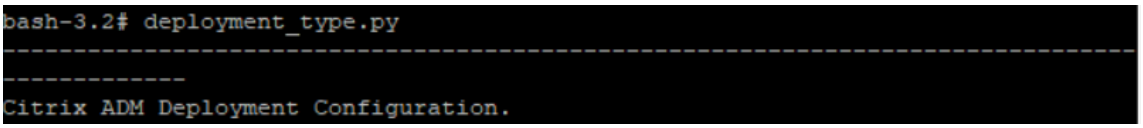
10. Speichern Sie die Konfigurationseinstellungen, nachdem Sie die erforderlichen IP-Adressen angegeben haben.
11. Melden Sie sich bei entsprechender Aufforderung mit den Anmeldeinformationen nsrecover/nsroot an.



> **Hinweis**
>
> Wenn Sie sich nach der Anmeldung die anfängliche Netzwerkkonfiguration aktualisieren möchten, geben Sie die Konfiguration ein `networkconfig`, aktualisieren Sie sie und speichern Sie die Konfiguration.

12. Führen Sie das Deployment-Skript aus, indem Sie den Befehl an der Shell-Eingabeaufforderung eingeben:

```
deployment_type.py
<!--NeedCopy-->
```



13. Wählen Sie den Bereitstellungstyp als **NetScaler ADM Server**aus. Wenn Sie keine Option auswählen, wird diese standardmäßig als Server bereitgestellt.

14. Geben Sie**Ja** ein, um NetScaler ADM als eigenständige Bereitstellung bereitzustellen.
15. Geben Sie**Ja**ein, um den NetScaler ADM Server neu zu starten.

> **Hinweis**
>
> Nach der Installation von NetScaler ADM können Sie die ursprünglichen Konfigurationseinstellungen später aktualisieren.

Verifizierung

Nachdem der Server installiert wurde, können Sie auf die GUI zugreifen, indem Sie die IP-Adresse des NetScaler ADM-Servers in die Adressleiste Ihres Browsers eingeben. Die standardmäßigen Administratoranmeldeinformationen für die Anmeldung am Server lauten nsroot/nsroot.

Der Browser zeigt das NetScaler ADM Konfigurationsprogramm an.

NetScaler ADM auf VMware ESXi

February 5, 2024

In diesem Dokument wird beschrieben, wie virtuelle NetScaler ADM Appliances auf VMware ESXi mithilfe des VMware vSphere-Clients installiert werden.

Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Installieren Sie eine unterstützte Version von VMware ESXi (6.0, 6.5, 6.7 und 7.0).
- Installieren Sie VMware Client auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
- Laden Sie die NetScaler ADM-Setupdateien herunter.

> Hinweis
>
> - VMotion wird nur von **NetScaler ADM 13.0 Build 47.22 oder höher** unterstützt. Sie können die Migration des auf einem ESXi-Hypervisor bereitgestellten ADM-Servers planen und automatisieren, einschließlich vSphere High Availability und vSphere DRS-Setups.
> - VMware Tools for NetScaler ADM werden als Teil des Software-Builds geliefert und können nicht separat aktualisiert oder geändert werden.

So installieren Sie NetScaler ADM

Befolgen Sie diese Schritte, um eine virtuelle ADM-Appliance auf VMware ESXi zu installieren.

> **Hinweis**
>
> Die Schritte und Bildschirmaufzeichnungen basieren auf VMware ESXi Version 6.0. Die GUI kann sich in anderen ESXi-Versionen unterscheiden. VMware ESXi Version 7.0.1c Build-Nummer 17325551 mit VMXNET3-Adapter wird in **NetScaler ADM 13.0 71.40 oder höher**unterstützt. In der VMware-Dokumentation finden Sie versionsspezifische Schritte.

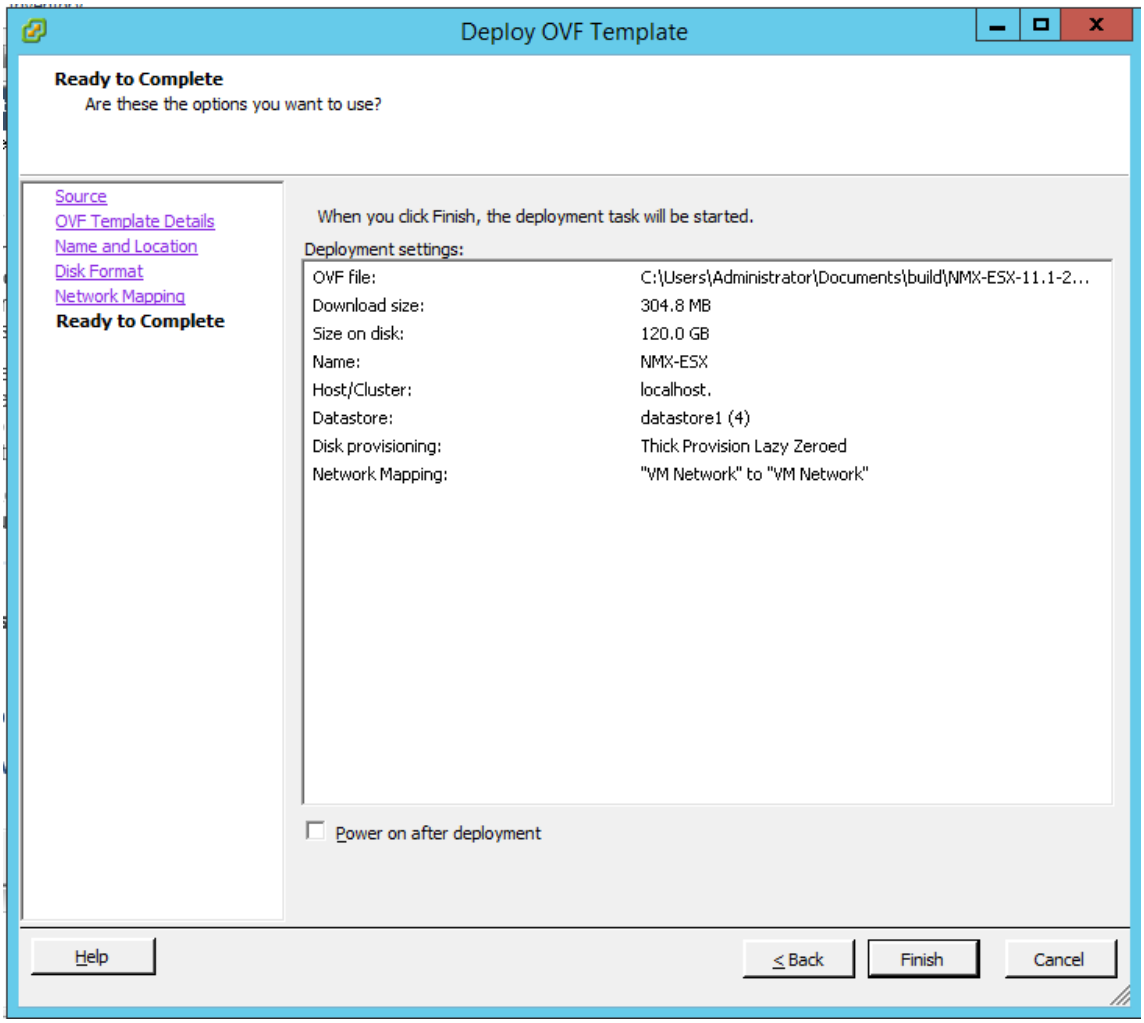
1. Starten Sie den VMware vSphere Client auf Ihrer Workstation.
2. Geben Sie im Textfeld **IP-Adresse/Name** die IP-Adresse des VMware ESXi-Servers ein, mit dem Sie eine Verbindung herstellen möchten.
3. Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein, und klicken Sie dann auf **Anmelden**.
4. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
5. Wählen **Sie im Dialogfeld OVF-Vorlagebereitstellen unter Aus einer Datei oder URL**bereitstellen die OVF-Datei aus, und klicken Sie auf**Weiter**.

   > **Hinweis**
   >
   > Falls eine Warnmeldung mit dem folgenden Text angezeigt wird: "Die Betriebssystemkennung wird auf dem ausgewählten Host nicht unterstützt, überprüfen Sie, ob der VMware-Server das FreeBSD-Betriebssystem unterstützt."Klicken Sie auf **Ja**.

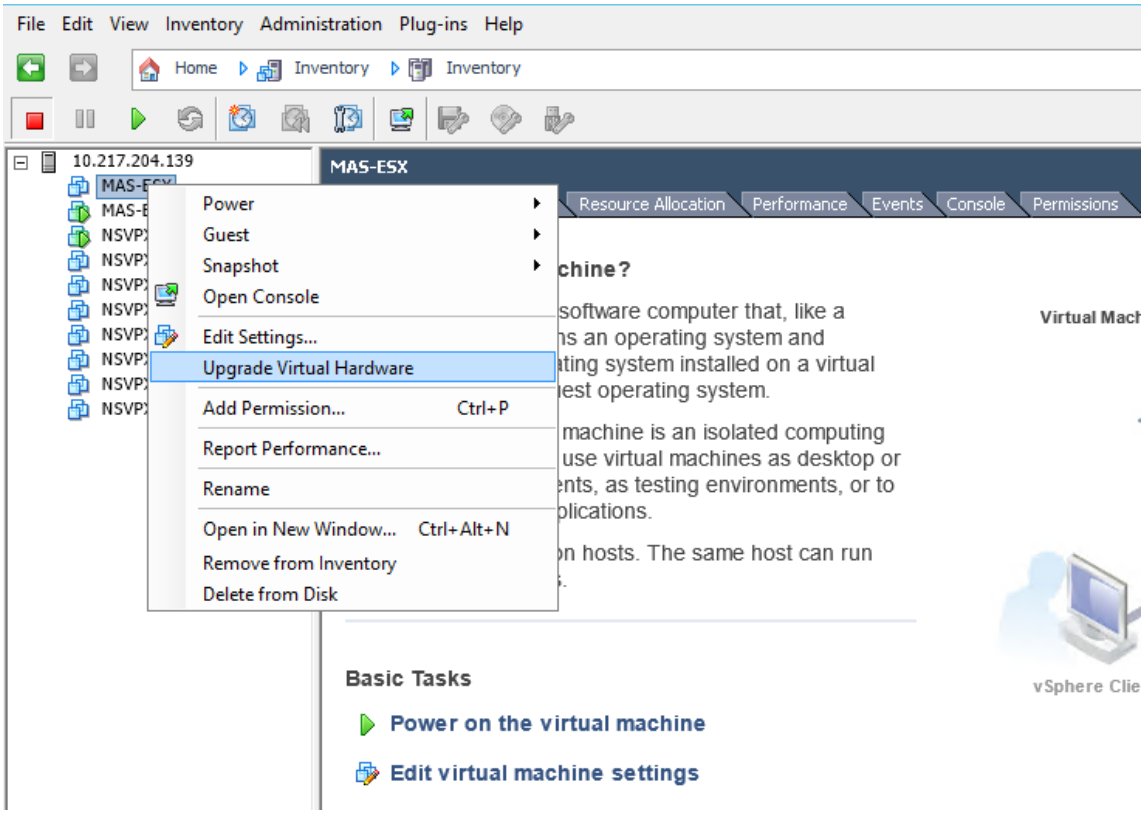
6. Klicken Sie auf der Seite **Details zur OVF-Vorlage** auf **Weiter**.
7. Geben Sie einen Namen für die virtuelle NetScaler ADM-Appliance ein, und klicken Sie dann auf **Weiter**.
8. Geben Sie das Datenträgerformat an, indem Sie entweder Thin Provisioned Format oder Thick Provisioned Format auswählen

   > **Hinweis**
   >
   > Citrix empfiehlt, dass Sie das **Thick Provisioned Format**auswählen.

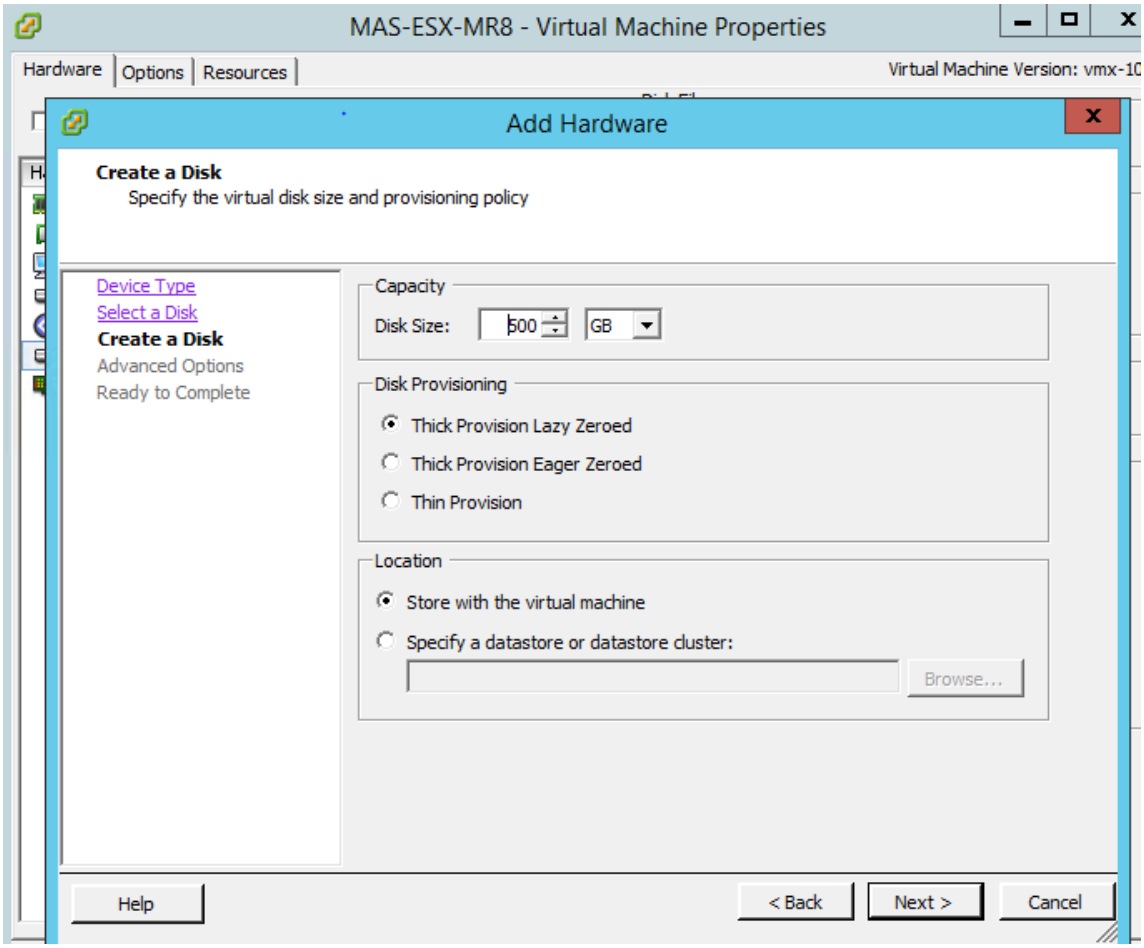
9. Klicken Sie auf **Fertig stellen**, um die Installation zu starten.



10. Sie können jetzt die virtuelle NetScaler ADM-Appliance starten.
11. Wählen Sie im Navigationsbereich die virtuelle Appliance aus, die Sie installiert haben. Klicken Sie im Menü **Inventar** mit der rechten Maustaste auf die **virtuelle Maschine**, und klicken Sie dann auf **Virtuelle Hardware aktualisieren**. Klicken **Sie im Dialogfeld Virtuelle Maschine bestätigen** auf **Ja**.

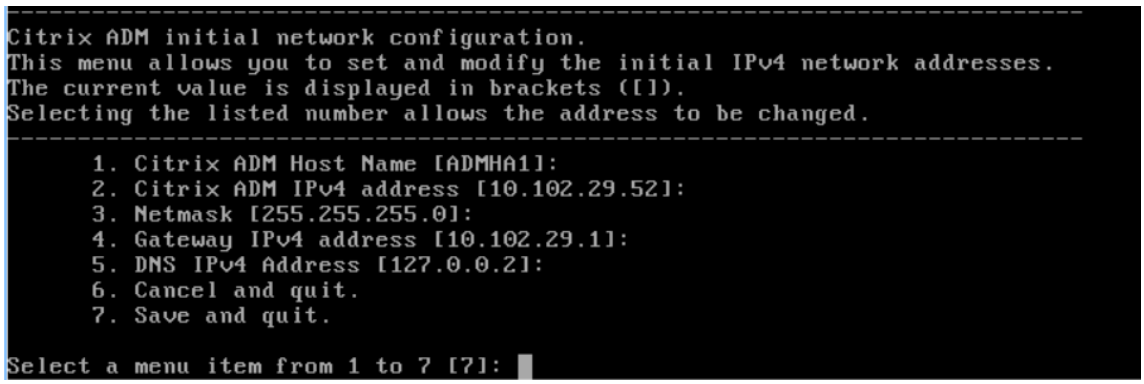


12. Klicken Sie im Menü **Inventar** auf **Virtuelle Maschine**und dann auf **Einstellungen bearbeiten**.
13. Klicken Sie im Dialogfeld **Eigenschaften der virtuellen Maschine** auf der Registerkarte **Hardware** auf **Speicher**, und geben Sie dann im rechten Bereich als **Speichergröße** 32 GB an.
14. Klicken Sie auf **CPUs**, und geben Sie dann im rechten Bereich die CPUs als 8 an. Klicken Sie auf **OK**.
15. Stellen Sie einen zusätzlichen Datenträger gemäß Ihrer Anforderung hinzu.



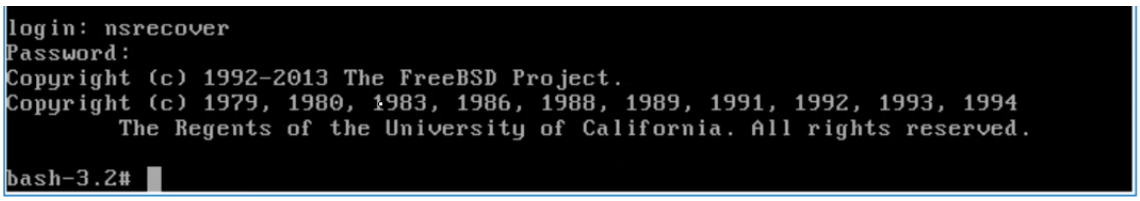
16. Wählen Sie im Navigationsbereich die virtuelle Appliance aus, die Sie installiert haben. Klicken Sie im Menü **Inventar** auf **Virtuelle Maschine**, klicken Sie auf **Einschalten**und dann **auf Einschalten**.

17. Klicken Sie auf die Registerkarte **Konsole**, um die Optionen für die anfängliche Netzwerkkonfiguration von NetScaler ADM anzuzeigen.



18. Speichern Sie die Konfigurationseinstellungen, nachdem Sie die erforderlichen IP-Adressen angegeben haben.

19. Melden Sie sich bei entsprechender Aufforderung mit den Anmeldeinformationen nsrecover/nsroot an.

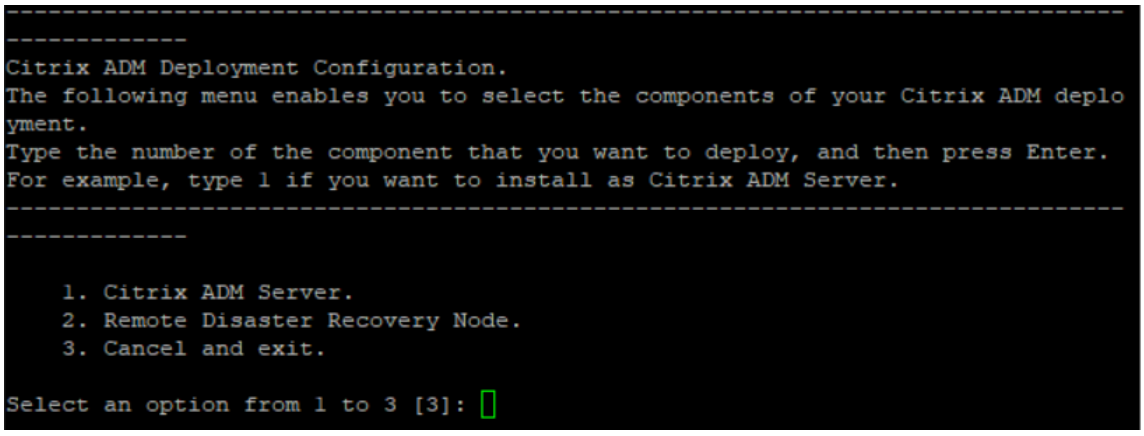


> **Hinweis**
>
> Wenn Sie sich nach der Anmeldung die anfängliche Netzwerkkonfiguration aktualisieren möchten, geben Sie die Konfiguration ein `networkconfig`, aktualisieren Sie sie und speichern Sie die Konfiguration.

20. Führen Sie das Deployment-Skript aus, indem Sie den Befehl an der Shell-Eingabeaufforderung eingeben:

```
deployment_type.py
<!--NeedCopy-->
```

21. Wählen Sie den Bereitstellungstyp als **NetScaler ADM Server**aus. Wenn Sie keine Option auswählen, wird diese standardmäßig als Server bereitgestellt.



22. Geben Sie**Ja**ein, um NetScaler ADM als eigenständige Bereitstellung bereitzustellen.
23. Geben Sie**Ja**ein, um den NetScaler ADM Server neu zu starten.

> **Hinweis**

> Nach der Installation von NetScaler ADM können Sie die ursprünglichen Konfigurationseinstellungen später aktualisieren.

Verifizierung

Nachdem der Server installiert wurde, können Sie auf die GUI zugreifen, indem Sie die IP-Adresse des NetScaler ADM-Servers in den Browser eingeben. Die standardmäßigen Administratoranmeldeinformationen für die Anmeldung am Server lauten nsroot/nsroot.

Der Browser zeigt das NetScaler ADM Konfigurationsprogramm an.

> **Hinweis:**
>
> Die typische ADM-Installationszeit beträgt auf VMware ESXi etwa 10 Minuten, kann auf einigen Systemen jedoch länger dauern.

Automatisieren Sie die Bereitstellung des NetScaler ADM Agenten auf VMware ESXi

February 5, 2024

Mit NetScaler ADM können Sie die Bereitstellung von NetScaler ADM-Agenten auf VMware ESXi automatisieren.

Als Administrator können Sie die folgenden Aktionen automatisieren:

- Den NetScaler ADM Agent konfigurieren
- Registrieren Sie den NetScaler ADM Agent und ändern Sie das Standardkennwort des Agenten.

Den NetScaler ADM Agent konfigurieren

Um die Konfiguration des Agenten zu automatisieren, fügen Sie die Werte für die folgenden Parameter in die OVF-Datei ein:

1. IP-Adresse
2. Netzmaske
3. Gateway
4. Nameserver
5. Hostname

> **Hinweis**
>
> Die OVF-Datei ist in der Agenten-Image-Datei verfügbar. Um die NetScaler ADM Agent-Datei herunterzuladen, gehen Sie zu. https://www.citrix.com/downloads/citrix-application-management/ Das Benennungsmuster der Agenten-Image-Datei lautet wie folgt: **MASAGENT-ESX-releasenumber-buildnumber.zip**

Registrieren Sie den NetScaler ADM Agent und ändern Sie das Standardkennwort

> **Hinweis**
>
> Bevor Sie das Standardkennwort registrieren und ändern, stellen Sie sicher, dass Sie die unter Konfiguration des NetScaler ADM-Agentenangegebenen Parameter hinzugefügt haben.

Um die Registrierung des NetScaler ADM Agents und die Änderung des Standardkennworts zu automatisieren, fügen Sie die Werte für die folgenden Parameter in derselben OVF-Datei hinzu:

1. IP des ADM-Servers
2. ADM-Benutzername
3. ADM-Kennwort
4. Neues Kennwort für den Agent

Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, stellen Sie sicher, dass Sie:

- Installieren Sie VMware vSphere 8.x auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
- Laden Sie die NetScaler ADM-Setupdateien herunter.

So konfigurieren und registrieren Sie einen NetScaler ADM Agent

1. Laden Sie die .OVF-Datei herunter und bearbeiten Sie sie
2. Installieren Sie die virtuelle NetScaler ADM-Appliance auf VMware ESXi
3. Überprüfen

Laden Sie die .OVF-Datei herunter und bearbeiten Sie sie

1. Extrahieren Sie die Dateien aus der Datei MASAGENT-ESX-releasenumber-buildnumber.zip an den gewünschten Speicherort. Die folgenden Dateien sind verfügbar:

- .ovf-Datei
- .vmdk-Datei
- .ova-Datei
- .mf-Datei

2. Open the .ovf file in any editor and add the following <ProductSection>..</ProductSection> sample code after the </VirtualHardwareSection> tag

```
<ProductSection>
    <Info>Information about the installed software</Info>
    <Product>Application Delivery management</Product>
    <Vendor>Citrix</Vendor>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.ip">
    <Label>IPAddress</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.netmask">
    <Label>Netmask</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.gateway">
    <Label>Gateway</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.nameserver">
    <Label>Nameserver</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.hostname">
    <Label>Hostname</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.ServerIP">
    <Label>ADM Server IP</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
```



```
37      ovf:key="eth0.ServerUname">
38      <Label>ADM Username</Label>
39      </Property>
40
41      <Property ovf:userConfigurable="true" ovf:password="true" ovf:value
           ="VALUE"
42      ovf:type="string" ovf:key="eth0.ServerPassword">
43      <Label>ADM Password</Label>
44      </Property>
45
46      <Property ovf:userConfigurable="true" ovf:password="true" ovf:value
           ="VALUE"
47      ovf:type="string" ovf:key="eth0.NewPassword">
48      <Label>Agent New Password</Label>
49      </Property>
50
51  </ProductSection>
52  <!--NeedCopy-->
```

1. Für Parameter, die Sie konfigurieren möchten, fügen Sie die entsprechenden Werte in ovf:value=”VALUE”hinzu

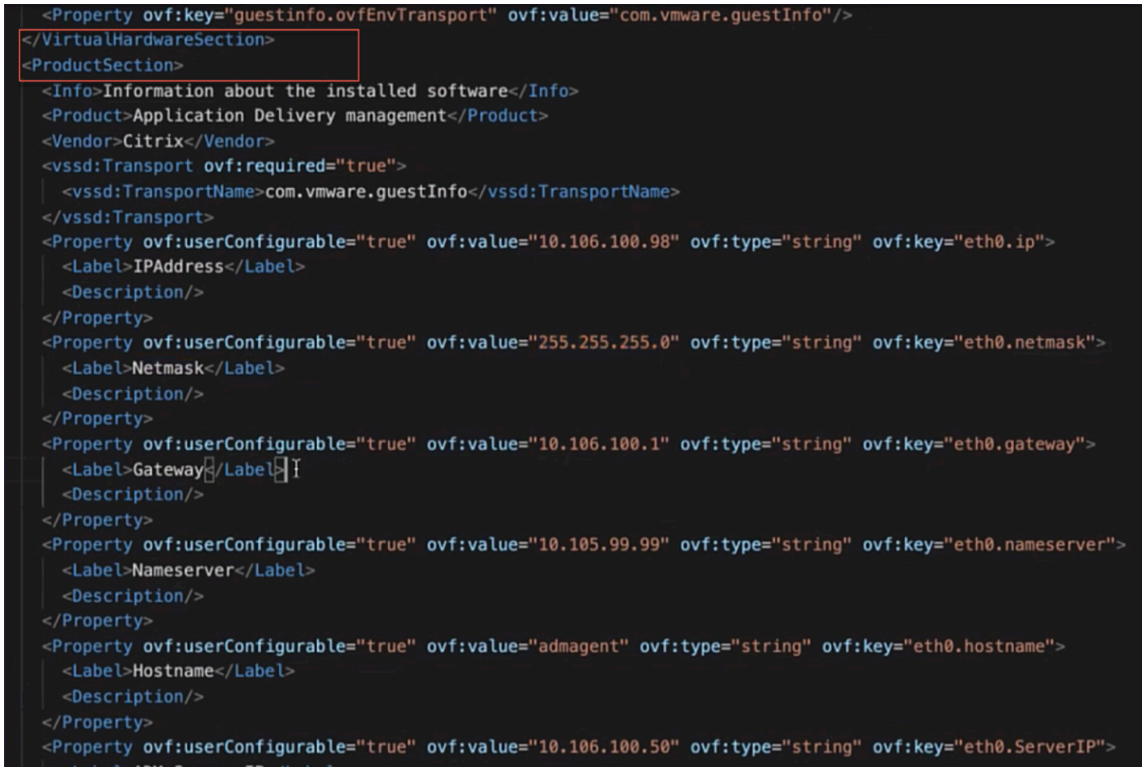
   - Um den NetScaler ADM Agent zu konfigurieren, fügen Sie die Werte zu den folgenden Parametern hinzu:

     - IP-Adresse
     - Netzmaske
     - Gateway
     - Nameserver
     - Hostname

   - Um das Standardkennwort des NetScaler ADM Agents zu registrieren und zu ändern, fügen Sie die Werte zu den folgenden Parametern hinzu:

     - IP des ADM-Servers
     - ADM-Benutzername
     - ADM-Kennwort
     - Neues Kennwort für den Agent

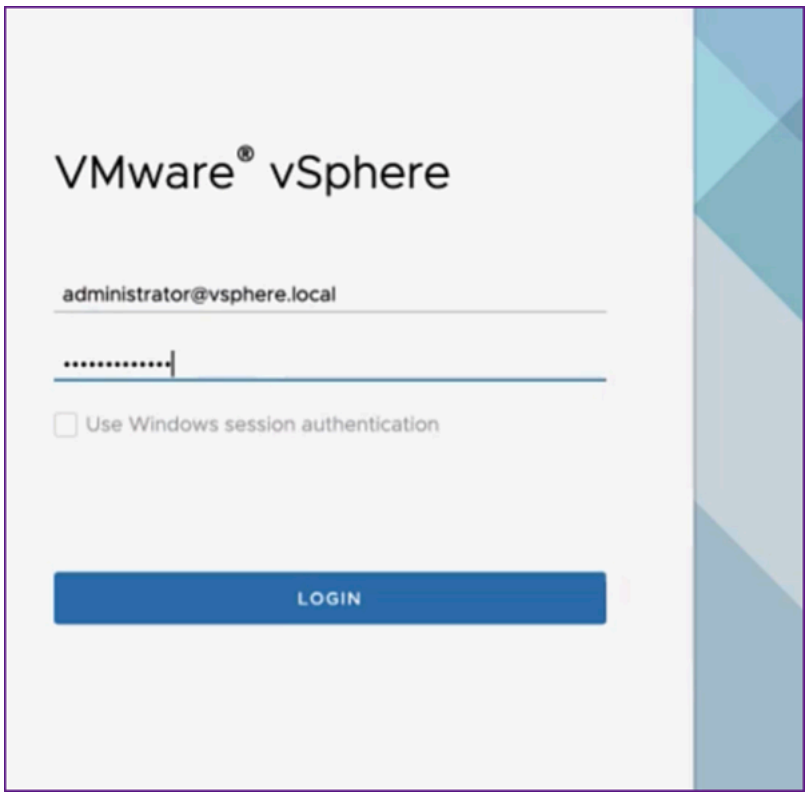
   > **Hinweis**
   >
   > - Sie müssen den NetScaler ADM Agent konfigurieren, bevor Sie sich registrieren und das Standardkennwort des Agenten ändern.
   > - Wenn Sie das Standardkennwort in der OVF-Datei nicht registrieren und ändern, müssen Sie diese Aktionen manuell ausführen, nachdem die VM bereitgestellt wurde.



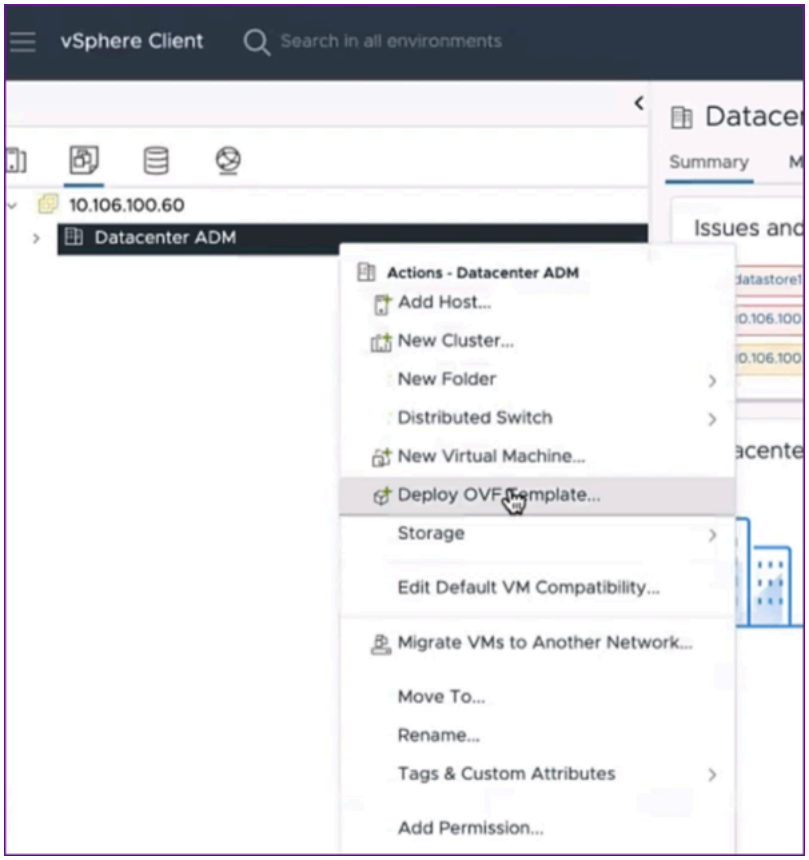
2. Nachdem Sie die Parameter und ihre Werte hinzugefügt haben, speichern Sie die OVF-Datei.

Installieren Sie die virtuelle NetScaler ADM-Appliance auf VMware ESXi

1. Melden Sie sich beim **VMware vSphere Client** an und geben Sie die Administratoranmeldedaten ein. Klicken Sie auf **Anmelden**.

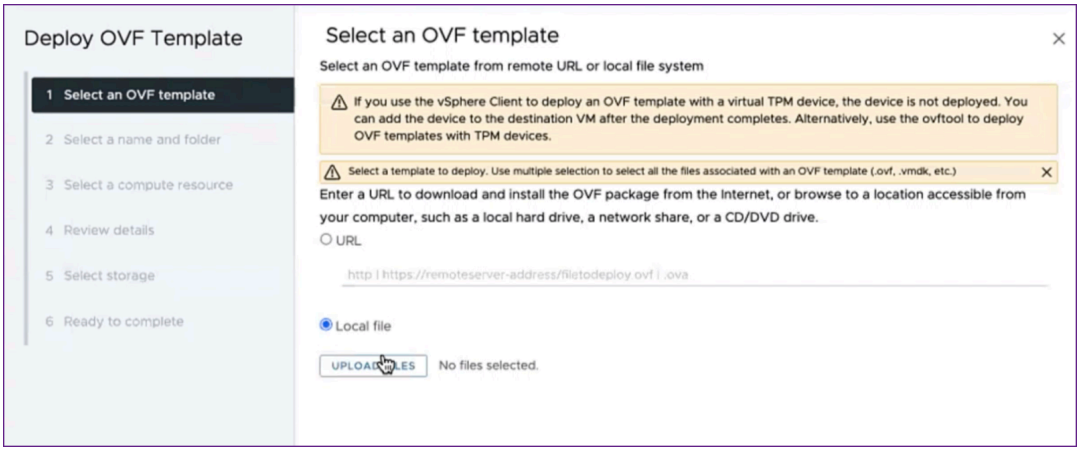


2. Wählen Sie Ihren ESXi-Server aus und klicken Sie mit der rechten Maustaste, um **OVF-Vorlage bereitstellen**auszuwählen.

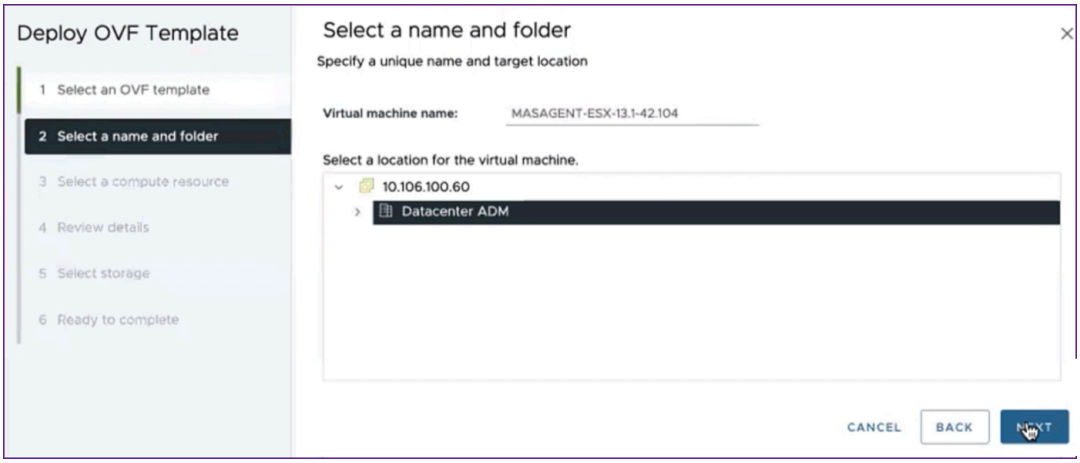


3. Gehen Sie auf der Seite „ **OVF-Vorlage bereitstellen** “wie folgt vor:

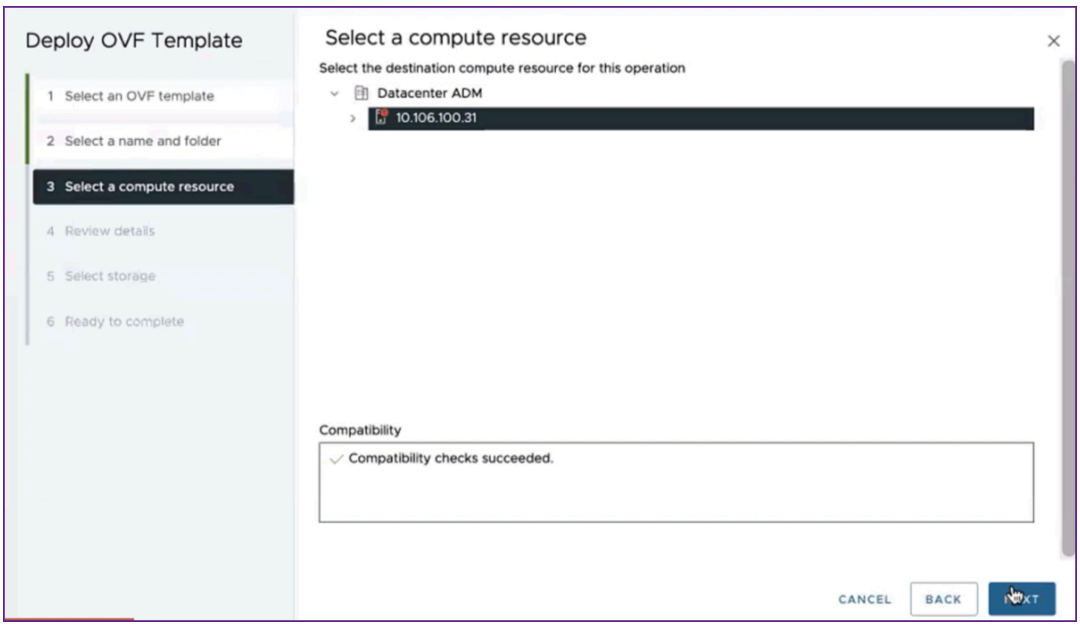
   a) **Wählen Sie eine OVF-Vorlage**aus: Wählen Sie **Lokale Datei** und navigieren Sie zu dem Ort, an dem Sie die bearbeitete OVF-Datei und die .vmdk-Datei gespeichert haben. Wählen Sie die Dateien aus und klicken Sie auf **Öffnen**, um sie hochzuladen. Klicken Sie auf **Weiter**.



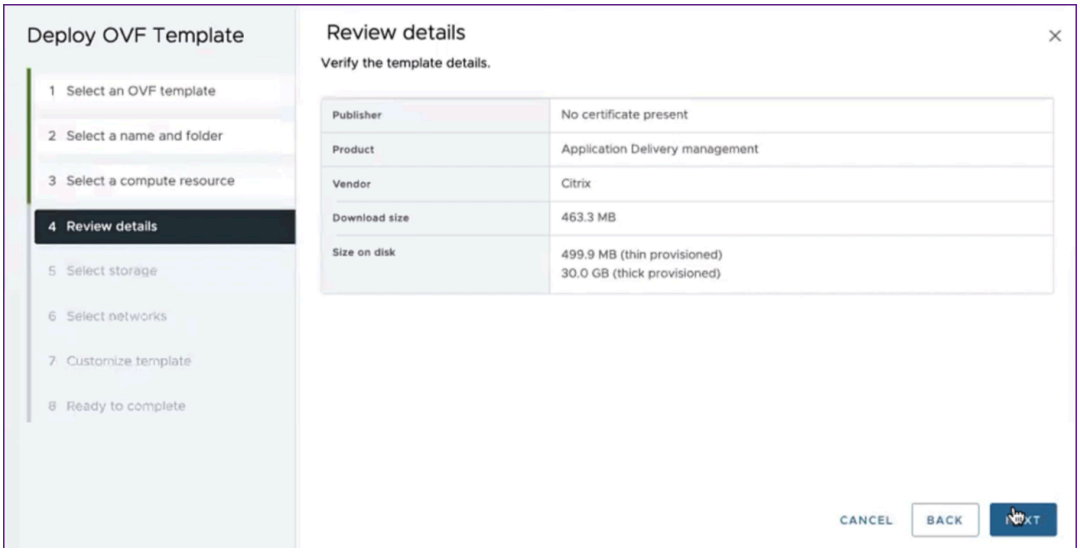
   b) **Wählen Sie einen Namen und einen Ordner**aus: Fügen Sie einen Namen für die virtuelle Appliance hinzu und wählen Sie den Speicherort auf dem ESXi aus, an dem Sie die virtuelle Maschine bereitstellen möchten. Klicken Sie auf **Weiter**.



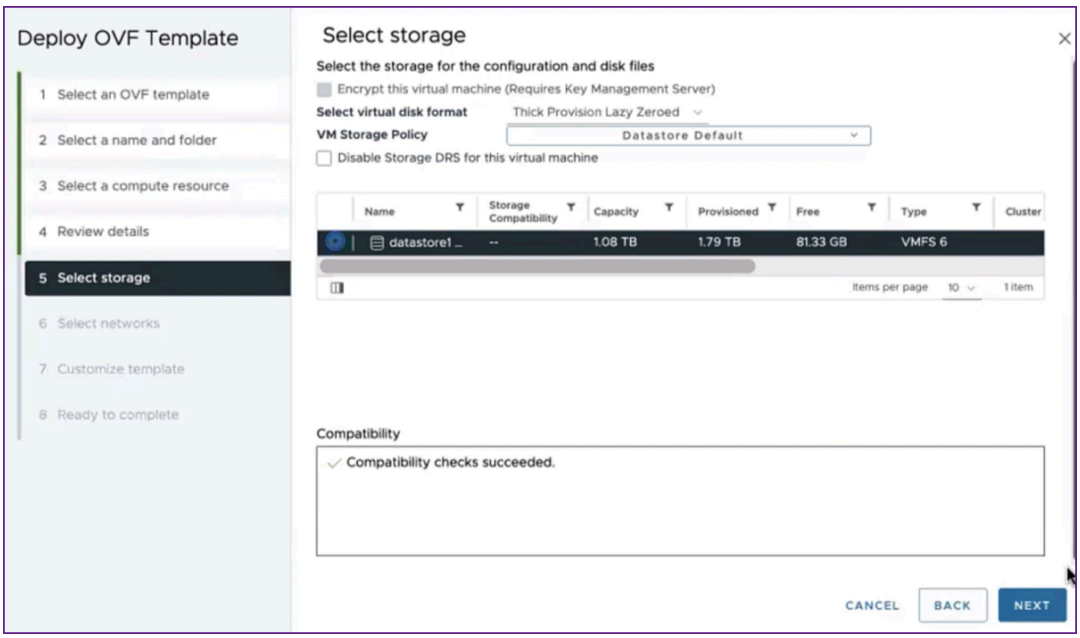
c) **Wählen Sie eine Rechenressource**aus: Wählen Sie eine Ressource aus, auf der die Vorlage ausgeführt werden soll, nachdem sie bereitgestellt wurde. Klicken Sie auf **Weiter**.



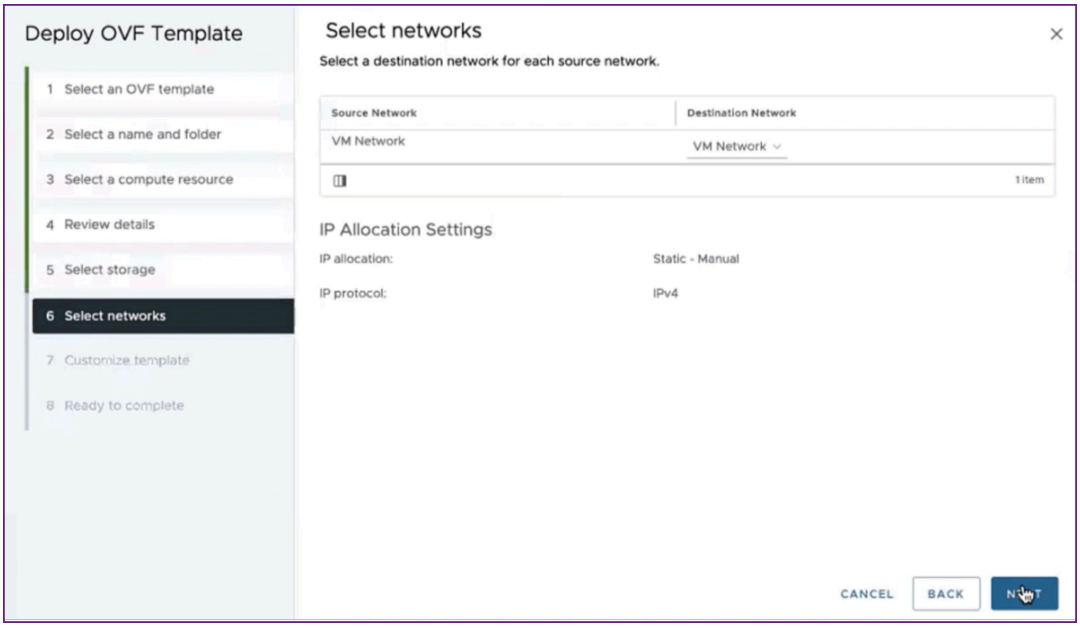
d) **Details überprüfen**: Überprüfen Sie die Details der OVF-Vorlage. Klicken Sie auf **Weiter**.



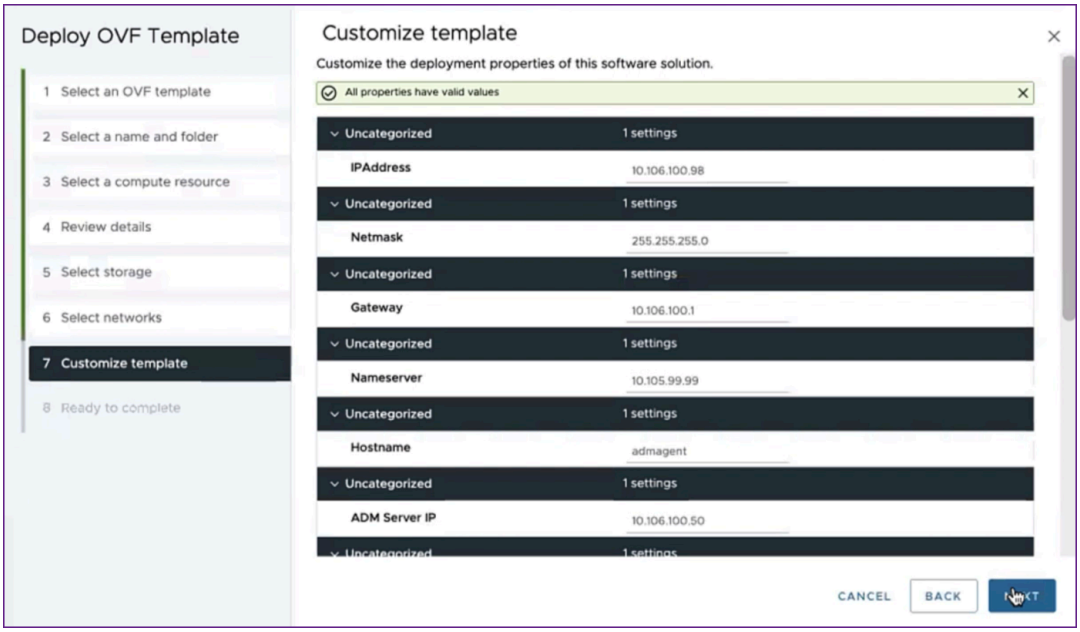
e) **Speicher wählen**: Wählen Sie einen Datenspeicher aus, um die OVF-Vorlage zu speichern. Klicken Sie auf **Weiter**.



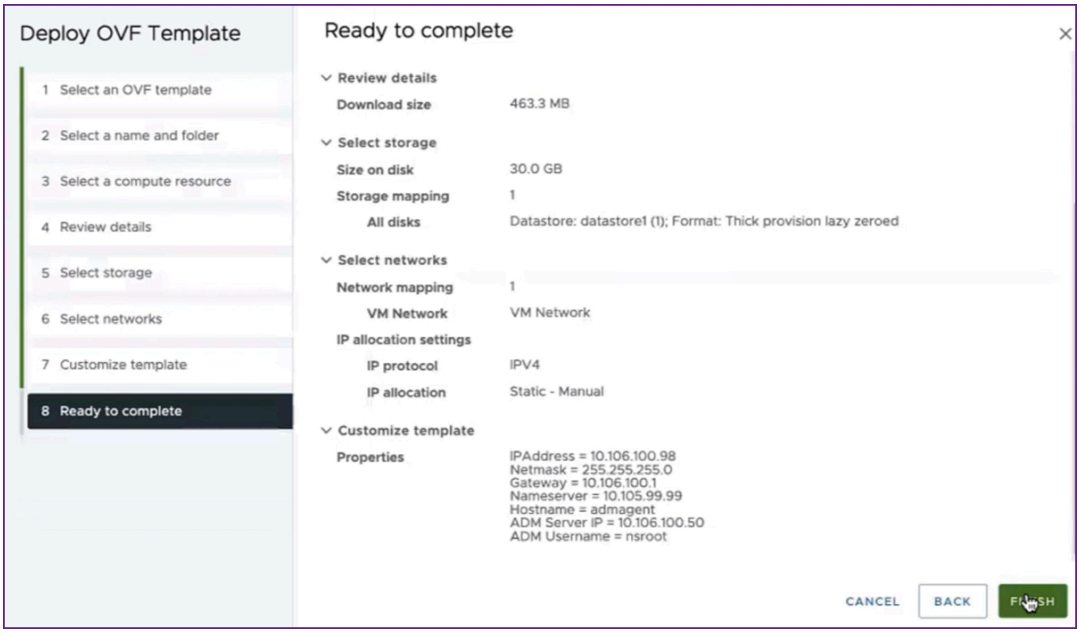
f) **Netzwerke auswählen**: Fahren Sie mit den Standardeinstellungen fort. Klicken Sie auf **Weiter**.



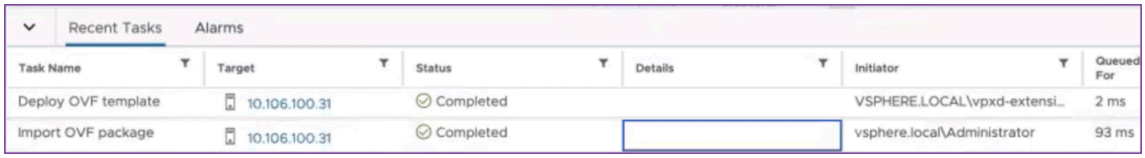
g) **Vorlage anpassen**: Überprüfen Sie alle Eigenschaften der OVF-Vorlage. Alle Parameter und Werte, die Sie in der OVF-Datei im Abschnitt .OVF-Datei herunterladen und bearbeiten hinzugefügt haben, werden angezeigt.



h) **Bereit zum Abschluss**: Um die Einstellungen zu speichern und den Bereitstellungsprozess zu starten, klicken Sie auf **Fertig stellen**.

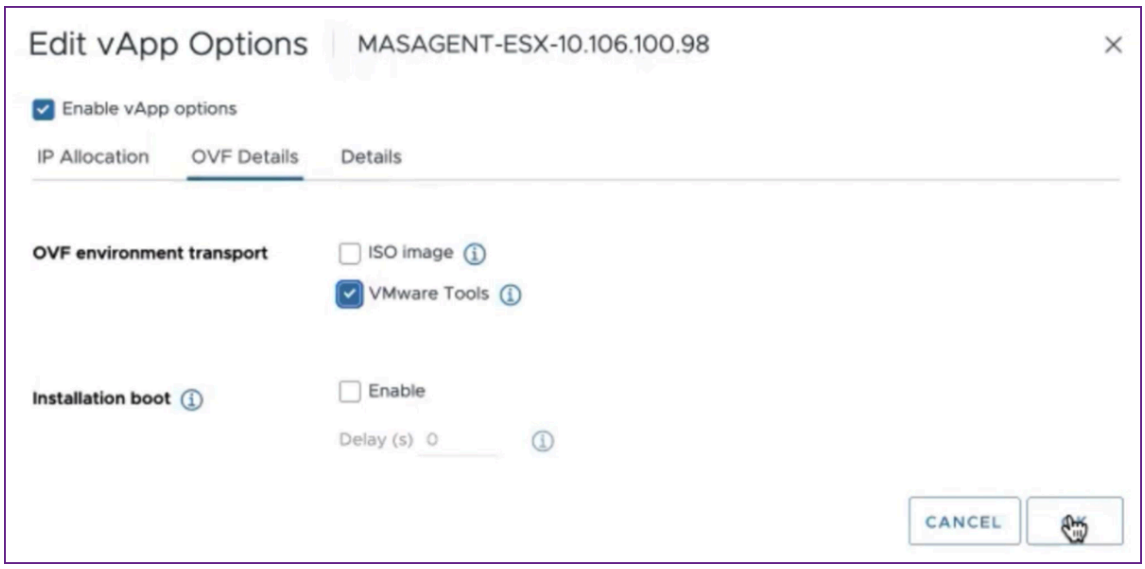


Warten Sie, bis die Bereitstellung abgeschlossen ist. Nachdem der Status des **Vorgangs „OVF-Vorlage bereitstellen** “zu 100% abgeschlossen ist, wird Ihr Agent bereitgestellt.

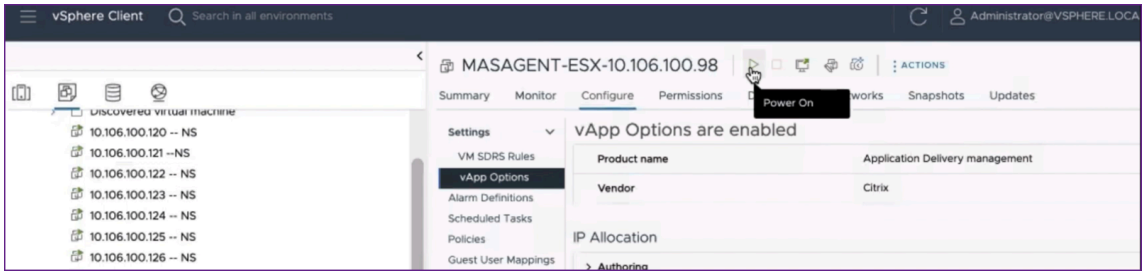


> **Wichtig!**
>
> Schalten Sie die virtuelle Appliance nicht ein, bevor Sie die Einstellungen bearbeitet haben.

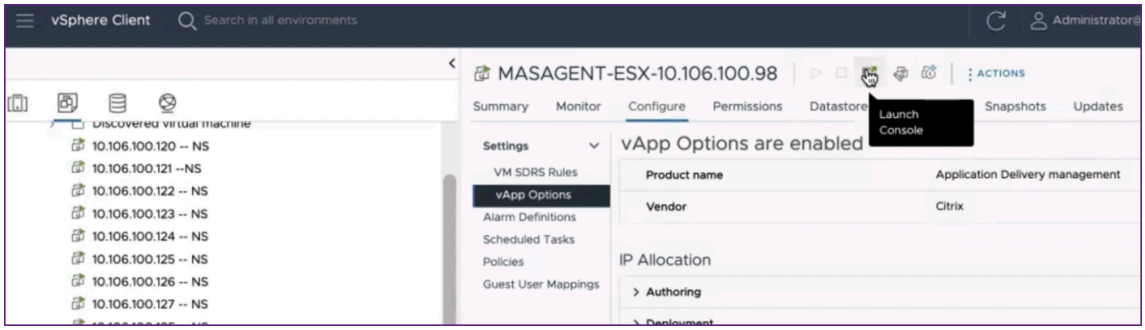
4. Klicken Sie auf die neue virtuelle Appliance, die Sie installiert haben, und navigieren **Sie zu Konfiguration > Einstellungen > vApp-Optionen > Bearbeiten**.
5. Navigieren **Sie im Fenster „vApp-Optionen bearbeiten** “zu **In den OVF-Details > OVF-Umgebungstransport**und wählen Sie **VMware Tools**aus. Klicken Sie auf **OK**.

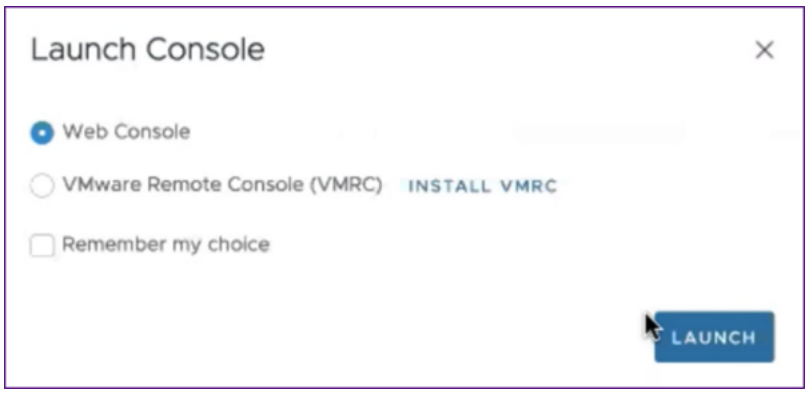


6. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie **auf Einschalten**. Als Alternative können Sie die Registerkarte **Zusammenfassung** der virtuellen Maschine auswählen und **auf Einschalten**klicken.

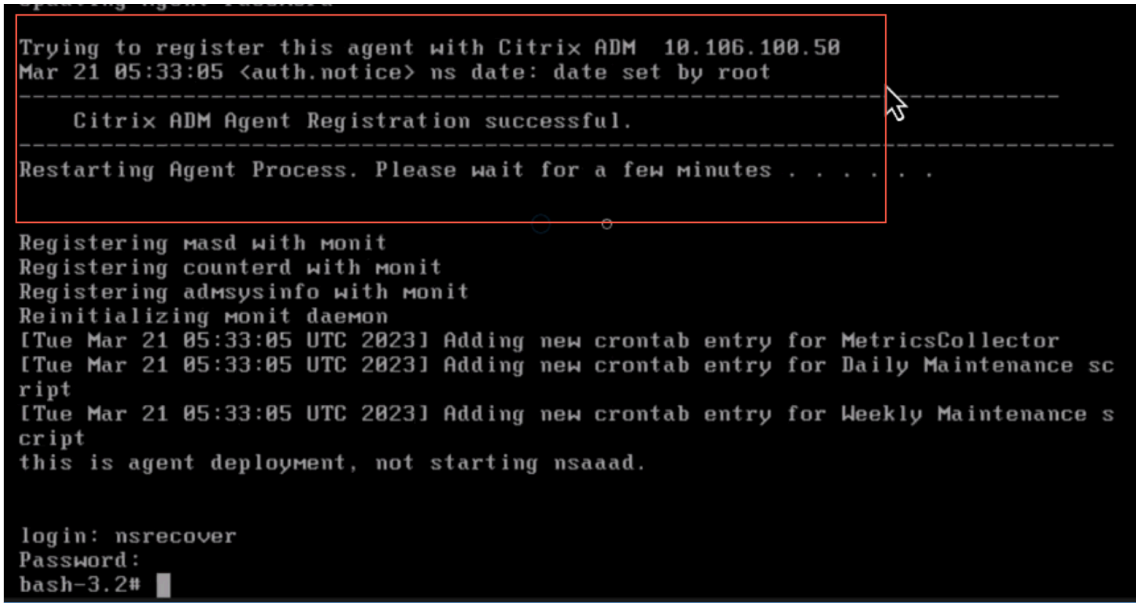


7. Wählen Sie auf der Registerkarte **Zusammenfassung** die Option **Webkonsole starten**aus. Wählen **Sie im Fenster Startkonsole** die Option **Web-Konsole**aus. Klicken Sie auf **Starten**.





8. In der Konsole wird eine Meldung über eine erfolgreiche Registrierung angezeigt, nachdem der NetScaler ADM Agent auf dem NetScaler ADM-Server registriert wurde. Um zu überprüfen, ob der NetScaler ADM Agent bereitgestellt und das Standardkennwort geändert wurde, melden Sie sich mit dem NetScaler ADM
   Agent-Benutzernamen und dem neuen Kennwort an.



Überprüfen

Gehen Sie wie folgt vor, um zu überprüfen, ob der NetScaler ADM-Agent bereitgestellt ist:

1. Nachdem der NetScaler ADM Agent bereitgestellt wurde, greifen Sie auf die NetScaler ADM GUI zu, indem Sie die
   IP-Adresse des NetScaler ADM-Servers in den Browser eingeben.
2. Loggen Sie sich mit Ihren Anmeldeinformationen auf dem Server ein.
3. Navigieren Sie zu **Infrastruktur > Instanzen > Agents**.
   Der neu bereitgestellte Agent wird auf der ESX-Plattform angezeigt.

NetScaler ADM im Kubernetes-Cluster

February 5, 2024

Lesen Sie den Abschnitt “Voraussetzungen”, bevor Sie virtuelle NetScaler ADM Appliances auf einem Kubernetes-Cluster installieren.

Voraussetzungen

Stellen Sie vor der Installation von ADM sicher, dass die folgenden Voraussetzungen erfüllt sind.

Kubernetes-Cluster

- Der Kubernetes-Cluster muss die folgende Version oder höher haben:
  - Serverversion v1.20
  - Clientversion v1.20

  Geben Sie den Befehl ein `kubectl version`, um die Version zu überprüfen.
- Die auf dem Cluster installierte Helm-Anwendung muss über die Clientversion v3.4.0 oder höher verfügen.

  Verwenden Sie den Befehl `helm version`, um die Version zu überprüfen.
- Der Kubernetes-Cluster CNI (Container Network Interface) muss Calico Version v3.21.1 oder höher sein.
- Auf allen untergeordneten Knoten im Cluster muss ein NFS-Client installiert sein. Dies liegt daran, dass die ADM-Anwendung die Daten und die Konfiguration auf Volumes, die auf einem Netzwerkdateiserver bereitgestellt werden, beibehalten. Um einen NFS-Client auf einem Ubuntu-basierten Untergebenen zu installieren, geben Sie die folgenden Befehle ein:

```
apt-get update
apt install nfs-common
```

- Die ADM-Anwendung benötigt 32 GB Arbeitsspeicher und 8 vCPUs im Cluster und 120 GB Speicherplatz auf NFS.

NFS-Freigabe

Die ADM-Anwendung benötigt persistente Volumes zum Speichern von Daten wie Konfiguration, Zertifikaten, Images und anderen. Zu diesem Zweck benötigt ADM NFS-Mounts. Die Anwendung benötigt zwei Ordner aus den freigegebenen Netzwerkeinhängungen:

- Eine zum Speichern von Dateien wie Zertifikaten, Images und anderen
- Die andere für die Datenbank

> Hinweis:
>
> Es wird empfohlen, ein NFS mit einer SSD zu haben.

Diese beiden Ordner können unterschiedlich oder gleich sein. Beide Ordner müssen 777 Berechtigungen haben. Der erste Ordner muss mindestens 10 GB Speicherplatz haben. Die Größe des zweiten Ordners hängt von der Datenmenge ab, die in der Datenbank dauerhaft sein muss. Die Mindestgröße beträgt 100 GB.
Für die Produktionsumgebung empfehlen wir eine NFS-Lösung in Produktionsqualität.

NetScaler Appliance

Die NetScaler Appliance ist als Eingangsgerät erforderlich. ADC stellt die erforderlichen Anwendungsdienste außerhalb des
Kubernetes-Clusters zur Verfügung. Die NetScaler Appliance muss sich außerhalb des Kubernetes-Clusters befinden, und die Workerknoten müssen über den ADC erreichbar sein. Gehen Sie wie folgt vor:

- Konfigurieren Sie ein SNIP auf dem ADC. ADC verwendet dieses SNIP, um die Worker-Knoten des Kubernetes-Clusters zu erreichen.
- Identifizieren Sie eine freie IP-Adresse, die als virtuelle Server-IP-Adresse verwendet werden soll, um die erforderlichen Anwendungsdienste außerhalb des Kubernetes-Clusters verfügbar zu machen.

Installieren von ADM auf Kubernetes Cluster

Gehen Sie folgendermaßen vor, um eine ADM-Appliance in einem Kubernetes-Cluster zu installieren:

1. Gehen Sie zur NetScaler-Website und laden Sie die Datei für das NetScaler ADM Helm Chart für Kubernetes herunter.
2. Extrahieren Sie den heruntergeladenen Helm Chart Tarball in das /var-Verzeichnis des Hauptknotens des Kubernetes-Clusters.
3. Öffnen Sie die `values.yaml`Datei unter dem `/var/citrixadm`Verzeichnis.
4. Geben Sie ein Kennwort für die Datenbank in das Feld `dbpasswd` in der Datei ein.
5. Ändern Sie die folgenden Werte. Die ADM-Anwendung verwendet diese Werte, um die NetScaler Appliance so zu konfigurieren, dass die Dienste für die externe Welt verfügbar sind:

- `ingressIP`: eine im NetScaler für den Zugriff auf die Anwendung konfigurierte virtuelle IP.
- `applicationID`: eine eindeutige ID, um die Ingress-Konfiguration vom Rest der Konfiguration auf der NetScaler Appliance zu unterscheiden.
- `ingressADCIP`: NetScaler IP-Adresse (NSIP), die als Eintritt für die ADM-Anwendung verwendet wird.
- `ingressADCUsername`: ein Benutzername für den Zugriff auf die NetScaler Appliance. Dieser Benutzer muss über Schreibrechte verfügen.
- `ingressADCPassword`: Kennwort für den Benutzernamen.

```
# ingressIP is the Virtual IP configured in the Citrix ADC for accessing the application
ingressIP: "xx.xx.xx.xx"

# coreDumpFilePath is the directory on slave nodes of the cluster which will be used to store core dumps files in case
application runs into faulty state
# this setting is optional
# Admin needs to create this directory on each of the slave nodes and then run the command: "echo <coreDumpFilePath_value>/
core.%h.%e.%p > /proc/sys/kernel/core_pattern"
coreDumpFilePath: "/var/mps/cores"

# applicationID is the identifier for ingress configuration
applicationID: "citrixadm"

# ingressADCIP is the NSIP of the northbound ADC used to expose the ADM application to the outside world
ingressADCIP: "xx.xx.xx.xx"

# ingressADCUsername is the username of the northbound ADC
ingressADCUsername: "nsroot"

# ingressADCUsername is the password for above username
ingressADCPassword: "nsroot"
```

6. Ändern Sie die folgenden Werte im **Speicherbereich** . Diese Werte geben die Persistenz an, die zum Speichern von Dateien erforderlich ist, die von der ADM-Anwendung benötigt werden.

   - `nfsServer`: Host-Name oder IP-Adresse des NFS-Servers
   - `path`: mounten Sie den Pfad für den Ordner, um Anwendungsdateien zu speichern.
   - `size`: mindestens 10 GB.

   > Hinweis
   >
   > Die Einheit für diesen Wert ist Gi. Zum Beispiel 10Gi, 20Gi.

7. Wechseln Sie zum **Speicherbereich** unter, `pg-datastore`und ändern Sie die folgenden Werte. Diese Werte geben die Persistenz an, die zum Erstellen einer Datenbank verwendet wird.

   - `nsfServer`: Hostname oder IP-Adresse des NFS-Servers.
   - `size`: mounten Sie einen Pfad für den Ordner, der für den Datenspeicher verwendet wird.
   - `path`: mindestens 100 GB.

   > Hinweis
   >
   > Die Einheit für diesen Wert ist Gi. Beispiel: 100Gi, 200Gi.

8. Gehen Sie zum Verzeichnis /var/citrix im Hauptknoten und führen Sie den folgenden Befehl aus, um eine ADM-Anwendung zu installieren:
   `helm install -n citrixadm --namespace <name> ./citrixadm`

   > Hinweis
   >
   > Dieser Helm-Befehl wird in der Helm-Version 3.x nicht unterstützt.

   Mit diesem Befehl werden auch die erforderlichen Pods in Ihrem Cluster installiert. Namespace-Argument ist optional. Wenn kein Namespace bereitgestellt wird, installiert Helm ADM im Standard-Namespace. Um die Verwaltung zu vereinfachen, installieren Sie ADM unter einem separaten Namespace.

9. Öffnen Sie Ihren Browser und geben Sie `http://< virtual server IP address >` ein und melden Sie sich mit den Anmeldeinformationen `nsroot`/`nsroot` beim ADM an. Für sicheren Zugriffstyp `https://< virtual server IP address >`.

> Hinweis
>
> Während der Bereitstellung erstellt die ADM-Anwendung Tabellen im Datenspeicher, was eine Weile dauern kann. Abhängig von den Ressourcen, die Kubernetes verschiedenen Pods der ADM-Anwendung zugewiesen haben, kann es 5 bis 15 Minuten dauern, bis der Dienst auftaucht.

NetScaler ADM auf Linux KVM-Server

February 5, 2024

Zu den Virtualisierungsplattformen, auf denen das NetScaler Application Delivery Management (ADM) bereitgestellt werden kann, gehört Linux-KVM.

Stellen Sie vor der Installation von NetScaler ADM auf Linux-KVM sicher, dass Ihr System über die Hardwarevirtualisierungserweiterungen verfügt, und stellen Sie sicher, dass die CPU-Virtualisierungserweiterungen verfügbar sind. Stellen Sie sicher, dass `virsh` (ein Befehlszeilentool zur Verwaltung virtueller Maschinen) auf dem Hypervisor verfügbar ist.

Verwenden Sie Ihre Administratoranmeldeinformationen, um sich bei der Citrix.com-Website anzumelden, auf die neuesten NetScaler ADM -Setupdateien zuzugreifen und sie auf Ihren Computer herunterzuladen. Installieren Sie dann den NetScaler ADM auf Ihrer Linux-KVM-Plattform und konfigurieren Sie ihn für Ihr Netzwerk.

Voraussetzungen

Stellen Sie vor der Installation der virtuellen NetScaler ADM-Appliance sicher, dass Linux-KVM-Version 3.6.11-4 und höher auf Hardware installiert ist, die die Mindestanforderungen erfüllt.

Hardwareanforderungen

Komponente	Voraussetzung
CPU	Ein 64-Bit-x86-Prozessor mit den Hardware-Virtualisierungsfunktionen, die im Intel VT-X Prozessor enthalten sind. Stellen Sie mindestens 2 CPU-Kerne bereit, um Linux-KVM zu hosten. **Hinweis** Um zu testen, ob Ihre CPU Linux-Host unterstützt, geben Sie an der Linux-Shell-Eingabeaufforderung den folgenden Befehl ein: `*. egrep'^flags.\* ( vmx | svm )'/proc/cpuinfo*` Wenn die BIOS-Einstellungen für die Erweiterung deaktiviert sind, müssen Sie sie im BIOS aktivieren. Es gibt keine spezifische Empfehlung für die Prozessorgeschwindigkeit, aber höher die Geschwindigkeit, desto besser ist die Leistung des NetScaler ADM.
Speicher (RAM)	Mindestens 4 GB für den Host-Linux-Kernel. Fügen Sie nach Bedarf für die VMs zusätzlichen Speicher hinzu.
Festplatte	Berechnen Sie den Speicherplatz für den Host-Linux-Kernel und die VM-Anforderungen. Eine einzelne NetScaler ADM VM benötigt 120 GB Festplattenspeicher.

> **Hinweis**
>
> Die angegebenen Speicher- und Festplattenanforderungen gelten für die Bereitstellung von NetScaler ADM auf der OpenStack-Plattform, da keine anderen virtuellen Maschinen auf dem Host ausgeführt werden. Die Hardwareanforderungen für OpenStack hängen von der Anzahl der virtuellen Maschinen ab, die darauf ausgeführt werden.

Softwareanforderungen

Citrix empfiehlt neuere Kernel, z. B. die 64-Bit-Version des 3.6.11-4-Kernels oder höher.

Netzwerkanforderungen NetScaler ADM unterstützt nur eine von VirtIO paravirtualisierte Netzwerkschnittstelle. Stellen Sie sicher, dass Sie diese Schnittstelle mit dem Verwaltungsnetzwerk des Linux-KVM-Hosts verbinden, damit NetScaler ADM und Linux-KVM kommunizieren können.

NetScaler ADM -Setupdateien herunterladen

NetScaler ADM-Setupdateien von `www.citrix.com` herunterladen:

1. Öffnen Sie einen Webbrowser und geben Sie www.citrix.com in die Adressleiste ein.
2. Zeigen Sie mit der Maus auf die Option **Anmelden**, klicken Sie auf **My Account**, geben Sie Ihre Citrix Anmeldeinformationen ein, und klicken Sie dann erneut auf **Anmelden**.
3. Navigieren Sie zum Abschnitt **Downloads**.
4. Wählen Sie in der **Download-Liste** die Option **NetScaler Application Delivery Management**aus.
5. Wählen Sie auf der Seite **NetScaler Application Delivery Management** die Version aus. Wählen Sie beispielsweise **Version 13.0**aus.
6. Klicken Sie auf **Produktsoftware**, um sie zu erweitern, und klicken Sie auf den neuesten Build. Wählen Sie beispielsweise **NetScaler MAS Release (Feature Phase) 13.0**Build 36.27 aus.

   Die ausgewählte Build-Seite wird angezeigt.
7. Wählen Sie in der Liste **Zum Download springen** die Option **NetScaler MAS Image für KVM, 13.0 Build xx.xx**
8. Klicken Sie auf **Datei herunterladen**, akzeptieren Sie die EULA und laden Sie die komprimierte Image-Datei in einen beliebigen Ordner auf Ihrem lokalen Computer herunter.

Installieren Sie das NetScaler Application Delivery Management auf Linux-KVM

1. Melden Sie sich mit SSH am KVM-Host an.
2. Kopieren Sie das Bild an der CLI-Eingabeaufforderung mithilfe eines der Dateiübertragungsprogramme in einen Ordner auf dem Server.
3. Navigieren Sie zu dem Verzeichnis, in dem Sie das heruntergeladene Bild gespeichert haben.
4. Führen Sie diese in der Befehlszeile aus:

a) Listet die Dateien im Verzeichnis auf und überprüft das Vorhandensein der Image-Datei.

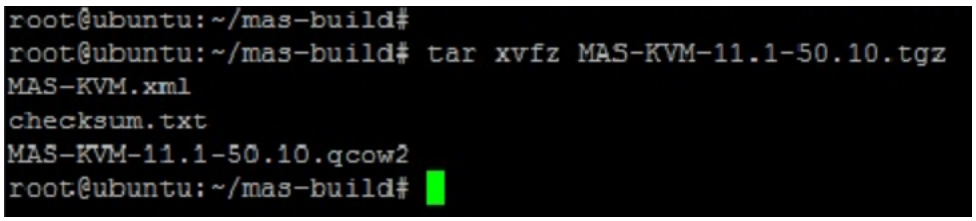
b) Verwenden Sie den Befehl tar, um die NetScaler Application Delivery Management-Imagedatei zu entpacken. Das entpackte Paket enthält die folgenden Komponenten:

i. Eine Domänen-XML-Datei, die die NetScaler ADM-Attribute spezifiziert

ii. Eine Textdatei, die die Prüfsumme des Domain-Disk-Images angibt

iii. Ein Domänendatenträgerimage

```
tar -xvfz MAS-KVM.tgz
MAS-KVM.xml
MAS-KVM.qcow2
checksum.txt
<!--NeedCopy-->
```



iv. Erstellen Sie eine Kopie von MAS-kvm.xml als Mas1-kvm.xml als Backupoption. Öffnen Sie die Datei MAS1-KVM.xml mit dem vi-Editor.

v. Bearbeiten Sie mas1-kVM.xml für die folgenden Netzwerkattribute:

A. `name` - Geben Sie den Namen an.

B. `mac` - Geben Sie die MAC-Adresse an.

C. `source file` - Geben Sie den absoluten Disk-Image-Quellpfad an. Der Dateipfad muss absolut sein.

> **Hinweis**
>
> Der Domänenname und die MAC-Adresse müssen eindeutig sein.

D. `mode` - Geben Sie den Modus an.

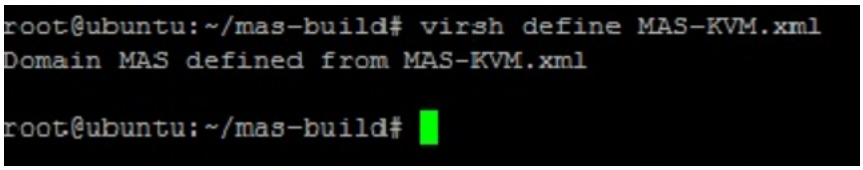
E. `model type` - Stellen Sie auf VirtIO.

F. `source dev` - Geben Sie das Interface an.

```
<name> MAS1-KVM</name>
<mac address='52:54:00:29:74:b3'/>
<source file='/var/ MAS-KVM.qcow2'/>
<source dev='eth0' mode='bridge'/>
<model type='virtio'/>
<!--NeedCopy-->
```

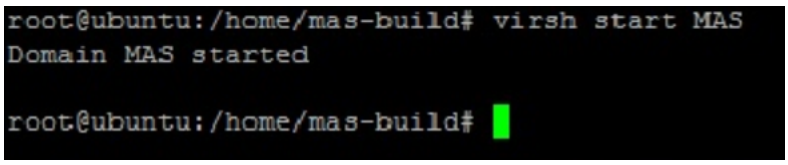

vi. Definieren Sie die VM-Attribute in der Datei MAS1-KVM.xml mit dem folgenden Befehl: `virsh define \<FileName\>.xml`

```
virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml
<!--NeedCopy-->
```



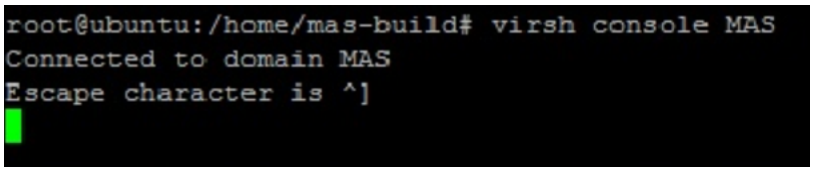
vii. Starten Sie den NetScaler ADM, indem Sie den folgenden Befehl eingeben: `virsh start \[\<DomainName\> | \<DomainUUID\>\]`

```
virsh start MAS
Domain MAS started
<!--NeedCopy-->
```



viii. Sie können eine Verbindung mit der virtuellen NetScaler ADM-Maschine herstellen, indem Sie den folgenden Befehl verwenden: `virsh console \<DomainName\>`

```
virsh console MAS
Connected to domain MAS
Escape character is ^]
<!--NeedCopy-->
```



Konfigurieren Sie das NetScaler Application Delivery Management

> **Hinweis**
>
> Auf einigen Linux-KVM-Hosts können FreeBSD-Gäste nicht ordnungsgemäß neu starten, wenn sie über mehr als eine CPU verfügen. Wenn die virtuelle NetScaler ADM-Appliance neu gestartet wird, reagieren die NetScaler ADM CLI und die GUI nicht mehr. Einzelheiten finden Sie unter https://bugs.launchpad.net/qemu/+bug/1329956
>
> Um zu vermeiden, dass die NetScaler ADM CLI und die GUI beim Neustart der virtuellen NetScaler

> ADM-Appliance nicht mehr reagiert, fahren Sie alle virtuellen Maschinen auf dem KVM-Host herunter und führen Sie Folgendes auf dem KVM-Host aus:
>
> 1. Entfernen Sie das kvm_intel-Modul mit dem folgenden Befehl:
>   `rmmod kvm\\_intel`
> 2. Deaktivieren Sie **ApicV** und laden Sie das kvm_intel-Modul mit dem folgenden Befehl neu:
>   `modprobe kvm\\_intel enable\\_apicv=N`
> 3. Starten Sie die virtuellen Maschinen auf dem KVM-Host.

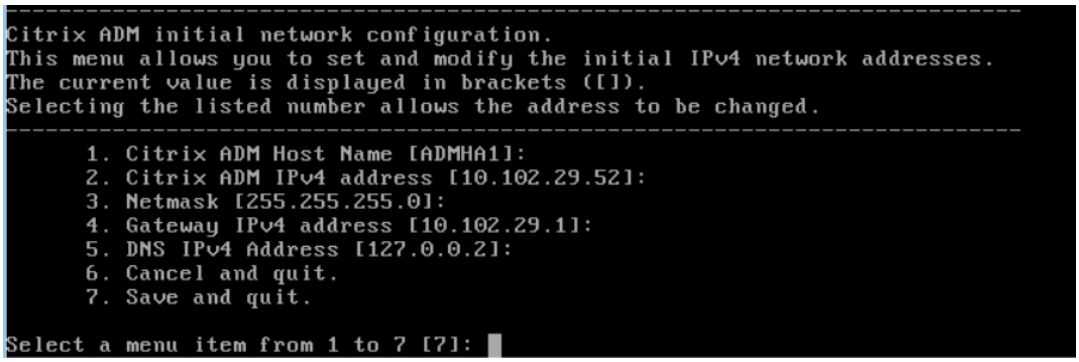
Nach der Installation des NetScaler ADM können Sie etwa 10 Minuten einplanen, bis die Dienste verfügbar werden, und melden Sie sich dann beim NetScaler ADM an.

1. Verwenden Sie in der Befehlszeile die standardmäßigen Anmeldeinformationen des Systemadministrators, um sich am System anzumelden:
   - Benutzername: `nsroot`
   - Kennwort: `nsroot`

   > **Hinweis**
   >
   > Nachdem Sie sich zum ersten Mal angemeldet haben, ändern Sie das Administratorkennwort. Konfigurieren Sie dann den MAS so, dass er in Ihrem Netzwerk funktioniert. Sie können das Kennwort über die NetScaler ADM Benutzeroberfläche ändern. Navigieren Sie auf der NetScaler ADM-Homepage zu **Einstellungen > Benutzerverwaltung > Benutzer**. Wählen Sie den Benutzer aus, klicken Sie auf **Bearbeiten**, und aktualisieren Sie das Kennwort im Feld Kennwort.

2. Geben Sie an der Eingabeaufforderung Folgendes ein: *shell*
3. Geben Sie **networkconfig** ein, um das NetScaler ADM-Menü für die erste Netzwerkkonfiguration aufzurufen. Konfigurieren Sie die Management-IP-Adresse.
4. Folgen Sie den Anweisungen, um die anfängliche Netzwerkkonfiguration von NetScaler ADM abzuschließen. Die Konsole zeigt die anfänglichen Netzwerkkonfigurationsoptionen von NetScaler ADM zum Festlegen der folgenden Parameter für das NetScaler ADM an. Der Hostname wird standardmäßig aufgefüllt.
   a) Geben Sie **2** ein, um die NetScaler ADM IPv4-Adresse zu aktualisieren —die Management-IP-Adresse, über die Sie auf ein NetScaler ADM zugreifen
   b) Geben Sie **3** ein, um die Netzmaske zu aktualisieren —die der Management-IP-Adresse zugeordnete Subnetzmaske
   c) Geben Sie **4** ein, um die Gateway-IPv4-Adresse zu aktualisieren —die Standard-Gateway-IP-Adresse für das Subnetz der Management-IP-Adresse des NetScaler ADM

d) Geben Sie **7** ein, um zu speichern und zu beenden - speichert Ihre Konfigurationsänderungen und beendet das System.



5. Führen Sie das Bereitstellungsskript aus, indem Sie den Befehl an der Shell-Eingabeaufforderung eingeben: `deployment_type.py`
6. Wählen Sie im angezeigten Bereitstellungsbildschirm den Bereitstellungstyp als **NetScaler ADM -Server**aus.

7. Geben Sie**Ja**ein, um NetScaler ADM als eigenständige Bereitstellung bereitzustellen.
8. Geben Sie **Ja** ein, um den NetScaler ADM Server neu zu starten.
9. Melden Sie sich nach dem Neustart des NetScaler ADM-Servers über die Befehlszeile oder die GUI bei NetScaler ADM an, indem Sie die standardmäßigen Administratoranmeldeinformationen als nsroot/nsroot verwenden.

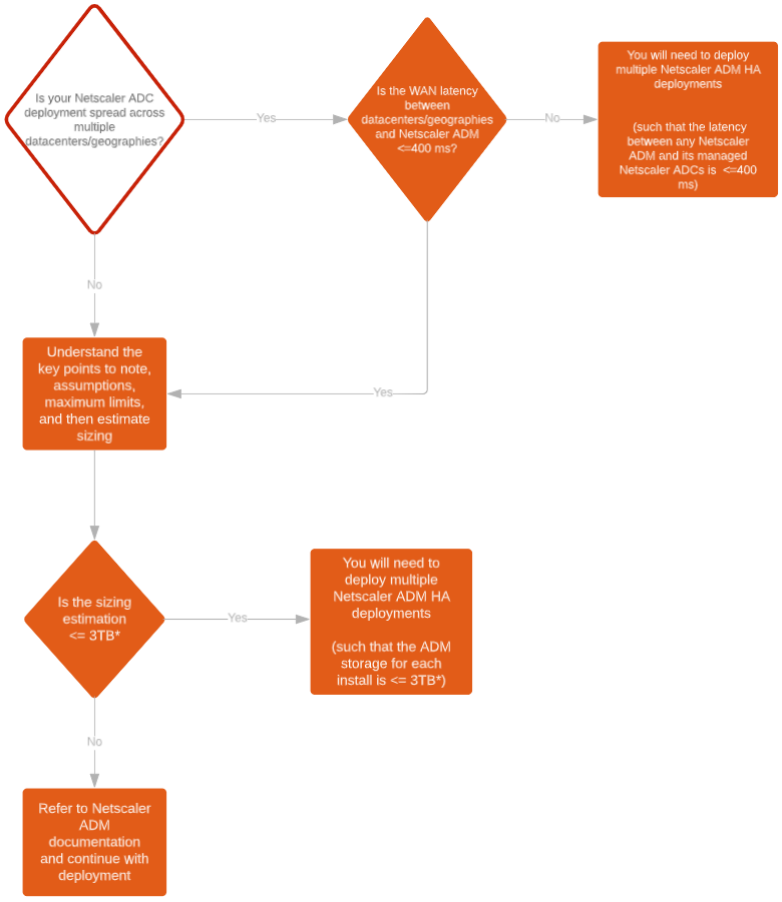
   Sie können später auf das NetScaler ADM zugreifen, indem Sie die IP-Adresse des NetScaler ADM-Servers in die Adressleiste Ihres Browsers eingeben. Die standardmäßigen Administratoranmeldedaten für die Anmeldung am Server sind *nsroot/nsroot*.

Bereitstellung mit hoher Verfügbarkeit konfigurieren

February 5, 2024

Hochverfügbarkeit (HA) bezieht sich auf ein System, das einem Benutzer jederzeit ohne Unterbrechung der Dienste zur Verfügung steht. Die Einrichtung einer hohen Verfügbarkeit ist bei Systemausfällen, Netzwerk- oder Anwendungsausfällen von entscheidender Bedeutung und eine wichtige Anforderung für jedes Unternehmen. Eine Hochverfügbarkeitsbereitstellung von zwei NetScaler ADM-Knoten im aktiv/passiven Modus mit denselben Konfigurationen sorgt für einen unterbrechungsfreien Betrieb.

Bereitstellungsszenario



> **Hinweis**
>
> Das validierte Maximalspeicherlimit für eine einzelne NetScaler ADM HA-Bereitstellung beträgt 3 TB. Weitere Informationen finden Sie im Bereitstellungshandbuch.

> **Wichtig!**
>
> **So greifen Sie mit HTTPS auf NetScaler ADM 12.1 Build 48.18 oder neuere Versionen zu:**
>
> Wenn Sie eine NetScaler-Instanz für den Lastenausgleich von NetScaler ADM in einem Hochverfügbarkeitsmodus konfiguriert haben, entfernen Sie zuerst die NetScaler-Instanz. Konfigurieren Sie dann eine Floating-IP, um im Hochverfügbarkeitsmodus auf NetScaler ADM zuzugreifen.

Im Folgenden sind die Vorteile einer Bereitstellung mit hoher Verfügbarkeit in NetScaler ADM aufgeführt:

- Ein verbesserter Mechanismus zur Überwachung der Herzschläge zwischen dem primären und sekundären Knoten.
- Ermöglicht eine physische Streaming-Replikation der Datenbank anstelle einer logischen bidirektionalen Replikation.
- Möglichkeit, die Floating-IP auf dem primären Knoten zu konfigurieren, sodass kein separater NetScaler-Load Balancer erforderlich ist.
- Ermöglicht einfachen Zugriff auf die NetScaler ADM-Benutzeroberfläche mithilfe der Floating-IP.
- Die NetScaler ADM-Benutzeroberfläche ist nur auf dem primären Knoten verfügbar. Durch die Verwendung des primären Knotens können Sie das Risiko vermeiden, auf den sekundären Knoten zuzugreifen und Änderungen daran vorzunehmen.
- Durch die Konfiguration der Floating-IP wird die Failover-Situation bewältigt, und eine Neukonfiguration der Instanzen ist nicht erforderlich.
- Bietet eine integrierte Fähigkeit, Split-Brain-Situationen zu erkennen und zu behandeln.

In der folgenden Tabelle werden die Begriffe beschrieben, die bei der Bereitstellung von Hochverfügbarkeit verwendet werden.

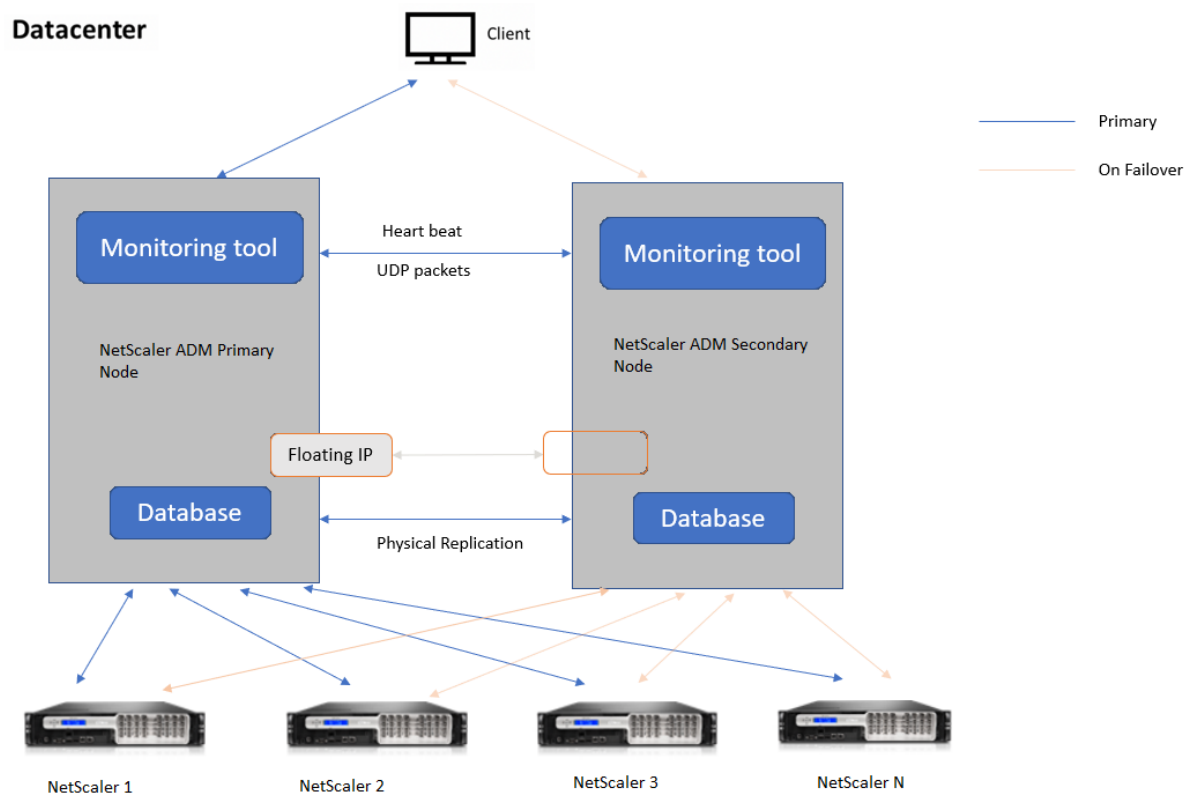
Begriff	Beschreibung
Primärer Knoten	Erster Knoten, der in der Hochverfügbarkeitsbereitstellung registriert wurde.
Sekundärer Knoten	Zweiter Knoten, der in der Hochverfügbarkeitsbereitstellung registriert wurde.

Begriff	Beschreibung
Herzschlag	Ein Mechanismus, der zum Austausch von Nachrichten zwischen primärem und sekundärem Knoten im Hochverfügbarkeits-Setup verwendet wird. Die Nachrichten bestimmen den Status und den Zustand der Anwendung auf jedem einzelnen Knoten.
Floating-IP-Adresse	Eine Floating-IP ist eine IP-Adresse, die sofort von einem Knoten auf einen anderen im selben Subnetz verschoben werden kann. Intern ist es als Alias auf der Netzwerkschnittstelle des primären Knotens eingerichtet. Bei einem Failover wird die Floating-IP nahtlos von der alten primären zur neuen verschoben. Sie ist bei der Einrichtung mit hoher Verfügbarkeit nützlich, da es Clients ermöglicht, mit den Hochverfügbarkeitsknoten über eine einzige IP-Adresse zu kommunizieren.

> **Hinweis**
>
> Weitere Informationen zu Port- und Protokolldetails finden Sie unter Ports.

Komponenten der Hochverfügbarkeitsarchitektur

Die folgende Abbildung zeigt die Architektur von zwei NetScaler ADM Knoten, die im Hochverfügbarkeitsmodus bereitgestellt werden.



In der Hochverfügbarkeitsbereitstellung wird ein NetScaler ADM Knoten als primärer Knoten (MAS 1) und der andere als sekundärer Knoten (MAS 2) konfiguriert. Wenn der primäre Knoten aus irgendeinem Grund ausfällt, übernimmt der sekundäre Knoten als neuer primärer Knoten.

Tool zur Überwachung

Das Überwachungstool ist ein interner Prozess zur Überwachung, Warnung und Behandlung von Failover-Situationen. Das Tool ist aktiv und wird auf jedem Knoten mit hoher Verfügbarkeit ausgeführt. Es ist verantwortlich für das Starten von Subsystemen, die Initiierung der Datenbank auf beiden Knoten, die Entscheidung über den primären oder sekundären Knoten, falls ein Failover vorliegt, usw.

Primärer Knoten

Der primäre Knoten akzeptiert Verbindungen und verwaltet die Instanzen. Alle Prozesse wie AppFlow, SNMP, LogStream, Syslog usw. werden vom primären Knoten verwaltet. Der Zugriff auf die NetScaler ADM-Benutzeroberfläche ist auf dem primären Knoten verfügbar. Die Floating-IP ist auf dem primären Knoten konfiguriert.

Sekundärer Knoten

Der sekundäre Knoten hört sich die vom primären Knoten gesendeten Heartbeat-Nachrichten an. Die Datenbank auf dem sekundären Knoten befindet sich nur im Read-Replikat-Modus. Keiner der Prozesse ist im sekundären Knoten aktiv und auf die NetScaler ADM-Benutzeroberfläche kann auf dem sekundären Knoten nicht zugegriffen werden.

Physische Streaming-Replikation

Die primären und sekundären Knoten synchronisieren sich über den Herzschlagmechanismus. Bei der physischen Streaming-Replikation der Datenbank startet der sekundäre Knoten im Read-Replikat-Modus. Der sekundäre Knoten hört sich die vom primären Knoten empfangenen Heartbeat-Nachrichten an. Wenn der sekundäre Knoten über einen Zeitraum von 180 Sekunden keine Herzschläge empfängt, gilt der primäre Knoten als ausgefallen. Dann übernimmt der sekundäre Knoten die Funktion des primären Knotens.

Heartbeat-Nachrichten

Heartbeat-Nachrichten sind User Datagram Packets (UDP), die zwischen primärem und sekundärem Knoten gesendet und empfangen werden. Es überwacht alle Subsysteme von NetScaler ADM und der Datenbank, um Informationen über den Knotenstatus, den Zustand, Prozesse usw. auszutauschen. Die Informationen werden jede Sekunde zwischen den Hochverfügbarkeitsknoten ausgetauscht. Benachrichtigungen werden als Warnung an den Administrator gesendet, wenn es zu einem Failover kommt oder der Hochverfügbarkeitsstatus unterbrochen wird.

Floating-IP-Adresse

Die Floating-IP ist dem primären Knoten im Hochverfügbarkeits-Setup zugeordnet. Es ist ein Alias, der der IP-Adresse des primären Knotens zugewiesen wurde und den der Client verwenden kann, um eine Verbindung zu NetScaler ADM im primären Knoten herzustellen. Da die Floating-IP auf dem primären Knoten konfiguriert ist, ist die Neukonfiguration der Instanz im Falle eines Failovers nicht erforderlich. Die Instances stellen erneut eine Verbindung mit derselben IP-Adresse her, um die neue primäre Instanz zu erreichen.

Wichtige Punkte, die es zu beachten gilt

- In einem Hochverfügbarkeits-Setup werden beide NetScaler ADM-Knoten im aktiv/passiven Modus bereitgestellt. Sie müssen sich in denselben Subnetzen befinden und dieselbe Softwareversion und denselben Build verwenden und dieselbe Konfiguration haben.

- Floating-IP-Adresse:
  - Die Floating-IP-Adresse ist auf dem primären Knoten konfiguriert.
  - Instanzen müssen nicht neu konfiguriert werden, wenn es zu einem Failover kommt.
  - Sie können über die Benutzeroberfläche auf einen Knoten mit hoher Verfügbarkeit zugreifen, indem Sie entweder die IP-Adresse des primären Knotens oder die Floating-IP verwenden.

    > **Hinweis**
    >
    > Citrix empfiehlt, die Floating-IP für den Zugriff auf die Benutzeroberfläche zu verwenden.

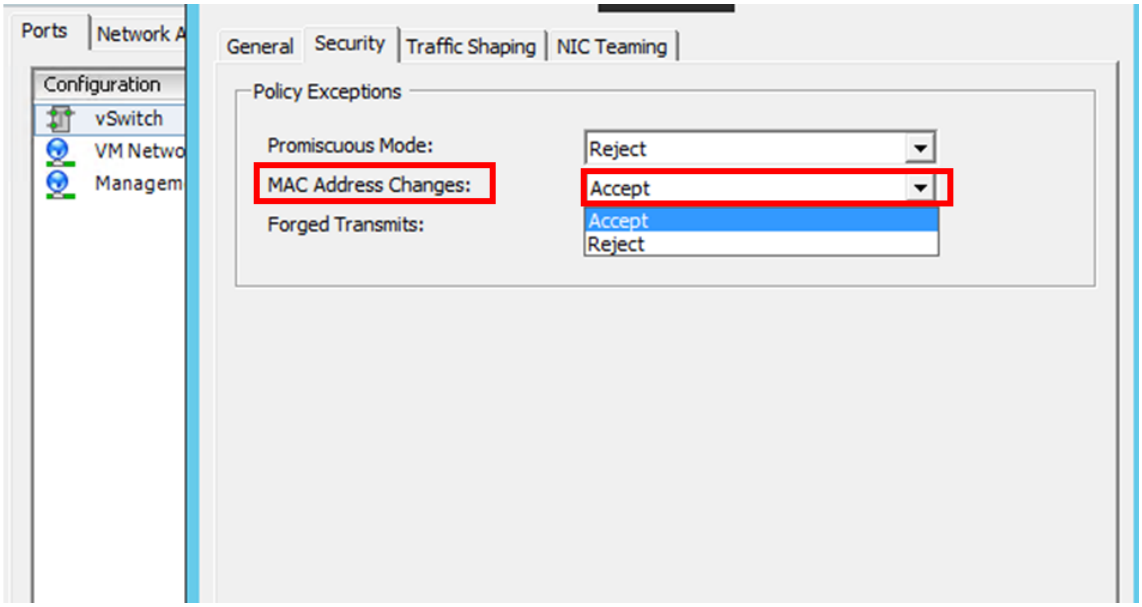
- Datenbank:
  - In einem Hochverfügbarkeits-Setup werden alle Konfigurationsdateien im Abstand von einer Minute automatisch vom primären Knoten zum sekundären Knoten synchronisiert.
  - Die Datenbanksynchronisierung erfolgt sofort durch physische Replikation der Datenbank.
  - Die Datenbank auf dem sekundären Knoten befindet sich im Read-Replikat-Modus.

- NetScaler ADM Upgrade:
  - Interne Prozesse führen implizit ein Upgrade von NetScaler ADM gegenüber früheren Versionen durch.

    > **Hinweis**
    >
    > Nach erfolgreichem Upgrade müssen Sie die Floating-IP konfigurieren.

- Der UDP-Standardport 5005 ist auf beiden Knoten für das Senden von Heartbeats und für das Empfangen von Nachrichten verfügbar.
- MAC-Adresse
  Die Einstellung für die Option „MAC-Adressänderungen“in einem Hypervisor wirkt sich auf den Datenverkehr aus, den eine virtuelle Maschine empfängt. Zulassen, dass MAC-Adressänderungen auf dem virtuellen Switch aktiviert werden, sodass die schwebende IP-Adresse nach dem Failover nahtlos auf den neuen primären Knoten verschoben wird.
  Stellen Sie beispielsweise bei der Bereitstellung von NetScaler ADM mit hoher Verfügbarkeit auf VMware ESXi sicher, dass Sie Änderungen an der MAC-Adresse akzeptieren. ESXi ermöglicht nun Anforderungen, die aktive MAC-Adresse in eine andere als die ursprüngliche MAC-Adresse zu ändern.

> **Hinweis:**
>
> **Für NetScaler ADM, das auf ESXI Version 6.7 bereitgestellt wird, können Sie die Option**MAC-Adressänderungen**auch auf Ablehnen setzen.** Nach dem Failover fließt der Datenverkehr unabhängig von der Einstellung für **MAC-Adressänderungen** nahtlos zum neuen primären Knoten. Daher ist es nicht zwingend erforderlich, Änderungen an der MAC-Adresse zu akzeptieren.
>
> Wenn NetScaler ADM auf der ESXI-Version kleiner als 6.7 bereitgestellt wird, stellen Sie sicher, dass die Option **MAC-Adressänderungen** auf Nur **akzeptieren** festgelegt ist.



Voraussetzungen

Bevor Sie die Hochverfügbarkeit für NetScaler ADM-Knoten einrichten, beachten Sie die folgenden Voraussetzungen:

- Die NetScaler ADM-Hochverfügbarkeitsbereitstellung wird ab NetScaler ADM Version 12.0 Build 51.24 unterstützt.
- Laden Sie die NetScaler Application Delivery Management-Imagedatei (.xva) von der NetScaler-Website herunter: https://www.citrix.com/downloads/

Citrix empfiehlt, dass Sie die CPU-Priorität (in den Eigenschaften der virtuellen Maschine) auf der höchsten Ebene festlegen, um das Planungsverhalten und die Netzwerklatenz zu verbessern.

In der folgenden Tabelle sind die Mindestanforderungen für die virtuellen Computerressourcen aufgeführt:

Komponente	Voraussetzung
RAM	**32 GB**
Virtuelle CPU	**8 CPUs**
Stauraum	Citrix empfiehlt die Verwendung der Solid-State-Drive-Technologie (SSD) für NetScaler ADM-Bereitstellungen. Der Standardwert ist 120 GB. Die tatsächliche Speicheranforderung hängt von der Schätzung der NetScaler ADM Größe ab. Wenn Ihre NetScaler ADM Speicheranforderung 120 GB überschreitet, müssen Sie einen zusätzlichen Datenträger bereitstellen. **Hinweis:** Sie können nur eine zusätzliche Festplatte hinzufügen. Citrix empfiehlt, zum Zeitpunkt der Erstbereitstellung den Speicher zu schätzen und zusätzlichen Datenträger anzuhängen. Weitere Informationen finden Sie unter So hängen Sie eine zusätzliche Festplatte an NetScaler ADM an .
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s oder 100 Mbit/s
Hypervisor	**Versionen**
Citrix Hypervisor	6.2 und 6.5
VMware ESXi	5.5 und 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu und Fedora

So richten Sie NetScaler ADM im Hochverfügbarkeitsmodus ein

1. Registrieren Sie den ersten Server (primärer Knoten) und stellen Sie ihn bereit.
2. Registrieren Sie den zweiten Server (sekundärer Knoten) und stellen Sie ihn bereit.
3. Stellen Sie den primären und sekundären Knoten für das Hochverfügbarkeits-Setup bereit.

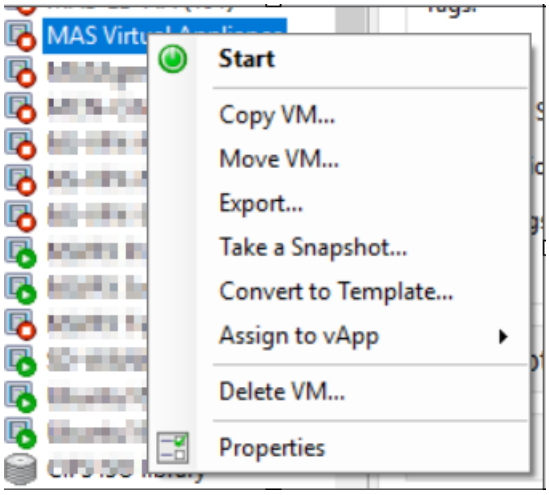
Registrieren und Bereitstellen des ersten Servers (primärer Knoten)

Um den ersten Knoten zu registrieren:

1. Verwenden Sie die XVA-Image-Datei, die Sie von der NetScaler-Site heruntergeladen haben, und importieren Sie sie in Ihren Hypervisor.

   > **Hinweis:**
   >
   > Es kann einige Minuten dauern, bis die XVA-Imagedatei importiert und gestartet wird. Sie können den Status unten auf dem Bildschirm sehen.
   >
   >
   >

2. Nachdem der Import erfolgreich ist, klicken Sie mit der rechten Maustaste, und klicken Sie auf **Start**.

3. Konfigurieren Sie auf der Registerkarte **Konsole** NetScaler ADM mit den anfänglichen Netzwerkkonfigurationen.

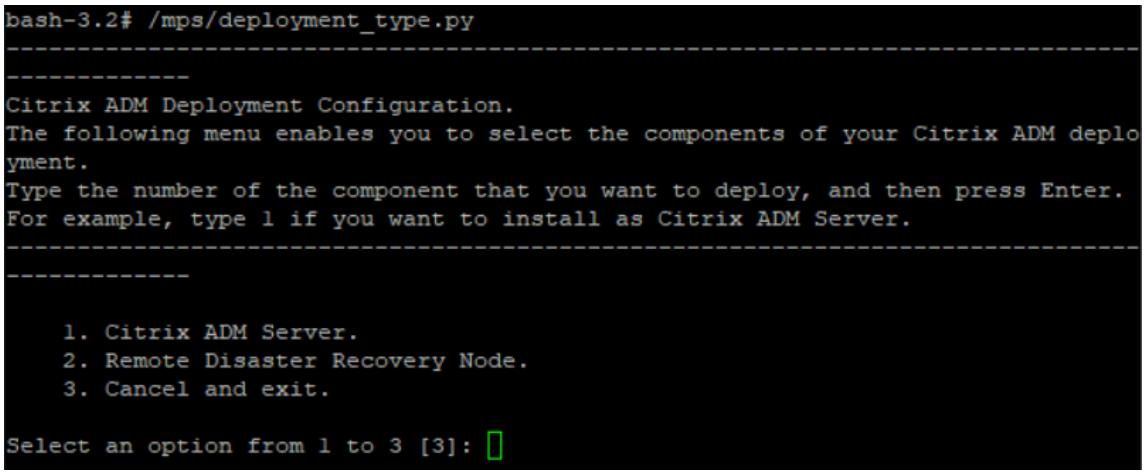
   

4. Nachdem die anfängliche Netzwerkkonfiguration abgeschlossen ist, fordert das System zur Anmeldung auf. Melden Sie sich mit den folgenden Anmeldeinformationen an: *nsrecover/nsroot*.

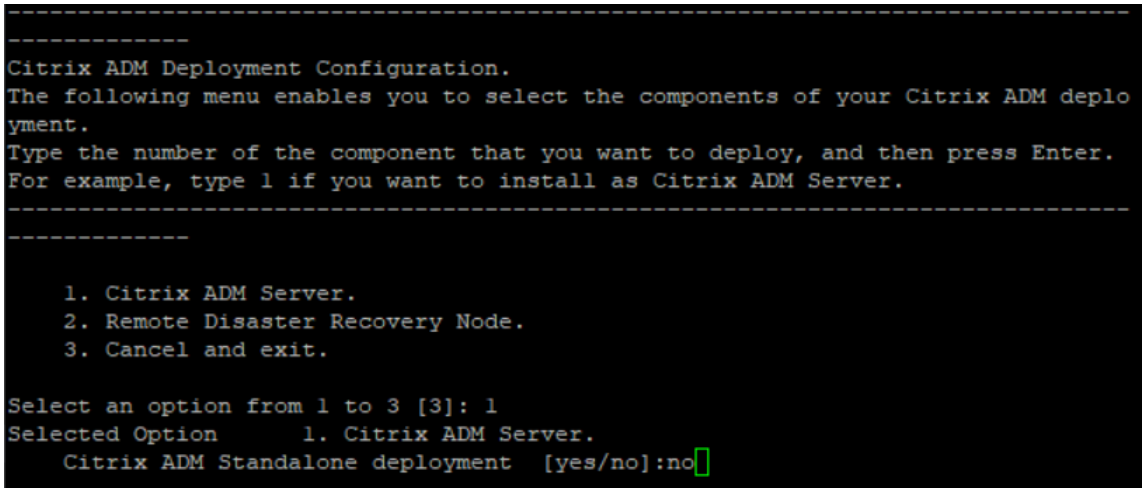
> **Hinweis**
>
> Wenn Sie sich nach der Anmeldung die anfängliche Netzwerkkonfiguration aktualisieren möchten, geben Sie die Konfiguration ein `networkconfig`, aktualisieren Sie sie und speichern Sie die Konfiguration.

5. Geben Sie **/mps/deployment_type.py**ein, um den primären Knoten bereitzustellen. Das Konfigurationsmenü für die NetScaler ADM Bereitstellung wird angezeigt.

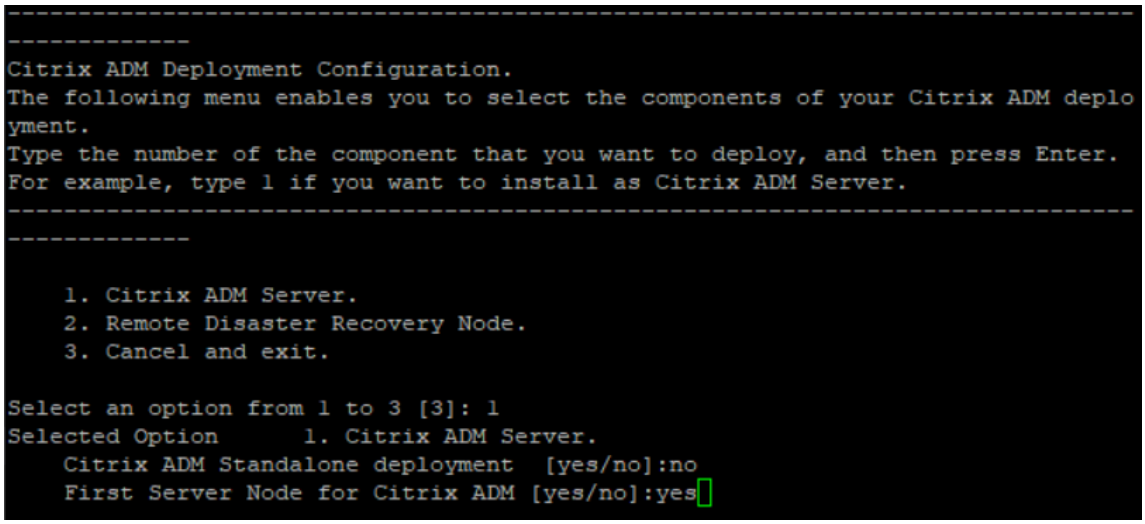
6. Wählen Sie **1** aus, um den NetScaler ADM -Server als primären Knoten zu registrieren.



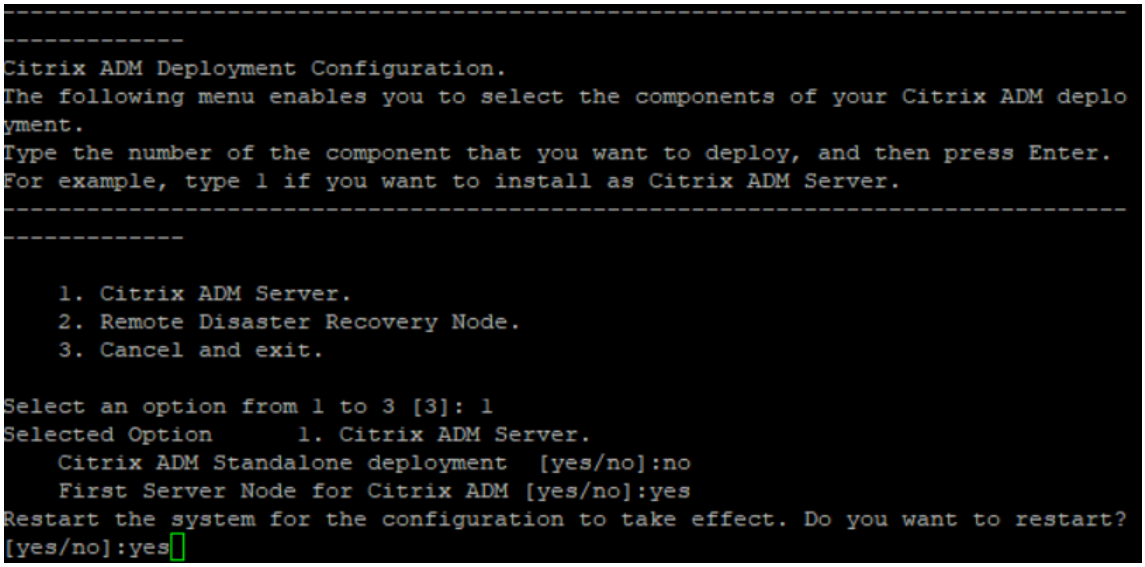
7. Die Konsole fordert Sie auf, die eigenständige NetScaler ADM Bereitstellung auszuwählen. Geben Sie**Nein** ein, um die Bereitstellung als Hochverfügbarkeit zu bestätigen.



8. Die Konsole fordert Sie auf, den ersten Serverknoten auszuwählen. Geben Sie**Ja** ein, um den Knoten als ersten Knoten zu bestätigen.



9. Die Konsole fordert Sie auf, das System neu zu starten. Geben Sie **Ja** ein, um neu zu starten.



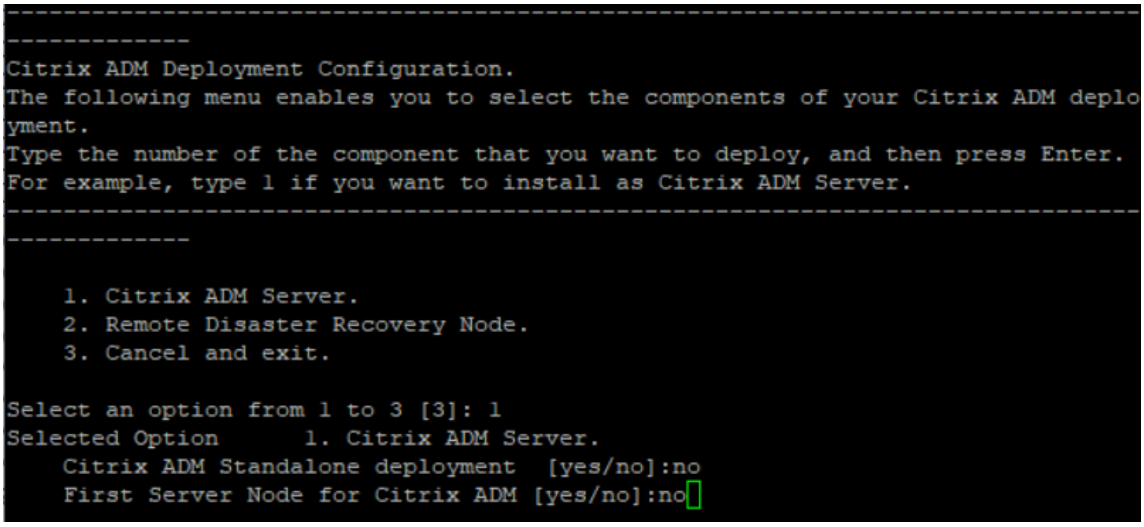
Das System wird neu gestartet und als primärer Knoten in der NetScaler ADM Benutzeroberfläche angezeigt.

Registrieren und Bereitstellen des zweiten Servers (sekundärer Knoten)

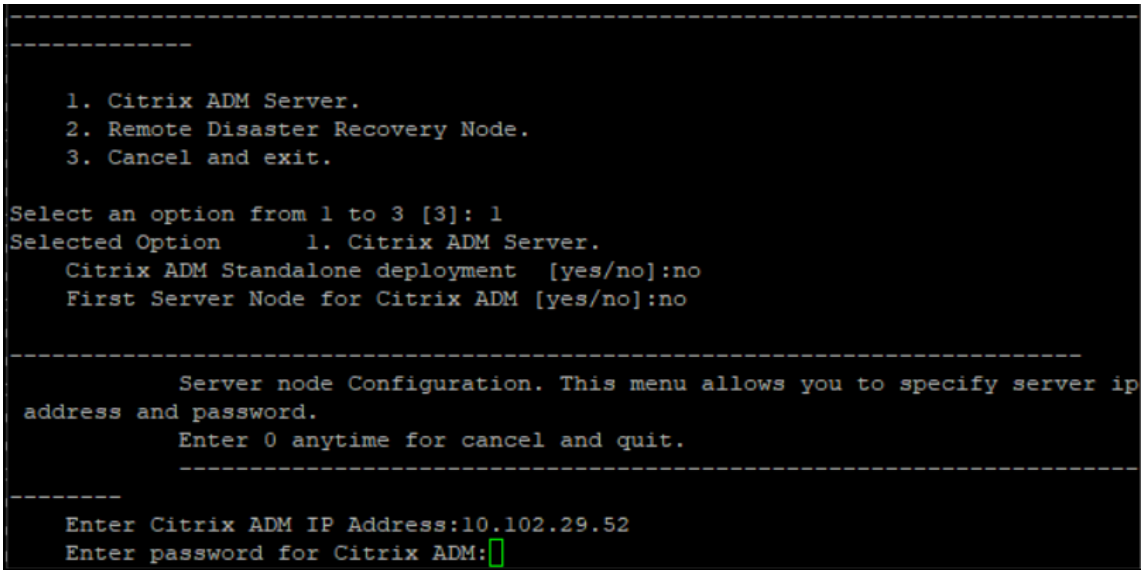
1. Verwenden Sie die **XVA-Image-Datei**, die Sie von der NetScaler-Site heruntergeladen haben, und importieren Sie sie in Ihren Hypervisor.
2. Konfigurieren Sie NetScaler ADM auf der Registerkarte **Konsole** mit den anfänglichen Netzwerkkonfigurationen, wie in der folgenden Abbildung dargestellt.
3. Nachdem die anfängliche Netzwerkkonfiguration abgeschlossen ist, fordert das System zur Anmeldung auf. Melden Sie sich mit den folgenden Anmeldeinformationen an: *nsrecover/nsroot*.

   > **Hinweis**
   >
   > Wenn Sie sich nach der Anmeldung die anfängliche Netzwerkkonfiguration aktualisieren möchten, geben Sie die Konfiguration ein `networkconfig`, aktualisieren Sie sie und speichern Sie die Konfiguration.

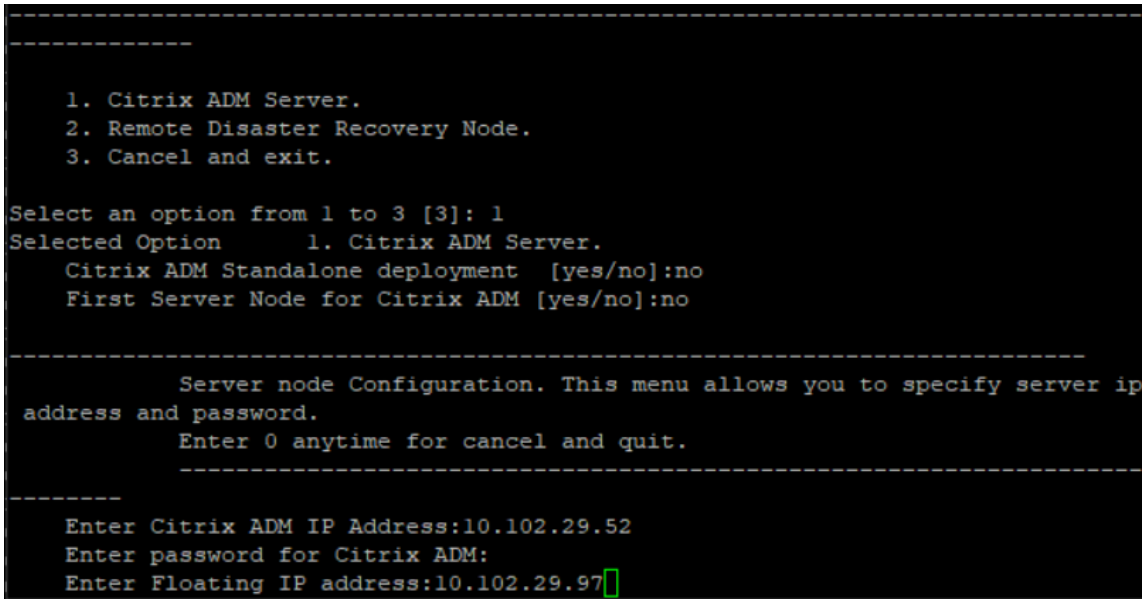
4. Geben Sie **/mps/deployment_type.py**ein, um den sekundären Knoten bereitzustellen. Das Konfigurationsmenü für die NetScaler ADM Bereitstellung wird angezeigt.
5. Wählen Sie **1** aus, um den NetScaler ADM-Server als sekundären Knoten zu registrieren.
6. Die Konsole fordert Sie auf, NetScaler ADM als eigenständige Bereitstellung auszuwählen. Geben Sie**Nein** ein, um die Bereitstellung als Hochverfügbarkeit zu bestätigen.
7. Die Konsole fordert Sie auf, den ersten Serverknoten auszuwählen. Geben Sie**Nein** ein, um den Knoten als zweiten Server zu bestätigen.



8. Die Konsole fordert Sie auf, die IP-Adresse und das Kennwort des primären Knotens einzugeben.



9. Die Konsole fordert Sie auf, die schwebende IP-Adresse einzugeben.



10. Die Konsole fordert Sie auf, das System neu zu starten. Geben Sie **Ja** ein, um neu zu starten.

> **Hinweis**
>
> - Eine Floating-IP-Adresse ist für die Bereitstellung von Knoten mit hoher Verfügbarkeit erforderlich.
> - Das System zeigt Fehlermeldungen an, wenn es Probleme mit der Konfiguration gibt.
> - Das System wird neu gestartet und es dauert einige Minuten, bis die Konfigurationen wirksam werden.

Bereitstellen des primären und sekundären Knotens als Hochverfügbarkeitspaar

Nach der Registrierung werden sowohl der primäre als auch der sekundäre Knoten auf der NetScaler ADM-Benutzeroberfläche angezeigt. Stellen Sie diese Knoten in einem Hochverfügbarkeitspaar bereit.

> **Hinweis**
>
> - Bevor Sie die Knoten in einem Hochverfügbarkeitspaar bereitstellen, stellen Sie sicher, dass der sekundäre Knoten nach der ersten Netzwerkkonfiguration mit einem Neustart abgeschlossen ist.
> - Nachdem die Bereitstellung der Hochverfügbarkeit abgeschlossen ist, verwenden Sie die Floating-IP, um auf die NetScaler ADM-Benutzeroberfläche zuzugreifen.

Gehen Sie wie folgt vor, um Knoten als Hochverfügbarkeitspaar bereitzustellen:

1. Öffnen Sie einen Webbrowser und geben Sie die IP-Adresse des ersten NetScaler ADM-Serverknotens ein.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der Startseite auf **Get Started**.
4. Wählen Sie den Bereitstellungstyp als**Zwei Server im Hochverfügbarkeitsmodus**aus, und klicken Sie auf**Weiter**.
5. Klicken Sie auf der Seite Bereitstellung auf**Bereitstellen**.
6. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **Ja**.

   NetScaler ADM wird neu gestartet und dauert etwa 10 Minuten, bis die Konfiguration wirksam wird.

   > **Hinweis**
   >
   > Sie können jetzt die Floating-IP-Adresse verwenden.

7. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler ADM an, klicken **Sie auf der Startseite auf Erste Schritte** und führen Sie optional die folgenden Schritte aus:

   a) Hinzufügen NetScaler-Instanzen

   b) Kundenidentität konfigurieren

   > **Hinweis**
   >
   > Sie können auch auf **Überspringen klicken, um den** Vorgang später abzuschließen, und auf **Fertig stellen**klicken.

8. Navigieren Sie zu **Einstellungen > Bereitstellung**, um die Bereitstellung zu überprüfen.

   Weitere Informationen finden Sie in den Häufig gestellten Fragen.

Hochverfügbarkeit deaktivieren

Sie können die Hochverfügbarkeit auf einem NetScaler ADM-Hochverfügbarkeitspaar deaktivieren und die Knoten in eigenständige NetScaler ADM-Server konvertieren.

> **Hinweis**
>
> Deaktivieren Sie die Hochverfügbarkeit vom primären Knoten aus.

Um die Hochverfügbarkeit zu deaktivieren:

1. Geben Sie in einem Webbrowser die IP-Adresse des primären NetScaler ADM-Serverknotens ein.
2. Geben Sie in die Felder **Benutzername**und**Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte**System** zu**Bereitstellung**, und klicken Sie auf**HA aufheben**.

   Es wird ein Dialog angezeigt. Klicken Sie auf **Ja**, um die Hochverfügbarkeitsbereitstellung zu unterbrechen.

Hochverfügbarkeit erneut bereitstellen

Nachdem Sie die Hochverfügbarkeit für eine eigenständige Bereitstellung deaktiviert haben, können Sie sie erneut in den Hochverfügbarkeitsmodus bereitstellen. Das erneute Bereitstellen von Hochverfügbarkeit ähnelt der Erstbereitstellung von Hochverfügbarkeit. Weitere Einzelheiten finden Sie unter Bereitstellen des primären und sekundären Knotens als Paar mit hoher Verfügbarkeit.

Hochverfügbarkeits-Failover-Szenarien

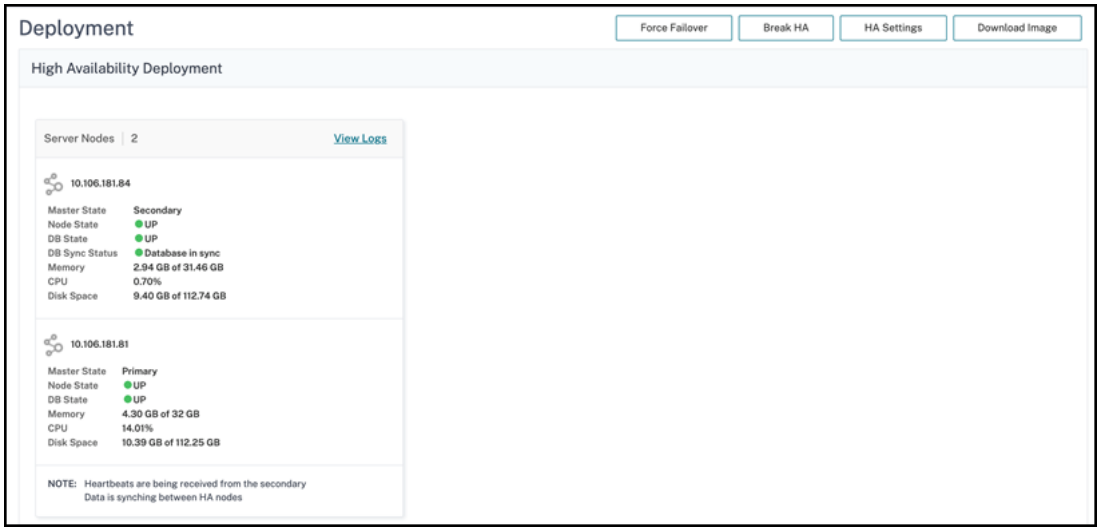
Ein Failover erfolgt, wenn eine der folgenden Bedingungen eintritt:

- **Knotenausfall**: Der primäre Knoten fällt aus, 180 Sekunden lang wird kein Herzschlag vom primären Knoten erkannt.
- **Anwendungsintegritätsfehler**: Der primäre Knoten ist gestartet und läuft, aber einer der NetScaler ADM Prozesse ist nicht mehr verfügbar.

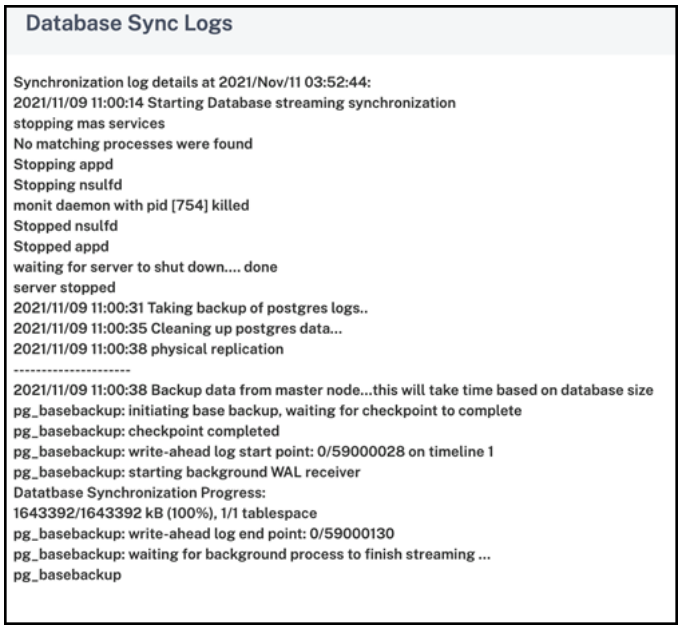
Meldungen des Datenbanksynchronisationsprotokolls

Im NetScaler ADM HA-Paar werden die Konfigurationsdateien automatisch vom primären Knoten zum sekundären Knoten synchronisiert, und die physische Streaming-Replikation der Datenbank erfolgt.

Wenn jedoch ein Streaming-Replikationsfehler vorliegt, wird die Schaltfläche “**Datenbank synchronisieren** “angezeigt. Sie können auf die Schaltfläche **Datenbank synchronisieren** klicken, um die Datenbanksynchronisierung zu starten.



Um den Fortschritt der Datenbanksynchronisierung anzuzeigen, klicken Sie auf **Protokolle anzeigen**. Die Meldung **Datenbank-Sync-Protokolle** wird angezeigt, und Sie können die Details des Synchronisierungsfortschritts in Echtzeit anzeigen.



Split-Hirn-Szenario

Wenn aufgrund einer Ausfallzeit der Netzwerkverbindung keine Kommunikation zwischen den beiden Knoten stattfindet, gilt Folgendes:

- Der primäre Knoten arbeitet weiterhin als primärer Knoten
- Der sekundäre Knoten übernimmt die Funktion des primären Knotens, da keine Herzschläge empfangen werden können

- Beide Knoten würden ihre einzelnen Datenbankinstanzen ausführen.

In einem Unternehmen wurden beispielsweise zwei NetScaler ADM-Knoten als primärer und sekundärer Knoten bereitgestellt. Aufgrund einer möglichen Ausfallzeit der Netzwerkverbindung wird die Kommunikation zwischen den beiden NetScaler ADM-Knoten vollständig unterbrochen. Da über 180 Sekunden lang kein Herzschlagaustausch stattfindet, betrachten sich beide Knoten als primärer Knoten. Beide Knoten fungieren als aktive Knoten und führen ihre eigenen Instanzen der Datenbank aus.

Ab NetScaler ADM 12.1 oder neueren Versionen wird diese Split-Brain-Situation problemlos bewältigt, nachdem die Netzwerkverbindung und der Taktschlag wiederhergestellt wurden. Hochverfügbarkeitssynchronisierung wird automatisch wiederhergestellt. Die Wiederherstellungszeit hängt von den Daten und der Geschwindigkeit der Verbindung zwischen den Knoten ab.

> **Hinweis**
>
> Während des Split-Brain-Zustands werden Änderungen, die am alten Primärknoten vorgenommen wurden, auf den neuen Primärknoten zurückgesetzt, wenn dieser wieder mit hoher Verfügbarkeit verbunden wird. Die Änderungen, die auf dem neuen Primärknoten während des Split-Gehirns aufgetreten sind, bleiben intakt.

Notfallwiederherstellung für hohe Verfügbarkeit konfigurieren

February 5, 2024

Katastrophe ist eine plötzliche Störung der Geschäftsfunktionen, die durch Naturkatastrophen oder durch Menschen verursachte Ereignisse verursacht werden. Katastrophen wirken sich auf den Betrieb des Rechenzentrums aus. Danach müssen die am Katastrophenort verlorenen Ressourcen und Daten vollständig neu aufgebaut und wiederhergestellt werden. Der Verlust von Daten oder Ausfallzeiten im Rechenzentrum ist entscheidend und reduziert die Business Continuity.

Die NetScaler ADM Disaster Recovery (DR)-Funktion bietet vollständige Systembackup- und Wiederherstellungsfunktionen für NetScaler ADM, das im Hochverfügbarkeitsmodus bereitgestellt wird. Zum Zeitpunkt der Wiederherstellung stehen Zertifikate, Konfigurationsdateien und ein vollständiges Backup der Datenbank auf der Wiederherstellungs-Site zur Verfügung.

In der folgenden Tabelle werden die Begriffe beschrieben, die bei der Konfiguration der Notfallwiederherstellung in NetScaler ADM verwendet werden.

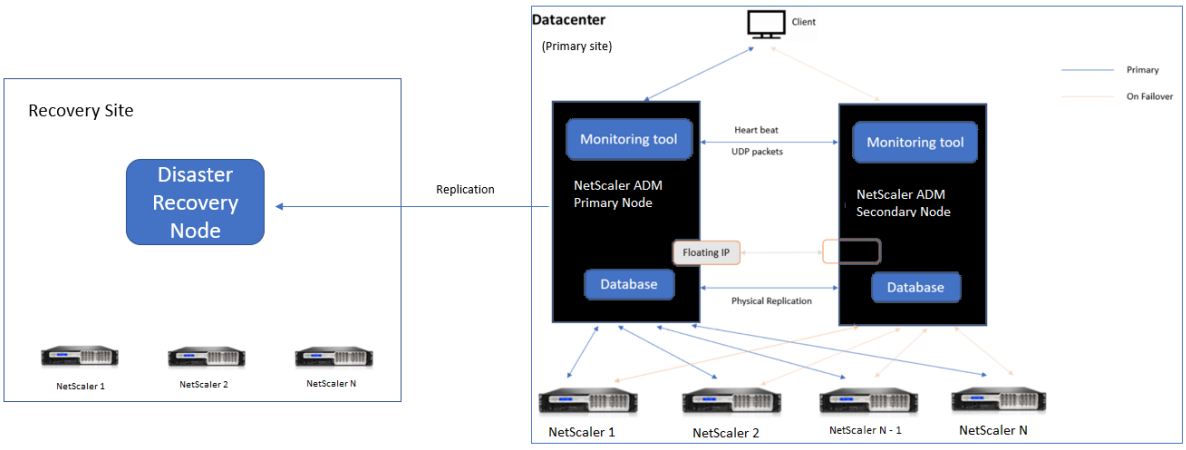
Begriff	Beschreibung
Primärer Standort (Rechenzentrum A)	Der primäre Standort verfügt über NetScaler ADM-Knoten, die im Hochverfügbarkeitsmodus bereitgestellt werden.
Wiederherstellungsstandort (Rechenzentrum B)	Die Wiederherstellungs-Site verfügt über einen Disaster Recovery-Knoten, der im eigenständigen Modus bereitgestellt wird. Dieser Knoten befindet sich im schreibgeschützten Modus und ist erst betriebsbereit, wenn der primäre Standort ausgefallen ist.
Knoten für die Notfallwiederherstellung	Der Wiederherstellungsknoten ist ein eigenständiger Knoten, der auf der Wiederherstellungs-Site bereitgestellt wird. Dieser Knoten wird betriebsbereit (zum neuen primären), falls eine Katastrophe am primären Standort auftritt und nicht funktionsfähig ist.

> **Hinweis**
>
> Der primäre Standort und der DR-Standort kommunizieren über die Ports 5454 und 22 miteinander, und diese Ports sind standardmäßig aktiviert.
>
> Weitere Informationen zu Port- und Protokolldetails finden Sie unter Ports.

Disaster Recovery-Workflow

Die folgende Abbildung zeigt den Disaster Recovery-Workflow, die Ersteinrichtung vor der Katastrophe und den Arbeitsablauf nach der Katastrophe.

Ersteinrichtung vor dem Notfall



Das Bild zeigt das Setup für die Notfallwiederherstellung vor dem Notfall.

Der primäre Standort verfügt über NetScaler ADM Knoten, die im Hochverfügbarkeitsmodus bereitgestellt werden. Weitere Informationen finden Sie unter Hochverfügbarkeitsbereitstellung

Auf der Wiederherstellungs-Site ist ein eigenständiger NetScaler ADM Disaster Recovery-Knoten remote bereitgestellt. Der Disaster Recovery-Knoten befindet sich im schreibgeschützten Modus und empfängt Daten vom primären Knoten, um ein Datenbackup zu erstellen. NetScaler-Instanzen auf der Wiederherstellungs-Site werden ebenfalls erkannt, sie werden jedoch von keinem Datenverkehr durchflossen. Während des Backup-Vorgangs werden alle Daten, Dateien und Konfigurationen vom primären Knoten auf dem Disaster Recovery-Knoten repliziert.

Voraussetzungen

Bevor Sie den Disaster Recovery-Knoten einrichten, beachten Sie die folgenden Voraussetzungen:

- Um die Disaster Recovery-Einstellungen zu aktivieren, müssen am primären Standort NetScaler ADM-Knoten im Hochverfügbarkeitsmodus konfiguriert sein.
- Die eigenständige Bereitstellung von NetScaler ADM am primären Standort unterstützt die Disaster Recovery-Funktion nicht.
- Das NetScaler ADM HA-Paar (am primären Standort) und der eigenständige Knoten (am DR-Standort) müssen dieselbe Softwareversion, denselben Build und dieselbe Konfiguration haben.

Citrix empfiehlt, dass Sie die CPU-Priorität (in den Eigenschaften der virtuellen Maschine) auf der höchsten Ebene festlegen, um das Planungsverhalten und die Netzwerklatenz zu verbessern.

In der folgenden Tabelle sind die Mindestanforderungen für die Konfiguration des Disaster Recovery-Knotens aufgeführt:

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8 CPUs
Stauraum	Citrix empfiehlt die Verwendung der Solid-State-Drive-Technologie (SSD) für NetScaler ADM-Bereitstellungen. Der Standardwert ist 120 GB. Die tatsächliche Speicheranforderung hängt von der Schätzung der NetScaler ADM Größe ab. Wenn Ihre NetScaler ADM Speicheranforderung 120 GB überschreitet, müssen Sie einen zusätzlichen Datenträger bereitstellen. **Hinweis:** Sie können nur eine weitere Festplatte hinzufügen. Citrix empfiehlt Ihnen, zum Zeitpunkt der Erstbereitstellung den Speicher zu schätzen und mehr Datenträger anzuhängen. Weitere Informationen finden Sie unter Bereitstellen eines zusätzlichen Datenträgers in NetScaler ADM.
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s oder 100 Mbit/s
Hypervisor	**Versionen**
Citrix Hypervisor	6.2 und 6.5
VMware ESXi	5.5 und 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu und Fedora

Erstmaliger Disaster Recovery-Setup

- Bereitstellen von NetScaler ADM im Hochverfügbarkeitsmodus
- Bereitstellen und Registrieren des NetScaler ADM Notfallwiederherstellungsknotens
- Disaster Recovery-Einstellungen über die Benutzeroberfläche aktivieren und deaktivieren

Bereitstellen von NetScaler ADM im Hochverfügbarkeitsmodus

Um die Disaster Recovery-Einstellungen einzurichten, stellen Sie sicher, dass NetScaler ADM im Hochverfügbarkeitsmodus bereitgestellt wird. Informationen zur Bereitstellung von NetScaler ADM in Hochverfügbarkeit finden Sie unterHochverfügbarkeitsbereitstellung

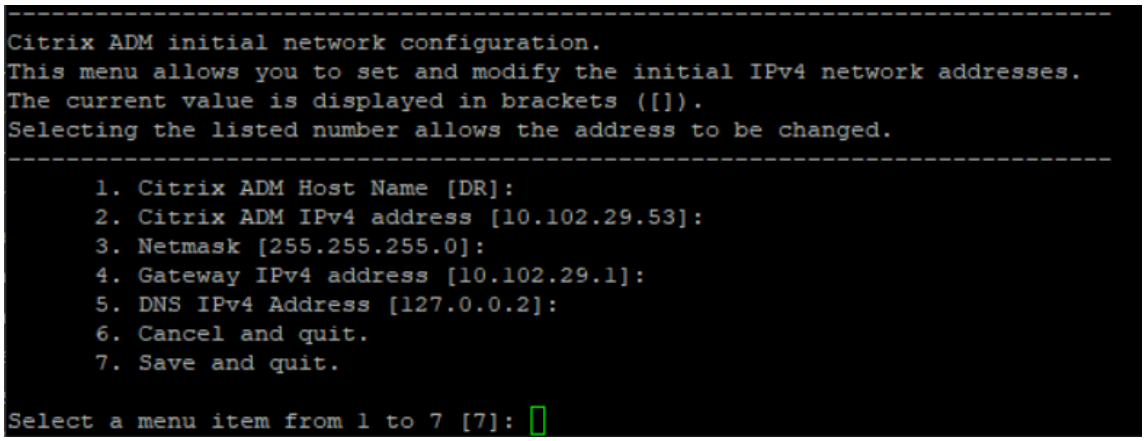
> **Hinweis**
>
> - NetScaler ADM, das im Hochverfügbarkeitsmodus bereitgestellt wird, muss auf die NetScaler ADM-Version 13.1 aktualisiert werden.
> - Eine**schwebende IP-Adresse ist obligatorisch**, um Disaster Recovery-Knoten beim primären Knoten zu registrieren.

Bereitstellen und Registrieren des NetScaler ADM Notfallwiederherstellungsknotens über die DR-Konsole

So registrieren Sie den NetScaler ADM Notfallwiederherstellungsknoten:

1. Laden Sie die `.xva` Image-Datei von der NetScaler-Website herunter und importieren Sie sie in Ihren Hypervisor.
2. Konfigurieren Sie auf der Registerkarte **Konsole** NetScaler ADM mit den anfänglichen Netzwerkkonfigurationen.

   > **Hinweis**
   >
   > Der Notfallwiederherstellungsknoten kann sich in einem anderen Subnetz befinden.

3. Nachdem die anfängliche Netzwerkkonfiguration abgeschlossen ist, fordert das System zur Anmeldung auf. Melden Sie sich mit den folgenden Anmeldeinformationen an —`nsrecover`/`nsroot`.

> **Wichtig**
>
> Ändern Sie während der Registrierung nicht die Anmeldeinformationen des DR-Knotens (`nsrecover`/`nsroot`). Sie können die Anmeldeinformationen des DR-Knotens ändern, nachdem Sie den DR-Knoten erfolgreich registriert haben.

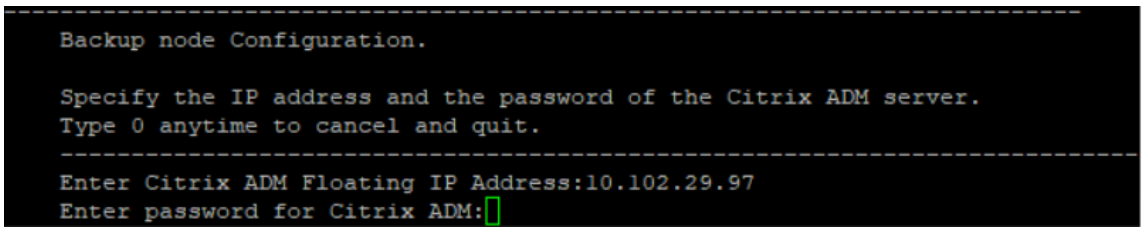
4. Um den Notfallwiederherstellungsknoten bereitzustellen, geben Sie **/mps/deployment_type.py** ein, und drücken Sie die Eingabetaste. Das Konfigurationsmenü für die NetScaler ADM Bereitstellung wird angezeigt.

```
bash-3.2# /mps/deployment_type.py
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

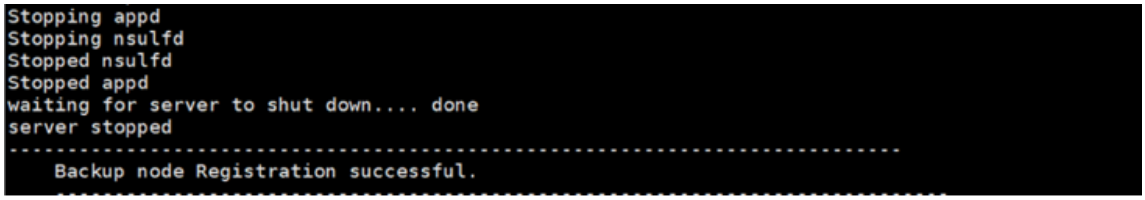
5. Wählen Sie **2** aus, um den Notfallwiederherstellungsknoten zu registrieren.

```
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 2
Selected Option      2. Remote Disaster Recovery Node.
```

6. Die Konsole fordert zur Eingabe einer Floating-IP-Adresse des Hochverfügbarkeitsknotens und des Kennworts auf.
7. Geben Sie die schwebende IP-Adresse und das Kennwort ein, um den Disaster Recovery-Knoten beim primären Knoten zu registrieren.



Der Notfallwiederherstellungsknoten ist jetzt erfolgreich registriert.



> **Hinweis**
>
> - Der Disaster Recovery-Knoten hat keine GUI.
> - Nach erfolgreicher Registrierung sind die standardmäßigen Administratoranmeldeinformationen für die Anmeldung am Server `nsroot`/`nsroot`.

8. Wenn Sie das Kennwort des DR-Knotens ändern möchten, führen Sie das folgende Skript aus:

```
/mps/change_freebsd_password.sh <username> <password>
<!--NeedCopy-->
```

Beispiel:

```
/mps/change_freebsd_password.sh nsroot new_password
<!--NeedCopy-->
```

Bereitstellen des Notfallwiederherstellungsknotens mit der NetScaler ADM GUI

Nachdem der Disaster Recovery-Knoten erfolgreich über die DR-Konsole registriert wurde, stellen Sie den DR-Knoten über die NetScaler ADM-GUI bereit. In diesem Schritt werden die Disaster Recovery-Einstellungen vom primären NetScaler ADM-Standort aus aktiviert.

1. Navigieren Sie zu **System > Systemverwaltung > Notfallwiederherstellungseinstellungen.**
2. Wählen Sie auf der Seite **Disaster Recovery** die Option **DR Node bereitstellen**aus.
3. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Ja**, um fortzufahren.

> **Hinweis**

> Die für das Systembackup benötigte Zeit hängt von der Datengröße und der Geschwindigkeit der WAN-Verbindung ab.

Nachdem Sie den DR-Knoten erfolgreich in der NetScaler ADM-GUI bereitgestellt haben, können Sie den Datenbankstatus, den Arbeitsspeicher, die CPU und die Festplattenauslastung des DR-Knotens überwachen.

Um die Disaster Recovery-Einstellungen zu deaktivieren, wählen Sie **DR Knoten entfernen**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Ja**, um fortzufahren.

Um den DR-Knoten erneut zu aktivieren, konfigurieren Sie den DR-Knoten für Ihr Hochverfügbarkeitspaar neu:

1. Melden Sie sich mit einem Hypervisor oder einer SSH-Konsole am DR-Knoten an.
2. Konfigurieren Sie den DR-Knoten, indem Sie das unter Deploy verfügbare Verfahren befolgen und den NetScaler ADM-Notfallwiederherstellungsknoten mithilfe der DR-Konsole registrieren.
3. Stellen Sie den Notfallwiederherstellungsknoten mit der NetScaler ADM GUIbereit.

Weitere Informationen finden Sie in den FAQs.

> **Wichtig!**
>
> - Es liegt in der Verantwortung des Administrators, festzustellen, dass eine Katastrophe am primären Standort aufgetreten ist.
> - Der Workflow zur Notfallwiederherstellung wird manuell vom Administrator initiiert, nachdem der primäre Standort ausfällt.
> - Ein Administrator muss den Prozess manuell initiieren, indem er ein Wiederherstellungsskript auf dem Disaster Recovery-Knoten am Recovery-Standort ausführt.
> - Wenn Sie das HA-Paar am primären Standort aktualisieren, müssen Sie auch manuell den eigenständigen Knoten am DR-Standort aktualisieren.

Workflow nach der Katastrophe

Wenn der primäre Standort nach einem Notfall ausfällt, muss der Disaster Recovery-Workflow wie folgt initiiert werden:

1. Der Administrator stellt fest, dass der primäre Standort von einer Katastrophe heimgesucht wurde und dieser nicht betriebsbereit ist.
2. Der Administrator leitet den Wiederherstellungsprozess ein.

3. Der Administrator muss basierend auf Ihren Anforderungen (an der Wiederherstellungs-Site) eines der folgenden Wiederherstellungsskripts manuell auf dem Disaster Recovery-Knoten ausführen:

   - Konfigurieren von SNMP, Syslog und Analytics auf dem DR-Knoten:

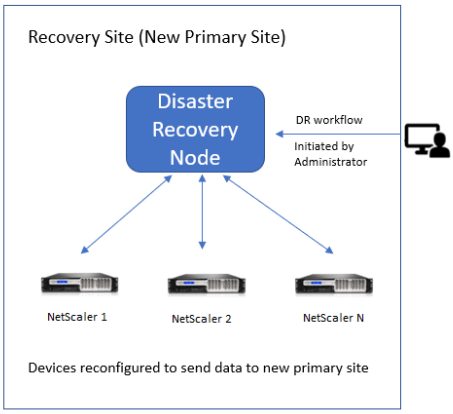
   ```
   /mps/scripts/pgsql/pgsql_restore_remote_backup.sh

   <!--NeedCopy-->
   ```

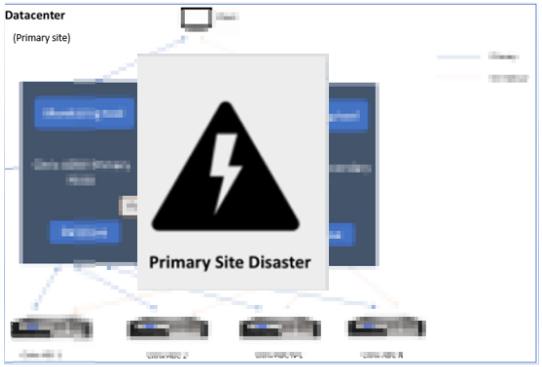
   - Konfigurieren Sie den DR-Knoten auch als Lizenzserver:

   ```
   /mps/scripts/pgsql/pgsql_restore_remote_backup.sh -reconfig-
       ls <IP-address-of-the-primary-site>

   <!--NeedCopy-->
   ```

4. Intern werden NetScaler Instanzen automatisch neu konfiguriert, um die Daten an den Notfallwiederherstellungsknoten zu senden, der jetzt zum neuen primären Standort geworden ist.

   Die folgende Abbildung zeigt, dass der Disaster Recovery-Workflow nach dem primären Standort mit einem Notfall verbunden ist.





> **Hinweis:**
>
> Nachdem Sie das Skript auf der DR-Site initiiert haben, wird die DR-Site nun zur neuen primären Site. Sie können auch auf die DR-Benutzeroberfläche zugreifen.

Nachträgliche Notfallwiederherstellung

Nachdem der Notfall aufgetreten ist und der Administrator das Wiederherstellungsskript initiiert, wird der Notfallstandort nun zum neuen primären Standort.

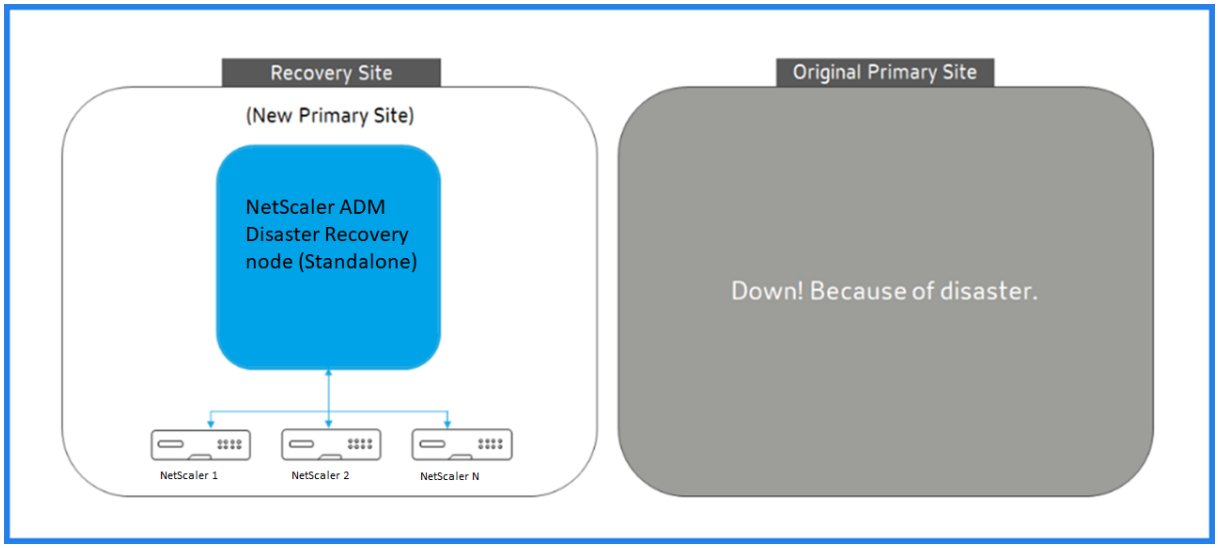
Wenn Sie die Konfigurationen später auf den ursprünglichen Standort zurücksetzen möchten, lesen Sie Wiederherstellen von Konfigurationen auf den ursprünglichen primären Standort.

Wichtig!

- Wenn Sie NetScaler ADM 12.1.49.x oder frühere Versionen installiert haben, erhalten Sie eine Frist von 30 Tagen, um Citrix zu kontaktieren, um die ursprüngliche Lizenz auf dem NetScaler ADM (am DR-Standort) erneut zu hosten.
- Für 12.1.50.x oder neuere Versionen wird die NetScaler ADM-Lizenz automatisch mit der DR-Site synchronisiert (Sie müssen sich nicht an Citrix wenden, um die Lizenz zu erhalten).
- Wenn Sie gepoolte Lizenzen für die Instances verwendet haben, unterstützen NetScaler mit Version **11.1 65.x oder höher**, **12.1 58.x oder höher**, **13.0 47.x oder höher** und NetScaler SDX **13.0 76.x oder höher** die automatische Lizenzierung von Serverupdates auf der DR-Site. Bei allen anderen Versionen müssen Sie die Instanzen für die DR-Site manuell neu konfigurieren.

Wiederherstellen von Konfigurationen auf den ursprünglichen primären Standort

Nach einem Notfall wird der konfigurierte Disaster Recovery (DR) -Knoten zum neuen primären Standort, und der Client-Verkehr fließt über diesen Knoten.



Weitere Informationen finden Sie unter Workflow nach der Katastrophe.

Wenn der ursprüngliche primäre Standort frei von Notfällen ist und Sie sich entscheiden, alle Vorgänge auf den primären Standort zu verschieben, konfigurieren Sie den ursprünglichen primären Standort so, dass er mit den Konfigurationen des DR-Knotens übereinstimmt.

Bevor Sie beginnen, stellen Sie sicher, dass sowohl der primäre Standort als auch der DR-Standort aktiv sind.

Gehen Sie wie folgt vor, um die Änderungen vom DR-Standort auf den ursprünglichen primären Standort zurückzusetzen:

1. Melden Sie sich an der ursprünglichen primären Site an und führen Sie den folgenden Befehl aus:

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password> &
<!--NeedCopy-->
```

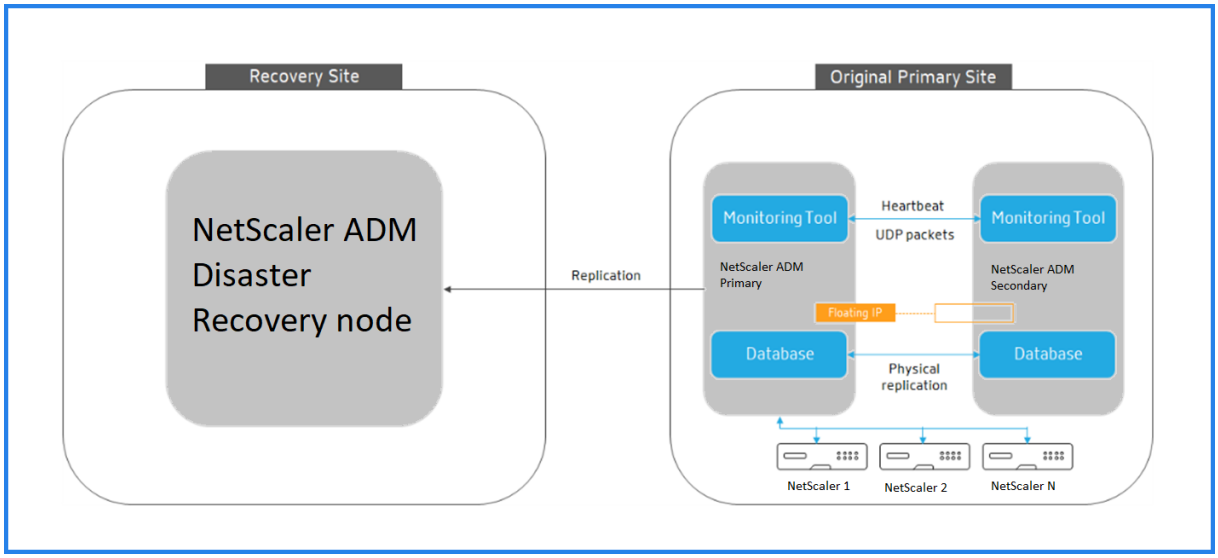
   Mit diesem Befehl werden nur Syslog, SNMP und Analytics für den primären Standort konfiguriert.

   Wenn Sie den primären Standort als gepoolten Lizenzserver für ADC-Instanzen konfigurieren möchten, führen Sie den folgenden Befehl aus:

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password>  -O yes &
<!--NeedCopy-->
```

   Der `-O` Befehl ruft die IP-Adresse der DR-Site ab und konfiguriert den primären Standort als gepoolten Lizenzserver neu.

2. Konfigurieren Sie den DR-Standort neu. Siehe Disaster Recovery-Setup bereitstellen.



Nachdem Sie die Konfigurationen vom DR-Standort auf den ursprünglichen primären Standort zurückgesetzt haben, fließt der Clientverkehr über den primären NetScaler ADM Knoten.

On-Prem-Agents für die Bereitstellung mehrerer Standorte konfigurieren

February 5, 2024

In früheren Versionen von NetScaler ADM können NetScaler-Instanzen, die in Remote-Rechenzentren bereitgestellt werden, von NetScaler ADM verwaltet und überwacht werden, die in einem primären Rechenzentrum ausgeführt werden. NetScaler-Instanzen sendeten Daten direkt an den primären NetScaler ADM, was zu einem Verbrauch der WAN-Bandbreite führte. Außerdem werden bei der Verarbeitung von Analysedaten CPU- und Speicherressourcen des primären NetScaler ADM verwendet.

Sie können Rechenzentren auf der ganzen Welt haben. Agenten spielen in den folgenden Szenarien eine wichtige Rolle:

- Installation von Agenten in Remote-Rechenzentren, sodass der WAN-Bandbreitenverbrauch reduziert wird.
- Um die Anzahl der Instanzen zu begrenzen, die Datenverkehr zur Datenverarbeitung direkt an das primäre NetScaler ADM senden.

> **Hinweis**
>
> - Die Installation von Agenten für Instanzen im Remote-Rechenzentrum wird empfohlen, aber nicht zwingend erforderlich. Bei Bedarf können Benutzer NetScaler-Instanzen direkt zum primären NetScaler ADM hinzufügen.
> - Wenn Sie Agents für ein oder mehrere Remote-Rechenzentren installiert haben, erfolgt die Kommunikation zwischen den Agenten und dem primären Standort über eine schwebende IP-Adresse. Weitere Informationen finden Sie unter Port.
> - Sie können Agents installieren und gepoolte Lizenzen auf die Instanzen in einem oder mehreren Remote-Rechenzentren anwenden. In diesem Szenario erfolgt die Kommunikation zwischen dem primären Standort und einem oder mehreren Remote-Rechenzentren über die Floating-IP.
> - Der on-premises NetScaler ADM-Agent unterstützt keine gepoolte Lizenzierung.

Ab NetScaler ADM 12.1 oder höher können Instanzen mit Agenten für die Kommunikation mit dem primären NetScaler ADM in einem anderen Rechenzentrum konfiguriert werden.

Agents arbeiten als Vermittler zwischen dem primären NetScaler ADM und den erkannten Instanzen in verschiedenen Rechenzentren. Die Installation von Agenten bietet folgende Vorteile:

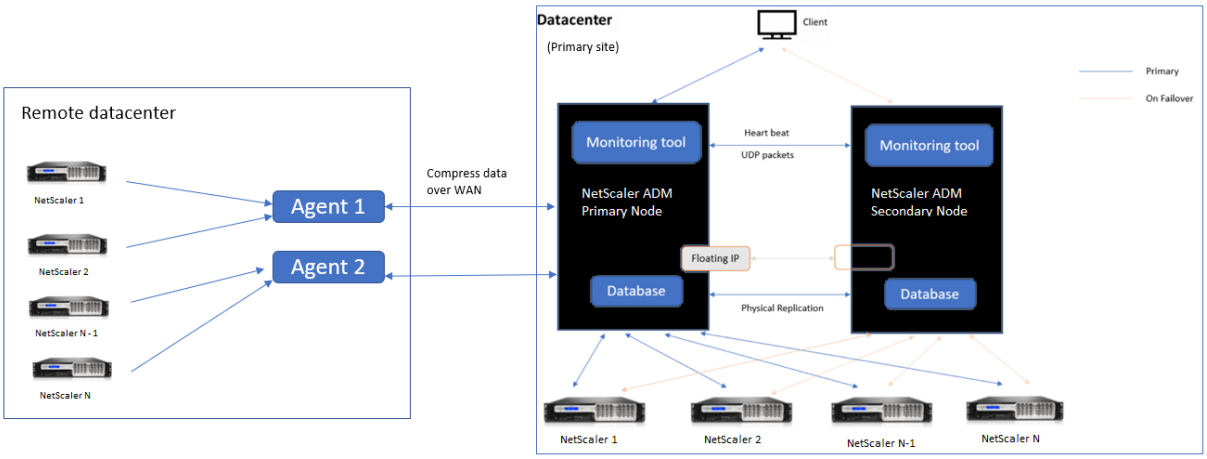
- Die Instanzen sind für Agenten so konfiguriert, dass die unverarbeiteten Daten direkt an Agenten anstatt an das primäre NetScaler ADM gesendet werden. Agenten führen die erste Ebene der Datenverarbeitung durch und senden die verarbeiteten Daten in komprimiertem Format zur Speicherung an das primäre NetScaler ADM.
- Agenten und Instanzen befinden sich im selben Rechenzentrum, sodass die Datenverarbeitung schneller erfolgt.

- Das Clustering der Agents ermöglicht die Neuverteilung von NetScaler-Instanzen beim Agent-Failover. Wenn ein Agent in einer Site ausfällt, wird der Datenverkehr von NetScaler-Instanzen auf einen anderen verfügbaren Agenten an derselben Site umgeschaltet.

> **Hinweis**
>
> Die Anzahl der Agenten, die pro Standort installiert werden sollen, hängt vom verarbeiteten Datenverkehr ab.

Architektur

Die folgende Abbildung zeigt NetScaler-Instanzen in zwei Rechenzentren und NetScaler ADM Hochverfügbarkeitsbereitstellung mit Agent-basierter Architektur an mehreren Standorten.



Auf dem primären Standort sind die NetScaler ADM Knoten in einer Hochverfügbarkeitskonfiguration bereitgestellt. Die NetScaler-Instanzen auf der primären Site sind direkt beim NetScaler ADM registriert.

Am sekundären Standort werden Agenten bereitgestellt und beim NetScaler ADM-Server am primären Standort registriert. Diese Agenten arbeiten in einem Cluster, um den kontinuierlichen Verkehrsfluss zu bewältigen, falls ein Agenten-Failover auftritt. Die NetScaler-Instanzen am sekundären Standort werden über Agenten innerhalb dieser Site beim primären NetScaler ADM-Server registriert. Die Instanzen senden Daten direkt an Agenten statt an primäres NetScaler ADM. Die Agenten verarbeiten die von den Instanzen empfangenen Daten und senden sie in einem komprimierten Format an das primäre NetScaler ADM. Agenten kommunizieren mit dem NetScaler ADM-Server über einen sicheren Kanal, und die über den Kanal gesendeten Daten werden aus Gründen der Bandbreiteneffizienz komprimiert.

Erste Schritte

- Installieren des Agenten in einem Rechenzentrum

  - Registrieren Sie den Agenten
  - Den Agenten an eine Site anhängen
- Hinzufügen NetScaler-Instanzen
  - Neue Instanz hinzufügen
  - Eine bestehende Instanz aktualisieren

Installieren des Agenten in einem Rechenzentrum

Sie können den Agenten installieren und konfigurieren, um die Kommunikation zwischen dem primären NetScaler ADM und den verwalteten NetScaler-Instanzen in einem anderen Rechenzentrum zu ermöglichen.

Sie können einen Agent auf den folgenden Hypervisoren in Ihrem Unternehmensrechenzentrum installieren:

- Citrix Hypervisor
- VMware ESXi
- Microsoft Hyper-V
- Linux KVM-Server

> **Hinweis**
>
> On-Prem-Agenten für die Multisite-Bereitstellung werden nur mit der NetScaler ADM-Hochverfügbarkeitsbereitstellung unterstützt.

Bevor Sie mit der Installation des Agenten beginnen, stellen Sie sicher, dass Sie über die erforderlichen virtuellen Computerressourcen verfügen, die der Hypervisor für jeden Agenten bereitstellen muss.

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8 CPUs
Speicherplatz	30 GB
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s

Ports

Für Kommunikationszwecke müssen die folgenden Ports zwischen dem Agenten und dem lokalen NetScaler ADM-Server geöffnet sein.

Typ	Port	Details	Richtung der Kommunikation
TCP	8443, 7443, 443	Für ausgehende und eingehende Kommunikation zwischen dem Agenten und dem NetScaler ADM lokalen Server.	NetScaler ADM Agent an NetScaler ADM

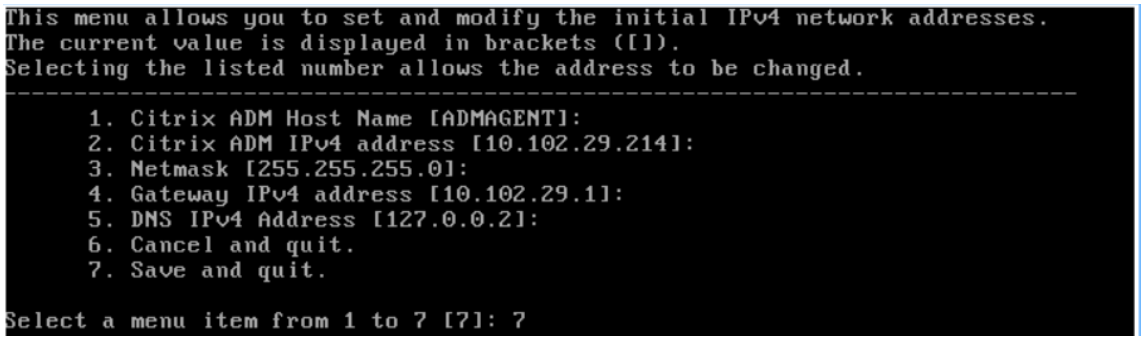
Die folgenden Ports müssen zwischen dem Agent und den NetScaler-Instanzen geöffnet sein.

Typ	Port	Details	Richtung der Kommunikation
TCP	80	Für die NITRO-Kommunikation zwischen Agent und NetScaler-Instanz.	NetScaler ADM an NetScaler und NetScaler an NetScaler ADM
TCP	22	Für die SSH-Kommunikation zwischen Agent und NetScaler-Instanz. Für die Synchronisierung zwischen NetScaler ADM-Servern, die im Hochverfügbarkeitsmodus bereitgestellt werden.	NetScaler ADM an NetScaler und NetScaler ADM Agent an NetScaler
UDP	4739	Für die AppFlow-Kommunikation zwischen Agent und NetScaler-Instanz.	NetScaler zu NetScaler ADM

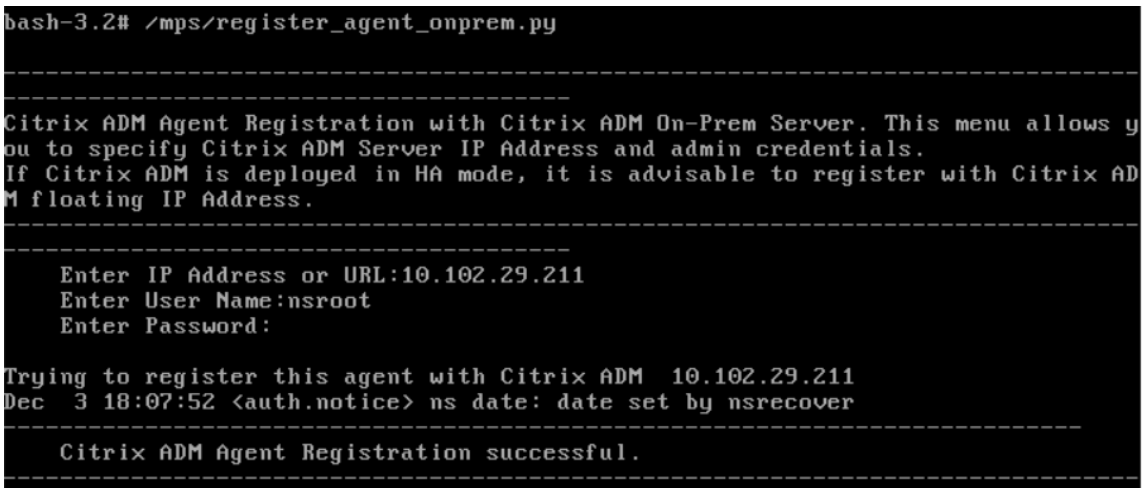
Typ	Port	Details	Richtung der Kommunikation
ICMP	Kein reservierter Port	Um die Netzwerkerreichbarkeit zwischen NetScaler ADM- und NetScaler-Instanzen oder dem sekundären NetScaler ADM-Server zu erkennen, der im Hochverfügbarkeitsmodus bereitgestellt wird.	
UDP	161, 162	Zum Empfangen von SNMP-Ereignissen von der NetScaler-Instanz an den Agenten.	Port 161 - NetScaler ADM zu NetScaler Port 162 - NetScaler zu NetScaler ADM
UDP	514	Um Syslog-Meldungen von der NetScaler-Instanz an den Agenten zu empfangen.	NetScaler zu NetScaler ADM
TCP	5557	Für die Logstream-Kommunikation zwischen Agent- und NetScaler-Instanzen.	NetScaler zu NetScaler ADM

Registrieren Sie den Agenten

1. Verwenden Sie die Agent-Image-Datei, die Sie von der NetScaler-Site heruntergeladen haben, und importieren Sie sie in Ihren Hypervisor. Das Benennungsmuster der Agentimagedatei ist wie folgt: **MASAGENT-<HYPERVISOR>-<Version.no>.** Beispiel: **MASAGENT-XEN-13.0-xy.xva**
2. Konfigurieren Sie auf der Registerkarte **Konsole** NetScaler ADM mit den anfänglichen Netzwerkkonfigurationen.
3. Geben Sie den NetScaler ADM-Hostnamen, die IPv4-Adresse und die Gateway-IPv4-Adresse ein. Wählen Sie Option 7, um die Konfiguration zu speichern und zu beenden.



4. Nach erfolgreicher Registrierung wird die Konsole aufgefordert, sich anzumelden. Verwenden Sie *nsrecover/nsroot* als Anmeldeinformationen.
5. Um den Agenten zu registrieren, geben Sie **/mps/register_agent_onprem.py**ein. Die Anmeldeinformationen für die NetScaler ADM Agent-Registrierung werden wie in der folgenden Abbildung dargestellt angezeigt.
6. Geben Sie die schwebende NetScaler ADM IP-Adresse und die Anmeldeinformationen des Benutzers ein.



Nachdem die Registrierung erfolgreich ist, wird der Agent neu gestartet, um den Installationsvorgang abzuschließen.

Nachdem der Agent neu gestartet wurde, greifen Sie auf die NetScaler ADM-GUI zu. Gehen Sie im Hauptmenü zur Seite **Infrastruktur > Instanzen > Agents**, um den Status des Agenten zu überprüfen. Der neu hinzugefügte Agent wird im Status **Hoch** angezeigt.

> **Hinweis**
>
> Das NetScaler ADM zeigt die Version des Agenten an und prüft außerdem, ob der Agent auf der neuesten Version ist. Das Download-Symbol bedeutet, dass der Agent nicht auf der neuesten Version ist und aktualisiert werden muss. Citrix empfiehlt, dass Sie die Agent-Version auf die NetScaler ADM Version aktualisieren.

Agent an eine Site anhängen

1. Wählen Sie den Agenten aus und klicken Sie auf **Site anhängen.**
2. Wählen Sie auf der Seite **Site anfügen** eine Site aus der Liste aus, oder erstellen Sie mit der Plusschaltfläche (+) eine Site.
3. Klicken Sie auf **Speichern**.

> **Hinweis**
>
> - Standardmäßig werden alle neu registrierten Agenten zum Standardrechenzentrum hinzugefügt.
> - Es ist wichtig, den Agent mit der richtigen Site zu verknüpfen. Im Falle eines Agentenfehlers werden die ihm zugewiesenen NetScaler-Instanzen automatisch auf andere funktionsfähige Agents am selben Standort umgestellt.

Agent-Aktionen

Unter **Infrastruktur > Agenten > Aktionen auswählen können Sie verschiedene Aktionen auf einen Agenten**anwenden.

Unter **Aktion auswählen**können Sie die folgenden Funktionen verwenden:

Installieren Sie ein neues Zertifikat: Wenn Sie ein anderes Agentzertifikat 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.

Generieren Sie eine Datei für den technischen Support: Generieren Sie eine Datei für den technischen Support für einen ausgewählten NetScaler ADM Agent. Sie können diese Datei herunterladen und an den technischen Support von Citrix zur Untersuchung und Fehlerbehebung senden.

Hinzufügen NetScaler-Instanzen

Instanzen sind NetScaler ADC-Appliances oder virtuelle Appliances, die Sie von NetScaler ADM aus über Agenten erkennen, verwalten und überwachen möchten. Sie können die folgenden NetScaler ADC-Appliances und virtuellen Appliances zu NetScaler ADM oder Agents hinzufügen:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX

- NetScaler CPX
- NetScaler Gateway
- Citrix SSL-Forward-Proxy

Weitere Informationen finden Sie unter Instanzen zu NetScaler ADM hinzufügen.

Eine vorhandene Instanz an den Agenten anhängen

Wenn eine Instanz bereits zum primären NetScaler ADM hinzugefügt wurde, können Sie sie an einen Agenten anhängen, indem Sie einen Agenten bearbeiten.

1. Navigieren Sie zu **Infrastruktur > Instanzen** und wählen Sie den Instanztyp aus. Beispiel: NetScaler.
2. Klicken Sie auf **Bearbeiten**, um eine vorhandene Instanz zu bearbeiten.
3. Klicken Sie, um den Agent auszuwählen.
4. Wählen Sie auf der Seite **Agent** den Agenten aus, dem Sie die Instanz zuordnen möchten, und klicken Sie dann auf **OK**.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass Sie die **Site** auswählen, mit der Sie die Instanz verknüpfen möchten.

Greifen Sie auf die GUI einer Instanz zu, um Ereignisse zu validieren

Nachdem die Instanzen hinzugefügt und der Agent konfiguriert wurde, greifen Sie auf die GUI einer Instanz zu, um zu überprüfen, ob das Trapziel konfiguriert ist.

Navigieren Sie in NetScaler ADM zu **Infrastruktur > Instanzen**. Wählen Sie unter **Instanzen**den Instanztyp aus, auf den Sie zugreifen möchten (z. B. NetScaler VPX), und klicken Sie dann auf die IP-Adresse einer bestimmten Instanz.

Die GUI der ausgewählten Instanz wird in einem Popupfenster angezeigt.

Standardmäßig ist der Agent als Trapziel auf der Instanz konfiguriert. Melden Sie sich zur Bestätigung an der GUI der Instanz an und überprüfen Sie die Trapziele.

> **Wichtig!**
>
> Das Hinzufügen eines Agenten für NetScaler-Instanzen in Remoterechenzentren wird empfohlen, ist aber nicht obligatorisch.

> Falls Sie die Instance direkt zum primären MAS hinzufügen möchten, wählen Sie beim Hinzufügen von Instanzen keinen **Agenten** aus.

NetScaler ADM Agenten-Failover

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

> **Wichtig!**
>
> - Stellen Sie sicher, dass die **Agent-Failover-Funktion** für Ihr Konto aktiviert ist. Informationen zum Aktivieren dieser Funktion finden Sie unter ADM-Funktionen aktivieren oder deaktivieren.
> - Wenn ein Agent ein Skript ausführt, stellen Sie sicher, dass das Skript auf allen Agents in der Site vorhanden ist. Daher kann der geänderte Agent das Skript nach dem Agent-Failover ausführen.

Informationen zum Anhängen einer Site an einen Agenten in der ADM-GUI finden Sie unter Anhängen eines Agenten an eine Site.

Um ein Agent-Failover zu erzielen, wählen Sie NetScaler ADM -Agents nacheinander aus, und fügen Sie sie an dieselbe Site an.

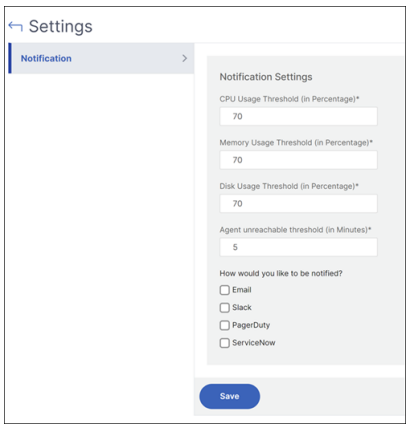
Beispielsweise sind zwei Agenten 10.106.1xx.2x und 10.106.1xx.3x am Standort Bangalore angeschlossen und betriebsbereit. Wenn ein Agent inaktiv wird, erkennt NetScaler ADM ihn und zeigt den Status als heruntergefahren an.

Wenn ein NetScaler ADM Agent in einer Site inaktiv wird (Status Heruntergefahren), wartet NetScaler ADM fünf Minuten darauf, dass der Agent aktiv wird (Status Up). Wenn der Agent inaktiv bleibt, verteilt NetScaler ADM die Instanzen automatisch auf die verfügbaren Agents an derselben Site neu.

NetScaler ADM löst die Instanzumverteilung alle 30 Minuten aus, um die Last zwischen den aktiven Agent in der Site auszugleichen.

Schwellenwert für nicht erreichbare Agenten und Benachrichtigung konfigurieren

Wenn ein Agent für eine bestimmte Dauer nicht erreichbar ist oder nicht erreichbar ist, können Sie per E-Mail, Slack, PagerDuty und ServiceNow eine Benachrichtigung über den Agentenstatus erhalten. Klicken Sie unter **Infrastruktur > Instanzen > Agents** auf **Einstellungen**, geben Sie die Dauer zwischen 5 Minuten und 60 Minuten an und wählen Sie die Benachrichtigungsmethode aus, über die Sie benachrichtigt werden möchten.



Installieren Sie einen ADM-Agenten als Microservice in einem Kubernetes-Cluster

February 5, 2024

Die Bereitstellung eines NetScaler ADM-Agenten als Microservice ist nützlich für die Verwaltung Ihres NetScaler CPX. Die in diesem Dokument verfügbaren Verfahren sind nur anwendbar, wenn der NetScaler ADM und der Kubernetes-Cluster in einem anderen Netzwerk konfiguriert sind. In diesem Szenario können Sie einen ADM-Agenten als Microservice konfigurieren, in dem der Kubernetes-Cluster gehostet wird.

> Hinweis
>
> Sie können auch einen On-Premises-Agent konfigurieren und den Agenten im Netzwerk registrieren, in dem der Kubernetes-Cluster gehostet wird.

Erste Schritte

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Instanzen > Agents**.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Download Agent Microservice** aus.
3. Geben Sie auf der Seite **Download Agent Microservice** die folgenden Parameter an:
    a) **Anwendungs-ID** —Eine String-ID, mit der der Dienst für den Agent im Kubernetes-Cluster definiert und dieser Agent von anderen Agents im selben Cluster unterschieden wird.
    b) **Kennwort** —Geben Sie ein Kennwort an, mit dem CPX dieses Kennwort verwendet, um CPX über den Agenten in ADM einzubringen.
    c) **Kennwort bestätigen** —Geben Sie dasselbe Kennwort zur Bestätigung an.

> Hinweis
>
> Sie dürfen das Standardkennwort (`nsroot`) nicht verwenden.

d) Klicken Sie auf **Yaml-Datei herunterladen**.

NetScaler ADM Agent im Kubernetes-Cluster installieren

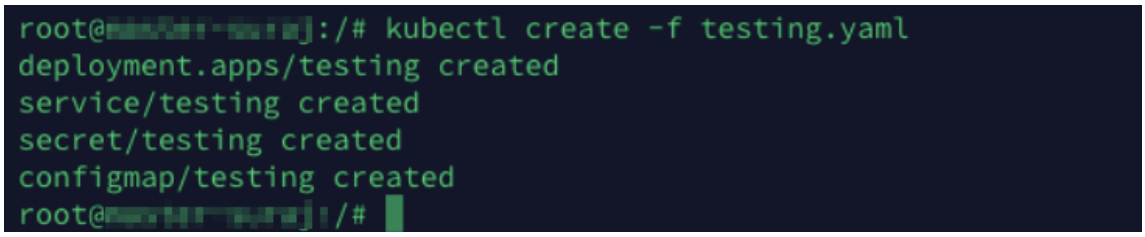
Im Hauptknoten von Kubernetes:

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 NetScaler ADM zu **Infrastruktur > Instanzen > Agents**, um den Agentstatus anzuzeigen.

Nachdem Sie den Agenten konfiguriert haben, können Sie die NetScaler CPX-Instanzen hinzufügen und Analysen im Service Graph anzeigen. Weitere Informationen:

- Hinzufügen von NetScaler CPX-Instanzen zu NetScaler ADM.
- Service-Graph wird eingerichtet.

NetScaler ADM-Bereitstellung mit einem Server auf eine Bereitstellung mit hoher Verfügbarkeit migrieren

February 5, 2024

Sie können Ihren NetScaler ADM-Einzelserver auf eine Hochverfügbarkeitsbereitstellung mit zwei NetScaler ADM-Servern aufrüsten. Ein Paar von NetScaler ADM-Servern mit hoher Verfügbarkeit

befindet sich im aktiv/passiven Modus, und beide Server haben dieselbe Konfiguration. Bei dieser Art der aktiv-passiven Bereitstellung wird ein NetScaler ADM-Server als primärer Knoten und der andere als sekundärer Knoten konfiguriert. Wenn der primäre Knoten aus irgendeinem Grund ausfällt, übernimmt der sekundäre Knoten die Arbeit.

Um einen NetScaler ADM-Einzelserver zu einem Hochverfügbarkeitspaar zu migrieren, müssen Sie einen neuen NetScaler ADM-Serverknoten bereitstellen, ihn als zweiten NetScaler ADM-Einzelserver konfigurieren und beide NetScaler ADM-Server als Hochverfügbarkeitspaar bereitstellen.

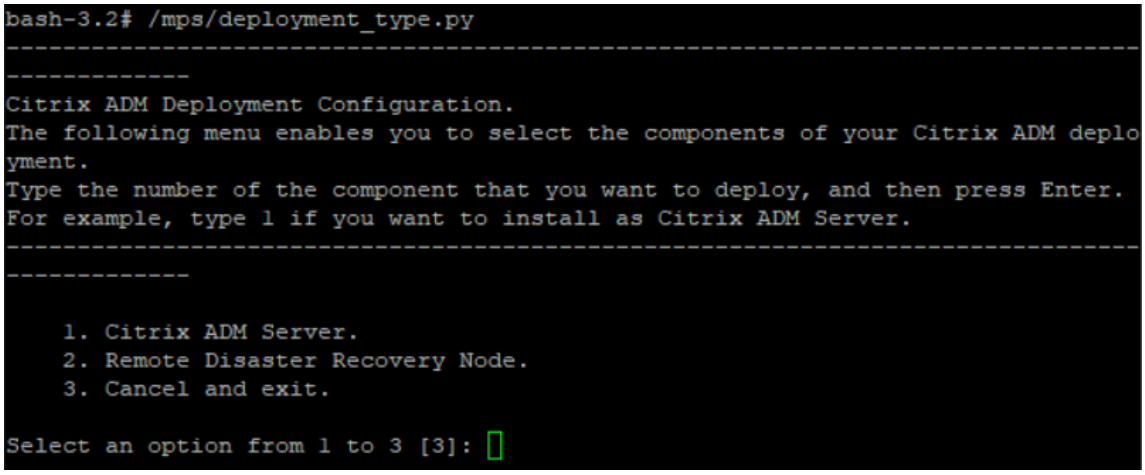
Die Migration eines NetScaler ADM-Einzelservers in einen Hochverfügbarkeitsmodus umfasst die folgenden Schritte:

1. Änderung des vorhandenen Serverknotens
2. Provisioning des zweiten Serverknotens
3. Bereitstellung der beiden Knoten im HA-Modus
4. Konfiguration des Hochverfügbarkeitspaars

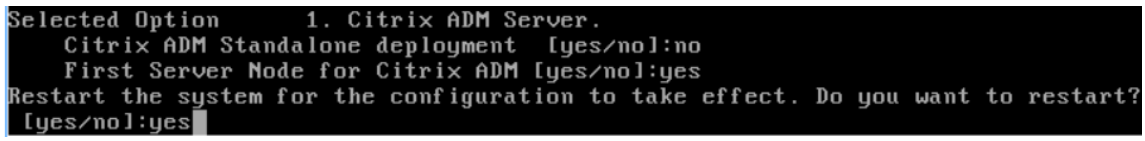
Ändern Sie den vorhandenen NetScaler ADM-Serverknoten

Um das NetScaler ADM vom Einzelserver in den Hochverfügbarkeitsmodus zu migrieren, müssen Sie den anfänglichen Bereitstellungstyp des Serverknotens in den Hochverfügbarkeitsmodus ändern.

1. Öffnen Sie auf einer Workstation oder einem Laptop die Konsole des vorhandenen NetScaler ADM-Serverknotens. Stellen Sie sich beispielsweise vor, dass Sie ein NetScaler ADM mit der IP-Adresse 10.106.171.17 als eigenständigen Server bereitgestellt haben.
2. Melden Sie sich bei NetScaler ADM an. Die Standardanmeldeinformationen sind `nsroot` und `nsroot`.
3. Geben Sie in der Shell-Eingabeaufforderung ein `/mps/deployment_type.py`, und **drücken Sie die EIN**
4. Wählen Sie als Bereitstellungstyp NetScaler ADMServer aus. Wenn Sie keine Option auswählen, wird diese standardmäßig als Server bereitgestellt.



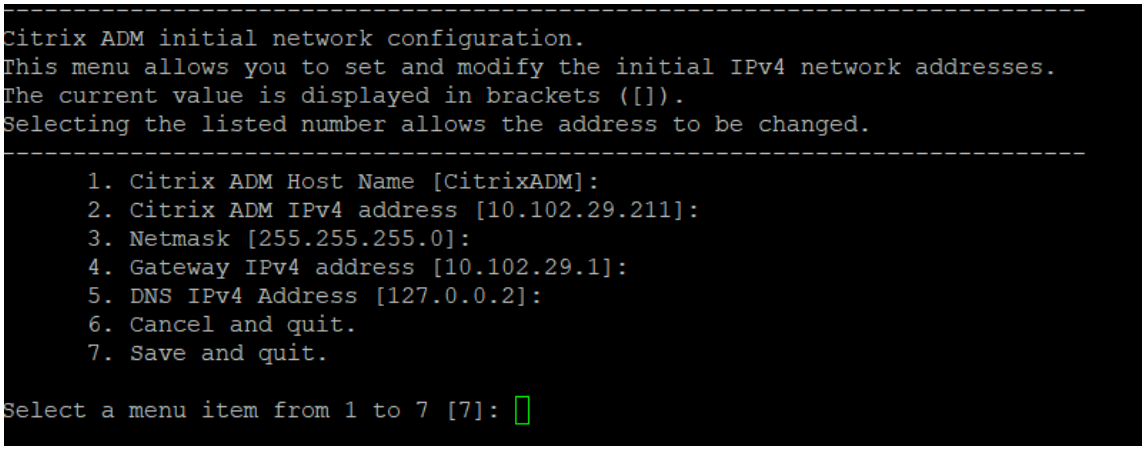
5. Die Bereitstellungskonsole fordert Sie auf, die Serverbereitstellung auszuwählen (als eigenständig). Geben Sie **Nein** ein, um die Bereitstellung als Hochverfügbarkeitspaar zu bestätigen.
6. Die Konsole fordert Sie auf, den (ersten Serverknoten) auszuwählen. Geben Sie **Ja** ein, um den Knoten als ersten Serverknoten zu bestätigen.
7. Die Konsole fordert Sie auf, den Server neu zu starten.
8. Geben Sie **Ja ein,** um den Neustart zu starten.



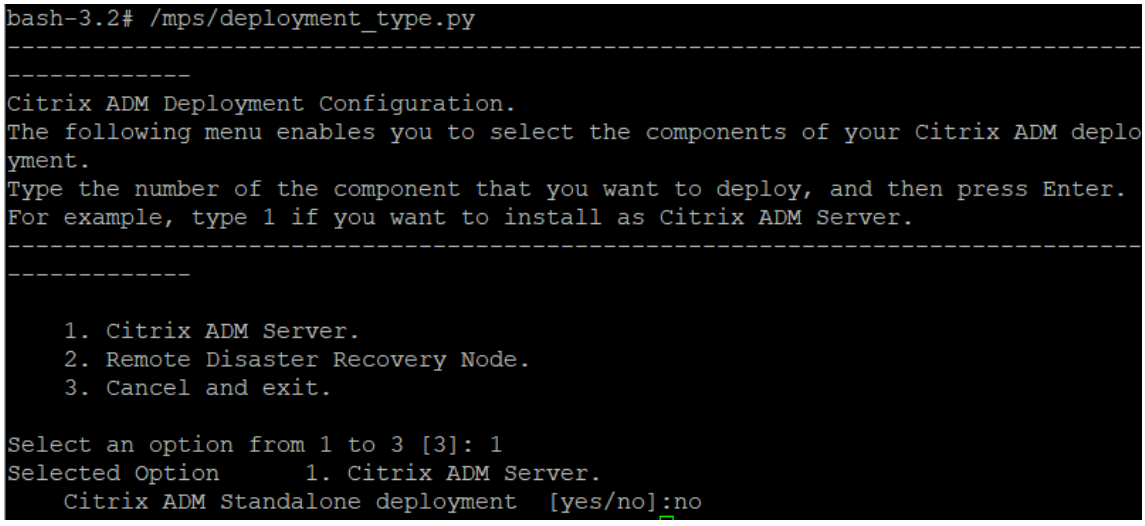
Bereitstellen des zweiten Serverknotens

Sie müssen den zweiten Server auf Ihrem Hypervisor bereitstellen. Verwenden Sie dieselbe Image-Datei, die Sie für die Installation des ersten Servers verwendet haben, oder rufen Sie eine Image-Datei derselben Version von der NetScaler-Site ab.

1. Importieren Sie die Imagedatei in Ihren Hypervisor, und konfigurieren Sie dann über die Registerkarte Konsole die anfänglichen Netzwerkkonfigurationsoptionen, wie auf dem folgenden Bildschirm erläutert:



2. Nachdem Sie die erforderlichen IP-Adressen angegeben haben, geben Sie in der Shell-Eingabeaufforderung /mps/deployment_type.py ein, und drücken Sie die Eingabetaste.
3. Wählen Sie als Bereitstellungstyp **NetScaler ADM**Server aus.
4. Die Bereitstellungskonsole fordert Sie auf, die Serverbereitstellung auszuwählen (als eigenständig). Geben Sie **Nein** ein, um die Bereitstellung als Hochverfügbarkeitspaar zu bestätigen.



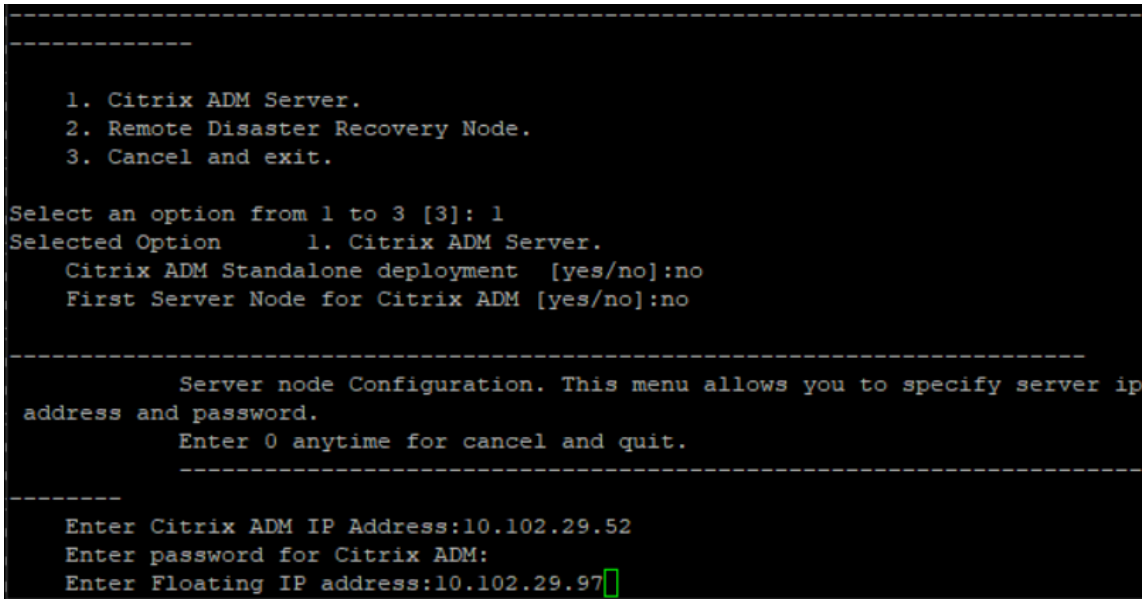
5. Die Konsole fordert Sie dann auf, den (ersten Serverknoten) auszuwählen. Geben Sie **Nein** ein, um den Knoten als zweiten Serverknoten zu bestätigen.


```
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:no
```

6. Geben Sie die IP-Adresse und das Kennwort des ersten Servers ein.

```
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:no

------------------------------------------------------------------------------
           Server node Configuration. This menu allows you to specify server ip
 address and password.
           Enter 0 anytime for cancel and quit.
           ------------------------------------------------------------------
--------
    Enter Citrix ADM IP Address:10.102.29.52
    Enter password for Citrix ADM:
```

7. Geben Sie die Floating-IP-Adresse des ersten Knotens ein.



8. Die Konsole fordert Sie auf, das System neu zu starten. Geben Sie **Ja** ein, um neu zu starten.

Stellen Sie die beiden Server in einem Hochverfügbarkeitsmodus bereit

Um den Installationsvorgang der beiden Serverknoten als Hochverfügbarkeitspaar abzuschließen, müssen Sie diese Knoten über die GUI des zuvor vorhandenen NetScaler ADM-Serverknotens bereitstellen. Die interne Kommunikation zwischen den beiden Servern wird gestartet, wenn Sie die beiden Serverknoten bereitstellen.

> **Wichtig**
>
> Bevor Sie Knoten mit hoher Verfügbarkeit bereitstellen, müssen Sie das Standardkennwort ändern.

1. Geben Sie in einem Webbrowser die IP-Adresse des zuvor vorhandenen NetScaler ADM -Serverknotens ein.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte **System** zu **Bereitstellung**, und klicken Sie auf **Bereitstellen**.
4. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **Ja**.

> **Hinweis**
>
> Nachdem Sie NetScaler ADM mit hoher Verfügbarkeit bereitgestellt haben, können Sie en-

> tweder auf den primären Knoten oder auf die Floating-IP zugreifen. Sie können nicht auf den sekundären Knoten ab Version 12.1 zugreifen.

5. Obwohl Sie die Floating-IP bei der Konfiguration des zweiten Serverknotens eingegeben haben, haben Sie die Möglichkeit, die FIP auf der **Systemseite** zu aktualisieren. Klicken Sie auf **HA-Einstellungen** > **Floating-IP-Adresse für den Hochverfügbarkeitsmodus konfigurieren**. Sie können die Floating-IP anzeigen, die Sie zuvor konfiguriert haben. Sie können eine neue IP-Adresse eingeben und auf **OK**klicken.

NetScaler Insight Center zu NetScaler ADM migrieren

February 5, 2024

Sie können jetzt Ihre NetScaler Insight Center er-Bereitstellung zu NetScaler ADM migrieren, ohne dass die vorhandene Konfiguration, Einstellungen oder Daten verloren gehen. Mit NetScaler ADM können Sie nicht nur die verschiedenen Analysen einsehen, die von den NetScaler-Instanzen einer Anwendung generiert werden, sondern auch die gesamte globale Infrastruktur für die Anwendungsbereitstellung von einer einzigen, einheitlichen Konsole aus verwalten, überwachen und Fehler beheben.

> **Hinweis**
>
> Die Migration wird derzeit nur auf NetScaler Insight Center Standalone-Instances unterstützt.

Voraussetzungen

Stellen Sie vor der Migration der virtuellen NetScaler Insight Center-Appliance zu NetScaler ADM sicher, dass die folgenden Anforderungen erfüllt sind:

- NetScaler Insight Center 11.1 Build 47.14 oder höher ist installiert.
- Sie haben die NetScaler ADM 12.0 Build 57.24 .tgz-Imagedatei heruntergeladen.

  > **Hinweis**
  >
  > Sie müssen NetScaler ADM 12.0 Build 57.24 installieren und dann auf den neuesten NetScaler ADM 13.1 Build aktualisieren. Weitere Informationen finden Sie unter Upgrade.

- Sie haben die neueste Version der NetScaler ADM 13.1 TGZ-Imagedatei heruntergeladen.

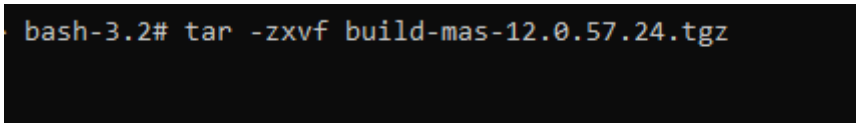
Hardwareanforderung

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8 CPUs
Speicherplatz	120 GB **Hinweis** Citrix empfiehlt,**500 GB**für eine bessere Leistung zu verwenden. Citrix empfiehlt außerdem die Verwendung der Solid-State-Drive-Technologie (SSD) für NetScaler ADM-Bereitstellungen.
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s oder 100 Mbit/s
Hypervisor-Anforderungen	
Citrix Hypervisor	6.2, 6.5
VMware ESX	5.5, 6.0
Microsoft Hyper-V	2012 R2
Linux - KVM	Ubuntu, Fedora

Ablauf der Installation

So migrieren Sie NetScaler Insight Center zu NetScaler ADM:

1. Melden Sie sich bei der Shell-Eingabeaufforderung von NetScaler Insight Center an.
2. Laden Sie NetScaler ADM 12.0 Build 57.24 in den Ordner */var/mps/mps_images* herunter.
3. Entfernen Sie die TGZ-Datei mithilfe des Befehls **tar -zxvf build-mas-12.0-57.24.tgz**.



4. Installieren Sie NetScaler ADM mithilfe der **. /installmas** (Befehl).

5. Nach der Installation von NetScaler ADM 12.0 Build 57.24 müssen Sie auf den neuesten NetScaler ADM 13.1 Build aktualisieren, indem Sie die obigen Schritte ausführen.

Nach der Migration werden alle NetScaler-Instanzen, die im NetScaler Insight Center-Inventar erkannt wurden, im **Abschnitt Infrastruktur > Instanzen** von NetScaler ADM angezeigt. Zum ersten Mal müssen Sie jedoch die virtuellen Server, die in den erkannten Appliances gehostet werden, manuell abfragen.

> **Hinweis**
>
> In NetScaler ADM fallen standardmäßig keine Lizenzkosten für die Verwaltung und Überwachung von zwei virtuellen Servern an, die innerhalb der erkannten NetScaler-Instanzen erstellt wurden. Installieren Sie die erforderlichen NetScaler ADM -Lizenzen, um mehr als zwei virtuelle Server zu überwachen und zu verwalten. Weitere Einzelheiten finden Sie unterNetScaler ADM-Lizenzierung.

Integration von NetScaler ADM und Citrix Director

February 5, 2024

Director lässt sich für Netzwerkanalysen und Leistungsmanagement in NetScaler ADM integrieren.

- Die Netzwerkanalyse ruft HDX Insight-Berichte von NetScaler ADM ab und bietet eine Anwendungs- und Desktopansicht des Netzwerks. Mit dieser Funktion bietet Director eine erweiterte Analyseansicht des ICA-Datenverkehrs in Ihrer Bereitstellung.
- Die Leistungsverwaltung bietet eine Verlaufsspeicherung und Trendberichte. Anhand der Beibehaltung historischer Daten können Sie im Gegensatz zur Echtzeitbewertung Trendberichte über Kapazität und Integrität usw. erstellen.

Nachdem Sie NetScaler ADM in Director integriert haben, bieten Ihnen HDX Insight-Berichte die folgenden Informationen in Director:

- Auf der Registerkarte Netzwerk auf der Seite Trends werden Latenz- und Bandbreiteneffekte für Anwendungen, Desktops und Benutzer in Ihrer gesamten Bereitstellung angezeigt.
- Auf der Seite Benutzerdetails werden Latenz- und Bandbreiteninformationen zu spezifischen Benutzersitzungen angezeigt.

Voraussetzungen

Hardwareanforderungen für die Migration von HDX Insight zu NetScaler ADM

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8
Stauraum	500 GB. Citrix empfiehlt die Verwendung der Solid-State-Drive-Technologie (SSD) für NetScaler ADM-Bereitstellungen.
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s oder 100 Mbit/s

Minimale Anforderungen

Stellen Sie vor der Konfiguration der Netzwerkintegration sicher, dass Sie einen RBAC-Benutzer mit HDX Insights-Zugriff erstellen.

Softwareanforderungen

Stellen Sie vor der Migration auf die virtuelle NetScaler ADM-Appliance sicher, dass die folgenden Anforderungen erfüllt sind:

- Director Version 1811 ist installiert.
- NetScaler HDX Insight Version 10.1 oder höher ist installiert
- HDX Insight und NetScaler ADM unterstützen Citrix VDA Version 7.0 und höher
- Citrix Workspace wird von Citrix Virtual Apps and Desktops ab Version 7.0 unterstützt.
- Stellen Sie sicher, dass MAC, Citrix Workspace für Mac, Version 11.8 und höher, und Windows Citrix Workspace für Windows 14.0 und höher verfügbar sind, um genaue ICA-RTT-Metriken anzuzeigen.
- NetScaler ADM Version 11.0 und höher ist installiert. Weitere Informationen zur Installation von NetScaler ADM finden Sie unter Bereitstellen von NetScaler ADM.

Einschränkungen

- Die Verfügbarkeit dieser Funktion richtet sich nach der Lizenzierung der Organisation und den Administratorberechtigungen.
- Die Round Trip Time (RTT) der ICA-Sitzung zeigt Daten für Citrix Workspace für Windows 3.4 oder höher und für Citrix Workspace für Mac 11.8 oder höher korrekt an. In früheren Versionen dieser Workspaces werden die Daten nicht korrekt angezeigt.
- In der Ansicht Trends werden HDX-Verbindungsanmeldedaten nicht für VDAs vor Version 7 erfasst. Für frühere VDAs werden die Diagrammdaten als 0 angezeigt.
- Bei Bereitstellungen, die bereits über eine externe Festplatte mit weniger als 500 GB Speicherplatz verfügen, können Sie keine weitere Festplatte hinzufügen.

> **Hinweis**
>
> - Weitere Informationen zu Director und Schritte zur Integration von NetScaler ADM mit Director finden Sie unterhttps://docs.citrix.com/en-us/citrix-virtual-apps-desktops/director/install-and-configure/hdx-insight.html.
> - Weitere Informationen zu HDX Insight finden Sie unterhttp://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html.

Stellen Sie einen zusätzlichen Datenträger für NetScaler ADM bereit

February 5, 2024

Die Speicheranforderungen für NetScaler Application Delivery Management (ADM) werden auf der Grundlage Ihrer NetScaler ADM-Größenschätzung ermittelt. NetScaler ADM bietet standardmäßig eine Speicherkapazität von 120 GB. Wenn Sie mehr als 120 GB zum Speichern Ihrer Daten benötigen, können Sie zusätzlichen Datenträger bereitstellen.

> **Hinweis:**
>
> - Schätzen Sie die Speicheranforderungen und schließen Sie eine zusätzliche Festplatte an den Server an.
> - Bei einer NetScaler ADM Bereitstellung mit einem Server können Sie zusätzlich zum Standarddatenträger nur einen Datenträger an den Server anhängen.
> - Für eine NetScaler ADM Hochverfügbarkeitsbereitstellung müssen Sie für jeden Knoten einen zusätzlichen Datenträger bereitstellen. Die Größe beider Festplatten muss identisch

> sein.
>
> - Wenn eine externe Festplatte mit geringerer Kapazität vorhanden ist, müssen Sie die Festplatte entfernen, bevor Sie eine neue Festplatte anschließen.
> - Wir empfehlen die Verwendung der Solid-State-Drive-Technologie (SSD) für NetScaler ADM-Bereitstellungen.

In diesem Dokument werden die folgenden Szenarien zum Bereitstellen eines zusätzlichen, neuen Datenträgers, zum Erstellen von Partitionen und zum Ändern der Größe des zusätzlichen Datenträgers erläutert:

1. Bereitstellen eines zusätzlichen Datenträgers in einem eigenständigen NetScaler ADM
2. Starten Sie das Datenträgerpartitionstool
3. Erstellen von Partitionen auf dem neuen zusätzlichen Datenträger
4. Ändern Sie die Größe der Partitionen in dem vorhandenen zusätzlichen Datenträger
5. Entfernen der Partitionen des zusätzlichen Datenträgers

Bereitstellen eines zusätzlichen Datenträgers in einem eigenständigen NetScaler ADM

1. Fahren Sie die virtuelle NetScaler ADM Maschine herunter.
2. Stellen Sie im Hypervisor einen zusätzliche Datenträger mit der erforderlichen Datenträgergröße für die virtuelle NetScaler ADM-Maschine bereit.

   Auf dem neu zugeordneten größeren Datenträger werden die Datenbankdaten und die NetScaler ADM Protokolldateien gespeichert. Die vorhandene Standardfestplatte mit 120 Gigabyte wird jetzt zum Speichern der Kerndateien, der Betriebssystemprotokolldateien usw. verwendet.
3. Starten Sie die virtuelle NetScaler ADM Maschine.

Starten Sie das Datenträgerpartitionstool

NetScaler ADM bietet jetzt das **NetScaler ADM Datenträgerpartitionstool**, ein neues Befehlszeilentool.

1. Mit dem Tool können Sie Partitionen auf dem neu hinzugefügten zusätzlichen Datenträger erstellen.
2. Mit dem Tool können Sie auch die Größe der vorhandenen zusätzlichen Festplatten ändern. Der vorhandene externe Datenträger darf jedoch nicht größer als 2 Terabyte sein.

> **Hinweis:**
>
> - Eine Größenänderung vorhandener Festplatten über 2 Terabyte kann zu Datenverlust führen. Dies liegt an einer bekannten Einschränkung der Plattform.
> - Um eine Speicherkapazität von mehr als 2 Terabyte zu erstellen, müssen Sie die vorhandenen Partitionen entfernen und mit diesem neuen Tool Partitionen erstellen.

3. Mit diesem neuen Tool können Sie jede Partitionsaktion auf der Festplatte explizit ausführen. Das Tool bietet Ihnen eine klare Sichtbarkeit und Kontrolle über den Datenträger und die zugehörigen Daten.

   > **Hinweis:**
   >
   > Sie können dieses Tool nur auf der zusätzlichen Festplatte verwenden, die Sie an den NetScaler ADM Server angeschlossen haben. Mit diesem Tool können Sie keine Partitionen auf der primären (Standard-) Festplatte erstellen.

So starten Sie das Festplattenpartitionstool:

1. Öffnen Sie eine SSH-Verbindung zum NetScaler ADM, indem Sie einen SSH-Client wie PuTTY verwenden.
2. Melden Sie sich mit den Anmeldeinformationen von `nsrecover`/`nsroot` bei NetScaler ADM an.
3. Wechseln Sie zur Shell-Eingabeaufforderung und geben Sie Folgendes ein:

```
/mps/DiskPartitionTool.py
<!--NeedCopy-->
```

> **Hinweis:**
>
> Für NetScaler ADM in der Hochverfügbarkeitsbereitstellung müssen Sie das Tool in beiden Knoten starten und Partitionen erstellen oder deren Größe ändern, nachdem Sie Datenträger an die jeweiligen virtuellen Maschinen angeschlossen haben.

Erstellen von Partitionen auf dem neuen zusätzlichen Datenträger

Der Befehl **create** wird verwendet, um Partitionen zu erstellen, wenn ein neuer sekundärer Datenträger hinzugefügt wird. Sie können diesen Befehl auch verwenden, um Partitionen auf einem vorhandenen sekundären Datenträger zu erstellen, nachdem die vorhandenen Partitionen mit dem Befehl "remove"gelöscht wurden.

```
(dpt): ?create
Creates a new partition on the attached disk. A swap partition of size 32GB is also created automatically.

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

> **Hinweis:**
>
> Beim Erstellen von Partitionen mit dem Festplattenpartitionstool gibt es keine Größenbeschränkung von 2 Terabyte. Das Tool kann Partitionen mit mehr als 2 Terabyte erstellen. Wenn Sie den Datenträger partitionieren, wird automatisch eine Swap-Partition der Größe 32 GB hinzugefügt. Die primäre Partition verwendet dann den gesamten verbleibenden Speicherplatz auf dem Datenträger.

Sobald der Befehl ausgeführt wurde, wird ein Partitionsschema der GUID-Partitionstabelle (GPT) erstellt. Außerdem werden eine 32 GB Swap-Partition und Datenpartition erstellt, um den Rest des Speicherplatzes zu nutzen. Ein neues Dateisystem wird dann auf der primären Partition erstellt.

> **Hinweis:**
>
> Dieser Vorgang kann einige Sekunden dauern, und Sie dürfen den Vorgang nicht unterbrechen.

```
(dpt): create

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

```
Creating GPT partition scheme...
da1 created

Creating partition 1 using (456287933) blocks. Leaving aside 32G for swap...
da1p1 added

Creating partition 2 for swap using remaining 32G...
da1p2 added

Formatting the new partition. This may take some time (~20 seconds). Please be patient and don't interrup the process...
```

Sobald der Befehl create abgeschlossen ist, wird die virtuelle Maschine automatisch neu gestartet, damit die neue Partition bereitgestellt wird.


```
Create Done.
VM has to be rebooted for the new partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

Nach dem Neustart wird die neue Partition unter /var/mps gemountet.

```
bash-3.2# df -k
Filesystem  1024-blocks     Used     Avail Capacity  Mounted on
/dev/md0         456046   374346     72580    84%    /
devfs                 1        1         0   100%    /dev
procfs                4        4         0   100%    /proc
fdescfs               1        1         0   100%    /dev/fd
/dev/da0s1a     1623950   284466   1209568    19%    /flash
/dev/da0s1e   116073918 2812298 103975708     3%    /var
/dev/da1p1    495168802   43854 455511444     0%    /var/mps
```

Die hinzugefügte Swap-Partition wird als Swap-Raum in der Ausgabe des Befehls "create" angezeigt.

```
CPU:  0.0% user,  0.0% nice,  0.0% system,  0.7% interrupt, 99.3% idle
Mem: 89M Active, 21M Inact, 123M Wired, 16M Cache, 74M Buf, 6965M Free
Swap: 37G Total, 37G Free
```

> **Hinweis:**
>
> Das Tool startet die virtuelle Maschine neu, nachdem die Partition erstellt wurde.

Ändern Sie die Größe der Partitionen in dem vorhandenen zusätzlichen Datenträger

Sie können den Befehl **resize** verwenden, um die Größe des angeschlossenen (sekundären) Datenträgers zu ändern. Sie können die Größe eines Datenträgers ändern, die ein `master boot record` (`MBR`) oder GPT-Schema hat. Die Größe der Festplatte muss weniger als 2 Terabyte betragen.

> **Hinweis:**
>
> - Der Befehl `resize` ist so konzipiert, dass er funktioniert, ohne dass vorhandene Daten verloren gehen. Wir empfehlen jedoch, wichtige Daten auf dieser Festplatte auf einem externen Speicher zu sichern, bevor Sie die Größe ändern. Datenbackup ist hilfreich in Fällen, in denen die Datenträgerdaten während des Größenänderungsvorgangs beschädigt werden

> können.
>
> - Stellen Sie sicher, dass Sie den Festplattenspeicher in Schritten von 100 GB Speicherplatz erhöhen, während Sie die Größe der Partitionen ändern. Eine solche schrittweise Erhöhung stellt sicher, dass Sie die Größe nicht häufiger ändern müssen.

```
(dpt): ?resize
Resizes existing partition on attached disk to utilize all space available. Pre-conditions are:
1. Secondary disk exists and capcity of disk < 2TB
2. A single partition exists on secondary disk and there is atleast 100GB to gain by resizing

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Der Befehl `resize` prüft, ob alle Voraussetzungen erfüllt sind, und fährt fort, wenn alle Voraussetzungen erfüllt sind und nachdem Sie der Größenänderung zugestimmt haben. Es stoppt die Prozesse, die auf die Festplatte zugreifen, was die NetScaler ADM-Subsysteme, PostgreSQL-DB-Prozesse und den NetScaler ADM-Monitorprozess umfasst. Sobald die Prozesse beendet wurden, wird die Bereitstellung des Datenträgers aufgehoben, um ihn für die Größenänderung vorzubereiten. Die Größenänderung erfolgt durch Erweitern der Partition, um den gesamten verfügbaren Speicherplatz zu belegen, und anschließendes Erweitern des Dateisystems. Wenn eine Swap-Partition auf dem Datenträger vorhanden ist, wird sie gelöscht und nach der Größenänderung am Ende des Datenträgers neu erstellt. Die Swap-Partition wird im Abschnitt Befehl **erstellen** des Dokuments erläutert.

> **Hinweis:**
>
> Der Prozess „wachsendes Dateisystem“kann einige Zeit in Anspruch nehmen. Achten Sie darauf, dass Sie den Vorgang nicht unterbrechen, während er läuft. Das Tool startet die virtuelle Maschine neu, nachdem Sie die Größe der Partition geändert haben.

```
(dpt): resize

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to resize (Y/N): y
```

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1...
da1p1 resized

Adding a swap partition da1p2...
da1p2 added

Formatting the newly added portions of the partition. This may take some time (~10 seconds). Please be patient and don't
 interrup the process...
```


Alle Zwischenschritte im Größenänderungsprozess (Anhalten von Anwendungen, Ändern der Größe des Datenträgers, wachsendes Dateisystem) werden auf der Konsole angezeigt. Sobald der Prozess abgeschlossen ist, wird die folgende Meldung angezeigt.

```
Resize Done.
VM has to be rebooted for the resized partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

Nach dem Neustart kann die Vergrößerung mit dem Befehl `df` beobachtet werden. Hier sind die Vorher-Nachher-Details, wenn Sie die Größe erhöhen:

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374864     72062    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1662048 105125958     2%    /var
/dev/da1s1a   152329216 3082226 137060654     2%    /var/mps
```

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374838     72088    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1666800 105121206     2%    /var
/dev/da1s1a   304651668 3137954 277141582     1%    /var/mps
```

Entfernen der Partitionen des zusätzlichen Datenträgers

Eine vorhandene Partition auf dem sekundären Datenträger kann auf bis zu 2 Terabyte verkleinert werden. Dieses Problem ist auf eine bekannte Einschränkung der Partition zurückzuführen. Wenn Sie einen Datenträger mit mehr als 2 Terabyte wünschen, schließen Sie einen neuen Datenträger an und partitionieren Sie ihn mit dem Datenträgerpartitionstools. Sie können die vorhandene Partition auch mithilfe des Befehls `remove` entfernen und dann eine Partition erstellen.

> **Hinweis:**
>
> Durch das Entfernen der vorhandenen Partition werden alle vorhandenen Daten gelöscht. Daher müssen alle kritischen Daten auf einem externen Speicher gesichert werden, bevor Sie diesen Befehl verwenden.

```
(dpt): ?remove
Removes existing partition from attached disk.

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Wenn Sie den Befehl „remove“ausführen, werden Sie zur Bestätigung aufgefordert. Nach der Bestätigung werden alle Prozesse (wie ADM-Subsysteme, PostgreSQL-Prozesse und ADM-Monitore) gestoppt,

die die sekundäre Festplatte verwenden. Wenn eine Swap-Partition vorhanden ist und Swap auf der Partition aktiviert ist, wird der Swap deaktiviert.

```
(dpt): remove

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

Wenn Sie “y”eingeben, wird die Bereitstellung des Datenträgers aufgehoben und alle Partitionen auf dem Datenträger.

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to remove existing partitions.
Disabling swap on partition: /dev/da1p2
Removing all partitions from: da1
Remove Done.
Rebooting VM now...
```

> **Hinweis:**
>
> Das Tool startet die virtuelle Maschine neu, nachdem Sie die Partition entfernt haben.

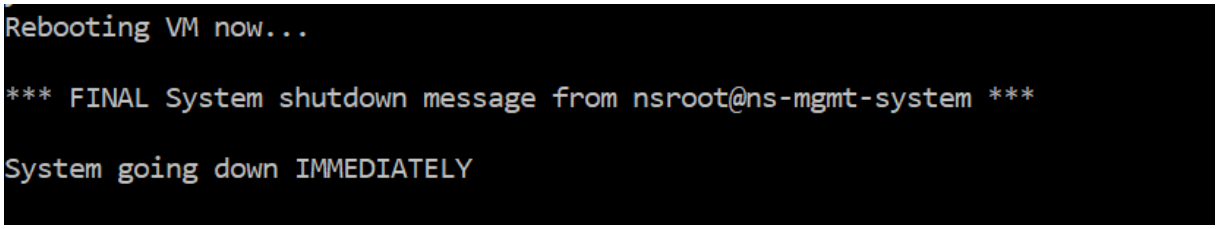
Starten Sie die virtuelle Maschine neu

Wenn eine Partition erstellt oder in der Größe geändert wird oder wenn eine Auslagerungsdatei erstellt wurde, starten Sie die virtuelle Maschine neu. Die Änderungen werden erst nach einem Neustart wirksam. Zu diesem Zweck wird ein **Reboot-Befehl** im Tool bereitgestellt.

```
(dpt): ?reboot
Reboot the VM. Note: VM has to be rebooted after new partition is created, existing one is resized or swap file is creat
ed.
The VM is rebooted automatically after these operations. If the automatic reboot does not happen, then this command can
be used to reboot the VM.
```

Sie werden zur Bestätigung aufgefordert, und nach der Bestätigung werden alle Prozesse (wie ADM-Subsysteme, PostgreSQL-Prozesse und ADM-Monitore) gestoppt. Die virtuelle Maschine wird dann neu gestartet.

```
(dpt): reboot
Are you sure you want to reboot the VM (Y/N): y
```

Erstellen einer Backupdatei der Datenträgerdaten

> **Hinweis:**
>
> Das Erstellen einer Sicherungsdatei erfordert Speicherplatz. Stellen Sie sicher, dass ausreichend Speicherplatz (50% oder mehr) vorhanden ist, bevor die Backup-Befehle ausgeführt werden.

So sichern Sie die NetScaler ADM-Daten, bevor Sie die Partitionen ändern oder entfernen:

1. Beenden Sie ADM.

```
/mps/masd stop
<!--NeedCopy-->
```

2. Stoppen Sie PostgreSQL.

```
su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
<!--NeedCopy-->
```

3. Beenden Sie ADM-Monitor.

```
/mps/scripts/stop_mas_monit.sh
<!--NeedCopy-->
```

4. Erstellen Sie einen Tarball.

```
cd /var
tar cvfz /var/mps/mps_backup.tgz mps
<!--NeedCopy-->
```

> **Hinweis:**
>
> Der Vorgang dauert je nach Größe der zu sichernden Daten einige Zeit.

5. Generieren Sie eine Prüfsumme.

```
md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
<!--NeedCopy-->
```

6. Kopieren Sie die Tarball- und Prüfsummendateien auf einen Remoteserver.
7. Überprüfen Sie die Richtigkeit des kopierten Tarballs. Generieren Sie eine Prüfsumme der übertragenen Datei und vergleichen Sie sie mit der Quellprüfsumme.

8. Entfernen Sie den Tarball von der virtuellen ADM-Maschine.

```
cd /var/mps/
rm mps_backup.tgz  mps_backup_checksum
<!--NeedCopy-->
```

Zusätzliche Befehle

Zusätzlich zu den zuvor aufgeführten Befehlen können Sie auch die folgenden Befehle im Tool verwenden:

Befehl “Hilfe”:

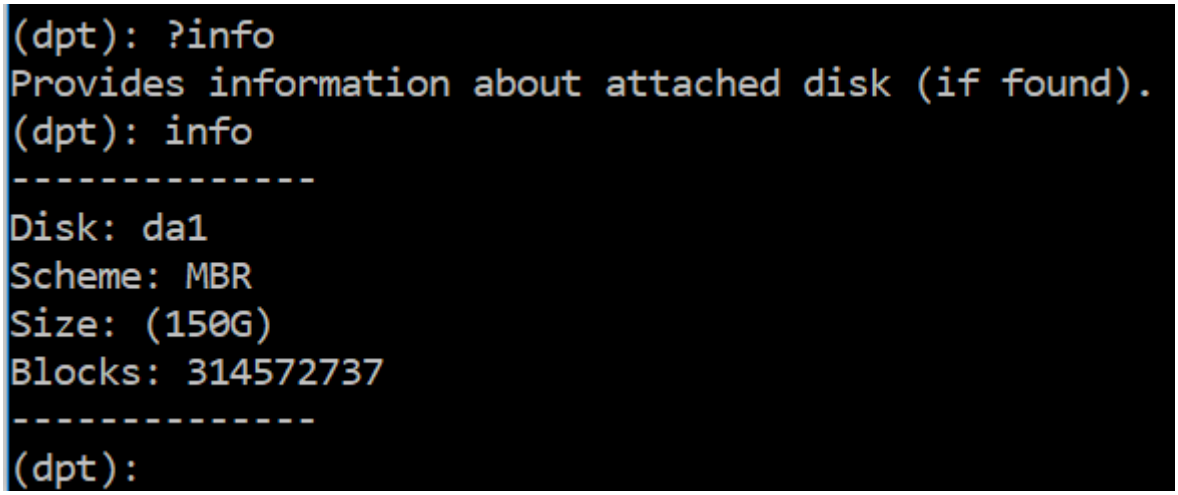
Um die unterstützten Befehle aufzulisten, geben Sie **help** oder **?** und drücken Sie Enter. Um weitere Hilfe zu den einzelnen Befehlen zu erhalten, drücken Sie **Hilfe** oder **?** gefolgt vom Befehlsnamen und drücken Sie die **Enter-Taste** .

```
(dpt): help

DPT Commands
------------
create  create_swapfile  exit  help  info  reboot  remove  resize

(dpt):
```

Info (Befehl):

Der Befehl **info** liefert Informationen über den angeschlossenen sekundären Datenträger, falls der Datenträger vorhanden ist. Der Befehl liefert den Gerätenamen, das Partitionsschema, die Größe in menschenlesbarer Form und die Anzahl der Datenträgerblöcke. Das Schema kann MBR oder GPT sein. Ein MBR-Schema bedeutet, dass die Festplatte mit einer früheren Version der NetScaler ADM-Version partitioniert wurde. Die MBR/GPT-basierte Partition kann in der Größe geändert werden, jedoch nicht über 2 Terabyte hinaus. Das GPT-Partitionsschema bedeutet, dass die Festplatte mit NetScaler ADM 12.1 oder höher partitioniert wurde.

> **Hinweis:**
>
> Eine GPT-Partition kann größer als 2 Terabyte sein, aber wenn sie erstellt wird. Sie können die Größe des Datenträgers jedoch nicht auf eine Größe von mehr als 2 Terabyte ändern, nachdem Sie einen Datenträger mit einer kleineren Größe erstellt haben. Dieses Problem ist eine bekannte Einschränkung der Plattform.



Create_swapfile (Befehl):

Die Standard-Swap-Partition auf der primären Festplatte von NetScaler ADM ist 4 GB, daher beträgt der Standardauslagerungsspeicher 4 GB. Für die Standardspeicherkonfiguration von NetScaler ADM, die 2 GB beträgt, ist dieser Swap-Speicherplatz ausreichend. Wenn Sie NetScaler ADM jedoch mit einer höheren Speicherkonfiguration ausführen, benötigen Sie mehr Auslagerungsspeicher auf dem Datenträger.

> **Hinweis:**
>
> Die Swap-Partition ist normalerweise eine dedizierte Partition, die während der Installation des Betriebssystems auf einer Festplatte (HDD) erstellt wird. Eine solche Partition wird auch als Swap Space bezeichnet. Eine Swap-Partition wird für virtuellen Speicher verwendet, die den zusätzlichen Hauptspeicher simuliert.

Bei sekundären Datenträgern, die in früheren Versionen von NetScaler ADM hinzugefügt wurden, wird standardmäßig keine Auslagerungspartition erstellt. Der Befehl “create_swapfile”ist für sekundäre Datenträger gedacht, die mit älteren NetScaler ADM-Versionen ohne Auslagerungspartition erstellt wurden. Der Befehl prüft auf Folgendes:

- Vorhandensein eines sekundären Datenträgers
- Datenträger, der bereitgestellt wird
- Größe des Datenträgers (mindestens 500 GB)
- Die Existenz der Auslagerungsdatei

Der Befehl `create_swapfile` ist nur nützlich, wenn der Speicher größer oder gleich 16 GB ist und nicht, wenn der Speicher knapp ist. Dieser Befehl prüft also auch, ob Speicher vorhanden ist, bevor mit der Erstellung der Auslagerungsdatei fortgefahren wird.


```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should n
ot be interrupted.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Wenn alle Bedingungen erfüllt sind und der Benutzer zustimmt, fortzufahren, wird eine 32-GB-Auslagerungsdatei auf der sekundären Festplatte erstellt. Die Erstellung der Auslagerungsdatei dauert einige Minuten und sorgt dafür, dass Sie den Vorgang während des Ablaufs nicht unterbrechen. Nach erfolgreichem Abschluss wird ein Neustart durchgeführt, damit die Auslagerungsdatei wirksam wird.

```
Creating swapfile. This may take some time (~5 mins). Please be patient and don't interrupt the process...
32768+0 records in
32768+0 records out
34359738368 bytes transferred in 724.061475 secs (47454173 bytes/sec)

Changing permissions for created swapfile...

Create (swapfile) Done.
VM has to be rebooted for the newly created swapfile to take effect.
```

Nach dem Neustart kann der Anstieg des Swap mit dem Befehl top beobachtet werden.

```
CPU:  1.7% user,  0.0% nice,  0.8% system,  0.2% interrupt, 97.4% idle
Mem: 1847M Active, 506M Inact, 382M Wired, 4684K Cache, 199M Buf, 4473M Free
Swap: 4198M Total, 4198M Free
```

```
CPU: 42.0% user,  0.0% nice,  7.6% system,  5.0% interrupt, 45.3% idle
Mem: 1805M Active, 423M Inact, 393M Wired, 4792K Cache, 199M Buf, 4587M Free
Swap: 36G Total, 36G Free
```

Befehl “Beenden”:

Um das Werkzeug zu verlassen, geben Sie exit ein, und drücken **Sie die Eingabetaste**.

```
(dpt): exit
bash-3.2#
```

Hinzufügen zusätzlicher Datenträger an NetScaler ADM, das in hoher Verfügbarkeit bereitgestellt wird

Stellen Sie sich vor, Sie haben ein Paar NetScaler ADM-Server in einer Hochverfügbarkeitssetup ohne sekundäre Festplatten konfiguriert. Denken Sie auch daran, dass Sie 2 oder mehr NetScaler-Instanzen hinzugefügt und überprüft und sichergestellt haben, dass alle Prozesse ausgeführt werden. Möglicherweise möchten Sie den virtuellen Maschinen in diesem Setup sekundäre Laufwerke hinzufügen. In einer Hochverfügbarkeitseinrichtung müssen Sie zusätzliche Datenträger zu beiden Knoten hinzufügen, wie in dieser Aufgabe beschrieben:

1. Fahren Sie den sekundären Knoten herunter.
2. Fügen Sie eine Festplatte über den Hypervisor hinzu.

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass Sie die Hauptfestplatte des sekundären Knotens nicht erweitern.

3. Starten Sie den sekundären Knoten.
4. Führen Sie das Partitionstool auf dem sekundären Knoten aus.
5. Nachdem der Datenträger hinzugefügt wurde, wird der sekundäre Knoten neu gestartet.
6. Fahren Sie den sekundären Knoten nach dem Neustart herunter.
7. Fahren Sie den primären Knoten herunter.
8. Fügen Sie eine Festplatte über den Hypervisor hinzu.

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass Sie die Hauptfestplatte des primären Knotens nicht erweitern.

9. Starten Sie den primären Knoten.
10. Führen Sie das Partitionstool auf dem primären Knoten aus.
11. Nachdem der Datenträger hinzugefügt wurde, wird der primäre Knoten neu gestartet.
12. Nachdem der primäre Knoten betriebsbereit ist, starten Sie den sekundären Knoten.
13. Stellen Sie sicher, dass der sekundäre Knoten betriebsbereit ist und die Datenbanken synchronisiert wurden.
14. Bestätigen Sie, dass alle Daten noch vorhanden sind.

Um die RAM-Kapazität auf beiden Knoten zu erhöhen:

1. Fahren Sie ADM_Secondary herunter, und erhöhen Sie die RAM-Größe je nach Bedarf. Starten Sie den Knoten nicht neu.
2. Fahren Sie ADM_primary herunter, und erhöhen Sie die RAM-Größe je nach Bedarf.

   Stellen Sie sicher, dass Sie die RAM-Größe auf beiden Knoten gleichmäßig erhöhen. Wenn Sie beispielsweise die RAM-Größe auf dem primären Knoten auf 16 GB erhöhen, tun Sie dasselbe auch auf dem sekundären Knoten.
3. Starten Sie ADM_Primary neu.
4. Überprüfen Sie nach dem Neustart von ADM_Primary, ob es sich um den primären Knoten handelt.

5. Starten Sie den Knoten ADM_Secondary. Stellen Sie nach dem Neustart sicher, dass es als sekundär angezeigt wurde und die DB-Synchronisierung funktioniert.
6. Bestätigen Sie, dass alle Daten noch vorhanden sind.

> **Hinweis:**
>
> Nachdem Sie das sekundäre Laufwerk hinzugefügt haben, dauert es einige Zeit, bis der primäre Knoten aktiviert ist. Außerdem erfordert das gesamte Hinzufügen von sekundären Datenträger zu beiden Knoten und die Erhöhung der RAM-Kapazität, dass beide Knoten für einige Zeit heruntergefahren sind. Berücksichtigen Sie diese Ausfallzeiten bei der Planung dieser Wartungsaktivität.

ADM On-Prem Cloud Connector

February 5, 2024

Sie können die ADM On-Prem Cloud Connector Connector-Funktion verwenden, um eine Verbindung zwischen ADM On-Prem und dem NetScaler Console-Dienst herzustellen.

> **Hinweis:**
>
> Der NetScaler ADM Service wurde jetzt in NetScaler Console Service umbenannt. Unsere Produktuberfläche und Dokumentation werden derzeit aktualisiert, um diesen Änderungen Rechnung zu tragen. Während dieser Zeit stoßen Sie möglicherweise auf die älteren und neueren Namen, auf die synonym verwiesen wird. Wir danken Ihnen für Ihr Verständnis während dieses Übergangs.

Diese Konnektivität ermöglicht es Ihnen, die folgende Funktion für die Verwendung in ADM On-Prem auszuwählen:

Sicherheitsempfehlung —Security Advisory unterstützt die automatische Identifizierung anfälliger NetScaler und bietet Vorteile bei der Behebung von Arbeitsabläufen. Mit Security Advisory können Sie alle neuen Common Vulnerabilities and Exposures (CVEs) verfolgen, die Auswirkungen von CVEs bewerten, die Behebung nachvollziehen und die Sicherheitslücken beheben. Als Administrator können Sie die NetScaler-Instanzen durch den regelmäßigen Scan oder durch manuelles Scannen auf neue CVEs überwachen und die erforderlichen Maßnahmen für die Behebung ergreifen. Weitere Informationen finden Sie unter Sicherheitsempfehlung.

Automatisierte Telemetrieerfassung —Wenn Sie die Flexed-Lizenzierung verwenden, empfehlen wir Ihnen, Cloud Connector zu aktivieren, den automatisierten Modus der Telemetriedatenerfassung. Weitere Informationen finden Sie unter Lizenz für flexible Kapazitäten .

Hinweise:

- Sie müssen die NetScaler-Instanzen nicht zum NetScaler Console Service hinzufügen oder migrieren.
- ADM On-Prem Cloud Connector erfordert, dass Sie eine Verbindung zum NetScaler Console-Dienst herstellen, indem Sie ein NetScaler Console-Dienstkonto einrichten (falls nicht bereits erstellt).
- Ab Version 14.1 8.x ersetzt ADM On-Prem Cloud Connector die Funktion Customer Identity.
- Nachdem Sie den ADM On-Prem Cloud Connector konfiguriert haben, ermöglicht es Citrix Cloud, Lizenz-, Konfiguration- und Nutzungsdaten zur Einhaltung der Lizenzbestimmungen zu sammeln und den Service zu verwalten, zu messen und zu verbessern. Weitere Informationen finden Sie unter Data Governance.

Voraussetzungen

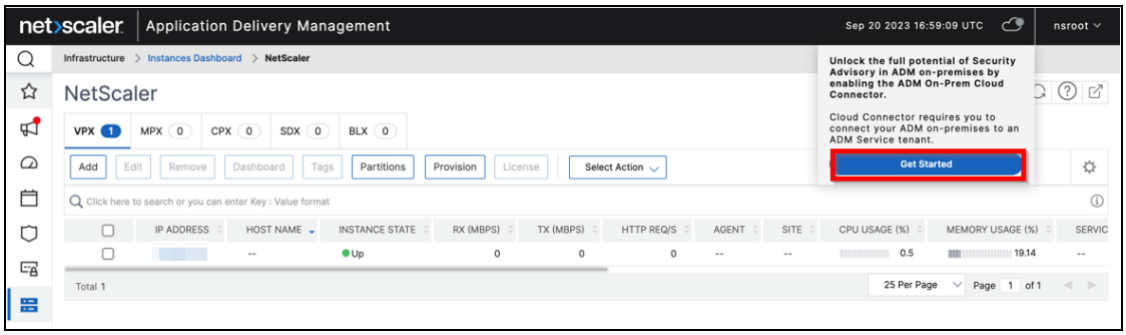
Bevor Sie ADM On-Prem Cloud Connector konfigurieren, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllen:

- Stellen Sie sicher, dass Sie über eine Internetverbindung verfügen oder dass ein Proxyserver in ADM vor Ort konfiguriert ist, um Zugriff auf Citrix Cloud zu erhalten.
- Stellen Sie sicher, dass die folgenden Endpunkt-URLs Zugriff haben:
  - Download-Service:
    `https://download.citrixnetworkapi.net`
  - Treuhand-Service:
    `*.citrixnetworkapi.net`
  - Dienst-URLs
    - `*.agent.adm.cloud.com`
    - `*.adm.cloud.com`
    - `adm.cloud.com`
  - Citrix Cloud-Konnektivität:
    - `Citrix.cloud.com`
    - `Accounts.cloud.com`
- Stellen Sie sicher, dass Sie den Popup-Blocker in dem Browser deaktiviert haben, von dem aus Sie auf die ADM-On-Prem-GUI zugreifen.

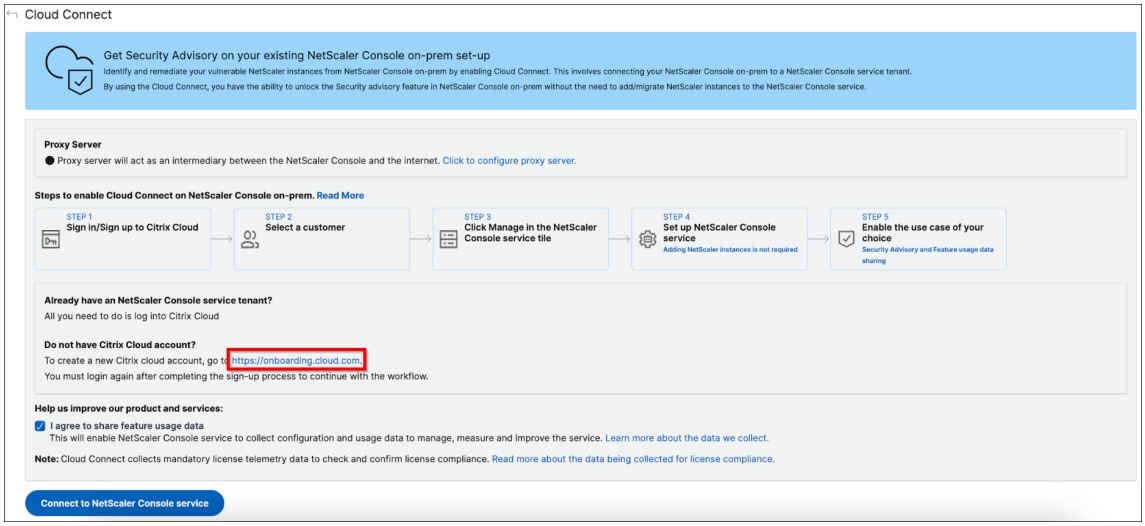
ADM On-Prem Cloud Connector konfigurieren

Workflow 1 —Wenn Sie ein neuer Benutzer ohne Citrix Cloud Cloud-Konto und NetScaler Console Service Tenant sind

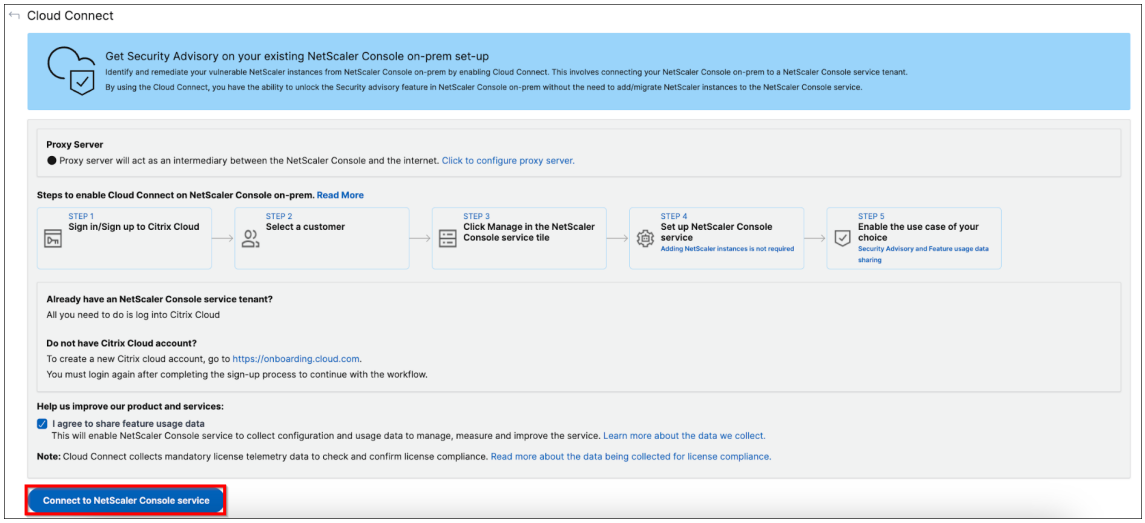
1. Klicken Sie in NetScaler ADM auf das **Cloud-Symbol** > **Erste Schritte.**



2. Klicken Sie auf der Konfigurationsseite von ADM On-Prem Cloud Connector auf den Link. `https://onboarding.cloud.com`

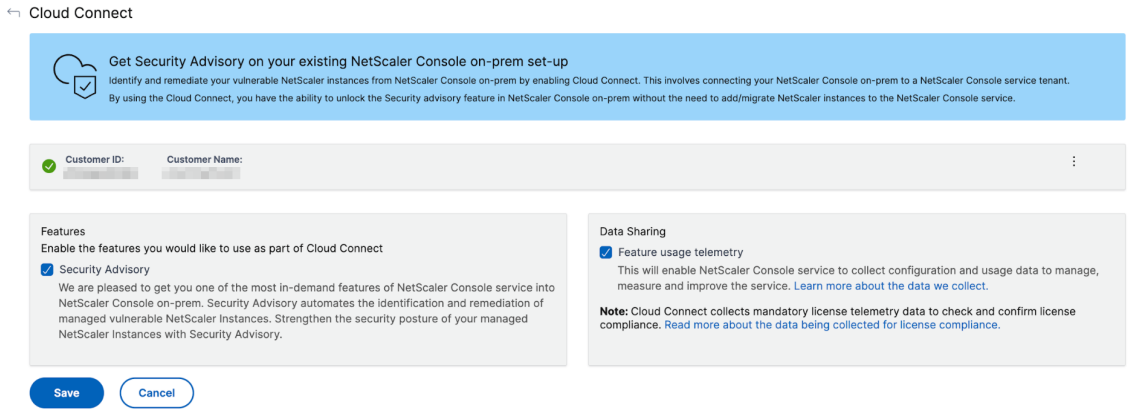


3. Gehen Sie wie in diesem Dokument beschrieben vor, um ein Citrix Cloud-Konto zu erstellen.
4. Nachdem Sie ein Citrix Cloud Cloud-Konto erstellt haben, müssen Sie sich erneut anmelden, indem Sie in **NetScaler ADM auf Mit NetScaler Console Service verbinden** klicken. Nach erfolgreicher Anmeldung leitet die Seite zu den Schritten zur Erstellung des NetScaler Console-Dienstmandanten weiter.

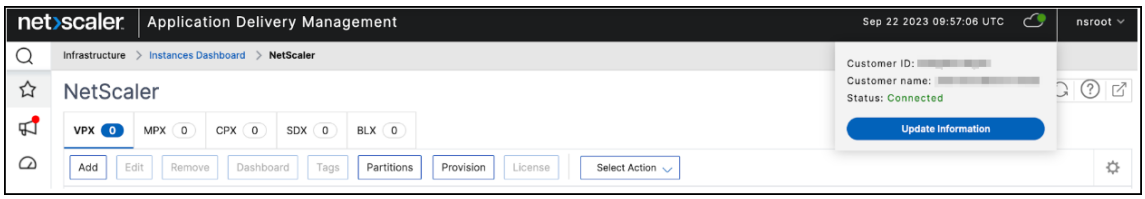


5. Wählen Sie eine Region aus, die Ihren Geschäftsanforderungen entspricht, und klicken Sie auf **Fertig**.
6. Wählen Sie eine Rolle aus und beenden Sie die Einrichtung.

   Es kann einige Minuten dauern, bis die Konfiguration abgeschlossen ist. In ADM können Sie den Bildschirm „ **ADM On-Prem Cloud Connector wird aktiviert** “sehen. Sie können entweder auf **Aktualisieren** klicken und warten, bis Sie die aktualisierte Konfigurationsseite erhalten, oder auf **Abbrechen** klicken, um diesen Bildschirm zu überspringen und später nach der aktualisierten Konfigurationsseite zu suchen.
7. Die Konfiguration des ADM On-Prem Cloud Connector ist abgeschlossen. Sie können auf der Konfigurationsseite des ADM On-Prem Cloud Connector die Sicherheitsempfehlung weiter aktivieren.
8. Wählen Sie **Sicherheitsempfehlung** und klicken Sie auf **Speichern**.

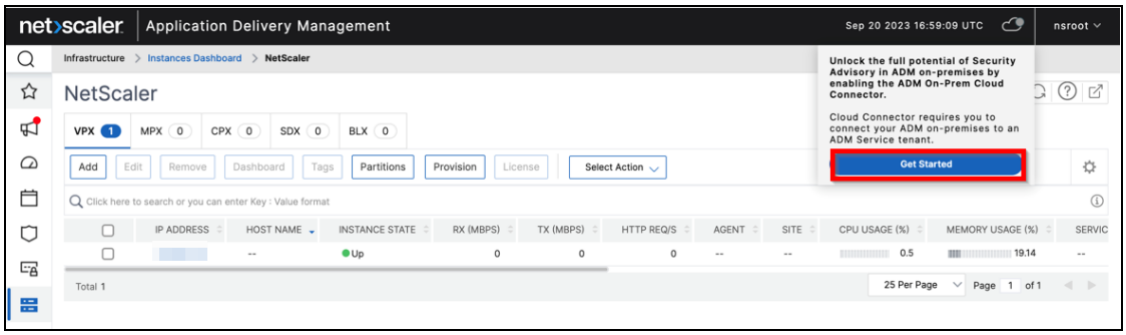


   Sie können den Status als verbunden sehen.

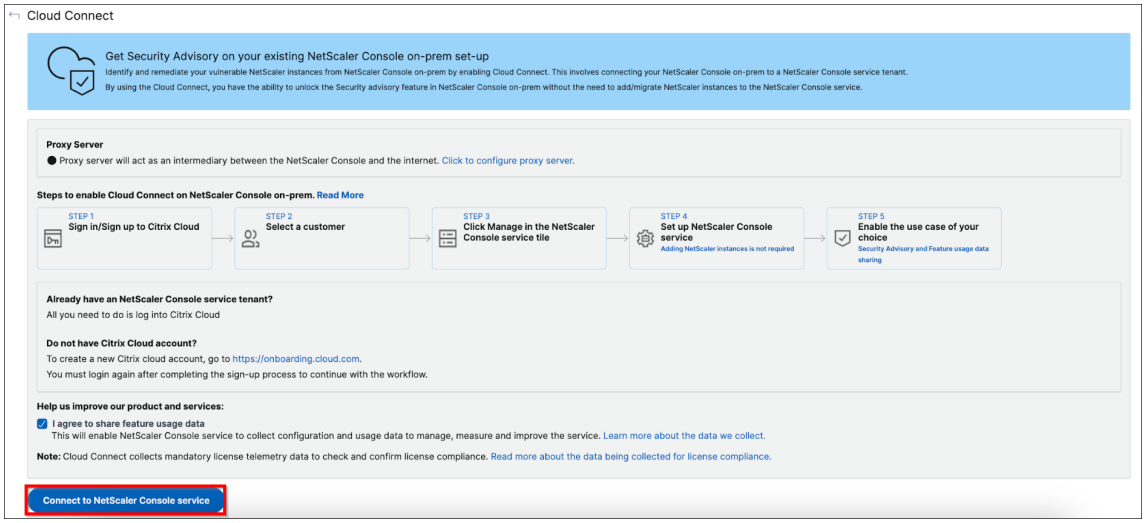


Workflow 2 —Wenn Sie ein Citrix Cloud Cloud-Konto, aber keinen NetScaler Console Service-Mandanten haben

1. Klicken Sie in NetScaler ADM auf das **Cloud-Symbol** > **Erste Schritte.**



2. Klicken Sie auf Mit **NetScaler Console Service verbinden** .

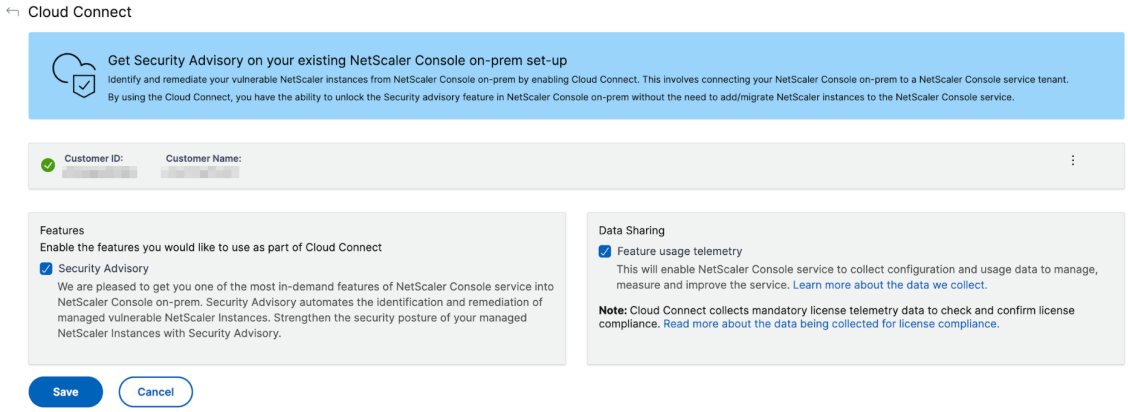


3. Sie werden zu einem neuen Tab weitergeleitet. Melden Sie sich bei Citrix Cloud an.
4. Sobald Sie die Meldung über eine erfolgreiche Anmeldung erhalten haben, leitet die Seite zu den ADM-Onboarding-Schritten weiter.
5. Wählen Sie eine Region aus, die Ihren Geschäftsanforderungen entspricht, und klicken Sie auf Fertig.
6. Wählen Sie eine Rolle aus und beenden Sie die Einrichtung.

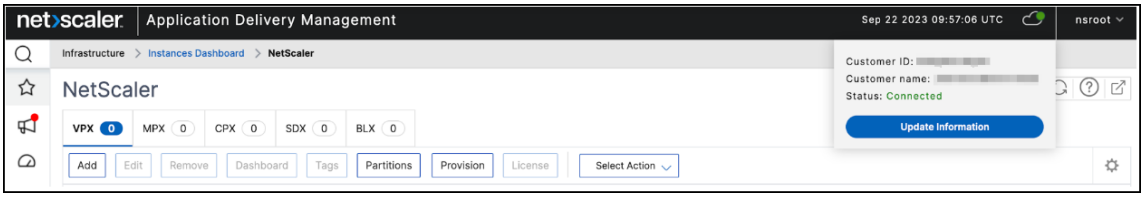
Es kann einige Minuten dauern, bis die Konfiguration abgeschlossen ist. In ADM können Sie den Bildschirm „ **ADM On-Prem Cloud Connector wird aktiviert** “sehen. Sie können entweder auf **Aktualisieren** klicken und warten, bis Sie die aktualisierte Konfigurationsseite erhalten, oder auf **Abbrechen** klicken, um diesen Bildschirm zu überspringen und später nach der aktualisierten Konfigurationsseite zu suchen.

7. Die Konfiguration des ADM On-Prem Cloud Connector ist abgeschlossen. Sie können auf der Konfigurationsseite des ADM On-Prem Cloud Connector die Sicherheitsempfehlung weiter aktivieren.

8. Wählen Sie **Sicherheitsempfehlung** und klicken Sie auf **Speichern**.

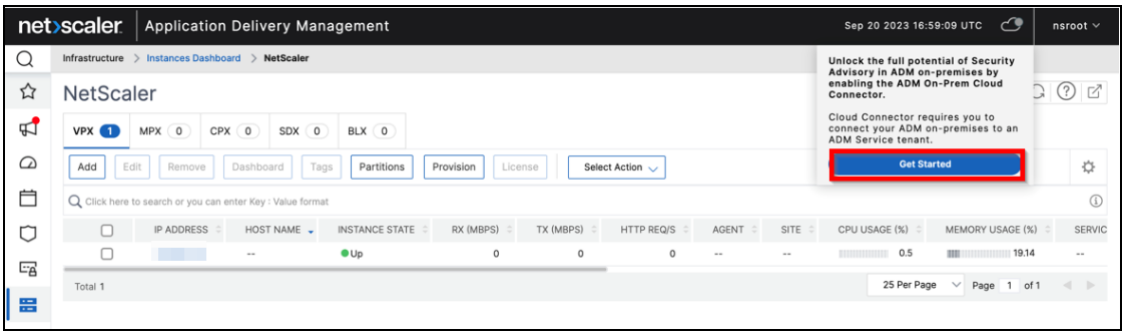


Sie können den Status als verbunden sehen.

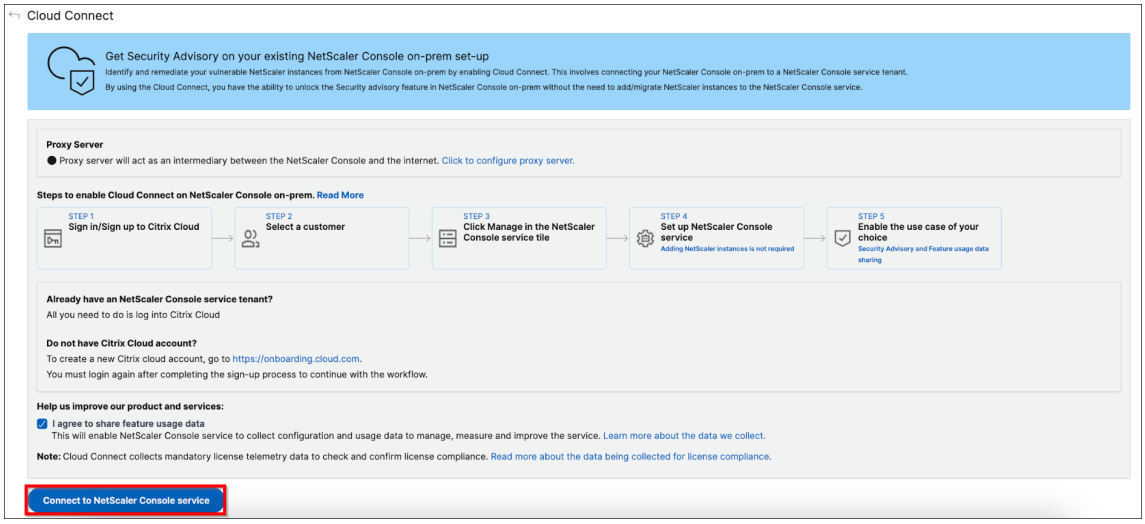


Workflow 3 —Wenn Sie ein vorhandener Benutzer sind, der sowohl ein Citrix Cloud Cloud-Konto als auch einen NetScaler Console-Dienstmandanten hat

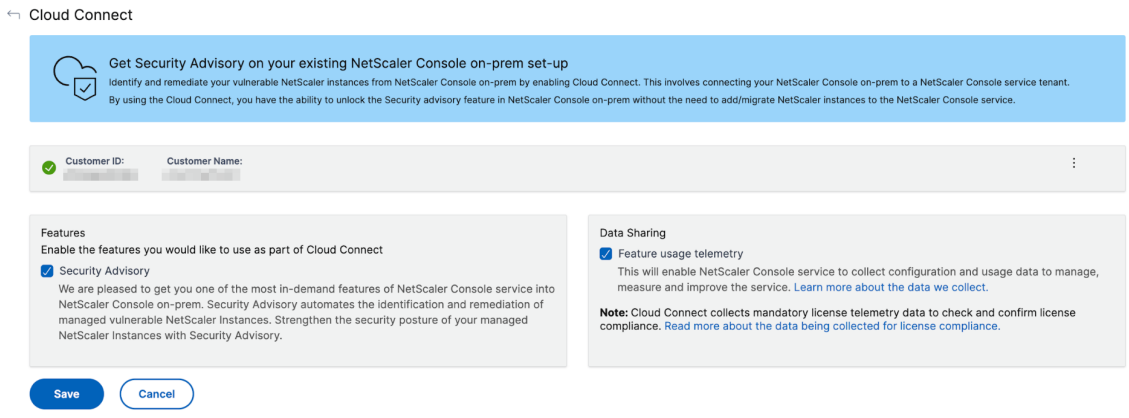
1. Klicken Sie in NetScaler ADM auf das **Cloud-Symbol** > **Erste Schritte.**



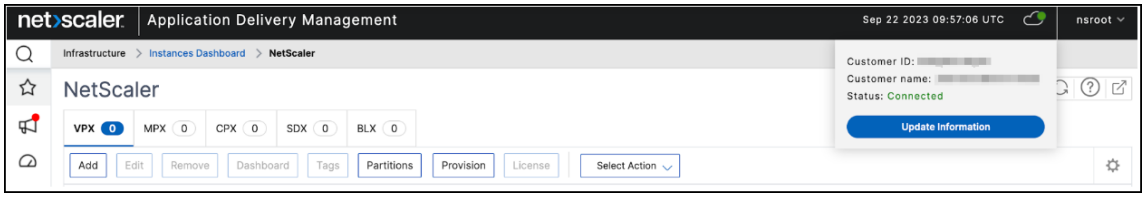
2. Klicken Sie auf Mit **NetScaler Console Service verbinden** .



3. Sie werden zu einem neuen Tab weitergeleitet. Melden Sie sich bei Citrix Cloud an und wählen Sie einen Mandanten aus. Nachdem Sie den Mandanten ausgewählt haben, erhalten Sie eine Meldung, dass die Anmeldung erfolgreich war.
4. Die Konfiguration des ADM On-Prem Cloud Connector ist abgeschlossen. Sie können auf der Konfigurationsseite des ADM On-Prem Cloud Connector die Sicherheitsempfehlung weiter aktivieren.
5. Wählen Sie **Sicherheitsempfehlung** und klicken Sie auf **Speichern**.



Sie können den Status als verbunden sehen.

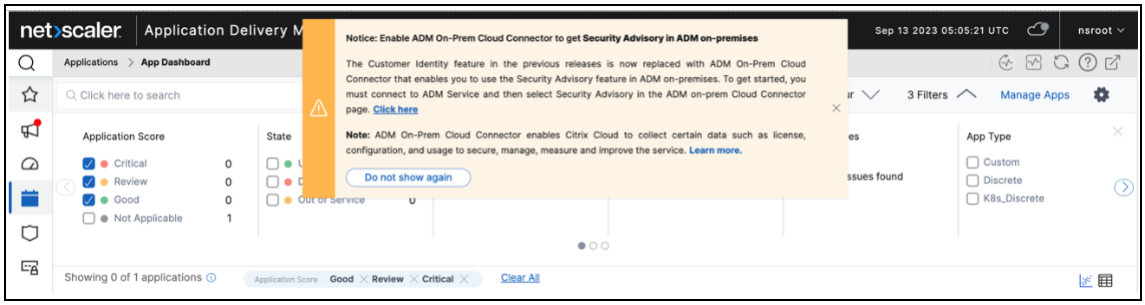


Was passiert, wenn Customer Identity bereits aktiviert ist?

Wenn Sie bereits ein Benutzer eines früheren Builds sind, bei dem Customer Identity aktiviert ist, die gemeinsame Nutzung von Daten ausgewählt und ein Upgrade auf den neuesten Build (14.1 8.x) durchgeführt wurde, gelten die folgenden Szenarien:

- Wenn Sie einen NetScaler Console-Dienstmandanten haben, wird ADM On-Prem Cloud Connector automatisch in Ihrem lokalen ADM aktiviert. Damit kann Citrix Cloud Lizenz-, Konfiguration- und Nutzungsdaten sammeln, um den Service zu verwalten, zu messen und zu verbessern. Weitere Informationen finden Sie unter Data Governance. Auf der Cloud Connector-Konfigurationsseite können Sie **Security Advisory** auswählen, um die Funktion zu verwenden.

  Die folgende Benachrichtigung wird angezeigt, wenn ADM On-Prem Cloud Connector automatisch in Ihrem NetScaler ADM konfiguriert ist.



- Wenn Sie keinen NetScaler Console-Dienstmandanten haben oder die gemeinsame Nutzung von Daten nicht als Teil der Kundenidentität aktiviert ist, wird der ADM On-Prem Cloud Connector nicht automatisch aktiviert und Sie müssen den Cloud Connector manuell konfigurieren. Nach der Konfiguration kann Citrix Cloud Lizenz-, Konfiguration- und Nutzungsdaten sammeln, um den Service zu verwalten, zu messen und zu verbessern. Erfahren Sie mehr über die Datenerhebung.

Andere Optionen

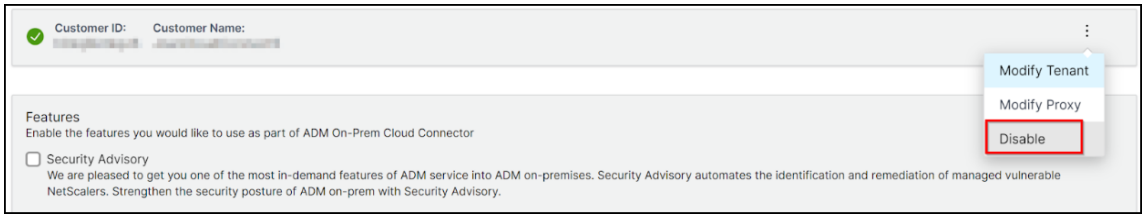
Nachdem Sie ADM On-Prem Cloud Connector aktiviert haben, können Sie die folgenden Optionen verwenden:

- **Mandant ändern** —Ermöglicht es Ihnen, den vorhandenen Mandanten zu ändern. Wenn Sie auf **Mandant ändern**klicken, werden Sie zu einer neuen Registerkarte weitergeleitet und müssen sich bei Citrix Cloud anmelden. Nach erfolgreicher Anmeldung können Sie einen anderen Mandanten auswählen.
- **Proxy ändern** —Ermöglicht es Ihnen, die Proxyeinstellungen in ADM On-Prem zu konfigurieren. Dies ist erforderlich, wenn NetScaler ADM über das Verwaltungsnetzwerk keinen direkten Zu-

griff auf das Internet hat. Klicken Sie in der Liste auf **Proxy ändern**, aktualisieren Sie die Details und klicken Sie dann auf **Speichern**.

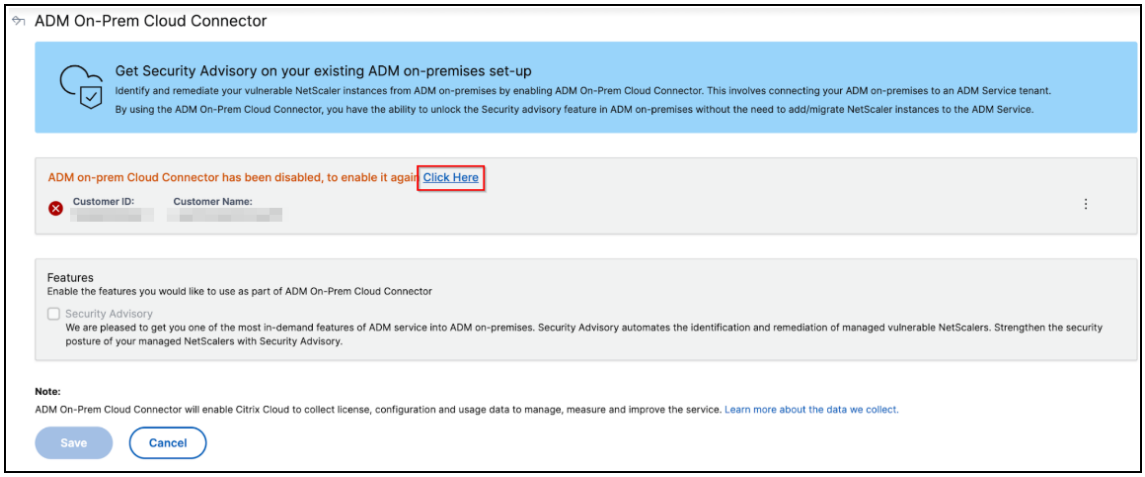
- **Deaktivieren**—**Deaktiviert** die ADM On-Prem Cloud Connector-Funktion. Wenn Sie sich für die Deaktivierung entscheiden, ist die Erfassung von Datenmetriken deaktiviert und Sie können die Vollversion der Sicherheitsempfehlung nicht verwenden.

  Um zu deaktivieren, klicken Sie in der Liste auf **Deaktivieren** .



  Eine Bestätigungsmeldung wird angezeigt. Klicken Sie zum Deaktivieren auf **Ja** .

  Sie können ADM On-Prem Cloud Connector später ohne weitere Schritte wieder aktivieren.



Sicherheitsempfehlung deaktivieren

Auf der Konfigurationsseite von ADM On-Prem Cloud Connector können Sie auch das Kontrollkästchen Sicherheitsempfehlung deaktivieren, um die **Sicherheitsempfehlung** zu deaktivieren. Die Datenmetriken werden weiterhin gesammelt.

Konfigurieren

February 5, 2024

Sie können nur mit der GUI auf einen NetScaler ADM-Server zugreifen. Sie müssen auf die GUI zugreifen, um Instanzen und Apps hinzuzufügen, Instanzen und Apps zu verwalten und zu überwachen, Analysen anzuzeigen und den NetScaler ADM -Server zu konfigurieren.

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

Die folgenden Browser werden unterstützt.

Webbrowser	Version
Internet Explorer	11.0 und höher
Google Chrome	Chrome 19 und höher
Safari	Safari 5.1.1 und höher
Mozilla Firefox	Firefox 3.6.25 und später

So greifen Sie auf die NetScaler ADM GUI zu:

Melden Sie sich mit den Administratoranmeldeinformationen bei NetScaler ADM an.

Nachdem Sie sich bei NetScaler ADM angemeldet haben, müssen Sie folgende Schritte ausführen:

- Instanzen zu NetScaler ADM hinzufügen. Sie müssen dem NetScaler ADM Server Instanzen hinzufügen, wenn Sie diese Instanzen verwalten und überwachen möchten.
- Ermöglichen Sie Analysen auf virtuellen Servern.Um Analysedaten für den Anwendungsdatenfluss anzuzeigen, müssen Sie die Analytics-Funktion auf den virtuellen Servern aktivieren, die Datenverkehr für die spezifischen Anwendungen empfangen.
- Konfigurieren Sie den NTP-Server auf NetScaler ADM. Sie müssen einen NTP-Server (Network Time Protocol) in NetScaler ADM konfigurieren, um seine Uhr mit dem NTP-Server zu synchronisieren.
- Konfigurieren Sie die Systemeinstellungen für eine optimale NetScaler ADM-Leistung. Bevor Sie NetScaler ADM zur Verwaltung und Überwachung Ihrer Instanzen und Anwendungen verwenden, wird empfohlen, einige Systemeinstellungen zu konfigurieren, die eine optimale Leistung Ihres NetScaler ADM-Servers gewährleisten.

Instanzen zu NetScaler ADM hinzufügen

February 5, 2024

Instanzen sind NetScaler Appliances oder virtuelle Appliances, die Sie von NetScaler ADM aus erkennen, verwalten und überwachen möchten. Sie müssen dem NetScaler ADM-Server Instanzen hinzufügen, wenn Sie diese Instanzen verwalten und überwachen möchten. Sie können NetScaler ADM die folgenden NetScaler Appliances und virtuellen Appliances hinzufügen:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway

Sie können Instanzen hinzufügen, wenn Sie den NetScaler ADM-Server zum ersten Mal oder später einrichten. Anschließend müssen Sie ein Instanzprofil angeben, mit dem NetScaler ADM auf die Instanz zugreifen kann.

> **Hinweis:**
>
> - NetScaler ADM verwendet die NetScaler IP (NSIP) -Adresse der NetScaler Instanzen für die Kommunikation. Informationen zu den Ports, die zwischen den NetScaler-Instanzen und NetScaler ADM geöffnet sein müssen, finden Sie unter Ports.
> - Informationen darüber, wie NetScaler ADM Instanzen erkennt, finden Sie unter Instanzen entdecken.

Erstellen eines NetScaler Profils

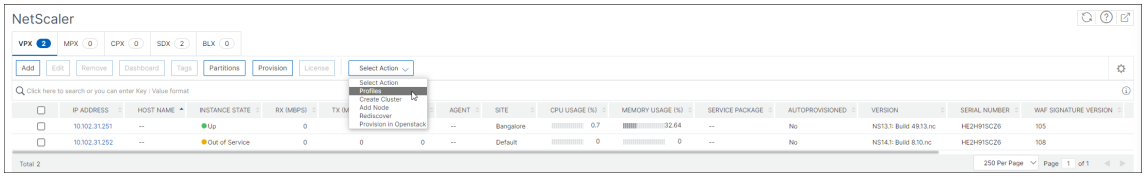
Das NetScaler-Profil enthält die Anmeldeinformationen, Ports und Authentifizierungstypen für das Hinzufügen von Instanzen zu NetScaler ADM. Für jeden Instanztyp ist ein Standardprofil verfügbar. Zum Beispiel ist `nsroot` das Standardprofil für NetScaler-Instanzen. Das Standardprofil wird mithilfe der standardmäßigen NetScaler Administratoranmeldeinformationen definiert. 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 ein NetScaler Profil auf der **Instanzseite** oder beim Hinzufügen oder Ändern einer Instanz erstellen.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie das Superadministratorkonto verwenden, um ein Instanzprofil zu erstellen.

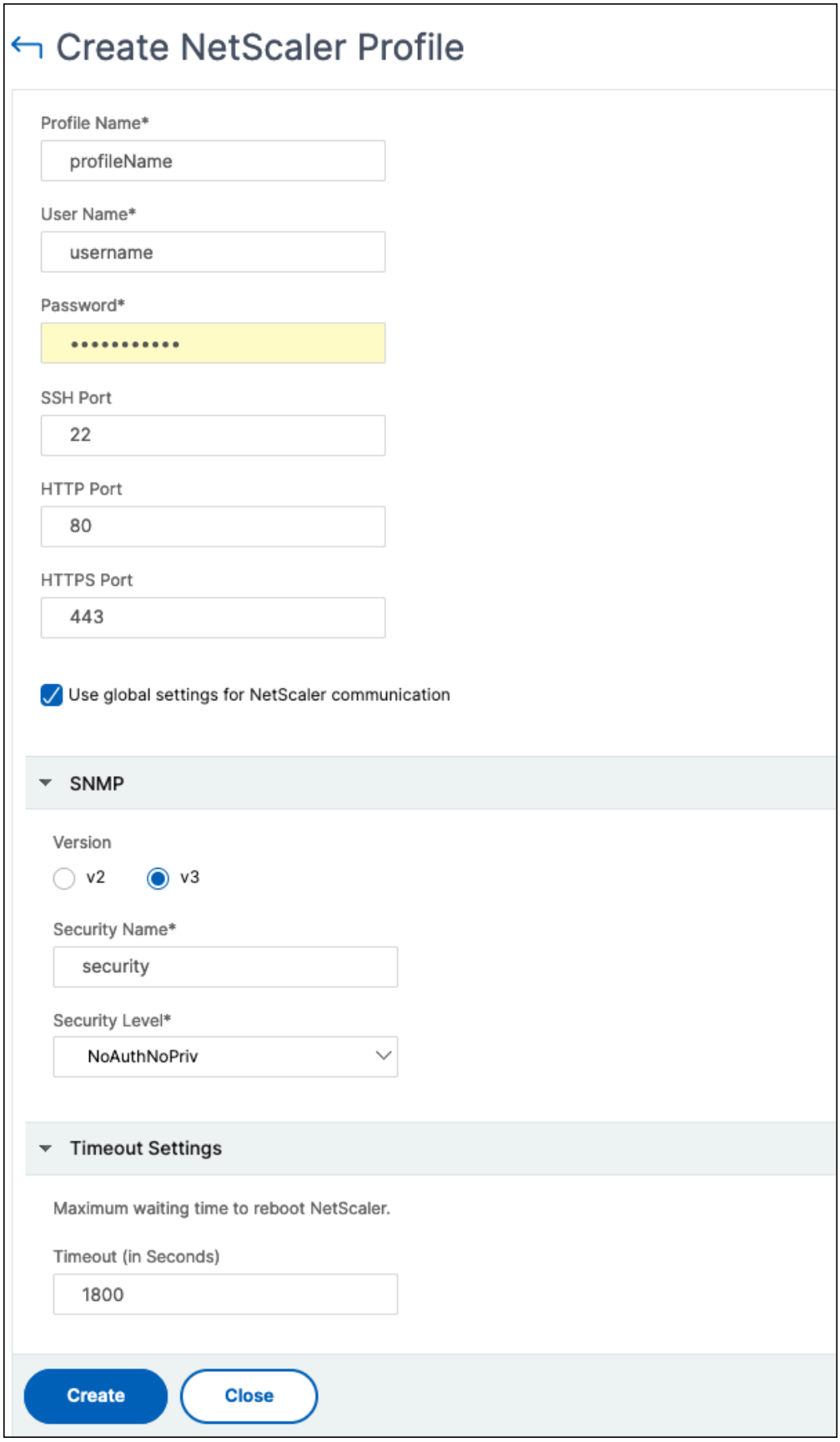
So erstellen Sie ein NetScaler Profil auf der Instanzseite:

1. Navigieren Sie zu **Infrastruktur > Instanzen**.
2. Wählen Sie eine Instanz aus. Beispiel: NetScaler.
3. Wählen Sie auf der NetScaler-Seite unter **Aktion auswählen** die Option **Profile**aus.



4. Wählen Sie auf der Seite **Admin-Profile** die Option **Hinzufügen**aus.

5. Gehen Sie auf der Seite **NetScaler-Profil erstellen** wie folgt vor:



a) **Profilname**: Geben Sie einen Profilnamen für die NetScaler-Instanz an.

b) **Benutzername**: Geben Sie einen Benutzernamen an, um sich bei der NetScaler-Instanz anzumelden.

c) **Kennwort**: Geben Sie ein Kennwort an, um sich an der NetScaler-Instanz anzumelden.

d) **SSH-Port**: Geben Sie den Port für die SSH-Kommunikation zwischen NetScaler ADM und der NetScaler-Instanz an.

e) **HTTP-Port**: Geben Sie den Port für die HTTP-Kommunikation zwischen NetScaler ADM und der NetScaler-Instanz an.

> **Hinweis:**
>
> Der Standard-HTTP-Port ist 80. Sie können auch den nicht standardmäßigen oder benutzerdefinierten HTTP-Port angeben, den Sie möglicherweise in Ihrer NetScaler CPX-Instanz konfiguriert haben. Der benutzerdefinierte HTTP-Port kann nur für die Kommunikation zwischen NetScaler ADM und NetScaler CPX verwendet werden.

f) **HTTPS-Port**: Geben Sie den Port für die HTTPS-Kommunikation zwischen NetScaler ADM und der NetScaler-Instanz an.

> **Hinweis:**
>
> Der Standard-HTTPS-Port ist 443. Sie können auch den nicht standardmäßigen oder benutzerdefinierten HTTPS-Port angeben, den Sie möglicherweise in Ihrer NetScaler CPX-Instanz konfiguriert haben. Der angepasste HTTPS-Port kann nur für die Kommunikation zwischen NetScaler ADM und NetScaler CPX verwendet werden.

g) **Globale Einstellungen für NetScaler-Kommunikation**verwenden: Wählen Sie diese Option, wenn Sie die Systemeinstellungen für die Kommunikation zwischen NetScaler ADM und NetScaler-Instanz verwenden möchten, andernfalls wählen Sie entweder HTTP oder https aus.

h) **SNMP-Version**: Wählen Sie entweder **SNMPv2** oder **SNMPv3** aus, und führen Sie die folgenden Schritte aus:

   i. Wenn Sie SNMPv2 auswählen, geben Sie den **Community-Namen** für die Authentifizierung an.

   ii. Wenn Sie SNMPv3 auswählen, geben Sie den **Sicherheitsnamen** und die **Sicherheitsstufe an**. Wählen Sie basierend auf der Sicherheitsstufe den **Authentifizierungstyp** und den **Datenschutztyp**aus.

   > **Hinweis:**
   >
   > Für NetScaler SDX wird nur **SNMPv2** unterstützt.

i) **Timeout-Einstellungen**: Geben Sie die Zeit an, die NetScaler ADM warten muss, bevor es nach einem Neustart eine Verbindungsanfrage an die NetScaler-Instanz sendet.

j) Wählen Sie **Create**.

Fügen Sie ADC-Instanzen zu NetScaler ADM hinzu

Sie können Instanzen hinzufügen, wenn Sie den NetScaler ADM-Server zum ersten Mal oder später einrichten.

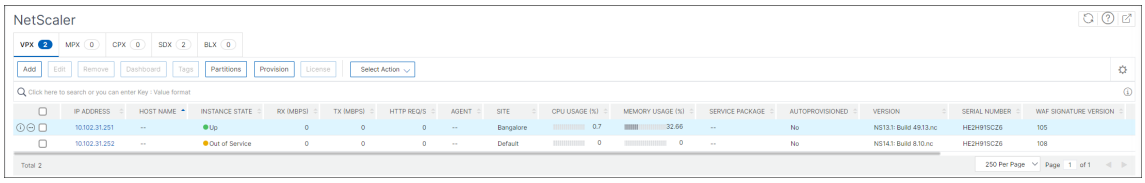
Um Instanzen hinzuzufügen, müssen Sie entweder den Hostnamen oder die IP-Adresse jeder NetScaler-Instanz oder einen Bereich von IP-Adressen angeben.

> **Hinweis:**
>
> - Um NetScaler-Instanzen hinzuzufügen, die in einem Cluster konfiguriert sind, müssen Sie entweder die Cluster-IP-Adresse oder einen der einzelnen Knoten im Cluster-Setup angeben. In NetScaler ADM wird der Cluster jedoch nur durch die Cluster-IP-Adresse dargestellt.
> - Bei NetScaler Instanzen, die als HA-Paar eingerichtet sind, wird beim Hinzufügen einer Instanz automatisch die andere Instanz im Paar hinzugefügt.

Wenn Sie eine Instanz aus Remotedaten hinzufügen, die mit einem On-Prem-Agenten konfiguriert sind, erfolgt die Traffic-Quelle über den ADM-Agenten.

So fügen Sie NetScaler ADM eine Instanzhinzu:

1. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler ADM an.
2. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** . Wählen Sie den Instanztyp aus, den Sie hinzufügen möchten (z. B. NetScaler VPX), und klicken Sie auf **Hinzufügen**.



3. Wählen Sie eine der folgenden Optionen:

   - **Geräte-IP-Adresse eingeben**: Geben Sie für NetScaler Instanzen entweder den Hostnamen oder die IP-Adresse der einzelnen Instanzen oder einen Bereich von IP-Adressen an.

     Wenn Sie mithilfe von SNIP ein ADC-HA-Paar ermitteln möchten, stellen Sie sicher, dass der INC-Modus (Independent Network Configuration) aktiviert ist. Und geben Sie die SNIP-Adressen im folgenden Format an:


```
<SNIP of primary instance>#<SNIP of secondary instance>
<!--NeedCopy-->
```

Beispiel: `10.10.10.11#10.10.10.12`

- **Aus Datei importieren**—Laden Sie von Ihrem lokalen System eine Textdatei hoch, die die IP-Adressen aller Instanzen enthält, die Sie hinzufügen möchten.

4. **Wählen Sie unter Profilname das entsprechende Instanzprofil aus, oder erstellen Sie ein Profil, indem Sie auf das Pluszeichen klicken.
5. Wählen Sie unter **Site** den Standort aus, an dem Sie die Instanz hinzufügen möchten, oder erstellen Sie einen Standort, indem Sie auf das Plussymbol klicken.**
6. Klicken Sie auf **OK** , um das Hinzufügen von Instanzen zu NetScaler ADM zu starten.

> **Hinweis:**
>
> Wenn Sie eine Instanz erneut entdecken möchten, navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**. Wählen Sie den Instanztyp aus (z. B. VPX), wählen Sie die Instanz aus, die Sie neu ermitteln möchten, und klicken Sie dann in der Liste **Aktion auswählen** auf **Wiedererkennen**.

Fügen Sie NetScaler CPX-Instanzen zu NetScaler ADM hinzu

NetScaler ADM wurde erweitert, um die Verbesserungen der CPX-Funktionen zu unterstützen. Die NetScaler CPX-Instanz wird jetzt in NetScaler ADM hinzugefügt, indem eine IP-Adresse für die CPX zusammen mit einem Geräteprofil bereitgestellt wird. Das Hinzufügen einer CPX-Instanz ähnelt jetzt dem Hinzufügen anderer ADC-Typen wie VPX oder MPX in ADM. Außerdem wurde die Registrierung von CPX in ADM verbessert. Wenn ein CPX gestartet wird, erkennt und registriert NetScaler ADM automatisch die CPX-Instanz. Eine CPX-Instanz wird nicht mehr über den Docker-Host erkannt.

1. Navigieren Sie zu **Infrastruktur > Instances > NetScaler** und klicken Sie auf **CPX**.
2. Klicken Sie auf **Hinzufügen**, um neue CPX-Instanzen in NetScaler ADM hinzuzufügen.
3. Die Seite **NetScaler CPX** hinzufügen wird geöffnet. Geben Sie die Werte für die folgenden Parameter ein:

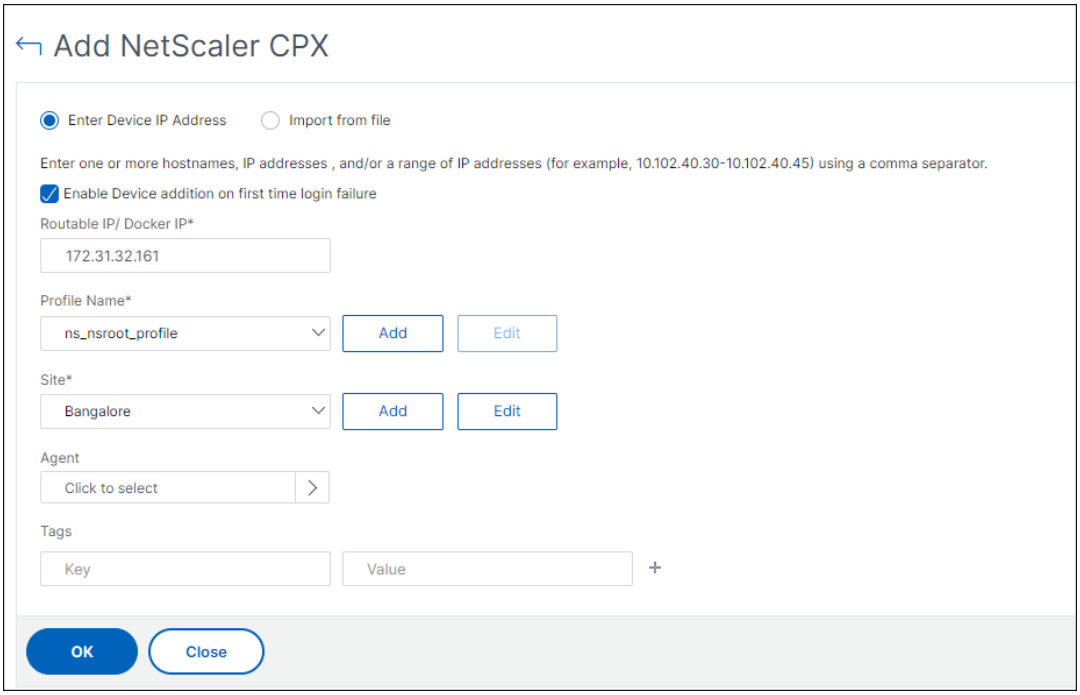
   a) Sie können CPX-Instanzen hinzufügen, indem Sie entweder die erreichbare IP-Adresse der CPX-Instanz oder die IP-Adresse des Docker-Containers angeben, in dem die CPX-Instanz gehostet wird.

   b) Wählen Sie das Profil der CPX-Instanz aus.

   c) Wählen Sie den Standort aus, an dem die Instanzen bereitgestellt werden sollen.

   d) Wählen Sie den Agenten aus.

e) Optional können Sie das Schlüssel-Wert-Paar für die Instanz eingeben. Das Hinzufügen eines Schlüssel-Wert-Paares erleichtert Ihnen die spätere Suche nach der Instanz.



> **Hinweis:**
>
> Für NetScaler CPX-Instanzen müssen Sie beim Erstellen des CPX-Instanzprofils die **HTTP-, HTTPS-, SSH**- und **SNMP-Portdetails** des Hosts angeben. Sie können auch den Portbereich, der vom Host veröffentlicht wurde, in den Feldern **Startport** und **Anzahl der Ports** angeben.

4. Klicken Sie auf **OK**.

Fügen Sie eine eigenständige NetScaler BLX-Instanz in NetScaler ADM hinzu

Eine eigenständige NetScaler BLX-Instanz ist eine einzelne Instanz, die auf dem dedizierten Host-Linux-Server ausgeführt wird.

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** .
2. Klicken Sie auf der Registerkarte **BLX** auf **Hinzufügen**.
3. Wählen Sie in der Liste **Instanztyp** die Option **Standalone** 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. 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 Host-Benutzernamen und das richtige Kennwort des Linux-Servers im Profil angegeben haben.

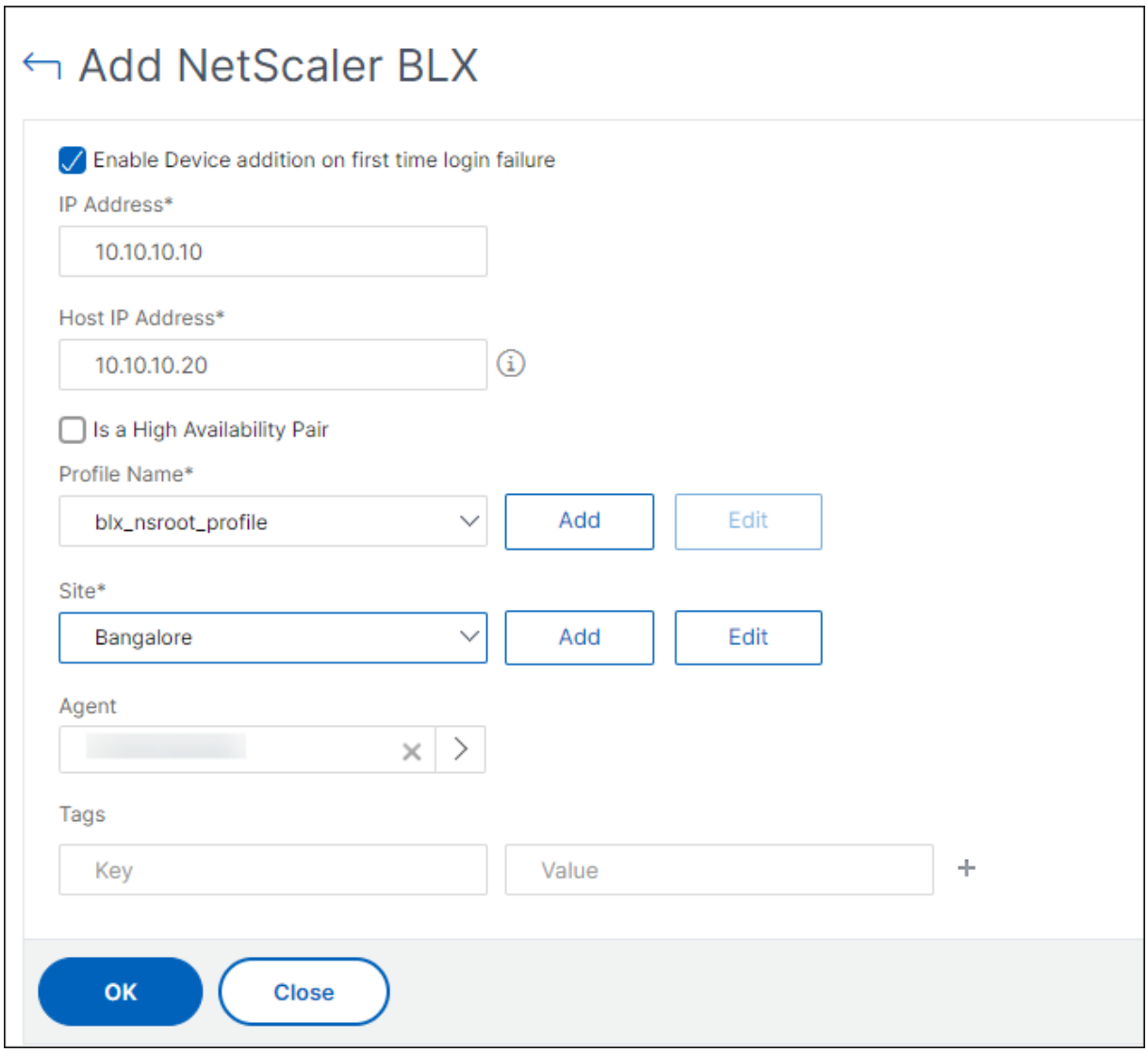
7. Wählen Sie in der Liste **Site** die Site aus, der Sie eine Instanz hinzufügen möchten.

   Wenn Sie eine Site hinzufügen möchten, klicken Sie auf **Hinzufügen**.

8. Wählen Sie in der Liste **Agent** den NetScaler ADM Agent aus, dem Sie die Instanz zuordnen möchten.

   Wenn auf Ihrem NetScaler ADM nur ein Agent konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.

9. Klicken Sie auf **OK**.



Fügen Sie hochverfügbare NetScaler BLX-Instanzen in NetScaler ADM hinzu

Die hochverfügbaren NetScaler BLX-Instanzen, die auf verschiedenen Host-Linux-Servern ausgeführt werden. Ein Linux-Server kann nicht mehr als eine BLX-Instanz hosten.

1. Klicken Sie auf der Registerkarte **BLX** auf **Hinzufügen**.
2. Wählen Sie die Option **Hochverfügbarkeit** aus der Liste **Instanztyp** aus.
3. Geben Sie im Feld **IP-Adresse** die IP-Adresse der BLX-Instanz an.
4. Geben Sie im Feld **Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die BLX-Instanz gehostet wird.
5. Geben Sie im Feld **Peer-IP-Adresse** die IP-Adresse der Peer-BLX-Instanz an.

6. Geben Sie im Feld **Peer-Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die Peer-BLX-Instanz gehostet wird.
7. Wählen Sie in der Liste **Profilname** das entsprechende Profil für eine BLX-Instanz aus, oder erstellen Sie ein Profil.

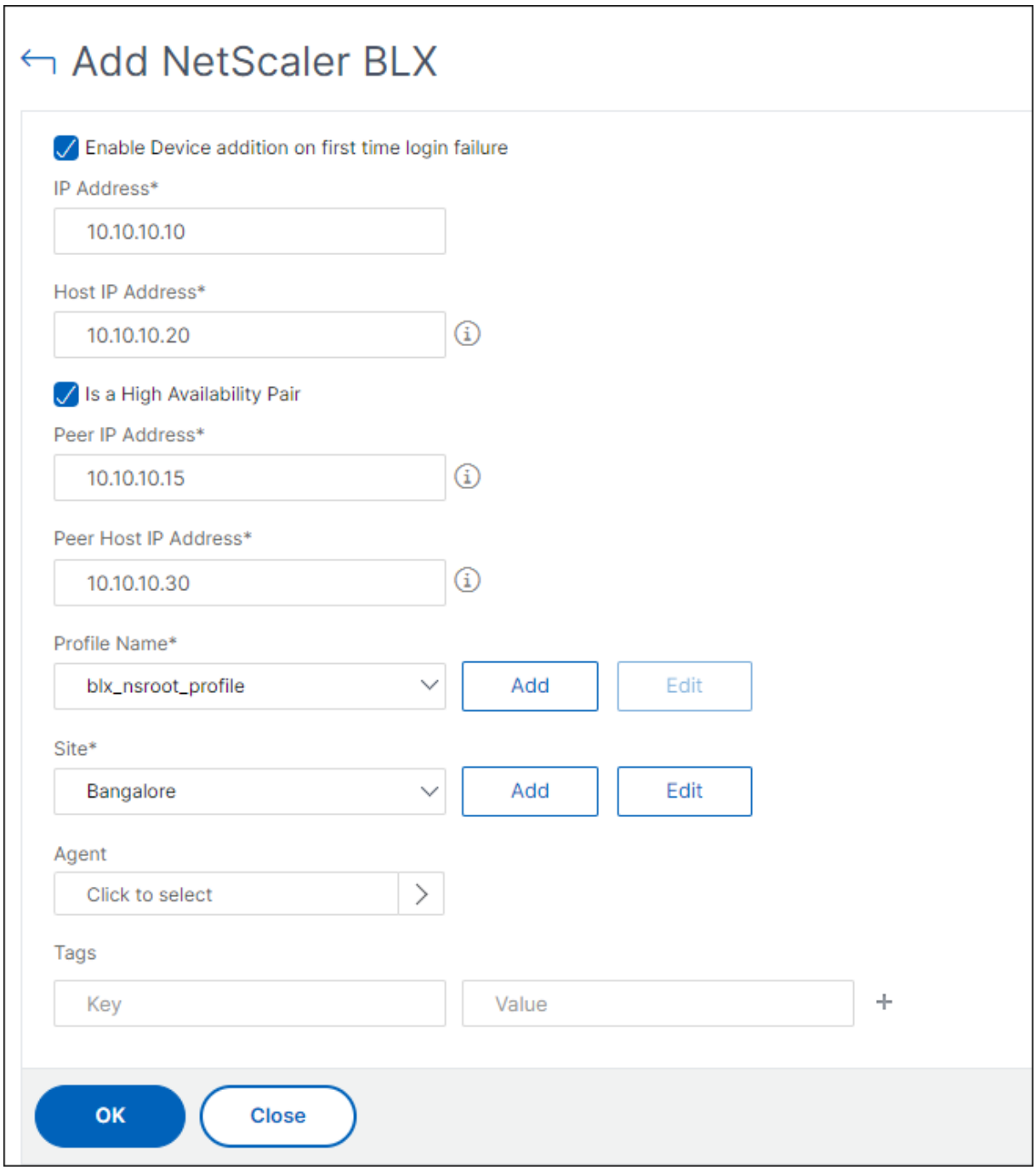
   Um ein Profil zu erstellen, klicken Sie auf **Hinzufügen**.

   > **Wichtig:**
   >
   > Stellen Sie sicher, dass Sie den richtigen Host-Benutzernamen und das richtige Kennwort des Linux-Servers im Profil angeben.

8. Wählen Sie in der Liste **Site** die Site aus, der Sie eine Instanz hinzufügen möchten.

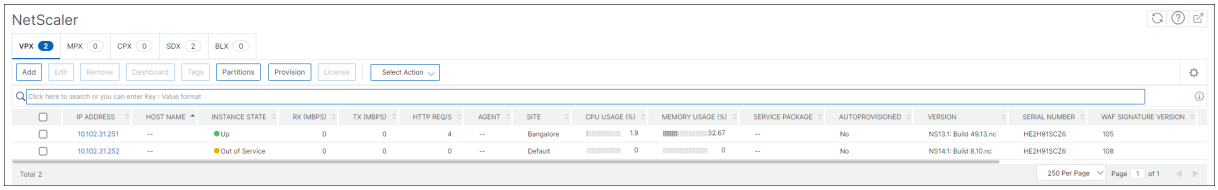
   Wenn Sie eine Site hinzufügen möchten, klicken Sie auf **Hinzufügen**.
9. Wählen Sie in der Liste **Agent** den NetScaler ADM Agent aus, dem Sie die Instanz zuordnen möchten.

   Wenn auf Ihrem NetScaler ADM nur ein Agent konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.
10. Klicken Sie auf **OK**.



Zugriff auf eine Instanz-GUI über das NetScaler ADM

1. Navigieren Sie zu **Infrastruktur > Instanzen** > **NetScaler** .
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 NetScaler IP-Adresse oder den Hostnamen.



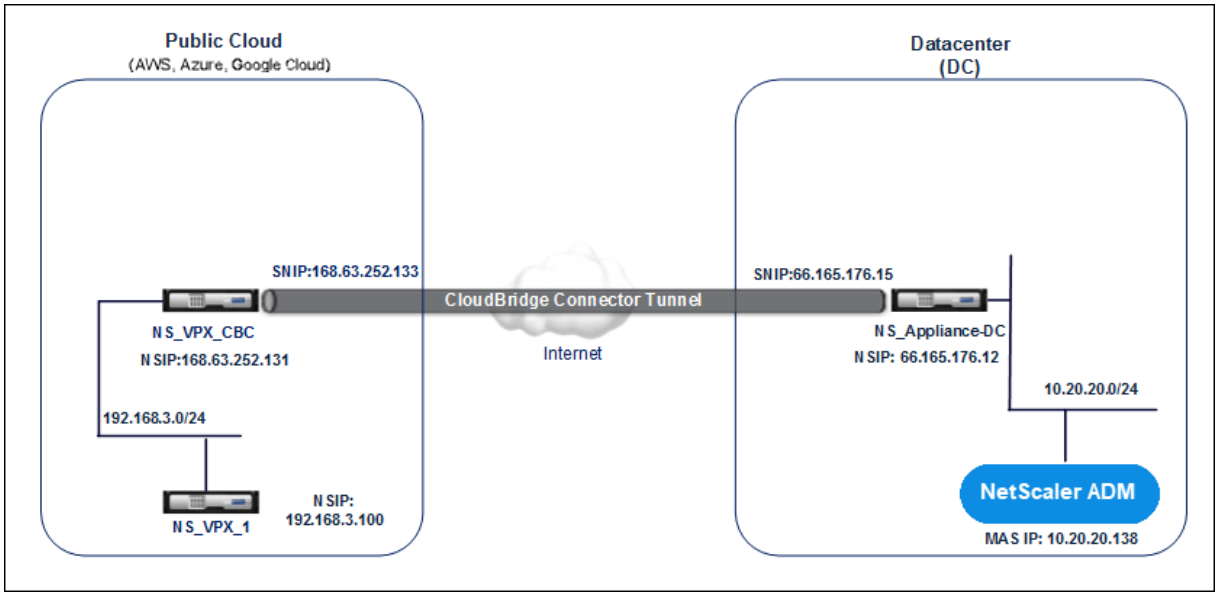
Die GUI der ausgewählten Instanz wird in einem Popup-Fenster angezeigt.

Hinzufügen von NetScaler VPX Instanzen, die in der Cloud bereitgestellt werden, zu NetScaler ADM

February 5, 2024

Sie können NetScaler ADM verwenden, um die NetScaler VPX-Instanzen zu verwalten und zu überwachen, die in einer öffentlichen Cloud wie Amazon Web Services (AWS), Microsoft Azure oder Google Cloud bereitgestellt werden. Sie müssen Layer 3-Konnektivität zwischen NetScaler ADM und den in der Public Cloud bereitgestellten NetScaler VPX-Instanzen herstellen. Um die Layer-3-Konnektivität herzustellen, können Sie Lösungen wie Direct Connect to AWS, VPN in Azure oder Connectoren von Drittanbietern wie Equinix usw. verwenden.

Die folgende Beispieltopologie verwendet Citrix CloudBridge Connector für Layer 3-Konnektivität zwischen NetScaler ADM und den in der Cloud bereitgestellten NetScaler VPX-Instanzen.

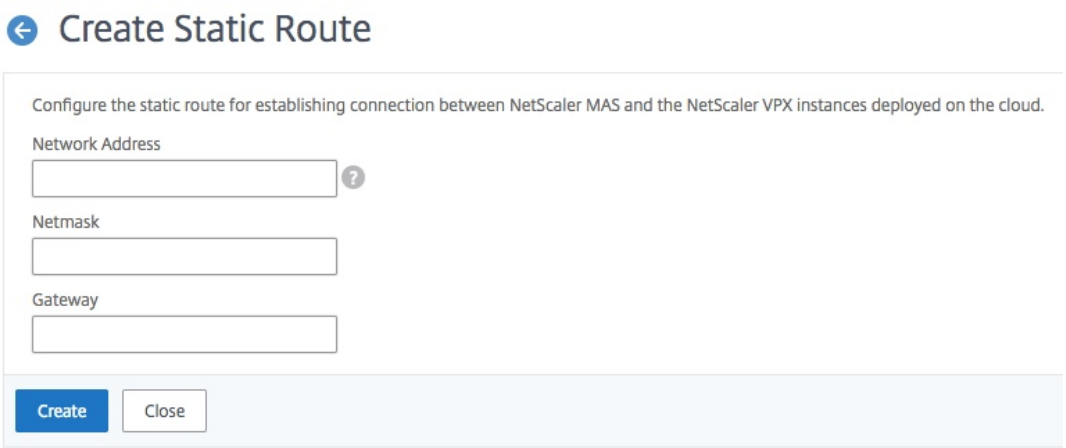


Ein Citrix CloudBridge Connector-Tunnel wird zwischen der NetScaler Appliance NS_Appliance-DC in einem Rechenzentrums-DC und der virtuellen NetScaler Appliance (VPX) NS_VPX_CBC in der Public Cloud eingerichtet. NS_Appliance-DC und NS_VPX_CBC ermöglichen die Kommunikation zwischen NetScaler ADM und der NetScaler VPX Instanz, NS_VPX_1, die in der Public Cloud bereitgestellt

wird. Nachdem die Kommunikation hergestellt wurde, können Sie NS_VPX_1 in NetScaler ADM entdecken.

Gehen Sie wie folgt vor, um diese Topologie zu konfigurieren:

1. Installieren, konfigurieren und starten Sie eine NetScaler VPX Instanz in der Public Cloud.
   - Anweisungen findenSie unter Installieren von NetScaler VPX auf AWS.
   - Anweisungen finden Sie unter Installieren von NetScaler VPX auf Microsoft Azure.
   - Anweisungen finden Sie unter Installieren von NetScaler VPX in Google Cloud.
2. Stellen Sie eine physische NetScaler Appliance bereit und konfigurieren Sie sie oder stellen Sie eine virtuelle NetScaler Appliance (VPX) auf einer Virtualisierungsplattform im Rechenzentrum bereit und konfigurieren Sie sie.
   - Anweisungen finden Sie unter Installieren einer NetScaler VPX-Instanz auf Citrix Hypervisor.
   - Anweisungen finden Sie unter Installieren virtueller Citrix Appliances auf VMware ESXi.
   - Anweisungen finden Sie unter Installieren virtueller NetScaler Appliances auf Microsoft Hyper-V.
3. Konfigurieren Sie den Citrix CloudBridge Connector zwischen dem Rechenzentrum und der Public Cloud. Anweisungen finden Sie unter Konfigurieren von Citrix CloudBridge Connector.
4. Konfigurieren Sie die statische Route zum Herstellen einer Verbindung zwischen NetScaler ADM und den in der Cloud bereitgestellten NetScaler VPX Instanzen wie folgt:
   a) Melden Sie sich bei NetScaler ADM an.
   b) Navigieren Sie zu **System > Statische Routen**, und klicken Sie auf **Hinzufügen**.



c) Geben Sie im Feld **Netzwerkadresse** die Adresse des Netzwerks ein, für das Sie eine statische Route von NetScaler ADM über den Connector einrichten möchten.

d) Geben Sie im Feld **Netzmaske** die Netzmaske für das Netzwerk ein.

e) Geben Sie im Feld **Gateway** die Adresse des Gateways ein.

5. Fügen Sie die NetScaler VPX Cloudinstanzen zum NetScaler ADM hinzu, indem Sie den Bereich der IP-Adressen von NetScaler VPX Instanzen in der Public Cloud angeben. Ausführliche Anweisungen finden Sie unter Instanzen zu NetScaler ADM hinzufügen.

Lizenzierung verwalten und Analysen auf virtuellen Servern aktivieren

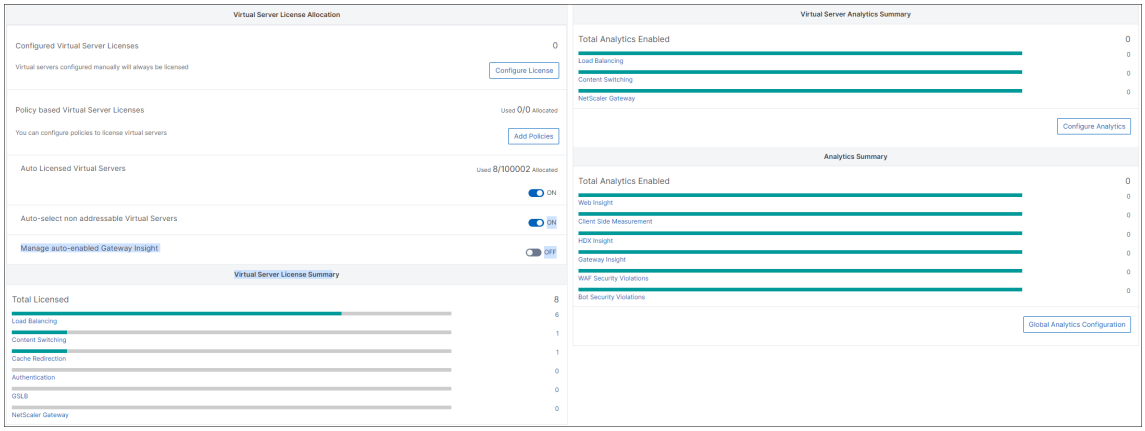
February 5, 2024

> **Hinweis**
>
> - Standardmäßig ist die Option **Automatisch lizenzierte virtuelle Server** aktiviert. Sie müssen sicherstellen, dass Sie über ausreichende Lizenzen verfügen, um die virtuellen Server zu lizenzieren. Wenn Sie über begrenzte Lizenzen verfügen und nur die ausgewählten virtuellen Server basierend auf Ihren Anforderungen lizenzieren möchten, deaktivieren Sie die Option **Automatisch lizenzierte virtuelle Server** . Navigieren Sie zu **Einstellungen > Lizenzierung und Analytics-Konfiguration** und deaktivieren Sie die Option **Automatisch lizenzierte virtuelle Server** unter **Zuweisung virtueller Server-Lizenzen**.

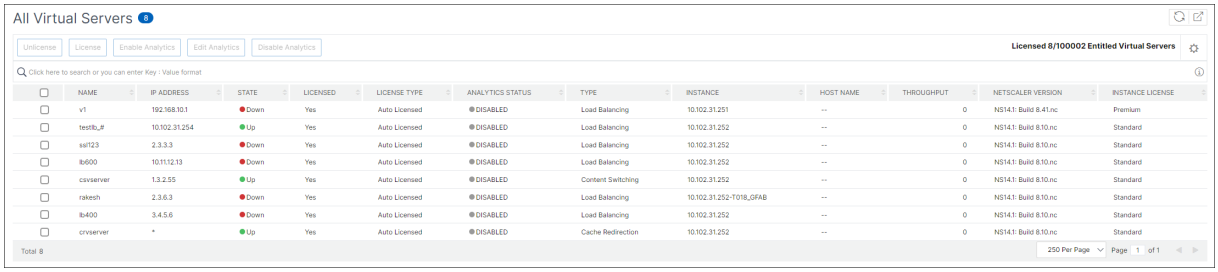
Der Prozess der Aktivierung von Analysen wird vereinfacht. Sie können den virtuellen Server lizenzieren und Analysen in einem einzigen Workflow aktivieren.

Navigieren Sie zu **Einstellungen > Lizenzierung und Analytics-Konfiguration**, um:

- Übersicht über **virtuelle Server-Lizenzen** anzeigen
- Zusammenfassung der **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:

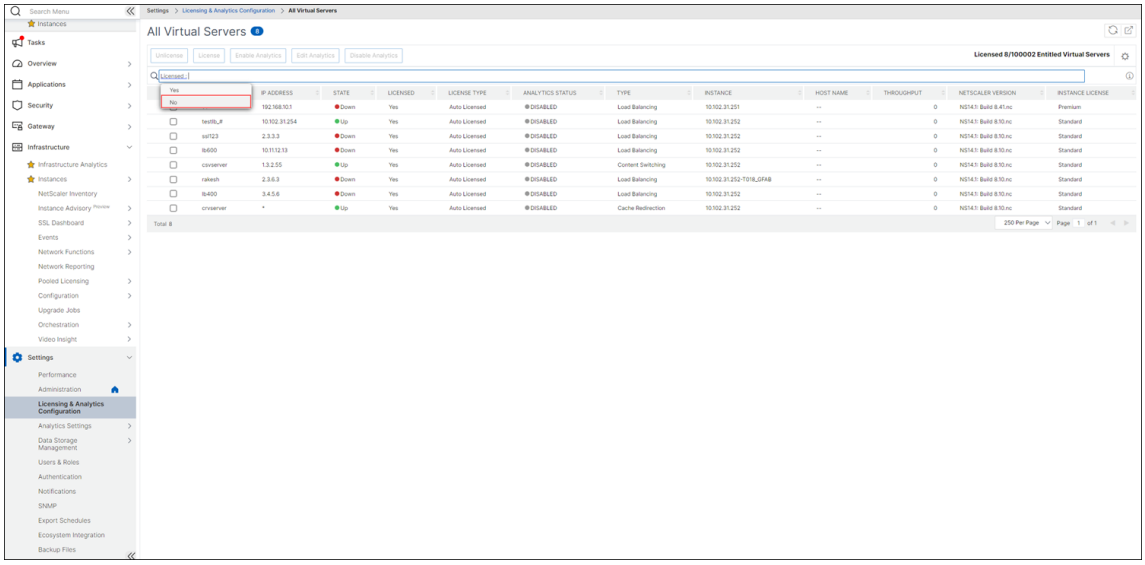
- Lizenz für nicht lizenzierte virtuelle Server beantragen
- Lizenz für lizenzierte virtuelle Server entfernen
- Analytik auf lizenzierten virtuellen Servern aktivieren
- Analytics bearbeiten
- Analytics deaktivieren

> **Hinweis**
>
> Die unterstützten virtuellen Server zum Aktivieren von Analysen sind Load Balancing, Content Switching und NetScaler Gateway.

Verwalten der Lizenzierung auf virtuellen Servern

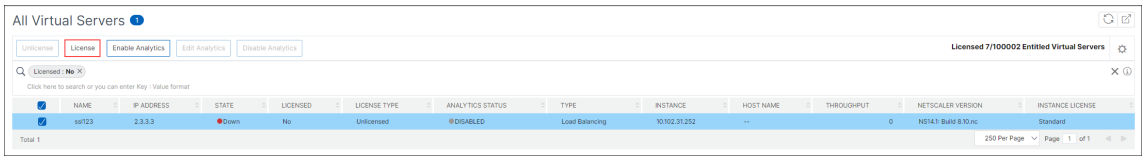
So lizenzieren Sie die virtuellen Server auf der Seite **Alle virtuellen Server** :

1. Klicken Sie auf die Suchleiste, wählen Sie **Lizenziert**und dann **Nein**aus.



Der Filter wird jetzt angewendet und nur die nicht lizenzierten virtuellen Server werden angezeigt.

2. Wählen Sie die virtuellen Server aus und klicken Sie dann auf **Lizenz**.



Um die Lizenz der virtuellen Server aufzuheben, gehen Sie auf der Seite **Alle virtuellen Server** wie folgt vor:

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

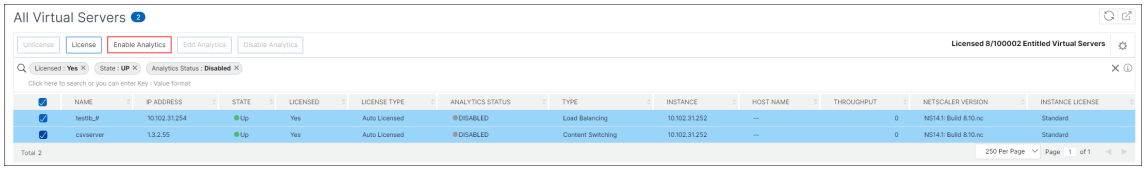
Im Folgenden sind die Voraussetzungen für die Aktivierung von Analysen für virtuelle Server aufgeführt:

- Sicherstellen, dass virtuelle Server **lizenziert** sind
- Stellen Sie sicher, dass Analysestatus **Deaktiviert**
- 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**.



> **Hinweis**
>
> Alternativ können Sie Analysen für eine bestimmte Instanz aktivieren:
>
> ```
> 1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler **, und wählen Sie dann den Instanztyp aus. Zum Beispiel VPX.
> 2
> 3 1. Wählen Sie die Instanz aus und wählen Sie in der Liste **„Aktion auswählen** “ die Option **Analytics konfigurieren ** aus.
> 4 1. Wählen Sie auf der Seite „Analytics auf virtuellen Servern konfigurieren “ den virtuellen Server aus und klicken Sie auf **Analytics aktivieren**.
> ```

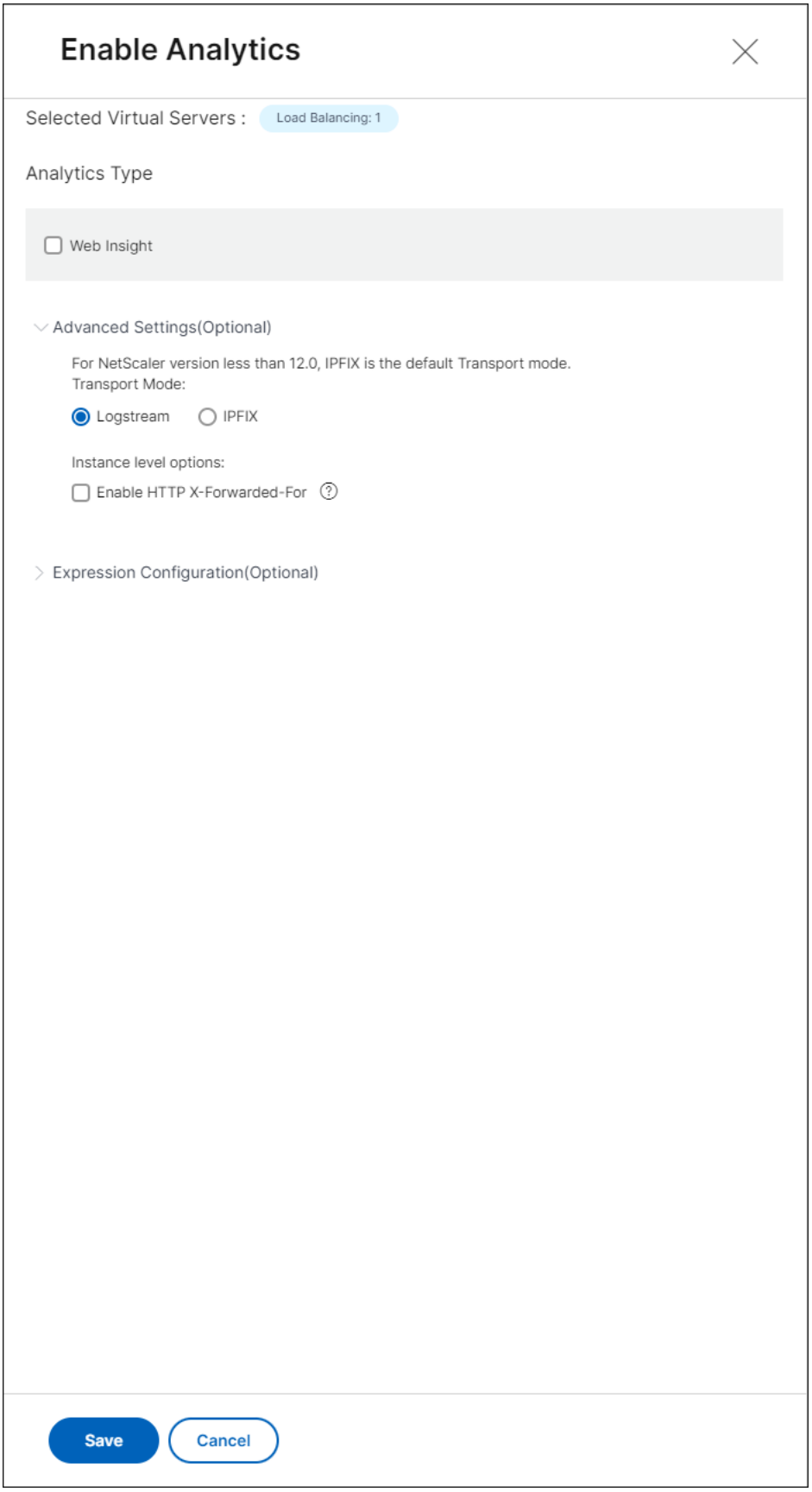
5. Gehen Sie im Fenster **Enable Analytics** wie folgt vor:
   a) Wählen Sie die Insight-Typen aus (Web Insight oder WAF-Sicherheitsverletzungen)
   b) Wählen Sie **Logstream** als Transportmodus

      > **Hinweis**
      >
      > Für NetScaler 12.0 oder früher ist **IPFIX** die Standardoption für den Transportmodus. Für NetScaler 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.
      >
      > Weitere Informationen zu IPFIX und Logstream finden Sie unter Logstream-Übersicht .

   c) Unter **Optionen auf Instanzebene**:
      - **HTTP X-Forwarded-For aktivieren** —Wählen Sie diese Option aus, um die IP-Adresse für die Verbindung zwischen Client und Anwendung über den HTTP-Proxy oder den Load Balancer zu ermitteln.
      - **NetScaler Gateway** —Wählen Sie diese Option aus, um Analysen für NetScaler Gateway anzuzeigen.

d) Der Ausdruck ist standardmäßig wahr

e) Klicken Sie auf **OK**.



> **Hinweis**
>
> - Wenn Sie virtuelle Server auswählen, die nicht lizenziert sind, lizenziert NetScaler ADM zuerst diese virtuellen Server und aktiviert dann Analysen.
> - Für Admin-Partitionen wird nur **Web Insight** unterstützt
> - Für virtuelle Server wie Cache-Umleitung , Authentifizierung und GSLB können Sie Analysen nicht aktivieren. Eine Fehlermeldung wird angezeigt.

Nachdem Sie auf **OK** geklickt haben, verarbeitet NetScaler ADM Analysen auf den ausgewählten virtuellen Servern zu aktivieren.

> **Hinweis**
>
> NetScaler ADM verwendet NetScaler SNIP für Logstream und NSIP für IPFIX. Wenn zwischen dem NetScaler ADM-Agenten und der NetScaler-Instance eine Firewall aktiviert ist, stellen Sie sicher, dass Sie den folgenden Port öffnen, damit NetScaler ADM AppFlow-Verkehr erfassen kann:

Transport-Modus	Quell-IP	Typ	Port
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

Analytics bearbeiten

So bearbeiten Sie Analysen auf den virtuellen Servern:

1. Wählen Sie die virtuellen Server aus

   > Hinweis
   >
   > Alternativ können Sie auch Analysen für eine bestimmte Instanz bearbeiten:

   ```
   1.  Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler **, und wählen Sie dann den Instanztyp aus. Zum Beispiel VPX.
   2
   3.  Wählen Sie die Instanz aus und klicken Sie auf **Analytics bearbeiten**.
   ```

2. Klicken Sie auf **Analytics bearbeiten**
3. Bearbeiten Sie die Parameter, die Sie anwenden möchten, im Fenster **“Analytics-Konfiguration bearbeiten** “
4. Klicken Sie auf **OK**.

Analytics deaktivieren

So deaktivieren Sie Analysen auf den ausgewählten virtuellen Servern:

1. Wählen Sie die virtuellen Server aus
2. Klicken Sie auf **Analytics deaktivieren**

NetScaler ADM deaktiviert die Analyse auf den ausgewählten virtuellen Servern

In der folgenden Tabelle werden die Features von NetScaler ADM beschrieben, die IPFIX und Logstream als Transportmodus unterstützen:

Feature	IPFIX	Logstream
Web Insight	•	•
Sicherheitsverletzungen der WAF	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Nicht unterstützt	•
CR-Einblick	•	•
IP-Reputation	•	•
AppFirewall	•	•
Kundenseitige Messung	•	•
Syslog/Auditlog	•	•

Einheitlicher Prozess zur Ermöglichung von Analysen auf virtuellen Servern

February 5, 2024

Neben dem vorhandenen Prozess zur Ermöglichung von Analysen können Sie auch einen einseitigen Workflow verwenden, um Analysen zu folgenden Themen zu konfigurieren:

- Alle vorhandenen lizenzierten virtuellen Server
- Die nachfolgenden lizenzierten virtuellen Server

Nach der Konfiguration macht diese Funktion die manuelle Aktivierung von Analysen auf den vorhandenen und nachfolgenden virtuellen Servern überflüssig.

Zu beachtende Punkte:

Bevor Sie Analytics konfigurieren, müssen Sie die folgenden Verhaltensweisen von NetScaler ADM verstehen:

- Wenn Sie diese Funktion zum ersten Mal konfigurieren, müssen Sie sicherstellen, dass die in diesem Dokument genannten Voraussetzungen erfüllt sind.
- Ändern Sie die Analyseeinstellungen später.

  Bedenken Sie, dass Sie die Analyseeinstellungen zum ersten Mal konfiguriert haben, indem Sie Web Insight, HDX Insight und Gateway Insight auswählen. Wenn Sie die Analyseeinstellungen später ändern und Gateway Insight abwählen möchten, wirken sich die Änderungen nicht auf die virtuellen Server aus, die bereits mit Analytics aktiviert sind.
- Die virtuellen Server, die bereits mit Analytics aktiviert sind.

  Bedenken Sie, dass Sie über 10 lizenzierte virtuelle Server verfügen und zwei davon bereits mit Analytics aktiviert sind. In diesem Szenario ermöglicht diese Funktion Analysen nur für die verbleibenden acht virtuellen Server.
- Die virtuellen Server, die mit Analytics manuell deaktiviert werden.

  Bedenken Sie, dass Sie über 10 lizenzierte virtuelle Server verfügen und die Analyse für zwei virtuelle Server manuell deaktiviert haben. In diesem Szenario ermöglicht diese Funktion Analysen nur für die verbleibenden acht virtuellen Server und überspringt die virtuellen Server, die manuell mit Analytics deaktiviert wurden.
- Die Optionen für**Bot-Sicherheitsverletzungen** und **WAF-Sicherheitsverletzungen** werden nur in virtuellen Premium-Servern unterstützt. Wenn die virtuellen Server nicht Premium-lizenziert sind, sind **Bot-Sicherheitsverletzungen** und **WAF-Sicherheitsverletzungen** nicht aktiviert.

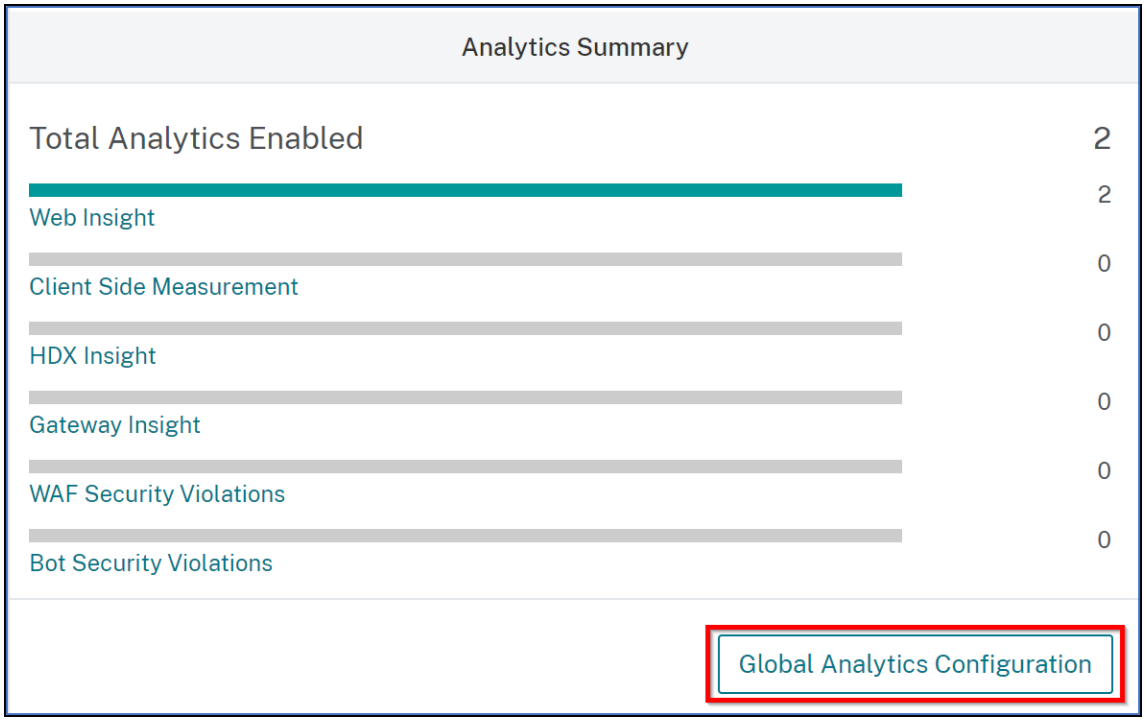
Voraussetzungen

Stellen Sie Folgendes sicher:

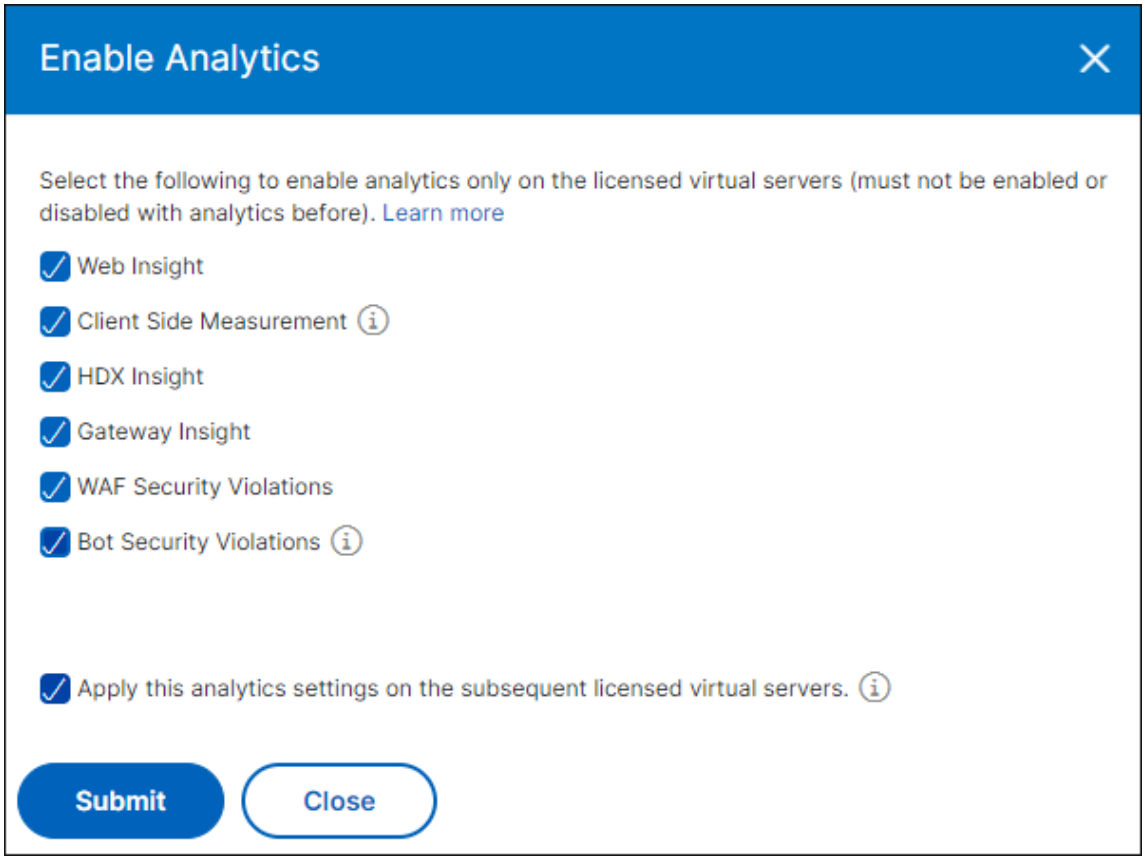
- Alle vorhandenen virtuellen Server sind lizenziert.
- Die Option “Automatisch lizenziert”ist aktiviert, um alle nachfolgenden virtuellen Server zu lizenzieren. Navigieren Sie zu **Einstellungen > Licensing & Analytics Config**, und aktivieren Sie unter **Virtuelle Server-Lizenzzuweisung**die Option **Automatisch lizenzierte virtuelle Server** .

Analytics aktivieren

1. Navigieren Sie zu **Einstellungen > Lizenzierung und Analytics-Konfiguration**.
2. Klicken Sie unter **Analytics-Zusammenfassung**auf **Global Analytics Configuration**.



3. Wählen Sie die Analysefunktionen aus, für die Sie Analysen auf den virtuellen Servern aktivieren möchten.
4. Um Analysen auf den nachfolgenden virtuellen Servern zu aktivieren, aktivieren Sie das Kontrollkästchen **Diese Analyseeinstellungen auf den nachfolgenden lizenzierten virtuellen Servern anwenden** .
5. Klicken Sie auf **Submit**.



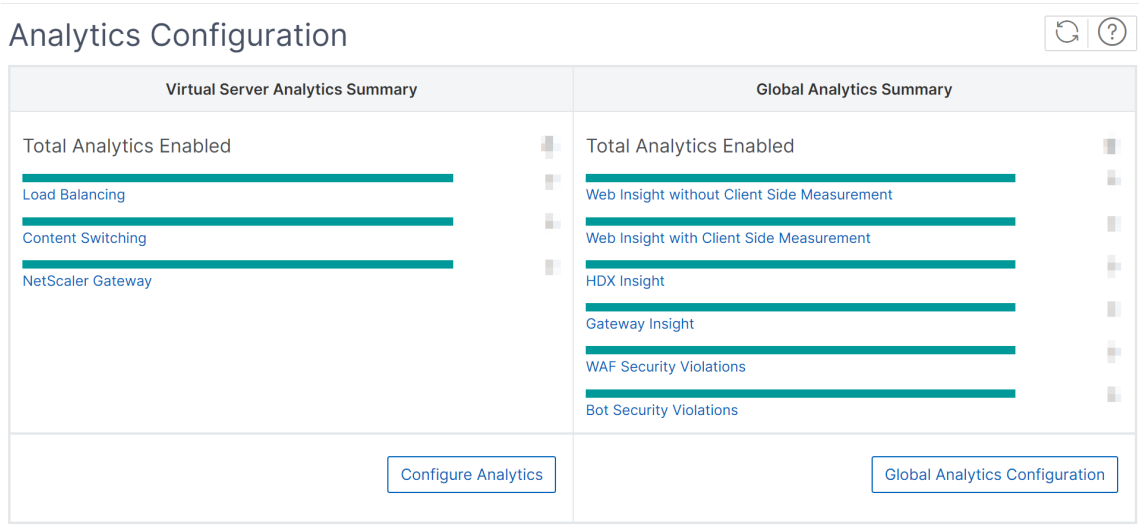
Analytik auf virtuellen Servern mit flexibler Lizenz konfigurieren

February 5, 2024

Voraussetzung für die Aktivierung von Analysen ist, dass die virtuellen Server lizenziert werden müssen. Wenn Sie eine flexible Lizenz verwenden, werden alle vorhandenen virtuellen Server und die nachfolgenden virtuellen Server automatisch lizenziert. Sie können mit der Konfiguration von Analytics fortfahren.

Sie können Analysen auf zwei Arten konfigurieren. Navigieren Sie zu **Einstellungen > Analytics-Konfiguration** , um Folgendes anzuzeigen:

- **Zusammenfassung**der virtuellen Serveranalysen —Ermöglicht die Konfiguration von Analysen auf den vorhandenen virtuellen Servern.
- **Globale Analyseübersicht**—Ermöglicht die Konfiguration von Analysen sowohl auf vorhandenen als auch auf nachfolgenden virtuellen Servern.



Analytik auf den vorhandenen virtuellen Servern konfigurieren

> **Hinweis:**
>
> Stellen Sie sicher, dass die virtuellen Server, für die Sie Analysen aktivieren möchten, den Status **UP** haben .

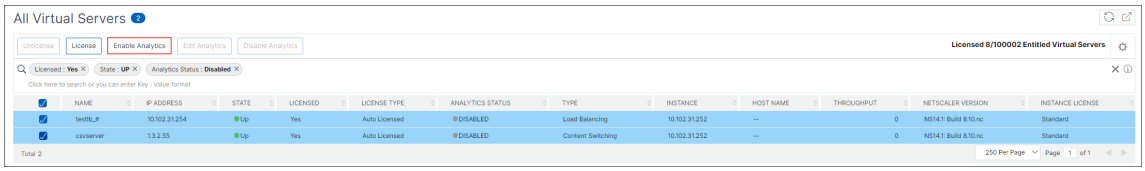
1. Klicken Sie unter **Virtual Server Analytics-Zusammenfassung**auf **Analytics konfigurieren**.

   Die Seite “**Alle virtuellen Server** “wird angezeigt. Sie haben folgende Möglichkeiten:

   - Analytics aktivieren
   - Analytics bearbeiten
   - Analytics deaktivieren

   > **Hinweis:**
   >
   > Die unterstützten virtuellen Server zum Aktivieren von Analysen sind Load Balancing, Content Switching und NetScaler Gateway.

2. Wählen Sie die virtuellen Server aus, und klicken Sie dann auf **Analytics aktivieren**.



> **Hinweis**
>
> Alternativ können Sie Analysen für eine Instanz aktivieren:

```
1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler
```



```
**, und wählen Sie dann den Instanztyp aus. Zum Beispiel
VPX.

1.  Wählen Sie die Instanz aus und wählen Sie in der Liste **
Aktion auswählen** die Option **Analytics konfigurieren**
aus.
1.  Wählen Sie auf der Seite „Analytics auf virtuellen Servern
 konfigurieren“  den virtuellen Server aus und klicken Sie
auf **Analytics aktivieren**.
```

3. Gehen Sie im Fenster **Enable Analytics** wie folgt vor:

   a) Wählen Sie die Einsichtstypen aus.

   b) Wählen Sie **Logstream** als Transportmodus.

   > **Hinweis:**
   >
   > Für NetScaler 12.0 oder früher ist **IPFIX** die Standardoption für den Transportmodus. Für NetScaler 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.
   >
   > Weitere Informationen zu IPFIX und Logstream finden Sie unter Logstream-Übersicht .

   c) Unter **Optionen auf Instanzebene**:

   - **HTTP X-Forwarded-For aktivieren** —Wählen Sie diese Option aus, um die IP-Adresse für die Verbindung zwischen Client und Anwendung über den HTTP-Proxy oder den Load Balancer zu ermitteln.
   - **NetScaler Gateway** —Wählen Sie diese Option aus, um Analysen für NetScaler Gateway anzuzeigen.

   d) Der Ausdruck ist standardmäßig “true”.

   e) Klicken Sie auf **OK**.

   > **Hinweis:**
   >
   > - Für Admin-Partitionen wird nur **Web Insight** unterstützt.
   > - Für virtuelle Server wie Cache-Umleitung , Authentifizierung und GSLB können Sie Analysen nicht aktivieren. Eine Fehlermeldung wird angezeigt.

Nachdem Sie auf **OK** geklickt haben, verarbeitet NetScaler ADM Analysen auf den ausgewählten virtuellen Servern zu aktivieren.

> **Hinweis**
>
> NetScaler ADM verwendet NetScaler SNIP für Logstream und NSIP für IPFIX. Wenn zwischen dem NetScaler ADM-Agenten und der NetScaler-Instance eine Firewall aktiviert ist, stellen Sie sicher, dass Sie den folgenden Port öffnen, damit NetScaler ADM AppFlow-Verkehr erfassen kann:

Transport-Modus	Quell-IP	Typ	Port
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

Analytics bearbeiten

So bearbeiten Sie Analysen auf den virtuellen Servern:

1. Wählen Sie die virtuellen Server aus.

   > **Hinweis:**
   >
   > Alternativ können Sie auch Analysen für eine Instanz bearbeiten:
   >
   > ```
   > 1.  Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler **, und wählen Sie dann den Instanztyp aus. Zum Beispiel VPX.
   > 2
   > 3  1.  Wählen Sie die Instanz aus und klicken Sie auf **Analytics bearbeiten**.
   > ```

2. Klicken Sie auf **Analytics bearbeiten**
3. Bearbeiten Sie die Parameter, die Sie anwenden möchten, im Fenster **Analytics-Konfiguration bearbeiten** .
4. Klicken Sie auf **OK**.

Analytics deaktivieren

So deaktivieren Sie Analysen auf den ausgewählten virtuellen Servern:

1. Wählen Sie die virtuellen Server aus.
2. Klicken Sie auf **Analytics deaktivieren** .

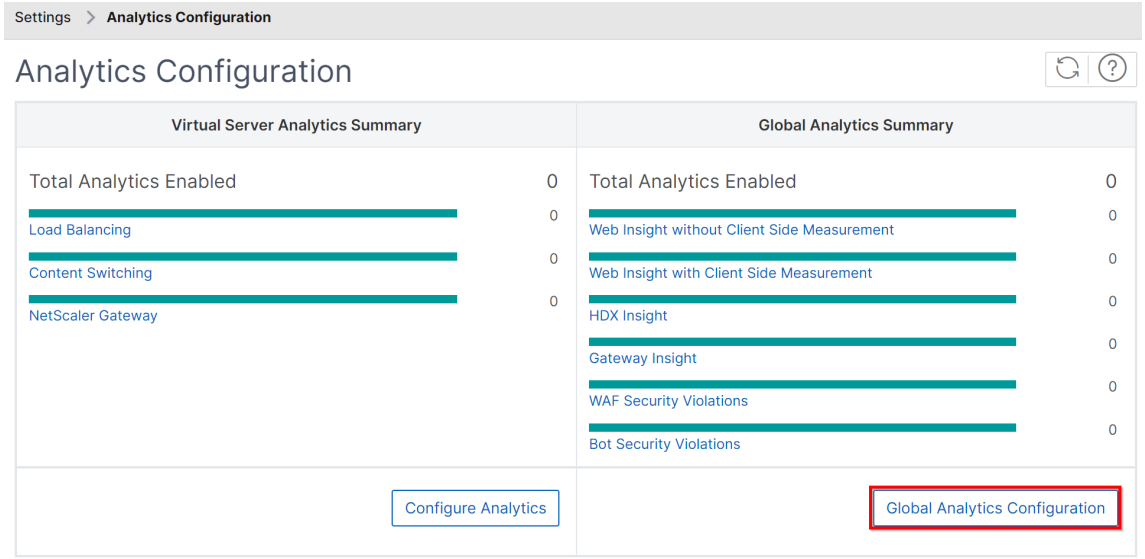
NetScaler ADM deaktiviert die Analysen auf den ausgewählten virtuellen Servern.

In der folgenden Tabelle werden die Features von NetScaler ADM beschrieben, die IPFIX und Logstream als Transportmodus unterstützen:

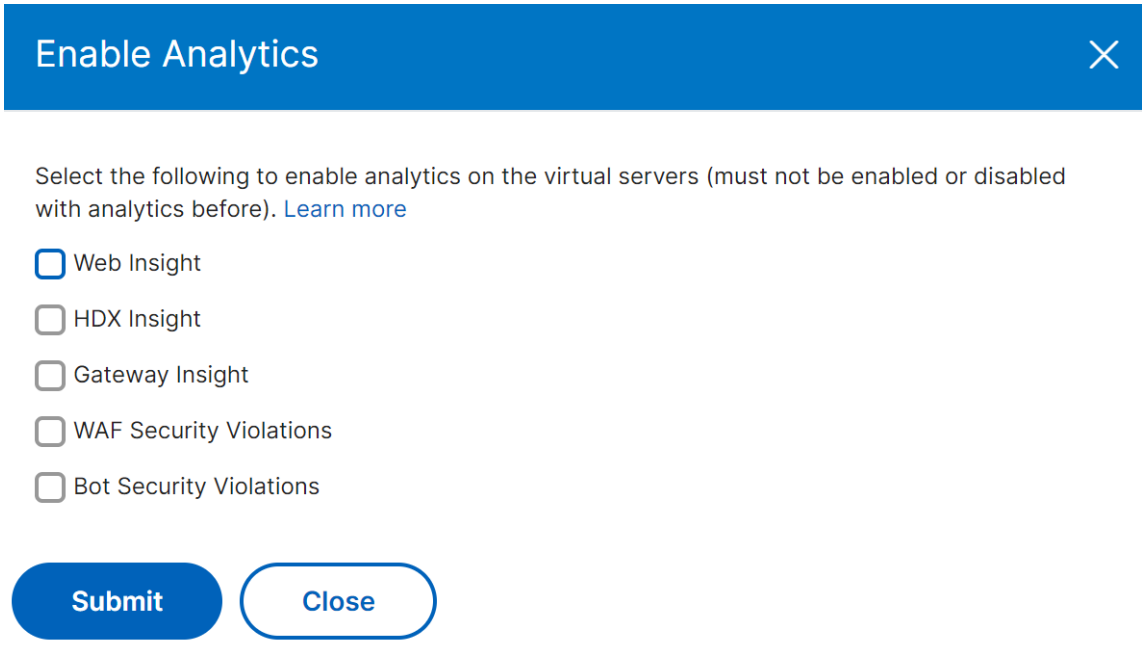
Feature	IPFIX	Logstream
Web Insight	•	•
Sicherheitsverletzungen der WAF	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Nicht unterstützt	•
CR-Einblick	•	•
IP-Reputation	•	•
AppFirewall	•	•
Kundenseitige Messung	•	•
Syslog/Auditlog	•	•

Analytik global konfigurieren

1. Klicken Sie unter **Global Analytics-Zusammenfassung** auf **Global Analytics-Konfiguration** .



2. Wählen Sie die Analysefunktionen aus, für die Sie Analysen auf den virtuellen Servern aktivieren möchten.
3. Klicken Sie auf Submit.



Nach der Konfiguration wird die Analyse sowohl auf vorhandenen als auch auf nachfolgenden virtuellen Servern aktiviert.

Wichtige Hinweise

- Beachten Sie, dass Sie die Global Analytics-Konfiguration zum ersten Mal konfiguriert haben, indem Sie Web Insight , HDX Insight und Gateway Insight ausgewählt haben. Wenn Sie die Analyseeinstellungen später erneut ändern und Gateway Insight abwählen, wirken sich die Änderungen nicht auf die virtuellen Server aus, auf denen bereits Analysen aktiviert sind.
- Bedenken Sie, dass Sie über 10 lizenzierte virtuelle Server verfügen und zwei von ihnen bereits für Analysen mithilfe der Option „ Analytik **konfigurieren** “aktiviert sind. In diesem Szenario werden die Analysen bei der Konfiguration der globalen Analytics-Konfiguration nur auf den verbleibenden acht virtuellen Servern angewendet.
- Bedenken Sie, dass Sie über 10 lizenzierte virtuelle Server verfügen und die Analyse für zwei virtuelle Server manuell deaktiviert haben. In diesem Szenario werden bei der Konfiguration der globalen Analytics-Konfiguration die Analysen nur auf die verbleibenden acht virtuellen Server angewendet. Die virtuellen Server, die manuell mit Analysen deaktiviert wurden, werden übersprungen.

Netzprofil der verwalteten NetScaler-Instanz zuweisen

February 5, 2024

Wenn Sie Analysen für die virtuellen Server in NetScaler ADM aktivieren, werden die AppFlow-Daten vom NetScaler über die NetScaler-Subnetz-IP-Adresse (SNIP) nach NetScaler ADM exportiert. In einigen Szenarien kann das SNIP aufgrund der Firewall im Netzwerk blockiert werden. In solchen Szenarien müssen Sie möglicherweise eine andere IP-Adresse als die SNIP verwenden. Weitere Informationen zum Netzprofil finden Sie unter Verwenden einer angegebenen Quell-IP für die Back-End-Kommunikation.

Sie können einer NetScaler-Instanz über NetScaler ADM ein Netzprofil zuweisen, um AppFlow-Daten von NetScaler nach NetScaler ADM zu exportieren.

Voraussetzungen

Stellen Sie Folgendes sicher:

- Die NetScaler-Instanzversion ist **13.0-48.4** oder höher.
- Das Netzprofil ist in NetScaler-Instanzen konfiguriert.

So weisen Sie ein Netzprofil in NetScaler ADM zu:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** .
2. Wählen Sie die Instanz aus und klicken Sie in der Liste **Select Action** auf **Configure Net Profiles**, um der Instanz ein Netzprofil zuzuweisen.
3. Wählen Sie ein Netzprofil aus der Liste aus und klicken Sie auf **Anwenden**.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie die Analyse für alle virtuellen Server deaktivieren, bevor Sie der Instanz ein Netzprofil zuweisen.

NTP-Server konfigurieren

February 5, 2024

Sie können einen NTP-Server (Network Time Protocol) in NetScaler ADM so konfigurieren, dass er seine Uhr mit dem NTP-Server synchronisiert. Durch die Konfiguration eines NTP-Servers wird

sichergestellt, dass die NetScaler ADM Uhr dieselben Datums- und Uhrzeiteinstellungen wie die anderen Server im Netzwerk aufweist.

So konfigurieren Sie einen NTP-Server auf NetScalerADM:

1. Navigieren Sie in der ADM-GUI zu **Einstellungen > Verwaltung**. Klicken Sie auf der Seite **Systemadministration** unter **Netzwerkkonfigurationen**auf **NTP-Server**. Klicken Sie dann auf **Hinzufügen**.
2. Geben Sie auf der Seite **NTP-Server erstellen** die folgenden Details ein:
    - **Servername/IP-Adresse** —Geben Sie den Domainnamen oder die IP-Adresse des NTP-Servers ein. Der Name oder die IP-Adresse können nicht geändert werden, nachdem Sie den NTP-Server hinzugefügt haben.
    - **Minimales Abfrageintervall** —Geben Sie den Mindestwert für das Intervall zwischen übertragenen NTP-Nachrichten in Sekunden als Trennschärfe von 2. Wenn das Mindestabfrageintervall beispielsweise 64 Sekunden betragen soll, was als 2^6 ausgedrückt werden kann, geben Sie 6 ein
    - **Maximales Abfrageintervall** —Geben Sie den Maximalwert für das Intervall zwischen übertragenen NTP-Nachrichten in Sekunden als Trennschärfe von 2. Wenn Sie beispielsweise möchten, dass das maximale Abfrageintervall 256 Sekunden beträgt, was als 2^8 ausgedrückt werden kann, geben Sie 8 ein.
    - **Schlüssel-ID**—Geben Sie die Schlüssel-ID ein, die für die symmetrische Schlüsselauthentifizierung mit dem NTP-Server verwendet werden kann. Fügen Sie keine Schlüssel-ID hinzu, wenn Sie Autokey auswählen.
    - **Autokey** —Wählen Sie **Autokey** aus, wenn Sie die Authentifizierung mit öffentlichen Schlüsseln für den NTP-Server verwenden möchten. Wählen Sie nicht aus, ob Sie eine Schlüssel-ID hinzufügen möchten.
    - **Bevorzugt** —Wählen Sie diese Option, wenn Sie diesen NTP-Server als bevorzugten Server für die Uhrsynchronisierung angeben möchten. Dies gilt nur, wenn mehr als ein Server konfiguriert ist.
3. Klicken Sie auf **Erstellen**.

So aktivieren Sie die NTP-Synchronisierung auf NetScaler ADM:

1. Navigieren Sie zu **System** > **NTP-Server**.
2. Klicken Sie auf **NTP-Synchronisierung** und **aktivieren Sie das Kontrollkästchen NTP-Synchronisierung** aktivieren.
3. Klicken Sie auf **OK**.

Systemeinstellungen konfigurieren

February 5, 2024

Bevor Sie NetScaler ADM zur Verwaltung und Überwachung Ihrer Instanzen und Anwendungen verwenden, wird empfohlen, einige Systemeinstellungen zu konfigurieren, um eine optimale Leistung Ihres NetScaler ADM-Servers zu gewährleisten.

Konfigurieren von Systemalarmen

Konfigurieren Sie Systemalarme, um sicherzustellen, dass Sie kritische oder größere Systemprobleme kennen. Sie möchten z. B. benachrichtigt werden, wenn die CPU-Auslastung hoch ist oder wenn mehrere Anmeldefehler auf dem Server auftreten. Für einige Alarmkategorien, wie CPUUsageHigh oder MemoryUsageHigh, können Sie Schwellenwerte festlegen und den Schweregrad (z. B. Critical oder Major) für jede Alarmkategorie definieren. Für einige Kategorien, wie inventoryFailed oder loginFailure, können Sie nur den Schweregrad definieren. Wenn der Schwellenwert für eine Alarmkategorie (z. B. MemoryUsageHigh) überschritten wird oder wenn ein Ereignis auftritt, das der Alarmkategorie entspricht (z. B. loginFailure), wird eine Meldung im System aufgezeichnet, und Sie können die Meldung als Syslog-Nachricht anzeigen.

So konfigurieren Sie Systemalarme:

1. Navigieren Sie zu **Einstellungen> SNMP**, und klicken Sie dann in der oberen rechten Ecke auf die Registerkarte **Alarme** .
2. Wählen Sie den Alarm aus, den Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie auf der Seite **Alarm konfigurieren** den Schweregrad des Alarms aus, und legen Sie den Schwellenwert fest.
4. Um die Alarme anzuzeigen, die den Schwellenwert überschritten haben oder für die ein Ereignis eingetreten ist, navigieren Sie zu **Einstellungen > Überwachung** und klicken Sie auf **Syslog-Meldungen**.

Konfigurieren von Systembenachrichtigungen

Sie können Benachrichtigungen an ausgewählte Benutzergruppen für verschiedene systembezogene Funktionen senden. Sie können einen Benachrichtigungsserver in NetScaler ADM einrichten und E-Mail- und SMS-Gateway server (Short Message Service) so konfigurieren, dass E-Mail- und Textbenachrichtigungen an Benutzer gesendet werden. Durch das Festlegen von Benachrichtigungen wird sichergestellt, dass Sie über Aktivitäten auf Systemebene wie Benutzeranmeldung oder Systemneustart informiert werden.

So konfigurieren Sie Systembenachrichtigungen:

1. Navigieren Sie zu **Einstellungen > Administration**. Klicken Sie auf der Seite **Systemadministration** unter **Ereignisbenachrichtigungen**auf **Ereignisbenachrichtigung konfigurieren und -digest > Ereignisbenachrichtigung**.
2. Wählen Sie auf der Seite **Einstellungen für Systembenachrichtigungen konfigurieren** die Kategorie oder Kategorie der Ereignisse aus, die von NetScaler ADM generiert wurden.
3. Konfigurieren Sie dann entweder den E-Mail-Server oder den SMS-Server, um Benachrichtigungen per E-Mail oder SMS oder beides zu erhalten.

Einstellungen für Systemausfall konfigurieren

Um die Menge der Berichtsdaten zu begrenzen, die in der Datenbank Ihres NetScaler ADM-Servers gespeichert werden, können Sie das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle aufbewahren soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00.00 Uhr) bereinigt.

So konfigurieren Sie die Einstellung für Systemausfall:

1. Navigieren Sie zu **Einstellungen> Systemadministration**. Klicken Sie unter **Datenbereinigung** auf **System- und Instanzdatenbereinigung**.
2. Geben Sie auf der **Systemseite** die Anzahl der Tage an, für die Daten aufbewahrt werden sollen, und klicken Sie auf **Speichern**.

Konfigurieren der Einstellungen für die Instanz Syslog-Ausschneiden

Um die Menge der in der Datenbank gespeicherten Syslog-Daten zu begrenzen, können Sie das Intervall angeben, in dem Syslog-Daten gelöscht werden sollen. Sie können die Anzahl der Tage angeben, nach denen die generischen Syslog-Daten aus NetScaler ADM gelöscht werden.

So konfigurieren Sie die Einstellungen zum Löschen von Instanzsyslog-Einstellungen:

1. Navigieren Sie zu **Einstellungen > Verwaltung > Datenbereinigung**.
2. Klicken Sie auf **System- und Instanzdaten aufschneiden > Instanzsyslog**.
3. Geben **Sie auf der Seite „Syslog-Prune-Einstellungen für die Instanz konfigurieren**“im Feld Generische **Syslog-Daten speichern** die Anzahl der Tage zwischen 1 und 180 an.
4. Klicken Sie auf **Speichern**.

Einstellungen für das Ausschneiden von Instanzereignissen konfigurieren

Um die Anzahl der Ereignismeldungsdaten zu begrenzen, die in der Datenbank Ihres NetScaler ADM-Servers gespeichert werden, können Sie das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle aufbewahren soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00:00 Uhr) beschnitten.

So konfigurieren Sie die Einstellungen für das Ausschneiden von Instanzereignissen:

1. Navigieren Sie zu **Einstellungen > Administration**.
2. Klicken Sie auf der Seite **Systemadministration** unter **Datenbereinigung** auf **System- und Instanzdatenbereinigung**.
3. Klicken Sie auf der Seite **Datenbereinigung** auf **Instanzereignisse**.
4. **Geben**Sie im Feld Zu speichernde Daten (Tage)**das Zeitintervall in Tagen ein, für das Sie Daten auf dem NetScaler ADM-Server speichern möchten, und klicken Sie auf Speichern.**

Einstellungen für das Systembackup konfigurieren

NetScaler ADM erstellt ein Backup des Systems automatisch jeden Tag um 00:30 Uhr. Standardmäßig werden drei Backupdateien gespeichert. Möglicherweise möchten Sie eine größere Anzahl von Backups des Systems beibehalten. Sie können die Sicherungsdatei auch verschlüsseln. Sie können das Backup auch auf einem externen Server speichern.

So konfigurieren Sie die Einstellungen für das Systembackup:

1. Navigieren Sie zu **Einstellungen > Administration**.
2. Klicken Sie unter **Backup**auf **System- und Instanz-Backup konfigurieren**.
3. Klicken Sie auf **System** und geben Sie auf der Seite **„System-Backup-Einstellungen konfigurieren** “die erforderlichen Werte an.

Konfigurieren der Einstellungen für das Instanzbackup

Wenn Sie den aktuellen Status einer NetScaler-Instance sichern, können Sie die Sicherungsdateien verwenden, um die Stabilität wiederherzustellen, falls die Instanz instabil wird. Dies ist besonders wichtig, bevor Sie ein Upgrade durchführen. Standardmäßig wird alle 12 Stunden ein Backup erstellt und drei Sicherungsdateien werden im System aufbewahrt.

So konfigurieren Sie Instanzbackupeinstellungen:

1. Navigieren Sie zu **Einstellungen > Administration**.

2. Klicken Sie unter **Backup**auf **System- und Instanz-Backup konfigurieren**.
3. **Klicken Sie unter**Configure Instance Backup Settings**auf Instance und geben Sie die erforderlichen Werte an.**

ADM-Features aktivieren oder deaktivieren

Als Administrator können Sie die folgenden Funktionen auf der Seite **Einstellungen > Verwaltung > Konfigurierbare Funktionen** aktivieren oder deaktivieren:

- **Agentfailover** : Das Agent-Failover kann auf einem Standort mit zwei oder mehr aktiven Agents auftreten. Wenn ein Agent in der Site inaktiv wird (DOWN Status), verteilt der NetScaler ADM Dienst die ADC-Instanzen des inaktiven Agents mit anderen aktiven Agenten neu. Weitere Informationen finden Sie unter Konfigurieren von On-Prem-Agenten für die Multisite-Bereitstellung.
- **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 NetScaler ADM konfigurierte Netzwerkfunktionsentitäten automatisch alle 60 Minuten ab. Weitere Informationen finden Sie unter Überblick über Statusabruf.
- **Instanzbackup**: Erstellen Sie ein Backup des aktuellen Status einer NetScaler-Instanz und verwenden Sie später die Backupdateien, um die ADC-Instanz in demselben Zustand wiederherzustellen. Weitere Informationen finden Sie unter Backup und Wiederherstellen von NetScaler-Instanzen.
- **Überwachung der Instanzkonfiguration** : Überwachen Sie Konfigurationsänderungen in verwalteten NetScaler-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 NetScaler-Instanz dar. In NetScaler ADM empfangene Ereignisse werden auf der Seite „ **Ereignisse** “(**Infrastruktur > Ereignisse**) angezeigt, und alle aktiven Ereignisse werden auf der Seite „Ereignismeldungen“angezeigt (**Infrastruktur > Ereignisse > Ereignismeldungen**). 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 Netzwerkberichte.
- **Instanz-SSL-Zertifikate** : NetScaler ADM bietet eine zentrale Ansicht der SSL-Zertifikate, die auf allen verwalteten NetScaler-Instanzen installiert sind. Weitere Informationen finden Sie unter SSL-Dashboard.

- **Instanzsyslog** : Sie können die Syslog-Ereignisse überwachen, die auf Ihren NetScaler-Instanzen generiert werden, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Nachrichten an NetScaler ADM umgeleitet werden.

Führen Sie die folgenden Schritte aus, um eine Funktion zu aktivieren:

1. Wählen Sie die Funktion aus der Liste aus, die Sie aktivieren möchten.
2. Klicken Sie auf **Aktivieren**.

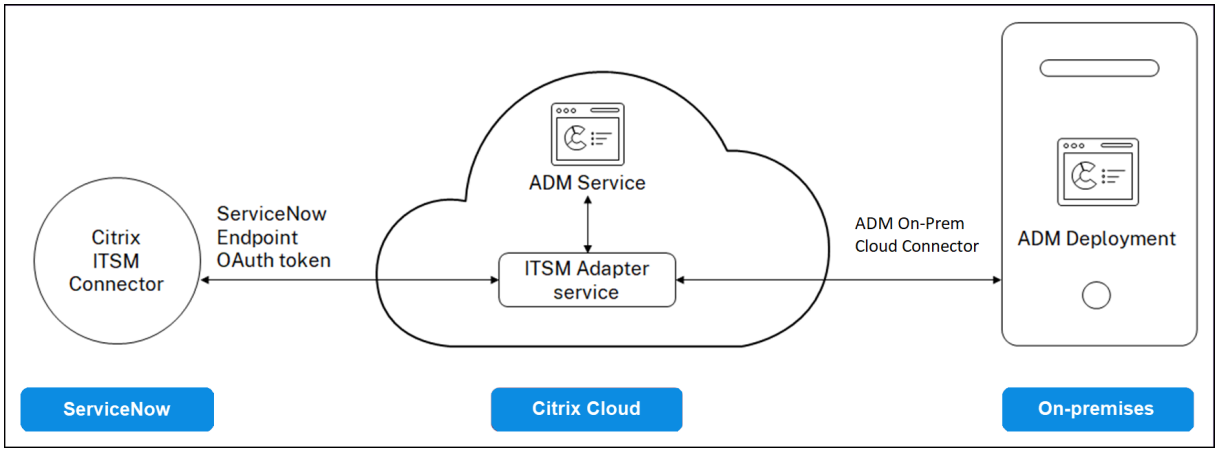
> **Wichtig**
>
> Wenn eine Funktion deaktiviert ist, kann der Benutzer die mit dieser Funktion verbundenen Vorgänge nicht ausführen.

Integration von NetScaler ADM in die ServiceNow-Instanz

February 5, 2024

Wenn Sie ServiceNow-Benachrichtigungen für NetScaler- und ADM-Ereignisse aktivieren möchten, integrieren Sie NetScaler ADM in die ServiceNow-Instanz. Diese Integration verwendet den Citrix ITSM-Connector für die Kommunikation zwischen NetScaler ADM und der ServiceNow-Instanz.

Die ServiceNow-Integration mit ADM verwendet den ITSM-Adapter-Dienst für die tokenbasierte Authentifizierung. Zu diesem Zweck wird eine Endpunktinstanz in ServiceNow erstellt. Weitere Informationen finden Sie unter Funktionsweise des ITSM-Adapters.



Um Ihre on-premises ADM-Bereitstellung mit einem ITSM-Adapter zu verbinden, stellen Sie sicher, dass Sie ADM On-Prem Cloud Connector konfiguriert haben. Weitere Informationen finden Sie unter ADM On-Prem Cloud Connector.

Stellen Sie für die ServiceNow-Integration mit ADM Build 14.1 4.x oder früher sicher, dass Sie die Kundenidentität konfigurieren. Weitere Informationen finden Sie unter Konfigurieren der Kundenidentität.

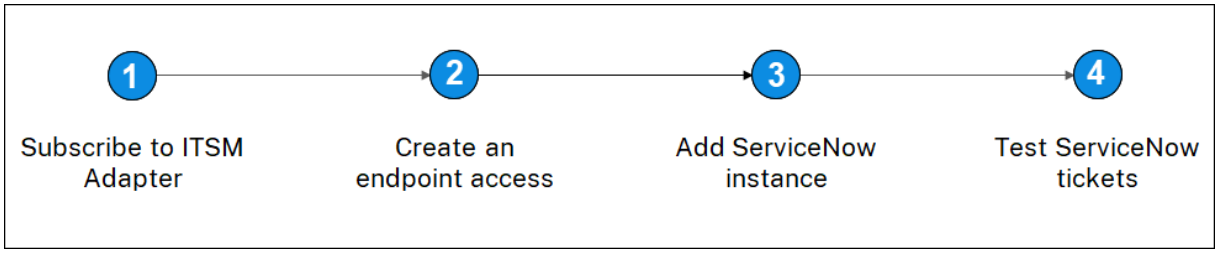
Voraussetzungen

Bevor Sie ADM mit ServiceNow integrieren, stellen Sie Folgendes sicher:

1. Melden Sie sich für Citrix Cloudan. Stellen Sie sicher, dass Sie Zugriff auf die Verwaltung von Citrix Cloud-Administratoren haben. Weitere Informationen finden Sie unter Verwalten von Citrix Cloud-Administratoren.

Wie integriert man ADM mit ServiceNow?

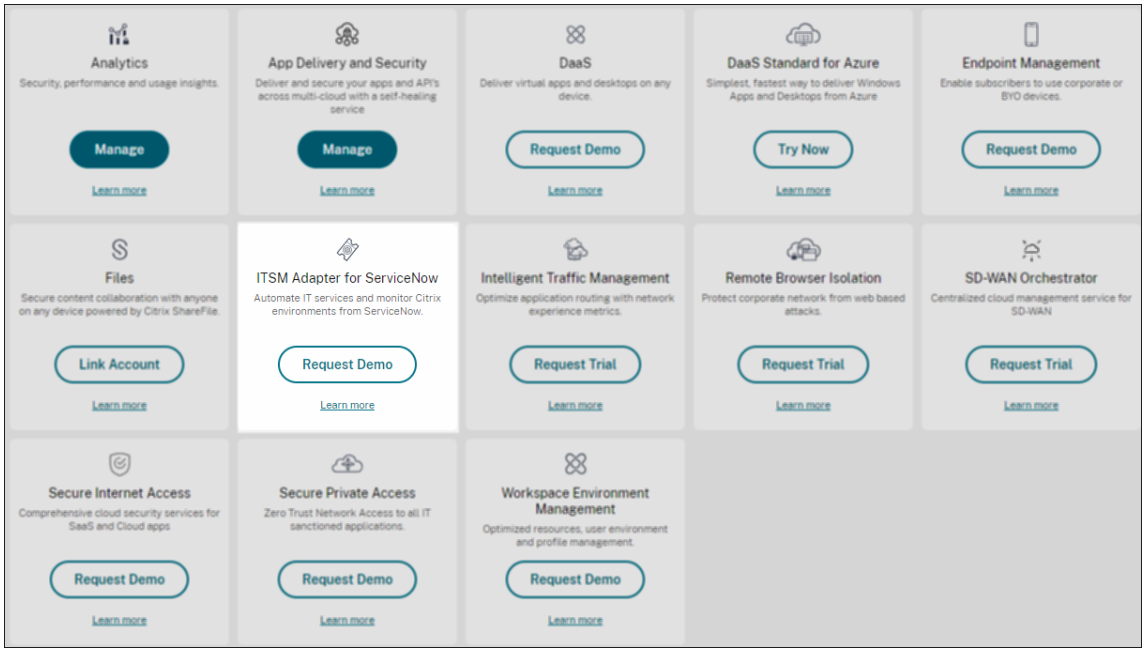
Führen Sie die folgenden Schritte aus, um NetScaler ADM mithilfe des ITSM-Connectors in ServiceNow zu integrieren:



1. Abonnieren Sie den ITSM-Adapterdienst in Citrix Cloud.
2. Erstellen Sie einen Endpunktzugriff in der ServiceNow-Instanz.
3. Fügen Sie eine ServiceNow-Instanzhinzu.
4. Testen Sie die automatische Generierung von ServiceNow-Tickets in ADM.

Schritt 1 —Abonnieren des ITSM-Adapterdienstes in Citrix Cloud

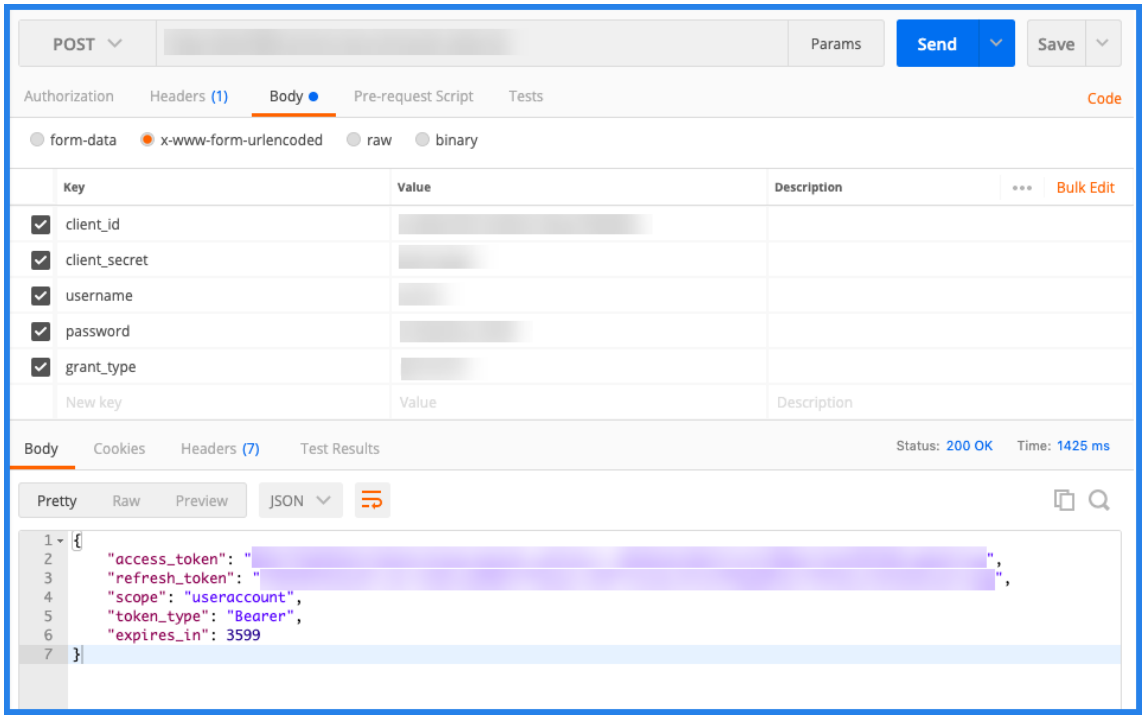
1. Klicken Sie auf der Kachel **ITSM-Adapter** auf **Testversion anfordern**.



2. Navigieren Sie zu **Identitätszugriff und Verwaltung** > **API-Zugriff**, und notieren Sie sich die **Client-ID** und **Client-Geheiminformationen**.

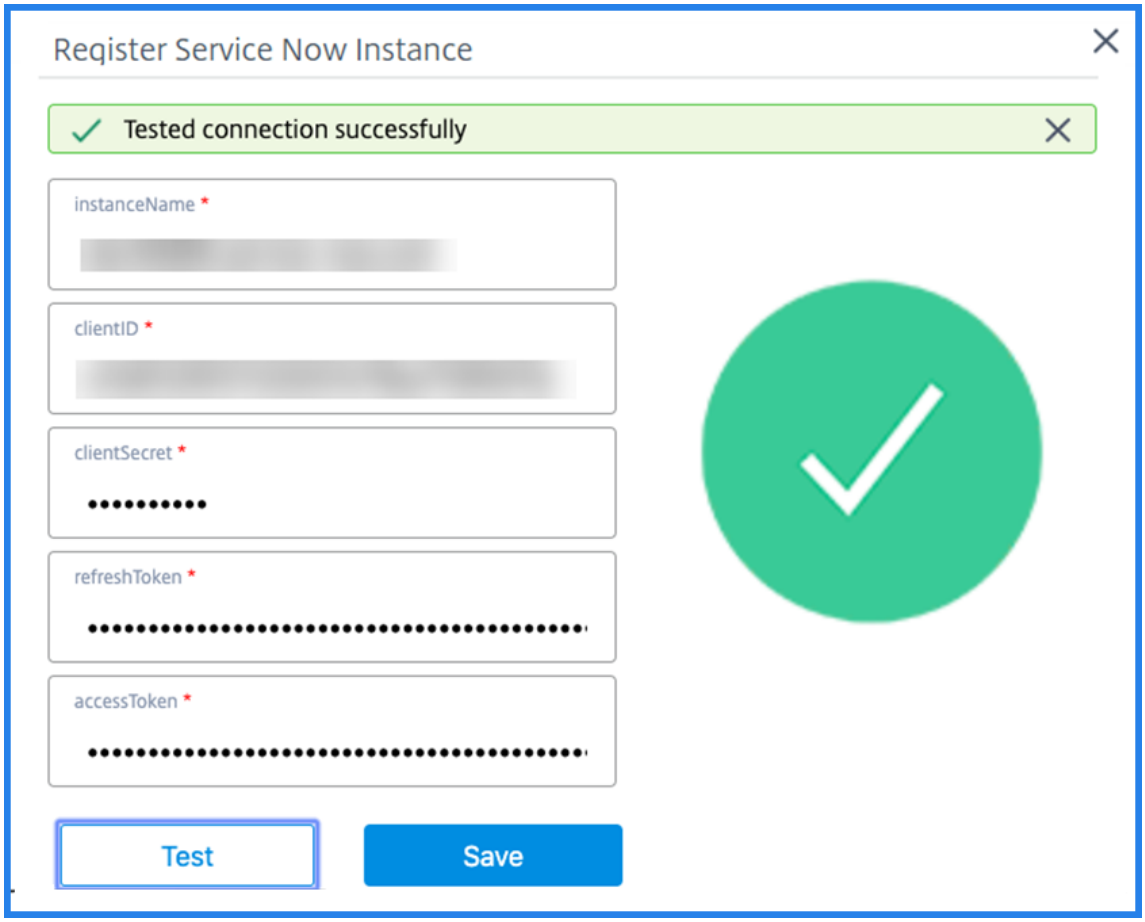
Schritt 2 —Erstellen eines Endpunktzugriffs in der ServiceNow-Instanz

1. Melden Sie sich mit Administratoranmeldeinformationen bei Ihrer ServiceNow-Instanz an.
2. Gehen Sie zum ServiceNow Store. Laden Sie den **Citrix ITSM-Connector**herunter und installieren Sie ihn.
3. Wählen Sie im Bereich **Citrix ITSM Connector** die Option **Home** aus und klicken Sie dann auf **Authentifizieren**. Geben Sie die Client-ID und das Secret ein, die Sie von Citrix Cloud notiert haben.
4. Testen Sie die Verbindung.
5. Speichern Sie die Konfiguration. Eine Bestätigung von ServiceNow wird angezeigt, die darauf hinweist, dass die Verbindung aktiv ist.
6. Erstellen Sie einen Endpunkt für den Zugriff auf eine ServiceNow-Instanz. Weitere Informationen finden Sie unter Erstellen eines Endpunkts für Clients für den Zugriff auf die Instanz.
7. Rufen Sie die Zugriffs- und Aktualisierungstoken mit der Client-ID und dem Clientgeheimnis ab. Siehe OAuth-Token.



Schritt 3 —ServiceNow-Instanz hinzufügen

1. Wählen Sie auf der Registerkarte **Verwalten** die Option ServiceNow-Instanz hinzufügen aus.
2. Geben Sie den **Instanznamen**, die **Client-ID**, das **Client-Geheimnis, dasAktualisierungstoken**und das**Zugriffstoken**an.
3. Klicken Sie auf **Test**.



Die ServiceNow-Instanz ist jetzt mit dem ITSM Adapter Service verbunden.

4. Nachdem Sie die Verbindung erfolgreich getestet haben, klicken **Sie auf Speichern**, um eine ServiceNow-Instanz hinzuzufügen.

Schritt 4 —Testen der automatischen Generierung von ServiceNow-Tickets in ADM

1. Melden Sie sich bei NetScaler ADM an.
2. Navigieren Sie zu **Konto > Benachrichtigungen** und wählen Sie **ServiceNow**aus.
3. Wählen Sie das ServiceNow-Profil aus der Liste aus.
4. Klicken Sie auf **Test**, um automatisch ein ServiceNow-Ticket zu generieren und die Konfiguration zu überprüfen.

   Wenn Sie ServiceNow-Tickets in der NetScaler ADM GUI anzeigen möchten, wählen Sie **ServiceNow Tickets**aus.

Stellen Sie ServiceNow-Benachrichtigungen in ADM ein

Nachdem die ServiceNow-Instanz auf dem ITSM-Adapter registriert wurde, können Sie ServiceNow-Benachrichtigungen für die folgenden Ereignisse in der NetScaler ADM-GUI einrichten:

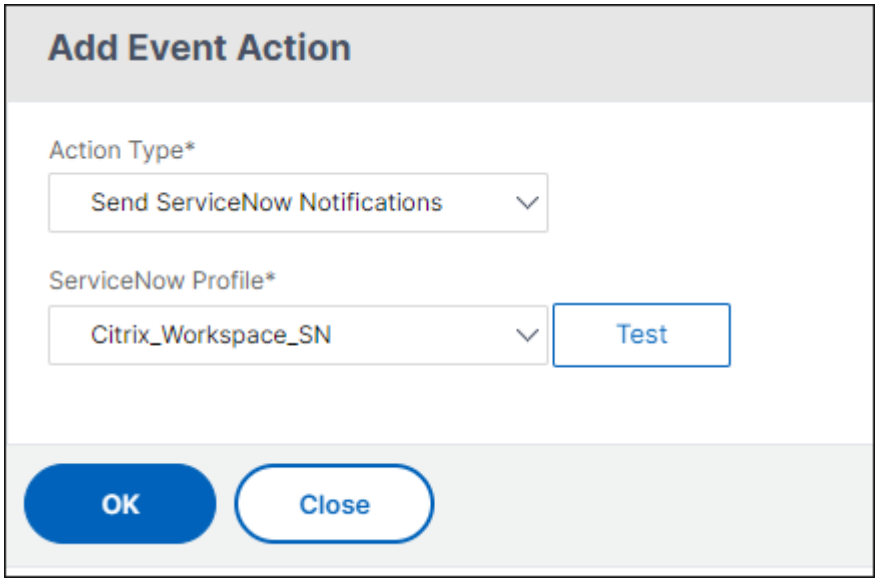
> **Wichtig**
>
> Diese Funktion wird von ServiceNow Cloud unterstützt.

- **NetScaler-Ereignisse**: NetScaler ADM kann die ServiceNow-Incidents für den ausgewählten Satz von NetScaler-Ereignissen aus ausgewählten verwalteten NetScaler-Instanzen generieren.

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

  Erstellen Sie eine Ereignisregel im ADM, indem Sie zu **Infrastruktur > Ereignisse > Regeln**navigieren. Weitere Informationen finden Sie unter ServiceNow-Benachrichtigungen senden.

- **Anwendungsanalyse**: NetScaler ADM kann ServiceNow-Vorfälle für die Anwendungen generieren, die den angegebenen Schwellenwert überschreiten.



  In diesem Beispiel wird ein ServiceNow-Vorfall generiert, wenn der App-Score von Anwendungen unter 90 fällt.

- **Das SSL-Zertifikat und die ADM-Lizenzereignisse**: NetScaler 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 eines SSL-Zertifikats finden Sie unter Ablauf des SSL-Zertifikats.

Informationen zum Senden von ServiceNow-Benachrichtigungen für den Ablauf einer ADM-Lizenz finden Sie unter Ablauf der NetScaler ADM-Lizenz.

Exportberichte exportieren oder planen

February 5, 2024

In NetScaler ADM können Sie einen umfassenden Bericht für das ausgewählte NetScaler ADM Feature exportieren. Dieser Bericht bietet Ihnen einen Überblick über die Zuordnung zwischen den Instanzen, Partitionen und entsprechenden Details.

NetScaler ADM zeigt funktionsspezifische geplante Exportberichte unter einzelnen ADM-Features an, die Sie anzeigen, bearbeiten oder löschen können. Um beispielsweise die Exportberichte von NetScaler-Instanzen anzuzeigen, navigieren Sie zu **Netzwerk > Instanzen > NetScaler** und klicken Sie auf das Exportsymbol. Sie können diese Berichte im PDF-, JPEG-, PNG- und CSV-Dateiformat exportieren.

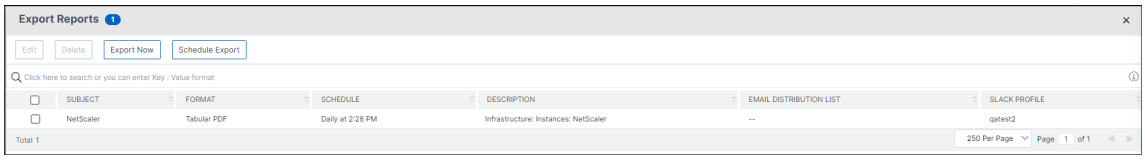
In **Berichte exportieren**können Sie die folgenden Aktionen ausführen:

- Exportieren eines Berichts auf einen lokalen Computer
- Exportberichte 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**.

Exportbericht planen

Um den Exportbericht in regelmäßigen Intervallen zu planen, geben Sie das Wiederholungsintervall an. NetScaler ADM sendet den exportierten Bericht an das konfigurierte E-Mail- oder Slack-Profil.

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 ausgewählten Feature-Namen 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 welcher Uhrzeit Sie den Bericht exportieren möchten.
    - **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** —Aktiviere das Kontrollkästchen und wähle 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

Gehen Sie wie folgt vor, 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

February 5, 2024

Jede NetScaler ADM-Version bietet neue und aktualisierte Funktionen mit erweiterter Funktionalität. Citrix empfiehlt, NetScaler ADM auf die neueste Version zu aktualisieren, um die neuen Funktionen und Fehlerbehebungen in Anspruch zu nehmen. Eine umfassende Liste von Verbesserungen, bekannten Problemen und Bugfixes ist in den Versionshinweisen enthalten, die jeder Versionsankündigung beiliegen. Es ist auch wichtig, den Lizenzierungsrahmen und die Arten von Lizenzen zu verstehen, die verwendet werden können, bevor Sie mit dem Upgrade beginnen. Informationen zur NetScaler ADM-Lizenzierung finden Sie unter Lizenzierung.

Die Informationen zum Upgrade-Pfad sind auch im Citrix Upgrade Guideverfügbar.

Upgradevorbereitung

Laden Sie das Upgrade-Paket von der NetScaler ADM Downloads-Seite herunter und folgen Sie den Anweisungen in diesem Artikel, um Ihr System auf den neuesten 14.1-Build zu aktualisieren. Nach Beginn des Upgradevorgangs wird ADM neu gestartet, und die vorhandenen Verbindungen werden beendet und wieder verbunden, wenn das Upgrade abgeschlossen ist. Die vorhandene Konfiguration wird beibehalten, aber NetScaler ADM verarbeitet keine Daten, bis das Upgrade abgeschlossen ist.

> **Wichtig!**
>
> Die NetScaler ADM-Version und der Build sollten **gleich oder höher** als Ihre NetScaler-Version und Ihr Build sein. Wenn Sie beispielsweise NetScaler ADM 12.1 Build 50.39 installiert haben, stellen Sie sicher, dass Sie NetScaler 12.1 Build 50.28/50.31 oder früher installiert haben.

Punkte, die vor dem Upgrade auf 14.1 zu beachtensind:

- Wenn Sie ein Upgrade von Version 11.1 oder Version 12.0 56.x und früheren Builds durchführen, führen Sie die folgenden Schritte aus:

1. Upgrade von der bestehenden Version auf 12.0 Build 57,24.
2. Führen Sie ein Upgrade auf den neuesten Build der Version 12.1 durch.
3. Aktualisieren Sie auf Version 13.1.
4. Aktualisieren Sie auf Version 14.1.

- Wenn Sie ein Upgrade von 12.0 Build 57.24 und höher durchführen, aktualisieren Sie zuerst auf 12.1, dann auf 13.1 und dann auf 14.1.
- Wenn Sie ein Upgrade von 12.1 durchführen, müssen Sie zuerst auf 13.0 64.xx und dann direkt auf 14.1 aktualisieren
- Wenn Sie ein Upgrade von Versionen vor 13.0 64.xx durchführen, sollten Sie für eine bessere Benutzererfahrung zuerst auf 13.0 64.xx und dann auf 14.1 aktualisieren.
- Nach dem erfolgreichen Upgrade auf 14.1 und der Anmeldung an der GUI wird empfohlen, das Kennwort zu ändern, wenn Sie das Standardkennwort verwenden.

Wichtige Punkte, die Sie vor dem Upgrade auf 14.1 xx.xx und höher beachten sollten

Wenn Sie die ADM-Software auf Version 14.1 xx.xx aktualisieren, wird Ihre ADM-Datenbank ebenfalls migriert. Diese Datenmigration findet statt, weil ADM jetzt PostgreSQL Version 10.11 verwendet.

> **Hinweis**
>
> Das Herunterstufen der ADM-Software wird nicht unterstützt. Versuchen Sie nicht, ein Downgrade durchzuführen.

Empfohlene Vorsichtsmaßnahmen:

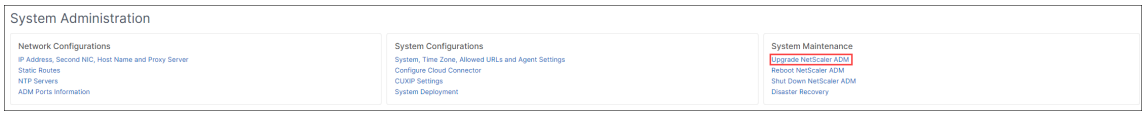
- Erstellen Sie für jedes Upgrade einen Snapshot des NetScaler ADM-Servers, wenn Sie auf 14.1 xx.xx und höher aktualisieren.
- Sichern Sie den NetScaler ADM -Server, bevor Sie das Upgrade durchführen.
- Nach dem Upgrade müssen Sie möglicherweise Verbindungen zwischen dem NetScaler ADM-Server und den verwalteten Instanzen wiederherstellen. Eine Bestätigungsaufforderung warnt Sie, dass Verbindungen fehlschlagen können, wenn Sie fortfahren.
- Wenn Sie auf eine Version zwischen 13.1.9.x und 13.1.30.x aktualisieren, setzt NetScaler ADM das vorhandene StyleBooks-Konfigurationspaket auf die frühere Version zurück.

  Um dieses Problem zu vermeiden, führen Sie ein Upgrade auf 13.1.33.50 Build durch.
- Nehmen Sie bei NetScaler ADM-Servern im Hochverfügbarkeits-Setup beim Upgrade keine Konfigurationsänderungen auf einem der Knoten vor.

> **Warnung**
>
> Aktualisieren Sie den Browser erst, wenn der Upgradevorgang erfolgreich abgeschlossen wurde. Überprüfen Sie die GUI auf die ungefähre Zeit für den Abschluss des Upgrades.

Aktualisieren Sie einen einzelnen NetScaler ADM Server auf 14.1 4.x

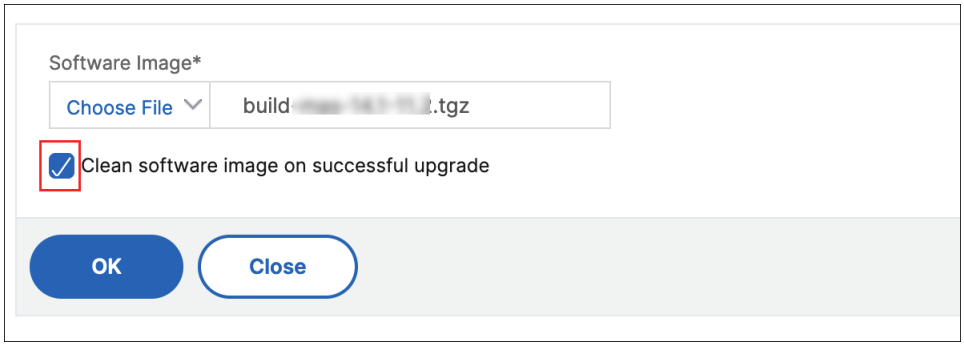
1. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler ADM an.
2. Navigieren Sie zu **Einstellungen** > **Administration** . Klicken Sie unter **Systemwartung** auf **NetScaler ADM aktualisieren**.



3. Aktivieren Sie auf der Seite **NetScaler ADM aktualisieren** das Kontrollkästchen **Software-Image bei erfolgreichem Upgrade bereinigen, um die Image-Dateien nach dem Upgrade** zu löschen. Wenn Sie diese Option auswählen, werden die NetScaler ADM Imagedateien beim Upgrade automatisch entfernt.

> **Hinweis**
>
> Diese Option ist standardmäßig ausgewählt. Wenn Sie dieses Kontrollkästchen nicht aktivieren, bevor Sie den Upgrade-Vorgang starten, müssen Sie die Images manuell löschen.

4. Sie können dann eine neue Image-Datei hochladen, indem Sie entweder **Lokal** (Ihr lokaler Computer) oder **Appliance**auswählen. Die Builddatei muss auf der virtuellen NetScaler ADM Appliance vorhanden sein.



5. Klicken Sie auf **OK**.
   Das Dialogfeld Bestätigen wird angezeigt. Klicken Sie auf **Ja**.

   Der Upgrade-Prozess wird gestartet.

Nachdem Ihre Konfiguration migriert wurde, können Sie sich bei der ADM-GUI anmelden. Bei der Anmeldung beginnen die historischen Daten im Hintergrund zu migrieren, während Sie weiterhin an ADM arbeiten können.

Während der Migration historischer Daten stehen einige der alten Daten möglicherweise nicht zur Verfügung. Die Zeit für die Migration Ihrer Datenbank hängt von der Größe der Daten und der Anzahl der Tabellen ab.

Sie können die Datenbankmigration mit der ADM-GUI überwachen. Klicken Sie auf **Upgrade-Fortschritt anzeigen** und der **Status der Datenbankmigration** wird angezeigt.

Aktualisieren Sie ein Hochverfügbarkeitspaar auf Version 14.1

Für NetScaler ADM -Server in einem Hochverfügbarkeitsmodus können Sie ein Upgrade durchführen, indem Sie entweder auf den aktiven Knoten oder auf die schwebende IP-Adresse zugreifen. Beide NetScaler ADM -Server werden automatisch auf den neuesten Build aktualisiert, sobald Sie den Upgradevorgang auf einem der Server initiieren.

Upgrade der Bereitstellung von NetScaler ADM Disaster Recovery

> **Hinweis:**
>
> Stellen Sie sicher, dass das Kennwort sowohl für das HA-Paar als auch für den Disaster Recovery-Knoten identisch ist.

Das Upgrade der NetScaler ADM Disaster Recovery-Bereitstellung erfolgt in zwei Schritten:

- Aktualisieren Sie die NetScaler ADM-Knoten, die im Hochverfügbarkeitsmodus am primären Standort konfiguriert sind. Später müssen Sie den Notfallwiederherstellungsknoten aktualisieren.
- Stellen Sie sicher, dass Sie die NetScaler ADM-Server, die mit hoher Verfügbarkeit bereitgestellt werden, aktualisiert haben, bevor Sie den Disaster Recovery-Knoten aktualisieren.

Aktualisieren des NetScaler ADM Notfallwiederherstellungsknotens

1. Laden Sie die NetScaler ADM-Upgrade-Image-Datei von der NetScaler-Website herunter.
2. Laden Sie diese Datei mit `nsrecover`-Anmeldeinformationen auf den Disaster Recovery-Knoten hoch.
3. Melden Sie sich mit den `nsrecover`-Anmeldeinformationen beim Disaster Recovery-Knoten an.
4. Navigieren Sie zu dem Ordner, in dem Sie die Imagedatei abgelegt haben, und entpacken Sie die Datei.


```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Wed May 15 05:27:10 2019 from 10.252.241.103
bash-3.2# cd /var/mps/mps_images
bash-3.2# tar xvfz build-mas-13.0-36.25.tgz
```

5. Führen Sie das folgende Skript aus:

   ./installmas

```
bash-3.2# ./installmas
```

Upgrade von On-Premises-Agents für die Bereitstellung an mehreren Standorten

Das Upgrade der NetScaler ADM Agent-Bereitstellung erfolgt in drei Schritten.
Stellen Sie sicher, dass Sie die folgenden Aufgaben ausgeführt haben, bevor Sie die On-Premises-Agents aktualisieren:

1. Aktualisieren Sie die NetScaler ADM -Server, die in Hochverfügbarkeit bereitgestellt werden.
2. Aktualisieren Sie den NetScaler ADM Notfallwiederherstellungsknoten.

   Weitere Informationen finden Sie unter Aktualisieren der NetScaler ADM-Disaster Recovery-Bereitstellung.

Upgrade der On-Premises-Agents

1. Laden Sie die NetScaler ADM Agent-Upgrade-Image-Datei von der NetScaler-Website herunter.
2. Laden Sie diese Datei mit den `nsrecover`-Anmeldeinformationen auf den Agentknoten hoch.
3. Stellen Sie sicher, dass Sie das richtige Agent-Upgradeimage herunterladen.
4. Melden Sie sich mit den `nsrecover`-Anmeldeinformationen beim On-Prem-Agent an.
5. Navigieren Sie zu dem Ordner, in dem Sie die Imagedatei abgelegt haben, und entpacken Sie die Datei.

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 30 08:50:48 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-masagent-12.1-502.109.tgz
```

6. Führen Sie das folgende Skript aus:

   `./installmasagent`


```
bash-3.2# ./installmasagent
```

Zusätzlichen Datenträger für NetScaler ADM-Server bereitstellen

Wenn Ihre NetScaler ADM-Speicheranforderungen den Standardspeicherplatz (120 GB) überschreiten, können Sie einen zusätzlichen Datenträger anschließen. Sie können mehr Datenträger sowohl in Bereitstellungen mit einem Server als auch in Bereitstellungen mit hoher Verfügbarkeit anhängen.

Wenn Sie NetScaler ADM von der Release-Version 12.1—13.10 aktualisieren, bleiben die Partitionen, die Sie in der früheren Version auf der zusätzlichen Festplatte erstellt haben, unverändert. Die Partitionen werden nicht entfernt oder in der Größe geändert.

Das Verfahren zum Bereitstellen weiterer Datenträger bleibt im aktualisierten Build unverändert. Sie können jetzt das neue Datenträgerpartitionierungstool in NetScaler ADM verwenden, um Partitionen auf dem neu hinzugefügten Datenträger zu erstellen. Sie können das Tool auch verwenden, um die Größe der Partitionen auf der vorhandenen More Disk zu ändern. Weitere Informationen zum Bereitstellen weiterer Datenträger und zur Verwendung des neuen Datenträgerpartitionierungstools finden Sie unter Bereitstellen eines zusätzlichen Datenträgers in NetScaler ADM.

Authentifizierung

February 5, 2024

Benutzer können entweder intern durch NetScaler ADM, extern durch einen Authentifizierungsserver oder beides authentifiziert werden. Wenn die lokale Authentifizierung verwendet wird, muss sich der Benutzer in der NetScaler ADM -Sicherheitsdatenbank befinden. Wenn der Benutzer extern authentifiziert wird, muss der „externe Name“des Benutzers je nach ausgewähltem Authentifizierungsprotokoll mit der externen Benutzeridentität übereinstimmen, die auf dem Authentifizierungsserver registriert ist.

NetScaler ADM unterstützt externe Authentifizierung durch RADIUS-, LDAP- und TACACS-Server. Diese einheitliche Unterstützung bietet eine gemeinsame Schnittstelle zur Authentifizierung und Autorisierung aller lokalen und externen Benutzer von Authentifizierungs-, Autorisierungs- und Buchhaltungsservern, die auf das System zugreifen. NetScaler ADM kann Benutzer unabhängig von den tatsächlichen Protokollen authentifizieren, die sie für die Kommunikation mit dem System verwenden. Wenn ein Benutzer versucht, auf eine NetScaler ADM-Implementierung zuzugreifen, die für die externe Authentifizierung konfiguriert ist, sendet der angeforderte Anwendungsserver den Benutzernamen und das Kennwort zur Authentifizierung an den RADIUS-, LDAP- oder TACACS-Server. Wenn die Authentifizierung erfolgreich ist, erhält der Benutzer Zugriff auf NetScaler ADM.

Externe Authentifizierungsserver

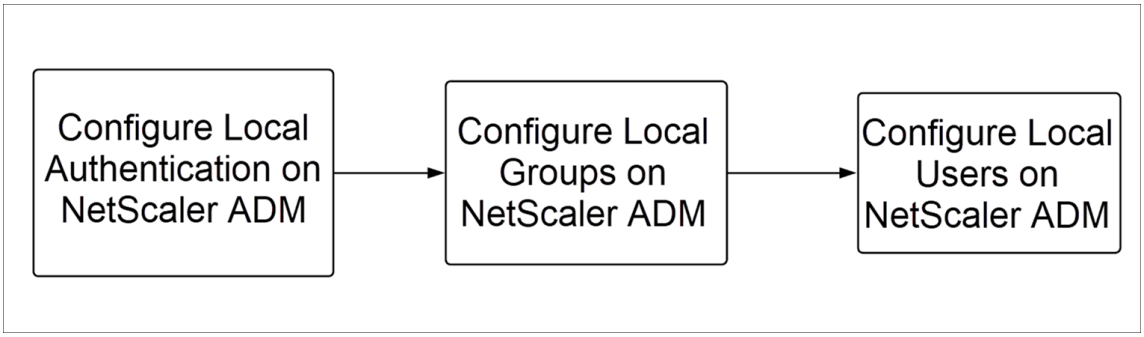
NetScaler ADM sendet alle Anforderungen an Authentifizierungs-, Autorisierungs- und Überwachungsdienste an den Remote-RADIUS-, LDAP- oder TACACS-Server. Der Remote-Authentifizierungs-, Autorisierungs- und Überwachungsserver erhält die Anfrage, validiert die Anfrage und sendet eine Antwort an NetScaler ADM. Bei der Konfiguration für die Verwendung eines RADIUS-, TACACS- oder LDAP-Servers für die Authentifizierung wird NetScaler ADM zu einem RADIUS-, TACACS- oder LDAP-Client. In jeder dieser Konfigurationen werden Authentifizierungsdatensätze in der Remotehostserver-Datenbank gespeichert. Der Kontoname, die zugewiesenen Berechtigungen und die Zeitbuchhaltungsdatensätze werden ebenfalls auf dem Authentifizierungs-, Autorisierungs- und Überwachungsserver für jeden Benutzer gespeichert.

Außerdem können Sie die interne Datenbank von NetScaler ADM verwenden, um Benutzer lokal zu authentifizieren. Sie erstellen Einträge in der Datenbank für Benutzer und deren Kennwörter und Standardrollen. Sie können auch die Authentifizierungsreihenfolge für bestimmte Authentifizierungstypen auswählen. Die Liste der Server in einer Servergruppe ist eine geordnete Liste. Der erste Server in der Liste wird immer verwendet, es sei denn, er ist nicht verfügbar. In diesem Fall wird der nächste Server in der Liste verwendet. Sie können Server so konfigurieren, dass sie die interne Datenbank als Fallback-Authentifizierungsbackup in die konfigurierte Liste der Authentifizierungs-, Autorisierungs- und Überwachungsserver aufnehmen.

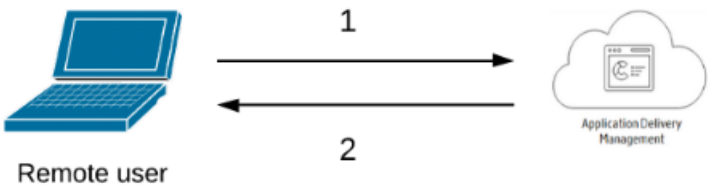
Authentifizieren von Benutzern in NetScaler ADM

Sie können Ihre Benutzer in NetScaler ADM auf zwei Arten authentifizieren:

- In NetScaler ADM konfigurierte lokale Benutzer



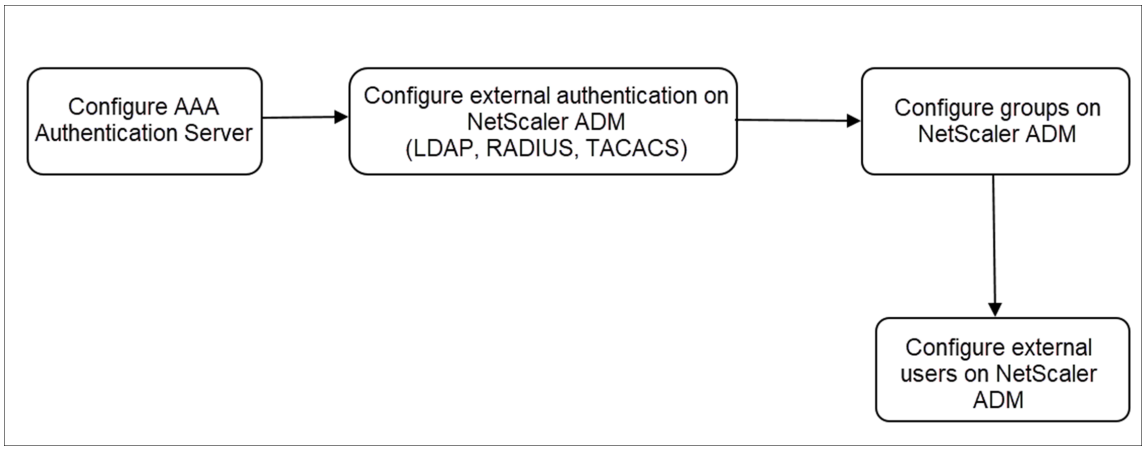
  Nach der Konfiguration ist der folgende Workflow für die Benutzerauthentifizierung auf dem lokalen Server beschrieben.



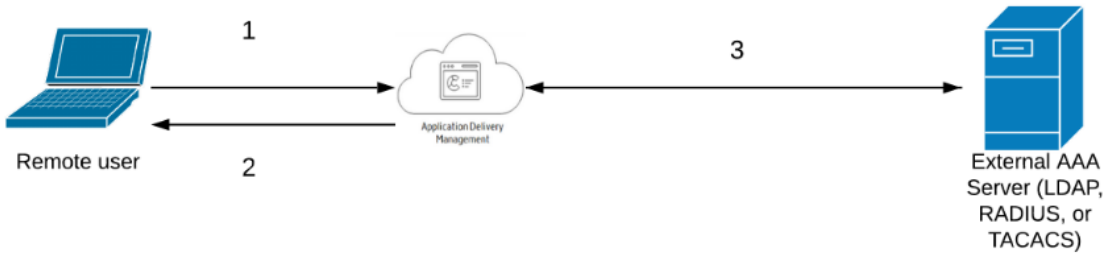
1 —Der Benutzer meldet sich bei NetScaler ADM an

2 —NetScaler ADM fordert die Benutzer zur Eingabe von Anmeldeinformationen für die Authentifizierung auf und prüft, ob die Anmeldeinformationen in der ADM-Datenbank übereinstimmen.

- Verwendung von externen Authentifizierungsservern



Nach der Konfiguration ist der folgende Workflow für die Benutzerauthentifizierung auf dem externen Authentifizierungs-, Autorisierungs- und Überwachungsserver beschrieben:



1 —Der Benutzer stellt eine Verbindung mit NetScaler ADM her

2 —NetScaler ADM fordert den Benutzer zur Eingabe von Anmeldeinformationen auf

3 —NetScaler ADM validiert die Anmeldeinformationen des Benutzers mit dem externen Authentifizierungs-, Autorisierungs- und Überwachungsserver. Wenn die Validierung erfolgreich ist, kann sich der Benutzer weiterhin anmelden

Externe Authentifizierungsserver in NetScaler ADM konfigurieren

February 5, 2024

Nachdem Sie den LDAP-, RADIUS- oder TACACS-Server konfiguriert haben, können Sie diese Server in NetScaler ADM hinzufügen.

LDAP-Authentifizierungsserver hinzufügen

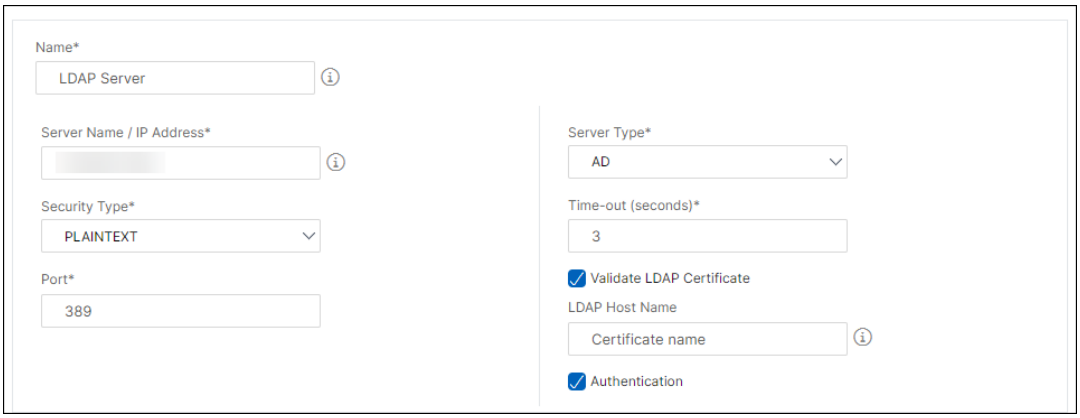
February 5, 2024

Wenn Sie das LDAP-Protokoll mit RADIUS- und TACAS-Authentifizierungsservern integrieren, können Sie ADM verwenden, um Benutzeranmeldeinformationen aus verteilten Verzeichnissen zu suchen und zu authentifizieren.

1. Navigieren Sie zu **Einstellungen> Authentifizierung**.
2. Wählen Sie die Registerkarte **LDAP** aus, und klicken Sie dann auf **Hinzufügen**.
3. Geben Sie auf der Seite „ **LDAP-Server erstellen** “die folgenden Parameter an:
    a) **Name** —Geben Sie den LDAP-Servernamen an
    b) **Servername/IP-Adresse** —Geben Sie die LDAP-IP-Adresse oder den Servernamen an
    c) **Sicherheitstyp** —Art der Kommunikation, die zwischen dem System und dem LDAP-Server erforderlich ist. Wählen Sie aus der Liste aus. Wenn die Klartextkommunikation unzureichend ist, können Sie verschlüsselte Kommunikation wählen, indem Sie entweder Transport Layer Security (TLS) oder SSL auswählen.
    d) **Port** —Standardmäßig wird Port 389 für PLAINTEXT verwendet. Sie können auch Port 636 für SSL/TLS angeben
    e) **Servertyp** —Wählen Sie Active Directory (AD) oder Novell Directory Service (NDS) als Typ des LDAP-Servers aus.
    f) **Timeout (Sekunden)** —Zeit in Sekunden, auf die das NetScaler ADM -System auf eine Antwort vom LDAP-Server wartet
    g) **LDAP-Hostname** —Aktivieren Sie das Kontrollkästchen „LDAP-Zertifikat validieren“und geben Sie den Hostnamen an, der in das Zertifikat eingegeben werden soll

    Deaktivieren Sie die **Authentifizierungsoption**, und geben Sie den öffentlichen SSH-Schlüssel an. Mit der schlüsselbasierten Authentifizierung können Sie jetzt die Liste der

öffentlichen Schlüssel, die auf dem Benutzerobjekt auf dem LDAP-Server gespeichert sind, über SSH abrufen.



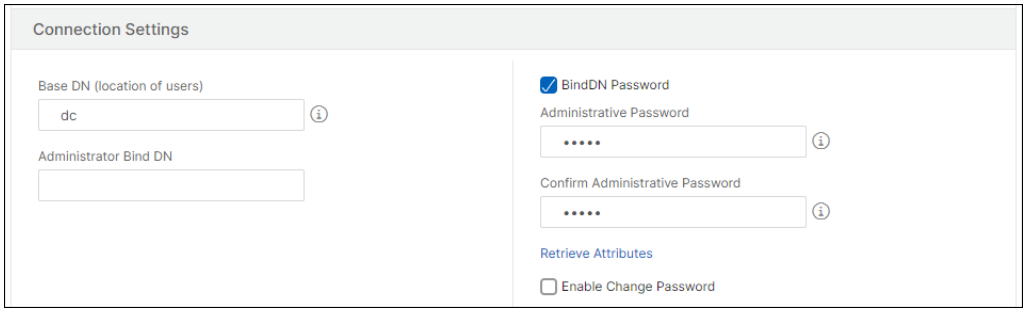
Geben Sie unter Verbindungseinstellungen die folgenden Parameter an:

i. **Basis-DN** —Der Basisknoten für den LDAP-Server, um die Suche zu starten

ii. **Administrator-Bind-DN** —Benutzername, der an den LDAP-Server gebunden ist. Zum Beispiel admin@aaa.local.

iii. **Bind-DN-Kennwort** —Wählen Sie diese Option, um ein Kennwort für die Authentifizierung bereitzustellen

iv. **Kennwort ändern aktivieren** —Wählen Sie diese Option, um die Kennwortänderung zu aktivieren



Geben Sie unter **Andere Einstellungen**die folgenden Parameter an

i. **Server-Anmeldenamensattribut** —Namensattribut, das vom System verwendet wird, um den externen LDAP-Server oder ein Active Directory abzufragen. Wählen Sie **samAccountname** aus der Liste aus.

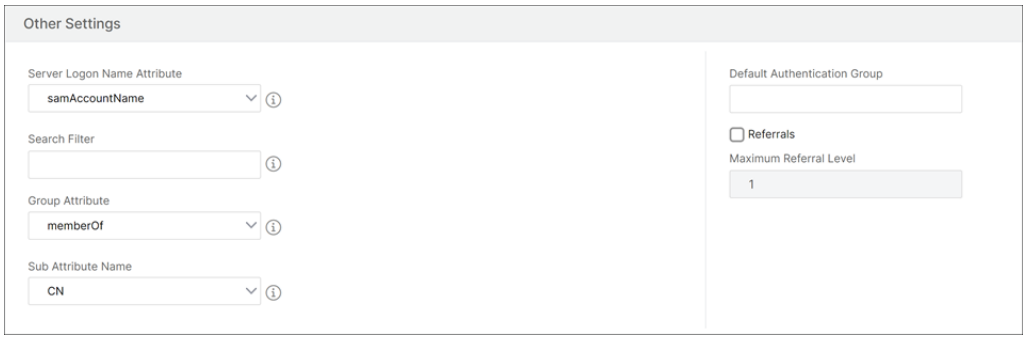
ii. **Suchfilter** —Konfigurieren Sie externe Benutzer für die Zwei-Faktor-Authentifizierung gemäß dem im LDAP-Server konfigurierten Suchfilter. Zum Beispiel würde vpnallowed=true mit ldaploginame `samaccount` und dem vom Benutzer bereitgestellten Benutzernamen bob eine LDAP-Suchzeichenfolge von: ergeben `&(vpnallowed=true)(samaccount=bob)`.

> Hinweis
>
> Standardmäßig sind die Werte im Suchfilter in Klammern eingeschlossen.

iii. **Gruppenattribut** —Wählen Sie MemberOf aus der Liste aus.

iv. **Name des Unterattributs** —Der Name des Unterattributs für die Gruppenextraktion vom LDAP-Server.

v. **Standardauthentifizierungsgruppe** —Standardgruppe, die zusätzlich zu den extrahierten Gruppen ausgewählt wird, wann die Authentifizierung erfolgreich ist.



4. Klicken Sie auf **Erstellen**.

   Der LDAP-Server ist jetzt konfiguriert.

   > **Hinweis**:
   >
   > Wenn die Benutzer Active Directory Gruppenmitglieder sind, müssen die Gruppe und die Namen der Benutzer in NetScaler ADM dieselben Namen von Active Directory Gruppenmitgliedern haben.

5. Aktivieren Sie die externen Authentifizierungsserver.

   Weitere Informationen zum Aktivieren externer Authentifizierungsserver finden Sie unter Externe Authentifizierungsserver und Fallback-Optionen aktivieren.

RADIUS-Authentifizierungsserver hinzufügen

February 5, 2024

1. Navigieren Sie zu **Einstellungen> Authentifizierung**.
2. Wählen Sie die Registerkarte **RADIUS** aus, und klicken Sie dann auf **Hinzufügen**.

   Geben Sie auf der Seite **RADIUS-Server erstellen** die folgenden Parameter an:

a) **Name** —Geben Sie einen RADIUS-Servernamen an

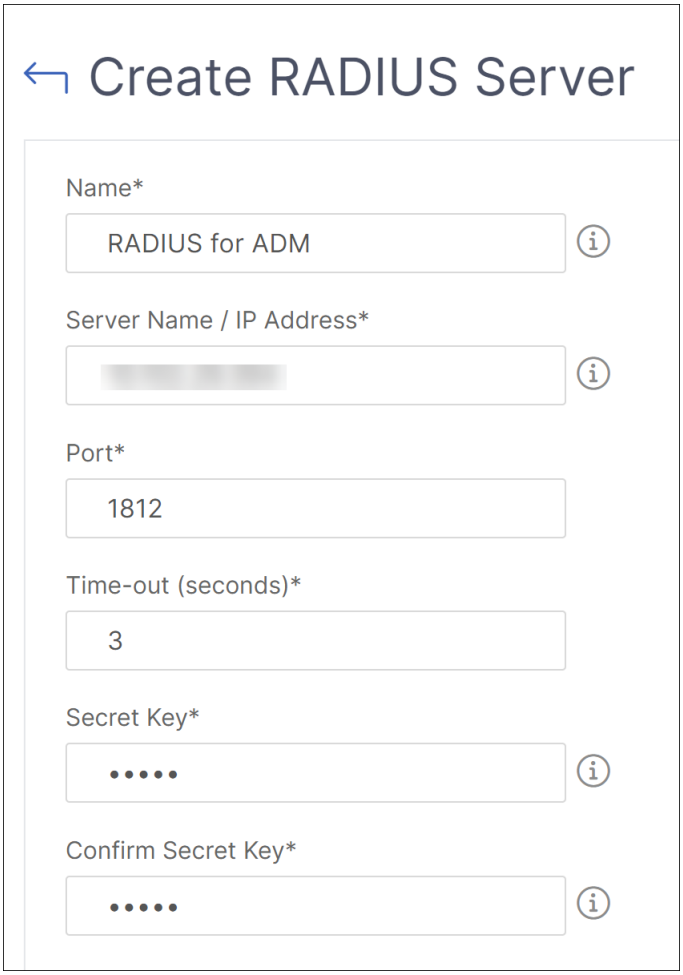
b) **Servername/IP-Adresse** —Geben Sie die IP-Adresse des RADIUS-Servers an

c) **Port** —Geben Sie die Portnummer an, auf der der RADIUS-Server gehostet wird. Der Standardport ist 1812

d) **Timeout (Sekunden)** —Zeit in Sekunden, für die das NetScaler ADM-System auf eine Antwort vom RADIUS-Server wartet

e) **Geheimer Schlüssel** —Geben Sie den geheimen RADIUS-Schlüssel für die Authentifizierung an

f) **Geheimen Schlüssel bestätigen** —Geben Sie den Schlüssel zur Bestätigung erneut an



Geben Sie unter **Details**die folgenden Parameter an:

i. **NAS-ID** —Geben Sie die ID an, um die Kennung an den RADIUS-Server zu senden

ii. **Group Vendor Identifier** —Geben Sie die Anbieter-ID für die Verwendung der RADIUS-Gruppenextraktion an.

iii. **Gruppenpräfix** —Eine Zeichenfolge, die Gruppennamen innerhalb eines RADIUS-Attributs für die RADIUS-Gruppenextraktion vorangeht

iv. **Gruppenattributtyp** —Geben Sie den Attributtyp für die RADIUS-Gruppenextraktion an

v. **Gruppentrennzeichen** —Eine Zeichenfolge, die Gruppennamen innerhalb eines RADIUS-Attributs für die RADIUS-Gruppenextraktion abgrenzt

vi. **IP Address Vendor Identifier** —Die Anbieter-ID in RADIUS bezeichnet die Intranet-IP. Ein Wert von 0 gibt an, dass das Attribut nicht herstellerkodiert ist.

vii. **Kennwort Vendor Identifier** —Anbieter-ID-Kennwort in der RADIUS-Antwort zum Extrahieren des Benutzerkennworts

viii. **IP-Adressattributtyp** —Remote-IP-Adressattribut, auf das der RADIUS antworten soll

ix. **Kennwortattributtyp** —Das Kennwortattribut, auf das RADIUS antworten soll

x. **Kennwortkodierung** —Wählen Sie pap, chap, mschapv1 oder mschapv2 aus der Liste aus. Dies gibt an, wie Kennwörter in den RADIUS-Paketen codiert werden sollten, die vom System zum RADIUS-Server übertragen werden.

xi. **Standardauthentifizierungsgruppe** —Standardgruppe, die zusätzlich zu den extrahierten Gruppen ausgewählt wird, wann die Authentifizierung erfolgreich ist

Wählen Sie Accounting aus, wenn die Appliance Auditinformationen auf dem RADIUS-Server protokollieren soll.

3. Klicken Sie auf **Erstellen**.

   Der RADIUS-Server ist jetzt konfiguriert.

4. Aktivieren Sie die externen Authentifizierungsserver.

   Weitere Informationen zum Aktivieren externer Authentifizierungsserver finden Sie unter Externe Authentifizierungsserver und Fallback-Optionen aktivieren.

TACACS-Authentifizierungsserver hinzufügen

February 5, 2024

1. Navigieren Sie zu **Einstellungen> Authentifizierung**.
2. Wählen Sie die Registerkarte **TACACS** aus, und klicken Sie dann auf **Hinzufügen**.
3. Geben Sie auf der Seite **TACACS erstellen** die folgenden Parameter an:

a) **Name** —Geben Sie einen TACACS-Servernamen an

b) **IP-Adresse** —Geben Sie die TACACS-IP-Adresse an

c) **Port** —Geben Sie die Portnummer an, auf der der TACACS-Server gehostet wird. Der Standardport ist 49

d) **Timeout (Sekunden)** —Zeit in Sekunden, auf die das NetScaler ADM -System auf eine Antwort vom LDAP-Server wartet

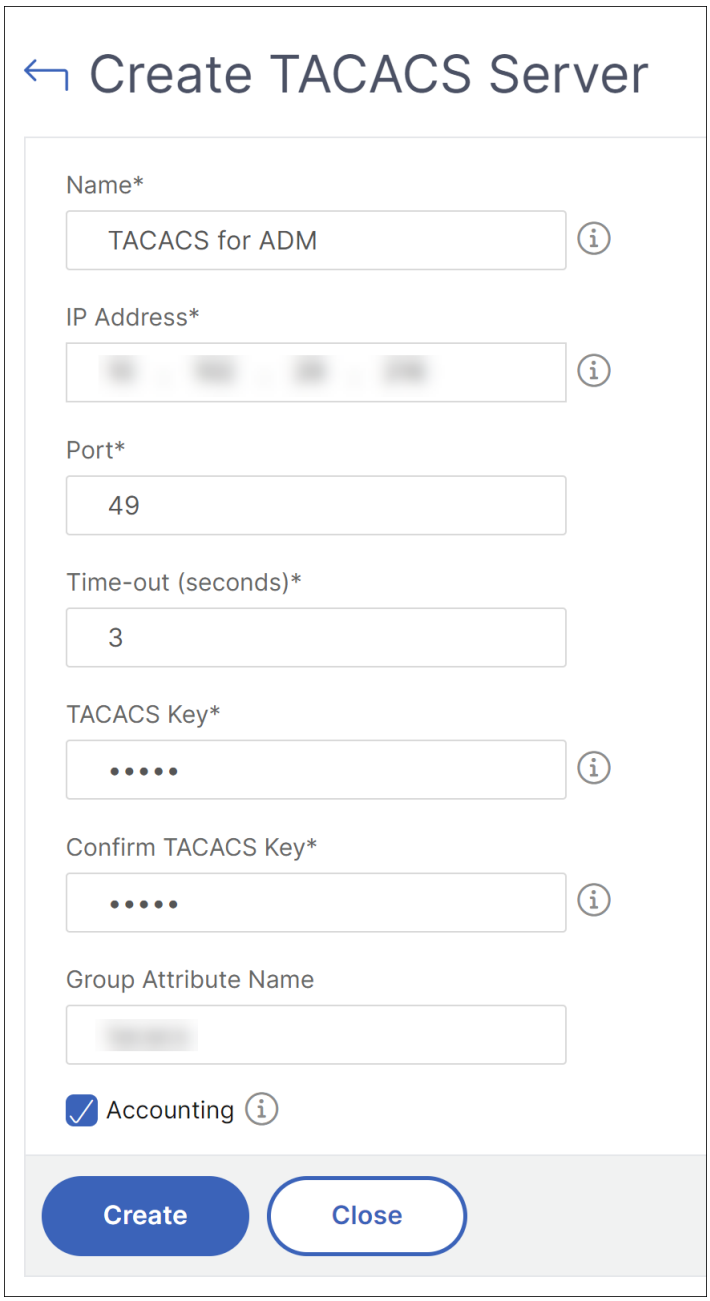
e) **TACACS-Schlüssel** —Geben Sie den TACACS-Schlüssel für die Authentifizierung an

f) **TACACS-Schlüssel bestätigen** —Geben Sie den TACACS-Schlüssel zur Bestätigung erneut an

g) **Name des Gruppenattributs** —Geben Sie den Gruppennamen an

Wählen Sie **Accounting** aus, wenn die Appliance Auditinformationen auf dem TACACS-Server protokollieren soll.

4. Klicken Sie auf **Erstellen**.



5. Aktivieren Sie die externen Authentifizierungsserver.

   Weitere Informationen zum Aktivieren externer Authentifizierungsserver finden Sie unter Externe Authentifizierungsserver und Fallback-Optionen aktivieren.

Benutzer in NetScaler ADM

February 5, 2024

Sie können Benutzerkonten lokal in NetScaler ADM erstellen, um die Benutzer auf Authentifizierungsservern zu ergänzen. Beispielsweise möchten Sie möglicherweise lokale Benutzerkonten für temporäre Benutzer wie Berater oder Besucher erstellen, ohne einen Eintrag für diese Benutzer auf dem Authentifizierungsserver zu erstellen.

Weitere Informationen zum Konfigurieren von Benutzern finden Sie unter Konfigurieren von Benutzern.

> Hinweis
>
> Wenn sich die Benutzer in Active Directory befinden, stellen Sie sicher, dass der Gruppenname in NetScaler ADM mit dem Namen der Active Directory-Gruppe auf dem externen Server übereinstimmt.

Benutzergruppen in NetScaler ADM

Mit NetScaler ADM können Sie Ihre Benutzer authentifizieren und autorisieren, indem Sie Gruppen erstellen und die Benutzer zu den Gruppen hinzufügen. Eine Gruppe kann entweder über „Admin“- oder „Nur Lesen“-Berechtigungen verfügen, und alle Benutzer in dieser Gruppe erhalten die gleichen Berechtigungen.

In NetScaler ADM:

- Eine Gruppe ist definiert als eine Sammlung von Benutzern mit ähnlichen Berechtigungen.
- Eine Gruppe kann eine oder mehrere Rollen haben
- Ein Benutzer ist als eine Entität definiert, die auf der Grundlage der zugewiesenen Berechtigungen Zugriff haben kann.
- Ein Benutzer kann einer oder mehreren Gruppen angehören.

Sie können lokale Gruppen in NetScaler ADM erstellen und die lokale Authentifizierung für die Benutzer in den Gruppen verwenden. Wenn Sie externe Server für die Authentifizierung verwenden, konfigurieren Sie die Gruppen auf NetScaler ADM so, dass sie den Gruppen entsprechen, die auf Authentifizierungsservern im internen Netzwerk konfiguriert sind. Wenn ein Benutzer sich anmeldet und authentifiziert wird und ein Gruppenname mit einer Gruppe auf einem Authentifizierungsserver übereinstimmt, erbt der Benutzer die Einstellungen für die Gruppe in NetScaler ADM.
Wenn Sie die lokale Authentifizierung verwenden, erstellen Sie Benutzer und fügen Sie sie zu Gruppen hinzu, die auf NetScaler ADM konfiguriert sind. Die Benutzer erben dann die Einstellungen für diese Gruppen.

Weitere Informationen zum Konfigurieren von Gruppen und zum Zuweisen von Gruppenberechtigungen finden Sie unter Konfigurieren von Gruppen.

Extrahieren einer Authentifizierungsservergruppe

February 5, 2024

> **Hinweis**
>
> Die TACACS-Serverextraktion wird von **NetScaler**ADM 13.0 unterstützt.

NetScaler ADM ermöglicht Ihnen:

- Extrahieren Sie die Liste der Gruppen, denen ein Benutzer auf dem externen Authentifizierungsserver angehört.
- Weisen Sie sie den Gruppeneinstellungen zu, die mit den auf dem externen Server konfigurierten Gruppen übereinstimmen.

Vorteile:

- Sie müssen keine Benutzer in NetScaler ADM erstellen, da sie auf dem externen Server verwaltet werden.
- NetScaler ADM führt die Autorisierung von Benutzern durch Zuweisen von Gruppenberechtigungen für den Zugriff auf bestimmte virtuelle Load Balancer-Server und für bestimmte Anwendungen auf dem System durch.

Externe Authentifizierungsserver und Fallback-Optionen aktivieren

February 5, 2024

Mit der Fallback-Option kann die lokale Authentifizierung übernommen werden, falls die externe Serverauthentifizierung fehlschlägt. Ein Benutzer, der sowohl auf NetScaler ADM als auch auf dem externen Authentifizierungsserver konfiguriert ist, kann sich bei NetScaler ADM anmelden, auch wenn die konfigurierten externen Authentifizierungsserver ausgefallen oder nicht erreichbar sind. Um sicherzustellen, dass die Fallback-Authentifizierung funktioniert:

- Nicht-NSRoot-Benutzer müssen auf NetScaler ADM zugreifen können, wenn der externe Server ausgefallen oder nicht erreichbar ist
- Sie müssen mindestens einen externen Server hinzufügen

NetScaler ADM unterstützt außerdem ein einheitliches System von Authentifizierungs-, Autorisierungs- und Abrechnungsprotokollen (AAA) (LDAP, RADIUS und TACACS) sowie lokale Authentifizierung.

Diese vereinheitlichte Unterstützung bietet eine gemeinsame Schnittstelle zur Authentifizierung und Autorisierung aller Benutzer und externen AAA-Clients, die auf das System zugreifen.

NetScaler ADM kann Benutzer unabhängig von den tatsächlichen Protokollen authentifizieren, die sie für die Kommunikation mit dem System verwenden.
Kaskadierende externe Authentifizierungsserver bieten einen kontinuierlichen, fehlerfreien Prozess zur Authentifizierung und Autorisierung externer Benutzer. Wenn die Authentifizierung auf dem ersten Authentifizierungsserver fehlschlägt, versucht NetScaler ADM, den Benutzer mithilfe des zweiten externen Authentifizierungsservers zu authentifizieren usw. Um die kaskadierte Authentifizierung zu aktivieren, müssen Sie die externen Authentifizierungsserver in NetScaler ADM hinzufügen. Sie können jeden Typ der unterstützten externen Authentifizierungsserver (RADIUS, LDAP und TACACS) hinzufügen.

Stellen Sie sich beispielsweise vor, dass Sie vier externe Authentifizierungsserver hinzufügen und zwei RADIUS-Server, einen LDAP-Server und einen TACACS-Server konfigurieren möchten. NetScaler ADM versucht, sich auf der Grundlage der Konfigurationen bei den externen Servern zu authentifizieren. In diesem Beispielszenario versucht NetScaler ADM:

- Stellen Sie eine Verbindung zum ersten RADIUS-Server her
- Stellen Sie eine Verbindung zum zweiten RADIUS-Server her, wenn die Authentifizierung mit dem ersten RADIUS-Server fehlgeschlagen ist
- Stellen Sie eine Verbindung zum LDAP-Server her, wenn die Authentifizierung mit beiden RADIUS-Servern fehlgeschlagen ist
- Stellen Sie eine Verbindung zum TACACS-Server her, wenn die Authentifizierung sowohl bei RADIUS-Servern als auch beim LDAP-Server fehlgeschlagen ist.

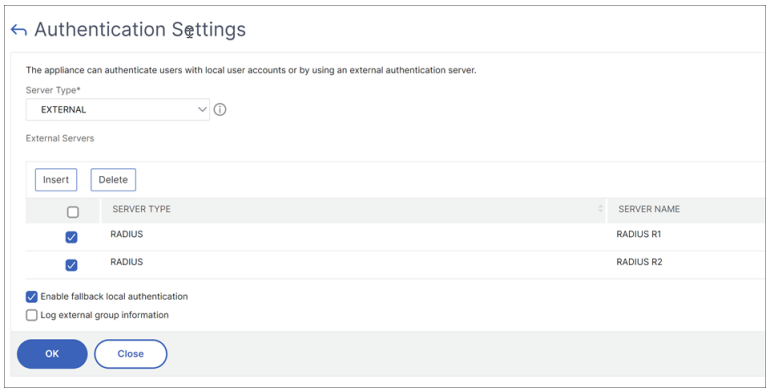
> Hinweis
>
> Sie können bis zu 32 externe Authentifizierungsserver in NetScaler ADM konfigurieren.

Konfigurieren von Fallback und Kaskadierung externer Server

1. Navigieren Sie zu **Einstellungen> Authentifizierung**.
2. Klicken Sie auf der Seite **Authentifizierung** auf **Einstellungen**.
3. Wählen Sie auf der Seite **Authentifizierungskonfiguration** in der Liste **Servertyp** die Option **EXTERNAL** aus (nur externe Server können kaskadiert werden).
4. Klicken Sie auf **Einfügen**und wählen Sie auf der Seite **Externe Server** einen oder mehrere Authentifizierungsserver aus, die kaskadiert werden sollen.

5. Aktivieren Sie das Kontrollkästchen **Lokale Fallback-Authentifizierung aktivieren**, wenn die lokale Authentifizierung übernommen werden soll, wenn die externe Authentifizierung fehlschlägt.
6. Aktivieren Sie das Kontrollkästchen **Externe Gruppeninformationen protokollieren**, wenn Sie die externen Benutzergruppeninformationen im Systemüberwachungsprotokoll erfassen möchten.
7. Klicken Sie auf **OK**, um die Seite zu schließen.

   Die ausgewählten Server werden unter Externe Server angezeigt:



Sie können die Reihenfolge der Authentifizierung auch angeben, indem Sie das Symbol neben den Servernamen verwenden, um Server in der Liste nach oben oder unten zu verschieben.

Zugriffssteuerung

February 5, 2024

Authentifizierung ist ein Prozess, mit dem Sie überprüfen, ob jemand der ist, der sie behauptet, dass sie sind. Um eine Authentifizierung durchzuführen, muss ein Benutzer bereits über ein Konto in einem System verfügen, das durch den Authentifizierungsmechanismus abgefragt werden kann, oder ein Konto muss im Rahmen des Prozesses der ersten Authentifizierung erstellt werden. NetScaler Application Delivery Management (ADM) bietet eine Methode zur Authentifizierung sowohl lokaler als auch externer Benutzer. Während lokale Benutzer intern authentifiziert werden, unterstützt NetScaler ADM die externe Authentifizierung mit den Protokollen RADIUS, LDAP und TACACS. Wenn ein Benutzer versucht, auf NetScaler ADM zuzugreifen, das für die externe Authentifizierung konfiguriert ist, sendet der angeforderte Anwendungsserver den Benutzernamen und das Kennwort zur Authentifizierung an den RADIUS-, LDAP- oder TACACS-Server. Nach der Authentifizierung wird das erforderliche Protokoll verwendet, um den Benutzer auf NetScaler ADM zu identifizieren.

Zugriffskontrolle ist der Prozess, bei dem die erforderliche Sicherheit für eine bestimmte Ressource durchgesetzt wird. Es handelt sich um eine Sicherheitstechnik, mit der reguliert werden kann, wer Ressourcen in einer Computerumgebung einsehen oder verwenden kann. Der Zweck der Zugriffskontrolle besteht darin, die Aktionen oder Vorgänge einzuschränken, die ein rechtmäßiger Benutzer eines Computersystems ausführen kann. Die Zugriffskontrolle schränkt ein, was ein Benutzer direkt tun kann und welche Programme, die im Namen der Benutzer ausgeführt werden, ausführen dürfen. Auf diese Weise zielt die Zugriffssteuerung darauf ab, Aktivitäten zu verhindern, die zu einer Sicherheitsverletzung führen können. Bei der Zugriffssteuerung wird davon ausgegangen, dass die Authentifizierung des Benutzers vor der Erzwingung der Zugriffssteuerung über einen Referenzmonitor erfolgreich überprüft wurde. NetScaler ADM ermöglicht eine differenzierte, rollenbasierte Zugriffskontrolle (RBAC), mit der die Administratoren Benutzern Zugriffsberechtigungen gewähren können, die auf den Rollen einzelner Benutzer innerhalb eines Unternehmens basieren. RBAC in NetScaler ADM wird durch das Erstellen von Zugriffsrichtlinien, Rollen, Gruppen und Benutzern erreicht.

Rollenbasierte Zugriffssteuerung

February 5, 2024

NetScaler ADM bietet eine differenzierte, rollenbasierte Zugriffskontrolle (RBAC), mit der Sie Zugriffsberechtigungen auf der Grundlage der Rollen einzelner Benutzer in Ihrem Unternehmen gewähren können. In diesem Zusammenhang ist der Zugriff die Möglichkeit, eine bestimmte Aufgabe auszuführen, z. B. eine Datei anzuzeigen, zu erstellen, zu ändern oder zu löschen. Rollen werden entsprechend der Autorität und Verantwortlichkeit der Benutzer innerhalb des Unternehmens definiert. Beispielsweise kann ein Benutzer alle Netzwerkvorgänge ausführen, während ein anderer Benutzer den Datenverkehrsfluss in Anwendungen beobachten und beim Erstellen von Konfigurationsvorlagen helfen kann.

Rollen werden durch in Richtlinien festgelegt. Nachdem Sie Richtlinien erstellt haben, erstellen Sie Rollen, binden jede Rolle an eine oder mehrere Richtlinien und weisen Benutzern Rollen zu. Sie können auch Benutzergruppen Rollen zuweisen.

Eine Gruppe ist eine Sammlung von Benutzern, die über gemeinsame Berechtigungen verfügen. Beispielsweise können Benutzer, die ein bestimmtes Rechenzentrum verwalten, einer Gruppe zugewiesen werden. Eine Rolle ist eine Identität, die Benutzern oder Gruppen auf der Grundlage bestimmter Bedingungen gewährt wird. In NetScaler ADM ist das Erstellen von Rollen und Richtlinien spezifisch für die RBAC-Funktion in NetScaler. 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. Stellen Sie sich beispielsweise einen SSL-/Sicherheitsadministrator und einen Anwendungsadministrator vor. 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. Ein Anwendungsadministrator muss nur auf die Ressourcen innerhalb des Bereichs zugreifen können.

Beispiel:

Chris, der Leiter der ADC-Gruppe, ist der Superadministrator von NetScaler ADM in seiner Organisation. Chris erstellt drei Administratorrollen: Sicherheitsadministrator, Anwendungsadministrator und Netzwerkadministrator.

David, der Sicherheitsadministrator, muss über vollständigen Zugriff auf die Verwaltung und Überwachung von SSL-Zertifikaten verfügen, aber auch über schreibgeschützten Zugriff für den Systemverwaltungsbetrieb verfügen.

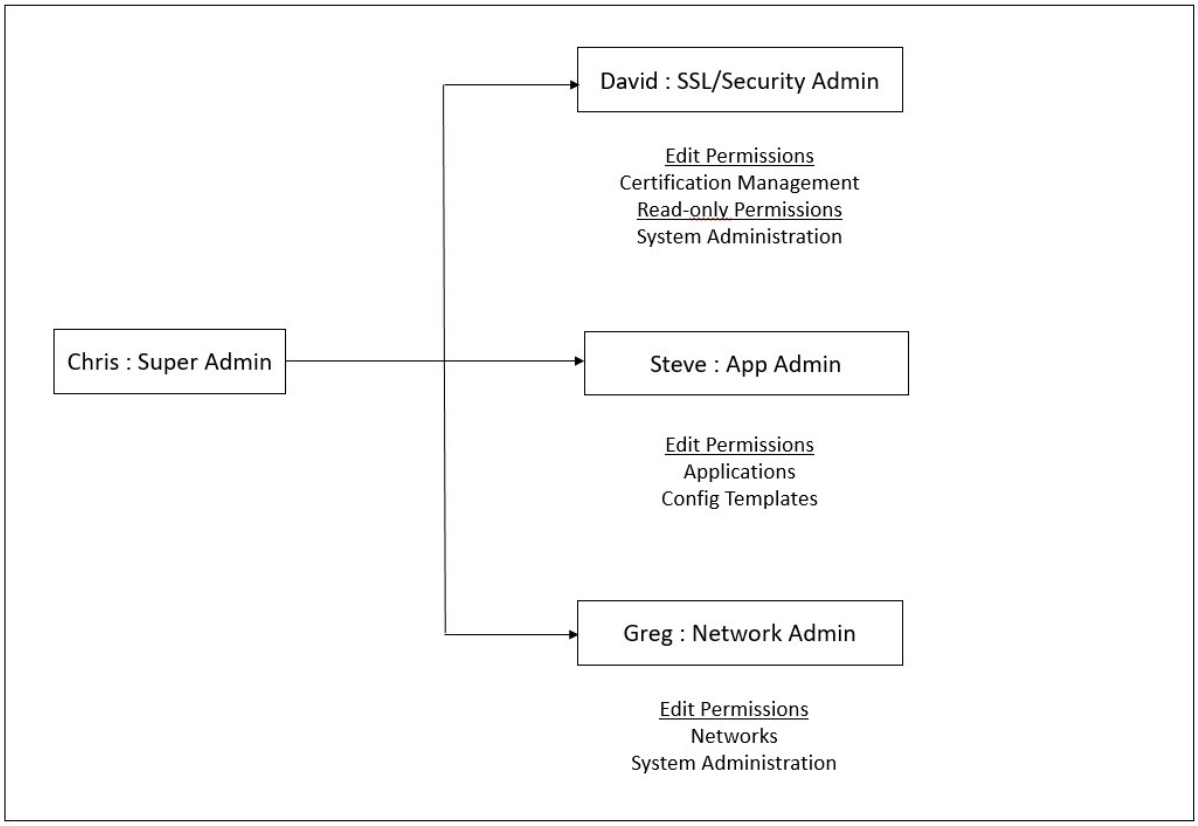
Steve, ein Anwendungsadministrator, benötigt nur Zugriff auf bestimmte Anwendungen und nur bestimmte Konfigurationsvorlagen.

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.

Benutzer von NetScaler ADM können lokal authentifiziert oder über einen externen Server (RADIUS/LDAP/TACACS) authentifiziert werden. RBAC-Einstellungen müssen unabhängig von der verwendeten Authentifizierungsmethode für alle Benutzer gelten.

Das folgende Bild zeigt die Berechtigungen, die Administratoren und andere Benutzer haben und ihre Rollen in der Organisation.



Einschränkungen

RBAC wird für die folgenden NetScaler ADM-Funktionen nicht vollständig unterstützt:

- **Analytics** - RBAC wird in den Analytics-Modulen nicht vollständig unterstützt. Die RBAC-Unterstützung ist auf Instanzebene beschränkt und gilt nicht auf Anwendungsebene in den Analysemodulen Web Insight, SSL Insight, Gateway Insight, HDX Insight und WAF Security Violations. Beispiel:

Beispiel 1: Instanzbasierte RBAC (unterstützt)

Ein Administrator, dem einige Instanzen zugewiesen wurden, kann unter **Web Insight** > **Instances** nur diese Instanzen und unter **Web Insight** > **Applications** nur die entsprechenden virtuellen Server sehen, da RBAC auf Instanzebene unterstützt wird.

Beispiel 2: Anwendungsbasiertes RBAC (nicht unterstützt)

Ein Administrator, dem einige Anwendungen zugewiesen wurden, kann alle virtuellen Server unter **Web Insight** > **Anwendungen** sehen, kann aber nicht auf sie zugreifen, da RBAC auf Anwendungsebene nicht unterstützt wird.

- **StyleBooks** —RBAC wird für StyleBooks nicht vollständig unterstützt.

  - In NetScaler ADM werden StyleBooks und Config Packs als separate Ressourcen betrachtet. Zugriffsberechtigungen, entweder zum Anzeigen, Bearbeiten oder beides, können für StyleBook und Config Packs separat oder gleichzeitig gewährt werden. Eine Anzeige- oder Bearbeitungsberechtigung für Konfigurationspakete ermöglicht dem Benutzer implizit das Anzeigen der StyleBooks, was für das Abrufen der Konfigurationspaketdetails und das Erstellen der Konfigurationspakete unerlässlich ist.
  - Die Zugriffsberechtigung für bestimmte StyleBook- oder Konfigurationspakete wird nicht unterstützt
    . Beispiel: Wenn die Instanz bereits ein Konfigurationspaket enthält, können Benutzer die Konfiguration auf einer NetScaler-Zielinstanz ändern, auch wenn sie keinen Zugriff auf diese Instanz haben.

- **Orchestrierung** - RBAC wird für Orchestration nicht unterstützt.

Zugriffsrichtlinien konfigurieren

February 5, 2024

Zugriffsrichtlinien definieren Berechtigungen. Eine Richtlinie kann auf einen einzelnen Benutzer oder eine Gruppe oder auf mehrere Benutzer und mehrere Gruppen angewendet werden. NetScaler Application Delivery Management (ADM) bietet vier vordefinierte Zugriffsrichtlinien:

1. **Admin-Richtlinie.** Gewährt Zugriff auf alle NetScaler ADM-Funktionen. Der Benutzer verfügt sowohl über Ansichts- als auch über Bearbeitungsberechtigungen, kann alle NetScaler ADM-Inhalte anzeigen und alle Bearbeitungsvorgänge ausführen. Das heißt, der Benutzer kann Operationen zum Hinzufügen, Ändern und Löschen an den Ressourcen ausführen.
2. **Richtlinie nur zum Lesen**. Gewährt schreibgeschützte Berechtigungen. Der Benutzer kann den gesamten Inhalt auf NetScaler ADM anzeigen, ist jedoch nicht berechtigt, irgendwelche Operationen auszuführen.
3. **appAdminPolicy**. Gewährt Administratorberechtigungen für den Zugriff auf die Anwendungsfunktionen in NetScaler 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.
4. **appReadOnlyPolicy**. Gewährt schreibgeschützte Berechtigung für Anwendungsfunktionen. Ein an diese Richtlinie gebundener Benutzer kann die Anwendungen anzeigen, aber keine Vorgänge zum Hinzufügen, Ändern, Löschen, Aktivieren oder Deaktivieren ausführen.

> **Hinweis:**
>
> Die vordefinierten Richtlinien können nicht bearbeitet werden.

Sie können auch Ihre eigenen (benutzerdefinierten) Richtlinien erstellen.

So erstellen Sie benutzerdefinierte Zugriffsrichtlinien:

1. Navigieren Sie in NetScaler ADM zu **Einstellungen > Benutzer und Rollen**Zugriffsrichtlinien.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Richtlinienname** den Namen der Richtlinie und die Beschreibung in das Feld **Richtlinienbeschreibung** ein.

   Im Abschnitt **Berechtigungen** werden alle NetScaler ADM-Funktionen mit Optionen zum Angeben von schreibgeschütztem Zugriff, Aktivieren/Deaktivieren oder Bearbeiten aufgeführt.
4. Klicken Sie auf das Symbol (+), um jede Feature-Gruppe in mehrere Features zu erweitern.

   a) 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 NetScaler ADM anzeigen.
   - **Aktivieren-Deaktivieren:** Diese Option ist nur für die **Netzwerkfunktionsfunktionen** verfügbar, die das Aktivieren oder Deaktivieren von Aktionen in NetScaler ADM ermöglichen. Benutzer können die Funktion aktivieren oder deaktivieren. Und der Benutzer kann auch die Aktion **Jetzt abfragen** ausführen.

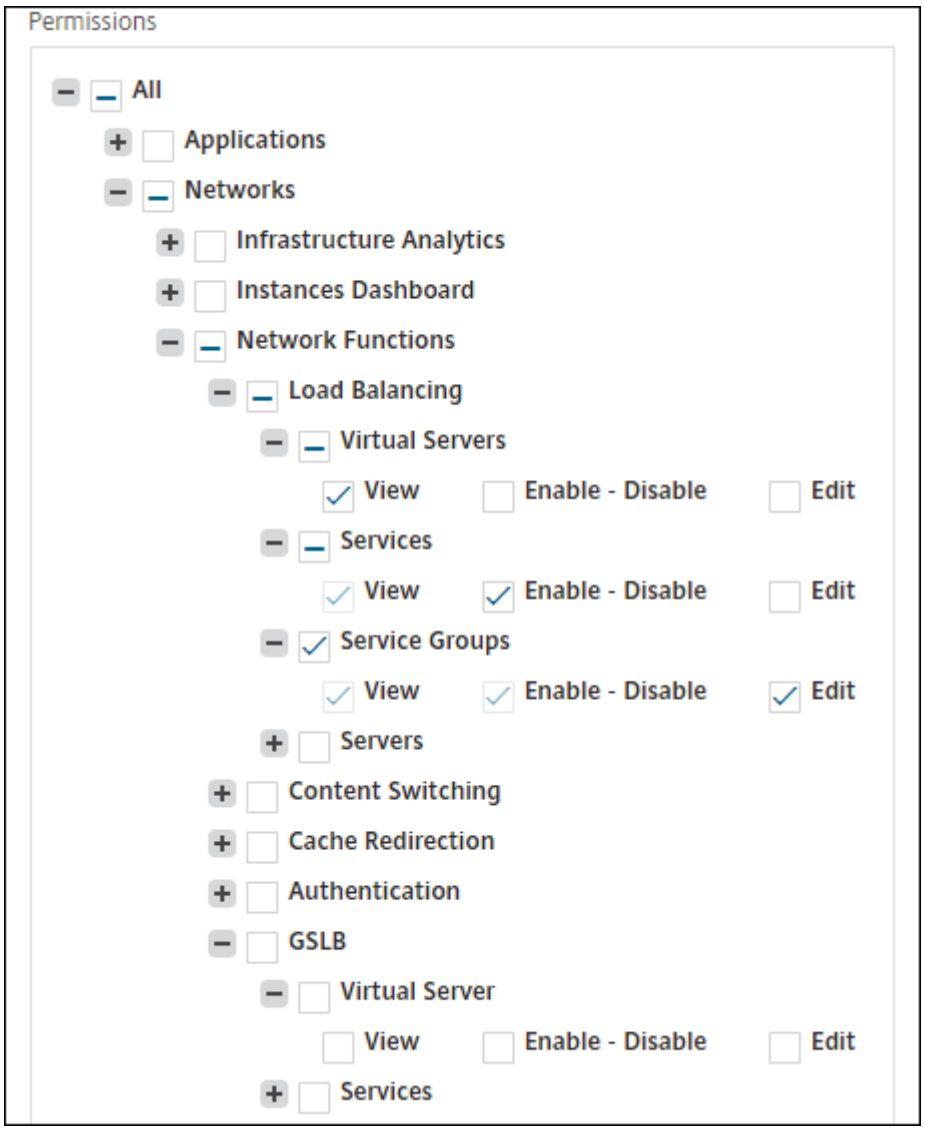
     Wenn Sie einem Benutzer die Berechtigung zum Aktivieren und **Deaktivieren** erteilen, wird auch die Berechtigung **Anzeigen** erteilt. Sie können diese Option nicht deaktivieren.
   - **Bearbeiten:** Diese Option gewährt dem Benutzer vollen Zugriff. Der Benutzer kann das Feature und seine Funktionen ändern.

     Wenn Sie die Berechtigung **Bearbeiten** erteilen, werden sowohl die Berechtigungen **Anzeigen** als auch **Aktivieren/Deaktivieren** gewährt. 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 Load Balancing und GSLB, um weitere Konfigurationsoptionen anzuzeigen.

   In der folgenden Abbildung haben die Konfigurationsoptionen der Load Balancing-Funktion unterschiedliche Berechtigungen:



Die **View-Berechtigung** wird einem Benutzer für die Funktion **Virtuelle Server** erteilt. Benutzer können die virtuellen Lastausgleichsserver in NetScaler ADM anzeigen. Um virtuelle Server anzuzeigen, navigieren Sie zu **Infrastruktur > Netzwerkfunktionen > Load Balancing** und wählen Sie die Registerkarte **Virtuelle Server** aus.

Die Berechtigung **Aktivieren-Deaktivieren** wird einem Benutzer für die Funktion **Dienste** gewährt. Mit dieser Berechtigung wird auch die **View-Berechtigung** erteilt. Benutzer können die Dienste aktivieren oder deaktivieren, die an einen virtuellen Lastausgleichsserver gebunden sind. Außerdem kann Benutzer die Aktion **Jetzt abfragen** für Dienste ausführen. Um Dienste zu aktivieren oder zu deaktivieren, navigieren Sie zu **Infrastruktur > Netzwerkfunktionen > Load Balancing** und wählen Sie die Registerkarte **Dienste** aus.

> **Hinweis:**
>
> Wenn ein Benutzer über die Berechtigung **Aktivieren/Deaktivieren** verfügt, ist die Aktion zum Aktivieren oder Deaktivieren eines Dienstes auf der folgenden Seite eingeschränkt:
>
> a) Navigieren Sie zu **Infrastruktur > Netzwerkfunktionen**.
>
> b) Wählen Sie einen virtuellen Server aus, und klicken Sie auf **Konfigurieren**.
>
> c) Wählen Sie die Seite **Load Balancing Virtual Server Service Binding** .
> Auf dieser Seite wird eine Fehlermeldung angezeigt, wenn Sie **Aktivieren** oder **Deaktivieren**auswählen.

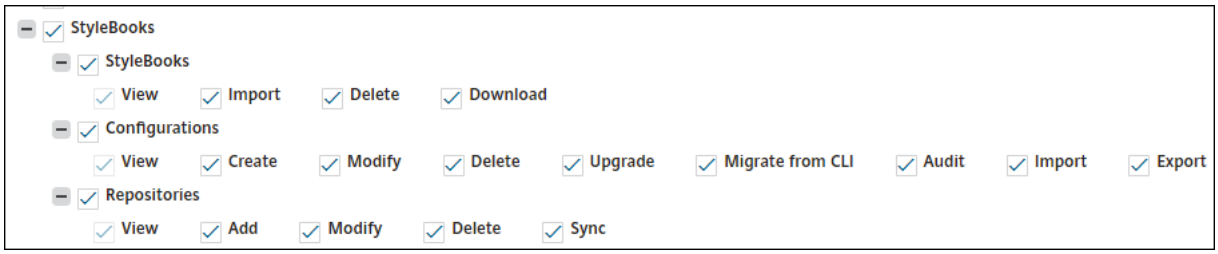
Die Berechtigung **Bearbeiten** wird einem Benutzer für die Funktion **Dienstgruppen** erteilt. Diese Berechtigung gewährt den vollen Zugriff, bei dem die Berechtigungen **Anzeigen** und **Enable-Disable** gewährt werden. Benutzer können die Dienstgruppen ändern, die an einen virtuellen Lastausgleichsserver gebunden sind. Um Dienstgruppen zu bearbeiten, navigieren Sie zu **Infrastruktur > Netzwerkfunktionen > Load Balancing** und wählen Sie die Registerkarte **Dienstgruppen** aus.

5. Klicken Sie auf **Erstellen**.

Erteilen von StyleBook-Berechtigungen für Benutzer

Sie können eine Zugriffsrichtlinie erstellen, um StyleBook-Berechtigungen wie Importieren, Löschen, Herunterladen und mehr zu erteilen.

> **Hinweis:**
>
> Die View-Berechtigung wird automatisch aktiviert, wenn Sie andere StyleBook-Berechtigungen gewähren.



Gruppen konfigurieren

February 5, 2024

In NetScaler ADM kann eine Gruppe sowohl auf Feature- als auch auf Ressourcenebene zugreifen. Beispielsweise kann eine Benutzergruppe nur auf ausgewählte NetScaler-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 NetScaler ADM dieselben Zugriffsrechte zugewiesen.

Sie können einen Benutzerzugriff in NetScaler ADM auf der einzelnen Ebene von Netzwerkfunktionsentitäten verwalten. Sie können dem Benutzer oder der Gruppe auf Entitätsebene dynamisch bestimmte Berechtigungen zuweisen.

NetScaler 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 NetScaler Gateway (VPN)
- **Services** - Lastenausgleich und GSLB-Dienste
- **Dienstgruppe** —Load Balancing und GSLB-Dienstgruppen
- **Server** —Load Balancing-Server

Erstellen einer Benutzergruppe

1. Navigieren Sie in NetScaler ADM zu **Einstellungen > Benutzer und Rollen Gruppen**.
2. Klicken Sie auf **Hinzufügen**.

   Die Seite **Systemgruppe erstellen** wird angezeigt.
3. Geben Sie im Feld **Gruppenname** den Namen der Gruppe ein. Die maximal zulässige Länge beträgt 64 Zeichen.
4. Geben Sie im Feld**Gruppenbeschreibung** eine Beschreibung Ihrer Gruppe ein. Eine gute Beschreibung der Gruppe hilft Ihnen, die Rolle und Funktion der Gruppe zu einem späteren Zeitpunkt besser zu verstehen.
5. Fügen Sie im Abschnitt **Rollen** eine oder mehrere Rollen zur Liste **Konfiguriert** hinzu oder verschieben Sie sie.

   > **Hinweis:**
   >
   > Unter der Liste **Verfügbar** können Sie auf **Neu** oder **Bearbeiten** klicken und Rollen erstellen oder ändern. Alternativ können Sie zu **Einstellungen > Benutzer und Rollen > Benutzer navigieren und Benutzer** erstellen oder ändern.

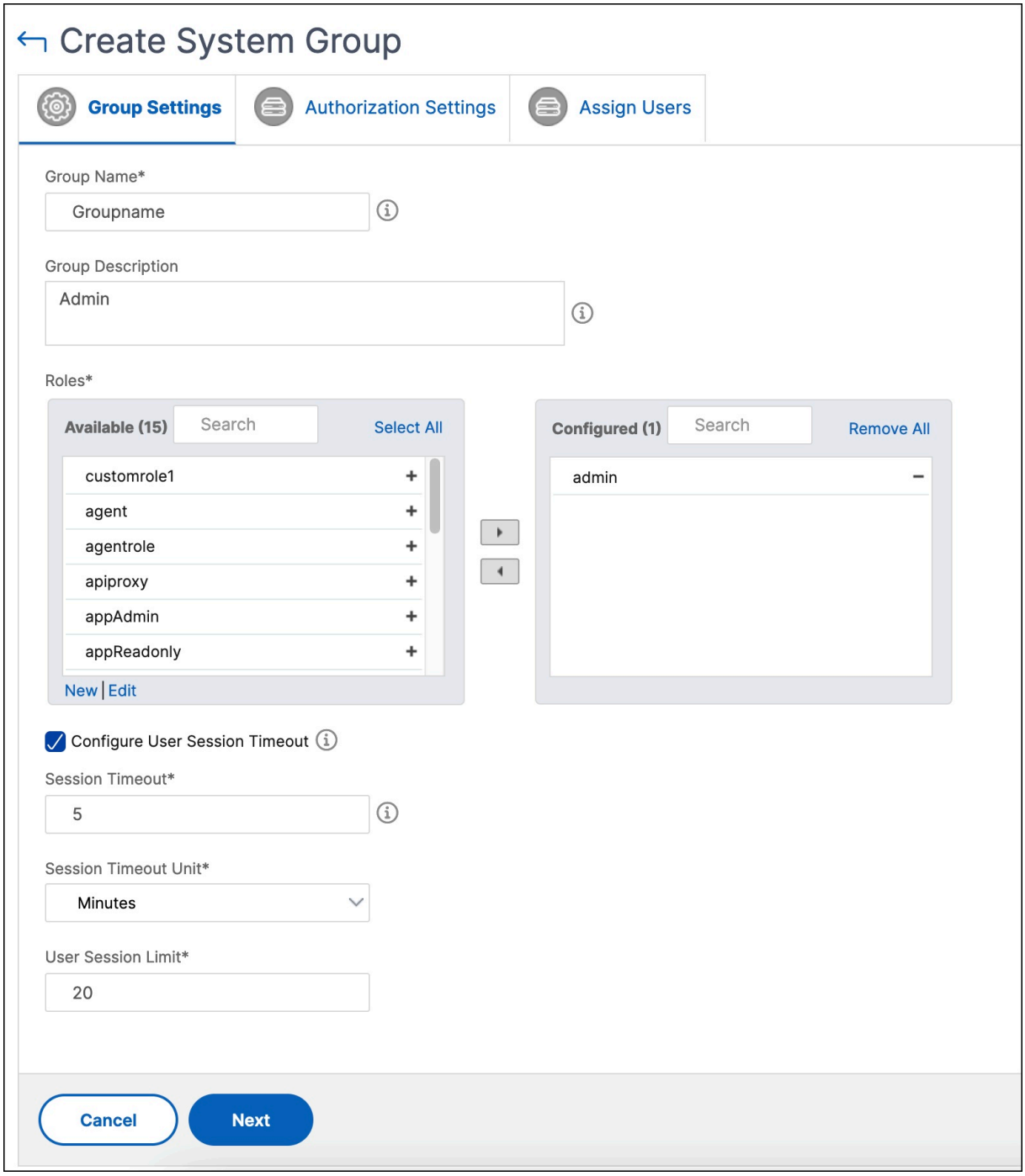
6. Wählen Sie **Benutzersitzungs-Timeout** konfigurieren, um den Zeitraum zu konfigurieren, in dem ein Benutzer aktiv bleiben soll.

   Wenn diese Option aktiviert ist, geben Sie die folgenden Parameter an:

   - **Sitzungs-Timeout**: Geben Sie den Zeitraum ein, für den eine Benutzersitzung aktiv bleiben muss. Der Standardwert ist 15.
   - **Sitzungs-Timeout-Einheit**: Wählen Sie die Timeout-Einheit in Minuten oder Stunden aus der Liste aus. Der Standardwert ist Minuten.

7. Geben Sie im Feld **Benutzersitzungslimit** die maximale Anzahl von Sitzungen ein, die pro Benutzer zulässig sind.

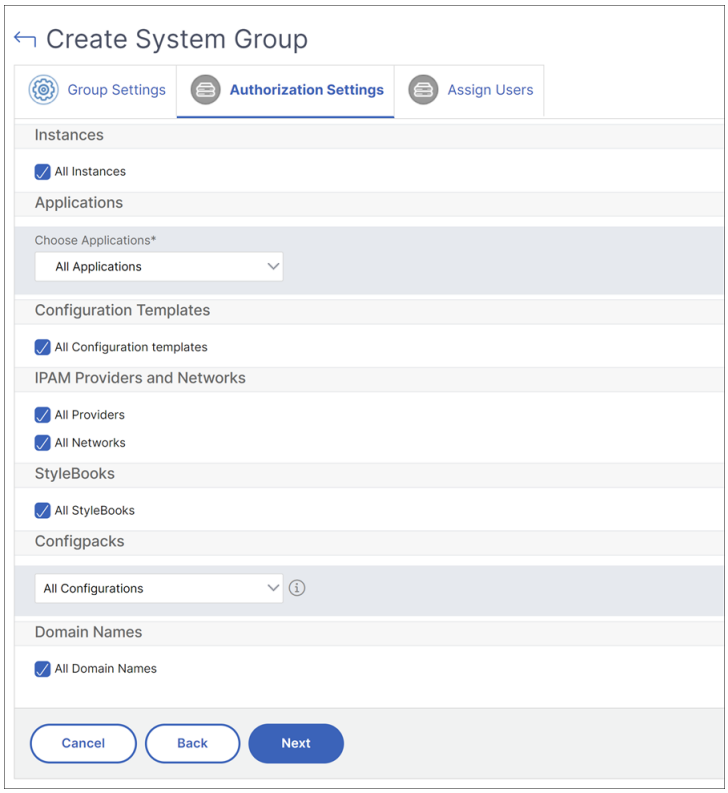
> **Hinweis:**
>
> Sie können bis zu 40 Benutzersitzungen konfigurieren. Standardmäßig sind Ihnen 20 Benutzersitzungen zugewiesen. Wenn Sie jedoch zu den Benutzergruppen Admin und Read-Only gehören, werden Ihnen standardmäßig 40 Benutzersitzungen zugewiesen, und dieser Wert kann nicht geändert werden.



1. Klicken Sie auf **Weiter**.Auf der Registerkarte **Autorisierungseinstellungen** können Sie Autorisierungseinstellungen für die folgenden Ressourcen angeben:

   - Autoscale-Gruppen
   - Instanzen
   - Anwendungen
   - Konfigurationsvorlagen

- StyleBooks
- Konfigurationspakete
- Domänennamen



Möglicherweise möchten Sie bestimmte Ressourcen aus den Kategorien auswählen, auf die Benutzer Zugriff haben können.

Autoscale-Gruppen:

Wenn Sie die spezifischen Autoscale-Gruppen auswählen möchten, die ein Benutzer anzeigen oder verwalten kann, gehen Sie wie folgt vor:

a) Deaktivieren Sie das Kontrollkästchen **Alle AutoScale-Gruppen** und klicken Sie auf **AutoScale-Gruppen hinzufügen**.

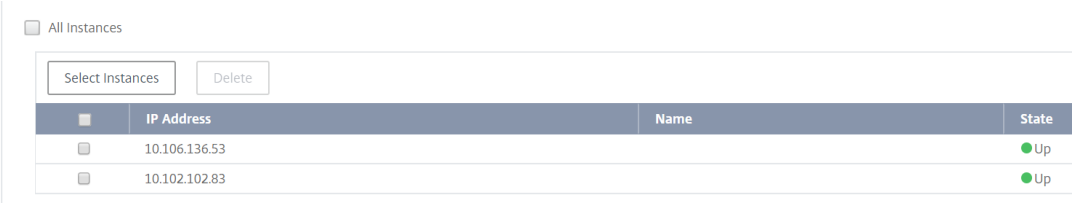
b) Wählen Sie die erforderlichen Autoscale-Gruppen aus der Liste aus, und klicken Sie auf **OK**.

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:

In der Liste **Anwendungen auswählen** können Sie einem Benutzer Zugriff auf die erforderlichen Anwendungen gewähren.

Sie können Anwendungen Zugriff gewähren, ohne deren Instanzen auszuwählen. Wenn Sie einem Benutzer Zugriff auf eine Anwendung gewähren, ist der Benutzer berechtigt, unabhängig von der Instanzauswahl nur auf diese Anwendung zuzugreifen.

Die folgenden Optionen sind verfügbar:

- **Alle Anwendungen:** Diese Option ist standardmäßig ausgewählt. Es fügt alle Anwendungen hinzu, die im NetScaler 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 hinzu, 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.
- **Individuellen Entitätstyp auswählen:** Mit dieser Option können Sie einen bestimmten Typ von Netzwerkfunktionsentität und entsprechende 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 **Auch auf gebundene Entitäten anwenden** autorisiert die Entitäten, die an den ausgewählten Entitätstyp gebunden sind. Wenn Sie beispielsweise eine Anwendung auswählen und die Option **Auch auf gebundene Entitäten anwenden**auswählen, autorisiert NetScaler ADM alle Entitäten, die an die ausgewählte Anwendung gebunden sind.

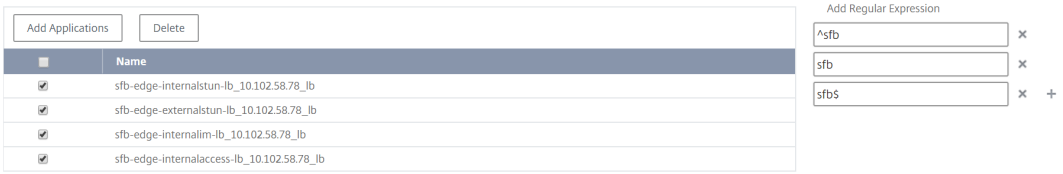
  > **Hinweis:**
  >
  > Um gebundene Entitäten zu autorisieren, wählen Sie nur einen Entitätstyp aus.

Sie können reguläre Ausdrücke verwenden, um die Netzwerkfunktionsentitäten zu suchen und hinzuzufügen, die die Regex-Kriterien für die Gruppen erfüllen. Der angegebene Regex-Ausdruck wird in NetScaler ADM beibehalten. Gehen Sie wie folgt vor, um einen regulären Ausdruck hinzuzufügen:

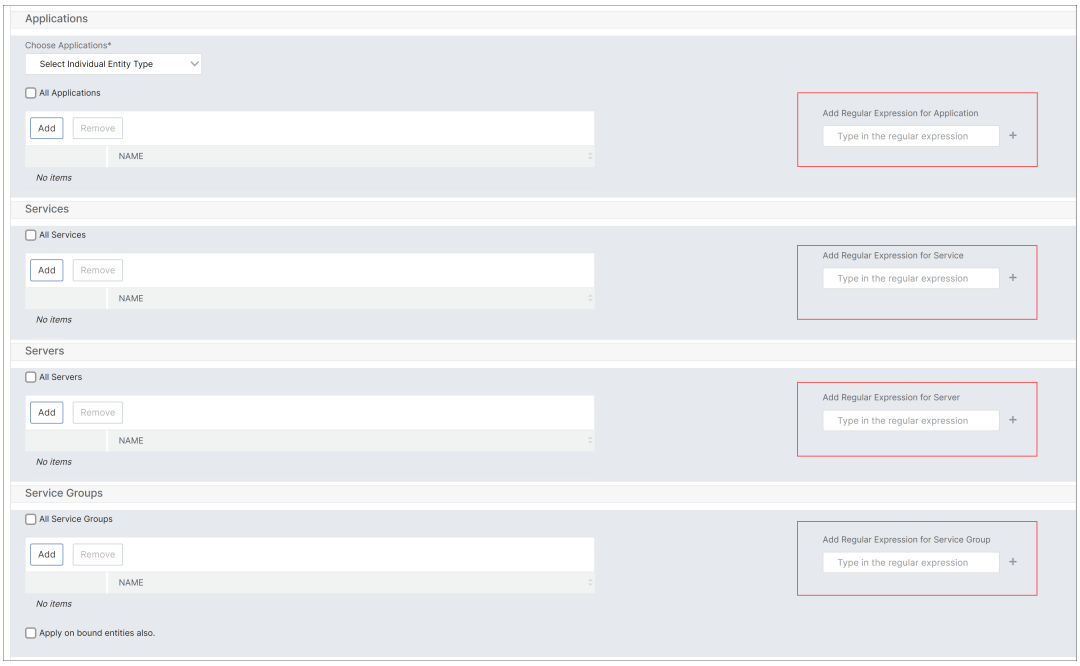
a) Klicken Sie auf **Regulären Ausdruck hinzufügen**.

b) Geben Sie den regulären Ausdruck im Textfeld an.

In der folgenden Abbildung wird erklärt, 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 entspricht nur dem Servernamen für den Entitätstyp **Server** und nicht der Server-IP-Adresse.

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 NetScaler ADM den Autorisierungsbereich auf die neuen Entitäten.

Vorlagen für die Konfiguration:

Wenn Sie die spezifische 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**.

StyleBooks:

Wenn Sie das spezifische StyleBook auswählen möchten, das ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

a) Deaktivieren Sie das Kontrollkästchen **Alle StyleBooks** und klicken Sie auf **StyleBook zur 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 Durchsuchen von StyleBooks verwenden möchten, wählen Sie den Bereich **Benutzerdefinierte Filter** aus. Eine Abfrage ist eine Zeichenfolge von Schlüssel-Wert-Paaren, wobei Schlüssel `name`, `namespace` und `version` sind.

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 sowohl die Operation `And` als auch `Or`.

Beispiel:

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

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

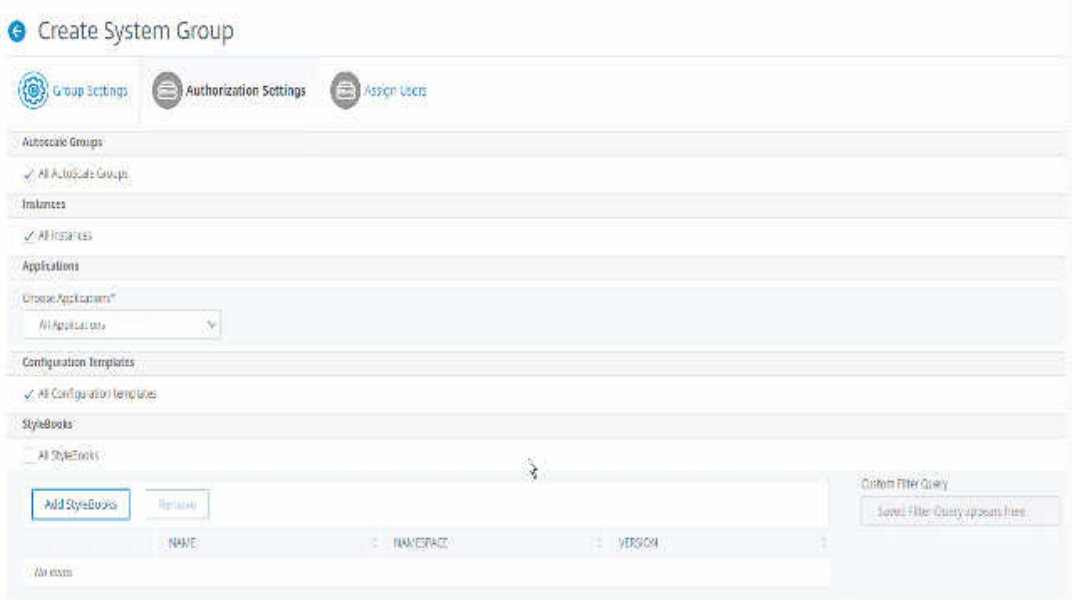
- StyleBook-Name ist entweder `lb-mon` oder `lb`.
- StyleBook Namespace ist `com.citrix.adc.stylebooks`.
- StyleBook-Version ist `1.0`.

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 "**Benutzerdefinierte Filter**"angezeigt. Basierend auf der gespeicherten Abfrage bietet das ADM dem Benutzer Zugriff 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 **Config Packs** eine der folgenden Optionen aus:

- **Alle Konfigurationen**: Diese Option ist standardmäßig ausgewählt. Es ermöglicht Benutzern, alle Konfigurationen zu verwalten, die sich in ADM befinden.
- **Alle Konfigurationen der ausgewählten StyleBooks**: Diese Option fügt alle Konfigurationspakete des ausgewählten StyleBook hinzu.
- **Spezifische Konfigurationen**: Mit dieser Option können Sie spezifische Konfigurationen für jedes StyleBook hinzufügen.

- **Alle von der Benutzergruppe erstellten Konfigurationen**: Mit dieser Option können Benutzer nur auf Konfigurationen zugreifen, die von Benutzern derselben Gruppe erstellt wurden.

  Sie können die entsprechenden Config Packs auswählen, wenn Sie Gruppen erstellen und dieser Gruppe Benutzer zuweisen.

Domänennamen:

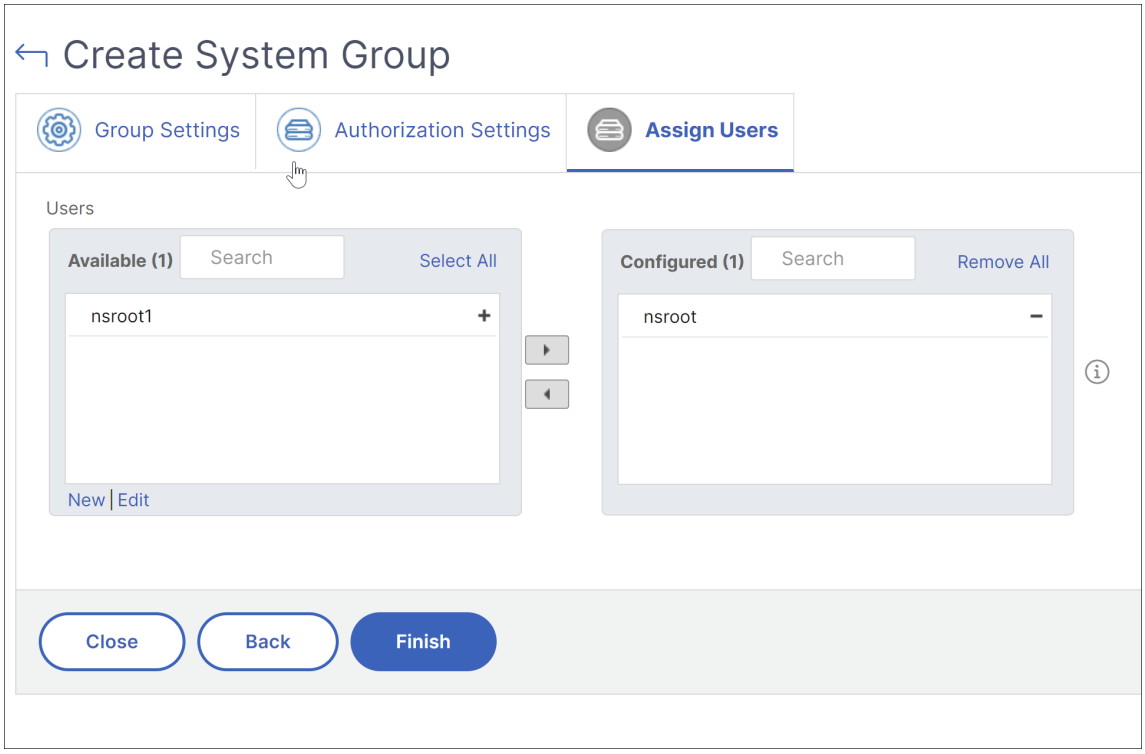
Wenn Sie den spezifischen Domänennamen auswählen möchten, den ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

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**.

2. Klicken Sie auf **Gruppe erstellen**.
3. 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 Benutzer auch hinzufügen, indem Sie auf **Neu**klicken.



4. Klicken Sie auf **Fertig stellen**.

Verwaltung des Benutzerzugriffs über mehrere Netzwerkfunktionsentitäten

Als Administrator können Sie den Benutzerzugriff auf der einzelnen Ebene der Netzwerkfunktionsentitäten in NetScaler ADM verwalten. Und Sie können dem Benutzer oder einer Gruppe auf Entitätsebene dynamisch bestimmte Berechtigungen zuweisen, indem Sie den Filter für reguläre Ausdrücke verwenden.

In diesem Dokument wird beschrieben, wie die Benutzerautorisierung auf Entitätsebene definiert wird.

Bevor Sie beginnen, erstellen Sie eine Gruppe. Weitere Informationen finden Sie unter Konfigurieren von Gruppen in NetScaler ADM .

Verwendungsszenario:

Stellen Sie sich ein Szenario vor, in dem eine oder mehrere Anwendungen (virtuelle Server) auf demselben Server gehostet werden. Ein Superadministrator (George) möchte Steve (einem Anwendungsadministrator) nur Zugriff auf App1 und nicht auf den Hosting-Server gewähren.

Die folgende Tabelle zeigt diese Umgebung, in der Server-A die Anwendungen App-1 und App-2 hostet.

Host-Server	Anwendung (virtueller Server)	Service	Service-Gruppe
Server A	App 1	App-service-1	App-service-group-1
Server A	App 2	App-service-2	App-service-group-2

> **Hinweis**
>
> NetScaler ADM behandelt virtuelle Server, Dienste, Dienstgruppen und Server als Netzwerkfunktionsentitäten. Der virtuelle Server vom Entitätstyp wird als Anwendung bezeichnet.

Um Netzwerkfunktionsentitäten Benutzerberechtigungen zuzuweisen, definiert George die Benutzerautorisierung wie folgt:

1. Navigieren Sie zu **Konto > Benutzerverwaltung > Gruppen** und fügen Sie eine Gruppe hinzu.
2. Wählen Sie auf der Registerkarte **Autorisierungseinstellungen** die Option Anwendungen auswählen aus.
3. Wählen Sie **Select Individual Entity Type**.
4. Wählen Sie den Entitätstyp **Alle Anwendungen** aus und fügen Sie die App-1-Entität aus der verfügbaren Liste hinzu.
5. Klicken Sie auf **Gruppe erstellen**.

6. Wählen Sie unter **Benutzer zuweisen** die Benutzer aus, die die Berechtigung benötigen. Für dieses Szenario wählt George Steves Benutzerprofil aus.
7. Klicken Sie auf **Fertig stellen**.

Mit dieser Autorisierungseinstellung kann Steve nur App-1 und keine anderen Netzwerkfunktionsentitäten verwalten.

> **Hinweis:**
>
> Stellen Sie sicher, dass die Option **Auch auf gebundene Entitäten anwenden** deaktiviert ist. Andernfalls gewährt NetScaler ADM Zugriff auf alle Netzwerkfunktionsentitäten, die an App-1 gebunden sind. Dadurch wird auch Zugriff auf den Hosting-Server gewährt.

Ein Superadministrator kann die regulären Ausdrücke (Regex) für jeden Entitätstyp angeben. Der reguläre Ausdruck wird im System gespeichert, um den Umfang der Benutzerautorisierung zu aktualisieren. Wenn neue Entitäten dem regulären Ausdruck ihres Entitätstyps entsprechen, kann NetScaler ADM Benutzern dynamisch Zugriff auf die spezifischen Netzwerkfunktionsentitäten gewähren.

Um Benutzerberechtigungen dynamisch zu gewähren, kann der Superadministrator reguläre Ausdrücke auf der Registerkarte **Autorisierungseinstellungen** hinzufügen.

In diesem Szenario fügt George App* als regulären Ausdruck für den Entitätstyp Applications hinzu und die Anwendungen, die den Regex-Kriterien entsprechen, werden in der Liste angezeigt. Mit dieser Autorisierungseinstellung kann Steve auf alle Anwendungen zugreifen, die dem Regex App* entsprechen. Sein Zugriff ist jedoch nur auf die Anwendungen beschränkt, nicht auf den gehosteten Server.

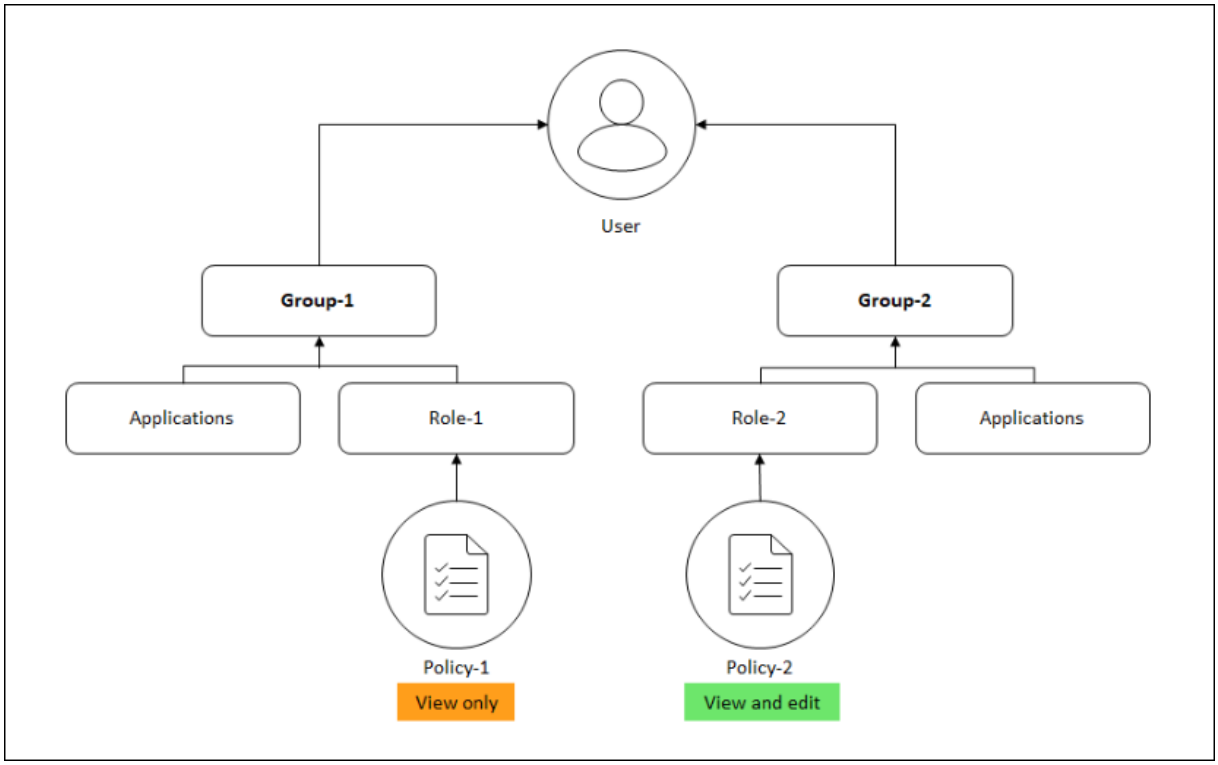
Wie sich der Benutzerzugriff basierend auf dem Berechtigungsumfang ändert

Wenn ein Administrator einen Benutzer zu einer Gruppe hinzufügt, die über unterschiedliche Zugriffsrichtlinieneinstellungen verfügt, wird der Benutzer mehreren Autorisierungsbereichen und Zugriffsrichtlinien zugeordnet.

In diesem Fall gewährt das ADM dem Benutzer je nach dem spezifischen Autorisierungsumfang Zugriff auf Anwendungen.

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

- **Policy-1** —Nur Berechtigungen 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 den Autorisierungsbereich der Gruppe 1 fällt.

Zuordnung von RBAC beim Upgrade von NetScaler ADM von 12.0 auf spätere Releases

Wenn Sie NetScaler ADM von 12.0 auf 13.1 aktualisieren, werden beim Erstellen von Gruppen keine Optionen zum Bereitstellen von “Lese-“oder “Lese”-Berechtigungen angezeigt. Diese Berechtigungen werden durch „Rollen und Zugriffsrichtlinien“ersetzt, die Ihnen mehr Flexibilität bieten, um den Benutzern rollenbasierte Berechtigungen zu erteilen. Die folgende Tabelle zeigt, wie die Berechtigungen in Version 12.0 Version 13.1 zugeordnet werden:

12.0	Nur Anwendungen zulassen	13.1
Admin Lese-/Schreibzugriff	False	`admin`
Admin Lese-/Schreibzugriff	True	`appAdmin`
Admin schreibgeschützt	False	`readonly`
Admin schreibgeschützt	True	`appReadonly`

Rollen konfigurieren

February 5, 2024

In NetScaler Application Delivery Management (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 Sie können 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 Erlaubnis zum Hinzufügen von NetScaler-Instanzen in NetScaler ADM gewähren, und die andere Richtlinie kann die Berechtigung zum Erstellen und Bereitstellen von StyleBooks und zur Konfiguration von NetScaler-Instanzen gewähren.

Wenn mehrere Richtlinien Bearbeitungs- und Leseberechtigungen für ein einzelnes Feature definieren, haben die Bearbeitungsberechtigungen Vorrang.

NetScaler ADM bietet vier vordefinierte Rollen:

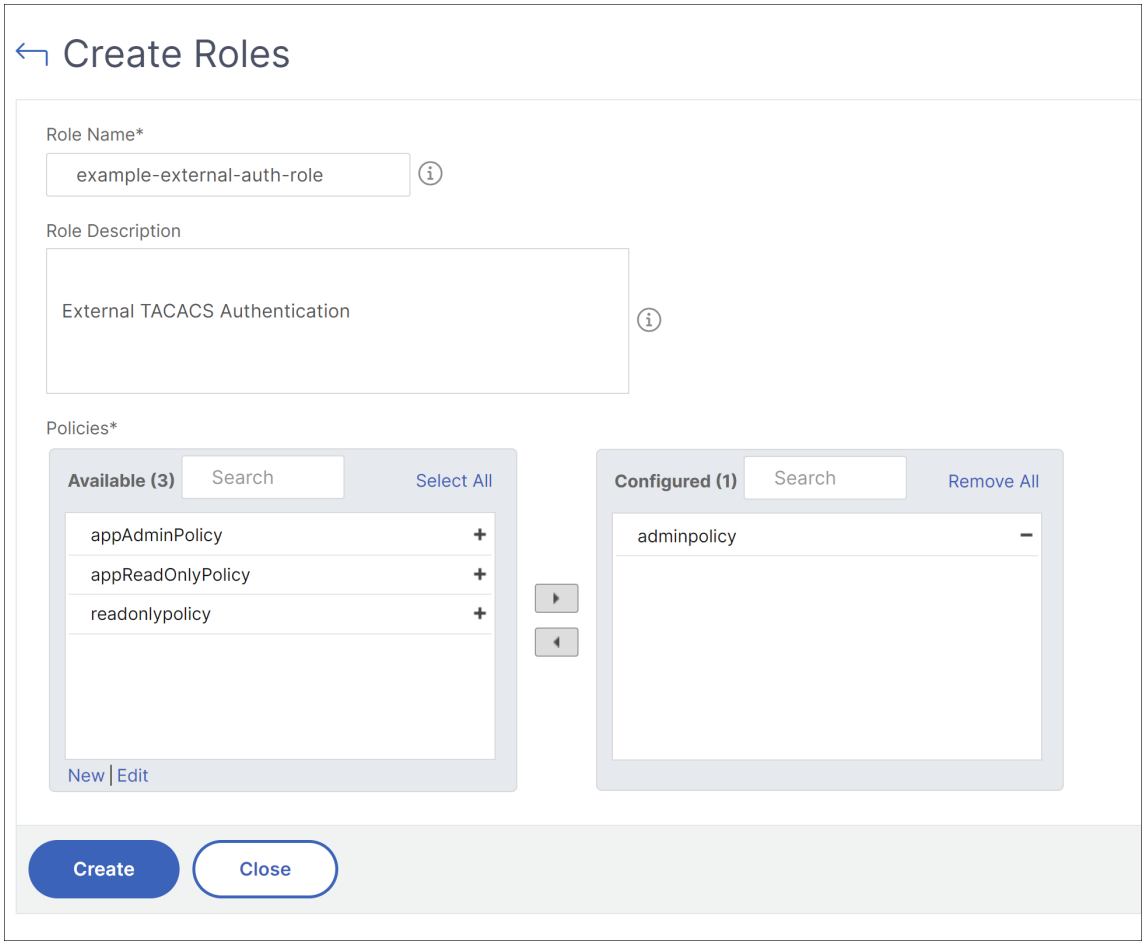
- **Administrator**. Hat Zugriff auf alle NetScaler ADM-Funktionen. (Diese Rolle ist an die Administratorrichtlinie gebunden.)
- **schreibgeschützt**. Schreibgeschützter Zugriff. (Diese Rolle ist an readonlypolicy gebunden.)
- **appAdmin**. Hat administrativen Zugriff nur auf die Anwendungsfunktionen in NetScaler ADM. (Diese Rolle ist an appAdminPolicy gebunden).
- **appReadonly**. Hat nur Lesezugriff auf die Anwendungsfunktionen. (Diese Rolle ist an appReadOnlyPolicy gebunden.)

> **Hinweis:**
>
> Die vordefinierten Rollen können nicht bearbeitet werden.

Sie können auch Ihre eigenen (benutzerdefinierten) Rollen erstellen.

So erstellen Sie Rollen und weisen ihnen Richtlinien zu:

1. Navigieren Sie in NetScaler ADM zu **Einstellungen > Benutzer**und Rollen.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie 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 oder verschieben Sie sie in die Liste **Konfiguriert**.



5. Klicken Sie auf **Erstellen**.

Benutzer konfigurieren

February 5, 2024

Standardmäßig hat NetScaler Application Delivery Management (ADM) einen Benutzer:

nsroot —Der Root-Benutzer (nsroot) hat volle Administratorrechte auf der Appliance. Der nsroot-Benutzer ist der Superadministrator von NetScaler ADM.

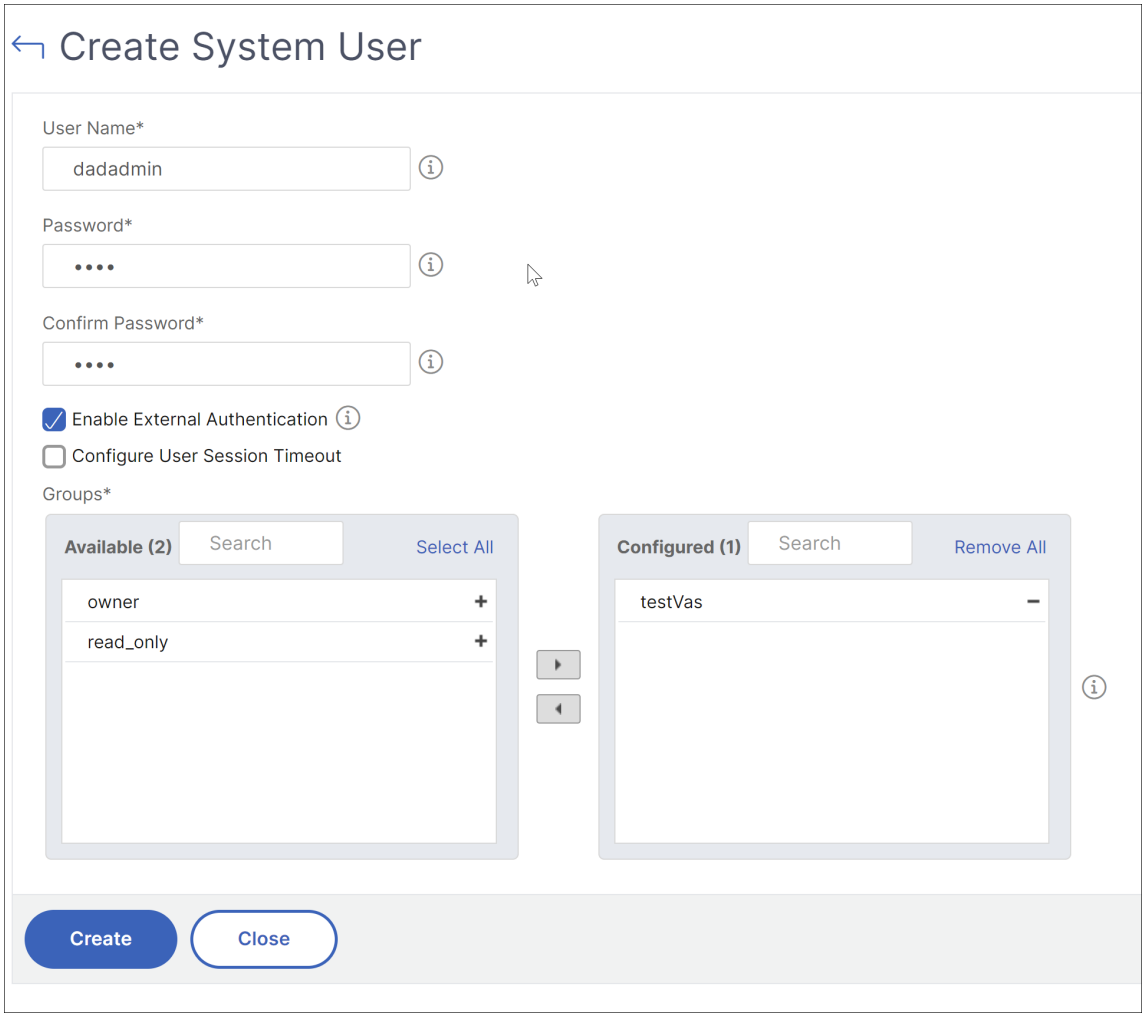
Sie können zusätzliche Benutzer erstellen, indem Sie Konten für sie konfigurieren. Wenn Sie neue Benutzer zu NetScaler ADM hinzufügen, können Sie deren Berechtigungen definieren, indem Sie die entsprechenden Gruppen, Rollen und Richtlinien zuweisen.

Sie können einen Benutzer einer Gruppe zuweisen und die Gruppe an Rollen binden. Sie können die Beziehung eins zu eins, eins zu viele oder viele zu viele zwischen Benutzern, Gruppen, Rollen und Zugriffsrichtlinien definieren. Ein Benutzer kann mehreren Gruppen zugewiesen werden. Eine Gruppe

kann mehrere Rollen haben, und mehrere Gruppen können identische Rollen haben.

So konfigurieren Sie Benutzer in NetScaler ADM:

1. Navigieren Sie in NetScaler ADM zu **Einstellungen > Benutzer**und Rollen.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie folgende Details ein:
   a) **Nutzername**. Name des Benutzers
   b) **Kennwort**. Kennwort, mit dem sich der Benutzer bei NetScaler ADM anmeldet
4. Wählen Sie optional **Externe Authentifizierung aktivieren**aus, damit der Benutzer über einen externen Authentifizierungsserver authentifiziert werden kann.
5. Wenn Sie Gruppen erstellt haben und den Benutzer einer Gruppe zuweisen möchten, verschieben Sie im Abschnitt **Gruppen** eine oder mehrere Gruppen aus der Liste **Verfügbar** in die Liste **Konfiguriert** .



6. Klicken Sie auf **Erstellen**.

Umsetzbare Aufgaben und Empfehlungen

February 5, 2024

> **Hinweis:**
>
> - Die Registerkarte „ **Aufgaben** “wurde in **Empfehlungen**umbenannt. Unter **Empfehlungen**können Sie die vorhandenen Aufgaben weiterhin überprüfen und auf **Anleitung klicken,** um die Aufgabe abzuschließen.
> - Die Registerkarte **Archiv** ist nicht mehr verfügbar. Stattdessen können Sie eine Empfehlung aus der Liste **verwerfen** .

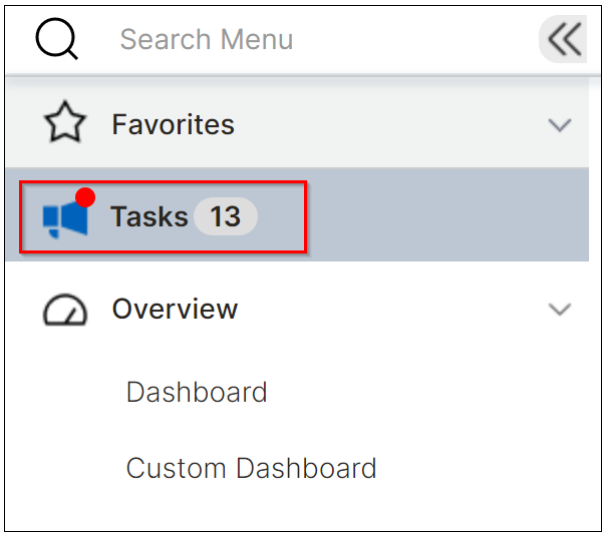
Möglicherweise haben Sie Hunderte von NetScaler-Instanzen erkannt und mehrere virtuelle Server (Anwendungen) von jeder Instanz aus konfiguriert. Als Administrator müssen Sie sicherstellen, dass alle NetScaler-Instanzen und Ihre Anwendungen effizient verwaltet werden, um Erkenntnisse für eine bessere Priorisierung und Fehlerbehebung zu erhalten.

Wenn Sie Ihre Infrastruktur weiter ausbauen, müssen Sie sich möglicherweise auch auf die kritischen Probleme konzentrieren, die sich auf Ihre Instanzen und Anwendungen auswirken und Ihre sofortige Aufmerksamkeit erfordern. Sie müssen auch sicherstellen, dass Ihre NetScaler ADM-Bereitstellung effizient, sicher und konform ist. Basierend auf Ihrer aktuellen Auslastung und Ihrem Abonnement können Sie mit der **Aufgabenfunktion** in NetScaler ADM sowohl umsetzbare **Aufgaben**, die Sie sofort ergreifen müssen, als auch **Empfehlungen anzeigen, um eine effiziente Bereitstellung sicherzustellen** .

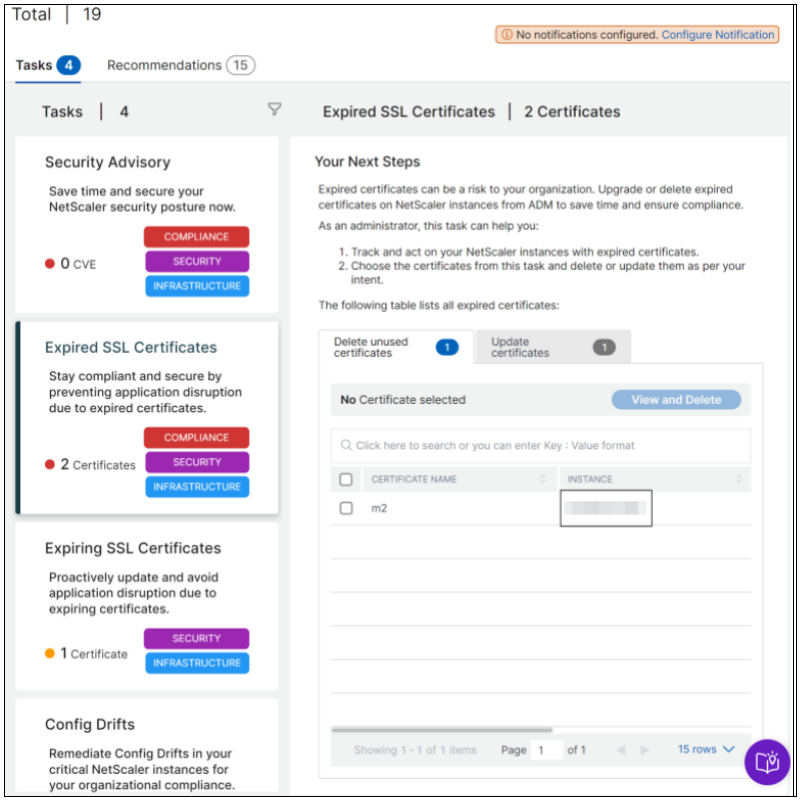
Als Administrator können Sie mithilfe dieser umsetzbaren **Aufgaben** und **Empfehlungen**:

- Verschaffen Sie sich einen sofortigen Überblick über alle Beobachtungen oder Probleme, die Ihr sofortiges Handeln erfordern.
- Konfigurieren Sie Benachrichtigungen, um Benachrichtigungen zu erhalten, wenn NetScaler ADM Aufgaben erkennt, und proaktiv Maßnahmen ergreift.
- Erzielen Sie eine effiziente Bereitstellung von NetScaler ADM- und NetScaler-Instanzen.
- Reduzieren Sie den entscheidenden Zeit- und Arbeitsaufwand bei der Identifizierung der kritischen Probleme.
- Stellen Sie sicher, dass Sie alle Funktionen von NetScaler ADM nutzen, aktivieren Sie die Produkterkennung und die vom Produkt empfohlenen Funktionen für eine effiziente Verwaltung der Bereitstellung.

Klicken Sie in der NetScaler ADM GUI auf **Aufgaben**, um sowohl **Aufgaben** als auch **Empfehlungen** anzuzeigen.

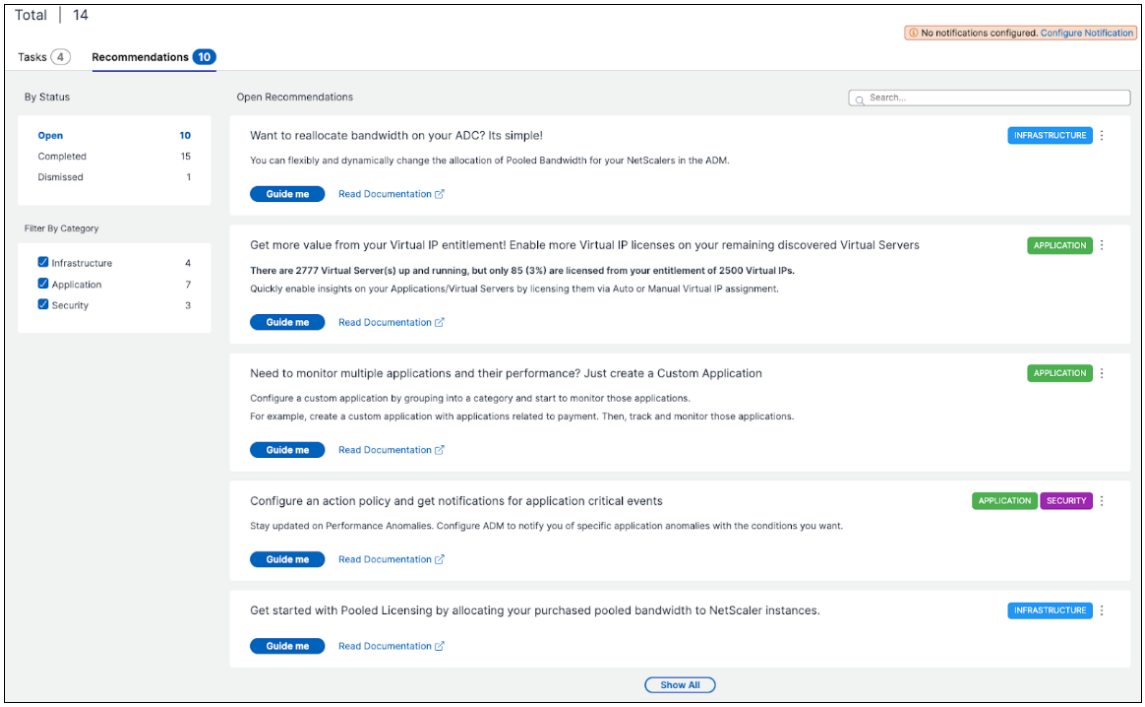


- **Aufgaben** —Ermöglicht es Ihnen, eine Liste von Aufgaben anzuzeigen, die Ihre sofortige Aufmerksamkeit und Aktion erfordern. Wenn Sie Ihre Infrastruktur erweitern, können einige kritische Probleme unbemerkt bleiben und zu Sicherheitslücken führen. NetScaler-Instanzen mit CVEs erfordern beispielsweise sofortige Aufmerksamkeit, und Sie müssen sofort Maßnahmen ergreifen, um sicherzustellen, dass die Instanzen im empfohlenen Build und in der empfohlenen Version ausgeführt werden. In **Aufgaben**können Sie diese Erkenntnisse sofort abrufen. Basierend auf Ihrer aktuellen Auslastung können Sie insgesamt 4 Aufgaben anzeigen. Die Aufgaben werden basierend auf dem Schweregrad (Kritisch und Mittel) angezeigt.



- **Empfehlungen** —Bietet bestimmte Empfehlungen, die auf Ihrer aktuellen Auslastung basieren, um Ihre NetScaler ADM-Bereitstellung zu verbessern. Sie können die Option „ **Mich führen** “verwenden, um jede Empfehlung auszufüllen. Jede Empfehlung, die Sie mithilfe der Option „ **Guide Me** “ausfüllen, wird in den Status Abgeschlossen verschoben. Sie können auch alle Empfehlungen verwerfen und sie werden in die Kategorie Abgelehnt **verschoben** . Um Ihre abgelehnten Empfehlungen anzuzeigen, verwenden Sie den Filter **Nach Status** und wählen Sie Abgelehnt **aus**, um diese abgelehnten Empfehlungen anzuzeigen.

  Sie können auch den **Filter Nach Kategorie** verwenden, um bestimmte Empfehlungen basierend auf den Kategorien (Infrastruktur, Anwendung und Sicherheit) zu filtern. Alternativ können Sie auch die **Suchleiste** verwenden und die ersten Zeichen eingeben, um zu der Aufgabe zu gelangen.



Aufgaben

Unter **Aufgaben**können Sie je nach Ihrer aktuellen ADM-Bereitstellung die folgenden 4 Aufgaben anzeigen.

- **Abgelaufene SSL-Zertifikate** —Stellt Informationen zu den abgelaufenen SSL-Zertifikaten bereit, die in Ihrem NetScaler ADM installiert sind. Wählen Sie diese Aufgabe aus, um die folgenden Tabs anzuzeigen:

  - **Unbenutzte Zertifikate löschen**: Zeigt die Zertifikate an, die in keiner NetScaler-Instanz verwendet werden. Um die Aufgabe abzuschließen, überprüfen Sie die nicht verwendeten Zertifikate, wählen Sie das Zertifikat aus und klicken Sie auf **Anzeigen und Löschen**.

    Empfohlene Maßnahme: Sie werden zu **Infrastruktur > SSL-Dashboard > SSL-Zertifikate** —**Abgelaufen**weitergeleitet. Um ein Zertifikat zu löschen, klicken Sie auf **Löschen**. Wenn Sie das Zertifikat aktualisieren möchten, wählen Sie das Zertifikat aus und klicken Sie auf **Aktualisieren**. Weitere Informationen finden Sie unter So aktualisieren Sie ein installiertes Zertifikat.

  - **Zertifikate aktualisieren**: Zeigt die Zertifikate an, die bereits abgelaufen sind. Um die Aufgabe abzuschließen, überprüfen Sie die Zertifikate, wählen Sie das Zertifikat aus und klicken Sie auf **Anzeigen und aktualisieren**.

    Empfohlene Maßnahme: Sie werden zu **Infrastruktur > SSL-Dashboard > SSL-Zertifikate** —**Abgelaufen**weitergeleitet. Wählen Sie das Zertifikat aus und klicken Sie auf

Aktualisieren oder **Löschen**. Weitere Informationen finden Sie unter So aktualisieren Sie ein installiertes Zertifikat.

- **Ablaufende SSL-Zertifikate** —Stellt Informationen zu den SSL-Zertifikaten bereit, die bald ablaufen.

  Empfohlene Maßnahme: Wählen Sie diese Aufgabe aus, um die Tabs anzuzeigen, die auf der Gesamtzahl der Tage vor dem Ablaufdatum basieren. Um die Aufgabe abzuschließen, wählen Sie das Zertifikat auf der Registerkarte aus und klicken Sie auf **Anzeigen und aktualisieren**. Sie werden zur entsprechenden Seite unter **Infrastruktur > SSL-Dashboard**weitergeleitet. Wählen Sie das Zertifikat aus und klicken Sie auf **Aktualisieren**. Weitere Informationen finden Sie unter So aktualisieren Sie ein installiertes Zertifikat.

- **Config Drifts** —Stellt Informationen über die Konfigurationsabweichungen (gespeichert im Vergleich zum laufenden Diff und Template im Vergleich zum laufenden Diff) in den NetScaler-Instanzen bereit. Wählen Sie diese Aufgabe aus, um die folgenden Tabs anzuzeigen:

  - **Instanzen mit ungespeicherter Konfiguration**: Sie können Instanzen mit der ungespeicherten Konfiguration anzeigen. Um die Aufgabe abzuschließen, wählen Sie die Instanz aus und klicken Sie auf **Konfiguration anzeigen und speichern**.

    Empfohlene Maßnahme: Sie werden zu **Infrastruktur > Konfiguration > Konfigurationsprüfung > Auditberichte** weitergeleitet und können die Instanzen mit ungespeicherten Konfigurationen anzeigen. Klicken Sie auf **Konfiguration speichern**, um diese Aufgabe abzuschließen. Weitere Informationen finden Sie in der Dokumentation.

  - **Instanzen mit Abweichungen von der Vorlage**: Sie können Instanzen anzeigen, die Template-Abweichungen aufweisen. Um die Aufgabe abzuschließen, wählen Sie die Instanz aus, klicken Sie auf **Richtige Befehle anzeigen und ausführen**.

    Empfohlene Maßnahme: Sie werden zu **Infrastruktur > Konfiguration > Konfigurationsprüfung > Auditberichte** weitergeleitet und können die Instanzen anzeigen, die Vorlagenabweichungen aufweisen. Folgen Sie der Dokumentation, um die Aufgabe abzuschließen.

- **Sicherheitsempfehlung** —Stellt Informationen zu den CVEs bereit, die sich auf Ihre NetScaler-Instanzen auswirken. Wählen Sie diese Aufgabe aus, um die folgenden Tabs anzuzeigen:

  - Entdeckte**CVEs: Zeigt die erkannten**CVEs und die NetScaler-Instanzen an, die sich auf die CVEs auswirken. Um diese Aufgabe abzuschließen, wählen Sie eine CVE aus und klicken Sie auf **Anzeigen und korrigieren.**

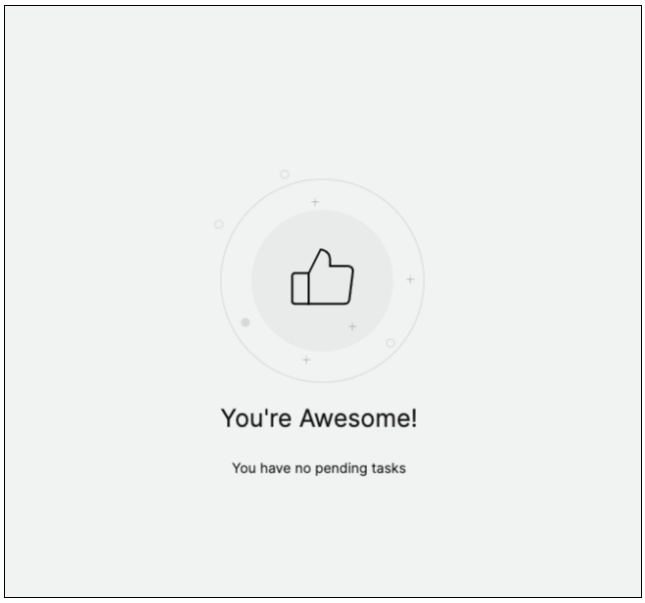
    Empfohlene Maßnahme: Sie werden unter **Infrastruktur > Instanzempfehlung >**Sicherheitsempfehlung**zur Seite mit Sicherheitshinweisen**weitergeleitet. Folgen Sie der Dokumentation, um die Aufgabe abzuschließen.

- **Betroffene Instanzen**: Zeigt die NetScaler-Instanzen an, die von CVEs betroffen sind. Um die Aufgabe abzuschließen, wählen Sie die Instanz aus und klicken Sie auf **Anzeigen und korrigieren.**

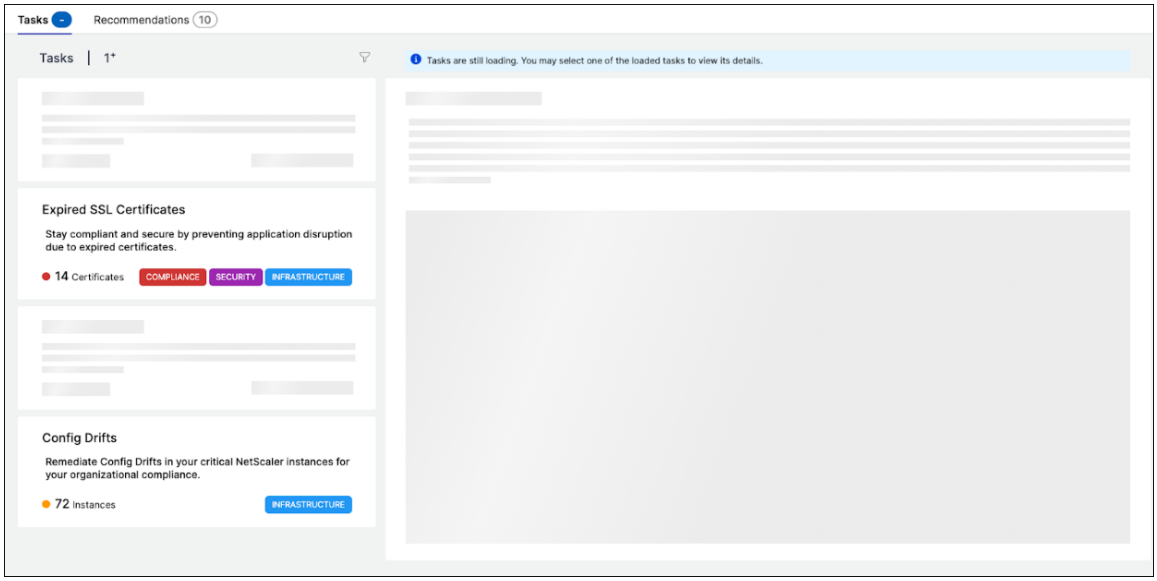
  Empfohlene Maßnahme: Sie werden unter **Infrastruktur > Instanzempfehlung >**Sicherheitsempfehlung**zur Seite mit Sicherheitshinweisen**weitergeleitet. Folgen Sie der Dokumentation, um die Aufgabe abzuschließen.

Hinweis:

- Sie können die folgende Seite anzeigen, wenn Ihr NetScaler ADM keine ausstehenden Aufgaben hat:



- In einigen Szenarien finden die Prüfungen auf allen Instanzen statt, und es kann zusätzliche Zeit dauern, bis alle Aufgaben geladen sind.



Empfehlungen

In der folgenden Tabelle werden die Empfehlungen beschrieben, die Sie in der NetScaler ADM GUI anzeigen können:

> **Hinweis**
>
> Für gepoolte Lizenzierungen erhalten Sie Empfehlungen, die auf Ihren bestehenden gepoolten Lizenzberechtigungen basieren.

Name der Empfehlung	Wann ist die Aufgabe in der GUI sichtbar?
ADC hinzufügen	Nach dem Onboarding in NetScaler ADM und wenn keine ADC-Instanz erkannt wird.
Fügen Sie einen externen ADM-Agent hinzu, um die maximalen Funktionen von NetScaler ADM zu nutzen	Wenn ein externer Agent nicht konfiguriert ist. Sie können mit einem integrierten Agent beginnen. Für die Nutzung aller Funktionen wie Analysen, gepoolte Lizenzierung usw. ist jedoch ein externer Agent erforderlich.
Registrieren Sie einen ADC von einem integrierten Agent für einen externen Agent	Nach dem Onboarding in NetScaler ADM mithilfe des Service Connect-Workflows werden die ADC-Instanzen mithilfe des integrierten Agent integriert. Sie können diese ADC-Instanzen bei einem externen Agent registrieren, um alle Funktionen wie Analysen, gepoolte Lizenzierung usw. zu nutzen.

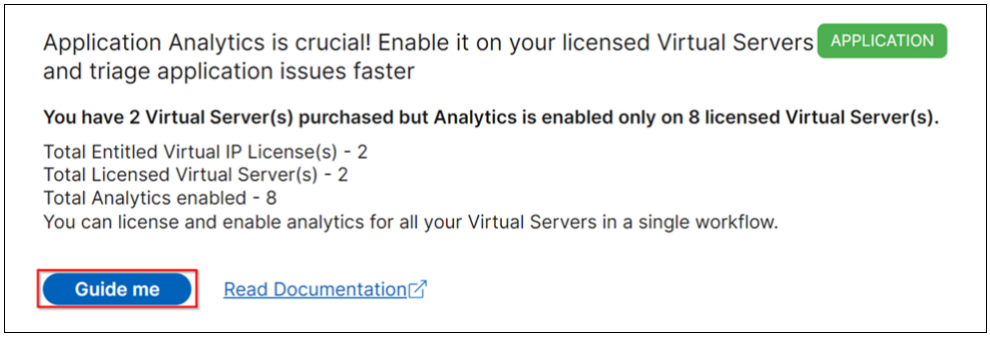
Name der Empfehlung	Wann ist die Aufgabe in der GUI sichtbar?
Anwendungsanalytik ist entscheidend! Aktivieren Sie es auf Ihren lizenzierten virtuellen Servern und beheben Sie Anwendungsprobleme schneller.	Wenn Sie über mehrere lizenzierte virtuelle Server verfügen, für die Analytik jedoch nicht aktiviert ist.
Möchten Sie die Bandbreite auf Ihrem ADC neu zuweisen? Es ist ganz einfach!	Wenn die gepoolten Lizenzen in der ADC-GUI zugewiesen werden und diese ADC-Instanzen in NetScaler ADM erkannt werden, können Sie die Neuzuweisung mit NetScaler ADM vornehmen.
Holen Sie mehr aus Ihrem virtuellen IP-Anspruch heraus! Aktivieren Sie mehr virtuelle IP-Lizenzen auf Ihren verbleibenden erkannten virtuellen Servern	Wenn Sie über die erforderlichen Lizenzen verfügen, aber nicht für alle virtuellen Server lizenziert sind.
Ermöglichen Sie den granularen rollenbasierten Zugriff für Ihre wichtigsten Unternehmensbenutzer	Wenn die rollenbasierte Zugriffskontrolle (RBAC) in NetScaler ADM noch nicht konfiguriert ist.
Konfigurieren Sie Regeln und verpassen Sie keine kritischen Ereignisse auf Ihren ADC-Instanzen	Wenn eine benutzerdefinierte Ereignisregel noch nicht konfiguriert ist.
Müssen Sie mehrere Anwendungen und deren Leistung überwachen? Erstellen Sie einfach eine benutzerdefinierte Anwendung	Wenn die benutzerdefinierte App noch nicht konfiguriert ist.
Informieren Sie Ihre Anwendungen und verpassen Sie keine kritischen Ereignisse	Wenn die Aktionsrichtlinie nicht für die Abweichung des App-Scores, die Serververarbeitungszeit, die Client-Netzwerklatenz, die Servernetzwerklatenz oder die Antwortzeit konfiguriert ist.
Vermeiden Sie Anwendungsausfälle und verpassen Sie niemals ablaufende SSL-Zertifikate in einer Anwendung	Wenn keine Warnungen oder Benachrichtigungen für die ablaufenden SSL-Zertifikate konfiguriert sind.
Sicherheitshinweis —Halten Sie Ihre ADCs mit CVEs und Gegenmaßnahmen auf dem neuesten Stand	Wenn die ADC-Instanzen Auswirkungen auf CVE haben.
Konfigurieren Sie eine Unternehmensrichtlinie und achten Sie auf Abweichungen	Wenn die SSL-Unternehmenseinstellungen nicht geändert wurden oder immer noch standardmäßig sind.
Aufgaben manuell wiederholen? Erstellen Sie Konfigurationsjobs und wenden Sie sie auf mehrere ADCs an	Wenn die Aufgabe **Config Job** noch nicht konfiguriert ist.

Name der Empfehlung	Wann ist die Aufgabe in der GUI sichtbar?
Verwalten und überwachen Sie den Instanz-Score, indem Sie die gewünschten Indikatoren auswählen.	Wenn die Standardeinstellungen und Schwellenwerte in den **Instanz-Score-Einstellungen** nicht geändert werden.
Verfolgen Sie Ihren Instanz-Score, indem Sie benutzerdefinierte Indikatoren Ihrer Wahl auswählen.	Wenn die App Score-Komponenten im App Dashboard standardmäßig verwendet werden und keine Anpassung vorgenommen wird.
Fügen Sie private IP-Blöcke hinzu, um Kundenanfragen in der Geo Map zu visualisieren	Wenn IP-Blöcke nicht konfiguriert sind. Sie können IP-Blöcke erstellen, um Client-Anfragen auf einer Geo-Map auf der Grundlage ihrer privaten IPs/Reichweite zuzuordnen und zu visualisieren.
Abonnieren und exportieren Sie Ihre AppSec-Verstöße in Echtzeit nach Splunk	Wenn die Splunk-Integration in NetScaler ADM noch nicht konfiguriert ist.
Passen Sie den Standardschwellenwert an oder erstellen Sie einen neuen Schwellenwert für Ihre Kubernetes-Dienste	Wenn im Servicediagramm nur Standardschwellenwerte verwendet werden und kein einzelner oder doppelter Schwellenwert auf die Dienste angewendet wird.
Konfigurieren Sie proaktiv Benachrichtigungsprofile und erhalten Sie Benachrichtigungen an Ihren Kommunikationszielen	Wenn ein Benachrichtigungsprofil noch nicht konfiguriert ist.
Planen Sie wiederkehrende Exporte und erhalten Sie Benachrichtigungen zu den Infrastrukturdetails	Falls noch keine Exportzeitpläne unter **Infrastruktur > Instanzen**konfiguriert sind.
Sie haben ServiceNow und möchten es in ADM integrieren?	Wenn die ServiceNow-Integration in NetScaler ADM noch nicht konfiguriert ist.
Automatisieren Sie die Verwaltung von SSL-Zertifikaten mit Venafi und ADM	Wenn der Venafi-Server noch nicht in NetScaler ADM konfiguriert ist.
Erneuern Sie Ihre Pool-Lizenz, bevor sie abläuft.	Wenn Ihre bestehende Lizenz in 30 Tagen abläuft.
Beginnen Sie mit Pooled Licensing, indem Sie Ihre gekaufte gepoolte Bandbreite NetScaler-Instanzen zuweisen.	Wenn Sie noch nicht mit der Zuweisung Ihrer gepoolten Lizenzberechtigungen begonnen haben.
Erwägen Sie den Kauf von mehr gepoolter Bandbreitenkapazität.	Wenn Sie 90% oder mehr Ihres gepoolten Bandbreitenanspruchs genutzt haben.

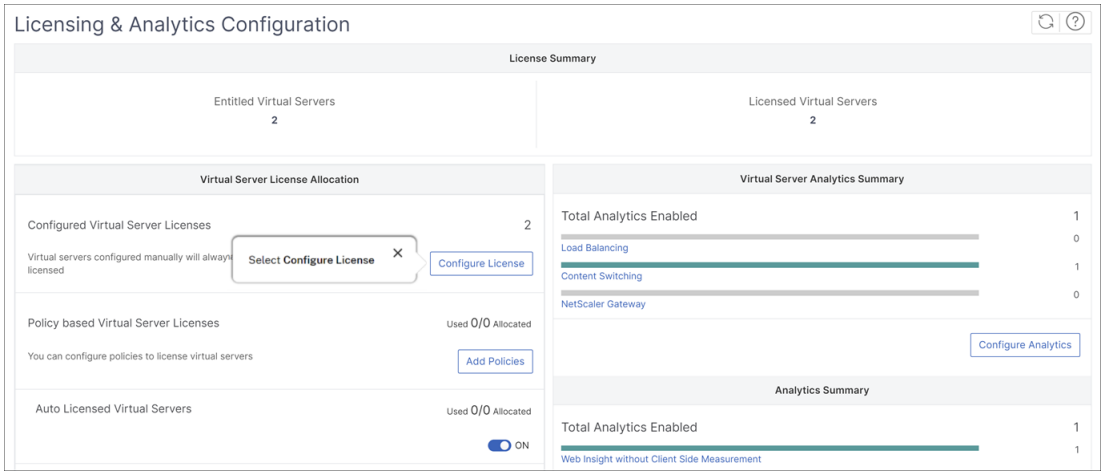
Name der Empfehlung	Wann ist die Aufgabe in der GUI sichtbar?
Ihr aktueller Anspruch auf gepoolte Bandbreite wird nicht ausreichend genutzt. Prüfen und erwägen Sie, mehr zuzuweisen	Wenn Ihre gepoolte Lizenzzuweisung weniger als 70% beträgt.

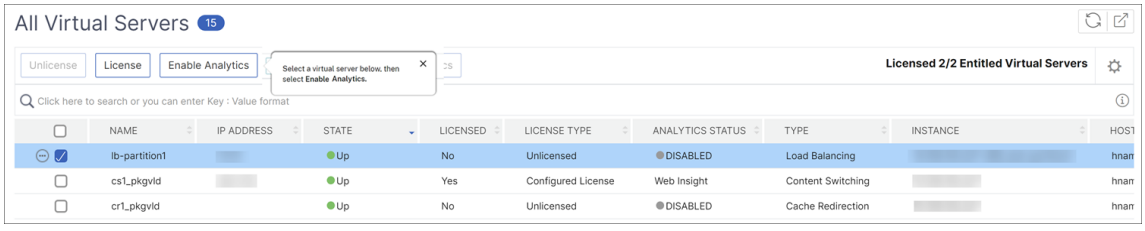
Wie verwende ich den Guide me-Workflow und vervollständige die Empfehlung?

Stellen Sie sich vor, dass Sie Analysen für alle lizenzierten virtuellen Server aktivieren möchten. Klicken Sie für die folgende Aufgabe auf **Guide me**:

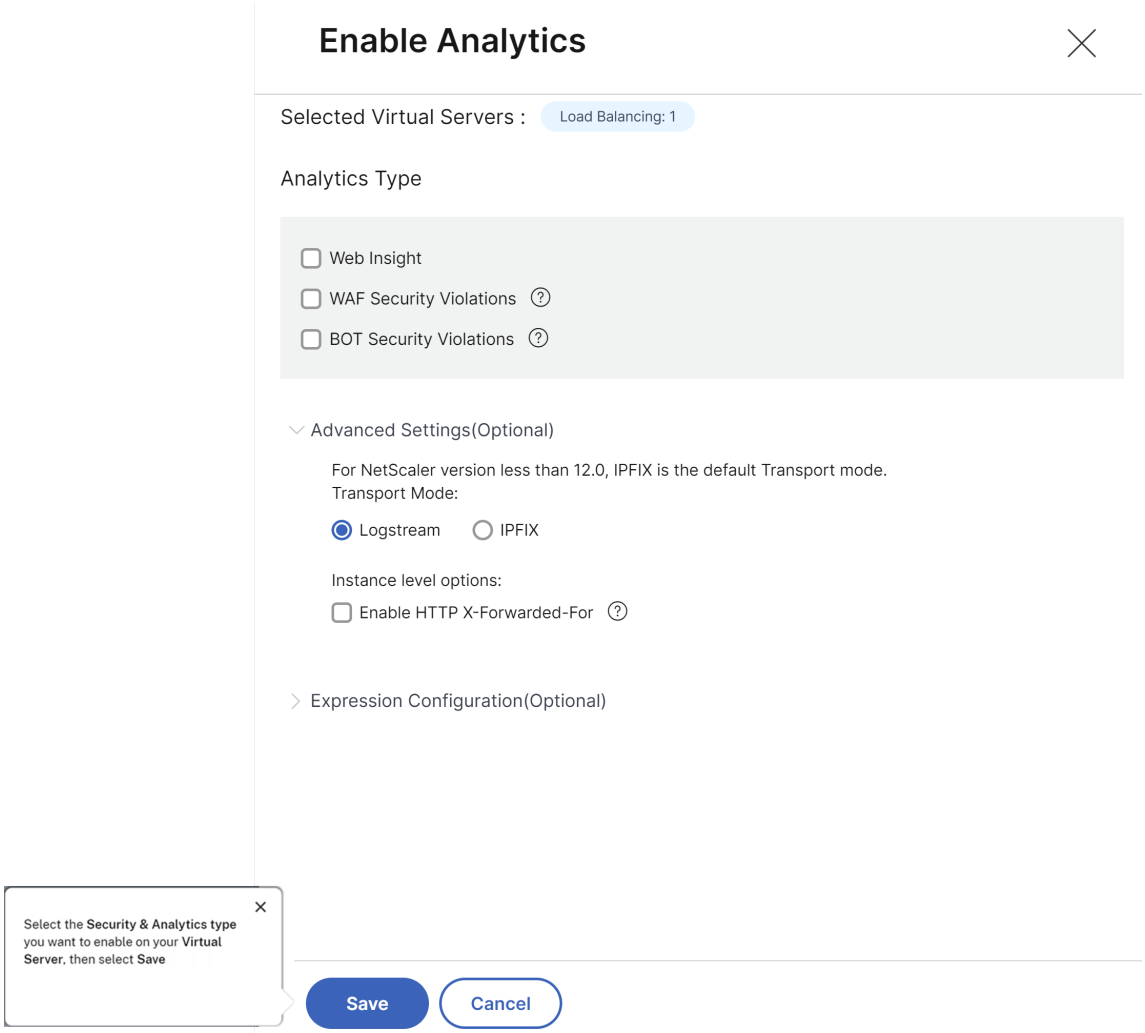


Der Workflow enthält die erforderlichen Vorschläge, um die Aufgabe abzuschließen. In diesem Beispiel folgen Sie, nachdem Sie auf **Guide me**geklickt haben, den bereitgestellten Tooltip-Vorschlägen:

1. 

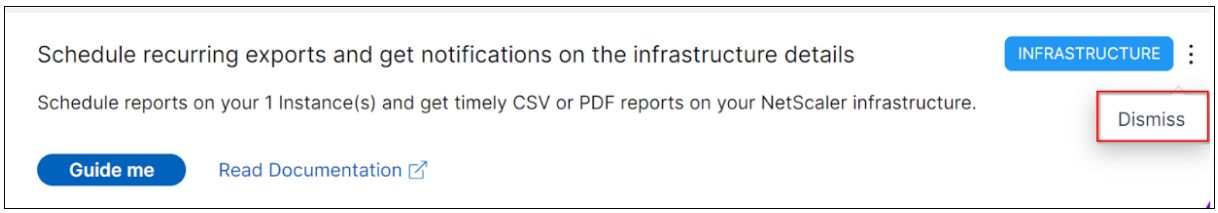
2. 

3.



Nachdem Sie den Analysetyp ausgewählt und auf **Analytics speichern** geklickt haben, ist die Empfehlung abgeschlossen und wird in den Status Abgeschlossen verschoben.

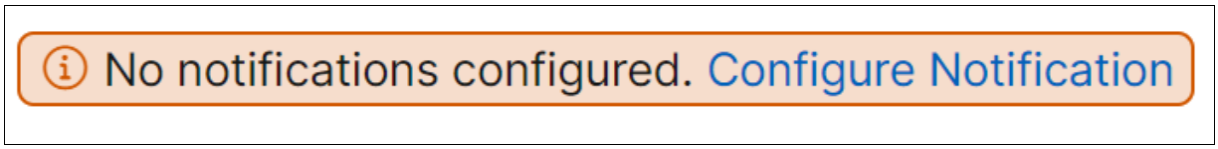
Wenn Sie eine Empfehlung zu einem späteren Zeitpunkt abschließen möchten, können Sie ebenfalls in der Liste die Option **Ablehnen** auswählen. Die Empfehlung wird dann in **Abgelehnt** verschoben.



Benachrichtigungen konfigurieren

Sie können jedes Mal, wenn NetScaler ADM offene Aufgaben identifiziert, die Ihre sofortige Aktion erfordern, konfigurieren und Benachrichtigungen erhalten. Wenn Sie keine Benachrichtigungen kon-

figuriert haben, können Sie oben rechts auf **Benachrichtigung konfigurieren** klicken.



Auf der Seite **Benachrichtigungen** können Sie Profile für **E-Mail** und **Slack** konfigurieren und dann auf **Speichern** klicken, um Benachrichtigungen zu erhalten. Für jeden Benachrichtigungstyp zeigt die NetScaler ADM GUI die konfigurierte Verteilerliste oder das konfigurierte Profil an. Der NetScaler ADM sendet Benachrichtigungen an die ausgewählte Verteilerliste oder das ausgewählte Profil.

Häufig gestellte Fragen

1. Warum gibt es Empfehlungen für die Administratoren?

   Derzeit beziehen sich die Empfehlungen speziell auf Bereitstellungen, die den Administratoren mehr bei Konfigurationen und Einrichtungsaufgaben helfen, um die Bereitstellung effizient zu gestalten. Es ermöglicht auch eine bessere Produkterkennung und Administratoren können wissen, was eine Aufgabe bewirkt und wie sie helfen kann, ohne Vorkenntnisse zu haben oder zu wissen, ob die Funktion in ADM existiert oder nicht.

2. Was passiert, wenn ich eine Empfehlung ablehne?

   Die Empfehlungen, die Sie ablehnen, werden in den Bereich **Abgewiesen**verschoben. Sie können diese Empfehlungen später vervollständigen.

3. Geht die Empfehlung auf **Abgeschlossen**, wenn ich einen Guide mich starte und in der Mitte lasse?

   Nein, die Empfehlung ist erst abgeschlossen, wenn die Aktion gespeichert oder abgeschlossen wurde.

4. Kann ich suchen oder filtern?

   Ja! Sie können die Suchleiste verwenden oder sich auf bestimmte Aufgaben beschränken, indem Sie die Kategorie aus der Liste auswählen.

5. Erhalte ich Aufgaben, um bei dynamischen Ereignissen Maßnahmen zu ergreifen?

   Ja! Derzeit können Sie sich insgesamt 4 umsetzbare Aufgaben ansehen. Weitere Informationen finden Sie unter Aufgaben.

6. Werden alle umsetzbaren Aufgaben und über 20 Empfehlungen angezeigt, auch wenn ich keine NetScaler-Instanzen in NetScaler ADM hinzugefügt habe?

   Nein. In NetScaler ADM müssen sowohl die NetScaler-Instanz als auch virtuelle Server verfügbar sein, um alle Aufgaben und Empfehlungen anzuzeigen.

7. Wie oft werden die Aufgaben aktualisiert?

   Wenn Sie im linken Navigationsbereich auf **Aufgaben** klicken, werden sie aktualisiert und sind mit dem neuesten Status verfügbar. Die Details werden abgerufen und aktualisiert.

Ein einheitliches Dashboard zum Anzeigen der wichtigsten Metrikdetails für die Instanz

February 5, 2024

In NetScaler ADM können Sie verschiedene Einblicke in die Nutzung und Leistung von Anwendungen, die ADC-Infrastruktur, Sicherheitsverletzungen (Bot und WAF) usw. anzeigen. Als Administrator müssen Sie möglicherweise zu verschiedenen Optionen in der ADM-GUI navigieren, um mehrere Einblicke anzuzeigen. Um beispielsweise die virtuellen Server (Anwendungen) und ADC-Instanz-Insights zu überprüfen:

- Sie müssen zuerst zu **Anwendungen > Dashboard** navigieren, um Einblicke in Anwendungen anzuzeigen.
- Anschließend müssen Sie zu **Infrastruktur > Infrastrukturanalyse** navigieren, um Erkenntnisse für ADC-Instanzen anzuzeigen.

Für eine bessere Überwachungserfahrung ist es erforderlich, dass Sie über ein Privileg verfügen, das einen Überblick über alle erforderlichen Erkenntnisse enthält. Navigieren Sie zu **Übersicht > Dashboard**, um ein Einzelbereichs-Dashboard mit einer Übersicht der wichtigsten Metrikdetails basierend auf den folgenden Kategorien zu visualisieren:

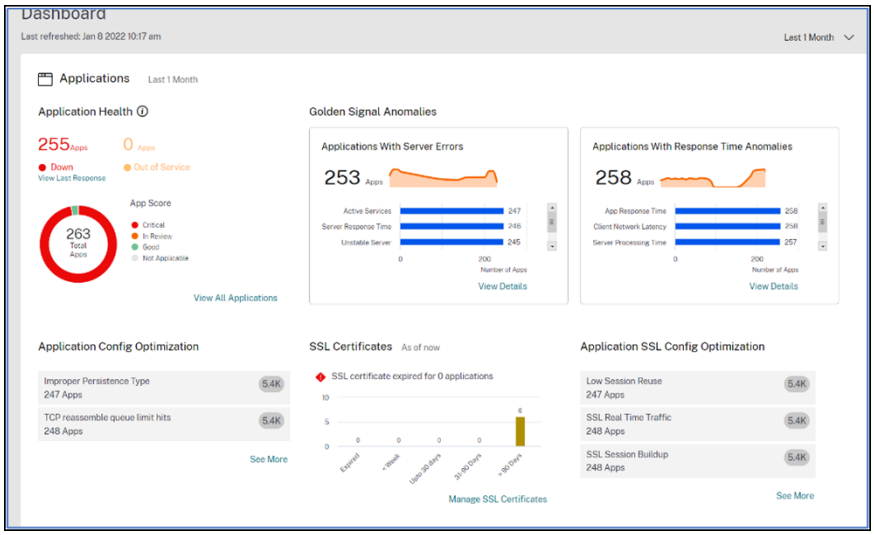
- Anwendungen
- ADC-Infrastruktur
- Anwendungssicherheit
- Gateway

Anwendungen

Unter **Anwendungen**können Sie Folgendes anzeigen:

- **Anwendungsintegrität** —Bietet einen Überblick über Anwendungen, die sich in Nicht **verfügbar** und **außer Betrieb**befinden, und zwar basierend auf ihrem Status wie **Kritisch**, **In Überprüfung**, **Gut**und **Nicht zutreffend**. Klicken Sie auf **Alle Anwendungen** anzeigen, um Details im App-Dashboard anzuzeigen.

- **Golden Signal Anomalien** —Bietet einen Überblick über Anwendungen mit Serverfehlern und Antwortzeitanomalien. Klicken Sie für weitere Informationen auf **Details anzeigen** .
- **Optimierung der Anwendungskonfiguration** —Bietet einen Überblick über die Gesamtzahl der Anwendungen, bei denen Leistungsprobleme auftreten. Klicken Sie auf **Mehr** anzeigen, um Details zum Problem im App-Dashboard anzuzeigen
- **SSL-Zertifikate** —Bietet einen Überblick über SSL-Zertifikate und deren Gültigkeit. Klicken Sie auf **SSL-Zertifikate verwalten** um weitere Informationen im SSL-Dashboard anzuzeigen.
- **Optimierung der SSL-Konfiguration von Anwendungen** —Bietet einen Überblick über die Gesamtzahl der Anwendungen, bei denen SSL-bezogene Probleme auftreten. Klicken Sie auf **Mehr** anzeigen, um Details zum Problem anzuzeigen.



ADC-Infrastruktur

Unter **ADC Infrastructure**können Sie die folgenden Schlüsselmetriken für die ADC-Instanz anzeigen:

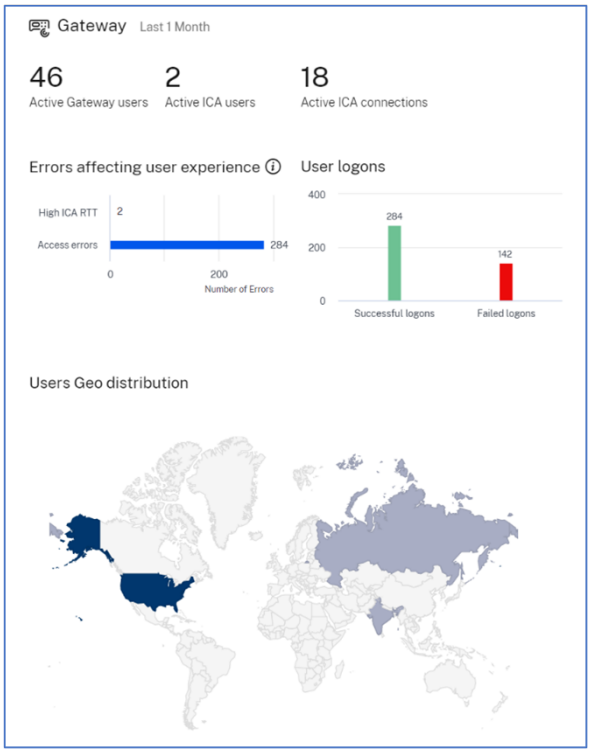
- **ADC-Instanzintegrität** —Bietet einen Überblick über die Gesamtzahl der ADC-Instanzen basierend auf dem Instanz-Score.
- **Von CVEs betroffene ADC-Instanzen** — Bietet einen Überblick über die Gesamtzahl der ADC-Instanzen, die von Common Vulnerabilities and Exposures (CVEs) betroffen sind.
- **ADC-Instanzprobleme** —Bietet einen Überblick über ADC-Instanzprobleme in Abhängigkeit von der Problemkategorie. Weitere Informationen finden Sie unter Infrastructure Analytics.
- **Zusammenfassung des ADC-Instanz-Upgrades** —Bietet einen Überblick über die Gesamtzahl der ADC-Instanzen, die sich nicht im neuesten Build befinden. Klicken Sie auf das ADC-Instanzanzeigedashboard, um weitere Informationen zu erhalten.

Anwendungssicherheit

Bietet einen Überblick über die Gesamtzahl der betroffenen Anwendungen und die Gesamtzahl der gemeldeten Verstöße (Bot und WAF) für die ausgewählte Dauer. Klicken Sie auf **Sicherheits-Dashboard** anzeigen, um die Sicherheits- und Bot-Verstöße anzuzeigen.

Gateway

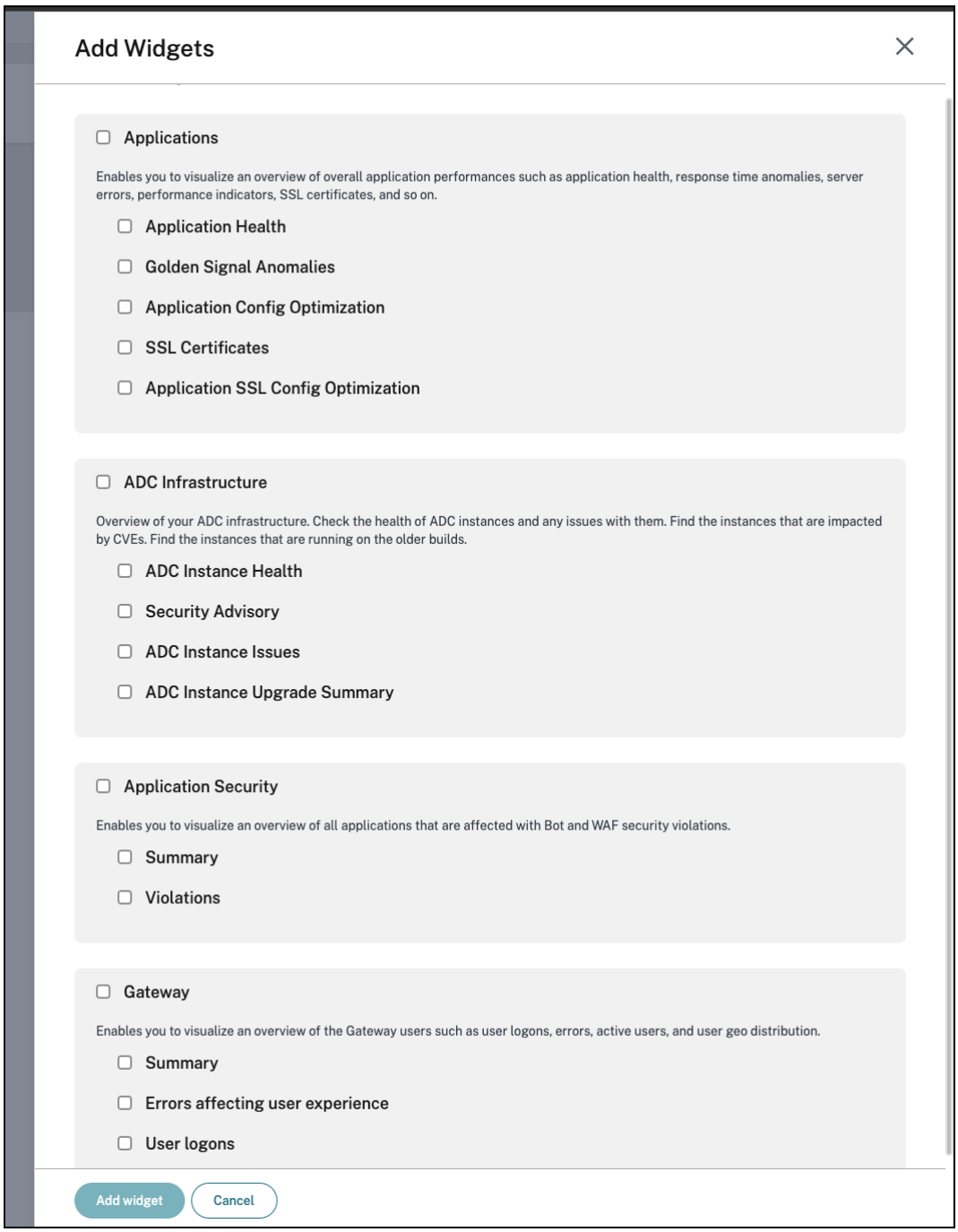
Bietet einen Überblick über die Gesamtzahl aktiver Gateway-Benutzer, die Gesamtzahl der aktiven ICA-Benutzer und die Gesamtzahl der aktiven ICA-Verbindungen. Sie können sich auch Fehler, Benutzeranmeldedetails und eine Geokarte anzeigen lassen, die Details zu den Benutzerstandorten enthält.



Dashboard anpassen

Sie können die Option **Dashboard bearbeiten** verwenden und die Dashboard-Ansicht nach Ihren Wünschen anpassen. Mit der Option **Dashboard bearbeiten** können Sie:

- Widgets ziehen
- Entfernen Sie das gesamte Widget (Anwendungen, ADC-Infrastruktur, Gateway oder Anwendungssicherheit).
- Entfernen Sie die kleineren Widgets, die unter jedem Widget vorhanden sind.
- Klicken Sie auf **Widget hinzufügen** und wählen Sie die erforderlichen Schlüsselmetriken aus, die Sie unter jedem Widget anzeigen möchten.



- Auf Standard zurücksetzen
- Auf zuletzt gespeichert zurücksetzen

Klicken Sie nach den Änderungen auf **Speichern**.

> **Hinweis**
>
> - Standardmäßig werden alle Widgets angezeigt. Wenn Sie das Dashboard anpassen, die Än-

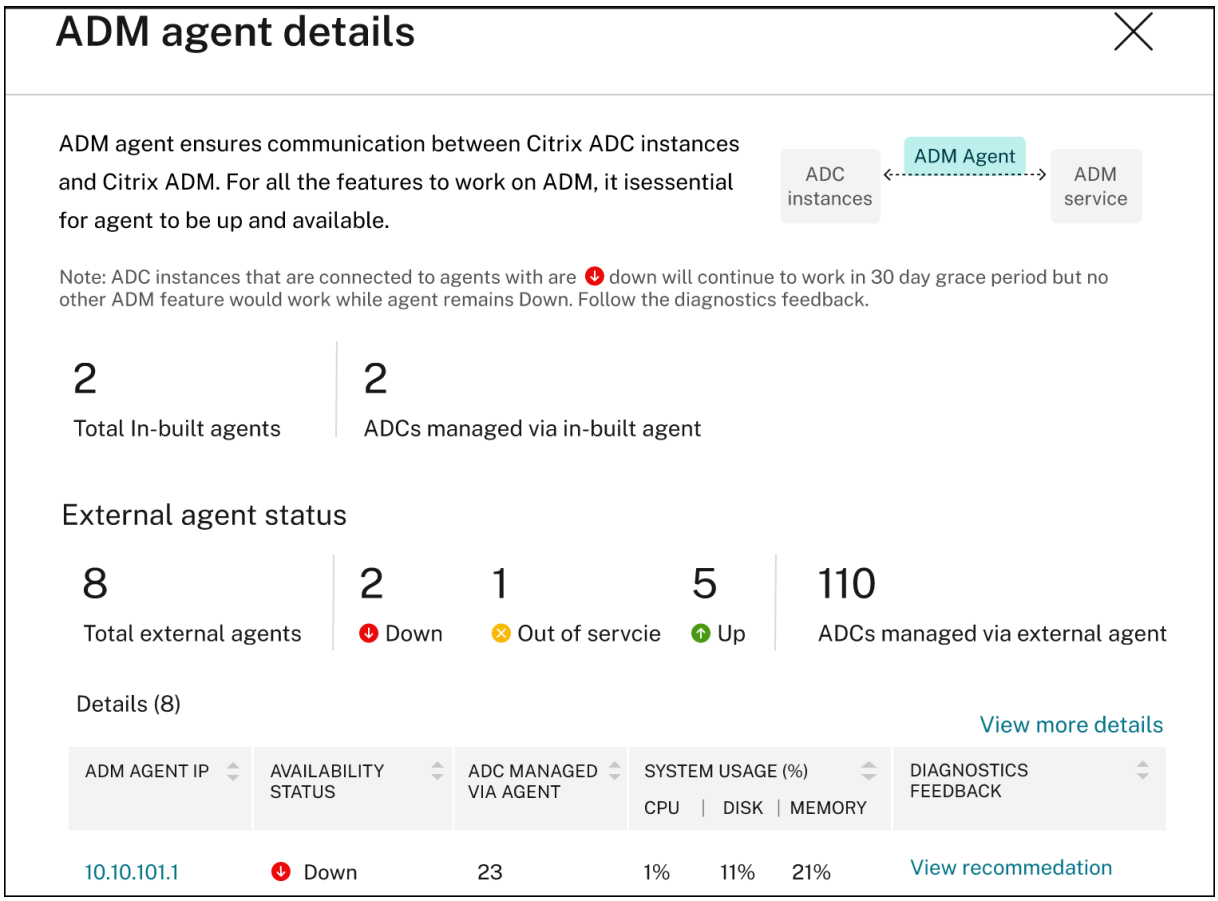
> derungen speichern und erneut die Option Auf **Standard zurücksetzen** verwenden, werden alle Widgets zum Dashboard hinzugefügt.
>
> - Die Option Auf **zuletzt gespeichert zurücksetzen** lädt die zuvor gespeicherte Konfiguration.

Agentdetails anzeigen

Im vereinheitlichten Dashboard können Sie eine Übersicht der ADM-Agentdetails visualisieren. Unter **Übersicht > Dashboard**können Sie neben dem **ADM-Agentstatus**den folgenden Status anzeigen, mit dem Sie die Gesamtverfügbarkeit der Agents analysieren können:

- **Alles verfügbar**. Zeigt an, dass alle Agents aktiv sind.
- **Alles nicht verfügbar**. Zeigt an, dass alle Agents ausgefallen und nicht zugänglich sind.
- **[Anzahl der Agents] nicht verfügbar**. Zeigt an, dass einige Agents ausgefallen sind und nicht zugänglich sind.
- **Alles außer Betrieb**. Zeigt an, dass alle Agents außer Betrieb sind.
- **[Anzahl der Agents] außer Betrieb**. Zeigt an, dass einige Agents außer Betrieb sind.
- **Externer Agent wurde nicht gefunden**. Zeigt an, dass kein Agent (über Hypervisoren) konfiguriert ist.

Klicken Sie auf **Details anzeigen**, um eine Übersicht der ADM-Agentdetails wie die Gesamtzahl der integrierten Agents, die Gesamtzahl der externen Agents, die Agent-IP, den Status, die Systemnutzung, Diagnoseprüfungen usw. anzuzeigen.



Filter erstellen und anwenden

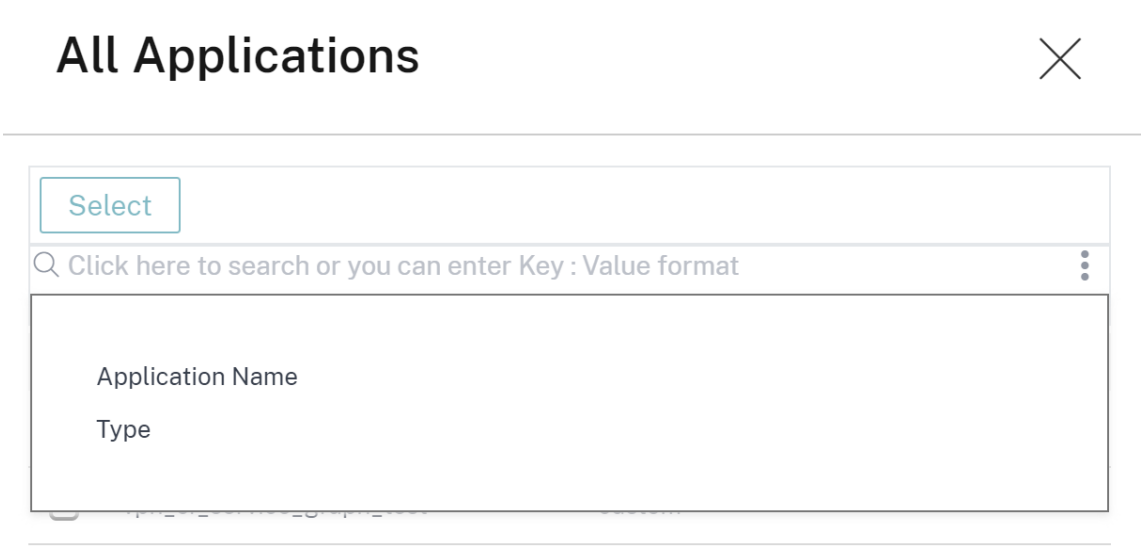
In den folgenden Fällen können Sie Filter anwenden und Erkenntnisse nur für die ausgewählten Instanzen oder Anwendungen anzeigen:

- Anwendungen
- ADC-Infrastruktur
- Anwendungssicherheit

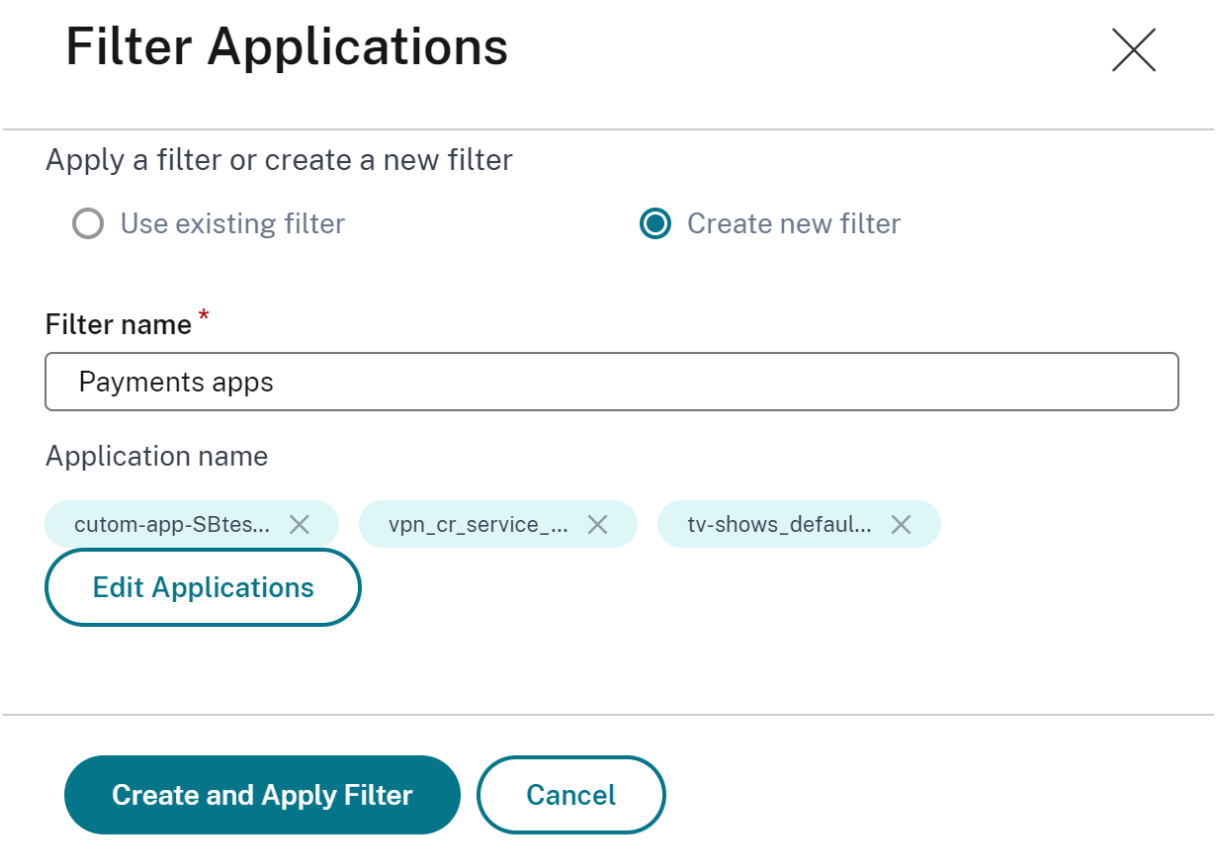
Standardmäßig sind alle Anwendungen ausgewählt. Sie können vom Dashboard aus einen benutzerdefinierten Filter erstellen, indem Sie auf das Filtersymbol in der Kachel klicken.

Im Fenster **Anwendungen filtern**:

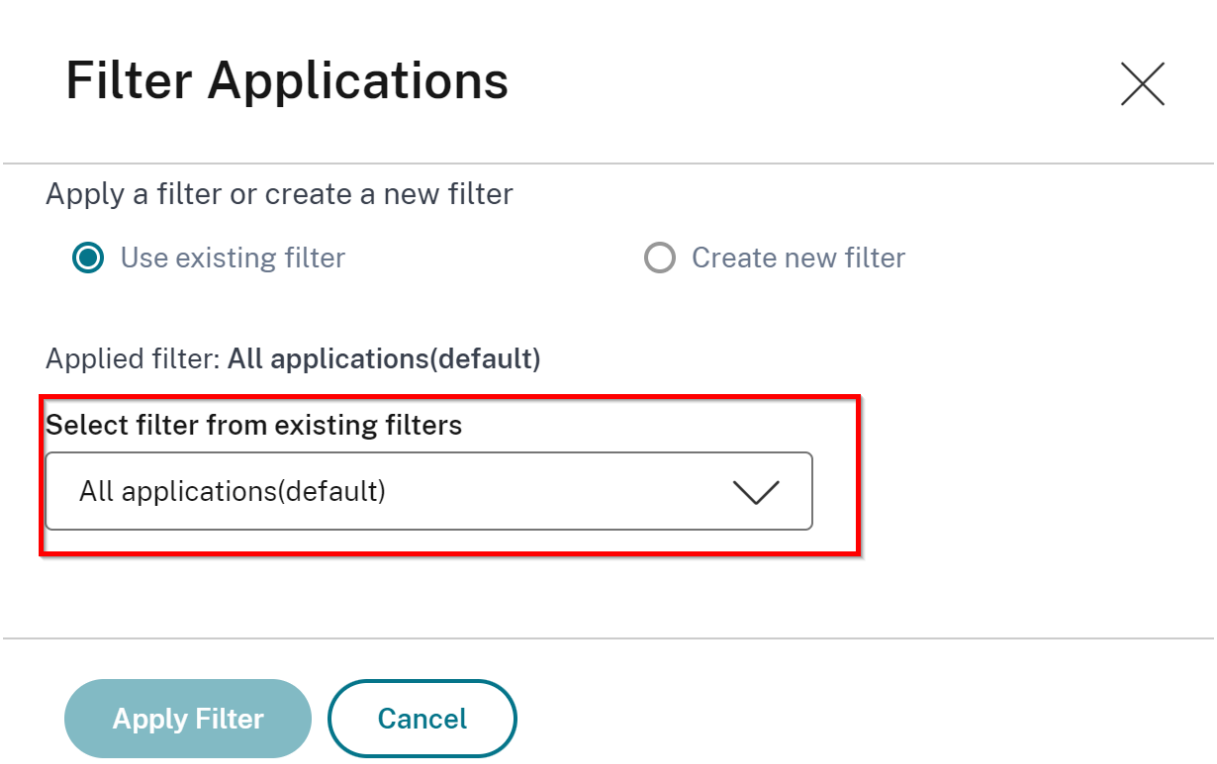
1. Wählen Sie **Neuen Filter erstellen** aus.
2. Geben Sie einen Filternamen ein, der Ihrer Wahl entspricht.
3. Klicken **Sie auf Anwendungen auswählen** und fügen Sie alle erforderlichen Anwendungen für den Filter hinzu. Wenn Sie Anwendungen auswählen, können Sie auch die Filter (**Anwendungsname** und **Typ**) verwenden und dann Anwendungen auswählen.



4. Klicken Sie auf **Filter erstellen und anwenden**.

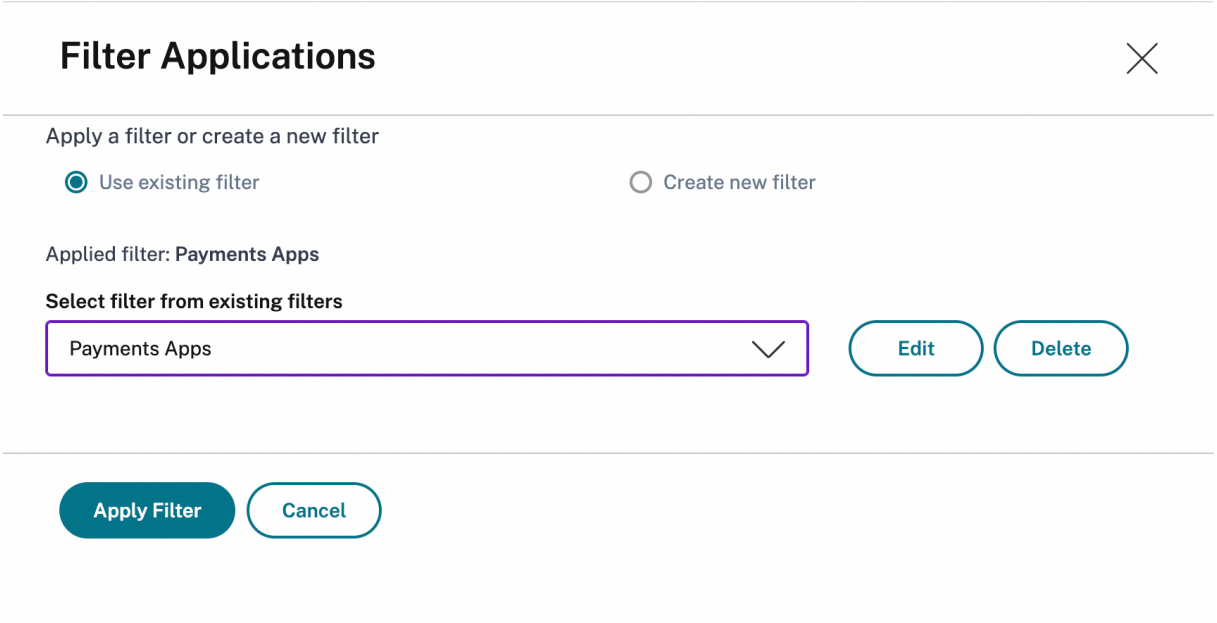


Der Filter ist jetzt erstellt und angewendet. Sie können weitere Filter erstellen, indem Sie dasselbe Verfahren befolgen. Nachdem Sie Filter erstellt haben, können Sie über die Liste **Filter aus vorhandenen Filtern auswählen** und anwenden.



Filter bearbeiten

Sie können einen Filter bearbeiten, indem Sie den Filter aus der Liste auswählen und auf **Bearbeiten** klicken. Mit der Bearbeitungsoption können Sie Anwendungen hinzufügen oder entfernen und dann den Filter aktualisieren.



Um einen Filter zu löschen, wählen Sie den Filter aus der Liste aus und klicken Sie auf **Löschen**.

> **Hinweis**
>
> Wenn Sie einen Filter mit Anwendungen erstellen und eine der Anwendungen im App-Dashboard gelöscht wird, werden die Anwendungsdetails sofort aus dem vereinheitlichten Dashboard entfernt.

Anwendungen

February 5, 2024

Mit der Anwendungsanalyse- und Verwaltungsfunktion von NetScaler ADM können Sie die Anwendungen mithilfe eines anwendungszentrierten Ansatzes überwachen. Dieser Ansatz hilft Ihnen dabei:

- Überprüfen Sie den Score und analysieren Sie die Gesamtleistung der Anwendungen
- Überprüfen Sie auf Probleme, die mit dem Server oder Client bestehen
- Erkennen Sie Anomalien in den Datenverkehrsströmen der Anwendung und ergreifen Sie Korrekturmaßnahmen

  > **Hinweis**
  >
  > Anwendungen beziehen sich auf einen oder mehrere virtuelle Server, die auf den Instanzen konfiguriert sind (NetScaler).

Sie können die Anwendungen für die Dauer wie 1 Stunde, 1 Tag, 1 Woche und 1 Monat überwachen.

Voraussetzungen

- Stellen Sie sicher, dass Sie NetScaler-Instanzen in NetScaler ADM hinzugefügt haben
- Stellen Sie sicher, dass Sie über eine gültige Lizenz für Ihre NetScaler-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

Anwendungsüberblick

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 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 können ganz einfach bestimmte Anwendungen überwachen, die in einer Kategorie zusammengefasst sind.

Sie können beispielsweise eine Kategorie für Ihr Datencenter1 erstellen und dessen ADC-Instanzen hinzufügen. Nachdem Sie eine Kategorie definiert und die Instanz für Ihr Datencenter1 hinzugefügt haben, wird das Anwendungs-Dashboard mit einer separaten Kategorie angezeigt, die alle Anwendungen umfasst, die sich auf Ihr Datencenter1 beziehen.

Wichtige Hinweise

- 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 NetScaler ADM Lizenzen für bis zu 2 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 NetScaler einen Ingress Controller für NetScaler MPX (Hardware), NetScaler VPX (virtualisiert) und NetScaler CPX (containerisiert) bereit. Weitere Informationen finden Sie unter NetScaler Ingress Controller.

Die diskreten Anwendungen, die mit den NetScaler CPX-Instanzen konfiguriert werden, werden als Microservices-Anwendungen bezeichnet.

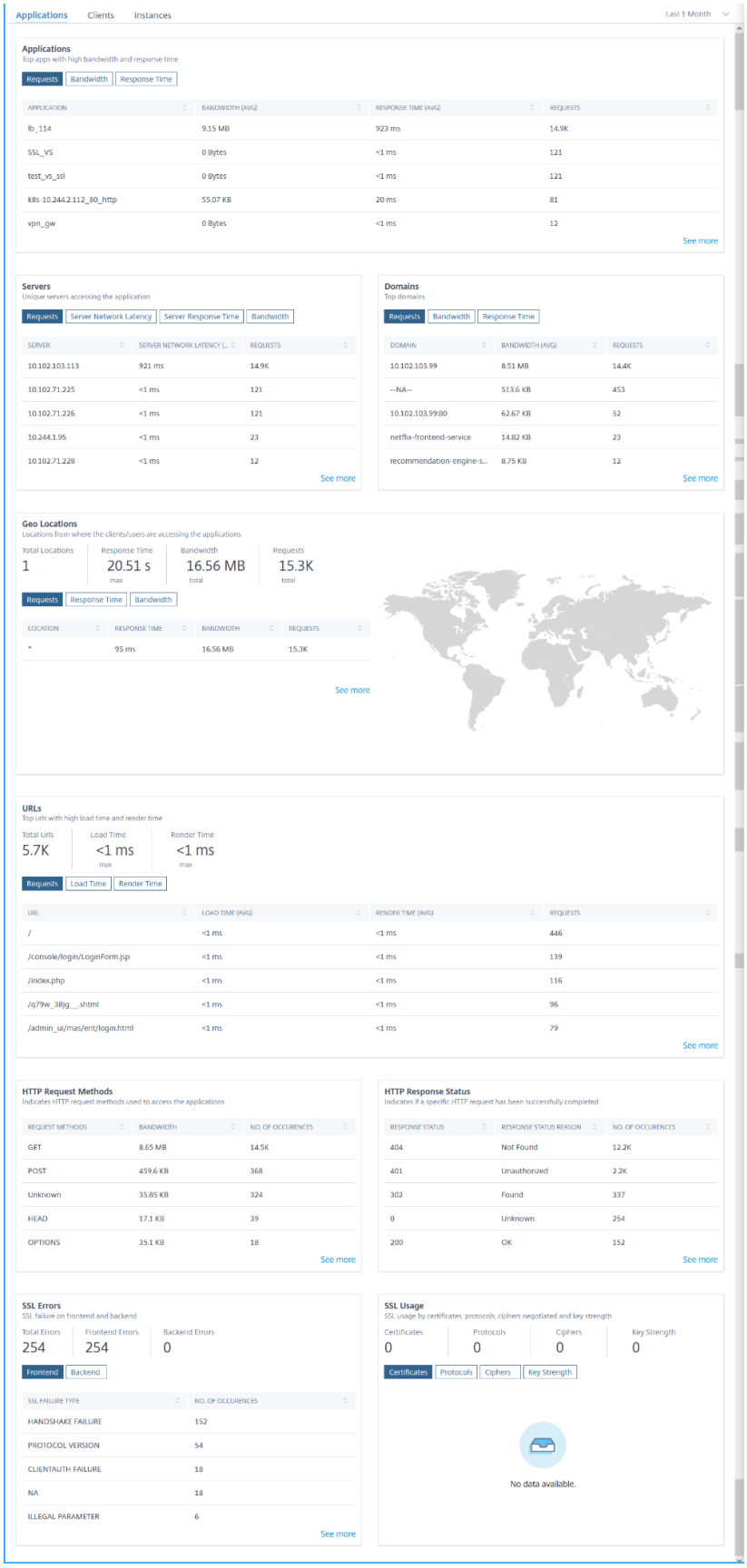
Web Insight-Dashboard

February 5, 2024

Die verbesserte Web Insight-Funktion wurde erweitert und bietet Einblicke in detaillierte Metriken für Webanwendungen, Clients und NetScaler-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
Anwendungen	Kunden	Instanzmetriken
Server	Geo Standorte	Anwendungen
Domänen	HTTP-Anforderungsmethoden	Domänen
Geo Standorte	HTTP-Antwortstatus	URLs
URLs	URLs	HTTP-Anforderungsmethoden
HTTP-Anforderungsmethoden	Betriebssystem	HTTP-Antwortstatus
HTTP-Antwortstatus	Browser	Kunden
SSL-Fehler	SSL-Fehler	Server
SSL-Nutzung	SSL-Nutzung	Betriebssystem
		Browser

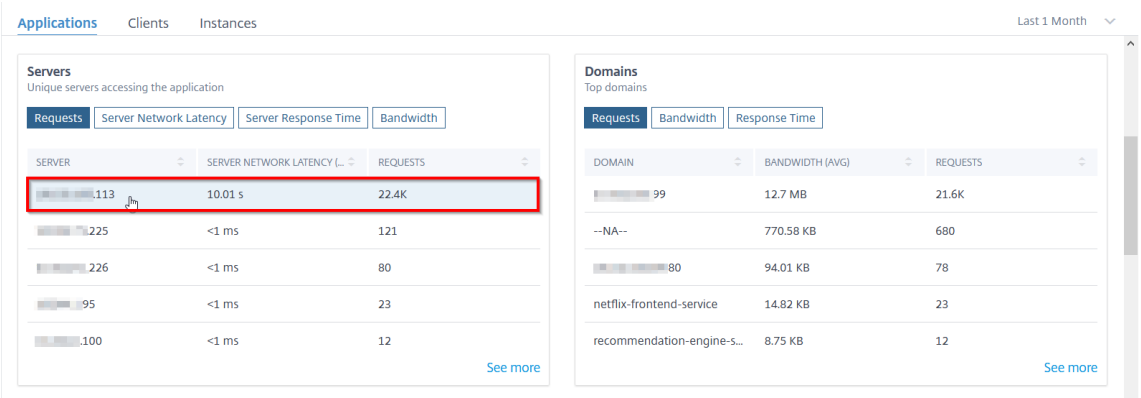


In jeder Metrik können Sie die Top-5-Ergebnisse anzeigen. Sie können klicken, um weitere Drill-downs durchzuführen, um das Problem zu analysieren und schneller Fehlerbehebungsmaßnahmen durchzuführen.

> **Hinweis:**
>
> - Ab Version **14.1-4.x** zeigt die Analyseansicht im Zeitreihendiagramm beim Drilldown einer Metrik Nullwerte (z. B. 0 ms und 0 Anfrage) für die gewählte Dauer an. Wenn früher für die gewählte Dauer kein Traffic oder keine Transaktion einging, wurden in der Analyseansicht die Diagramme angezeigt, indem diese Nullwerte übersprungen wurden.
> - In einigen Szenarien ist NetScaler möglicherweise nicht in der Lage, die RTT-Werte für einige Transaktionen zu berechnen. Für solche Transaktionen zeigt NetScaler ADM die RTT-Werte als
>
> - **NA** —Zeigt an, wenn die ADC-Instanz den RTT nicht berechnen kann.
> - **< 1 ms** —Zeigt an, wenn die ADC-Instanz den RTT in Dezimalstellen zwischen 0 ms und 1 ms berechnet. Zum Beispiel 0,22 ms.

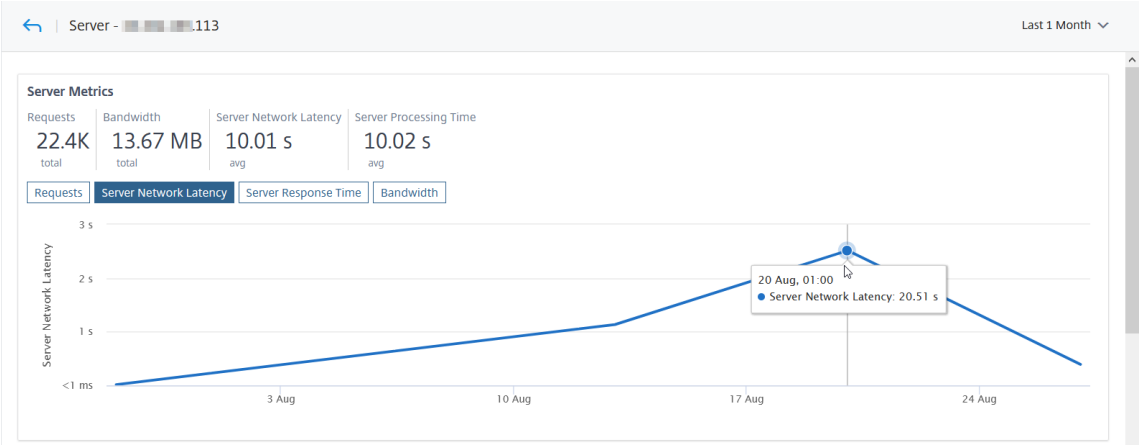
Bedenken Sie beispielsweise, dass Sie die Latenz des Servernetzwerks für eine Dauer von einem Monat analysieren und entscheiden möchten, ob Sie die Produktionsumgebung vergrößern oder verkleinern möchten. Um dies zu analysieren:

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.

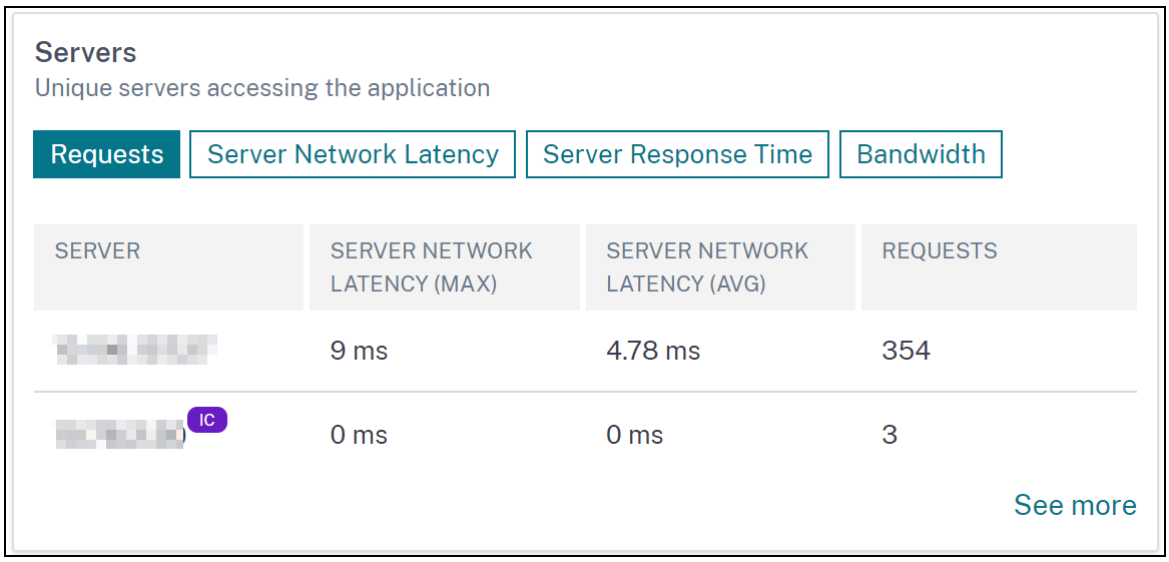


Die durchschnittliche Latenz zeigt 10,01 s an, und aus dem Diagramm können Sie analysieren, dass die Latenz des Servernetzwerks für den letzten Monat hoch zu sein scheint. Als Administrator können Sie sich entscheiden, die Produktionsumgebung zu vergrößern.

Integrierte Cache-Anfragen

Der integrierte Cache bietet In-Memory-Speicher auf der NetScaler-Appliance und stellt Webinhalte für Benutzer bereit, ohne dass ein Roundtrip zu einem Ursprungsserver erforderlich ist.

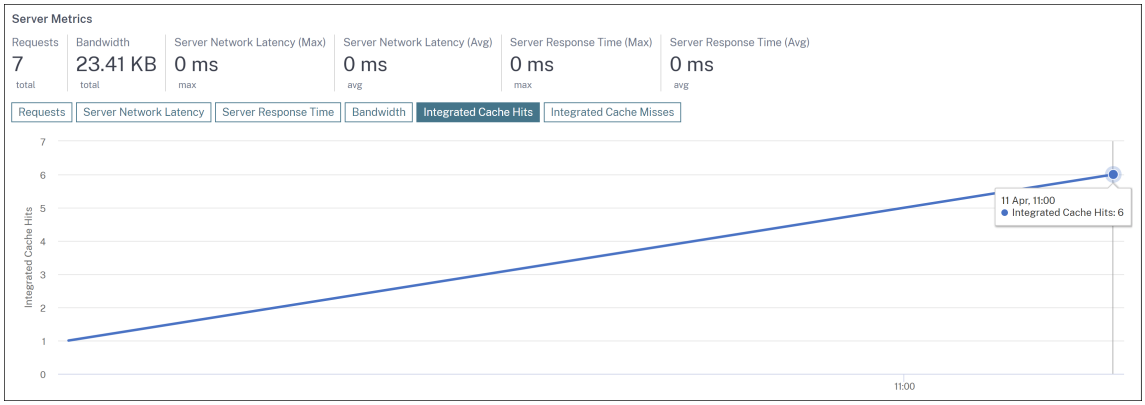
Die Integrationscache-Anfragen sind derzeit unter **Servern** mit einer IC-Benachrichtigung neben der IP-Adresse des virtuellen ADC-Servers sichtbar. Alle anderen Anfragen sind mit der IP-Adresse des Ursprungsservers sichtbar.



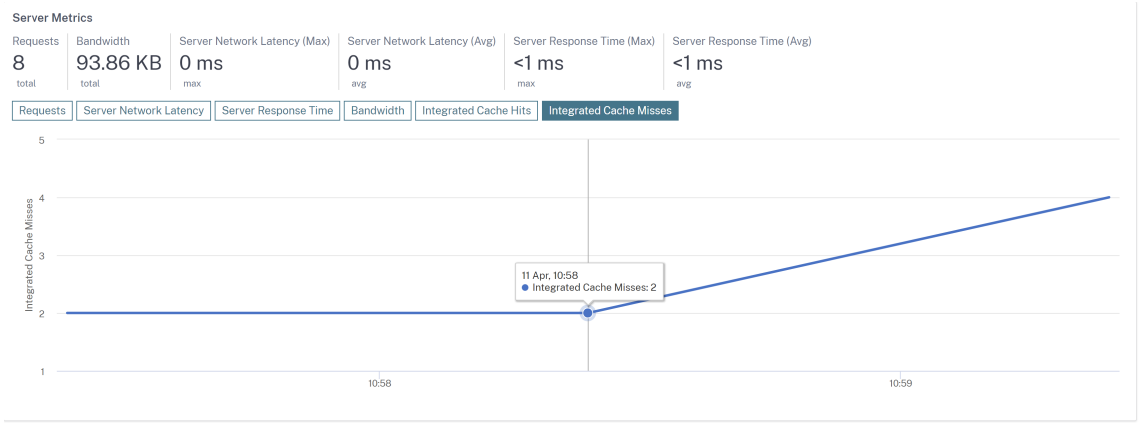
Wenn Sie einen Server aufschlüsseln, um weitere Details anzuzeigen, werden in den **Servermetriken** die Registerkarten „Treffer“und „Fehlschläge“im integrierten Cache angezeigt.

Die Diagrammansicht in:

- Auf der Registerkarte **Integrated Cache Hits** können Sie die gesamten Antworten anzeigen, die die NetScaler Appliance aus dem Cache bereitstellt.



- Auf der Registerkarte **Integrated Cache** Misses können Sie die gesamten Antworten anzeigen, die die NetScaler Appliance vom Originalserver bereitstellt.



Beheben von Web Insight-Problemen

Einzelheiten finden Sie im Dokument zur Fehlerbehebung bei Problemen mit Web Insight.

Die Hauptursache für Anwendungslatenz anzeigen

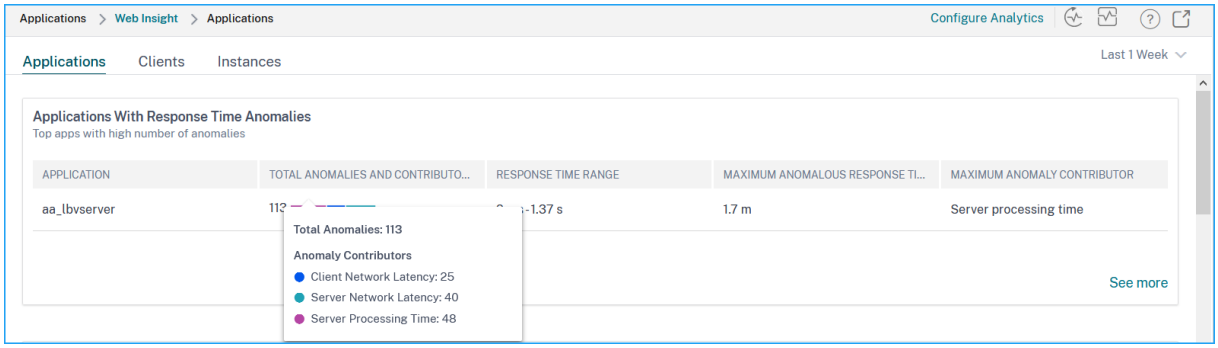
February 5, 2024

Anwendungsverlangsamung ist ein wichtiges Anliegen für jede Organisation, da dies zu geschäftlichen Auswirkungen oder Produktivität führt. Unter **Anwendungen > Web Insight**können Sie jetzt eine neue Metrik mit dem Namen **Anwendungen mit Reaktionszeitanomalien**anzeigen. Mithilfe dieser Metrik können Sie als Administrator analysieren, ob die Anwendungslatenz auf die folgenden Ursachen zurückzuführen ist:

- Netzwerklatenz des Clients
- Servernetzwerklatenz
- Verarbeitungszeit des Servers

NetScaler ADM führt jede Stunde Anomalieprüfungen durch und meldet Anomalien für den Verkehr der letzten 1 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.

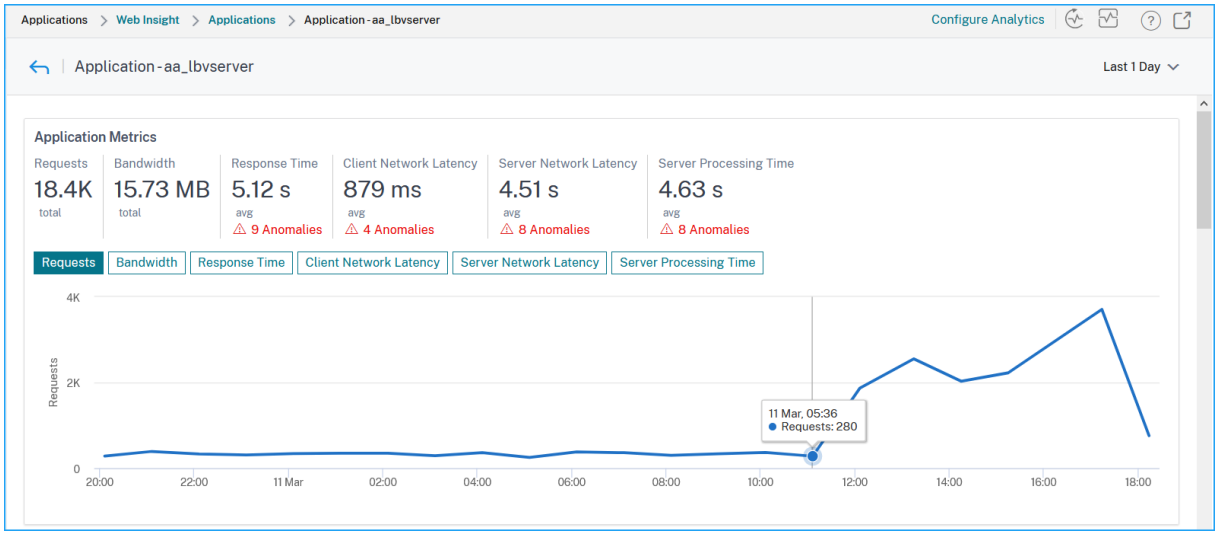
Auf der Seite "**Anwendungen > Web Insight** "können Sie die Anwendungen mit Anomalien der Reaktionszeit für die ausgewählte Dauer anzeigen. Die Metrik "**Anwendungen mit Antwortanomalien** "zeigt die fünf wichtigsten Anwendungen basierend auf den gesamten Anomalien an. Klicken Sie auf **Mehr** anzeigen, 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.
- **Maximum Anomaly Contributor** —Gibt an, ob die maximale Anzahl von Anomalien für die Anwendung aus Client-Netzwerklatenz, Server-Netzwerklatenz oder Serververarbeitungszeit stammt.

Anwendungsdrilldown

Klicken Sie auf eine Anwendung, um die Details zu **Anwendungsmetriken** für die ausgewählte Dauer anzuzeigen.



Mit den **Anwendungsmetriken** können Sie Folgendes anzeigen:

- **Zusammenfassung** —Eine Übersicht zur Visualisierung der Anwendungsleistung wie Reaktionszeit, Anfragen und Bandbreite.
- **Anfragen** —Die Gesamtzahl der von der Anwendung eingegangenen Anfragen. Sie können auch die Anfragen der fünf wichtigsten Kunden auf der Grundlage der Gesamtzahl der Anfragen anzeigen.
- **Bandbreite** —Die gesamte Bandbreite, die von der Anwendung verarbeitet wird. Sie können auch den Bandbreitenverbrauch der fünf wichtigsten Server auf der Grundlage des gesamten Bandbreitenverbrauchs anzeigen.
- **Reaktionszeit** —Eine Übersicht zur Darstellung der Client-Netzwerklatenz, der Server-Netzwerklatenz und der Serververarbeitungszeit in derselben Grafik.
- **Client-Netzwerklatenz** —Die durchschnittliche Client-Netzwerklatenz (vom Client zum ADC).
- **Server-Netzwerklatenz** —Die durchschnittliche Latenz des Servernetzwerks (vom ADC zum Server).
- **Serververarbeitungszeit** —Die durchschnittliche Serververarbeitungszeit (vom Server zum ADC).

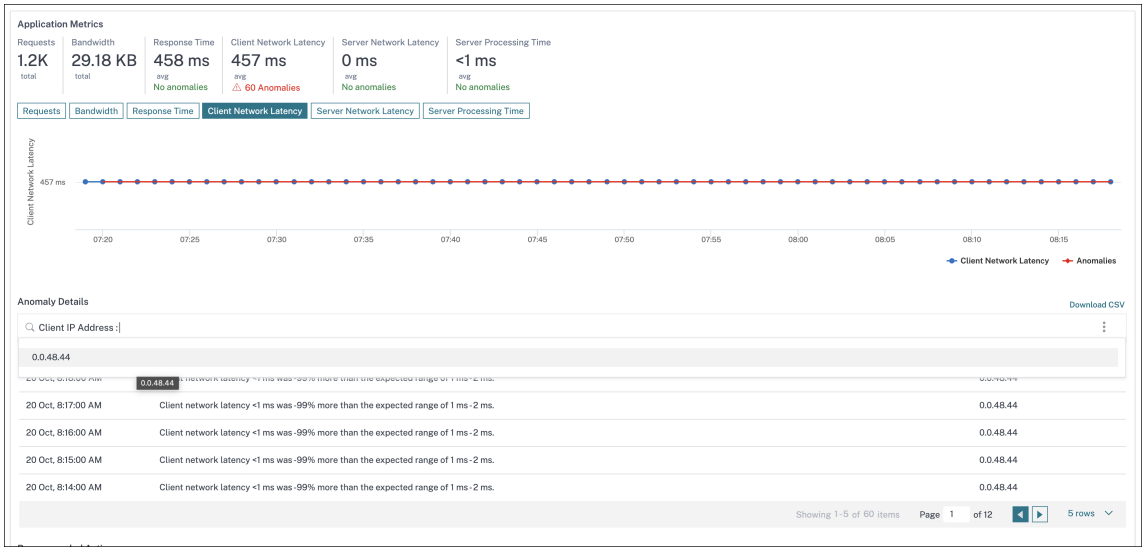
Wenn die Anwendung Anomalien aufweist, können Sie anzeigen, ob die Anomalien aus der Latenz des Client-Netzwerks, der Latenz des Servernetzwerks oder der Serververarbeitungszeit stammen. Klicken Sie auf jede Registerkarte, um Details anzuzeigen.

Auf den Registerkarten **Client-Netzwerklatenz** und **Server-Netzwerklatenz** können Sie Folgendes anzeigen:

- **Eine Suchleiste** —Klicken Sie auf die Suchleiste, um die IP-Adressen aller Clients (in Client Network Latency) und Server (in Server Network Latency) anzuzeigen. Sie können die IP-Adresse

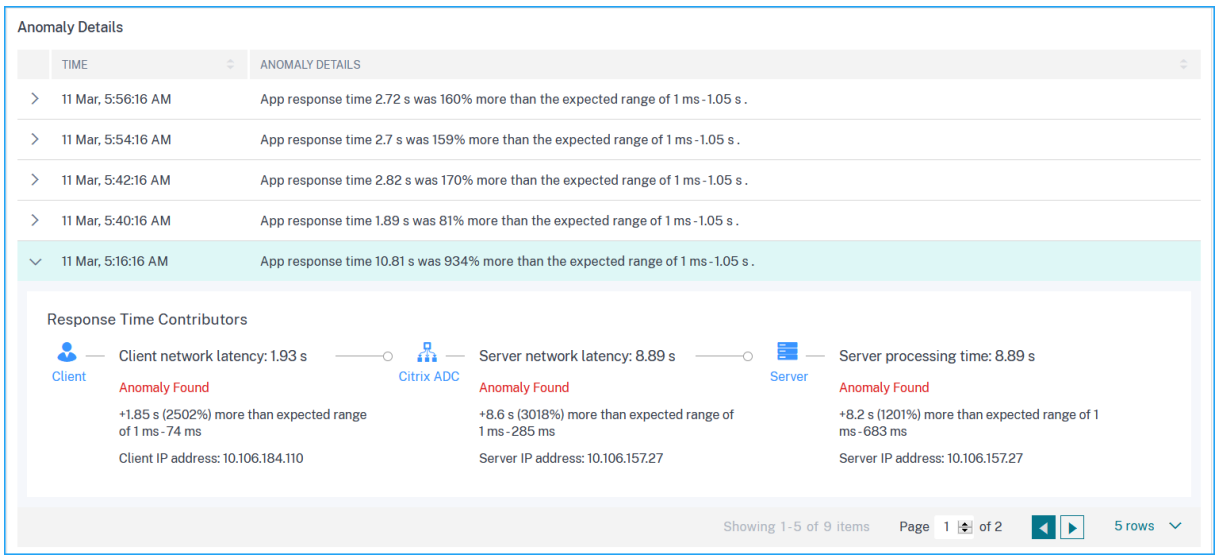
auswählen, um die Ergebnisse zu filtern.

- **Eine Exportoption**—Klicken Sie auf **CSV herunterladen** , um die Details im CSV-Format zu exportieren.

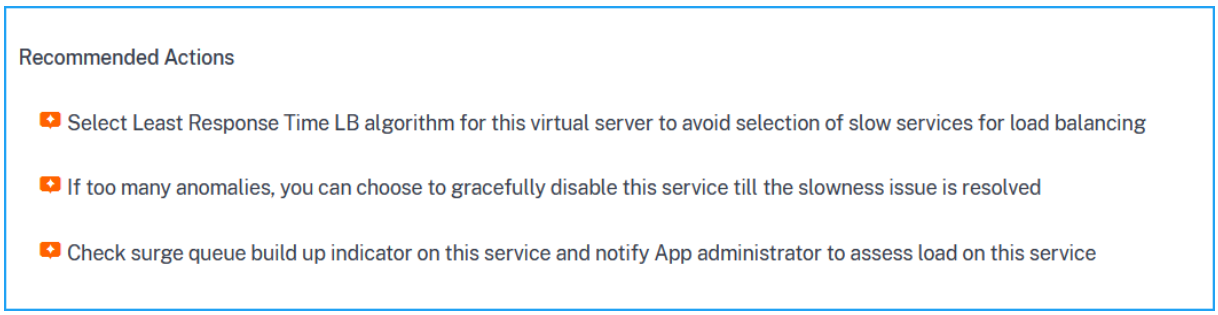


Reaktionszeit

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.



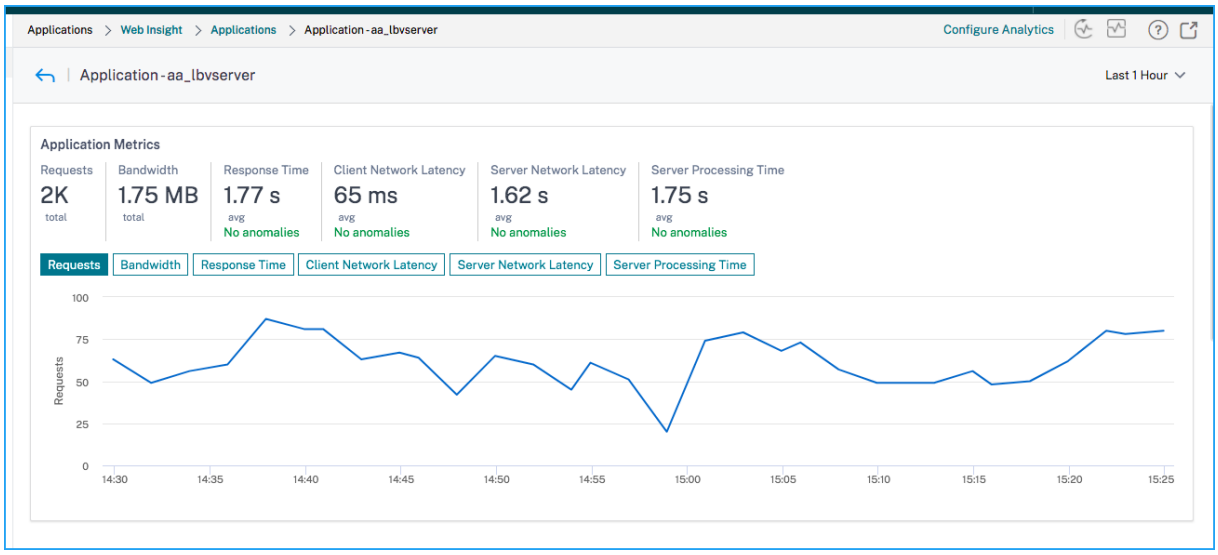
Die **empfohlenen Maßnahmen** schlagen Ihnen die möglichen Lösungen für die Anomalien vor.



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.



Service-Diagramm

February 5, 2024

Mit der Service Graph-Funktion in NetScaler 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. Sie können sich das Service-Diagramm ansehen für:

- Für alle NetScaler-Instanzen konfigurierte Anwendungen

- Kubernetes-Anwendungen
- 3-stufige Webanwendungen

Dienstdiagramm für Anwendungen über alle NetScaler-Instanzen hinweg

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

- Verstehen, aus welcher Region die Benutzer auf die spezifischen Anwendungen zugreifen (dreistufige Web-Apps und Microservices-App)
- Visualisieren der Infrastrukturansicht (NetScaler-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 NetScaler-Instanzen, die mit den jeweiligen Rechenzentren verbunden sind

  > **Hinweis**
  >
  > Sie können Rechenzentren nur anzeigen, wenn Sie über GSLB-Apps verfügen.

- Informationen zu den Kundenmetri
- Informationen zu den NetScaler-Metriken
- Alle NetScaler-Instanzen mit diskreten Anwendungen, benutzerdefinierten Anwendungen und diskreten Microservice-Anwendungen
- Die 4 Anwendungen mit niedriger Punktzahl, die zu benutzerdefinierten Apps, diskreten Apps und Microservices-Apps gehören
- Die Metrikinformationen für die vier besten virtuellen Server mit niedriger Bewertung
- 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 von Anwendungen im Service Graph.

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 Sie Engpässe, die durch die wechselseitige Abhängigkeit verschiedener Komponenten Ihrer Anwendungen entstehen
- Sammeln Sie Einblicke in die Abhängigkeiten der verschiedenen Komponenten Ihrer Anwendungen
- Überwachen Sie Dienste innerhalb des Kubernetes-Clusters
- Überwachen Sie, welcher Dienst Probleme hat
- Prüfen Sie die Faktoren, die zu Leistungsproblemen beitragen
- Detaillierte Sichtbarkeit der HTTP-Transaktionen des Dienstes anzeigen
- Analysieren der HTTP-, TCP- und SSL-Metriken

Durch die Visualisierung dieser Metriken in NetScaler ADM können Sie die Ursache von Problemen analysieren und die erforderlichen Fehlerbehebungsaktionen schneller durchführen. Das Service-Diagramm 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. Informationen zu den ersten Schritten finden Sie unter Service Graph einrichten.

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 Rechenzentrums-, ADC-Instanz-, CS- und LB-Server anzeigen.
- Ende-zu-Ende-Transaktionen vom Kunden zum Service
- Der Ort, von dem aus der Client auf die Anwendung zugreift
- Der Name des Rechenzentrums, in dem die Clientanforderungen verarbeitet werden, und die zugehörigen NetScaler-Metriken des Rechenzentrums (nur für GSLB-Anwendungen)
- Metrikdetails für Client, Service und virtuelle Server

- Wenn die Fehler vom Kunden oder vom Dienst stammen
- Der Dienststatus wie "**Kritisch**", "**Überprüfung**"und "**Gut**". NetScaler ADM zeigt den Dienststatus basierend auf der Reaktionszeit des Dienstes und der Fehleranzahl an.
  - **Kritisch (rot)** —Zeigt an, wenn die durchschnittliche Reaktionszeit des Service > 200 ms UND Fehlerzähler > 0
  - **Überprüfung (orange)** —Zeigt an, wenn die durchschnittliche Reaktionszeit des Service > 200 ms ODER Fehlerzähler > 0
  - **Gut (grün)** —Zeigt keinen Fehler an und durchschnittliche Reaktionszeit < 200 ms
- Der Kundenstatus wie "**Kritisch**", "**Überprüfung**"und "**Gut**". NetScaler ADM zeigt den Clientstatus basierend auf der Latenz des Clientnetzwerks und der Fehleranzahl an.
  - **Kritisch (rot)**—Zeigt an, wenn die durchschnittliche Netzwerklatenz des Clients > 200 ms UND Fehleranzahl > 0
  - **Überprüfung (orange)** —Zeigt an, wenn die durchschnittliche Clientnetzwerklatenz > 200 ms ODER Fehlerzähler > 0
  - **Gut (grün)** —Zeigt keinen Fehler an und durchschnittliche Latenz des Client-Netzwerks < 200 ms
- Der Status des virtuellen Servers wie "**Kritisch**", "**Überprüfung**"und "**Gut**". NetScaler ADM zeigt den Status des virtuellen Servers basierend auf dem App-Score an.
  - **Kritisch (rot)** —Zeigt an, wenn der App-Wert < 40 ist
  - **Überprüfung (orange)** —Zeigt an, wenn der App-Score zwischen 40 und 75 liegt
  - **Gut (grün)** —Zeigt an, wenn der App-Score > 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 Service-Diagramm für die Anwendung nicht sichtbar.
- Sie können Metriken für Clients und Services in Service Graph nur anzeigen, wenn aktive Transaktionen zwischen virtuellen Servern und Webanwendungen 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.

StyleBooks

February 5, 2024

StyleBooks vereinfachen die Verwaltung komplexer NetScaler Konfigurationen für Ihre Anwendungen. Ein StyleBook ist eine Vorlage, mit der Sie NetScaler-Konfigurationen erstellen und verwalten können. Sie können ein StyleBook zum Konfigurieren einer bestimmten Funktion von NetScaler erstellen, oder Sie können ein StyleBook entwerfen, um Konfigurationen für eine Bereitstellung von Unternehmensanwendungen wie Microsoft Exchange oder Lync zu erstellen.

StyleBooks passen gut zu den Prinzipien von Infrastructure-as-Code, die von DevOps-Teams praktiziert werden, wo Konfigurationen deklarativ und versionsgesteuert sind. Die Konfigurationen werden ebenfalls wiederholt und 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 Status"der Konfiguration konzentrieren und nicht auf die Schritt-für-Schritt-Anweisungen, wie Sie diese auf einer bestimmten NetScaler Instanz erreichen können. NetScaler Application Delivery Management (ADM) berechnet den Unterschied zwischen dem vorhandenen Status auf einem NetScaler und dem gewünschten Status, den Sie angegeben haben, 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 NetScaler 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 Namespace 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 Namespace), um dieses eindeutige Zeichen zu erhalten. Mit dem Versionsupdate können Sie auch mehrere Versionen desselben StyleBook verwalten.
- **Composable**: Nachdem ein StyleBook definiert wurde, kann das StyleBook als Einheit zum Erstellen anderer StyleBooks verwendet werden. Sie können vermeiden, gängige Konfigurations-

muster zu wiederholen. Es ermöglicht Ihnen auch, Standardbausteine in Ihrer Organisation festzulegen. Da StyleBooks versioniert sind, führen Änderungen an vorhandenen StyleBooks zu neuen StyleBooks, wodurch sichergestellt wird, dass abhängige StyleBooks niemals unbeabsichtigt beschädigt werden.

- **App-Centric**: StyleBooks können verwendet werden, um die NetScaler-Konfiguration einer vollständigen Anwendung zu definieren. Die Konfiguration der Anwendung kann mithilfe von Parametern abstrahiert werden. Daher können Benutzer, die Konfigurationen von einem StyleBook aus erstellen, mit einer einfachen Oberfläche interagieren, die darin besteht, einige Parameter auszufüllen, um eine möglicherweise komplexe NetScaler-Konfiguration zu erstellen. Konfigurationen, die aus StyleBooks erstellt werden, sind nicht an die Infrastruktur gebunden. Eine einzelne Konfiguration kann somit auf einem oder mehreren NetScalern bereitgestellt und auch zwischen Instanzen verschoben werden.
- **Automatisch generierte Benutzeroberfläche**: NetScaler ADM generiert automatisch UI-Formulare, die zum Ausfüllen der Parameter des StyleBook verwendet werden, wenn die Konfiguration über die NetScaler ADM GUI erfolgt. StyleBook-Autoren müssen keine neue GUI-Sprache erlernen oder Benutzeroberflächenseiten und -formulare separat erstellen.
- **API-gesteuert**: Alle Konfigurationsvorgänge werden mithilfe der NetScaler 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 StyleBooks zur Laufzeit ermitteln.

Sie können ein StyleBook verwenden, um mehrere Konfigurationen zu erstellen. Jede Konfiguration wird als Config Pack 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 NetScaler-Instanz ausführen. Diese Konfiguration wird als Konfigurationspaket gespeichert. Sie können dasselbe StyleBook verwenden, um eine weitere Konfiguration mit anderen Werten zu erstellen und sie auf derselben oder einer anderen NetScaler-Instanz auszuführen. Für diese Konfiguration wird ein neues Konfigurationspaket erstellt. Ein Konfigurationspaket wird sowohl auf NetScaler ADM als auch auf der NetScaler-Instanz gespeichert, auf der die Konfiguration ausgeführt wird.

Sie können entweder Standard-StyleBooks verwenden, die im Lieferumfang von NetScaler ADM enthalten sind, um Konfigurationen für Ihre Bereitstellung zu erstellen, oder eigene StyleBooks entwerfen und in NetScaler ADM importieren. Sie können die StyleBooks verwenden, um Konfigurationen entweder mithilfe der NetScaler 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

AnwendungsSicherheitsdashboard

February 5, 2024

Das **App Security-Dashboard** bietet Ihnen einen Überblick über die Sicherheitsmetriken für die entdeckten/lizenzierten Anwendungen. In diesem Dashboard werden die Sicherheitsangriffsinformationen für die erkannten/lizenzierten Anwendungen angezeigt, z. B. Sync-Angriffe, Small-Flod-Angriffe, DNS-Flood-Angriffe usw.

So zeigen Sie die Sicherheitsmetriken im App-Sicherheitsdashboard an:

1. Navigieren Sie zu **Sicherheit** > **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 Kritikalität von Angriffen auf die Anwendung angibt. Je kritischer die Angriffe auf eine Anwendung sind, desto höher ist der Bedrohungsindex für diese Anwendung. Die Werte reichen von 1 bis 7.

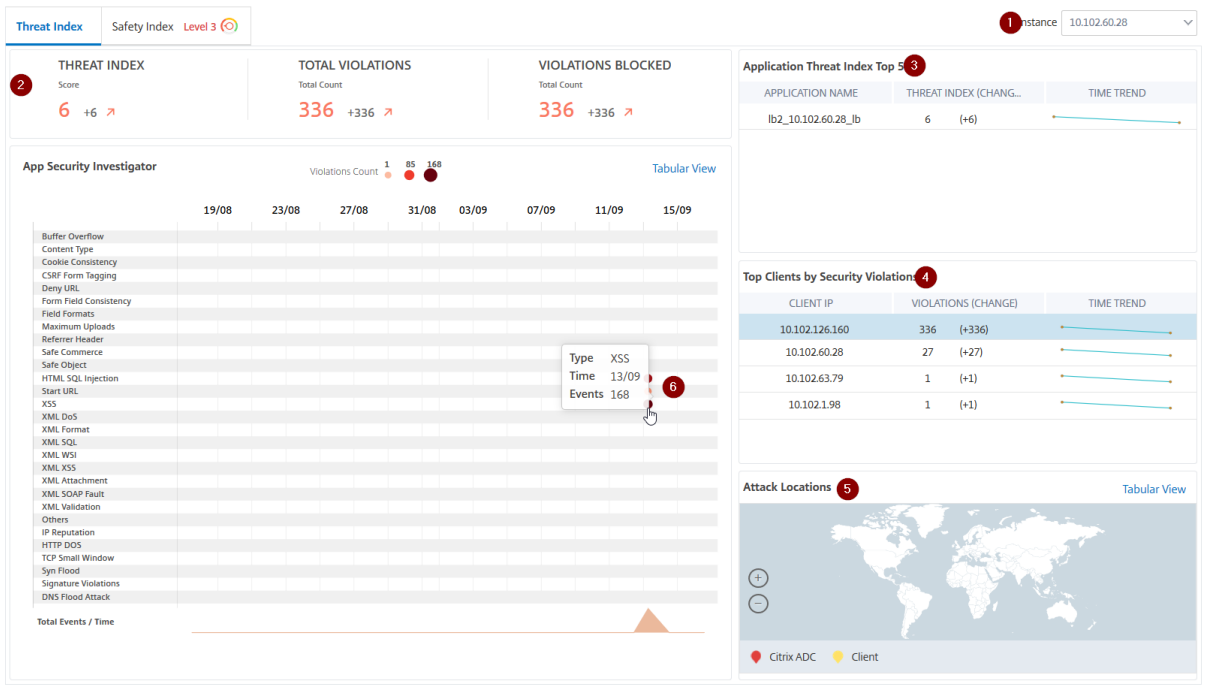
     Der Bedrohungsindex basiert auf Angriffsinformationen. Die angriffsbezogenen Informationen wie Verstoßtyp, Angriffskategorie, Standort und Client-Details geben einen Einblick in die Angriffe auf die Anwendung. Verstöße werden nur dann an NetScaler ADM gesendet, wenn eine Verletzung oder ein Angriff auftritt. Eine große Anzahl von Sicherheitslücken und Sicherheitslücken führt zu einem hohen Bedrohungsindexwert.

   - **Sicherheitsindex**. Ein einstelliges Bewertungssystem, das angibt, wie sicher Sie die NetScaler-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 NetScaler -Systems. Für einen hohen Sicherheitsindex müssen beide Konfigurationen stark sein. Wenn beispielsweise strenge Prüfungen der Anwendungsfirewall vorhanden sind, aber Sicherheitsmaßnahmen für NetScaler-Systeme, z. B. ein sicheres Kennwort für den `nsroot` Benutzer, nicht bereitgestellt werden, wird Anwendungen ein niedriger Sicherheitsindexwert zugewiesen.

Sie können die im **App Security Investigator**gemeldeten Diskrepanzen einsehen.

Bedrohungsindizes



1 - Zeigt die IP-Adresse der NetScaler-Instanz an, für die Sie Details anzeigen können.

2 —Zeigt Details wie den Bedrohungsindex, die Gesamtzahl der aufgetretenen Verstöße und die Gesamtzahl der blockierten Verstöße an.

3 - Zeigt den virtuellen Server der ausgewählten Instanz an.

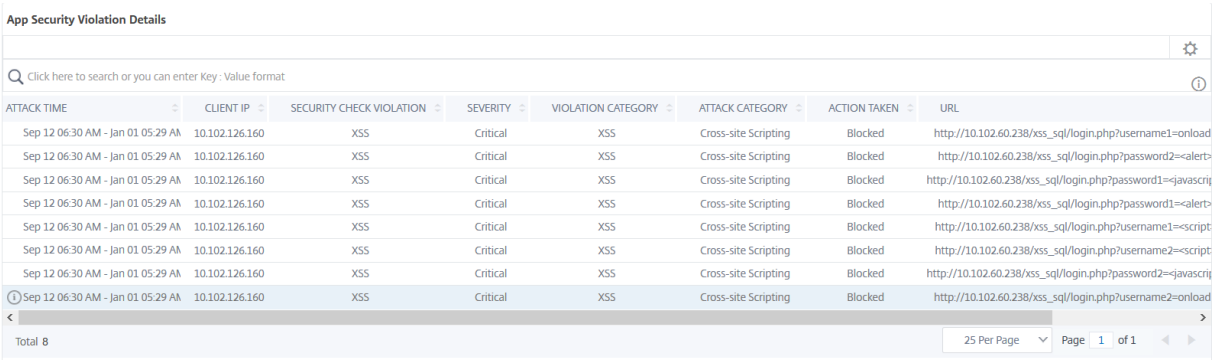
4 - Zeigt die Sicherheitsverletzungen basierend auf Clients an. Das Diagramm App Security Investigator wird für jeden Client angezeigt. Sie können auf jede Client-IP klicken, um die Ergebnisse anzuzeigen.

5 - Zeigt die Verstöße in Kartenansicht und Tabellenansicht an.

6 - Zeigt die Details des Verstoßes 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 Cross-Site-Scripting (Cross-Site-Skript) anzeigen möchten, klicken Sie auf das Diagramm, das für **XSS** in **App Security Investigator**ausgefüllt ist.

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.

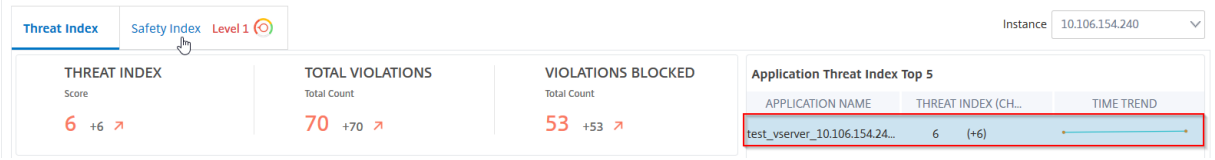
Sicherheitsindex Details

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 durchführen.

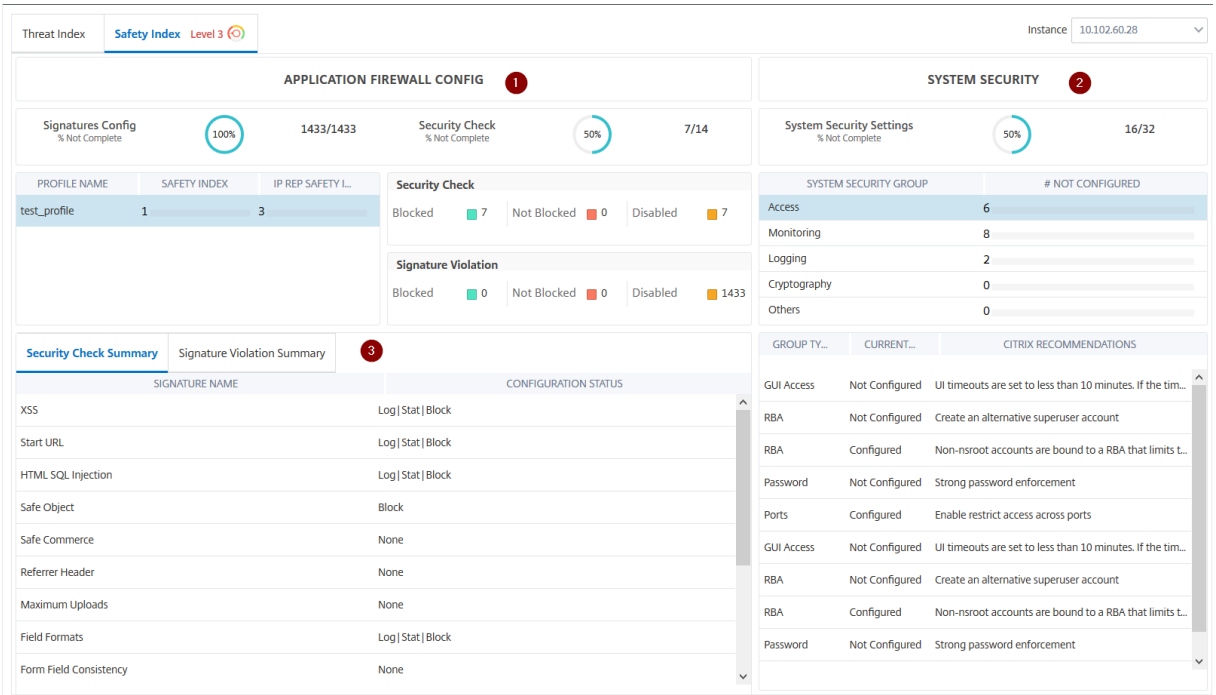
Die Zusammenfassung des Sicherheitsindex gibt Ihnen Informationen über die Wirksamkeit der folgenden Sicherheitskonfigurationen:

- **Konfiguration der Anwendungsfirewall**. Zeigt an, wie viele Signatur- und Sicherheitseinheiten nicht konfiguriert sind.
- **NetScaler 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 aktuellen Status und zu den Empfehlungen von Citrix zu erhalten.

3 - Zeigt die Zusammenfassung für Sicherheitsprüfung und Signaturverletzung an.

Sie können auch eine Zusammenfassung der Bedrohungsumgebung anzeigen, indem Sie die **WAF-Sicherheitsverletzungen** für virtuelle Server aktivieren und dann zu **Sicherheit** > **Sicherheitsverletzungen**navigieren.

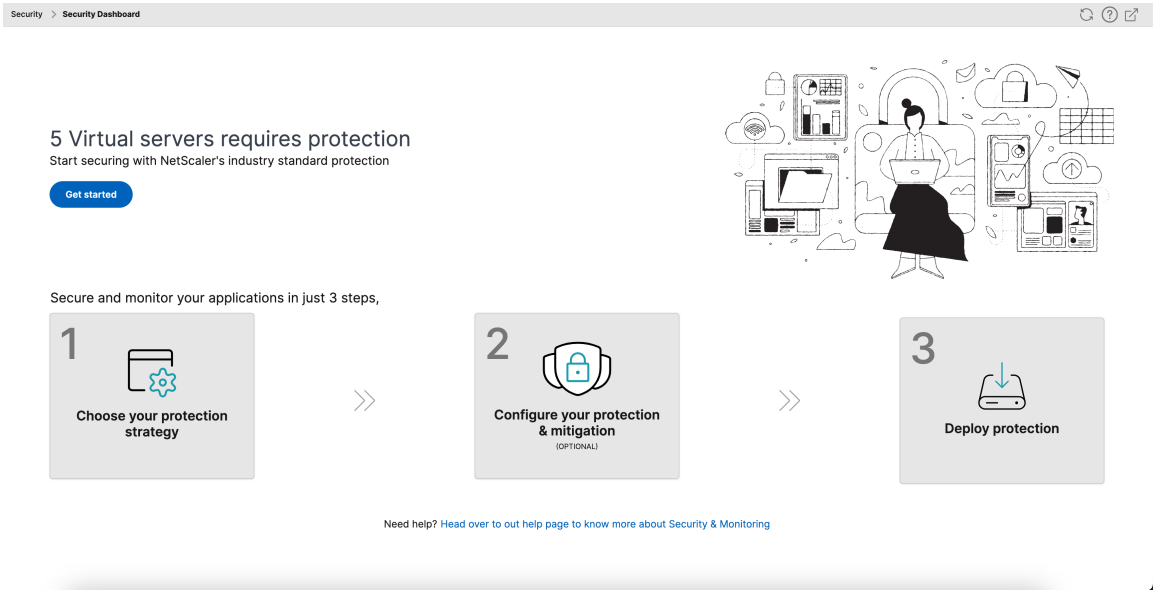
Einheitliches Sicherheitsdashboard

February 5, 2024

Das **Unified Security** Dashboard ist ein Dashboard mit einem einzigen Bereich, in dem Sie Schutzmaßnahmen konfigurieren, Analysen aktivieren und die Schutzmaßnahmen in Ihrer Anwendung bereitstellen können. In diesem Dashboard können Sie aus verschiedenen Vorlagenoptionen wählen und den gesamten Konfigurationsprozess in einem einzigen Workflow abschließen. Navigieren Sie zunächst zu **Sicherheit > Sicherheitsdashboard** und klicken Sie dann auf **Anwendung verwalten**. Auf der Seite **„Anwendung verwalten** “können Sie Details zu Ihren gesicherten und ungesicherten Anwendungen einsehen.

Hinweis:

- Wenn Sie ein neuer Benutzer sind oder keinen Schutz über StyleBooks oder direkt auf NetScaler-Instanzen konfiguriert haben, wird die folgende Seite angezeigt, nachdem Sie auf Security > **Security**Dashboard geklickt haben.

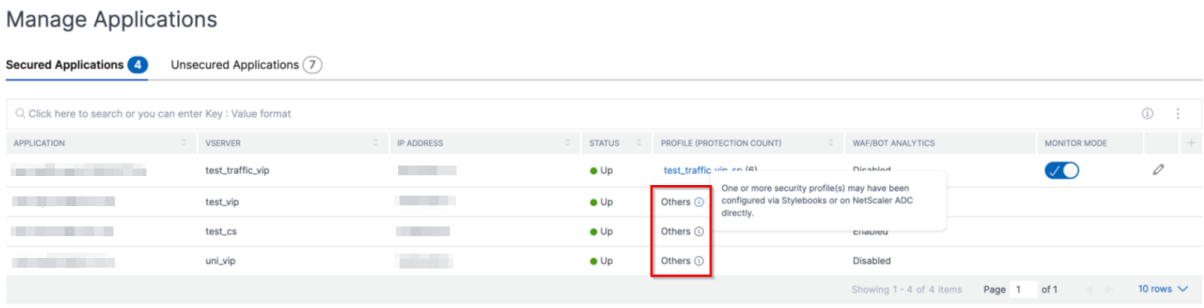


- Sie können die Gesamtzahl der virtuellen Server anzeigen, die geschützt werden müssen. Klicken Sie auf **Erste Schritte**, um Details in **Unsecured Applications**anzuzeigen.
- Die für die Konfiguration von Schutzmaßnahmen in Frage kommenden virtuellen Servertypen sind Load Balancing und Content Switching.

Gesicherte Anwendungen

Sie können Details anzeigen, nachdem Sie die Schutzmaßnahmen mit dem einheitlichen Sicherheitsdashboard konfiguriert haben. Weitere Informationen finden Sie unter Schutzmaßnahmen für ungesicherte Anwendungen konfigurieren.

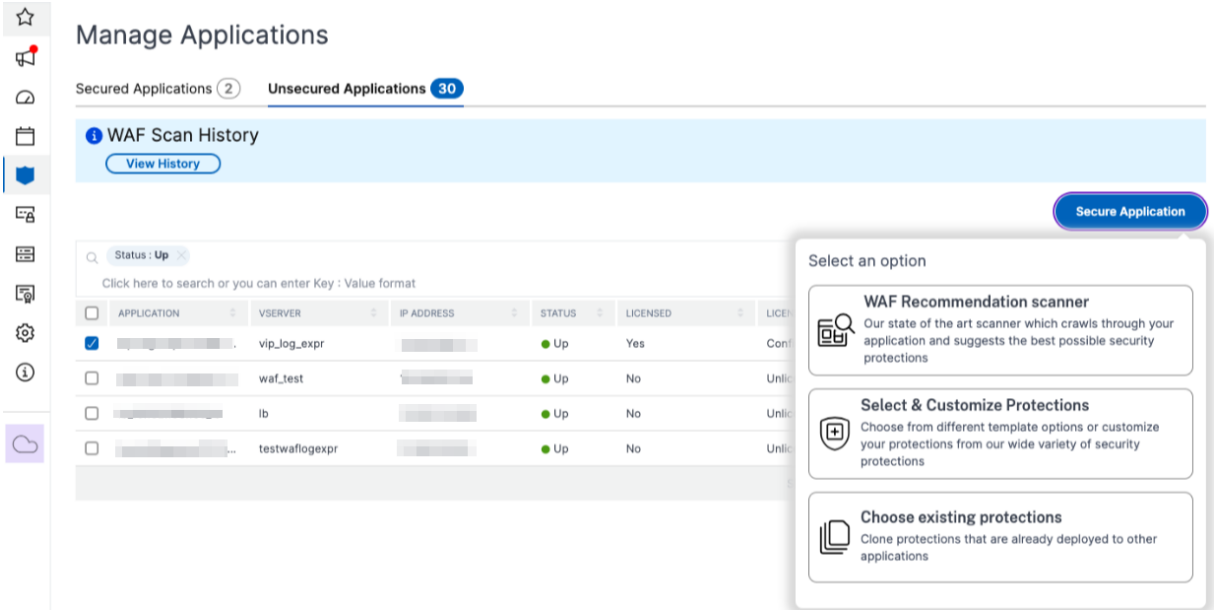
Wenn Sie bereits Schutzmaßnahmen direkt auf den NetScaler-Instanzen oder über StyleBooks konfiguriert haben, können Sie die Anwendungen auf der Registerkarte **Gesicherte Anwendungen** anzeigen, die unter **Profil** als **Andere** markiert sind.



Schutzmaßnahmen für ungesicherte Anwendungen konfigurieren

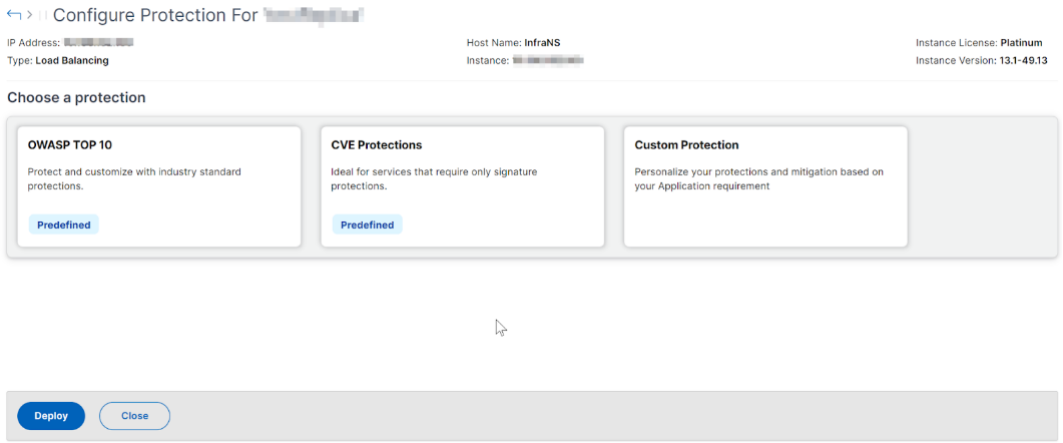
> **Hinweis:**
>
> Die maximale Anzahl unterstützter Konfigurationsentitäten (Regeln) in der Blockliste ist 32.

Wählen Sie auf der Registerkarte **Unsichere Anwendungen** eine Anwendung aus und klicken Sie auf **Sichere Anwendung**.



Sie können eine der folgenden Optionen auswählen, um Ihre Anwendung zu schützen:

- **WAF-Empfehlungsscanner**—Mit dieser Option können Sie einen Scan für Ihre Anwendung ausführen. Basierend auf bestimmten Parametern des Scans schlägt Ihnen das Ergebnis die Schutzmaßnahmen für Ihre Anwendung vor. Sie könnten erwägen, diese Empfehlungen anzuwenden.
- **Schutzmaßnahmen auswählen und anpassen**—Mit dieser Option können Sie aus verschiedenen Vorlagenoptionen auswählen oder Ihre Schutzmaßnahmen anpassen und bereitstellen.



  - **OWASP Top 10** —Eine vordefinierte Vorlage, die den branchenüblichen Schutz vor den Top-10-Sicherheitsrisiken von OWASP bietet. Weitere Informationen finden Sie unter `https://owasp.org/www-project-top-ten/`.
  - **CVE-Schutz** —Sie können den Signatursatz aus der Liste der vorkonfigurierten Signaturregeln erstellen, die nach bekannten Schwachstellenkategorien klassifiziert sind. Sie können Signaturen auswählen, um die Protokollierung oder Blockierung von Aktionen zu konfigurieren, wenn ein Signaturmuster dem eingehenden Datenverkehr entspricht. Die Protokollnachricht enthält die Details der Sicherheitsanfälligkeit.
  - **Benutzerdefinierter Schutz** —Wählen Sie die Schutzmaßnahmen aus und setzen Sie sie entsprechend Ihren Anforderungen ein.

- **Vorhandene Schutzmaßnahmen auswählen** —Mit dieser Option werden die Schutzmaßnahmen geklont, die in einer vorhandenen Anwendung bereitgestellt werden. Wenn Sie dieselben Schutzmaßnahmen für eine andere Anwendung bereitstellen möchten, können Sie diese Option auswählen und sie unverändert für eine andere Anwendung bereitstellen. Sie können diese Option auch als Vorlage auswählen, die Schutzmaßnahmen ändern und dann bereitstellen.

WAF-Empfehlungsscanner

> **Hinweis:**
>
> - Sie können jeweils nur einen Scan für eine Anwendung ausführen. Um einen neuen Scan für dieselbe Anwendung oder eine andere Anwendung zu starten, müssen Sie warten, bis der vorherige Scan abgeschlossen ist.
> - Sie können auf **Verlauf anzeigen** klicken, um den Verlauf und den Status der vergangenen Scans anzuzeigen. Sie können auch auf **Bericht anzeigen** klicken und dann die Empfehlungen später anwenden.

Voraussetzungen:

- Die NetScaler-Instanz muss 13.0 41.28 oder höher (für Sicherheitsüberprüfungen) und 13.0 oder höher (für Signaturen) sein.
- Muss die Premium-Lizenz haben.
- Muss der virtuelle Lastausgleichsserver sein.

Um mit dem WAF-Empfehlungsscan zu beginnen, müssen Sie die folgenden Informationen angeben:

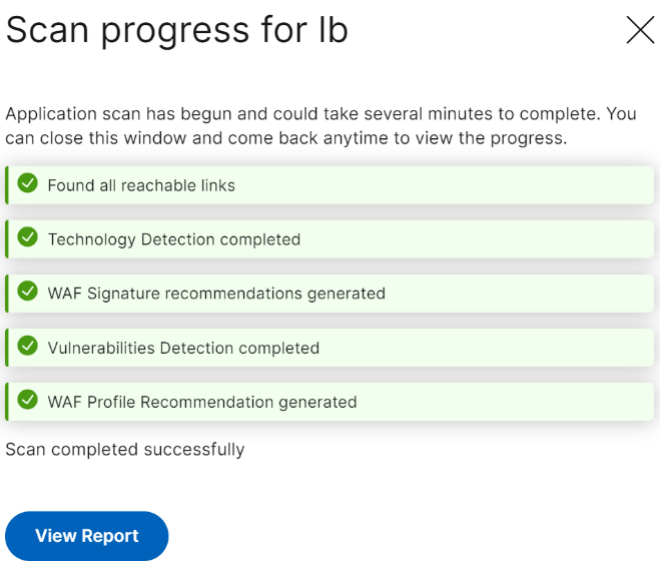
1. Unter **Scanparameter**:
    - **Domain name** —Geben Sie eine gültige, zugängliche IP-Adresse oder den öffentlich erreichbaren Domänennamen an, der der Anwendung zugeordnet ist. Beispiel: `www.example.com`.
    - **HTTP-/HTTPS-Protokoll** —Wählen Sie das Protokoll der Anwendung aus.
    - **Traffic Timeout** —Die Wartezeit (in Sekunden) für eine einzelne Anfrage während des Scans. Der Wert muss größer als 0 sein.
    - **URL, von der aus der Scan gestartet** werden soll —Die Startseite der Anwendung, von der aus der Scan gestartet werden soll. Beispiel: `https://www.example.com/home`. Die URL muss eine gültige IPv4-Adresse sein. Wenn die IP-Adressen privat sind, müssen Sie sicherstellen, dass die private IP-Adresse von der NetScaler ADM Management-IP aus zugänglich ist.
    - **Anmelde-URL** —Die URL, an die die Anmeldedaten zur Authentifizierung gesendet werden. In HTML wird diese URL allgemein als Aktions-URL bezeichnet.
    - **Authentifizierungsmethode** —Wählen Sie die unterstützte Authentifizierungsmethode (formularbasiert oder kopfbasiert) für Ihre Anwendung aus.
        - Für die formularbasierte Authentifizierung muss ein Formular mit den Anmeldeinformationen an die Anmelde-URL gesendet werden. Diese Anmeldeinformationen müssen in Form von Formularfeldern und ihren Werten vorliegen. Die Anwendung teilt dann das Sitzungscookie, das zur Aufrechterhaltung der Sitzungen während des Scans verwendet wird.
        - Die Header-basierte Authentifizierung erfordert den Authentication-Header und seinen Wert im Header-Abschnitt. Der Authentifizierungsheader muss einen gültigen Wert haben und wird verwendet, um Sitzungen während des Scans aufrechtzuerhalten. Die Formularfelder sollten für Header-basierte Felder leer gelassen werden.
    - **Anforderungsmethode** —Wählen Sie die HTTP-Methode, die beim Senden von Formulardaten an die Anmelde-URL Die zulässigen Anforderungsmethoden sind **POST**, **GET**und **PUT**.

- **Formularfelder** —Geben Sie die Formulardaten an, die an die Anmelde-URL gesendet werden sollen Formularfelder sind nur erforderlich, wenn Sie die formularbasierte Authentifizierung auswählen. Sie müssen in den Schlüssel-Wert-Paaren angeben, wobei **Feldname** der Schlüssel und **Feldwert der Wert** ist. Stellen Sie sicher, dass alle Formularfelder, die für die Anmeldung erforderlich sind, korrekt hinzugefügt wurden, einschließlich Kennwörter. Die Werte werden verschlüsselt, bevor sie in der Datenbank gespeichert werden. Sie können auf **Hinzufügen** klicken, um mehrere Formularfelder hinzuzufügen. Zum Beispiel **Feldname** —Benutzername und **Feldwert** —admin.
- **Abmelde-URL** —Geben Sie die URL an, die die Sitzung nach dem Zugriff beendet. Beispiel: `https://www.example.com/customer/logout`.

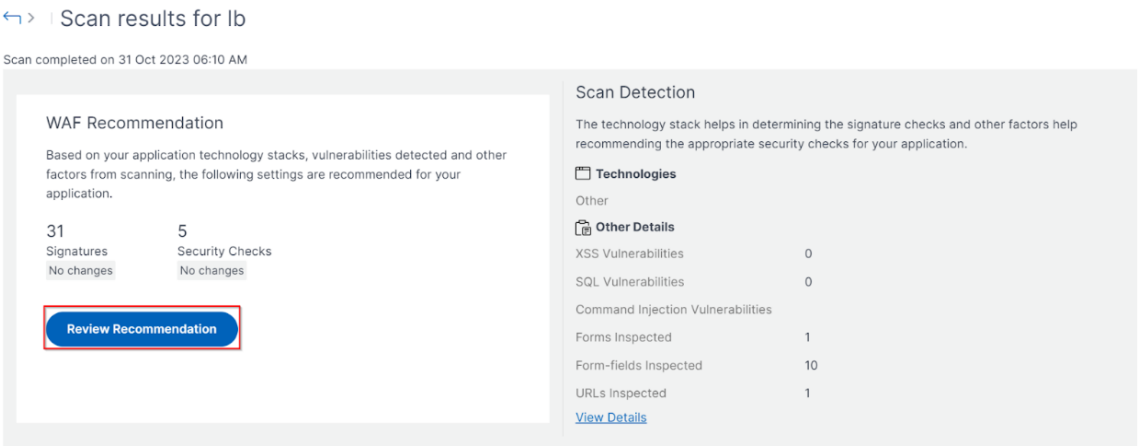
2. Unter **Scankonfigurationen**:

   - **Zu prüfende Sicherheitslücken** —Wählen Sie die Sicherheitslücken aus, die der Scanner erkennen soll. Derzeit wird dies für Verstöße gegen SQL Injection und Cross-Site-Skripting durchgeführt. Standardmäßig sind alle Verstöße ausgewählt. Nach Auswahl der Schwachstellen werden diese Angriffe auf die Anwendung simuliert, um die potenzielle Sicherheitsanfälligkeit zu melden. Es wird empfohlen, diese Erkennung zu aktivieren, die sich nicht in der Produktionsumgebung befindet. Alle anderen Sicherheitslücken werden ebenfalls gemeldet, ohne diese Angriffe auf die Anwendung zu simulieren.
   - **Größenbeschränkung der Antwort** —Die maximale Grenze für die Antwortgröße. Antworten, die über den genannten Wert hinausgehen, werden nicht gescannt. Das empfohlene Limit liegt bei 10 MB (1000000 Byte).
   - **Parallelität** von Anfragen —Die Gesamtzahl der parallel an die Webanwendung gesendeten Anforderungen.

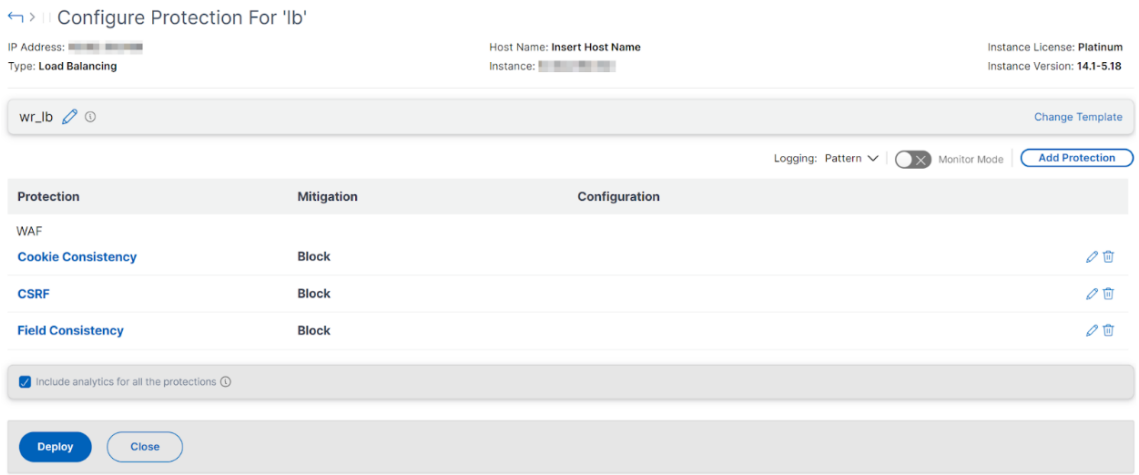
3. Die Konfiguration der WAF-Scaneinstellungen ist abgeschlossen. Sie können auf **Scan starten** klicken, um den Scanvorgang zu starten, und warten, bis der Vorgang abgeschlossen ist. Nachdem der Scan abgeschlossen ist, klicken Sie auf **Bericht anzeigen**.



4. Klicken Sie auf der Seite mit den Scanergebnissen auf **Empfehlung überprüfen**.



5. Überprüfen Sie die Schutzmaßnahmen oder bearbeiten/fügen Sie weitere Schutzmaßnahmen hinzu und klicken Sie auf **Bereitstellen**.

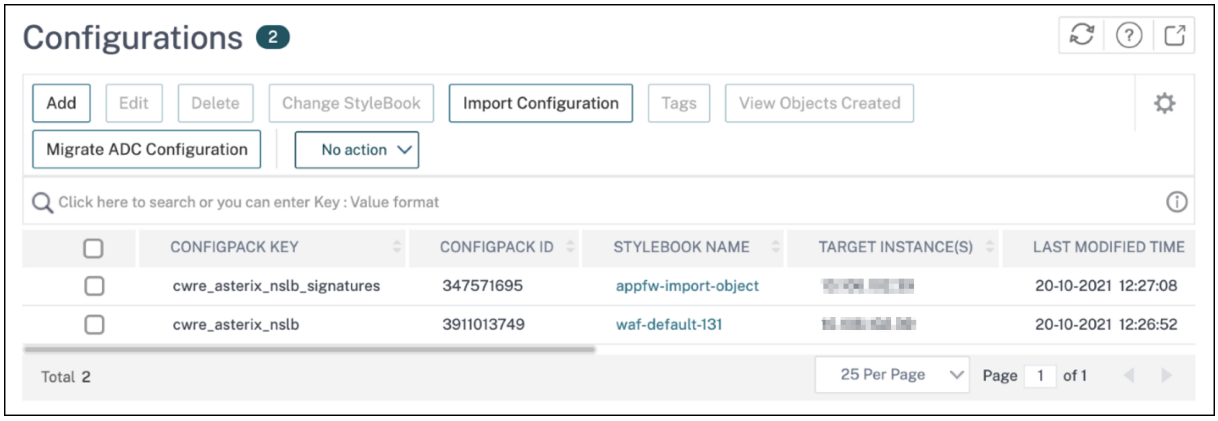


Wenn Sie Sicherheitsüberprüfungen erfolgreich durchführen:

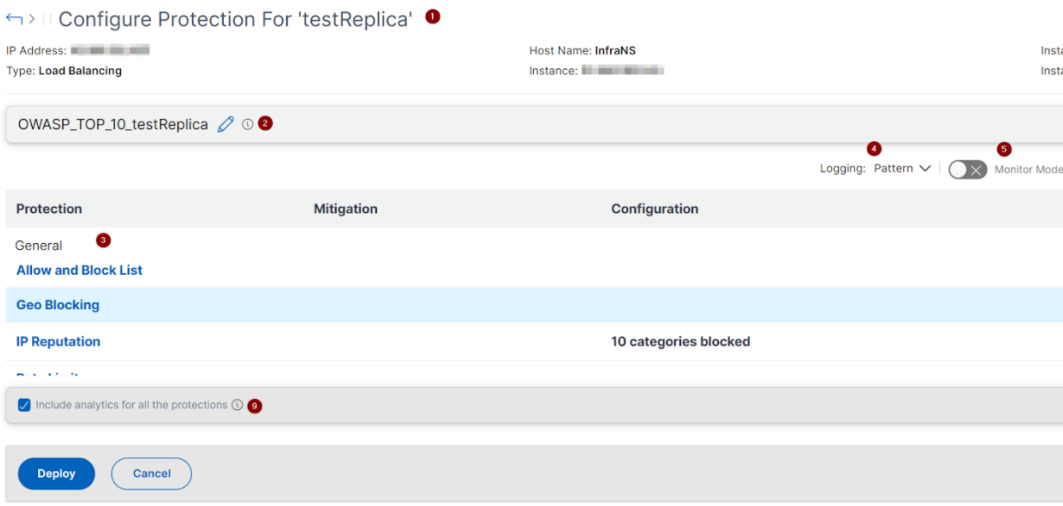
- Die Konfiguration wird je nach Version über StyleBooks auf die NetScaler-Instanz angewendet.
  - Für NetScaler 13.0 wird StyleBook `unified-appsec-protection-130` verwendet.
  - Für NetScaler 13.1 wird StyleBook `unified-appsec-protection-131` verwendet.
  - Für NetScaler 14.1 wird StyleBook `unified-appsec-protection-141` verwendet.
- Das Profil `Appfw` wird auf Ihrem NetScaler erstellt und mithilfe von `policylabel` an die Anwendung gebunden.
- Die Signaturen sind an das appfw-Profil gebunden, wenn die empfohlenen Signaturen bereits angewendet wurden.

> **Hinweis**
>
> Sicherheitsprüfungen werden in NetScaler 13.0 41.28 oder einer späteren Version unterstützt.

Sie können überprüfen, ob die WAF-Profile und -Signaturen über die Standard-StyleBooks angewendet werden, indem Sie zu **Anwendungen > Konfiguration > Config Packs**navigieren.



Schutzmaßnahmen auswählen und anpassen



Die 10 besten OWASP

1 —Stellt Informationen zur Anwendung bereit, z. B. IP-Adresse, Typ des virtuellen Servers, Lizenztyp, von welcher Instanz aus die Anwendung konfiguriert wird usw.

2 —Zeigt die ausgewählte Vorlage an. Sie können es nach Ihrer Wahl umbenennen.

3 - Zeigt die Schutzmaßnahmen an. Für einige Schutzmaßnahmen sind zusätzliche Informationen erforderlich.

4 —Zeigt den ausführlichen Logtyp an. Sie können die folgenden Optionen wählen:

- **Muster**. Protokolliert nur Verletzungsmuster.
- **Musternutzlast**. Protokolliert das Verletzungsmuster und 150 Byte zusätzliche JSON-Nutzlast.
- **Muster, Nutzlast, Header**. Protokolliert das Verletzungsmuster, 150 Byte an zusätzlichen JSON-Nutzdaten und HTTP-Header-Informationen.

5 - Ermöglicht es Ihnen, den Monitormodus zu aktivieren. Wenn Sie den Überwachungsmodus aktivieren, wird der Datenverkehr nur protokolliert und die Schadensbegrenzungen werden nicht aktiviert.

6 —Ermöglicht es Ihnen, weitere Schutzmaßnahmen hinzuzufügen. Klicken Sie auf **Schutzmaßnahmen hinzufügen** und überprüfen Sie, ob Sie welche hinzufügen möchten.

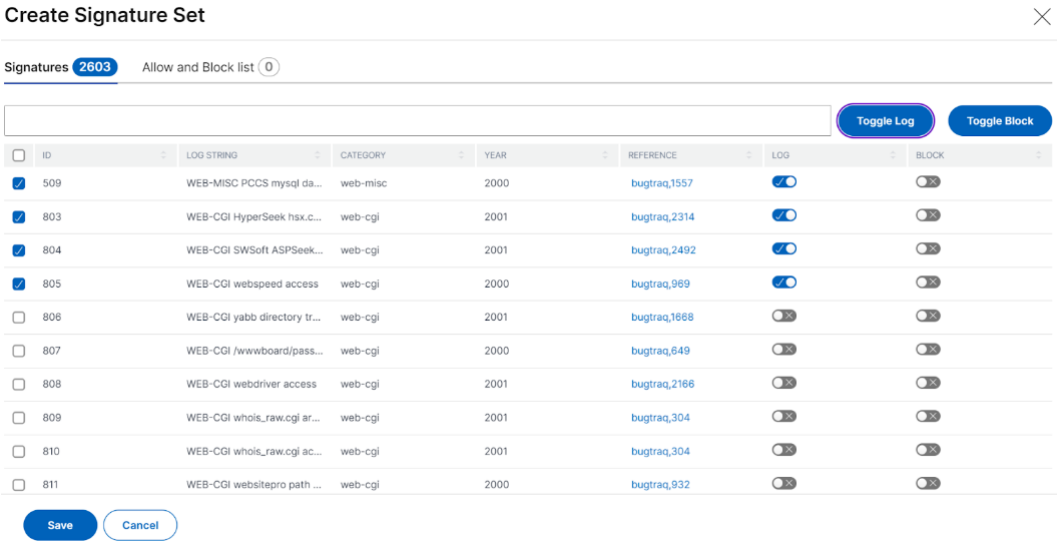
7 —Ermöglicht die Auswahl einer neuen Vorlage mithilfe der Option Vorlage ändern.

8 —Ermöglicht es Ihnen, den Schutz zu bearbeiten oder zu löschen.

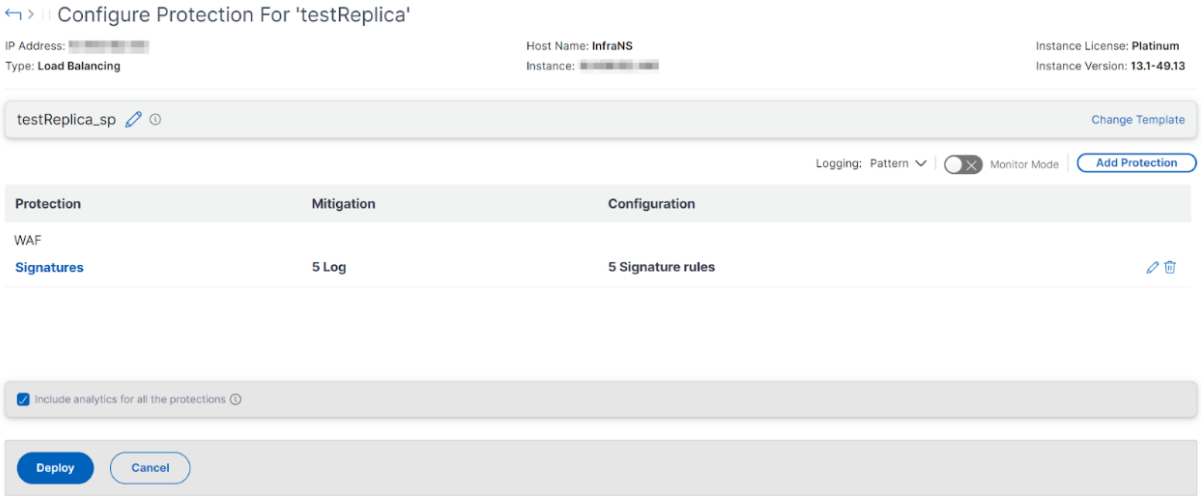
9 —Aktiviert Analysen für die von Ihnen ausgewählten Schutzmaßnahmen. Diese Option ist standardmäßig ausgewählt. Sie können Analysen für die konfigurierten Schutzmaßnahmen unter **Sicherheit > Sicherheitsverletzungen**einsehen.

Nachdem Sie die Schutzmaßnahmen konfiguriert haben, klicken Sie auf **Bereitstellen**.

CVE-Schutz Um den CVE-Schutz bereitzustellen, klicken Sie auf **CVE-Schutz erstellen**. Wählen Sie auf der Seite **Signatursatz erstellen** die Signaturen aus der Liste aus, um die Protokoll- oder Blockaktion zu konfigurieren, und klicken Sie dann auf **Speichern**.

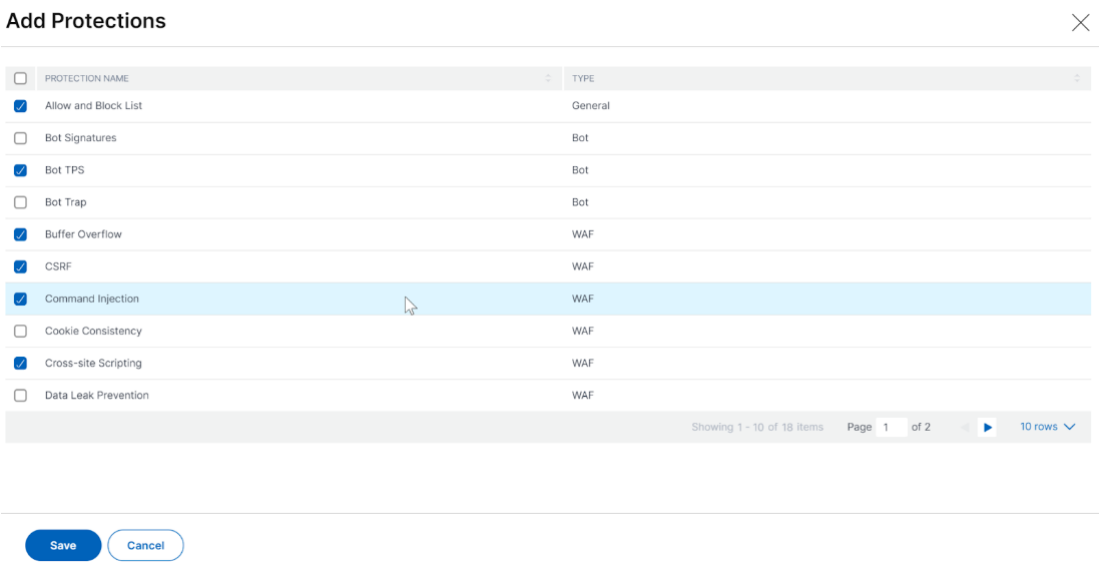


Nachdem Sie auf **Speichern**geklickt haben, können Sie die Signaturen anzeigen, die der Konfigurationsseite hinzugefügt wurden.



Sie können auch auf **Schutz hinzufügen** klicken, um der Anwendung weitere Schutzmaßnahmen hinzuzufügen. Nachdem Sie alle Schutzmaßnahmen konfiguriert haben, klicken Sie auf **Bereitstellen**.

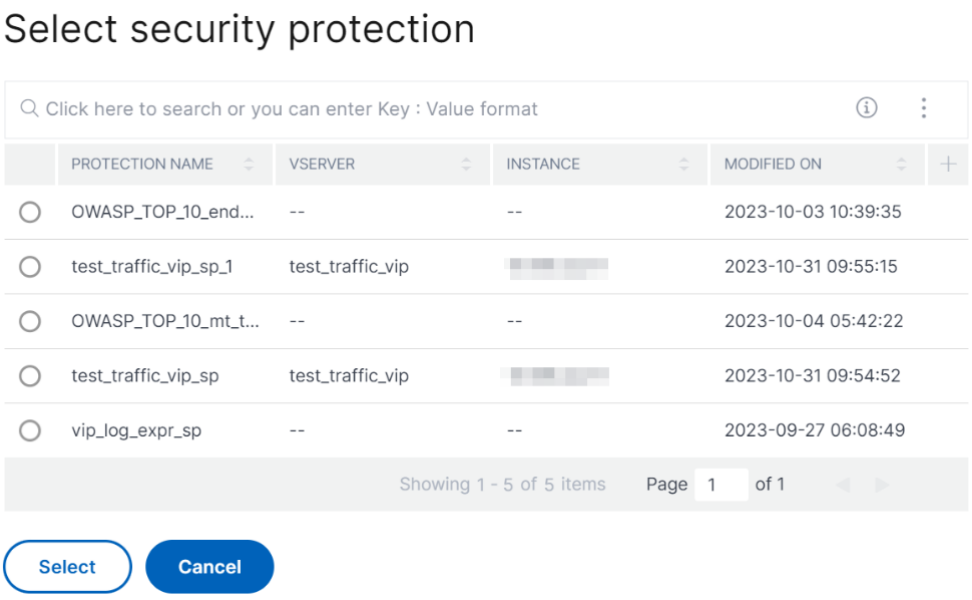
Benutzerdefinierter Schutz Klicken Sie auf **Neuen Schutz erstellen, um die Bereitstellung mit Schutzmaßnahmen**durchzuführen, die Ihren Anforderungen entsprechen. Wählen Sie auf der Seite **Schutzmaßnahmen hinzufügen** die Schutzmaßnahmen aus, die Sie bereitstellen möchten, und klicken Sie auf **Speichern**.



Nachdem Sie auf **Speichern**geklickt haben, überprüfen Sie die ausgewählten Schutzmaßnahmen auf der Konfigurationsseite und klicken Sie dann auf **Bereitstellen**.

Wählen Sie vorhandene Schutzmaßnahmen

Um vorhandene Schutzmaßnahmen von einer Anwendung auf eine andere anzuwenden, wählen Sie einen vorhandenen Schutz aus der Liste aus.



Nachdem Sie einen Schutz ausgewählt haben, werden die vorhandenen Schutzmaßnahmen geklont und auf der Konfigurationsseite angezeigt. Sie können je nach Anforderung Änderungen vornehmen und dann auf **Bereitstellen**klicken.

Details zu Sicherheitsverletzungen bei Anwendungen anzeigen

February 5, 2024

Webanwendungen, die dem Internet ausgesetzt sind, sind drastisch anfällig für Angriffe geworden. Mit NetScaler ADM können Sie verwertbare Details zu Verstößen visualisieren, um Anwendungen vor Angriffen zu schützen. ****Navigieren Sie zu ****Sicherheit** > Sicherheitsverstöße , um eine zentrale Lösung für Folgendes zu finden:

- Visualisieren Sie Anwendungen mit vollem Einblick in die Bedrohungsdetails, die sowohl mit WAF-Sicherheitsverletzungen als auch mit Bot-Sicherheitsverletzungen verbunden sind
- 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.

Voraussetzung

Stellen Sie sicher, dass **Metrics Collector** aktiviert ist Standardmäßig ist **Metrics Collector** auf der NetScaler-Instanz aktiviert. Weitere Informationen finden Sie unter Konfigurieren von Intelligent App Analytics.

Integration mit Splunk

February 5, 2024

Sie können NetScaler ADM jetzt in Splunk integrieren, um Analysen für Folgendes einzusehen:

- Verstöße gegen die WAF
- Bot-Verstöße
- SSL Certificate Insights

- Ereignisse und Metriken

Das Splunk-Add-on ermöglicht Ihnen:

- Kombinieren Sie alle anderen externen Datenquellen.
- Bieten Sie eine bessere Sichtbarkeit von Analysen an einem zentralen Ort.

NetScaler ADM erfasst Bot-, WAF- und SSL-Ereignisse und sendet sie regelmäßig an Splunk. Das Splunk Common Information Model (CIM) -Add-on konvertiert die Ereignisse in CIM-kompatible Daten. Als Administrator können Sie mithilfe der CIM-kompatiblen Daten die Ereignisse im Splunk-Dashboard einsehen.

Für eine erfolgreiche Integration müssen Sie:

- Splunk für den Empfang von Daten von NetScaler ADM konfigurieren
- NetScaler ADM so konfigurieren, dass Daten nach Splunk exportiert werden
- Dashboards in Splunk anzeigen

Splunk für den Empfang von Daten von NetScaler ADM konfigurieren

In Splunk müssen Sie Folgendes machen:

1. Splunk HTTP Event Collector-Endpunkt einrichten und ein Token generieren
2. Splunk Common Information Model (CIM)-Add-on installieren
3. Installieren Sie den CIM-Normalizer (gilt nur für WAF- und Bot-Insights)
4. Beispieldashboard in Splunk vorbereiten

Splunk HTTP Event Collector-Endpunkt einrichten und ein Token generieren

Sie müssen zuerst den HTTP-Event-Collector in Splunk einrichten. Dieses Setup ermöglicht die Integration zwischen ADM und Splunk, um die Daten zu senden. Als Nächstes müssen Sie in Splunk ein Token generieren, um:

- Aktivieren Sie die Authentifizierung zwischen ADM und Splunk.
- Empfangen Sie Daten über den Event Collector-Endpunkt.

1. Melden Sie sich bei Splunk an.
2. Navigieren Sie zu **Einstellungen > Dateneingaben > HTTP-Event-Collector** und klicken Sie auf **Neu hinzufügen**.
3. Geben Sie die folgenden Parameter an:

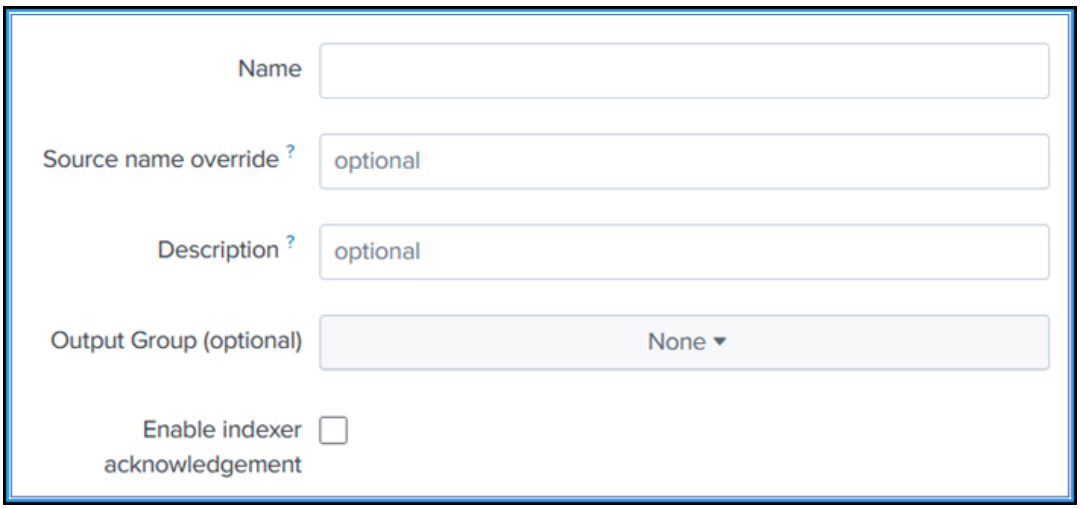
a) **Name**: Geben Sie einen Namen Ihrer Wahl an.

b) **Quellnamenüberschreibung (optional)**: Wenn Sie einen Wert festlegen, überschreibt dieser den Quellwert für den HTTP-Ereignissammler.

c) **Beschreibung (optional)**: Geben Sie eine Beschreibung an.

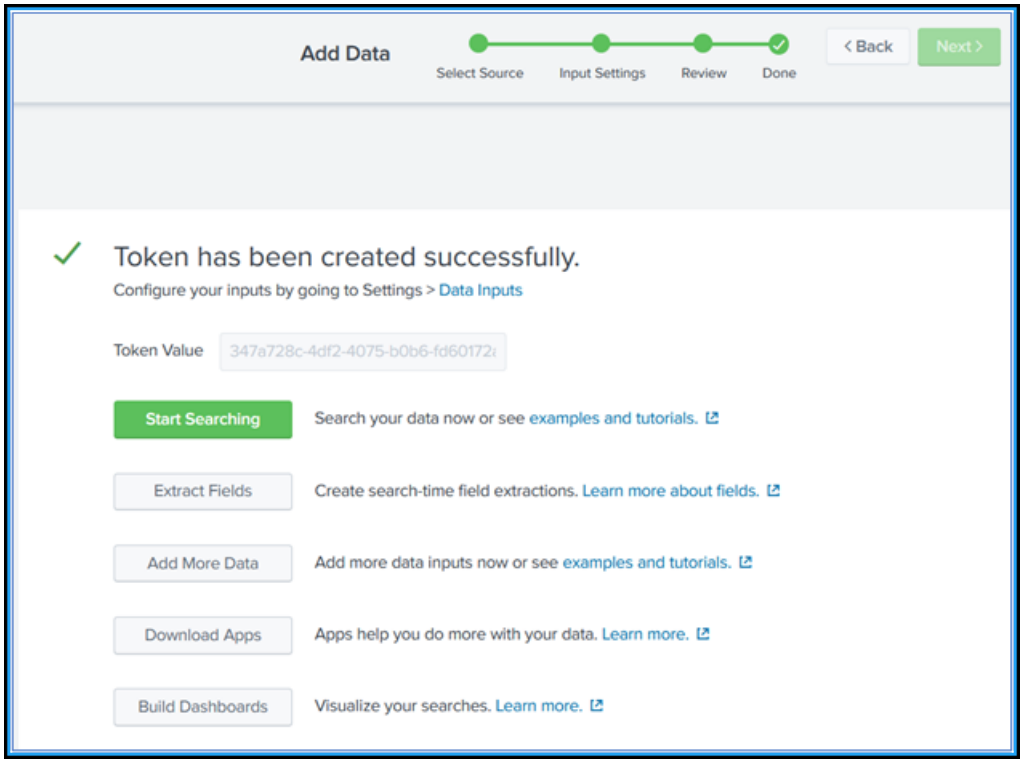
d) **Ausgabegruppe (optional)**: Standardmäßig ist diese Option als Keine ausgewählt.

e) **Indexerbestätigung aktivieren**: Diese Option ist standardmäßig nicht ausgewählt.



4. Klicken Sie auf **Weiter**.
5. Optional können Sie auf der Seite mit den **Eingabeeinstellungen zusätzliche Eingabeparameter** festlegen.
6. Klicken Sie auf **Überprüfen**, um die Eingaben zu überprüfen, und klicken Sie dann auf **Senden**.

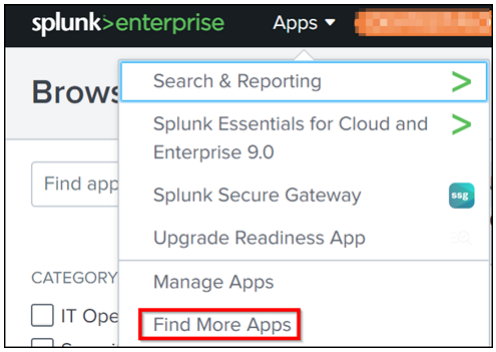
   Ein Token wird generiert. Sie müssen dieses Token verwenden, wenn Sie Details in NetScaler ADM hinzufügen.



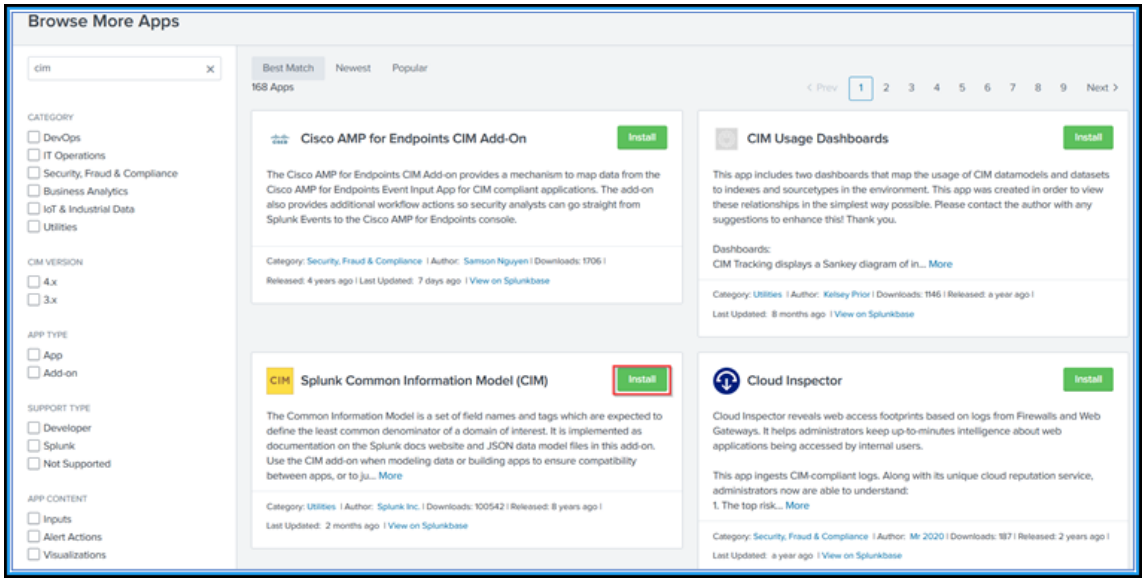
Splunk Common Information Model installieren

In Splunk müssen Sie das Splunk CIM-Add-on installieren. Dieses Add-on stellt sicher, dass die von NetScaler ADM zur Normalisierung der aufgenommenen Daten empfangenen Daten empfangen werden und einem gemeinsamen Standard entsprechen, bei dem dieselben Feldnamen und Event-Tags für äquivalente Ereignisse verwendet werden.

1. Melden Sie sich bei Splunk an.
2. Navigieren Sie zu **Apps > Weitere Apps suchen**.



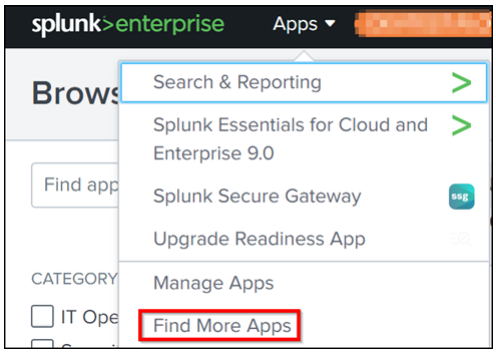
3. Geben Sie **CIM** in die Suchleiste ein und drücken **Sie die Eingabetaste**, um das **Splunk Common Information Model (CIM)** -Add-on aufzurufen, und klicken Sie auf **Installieren**.



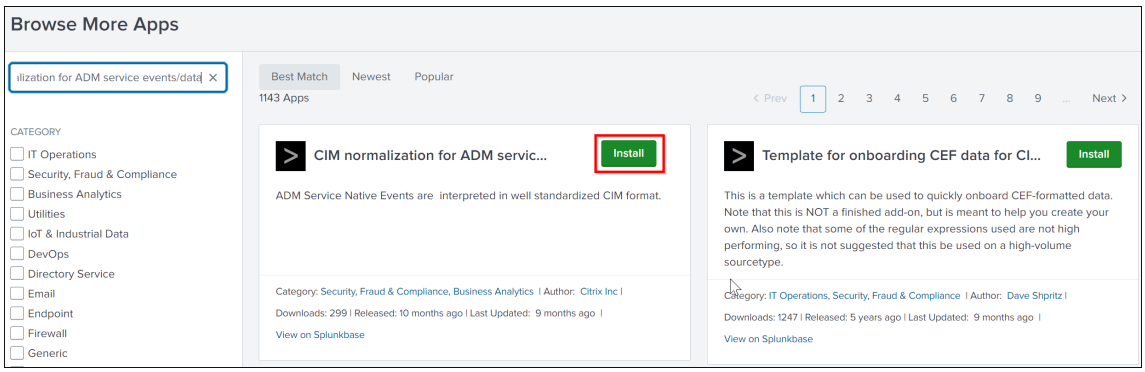
Installieren Sie den CIM-Normalizer

Der CIM-Normalizer ist ein zusätzliches Plug-in, das Sie installieren müssen, um die WAF- und Bot-Insights in Splunk anzeigen zu können.

1. Navigieren Sie im Splunk-Portal zu **Apps > Weitere Apps finden**.



2. Geben Sie **CIM-Normalisierung für ADM-Dienstereignise/Daten** in die Suchleiste ein und drücken Sie die **Eingabetaste**, um das Add-On abzurufen, und klicken Sie auf **Installieren.**



Beispieldashboard in Splunk vorbereiten

Nach der Installation von Splunk CIM müssen Sie ein Beispiel-Dashboard vorbereiten, das eine Vorlage für WAF und Bot, Einblicke in SSL-Zertifikate sowie Ereignisse und Metriken verwendet. Sie können die Dashboard-Vorlagendatei (`.tgz`) herunterladen, ihren Inhalt mit einem beliebigen Editor (z. B. Notepad) kopieren und ein Dashboard erstellen, indem Sie die Daten in Splunk einfügen.

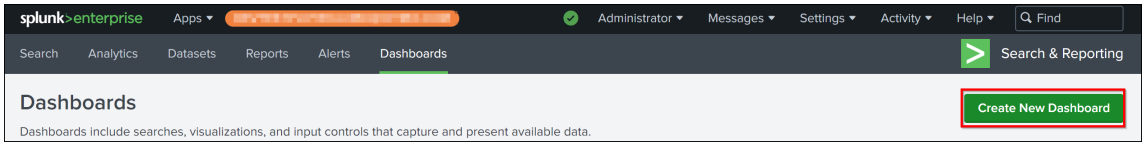
> **Hinweis:**
>
> Das folgende Verfahren zur Erstellung eines Beispiel-Dashboards gilt für alle Anwendungsfälle. Sie müssen die erforderliche `json`-Datei verwenden.

1. Melden Sie sich auf der Citrix-Downloadseite an und laden Sie das Beispiel-Dashboard herunter, das unter Beispiel-Dashboards für Endgeräte von Drittanbietern verfügbar ist.
2. Extrahieren Sie die Datei, öffnen Sie die `json`-Datei mit einem beliebigen Editor und kopieren Sie die Daten aus der Datei.

   Nach dem Extrahieren erhalten Sie drei `json`-Dateien. Benutze die:

   - `adm_splunk_security_violations.json` Datei zum Erstellen eines WAF- und Bot-Beispiel-Dashboards.
   - `adm_splunk_ssl_certificate.json` Datei zum Erstellen eines Beispiel-Dashboards für SSL-Zertifikatsinformationen.
   - `adm_splunk_events_and_metrics_history.json` Datei, um ein ADM-Ereignis- und Metrik-Dashboard zu erstellen.

3. Navigieren Sie im Splunk-Portal zu **Search & Reporting > Dashboards** und klicken Sie dann auf **Neues Dashboard erstellen**.



4. Geben Sie auf der Seite **Neues Dashboard erstellen** die folgenden Parameter an:

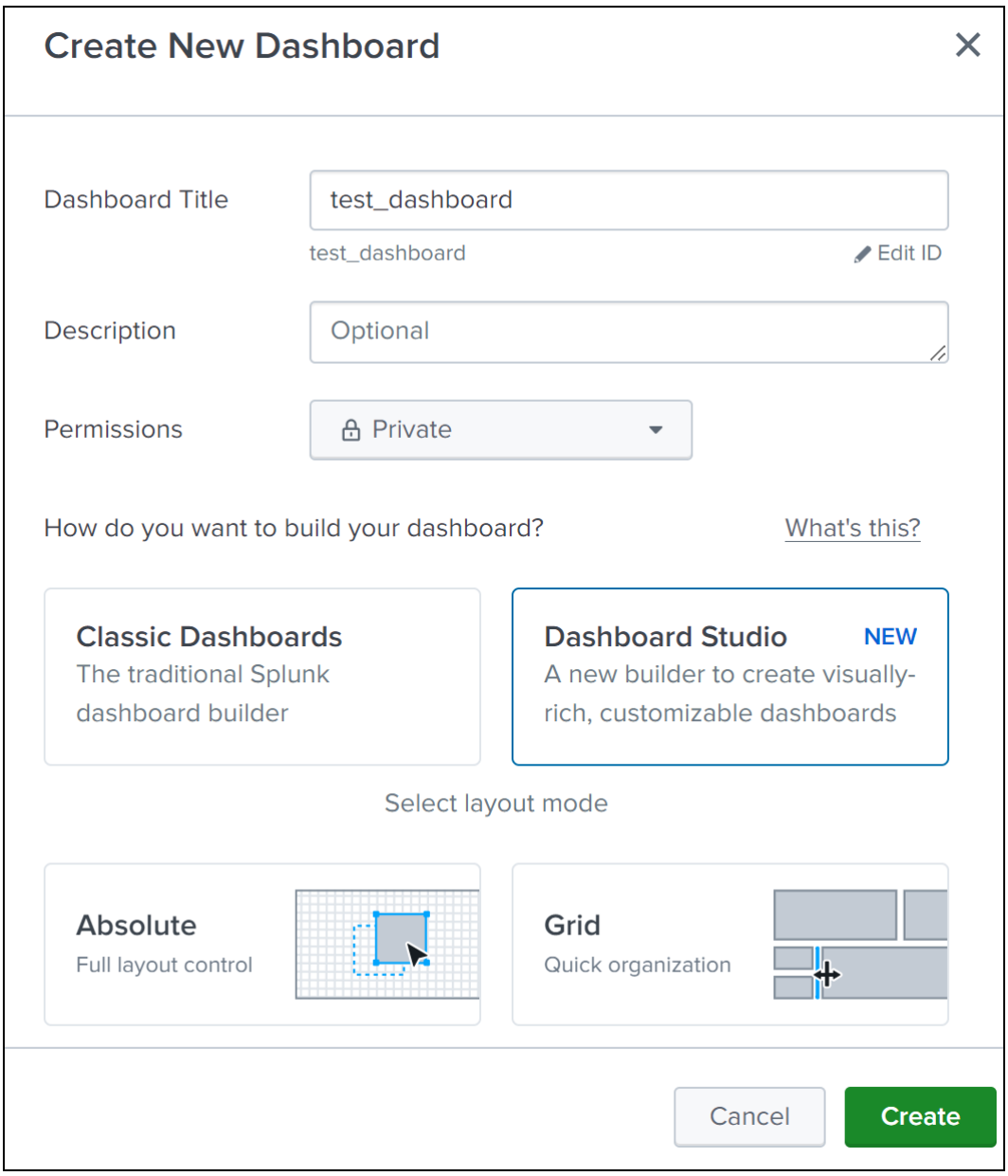
   a) **Dashboard-Titel** —Geben Sie einen Titel Ihrer Wahl ein.

   b) **Beschreibung** —Optional können Sie eine Beschreibung als Referenz angeben.

   c) **Erlaubnis** —Wählen Sie je nach Anforderung **Privat** oder **In App geteilt** aus.

   d) Wählen Sie **Dashboard Studio** aus.

   e) Wählen Sie ein beliebiges Layout (**Absolute** oder **Grid**) aus, und klicken Sie dann auf **Erstellen**.

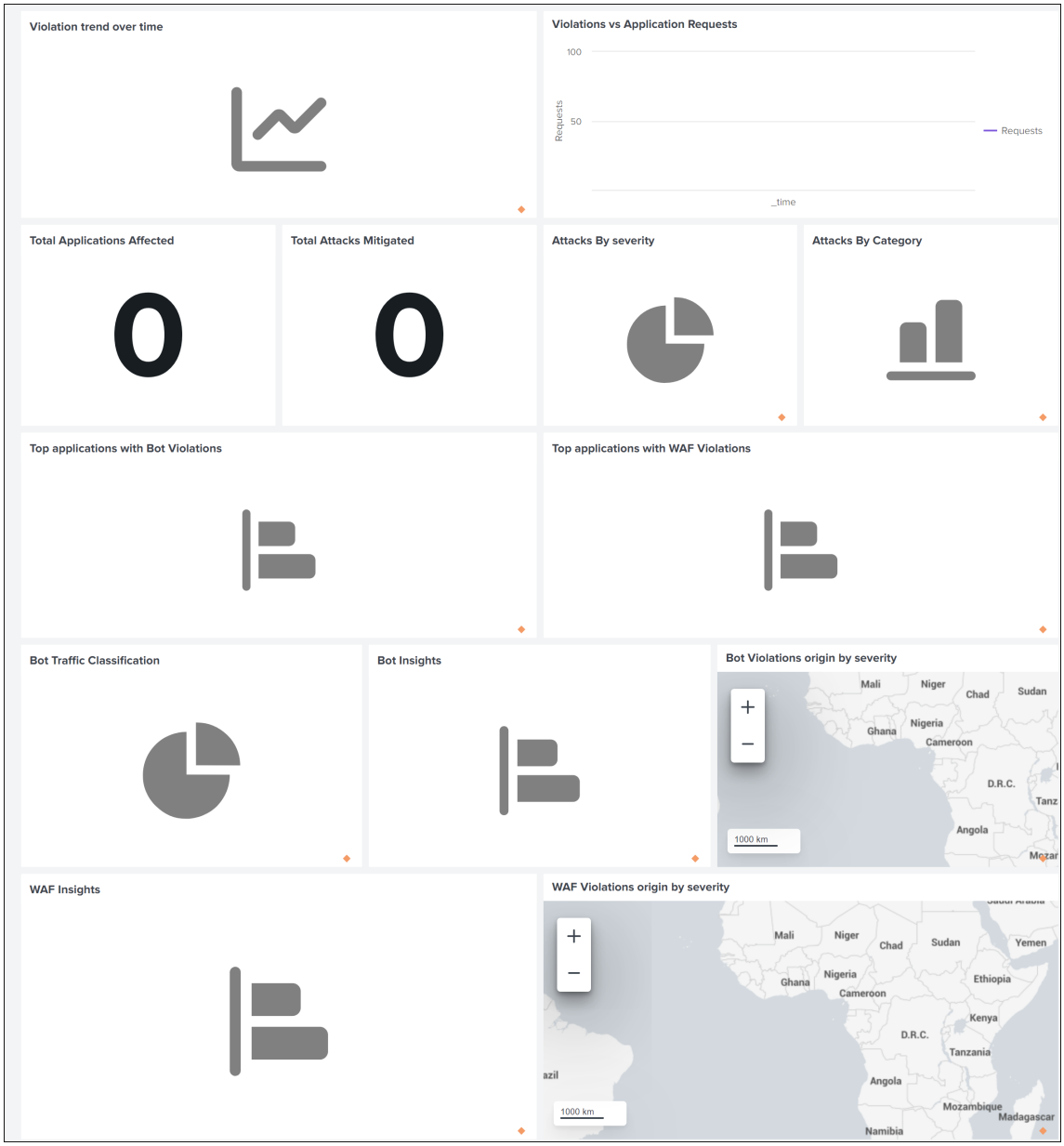


Nachdem Sie auf **Erstellen** geklickt haben, wählen Sie das **Quellsymbol** aus dem Layout aus.

5. Löschen Sie die vorhandenen Daten, fügen Sie die Daten ein, die Sie in Schritt 2 kopiert haben, und klicken Sie auf **Zurück**.
6. Klicken Sie auf **Speichern**.

   Sie können das Beispiel-Dashboard anzeigen.

   Im Folgenden finden Sie ein Beispiel-Dashboard für WAF und Bot.



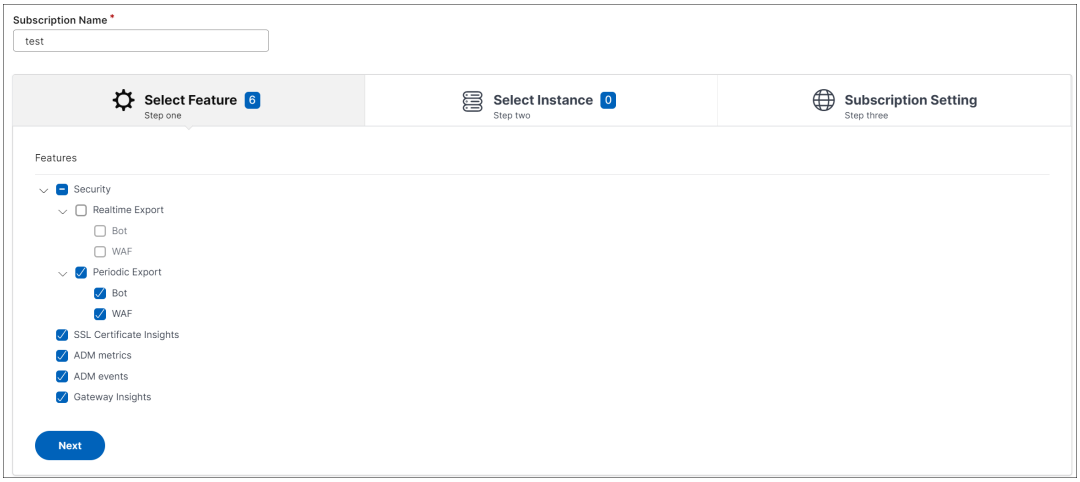
NetScaler ADM so konfigurieren, dass Daten nach Splunk exportiert werden

In Splunk haben Sie jetzt alles bereit. Der letzte Schritt besteht darin, NetScaler ADM zu konfigurieren, indem ein Abonnement erstellt und das Token hinzugefügt wird.

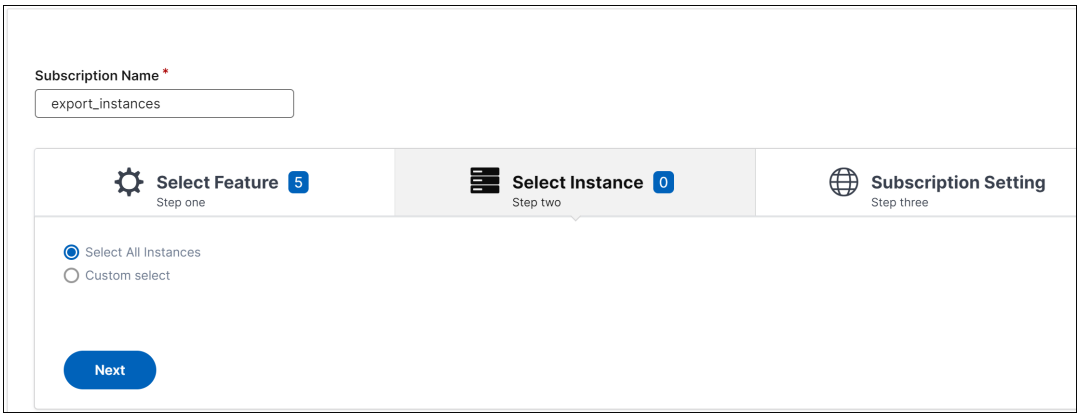
Nach Abschluss des folgenden Verfahrens können Sie das aktualisierte Dashboard in Splunk einsehen, das derzeit in Ihrem NetScaler ADM verfügbar ist:

1. Melden Sie sich bei NetScaler ADM an.
2. Navigieren Sie zu **Einstellungen > Ökosystemintegration**.

3. Klicken Sie auf der Seite **Abonnements** auf **Hinzufügen**.
4. Geben Sie im Feld **Abonnementname einen Namen** Ihrer Wahl ein.
5. Auf der Registerkarte **Feature auswählen** können Sie die Features auswählen, die Sie exportieren möchten, und auf **Weiter**klicken.
    - **Echtzeit-Export** —Die ausgewählten Verstöße werden sofort nach Splunk exportiert.
    - **Periodischer Export** —Die ausgewählten Verstöße werden basierend auf der von Ihnen ausgewählten Dauer nach Splunk exportiert.



6. Auf der Registerkarte **Instanz auswählen** können Sie entweder **Alle Instanzen auswählen** oder **Benutzerdefiniert auswählen**und dann auf **Weiter**klicken.
    - **Wählen Sie Alle Instanzen** —Exportiert Daten aus allen NetScaler-Instanzen nach Splunk.
    - **Benutzerdefinierte Auswahl** —Ermöglicht es Ihnen, die NetScaler-Instanzen aus der Liste auszuwählen. Wenn Sie bestimmte Instanzen aus der Liste auswählen, werden die Daten nur von den ausgewählten NetScaler-Instanzen nach Splunk exportiert.



7. Gehen Sie auf der Registerkarte **Abonnementeinstellungen** wie folgt vor:

a) **Endpunkttyp** —Wählen Sie **Splunk**aus.

b) **Endpunkt-URL** —Geben Sie die Splunk-Endpunktdetails an. Der Endpunkt muss das Format https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event haben.

> **Hinweis**
>
> Aus Sicherheitsgründen wird die Verwendung von HTTPS empfohlen.

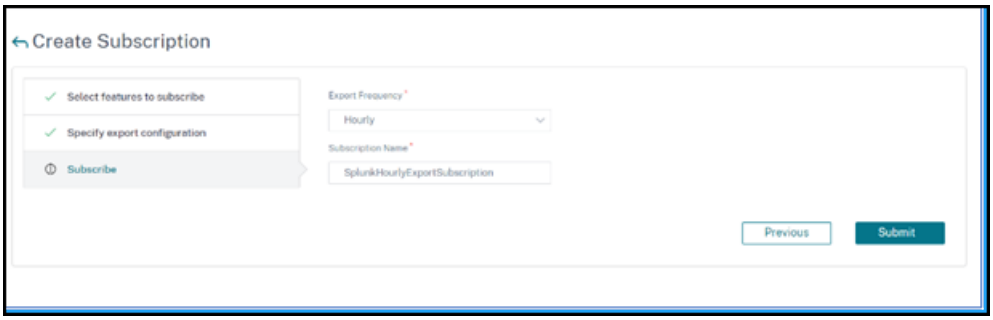
- **SPLUNK_PUBLIC_IP** —Eine gültige IP-Adresse, die für Splunk konfiguriert wurde.
- **SPLUNK_HEC_PORT** —Gibt die Portnummer an, die Sie während der Konfiguration des HTTP-Ereignisendpunkts angegeben haben. Die Standardportnummer ist 8088.
- **Services/Collector/Event** —Gibt den Pfad für die HEC-Anwendung an.

c) **Authentifizierungstoken** —Kopieren Sie das Authentifizierungstoken von der Splunk-Seite und fügen Sie es

d) **Häufigkeit auswählen** —Wählen Sie **Täglich** oder **Stündlich** aus der Liste aus. Basierend auf der Auswahl exportiert NetScaler ADM die Details nach Splunk.

> **Hinweis**
>
> Gilt nur, wenn Sie im **Periodischen Export**Verstöße ausgewählt haben.

e) Klicken Sie auf **Submit**.



> **Hinweis**
>
> - Wenn Sie zum ersten Mal mit der Option **Periodischer Export** konfigurieren, werden die ausgewählten Feature-Daten sofort an Splunk übertragen. Die nächste Exporthäufigkeit erfolgt basierend auf Ihrer Auswahl (täglich oder stündlich).
> - Wenn Sie zum ersten **Mal mit der Option Echtzeitexport** konfigurieren, werden die ausgewählten Feature-Daten sofort an Splunk übertragen, sobald die Verstöße in NetScaler ADM erkannt werden.

Dashboards in Splunk anzeigen

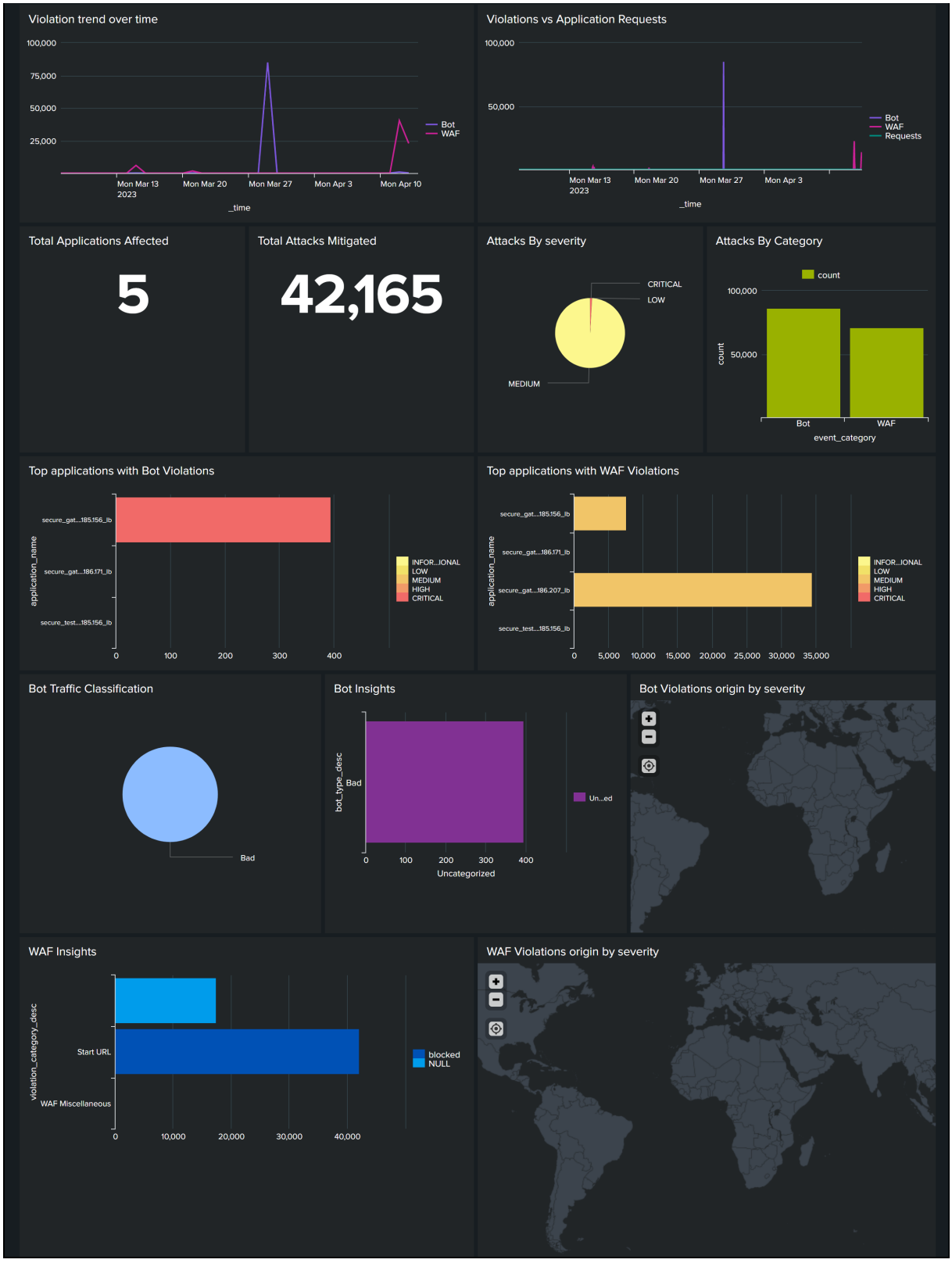
Nachdem Sie die Konfiguration in NetScaler ADM abgeschlossen haben, werden die Daten aus NetScaler ADM exportiert und die Ereignisse werden in Splunk angezeigt.

> **Hinweis:**
>
> Klicken Sie im NetScaler ADM SSL-Dashboard (**Infrastruktur** > SSL-Dashboard) auf **Poll Now**, um sofort die aktualisierten Daten zu SSL-Zertifikaten in Splunk einzusehen.

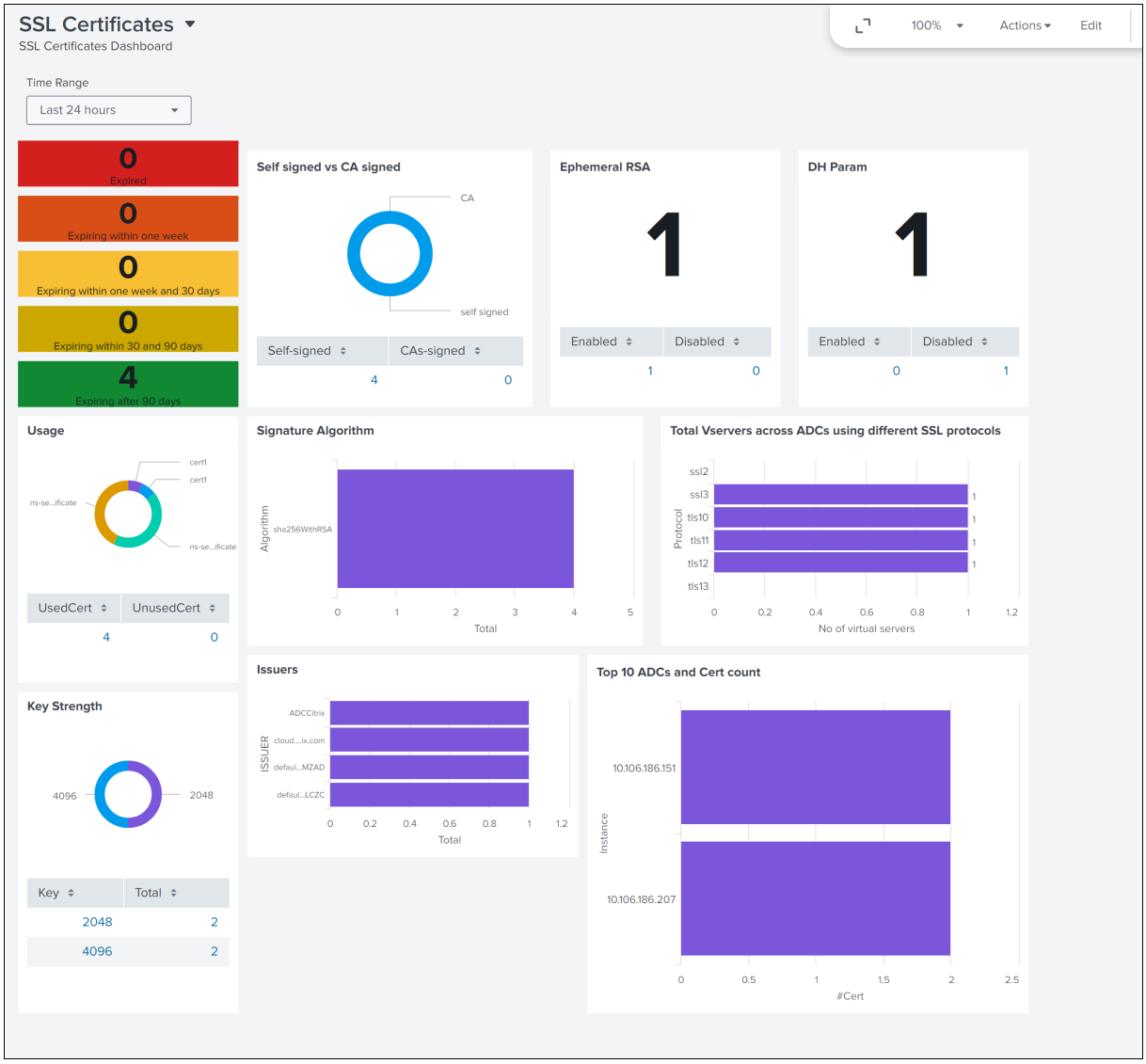
Sie sind bereit, das aktualisierte Dashboard in Splunk ohne weitere Schritte anzuzeigen.

Gehen Sie zu Splunk und klicken Sie auf das Dashboard, das Sie erstellt haben, um das aktualisierte Dashboard anzuzeigen.

Im Folgenden finden Sie ein Beispiel für das aktualisierte WAF- und Bot-Dashboard:

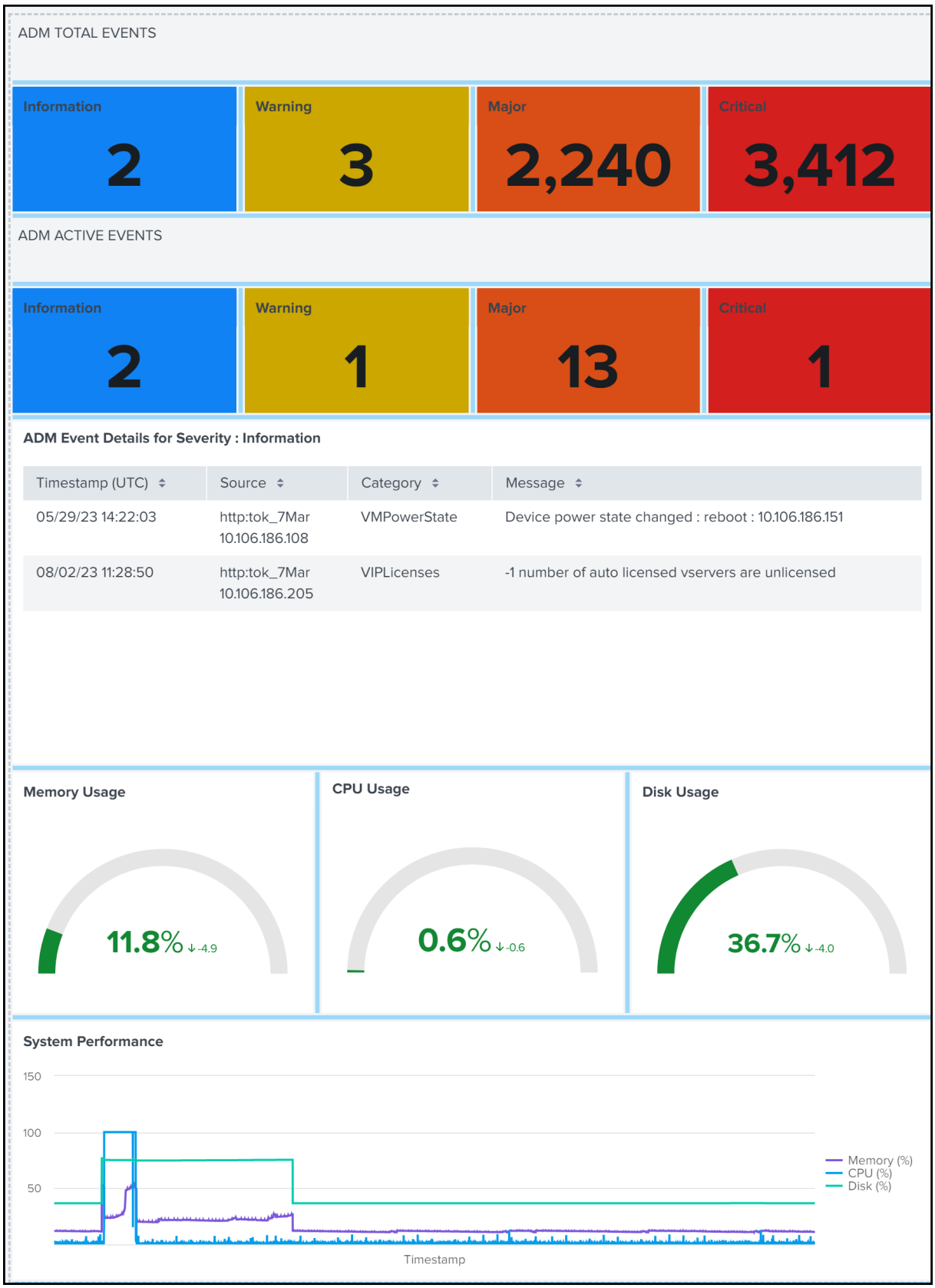


Das folgende Dashboard ist ein Beispiel für das aktualisierte SSL Certificate Insights-Dashboard.



Das folgende Dashboard ist ein Beispiel für das aktualisierte Ereignis- und Metrik-Dashboard.

> **Hinweis:**
>
> Die Nutzungsdaten für Speicher, CPU und Datenträger zeigen den aktuellen Wert aus dem NetScaler ADM. Der Auf- und Abwärtstrend dieser Werte wird auf der Grundlage des Vergleichs des vorherigen Werts alle 5 Minuten angezeigt.



Neben dem Dashboard können Sie nach der Erstellung des Abonnements auch Daten in Splunk anzeigen.

1. Klicken Sie in Splunk auf **Search & Reporting**.
2. In der Suchleiste:
    - Geben Sie `sourcetype="metrics"` ein und wählen Sie die Dauer aus der Liste aus, um die ADM-Metrikdaten anzuzeigen.
    - Geben Sie `sourcetype="event"` ein und wählen Sie die Dauer aus der Liste aus, um die ADM-Ereignisdaten anzuzeigen.
    - Geben Sie `sourcetype="bot"` oder `sourcetype="waf"` ein und wählen Sie die Dauer aus der Liste aus, um Bot-/WAF-Daten anzuzeigen.
    - Geben Sie `sourcetype="ssl"` ein und wählen Sie die Dauer aus der Liste aus, um die Insightsdaten des SSL-Zertifikats anzuzeigen.

Integration mit New Relic

February 5, 2024

Sie können NetScaler ADM jetzt in New Relic integrieren, um Analysen zu WAF- und Bot-Verstößen in Ihrem New Relic-Dashboard anzuzeigen. Mit dieser Integration können Sie:

- Kombinieren Sie alle anderen externen Datenquellen in Ihrem New Relic Dashboard.
- Verschaffen Sie sich einen Überblick über Analysen an einem zentralen Ort.

NetScaler ADM sammelt Bot- und WAF-Ereignisse und sendet sie je nach Ihrer Wahl entweder in Echtzeit oder in regelmäßigen Abständen an New Relic. Als Administrator können Sie die Bot- und WAF-Ereignisse auch in Ihrem New Relic-Dashboard einsehen.

Voraussetzungen

Für eine erfolgreiche Integration müssen Sie:

- Rufen Sie einen New Relic-Ereignisendpunkt im folgenden Format ab:

  `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`

  Weitere Informationen zur Konfiguration eines Event-Endpunkts finden Sie in der New Relic-Dokumentation.

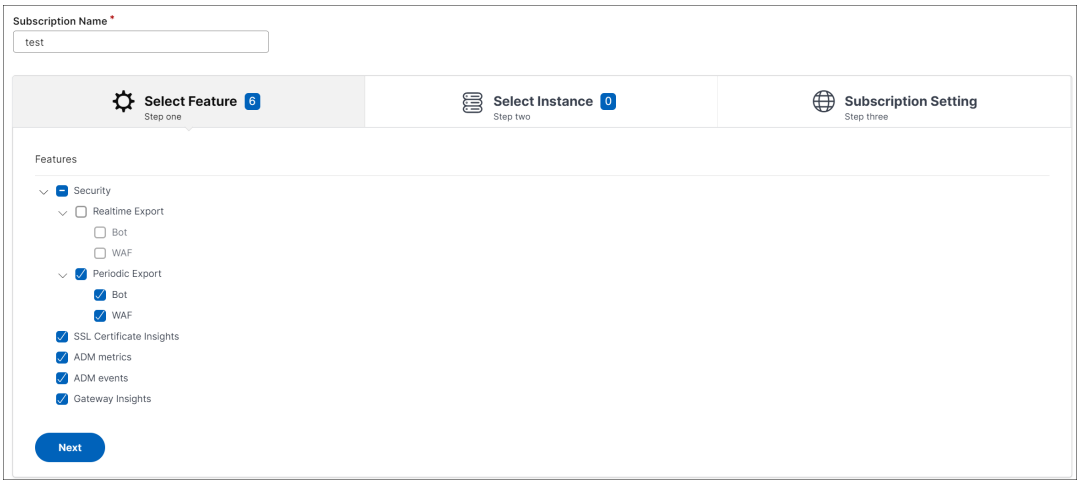
Weitere Informationen zum Abrufen einer Konto-ID finden Sie in der New Relic-Dokumentation.

- Besorgen Sie sich einen New Relic-Schlüssel. Weitere Informationen finden Sie in der New Relic-Dokumentation.
- Schlüsseldetails in NetScaler ADM hinzufügen

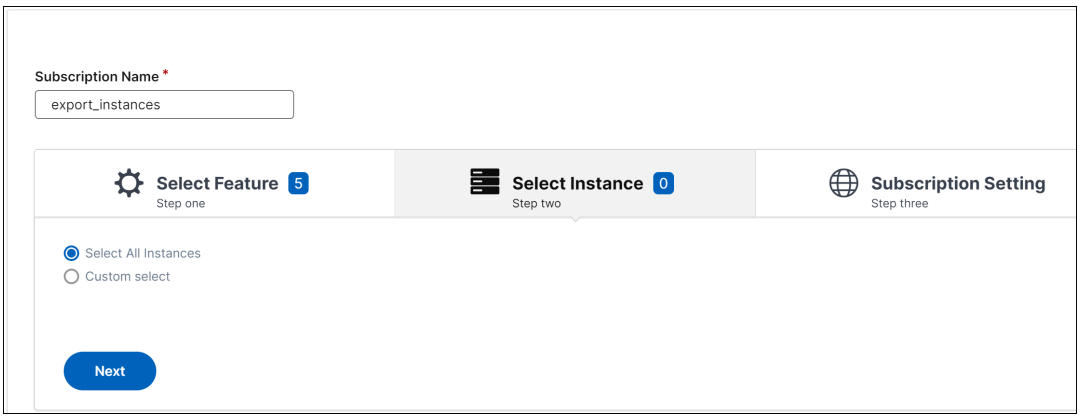
Schlüsseldetails in NetScaler ADM hinzufügen

Nachdem Sie ein Token generiert haben, müssen Sie Details in NetScaler ADM hinzufügen, um es in New Relic zu integrieren.

1. Melden Sie sich bei NetScaler ADM an.
2. Navigieren Sie zu **Einstellungen > Ökosystemintegration**.
3. Klicken Sie auf der Seite **Abonnements** auf **Hinzufügen**.
4. Wählen Sie auf der Registerkarte **Feature auswählen** die Features aus, die Sie exportieren möchten, und klicken Sie auf **Weiter**.
    - **Echtzeitexport** —Die ausgewählten Verstöße werden sofort nach New Relic exportiert.
    - **Periodischer Export** —Die ausgewählten Verstöße werden basierend auf der von Ihnen ausgewählten Dauer nach New Relic exportiert.



5. Auf der Registerkarte **Instanz auswählen** können Sie entweder **Alle Instanzen auswählen** oder **Benutzerdefiniert auswählen**und dann auf **Weiter**klicken.
    - **Alle Instanzen auswählen** —Exportiert Daten aus allen NetScaler-Instanzen nach New Relic.
    - **Benutzerdefinierte Auswahl** —Ermöglicht es Ihnen, die NetScaler-Instanzen aus der Liste auszuwählen. Wenn Sie bestimmte Instanzen aus der Liste auswählen, werden die Daten nur von den ausgewählten NetScaler-Instanzen nach New Relic exportiert.



6. Gehen Sie auf der Registerkarte **Abonnementeinstellungen** wie folgt vor:

   a) **Endpunkttyp** —Wählen Sie **New Relic**.

   b) **Endpunkt-URL** —Geben Sie die Endpunktdetails von New Relic an. Der Endpunkt muss das Format `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events` haben.

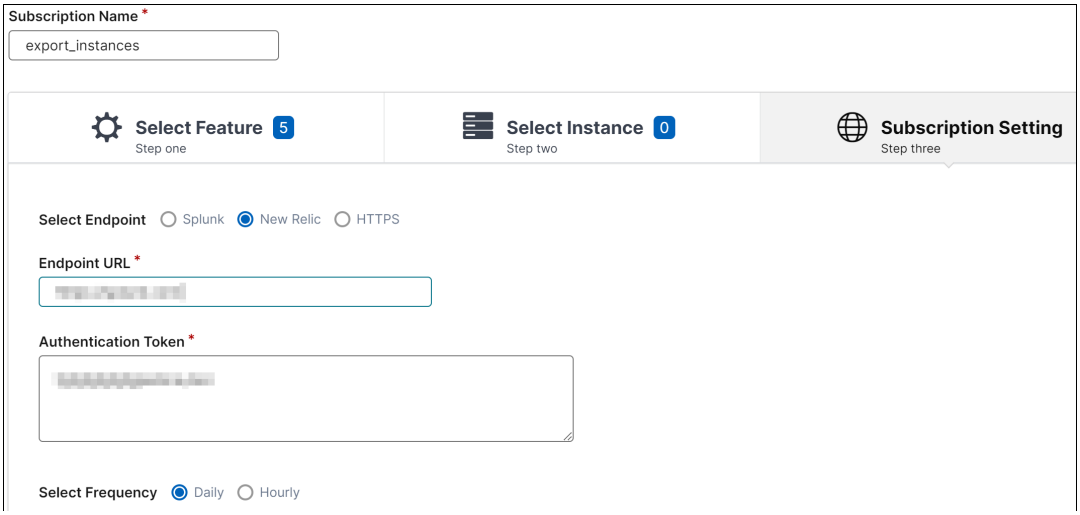
   > **Hinweis**
   >
   > Aus Sicherheitsgründen wird die Verwendung von HTTPS empfohlen.

   c) **Authentifizierungstoken** —Kopieren Sie das Authentifizierungstoken von der New Relic-Seite und fügen Sie es ein.

   d) **Häufigkeit auswählen** —Wählen Sie **Täglich** oder **Stündlich** aus der Liste aus. Basierend auf der Auswahl exportiert NetScaler ADM die Details nach New Relic.

   > **Hinweis**
   >
   > Gilt nur, wenn Sie im **Periodischen Export**Verstöße ausgewählt haben.

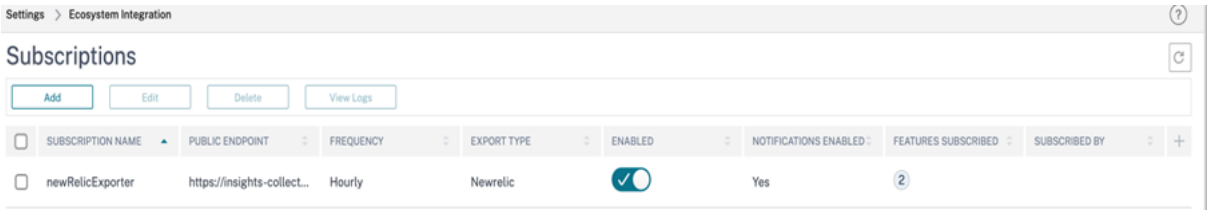
   e) Klicken Sie auf **Submit**.



Hinweis

- Wenn Sie die Option **Periodischer Export** zum ersten Mal konfigurieren, werden die ausgewählten Feature-Daten sofort an New Relic übertragen. Die nächste Exporthäufigkeit erfolgt basierend auf Ihrer Auswahl (täglich oder stündlich).
- Wenn Sie zum ersten **Mal mit der Option Echtzeitexport** konfigurieren, werden die ausgewählten Daten sofort an New Relic übertragen, sobald die Verstöße in NetScaler ADM erkannt werden.

Die Konfiguration ist abgeschlossen. Einzelheiten können Sie auf der Seite **Abonnements** einsehen.

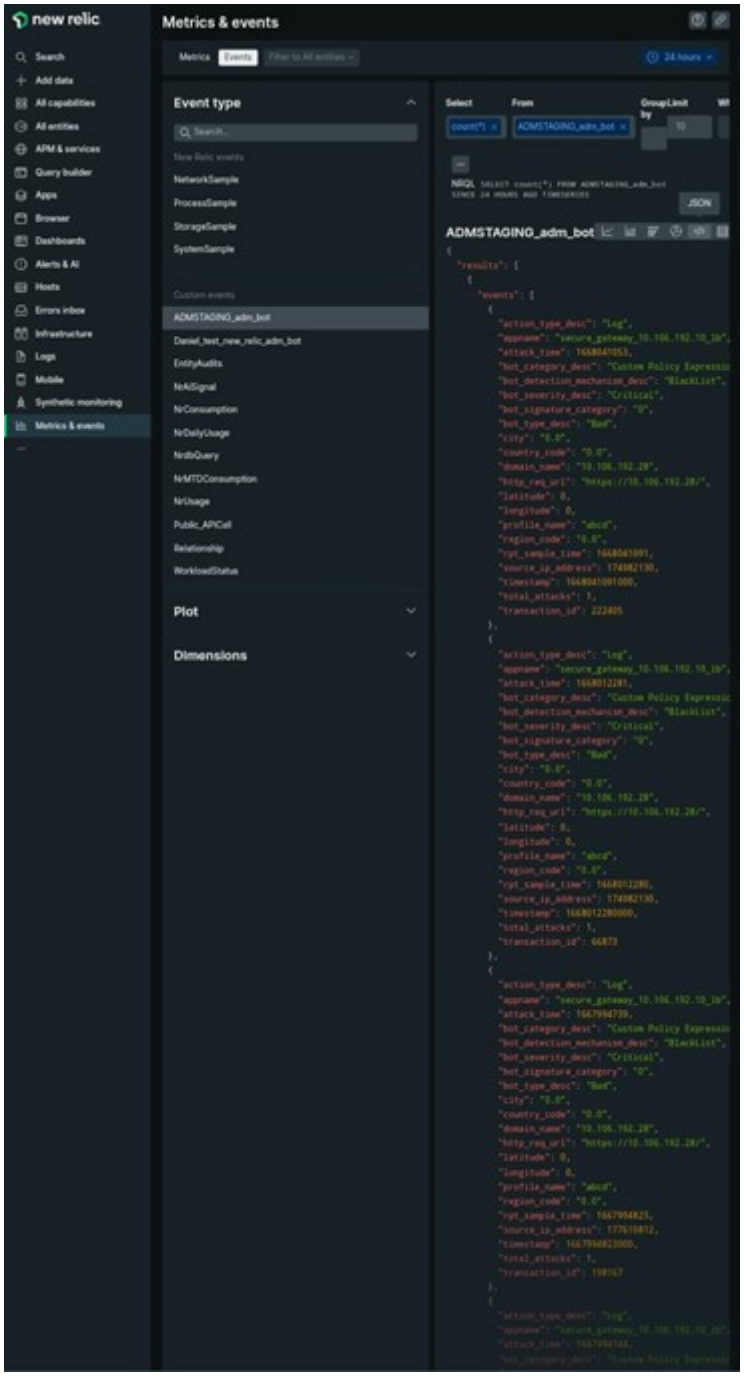


New Relic Dashboard

Wenn die Ereignisse in New Relic exportiert werden, können Sie die Ereignisdetails unter **Metriken und Ereignisse** im folgenden JSON-Format anzeigen:

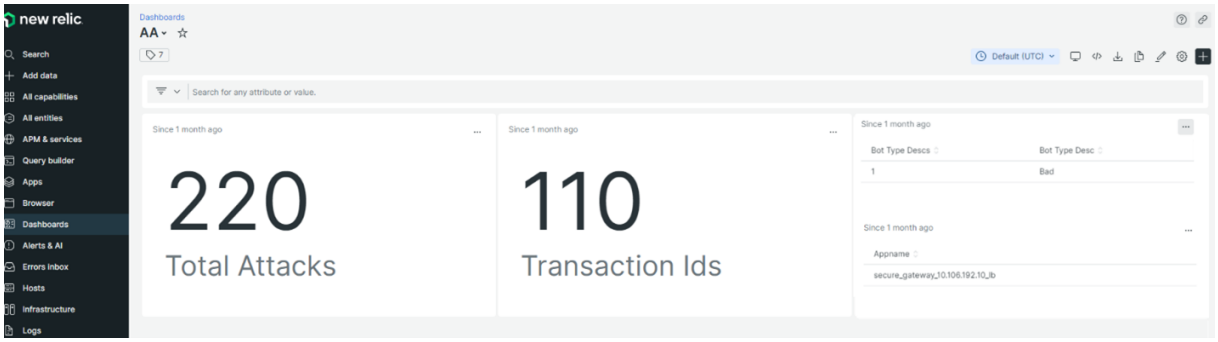
<subscription_name>_adm_<event name> wobei der Eventname Bot, WAF usw. sein kann.

Im folgenden Beispiel ist ADMSTAGING <subscription_name> und Bot <event_name>.



Sobald Sie die JSON-Daten in Ihr New Relic-Dashboard aufgenommen haben, können Sie als Administrator die NRQL (New Relic Query Language) verwenden und ein benutzerdefiniertes Dashboard mit Facetten und Widgets nach Ihrer Wahl erstellen, indem Sie Abfragen rund um die aufgenommenen Daten erstellen. Weitere Informationen finden Sie unter `https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/`.

Im Folgenden finden Sie ein Beispiel-Dashboard, das mit NRQL erstellt wurde:



Um dieses Dashboard zu erstellen, sind die folgenden Abfragen erforderlich:

- Widget 1: Gesamtzahl einzigartiger Angriffe in der Tabelle “Ereignisse”

  ```
  SELECT count(total_attacks)from <event_name> since 30 days ago
  ```

- Widget 2: Eindeutige Transaktions-IDs in der Ereignistabelle

  ```
  SELECT uniqueCount(transaction_id)from <event_name> since 30 days
   ago
  ```

- Widget 3: Gesamtzahl einzigartiger Bot-Typen und ihre Anzahl

  ```
  SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc)from <
  event_name> since 30 days ago
  ```

- Widget 4: Gesamtzahl eindeutiger App-Namen, bei denen Bot-Verstöße angezeigt werden

  ```
  SELECT uniques(appname)from <event_name> since 30 days ago
  ```

Gateway Insight

February 5, 2024

In einer NetScaler Gateway-Bereitstellung ist der Einblick in die Zugriffsdetails eines Benutzers unerlässlich, um Probleme mit Zugriffsfehlern zu beheben. Als Netzwerkadministrator möchten Sie wissen, wann sich ein Benutzer nicht bei NetScaler Gateway anmelden kann, und Sie möchten die Benutzeraktivität und die Gründe für den Anmeldefehler kennen. Diese Informationen sind normalerweise nicht verfügbar, es sei denn, der Benutzer sendet eine Lösungsanfrage.

Gateway Insight bietet Einblick in die Fehler, die bei der Anmeldung bei NetScaler Gateway auftreten, unabhängig vom Zugriffsmodus. Sie können eine Liste aller verfügbaren Benutzer, die Anzahl der aktiven Benutzer, die Anzahl der aktiven Sitzungen sowie die Bytes und Lizenzen anzeigen, die von allen Benutzern zu einem bestimmten Zeitpunkt verwendet werden. Sie können die Endpunktanalyse (EPA), Authentifizierung, Single Sign-On (SSO) und Fehler beim Starten von Anwendungen für einen

Benutzer anzeigen. Sie können auch die Details zu aktiven und beendeten Sitzungen für einen Benutzer anzeigen.

Gateway Insight bietet auch Einblick in die Gründe für das Fehlschlagen des Anwendungsstarts 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 gesamten Byte und die von den Anwendungen verbrauchte Bandbreite 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 Gesamtanzahl der Bytes und die Bandbreite aller Gateways, die mit einem NetScaler Gateway Gerät verknüpft sind, jederzeit anzeigen. Sie können EPA, Authentifizierung, Single Sign-On und Anwendungsstartfehler für ein Gateway anzeigen. Sie können auch die Details aller Benutzer, die einem Gateway zugeordnet sind, und deren Anmeldeaktivitäten anzeigen.

Alle Protokollmeldungen werden in der NetScaler ADM-Datenbank gespeichert, sodass Sie Fehlerdetails für einen beliebigen Zeitraum anzeigen können. Sie können auch eine Zusammenfassung der Anmeldefehler anzeigen und feststellen, in welcher Phase des Anmeldevorgangs ein Fehler aufgetreten ist.

Punkte zu beachten

- Gateway Insight wird in den folgenden Bereitstellungen unterstützt:
  - Access Gateway
  - Unified Gateway
- Die NetScaler ADM-Version und der Build müssen mit denen des NetScaler Gateway-Geräts identisch oder höher sein.
- Eine Stunde Gateway Insight-Berichte können für NetScaler Instanzen mit Advanced-Lizenz angezeigt werden. Eine Premium-Lizenz ist ein Muss, um Gateway Insight-Berichte länger als eine Stunde anzusehen.

Einschränkungen

- NetScaler Gateway unterstützt Gateway Insight nicht, wenn die Authentifizierungsmethode als zertifikatbasierte Authentifizierung konfiguriert ist.
- Für Gateway Insight-Berichte werden Geostandortinformationen nicht von der NetScaler Appliance bereitgestellt.

- 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 sind Fehler auf der NetScaler Gateway-Appliance in der zweiten DMZ nicht sichtbar.
- Probleme mit dem Remotedesktopprotokoll (RDP) -Desktop-Zugriff werden nicht gemeldet.
- Gateway Insight wird für die folgenden Authentifizierungstypen unterstützt. Wenn ein anderer Authentifizierungstyp als diese verwendet wird, können Abweichungen in Gateway Insight auftreten.
  - Lokal
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - Natives OTP
  - OAuth OpenID Verbinden

    Für die OAuth-OpenID Connect-Authentifizierung kann NetScaler als OAuth-OpenID Connect Relying Party (RP) oder OAuth-OpenID Connect Identity Provider (IdP) fungieren. Wenn die Authentifizierung erfolgreich ist, wird der Benutzername im Gateway Insight-Bericht auf der Registerkarte Benutzer gemeldet. Sie können jedoch nicht feststellen, ob die Sitzung bei IdP oder RP erstellt wurde.

    Hinweis: Die OAuth-OpenID Connect-Authentifizierung wird von NetScaler ADM Release 13.1 Build 4.xx und höher unterstützt.

Gateway Insight aktivieren

Um Gateway Insight für Ihr NetScaler Gateway Gerät zu aktivieren, müssen Sie das NetScaler Gateway-Gerät zunächst NetScaler ADM hinzufügen. Anschließend müssen Sie AppFlow für den virtuellen Server aktivieren, der die VPN-Anwendung darstellt. Informationen zum Hinzufügen von Geräten zu NetScaler ADM finden Sie unter Geräte hinzufügen.

> **Hinweis**
>
> Um Fehler bei der Endpunktanalyse (EPA) in NetScaler ADM anzuzeigen, müssen Sie die AppFlow-Authentifizierung, -Autorisierung und die Protokollierung von Benutzernamen auf dem NetScaler Gateway-Gerät aktivieren.

Das folgende Verfahren zum Aktivieren von Gateway Insight ist anwendbar, wenn NetScaler ADM **13.0 Build 36.27** lautet:

1. Navigieren Sie zu **Infrastruktur > Instanzen**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 auf der Seite Configure Insight** unter **Configure Analytics** die Option **NetScaler Gateway** aus.
4. Wählen Sie den virtuellen Server aus und klicken Sie dann auf **AppFlow aktivieren**.
5. Klicken Sie auf dem Bildschirm **AppFlow aktivieren** in der Liste **Ausdruck auswählen** auf true.
6. Aktivieren Sie neben **Transportmodus** das Kontrollkästchen **Logstream**.

   > **Hinweis**
   >
   > Sie können entweder **IPFIX** oder **Logstream** als Transportmodus wählen.
   >
   > Weitere Informationen zu **IPFIX** und **Logstream** finden Sie unter **Logstream-Übersicht**.

7. Klicken Sie auf **OK**.

Für NetScaler ADM Version 13.0 Build 41.x oder höher

1. Navigieren Sie zu **Infrastruktur > Instanzen**, und wählen Sie die Instanz aus.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
3. Wählen Sie den virtuellen Server aus und klicken Sie auf **Analytics aktivieren**.
4. Unter **Erweiterte Optionen**:
   a) Wählen Sie **Logstream** aus
   b) Wählen Sie **NetScaler Gateway** aus
5. Klicken Sie auf **OK**.

Aktivieren der AppFlow-Authentifizierung, Autorisierung und Auditing-Benutzernamenprotokollierung auf einer NetScaler Gateway-Appliance 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**.

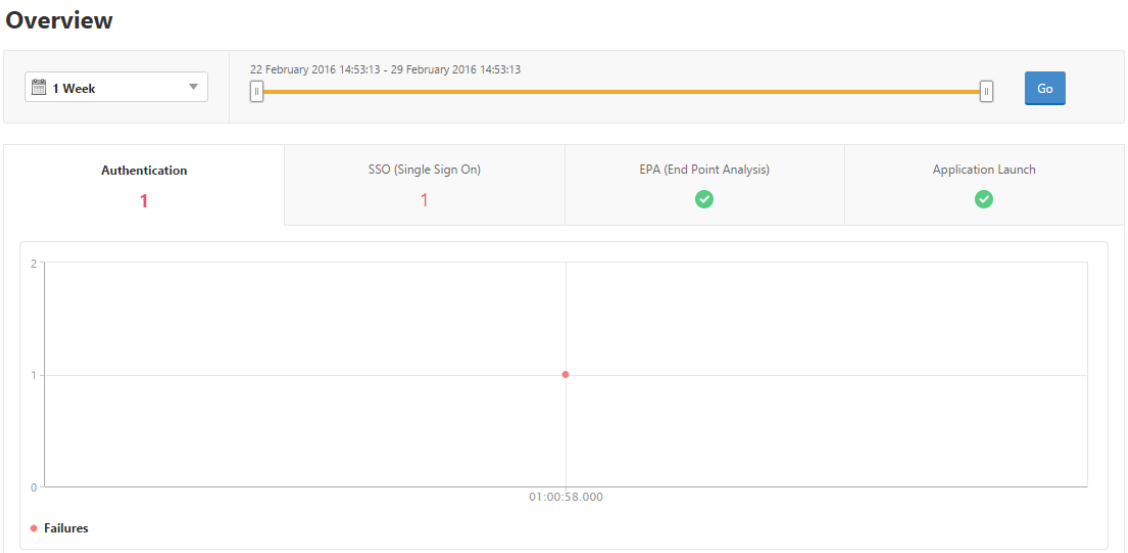
Gateway Insight-Berichte anzeigen

In NetScaler ADM können Sie Berichte für alle Benutzer, Anwendungen und Gateways anzeigen, die den NetScaler Gateway-Appliances zugeordnet sind, und Sie können Details für einen bestimmten Benutzer, eine bestimmte Anwendung oder ein 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. NetScaler ADM Analytics unterstützt jetzt die auf virtuellen IP-Adressen basierende 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 zum Zuweisen von Benutzern zur Gruppe finden Sie unter Konfigurieren von Gruppen.

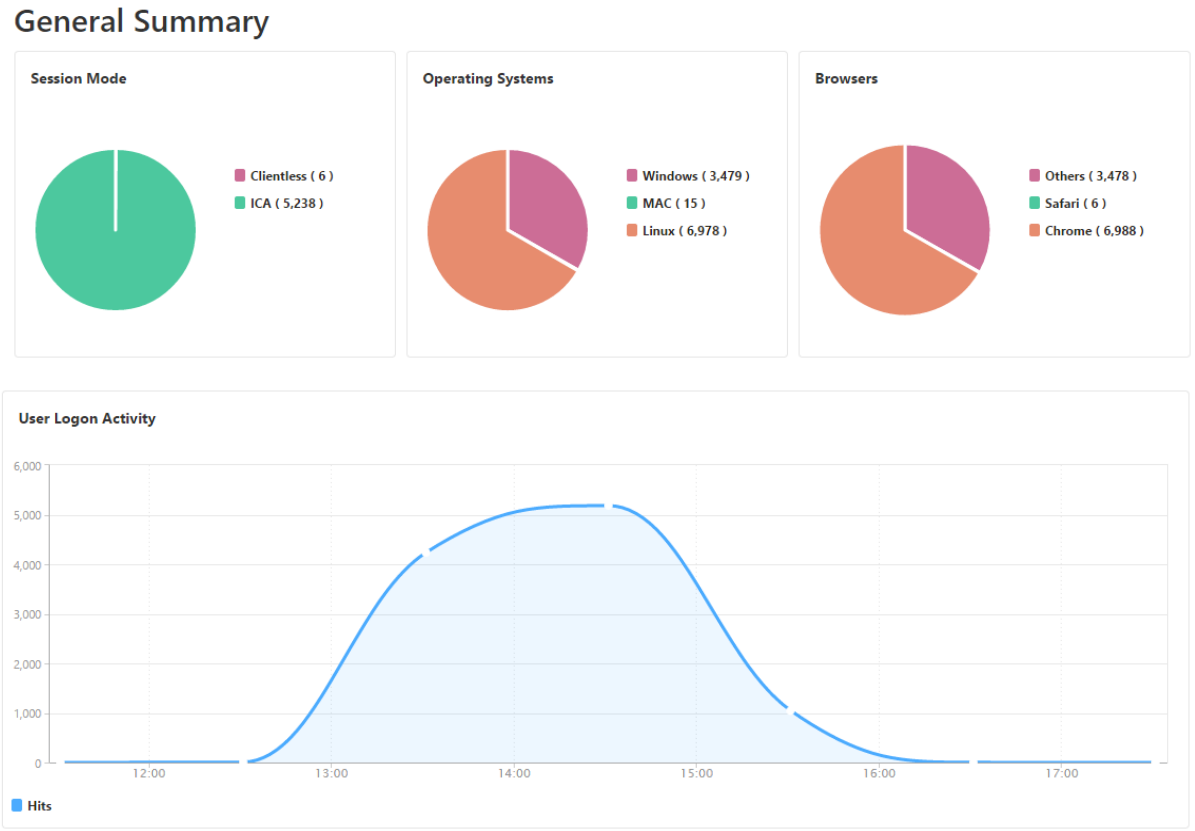
So zeigen Sie EPA-, SSO-, Authentifizierungs-, Autorisierungs- und Anwendungsstartfehler an

1. Navigieren Sie in NetScaler ADM zu **Gateway > Gateway Insight**.
2. Wählen Sie den Zeitraum aus, für den Sie die Benutzerdetails anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.
3. Klicken Sie auf die Registerkarten EPA (Endpunktanalyse), Authentifizierung, Autorisierung, SSO (Single Sign On) oder Anwendungsstart, um die Fehlerdetails anzuzeigen.



So zeigen Sie eine Zusammenfassung der Sitzungsmodi, Clients und der Anzahl der Benutzer an

Navigieren Sie in NetScaler ADM zu **Gateway > Gateway Insight**, und scrollen Sie nach unten, um die Berichte anzuzeigen.



Anzeigen von Gateway Insight-Berichten für Benutzer

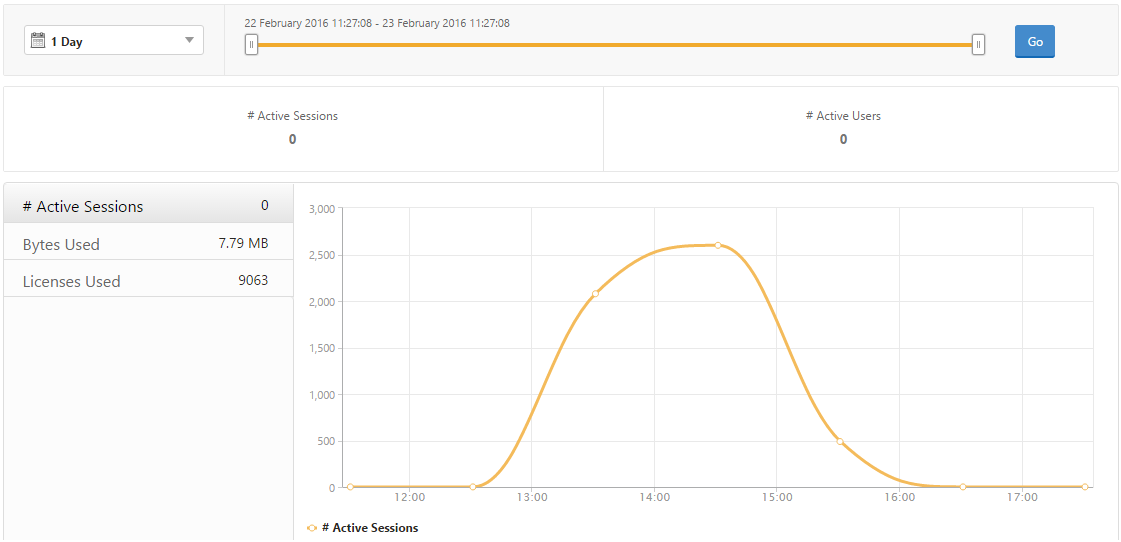
Sie können die Berichte anzeigen für:

- Alle mit den NetScaler Gateway-Appliances verknüpften Benutzer
- Fehler bei EPA, Authentifizierung, SSO und Anwendungsstart für einen Benutzer.
- Die Details von aktiven und beendeten Sitzungen für einen Benutzer.
- Die Arten von Sitzungsmodi wie Full Tunnel, Clientless VPN und ICA-Proxy.

So zeigen Sie Benutzerdetails an

1. Navigieren Sie in NetScaler ADM zu **Gateway > Gateway Insight > Benutzer**.

2. Wählen Sie den Zeitraum aus, für den Sie die Benutzerdetails anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.
3. Sie können die Anzahl der aktiven Benutzer, die Anzahl der aktiven Sitzungen, Bytes und Lizenzen anzeigen, die von allen Benutzern während des Zeitraums verwendet werden.

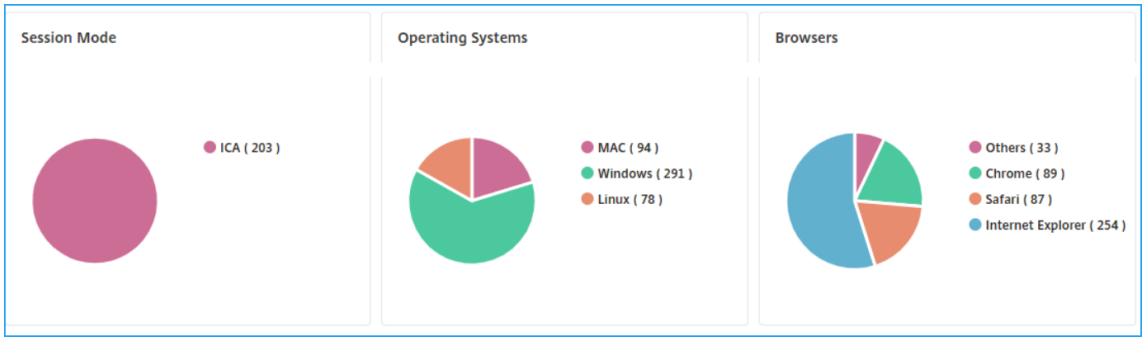


Scrollen Sie nach unten, um eine Liste der verfügbaren Benutzer und aktiven Benutzer anzuzeigen.

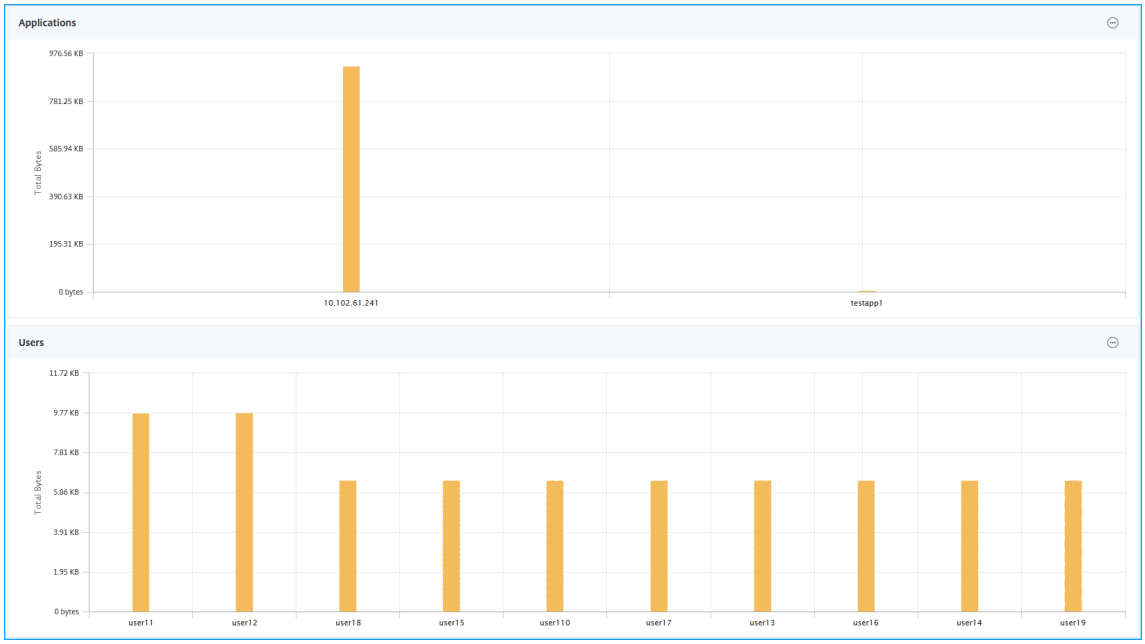
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

Klicken Sie auf der Registerkarte **Benutzer** oder **Aktive Benutzer** auf einen Benutzer, um die folgenden Benutzerdetails anzuzeigen:

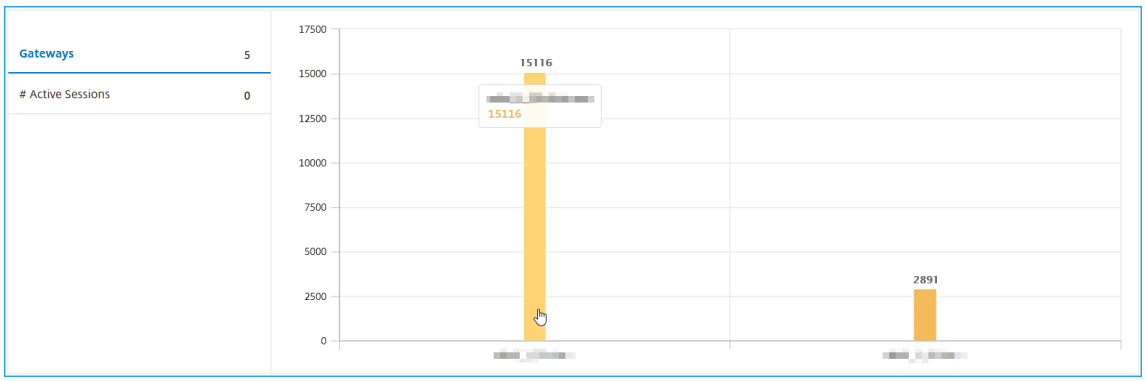
- **Benutzerdetails** - Sie können Erkenntnisse für jeden Benutzer anzeigen, der mit den ADC Gateway-Appliances verknüpft ist. Navigieren Sie zu **Gateway** > **Gateway Insight** > **Users** und klicken Sie auf einen Benutzer, um Informationen für den ausgewählten Benutzer wie Sitzungsmodus, Betriebssystem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



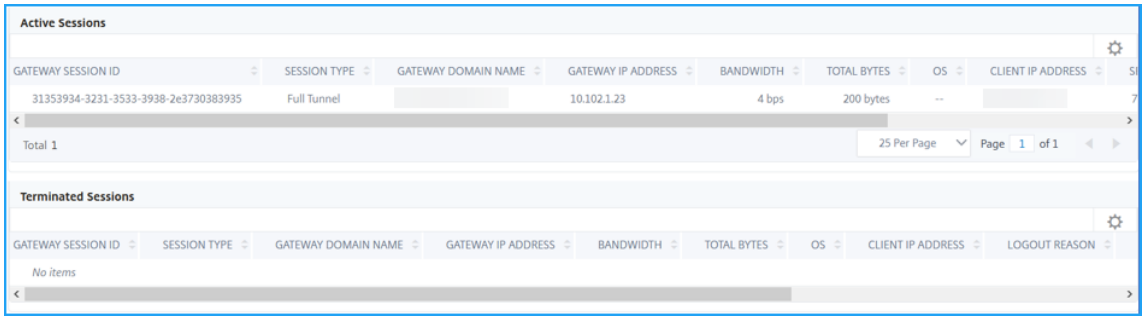
- **Benutzer und Anwendungen für das ausgewählte Gateway** —Navigieren Sie zu **Gateway** > **Gateway Insight** > **Gateway** und klicken Sie auf einen Gateway-Domänennamen, um die Top 10 Anwendungen und Top 10 Benutzer anzuzeigen, die mit dem ausgewählten Gateway verknüpft sind.



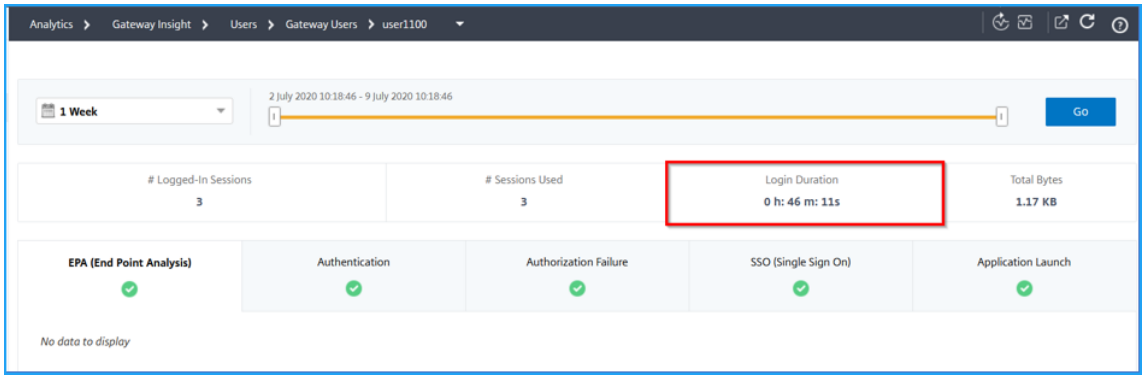
- **Weitere Optionen für Anwendungen und Benutzer anzeigen** —Für mehr als 10 Anwendungen und Benutzer können Sie auf das Mehr-Symbol in Anwendungen und Benutzer klicken, um alle Benutzer- und Anwendungsdetails anzuzeigen, die mit dem ausgewählten Gateway verknüpft sind.
- **Zeigen Sie Details an, indem Sie auf das Balkendiagramm klicken** —Wenn Sie auf ein Balkendiagramm klicken, können Sie die relevanten Details anzeigen. Navigieren Sie beispielsweise zu **Gateway > Gateway Insight > Gateway** und klicken Sie auf das Gateway-Balkendiagramm, 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

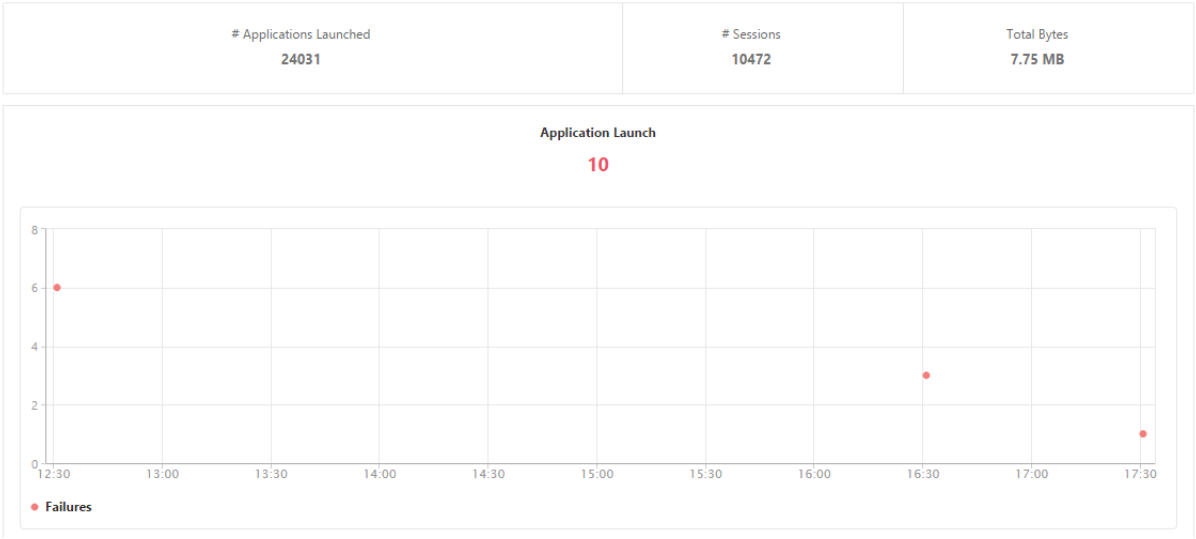
Anzeigen von Gateway Insight-Berichten für Anwendungen

Sie können die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen, die Anzahl der gesamten Byte und die von den Anwendungen verbrauchte Bandbreite anzeigen. Sie können Details der Benutzer, Sitzungen, Bandbreite und Startfehler für eine Anwendung anzeigen.

So zeigen Sie Anwendungsdetails an

1. Navigieren Sie in NetScaler ADM zu **Gateway > Gateway Insight > Applications** .
2. Wählen Sie den Zeitraum aus, für den Sie die Anwendungsdetails anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.

Sie können jetzt die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen, die Anzahl der gesamten Byte und die von den Anwendungen verbrauchte Bandbreite 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.

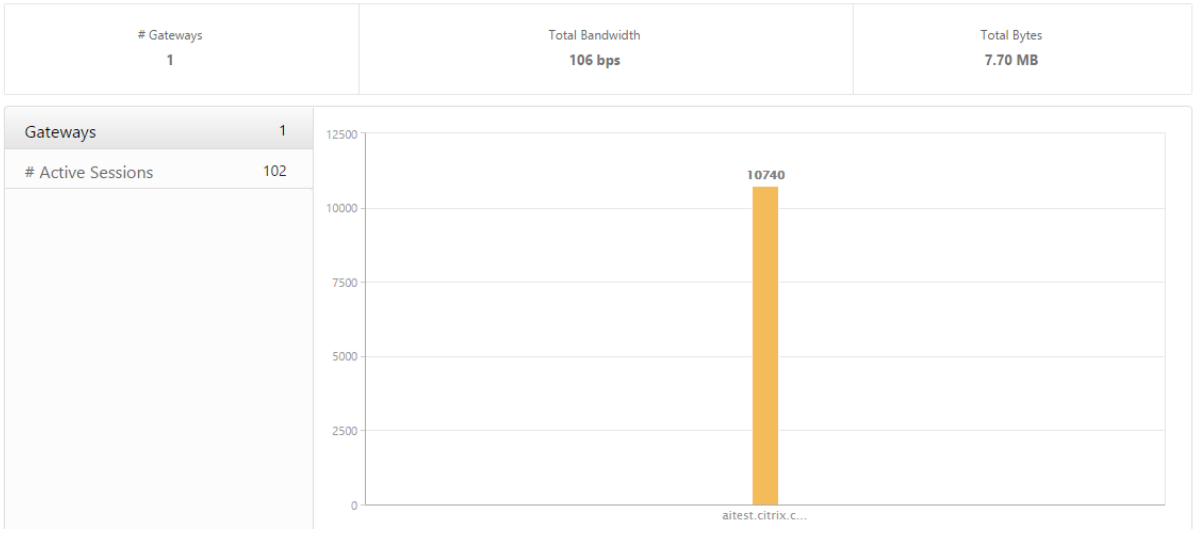
Anzeigen von Gateway Insight-Berichten für Gateways

Sie können die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die Gesamtanzahl der Bytes und die Bandbreite aller Gateways, die mit einem NetScaler Gateway Gerät verknüpft sind, jederzeit anzeigen. Sie können EPA, Authentifizierung, Single Sign-On und Anwendungsstartfehler für ein Gateway anzeigen. Sie können auch die Details aller Benutzer, die einem Gateway zugeordnet sind, und deren Anmeldeaktivitäten anzeigen.

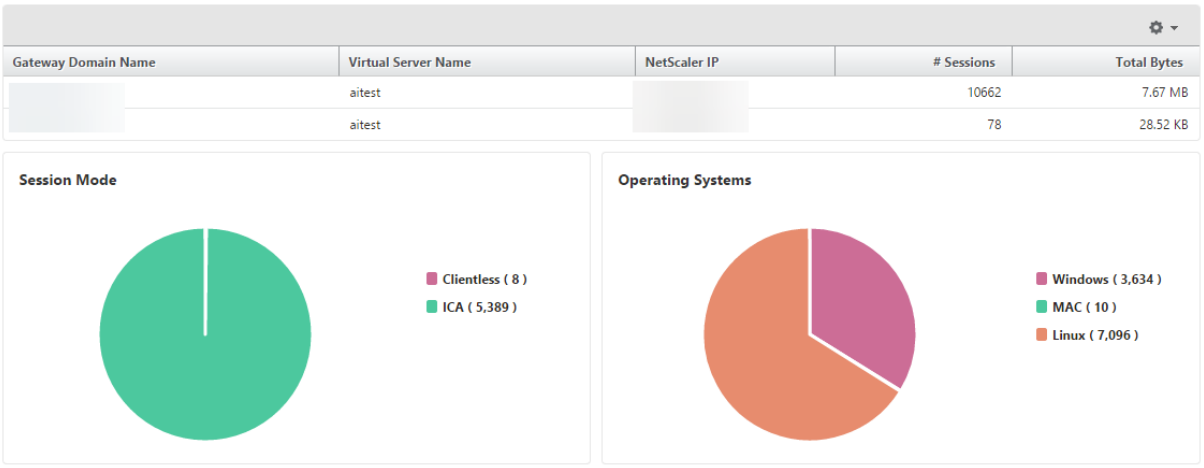
So zeigen Sie Gateway Details an

1. Navigieren Sie in **NetScaler ADM** zu **Gateway > Gateway Insight > Gateways** .
2. Wählen Sie den Zeitraum aus, für den Sie die Gateway Details anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.

Sie können jetzt die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die Gesamtanzahl der Bytes und die Bandbreite anzeigen, die von allen Gateways verwendet wird, die mit einem NetScaler Gateway Gerät verknüpft sind.



Führen Sie einen Bildlauf nach unten durch, um die Gatewaydetails wie Gatewaydomänenname, Name des virtuellen Servers, NetScaler 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.

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.
> - Geokartenberichte werden nur exportiert, wenn der NetScaler ADM über eine Internetverbindung verfügt.

Um einen Bericht zu exportieren

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 fügen Sie einen E-Mail-Server oder eine E-Mail-Verteilerliste hinzu:

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Einstellungen > Benachrichtigungen > E-Mail**.
2. Wählen Sie im rechten Bereich **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 der Benutzer auf NetScaler Gateway-Geräten zu erhalten.

Ein Benutzer kann sich nicht beim NetScaler Gateway Gerät oder bei den internen Webservern anmelden

Sie sind ein NetScaler Gateway-Administrator, der NetScaler Gateway-Appliances über NetScaler ADM überwacht, und Sie möchten sehen, warum sich ein Benutzer nicht anmelden kann oder in welcher Phase des Anmeldevorgangs der Fehler aufgetreten ist.

Mit NetScaler ADM können Sie die Fehlerdetails der Benutzeranmeldung in den folgenden Phasen des Anmeldevorgangs anzeigen:

- Authentifizierung
- Endpunktanalyse (EPA)
- Single Sign-On

In NetScaler ADM können Sie nach einem bestimmten Benutzer suchen und dann alle Details für diesen Benutzer anzeigen.

So suchen Sie nach einem Benutzer:

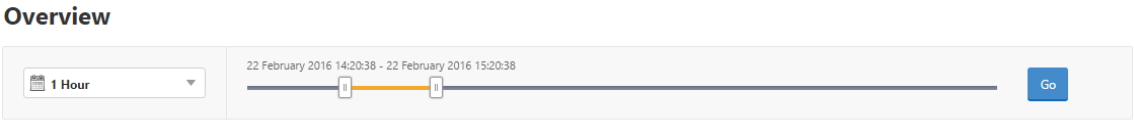
Navigieren Sie in NetScaler ADM zu **Gateway > Gateway Insight** und geben Sie im Textfeld Nach **Benutzern suchen** den Benutzer an, den Sie suchen möchten.

Authentifizierungsfehler

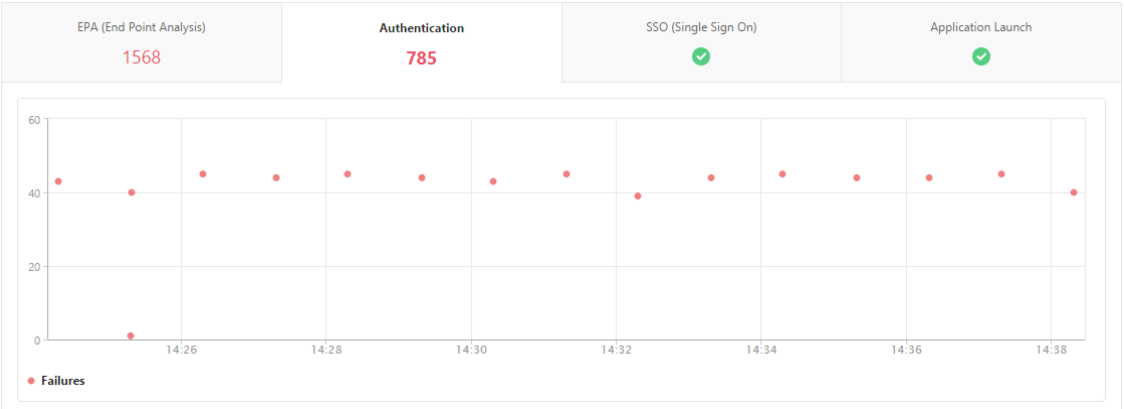
Sie können Authentifizierungsfehler wie falsche Anmeldeinformationen oder keine Antwort vom Authentifizierungsserver anzeigen. Sie können auch den Faktor sehen, bei dem die Authentifizierung fehlgeschlagen ist.

So zeigen Sie die Details zum Authentifizierungsfehler an:

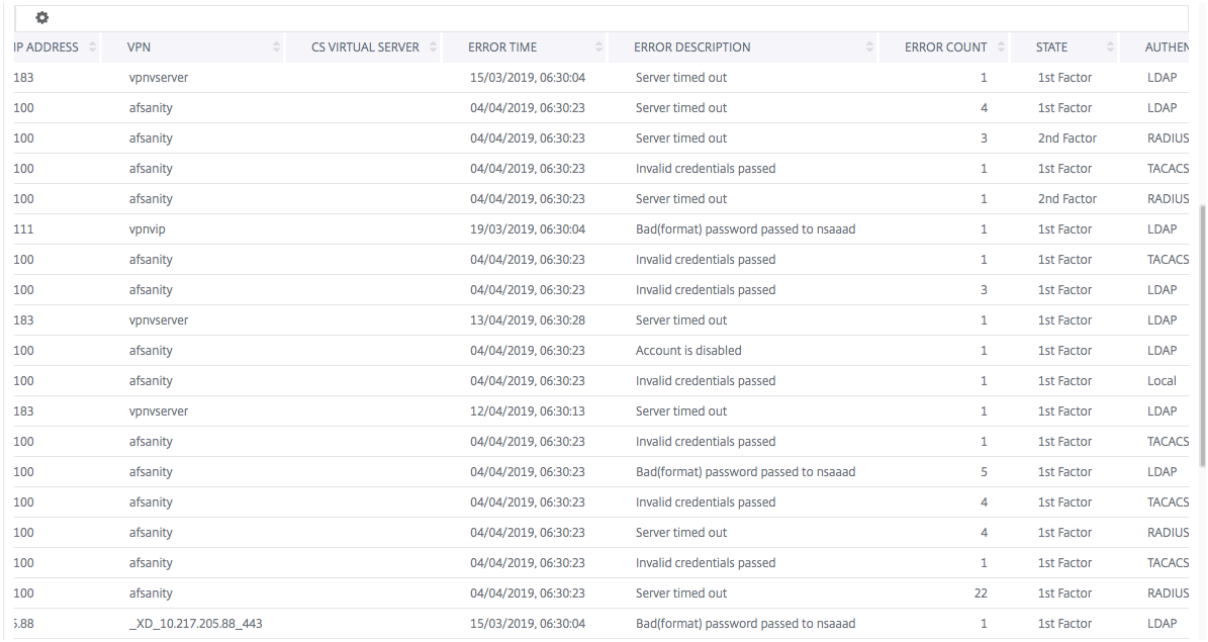
1. Navigieren Sie in NetScaler ADM zu **Gateway > Gateway Insight**.
2. Wählen Sie im Abschnitt **Übersicht** den Zeitraum aus, für den Sie die Authentifizierungsfehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.



3. Klicken Sie auf die Registerkarte **Authentifizierung**. Sie können die Anzahl der Authentifizierungsfehler zu einem bestimmten Zeitpunkt 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 der n-te Faktor angezeigt, bei dem der Fehler aufgetreten ist.



IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR TIME	ERROR DESCRIPTION	ERROR COUNT	STATE	AUTHEN
183	vpnvserver		15/03/2019, 06:30:04	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	3	2nd Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	1	2nd Factor	RADIUS
111	vpnvip		19/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	3	1st Factor	LDAP
183	vpnvserver		13/04/2019, 06:30:28	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Account is disabled	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	Local
183	vpnvserver		12/04/2019, 06:30:13	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Bad(format) password passed to nsaaad	5	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	4	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	22	1st Factor	RADIUS
.88	_XD_10.217.205.88_443		15/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die Authentifizierungsfehler und andere Details für diesen Benutzer anzuzeigen. Sie können die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen, indem Sie das Einstellungssymbol verwenden.

> **Wichtig:**
>
> Wenn die OAuth-OpenID Connect-Authentifizierung fehlschlägt, wird der Benutzername im Gateway Insight-Bericht für einige der Fehler als **NA** angezeigt, z. B. "Fehler bei der Token-Überprüfung". Bei diesem Fehler sind die Benutzernamen für einen Authentifizierungsfehler aufgrund eines "Fehlers bei der Token-Überprüfung"bei der OAuth-OpenID-Verbindungspartei nicht verfügbar.

USERNAME	CITRIX ADC IP ADDRESS	CLIENT IP ADDRESS	GATEWAY IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR DESCRIPTION
-NA-	[redacted]	[redacted]	[redacted]	gitest.citrix.com		Relying party: Token verification failed
-NA-	[redacted]	[redacted]	[redacted]	gitest.citrix.com		Relying party: Incoming URL query parameter from user agent is NULL in /nf/auth/doOAuth requ
-NA-	[redacted]	[redacted]	[redacted]	gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-	[redacted]	[redacted]	[redacted]	gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-	[redacted]	[redacted]	[redacted]	vpnvserver		Relying party: Token verification failed
-NA-	[redacted]	[redacted]	[redacted]	vpnvserver		Relying party: Token verification failed
-NA-	[redacted]	[redacted]	[redacted]	vpnvserver		Relying party: Token verification failed
-NA-	[redacted]	[redacted]	[redacted]	vpnvserver		Relying party: Token decryption failure

EPA-Fehler

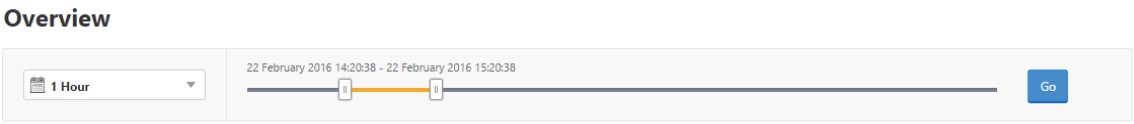
Sie können EPA-Fehler in der Vor- oder Nachauthentifizierungsphase anzeigen.

> **Wichtig:**
>
> NetScaler Gateway meldet EPA-Fehler an NetScaler ADM sowohl für klassische als auch für erweiterte Ausdrücke. Für die erweiterten Ausdrücke werden die Richtliniennamen nicht im Gate-

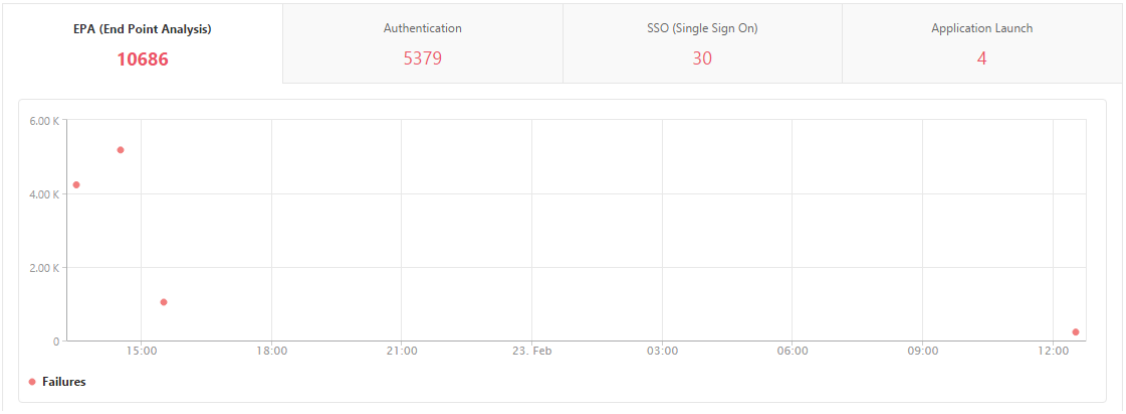
> way Insight-Dashboard angezeigt. Die Fehler werden gemeldet, wenn EPA als einer der Faktoren im nFactor-Authentifizierungsablauf konfiguriert ist.

So zeigen Sie EPA-Fehlerdetails an:

1. Navigieren Sie in NetScaler ADM zu **Gateway > Gateway Insight**.
2. Wählen Sie im Abschnitt Übersicht den Zeitraum aus, für den Sie die EPA-Fehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.



3. Klicken Sie auf die Registerkarte **EPA (Endpunktanalyse)**. Sie können die Anzahl der EPA-Fehler jederzeit im Diagramm **Fehler** anzeigen.



Scrollen Sie nach unten, um Details zu jedem EPA-Fehler wie **Benutzername, NetScaler-IP-Adresse, Gateway-IP-Adresse, VPN, Fehlerzeit, Richtlinienname, Gateway-Domainname** und mehr aus der Tabelle auf derselben Registerkarte anzuzeigen.

In der Spalte **Fehlerbeschreibung** in der Tabelle wird der Grund für den EPA-Fehler angezeigt. Beispielsweise wird die Fehlermeldung „Fehler bei der EPA-Pre-Auth Überprüfung“angezeigt, wenn eine EPA-Prüfung aufgrund von nFactor-EPA-Fehlern fehlschlägt.

In der Spalte **Richtlinienname** wird die Richtlinie angezeigt, die zu dem 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 anpassen, um Spalten hinzuzufügen oder zu löschen, indem Sie den Abwärtspfeil verwenden. Die Fall-ID wird bei Einträgen angezeigt, denen kein Benutzername zugewiesen wurde, wenn EPA als Faktor im nFactor-Authentifizierungsablauf verwendet wird.

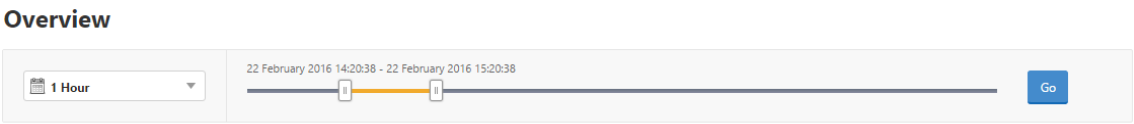
> **Hinweis**
>
> NetScaler Gateway meldet die EPA-Fehler nicht, wenn der Ausdruck “ClientSecurity”als Richtlinienregel für VPN-Sitzungen konfiguriert ist.

SSO-Fehler

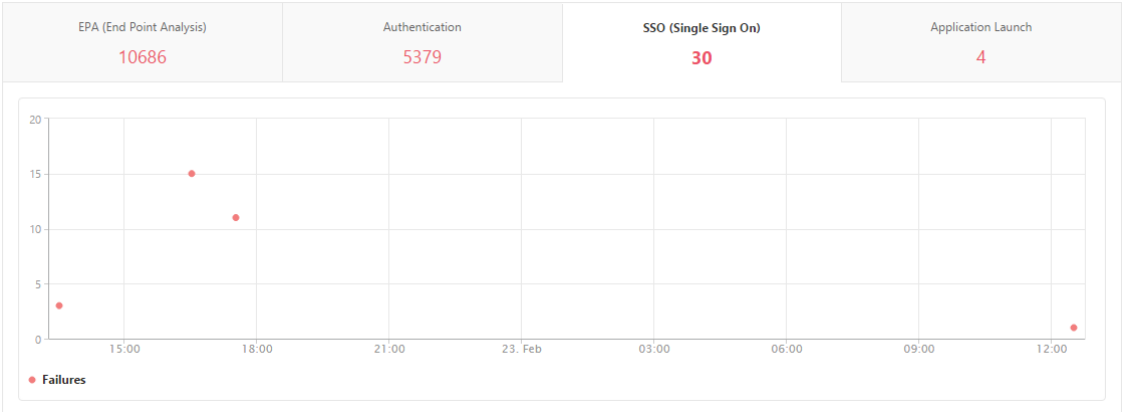
Sie können zu jedem Zeitpunkt alle SSO-Fehler für einen Benutzer einsehen, der über die NetScaler Gateway-Appliance auf beliebige Anwendungen zugreift.

So zeigen Sie die Details zum SSO-Fehler an:

1. Navigieren Sie in NetScaler ADM zu **Gateway > Gateway Insight**.
2. Wählen Sie im Abschnitt Übersicht den Zeitraum aus, für den Sie die SSO-Fehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. 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, NetScaler 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

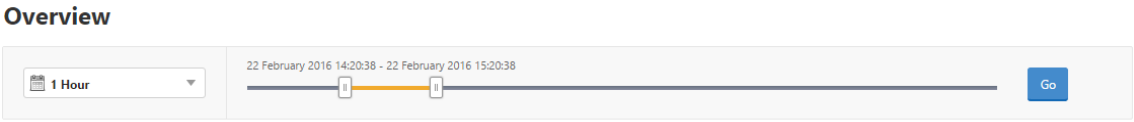
Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die SSO-Fehler und andere Details für diesen Benutzer anzuzeigen. Sie können die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen, indem Sie den Abwärtspfeil verwenden.

Nach erfolgreicher Anmeldung bei NetScaler Gateway kann ein Benutzer keine virtuelle Anwendung starten

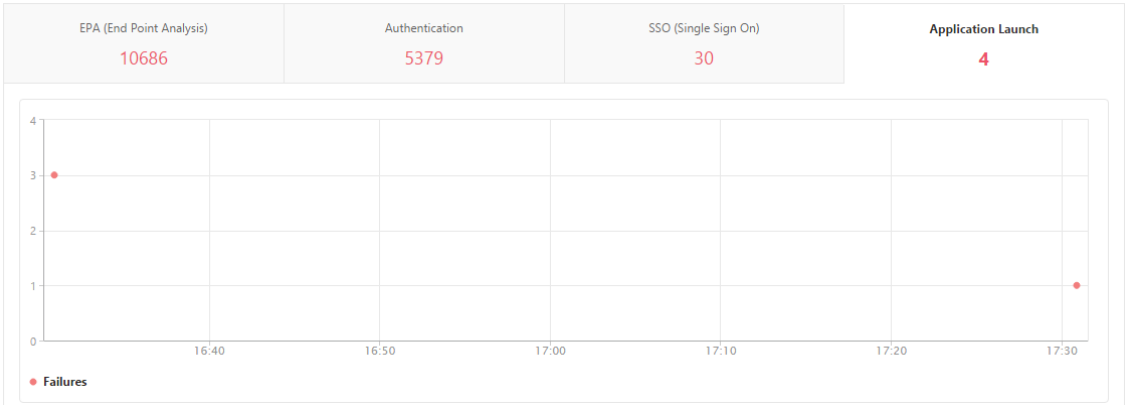
Bei einem Fehler beim Starten der Anwendung erhalten Sie Einblick in die Gründe, z. B. unzugängliche Secure Ticket Authority (STA) - oder Citrix Virtual App-Server oder ein ungültiges STA-Ticket. Sie können den Zeitpunkt des Auftretens des Fehlers, Details des Fehlers und die Ressource anzeigen, für die die STA-Validierung fehlgeschlagen ist.

So zeigen Sie Details zum Anwendungsstart an:

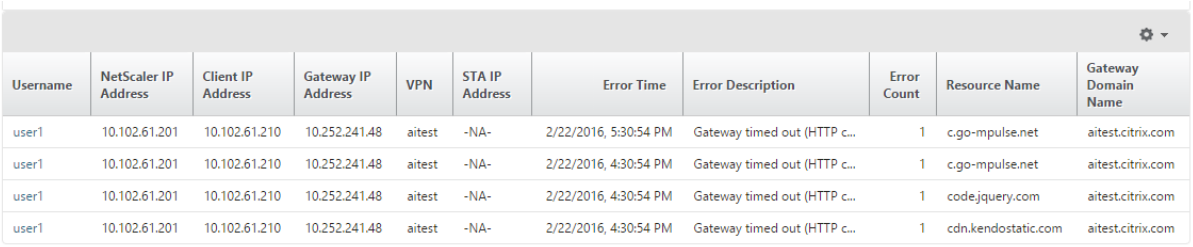
1. Navigieren Sie in NetScaler ADM zu **Gateway > Gateway Insight**.
2. Wählen Sie im Abschnitt **Übersicht** den Zeitraum aus, für den Sie die SSO-Fehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.



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 durch, um Details zu jedem Anwendungsstartfehler wie **NetScaler 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

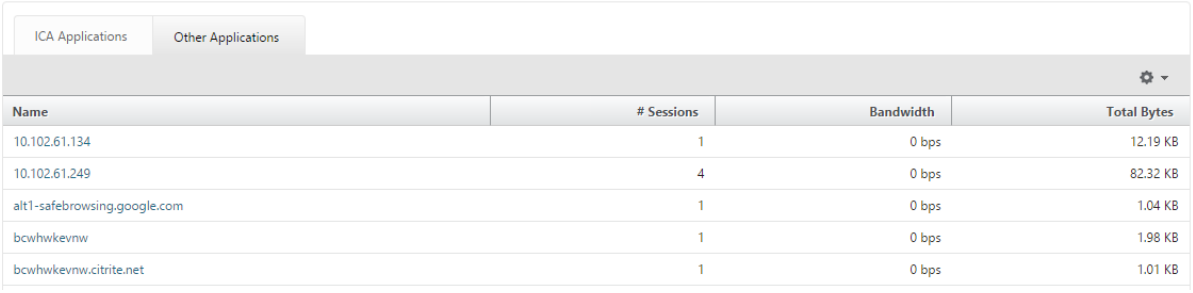
Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die Programmstartfehler und andere Details für diesen Benutzer anzuzeigen. Sie können die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen, indem Sie den Abwärtspfeil verwenden.

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 NetScaler ADM die Gesamtbytes und die Bandbreite anzeigen, die von dieser Anwendung verbraucht werden.

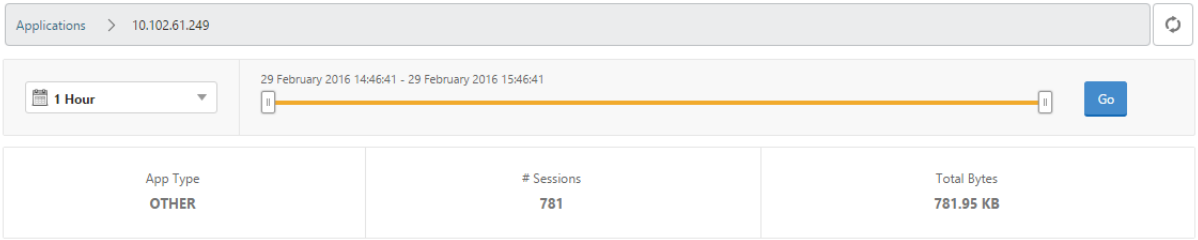
So zeigen Sie die Gesamtanzahl von Bytes und Bandbreite an, die von einer Anwendung verbraucht wird:

Navigieren Sie in NetScaler ADM zu **Gateway > Gateway Insight > Applications**, scrollen Sie nach unten und klicken Sie auf der Registerkarte **Andere Anwendungen** auf die Anwendung, für die Sie die Details anzeigen möchten.

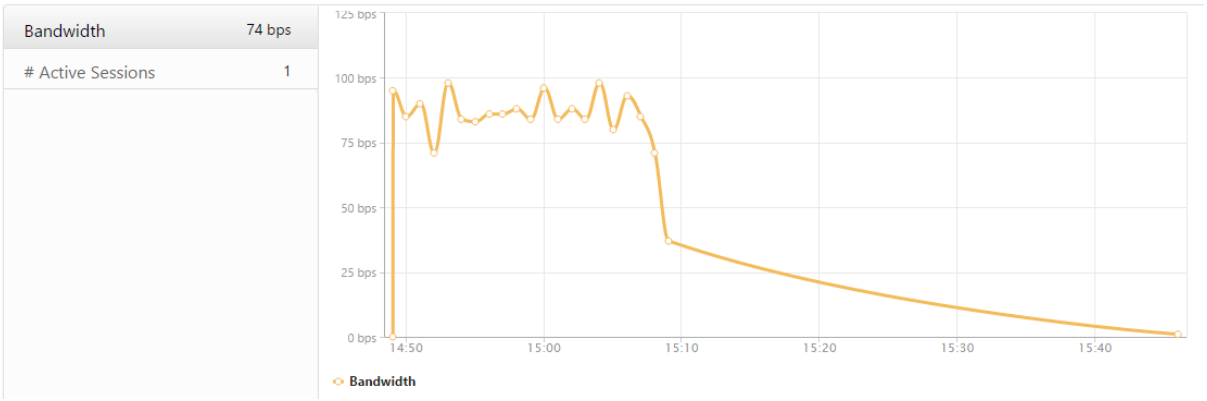


Name	# Sessions	Bandwidth	Total Bytes
10.102.61.134	1	0 bps	12.19 KB
10.102.61.249	4	0 bps	82.32 KB
alt1-safebrowsing.google.com	1	0 bps	1.04 KB
bcwhwkevnw	1	0 bps	1.98 KB
bcwhwkevnw.citrite.net	1	0 bps	1.01 KB

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.

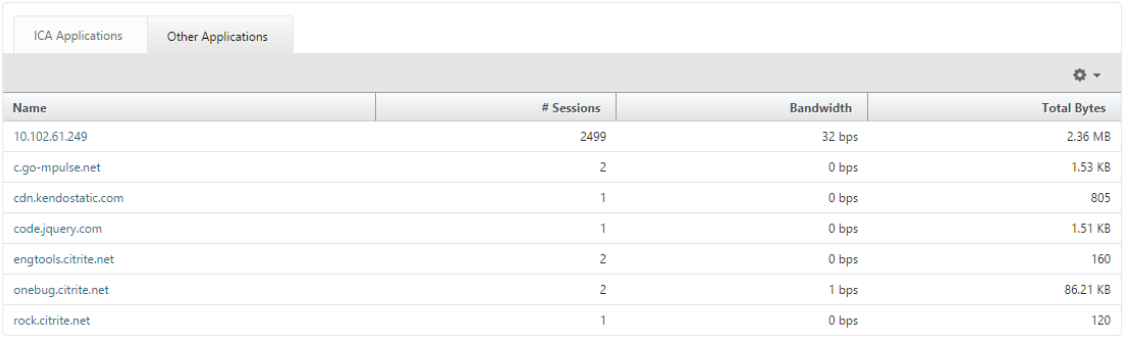


Ein Benutzer hat sich erfolgreich bei NetScaler Gateway angemeldet, kann jedoch nicht auf bestimmte Netzwerkressourcen im internen Netzwerk zugreifen

Mit Gateway Insight können Sie feststellen, ob der Benutzer Zugriff auf die Netzwerkressourcen hat oder nicht. Sie können auch den Namen der Richtlinie anzeigen, die zu dem Fehler geführt hat.

So zeigen Sie den Benutzerzugriff auf Ressourcen an:

1. Navigieren Sie in NetScaler ADM zu **Gateway > Gateway Insight > Applications**.
2. Scrollen Sie auf dem angezeigten Bildschirm nach unten, und wählen Sie 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

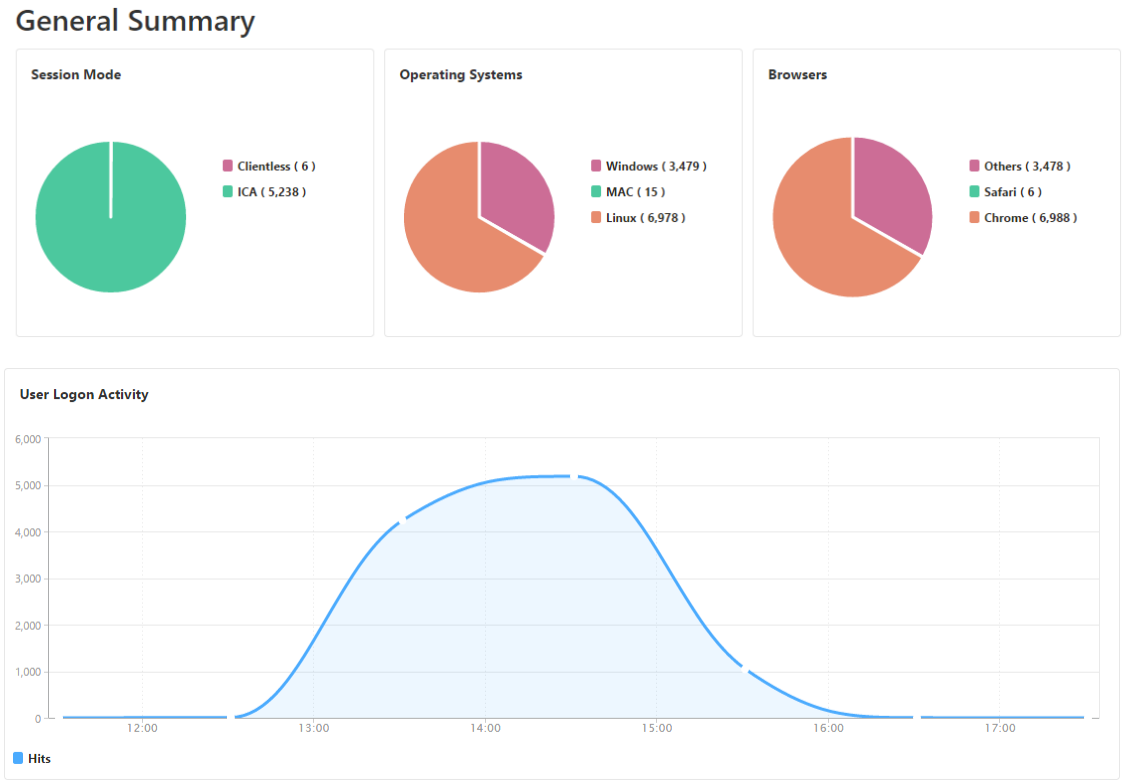
3. Scrollen Sie nach unten und in der Tabelle **Benutzer** werden alle Benutzer angezeigt, die Zugriff auf diese Anwendung haben.

Verschiedene Benutzer verwenden möglicherweise unterschiedliche NetScaler Gateway Bereitstellungen oder melden sich über unterschiedliche Zugriffsmodi bei NetScaler Gateway 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 festlegen, ob die Bereitstellung eines Benutzers ein einheitliches Gateway oder eine klassische NetScaler Gateway-Bereitstellung ist. Bei Unified Gateway Bereitstellungen können Sie den Namen und die IP-Adresse des virtuellen Content Switching-Servers sowie den Namen des virtuellen VPN-Servers anzeigen.

Um die Zusammenfassung der Sitzungsmodi, der Art der Clients und der Anzahl der angemeldeten Benutzer anzuzeigen, gehen Sie wie folgt vor:

1. Navigieren Sie in NetScaler ADM zu **Gateway > 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.



Gateway Insight-Probleme beheben

February 5, 2024

Wenn die Gateway Insight-Lösung nicht wie erwartet funktioniert, liegt das Problem möglicherweise an einer der folgenden Ursachen. Informationen zur Fehlerbehebung finden Sie in den Checklisten in den entsprechenden Abschnitten.

- Gateway Insight-Konfiguration.
- Verbindungsproblem zwischen NetScaler und NetScaler ADM.
- Datensatzgenerierung in NetScaler.
- Validierungen in NetScaler ADM.

Checkliste für die Konfiguration von Gateway Insight

- Stellen Sie sicher, dass die AppFlow-Funktion in der NetScaler Appliance aktiviert ist. Einzelheiten finden Sie unter AppFlow aktivieren.
- Überprüfen Sie die Gateway Insight-Konfiguration in der laufenden Konfiguration von NetScaler.

Führen Sie den Befehl `show running | grep -i <appflow_policy>` 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
<!--NeedCopy-->
```

Der Bind-Typ OTHERTCP_REQUEST ist auch für Gateway Insight erforderlich.

```
bind vpn vserver afsanity -policy afp -priority 100 -type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```

- 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 HDX Insight-Datenerfassung aktivieren.
- Für Double-Hop muss Gateway Insight auf beiden Hops konfiguriert sein.
- Überprüfen Sie die Parameter `appflowlog` auf dem virtuellen NetScaler Gateway/VPN-Server. Einzelheiten finden Sie unter AppFlow für virtuelle Server aktivieren.

Konnektivität zwischen NetScaler und NetScaler ADM Checkliste

- Überprüfen Sie den AppFlow Collector-Status in NetScaler. Einzelheiten finden Sie unter So überprüfen Sie den Status der Konnektivität zwischen NetScaler 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 **Einstellungen > AppFlow > Richtlinien** navigieren, um die AppFlow-Richtlinientreffer zu überprüfen.
- Überprüfen Sie jede Firewall, die AppFlow Ports 4739 oder 5557 blockiert.

Datensatzgenerierung in NetScaler Checkliste

- Führen Sie den Befehl `nsconmsg -d stats -g ai_tot` aus und suchen Sie nach den Statistik-Inkrementen in NetScaler.
- Zeichnen Sie `nstrace logs` auf und prüfen Sie CFLOW-Pakete, um zu bestätigen, dass NetScaler AppFlow-Datensätze exportiert.

> **Hinweis:**
>
> Die `nstrace logs` sind nur für IPFIX erforderlich. Bei Logstream bestätigen nstrace-Protokolle nicht, ob die ADC-Appliance die AppFlow-Datensätze exportiert hat.

Validierung von Datensätzen in NetScaler 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 NetScaler ADM AppFlow-Einträge erhält.
- Stellen Sie sicher, dass die NetScaler-Instanz zum NetScaler ADM hinzugefügt wird.
- Stellen Sie sicher, dass der virtuelle NetScaler Gateway/VPN-Server in NetScaler ADM lizenziert ist.

Validierung von Logstream-Protokollen in NetScaler ADM

Die Validierung der von NetScaler ADM empfangenen Logstream-Daten kann mit den folgenden Methoden erfolgen:

- **Aktivieren der Datendatensatzprotokollierung in NetScaler ADM**

  Nach der Aktivierung können die Protokolle in /var/mps/log/mps_afdecoder.log angezeigt werden

- **Aktivieren der Protokollierung von ULFD-Bibliothek**

  Führe den Befehl aus `/mps/decoder_enable_debug`

  Die Protokolle werden in `/var/ulflog/libulfd.log` aufgezeichnet

  Sie können die Protokollierung mit dem Befehl `/mps/decoder_disable_debug` deaktivieren

Gateway Insight-Zähler

Die folgenden Gateway Insight-Leistungsindikatoren 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
- ai_tot_appflow_pol_eval_in_gwinsight
- ai_tot_app_launch_success

AppFlow-Einträge im NetScaler-Protokoll

Ab Release 13.0 Build 71.x können Sie die NetScaler-Protokolle überprüfen, um zu bestätigen, ob die AppFlow-Datensätze exportiert werden. Die Standardprotokollstufe von `syslogparams` erfasst alle Fehler- und Informationsprotokolle. Falls Sie keine Ahnung über die Fehler finden, aktivieren Sie alle Protokollebenen einschließlich DEBUG in `syslogparams`, um sogar die DEBUG-Protokolle zu erfassen.

Beispielprotokolle

```
1 <local0.info> … GMT 0-PPE-0 : default SSLVPN Message 147 0 : "
     GwInsight: Sent auth record Func=ns_sslvpn_export_auth_data Username
     =<name> Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid>
     Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<
     vpnfqdn> Authtype=3 EPAid=(null) AuthStage=1 AuthDuration=309
     AuthAgent=<auth_server_ip> Groupname= Policyname=<name>
     CurfactorPolname=<name> NextfactorPolname= CSecExpr= Devicetype
     =16777219 Deviceid=0 email="
2 <local0.err> … GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight
     : Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is
     zero"
3 <local0.err> … GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight
     : Func=update_session_appflow_collector pcb or session is NULL"
4 <local0.info> … GMT 0-PPE-0 : default SSLVPN Message 165 0 : "
     GwInsight: Sent session update record Func=
     ns_sslvpn_send_update_record Username=<> Clientip=<ip>:<port> Destip
     =<ip>:80 SessSeq=1 Sessid=<sessid> Gwip=<ip>:443 StatusCode=0
     CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=0 SessState
     =2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/Citrix/Store
5 Web BackendServername= SSOurl= email="
6 SSO logs:
7 <!--NeedCopy-->
```



```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 463 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=1
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 582 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=3
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 513 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=2
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:443 SessSeq=c Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =155 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=6
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

Wenden Sie sich an den technischen Support von Citrix

Stellen Sie für eine schnelle Lösung sicher, dass Sie über die folgenden Informationen verfügen, bevor Sie sich an den technischen Support von Citrix wenden:

- Einzelheiten zur Bereitstellung und Netzwerktopologie.
- NetScaler- und NetScaler ADM-Versionen.
- Technisches Support-Paket für NetScaler und NetScaler ADM.
- `nstrace` während der Ausgabe erfassen.

Bekannte Probleme

Bekannte Probleme mit Gateway Insight finden Sie in den ADC-Versionshinweisen.

HDX Insight

February 5, 2024

HDX Insight bietet einen umfassenden Überblick über den HDX-Verkehr an Citrix Virtual Apps and Desktop, der über NetScaler übertragen wird. Außerdem können Administratoren Client- und Netzwerklatenzmetriken, historische Berichte und End-to-End-Leistungsdaten in Echtzeit anzeigen und Leistungsprobleme beheben. Die Verfügbarkeit von Echtzeit- und historischen Sichtbarkeitsdaten ermöglicht es NetScaler Application Delivery Management (ADM), eine Vielzahl von Anwendungsfällen zu unterstützen.

Damit Daten angezeigt werden, müssen Sie AppFlow auf Ihren virtuellen NetScaler Gateway-Servern aktivieren. AppFlow kann über das IPFIX-Protokoll oder die LogStream-Methode bereitgestellt werden.

> **Hinweis**
>
> Aktivieren Sie die folgenden Richtlinieneinstellungen, damit ICA-Rundtrip-Zeitberechnungen protokolliert werden können:

- ICA Roundtrip Berechnung
- ICA-Roundtrip-Berechnungs
- 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 Bandbreiteninformationen auch von einzelnen virtuellen Kanälen wie Audio, Druckerzuordnung und Clientlaufwerkszuordnung abrufen.

> **Hinweis**
>
> Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, Zugriff auf Anwendungsebene für die Gruppe gewähren und Benutzer der Gruppe zuweisen. NetScaler ADM Analytics unterstützt jetzt die auf virtuellen IP-Adressen basierende 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 zum Zuweisen von Benutzern zur Gruppe finden Sie unter Konfigurieren von Gruppen.

Sie können auch zu **Gateway > HDX Insight > Applications** navigieren und auf **Startdauer**klicken, um die Zeit anzuzeigen, die für den Start der Anwendung benötigt wird. Sie können auch den Benutzeragents aller verbundenen Benutzer anzeigen, indem Sie zu **Gateway > HDX Insight > Benutzer** navigieren.

> **Hinweis:** HDX Insight unterstützt Admin Partitions, die in NetScaler Instanzen konfiguriert sind, die auf der 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

Identifizierung der Hauptursache für Probleme mit langsamer Leistung

Szenario 1

Der Benutzer hat Verzögerungen beim Zugriff auf Citrix Virtual Apps and Desktops.

Die Verzögerungen können auf Latenz im Servernetzwerk, durch das Servernetzwerk verursachte ICA-Verkehrsverzögerungen oder Latenz im Client-Netzwerk zurückzuführen sein.

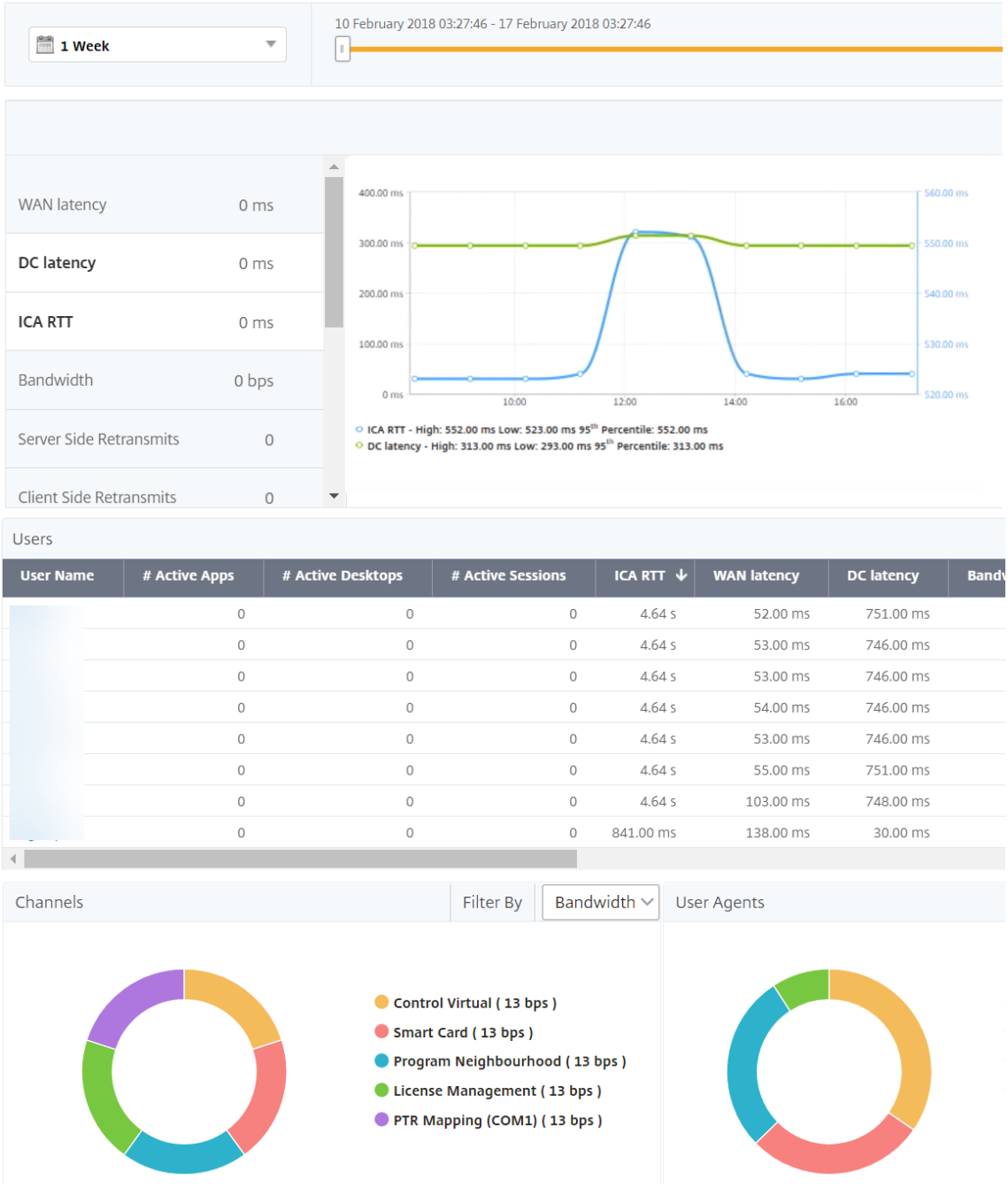
Analysieren Sie die folgenden Metriken, um die Grundursache des Problems zu ermitteln:

- WAN-Latenz
- DC-Latenz
- Hostverzögerung

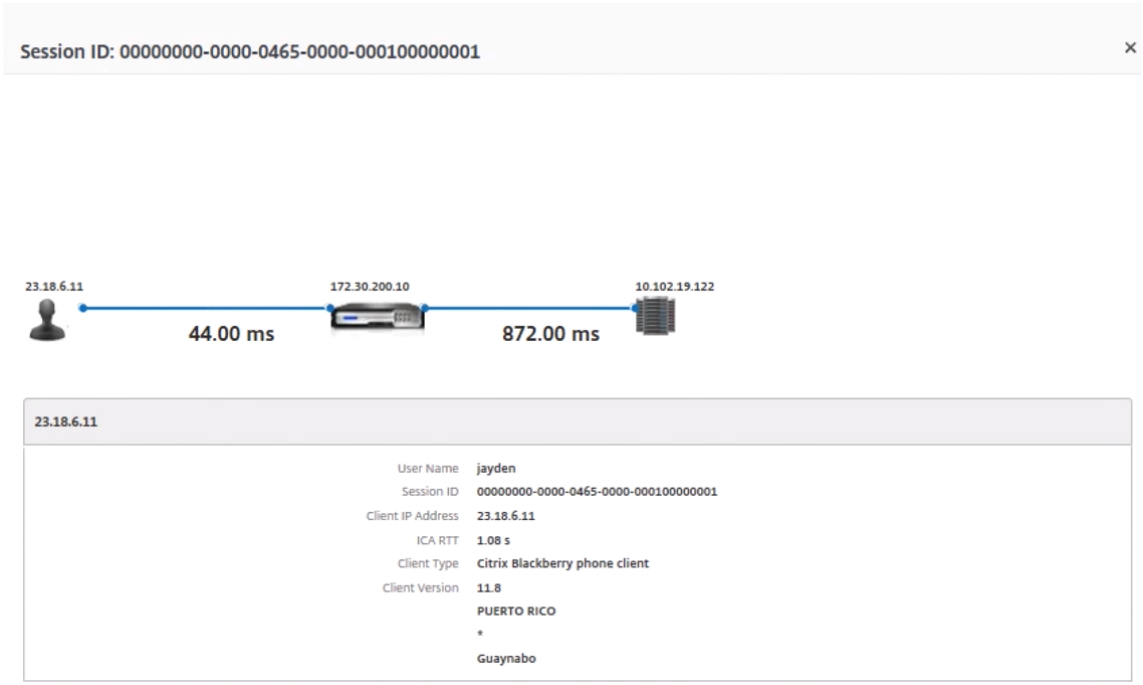
So zeigen Sie die Client-Metriken an:

1. Navigieren Sie zu **Gateway > 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, ein 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 Sitzungen**den Mauszeiger über den**RTT-Wert**, und notieren Sie die Hostverzögerung, DC-Latenz und WAN-Latenz.
5. Klicken Sie in der Tabelle**Aktuelle Sitzungen** 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 die **Hostverzögerungen** 6 Sekunden. Dies weist darauf hin, dass es beim Benutzer aufgrund der vom Servernetzwerk verursachten durchschnittlichen Latenz zu Verzögerungen kommt.

Szenario 2

Beim Starten einer Anwendung auf Citrix Virtual App oder Desktop kommt es beim Benutzer zu Verzögerungen

Die Verzögerung kann auf Latenz im Servernetzwerk, durch das Servernetzwerk verursachte ICA-Verkehrsverzögerungen, Latenz im Client-Netzwerk oder auf die zum Starten einer Anwendung benötigte Zeit zurückzuführen sein.

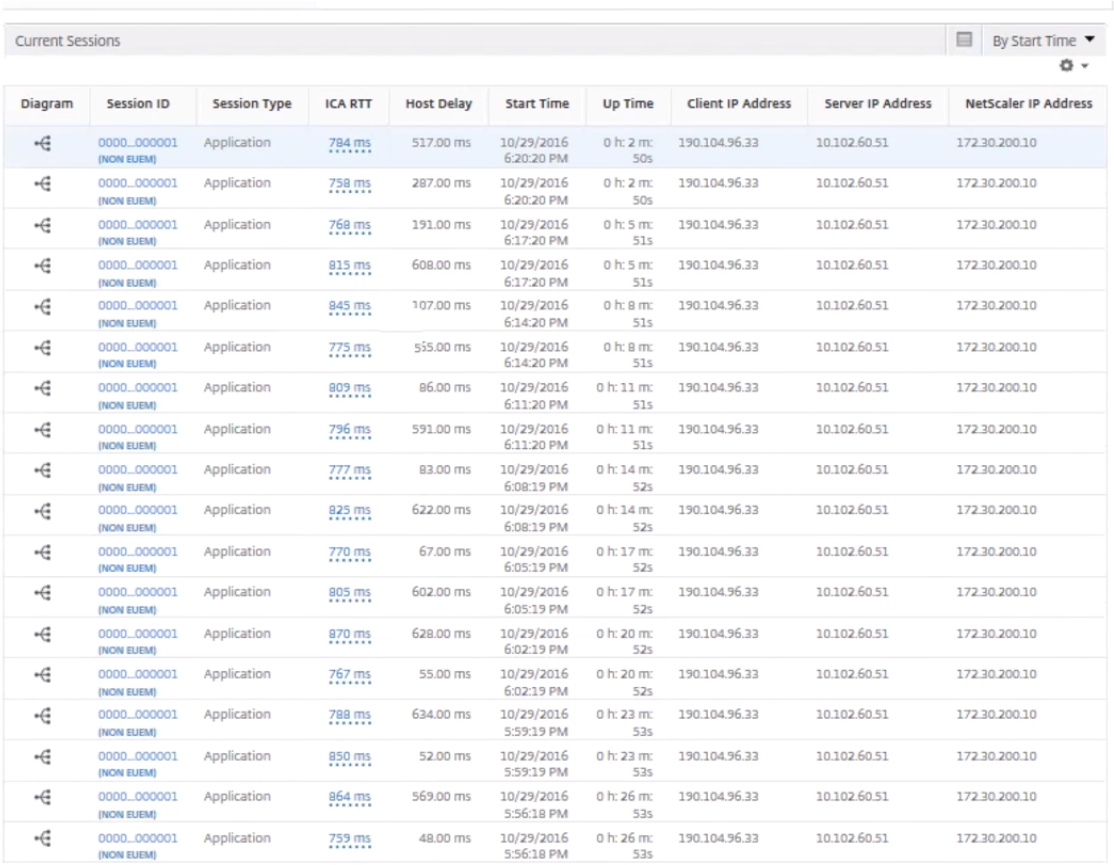
Analysieren Sie die folgenden Metriken, um die Grundursache des Problems zu ermitteln:

- WAN-Latenz
- DC-Latenz
- Host-Verzögerung

So zeigen Sie die Benutzermetriken an:

1. Navigieren Sie zu **Gateway > HDX Insight > Benutzer .**
2. Scrollen Sie nach unten und klicken Sie auf den Benutzernamen

3. Beachten Sie in der grafischen Darstellung die WAN-Latenz-, DC-Latenz- und RTT-Werte für die jeweilige Sitzung.
4. Beachten Sie, dass die Hostverzögerung in der Tabelle **Aktuelle Sitzungen**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	515.00 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, aber die **Host-Delay** beträgt 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 NetScaler ADM verwenden, auf dem Software 11.1 Build 51.21 oder höher ausgeführt wird. Um diese Metriken anzuzeigen, navigieren Sie zu **Gateway > HDX Insight > Benutzer** und wählen Sie einen Benutzernamen aus. Die Benutzermetriken werden in der Tabelle neben dem Diagramm angezeigt.

Geomaps für HDX Insight

Die NetScaler ADM Geomaps-Funktion zeigt die Nutzung von Anwendungen an verschiedenen geografischen Standorten auf einer Karte an. Administratoren können diese Informationen verwenden, um die Trends bei der Anwendungsnutzung an verschiedenen geografischen Standorten zu verstehen.

Sie können NetScaler ADM so konfigurieren, dass die Geomaps für einen bestimmten geografischen Standort oder ein bestimmtes LAN angezeigt werden, indem Sie den privaten IP-Bereich (Start- und End-IP-Adresse) für den Standort angeben.

Sie können auch die Details der historischen und aktiven Benutzer in den Geostandskarten in HDX Insight anzeigen. Navigieren Sie zu **Gateway > HDX Insight**, und klicken Sie im Abschnitt **World** der Karte auf das Land oder die Region, für die Sie die Details anzeigen möchten. Sie können weiter aufgliedern, um Informationen nach Stadt und Bundesland anzuzeigen.

So konfigurieren Sie eine Geomap für Rechenzentren:

Navigieren Sie zu **Einstellungen > Analytics-Einstellungen > IP-Blöcke**, um Geomaps für einen bestimmten Standort zu konfigurieren.

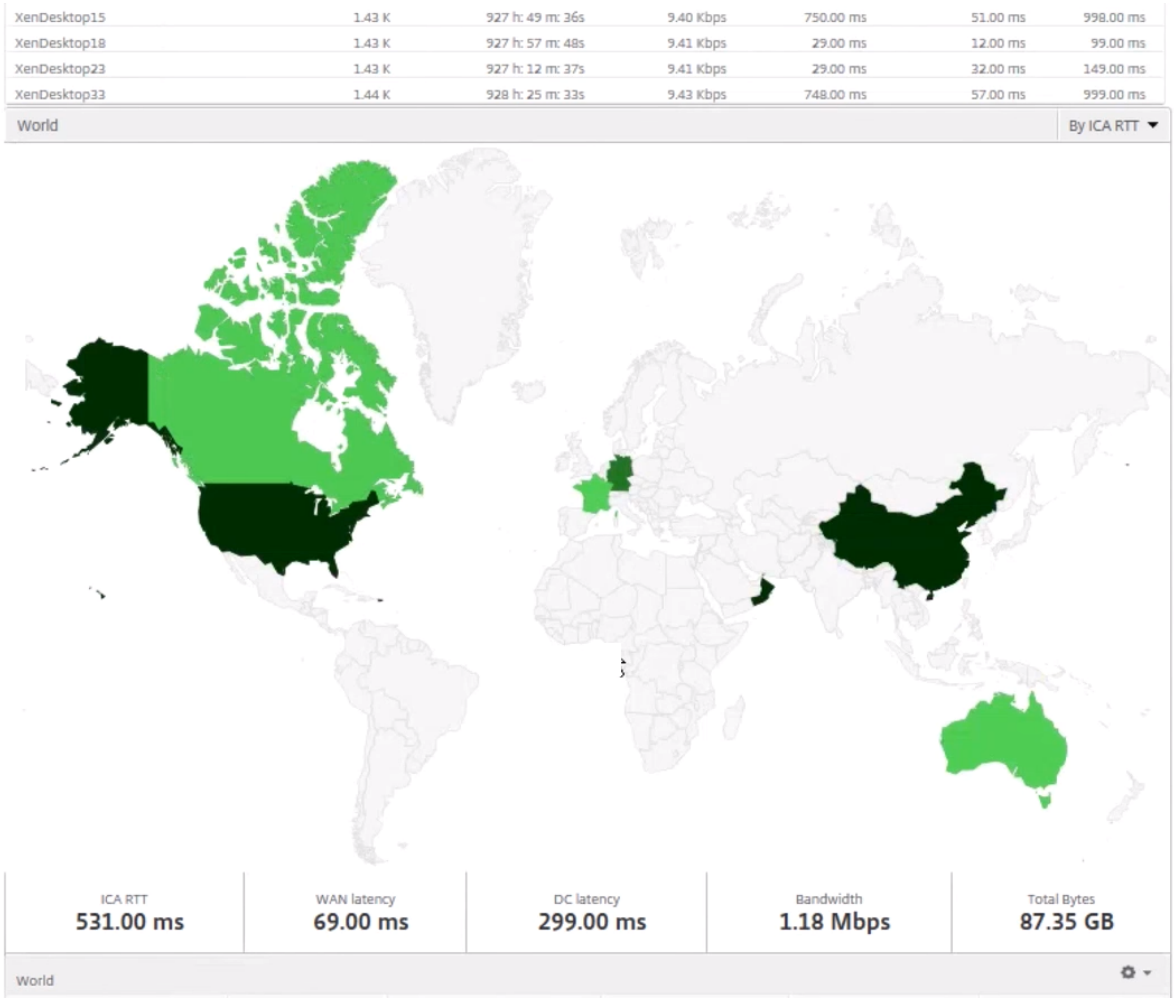
Anwendungsfall

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 NetScaler Gateway-Appliance auf SClara.x.com, um auf den VPN-Verkehr zuzugreifen. Die indischen Benutzer verwenden die NetScaler Gateway-Appliance auf India.x.com, um auf den VPN-Verkehr zuzugreifen.

Während eines bestimmten Zeitintervalls, beispielsweise von 10 bis 17 Uhr, stellen die Benutzer in Santa Clara eine Verbindung zu Sclara.x.com her, um auf den VPN-Verkehr zuzugreifen. Die meisten Benutzer greifen auf dasselbe NetScaler Gateway zu, was zu einer Verzögerung bei der Verbindung mit dem VPN führt, sodass einige Benutzer eine Verbindung zu India.x.com anstelle von SClara.x.com herstellen.

Ein NetScaler-Administrator, der den Datenverkehr analysiert, kann die Geokarten-Funktionalität verwenden, um den Datenverkehr im Büro von Santa Clara anzuzeigen. Die Karte zeigt, dass die Reaktionszeit im Büro von Santa Clara hoch ist, da das Büro in Santa Clara nur über ein NetScaler Gateway Gerät verfügt, über das Benutzer auf VPN-Datenverkehr zugreifen können. Der Administrator kann daher entscheiden, ein anderes NetScaler Gateway zu installieren, sodass Benutzer über zwei lokale NetScaler Gateway-Geräte verfügen, über die auf das VPN zugreifen können.



Einschränkungen

Wenn NetScaler-Instances über eine Advanced-Lizenz verfügen, werden die in NetScaler ADM für HDX Insight festgelegten Schwellenwerte nicht ausgelöst, da Analysedaten nur für eine Stunde erfasst wer-

den.

Aktivieren der HDX Insight Datenerfassung

February 5, 2024

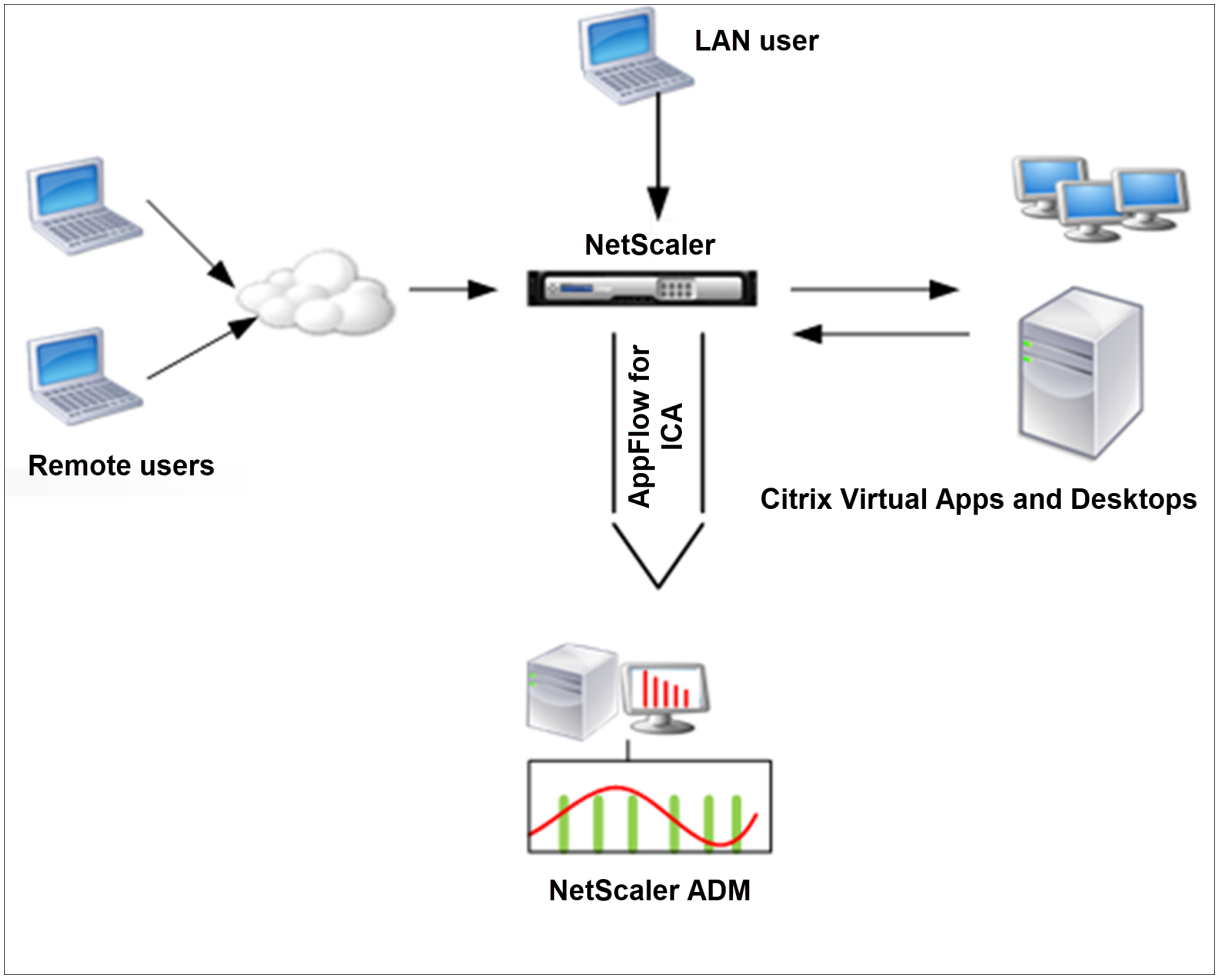
HDX Insight ermöglicht es der IT, ein außergewöhnliches Benutzererlebnis zu bieten, indem es beispiellose durchgängige Einblicke in den ICA-Verkehr bietet, der die NetScaler-Instances durchläuft. HDX Insight ist Teil von NetScaler Application Delivery Management (ADM) Analytics. HDX Insight bietet überzeugende 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 im NetScaler unterscheidet sich von der Position der Appliance in der Bereitstellungstopologie.

Aktivierung der Datenerfassung für die Überwachung von NetScalern, die im LAN-Benutzermodus eingesetzt werden

Externe Benutzer, die auf Citrix Virtual App- und Desktop-Anwendungen zugreifen, müssen sich am NetScaler Gateway authentifizieren. Interne Benutzer müssen jedoch möglicherweise nicht an NetScaler Gateway weitergeleitet werden. Außerdem muss der Administrator in einer Bereitstellung im transparenten Modus die Routingrichtlinien manuell anwenden, damit die Anforderungen an die NetScaler Appliance umgeleitet werden.

Um diese Herausforderungen zu meistern und LAN-Benutzer direkt mit Citrix Virtual App- und Desktop-Anwendungen zu verbinden, können Sie das NetScaler Gerät im LAN-Benutzermodus bereitstellen, indem Sie einen virtuellen Cacheumleitungsserver konfigurieren, der als SOCKS-Proxy auf dem NetScaler Gateway Gerät fungiert.



> **Hinweis:** NetScaler ADM und NetScaler Gateway Gerät befinden sich im selben Subnetz.

Um in diesem Modus bereitgestellte NetScaler Appliances zu überwachen, fügen Sie zuerst die NetScaler Appliance zur NetScaler Insight-Bestandsliste hinzu, aktivieren Sie AppFlow und zeigen Sie dann die Berichte im Dashboard an.

Nachdem Sie die NetScaler Appliance zur NetScaler ADM Bestandsliste hinzugefügt haben, müssen Sie AppFlow für die Datenerfassung aktivieren.

> **Hinweis**
>
> - Auf einer ADC-Instanz können Sie zu **Settings > AppFlow > Collectors**navigieren, um zu überprüfen, ob der Collector (d. h. NetScaler ADM) aktiv ist oder nicht. Die NetScaler Instanz sendet AppFlow Datensätze mithilfe von NSIP an NetScaler ADM. Die Instanz verwendet jedoch ihren SNIP, um die Konnektivität mit NetScaler ADM zu überprüfen. Stellen Sie also sicher, dass das SNIP auf der Instanz konfiguriert ist.
> - Sie können die Datenerfassung auf einem NetScaler, der im LAN-Benutzermodus bereitgestellt wird, nicht mithilfe des NetScaler ADM Konfigurationsdienstprogramms aktivieren.

- Detaillierte Informationen zu den Befehlen und ihrer Verwendung finden Sie in der Befehlsreferenz .
- Informationen zu Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke .

So konfigurieren Sie die Datenerfassung auf einer NetScaler Appliance mithilfe der Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Melden Sie sich bei einer 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 NetScaler Gateway-Gerät auf das LAN-Netzwerk zugreifen, fügen Sie eine Aktion hinzu, die durch eine Richtlinie angewendet wird, die dem VPN-Verkehr entspricht.

```
add vpn trafficAction <name> <qual> [-HDX ( ON or 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 NetScaler ADM als AppFlow Collector auf der NetScaler Appliance hinzu.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Example:

‘‘‘

add appflow collector MyInsight -IPAddress 192.168.1.101

‘‘‘

4. Erstellen Sie eine AppFlow Aktion, und ordnen Sie den Kollektor der Aktion zu.

```
add appflow action <name> -collectors <string>
```

Beispiel:

```
add appflow action act -collectors MyInsight
```

5. Erstellen Sie eine AppFlow Richtlinie, um die Regel zum Generieren des Datenverkehrs anzugeben.

```
add appflow policy <policyname> <rule> <action>
```

Beispiel:

```
add appflow policy pol true act
```

6. Binden Sie die AppFlow-Richtlinie an einen globalen Bindepunkt.

```
bind appflow global <policyname> <priority> -type <type>
```

Beispiel:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> **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
```

Beispiel:

```
set appflow param -flowRecordInterval 60
```

8. Speichern Sie die Konfiguration. Typ: `save ns config`

Aktivieren der Datenerfassung für im Single-Hop-Modus bereitgestellte NetScaler Gateway-Geräte

Wenn Sie NetScaler Gateway im Single-Hop-Modus bereitstellen, befindet es sich am Netzwerkrand. Die Gateway-Instanz stellt ICA-Proxy-Verbindungen zur Desktop-Bereitstellungsinfrastruktur bereit. Single-Hop ist das einfachste und gebräuchlichste Deployment. Der Single-Hop-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 NetScaler-Appliances zu.

Um mit der Erfassung der Berichte zu beginnen, müssen Sie die NetScaler Gateway-Appliance zum NetScaler ADM-Inventar (Application Delivery Management) hinzufügen und AppFlow auf ADM aktivieren.

So aktivieren Sie die AppFlow Funktion von NetScaler ADM:

1. Geben Sie in einem Webbrowser die IP-Adresse des NetScaler ADM ein (z. B. http://192.168.100.1).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **Infrastruktur > Instanzen** und wählen Sie die NetScaler-Instanz aus, für die Sie Analysen aktivieren möchten.
4. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
5. Wählen Sie die virtuellen VPN-Server aus, und klicken Sie auf **Analytics aktivieren**.
6. Wählen Sie **HDX Insight** und dann **ICA** aus.
7. Klicken Sie auf **OK**.

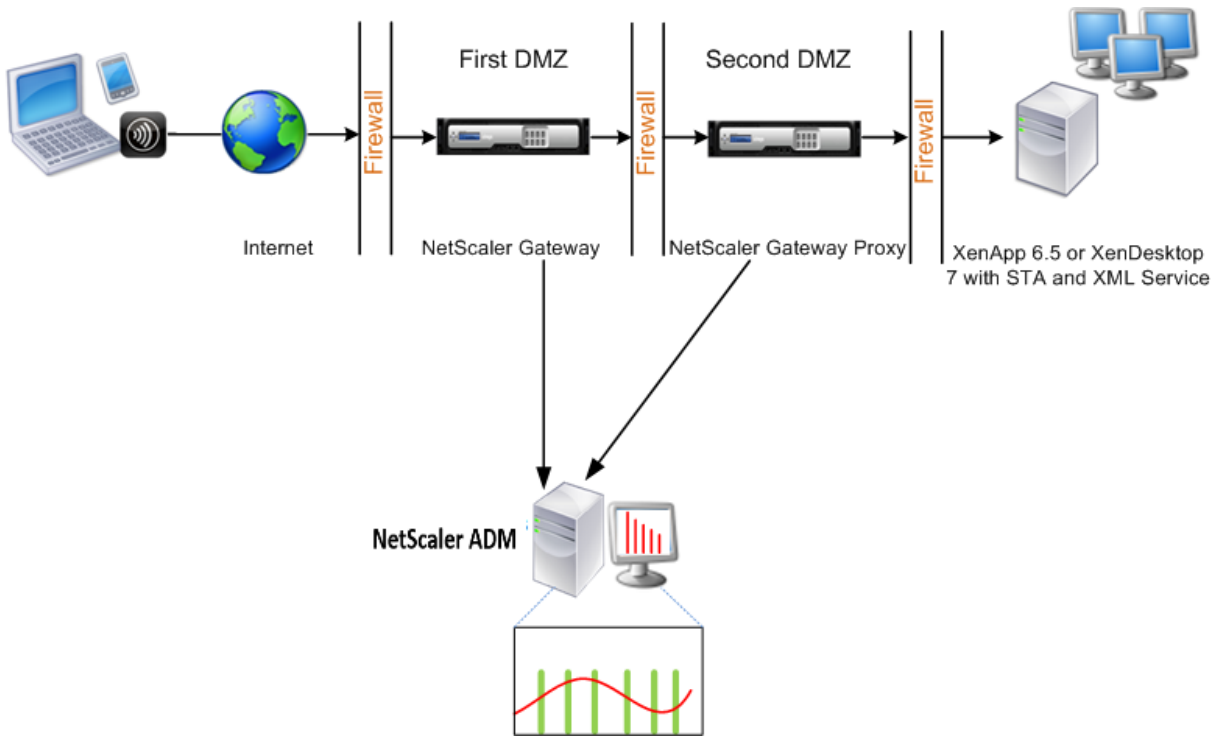
> **Hinweis**
>
> Wenn Sie AppFlow im Single-Hop-Modus aktivieren, werden die folgenden Befehle im Hintergrund ausgeführt. Diese Befehle werden hier explizit zur Fehlerbehebung angegeben.

```
- 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
```


Virtuelle EUEM-Kanaldaten sind Teil von HDX Insight Daten, die NetScaler ADM von Gateway-Instanzen erhält. Der virtuelle EUEM-Kanal stellt die Daten über ICA-RTT bereit. Wenn der virtuelle EUEM-Kanal nicht aktiviert ist, werden die verbleibenden HDX Insight Daten weiterhin in NetScaler ADM angezeigt.

Aktivieren der Datenerfassung für im Double-Hop-Modus bereitgestellte NetScaler Gateway-Geräte

Der NetScaler Gateway -Doppelhop-Modus bietet zusätzlichen Schutz für das interne Netzwerk einer Organisation, da ein Angreifer mehrere Sicherheitszonen oder demilitarisierte Zonen (DMZ) durchdringen muss, um die Server im sicheren Netzwerk zu erreichen. Wenn Sie die Anzahl der Hops (NetScaler Gateway Geräte) analysieren möchten, über die die ICA-Verbindungen weitergeleitet werden, sowie die Details zur Latenz für jede TCP-Verbindung und wie sie mit der gesamten ICA-Latenz verglichen wird, die vom Client wahrgenommen wird, müssen Sie NetScaler ADM installieren, damit die NetScaler Gateway-Geräte diese wichtigen Statistiken zu berichten.



Das NetScaler Gateway in der ersten DMZ verarbeitet Benutzerverbindungen und führt die Sicherheitsfunktionen eines SSL-VPN aus. Dieses NetScaler Gateway verschlüsselt Benutzerverbindungen, bestimmt, wie die Benutzer authentifiziert werden, und steuert den Zugriff auf die Server im internen Netzwerk.

Das NetScaler Gateway in der zweiten DMZ dient als NetScaler Gateway-Proxygerät. Dieses NetScaler Gateway ermöglicht es dem ICA-Datenverkehr, die zweite DMZ zu durchlaufen, um

Benutzerverbindungen zur Serverfarm herzustellen.

Das NetScaler ADM kann entweder im Subnetz bereitgestellt werden, das zur NetScaler Gateway-Appliance in der ersten DMZ gehört, oder im Subnetz, das zur zweiten DMZ der NetScaler Gateway-Appliance gehört. Im obigen Bild werden NetScaler ADM und NetScaler Gateway in der ersten DMZ im selben Subnetz bereitgestellt.

Im Double-Hop-Modus sammelt NetScaler ADM TCP-Datensätze von einer Appliance und ICA-Einträge von der anderen Appliance. Nachdem Sie die NetScaler Gateway-Appliances zum NetScaler ADM-Inventar hinzugefügt und die Datenerfassung aktiviert haben, exportiert jede der Appliances die Berichte, indem sie die Hop-Anzahl und die Verbindungsketten-ID verfolgt.

Damit NetScaler ADM identifiziert, welche Appliance Datensätze exportiert, wird jede Appliance mit einer Hop-Anzahl angegeben, und jede Verbindung wird mit einer Verbindungsketten-ID angegeben. Die Hop-Anzahl stellt die Anzahl der NetScaler Gateway-Geräte dar, über die der Datenverkehr von einem Client zu den Servern fließt. Die Verbindungsketten-ID stellt die End-to-End-Verbindungen zwischen dem Client und dem Server dar.

NetScaler ADM verwendet die Hop-Anzahl und die Verbindungsketten-ID, um die Daten der NetScaler Gateway-Appliances miteinander zu verknüpfen und die Berichte zu generieren.

Um NetScaler Gateway-Appliances zu überwachen, die in diesem Modus bereitgestellt werden, müssen Sie zuerst das NetScaler Gateway dem NetScaler ADM-Bestand hinzufügen, AppFlow auf NetScaler ADM aktivieren und dann die Berichte auf dem NetScaler ADM Dashboard anzeigen.

Konfigurieren Sie HDX Insight auf virtuellen Servern, die für Optimal Gateway verwendet werden

Schritte zum Konfigurieren von HDX Insight auf virtuellen Servern, die für Optimal Gateway verwendet werden:

1. Navigieren Sie zu **Infrastruktur > Instanzen** und wählen Sie die NetScaler-Instanz aus, für die Sie Analysen aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
3. Wählen Sie den für die Authentifizierung konfigurierten virtuellen VPN-Server aus und klicken Sie auf **Enable Analytics**.
4. Wählen Sie **HDX Insight** und dann **ICA** aus.
5. Wählen Sie je nach Bedarf weitere erweiterte Optionen aus.
6. Klicken Sie auf **OK**.
7. Wiederholen Sie die Schritte 3 bis 6 auf dem anderen virtuellen VPN-Server.

Aktivieren der Datenerfassung auf NetScaler ADM

Wenn Sie NetScaler ADM aktivieren, um die ICA-Details von beiden Appliances zu erfassen, sind die erfassten Details redundant. Das ist, dass beide Appliances die gleichen Metriken melden. Um diese Situation zu umgehen, müssen Sie AppFlow für ICA auf einer der ersten NetScaler Gateway-Appliances 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 NetScaler ADM:

1. Geben Sie in einem Webbrowser die IP-Adresse des NetScaler ADM ein (z. B. http://192.168.100.1).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **Infrastruktur > Instanzen** und wählen Sie die NetScaler-Instanz aus, für die Sie Analysen aktivieren möchten.
4. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
5. Wählen Sie die virtuellen VPN-Server aus, und klicken Sie auf **Analytics aktivieren**.
6. Wählen Sie **HDX Insight** und dann **ICA** oder **TCP** für ICA-Verkehr bzw. TCP-Verkehr aus.

   > **Hinweis**
   >
   > Wenn die AppFlow-Protokollierung für die jeweiligen Dienste oder Dienstgruppen auf der NetScaler Appliance nicht aktiviert ist, zeigt das NetScaler ADM-Dashboard die Datensätze nicht an, auch wenn in der Insight-Spalte Aktiviert angezeigt wird.

7. Klicken Sie auf **OK**.

Konfigurieren von NetScaler Gateway Geräten zum Exportieren von Daten

Nach der Installation der NetScaler Gateway Geräte müssen Sie die folgenden Einstellungen auf den NetScaler Gateway-Geräten konfigurieren, um die Berichte in NetScaler ADM zu exportieren:

- Konfigurieren Sie virtuelle Server der NetScaler Gateway-Geräte in der ersten und zweiten DMZ für die Kommunikation miteinander.
- Binden Sie den virtuellen NetScaler Gateway-Server in der zweiten DMZ an den virtuellen NetScaler Gateway-Server in der ersten DMZ.
- Aktivieren Sie Double Hop auf dem NetScaler Gateway in der zweiten DMZ.
- Deaktivieren Sie die Authentifizierung auf dem virtuellen NetScaler Gateway-Server in der zweiten DMZ.

- Aktivieren Sie eines der NetScaler Gateway-Appliances, um ICA-Datensätze zu exportieren
- Aktivieren Sie das andere NetScaler Gateway-Gerät, um TCP-Datensätze zu exportieren:
- Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway-Appliances.

NetScaler Gateway über die Befehlszeilenschnittstelle konfigurieren:

1. Konfigurieren Sie den virtuellen NetScaler Gateway-Server in der ersten DMZ für die Kommunikation mit dem virtuellen NetScaler Gateway-Server in der zweiten DMZ.

```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (
    ON or OFF)] [-imgGifToPng]

add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
```

2. Binden Sie den virtuellen NetScaler Gateway-Server in der zweiten DMZ an den virtuellen NetScaler Gateway-Server in der ersten DMZ. Führen Sie den folgenden Befehl auf dem NetScaler Gateway in der ersten DMZ aus:

```
bind vpn vserver <name> -nextHopServer <name>

bind vpn vserver vs1 -nextHopServer nh1
```

3. Aktivieren Sie Double Hop und AppFlow auf dem NetScaler Gateway in der zweiten DMZ.

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [-
     appflowLog ( ENABLED or DISABLED )]

set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
```

4. Deaktivieren Sie die Authentifizierung auf dem virtuellen NetScaler Gateway-Server in der zweiten DMZ.

```
set vpn vserver <name> [-authentication (ON or OFF)]

set vpn vserver vs -authentication OFF
```

5. Aktivieren Sie eine der NetScaler 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
```

6. Aktivieren Sie die andere NetScaler Gateway-Appliance zum Exportieren von ICA-Datensätzen:

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

```



```
3 bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
     ICA_REQUEST
```

7. Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway-Appliances:

```
1 set appFlow param [-connectionChaining (ENABLED or DISABLED)]
2
3 set appflow param -connectionChaining ENABLED
```

NetScaler Gateway über das Konfigurationsdienstprogramm konfigurieren:

1. Konfigurieren Sie das NetScaler Gateway in der ersten DMZ für die Kommunikation mit dem NetScaler Gateway in der zweiten DMZ und binden Sie das NetScaler Gateway in der zweiten DMZ an das NetScaler Gateway in der ersten DMZ.

   a) Erweitern Sie auf der Registerkarte **Konfiguration NetScaler 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 Next-Hop-Server an das zweite NetScaler Gateway-Gerät.

2. Aktivieren Sie Double Hop auf dem NetScaler Gateway in der zweiten DMZ.

   a) Erweitern Sie auf der Registerkarte **KonfigurationNetScaler 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 More, wählen Sie **Double Hop** und klicken Sie auf **OK**.

3. Deaktivieren Sie die Authentifizierung auf dem virtuellen Server auf dem NetScaler Gateway in der zweiten DMZ.

   a) Erweitern Sie auf der Registerkarte **Konfiguration NetScaler 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 NetScaler Gateway-Appliances zum Exportieren von TCP-Datensätzen.

   a) Erweitern Sie auf der Registerkarte **Konfiguration NetScaler 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 Choose Type** die Option**Other TCP-Request**aus.

d) Klicken Sie auf **Weiter**.

e) Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Schließen**.

5. Aktivieren Sie die andere NetScaler Gateway-Appliance zum Exportieren von ICA-Datensätzen:

a) Erweitern Sie auf der Registerkarte **Konfiguration NetScaler 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 **Richtlinie auswählen** 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 NetScaler Gateway-Appliances.

a) Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **Appflow**.

b) Doppelklicken Sie im rechten Bereich in der Gruppe **Einstellungen** auf **Change Appflow Settings**.

c) Wählen Sie **Verbindungsverkettung** aus, und klicken Sie auf **OK**.

7. Konfigurieren Sie das NetScaler Gateway in der ersten DMZ für die Kommunikation mit dem NetScaler Gateway in der zweiten DMZ und binden Sie das NetScaler Gateway in der zweiten DMZ an das NetScaler Gateway in der ersten DMZ.

a) Erweitern Sie auf der Registerkarte Konfiguration **NetScaler 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**Veröffentlichte Anwendungen**.

c) Klicken Sie auf**Next Hop Server** und binden Sie einen Next-Hop-Server an das zweite NetScaler Gateway-Gerät.

8. Aktivieren Sie Double Hop auf dem NetScaler Gateway in der zweiten DMZ.
    a) Erweitern Sie auf der Registerkarte Konfiguration **NetScaler 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 More, wählen Sie **Double Hop** aus und klicken Sie auf **OK**.
9. Deaktivieren Sie die Authentifizierung auf dem virtuellen Server auf dem NetScaler Gateway in der zweiten DMZ.
    a) Erweitern Sie auf der Registerkarte Konfiguration NetScaler 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**.
10. Aktivieren Sie eine der NetScaler Gateway-Appliances zum Exportieren von TCP-Datensätzen.
    a) Erweitern Sie auf der Registerkarte Konfiguration **NetScaler 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 Choose Type** die Option**Other TCP-Request**aus.
    d) Klicken Sie auf **Weiter**.
    e) Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Schließen**.
11. Aktivieren Sie die andere NetScaler Gateway-Appliance, um ICA-Datensätze zu exportieren.
    a) Erweitern Sie auf der Registerkarte Konfiguration **NetScaler 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 Choose Type**die Option**Other TCP-Request**aus.
    d) Klicken Sie auf **Weiter**.
    e) Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Schließen**.
12. Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway-Appliances.

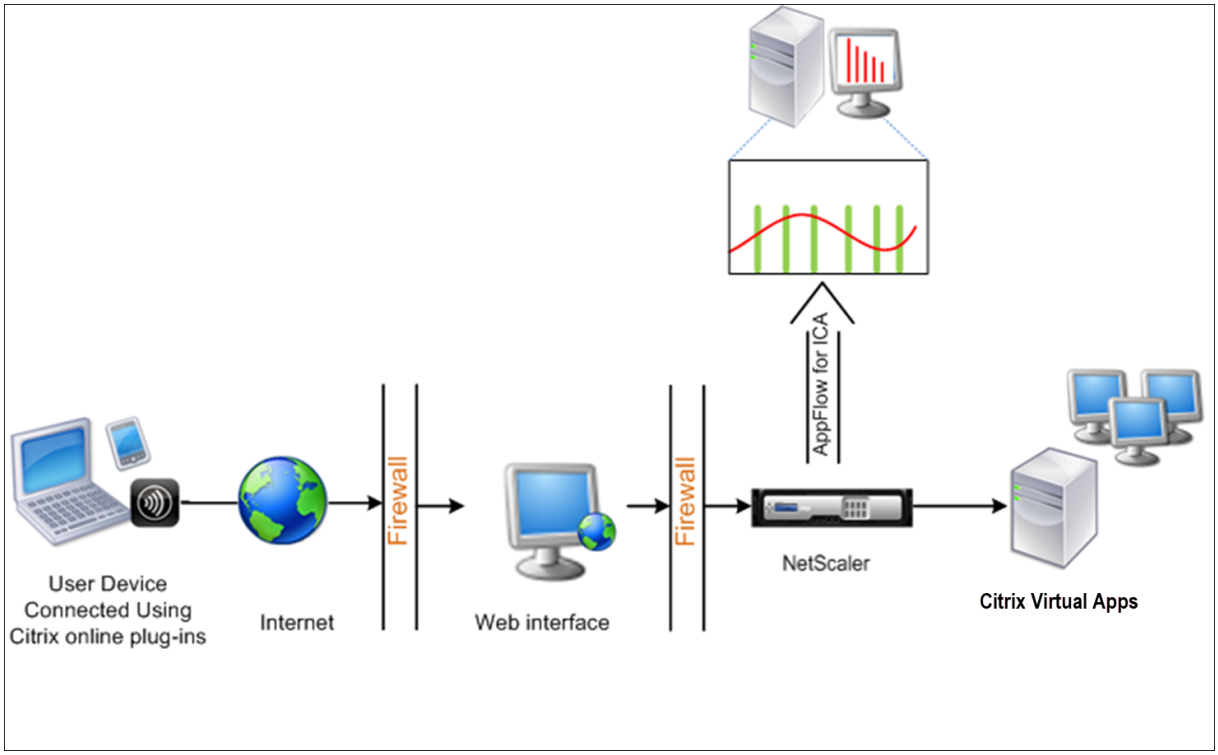
Aktivieren Sie die Datenerfassung für die Überwachung von NetScalern, die im transparenten Modus eingesetzt werden

Wenn ein NetScaler im transparenten Modus bereitgestellt wird, können die Clients direkt auf die Server zugreifen, ohne dass ein virtueller Server vorhanden ist. Wenn eine NetScaler Appliance im transparenten Modus in einer Citrix Virtual Apps and Desktop-Umgebung bereitgestellt wird, wird der ICA-Verkehr nicht über ein VPN übertragen.

Nachdem Sie NetScaler zur NetScaler ADM Bestandsliste hinzugefügt haben, müssen Sie AppFlow für die Datensammlung aktivieren. Die Aktivierung der Datenerfassung hängt vom Gerät und vom Modus ab. In diesem Fall müssen Sie NetScaler ADM als AppFlow-Collector auf jeder NetScaler 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 NetScaler, der im transparenten Modus bereitgestellt wird, nicht mithilfe des NetScaler ADM Konfigurationsdienstprogramms aktivieren.
> - Detaillierte Informationen zu den Befehlen und ihrer Verwendung finden Sie in der Befehlsreferenz .
> - Informationen zu Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke .

Die folgende Abbildung zeigt die Netzwerkbereitstellung eines NetScaler ADM, wenn ein NetScaler im transparenten Modus bereitgestellt wird:



So konfigurieren Sie die Datenerfassung auf einer NetScaler Appliance mithilfe der Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Melden Sie sich bei einer Appliance an.
2. Geben Sie die ICA-Ports an, an denen die NetScaler Appliance auf Datenverkehr wartet.

```
set ns param --icaPorts <port>...
```

Beispiel:

```
set ns param -icaPorts 2598 1494
```

> **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 NetScaler Appliance hinzu.

```
add appflow collector <name> -IPAddress <ip_addr>
```

Beispiel:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

> **Hinweis** Um die auf der NetScaler 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> ...
```

Beispiel:

add AppFlow action act-collectors MyInsight

5. Erstellen Sie eine AppFlow Richtlinie, um die Regel zum Generieren des Datenverkehrs anzugeben.

```
add appflow policy <policyname> <rule> <action>
```

Beispiel:

```
add appflow policy pol true act
```

6. Binden Sie die AppFlow-Richtlinie an einen globalen Bindepunkt.

```
bind appflow global <policyname> <priority> -type <type>
```


Beispiel:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> **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
```

Beispiel:

```
set appflow param -flowRecordInterval 60
```

8. Speichern Sie die Konfiguration. Typ: `save ns config`

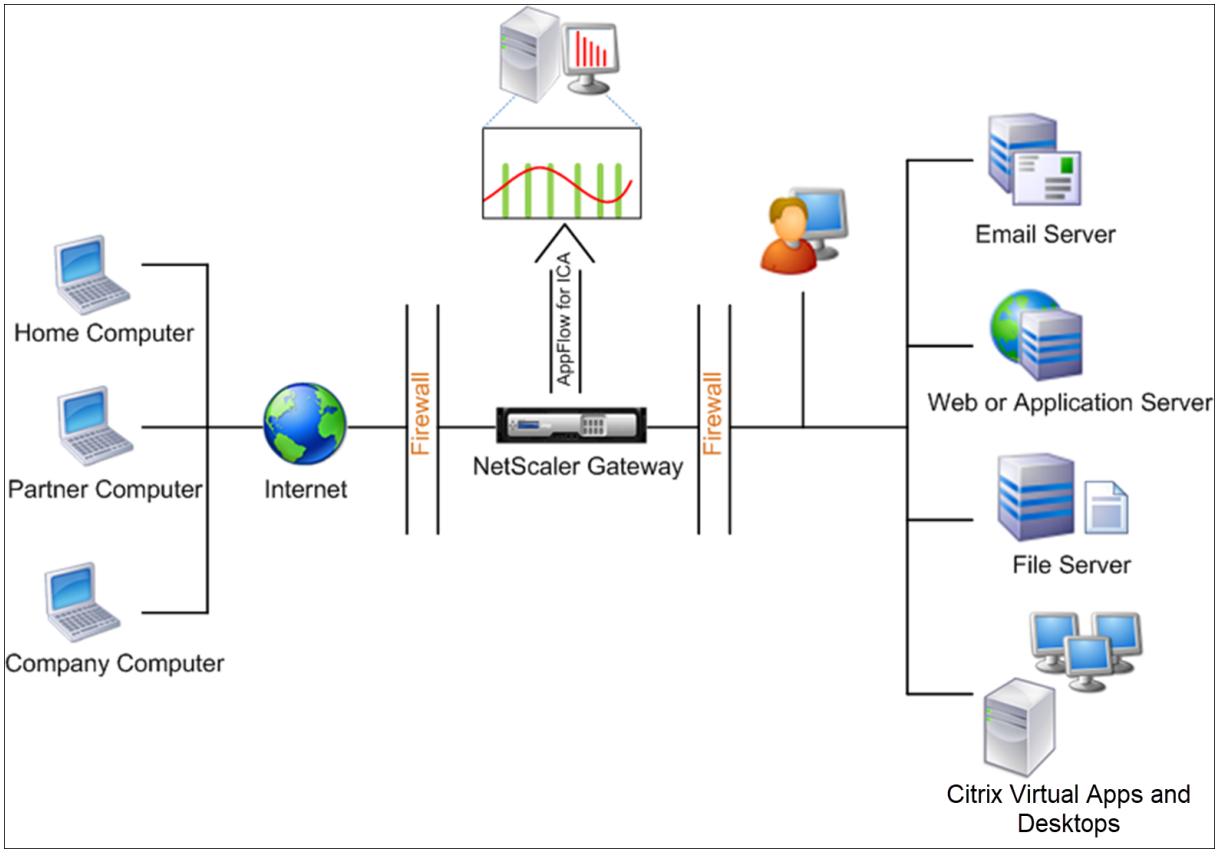
‘‘

Datenerfassung für NetScaler Gateway-Geräte im Single-Hop-Modus aktivieren

February 5, 2024

Wenn Sie NetScaler Gateway im Single-Hop-Modus bereitstellen, befindet es sich am Netzwerkrand. Die Gateway-Instanz stellt ICA-Proxy-Verbindungen zur Desktop-Bereitstellungsinfrastruktur bereit. Single-Hop ist das einfachste und gebräuchlichste Deployment. Der Single-Hop-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 NetScaler-Appliances zu.

Um mit der Erfassung der Berichte zu beginnen, müssen Sie die NetScaler Gateway-Appliance zum NetScaler ADM-Inventar (Application Delivery Management) hinzufügen und AppFlow auf ADM aktivieren.



So aktivieren Sie die AppFlow Funktion von ADM:

1. Navigieren Sie zu **Infrastruktur** > **Instanzen** und wählen Sie die NetScaler-Instanz aus, für 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 in das Feld **Enable AppFlow** den Wert **true**ein und wählen Sie **ICA**aus.
5. Klicken Sie auf **OK**.

> **Hinweis**
>
> Wenn Sie AppFlow im Single-Hop-Modus aktivieren, werden die folgenden Befehle im Hintergrund ausgeführt. 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
```

Virtuelle EUEM-Kanaldaten sind Teil von HDX Insight Daten, die NetScaler ADM von Gateway-Instanzen erhält. Der virtuelle EUEM-Kanal stellt die Daten über ICA-RTT bereit. Wenn der virtuelle EUEM-Kanal nicht aktiviert ist, werden die verbleibenden HDX Insight Daten weiterhin in NetScaler ADM angezeigt.

Datenerfassung zur Überwachung von NetScalern aktivieren, die im transparenten Modus eingesetzt werden

February 5, 2024

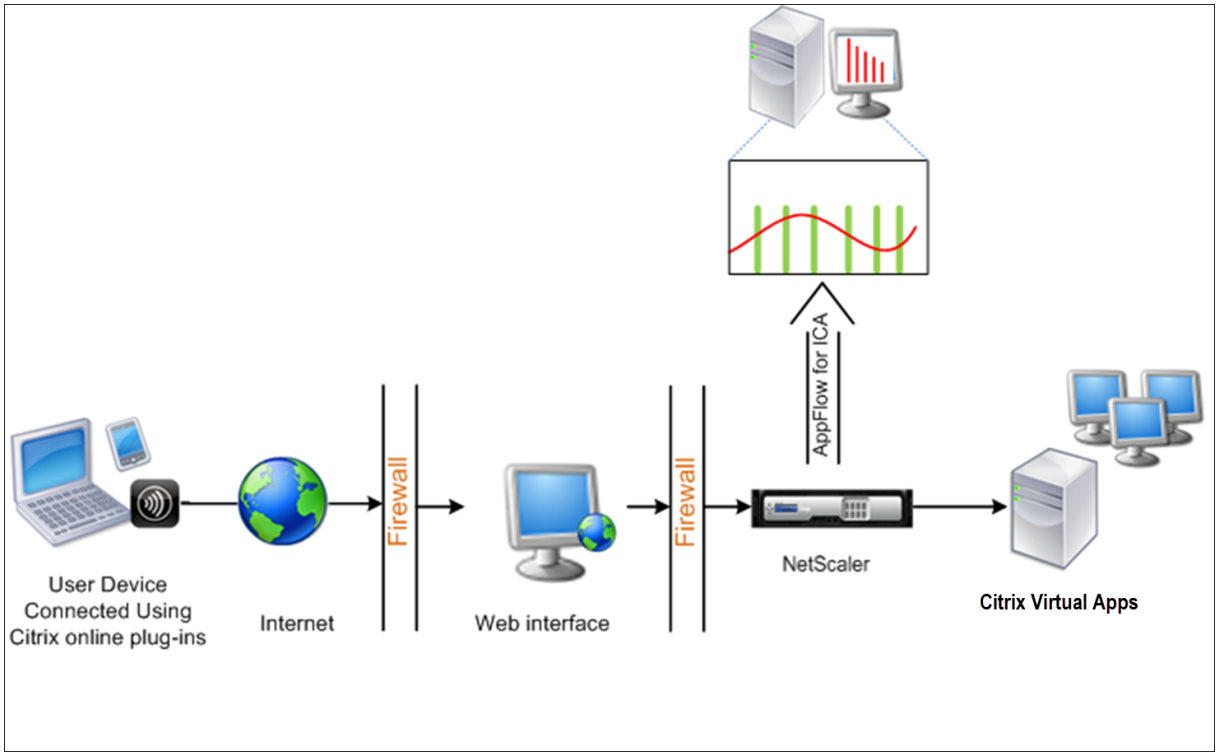
Wenn ein NetScaler im transparenten Modus bereitgestellt wird, können die Clients direkt auf die Server zugreifen, ohne dass ein virtueller Server vorhanden ist. Wenn ein NetScaler im transparenten Modus in einer Citrix Virtual Apps and Desktops-Umgebung bereitgestellt wird, wird der ICA-Verkehr nicht über ein VPN übertragen.

Nachdem Sie NetScaler zur NetScaler ADM Bestandsliste hinzugefügt haben, müssen Sie AppFlow für die Datensammlung aktivieren. Die Aktivierung der Datenerfassung hängt vom Gerät und vom Modus ab. In diesem Fall müssen Sie NetScaler ADM als AppFlow-Collector auf jeder NetScaler-Instanz hinzufügen und eine AppFlow-Richtlinie konfigurieren, um den gesamten oder bestimmten ICA-Verkehr zu erfassen, der durch die Appliance fließt.

Hinweis

- Sie können die Datenerfassung auf einem NetScaler, der im transparenten Modus bereitgestellt wird, nicht mithilfe des NetScaler ADM Konfigurationsdienstprogramms aktivieren.
- Detaillierte Informationen zu den Befehlen und ihrer Verwendung finden Sie in der Befehlsreferenz .
- Informationen zu Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke .

Die folgende Abbildung zeigt die Netzwerkbereitstellung eines NetScaler ADM, wenn ein NetScaler im transparenten Modus bereitgestellt wird:



So konfigurieren Sie die Datenerfassung auf einer NetScaler Appliance mithilfe der Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Melden Sie sich bei einer Appliance an.
2. Geben Sie die ICA-Ports an, an denen die NetScaler 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 NetScaler-Instanz hinzu.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Beispiel:


```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> **Hinweis** Um die AppFlow-Collector anzuzeigen, die für die NetScaler-Instanz konfiguriert sind, 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 Bindepunkt.

```
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.

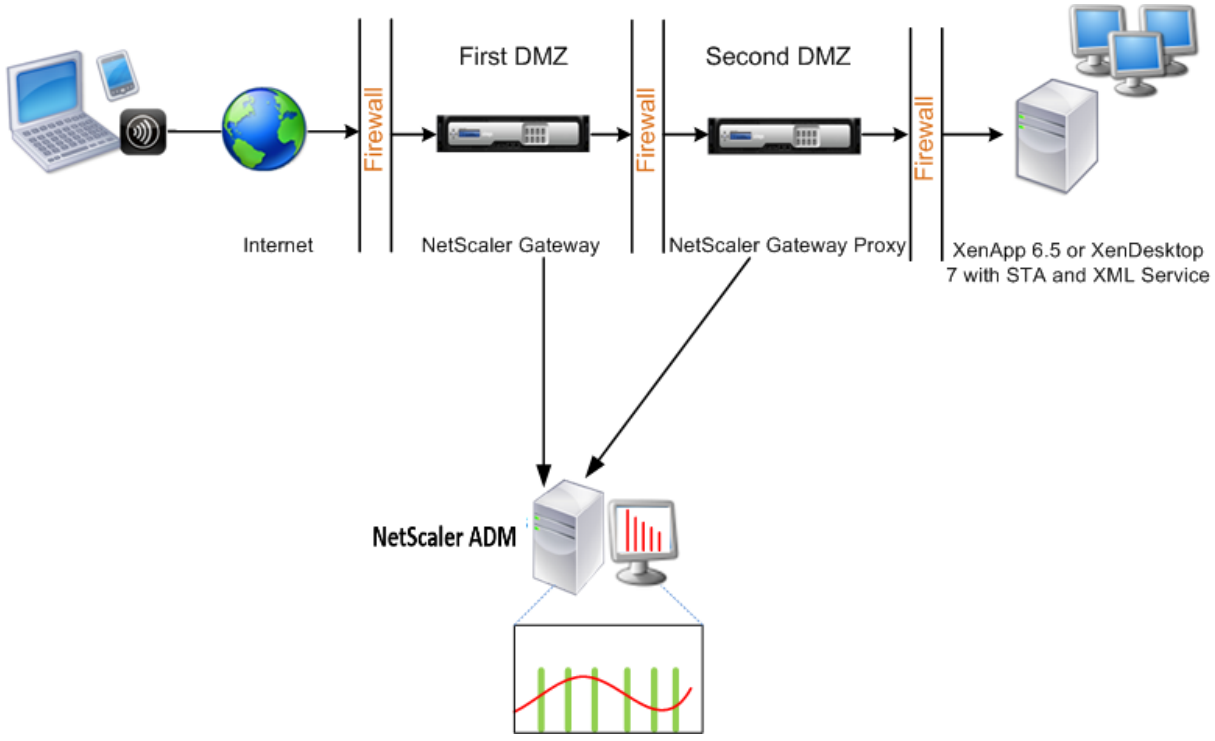

```
save ns config
<!--NeedCopy-->
```

Datenerfassung für NetScaler Gateway-Appliances im Double-Hop-Modus aktivieren

February 5, 2024

Der Doppel-Hop-Modus von NetScaler Gateway bietet zusätzlichen Schutz für das interne Netzwerk einer Organisation, da ein Angreifer mehrere Sicherheitszonen oder entmilitarisierte Zonen (DMZ) durchdringen muss, um die Server im sicheren Netzwerk zu erreichen. Wenn Sie die Anzahl der Hops (NetScaler Gateway Geräte) analysieren möchten, über die die ICA-Verbindungen weitergeleitet werden, sowie die Details zur Latenz für jede TCP-Verbindung und wie sie mit der gesamten ICA-Latenz verglichen wird, die vom Client wahrgenommen wird, müssen Sie NetScaler ADM installieren, damit die NetScaler Gateway-Geräte diese wichtigen Statistiken zu berichten.

Abbildung 3. NetScaler ADM im Double-Hop-Modus bereitgestellt



Das NetScaler Gateway in der ersten DMZ verarbeitet Benutzerverbindungen und führt die Sicherheitsfunktionen eines SSL-VPN aus. Dieses NetScaler Gateway verschlüsselt Benutzerverbindungen, bestimmt, wie die Benutzer authentifiziert werden, und steuert den Zugriff auf die Server im internen

Netzwerk.

Das NetScaler Gateway in der zweiten DMZ dient als NetScaler Gateway-Proxygerät. Dieses NetScaler Gateway ermöglicht es dem ICA-Datenverkehr, die zweite DMZ zu durchlaufen, um Benutzerverbindungen zur Serverfarm herzustellen.

Das NetScaler ADM kann entweder im Subnetz bereitgestellt werden, das zur NetScaler Gateway-Appliance in der ersten DMZ gehört, oder im Subnetz, das zur zweiten DMZ der NetScaler Gateway-Appliance gehört. Im obigen Bild werden NetScaler ADM und NetScaler Gateway in der ersten DMZ im selben Subnetz bereitgestellt.

Im Double-Hop-Modus sammelt NetScaler ADM TCP-Datensätze von einer Appliance und ICA-Einträge von der anderen Appliance. Nachdem Sie die NetScaler Gateway-Appliances zum NetScaler ADM-Bestand hinzugefügt und die Datenerfassung aktiviert haben, exportiert jede Appliance die Berichte, indem sie die Hop-Anzahl und die Verbindungsketten-ID verfolgt.

Damit NetScaler ADM identifiziert, welche Appliance Datensätze exportiert, wird jede Appliance mit einer Hop-Anzahl angegeben, und jede Verbindung wird mit einer Verbindungsketten-ID angegeben. Die Hop-Anzahl stellt die Anzahl der NetScaler Gateway-Geräte dar, über die der Datenverkehr von einem Client zu den Servern fließt. Die Verbindungsketten-ID stellt die End-to-End-Verbindungen zwischen dem Client und dem Server dar.

NetScaler ADM verwendet die Hop-Anzahl und die Verbindungsketten-ID, um die Daten der NetScaler Gateway-Appliances miteinander zu verknüpfen und die Berichte zu generieren.

Um NetScaler Gateway-Appliances zu überwachen, die in diesem Modus bereitgestellt werden, müssen Sie zuerst das NetScaler Gateway dem NetScaler ADM-Bestand hinzufügen, AppFlow auf NetScaler ADM aktivieren und dann die Berichte auf dem NetScaler ADM Dashboard anzeigen.

Aktivieren der Datenerfassung auf NetScaler ADM

Wenn Sie NetScaler ADM aktivieren, um die ICA-Details von beiden Appliances zu erfassen, sind die erfassten Details redundant. Das ist, dass beide Appliances die gleichen Metriken melden. Um diese Situation zu umgehen, müssen Sie AppFlow für TCP auf einem der ersten NetScaler Gateway-Appliances und dann AppFlow für ICA auf dem zweiten Gerät 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 NetScaler ADM:

1. Navigieren Sie zu **Infrastruktur > Instanzen** und wählen Sie die NetScaler-Instanz aus, für 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 Enable AppFlow** den **Wert true** ein, und wählen Sie **ICA/TCP** für ICA-Verkehr einen TCP-Verkehr aus.

   > **Hinweis**
   >
   > Wenn die AppFlow-Protokollierung für die Dienste oder Dienstgruppen auf der NetScaler Appliance nicht aktiviert ist, zeigt das NetScaler ADM Dashboard die Datensätze nicht an, selbst wenn in der Spalte Insight Aktiviert angezeigt wird.

5. Klicken Sie auf **OK**.

Konfigurieren von NetScaler Gateway-Geräten zum Exportieren von Daten

Nach der Installation der NetScaler Gateway Geräte müssen Sie die folgenden Einstellungen auf den NetScaler Gateway-Geräten konfigurieren, um die Berichte in NetScaler ADM zu exportieren:

- Konfigurieren Sie virtuelle Server der NetScaler Gateway-Geräte in der ersten und zweiten DMZ für die Kommunikation miteinander.
- Binden Sie den virtuellen NetScaler Gateway-Server in der zweiten DMZ an den virtuellen NetScaler Gateway-Server in der ersten DMZ.
- Aktivieren Sie Double Hop auf dem NetScaler Gateway in der zweiten DMZ.
- Deaktivieren Sie die Authentifizierung auf dem virtuellen NetScaler Gateway-Server in der zweiten DMZ.
- Aktivieren Sie eines der NetScaler Gateway-Appliances, um ICA-Datensätze zu exportieren
- Aktivieren Sie das andere NetScaler Gateway-Gerät, um TCP-Datensätze zu exportieren:
- Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway-Appliances.

Konfigurieren Sie NetScaler Gateway mit der Befehlszeilenschnittstelle:

1. Konfigurieren Sie den virtuellen NetScaler Gateway-Server in der ersten DMZ für die Kommunikation mit dem virtuellen NetScaler Gateway-Server in der zweiten DMZ.

---

add vpn nextHopServer [**-secure**(ON OFF)] [**-imgGifToPng**] …

```
1 add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
2 <!--NeedCopy-->
```

2. Binden Sie den virtuellen NetScaler Gateway-Server in der zweiten DMZ an den virtuellen NetScaler Gateway-Server in der ersten DMZ. Führen Sie den folgenden Befehl auf dem NetScaler Gateway in der ersten DMZ aus:

   bind vpn vserver <name> **-nextHopServer** <name>


```
1 bind vpn vserver vs1 -nextHopServer nh1
2 <!--NeedCopy-->
```

3. Aktivieren Sie Double Hop und AppFlow auf dem NetScaler Gateway in der zweiten DMZ.

set vpn vserver [**- doubleHop** (ENABLED DISABLED)] [**- appflowLog** (ENABLED DISABLED)]

```
1 set vpn vserver vpnhop2 -doubleHop ENABLED -appFlowLog ENABLED
2 <!--NeedCopy-->
```

4. Deaktivieren Sie die Authentifizierung auf dem virtuellen NetScaler Gateway-Server in der zweiten DMZ.

set vpn vserver [**-authentication** (ON OFF)]

```
1 set vpn vserver vs -authentication OFF
2 <!--NeedCopy-->
```

5. Aktivieren Sie eine der NetScaler Gateway-Appliances zum Exportieren von TCP-Datensätzen.

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
1 bind vpn vserver vpn1 -policy appflowpol1 -priority 101 -type
     OTHERTCP_REQUEST
2 <!--NeedCopy-->
```

6. Aktivieren Sie die andere NetScaler Gateway-Appliance zum Exportieren von ICA-Datensätzen:

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
1 bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
     ICA_REQUEST
2 <!--NeedCopy-->
```

7. Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway-Appliances:

set appFlow param [**-connectionChaining** (ENABLED DISABLED)]

```
1 set appflow param -connectionChaining ENABLED
2 <!--NeedCopy-->
```


Konfigurieren von NetScaler Gateway mit dem Konfigurationsdienstprogramm:

1. Konfigurieren Sie das NetScaler Gateway in der ersten DMZ für die Kommunikation mit dem NetScaler Gateway in der zweiten DMZ und binden Sie das NetScaler Gateway in der zweiten DMZ an das NetScaler Gateway in der ersten DMZ.

    a) Erweitern Sie auf der Registerkarte **Konfiguration NetScaler 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 Next-Hop-Server an das zweite NetScaler Gateway-Gerät.

2. Aktivieren Sie Double Hop auf dem NetScaler Gateway in der zweiten DMZ.

    a) Erweitern Sie auf der Registerkarte **KonfigurationNetScaler 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 **More**, wählen Sie **Double Hop**, und klicken Sie auf**OK**.

3. Deaktivieren Sie die Authentifizierung auf dem virtuellen Server auf dem NetScaler Gateway in der zweiten DMZ.

    a) Erweitern Sie auf der Registerkarte **Konfiguration NetScaler 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 NetScaler Gateway-Appliances zum Exportieren von TCP-Datensätzen.

    a) Erweitern Sie auf der Registerkarte **Konfiguration NetScaler 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 Dropdownliste 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 NetScaler Gateway-Appliance zum Exportieren von ICA-Datensätzen:

   a) Erweitern Sie auf der Registerkarte **Konfiguration NetScaler 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 Dropdownliste **Richtlinie auswählen** die Option **AppFlow** aus, und wählen Sie in der Dropdownliste "Typ wählen"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 NetScaler Gateway-Appliances.

   a) Navigieren Sie auf der Registerkarte**Konfiguration**zu**Einstellungen > 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**.

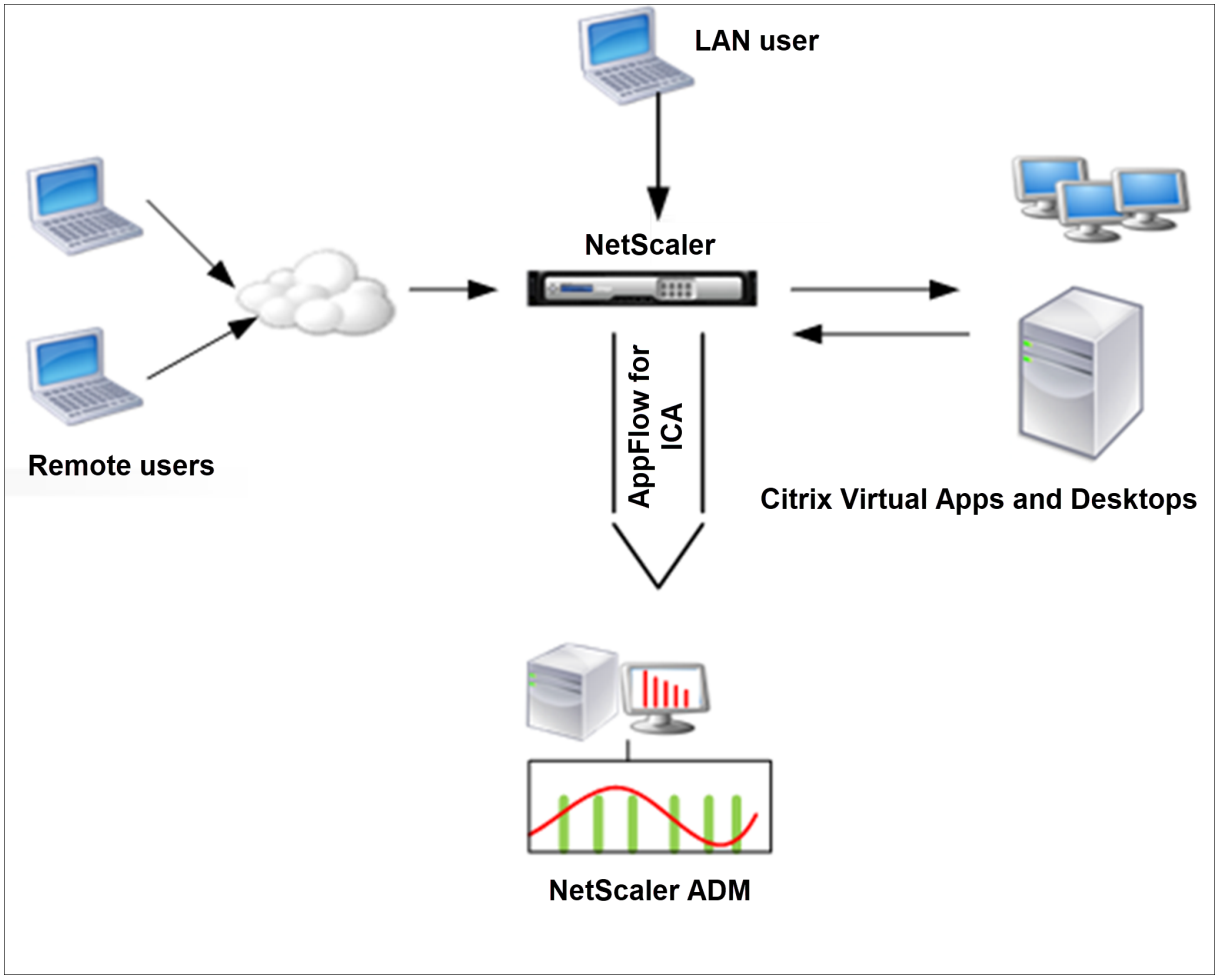
Datenerfassung zur Überwachung von NetScalern aktivieren, die im LAN-Benutzermodus eingesetzt werden

February 5, 2024

Externe Benutzer, die auf Citrix Virtual App- oder Desktop-Anwendungen zugreifen, müssen sich am NetScaler Gateway authentifizieren. Interne Benutzer müssen jedoch möglicherweise nicht an NetScaler Gateway weitergeleitet werden. Außerdem muss der Administrator in einer Bereitstellung im transparenten Modus die Routingrichtlinien manuell anwenden, damit die Anforderungen an die NetScaler Appliance umgeleitet werden.

Um diese Herausforderungen zu meistern und LAN-Benutzer direkt mit Citrix Virtual Apps and Desktops s-Anwendungen zu verbinden, können Sie das NetScaler Gerät im LAN-Benutzermodus bereitstellen, indem Sie einen virtuellen Cacheumleitungsserver konfigurieren, der als SOCKS-Proxy auf dem NetScaler Gateway Gerät fungiert.

Figure 4. NetScaler ADM im LAN-Benutzermodus bereitgestellt



Hinweis: NetScaler ADM und NetScaler Gateway Gerät befinden sich im selben Subnetz.

Um in diesem Modus bereitgestellte NetScaler Appliances zu überwachen, fügen Sie zuerst die NetScaler Appliance zur NetScaler Insight-Bestandsliste hinzu, aktivieren Sie AppFlow und zeigen Sie dann die Berichte im Dashboard an.

Nachdem Sie die NetScaler Appliance zur NetScaler ADM Bestandsliste hinzugefügt haben, müssen Sie AppFlow für die Datenerfassung aktivieren.

> **Hinweis**
>
> - Sie können die Datenerfassung auf einem NetScaler, der im LAN-Benutzermodus bereitgestellt wird, nicht mithilfe des NetScaler ADM Konfigurationsdienstprogramms aktivieren.
> - Detaillierte Informationen zu den Befehlen und ihrer Verwendung finden Sie in der Befehlsreferenz .
> - Informationen zu Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke .

So konfigurieren Sie die Datenerfassung auf einer NetScaler Appliance mithilfe der Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Melden Sie sich bei einer 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 NetScaler Gateway -Gerät auf das LAN-Netzwerk zugreifen, fügen Sie eine Aktion hinzu, die von einer Richtlinie angewendet wird, 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 NetScaler ADM als AppFlow Collector auf der NetScaler 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 Bindepunkt.

```
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-->
```


Schwellenwerte erstellen und Warnungen für HDX Insight konfigurieren

February 5, 2024

Mit HDX Insight auf NetScaler Application Delivery Management (ADM) können Sie den HDX-Verkehr überwachen, der durch NetScaler-Instances fließt. Mit NetScaler ADM können Sie Schwellenwerte für verschiedene Leistungsindikatoren festlegen, die zur Überwachung des Insight-Datenverkehrs verwendet werden. Sie können auch Regeln konfigurieren und Warnungen in NetScaler ADM erstellen.

Der HDX-Datenverkehrstyp ist mit verschiedenen Entitäten wie Anwendungen, Desktops, Gateways, Lizenzen und Benutzern verknüpft. Jede Entität kann verschiedene Metriken enthalten, die ihnen zugeordnet sind. Beispielsweise ist die Anwendungseinheit mit verschiedenen Treffern, der von der Anwendung verbrauchten Bandbreite und der Reaktionszeit des Servers verknüpft. Eine Benutzerentität kann WAN-Latenz, DC-Latenz, ICA RTT und Bandbreite zugeordnet werden, die von einem Benutzer belegt wird.

Die Schwellenwertverwaltung für HDX Insight in NetScaler ADM ermöglichte es Ihnen, proaktiv Regeln zu erstellen und Warnungen zu konfigurieren, wenn die festgelegten Schwellenwerte überschritten werden. Diese Schwellenwertverwaltung wurde nun erweitert, um eine Gruppe von Schwellenwertregeln zu konfigurieren. Sie können jetzt die Gruppe anstelle einzelner Regeln überwachen. Eine Schwellenwertregelgruppe umfasst eine oder mehrere benutzerdefinierte 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. Im Falle einer Benutzerentität kann die Schwellengruppe auch mit einer Geolocation verknüpft werden.

Eine Warnung wird nur dann auf NetScaler ADM generiert, wenn alle Regeln in der konfigurierten Schwellenwertgruppe verletzt werden. Beispielsweise können Sie eine Anwendung anhand der Gesamtzahl der Sitzungsstarts und auch der Anzahl der 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 z. B. Anwendungsentität auswählen und dann Gesamte Sitzungsstartanzahl oder App-Startanzahl auswählen. Sie können für

jede Kombination aus einer Entität und einer Metrik eine Regel erstellen. Verwenden Sie die bereitgestellten Komparatoren (>, <, >= und <=) und geben Sie einen Schwellenwert für jede Metrik ein.

> **Hinweis**
>
> Wenn Sie nicht mehrere Entitäten in einer einzelnen Gruppe überwachen möchten, müssen Sie für jede Entität eine separate Schwellenwertregelgruppe erstellen.

Wenn der Wert eines Zählers den Wert eines Schwellenwerts überschreitet, generiert NetScaler ADM ein Ereignis, das auf eine Schwellenwertverletzung hinweist, und für jedes Ereignis wird eine Warnung erstellt.

Sie müssen konfigurieren, wie Sie die Warnung erhalten. Sie können die Anzeige der Warnung auf NetScaler ADM aktivieren und/oder die Warnung als E-Mail oder als SMS auf Ihrem Mobilgerät empfangen. Für die letzten beiden Aktionen müssen Sie den E-Mail-Server oder den SMS-Server auf NetScaler ADM konfigurieren.

Schwellenwertgruppen können auch an Geolocations gebunden werden, um die geospezifische Überwachung der Benutzerentität zu ermöglichen.

Beispiele für Anwendungsfälle

ABC Inc. ist ein globales Unternehmen und hat 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 über NetScaler Gateway und Citrix GSLB-basierte Umleitung auf 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 User-Experience-Metriken wie ICA-RTTs und Latenzen überprüfen und etwaige Abweichungen proaktiv erhöhen.

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 der ICA-RTT für einen Standort in der Nähe des Rechenzentrums 5 - 10 ms betragen, während der ICA-RTT für einen Remote-Standort 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 bei Verstößen pro Gebiet gewarnt werden. Eric ist auch in der Lage, die Verfolgung mehrerer Metriken innerhalb einer Schwellenwertregelgruppe zu kombinieren und die Grundursache auf Kapazitätsprobleme einzugrenzen, falls vorhanden. Eric ist jetzt in der Lage, jede Abweichung proaktiv zu verfolgen, ohne

sich Gedanken über die Komplexität machen zu müssen, die mit der manuellen Überprüfung aller Portfoliokennzahlen von Citrix Virtual Apps and Desktops verbunden ist.

So erstellen Sie eine Schwellenwertregelgruppe und konfigurieren Warnungen für HDX Insight mit NetScaler ADM:

1. Navigieren Sie in NetScaler ADM zu **Einstellungen > 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:

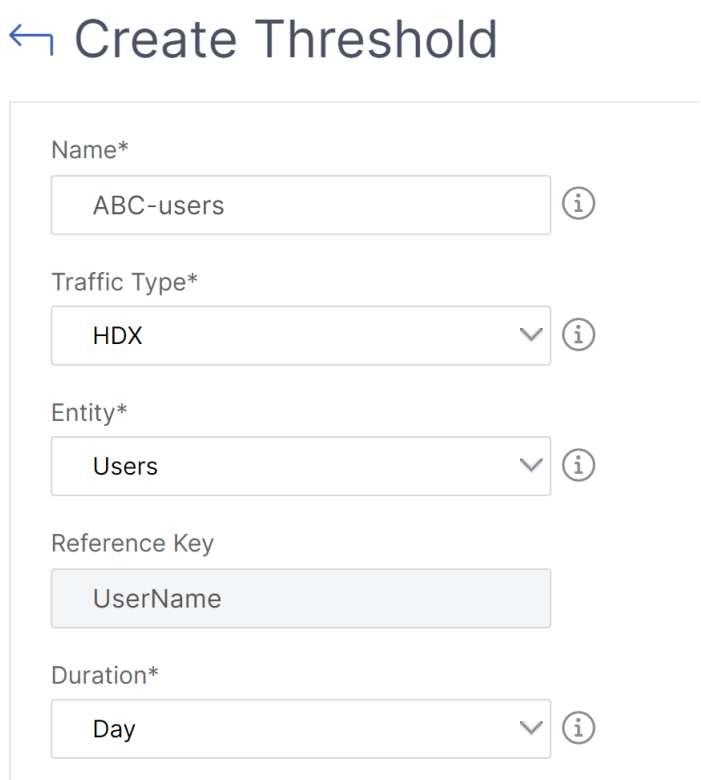
    a) **Name**. Geben Sie einen Namen zum Erstellen eines Ereignisses ein, für das NetScaler ADM eine Warnung generiert.

    b) **Art des Datenverkehrs**. Wählen Sie im Listenfeld HDX aus.

    c) **Entität**. Wählen Sie im Listenfeld die Kategorie oder den Ressourcentyp aus. Die Entitäten unterscheiden sich für jeden Datenverkehrstyp, den Sie zuvor ausgewählt haben.

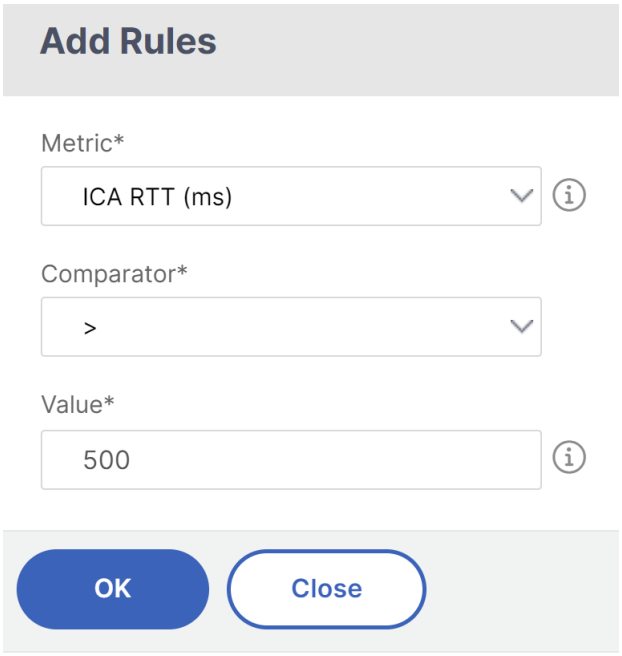
    d) **Referenz-Schlüssel**. Basierend auf dem Traffic-Typ und der Entität, die Sie ausgewählt haben, wird automatisch ein Referenzschlüssel generiert.

    e) **Dauer**. Wählen Sie im Listenfeld 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.

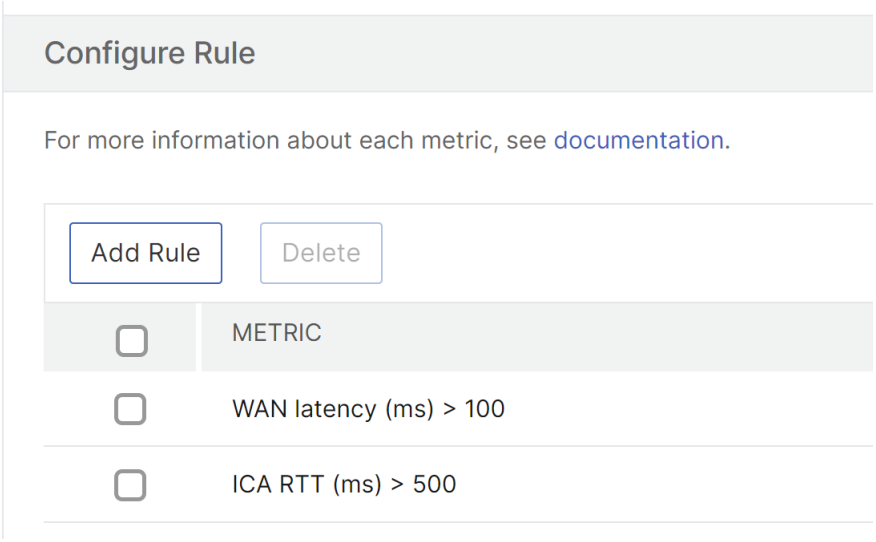


3. Erstellen von Schwellenwertregelgruppen für alle Entitäten:

   Für HDX-Verkehr müssen Sie eine Regel erstellen, indem Sie auf **Regel hinzufügen klicken.**Geben Sie die Werte in das Popup-Fenster **Regeln hinzufügen** ein, das geöffnet wird.

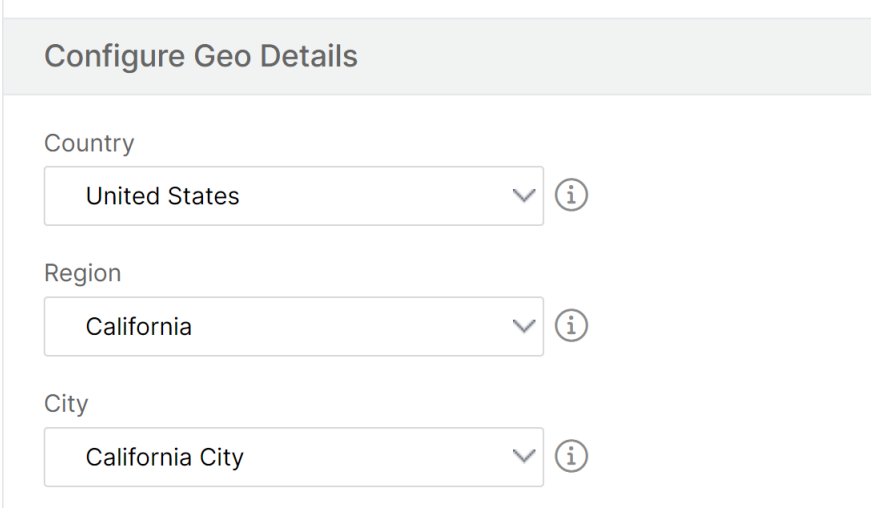


   Sie können mehrere Regeln erstellen, um jede Entität zu überwachen. Wenn Sie mehrere Regeln in einer einzigen Gruppe erstellen, können Sie die Entitäten als Gruppe von Schwellenwertregeln anstelle einzelner Regeln überwachen. Klicken Sie auf **OK**, um das Fenster zu schließen.



4. Konfigurieren von Geolocation-Tagging für Benutzerentität

Optional können Sie im Abschnitt **Geo-Details konfigurieren** eine standortbasierte Warnung für die Benutzerentität 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 NetScaler ADM mit der Überwachung der Entitäten beginnen kann.
6. Konfigurieren Sie optional Aktionen wie E-Mail-Benachrichtigungen und SMS-Benachrichtigungen.
7. Klicken Sie auf **Erstellen**, um eine Schwellenregelgruppe zu erstellen.

Anzeigen von HDX Insight-Berichten und -Metriken

February 5, 2024

HDX Insight bietet vollständige Transparenz der Berichte und Metriken im Zusammenhang mit HDX-Datenverkehr auf Ihren NetScaler-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 App oder den Desktop zugreifen.
- **Anwendungen:**Zeigt die Berichte für die Gesamtzahl der Anwendungen und alle zugehörigen relevanten Informationen an, z. B. die Gesamtzahl der Starts der Anwendungen innerhalb des angegebenen Zeitintervalls.
- **Instanzen**: Zeigt die Berichte auf den NetScaler Instanzen an, die als Gateways für eingehenden Datenverkehr fungieren.

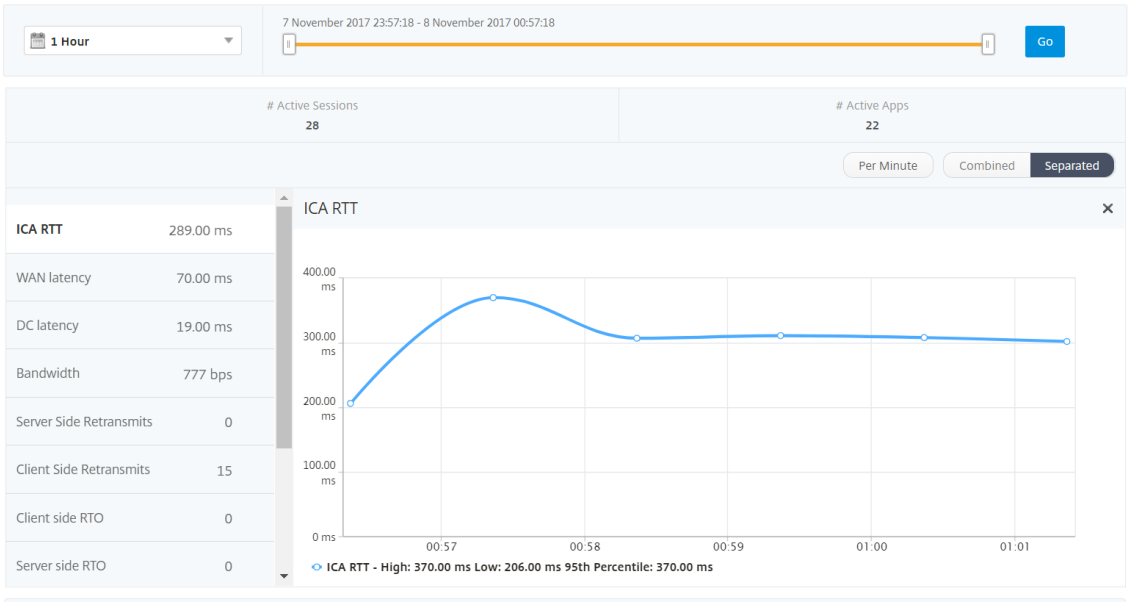
- **Desktops**: Zeigt die Berichte für die im ausgewählten Zeitraum verwendeten Desktops an.
- **Lizenzen**: Zeigt die Berichte für die Gesamtzahl der innerhalb des angegebenen Zeitfensters verwendeten SSL-VPN-Lizenzen an.

Berichte und Metriken der Benutzeransicht

Die Berichte und Metriken in dieser Ansicht werden pro Benutzer von Citrix Virtual Apps and Desktops angezeigt.

So navigieren Sie zur Benutzeransicht:

1. Navigieren Sie zu **Gateway > HDX Insight > Benutzer**



Berichte und Metriken der Benutzeransicht bestehen aus den folgenden Abschnitten:

- Zusammenfassende Ansicht
- Ansicht pro Benutzer
- Session-Ansicht pro Benutzer

Übersichtsansicht

In der Zusammenfassungsansicht werden die Berichte für alle Benutzer angezeigt, die sich während der ausgewählten Zeitleiste angemeldet haben. Alle Metriken/Berichte in dieser Ansicht zeigen die ihnen entsprechenden Werte für den ausgewählten Zeitraum an, sofern nicht anders angegeben.

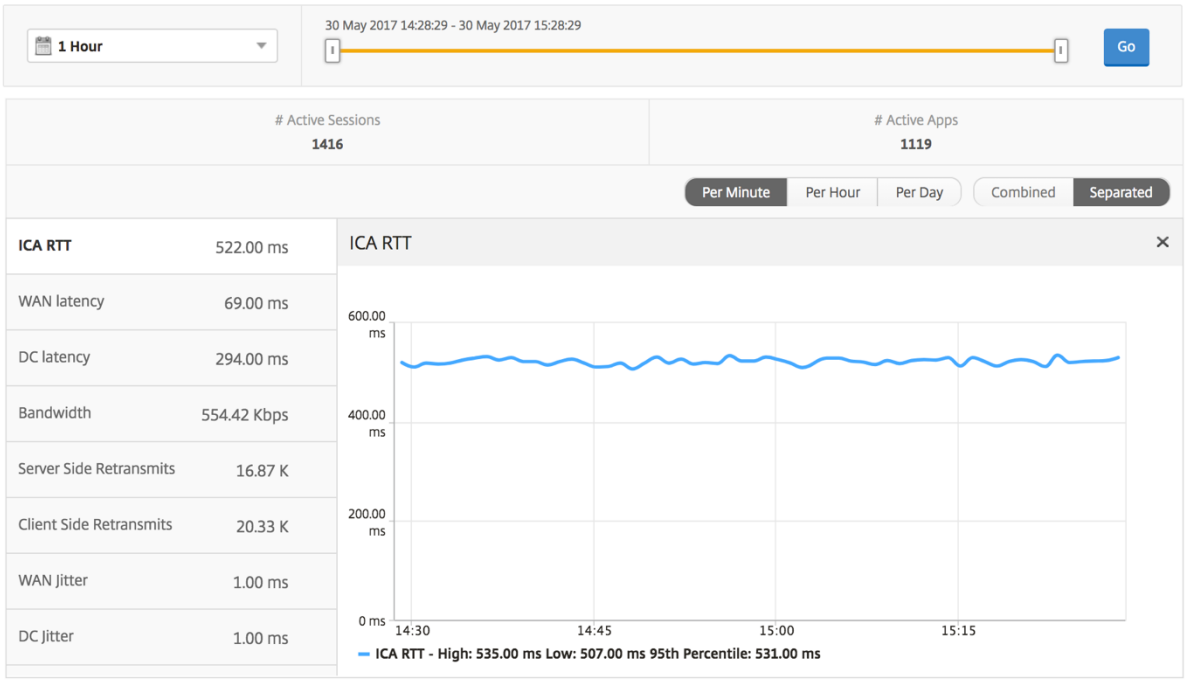
So ändern Sie den ausgewählten Zeitraum:

1. Verwenden Sie die Zeitraumeliste oder den Zeitschieberegler, um das gewünschte Zeitintervall einzustellen.
2. Klicken Sie auf **Go**.

Liniendiagramm

Metriken	Beschreibung
Anzahl 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 NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- ODER CVAD- oder StoreFront-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.

Metriken	Beschreibung
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler 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.

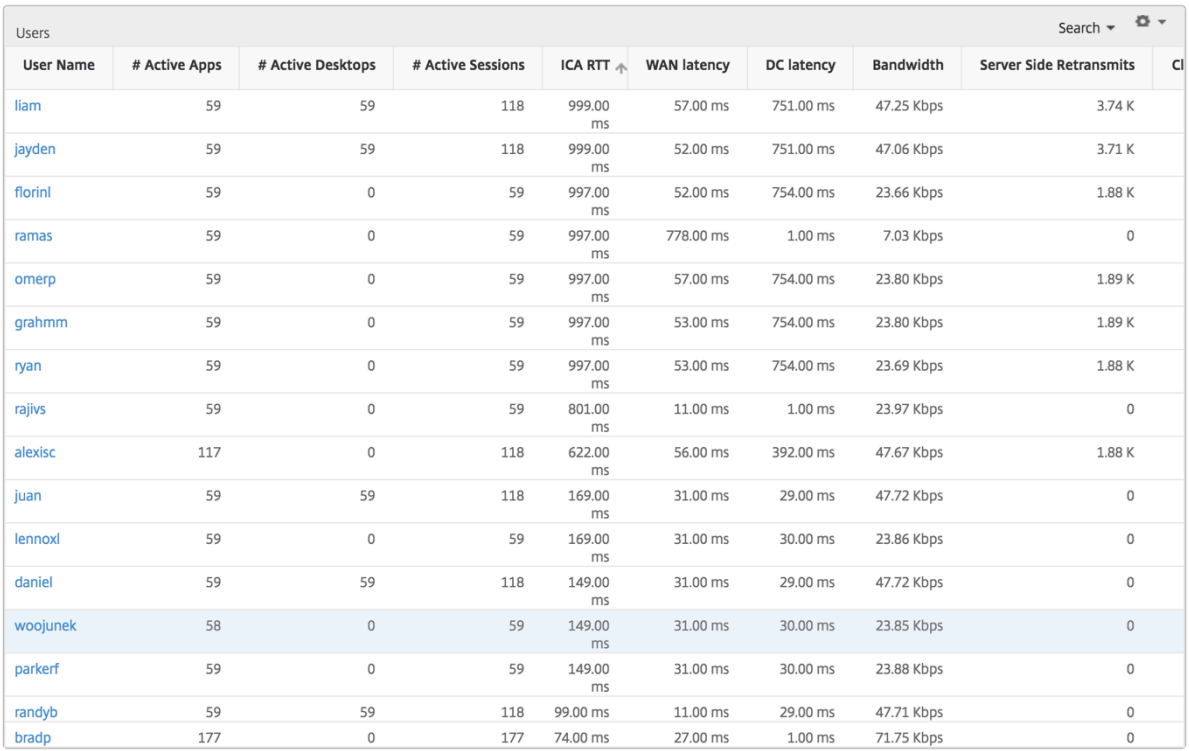


Bericht "Benutzerzusammenfassung" Im Folgenden finden Sie die Metriken, die für diesen Bericht spezifisch sind.

Metriken	Beschreibung
Anzahl 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 NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler 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.

Metriken	Beschreibung
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.

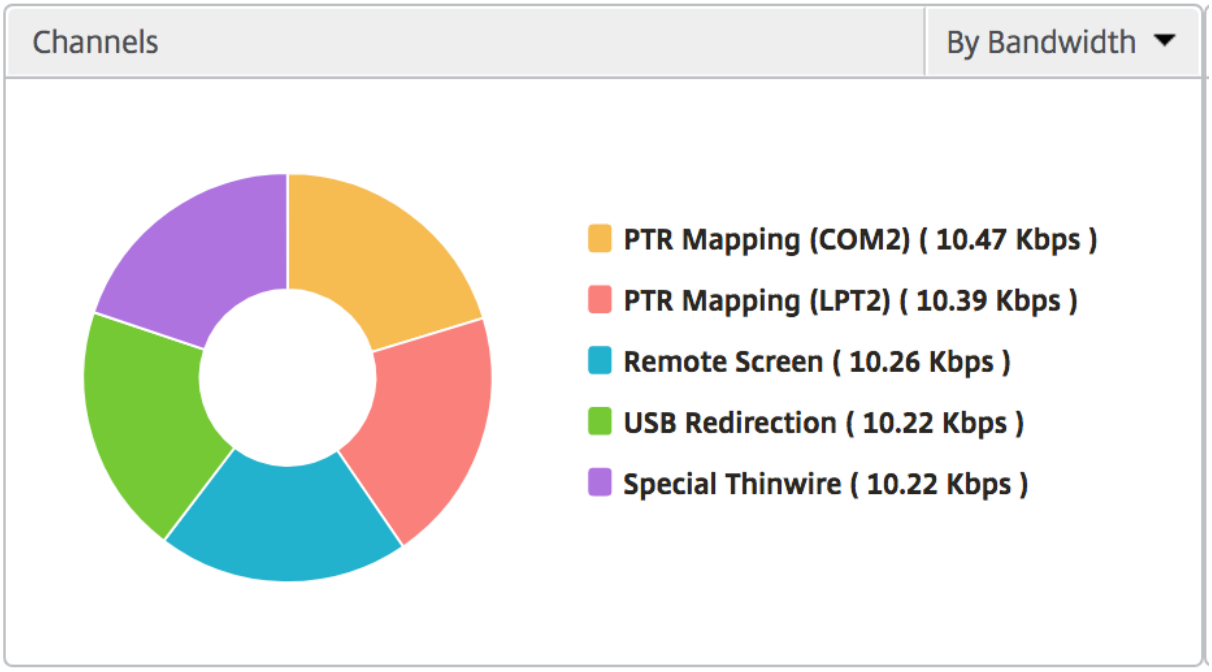


Users

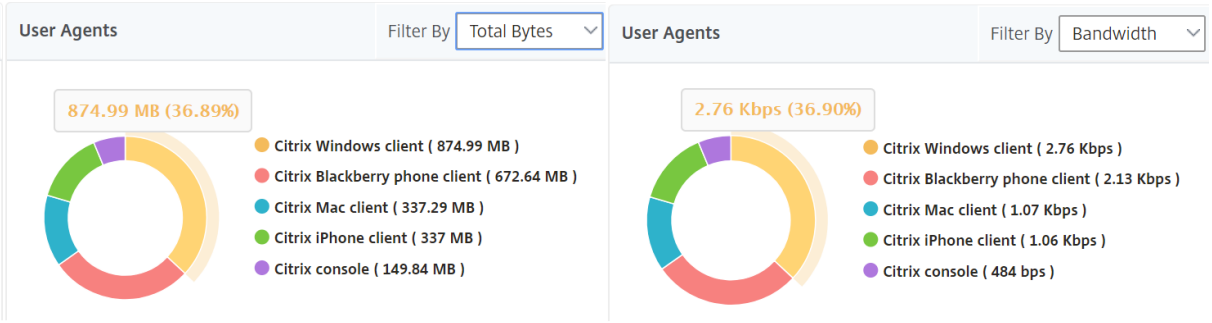
Search

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	

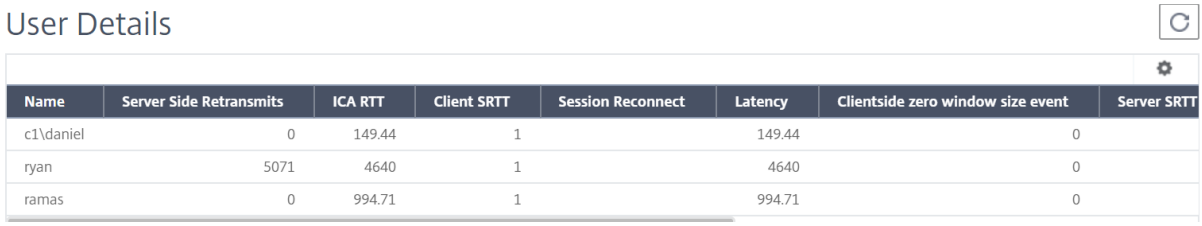
Kanäle Kanäle stellen die Gesamtbandbreite oder die Gesamtzahl der von jedem virtuellen ICA-Kanal verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Benutzer-Agenten Benutzeragenten stellen die Gesamtbandbreite/die Gesamtzahl der von jedem Workspace-Client verbrauchten Byte in Form eines Ringdiagramms dar. Jedes farbige Segment im Diagramm steht für einen Workspace-Client. Die Länge des Segments hängt von der Anzahl der Benutzer ab, die ihre Anwendungen auf diesem Workspace-Client starten. Sie können die Metriken auch nach Bandbreite oder Gesamtzahl der Bytes sortieren.



Klicken Sie auf jedes Segment, um die Details der Benutzer anzuzeigen, die diesen Workspace-Client verwenden.

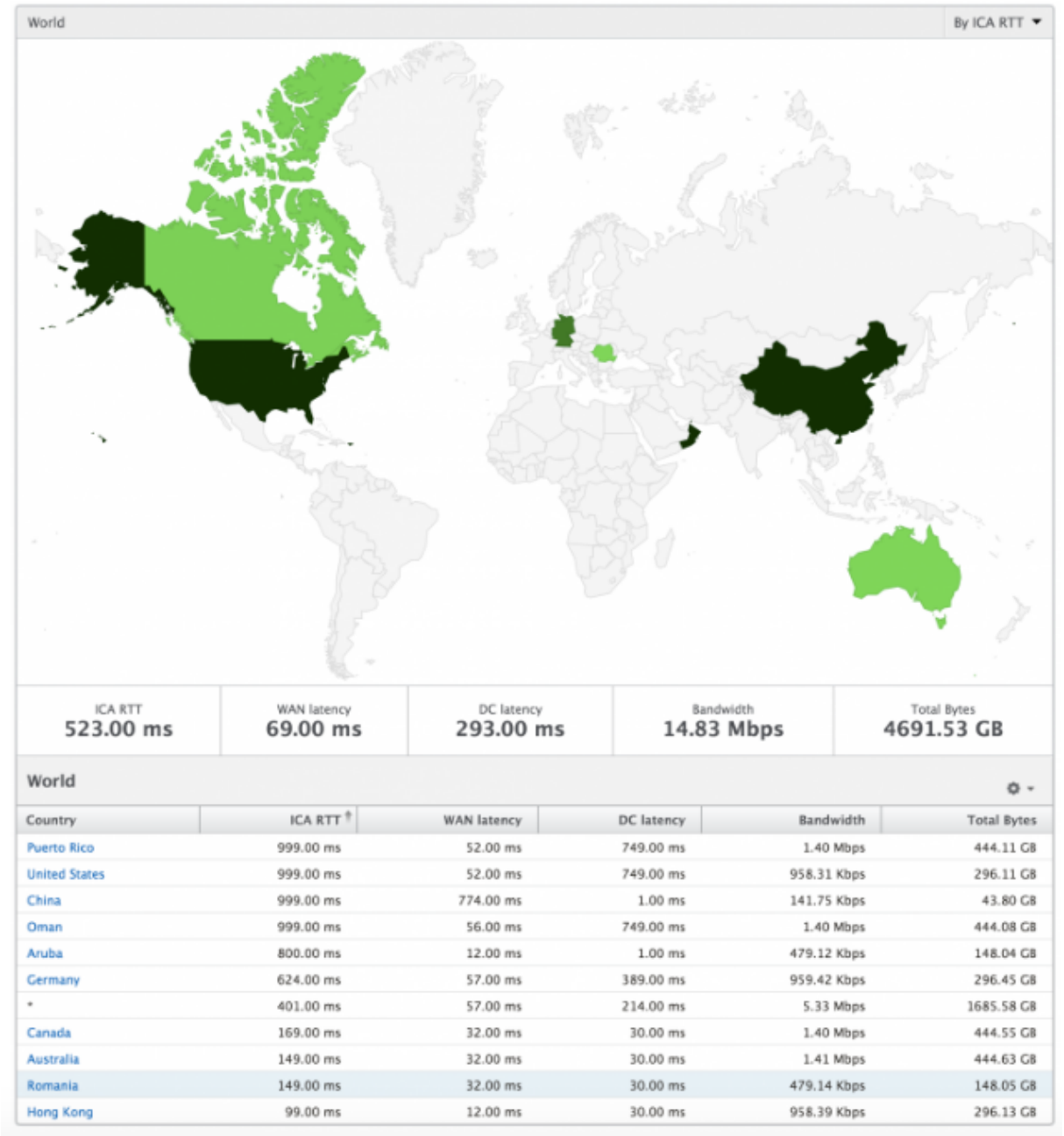


Anzahl der Schwellenwertverstöße Die Metriken für die Anzahl der Schwellenwertverstöße stellen die Anzahl der Schwellenwerte dar, die im ausgewählten Zeitraum überschritten wurden.

Weltkarte Mit der Weltkartenansicht in HDX Insight können Administratoren die historischen und aktiven Benutzerdetails aus geografischer Sicht anzeigen. Die Administratoren können eine Weltsicht auf das System haben, einen Drilldown zu einem bestimmten Land und auch weiter in Städte hineinfahren, indem sie einfach auf die Region klicken. Die Administratoren können weitere Informationen nach Stadt und Bundesstaat anzeigen. Ab NetScaler ADM Version 12.0 und höher können Sie einen Drilldown zu Benutzern 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 eines bestimmten Benutzers:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Gateway > HDX Insight > Benutzer** .

3. Wählen Sie im Übersichtsbericht Benutzer einen bestimmten Benutzer aus.

Liniendiagramm Das Liniendiagramm zeigt eine Zusammenfassung aller Metriken für den ausgewählten Benutzer während des ausgewählten Zeitraums an.

Bericht über aktuelle/abgeschlossene Sitzungen Dieser Bericht bezieht sich auf 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 NetScaler passiert, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Workspace-Typ —Citrix Windows Client usw.
Clientversion	Workspace-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.

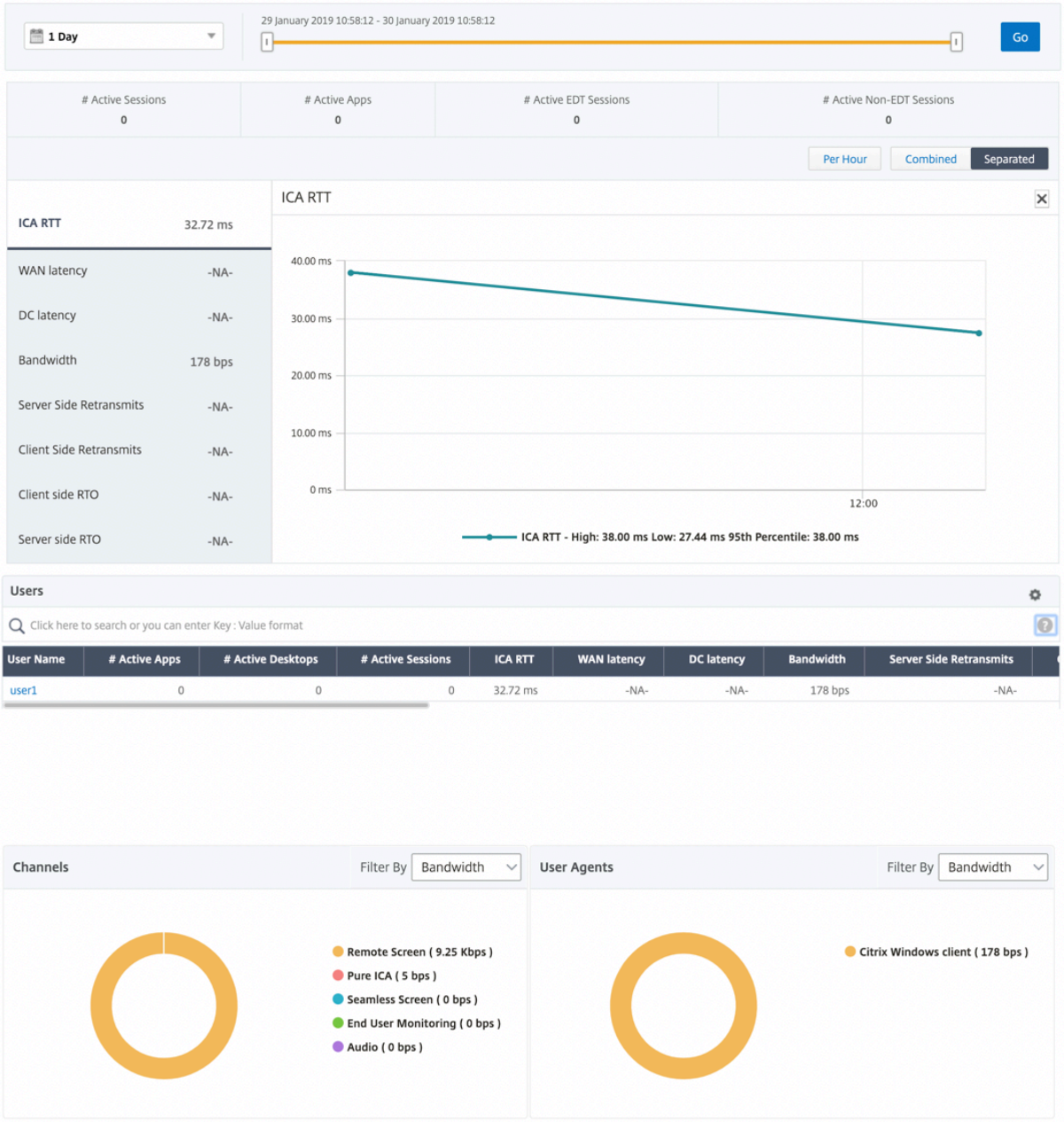
Metriken	Beschreibung
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway Benutzer/transparenter Modus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet 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 gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde 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 NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.

Metriken	Beschreibung
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler 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 NetScaler und dem Backend-Server aufgetreten ist.

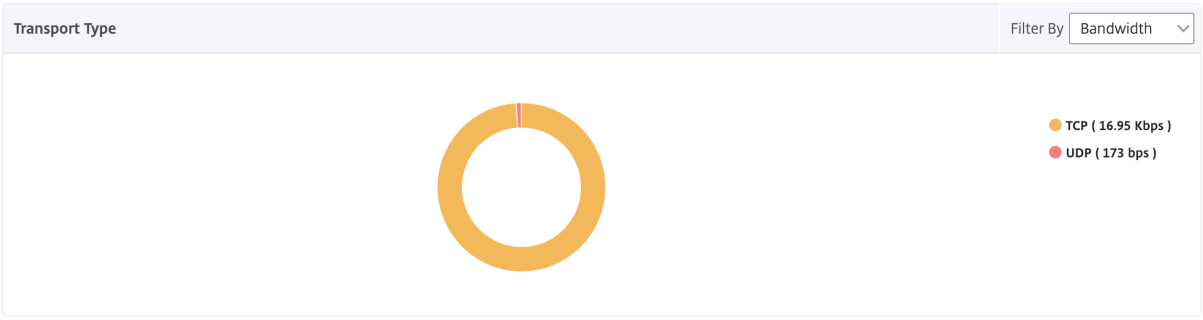
Unterstützung für EDT in HDX Insight

NetScaler Application Delivery Management (ADM) unterstützt jetzt Enlightened Data Transport (EDT) zur Anzeige von Analysen für HDX Insight. Das heißt, ADM unterstützt jetzt sowohl das UDP- als auch das TCP-Protokoll. Die EDT-Unterstützung für NetScaler Gateway gewährleistet eine hochauflösende Benutzererfahrung virtueller Desktops während der Sitzung für Benutzer, die Citrix Workspace ausführen.

HDX Insight zeigt jetzt die Anzahl der EDT-Sitzungen und Nicht-EDT-Sitzungen als Teil des Berichts über 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, erneute Übertragungen, RTOs. Einige dieser Metriken sind für Benutzer mit EDT-Sitzungen nicht verfügbar, da sie derzeit aus dem TCP-Stack berechnet werden. Daher erscheinen sie als “NA”.



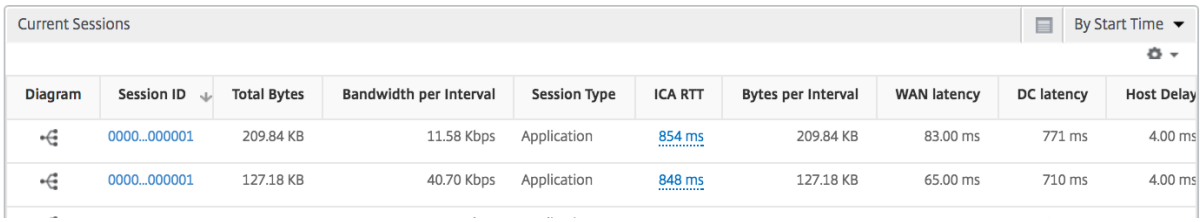
Es wurde ein neues Donutdiagramm eingeführt, mit dem Sie die vom Benutzer verbrauchte Bandbreite und die Gesamtzahl der Bytes basierend auf dem von den Benutzern verwendeten Protokolltyp sehen können.

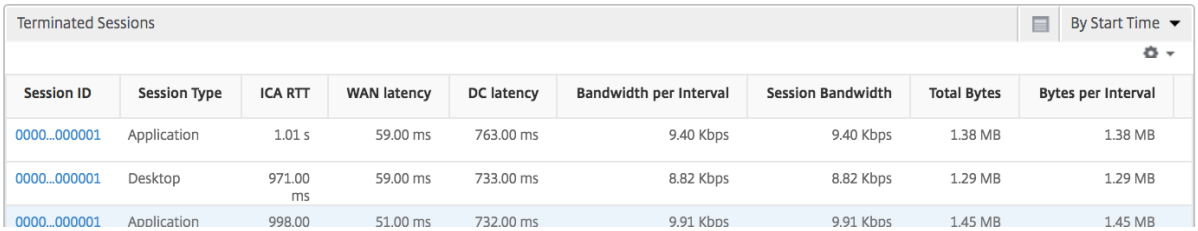


> **Hinweis:**
>
> EDT in HDX Insight wird von NetScaler ADM ab Version 12.1 Build 50.28 unterstützt und ist für ADC-Instanzen ab Version 12.1 Build 49.23 verfügbar.

HDX Insight Metriken, die ab NetScaler ADM 12.0 und höher verfügbar sind:

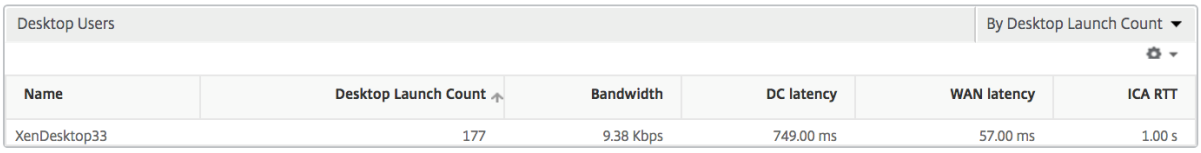
L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der NetScaler-Instanz beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.
L7 Serverseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem NetScaler 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 definierter Schwellenwert für ein festgelegtes Zeitintervall überschritten wird.
Durchschnittliche Latenz bei Sicherheitsverletzungen	Der Durchschnittswert der L7-Latenz, wenn sich das System in einem Zustand “L7-Latenz verletzt”befindet.
Anzahl von L7-Schwellenwertverletzungen	Gibt an, wie oft eine L7-Schwellenverletzung aufgetreten ist.



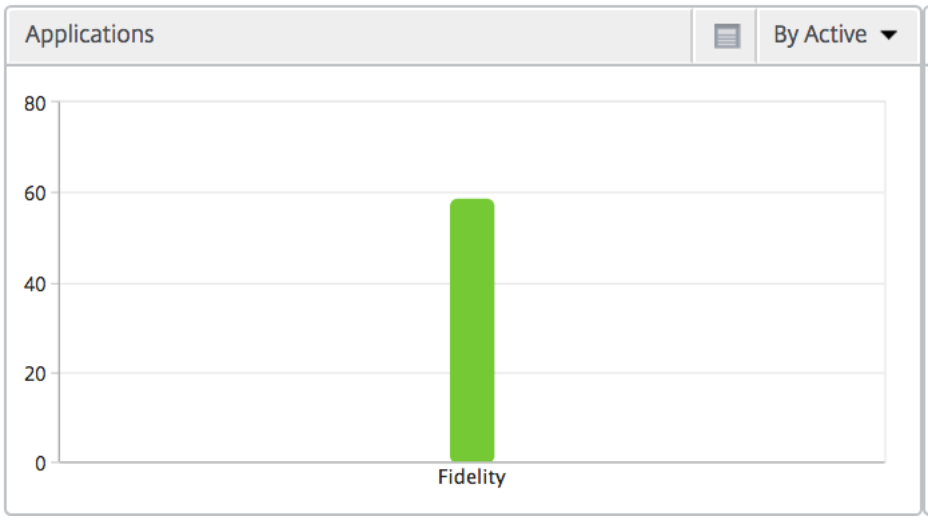


Desktop-Benutzer Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

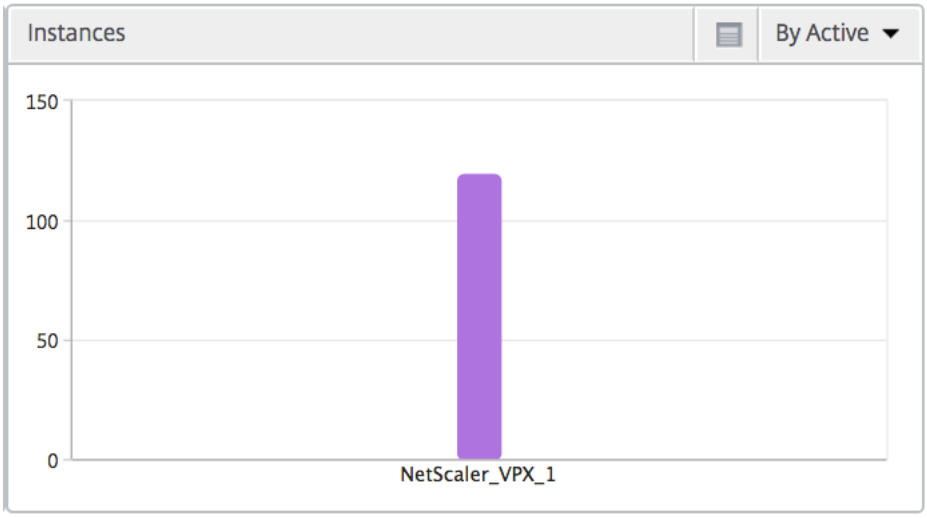
Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.
DC-Latenz	Latenz, die durch die Serverseite des Netzwerks verursacht wird. zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler 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.



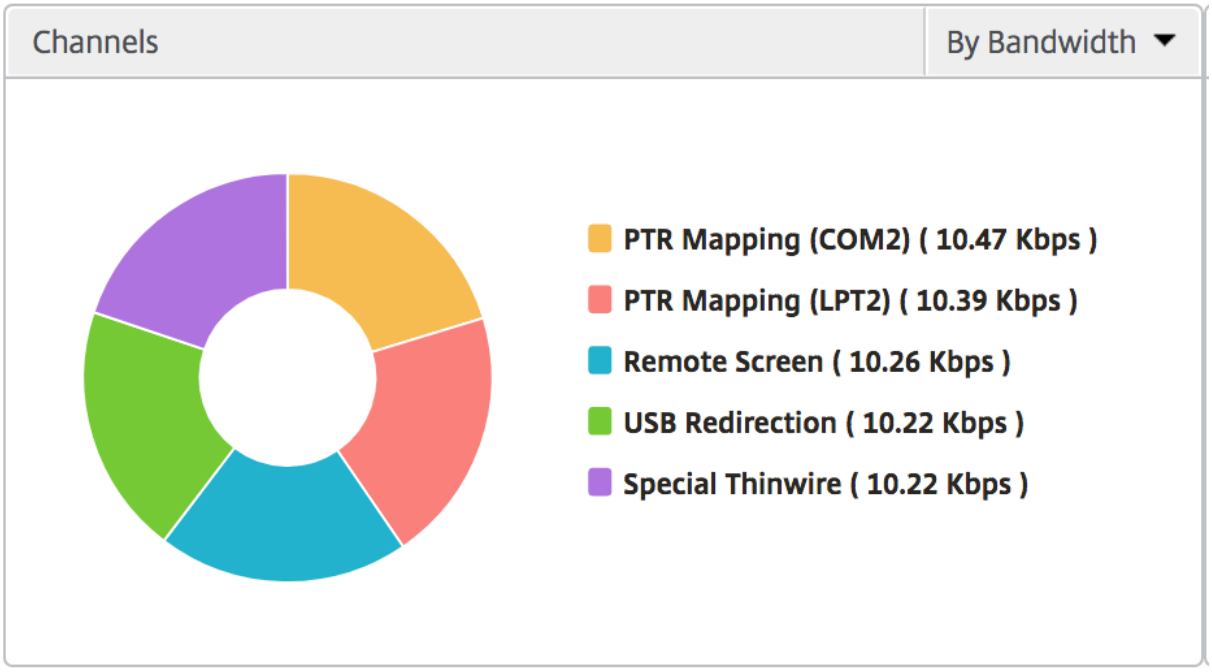
Anwendungen Ein Balkendiagramm, das Apps sortiert nach Aktiv, Gesamtzahl der Sitzungsstarts, Gesamtanzahl des App-Starts und Startdauer darstellt.



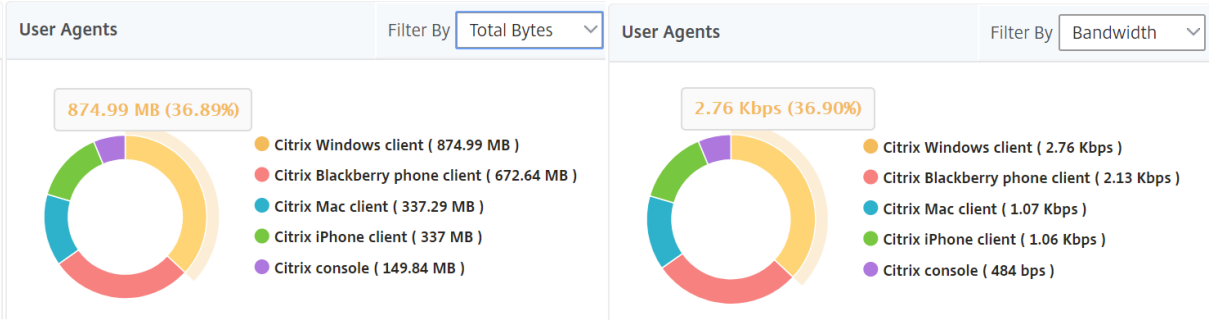
Instanzen Ein Balkendiagramm, das NetScaler Instanzen darstellt, sortiert nach Active und Apps insgesamt



Kanäle Kanäle stellen die Gesamtbandbreite oder die Gesamtzahl der von jedem virtuellen ICA-Kanal verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Benutzer-Agenten Benutzeragenten stellen die gesamte Bandbreite/Gesamtanzahl der von jedem Endpunkt verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Sitzungsansicht pro Benutzer Die Sitzungsansicht pro Benutzer bietet Berichte für die Sitzung eines bestimmten ausgewählten Benutzers.

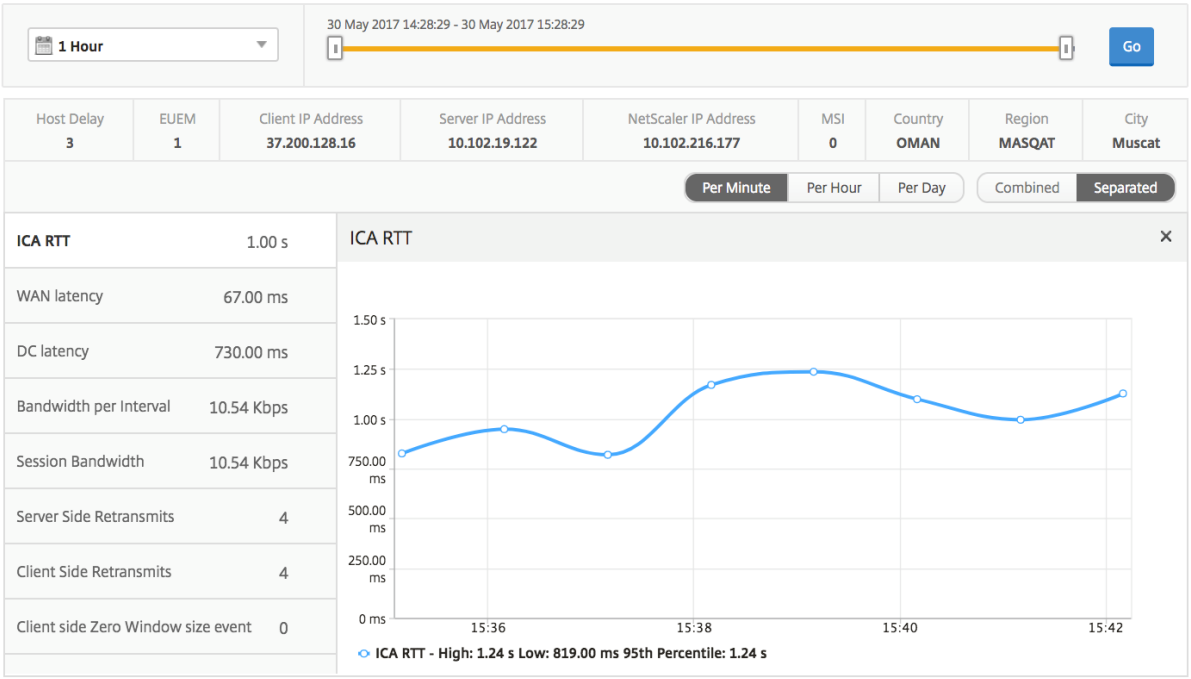
So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

1. Navigieren Sie zu **Gateway > HDX Insight > Benutzer** .
2. Wählen Sie im Abschnitt **Benutzerübersichtsbericht** einen bestimmten Benutzer aus.
3. Wählen Sie in der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** eine Sitzung aus.

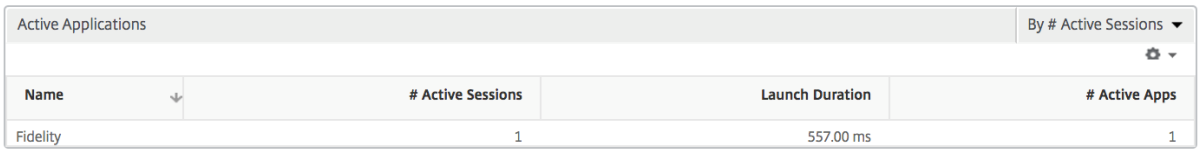
Zeitleistendiagramm

Metriken	Beschreibung
Wiederverbindung der Sitzung	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 erlebt, die auf Citrix Virtual Apps bzw. Desktops gehostet werden.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die durch die Serverseite des Netzwerks verursacht wird. zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Backend-Server aufgetreten ist.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.

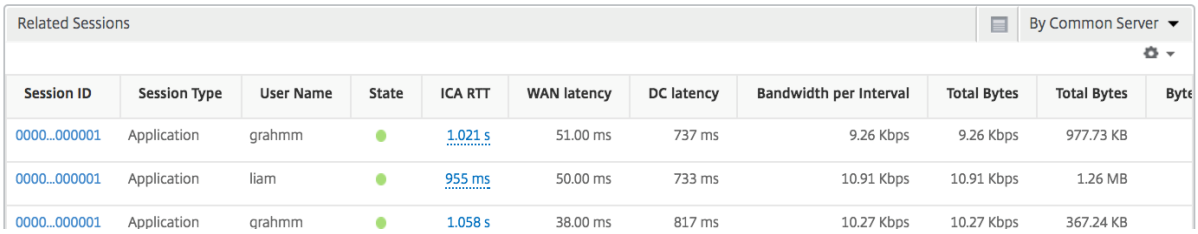
Metriken	Beschreibung
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt 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.



Verwandte Sitzungen Im Abschnitt "Sessions"werden die zugehörigen Sitzungen der Sitzungen des ausgewählten Benutzers angezeigt. Die Beziehung kann als gemeinsame Server oder gemeinsames NetScaler ausgewählt werden.



Berichte und Metriken der Anwendungsansicht

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf Citrix Virtual Apps.

So navigieren Sie zur Anwendungsansicht:

1. Navigieren Sie zu **Gateway > HDX Insight > Anwendungen** .

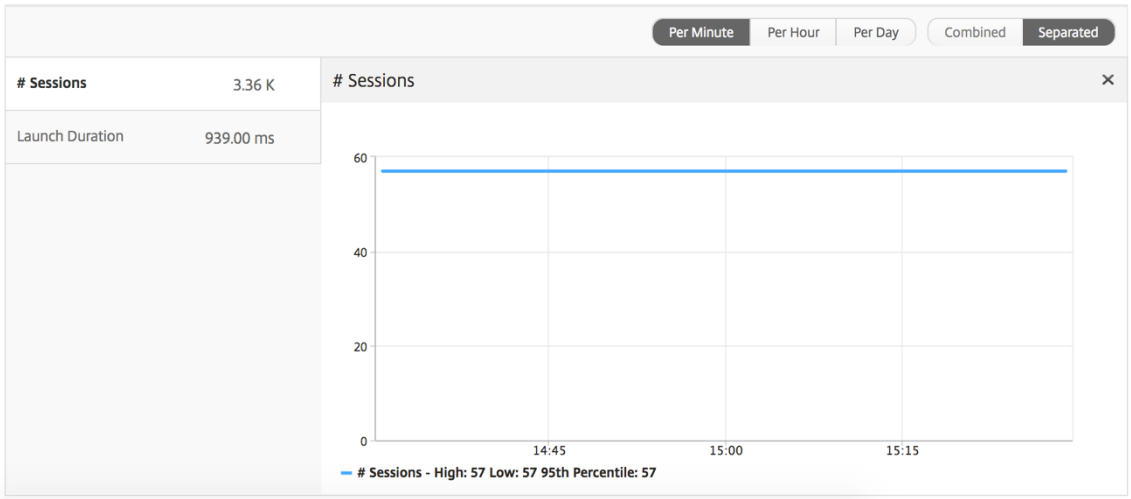
Übersichtsansicht

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.

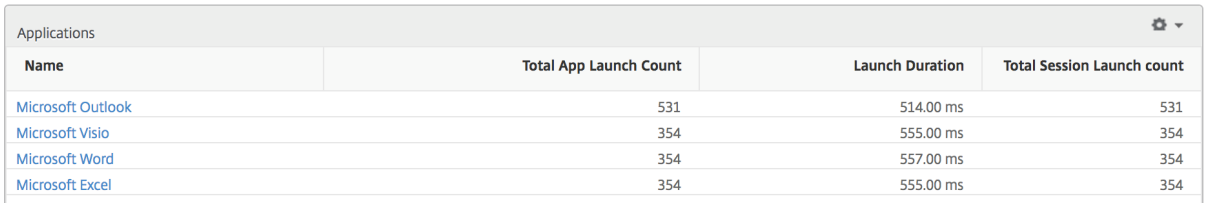
Liniendiagramm

Metriken	Beschreibung
Anzahl Sitzungen	Gesamtzahl der Sitzungen während eines bestimmten Zeitintervalls.
Dauer des Starts	Durchschnittliche Zeit zum Starten einer Anwendung.



Zusammenfassender Bericht für Anwendungen

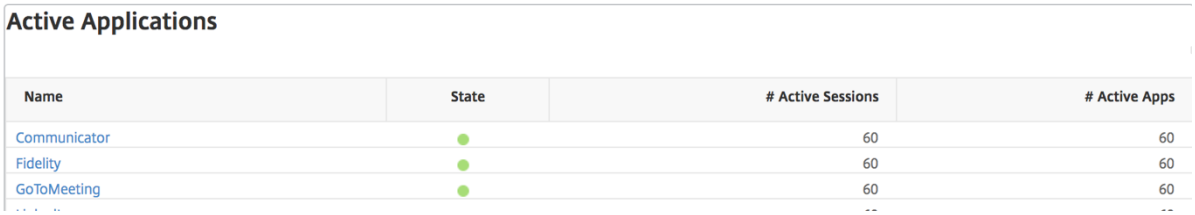
Metriken	Beschreibung
Name	Name der Citrix Virtual App.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual App-Sitzungen während des angegebenen Zeitintervalls.
App-Starts insgesamt	Gesamtzahl der Citrix Virtual App-Anwendungen, die während des angegebenen Zeitintervalls gestartet wurden.
Startdauer	Durchschnittliche Zeit für den Start der Citrix Virtual App.



Bericht über aktive Anwendungen

Metriken	Beschreibung
Name	Name der Citrix Virtual App.

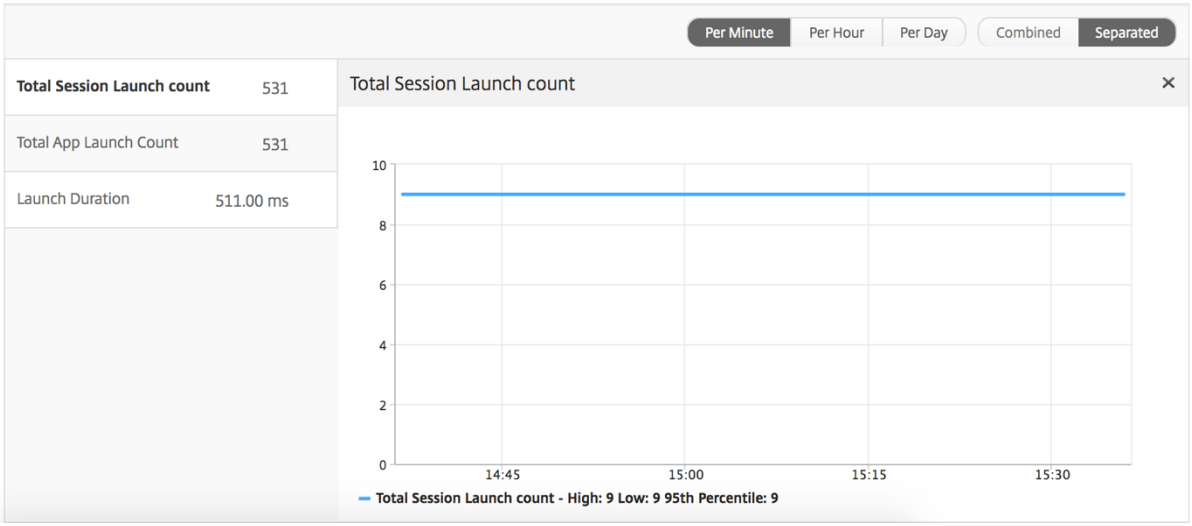
Metriken	Beschreibung
Status	Zeigt den Status der Anwendung an: Grün-Aktiv, Rot-Inaktiv
Anzahl aktiver Sitzungen	Anzahl der aktiven Benutzersitzungen, die diese App während eines bestimmten Zeitintervalls verwenden.
Anzahlt aktiver Apps	Anzahl der aktiven Sitzungen für diese Anwendung.



Bericht "Schwellenwert" Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* im ausgewählten Zeitraum als Anwendung ausgewählt wurde. Weitere Informationen finden Sie unter Erstellen von Schwellenwerten.

Liniendiagramm

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Dauer des Starts	Durchschnittliche Zeit zum Starten einer Anwendung.



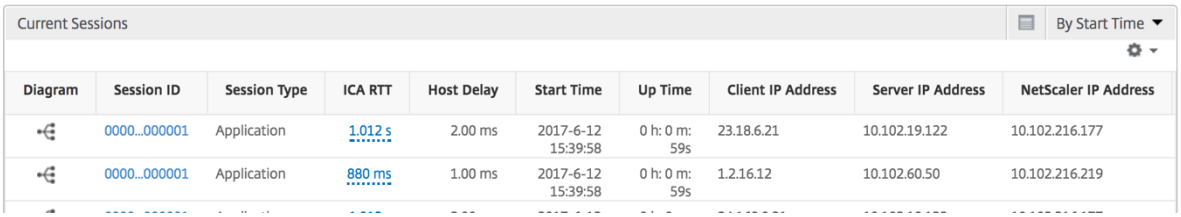
Bericht zu aktuellen Sitzungen

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 NetScaler passiert, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Workspace-Typ —Citrix Windows Client usw.

Metriken	Beschreibung
Clientversion	Workspace-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway Benutzer/transparenter Modus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet 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 gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die auf Citrix Virtual Apps bzw. Desktops gehostet werden.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.

Metriken	Beschreibung
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-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 NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler 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 NetScaler und dem Backend-Server aufgetreten ist.
Benutzername	Der Benutzername des Benutzers, der auf diese bestimmte Citrix Virtual App zugreift.
Sitzungs-ID	Eindeutige Kennung für die Citrix Virtual App-Sitzung.
Sitzungstyp	Wird “Anwendung”sein.
Status	Sitzungsstatus: Grün für aktiv, Rot für Inaktiv.
Maximale Verletzungslatenz	Der höchste Wert der L7-Latenz, wenn ein definierter Schwellenwert für ein festgelegtes Zeitintervall überschritten wird.

Metriken	Beschreibung
Durchschnittliche Latenz bei Sicherheitsverletzungen	Der Durchschnittswert der L7-Latenz, wenn sich das System in einem Zustand “L7-Latenz verletzt”befindet.
Anzahl von L7-Schwellenwertverletzungen	Gibt an, wie oft eine L7-Schwellenverletzung aufgetreten ist.
L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der NetScaler-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 NetScaler Gerät und der Citrix Virtual App beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.



Sitzungsansicht pro Anwendung

Die Session-Ansicht pro Anwendung zeigt Berichte für eine bestimmte ausgewählte Anwendungssitzung an.

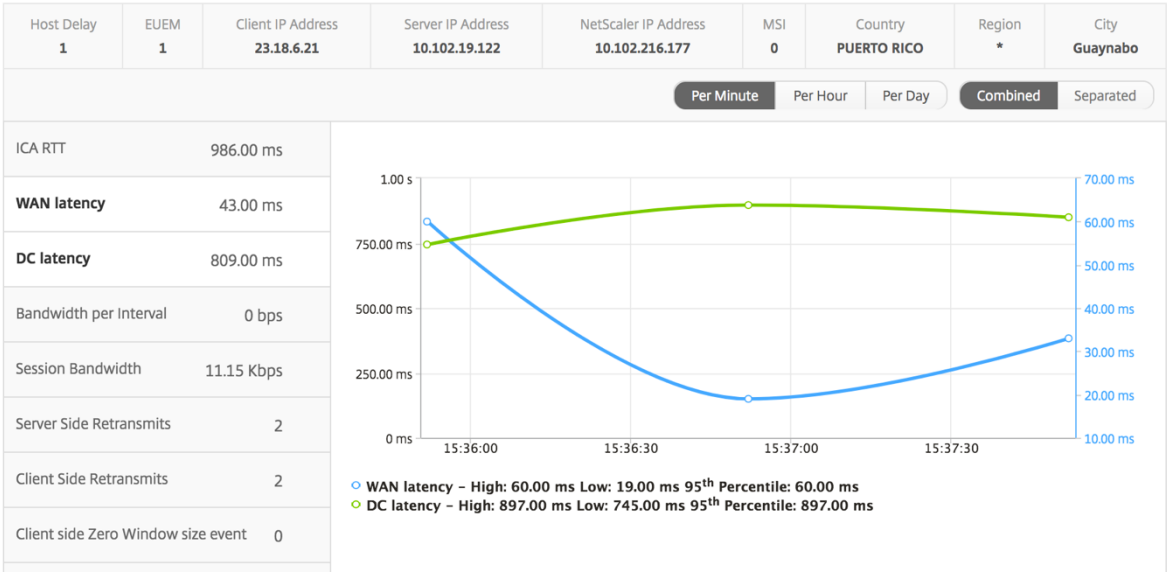
So zeigen Sie die Sitzungsberichte an:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Gateway > HDX Insight > Anwendungen** .
3. Wählen Sie im Anwendungsübersichtsbericht einen bestimmten Benutzer aus.
4. Eine Sitzung aus dem Bericht über aktuelle Sitzungen ausgewählt.

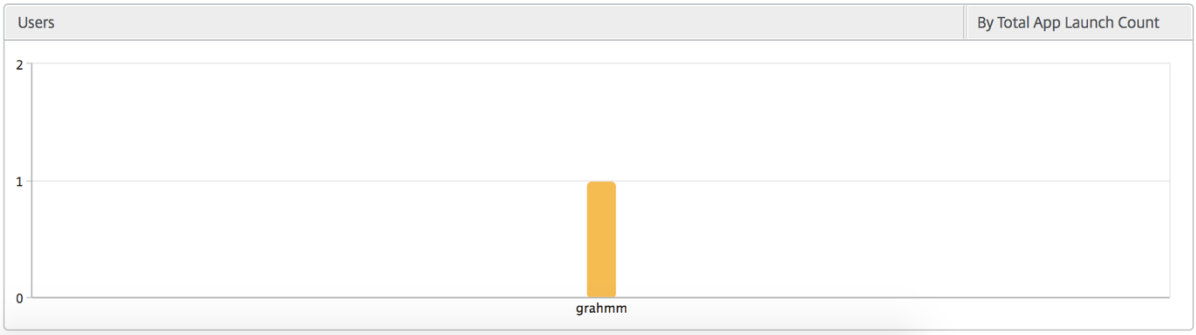
Liniendiagramm

Metriken	Beschreibung
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder 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 Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
Serverseitiges Ereignis mit Zero Window-Größe	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zu Backend-Servern.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.

Metriken	Beschreibung
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler 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.



Benutzerbalkendiagramm Das Balkendiagramm des Benutzers stellt die Benutzer dar, die in dieser speziellen App angemeldet sind.



Berichte und Metriken für Desktopansichten

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf Citrix Virtual Desktops.

So navigieren Sie zur Desktopansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Gateway > HDX Insight > Desktop** .

Übersichtsansicht

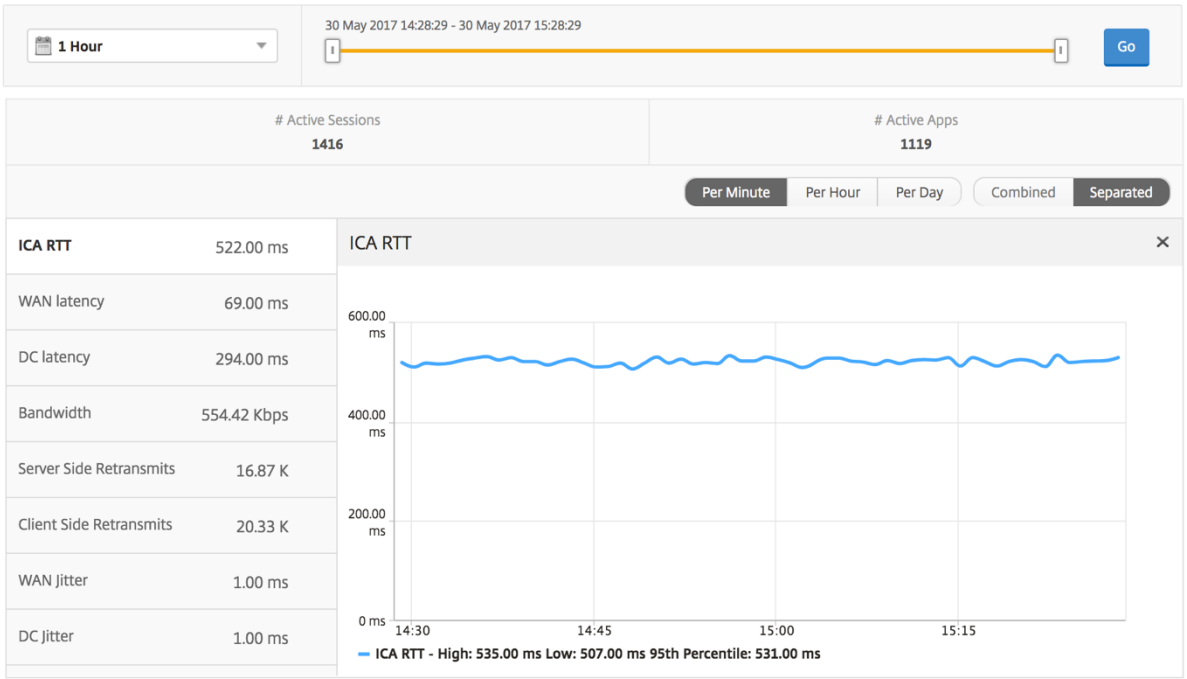
In der Zusammenfassungsansicht werden die Berichte für alle Citrix Virtual Desktops angezeigt, die während der ausgewählten Zeitleiste angemeldet sind.

Alle Metriken/Berichte, sofern nicht ausdrücklich erwähnt, haben die Werte, die ihnen für den ausgewählten Zeitraum entsprechen.

Liniendiagramm

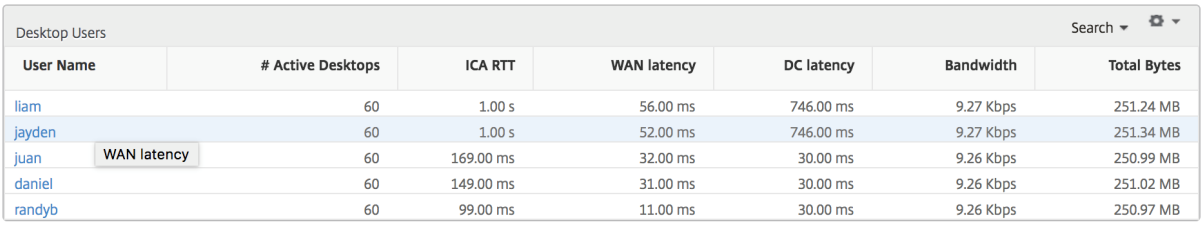
Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.

Metriken	Beschreibung
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler 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.



Desktop-Sammelbericht

Metriken	Beschreibung
Aktive Sitzungen	Gesamtzahl der aktiven Citrix Virtual Desktop-Sitzungen während eines bestimmten Zeitintervalls.
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 Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.



Bericht "Schwellenwert" Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* in der ausgewählten Periode als Desktop ausgewählt wurde. Weitere Informationen finden Sie unter Erstellen von Schwellenwerten.

Pro Desktop-Ansicht

Die Ansicht pro Desktop bietet detaillierte Berichte zur Endbenutzererfahrung für einen ausgewählten Citrix Virtual Desktop.

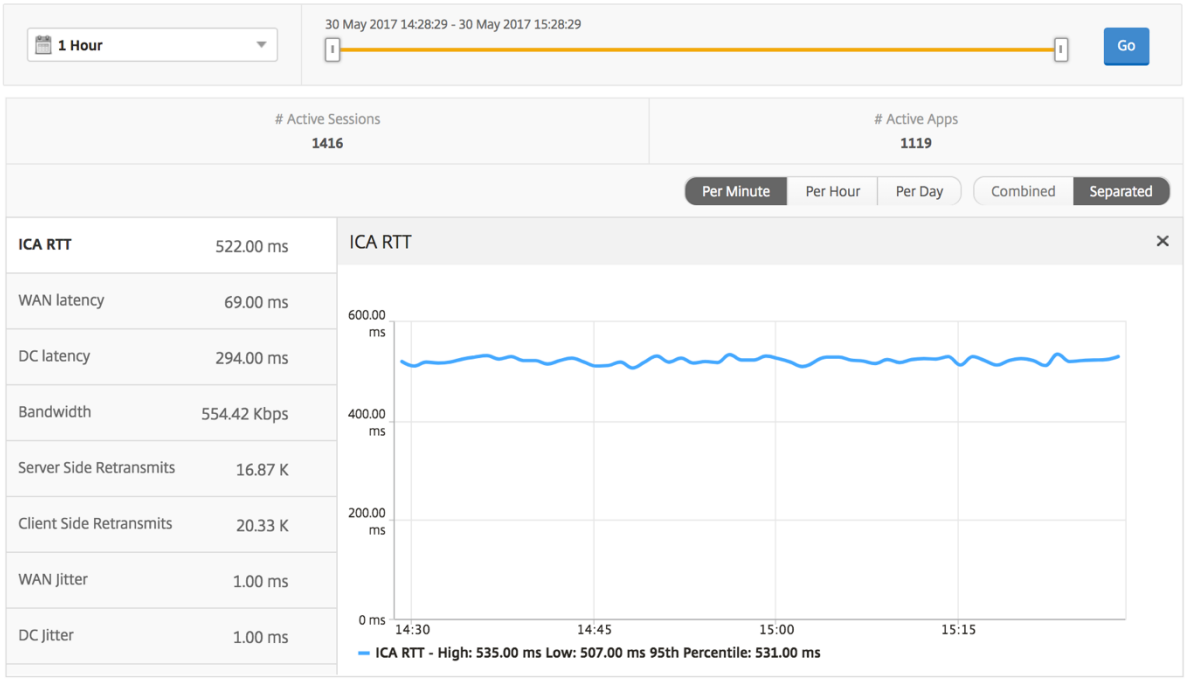
So navigieren Sie zur jeweiligen Desktop-Ansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics > HDX Insight > Desktop**.
3. Wählen Sie im **Desktop-Zusammenfassungsberichteinen bestimmten Desktop**aus.

Liniendiagramm

Metriken	Beschreibung
Anzahl 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 Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.

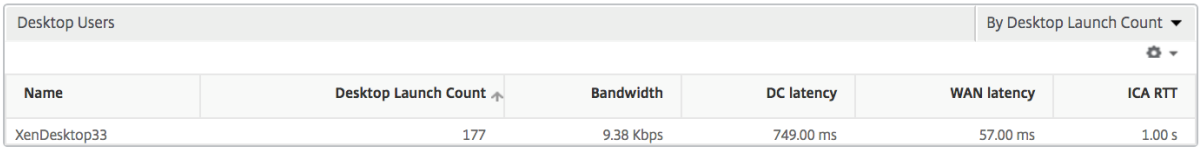
Metriken	Beschreibung
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler 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.



Bericht "Desktop-Benutzer" Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.

Metriken	Beschreibung
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler 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 Apps and Desktops gehostet wird.



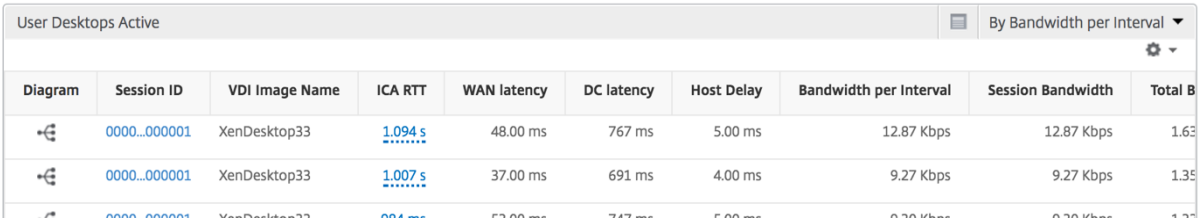
Benutzerdesktops Aktiv/Inaktiv Bericht Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

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 NetScaler passiert, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.

Metriken	Beschreibung
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Workspace-Typ —Citrix Windows Client usw.
Clientversion	Workspace-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway Benutzer/transparenter Modus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet 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 gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.

Metriken	Beschreibung
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde 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 Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-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 NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler 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 NetScaler und dem Backend-Server aufgetreten ist.
VDI-Imagename	Name des Citrix Virtual Desktop, mit dem der Benutzer verbunden ist
Diagramm	



Sitzungsansicht pro Desktop-Sitzung

Pro Desktop-Sitzungsansicht stellt Berichte für eine bestimmte ausgewählte Citrix Virtual Desktop-Sitzung bereit.

So navigieren Sie zur Desktop-Sitzungsansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics > HDX Insight > Desktop**.
3. Wählen Sie im **Desktopübersichtsbericht einen bestimmten Desktop**aus.
4. Wählen Sie eine Sitzung aus dem Bericht über aktuelle Sitzungen aus.

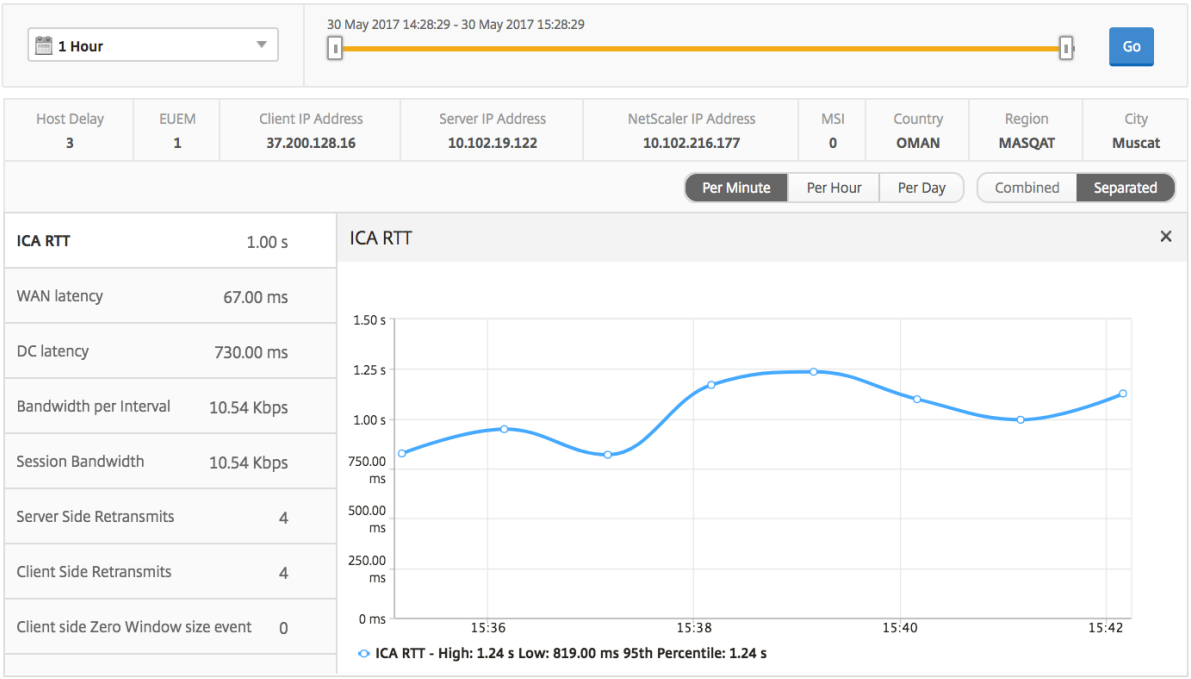
Zeitleistendiagramm Die Sitzungsansicht pro Benutzer bietet Berichte für die Sitzung eines bestimmten ausgewählten Benutzers.

So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Gateway > HDX Insight > Benutzer** .
3. Wählen Sie im Abschnitt **Benutzerübersichtsbericht** einen bestimmten Benutzer aus.
4. Wählen Sie in der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** eine Sitzung aus.

Metriken	Beschreibung
Wiederverbindung der Sitzung	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 Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Backend-Server aufgetreten ist.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.

Metriken	Beschreibung
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.



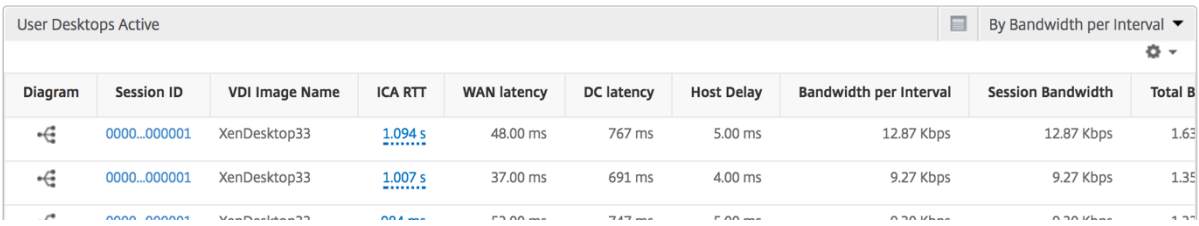
Bericht zu verwandten Desktop-Sitzungen Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

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 NetScaler passiert, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.

Metriken	Beschreibung
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Workspace-Typ —Citrix Windows Client usw.
Clientversion	Workspace-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway Benutzer/transparenter Modus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet 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 gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.

Metriken	Beschreibung
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde 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 Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-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 NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler 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 NetScaler und dem Backend-Server aufgetreten ist.



Instanzansicht von Berichten und Metriken

Die Berichte und Metriken in der Instanzansicht konzentrieren sich auf die NetScaler Instanzen.

So navigieren Sie zur Instanzansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics > HDX Insight > Instances**.

Berichte und Metriken zur Instanzansicht bestehen aus den folgenden Abschnitten:

- Instanzzusammenfassungsansicht
- Ansicht pro Instanz

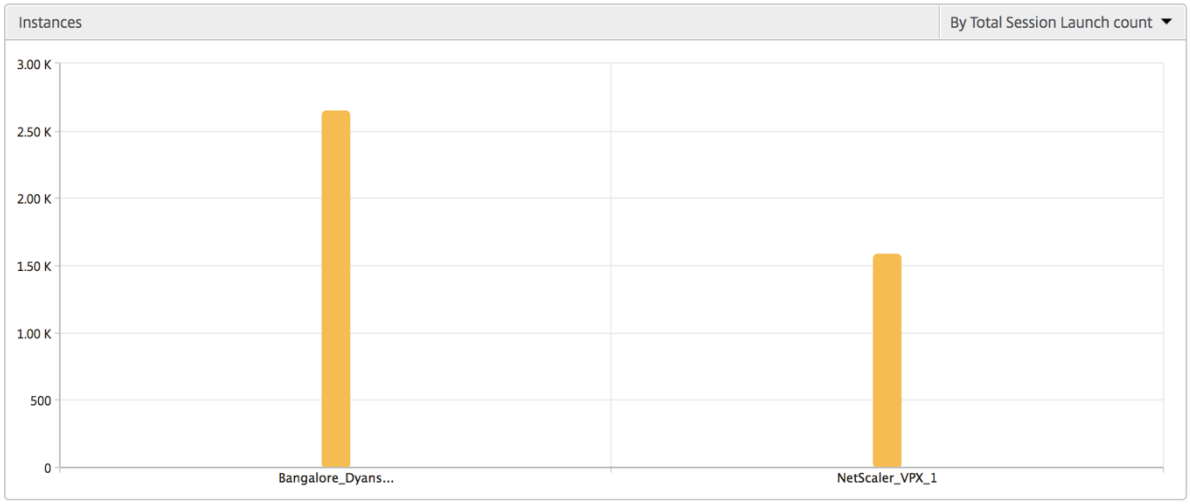
Instanz-Zusammenfassungsansicht

Diese Ansicht wird als Zusammenfassungsansicht bezeichnet, da sie die Berichte für alle NetScaler Instanzen anzeigt, die NetScaler ADM hinzugefügt werden.

Alle unten aufgeführten Metriken/Berichte, sofern nicht explizit erwähnt, haben die Werte, die ihnen für den ausgewählten Zeitraum entsprechen.

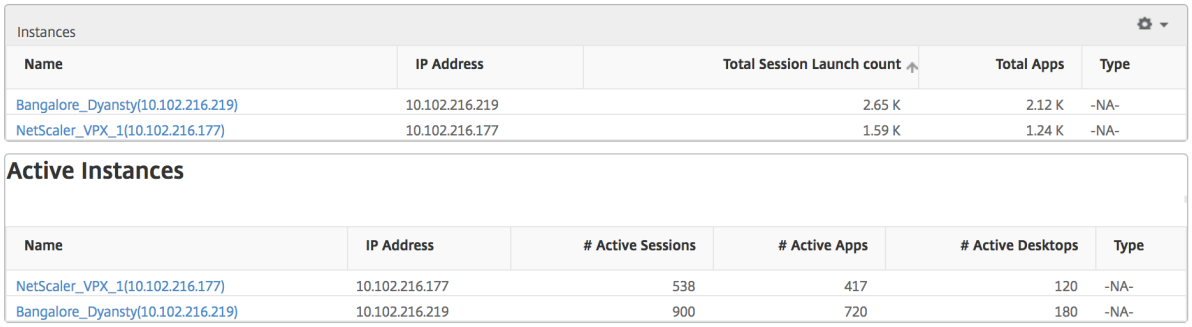
Instanz-Balkendiagramm

In diesem Diagramm wird die Instanz im Vergleich zur Gesamtzahl der Sitzungsstarts angezeigt.	Gesamtzahl der Apps, die aus der Liste oben rechts auf der Diagrammfläche ausgewählt werden können.



Übersichtsbericht "Instanz/Aktive Instanzen"

Metriken	Beschreibung
Name	Hostname der NetScaler-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	–



Instances

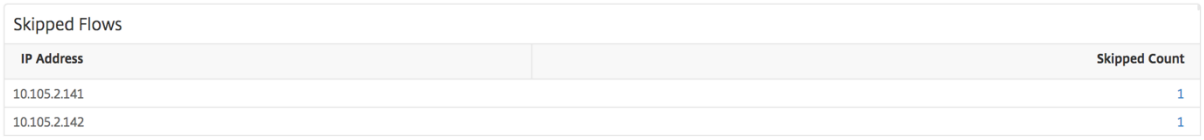
Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

Bericht "Schwellenwert" 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 Erstellen von Schwellenwerten.

Übersprungene Flows Ein übersprungener Flow ist ein Datensatz, der die Parsing ICA-Verbindung übersprungen hat. Dies kann verschiedene Gründe haben, z. B. die Verwendung nicht unterstützter Versionen von Citrix Virtual Apps and Desktops, die nicht unterstützte Version von Workspace oder Workspace-Typ usw. Diese Tabelle zeigt die IP-Adresse und die Anzahl der übersprungenen Datenflüsse. Diese Arbeitsbereiche dürfen nicht Teil von Arbeitsbereichen auf der Whitelist sein. Daher werden diese Sitzungen von der Überwachung übersprungen.



Skipped Flows

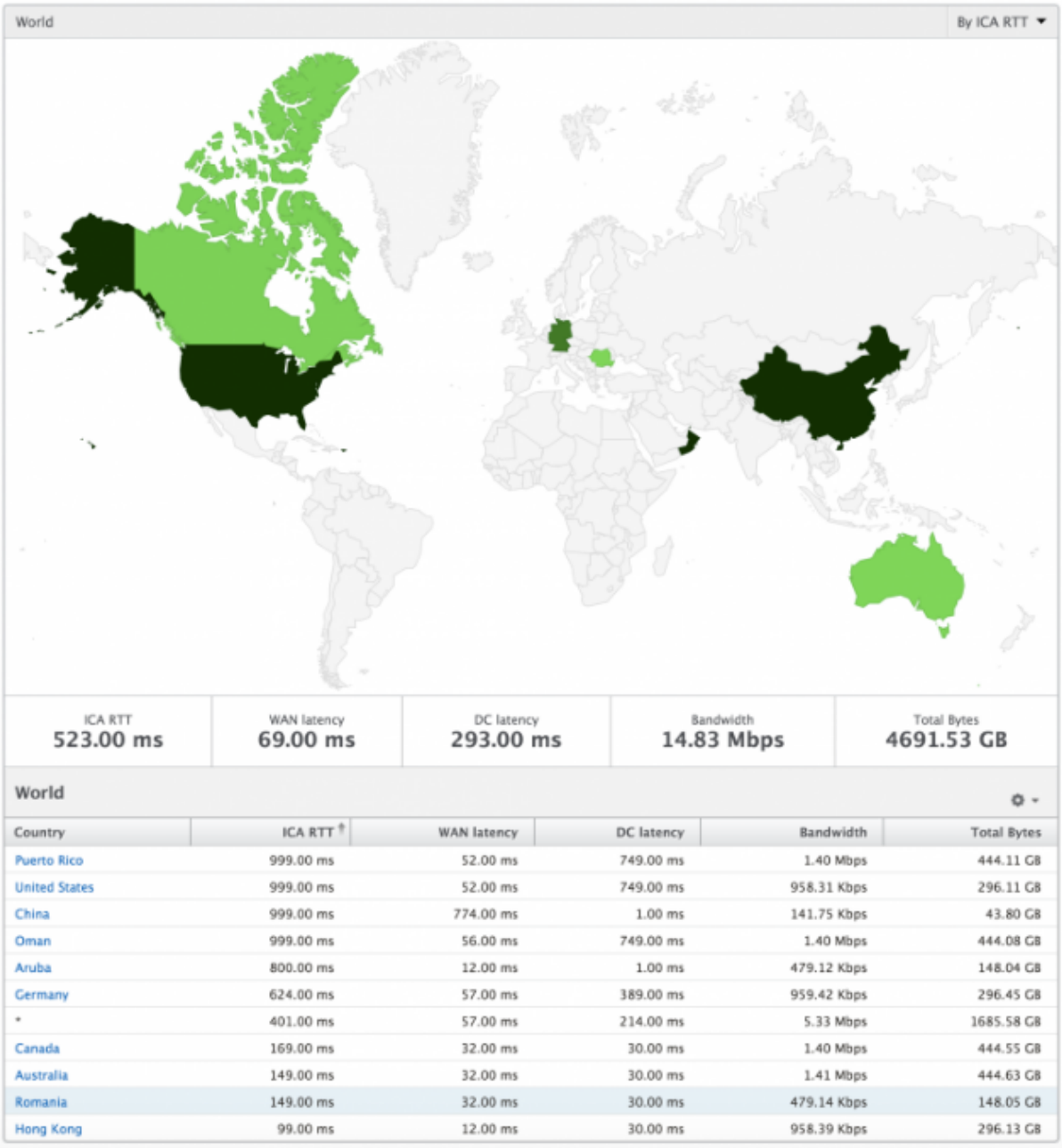
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

Weltansicht Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die historischen und aktiven Benutzerdetails aus geografischer Sicht anzuzeigen. 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 NetScaler ADM Version 12.0 und höher können Sie einen Drilldown zu Benutzern 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 Instanz

Die Ansicht pro Instanz bietet detaillierte Berichte über die Benutzererfahrung für eine bestimmte ausgewählte NetScaler Instanz.

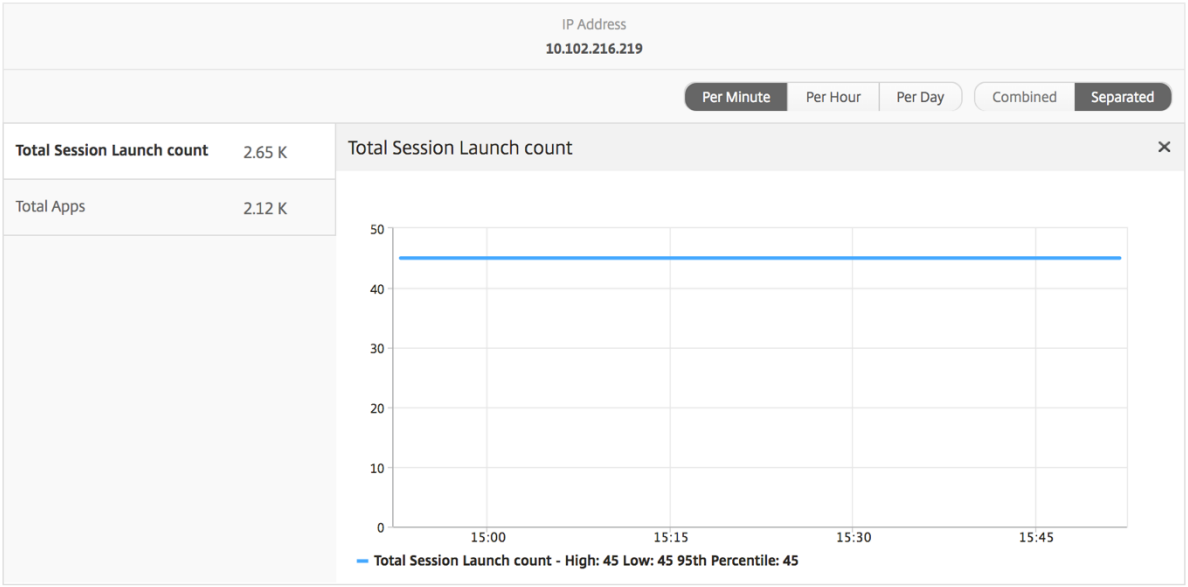
So navigieren Sie zur Instanzansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.

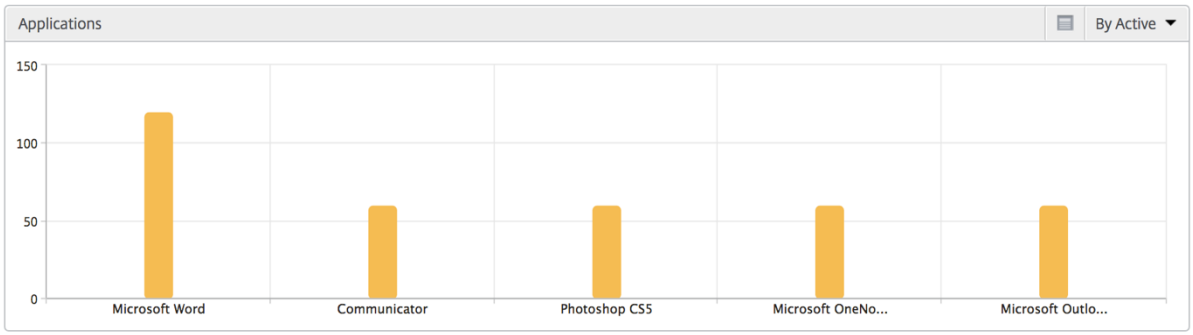
2. Navigieren Sie zu **Analytics > HDX Insight > Instances**.
3. Wählen Sie in der **Auswertung "Instanzübersicht"** eine bestimmte Instanz aus.

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.

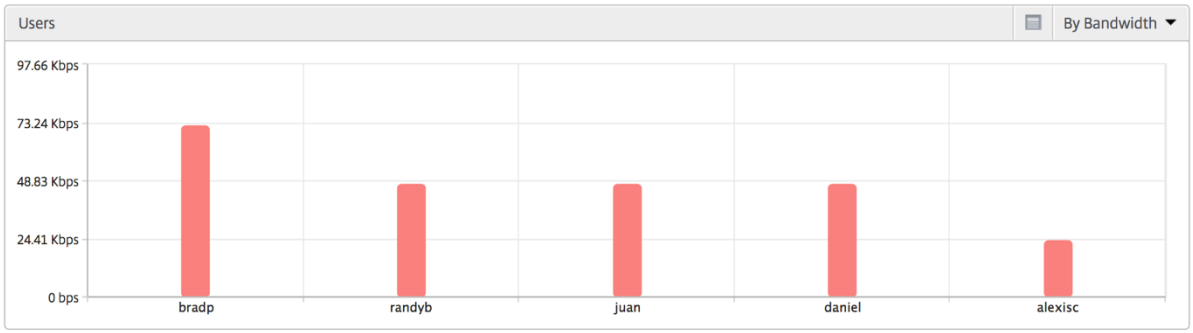


Balkendiagramm für Anwendungen Zeigt die 5 wichtigsten Anwendungen basierend auf den folgenden Kriterien an: nach aktiven Apps, Gesamtzahl der Sitzungsstarts, Gesamtzahl der App-Startstarts oder Startdauer.



Balkendiagramm "Benutzer" Das Balkendiagramm "Benutzer"zeigt die fünf wichtigsten Benutzer anhand der folgenden Kriterien an:

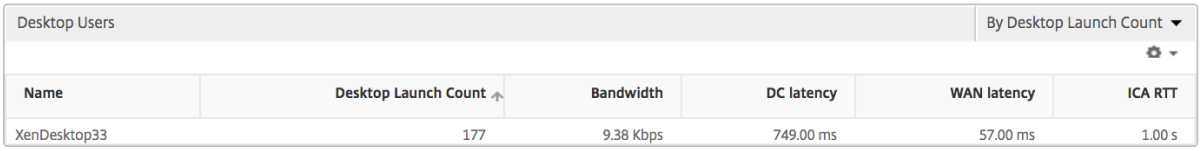
- Bandbreite
- WAN-Latenz
- DC-Latenz
- ICA RTT



Bericht "Desktop-Benutzer" Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.

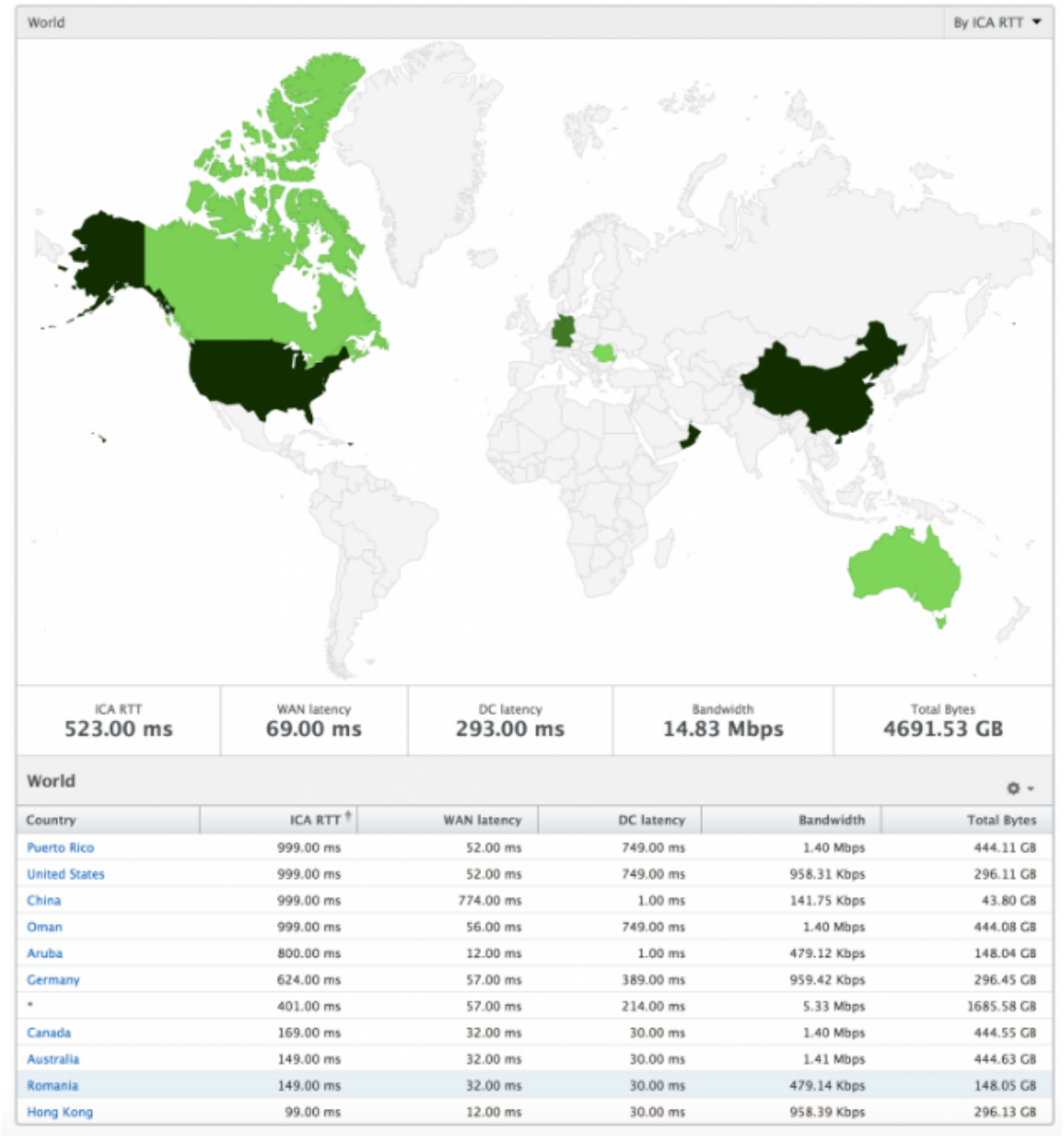
Metriken	Beschreibung
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops 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 einen weiteren Drilldown durchführen, um Informationen nach Stadt und Bundesland anzuzeigen. Ab NetScaler ADM Version 12.0 und höher können Sie einen Drilldown zu Benutzern 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

Lizenzansicht Berichte und Metriken

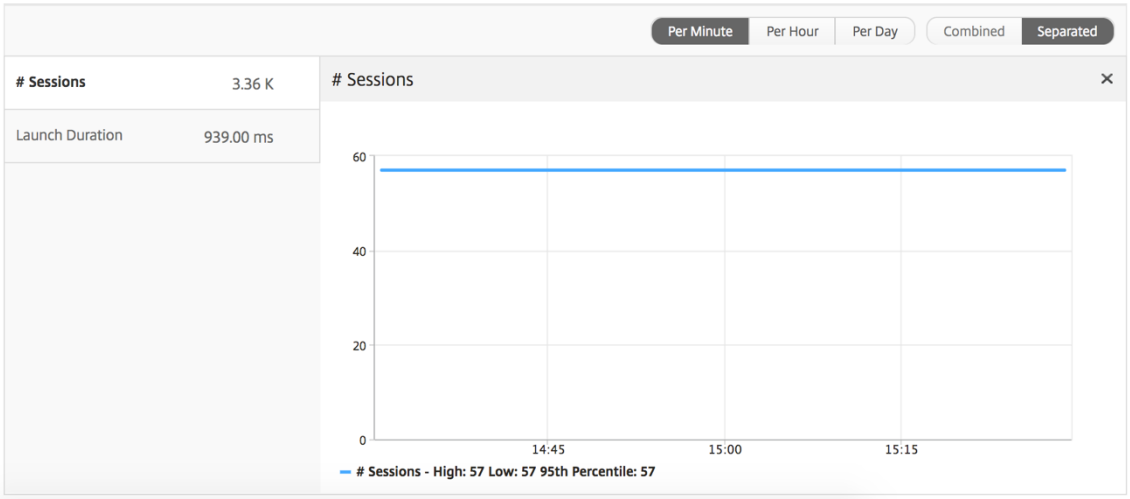
Die Lizenzansicht enthält Details zu den NetScaler Gateway-Lizenzinformationen.

So navigieren Sie zur Lizenzansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics > HDX Insight > Lizenzen**.

Liniendiagramm

Metriken	Beschreibung
Verwendete Lizenzen	Die NetScaler Gateway CCU-Lizenzen, die während der ausgewählten Zeitleiste verwendet werden. Jede Zählung steht für die Anzahl der Benutzersitzungen. Dies ist unabhängig von den Anwendungs- und Desktopsitzungen, die von diesem Benutzer gestartet wurden.
Gesamtzahl der Lizenzen	Gesamtzahl der NetScaler Gateway CCU-Lizenzen, die der Kunde nutzen kann.



Bericht "Schwellenwert" Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* im ausgewählten Zeitraum als Lizenz ausgewählt wurde. Weitere Informationen finden Sie unter Erstellen von Schwellenwerten.

Berichte und Metriken der Anwendungsansicht

February 5, 2024

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf Citrix Virtual Apps.

So navigieren Sie zur Anwendungsansicht:

1. Navigieren Sie zu **Gateway > HDX Insight > Anwendungen** .

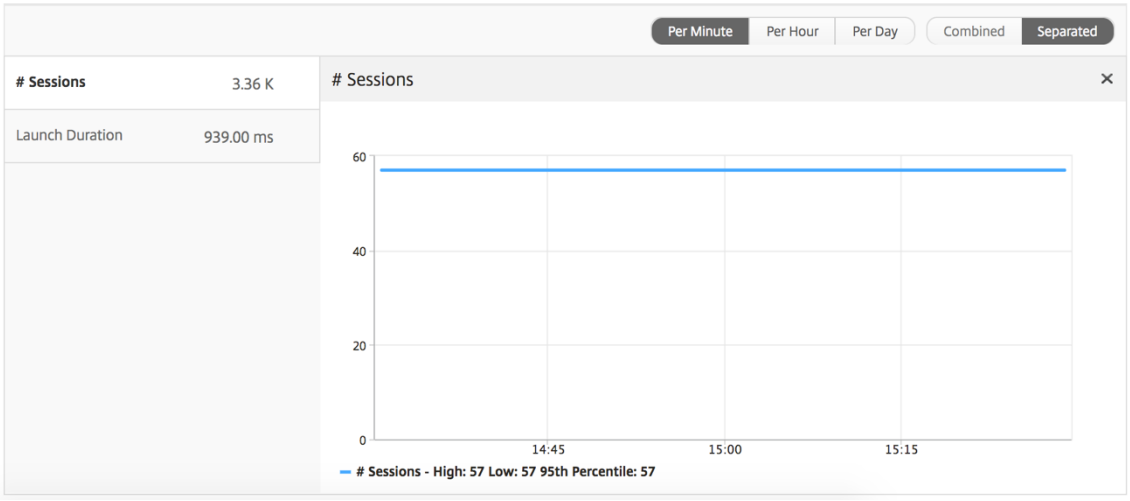
Übersichtsansicht

In der Zusammenfassungsansicht werden die Berichte für alle Anwendungen angezeigt, die während der ausgewählten Zeitachse angemeldet sind.

Alle unten aufgeführten Metriken/Berichte haben, sofern nicht ausdrücklich erwähnt, die entsprechenden Werte für den ausgewählten Zeitraum.

Liniendiagramm

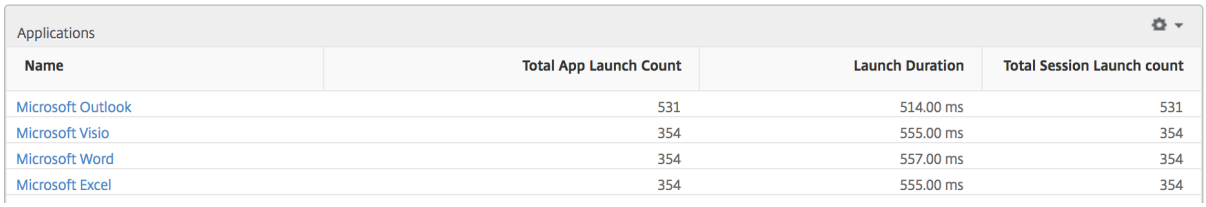
Metriken	Beschreibung
Anzahl Sitzungen	Gesamtzahl der Sitzungen während eines bestimmten Zeitintervalls.
Dauer des Starts	Durchschnittliche Zeit zum Starten einer Anwendung.



Zusammenfassender Bericht für Anwendungen

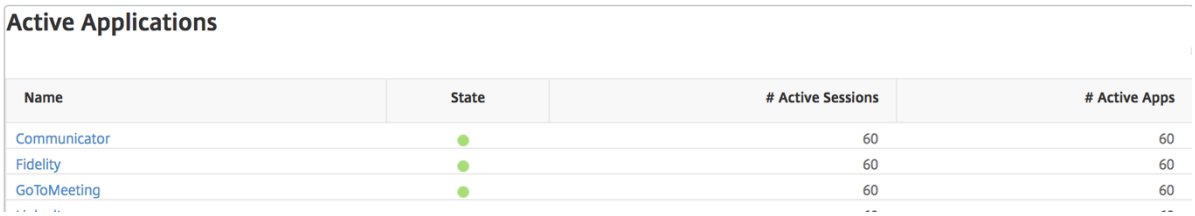
Metriken	Beschreibung
Name	Name der Citrix Virtual App.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual App-Sitzungen während des angegebenen Zeitintervalls.

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 über aktive Anwendungen

Metriken	Beschreibung
Name	Name der Citrix Virtual App.
Status	Zeigt den Status der Anwendung an: Grün-Aktiv, Rot-Inaktiv
Anzahl aktiver Sitzungen	Anzahl der aktiven Benutzersitzungen, die diese App während eines bestimmten Zeitintervalls verwenden.
Anzahlt aktiver Apps	Anzahl der aktiven Sitzungen für diese Anwendung.

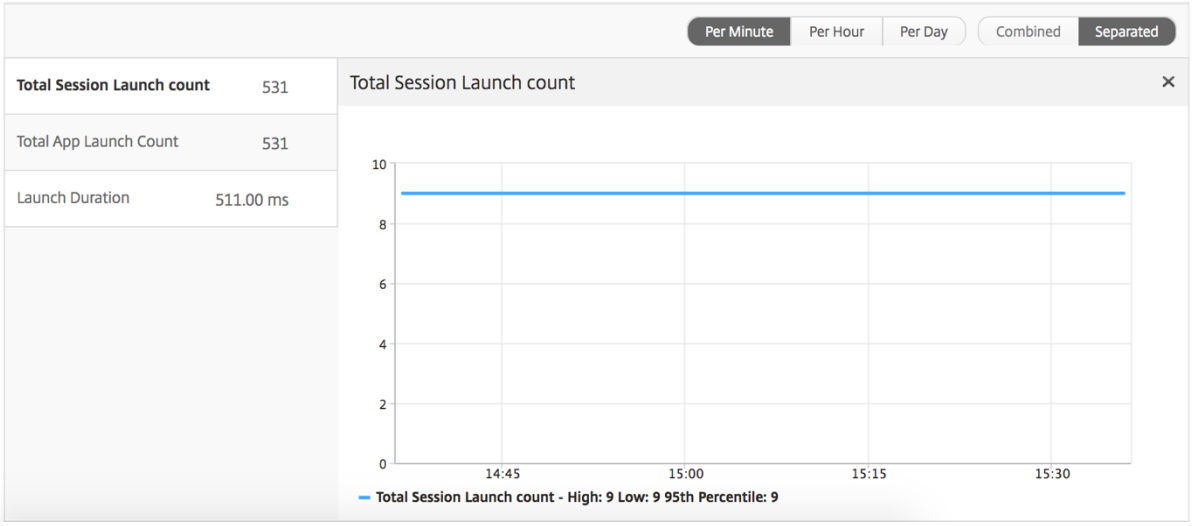


Bericht “Schwellenwert”

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* im ausgewählten Zeitraum als Anwendung ausgewählt wurde. Weitere Informationen finden Sie unter So erstellen Sie Schwellenwerte und Warnungen .

Liniendiagramm

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Dauer des Starts	Durchschnittliche Zeit zum Starten einer Anwendung.



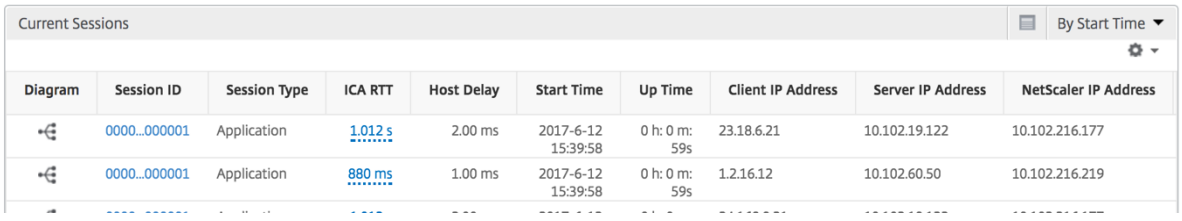
Bericht zu aktuellen Sitzungen

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 NetScaler passiert, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.

Metriken	Beschreibung
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Workspace-Typ —Citrix Windows Client usw.
Clientversion	Workspace-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway Benutzer/transparenter Modus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet 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 gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.

Metriken	Beschreibung
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde 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 Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zu Backend-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 NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler 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 NetScaler und dem Backend-Server aufgetreten ist.

Metriken	Beschreibung
Benutzername	Der Benutzername des Benutzers, der auf diese bestimmte Citrix Virtual App zugreift.
Sitzungs-ID	Eindeutige Kennung für die Citrix Virtual App-Sitzung.
Sitzungstyp	Wird “Anwendung”sein.
Status	Sitzungsstatus: Grün für aktiv, Rot für Inaktiv.
Maximale Verletzungslatenz	Der höchste Wert der L7-Latenz, wenn ein definierter Schwellenwert für ein festgelegtes Zeitintervall überschritten wird.
Durchschnittliche Latenz bei Sicherheitsverletzungen	Der Durchschnittswert der L7-Latenz, wenn sich das System in einem Zustand “L7-Latenz verletzt”befindet.
Anzahl von L7-Schwellenwertverletzungen	Gibt an, wie oft eine L7-Schwellenverletzung aufgetreten ist.
L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der NetScaler-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 NetScaler Gerät und der Citrix Virtual App beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.



Sitzungsansicht pro Anwendung

Die Session-Ansicht pro Anwendung zeigt Berichte für eine bestimmte ausgewählte Anwendungssitzung an.

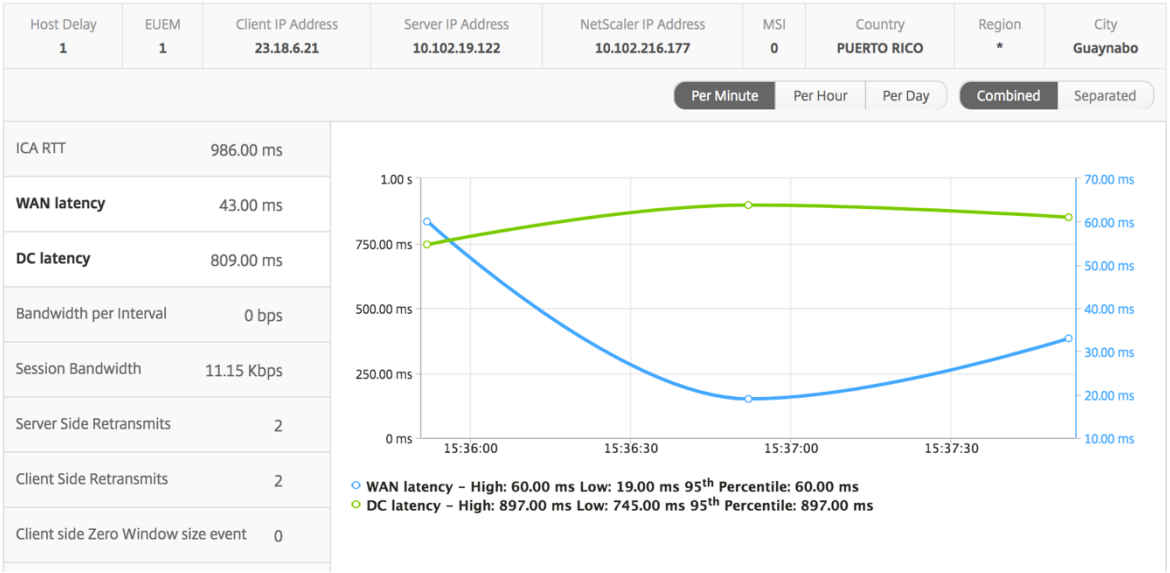
So zeigen Sie die Sitzungsberichte an:

1. Navigieren Sie zu **Gateway > HDX Insight > Anwendungen** .
2. Wählen Sie im Anwendungsübersichtsbericht einen bestimmten Benutzer aus.
3. Eine Sitzung aus dem Bericht über aktuelle Sitzungen ausgewählt.

Liniendiagramm

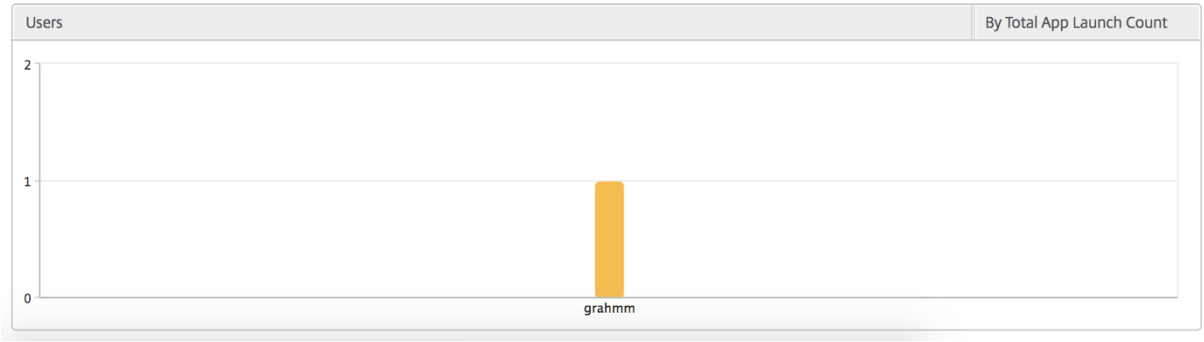
Metriken	Beschreibung
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
Serverseitiges Ereignis mit Zero Window-Größe	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zu Backend-Servern.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.

Metriken	Beschreibung
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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler 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.



Benutzerbalkendiagramm

Das Balkendiagramm des Benutzers stellt die Benutzer dar, die in dieser speziellen App angemeldet sind.



Desktop-View-Berichte und Metriken

February 5, 2024

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf Citrix Virtual Desktops.

So navigieren Sie zur Desktopansicht:

1. Navigieren Sie zu **Gateway > HDX Insight > Desktop** .

Übersichtsansicht

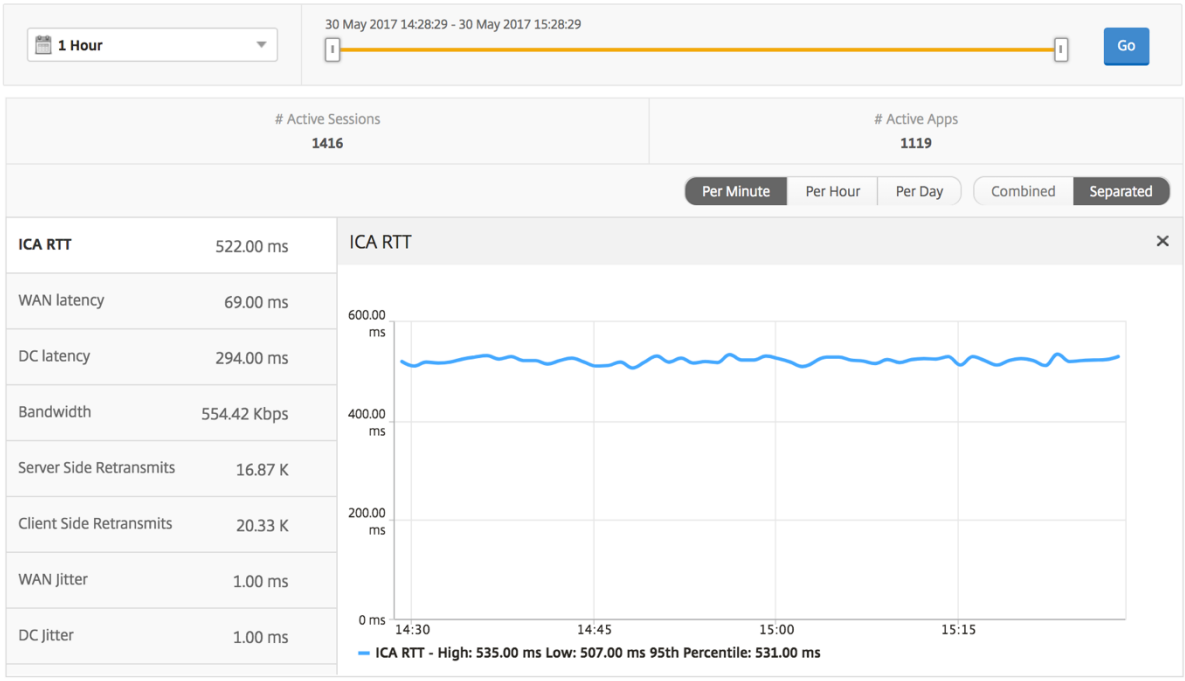
In der Zusammenfassungsansicht werden die Berichte für alle Citrix Virtual Desktops angezeigt, die während der ausgewählten Zeitleiste angemeldet sind.

Alle Metriken/Berichte, sofern nicht ausdrücklich erwähnt, haben die Werte, die ihnen für den ausgewählten Zeitraum entsprechen.

Liniendiagramm

Metriken	Beschreibung
Anzahl 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 Apps and Desktops gehostet wird.

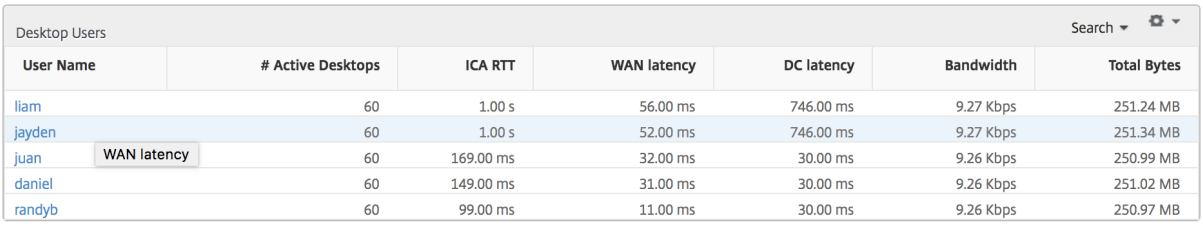
Metriken	Beschreibung
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler 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.



Desktop-Sammelbericht

Metriken	Beschreibung
Aktive Sitzungen	Gesamtzahl der aktiven Citrix Virtual Desktop-Sitzungen während eines bestimmten Zeitintervalls.
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 Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.

Metriken	Beschreibung
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.



Bericht “Schwellenwert”

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* in der ausgewählten Periode als Desktop ausgewählt wurde. Weitere Informationen finden Sie unter So erstellen Sie Schwellenwerte und Warnungen .

Pro Desktop-Ansicht

Die Ansicht pro Desktop bietet detaillierte Berichte zur Endbenutzererfahrung für einen ausgewählten Citrix Virtual Desktop.

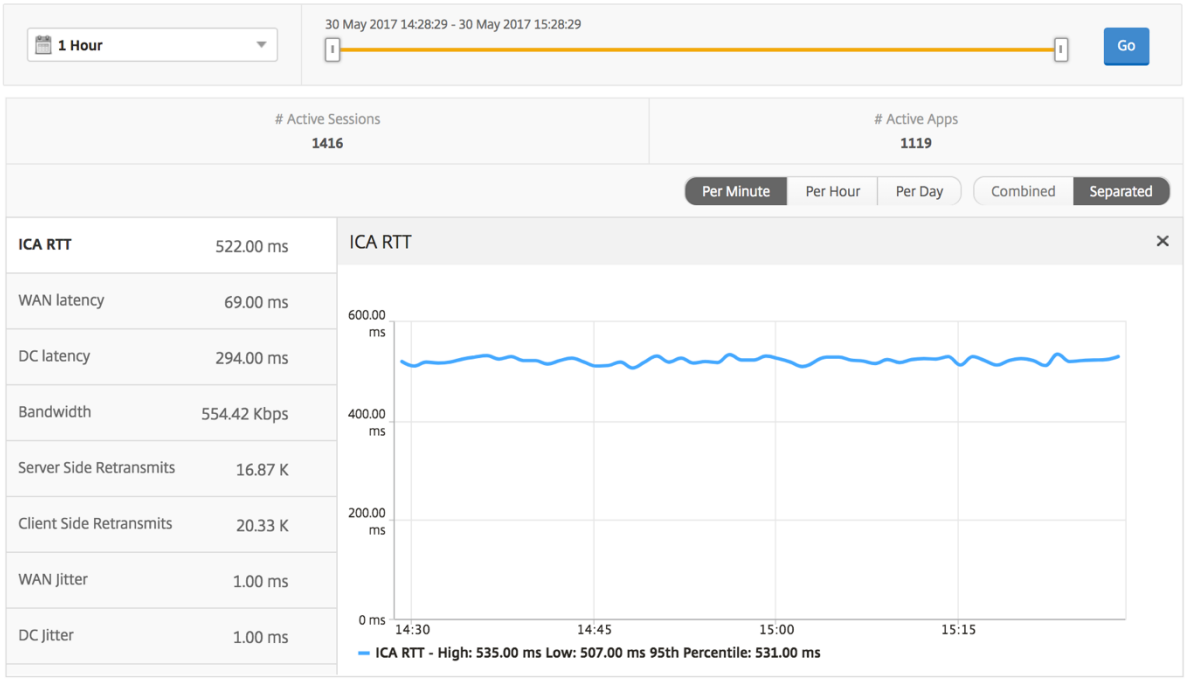
So navigieren Sie zur jeweiligen Desktop-Ansicht:

1. Navigieren Sie zu **Analytics > HDX Insight > Desktop**.
2. Wählen Sie im **Desktop-Zusammenfassungsberichteinen bestimmten Desktop**aus.

Liniendiagramm

Metriken	Beschreibung
Anzahl 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.

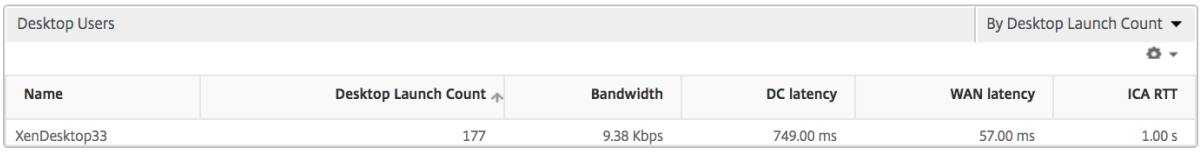
Metriken	Beschreibung
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler 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.



Bericht für Desktopbenutzer

Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zu Backend-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler 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 Apps and Desktops gehostet wird.



Benutzerdesktops Aktiv/Inaktiv Bericht

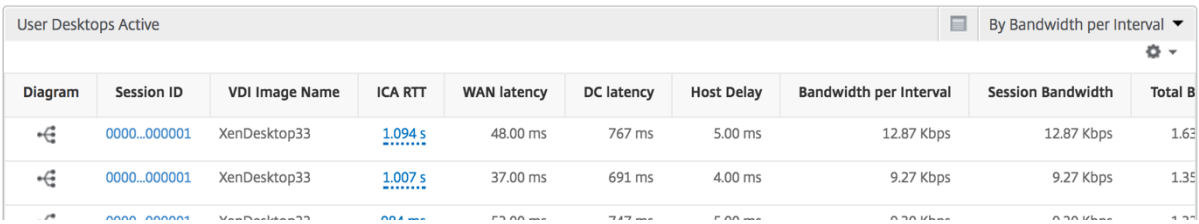
Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

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 durch die NetScaler ADCs geleitet wird, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Workspace-Typ —Citrix Windows Client usw.
Clientversion	Workspace-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.

Metriken	Beschreibung
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway Benutzer/transparenter Modus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet 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 gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die auf Citrix Virtual Apps bzw. Desktops gehostet werden.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zu Backend-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.

Metriken	Beschreibung
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler 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 NetScaler 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 **Gateway > HDX Insight > Desktop** .
2. Wählen Sie im **Desktopübersichtsbericht einen bestimmten Desktop**aus.
3. Wählen Sie eine Sitzung aus dem Bericht über aktuelle Sitzungen aus.

Zeitleistendiagramm

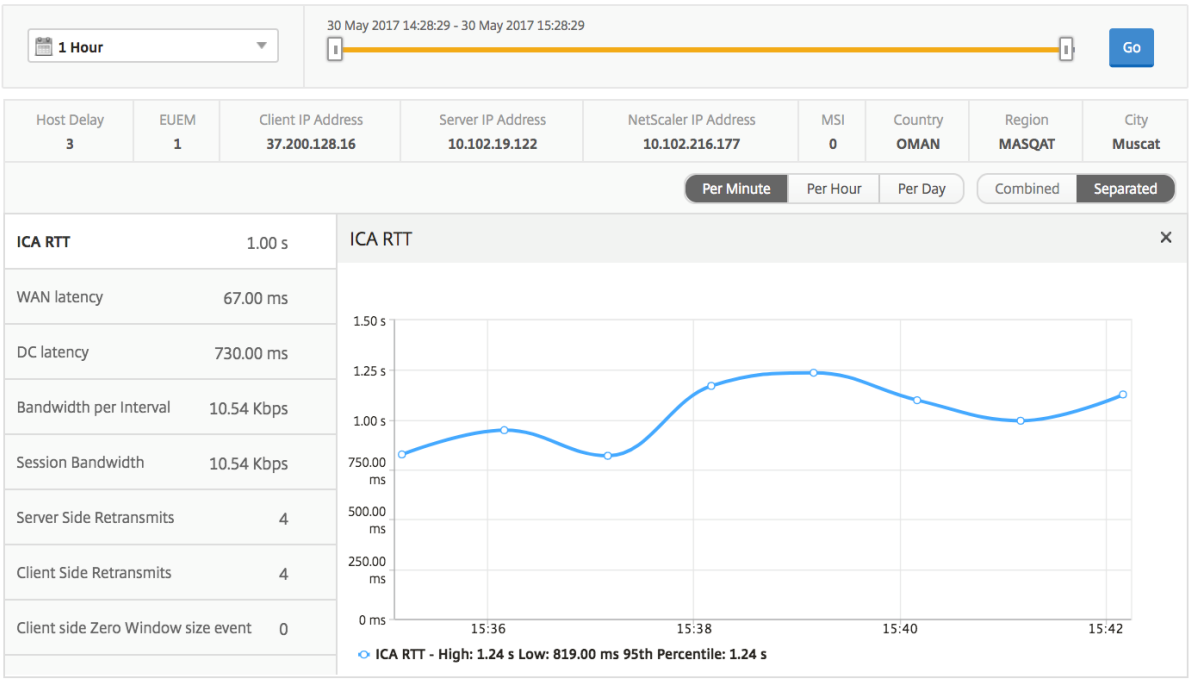
Die Sitzungsansicht pro Benutzer bietet Berichte für die Sitzung eines bestimmten ausgewählten Benutzers.

So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

1. Navigieren Sie zu **Gateway > HDX Insight > Benutzer** .
2. Wählen Sie im Abschnitt **Benutzerübersichtsbericht** einen bestimmten Benutzer aus.
3. Wählen Sie in der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** eine Sitzung aus.

Metriken	Beschreibung
Wiederverbindung der Sitzung	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App and Desktop-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 erlebt, die auf Citrix Virtual App bzw. Desktop gehostet werden.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zu Backend-Servern.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler und Backend-Server übertragenen Pakete.

Metriken	Beschreibung
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Backend-Server aufgetreten ist.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht 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.



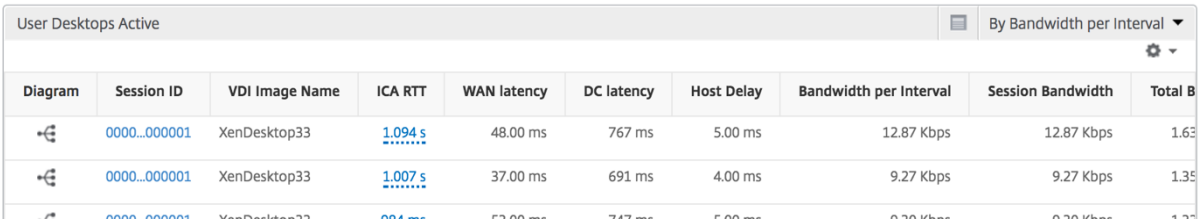
Bericht zu verwandten Desktopsitzungen

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 NetScaler passiert, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.

Metriken	Beschreibung
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Receiver-Typ: Citrix Windows Client und so weiter
Clientversion	Receiver-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway Benutzer/transparenter Modus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet 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 gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde 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 NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zu Backend-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 NetScaler und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler 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 NetScaler und dem Backend-Server aufgetreten ist.
VDI-Imagename	Name des Citrix Virtual Desktop, mit dem der Benutzer verbunden ist



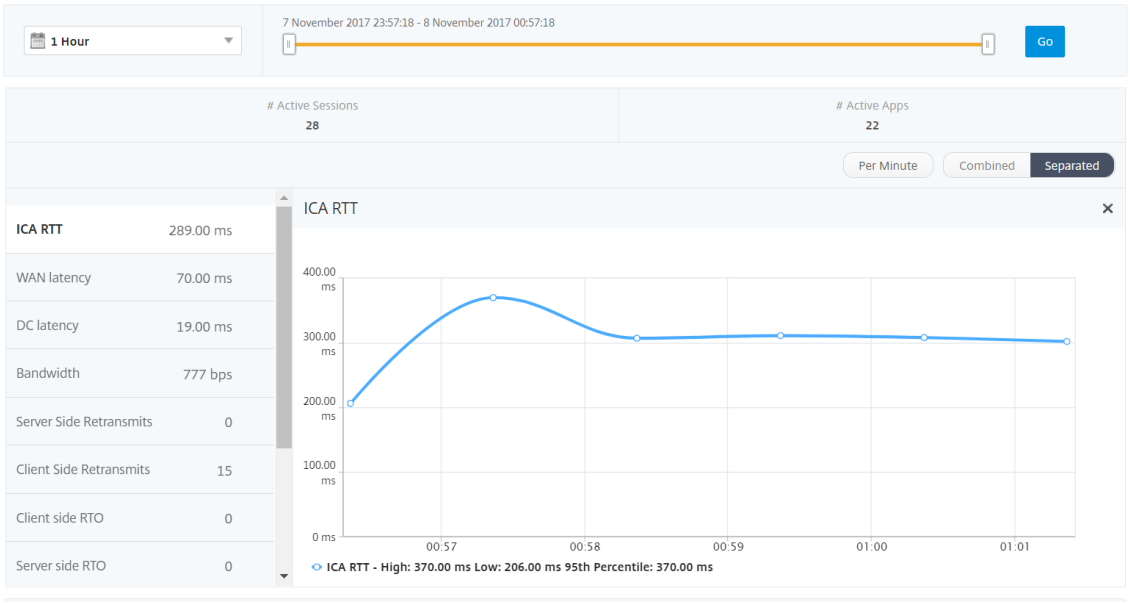
Berichte und Metriken der Benutzeransicht

February 5, 2024

Die Berichte und Metriken in dieser Ansicht werden pro Citrix Virtual Apps und Desktop-Benutzer angezeigt.

So navigieren Sie zur Ansicht Benutzer:

1. Navigieren Sie zu **Gateway > HDX Insight > Benutzer**



Übersichtsansicht

In der Zusammenfassungsansicht werden die Berichte für alle Benutzer angezeigt, die sich während der ausgewählten Zeitleiste angemeldet haben. Alle Metriken/Berichte in dieser Ansicht zeigen die ihnen entsprechenden Werte für den ausgewählten Zeitraum an, sofern nicht anders angegeben.

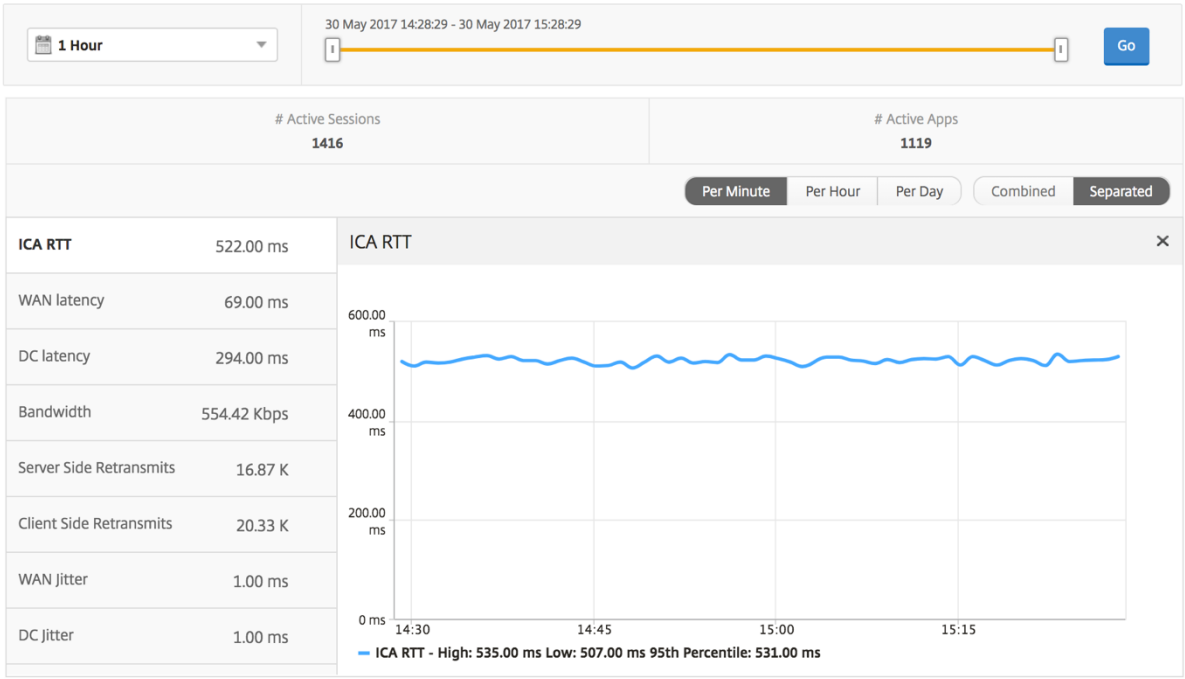
So ändern Sie den ausgewählten Zeitraum:

1. Verwenden Sie die Zeitraumeliste oder den Zeitschieberegler, um das gewünschte Zeitintervall einzustellen.
2. Klicken Sie auf **Go**.

Liniendiagramm

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App and Desktop-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 NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis hin zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.

Metriken	Beschreibung
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.
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.



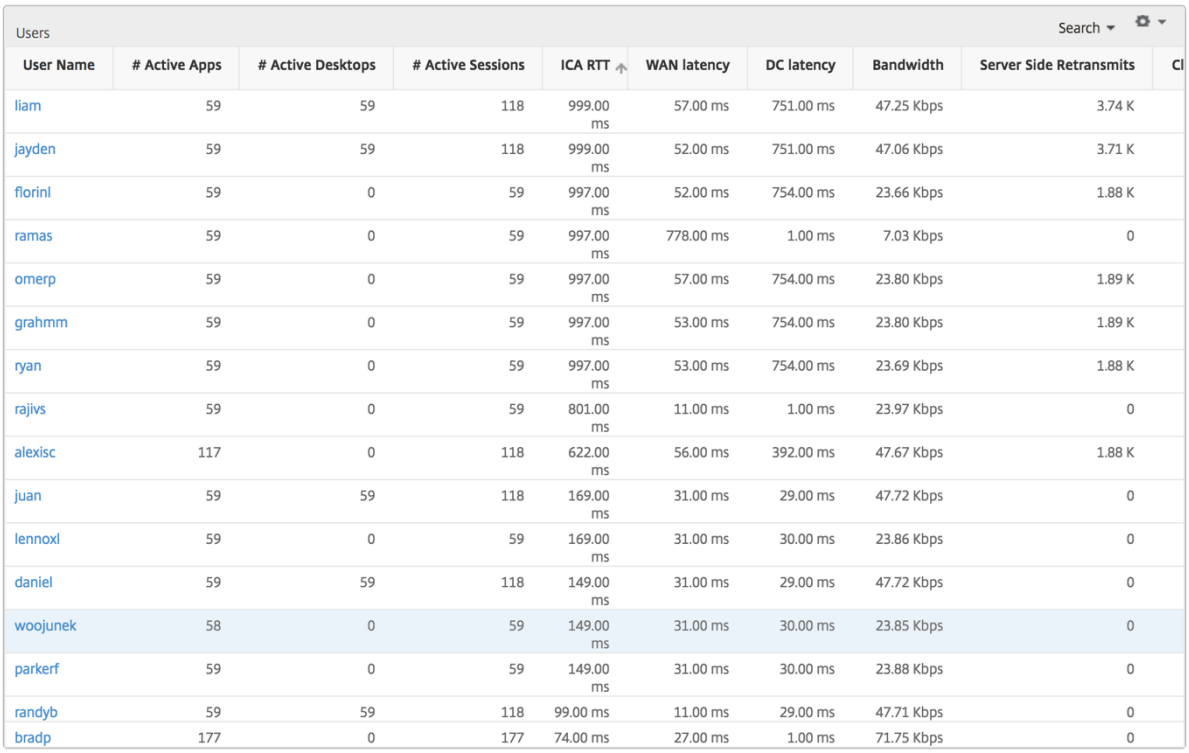
Bericht “Benutzerzusammenfassung”

Im Folgenden finden Sie die Metriken, die für diesen Bericht spezifisch sind.

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App and Desktop-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 NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis hin zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.
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.

Metriken	Beschreibung
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.



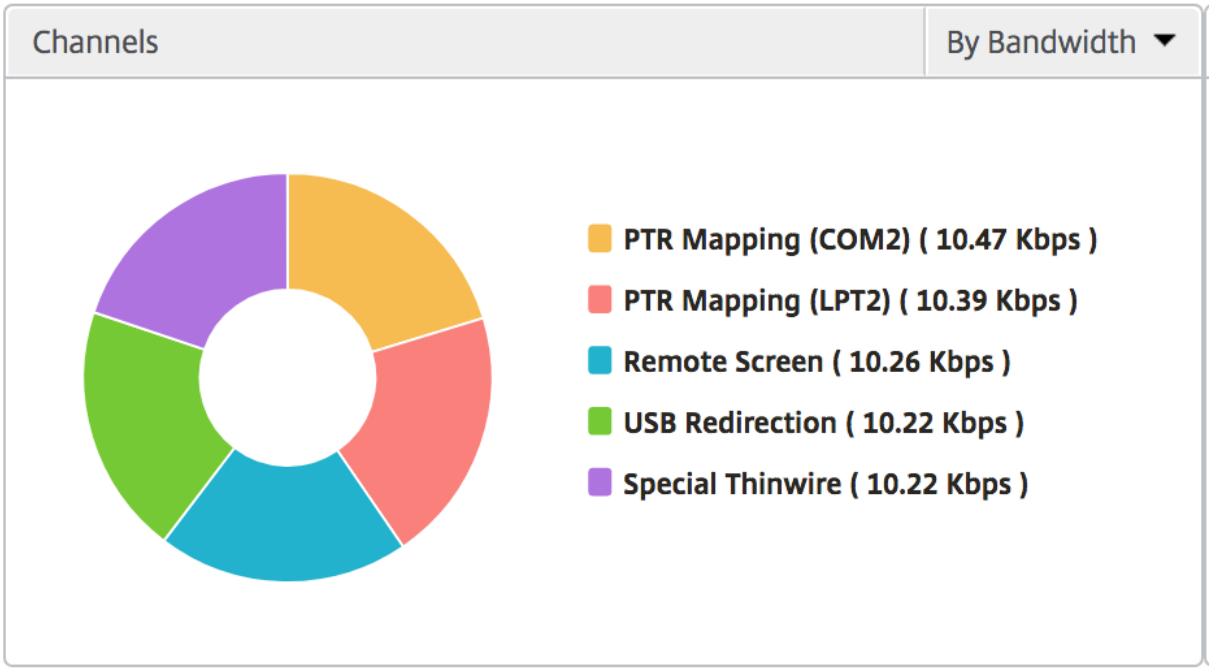
Users

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	

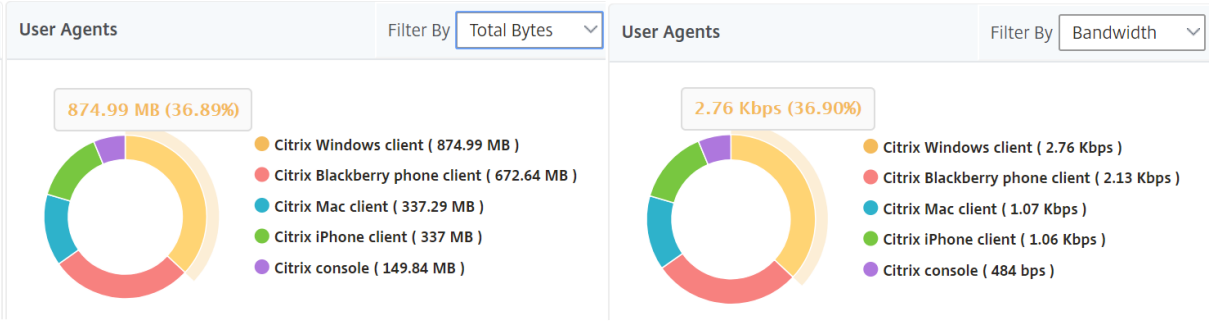
Kanäle

Kanäle stellen die Gesamtbandbreite oder die Gesamtzahl der von jedem virtuellen ICA-Kanal verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Benutzer-Agenten

Benutzeragenten stellen die gesamte Bandbreite/Gesamtanzahl der von jedem Endpunkt verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Anzahl der Schwellenwertverstöße

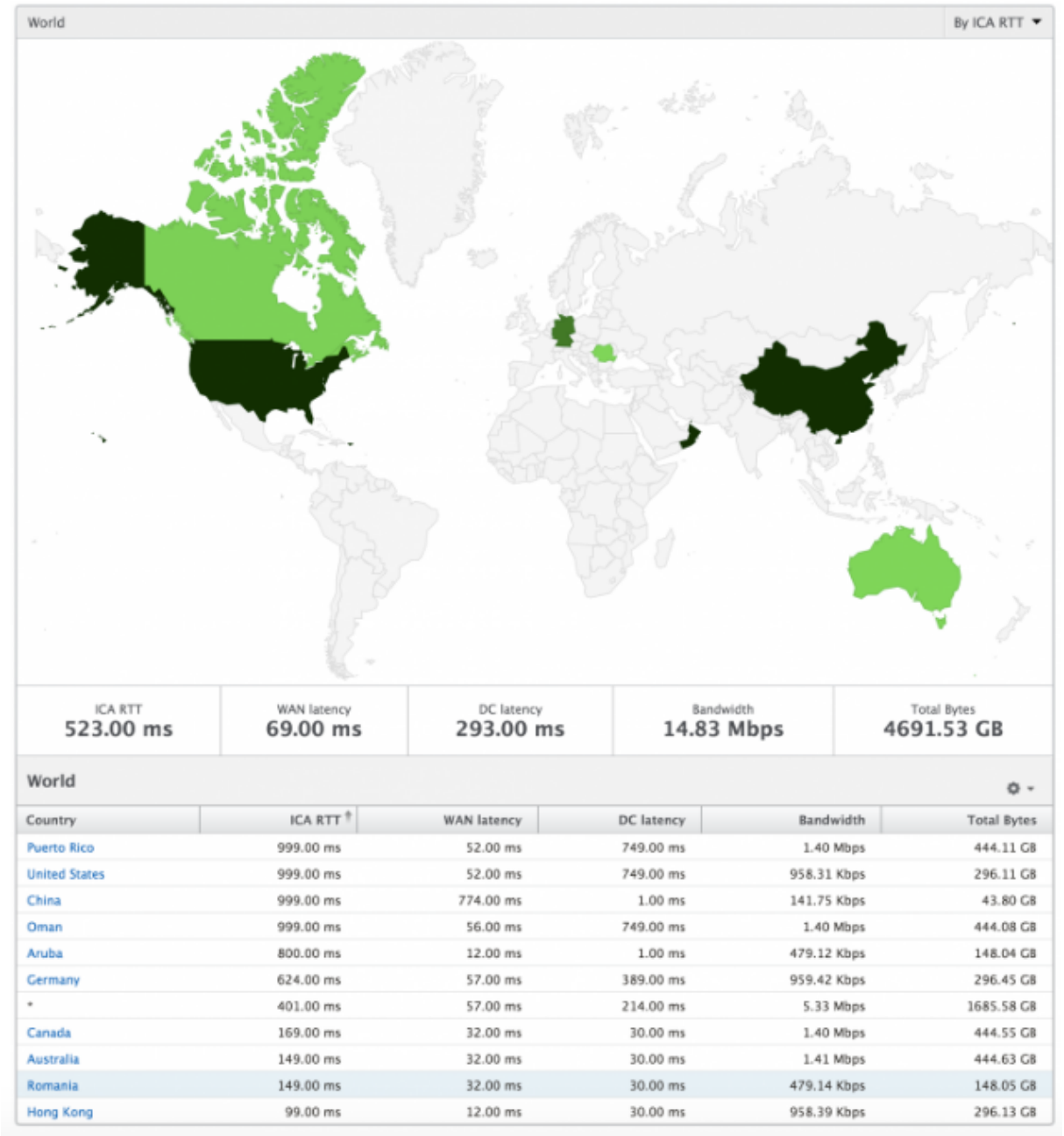
Die Metriken für die Anzahl der Schwellenwertverstöße stellen die Anzahl der Schwellenwerte dar, die im ausgewählten Zeitraum überschritten wurden. Weitere Informationen finden Sie unter So erstellen Sie Schwellenwerte und Warnmeldungen.

Weltkarte

Mit der Weltkartenansicht in HDX Insight können Administratoren die historischen und aktiven Benutzerdetails aus geografischer Sicht anzeigen. 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 einen weiteren Drilldown durchführen, um Informationen nach Stadt und Bundesland anzuzeigen. Ab NetScaler ADM Version 12.0 und höher können Sie einen Drilldown zu Benutzern 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 eines bestimmten Benutzers:

1. Navigieren Sie zu **Gateway > HDX Insight > Benutzer** .
2. Wählen Sie im Übersichtsbericht Benutzer einen bestimmten Benutzer aus.

Liniendiagramm

Das Liniendiagramm zeigt eine Zusammenfassung aller Metriken für den ausgewählten Benutzer während des ausgewählten Zeitraums an.

Bericht über aktuelle/abgeschlossene Sitzungen

Dieser Bericht bezieht sich auf 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 durch die NetScaler ADCs geleitet wird, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Workspace-Typ —Citrix Windows Client usw.
Clientversion	Workspace-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.

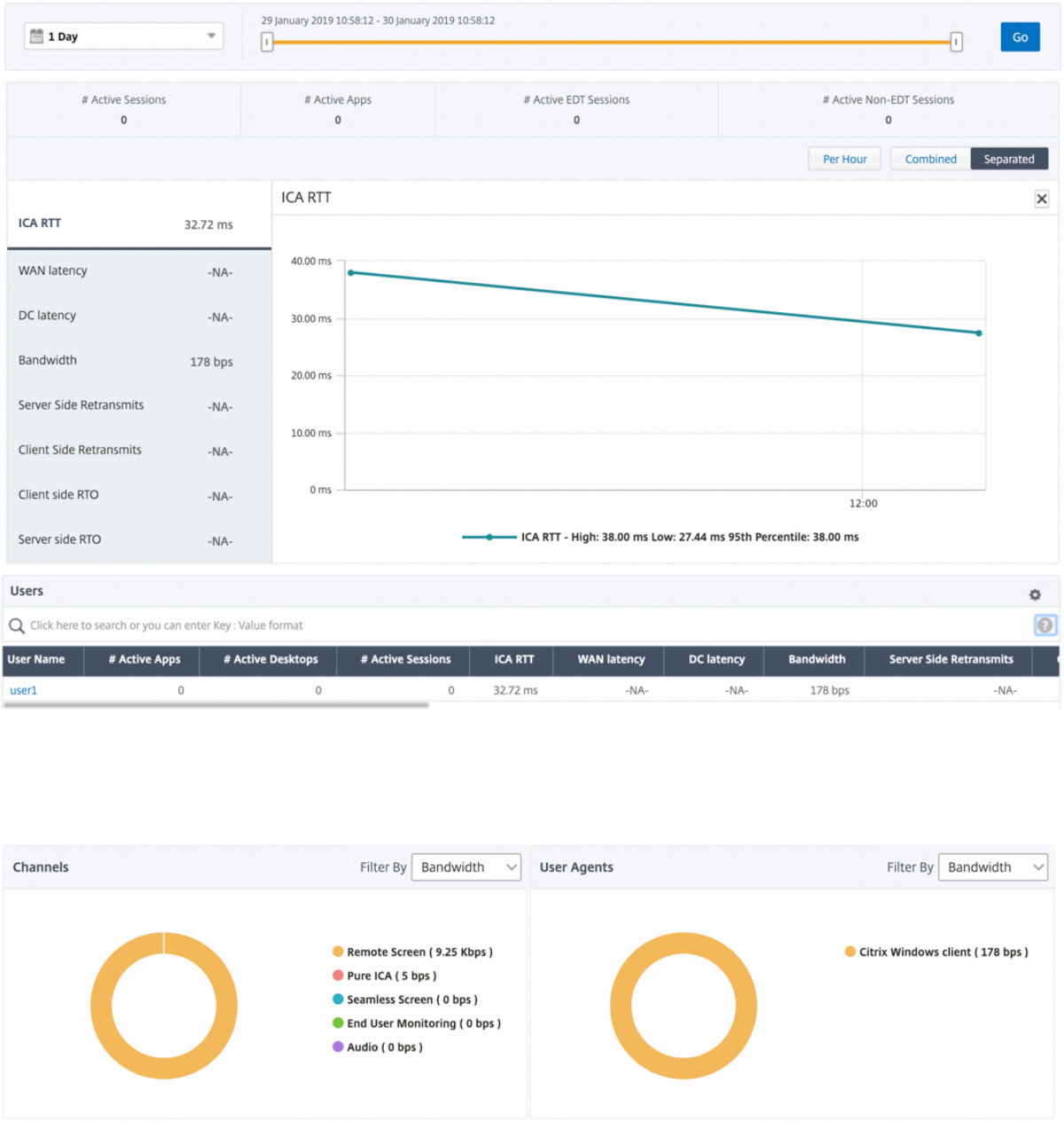
Metriken	Beschreibung
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway Benutzer/transparenter Modus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet 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 gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde 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 NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis hin zu Backend-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.

Metriken	Beschreibung
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler 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	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.

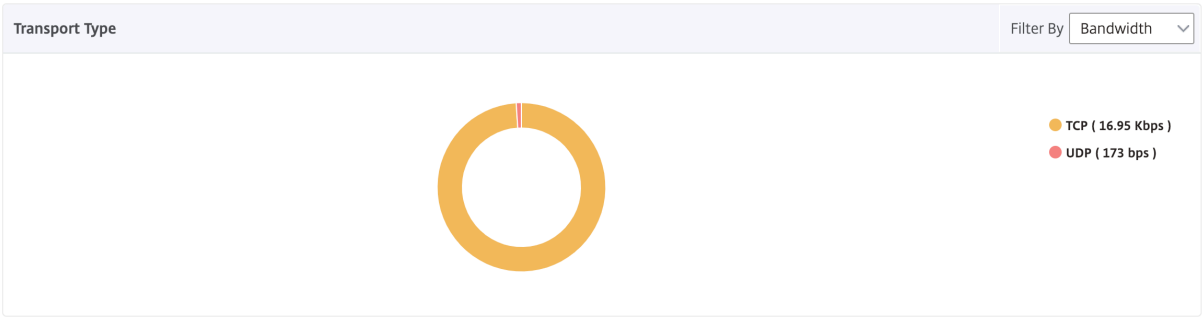
Unterstützung für EDT in HDX Insight

NetScaler Application Delivery Management (ADM) unterstützt jetzt Enlightened Data Transport (EDT) zur Anzeige von Analysen für HDX Insight. Das heißt, ADM unterstützt jetzt sowohl das UDP- als auch das TCP-Protokoll. Die EDT-Unterstützung für NetScaler Gateway gewährleistet eine hochauflösende Benutzererfahrung virtueller Desktops während der Sitzung für Benutzer, die Citrix Workspace ausführen.

HDX Insight zeigt jetzt die Anzahl der EDT-Sitzungen und Nicht-EDT-Sitzungen als Teil des Berichts über 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, Rückübertragungen und RTOs. Einige dieser Metriken sind für Benutzer mit EDT-Sitzungen nicht verfügbar, da sie derzeit anhand des TCP-Stacks berechnet werden. Daher erscheinen sie als “NA”.

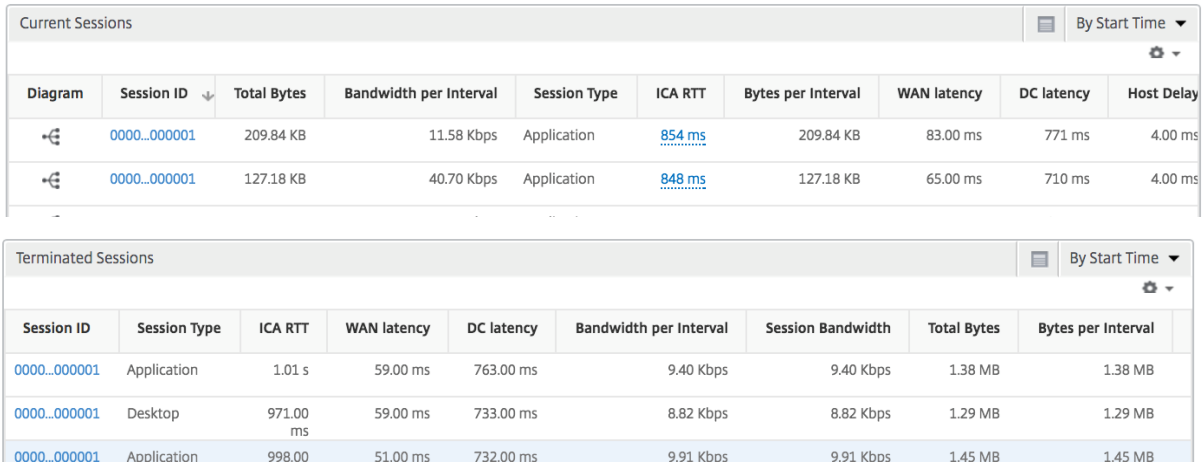


Es wurde ein neues Donutdiagramm eingeführt, mit dem Sie die vom Benutzer verbrauchte Bandbreite und die Gesamtzahl der Bytes basierend auf dem von den Benutzern verwendeten Protokolltyp sehen können.



HDX Insight Metriken, die ab NetScaler ADM 12.0 und höher verfügbar sind:

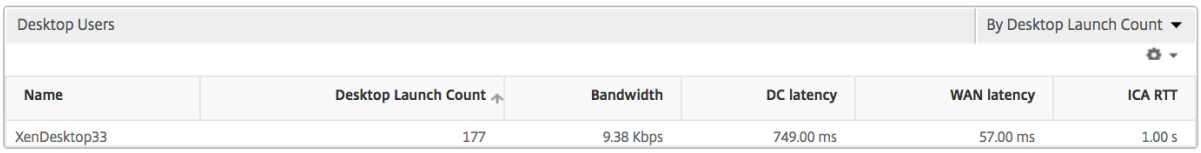
L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der NetScaler-Instanz beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.
L7 Serverseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem NetScaler 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 definierter Schwellenwert für ein festgelegtes Zeitintervall überschritten wird.
Durchschnittliche Latenz bei Sicherheitsverletzungen	Der Durchschnittswert der L7-Latenz, wenn sich das System in einem Zustand “L7-Latenz verletzt”befindet.
Anzahl von L7-Schwellenwertverletzungen	Gibt an, wie oft eine L7-Schwellenverletzung aufgetreten ist.



Desktopbenutzer

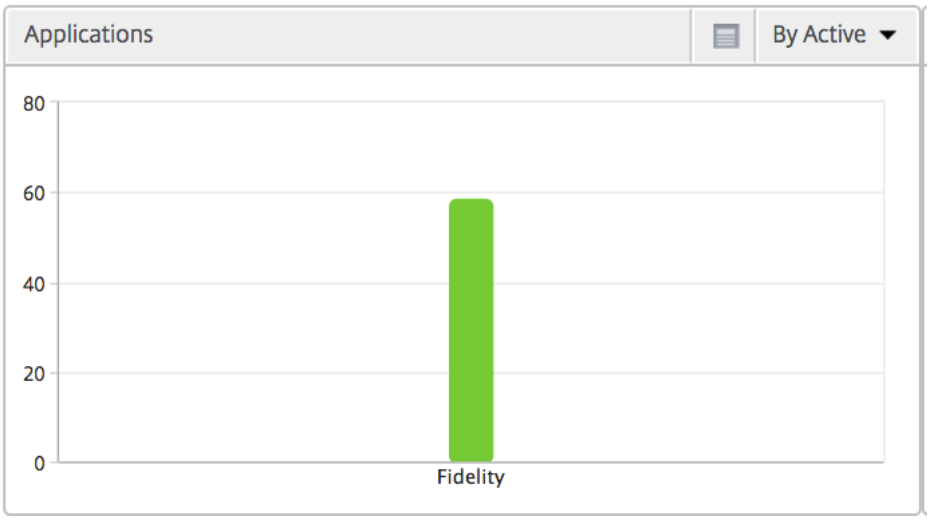
Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis hin zu Backend-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler 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.



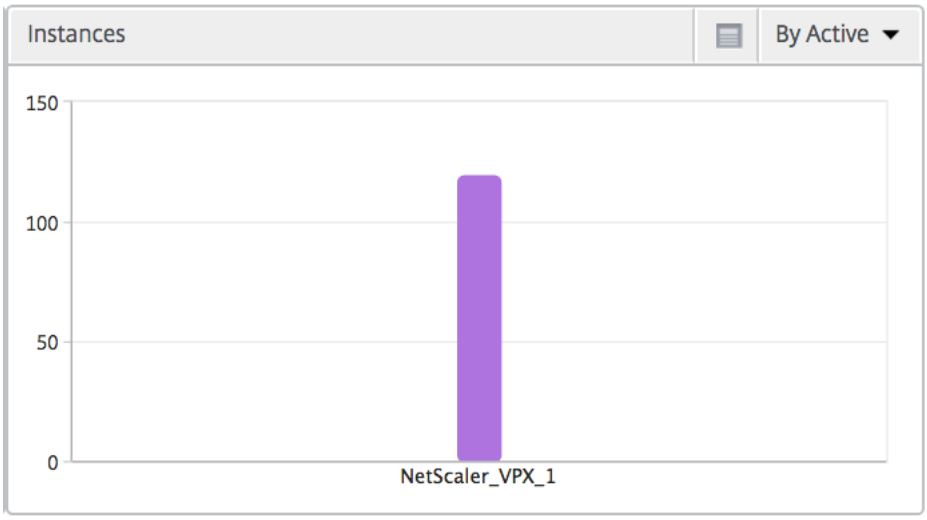
Anwendungen

Ein Balkendiagramm, das Apps sortiert nach Aktiv, Gesamtzahl der Sitzungsstarts, Gesamtanzahl des App-Starts und Startdauer darstellt.



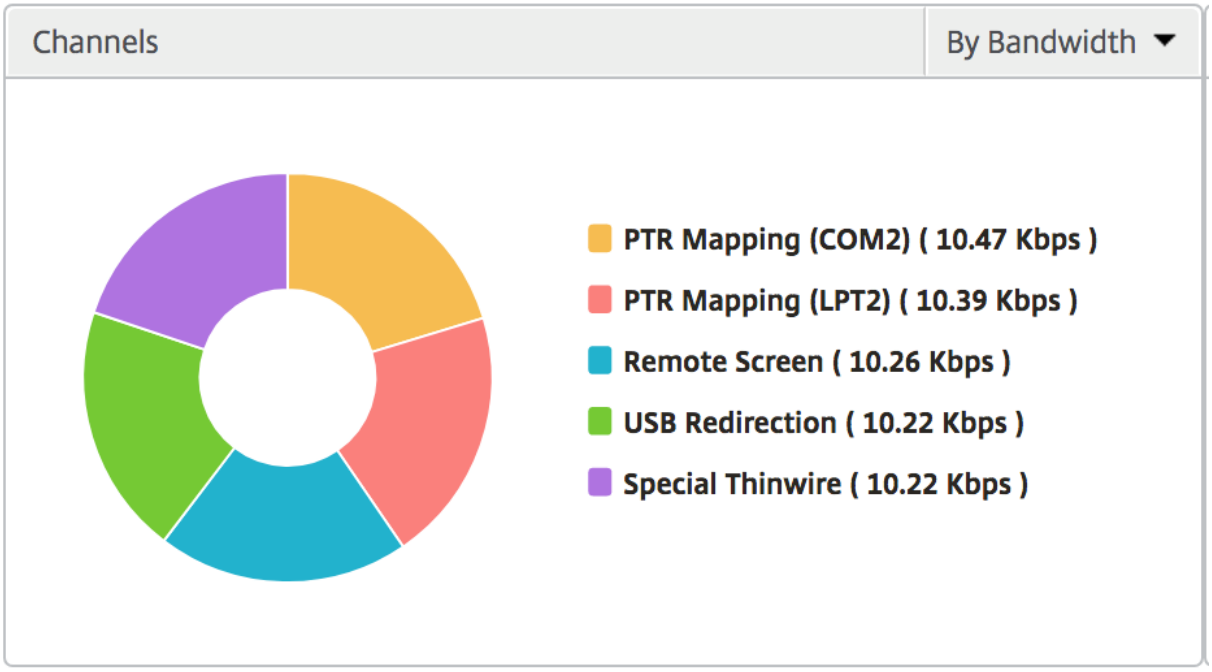
Instanzen

Ein Balkendiagramm, das NetScaler Instanzen darstellt, sortiert nach Active und insgesamt Apps



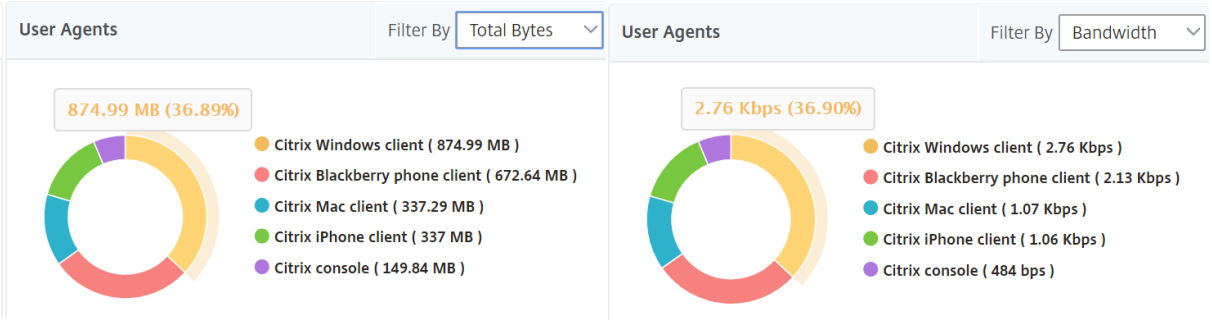
Kanäle

Kanäle stellen die Gesamtbandbreite oder die Gesamtzahl der von jedem virtuellen ICA-Kanal verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Benutzer-Agenten

Benutzeragenten stellen die gesamte Bandbreite/Gesamtanzahl der von jedem Endpunkt verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Sitzungsansicht pro Benutzer

Die Sitzungsansicht pro Benutzer bietet Berichte für die Sitzung eines bestimmten ausgewählten Benutzers.

So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

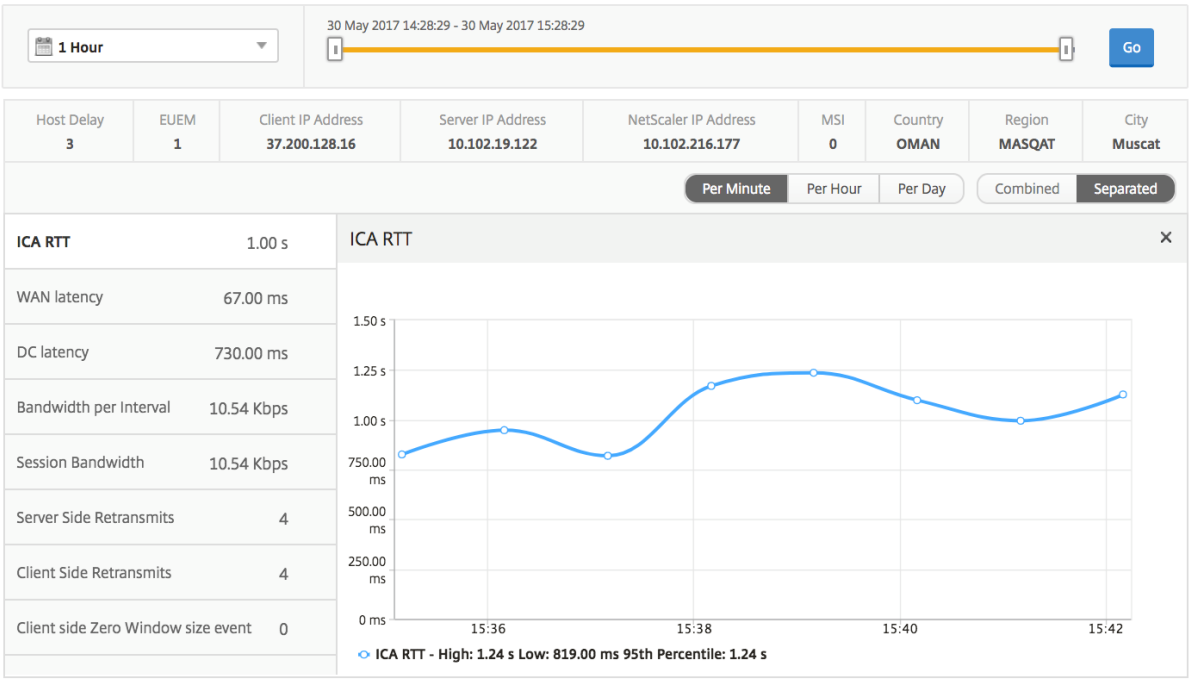
1. Navigieren Sie zu **Gateway > HDX Insight > Benutzer** .
2. Wählen Sie im Abschnitt **Benutzerübersichtsbericht** einen bestimmten Benutzer aus.

3. Wählen Sie in der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** eine Sitzung aus.

Zeitleistendiagramm

Metriken	Beschreibung
Wiederverbindung der Sitzung	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App and Desktop-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 NetScaler bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis hin zu Backend-Servern.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. 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	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.

Metriken	Beschreibung
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht 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.

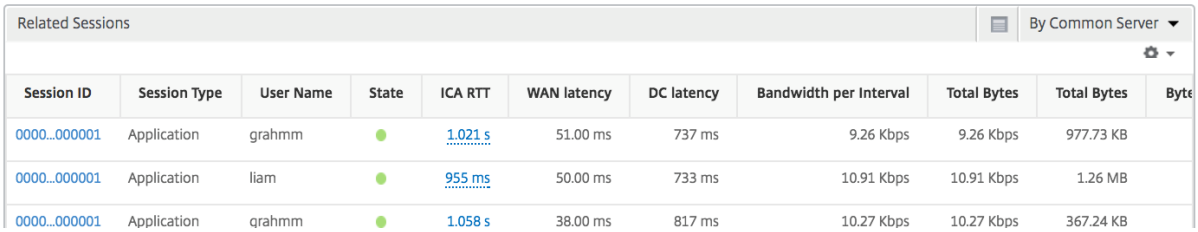


Aktive Anwendung

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.

Verwandte Sitzungen

Im Abschnitt “Sessions”werden die zugehörigen Sitzungen der Sitzungen des ausgewählten Benutzers angezeigt. Die Beziehung kann als gemeinsame Server oder gemeinsames NetScaler ausgewählt werden.



Session ID	Session Type	User Name	State	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Total Bytes	Total Bytes	Byte
0000...000001	Application	grahmm		1.021 s	51.00 ms	737 ms	9.26 Kbps	9.26 Kbps	977.73 KB	
0000...000001	Application	liam		955 ms	50.00 ms	733 ms	10.91 Kbps	10.91 Kbps	1.26 MB	
0000...000001	Application	grahmm		1.058 s	38.00 ms	817 ms	10.27 Kbps	10.27 Kbps	367.24 KB	

Instanzansichtsberichte und -metriken

February 5, 2024

Die Berichte und Metriken in der Instanzansicht konzentrieren sich auf die NetScaler Instanzen.

So navigieren Sie zur Instanzansicht:

1. Navigieren Sie zu **Gateway > HDX Insight > Instanzen** .

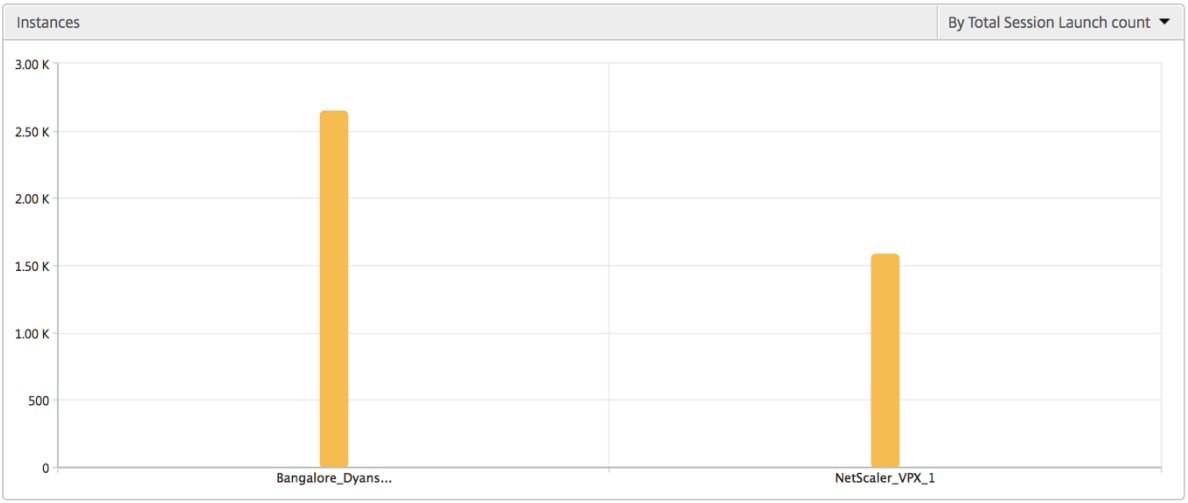
Instanz-Zusammenfassungsansicht

Diese Ansicht wird als Zusammenfassungsansicht bezeichnet, da sie die Berichte für alle NetScaler Instanzen anzeigt, die NetScaler ADM hinzugefügt werden.

Alle Metriken/Berichte haben, sofern nicht ausdrücklich erwähnt, die ihnen entsprechenden Werte für den ausgewählten Zeitraum.

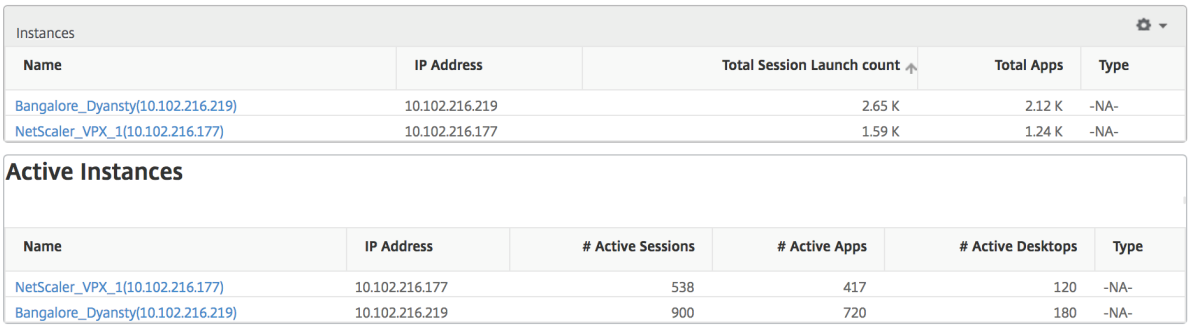
Instanz-Balkendiagramm

Dieses Diagramm zeigt die Instanz im Vergleich zur Gesamtzahl der Sitzungsstarts und der Gesamtzahl der Apps an, die in der Liste oben rechts auf der Diagrammfläche ausgewählt werden können.



Übersichtsbericht “Instanz/Aktive Instanzen”

Metriken	Beschreibung
Name	Hostname der NetScaler-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	–


Instances

Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

Bericht “Schwellenwert”

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 So erstellen Sie Schwellenwerte und Warnungen .

Übersprungene Flows

Ein übersprungener Flow ist ein Datensatz, der die Parsing ICA-Verbindung übersprungen hat. Dies kann verschiedene Gründe haben, z. B. die Verwendung nicht unterstützter Versionen von Citrix Virtual Apps and Desktops, nicht unterstützte Versionen von Workspace oder Workspace-Typ usw. Diese Tabelle zeigt die IP-Adresse und die Anzahl der übersprungenen Flows. Diese Arbeitsbereiche dürfen nicht Teil von Arbeitsbereichen auf der Whitelist sein. Daher werden diese Sitzungen von der Überwachung übersprungen.

See **Error! Hyperlinkverweis ist nicht gültig** für weitere Details zu Problemen im Zusammenhang mit der ICA-Analyse.

Skipped Flows

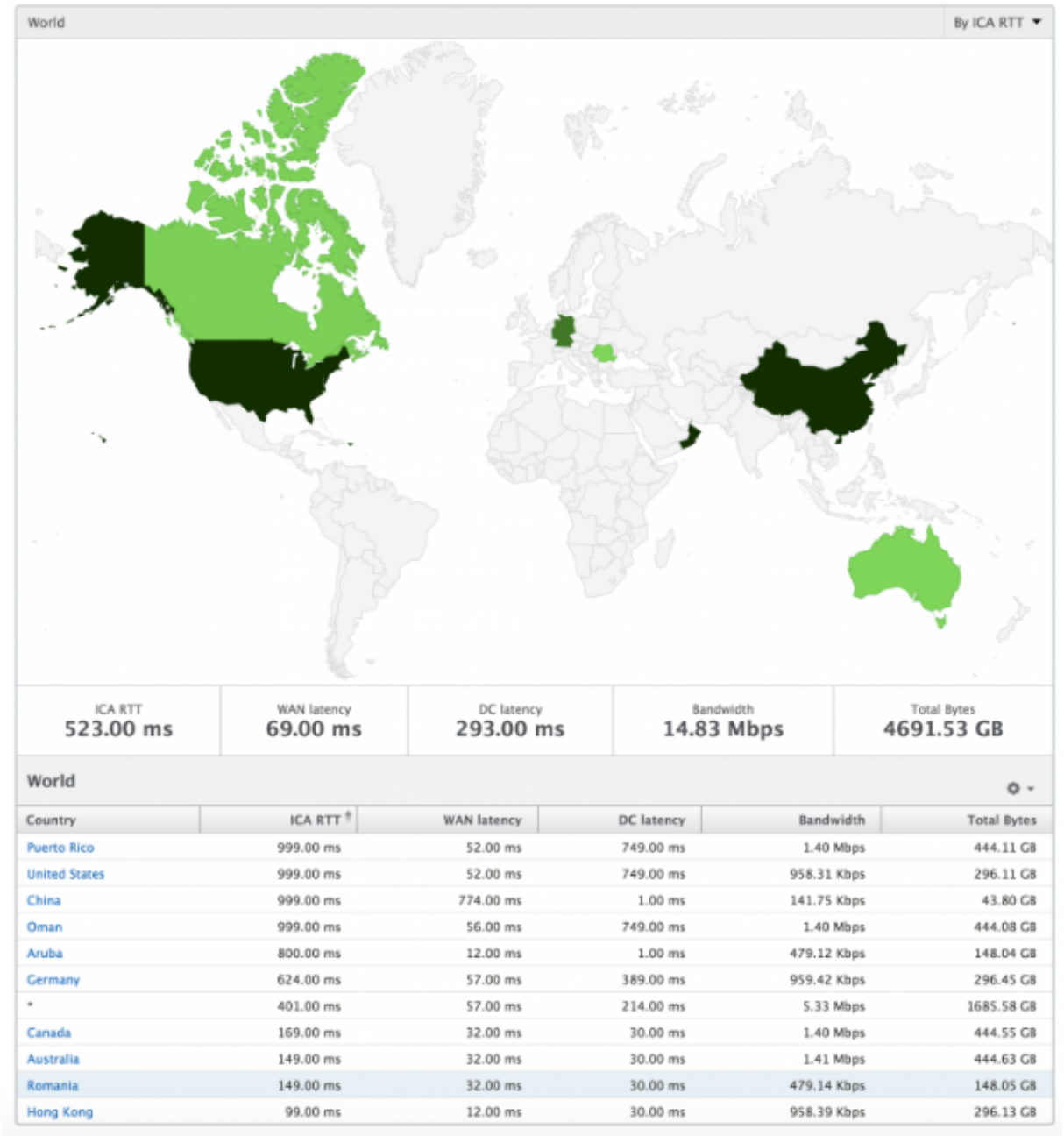
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

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 NetScaler Version 12.0 und höher können Sie Benutzer aufschlüsseln, 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 Instanz

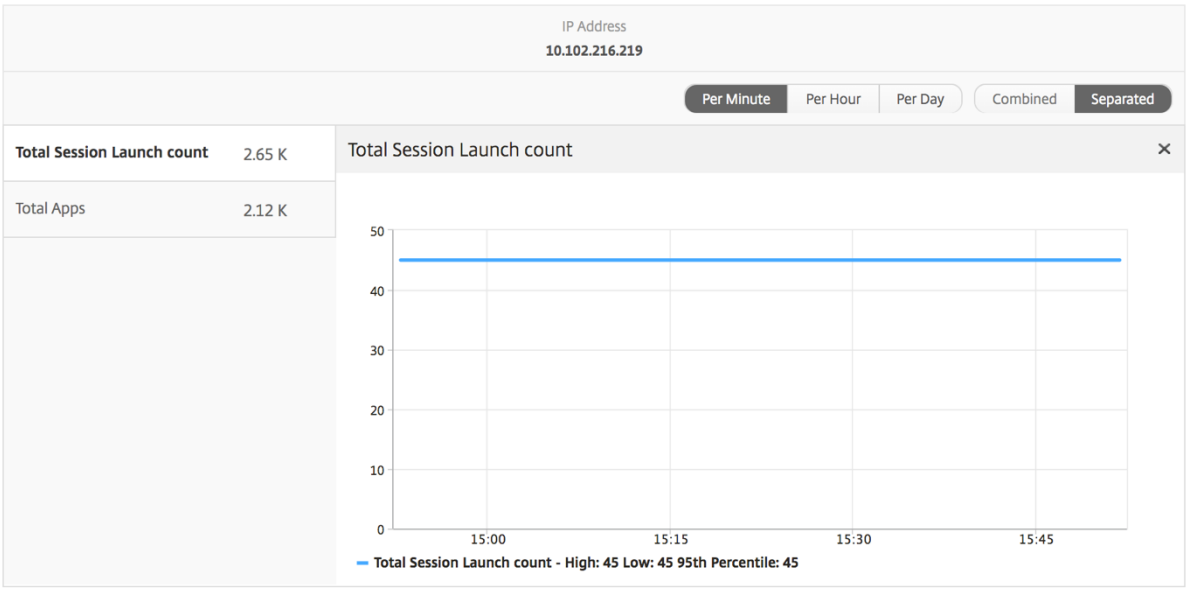
Die Ansicht pro Instanz bietet detaillierte Berichte über die Benutzererfahrung für eine bestimmte ausgewählte NetScaler Instanz.

So navigieren Sie zur Instanzansicht:

1. Navigieren Sie zu **Gateway > HDX Insight > Instanzen** .
2. Wählen Sie in der **Auswertung** “**Instanzübersicht**” eine bestimmte Instanz aus.

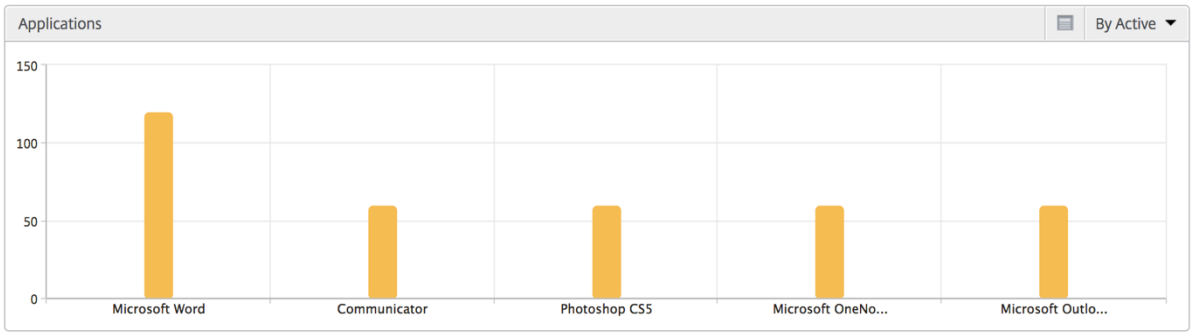
Liniendiagramm

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.



Balkendiagramm für Anwendungen

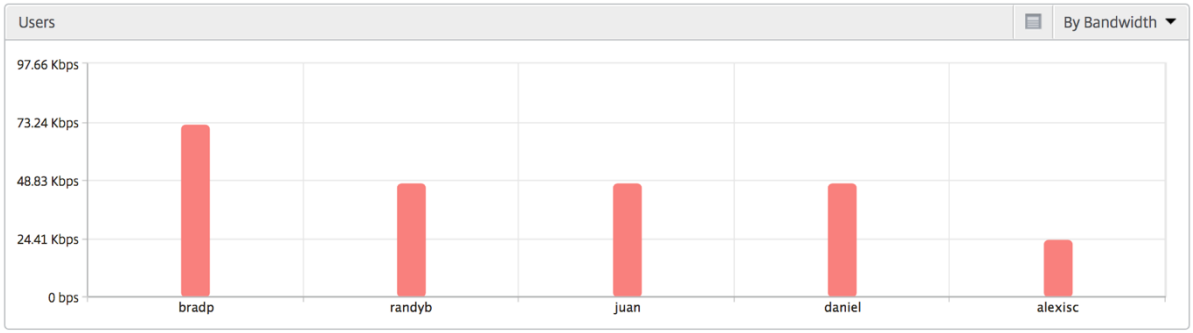
Zeigt die 5 wichtigsten Anwendungen basierend auf den folgenden Kriterien an: nach aktiven Apps, Gesamtzahl der Sitzungsstarts, Gesamtzahl der App-Startstarts oder Startdauer.



Balkendiagramm “Benutzer”

Das Balkendiagramm “Benutzer”zeigt die fünf wichtigsten Benutzer anhand der folgenden Kriterien an:

- Bandbreite
- WAN-Latenz
- DC-Latenz
- ICA RTT

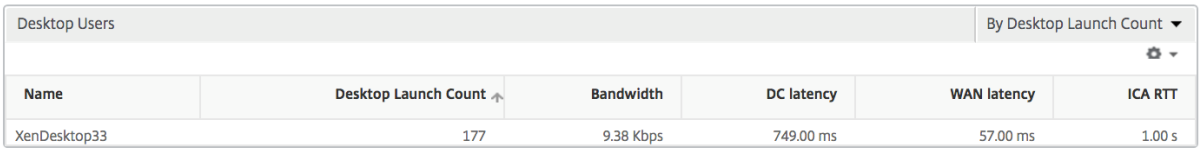


Bericht für Desktopbenutzer

Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.

Metriken	Beschreibung
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler bis zu Backend-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler 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.

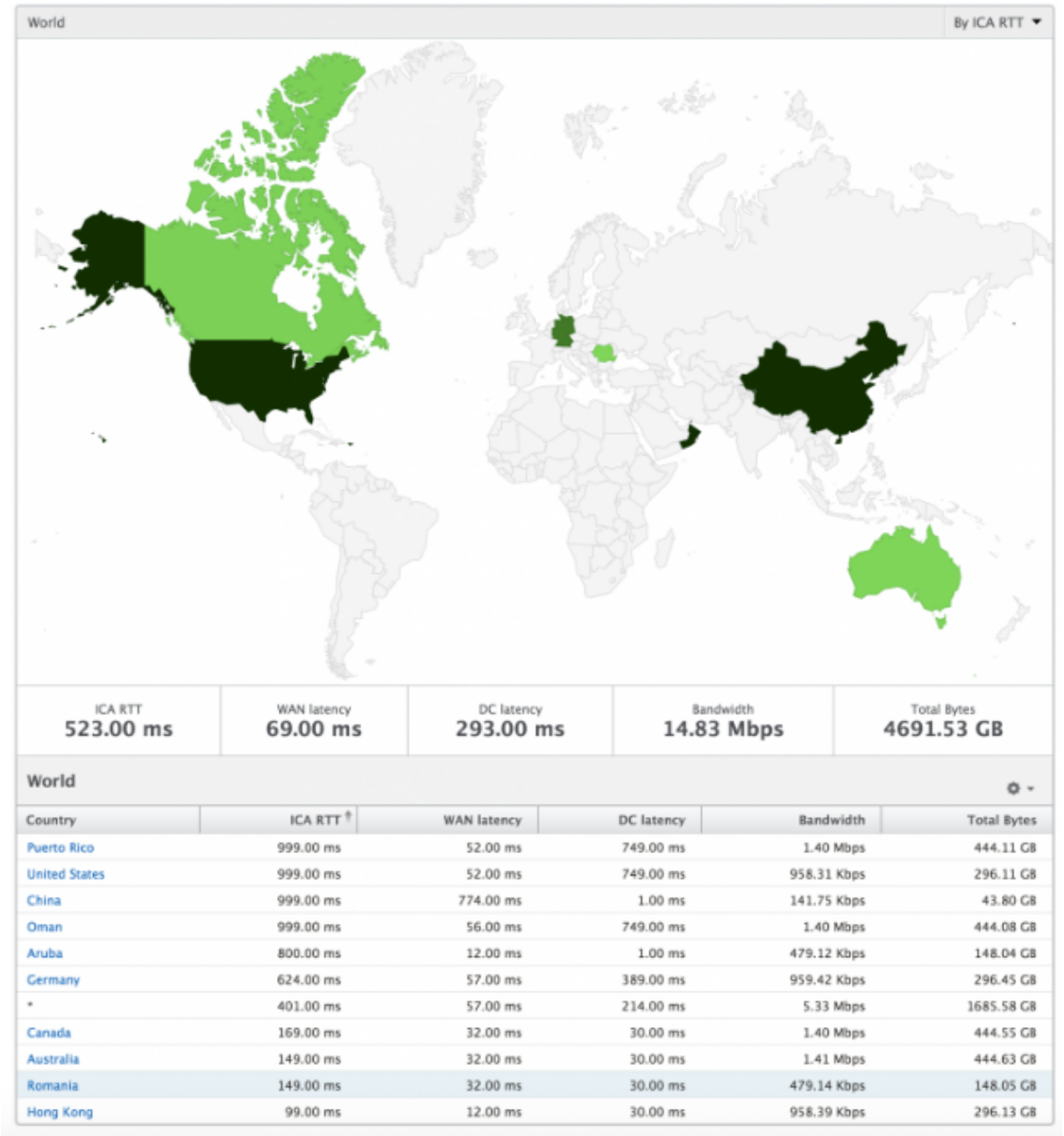


Weltansicht

Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die historischen und aktiven Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltsicht auf das System haben, einen Drilldown zu einem bestimmten Land und auch weiter in Städte hineinfahren, indem sie auf die Region klicken. Die Administratoren können weitere Informationen nach Stadt und Bundesstaat anzeigen. Ab NetScaler ADM Version 12.0 und höher können Sie einen Drilldown zu Benutzern 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

Lizenzansichtsberichte und -metriken

February 5, 2024

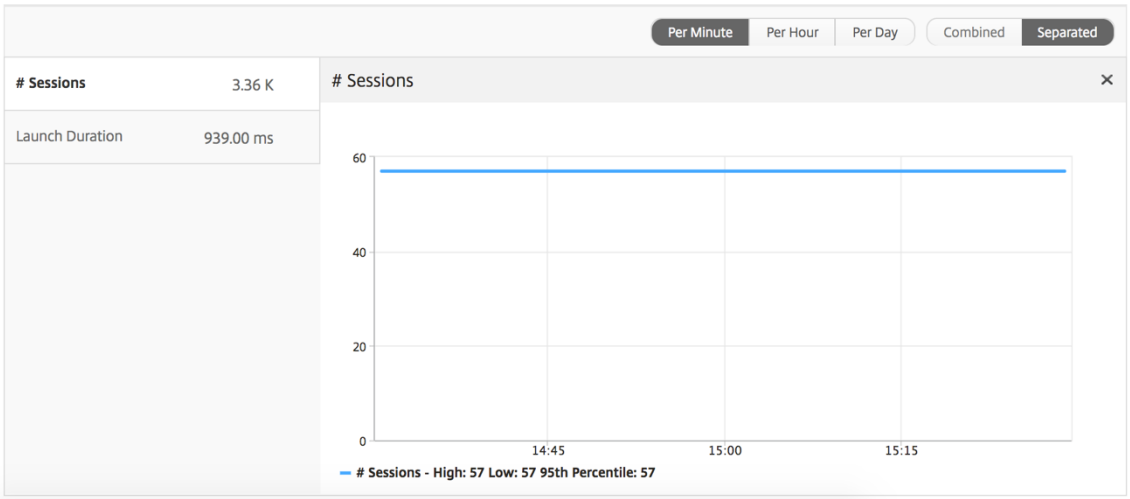
Die Lizenzansicht enthält Details zu den NetScaler Gateway-Lizenzinformationen.

So navigieren Sie zur Lizenzansicht:

1. Navigieren Sie zu **Gateway > HDX Insight > Lizenzen** .

Liniendiagramm

Metriken	Beschreibung
Verwendete Lizenzen	Die NetScaler Gateway CCU-Lizenzen, die während der ausgewählten Zeitleiste verwendet werden. Jede Zählung steht für die Anzahl der Benutzersitzungen. Dies ist unabhängig von den Anwendungs- und Desktopsitzungen, die von diesem Benutzer gestartet wurden.
Gesamtzahl der Lizenzen	Gesamtzahl der NetScaler Gateway CCU-Lizenzen, die der Kunde nutzen kann.



Bericht “Schwellenwert”

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* im ausgewählten Zeitraum als Lizenz ausgewählt wurde. Weitere Informationen finden Sie unter So erstellen Sie Schwellenwerte und Warnungen .

Problemen mit HDX Insight beheben

February 5, 2024

Wenn die HDX Insight-Lösung nicht wie erwartet funktioniert, liegt das Problem möglicherweise an einem der folgenden Probleme. Informationen zur Fehlerbehebung finden Sie in den Checklisten in den entsprechenden Abschnitten.

- HDX Insight-Konfiguration.
- Konnektivität zwischen NetScaler und NetScaler ADM.
- Datensatzgenerierung für HDX/ICA-Verkehr in NetScaler.
- Population von Datensätzen in NetScaler ADM.

Checkliste zur Konfiguration von HDX Insight

- Stellen Sie sicher, dass die AppFlow Funktion in NetScaler aktiviert ist. Einzelheiten finden Sie unter AppFlow aktivieren.
- Überprüfen Sie die HDX Insight Konfiguration in der NetScaler 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 ICA_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-Bereitstellungen sicher, dass die HDX Insight AppFlow-Richtlinie an den virtuellen VPN-Server gebunden ist, auf dem HDX/ICA-Verkehr 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 NetScaler Gateway oder dem virtuellem VPN-Server für die Access Gateway- oder Double-Hop-Bereitstellung aktiviert ist. Einzelheiten finden Sie unter AppFlow für virtuelle Server aktivieren.
- Aktivieren Sie “Connection Chaining”in Double-Hop-NetScaler. Einzelheiten finden Sie unter Konfigurieren von NetScaler 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 dem NetScaler-Hochverfügbarkeitspaar.

Konnektivität zwischen NetScaler und NetScaler ADM Checkliste

- Überprüfen Sie den AppFlow Collector-Status in NetScaler. Einzelheiten finden Sie unter So überprüfen Sie den Status der Konnektivität zwischen NetScaler 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 **Einstellungen > 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 NetScaler 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: **Analyse der ICA-Verbindung wurde übersprungen —HDX Insight wird für diesen Host nicht unterstützt**

  Ursache: Nicht unterstützte Citrix Virtual Apps and Desktops-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 von Citrix Workspace

  Lösung: Aktualisieren Sie Citrix Workspace 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 von ICA-Verkehr

  Lösung: Für diese ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wurde.
- 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 spezielle ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wurde.

- Protokoll: **EUEM ICA RTT fehlt**

  Ursache: Kanaldaten der Endbenutzer-Erlebnisüberwachung können nicht analysiert werden

  Lösung: Stellen Sie sicher, dass der Dienst zur Überwachung der Benutzererfahrung auf den Citrix Virtual Apps and Desktops-Servern gestartet wurde. Stellen Sie sicher, dass Sie die unterstützten Versionen der Citrix Workspace App verwenden.

- Protokoll: **Ungültiger Channel-Header**

  Ursache: Channel-Header konnte nicht identifiziert werden

  Lösung: Für diese spezielle ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wurde.

- Protokoll: **Code überspringen**

  Wenn Sie einen der folgenden Werte für den Überspringen-Code sehen, werden die Insight-Details übersprungen.

  > Skip-Code 0 zeigt an, dass der Datensatz erfolgreich aus NetScaler exportiert wurde.

Code überspringen	Fehlermeldung	Ursache des Fehlers
100	NS_ICA_ERR_NULL_FRAG	Fehler bei der Behandlung von ICA-Fragmenten, wahrscheinlich aufgrund von Speicherbedingungen
101	NS_ICA_ERR_INVALID_HS_CMD	Ungültiger Handshake-Befehl erhalten
102	NS_ICA_ERR_REDUC_PARAM_CNT	Ungültiger Parameter für V3-Expander-Initialisierung angegeben
103	NS_ICA_ERR_REDUC_INIT	Der V3-Expander konnte nicht korrekt initialisiert werden
104	NS_ICA_ERR_REDUC_PARAM_BYTES	Unzureichende Byte, um einem Kanal einen Coder zuzuweisen
105	NS_ICA_ERR_INVALID_CHANNEL	Ungültige ICA-Kanal Nummer
106	NS_ICA_ERR_INVALID_DECODER	Ungültiger Decoder für einen Kanal angegeben
107	NS_ICA_ERR_INVALID_TW_PARAM	Ungültige Parameteranzahl für Thinwire-Kanal angegeben
108	NS_ICA_ERR_INVALID_TW_DECODER	Ungültiger Decoder für Thinwire-Kanal

Code überspringen	Fehlermeldung	Ursache des Fehlers
109	NS_ICA_ERR_REDUC_NO_DECODER	Kein Decoder für Kanal definiert
110	NS_ICA_ERR_REDUC_V3_EXPANDER	Kanaldaten konnten nicht erweitert werden
111	NS_ICA_ERR_REDUC_BYTES_V3_OOB	Expander-Fehler: Byte verbrauchten mehr als verfügbare Byte
112	NS_ICA_ERR_REDUC_BYTES_OOR	Fehler: Unkomprimierter 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 unzureichender Speicherbedingungen
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	Speicherzuweisungsfehler für Expander-Kontext
117	NS_ICA_ERR_ICA_OLD_SERVER	Alter Server, Capability-Blöcke werden nicht unterstützt
118	NS_ICA_ERR_PIR_MANY_FRAG	Die Paket-Init-Anforderung ist fragmentiert und kann nicht verarbeitet werden
119	NS_ICA_ERR_INIT_ICA_CAPS	Initialisierungsfehler der ICA-Fähigkeit
120	NS_ICA_ERR_NO_MSI_SUPPORT	Der Host unterstützt keine MSI-Funktion. Zeigt eine niedrigere XenApp-Version als 6.5 oder eine niedrigere XenDesktop-Version als 5.0 an
121	NS_ICA_ERR_CGP_INVALID_CMD	Ungültiger CGP-Befehl gefunden
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	Unzureichende Byte über Kanal
123	NS_ICA_ERR_CHANNEL_DATA	Falsche Daten auf dem Kanal EUEM, CONTROL oder SEAMLESS

Code überspringen	Fehlermeldung	Ursache des Fehlers
124	NS_ICA_ERR_INVALID_PURE_CMD	Ungültiger Befehl bei der Verarbeitung reiner ICA-Kanaldaten
125	NS_ICA_ERR_INVALID_PURE_LEN	Ungültige Länge bei der Verarbeitung reiner ICA-Kanaldaten festgestellt
126	NS_ICA_ERR_INVALID_PURE_LEN	Bei der Verarbeitung von PURE ICA-Kanaldaten wurde eine ungültige Länge gefunden
127	NS_ICA_ERR_INVALID_CLNT_DATA	Ungültige Datenlänge vom Client erhalten
128	NS_ICA_ERR_MSI_GUID_SZ	Fehler in der MSI-GUID-Größe
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	Ungültiger Kanalheader erkannt
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_ID	Abruf der wiederverbundenen Sitzung ist fehlgeschlagen
131	NS_ICA_ERR_DISABLE_SR_NON_RECONNECT	Deaktivieren von SR
132	NS_ICA_ERR_REDUC_NOT_V3	Nicht unterstützte ICA-Reducer-Version
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Komprimierung deaktiviert, wird vom Host nicht berücksichtigt
134	NS_ICA_ERR_IDENT_PROTO	Das ICA- oder CGP-Protokoll konnte nicht identifiziert werden, es wurden falsche Workspaces angezeigt
135	NS_ICA_ERR_INVALID_SIGNATURE	Falsche ICA-Signatur oder magische Zeichenfolge
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_LARGE	ICA-Frame ist zu groß und überschreitet 1460 Bytes

Code überspringen	Fehlermeldung	Ursache des Fehlers
139	NS_ICA_ERR_FORWARD	Fehler beim Weiterleiten der ICA-Daten
140	NS_ICA_ERR_MAX_HOLES	Der CGP-Befehl kann nicht verarbeitet werden, da er über das unterstützte Limit hinaus aufgeteilt ist
141	NS_ICA_ERR_ASSEMBLE_FRAME	ICA-Rahmen kann nicht korrekt wieder zusammengebaut werden
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	Die Version für diesen Workspace (Client) wurde übersprungen, da er nicht in der Zulassungsliste enthalten ist
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	Der Analysestatus für das Wiederverbindungscookie des Clients kann nicht erkannt werden
144	NS_ICA_ERR_SYNCUP_RECONNECT_LEN	Ungültige Länge des Wiederverbindungs-Cookies wurde nach der Wiederverbindung erkannt
145	NS_ICA_ERR_INVALID_RECONNECT_ID	Client reconnects Cookie hat die erforderliche Einschränkung verpasst
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	Ungültige Workspace-Versionszeichenfolge vom Client empfangen
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	Ungültige Produkt-ID vom Kunden erhalten
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	Ungültige Kanallänge nach der Erweiterung
149	NS_ICA_ERR_SPECIAL_THINWIRE	Dekomprimierungsfehler
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	Nicht genügend Byte für Seamless-Befehl
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Unzureichende Byte für den EUEM-Befehl festgestellt

Code überspringen	Fehlermeldung	Ursache des Fehlers
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	Ungültiges Ereignis für Seamless Channel Parsing
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Ungültiges Ereignis für CTRL-Kanalanalyse
154	NS_ICA_ERR_EUEM_INVALID_EVENT	Ungültiges Ereignis für EUEM-Kanal-Parsing
155	NS_ICA_ERR_USB_INVALID_EVENT	Ungültiges Ereignis für USB-Kanal-Parsing
156	NS_ICA_ERR_PURE_INVALID_EVENT	Ungültiges Ereignis für reines Kanalparsing
157	NS_ICA_ERR_VCP_INVALID_EVENT	Ungültiges Ereignis für das Parsen virtueller Kanäle
158	NS_ICA_ERR_ICAP_INVALID_EVENT	Ungültiges Ereignis für ICA-Datenanalyse
159	NS_ICA_ERR_CGPP_INVALID_EVENT	Ungültiges Ereignis für CGP-Datenanalyse
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	Ungültiger Status für einen crypt-Befehl in der Basisverschlüsselung
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	Ungültiger crypt-Befehl in der Basisverschlüsselung
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	Ungültiger Status für einen crypt-Befehl in der RC5-Verschlüsselung
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	Ungültiger crypt-Befehl in der 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_REDUCER_V3	VER_V3 unterstützt Reducer Version 3 nicht
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Workspace unterstützt Reducer Version 3 nicht
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Unerwartete Anzahl von Byte im ICA-Handshake

Code überspringen	Fehlermeldung	Ursache des Fehlers
169	NS_ICA_ERR_HIGHER_RECONSEQ	Höhere CGP-Wiederaufnahme-Sequenznummer aus Peer-Post-Wiederverbindungen
170	NS_ICA_ERR_DESCSRINFO_ABSENT	Der 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_END	Fehler beim Analysieren der Details zum Sitzungsende aus den Insight-Kanaldaten
175	NS_ICA_ERR_NON_NSAP_SN	ICA-Parsing auf Dienstknoten wurde übersprungen, da keine Insight-Channel-Unterstützung vorhanden ist
176	NS_ICA_ERR_NON_NSAP_CLIENT	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_TKT_FETCH	Fehler beim Abrufen des Dienstes verbindet das Ticket im Serviceknoten
180	NS_ICA_ERR_SN_HIGHER_RECONSEQ	Fehler beim Empfangen einer höheren Sequenznummer für die Wiederverbindung im Dienstknoten
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 [0
x8820220228], 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 [0
x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

Zähler für Fehler

Verschiedene Zähler werden beim ICA-Parsen 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.

HDX-Leistungsindikatorname	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_tot_ica_conn	Gibt die Gesamtzahl der von NS erkannten reinen ICA-Verbindungen an. Wird immer dann erhöht, wenn eine ICA-Verbindung erkannt wird, die auf der ICA-Signatur auf einer Client-Leiterplatte basiert.	Statistiken

HDX-Leistungsindikatorname	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_tot_cgp_conn	Zeigt die Gesamtzahl der von NS erkannten CGP-Verbindungen an (Sitzungszuverlässigkeit EIN). Wird immer dann erhöht, wenn eine CGP-Verbindung basierend auf der CGP-Signatur auf einer Client-PCB erkannt wird.	Statistiken
hdx_dbg_tot_udt_conn	Zeigt die Gesamtzahl der von NS erkannten UDP-ICA-Verbindungen an	Statistiken
hdx_dbg_tot_nsap_conn	Gibt die Gesamtzahl der von NS erkannten NSAP-unterstützten Verbindungen an	Statistiken
hdx_tot_skip_conn	Gibt an, wie viele ICA-Verbindungen vom Parser aufgrund einer ungültigen ICA- oder CGP-Signatur übersprungen	Statistiken
hdx_dbg_active_conn	Gesamtzahl der aktiven EDT/CGP/ICA-Verbindungen zu diesem Zeitpunkt.	Statistiken
hdx_dbg_active_nsap_conn	Gesamtzahl der aktiven 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 der transparenten Benutzerzugriffe	Stats/Diagnostik
hdx_dbg_ag_user	Gesamtzahl der Access Gateway-Benutzerzugriffe	Stats/Diagnostik
hdx_dbg_lan_user	Gesamtzahl der Zugriffe auf den LAN-Benutzermodus	Stats/Diagnostik

HDX-Leistungsindikatorname	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_basic_enc	Gibt die Anzahl der ICA-Verbindungen an, die die Standardverschlüsselung verwenden	Stats/Diagnostik
hdx_advanced_enc	Gibt die Anzahl der ICA-Verbindungen an, die erweiterte RC5-basierte Verschlüsselung verwenden	Stats/Diagnostik
hdx_dbg_reconnected_session	Gesamtzahl der Wiederverbindungsanforderungen vom Client ohne NetScaler-Fehler	Stats/Diagnostik
hdx_dbg_host_rejected_ns_reconnect	Gesamtzahl der Hosts, die Wiederverbindungsanforderungen nach Client abgelehnt haben	Stats/Diagnostik
hdx_euem_available	Gibt die Anzahl der Verbindungen an, für die der Kanal End User Experience Monitoring verfügbar ist. Für die Erfassung von Statistiken wie ICA-RTT ist ein Kanal zur Überwachung der Nutzererfahrung erforderlich.	Stats/Diagnostik
hdx_err_disabled_sr	Die Sitzungszuverlässigkeit wird mit dem Regler `nsapimgr` deaktiviert. Die Sitzung funktioniert für diese Sitzung nicht.	Fehler
hdx_err_skip_no_msi	Dem XA/XD-Server fehlt die MSI-Fähigkeit. Dies weist auf eine ältere Serverversion hin und HDX Insight überspringt diese Verbindung.	Fehler
hdx_err_skip_old_server	Alte, nicht unterstützte Serverversion	Fehler

HDX-Leistungsindikatorname	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_err_clnt_not_whitelist	Der Client-Workspace ist nicht in der Zulassungsliste enthalten, HDX Insight überspringt diese Verbindung	Fehler
hdx_sm_ica_cam_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CAM_CHANNEL	Diagnose
hdx_sm_ica_usb_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_USB_CHANNEL	Diagnose
hdx_sm_ica_clip_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CLIP_CHANNEL	Diagnose
hdx_sm_ica_ccm_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CCM_CHANNEL	Diagnose
hdx_sm_ica_cdm_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CDM_CHANNEL	Diagnose
hdx_sm_ica_com1_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_COM1_CHANNEL	Diagnose
hdx_sm_ica_com2_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_COM2_CHANNEL	Diagnose
hdx_sm_ica_cpm_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CPM_CHANNEL	Diagnose

HDX-Leistungsindikatorname	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_sm_ica_lpt1_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_LPT1_CHANNEL	Diagnose
hdx_sm_ica_lpt2_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_LPT2_CHANNEL	Diagnose
dx_dbg_sm_ica_msi_disabled	Gesamtzahl der Fälle, in denen MSI über die SmartAccess-Richtlinie deaktiviert ist	Diagnose
hdx_sm_ica_file_channel_disabled	Die Gesamtzahl 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 der abgelehnten 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 ausgelaufenen USB-Geräte	Diagnose
hdx_dbg_usb_device_stopped	Gesamtzahl der gestoppten USB-Geräte	Diagnose

nstrace-Validierung

Suchen Sie nach dem CFLOW-Protokoll, um zu sehen, dass alle AppFlow-Datensätze aus NetScaler ausgehen.

Grundgesamtheit der Datensätze in der NetScaler 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 NetScaler ADM AppFlow-Einträge erhält.
- Bestätigen Sie, dass NetScaler-Instanz zu NetScaler ADM hinzugefügt wird.
- Überprüfen Sie, ob der virtuelle NetScaler Gateway/VPN-Server in NetScaler ADM lizenziert ist.
- Stellen Sie sicher, dass Multi-Hop-Parametereinstellung für Double-Hop aktiviert ist
- Stellen Sie sicher, dass NetScaler Gateway für den zweiten Hop in der Double-Hop-Bereitstellung freigegeben

Bevor Sie den technischen Support von Citrix kontaktieren

Stellen Sie für eine schnelle Lösung sicher, dass Sie über die folgenden Informationen verfügen, bevor Sie sich an den technischen Support von Citrix wenden:

- Einzelheiten zur Bereitstellung und Netzwerktopologie.
- NetScaler- und NetScaler ADM-Versionen.
- Serverversionen von Citrix Virtual Apps and Desktops.
- Client Workspace-Versionen.
- Anzahl der aktiven ICA-Sitzungen, bei denen das Problem aufgetreten ist.
- Das technische Supportpaket wird durch Ausführen des Befehls `show techsupport` an der NetScaler-Eingabeaufforderung erfasst.
- Technischer Support Paket für NetScaler ADM erfasst.
- Paketspuren wurden auf allen NetScaler erfasst.
  Um eine Paketablaufverfolgung zu starten, geben Sie Folgendes ein: `start nstrace -size 0'`
  Um eine Paketablaufverfolgung zu stoppen: `stop nstrace`
- Sammeln Sie Einträge in der ARP-Tabelle des Systems, indem Sie den Befehl `show arp` ausführen.

Bekannte Probleme

Bekannte Probleme mit HDX Insight finden Sie in den ADC-Versionshinweisen.

Infrastrukturanalyse

February 5, 2024

Ein wichtiges Ziel für Netzwerkadministratoren ist die Überwachung von NetScaler-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. Sie können alle wahrscheinlichen Probleme bei Konfiguration, Einrichtung, Konnektivität, Zertifikaten und anderen beheben, die sich auf die Anwendungsnutzung oder -leistung auswirken könnten. Zum Beispiel kann eine plötzliche Änderung des Anwendungsdatenverkehrs auf eine Änderung der SSL-Konfiguration zurückzuführen sein, wie die Deaktivierung eines SSL-Protokolls. Administratoren müssen in der Lage sein, die Korrelation zwischen diesen Datenpunkten schnell zu erkennen, um Folgendes sicherzustellen:

- Die 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

Die Infrastructure Analytics-Funktion vereinfacht den Prozess der Datenanalyse, indem sie mehrere Datenquellen korreliert und zu einem messbaren Ergebnis quantifiziert, das den Zustand einer Instanz definiert. Mit dieser Funktion erhalten die Administratoren eine zentrale Anlaufstelle, um zu erfahren, ob ein Problem vorliegt, woher das Problem stammt und welche möglichen Abhilfemaßnahmen sie durchführen können.

Analytik der Infrastruktur

Die Infrastrukturanalysefunktion von NetScaler Application Delivery Management (ADM) fasst alle von den NetScaler-Instances gesammelten Daten zusammen und quantifiziert sie in einem **Instance-Score**, der den Zustand der Instances definiert. Die Instanzbewertung wird in einer tabellarischen Ansicht oder als Circlepack-Visualisierung zusammengefasst. Mit der Funktion Infrastructure Analytics können Sie die Faktoren visualisieren, die zu einem Problem in den Instanzen geführt haben oder dazu führen könnten. Diese Visualisierung hilft Ihnen auch dabei, die Aktionen zu bestimmen, die ausgeführt werden müssen, um das Problem und sein erneutes Auftreten zu verhindern.

Instanz-Score

Die Instanzbewertung gibt den Zustand einer ADC-Instanz an. Eine Punktzahl von 100 bedeutet eine absolut gesunde Instanz ohne Probleme. Die Instanz-Bewertung erfasst verschiedene Ebenen potenzieller Probleme auf der Instanz. Es handelt sich um eine quantifizierbare Messung des Instanzzustands, und mehrere "Gesundheitsindikatoren"tragen zum Score bei.

Integritätsindikatoren sind die Bausteine des Instanz-Scores, bei dem der Score regelmäßig für einen vordefinierten "Überwachungszeitraum"berechnet wird, basierend auf allen erkannten Indikatoren in diesem Zeitfenster. Derzeit berechnet Infrastructure Analytics den Instanz-Score einmal pro Stunde auf der Grundlage der von den Instanzen gesammelten Daten.
Ein Indikator kann als jede Aktivität (ein Ereignis oder ein Problem) definiert werden, die zu einer der folgenden Kategorien auf den Instanzen gehört.

- Indikatoren für Systemressourcen
- Indikatoren für kritische Ereignisse
- SSL-Konfigurationsindikatoren
- Konfigurationsabweichungsindikatoren

Gesundheitsindikatoren

- Indikatoren für Systemressourcen

  Im Folgenden finden Sie die kritischen Systemressourcenprobleme, die auf NetScaler-Instanzen auftreten und von NetScaler ADM überwacht werden können.

  - **Hohe CPU-Auslastung**. Die CPU-Auslastung hat den höheren Schwellenwert in der NetScaler-Instanz überschritten.
  - **Hohe Speicherauslastung**. Die Speicherauslastung hat den höheren Schwellenwert in der NetScaler-Instanz überschritten.
  - **Hohe Datenträgernutzung**. Die Datenträgerauslastung hat den höheren Schwellenwert in der NetScaler-Instanz überschritten.
  - **Datenträgerfehler**. Es gibt Fehler auf Festplatte 0 oder Festplatte 1 auf dem Hypervisor, auf dem die ADC-Instanz installiert ist.
  - **Stromausfall**. Die Stromversorgung ist ausgefallen oder wurde von der ADC-Instanz getrennt.
  - **Ausfall der SSL-Karte**. Die auf der Instanz installierte SSL-Karte ist ausgefallen.
  - **Flash-Fehler**. Bei der NetScaler-Instanz sind Compact Flash Fehler aufgetreten.

  - **NIC verwirft**. Die von der NIC-Karte verworfenen Pakete haben den höheren Schwellenwert in der NetScaler-Instanz überschritten.

Weitere Informationen zu diesen Systemressourcenfehlern finden Sie unter Das Instanz-Dashboard.

- Indikatoren für kritische Ereignisse

  Die folgenden kritischen Ereignisse werden anhand der Ereignisverwaltungsfunktion von ADM identifiziert, die für den Schweregrad „Kritisch“konfiguriert sind.

  - **HA-Synchronisierung fehlgeschlagen**. Die Konfigurationssynchronisierung zwischen den ADC-Instanzen mit hoher Verfügbarkeit ist auf dem sekundären Server fehlgeschlagen.
  - **HA kein Herzschlag**. Der Primärserver in zwei ADC-Instances mit hoher Verfügbarkeit empfängt keine Herzschläge vom sekundären Server.
  - **HA bad secondary state**. Der sekundäre Server in zwei ADC-Instanzen mit hoher Verfügbarkeit befindet sich im Status Down, Unknown oder Stay secondary.
  - **Nichtübereinstimmung der HA-Version**. Die Version der ADC-Software-Images, die auf zwei ADC-Instanzen mit hoher Verfügbarkeit installiert sind, stimmt nicht überein.
  - **Fehler bei der Clustersynchron** Die Konfigurationssynchronisierung zwischen den ADC-Instanzen im Clustermodus ist fehlgeschlagen.
  - **Nichtübereinstimmung der Clusterversion**. Die Version der ADC-Software-Images, die auf den ADC-Instanzen im Clustermodus installiert sind, stimmt nicht überein.
  - **Fehler bei der Clusterverbreitung**. 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 unter Ändern des gemeldeten Schweregrads von Ereignissen, die in NetScaler-Instanzen auftreten.

  Weitere Informationen zu Ereignissen in NetScaler ADM finden Sie unter Ereignisse.

- SSL-Konfigurationsindikatoren

  - **Nicht empfohlene Schlüsselstärke**. Die Hauptstärke der SSL-Zertifikate entspricht nicht den NetScaler-Standards
  - **Nicht empfohlener Aussteller**. Der Herausgeber des SSL-Zertifikats wird von Citrix nicht empfohlen.

  - **SSL-Zertifikate sind abgelaufen**. Das in der ADC-Instanz installierte SSL-Zertifikat ist abgelaufen.
  - **Ablauf der SSL-Zertifikate ist fällig**. Das in der ADC-Instanz installierte SSL-Zertifikat läuft in der nächsten Woche ab.
  - **Nicht empfohlene Algorithmen**. Die Signaturalgorithmen der in der ADC-Instanz installierten SSL-Zertifikate entsprechen nicht den NetScaler-Standards.

Weitere Informationen zu SSL-Zertifikaten finden Sie unter SSL-Dashboard.

- Konfigurationsabweichungsindikatoren
  - **Konfigurationsdrift-Vorlage**. Es gibt eine Abweichung (ungespeicherte Änderungen) in der Konfiguration von den Überwachungsvorlagen, die Sie mit bestimmten Konfigurationen erstellt haben, die Sie für bestimmte Instanzen überwachen möchten.
  - **Standardeinstellung für Konfigurationsabweichung**. Es gibt eine Drift (nicht gespeicherte Änderungen) in der Konfiguration aus den Standardkonfigurationsdateien.

Weitere Informationen zu Konfigurationsabweichungen und zur Ausführung von Auditberichten zur Überprüfung von Konfigurationsabweichungen finden Sie unter Auditberichte anzeigen .

ADC-Kapazitätsprobleme anzeigen

Wenn eine ADC-Instanz den größten Teil ihrer verfügbaren Kapazität verbraucht hat, kann es während der Verarbeitung des Client-Datenverkehrs zu einem Paket-Drop kommen. Dieses Problem führt zu einer geringen Leistung in einer ADC-Instanz. Wenn Sie solche ADC-Kapazitätsprobleme verstehen, können Sie proaktiv zusätzliche Lizenzen zuweisen, um die ADC-Leistung aufrechtzuerhalten.

So zeigen Sie ADC-Kapazitätsprobleme an:

1. Navigieren Sie zu **Infrastruktur > 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 sind nach den folgenden Kapazitätsparametern kategorisiert:

- **Durchsatzlimit erreicht** —Die Anzahl der Pakete, die in der Instanz nach Erreichen des Durchsatzlimits verworfen wurden.
- **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 nach Erreichen des PPS-Grenzwerts verworfen wurden.

- **SSL-Durchsatzrate Limit** —Gibt an, wie oft das SSL-Durchsatzlimit erreicht wurde.
- **SSL-TPS-Ratenlimit** —Gibt an, wie oft das SSL-TPS-Limit erreicht wurde.

Das ADM berechnet die Instanzbewertung anhand des definierten Kapazitätsschwellenwerts.

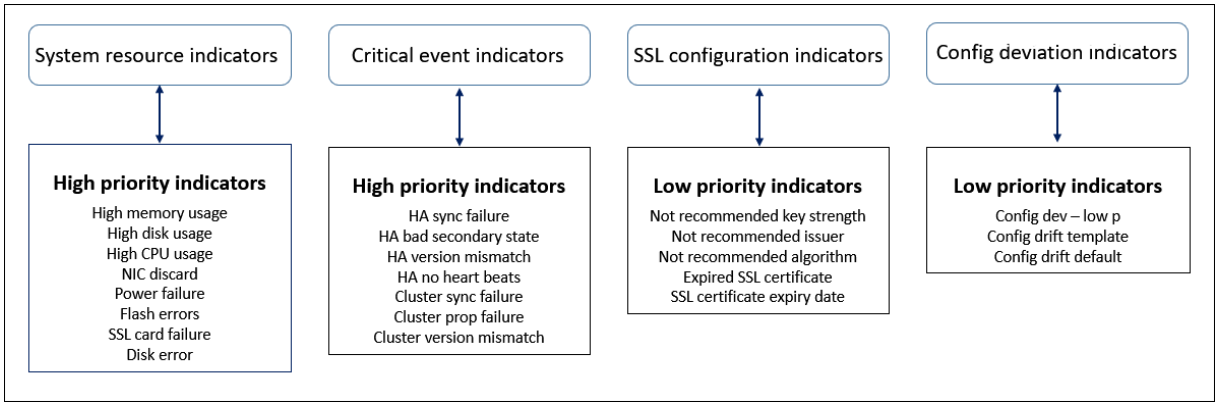
- Niedriger Schwellenwert —1 Zählerinkrement für Paketverlust oder Ratenbegrenzung
- Hoher Schwellenwert —10.000 Paketverlust oder Erhöhung des Ratenlimit-Zählers

Wenn eine ADC-Instance den Kapazitätsschwellenwert überschreitet, wirkt sich dies daher auf die Instance-Bewertung aus.

Wenn Pakete fallen oder der Zähler für die Ratenbegrenzung inkrementiert wird, wird ein Ereignis in der Kategorie `ADCCapacityBreach` generiert. Um diese Ereignisse einzusehen, navigieren Sie zu **Konten > Systemereignisse**.

Wert von Gesundheitsindikatoren

Die Indikatoren werden anhand ihrer Werte wie folgt in Indikatoren mit hoher Priorität und Indikatoren mit niedriger Priorität eingeteilt:



Den Gesundheitsindikatoren innerhalb derselben Indikatorengruppe werden unterschiedliche Gewichtungen zugewiesen. Ein Indikator kann mehr zu einem niedrigeren Instanz-Score 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 auf einer Instanz eine größere Anzahl von Indikatoren erkannt wird, ist der Instanzwert umso geringer.

Der Wert eines Indikators wird auf der Grundlage der folgenden Regeln berechnet. Der Indikator soll auf eine der folgenden drei Arten erkannt werden:

1. **Basierend auf einer Aktivität**. Beispielsweise wird ein Systemressourcenindikator ausgelöst, wenn in der Instanz ein Stromausfall auftritt, und dieser Indikator verringert den Wert der Instanzbewertung. Wenn der Indikator gelöscht ist, wird die Strafe gelöscht und der Instanzwert erhöht sich.

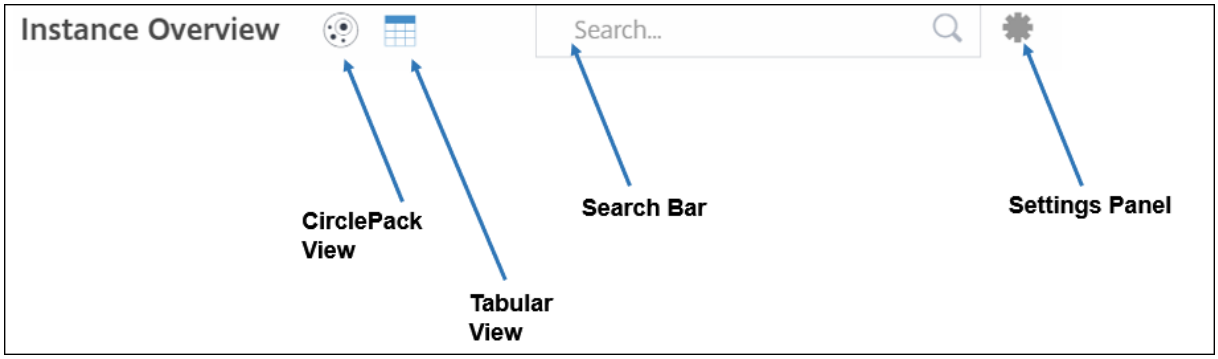
2. **Basierend auf der Verletzung des Schwellenwerts**. Beispielsweise wird eine Systemressourcenanzeige ausgelöst, wenn die NIC-Karte Pakete verwirft und der Schwellenwert überschritten wird.
3. **Basierend auf der Verletzung des niedrigen und hohen Schwellenwerts**. Hier kann ein Indikator auf zwei Arten ausgelöst werden:
    - Wenn der Wert des Indikators zwischen niedrigen und hohen Schwellenwerten liegt, wird in diesem Fall eine Teilstrafe auf die Instanzbewertung erhoben.
    - Wenn der Wert den hohen Schwellenwert überschreitet, wird in diesem Fall eine volle Strafe auf die Instanzbewertung erhoben.
    - Wenn der Wert unter einen niedrigen Schwellenwert fällt, wird keine Strafe auf den Instanz-Score erhoben.

Beispielsweise ist die CPU-Auslastung ein Systemressourcenindikator, der ausgelöst wird, wenn der Nutzungswert den niedrigen Schwellenwert überschreitet und wenn der Wert den hohen Schwellenwert überschreitet.

Dashboard für Infrastrukturanalysen

Navigieren Sie zu **Infrastruktur > Infrastructure Analytics**.

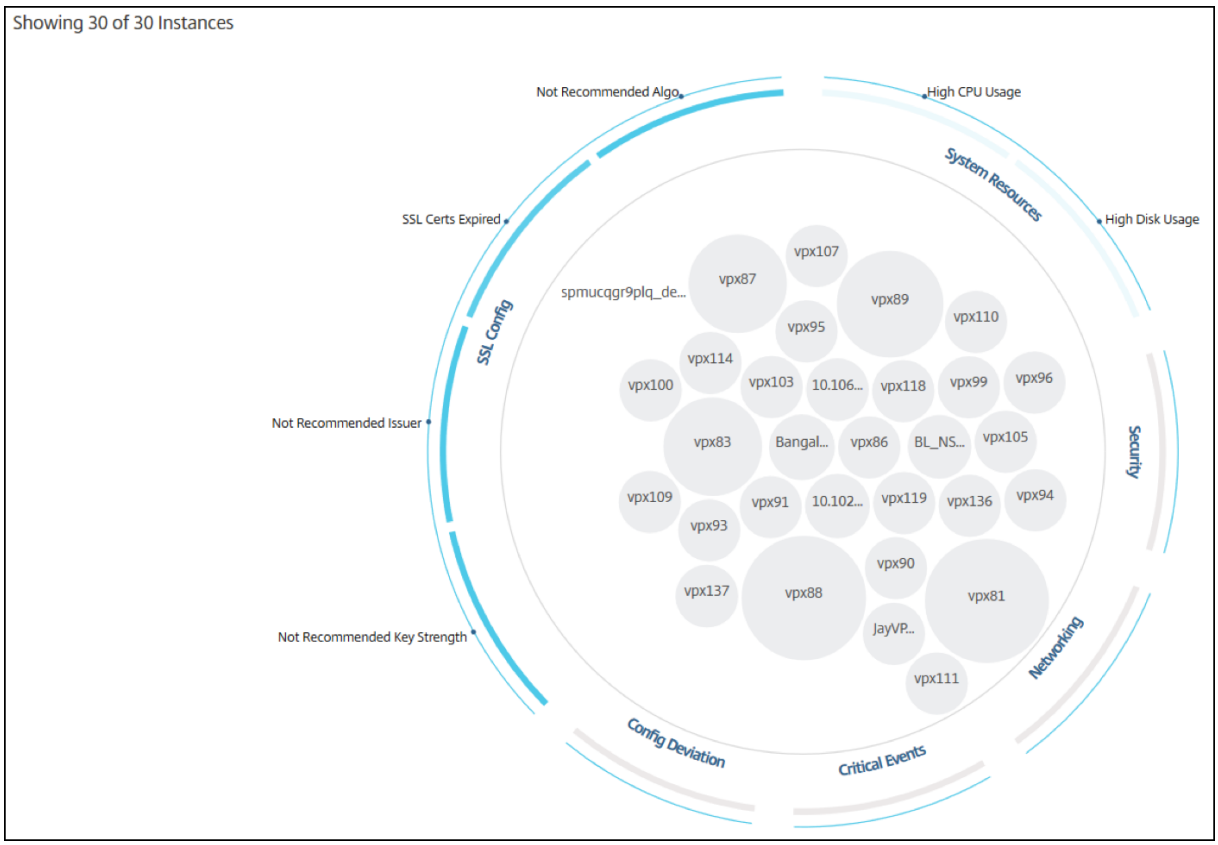
Die Infrastructure Analytics kann im **Circle Pack-** oder **Tabellenformat** angezeigt werden. Sie können zwischen den beiden Formaten hin- und herschalten.



- In der Tabellenansicht 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 rechts auf der Seite das Zusammenfassungsfenster angezeigt.
- Klicken Sie auf das Symbol **Einstellungen**, um die **Einstellungsleiste** anzuzeigen.
- In beiden Ansichtsformaten zeigt das Zusammenfassungsfenster Details aller Instanzen in Ihrem Netzwerk an.

Kreispaketansicht

Kreispackdiagramme zeigen Instanzgruppen als eng organisierte Kreise. Sie zeigen oft Hierarchien, in denen kleinere Instanzgruppen entweder ähnlich gefärbt sind wie andere in derselben Kategorie oder in größeren Gruppen verschachtelt sind. Circle Packs stellen hierarchische Datensätze dar und zeigen verschiedene Ebenen in der Hierarchie und wie sie miteinander interagieren.



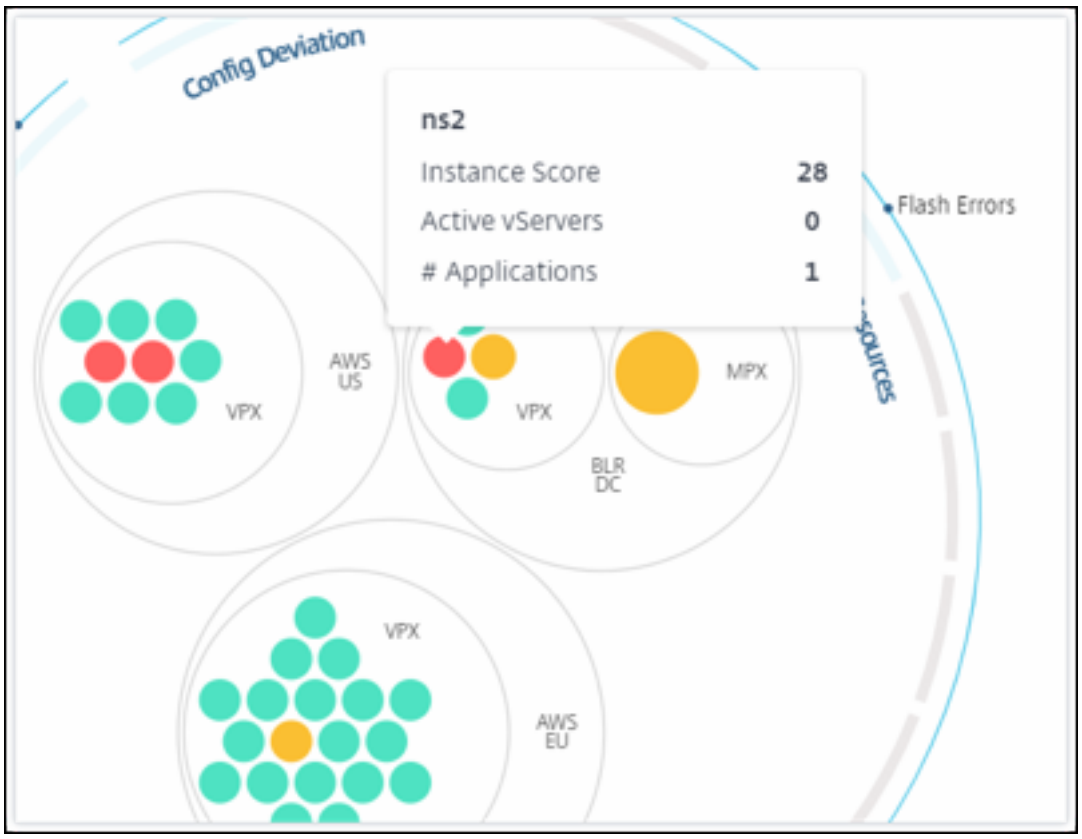
Instanzkreise

Farbe. Jede Instanz wird im Circle Pack als farbiger Kreis dargestellt. Die Farbe des Kreises zeigt den Zustand dieser Instanz an.

- **Grün** —Instanz-Score liegt zwischen 100 und 80. Die Instanz ist gesund.
- **Gelb** —Die Bewertung der Instanz liegt zwischen 80 und 50; einige Probleme wurden festgestellt und müssen überprüft werden.
- **Rot** —Instanz-Score liegt unter 50. Die Instanz befindet sich in einer kritischen Phase, da bei dieser Instanz mehrere Probleme festgestellt wurden.

Größe. Die Größe dieser farbigen Kreise gibt die Anzahl der virtuellen Server an, die auf dieser Instanz konfiguriert sind. Ein größerer Kreis zeigt an, dass es eine größere Anzahl virtueller Server gibt.

Sie können den Mauszeiger auf jeden Instanzkreis (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 auf dieser Instanz konfigurierten Anwendungen an.

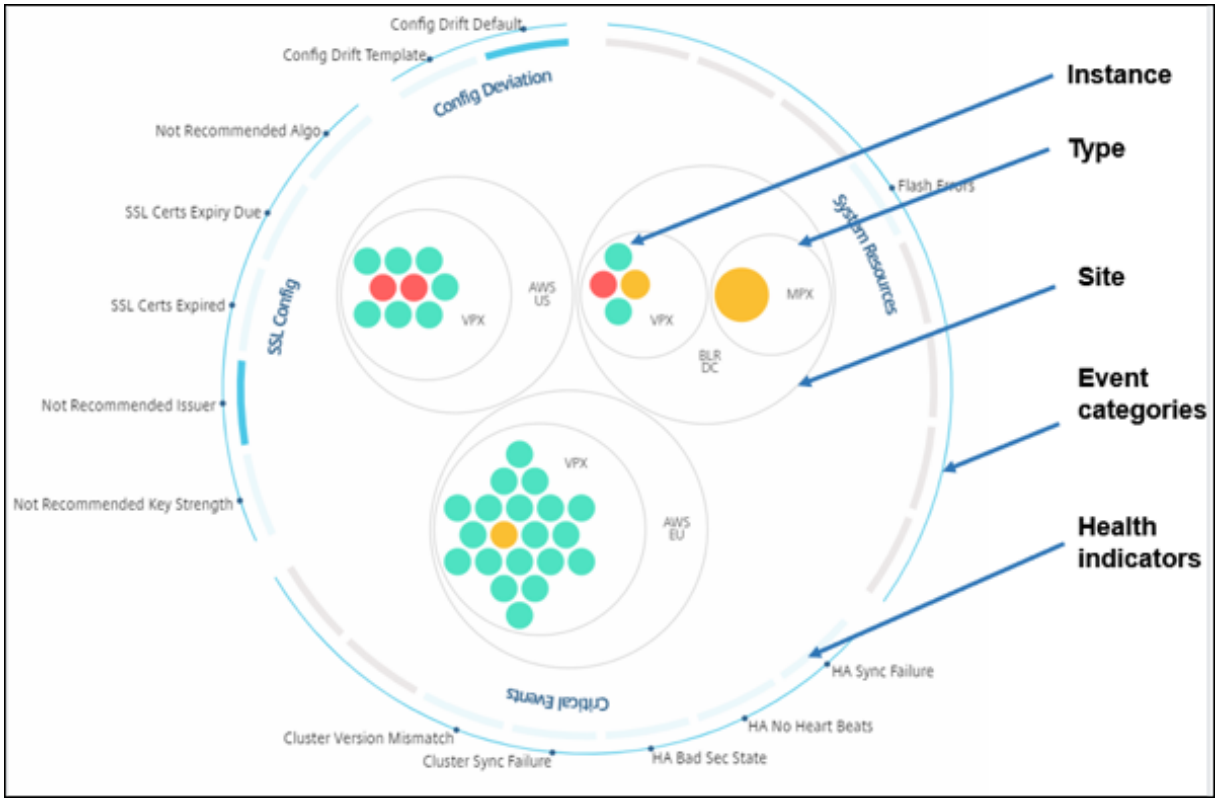


Gruppierte Instanzkreise

Das Circle Pack besteht zu Beginn aus Instanzkreise, die anhand der folgenden Kriterien gruppiert, verschachtelt oder innerhalb eines anderen Kreises gepackt werden:

- der Standort, an dem sie eingesetzt werden
- die Art der bereitgestellten Instanzen - VPX, MPX, SDX und CPX
- das virtuelle oder physische Modell der ADC-Instanz
- Auf den Instanzen installierte ADC-Image-Version

Die folgende Abbildung zeigt ein Circle Pack, in dem die Instanzen zuerst nach der Site oder dem Datencenter gruppiert werden, an dem sie bereitgestellt werden, und dann anhand ihres Typs, VPX und MPX weiter gruppiert werden.

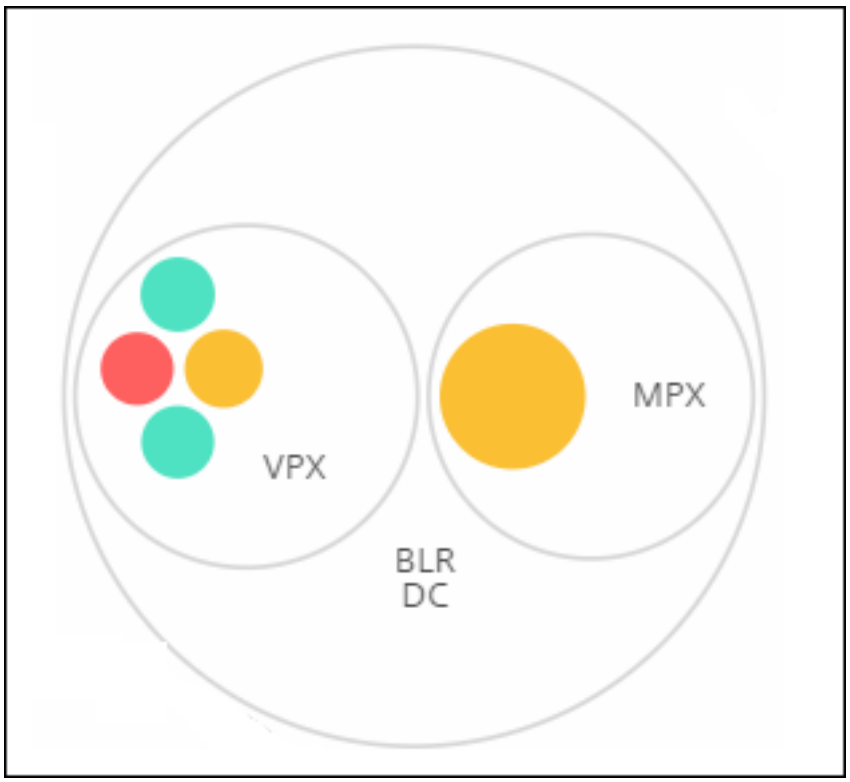


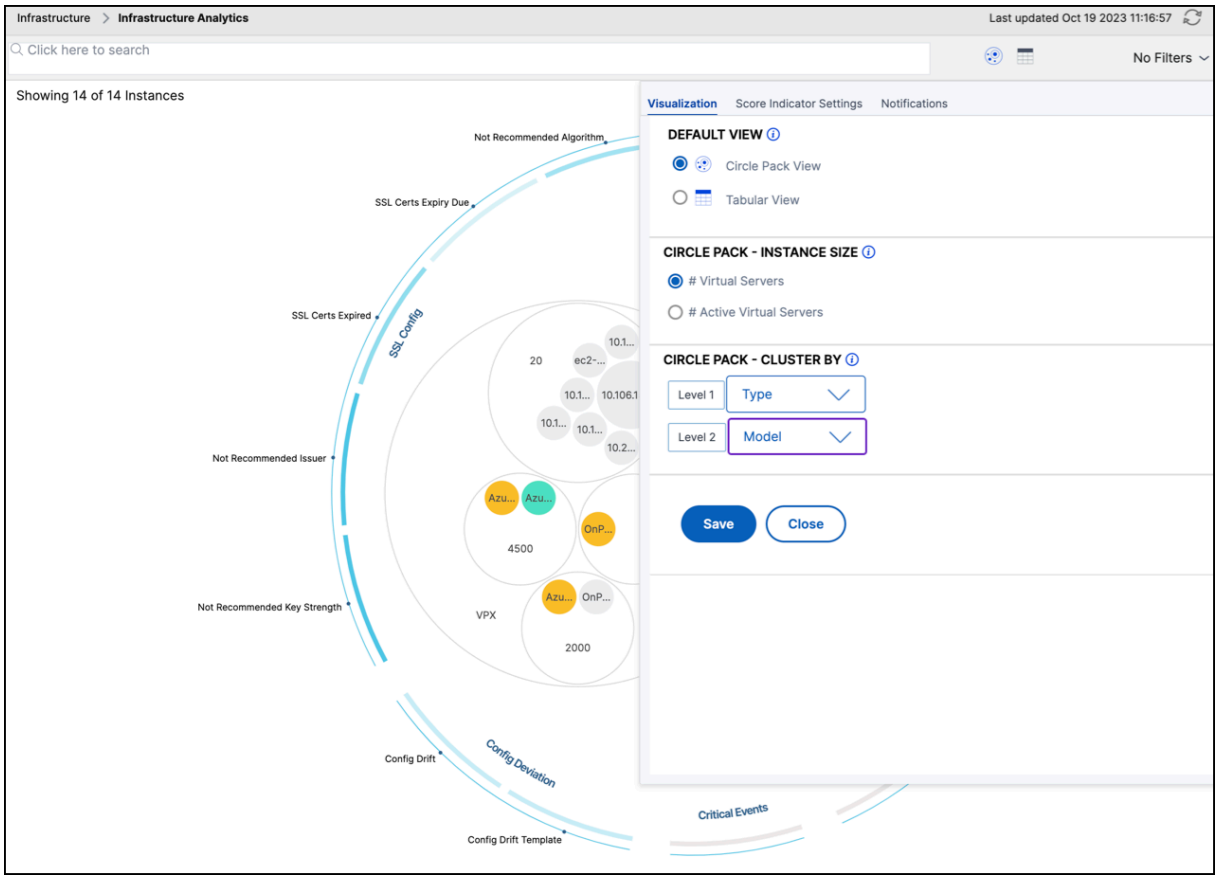
Alle diese verschachtelten Kreise werden von zwei äußersten Kreisen begrenzt. Die äußeren beiden Kreise stellen die vier Kategorien von Ereignissen dar, die vom NetScaler ADM überwacht werden (Systemressourcen, kritische Ereignisse, SSL-Konfiguration und Konfigurationsabweichung) sowie die beitragenden Integritätsindikatoren.

Gruppierte Instanzkreise

NetScaler ADM überwacht viele Instanzen. Um die Überwachung und Wartung dieser Instanzen zu vereinfachen, können Sie sie mit Infrastructure Analytics auf zwei Ebenen clustern. Das heißt, die Instanzgruppierungen können innerhalb einer anderen Gruppierung verschachtelt werden.

Zum Beispiel verfügt das BLR-Rechenzentrum über zwei Arten 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 jetzt leicht erkennen, wie viele Instanztypen in den von Ihnen verwalteten Sites bereitgestellt werden.

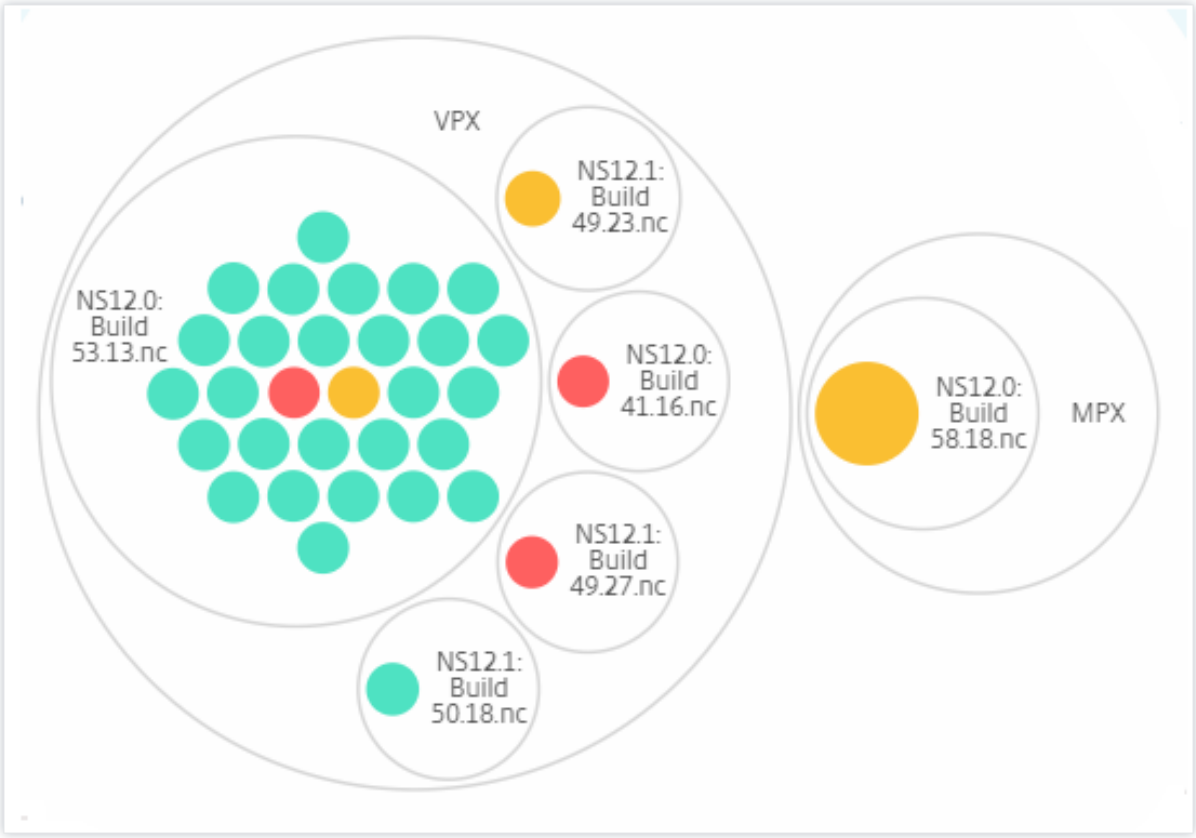




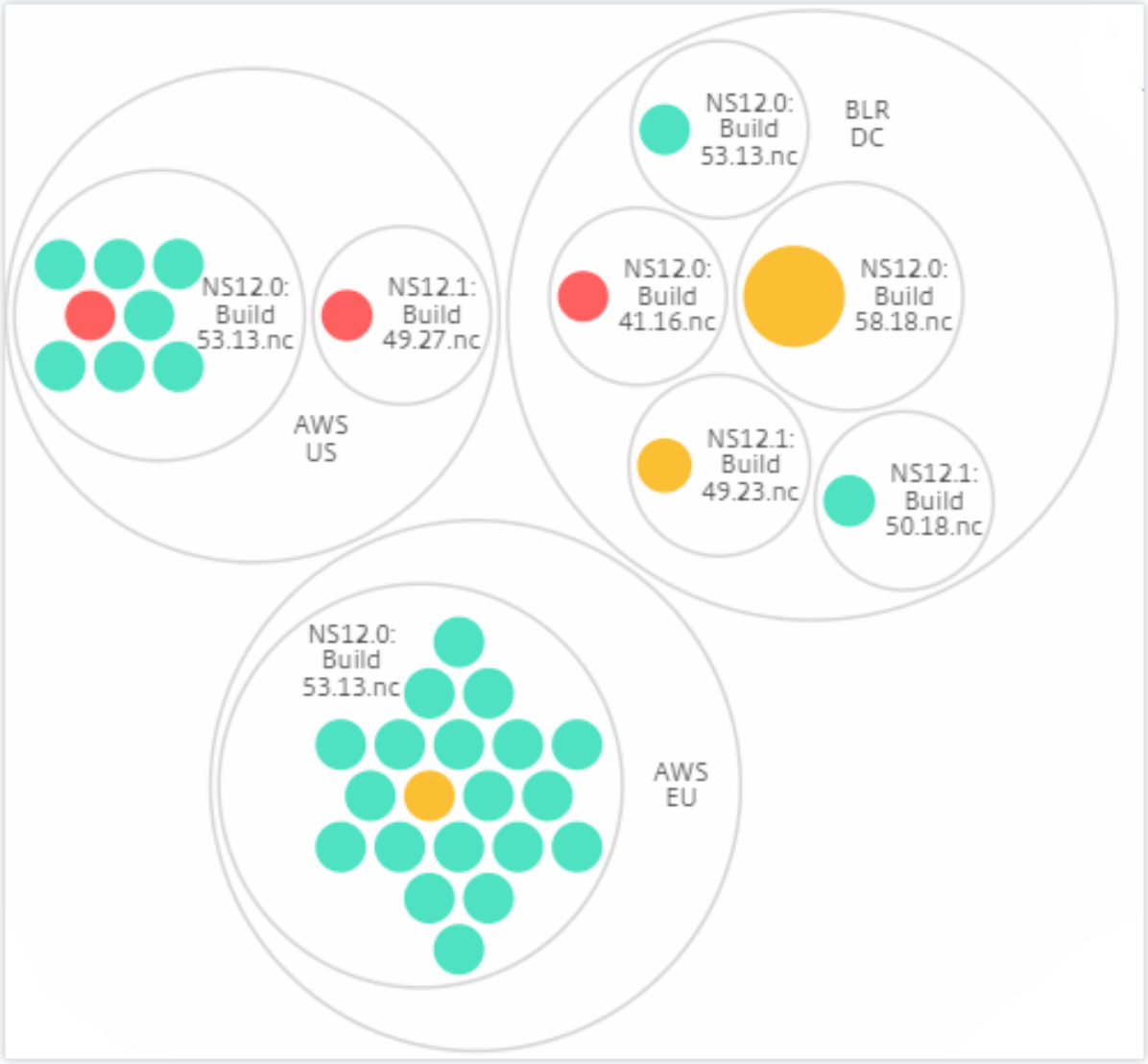
Ein paar weitere Beispiele für zweistufiges Clustering sind wie folgt:

Standort und Modell:

Typ und Ausführung:

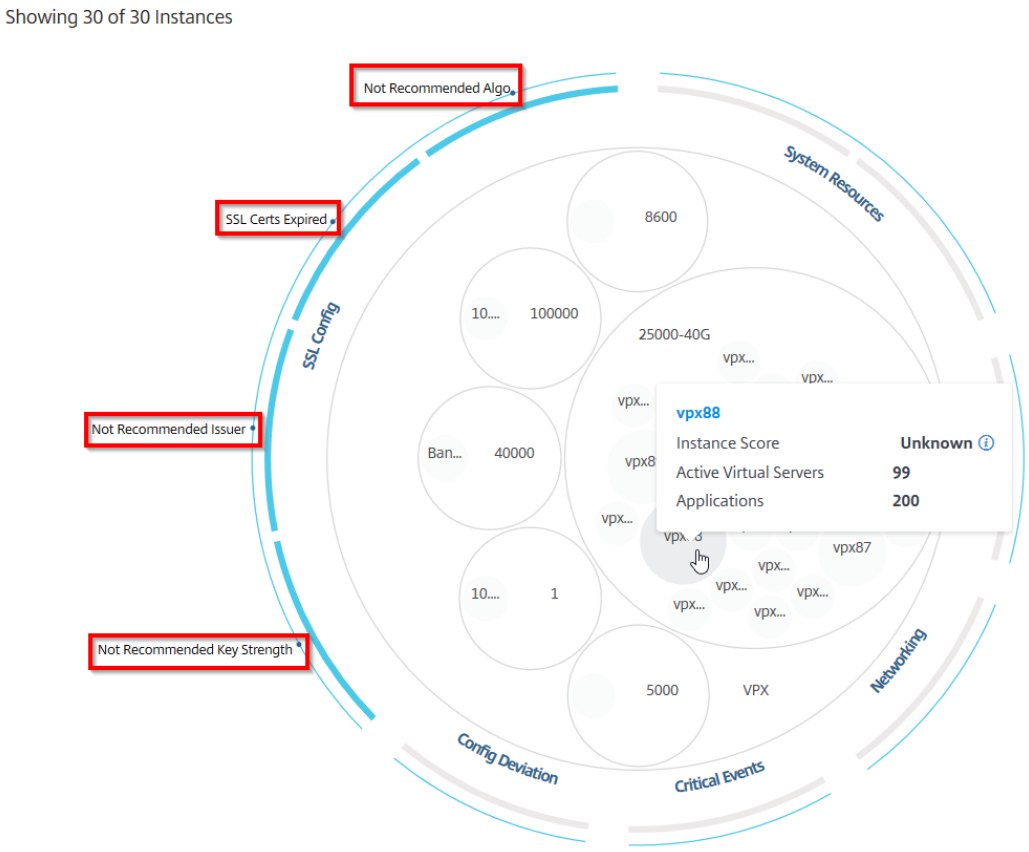


Website und Version:



Wie benutzt man Circle Pack

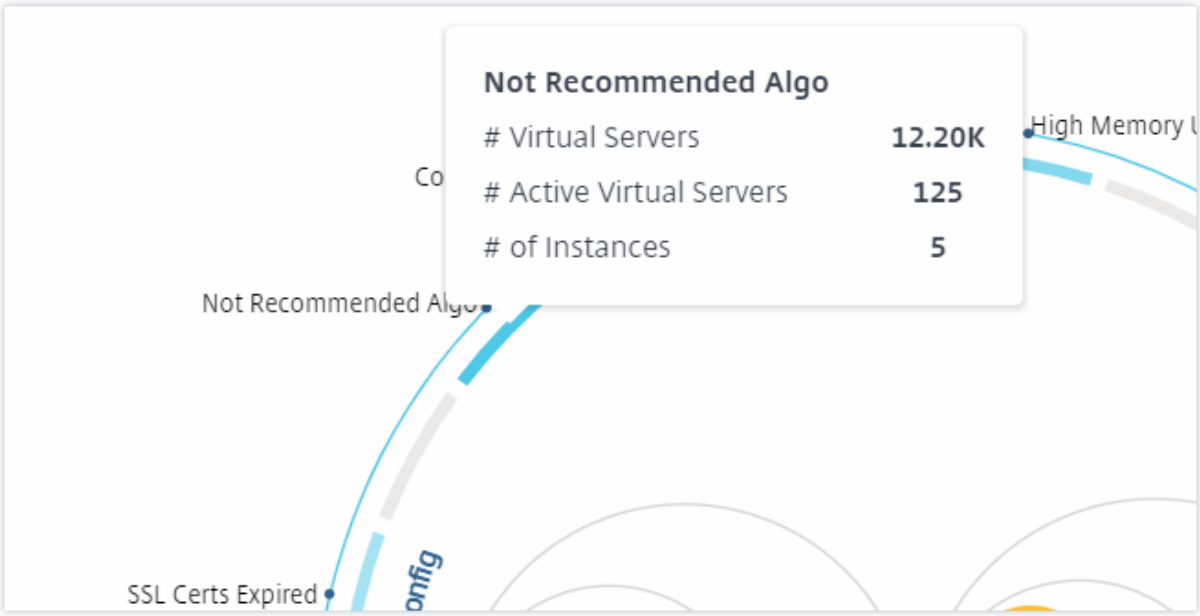
Klicken Sie auf jeden der farbigen Kreise, um diese Instanz hervorzuheben.



Abhängig von den Ereignissen, die in dieser Instanz aufgetreten sind, werden nur diese Gesundheitsindikatoren auf den äußeren Kreisen hervorgehoben. Die folgenden beiden Bilder des Circle Pack zeigen beispielsweise unterschiedliche Risikoindikatoren, 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 Algoum den zusammenfassenden Bericht dieses Risikoindikators anzuzeigen.

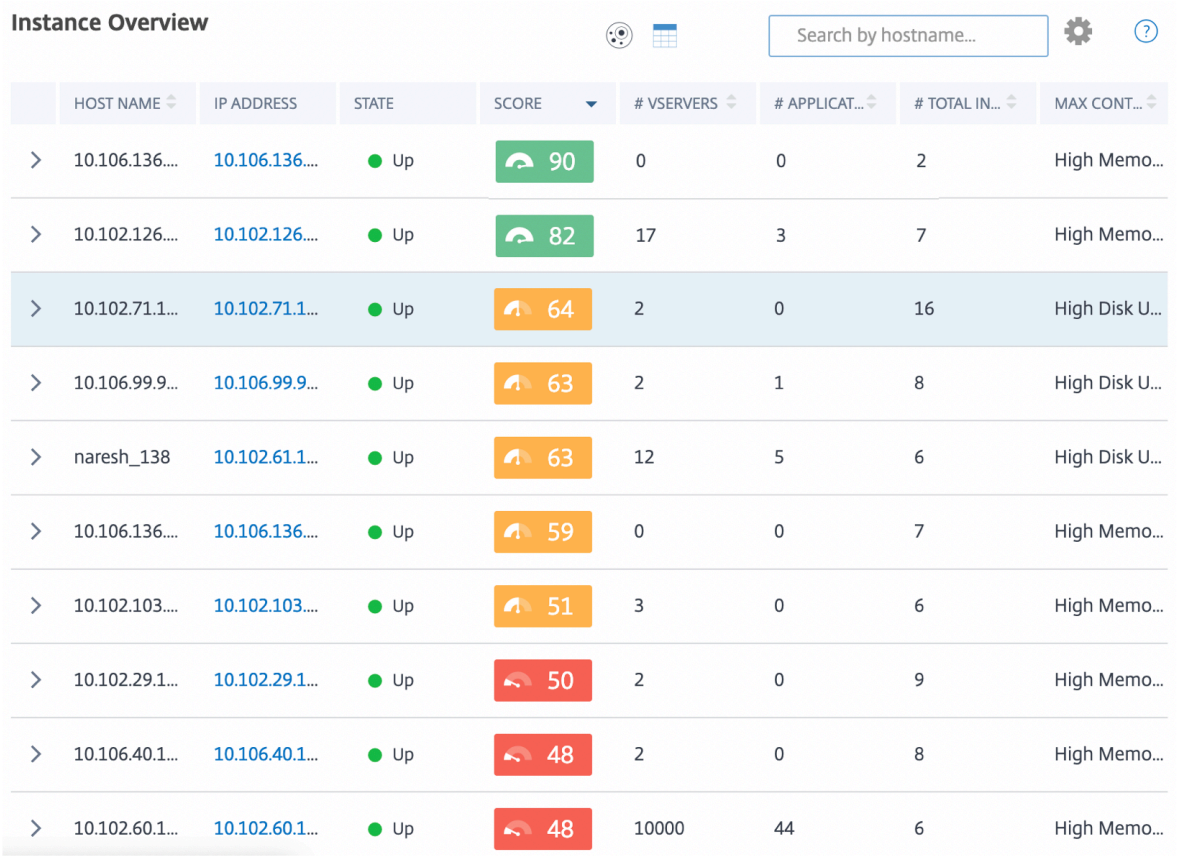


Tabellarische Ansicht

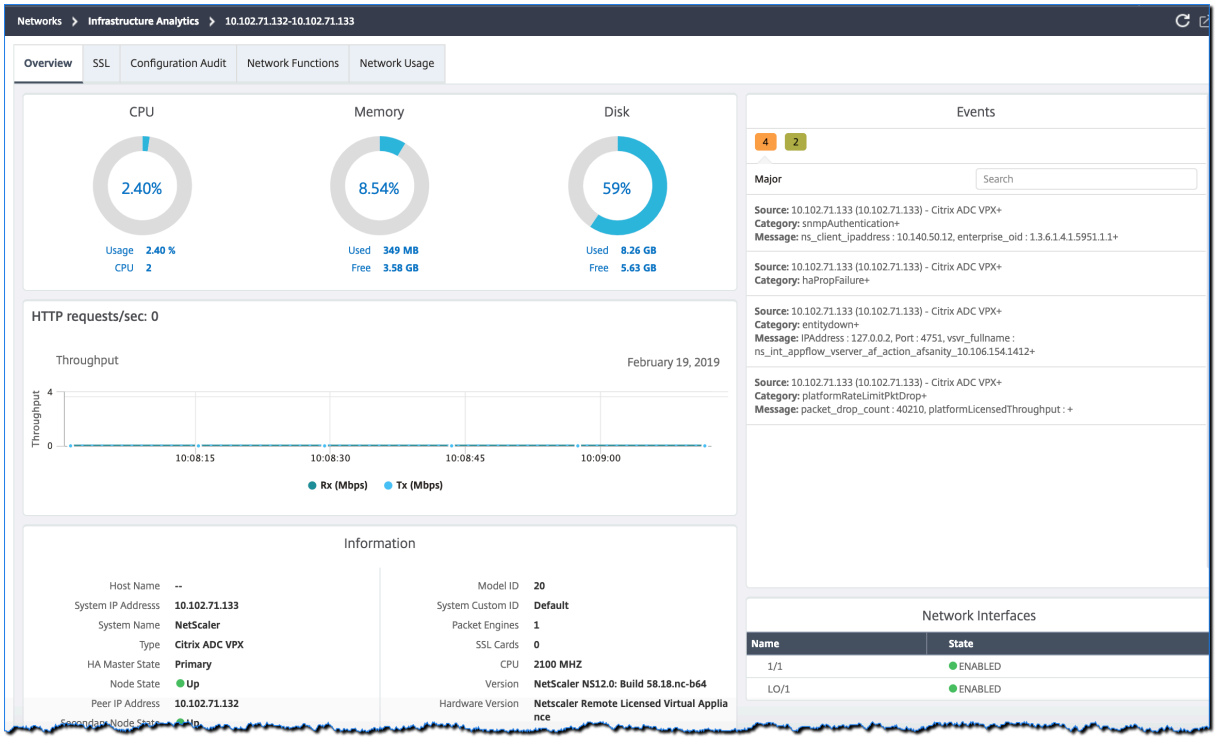
In der tabellarischen Ansicht werden die Instanzen und die Details dieser Instanzen in einem tabellarischen Format angezeigt. Die Details, die angezeigt werden, lauten wie folgt:

- Hostname der Instanz
- Die IP-Adresse der Instanz
- Status der Instanz
- Instanz-Score
- Anzahl der auf dieser Instanz konfigurierten virtuellen Server
- Anzahl der auf dieser Instanz konfigurierten Anwendungen
- Gesamtzahl der Risikoindikatoren
- Das Ereignis, das mehr zu einem niedrigeren Instanz-Score beiträgt

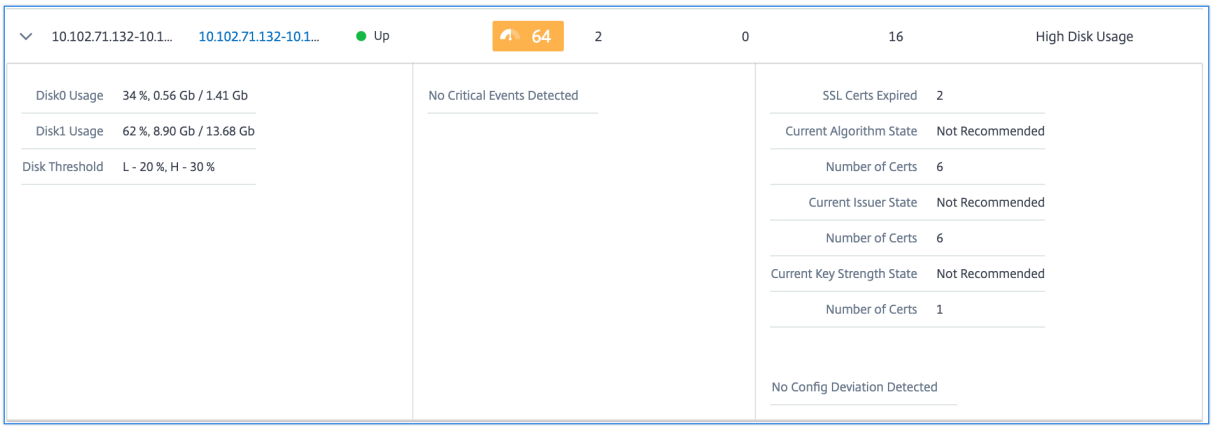
Die Instanzen, die sich im kritischen Zustand befinden, stehen ganz oben in der Tabelle, gefolgt von den Instanzen, die überprüft werden müssen, und dann den gesünderen Instanzen.



Klicken Sie in der tabellarischen Ansicht auf die IP-Adresse der Instanz, um weitere Details 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 zur SSL-Zertifikatsverwaltung, zur Konfigurationsprüfung, zu Netzwerkfunktionen sowie einen Netzwerkbericht einsehen, der die detaillierte Netzwerknutzung der Instanz zeigt. Scrollen Sie weiter nach unten, um die Liste der Funktionen und Modi zu sehen, die in dieser Instanz aktiviert sind.



Sie können auch auf den Pfeil am Anfang jeder Zeile klicken, um die Zeile für weitere Details zu erweitern.



In der erweiterten Tabellenzeile werden die Fehler angezeigt, die in der Instanz für alle Kategorien aufgetreten sind. Im obigen Beispiel können Sie sehen, dass Fehler in den Systemressourcen, der SSL-Konfiguration und Abweichungen in den Konfigurationsdateien aufgetreten sind. Aus der Instanz wurden jedoch keine kritischen Ereignisse gemeldet.

So verwenden Sie das Übersichts-Panel

Das **Zusammenfassungspanel** hilft Ihnen dabei, sich effizient und schnell auf die Fälle zu konzentrieren, die überprüft werden müssen oder in einem kritischen Zustand sind. Das Panel ist in drei

Registerkarten unterteilt: Übersicht, Instanzinformation und Verkehrsprofil. Durch die Änderungen, die Sie in diesem Fenster vornehmen, wird die Anzeige sowohl im Circle Pack- als auch im Tabellenansichtsformat geändert. In den folgenden Abschnitten werden diese Registerkarten ausführlicher beschrieben. Die Beispiele in den folgenden Abschnitten helfen Ihnen dabei, die verschiedenen Auswahlkriterien effizient zu verwenden, um die von den Instanzen gemeldeten Probleme zu analysieren.

Überblick:

Auf der Registerkarte **Übersicht** können Sie die Instanzen basierend auf Hardwarefehlern, Nutzung, 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
- Systemausfälle
- Kritische Ereignisse
- Ablauf von SSL-Zertifikaten

Die folgenden Beispiele veranschaulichen, wie Sie mit dem **Übersichtsfenster** interagieren können, um die Instanzen zu isolieren, die Fehler melden.

Beispiel 1: Zeigen Sie Instanzen an, die sich in einem 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% bewertet. 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.

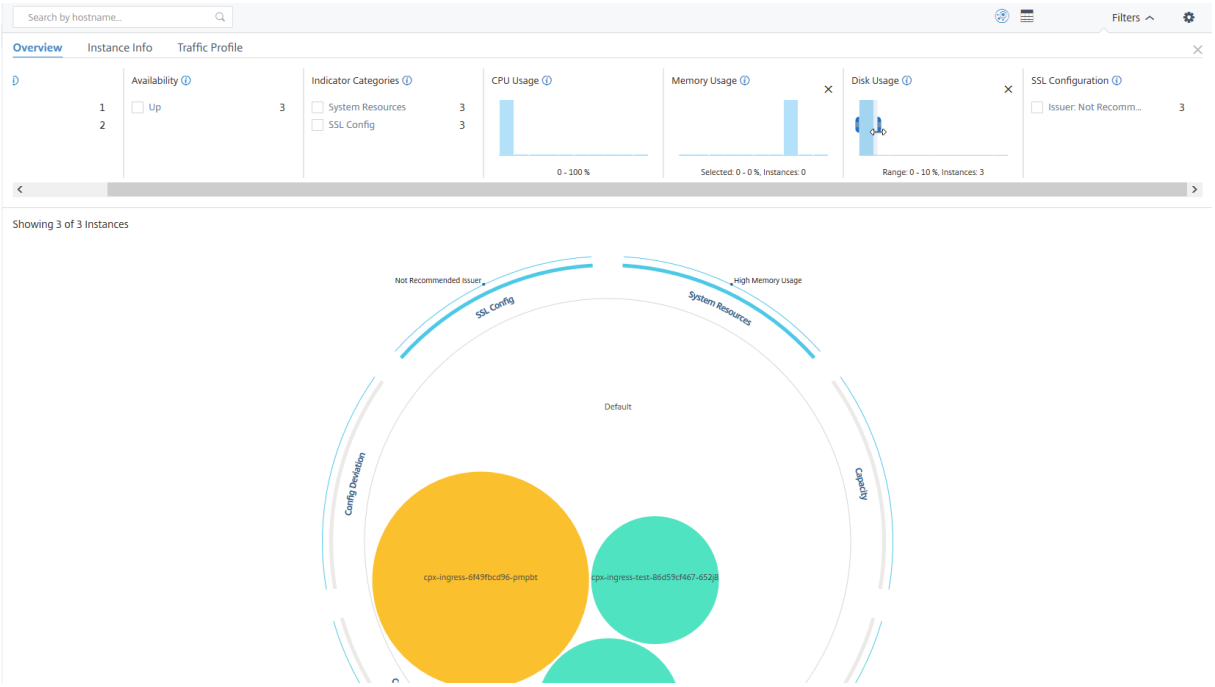
Beispiel 2: Zeigen Sie Instanzen an, die zwischen 10 und 20% des zugewiesenen Speichers verbrauchen:

Klicken Sie im Abschnitt Speicherverbrauch auf das Balkendiagramm. Die Legende zeigt, dass der ausgewählte Bereich zwischen 10 und 20% liegt und 29 Instanzen in diesem Bereich arbeiten.

Sie können in diesen Histogrammen auch mehrere Bereiche auswählen.

Beispiel 3: Instances anzeigen, die in mehreren Bereichen viel Speicherplatz beanspruchen:

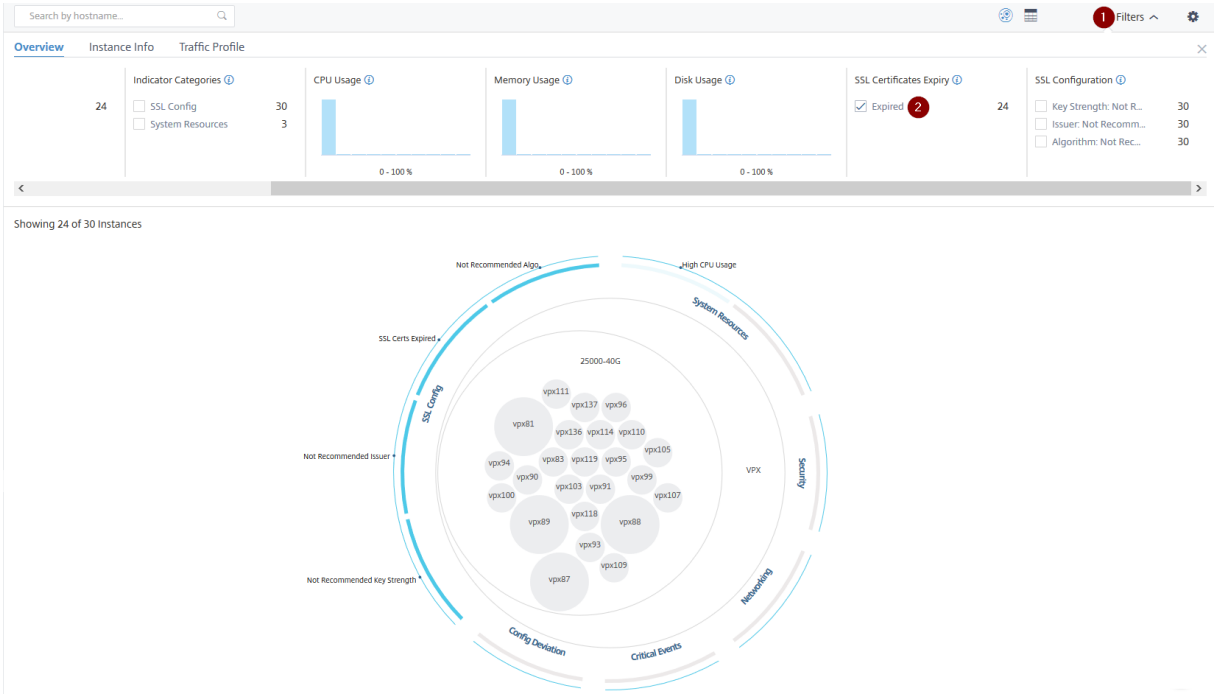
Um Instanzen anzuzeigen, die Speicherplatz zwischen 0 und 10% belegt haben, ziehen Sie den Mauszeiger über die beiden Bereiche.



> **Hinweis**
>
> Klicken Sie auf “X”, um die Auswahl zu entfernen. Sie können auch auf **Zurücksetzen** klicken, um Mehrfachauswahlen zu entfernen.

Die horizontalen Balkendiagramme im **Übersichtsfenster** zeigen 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: Zeigen Sie Instanzen für abgelaufene SSL-Zertifikate an:



1 —Klicken Sie auf die **Filterliste** .

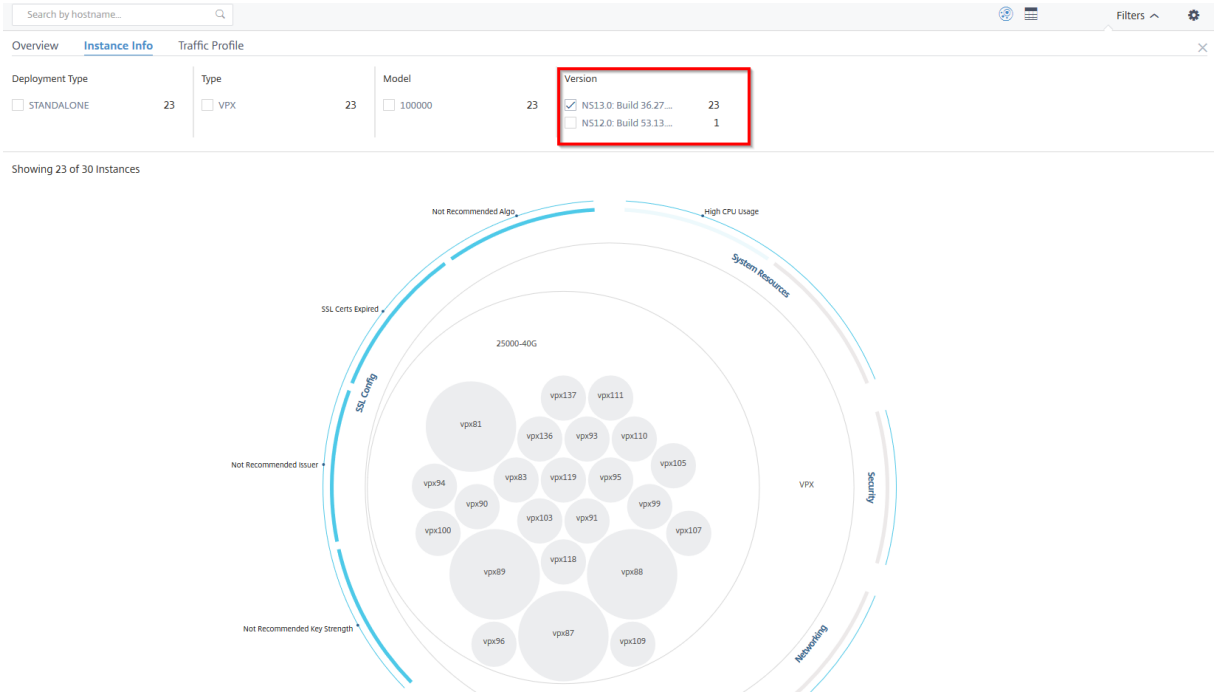
2 —Aktivieren Sie im Abschnitt **Ablauf von SSL-Zertifikaten** das Kontrollkästchen **Abgelaufen**, um die Instanzen anzuzeigen.

Instanzinformationen

Im Bereich **Instanzinformationen** können Sie Instanzen basierend auf dem Bereitstellungstyp, dem Instanztyp, dem Modell und der Softwareversion anzeigen. Sie können mehrere Kontrollkästchen aktivieren, um Ihre Auswahl einzugrenzen.

Beispiel 5: Zeigen Sie NetScaler VPX-Instanzen mit einer bestimmten Build-Nummer an:

Wählen Sie die Version aus, die Sie anzeigen möchten.



Traffic-Profil

Die Histogramme im Bereich **Traffic-Profil** stellen eine aggregierte Anzahl von Instanzen dar, die auf dem lizenzierten Durchsatz der Instanzen, der Anzahl der Anfragen, Verbindungen und Transaktionen basieren, die von den Instanzen verarbeitet werden. Wählen Sie das Balkendiagramm aus, um Instanzen in diesem Bereich anzuzeigen.

Beispiel 6: Instanzen anzeigen, die TCP-Verbindungen unterstützen:

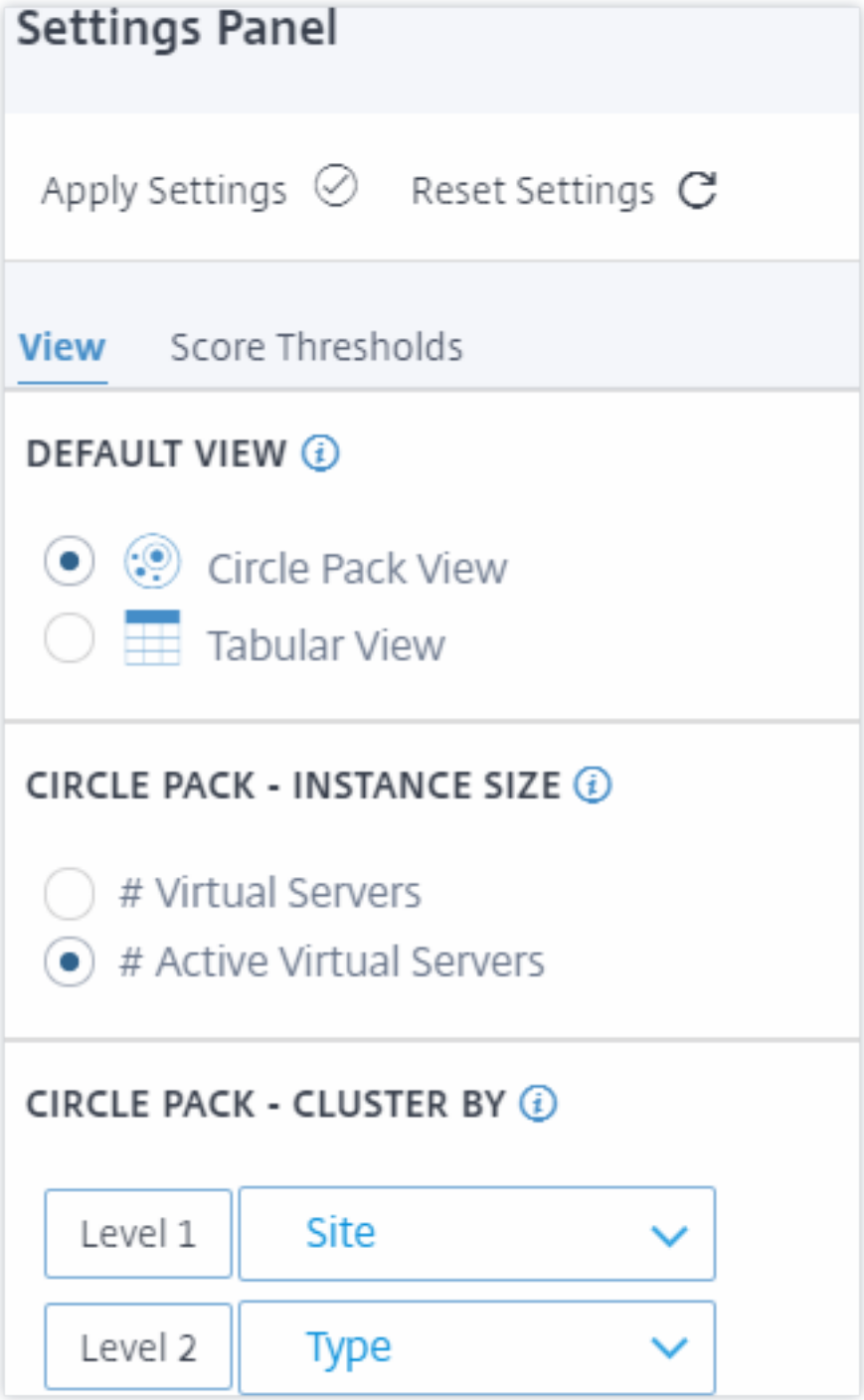
Die folgende Abbildung zeigt die Anzahl der Instanzen, die TCP-Verbindungen unterstützen.

So verwenden Sie das Einstellungsfeld

Im Bereich **Einstellungen** können Sie die Standardansicht von 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 Tabs unterteilt: Ansicht und Punktegrenzwerte.

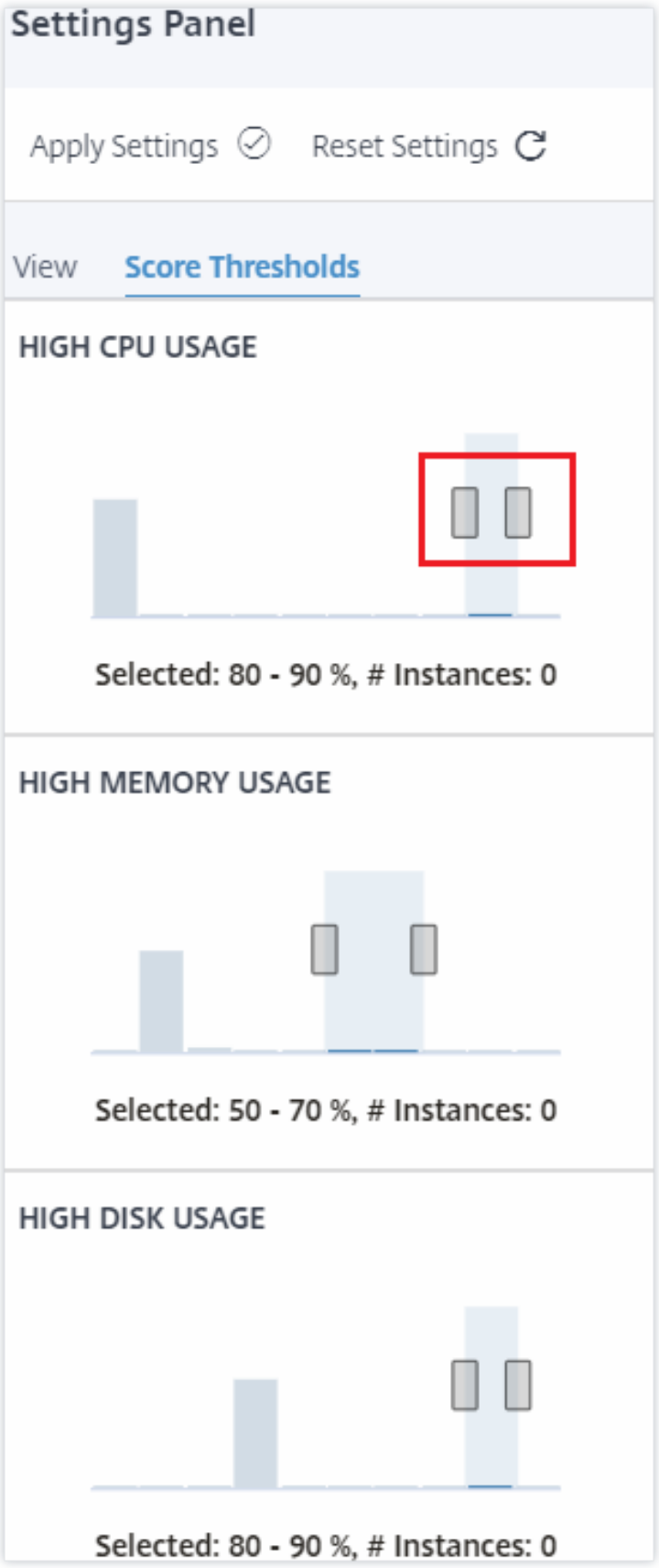
View

- **Standardansicht**. Wählen Sie **Circle Pack** oder Tabellarisches Format als Standardansicht auf der Analyseseite aus. Das Format, das Sie auswählen, wird angezeigt, wenn Sie in NetScaler ADM auf die Seite zugreifen.
- **Circle Pack —Instanzgröße**. Lässt die Größe des Instanzkreises entweder auf die Anzahl der virtuellen Server oder die Anzahl der aktiven virtuellen Server zu.
- **Circle Pack - Cluster von**. Entscheiden Sie sich für das zweistufige Clustering der Instanzkreise. Weitere Informationen zum Instanzclustering finden Sie unter Clustered Exemplarkreise.



Score-Schwellenwerte

Sie können die niedrigen und hohen Schwellenwerte für eine hohe CPU-, Arbeitsspeicher- und Festplattenauslastung je nach den Datenverkehrsanforderungen in Ihrem Unternehmen ändern. Ziehen Sie die Griffe in jedem der Auswahlhistogramme, um die Werte festzulegen.



> **Hinweis:**
>
> Klicken Sie auf **Einstellungen übernehmen**, um diese Änderungen zu übernehmen, 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 die meiste Aufmerksamkeit benötigen, innerhalb weniger Sekunden. Um die Datenvisualisierung genauer zu verstehen, betrachten wir den Fall von Chris, einem Netzwerkadministrator von Example-Company.

Chris verwaltet viele NetScaler-Instanzen in der Organisation. Einige der Instanzen verarbeiten viel Traffic, und Chris muss sie genau beobachten. Chris stellt fest, dass einige stark frequentierte Instances nicht mehr den gesamten Traffic verarbeiten, der durch sie fließt. Um diesen Rückgang zu analysieren, musste Chris zuvor mehrere Datenberichte aus verschiedenen Quellen lesen. Chris musste mehr Zeit damit verbringen, die Daten manuell zu korrelieren und festzustellen, welche Instanzen sich nicht in einem optimalen Zustand befinden und Aufmerksamkeit erfordern.

Chris verwendet die Infrastructure Analytics-Funktion, um den Zustand aller Instanzen visuell zu sehen.

Die folgenden zwei Beispiele veranschaulichen, wie Infrastructure Analytics Chris bei Wartungsaktivitäten unterstützt:

Beispiel 1 - So überwachen Sie den SSL-Verkehr:

Chris bemerkt im Circle Pack, dass eine Instanz einen niedrigen Instanzwert hat und sich diese Instanz im Status “Kritisch”befindet. Chris klickt auf diese Instanz, um zu sehen, was das Problem ist. In der Instanzübersicht wird angezeigt, dass auf dieser Instanz ein SSL-Kartenfehler aufgetreten ist und die Instanz keinen SSL-Verkehr verarbeiten kann (der SSL-Verkehr wurde reduziert). Chris extrahiert diese Informationen und sendet einen Bericht an das Team, um das Problem sofort zu untersuchen.

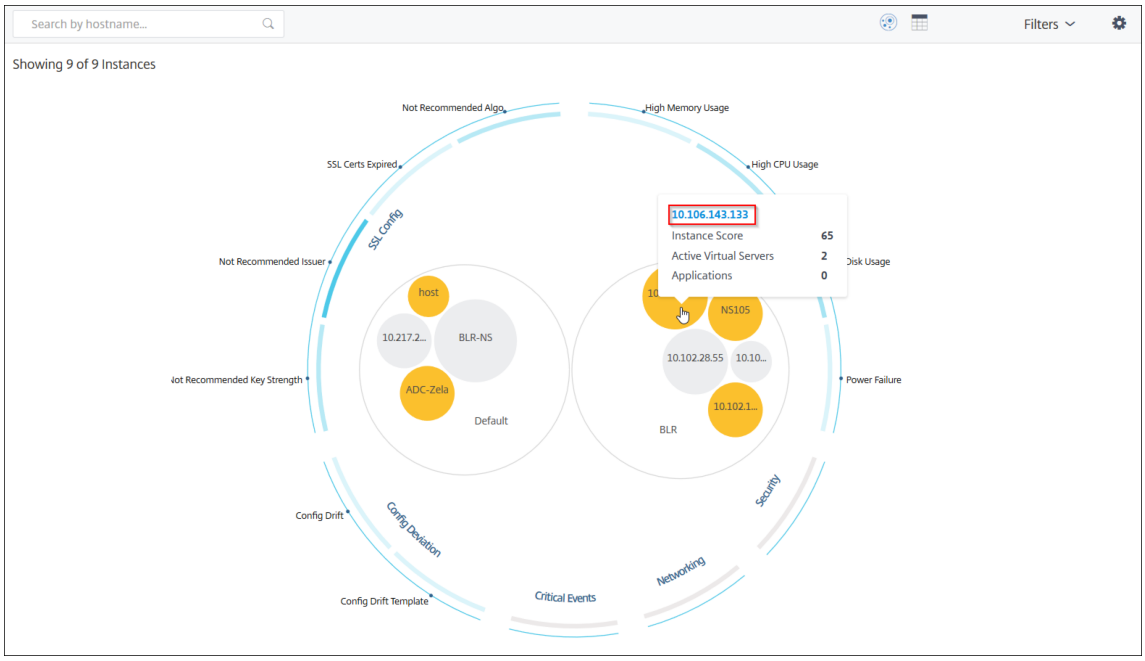
Beispiel 2 - So überwachen Sie Konfigurationsänderungen:

Chris bemerkt auch, dass sich eine andere Instanz im Status “Überprüfung”befindet und dass es in letzter Zeit eine Konfigurationsabweichung gegeben hat. Wenn Chris auf den Risikoindikator für Konfigurationsabweichungen klickt, bemerkt Chris, dass Konfigurationsänderungen im Zusammenhang mit RC4 Cipher, SSL v3, TLS 1.0 und TLS 1.1 vorgenommen wurden, die möglicherweise auf Sicherheitsbedenken zurückzuführen sind. Chris stellt außerdem fest, dass das SSL-Transaktions-Traffic-Profil für diese Instanz ausgefallen ist. Chris exportiert diesen Bericht und sendet ihn an den Administrator, um weitere Informationen zu erhalten.

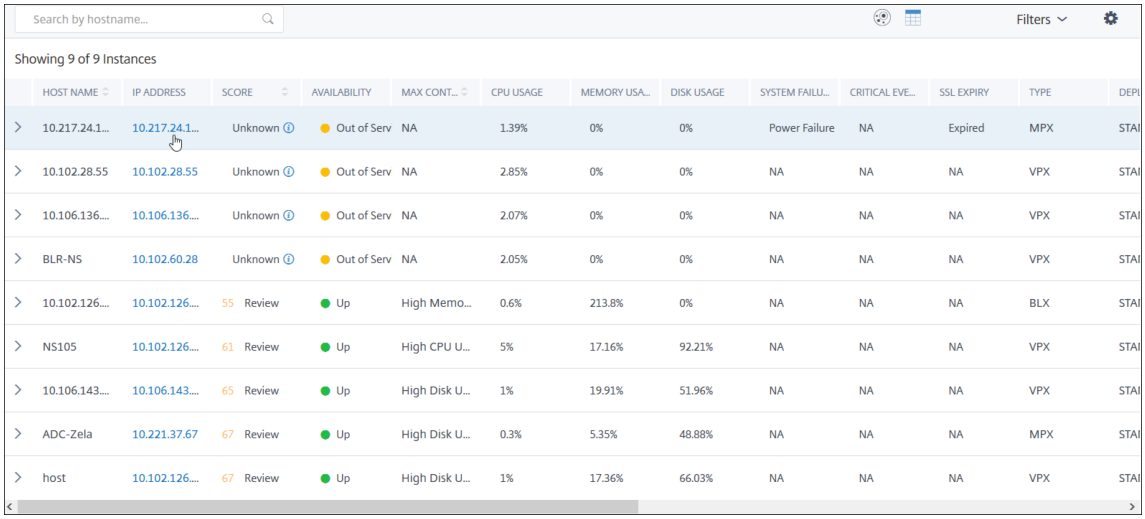
Instanzdetails in Infrastructure Analytics anzeigen

February 5, 2024

1. Navigieren Sie zu **Infrastruktur > Infrastructure Analytics**
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** —Bezeichnet den Hostnamen, der der ADC-Instanz zugewiesen ist
- **IP-Adresse** —Gibt die IP-Adresse der ADC-Instanz an
- **Score** —Gibt den ADC-Instanz-Score und den Status wie Kritisch, Gut und Fair an

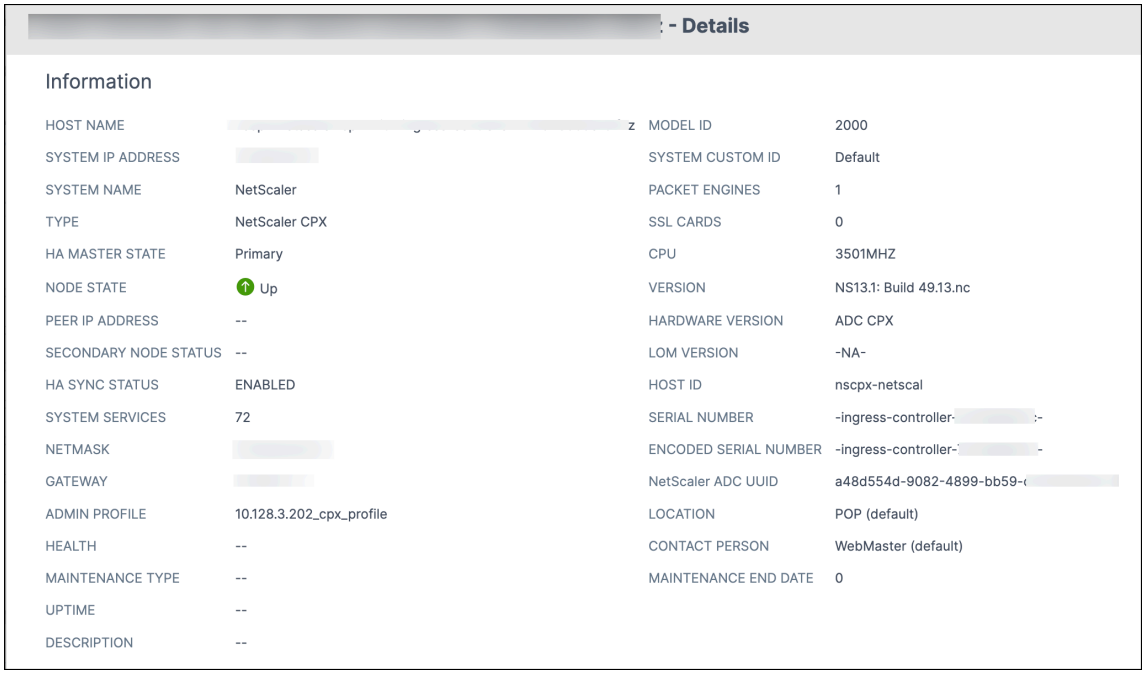
- **Verfügbarkeit** —Gibt den Status der ADC-Instance an, z. B. **Up**, **Down**oder **Out of Service**.
- **Max. Beitrag** —Gibt die Problemkategorie an, in der die ADC-Instanz die maximale Fehleranzahl aufweist.
- **CPU-Auslastung** —Gibt den aktuellen CPU-Prozentsatz an, der von der Instanz verwendet wird
- **Speichernutzung** —Gibt den aktuellen Speicherprozentsatz an, der von der Instanz verwendet wird
- **Datenträgernutzung** —Gibt den aktuellen Datenträgerprozentsatz an, der von der Instanz verwendet
- **Systemfehler** —Gibt die Gesamtzahl der Fehler für das Instanzsystem an
- **Kritische Ereignisse** —Bezeichnet die Ereigniskategorie, in der die NetScaler-Instanz die maximalen Ereignisse aufweist.
- **SSL-Ablauf** —Gibt den Status des auf der ADC-Instanz installierten SSL-Zertifikats an
- **Typ** —Bezeichnet den ADC-Instanztyp wie VPX, SDX, MPX oder CPX
- **Bereitstellung** —Gibt an, ob die ADC-Instanz als eigenständige Instanz oder HA-Paar bereitgestellt wird
- **Modell** —Bezeichnet die Modellnummer der ADC-Instanz
- **Version** —Bezeichnet die ADC-Instanzversion und Build-Nummer
- **Durchsatz** —Gibt den aktuellen Netzwerkdurchsatz von der ADC-Instanz an.
- **HTTPS-Anforderung/Sekunde** —Bezeichnet die aktuellen HTTPS-Anforderungen/s, die von der ADC-Instanz empfangen wurden
- **TCP-Verbindung** —Bezeichnet die aktuell aufgebauten TCP-Verbindungen
- **SSL-Transaktion** —bezeichnet die aktuellen SSL-Transaktionen, die von der ADC-Instanz verarbeitet werden
- **Site** —Gibt den Namen der Site an, auf der die ADC-Instanz bereitgestellt wird.

> **Hinweis**
>
> Alle 5 Minuten werden die aktuellen Werte für CPU-Auslastung, Speichernutzung, Datenträgerauslastung, Durchsatz usw. aktualisiert.

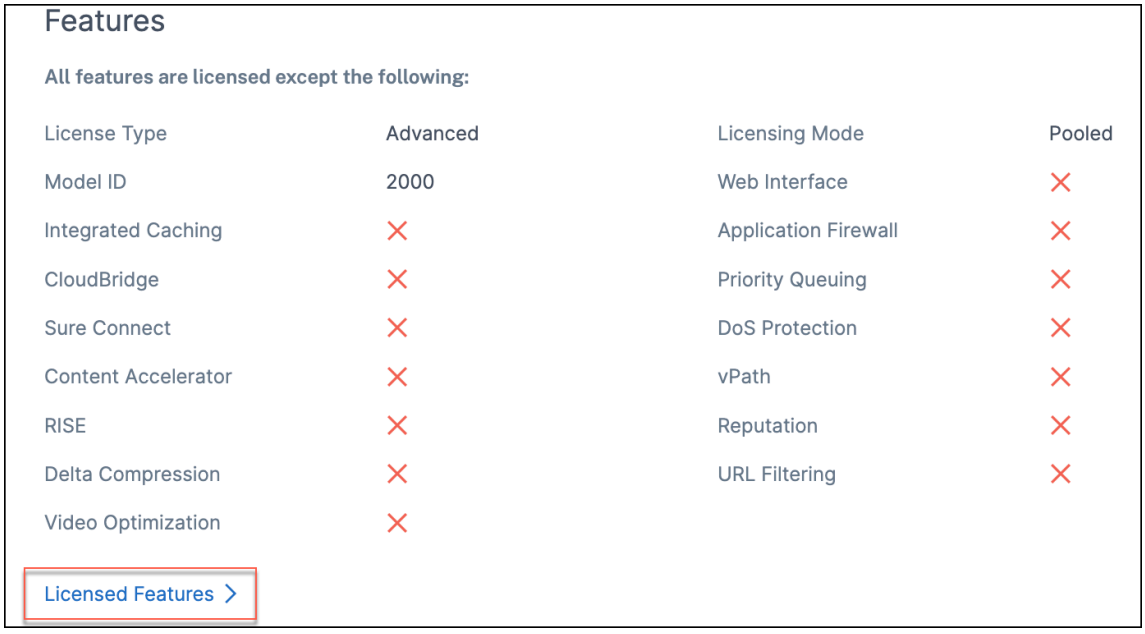
Klicken Sie auf **Instanzdetails**, um die Details anzuzeigen.

Die folgenden Details werden angezeigt:

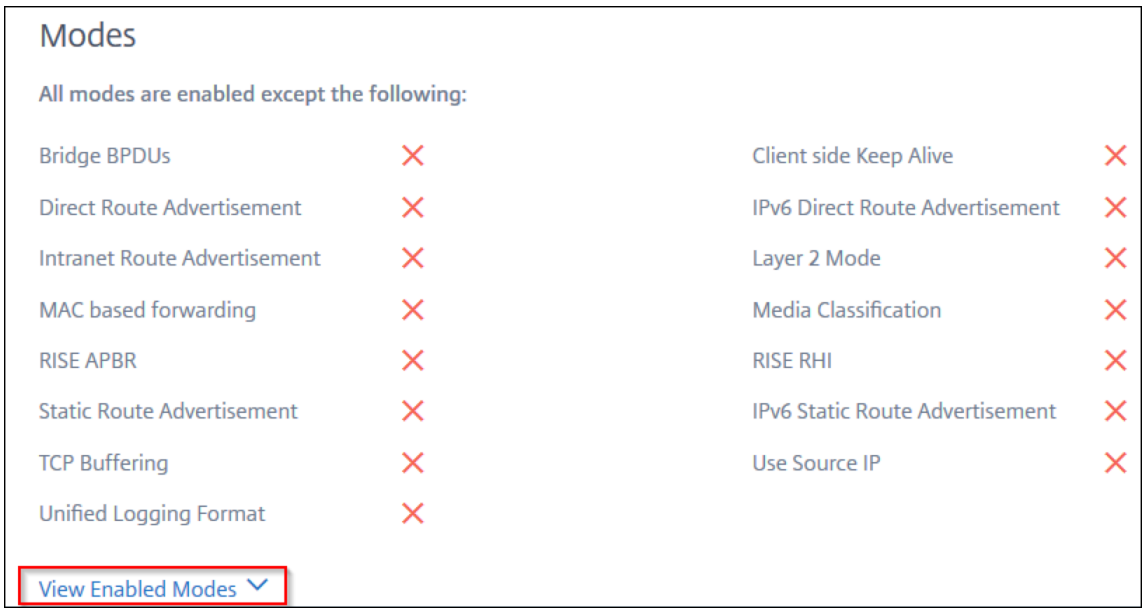
- **Informationen** —Instanzdetails wie Instanztyp, Bereitstellungstyp, Version, Modell.



- **Funktionen** —Standardmäßig werden die Funktionen angezeigt, die nicht lizenziert sind. Klicken Sie auf **Lizenzierte Funktionen**, um die lizenzierten Funktionen anzuzeigen.

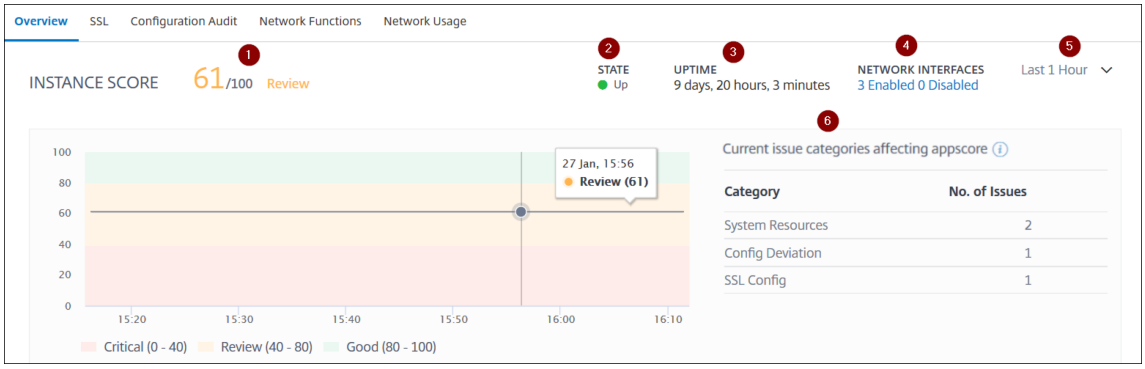


- **Modi** —Standardmäßig werden alle Modi angezeigt, die auf der Instanz deaktiviert sind. Klicken Sie auf **Aktivierte Modi** anzeigen, um die aktivierten Modi auf der Instanz anzuzeigen.



Das Instanz-Dashboard bietet eine Instanzübersicht, in der Sie die folgenden Details sehen können:

- **Instanz-Score**



1 —Gibt die aktuelle NetScaler-Instanzbewertung für die ausgewählte Zeitdauer an. Das Endergebnis wird als **100 minus Gesamtstrafen**berechnet. Das Diagramm zeigt die Score-Bereiche für die ausgewählte Zeitdauer an.

2 —Zeigt den Status der NetScaler-Instanz an, z. B. **Up**, **Down**und **Out of Service**.

3 —Gibt die Dauer an, die die NetScaler-Instanz ausgeführt wird.

4 —Zeigt die Gesamtzahl der für die Instanz aktivierten und deaktivierten Netzwerkschnittstellen an. Klicken Sie hier, um Details wie den Namen der Netzwerkschnittstelle und den Status (aktiviert oder deaktiviert) anzuzeigen.

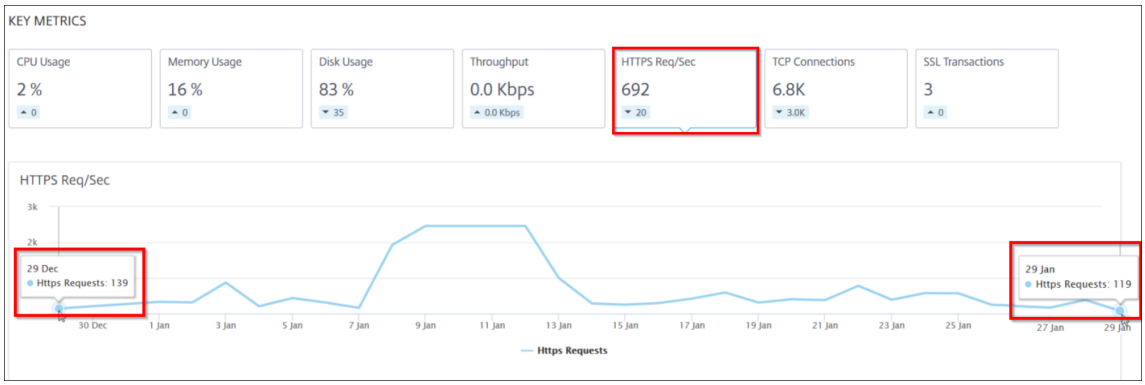
5 —Wählen Sie die Zeitdauer aus der Liste aus, um die Instanzdetails anzuzeigen.

6 —Zeigt die Gesamtzahl der Probleme und die Problemkategorie der ADC-Instanz an.

- **Wichtige Metriken**

Klicken Sie auf jede Registerkarte, 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 gewählte Zeitdauer beträgt 1 Stunde. Der Wert **692** ist der durchschnittliche HTTPS-Req/Sek für die Dauer von 1 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 für die ausgewählte Zeitdauer in einem Diagrammformat anzeigen:

- **CPU-Auslastung** —Der durchschnittliche CPU-Prozentsatz der Instanz für die ausgewählte Dauer (wird sowohl für die Paket-CPU als auch für die Verwaltungs-CPU angezeigt).
- **Speichernutzung** —Die durchschnittliche Speichernutzung in% der Instanz für die ausgewählte Dauer.
- **Datenträgernutzung** —Der durchschnittliche Speicherplatz in % der Instanz für die ausgewählte Dauer.
- **Durchsatz** —Der durchschnittliche Netzwerkdurchsatz, der von der Instanz für die ausgewählte Dauer verarbeitet wird.
- **HTTPS-Anforderung/Sekunde** —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 eingerichtet wurden.
- **SSL-Transaktionen** —Die durchschnittlichen SSL-Transaktionen, die von der Instanz für die ausgewählte Dauer verarbeitet wurden.

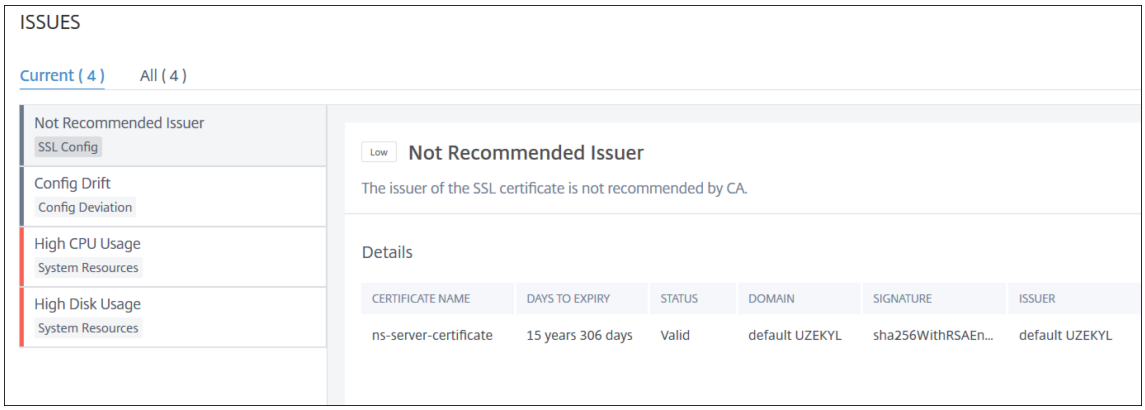
- **Probleme**

  Sie können die folgenden Probleme anzeigen, die in der NetScaler-Instanz auftreten:

Kategorie der Ausgabe	Beschreibung	Probleme
Systemressourcen	Zeigt alle Probleme im Zusammenhang mit der NetScaler-Systemressource wie CPU, Arbeitsspeicher und Festplattenauslastung an.	– Hohe CPU-Auslastung – Hoher Speicherverbrauch – Hohe Datenträgernutzung – SSL-Kartenfehler – Stromausfall – Datenträgerfehler – Flashfehler – NIC Discards
SSL-Konfiguration	Zeigt alle Probleme im Zusammenhang mit der SSL-Konfiguration auf der NetScaler-Instanz an.	– SSL-Zertifikate sind abgelaufen – Nicht empfohlener Herausgeber – Nicht empfohlener Algorithmus – Nicht empfohlene Schlüsselstärke
Abweichung der Konfiguration	Zeigt alle Probleme im Zusammenhang mit den Konfigurationsaufträgen an, die in der NetScaler-Instanz angewendet werden.	– Konfigurationsdrift – Running vs Template
Kritische Ereignisse	Zeigt alle kritischen Ereignisse im Zusammenhang mit NetScaler-Instanzen an, die im HA-Paar und im Cluster konfiguriert sind.	– Ausfall von Cluster Prop

Kategorie der Ausgabe	Beschreibung	Probleme
Netzwerke	Zeigt die Betriebsprobleme an, die in den Instanzen auftreten.	– Fehler bei der Cluster – Nicht übereinstimmende Cluster-Versionen – HA Schlechter Sekundärstaat – HA Keine Hitze schlägt – HA-Synchronisierungsfehler – Nichtübereinstimmung der HA-Version Weitere Informationen finden Sie unter Verbesserte Infrastrukturanalyse mit neuen Indikatoren.

Klicken Sie auf die einzelnen Registerkarten, um das Problem zu analysieren und zu beheben. Stellen Sie sich beispielsweise vor, dass eine Instanz für die ausgewählte Zeitdauer die folgenden Fehler 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

February 5, 2024

Wenn eine ADC-Instanz den größten Teil ihrer verfügbaren Kapazität verbraucht hat, kann es während der Verarbeitung des Client-Datenverkehrs zu einem Paket-Drop kommen. Dieses Problem führt zu einer geringen 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 **Infrastruktur > Infrastructure Analytics**.
2. Wählen Sie die Ansicht des Kreispakets aus.

> **Hinweis**
>
> In **Infrastructure Analytics**zeigen das Circle-Pack und die tabellarischen Ansichten die Ereignisse und Probleme an, die in der letzten Stunde aufgetreten sind.

Die folgende Abbildung legt nahe, dass die Kapazitätsprobleme in der ausgewählten Instanz auftreten:

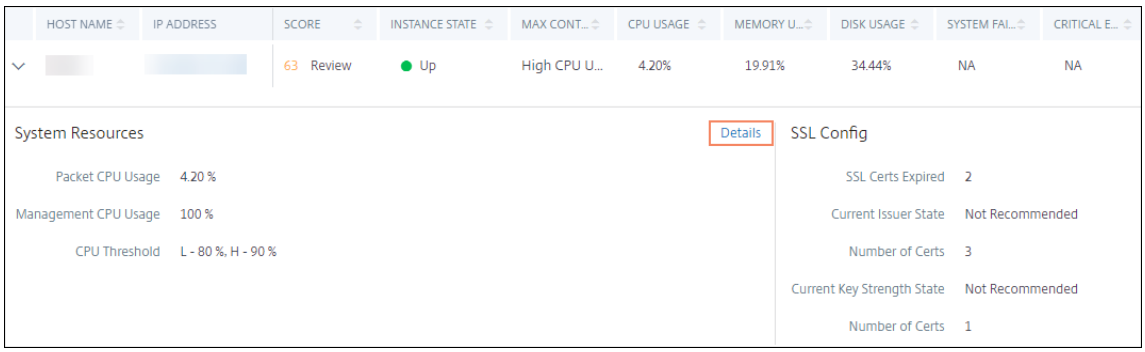
Die Probleme sind nach den folgenden Kapazitätsparametern kategorisiert:

- **Durchsatzlimit erreicht** —Die Anzahl der Pakete, die in der Instanz nach Erreichen des Durchsatzlimits verworfen wurden.
- **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 verworfen wurden, nachdem das PPS-Limit erreicht wurde.
- **SSL-Durchsatzrate Limit** —Gibt an, wie oft das SSL-Durchsatzlimit erreicht wurde.
- **SSL-TPS-Ratenlimit** —Gibt an, wie oft das SSL-TPS-Limit erreicht wurde.

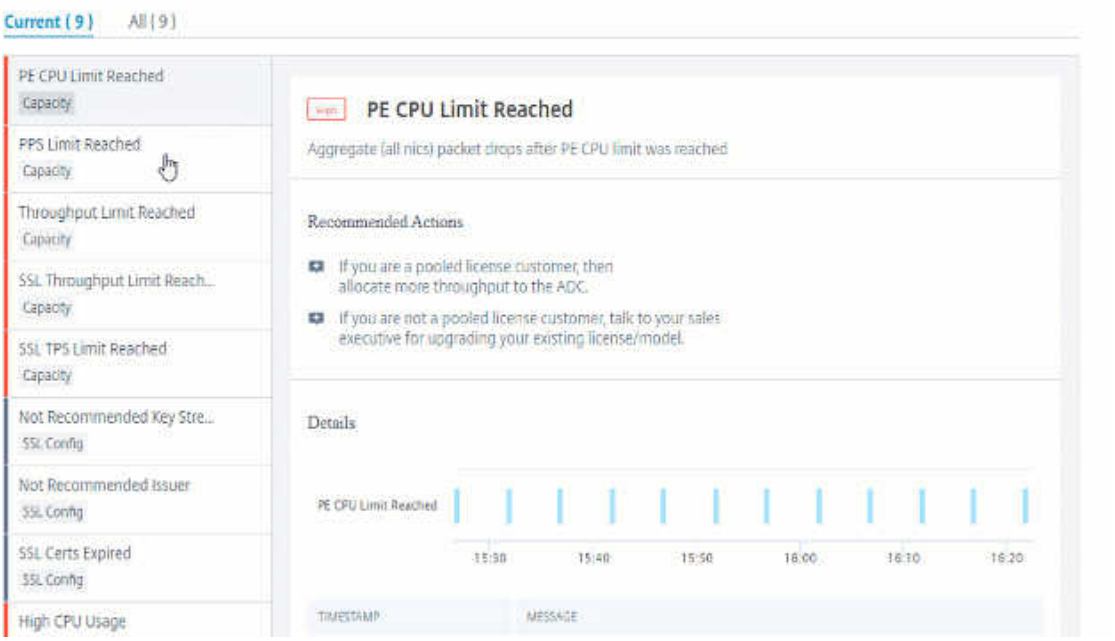
Empfohlene Maßnahmen zur Lösung von Kapazitätsproblemen anzeigen

Der ADM empfiehlt Maßnahmen, mit denen Kapazitätsprobleme gelöst werden können. Führen Sie die folgenden Schritte aus, um die empfohlenen Aktionen anzuzeigen:

1. Wählen Sie unter **Infrastruktur > 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 Maßnahmen zur Behebung von Kapazitätsproblemen 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.

Das ADM berechnet die Instanzbewertung anhand des definierten Kapazitätsschwellenwerts.

- **Niedriger Schwellenwert** —1 Zählerinkrement für Paketverlust oder Ratenbegrenzung
- **Hoher Schwellenwert** —10.000 Paketverlust oder Erhöhung des Ratenlimit-Zählers

Wenn eine ADC-Instanz den Kapazitätsschwellenwert überschreitet, wirkt sich dies auf den Instanzwert aus.

Wenn Pakete fallen oder der Zähler für die Ratenbegrenzung inkrementiert wird, wird ein Ereignis in der Kategorie `ADCCapacityBreach` generiert. Um diese Ereignisse einzusehen, navigieren Sie zu **Konten > Systemereignisse**.

Verbesserte Infrastrukturanalyse mit neuen Indikatoren

February 5, 2024

Mit NetScaler ADM Infrastructure Analyticskönnen Sie:

- Zeigen Sie eine neue Reihe von Betriebsproblemen an, die in NetScaler-Instanzen auftreten.
- Zeigen Sie Fehlermeldungen an und überprüfen Sie Empfehlungen zur Behebung der Probleme.

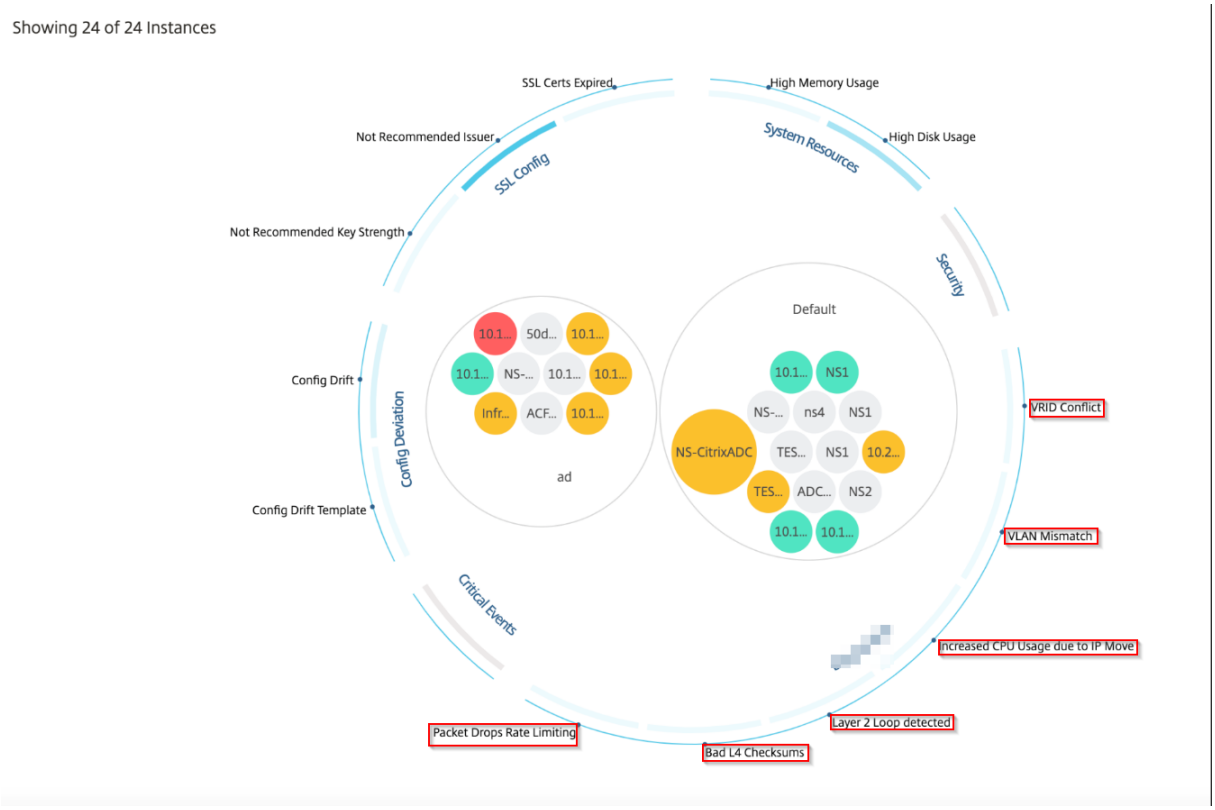
Als Administrator können Sie schnell die Ursachenanalyse von Problemen identifizieren.

> **Hinweis**
>
> Regelindikatoren werden nicht unterstützt für:
>
> - NetScaler-Instanzen, die im Clustermodus konfiguriert sind.
> - NetScaler-Instanzen, die mit Administratorpartitionen konfiguriert sind.

Navigieren Sie in NetScaler ADM zu **Infrastructure > Infrastructure Analytics**, um Indikatoren anzuzeigen für:

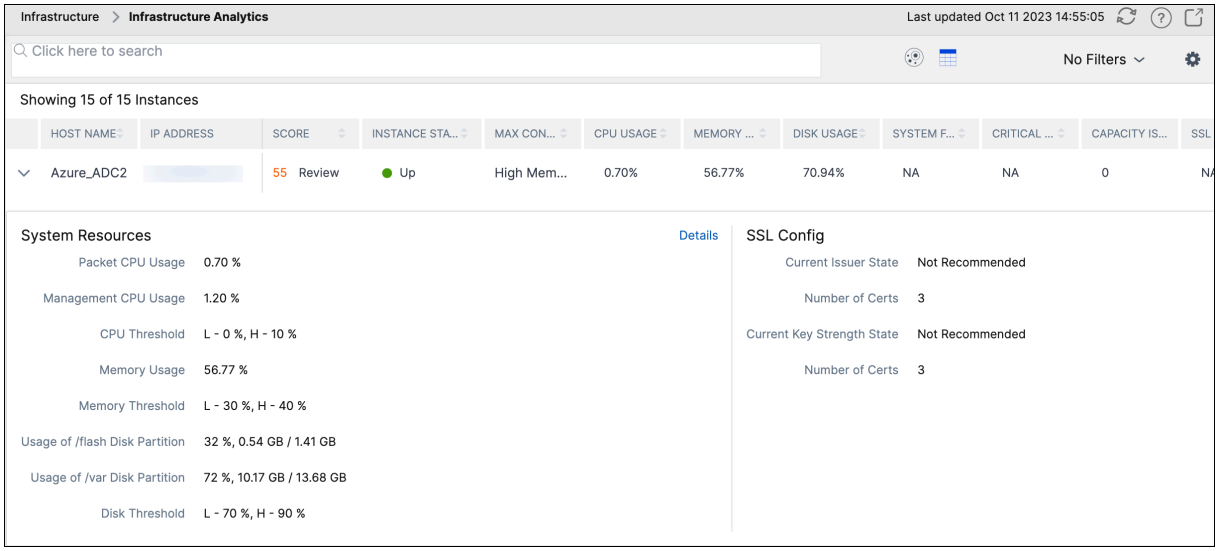
Indikatorname in Infrastructure Analytics	Beschreibung
Fehler bei Portzuweisung	Erkennt, wenn NetScaler SNIP verwendet, um mit einer neuen Serververbindung zu kommunizieren, und die Gesamtzahl der auf diesem SNIP verfügbaren Ports erschöpft ist. Die empfohlene Aktion besteht darin, ein weiteres SNIP im selben Subnetz hinzuzufügen.
Keine Standard-Routenkonfiguration	Erkennt, wenn der Datenverkehr aufgrund der Nichtverfügbarkeit von Routen unterbrochen wird.
IP-Konflikt	Erkennt, ob dieselbe IP-Adresse auf zwei oder mehr Instanzen in einem Netzwerk konfiguriert oder angewendet wurde.
VRID-Konflikt	Erkennt, wenn zeitweise Zugriffsprobleme für die angegebene VRID auftreten.
VLAN-Nichtübereinstimmung	Erkennt, ob während der an IP-Subnetze gebundenen VLAN-Konfiguration Fehler auftreten.

Indikatorname in Infrastructure Analytics	Beschreibung
TCP-Angriff auf kleine Fenster	Erkennt, wenn möglicherweise ein kleiner Fensterangriff im Gange ist. Diese Warnung dient nur zur Information, da ADC diesen Angriff bereits abwehrt.
Schwellenwert für die Rat	Erkennt basierend auf dem konfigurierten Schwellenwert für die Ratenkontrolle, wenn Pakete verworfen
Persistenz-Limit	Erkennt, wann maximale Treffer auf den NetScaler-Speicher angewendet werden.
Nichtübereinstimmung mit GSLB-Site-	Erkennt, wenn GSLB-Konfigurationssynchronisierungsfehler aufgrund einer Nichtübereinstimmung des Site-Namens auftreten
Falscher IP-Header	Erkennt, wenn Plausibilitätsprüfungen für IPv4-Pakete fehlgeschlagen sind.
Schlechte L4-Prüfsumme	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 ein hohes Maß an Softwarepaketsteuerung aufgrund der Verwendung eines asymmetrischen RSS-Schlüsseltyps.
Layer-2-Schleife	Erkennt das Vorhandensein von Layer-2-Schleifen im Netzwerk.
Getaggt: VLAN mismatch	Erkennt, wenn markierte VLAN-Pakete auf einer Schnittstelle ohne Tags empfangen werden.



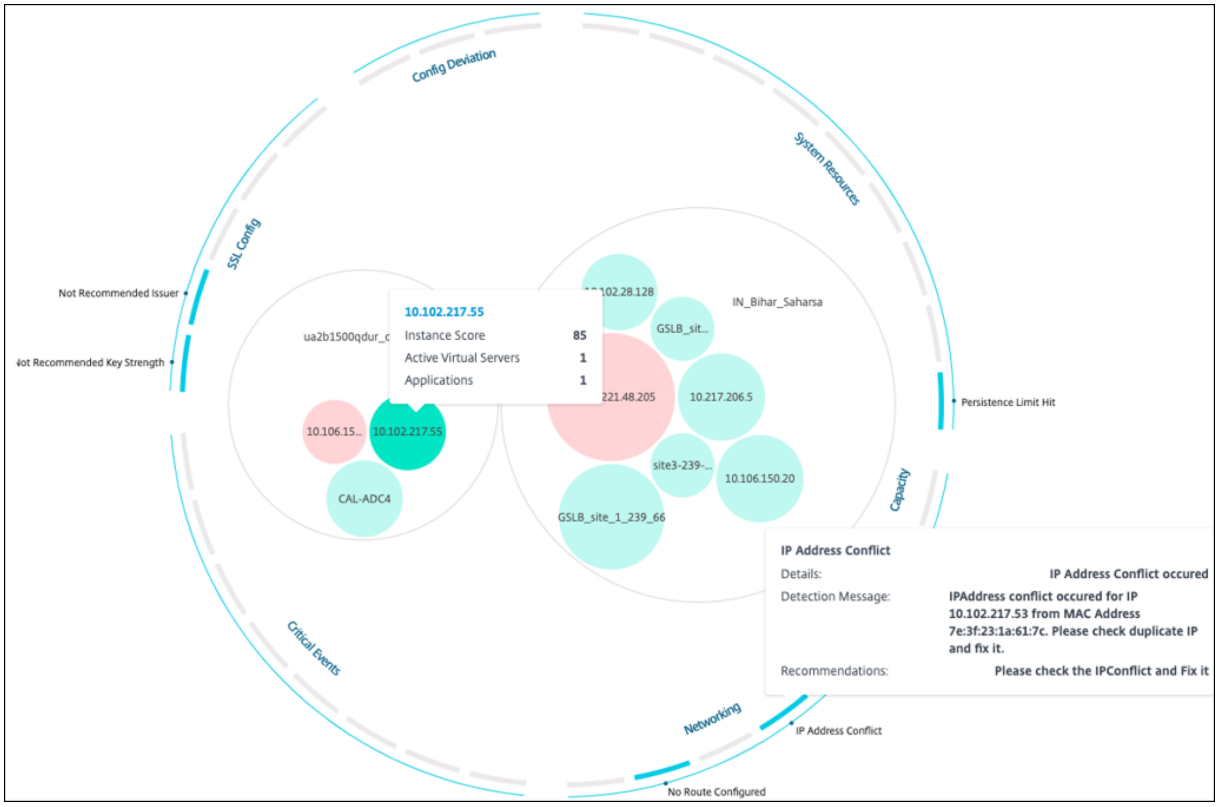
Tabellarische Ansicht

Sie können auch Anomalien anzeigen, indem Sie die Option Tabellenansicht in **Infrastructure Analytics**verwenden. Navigieren Sie zu **Infrastructure > Infrastructure Analytics**, und klicken Sie dann auf , um alle verwalteten Instanzen anzuzeigen. Klicken Sie auf , um weitere Informationen anzuzeigen.



Details einer Anomalie anzeigen

Wenn Sie beispielsweise Details zu **IP-Adresskonflikten** im Netzwerk anzeigen möchten, klicken Sie auf die Anomalie, die für den IP-Adresskonflikt angezeigt wird, um die Details anzuzeigen.



- **Details** - Zeigt an, welche Anomalie festgestellt wurde
- **Erkennungsmeldung** —Zeigt die MAC-Adresse an, für die die IP-Adresse den Konflikt hat
- **Empfehlungen** —Gibt das Aktionselement zur Lösung dieses IP-Adresskonflikts an

Instanzverwaltung

February 5, 2024

Instanzen sind Citrix Application Delivery Controller (ADC) -Appliances, die Sie mithilfe von NetScaler Application Delivery Management (ADM) verwalten, überwachen und Fehler beheben können. Sie müssen Instanzen zu NetScaler ADM hinzufügen, um sie zu überwachen. Instanzen können hinzugefügt werden, wenn Sie NetScaler ADM oder später einrichten. Nachdem Sie NetScaler 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 usw. ausführen möchten. Ein privater IP-Block gruppiert Ihre Instanzen basierend auf ihren geografischen Standorten.

Eine Instanz hinzufügen

Sie können Instanzen hinzufügen, wenn Sie den NetScaler ADM-Server zum ersten Mal oder später einrichten. Um Instanzen hinzuzufügen, müssen Sie entweder den Hostnamen oder die IP-Adresse jeder NetScaler-Instanz oder einen Bereich von IP-Adressen angeben.

Informationen zum Hinzufügen einer Instanz zu NetScaler ADM finden Sie unter Hinzufügen von Instanzen zu NetScaler ADM.

Wenn Sie dem NetScaler ADM -Server eine Instanz hinzufügen, fügt sich der Server implizit als Trap-Ziel für die Instanz hinzu und sammelt die Bestandsaufnahme der Instanz. Weitere Informationen finden Sie unter Wie NetScaler ADM Instanzen erkennt.

Nachdem Sie eine Instanz hinzugefügt haben, können Sie sie löschen, indem Sie zu **Infrastruktur > Instanzen** navigieren und auf **Alle Instanzen**klicken. Wählen Sie auf der Seite Instanzen die Instanz aus, die Sie löschen möchten, und klicken Sie auf **Entfernen**.

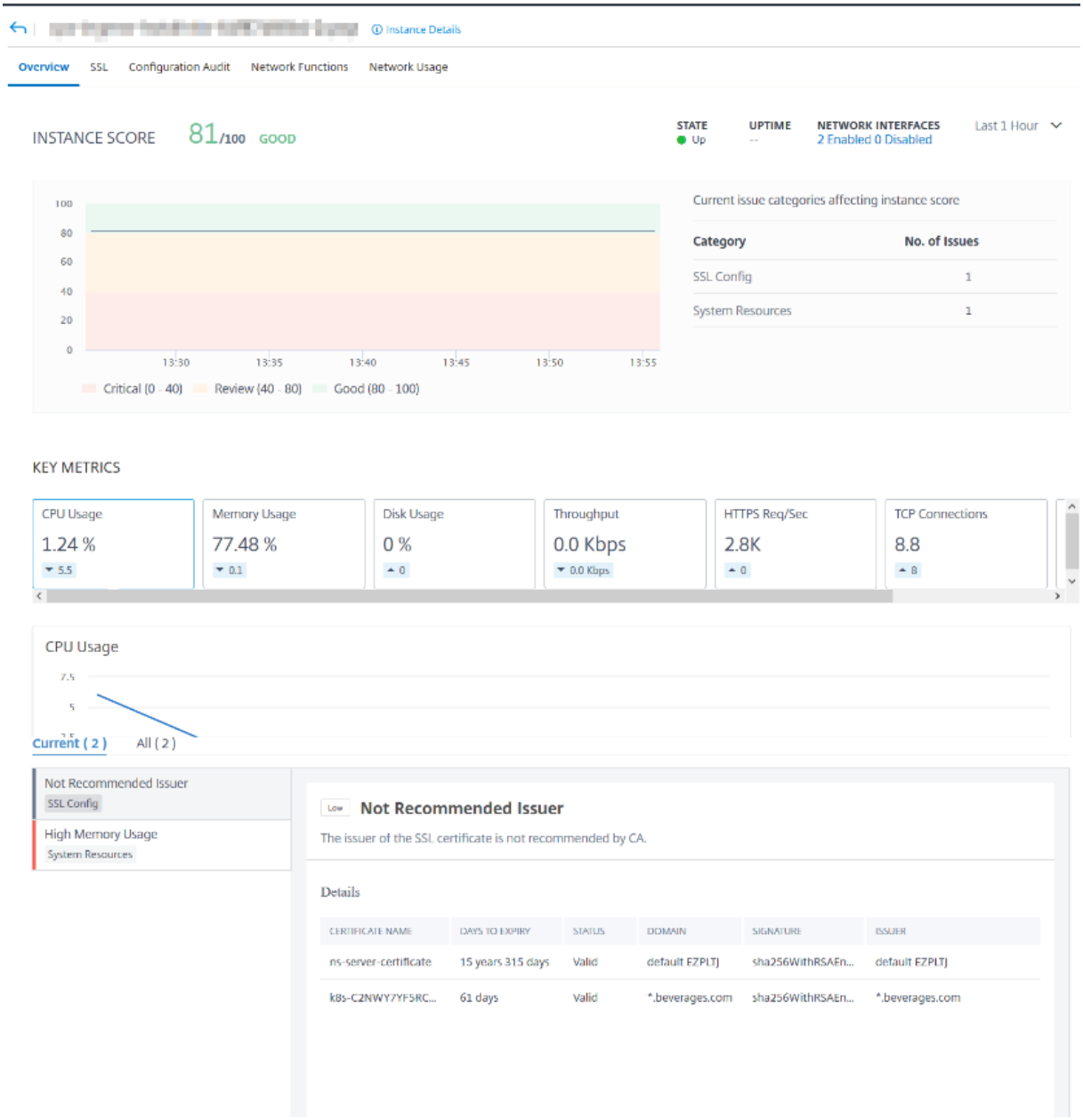
So verwenden Sie das Instanz-Dashboard

Das Instanzen-Dashboard in NetScaler ADM zeigt Daten in einem tabellarischen und grafischen Format für die ausgewählte Instanz an. Daten, die während des Abfragevorgangs von Ihrer Instanz gesammelt wurden, werden im Dashboard angezeigt.

Standardmäßig werden verwaltete Instanzen jede Minute zur Datenerfassung abgefragt. Statistische Informationen wie Status, HTTP-Anforderungen pro Sekunde, CPU-Auslastung, Speicherauslastung und Durchsatz werden kontinuierlich mithilfe von 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 **Infrastruktur > Instanzen**. Wählen Sie in der Zusammenfassung 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 ausgewählten Instanz an. Sie können auch Ereignisse anzeigen, die von der Instanz generiert werden und die Durchsatzdaten. Instanzspezifische Informationen wie die IP-Adresse, die Hardware- und LOM-Versionen, die Profildetails, die Seriennummer, die Kontaktperson usw. werden hier ebenfalls 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 Instanzdetails.

- **SSL-Dashboard**. Sie können die Registerkarte SSL im Dashboard für jede Instanz verwenden,

um die Details der SSL-Zertifikate, virtuellen SSL-Server und SSL-Protokolle Ihrer ausgewählten Instanz einzusehen oder zu überwachen. Sie können auf die „Zahlen“in den Grafiken klicken, um weitere Details anzuzeigen.

- **Prüfung der Konfiguration**. Sie können die Registerkarte Konfigurationsüberprüfung verwenden, um alle Konfigurationsänderungen anzuzeigen, die an der ausgewählten Instanz vorgenommen wurden. Die Diagramme für den**gespeicherten Status der NetScaler-Konfiguration** und die **Driftdiagramme der NetScaler-Konfiguration**auf dem Dashboard zeigen allgemeine Details zu Konfigurationsänderungen, die im Vergleich zu nicht gespeicherten Konfigurationen gespeichert wurden.
- **Netzwerk-Funktionen**. Mithilfe des Dashboards für Netzwerkfunktionen können Sie den Status der Entitäten überwachen, die auf der ausgewählten NetScaler-Instanz konfiguriert sind. Sie können Diagramme für Ihre virtuellen Server anzeigen, in denen Daten wie Clientverbindungen, Durchsatz und Serververbindungen angezeigt werden.
- **Netzwerk-Nutzung**. Sie können die Netzwerkleistungsdaten für Ihre ausgewählte Instanz auf der Registerkarte Netzwerknutzung 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 Plussymbol in der unteren rechten Ecke des Bildschirms klicken, um einen weiteren Leistungsbericht hinzuzufügen.

Global verteilte Standorte überwachen

February 5, 2024

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 NetScaler Application Delivery Management (ADM) bietet Ihnen eine grafische Darstellung Ihrer Standorte und unterteilt Ihre Netzwerküberwachungserfahrung nach Regionen. Mit Geomaps können Sie Ihre Netzwerkinstanzverteilung nach Standort visualisieren und Netzwerkprobleme überwachen.

Im folgenden Abschnitt wird erläutert, wie Sie Rechenzentren in NetScaler ADM überwachen können.

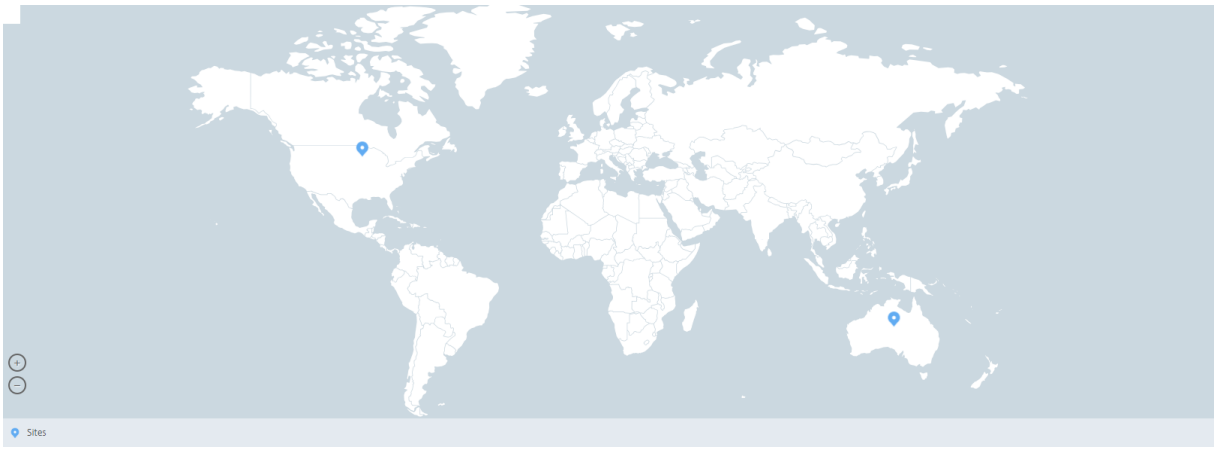
Die NetScaler ADM -Site ist eine logische Gruppierung von ADC-Instanzen (Citrix Application Delivery Controller) an einem bestimmten geografischen Standort. Zum Beispiel, während ein Standort Ama-

zon Web Services (AWS) zugewiesen ist und ein anderer Standort Azure™ zugewiesen sein kann. Noch eine andere Website wird auf dem Gelände des Mandanten gehostet. NetScaler ADM verwaltet und überwacht alle NetScaler-Instanzen, die mit allen Standorten verbunden sind. Sie können NetScaler ADM verwenden, um Syslog, AppFlow, SNMP und alle derartigen Daten, die von den verwalteten Instanzen stammen, zu überwachen und zu sammeln.

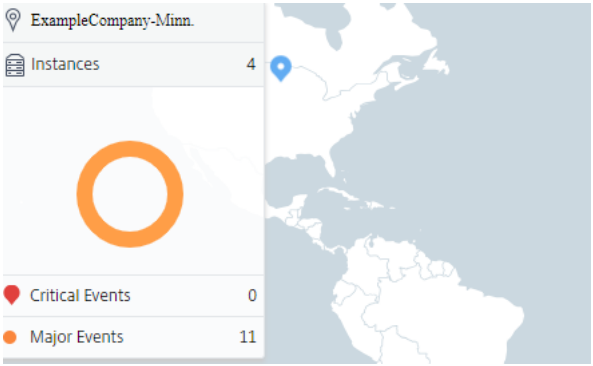
Geomaps in NetScaler ADM bieten Ihnen eine grafische Darstellung Ihrer Websites. Geomaps schlüsselt auch Ihre Netzwerküberwachungserfahrung nach Geografie auf. Mit Geomaps können Sie Ihre Netzwerkinstanzverteilung nach Standort visualisieren und alle Netzwerkprobleme überwachen. Sie können zur Seite **Infrastruktur > Instanzen** navigieren, um eine visuelle Darstellung der auf der Weltkarte erstellten Websites zu erhalten.

Anwendungsfall

Ein führendes Mobilfunkanbieterunternehmen, ExampleCompany, verließ sich beim Hosten seiner Ressourcen und Anwendungen auf private Dienstleister. Das Unternehmen hatte bereits zwei Standorte - einen in Minneapolis in den USA und einen weiteren in Alice Springs in Australien. In diesem Bild sehen Sie, dass zwei Marker die beiden vorhandenen Standorte darstellen.

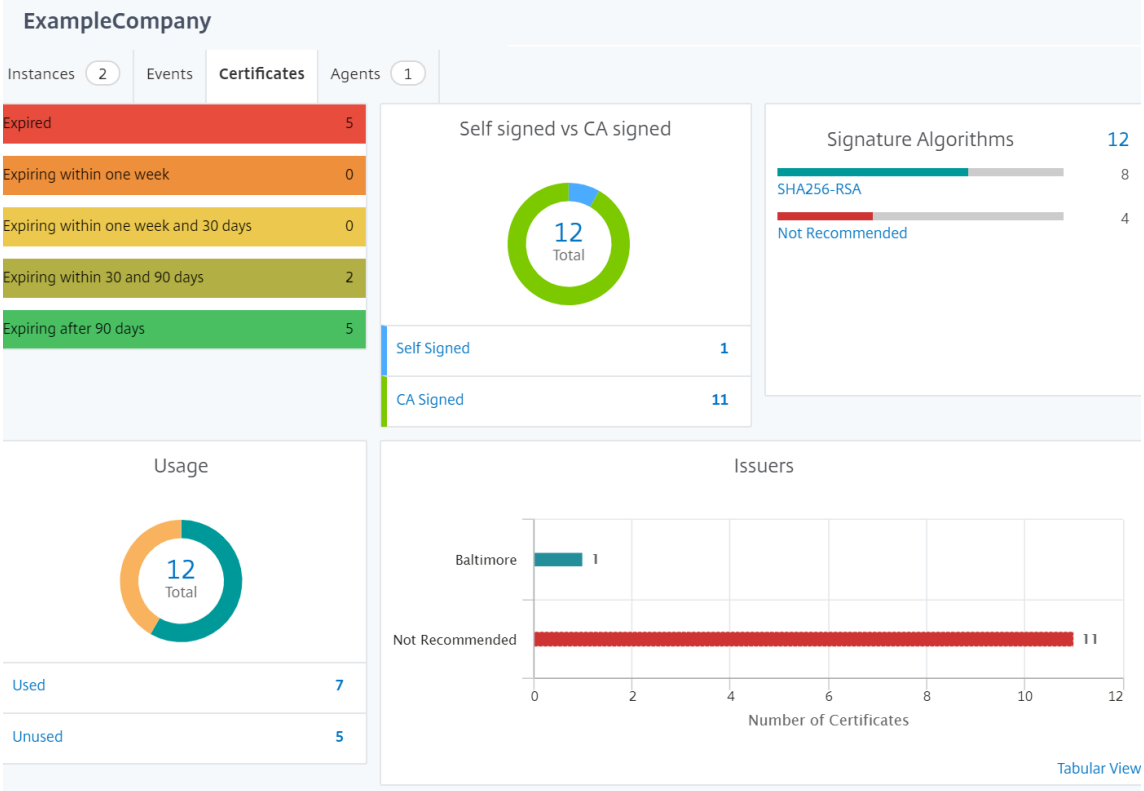


Die Marker zeigen auch eine Zahl an, die die Anzahl der Anwendungen an jedem Standort anzeigt. Sie können auf diese Marker klicken, um weitere Informationen zu den einzelnen Websites zu erhalten.



Klicken Sie auf die Registerkarten, um weitere Informationen anzuzeigen:

- Registerkarte “**Instanzen** “: Sehen Sie sich auf dieser Registerkarte Folgendes an:
  - IP-Adresse jeder Netzwerkinstanz
  - Typ der Instanz
  - Anzahl der kritischen Ereignisse auf ihnen
  - Bedeutende Ereignisse und alle Ereignisse, die auf einer NetScaler-Instanz ausgelöst werden.
- Registerkarte**Ereignisse** : Zeigen Sie eine Liste kritischer und bedeutender Ereignisse an, die in den Instanzen ausgelöst wurden.
- Registerkarte**Zertifikate** : Sehen Sie sich auf dieser Registerkarte Folgendes an:
  - Liste der Zertifikate aller Instanzen
  - Ablauf-Status
  - Wichtige Informationen und die 10 wichtigsten Instanzen durch viele verwendete Zertifikate.
- Registerkarte **Agents**: Zeigt eine Liste der Agents an, an die die Instanzen gebunden sind.



Geomaps konfigurieren

ExampleCompany hat beschlossen, einen dritten Standort in Bangalore, Indien, einzurichten. Das Unternehmen wollte die Cloud testen, indem es einige seiner weniger kritischen, internen IT-Anwendungen an das Büro in Bangalore verlagerte. Das Unternehmen entschied sich für die Nutzung der AWS-Cloud-Computing-Services.

Als Administrator müssen Sie zuerst eine Site erstellen und anschließend die NetScaler-Instanzen in NetScaler ADM hinzufügen. Sie müssen außerdem die Instanz zur Site hinzufügen, einen Agent hinzufügen und den Agent an die Site binden. NetScaler ADM erkennt dann den Standort, zu dem die NetScaler-Instanz und der Agent gehören.

Weitere Informationen zum Hinzufügen von NetScaler-Instanzen finden Sie unter Hinzufügen von Instanzen.

So erstellen Sie Websites:

Erstellen Sie Sites, bevor Sie Instanzen in NetScaler ADM hinzufügen. Die Bereitstellung von Standortinformationen ermöglicht es Ihnen, den Standort genau zu lokalisieren.

Navigieren Sie zu **Infrastruktur > Instanzen > Sites**, und klicken Sie dann auf **Hinzufügen**.

1. Geben Sie auf der Seite **Site erstellen** die folgenden Informationen an:

   a) **Standorttyp**: Wählen Sie **Rechenzentrum**aus.

   > **Hinweis**
   >
   > Der Standort kann als primäres Rechenzentrum oder als Zweigstelle fungieren. Wählen Sie entsprechend.

   b) **Typ**: Wählen Sie AWS als Cloud-Anbieter aus der Liste aus.

   > **Hinweis**
   >
   > Aktivieren Sie das Kontrollkästchen **Vorhandene VPC als Site verwenden** entsprechend.

   c) **Site-Name**: Geben Sie den Namen der Site ein.

   d) **Stadt**: Geben Sie die Stadt ein.

   e) **Postleitzahl**: Geben Sie die Postleitzahl ein.

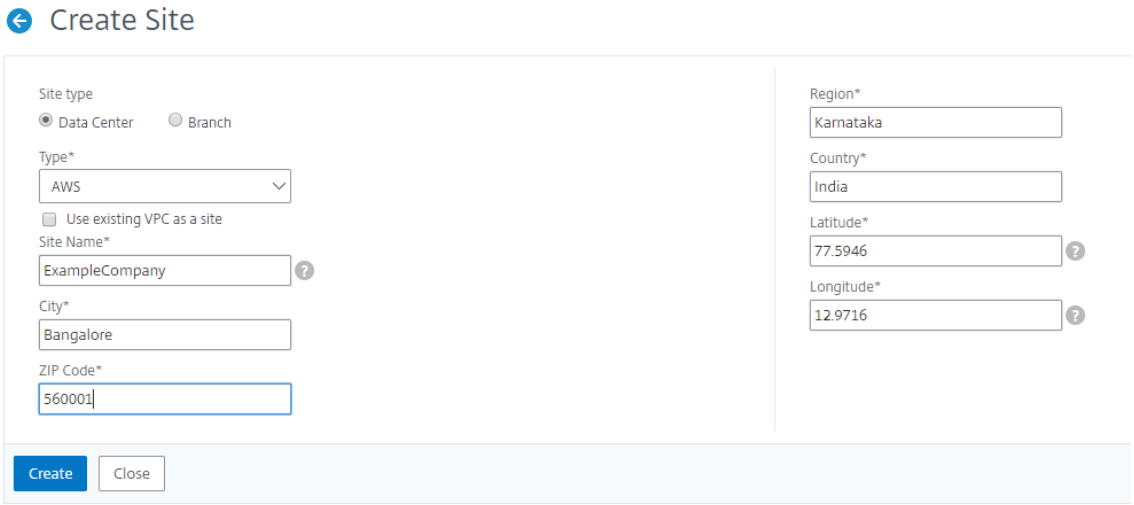
   f) **Region**: Geben Sie die Region ein.

   g) **Land**: Geben Sie das Land ein

   h) **Breitengrad**: Geben Sie den Breitengrad des Standorts ein.

i) **Längengrad**: Geben Sie den Längengrad der Position ein.

2. Klicken Sie auf **Erstellen**.

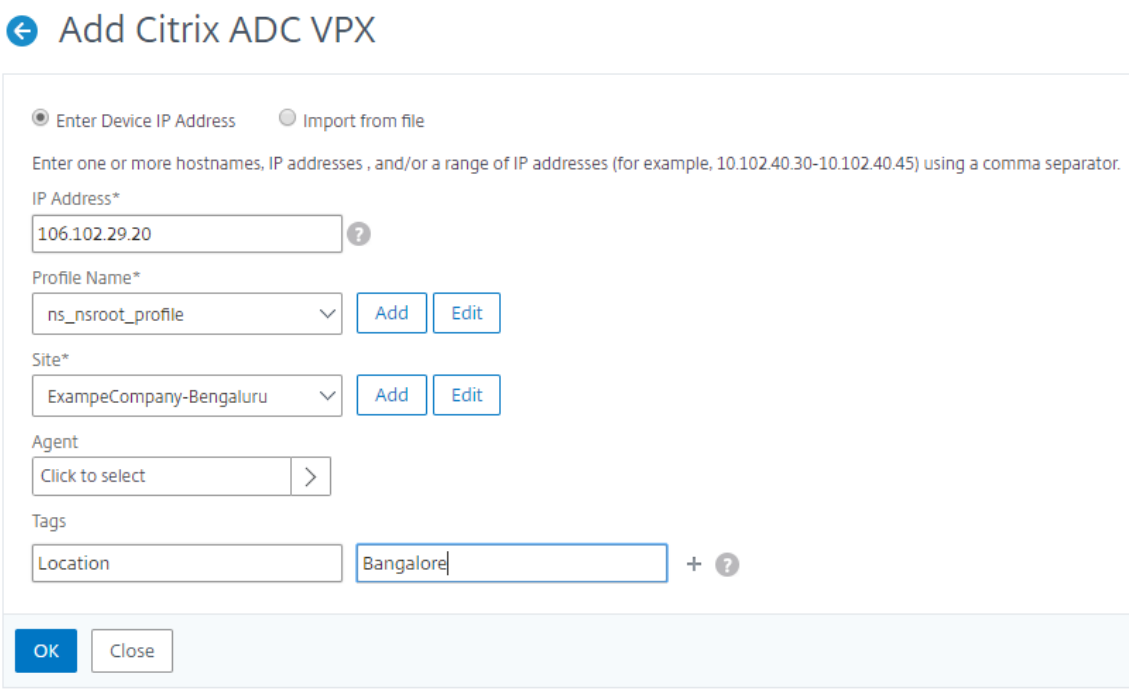


So fügen Sie Instanzen hinzu und wählen Sie Sites aus:

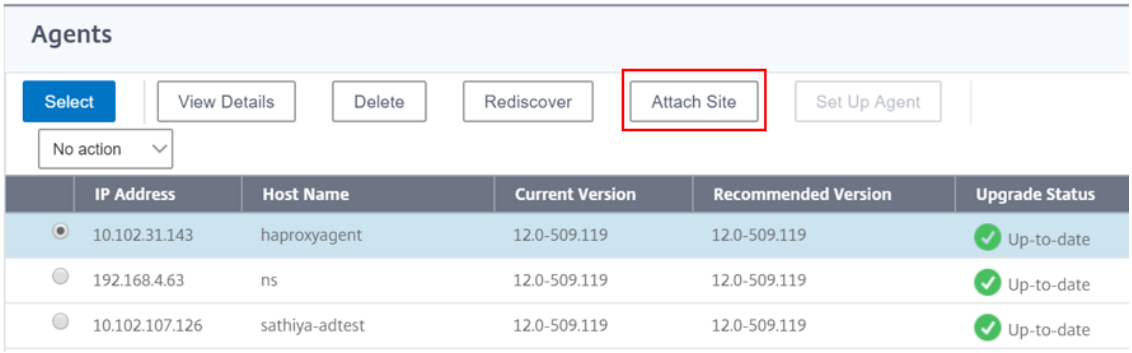
Nach dem Erstellen von Sites müssen Sie Instanzen in NetScaler ADM hinzufügen. Sie können die zuvor erstellte Site auswählen, oder Sie können auch eine Site erstellen und die Instanz zuordnen.

Nach dem Erstellen von Sites müssen Sie Instanzen in NetScaler ADM hinzufügen. Sie können die zuvor erstellte Site auswählen, oder Sie können auch eine Site erstellen und die Instanz zuordnen.

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur**> Instances.
2. Wählen Sie den Typ der Instanz aus, die Sie erstellen möchten, und klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **NetScaler VPX hinzufügen** die IP-Adresse ein und wählen Sie das Profil aus der Liste aus.
4. Wählen Sie die Site aus der Liste aus. Sie können auf das Pluszeichen neben dem Feld **Site** klicken, um eine Site zu erstellen, oder auf das Bearbeitungssymbol klicken, um die Details der Standardwebsite zu ändern.
5. Klicken Sie auf den Pfeil nach rechts, und wählen Sie den Agent aus der angezeigten Liste aus.



6. Nachdem Sie den Agent ausgewählt haben, müssen Sie den Agent der Site zuordnen. In diesem Schritt kann der Agent an die Site gebunden werden. Wählen Sie den Agenten aus und klicken Sie auf **Site anhängen**.



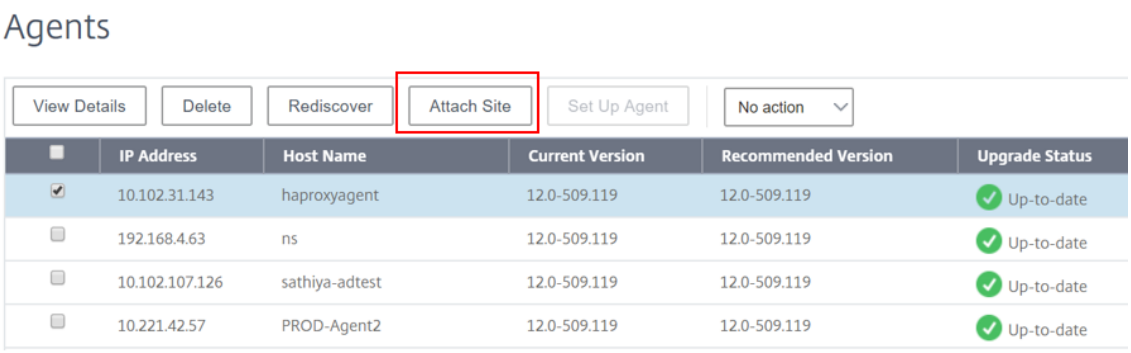
1. Wählen Sie die Website aus der Liste aus, und klicken Sie auf **Speichern**.

1. Klicken Sie auf **OK**.

Sie können auch einen Agent an eine Site anhängen, indem Sie zu **Infrastruktur > Instanzen > Agents** navigieren.

So verknüpfen Sie einen NetScaler ADM Agent mit der Site:

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Instanzen > Agents**.
2. Wählen Sie den Agent aus, und klicken Sie auf **Site anhängen**.



1. Sie können die Website zuordnen und auf **Speichern**klicken.

NetScaler ADM beginnt mit der Überwachung der NetScaler Instanzen, die in Bangalore-Standort hinzugefügt werden, zusammen mit den Instanzen an den beiden anderen Standorten.

Tags erstellen und Instanzen zuweisen

February 5, 2024

NetScaler Application Delivery Management (ADM) ermöglicht es Ihnen jetzt, Ihre Citrix Application Delivery Controller (ADC) -Instanzen mit Tags zu verknüpfen. Ein Tag ist ein Schlüsselwort oder ein aus einem Wort bestehendes 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 helfen, eine Instanz zu beschreiben. Mit Tags können Sie Instanzen anhand dieser spezifischen Schlüsselwörter klassifizieren und suchen. Sie können einer einzelnen Instanz auch mehrere Tags zuweisen.

Die folgenden Anwendungsfälle helfen Ihnen zu verstehen, wie das Tagging von Instanzen Ihnen hilft, diese besser zu überwachen.

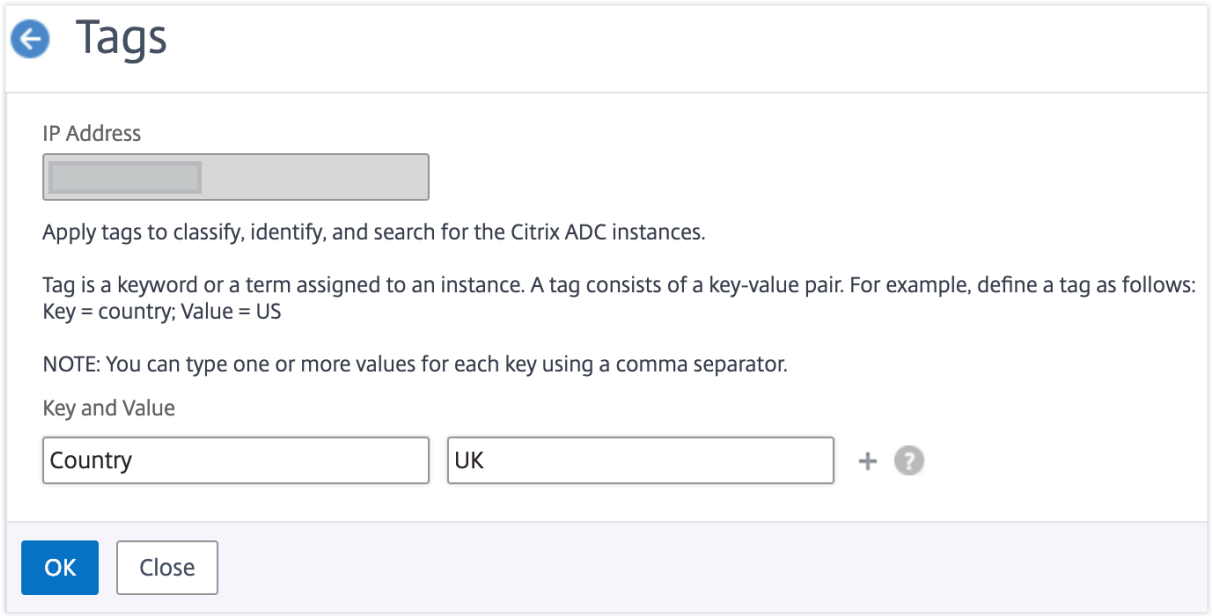
- **Anwendungsfall 1**: Sie können ein Tag erstellen, um alle Instanzen in Großbritannien zu identifizieren. Hier können Sie ein Tag mit dem Schlüssel “Country”und dem Wert als “UK”erstellen. Dieses Tag hilft Ihnen bei der Suche und Überwachung all dieser Instanzen in Großbritannien.
- **Anwendungsfall 2**: Sie möchten nach Instanzen suchen, die sich in der Stagingumgebung befinden. Hier können Sie ein Tag mit dem Schlüssel “Purpose”und dem 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 NetScaler-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.

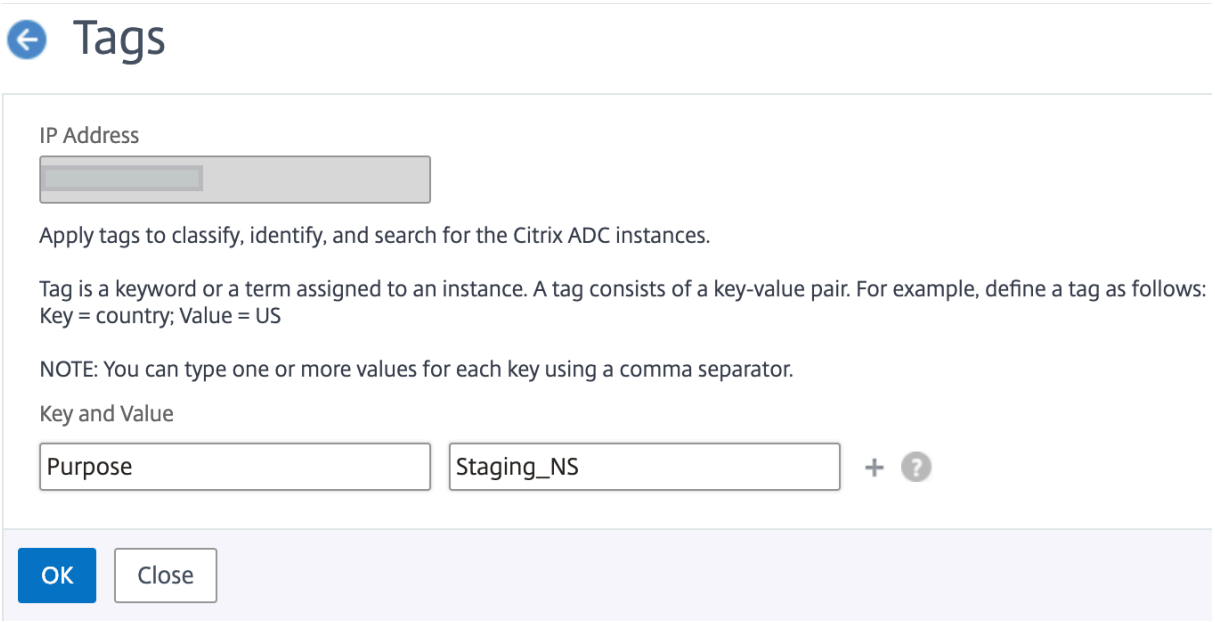
So weisen Sie der NetScaler VPX Instanz Tags zu:

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Instanzen > NetScaler**.
2. Wählen Sie die Registerkarte **NetScaler VPX** aus.
3. Wählen Sie den erforderlichen NetScaler VPX aus.
4. Klicken Sie **auf Tags**.
5. Erstellen Sie Tags und klicken Sie auf **OK**.

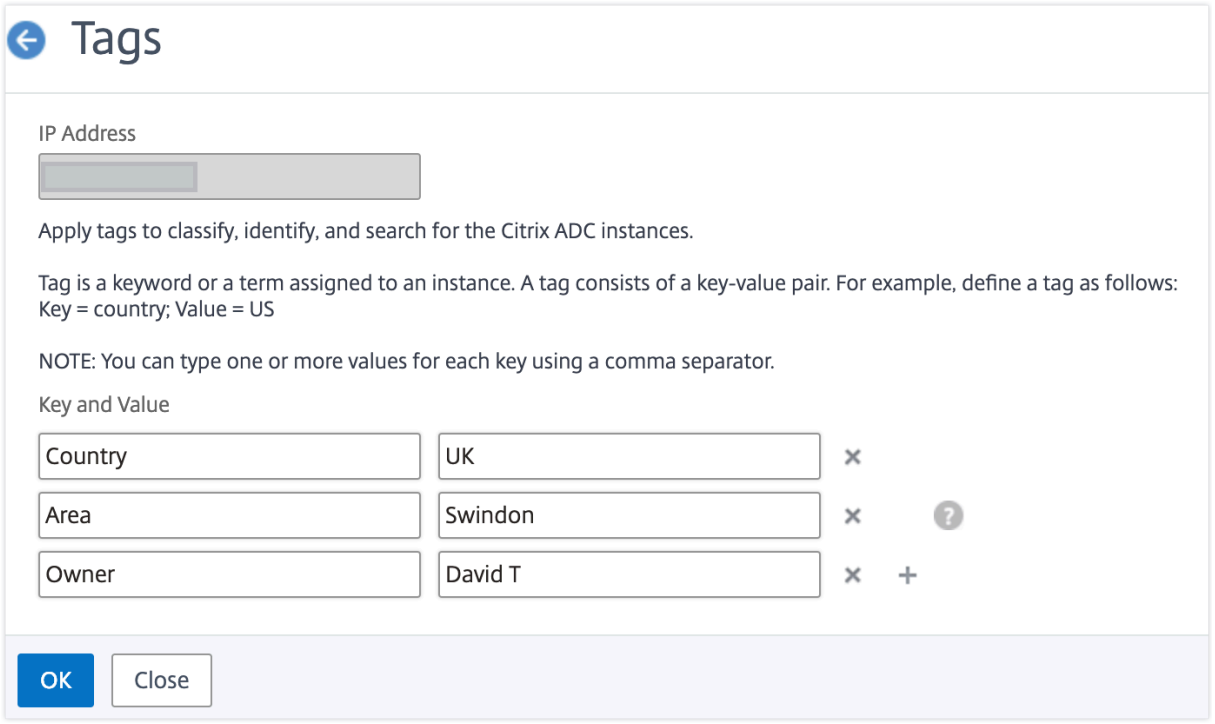
Im angezeigten **Tags-Fenster** können Sie Ihre eigenen "Schlüssel-Wert"-Paare erstellen, indem Sie jedem von Ihnen erstellten Schlüsselwort Werte zuweisen.

Die folgenden Bilder zeigen beispielsweise einige erstellte Keywords und deren Werte. Sie können eigene Schlüsselwörter hinzufügen und für jedes Schlüsselwort einen Wert eingeben.



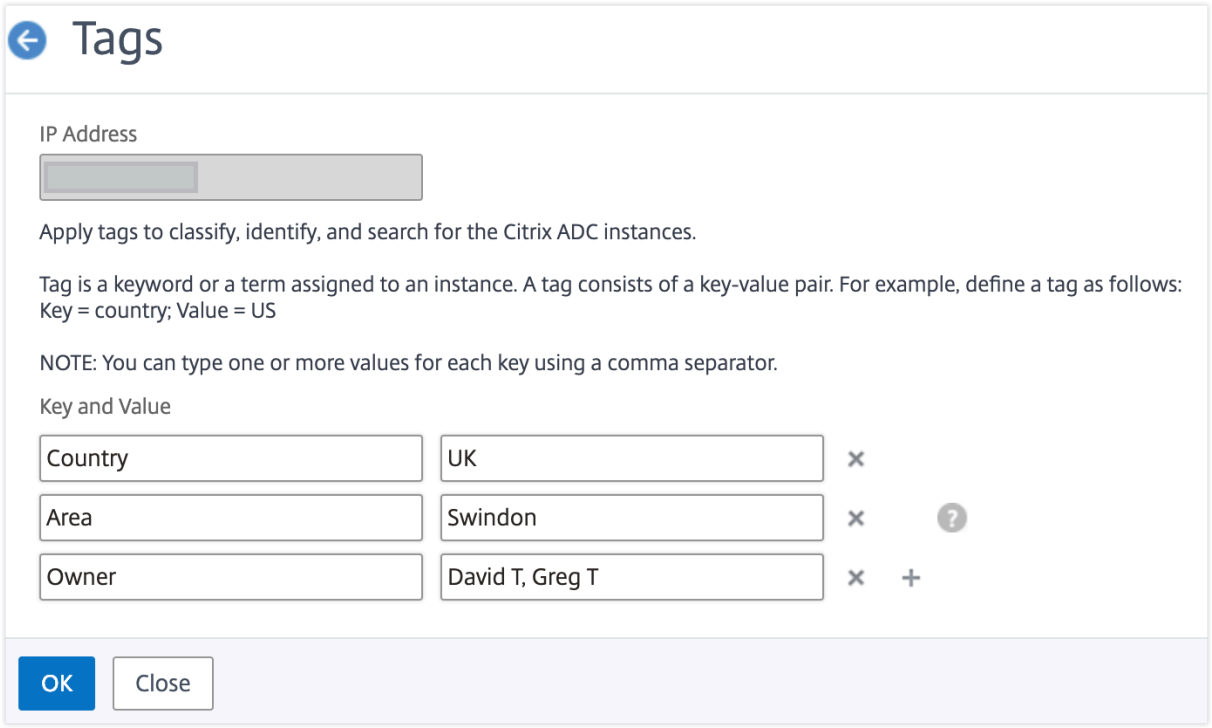


Sie können auch mehrere Tags hinzufügen, indem Sie auf “+”klicken. Durch das Hinzufügen mehrerer und aussagekräftiger Tags können Sie effizient nach den Instanzen suchen.



Sie können einem Schlüsselwort mehrere Werte hinzufügen, indem Sie sie durch Kommas trennen.

Sie weisen beispielsweise einem anderen Kollegen, Greg T., die Administratorrolle zu. 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. NetScaler ADM erkennt die durch Kommas getrennten Werte in zwei verschiedene Werte.



Weitere Informationen zum Suchen nach Instanzen basierend auf Tags finden Sie unter Suchen von Instanzen mithilfe von Werten von Tags und Eigenschaften.

> **Hinweis**
>
> Sie können später neue Tags hinzufügen oder vorhandene Tags löschen. Es gibt keine Einschränkung für die Anzahl der Tags, die Sie erstellen.

Instanzen über Werte von Tags und Eigenschaften suchen

February 5, 2024

Es kann vorkommen, dass NetScaler Application Delivery Management (ADM) viele NetScaler-Instanzen verwaltet. Als Administrator möchten Sie möglicherweise die Flexibilität, die Instanzinventar anhand bestimmter Parameter zu durchsuchen. NetScaler ADM bietet jetzt eine verbesserte Suchfunktion, um eine Teilmenge von NetScaler-Instanzen basierend auf den Parametern zu durchsuchen, die Sie im Suchfeld definieren. Sie können anhand von zwei Kriterien —Tags und Eigenschaften —nach den Instanzen suchen.

- **Tags**. Tags sind Begriffe oder Schlüsselwörter, die Sie einer NetScaler-Instanz zuweisen können, um eine zusätzliche Beschreibung der NetScaler-Instanz hinzuzufügen. Sie können

Ihre NetScaler-Instanzen nun Tags zuordnen. Diese Tags können verwendet werden, um die NetScaler-Instanzen besser zu identifizieren und zu suchen.

- **Eigenschaften**. Jede NetScaler-Instanz, die in NetScaler 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 NetScaler-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 UP-Status der Instanzen können Sie auch die 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 Erstellen von Tags und Zuweisen zu Instanzen.

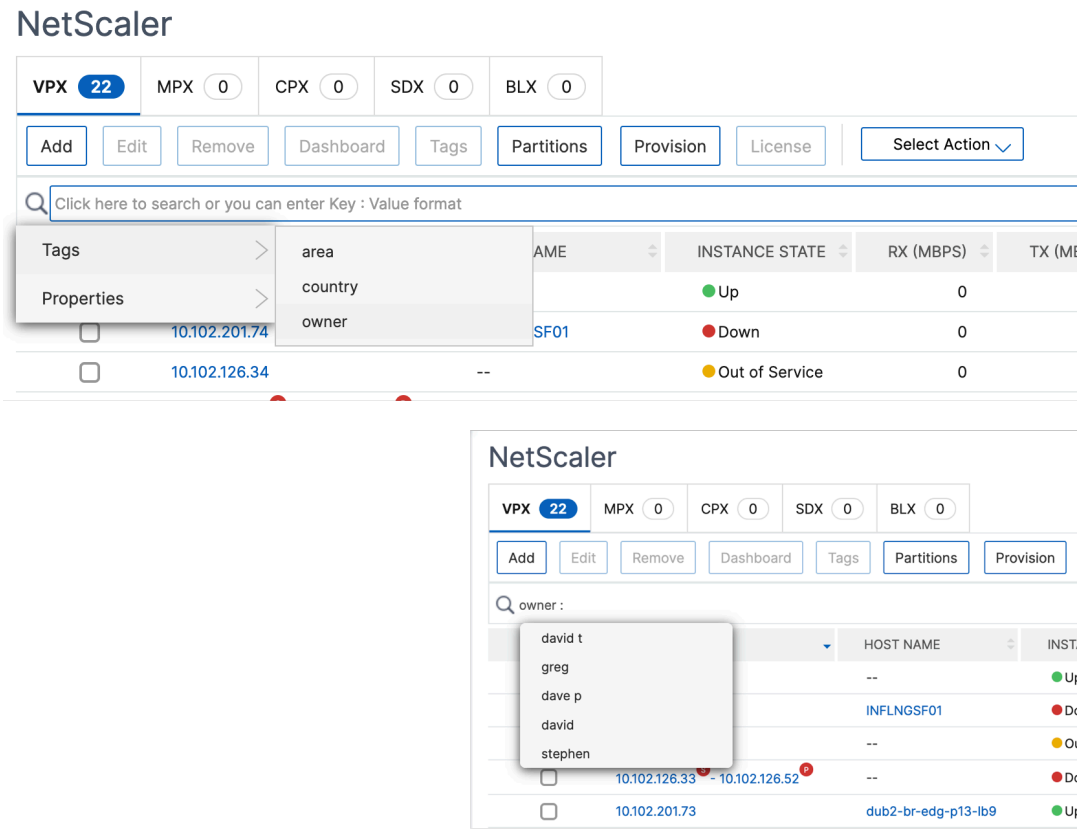
Sie können eine Kombination aus Tags und Eigenschaften verwenden, um eigene Suchkriterien zu erstellen.

So suchen Sie nach NetScaler VPX Instanzen

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Instanzen > NetScaler** > **VPX** .
2. Klicken Sie auf das Suchfeld. Sie können einen Suchausdruck erstellen, indem Sie Tags oder Eigenschaften verwenden oder beide kombinieren.

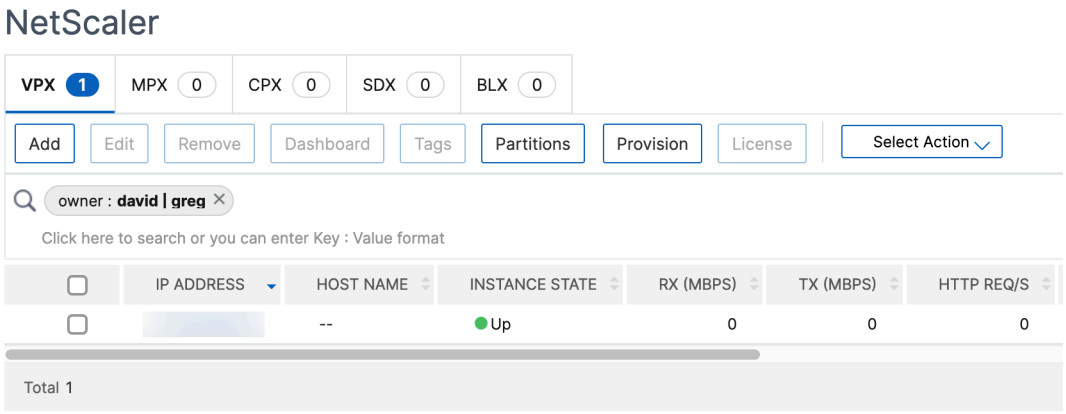
   Die folgenden Beispiele zeigen, wie Sie den Suchausdruck effizient verwenden können, um nach der Instanz zu suchen.

   a) Wählen Sie die Option **Tags** und dann **Besitzer**aus. Wählen Sie “David T.”

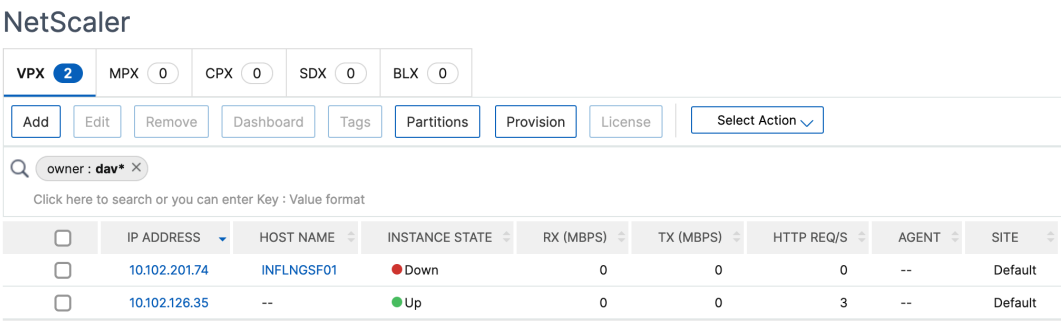


NetScaler ADM unterstützt reguläre Ausdrücke und Platzhalterzeichen in den Suchausdrücken.

b) Sie können reguläre Ausdrücke verwenden, um die Suchkriterien weiter zu erweitern. Sie möchten beispielsweise Instanzen suchen, die entweder David oder Stephen gehören. In einem solchen Fall können Sie die Werte eingeben, indem Sie die Werte durch einen |-Ausdruck trennen.



c) Sie können auch Platzhalterzeichen verwenden, um ein oder mehrere Zeichen zu ersetzen oder darzustellen. Sie können beispielsweise Dav* nach allen Instanzen suchen, die David T und Dave P gehören.



> **Hinweis**
>
> Weitere Informationen zu regulären Ausdrücken und Platzhalterzeichen sowie deren Verwendung finden Sie in der Suchleiste auf das Symbol Informationen.

Adminpartitionen von NetScaler-Instanzen verwalten

February 5, 2024

Sie können Admin-Partitionen auf Ihren Citrix Application Delivery Controller (ADC) -Instanzen konfigurieren, sodass verschiedenen Gruppen in Ihrer Organisation unterschiedliche Partitionen auf derselben NetScaler-Instanz zugewiesen werden. Ein Netzwerkadministrator kann mit der Verwaltung mehrerer Partitionen auf mehreren NetScaler-Instanzen beauftragt werden.

NetScaler Application Delivery Management (ADM) bietet eine nahtlose Möglichkeit, alle Partitionen, die einem Administrator gehören, von einer einzigen Konsole aus zu verwalten. Sie können diese Partitionen verwalten, ohne andere Partitionskonfigurationen zu stören.

Damit mehrere Benutzer verschiedene Admin-Partitionen verwalten können, müssen Sie Gruppen erstellen und dann Benutzer und Partitionen diesen Gruppen zuweisen. Jeder Benutzer kann nur die Partitionen in der Gruppe anzeigen und verwalten, zu der der Benutzer gehört. Jede Admin-Partition wird in NetScaler ADM als Instanz betrachtet. Wenn Sie eine NetScaler-Instanz entdecken, werden die für diese NetScaler-Instanz konfigurierten Adminpartitionen automatisch dem System hinzugefügt.

Stellen Sie sich vor, Sie haben zwei NetScaler VPX-Instanzen mit zwei Partitionen, die auf jeder Instanz konfiguriert sind. Beispielsweise hat die NetScaler Instanz 10.102.216.49 Partition_1, Partition_2 und Partition_3, und die NetScaler-Instanz 10.102.29.120 hat p1 und p2, wie in der folgenden Abbildung gezeigt.

Um die Partitionen anzuzeigen, navigieren Sie zu**Infrastruktur > Instanzen > NetScaler > VPX**, und klicken Sie dann auf **Partitionen**.

Sie können user-p1 die folgenden Partitionen zuweisen: 10.102.29.120-p1 und 10.102.216.49-Partition_1. Und Sie können user-p2 der Verwaltung der Partitionen 10.102.29.80-p2, 10.102.216.49-Partition_2 und 10.102.216.49-Partition_3 zuweisen.

Dann müssen Sie die beiden Benutzer user-p1 und user-p2 erstellen und die Benutzer den Gruppen zuweisen, die Sie für sie erstellt haben.

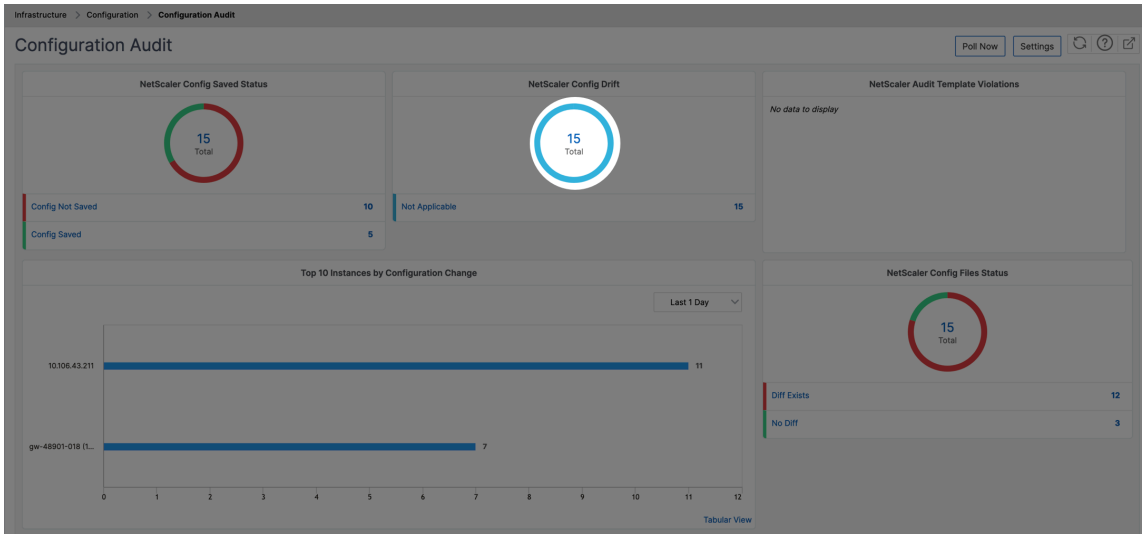
Zunächst müssen Sie zwei Gruppen mit entsprechenden Berechtigungen erstellen (Beispiel: Administratorberechtigungen) und die erforderlichen Admin-Partitionsinstanzen in jede Gruppe aufnehmen. Erstellen Sie beispielsweise die Systemgruppe partition1-admin und fügen Sie dieser Gruppe die NetScaler-Administratorpartitionen 10.102.29.120-p1 und 10.102.216.49-Partition_1 hinzu. Erstellen Sie außerdem die Systemgruppe partition2-admin und fügen Sie die NetScaler-Administratorpartitionen 10.102.29.120-p2, 10.102.216.49-Partition_2 und 10.102.216.49-Partition_3 und zu dieser Gruppe hinzu.

Nachdem Sie die Admin-Partition erstellt haben, können Sie zu Prüfungszwecken auch die Funktion zum Unterschied des Versionsverlaufs und die Funktion Auditvorlage für die Admin-Partition verwenden.

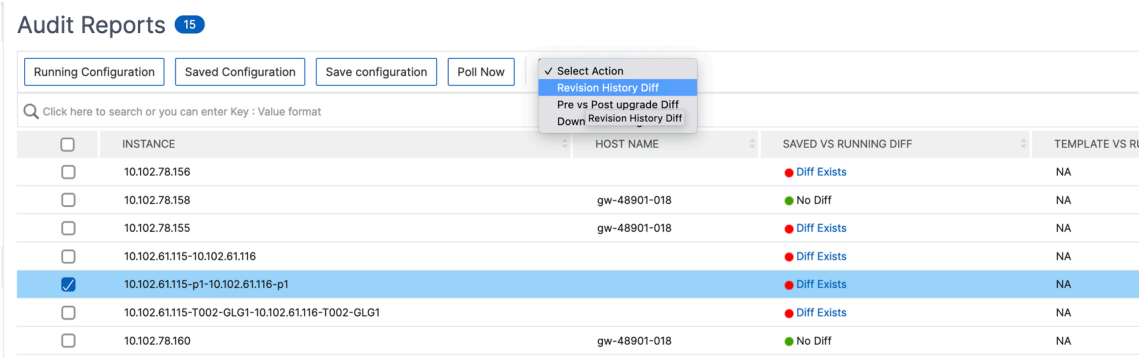
Der Unterschied zwischen dem Versionsverlauf für die Admin-Partition ermöglicht es Ihnen, den Unterschied zwischen den fünf neuesten Konfigurationsdateien für eine partitionierte NetScaler-Instance zu sehen. Sie können die Konfigurationsdateien miteinander vergleichen (Beispiel Configuration Revision —1 mit Configuration Revision -2) oder mit der aktuell laufenden/gespeicherten Konfiguration mit Configuration Revision. 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:

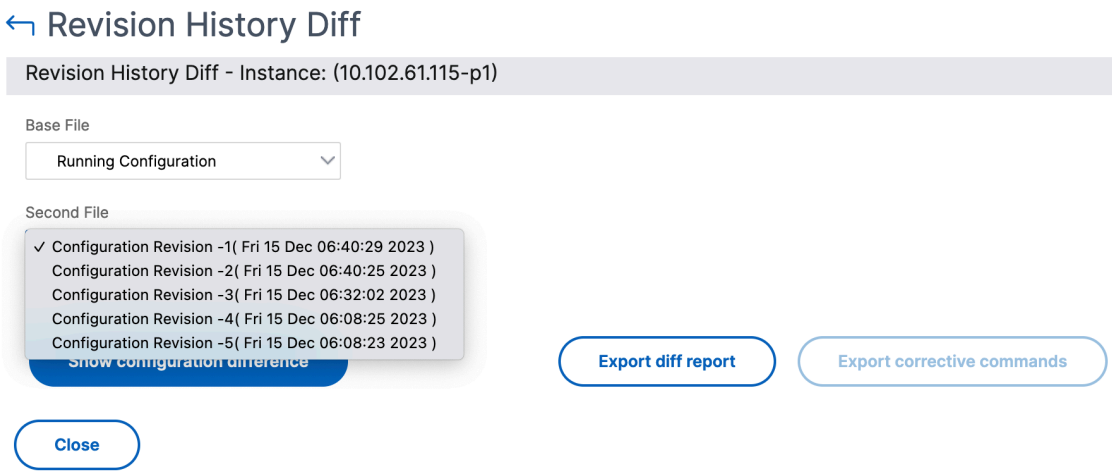
1. Navigieren Sie zu **Infrastruktur > Configuration Audit.** Klicken Sie in das Donutdiagramm, das den Status der Instanzkonfiguration darstellt. Klicken Sie auf der Seite **Überwachungsberichte**, die geöffnet wird, auf die partitionierte NetScaler Instanz.



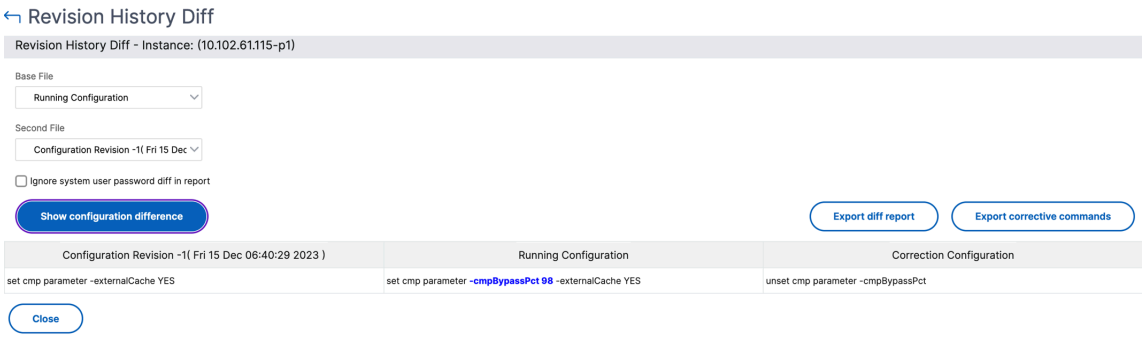
2. Klicken Sie im Menü **Aktion** auf **Versionsverlauf Diff.**



3. Wählen Sie auf der Seite **Versionsverlauf-Diff** die Dateien aus, die Sie vergleichen möchten. Vergleichen Sie beispielsweise die gespeicherte Konfiguration mit der Konfigurationsversion -1, und klicken Sie dann auf **Konfigurationsdifferenz anzeigen**.



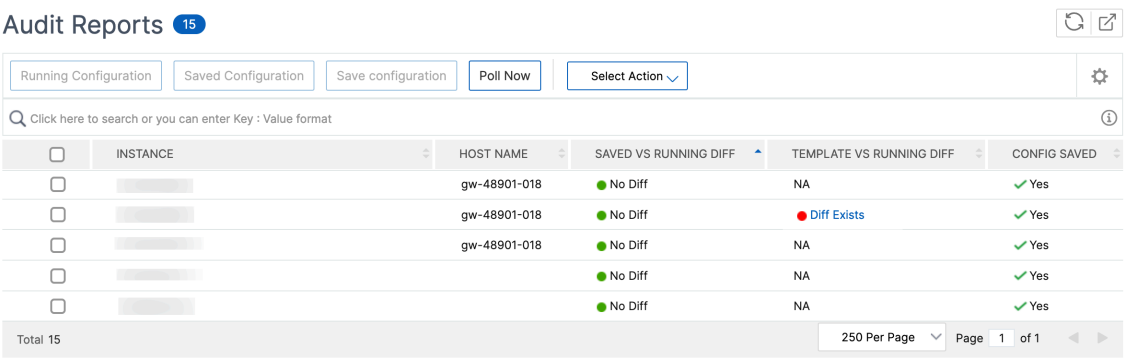
4. Sie können dann den Unterschied zwischen den fünf neuesten Konfigurationsdateien für die ausgewählte partitionierte NetScaler Instanz anzeigen, wie unten gezeigt. Sie können auch die Korrekturkonfigurationsbefehle anzeigen und diese Korrekturbefehle in Ihren lokalen Ordner exportieren. Diese Korrekturbefehle 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).



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 „ **Template vs. Running Diff** “auf 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.

So zeigen Sie die Vorlage im Vergleich zu den laufenden Differenzen an:

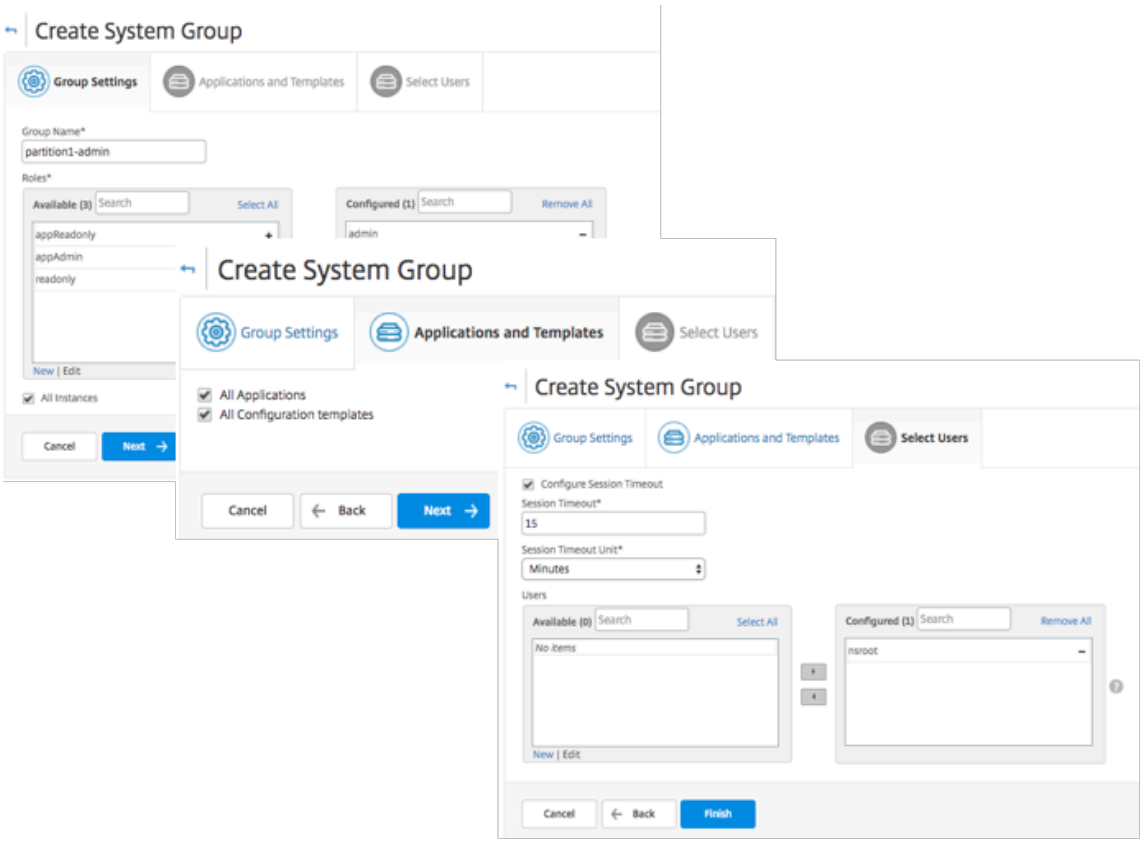
1. Klicken Sie auf der Seite “**Audit-Berichte** “auf die partitionierte NetScaler-Instanz.



2. Wenn zwischen der Audit-Vorlage und der laufenden Differenz ein Unterschied besteht, wird die Differenz 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 erstellen Sie Gruppen:

1. Navigieren Sie zu **Einstellungen > Benutzerverwaltung > Gruppen**, und klicken Sie dann auf **Hinzufügen**.
2. Geben **Sie auf der Seite "Systembenutzer erstellen** "Folgendes an:
   - Registerkarte „**Gruppeneinstellungen** ": Geben Sie den Gruppennamen und die Rollenberechtigungen ein. Um den Zugriff auf bestimmte Instances zu ermöglichen, deaktivieren Sie das Kontrollkästchen**All Instances**und wählen Sie dann Ihre Instances auf der Seite **Select Instances aus** .
   - Registerkarte „**Anwendungen und Vorlagen** ": Sie können wählen, ob Sie diese Gruppe für alle Anwendungen und Konfigurationsvorlagen verwenden möchten.
   - Registerkarte**Benutzer auswählen** : Wählen Sie Benutzer aus, die Sie dieser Gruppe hinzufügen möchten. Sie können auf den Link **Neu** in der Tabelle **Verfügbar** klicken, um neue Benutzer zu erstellen. Konfigurieren Sie optional das Sitzungstimeout, in dem Sie den Zeitraum konfigurieren können, wie lange ein Benutzer aktiv bleiben kann.
3. Klicken Sie auf **Fertig stellen**.



So erstellen Sie Benutzer:

1. Navigieren Sie zu**Einstellungen > Benutzerverwaltung > Benutzer**, und klicken Sie dann auf **Hinzufügen**.

2. Geben Sie auf der Seite "**Systembenutzer erstellen**"den Benutzernamen und das Kennwort an. Optional können Sie die externe Authentifizierung aktivieren und das Sitzungs-Timeout konfigurieren.
3. Weisen Sie den Benutzer einer Gruppe zu, indem Sie den Gruppennamen aus der Liste**Verfügbar zur**Liste**Konfiguriert**hinzufügen.
4. Klicken Sie auf **Erstellen**.

Melden Sie sich jetzt ab und melden Sie sich mit Benutzer-p1-Anmeldeinformationen an. Sie können nur die Admin-Partitionen anzeigen und verwalten, die Ihnen zur Verwaltung und Überwachung zugewiesen sind.

NetScaler Hochverfügbarkeitspaar erstellen

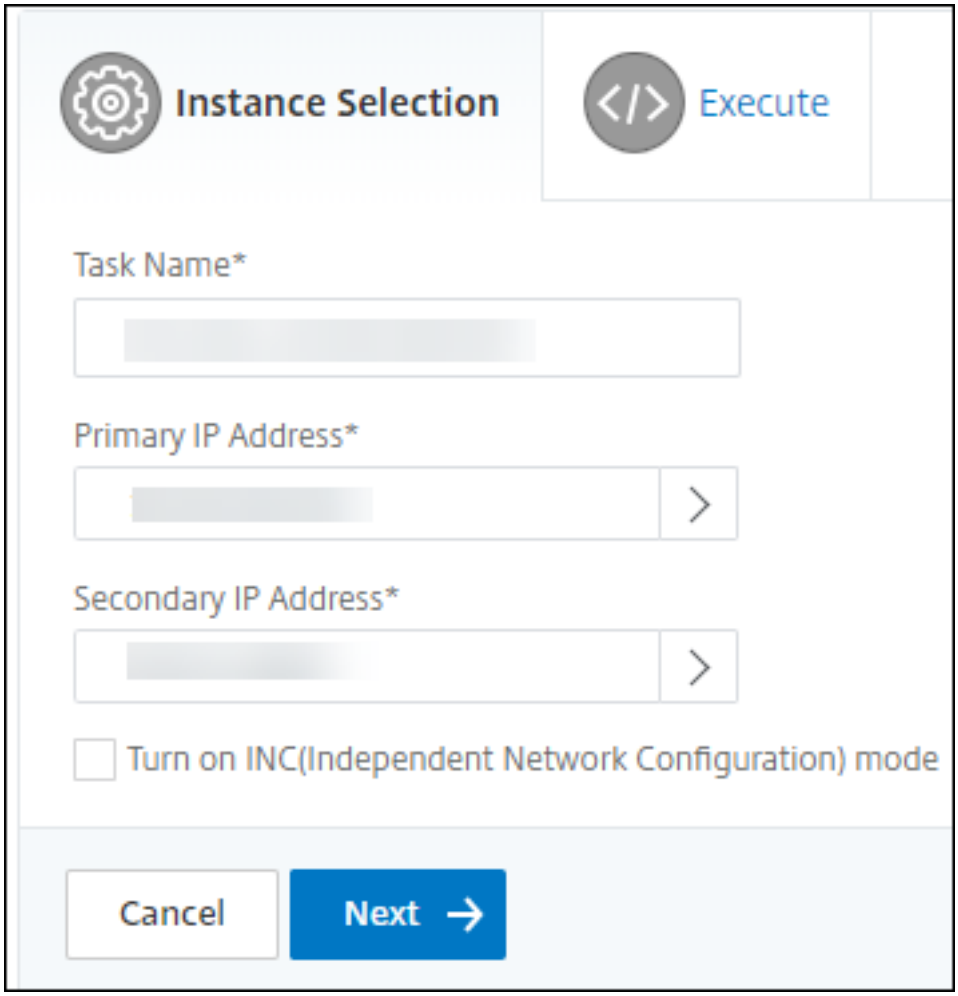
February 5, 2024

Ein NetScaler-Hochverfügbarkeitspaar (HA) kann bei Ausfallzeiten oder Netzwerkausfällen einen unterbrechungsfreien Betrieb gewährleisten. Sie können ein HA-Paar von ADC-Instanzen mit NetScaler ADM erstellen. Weitere Informationen finden Sie unter NetScaler Hochverfügbarkeit.

Führen Sie die folgenden Schritte aus, um ein HA-Paar von ADC-Instanzen in NetScaler ADM zu erstellen:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** .
2. Wählen Sie eine ADC-Instanz aus der Liste aus, mit der Sie ein HA-Paar erstellen möchten.

   Die ausgewählte Instanz wird zu einer primären Instanz im HA-Paar.
3. Klicken Sie auf **Aktion auswählen > HA-Paar erstellen**.
4. Führen Sie unter **Instanzauswahl**die folgenden Schritte aus:
   a) Klicken Sie unter **Sekundäre IP-Adresse**, um eine sekundäre Instanz auszuwählen.
   b) Wählen Sie eine ADC-Instanz aus, die Sie als sekundäre Instanz im HA-Paar konfigurieren möchten.
   c) Wählen Sie optional **den INC-Modus (Independent Network Configuration) aktivieren**, wenn die Instanzen des HA-Paars in zwei Subnetzen sind.
   d) Klicken Sie auf **Weiter**.



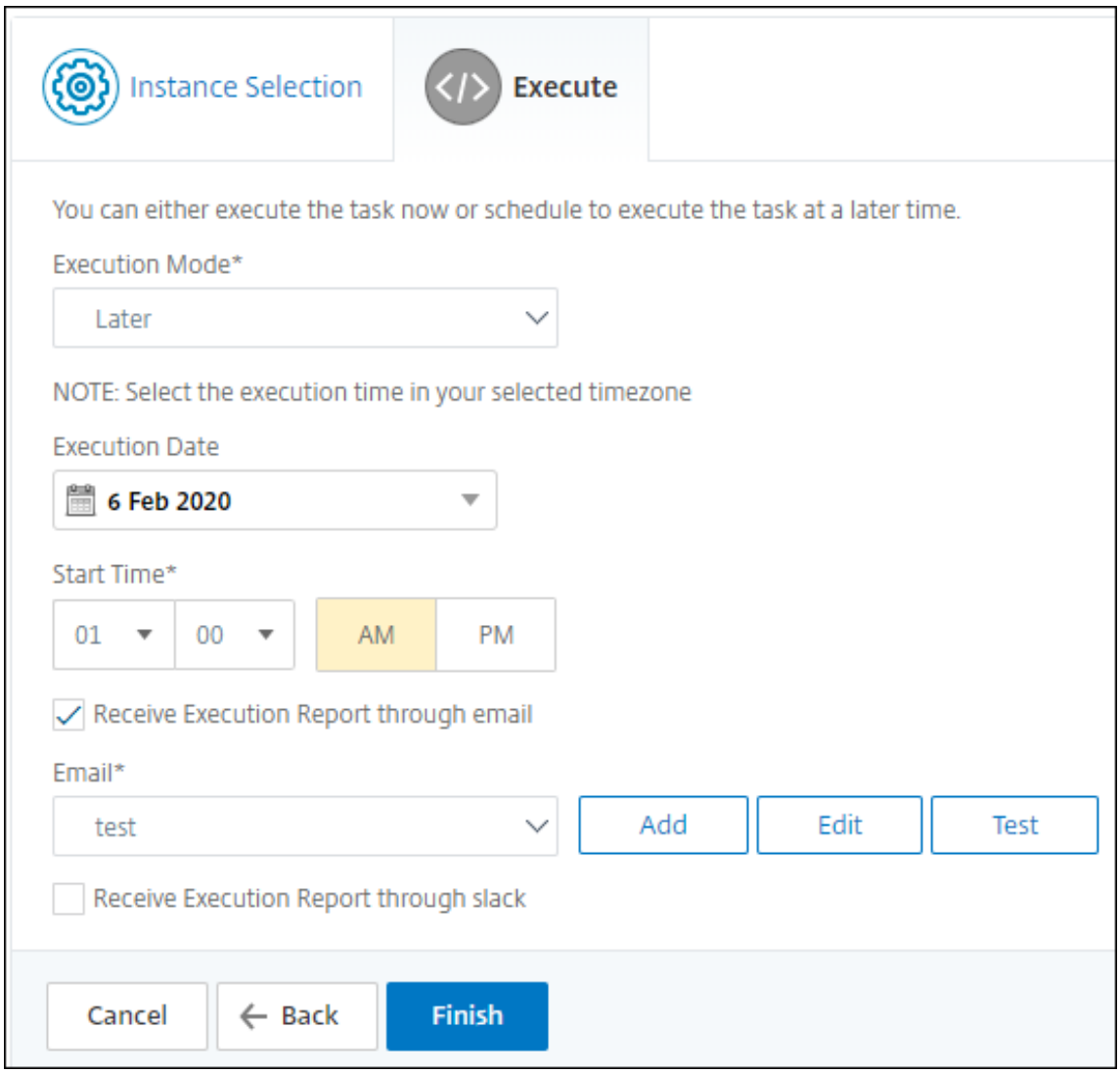
5. In **Execute**können Sie entscheiden, ob Sie jetzt oder zu einem späteren Zeitpunkt ein HA-Paar erstellen möchten.

   a) Wählen Sie im **Ausführungsmodus**einen der folgenden Ausführungsmodi aus:

   - **Jetzt** —Wählen Sie diese Option, um jetzt ein HA-Paar zu erstellen.
   - **Später** - Wählen Sie diese Option, um ein HA-Paar zu einem bestimmten Datum und einer bestimmten Uhrzeit zu erstellen.

   b) Wenn Sie **Später** in der Liste **Ausführungsmodus** ausgewählt haben, wählen Sie **Ausführungsdatum** und **Startzeit** aus, wenn Sie diesen Task ausführen möchten.

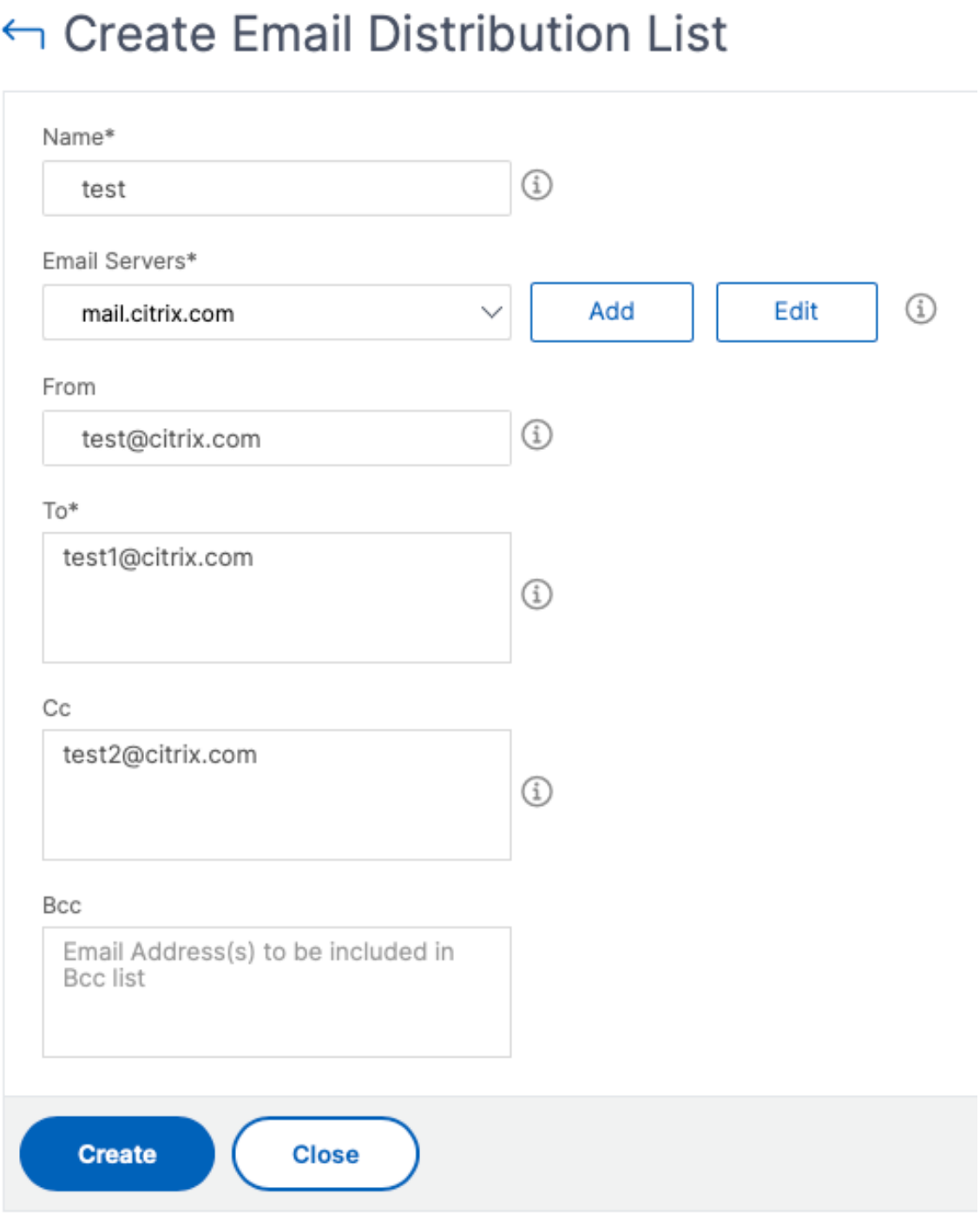
   > **Hinweis**
   >
   > Die Ausführungszeit wird in der Zeitzone angezeigt, die in NetScaler ADM festgelegt ist.



Sie können einen Ausführungsbericht dieser Aufgabe über Folgendes erhalten:

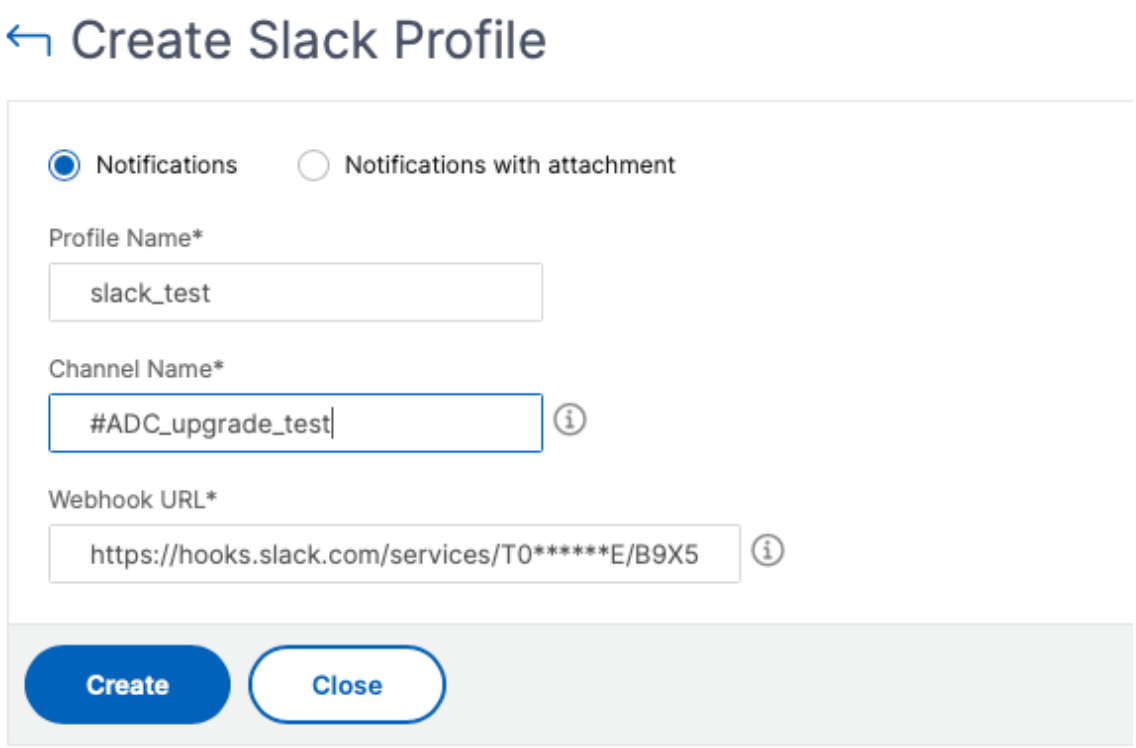
- **E-Mail** —Wählen Sie den E-Mail-Versand aus der Liste aus.

  Um eine Verteilerliste hinzuzufügen, klicken Sie auf **Hinzufügen**. Geben Sie die erforderlichen Parameter an, um die Verteilerliste hinzuzufügen, und klicken Sie auf **Erstellen**.



- **Slack** —Wähle das Slack-Profil aus der Liste aus.

  Um ein Slack-Profil hinzuzufügen, klicken Sie auf **Hinzufügen**. Geben Sie den **Profilnamen**, den **Kanalnamen**und das **Token** an und klicken Sie auf **Erstellen**.



Backup und Wiederherstellen von NetScaler-Instanzen

February 5, 2024

Sie können den aktuellen Status einer NetScaler Instanz sichern und später die gesicherten Dateien verwenden, um sie in demselben Zustand wiederherzustellen. Erstellen Sie immer ein Backup einer Instance, bevor Sie sie aktualisieren oder aus Vorsichtsgründen. Backup eines stabilen Systems ermöglicht es Ihnen, es wieder zu einem stabilen Punkt wiederherzustellen, wenn es instabil wird.

Es gibt mehrere Möglichkeiten, Backups und Wiederherstellungen auf einer NetScaler-Instanz durchzuführen. Sie können manuell ein Backup der NetScaler Konfigurationen mit der GUI und der CLI anlegen und es wiederherstellen. Sie können NetScaler ADM auch verwenden, um automatische Backups und manuelle Wiederherstellungen durchzuführen.

NetScaler ADM sichert den aktuellen Status der verwalteten NetScaler-Instanzen mithilfe von NITRO -Aufrufen und der Secure Shell (SSH) und Secure Copy (SCP) Protokolle.

NetScaler ADM erstellt ein vollständiges Backup und stellt die folgenden NetScaler-Instanztypen wieder her:

- NetScaler SDX

- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

> **Hinweis:**
>
> - Stellen Sie sicher, dass das NetScaler ADM-Profil über Administratorzugriff verfügt, um ADC-Instanzen zu Backup und wiederherzustellen.
> - Von NetScaler ADM aus können Sie den Backup- und Wiederherstellungsvorgang auf einem NetScaler 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/device_backup/
<!--NeedCopy-->
```

Um Probleme aufgrund der Nichtverfügbarkeit von Speicherplatz zu vermeiden, können Sie in diesem Verzeichnis maximal 50 Backupdateien pro ADC-Instanz speichern.

Um NetScaler-Instanzen zu sichern und wiederherzustellen, müssen Sie zunächst die Backupeinstellungen auf NetScaler ADM konfigurieren. Nach der Konfiguration der Einstellungen können Sie eine einzelne NetScaler-Instanz oder mehrere Instanzen auswählen und eine Backup der Konfigurationsdateien in diesen Fällen erstellen. Bei Bedarf können Sie die NetScaler-Instanzen auch mithilfe dieser gesicherten Dateien wiederherstellen.

Konfigurieren der Einstellungen für das Instanzbackup

Auf der Seite **Instanz Backup Settings** können Sie Einstellungen in NetScaler ADM konfigurieren, um eine ausgewählte NetScaler Instanz oder mehrere Instanzen zu sichern:

1. Navigieren Sie in NetScaler ADM zu **Einstellungen** > **Administration**.
2. Wählen Sie unter **Backup** die Option **System- und Instanz-Backup konfigurieren** aus.
3. Wählen Sie **Instance** aus und geben Sie Folgendes an:
    - **Instanzbackup aktivieren**: NetScaler ADM ist standardmäßig für das Erstellen von Backups von NetScaler Instanzen aktiviert. Deaktivieren Sie diese Option, wenn Sie keine Sicherungsdateien für die Instanzen erstellen möchten.
    - **Datei mit Kennwort schützen**: (optional) Wählen Sie die Option zum Kennwortschutz, um die Sicherungsdatei zu verschlüsseln. Durch die Verschlüsselung der Sicherungsdatei

wird sichergestellt, dass alle vertraulichen Informationen in der Sicherungsdatei sicher sind.

> **Hinweis:**
>
> Sie können die verschlüsselte Sicherungsdatei auf Ihren lokalen Computer herunterladen, aber Sie können die Datei weder mit der NetScaler ADM-GUI noch mit einem Texteditor öffnen. Beim Wiederherstellen der verschlüsselten Backupdatei werden Sie aufgefordert, das Kennwort anzugeben. Sie können jedoch eine unverschlüsselte Sicherungsdatei auf Ihrem System öffnen.

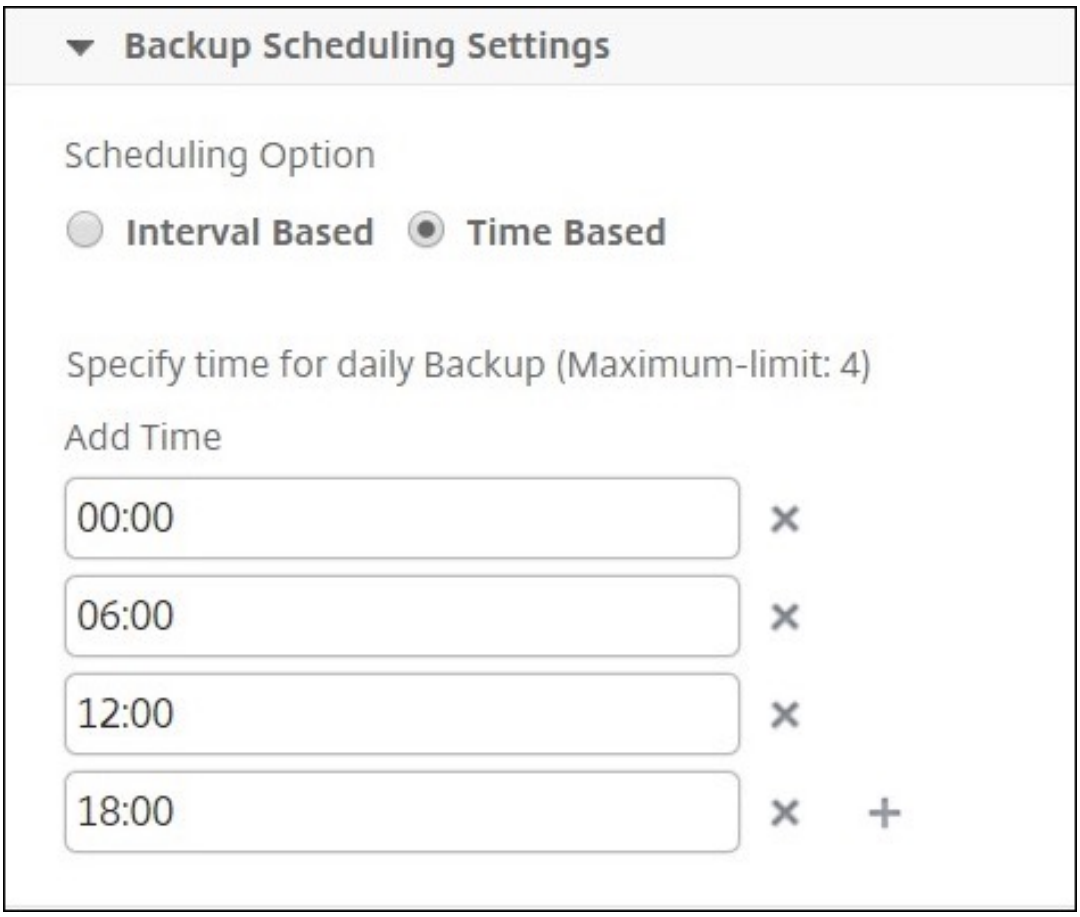
- **Anzahl der beizubehaltenden Backupdateien**: Geben Sie die Anzahl der Backupdateien an, die in NetScaler ADM aufbewahrt werden sollen. Sie können bis zu 50 Backup-Dateien pro ADC-Instance aufbewahren. Der Standardwert ist drei Backupdateien.

  > **Hinweis:**
  >
  > Jede Sicherungsdatei entspricht einem gewissen Speicherbedarf. Wir empfehlen, dass Sie eine optimale Anzahl von NetScaler-Backupdateien gemäß Ihren Anforderungen auf NetScaler ADM speichern.

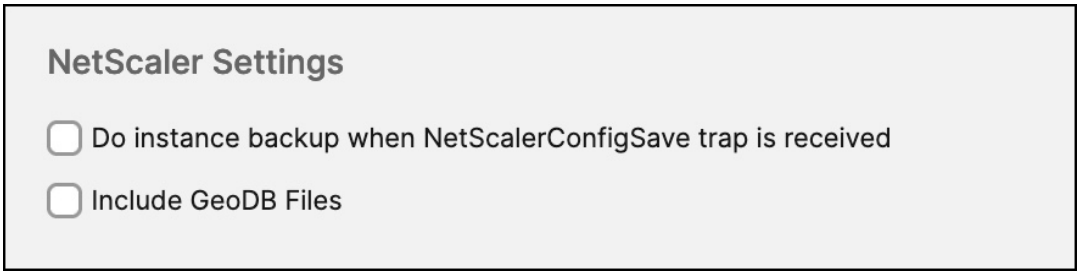
- **Einstellungen für die Backupplanung**: (optional) Zum Erstellen von Backupdateien stehen zwei Optionen zur Verfügung, obwohl Sie jeweils nur eine Option verwenden können:

  a) Die Standardoption für die Backupplanung ist “intervalbasiert”. Nach Ablauf des angegebenen Intervalls wird in NetScaler ADM eine Sicherungsdatei erstellt. Das Standardintervall für Backups ist 12 Stunden.

  b) Sie können auch den Typ der geplanten Backups in “zeitbasiert”ändern. Geben Sie in dieser Option die Uhrzeit im `hours:minutes` Format an, um Instanzen zur angegebenen Zeit zu sichern. Mit NetScaler ADM können maximal vier tägliche Backups auf den Instanzen durchgeführt werden.



- **NetScaler Einstellungen**: (optional) Standardmäßig erstellt NetScaler ADM keine Backupdatei, wenn das Trap "NetScalerConfigSave"empfängt. Sie können jedoch die Option aktivieren, eine Sicherungsdatei zu erstellen, wenn eine NetScaler-Instanz einen „NetScalerConfigSave"-Trap an NetScaler ADM sendet. Eine NetScaler-Instanz sendet jedes Mal „NetScalerConfigSave", wenn die Konfiguration auf der Instanz gespeichert wird.
- **Geodatabase-Dateien**: (optional) Standardmäßig erstellt NetScaler ADM keine Sicherungskopien der GeoDatabase-Dateien. Sie können die Option aktivieren, um ein Backup dieser Dateien auch zu erstellen.



- **Externe Übertragung:**(optional) Mit NetScaler ADM können Sie die Backupdateien der NetScaler Instanz an einen externen Speicherort übertragen:

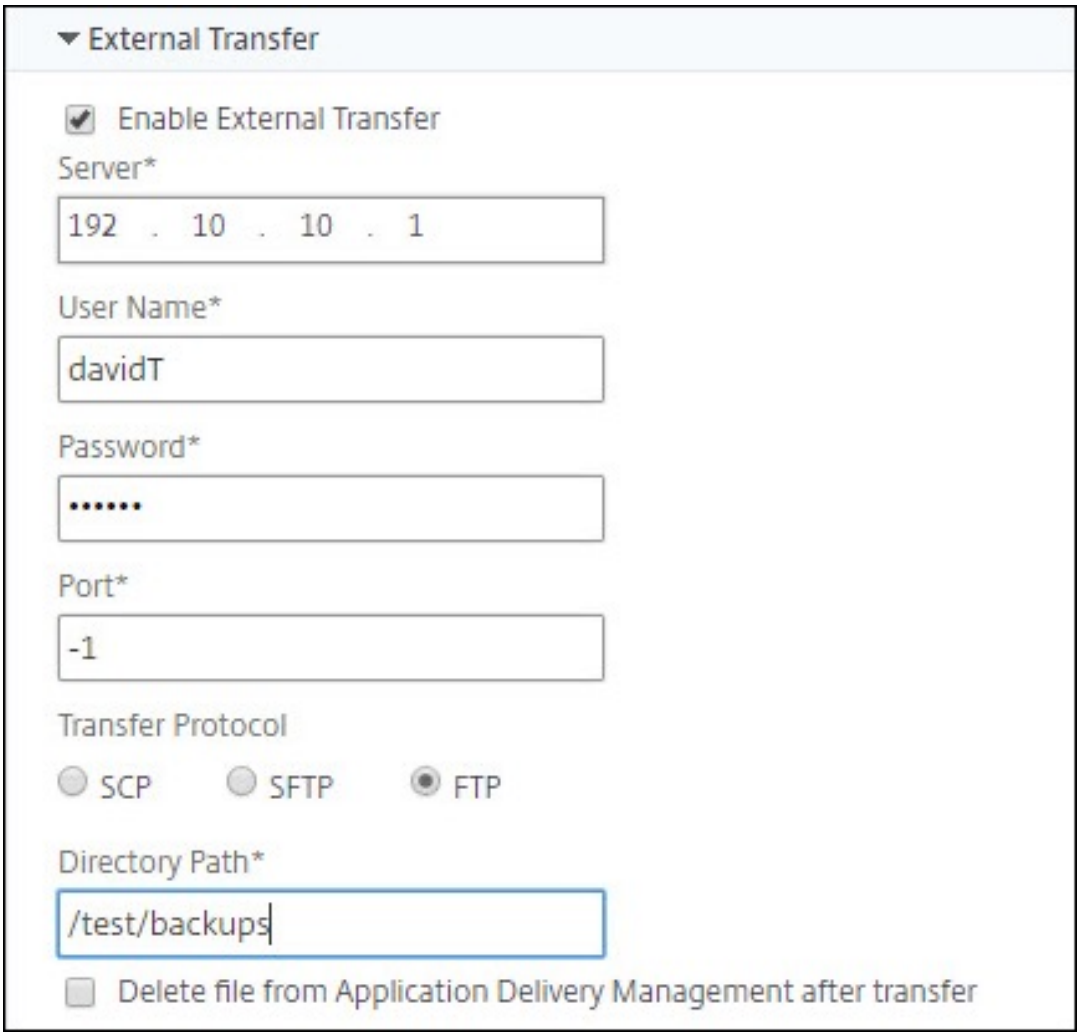
a) Geben Sie die IP-Adresse des Standorts an.

b) Geben Sie den Benutzernamen und das Kennwort des externen Servers an, auf den Sie die Backupdateien übertragen möchten.

c) Geben Sie das Übertragungsprotokoll und die Portnummer an.

d) Sie können den Verzeichnispfad angeben, in dem die Datei gespeichert werden muss.

e) Optional können Sie die Sicherungsdatei auch aus NetScaler ADM löschen, nachdem Sie sie auf den externen Server übertragen haben.



Hinweis:

NetScaler ADM sendet einen SNMP-Trap oder eine Syslog-Benachrichtigung an sich selbst, wenn für eine der ausgewählten NetScaler-Instanzen ein Backup-Fehler auftritt.

Erstellen eines Backups für eine ausgewählte NetScaler-Instanz über NetScaler ADM

Führen Sie diese Aufgabe aus, wenn Sie eine ausgewählte NetScaler-Instanz oder mehrere Instanzen sichern möchten:

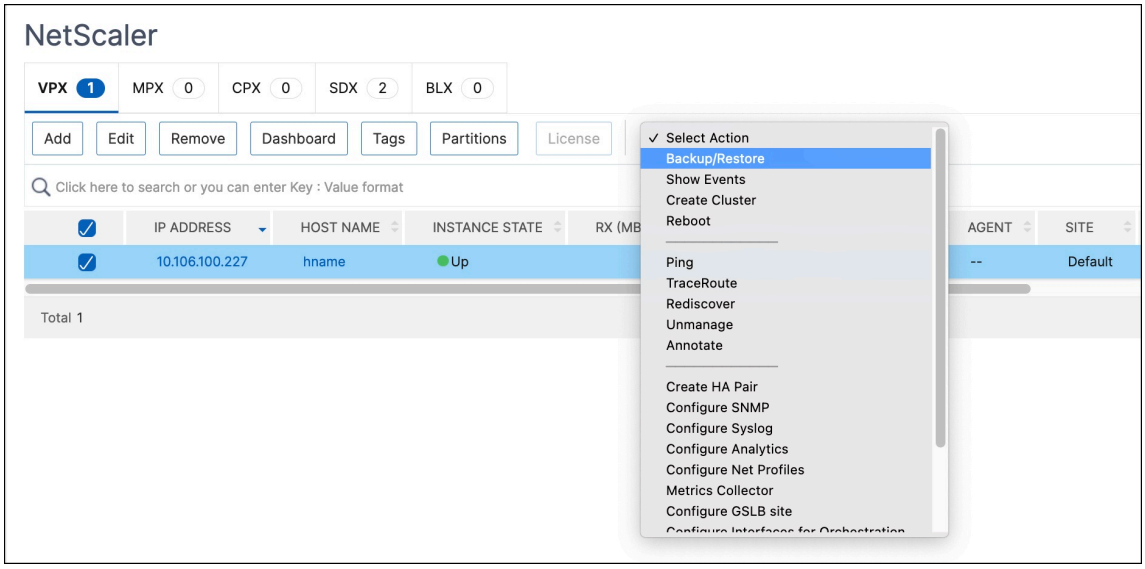
1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Instanzen**. Wählen Sie unter**Instances**den Instanztyp (z. B. NetScaler VPX) aus, der auf dem Bildschirm angezeigt werden soll.
2. Wählen Sie die Instanz aus, die Sie sichern möchten.
    - Wählen Sie für MPX-, VPX- und BLX-Instanzen in der Liste **Aktion auswählen** die Option**Backup/Wiederherstellen** aus.
    - Klicken Sie für eine SDX-Instanz auf **Backup/Restore**.
3. Klicken Sie auf der Seite **Backupdateien** auf **Backup**.
4. Sie können angeben, ob die Backupdatei verschlüsselt werden soll, um mehr Sicherheit zu gewährleisten. Sie können entweder Ihr Kennwort eingeben oder das globale Kennwort verwenden, das Sie zuvor auf der Seite Instanz-Backup-Einstellungenangegeben haben.
5. Klicken Sie auf **Weiter**.

Wiederherstellen einer NetScaler-Instanz über NetScaler ADM

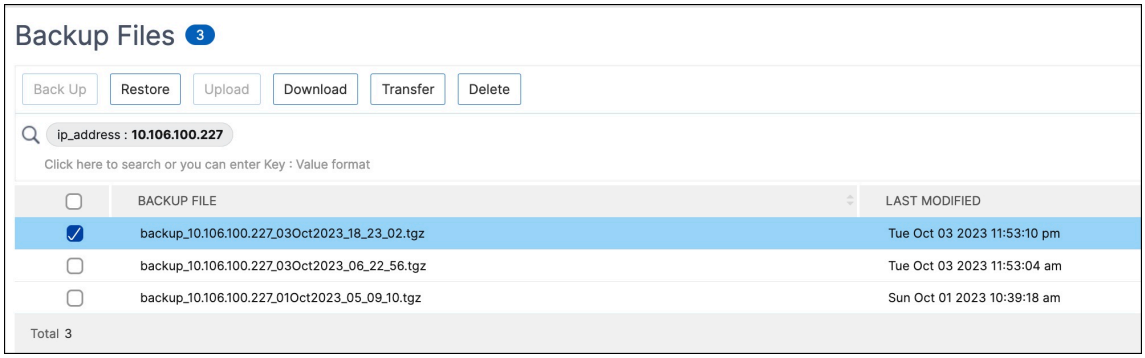
> **Hinweis:**
>
> Wenn Sie NetScaler-Instanzen in einem HA-Paar haben, müssen Sie Folgendes beachten:
>
> - Stellen Sie dieselbe Instanz wieder her, aus der die Backupdatei erstellt wurde. Betrachten wir beispielsweise ein Szenario, dass ein Backup von der primären Instanz des HA-Paares genommen wurde. Stellen Sie während des Wiederherstellungsvorgangs sicher, dass Sie dieselbe Instanz wiederherstellen, auch wenn es sich nicht mehr um die primäre Instanz handelt.
> - Wenn Sie den Wiederherstellungsprozess auf der primären ADC-Instanz initiieren, können Sie nicht auf die primäre Instanz zugreifen und die sekundäre Instanz wird in **STAYSECONDARY**geändert. Sobald der Wiederherstellungsprozess auf der primären Instanz abgeschlossen ist, wechselt die sekundäre ADC-Instanz vom Modus **STAYSECONDARY** in den **ENABLED-Modus** und wird wieder Teil des HA-Paars. Sie können mit einer möglichen Ausfallzeit auf der primären Instanz rechnen, bis der Wiederherstellungsprozess abgeschlossen ist.

Führen Sie diese Aufgabe aus, um eine NetScaler-Instanz mithilfe der zuvor erstellten Backupdatei wiederherzustellen:

1. Navigieren Sie zu**Infrastruktur > Instanzen**, wählen Sie die Instanz aus, die Sie wiederherstellen möchten, und klicken Sie dann auf**Aktion auswählen > Sicherung/Wiederherstellung**.



2. Wählen Sie auf der Seite**Backupdateien**die Backupdatei aus, die die wiederherzustellenden Einstellungen enthält, und klicken Sie dann auf**Wiederherstellen**.



Wiederherstellen einer NetScaler SDX-Appliance mit NetScaler ADM

In NetScaler ADM umfasst das Backup der NetScaler SDX-Appliance Folgendes:

- NetScaler-Instanzen, die auf der Appliance gehostet werden
- SVM-SSL-Zertifikate und -Schlüssel
- Einstellungen für die Instanzbereinigung (im XML-Format)
- Instanzbackupeinstellungen (im XML-Format)
- Abfrageeinstellungen für SSL-Zertifikate (im XML-Format)
- SVM-Datenbankdatei
- NetScaler Konfigurationsdateien von Geräten, die auf SDX vorhanden sind
- NetScaler Build-Images

- NetScaler XVA-Images, diese Images werden am folgenden Speicherort gespeichert: `/var/mps/sdx_images/`
- SDX-Einzelpaket-Image (SVM+XS)
- Instanz-Images von Drittanbietern (sofern bereitgestellt)

Stellen Sie Ihre NetScaler SDX-Appliance auf die in der Sicherungsdatei verfügbare Konfiguration wieder her. Während der Wiederherstellung der Appliance wird die gesamte aktuelle Konfiguration gelöscht.

Wenn Sie die NetScaler SDX-Appliance mithilfe einer Backup einer anderen NetScaler SDX-Appliance wiederherstellen, stellen Sie sicher, dass Sie die Lizenzen hinzufügen und die Management Service-Netzwerkeinstellungen der neuen Appliance so konfigurieren, dass sie mit den Einstellungen in der Sicherungsdatei übereinstimmen, bevor Sie den Wiederherstellungsvorgang starten. Das heißt, die neue Appliance muss lizenziert sein und die Mindestlizenzanforderungen der Backup-Datei erfüllen. Wenn das Backup beispielsweise fünf VPX-Instances mit insgesamt 5 GB hatte, muss die neue Appliance auch in der Lage sein, diese Anforderungen zu unterstützen. Oder wenn die Backup-Appliance über eine Platin-Lizenz verfügte, muss die neue Appliance über dieselbe oder eine höhere Lizenz verfügen. Netzwerkeinstellungen wie IP-Adresse, Netzmaske, Gateway, XenServer-IP-Adresse und DNS-Server müssen auf der neuen Appliance ordnungsgemäß konfiguriert sein.

Bevor Sie die SDX-Appliance wiederherstellen, stellen Sie sicher, dass die gesicherte SDX-Appliance-Plattformvariante mit der Appliance identisch ist. Sie können nicht von einer anderen Plattformvariante wiederherstellen.

> **Hinweis:**
>
> Bevor Sie eine SDX RMA-Appliance wiederherstellen, stellen Sie sicher, dass die gesicherte Version entweder der RMA-Version entspricht oder höher ist.

So stellen Sie die SDX-Appliance aus der gesicherten Datei wieder her:

1. Navigieren Sie in der NetScaler ADM GUI zu **Infrastructure > Instances > NetScaler > SDX**. Wählen Sie eine Instanz aus.
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 neu verpackte Backupdatei aus und klicken Sie auf **Wiederherstellen**.

Failovers auf die sekundäre NetScaler-Instanz erzwingen

February 5, 2024

Möglicherweise möchten Sie einen Failover erzwingen, wenn Sie beispielsweise die primäre Citrix Application Delivery Controller (ADC) -Instanz ersetzen oder aktualisieren müssen. Sie können ein Failover entweder 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 aktiv ist.

Ein erzwungenes Failover wird nicht weitergegeben oder synchronisiert. Um den Synchronisierungsstatus nach einem erzwungenen Failover anzuzeigen, können Sie den Status der Instanz anzeigen.

Ein erzwungenes Failover schlägt unter den 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 ihr Status AKTIV ist, um ein Failover zu erzwingen.
- Die sekundäre Instanz ist konfiguriert, um sekundär zu bleiben.

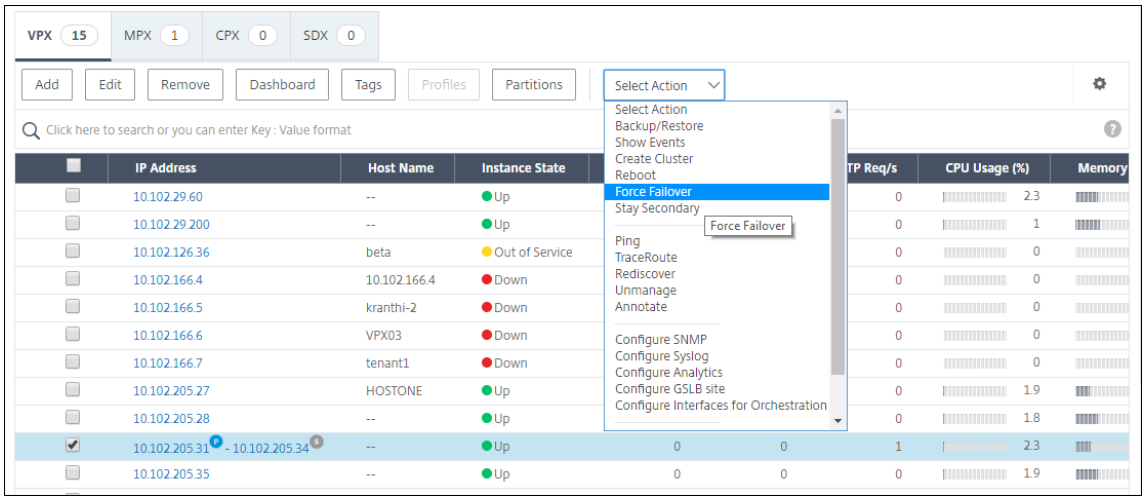
Die NetScaler-Instanz zeigt eine Warnmeldung an, wenn ein potenzielles Problem beim Ausführen des Force-Failoverbefehls erkannt wird. Die Nachricht enthält die Informationen, die die Warnung ausgelöst haben, und fordert eine Bestätigung an, bevor Sie fortfahren.

Sie können ein Failover auf einer primären Instanz oder einer sekundären Instanz erzwingen.

So erzwingen Sie ein Failover auf die sekundäre NetScaler-Instanz mithilfe von NetScaler ADM:

1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zu **Infrastructure > Instances > NetScaler > VPX** Tab und wählen Sie dann 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 Menü **Aktion** die Option **Force Failover**aus.

4. Klicken Sie auf **Ja**, um die Aktion “Failover erzwingen”zu bestätigen.



Erzwingen, dass eine sekundäre NetScaler-Instanz sekundär bleibt

February 5, 2024

In einem HA-Setup kann der sekundäre Knoten unabhängig vom Status des primären Knotens gezwungen werden, sekundär 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. Sie möchten, dass er der sekundäre Knoten bleibt, selbst wenn er einen Fehler im primären Knoten erkennt.

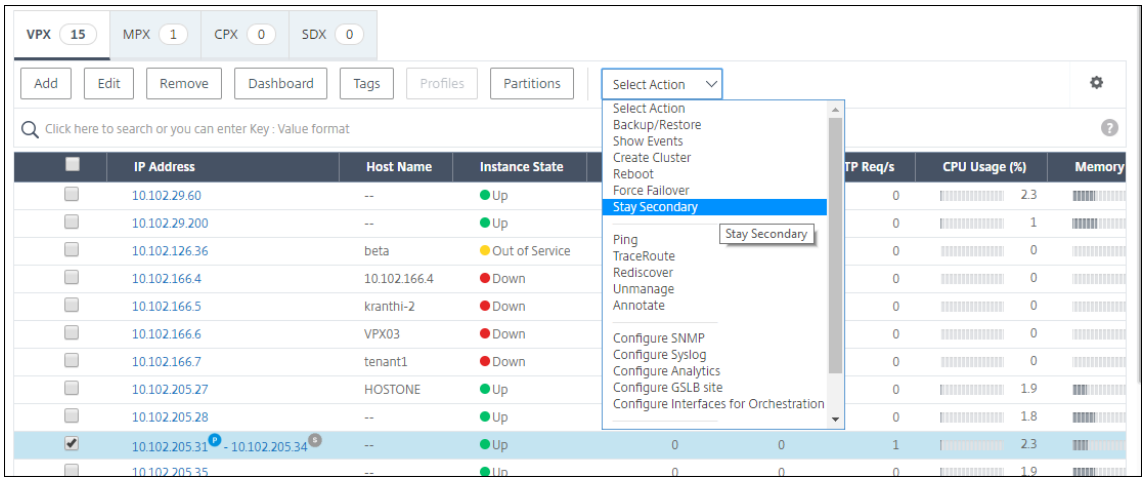
Wenn Sie den sekundären Knoten zwingen, sekundär zu bleiben, bleibt er sekundär, selbst wenn der primäre Knoten ausfällt. Wenn Sie erzwingen, dass der Status eines Knotens in einem HA-Paar sekundär bleibt, nimmt er nicht an Übergängen des HA-Zustands der Maschine teil. Der Status des Knotens wird als STAYSECONDARY angezeigt.

> **Hinweis**
>
> Wenn Sie ein System zwingen, sekundär zu bleiben, wird der erzwungene Prozess weder propagiert noch synchronisiert. Sie wirkt sich nur auf den Knoten aus, auf dem Sie den Befehl ausführen.

So konfigurieren Sie mithilfe von NetScaler ADM eine sekundäre NetScaler-Instanz, um mithilfe von NetScaler ADM sekundär zu bleiben:

1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zu **Infrastructure > Instances **NetScaler>VPX** Tab und wählen Sie dann 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 Menü **Aktion** die Option **Sekundär bleiben**aus.
4. Klicken Sie auf **Ja**, um die Ausführung der Aktion “Sekundär bleiben”zu bestätigen.



Instanzgruppen erstellen

February 5, 2024

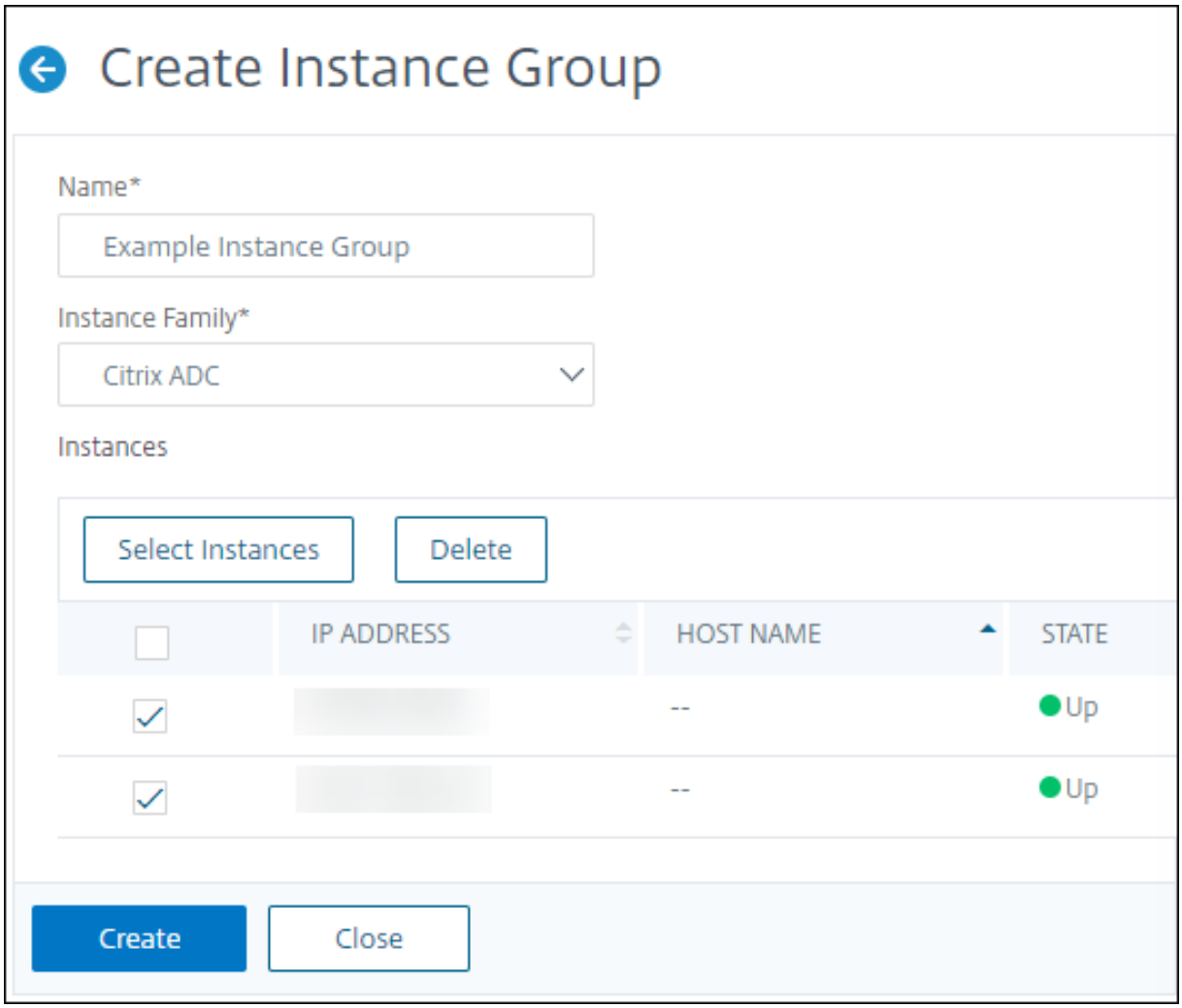
Um eine Instanzgruppe zu erstellen, müssen Sie zuerst alle NetScaler-Instanzen zu NetScaler ADM hinzufügen. Nachdem Sie die Varianten erfolgreich hinzugefügt haben, erstellen Sie Instanzgruppen basierend auf ihrer Instanzfamilie. Das Erstellen einer Gruppe von Instanzen hilft Ihnen dabei, für die gruppierten Instanzen gleichzeitig Upgrades und Backups zu erstellen oder sie wiederherzustellen.

So erstellen Sie eine Instanzgruppe mit NetScaler ADM

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Instanzgruppen**, und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie einen Namen für Ihre Instanzgruppe an, und wählen Sie **NetScaler** aus der Liste **Instanzfamilie** aus.
3. Klicken Sie auf **Instanz auswählen**. Wählen Sie auf der Seite **Instanzen auswählen** die Instanzen aus, die Sie gruppieren möchten, und klicken Sie auf **Auswählen**.

   In der Tabelle sind die ausgewählten Instanzen und ihre Details aufgeführt. Wenn Sie eine Instanz aus der Gruppe entfernen möchten, wählen Sie die Instanz aus der Tabelle aus und klicken Sie auf **Löschen** .

4. Klicken Sie auf **Erstellen**.



Bereitstellung von NetScaler VPX-Instanzen auf SDX mithilfe von ADM

February 5, 2024

Sie können mithilfe von NetScaler ADM eine oder mehrere NetScaler VPX-Instanzen auf der SDX-Appliance 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, schränkt der ADM Sie davon Provisioning, weitere NetScaler-Instanzen bereitzustellen.

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:

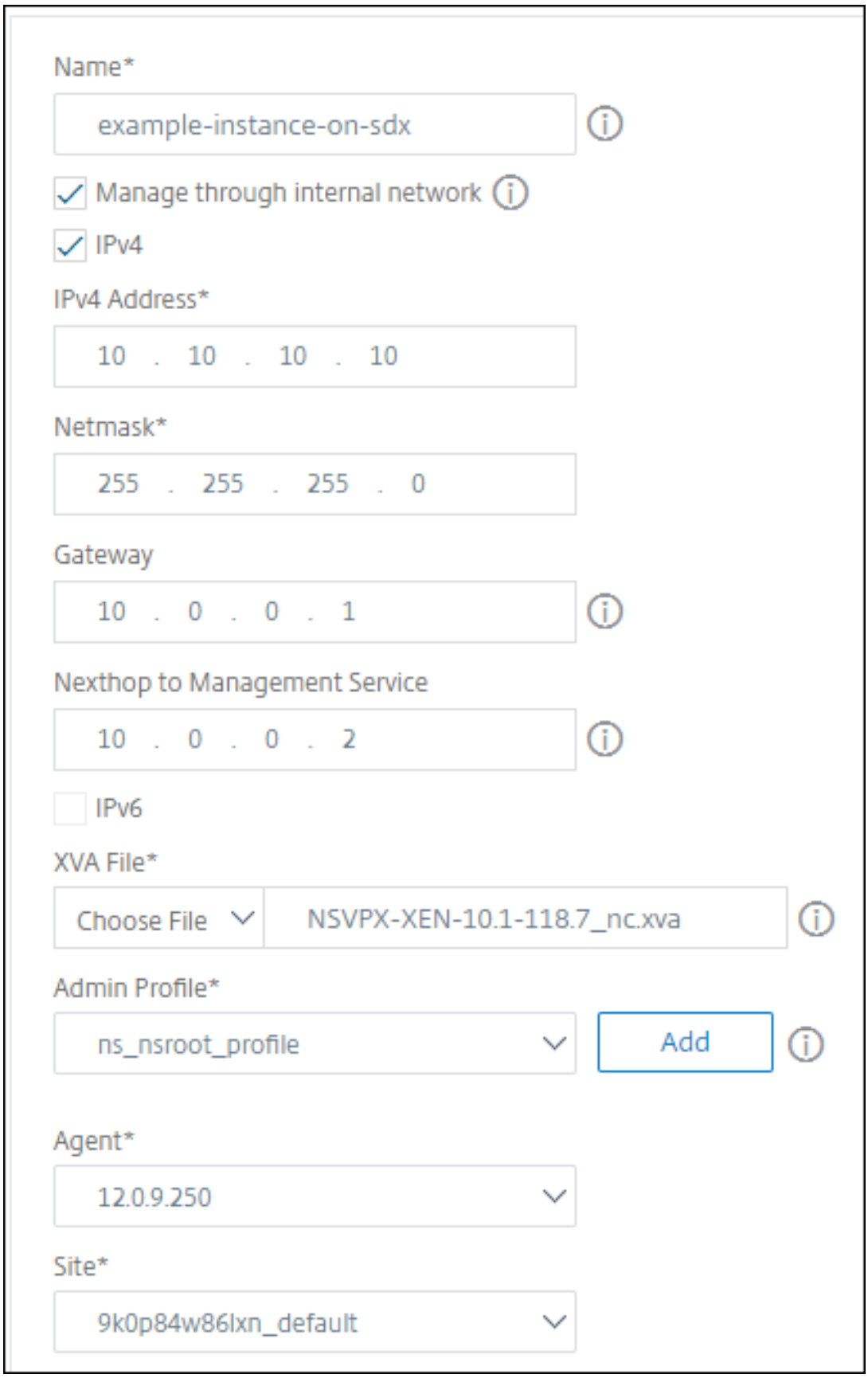
1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** .
2. Wählen Sie auf der Registerkarte **SDX** eine SDX-Instanz aus, in der Sie eine VPX-Instanz bereitstellen möchten.
3. Wählen Sie unter **Aktion auswählen** die Option **VPX bereitstellen** aus.

Schritt 1 - Hinzufügen einer VPX-Instanz

Der ADM verwendet die folgenden Informationen, um VPX-Instanzen in einer SDX-Appliance zu konfigurieren:

- **Name** - Geben Sie einen Namen für eine ADC-Instanz an.
- Richten Sie ein Kommunikationsnetzwerk zwischen SDX und VPX ein. Wählen Sie dazu die gewünschten Optionen aus der Liste aus:
  - **Über internes Netzwerk verwalten** —Diese Option richtet ein internes Netzwerk für die Kommunikation zwischen dem ADM und einer VPX-Instanz ein.
  - **IP-Adresse** - Sie können eine **IPv4-** oder **IPv6-Adresse** oder beides auswählen, um die NetScaler VPX-Instanz zu verwalten. Eine VPX-Instanz kann nur eine Verwaltungs-IP haben (auch NetScaler IP genannt). Sie können die NetScaler IP-Adresse nicht entfernen.

    Weisen Sie für die ausgewählte Option dem ADM-Server eine Netzmaske, ein Standard-Gateway 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 Agent aus, dem Sie die Instanzen zuordnen möchten
- **Site** —Wählen Sie die Site aus, zu der die Instanz hinzugefügt werden soll.



Schritt 2 —Zuteilung von Lizenzen

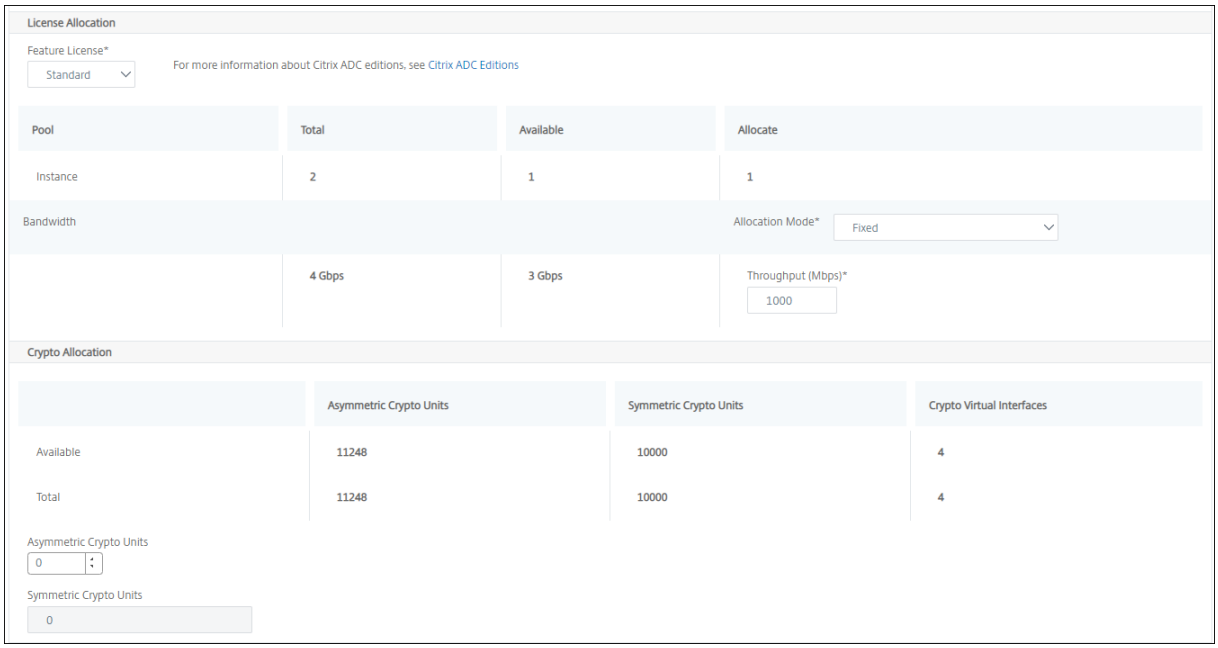
Geben Sie im Abschnitt **Lizenzzuweisung** die VPX-Lizenz an. Sie können Standard-, Advanced- und Premium-Lizenzen verwenden.

- **Zuweisungsmodus** - Sie können den **festen** oder den **Burstable-Modus** 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 for Secure Web Gateway) für Citrix Secure Web Gateway (SWG) -Instanzen auf SDX-Appliances. Dieses Instanz-Paket unterscheidet sich von der SDX-Plattformlizenz oder dem SDX-Instanzpaket.
>
> 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.

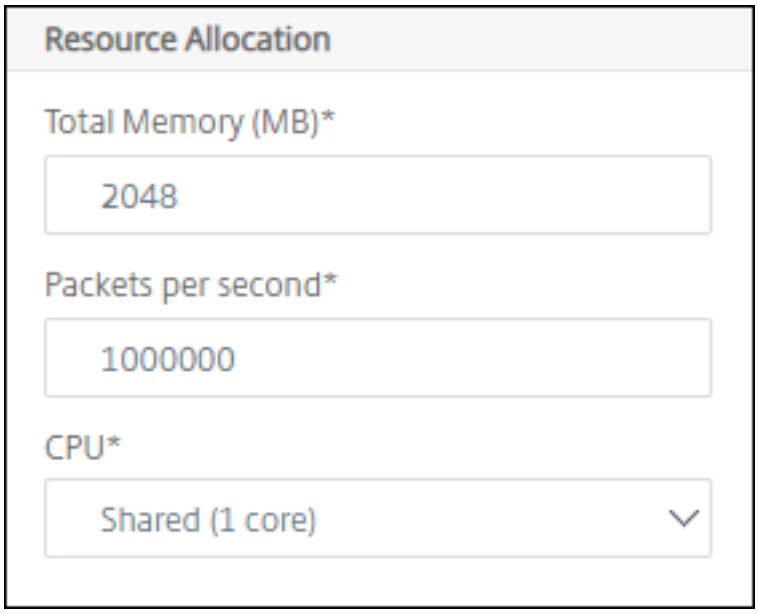
- **Gesamtspeicher (MB)** - Weisen Sie einer Instanz den gesamten Arbeitsspeicher zu. Der Mindestwert ist 2048 MB.
- **Pakete pro Sekunde** - Geben Sie die Anzahl der Pakete an, die pro Sekunde übertragen werden sollen.
- **CPU** —Geben Sie die Anzahl der CPU-Kerne für eine Instanz an. Sie können gemeinsam 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 der Ressourcenknappheit verwenden.

  Starten Sie Instanzen neu, auf denen CPU-Kerne neu zugewiesen wurden, um Leistungseinbußen

  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 außerdem maximal 11 Kerne zuweisen.

  > **Hinweis**
  >
  > Für eine Instanz beträgt der maximale Durchsatz, den Sie konfigurieren, 180 Gbit/s.



In der folgenden Tabelle sind die unterstützte VPX, die Single Bungle-Image-Version und die Anzahl der Kerne aufgeführt, die Sie einer Instanz zuweisen können:

Plattformname	Kerne insgesamt	Gesamtzahl der für VPX-Provisioning verfügbaren Kerne	Maximale Kerne, die einer einzelnen Instanz zugewiesen werden können
SDX 8015, SDX 8400 und SDX 8600	4	3	3
SDX 8900	8	7	7
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
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS und SDX 14100. FIPS	12	10	5

Plattformname	Kerne insgesamt	Gesamtzahl der für VPX-Provisioning verfügbaren Kerne	Maximale Kerne, die einer einzelnen Instanz zugewiesen werden können
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
SDX 16000	64	30	16
SDX 9100	20	9	9

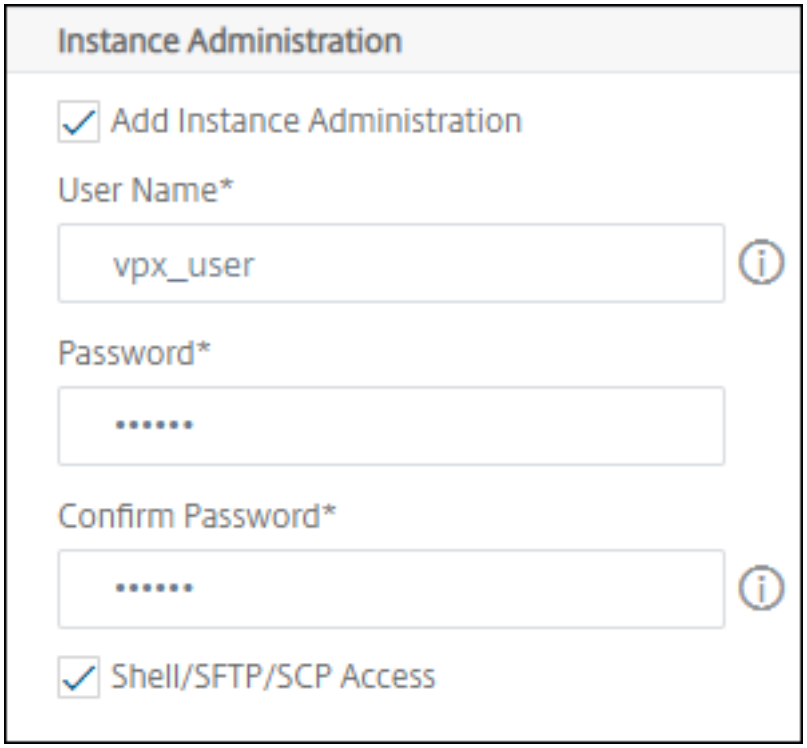
> **Hinweis:**
>
> Auf der SDX 26xxx-Plattform können einer VPX-Instanz maximal 26 CPU-Kerne zugewiesen werden. Wenn der Instanz Kryptoeinheiten zugewiesen sind, hängt die maximale Anzahl von Kernen von der Anzahl der Kryptoeinheiten und Datenschnittstellen ab.
>
> Wenn Sie beispielsweise einer Instanz 24000 Kryptoeinheiten 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 Kryptoeinheiten schlägt die Bereitstellung von VPX-Instanzen 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 NetScaler-Instanzadministrator. Dieser Benutzer hat 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 NetScaler-Instanzadministrator**gewährt wird. Diese Option ist standardmäßig ausgewählt.



Schritt 5 —Netzwerkeinstellungen festlegen

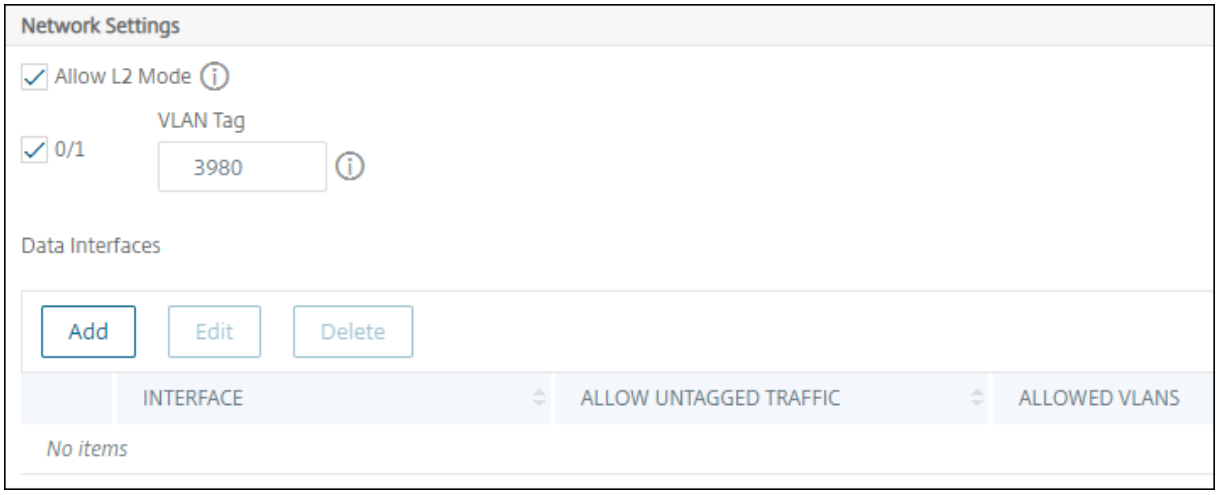
Wählen Sie die erforderlichen Netzwerkeinstellungen für eine Instanz aus:

- **L2-Modus unter Netzwerkeinstellungen** zulassen: Sie können den L2-Modus auf der NetScaler-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 NetScaler-Instanz.

  > **Hinweis**
  >
  > Wenn Sie den L2-Modus für eine Instanz deaktivieren, müssen Sie sich bei der Instanz anmelden und den L2-Modus von dieser Instanz aus deaktivieren. Andernfalls werden möglicherweise alle anderen NetScaler-Modi deaktiviert, nachdem Sie die Instanz neu gestartet haben.

- **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.



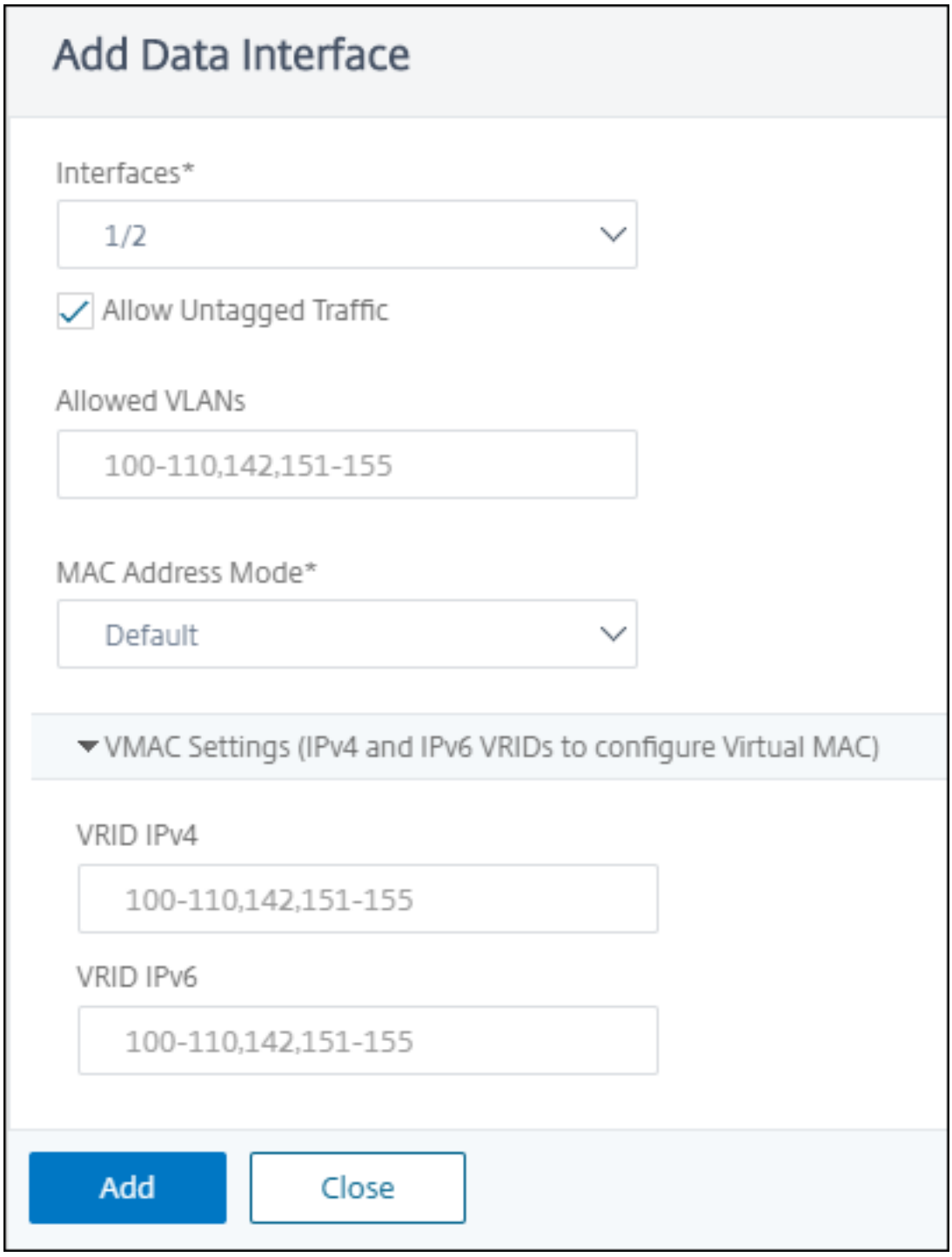
Klicken Sie unter **Datenschnittstellen**auf **Hinzufügen**, um Datenschnittstellen hinzuzufügen, und geben Sie Folgendes an:

- **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 zeigt 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 NetScaler-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 außer Kraft setzt.
  - **Generiert** - Generiert eine MAC-Adresse mithilfe der zuvor festgelegten Basis-MAC-Adresse. Informationen zum Festlegen einer MAC-Basisadresse finden Sie unter Zuweisen einer MAC-Adresse zu einer Schnittstelle.

- **VMAC-Einstellungen (IPv4- und IPv6-VRIDs zur Konfiguration des virtuellen MAC)**
  - **VRID IPV4** —Die IPv4-VRID, die den 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 —Festlegen der Management-VLAN-Einstellungen

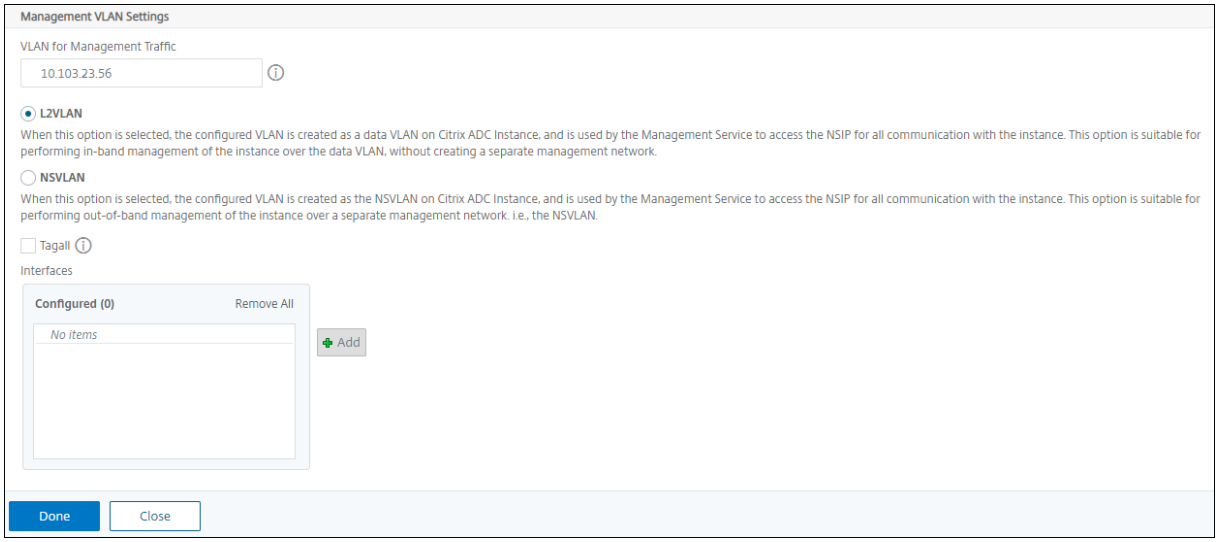
Der Verwaltungsdienst und die Verwaltungsadresse (NSIP) der VPX-Instanz befinden sich im selben Subnetz, und die Kommunikation erfolgt über eine Verwaltungsschnittstelle.

Wenn sich der Verwaltungsdienst und die Instanz in unterschiedlichen Subnetzen 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 Ihre Bereitstellung erfordert, dass NSIP während der Bereitstellung der VPX-Instanz nur über die ausgewählte Schnittstelle zugänglich ist, wählen Sie **NSVLAN**aus. Und das NSIP wird über andere Schnittstellen nicht mehr zugänglich.

- HA-Heartbeats werden nur auf 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 Befehl `clear config full` auf der VPX-Instanz löscht die VLAN-Konfiguration, wenn **NSVLAN** nicht ausgewählt ist.

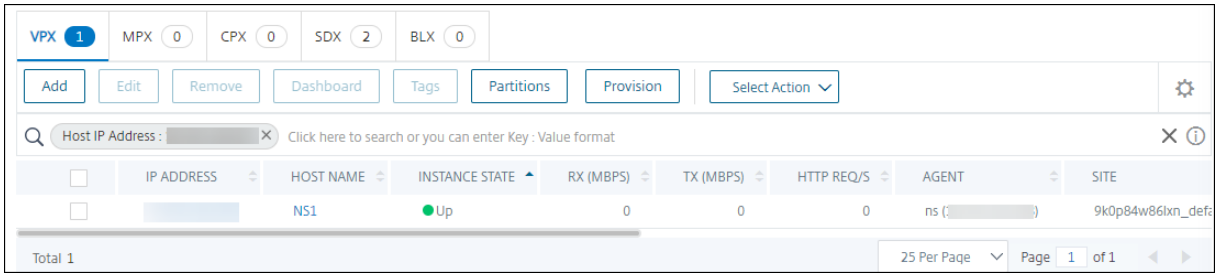


Klicken Sie auf **Fertig**, um eine VPX-Instanz bereitzustellen.

Zeigen Sie die bereitgestellte VPX-Instanz an

Führen Sie die folgenden Schritte aus, um die neu bereitgestellte Instanz anzuzeigen:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** .
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.



Rediscovery mehrerer NetScaler VPX-Instanzen

February 5, 2024

Sie können mehrere NetScaler VPX-Instanzen in Ihrem NetScaler Application Delivery Management (ADM) -Setup wiederfinden. Sie können auch mehrere NetScaler VPX-Instanzen wiederfinden, wenn Sie die neuesten Zustände und Konfigurationen dieser Instanzen einsehen möchten. Der NetScaler ADM Server erkennt alle NetScaler VPX-Instanzen erneut und überprüft, ob die Citrix Application Delivery Controller (ADC) -Instanzen erreichbar sind.

So erkennen Sie mehrere NetScaler VPX-Instanzen erneut:

1. Geben Sie in einem Webbrowser die IP-Adresse des NetScaler ADM-Servers ein (z. B.). http://192.168.100.1
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein. Die Standardanmeldeinformationen des Administrators sind `nsrootnsroot`
3. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** > **VPX** und wählen Sie die Instanzen aus, die Sie erneut ermitteln möchten.
4. Klicken **Sie im Menü Aktion auswählen** auf **Neu entdecken**.
5. 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 NetScaler VPX Instanzen angezeigt.

Verwalten einer Instanz aufheben

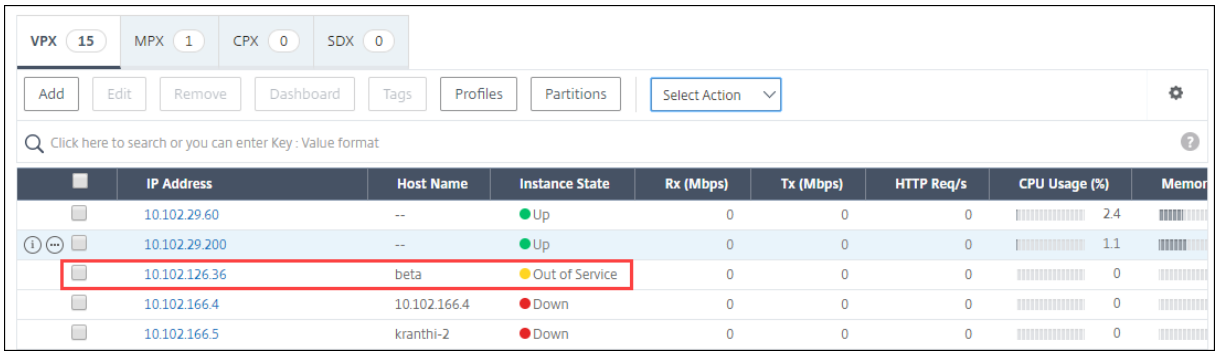
February 5, 2024

Wenn Sie den Informationsaustausch zwischen NetScaler Application Delivery Management (ADM) und den Instances in Ihrem Netzwerk beenden möchten, können Sie die Verwaltung der Instances aufheben.

So heben Sie die Verwaltung einer Instanz auf:

Navigieren Sie zur Registerkarte **Infrastruktur > Instanzen > NetScaler** > **VPX** . Klicken Sie in der Liste der Instanzen mit der rechten Maustaste auf eine Instanz, und wählen Sie dann **Verwalten aufheben**aus, oder wählen Sie die Instanz aus, und wählen Sie in der Liste **Aktion auswählen**die Option **Verwalten aufheben**aus.

Der Status der ausgewählten Instanz ändert sich in "**Abgemeldet**", wie in der folgenden Abbildung dargestellt.



Die Instanz wird nicht mehr von NetScaler ADM verwaltet und tauscht keine Daten mehr mit NetScaler ADM aus.

Tracing einer Route zu einer Instanz

February 5, 2024

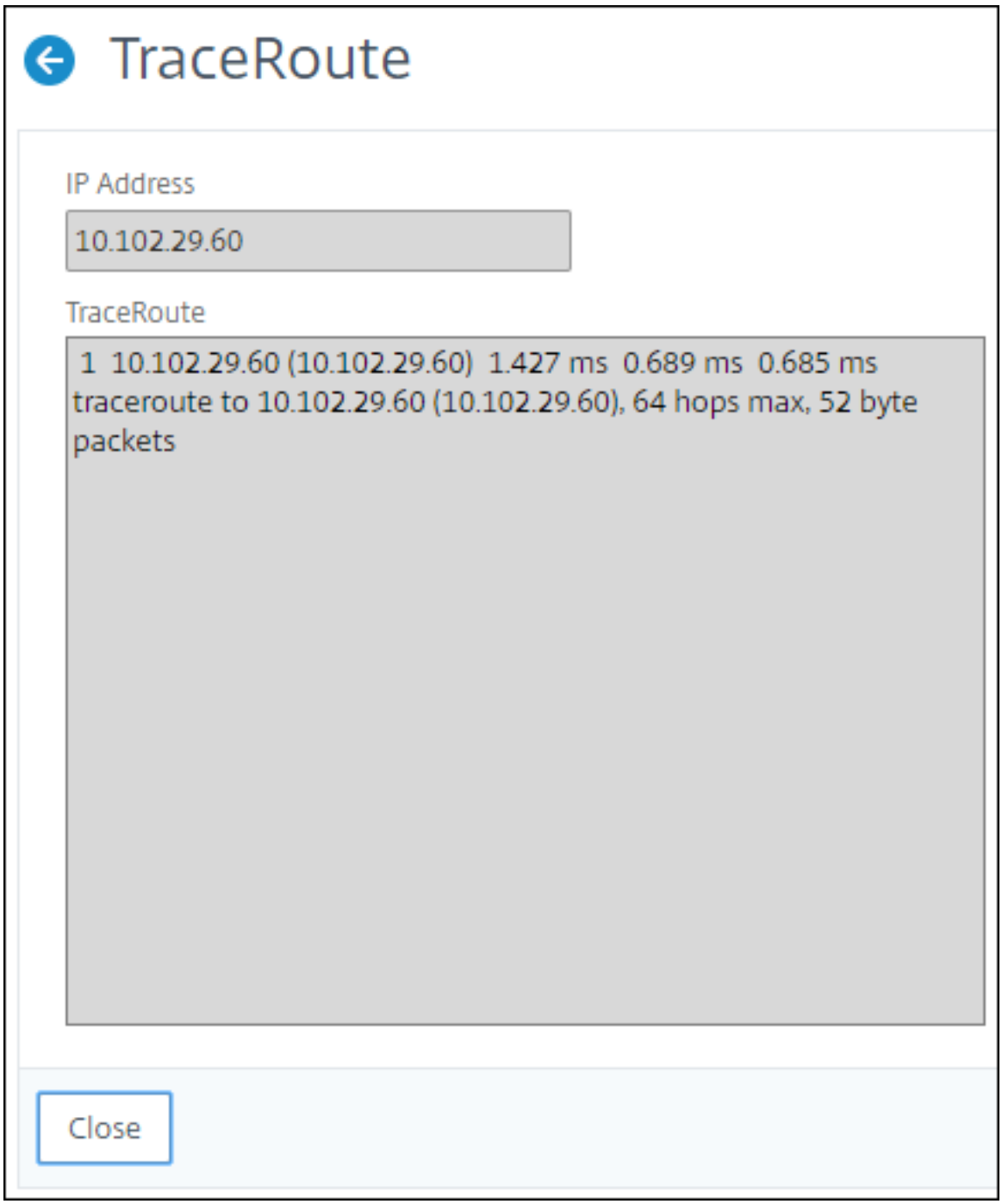
Wenn Sie die Route eines Pakets vom NetScaler Application Delivery Management (ADM) zu einer Instance verfolgen, können Sie Informationen wie die Anzahl der Hops finden, die erforderlich sind, um die Instance zu erreichen. Traceroute verfolgt den Pfad des Pakets von Quelle zu Ziel. Es zeigt die Liste 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 Traceroute, wo das Problem besteht.

So verfolgen Sie die Route einer Instanz:

1. **Navigieren Sie in NetScaler ADM zum Tab**Infrastruktur > Instances > NetScaler > VPX**.**
2. 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 im Menü **Aktion auswählen** auf **TraceRoute**.

Das **TraceRoute**-Meldungsfeld zeigt die Route zur Instance und die von jedem Hop verbrauchte Zeit in Millisekunden an.



Konfigurationen von einer NetScaler-Instanz auf eine andere replizieren

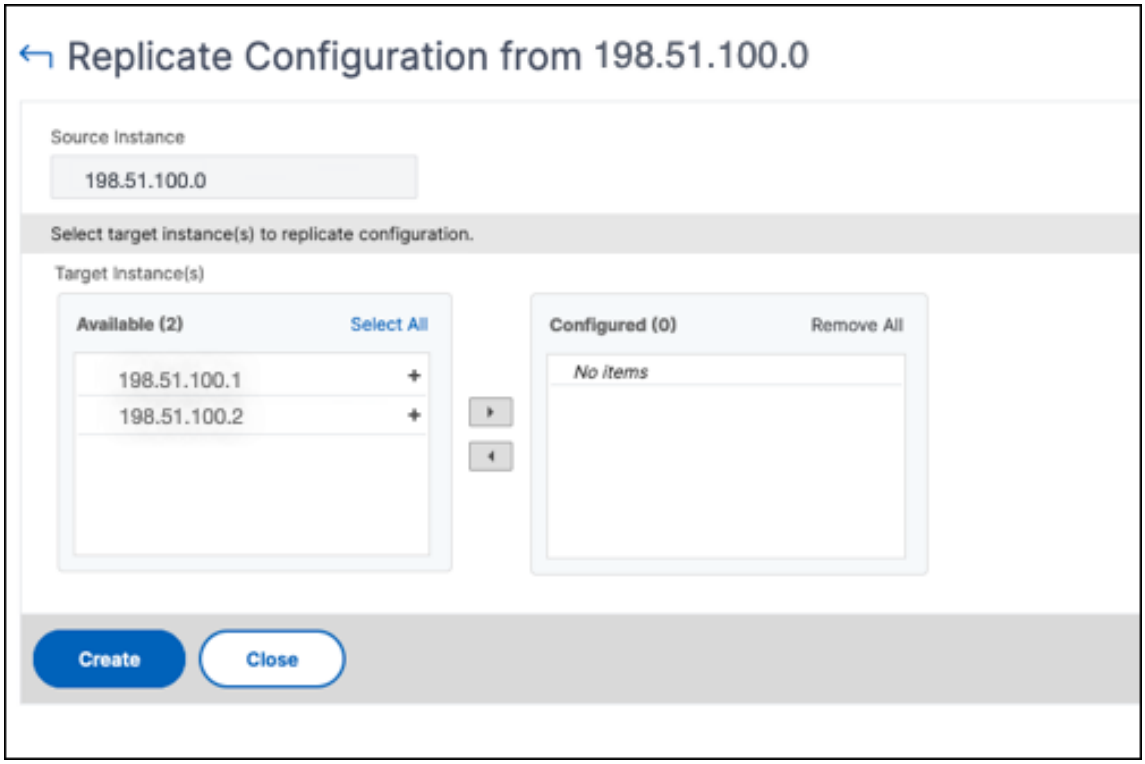
February 5, 2024

Sie können die Funktion Konfiguration replizieren von NetScaler ADM verwenden, um Konfiguratio-

nen aus einer NetScaler-Instanz zu kopieren und sie auf einer einzelnen Instanz oder vielen Instanzen zu replizieren.

Konfigurationen von einer Instanz auf andere NetScaler-Instanzen replizieren

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** . Wählen Sie die Quellinstanz aus, deren Konfigurationen Sie auf andere Instances replizieren möchten, und klicken Sie in der Liste **Aktion auswählen** auf **Konfiguration replizieren**.
2. Wählen Sie unter **Konfiguration replizieren** die Zielinstanz aus, auf die Sie die Konfigurationen aus der Quellinstanz anwenden möchten. Sie können die Konfigurationen von einer einzelnen Quellinstanz auf eine einzelne Instanz oder viele Zielinstanzen replizieren.



3. Klicken Sie auf **Erstellen**.

Die replizierten Konfigurationen werden der Liste der NetScaler-Instanzen hinzugefügt. Um den Status der replizierten Instanzen anzuzeigen, klicken Sie auf das Aktualisierungssymbol.

> **Hinweis:**
>
> Während der Replikation werden alle Netzwerk-IPs der Quellinstanz auf die Zielinstanz repliziert. Wenn sich die Zielinstanz in einem anderen Netzwerk als die Quellinstanz befindet, sind die IPs in der Zielinstanz möglicherweise nicht erreichbar. Wenn IPs nicht erreichbar sind, wird der Status der Entitäten in der Zielinstanz als Ausgefallen angezeigt.

> Um den Status der auf Ihrer verwalteten NetScaler-Instanz konfigurierten Entitäten anzuzeigen, navigieren Sie zu **Infrastruktur > Netzwerkfunktionen**.

SSL Zertifikatsverwaltung

February 5, 2024

Jede Organisation oder einzelne Website, die den Umgang mit vertraulichen oder sensiblen Informationen erfordert, muss über ein SSL-Zertifikat verfügen. Das SSL-Zertifikat auf einem Webserver garantiert die Authentizität des Webservers gegenüber dem verbindenden Client. Es authentifiziert nicht nur die Identität einer Website, sondern hilft auch bei der Generierung des Sitzungsschlüssels, der später für die Verschlüsselung der gesamten Sitzung verwendet wird.

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 Application Delivery Controller (ADC) -Appliance befindet, wird verwendet, um die Verschlüsselung und Entschlüsselung des asymmetrischen Schlüssels (oder des öffentlichen Schlüssels) abzuschließen.

NetScaler Application Delivery Management (ADM) bietet Ihnen eine einheitliche Konsole zur Automatisierung der Installation, Aktualisierung, Löschung, Verknüpfung und des Herunterladens von SSL-Zertifikaten. Es hilft dabei, den Ruf der Website und das Vertrauen der Kunden zu erhalten. NetScaler ADM optimiert jetzt alle Aspekte der Zertifikatverwaltung für Sie. Über eine einheitliche Konsole können Sie automatisierte Richtlinien konfigurieren, um den empfohlenen Aussteller, die Schlüsselstärke, das Protokoll und die Algorithmen gemäß den IT-Richtlinien der Organisation sicherzustellen. Auf diese Weise können Sie Zertifikate, die unbenutzt sind oder kurz vor dem Ablauf stehen, genau im Auge behalten.

Sie können ein SSL-Zertifikat und einen Schlüssel auf eine der folgenden Arten beziehen:

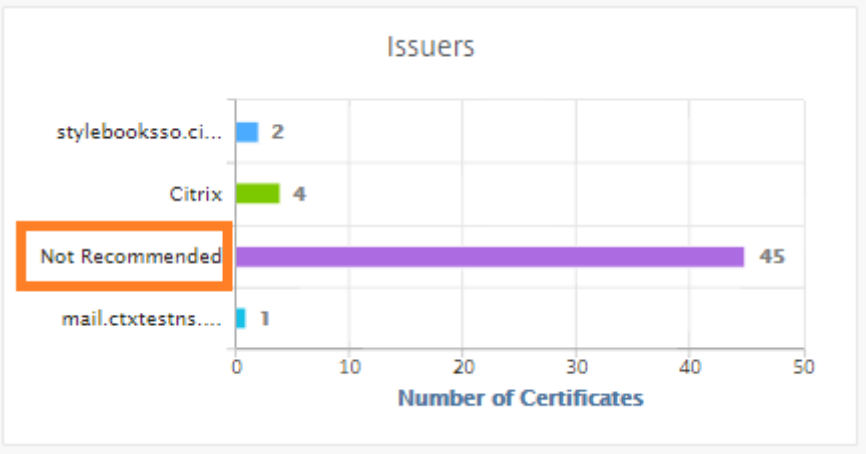
- Von einer autorisierten Zertifizierungsstelle (CA) wie Verisign
- Durch Generieren eines neuen SSL-Zertifikats und eines neuen Schlüssels auf der NetScaler-Appliance

SSL-Richtlinieneinstellungen für Unternehmen

Jedes Unternehmen hat seine eigene SSL-Richtlinie und definiert die Anforderungen, die alle SSL-Zertifikate einhalten müssen. Sicherheit war bei allen Unternehmensbenutzern immer zu den obersten Prioritäten und daher spielen SSL-Einstellungen eine wichtige Rolle.

Zum Beispiel schreibt eine ABC-Gesellschaft vor, dass alle Zertifikate mindestens wichtige Stärken von 2.048 Bit und mehr haben müssen. Die Zertifikate müssen von vertrauenswürdigen Zertifizierungsstellen oder Emittenten autorisiert werden. Administratoren müssen alle diese SSL-Parameter überprüfen, um sicherzustellen, dass die Zertifikate die Unternehmensrichtlinien einhalten. Es ist eine mühsame Aufgabe, jedes Zertifikat manuell zu überprüfen. Um dieses Szenario zu überwinden, hilft Ihnen das NetScaler ADM bei der Konfiguration von SSL-Richtlinieneinstellungen für Unternehmen und zeigt jedes Nicht-Compliance-Zertifikat mit dem Tag "Nicht empfohlen"an.

Sie können die Zusammenfassung der Non-Compliance-Zertifikate (nicht empfohlen) im SSL-Dashboard anzeigen.



> **Hinweis**
>
> Die "Nicht empfohlenen"Zertifikate werden basierend auf verschiedenen Parametern kategorisiert und Sie können sie in relevanten Komponenten anzeigen.

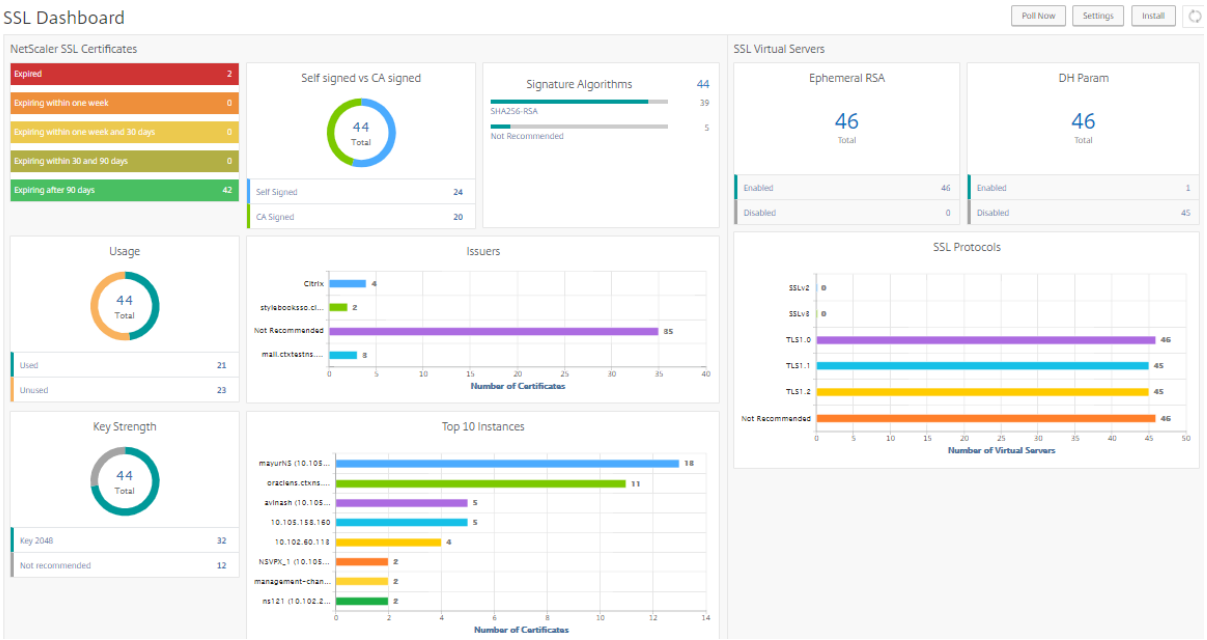
So funktioniert das NetScaler ADM-Zertifikat

SSL Dashboard bietet Ihnen eine visuelle Darstellung aller SSL-Zertifikate, die auf verschiedenen NetScaler-Instanzen installiert sind. Das SSL-Dashboard enthält die folgenden Informationen für jedes Zertifikat, das auf NetScaler-Instanzen installiert ist. Es ist auf der Grundlage der folgenden kategorisiert:

- **Selbstsigniert gegen CA signiert.** Der selbstsignierte und CA-signierte Bereich hilft Ihnen, die Zertifikate in selbstsignierte Zertifikate und CA-signierte Zertifikate zu unterteilen.
- **Signature-Algorithmen.** In diesem Abschnitt werden die SSL-Zertifikate basierend auf Signaturalgorithmen getrennt, die für die Verschlüsselung verwendet werden.
- **Verwendung.** In diesem Abschnitt werden Ihre SSL-Zertifikate basierend auf verwendeten und ungenutzten Zertifikaten getrennt. Unbenutzte Zertifikate erfordern besondere Aufmerk-

samkeit, da sie möglicherweise verpasst wurden, um an die virtuellen Server gebunden zu sein.

- **Emittenten.** In diesem Abschnitt trennt sich die SSL-Zertifikate basierend auf dem Aussteller der Zertifikate.
- **Wichtigste Stärke.** In diesem Abschnitt werden die SSL-Zertifikate basierend auf der Schlüsselstärke eines privaten Schlüssels getrennt.
- **Top-10-Instanz.** Dieser Abschnitt enthält die Details der 10 wichtigsten NetScaler-Instanzen basierend auf der Anzahl der installierten SSL-Zertifikate.



Anwendungsfälle für die Verwaltung von SSL-Zertifikaten

In den folgenden Anwendungsfällen wird beschrieben, wie Sie das SSL-Zertifikat verwenden können, um die Zertifikate über mehrere NetScaler-Instanzen hinweg zu verwalten und zu überwachen.

Installieren von SSL-Zertifikaten

Stellen Sie sich vor, Sie haben eine Flotte von NetScaler-Instanz, auf denen Sie die erforderlichen SSL-Zertifikate bereitstellen müssen. NetScaler ADM bietet Ihnen eine einheitliche Konsole, mit der Sie die SSL-Zertifikate in einem Versuch für mehrere NetScaler-Instanzen bereitstellen können.

Beispielsweise möchten Sie möglicherweise einige SSL-Zertifikate auf einer oder mehreren NetScaler-Instanzen installieren. Mit diesem Ansatz können Sie den manuellen Eingriff bei der Installation des SSL-Zertifikats auf jeder NetScaler-Instanz minimieren. Sie können eine Masseninstallation von SSL-Zertifikaten über eine oder mehrere NetScaler-Instanzen durchführen.

Um eine Zusammenfassung der SSL-Zertifikate zu erhalten, melden Sie sich bei **NetScaler ADM**an und navigieren Sie dann zu **Infrastruktur > SSL-Dashboard**.

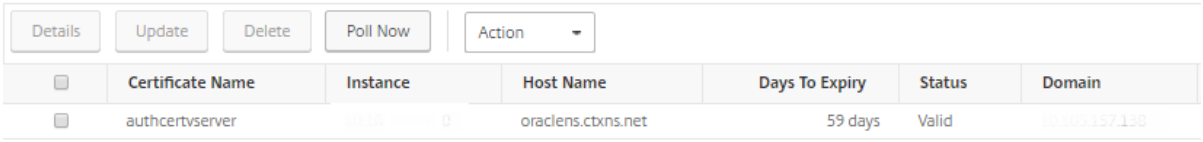
Benachrichtigungseinstellungen für Ablauf des Zertifikats

In diesem Anwendungsfall haben Sie möglicherweise viele Zertifikate für mehrere NetScaler-Instanzen, und es wird zu einem Overhead, um den Ablauf jedes Zertifikats zu verfolgen. Es ist eine mühsame Aufgabe, jedes Zertifikat manuell zu verfolgen und zu aktualisieren, bevor es abläuft. Um solche Szenarien zu vermeiden, können Sie NetScaler ADM so konfigurieren, dass die Benachrichtigungen oder Warnungen an die konfigurierten E-Mail-, Pager-, Slack- oder ServiceNow-Profile gesendet werden. Auf diese Weise können Sie sich über die Ablaufdaten der Zertifikate auf dem Laufenden halten und die Zertifikate lange vor den Ablaufdaten erneuern.

Beispielsweise vergessen Sie möglicherweise, das Zertifikat zu verfolgen, das kurz vor dem Ablauf steht. Und das Zertifikat läuft ab, was zu einem Dienstausfall führt, der sich auf zahlreiche Anwendungen für die Benutzer auswirken kann. Mit den Einstellungen für Benachrichtigungen über den Ablauf von ADM-Zertifikaten können Sie solche unvorhergesehenen Szenarien vermeiden.

Sie können die Zusammenfassung anzeigen und die Zertifikate, die kurz vor dem Ablauf stehen, auf dem **SSL-Dashboard**verfolgen.

Um den Bericht über abzulaufende Zertifikate in beliebiger Dauer anzuzeigen, können Sie auf die Kachel klicken, um die Details aller derartigen Zertifikate zu erhalten, die in diesem Fenster ablaufen.



Erneuerung von Zertifikaten

Sie können die Zertifikate jetzt von NetScaler ADM erneuern. Sie können entweder die vorhandenen Zertifikate erneuern oder die Zertifikate basierend auf den folgenden Kriterien erstellen:

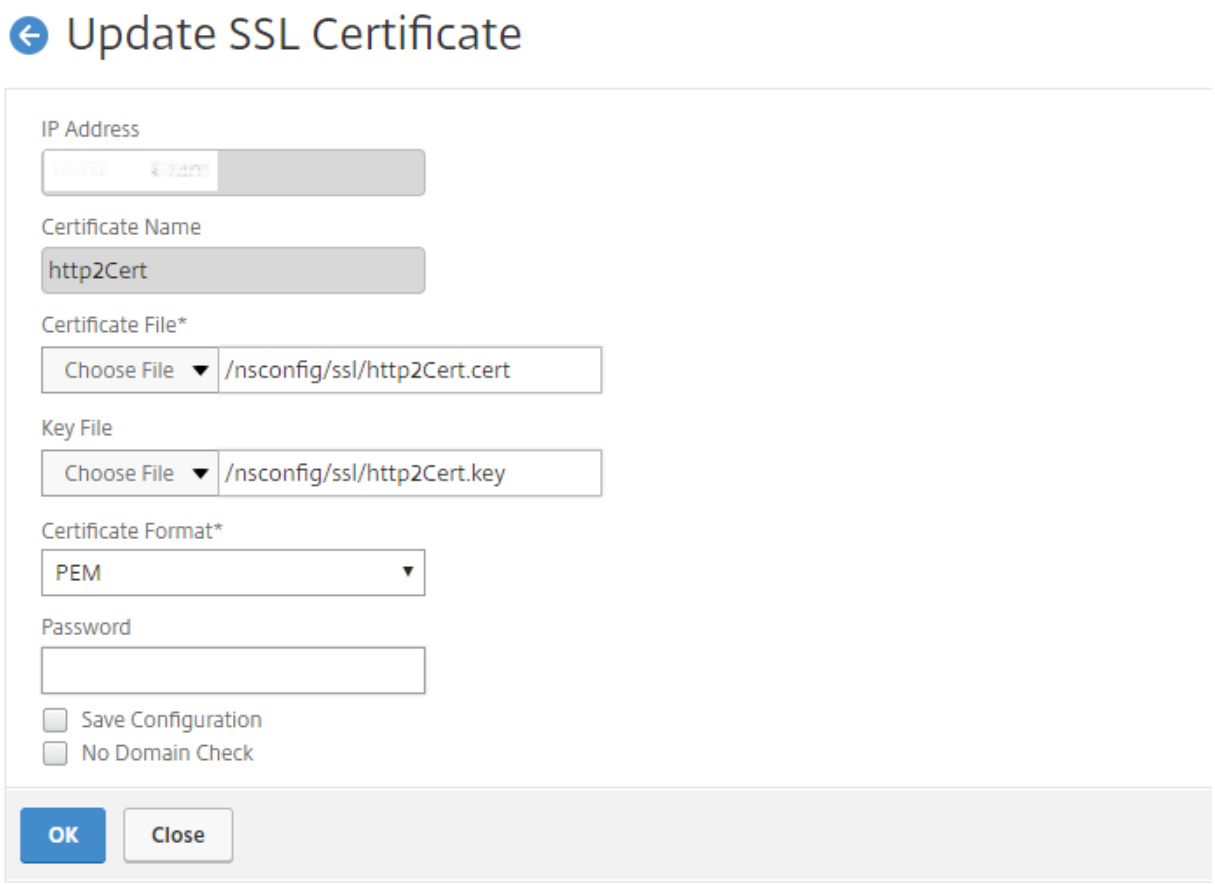
Aktualisieren Sie das vorhandene Zertifikat In diesem Anwendungsfall müssen Sie ein vorhandenes Zertifikat aktualisieren, sobald Sie ein erneuertes Zertifikat von der Zertifizierungsstelle (CA) erhalten haben. Sie können jetzt die vorhandenen Zertifikate von NetScaler ADM aktualisieren, ohne sich bei NetScaler-Instanzen anzumelden.

Beispielsweise kann es einige Änderungen oder Änderungen an den vorhandenen Zertifikaten geben. Die CA stellt erneuerte Zertifikate aus. Anstatt zur NetScaler Appliance zu gehen, können Sie jetzt das SSL-Zertifikat von NetScaler ADM aktualisieren.

Um ein Zertifikat zu aktualisieren, melden Sie sich bei NetScaler ADM an und navigieren Sie dann zu **Infrastruktur > SSL-Dashboard**.

Wählen Sie das Zertifikat aus, das Sie aktualisieren möchten, und klicken Sie auf **Aktualisieren**.

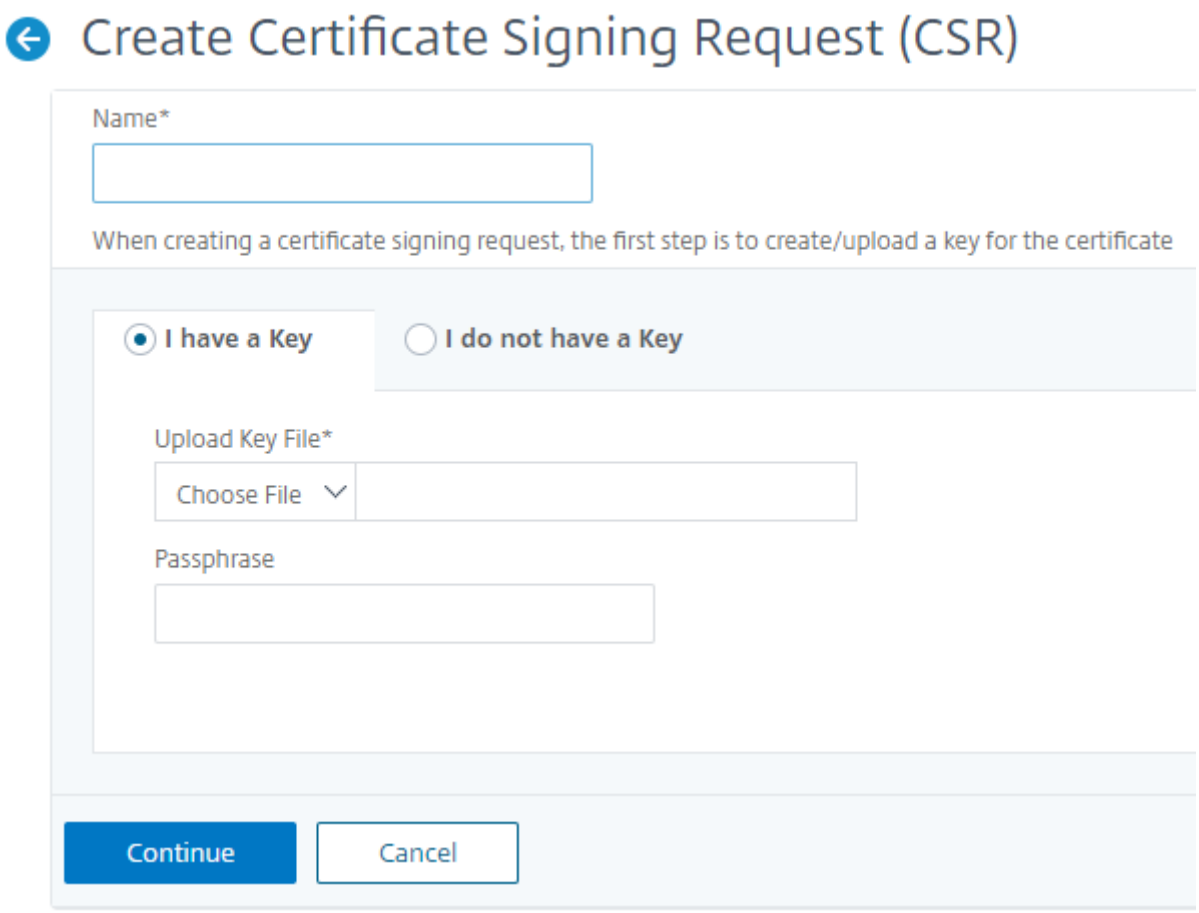
Sie haben die Möglichkeit, die relevanten Felder des ausgewählten Zertifikats von NetScaler ADM zu aktualisieren.



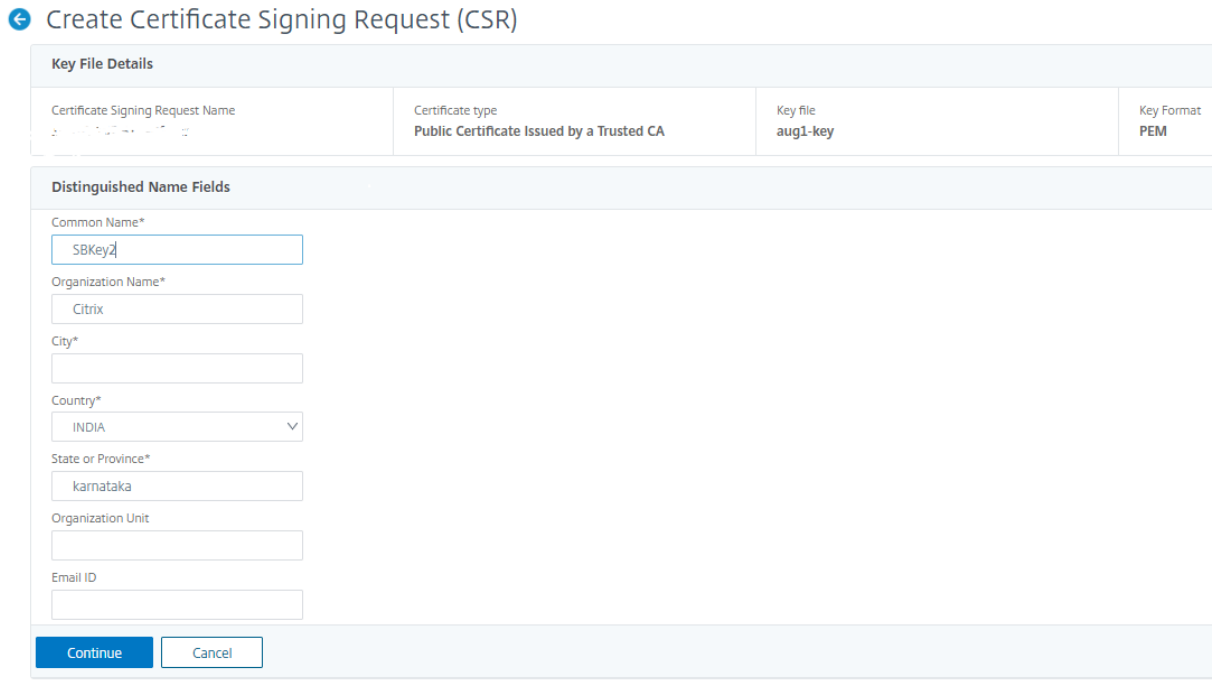
Erstellen einer Zertifikatsignieranforderung Stellen Sie sich einen Anwendungsfall vor, in dem eines der SSL-Zertifikate nicht den Richtlinien der Organisation entspricht. Sie möchten ein neues Zertifikat von der Zertifizierungsstelle erhalten. Sie können jetzt eine Zertifikatsignieranforderung (CSR) von NetScaler ADM generieren. Ein CSR und ein öffentlicher Schlüssel können an eine CA gesendet werden, um das SSL-Zertifikat zu erhalten.

Um CSR zu bestimmen und zu erstellen, wählen Sie das gewünschte Zertifikat aus und klicken Sie auf **CSR erstellen**.

Sie müssen ein öffentliches oder privates Schlüsselwertpaar haben. Um einen Schlüssel hochzuladen, klicken Sie auf **Datei auswählen** und wählen Sie aus der Liste aus. Um einen Schlüssel zu erstellen, wählen Sie **Ich habe keine Schlüsseloption** und geben Sie die relevanten Parameter an.

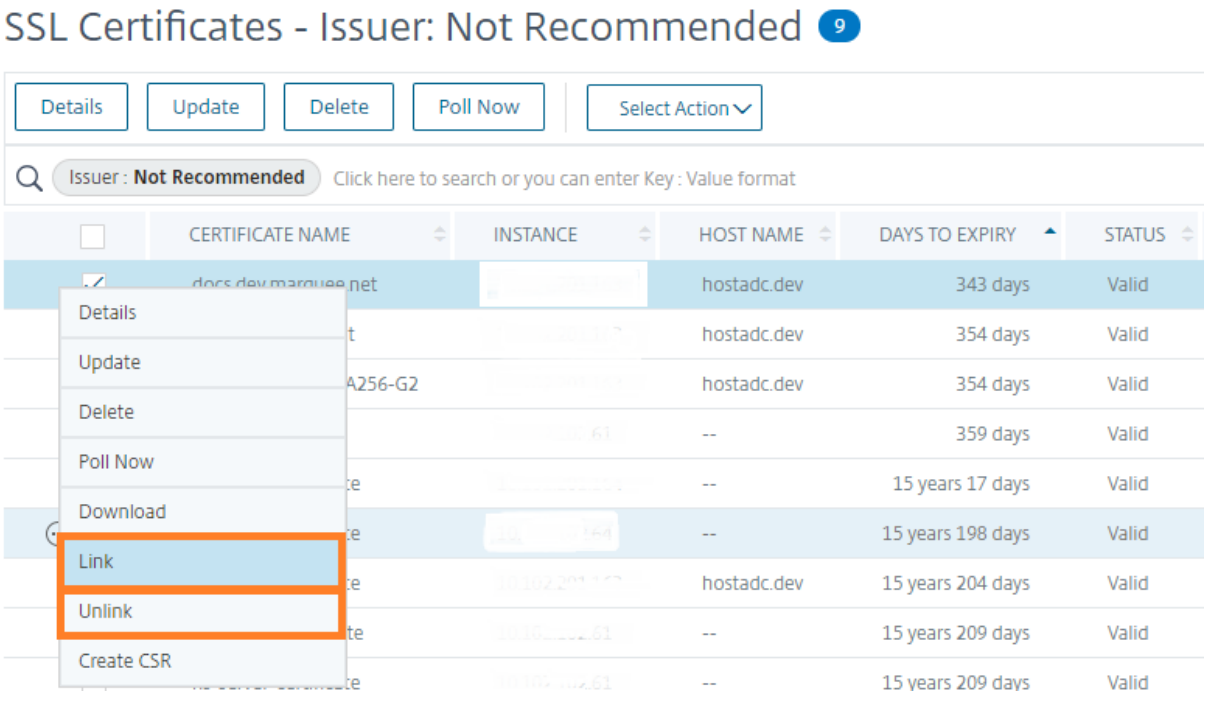


Um weitere Details zum ausgewählten Schlüssel wie Common Name, Org Name, Stadt, Land, Bundesland, Org Unit und E-Mail-ID anzugeben, um die CSR zu erstellen.



SSL-Zertifikate verknüpfen und aufheben

Sie können mehrere SSL-Zertifikate aneinander binden, um ein Zertifikatspaket zu erstellen. Um ein Zertifikat mit einem anderen Zertifikat zu verknüpfen, muss der Aussteller des ersten Zertifikats mit der Domäne des zweiten Zertifikats übereinstimmen.

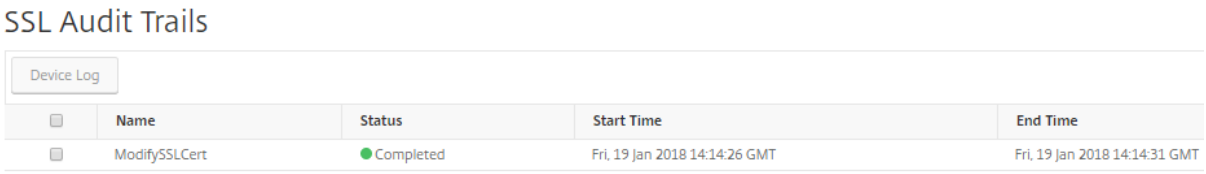


Auditprotokolle

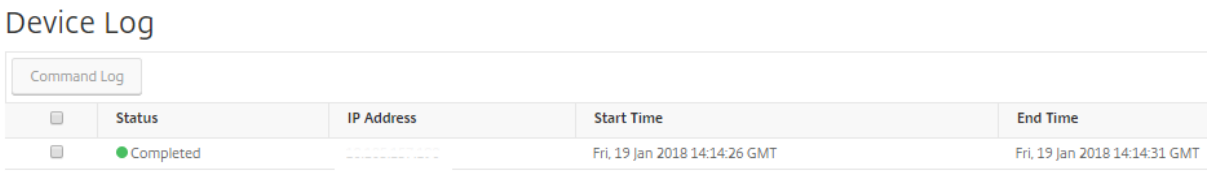
Audit Logs ist eine Sammlung von Textprotokolldateien, die vom NetScaler ADM generiert werden. Es zeigt eine Historie von SSL-Zertifikaten, die mithilfe von NetScaler ADM für die spezifische NetScaler Appliance hinzugefügt, geändert und geändert werden. Die Überwachungsprotokolle zeigen auch die IP-Adresse der NetScaler Appliance, den Status, die Startzeit und die Endzeit des jeweiligen Vorgangs an.

In diesem Beispiel möchten Sie möglicherweise die Änderung überprüfen, die über einen Zeitraum für das jeweilige Zertifikat stattgefunden hat. Und Sie haben die Möglichkeit, den Verlauf der Änderungen am Zertifikat über das Geräteprotokoll und das Befehlsprotokoll anzuzeigen.

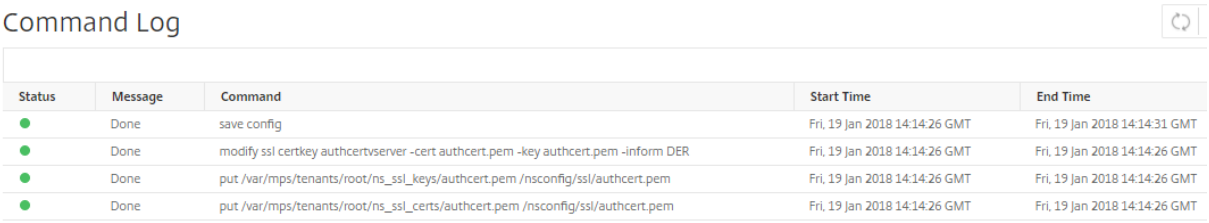
Um die Informationen von SSL-Zertifikaten zu ermitteln, klicken Sie im **SSL-Dashboard**auf **Audit Log**. Die Anwendungsübersicht enthält den Status der SSL-Zertifikate mit Startzeit und Endzeit.



Um die Informationen der NetScaler Appliance eines bestimmten SSL-Zertifikats zu ermitteln, aktivieren Sie das entsprechende Kontrollkästchen Ihres Wunschzertifikats. Klicken Sie auf **Geräte-Log**



Um die Informationen des Befehlstyps und der Meldung anzuzeigen, klicken Sie auf **Befehlsprotokoll**.



Verwenden des SSL-Dashboards

February 5, 2024

Sie können das SSL-Zertifikat-Dashboard in NetScaler Application Delivery Management (ADM) verwenden, um Diagramme anzuzeigen, anhand derer Sie die Zertifikatsaussteller, die wichtigsten Stärken und Signaturalgorithmen verfolgen können. Das SSL-Zertifikat-Dashboard zeigt außerdem Diagramme an, die Folgendes angeben:

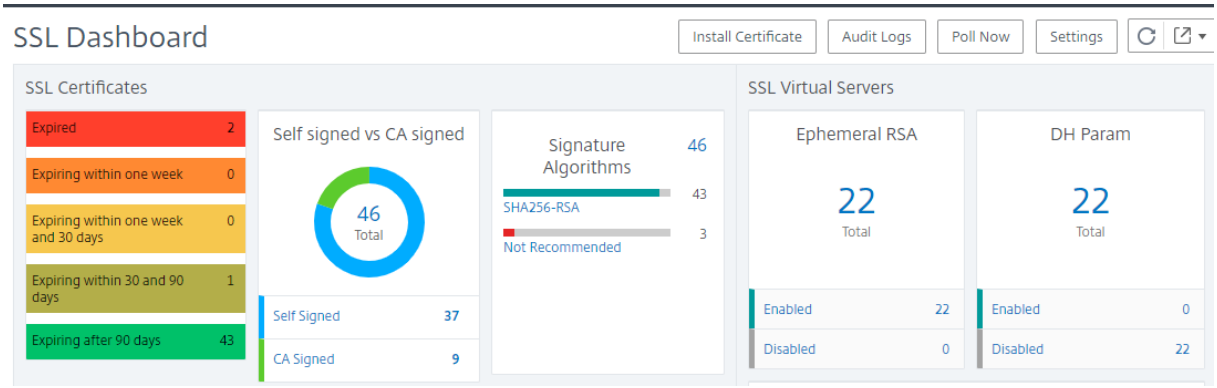
- Anzahl der Tage, nach denen Zertifikate ablaufen
- Anzahl verwendeter und nicht verwendeter Zertifikate
- Anzahl selbstsignierter und von einer Zertifizierungsstelle signierter Zertifikate
- Anzahl der Emittenten
- Signatur-Algorithmen
- SSL-Protokolle
- Top 10 Instanzen nach Anzahl der verwendeten Zertifikate

So überwachen Sie SSL-Zertifikate

Sie können das SSL-Dashboard auf NetScaler ADM verwenden, um Ihre Zertifikate zu überwachen, wenn Ihr Unternehmen über eine SSL-Richtlinie verfügt, in der Sie bestimmte SSL-Zertifikatsanforderungen definiert haben, z. B. müssen alle Zertifikate eine Mindestschlüsselstärke von 2048 Bit haben und eine vertrauenswürdige Zertifizierungsstelle muss sie autorisieren.

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 Zertifikatnamen, die Instanz, auf der es verwendet wird, seine Gültigkeit, seinen Signaturalgorithmus usw. anzuzeigen.

Um SSL-Zertifikate in NetScaler ADM zu überwachen, navigieren Sie zu **Infrastruktur > SSL-Dashboard**.



Mit NetScaler ADM können Sie SSL-Zertifikate abfragen und alle SSL-Zertifikate der Instanzen sofort NetScaler ADM hinzufügen. Um dies zu tun,

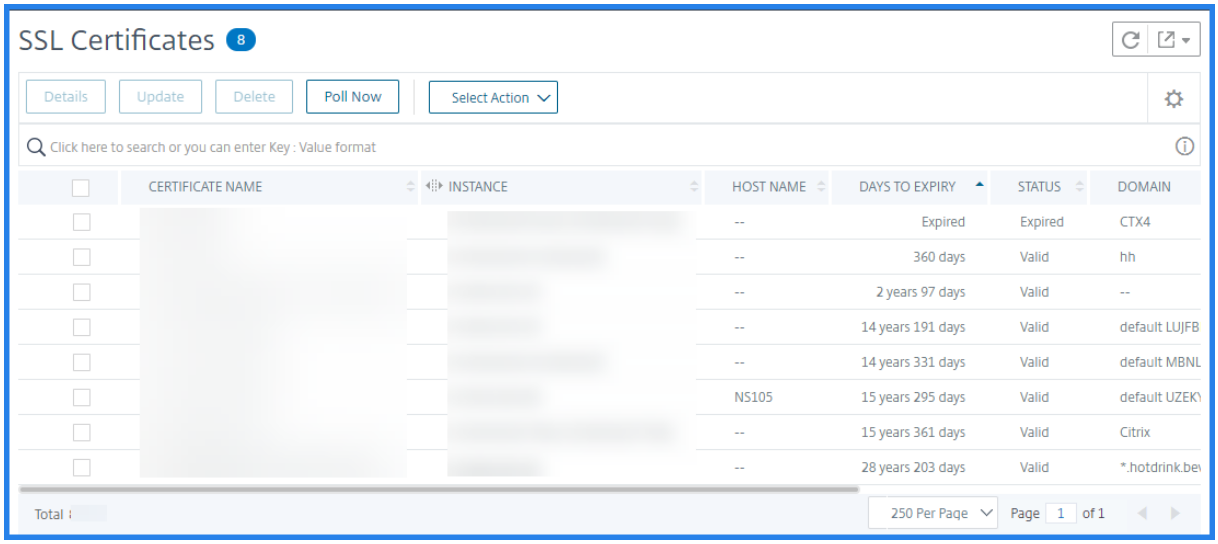
1. Navigieren Sie zu **Infrastruktur > SSL-Dashboard**.
2. Klicken Sie auf **Jetzt abfragen**.

   Auf der Seite **Jetzt abfragen** können Sie entweder alle verwalteten ADC-Instances abfragen oder bestimmte Instances auswählen.
3. Klicken Sie auf **Abruf starten**.

Im **SSL-Dashboard**können Sie die ADC-SSL-Zertifikate, virtuellen SSL-Server und SSL-Protokolle überwachen.

Sie können auf die Metriken im Dashboard klicken, um Details zu SSL-Zertifikaten, virtuellen SSL-Servern oder SSL-Protokollen anzuzeigen.

Wenn Sie beispielsweise auf die Nummer unter **Self signed vs CA signed** auf dem Dashboard klicken, zeigt die ADM-GUI alle SSL-Zertifikate auf den NetScaler Instanzen an.



Das NetScaler ADM SSL-Dashboard zeigt auch die Verteilung der SSL-Protokolle an, die auf Ihren virtuellen Servern ausgeführt werden. Als Administrator können Sie die Protokolle, die Sie überwachen möchten, über die SSL-Richtlinie angeben. Weitere Informationen finden Sie unter Konfigurieren von SSL-Richtlinien. Die unterstützten Protokolle sind SSLv2, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 und TLS 1.3. Die auf virtuellen Servern verwendeten SSL-Protokolle werden in einem Balkendiagrammformat angezeigt. Durch Klicken auf ein bestimmtes Protokoll wird eine Liste der virtuellen Server angezeigt, die dieses Protokoll verwenden.

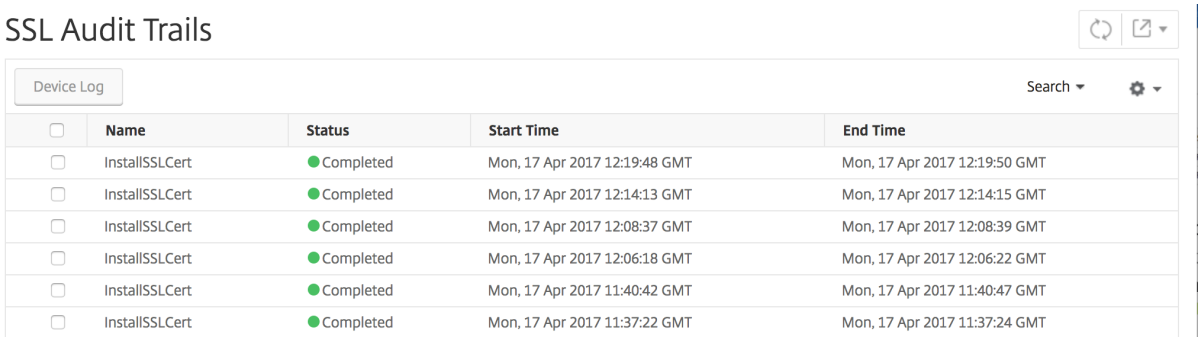
Ein Ringdiagramm wird angezeigt, nachdem Diffie-Hellman (DH) - oder Ephemeral RSA-Schlüssel im SSL-Dashboard aktiviert oder deaktiviert wurden. Diese Schlüssel ermöglichen eine sichere Kommunikation mit Exportclients, auch wenn das Serverzertifikat keine Exportclients unterstützt, wie im Fall

eines 1024-Bit-Zertifikats. Wenn Sie auf das entsprechende Diagramm klicken, wird eine Liste der virtuellen Server angezeigt, auf denen DH- oder Ephemere RSA-Schlüssel aktiviert sind.

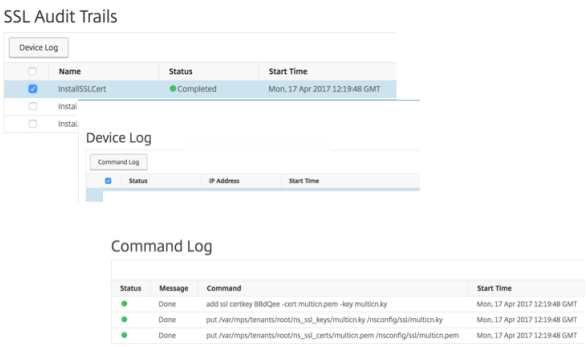
So zeigen Sie Audit-Trails für SSL-Zertifikate an

Sie können jetzt Protokolldetails von SSL-Zertifikaten auf NetScaler ADM anzeigen. In den Protokolldetails werden Vorgänge angezeigt, die mit SSL-Zertifikaten auf NetScaler ADM ausgeführt wurden, z. B.: Installieren von SSL-Zertifikaten, Verknüpfen und Aufheben der Verknüpfung von SSL-Zertifikaten, Aktualisieren von SSL-Zertifikaten und Löschen von SSL- Audit-Pfadinformationen sind nützlich, während SSL-Zertifikatänderungen in einer Anwendung mit mehreren Eigentümern überwacht werden.

Um ein Überwachungsprotokoll für einen bestimmten Vorgang anzuzeigen, der mit NetScaler ADM mithilfe von SSL-Zertifikaten ausgeführt wird, navigieren Sie zu **Infrastruktur > SSL-Dashboard** > und klicken Sie auf **Überwach**



Für einen bestimmten Vorgang, der mit 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.



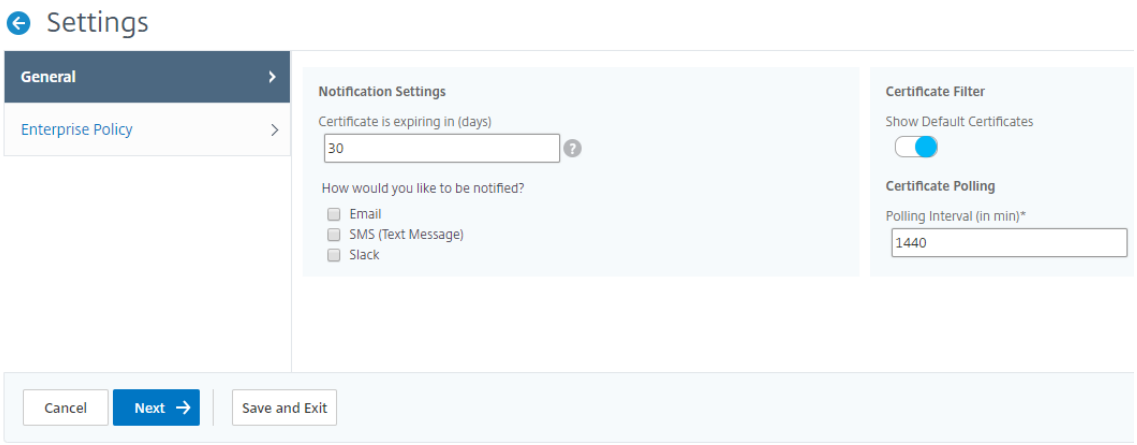
So schließen Sie standardmäßige NetScaler Zertifikate im SSL-Dashboard aus

Mit NetScaler ADM können Sie NetScaler-Standardzertifikate, die in den SSL-Dashboard-Diagrammen angezeigt werden, je nach Ihren Einstellungen ein- oder ausblenden. Standardmäßig werden alle Zer-

tifikate im SSL-Dashboard angezeigt, einschließlich Standardzertifikaten.

So blenden Sie Standardzertifikate auf dem SSL-Dashboard ein oder aus:

1. Navigieren Sie in der NetScaler ADM-GUI zu **Infrastruktur > SSL-Dashboard** .
2. Klicken Sie auf der Seite **SSL-Dashboard** auf **Einstellungen**.
3. Wählen Sie auf der Seite **Einstellungen** die Option **Allgemein** aus.
4. Geben Sie die Anzahl der Tage ein, an denen das Zertifikat abläuft, um eine Benachrichtigung über den Ablauf des Zertifikats zu erhalten.
5. Wählen Sie die Benachrichtigungsmethode und erstellen Sie die entsprechenden Profile.
6. Deaktivieren Sie im Abschnitt **Zertifikatsfilter** das Kontrollkästchen **Standardzertifikate anzeigen** und klicken Sie auf **Speichern und beenden**.



Anzeigen, Hochladen und Herunterladen von SSL-Dateien

Um SSL-Dateien auf NetScaler ADM anzuzeigen, navigieren Sie **auf NetScaler ADM zu Infrastruktur > SSL Dashboard > SSL-Dateien**.

Sie können die folgenden Dateien auf NetScaler ADM anzeigen, hochladen und herunterladen:

- SSL-Zertifikate
- SSL-Schlüssel
- SSL-CSRs

Um SSL-Dateien auf einer NetScaler-Instanz anzuzeigen und herunterzuladen, navigieren Sie zu **Infrastruktur > SSL Dashboard > SSL-Dateien auf NetScaler**.

Sie können erst auf die SSL-Dateien zugreifen, nachdem die NetScaler-Instanzen entweder manuell oder über einen geplanten Sicherungsvorgang gesichert wurden.

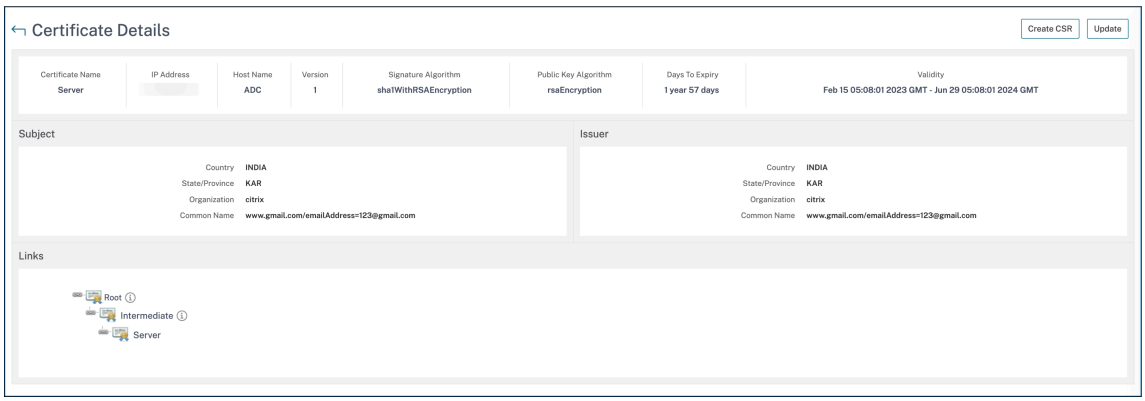
> **Wichtig:**
>
> Um den Download von SSL-Dateien von ADC-Instanzen zu aktivieren, aktivieren Sie die **Instanz-SSL-Zertifikatfunktion**. Weitere Informationen finden Sie unter ADM-Funktionen aktivieren oder deaktivieren.

SSL-Zertifikatskette anzeigen

Sie können die gesamte Zertifikatskette von den Zwischenzertifikaten bis zum Root-CA-Zertifikat anzeigen.

So sehen Sie sich eine Zertifikatskette an:

1. Navigieren Sie zu **Infrastruktur > SSL-Dashboard** und klicken Sie auf die SSL-Zertifikate in einer beliebigen Kachel.
2. Wählen Sie auf der Seite **SSL-Zertifikate** ein Zertifikat aus und klicken Sie auf **Details**. Die Zertifikatskette wird unter **Links** angezeigt.



Benachrichtigungen für das Ablaufdatum des SSL-Zertifikats einrichten

February 5, 2024

Als Sicherheitsadministrator können Sie Benachrichtigungen einrichten, die Sie informieren, wenn Zertifikate bald ablaufen, und Informationen darüber enthalten, welche Citrix Application Delivery Controller (ADC) -Instanzen diese Zertifikate verwenden. Durch die Aktivierung von Benachrichtigungen können Sie Ihre SSL-Zertifikate rechtzeitig erneuern.

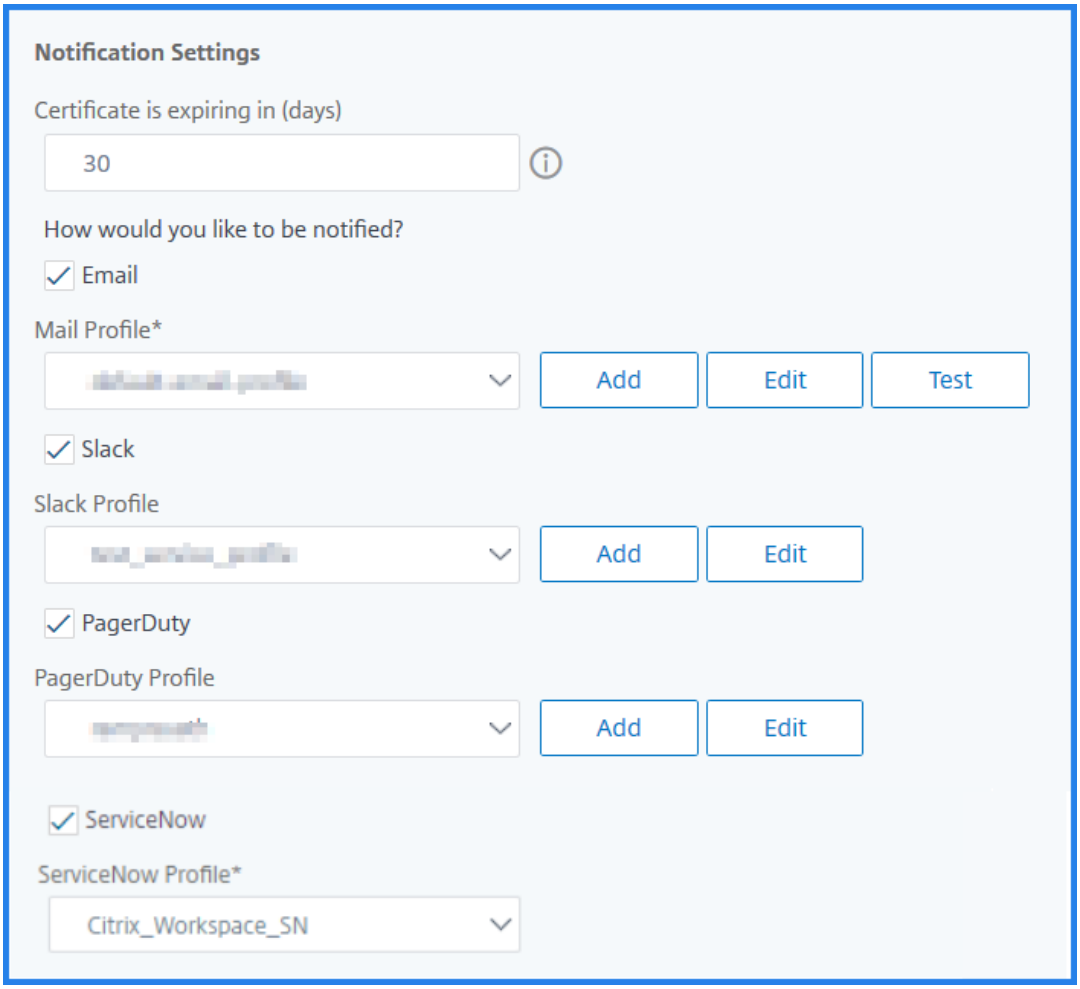
Sie können beispielsweise festlegen, dass eine E-Mail-Benachrichtigung 30 Tage vor Ablauf Ihres Zertifikats an eine E-Mail-Verteilerliste gesendet wird.

So richten Sie Benachrichtigungen von NetScaler ADM ein:

1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zu **Infrastruktur**SSL-Dashboard.
2. Klicken Sie auf der Seite **SSL-Dashboard** auf **Einstellungen**.
3. Klicken Sie auf der Seite **SSL-Einstellungen** auf das Symbol **Bearbeiten**.
4. Geben Sie im Abschnitt **Benachrichtigungseinstellungen** an, wann Sie die Benachrichtigung versenden möchten, und geben Sie die Anzahl der Tage vor dem Ablaufdatum an.
5. Wählen Sie die Art der Benachrichtigung, die Sie senden möchten. Wählen Sie den Benachrichtigungstyp und die Verteilerliste aus dem Drop-down-Menü aus. Die Benachrichtigungstypen sind wie folgt:

   - **E-Mail**—Geben Sie einen Mailserver und Profildetails an. Eine E-Mail wird ausgelöst, wenn Ihre Zertifikate bald ablaufen.
   - **SMS** —Geben Sie einen SMS-Server (Short Message Service) und Profildetails an. Eine SMS-Nachricht wird ausgelöst, wenn Ihre Zertifikate bald ablaufen.
   - **Slack** - Geben Sie die Details des Slack Profils an.
   - **PagerDuty-Warnungen** - Geben Sie ein PagerDuty-Profil an Basierend auf den in Ihrem PagerDuty-Portal konfigurierten Benachrichtigungseinstellungen wird eine Benachrichtigung gesendet, wenn Ihre Zertifikate bald ablaufen.
   - **ServiceNow** - Eine Benachrichtigung wird an das standardmäßige ServiceNow-Profil gesendet, wenn Ihre Zertifikate bald ablaufen.

     > **Wichtig**
     >
     > Stellen Sie sicher, dass der Citrix Cloud ITSM-Adapter für ServiceNow konfiguriert und in NetScaler ADM integriert ist. Weitere Informationen finden Sie unter Integrieren von NetScaler ADM mit ServiceNow-Instanz.



6. Klicken Sie auf **Speichern und Beenden**.

NetScaler ADM sendet nun SSL-Zertifikatablauftrap an den externen Trap-Zielserver, wenn Ihre SSL-Zertifikate abgelaufen sind. NetScaler ADM sendet einen Trap, wenn die folgenden beiden Bedingungen erfüllt sind:

- Sie haben die Anzahl der Tage, an denen das Zertifikat abläuft, auf der Seite mit den SSL-Dashboard-Einstellungen konfiguriert.
- Sie haben das Trap-Ziel hinzugefügt.

Sie können Trap-Ziele festlegen, indem Sie zu **Einstellungen > SNMP > Trap-Ziele**navigieren. Geben Sie die IP-Adresse des Ziel-SNMP-Servers ein, an den die Traps gesendet werden. Geben Sie die Portnummer ein und geben Sie „public“(ohne Anführungszeichen) als Community-Zeichenfolge ein.

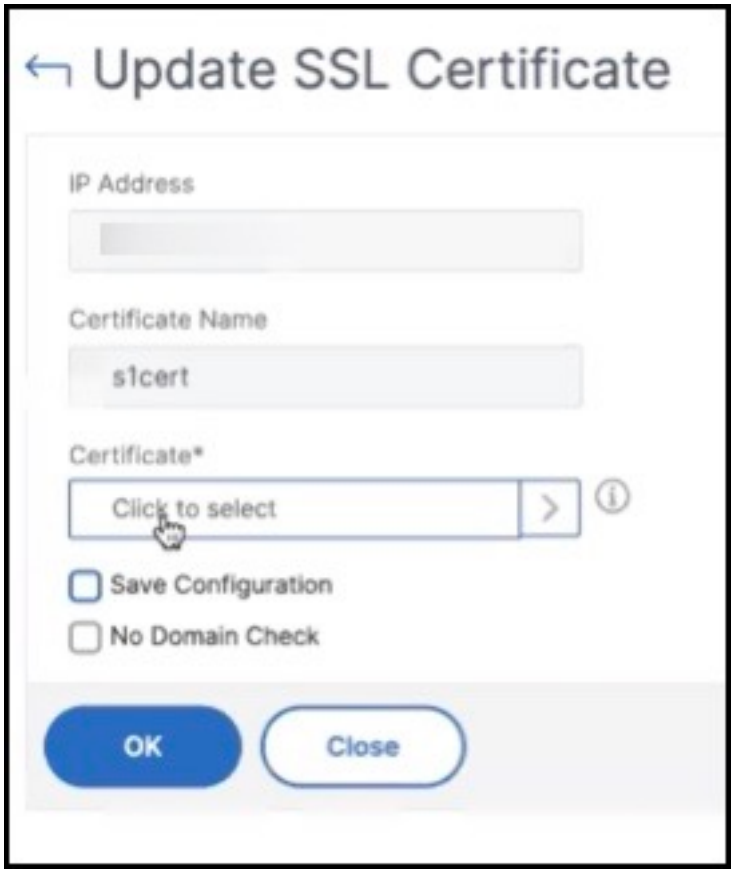
Installiertes Zertifikat aktualisieren

February 5, 2024

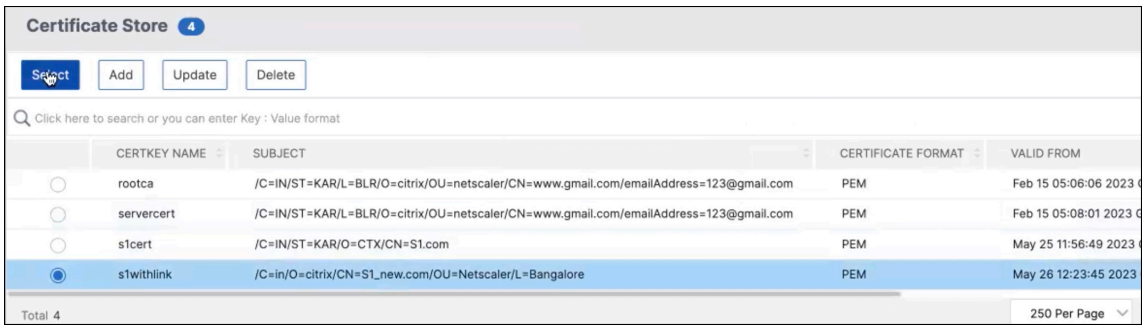
Nachdem Sie ein erneuertes Zertifikat von der Zertifizierungsstelle (CA) erhalten haben, müssen Sie sich nicht bei einzelnen NetScaler-Instanzen anmelden, um die Zertifikate zu aktualisieren. Sie können die vorhandenen Zertifikate in NetScaler ADM mit Zertifikaten aus dem Zertifikatsspeicher aktualisieren.

So aktualisieren Sie ein SSL-Zertifikat von NetScaler ADM:

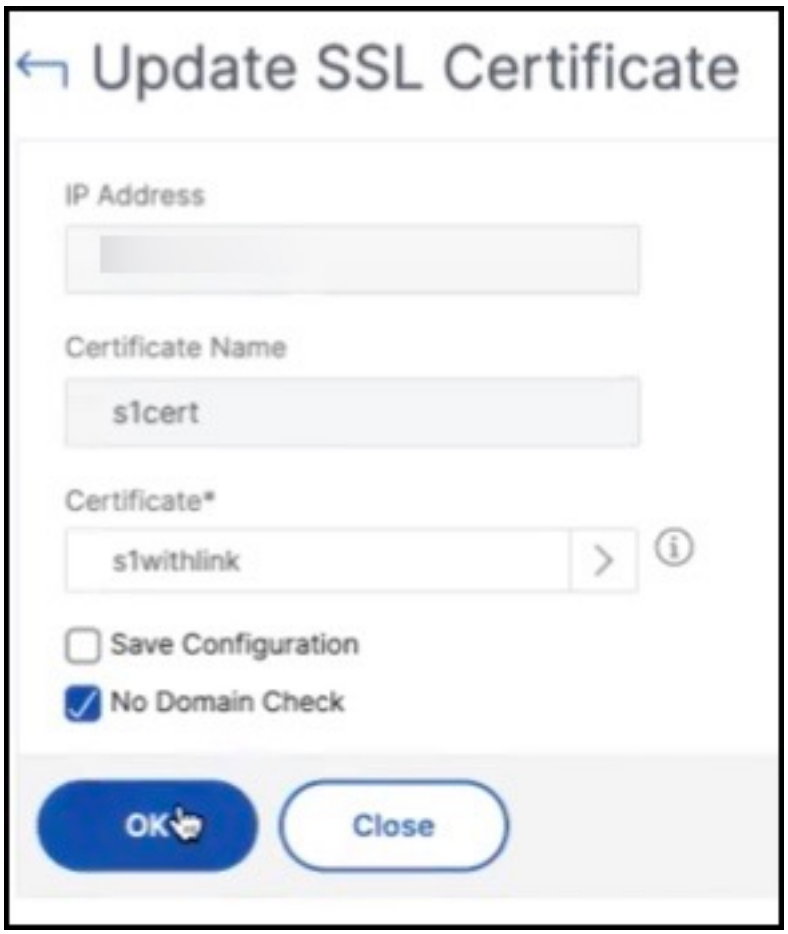
1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > SSL Dashboard**.
2. Klicken Sie auf eine der Diagramme, um die Liste der SSL-Zertifikate anzuzeigen.
3. Wählen Sie auf der Seite **SSL-Zertifikate** ein Zertifikat aus und klicken Sie auf **Aktualisieren**. Alternativ klicken Sie auf das SSL-Zertifikat, um die Details anzuzeigen, und klicken Sie dann oben rechts auf der Seite **SSL-Zertifikat** auf **Aktualisieren**.
4. Wählen Sie auf der Seite **SSL-Zertifikat aktualisieren** die Option **Zertifikat** aus, um die Seite „ **Zertifikatsspeicher** “anzuzeigen.



5. Wählen Sie auf der Seite „ **Zertifikatsspeicher** “die Zertifikatsdatei aus, die Sie hinzufügen möchten. Klicken Sie auf **Select**.



6. Wenn der Domainname des neuen Zertifikats nicht mit dem alten Zertifikat übereinstimmt, wählen Sie **No Domain Check**, wenn der Server die neue Domain hosten soll.



Klicken Sie auf **OK**. Alle virtuellen SSL-Server, an die dieses Zertifikat gebunden ist, werden automatisch aktualisiert.

> **Hinweis:**
>
> Wenn Sie ein vorhandenes SSL-Zertifikat mit einer Zertifikatskette aus dem Zertifikatsspe-

> icher aktualisieren, wird das vorhandene Zertifikat mit den verknüpften Zertifikaten aktualisiert. Wählen Sie das Zertifikat aus und klicken Sie auf **Details**, um die Zertifikatskette anzuzeigen.

SSL-Zertifikate auf einer NetScaler-Instanz installieren

February 5, 2024

Stellen Sie vor der Installation von SSL-Zertifikaten auf Citrix Application Delivery Controller (ADC) -Instanzen sicher, dass die Zertifikate von vertrauenswürdigen Zertifizierungsstellen ausgestellt wurden. Stellen Sie außerdem sicher, dass die Schlüsselstärke der Zertifikatschlüssel 2048 Bit oder höher beträgt und dass die Schlüssel mit sicheren Signaturalgorithmen signiert sind.

So installieren Sie ein SSL-Zertifikat von einer anderen NetScaler-Instanz:

Sie können auch ein Zertifikat von einer ausgewählten NetScaler-Instance importieren und es über die NetScaler Application Delivery Management (ADM) GUI auf andere zielgerichtete NetScaler-Instances anwenden.

1. Navigieren Sie zu **Infrastruktur > SSL-Dashboard**.
2. Klicken Sie in der rechten oberen Ecke des SSL-Dashboards auf **Installieren**.
3. Geben Sie auf der Seite „ **SSL-Zertifikat auf NetScaler-Instances installieren**“die folgenden Parameter an:

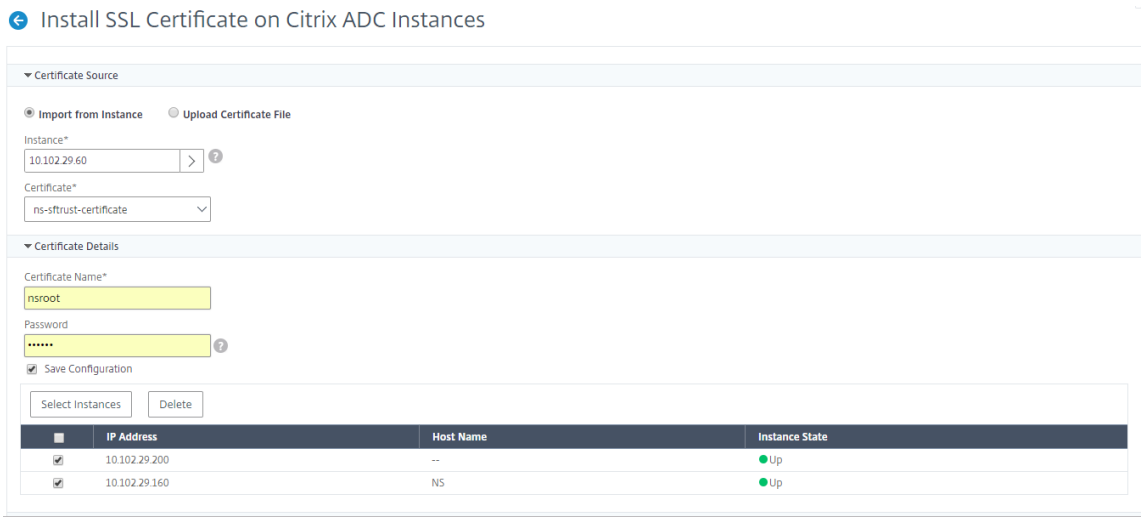
    a) Zertifikatquelle
    Wählen Sie die Option aus der **Instanz importieren aus**.

    - Wählen Sie die **Instanz** aus, aus der Sie das Zertifikat importieren möchten.
    - Wählen Sie das **Zertifikat** aus der Liste aller SSL-Zertifikatsdateien auf der Instanz aus.

    b) Zertifikatdetails

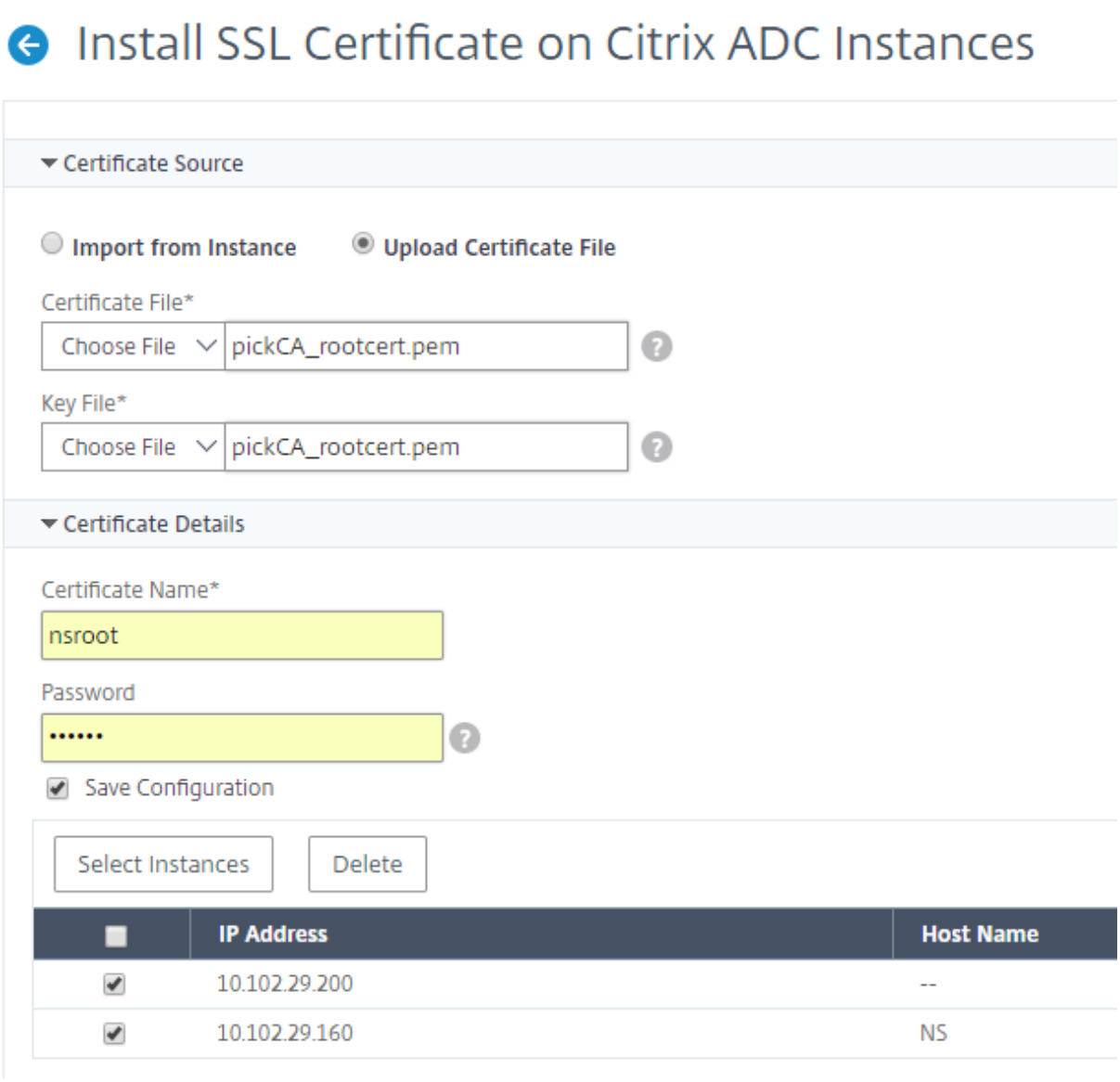
    - **Name des Zertifikats**. Geben Sie einen Namen für den Zertifikatsschlüssel an.
    - **Kennwort**. Kennwort zum Verschlüsseln des privaten Schlüssels. Sie können diese Option verwenden, um verschlüsselte private Schlüssel hochzuladen.

4. Klicken Sie auf **Instanzen auswählen**, um die NetScaler-Instanzen auszuwählen, auf denen Sie Ihre Zertifikate installieren möchten.
5. Klicken Sie auf **OK**.



So installieren Sie ein SSL-Zertifikat von NetScaler ADM:

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > SSL Dashboard**.
2. Klicken Sie in der rechten oberen Ecke des Dashboards auf **Installieren**.
3. Wählen Sie auf der Seite **SSL-Zertifikat auf NetScaler Instanz installieren** die Option **Zertifikatdatei hochladen** aus, und geben Sie 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 NetScaler ADM-Instanz vorhanden sein).
   - **Schlüsseldatei** - Laden Sie die Schlüsseldatei hoch.
   - **Zertifikatsname** —Geben Sie einen Namen für den Zertifikatsschlüssel an.
   - **Kennwort** —Kennwort zum Verschlüsseln des privaten Schlüssels. Sie können diese Option verwenden, um verschlüsselte private Schlüssel hochzuladen.
   - **Instanzen auswählen** —Wählen Sie die NetScaler ADM-Instances aus, auf denen Sie Ihre Zertifikate installieren möchten.
4. Um die Konfiguration für die spätere Verwendung zu **speichern, aktivieren Sie das Kontrollkästchen Konfiguration speichern** .
5. Klicken Sie auf **OK**.



Zertifikatsignieranforderung (CSR) erstellen

February 5, 2024

Eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) ist ein Block mit verschlüsseltem Text, der auf dem Server generiert wird, auf dem das Zertifikat verwendet wird. Es enthält Informationen, die in das Zertifikat aufgenommen werden, wie z. B. den Namen Ihrer Organisation, den allgemeinen Namen (Domainname), den Ort und das Land.

So erstellen Sie eine CSR mit NetScaler ADM:

1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zu **Infrastruktur**SSL-

Dashboard.

2. Klicken Sie auf eines der Diagramme, um die Liste der installierten SSL-Zertifikate anzuzeigen. 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:

   - **Schlüssel hochladen** —Wählen Sie die Option **Ich habe einen Schlüssel** aus. Um Ihre Schlüsseldatei hochzuladen, wählen Sie entweder **Lokal** (Ihr lokaler Computer) oder **Appliance** (die Schlüsseldatei muss in der virtuellen NetScaler ADM-Instanz vorhanden sein).
   - **Schlüssel erstellen** —Wählen Sie die Option Ich habe keinen Schlüssel aus, und geben Sie dann die folgenden Parameter an:

Verschlüsselungsalgorithmus	Art des Schlüssels. Zum Beispiel RSA.
Name der Schlüsseldatei	Name für Ihre Datei, in der der RSA-Schlüssel gespeichert ist.
Größe des Schlüssels	Schlüsselgröße in Bit.
Öffentlicher Exponentenwert	Wählen Sie entweder **3** oder **F4** aus der bereitgestellten Dropdown-Liste aus. Dieser Wert ist Teil des Verschlüsselungsalgorithmus, der zum Erstellen Ihres RSA-Schlüssels erforderlich ist.
Schlüssel-Format	Standardmäßig ist PEM 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 auswählen, müssen Sie eine PEM-Passphrase angeben.
PEM-Passphrase	Wenn Sie den PEM-Kodierungsalgorithmus ausgewählt haben, geben Sie eine Passphrase ein.
PEM-Passphrase bestätigen	Bestätigen Sie Ihre PEM-Passphrase.

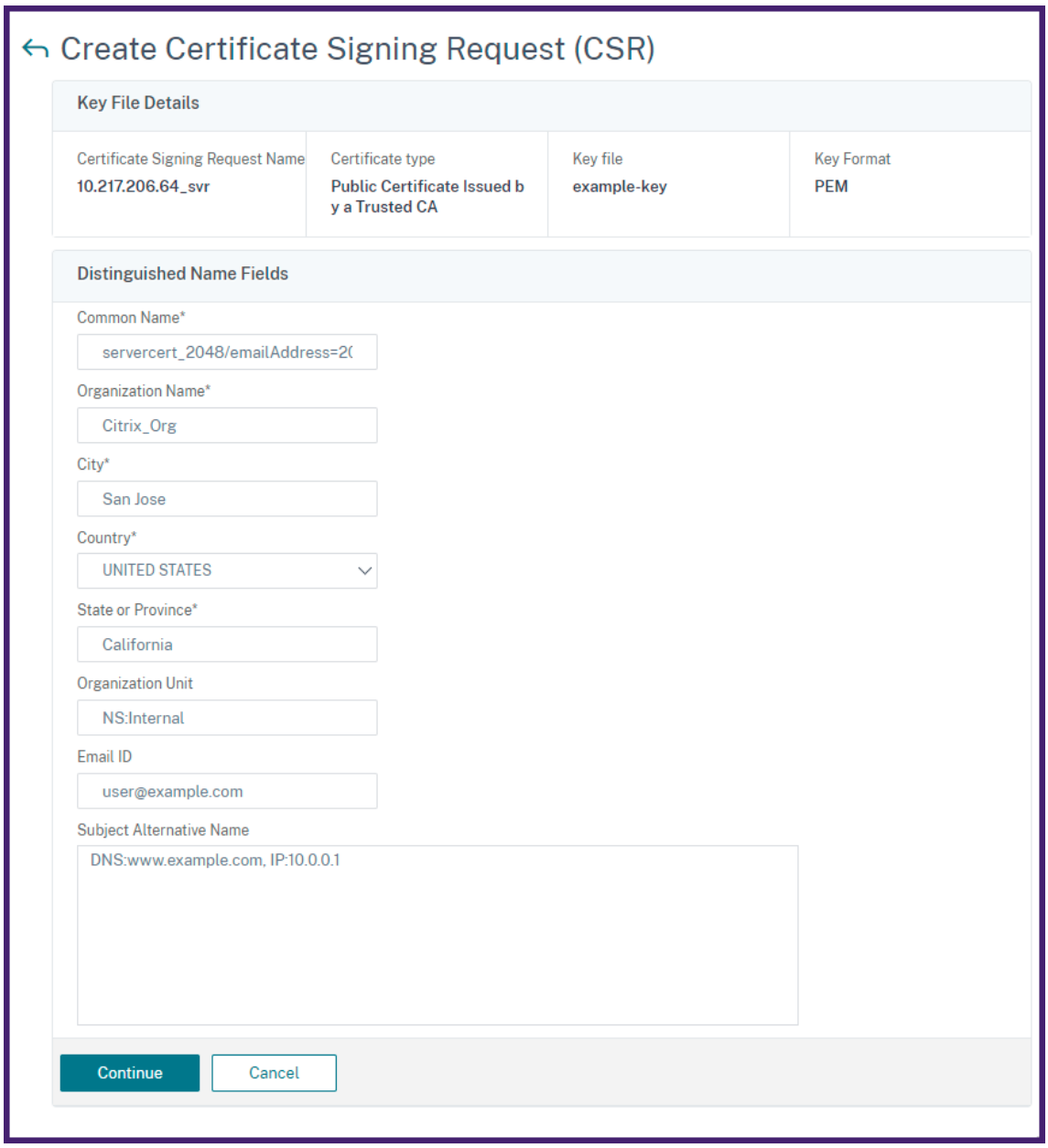
5. Klicken Sie auf **Weiter**.
6. Geben Sie auf der folgenden Seite weitere Details an.

   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

February 5, 2024

Sie erstellen ein Zertifikatspaket, 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“von Zertifikat A der „Domäne“von Zertifikat B entsprechen.

So verknüpfen Sie mithilfe von NetScaler ADM ein SSL-Zertifikat mit einem anderen Zertifikat:

1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zu **Infrastruktur**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 wählen Sie dann in der Dropdownliste **Aktion** die Option **Verknüpfung** aus.
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 zum Verknüpfen gefunden.

So heben Sie die Verknüpfung eines SSL-Zertifikats mithilfe von NetScaler ADM auf:

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > 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 wählen Sie dann **Verknüpfung aufheben** aus der Dropdownliste **Aktion** aus.
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.

Unternehmensrichtlinie konfigurieren

February 5, 2024

In NetScaler Application Delivery Management (ADM) können Sie eine Unternehmensrichtlinie konfigurieren und alle vertrauenswürdigen Zertifizierungsstellen sowie sichere Signaturalgorithmen hinzufügen und die empfohlene Schlüsselstärke für Ihre Zertifikatsschlüssel auswählen. Wenn eines der auf Ihrer Citrix Application Delivery Controller (ADC) -Instanz installierten Zertifikate nicht zur Unternehmensrichtlinie hinzugefügt wurde, zeigt das SSL-Zertifikats-Dashboard den Aussteller dieser Zertifikate als **nicht empfohlen**an.

Wenn die Schlüsselstärke des Zertifikats nicht mit der in der Unternehmensrichtlinie empfohlenen Schlüsselstärke übereinstimmt, zeigt das SSL-Zertifikats-Dashboard die Stärken dieser Schlüssel außerdem als **Nicht empfohlen** an.

So konfigurieren Sie eine Unternehmensrichtlinie auf NetScaler ADM:

1. **Navigieren Sie in NetScaler ADM zu**Infrastruktur**>**SSL-Dashboard**und klicken Sie dann auf Einstellungen.**
2. Klicken Sie auf der Seite SSL-Einstellungen auf das Symbol **Bearbeiten**, um alle vertrauenswürdigen Zertifizierungsstellen und sicheren Signaturalgorithmen hinzuzufügen und die empfohlene Schlüsselstärke für Ihre Zertifikate und Schlüssel auszuwählen.
3. Klicken Sie auf **Speichern**, um Ihre Unternehmensrichtlinie zu speichern.

> **Hinweis**
>
> Das SSL-Dashboard zeigt nur die **Signaturalgorithmen** an, die über die Option **Einstellungen** ausgewählt wurden, und andere werden als **Nicht empfohlen**angezeigt.

SSL-Zertifikate von NetScaler-Instanzen abfragen

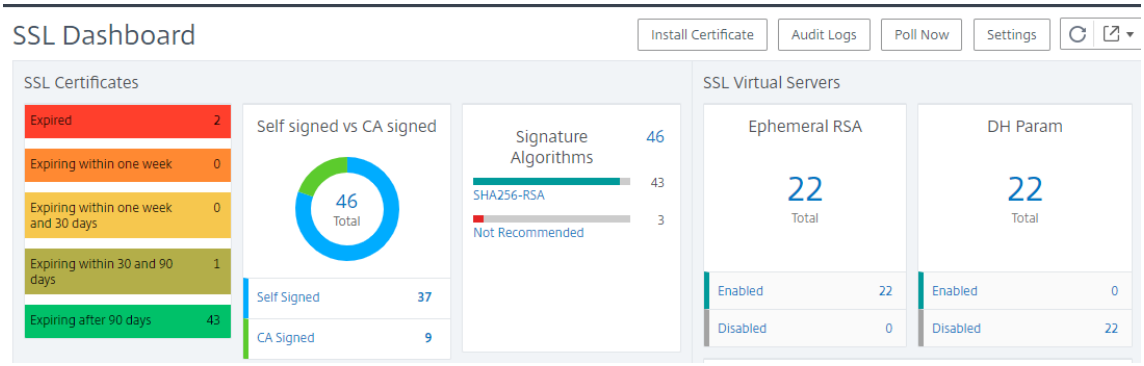
February 5, 2024

NetScaler Application Delivery Management (ADM) fragt SSL-Zertifikate automatisch alle 24 Stunden ab, indem es NITRO-Aufrufe und das Secure Copy (SCP) -Protokoll verwendet. Sie können die SSL-Zertifikate auch manuell abfragen, um neu hinzugefügte SSL-Zertifikate auf den Citrix Application Delivery Controller (ADC) -Instanzen zu ermitteln. Durch das Abrufen aller NetScaler-Instanzen SSL-Zertifikate wird das Netzwerk stark belastet.

Anstatt alle SSL-Zertifikate der NetScaler-Instanzen abzufragen, können Sie manuell nur die SSL-Zertifikate einer ausgewählten Instanz oder Instanzen abfragen.

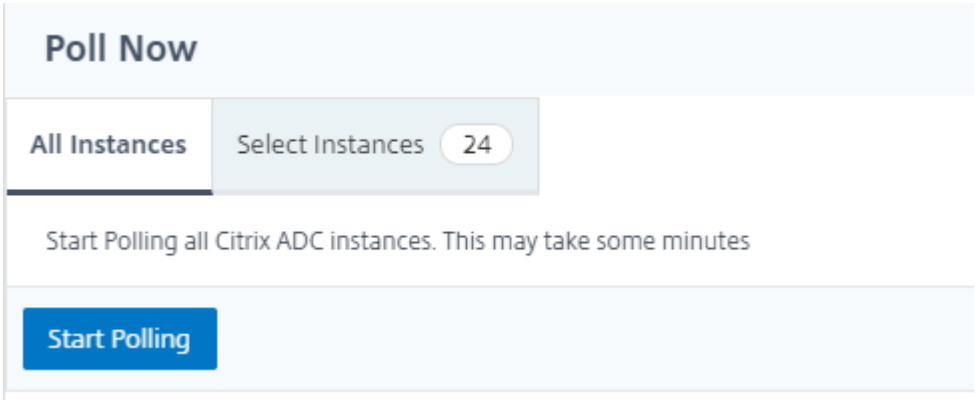
So fragen Sie SSL-Zertifikate auf NetScaler-Instanzen ab:

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > SSL Dashboard**.
2. Klicken Sie auf der Seite **SSL-Dashboard** oben rechts auf **Jetzt abfragen**.

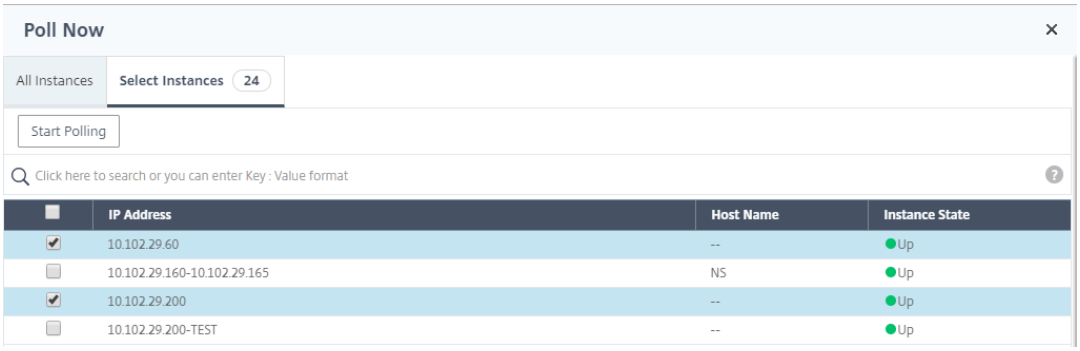


3. Die Seite **Jetzt abfragen** wird geöffnet und bietet Ihnen die Möglichkeit, alle NetScaler-Instanzen im Netzwerk oder die ausgewählten Instanzen abzufragen.

   a) Um die SSL-Zertifikate aller NetScaler-Instanzen abzufragen, wählen Sie die Registerkarte **Alle Instanzen** und klicken Sie auf **Abfrage starten**.



   b) Um bestimmte Instanzen abzufragen, wählen Sie die Registerkarte**Instanzenauswählen**aus, wählen Sie die Instanzen aus der Liste aus und klicken Sie auf**Jetzt abfragen**.



Verwenden Sie den NetScaler ADM-Zertifikatsspeicher, um SSL-Zertifikate zu verwalten

February 5, 2024

Mit dem NetScaler ADM-Zertifikatspeicher können Sie Ihre SSL-Zertifikate an einem Ort speichern und verwalten. Sie können die gespeicherten Zertifikate später verwenden, um NetScaler-Einstellungen zu konfigurieren.

Der Zertifikatsspeicher ermöglicht es Ihnen, SSL-Zertifikate hinzuzufügen, zu aktualisieren und zu löschen. Sie können den Zertifikatsspeicher auch verwenden, um ein Zertifikat aus einer NetScaler-Instanz zu importieren und es auf andere NetScaler-Zielinstanzen anzuwenden.

Fügen Sie dem Zertifikatsspeicher SSL-Zertifikate hinzu

1. Navigieren Sie zu **Infrastruktur > SSL-Dashboard > Zertifikatsspeicher**. Klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Zertifikat hinzufügen** die folgenden Details ein:
    - **Certkey Name** —Geben Sie einen Namen für das Zertifikat ein. Der Name darf nur alphanumerische ASCII-Zeichen, Unterstriche und Bindestriche enthalten und darf weniger als 30 Zeichen lang sein. Sie können den Namen nicht ändern, nachdem das Zertifikat erstellt wurde.
    - **Zertifikatsdatei** —Navigieren Sie zu Ihrem lokalen Laufwerk und laden Sie die Zertifikatsdatei hoch.
    - **Schlüsseldatei** —Laden Sie die Schlüsseldatei von Ihrem lokalen Computer hoch.
    - **Kennwort** —Wenn Sie einen verschlüsselten privaten Schlüssel im PEM-Format haben, geben Sie die Passphrase ein, mit der der private Schlüssel verschlüsselt wurde.
    - **Zertifikatskette hinzufügen** —Wählen Sie diese Option, um das Zertifikat zu einer Zertifikatskette hinzuzufügen.
    - **Certificate Chain** —Navigieren Sie zu Ihrem lokalen Laufwerk und laden Sie die Zertifikatsdatei hoch.
    - Klicken Sie auf **Erstellen**.

Aktualisieren Sie SSL-Zertifikate im Zertifikatsspeicher

1. Navigieren Sie zu **Infrastruktur > SSL-Dashboard > Zertifikatsspeicher**. Wählen Sie das Zertifikat aus, das Sie aktualisieren möchten, und klicken Sie auf **Aktualisieren**.

2. Geben Sie auf der Seite **Zertifikat aktualisieren** die folgenden Details ein:

    - **Certkey Name** —Zeigt den Namen des Zertifikats an, das Sie für die Aktualisierung ausgewählt haben.
    - **Zertifikatsdatei** —Um die Zertifikatsdatei zu aktualisieren, laden Sie eine Zertifikatsdatei hoch.
    - **Schlüsseldatei** —Um die Schlüsseldatei zu aktualisieren, laden Sie eine Schlüsseldatei von Ihrem lokalen Computer hoch.
    - **Kennwort** —Wenn Sie einen verschlüsselten privaten Schlüssel im PEM-Format haben, geben Sie die Passphrase ein, mit der der private Schlüssel verschlüsselt wurde.
    - **Zertifikatskette hinzufügen** —Wählen Sie diese Option, um das Zertifikat zu einer Zertifikatskette hinzuzufügen.
    - **Certificate Chain** —Navigieren Sie zu Ihrem lokalen Laufwerk und laden Sie die Zertifikatsdatei hoch.
    - Klicken Sie auf **OK**.

Löschen Sie SSL-Zertifikate aus dem Zertifikatsspeicher

1. Navigieren Sie zu **Infrastruktur > SSL-Dashboard > Zertifikatsspeicher**. Klicken Sie auf **Hinzufügen**.
2. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**, um das Zertifikat zu löschen.

Installieren Sie SSL-Zertifikate auf NetScaler-Instanzen

1. Navigieren Sie zu **Infrastruktur > SSL-Dashboard > Zertifikatsspeicher**. Wählen Sie das Zertifikat aus, das Sie auf einer NetScaler-Instanz installieren möchten.
2. Geben Sie auf der Seite **SSL-Zertifikat auf NetScaler-Instances installieren** die folgenden Details ein:

    a. **Quelle des Zertifikats**

    - **Zertifikat** —Zeigt den Namen des ausgewählten Zertifikats an.

    b. **Einzelheiten zum Zertifikat**

    - **Zertifikatsname** —Zeigt den Namen des Zertifikats an.
    - **Konfiguration speichern** —Wählen Sie diese Option, um die NetScaler-Konfiguration zu speichern. Die NetScaler-Konfiguration wird nach der Installation des Zertifikats gespeichert.

3. Klicken Sie auf **Instanzen auswählen**, um die NetScaler-Instanzen auszuwählen, auf denen Sie Ihre Zertifikate installieren möchten.

Klicken Sie auf **OK**.

Zertifikate aus NetScaler-Instanzen importieren

1. Navigieren Sie zu **Infrastruktur > SSL-Dashboard > Zertifikatsspeicher**. Klicken Sie auf **ADC-Zertifikate importieren**.
2. Auf der Seite **ADC-Zertifikate importieren** können Sie eine der folgenden Registerkarten auswählen:

   - **ADC-Zertifikate importieren** —Klicken Sie auf **Abfrage starten, um alle SSL-Zertifikate auf allen NetScaler-Instanzen abzufragen** .
   - **Instanzen auswählen** —Wählen Sie eine NetScaler-Instanz aus und klicken Sie auf **ADC-Zertifikate importieren, um SSL-Zertifikate** nur für die ausgewählte NetScaler-Instanz abzufragen.

   Nach der Abfrage werden die SSL-Zertifikate und Schlüsseldateien heruntergeladen und dem Zertifikatsspeicher hinzugefügt.

   > **Hinweis:**
   >
   > Der Importvorgang schlägt für Zertifikate fehl, wenn identische Zertifikatsnamen im Speicher vorhanden sind. Der Importvorgang ruft jedoch weiterhin die verbleibenden Zertifikate ab und fügt NetScaler-Zertifikate, falls verfügbar, dem Speicher hinzu.

Verwaltung benutzerdefinierter Datenbankzertifikate und Verschlüsselungen in einer Hochverfügbarkeitsbereitstellung

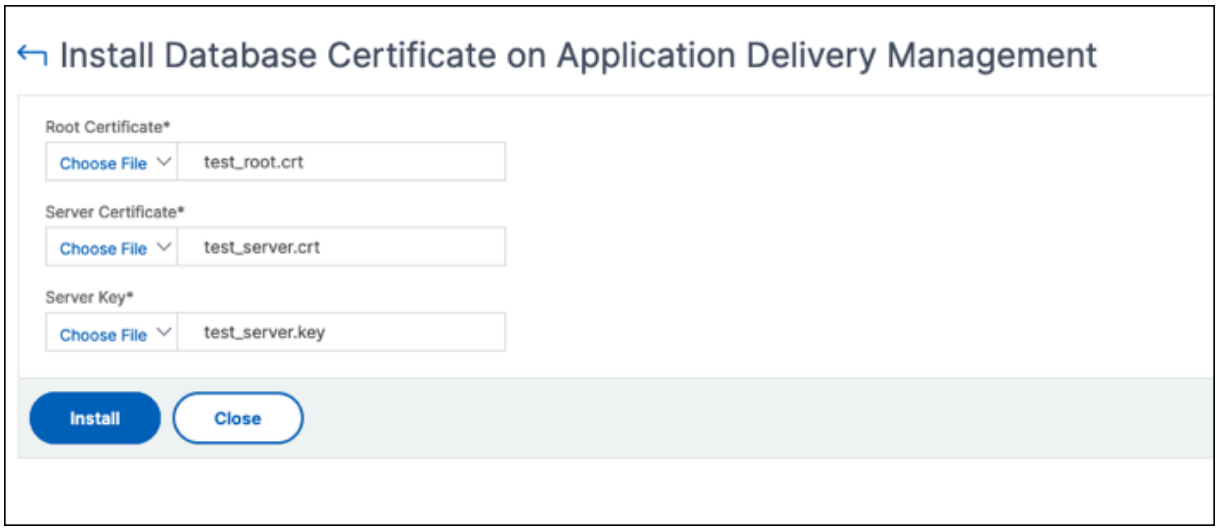
February 5, 2024

Mit NetScaler ADM können Sie die integrierten Standarddatenbankzertifikate durch Ihre eigenen Zertifikate einer vertrauenswürdigen Zertifizierungsstelle ersetzen. Sie können auch Ihre eigenen Cipher Suites in der NetScaler ADM-Datenbank konfigurieren. Diese Funktion bietet mehr Flexibilität und Sicherheit für Ihre Zertifikatsverwaltungsanforderungen und sichert die gesamte Kommunikation zwischen Ihren HA-Knoten mit vertrauenswürdigen SSL-Zertifikaten.

Installieren Sie Ihre Datenbankzertifikate auf NetScaler ADM

So installieren Sie Ihre Zertifikate in einem HA-Setup:

1. Navigieren Sie zu **Einstellungen > HA-Bereitstellung** und klicken Sie auf **Datenbankzertifikate**.
2. Klicken Sie auf die Registerkarte **Installiertes Zertifikat** und dann auf **Neues Zertifikat installieren**.
3. Laden Sie auf der Seite **Datenbankzertifikat auf Application Delivery Management installieren** ein Stammzertifikat, ein Serverzertifikat und einen Serverschlüssel hoch. Sie haben folgende Optionen:
    - **Wählen Sie „Datei“> „Lokal**“, um ein Zertifikat oder eine Schlüsseldatei von Ihrem lokalen Computer hochzuladen.
    - **Wählen Sie Datei > Appliance**, um ein Zertifikat oder eine Schlüsseldatei hochzuladen, die auf NetScaler ADM vorhanden ist.
4. Klicken Sie auf **Installieren**.



Hinweis:

Wenn es mehrere Kettenzertifikate gibt, müssen Sie sie in einer einzigen Datei kombinieren. Stellen Sie sicher, dass die Reihenfolge der Verkettung korrekt ist, wobei zuerst die Zwischenzertifikate und dann das Stammzertifikat stehen. Diese Reihenfolge ist unerlässlich, damit die Zertifikatskette korrekt erkannt wird.

Mit dem folgenden Befehl wird beispielsweise der Inhalt jeder Zertifikatsdatei (intermediate_certificate1.crt, intermediate_certificate2.crt und root_certificate.crt) an die Datei mit dem Namen combined_certs.crt angehängt:

```
cat intermediate_certificate1.crt >> combined_certs.crt
```

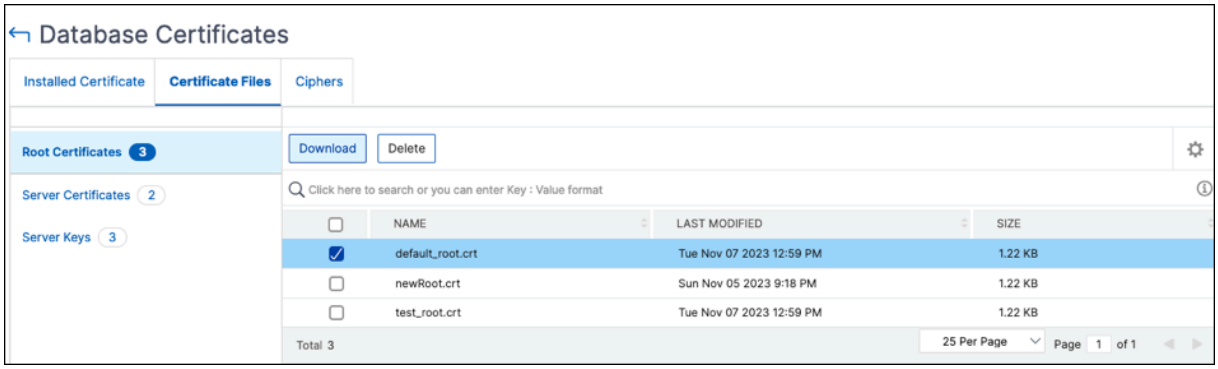


```
cat intermediate_certificate2.crt >> combined_certs.crt

cat root_certificate.crt >> combined_certs.crt
```

Installierte Datenbankzertifikate verwalten

So können Sie Ihre installierten Zertifikate anzeigen, herunterladen und löschen:

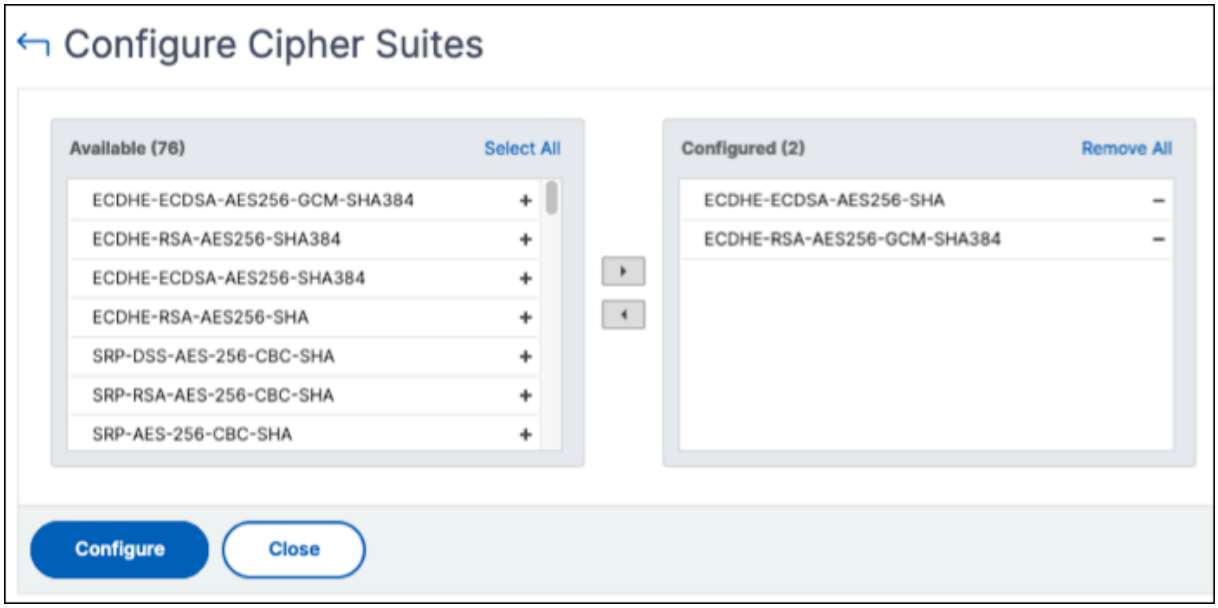
1. Navigieren Sie zu **Einstellungen > HA-Bereitstellung** und klicken Sie auf **Datenbankzertifikate**.
2. Klicken Sie auf die Registerkarte **Zertifikatsdateien** und wählen Sie **Stammzertifikate, Serverzertifikate**oder **Serverschlüssel** aus, um die entsprechenden Dateien anzuzeigen.
3. Um eine Datei auf Ihren lokalen Computer herunterzuladen, klicken Sie auf **Herunterladen**.
4. Um eine Zertifikatsdatei zu löschen, wählen Sie die Datei aus und klicken Sie auf **Löschen**. Klicken Sie im angezeigten Bestätigungsdialogfeld auf **OK**.



Datenbankverschlüsselungssammlungen konfigurieren

So konfigurieren Sie Cipher Suites für eine HA-Bereitstellung:

1. Navigieren Sie zu **Einstellungen > HA-Bereitstellung** und klicken Sie auf **Datenbankzertifikate**.
2. Klicken Sie auf die Registerkarte **Ciphers** und dann auf Cipher **konfigurieren**.
3. Wählen Sie auf der Seite **Cipher Suites konfigurieren** eine oder mehrere Chiffren aus der verfügbaren Verschlüsselungsliste aus.
4. Klicken Sie auf **Konfigurieren**. Klicken Sie im angezeigten Bestätigungsdialogfeld auf **Ja**, um die Verschlüsselungseinstellungen zu ändern.



> **Hinweis:**
>
> Durch das Ändern der Verschlüsselungseinstellungen werden die sekundären NetScaler ADM- und Disaster Recovery-Knoten neu gestartet.

Ereignisse

February 5, 2024

Wenn die IP-Adresse einer Citrix Application Delivery Controller (ADC) -Instanz zu NetScaler Application Delivery Management (ADM) hinzugefügt wird, sendet NetScaler 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 NetScaler-Instanz dar. Wenn beispielsweise ein Systemausfall oder eine Änderung in der Konfiguration vorliegt, wird ein Ereignis generiert und auf dem NetScaler ADM -Server aufgezeichnet. In NetScaler ADM empfangene Ereignisse werden auf der Seite "Ereignisse"(**Infrastruktur > Ereignisse**) angezeigt, und alle aktiven Ereignisse werden auf der Seite "Ereignismeldungen"angezeigt (**Infrastruktur > Ereignisse > Ereignismeldungen**).

NetScaler ADM überprüft auch die auf Instanzen generierten Ereignisse, um Alarme mit unterschiedlichen Schweregraden zu bilden. Diese Alarme werden dann als Nachrichten angezeigt, von denen einige möglicherweise sofortige Aufmerksamkeit erfordern. Beispielsweise kann ein Systemausfall als "kritischer"Ereignisschweregrad eingestuft werden und müsste sofort behoben werden.

Sie können Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Regeln erleichtern die Überwachung der Ereignisse, die viele sein können, die in Ihrer NetScaler-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, NetScaler-Instanzen, Kategorie, Fehlerobjekte, Konfigurationsbefehle und Meldungen.

Sie können auch sicherstellen, dass mehrere Benachrichtigungen für ein Ereignis für ein bestimmtes Zeitintervall ausgelöst werden, bis das Ereignis gelöscht wird. Als zusätzliche Maßnahme können Sie Ihre E-Mail mit einer bestimmten Betreffzeile und einer Benutzernachricht anpassen und einen Anhang hochladen.

Ereignisdashboard verwenden

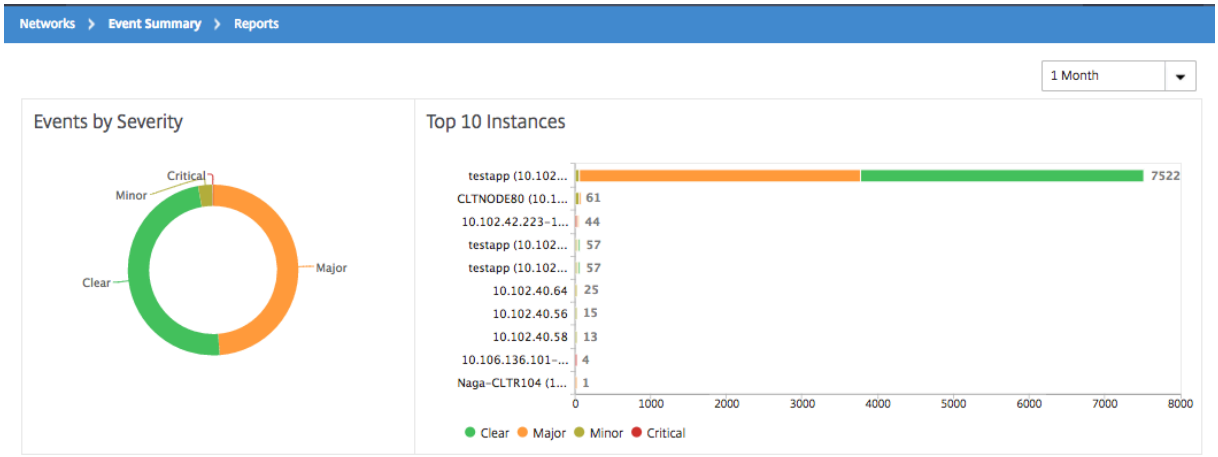
February 5, 2024

Als Netzwerkadministrator können Sie Details wie Konfigurationsänderungen, Anmeldebedingungen, Hardwarefehler, Schwellenwertverletzungen und Änderungen des Entitätsstatus auf Ihren Citrix Application Delivery Controller (ADC) -Instanzen sowie Ereignisse und deren Schweregrad für bestimmte Instanzen einsehen. Sie können das Event-Dashboard von NetScaler Application Delivery Management (ADM) verwenden, um Berichte einzusehen, die für Details zum Schweregrad kritischer Ereignisse für all Ihre NetScaler-Instances generiert wurden.

So zeigen Sie die Details im Ereignis-Dashboard an:

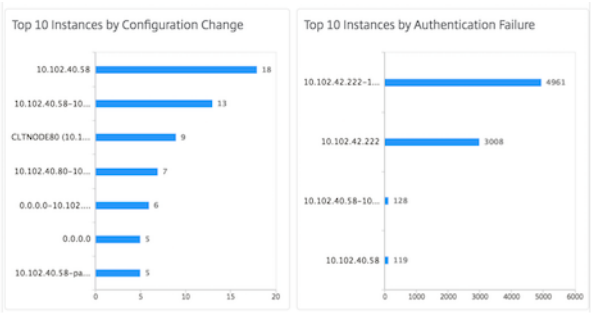
Navigieren Sie zu **Infrastruktur > Ereignisse > Berichte**.

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.

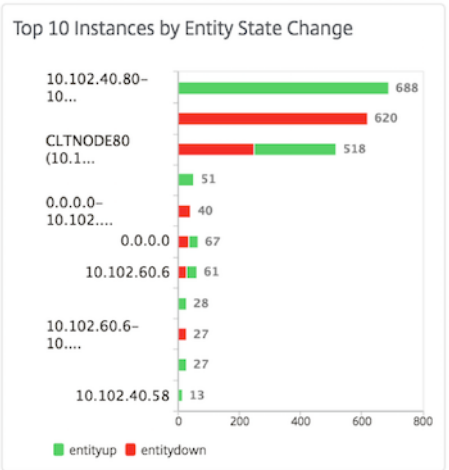


Sie können weitere Details anzeigen, indem Sie zum NetScaler-Instanztyp navigieren (**Infrastruktur > Ereignisse > Berichte** > **NetScaler/NetScaler SDX**), um Folgendes anzuzeigen:

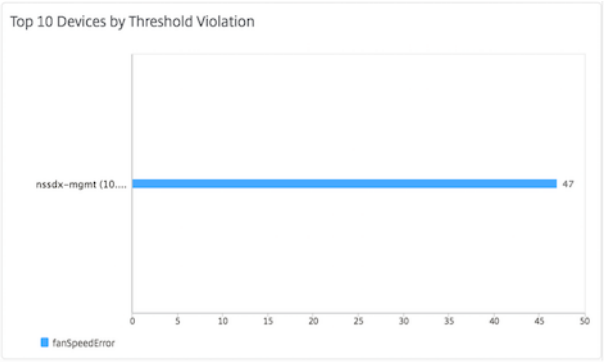
- Top 10 Geräte nach Hardwarefehler
- Top 10 Geräte nach Konfigurationsänderung
- Top 10 Geräte durch Authentifizierungsfehler



- Top 10 Geräte nach Entitätsstatusänderungen



- Top 10 Geräte nach Schwellenverletzung



Ereignisalter für Ereignisse festlegen

February 5, 2024

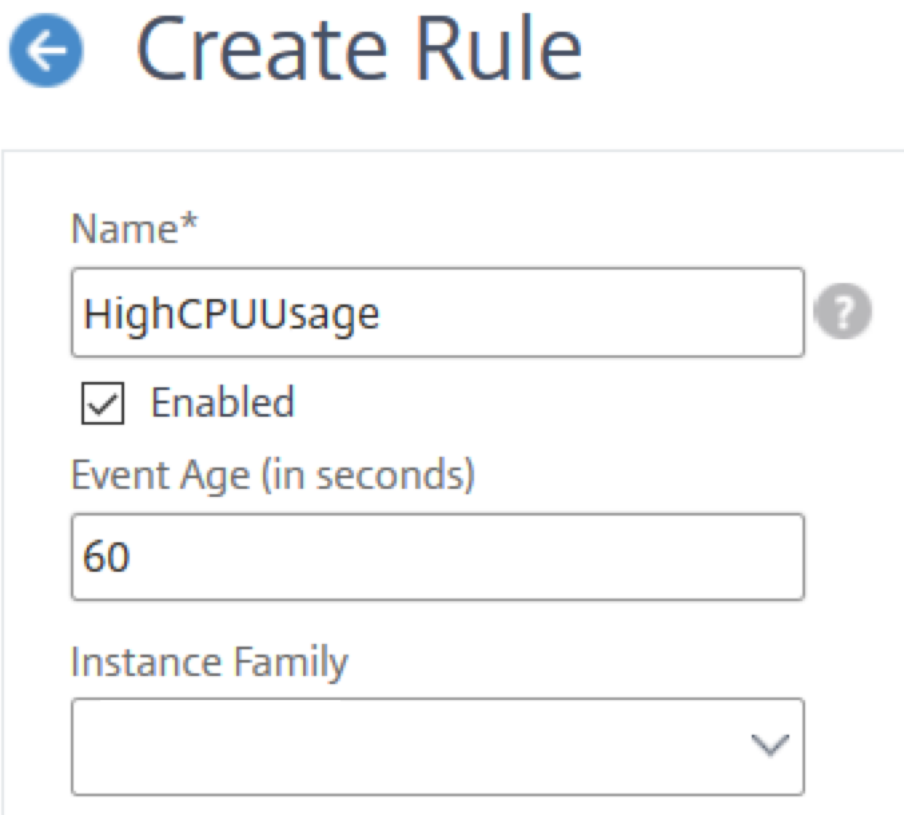
Sie können die Option Ereignisalter festlegen, um das Zeitintervall (in Sekunden) anzugeben. NetScaler ADM überwacht die Appliances bis zur festgelegten Dauer und generiert nur dann ein Ereignis, wenn das Ereignisalter die festgelegte Dauer überschreitet.

> Hinweis:
>
> Der Mindestwert für das Ereignisalter ist 60 Sekunden. Wenn Sie das Feld **Ereignisalter** leer lassen, wird die Ereignisregel unmittelbar nach dem Auftreten des Ereignisses angewendet.

Stellen Sie sich beispielsweise vor, dass Sie verschiedene ADC-Appliances verwalten und per E-Mail benachrichtigt werden möchten, wenn einer Ihrer virtuellen Server für 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 NetScaler ADM fest:

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > 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.



Stellen Sie sicher, dass alle ko-bezogenen Traps im Abschnitt **Kategorie** festgelegt sind, und legen Sie auch den entsprechenden Schweregrad im Abschnitt **Schweregrad** fest, wenn Sie das Ereignisalter festlegen. Wählen Sie im vorherigen Beispiel die `entityofs` Traps `entityup` `entitydown`, und aus.

Ereignisfilter planen

February 5, 2024

Nachdem Sie einen Filter für Ihre Regel erstellt haben und nicht möchten, dass der NetScaler Application Delivery Management (ADM) -Server 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 eine große Anzahl von E-Mail-Benachrichtigungen, wenn NetScaler

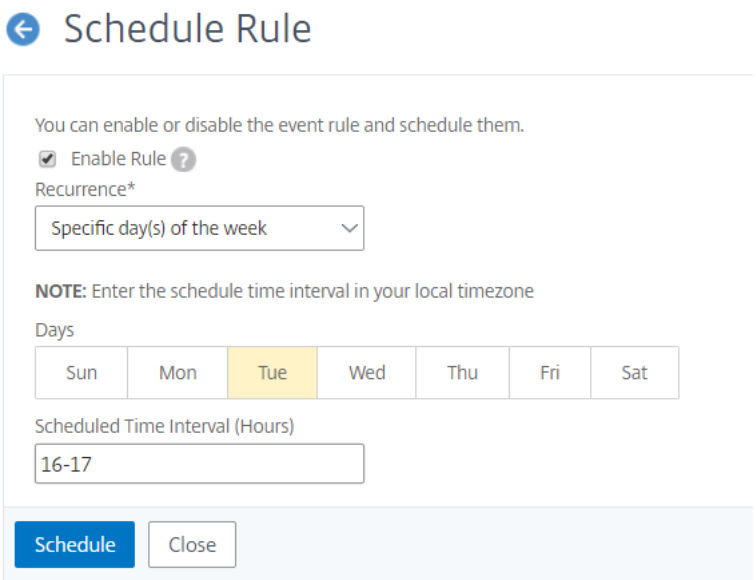
ADM diese Traps empfängt. Wenn Sie möchten, dass der Server diese E-Mail-Benachrichtigungen nur während eines bestimmten Zeitraums sendet, können Sie dies tun, indem Sie einen Filter planen.

So planen Sie einen Filter mit NetScaler ADM:

1. Navigieren Sie im NetScaler ADM zu **Infrastruktur > 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. Wählen Sie entweder einen bestimmten Wochentag oder ein bestimmtes Datum in einem Monat aus.
    - **Tage**: Wählen Sie den Wochentag aus, an dem die Regel ausgeführt werden soll. Sie können mehrere Tage auswählen.
    - **Termine**: Geben Sie die Daten ein. Sie können mehrere Datumsangaben als kommagetrennte Werte eingeben.
    - **Geplantes Zeitintervall (Stunden)** —Stunden, in denen die Regel geplant werden soll (verwenden Sie das 24-Stunden-Format).

4. Klicken Sie auf **Zeitplan**.



Wiederholte E-Mail-Benachrichtigungen für Ereignisse festlegen

February 5, 2024

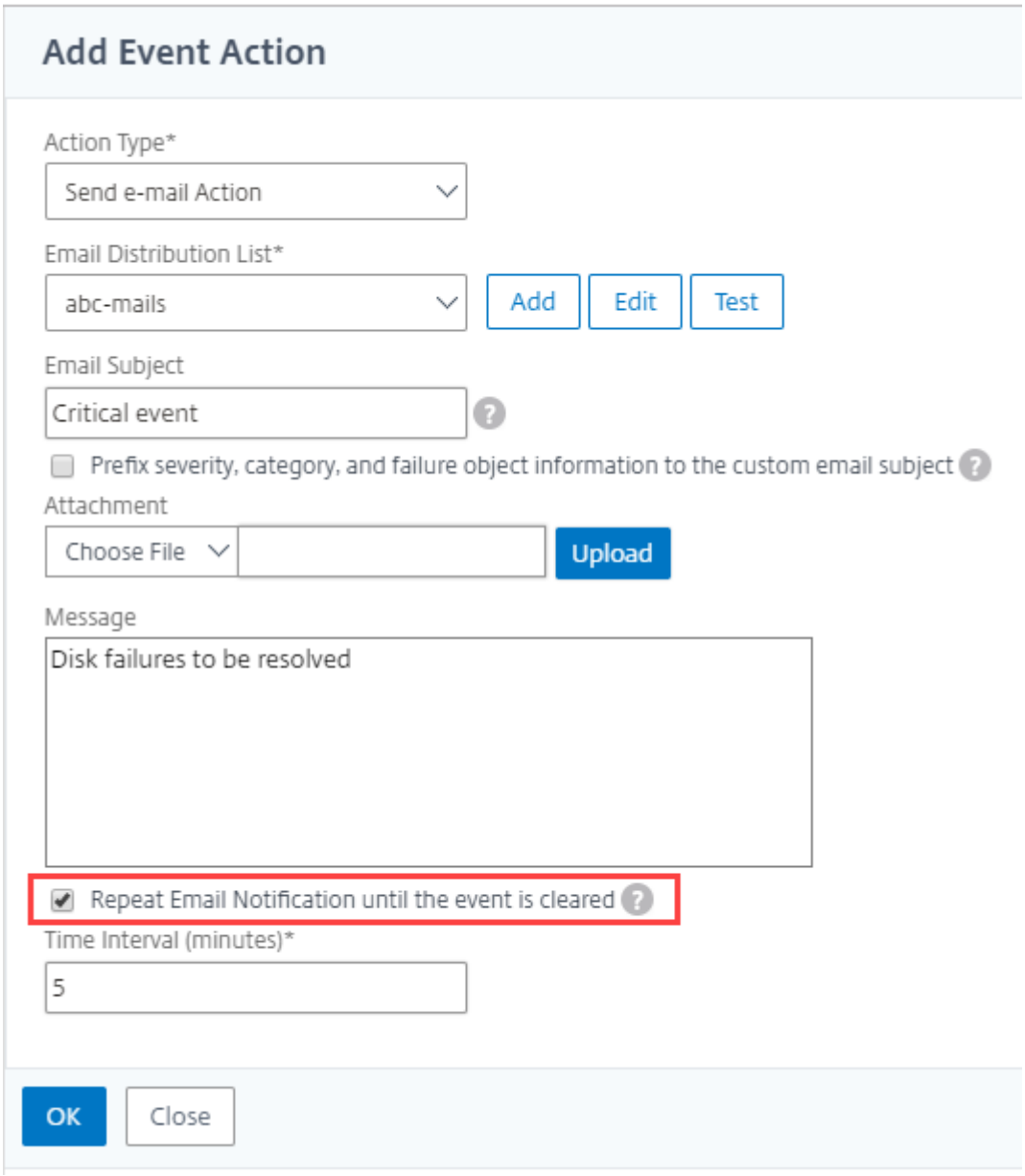
Um sicherzustellen, dass alle kritischen Ereignisse behandelt werden und keine wichtigen E-Mail-Benachrichtigungen übersehen werden, können Sie sich dafür entscheiden, wiederholte E-Mail-Benachrichtigungen zu senden, wenn die Eventregeln die von Ihnen ausgewählten Kriterien erfüllen. Wenn Sie beispielsweise eine Ereignisregel für Instanzen mit Datenträgerausfällen erstellt haben und Sie benachrichtigt werden möchten, bis das Problem behoben ist, können Sie sich 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 er die Benachrichtigung gesehen hat oder die Ereignisregel gelöscht wurde.

> **Hinweis**
>
> Ereignisse können nur automatisch gelöscht werden, wenn ein entsprechender "Clear"-Trap eingerichtet und von Ihrer Citrix Application Delivery Controller (ADC)-Instanz gesendet wird.
>
> Um ein Ereignis manuell zu löschen, können Sie Folgendes tun:
>
> - Navigieren Sie zu **Infrastruktur > Ereignisse > Ereigniszusammenfassung**, wählen Sie eine **Kategorie** aus, wählen Sie ein Ereignis in der Kategorie aus und klicken Sie auf **Löschen**.
> - Oder navigieren Sie zu **Infrastruktur > Ereignisse > Ereignismeldungen**. Wählen Sie einen Instanztyp aus, wählen Sie ein Ereignis aus dem unten stehenden Raster aus, und klicken Sie auf **Löschen**.

So legen Sie wiederholte E-Mail-Benachrichtigungen von NetScaler ADM fest:

1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zu **Infrastruktur > 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 Veranstaltungsregeln auf **Aktion hinzufügen** . Wählen Sie dann in der Dropdownliste****Aktionstyp die Option E-Mail-Aktion** senden** und wählen Sie eine **E-Mail-Verteilerliste**aus.
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

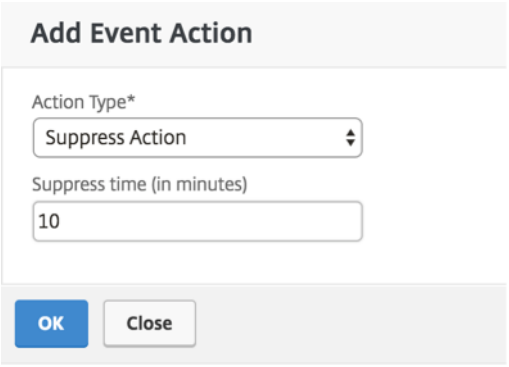
February 5, 2024

Wenn Sie die Ereignisaktion **Aktion unterdrücken** wählen, 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 NetScaler ADM die Unterdrückungszeit als Null und läuft nie ab.

So unterdrücken Sie Ereignisse mithilfe von NetScaler ADM:

1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zu **Infrastruktur > Ereignisse > Regeln**. Klicken Sie auf **Hinzufügen**.
2. 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** "in der Dropdownliste **Aktionstyp die Option Aktionunterdrücken** aus, und geben Sie den Zeitraum in Minuten an, für den ein Ereignis unterdrückt werden muss.
5. Klicken Sie auf **OK**.



Ereignisregeln erstellen

February 5, 2024

Sie können Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Regeln erleichtern die Überwachung einer großen Anzahl von Ereignissen, die in Ihrer Infrastruktur generiert werden.

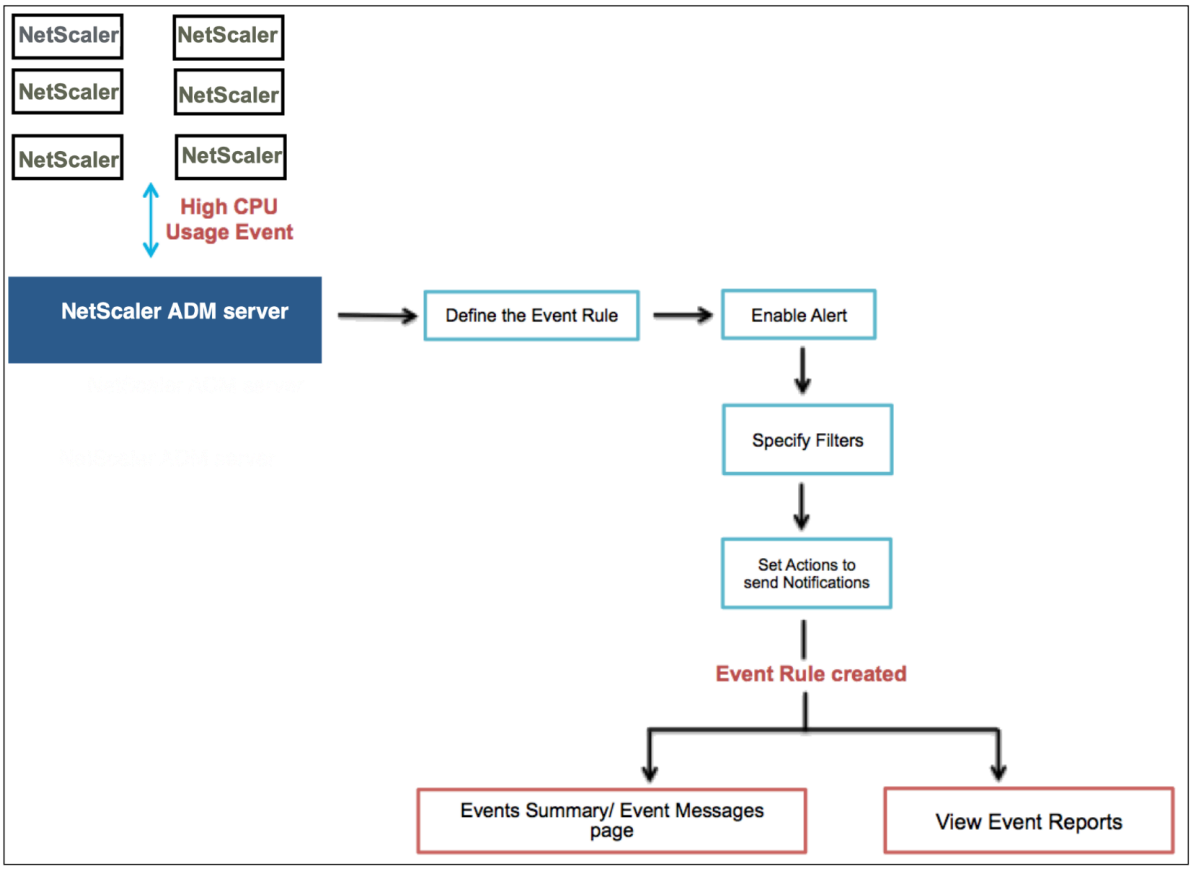
Sie können eine Reihe von Ereignissen filtern, indem Sie Regeln mit bestimmten Bedingungen konfigurieren und den Regeln Aktionen zuweisen. Wenn die generierten Ereignisse die Filterkriterien in der Regel erfüllen, wird die mit der Regel verknüpfte Aktion ausgeführt. Die Bedingungen für die Erstellung von Filtern sind: Schweregrad, Citrix Application Delivery Controller Instanzen (NetScaler), Kategorie, Fehlerobjekte, Konfigurationsbefehle und Meldungen.

Sie können den Ereignissen die folgenden Aktionen zuweisen:

- **E-Mail-Aktion senden**: 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.
- **Slack-Benachrichtigungen**senden: Sende 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 Aktionen für Ereignisregeln 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 für bestimmte NetScaler-Instanzen überwachen, wenn diese Ereignisse zu einem Ausfall Ihrer NetScaler-Instanzen führen können. Sie haben folgende Möglichkeiten:

- Erstellen Sie eine Regel zur Überwachung der Instanzen und geben Sie eine Aktion an, mit der Sie eine E-Mail-Benachrichtigung erhalten, wenn ein Ereignis in der Kategorie “Hohe CPU-Auslastung”eintritt.
- Planen Sie die Regel so, dass sie zu einer bestimmten Zeit ausgeführt wird, z. B. zwischen 11 und 23 Uhr, damit Sie nicht jedes Mal benachrichtigt werden, wenn ein Ereignis generiert wird.

Das Konfigurieren einer Ereignisregel umfasst die folgenden Aufgaben:

1. Definieren Sie die Regel
2. Wählen Sie den Schweregrad des Ereignisses aus, das die Regel erkennt
3. Ereigniskategorie angeben
4. NetScaler-Instanzen angeben, für die die Regel gilt
5. Fehlerobjekte auswählen
6. Erweiterte Filter angeben

7. Aktionen angeben, die ausgeführt werden sollen, wenn die Regel ein Ereignis erkennt

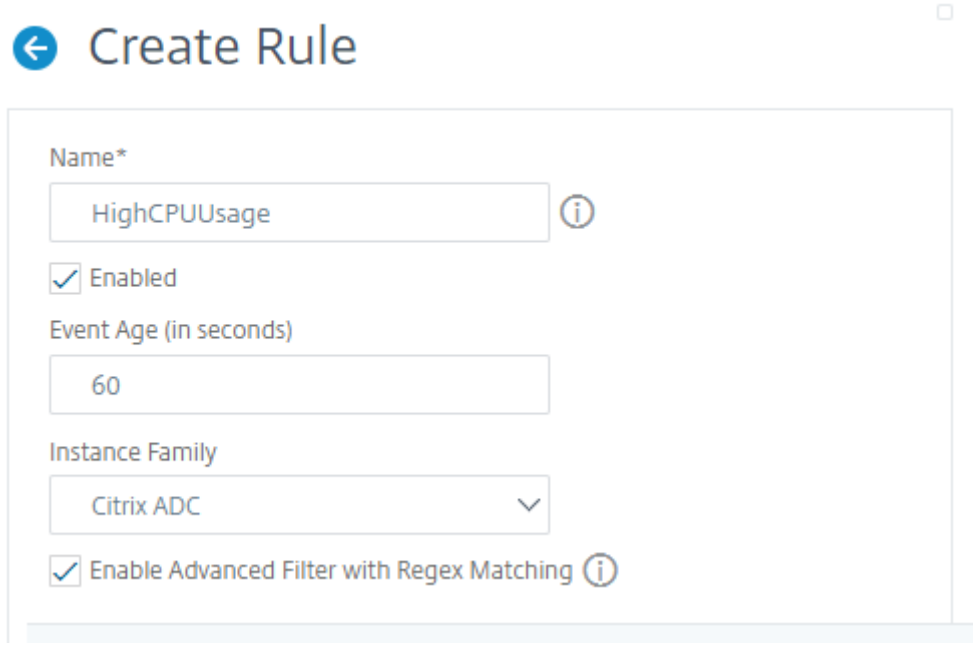
Schritt 1 - Definieren einer Ereignisregel

Navigieren Sie zu **Infrastruktur > 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 NetScaler ADM eine Ereignisregel aktualisiert.

> Hinweis:
>
> Der Mindestwert für das Ereignisalter ist 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 NetScaler-Instanz 60 Sekunden oder länger ein Ereignis mit “hoher CPU-Auslastung”aufweist. Sie können das Ereignisalter auf 60 Sekunden festlegen, sodass Sie jedes Mal, wenn Ihre NetScaler-Instanz 60 Sekunden oder länger ein Ereignis mit “hoher CPU-Auslastung” aufweist, eine E-Mail-Benachrichtigung mit Details zum Ereignis erhalten.



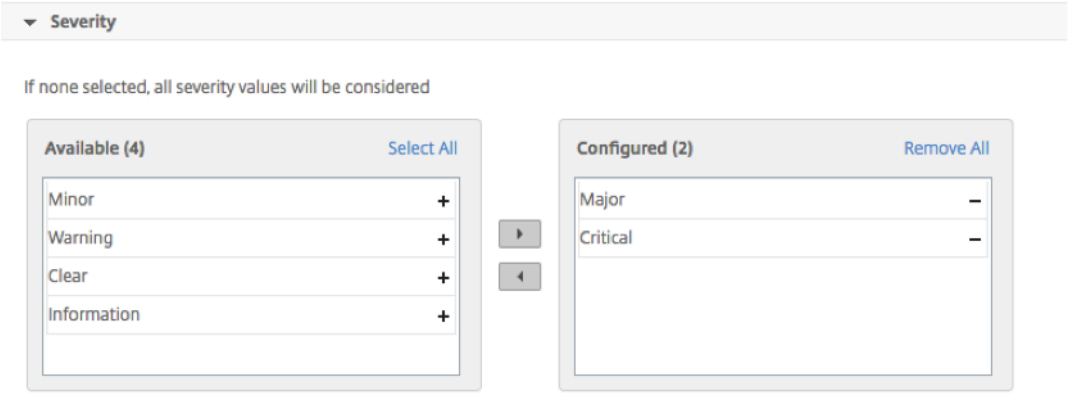
Sie können Ereignisregeln auch nach **Instanzfamilie** filtern, um die NetScaler-Instanz zu verfolgen, von der NetScaler ADM ein Ereignis empfängt.

Wenn Sie einen anderen regulären Ausdruck als den Mustervergleich mit Sternchen (*) einschließen möchten, wählen Sie **Erweiterte Filter mit Regex-Abgleich 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.

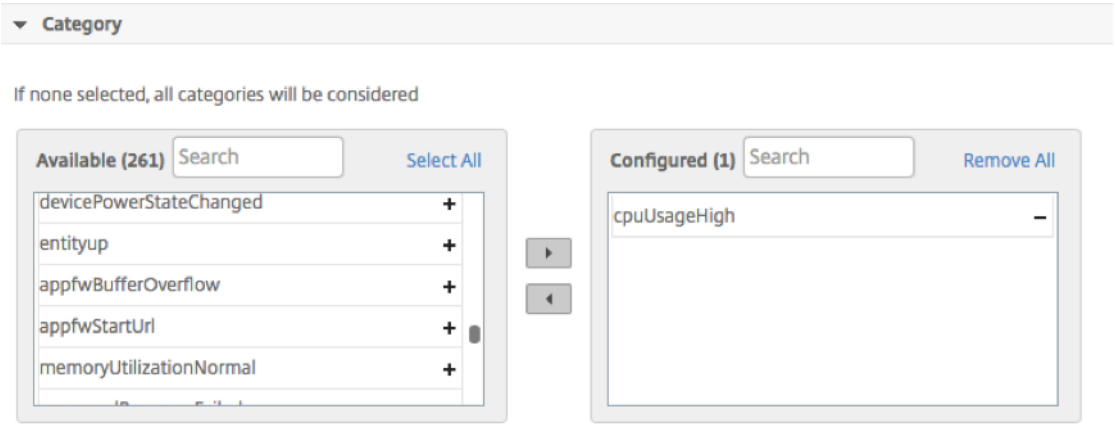


> **Hinweis**
>
> Sie können den Schweregrad sowohl für generische als auch für fortgeschrittene Ereignisse konfigurieren. Um den Schweregrad der Ereignisse für NetScaler-Instanzen zu ändern, die auf NetScaler ADM verwaltet werden, navigieren Sie zu **Infrastruktur > Ereignisse > Ereigniseinstellungen**. 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 —Event-Kategorie angeben

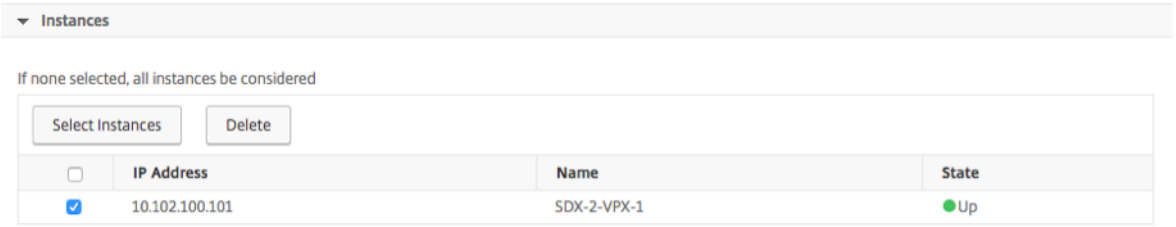
Sie können die Kategorie oder Kategorien der Ereignisse angeben, die von Ihren NetScaler-Instanzen generiert werden. Alle Kategorien werden auf NetScaler-Instanzen erstellt. Diese Kategorien werden dann mit NetScaler ADM zugeordnet, das zur Definition von Ereignisregeln verwendet werden kann. Wählen 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 NetScaler-Instanzen

Wählen Sie die IP-Adressen der NetScaler-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

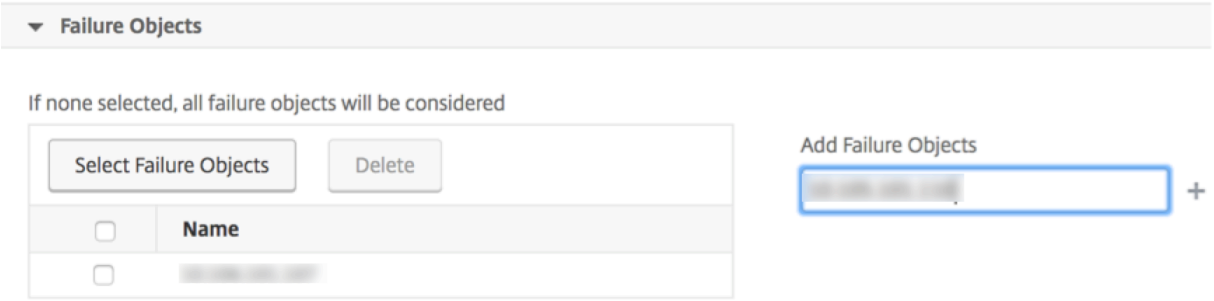
Sie können entweder ein Versagensobjekt aus der bereitgestellten Liste auswählen oder ein Fehlerobjekt hinzufügen, für das ein Ereignis generiert wurde. Sie können auch einen regulären Ausdruck angeben, um Fehlerobjekte hinzuzufügen. Abhängig vom angegebenen regulären Ausdruck werden die Fehlerobjekte automatisch zur Liste hinzugefügt. Fehlerobjekte sind Entitätsinstanzen oder Leistungsindikatoren, für die ein Ereignis generiert wurde.

> **Wichtig**
>
> Um Fehlerobjekte mit regulärem Ausdruck aufzulisten, wählen Sie in Schritt 1**Erweiterten Filter mit Regex-Abgleich aktivieren**.

Das Fehlerobjekt wirkt sich auf die Art und Weise aus, wie ein Ereignis verarbeitet wird, und stellt sicher, dass es genau das gemeldete Problem widerspiegelt. Mit diesem Filter können Sie Probleme auf den Fehlerobjekten schnell verfolgen und die Ursache für ein Problem identifizieren. Wenn ein

Benutzer beispielsweise Anmeldeprobleme hat, ist das Fehlerobjekt hier der Benutzername oder das Kennwort, z. `nsroot`B.

Diese Liste kann Leistungsindikatornamen für alle mit Schwellenwert verbundenen Ereignisse, Entitätsnamen für alle Entity-bezogenen Ereignisse, Zertifikatnamen für zertifikatbezogene Ereignisse usw. enthalten.

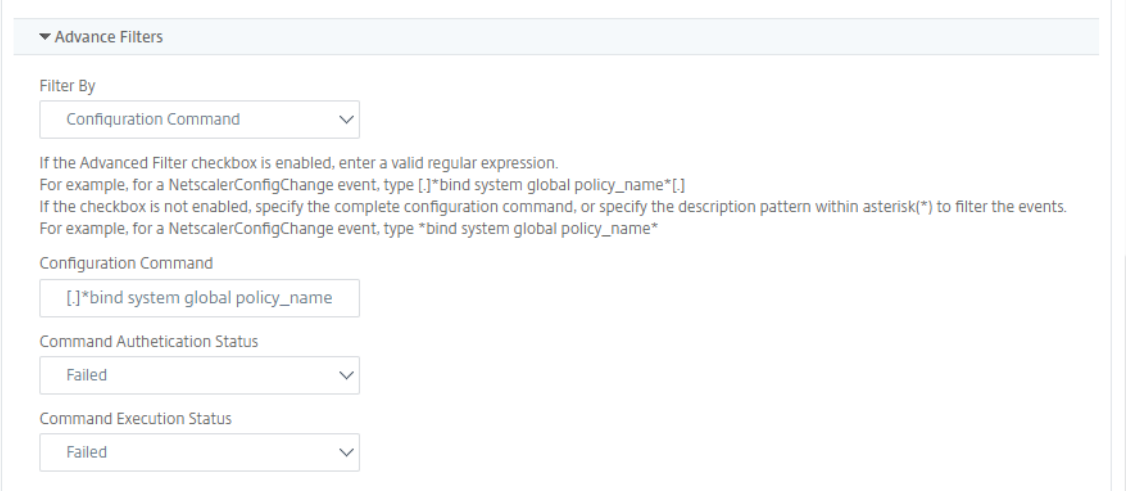


Schritt 6 - Angeben von erweiterten Filtern

Sie können eine Ereignisregel weiter filtern nach:

- **Konfigurationsbefehle** - Sie können den vollständigen Konfigurationsbefehl angeben oder einen regulären Ausdruck angeben, um Ereignisse zu filtern.

  Sie können die Ereignisregel weiter nach dem Authentifizierungsstatus des Befehls und/oder seinem Ausführungsstatus filtern. Geben Sie beispielsweise für a `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 Ereignis `NetscalerConfigChange` die Option `[.]*`

`ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)` ein.

Schritt 7 —Aktionen für Ereignisregeln 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 Action
- Trap-Aktion senden
- Befehls-Aktion ausführen
- Job-Aktion ausführen
- Aktion unterdrücken
- Slack Benachrichtigungen senden
- PagerDuty-Benachrichtigungen senden
- ServiceNow-Benachrichtigungen senden

So richten Sie eine E-Mail-Ereignisregelaktion ein

Wenn Sie den Aktionstyp Aktion E-Mail senden auswählen, wird eine E-Mail ausgelöst, wenn die Ereignisse die definierten Filterkriterien erfüllen. Sie müssen entweder eine E-Mail-Verteilerliste erstellen, indem Sie E-Mail-Server- oder E-Mail-Profildetails angeben, oder Sie können eine E-Mail-Verteilerliste auswählen, die Sie zuvor erstellt haben.

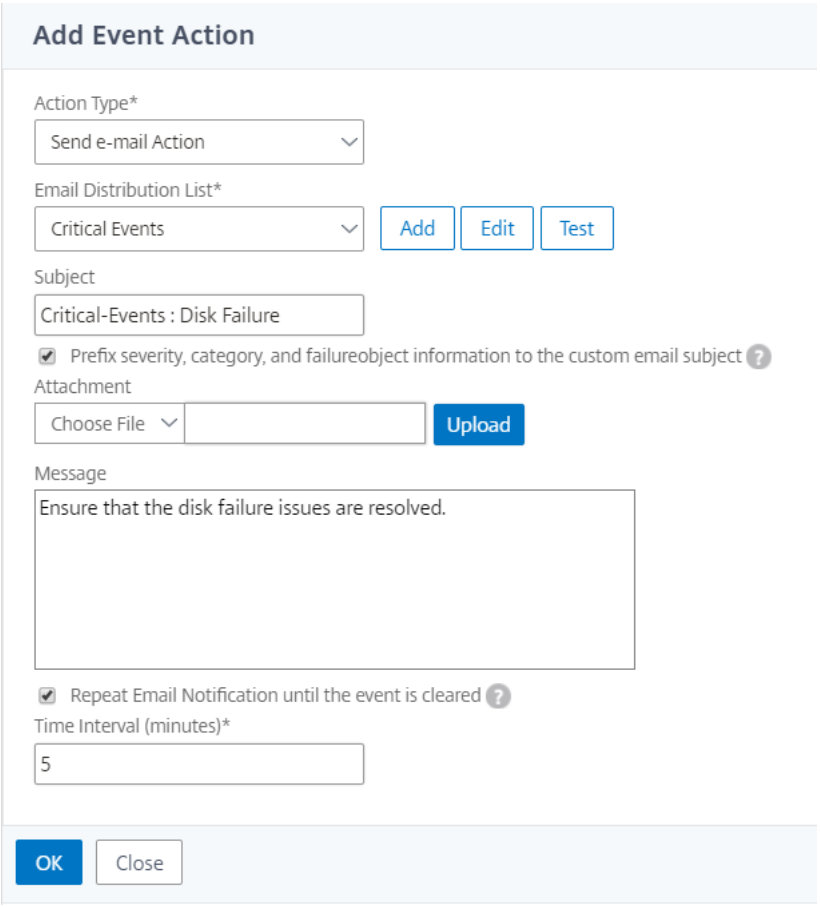
Aufgrund einer hohen Anzahl virtueller Server, die in NetScaler ADM konfiguriert werden, erhalten Sie möglicherweise täglich eine hohe Anzahl von E-Mails. Die E-Mails haben eine standardmäßige Betreffzeile, die Informationen über den Schweregrad des Ereignisses, die Kategorie des Ereignisses und das Fehlerobjekt enthält. 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 und den Namen des Fehlerobjekts hinzuzufügen.

Sie können auch eine benutzerdefinierte Betreffzeile und eine Benutzernachricht hinzufügen und einen Anhang 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 jetzt 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.

Sie können auch sicherstellen, dass alle kritischen Ereignisse behandelt werden und keine wichtigen E-Mail-Benachrichtigungen verpasst werden, indem **Sie das Kontrollkästchen E-Mail-Benachrichtigung wiederholen, bis das Ereignis deaktiviert ist**, um wiederholte E-Mail-Benachrichtigungen für Ereignisregeln zu senden, die die von Ihnen ausgewählten Kriterien erfüllen. Wenn Sie beispielsweise eine Ereignisregel für Instanzen mit Datenträgerausfällen erstellt haben und Sie benachrichtigt werden möchten, bis das Problem behoben ist, können Sie sich 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 die Definition einer Trap-Verteilerliste (oder eines Trap-Ziels und Trap-Profildetails) werden Trap-Nachrichten an bestimmte Trap-Listener gesendet, wenn die 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 in NetScaler 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 dem Typ der Fallen, die in der Kategorie des Filters definiert sind.
$entity	Dieser Parameter entspricht den Entitätsinstanzen oder Leistungsindikatoren, für die ein Ereignis generiert wurde. Sie kann die Leistungsindikatornamen für alle Ereignisse im Zusammenhang mit dem Schwellenwert, Entitätsnamen für alle entitätsbezogenen Ereignisse und Zertifikatsnamen für alle zertifikatbezogenen Ereignisse enthalten.
$severity	Dieser Parameter entspricht dem Schweregrad des Ereignisses.
$ failure.obj	Das Fehlerobjekt wirkt sich auf die Art und Weise aus, wie ein Ereignis verarbeitet wird, und stellt sicher, dass das Fehlerobjekt genau das gemeldete Problem 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.

Stellen Sie sich beispielsweise vor, dass Sie eine Aktion zum Ausführen von Befehlen festlegen möchten, wenn der Status eines virtuellen Lastausgleichsservers **auf Nicht verfügbar**ist Als Administrator sollten Sie eine schnelle Problemumgehung in Betracht ziehen, indem Sie einen weiteren virtuellen Server hinzufügen. In NetScaler ADM können Sie:

- Schreiben Sie eine Skriptdatei (.sh).

  Im Folgenden finden Sie eine Beispielskriptdatei (.sh):

```
1  #!/bin/sh
2  source=$1
3  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 Ort auf dem NetScaler ADM Agent. Beispiel: `/var`.
- Geben Sie den Speicherort der SH-Datei in NetScaler 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 Sie die 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. Wählen oder erstellen Sie ein Fehlerobjekt für den virtuellen Server
6. Klicken Sie unter **Ereignisregelaktionen**auf **Aktion hinzufügen**, und wählen Sie in der Liste ****Aktionstyp die Option Befehlsaktion** ausführen** aus.
7. Klicken **Sie unter Liste der Befehlsausführung**auf **Hinzufügen**.

   Die Seite “Befehlsverteilerliste erstellen”wird angezeigt.

   a) Geben Sie unter **Profilname**einen Namen Ihrer Wahl an

   b) Geben Sie **unter Run Command**den NetScaler ADM Agent-Speicherort an, in dem das Skript ausgeführt werden muss. Beispiel: `/sh/var/demo.sh $source $failureobj`.

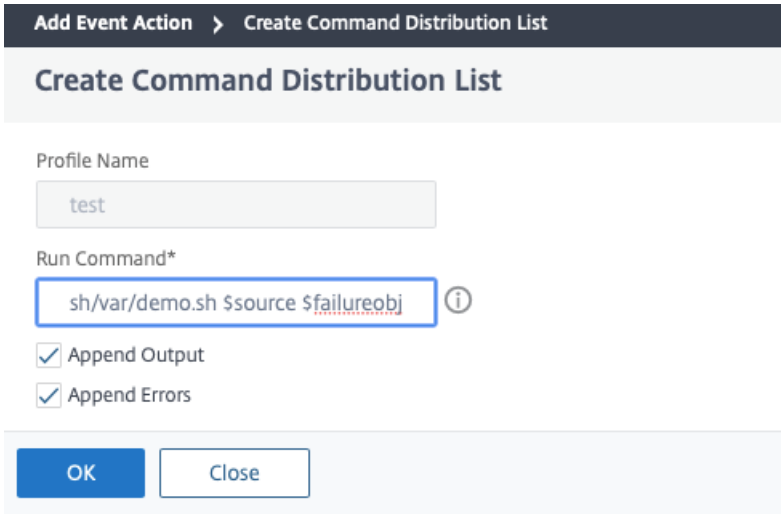
   c) Wählen Sie **Ausgabe anhängen** und **Fehler anhängen**.

   > **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 NetScaler ADM -Serverprotokolldateien generiert wurden (falls vorhanden). Wenn Sie diese Optionen nicht aktivieren, verwirft NetScaler 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**.



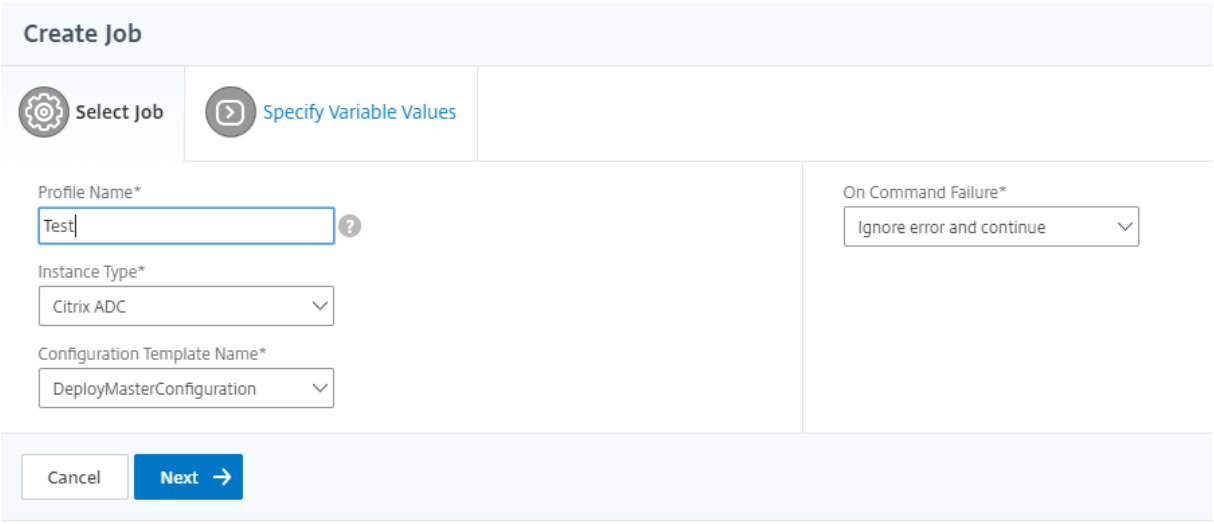
> **Hinweis**
>
> Sie können die Optionen **Ausgabe anfügen** und **Fehler anhängen** aktivieren, wenn Sie die Ausgabe und die Fehler speichern möchten, die bei der Ausführung eines Befehlsskripts in den NetScaler ADM -Serverprotokolldateien generiert wurden (falls vorhanden). Wenn Sie diese Optionen nicht aktivieren, verwirft NetScaler ADM alle Ausgaben und Fehler, die während der Ausführung des Befehlsskripts generiert wurden.

So legen Sie die `Execute` Job-Aktion fest

Durch die Erstellung eines Profils mit Konfigurationsaufträgen wird ein Job als integrierter Job oder als benutzerdefinierter Job für NetScaler- und NetScaler SDX-Instanzen für Ereignisse und Alarme ausgeführt, die den von Ihnen angegebenen Filterkriterien entsprechen.

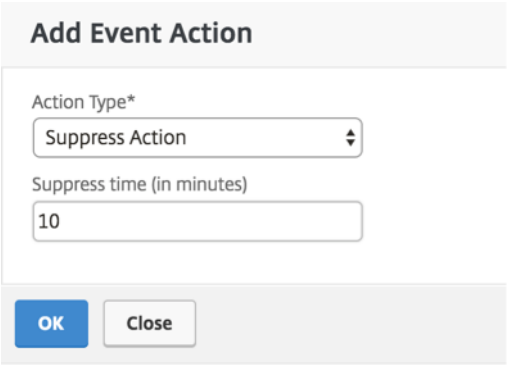
1. Klicken Sie unter **Ereignisregelaktionen**auf **Aktion hinzufügen** und wählen Sie aus der Dropdownliste ****Aktionstyp die Option Job-Aktion** ausführen** aus.
2. Erstellen Sie ein Profil mit einem Job, den Sie ausführen möchten, wenn die Ereignisse die definierten Filterkriterien erfüllen.
3. Geben 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 NetScaler ADM fest

Konfigurieren Sie den erforderlichen Slack-Channel, indem Sie den Profilnamen und die Webhook-URL in der NetScaler ADM GUI angeben. Die Ereignisbenachrichtigungen werden dann an diesen Kanal gesendet. Sie können mehrere Slack Kanäle konfigurieren, um diese Benachrichtigungen zu erhalten

1. Navigieren Sie in NetScaler ADM zu**Infrastruktur > 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 überwacht werden müssen.
3. Klicken Sie unter**Ereignisregelaktionen**auf**Aktion hinzufügen**. Wähle dann in der Liste**Aktionstyp**die Option**Slack-Benachrichtigungen senden** aus und wähle **Slack-Profilliste aus.**
4. Sie können auch eine Slack-Profilliste hinzufügen, indem Sie neben dem Feld **Slack-Profilliste** 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 NetScaler ADM konfiguriert werden soll.
    b) **Name des Kanals**. 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:**
>
> Du kannst die Slack-Profile auch hinzufügen, indem du zu **System** > **Benachrichtigungen** > **Slack-Profile**navigierst. Klicken Sie auf **Hinzufügen** und erstellen Sie das Profil wie im vorherigen Abschnitt beschrieben.

Du kannst den Status der von dir erstellten Slack-Profile anzeigen.

Ihre Ereignisregel wird jetzt mit geeigneten Filtern und gut definierten Ereignisregelaktionen erstellt.

So richten Sie PagerDuty-Benachrichtigungen von NetScaler ADM ein

Sie können in NetScaler 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 auf einer registrierten Nummer konfigurieren.

Bevor Sie ein PagerDuty-Profil in NetScaler ADM hinzufügen, stellen Sie sicher, dass Sie die erforderlichen Konfigurationen in PagerDuty abgeschlossen haben. Weitere Informationen finden Sie in der 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 NetScaler-Instanzen generiert werden.
- **Lizenzen** —Liste der Lizenzen, die derzeit aktiv sind, bald ablaufen usw.
- **SSL-Zertifikate** —Liste der SSL-Zertifikate, die NetScaler-Instanzen hinzugefügt werden.

Um ein PagerDuty-Profil in ADM hinzuzufügen:

1. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler ADM an.
2. Navigieren Sie zu **Einstellungen > Benachrichtigungen > PagerDuty-Profile**.
3. Klicken Sie auf **Hinzufügen**, um ein neues 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 erhalten.
   c) Klicken Sie auf **Erstellen**.

   Anwendungsfall:

   Stellen Sie sich ein Szenario vor, das Sie

   - möchten Benachrichtigungen an Ihr PagerDuty-Profil senden.
   - habe Telefonanruf als Option in PagerDuty konfiguriert, um Benachrichtigungen zu erhalten.
   - möchte Telefonanrufwarnungen für NetScaler-Ereignisse erhalten.

   Schrittfolge zum Konfigurieren:

   a) Navigiere zu **Ereignisse** > **Regeln**
   b) Konfigurieren Sie auf der Seite **Regel erstellen** alle anderen Parameter, um eine Regel zu erstellen.
   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**.

Sobald die Konfiguration abgeschlossen ist, erhalten Sie einen Anruf, wenn ein neues Ereignis für die NetScaler Instanz generiert wird. Aus dem Telefonanruf können Sie entscheiden:

- Bestätigen Sie das Ereignis
- Markiere es als gelöst
- Eskalieren Sie zu einem anderen Teammitglied

So generieren Sie ServiceNow-Vorfälle automatisch aus NetScaler ADM

Sie können ServiceNow-Vorfälle für NetScaler ADM-Ereignisse automatisch generieren, indem Sie das ServiceNow-Profil auf der NetScaler ADM-GUI auswählen. Sie müssen das ServiceNow-Profil in NetScaler ADM auswählen, um eine Ereignisregel zu konfigurieren.

Bevor Sie eine Ereignisregel zum automatischen Generieren von ServiceNow-Vorfällen konfigurieren, integrieren Sie NetScaler ADM in eine ServiceNow-Instanz. Weitere Informationen finden Sie unter Konfigurieren des ITSM-Adapters für ServiceNow.

Um eine Ereignisregel zu konfigurieren, navigieren Sie zu **Ereignisse** > **Regeln**.

1. Konfigurieren Sie auf der Seite **Regel erstellen** alle anderen Parameter, um eine Regel zu erstellen.
2. Klicken **Sie unter Regelaktionen erstellen**auf **Aktion hinzufügen**.

   Die Seite **“Ereignisaktion hinzufügen** ‘‘wird angezeigt.

   a) Wählen Sie unter **Aktionstyp**die Option **ServiceNow-Benachrichtigungen senden**aus.

   b) Wählen Sie **ServiceNow ServiceNow-Profil**das Profil **Citrix_Workspace_SN** aus der Liste aus.

   c) Klicken Sie auf **OK**.

Gemeldeten Schweregrad von Ereignissen auf NetScaler-Instanzen ändern

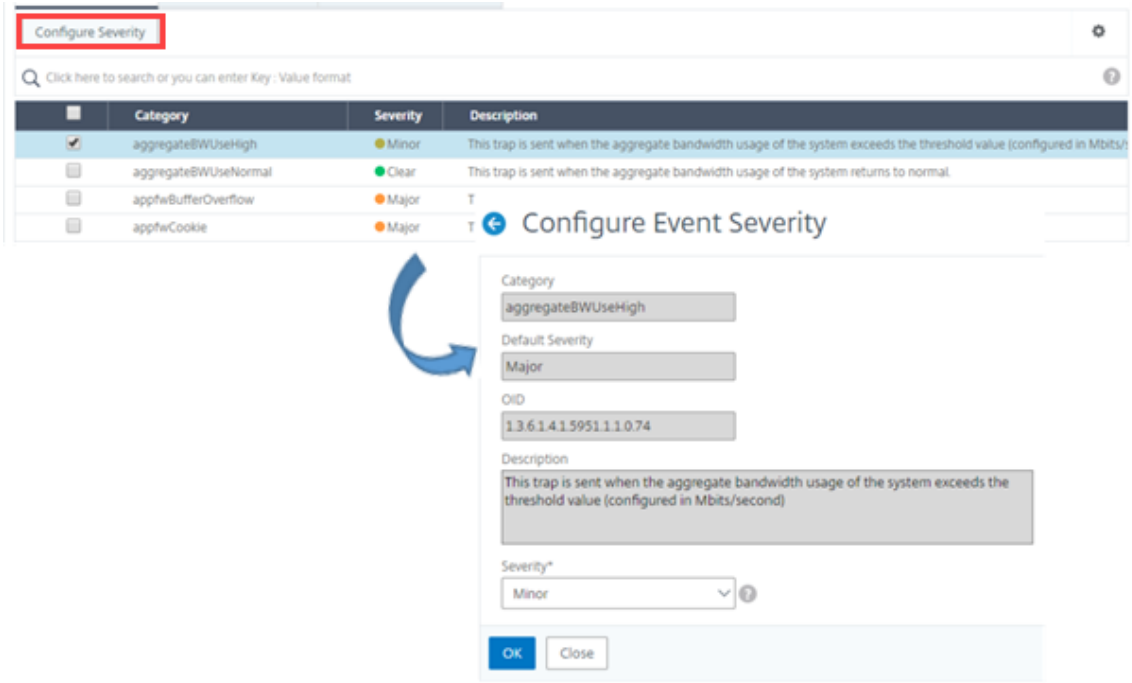
February 5, 2024

Sie können die Berichterstattung über Ereignisse verwalten, die auf all Ihren Geräten generiert wurden, sodass Sie Ereignisdetails zu einem bestimmten Ereignis in einer bestimmten Instanz einsehen und Berichte auf der Grundlage des Schweregrads des Ereignisses einsehen können. Sie können Ereignisregeln erstellen, die die Standardeinstellungen für den Schweregrad verwenden, und Sie können die Schweregradeinstellungen ändern. Sie können den Schweregrad für allgemeine und unternehmensspezifische Ereignisse konfigurieren.

Sie können die folgenden Schweregrade definieren: Kritisch, Groß, Minor, Warnung und Klar.

So ändern Sie den Schweregrad des Ereignisses:

1. Navigieren Sie zu **Infrastruktur > Ereignisse > Ereigniseinstellungen**.
2. Klicken Sie auf die Registerkarte für den Instanztyp von Citrix Application Delivery Controller (ADC), den Sie ändern möchten. Wählen Sie dann die Kategorie aus der Liste aus und klicken Sie auf **Schweregrad konfigurieren**.
3. Wählen **Sie unter Konfigurieren des Ereignisschweregrads**den Schweregrad aus der Drop-downliste aus.
4. Klicken Sie auf **OK**.

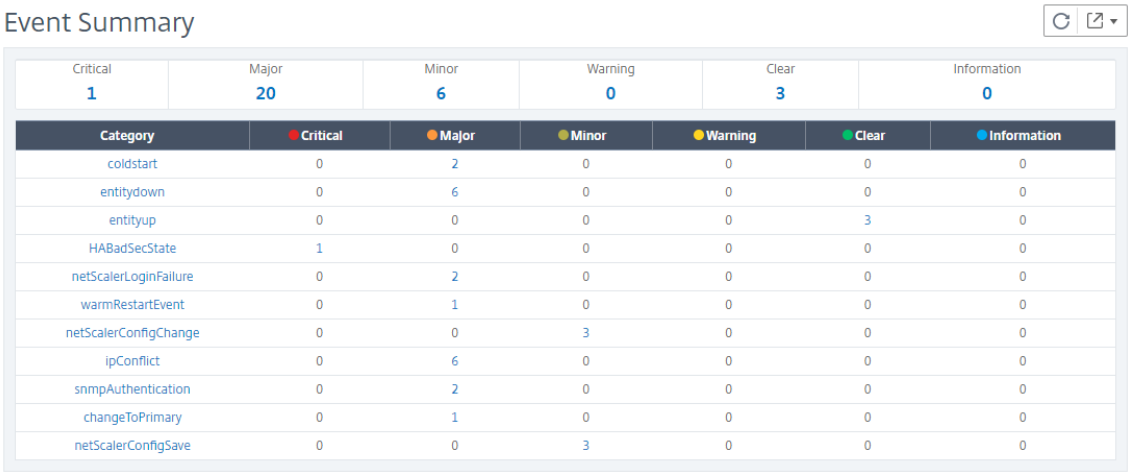


Zusammenfassung der Ereignisse anzeigen

February 5, 2024

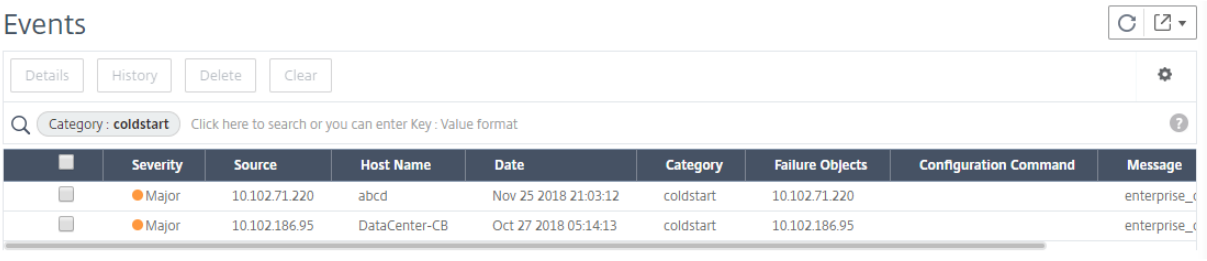
Sie können jetzt eine Seite mit der Zusammenfassung der Ereignisse aufrufen, um die auf Ihrem NetScaler Application Delivery Management (ADM) -Server empfangenen Ereignisse und Traps zu überwachen. Navigieren Sie zu **Infrastruktur > Ereignisse**. Auf der Seite Ereignisübersicht werden die folgenden Informationen in einem tabellarischen Format angezeigt:

- **Zusammenfassung aller Ereignisse, die NetScaler ADM erhalten hat**. Die Ereignisse sind nach Kategorien sortiert, und die verschiedenen Schweregrade werden in verschiedenen Spalten angezeigt: Kritisch, schwerwiegend, geringfügig, Warnung, Klar und Information. Ein kritisches Ereignis tritt beispielsweise auf, wenn eine Citrix Application Delivery Controller Instanz (ADC) ausfällt und keine Informationen an den NetScaler ADM -Server sendet. Während des Ereignisses wird eine Benachrichtigung an einen Administrator gesendet, in der der Grund erläutert wird, warum die Instanz ausgefallen ist, die Zeit, in der sie nicht verfügbar war, und so weiter. Das Ereignis wird dann auf der Seite “Ereignisübersicht”aufgezeichnet, auf der Sie eine Zusammenfassung anzeigen und auf die Details des Ereignisses zugreifen können.



- **Anzahl der empfangenen Traps für jede Kategorie**. Die Anzahl der empfangenen Traps, kategorisiert nach Schweregrad. Standardmäßig hat jeder Trap, der von NetScaler-Instanzen an NetScaler ADM gesendet wird, einen zugewiesenen Schweregrad, aber als Netzwerkadministrator können Sie den Schweregrad in der NetScaler ADM GUI angeben.

Wenn Sie auf einen Kategorietyp oder einen Trap 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 der Hostname der NetScaler Instanz, das Datum, an dem das Trap empfangen wurde, die Kategorie, Fehlerobjekte, die Ausführung des Konfigurationsbefehls und die Meldung.



Ereignisschweregrade und SNMP-Trap-Details anzeigen

February 5, 2024

Wenn Sie ein Ereignis und seine Einstellungen in NetScaler Application Delivery Management (ADM) erstellen, können Sie das Ereignis sofort auf der Seite mit der Ereigniszusammenfassung anzeigen. Ebenso können Sie den Zustand, die Verfügbarkeit, die Modelle und die Versionen aller Citrix Application Delivery Controller (ADC) -Instanzen, die Ihrem NetScaler ADM-Server hinzugefügt wurden, im Infrastruktur-Dashboard bis ins kleinste Detail 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 NetScaler-Instanzen einfacher anzeigen und überwachen können.

Beispielsweise können Ereignisse mit einem **kritischen** Schweregrad selten auftreten. Wenn diese kritischen Ereignisse jedoch in Ihrem Netzwerk auftreten, sollten Sie möglicherweise weiter untersuchen, Fehler 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.

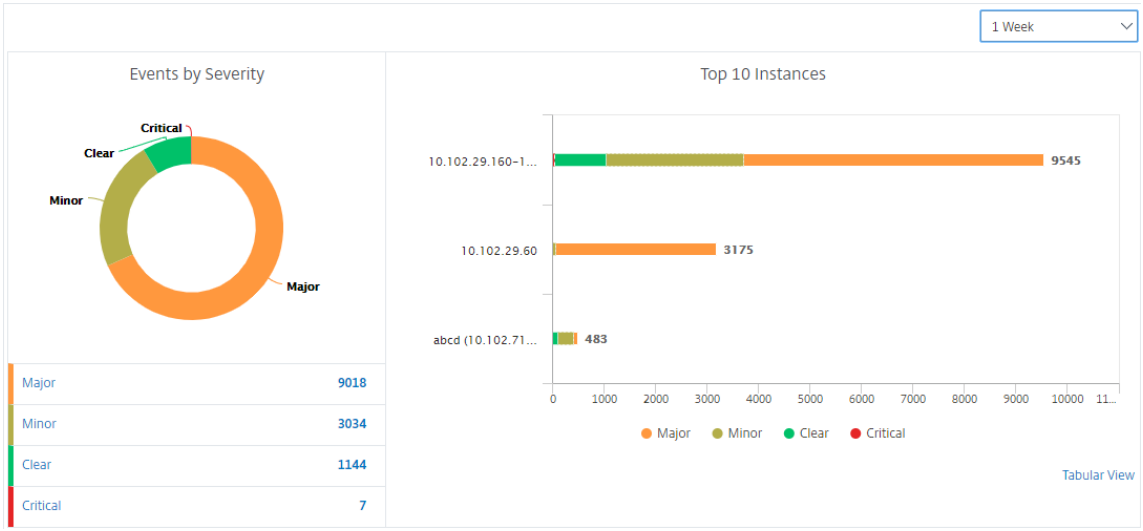
Ebenso können Sie den Zustand einer NetScaler VPX-Instanz im Dashboard einsehen. Sie können die Zeit maskieren, in der die Instanz gestartet und ausgeführt wurde, und nur die Zeiten anzeigen, in denen die Instanz außer Betrieb war. Wenn Sie auf das Diagramm klicken, gelangen Sie zur Seite dieser Instanz, auf der *der Out-Of-Service-Filter* bereits angewendet wurde, und sehen Sie Details wie Hostname, die Anzahl der HTTP-Anforderungen, die pro Sekunde empfangen wurden, die CPU-Auslastung usw. Sie können auch die Instanz auswählen und das Dashboard der jeweiligen Citrix Instanz für weitere Details einsehen.

So wählen Sie bestimmte Ereignisse nach Schweregrad in NetScaler ADM aus:

1. Melden Sie sich mit Ihren Administratoranmeldeinformationen bei NetScaler ADM an.
2. Navigieren Sie zu **Infrastruktur > Dashboard**.

   Oder

   Navigieren Sie zu **Infrastruktur > Ereignisse > Berichte**.
3. Wählen Sie im Menü in der oberen rechten Ecke der Seite die Dauer aus, für die Ereignisse nach Schweregrad angezeigt werden sollen.

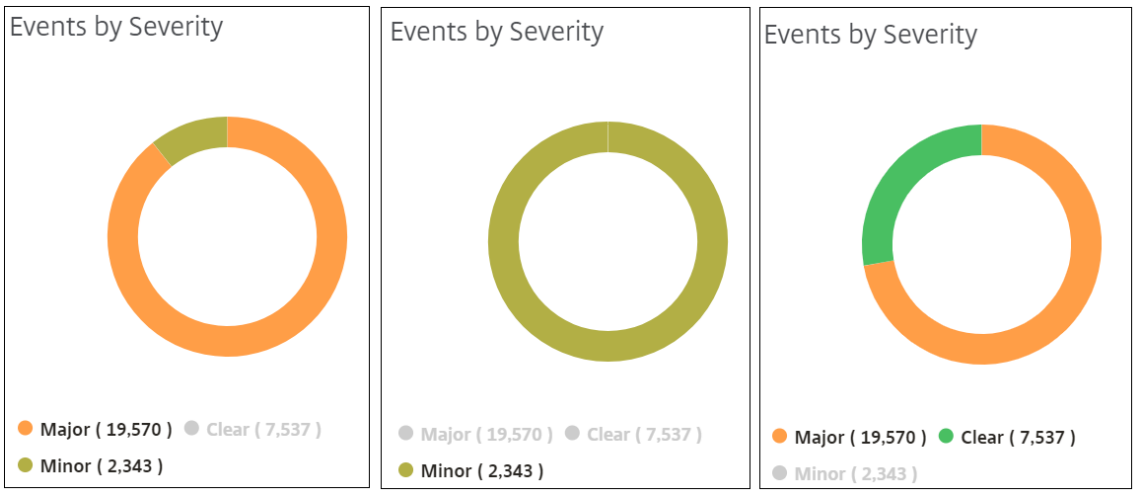


4. Das Donutdiagramm **Ereignisse nach Schweregrad**zeigt eine visuelle Darstellung aller Ereignisse nach ihrem Schweregrad an. Verschiedene Arten von Ereignissen werden als unterschiedliche farbige Abschnitte dargestellt, und die Länge jedes Abschnitts entspricht der Gesamtzahl der Ereignisse dieser Art von Schweregrad.
5. Sie können auf jeden Abschnitt des Donut-Diagramms klicken, um die entsprechende Seite mit dem **Schweregrad basierenden Ereignissen** anzuzeigen, auf der die folgenden Details für den ausgewählten Schweregrad für die ausgewählte Dauer angezeigt werden:

   - Instanz-Quelle
   - Daten des Ereignisses
   - Kategorie der Ereignisse, die von der NetScaler-Instanz generiert werden
   - Nachrichtenbenachrichtigung gesendet

   > **Hinweis**
   >
   > Unterhalb des Donut-Diagramms sehen Sie eine Liste der Schweren, die im Diagramm dargestellt sind. Standardmäßig werden in einem Donutdiagramm alle Ereignisse aller Schweregradtypen angezeigt. Daher werden alle Schweregradtypen in der Liste hervorgehoben. Sie können die Schweregrade umschalten, um den gewählten Schweregrad ein-

facher anzuzeigen und zu überwachen.



So zeigen Sie NetScaler SNMP-Trapdetails auf NetScaler ADM an:

Sie können nun die Details der einzelnen SNMP-Traps anzeigen, die von den verwalteten NetScaler Instanzen auf dem NetScaler ADM-Server auf der Seite **Ereigniseinstellungen** empfangen wurden. Navigieren Sie zu **Infrastruktur > 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 mit dem Ereignis verbundenen Nachrichten an.

Beispielsweise wird bei einem Ereignis mit der Trap-Kategorie **monRespTimeoutBelowThresh** die Beschreibung des Traps wie folgt angezeigt: “Dieser Trap wird gesendet, wenn das Antwort-Timeout für eine Monitorprobe wieder normal ist und unter dem eingestellten Schwellenwert liegt.”

Anzeigen und Exportieren von NetScaler Syslog-Nachrichten

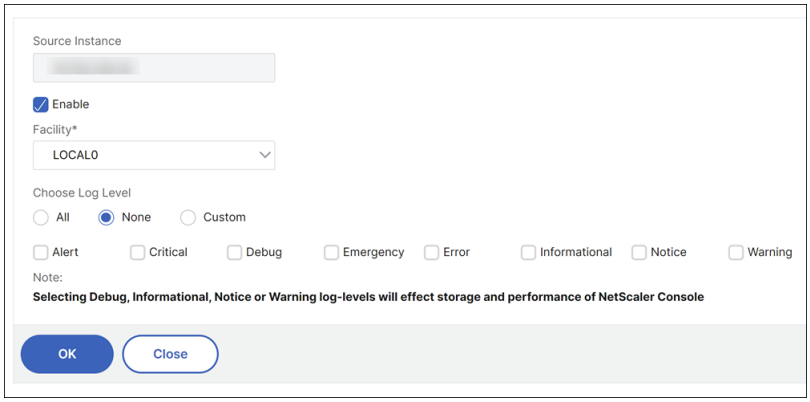
February 5, 2024

Über Ihre ADM-Software können Sie die Syslog-Ereignisse überwachen, die auf Ihren Citrix Application Delivery Controller (ADC) -Instanzen generiert werden. Dazu müssen Sie ADM als Syslog-Server für Ihre NetScaler-Instanzen konfigurieren. Nachdem Sie ADM konfiguriert haben, werden alle Syslog-Nachrichten von den ADC-Instanzen zu ADM umgeleitet.

Konfigurieren von ADM als Syslog-Server

Gehen Sie folgendermaßen vor, um ADM als Syslog-Server zu konfigurieren:

1. Navigieren Sie in der ADM-GUI zu **Infrastruktur > Instanzen**.
2. Wählen Sie die NetScaler-Instanz aus, aus der die Syslog-Nachrichten gesammelt und in NetScaler 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 Einrichtung auf lokaler Ebene oder auf Benutzerebene aus.
6. Wählen Sie die erforderliche Protokollebene für die Syslog-Meldungen aus.
7. Klicken Sie auf **OK**.

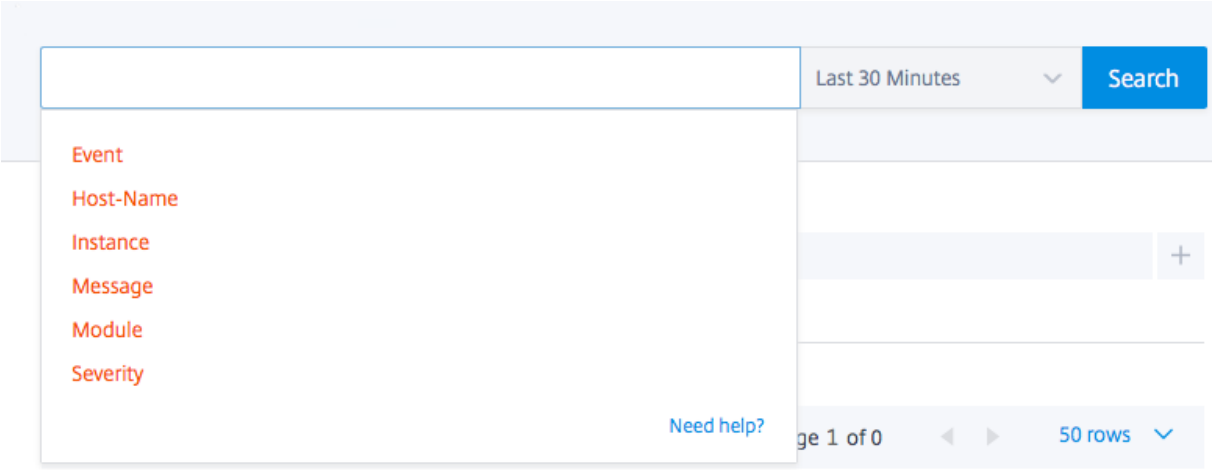


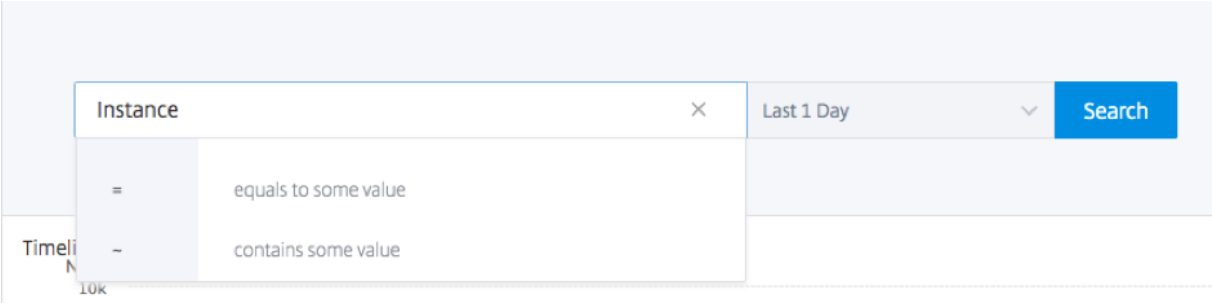
Mit diesen Schritten werden alle Syslog-Befehle in der NetScaler-Instanz konfiguriert, und NetScaler ADM beginnt mit dem Empfang der Syslog-Nachrichten.

Anzeigen und Durchsuchen von Syslog-Nachrichten

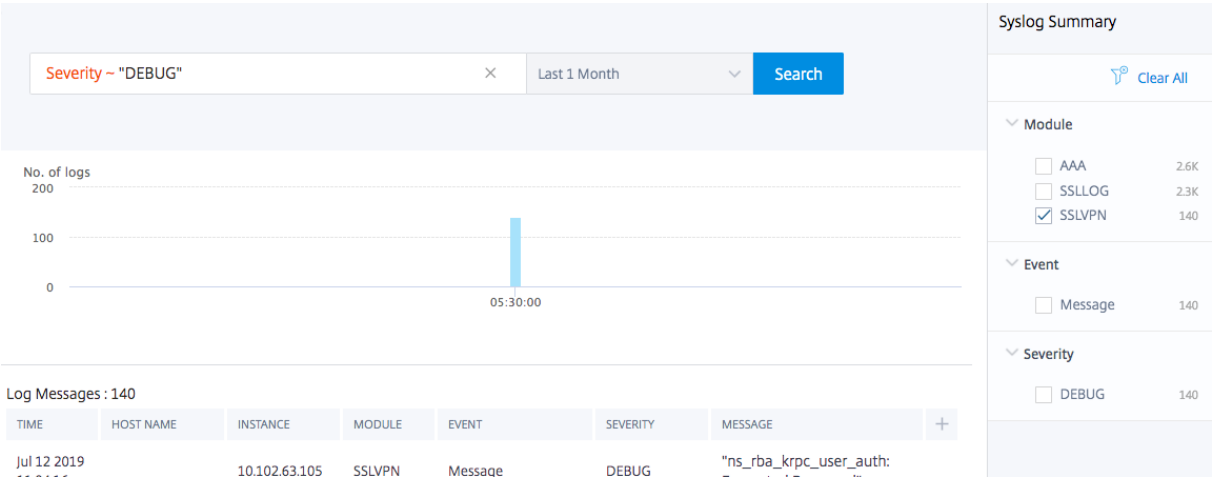
Sie können alle Syslog-Nachrichten anzeigen, die auf Ihren verwalteten NetScaler-Instanzen generiert wurden. Die Syslog-Meldungen werden zentral in der Datenbank gespeichert und sind zu Überwachungszwecken unter **Infrastruktur > Ereignisse > Syslog-Meldungen** verfügbar. Sie können diese Protokollierungsinformationen kombinieren und Berichte für Analysen aus den gesammelten Daten ableiten.

Darüber hinaus können Sie mithilfe von Filtern die Suchergebnisse von Syslog-Nachrichten eingrenzen und genau das finden, wonach Sie suchen, und zwar in Echtzeit. Klicken Sie auf **Hilfe?**, um die integrierte Suchhilfe zu öffnen.





Fügen Sie als Nächstes den Suchbegriff hinzu. Für einige Kategorien wird eine vorausgefüllte 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 Ihre Suche weiter eingrenzen, indem Sie Optionen im Bereich **Syslog Summary** auswählen.

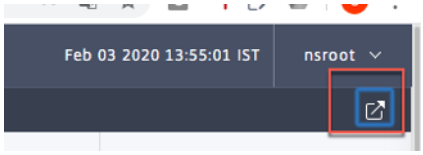


Exportieren und planen Sie Syslog-Nachrichten

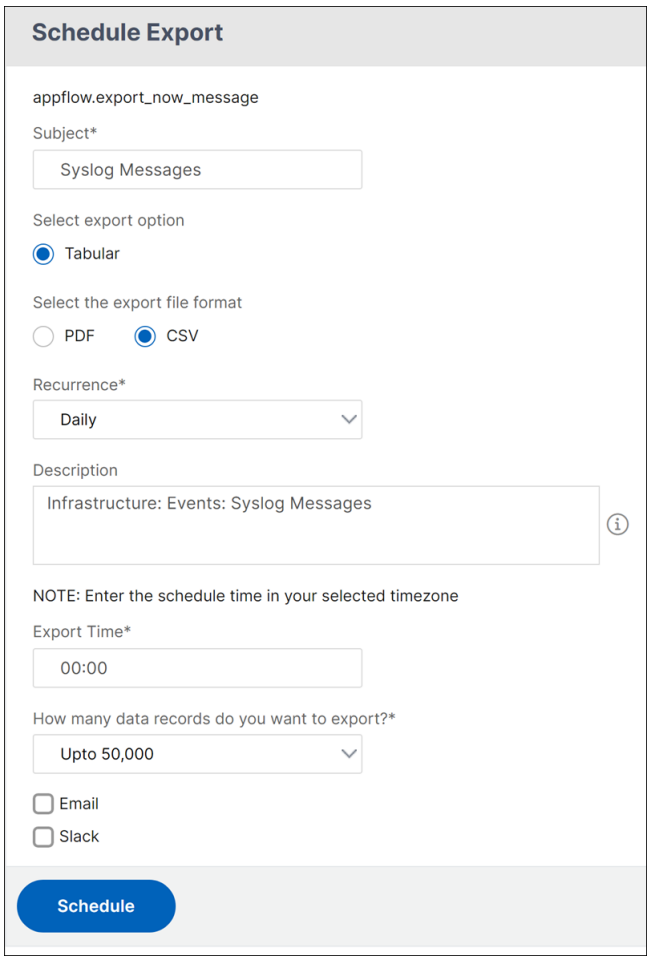
Sie können Syslog-Nachrichten anzeigen, ohne sich bei ADM anzumelden, indem Sie einen Export aller auf dem Server empfangenen Syslog-Nachrichten planen. Sie können Syslog-Nachrichten ex-

portieren, die auf Ihren ADC-Instanzen in PDF-, CSV-, PNG- und JPEG-Formaten generiert werden. Du kannst den Export dieser Berichte in bestimmte E-Mail-Adressen oder Slack-Konten in verschiedenen Intervallen planen.

Um die Protokollmeldungen zu exportieren und zu planen, klicken Sie auf das Pfeilsymbol in der oberen rechten Ecke.



- Um die Protokollmeldungen zu exportieren, klicken Sie auf **Exportieren > Jetzt exportieren**, wählen Sie das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.
- Um den Export von Syslog-Nachrichten zu planen, klicken Sie auf **Exportieren Berichte > Bericht planen**und legen Sie die erforderlichen Parameter fest. Du kannst den Bericht per E-Mail oder Slack erhalten.



Syslog-Nachrichten unterdrücken

February 5, 2024

Bei der Konfiguration als Syslog-Server empfängt NetScaler Application Delivery Management (ADM) alle Syslog-Nachrichten, die von den konfigurierten Citrix Application Delivery Controller (ADC) -Instanzen an ihn gesendet werden. Möglicherweise gibt es eine große Anzahl von Nachrichten, die Sie möglicherweise nicht sehen möchten. Beispielsweise sind Sie möglicherweise nicht daran interessiert, alle Meldungen auf Informationsebene zu sehen. Sie können nun einige Syslog-Nachrichten verwerfen, die Sie nicht interessieren. Sie können einige der Syslog-Meldungen, die in NetScaler ADM eingehen, unterdrücken, indem Sie einige Filter einrichten. NetScaler ADM löscht alle Nachrichten, die den Kriterien entsprechen. Diese gelöschten Nachrichten werden nicht auf der NetScaler ADM GUI angezeigt, und diese Nachrichten werden auch nicht in der NetScaler ADM-Datenbank des Kunden gespeichert.

Sie können einige der protokollierten Syslog-Meldungen, die in NetScaler ADM eingehen, 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 NetScaler-Instanz oder mehreren Instanzen stammen. Sie können auch ein Textmuster für NetScaler ADM bereitstellen, um Nachrichten zu suchen und zu unterdrücken. NetScaler ADM löscht alle Nachrichten, die den Kriterien entsprechen. Diese gelöschten Nachrichten werden nicht auf der NetScaler ADM GUI angezeigt, und diese Nachrichten werden auch nicht in der Kundendatenbank gespeichert. Daher wird eine gute Menge an Speicherplatz auf dem Speicherserver gespart.

Einige Anwendungsfälle für die Unterdrückung von Syslog-Meldungen lauten wie folgt:

- Wenn Sie alle Meldungen auf Informationsebene ignorieren möchten, unterdrücken Sie Level 6 (informativ)
- Wenn Sie nur Firewall-Fehlerbedingungen aufzeichnen möchten, unterdrücken Sie alle Ebenen außer Stufe 3 (Fehler)

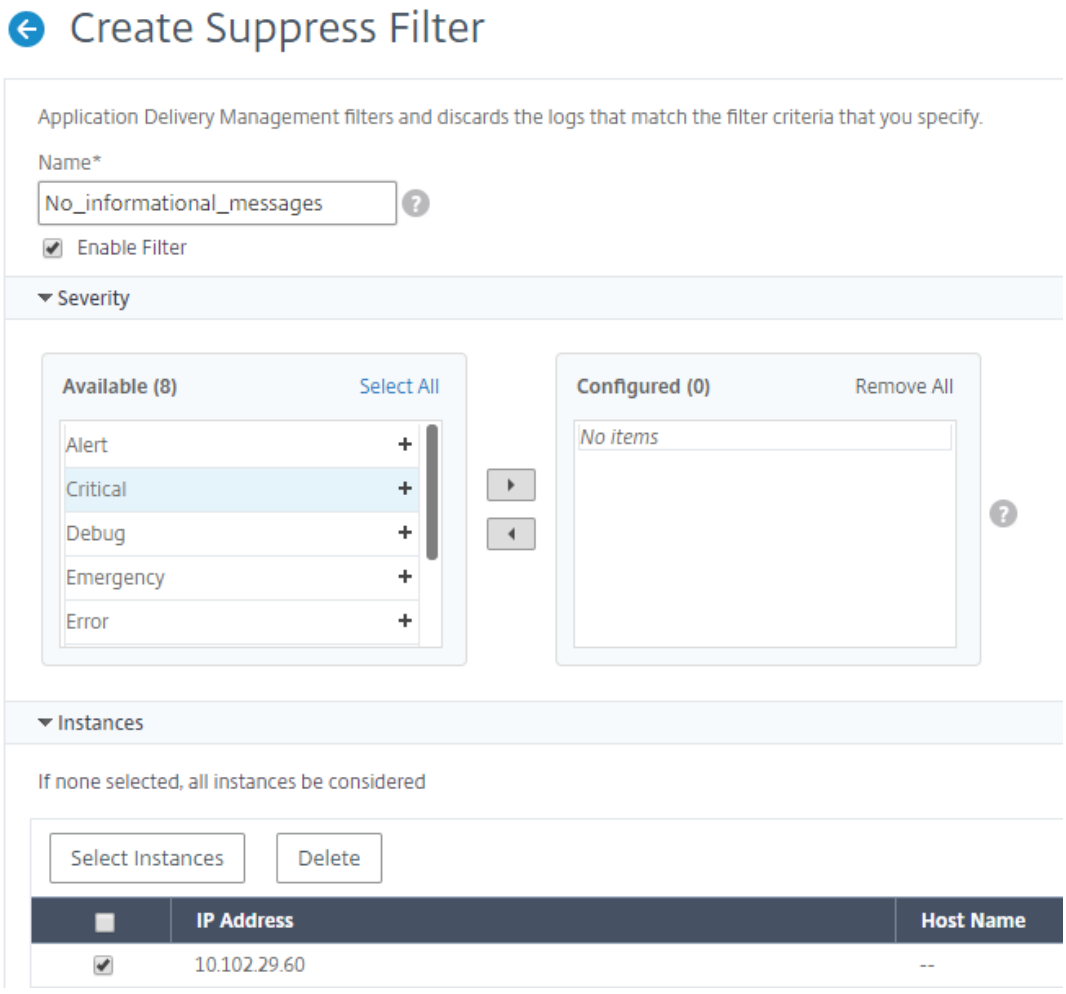
Unterdrücken von Syslog-Nachrichten durch Erstellen von Filtern

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Ereignisse > Syslog-Meldungen** > **Filter unterdrücken**.
2. 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 NetScaler-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 Protokollebenen aus, für die Sie die Meldungen unterdrücken müssen, und fügen Sie Wenn Sie beispielsweise keine eingehenden Informationsmeldungen anzeigen möchten, können Sie Informativ auswählen, um diese Meldungen zu unterdrücken.

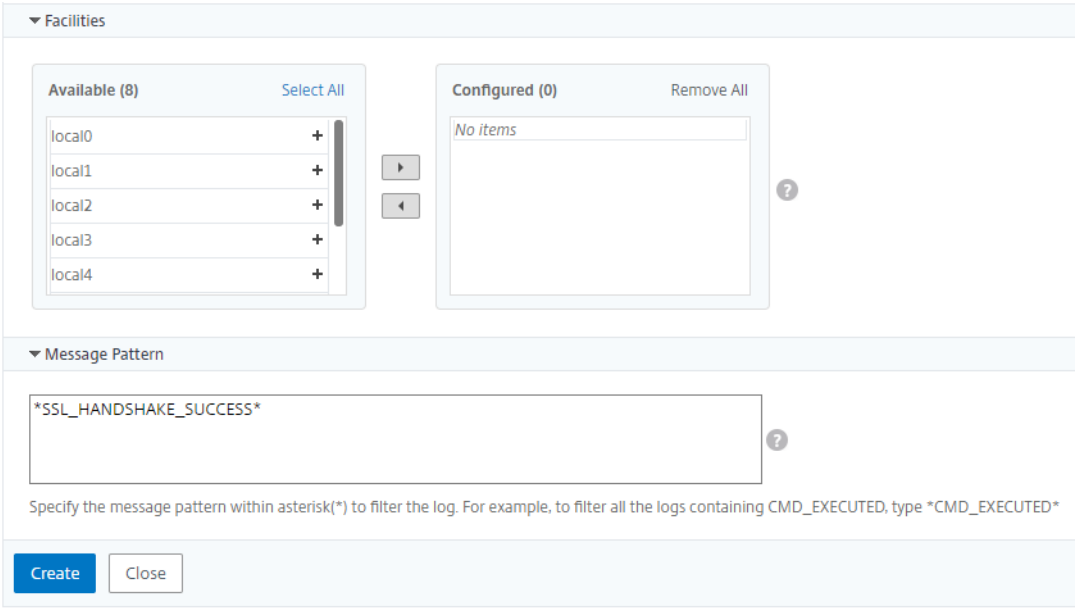
c) **Instanzen** - Wählen Sie die NetScaler-Instanzen aus, für die die Syslog-Meldungen konfiguriert wurden.



d) **Einrichtungen** - Wählen Sie die Einrichtung aus, um Nachrichten auf der Grundlage der Quelle zu unterdrücken, die sie generiert.

e) **Nachrichtenmuster** —Sie können auch ein Textmuster eingeben, das von einem

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 NetScaler ADM angezeigt werden können, müssen Sie den Filter deaktivieren.

1. Navigieren Sie zu **Infrastruktur > Ereignisse > Syslog-Meldungen** > **Filter unterdrücken**, und wählen Sie auf der Seite **Filter unterdrücken** den Filter aus, und klicken Sie auf **Bearbeiten**.
2. **Deaktivieren Sie auf der Seite Filter unterdrücken** das Kontrollkästchen **Filter aktivieren**, um den Filter zu deaktivieren.

Löscheinstellungen für Instanzereignisse konfigurieren

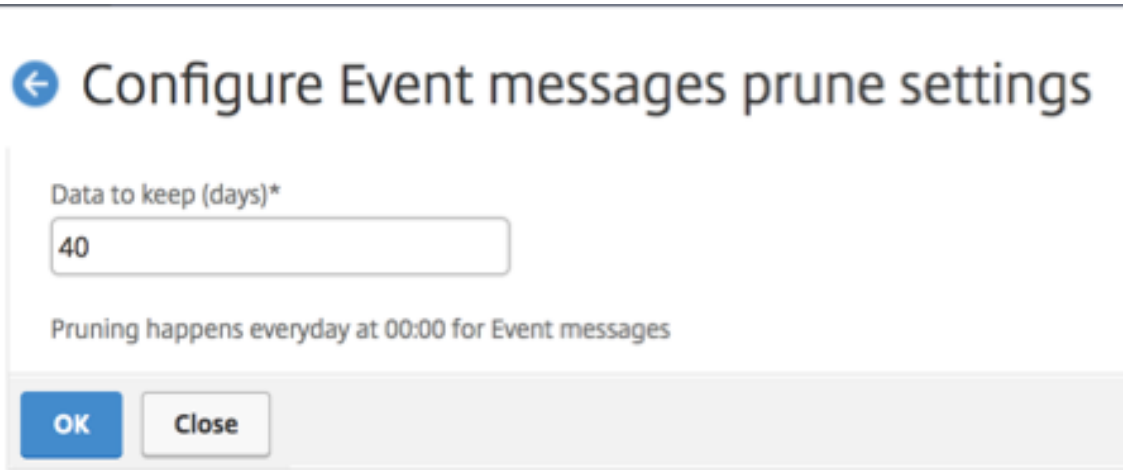
February 5, 2024

Citrix Application Delivery Controller (ADC) -Instanzen, die von Ihrem NetScaler Application Delivery Management (ADM) -Server verwaltet werden, senden kontinuierlich Ereignismeldungsdaten, die auf NetScaler ADM gespeichert werden. Sie können das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle beibehalten soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00.00 Uhr) bereinigt.

> **Hinweis**
>
> Der Wert, den Sie angeben können, darf 40 Tage nicht überschreiten oder weniger als 1 Tag betragen.

So konfigurieren Sie Prune-Einstellungen für Instanzereignisse:

1. Navigieren Sie zu **System** > **Systemadministration**.
2. Klicken Sie unter**Prune-Einstellungen**auf**Instanzereignisse Prune-Einstellungen**.
3. Geben Sie das Zeitintervall in Tagen ein, für das Sie Daten auf dem NetScaler ADM -Server beibehalten möchten, und klicken Sie auf**OK**.



Netzwerkfunktionen

February 5, 2024

Mit der Funktion Netzwerkfunktionen können Sie den Status der Entitäten überwachen, die auf Ihren verwalteten Citrix Application Delivery Controller (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”bietet Ihnen die folgenden Grafiken:

- Top 5 virtuelle Server mit den höchsten Client-Verbindungen
- Top 5 virtuelle Server mit den höchsten Serververbindungen
- Top 5 virtuelle Server mit maximalem Durchsatz (MB/s)

- Unterste 5 virtuelle Server mit niedrigstem Durchsatz (MB/s)
- Top 5 Instanzen mit den meisten virtuellen Servern
- Status der virtuellen Server
- Integrität der virtuellen Lastausgleichsserver
- Protokolle

Berichte für Lastausgleichseinheiten generieren

February 5, 2024

Mit NetScaler Application Delivery Management (ADM) können Sie die Berichte der Citrix Application Delivery Controller (ADC) -Instanzentitäten auf allen Ebenen anzeigen. Es gibt zwei Arten von Berichten, die Sie unter NetScaler ADM > Network Functions herunterladen können: konsolidierte Berichte und einzelne Berichte.

Konsolidierte Berichte: Sie können einen konsolidierten oder zusammenfassenden Bericht für alle Entitäten herunterladen und anzeigen, die auf NetScaler-Instanzen verwaltet werden.

Mit diesem Bericht erhalten Sie einen Überblick über die Zuordnung zwischen den NetScaler-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.

NetScaler IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca3			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing				

Der konsolidierte Bericht hat ein CSV-Format. Die Einträge in jeder Spalte werden wie folgt beschrieben:

- **NetScaler IP-Adresse**: IP-Adresse der NetScaler-Instanz wird im Bericht angezeigt
- **NetScaler HostName**: Der Hostname wird im Bericht angezeigt.
- **Partition**: Die IP-Adresse der administrativen Partition wird angezeigt
- **Virtueller Server**: <name_of_the_virtual_server>#virtual_IP_address :port_number

- **Dienste**: <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_Address:Port

> **Hinweis**
>
> - Wenn kein Hostname verfügbar ist, wird die entsprechende IP-Adresse angezeigt.
> - Leere Spalten geben an, dass die entsprechenden Entitäten für diese NetScaler-Instanz nicht konfiguriert sind.

Einzelberichte: Sie können auch unabhängige Berichte aller Instanzen und Entitäten herunterladen und anzeigen. Sie können beispielsweise einen Bericht nur für virtuelle Lastausgleichsserver oder Lastausgleichsdienste oder Lastausgleichsdienstgruppen herunterladen.

Mit NetScaler ADM können Sie den Bericht sofort herunterladen. Sie können den Bericht auch so planen, dass er einmal täglich, einmal pro Woche oder einmal pro Monat zu einem festen Zeitpunkt erstellt wird.

Erstellen eines kombinierten Lastausgleichsberichts

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Netzwerkfunktionen > Load Balancing.**
2. Klicken Sie auf der Seite **Load Balancing**  .
3. Auf der sich öffnenden Seite **Exportieren** haben Sie zwei Optionen, um den Bericht anzuzeigen:
   a) Wählen Sie die Registerkarte **Jetzt exportieren** und klicken Sie auf **OK**.

      Der konsolidierte Bericht wird auf Ihr System heruntergeladen.

   b) Wählen Sie die Registerkarte **Bericht planen**, um das Generieren und Exportieren des Berichts in regelmäßigen Abständen zu planen. 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 im Drop-down-Listenfeld die Option **Täglich**, **Wöchentlich**oder **Monatlich** aus.

      ii. **Wiederholungszeit** —Geben Sie die Zeit als Stunde:Minute im 24-Stunden-Format ein.

      iii. **E-Mail-Profil** - Wählen Sie ein Profil aus dem Dropdownlistenfeld aus, oder klicken Sie auf **+**, um ein E-Mail-Profil zu erstellen.

> **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 alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Erstellen eines individuellen Lastausgleichsentitätsberichts

Sie können einen individuellen 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 NetScaler ADM zu **Infrastruktur > Netzwerkfunktionen > Load Balancing > Services.**
2. Klicken Sie auf der Seite **Dienste** oben rechts auf die Schaltfläche **Exportieren**.
   a) Wählen Sie die Registerkarte **Jetzt exportieren**, wenn Sie den Bericht in diesem Moment generieren und anzeigen möchten.
   b) Wählen Sie **Export planen**, um die Generierung und den Export des Berichts in regelmäßigen Abständen zu planen.

> **Hinweis**
>
> Sie können die Berichte nur herunterladen oder als E-Mail-Anhänge exportieren. Sie können die Berichte auf der NetScaler ADM GUI nicht anzeigen.

Netzwerkfunktionenberichte exportieren oder planen

February 5, 2024

In NetScaler Application Delivery Management (ADM) können Sie einen umfassenden Bericht für ausgewählte Netzwerkfunktionen wie Load Balancing, Content Switching, Cache-Umleitung, Global Server Load Balancing (GSLB), Authentifizierung und NetScaler Gateway erstellen. Dieser Bericht ermöglicht Ihnen einen allgemeinen Überblick über die Zuordnung zwischen den NetScaler-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
- Daten partitionieren
- Name des virtuellen Servers
- Typ des virtuellen Servers
- Virtueller Server
- Virtueller LB-Zielserver

> **Hinweis**
>
> Für virtuelle Server mit Content Switching und Cache-Umleitung werden in der Spalte Virtueller Ziel-LB-Server alle LB-Server aufgeführt, d. h. sowohl Standardserver als auch richtlinienbasierte Server.
>
> - Name des Dienstes
> - Name der Dienstgruppe

Sie können planen, diese Berichte in unterschiedlichen Intervallen an bestimmte E-Mail-Adressen zu exportieren.

> **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 in NetScaler ADM keine

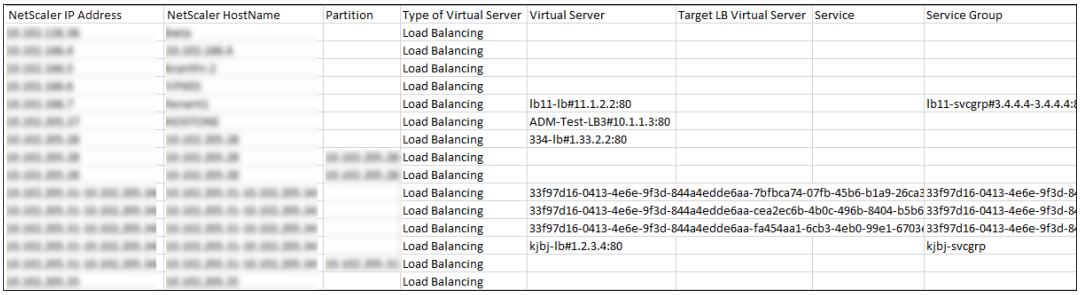
> separate Liste virtueller SSL-Server verwaltet wird.
> - Wenn ein neuer Bericht generiert wird, werden die älteren Berichte automatisch aus Ihrem Konto gelöscht.
> - Sie können keinen Netzwerkfunktionsbericht für HAProxy generieren.

So exportieren und planen Sie Berichte über Netzwerkfunktionen:

1. Navigieren Sie zu **Infrastruktur > Netzwerkfunktionen**.
2. Klicken Sie auf der Seite**Netzwerkfunktionen** im rechten Bereich oben rechts auf der Seite auf**Bericht generieren**.
3. Auf der Seite **Bericht generieren** haben Sie die folgenden 2 Optionen:

   a) Wählen Sie die Registerkarte **Jetzt exportieren** und klicken Sie auf **OK**. Der Bericht wird auf Ihr System heruntergeladen.

   Die folgende Abbildung zeigt ein Beispiel für einen Bericht über Netzwerkfunktionen.



NetScaler IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca3			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing				

   b) Wählen Sie die Registerkarte**Bericht planen**, um den Bericht in regelmäßigen Abständen zu generieren und zu exportieren. 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 im Dropdownlistenfeld**Täglich**,**Wöchentlich**oder**Monatlich**aus.

      ii. **Wiederholzeit**- Geben Sie die Zeit als Stunde: Minute im 24-Stunden-Format ein.

      iii. **E-Mail-Profil**—Wählen Sie ein Profil aus dem Drop-down-Listenfeld aus, oder klicken Sie auf**+**, 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.

Netzwerkberichterstellung

February 5, 2024

Sie können die Ressourcennutzung optimieren, indem Sie Ihre Netzwerkberichte auf NetScaler Application Delivery Management (NetScaler 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 (NetScaler) -Instanzen bereitgestellt, um den Datenverkehr auszugleichen, Inhalte zu wechseln oder 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.

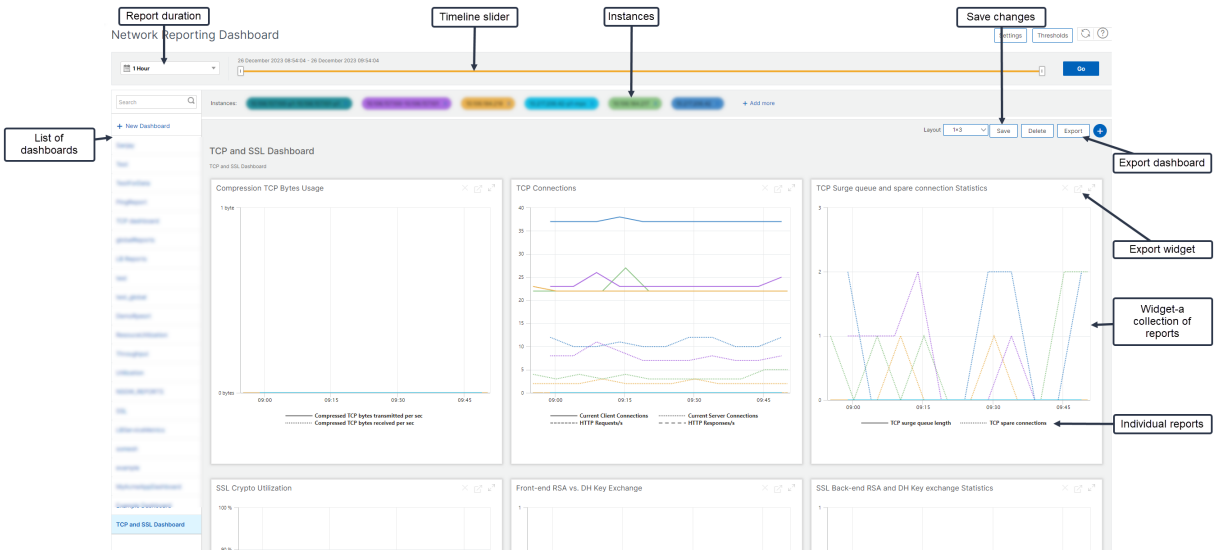
Mit NetScaler ADM können Sie jetzt Berichte nicht nur für Instanzen auf globaler Ebene erstellen, sondern auch für Entitäten wie virtuelle Server und Netzwerkschnittstellen. Die Instanzfamilie umfasst NetScaler-Instanzen. Die virtuellen Server, für die Sie Berichte erstellen können, sind wie folgt:

- Load Balancing-Server, Dienste und Dienstgruppen
- Content Switching-Server
- Cache-Umleitungsserver
- Globaler Service Load Balancing (GSLB)
- Authentifizierung
- NetScaler Gateway

Das Netzwerkberichts-Dashboard in NetScaler ADM ist hochgradig anpassbar. Sie können jetzt mehrere Dashboards für verschiedene Instanzen, virtuelle Server und andere Entitäten erstellen.

Netzwerkberichterstattungs-Dashboard

Das folgende Bild ruft die verschiedenen Funktionen im Dashboard auf:

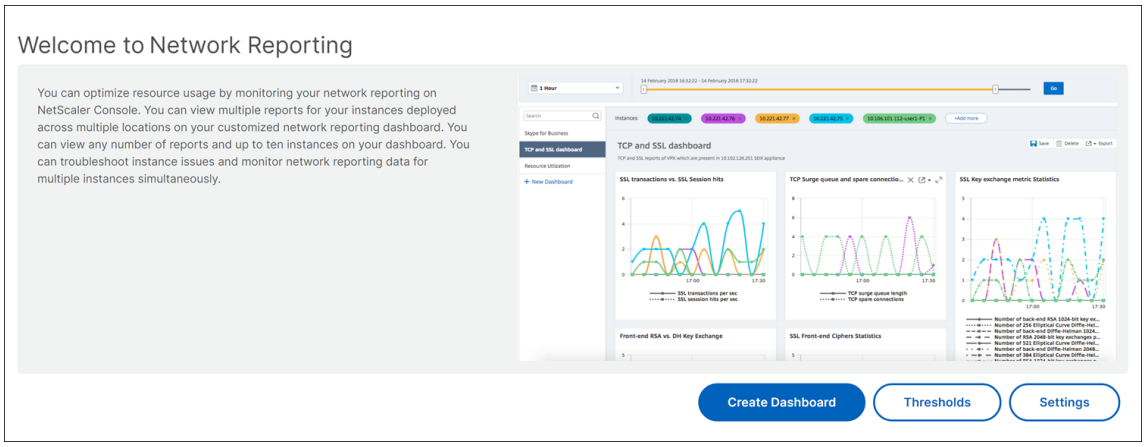


- Im linken Bereich werden alle benutzerdefinierten Dashboards aufgelistet, die in NetScaler ADM erstellt werden. Sie können auf einen von ihnen klicken, um die verschiedenen Berichte anzuzeigen, aus denen das Dashboard besteht. Beispielsweise enthält ein TCP- und SSL-Dashboard verschiedene Berichte, 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 komprimierter TCP-Byte-Nutzungsbericht Berichte für komprimierte TCP-Bytes, die pro Sekunde übertragen und empfangen wurden.
- Sie können Berichte für eine Stunde, einen Tag, eine Woche oder für einen Monat anzeigen. Darüber hinaus können Sie jetzt den Timeline-Schieberegler verwenden, um die Dauer der Berichte anzupassen, die auf dem NetScaler 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 der Erstellung des Berichts planen. Sie können auch eine E-Mail-Verteilerliste konfigurieren, an die die Berichte gesendet werden müssen.
- 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 NetScaler 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.

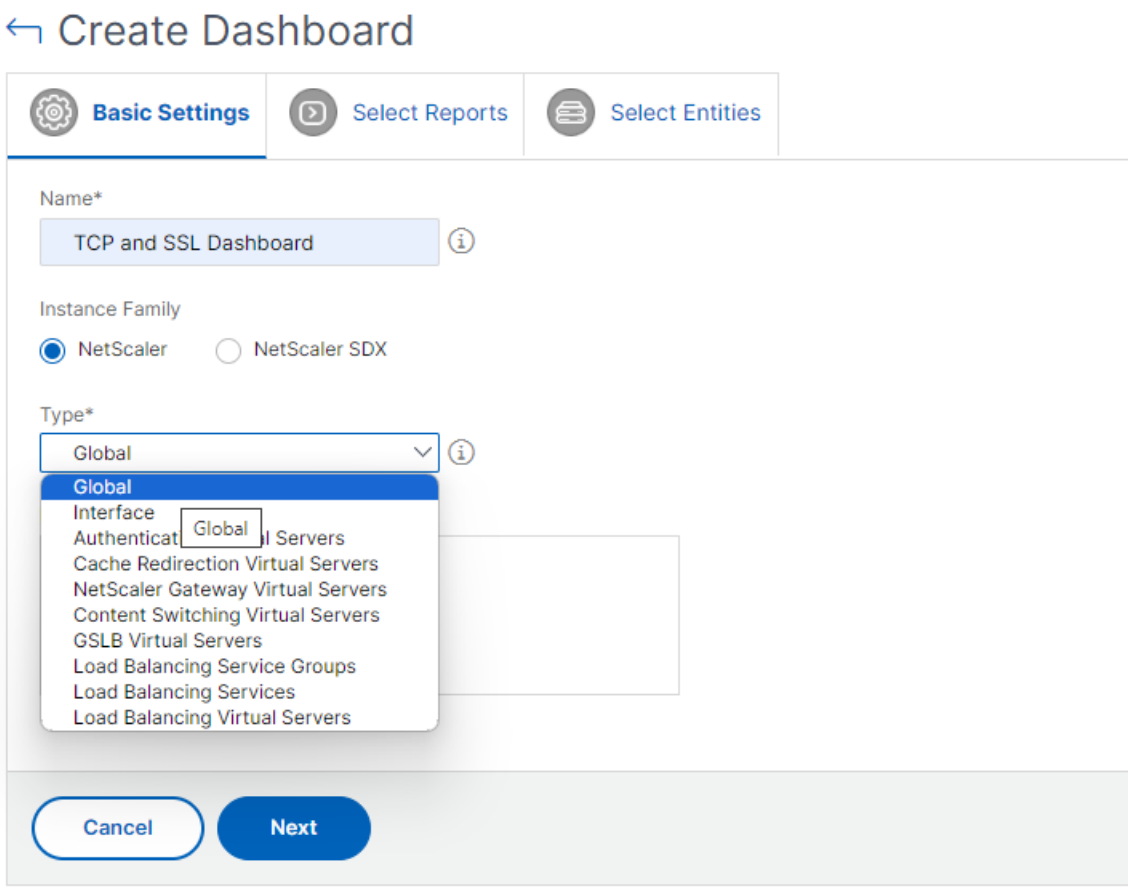
Im folgenden Abschnitt werden ausführlich die Aufgaben zum Erstellen eines Dashboards, zum Generieren von Berichten und zum Exportieren von Berichten erläutert.

So zeigen Sie ein Dashboard an oder erstellen Sie es:

1. Navigieren Sie in NetScaler ADM zu **Infrastructure > Network Reporting**.

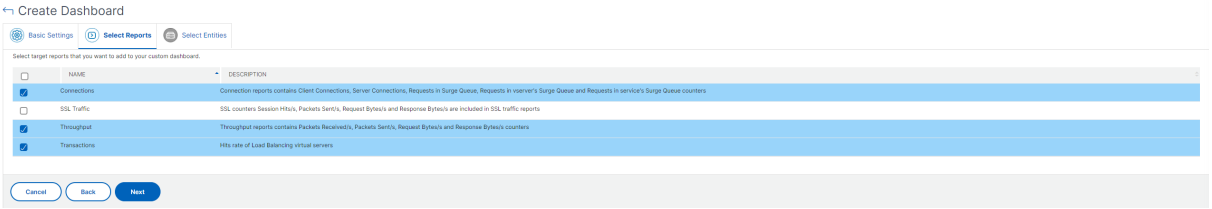


2. Klicken Sie auf Dashboard anzeigen, um die vorhandenen **Dashboards anzuzeigen**. Die Seite **Network Reporting Dashboard** wird geöffnet, auf der Sie alle Dashboards und Berichtwidgets anzeigen können.
3. Um ein Dashboard zu erstellen, klicken Sie auf **Neues Dashboard**. Die Seite Dashboard erstellen 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 Instanztyp aus - NetScaler oder NetScaler SDX.
   c) **Typ**. Wählen Sie den Entitätstyp aus, für den Sie Berichte erstellen möchten. Wählen Sie in diesem Beispiel virtuelle Server für den Lastenausgleich aus.
   d) **Beschreibung**. Geben Sie eine aussagekräftige Beschreibung für das Dashboard ein.
5. Klicken Sie auf **Weiter**. Alle unterstützten Berichte für die Instanz und die spezifische Entität werden angezeigt.
6. **Wählen Sie auf der Registerkarte Berichte** auswählen die erforderlichen Berichte aus. In diesem Beispiel können Sie Transaktionen, Verbindungen und Durchsatz auswählen. Klicken

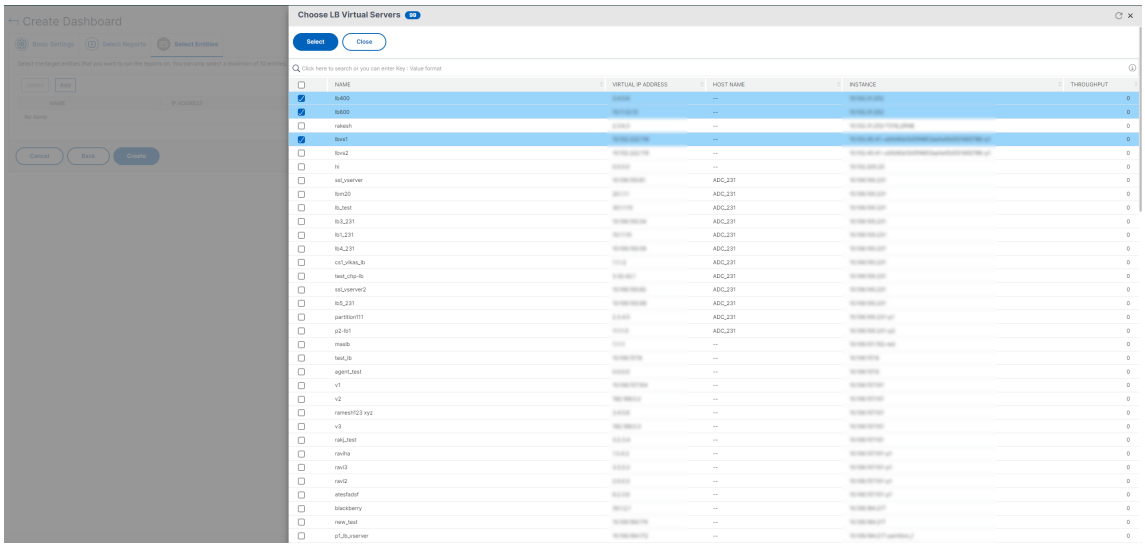
Sie auf **Weiter**.



1. 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.

2. Wählen Sie die Entitäten aus, die Sie überwachen möchten.



3. Klicken Sie auf **Erstellen**.

Das Dashboard wird erstellt und zeigt alle von Ihnen ausgewählten Berichte an.

> **Hinweis**
>
> Derzeit können Änderungen, die Sie an Legenden oder Filtern vornehmen, nicht gespeichert werden.

Exportieren von Netzwerkberichten

Sie können Widget-Berichte zwar in den Formaten .pdf, .png, .jpeg oder .csv exportieren, aber Sie können die gesamten Dashboards nur in den Formaten .pdf, .jpeg oder .png exportieren.

> **Hinweis**
>
> Sie können keine Berichte in NetScaler ADM exportieren, wenn Sie über schreibgeschützte Berechtigungen verfügen. Sie benötigen eine Bearbeitungsberechtigung, um eine Datei in NetScaler ADM erstellen und die Datei exportieren zu können.

So exportieren Sie Dashboard-Berichte:

1. Navigieren Sie zu **Infrastruktur > Network Reporting**
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** . 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 Dashboardseite “**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 jede Woche generiert und zeigt den Status des Dashboards an. Der Bericht überschreibt den Zeit- und Datumsstempel, sofern vom Benutzer festgelegt.

> **Hinweis**
>
> - Wenn Sie Wöchentliche Wiederholung auswählen, 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.

Bei der Planung 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.

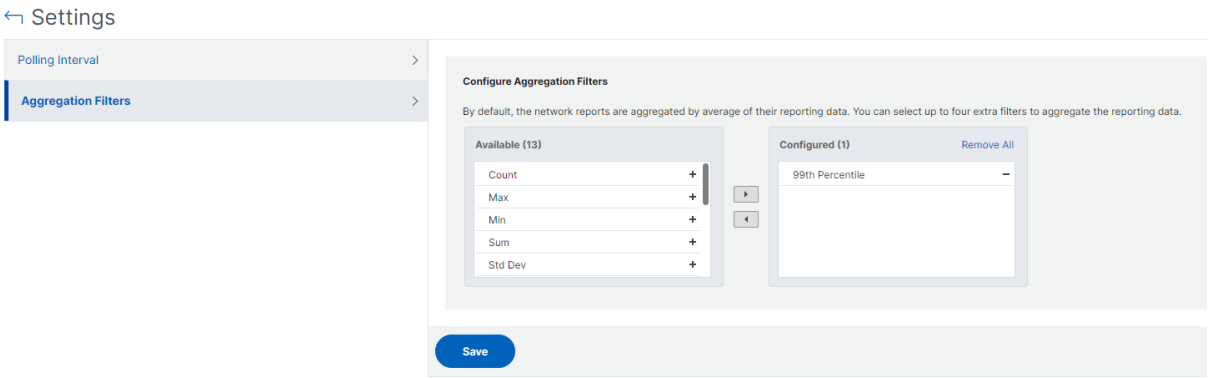
Beispielsweise können Sie für Netzwerkberichte, die von einem bestimmten virtuellen Server stammen, den Betreff als “authentication-reports-10.106.118.120”eingeben, wobei 10.106.118.120 die IP-Adresse des überwachten virtuellen Servers ist.

> **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.

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 auf die Daten angewendeten Aggregationen können Sie analysieren und sicherstellen, dass alle Ressourcen optimal genutzt werden. Navigieren Sie zu **Netzwerk > Netzwerkberichterstattung** und wählen Sie die Zeitdauer 1 Tag oder später aus, um die Option **Anzeigen nach** aufzurufen.

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:

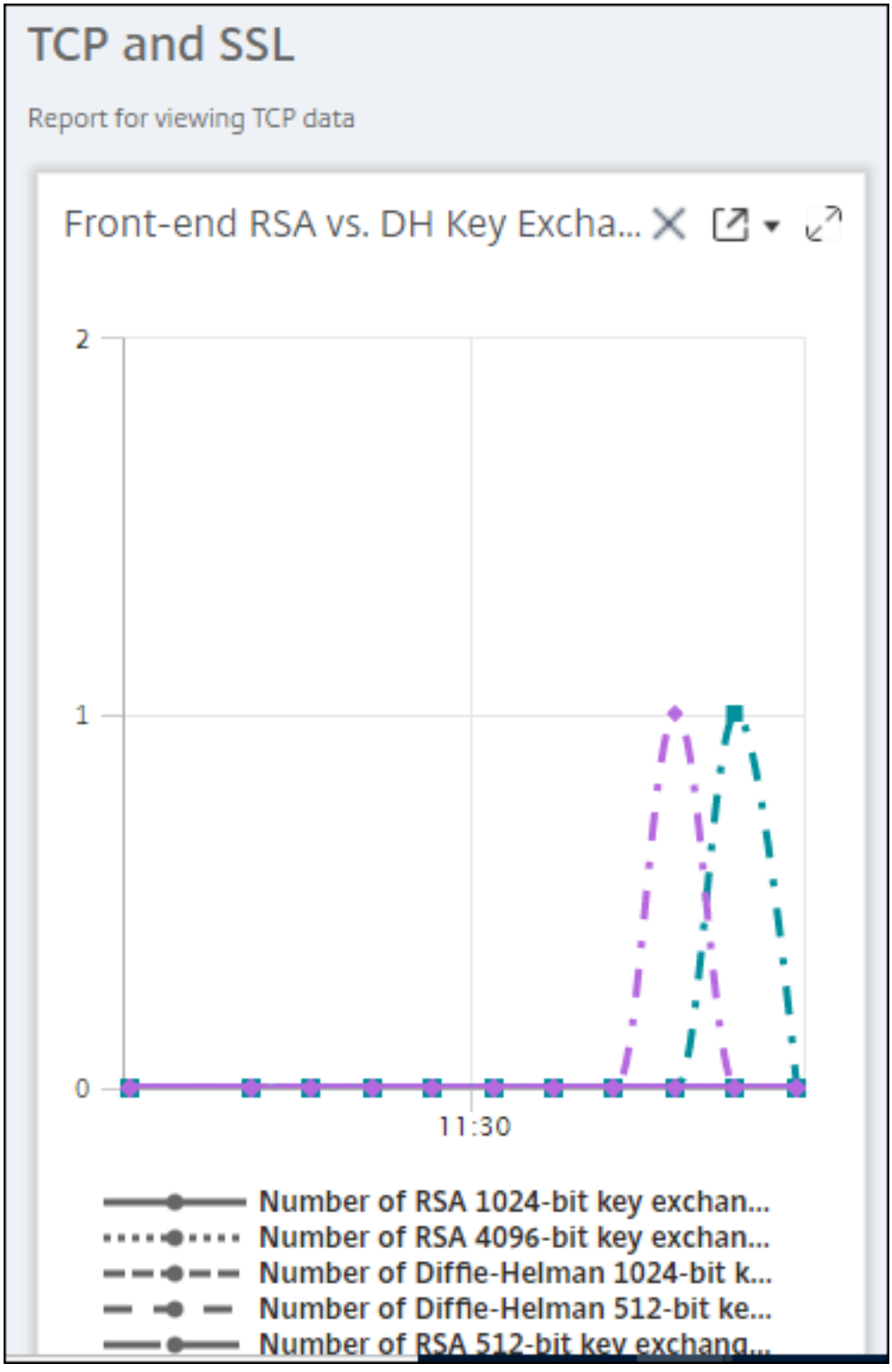
- Anzahl
- Max.
- Min
- Summe
- Std Dev
- Varianz

- 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 NetScaler ADM ungefähr eine Stunde, um Berichte für die ausgewählten Aggregationsoptionen zu erstellen.

So exportieren Sie Widget-Berichte:

1. Navigieren Sie zu **Infrastruktur > Network Reporting**.
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 auch auf **Skype for Business**.
4. Wählen Sie ein Widget aus. Wählen Sie beispielsweise **Load Balancing Virtual Server Transactions**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 NetScaler ADM

Um den Status einer NetScaler-Instanz zu überwachen, können Sie Schwellenwerte für Leistungsindikatoren festlegen und Benachrichtigungen erhalten, wenn ein Schwellenwert überschritten wird. In NetScaler ADM können Sie Schwellenwerte konfigurieren und sie 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 (wie in der Regel festgelegt) überschreitet oder unterschreitet, wird ein Ereignis mit dem angegebenen Schweregrad generiert, um auf ein leistungsbezogenes Problem hinzuweisen. Wenn der Zählerwert zu einem Wert zurückkehrt, den Sie als normal betrachten, wird das Ereignis gelöscht. Diese Ereignisse können angezeigt werden, indem Sie zu **Infrastruktur > Ereignisse > Berichte**navigieren. Auf der Seite Berichte können Sie auf den Donut **Ereignisse nach Schweregrad** klicken, um Ereignisse nach 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 NetScaler ADM zu **Infrastruktur > Netzwerkberichterstattung > 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 NetScaler.
    - **Name des Berichts**. 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. Im Abschnitt **Regel konfigurieren** können Sie die folgenden Details angeben:
    - **metrisch**. Wählen Sie die Metrik aus, für die Sie einen Schwellenwert festlegen möchten.
    - **Komparator**. Wählen Sie einen Komparator, um zu überprüfen, ob der überwachte Wert größer oder gleich oder kleiner oder gleich dem Schwellenwert ist.
    - **Schwellenwert**. Geben Sie den Wert ein, für den die Schwere des Ereignisses berechnet wird. Beispielsweise können Sie ein Ereignis mit dem Schweregrad eines kritischen Ereignisses 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 **Infrastruktur > Ereignisse > Berichte**navigieren. Auf der Seite Berichte können Sie auf den Donut **Ereignisse nach Schweregrad** klicken, um Ereignisse nach Schweregrad anzuzeigen.

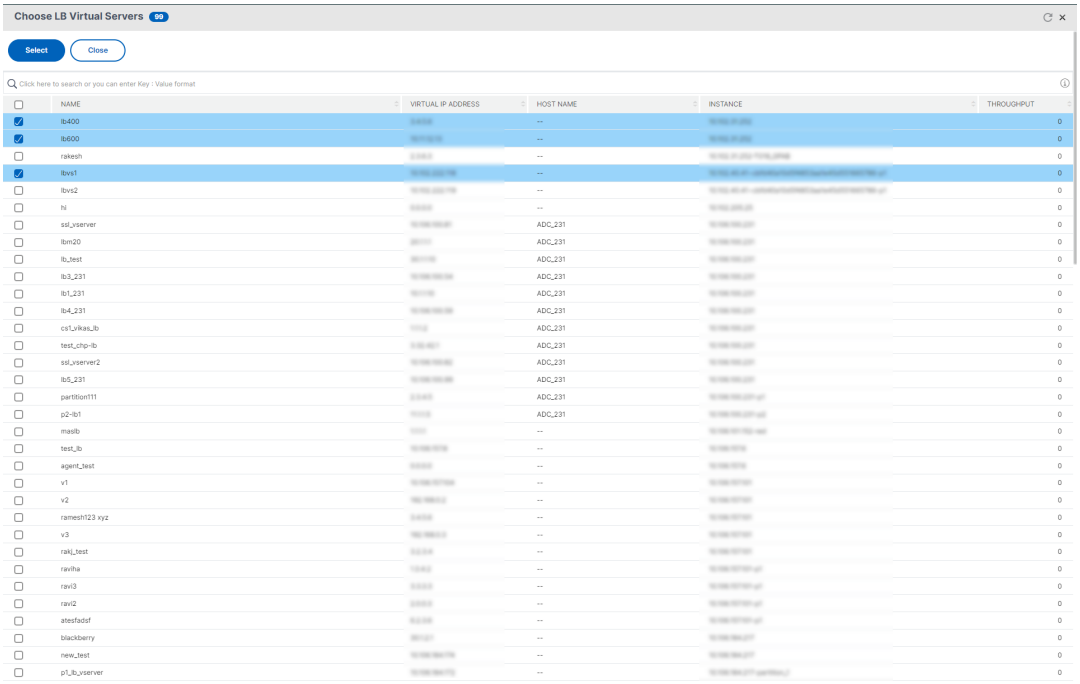
- **Wert löschen**. Geben Sie den Wert ein, der angibt, wann der Wert gelöscht werden soll. Beispielsweise können Sie den Schwellenwert Aktuelle Clientverbindungen löschen, wenn der überwachte Wert 50 Prozent erreicht. Geben Sie in diesem Fall 50 als Löschwert ein.
- **Schwere des Ereignisses**. Wählen Sie die Sicherheitsstufe aus, die Sie für den Schwellenwert festlegen möchten.

4. Sie können Instanzen und Entitäten auswählen, denen der Schwellenwert zugewiesen werden soll. Wählen Sie im Abschnitt **Instanzen** eine der folgenden Optionen:

   - **Alle Instanzen**. Der Schwellenwert ist für alle Instanzen festgelegt.
   - **Bestimmte Instanzen**. Der Schwellenwert wird für bestimmte Instanzen festgelegt. Verwenden Sie den Pfeil nach rechts, um Instanzen von der Liste **Verfügbar** in die Liste **Konfiguriert** zu verschieben. Der Schwellenwert wird für die Instanzen in der Liste **Konfiguriert** festgelegt.
   - **Bestimmte Entitäten**. Der Schwellenwert wird für bestimmte Entitäten festgelegt.

     Klicken Sie auf **Hinzufügen**, um die Entitäten auszuwählen.

     Je nach ausgewähltem Berichtstyp im Feld **Berichtsname** wird ein Fenster mit der Liste der Entitäten angezeigt. In diesem Beispiel wird das Fenster **Choose LB Virtual Servers** angezeigt.



Wählen Sie die Entitäten aus, für die Sie einen Schwellenwert festlegen möchten. Klicken Sie auf **Select**. Die ausgewählten Entitäten werden im Abschnitt **Instanzen** angezeigt.

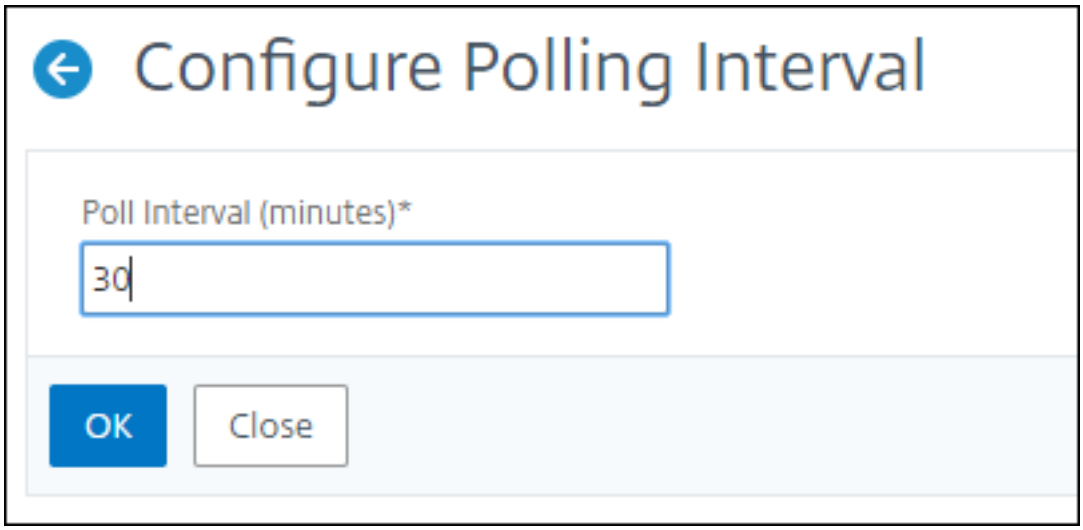
> **Hinweis:**
>
> Die Option **Spezifische Entitäten** wird nur angezeigt, wenn Sie unter **Bericht-sname**die Option vserverbasierte Berichte auswählen. Wenn Sie beispielsweise **LB Service Statistics**auswählen

5. Sie können auch eine **Ereignisnachricht**hinzufügen. Geben Sie eine Nachricht ein, die angezeigt werden soll, wenn der Schwellenwert erreicht ist. NetScaler ADM hängt den überwachten Wert und den Schwellenwert an diese Nachricht an.
6. Wählen Sie**Aktivieren**, um den Schwellenwert für die Generierung von Alarmen zu aktivieren.
7. Optional kannst du **Aktionen** wie E-Mail- oder Slack-Benachrichtigungen oder sowohl E-Mail- als auch Slack-Benachrichtigungen konfigurieren.
8. Klicken Sie auf **Erstellen**.

Festlegen des Intervalls für Leistungsabfragen

Standardmäßig erfassen NITRO -Aufrufe alle 5 Minuten Leistungsdaten für das Netzwerk-Reporting. 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 Leistungsabfrageintervall festzulegen, navigieren Sie zu **Infrastruktur > Netzwerkberichterstattung**, und klicken Sie auf**Abfrageintervall 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 NetScaler ADM konfigurieren. Diese Einstellung begrenzt die Menge der Netzwerkberichtsdaten, die in der Datenbank des NetScaler 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 30 Tage nicht überschreiten oder kleiner als 1 Tag sein.

Konfigurationsaufträge

February 5, 2024

Der Konfigurationsmanagementprozess von NetScaler Application Delivery Management (NetScaler ADM) gewährleistet die korrekte Replikation von Konfigurationsänderungen, Systemupgrades und anderen Wartungsaktivitäten auf mehreren Citrix Application Delivery Controller (ADC) -Instanzen im Netzwerk.

NetScaler 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 NetScaler ADM. Ein Konfigurationsauftrag enthält eine Reihe von Konfigurationsbefehlen, die Sie auf einem oder mehreren verwalteten Geräten ausführen können.

Konfigurationsjobs können entweder SSH-Befehle verwenden, um Konfigurationsbefehle auszuführen, oder SCP verwenden, um Dateien entweder lokal oder auf eine andere Appliance zu kopieren. Beispielsweise können wir ein HA-Failover oder HA-Upgrade planen.

Sie können einen Konfigurationsauftrag erstellen, indem Sie eine der folgenden vier Optionen in NetScaler 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 sie zum Konfigurieren von Aufträgen zu verwenden.

Integrierte Vorlage: 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 integrierten Vorlagen sind mit ihren Beschreibungen in der folgenden Tabelle aufgeführt. Sie können einen Job planen, indem Sie die integrierte Vorlagenoption verwenden. Ein Job ist ein Satz 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.

Instanz

Sie können ein Einzelbündel-Upgrade Ihrer NetScaler SDX-Instanzen mit NetScaler Version 11.0 und höher durchführen. Um ein Einzelbündel-Upgrade durchzuführen, verwenden Sie einen integrierten Task in NetScaler ADM. Sie können eine NetScaler-Instanz auch aktualisieren, indem Sie die ausgeführte Konfiguration oder eine gespeicherte Konfiguration extrahieren und die Befehle auf einer anderen NetScaler-Instanz desselben Typs ausführen. Auf diese Weise können Sie die Konfiguration einer Instanz auf der anderen replizieren.

Datei

Sie können eine Konfigurationsdatei von Ihrem lokalen Computer hochladen und Jobs erstellen.

Vorteile der Verwendung einer Datei

- Sie können eine beliebige Textdatei verwenden, um eine wiederverwendbare Quelle für Konfigurationsbefehle zu erstellen.
- Jegliche 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 NetScaler-Sitzung zu erhalten. Wenn Sie den Auftrag ausführen, werden Änderungen in der ns.conf auf der ausgewählten Instanz aufgezeichnet und in NetScaler ADM kopiert.

Verwandte Artikel

- Verwendung des SCP (put) -Befehls in Konfigurationsjobs
- So verwenden Sie Variablen in Konfigurationsjobs
- So erstellen Sie Konfigurationsaufträge aus Korrekturbefehlen
- So verwenden Sie Konfigurationsvorlagen, um Auditvorlagen zu erstellen
- So verwenden Sie Record-and-Play zum Erstellen von Konfigurationsaufträgen
- So verwenden Sie die Masterkonfigurationsvorlage auf NetScaler ADM

Erstellen eines Konfigurationsauftrags

February 5, 2024

Ein Auftrag ist eine Reihe von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen erstellen und ausführen können. Mit der NetScaler Application Delivery Management (ADM) -GUI können Sie Jobs erstellen, um Konfigurationsänderungen zwischen [Instanzen vorzunehmen, Konfigurationen auf mehreren Instanzen in Ihrem Netzwerk zu replizieren](https://docs.citrix.com/de-de/netscaler-mas/11-1/configuration-jobs-replicate-configuration.html) und Konfigurationsaufgaben aufzuzeichnen und abzuspielen und sie in CLI-Befehle umzuwandeln.

Mit der Funktion Konfigurationsaufträge von NetScaler ADM können Sie einen Konfigurationsauftrag erstellen, E-Mail-Benachrichtigungen senden und Ausführungsprotokolle der erstellten Aufträge überprüfen.

So erstellen Sie einen Konfigurationsauftrag auf NetScaler ADM:

1. Navigieren Sie zu **Infrastruktur > Konfigurationsaufträge**.
2. Klicken Sie auf **Job erstellen**.
3. Geben Sie auf der Seite **Job erstellen** auf der Registerkarte **Konfiguration auswählen** den Job-Namen 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 **Konfigurationsvorlage**, **In-Built-Vorlage**, **Master-Konfiguration**, **Aufnahme und Wiedergabe**, **Instanz** und **Datei**sein.

    > **Hinweis**
    >
    > Wenn Sie die `Deploy Master Configuration Job` Vorlage zum ersten Mal hinzufügen, fügen Sie eine Vorlage eines anderen Typs hinzu, dann wird die gesamte Auftragsvorlage zu einem `Master Configuration` Typ.

    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

dort 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 eine Vorschau der 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 Ihre benutzerdefinierten Befehle anzugeben, aktivieren Sie die benutzerdefinierte Rollback-Option.

> **Wichtig**
>
> Damit das benutzerdefinierte Rollback wirksam wird, schließen Sie den Assistenten zum **Erstellen eines Auftrags** ab. Wählen Sie auf der Registerkarte **Ausführen** die Option **Rollback Erfolgreicher Befehle** aus der Liste **Bei Befehlsfehler** aus.

5. **Wählen Sie auf der Registerkarte Instanzen** auswählen die Instanzen aus, für die Sie die Konfigurationsüberwachung ausführen möchten.

   a) In einem NetScaler 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.

6. Auf der Registerkarte**Variablenwerte angeben** stehen Ihnen zwei Optionen zur Verfügung:

   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 NetScaler ADM Server hoch.

b) Geben Sie gemeinsame Werte für die Variablen ein, die Sie für alle Instanzen definiert haben

c) Klicken Sie auf **Weiter**.

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.

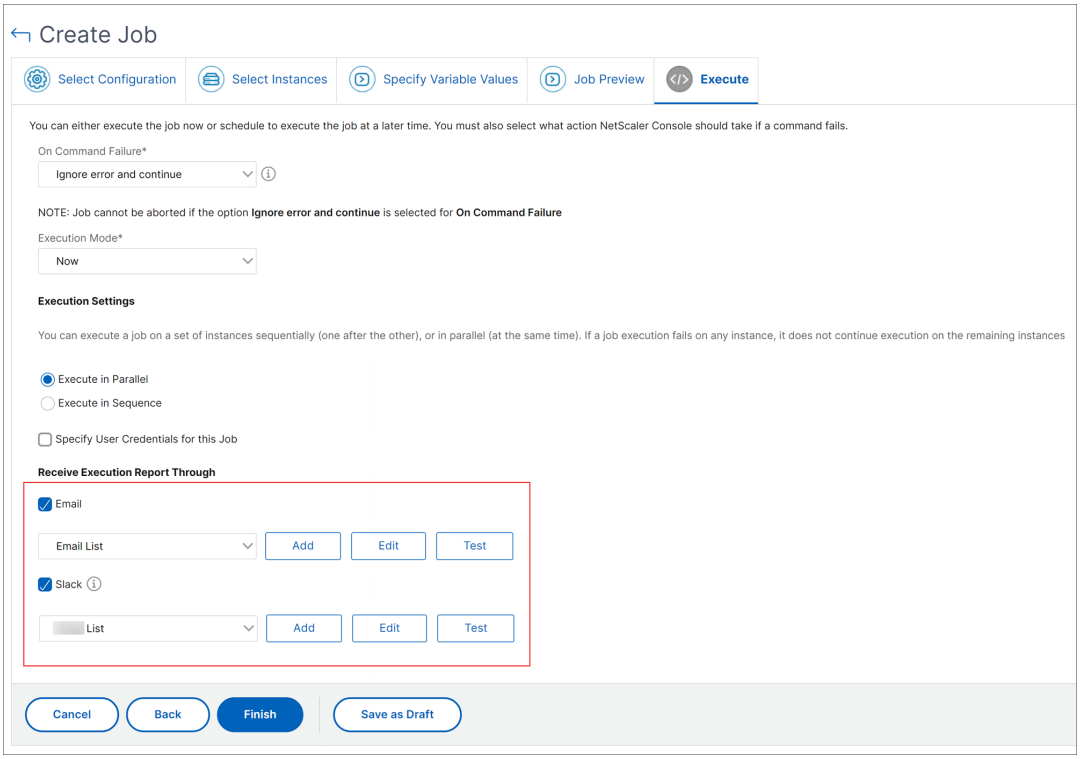
1. Navigieren Sie zu **Infrastruktur > Konfigurationsaufträge**.
2. Wählen Sie den Job aus, den Sie E-Mail- und Slack -Benachrichtigung aktivieren möchten, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Registerkarte **Ausführen** zum Bereich **Ausführungsbericht empfangen über** :

   - Aktivieren Sie das Kontrollkästchen **E-Mail** und wählen Sie die E-Mail-Verteilerliste aus, an die Sie den Ausführungsbericht senden möchten.

     Wenn Sie eine E-Mail-Verteilerliste hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie die E-Mail-Serverdetails an.

   - Aktivieren Sie das Kontrollkästchen **Slack** und wählen Sie den Slack-Kanal aus, 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 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 **Infrastruktur > 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 **Ausführungsbericht empfangen über** :

   - Aktivieren Sie das Kontrollkästchen **E-Mail** und wählen Sie die E-Mail-Verteilerliste aus, an die Sie den Ausführungsbericht senden möchten.

     Wenn Sie eine E-Mail-Verteilerliste hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie die E-Mail-Serverdetails an.

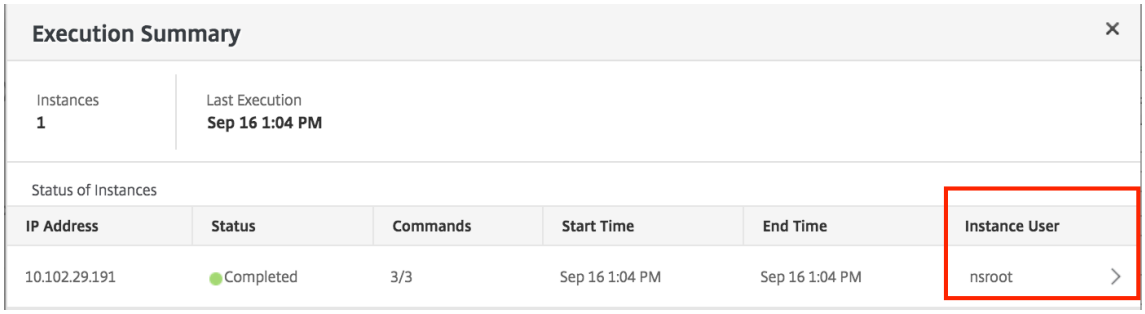
   - Aktivieren Sie das Kontrollkästchen **Slack** und wählen Sie den Slack-Kanal aus, an den Sie den Ausführungsbericht senden möchten.

     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 **Infrastruktur > 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, bei der der Auftrag ausgeführt wird
    - Die Befehle werden für den Auftrag ausgeführt
    - Die Start- und Endzeit des Auftrags und
    - Der Name des Instanzbenutzers



Auditberichte anzeigen

February 5, 2024

(NetScaler ADM) ermöglicht es Ihnen, den Vergleichsbericht zur Konfigurationsprüfung im Abschnitt zur Konfigurationsprüfung anzuzeigen und herunterzuladen. Im Abschnitt zur Konfigurationsprüfung können Sie Folgendes exportieren:

- Zusammenfassungsbericht über alle Instanzen pro Instanz
- Granularer Differenzbericht (Diff) für jedes Instanz-Template-Paar

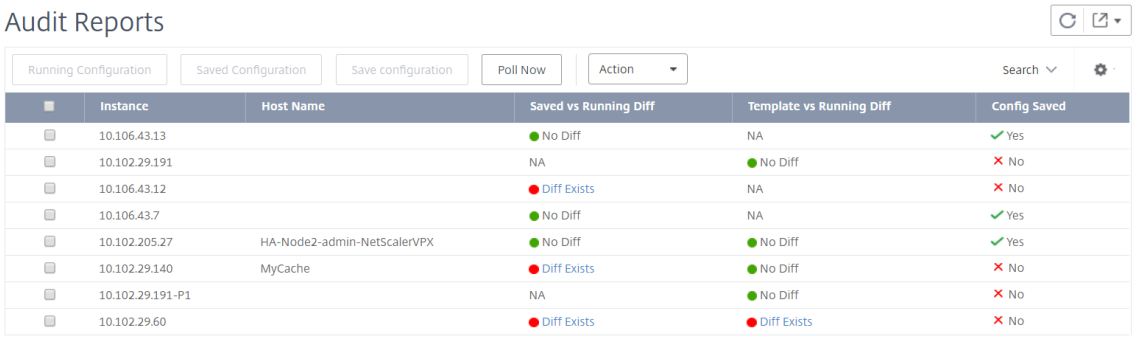
Die Auditvorlagen in **den Auditvorlagen**werden zum geplanten Zeitpunkt anhand der Konfigurationen in den angegebenen Instanzen ausgeführt. Das Diagramm **NetScaler Config Drift** im **Konfigurationsüberprüfungs-Dashboard** zeigt allgemeine Details zu Konfigurationsänderungen an, die für nicht gespeicherte Konfigurationen gespeichert wurden. Wenn Sie auf das **NetScaler Config Drift**-Diagramm klicken, wird auf der darauffolgenden **Seite „**Auditberichte “eine Liste von

Instanzen angezeigt, in der sowohl „Diff existiert“als auch „Kein Unterschied“angezeigt wird. „ Sie können die von NetScaler ADM angezeigten Differenzberichte herunterladen.

NetScaler ADM bietet auch die Option, den automatischen Export eines Diff-Berichts als E-Mail-Anhang zu planen. Weitere Informationen zum Planen des Exports von Berichten finden Sie unter Erstellen von Überwachungsvorlagen.

So exportieren Sie Konfigurationsüberwachungsberichte:

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Konfiguration > Konfigurationsüberprüfung**.
2. Klicken Sie auf der Seite **Configuration Audit** in das Diagramm **NetScaler Config Drift** .
3. Auf der Seite **Auditberichte** 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.

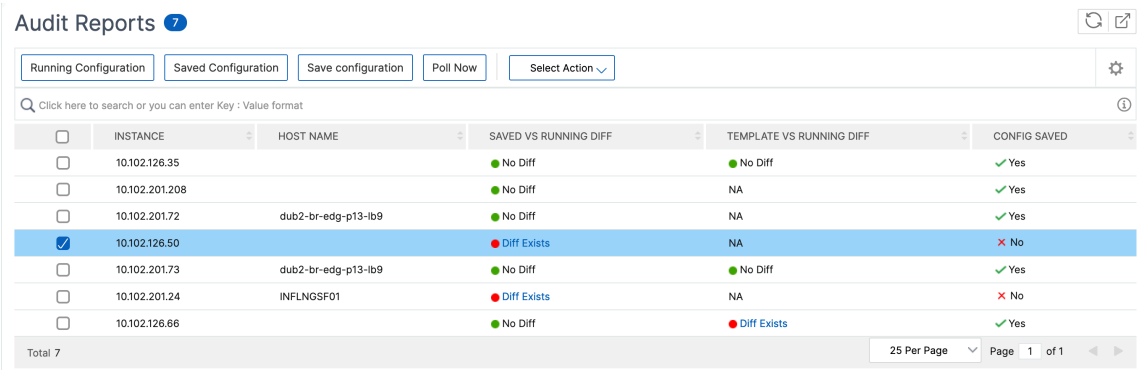


Im Bild sehen Sie, dass für einige Instanzen ein Diff nur in **Saved Vs Running Diff** vorhanden ist und für einige Instanzen ein Diff nur in **Template vs Running Diff** vorhanden ist. In einigen Fällen gibt es Unterschiede sowohl zwischen **Saved Vs Running Diff** als auch **Template vs Running Diff.**

Gespeichert Vs Laufdiff

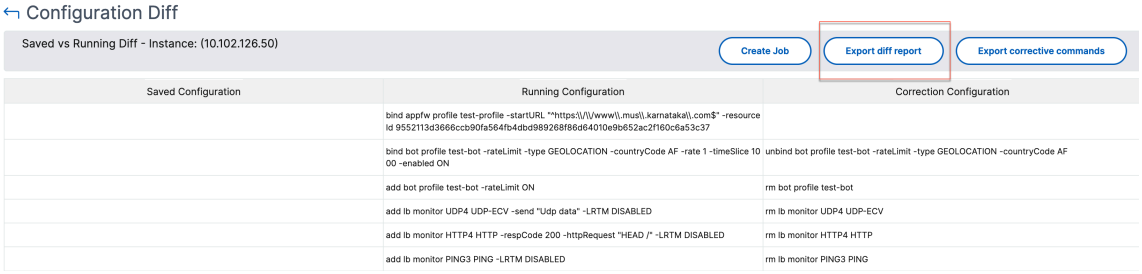
Sie können einen Bericht über den Unterschied zwischen der auf der Instanz gespeicherten Konfiguration und der Konfiguration, die derzeit auf der Instanz ausgeführt wird, anzeigen.

1. Klicken Sie unter **Saved Vs Running**Diff auf Diff Exists**für eine Instanz.**



Sie können den Bericht für die gespeicherte Konfiguration anzeigen, indem Sie den Konfigurationsunterschied für diese Instanz ausführen.

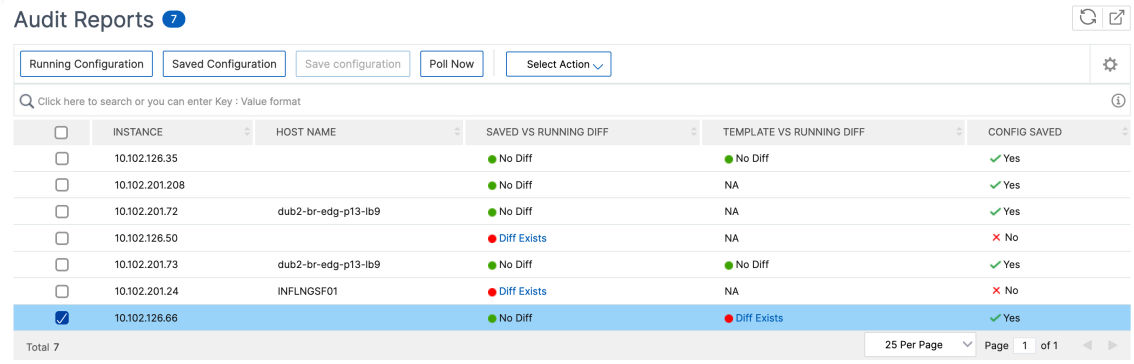
2. Klicken Sie auf **Diff-Bericht exportieren**, um eine CSV-Datei des Diff-Berichts herunterzuladen. Sie können auch auf **Korrekturbefehle exportieren** klicken, um die Befehle in eine TXT-Datei zu exportieren. Sie können dann die Befehle auf der zugehörigen NetScaler ADM-Instanz von Configuration Jobs aus ausführen, um die Konfiguration in dieser Instanz zu korrigieren.



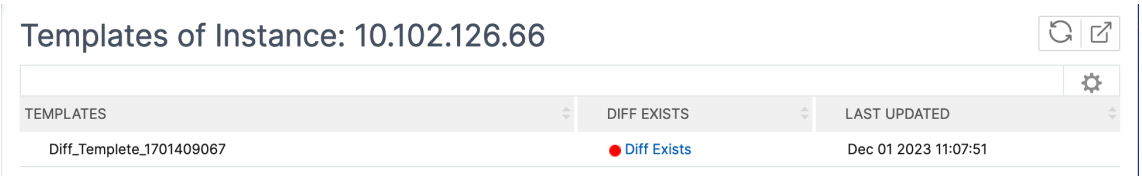
Template gegen Running Diff

Das **Template vs Running Diff** enthält alle Vorlagen außer **Saved Vs Running Diff**, der Standardvorlage. Sie können den Unterschied zwischen der Vorlage und der laufenden Konfiguration anzeigen.

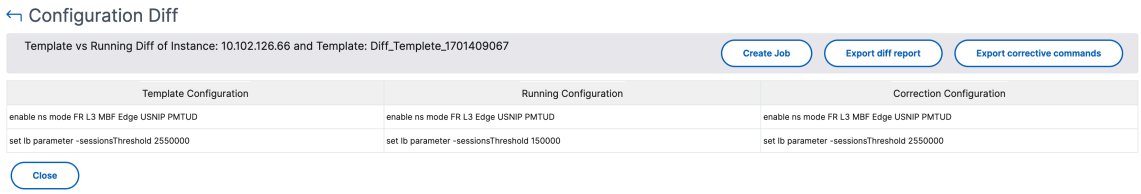
1. Klicken Sie für eine der Instanzen unter **Template vs Running Diff auf Diff**Exists**.**



2. Die Vorlagen zeigen die Unterschiede, wenn die NetScaler ADM-Instanz von der in der Vorlage angegebenen Konfiguration abweicht.



3. Klicken Sie erneut auf**Diff Existent**. Die folgende Abbildung zeigt die Konfiguration, nach der die Vorlage sucht, die laufenden Konfigurationen und die Korrekturkonfigurationen oder die Befehle, die zur Korrektur der Konfiguration ausgeführt werden müssen. Wenn das Feld **Laufende Konfiguration** leer ist, bedeutet das, dass Befehle entweder nicht konfiguriert sind oder entfernt wurden.



4. 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. Sie können dann die Befehle in der CLI ausführen, um die Konfiguration in der Instanz zu korrigieren.

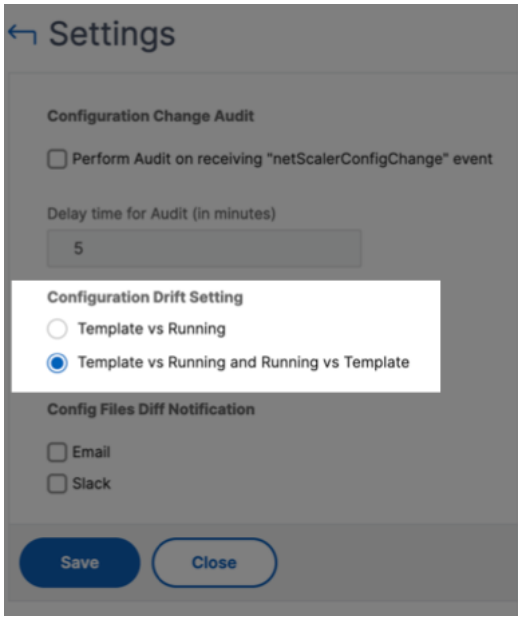
Template_vs_Running_Diff_of_Instance _10.102.126.66_and_Template _Diff_Templete_1701409067

Template Configuration	Running Configuration	Correction Configuration	
enable ns mode FR L3 MBF Edge USNIP PMTUD	enable ns mode FR L3 Edge USNIP PMTUD	enable ns mode FR L3 MBF Edge USNIP PMTUD	
set lb parameter -sessionsThreshold 2550000	set lb parameter -sessionsThreshold 150000	set lb parameter -sessionsThreshold 2550000	

Sie können auch die Einstellung Template vs Running und Running vs Template Drift verwenden, um die Konfiguration auf beiden Arten zu vergleichen:

- Vergleicht die Audit-Vorlagenkonfiguration mit der laufenden Konfiguration auf der Instanz.
- Vergleicht die laufende Konfiguration auf der Instanz mit der Audit-Vorlage.

Standardmäßig ist das Template vs. Die Einstellung Laufdrift ist ausgewählt. Um die Drift-Einstellung zu ändern, wählen Sie auf der Seite **Configuration Audit** die Option **Einstellungen** aus.



Anzeigen der Dateistatus-Überwachungsberichte

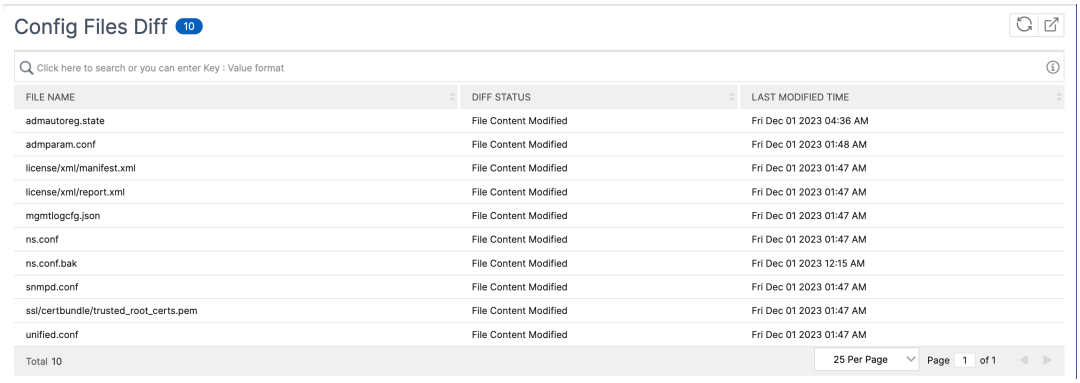
Verwenden Sie das NetScaler-Dateistatusdiagramm , um zu überwachen, ob Dateien zum Ordner hinzugefügt, geändert oder aus dem **nsconfig**Ordner entfernt werden.“ Wenn die Lizenzdatei beispielsweise auf einer NetScaler-Instanz aktualisiert wird, können Sie überprüfen, wann diese Datei zuletzt aktualisiert wurde, und die erforderlichen Maßnahmen ergreifen.

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsüberprüfung**.
2. Klicken Sie auf der Seite **Configuration Audit** auf das Diagramm **NetScaler Config File Status** .

   Auf der Seite **Auditberichte** werden Instanzen mit dem Status “Vergleich”aufgeführt.

   Der **Diff-Status** wird für das Intervall zwischen der **vorherigen Abfragezeit** und der **letzten Abfragezeit**berechnet. Der **Diff-Status** kann einer der folgenden sein:

   - ** **Diff existiert** —**Dieser Status gibt an, dass sich die Dateien im Ordner `nsconfig` einer Instanz seit dem letzten Abfragezeitpunkt geändert haben.**** Um die Änderungen an der Datei anzuzeigen, klicken Sie auf **Diff Existiert**.



- **Kein Diff** - Dieser Status zeigt an, dass sich die Dateien im`nsconfig` Ordner seit der vorherigen Abfragezeit nicht geändert haben.
- **NA**—Dieser Status weist darauf hin, dass die Überwachung des Dateistatus nicht möglich ist. Dieser Status wird angezeigt, wenn der NetScaler ADM die Instanz nicht abfragt. Wenn beispielsweise eine Instanz neu hinzugefügt wird oder ein Instanzstatus inaktiv ist, findet keine Abfrage der Instanz statt.

Konfigurationsänderungen über alle Instanzen hinweg überwachen

February 5, 2024

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 NetScaler-Instanzen hinweg überwachen, Konfigurationsfehler beheben und nicht gespeicherte Konfigurationen nach einem plötzlichen Herunterfahren des Systems wiederherstellen.

Sie können Prüfungsvorlagen mit bestimmten Konfigurationen erstellen, um bestimmte Instanzen zu überprüfen. NetScaler ADM vergleicht diese Instanzen mit der Überwachungsvorlage und meldet, wenn eine Nichtübereinstimmung in der Konfiguration vorliegt. Der Konfigurationsvergleichsbericht ermöglicht es Ihnen, Fehler zu beheben und unerwünschte Konfigurationsänderungen zu korrigieren.

Sie können die Ausführung der Audit-Vorlage automatisieren, indem Sie:

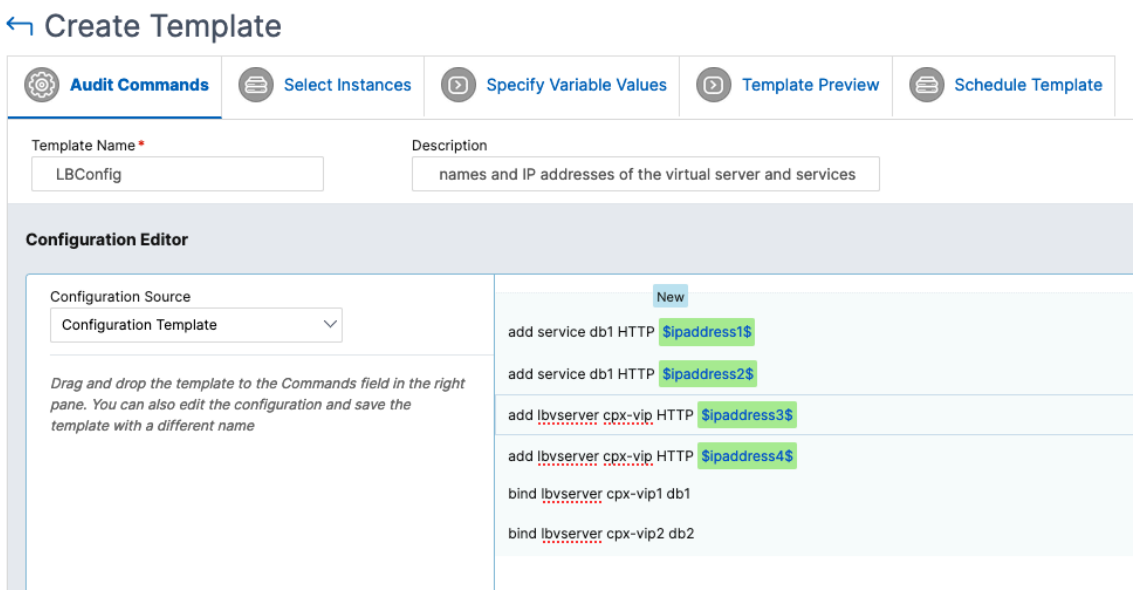
- Planung des Zeitpunkts, zu dem die Vorlage ausgeführt werden muss.
- Festlegen der Häufigkeit, mit der NetScaler ADM die Vorlage ausführen muss. Sie können die Vorlage täglich, an einem bestimmten Tag in einer Woche oder an einem bestimmten Datum in einem Monat ausführen.

Sie haben auch die Möglichkeit, den von NetScaler ADM generierten Diff-Bericht an angegebene E-Mail-Adressen zu senden, die Sie konfigurieren können. Mit dieser Option können Benutzer den Bericht als E-Mail-Anhang oder als Slack-Benachrichtigung erhalten. Sie müssen sich nicht bei NetScaler ADM anmelden, um die Berichte manuell zu exportieren.

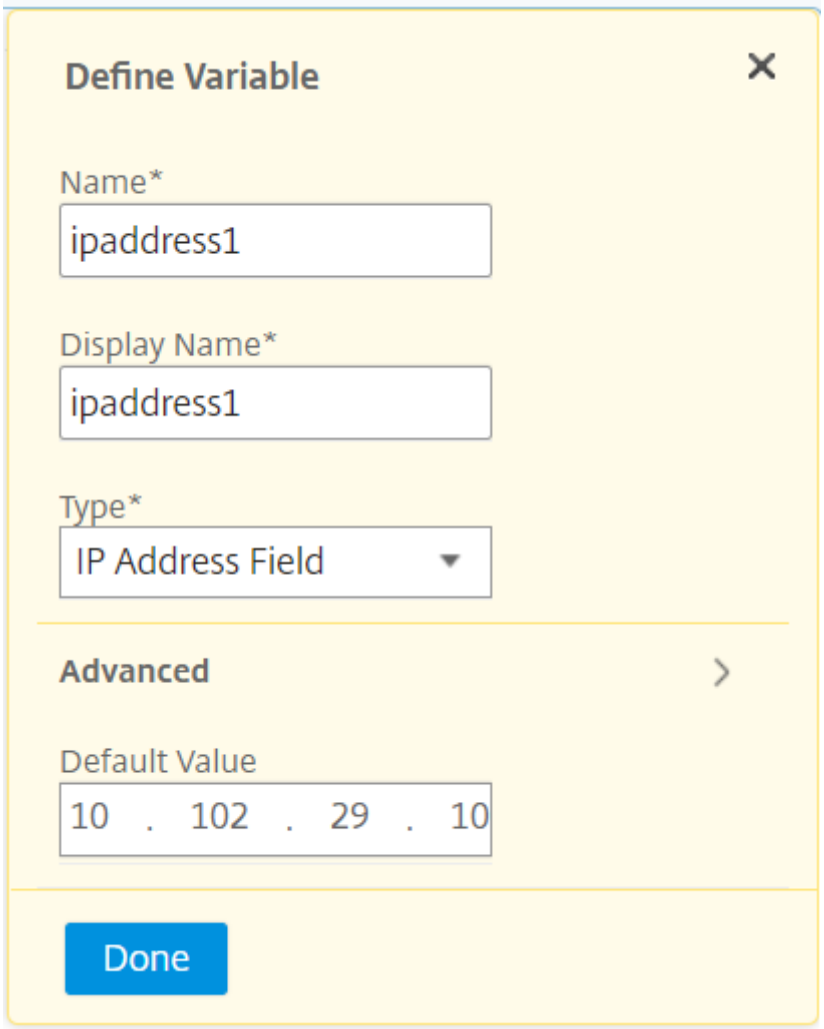
> **Hinweis:**
>
> Die Option **Umbenennen** ist für die Standardkonfigurationsvorlagen deaktiviert. Sie können jedoch benutzerdefinierte Konfigurationsvorlagen umbenennen.

So erstellen Sie Überwachungsvorlagen:

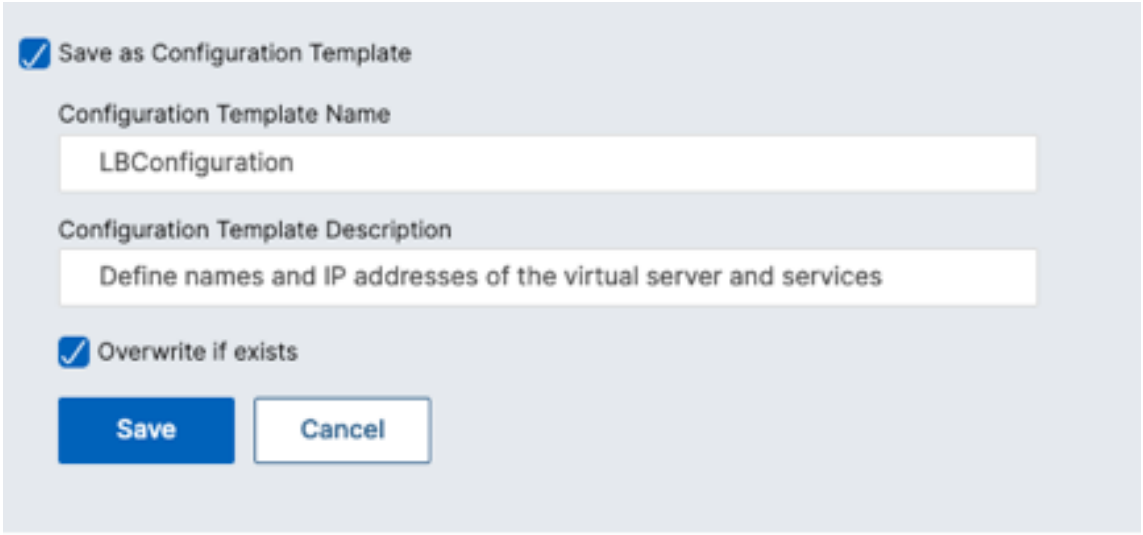
1. Navigieren Sie zu **Infrastruktur > Konfiguration > Configuration Audit >** Auditvorlagen und klicken Sie auf **Hinzufügen** .
2. Geben Sie auf der Seite „ **Vorlage erstellen** “und auf der Registerkarte „ **Audit-Befehle** “den Namen der Vorlage und ihre Beschreibung an.
3. Geben Sie auf der Seite **Konfigurations-Editor** Ihre Befehle ein und speichern Sie die Befehle als Konfigurationsvorlage. Sie können auch eine vorhandene Vorlage aus dem linken Bereich 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 jetzt in „$ “eingeschlossen.



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 die Variable angeben möchten.

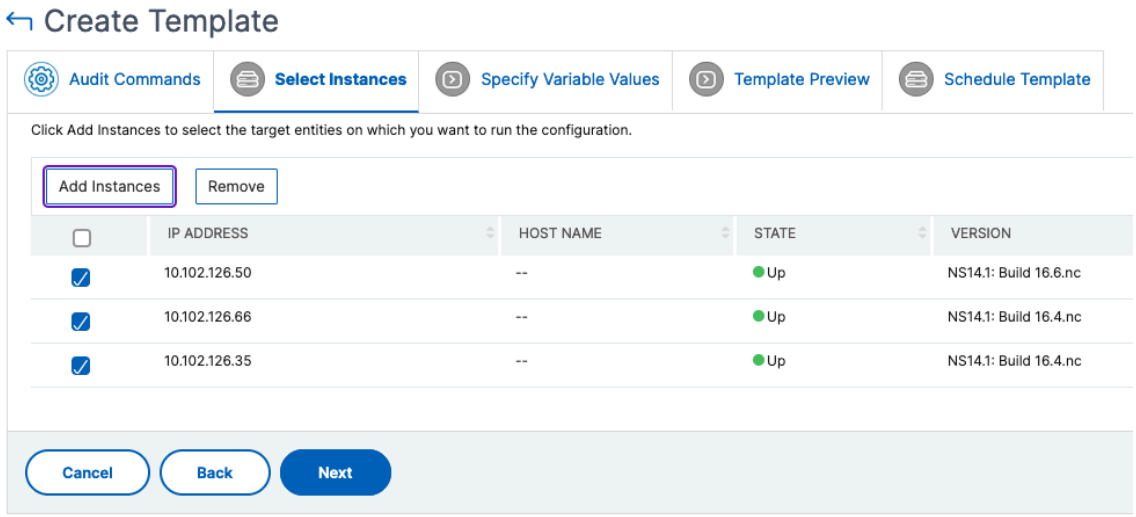


Sie können die Befehle auch als Konfigurationsvorlage speichern.



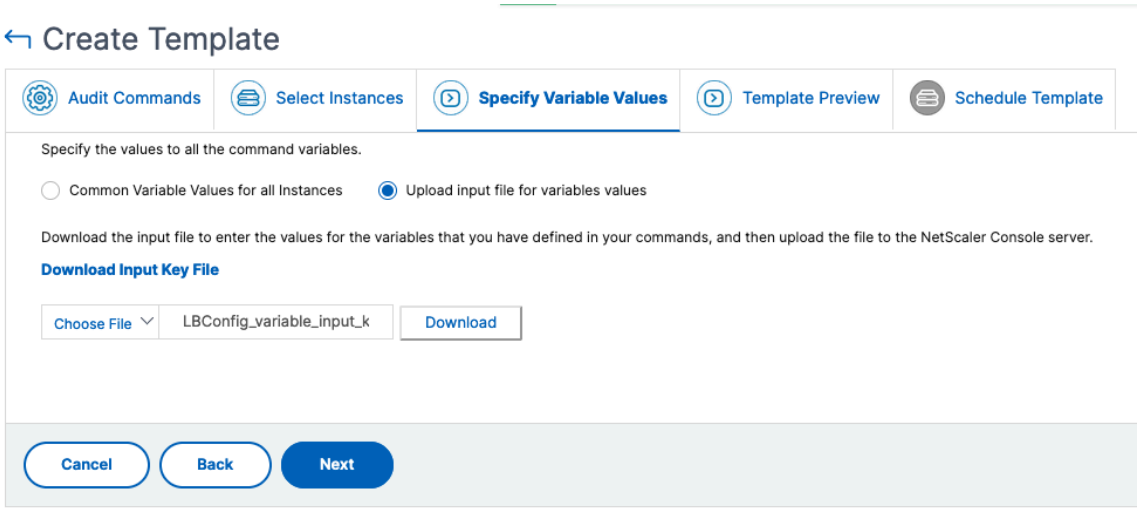
5. Klicken Sie auf**Speichern** und dann auf **Weiter**.

6. Wählen Sie auf der Registerkarte **Instanzen auswählen** die Instanzen aus, auf denen die Konfigurationsüberwachung ausgeführt werden soll, und klicken Sie auf **Weiter**.

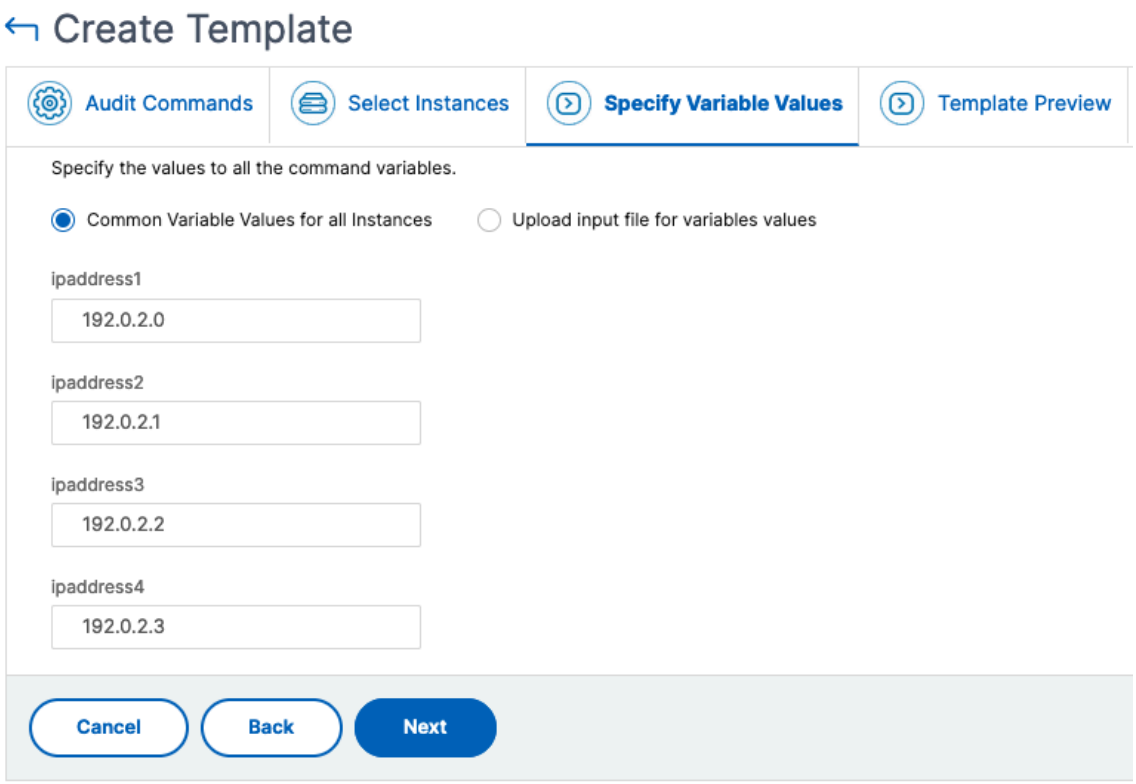


7. Auf der Registerkarte**Variablenwerte angeben** stehen Ihnen zwei Optionen zur Verfügung:

   a) Laden Sie die Eingabedatei herunter, um die Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben. Laden Sie die Datei nach Eingabe der Variablen auf den NetScaler ADM Server hoch.

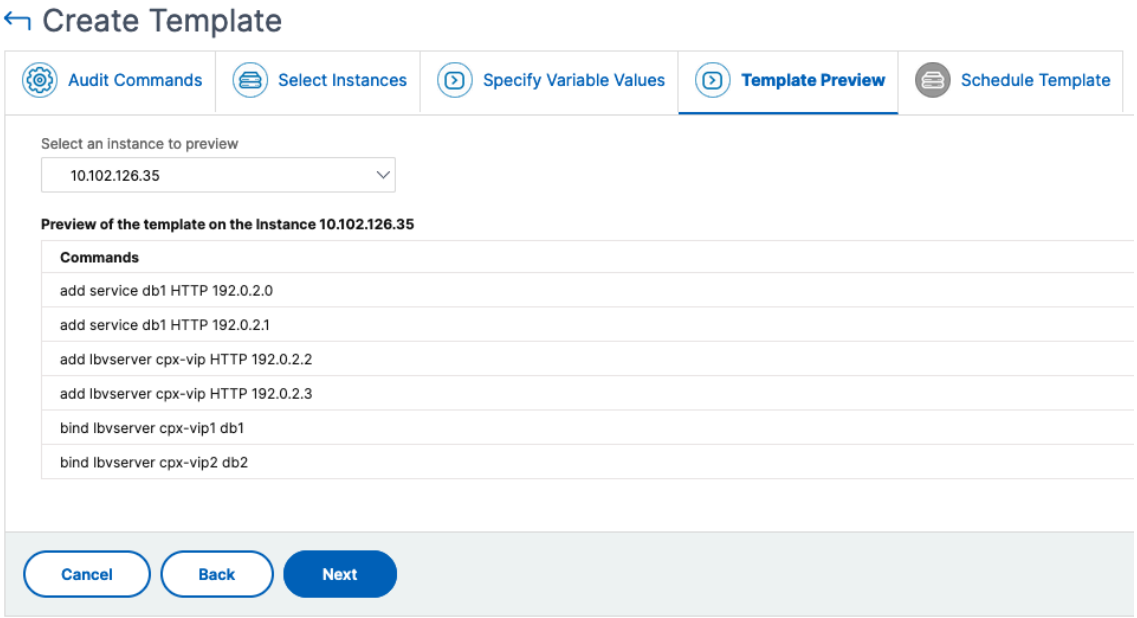


   a) Geben Sie gemeinsame Werte für die Variablen ein, die Sie für alle Instanzen definiert haben.



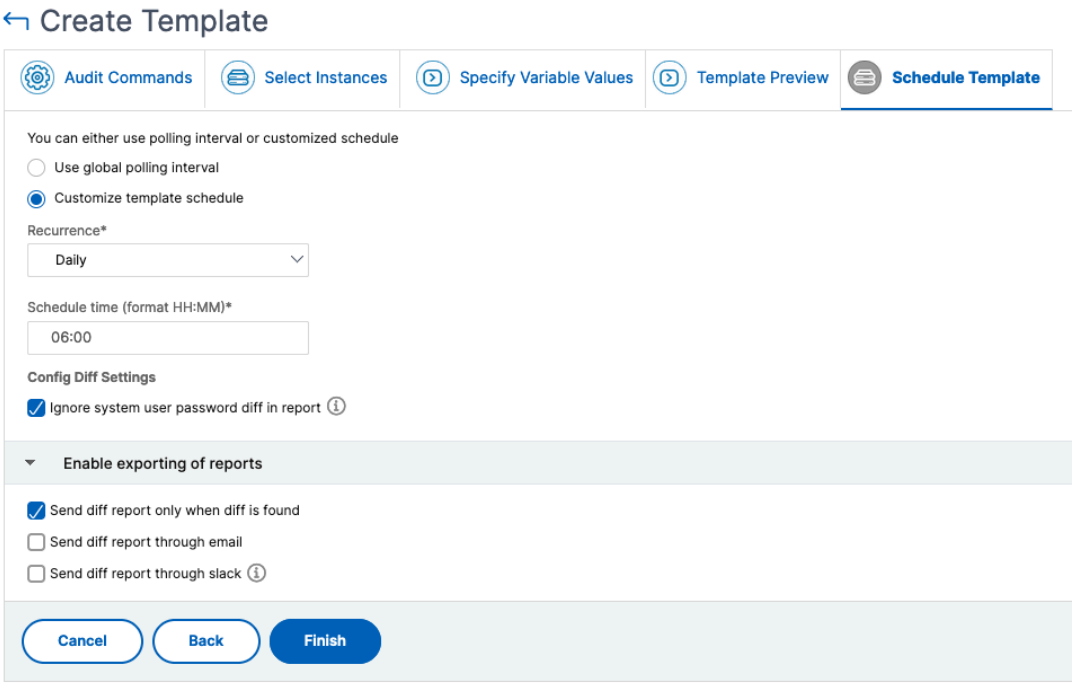
> **Hinweis:**
>
> Wenn Sie jede Instanz mit unterschiedlichen Werten prüfen möchten, müssen Sie in der Eingabedatei für jede Instanz separate Variablen erstellen.

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 Polling-Intervall** Wählen Sie diese Option aus, um die Vorlage auf den Instanzen zu einem Zeitpunkt auszuführen, der global auf NetScaler 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.
        - Geben Sie die Häufigkeit und den Zeitpunkt für die Ausführung der Prüfungsvorlagen an.
    - **Aktiviert den Export von Berichten**. Verwenden Sie diese Option, um:
        - **Diff-Bericht senden, nur Diff wurde gefunden**
        - **Senden Sie den Vergleichsbericht per E-Mail**. Konfigurieren Sie das E-Mail-Profil, an das der Diff-Bericht als E-Mail-Anhang gesendet werden muss.
        - **Senden Sie den Diff-Bericht über Slack**. Konfiguriere den Slack-Kanal, an den der Diff-Bericht als Benachrichtigung gesendet werden muss.



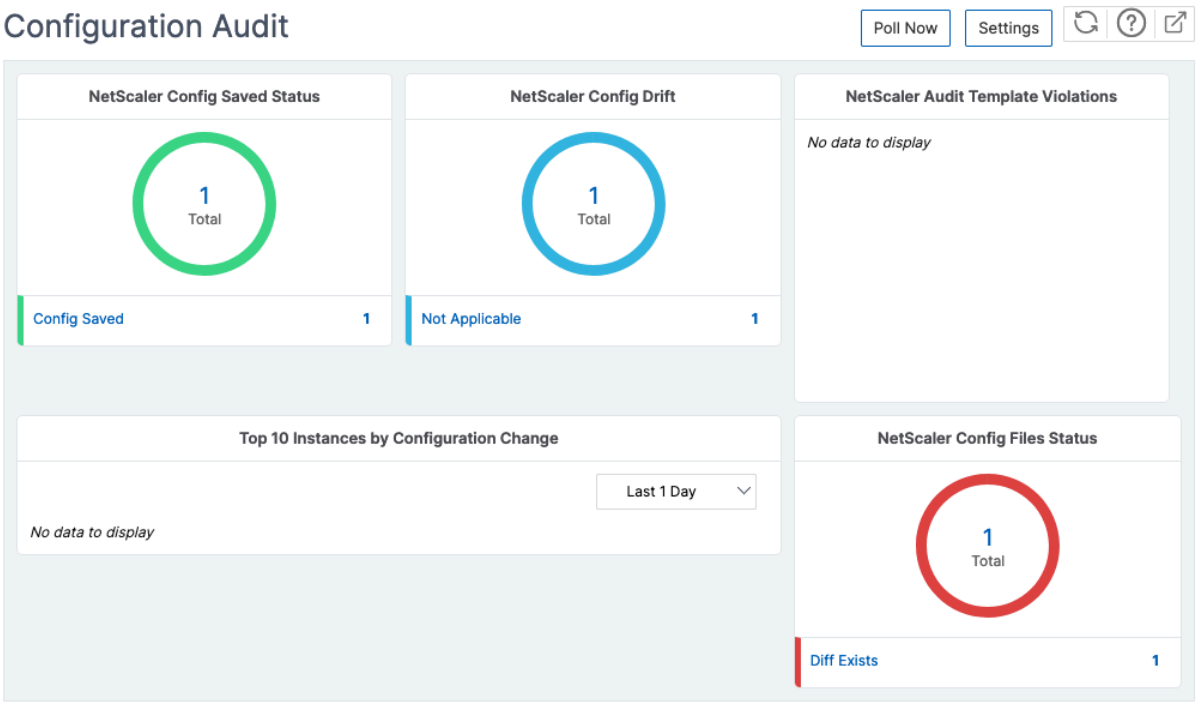
11. Klicken Sie auf **Fertig stellen**.

Die Überwachungsvorlage wird in der Liste **Überwachungsvorlagen** angezeigt und zum geplanten Zeitpunkt für die Konfigurationen in den angegebenen Instanzen ausgeführt.

Anzeigen von Konfigurationsänderungen

Sie können das **Configuration Audit**-Dashboard auch verwenden, um allgemeine Details zu Konfigurationsänderungen anzuzeigen, wie 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

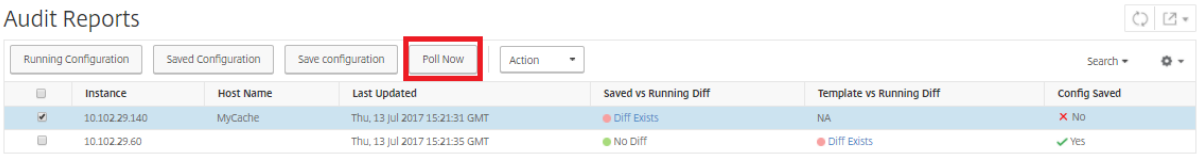


Mit NetScaler ADM können Sie Konfigurationsaudits manuell abfragen und alle Konfigurationsaudits der Instanzen sofort dem NetScaler ADM hinzufügen. Navigieren Sie dazu zu **Infrastruktur > Konfiguration > Konfigurationsüberprüfung**, klicken Sie auf **Jetzt abfragen**. Auf der Popup-Seite **Jetzt abfragen** können Sie alle NetScaler-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 NetScaler Konfiguration**
- **NetScaler 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 NetScaler Konfigurationsdatei** enthält den Status der NetScaler Dateien, die im`nsconfig` Ordner vorhanden sind. NetScaler ADM zeichnet Änderungen in Dateien innerhalb des Ordners `nsconfig`auf und vergleicht diese und zeigt die Unterschiede an. Weitere Informationen finden Sie unter Anzeigen der Berichte zur Dateistatusprüfung

Konfigurationsüberwachungsbenachrichtigungen festlegen

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsüberprüfung**.
2. Klicken Sie auf der Seite **Configuration Audit** auf **Einstellungen** .
3. Klicken Sie auf **der Seite**mit den Benachrichtigungseinstellungen auf das Symbol **Bearbeiten** , um die Benachrichtigungseinstellungen zu aktivieren.
4. Wählen Sie das Kontrollkästchen **Aktiviert** aus. Wählen Sie eine E-Mail-Verteilerliste aus der Dropdownliste aus. Sie können auch eine E-Mail-Verteilerliste erstellen, indem Sie auf das Symbol **+** klicken und Details des E-Mail-Servers angeben.

Konfigurationshinweise zur Netzwerkkonfiguration erhalten

February 5, 2024

Sie richten Ihre NetScaler-Instanzen mit optimalen Konfigurationen ein, damit Sie eine optimale Leistung für Ihre Anwendungen erzielen können. Einige Konfigurationen sind jedoch möglicherweise keine Standardkonfigurationen, die sich auf die Leistung Ihrer Anwendungen auswirken können.

Um Sie bei der Optimierung Ihrer Anwendungsleistung zu unterstützen, analysiert NetScaler ADM die Konfiguration der NetScaler-Instanz und gibt Ihnen Empfehlungen. Sie können die empfohlenen Konfigurationen von NetScaler ADM anwenden.

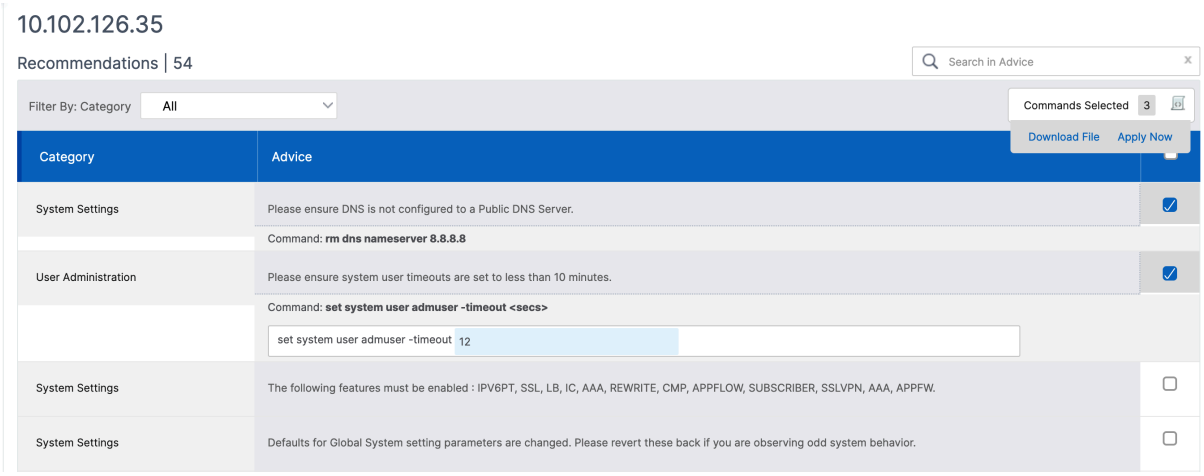
So analysieren Sie die NetScaler-Instanz:

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsaudit > 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 NetScaler Instanz aus, die Sie analysieren möchten.

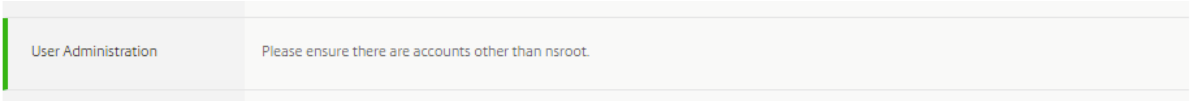
NetScaler ADM analysiert die Konfiguration auf Ihrer Instanz und stellt eine Liste von Konfigurationsempfehlungen bereit, wie in der folgenden Abbildung gezeigt. Klicken Sie auf das Kontrollkästchen neben einer Konfigurationsempfehlung, um die Korrekturbefehle anzuzeigen.



Wenn Sie Ihre Konfiguration aktualisieren möchten, geben Sie die Werte für die Variablen in den Korrekturbefehlen an und klicken Sie auf **Jetzt anwenden** .

> **Hinweis:**
>
> Die hier aufgeführten Befehle sind nur Empfehlungen. Ein Benutzer mit Lese- und Schreibzugriff kann mit dieser Funktion jeden Befehl bearbeiten. Stellen Sie sicher, dass Sie Benutzern einen eingeschränkten privilegierten Zugriff gewähren, von denen Sie glauben, dass sie die Befehle nicht bearbeiten dürfen.

Wenn der Befehl erfolgreich auf der Netzwerkinstanz ausgeführt wurde, verschwindet das Kontrollkästchen neben dem Hinweis.



Wenn Sie die Details der Befehle anzeigen möchten, die auf Ihrer Netzwerkinstanz ausgeführt werden, navigieren Sie zu **Infrastruktur > Instances >**<Instance_Type\> , wählen Sie die IP-Adresse der Instance aus und klicken Sie dann in der Dropdownliste **Aktionen** auf **Ereignisse** anzeigen .

Sehen Sie sich auf der Seite **Ereignisse** die Details der Konfigurationsänderung an.

Konfigurationsprüfung von NetScaler-Instanzen abfragen

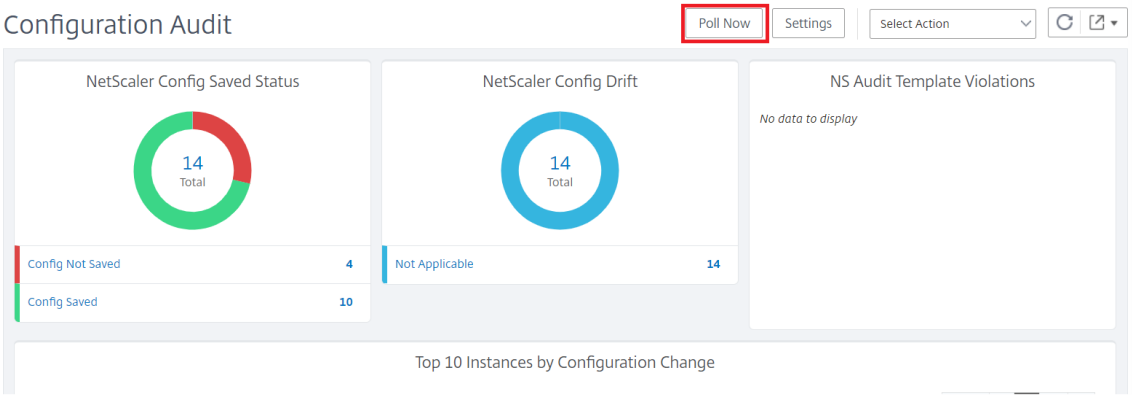
February 5, 2024

NetScaler ADM fragt die Konfigurationsüberprüfungen automatisch alle 10 Stunden ab, um nach Konfigurationsänderungen zu suchen, die auf NetScaler-Instanzen auftreten. Sie können die Konfigurationsprüfungen auch manuell abfragen, um die letzten Änderungen zu erkennen. Das Abrufen aller NetScaler-Instanzen führt jedoch zu einer hohen Belastung des Netzwerks.

Anstatt das gesamte NetScaler-Instanzkonfigurationsaudit abzufragen, können Sie manuell nur die Konfigurationsaudits einer oder mehrerer ausgewählter Instanzen abfragen.

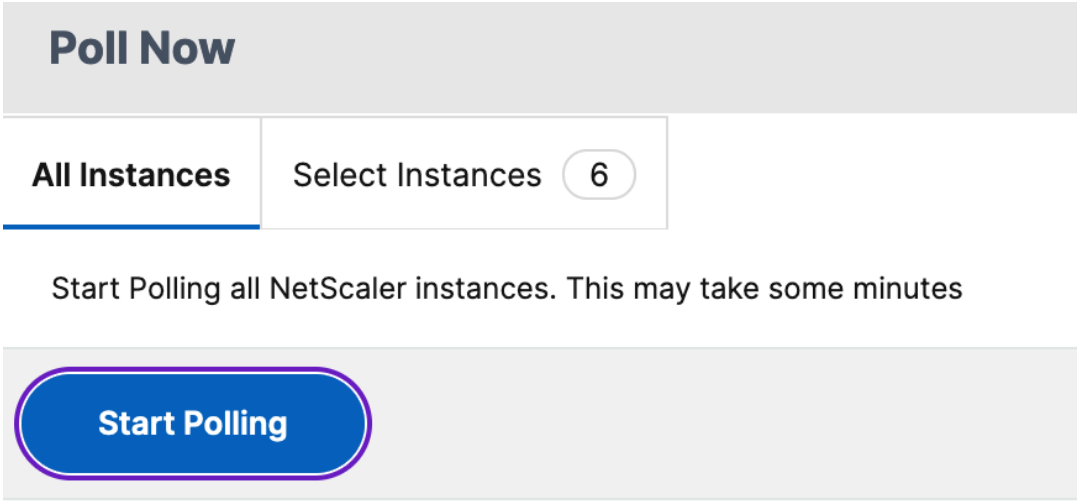
So fragen Sie Konfigurationsaudits von NetScaler-Instanzen ab:

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Konfiguration > Konfigurationsüberprüfung**.
2. Klicken Sie unter **Configuration Audit** auf **Jetzt** abfragen .

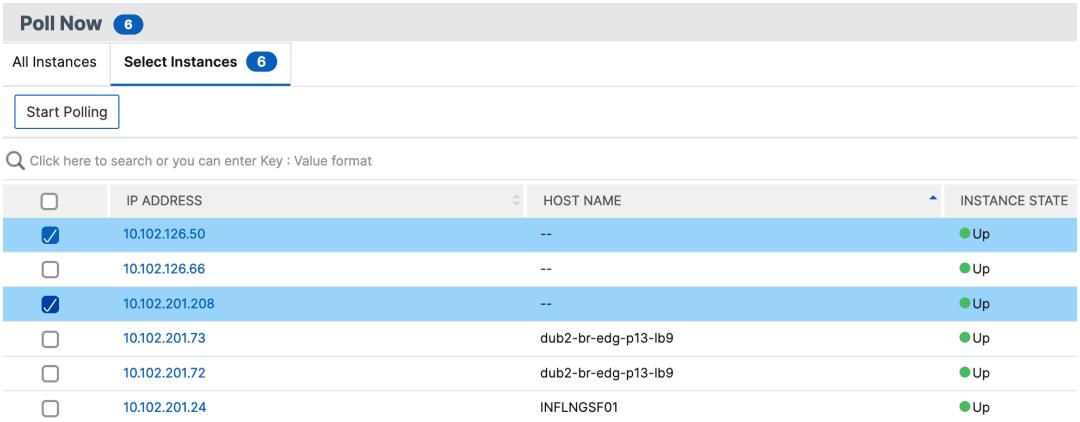


3. Die Seite **Jetzt abfragen** wird geöffnet und bietet Ihnen die Möglichkeit, alle NetScaler-Instanzen im Netzwerk abzufragen oder ausgewählte Instanzen abzufragen.

   a) Um alle NetScaler-Instanzen abzufragen, wählen Sie die Registerkarte **Alle Instanzen**, und klicken Sie auf **Polling starten**.



   b) Um bestimmte Instanzen abzufragen, wählen Sie die Registerkarte**Instanzenauswählen**aus, wählen Sie die Instanzen aus der Liste aus und klicken Sie auf**Jetzt abfragen**.



Konfigurations-Audit-Diff für ConfigChange SNMP-Traps generieren

February 5, 2024

Wenn eine Konfigurationsänderung in einer NetScaler-Instanz im Netzwerk erfolgt, wird die Konfigurationsdatei aktualisiert. Die Instanz sendet einen ConfigChange SNMP-Trap an NetScaler ADM. Sie können NetScaler ADM aktivieren, um eine Konfigurationsüberprüfung für diese Instanz durchzuführen, wenn die Instanz einen ConfigChange SNMP-Trap sendet.

****Wenn es einen Unterschied zwischen der Konfiguration der Prüfungsvorlage und der aktuellen Konfiguration gibt, wird auf der Seite „ Auditbericht "die Statusmeldung Diff Exists angezeigt. Klicken Sie auf den Link **Diff Exists** , um zur Seite **Configuration Diff** zu gelangen, auf der Sie den Korrekturbefehl anzeigen können. Sie können diese fehlerbehebenden Befehle verwenden, um einen Konfigurationsauftrag zu erstellen und diesen auf den spezifischen NetScaler-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 auf NetScaler ADM.

So führen Sie Konfigurationsüberwachungsvorlagen beim Empfang von ConfigChange SNMP-Trap aus:

Mit NetScaler ADM können Sie die Option zum Ausführen der Konfigurationsüberwachungsvorlage in NetScaler ADM aktivieren.

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Konfiguration > Konfigurationsüberprüfung**.
2. Klicken Sie auf der Seite **Konfigurationsüberwachung** auf**Einstellungen**.

3. Wählen Sie **Prüfung bei Empfang des Ereignisses „NetScalerConfigChange“durchführen** aus.

> **Hinweis:**
>
> NetScaler ADM führt eine Konfigurationsüberprüfung für jede Instanz durch, die in Zukunft die NetScalerConfigChange SNMP-Traps empfängt.

1. **Geben Sie im Feld Zeitverzögerung für die Ausführung der Prüfungsvorlage (in Minuten) die Minuten ein. NetScaler ADM führt die Konfigurationsüberwachungsvorlage auf der NetScaler-Instanz nach dieser Zeitverzögerung aus, wenn sie das ConfigChange-SNMP-Trap von dieser Instanz empfängt.

Konfigurationsaudit

February 5, 2024

Dieses Dokument enthält Themen zu folgenden Themen:

- Auditberichte anzeigen
- Konfigurationsänderungen über alle Instanzen hinweg überwachen
- Konfigurationshinweise zur Netzwerkkonfiguration erhalten
- Konfigurationsprüfung von NetScaler-Instanzen abfragen
- Konfigurations-Audit-Diff für ConfigChange SNMP-Traps generieren

Upgradeaufträge

February 5, 2024

Sie können die folgenden Wartungsaufgaben mit NetScaler ADM erstellen. Anschließend können Sie die Wartungsaufgaben zu einem bestimmten Datum und einer bestimmten Uhrzeit planen.

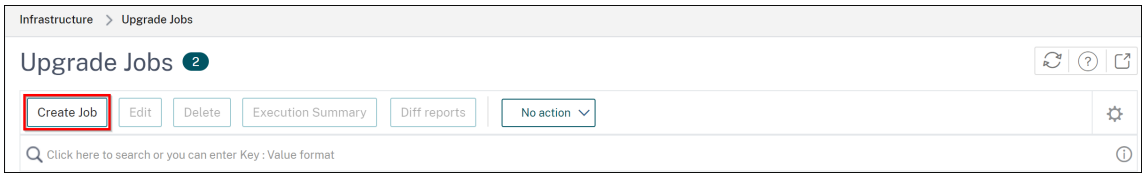
- Upgrade von NetScaler-Instanzen
- Upgrade von NetScaler SDX-Instanzen
- Aktualisieren Sie NetScaler BLX-Instanzen
- Aktualisieren von NetScaler-Instanzen in der Autoscale-Gruppe

- Konfigurieren des HA-Paares von NetScaler-Instanzen
- HA-Instanzpaar in Cluster konvertieren

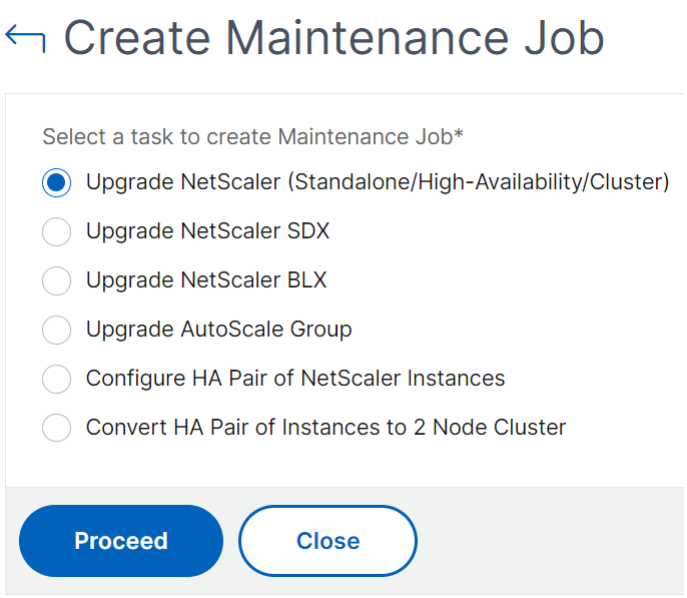
> **Hinweis:**
>
> Wenn ein Upgrade-Job fehlschlägt, entfernt NetScaler ADM die Build-Dateien und andere extrahierte Dateien, um sicherzustellen, dass NetScaler-Instanzen über ausreichend Speicherplatz für den nächsten Upgrade-Versuch verfügen.

Planen des Upgrades von NetScaler-Instanzen

1. Gehen Sie zu **Infrastruktur > Upgrade-Jobs**. Klicken Sie auf **Job erstellen**.

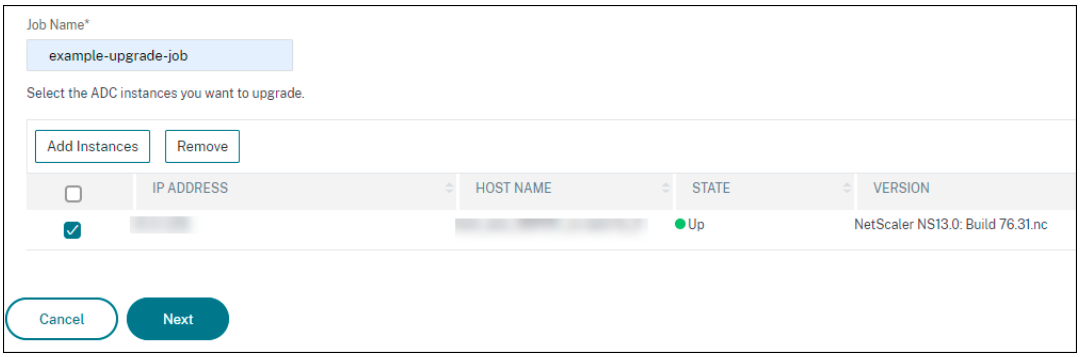


2. Wählen Sie unter **Wartungsaufträge erstellen**die Option **NetScaler (Standalone/Hochverfügbarkeit/Cluster) aktualisieren** aus und klicken Sie auf **Fortfahren**.



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 das Image auszuwählen. Wählen Sie eine der folgenden Optionen aus der Liste **Software-Image** aus:

   - **Lokal** —Wählen Sie die Instanzupgradedatei von Ihrem lokalen Computer
   - **Appliance** - Wählen Sie die Instanzupgradedatei im NetScaler ADM-Dateibrowser aus. Die NetScaler ADM-GUI zeigt die Instanzdateien an, die unter `/var/mps/mps_images` vorhanden sind.
     - **Image-Upload auf ADC überspringen, wenn das ausgewählte Image bereits verfügbar ist** —Wählen Sie diese Option aus, wenn das Image bereits in der NetScaler-Instanz vorhanden ist.
     - **Software-Image von NetScaler bei erfolgreichem Upgrade bereinigen**: Wählen Sie diese Option, um das hochgeladene Image in der ADC-Instanz nach dem Instanz-Upgrade zu löschen.

6. Klicken Sie auf **Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten.

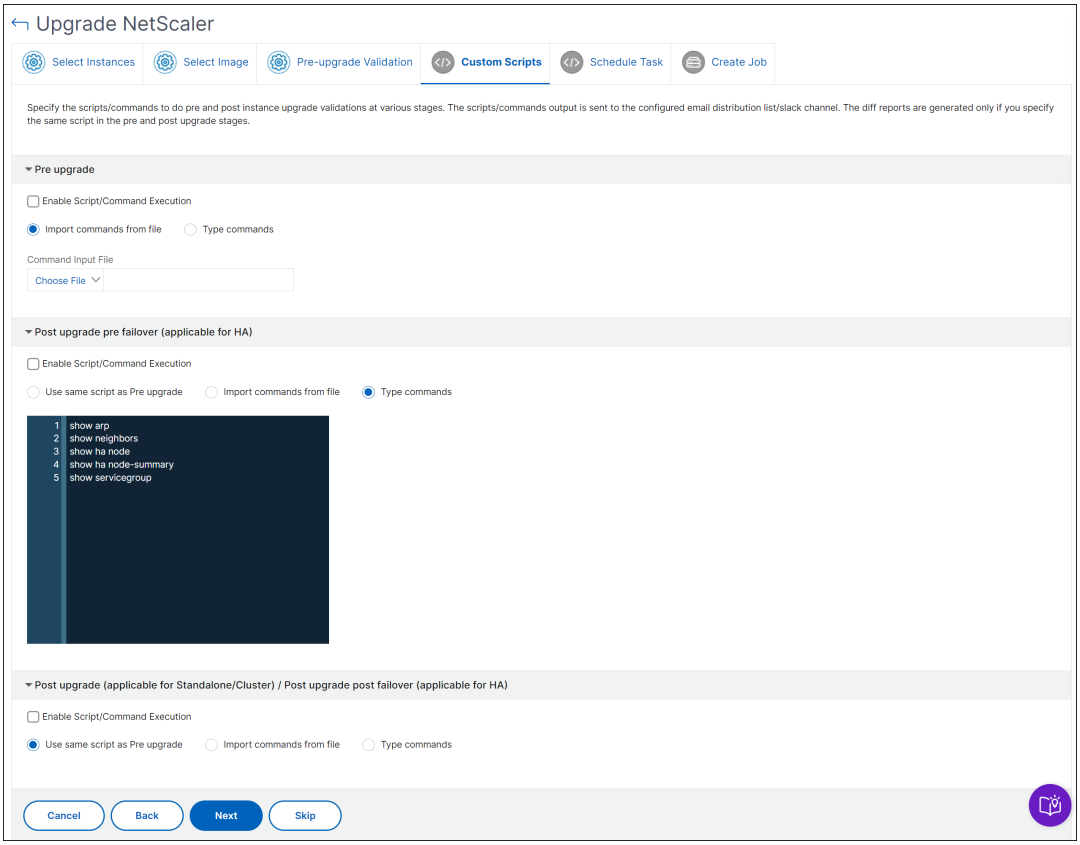
   Auf der Registerkarte **Überprüfung vor dem Upgrade** werden die ausgefallenen Instanzen angezeigt Entfernen Sie die fehlerhaften Instanzen und klicken Sie auf **Weiter**

   > **Wichtig!**
   >
   > Wenn Sie die Cluster-IP-Adresse angeben, führt NetScaler ADM die Überprüfung vor dem Upgrade nur für die angegebene Instanz durch, nicht auf den anderen Clusterknoten.

7. 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 Skripts 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 Statistik der virtuellen Server und Dienste.
- Die dynamischen Routen.

8. Klicken Sie auf **Weiter**. 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 **Zweistufiges Upgrade für Knoten in HA durchführen**aus.

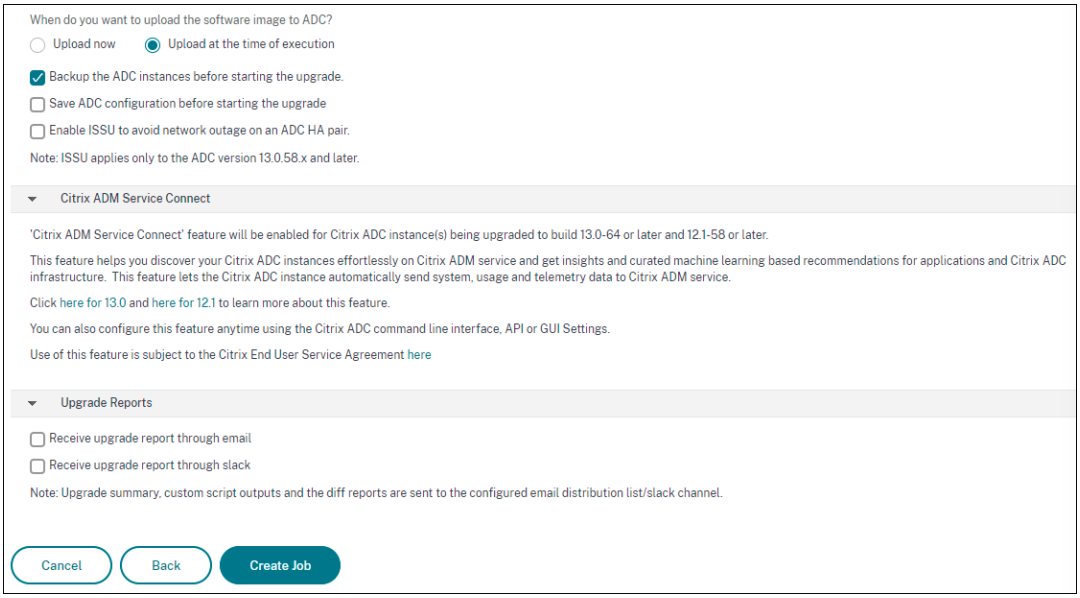
Geben Sie das **Ausführungsdatum** und die **Startzeit an**, zu der Sie eine andere Instanz im HA-Paar aktualisieren möchten.

9. Klicken Sie auf **Weiter**. Geben Sie unter **Job erstellen** die folgenden Details an:

   a) Geben Sie an, wann Sie das Image auf 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 des Ausführens** - Wählen Sie diese Option, um das Image hochzuladen, wenn der Upgradeauftrag ausgeführt wird.
      - **Erstellen Sie ein Backup der ADC-Instanzen, bevor Sie das Upgrade starten.** - Erstellt ein Backup der ausgewählten ADC-Instanzen.
      - **Speichert die ADC-Konfiguration vor dem Start des Upgrades** - Speichert die Konfigurationsaufträge, die vor dem Upgrade auf der Instanz konfiguriert wurden.
      - **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.

   - **NetScaler ADM Service Connect** —Wenn Sie ein Upgrade auf Build **13.0-64 oder höher** und **12.1-58 oder höher**durchführen, wird NetScaler ADM Service Connect automatisch aktiviert. Weitere Informationen finden Sie unter Berührungsarmes Onboarding von NetScaler-Instanzen mit NetScaler ADM Service Connect.
   - **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 findest du unter Erstellen eines Slack-Profils.



10. Klicken Sie auf **Job erstellen**.

Planen des Upgrades von NetScaler SDX-Instanzen

1. Gehen Sie zu **Infrastruktur > Upgrade-Jobs**. Klicken Sie auf **Job erstellen**.
2. Wählen Sie **NetScaler SDX aktualisieren** und klicken Sie auf **Weiter**.
3. Klicken Sie auf der Seite **Upgrade von NetScaler SDX** auf der Registerkarte **Instanzauswahl**:
   a) Fügen Sie einen **Aufgabennamen**hinzu.
   b) Wählen Sie in der Liste **Software-Image** entweder **Lokal** (Ihr lokaler Computer) oder **Appliance** (die Builddatei muss auf der virtuellen NetScaler ADM-Appliance vorhanden sein).

      Der Upload-Prozess beginnt.
   c) Fügen Sie die NetScaler 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 NetScaler SDX-Instanz jetzt zu aktualisieren, und klicken Sie auf **Fertig stellen**.
5. Um eine NetScaler 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 NetScaler-Instanz auswählen und auf **Fertig stellen**klicken.
6. Sie können auch E-Mail- und Slack-Benachrichtigungen aktivieren, um den Ausführungsbericht der aktualisierten NetScaler SDX-Instanz zu erhalten. **Klicken Sie auf das Kontrollkästchen**

Ausführungsbericht per E-Mailempfangen und Ausführungsbericht über Slack empfangen, um die Benachrichtigungen zu aktivieren.

Weitere Informationen zum Konfigurieren der E-Mail-Verteilerliste und des Slack-Channels finden Sie in **Schritt 8** unter Planen des Upgrades von NetScaler-Instanzen.

Planen Sie das Upgrade von NetScaler BLX-Instanzen

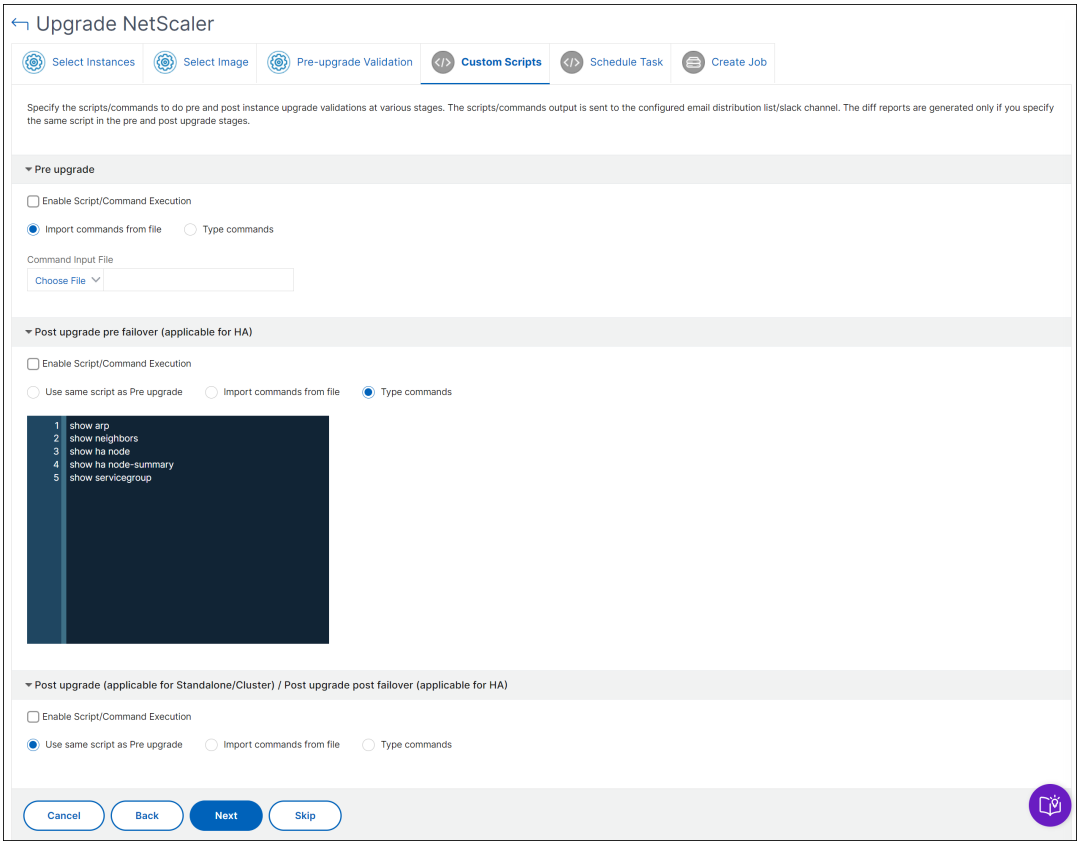
1. Gehen Sie zu **Infrastruktur > Upgrade-Jobs**. Klicken Sie auf **Job erstellen**.
2. Wählen **Sie unter Wartungsjobs erstellen**die Option **NetScaler BLX aktualisieren** aus und klicken Sie auf **Fortfahren**.
3. Geben Sie unter **Instanz auswählen**einen Namen Ihrer Wahl für **Auftragsname ein**.
4. Klicken Sie auf **Instanzen hinzufügen**, um die BLX-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 das Image auszuwählen. Wählen Sie eine der folgenden Optionen aus der Liste **Software-Image** aus:
   - **Lokal** —Wählen Sie die Instanzupgradedatei von Ihrem lokalen Computer
   - **Appliance** - Wählen Sie die Instanzupgradedatei im NetScaler ADM-Dateibrowser aus. Die NetScaler ADM-GUI zeigt die Instanzdateien an, die unter `/var/mps/mps_images` vorhanden sind.
     - **Image-Upload auf ADC überspringen, wenn das ausgewählte Image bereits verfügbar ist** —Wählen Sie diese Option aus, wenn das Image bereits in der NetScaler-Instanz vorhanden ist.
     - **Software-Image von NetScaler bei erfolgreichem Upgrade bereinigen**: Wählen Sie diese Option, um das hochgeladene Image in der ADC-Instanz nach dem Instanz-Upgrade zu löschen.
6. Klicken Sie auf **Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten.

   Auf der Registerkarte **Überprüfung vor dem Upgrade** werden die ausgefallenen Instanzen angezeigt Entfernen Sie die fehlerhaften Instanzen und klicken Sie auf **Weiter**

> **Wichtig!**
>
> Wenn Sie die Cluster-IP-Adresse angeben, führt NetScaler ADM die Überprüfung vor dem Upgrade nur für die angegebene Instanz durch, nicht auf den anderen Clusterknoten.

7. 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 Skripts 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 Statistik der virtuellen Server und Dienste.

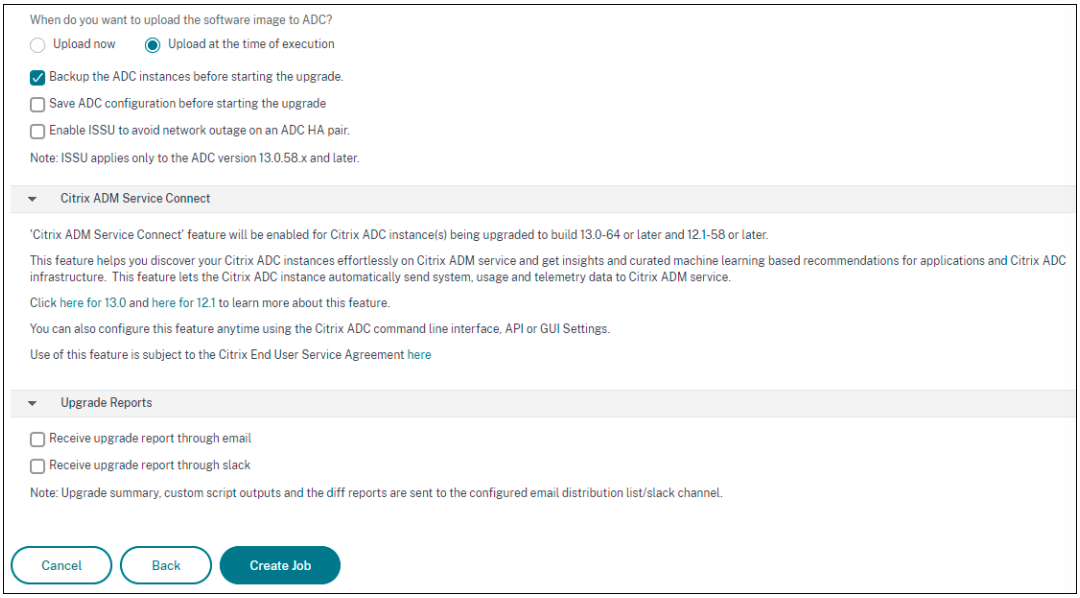
- Die dynamischen Routen.

8. Klicken Sie auf **Weiter**. 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 HA-Paar in zwei Stufen aktualisieren möchten, wählen Sie **Zweistufiges Upgrade für Knoten in HA durchführen**aus.

     Geben Sie das **Ausführungsdatum** und die **Startzeit an**, zu der Sie eine andere Instanz im HA-Paar aktualisieren möchten.
9. Klicken Sie auf **Weiter**. Geben Sie unter **Job erstellen** die folgenden Details an:
   a) Geben Sie an, wann Sie das Image auf 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 des Ausführens** - Wählen Sie diese Option, um das Image hochzuladen, wenn der Upgradeauftrag ausgeführt wird.
      - **Backup der ADC-Instanzen erstellen, vor dem Starten des Upgrades** - Erstellt ein Backup ausgewählten ADC-Instanzen.
      - **Speichert die ADC-Konfiguration vor dem Start des Upgrades** - Speichert die Konfigurationsaufträge, die vor dem Upgrade auf der Instanz konfiguriert wurden.
      - **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.
   - **NetScaler ADM Service Connect** —Wenn Sie ein Upgrade auf Build **13.0-64 oder höher** und **12.1-58 oder höher**durchführen, wird NetScaler ADM Service Connect automatisch aktiviert. Weitere Informationen finden Sie unter Berührungsarmes Onboarding von NetScaler-Instanzen mit NetScaler ADM Service Connect.
   - **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 findest du unter Erstellen eines Slack-Profils.



10. Klicken Sie auf **Job erstellen**.

Ein Upgrade der Autoscale-Gruppe planen

Führen Sie die folgenden Schritte aus, um alle Instanzen in den Clouddiensten zu aktualisieren, die Teil der Autoscale-Gruppe sind:

1. Gehen Sie zu **Infrastruktur > Upgrade-Jobs**. Klicken Sie auf **Job erstellen**.
2. Wählen Sie **Autoscale-Gruppe aktualisieren** aus und klicken Sie auf **Weiter**.
3. Auf der Registerkarte **Upgradeeinstellungen**:
   a) Wählen Sie die **Autoscale-Gruppe** aus, die Sie aktualisieren möchten.
   b) Wählen Sie unter **Image** die NetScaler-Version aus. Dieses Image ist die vorhandene Version von NetScaler-Instanzen in der Autoscale-Gruppe.
   c) Durchsuchen Sie in **NetScaler Image**die NetScaler Versionsdatei, auf die Sie ein Upgrade durchführen möchten.

      Wenn Sie **Graceful Upgrade**aktivieren, wartet die Upgrade-Aufgabe, bis der angegebene Zeitraum für die Drain-Verbindung abgelaufen ist.
   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 die NetScaler-Instanzen sofort zu aktualisieren.
- **Später:** Um das Upgrade der NetScaler-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. **Klicken Sie auf das Kontrollkästchen Ausführungsbericht per E-Mailempfangen und Ausführungsbericht über Slack** empfangen, um die Benachrichtigungen zu aktivieren.

5. Klicken Sie auf **Fertig stellen**.

Planen der Konfiguration des HA-Paares von NetScaler-Instanzen

1. Gehen Sie zu **Infrastruktur > Upgrade-Jobs**. Klicken Sie auf **Job erstellen**.
2. Wählen Sie **HA Pair of NetScaler-Instanzen konfigurieren** und klicken Sie auf **Proceed**.
3. Klicken Sie auf der Seite **NetScaler HA-Paar** auf der Registerkarte **Instanzauswahl**:

   a) Fügen Sie einen **Aufgabennamen**hinzu.

   b) Wählen Sie die primäre IP-Adresse aus. Klicken Sie auf **OK**.

   c) Geben Sie das Kennwort für den primären RPC-Knoten ein.

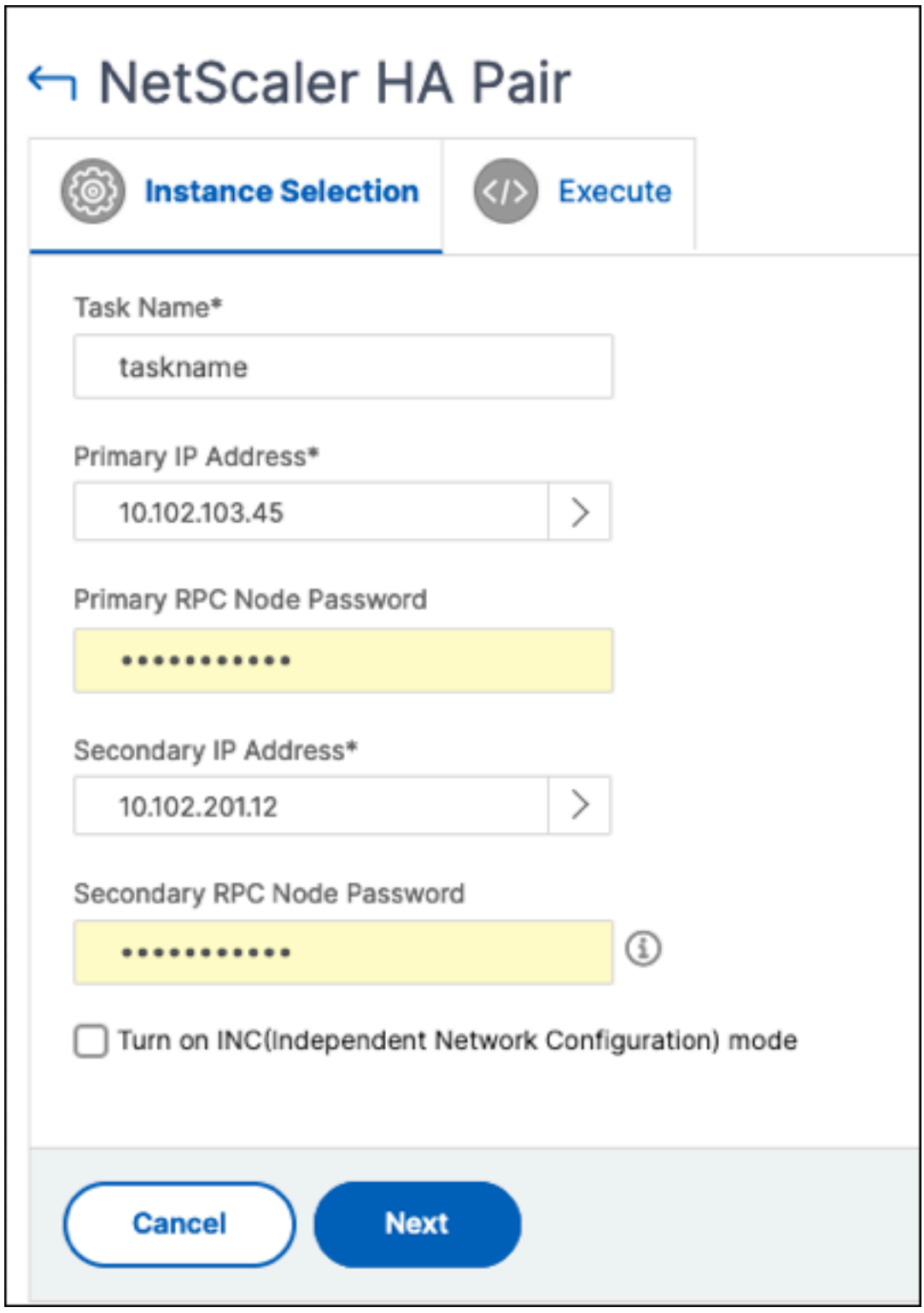
   d) Wählen Sie die sekundäre IP-Adresse aus. Klicken Sie auf **OK**.

   > **Hinweis:**
   >
   > Die Kennwortfelder für den RPC-Knoten sind in NetScaler Version 14.1 und höher verfügbar.

   e) Geben Sie das Kennwort für den sekundären RPC-Knoten ein.

   f) Klicken Sie hier, um **den INC-Modus (Independent Network Configuration)** zu aktivieren, wenn die HA-Paarinstanzen in zwei Subnetzen vorhanden sind.

   g) Klicken Sie auf **Weiter**.



4. Wählen Sie auf der Registerkarte **Task planen** in der Liste **Ausführungsmodus** die Option **Jetzt** aus, um eine NetScaler-Instanz jetzt zu aktualisieren, und klicken Sie auf **Fertig stellen**.
5. Um später ein NetScaler HA-Paar zu aktualisieren, wählen Sie **Später** aus der Liste **Aus-**

führungsmodus aus. Anschließend können Sie das Ausführungsdatum und die Startzeit für das Upgrade der NetScaler-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. **Klicken Sie auf das Kontrollkästchen Ausführungsbericht per E-Mailempfangen und Ausführungsbericht über Slack** empfangen, um die Benachrichtigungen zu aktivieren.

   Weitere Informationen zum Konfigurieren der E-Mail-Verteilerliste und des Slack-Channels finden Sie in **Schritt 8** unter Planen des Upgrades von NetScaler-Instanzen.

Planen Sie die Konvertierung von HA-Instanzen in Cluster

1. Gehen Sie zu **Infrastruktur > Upgrade-Jobs**. Klicken Sie auf **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 NetScaler-Instanz jetzt zu aktualisieren, und klicken Sie auf **Fertig stellen**.
5. Um später zu aktualisieren, wählen Sie **Später** aus der Liste **Ausführungsmodus** aus. Anschließend können Sie das **Ausführungsdatum** und die **Startzeit** für das Upgrade der NetScaler HA-Paarinstanz auswählen und auf **Fertig stellen**klicken.
6. Sie können auch E-Mail- und Slack-Benachrichtigungen aktivieren, um den Ausführungsbericht für das Upgrade einer NetScaler SDX-Instanz zu erhalten. **Klicken Sie auf das Kontrollkästchen Ausführungsbericht per E-Mailempfangen und Ausführungsbericht über Slack** empfangen, um die Benachrichtigungen zu aktivieren.

   Weitere Informationen zur Konfiguration der E-Mail-Verteilerliste und des Slack-Channels finden Sie in **Schritt 8** unter Planen des Upgrades von NetScaler-Instanzen .

Aufträge zum Upgrade von NetScaler-Instanzen verwenden

February 5, 2024

Sie können NetScaler Application Delivery Management (ADM) verwenden, um eine oder mehrere NetScaler-Instances zu aktualisieren. Sie müssen das Lizenzierungsframework und die Lizenztypen kennen, bevor Sie eine Instanz aktualisieren.

Wenn Sie Ihre NetScaler-Instanz durch Erstellen eines Wartungsauftrags aktualisieren, führen Sie die Vorvalidierungsprüfung für die Instanzen 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 die Festplattenauslastung** —Wenn der `/var` Ordner weniger als 6 GB Speicherplatz hat und der `/flash` Ordner weniger als 200 MB Speicherplatz hat, bereinigen Sie den Speicherplatz. Überprüfen Sie die folgenden Ordnerpfade, um den Speicherplatz zu leeren:
   - `/var/nstrace`
   - `/var/log`
   - `/var/nslog`
   - `/var/tmp/support`
   - `/var/core`
   - `/var/crash`
   - `/var/nsinstall`
   - `/var/netscaler/nsbackup`
3. **Überprüfen Sie auf Datenträger-Hardwareprobleme** - Beheben Sie ggf. die Hardwareprobleme.

Sie können ein NetScaler HA-Paar in zwei Schritten aktualisieren:

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.

Beachten Sie beim Upgrade eines NetScaler HA-Paars Folgendes:

- Der sekundäre Knoten wird zuerst aktualisiert.
- Synchronisation und Weitergabe der Knoten werden deaktiviert, bis beide Knoten erfolgreich aktualisiert wurden.
- Nach dem erfolgreichen HA-Paar-Upgrade erscheint eine Fehlermeldung in der Ausführungshistorie. Diese Meldung wird angezeigt, wenn sich Ihre Knoten im HA-Paar auf unterschiedlichen Builds oder Versionen befinden. Diese Meldung zeigt an, dass die Synchronisierung zwischen primären und sekundären Knoten deaktiviert ist.

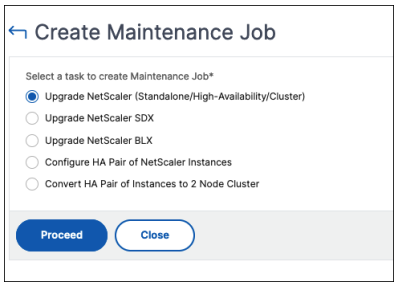
Wenn Sie einen NetScaler-Cluster aktualisieren, führt der ADM die Validierung vor dem Upgrade nur für die angegebene Instanz durch. Überprüfen und beheben Sie vor dem Upgrade die Probleme mit Anpassungen, Festplattenauslastung und Hardwareproblemen auf den Clusterknoten.

Erstellen Sie einen Upgrade-Wartungsauftrag, um NetScaler-Instanzen zu aktualisieren

> **Hinweis**
>
> NetScaler-Upgrade von einer höheren Version auf eine niedrigere Version wird nicht unterstützt. Wenn Ihre NetScaler-Instanz beispielsweise 13.0 82.x ist, können Sie die NetScaler-Instanz nicht auf 13.0 79.x oder eine andere frühere Version herunterstufen.

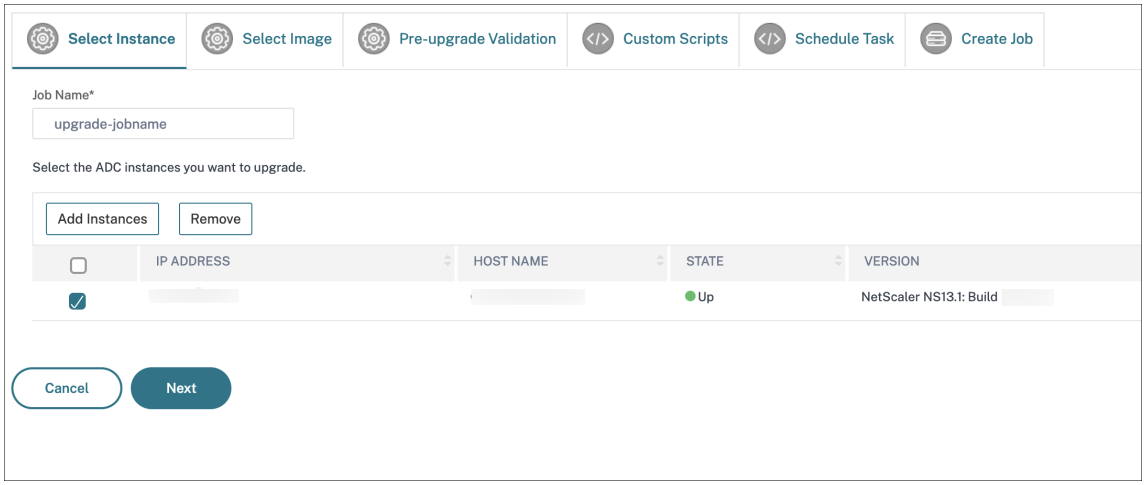
1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Upgrade-Jobs**. Klicken Sie auf die Schaltfläche **Job erstellen**.

2. Wählen Sie unter **Wartungsaufträge erstellen**die Option **NetScaler (Standalone/Hochverfügbarkeit/Cluster) aktualisieren** aus und klicken Sie auf **Fortfahren**.



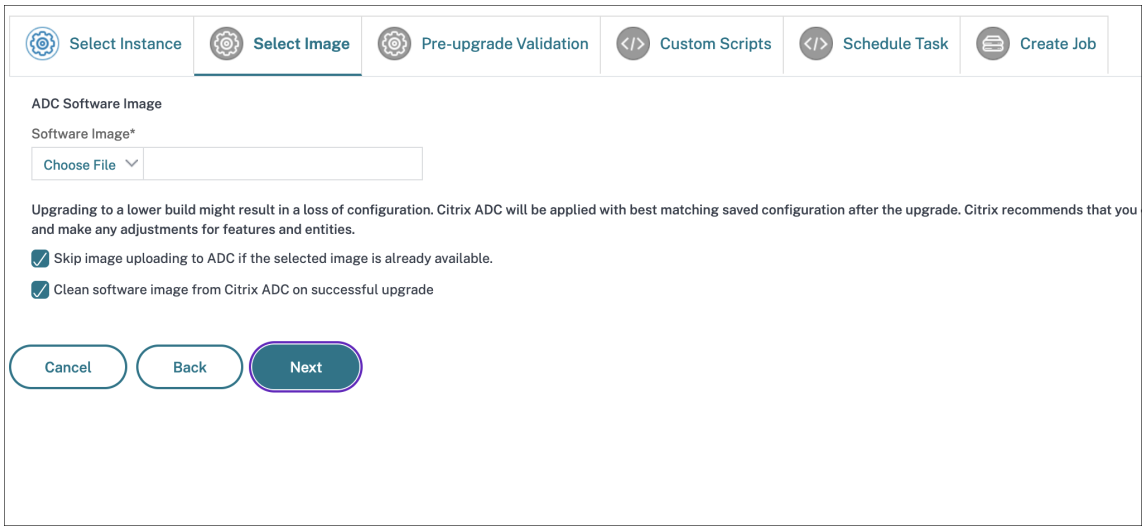
3. Geben Sie unter **Instanz auswählen**einen Namen Ihrer Wahl für **Auftragsname ein**.
4. Klicken Sie auf **Instanzen hinzufügen**, um NetScaler-Instanzen hinzuzufügen, die Sie aktualisieren möchten.
    - Um ein NetScaler-Hochverfügbarkeitspaar zu aktualisieren, wählen Sie die IP-Adressen des Hochverfügbarkeitspaars aus (gekennzeichnet durch das hochgestellte Zeichen ‘S’ und ‘P’).

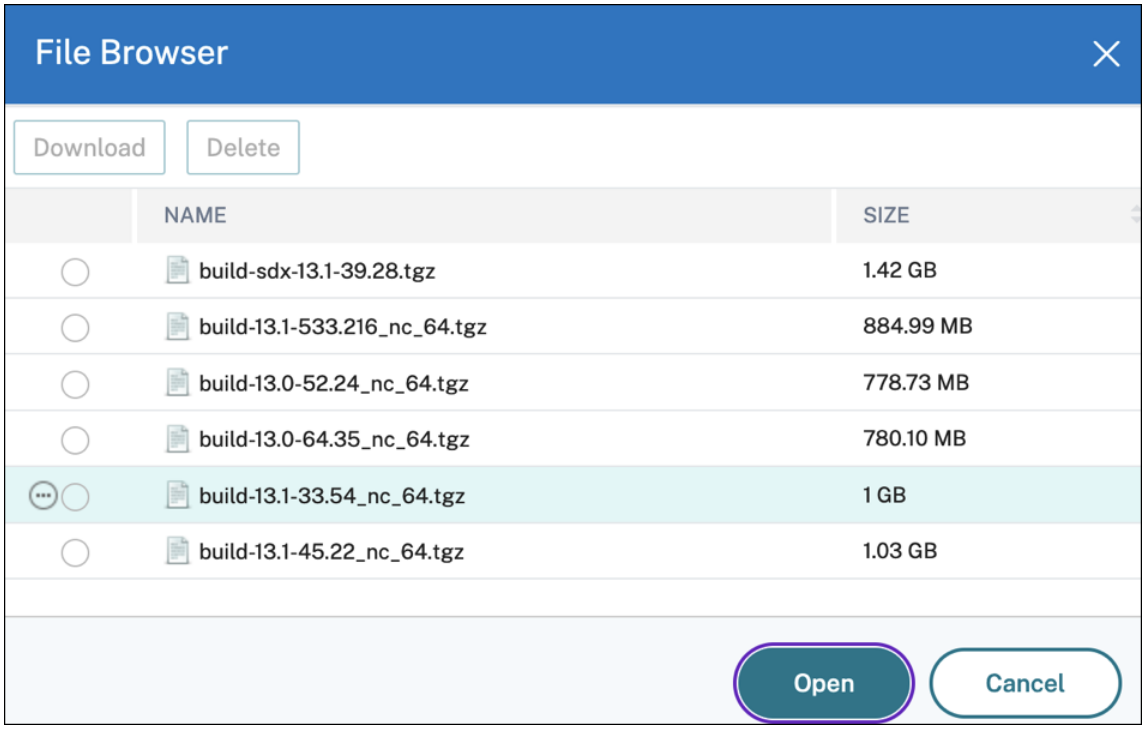
- Um einen Cluster zu aktualisieren, wählen Sie die Cluster-IP-Adresse aus (gekennzeichnet durch das hochgestellte Zeichen von ‘C’).



5. Wählen Sie auf der Registerkarte **Select Image** ein NetScaler-Image von Ihrem lokalen Laufwerk oder aus den Build-Images aus.

   - **Lokal** —Wählen Sie die Instanzupgradedatei von Ihrem lokalen Computer
   - **Appliance** —Wählen Sie die Instance-Upgrade-Datei in einem NetScaler ADM-Dateibrowser aus. Die NetScaler ADM-GUI zeigt die Instanzdateien an, die unter `/var/mps/ns_images` vorhanden sind.





- **Überspringen Sie das Hochladen von Bildern auf NetScaler, wenn das ausgewählte Image bereits verfügbar ist** —Diese Option überprüft, ob das ausgewählte Image in NetScaler verfügbar ist. Beim Upgrade-Job wird das Hochladen eines neuen Images übersprungen und das in NetScaler verfügbare Image verwendet.
- **Software-Image von NetScaler bei erfolgreichem Upgrade bereinigen** —Diese Option löscht das hochgeladene Image in der NetScaler-Instanz nach dem Instanz-Upgrade.

Klicken Sie auf **Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten.

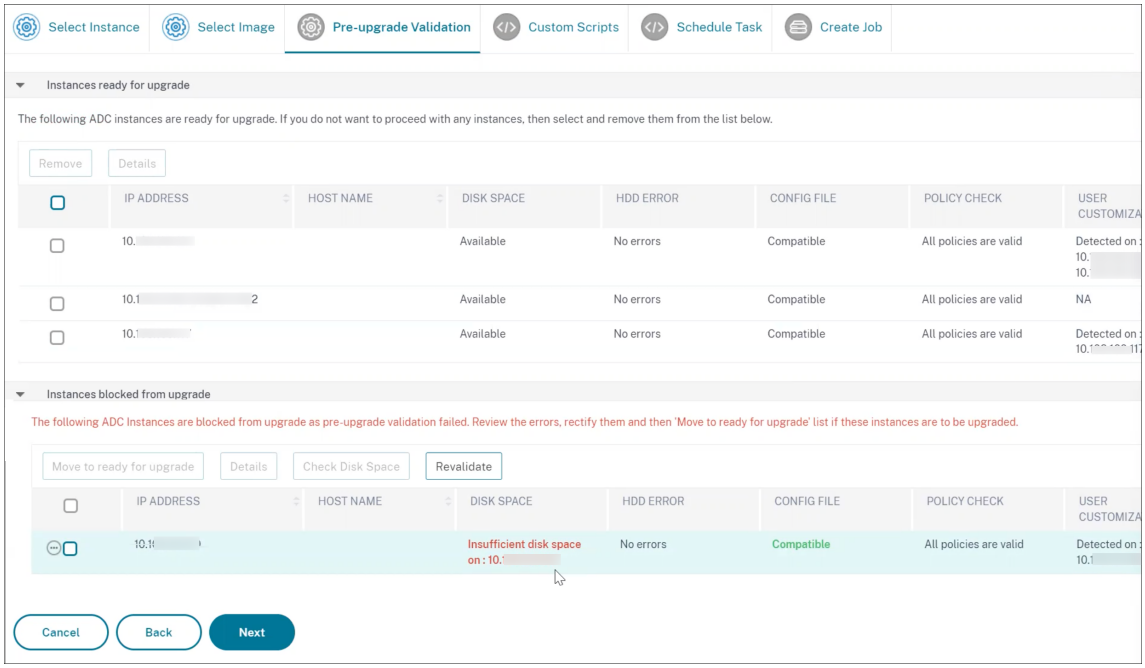
> **Hinweis:**
>
> - Die heruntergeladenen NetScaler-Images werden im NetScaler ADM Agent gespeichert und sind in `/var/mps/adcimages` vorhanden. Diese zwischengespeicherten Images können für mehrere NetScaler-Upgrades verwendet werden, sodass Sie nicht jedes Mal ein Image für ein Upgrade herunterladen müssen.
> - NetScaler ADM löscht die zwischengespeicherten NetScaler-Images alle drei Tage, basierend auf dem Zeitpunkt der letzten Änderung der Images. Im NetScaler ADM Agent werden jeweils nur die letzten beiden Imagedateien zwischengespeichert.

6. Auf der Registerkarte **Pre-upgrade validation** werden die folgenden Abschnitte angezeigt:

   - **Instanzen, die für das Upgrade bereit sind**. Sie können mit dem Upgrade dieser Instanzen fortfahren.

- **Für das Upgrade blockierte Instanzen**. Diese NetScaler-Instanzen sind aufgrund von Validierungsfehlern vor dem Upgrade für das Upgrade gesperrt.

  Sie können die Fehler überprüfen, korrigieren und dann für das Upgrade auf **Move to ready for upgrade** klicken. Wenn Sie auf einer Instanz nicht genügend Speicherplatz haben, können Sie den Speicherplatz überprüfen und bereinigen. Siehe NetScaler-Speicherplatz bereinigen.



- **Richtlinienprüfung**: Wenn NetScaler ADM nicht unterstützte klassische Richtlinien findet, können Sie diese Richtlinien entfernen, um einen Upgrade-Auftrag zu erstellen.

> **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.

7. 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:

   Die benutzerdefinierten Skripts werden verwendet, um die Änderungen vor und nach einem NetScaler-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 Statistik der virtuellen Server und Dienste.

- Die dynamischen Routen.

Ein Instanz-Upgrade hat mehrere Phasen. Sie können jetzt festlegen, dass diese Skripte in den folgenden Phasen ausgeführt werden:

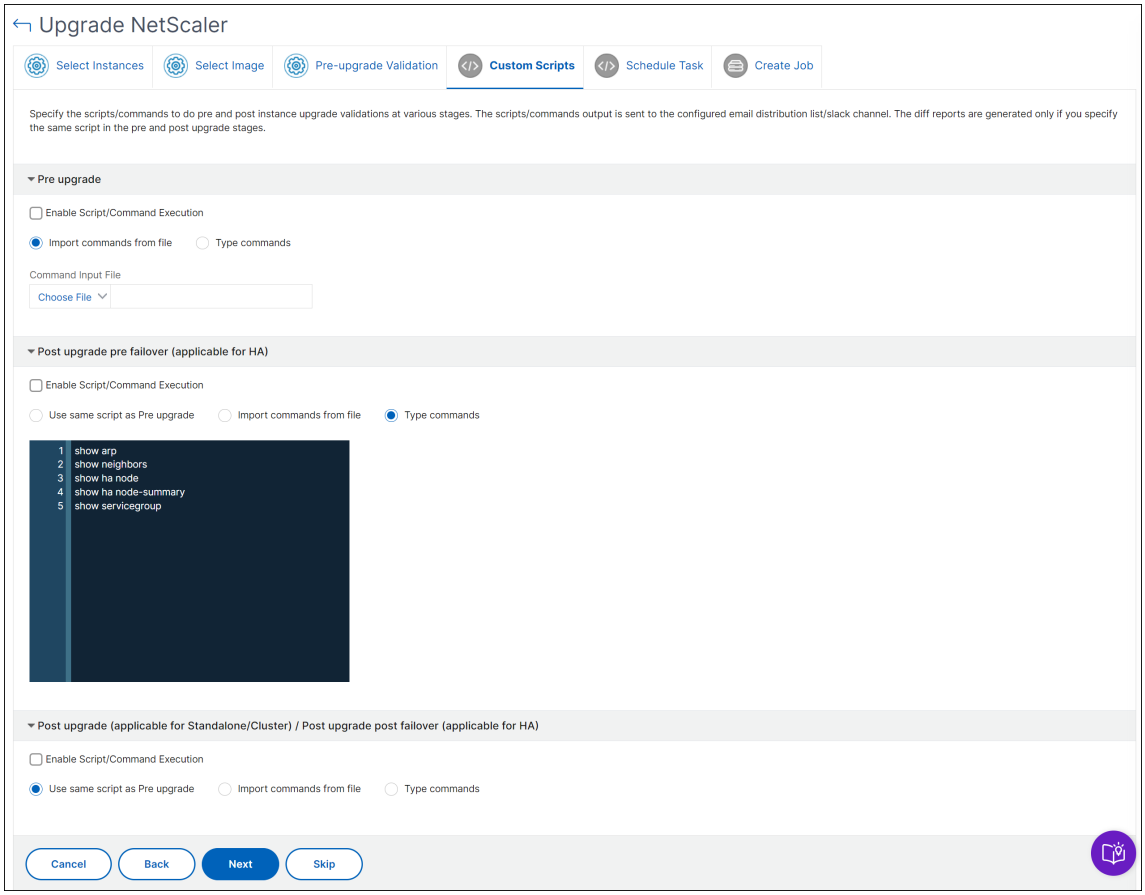
- **Vor dem Upgrade**: Das angegebene Script wird vor dem Upgrade einer Instanz ausgeführt.
- **Vorab-Failover nach dem Upgrade (gilt für HA)**: Diese Phase gilt nur für die Bereitstellung mit hoher Verfügbarkeit. Das angegebene Skript wird nach dem Upgrade der Knoten, jedoch vor ihrem Failover ausgeführt.
- **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.

> **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.

- **Befehle aus Datei importieren**: Wählen Sie die Befehlseingabedatei von Ihrem lokalen Computer aus.
- **Befehle eingeben**: Geben Sie die 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.



8. 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 NetScaler HA-Paar in zwei Schritten aktualisieren möchten, wählen Sie **Zweistufiges Upgrade für Knoten in HA durchführen**aus.

     Geben Sie das **Ausführungsdatum** und die **Startzeit an**, zu der Sie eine andere Instanz im HA-Paar aktualisieren möchten.

9. Geben Sie unter **Job erstellen** die folgenden Details an:

   a) Wählen Sie eine der folgenden Optionen aus der Liste **Software-Image** aus:

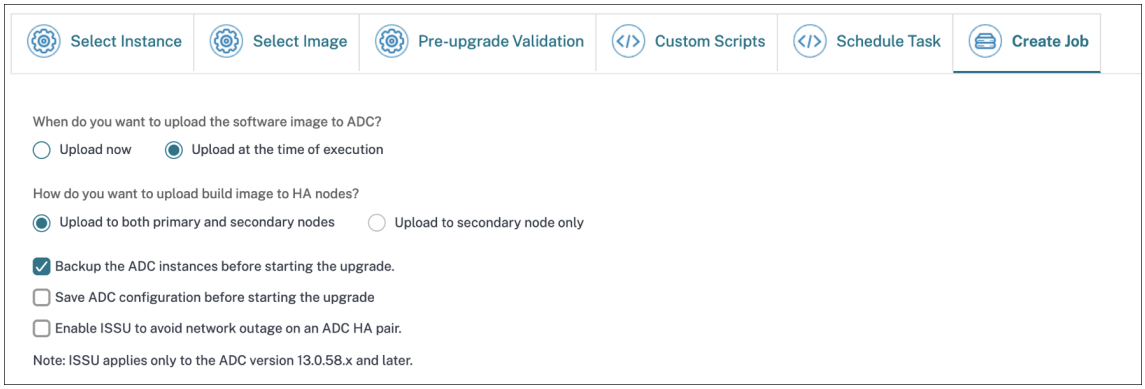
      - **Lokal** —Wählen Sie die Instanzupgradedatei von Ihrem lokalen Computer
      - **Appliance** —Wählen Sie die Instance-Upgrade-Datei in einem ADM-Dateibrowser aus. Die ADM-GUI zeigt die Instanzdateien an `/var/mps/mps_images`, die vorhanden sind.

b) Geben Sie an, wann Sie das Image auf 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 des Ausführens** - Wählen Sie diese Option, um das Image hochzuladen, wenn der Upgradeauftrag ausgeführt wird.

Für ein Hochverfügbarkeitspaar können Sie die Knoten angeben, auf die Sie das Image hochladen möchten:

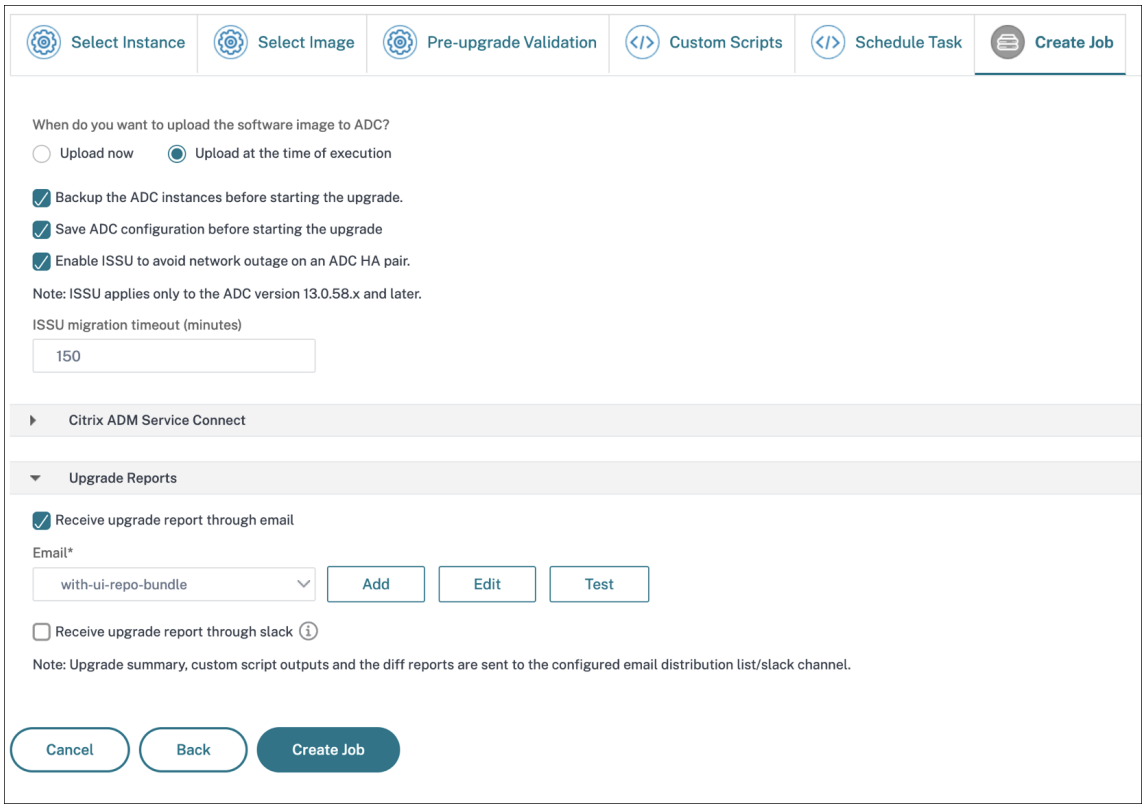
- **Sowohl auf den primären als auch auf den sekundären Knoten hochladen**: Laden Sie die Build-Image-Datei sowohl auf den primären als auch auf den sekundären Knoten hoch.
- **Nur auf den sekundären Knoten hochladen**: Laden Sie die Build-Image-Datei nur auf den sekundären Knoten hoch. Nach dem Upgrade des sekundären Knotens erfolgt ein Failover und die Build-Image-Datei wird auf den neuen sekundären Knoten hochgeladen, der zuvor der primäre Knoten war.



Weitere Informationen zu den verfügbaren Planungsszenarien für Hochverfügbarkeitspaare finden Sie unter Planung von Upgrade-Jobs für Hochverfügbarkeitspaare.

- **Software-Image von NetScaler bei erfolgreichem Upgrade bereinigen** —Wählen Sie diese Option, um das hochgeladene Image in der NetScaler-Instanz nach dem Instanzupgrade zu löschen.
- **Erstellen Sie ein Backup der NetScaler-Instanzen, bevor Sie das Upgrade starten.** - Erstellt ein Backup der ausgewählten NetScaler-Instanzen.
- **Den primären und sekundären Status der HA-Knoten nach dem Upgrade beibehalten**: Wählen Sie diese Option, wenn der Upgrade-Job nach dem Upgrade jedes Knotens einen Failover starten soll. Auf diese Weise behält der Upgrade-Job den primären und sekundären Status der Knoten bei.
- **NetScaler-Konfiguration speichern, bevor das Upgrade gestartet wird** —Speichert die laufende NetScaler-Konfiguration, bevor die NetScaler-Instanzen aktualisiert werden.

- **Aktivieren Sie ISSU, um Netzwerkausfälle auf dem NetScaler HA-Paar zu vermeiden** —ISSU gewährleistet ein Upgrade ohne Ausfallzeiten auf einem NetScaler-Hochverfügbarkeitspaar. Diese Option bietet eine Migrationsfunktionalität, die die vorhandenen Verbindungen während des Upgrades berücksichtigt. So können Sie ein NetScaler 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 findest du unter Erstellen eines Slack-Profils.

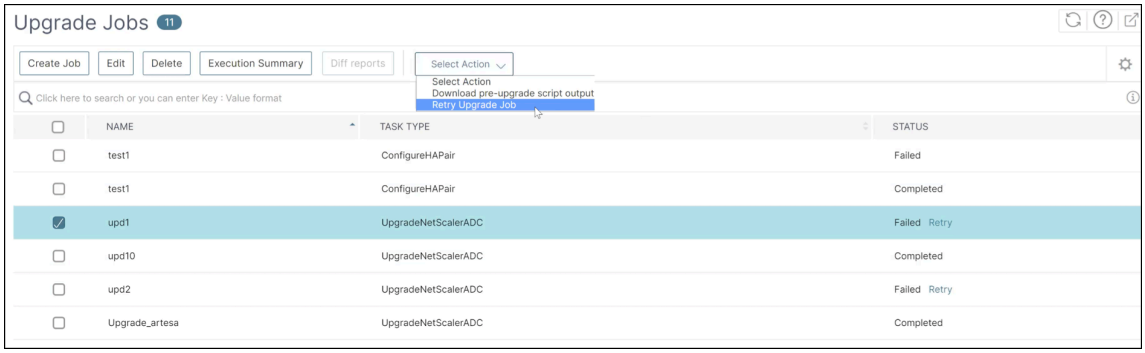


10. Klicken Sie auf **Job erstellen**.

Der Upgrade-Job wird unter **Infrastruktur > Upgrade-Jobs**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.

Fehlgeschlagene Upgrade-Jobs erneut versuchen

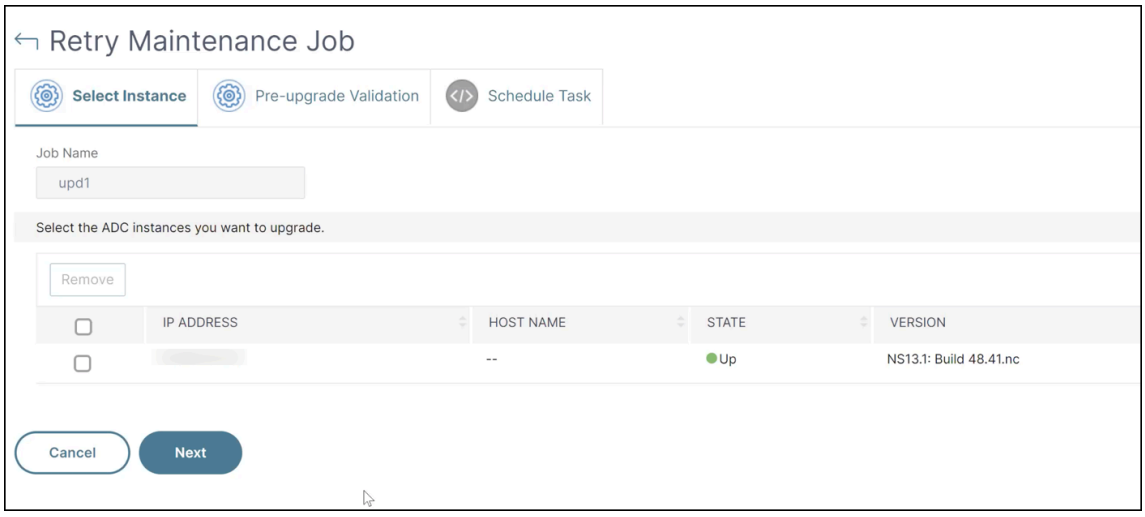
1. Wählen Sie unter **Infrastruktur > Upgrade-Jobs**den fehlgeschlagenen Upgrade-Job aus und klicken Sie auf **Erneut versuchen**. Alternativ können Sie auch zu **Aktion auswählen > Upgrade-Job erneut versuchen** navigieren, um einen fehlgeschlagenen Job erneut zu versuchen.



2. Geben Sie unter **Select Instance**die folgenden Details an:

   - **Jobname** —Geben Sie einen Namen für das Upgrade ein.
   - Wählen Sie die NetScaler-Instanzen, die Sie aktualisieren möchten, aus der Liste aus. Um alle Instanzen zu löschen, klicken Sie auf **Entfernen**.

   Klicken Sie auf **Weiter**, um den Validierungsprozess zu starten.

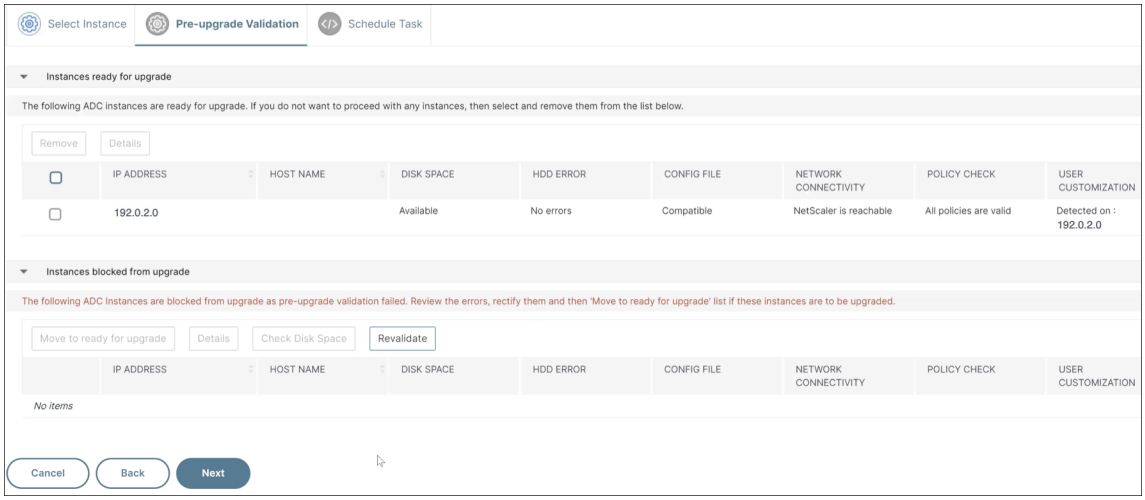


3. Auf der Registerkarte **Pre-upgrade validation** werden die folgenden Abschnitte angezeigt:

   - **Instanzen, die für das Upgrade bereit sind**. Sie können mit dem Upgrade dieser Instanzen fortfahren.
   - **Für das Upgrade blockierte Instanzen**. Diese NetScaler-Instanzen sind aufgrund von Validierungsfehlern vor dem Upgrade für das Upgrade gesperrt.

Sie können die Fehler überprüfen, korrigieren und dann für das Upgrade auf **Move to ready for upgrade** klicken. Wenn Sie auf einer Instanz nicht genügend Speicherplatz haben, können Sie den Speicherplatz überprüfen und bereinigen. Weitere Informationen finden Sie unter Bereinigen des NetScaler-Festplattenspeichers.

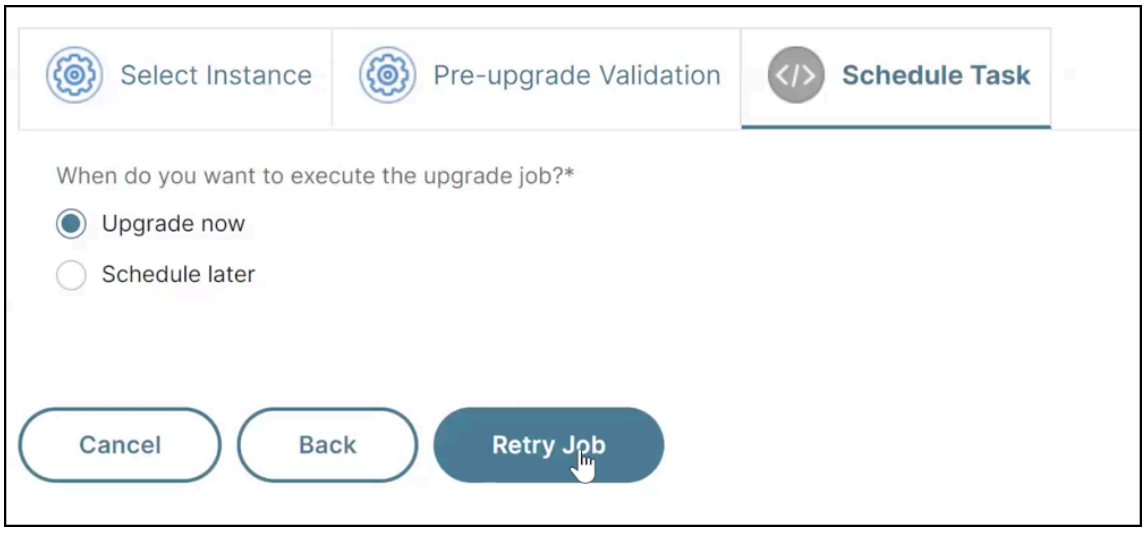
- **Richtlinienprüfung**: Wenn NetScaler ADM nicht unterstützte klassische Richtlinien findet, können Sie diese Richtlinien entfernen, um einen Upgrade-Auftrag zu erstellen.



Klicken Sie auf **Weiter**.

4. 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.



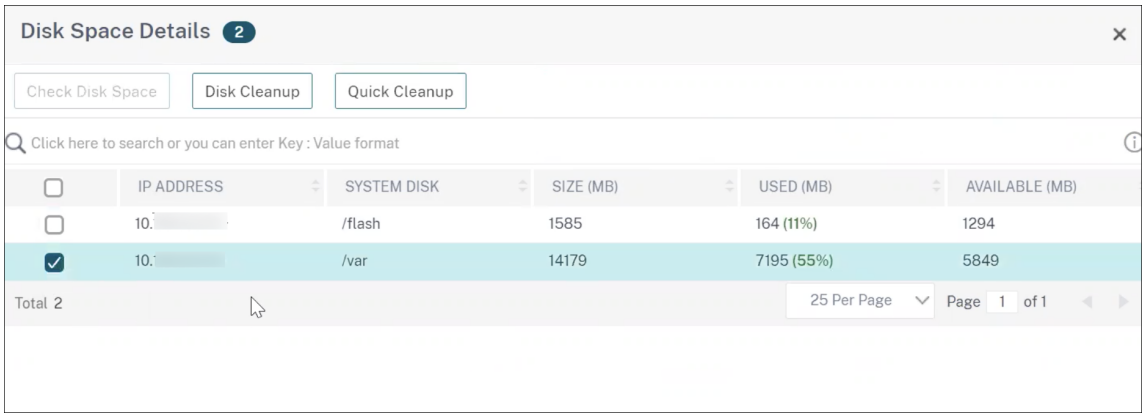
Klicken Sie auf **Wiederholen**.

NetScaler-Speicherplatz bereinigen

Wenn beim Upgrade einer NetScaler-Instanz das Problem mit unzureichendem Speicherplatz auftritt, bereinigen Sie den Speicherplatz über die NetScaler ADM-GUI selbst.

1. Auf der Registerkarte **Pre-upgrade validation** werden im Abschnitt **Instances blocked from upgrade** die Instanzen angezeigt, bei denen das Upgrade aufgrund von unzureichendem Speicherplatz fehlgeschlagen ist. Wählen Sie die Instanz aus, bei der das Speicherplatzproblem auftritt.
2. Klicken Sie auf **Speicherplatz überprüfen**.

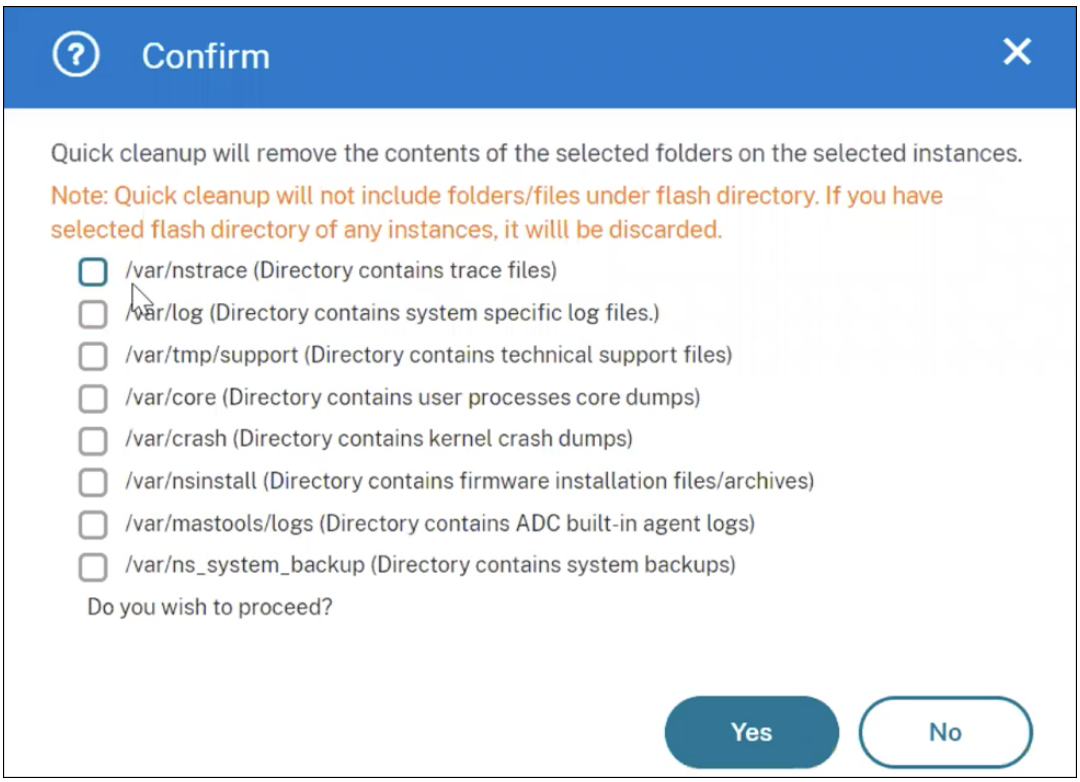
   Ein Bereich mit **Speicherplatzdetails** wird angezeigt. In diesem Bereich werden die Instanzen, der verwendete Speicher und der verfügbare Speicher angezeigt.



3. Wählen Sie im Bereich **Disk Space Details** die Instanz aus, die bereinigt werden muss, und führen Sie einen der folgenden Schritte aus:

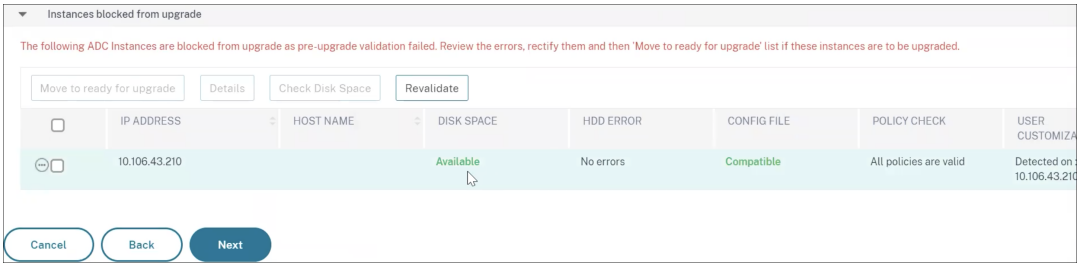
   a) **Disk Cleanup** - Navigieren Sie zu den erforderlichen Ordnern oder Verzeichnissen und löschen Sie sie, um Speicherplatz freizugeben.

   b) **Quick Cleanup** - Geben Sie schnell Speicherplatz frei, indem Sie mehrere Ordner löschen. Wählen Sie im daraufhin angezeigten **Bestätigungsbereich** die Ordner aus, die Sie löschen möchten, und klicken Sie auf **Ja**.



c) Nachdem Sie den Speicherplatz freigegeben haben, können Sie überprüfen, ob jetzt ausreichend Speicherplatz für ein Upgrade der Instanz verfügbar ist. Klicken Sie im Abschnitt **Instances blocked from upgrade** auf **Revalidate**.

Im folgenden Beispiel ist Speicherplatz verfügbar. Sie können jetzt auf **Move to ready for upgrade** klicken, um die Instanz zu aktualisieren, oder auf **Weiter** klicken, um mit dem nächsten Schritt fortzufahren.



Planung von Upgrade-Jobs für ein NetScaler Hochverfügbarkeitspaar

In der folgenden Tabelle sind die verschiedenen Planungsszenarien auf der Seite „ **Aufgabe planen** “und die entsprechenden Upgrade-Optionen aufgeführt, die auf der Seite „ **Job erstellen** “verfügbar sind:

Wann möchten Sie den Upgrade-Job ausführen?	Wann möchten Sie das Software-Image auf NetScaler hochladen?	Wie möchten Sie das Build-Image auf HA-Knoten hochladen?
Jetzt aufrüsten	Nicht zutreffend	**Sowohl auf den primären als auch auf den sekundären Knoten hochladen** (Standardoption)
Später planen	**Zum Zeitpunkt der Ausführung hochladen** (Standardoption)	**Sowohl auf den primären als auch auf den sekundären Knoten hochladen** (Standardoption)
Später planen (wenn **die Option Zweistufiges Upgrade für Knoten in HA durchführen** ausgewählt ist)	**Zum Zeitpunkt der Ausführung hochladen** (Standardoption)	**Jetzt hochladen** **Nur auf den sekundären Knoten hochladen** (Standard und einzige Option) **Jetzt hochladen**

Laden Sie einen kombinierten Vergleichsbericht eines NetScaler-Upgrade-Jobs herunter

Sie können einen Diff-Bericht eines NetScaler-Upgrade-Jobs herunterladen, wenn benutzerdefinierte Skripts angegeben sind. Ein Diff-Bericht enthält die Unterschiede zwischen den Ausgaben des Pre-Upgrade- und Post-Upgrade-Skripts. Mit diesem Bericht können Sie feststellen, welche Änderungen an der NetScaler-Instanz nach dem Upgrade vorgenommen wurden.

> **Hinweis**
>
> Der Diff-Bericht wird nur generiert, wenn Sie dasselbe Skript in den Phasen vor dem Upgrade und nach dem Upgrade angeben.

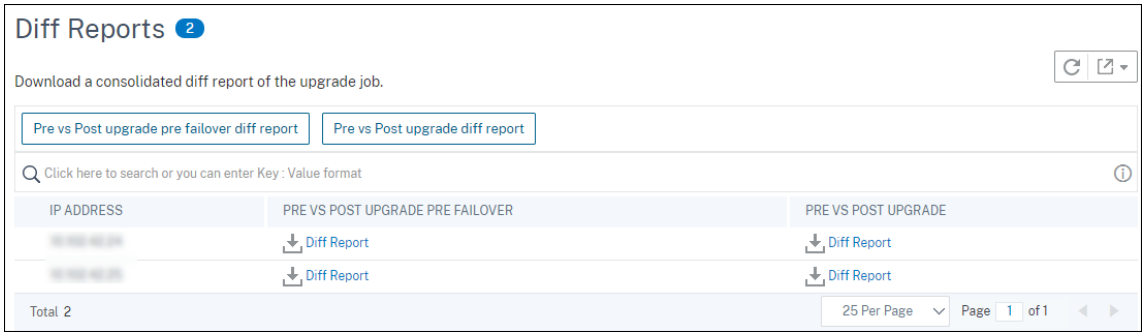
Um einen Diff-Bericht über einen Upgrade-Job herunterzuladen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Infrastruktur > Konfigurationsaufträge > 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**



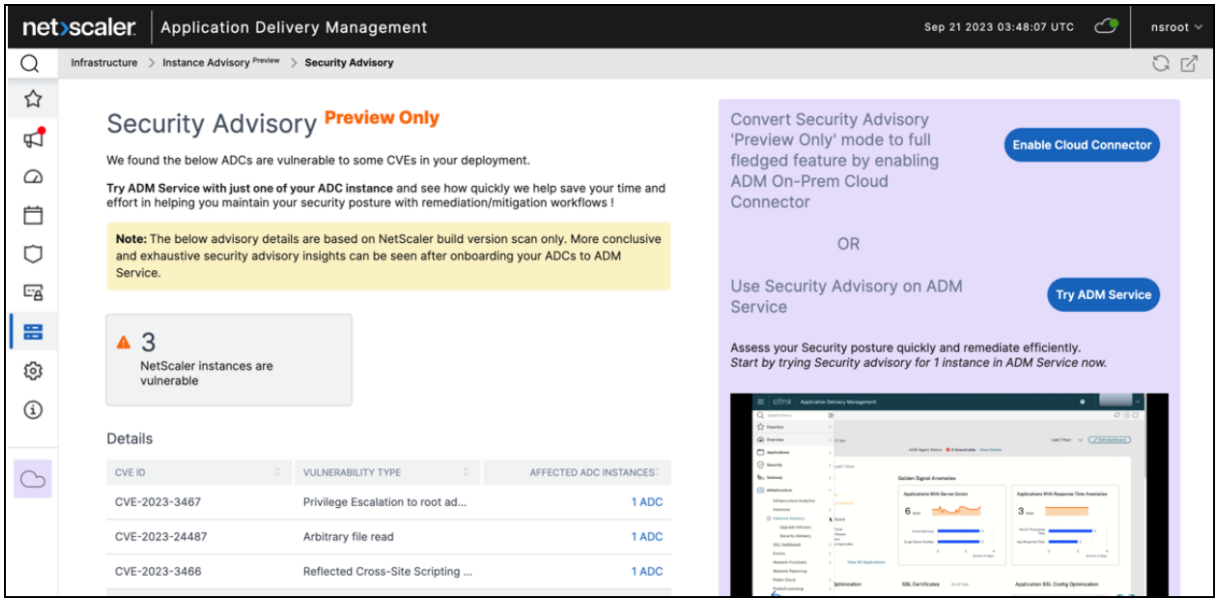
Sicherheitsempfehlungen

February 5, 2024

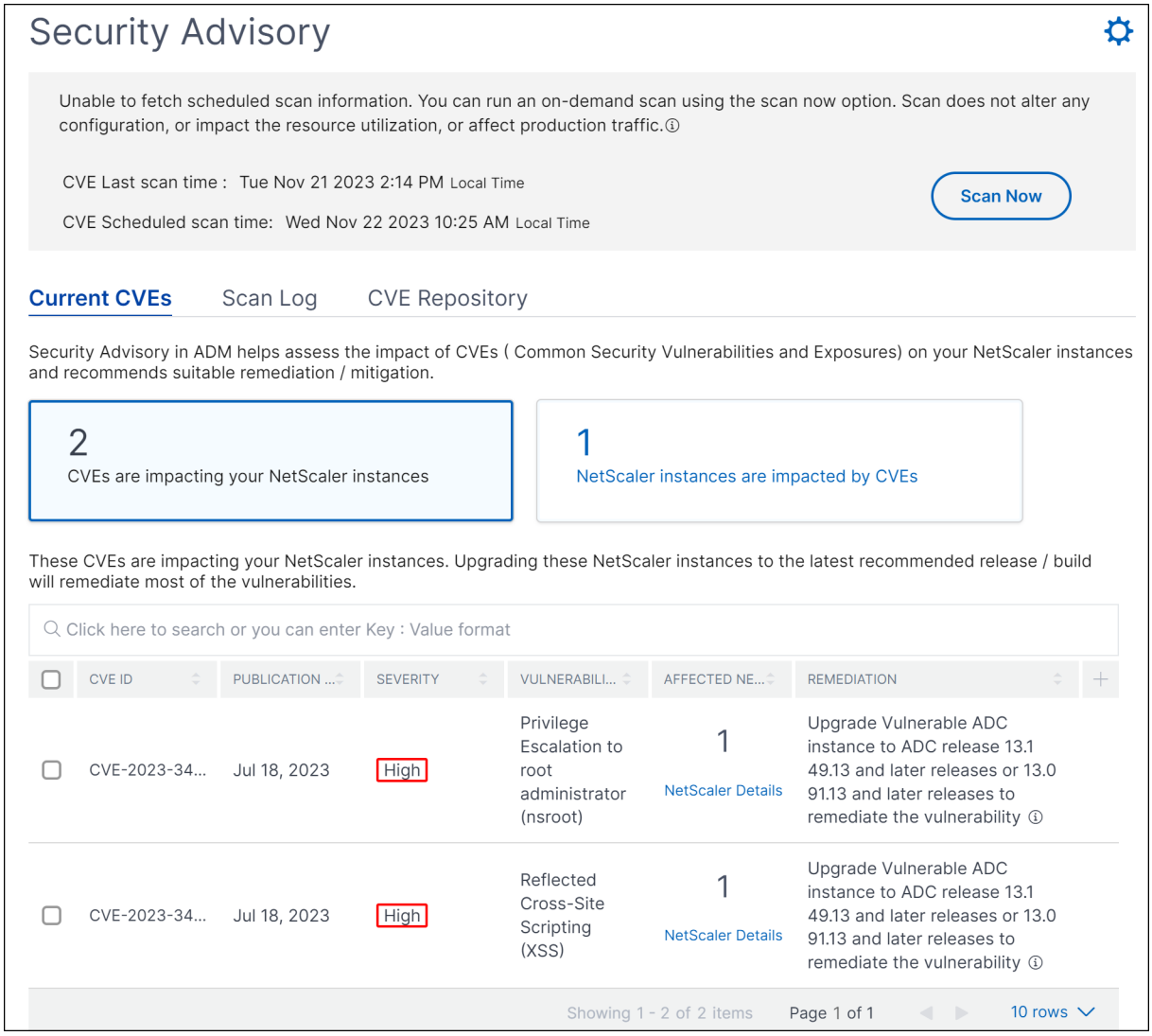
Eine sichere und belastbare Infrastruktur ist die Lebensader jeder Organisation. Unternehmen müssen neue Common Vulnerabilities and Exposures (CVEs) verfolgen und die Auswirkungen von CVEs auf ihre Infrastruktur bewerten. Sie müssen auch die Abhilfemaßnahmen zur Behebung der Sicherheitslücken verstehen und planen. Die Sicherheitsempfehlung in NetScaler ADM ermöglicht es Ihnen, die CVEs zu identifizieren, die Ihre NetScaler-Instanzen gefährden, und empfiehlt Abhilfemaßnahmen.

Ab Build 14.1 8.x können Sie die Vollversion des Security Advisory verwenden, indem Sie **ADM On-Prem Cloud Connector** konfigurieren und **Security Advisory** aktivieren.

Wenn Sie ADM On-Prem Cloud Connector nicht konfiguriert haben, können Sie sich nur die Vorschauversion von Security Advisory ansehen. Sie können auf **Cloud Connector aktivieren** klicken und die Konfiguration abschließen, um die Vollversion der Sicherheitsempfehlung zu verwenden. Weitere Informationen finden Sie unter ADM On-Prem Cloud Connector.



Nachdem Sie ADM On-Prem Cloud Connector konfiguriert und Security Advisory aktiviert haben, können Sie die aktualisierte Seite mit der Sicherheitsempfehlung aufrufen.



Als Administrator müssen Sie sicherstellen, dass Sie alle neuen Common Vulnerabilities and Exposures (CVEs) verfolgen, die Auswirkungen von CVEs bewerten, die Behebung verstehen und die Sicherheitslücken schließen.

Funktionen zur Sicherheitsberatung

Die folgenden Sicherheitsempfehlungen helfen Ihnen beim Schutz Ihrer Infrastruktur:

Features	Beschreibung
Systemscan	Scannt standardmäßig alle verwalteten Instanzen einmal pro Woche. NetScaler ADM entscheidet über Datum und Uhrzeit der Systemscans, und Sie können sie nicht ändern.

Features	Beschreibung
Scannen auf Anforderung	Sie können die Instanzen bei Bedarf manuell scannen. Wenn die nach dem letzten Systemscan verstrichene Zeit erheblich ist, können Sie einen Anforderungsscan ausführen, um die aktuelle Sicherheitslage zu bewerten. Oder scannen Sie, nachdem eine Korrektur vorgenommen wurde, um den geänderten Status zu beurteilen.
CVE-Auswirkungsanalyse	Zeigt die Ergebnisse aller CVEs, die sich auf Ihre Infrastruktur auswirken, und aller NetScaler-Instanzen, die betroffen sind, und schlägt Gegenmaßnahmen vor. Verwenden Sie diese Informationen, um Abhilfemaßnahmen zur Behebung von Sicherheitsrisiken anzuwenden.
Protokoll scannen	Speichert die Kopien der letzten fünf Scans. Sie können diese Berichte im CSV- und PDF-Format herunterladen und analysieren.
CVE-Repositorium	Bietet einen detaillierten Überblick über alle NetScaler-bezogenen CVEs, die Citrix seit Dezember 2019 angekündigt hat und die sich auf Ihre NetScaler-Infrastruktur auswirken könnten. Sie können diese Ansicht verwenden, um die CVEs im Bereich der Sicherheitsberatung zu verstehen und mehr über den CVE zu erfahren. Informationen zu CVEs, die nicht unterstützt werden, finden Sie unter Nicht unterstützte CVEs in Security Advisory.

Wichtige Hinweise

- Die Sicherheitsempfehlung unterstützt keine NetScaler-Builds, die das Ende des Lebenszyklus (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.
- Für die CVE-Erkennung unterstützte Instanzen: alle NetScaler (SDX, MPX, VPX) und Gateway.
- Unterstützte CVEs: Alle CVEs nach Dezember 2019.

> **Hinweis:**
>
> Die Erkennung und Behebung von Sicherheitslücken, die sich auf das NetScaler Gateway-Plug-In für Windows auswirken, wird von der NetScaler ADM Security Advisory nicht unterstützt. Informationen zu CVEs, die nicht unterstützt werden, finden Sie unter Nicht unterstützte CVEs in Security Advisory.

- Die NetScaler ADM-Sicherheitsempfehlung berücksichtigt bei der Identifizierung der Sicherheitsanfälligkeit keine Fehlkonfiguration von Funktionen.
- Die NetScaler ADM-Sicherheitsempfehlung unterstützt nur die Identifizierung und Behebung der CVEs. Es unterstützt nicht die Identifizierung und Behebung der im Sicherheitsartikel hervorgehobenen Sicherheitsbedenken.
- Umfang der NetScaler-, Gateway-Versionen: Die Funktion ist auf Haupt-Builds beschränkt. Die Sicherheitsempfehlung umfasst keine speziellen Builds in ihrem Geltungsbereich.
  - Die Sicherheitsempfehlung wird in der Admin-Partition nicht unterstützt.
- Die folgenden Scanarten sind für CVEs verfügbar:
  - **Versionsscan**: Für diesen Scan wird NetScaler ADM benötigt, um die Version einer NetScaler-Instanz mit den Versionen und Builds zu vergleichen, für die der Fix verfügbar ist. Dieser Versionsvergleich hilft NetScaler ADM Security Advisory dabei, festzustellen, ob der NetScaler für das CVE anfällig ist. Wenn beispielsweise ein CVE in einer NetScaler-Version und Build xx.yy behoben ist, betrachtet die Sicherheitsempfehlung alle NetScaler-Instanzen auf Builds unter xx.yy als anfällig. Versionsscans werden heute in der Sicherheitsempfehlung unterstützt.
  - **Konfigurationsscan**: Für diesen Scan muss NetScaler ADM ein für den CVE-Scan spezifisches Muster mit der NetScaler-Konfigurationsdatei (nsconf) abgleichen. Wenn das spezifische Konfigurationsmuster in der NetScaler ns.conf-Datei vorhanden ist, wird die Instanz als anfällig für diese CVE angesehen. Dieser Scan wird normalerweise beim Versions-Scan verwendet.
    Config Scan wird heute in der Sicherheitsempfehlung unterstützt.
  - **Benutzerdefinierter Scan**: Für diesen Scan muss NetScaler ADM eine Verbindung mit der verwalteten NetScaler-Instanz herstellen, ein Skript an diese senden und das Skript ausführen. Anhand der Skriptausgabe kann NetScaler ADM ermitteln, ob der NetScaler für das CVE anfällig ist. Beispiele hierfür sind eine spezifische Shell-Befehlsausgabe, eine spezifische CLI-Befehlsausgabe, bestimmte Protokolle und das Vorhandensein oder der Inhalt bestimmter Verzeichnisse oder Dateien. Security Advisory verwendet auch benutzerdefinierte Scans für Übereinstimmungen mit mehreren Konfigurationsmustern, wenn die Konfigurationssuche dabei nicht helfen kann. Bei CVEs, die benutzerdefinierte

Scans erfordern, wird das Skript jedes Mal ausgeführt, wenn Ihr geplanter Scan oder ein Anforderungsscan Weitere Informationen zu den gesammelten Daten und Optionen für bestimmte benutzerdefinierte Scans finden Sie in der Sicherheitsempfehlung für dieses CVE.

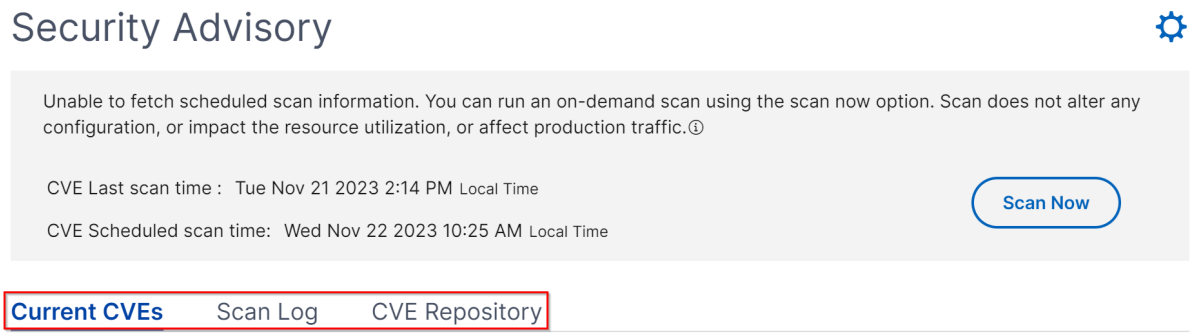
- Scans wirken sich nicht auf den Produktionsdatenverkehr auf NetScaler aus und ändern keine NetScaler-Konfiguration auf NetScaler.
- NetScaler ADM Security Advisory unterstützt keine CVE-Risikominderung. Wenn Sie eine Risikominderung (temporäre Problemumgehung) auf die NetScaler-Instanz angewendet haben, identifiziert ADM den NetScaler weiterhin als anfälligen NetScaler, bis Sie die Behebung abgeschlossen haben.
- Für die FIPS-Instanzen wird der CVE-Scan nicht unterstützt.

So verwenden Sie das Sicherheits-Advisory-Dashboard

Um auf das **Security Advisory-Dashboard** zuzugreifen, navigieren Sie über die NetScaler ADM-GUI zu **Infrastruktur > Instanzberatung > Security Advisory**.

Das Dashboard enthält drei Registerkarten:

- Aktuelle CVEs
- Protokoll scannen
- CVE-Repository



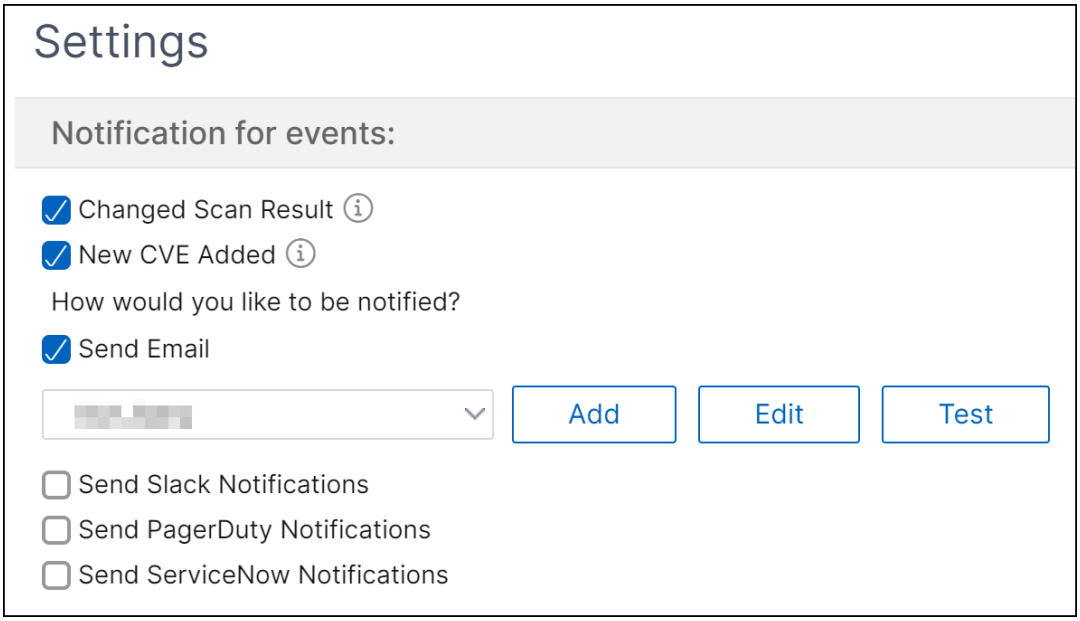
> **Wichtig:**
>
> In der **Sicherheits-Advisory-GUI** oder im Bericht werden möglicherweise nicht alle CVEs angezeigt, und Sie sehen möglicherweise nur eine CVE. Klicken Sie als Workaround auf **Jetzt scannen**, um einen Anforderungsscan auszuführen. Nachdem der Scan abgeschlossen ist, werden alle CVEs im Bereich (ungefähr 15) in der Benutzeroberfläche oder im Bericht angezeigt.

In der oberen rechten Ecke des Dashboards befindet sich das Einstellungssymbol, mit dem Sie:

- Aktiviere und deaktiviere Benachrichtigungen.

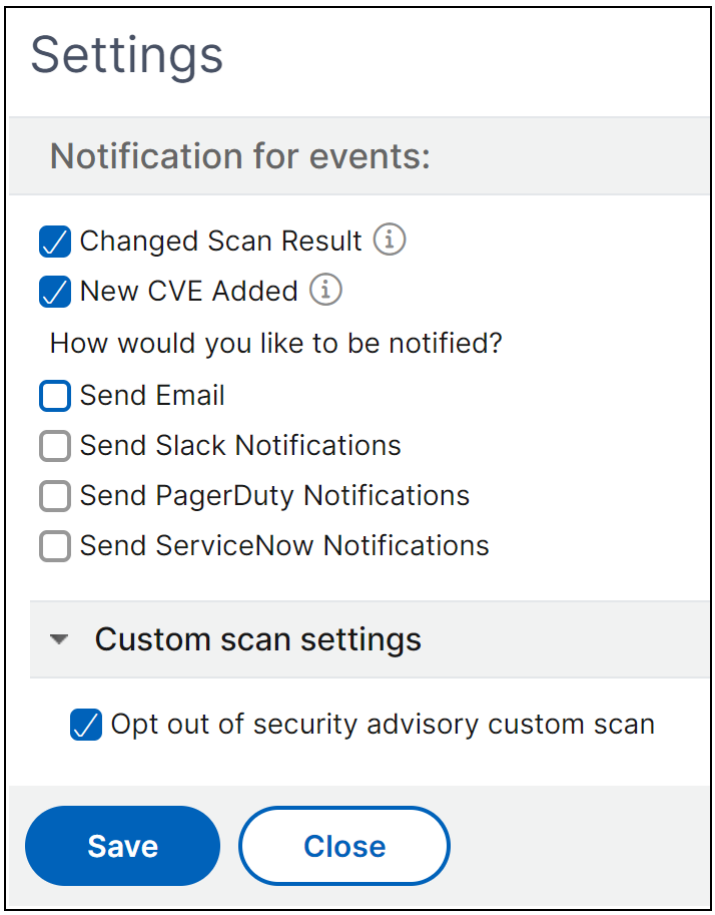
  Sie können die folgenden Benachrichtigungen über die Auswirkungen von CVE erhalten.

  - E-Mail-, Slack-, PagerDuty- und ServiceNow-Benachrichtigungen für Änderungen der CVE-Scanergebnisse und neue CVEs, die dem CVE-Repository hinzugefügt wurden.
  - Cloud-Benachrichtigung für Änderungen der CVE-Impact-Scanergebnisse.



- Benutzerdefinierte Sucheinstellungen konfigurieren

  Sie können auf die Liste **Benutzerdefinierte Scaneinstellungen** klicken, um das Kontrollkästchen für zusätzliche Einstellungen anzuzeigen. Sie haben die Möglichkeit, das Kontrollkästchen zu aktivieren und sich von diesen benutzerdefinierten CVE-Scans abzumelden. Die Auswirkungen der CVEs, die einen benutzerdefinierten Scan benötigen, werden in der Sicherheitsempfehlung für Ihre NetScaler-Instanzen nicht bewertet.



Aktuelle CVEs

Diese Registerkarte zeigt die Anzahl der CVEs, die sich auf Ihre Instanzen auswirken, sowie die Instanzen, die von CVEs betroffen sind. 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 NetScaler-Instanzen auswirken, enthält die folgenden Details.

CVE-ID: Die ID des CVE, der sich auf die Instanzen auswirkt.

Veröffentlichungsdatum: Das Datum, an dem das Sicherheitsbulletin für dieses CVE veröffentlicht wurde.

Schweregrad: Art des Schweregrads (hoch/mittel/kritisch) und Score. Um die Punktzahl zu sehen, bewegen Sie den Mauszeiger über den Schweregradtyp.

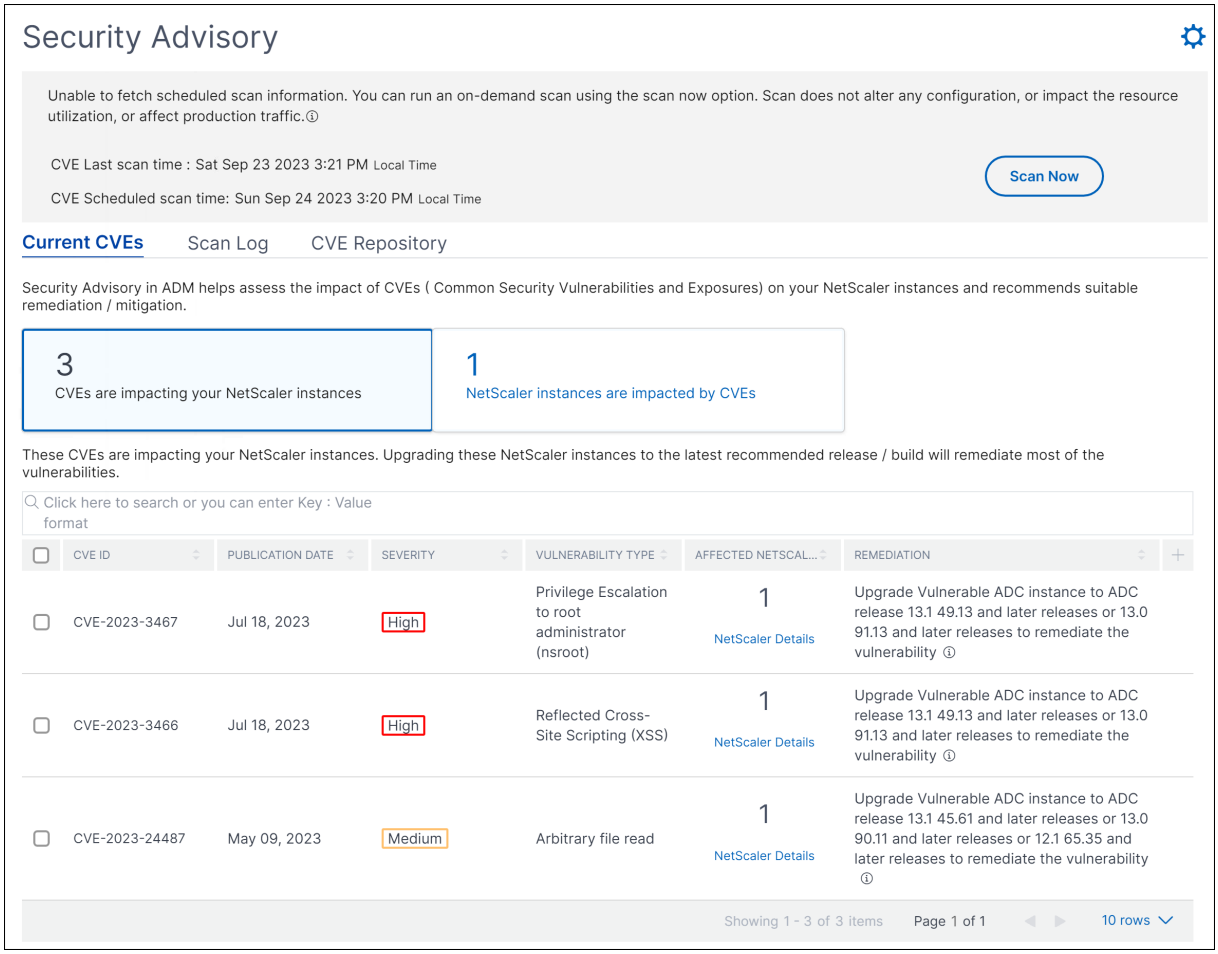
Schwachstellentyp: Die Art der Sicherheitsanfälligkeit für dieses CVE.

Betroffene NetScaler-Instanzen: Die Anzahl der Instanzen, auf die sich die CVE-ID auswirkt. Wenn Sie mit der Maus darüber fahren, wird die Liste der NetScaler-Instanzen angezeigt.

Behebung: Die verfügbaren Abhilfemaßnahmen, 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 NetScaler-Details unter **Betroffene NetScaler-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.

In diesem Bildschirm beträgt die Anzahl der CVEs, die sich auf Ihre Instanzen auswirken, 3 CVEs, und die Instanzen, die von diesen CVEs betroffen sind, sind eins.

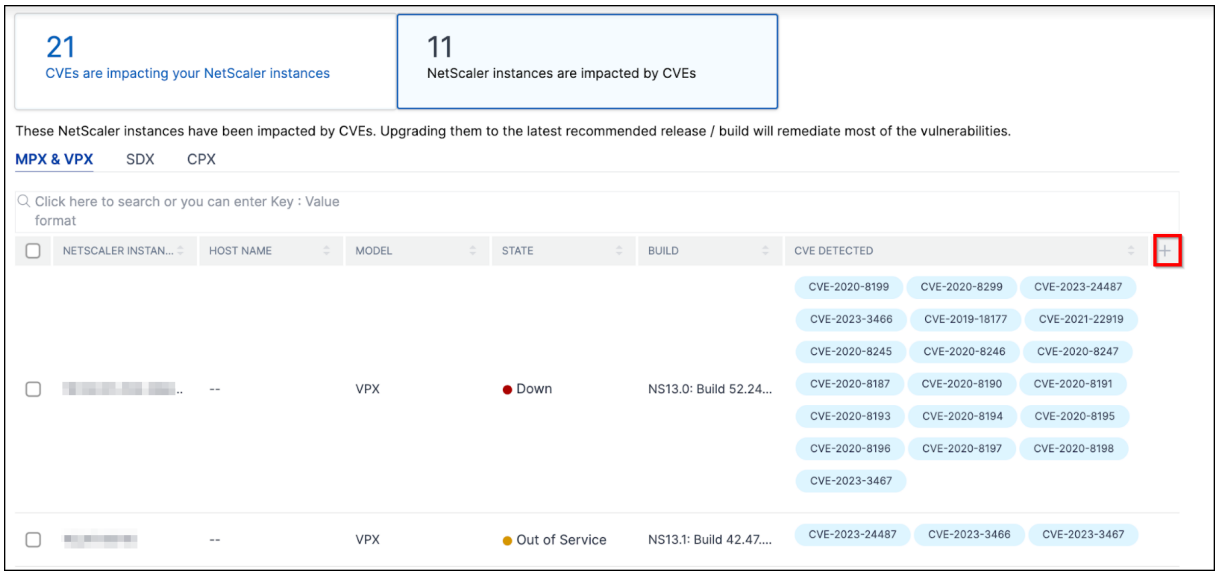


Auf der Registerkarte **<number of>NetScaler-Instanzen sind von CVEs betroffen** werden alle betroffenen NetScaler ADM-Instanzen angezeigt. Die Tabelle zeigt die folgenden Details:

- NetScaler IP-Adresse
- Hostname
- NetScaler Modellnummer

- Status des NetScaler
- Softwareversion und Build
- Liste der CVEs, die sich auf den NetScaler auswirken.

Sie können jede dieser Spalten je nach Bedarf hinzufügen oder entfernen, indem Sie auf das Pluszeichen klicken.



Um das Sicherheitsproblem zu beheben, wählen Sie die NetScaler-Instanz aus und wenden Sie die empfohlene Behebung an. Die meisten CVEs benötigen ein Upgrade als Standardisierung, während andere ein Upgrade und einen zusätzlichen Schritt als Standardisierung benötigen.

- Informationen zur Behebung von CVE-2020-8300 finden Sie unter Korrigieren von Sicherheitslücken für CVE-2020-8300.
- Informationen zu CVE-2021-22927 und CVE-2021-22920 finden Sie unter Korrigieren von Sicherheitslücken für CVE-2021-22927 und CVE-2021-22920.
- Informationen zu CVE-2021-22956 finden Sie unter Identifizieren und Beheben von Sicherheitslücken für CVE-2021-22956
- Informationen zu CVE-2022-27509 finden Sie unter Korrigieren von Sicherheitslücken für CVE-2022-27509

> **Hinweis**
>
> Wenn Ihre NetScaler-Instanzen über Anpassungen verfügen, finden Sie weitere Informationen unter Überlegungen zum Upgrade für benutzerdefinierte NetScaler-Konfigurationen, bevor Sie ein NetScaler-Upgrade planen.

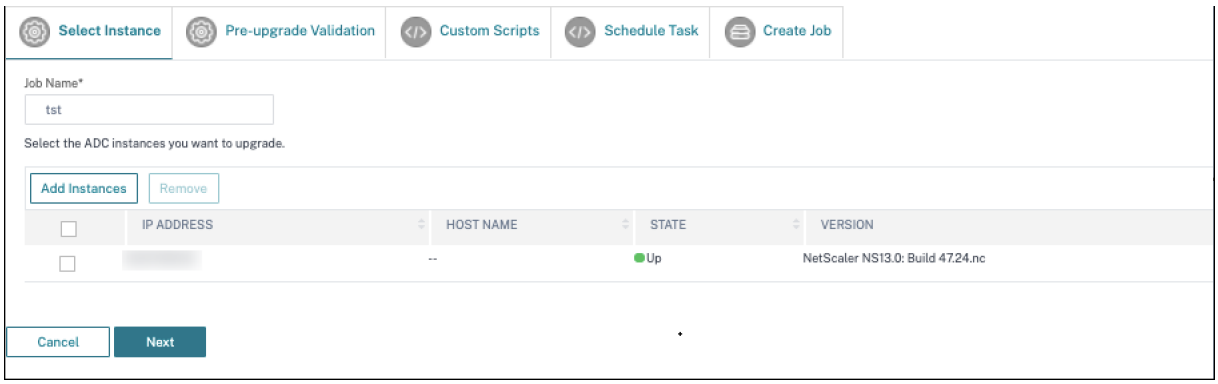
Upgrade: Sie können die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, die das Update enthalten. Dieses Detail ist in der Behebungsspalte zu sehen. Wählen

Sie zum Upgrade die Instanz aus und klicken Sie dann auf **Weiter zum Upgrade-Workflow**. Im Upgrade-Workflow wird der anfällige NetScaler automatisch als Ziel-NetScaler aufgefüllt.

> **Hinweis**
>
> Die Releases 12.0, 11.0, 10.5 und niedriger sind bereits Ende des Lebenszyklus (EOL). Wenn Ihre NetScaler-Instanzen auf einer dieser Versionen ausgeführt werden, führen Sie ein Upgrade auf eine unterstützte Version durch.

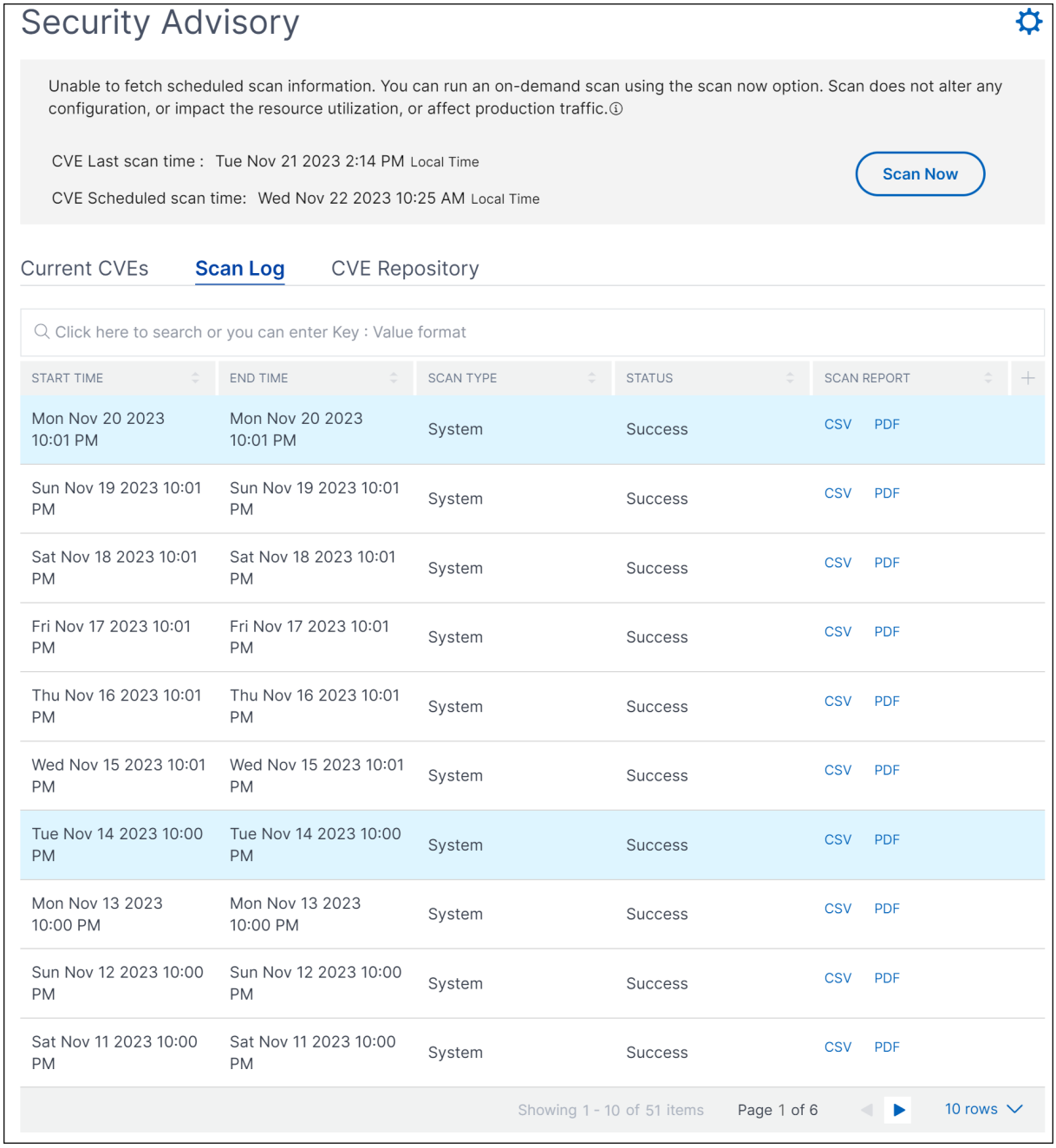
Der Upgrade-Workflow beginnt. Weitere Informationen zur Verwendung von NetScaler ADM zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Jobszum Upgrade von NetScaler-Instanzen.

> **Hinweis**
>
> Die Version und der Build, auf die Sie upgraden möchten, liegt in Ihrem Ermessen. Lesen Sie die Hinweise in der Spalte “Behebung”, um zu erfahren, welche Version und welche Builds den Sicherheitsupdate enthalten. Wählen Sie dementsprechend ein unterstütztes Release und Build aus, das noch nicht das Ende der Lebensdauer erreicht hat.



Protokoll scannen

Auf der Registerkarte werden Berichte der letzten fünf CVE-Scans angezeigt, die sowohl Standard-systemscans als auch benutzerinitiierte On-Demand-Scans enthalten. Sie können den Bericht jedes Scans im CSV- und PDF-Format herunterladen. Wenn gerade ein Scan auf Anforderung ausgeführt wird, können Sie auch den Abschlussstatus sehen.

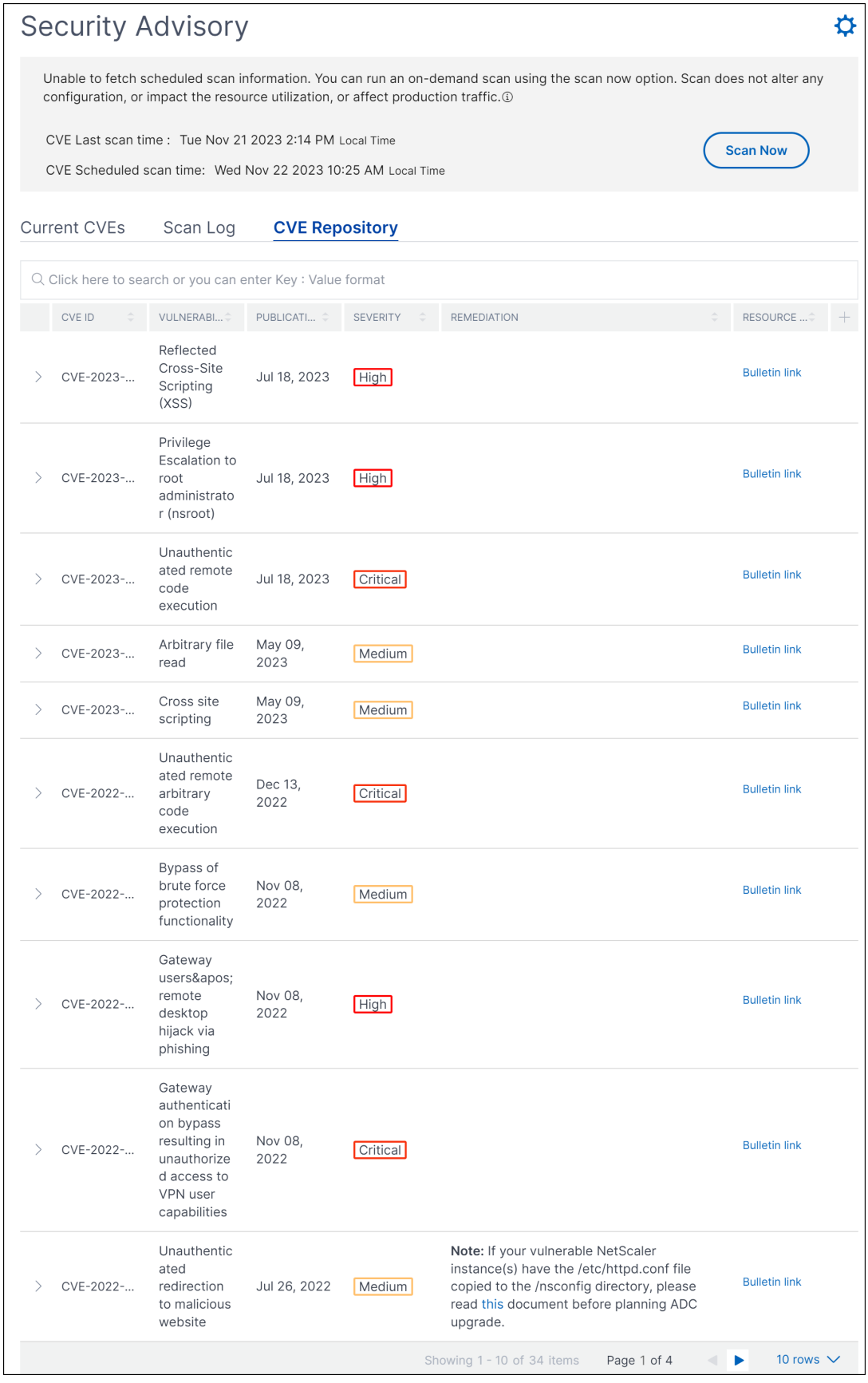


CVE-Repository

Diese Registerkarte enthält die neuesten Informationen aller CVEs ab Dezember 2019 sowie die folgenden Details:

- CVE-IDs
- Art der Sicherheitslücke
- Datum der Veröffentlichung

- Schweregrad
- Sanierung
- Links zu Sicherheitsbulletins



Security Advisory

Unable to fetch scheduled scan information. You can run an on-demand scan using the scan now option. Scan does not alter any configuration, or impact the resource utilization, or affect production traffic.

CVE Last scan time : Tue Nov 21 2023 2:14 PM Local Time

CVE Scheduled scan time: Wed Nov 22 2023 10:25 AM Local Time

Scan Now

Current CVEs | Scan Log | CVE Repository

Click here to search or you can enter Key : Value format

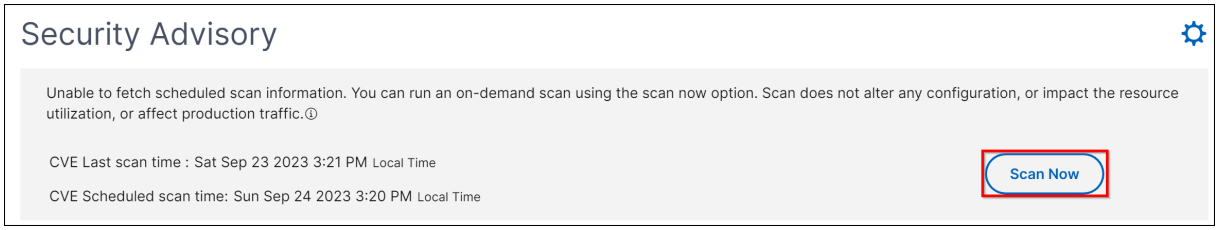
CVE ID	VULNERABI...	PUBLICATI...	SEVERITY	REMEDIATION	RESOURCE ...
CVE-2023-...	Reflected Cross-Site Scripting (XSS)	Jul 18, 2023	High		Bulletin link
CVE-2023-...	Privilege Escalation to root administrator (nsroot)	Jul 18, 2023	High		Bulletin link
CVE-2023-...	Unauthenticated remote code execution	Jul 18, 2023	Critical		Bulletin link
CVE-2023-...	Arbitrary file read	May 09, 2023	Medium		Bulletin link
CVE-2023-...	Cross site scripting	May 09, 2023	Medium		Bulletin link
CVE-2022-...	Unauthenticated remote arbitrary code execution	Dec 13, 2022	Critical		Bulletin link
CVE-2022-...	Bypass of brute force protection functionality	Nov 08, 2022	Medium		Bulletin link
CVE-2022-...	Gateway users' remote desktop hijack via phishing	Nov 08, 2022	High		Bulletin link
CVE-2022-...	Gateway authentication bypass resulting in unauthorized access to VPN user capabilities	Nov 08, 2022	Critical		Bulletin link
CVE-2022-...	Unauthenticated redirection to malicious website	Jul 26, 2022	Medium	**Note:** If your vulnerable NetScaler instance(s) have the /etc/httpd.conf file copied to the /nsconfig directory, please read this document before planning ADC upgrade.	Bulletin link

Showing 1 - 10 of 34 items Page 1 of 4 10 rows

Jetzt durchsuchen

Sie können die Instanzen jederzeit nach Ihren Bedürfnissen scannen.

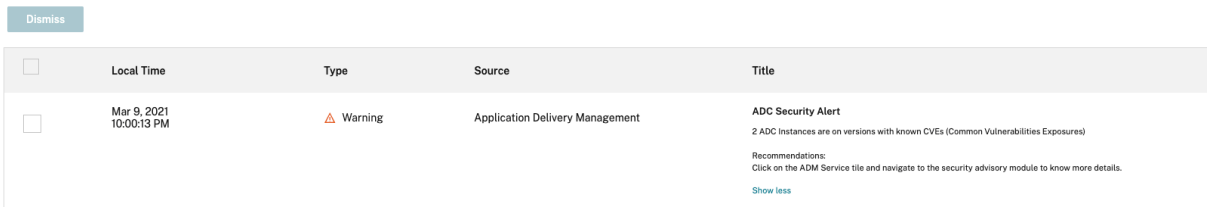
Klicken Sie auf **Jetzt scannen**, um nach CVEs zu suchen, die sich auf Ihre NetScaler-Instanzen auswirken. Sobald der Scan abgeschlossen ist, werden die überarbeiteten Sicherheitsdetails in der Benutzeroberfläche für Sicherheitsempfehlungen angezeigt.



NetScaler ADM benötigt einige Minuten, um den Scan abzuschließen.

Benachrichtigung

Als Administrator erhalten Sie Citrix Cloud-Benachrichtigungen, aus denen hervorgeht, wie viele NetScaler-Instanzen durch CVEs gefährdet sind. Um die Benachrichtigungen anzuzeigen, klicken Sie auf das Glockensymbol in der oberen rechten Ecke der NetScaler ADM GUI.



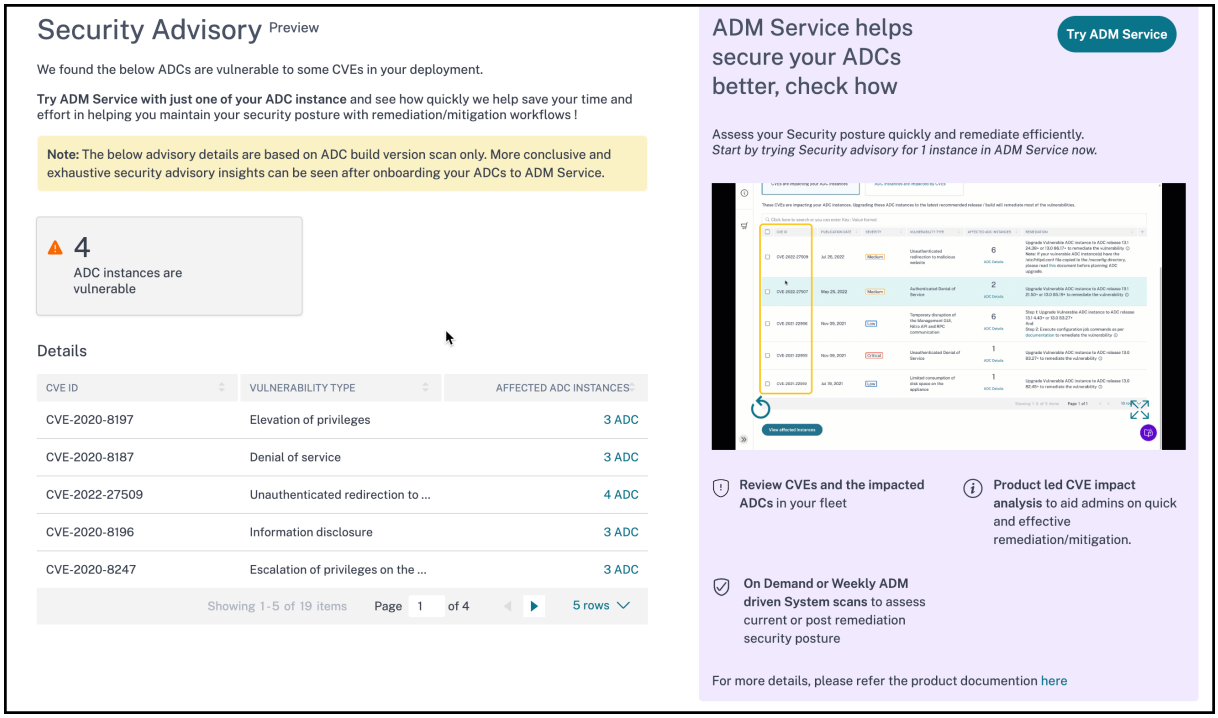
Sicherheitsempfehlung in 14.1 4.x oder früheren Builds

Wenn Sie frühere Builds verwenden, können Sie nur die Vorschauversion der Sicherheitsempfehlung verwenden. In der Vorschauversion werden nur die NetScaler CVEs und die ADC-Instanzen hervorgehoben, die in ADM Service integriert sind und die gefährdet sind. Wenn Sie die Vollversion der Security Advisory-Funktion verwenden möchten, müssen Sie ADM On-Prem Cloud Connector aktivieren.

> **WICHTIG**
>
> Eine detaillierte Analyse der Auswirkungen von CVE und aussagekräftige Informationen zu benutzerdefinierten Scans/Systemscans sowie zu Workflows zur Behebung und Abschwächung finden Sie unter **NetScaler ADM Service**.

Sicherheitsempfehlung anzeigen

Um auf die **Sicherheitsempfehlung** zuzugreifen, navigieren Sie zu **Infrastruktur > Instanzberatung > Sicherheitsempfehlung**. Sie können den Sicherheitsstatus aller ADC-Instanzen sehen, die Sie über NetScaler ADM verwalten.



Die On-Premises-Sicherheitsempfehlung von NetScaler ADM führt nur einen ADC-Versionsscan durch, um nach CVEs zu suchen. Die folgenden Informationen werden angezeigt.

- **CVE-ID**: Die ID des CVE, der sich auf die Instanzen auswirkt.
- **Schwachstellentyp**: Die Art der Sicherheitsanfälligkeit für dieses CVE.
- **Betroffene ADC-Instanzen**: Die Anzahl der Instanzen, auf die sich die CVE-ID auswirkt.

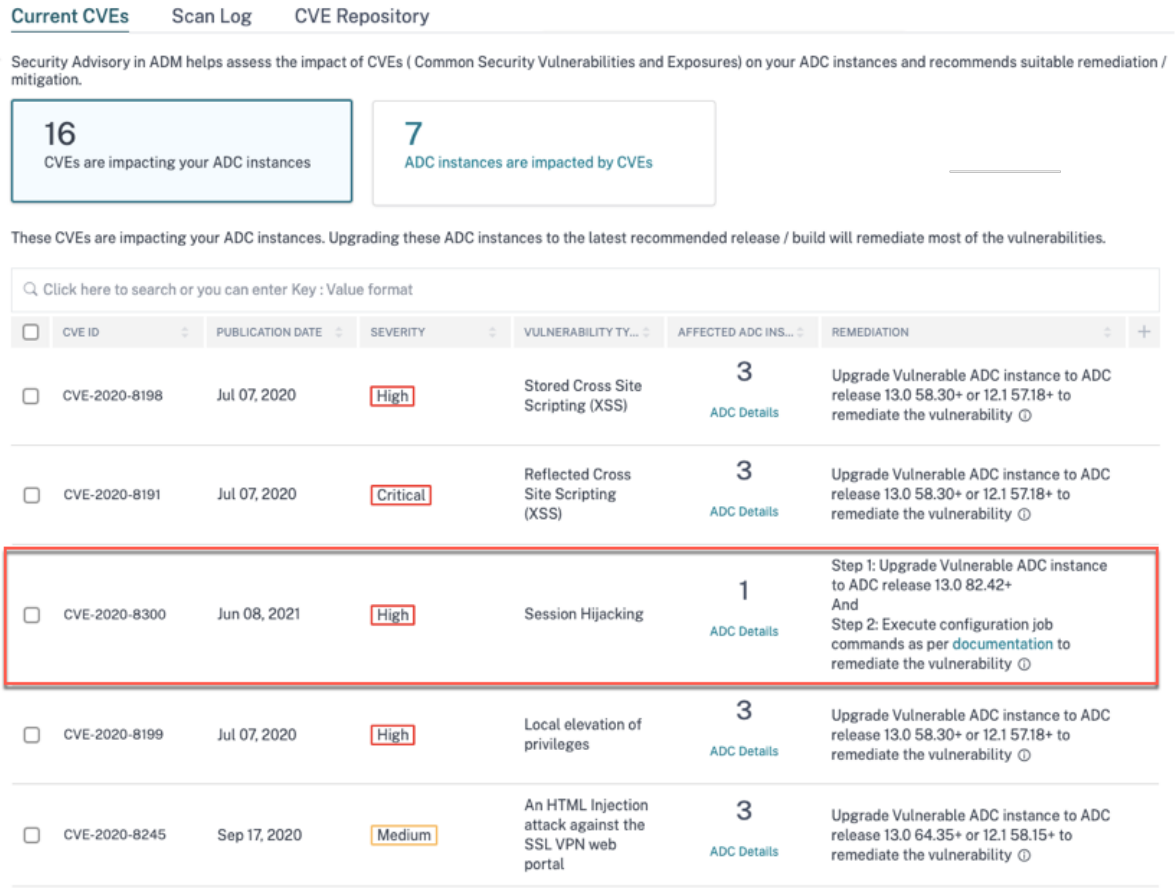
Mit der On-Premises-Sicherheitsempfehlung von NetScaler ADM können Sie auch eine der ADC-Instanzen auswählen und die ADC-Instanz in den ADM Service integrieren. Klicken Sie auf **ADM Service testen** und binden Sie die ADC-Instanz in den ADM Service ein. Mit ADM Service Security Advisory können Sie den Schwachstellentyp eines bestimmten CVE überprüfen und Informationen zur Minderung und Behebung der Sicherheitsanfälligkeit abrufen.

Weitere Informationen zur ADM Service Security Advisory finden Sie in der GIF-Animation auf der Seite mit den **Sicherheitshinweisen** .

Sicherheitsrisiko CVE-2020-8300 korrigieren

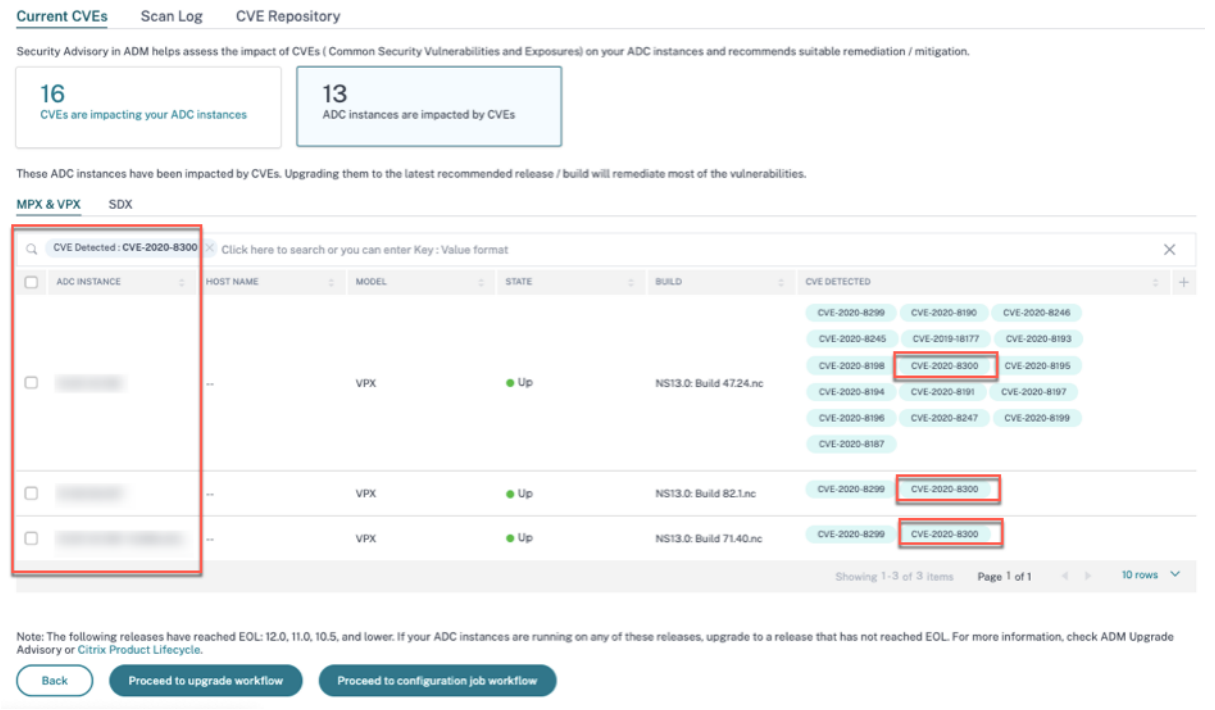
February 5, 2024

Im NetScaler ADM Security Advisory Dashboard unter **Current CVEs > <number of> ADC instances are impacted by CVEs**, können Sie alle Instanzen sehen, die aufgrund dieses speziellen CVE anfällig sind. Um die Details der von CVE-2020-8300 betroffenen Instanzen zu überprüfen, wählen Sie **CVE-2020-8300** aus und klicken Sie auf **Betroffene Instanzen anzeigen**.



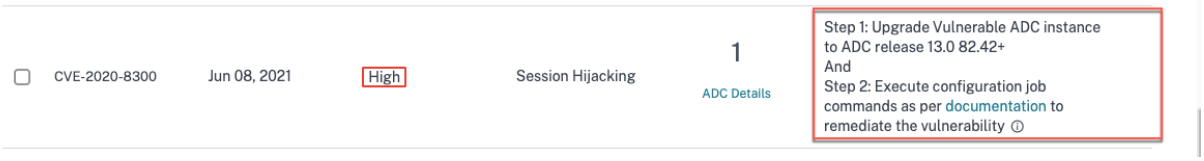
> **Hinweis**
>
> Weitere Informationen zum Security Advisory Dashboard finden Sie unter Security Advisory.

Das Fenster **<number of> ADC instances impacted by CVEs** wird angezeigt. Hier sehen Sie die Anzahl und Details der ADC-Instanzen, die von CVE-2020-8300 betroffen sind.



CVE-2020-8300 korrigieren

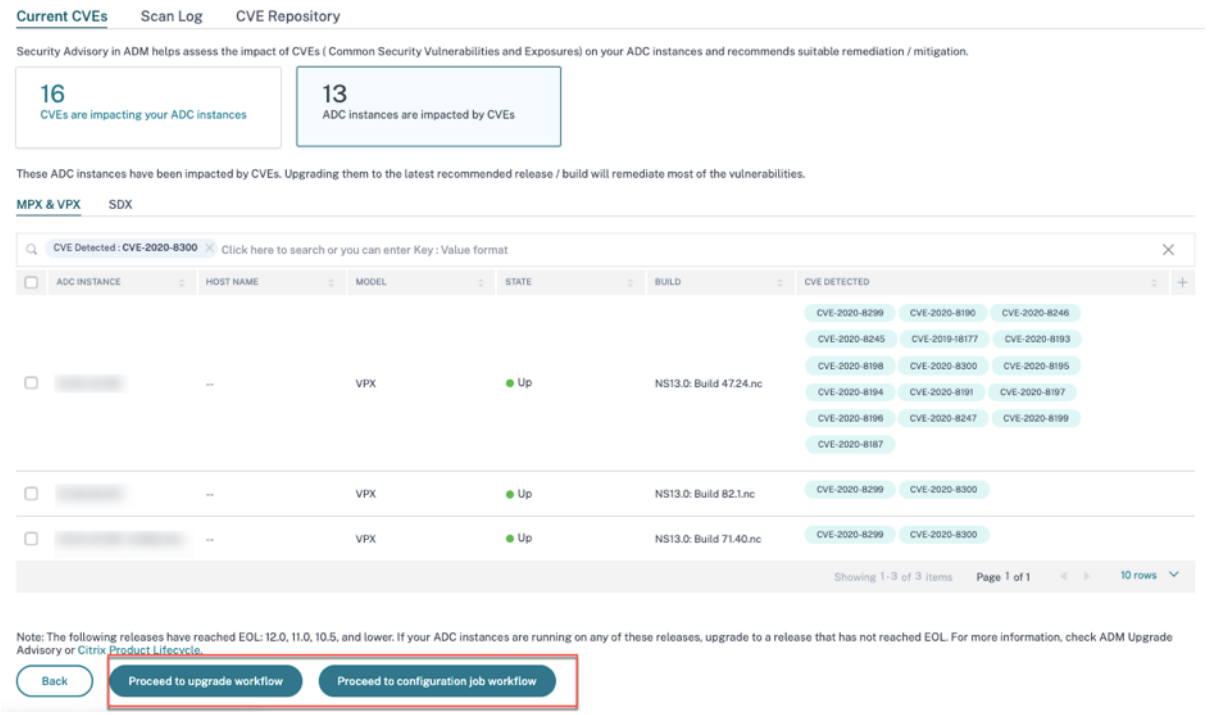
Bei ADC-Instanzen, die von CVE-2020-8300 betroffen sind, ist die Standardisierung ein zweistufiger Prozess. In der GUI können Sie unter **Aktuelle CVEs > ADC-Instanzen sind von CVEs betroffen**, Schritt 1 und 2 sehen.



Die zwei Schritte beinhalten:

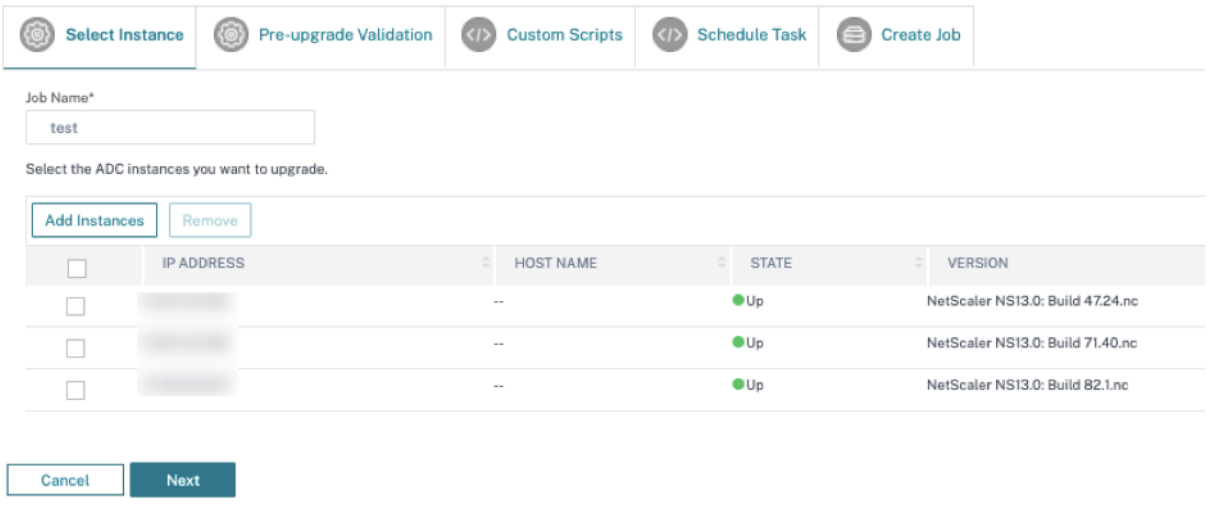
1. Upgrade der anfälligen ADC-Instanzen auf eine Version und einen Build, der das Update enthält.
2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen. Führen Sie diesen Schritt für jeden anfälligen ADC nacheinander aus und schließen Sie alle SAML-Aktionen und SAML-Profile für diesen ADC ein.

Unter **Aktuelle CVEs > ADC-Instanzen, die von CVEs betroffen sind**, sehen Sie zwei separate Workflows für diesen zweistufigen Standardisierungsprozess: **Fortfahren zum Upgrade-Workflow** und **Weiter zum Workflow des Konfigurationsauftrags**.



Schritt 1: Upgrade der anfälligen ADC-Instanzen

Um ein Upgrade der anfälligen Instanzen durchzuführen, wählen Sie die Instanzen aus und klicken Sie **auf Fortfahren mit** Der Upgrade-Workflow wird mit den bereits aufgefüllten anfälligen ADC-Instanzen geöffnet



Weitere Informationen zur Verwendung von NetScaler ADM zum Aktualisieren von ADC-Instanzen finden Sie unter Erstellen eines ADC-Upgrade-Auftrags.

> **Hinweis**
>
> Dieser Schritt kann für alle anfälligen ADC-Instanzen sofort ausgeführt werden.

Schritt 2: Anwenden von Konfigurationsbefehlen

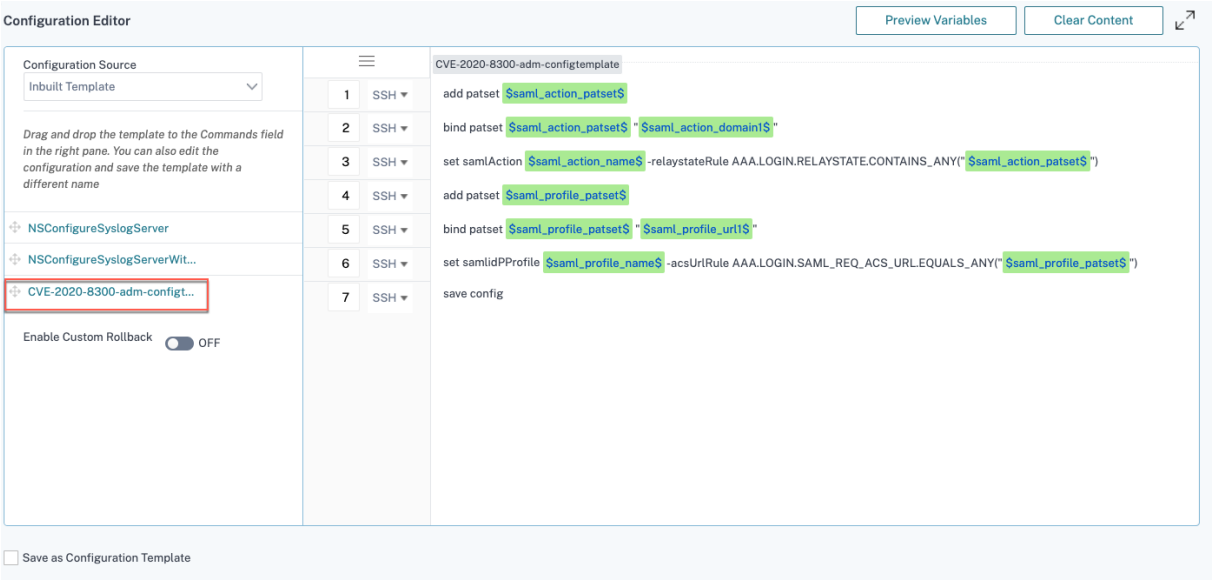
Nachdem Sie die betroffenen Instanzen aktualisiert haben, wählen Sie im Fenster **<number of> Von CVEs betroffene ADC-Instanzen** eine Instanz aus, die von CVE-2020-8300 betroffen ist, und klicken Sie auf **Weiter zum Workflow des Konfigurationsauftrags**. Der Workflow umfasst die folgenden Schritte.

1. Anpassen der Konfiguration.
2. Überprüfung der automatisch ausgefüllten betroffenen Instanzen.
3. Angabe von Eingaben für Variablen für den Job.
4. Überprüfung der endgültigen Konfiguration mit aufgefüllten Variableneingaben.
5. Den Job ausführen.

Beachten Sie die folgenden Punkte, bevor Sie eine Instanz auswählen und auf **Weiter zum Workflow des Konfigurationsauftrags**klicken:

- Für eine ADC-Instanz, die von mehreren CVEs betroffen ist (z. B. CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 und CVE-2021-22956): Wenn Sie die Instanz auswählen und auf **Weiter zum Workflow des Konfigurationsauftrags**klicken, wird die integrierte Konfigurationsvorlage unter Konfiguration auswählen nicht automatisch ausgefüllt. Ziehen Sie die entsprechende Konfigurationsjob-Vorlage manuell unter **Security Advisory Template** in den Konfigurationsjob-Fensterbereich auf der rechten Seite.
- Für mehrere ADC-Instanzen, die nur von CVE-2021-22956 betroffen sind: Sie können Konfigurationsjobs auf allen Instanzen gleichzeitig ausführen. Sie haben beispielsweise ADC 1, ADC 2 und ADC 3, und alle von ihnen sind nur von CVE-2021-22956 betroffen. Wählen Sie alle diese Instanzen aus und klicken Sie auf **Weiter zum Workflow des Konfigurationsauftrags**. Die integrierte Konfigurationsvorlage wird automatisch unter **Konfiguration auswählen**ausgefüllt.
- Bei mehreren ADC-Instanzen, die von CVE-2021-22956 betroffen sind, und einem oder mehreren anderen CVEs (z. B. CVE-2020-8300, CVE-2021-22927 und CVE-2021-22920), bei denen die Standardisierung auf jeden ADC gleichzeitig angewendet werden muss: Wenn Sie diese Instanzen auswählen und auf **Weiter zum Workflow des Konfigurationsauftrags**klicken, wird ein Fehler angezeigt Es wird eine Meldung angezeigt, in der Sie aufgefordert werden, den Konfigurationsjob auf jedem ADC gleichzeitig auszuführen.

Schritt 1: Konfiguration wählen Im Workflow des Konfigurationsauftrags wird die integrierte Konfigurationsvorlage automatisch unter **Konfiguration auswählen**ausgefüllt.



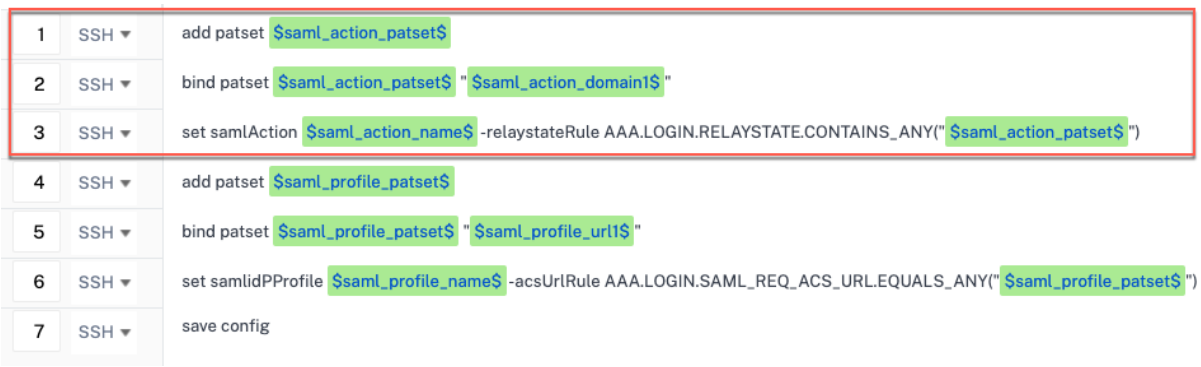
Führen Sie nacheinander einen separaten Konfigurationsauftrag für jede betroffene ADC-Instanz aus und schließen Sie alle SAML-Aktionen und SAML-Profile für diesen ADC ein. Wenn Sie beispielsweise zwei anfällige ADC-Instanzen mit jeweils zwei SAML-Aktionen und zwei SAML-Profilen haben, müssen Sie diesen Konfigurationsauftrag zweimal ausführen. Einmal pro ADC, das alle seine SAML-Aktionen und SAML-Profile abdeckt.

ADC 1	ADC2
Job 1: zwei SAML-Aktionen +zwei SAML-Profile	Job 2: zwei SAML-Aktionen +zwei SAML-Profile

Geben Sie dem Job einen Namen und passen Sie die Vorlage an die folgenden Spezifikationen an. Die integrierte Konfigurationsvorlage ist nur eine Gliederung oder Basisvorlage. Passen Sie die Vorlage basierend auf Ihrer Bereitstellung an die folgenden Anforderungen an:

a. **SAML-Aktionen und die zugehörigen Domänen**

Abhängig von der Anzahl der SAML-Aktionen, die Sie in Ihrer Bereitstellung haben, müssen Sie die Zeilen 1—3 replizieren und die Domänen für jede SAML-Aktion anpassen.



Wenn Sie beispielsweise zwei SAML-Aktionen haben, wiederholen Sie die Zeilen 1—3 zweimal und passen Sie die Variablendefinitionen für jede SAML-Aktion entsprechend an.

Und wenn Sie N Domänen für eine SAML-Aktion haben, müssen Sie die Zeile `bind patset $saml_action_patset$ “$saml_action_domain1$”` mehrmals manuell eingeben, um sicherzustellen, dass die Zeile N Mal für diese SAML-Aktion angezeigt wird. Und ändern Sie die folgenden Variablendefinitionsnamen:

- `saml_action_patset`: ist die Konfigurations-Template-Variable und stellt den Wert des Namens des Mustersatzes (patset) für die SAML-Aktion dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsjob-Workflows angeben. Weitere Informationen finden Sie im Abschnitt Schritt 3: Variablenwerte angeben in diesem Dokument.
- `saml_action_domain1`: ist die Konfigurationsvorlagenvariable und stellt den Domänennamen für diese spezifische SAML-Aktion dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsjob-Workflows angeben. Weitere Informationen finden Sie im Abschnitt Schritt 3: Variablenwerte angeben in diesem Dokument.

Führen Sie den Befehl aus, um alle SAML-Aktionen für ein Gerät zu finden `show samlaction`.

```
> show samlaction -summary
-------------------------------------------------------------------------------------------------------------------------------------------------
     Name            Username field  Decryption key       Encryption key       Url to be redirected to
                     Reject unsigned assertions Issuer name          Two factor Smart Group
-------------------------------------------------------------------------------------------------------------------------------------------------
1    SamlSPAct1                      idp_private_public   sp_private_public    https://<IP3>/saml/login
                     ON         http://<IP1>         OFF
2    SamlSPAct2                      idp_private_public   sp_private_public    https://          /saml/login
                     ON         http://              OFF
 Done
```

b. **SAML-Profile und die zugehörigen URLs**

Replizieren Sie die Zeilen 4—6, abhängig von der Anzahl der SAML-Profile, die Sie in Ihrer Bereitstellung haben. Passen Sie die URLs für jedes SAML-Profil an.

```
1  SSH  add patset $saml_action_patset$
2  SSH  bind patset $saml_action_patset$ "$saml_action_domain1$"
3  SSH  set samlAction $saml_action_name$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("$saml_action_patset$")
4  SSH  add patset $saml_profile_patset$
5  SSH  bind patset $saml_profile_patset$ "$saml_profile_url1$"
6  SSH  set samlidPProfile $saml_profile_name$ -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.EQUALS_ANY("$saml_profile_patset$")
7  SSH  save config
```

Wenn Sie beispielsweise zwei SAML-Profile haben, geben Sie die Zeilen 4—6 zweimal manuell ein und passen Sie die Variablendefinitionen für jede SAML-Aktion entsprechend an.

Und wenn Sie N Domänen für eine SAML-Aktion haben, müssen Sie die Zeile `bind patset $saml_profile_patset$ “$saml_profile_url1$”` mehrmals manuell eingeben, um

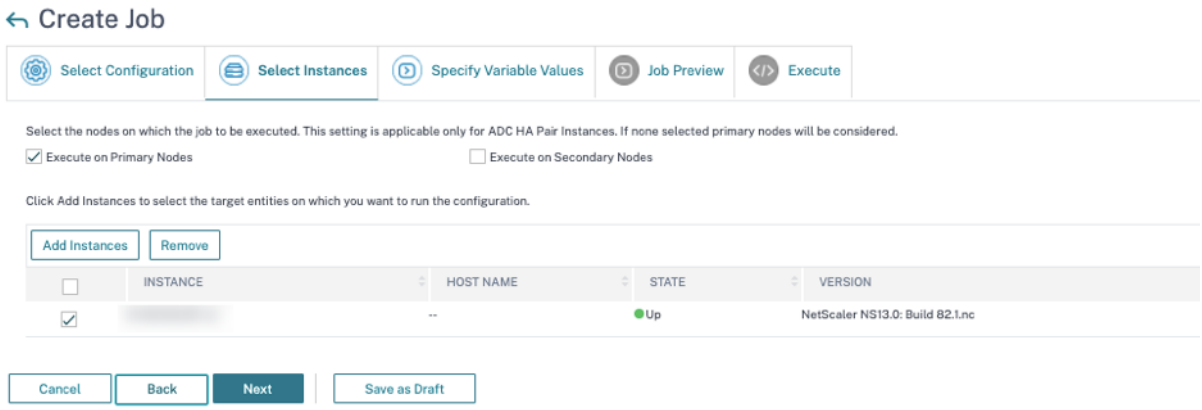
sicherzustellen, dass die Zeile N Mal für dieses SAML-Profil angezeigt wird. Und ändern Sie die folgenden Variablendefinitionsnamen:

- `saml_profile_patset`: ist die Konfigurations-Template-Variable und stellt den Wert des Namens des Mustersatzes (Patset) für das SAML-Profil dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsjob-Workflows angeben. Weitere Informationen finden Sie im Abschnitt Schritt 3: Variablenwerte angeben in diesem Dokument.
- `saml_profile_url1`: ist die Konfigurationsvorlagenvariable und stellt den Domänennamen für dieses spezifische SAML-Profil dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsjob-Workflows angeben. Weitere Informationen finden Sie im Abschnitt Schritt 3: Variablenwerte angeben in diesem Dokument.

Führen Sie den Befehl `show samlidpProfile` aus, um alle SAM-Profile für ein Gerät zu finden.

Schritt 2: Wählen Sie die Instanz aus

Die betroffene Instanz wird automatisch unter **Ausgewählte Instanzen**aufgefüllt. Wählen Sie die Instanz und klicken Sie auf **Weiter**.

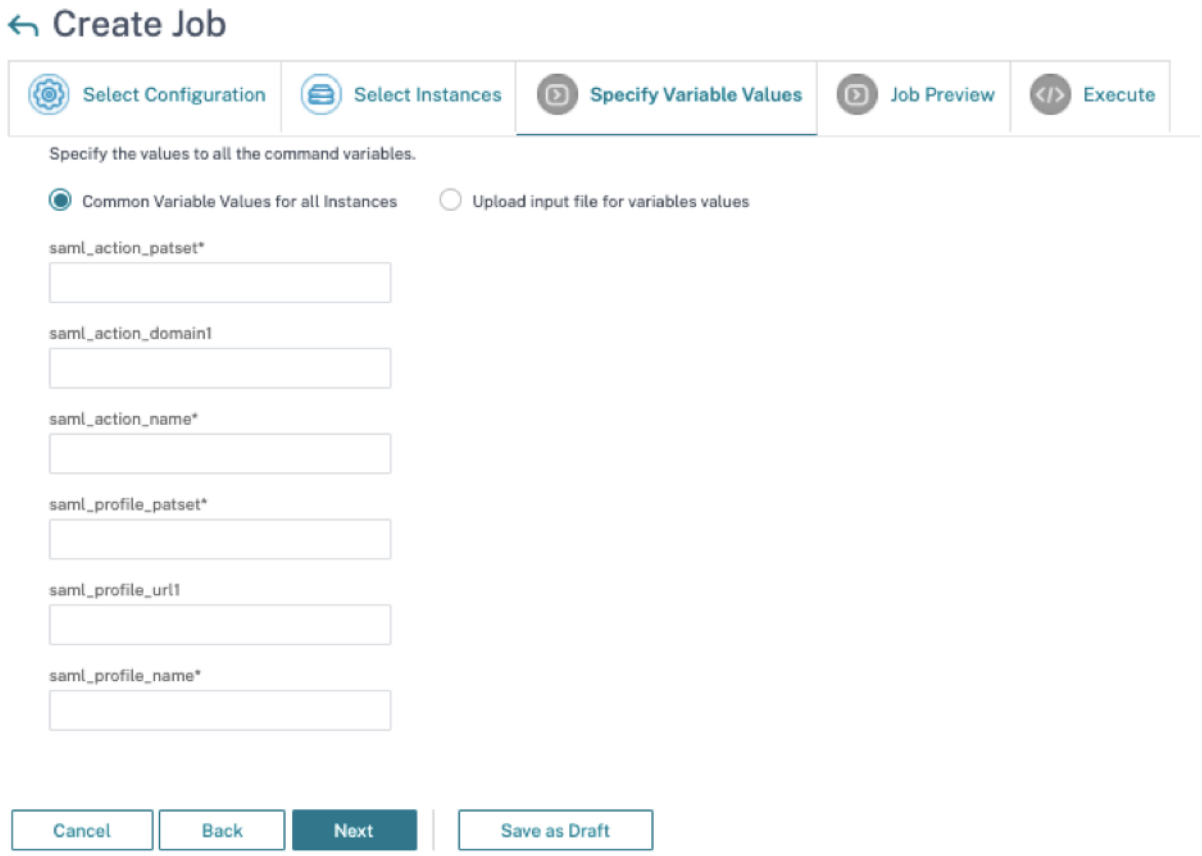


Schritt 3: Variablenwerte angeben Geben Sie die Werte der Variablen ein.

- `saml_action_patset`: Namen für die SAML-Aktion hinzufügen
- `saml_action_domain1`: Domäne im Format `https://<example1.com>/` eingeben
- `saml_action_name`: Dieselbe SAML-Aktion eingeben, für die Sie den Job konfigurieren

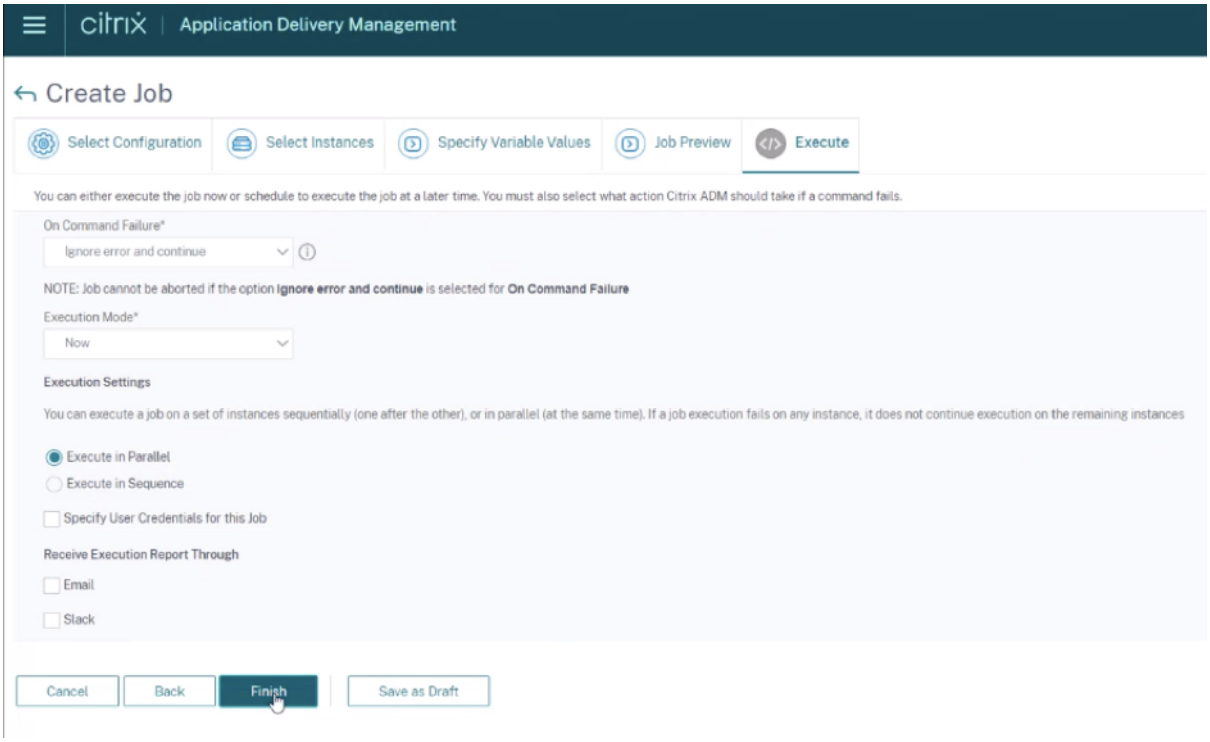
- `saml_profile_patset`: Namen für das SAML-Profil hinzufügen
- `saml_profile_url1`: URL in diesem Format eingeben: `https://<example2.com>/cgi/samlauth`
- `saml_profile_name`: Dasselbe SAML-Profil eingeben, für das Sie den Job konfigurieren

> **Hinweis**
>
> Für URLs ist die Erweiterung nicht immer `cgi/samlauth`. Es hängt davon ab, welche Autorisierung durch Dritte Sie haben, und dementsprechend müssen Sie die Erweiterung angeben.



Schritt 4: Vorschau der Konfiguration Zeigt eine Vorschau der in die Konfiguration eingefügten Variablenwerte an und klicken Sie auf **Weiter**.

Schritt 5: Führen Sie den Job aus Klicken Sie auf **Fertigstellen**, um den Konfigurationsauftrag auszuführen.



Nachdem der Job ausgeführt wurde, wird er unter **Infrastruktur > Konfiguration > Konfigurationsjobs**angezeigt.

Nachdem Sie die beiden Korrekturschritte für alle anfälligen ADCs abgeschlossen haben, können Sie einen Anforderungsscan ausführen, um die überarbeitete Sicherheitslage zu überprüfen.

Zu beachtende Punkte für das NetScaler ADM Express-Konto

Das NetScaler ADM Express-Konto verfügt über eingeschränkte Funktionen, zu denen nur Einschränkungen für zwei Konfigurationsaufträge gehören.

Für die CVE-2020-8300-Korrektur müssen Sie so viele Konfigurationsaufträge ausführen wie die Anzahl Ihrer anfälligen ADC-Instanzen. Wenn Sie also ein Express-Konto haben und mehr als zwei Konfigurationsaufträge ausführen müssen, befolgen Sie diese Problemumgehung.

Problemumgehung: Führen Sie zwei Konfigurationsjobs für zwei anfällige ADC-Instanzen aus und löschen Sie dann beide Jobs, um die nächsten beiden Jobs für die nächsten beiden anfälligen ADC-Instanzen weiter auszuführen. Fahren Sie fort, bis Sie alle anfälligen Instanzen abgedeckt haben. Bevor Sie die Jobs löschen, können Sie den Bericht zur späteren Verwendung herunterladen. Um den Bericht herunterzuladen, wählen Sie unter **Netzwerk > Jobs**die Jobs aus und klicken Sie unter **Aktionen** auf **Herunterladen**.

Beispiel: Wenn Sie sechs anfällige ADC-Instanzen haben, führen Sie jeweils zwei Konfigurationsjobs auf zwei anfälligen Instanzen aus und löschen Sie dann beide Konfigurationsjobs. Wiederholen Sie

diesen Schritt noch zweimal. Am Ende hätten Sie sechs Konfigurationsjobs für jeweils sechs ADC-Instanzen ausgeführt. In der NetScaler ADM UI unter **Infrastruktur > Jobs**sehen Sie nur die letzten beiden Konfigurationsjobs.

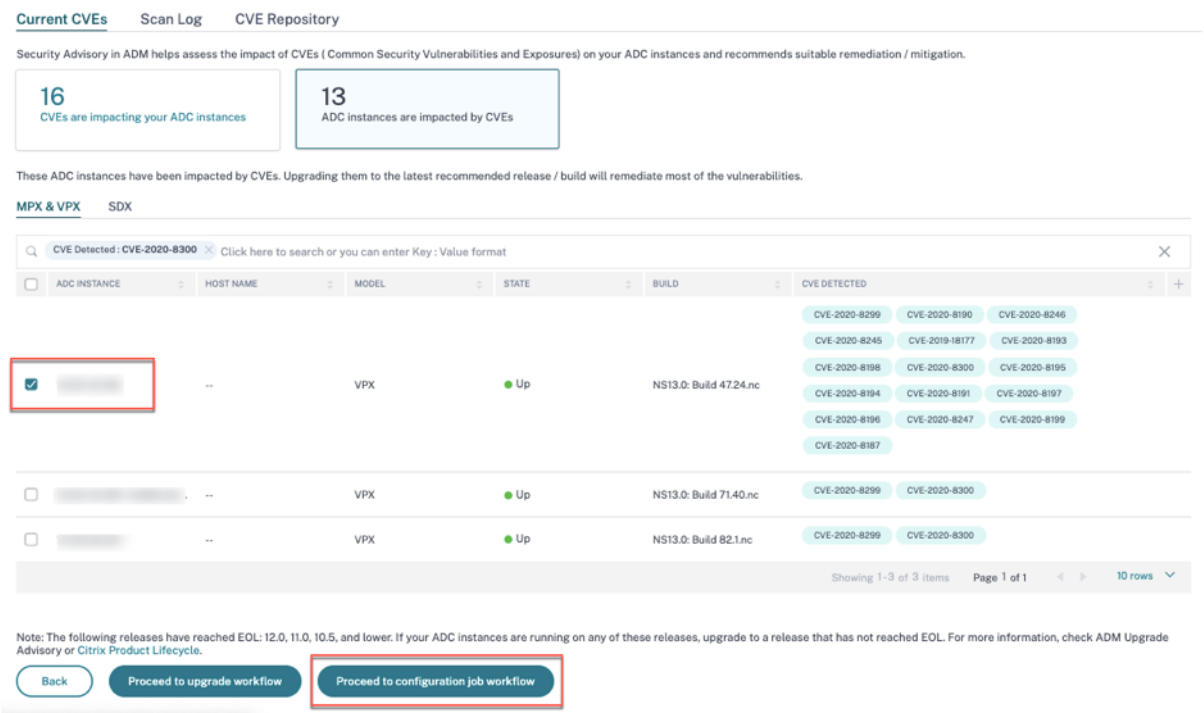
Szenario

In diesem Szenario sind drei ADC-Instanzen anfällig für CVE-2020-8300, und Sie müssen alle Instanzen standardisieren. Führen Sie die folgenden Schritte aus:

1. Führen Sie ein Upgrade aller drei ADC-Instanzen durch, indem Sie die im Abschnitt **Upgrade einer Instanz** in diesem Dokument beschriebenen Schritte ausführen.
2. Wenden Sie den Konfigurationspatch mithilfe des Konfigurationsjob-Workflows auf jeweils einen ADC an. Sehen Sie sich die Schritte an, die im Abschnitt **Konfigurationsbefehle anwenden** in diesem Dokument beschrieben werden.

Der anfällige ADC 1 hat die folgende Konfiguration:

Zwei SAML-Aktionen	Zwei SAML-Profile
SAML-Aktion 1 hat eine Domäne und SAML-Aktion 2 hat zwei Domänen	SAML-Profil 1 hat eine URL und SAML-Profil 2 hat zwei URLs.



Wählen Sie ADC 1 und klicken Sie auf **Weiter zum Workflow des Konfigurationsauftrags** Die integrierte Vorlage wird automatisch ausgefüllt. Geben Sie als Nächstes einen Auftragsnamen an und passen Sie die Vorlage entsprechend der angegebenen Konfiguration an.

In den folgenden Tabellen sind die Variablendefinitionen für benutzerdefinierte Parameter aufgeführt.

Tabelle 1. Variablendefinitionen für SAML-Aktionen

ADC-Konfiguration	Variablendefinition für Patset	Variablendefinition für den SAML-Aktionsnamen	Variablendefinition für Domain
SAML action 1 hat eine Domain	saml_action_patset1	saml_action_name1	saml_action_domain1
SAML-Aktion 2 hat zwei Domänen	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

Tabelle 2. Variablendefinitionen für SAML-Profile

ADC-Konfiguration	Variablendefinition für Patset	Variablendefinition für SAML-Profilnamen	Variablendefinition für URL
SAML-Profil 1 hat eine URL	saml_profile_patset1	saml_profile_name1	saml_profile_url1
SAML-Profil 2 hat zwei URLs	saml_profile_patset2	saml_profile_name2	saml_profile_url2, saml_profile_url3

Wählen Sie unter **Instanzen auswählen** ADC 1 aus und klicken Sie auf **Weiter**. Das Fenster **Variablenwerte angeben** wird angezeigt. In diesem Schritt müssen Sie Werte für alle im vorherigen Schritt definierten Variablen angeben.

Überprüfen Sie als Nächstes die Variablen.

Klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um den Job auszuführen.

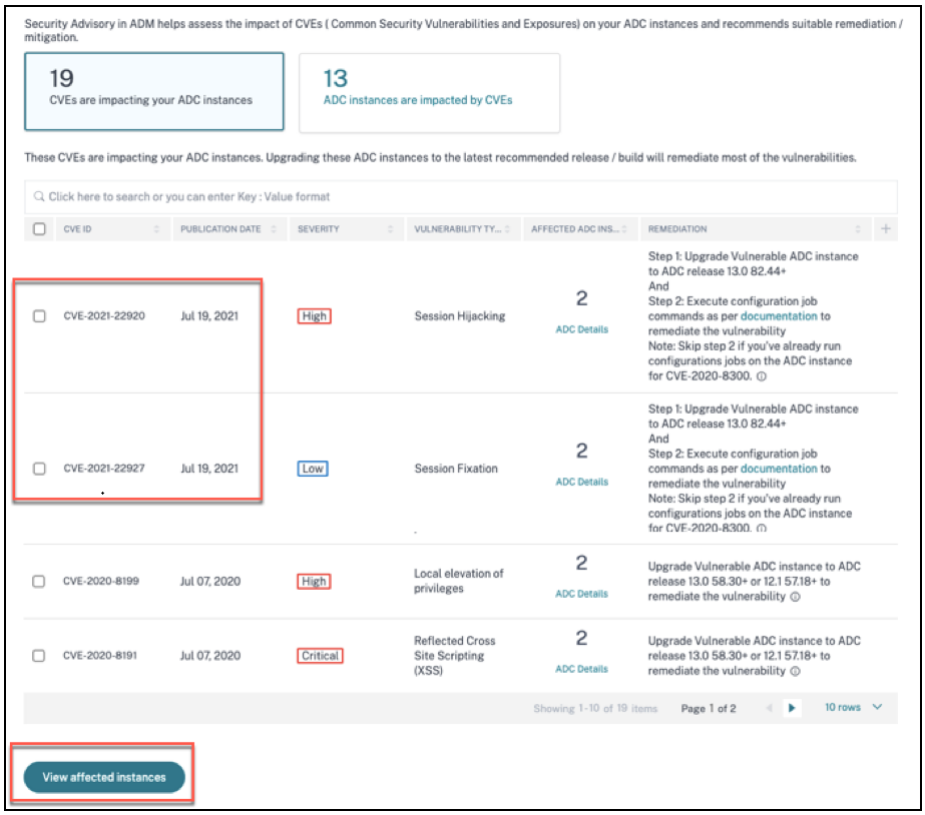
Nachdem der Job ausgeführt wurde, wird er unter **Infrastruktur > Konfiguration > Konfigurationsjobs**angezeigt.

Führen Sie nach Abschluss der beiden Standardisierungsschritte für ADC1 dieselben Schritte aus, um ADC 2 und ADC 3 zu standardisieren. Nach Abschluss der Standardisierung können Sie einen Anforderungsscan ausführen, um die überarbeitete Sicherheitslage zu überprüfen.

Sicherheitsrisiko CVE-2021-22927 und CVE-2021-22920 korrigieren

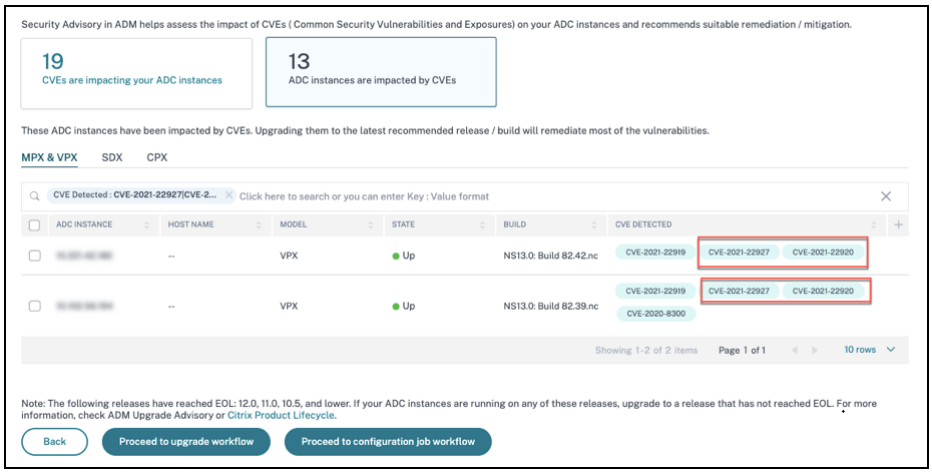
February 5, 2024

Im NetScaler ADM Security Advisory Dashboard unter **Current CVEs > <number of> ADC instances are impacted by CVEs** können Sie alle Instanzen sehen, die aufgrund von CVE-2021-22927 und CVE-2021-22920 anfällig sind. Um die Details der Instanzen zu überprüfen, die von diesen beiden CVEs betroffen sind, wählen Sie mindestens eine CVEs aus und klicken Sie auf **Betroffene Instanzen anzeigen**.



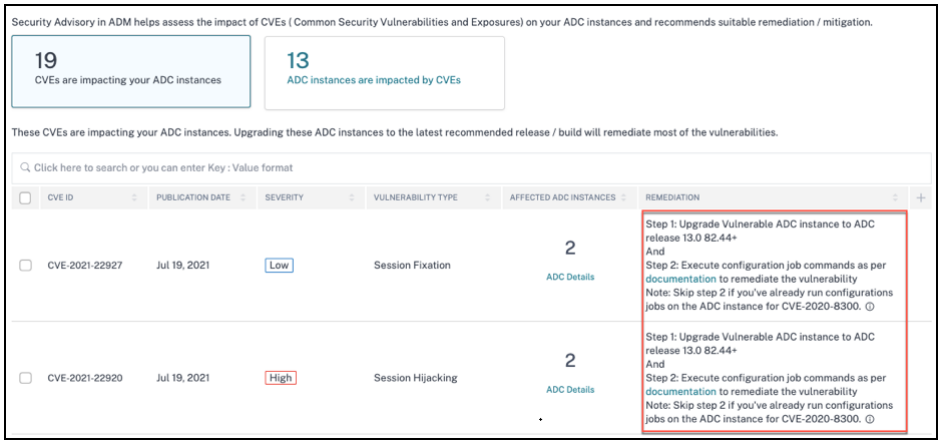
> **Hinweis**
>
> Es kann einige Stunden dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2021-22927 und CVE-2021-22920 im Sicherheitsberatungsmodul widerspiegelt. Um die Auswirkungen früher zu erkennen, starten Sie einen Anforderungsscan, indem Sie auf **Jetzt scannen**klicken.
>
> Weitere Informationen zum Security Advisory Dashboard finden Sie unter Security Advisory.

Das Fenster **<number of> ADC instances impacted by CVEs** wird angezeigt. In der folgenden Bildschirmaufnahme sehen Sie die Anzahl und Details der ADC-Instanzen, die von CVE-2021-22927 und CVE-2021-22920 betroffen sind.



Reparieren Sie CVE-2021-22927 und CVE-2021-22920

Für die von CVE-2021-22927 und CVE-2021-22920 betroffenen ADC-Instanzen ist die Behebung ein zweistufiger Prozess. In der GUI können Sie unter **Aktuelle CVEs > ADC-Instanzen sind von CVEs betroffen**, Schritt 1 und 2 sehen.

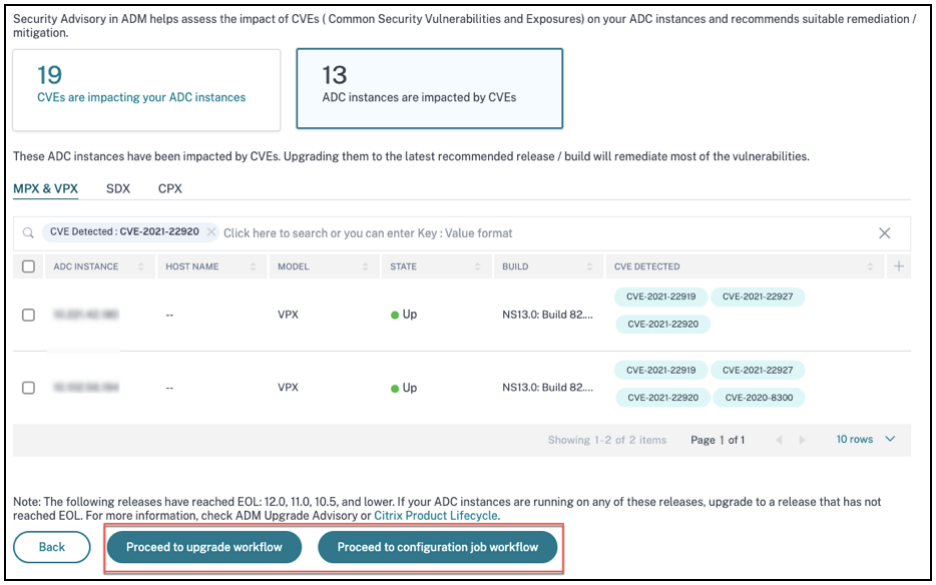


Die zwei Schritte beinhalten:

1. Upgrade der anfälligen ADC-Instanzen auf eine Version und einen Build, der das Update enthält.
2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen. Führen Sie diesen Schritt für jeden anfälligen ADC nacheinander aus und schließen Sie alle SAML-Aktionen für diesen ADC ein.

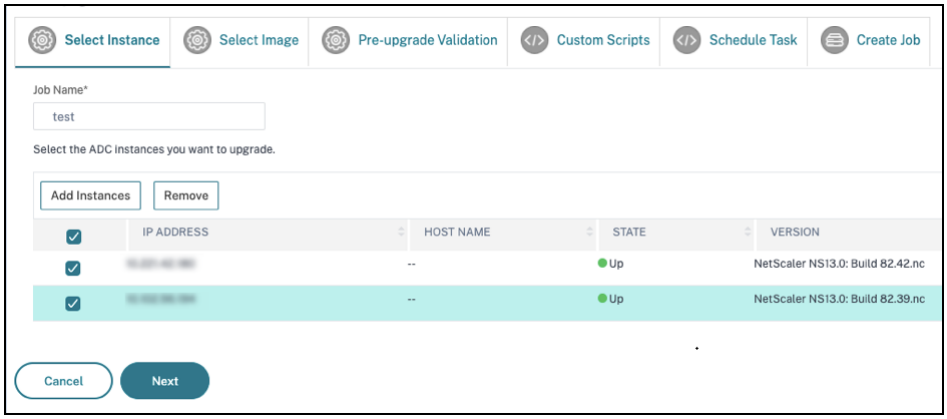
> **Hinweis**
>
> Überspringen Sie Schritt 2, wenn Sie bereits Konfigurationsjobs auf der ADC-Instanz für CVE-2020-8300ausgeführt haben.

Unter **Aktuelle CVEs > ADC-Instanzen, die von CVEs betroffen sind**, sehen Sie zwei separate Workflows für diesen zweistufigen Standardisierungsprozess: **Fortfahren zum Upgrade-Workflow** und **Weiter zum Workflow des Konfigurationsauftrags**.



Schritt 1: Upgrade der anfälligen ADC-Instanzen

Um ein Upgrade der anfälligen Instanzen durchzuführen, wählen Sie die Instanzen aus und klicken Sie **auf Fortfahren mit** Der Upgrade-Workflow wird mit den bereits aufgefüllten anfälligen ADC-Instanzen geöffnet



Weitere Informationen zur Verwendung von NetScaler ADM zum Aktualisieren von ADC-Instanzen finden Sie unter Erstellen eines ADC-Upgrade-Auftrags.

> **Hinweis**
>
> Dieser Schritt kann für alle anfälligen ADC-Instanzen sofort ausgeführt werden.
>
> **Hinweis**
>
> Nachdem Sie Schritt 1 für alle ADC-Instanzen abgeschlossen haben, die für CVE-2021-22920 und CVE-2021-22927 anfällig sind, führen Sie einen Anforderungsscan durch. Die aktualisierte Sicherheitslage unter **Aktuelle CVEs hilft** Ihnen zu verstehen, ob die ADC-Instanzen immer noch für eine dieser CVEs anfällig sind. In der neuen Haltung können Sie auch überprüfen, ob Sie Konfigurationsjobs ausführen müssen.
> Wenn Sie bereits die entsprechenden Konfigurationsjobs auf die ADC-Instanz für CVE-2020-8300 angewendet haben und nun die ADC-Instanz aktualisiert haben, wird die Instanz nach dem Anforderungsscan nicht mehr als anfällig für CVE-2020-8300, CVE-2021-22920 und CVE-2021-22927 angezeigt.

Schritt 2: Anwenden von Konfigurationsbefehlen

Nachdem Sie die betroffenen Instanzen aktualisiert haben, wählen Sie im Fenster **<number of> Von CVEs betroffene ADC-Instanzen** eine Instanz aus, die von CVE-2021-22927 und CVE-2021-22920 betroffen ist, und klicken Sie auf **Weiter zum Workflow des Konfigurationsauftrags**. Der Workflow umfasst die folgenden Schritte.

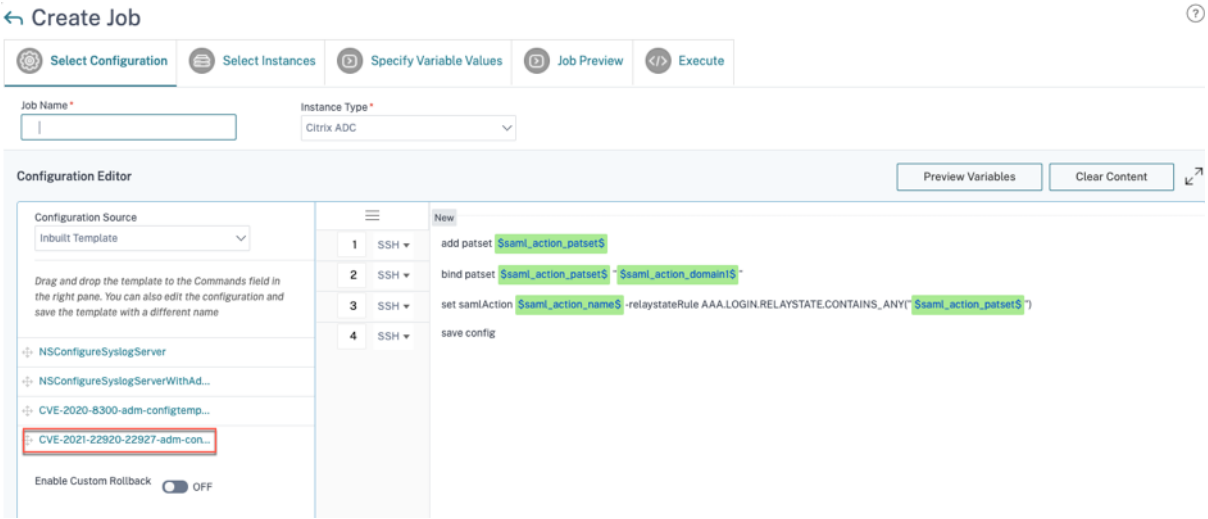
1. Anpassen der Konfiguration.
2. Überprüfung der automatisch ausgefüllten betroffenen Instanzen.
3. Angabe von Eingaben für Variablen für den Job.
4. Überprüfung der endgültigen Konfiguration mit aufgefüllten Variableneingaben.
5. Den Job ausführen.

Beachten Sie die folgenden Punkte, bevor Sie eine Instanz auswählen und auf **Weiter zum Workflow**

des Konfigurationsauftragsklicken:

- Für eine ADC-Instanz, die von mehreren CVEs betroffen ist (z. B. CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 und CVE-2021-22956): Wenn Sie die Instanz auswählen und auf **Weiter zum Workflow des Konfigurationsauftrags**klicken, wird die integrierte Konfigurationsvorlage unter Konfiguration auswählen nicht automatisch ausgefüllt. Ziehen Sie die entsprechende Konfigurationsjob-Vorlage manuell unter **Security Advisory Template** in den Konfigurationsjob-Fensterbereich auf der rechten Seite.
- Für mehrere ADC-Instanzen, die nur von CVE-2021-22956 betroffen sind: Sie können Konfigurationsjobs auf allen Instanzen gleichzeitig ausführen. Sie haben beispielsweise ADC 1, ADC 2 und ADC 3, und alle von ihnen sind nur von CVE-2021-22956 betroffen. Wählen Sie alle diese Instanzen aus und klicken Sie auf **Weiter zum Workflow des Konfigurationsauftrags**. Die integrierte Konfigurationsvorlage wird automatisch unter **Konfiguration auswählen**ausgefüllt.
- Bei mehreren ADC-Instanzen, die von CVE-2021-22956 betroffen sind, und einem oder mehreren anderen CVEs (z. B. CVE-2020-8300, CVE-2021-22927 und CVE-2021-22920), bei denen die Standardisierung auf jeden ADC gleichzeitig angewendet werden muss: Wenn Sie diese Instanzen auswählen und auf **Weiter zum Workflow des Konfigurationsauftrags**klicken, wird ein Fehler angezeigt Es wird eine Meldung angezeigt, in der Sie aufgefordert werden, den Konfigurationsjob auf jedem ADC gleichzeitig auszuführen.

Schritt 1: Konfiguration wählen Im Workflow des Konfigurationsauftrags wird die integrierte Konfigurationsbasisvorlage automatisch unter **Konfiguration auswählen** ausgefüllt.



Hinweis

Wenn die in Schritt 2 zum Anwenden von Konfigurationsbefehlen ausgewählte ADC-Instanz anfällig für CVE-2021-22927, CVE-2021-22920 und auch CVE-2020-8300 ist, wird die Basisvorlage

> für CVE-2020-8300 automatisch ausgefüllt. Die Vorlage CVE-2020-8300 ist ein Supersatz der Konfigurationsbefehle, die für alle drei CVEs erforderlich sind. Passen Sie diese Basisvorlage entsprechend Ihrer ADC-Instanzbereitstellung und den Anforderungen an.

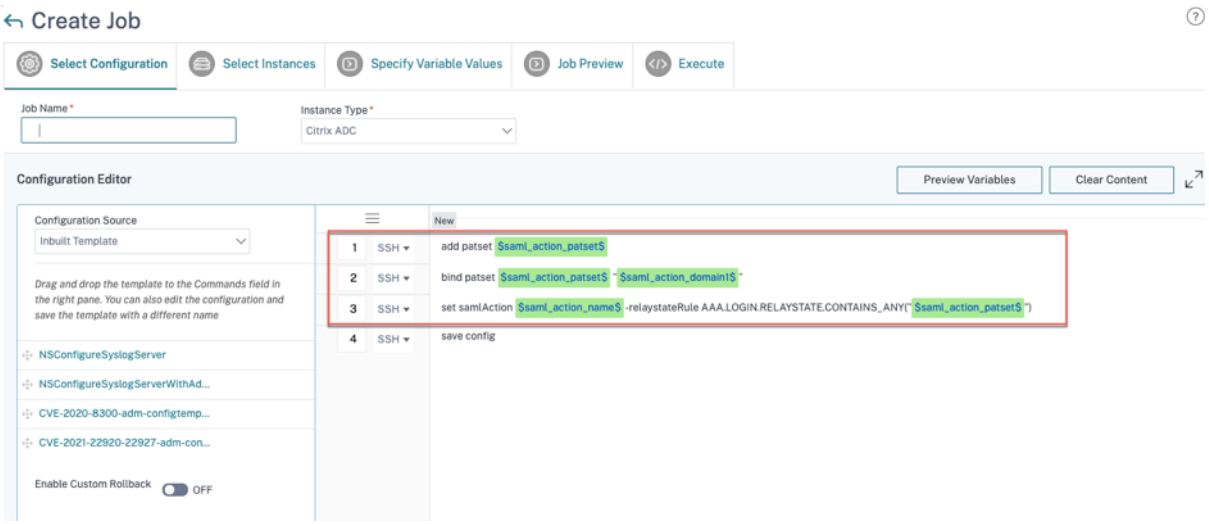
Sie müssen für jede betroffene ADC-Instanz nacheinander einen separaten Konfigurationsauftrag ausführen und alle SAML-Aktionen für diesen ADC einbeziehen. Wenn Sie beispielsweise zwei anfällige ADC-Instanzen mit jeweils zwei SAML-Aktionen haben, müssen Sie diesen Konfigurationsauftrag zweimal ausführen. Einmal pro ADC, das alle seine SAML-Aktionen abdeckt.

ADC 1	ADC2
Job 1: zwei SAML-Aktionen	Job 2: zwei SAML-Aktionen

Geben Sie dem Job einen Namen und passen Sie die Vorlage an die folgenden Spezifikationen an. Die integrierte Konfigurationsvorlage ist nur eine Gliederung oder Basisvorlage. Passen Sie die Vorlage basierend auf Ihrer Bereitstellung an die folgenden Anforderungen an:

a. **SAML-Aktionen und die zugehörigen Domänen**

Abhängig von der Anzahl der SAML-Aktionen, die Sie in Ihrer Bereitstellung haben, müssen Sie die Zeilen 1—3 replizieren und die Domänen für jede SAML-Aktion anpassen.

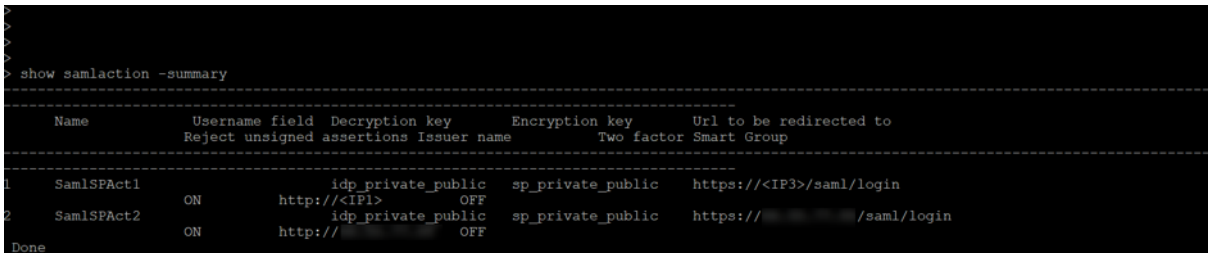


Wenn Sie beispielsweise zwei SAML-Aktionen haben, wiederholen Sie die Zeilen 1—3 zweimal und passen Sie die Variablendefinitionen für jede SAML-Aktion entsprechend an.

Und wenn Sie N Domänen für eine SAML-Aktion haben, müssen Sie die Zeile `bind patset $saml_action_patset$ "$saml_action_domain1$"` mehrmals manuell eingeben, um sicherzustellen, dass die Zeile N Mal für diese SAML-Aktion angezeigt wird. Und ändern Sie die folgenden Variablendefinitionsnamen:

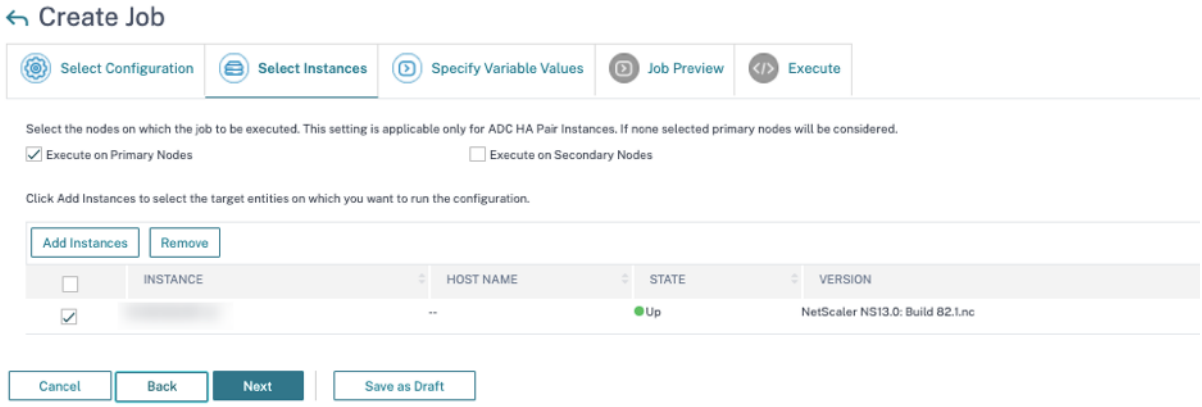
- `saml_action_patset`: ist die Konfigurations-Template-Variable und stellt den Wert des Namens des Mustersatzes (patset) für die SAML-Aktion dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsjob-Workflows angeben. Weitere Informationen finden Sie im Abschnitt Schritt 3: Variablenwerte angeben in diesem Dokument.
- `saml_action_domain1`: ist die Konfigurationsvorlagenvariable und stellt den Domänennamen für diese spezifische SAML-Aktion dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsjob-Workflows angeben. Weitere Informationen finden Sie im Abschnitt Schritt 3: Variablenwerte angeben in diesem Dokument.

Führen Sie den Befehl aus, um alle SAML-Aktionen für ein Gerät zu finden `show samlaction`.



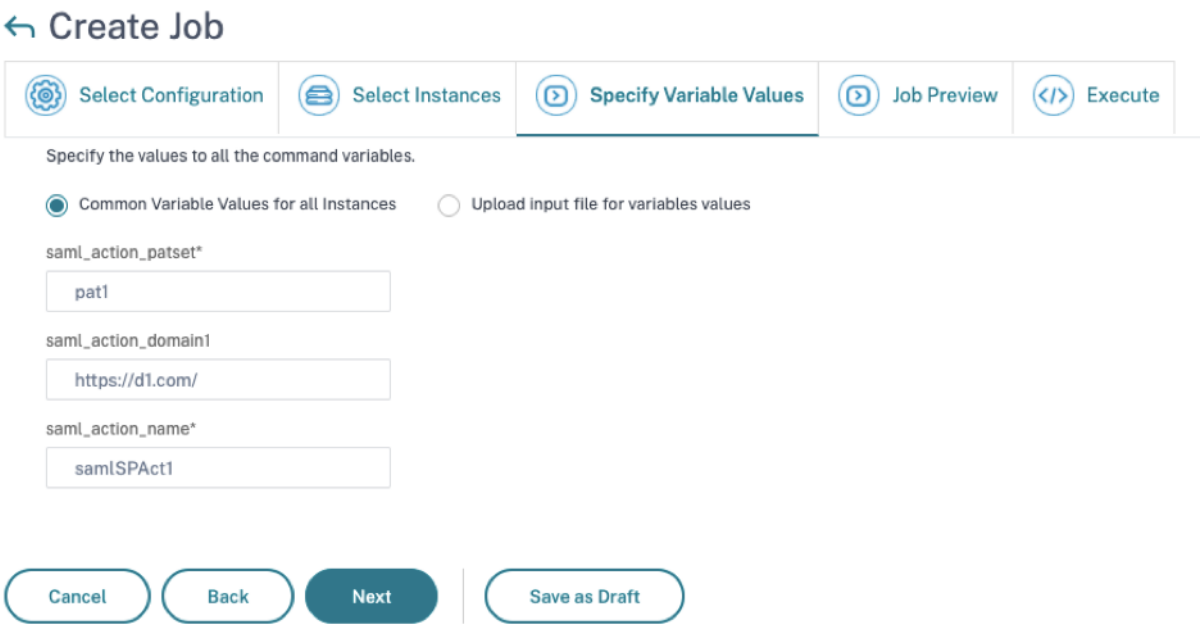
Schritt 2: Wählen Sie die Instanz aus

Die betroffene Instanz wird automatisch unter **Ausgewählte Instanzen**aufgefüllt. Wählen Sie die Instanz und klicken Sie auf **Weiter**.

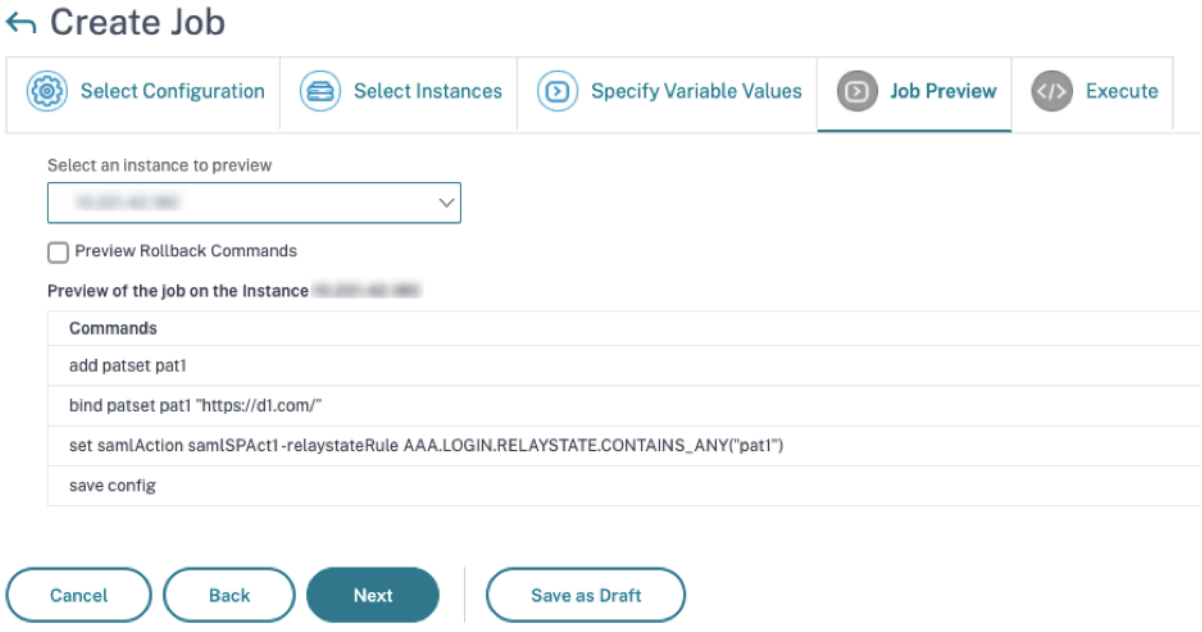


Schritt 3: Variablenwerte angeben Geben Sie die Werte der Variablen ein.

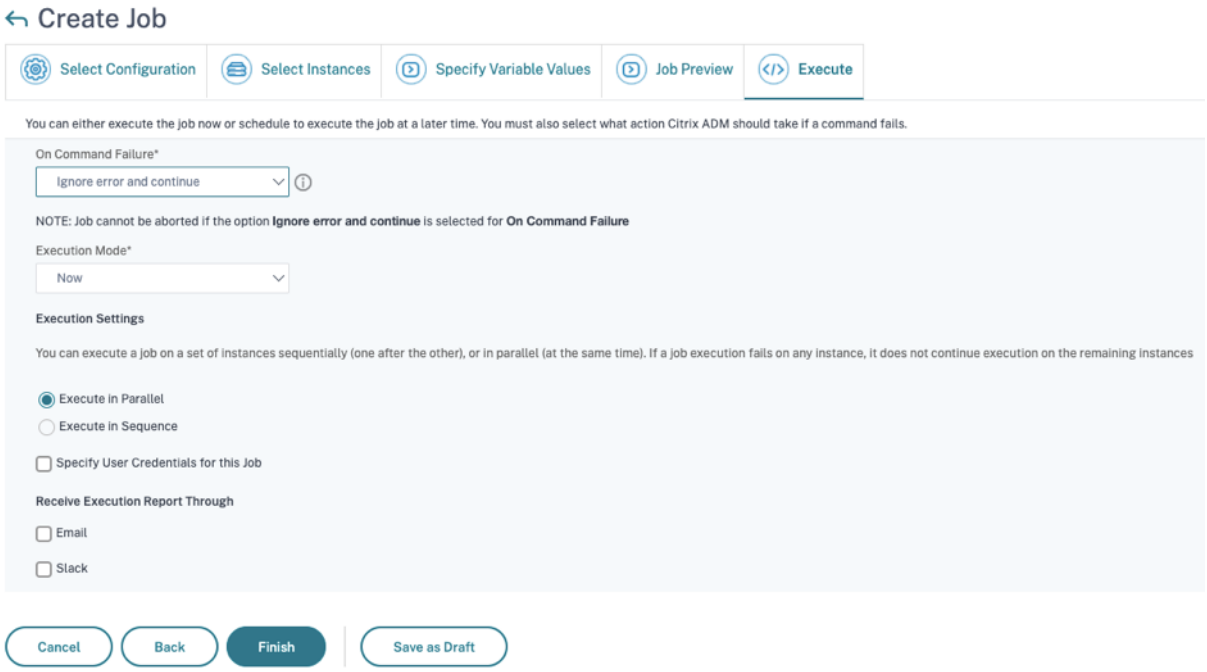
- `saml_action_patset`: Namen für die SAML-Aktion hinzufügen
- `saml_action_domain1`: Domäne im Format `https://<example1.com>/` eingeben
- `saml_action_name`: Dieselbe SAML-Aktion eingeben, für die Sie den Job konfigurieren



Schritt 4: Vorschau der Konfiguration Zeigt eine Vorschau der in die Konfiguration eingefügten Variablenwerte an und klicken Sie auf **Weiter**.



Schritt 5: Führen Sie den Job aus Klicken Sie auf **Fertigstellen**, um den Konfigurationsauftrag auszuführen.



Nachdem der Job ausgeführt wurde, wird er unter **Infrastruktur > Konfiguration > Konfigurationsjobs**angezeigt.

Nachdem Sie die beiden Korrekturschritte für alle anfälligen ADCs abgeschlossen haben, können Sie einen Anforderungsscan ausführen, um die überarbeitete Sicherheitslage zu überprüfen.

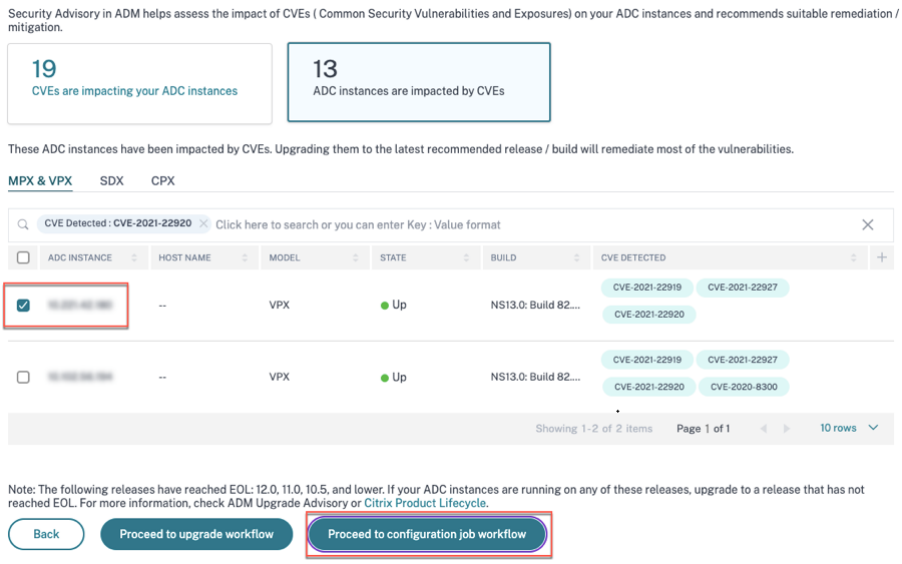
Szenario

In diesem Szenario sind zwei ADC-Instanzen anfällig für CVE-2021-22920, und Sie müssen alle Instanzen standardisieren. Führen Sie die folgenden Schritte aus:

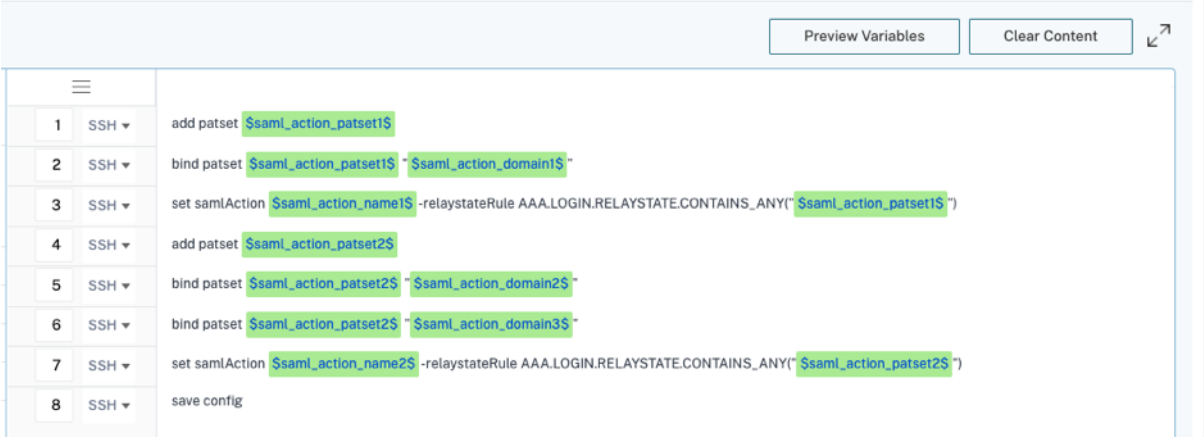
1. Führen Sie ein Upgrade aller drei ADC-Instanzen durch, indem Sie die im Abschnitt “Upgrade einer Instanz”in diesem Dokument angegebenen Schritte ausführen.
2. Wenden Sie den Konfigurationspatch mithilfe des Konfigurationsjob-Workflows auf jeweils einen ADC an. Lesen Sie die Schritte, die im Abschnitt “Konfigurationsbefehle anwenden”in diesem Dokument beschrieben werden.

Der anfällige ADC 1 hat zwei SAML-Aktionen:

- SAML action 1 hat eine Domain
- SAML-Aktion 2 hat zwei Domänen



Wählen Sie ADC 1 und klicken Sie auf **Weiter zum Workflow des Konfigurationsauftrags** Die integrierte Basisvorlage wird automatisch ausgefüllt. Geben Sie als Nächstes einen Auftragsnamen an und passen Sie die Vorlage entsprechend der angegebenen Konfiguration an.

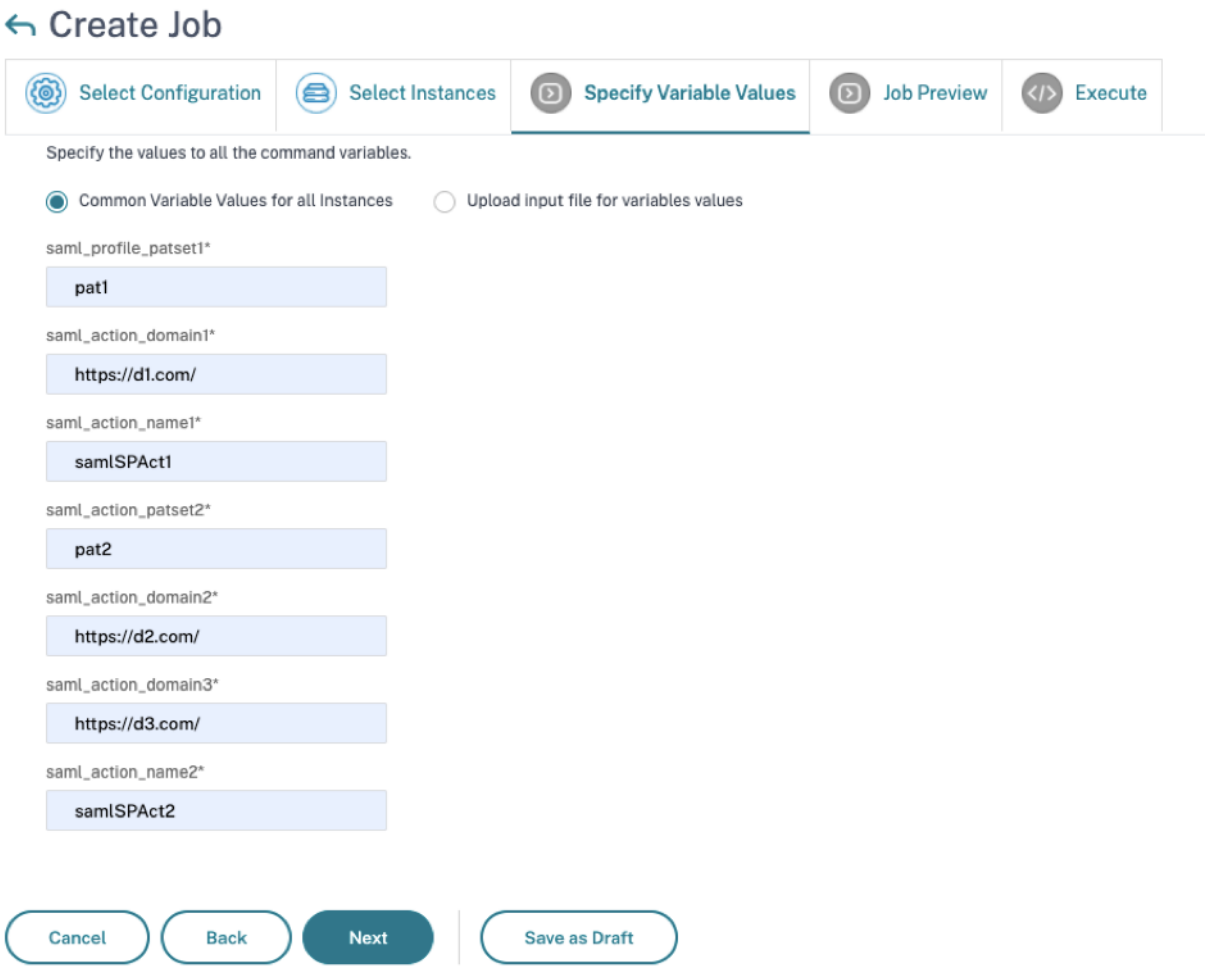


In der folgenden Tabelle sind die Variablendefinitionen für benutzerdefinierte Parameter aufgeführt.

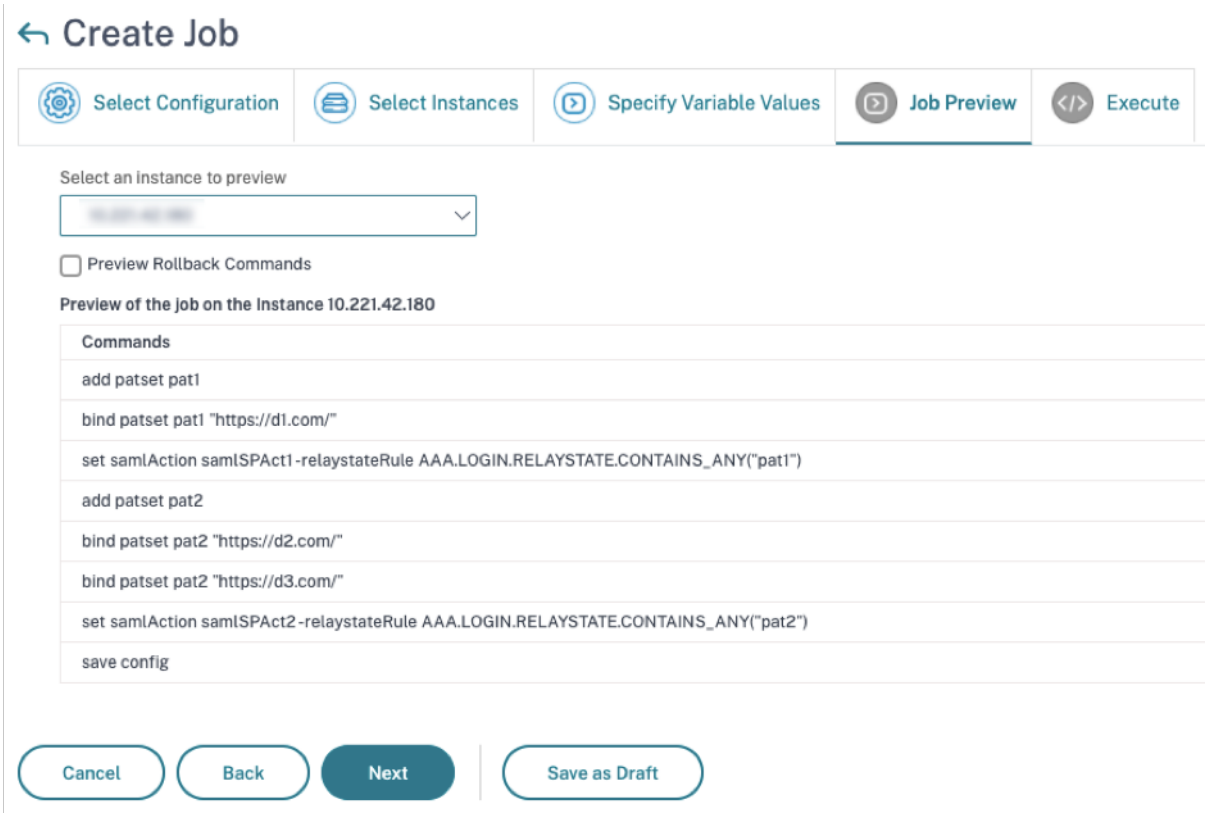
Tabelle. Variablendefinitionen für SAML-Aktionen

ADC-Konfiguration	Variablendefinition für Patset	Variablendefinition für den SAML-Aktionsnamen	Variablendefinition für Domain
SAML action 1 hat eine Domain	saml_action_patset1	saml_action_name1	saml_action_domain1
SAML-Aktion 2 hat zwei Domänen	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

Wählen Sie unter **Instanzen auswählen** ADC 1 aus und klicken Sie auf **Weiter**. Das Fenster **Variablenwerte angeben** wird angezeigt. In diesem Schritt müssen Sie Werte für alle im vorherigen Schritt definierten Variablen angeben.



Überprüfen Sie als Nächstes die Variablen.



Klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um den Job auszuführen.

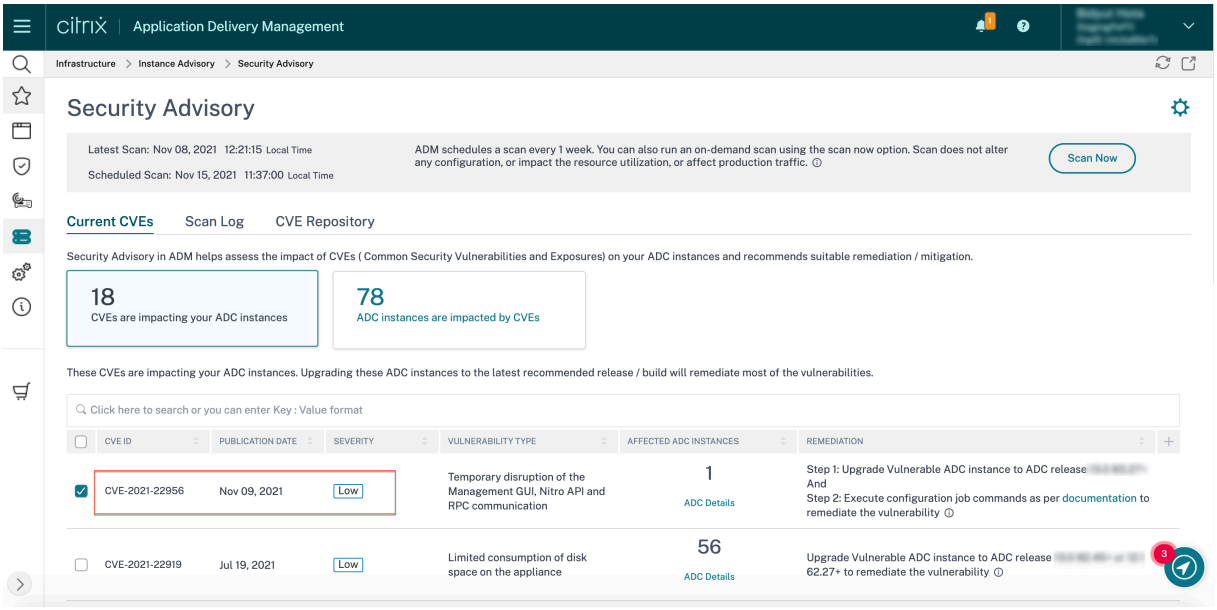
Nachdem der Job ausgeführt wurde, wird er unter **Infrastruktur > Konfiguration > Konfigurationsjobs**angezeigt.

Führen Sie nach Abschluss der beiden Standardisierungsschritte für ADC1 dieselben Schritte aus, um ADC 2 und ADC 3 zu standardisieren. Nach Abschluss der Standardisierung können Sie einen Anforderungsscan ausführen, um die überarbeitete Sicherheitslage zu überprüfen.

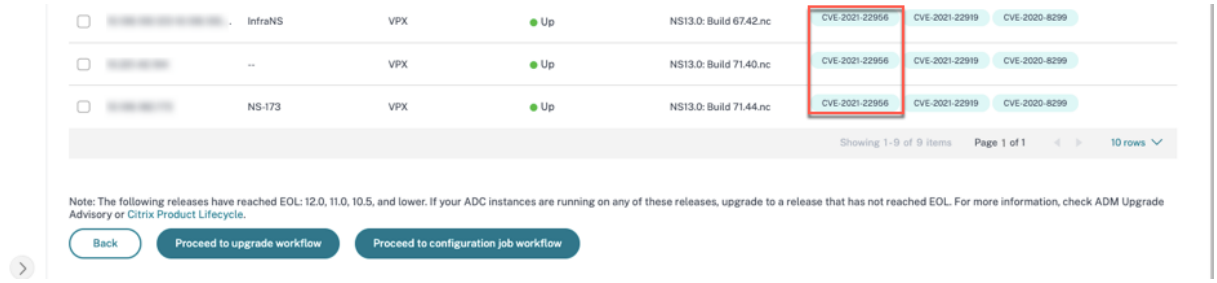
Sicherheitsrisiko CVE-2021-22956 identifizieren und korrigieren

February 5, 2024

Im NetScaler ADM Security Advisory Dashboard unter**Aktuelle CVEs <number of>**ADC-Instanzen sind von allgemeinen Schwachstellen und Exposures (CVEs) betroffen, können Sie alle Instanzen sehen, die aufgrund dieser speziellen CVE anfällig sind. Um die Details der von CVE-2021-22956 betroffenen Instanzen zu überprüfen, wählen Sie CVE-2021-22956 und klicken Sie auf **Betroffene Instanzen anzeigen**.



Das Fenster "Von CVEs betroffene<number of>ADC-Instanzen"wird angezeigt. Hier sehen Sie die Anzahl und Details der ADC-Instanzen, die von CVE-2021-22956 betroffen sind.



Weitere Informationen zum Security Advisory Dashboard finden Sie unter Security Advisory.

> **Hinweis**
>
> Es kann einige Zeit dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2021-22956 im Sicherheitsberatungsmodul widerspiegelt. Um die Auswirkungen früher zu erkennen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen**klicken.

Identifizieren von CVE-2021-22956 betroffenen Instanzen

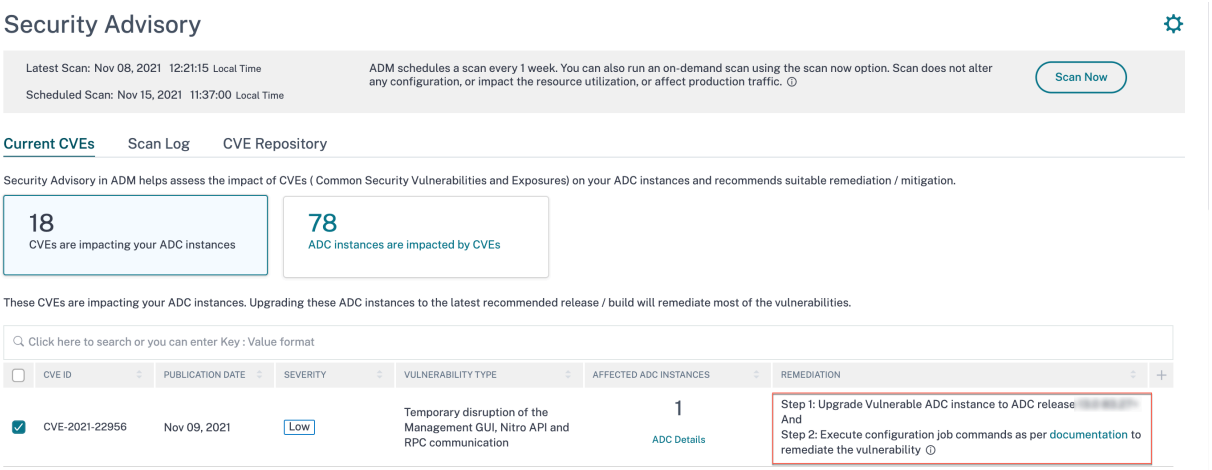
CVE-2021-22956 erfordert einen benutzerdefinierten Scan, bei dem der ADM Service eine Verbindung mit der verwalteten ADC-Instanz herstellt und ein Skript an die Instanz sendet. Das Skript wird auf der ADC-Instanz ausgeführt und überprüft die Parameter der Apache-Konfigurationsdatei (`httpd.conf file`) und die maximalen Clientverbindungen (`maxclient`), um festzustellen, ob eine Instanz verwundbar ist oder nicht. Die Informationen, die das Skript mit dem ADM Service teilt, sind der Schwachstellenstatus im booleschen Wert (true oder false). Das Skript gibt dem ADM Service auch

eine Liste von Zählern für max_clients für verschiedene Netzwerkschnittstellen zurück, z. B. lokaler Host, NSIP und SNIP mit Verwaltungszugriff.

Dieses Skript wird jedes Mal ausgeführt, wenn Ihre geplanten Scans auf Anforderung ausgeführt werden. Nachdem der Scan abgeschlossen ist, wird das Skript aus der ADC-Instanz gelöscht.

Korrigieren CVE-2021-22956

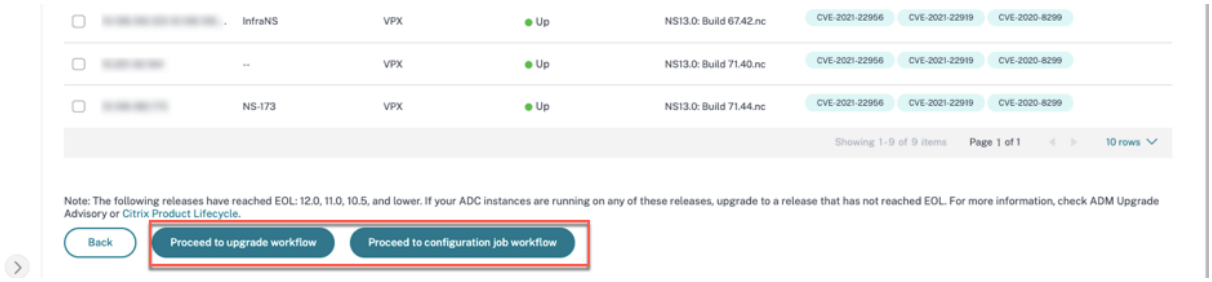
Für von CVE-2021-22956 betroffene ADC-Instanzen ist die Behebung ein zweistufiger Prozess. In der GUI können Sie unter**Aktuelle CVEs > ADC-Instanzen sind von CVEs betroffen**, Schritt 1 und 2 sehen.



Die zwei Schritte beinhalten:

1. Upgrade der anfälligen ADC-Instanzen auf eine Version und einen Build, der das Update enthält.
2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen.

Unter Aktuelle CVEs > ADC-Instanzen, die von CVEs betroffen sind, sehen Sie zwei separate Workflows für diesen zweistufigen Standardisierungsprozess: Fortfahren zum Upgrade-Workflow und Weiter zum Workflow des Konfigurationsauftrags.



Schritt 1: Upgrade der anfälligen ADC-Instanzen

Um ein Upgrade der anfälligen Instanzen durchzuführen, wählen Sie die Instanzen aus und klicken Sie **auf Fortfahren mit** Der Upgrade-Workflow wird mit den bereits aufgefüllten anfälligen ADC-Instanzen geöffnet

Weitere Informationen zur Verwendung von NetScaler ADM zum Aktualisieren von ADC-Instanzen finden Sie unter Erstellen eines ADC-Upgrade-Auftrags.

> **Hinweis**
>
> Dieser Schritt kann für alle anfälligen ADC-Instanzen sofort ausgeführt werden.

Schritt 2: Anwenden von Konfigurationsbefehlen

Nachdem Sie die betroffenen Instanzen aktualisiert haben, wählen Sie im Fenster **<number of> Von CVEs betroffene ADC-Instanzen** die von CVE-2021-2295 betroffene Instanz aus und klicken Sie auf **Weiter zum Workflow des Konfigurationsauftrags**. Der Workflow umfasst die folgenden Schritte.

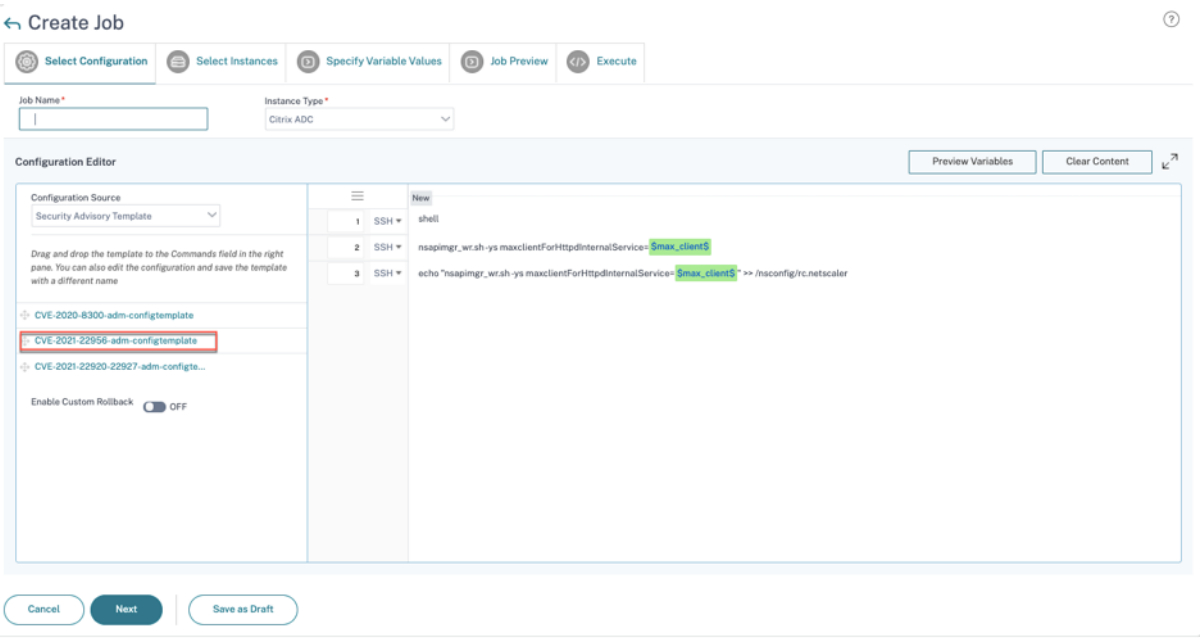
1. Anpassen der Konfiguration.
2. Überprüfung der automatisch ausgefüllten betroffenen Instanzen.
3. Angabe von Eingaben für Variablen für den Job.
4. Überprüfung der endgültigen Konfiguration mit aufgefüllten Variableneingaben.
5. Den Job ausführen.

Beachten Sie die folgenden Punkte, bevor Sie eine Instanz auswählen und auf **Weiter zum Workflow des Konfigurationsauftrags**klicken:

- Für eine ADC-Instanz, die von mehreren CVEs betroffen ist (z. B. CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 und CVE-2021-22956): Wenn Sie die Instanz auswählen und auf **Weiter zum Workflow des Konfigurationsauftrags**klicken, wird die integrierte Konfigurationsvorlage unter Konfiguration auswählen nicht automatisch ausgefüllt. Ziehen Sie die entsprechende Konfigurationsjob-Vorlage manuell unter **Security Advisory Template** in den Konfigurationsjob-Fensterbereich auf der rechten Seite.
- Für mehrere ADC-Instanzen, die nur von CVE-2021-22956 betroffen sind: Sie können Konfigurationsjobs auf allen Instanzen gleichzeitig ausführen. Sie haben beispielsweise ADC 1, ADC 2 und ADC 3, und alle von ihnen sind nur von CVE-2021-22956 betroffen. Wählen Sie alle diese Instanzen aus und klicken Sie auf **Weiter zum Workflow des Konfigurationsauftrags**. Die integrierte Konfigurationsvorlage wird automatisch unter **Konfiguration auswählen**ausgefüllt. Beziehen Sie sich auf das bekannte Problem NSADM-80913 in den Versionshinweisen.
- Bei mehreren ADC-Instanzen, die von CVE-2021-22956 betroffen sind, und einem oder mehreren anderen CVEs (z. B. CVE-2020-8300, CVE-2021-22927 und CVE-2021-22920), bei de-

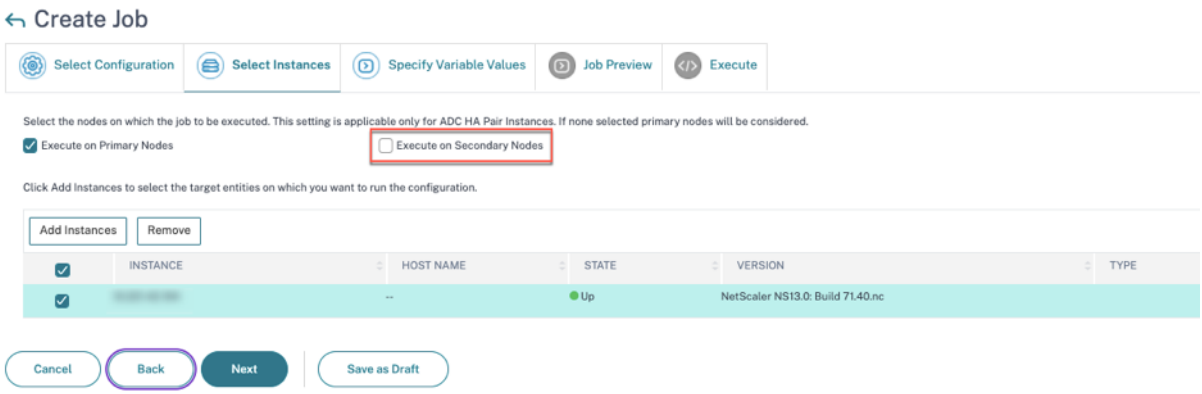
nen die Standardisierung auf jeden ADC gleichzeitig angewendet werden muss: Wenn Sie diese Instanzen auswählen und auf **Weiter zum Workflow des Konfigurationsauftrags**klicken, wird ein Fehler angezeigt Es wird eine Meldung angezeigt, in der Sie aufgefordert werden, den Konfigurationsjob auf jedem ADC gleichzeitig auszuführen.

Schritt 1: Konfiguration wählen Im Workflow des Konfigurationsauftrags wird die integrierte Konfigurationsbasisvorlage automatisch unter **Konfiguration auswählen** ausgefüllt.



Schritt 2: Wählen Sie die Instanz aus

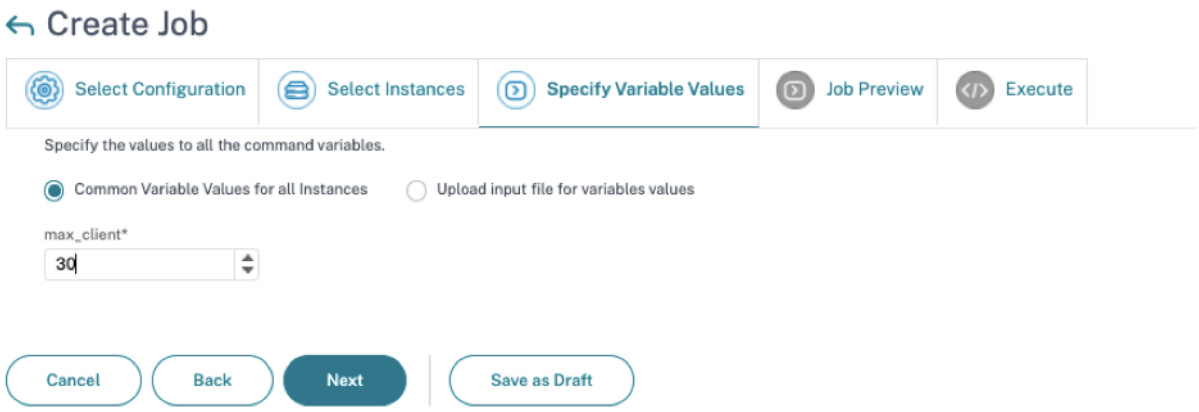
Die betroffene Instanz wird automatisch unter **Ausgewählte Instanzen**aufgefüllt. Wählen Sie die Instanz aus. Wenn diese Instanz Teil eines HA-Paars ist, wählen Sie **Auf sekundären Knoten ausführen**aus. Klicken Sie auf **Weiter**.



> **Hinweis**
>
> Für ADC-Instanzen im Clustermodus unterstützt ADM mithilfe der ADM-Sicherheitsempfehlung die Ausführung des Konfigurationsauftrags nur auf dem CCO-Knoten (Cluster Configuration Coordinator). Führen Sie die Befehle auf Nicht-CCO-Knoten separat aus.

`rc.netscaler` wird über alle HA- und Clusterknoten hinweg synchronisiert, sodass die Standardisierung nach jedem Neustart dauerhaft ist.

Schritt 3: Variablenwerte angeben Geben Sie die Werte der Variablen ein.



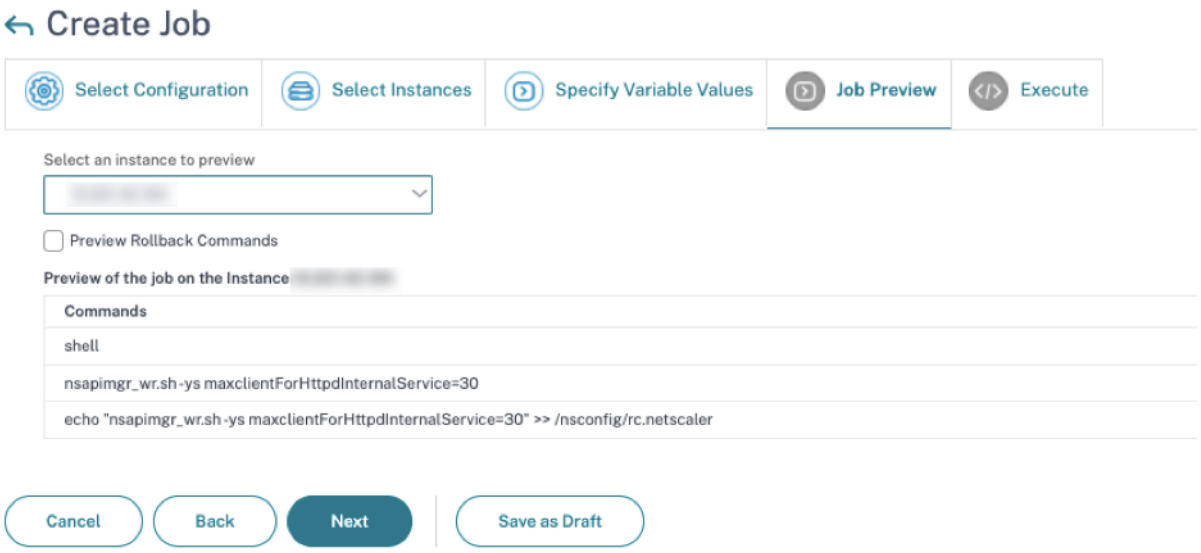
Wählen Sie eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:

Gemeinsame Variablenwerte für alle Instanzen: Geben Sie einen gemeinsamen Wert für die Variable ein `max_client`.

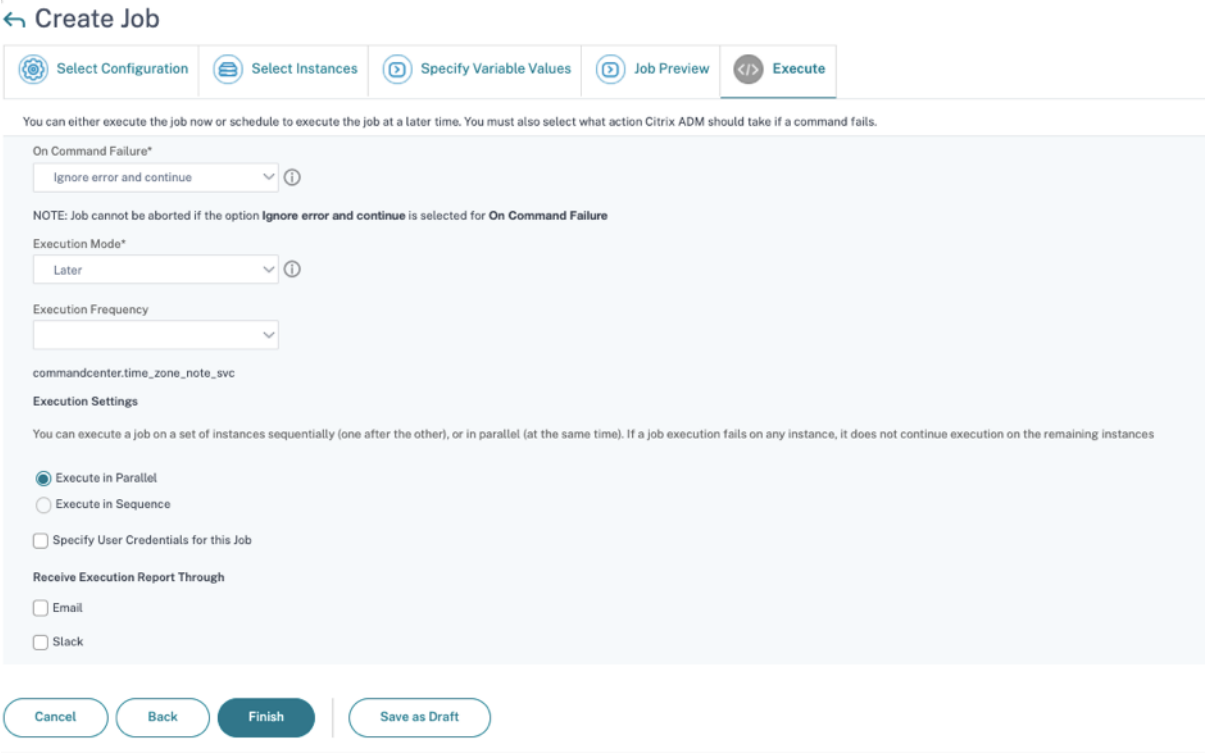
Eingabedatei für Variablenwerte hochladen: Klicken Sie auf **Eingabeschlüsseldatei herunterladen**, um eine Eingabedatei herunterzuladen. Geben Sie in der Eingabedatei Werte für die Variable `max_client` ein und laden Sie die Datei dann auf den ADM-Server hoch. Lesen Sie das bekannte Problem NSADM-80913 in den Versionshinweisen zu einem Problem mit dieser Option.

> **Hinweis**
>
> Für beide oben genannten Optionen ist der empfohlene Wert für `max_client` 30. Sie können den Wert entsprechend Ihrem aktuellen Wert festlegen. Sollte jedoch nicht Null sein, und sollte kleiner oder gleich max_client in der Datei `/etc/httpd.conf` sein. Sie können den aktuellen Wert überprüfen, der in der Konfigurationsdatei des Apache HTTP-Servers `/etc/httpd.conf` festgelegt ist, indem Sie die Zeichenfolge `MaxClients` in der ADC-Instanz suchen

Schritt 4: Vorschau der Konfiguration Zeigt eine Vorschau der in die Konfiguration eingefügten Variablenwerte an und klicken Sie auf **Weiter**.



Schritt 5: Führen Sie den Job aus Klicken Sie auf **Fertigstellen**, um den Konfigurationsauftrag auszuführen.



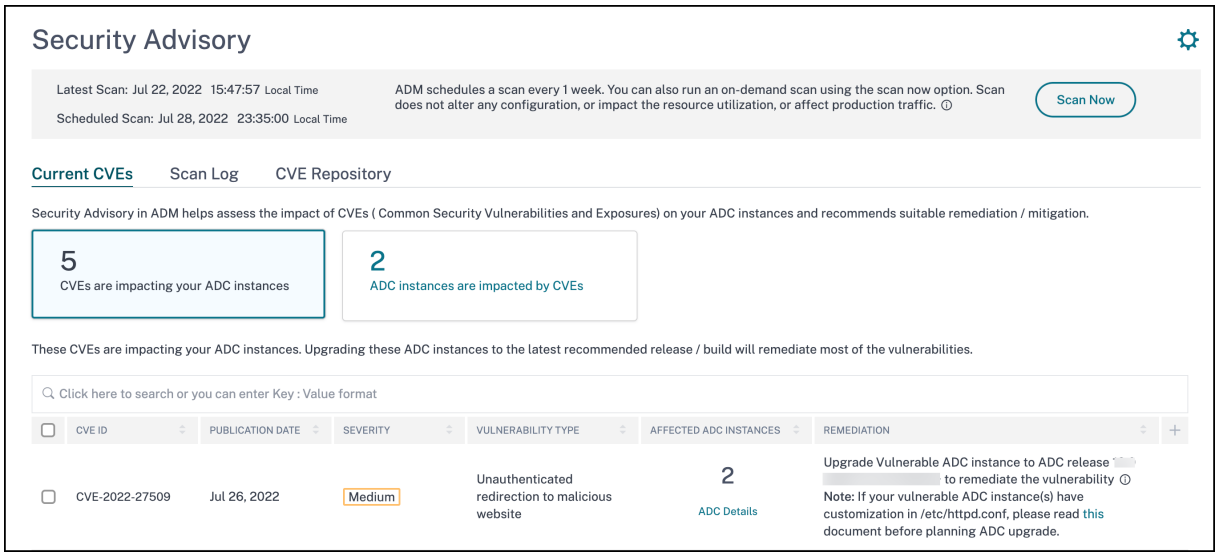
Nachdem der Job ausgeführt wurde, wird er unter **Infrastruktur > Konfiguration > Konfigurationsjobs**angezeigt.

Nachdem Sie die beiden Korrekturschritte für alle anfälligen ADCs abgeschlossen haben, können Sie einen Anforderungsscan ausführen, um die überarbeitete Sicherheitslage zu überprüfen.

Sicherheitsrisiko CVE-2022-27509 identifizieren und korrigieren

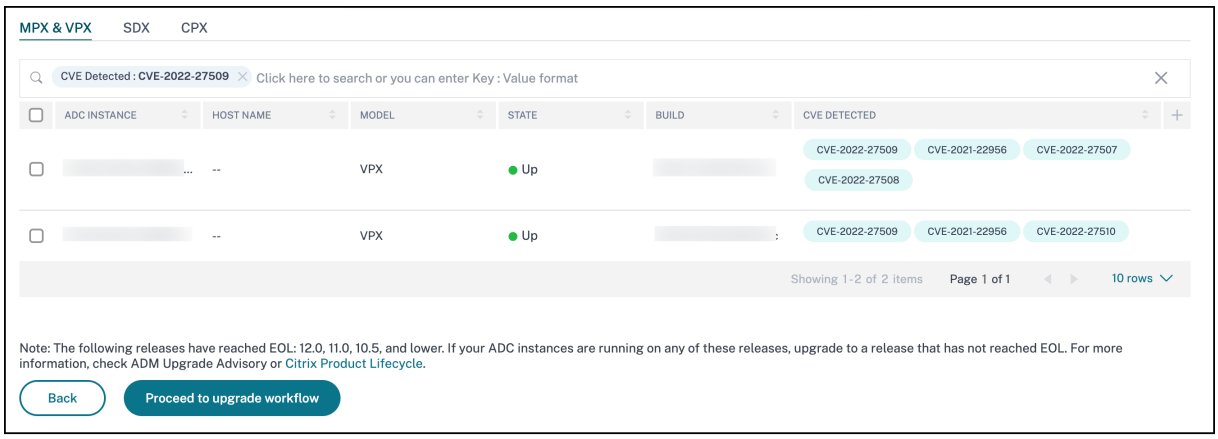
February 5, 2024

Im NetScaler ADM Security Advisory Dashboard unter **Current CVEs <number of> ADC instances are impacted by CVEs** sehen Sie alle Instanzen, die aufgrund von CVE-2022-27509 anfällig sind. Um die Details der von den CVEs betroffenen Instanzen zu überprüfen, wählen Sie CVE-2022-27509 und klicken Sie auf **Betroffene Instanzen anzeigen**.



> **Hinweis**
>
> Um den Grund für die ADC-Schwachstelle zu verstehen, laden Sie den CSV-Bericht auf der Registerkarte Scanprotokolle in Security Advisory herunter.

Das Fenster **<number of> ADC instances impacted by CVEs** wird angezeigt. In der folgenden Bildschirmaufnahme sehen Sie die Anzahl und Details der ADC-Instanzen, die von CVE-2022-27509 betroffen sind.



Weitere Informationen zum Security Advisory Dashboard finden Sie unter Security Advisory.

> **Hinweis**
>
> Es kann einige Stunden dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2022-27509 im Sicherheitsberatungsmodul widerspiegelt. Um die Auswirkungen früher zu erkennen, starten Sie einen Anforderungsscan, indem Sie auf **Jetzt scannen**klicken.

Identifizieren von CVE-2022-27509 betroffenen Instanzen

CVE-2022-27509 erfordert eine Kombination aus benutzerdefiniertem Scan und Versionsscan. Im Rahmen des benutzerdefinierten Scans stellt der ADM Service eine Verbindung mit der verwalteten ADC-Instanz her und sendet ein Skript an die Instanz. Das Skript wird auf der ADC-Instanz ausgeführt und ermittelt, ob die Instanz anfällig ist. Dieses Skript wird jedes Mal ausgeführt, wenn Ihr geplanter Scan oder ein Scan auf Anforderung

Nachdem der Scan abgeschlossen ist, wird das Skript aus der ADC-Instanz gelöscht.

Sie können diese benutzerdefinierten Scans von Security Advisory auch deaktivieren. Weitere Informationen zu benutzerdefinierten Sucheinstellungen und zum Deaktivieren benutzerdefinierter Scans finden Sie im Abschnitt **Konfigurieren der Einstellungen für die benutzerdefinierte Suche** auf der Seite **Sicherheitsempfehlung** .

Korrigieren CVE-2022-27509

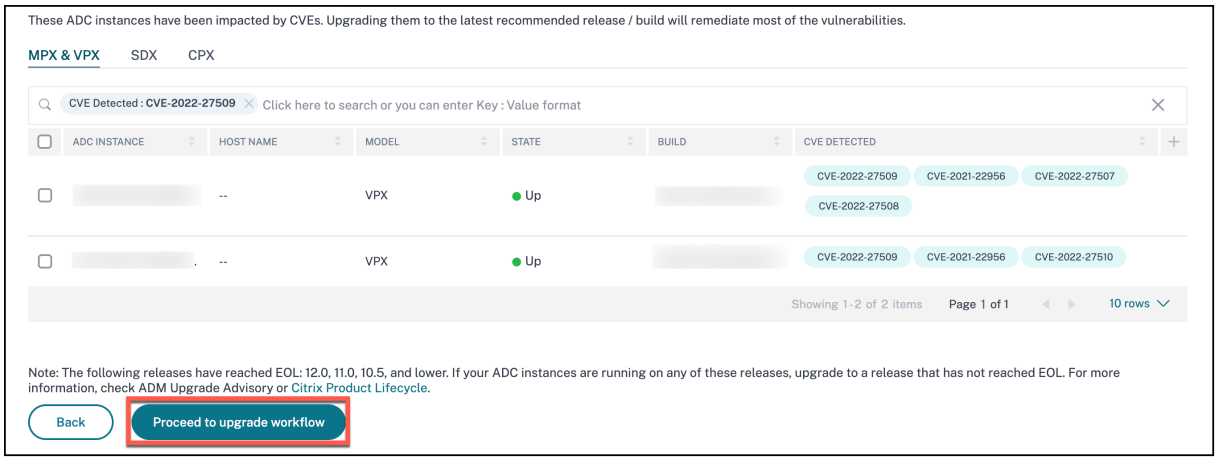
Bei ADC-Instanzen, die von CVE-2022-27509 betroffen sind, ist die Standardisierung ein einstufiger Prozess, und Sie müssen die anfälligen ADC-Instanzen auf eine Version und einen Build aktualisieren, die das Update enthalten. In der GUI können Sie unter **Aktuelle CVEs > ADC-Instanzen sind von CVEs betroffen**, den Schritt zur Standardisierung sehen.

Unter **Aktuelle CVEs > Von CVEs betroffene ADC-Instanzen**sehen Sie den folgenden Workflow für diesen einstufigen Standardisierungsprozess: **Fortfahren mit dem Upgrade-Workflow**.

Um ein Upgrade der anfälligen Instanzen durchzuführen, wählen Sie die Instanzen aus und klicken Sie **auf Fortfahren mit** Der Upgrade-Workflow wird mit den bereits aufgefüllten anfälligen ADC-Instanzen geöffnet

> **WICHTIG**
>
> Wenn Ihre anfälligen ADC-Instanzen die Datei /etc/httpd.conf in das Verzeichnis /nsconfig kopiert haben, lesen Sie vor dem Planen eines ADC-Upgrades die Upgrade-Überlegungen für angepasste ADC-Konfigurationen .

Weitere Informationen zur Verwendung von NetScaler ADM zum Aktualisieren von ADC-Instanzen finden Sie unter Erstellen eines ADC-Upgrade-Auftrags.



Nicht unterstützte CVEs in den Sicherheitsempfehlungen

February 5, 2024

Die NetScaler ADM Security Advisory verfolgt alle neuen Common Vulnerabilities and Exposures (CVEs) und bewertet die Auswirkungen von CVEs auf die Infrastruktur. Sie können die Empfehlungen überprüfen und geeignete Maßnahmen ergreifen. Es gibt jedoch einige CVEs, die nicht unterstützt werden, und die Erkennung und Behebung der Sicherheitsanfälligkeiten liegt außerhalb des Bereichs der NetScaler ADM Security Advisory.

- **CVE-2022—21827**:

  CVE-2022-21827 wirkt sich auf das NetScaler Gateway-Plug-In für Windows aus, die vor 21.9.1.2 unterstützt wurden.

  Die Erkennung und Behebung von Sicherheitslücken, die sich auf das NetScaler Gateway-Plug-In für Windows auswirken, wird von NetScaler ADM nicht unterstützt. Außerdem können Sicherheitsanfälligkeiten des NetScaler Gateway-Plug-ins nicht bewertet werden, indem Prüfungen auf der ADC-Seite durchgeführt, die ADC-Version überprüft oder die ADC-Konfiguration überprüft wird. Die Erkennung und Standardisierung für diesen CVE kann nur anhand der auf dem Client bereitgestellten Version des NetScaler Gateway-Plug-ins für Windows bewertet werden.

  Daher liegt die Erkennung und Behebung dieser Sicherheitsanfälligkeit außerhalb des Bereichs der NetScaler ADM Security Advisory.

Upgrade-Empfehlung (Preview)

February 5, 2024

Als Netzwerkadministrator können Sie viele ADC-Instanzen verwalten, die auf verschiedenen ADC-Builds in NetScaler ADM ausgeführt werden. Die Überwachung des Lebenszyklus jeder ADC-Instanz kann eine umständliche Aufgabe sein. Sie müssen die NetScaler-Produktmatrix aufrufenund die ADC-Instances identifizieren, die das Ende des Lebenszyklus (EOL) oder das Ende der Wartung (EOM) erreichen oder erreicht haben. Planen Sie dann ihr Upgrade.

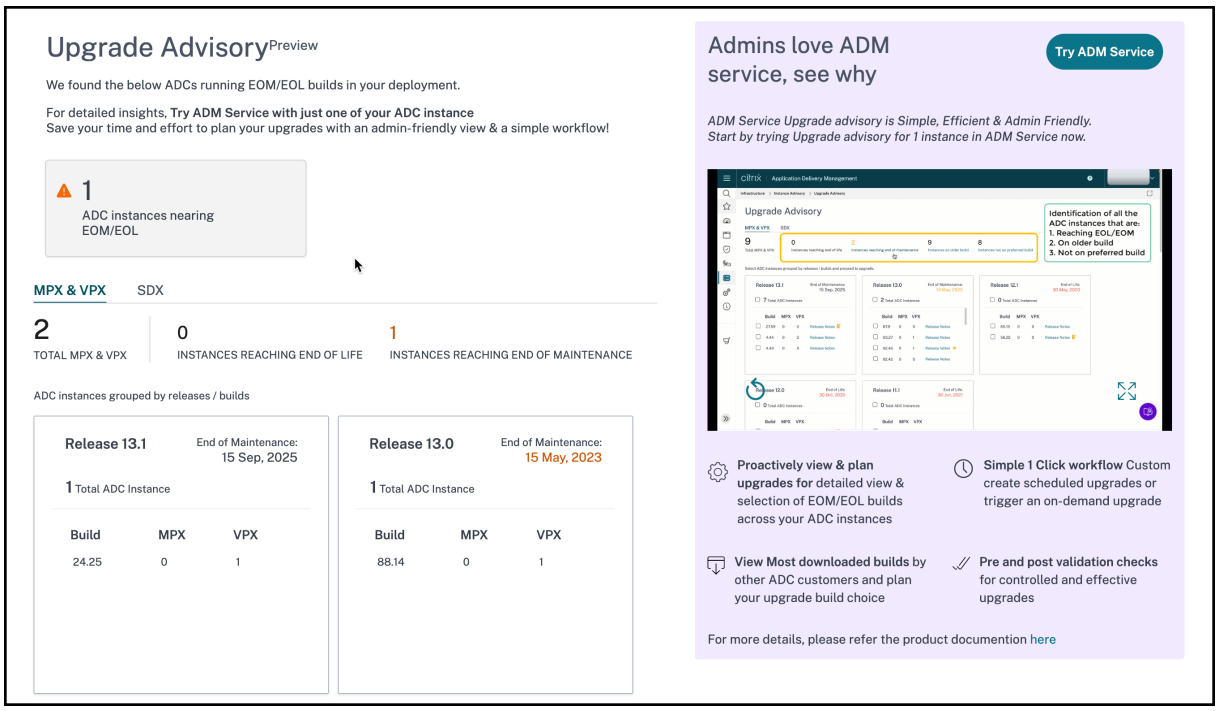
NetScaler ADM on-premises Upgrade Advisory führt einen Versionsscan auf den ADCs durch und bietet eine Ansicht der EOM/EOL-Builds in Ihren ADC-Instanzen.

> **WICHTIG**
>
> Für detaillierte Einblicke und den Arbeitsablauf zum Upgrade der ADC-Instanzen probieren Sie **NetScaler ADM Service**.

Upgrade-Advisory anzeigen

Navigieren Sie zu **Infrastructure > Instance Advisory > Upgrade Advisory** und sehen Sie sich die folgenden Informationen an:

- Gesamtzahl der ADC-Instanzen.
- Instanzen, die das Lebensende erreichen.
- Instanzen, die das Ende der Wartung erreichen.



Auf der Seite **Upgrade Advisory** werden die ADC-Instanzen nach ihren Releases gruppiert.

Mit der On-Premises-Upgrade-Empfehlung von NetScaler ADM können Sie auch eine der ADC-Instanzen auswählen und die ADC-Instanz in den ADM Service integrieren. Klicken Sie auf **ADM Service testen** und binden Sie die ADC-Instanz in den ADM Service ein. ADM Service Upgrade Advisory bietet Ihnen den Workflow für das Upgrade per ausgewählter ADC-Instanz.

Weitere Informationen zur ADM Service Upgrade Advisory finden Sie in der GIF-Animation auf der Seite mit den **Upgrade-Empfehlungen**.

Orchestrierung

February 5, 2024

Beim Software Defined Networking (SDN) verwaltet ein Softwareanwendungscontroller ein Netzwerk und seine Aktivitäten, anstatt Hardware, die das Netzwerk unterstützt. Das heißt, SDN ermöglicht es den Netzwerkadministratoren, eine physische Netzwerkkonnektivität in eine logische Netzwerkkonnektivität zu virtualisieren und Netzwerkdienste mithilfe eines softwarebasierten zentralen Managementtools zu verwalten. SDN ermöglicht es Netzwerktechnikern und Administratoren, auf sich schnell ändernde Geschäftsanforderungen zu reagieren.

Die bekannteren Vorteile von SDN sind zwar die Programmierbarkeit des Datenverkehrs, die größere Flexibilität, die Möglichkeit, eine richtliniengesteuerte Netzwerküberwachung einzurichten und die

Implementierung von Netzwerkautomatisierung, einige der spezifischen Vorteile von SDN sind jedoch im Folgenden aufgeführt:

- Zentralisierte Netzwerkbereitstellung
- Erhöhte Netzwerksicherheit auf granularer Ebene
- Geringere Betriebskosten
- Höheres Maß an Cloud-Abstraktion
- Garantierte Bereitstellung von Inhalten
- Geringere Netzwerkausfallzeiten

NetScaler Application Delivery Management (ADM) unterstützt SDN in Unternehmensnetzwerken, indem es SDN-Controller verschiedener Anbieter integriert. NetScaler ADM unterstützt sowohl VMware NSX Manager als auch Cisco Application Policy Infrastructure Controller (APIC).

VMware NSX Manager

NetScaler ADM lässt sich in die VMware-Netzwerkvirtualisierungsplattform integrieren, um die Bereitstellung, Konfiguration und Verwaltung von NetScaler-Diensten zu automatisieren. Diese Integration reduziert die traditionelle Komplexität, die mit der physischen Netzwerktopologie verbunden ist, und ermöglicht es vSphere/vCenter-Administratoren, NetScaler-Dienste schneller programmgesteuert bereitzustellen.

VMware NSX Manager macht logische Firewalls, Switches, Router, Ports und andere Netzwerkelemente verfügbar, um virtuelle Netzwerke zwischen verschiedenen Hypervisoren, Cloud-Managementsystemen und zugehöriger Netzwerkhardware zu ermöglichen. Es unterstützt auch externe Netzwerke und Sicherheitsdienste.

Die Cloud Orchestration-Funktion von NetScaler ADM ermöglicht die Integration von NetScaler-Produkten in VMware NSX und bietet die folgenden Funktionen:

- Möglichkeit, einem bestimmten Edge-Gateway im Rahmen der Serviceeinfügung ein vorab bereitgestelltes VPX auf Abruf zuzuweisen.
- Möglichkeit, erweiterte Funktionen von NetScaler wie SSL und CS sowie grundlegenden Lastenausgleich über Anwendungsvorlagen auf Instanzen zu konfigurieren, die in der NSX-Umgebung ausgeführt werden.
- Möglichkeit, im Rahmen der Dienstlöschung die Zuweisung eines VPX von einem bestimmten Edge-Gateway zu trennen und dasselbe VPX einem anderen Edge-Gateway neu zuzuweisen.
- Möglichkeit zur schnellen Bereitstellung von NetScaler Funktionen über die vCenter Konsole im Rahmen des Bereitstellungsworkflows der gesamten Infrastruktur, die für eine Anwendung erforderlich ist.

Vorteile:

- Automatisierte, bedarfsgerechte Zuweisung neuer ADC-Dienste als Teil eines Workflows zur Anwendungsbereitstellung
- Vereinfachte Konfiguration anwendungsspezifischer, erweiterter ADC-Funktionalität durch Anwendungsvorlagen
- Mehrmandantenübergreifende Aufgabentrennung und Self-Service-Nutzungsmodell bei gleichzeitiger Bereitstellung eines zentralen Kontrollpunkts für Cloud-Administratoren
- Einfachere Integration mit NetScaler ADM -APIs, die unerwartete zukünftige Verwendungen unterstützen.

Weitere Informationen zum Konfigurieren von VMware NSX Manager auf NetScaler ADM finden Sie unter Integrieren von NetScaler Appliances mit VMware NSX Manager.

Cisco ACI Hybrid-Modus

Cisco ACI hat die Unterstützung für den Hybrid-Modus in Version 1.3 (2f) eingeführt. Im Hybridmodus können Sie die Netzwerkautomatisierung über den Application Policy Infrastructure Controller (APIC) durchführen und gleichzeitig die L4-L7-Konfiguration an NetScaler ADM delegieren, das als Gerätemanager im APIC fungiert.

Die NetScaler Hybridmodus-Lösung wird von einem Hybridmodusgerätepaket und NetScaler ADM unterstützt. Sie müssen das Paket des Hybrid-Modus-Gerätes im APIC hochladen. Weitere Informationen finden Sie unterNetScaler Automation Verwenden von NetScaler ADM im Hybridmodus von Cisco ACI.

OpenStack: Integrieren von NetScaler Instanzen

February 5, 2024

Die Cloud Orchestration-Funktion von NetScaler Application Delivery Management (ADM) ermöglicht die Integration von NetScaler-Produkten in die OpenStack-Plattform. Durch die Verwendung dieser Funktion mit OpenStack-Plattform können OpenStack-Benutzer die Lastenausgleichsfunktion (LBaaS) des NetScaler nutzen. Danach können die OpenStack-Benutzer ihre Load Balancer-Konfigurationen von OpenStack aus in der NetScaler-Instanz bereitstellen.

Die folgenden Abschnitte enthalten eine kurze Beschreibung der Funktionen des NetScaler ADM- und OpenStack-Integrationsworkflows.

NetScaler -Treiber für OpenStack Neutron LBaaS

Das OpenStack Neutron LBaaS-Plug-In enthält einen NetScaler-Treiber, der OpenStack die Kommunikation mit dem NetScaler ADM ermöglicht. OpenStack verwendet diesen Treiber, um alle Lastausgleichskonfigurationen, die über LBaaS-APIs durchgeführt werden, an das NetScaler ADM weiterzuleiten, das die Load Balancer-Konfiguration für die gewünschten NetScaler Instanzen erstellt. OpenStack verwendet den Treiber auch, um NetScaler ADM in regelmäßigen Abständen aufzurufen, um den Status verschiedener Entitäten (wie VIPs und Pools) aller Load-Balancing-Konfigurationen von den NetScalern abzurufen. Die NetScaler-Treibersoftware für die OpenStack-Plattform ist zusammen mit dem NetScaler ADM enthalten. Um die Treiber herunterzuladen und zu installieren, müssen Sie zuerst NetScaler ADM installieren und die Anwendung starten.

NetScaler ADM und OpenStack miteinander registrieren

Sie müssen zuerst OpenStack-Informationen auf dem NetScaler ADM registrieren. Geben Sie die IP-Adresse des OpenStack-Controllers und die Administratoranmeldeinformationen für die Cloud sowie die Benutzeranmeldeinformationen des OpenStack NetScaler-Treibers an. Später können Sie dieselben Anmeldeinformationen im Abschnitt NetScaler_Driver der Neutron-Konfigurationsdatei (neutron.conf) angeben, sodass der NetScaler-Treiber in OpenStack während LB-Konfigurationen eine Verbindung zu NetScaler ADM herstellen kann.

Nachdem OpenStack und NetScaler ADM miteinander registriert sind, können beide miteinander kommunizieren. Außerdem können OpenStack-Benutzer ihre vorhandenen Anmeldeinformationen in OpenStack verwenden, um sich an der NetScaler ADM-Benutzeroberfläche anzumelden und zu überprüfen, wie ihre LB-Konfigurationen in NetScalers funktionieren.

Mandanten in OpenStack

In OpenStack wird ein Tenant auch als Projekt bezeichnet. Ein Mandant ist eine Gruppe von Benutzern. Ein Mandant oder ein Projekt kann auch als eine Gruppe von Ressourcen (Rechenleistung, Netzwerk, Speicher usw.) definiert werden, die einer isolierten Benutzergruppe zugewiesen sind.

Richtlinien für die Platzierung

Platzierungsrichtlinien bieten die Flexibilität bei der Entscheidung über die NetScaler Instanz, die in jeder von Benutzern erstellten Load Balancer-Konfiguration verwendet wird. Alternativ bietet das NetScaler ADM auch die Option, eine NetScaler-Instanz auf der Grundlage von OpenStack-Mandanten zuzuweisen.

Servicepakete

Servicepakete sind Pakete, die Richtlinien/SLAS, Konfigurationsspezifikationen für Geräte oder automatische Bereitstellung sowie Richtlinien für Mandanten und Platzierungen miteinander verbinden. Ein Servicepaket wird normalerweise anhand der Isolationsrichtlinien definiert, die dem Mandanten zur Verfügung gestellt werden.

Im Folgenden sind einige Punkte im Zusammenhang mit Servicepaketen aufgeführt:

- Ein Mandant kann nicht an mehr als einem Servicepaket teilnehmen.
- Dem gleichen Servicepaket können mehrere Mandanten zugeordnet werden.
- In einem Servicepaket, das für die automatische Bereitstellung festgelegt ist, können virtuelle NetScaler Instanzen nur von einem Plattformtyp (auf der SDX-Plattform oder auf der OpenStack Compute-Plattform) erstellt werden.

Von LBaaS V1 und LBaaS V2 unterstützte Funktionen

Während der LBaaS V1-Treiber in OpenStack Vorgänge über die Benutzeroberfläche von OpenStack Horizon unterstützt, unterstützt der LBaaS V2-Treiber nur Befehlszeilenoperationen.

Die folgende Liste zeigt die Funktionen, die sowohl auf LBaaS V1 als auch auf LBaaS V2 auf OpenStack unterstützt werden:

- LBaaS V1
  - Lastausgleich
- LBaaS V2
  - Lastausgleich
  - SSL Offload mit Zertifikaten, die von **Barbican**, dem Schlüsselmanager in OpenStack, verwaltet werden
  - Zertifikatspakete (einschließlich zwischengeschalteter Zertifizierungsstellen)
  - SNI-Unterstützung

Dieses Dokument enthält Informationen über:

- Anwendungsfallszenario
- NetScaler ADM Integration mit OpenStack-Workflow
- Prerequisites
- Vorkonfigurationsaufgaben in NetScaler ADM und OpenStack

- Konfigurationsschritte für LBaaS V1 mit Horizon
- Konfigurationsschritte für LBaaS V2 über die Befehlszeile
- Manuelle Provisioning der NetScaler VPX-Instanz auf OpenStack
- Integration von NetScaler ADM mit OpenStack Heat Services
- Überwachen von OpenStack-Anwendungen in NetScaler ADM

Anwendungsfallszenario

Das folgende Anwendungsszenario erklärt den Workflow der Integration von NetScaler ADM in die OpenStack-Plattform:

Ein Unternehmen, Example-Cloud-Provider, hat OpenStack-Komponenten verwendet, um eine Cloud einzurichten, um seinen Mandanten eine Infrastruktur bereitzustellen. Steve ist der Administrator dieses Cloud-Anbieters, während Tom ein Mandant der Cloud-Infrastruktur des Example-Cloud-Providers ist. Die Organisation von Tom, Example-Sportsonline.com, erfordert zwei Server S1 und S1, und Tom benötigt auch ein dediziertes NetScaler Gerät, um den Datenverkehr zwischen Servern S1 und S2 auf OpenStack-Plattform auszugleichen.

Um diese Anforderung zu erfüllen, muss Steve sowohl OpenStack als auch NetScaler ADM installieren und konfigurieren und sie auf miteinander kompatible Geräte vorbereiten. Steve muss in OpenStack ein Mandantenkonto mit dem Namen Example-Sportonline erstellen und dann dem Mandantenkonto Ressourcen zuweisen. Steve muss auch verschiedene Anmeldeinformationen (Benutzer) für Example-SportsOnline erstellen, um die Ressourcen und Konfiguration zu verwalten. Tom kann jetzt die beiden Server S1 und S2 auf OpenStack erstellen, um den Datenverkehr in seiner Organisation zu verwalten.

Steve muss OpenStack-Details bei NetScaler ADM registrieren und den NetScaler LBaaS-Treiber in der OpenStack-Netzwerkkomponente Neutron konfigurieren. Nach Abschluss der Registrierung zeigt NetScaler ADM die Details aller Mandanten aus dem OpenStack an. Steve kann Example-SportsOnline aus der Liste auswählen, wer die NetScaler LBaaS-Funktionen nutzen möchte, und Tom so konfigurieren, dass er einen dedizierten NetScaler für seine Load Balancer-Konfigurationen in NetScaler ADM erhält.

Zu diesem Zweck kann Steve entweder mithilfe der NetScaler ADM-Benutzeroberfläche eine NetScaler VPX-Instanz auf der Rechenebene (Nova) von OpenStack bereitstellen oder MAS aktivieren, bei Bedarf automatisch eine NetScaler VPX-Instanz bereitzustellen, wenn Tom seine LB-Konfiguration in OpenStack durchführt. In beiden Fällen verwaltet NetScaler ADM die VPX-Instanz. Um dies zu erreichen, erstellt Steve ein Servicepaket in NetScaler ADM und definiert die Bedingungen im Servicepaket, die im SLA mit Tom vereinbart wurden. Steve wählt beispielsweise die „dedizierte “Isolationsrichtlinie aus, um Tom eine dedizierte Instanz für die Bereitstellung von Load Balancer-Konfigurationen zur Verfügung zu stellen. Das heißt, Steve wählt im Servicepaket eine Instanz aus,

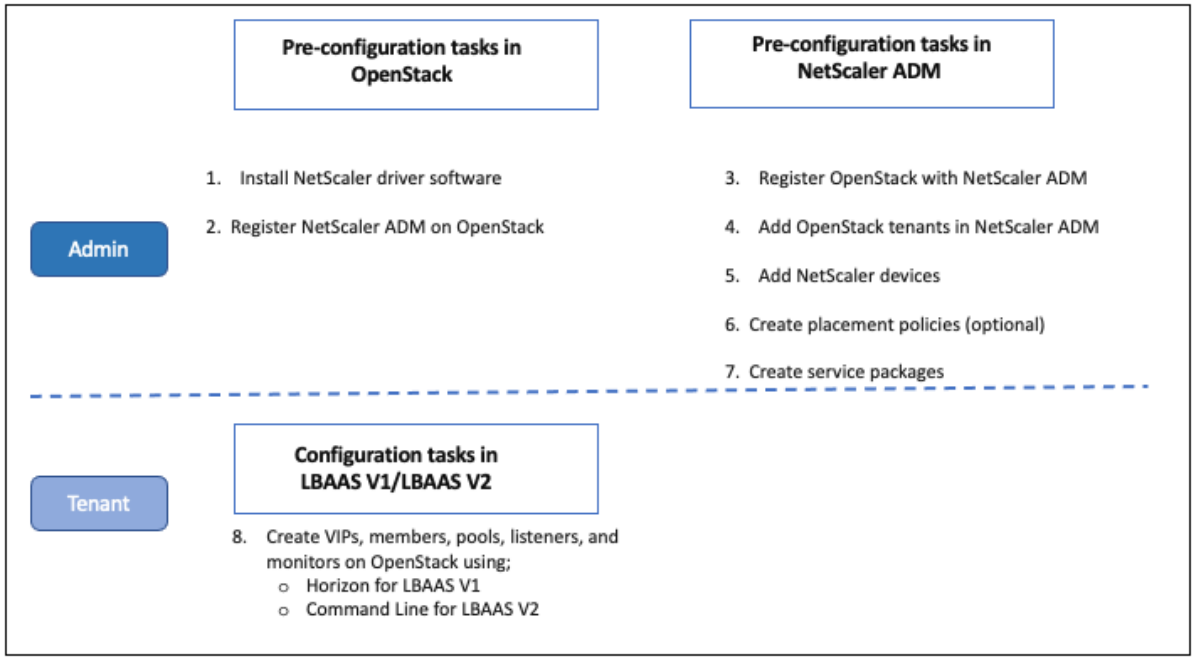
die nicht gemeinsam genutzt wird, für Tom. Anschließend weist er dem Servicepaket viele NetScaler VPX-Instanzen zu und verknüpft Example-SportsOnline zusammen mit anderen Mandanten, die einen dedizierten NetScaler für das Servicepaket benötigen. Wenn Tom seine erste Load Balancer-Konfiguration durchführt, weist NetScaler ADM daher Example-SportsOnline eine der NetScaler VPX-Instanzen im Servicepaket zu und stellt seine Konfiguration auch in diesem NetScaler bereit.

Tom kann jetzt Lastausgleichskonfigurationen erstellen, indem Pools, virtuelle IPs (VIP) und Integritätsmonitore mit OpenStack LBaaS/UI erstellt werden. Pools und VIPs in OpenStack werden als Servicegruppen und virtuelle Server auf der NetScaler-Instanz bereitgestellt. Tom kann auch Integritätsmonitore zur Überwachung der Server einrichten und Anwendungsdatenverkehr nur an die Server senden, die zu einem beliebigen Zeitpunkt in Betrieb sind und von NetScaler aus erreichbar sind.

Die in OpenStack erstellte Load-Balancing-Konfiguration ist jetzt auf der NetScaler-Instanz implementiert. Sobald die NetScaler VPX Instanz vollständig konfiguriert ist, übernimmt die Lastenausgleichsfunktion und nimmt Anwendungsdatenverkehr an und gleicht den Datenverkehr zwischen den Servern S1 und S2 aus, die von Tom erstellt wurden.

NetScaler ADM Integration mit OpenStack-Workflow

Das folgende Flussdiagramm zeigt den Workflow, dem Sie folgen müssen, wenn Sie LBaaS V1 und LBaaS V2 konfigurieren.



NSX Manager: Manuelle Provisioning von NetScaler Instanzen

February 5, 2024

NetScaler Application Delivery Management (ADM) lässt sich in die VMware-Netzwerkvirtualisierungsplattform integrieren, um die Bereitstellung, Konfiguration und Verwaltung von NetScaler-Diensten zu automatisieren. Diese Integration abstrahiert die traditionellen Komplexitäten, die mit der physischen Netzwerktopologie verbunden sind, und ermöglicht es vSphere/vCenter-Administratoren, NetScaler Dienste programmgesteuert schneller bereitzustellen.

Dieser Artikel enthält eine Liste von Aufgaben, die Sie sowohl auf VMware NSX Manager als auch auf NetScaler ADM ausführen müssen.

> **Hinweis: Stellen Sie**
>
> sicher, dass VMware NSX für vSphere 6.2 und höher installiert und konfiguriert ist und dass die Edge-Gateways, DLR und virtuellen Maschinen, für die ein Lastenausgleich erforderlich ist, bereits erstellt wurden.

Voraussetzungen

- Installieren Sie VMware ESXi Version 4.1 oder höher mit Hardware, die die Mindestanforderungen erfüllt.
- Installieren Sie VMware Client auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
- Installieren Sie VMware OVF Tool (erforderlich für VMware ESXi Version 4.1) auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
- Installieren Sie NetScaler ADM auf einem der unterstützten Hypervisoren.

  Aufgaben zum Installieren von NetScaler ADM Build 13.1 auf einem der unterstützten Hypervisoren finden Sie unter Bereitstellen von NetScaler ADM.

VMware ESXi Hardwareanforderungen

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die Sie auf Ihrem VMware ESXi-Server benötigen, um eine virtuelle NetScaler ADM-Appliance zu installieren.

Komponente	Voraussetzung

RAM	8 GB
Virtuelle CPU	8
Speicherplatz	500 GB
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s

> **Hinweis:**
>
> Die oben angegebenen Speicher- und Festplattenanforderungen gelten für die Bereitstellung von NetScaler ADM auf einem VMware ESXi-Server, da auf dem Host keine anderen virtuellen Maschinen ausgeführt werden. Die Hardwareanforderungen für den VMware ESXi-Server hängen von der Anzahl der darauf ausgeführten virtuellen Maschinen ab.

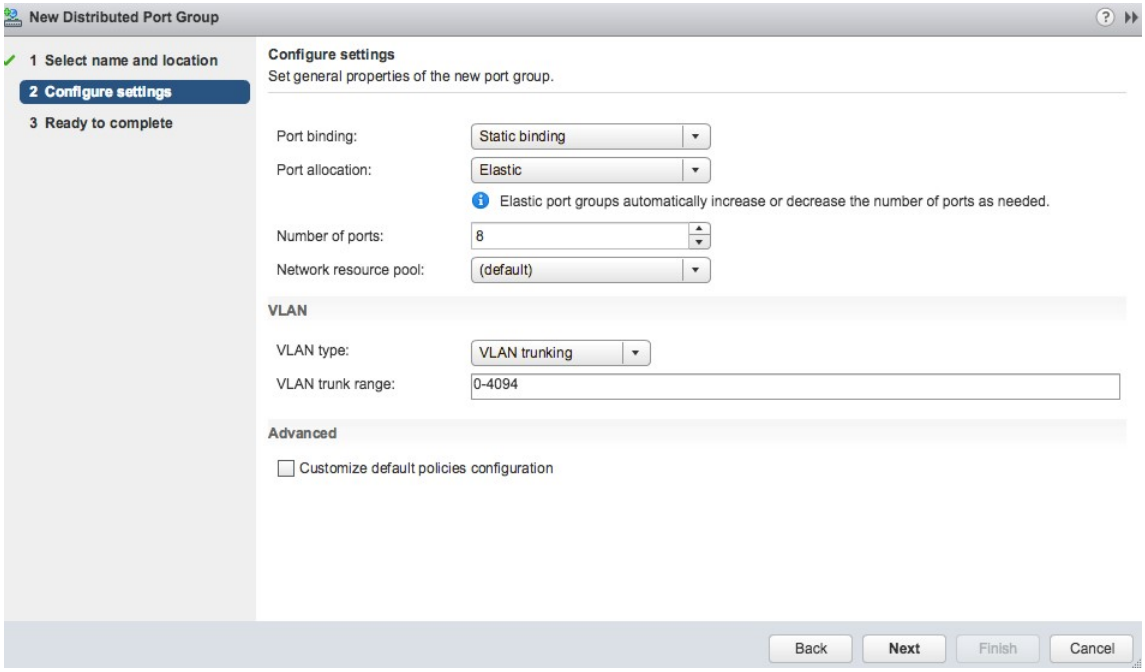
Konfiguration von VMware NSX

- Erstellen Sie einen Pool von NetScaler VPX-Instanzen mit unterschiedlichen Kapazitäten, die den verschiedenen Servicepaketen hinzugefügt werden.

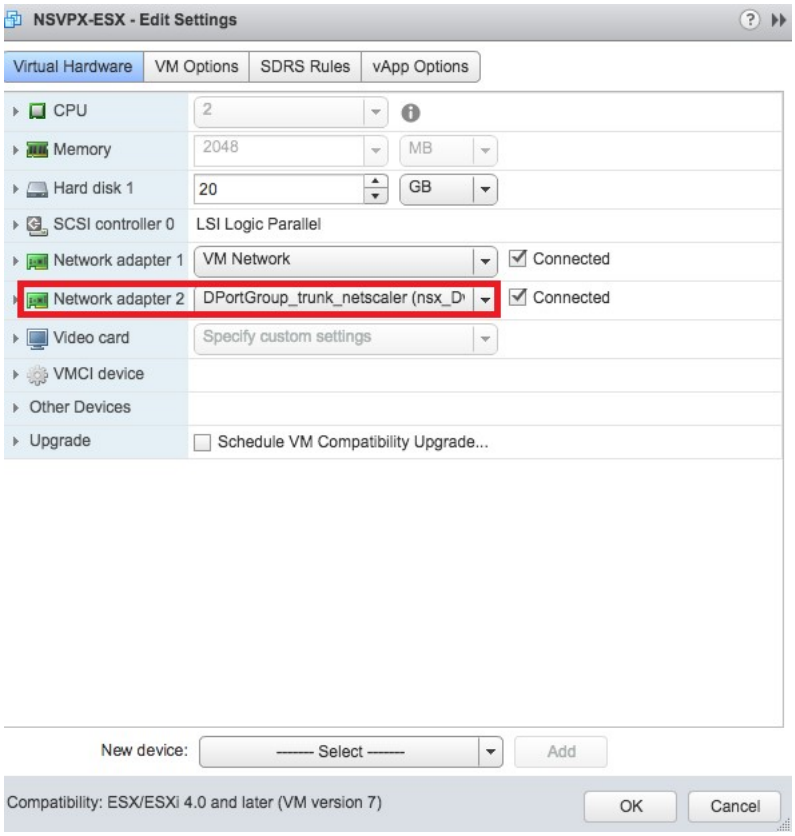
Beispiel:

- Erstellen Sie fünf NetScaler VPX-Instanzen von VPX1000 (1 Gbit/s). Diese Instanzen werden dem Gold-Servicepaket hinzugefügt.
- Erstellen Sie fünf NetScaler VPX-Instanzen von VPX10 (10 Mbit/s). Diese Instanzen werden dem Bronze-Servicepaket hinzugefügt.

1. Navigieren Sie im vSphere-Client zu **Netzwerk**, und erstellen Sie eine Portgruppe vom Typ VLAN-Trunking mit Bereich, z. B. 101-105 (Sie können sogar den vollständigen Bereich angeben, aber nur für die erforderlichen VLANs eine Portgruppe vom Typ VLAN erstellen).

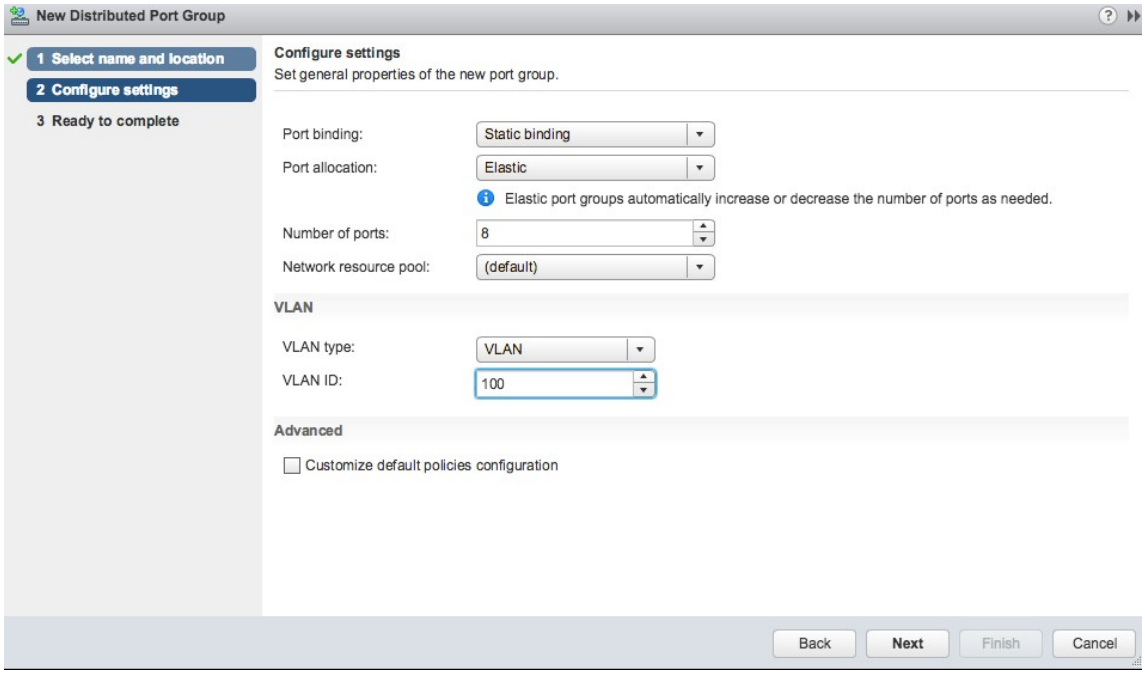


2. Erstellen Sie eine neue Schnittstelle für jede NetScaler VPX Instanz, und fügen Sie sie der oben erstellten Trunk-Portgruppe des VLAN-Bereichs an.



3. Navigieren Sie im vSphere-Client zu **Netzwerk**, und erstellen Sie eine Portgruppe vom Typ VLAN.

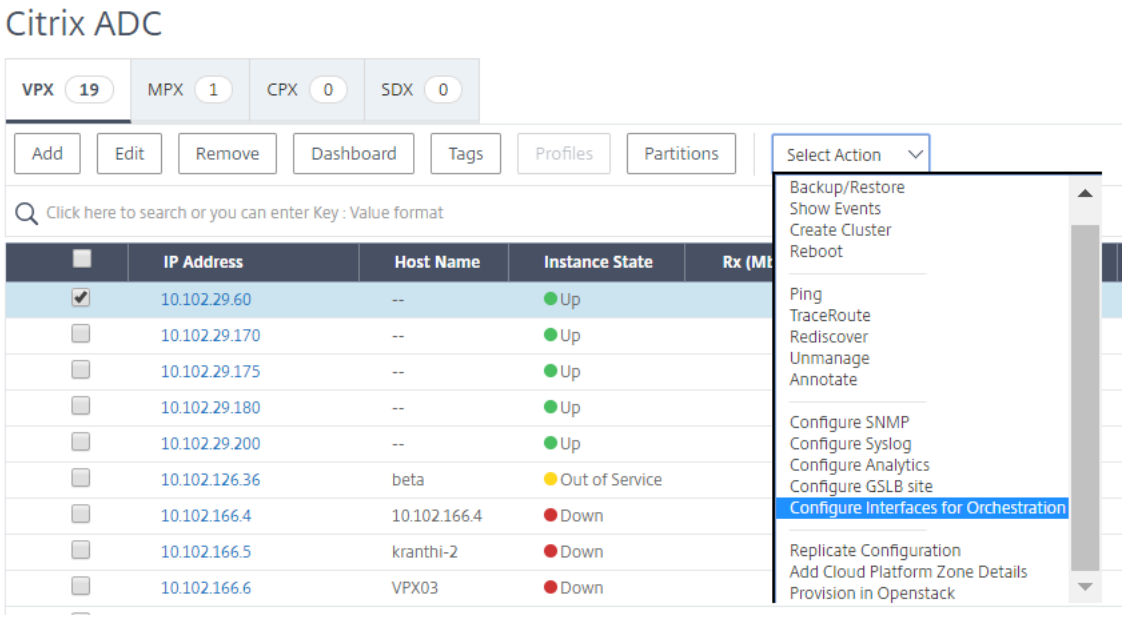
Wenn beispielsweise die anfängliche Trunked Portgruppe mit Bereich 101-105 erstellt wurde, erstellen Sie fünf VLAN-Portgruppen, eine pro VLAN, d. h. eine Portgruppe mit VLAN 101, eine andere mit VLAN102 usw., bis VLAN 105.



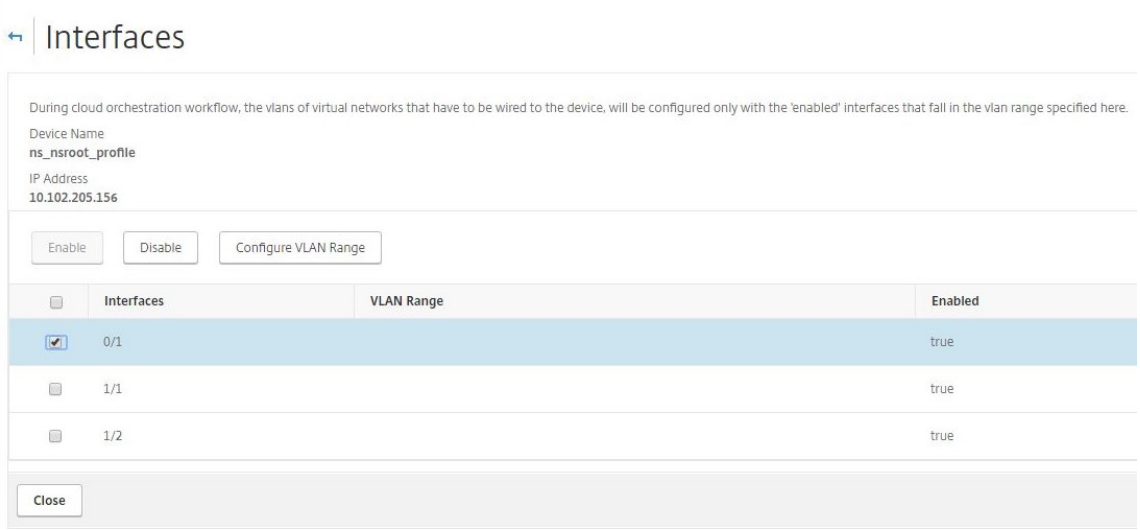
Hinzufügen der NetScaler VPX Instanz in NetScaler ADM

Fügen Sie NetScaler VPX-Instanzen in NetScaler ADM hinzu und geben Sie den VLAN-Bereich der Bündelgruppe für jedes Gerät an.

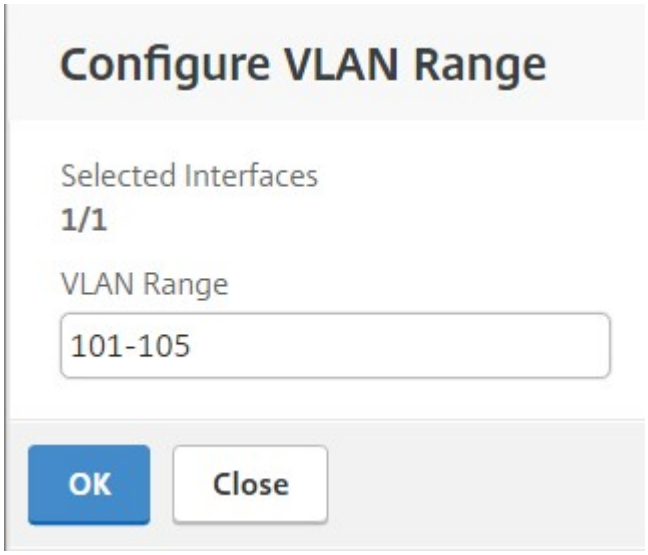
1. **Navigieren Sie in NetScaler ADM zu**Infrastruktur**>**Instances**>**NetScaler VPX**und klicken Sie auf Hinzufügen.**
2. Geben Sie auf der Seite **NetScaler VPX hinzufügen** entweder die Hostnamen der Instanzen, die IP-Adresse jeder Instanz oder einen Bereich von IP-Adressen an, und wählen Sie dann ein Instanzprofil aus der Liste Profilnamen aus**.** Sie können auch ein neues Instanzprofil erstellen, indem Sie auf das Symbol + klicken.
3. Klicken Sie auf **OK**.
4. **Wählen Sie die neu hinzugefügte NetScaler VPX-Instanz aus der Liste auf der**NetScaler VPX-Seite**aus und klicken Sie im Feld Aktion auf den Abwärtspfeil.** Wählen Sie **Interfaces für Orchestration konfigurieren**aus.



5. Wählen Sie auf der Seite **Schnittstellen** die Verwaltungsschnittstelle aus, und klicken Sie auf **Deaktivieren**, um die Bindung von VLAN an die Verwaltungsschnittstelle zu deaktivieren.



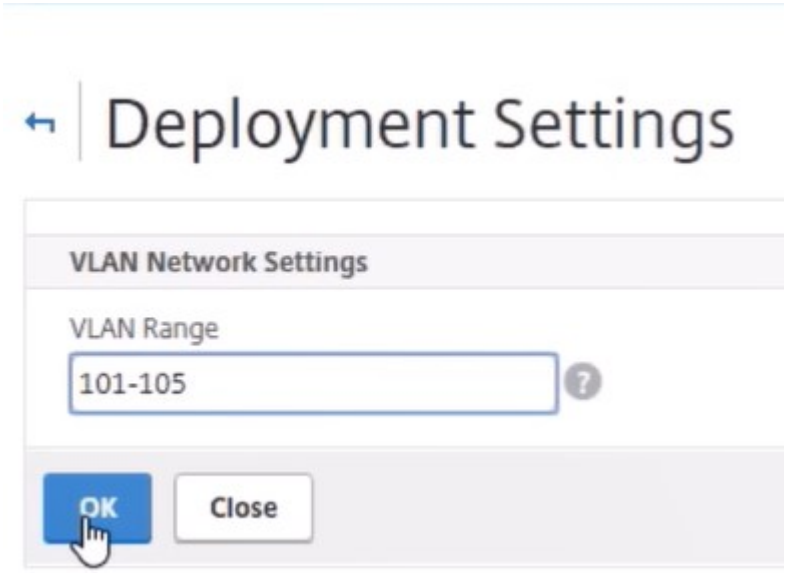
6. Wählen Sie auf der Seite **Schnittstellen** die erforderliche Schnittstelle aus, und klicken Sie auf **VLAN-Bereich konfigurieren**.
7. Geben Sie den in NSX Manager konfigurierten VLAN-Bereich ein, klicken Sie auf **OK**, und klicken Sie dann auf **Schließen**.



Registrieren von VMware NSX Manager bei NetScaler ADM

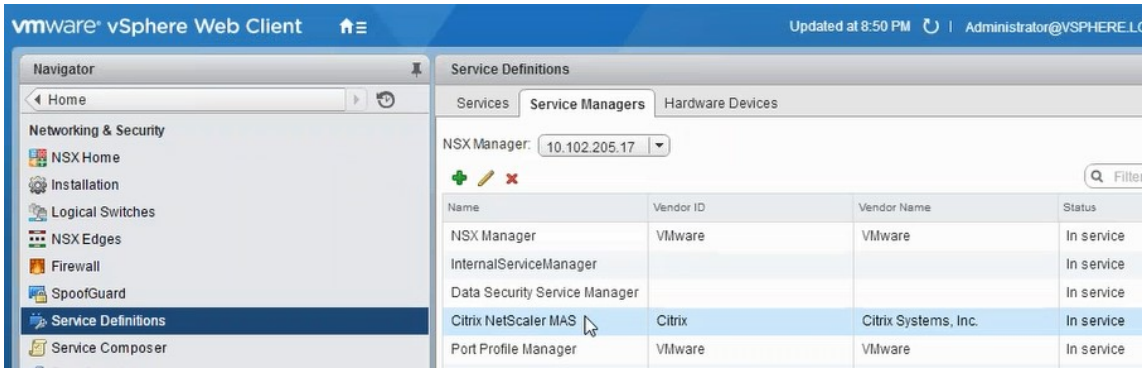
Registrieren Sie VMware NSX Manager bei NetScaler ADM, um einen Kommunikationskanal zwischen ihnen einzurichten.

1. Navigieren Sie in NetScaler ADM in der Dropdownliste zu**Orchestration> SDN Orchestration**>**VMware NSX Manager**und klicken Sie auf**NSX Manager-Einstellungen konfigurieren**.
2. **Legen Sie auf der Seite NSX Manager-Einstellungen konfigurieren** die folgenden Parameter fest:
   a) NSX Manager-IP-Adresse: IP-Adresse von NSX Manager.
   b) NSX Manager-Benutzername —Administratorbenutzername von NSX Manager.
   c) Kennwort - Kennwort des administrativen Benutzers von NSX Manager.
3. Legen Sie im Abschnitt **NetScaler ADM-Konto, das von NSX Manager verwendet wird**, den Benutzernamen und das Kennwort des NetScaler-Treibers für den NSX Manager fest. NetScaler ADM authentifiziert Load Balancer Konfigurationsanforderungen von NSX Manager mithilfe dieser Anmeldeinformationen.
4. Klicken Sie auf **OK**.
5. Navigieren Sie zu **Orchestration** > **System** > **Deployment Settings.** Geben Sie den VLAN-Bereich an, der in Trunked Port Group konfiguriert wurde.



6. Melden Sie sich bei NSX Manager auf vSphere Web Client an, und navigieren Sie zu **Dienstdefinitionen** > **Service Manager**.

   Sie können Citrix NetScaler ADM als einen der Service Manager betrachten. Dies zeigt an, dass die Registrierung erfolgreich ist und ein Kommunikationskanal zwischen NSX Manager und NetScaler ADM eingerichtet wird.



Erstellen eines Servicepakets in NetScaler ADM

1. Navigieren Sie in NetScaler ADM zu**Orchestration >**SDN Orchestration****>**VMware NSX Manager**> **Service Packages**und klicken Sie auf **Hinzufügen, um ein neues Servicepaket hinzuzufügen** .
2. Legen Sie auf der Seite **Service Package** im Abschnitt **Grundeinstellungen** die folgenden Parameter fest:

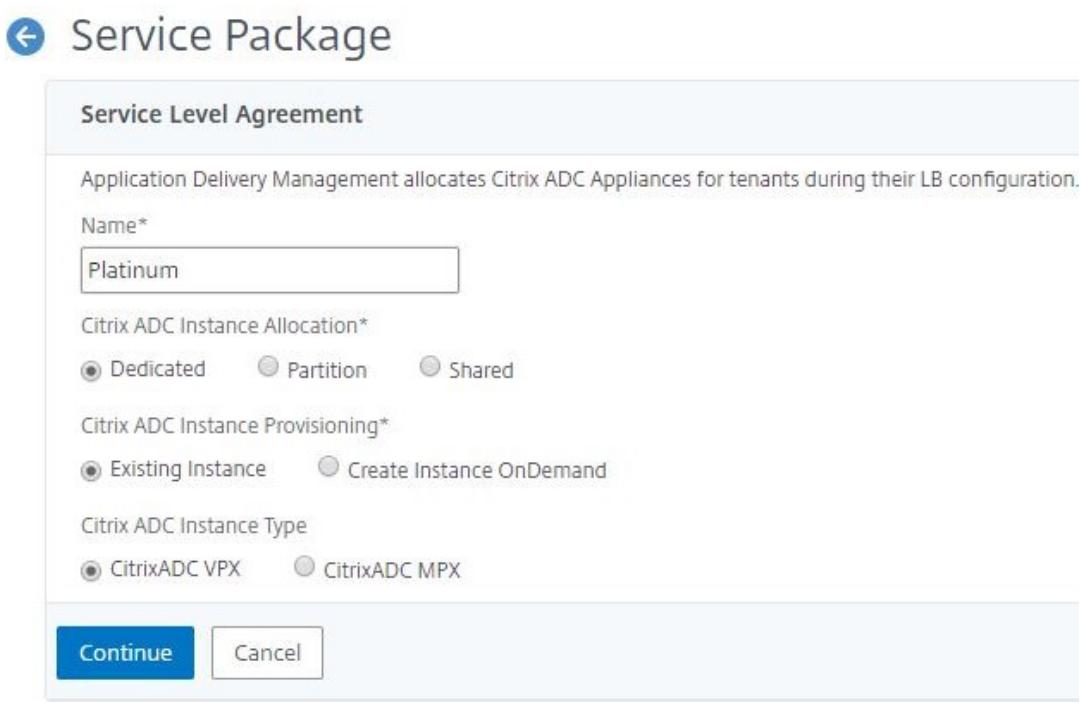
   a) Name —geben Sie den Namen eines Servicepakets ein

   b) Isolationsrichtlinie —standardmäßig ist die Isolationsrichtlinie auf Dedicated gesetzt

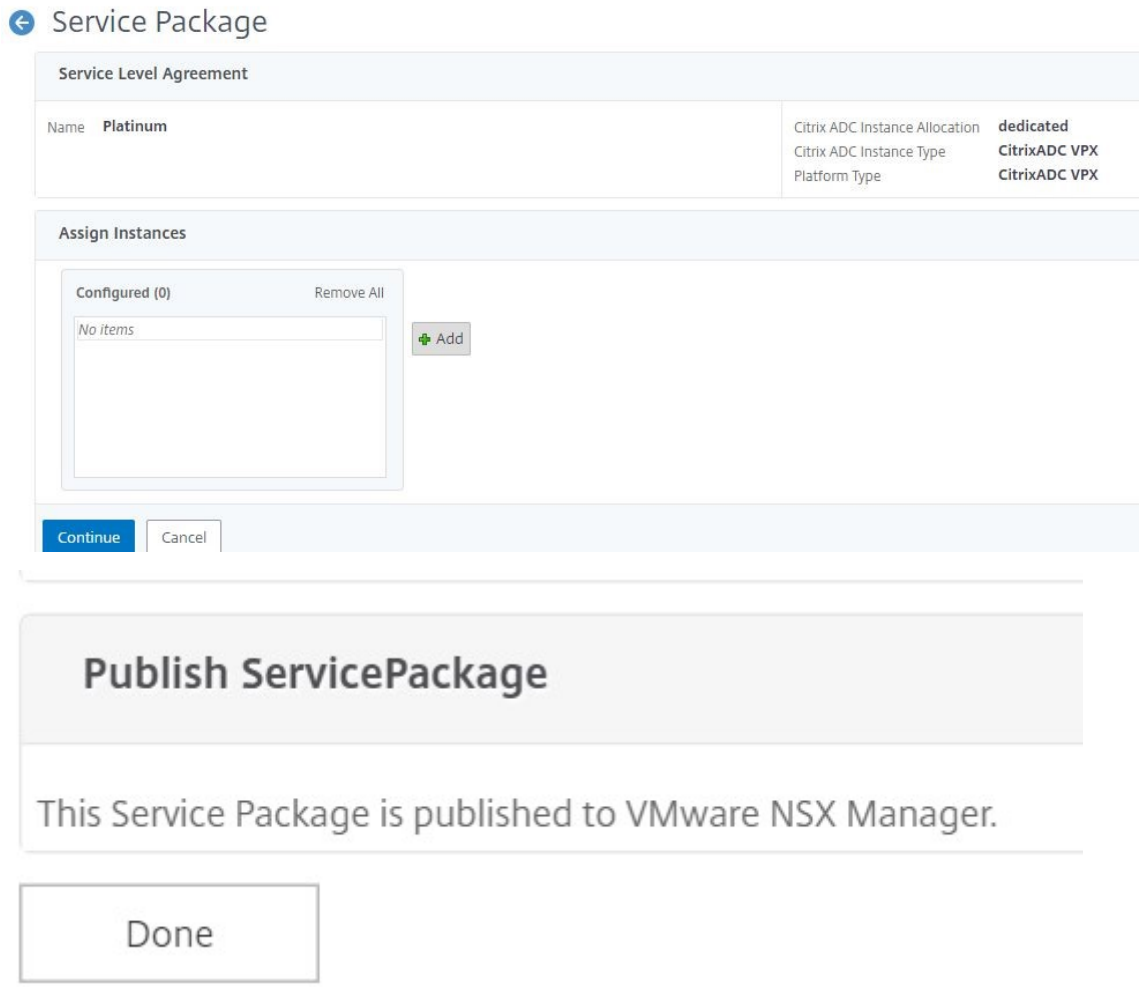
c) Gerätetyp —standardmäßig ist der Gerätetyp auf NetScaler VPX eingestellt

> **Hinweis**
>
> Diese Werte sind in dieser Version standardmäßig festgelegt und können nicht geändert werden.

d) Klicken Sie auf **Weiter**.



3. Wählen **Sie im Abschnitt Geräte zuweisen** das vorab bereitgestellte VPX für dieses Paket aus, und klicken Sie auf **Weiter**.
4. Klicken Sie im Abschnitt **Servicepaket veröffentlichen** auf **Weiter**, um das Servicepaket in VMware NSX zu veröffentlichen, und klicken Sie dann auf **Fertig**.



Mit diesem Verfahren wird ein Servicepaket im NSX Manager konfiguriert. Einem Dienst können mehrere Geräte hinzugefügt werden, und mehrere Edges können dasselbe Servicepaket verwenden, um die NetScaler VPX-Instanz an NetScaler ADM auszulagern.

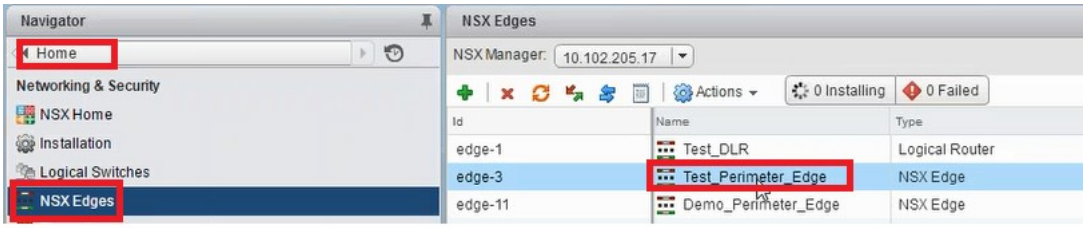
5. **Melden Sie sich beim NSX Manager auf dem vSphere Web Client an und navigieren Sie zu**Service Definitions**> Services.**

   Sie können sehen, dass das NetScaler ADM Dienstpaket registriert ist.

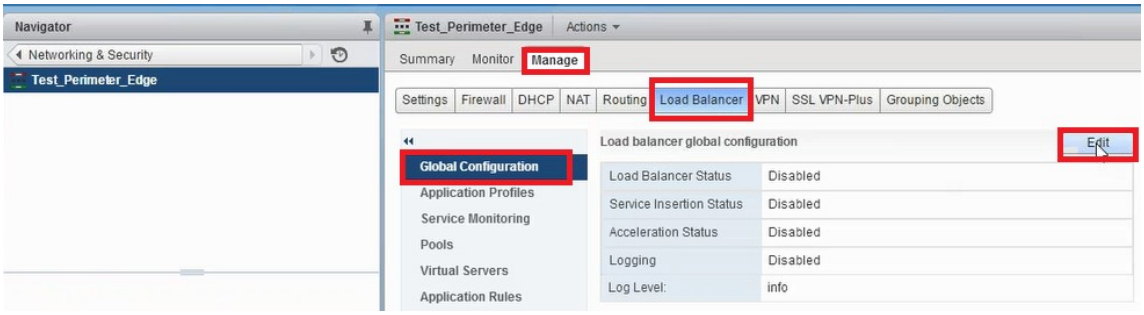
Ausführen des Lastausgleichsdiensteinfügens für Edge

Führen Sie das Einfügen des Load Balancer-Dienstes auf dem zuvor erstellten NSX Edge-Gateway durch (lagern Sie die Lastausgleichsfunktion von NSX LB auf NetScaler aus).

1. Navigieren Sie in NSX Manager zu **Home** > **NSX Edges**, und wählen Sie das Edge-Gateway aus, das Sie konfiguriert haben.

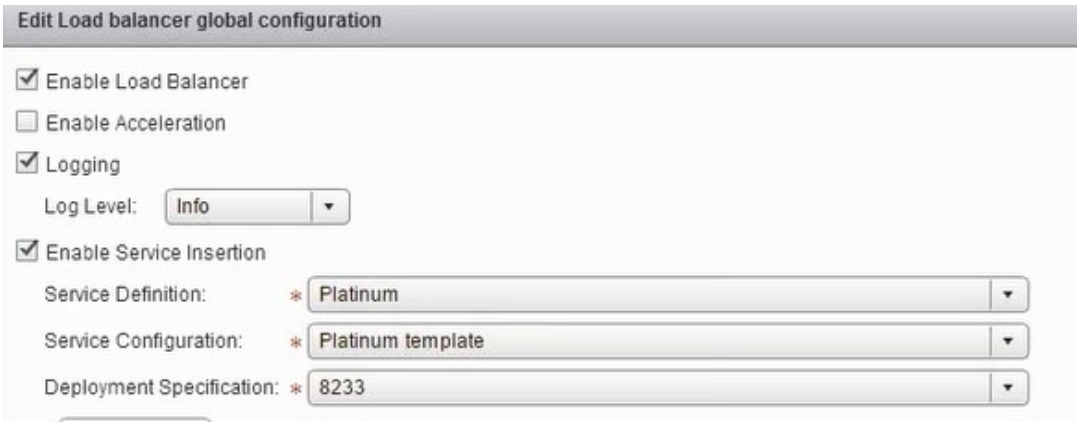


2. Klicken Sie auf **Verwalten**, wählen Sie auf der Registerkarte **Load Balancer** die Option **Globale Konfiguration** aus, und klicken Sie auf **Bearbeiten**.



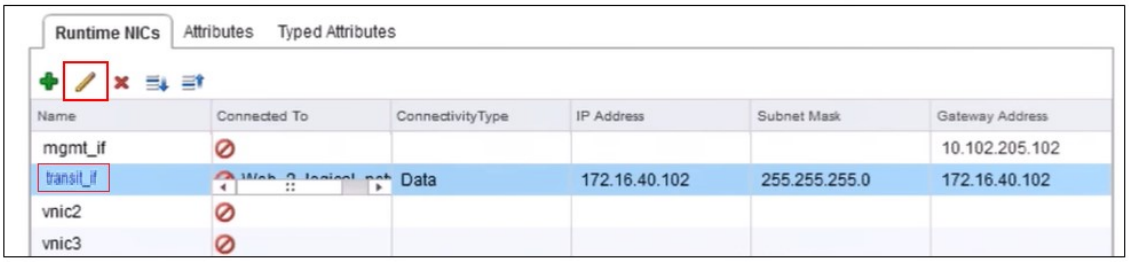
3. Wählen Sie **Load Balancer aktivieren**, **Protokollierung**, **Diensteinfügung aktivieren** aus, um sie zu aktivieren.

   a) Wählen Sie unter **Dienstdefinition** das Dienstpaket aus, das in NetScaler ADM erstellt und in NSX Manager veröffentlicht wurde.

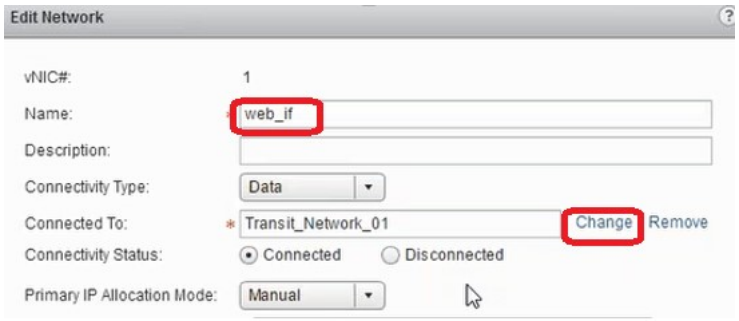


4. Wählen Sie die vorhandenen Laufzeit-NICs aus, und klicken Sie auf das Symbol Bearbeiten, um Laufzeit-NICs zu bearbeiten, die bei der Zuweisung von NetScaler VPX verbunden werden

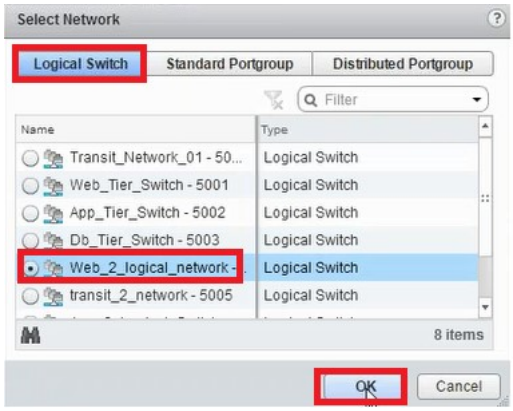
müssen.



5. Bearbeiten Sie den Namen der Netzwerkkarte, geben Sie Konnektivitätstyp als **Daten**an, und klicken Sie auf **Ändern**.

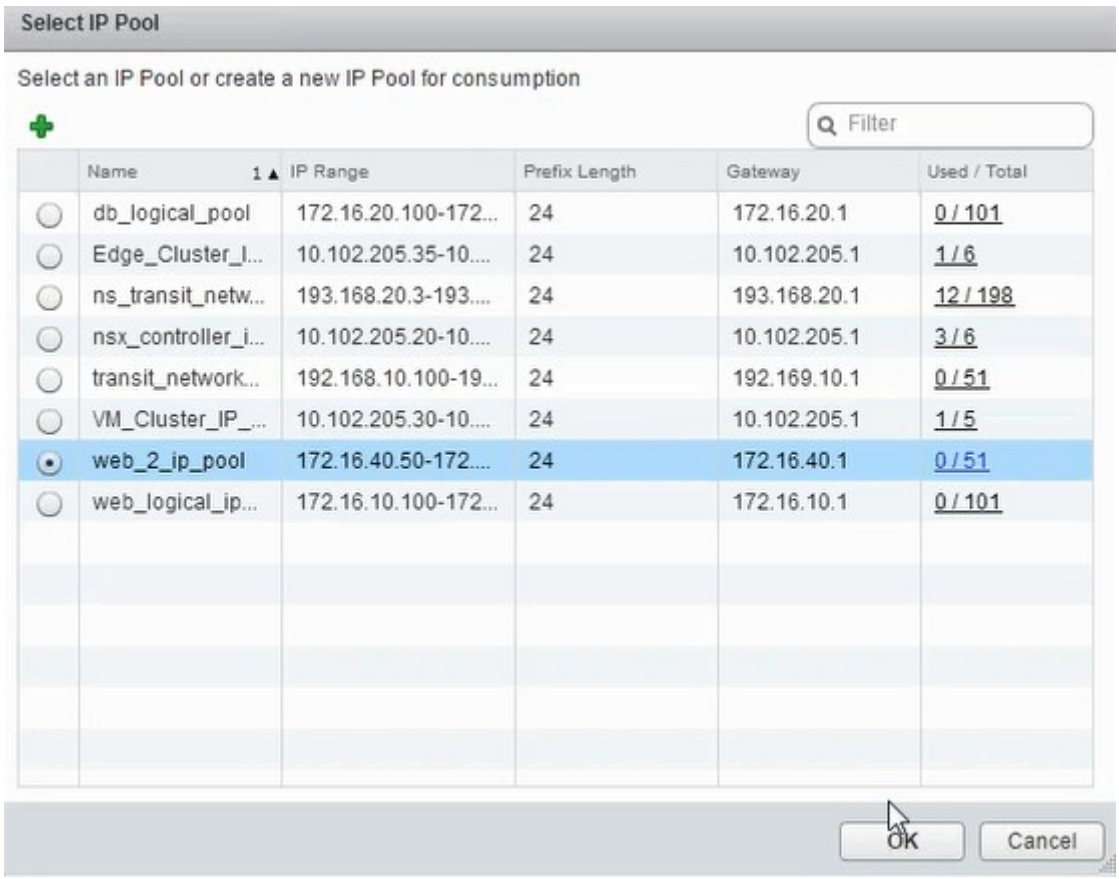


6. Wählen Sie den entsprechenden logischen Web-Switch aus.



7. Wählen Sie im **primären IP-Zuordnungsmodus**die Option IP-Pool aus der Dropdownliste aus, und klicken Sie auf den Pfeil nach unten im Feld IP-Pool.

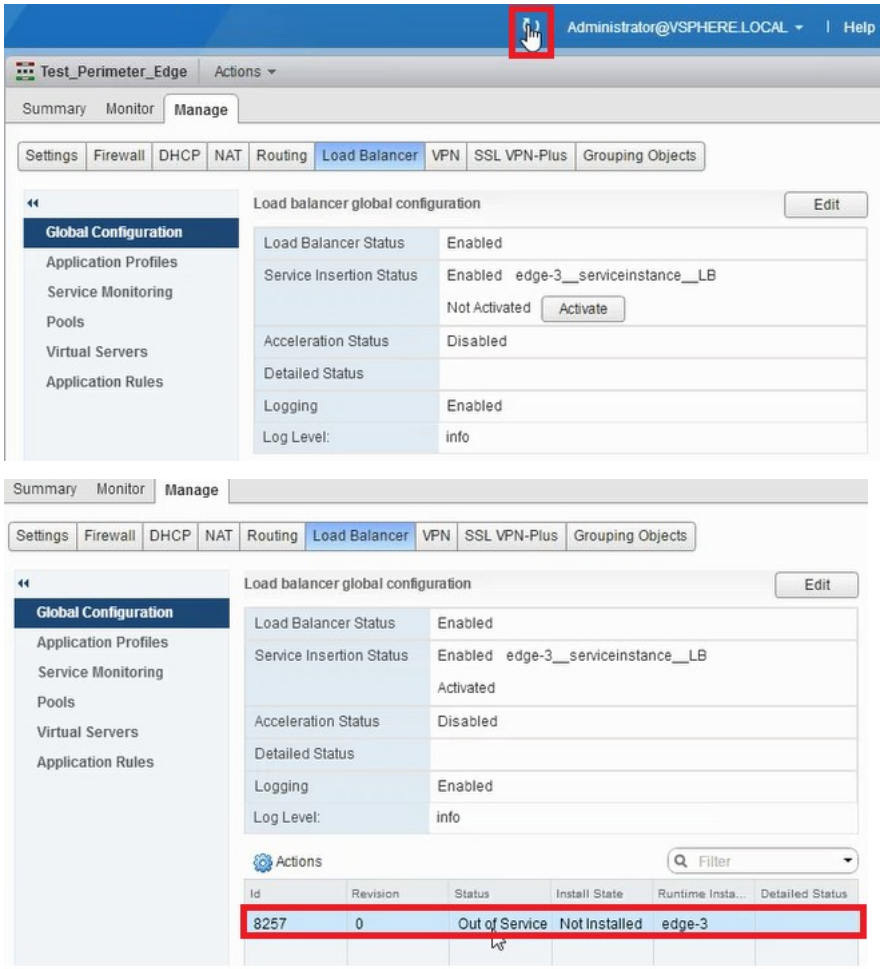
8. **Wählen Sie im Fenster IP-Pool** auswählen den entsprechenden IP-Pool aus, und klicken Sie auf **OK**.



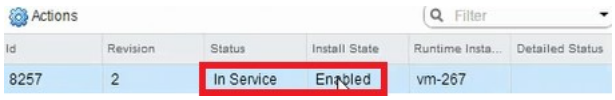
Die IP-Adresse wird erfasst und als Quellnetz-IP-Adresse in der NetScaler VPX Appliance festgelegt. Im NSX Manager wird ein L2-Gateway erstellt, um das VXLAN dem VLAN zuzuordnen.

> **Hinweis**
>
> Alle Datenschnittstellen sind als Laufzeit-NICs verbunden und sind Teil von Schnittstellen für das DLR.

9. Aktualisieren Sie die Ansicht, um die Erstellung der Laufzeit anzuzeigen.



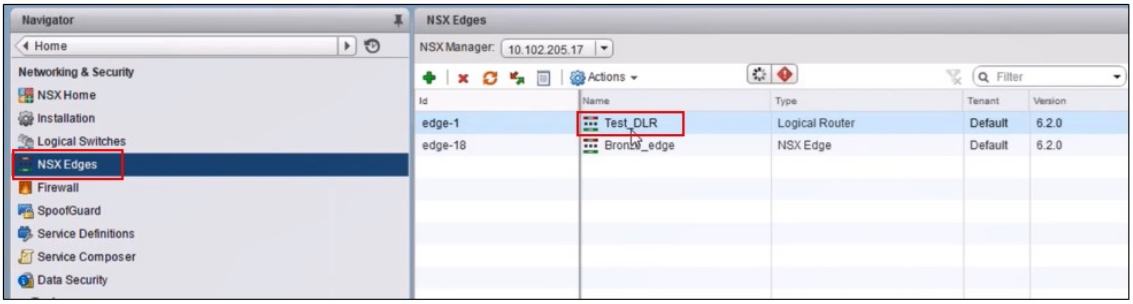
10. Nachdem die VM gestartet wurde, ändert sich der Wert von Status **in In Dienst** und der Wert des Installationsstatus in **Aktiviert**.



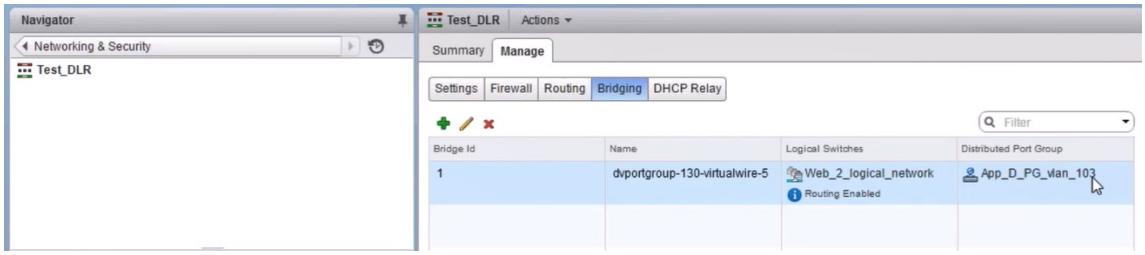
> **Hinweis:**Navigieren Sie
>
> in NetScaler ADM zu **Orchestration** > **Requests**, um Fortschrittsdetails zum Abschluss der LB-Diensteinfügung anzuzeigen.

L2-Gateway auf NSX Manager anzeigen

1. Melden Sie sich beim NSX Manager auf vSphere Web Client an, navigieren Sie zu **NSX Edges**, und wählen Sie das erstellte DLR aus.



2. Navigieren Sie auf der DLR-Seite zu **Verwalten** > **Bridging**. Das L2-Gateway wird in der Liste angezeigt.

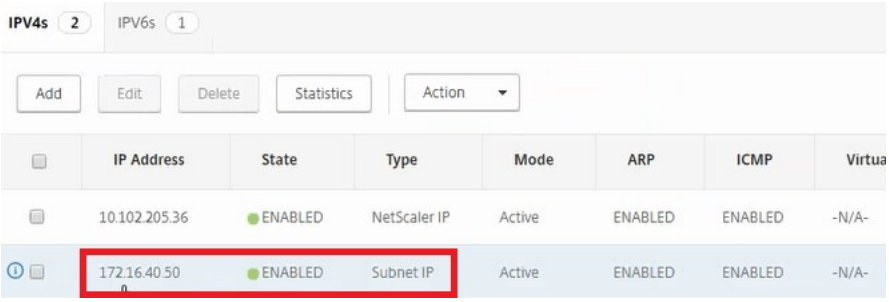


> **Hinweis**
>
> Ein L2-Gateway wird für jede Datenschnittstelle erstellt.

Zugeteilten NetScaler anzeigen

1. Melden Sie sich mit der in NetScaler ADM angezeigten IP-Adresse bei der NetScaler VPX-Instanz an. Navigieren Sie dann zu **Konfiguration** > **System** > **Netzwerk**. Im rechten Bereich können Sie sehen, dass die beiden IP-Adressen hinzugefügt wurden. Klicken Sie auf den Hyperlink IP-Adresse, um die Details anzuzeigen.

Die Subnetz-IP-Adresse entspricht der IP-Adresse der im NSX hinzugefügten Weboberfläche.



2. Navigieren Sie zu **Konfiguration** > **System** > **Lizenzen**, um die Lizenzen anzuzeigen, die auf diese Instanz angewendet werden.

Konfigurieren von NetScaler VPX Instanz mit StyleBook

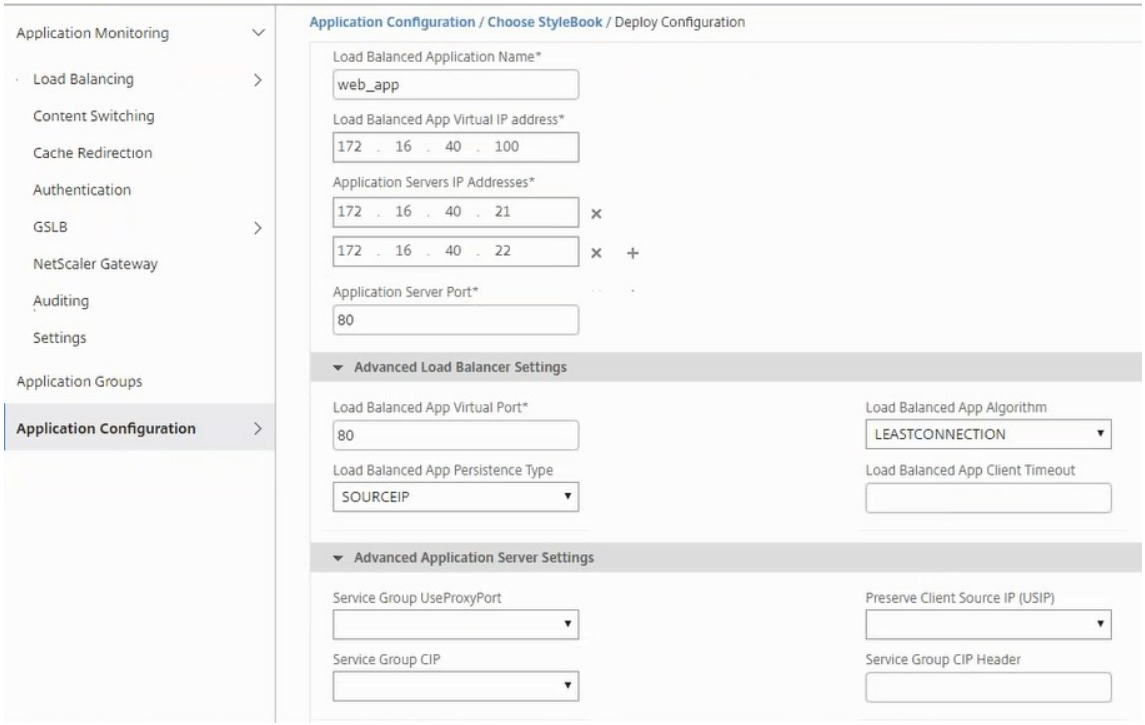
1. Navigieren Sie in NetScaler ADM zu **Orchestration** > **SDN Orchestration** > **NSX Manager konfigurieren** > **Edge-Gateways**.

   Notieren Sie sich die NetScaler-Instanz-IP, die dem jeweiligen Edge-Gateway zugewiesen ist, auf das die Load Balancing-Konfiguration über StyleBooks angewendet werden muss.

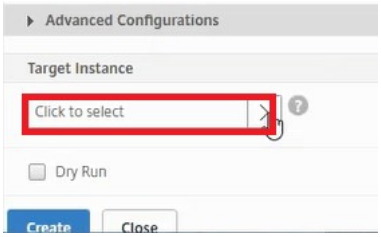
2. Erstellen Sie ein neues StyleBook. Navigieren Sie zu **Applications** > **Configuration**, importieren Sie das StyleBook und wählen Sie das StyleBook aus der Liste aus.

   Informationen zum Erstellen eines neuen StyleBook finden Sie unter Erstellen Sie Ihr eigenes StyleBook.

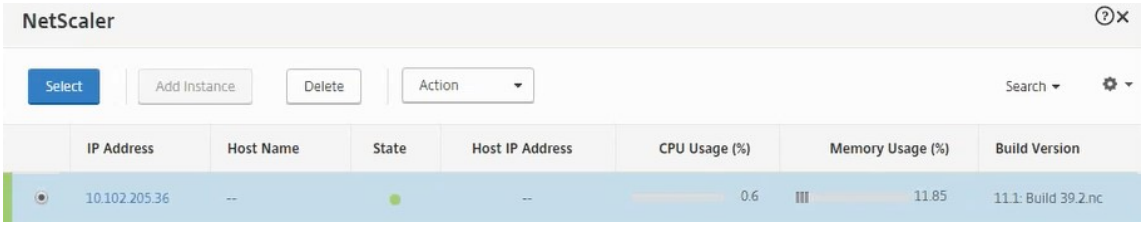
3. Geben Sie Werte für alle erforderlichen Parameter an.



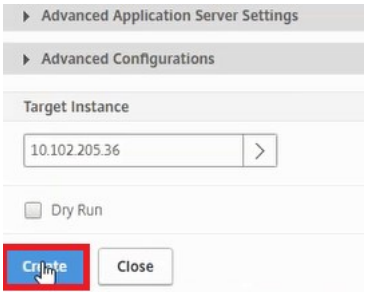
4. Geben Sie die NetScaler VPX Instanz an, auf der diese Konfigurationseinstellungen ausgeführt werden sollen.



5. Wählen Sie die zuvor notierte IP-Instanz aus, und klicken Sie auf **Auswählen**.

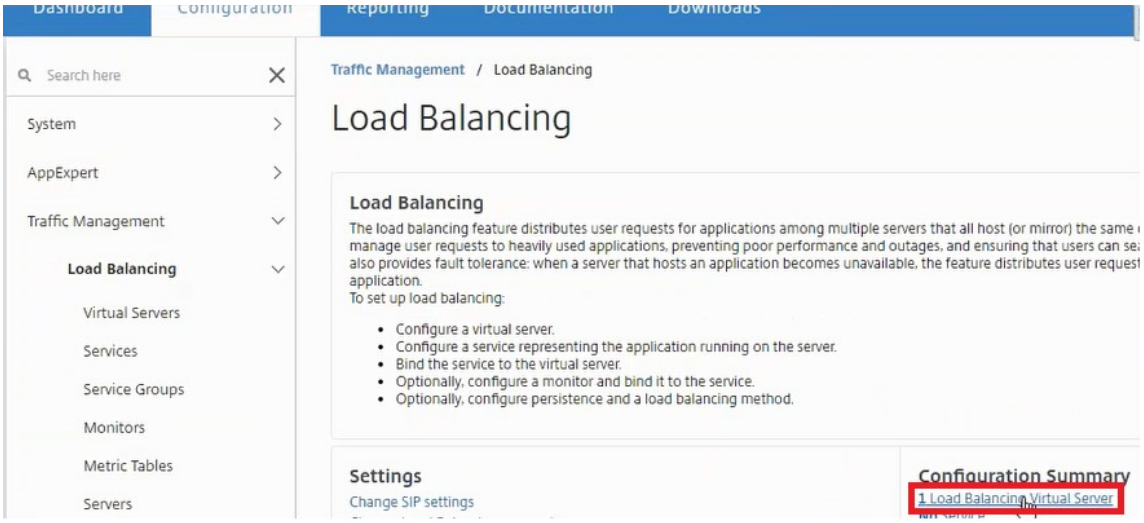


6. Klicken Sie auf **Erstellen**, um die Konfiguration auf das ausgewählte Gerät anzuwenden.

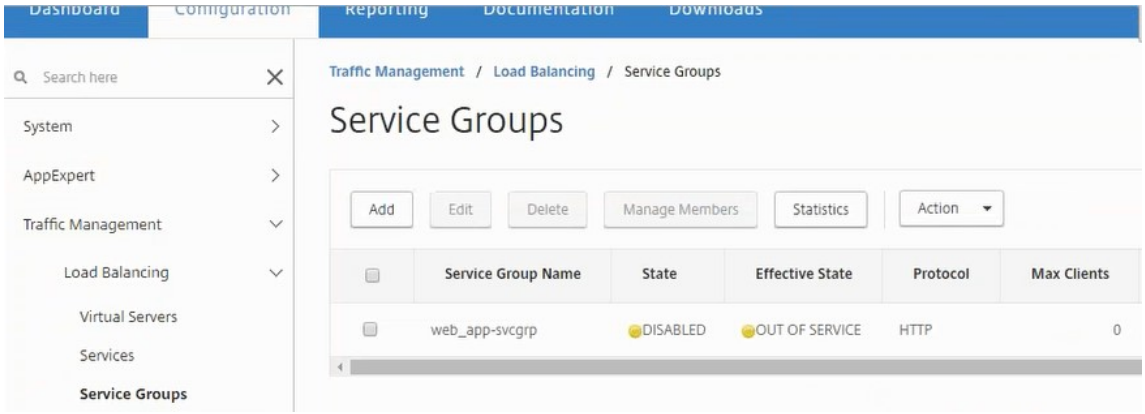


Load Balancer-Konfiguration anzeigen

1. Melden Sie sich bei der NetScaler VPX Instanz an, navigieren Sie zu **Configuration** > **Traffic Management** > **Load Balancing**, um den virtuellen Lastausgleichsserver anzuzeigen, der erstellt wird.



Sie können auch die erstellten Dienstgruppen anzeigen.

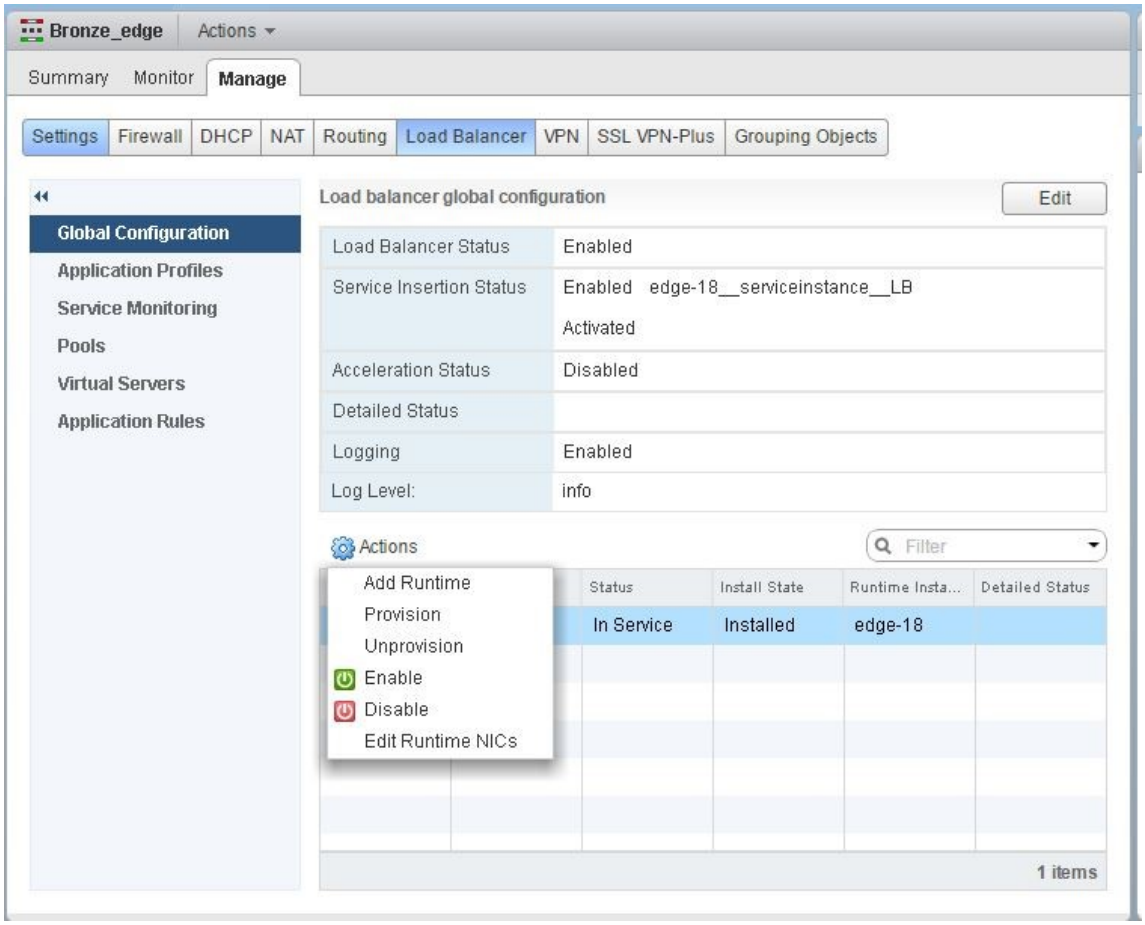


2. Wählen Sie die Dienstgruppe aus, und klicken Sie auf **Mitglieder verwalten**. Auf der Seite **Dienstgruppenmitglied konfigurieren** werden die Mitglieder angezeigt, die der Dienstgruppe zugeordnet sind.

Löschen des Load Balancer-Dienstes

1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Konfiguration**und klicken Sie auf das **X-Symbol**, um die Anwendungskonfiguration zu löschen.
2. Melden Sie sich beim NSX Manager auf dem vSphere Web Client an und navigieren Sie zu dem Edge-Gateway, mit dem die NetScaler VPX-Instanz verbunden ist.
3. Navigieren Sie zu **Verwalten** > **Load Balancer** > **Globale Konfiguration**, klicken Sie mit der rechten Maustaste auf den Laufzeiteintrag, und wählen Sie **Bereitstellung aufheben**.

> **Hinweis:**
>
> Edge Gateways in NetScaler ADM entspricht Laufzeiteinträgen in NSX Manager.



Die NetScaler VPX Instanz wird außer Betrieb gesetzt.

4. Navigieren Sie in NetScaler ADM zu **Orchestration** > **SDN Orchestration** > **NSX Manager konfigurieren** > **Edge-Gateways**. Stellen Sie sicher, dass die entsprechende Zuordnung des Edge-Gateways zur gelöschten Instanz nicht vorhanden ist.

NSX Manager: Automatische Provisioning von NetScaler Instanzen

February 5, 2024

Übersicht

NetScaler Application Delivery Management (ADM) lässt sich in die VMware-Netzwerkvirtualisierungsplattform integrieren, um die Bereitstellung, Konfiguration und Verwaltung von NetScaler-Diensten zu automatisieren. Diese Integration abstrahiert die traditionellen Komplexitäten, die mit der physischen

Netzwerktopologie verbunden sind, und ermöglicht es vSphere/vCenter-Administratoren, NetScaler Dienste programmgesteuert schneller bereitzustellen.

Beim Einfügen und Löschen von Lastausgleichsdiensten auf VMware NSX Manager stellt NetScaler ADM die NetScaler-Instanzen dynamisch bereit und zerstört sie. Für diese dynamische Bereitstellung müssen die NetScaler VPX-Lizenzzuweisungen in NetScaler ADM automatisiert werden. Wenn die NetScaler-Lizenzen auf das NetScaler ADM hochgeladen werden, übernimmt NetScaler ADM die Rolle des Lizenzservers.

Voraussetzungen

> **Hinweis**
>
> Diese Integration wird nur für **VMware NSX for vSphere 6.1 oder früher**unterstützt.

- NetScaler ADM, Version 13.0, hochverfügbar und auf ESX installiert.
- NetScaler VPX, Version 13.0
- NetScaler VPX-Lizenzen für NetScaler VPX-Instanzen, Version 13.0
- Installieren Sie VMware ESXi Version 4.1 oder höher mit Hardware, die die Mindestanforderungen erfüllt.
- Installieren Sie VMware Client auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
- Installieren Sie VMware OVF Tool (erforderlich für VMware ESXi Version 4.1) auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.

Bereitstellung von NetScaler ADM und NetScaler Instances mit hoher Verfügbarkeit

Um das NetScaler ADM HA-Setup bereitzustellen, installieren Sie die NetScaler ADM-Image-Datei, die Sie von der NetScaler-Website heruntergeladen haben. Weitere Informationen zum Bereitstellen des NetScaler ADM HA-Setups finden Sie unter Bereitstellen von NetScaler ADM in Hochverfügbarkeit.

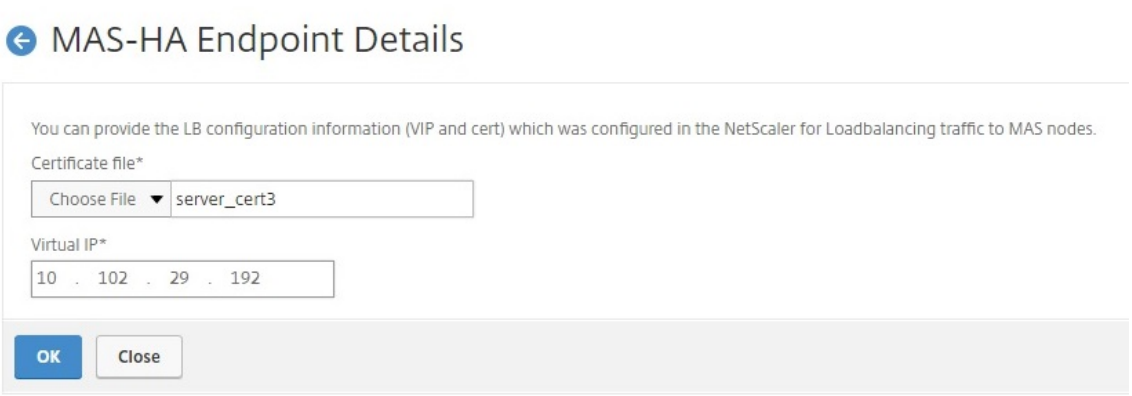
Einrichten von NetScaler ADM HA Endpoint Details

Um VMware NSX Manager in NetScaler ADM zu integrieren, das in einem HA-Modus bereitgestellt wird, müssen Sie zunächst die virtuelle IP-Adresse der NetScaler-Load-Balancing-Instanz eingeben. Sie müssen auch die Zertifikatsdatei, die auf dem virtuellen NetScaler Load Balancing-Server vorhanden ist, in das NetScaler ADM-Dateisystem hochladen.

Gehen Sie wie folgt vor, um Informationen zur Load-Balancing-Konfiguration in NetScaler ADM bereitzustellen:

1. **Navigieren Sie im NetScaler ADM HA-Knoten zu**System**> Deployment.**
2. Klicken Sie oben rechts auf **HA-Einstellungen**, und klicken Sie auf der Seite **MAS-HA-Einstellungen** auf **MAS-HA-Endpunktdetails**.

3. Laden Sie auf der Seite "**MAS-HA-Endpoint-Details** "dasselbe Zertifikat hoch, das bereits auf der NetScaler Instanz für den Lastausgleich vorhanden ist.
4. Geben Sie die virtuelle IP-Adresse der NetScaler Instanz für den Lastausgleich ein, und klicken Sie auf **OK**.



Registrieren von VMware NSX Manager bei NetScaler ADM

Wenn Sie zwei NetScaler ADM-Server mit hoher Verfügbarkeit einrichten, befinden sich die beiden Serverknoten im aktiv/passiven Modus. Melden Sie sich beim primären NetScaler ADM-Serverknoten an, um VMware NSX Manager bei NetScaler ADM in HA zu registrieren und einen Kommunikationskanal zwischen ihnen zu erstellen.

So registrieren Sie VMware NSX Manager bei NetScaler ADM in HA:

1. **Navigieren Sie im primären NetScaler ADM-Serverknoten zu**Orchestration > SDN Orchestration****> VMware NSX Manager**.**
2. Klicken Sie auf **NSX Manager-Einstellungen konfigurieren**.
3. **Legen Sie auf der Seite NSX Manager-Einstellungen konfigurieren** die folgenden Parameter fest:

a) NSX Manager-IP-Adresse: IP-Adresse von NSX Manager.

b) NSX Manager-Benutzername —Administratorbenutzername von NSX Manager.

c) Kennwort - Kennwort des administrativen Benutzers von NSX Manager.

4. Geben Sie im Abschnitt NetScaler ADM-Konto, das von NSX Manager verwendet wird, das NetScaler-Treiberkennwort für den NSX Manager ein.
5. Klicken Sie auf **OK**.

Hochladen von Lizenzen in NetScaler ADM

Laden Sie die NetScaler VPX Lizenzen auf NetScaler ADM hoch, damit NetScaler ADM den Instanzen während der Orchestrierung mit NSX automatisch Lizenzen zuweisen kann.

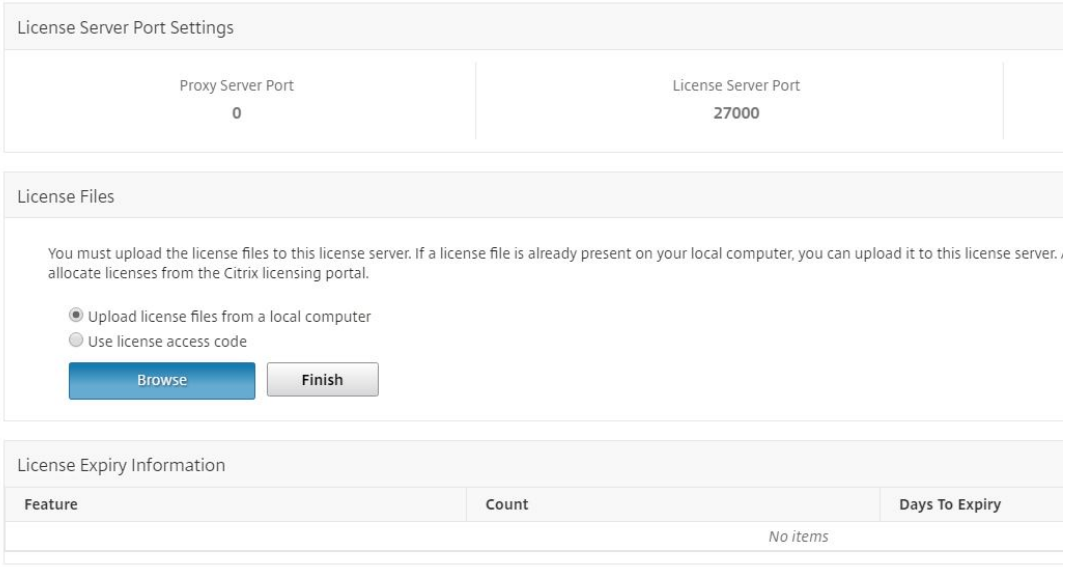
So installieren Sie Lizenzdateien auf NetScaler ADM:

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Gepoolte Lizenzierung**.
2. Wählen Sie im Abschnitt **Lizenzdateien** eine der folgenden Optionen aus:

   a) **Upload von Lizenzdateien von einem lokalen Computer** : Wenn eine Lizenzdatei bereits auf dem lokalen Computer vorhanden ist, können Sie sie in NetScaler ADM hochladen. Um Lizenzdateien hinzuzufügen, klicken Sie auf **Durchsuchen** und wählen Sie die Lizenzdatei (.lic) aus, die Sie hinzufügen möchten. Dann klick **Fertig stellen**.

   b) **Lizenzzugangscode verwenden** - Citrix sendet den Lizenzzugangscode für die von Ihnen erworbenen Lizenzen per E-Mail. Um Lizenzdateien hinzuzufügen, geben Sie den Lizenzzugriffscode in das Textfeld ein und klicken Sie dann auf **Lizenzen abrufen**.

   > **Hinweis:**Sie können dem NetScaler ADM
   >
   > jederzeit über die Lizenzeinstellungen weitere Lizenzen hinzufügen.



Hochladen von NetScaler VPX Images in NetScaler ADM

Fügen Sie NetScaler Images zu NetScaler ADM hinzu, damit NetScaler ADM diese Images wie im Servicepaket definiert verwendet.

So laden Sie NetScaler VPX-Images in NetScaler ADM hoch:

1. Navigieren Sie in NetScaler ADM zu **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **ESX NSVPX-Images**.
2. Klicken Sie auf **Hochladen**, und wählen Sie im lokalen Speicherordner das NetScaler VPX Zip-Paket aus.

Servicepakete in NetScaler ADM erstellen

Erstellen Sie Servicepakete in NetScaler ADM, um den Satz von SLAs zu definieren, der angibt, wie die NetScaler Ressourcen zugewiesen werden.

So erstellen Sie Servicepakete in NetScaler ADM:

1. Navigieren Sie in NetScaler ADM zu**Orchestration >**SDN Orchestration****>**VMware NSX Manager**> **Service Packages**und klicken Sie auf **Hinzufügen, um ein neues Servicepaket hinzuzufügen** .
2. Legen Sie auf der Seite **Service Package** im Abschnitt **Grundeinstellungen** die folgenden Parameter fest:

    a) Name —Name eines Servicepakets

b) Isolationsrichtlinie —wählen Sie **Dediziert**

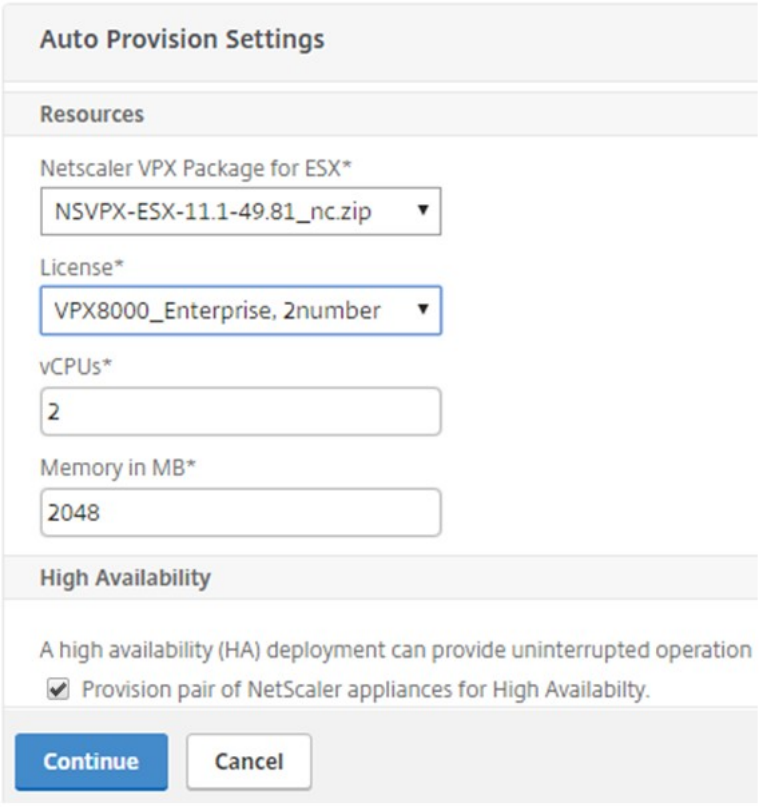
c) **NetScaler Instance Provisioning —wählen Sie Create Instance OnDemand**

d) Auto Provision Platform —wählen Sie **CitrixNetScaler**SDX

e) Klicken Sie auf **Weiter**.

3. **Wählen Sie im Abschnitt**Automatische Bereitstellungseinstellungen**das kürzlich hochgeladene NetScaler VPX-ZIP-Paket für die Bereitstellung auf der NSX-Plattform aus, wählen Sie die entsprechende Lizenz aus und klicken Sie auf Weiter.**

> **Hinweis Aktivieren Sie**
>
> im Abschnitt "**Hohe Verfügbarkeit** "das Kontrollkästchen, um NetScaler Instanzen für HA bereitzustellen.



> **Hinweis**
>
> Der Name der Lizenz, der in dem in der obigen Abbildung gezeigten Listenfeld angezeigt wird, Vpx8000_Advanced, 2-Nummer ist ein Beispiel und wird wie folgt erklärt:
>
> - VPX: Die Lizenz besteht darin, NetScaler VPX Instanzen bereitzustellen.
> - 8000 —Die nutzbare Bandbreite beträgt 8 GB

> - Advanced —NetScaler bietet drei Lizenztypen: Standard, Advanced und Premium
> - 2 Nummer - zwei NetScaler VPX Instanzen können mit dieser Lizenz bereitgestellt werden
>
> Der Name der Lizenz, der im**Listenfeld Lizenz** angezeigt wird, hängt von der Lizenz ab, die Sie von Citrix erworben haben.

4. Klicken Sie auf **Weiter**.
5. Das Servicepaket wird in NSX Manager veröffentlicht. Navigieren Sie in NSX Manager zu **Service Definitions** > **Service Manager**. Sie können NetScaler ADM als einen der Service Manager betrachten. Dies bedeutet, dass die Registrierung erfolgreich war und eine bidirektionale Kommunikation zwischen dem NSX Manager und NetScaler ADM hergestellt wurde.

> **Hinweis**
>
> Für NetScaler ADM in der Hochverfügbarkeitsbereitstellung werden die Lizenzen nur in den NetScaler ADM-Lizenzserverknoten hochgeladen. Die NetScaler ADM Knoten befinden sich im Aktiv-passiven Modus.

Ausführen des Lastausgleichsdiensteinfügens für Edge

Führen Sie die Einfügung des Lastausgleichsdienstes auf dem vorhandenen NSX Edge Gateway durch, d. h. die Lastausgleichsfunktion vom NSX Load Balancer auf NetScaler.

So fügen Sie den Load Balancing-Dienst auf NSX Edge Gateway ein:

1. Navigieren Sie in NSX Manager zu **Home** > **Netzwerk und Sicherheit** > **NSX Edges**, und doppelklicken Sie, um das von Ihnen konfigurierte Edge-Gateway auszuwählen.
2. Klicken Sie auf **Verwalten**, wählen Sie auf der Registerkarte **Load Balancer** die Option **Globale Konfiguration** aus, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie **Load Balancer aktivieren** und **Service Insertion aktivieren** aus, um sie zu aktivieren.
4. Wählen Sie unter **Service Definition**das Servicepaket aus, das in NSX Manager veröffentlicht wurde.
5. Konfigurieren Sie eine virtuelle Netzwerkkarte für die Verwaltungsschnittstelle und eine oder mehrere virtuelle Netzwerkkarten für Datenschnittstellen. Wählen Sie die Netzwerke für die Verwaltung und die Daten entsprechend aus.

> **Hinweis**
>
> Wählen Sie im Modus Primäre IP-Zuweisung die Option IP-Pool aus. NetScaler ADM unter-

> stützt keine manuelle oder DHCP-Zuweisung von IP-Adressen.

6. Klicken Sie auf das Aktualisierungssymbol, um die Erstellung der Laufzeit zu sehen.

   > **Hinweis:**
   >
   > Da Sie in der HA-Bereitstellung zwei NetScaler VPX-Instanzen bereitstellen, werden im NSX Manager zwei Laufzeiten erstellt.
   >
   > Möglicherweise müssen Sie den Bildschirm aktualisieren, um die auf dem Bildschirm angezeigten Laufzeiten zu sehen.

7. Wählen Sie die Laufzeit aus, klicken Sie auf **Aktionen**und wählen Sie im Popupmenü die Option **Installieren** aus. Für HA wiederholen Sie dies auch für die andere Laufzeit.
8. Wenn beide virtuellen Maschinen gestartet werden, ändert sich der Wert von Status in "In Dienst"und der Wert des Installationsstatus ändert sich in "Aktiviert".

   > **Hinweis:**
   >
   > Möglicherweise müssen Sie den Bildschirm aktualisieren, um die Statusänderung zu sehen.

9. Navigieren Sie in NetScaler ADM zu **Orchestration** > **Requests**, um die Fortschrittsdetails beim Abschluss der Diensteinfügung einzusehen. Sie können sehen, dass eine Anfrage zur Erstellung und Aktualisierung der Laufzeit bei NetScaler ADM eingegangen ist. Wenn die Laufzeit aktualisiert wurde, wählen Sie die Anforderung aus und klicken Sie auf die Schaltfläche **Aufgaben**, um zu sehen, dass NetScaler ADM zu NSX Manager hinzugefügt wurde.

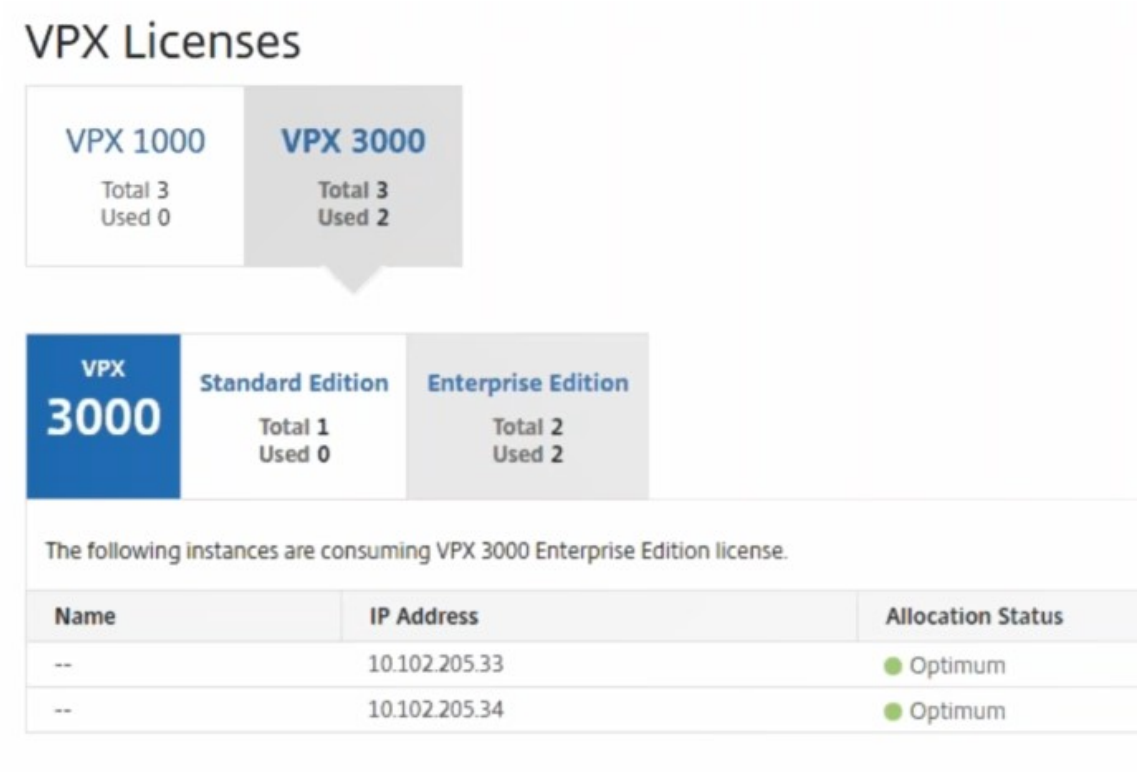
   Für HA wird es zwei Anfragen geben, um zwei Laufzeiten in NetScaler ADM zu erstellen und zu aktualisieren. Wenn beide Laufzeiten aktualisiert wurden, wählen Sie beide Anfragen aus und klicken Sie auf die Schaltfläche **Aufgaben**, um zu überprüfen, ob zwei NetScaler ADM HA-Knoten in NSX Manager hinzugefügt wurden.

10. **Navigieren Sie in NetScaler ADM zu**Orchestration > **SDN Orchestration**** > **VMware** NSX Manager > Edge Gateways.** Im rechten Bereich können Sie sehen, dass der NetScaler VPX dem NSX Edge Gateway hinzugefügt wurde.

    Für HA können Sie sehen, dass dem NSX Edge Gateway zwei NetScaler VPX-Instanzen im HA-Modus hinzugefügt wurden.

11. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Gepoolte Lizenzierung > VPX-Lizenzen**. Wählen Sie die NetScaler VPX -Lizenz und die installierte Edition aus.

    Die NetScaler VPX Instanzen, die sich im HA-Modus befinden, verbrauchen zwei Lizenzen, und der Status wird wie folgt auf dem Bildschirm angezeigt.



Wenn die Diensteinfügung abgeschlossen ist, können Sie StyleBooks verwenden, um die NetScaler Instanzen mit einer der folgenden beiden Methoden zu konfigurieren:

- Konfigurieren der Lastenausgleichsdienste auf NetScaler VPX in VMware NSX Manager GUI
- Konfigurieren der Lastenausgleichsdienste auf NetScaler VPX in der NetScaler ADM GUI

Konfigurieren der Lastenausgleichsdienste auf NetScaler VPX in VMware NSX Manager GUI

Führen Sie die folgende Aufgabe aus, um die Konfiguration von Lastausgleichsdiensten auf dem NSX Edge-Gateway gerät mithilfe integrierter StyleBooks zu aktivieren.

Navigieren Sie in NSX Manager zu **Home** > **Netzwerk und Sicherheit** > **NSX Edges**, und doppelklicken Sie, um das von Ihnen konfigurierte Edge-Gateway auszuwählen.

Pools und Poolmitglieder erstellen

Erstellen Sie einen Pool von Servern und Mitgliedern mit unterschiedlichen Kapazitäten.

1. Klicken Sie auf **Verwalten**und wählen Sie auf der Registerkarte **Load Balancer** die Option **Pools**aus und klicken Sie auf das Symbol "**+**", um einen neuen Pool hinzuzufügen, und legen Sie die folgenden Parameter fest:

a) Name —Name des neuen Pools

b) Algorithmus - Wählen Sie einen Algorithmus aus der Dropdownliste aus, auf der der Pool ausgewählt wird.

c) Monitore —Stellen Sie sicher, dass der Servicemonitor auf default_http_monitor eingestellt ist

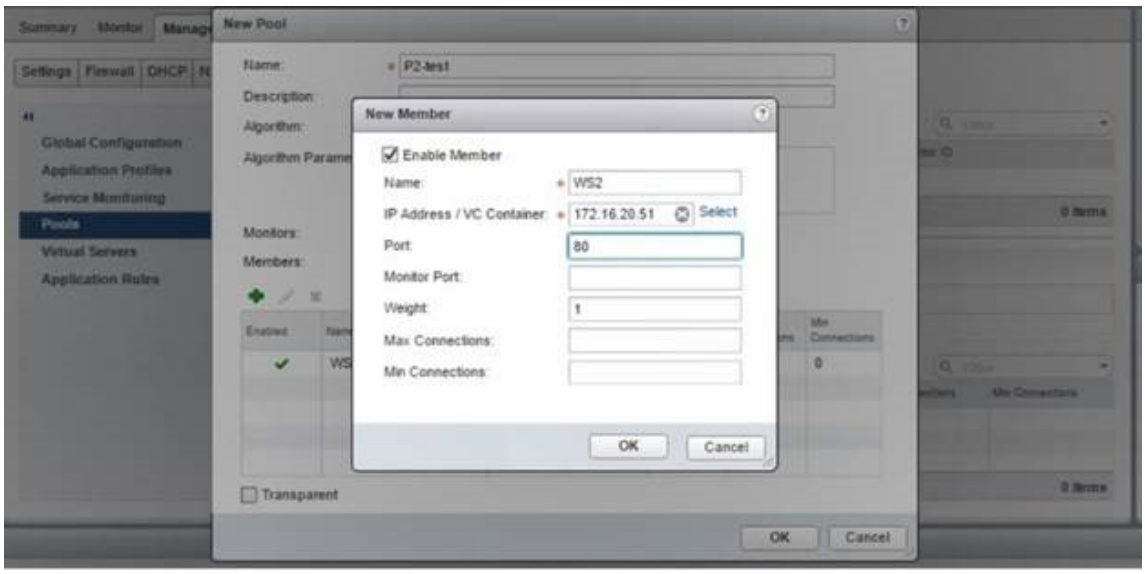
d) Mitglieder —Klicken Sie auf „+“, um Mitglieder zum Pool hinzuzufügen, und geben Sie die erforderlichen Parameter in das Fenster Neues Mitglied ein.

i. Name - Name des Mitglieds

ii. IP-Adresse/VC-Container —Klicken Sie auf Auswählen, um das Objekt aus der verfügbaren Liste auszuwählen, oder geben Sie die IP-Adresse des Objekts ein.

2. Klicken Sie auf **OK**.

Fügen Sie beliebig viele Mitglieder hinzu.



Erstellen virtueller Server

Erstellen Sie einen Satz virtueller Server, und weisen Sie jedem virtuellen Server einen Pool zu.

1. Klicken Sie auf **Verwalten**und wählen Sie auf der Registerkarte Load Balancer die Option **Virtuelle Server**aus und klicken Sie auf das Symbol “**+**“, um einen virtuellen Server hinzuzufügen, und legen Sie die folgenden Parameter fest:

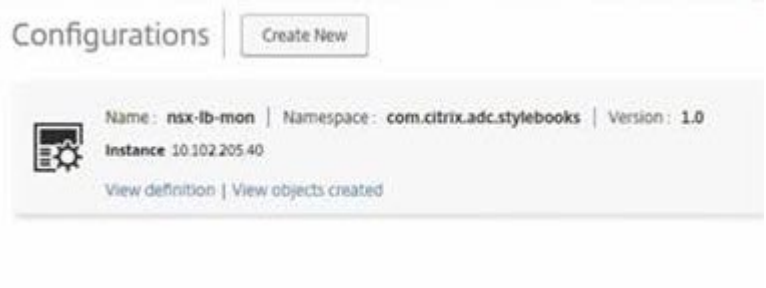
a) Anwendungsprofil —Standardmäßig wird das Dienstprofil angezeigt, das Sie in NetScaler ADM erstellt haben.

b) Name —Name des virtuellen Servers.

c) IP-Adresse —Klicken Sie auf Auswählen, um einen vorhandenen Pool von IP-Adressen auszuwählen oder einen neuen Pool von IP-Adressen zu erstellen.

d) Standardpool - Wählen Sie den Standardpool aus der Dropdownliste aus.

2. Klicken Sie auf **OK**.
3. Navigieren Sie in NetScaler ADM zu **Orchestration** > **Requests**, um Fortschrittsdetails zum Abschluss der Diensterstellung auf einer oder mehreren ausgewählten NetScaler Instanzen anzuzeigen.
4. Navigieren Sie in NetScaler ADM zu **Applications** > **Configuration**, und überprüfen Sie, ob das `nsx-lb-mon` Config Pack erstellt wurde.



Konfigurieren der Lastenausgleichsdienste auf NetScaler VPX in der NetScaler ADM GUI

Stellen Sie mithilfe von NetScaler ADM StyleBooks Load Balancer-Konfigurationen auf der NetScaler-Instanz bereit. Für HA wird die Konfiguration auf beiden NetScaler-Instanzen bereitgestellt, die sich in HA befinden.

So erstellen Sie Konfigurationspakete über StyleBooks:

1. Navigieren Sie in NetScaler ADM zu **Applications** > **Configuration** > **Create New**und wählen Sie das **HTTP/SSL LoadBalancing (with Monitors**) StyleBook aus der Liste aus. Das StyleBook wird als Benutzeroberflächenseite geöffnet, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben.
2. Geben Sie Werte für alle erforderlichen Parameter an.
3. Wählen Sie die NetScaler VPX-Zielinstanz aus, die in der NSX-Umgebung bereitgestellt wird, und klicken Sie auf **Erstellen**, um die Konfiguration auf das ausgewählte Gerät anzuwenden. Wählen Sie für die HA-Bereitstellung die Instanzen aus, die sich im HA-Modus befinden.

Überprüfung der Erstellung virtueller Server und Dienstgruppen in NetScaler VPX-Instanzen

Sie können sehen, dass die Dienstgruppen und virtuellen Server erstellt werden, indem Sie sich bei der NetScaler VPX-Instanz anmelden.

So zeigen Sie die Dienstgruppen und virtuellen Server an:

1. Melden Sie sich bei der NetScaler VPX-Instanz an. Für die HA-Bereitstellung müssen Sie sich bei beiden NetScaler-Instanzen anmelden, die sich in HA befinden.
2. Navigieren Sie zu **Konfiguration** > **System** > **Netzwerk**. Im rechten Bereich können Sie die hinzugefügten IP-Adressen sehen. Klicken Sie auf den Hyperlink IP-Adresse, um die Details anzuzeigen. Sie können sehen, dass die Subnetz-IP-Adresse mit der IP-Adresse der Webschnittstelle übereinstimmt, die in NSX hinzugefügt wurde.
3. Navigieren Sie als Nächstes zu **Traffic Management** > **Load Balancing** > **Virtuelle Server** und sehen Sie sich die Details des virtuellen Servers an.
4. Navigieren Sie als Nächstes zu **Service Groups** und sehen Sie sich die Servicegruppendetails an.
5. Navigieren Sie schließlich zu **Konfiguration** > **System** > **Lizenzen**, um die Lizenzen anzuzeigen, die auf diese Instanz angewendet werden.

Load Balancing Services löschen

Wenn die Lastenausgleichsdienste für die NetScaler VPX-Instanzen, die auf dem NSX Manager bereitgestellt werden, nicht mehr erforderlich sind, können Sie die zuvor durchgeführten Diensteinfügungen löschen.

So löschen Sie die Konfiguration und das Einfügen von Diensten:

1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Konfiguration**, wählen Sie die erstellte Anwendungskonfiguration aus und löschen Sie dann die Konfiguration, indem Sie auf das Symbol „X“klicken.
2. Navigieren Sie in NSX Manager zu dem Edge-Gateway, mit dem die NetScaler VPX-Instanz verbunden ist. **Navigieren Sie zu**Manage**>**Load Balancer**>**Global Configuration**, klicken Sie mit der rechten Maustaste auf den Runtime-Eintrag und klicken Sie dann auf Bereitstellung aufheben.** Die virtuelle Maschine wird außer Betrieb genommen.
3. Navigieren Sie in NetScaler ADM zu **Orchestration** > **Cloud Orchestration** > **Edge-Gateways**. Stellen Sie sicher, dass es keine entsprechende Zuordnung von Edge-Gateway zu gelöschter Instanz gibt.

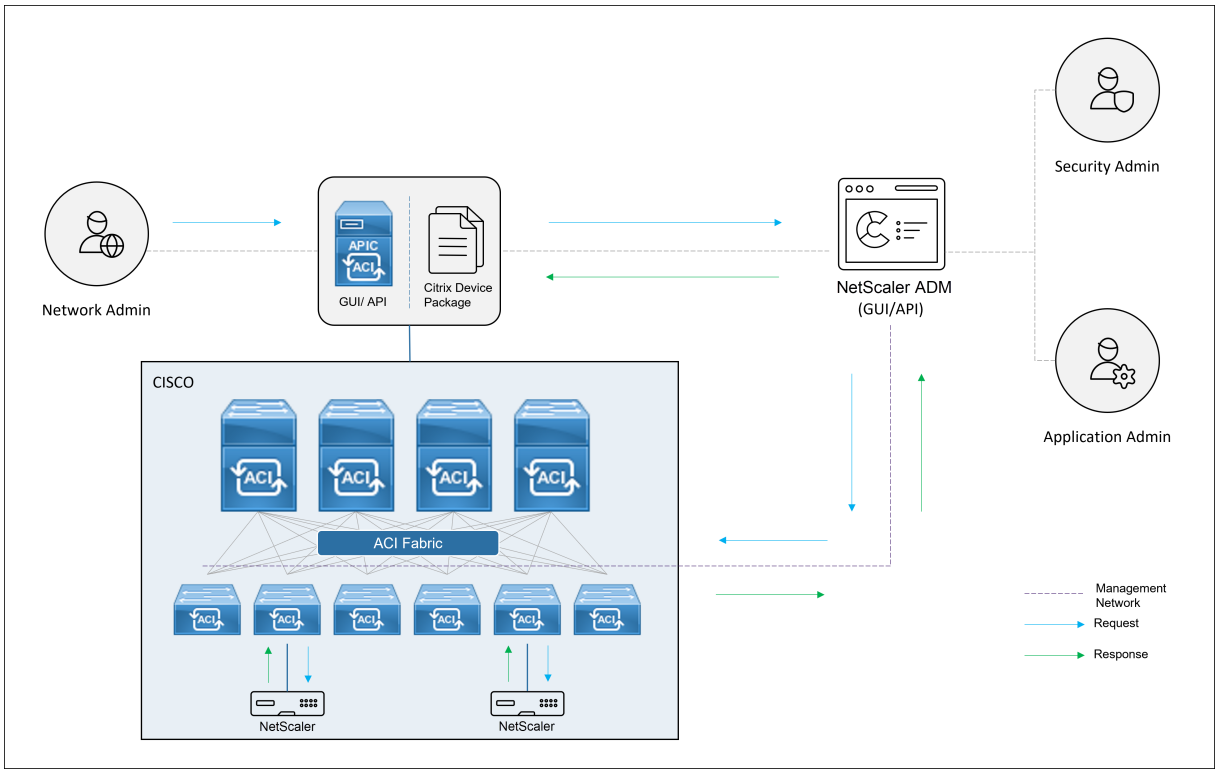
NetScaler Automatisierung mit NetScaler ADM im Cisco ACI-Hybridmodus

February 5, 2024

Cisco ACI hat die Unterstützung für den Hybrid-Modus in Version 1.3 (2f) eingeführt. Im Hybridmodus können Sie die Netzwerkautomatisierung über den Application Policy Infrastructure Controller (APIC) durchführen und gleichzeitig die L4-L7-Konfiguration an NetScaler Application Delivery Management (ADM) delegieren, das als Gerätemanager im APIC fungiert.

Die NetScaler Hybridmodus-Lösung wird von einem Hybridmodusgerätepaket und NetScaler ADM unterstützt. Sie müssen das Paket des Hybrid-Modus-Gerätes im APIC hochladen. Dieses Paket enthält alle konfigurierbaren Netzwerk-L2-L3-Entitäten von NetScaler. Die Anwendungsparität wird von StyleBook von NetScaler ADM dem APIC zugeordnet. Mit anderen Worten, StyleBook fungiert als Referenz zwischen L2-L3- und L4-L7-Konfigurationen für eine bestimmte Anwendung. Sie müssen bei der Konfiguration der Netzwerkentitäten aus dem APIC für NetScaler einen StyleBook-Namen angeben.

Die folgende Abbildung bietet einen Überblick über NetScaler in einer Lösung im Hybridmodus:

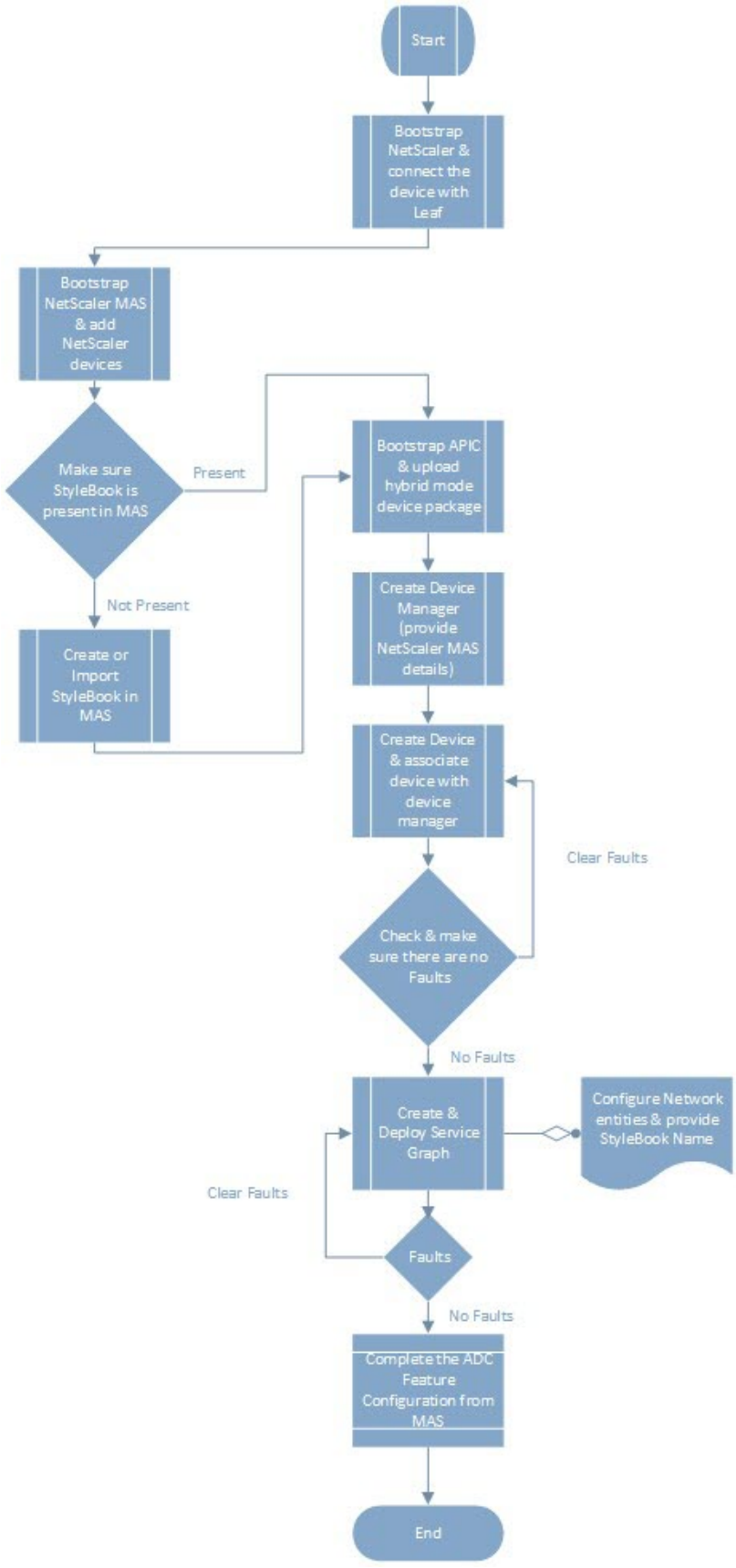


Im Hybridmodus wird die NetScaler Konfiguration in den folgenden zwei Phasen durchgeführt:

1. Netzwerkstitching erfolgt über die Cisco APIC
2. Die Konfiguration erfolgt über das NetScaler ADM

Für jede bestimmte Anwendung muss ein Netzwerkadministrator im Rahmen der Erstellung und Bereitstellung des Service-Graphen im Cisco APIC netzwerkspezifische Details wie IP-Adressen, Port, VLAN (automatisiert) usw. angeben. Diese Konfigurationsdetails werden dann über das Gerätepaket an NetScaler ADM übertragen, und NetScaler ADM verarbeitet sie intern und konfiguriert den NetScaler. Ein Anwendungsadministrator erstellt die ADC-bezogene Konfiguration der Anwendung mithilfe von StyleBook in NetScaler ADM. Diese Konfigurationen werden dann von NetScaler ADM an den NetScaler übertragen. Der Cisco APIC und NetScaler ADM kommunizieren über das Verwaltungsnetzwerk mit dem ADC.

Das folgende Diagramm zeigt einen NetScaler Workflow in der Hybridlösung:



NetScaler Gerätepaket im Cloud Orchestrator-Modus von Cisco ACI

February 5, 2024

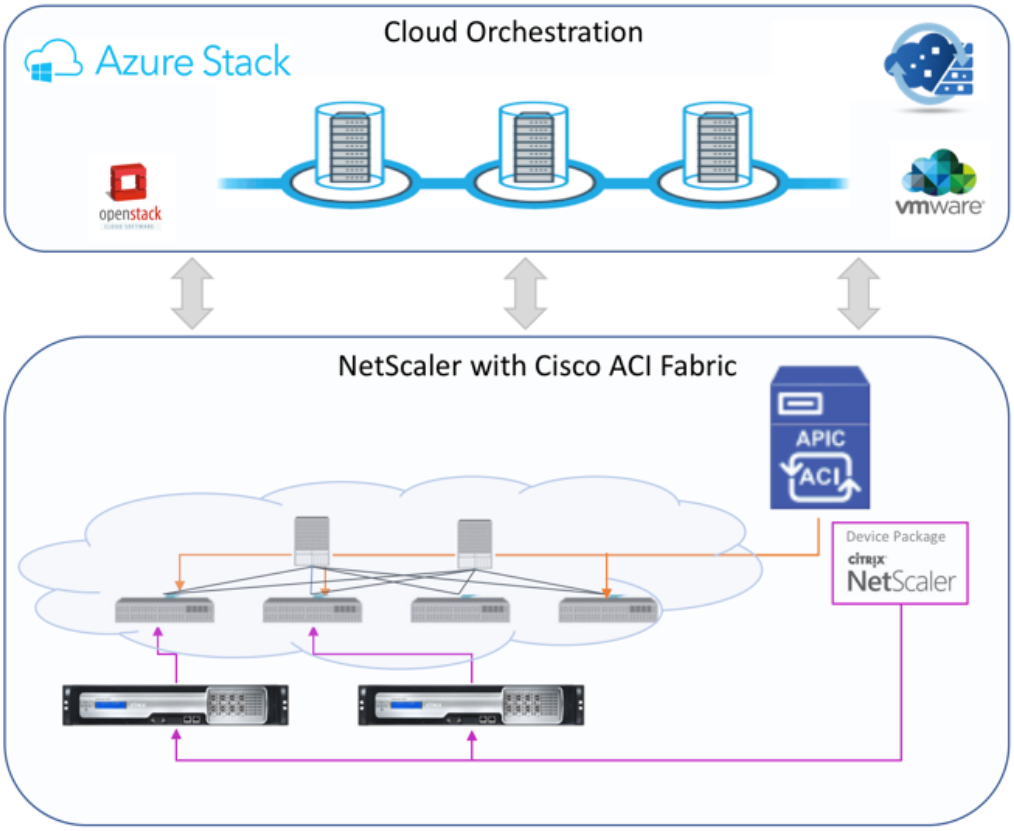
Mit Application Policy Infrastructure Controller (APIC), Version 3.1, erweitern NetScaler und Cisco ACI das gemeinsame Integrationsportfolio, um eine neue Lösung bereitzustellen, die auf die Bedürfnisse des Kunden zugeschnitten ist. Der neue Integrationsmodus ACI Cloud Orchestrator Mode, vereinfacht L4-L7-Integrationen, indem die Komplexität der Konfiguration durch standardisierte Parameter abstrahiert wird. Die Lösung automatisiert nahtlos L4-L7-Services und erreicht so die Ziele agiler Anwendungsbereitstellungen, betrieblicher Flexibilität und Einfachheit.

Der Cisco ACI Cloud Orchestrator-Modus mithilfe der NetScaler-Lösung bietet folgende Vorteile:

- Die Automatisierung von L4-L7-Diensten reduziert menschliche Fehler.
- Die vorgefertigte Integration der Cisco ACI-Lösung hilft Ihnen, die Bereitstellungszeit zu verkürzen und die Leistung von Anwendungen wie Webanwendungen, virtuellen Maschinen und SQL zu steigern.
- Vollständig integrierte Transparenz in den Zustand von Anwendungen wie Webanwendungen, virtuellen Maschinen und SQL über physische und virtuelle Netzwerkkomponenten hinweg.

Der ACI-Cloud-Orchestrator-Modus bietet Ihnen jetzt mehr Möglichkeiten, die neue vereinfachte APIC-GUI direkt zu verwenden oder indem Sie einen beliebigen Cloud-Orchestrator wie Cisco Cloud Center, Windows Azure Pack, OpenStack, vRealize oder einen anderen auswählen, je nach Ihren Wünschen. Diese neue Änderung wird erreicht, indem eine Reihe von ADC-Attributen als ADC-Schema verfügbar gemacht wird. Diese Attribute werden in den Funktionsprofilen der Gerätepakete abgebildet. Sie können Werte für diese Attribute angeben, während Sie den ADC-Dienst vom Cloud-Orchestrator (Cisco Cloud Center oder Wireless Application Protocol (WAP)) bereitstellen.

Die folgende Abbildung bietet einen Überblick über NetScaler in einer Cloud-Orchestrierungslösung:

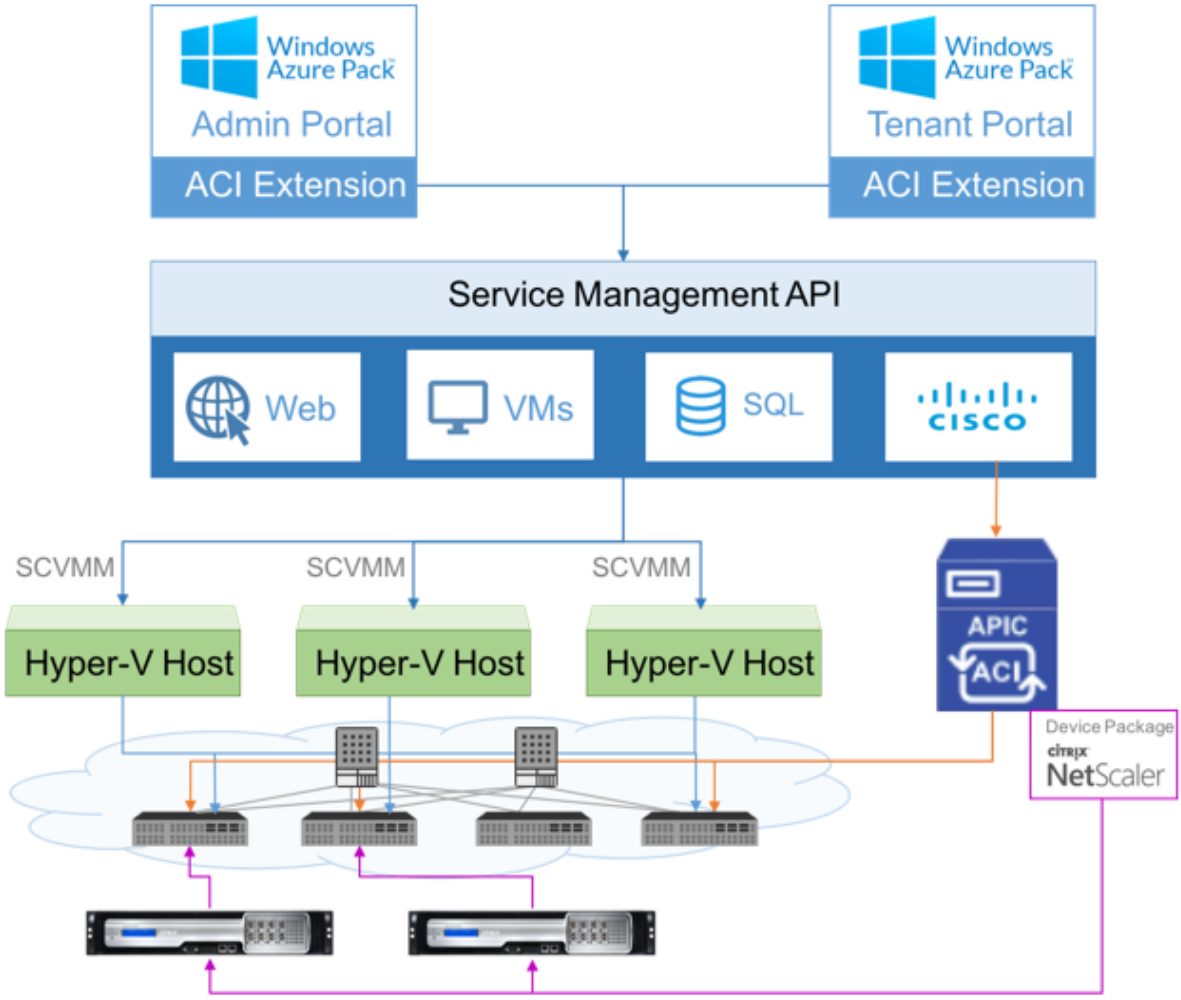


Die Lösung für den Cloud-Orchestrator-Modus mit Microsoft Azure Pack umfasst viele Integrationspunkte, wie Azure Pack zu Cisco APIC, Cisco APIC zu System Central Virtual Machine Manager (SCVMM) und Cisco APIC zu NetScaler. Als Mandant in der Private Cloud können Sie NAT aktivieren, Netzwerkdienste bereitstellen und einen Load Balancer hinzufügen.

Azure Pack unterstützt Mandanten- und Administratorportale, und jedes von ihnen verfügt über eigene Vorgänge, die ausgeführt werden können.

- Als Administrator können Sie administrative Aufgaben wie die ACI-Registrierung, den VIP-Bereich, die NetScaler-Gerätezuordnung mit der Cloud der virtuellen Maschine und die Erstellung von Mandantenbenutzerkonten ausführen.
- Als Mandant können Sie Aufgaben wie das Anmelden am Azure Pack-Mandantenportal und das Konfigurieren des Netzwerks, der Brückendomänen und des virtuellen Routing and Forwarding (VRFs) ausführen und die NetScaler Load Balancing- und RNAT-Funktionen verwenden.

Die folgende Abbildung bietet einen Überblick über Azure Pack in einer Lösung im Cloudmodus:



Wichtig!

- Der Cloud-Administrator kann das von APIC unterstützte L4-L7-Schema unterstützen, und alle zusätzlichen Änderungen können vom APIC-Administrator direkt im APIC vorgenommen werden. Auf diese Weise können Sie NetScaler auf dem Niveau des unterstützten Funktionssatzes konfigurieren und bereitstellen.
- Mandanten können mehrere VIP-Adressen mit unterschiedlichen Ports für dasselbe Netzwerk bereitstellen. Sie müssen sicherstellen, dass die Kombination von IP und Port eindeutig ist.
- Das NetScaler-Gerätepaket unterstützt nur die Bereitstellung mit einem Kontext. Jeder Mandant erhält eine dedizierte NetScaler-Instanz.
- Wireless Application Protocol (WAP) unterstützt NetScaler MPX-Appliances und NetScaler VPX-Appliances (einschließlich NetScaler VPX-Instanzen, die auf der NetScaler SDX-

> Plattform bereitgestellt werden).

Das Gerätepaket im Cloud-Orchestrator-Modus unterstützt sowohl den vollständig verwalteten Modus als auch den Service Manager-Modus. Das vollständig verwaltete Modus-Paket unterstützt eine Vielzahl von Funktionsprofilen, z. B. einfacher Lastausgleich, Content Switching, SSL-Offload und andere Profile. Diese Funktionsprofile decken einen vollständigen Funktionssatz und den Bereitstellungsmodus des NetScaler ab. In ähnlicher Weise unterstützt das Gerätepaket im Service Manager-Modus die ein- und zweiarmige Konfiguration und Bereitstellung von NetScaler mithilfe von APIC. Das NetScaler Application Delivery Management (ADM) fungiert als Service Manager für APIC, und Sie können NetScaler ADM verwenden, um NetScaler L4-L7-Parameter zu konfigurieren.

> **Hinweis**
>
> Im Service Manager-Modus (Hybridmodus) können Sie dieselbe Server-IP-Adresse, die bereits in der NetScaler Appliance vorhanden ist, nicht wiederverwenden oder neu zuweisen.

Das Funktionsprofil des Cloud-Orchestrator-Modus verfügt über eine Reihe von Parametern, die dem ADC-Schema des APICs zugeordnet sind, und der Orchestrator verwendet diese Parameter. Der Cloud-Orchestrator liefert die Werte für ADC-Parameter (VIP, während der NetScaler über APIC bereitgestellt wird). Der Orchestrator kommuniziert mit den APIs von APIC und übergibt die ADC-spezifischen Details als Teil der Nutzlast für ein bestimmtes Funktionsprofil. Intern extrahiert APIC die Werte und übergibt sie an das Gerätepaket, das den NetScaler intern konfiguriert.

Weitere Informationen zur vollständigen Liste der ADC-Schemas, die von Cisco APIC unterstützt werden, finden Sie im Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 3.x und früher).

Das Gerätepaket für den vollständig verwalteten Modus unterstützt die folgenden Funktionsprofile:

1. LB-HTTP-One-Arm-ProfileCM
2. LB-HTTP-Two-Arm-ProfileCM
3. LB-HTTP-Two-Arm-ServiceBackendProfileCM
4. CS-HTTP-LB-Service-ProfileCM
5. CS-SSL-LB-Service-ProfileCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHIC
11. SSLVServerProfileForAnywhereModeCM

12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM
16. CSLBServerProfileCM
17. GSLBServerProfileCM
18. CMPServerProfileCM
19. CRServerProfileC
20. DNSServerProfileCM
21. DSServerProfileCM
22. ICServerProfileCM
23. SSLVPNServerProfileCM
24. AppFWServerProfileCM
25. AAAServerProfileCM
26. AAASyslogServerProfileCM
27. IPv6WebInlineVServerProfileCM

Das Gerätepaket für den Dienstverwaltungsmodus unterstützt die folgenden Funktionsprofile im Cloud-Modus:

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

NetScaler unterstützt die oben genannten Funktionsprofile. Der APIC unterstützt eine Teilmenge dieser Parameter im ADC-Schema. Wenn im Funktionsprofil nicht unterstützte Attribute von Cisco ACI vorhanden sind, müssen Sie das Funktionsprofil des Cloud Orchestrator-Modus klonen und die Werte für alle nicht unterstützten Attribute von APIC bereitstellen und die Attribute speichern. Später kann der Orchestrator das neu geklonte Funktionsprofil verwenden.

Das Citrix Cloud-Modus-Gerätepaket unterstützt NetScaler 12.0 und der Service Manager-Modus verwendet auch NetScaler ADM 12.0. Das Gerätepaket hat die Modellversion von 1.0 auf 2.0 geändert und kann als Neuinstallation verwendet werden. Das Gerätepaket im Cloud-Orchestrator-Modus

kann nicht von früheren Gerätepaketversionen aktualisiert werden, da die Modellversion geändert wurde.

Gerätepakete im Cloud-Orchestrator-Modus können auch in der regulären Bereitstellung verwendet werden. Das Paket verpflichtet den Benutzer nicht, NetScaler über einen Cloud-Orchestrator bereitzustellen. Das Gerätepaket ist nur mit APIC und APIC mit Cloud Orchestrator kompatibel.

Verwalten der Kubernetes Ingress-Konfiguration in NetScaler ADM

February 5, 2024

Kubernetes (K8s) ist eine Open Source-Container-Orchestrierungsplattform, die die Bereitstellung, Skalierung und Verwaltung von Cloud-nativen Anwendungen automatisiert.

Kubernetes bietet die Ingress-Funktion, mit der Clientdatenverkehr außerhalb des Clusters auf Microservices einer Anwendung zugreifen kann, die innerhalb des Kubernetes-Clusters ausgeführt wird. ADC-Instanzen können als Ingress zu Anwendungen dienen, die in einem Kubernetes-Cluster ausgeführt werden. ADC-Instanzen können den Lastenausgleich durchführen und den Nord-Süd-Datenverkehr von den Clients zu allen Microservices innerhalb des Kubernetes-Clusters weiterleiten.

> **Hinweis**
>
> - NetScaler ADM unterstützt die Ingress-Funktion auf den Clustern mit Kubernetes Version 1.14—1.21.
> - NetScaler ADM unterstützt NetScaler VPX- und MPX-Appliances als Ingress-Geräte.
> - In der Kubernetes-Umgebung gleicht die NetScaler-Instanzlast nur den Diensttyp “Node-Port”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 basierend auf der Ingress-Richtlinie verschiedenen Anwendungen zuweisen.

Sie können eine Ingress-Konfiguration mit Kubernetes `kubectl` oder APIs erstellen und bereitstellen. Sie können auch einen Ingress von NetScaler ADM aus konfigurieren und bereitstellen.

Sie können die folgenden Aspekte der Kubernetes-Integration in ADM angeben:

- **Cluster** —Sie können Kubernetes-Cluster registrieren oder deren Registrierung aufheben, für die ADM Ingress-Konfigurationen bereitstellen kann. Wenn Sie einen Cluster in NetScaler ADM registrieren, geben Sie die Kubernetes-API-Serverinformationen an. Wählen Sie dann einen

ADM-Agenten 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 die Cluster-, Site- und Instanzinformationen an, wenn Sie eine Richtlinie hinzufügen.
- **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 angeben (um die SSL-Verarbeitung auf der ADC-Instanz auszulagern) mithilfe geheimer Kubernetes-Ressourcen.

NetScaler ADM ordnet die Ingress-Konfigurationen mithilfe von Ingress-Richtlinien automatisch ADC-Instanzen zu.

Für jede erfolgreiche Ingress-Konfiguration generiert NetScaler 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 NetScaler-Instanzen als Ingress-Geräte in Kubernetes-Clustern zu verwenden, stellen Sie sicher, dass Sie Folgendes haben:

- Kubernetes Cluster an Ort und Stelle.
- Kubernetes-Cluster in NetScaler ADM registriert.

Konfigurieren Sie NetScaler ADM mit einem geheimen Token für die Verwaltung eines Kubernetes-Clusters

Damit NetScaler ADM Ereignisse von Kubernetes empfangen kann, müssen Sie ein Dienstkonto in Kubernetes für NetScaler ADM erstellen. Konfigurieren Sie das Dienstkonto mit den erforderlichen RBAC-Berechtigungen im Cluster.

1. Erstellen Sie ein Dienstkonto für NetScaler ADM. Beispielsweise kann der Name des Dienstkontos sein`citrixadm-sa`. Informationen zum Erstellen eines Dienstkontos finden Sie unter Verwenden mehrerer Dienstkonten.
2. Verwenden Sie die`cluster-admin` Rolle, um das NetScaler ADM Dienstkonto zu binden. Diese Bindung gewährt einem Dienstkonto eine clusterübergreifende `ClusterRole`. 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 NetScaler ADM Dienstkonto an die`cluster-admin` Rolle gebunden wurde, verfügt das Dienstkonto über den clusterweiten Zugriff. Weitere Informationen finden Sie unter `kubectl` create `clusterrolebinding`.

3. Beziehen Sie das Token aus dem erstellten Dienstkonto.

   Führen Sie beispielsweise den folgenden Befehl aus, um das Token für das Dienstkonto `citrixadm-sa` anzuzeigen:

```
kubectl describe sa citrixadm-sa
<!--NeedCopy-->
```

4. Führen Sie den folgenden Befehl aus, um die geheime Zeichenfolge des Tokens abzurufen:

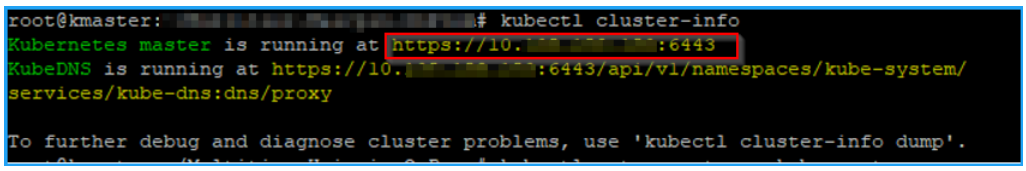
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

Fügen Sie den Kubernetes-Cluster in NetScaler ADM hinzu

Nachdem Sie einen NetScaler ADM Agent konfiguriert und statische Routen konfiguriert haben, müssen Sie den Kubernetes-Cluster in NetScaler ADM registrieren.

So registrieren Sie den Kubernetes-Cluster:

1. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler 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-Hauptknoten abrufen.
      i. Führen Sie auf dem Hauptknoten von Kubernetes den Befehl `kubectl cluster-info` aus.



ii. Geben Sie die URL ein, die für **Kubernetes master is running at** angezeigt wird.

c) **Authentifizierungstoken** —Geben Sie die Authentifizierungstoken-Zeichenfolge an , die Sie erhalten, während Sie NetScaler ADM für die Verwaltung eines Kubernetes Das Authentifizierungstoken ist erforderlich, um den Zugriff für die Kommunikation zwischen dem Kubernetes-Cluster und NetScaler ADM zu überprüfen. So generieren Sie ein Authentifizierungstoken:

i. Führen Sie auf dem Hauptknoten von Kubernetes die folgenden Befehle aus:

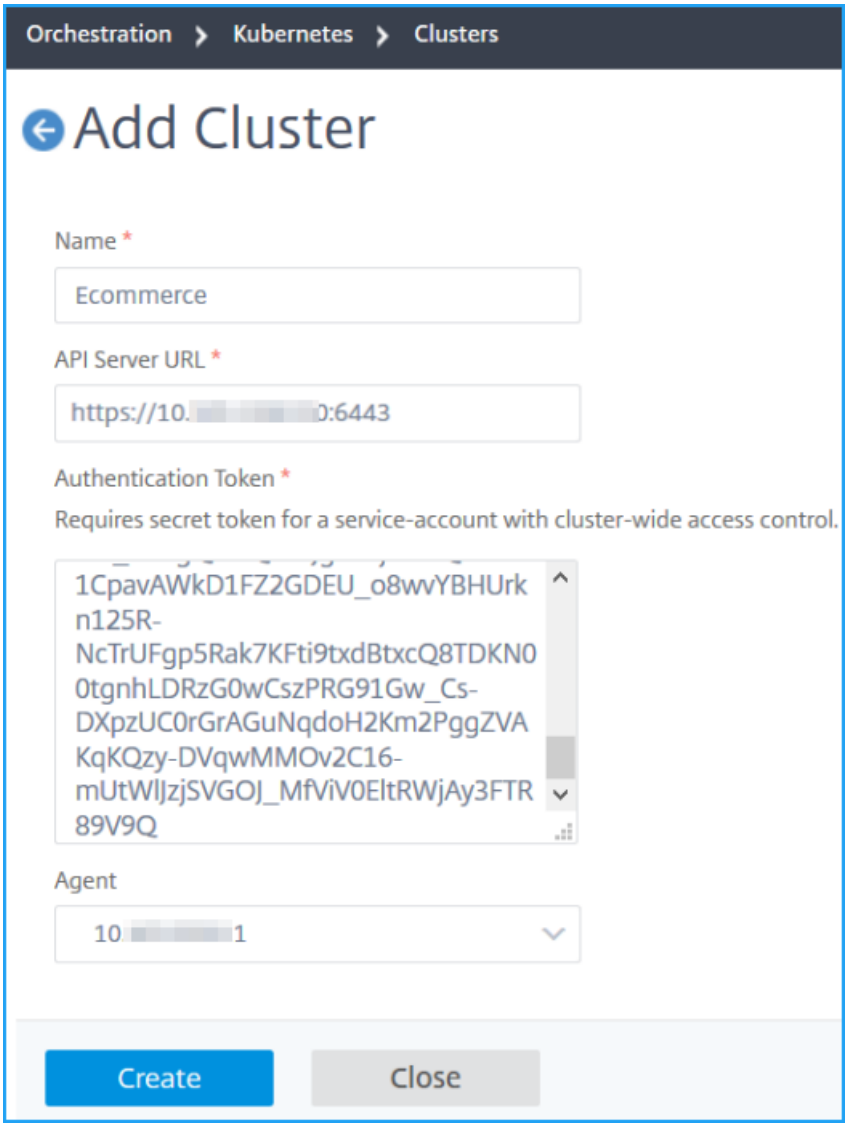
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

ii. Kopieren Sie das generierte Token und fügen Sie es als Authentifizierungstoken ein

Weitere Informationen finden Sie in der Kubernetes-Dokumentation.

d) Wählen Sie den Agent aus der Liste aus.

e) Klicken Sie auf **Erstellen**.



Definieren einer Ingress-Richtlinie

Die Ingress-Richtlinie entscheidet, welcher NetScaler zum Bereitstellen einer Ingress-Konfiguration verwendet wird, basierend auf dem Ingress-Cluster oder Namespace.

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** für die Bereitstellung der Ingress-Konfiguration auf einem Kubernetes-Cluster. Diese Bedingungen basieren normalerweise auf Ingress-Cluster und Namespace.

c) Im Infrastruktur-Panel

- **Standort** —Wählen Sie eine Website aus der Liste aus.
- **Instanz** —Wählen Sie die ADC-Instanz aus der Liste aus.

Die **Site** - und **Instanz-Listen** füllen die Optionen basierend auf der Cluster-Auswahl im Bereich "**Bedingungen** "auf.

In diesen Listen werden die Sites oder Instanzen angezeigt, die mit dem NetScaler 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 in **Infrastruktur > IPAM**erstellten Netzwerke angezeigt.

e) Klicken Sie auf **Erstellen**.

Stellen Sie die Ingress-Konfiguration bereit

Sie können die Ingress-Konfiguration über Kubernetes mithilfe der `kubectl`Kubernetes-API oder anderer Tools bereitstellen. Sie können die Ingress-Konfiguration auch direkt von NetScaler ADM aus bereitstellen.

1. Navigieren Sie zu **Orchestration > 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 in **Cluster**den Kubernetes-Cluster aus, auf dem Sie einen Ingress bereitstellen möchten.

   c) Wählen Sie den **Cluster-Namespace** aus der Liste aus. In diesem Feld werden die Namespaces aufgeführt, die im angegebenen Kubernetes-Cluster vorhanden sind.

   d) Wählen Sie optional **Frontend-IP-Adresse automatisch zuweisen**.

   e) Wählen Sie **in der Liste Ingress Protocol** aus. Wenn Sie **HTTPS**auswählen, geben Sie den **TLS-Schlüssel an**.

   Dieses Geheimnis bettet die geheime Kubernetes-Ressource ein, die das HTTPS-Zertifikat und den privaten Schlüssel einbettet.

   Ein HTTPS-Ingress erfordert ein TLS-basiertes Secret, das auf dem Kubernetes-Cluster konfiguriert ist. Geben Sie die Felder `tls.crt` und `tls.key` an, um das Serverzertifikat bzw. den Zertifikatsschlüssel aufzunehmen.

f) Geben Sie für das Weiterleiten von Inhalten die folgenden Details an:

- **URL-Pfade** —Geben Sie den Pfad an, der mit dem Kubernetes-Dienst und Port verknüpft ist.
- **Kubernetes-Dienst** —Geben Sie den gewünschten Dienst an.
- **Port** —Geben Sie den Dienst-Port an.
- **LB-Methode** —Wählen Sie die bevorzugte Lastausgleichsmethode für den ausgewählten Kubernetes-Dienst aus.

  Bei der ausgewählten Methode wird die Ingress-Spezifikation mit einer entsprechenden Anmerkung aktualisiert. Wenn Sie beispielsweise die **ROUNDROBIN-Methode** auswählen, wird die Citrix Anmerkung wie folgt angezeigt:

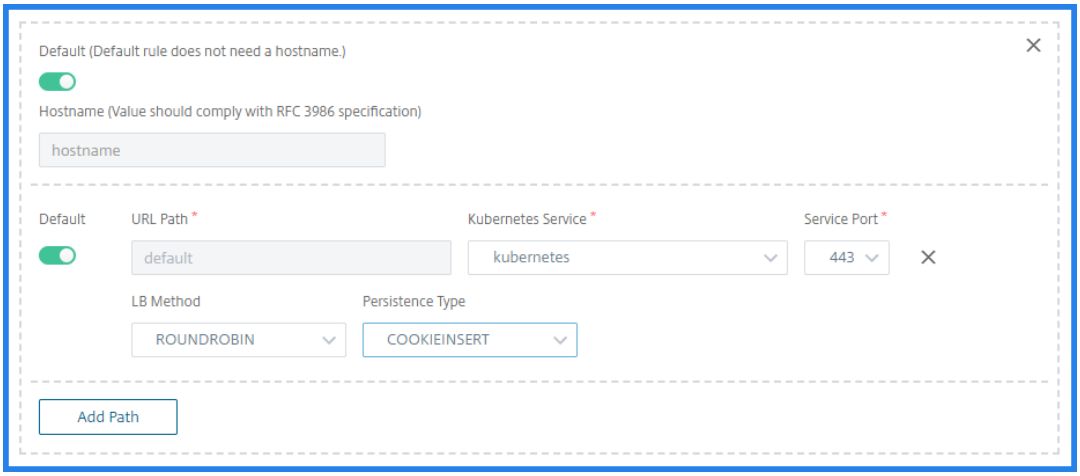
```
1  "lbmethod":"ROUNDROBIN"
2  <!--NeedCopy-->
```

- **Persistenztyp** —Wählen Sie den bevorzugten Persistenztyp für den Lastausgleich 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 Anmerkung 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 Clientdatenverkehr basierend auf den folgenden Angaben zu einem bestimmten Dienst um:

- Der angeforderte URL-Pfad und Port.

- Die definierte LB-Methode und der Persistenztyp.

> **Hinweis:**
>
> Es wird erwartet, dass die in einer Ingress-Konfiguration verwendeten Kubernetes-Dienste vom Typ NodePort sind.

g) Geben Sie optional eine **Ingress-Beschreibung**an.

h) klicken Sie auf **Bereitstellen**.

Wenn Sie die Konfiguration vor der Bereitstellung überprüfen möchten, klicken Sie auf **Ingress-Spezifikation generieren**. Die angegebene Ingress-Konfiguration wird im YAML-Format angezeigt. Nachdem Sie die Konfiguration überprüft haben, klicken Sie auf **Bereitstellen**.

> **Hinweis Wenden Sie**
> Lizenzen auf die virtuellen Server an, die mit Ingress-Konfigurationen erstellt wurden. Führen Sie die folgenden Schritte aus, um die Lizenz anzuwenden:
>
> 1. Gehen Sie zu **Einstellungen > Lizenzierung und Analytics-Konfiguration**.
> 2. Aktivieren Sie unter **Virtueller Server-Lizenzübersicht**die **Option Virtuelle Server automatisch auswählen**.

Video Insight

February 5, 2024

Die Video Insight-Funktion bietet eine einfache und skalierbare Lösung für die Überwachung der Metriken der Videooptimierungstechniken, die von NetScaler Appliances zur Verbesserung der Kundenerfahrung und betrieblichen Effizienz verwendet werden. Sie bietet folgende Vorteile:

- Verwalten Sie das Netzwerk bei Überlastung in Spitzenzeiten.
- Verbessern Sie die Konsistenz der Videowiedergabe und reduzieren Sie Videoverzögerungen
- Aktivieren Sie neue Videodienstangebote (z. B. Binge-on-Videodienste).
- Ermöglichen Sie Kunden die Auswahl der besten nachhaltigen Videoqualität.
- Bieten Sie dem Abonnenten eine konsistente Benutzererfahrung.

Bei der Optimierung des Videoverkehrs verwendet die NetScaler Appliance einen speziellen Mechanismus, um die Videobitrate dynamisch zu beschleunigen, und eine Zufallsabtastung, um die

Einsparungen durch die Optimierungstechnik abzuschätzen. Weitere Informationen zur NetScaler-Videooptimierungsfunktion finden Sie unter Videooptimierung. Wenn Sie die NetScaler-Appliance in NetScaler Application Delivery Management (ADM) integrieren, erfasst sie wichtige Informationen aus den Videodaten, die durch die NetScaler-Appliance fließen. Sie können diese Informationen verwenden, um die optimierte und nicht optimierte Leistung des ABR-Videoverkehrs zu vergleichen, die Einsparungen aufgrund der Optimierung zu ermitteln und so weiter.

> **Hinweis**
>
> Die Statistiken der nicht optimierten Sitzungen in NetScaler ADM entsprechen den Sitzungen, die Sie in der NetScaler Appliance ausgewählt haben. Weitere Informationen zur Zufallsstichprobe finden Sie unterVideooptimierung.

Video Insight in NetScaler ADM stellt Metriken für die folgenden Arten von Videoverkehr bereit:

- Progressiver Download (PD) von Videos über HTTP
- ABR-Videos über HTTP
- ABR-Videos über HTTPS
- YouTube ABR-Videos über QUIC

Video Insight konfigurieren

> **Hinweis**
>
> Video Insight wird auf NetScaler-Instanzen mit NetScaler Premium-Lizenz unterstützt. Die NetScaler Premium-Lizenz wird für NetScaler Telco-Plattformen (VPX T1000 und VPX-T) unterstützt.

Um Video Insight auf einer NetScaler-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 NetScaler ADM-Servers angeben, auf dem Sie die Berichte überwachen möchten.

Um Videoinformationen für eine NetScaler-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`

enable feature AppFlow

Beispiel

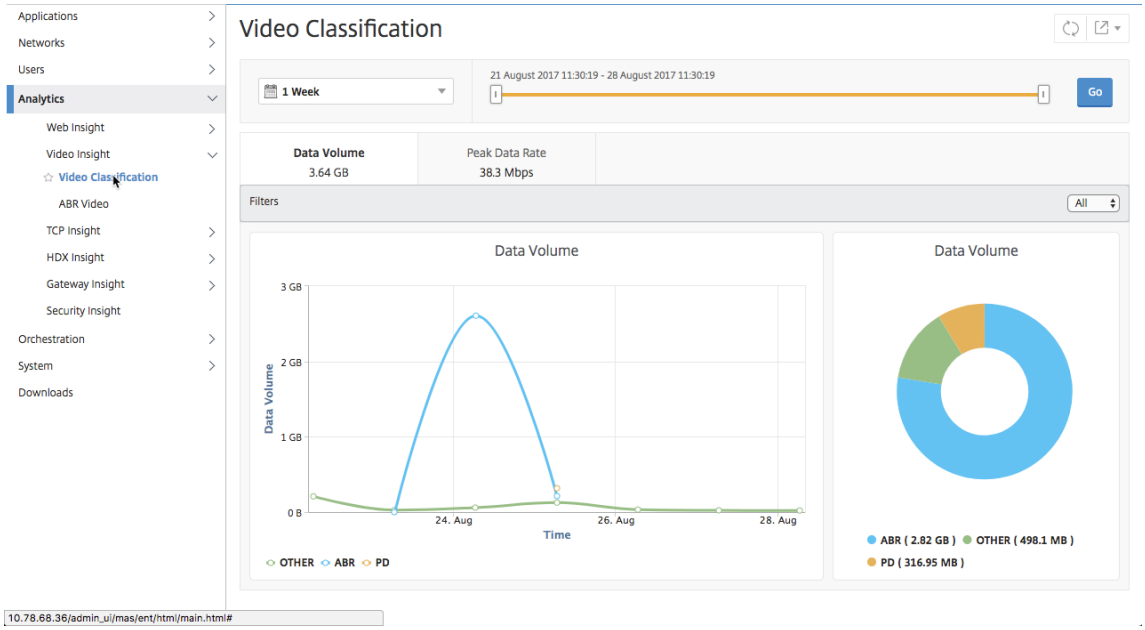
```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
   Transport logstream
set appflow param -videoInsight ENABLED
add appflow action act1 -collectors col1 -videoAnalytics ENABLED
add appflow policy appol true act1
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
<!--NeedCopy-->
```

Anzeigen der Video Insight-Metriken in NetScaler ADM

Nachdem Sie Video Insight in NetScaler 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.

So sehen Sie sich die Video Insight-Metriken in NetScaler ADM an:

1. Geben Sie in einem Webbrowser die IP-Adresse der virtuellen NetScaler 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 > Video Insight**.



> **Hinweis**
>
> Die von der Legende **OTHER** in den Diagrammen bereitgestellten Werte 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.

Netzwerkeffizienz anzeigen

February 5, 2024

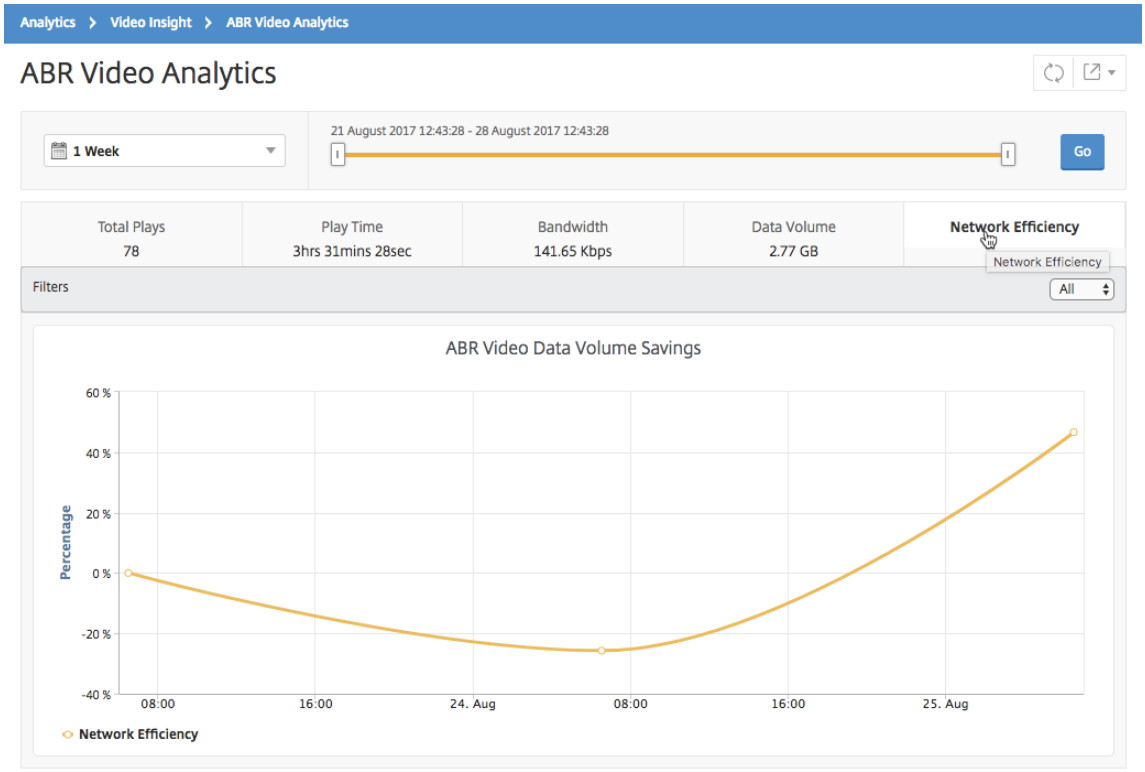
Für einen bestimmten Zeitraum stellt NetScaler Application Delivery Management (ADM) ein Diagramm bereit, das das Verhältnis von optimierten zu nicht optimierten Videositzungen im Zeitrahmen zeigt. Es zeigt auch den Prozentsatz der durch die Optimierung eingesparten Bandbreite an. Der Prozentsatz der eingesparten 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 eingesparten Bandbreite:

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**.



Datenvolumen von optimierten und nicht optimierten ABR-Videos vergleichen

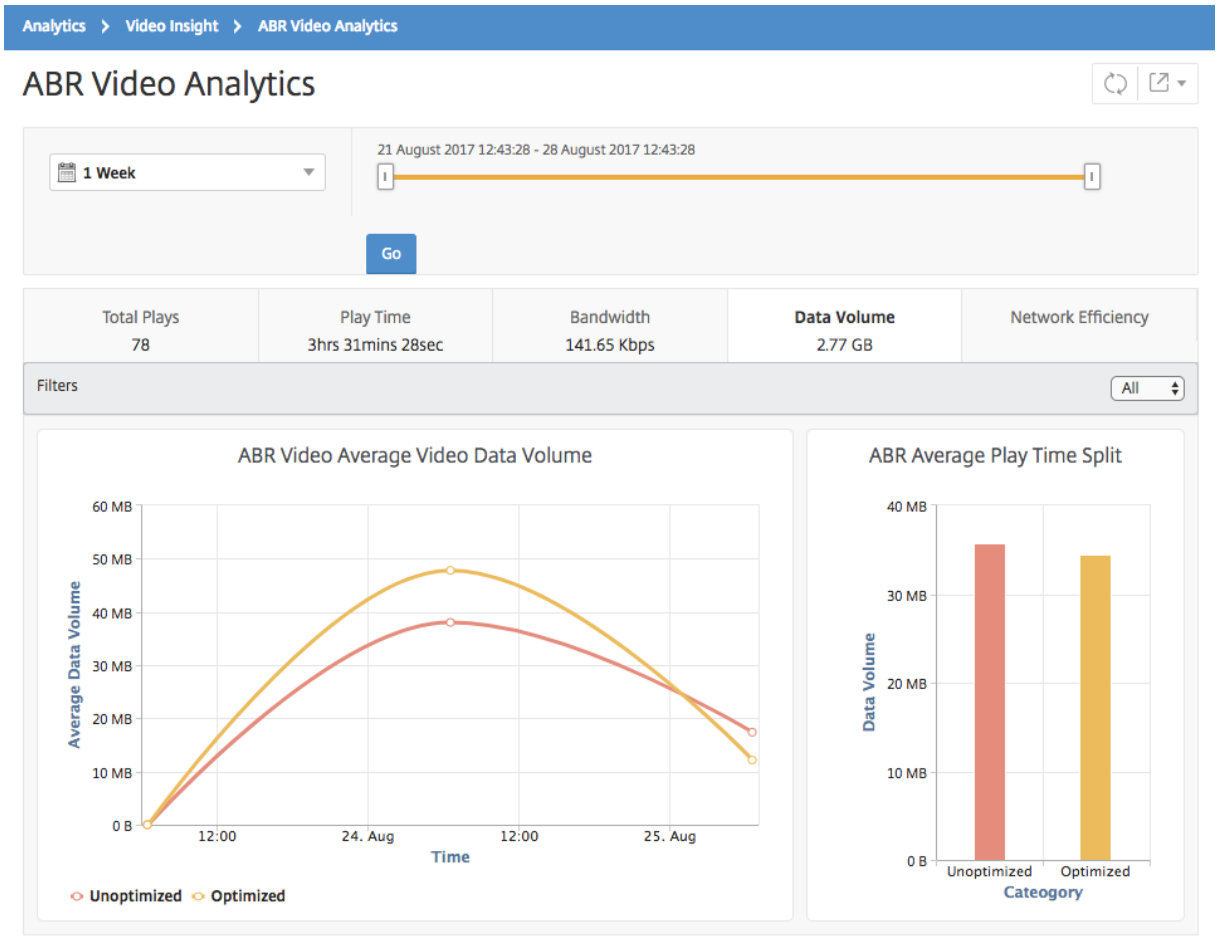
February 5, 2024

Für einen bestimmten Zeitraum zeigt NetScaler Application Delivery Management (ADM) das Datenvolumen an, das von optimierten und nicht optimierten ABR-Videos verwendet wird, sodass Sie die beiden Volumes vergleichen können.

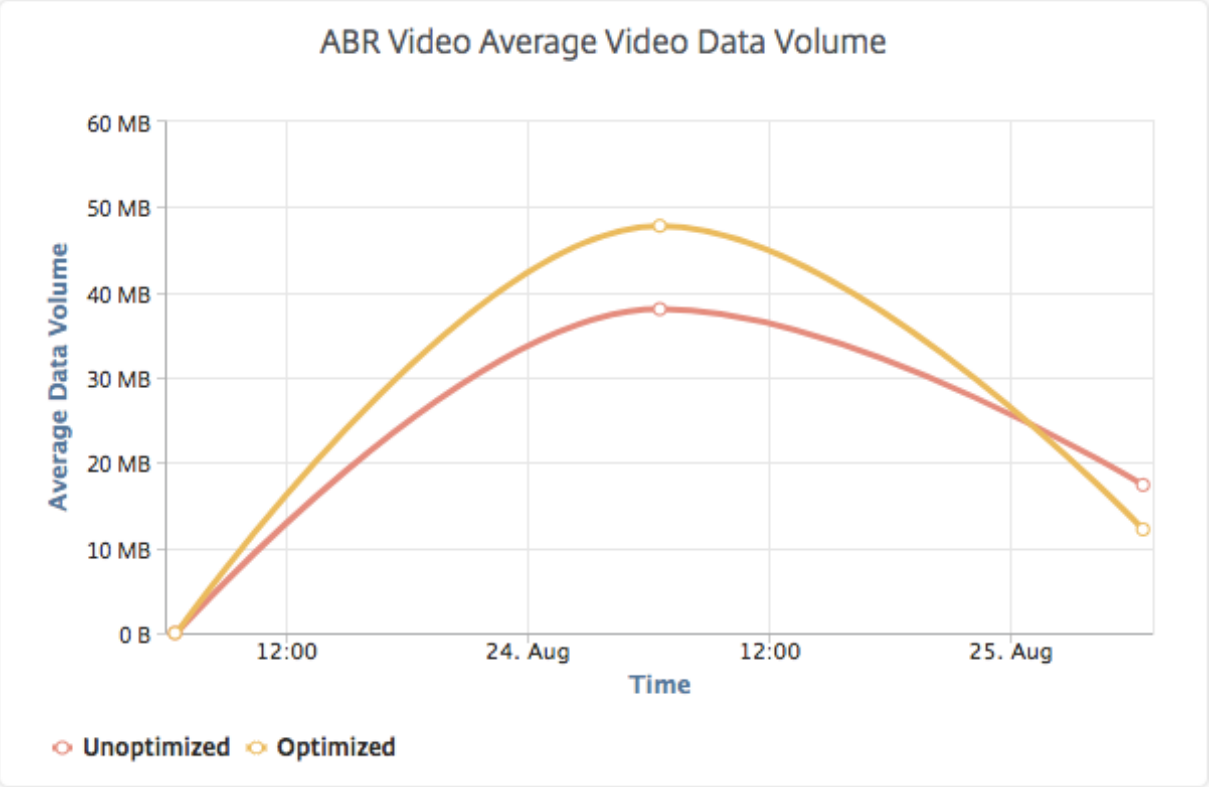
Um das von ABR-Videos verwendete Datenvolumen zu sehen:

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:



Typs der gestreamten Videos und des vom Netzwerk verbrauchten Datenvolumens anzegien

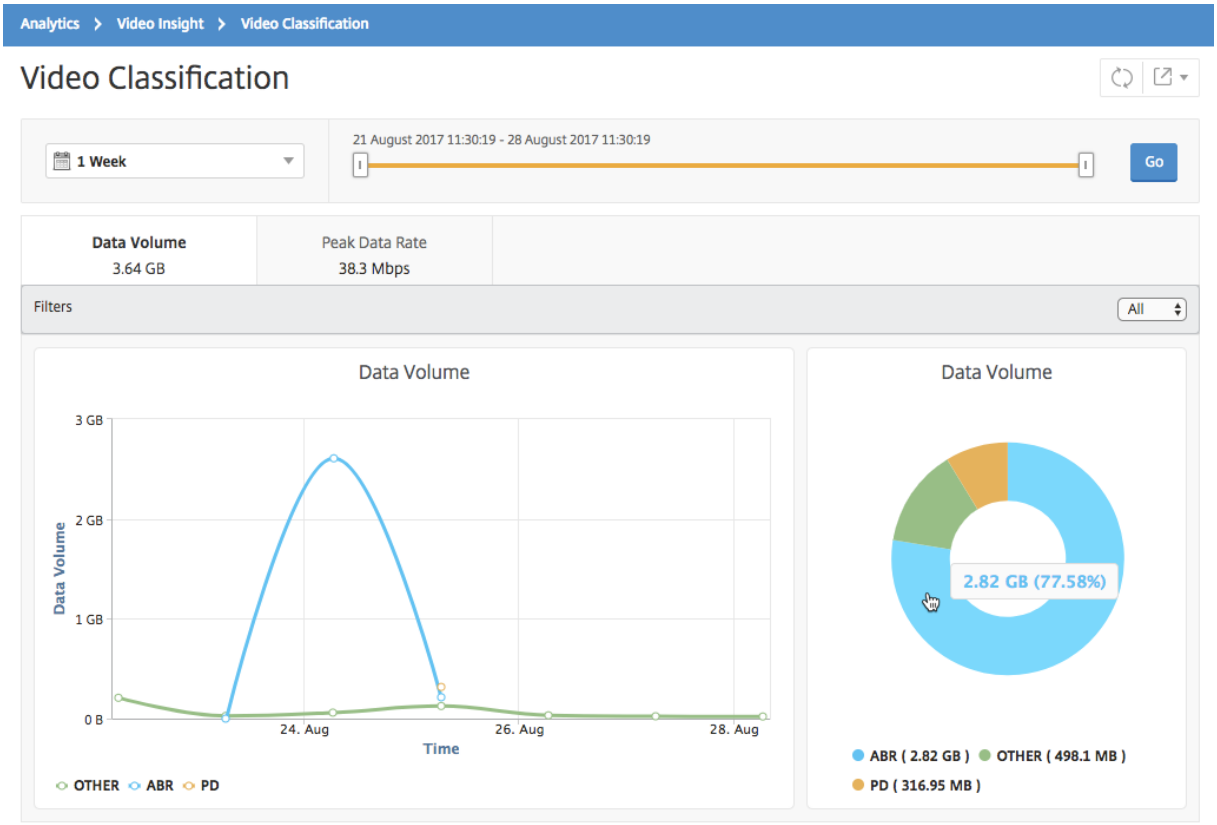
February 5, 2024

Die NetScaler Appliance erkennt den verschlüsselten oder unverschlüsselten Videoverkehr in Ihrem Netzwerk und die Art des Videostreamings (PD oder ABR). NetScaler Application Delivery Management (ADM) zeigt diese Metriken und das vom Video-Traffic verbrauchte Datenvolumen für einen definierten Zeitraum an.

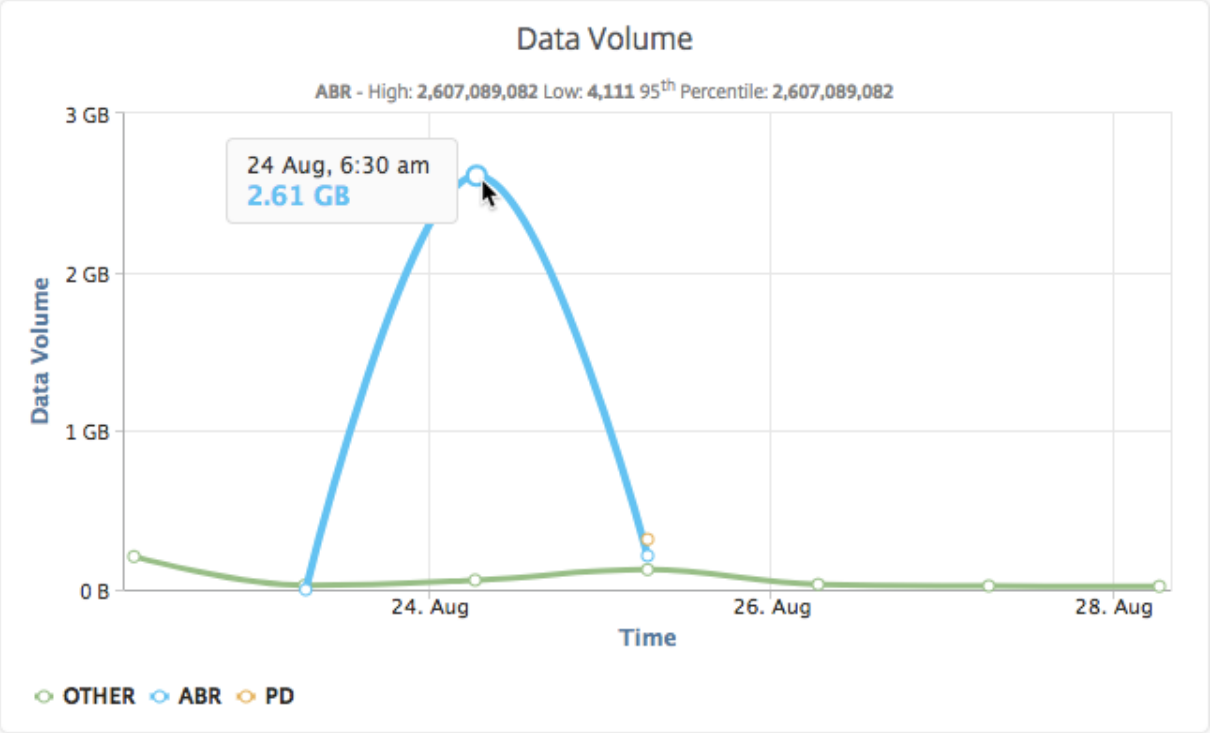
So sehen Sie die Arten von Videos und das verbrauchte Datenvolumen:

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**.

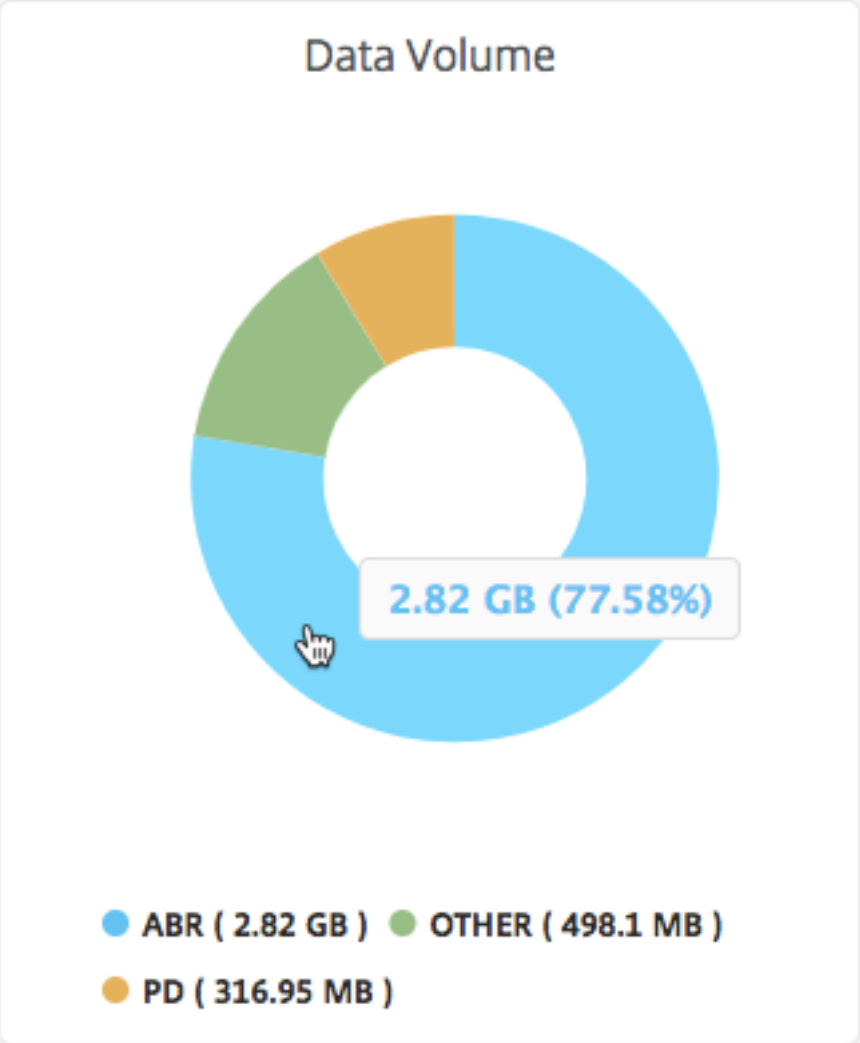
Sie können die Liste **Filter** verwenden, um den HTTP-, HTTPS- oder QUIC-Datenverkehr auszuwählen.



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.



Optimierte und nicht optimierte Wiedergabezeit von ABR-Videos vergleichen

February 5, 2024

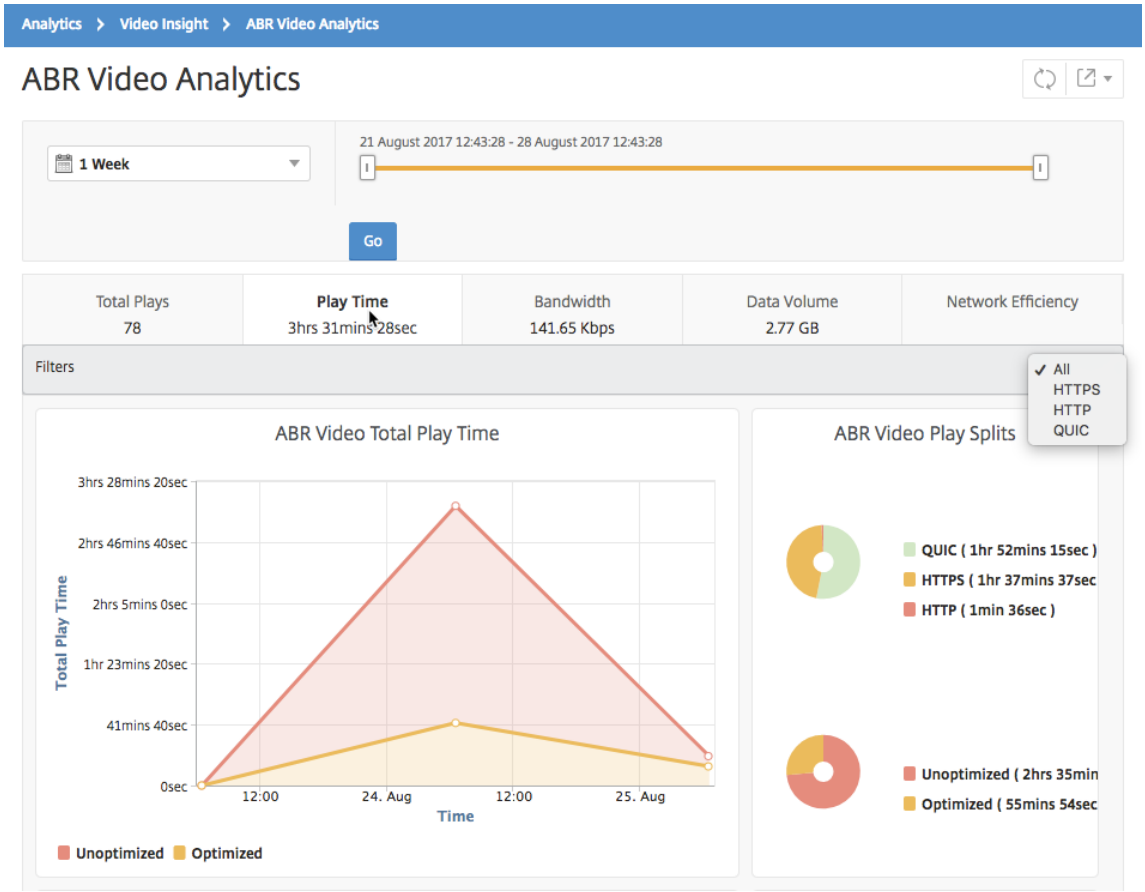
Für einen bestimmten Zeitraum liefert NetScaler Application Delivery Management (ADM) die Wiedergabezeit von ABR-Videos und ermöglicht es Ihnen auch, die Wiedergabezeit optimierter und nicht optimierter ABR-Videos in Ihrem Netzwerk zu vergleichen.

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.

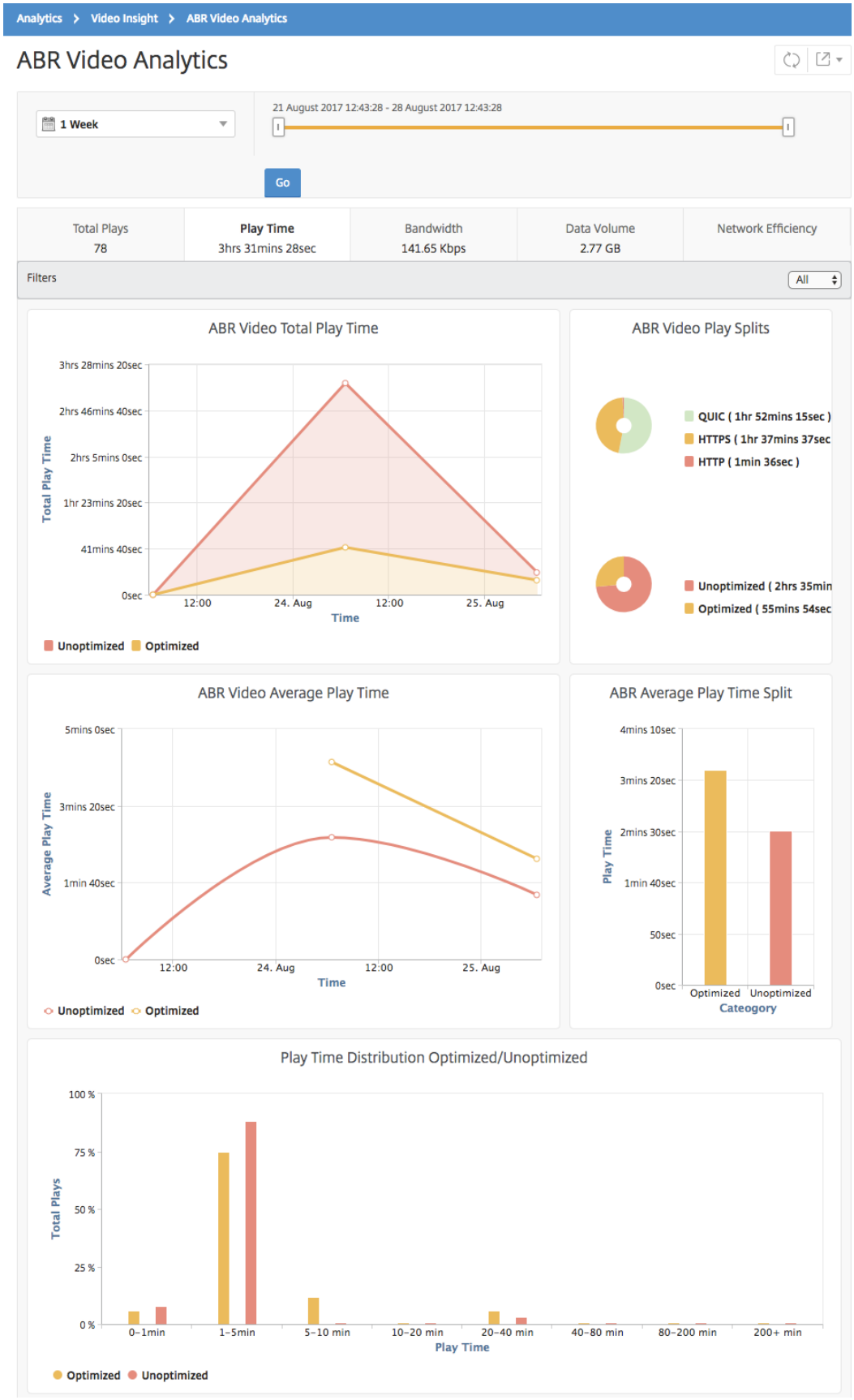
3. Klicken Sie auf **Los** und wählen Sie die Registerkarte **Wiedergabezeit** aus.

   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
- Gesamtwiedergabezeit optimierter und nicht optimierter Wiedergaben von ABR-Videos aus Ihrem Netzwerk für den ausgewählten Zeitraum
- Gesamtspielzeit von verschlüsselten und unverschlüsselten ABR-Videos
- Durchschnittliche Wiedergabezeit von ABR-Videos
- Durchschnittliche Wiedergabezeit optimierter und nicht optimierter Wiedergaben von ABR-Videos
- Durchschnittliche Wiedergabezeit von verschlüsselten und unverschlüsselten ABR-Videos
- Wiedergabe der Zeitverteilung zwischen optimierten und nicht optimierten ABR-Videos



Bandbreitenverbrauch optimierter und nicht optimierter ABR-Videos vergleichen

February 5, 2024

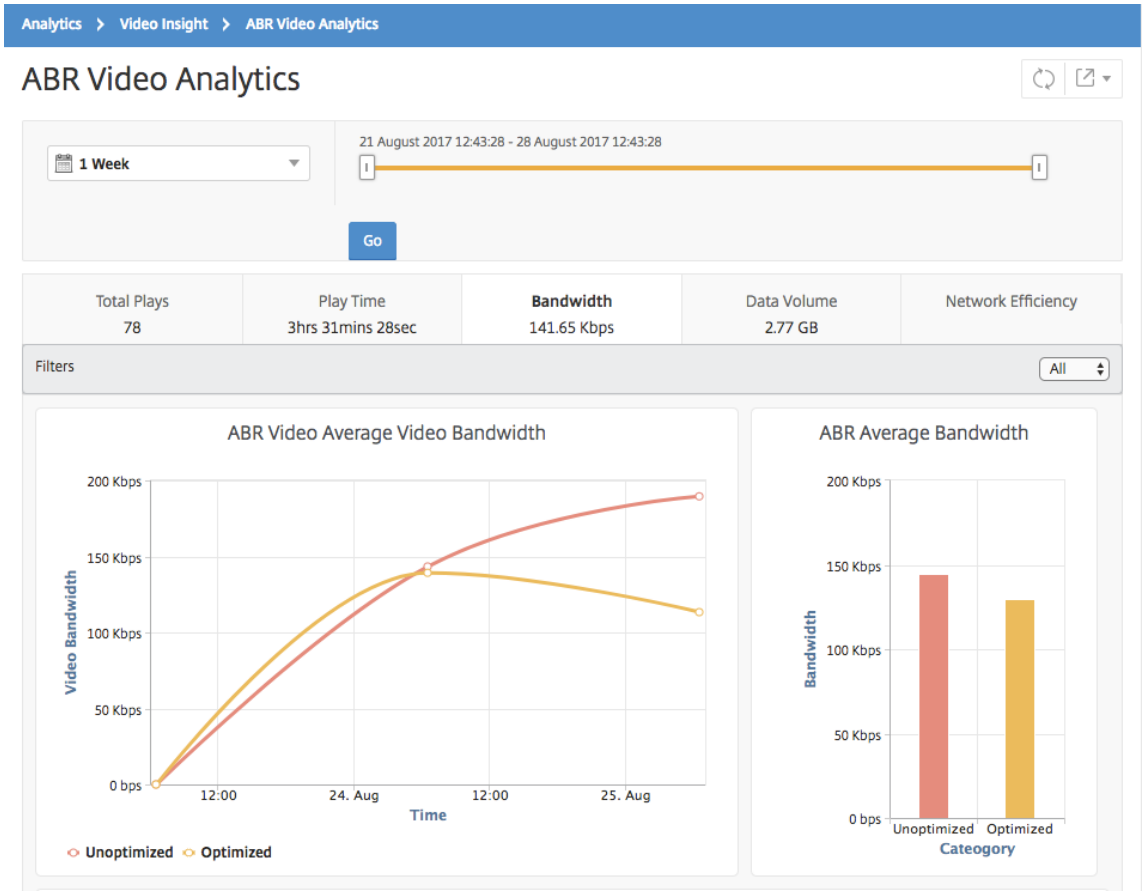
Für einen bestimmten Zeitraum stellt NetScaler Application Delivery Management (ADM) die Bandbreite bereit, die von optimierten und nicht optimierten ABR-Videos verbraucht wird. Außerdem können Sie die Bandbreite vergleichen, die von optimierten und nicht optimierten ABR-Videos in Ihrem Netzwerk verbraucht wird, basierend auf:

- Spielzeit
- Datenvolume

Um den Bandbreitenverbrauch anzuzeigen:

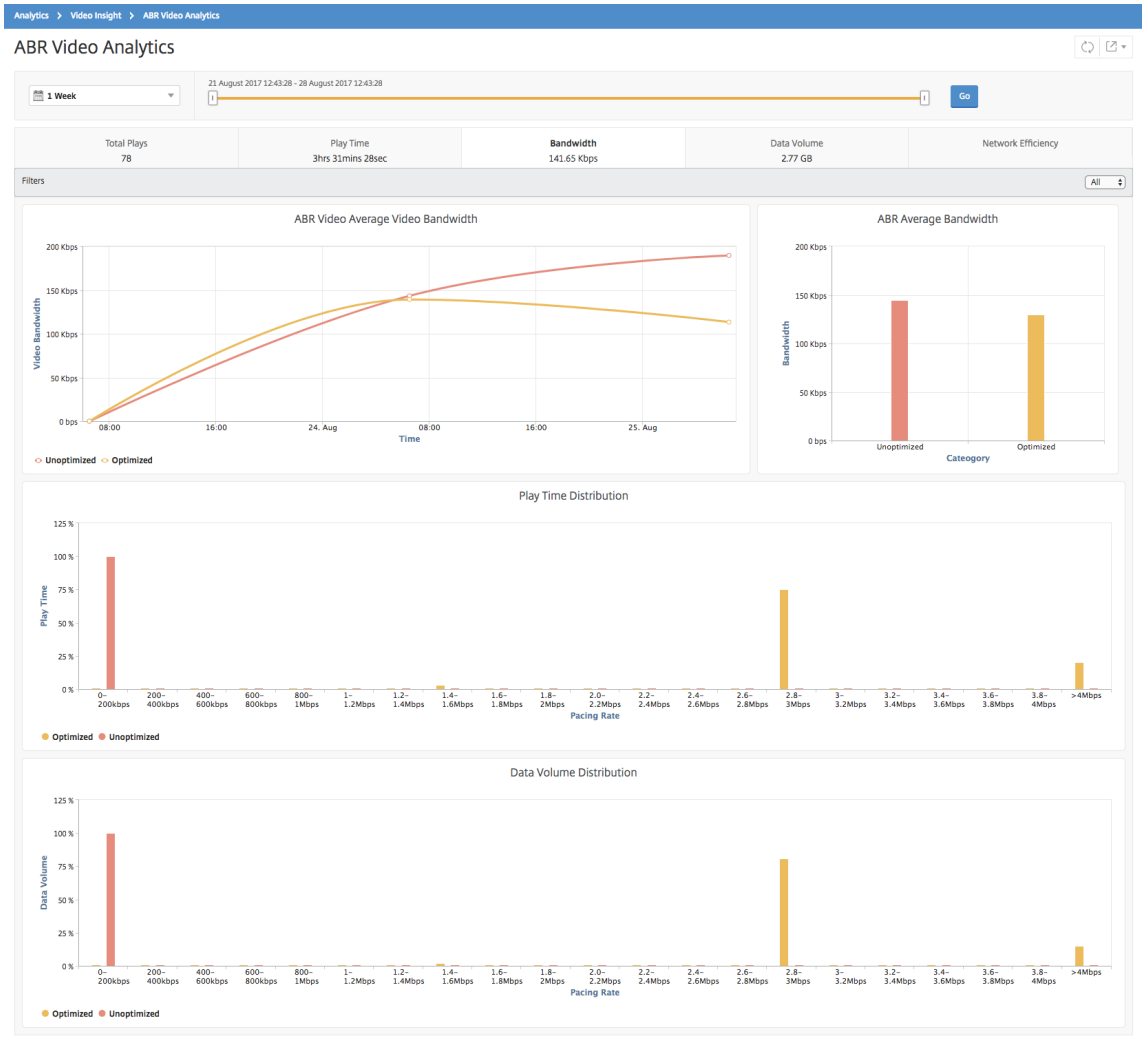
1. Navigieren Sie zu **Analytics > Video Insight** und klicken Sie auf **ABR Video Analytics**.
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.
3. Klicken Sie auf **Los** und wählen Sie die Registerkarte **Bandbreite** aus.

   Sie können die HTTP-, HTTPS- oder QUIC-ABR-Videos in der Liste **Filter** auswählen.



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.
- Die verbrauchte Bandbreite basiert auf der Verteilung der Wiedergabezeit zwischen optimierten und nicht optimierten ABR-Videos.
- Bandbreitenverbrauch basierend auf dem Datenvolumen, das zwischen optimierten und nicht optimierten ABR-Videos verteilt wird.



Optimierte und nicht optimierte Wiedergabezahlen von ABR-Videos vergleichen

February 5, 2024

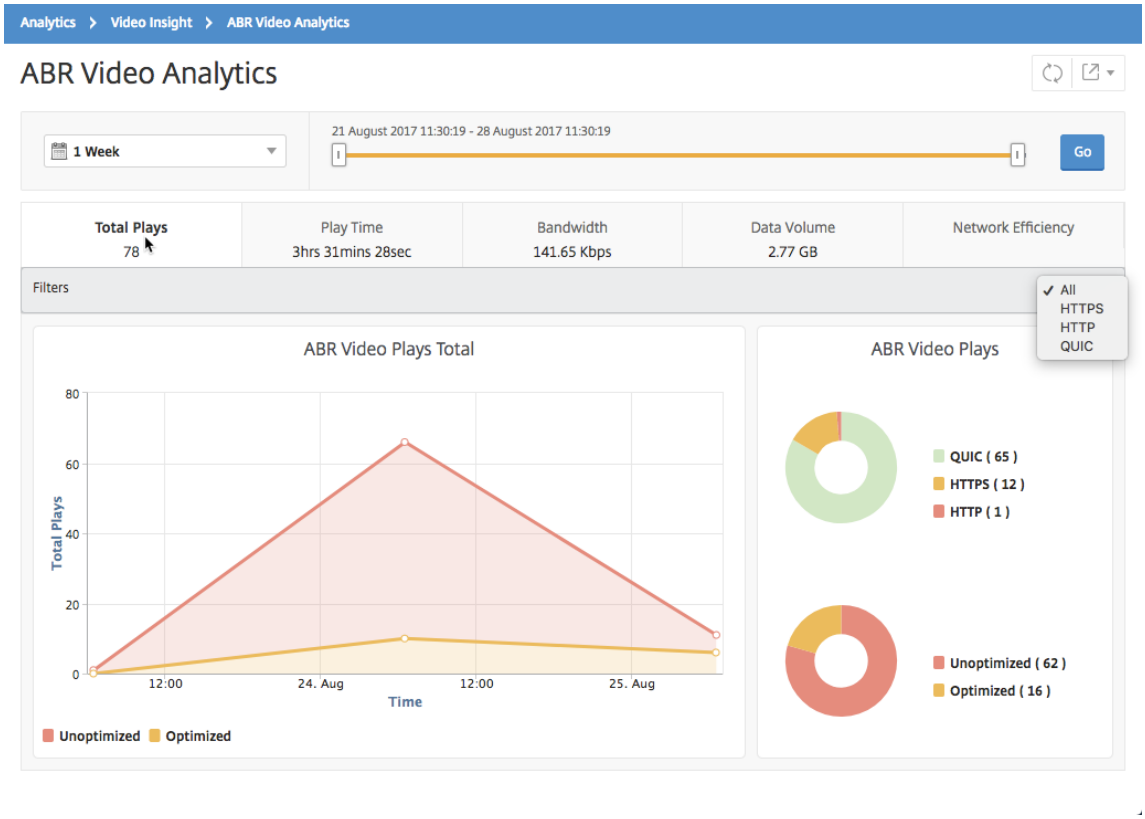
Für einen bestimmten Zeitraum zeigt NetScaler Application Delivery Management (ADM) die Anzahl der Abspielungen von ABR-Videos an und ermöglicht es Ihnen, die Anzahl der optimierten und unoptimierten Abspielungen in Ihrem Netzwerk zu vergleichen.

Um die Anzahl der Spiele zu sehen:

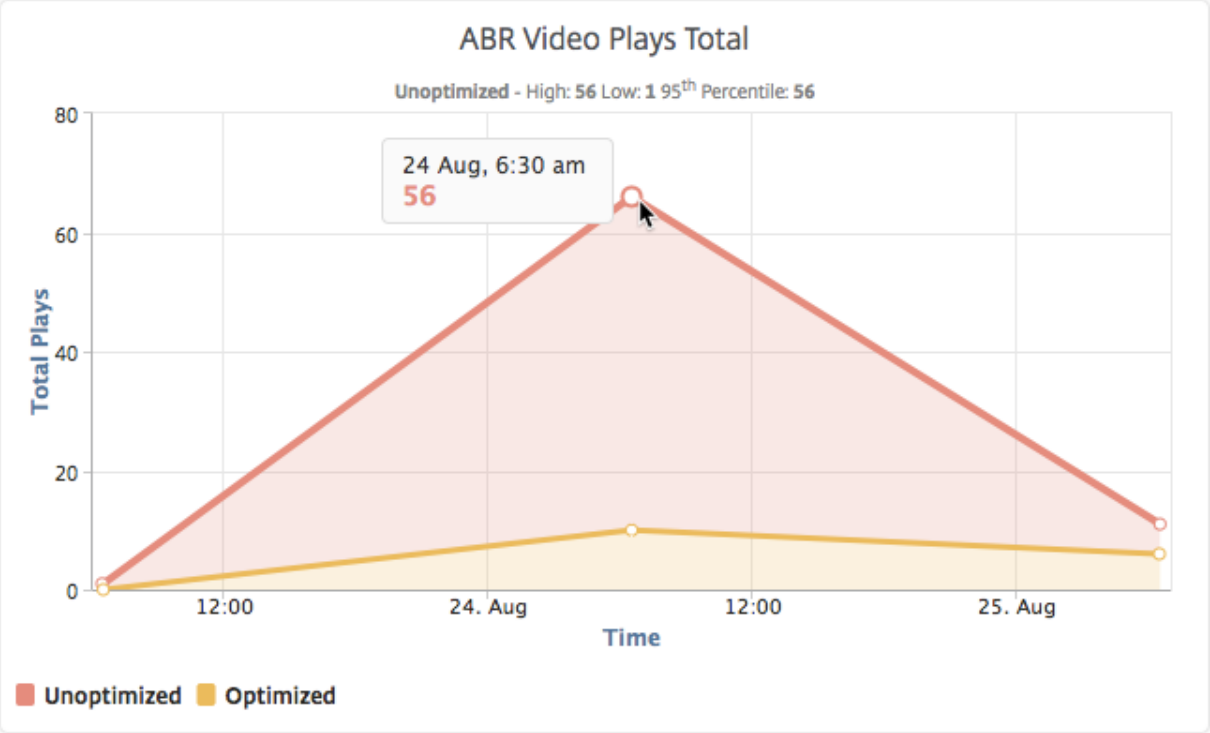
1. Navigieren Sie zu **Analytics > Video Insight**und klicken Sie auf **ABR Video Analytics**.
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.

3. Klicken Sie auf **Los** und wählen Sie die Registerkarte **Anzahl der Wiedergaben**.

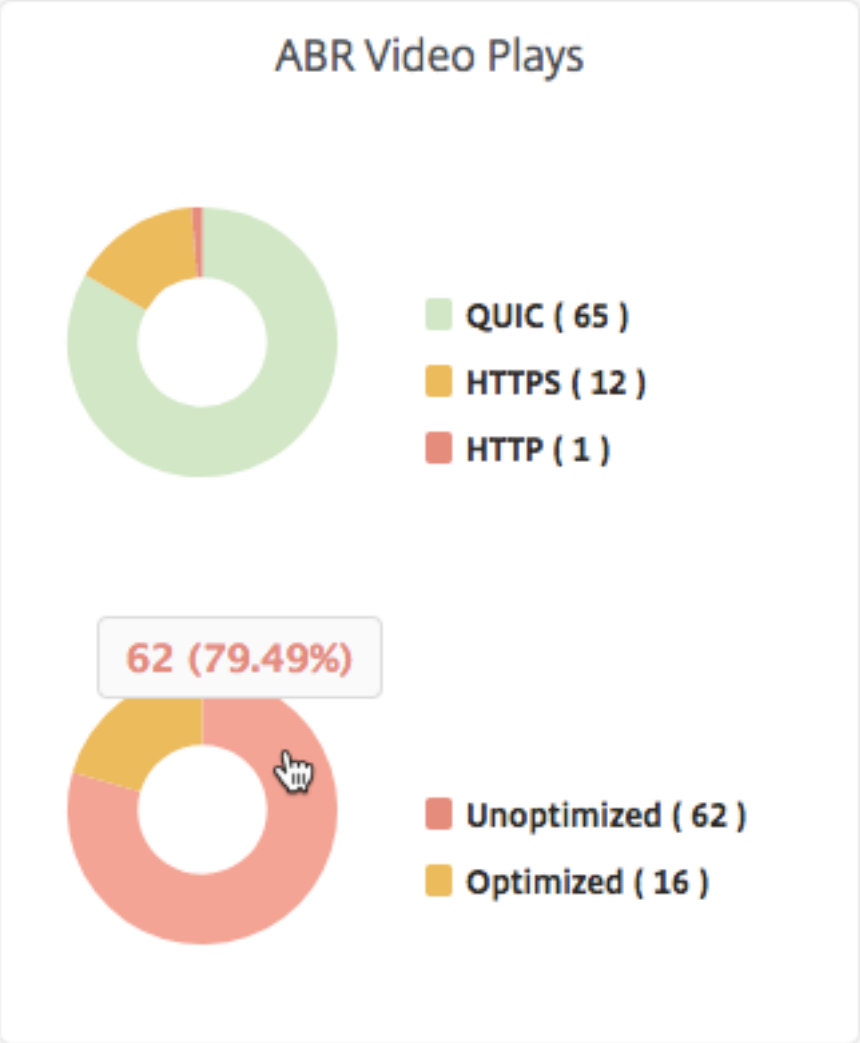
   Sie können die Liste **Filter** verwenden, um die HTTP-, HTTPS- oder QUIC-ABR-Videos auszuwählen.



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.



Spitzendatenrate für einen bestimmten Zeitraum anzeigen

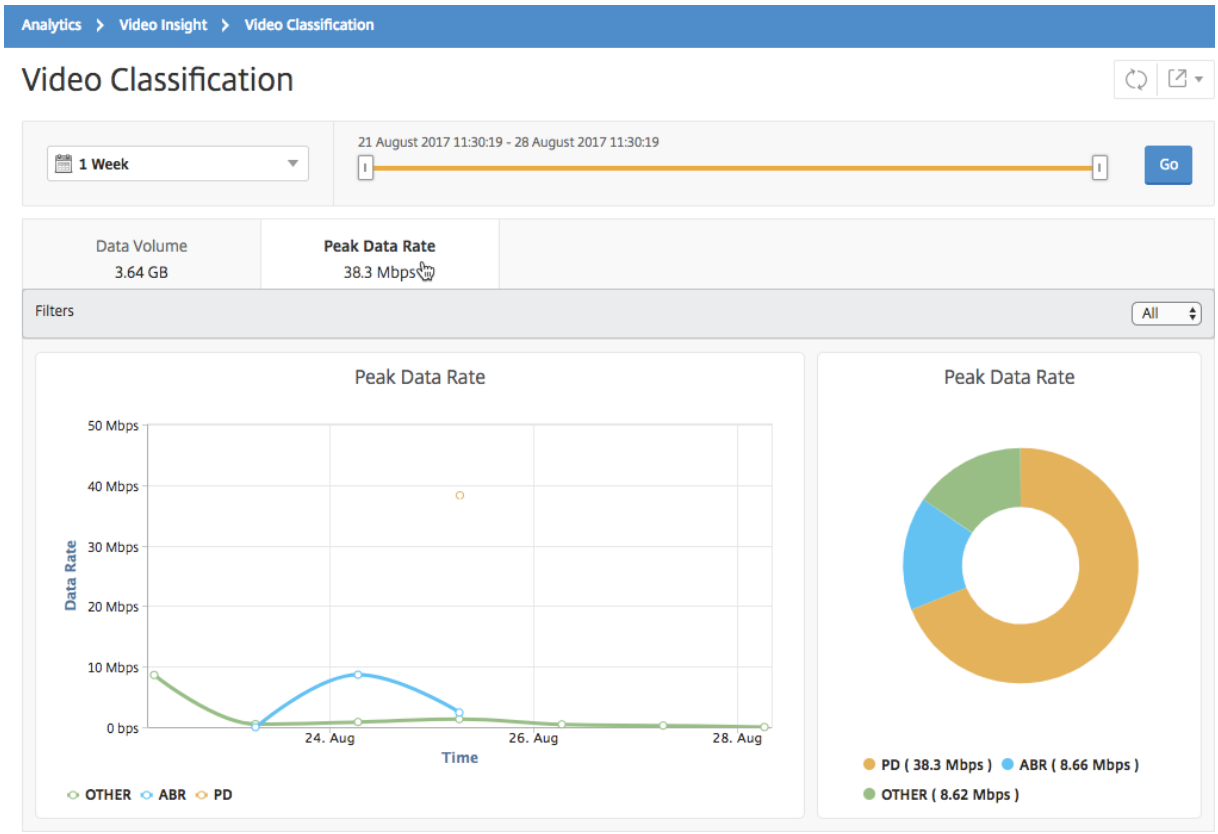
February 5, 2024

NetScaler Application Delivery Management (ADM) zeigt Ihnen den Spitzendurchsatz oder die maximale Datenrate des Videoverkehrs in Ihrem Netzwerk.

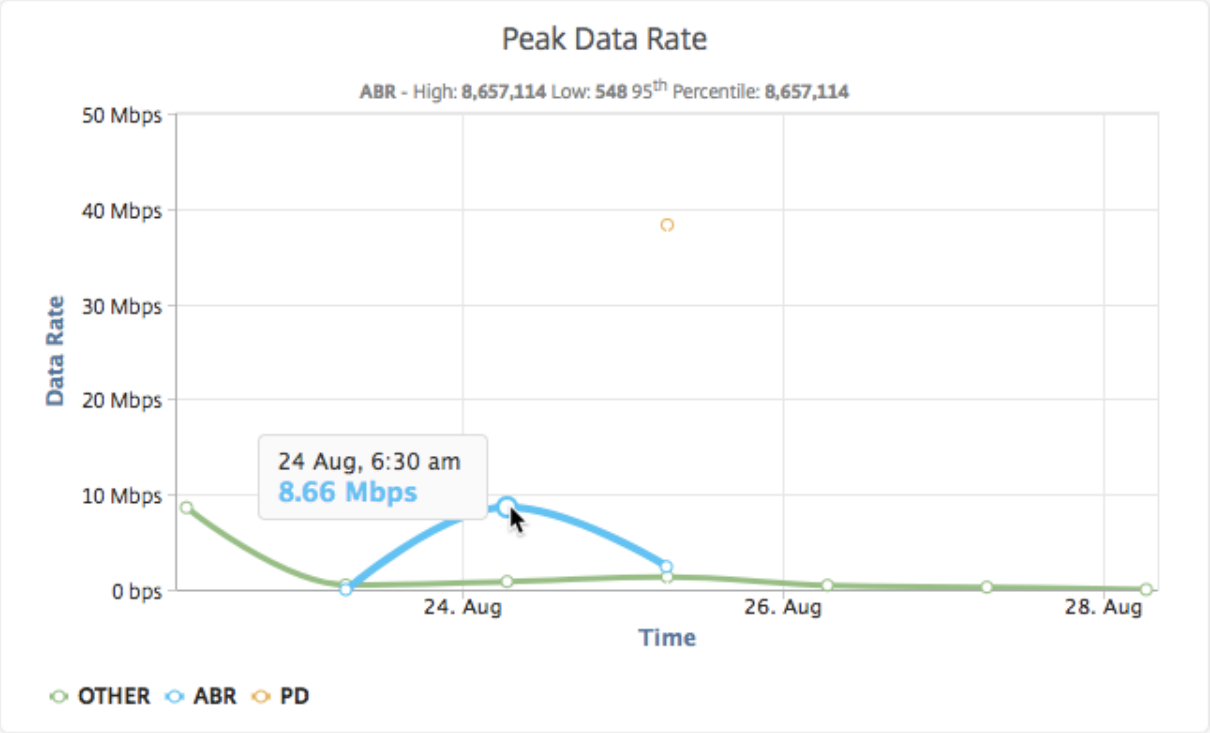
So sehen Sie die Spitzendatenrate des Videoverkehrs:

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.

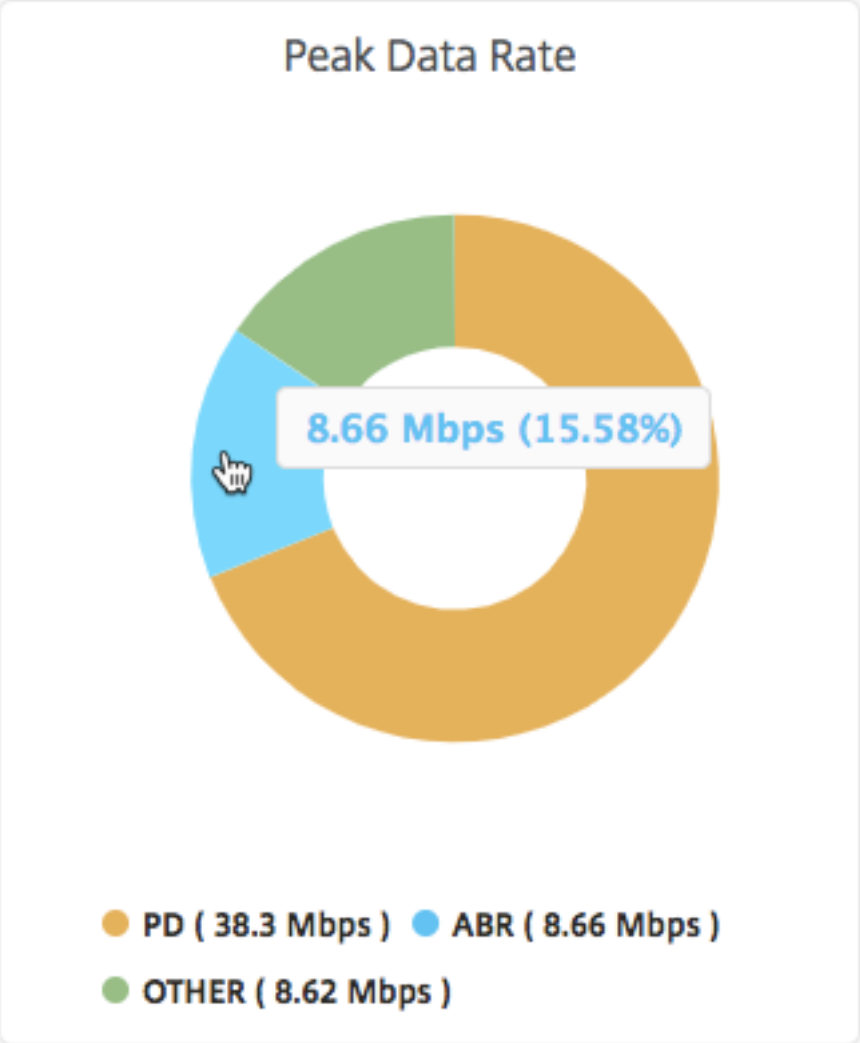
Sie können die Liste **Filter** verwenden, um den HTTP-, HTTPS- oder QUIC-Datenverkehr auszuwählen.



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.



Konfigurieren der IP-Adressverwaltung (IPAM)

February 5, 2024

NetScaler ADM IPAM ermöglicht Ihnen die automatische Zuweisung und Freigabe von IP-Adressen in von NetScaler ADM verwalteten Konfigurationen. Sie können IPs aus Netzwerken oder IP-Bereichen zuweisen, die mit den folgenden IP-Anbietern definiert wurden:

- Integrierter NetScaler ADM-IPAM-Anbieter.
- Infoblox IPAM-Lösung.

Sie können NetScaler ADM IPAM verwenden in:

- **StyleBooks**: Weisen Sie virtuelle Server automatisch IPs zu, wenn Sie Konfigurationen erstellen.

- **API-Gateway**: Weisen Sie dem API-Proxy automatisch eine IP-Adresse zu.

Sie können auch die IP-Adressen in jedem Netzwerk oder den von NetScaler ADM verwalteten IP-Bereich verfolgen.

Einen externen IP-Adressanbieter hinzufügen

NetScaler ADM verfügt über einen integrierten IPAM-Anbieter zur Verwaltung von IPs und IP-Bereichen. Sie können auch einen externen IP-Adressanbieter für NetScaler ADM verwenden.

> **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.
> - 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 aus, um eine externe IPAM-Anbieterlösung in NetScaler ADM hinzuzufügen:

1. Navigieren Sie zu **Einstellungen > IPAM**.
2. Klicken Sie unter **Anbieter**auf **Hinzufügen**.
3. Geben Sie die folgenden Details an, um einen IPAM-Anbieter hinzuzufügen:
    - **Name** - Geben Sie den IP-Providernamen an, der in NetScaler 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 NetScaler 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**.

Infoblox DDI als externer Anbieter

Derzeit unterstützt NetScaler ADM Infoblox DDI als externen Anbieter.

Sie können NetScaler ADM IPAM mit dem Infoblox-Anbieter verwenden, um die folgenden Aktionen auszuführen:

- IPAM-Netzwerke auflisten
- IPAM-Netzwerke erstellen, aktualisieren und löschen
- Reservieren und Freigeben einer IP-Adresse aus IPAM-Netzwerken

Erstellen Sie ein IPAM-Netzwerk Um ein NetScaler ADM IPAM-Netzwerk mithilfe des Infoblox-Anbieters zu erstellen, muss auf Infoblox ein Netzwerk mit demselben CIDR-IP-Bereich vorhanden sein.

Wenn Sie ein IPAM-Netzwerk in NetScaler ADM erstellen, registrieren Sie nur die Verwendung des Infoblox-Netzwerks in NetScaler ADM. ADM arbeitet dann mit Infoblox zusammen, um die vom Netzwerk zugewiesenen IP-Adressen zu verwalten. Das InfoBlox-Netzwerk kann weiterhin außerhalb von NetScaler ADM verwendet werden.

Ähnlich verhält es sich, wenn Sie das NetScaler ADM IPAM-Netzwerk löschen, NetScaler ADM die Registrierung des Infoblox-Netzwerks aufhebt. Das bedeutet, dass NetScaler ADM nicht mehr mit Infoblox für die IP-Adressverwaltung in diesem Netzwerk interagiert.

DDI-APIs von Infoblox NetScaler ADM IPAM verwendet die folgenden Infoblox-APIs, um die jeweiligen Aktionen auszuführen:

- (/network) —Listet alle verfügbaren Infoblox-Netzwerke auf
- (/network?network={id}) —Ruft Details zu einem bestimmten Infoblox-Netzwerk ab
- (/ipv4address) —Listet alle IPs in einem Infoblox-Netzwerk auf
- (/record:host) —Ruft Details einer bestimmten IP-Adresse ab
- (/{IP}) —Reserviert und gibt IPs in einem Infoblox-Netzwerk frei

Weitere Informationen zu den Infoblox-APIs finden Sie im Infoblox REST API-Referenzhandbuch, das unter Infoblox DDI verfügbar ist.

Ein Netzwerk hinzufügen

Fügen Sie ein Netzwerk hinzu, um IPAM mit verwalteten NetScaler ADM-Konfigurationen zu verwenden.

1. Navigieren Sie zu **Einstellungen > 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 NetScaler ADM zu identifizieren.
   - **Anbieter** —Wählen Sie den Anbieter aus der Liste aus.

     In dieser Liste werden die in NetScaler ADM hinzugefügten Anbieter angezeigt.
   - **Netzwerktyp** - Wählen Sie **IP-Bereich** oder **CIDR** aus der Liste basierend auf Ihren Anforderungen aus.
   - **Netzwerkwert** —Geben Sie den Netzwerkwert an.

     > **Hinweis:**
     >
     > NetScaler 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 **Einstellungen > IPAM**.

2. Klicken Sie auf der Registerkarte **Netzwerke** auf **Alle zugewiesenen IPs**anzeigen.

   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 NetScaler 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 Konfigurationsressourcentyp wird die Konfigurationspaket-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 Zugeordnete **IPs freigeben**.

Verwenden von ADM-Audit-Protokollen zur Verwaltung und Überwachung Ihrer Infrastruktur

February 5, 2024

Sie können den NetScaler ADM Service verwenden, um alle Ereignisse auf ADM und Syslog-Ereignisse zu verfolgen, die auf ADM-verwalteten ADC-Instanzen generiert wurden. Diese Meldungen können Ihnen bei der Verwaltung und Überwachung Ihrer Infrastruktur helfen. Protokollnachrichten sind jedoch nur dann eine hervorragende Informationsquelle, wenn Sie sie überprüfen, und ADM vereinfacht die Überprüfung von Protokollnachrichten.

Sie können Filter verwenden, um nach ADM-Syslog- und Audit-Logmeldungen zu suchen. Die Filter helfen dabei, Ihre Ergebnisse einzugrenzen und in Echtzeit genau das zu finden, wonach Sie suchen. Die integrierte Suchhilfe hilft Ihnen beim Filtern der Protokolle. Eine andere Möglichkeit, Protokollmeldungen anzuzeigen, besteht darin, sie in die Formate PDF, CSV, PNG und JPEG zu exportieren. Sie können den Export dieser Berichte an bestimmte E-Mail-Adressen in verschiedenen Intervallen planen.

Sie können die folgenden Arten von Protokollmeldungen in der ADM-GUI überprüfen:

- Auditprotokolle im Zusammenhang mit ADC-Instanz
- ADM-bezogene Überwachungsprotokolle
- Audit-Protokolle für Anwendungen

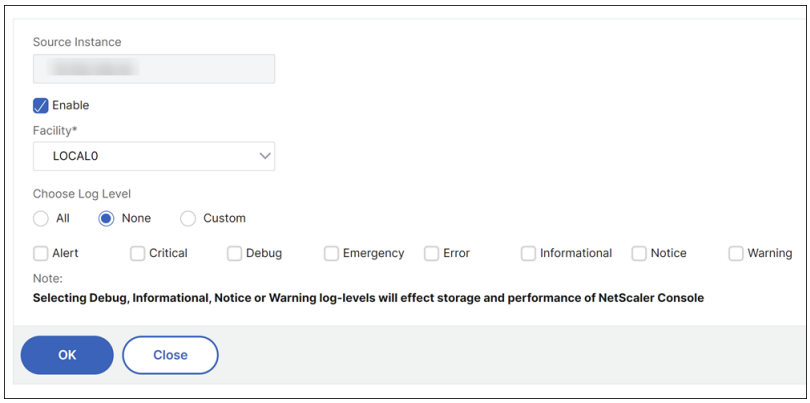
Auditprotokolle im Zusammenhang mit ADC-Instanz

Bevor Sie ADC-Instanz-bezogene Syslog-Nachrichten von ADM anzeigen können, konfigurieren Sie den NetScaler ADM Dienst als Syslog-Server für die NetScaler-Instanz. Nachdem die Konfiguration abgeschlossen ist, werden alle Syslog-Meldungen von der Instanz an ADM umgeleitet.

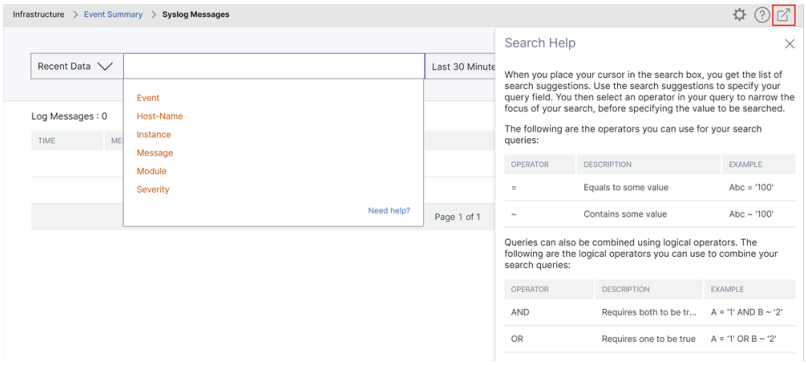
Konfigurieren von ADM Service als Syslog-Server

Gehen Sie folgendermaßen vor, um ADM als Syslog-Server zu konfigurieren:

1. Navigieren Sie in der ADM-GUI zu **Infrastruktur > Instanzen**.
2. Wählen Sie die NetScaler-Instanz aus, aus der die Syslog-Nachrichten gesammelt und in NetScaler 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 Einrichtung auf lokaler Ebene oder auf Benutzerebene aus.
6. Wählen Sie die erforderliche Protokollebene für die Syslog-Meldungen aus.
7. Klicken Sie auf **OK**.



Mit diesen Schritten werden alle Syslog-Befehle in der NetScaler-Instanz konfiguriert, und NetScaler ADM beginnt mit dem Empfang der Syslog-Nachrichten. Sie können die Meldungen anzeigen, indem Sie zu **Infrastruktur > Ereignisse > Syslog-Meldungen**navigieren. Klicken Sie auf **Hilfe?**, 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 Anzeigen und 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 im ADM vorhandenen Überwachungsprotokollmeldungen anzuzeigen, navigieren Sie zu **Einstellungen > ADM-Überwachungsprotokollnachrichten**.

Um die Protokollmeldungen zu exportieren, klicken Sie auf das Pfeilsymbol in der oberen rechten Ecke.

Anwendungsbezogene Audit-Logs

Sie können die Überwachungsprotokollmeldungen für alle ADM-Anwendungen oder für eine bestimmte Anwendung anzeigen.

- Um alle Überwachungsprotokollmeldungen für alle im ADM vorhandenen Anwendungen anzuzeigen, navigieren Sie zu **Infrastruktur > Netzwerkfunktionen > Überwachung**.
- Um Überwachungsprotokollmeldungen für eine bestimmte Anwendung im ADM anzuzeigen, navigieren Sie zu **Anwendungen > Dashboard**, klicken Sie auf einen virtuellen Server und wählen Sie **Überwachungsprotokoll**aus.

NetScaler-Lizenzmanagement für flexible und gepoolte Lizenzen

February 5, 2024

> **Hinweis:**
>
> Informationen zu den verschiedenen Typen von NetScaler-Lizenzen finden Sie unter Übersicht über die Lizenzierung .

Alle Details zu Ihren Lizenzen, wie Porteinstellungen, Lizenzdateien, Ablaufinformationen und Benachrichtigungseinstellungen, sind auf dieser Seite aufgeführt. Sie können Lizenzen anwenden, Ablaufprüfungen für Lizenzen konfigurieren und Benachrichtigungen für die Lizenznutzung und die Tage bis zum Ablauf einrichten.

Porteinstellungen für den Lizenzserver

Ports werden von NetScaler-Instanzen für die Kommunikation mit dem Lizenzserver verwendet. Klicken Sie auf das Symbol **Bearbeiten** und geben Sie Werte für die folgenden Parameter an:

- **Lizenzserver-Port**: Der Proxyserver-Port, der von NetScaler-Instanzen für den Zugriff auf das Citrix-Lizenzierungsportal für die Lizenzzuweisung verwendet wird. Standardwert: 27000.
- **Vendor Daemon Port**: Der Lizenzserver-Port, der von NetScaler-Instanzen für die Kommunikation mit dem Lizenzserver verwendet wird. Standardwert: 7279.
- **Proxy-Server-Port**: NetScaler ADM kann als HTTP-Forward-Proxy für NetScaler-Instanzen verwendet werden, um auf das MyCitrix-Portal für den automatisierten Lizenzabruf zuzugreifen. Um diese Funktion zu aktivieren, geben Sie einen TCP-Port an, auf dem der Proxy lauscht.

Lizenzdateien

Die auf Ihrem NetScaler vorhandenen Lizenzdateien sind in diesem Abschnitt aufgeführt. Sie können Lizenzen hinzufügen, löschen und herunterladen. Sie müssen Lizenzen beantragen, bevor sie verwendet werden können.

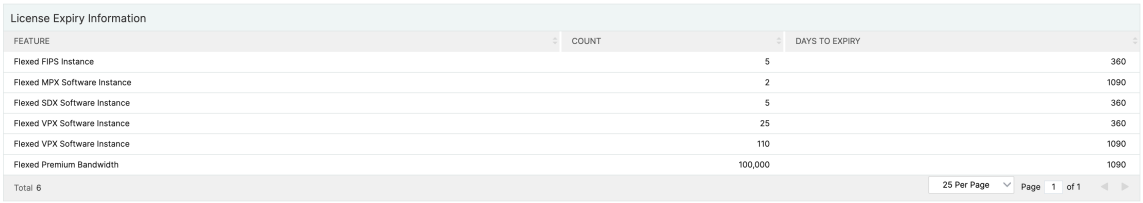
Eine Lizenzdatei anwenden

1. Navigieren Sie zu **NetScaler Licensing > License Management** .
2. **Klicken Sie im Abschnitt Lizenzdateien auf Lizenzdatei hinzufügen** und wählen Sie eine der folgenden Optionen aus:
    - **Laden Sie Lizenzdateien von einem lokalen Computer**hoch: Wenn auf Ihrem lokalen Computer bereits eine Lizenzdatei vorhanden ist, können Sie sie auf NetScaler ADM hochladen.

- **Lizenzzugangscode verwenden : Geben Sie**den Lizenzzugangscode für die Lizenz an, die Sie bei Citrix gekauft haben. Klicken Sie auf **Lizenzen** abrufen und dann auf **Fertig** stellen .

3. Klicken Sie auf **Fertig stellen**.
   Die Lizenzdateien werden zu NetScaler ADM hinzugefügt.
   Im Abschnitt **Informationen zum Ablauf der Lizenz** sind die in NetScaler ADM vorhandenen Lizenzen, die Anzahl und die verbleibenden Tage bis zum Ablauf aufgeführt.

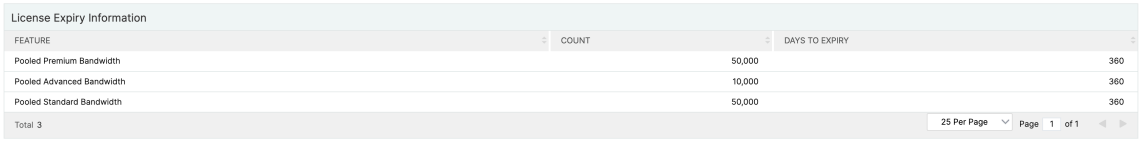
   Der folgende Screenshot zeigt die Anzahl der Fleced NetScaler VPX-, NetScaler MPX-, NetScaler SDX- und NetScaler VPX FIPS-Softwareinstanzlizenzen, die vorhandene Flexed-Premium-Bandbreitenkapazität und die Tage bis zum Ablauf.

   
   License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Flexed FIPS Instance	5	360
Flexed MPX Software Instance	2	1090
Flexed SDX Software Instance	5	360
Flexed VPX Software Instance	25	360
Flexed VPX Software Instance	110	1090
Flexed Premium Bandwidth	100,000	1090

   Total 6 — 25 Per Page — Page 1 of 1

   Der folgende Screenshot zeigt die verfügbare gepoolte Standard-, Advanced- und Premium-Bandbreite sowie die Tage bis zum Ablauf.

   
   License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Pooled Premium Bandwidth	50,000	360
Pooled Advanced Bandwidth	10,000	360
Pooled Standard Bandwidth	50,000	360

   Total 3 — 25 Per Page — Page 1 of 1

4. Wählen Sie eine Lizenzdatei aus und klicken Sie auf **Lizenzen anwenden** .

Eine Lizenzdatei löschen

Um eine Lizenzdatei zu löschen, wählen Sie eine oder mehrere Dateien aus und klicken Sie auf **Löschen** . Wenn Sie eine Lizenz löschen, müssen Sie zuerst die Lizenz hinzufügen und erst dann können Sie sie anwenden.

Laden Sie eine Lizenzdatei herunter

**Um eine Lizenzdatei herunterzuladen, wählen Sie eine Datei aus und klicken Sie auf Herunterladen . Sie können die Lizenzdatei offline als Backup speichern.

Informationen zum Ablauf der Lizenz

Sie können jetzt den Schwellenwert für Lizenzablaufzeiten für Lizenzen mit flexibler oder gepoolter Kapazität konfigurieren. Wenn der Schwellenwert festgelegt ist, sendet NetScaler ADM Benachrich-

tigungen per E-Mail oder SMS, wenn eine Lizenz abläuft. Ein SNMP-Trap und eine Benachrichtigung werden ebenfalls gesendet, wenn die Lizenz auf NetScaler ADM abgelaufen ist.

Ein Ereignis wird generiert, wenn eine Benachrichtigung über den Ablauf der Lizenz gesendet wird. Dieses Ereignis kann in NetScaler ADM unter **Infrastruktur > Ereignisse** angezeigt werden.

Ablauf der Lizenz anzeigen

1. Navigieren Sie zu **NetScaler Licensing > License Management** .
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 abläuft.
    - **Anzahl**: Anzahl der betroffenen virtuellen Server oder Instanzen.
    - **Tage bis zum Ablauf**: Anzahl der Tage vor Ablauf der Lizenz.

> **Hinweis:**
>
> Wenn Sie dem Pool neue Lizenzen hinzufügen, verwenden die NetScaler-Instanzen die neuen Lizenzen nach Ablauf ihrer vorhandenen Lizenzen.

Benachrichtigungseinstellungen

Geben Sie die Einstellungen an, auf deren Grundlage Benachrichtigungen über die Lizenznutzung und die Tage bis zum Ablauf gesendet werden.

1. **Klicken Sie**im Abschnitt **Benachrichtigungseinstellungen auf das Symbol**Bearbeiten**und wählen Sie Bei Lizenznutzung benachrichtigen** aus. Legen Sie den Warnschwellenwert fest. Dabei handelt es sich um einen Prozentsatz der Kapazität der flexiblen oder gepoolten Lizenz, der zum Senden einer Benachrichtigung verwendet werden soll.
2. Wählen Sie die Art der Benachrichtigung aus, die Sie senden möchten, wenn Lizenzen den Schwellenwert erreichen oder ablaufen, indem Sie das entsprechende Kontrollkästchen auswählen. Die Benachrichtigungstypen lauten wie folgt. Wählen Sie einen Benachrichtigungstyp aus und klicken Sie auf **Hinzufügen** , um Details hinzuzufügen. Sie können auch testen, ob jede Benachrichtigung zugestellt wird, bevor Sie Ihre Einstellungen speichern.
    - **E-Mail**: E-Mail-Profil oder Verteilerliste für den Versand von Benachrichtigungen. Weitere Informationen finden Sie unter Erstellen einer E-Mail-Verteilerliste.
    - **SMS**: SMS-Profil oder Verteilerliste für den Versand von Benachrichtigungen.
    - **Slack**: Slack-Profildetails zum Senden von Benachrichtigungen.
    - **PagerDuty**: PagerDuty-Profil zum Senden von Benachrichtigungen.

- **ServiceNow**: Das Citrix ServiceNow-Profil ist standardmäßig angegeben und ist die einzige derzeit verfügbare Option.
  Weitere Informationen zum Erstellen dieser Profile finden Sie unter Benachrichtigungen konfigurieren

3. Geben Sie die Tage bis zum Ablauf an. Dies ist die Anzahl der Tage, vor der Sie über den Ablauf der Lizenz informiert werden möchten.
4. Klicken Sie auf **Speichern**.

Erstellen einer E-Mail-Verteilerliste

Führen Sie die folgenden Schritte aus, um eine E-Mail-Verteilerliste zu erstellen:

1. Wählen Sie E-**Mail** aus und klicken Sie auf **Hinzufügen** .
2. Geben Sie unter **E-Mail-Verteilerliste erstellen**die folgenden Details an:

   - **Name** - Geben Sie den Namen der Verteilerliste an.
   - **E-Mail-Server**—Wählen Sie den E-Mail-Server aus, der eine E-Mail-Benachrichtigung sendet. Um einen E-Mail-Server hinzuzufügen, klicken Sie auf Hinzufügen. Geben Sie den Servernamen/die IP-Adresse und den Port an. Wählen Sie Authentifizierung aus, um die Authentifizierung für den Zugriff auf den E-Mail-Server vorzuschreiben. Wählen Sie Sicher, wenn der E-Mail-Server die SSL-Authentifizierung unterstützt. Klicken Sie auf Erstellen.
   - **Von**—Geben Sie die E-Mail-Adresse an, von der NetScaler ADM die Nachricht sendet.
   - **An**—Geben Sie die E-Mail-Adressen an, an die der NetScaler ADM die Nachricht sendet.
   - **Cc**—Geben Sie die E-Mail-Adressen an, an die der NetScaler ADM die Nachricht kopiert.
   - **Bcc**—Geben Sie die E-Mail-Adressen an, an die NetScaler ADM die Nachricht blind kopiert (zeigt die E-Mail-Adresse nicht an).

3. Klicken Sie auf **Erstellen**.

Erstellen Sie eine SMS-Verteilerliste

Führen Sie die folgenden Schritte aus, um die SMS-Benachrichtigungseinstellungen zu konfigurieren:

1. Klicken Sie in **SMS**auf **Hinzufügen**.
2. Geben Sie unter **SMS-Verteilerliste erstellen**die folgenden Details an:

   - **Name** - Geben Sie den Namen der Verteilerliste an.
   - **SMS-Server**—Wählen Sie den SMS-Server aus, der SMS-Benachrichtigungen sendet. Um einen SMS-Server hinzuzufügen, klicken Sie auf **Hinzufügen** . Geben Sie die Serverdetails an und klicken Sie auf **Erstellen** .

- **An**—Geben Sie die Telefonnummer an, an die der NetScaler ADM die Nachricht sendet.

3. Klicken Sie auf **Erstellen**.

Erstellen eines Slack Profils

Führen Sie die folgenden Schritte aus, um ein Slack Profil zu erstellen:

1. Klicken Sie in **Slack**auf **Hinzufügen**.
2. Geben Sie unter **"Slack-Profil erstellen**"die folgenden Details an:

   - **Profilname** —Geben Sie den Profilnamen an. Dieser Name wird in der Slack-Profilliste angezeigt.
   - **Kanalname**—Geben Sie den Namen des Slack-Kanals an, an den der NetScaler ADM die Benachrichtigung sendet.
   - **Webhook-URL** —Geben Sie die Webhook-URL des Kanals an. Eingehende Webhooks sind eine einfache Möglichkeit, Nachrichten aus externen Quellen in Slack zu posten. Die URL ist intern mit dem Kanalnamen verknüpft. Alle Event-Benachrichtigungen, die an diese URL gesendet werden, werden auf dem dafür vorgesehenen Slack-Kanal veröffentlicht. Ein Beispiel für einen Webhook lautet wie folgt: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK.

Erstellen eines PagerDuty-Profils

Mit PagerDuty können Sie Benachrichtigungen per E-Mail, SMS, Push-Benachrichtigungen und Telefonanrufe auf einer registrierten Nummer konfigurieren. Bevor Sie ein PagerDuty-Profil in NetScaler Application Delivery and Management hinzufügen, stellen Sie sicher, dass Sie die erforderlichen Konfigurationen in PagerDuty abgeschlossen haben. Informationen zum Einstieg in PagerDuty finden Sie in der PagerDuty-Dokumentation.

Führen Sie die folgenden Schritte aus, um ein PagerDuty-Profil zu erstellen:

1. Klicken Sie in **PagerDuty**auf **Hinzufügen**.
2. Geben Sie unter **PagerDuty-Profil erstellen**die folgenden Details an:

   - **Profilname**—Geben Sie einen Profilnamen an. Dieser Name wird von verschiedenen Modulen verwendet, z. B. von Eventregeln und SSL-Benachrichtigungen, um PagerDuty-Benachrichtigungen zu senden.
   - **Integrationsschlüssel** —Geben Sie den Integrationsschlüssel an. Sie können diesen Schlüssel von Ihrem PagerDuty-Portal erhalten.

3. Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Services und Integrationen in der PagerDuty-Dokumentation.

Das ServiceNow-Profil anzeigen

Um ServiceNow-Benachrichtigungen für NetScaler-Ereignisse und NetScaler ADM-Ereignisse zu aktivieren, müssen Sie NetScaler Application Delivery and Management mithilfe des ITSM-Connectors in ServiceNow integrieren. Weitere Informationen finden Sie unter Integrieren von NetScaler ADM mit der ServiceNow-Instanz.

Führen Sie die folgenden Schritte aus, um das ServiceNow-Profil anzuzeigen und zu überprüfen:

1. In **ServiceNow** ist das Profil **Citrix_Workspace_SN** standardmäßig ausgewählt.
2. Klicken Sie auf **Test**, um automatisch ein ServiceNow-Ticket zu generieren und die Konfiguration zu überprüfen.

Lizenz mit flexibler Kapazität

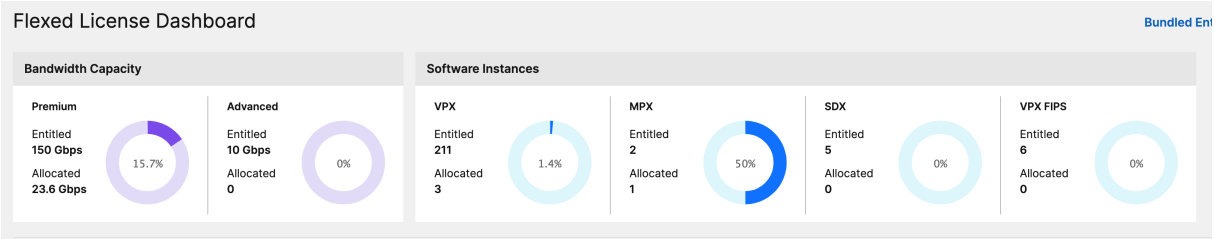
February 5, 2024

NetScaler Flected Licensing ist das neue Lizenzierungsframework, das darauf abzielt, den Lizenzverwaltungsprozess zu vereinfachen. Ihre Flexed-Lizenz umfasst Softwareinstanzlizenzen (VPX/CPX/BLX, SDX, MPX und VPX FIPS) und Bandbreitenkapazitätslizenzen. Sie müssen die Flexed-Lizenz auf den NetScaler Console-Dienst oder NetScaler ADM vor Ort anwenden. Sie müssen auch die MPX Z-Cap- und SDX Z-Cap-Lizenz auf NetScaler MPX- bzw. NetScaler SDX-Hardware anwenden. Sie können sie dann allen NetScaler-Formfaktoren zuweisen, die in der Cloud oder vor Ort bereitgestellt werden.

Eine Flexed-Lizenz bietet auch Analysen für eine unbegrenzte Anzahl virtueller Server.

Wenn Sie eine gepoolte Lizenz haben und jetzt eine Flexed-Lizenz gekauft haben, können Sie Ihre Lizenzdetails im Flexed-Lizenz-Dashboard einsehen. Die kombinierte Bandbreite und die Instanzen werden im Flexed-Lizenz-Dashboard angezeigt.

Die Bandbreitenlizenz umfasst in der Regel nur die Premium-Edition, es sei denn, Sie hatten zuvor eine Pooled Standard- oder Advanced-Lizenz. In diesem Fall werden die Standard-, Advanced- und Premium-Editionen im Flexed-Lizenz-Dashboard angezeigt.



Weitere Informationen finden Sie im Flexed-Lizenz-Dashboard .

Sie können die Flexed-Lizenzierung verwenden, um die Bandbreitennutzung zu maximieren, indem Sie sicherstellen, dass einer Instance die erforderliche Bandbreite zugewiesen wird und nicht mehr als deren Bedarf. Erhöhen oder verringern Sie die Bandbreite, die einer Instanz zur Laufzeit zugewiesen ist, ohne den Datenverkehr zu beeinträchtigen.

Erfassung von Telemetrien im Rahmen der Flexed-Lizenzierung

Um die aktuellen Flexed-Lizenzanforderungen zu erfüllen, aktivieren Sie bitte den ADM On-Prem Cloud Connector. Diese Funktion verbindet Ihren lokalen ADM Service mit dem ADM-Dienst (jetzt in NetScaler Console Service umbenannt) für die Telemetrieerfassung. Wir empfehlen, die Telemetrieerfassung zu aktivieren, wenn Sie die Flexed-Lizenzierung verwenden. Informationen zum Aktivieren von ADM On-Prem Cloud Connector finden Sie unter Cloud Connector.

ADM On-Prem Cloud Connector ermöglicht es Citrix Cloud, Lizenz-, Konfigurations- und Nutzungsdaten zur Einhaltung der Lizenzbestimmungen zu sammeln und den Service zu verwalten, zu messen und zu verbessern. Erfahren Sie mehrüber die Daten, die wir sammeln.

> **Hinweis:**
>
> Zusätzlich zu diesem automatisierten Modus der Datenerfassung wird in einer zukünftigen Version ein manueller Modus zum Aktivieren und Teilen der Telemetriedaten verfügbar sein. Sie können die Telemetriedaten im automatisierten oder im manuellen Modus teilen. Sobald beide Modi verfügbar sind, müssen die Telemetriedaten geteilt werden. Andernfalls werden Support und Wartung nach 90 Tagen ausgesetzt.

Hardware ohne Kapazität

Wenn MPX- und SDX-Instanzen über die NetScaler Flexed-Lizenzierung verwaltet werden, werden sie als „Hardware ohne Kapazität“bezeichnet, da diese Instanzen erst funktionieren, wenn sie Ressourcen aus dem Bandbreitenpool auschecken. Daher werden diese Plattformen auch als MPX-Z- und SDX-Z-Appliances bezeichnet.

Für Hardware ohne Kapazität ist eine Z-Cap-Lizenz erforderlich, um die Bandbreite aus dem gemeinsamen Pool auszuchecken.

> **Hinweis:**
>
> - Die Installation der Nullkapazitätslizenz funktioniert genauso wie andere lokale NetScaler-Lizenzen. Weitere Informationen zum Erwerb und zur Installation einer Nullkapazitätslizenz finden Sie im Lizenzleitfaden für NetScaler.

Verwaltung und Installation von Z-Cap-Lizenzen

Sie müssen eine Z-Cap-Lizenz manuell installieren, indem Sie die Hardware-Seriennummer oder den Lizenzzugangscode verwenden. Nachdem eine Z-Cap-Lizenz installiert wurde, ist sie an die Hardware gebunden und kann nicht bei Bedarf von allen NetScaler-Hardwareinstanzen gemeinsam genutzt werden. Sie können die Z-Cap-Lizenz jedoch manuell auf eine andere NetScaler-Hardwareinstanz verschieben.

NetScaler MPX-Instanzen, auf denen die NetScaler-Softwareversion 11.1 Build 54.14 oder höher ausgeführt wird, und NetScaler SDX-Instanzen, auf denen 11.1 Build 58.13 oder höher ausgeführt wird, unterstützen die NetScaler Flexed-Lizenzierung. Weitere Informationen finden Sie in **Tabelle 1. Unterstützte Flexed-Lizenzierung für MPX- und SDX-Instanzen**.

Standalone NetScaler VPX-Instanzen

NetScaler VPX-Instanzen, auf denen NetScaler Software Release 11.1 Build 54.14 und höher ausgeführt wird, unterstützen Flexed-Lizenzen auf den folgenden Hypervisoren:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

NetScaler VPX-Instanzen, auf denen die NetScaler-Softwareversion 12.0 Build 51.24 und höher ausgeführt wird, auf den folgenden Hypervisoren und Cloud-Plattformen unterstützen Flexed-Lizenzen:

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

NetScaler VPX-Instanzen, auf denen die NetScaler-Softwareversionen 13.0 und 13.1 (alle Versionen) auf den folgenden Hypervisoren und Cloud-Plattformen ausgeführt werden, unterstützen Flexed-Lizenzen:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS

- Microsoft Azure
- Google Cloud

> **Hinweis:**
>
> Um die Kommunikation zwischen NetScaler ADM und Microsoft Azure oder AWS zu ermöglichen, muss ein IPSEC-Tunnel konfiguriert werden. Weitere Informationen finden Sie unter Hinzufügen von in der Cloud bereitgestellten NetScaler VPX-Instanzen zu NetScaler ADM. Im Gegensatz zu Hardware ohne Kapazität benötigt NetScaler VPX keine Lizenz ohne Kapazität. Um den Datenverkehr zu verarbeiten, muss er Bandbreite und eine Instanzlizenz aus dem Pool auschecken.

Eigenständige NetScaler CPX-Instanzen

NetScaler CPX-Instanzen, die auf einem Docker-Host bereitgestellt werden, unterstützen die Flexed-Lizenzierung. Im Gegensatz zu Hardware ohne Kapazität benötigt NetScaler CPX keine Z-Cap-Lizenz. Eine einzelne NetScaler CPX-Instanz, die einen Durchsatz von bis zu 1 Gbit/s verbraucht, checkt nur eine Instanz und keine Bandbreite aus dem Lizenzpool aus. Stellen Sie sich beispielsweise vor, Sie haben 20 NetScaler CPX-Instanzen mit einem Bandbreitenpool von 20 Gbit/s. Wenn eine der NetScaler CPX-Instanzen einen Durchsatz von 500 Mbit/s verbraucht, bleibt der Bandbreitenpool für die verbleibenden 19 NetScaler CPX-Instanzen bei 20 Gbit/s.

Wenn dieselbe NetScaler CPX-Instanz anfängt, einen Durchsatz von 1500 Mbit/s zu verbrauchen, hat der Bandbreitenpool 19,5 Gbit/s für die verbleibenden 19 NetScaler CPX-Instanzen.

Bei der Flexed-Lizenzierung können Sie mehr Bandbreite nur in Vielfachen von 10 Mbit/s hinzufügen.

Eigenständige NetScaler BLX-Instanzen

NetScaler BLX-Instanzen unterstützen die Flexed-Lizenzierung. Für eine NetScaler BLX-Instanz ist keine Z-Cap-Lizenz erforderlich. Um den Datenverkehr zu verarbeiten, muss eine NetScaler BLX-Instanz die Bandbreite und eine Instanzlizenz aus dem Pool auschecken.

Bandbreiten-Pool

Der Bandbreitenpool ist die Gesamtbandbreite, die von NetScaler-Instanzen gemeinsam genutzt werden kann, sowohl physisch als auch virtuell. Der Bandbreitenpool umfasst einen Pool für die Premium-Softwareedition. Wenn Sie von der Pooled- zur Flexed-Lizenzierung wechseln, finden Sie möglicherweise eine Mischung aus Standard-, Advanced- und Premium-Softwareversionen. Für eine bestimmte NetScaler MPX/VPX/CPX/BLX-Instanz kann die Bandbreite aus verschiedenen Pools nicht

gleichzeitig ausgecheckt werden. Der Bandbreitenpool, aus dem er Bandbreite auschecken kann, hängt von seiner Software-Edition ab, für die er lizenziert ist.

Instanzpool

Es gibt drei Arten von Software-Instanzpools:

- VPX/CPX/BLX-Softwareinstanz
- MPX-Softwareinstanz (derselbe Pool gilt für MPX FIPS)
- SDX-Softwareinstanz (derselbe Pool gilt für SDX FIPS)
- VPX FIPS-Softwareinstanz

Beim Auschecken aus dem Pool werden mit einer Lizenz die Ressourcen der Softwareinstanz freigeschaltet, einschließlich CPUs/PEs, SSL-Kerne, Pakete pro Sekunde und Bandbreite.

NetScaler ADM-Lizenzserver

Die NetScaler Flexed-Lizenzierung verwendet den als Lizenzserver konfigurierten NetScaler ADM zur Verwaltung von Flexed-Lizenzen: Bandbreitenpool-Lizenzen und Instance-Pool-Lizenzen.

Beim Auschecken von Lizenzen aus Bandbreiten- und Instanzpool bestimmt der NetScaler Formfaktor und die Hardwaremodell auf einer Hardware mit null Kapazität

- Die minimale Bandbreite und die Anzahl der Instanzen, die eine NetScaler-Instanz auschecken muss, bevor sie funktionsfähig ist.
- Die maximale Bandbreite und die Anzahl der Instanzen, die ein NetScaler auschecken kann.
- Die minimale Bandbreiteneinheit für jeden Bandbreiten-Check-out Die minimale Bandbreiteneinheit ist die kleinste Bandbreiteneinheit, die ein NetScaler aus einem Pool auschecken muss. Bei jedem Auschecken muss es sich um ein ganzzahliges Vielfaches der Mindestbandbreiteneinheit handeln. Wenn die Mindestbandbreiteneinheit eines NetScaler beispielsweise 1 Gbit/s beträgt, können 1000 Mbit/s ausgecheckt werden, jedoch nicht 200 Mbit/s oder 150,5 Gbit/s. Die minimale Bandbreiteneinheit unterscheidet sich von der minimalen Bandbreitenanforderung. Eine NetScaler-Instanz kann nur ausgeführt werden, wenn sie mindestens mit der minimalen Bandbreite lizenziert wurde. Sobald die minimale Bandbreite erreicht ist, kann die Instanz mit der minimalen Bandbreiteneinheit mehr Bandbreite auschecken.

In den Tabellen 1, 2, 3 und 4 werden die maximale Bandbreite/Instanzen, minimale Bandbreite/Instanzen und minimale Bandbreiteneinheit für alle unterstützten NetScaler-Instanzen zusammengefasst. Tabelle 5 fasst die Lizenzanforderungen für verschiedene Formfaktoren für alle unterstützten NetScaler-Instanzen zusammen. Die folgenden Tabellen beziehen sich auf die Systemanforderungen.

> **Hinweis:**
>
> Die Mindestbandbreiten-Checkout-Einheit für NetScaler CPX/BLX/VPX beträgt 10 Mbit/s. Die Mindestbandbreiten-Checkout-Einheit für NetScaler MPX/SDX beträgt 1 Gbit/s.

Tabelle 1A. Unterstützte flexible Kapazität für MPX

Produkt-Linie	Minimale Bandbreite (Gbit/s)	Maximale Bandbreite (Gbit/s)	Einheit für minimale Bandbreite
MPX 5900Z	1	10	1 Gbit/s
MPX 8900Z	5	30	1 Gbit/s
MPX 8900Z FIPS	5	20	1 Gbit/s
MPX 9100Z	10	95	1 Gbit/s
MPX 9100Z FIPS	10	95	1 Gbit/s
MPX 14000Z	20	100	1 Gbit/s
MPX 14000Z-40G	20	100	1 Gbit/s
MPX 14000Z-40S	40	100	1 Gbit/s
MPX 14000Z FIPS	30	80	1 Gbit/s
MPX 15000Z	20	120	1 Gbit/s
MPX 15000Z-50G	20	120	1 Gbit/s
MPX 15000Z FIPS	30	120	1 Gbit/s
MPX 16000Z	30	250	1 Gbit/s
MPX 22000Z	40	120	1 Gbit/s
MPX 24000Z	100	150	1 Gbit/s
MPX 25000Z	100	160	1 Gbit/s
MPX 25000Z-40G	100	200	1 Gbit/s
MPX 26000Z	100	200	1 Gbit/s
MPX 26000Z-50S	100	200	1 Gbit/s
MPX 26000Z-100 G	100	200	1 Gbit/s

Tabelle 1A. Unterstützte flexible Kapazität für NetScaler SDX-Versionen vor Build 13.0-47.x

Produkt-Linie	Minimale Bandbreite (Gbit/s)	Maximale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
SDX 8900Z	10	30	2	7	1 Gbit/s
SDX 14000Z	20	100	5	25	1 Gbit/s
SDX 14000Z-40 G	40	100	20	25	1 Gbit/s
SDX 15000Z	20	120	5	55	1 Gbit/s
SDX 15000Z-50G	20	120	5	55	1 Gbit/s
SDX 22000Z	40	120	80	80	1 Gbit/s
SDX 24000Z	100	150	80	80	1 Gbit/s
SDX 25000Z	100	200	20	115	1 Gbit/s
SDX 25000Z-40G	100	200	20	115	1 Gbit/s
SDX 26000Z	100	200	20	115	1 Gbit/s
SDX 26000Z-50S	100	200	20	115	1 Gbit/s
SDX 26000Z-100G	100	200	20	115	1 Gbit/s

Tabelle 1B. Unterstützte flexible Kapazität für NetScaler SDX Version 13 (Build 13.0-47.x und höher), Version 13.1 (Build vor 51.x) und Version 14.1 (Build früher 12.x)

Produkt-Linie	Minimale Bandbreite (Gbit/s)	Maximale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
SDX 8900Z	5	30	1	7	1 Gbit/s
SDX 9100Z	10	95	2	7	1 Gbit/s
SDX 14000Z	10	100	2	25	1 Gbit/s
SDX 14000Z-40 G	20	100	10	25	1 Gbit/s

Produkt-Linie	Minimale Bandbreite (Gbit/s)	Maximale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
SDX 15000Z	10	120	2	55	1 Gbit/s
SDX 15000Z-50G	10	120	2	55	1 Gbit/s
SDX 16000Z	15	250	10	55	1 Gbit/s
SDX 22000Z	20	120	40	80	1 Gbit/s
SDX 24000Z	50	150	40	80	1 Gbit/s
SDX 25000Z	50	200	10	115	1 Gbit/s
SDX 25000Z-40G	50	200	10	115	1 Gbit/s
SDX 26000Z	50	200	10	115	1 Gbit/s
SDX 26000Z-50S	50	200	10	115	1 Gbit/s
SDX 26000Z-100G	50	200	10	115	1 Gbit/s

Tabelle 1C. Unterstützte flexible Kapazität für NetScaler SDX Version 13.1 (Build 51.x und höher) und Version 14.1 (Build 12.x und höher)

Produkt-Linie	Minimale Bandbreite (Gbit/s)	Maximale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
SDX 8900Z	5	30	1	7	1 Gbit/s
SDX 9100Z	10	95	1	7	1 Gbit/s
SDX 14000Z	10	100	1	25	1 Gbit/s
SDX 14000Z-40 G	20	100	1	25	1 Gbit/s
SDX 15000Z	10	120	1	55	1 Gbit/s
SDX 15000Z-50G	10	120	1	55	1 Gbit/s

Produkt-Linie	Minimale Bandbreite (Gbit/s)	Maximale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
SDX 16000Z	15	250	1	55	1 Gbit/s
SDX 22000Z	20	120	1	80	1 Gbit/s
SDX 24000Z	50	150	1	80	1 Gbit/s
SDX 25000Z	50	200	1	115	1 Gbit/s
SDX 25000Z-40G	50	200	1	115	1 Gbit/s
SDX 26000Z	50	200	1	115	1 Gbit/s
SDX 26000Z-50S	50	200	1	115	1 Gbit/s
SDX 26000Z-100G	50	200	1	115	1 Gbit/s

> **Hinweise:**
>
> - Die Mindestabnahmemenge kann von der Mindestsystemanforderung abweichen.
> - Auf NetScaler SDX, auf dem Build 14.1-12.x und höher ausgeführt wird, mit einer Flexed-Lizenz wird die Beschränkung zum Auschecken einer Mindestanzahl von Instanzlizenzen aufgehoben. Das heißt, Sie können mindestens eine Instanzlizenz auschecken.

Tabelle 2. Unterstützte minimale/maximale Bandbreite und minimale/maximale Instanzen für NetScaler CPX-Instanzen

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Mbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
CPX	10	10	1	1	10 MBit/s

Tabelle 3. Unterstützte minimale/maximale Bandbreite und minimale/maximale Instanzen für NetScaler VPX-Instanzen auf Hypervisoren und Cloud-Diensten

Hypervisor/Cloud-Dienst	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Mbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
Citrix Hypervisor	40 Gbit/s	10 MBit/s	1	1	10 MBit/s
VMware ESXI	100 Gbit/s	10 MBit/s	1	1	10 Mbit/s
Linux KVM	100 Gbit/s	10 MBit/s	1	1	10 Mbit/s
Microsoft Hyper-V	3 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
AWS	30 Gbit/s	10 MBit/s	1	1	10 MBit/s
Azure	10 Gbit/s	10 MBit/s	1	1	10 MBit/s
Google Cloud	10 Gbit/s	10 MBit/s	1	1	10 MBit/s

> Hinweis:
>
> Die Mindestabnahmemenge unterscheidet sich von der Mindestsystemanforderung.

Tabelle 4. Unterstützte minimale/maximale Bandbreite und minimale/maximale Instanzen für NetScaler BLX-Instanzen

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Mbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
BLX	100	10	1	1	10 MBit/s

Tabelle 5. Lizenzanforderungen ohne Kapazität für verschiedene Formfaktoren

Produkt-Linie	Hardware ohne Kapazität
MPX	Lizenz erforderlich
SDX	Lizenz erforderlich
VPX	-
CPX	-

Produkt-Linie	Hardware ohne Kapazität
BLX	-

Flexed-Lizenzierung konfigurieren

February 5, 2024

> **Hinweis:**
>
> Wenn Sie gepoolte Lizenzen haben und jetzt Flexed-Lizenzen gekauft und angewendet haben, wird die kombinierte Berechtigung im Flexed-Lizenz-Dashboard angezeigt.

Mit der NetScaler Flexed-Lizenzierung können Sie Bandbreiten- oder Instanzlizenzen für verschiedene NetScaler-Formfaktoren gemeinsam nutzen. Verwenden Sie diese flexible Kapazität für die Instanzen, die sich im Rechenzentrum oder in öffentlichen Clouds befinden. Wenn eine Instanz die Ressourcen nicht mehr benötigt, checkt sie die zugewiesene Kapazität wieder in den gemeinsamen Pool ein. Verwenden Sie die freigegebene Kapazität auf anderen NetScaler-Instanzen, die Ressourcen benötigen, wieder.

Sie können die Flexed-Lizenzierung verwenden, um die Bandbreitennutzung zu maximieren, indem Sie sicherstellen, dass einer Instance die erforderliche Bandbreite zugewiesen wird und nicht mehr, als sie benötigt wird. Erhöhen oder verringern Sie die Bandbreite, die einer Instanz zur Laufzeit zugewiesen ist, ohne den Datenverkehr zu beeinträchtigen.

Sie können die folgenden Aufgaben in NetScaler ADM ausführen:

1. Laden Sie die Flexed-Lizenzdateien (Bandbreitenpool oder Software-Instanzpool) auf den Lizenzserver hoch.

   > **Hinweis:**
   >
   > Der Lizenzserver ist der NetScaler ADM On-Prem-Server.

2. Laden Sie die SDX- oder MPX-Nullkapazitätslizenzen auf die SDX- oder MPX-Hardware hoch und weisen Sie NetScaler-Instanzen bei Bedarf Lizenzen aus dem Lizenzpool zu.

   - Schauen Sie sich die Lizenzen von NetScaler-Instanzen auf der Grundlage der Mindest- und Höchstkapazität der Instanz an.

Sie können Flexed-Lizenzen, einschließlich Bandbreite, Instanz und Z-Cap-Lizenzen, von citrix.com herunterladen. Weitere Informationen finden Sie im Lizenzierungsleitfaden für NetScaler.

NetScaler Flexed-Lizenzierungsstatus

Die Flexed-Lizenzierungsstatus geben die Lizenzanforderungen für eine NetScaler-Instanz an. Die mit Flexed-Lizenzierung konfigurierten NetScaler-Instanzen zeigen einen der folgenden Zustände an:

- **Zugeteilt**: Die Instanz wird mit der richtigen Lizenzkapazität ausgeführt.
- **Grace**: Die Instanz wird mit einer Kulanzlizenz ausgeführt.
- **Verbindung unterbrochen**: Die Kommunikation von NetScaler ADM zur Instanz funktioniert nicht.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie die Flexed-Lizenzierung konfigurieren:

- Die `27000`und `7279`-Ports sind von NetScaler zu NetScaler ADM erreichbar, um Lizenzen auszuchecken. Weitere Informationen finden Sie unter Systemanforderungen.

Schritt 1 —Anwenden von Lizenzen in NetScaler ADM

1. Navigieren Sie zu **NetScaler Licensing > License Management** .
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 auf Ihrem lokalen Computer bereits eine Lizenzdatei vorhanden ist, können Sie sie in NetScaler ADM hochladen.
   - **Verwenden Sie den Lizenzzugriffscode**. 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**.

   > **Hinweis:**
   >
   > **Sie können NetScaler ADM jederzeit über die Lizenzeinstellungen weitere Lizenzen hinzufügen.**

3. Klicken Sie auf **Fertig stellen**.

   Die Lizenzdateien werden zu NetScaler ADM hinzugefügt. Im Abschnitt **Informationen zum Ablauf der Lizenz** sind die im NetScaler ADM vorhandenen Lizenzen sowie 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**.

   Diese Aktion ermöglicht es NetScaler-Instanzen, die ausgewählte Lizenz als Flexed-Lizenz zu verwenden.

Schritt 2 —NetScaler ADM als Lizenzserver registrieren und Lizenzen zuweisen

Sie können den NetScaler ADM als Lizenzserver für eine NetScaler-Instanz registrieren.

Registrieren Sie einen NetScaler ADM Server mit der GUI

Registrieren Sie in der NetScaler ADM-GUI den NetScaler ADM-Server, der einer NetScaler-Instanz zugeordnet ist.

1. Melden Sie sich bei NetScaler 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 zugehörigen NetScaler ADM-Servers an, die beim NetScaler ADM registriert ist.
6. Wählen Sie **Bei NetScaler ADM registrieren**.
7. Geben Sie Ihre NetScaler ADM Server-Anmeldeinformationen ein, um eine Instanz bei NetScaler ADM zu registrieren, und klicken Sie auf **Weiter**. In NetScaler ADM ist einer der Server der Lizenzserver.
8. Wählen Sie **unter Lizenzen zuweisen**die Lizenzversion aus und geben Sie die erforderliche Bandbreite an.

   Weisen Sie erstmals Lizenzen in NetScaler zu. Sie können die Lizenzzuweisung später von der NetScaler 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.

Fügen Sie mithilfe der CLI einen NetScaler ADM Server hinzu

Wenn eine NetScaler-Instanz keine GUI hat, verwenden Sie die folgenden CLI-Befehle, um einen NetScaler ADM-Server hinzuzufügen, der einer Instanz zugeordnet ist:

1. Melden Sie sich bei der NetScaler Konsole an.
2. Fügen Sie die IP-Adresse des zugehörigen NetScaler ADM-Servers hinzu, die bei NetScaler ADM registriert ist. Der Standardlizenzport ist 27000.

```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-
    license-port-number>
<!--NeedCopy-->
```

3. Zeigen Sie die im Lizenzserver verfügbare Lizenzbandbreite an:

```
> sh ns licenseserverpool
<!--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-->
```

> **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 —Bearbeiten der flexiblen Bandbreite für NetScaler-Instanzen

1. Navigieren Sie zu **NetScaler Licensing > Flected Licensing > Dashboard** .
2. Wählen Sie im Abschnitt **Licensed NetScalers** eine Instance aus und klicken Sie auf Bandbreite **bearbeiten** .
3. Geben Sie auf der Seite Bandbreite **bearbeiten** eine Zahl in die Spalte **Zuweisen** ein.
4. Klicken Sie auf **Submit**.

NetScaler MPX-Z

MPX-Z ist die NetScaler MPX-Appliance, die Flexed-Capacity aktiviert. MPX-Z unterstützt den Bandbreitenpool nur für Premium Edition-Lizenzen.

MPX-Z benötigt eine Lizenz, bevor es eine Verbindung zum Lizenzserver herstellen kann. Sie können die MPX-Z-Lizenz auf eine der folgenden Arten installieren:

- Hochladen der Lizenzdatei von einem lokalen Computer.
- Verwenden der Hardware-Seriennummer der Instanz.
- Der Lizenzzugangscode aus dem Abschnitt **System** > **Lizenzen** der GUI der Instanz.

Wenn Sie die MPX-Z-Lizenz entfernen, wird MPX nicht mehr lizenziert. Die Lizenzen werden auf dem Lizenzserver veröffentlicht.

Sie können die Bandbreite einer MPX-Z-Instanz dynamisch ohne Neustart ändern. Ein Neustart ist nur erforderlich, wenn Sie die Lizenzversion ändern möchten.

> **Hinweis:**
>
> Wenn Sie die Instance neu starten, checkt sie automatisch die Flexed-Lizenzen aus, die für die konfigurierte Kapazität erforderlich sind.

NetScaler SDX-Z

SDX-Z ist die NetScaler SDX-Appliance, die Flexed-Capacity aktiviert. SDX-Z unterstützt Bandbreite und Instanzpool für die Premium Edition-Lizenzen.

SDX-Z benötigt eine Lizenz, bevor es eine Verbindung zum Lizenzserver herstellen kann. Sie können die SDX-Z-Lizenz auf eine der folgenden Arten installieren:

- Hochladen der Lizenzdatei von einem lokalen Computer.
- Verwenden der Hardware-Seriennummer der Instanz.
- Der Lizenzzugangscode aus dem Abschnitt **System** > **Lizenzen** der GUI der Instanz.

Wenn Sie die SDX-Z-Lizenz entfernen, wird SDX nicht mehr lizenziert. Die Lizenzen werden auf dem Lizenzserver veröffentlicht.

Sie können die Bandbreite einer SDX-Z-Instanz ohne Neustart dynamisch ändern.

> **Hinweis:**
>
> Wenn Sie die Instance neu starten, checkt sie automatisch die Flexed-Lizenzen aus, die für die konfigurierte Kapazität erforderlich sind.

NetScaler Hochverfügbarkeitspaar

Bevor Sie beginnen, stellen Sie sicher, dass der NetScaler ADM Server als Lizenzserver konfiguriert ist. Weitere Informationen finden Sie unter NetScaler ADM als Lizenzserver konfigurieren

Wenn Sie die Bandbreite einem NetScaler HA-Paar zuweisen, checkt das NetScaler ADM die der primären Instance zugewiesene Bandbreite aus. Sie müssen den Vorgang für die sekundäre Instanz wiederholen.

Informationen zum Zuweisen von Poollizenzen zu einem NetScaler HA-Paar finden Sie unter Zuweisen von Flexed-Lizenzen zu NetScaler-Instanzen

Auf der Seite **Flexing Capacity** werden die Instanzen und ihre zugewiesene Kapazität separat angezeigt.

Flexibles Lizenz-Dashboard

February 5, 2024

Das Flexed-Lizenz-Dashboard bietet Ihnen einen umfassenden Überblick über die Bandbreitenkapazität und die von Ihnen gekauften Instances.

Bandbreitenkapazität für alle Editionen und Instanzdetails für verschiedene Formfaktoren wie MPX, VPX und SDX werden auf dieser Seite angezeigt. NetScaler MPX und NetScaler MPX FIPS haben dieselbe Lizenzdatei. In ähnlicher Weise haben NetScaler SDX und NetScaler SDX FIPS dieselbe Lizenzdatei. NetScaler VPX FIPS hat jedoch eine andere Datei als NetScaler VPX und wird separat angezeigt. Außerdem benötigen NetScaler BLX und NetScaler CPX NetScaler VPX-Lizenzen und sind Teil der Berechtigung und Zuweisung für VPX. Eine Flexed-Lizenz unterstützt nur die Premium-Edition. Wenn Sie jedoch Flexed-Lizenzen gekauft haben und zuvor über gepoolte Standard- oder Advanced-Bandbreitenkapazität verfügten, werden die Details zur Bandbreitenkapazität (Standard oder Advanced) auch im Flexed-Lizenz-Dashboard aufgeführt.

Einzelheiten zu Ihren lizenzierten NetScaler-Instanzen finden Sie im Abschnitt **Lizenzierte** NetScaler . Sie können eine Instance auswählen und die Bandbreite bearbeiten oder die Lizenz für diese Instance freigeben.

Sie können die Ergebnisse anhand der folgenden Parameter filtern:

- Nach Bandbreite filtern
  - Premium
  - Erweitert
  - Standard
- Formfaktor
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX

- Status der Lizenz
  - Verbindung unterbrochen
  - Kulanzzeitraum
  - Zugeteilt

Bearbeiten Sie die zugewiesene Bandbreite auf einer NetScaler-Instanz

1. Navigieren Sie zu **NetScaler Licensing > Flected Licensing > Dashboard** .
2. Wählen Sie im Abschnitt **Licensed NetScalers** eine Instance aus und klicken Sie auf Bandbreite **bearbeiten** .
3. Geben Sie auf der Seite Bandbreite **bearbeiten** eine Zahl in die Spalte **Zuweisen** ein.
4. Klicken Sie auf **Submit**.

Lizenzen auf einer NetScaler-Instanz freigeben

Um Lizenzen auf eine andere Instanz zu übertragen, müssen Sie die Lizenz auf der aktuellen Instanz freigeben und dann die Lizenz auf die neue Instanz anwenden. Wenn Sie **Lizenz freigeben** auswählen, wird Folgendes bewirkt:

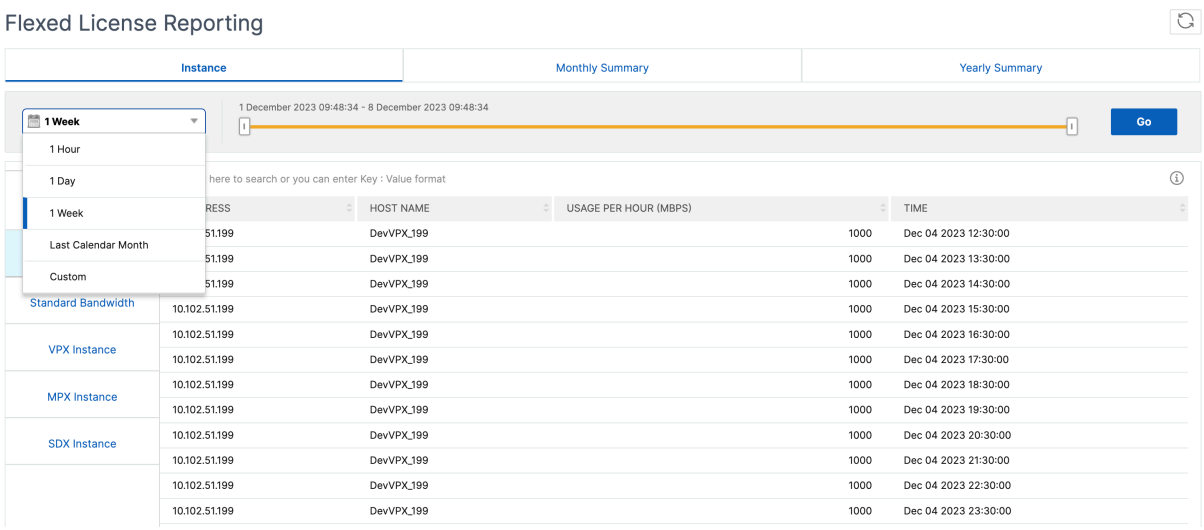
- Gibt alle Lizenzen, die auf dieser Instanz ausgecheckt sind, auf den Lizenzserver frei.
- Löscht die Lizenzserverkonfiguration auf dieser Instanz.

Wenn Sie Ja auswählen**,**wird Ihre NetScaler-Instanz nicht mehr lizenziert und kann keinen Datenverkehr verarbeiten.

Flexibles Lizenzreporting

February 5, 2024

Sie können Details zu Ihrer Softwareinstanz sowie zur Bandbreitenlizenzzuweisung und -berechtigung einsehen, um zu erfahren, wie viel von der Berechtigung zugewiesen wird. Sie können Instance-Details einsehen, z. B. welche Instance wie viel Bandbreite verbraucht (Nutzung pro Stunde) und zu welchem Zeitpunkt dies der Fall ist. Sie können den Zeitraum von einer Stunde bis zu einem benutzerdefinierten Zeitraum angeben.



**Auf den Registerkarten Monatsübersicht und Jahresübersicht **sind grafische Ansichten verfügbar. Die folgenden Grafiken sind einige Beispiele für die Inanspruchnahme und Zuweisung von Software-instanzen.

NetScaler Pool-Kapazität

February 5, 2024

Die NetScaler Pooled-Kapazität ermöglicht es Ihnen, Bandbreiten- oder Instanzlizenzen für verschiedene NetScaler-Formfaktoren gemeinsam zu nutzen. Für abonnementbasierte Instanzen mit virtueller CPU können Sie die virtuelle CPU-Lizenz instanzübergreifend teilen. Verwenden Sie diese gepoolte Kapazität für die Instanzen, die sich im Rechenzentrum oder in öffentlichen Clouds befinden. Wenn eine Instanz die Ressourcen nicht mehr benötigt, checkt sie die zugewiesene Kapazität wieder in den gemeinsamen Pool ein. Verwenden Sie die freigegebene Kapazität für andere

NetScaler-Instanzen, die Ressourcen benötigen.

Sie können die gepoolte Lizenzierung verwenden, um die Bandbreitennutzung zu maximieren, indem Sie sicherstellen, dass einer Instance die erforderliche Bandbreite zugewiesen wird und nicht mehr, als sie benötigt wird. Erhöhen oder verringern Sie die Bandbreite, die einer Instanz zur Laufzeit zugewiesen ist, ohne den Datenverkehr zu beeinträchtigen. Mit den gepoolten Kapazitätslizenzen können Sie die Instanzbereitstellung automatisieren.

So funktioniert die NetScaler Pooled Capacity Licensing

Die NetScaler Pooled-Kapazität besteht aus den folgenden Komponenten:

- NetScaler-Instanzen, die kategorisiert werden können in:
  - Hardware ohne Kapazität
  - Eigenständige NetScaler VPX-Instanzen oder NetScaler CPX-Instanzen oder NetScaler BLX-Instanzen
- Bandbreitenpool
- Instanzpool
- NetScaler ADM als Lizenzserver konfiguriert

Hardware ohne Kapazität

Wenn sie über NetScaler Pooled Capacity verwaltet werden, werden MPX- und SDX-Instanzen als „Hardware ohne Kapazität“bezeichnet, da diese Instanzen erst funktionieren, wenn sie Ressourcen aus den Bandbreiten- und Instanzpools auschecken. Daher werden diese Plattformen auch als MPX-Z- und SDX-Z-Appliances bezeichnet.

Hardware ohne Kapazität erfordert eine Plattformlizenz, um Bandbreite und Instanzlizenz aus dem gemeinsamen Pool auschecken zu können.

> **Hinweis**
>
> - Für MPX-Instanzen ist kein Instanz-Lizenzabonnement erforderlich. In Tabelle 1 auf dieser Seite finden Sie die unterstützte gepoolte Kapazität für MPX- und SDX-Instanzen. In Tabelle 5 finden Sie die Lizenzanforderungen für verschiedene MPX- und SDX-Formfaktoren.
> - Die Installation der Nullkapazitätslizenz funktioniert genauso wie andere lokale NetScaler-Lizenzen. Weitere Informationen zum Erwerb und zur Installation einer Nullkapazitätslizenz finden Sie im Lizenzleitfaden für NetScaler.

Verwalten und Installieren von Plattformlizenzen

Sie müssen eine Plattformlizenz manuell installieren, indem Sie die Hardwareseriennummer oder den Lizenzzugriffscode verwenden. Nachdem eine Plattformlizenz installiert wurde, ist sie an die Hardware gebunden und kann bei Bedarf nicht für NetScaler-Hardwareinstanzen freigegeben werden. Sie können die Plattformlizenz jedoch manuell auf eine andere NetScaler Hardwareinstanz verschieben.

NetScaler MPX MPX-Instances, auf denen die NetScaler-Softwareversion 11.1 Build 54.14 oder höher ausgeführt wird, und NetScaler SDX-Instanzen, auf denen 11.1 Build 58.13 oder höher ausgeführt wird, unterstützen NetScaler Pooled-Kapazität. Weitere Informationen finden Sie in **Tabelle 1. Unterstützte gepoolte Kapazität für MPX- und SDX-Instanzen**.

Standalone NetScaler VPX-Instanzen

NetScaler VPX-Instances, auf denen die NetScaler Softwareversion 11.1 Build 54.14 und höher ausgeführt wird, unterstützen die folgenden Hypervisoren gepoolte Kapazität:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

NetScaler VPX-Instanzen, auf denen die NetScaler-Softwareversion 12.0 Build 51.24 und höher auf den folgenden Hypervisoren und Cloud-Plattformen ausgeführt wird, unterstützen gepoolte Kapazität:

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

NetScaler VPX-Instances, auf denen die NetScaler-Softwareversionen 13.0 und 13.1 (alle Versionen) auf den folgenden Hypervisoren und Cloud-Plattformen ausgeführt werden, unterstützen gepoolte Kapazität:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS

- Microsoft Azure
- Google Cloud

> **Hinweis**
>
> Um die Kommunikation zwischen NetScaler ADM und Microsoft Azure oder AWS zu ermöglichen, muss ein IPSEC-Tunnel konfiguriert werden.Weitere Informationen finden Sie unter Hinzufügen von in der Cloud bereitgestellten NetScaler VPX-Instanzen zu NetScaler ADM.
> Im Gegensatz zu Hardware ohne Kapazität benötigt NetScaler VPX keine Plattformlizenz. Um den Datenverkehr zu verarbeiten, muss er Bandbreite und eine Instanzlizenz aus dem Pool auschecken.

Eigenständige NetScaler CPX-Instanzen

NetScaler CPX-Instanzen, die auf einem Docker-Host bereitgestellt werden, unterstützen gepoolte Kapazität. Im Gegensatz zu Hardware ohne Kapazität benötigt NetScaler CPX keine Plattformlizenz. Eine einzelne NetScaler CPX-Instanz, die einen Durchsatz von bis zu 1 Gbit/s verbraucht, checkt nur eine Instanz und keine Bandbreite aus dem Lizenzpool aus. Stellen Sie sich beispielsweise vor, Sie haben 20 NetScaler CPX-Instanzen mit einem Bandbreitenpool von 20 Gbit/s. Wenn eine der NetScaler CPX-Instanzen einen Durchsatz von 500 Mbit/s verbraucht, bleibt der Bandbreitenpool für die verbleibenden 19 NetScaler CPX-Instanzen bei 20 Gbit/s.

Wenn dieselbe NetScaler CPX-Instanz anfängt, einen Durchsatz von 1500 Mbit/s zu verbrauchen, hat der Bandbreitenpool 19,5 Gbit/s für die verbleibenden 19 NetScaler CPX-Instanzen.

Bei der Poollizenzierung können Sie mehr Bandbreite nur in Vielfaches von 10 Mbit/s hinzufügen.

Eigenständige NetScaler BLX-Instanzen

NetScaler BLX-Instances unterstützen gepoolte Kapazitätslizenzen. Eine NetScaler BLX-Instanz erfordert keine Plattformlizenz. Um den Datenverkehr zu verarbeiten, muss eine NetScaler BLX-Instanz die Bandbreite und eine Instanzlizenz aus dem Pool auschecken.

Bandbreiten-Pool

Der Bandbreitenpool ist die Gesamtbandbreite, die von NetScaler-Instanzen gemeinsam genutzt werden kann, sowohl physisch als auch virtuell. Der Bandbreitenpool umfasst separate Pools für jede Software-Edition (Standard, Advanced und Premium). Eine bestimmte NetScaler-Instanz kann keine Bandbreite aus verschiedenen Pools gleichzeitig ausgecheckt haben. Der Bandbreitenpool, aus dem er Bandbreite auschecken kann, hängt von seiner Software-Edition ab, für die er lizenziert ist.

Instanzpool

Der Instanzpool definiert die Anzahl der NetScaler VPX-Instanzen oder NetScaler CPX-Instanzen oder NetScaler BLX-Instanzen, die über NetScaler Pooled Capacity verwaltet werden können, oder die Anzahl der NetScaler VPX-Instanzen in einer SDX-Z-Instanz.

Beim Auschecken aus dem Pool entsperrt eine Lizenz die Ressourcen der MPX-Z-, SDX-Z-, VPX-, NetScaler CPX- und NetScaler BLX-Instanz, einschließlich CPUs/PES, SSL-Kerne, Pakete pro Sekunde und Bandbreite.

> **Hinweis**
>
> Der Verwaltungsdienst eines SDX-Z verbraucht keine Instanz.

NetScaler ADM-Lizenzserver

NetScaler Pooled Capacity verwendet den als Lizenzserver konfigurierten NetScaler ADM zur Verwaltung von gepoolten Kapazitätslizenzen: Bandbreitenpool-Lizenzen und Instance-Pool-Lizenzen. Sie können die NetScaler ADM-Software verwenden, um gepoolte Kapazitätslizenzen ohne eine NetScaler ADM-Lizenz zu verwalten.

Beim Auschecken von Lizenzen aus Bandbreiten- und Instanzpool bestimmt der NetScaler Formfaktor und die Hardwaremodell auf einer Hardware mit null Kapazität

- Die minimale Bandbreite und die Anzahl der Instanzen, die eine NetScaler-Instanz auschecken muss, bevor sie funktionsfähig ist.
- Die maximale Bandbreite und die Anzahl der Instanzen, die ein NetScaler auschecken kann.
- Die minimale Bandbreiteneinheit für jeden Bandbreiten-Check-out Die minimale Bandbreiteneinheit ist die kleinste Bandbreiteneinheit, die ein NetScaler aus einem Pool auschecken muss. Bei jedem Auschecken muss es sich um ein ganzzahliges Vielfaches der Mindestbandbreiteneinheit handeln. Wenn die Mindestbandbreiteneinheit eines NetScaler beispielsweise 1 Gbit/s beträgt, können 1000 Mbit/s ausgecheckt werden, jedoch nicht 200 Mbit/s oder 150,5 Gbit/s. Die minimale Bandbreiteneinheit unterscheidet sich von der minimalen Bandbreitenanforderung. Eine NetScaler-Instanz kann nur ausgeführt werden, wenn sie mindestens mit der minimalen Bandbreite lizenziert wurde. Sobald die minimale Bandbreite erreicht ist, kann die Instanz mit der minimalen Bandbreiteneinheit mehr Bandbreite auschecken.

In den Tabellen 1, 2, 3 und 4 werden die maximale Bandbreite/Instanzen, minimale Bandbreite/Instanzen und minimale Bandbreiteneinheit für alle unterstützten NetScaler-Instanzen zusammengefasst. Tabelle 5 fasst die Lizenzanforderungen für verschiedene Formfaktoren für alle unterstützten NetScaler-Instanzen zusammen:

Tabelle 1. Unterstützte gepoolte Kapazität für MPX- und SDX-Instanzen

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
MPX 5900Z	10	1	–	–	1 Gbit/s
MPX 8900Z	30	5	Nicht verfügbar	Nicht verfügbar	1 Gbit/s
MPX 9100Z	30	10	Nicht verfügbar	Nicht verfügbar	1 Gbit/s
MPX 8900Z FIPS	33	5	Nicht verfügbar	Nicht verfügbar	1 Gbit/s
MPX 14000Z Serie	100	20	Nicht verfügbar	Nicht verfügbar	1 Gbit/s
MPX 14000Z 40G Serie	100	20	–	–	1 Gbit/s
MPX 14000Z FIPS Serie	100	20	–	–	1 Gbit/s
MPX 14000Z 40S Serie	100	20	–	–	1 Gbit/s
MPX 15000Z Serie	120	20	–	–	1 Gbit/s
MPX 15000Z FIPS Serie	120	20	–	–	1 Gbit/s
MPX 15000Z 50G Serie	120	20	–	–	1 Gbit/s
MPX 16000Z Serie	200	30	–	–	1 Gbit/s
MPX 22000Z-Serie	120	40	–	–	1 Gbit/s
MPX 24000Z Serie	150	100	–	–	1 Gbit/s
MPX 25000Z 40 G	200	100	–	–	1 Gbit/s
MPX 25000ZA	200	100	–	–	1 Gbit/s

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
MPX 26000Z Serie	200	100	–	–	1 Gbit/s
MPX 26000Z 100G Serie	200	100	–	–	1 Gbit/s
MPX 26000Z 50S Serie	200	100	–	–	1 Gbit/s
SDX 8900Z	30	10	1	7	1 Gbit/s
SDX 9100Z	95	20	1	7	1 Gbit/s
SDX 14000Z-Serie	100	10	1	25	1 Gbit/s
SDX 14000Z 40G Serie	100	1	2	25	1 Gbit/s
SDX 14000Z 40S Serie	100	20	1	25	1 Gbit/s
SDX 14000Z FIPS-Serie	100	10	1	25	1 Gbit/s
SDX 15000Z 50G	120	10	1	55	1 Gbit/s
SDX 15000Z	120	10	1	55	1 Gbit/s
SDX 16000Z-Serie	200	15	1	55	1 Gbit/s
SDX 22000Z-Serie	120	20	1	80	1 Gbit/s
SDX 25000Z 40 G	200	50	1	115	1 Gbit/s
SDX 25000ZA	200	50	1	115	1 Gbit/s
SDX 26000Z 100 G	200	50	1	115	1 Gbit/s
SDX 26000Z	200	50	1	115	1 Gbit/s
SDX 26000Z 50S	200	50	1	115	1 Gbit/s

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
SDX 24000Z-Serie	150	50	1	80	1 Gbit/s

> Hinweis
>
> Die Mindestbandbreite und Instanzen gelten für SDX-Instanzen, auf denen die folgenden Releases ausgeführt werden: 11.1 64.x, 12.0 63.x, 12.1 54.x und 13.0 41.x.
>
> Die Mindestabnahmemenge unterscheidet sich von der Mindestanforderung des Systems.

Tabelle 2. Unterstützte gepoolte Kapazität für NetScaler CPX-Instanzen

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Mbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
CPX	10	10	1	1	10 MBit/s

Tabelle 3. Unterstützte gepoolte Kapazität für NetScaler VPX-Instanzen auf Hypervisoren und Cloud-Diensten

Hypervisor/Cloud-Dienst	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Mbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
Citrix Hypervisor	40 Gbit/s	10 MBit/s	1	1	10 MBit/s
VMware ESXI	100 Gbit/s	10 MBit/s	1	1	10 Mbit/s
Linux KVM	100 Gbit/s	10 MBit/s	1	1	10 Mbit/s
Microsoft Hyper-V	3 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
AWS	30 Gbit/s	10 MBit/s	1	1	10 MBit/s
Azure	10 Gbit/s	10 MBit/s	1	1	10 MBit/s
Google Cloud	10 Gbit/s	10 MBit/s	1	1	10 MBit/s

Hypervisor/Cloud-Dienst	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Mbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite

> Hinweis:
>
> Die Mindestabnahmemenge unterscheidet sich von der Mindestsystemanforderung.

Tabelle 4. Unterstützte gepoolte Kapazität für NetScaler BLX-Instances

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Mbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
BLX	100	10	1	1	10 MBit/s

Tabelle 5. Lizenzvoraussetzung für verschiedene Formfaktoren

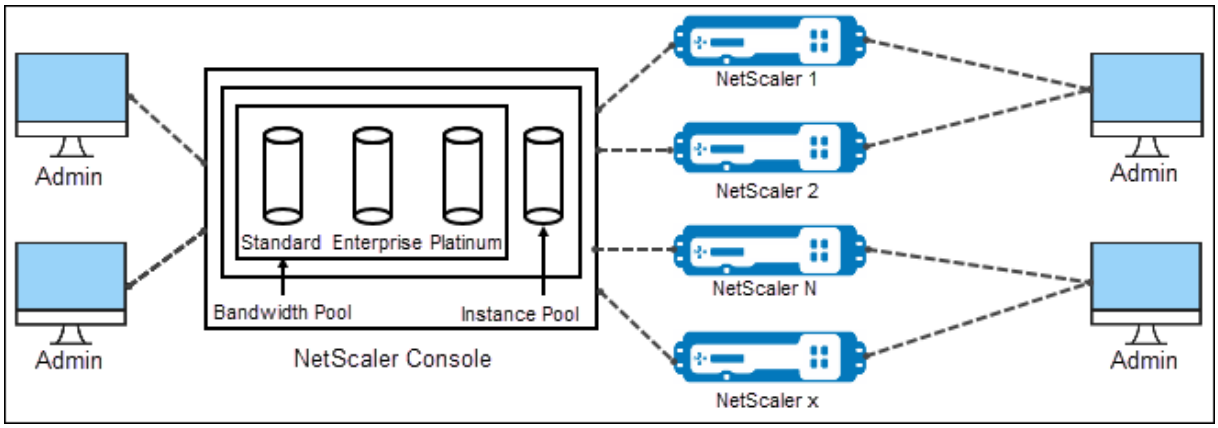
Produkt-Linie	Kauf von Hardware ohne Kapazität	Bandbreite und Editionsabonnement	Instanz-Abonnement
MPX	Lizenz erforderlich	Lizenz erforderlich	-
SDX	Lizenz erforderlich	Lizenz erforderlich	Lizenz erforderlich
VPX	-	Lizenz erforderlich	Lizenz erforderlich
CPX	-	-	Lizenz erforderlich
BLX	-	Lizenz erforderlich	Lizenz erforderlich

NetScaler Pooled Capacity konfigurieren

February 5, 2024

Um NetScaler Pooled Capacity zu verwenden, konfigurieren Sie NetScaler ADM als Lizenzserver für die erforderlichen NetScaler-Instanzen. NetScaler-Instanzen checken Lizenzen vom NetScaler ADM ein und aus. Sie können die folgenden Aufgaben in der NetScaler Application Delivery and Management GUI ausführen:

- Laden Sie die Lizenzdateien für gepoolte Kapazitäten (Bandbreite und Instanzpool) auf den Lizenzserver hoch.
- Weisen Sie den NetScaler Instanzen nach Bedarf Lizenzen aus dem Lizenzpool zu.
- Prüfen Sie die Lizenzen von NetScaler-Instanzen (MPX-Z /SDX-Z/VPX/CPX/BLX) basierend auf der minimalen und maximalen Kapazität der Instanz.
- Konfigurieren Sie die gepoolte Kapazität für NetScaler FIPS-Instanzen zum Ein- oder Auschecken von Lizenzen.



Unterstützte Hardware- und Softwareversionen

Unterstützte Hardware- und Softwareversionen für gepoolte Kapazität finden Sie unter NetScaler Pooled capacity.

Status der gepoolten NetScaler Kapazität

Die Status der gepoolten Kapazität geben die Lizenzanforderungen für eine NetScaler-Instanz an. Die mit gepoolter Kapazität konfigurierten NetScaler-Instanzen zeigen einen der folgenden Zustände an:

- **Optimal**: Die Instanz wird mit der richtigen Lizenzkapazität ausgeführt.
- **Kapazitätskonflikt**: Instanz läuft mit einer Kapazität, die geringer ist als die vom Benutzer konfigurierte.
- **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 bei NetScaler ADM für die Verwaltung registriert, oder die NITRO-Kommunikation von NetScaler ADM zu den Instanzen funktioniert nicht.

- **Nicht zugewiesen**: Die Lizenz wird in der Instanz nicht zugewiesen.

Schritt 1 —Anwenden von Lizenzen in NetScaler ADM

1. Navigieren Sie in NetScaler ADM zu **NetScaler Licensing > Pooled Licensing** .
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 auf Ihrem lokalen Computer bereits eine Lizenzdatei vorhanden ist, können Sie sie in NetScaler ADM hochladen.
   - **Verwenden Sie den Lizenzzugriffscode**. 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**.

   > **Hinweis**
   >
   > Sie können jederzeit in den **Lizenzeinstellungen**weitere Lizenzen zu NetScaler ADM hinzufügen.

3. Klicken Sie auf **Fertig stellen**.

   Die Lizenzdateien werden zu NetScaler ADM hinzugefügt. Auf der Registerkarte **Informationen zum Ablauf** der Lizenz sind die in NetScaler 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**.

   Diese Aktion ermöglicht es NetScaler-Instanzen, die ausgewählte Lizenz als gepoolte Kapazität zu verwenden.

Weitere Informationen zur Anwendung von gepoolten Lizenzen auf NetScaler Application Delivery and Management finden Sie im entsprechenden Video:

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Schritt 2 —NetScaler ADM als Lizenzserver registrieren

Gehen Sie wie folgt vor, um NetScaler ADM als Lizenzserver für eine NetScaler-Instanz zu registrieren:

- GUI verwenden
- CLI verwenden

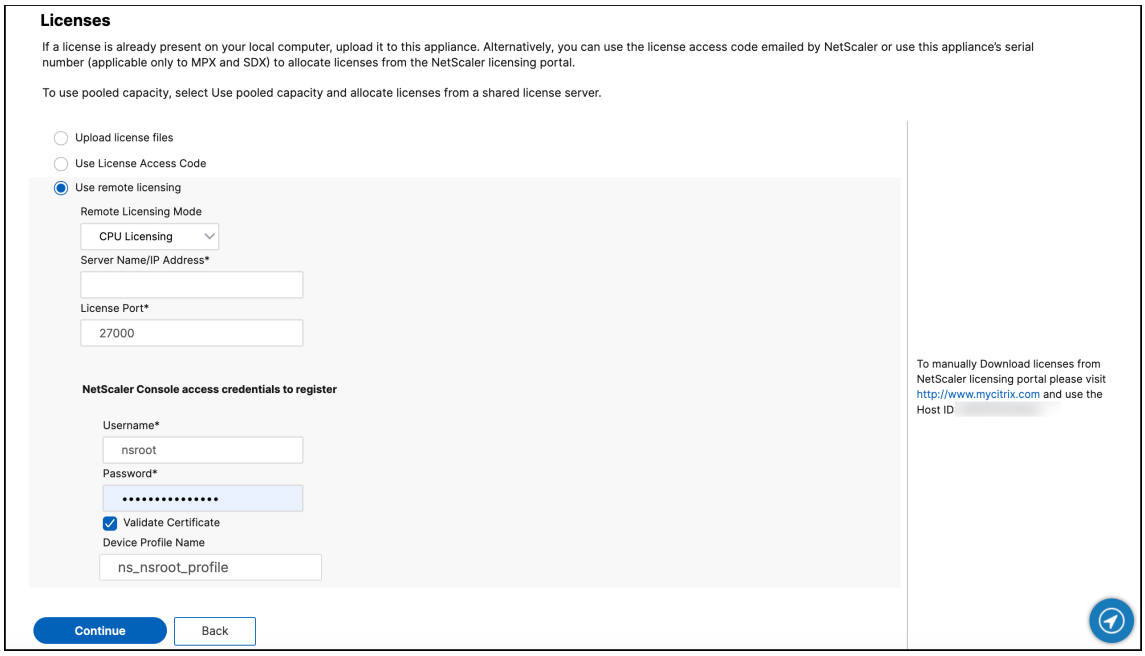
Verwenden Sie die GUI, um NetScaler ADM als Lizenzserver zu registrieren

Registrieren Sie in der NetScaler GUI den NetScaler ADM Server als Lizenzserver.

1. Melden Sie sich bei NetScaler 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 NetScaler ADM-Servers an.

   > Verwenden Sie für eine HA-Bereitstellung eine Floating-IP. Weitere Informationen zur Konfiguration finden Sie unter Configure High Availability Deployment.
   >
   > Informationen zu einer Bereitstellung, die einen eigenständigen NetScaler ADM oder einen Agenten verwendet, finden Sie unter Übersicht über die Lizenzierung.

6. Wählen Sie **Bei NetScaler ADM registrieren**.
7. Geben Sie Ihre NetScaler ADM-Anmeldeinformationen ein, um eine Instanz bei NetScaler ADM zu registrieren, und klicken Sie auf **Weiter**.



8. Wählen Sie **unter Lizenzen zuweisen**die Lizenzversion aus und geben Sie die erforderliche Bandbreite an.

   Weisen Sie erstmals Lizenzen in NetScaler zu. Sie können die Lizenzzuweisung später von der NetScaler ADM GUI ändern oder freigeben.

a) 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 Sie CLI, um NetScaler ADM als Lizenzserver hinzuzufügen

Wenn eine NetScaler-Instanz keine GUI hat, verwenden Sie die folgenden CLI-Befehle, um den NetScaler ADM-Server als Lizenzserver hinzuzufügen:

1. Melden Sie sich bei der NetScaler Konsole an.
2. Fügen Sie die NetScaler ADM Server-IP-Adresse hinzu:

```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-port-number> -licensemode <license-mode>
<!--NeedCopy-->
```

   Weitere Informationen finden Sie unter Lizenzierungsübersicht.

3. Zeigen Sie die auf dem Lizenzserver verfügbare Lizenzbandbreite an.

```
> sh ns licenseserverpool
<!--NeedCopy-->
```

   Mit diesem Befehl werden die Lizenzen basierend auf dem angegebenen Lizenzmodus beim Hinzufügen des Lizenzservers aufgelistet.

   Beispiel-1:

   Wenn der angegebene Lizenzmodus lautet `CICO`, enthält die Ausgabe nur CICO-Lizenzen.

```
> add licenseserver [redacted] -licensemode CICO
 Done
> sh licenseserverpool
        VPX8000P Total                  : 1
        VPX8000P Available              : 1
```

   Beispiel-2:

   Wenn der angegebene Lizenzmodus lautet `Pooled`, enthält die Ausgabe nur gepoolte Kapazitätslizenzen.


```
> add licenseserver [redacted] -licensemode Pooled
 Done
> sh licenseserverpool
        Instance Total                      : 40
        Instance Available                  : 38
        Standard Bandwidth Total            : 210.00 Gbps
        Standard Bandwidth Available        : 210.00 Gbps
        Enterprise Bandwidth Total          : 50.00 Gbps
        Enterprise Bandwidth Available      : 50.00 Gbps
        Platinum Bandwidth Total            : 210.00 Gbps
        Platinum Bandwidth Available        : 205.00 Gbps
```

Beispiel-3:

Wenn der angegebene Lizenzmodus lautet vCPU, enthält die Ausgabe nur virtuelle CPU-Lizenzen.

```
> add licenseserver [redacted] -licensemode vCPU
 Done
> sh licenseserverpool
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

Um alle Lizenzen zusammen anzuzeigen, führen Sie den folgenden Befehl aus:

```
1 > sh ns licenseserverpool -getallLicenses
2 <!--NeedCopy-->
```

Beispielausgabe:

```
> sh licenseserverpool -getallLicenses
        Instance Total                      : 40
        Instance Available                  : 33
        Standard Bandwidth Total            : 210.00 Gbps
        Standard Bandwidth Available        : 210.00 Gbps
        Enterprise Bandwidth Total          : 50.00 Gbps
        Enterprise Bandwidth Available      : 50.00 Gbps
        Platinum Bandwidth Total            : 210.00 Gbps
        Platinum Bandwidth Available        : 205.00 Gbps
        VPX8000P Total                      : 1
        VPX8000P Available                  : 1
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

4. Weisen Sie die Lizenzbandbreite aus der erforderlichen Lizenzedition zu:

```
1 > set ns capacity -unit <specify-mbps-or-gbps> -bandwidth <specify
      -amount-license-bandwidth> -edition <specify-license-edition>
```



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

Die Lizenzversion kann **Standard** oder **Enterprise** oder **Platinum**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 NetScaler-Instanzen

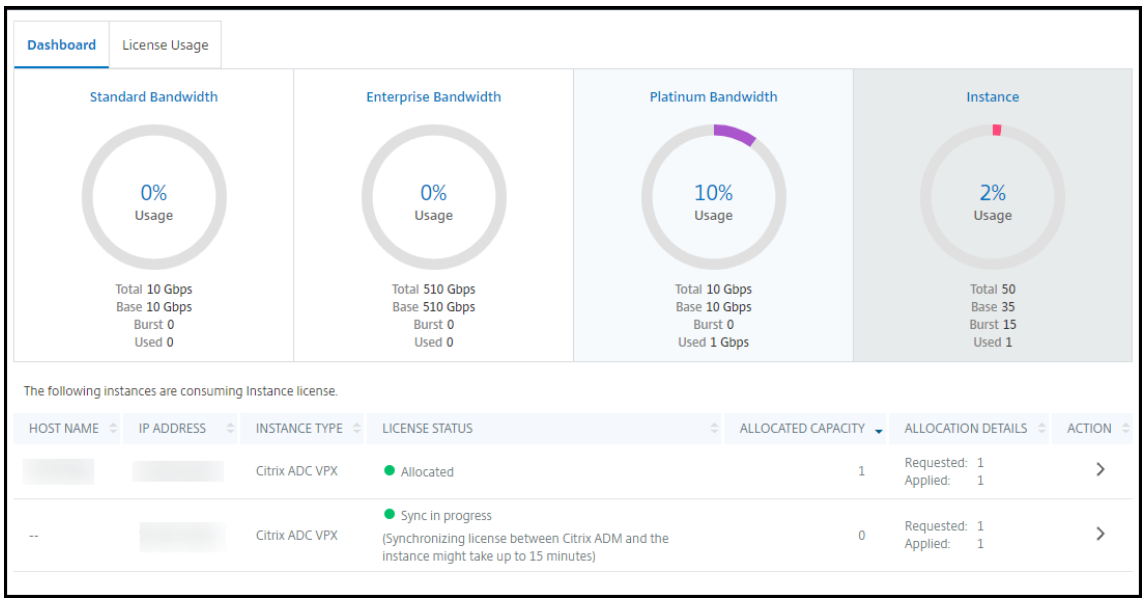
So weisen Sie gepoolte Kapazitätslizenzen über die NetScaler ADM-GUI zu:

1. Melden Sie sich bei NetScaler ADM an.
2. Navigieren Sie zu **Infrastruktur > Lizenzen > Bandbreitenlizenzen > Gepoolte Kapazität**.

   Die FIPS-Instanzkapazität wird nur angezeigt, wenn Sie FIPS-Instanzlizenzen in NetScaler ADM hochladen.
3. Klicken Sie auf den Lizenzpool, den Sie verwalten möchten.

   > **Hinweis**
   >
   > Das Feld **Zugeordnete Kapazität** spiegelt die geänderte Bandbreite nicht sofort wider. Die Bandbreitenänderung wird nach dem NetScaler-Warm-Neustart wirksam.
   >
   > In **Allocation Details**werden die Felder **Angefordert** und **Angewendet** aktualisiert, wenn Sie die Bandbreitenzuweisung der Instanz ändern.

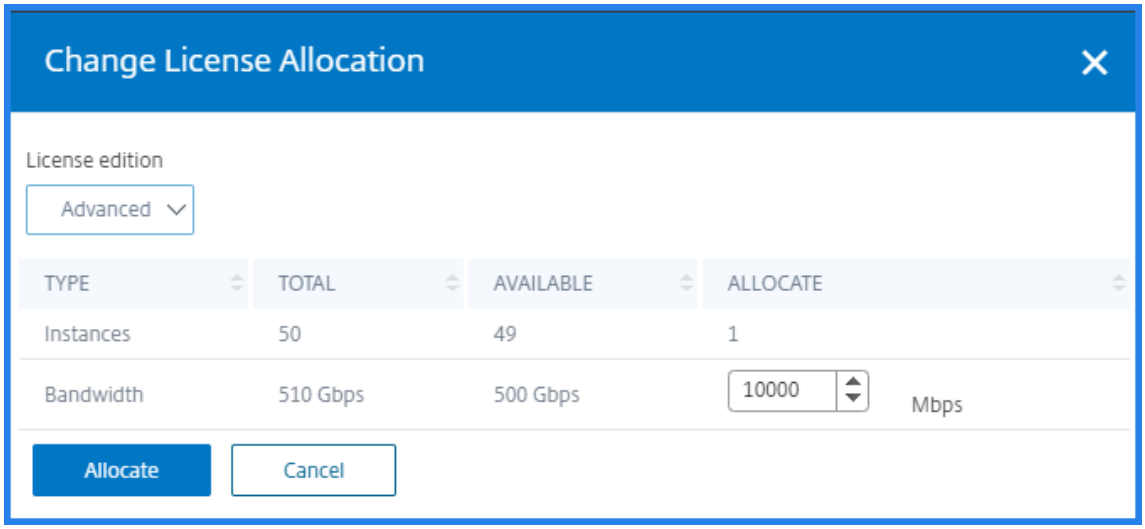
4. **Wählen Sie eine NetScaler-Instanz aus der Liste der verfügbaren Instanzen aus, indem Sie auf die Schaltfläche klicken.



In der Spalte **LIZENZSTATUS** werden die entsprechenden Statusmeldungen zur Lizenzzuweisung angezeigt.

> **Hinweis:**
>
> Auf der Registerkarte **Unmanaged Instances** werden die Instanzen angezeigt, die in NetScaler 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 der **Allocate-Liste** festlegen. Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie auf **Zuweisen**.
8. Sie können die zugewiesene Lizenzversion auch über die Listenoptionen im **Fenster Lizenzzuordnung ändern ändern**.



> **Hinweis**
>
> Starten Sie eine Instanz im Warm-Modus neu, wenn Sie die Lizenzversion ändern.

Weitere Informationen zum Ändern der Bandbreitenzuweisung finden Sie im entsprechenden Video:

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Konfiguration der gepoolten Kapazität auf NetScaler-Instanzen

Sie können gepoolte Kapazitätslizenzen auf den folgenden NetScaler-Instanzen konfigurieren:

- NetScaler-Instanzen
- NetScaler VPX-Instanzen
- NetScaler Hochverfügbarkeitspaar

NetScaler MPX-Instanzen

MPX-Z ist die NetScaler MPX-Appliance mit aktivierter Poolkapazität. MPX-Z unterstützt Bandbreiten-Pooling für Premium-, Advanced- oder Standard Edition-Lizenzen.

MPX-Z benötigt Plattformlizenzen, bevor es eine Verbindung zum Lizenzserver herstellen kann. Sie können die MPX-Z-Plattformlizenz mit einer der folgenden Methoden installieren:

- Hochladen der Lizenzdatei von einem lokalen Computer.
- Verwenden der Hardware-Seriennummer der Instanz.
- Der Lizenzzugangscode aus dem Abschnitt **System** > **Lizenzen** der GUI der Instanz.

Wenn Sie die MPX-Z-Plattformlizenz entfernen, ist die Funktion „Gepoolte Kapazität“deaktiviert. Die Instanzlizenzen werden für den Lizenzserver freigegeben.

Sie können die Bandbreite einer MPX-Z-Instanz dynamisch ohne Neustart ändern. Ein Neustart ist nur erforderlich, wenn Sie die Lizenzversion ändern möchten.

> **Hinweis:**
>
> Wenn Sie die Instance neu starten, checkt sie automatisch die gepoolten Lizenzen aus, die für die konfigurierte Kapazität erforderlich sind.

NetScaler VPX-Instanzen

Eine NetScaler VPX-Instanz, die Pooled Capacity aktiviert, kann Lizenzen aus einem Bandbreitenpool (Premium/Advanced/Standard Editionen) auschecken. Sie können die NetScaler-GUI verwenden, um Lizenzen vom Lizenzserver auszuchecken.

Sie können die Bandbreite einer VPX-Instanz dynamisch ohne Neustart ändern. Ein Neustart ist nur erforderlich, wenn Sie die Lizenzversion ändern möchten.

> **Hinweis:**
>
> Wenn Sie die Instanz neu starten, werden die konfigurierten gepoolten Kapazitätslizenzen automatisch vom NetScaler ADM Server ausgecheckt.

NetScaler Hochverfügbarkeitspaar

Bevor Sie beginnen, stellen Sie sicher, dass der NetScaler ADM Server als Lizenzserver konfiguriert ist. Weitere Informationen finden Sie unter Konfigurieren von NetScaler ADM als Lizenzserver.

Für NetScaler-Instanzen, die in einem Hochverfügbarkeitsmodus konfiguriert sind, müssen Sie die gepoolte Kapazität auf jedem Knoten des Hochverfügbarkeitspaars konfigurieren. Sowohl für den primären als auch für den sekundären Knoten müssen Sie Lizenzen mit derselben Kapazität zuweisen. Wenn Sie beispielsweise 1 Gbit/s Kapazität von jeder Instanz im HA-Paar benötigen, benötigen Sie die doppelte Kapazität (2 Gbit/s) aus dem gemeinsamen Pool. Dann können Sie jedem Knoten eine Kapazität von 1 Gbit/s zuweisen.

Um jedem Knoten im Paar eine Poollizenz zuzuweisen, folgen Sie den Schritten unter Zuweisen von gepoolten Lizenzen zu NetScaler-Instances. Weisen Sie zuerst die Lizenz dem ersten Knoten zu und wiederholen Sie dann die gleichen Schritte, um dem zweiten Knoten die Lizenz zuzuweisen.

Aktualisieren Sie eine unbefristete Lizenz in NetScaler VPX auf NetScaler Pooled Capacity

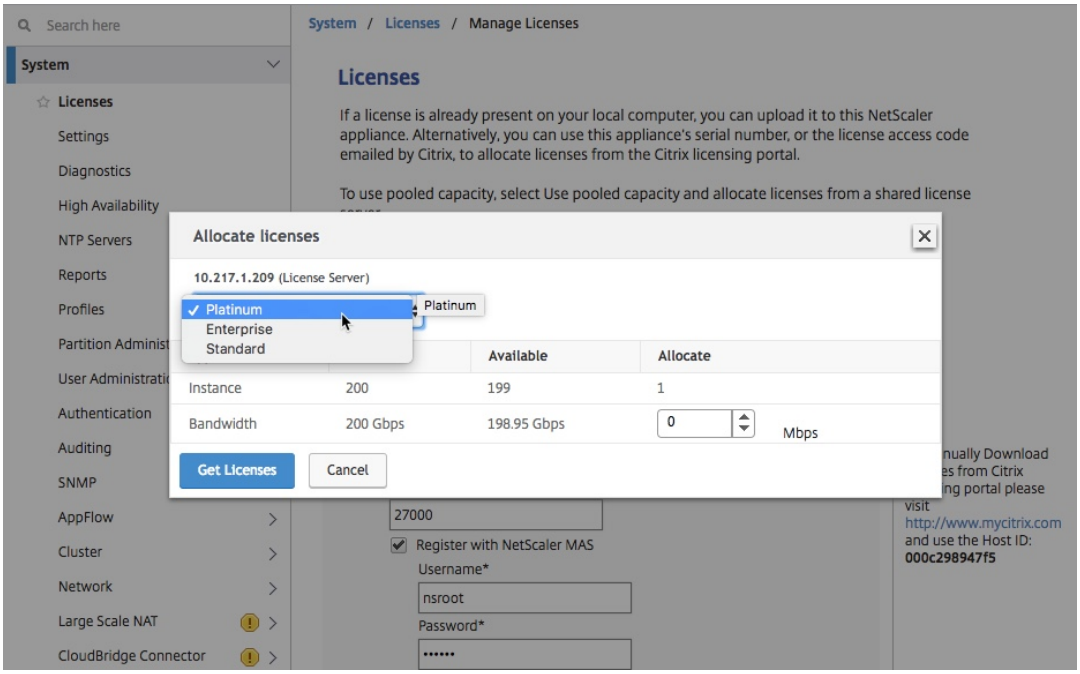
February 5, 2024

NetScaler VPX-Instances mit unbefristeter Lizenz können auf eine ADC Pooled-Kapazitätslizenz aktualisiert werden. Durch ein Upgrade auf eine gepoolte Kapazitätslizenz können Sie den VPX-Instanzen bei Bedarf Lizenzen aus dem Lizenzpool zuweisen. Sie können auch eine gepoolte Kapazitätslizenz für ADC-Instanzen konfigurieren, die in einem Hochverfügbarkeitsmodus konfiguriert sind. Informationen zur Konfiguration der gepoolten Kapazitätslizenz für VPX-Instances im Hochverfügbarkeitsmodus finden Sie unter Upgrading the Perpetual License in NetScaler VPX High Availability Pair auf NetScaler Pooled Capacity.

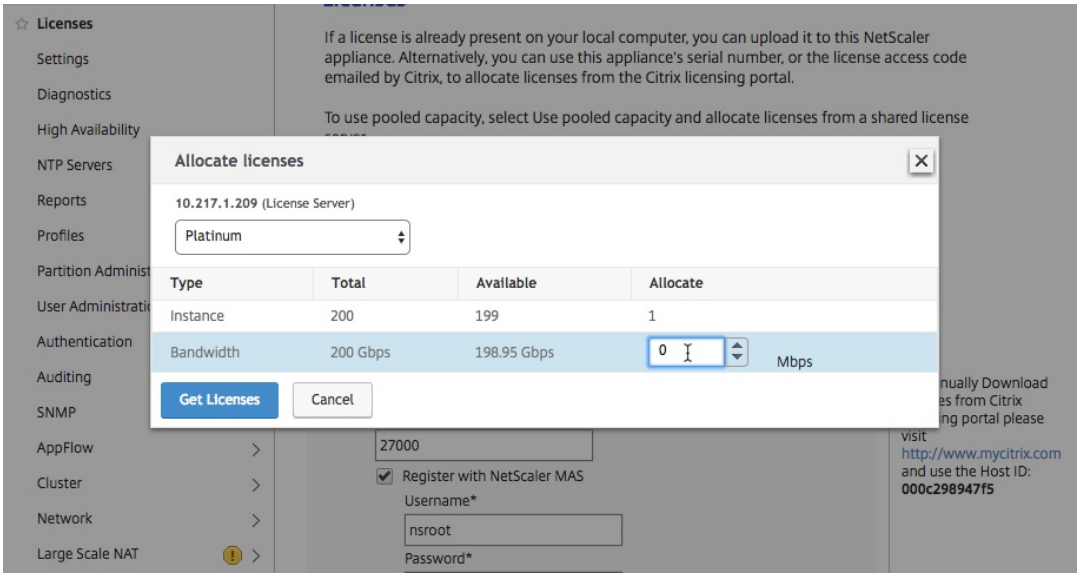
Voraussetzungen

So führen Sie ein Upgrade auf NetScaler Pooled-Kapazität durch:

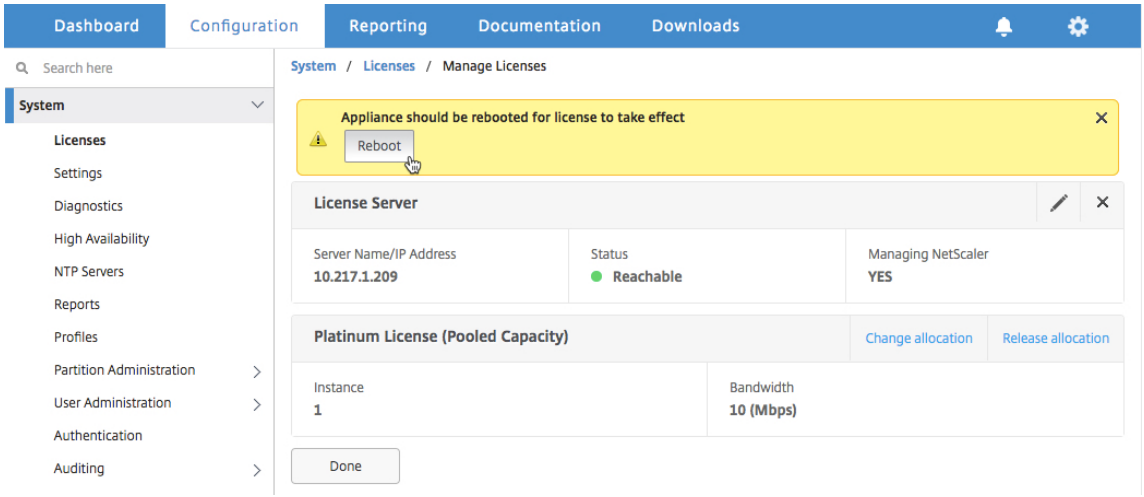
1. Geben Sie in einem Webbrowser die IP-Adresse der VPX-Instanz ein, z. http://192.168.100.1B.
2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der **Willkommensseite** auf **Weiter**.
4. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System > Lizenzen** und klicken Sie auf **Lizenzen verwalten** .
5. Klicken Sie auf der Seite **Lizenzen** auf **Neue Lizenz hinzufügen**.
6. Wählen Sie auf der Seite **Lizenzen** die Option **Remote-Lizenzierung verwenden** aus, und führen Sie die folgenden Schritte aus:
    a) Wählen Sie in der Dropdownliste **Remotelizenzierungsmodus** die Option **Pooled Licensing**.
    b) Geben Sie im Feld **Servername/IP-Adresse** die Details des Lizenzservers ein.
    c) Stellen Sie sicher, dass das Kontrollkästchen **Bei NetScaler ADM registrieren** aktiviert ist, und geben Sie die NetScaler ADM-Anmeldeinformationen ein, wenn Sie die Poollizenzen Ihrer Instanz über NetScaler ADM verwalten möchten.
    d) Klicken Sie auf **Weiter**.
7. Gehen Sie unter **Lizenzen zuweisen** wie folgt vor:
    a) Wählen Sie die Lizenzversion aus der Dropdownliste aus.



b) Weisen Sie der NetScaler Appliance im Menü **Zuweisen** die Bandbreite zu, und klicken Sie auf **Lizenzen abrufen**.



8. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Neu starten**, um die Appliance neu zu starten.



9. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
10. Nachdem die VPX-Instanz neu gestartet wurde, melden Sie sich bei der Instanz an. Klicken Sie auf der **Willkommensseite** auf **Weiter**.

    Auf der Seite **Lizenzen** werden alle Funktionen angezeigt, die auf der NetScaler VPX-Appliance lizenziert sind. Klicken Sie auf **X**.
11. Navigieren Sie zu **System > Lizenzen**, und klicken Sie auf **Lizenzen verwalten**.

    Auf der Seite **Lizenzen verwalten** können Sie die Details des Lizenzservers, der Lizenzedition und der zugewiesenen Bandbreite anzeigen.

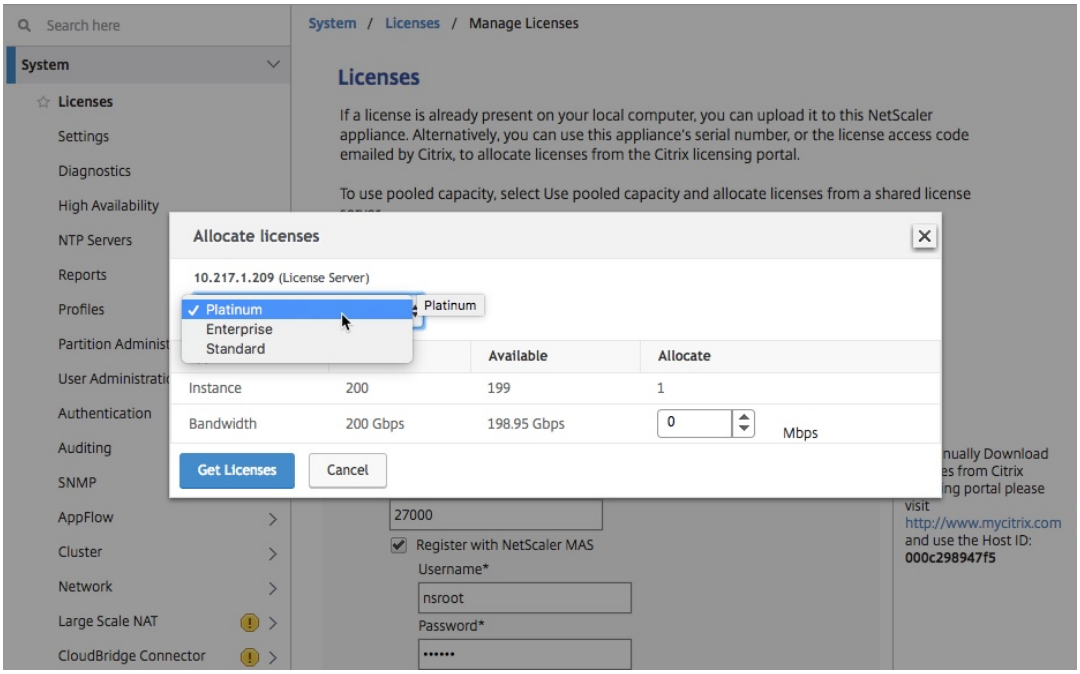
Aktualisieren Sie die unbefristete Lizenz im NetScaler VPX-Hochverfügbarkeitspaar auf NetScaler Pooled-Kapazität

Für VPX-Instanzen, die in einem Hochverfügbarkeitsmodus konfiguriert sind, müssen Sie die gepoolte Kapazität sowohl auf der primären als auch auf der sekundären Instanz im HA-Paar konfigurieren. Sowohl für die primäre als auch für die sekundäre Instanz müssen Sie Lizenzen mit derselben Kapazität zuweisen. Wenn Sie beispielsweise 1 Gbit/s Kapazität von jeder Instanz im HA-Paar benötigen, benötigen Sie die doppelte Kapazität (2 Gbit/s) aus dem gemeinsamen Pool. Anschließend können Sie den primären und sekundären Instanzen im HA-Paar jeweils 1 Gbit/s Kapazität zuweisen.

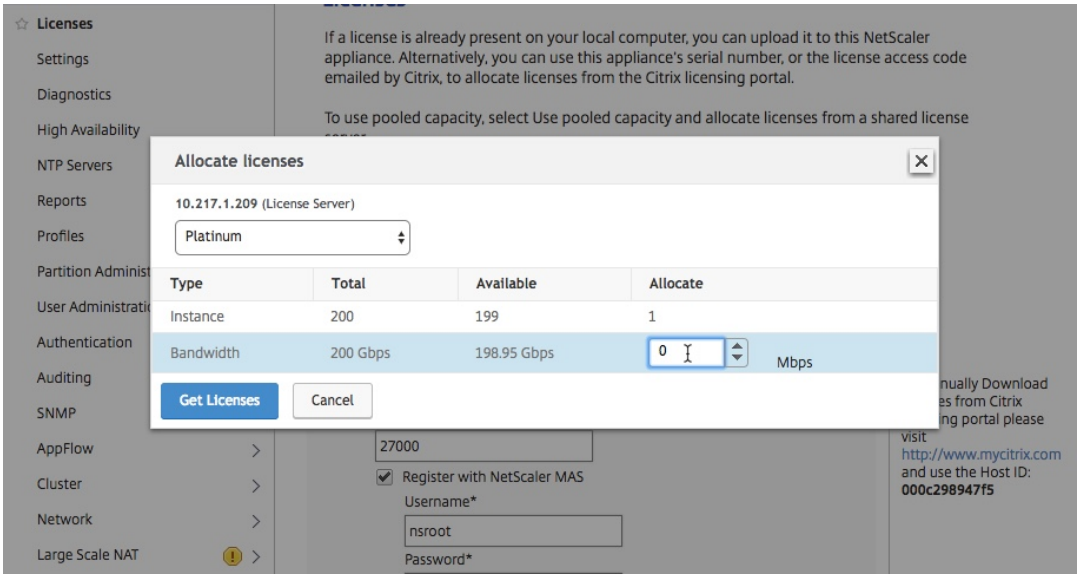
So aktualisieren Sie ein vorhandenes NetScaler VPX HA-Setup auf NetScaler Pooled Capacity:

1. Melden Sie sich bei der sekundären VPX-Instanz (Knoten 2) an. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler Appliance ein, `http://192.168.100.1`z.
2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der **Willkommensseite** auf **Weiter**.

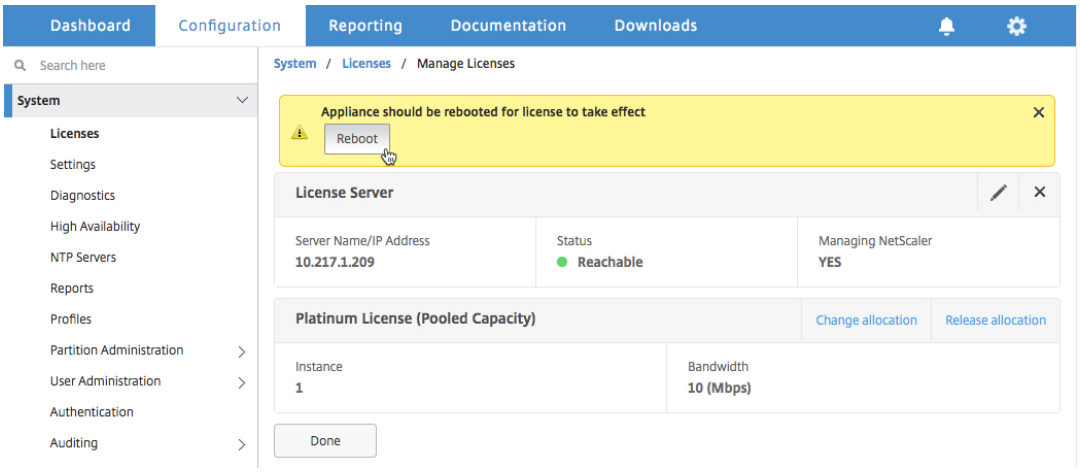
4. Navigieren Sie auf der Registerkarte Konfiguration zu **System > Lizenzen**, und klicken Sie auf **Lizenzen verwalten**.
5. Klicken Sie auf der Seite **Lizenzen** auf **Neue Lizenz hinzufügen**.
6. Wählen Sie **Remote-Lizenzierung verwenden** und gehen Sie wie folgt vor:
   a) Wählen Sie in der Dropdownliste **Remotelizenzierungsmodus** die Option **Pooled Licensing**.
   b) Geben Sie im Feld **Servername/IP-Adresse** die Details des Lizenzservers ein.
   c) Stellen Sie sicher, dass das Kontrollkästchen **Bei NetScaler ADM registrieren** aktiviert ist, und geben Sie die NetScaler ADM-Anmeldeinformationen ein, wenn Sie die Poollizenzen Ihrer Instanz über NetScaler ADM verwalten möchten.
   d) Klicken Sie auf **Weiter**.
7. Gehen Sie unter **Lizenzen zuweisen** wie folgt vor:
   a) Wählen Sie die Lizenzversion aus der Dropdownliste aus.



   b) Weisen Sie der NetScaler Appliance im Menü **Zuweisen** die Bandbreite zu, und klicken Sie auf **Lizenzen abrufen**.



c) Wenn Sie dazu aufgefordert werden, klicken Sie auf **Reboot**, um die Instanz



8. Klicken **Sie im Dialogfeld „Bestätigen** “auf **Ja**.

   Die VPX-Instanz wird neu gestartet.

   Wenn Sie dazu aufgefordert werden, klicken Sie auf **Neustart**, um die Appliance Nachdem die Appliance mit der neuen Lizenz in Betrieb genommen wurde, erzwingen Sie ein Failover, indem Sie eingeben `force ha failover`. Dieses Failover stellt sicher, dass das HA-Paar in gutem Zustand ist.

9. Melden Sie sich nach dem Failover bei der neuen sekundären VPX-Instanz (Knoten 1) an und wiederholen Sie denselben Vorgang, um die neue sekundäre Instanz zum Pool hinzuzufügen.

   Wenn Sie die primären und sekundären Instances im HA-Paar auf Ihre ursprüngliche HA-Paarkonfiguration ändern möchten, erzwingen Sie ein Failover. Führen Sie den folgenden Befehl für eine Instanz im HA-Paar aus:


```
  > force ha failover
<!--NeedCopy-->
```

10. Um zu überprüfen, ob die VPX-Instanz auf eine gepoolte Kapazitätslizenz aktualisiert wurde, melden Sie sich bei der primären und sekundären Instanz an und führen Sie die folgenden Schritte aus.

    a) Klicken Sie auf der **Willkommensseite** auf **Weiter**.

    b) Navigieren Sie auf der Registerkarte Konfiguration zu **System > Lizenzen**, und klicken Sie auf **Lizenzen verwalten**. Auf der Seite **Lizenzen verwalten** können Sie die Details des Lizenzservers, der Lizenzedition und der zugewiesenen Bandbreite anzeigen.

Upgrade einer unbefristeten Lizenz in NetScaler MPX auf NetScaler Pooled Capacity

February 5, 2024

NetScaler MPX mit unbefristeter Lizenz kann auf eine NetScaler Pooled Capacity-Lizenz aktualisiert werden. Wenn Sie auf die NetScaler Pooled-Capacity-Lizenz aktualisieren, können Sie Lizenzen aus dem Lizenzpool zu NetScaler-Appliances bei Bedarf zuweisen. Sie können auch eine NetScaler Pooled-Kapazitätslizenz für NetScaler-Instanzen konfigurieren, die im Hochverfügbarkeitsmodus konfiguriert sind. Informationen zum Konfigurieren der NetScaler Pooled Capacity-Lizenz für NetScaler MPX MPX-Instanzen im Hochverfügbarkeitsmodus finden Sie unter Upgrade der unbefristeten Lizenz im NetScaler MPX MPX-Hochverfügbarkeitspaar auf NetScaler Pooled-Kapazität.

> **Hinweis**
>
> Die Umwandlung von einer unbefristeten Lizenz in eine gepoolte Kapazitätslizenz ist ein einseitiger Prozess für den Lizenzanspruch. Sie können die Lizenz für gepoolte Kapazität nicht auf unbefristet zurücksetzen.
>
> **Wichtig!**
>
> Für ein Upgrade von NetScaler MPX auf eine NetScaler Pooled Capacity License müssen Sie die MPX-Z-Lizenz auf die Appliance hochladen.

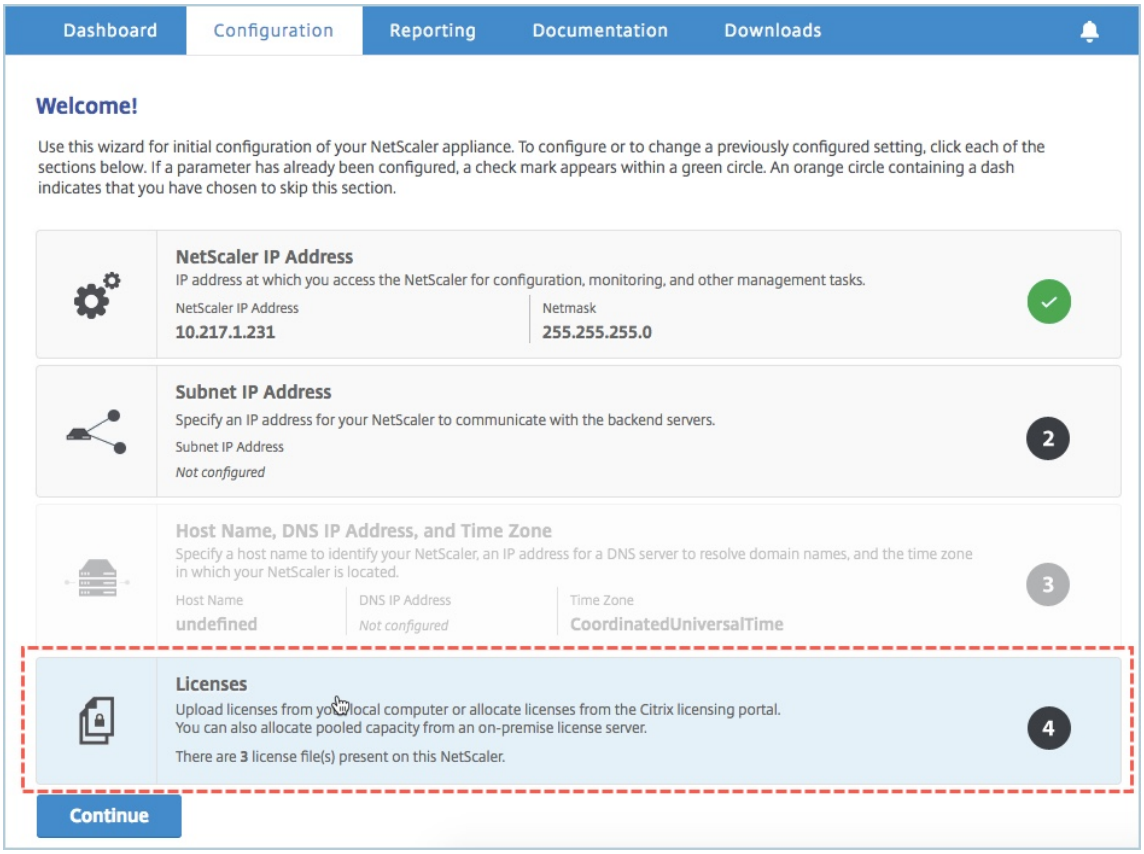
So führen Sie ein Upgrade auf NetScaler Pooled-Kapazität durch:

1. Geben Sie in einem Webbrowser die IP-Adresse des NetScaler ein, z. Bhttp://192.168.100.1.
2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der **Willkommensseite** auf **Weiter**.

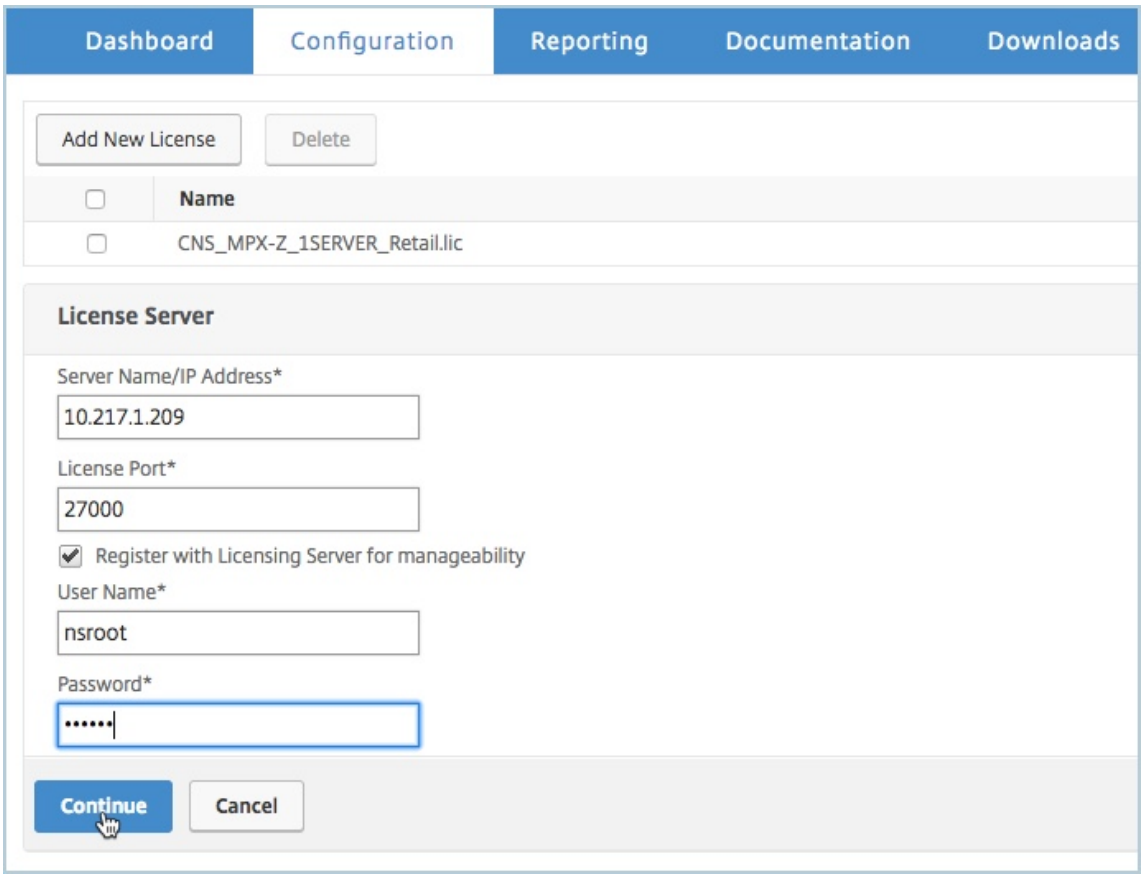
4. Laden Sie die Null-Kapazitätslizenz (MPX-Z-Lizenz) hoch. Navigieren Sie auf der Registerkarte Konfiguration zu **System** > **Lizenzen** .
5. Klicken Sie im Detailbereich auf **Lizenzen verwalten** und dann auf **Neue Lizenz** hinzufügen.
6. **Wählen Sie auf der Seite**Lizenzen**die Option Lizenzdateien hochladen** aus und klicken **Sie**auf Durchsuchen , um die Nullkapazitätslizenz von Ihrem lokalen Computer auszuwählen.
7. Klicken Sie nach dem Hochladen der Lizenz auf **Neu starten**, um die Appliance neu zu starten.

   > **Warnung**
   >
   > Nach der Anwendung der MPX-Z-Lizenz werden die Funktionen, einschließlich SSL-Offloading auf der Appliance, nicht lizenziert. Die Appliance beendet die Verarbeitung von HTTPS-Anforderungen.
   >
   > Wenn die Option **Nur sicherer Zugriff** auf der Appliance vor dem Upgrade aktiviert ist, können Sie über die NetScaler ADM-GUI mithilfe von HTTPS keine Verbindung zur Appliance herstellen.

8. Klicken Sie auf der Seite **Bestätigen** auf **Ja**.
9. Melden Sie sich nach dem Neustart der Appliance an.
10. Klicken Sie auf der Willkommensseite auf den Abschnitt **Lizenzen** .



11. Führen Sie im Abschnitt **Lizenzserver** die folgenden Schritte aus:



a) Geben Sie im Feld **Servername/IP-Adresse** die Details des Lizenzservers ein.

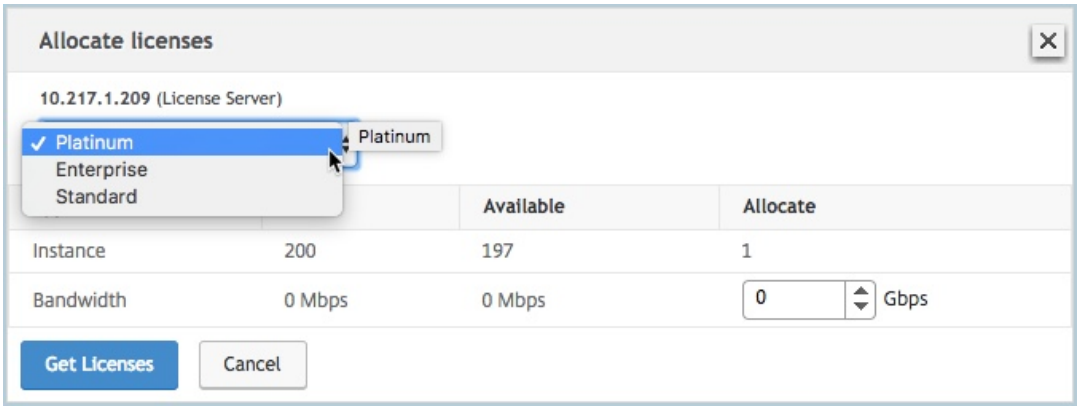
b) Geben Sie im Feld **Lizenzport** den Lizenzserver-Port ein. Standardwert: 27000.

c) Wenn Sie die Poollizenzen Ihrer Instanz über NetScaler ADM verwalten möchten, aktivieren Sie das Kontrollkästchen Zur **Verwaltbarkeit beim Lizenzserver registrieren und geben** Sie die NetScaler ADM-Anmeldeinformationen ein.

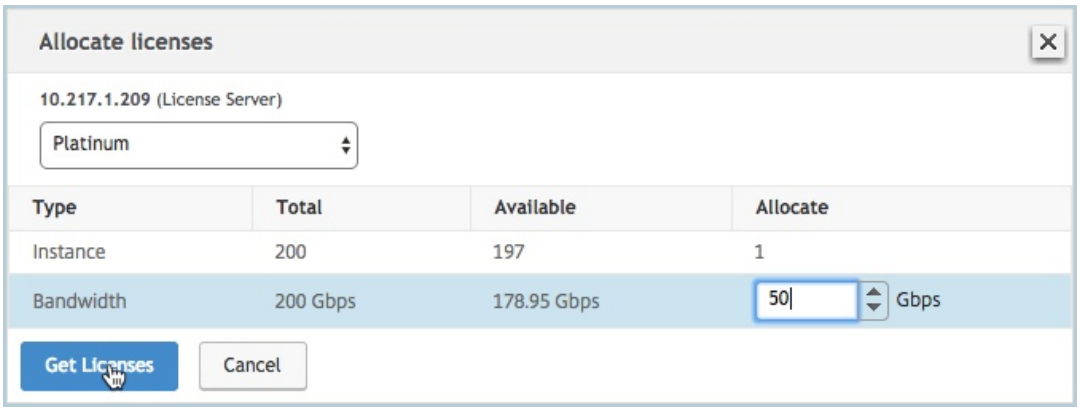
d) Klicken Sie auf **Weiter**.

12. Gehen Sie unter **Lizenzen zuweisen** wie folgt vor:

a) Wählen Sie die Lizenzversion aus der Dropdownliste aus.



b) Weisen Sie NetScaler im Menü **Zuweisen** die Bandbreite zu und klicken Sie auf **Lizenzen abrufen**.



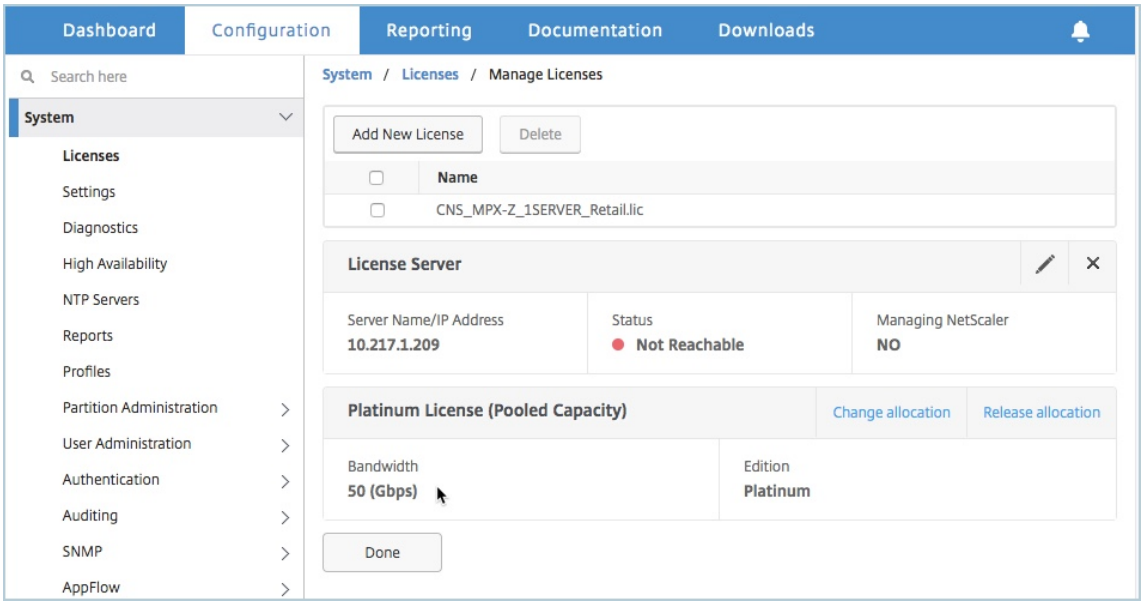
c) Wenn Sie dazu aufgefordert werden, klicken Sie auf **Neu starten**, um die Appliance neu zu starten.

13. Melden Sie sich nach dem Neustart von NetScaler MPX bei NetScaler MPX an. Klicken Sie auf der **Willkommensseite** auf **Weiter**.

    Auf der Seite **Lizenzen** werden alle lizenzierten Funktionen aufgelistet.

14. Navigieren Sie zu **System > Lizenzen**, und klicken Sie auf **Lizenzen verwalten**.

    Auf der Seite **Lizenzen verwalten** können Sie die Details des Lizenzservers, der Lizenzedition und der zugewiesenen Bandbreite anzeigen.



Aktualisierung der unbefristeten Lizenz im NetScaler MPX-Hochverfügbarkeitspaar auf NetScaler Pooled-Kapazität

Für die MPX-Appliances, die im Hochverfügbarkeitsmodus konfiguriert sind, müssen Sie die gepoolte Kapazität sowohl auf der primären als auch auf der sekundären NetScaler-Instanz im HA-Paar konfigurieren. Weisen Sie sowohl den primären als auch den sekundären NetScaler-Instanzen im HA-Paar Lizenzen mit derselben Kapazität zu. Wenn Sie beispielsweise 1 Gbit/s Kapazität von jeder Instanz im HA-Paar benötigen, müssen Sie 2 Gbit/s Kapazität aus dem gemeinsamen Pool zuweisen. Mit einer Kapazität von 2 Gbit/s können Sie den primären und sekundären NetScaler-Instanzen im HA-Paar jeweils 1 Gbit/s zuweisen.

> **Wichtig!**
>
> Um NetScaler MPX für die Verwendung der NetScaler Pooled-Kapazitätslizenz zu aktualisieren, müssen Sie den MPX-Z auf die Appliance hochladen.

Voraussetzungen

Stellen Sie sicher, dass Sie die MPX-Z-Lizenz sowohl auf die primäre als auch auf die sekundäre Instanz im HA-Paar hochladen.

So laden Sie die MPX-Z-Lizenz auf die NetScaler MPX-Instanzen im HA-Paar hoch:

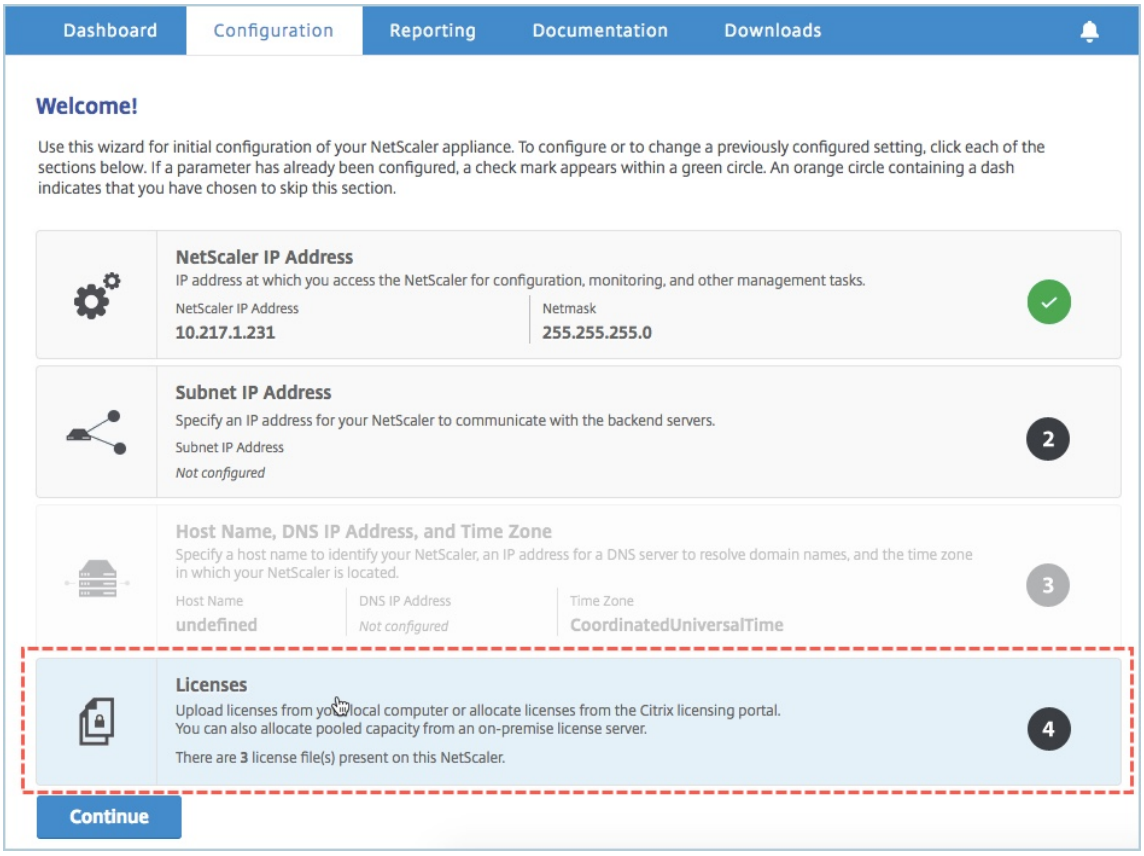
1. Geben Sie in einem Webbrowser die IP-Adresse der Appliance ein, z. http://192.168.100.1B.
2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der **Willkommensseite** auf **Weiter**.

4. Laden Sie die Null-Kapazitätslizenz (MPX-Z-Lizenz) hoch. Navigieren Sie auf der Registerkarte **Configuration** zu **System > Licenses**.
5. Klicken Sie im Detailbereich auf **Lizenzen verwalten** und dann auf **Neue Lizenz hinzufügen**.
6. **Wählen Sie auf der Seite**Lizenzen**die Option Lizenzdateien hochladen** aus und klicken **Sie**auf Durchsuchen , um die Nullkapazitätslizenz von Ihrem lokalen Computer auszuwählen.

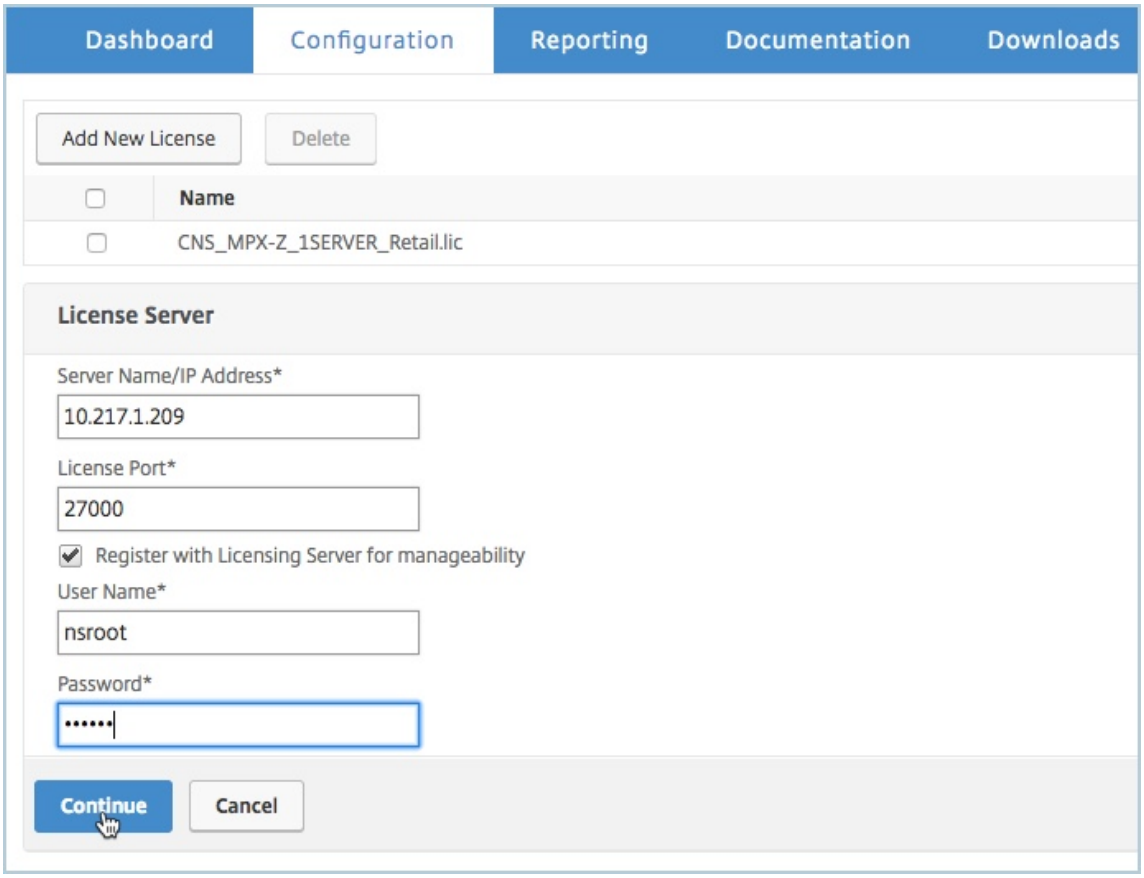
   Nach dem Hochladen der Lizenz werden Sie aufgefordert, die Appliance neu zu starten.
7. Klicken Sie auf **Neu starten**, um die Appliance neu zu starten.
8. Klicken Sie auf der Seite **Bestätigen** auf **Ja**.

So aktualisieren Sie ein vorhandenes HA-Setup auf NetScaler Pooled Capacity:

1. Melden Sie sich bei der sekundären NetScaler MPX-Instanz an. Geben Sie in einem Webbrowser die IP-Adresse von NetScaler ein, z. Bhttp://192.168.100.1.
2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der **Willkommensseite** auf den Abschnitt **Lizenzen**.



4. Führen Sie im Abschnitt **Lizenzserver** die folgenden Schritte aus:



a) Geben Sie im Feld **Servername/IP-Adresse** die Details des Lizenzservers ein.

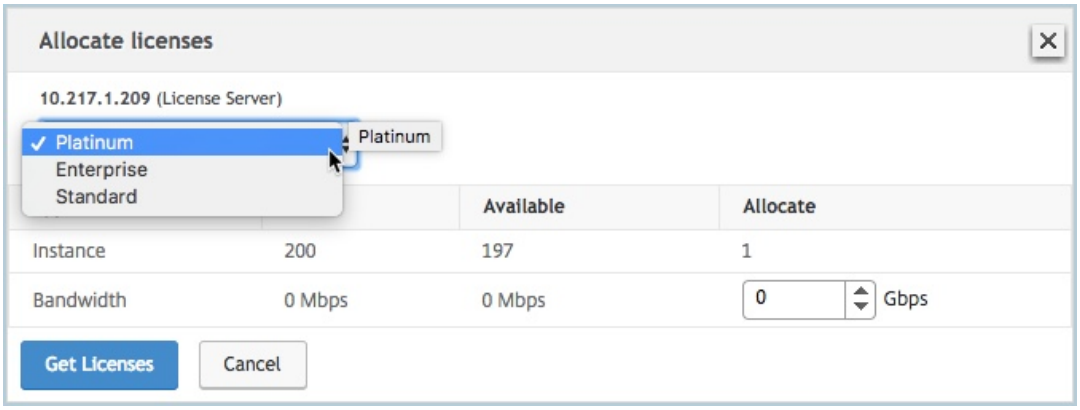
b) Geben Sie im Feld **Lizenzport** den Lizenzserver-Port ein. Standardwert: 27000.

c) Wenn Sie die Poollizenzen Ihrer Instanz über NetScaler ADM verwalten möchten, aktivieren Sie das Kontrollkästchen Zur **Verwaltbarkeit beim Lizenzserver registrieren und geben** Sie die NetScaler ADM-Anmeldeinformationen ein.

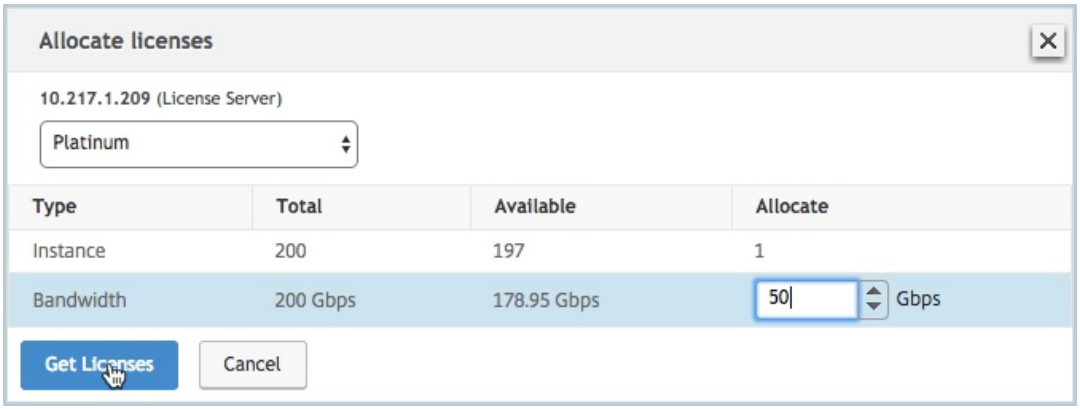
d) Klicken Sie auf **Weiter**.

5. Gehen Sie unter **Lizenzen zuweisen** wie folgt vor:

a) Wählen Sie die Lizenzversion aus der Dropdownliste aus.



b) Weisen Sie NetScaler im Menü **Zuweisen** die Bandbreite zu und klicken Sie auf **Lizenzen abrufen**.



c) Wenn Sie dazu aufgefordert werden, klicken Sie auf **Neustart**, um die Appliance Nachdem die Appliance mit der neuen Lizenz in Betrieb genommen wurde, erzwingen Sie ein Failover, indem Sie eingeben `force ha failover`. Dieses Failover stellt sicher, dass das HA-Paar in gutem Zustand ist.

6. Melden Sie sich beim vorhandenen primären NetScaler MPX an und starten Sie die Appliance neu. Führen Sie folgende Schritte aus:

   a) Geben Sie in einem Webbrowser die IP-Adresse des NetScaler ein, z. Bhttp://192.168.100.1.

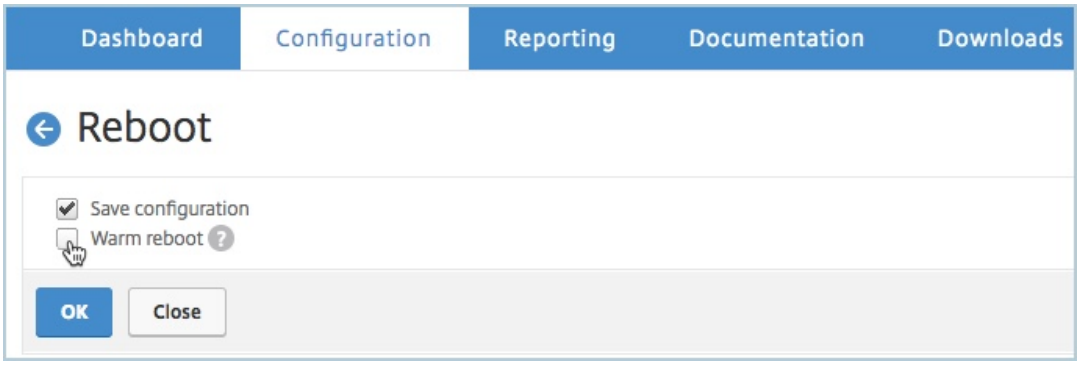
   b) Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein.

   c) Klicken Sie auf der **Willkommensseite** auf **Weiter**.

   d) Klicken Sie auf der Registerkarte **Konfiguration** auf **System**.

   e) Klicken Sie auf der Seite **System** auf **Neu starten**.

   f) Wählen Sie auf der Seite **Neustart** die Option **Warm reboot** aus, und klicken Sie auf **OK**.



Nach dem Neustart des primären NetScaler MPX wird es zum sekundären NetScaler MPX im HA-Paar. Wenn Sie die primären und sekundären Instances im HA-Paar auf Ihre ursprüngliche HA-Paarkonfiguration ändern möchten, erzwingen Sie ein Failover. Führen Sie den folgenden Befehl für eine Instanz im HA-Paar aus:

```
> force ha failover
<!--NeedCopy-->
```

Aktualisieren Sie eine unbefristete Lizenz in einem NetScaler SDX auf NetScaler Pooled Capacity

February 5, 2024

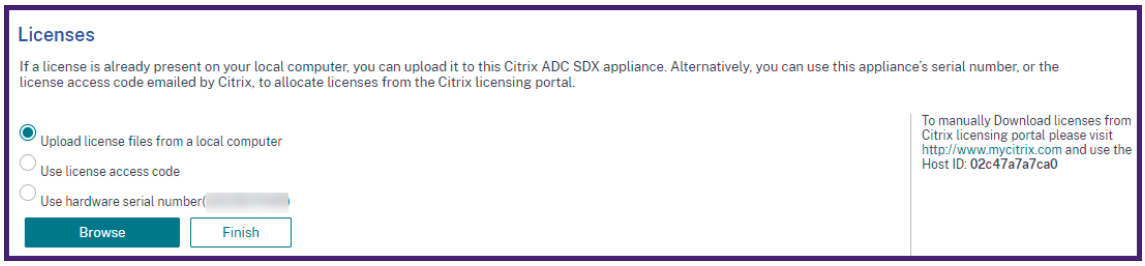
NetScaler SDX mit unbefristeter Lizenz kann auf eine NetScaler Pooled-Kapazitätslizenz aktualisiert werden. Durch ein Upgrade auf die NetScaler Pooled Capacity-Lizenz können Sie NetScaler bei Bedarf Lizenzen aus dem Lizenzpool zuweisen. Sie können auch eine NetScaler Pooled-Kapazitätslizenz für NetScaler-Instanzen konfigurieren, die im Hochverfügbarkeitsmodus konfiguriert sind.

> **Wichtig!**
>
> Die Umwandlung von einer unbefristeten Lizenz in eine gepoolte Kapazitätslizenz ist ein einseitiger Lizenzanspruch. Sie können die Lizenz für gepoolte Kapazität nicht wieder auf unbefristet zurücksetzen.
>
> - Für ein Upgrade von NetScaler SDX auf eine NetScaler Pooled Capacity-Lizenz müssen Sie die SDX-Z-Lizenz auf die Appliance hochladen.
> - Stellen Sie sicher, dass Sie die Berechtigung haben, NetScaler-Instanzen in NetScaler ADM hinzuzufügen.
> - Um sicherzustellen, dass die aktuellen Lizenzen nicht beeinträchtigt werden, muss der Kunde dieselbe Anzahl von Instanzen und dieselbe Bandbreite zuweisen, die im Rahmen

> der unbefristeten Lizenz verfügbar sind.

So führen Sie ein Upgrade auf NetScaler Pooled-Kapazität durch:

1. Geben Sie in einem Webbrowser die IP-Adresse von NetScaler SDX ein, z. http://192.168.100.1B.
2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der **Willkommensseite** auf **Weiter**.
4. Laden Sie die Lizenz ohne Kapazität hoch. Navigieren Sie auf der Registerkarte Konfiguration zu **System** > **Lizenzen** .
5. Klicken Sie auf der Seite **Lizenzen verwalten** auf **Lizenzdatei hinzufügen**.
6. **Wählen Sie auf der Seite**Lizenzen**die Option Lizenzdateien von einem lokalen Computer hochladen** aus und klicken **Sie**auf Durchsuchen , um die Nullkapazitätslizenz von Ihrem lokalen Computer auszuwählen. Klicken Sie dann auf **Finish**.



   Sobald die Nullkapazitätslizenz erfolgreich angewendet wurde, wird der Abschnitt **Gepoolte Lizenzen** auf der Seite **Lizenzen** angezeigt.

   > **Hinweis**
   >
   > Um die alte Lizenzdatei zu entfernen, müssen Sie Ihr NetScaler SDX nicht neu starten, damit es keine Ausfallzeiten gibt. Wenn Sie weitere Hilfe benötigen, wenden Sie sich an den NetScaler-Support .

7. Führen Sie im Abschnitt **Pooled Lizenzen** die folgenden Schritte aus:

   a) Geben Sie im Feld **Lizenzservername oder IP-Adresse** die Details des Lizenzservers ein.

      - Wenn Sie den NetScaler ADM Server als Lizenzserver konfigurieren möchten, geben Sie die IP-Adresse des NetScaler ADM Servers an.
      - Wenn Sie einen Agenten für die Kommunikation mit dem NetScaler ADM Server verwenden, geben Sie die IP-Adresse des NetScaler ADM Agents an.

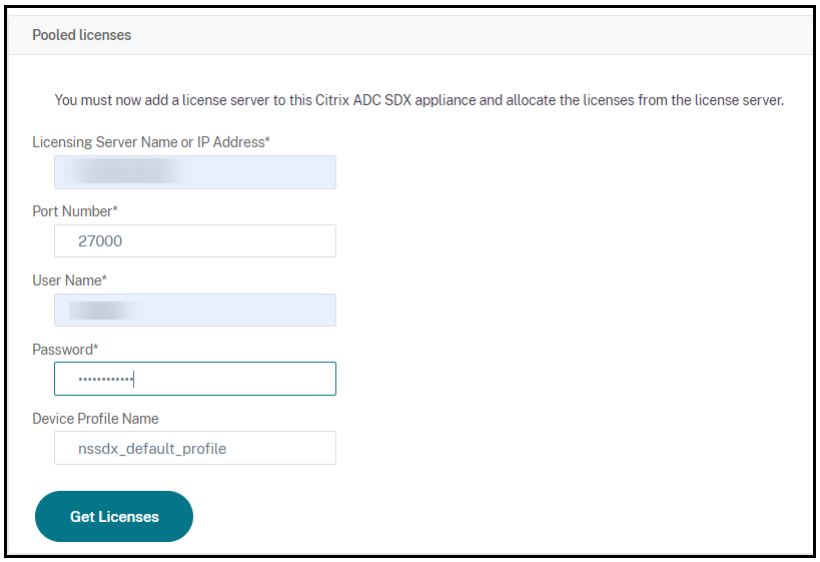
   b) Geben Sie im Feld **Portnummer** den Lizenzserverport ein. Standardwert: 27000.

   c) Geben Sie den **Benutzernamen** und das **Kennwort** des Lizenzservers an.

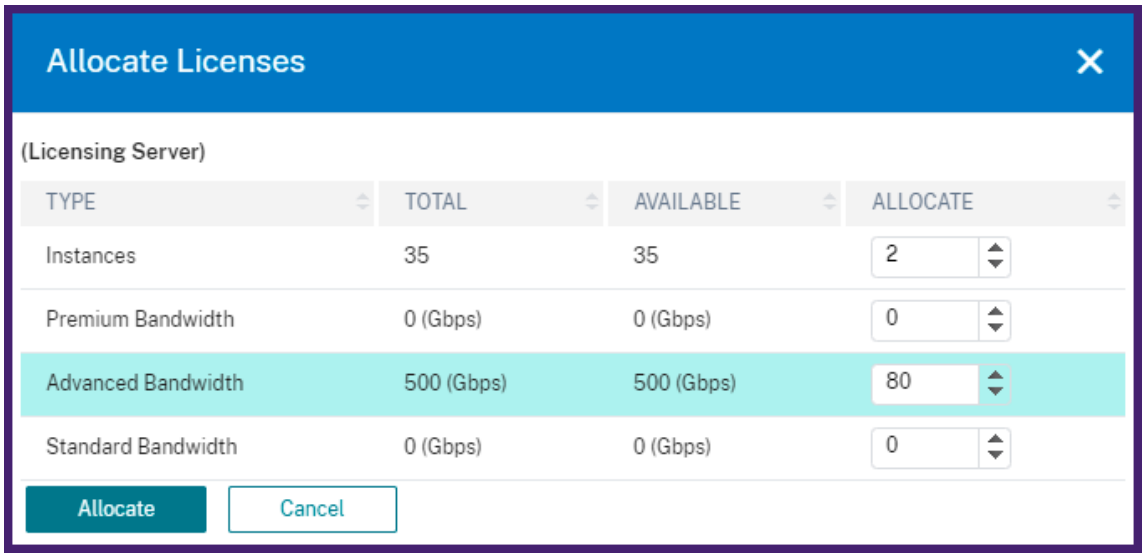
      - Geben Sie für den NetScaler ADM Server die Administratoranmeldedaten ein.

- Geben Sie für den NetScaler ADM Agent die Agent-Anmeldeinformationen ein.

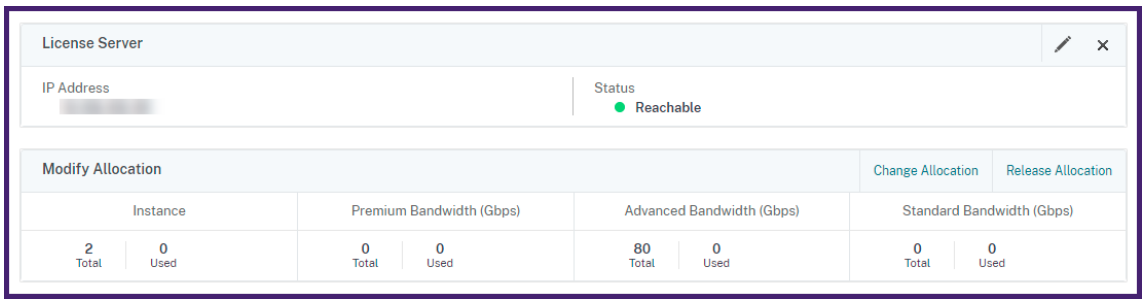
d) Klicken Sie auf **Get Licenses**.



8. Geben Sie im Fenster **Lizenzen zuweisen** die erforderlichen Instanzen und Bandbreite an, und klicken Sie auf **Zuweisen**.



Auf der Seite **Lizenzen verwalten** können Sie die Details des Lizenzservers, der Lizenz-Edition sowie der zugewiesenen Instanz und der Bandbreite aus dem Pool anzeigen.



> **Hinweis**
>
> Für das Upgrade einer unbefristeten Lizenz auf Pooled Capacity ist kein Neustart der SDX-Appliance erforderlich.

NetScaler Poolkapazität auf NetScaler-Instanzen im Clustermodus

February 5, 2024

Sie können NetScaler Pooled Capacity auf den als Cluster konfigurierten NetScaler-Instanzen konfigurieren. Im Folgenden sind die Voraussetzungen für die Konfiguration der gepoolten Kapazität auf NetScaler-Instanzen im Clustermodus aufgeführt:

- Instanzen werden einzeln in einem Lizenzmodus mit gepoolter Kapazität ausgeführt, um den Cluster zu bilden.
- Alle Instances müssen mit derselben Bandbreite ausgeführt werden.
- Alle Instanzen haben die gepoolte Kapazität aus derselben NetScaler Application Delivery and Management ausgecheckt.
- Neue Instanzen können einem vorhandenen NetScaler-Cluster nur hinzugefügt werden, wenn ihre Kapazität und NetScaler ADM-Konfigurationen mit denen der vorhandenen Instanzen im Cluster übereinstimmen.

Bei jedem Kapazitäts-Check-out aus dem NetScaler-Cluster wird allen Clusterknoten dieselbe Kapazität zugewiesen, und die Checkout-Bandbreite = bereitgestellte Bandbreite * Anzahl der Knoten.

Wenn Sie beispielsweise 50 Mbit/s Bandbreite vom NetScaler Cluster auschecken und der Cluster 12 Instanzen enthält, erhält jede Instanz automatisch 50 Mbit/s. Und 600 Mbit/s werden aus dem Pool ausgecheckt.

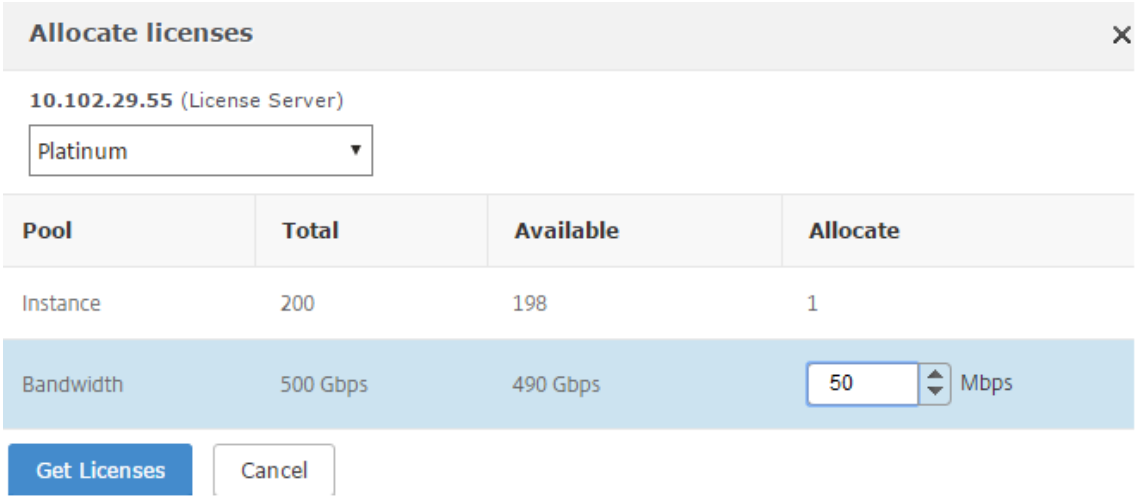
> **Hinweis**
>
> Wenn eine oder mehrere Instances im Cluster nicht mehr reagieren, verarbeitet der Cluster den Datenverkehr mit der Kapazität der verbleibenden Instances weiter.

Ordnen Sie einem ADC-Cluster ADC-Poolkapazität zu

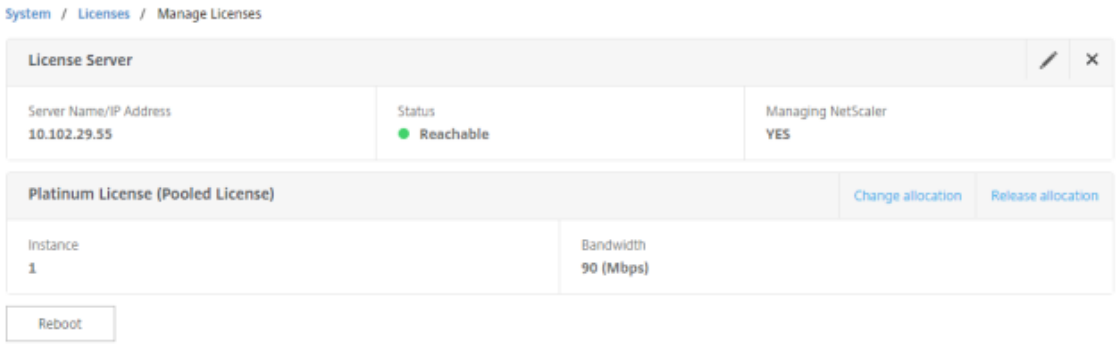
Weisen Sie jedem Clusterknoten Lizenzen separat zu. Weil die Befehle zur Weitergabe und Synchronisierung von Lizenzen zwischen den Clusterknoten deaktiviert sind.

Wiederholen Sie das folgende Verfahren auf jedem Clusterknoten:

1. Geben Sie in einem Webbrowser die NetScaler-IP-Adresse (NSIP) ein. Beispiel: `http://192.168.100.1`.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System > Lizenzen > Lizenzen verwalten** . Klicken Sie auf **Neue Lizenz hinzufügen** und wählen Sie **Pool-Lizenzierung verwenden** aus.
4. Geben Sie den Namen oder die Adresse des Lizenzservers in das Feld **Servername/IP-Adresse** ein.
5. Wenn Sie die Poollizenzen Ihrer Instanz über NetScaler ADM verwalten möchten, aktivieren Sie das Kontrollkästchen Zur Verwaltbarkeit **bei NetScaler ADM registrieren** und geben Sie die NetScaler ADM-Anmeldeinformationen ein.
6. Wählen Sie die Lizenzedition und die erforderliche Bandbreite aus, und klicken Sie auf **Lizenzen abrufen**.

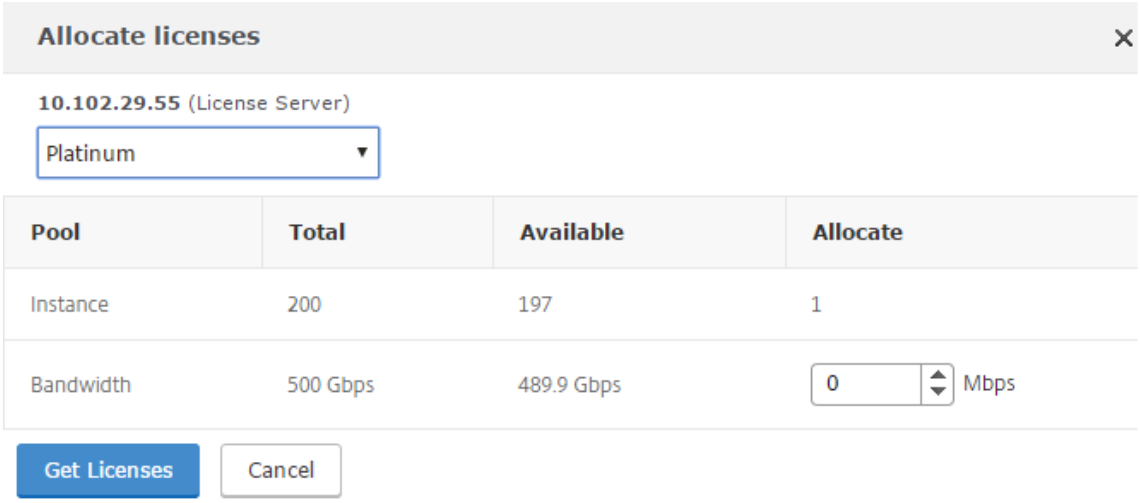


7. Sie können die Lizenzzuweisung ändern oder freigeben, indem Sie **Zuordnung ändern oder Zuordnungfreigeben**wählen.



8. Wenn Sie auf **Zuweisung ändern**klicken, werden in einem Popup-Fenster die auf dem Lizenzserver verfügbaren Lizenzen angezeigt.

> **Hinweis**
>
> Die Bandbreitenzuweisung muss ein integrales Vielfaches der minimalen Bandbreiteneinheit des entsprechenden Formfaktors sein.



9. Sie können der NetScaler Instanz Bandbreite oder Instanzen über die Dropdownliste **Zuweisen zuweisen**. Klicken Sie dann auf **Lizenzen holen**.
10. Sie können die Lizenzversion und die erforderliche Bandbreite aus den Dropdownlisten im Popup-Fenster auswählen.

> **Hinweis**
>
> Ein Neustart ist nicht erforderlich, wenn Sie die Bandbreitenzuweisung ändern, aber ein warmer Neustart ist erforderlich, wenn Sie die Lizenzversion ändern.

Weisen Sie einem ADC-Cluster mithilfe der CLI gepoolte ADC-Kapazität zu

Weisen Sie jedem Clusterknoten Lizenzen separat zu. Weil die Befehle zur Weitergabe und Synchronisierung von Lizenzen zwischen den Clusterknoten deaktiviert sind.

Wiederholen Sie das folgende Verfahren auf jedem Clusterknoten:

1. Geben Sie in einem SSH-Client die NetScaler-IP-Adresse (NSIP) 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 NetScaler VPX Appliance 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
```


Erwartete Verhaltensweisen, wenn Probleme auftreten

February 5, 2024

Im Folgenden ist das erwartete Verhalten der Lizenzserver und NetScaler-Instanzen aufgeführt, wenn bei ihnen die beschriebenen Probleme auftreten:

Der Lizenzserver reagiert nicht mehr

> **Warnung**
>
> Der Lizenzserver antwortet nicht. NetScaler arbeitet 30 Tage lang mit der aktuellen Kapazität. Wenn nach 30 Tagen die Konnektivität zum Lizenzserver nicht wiederhergestellt wird, verliert der NetScaler seine aktuelle Kapazität und stoppt die Verarbeitung des Datenverkehrs.

Wenn der Lizenzserver nicht mehr reagiert, gibt die NetScaler Instanz den Grace Period ein, bis die Konnektivität wiederhergestellt wird.

NetScaler Pooled Instance reagiert nicht mehr

Wenn die NetScaler Pooled-Instanz nicht mehr reagiert und sich der Lizenzserver in einem fehlerfreien Zustand befindet, checkt der Lizenzserver nach 10 Minuten alle Lizenzen der NetScaler-Instanz ein. Wenn die Instanz neu gestartet wird, sendet sie eine Aufforderung, alle Lizenzen vom Lizenzserver auszuchecken.

Sowohl der Lizenzserver als auch die NetScaler Pooled Instance reagieren nicht mehr

Wenn sowohl der Lizenzserver als auch die NetScaler Pooled-Instanz neu gestartet und die Verbindung wieder hergestellt wird, checkt der Lizenzserver alle seine Lizenzen nach 10 Minuten ein, und die NetScaler Pooled-Instanzen checken die Lizenzen automatisch aus, nachdem der Neustart abgeschlossen ist.

Die NetScaler Pooled-Instanz wird ordnungsgemäß heruntergefahren

Während eines ordnungsgemäßen Herunterfahrens können Sie die Lizenzen einchecken oder die Lizenzen beibehalten, die vor dem ordnungsgemäßen Herunterfahren zugewiesen wurden. Wenn Sie die Lizenzen in der NetScaler Pooled-Instanz überprüfen möchten, ist sie nach dem Neustart nicht lizenziert. Wenn Sie die Lizenzen beibehalten möchten, werden sie beim Herunterfahren der Instanz beim Lizenzierungsserver eingecheckt. Nach dem Neustart der Instanz stellt sie die Verbindung

mit dem Lizenzserver wieder her und checkt die Lizenzen wie in der gespeicherten Konfiguration angegeben aus.

Wenn das System neu gestartet wird und das Auschecken fehlschlägt, weil im Pool keine Kapazität verfügbar ist, überprüft NetScaler das Inventar der NetScaler Application Delivery and Management-Poollizenzen und checkt alle verfügbaren Kapazitäten aus. Ein SNMP-Alarm wird ausgelöst, um diesen Zustand dem Benutzer mitzuteilen, wenn der NetScaler nicht mit voller Kapazität gemäß der Konfiguration ausgeführt wird. Wenn im Bandbreitenpool keine Kapazität verfügbar ist, wird die Pool-Instance nicht mehr lizenziert.

Netzwerk verliert Konnektivität

> **Fehlermeldung (Syslog)**
>
> Der Lizenzserver reagiert nicht.

Wenn sich der Lizenzserver und die NetScaler Pooled-Instances in einem fehlerfreien Zustand befinden, die Netzwerkkonnektivität jedoch unterbrochen wird, arbeiten die Instances 30 Tage lang mit ihrer aktuellen Kapazität weiter. Wenn die Konnektivität zum Lizenzserver nach 30 Tagen nicht wiederhergestellt wird, verlieren die Instanzen ihre Kapazität und beenden die Verarbeitung des Datenverkehrs, und der Lizenzserver checkt alle Lizenzen ein. Nachdem der Lizenzserver die Verbindung mit den NetScaler Instanzen wiederhergestellt hat, checken die Instanzen die Lizenzen erneut aus.

Kulanzzeitraum

Wenn sich eine NetScaler Pooled-Instanz in einem fehlerfreien Zustand befindet und der Lizenzserver nicht mehr reagiert, arbeitet die Instanz 30 Tage lang mit der aktuellen Kapazität weiter. Wenn die Konnektivität zum Lizenzserver nach 30 Tagen nicht wiederhergestellt wird, verliert die Instanz ihre Kapazität und beendet die Verarbeitung des Datenverkehrs.

Szenarien für den Ablauf von flexiblen oder gepoolten Lizenzen und das Verhalten bei Verbindungsproblemen

February 5, 2024

In diesem Dokument werden verschiedene Szenarien des Ablaufs der Lizenz und des Verhaltens von Verbindungsproblemen in NetScaler MPX, NetScaler SDX und NetScaler VPX/NetScaler BLX/NetScaler CPX vorgestellt.

Arten von Flexed-Lizenzen

- Softwareinstanz (VPX/BLX/CPX, SDX, MPX, VPX FIPS)
- Bandbreitenkapazität

MPX FIPS verwendet eine Lizenz aus dem MPX-Softwarepool. SDX FIPS verwendet eine Lizenz aus dem SDX-Softwarepool. VPX FIPS verwendet eine Lizenz aus dem VPX FIPS-Softwarepool.

Szenario: MPX-Formfaktor

Sie verwenden die Flexed/Pooled-Lizenzierung und die Lizenzen laufen bald ab. Die folgenden Szenarien erläutern das Verhalten, wenn eine neue Lizenz vor und nach Ablauf der Laufzeit auf NetScaler Application Delivery and Management hochgeladen wird oder wenn keine Lizenzdatei vorhanden ist.

Vor Ablauf der Laufzeit

Wenn die neue Lizenz vor Ablauf der Laufzeit hochgeladen wird und die alte Lizenz noch gültig ist, sind zwei verschiedene Kapazitätspools (alt und neu) verfügbar.

- Wenn NetScaler läuft, wechselt es nahtlos zur neuen Flexed/Pooled-Lizenz, nachdem die alte Lizenz abgelaufen ist.
- Ein Neustart ist nicht erforderlich.
- NetScaler erfordert keine manuelle Neukonfiguration der Kapazität.

Nach Ablauf der Laufzeit

In diesem Fall ist der bestehende Kapazitätspool abgelaufen.

- NetScaler läuft lizenziert weiter, bis es neu gestartet wird.
- Wenn NetScaler neu gestartet wird und keine gültige Lizenzdatei vorhanden ist, wird die Lizenz aufgehoben.
- Wenn NetScaler aktiv bleibt, um die neue Lizenz abzuholen, muss sie manuell neu konfiguriert werden (Kapazität neu zugewiesen).

Szenario: SDX-Formfaktor

Sie verwenden die Flexed/Pooled-Lizenzierung und die Lizenzen laufen bald ab. Die folgenden Szenarien erläutern das Verhalten, wenn eine neue Lizenz vor und nach Ablauf der Laufzeit auf NetScaler Application Delivery and Management hochgeladen wird oder wenn keine Lizenzdatei vorhanden ist.

Vor Ablauf der Laufzeit

Wenn die neue Lizenz vor Ablauf der Laufzeit hochgeladen wird und die alte Lizenz noch gültig ist, sind zwei verschiedene Kapazitätspools (alt und neu) verfügbar.

- Wenn NetScaler läuft, wechselt es nahtlos zur neuen Flexed/Pooled-Lizenz, nachdem die alte Lizenz abgelaufen ist.
- Ein Neustart ist nicht erforderlich.
- NetScaler erfordert keine manuelle Neukonfiguration der Kapazität.

Nach Ablauf der Laufzeit

In diesem Fall ist der bestehende Kapazitätspool abgelaufen.

- NetScaler läuft lizenziert weiter, bis es neu gestartet wird.
- Wenn der Management Service neu gestartet wird und keine gültige Lizenzdatei vorhanden ist, wird der Durchsatz aller VPX auf 1 Mbit/s reduziert.
- Wenn der Management Service aktiv bleibt, um die neue Lizenz abzuholen, muss er manuell neu konfiguriert werden (Kapazität neu zugewiesen).

Szenario: VPX/BLX/CPX-Formfaktor

Sie verwenden die Flexed/Pooled-Lizenzierung und die Lizenzen laufen bald ab. Die folgenden Szenarien erläutern das Verhalten, wenn eine neue Lizenz vor und nach Ablauf der Laufzeit auf NetScaler Application Delivery and Management hochgeladen wird oder wenn keine Lizenzdatei vorhanden ist.

Vor Ablauf der Laufzeit

Wenn die neue Lizenz vor Ablauf der Laufzeit hochgeladen wird und die alte Lizenz noch gültig ist, sind zwei verschiedene Kapazitätspools (alt und neu) verfügbar.

- Wenn NetScaler läuft, wechselt es nahtlos zur neuen Flexed/Pooled-Lizenz, nachdem die alte Lizenz abgelaufen ist.
- Ein Neustart ist nicht erforderlich.
- NetScaler erfordert keine manuelle Neukonfiguration der Kapazität.

Nach Ablauf der Laufzeit

In diesem Fall ist der bestehende Kapazitätspool abgelaufen.

- NetScaler läuft lizenziert weiter, bis es neu gestartet wird.

- Wenn NetScaler neu gestartet wird und keine gültige Lizenzdatei vorhanden ist, werden VPX und BLX nicht mehr lizenziert und CPX wird zu CPX Express.
- Wenn NetScaler aktiv bleibt, um die neue Lizenz abzuholen, muss sie manuell neu konfiguriert werden (Kapazität neu zugewiesen).

Zusammenfassung

Die folgende Tabelle fasst das Verhalten aller NetScaler-Formfaktoren zusammen, wenn keine neue Lizenz für NetScaler Application Delivery and Management angewendet wird:

Formfaktor	Nach Ablauf der Lizenz	Nach dem Neustart von NetScaler
VPX/BLX	Läuft bis zum Neustart weiter	VPX/BLX wird nicht lizenziert
CPX	Läuft bis zum Neustart weiter	CPX wird CPX Express
MPX	Läuft bis zum Neustart weiter	MPX wird nicht lizenziert
SDX	Läuft bis zum Neustart weiter	Der Durchsatz aller VPX wird auf 1 Mbit/s reduziert (wodurch sie unbrauchbar werden)

Szenarien für das Verhalten bei Verbindungsproblemen

Wenn die Konnektivität zwischen NetScaler und NetScaler Application Delivery and Management auf dem lokalen Server unterbrochen wird, ist das Verhalten wie folgt:

- NetScaler wird für 30 Tage in Betrieb genommen.
- Während dieser Nachfrist funktioniert die Lizenzierungsfunktion bis zum dreißigsten Tag weiter.
- Am einunddreißigsten Tag
  - NetScaler VPX/NetScaler CPX/NetScaler BLX und NetScaler MPX werden einem erzwungenen Neustart unterzogen und verlieren ihre Lizenz.
  - Der Durchsatz auf allen VPX auf NetScaler SDX wird auf 1 Mbit/s reduziert.

Konfigurieren Sie den NetScaler Application Delivery and Management Server als flexiblen oder gepoolten Lizenzserver

February 5, 2024

Als Administrator können Sie den NetScaler Application Delivery and Management Server nur als Flexen- oder Pool-Lizenzserver konfigurieren. Bei dieser Konfiguration empfängt der NetScaler ADM Server nur Lizenzdaten von NetScaler-Instanzen.

Manchmal haben Sie möglicherweise das regulatorische Mandat, das es vorschreibt, die Daten von NetScaler-Instanzen daran zu hindern, die regulatorische Zone zu verlassen. In solchen Situationen können Sie eine lokale Instanz des ADM-Servers vor Ort in Ihrer regulatorischen Zone bereitstellen, um die Verwaltungs-, Überwachungs- und Analysefunktionen zu nutzen. Wenn Sie dieselbe Methode verwenden, um die Funktion für flexible oder gepoolte Lizenzen zu verwenden, müssen Sie Flexe- oder Pool-Lizenzen auf verschiedene NetScaler ADM-Lizenzserver aufteilen. Dieser Ansatz bietet Ihnen nicht die Flexibilität, Flexe- oder Pool-Lizenzen Ihren global bereitgestellten NetScaler-Instances zuzuweisen.

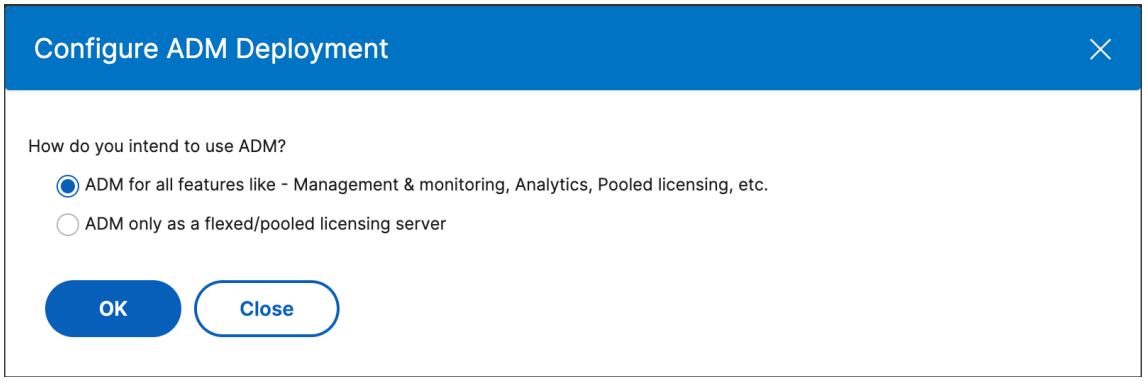
Konfigurieren Sie den NetScaler ADM Server daher nur als Flexe- oder Pool-Lizenzserver. Der NetScaler ADM Server empfängt nur Lizenzdaten von allen NetScaler-Instanzen. So können Sie die regulatorischen Vorgaben einhalten und flexible oder gepoolte Kapazitätslizenzen dynamisch auf global eingesetzte NetScaler-Instances verteilen.

So konfigurieren Sie den NetScaler ADM Server nur als Flexing- oder Pooled-Lizenzserver

Bevor Sie beginnen, stellen Sie sicher, dass dem NetScaler ADM Server keine NetScaler-Instanzen hinzugefügt werden. Fügen Sie NetScaler-Instanzen erst hinzu, nachdem Sie Schritt 4 abgeschlossen haben.

Gehen Sie wie folgt vor, um den NetScaler ADM Server nur für den Flexing- oder Pooled-Lizenzserver zu konfigurieren:

1. Navigieren Sie zu **Einstellungen > Administration**.
2. Wählen Sie im Abschnitt “**Systemkonfigurationen** “die Option **Systembereitstellung**aus.
3. Wählen Sie in **ADM Deployment** die Option **ADM only als flexiblen/gepoolten** Lizenzserver aus.



4. Klicken Sie auf **OK**.

   Bei dieser Aktion wird nur die Funktion für die flexible oder gepoolte Lizenzierung beibehalten und die folgenden NetScaler ADM-Funktionen deaktiviert:

   - NetScaler ADM-Backup
   - Ereignisverwaltung
   - SSL Zertifikatsverwaltung
   - Netzwerkberichterstellung
   - Netzwerkfunktionen
   - Konfigurationsaudit

   > **Hinweis**
   >
   > Die NetScaler ADM-Analysefunktion ist standardmäßig deaktiviert. Stellen Sie sicher, dass Sie diese Funktion deaktivieren, wenn Sie sie aktiviert haben.

   Klicken Sie im Bestätigungsfeld auf **Ja**.

   Die NetScaler ADM GUI zeigt jetzt nur noch die Funktion Flexe oder Pooled Licensing an. Und die übrigen Funktionen werden nicht angezeigt.

5. Nachdem Sie NetScaler ADM nur für die Lizenzierungsfunktion konfiguriert haben, fügen Sie NetScaler-Instanzen auf der Seite **Infrastruktur > Instanzen** hinzu.

> **Hinweis**
>
> - Sie können eine NetScaler-Instanz auf einem oder mehreren NetScaler ADM-Servern hinzufügen. Wenn Sie das Kennwort solcher NetScaler-Instanzen ändern, stellen Sie sicher, dass Sie das Kennwort auf allen NetScaler ADM-Servern aktualisieren, auf denen die Instanz erkannt wurde.
> - Ein Benutzer kann weiterhin einige Operationen mit den deaktivierten Funktionen in der NetScaler ADM GUI ausführen. Zum Beispiel Event-Polling und NetScaler-Backup. Wenn Sie als Superadministrator solche Operationen einschränken möchten, deaktivieren Sie den Benutzerzugriff für andere Administratoren mithilfe einer entsprechenden Zugriffsrichtlinie. Weitere Informationen finden Sie unter Konfigurieren von Zugriffsrichtlinien in NetScaler ADM.

NetScaler VPX- und NetScaler BLX-Lizenzen ein und auschecken

February 5, 2024

Sie können NetScaler VPX- und NetScaler BLX-Lizenzen NetScaler-Instanzen bei Bedarf von NetScaler Application Delivery and Management aus zuweisen. Die NetScaler ADM-Software speichert und verwaltet die Lizenzen, die über ein Lizenzierungsframework verfügen, das eine skalierbare und automatisierte Lizenzbereitstellung ermöglicht. Eine Instanz kann die Lizenz von NetScaler ADM auschecken, wenn sie bereitgestellt wird. Wenn eine Instanz entfernt oder zerstört wird, überprüft die Instanz ihre Lizenz an die NetScaler ADM -Software zurück.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Sie verwenden ein NetScaler VPX-Image, auf dem die Softwareversion 12.0 ausgeführt wird. Zum Beispiel: nsvpx-ESX-12.0-xx.xx_NC.zip
- Sie haben NetScaler ADM mit Version 12.0 installiert. Zum Beispiel: MAS-ESX-12.0-xx.xx.zip

> **Hinweis**
>
> Um bestehende NetScaler VPX-Lizenzen von NetScaler ADM zu verwalten, müssen Sie die Lizenzen auf NetScaler ADM neu hosten.

Lizenzen in NetScaler ADM installieren

> **Hinweis Bevor Sie**
>
> Lizenzen installieren, starten Sie die virtuelle NetScaler ADM-Appliance neu, falls Sie die Software-Edition oder die Bandbreite geändert haben.

So installieren Sie Lizenzdateien auf NetScaler ADM:

1. Geben Sie in einem Webbrowser die IP-Adresse des NetScaler ADM ein (z. B. http://192.168.100.1).
2. Geben Sie unter Benutzername und Kennwort die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu**Infrastruktur > Gepoolte Lizenzierung**.
4. 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 NetScaler ADM hochladen. Um Lizenzdateien hinzuzufügen, klicken Sie auf **Durchsuchen** und wählen Sie die Lizenzdatei (.lic) aus, die Sie hinzufügen möchten. Dann klick **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.

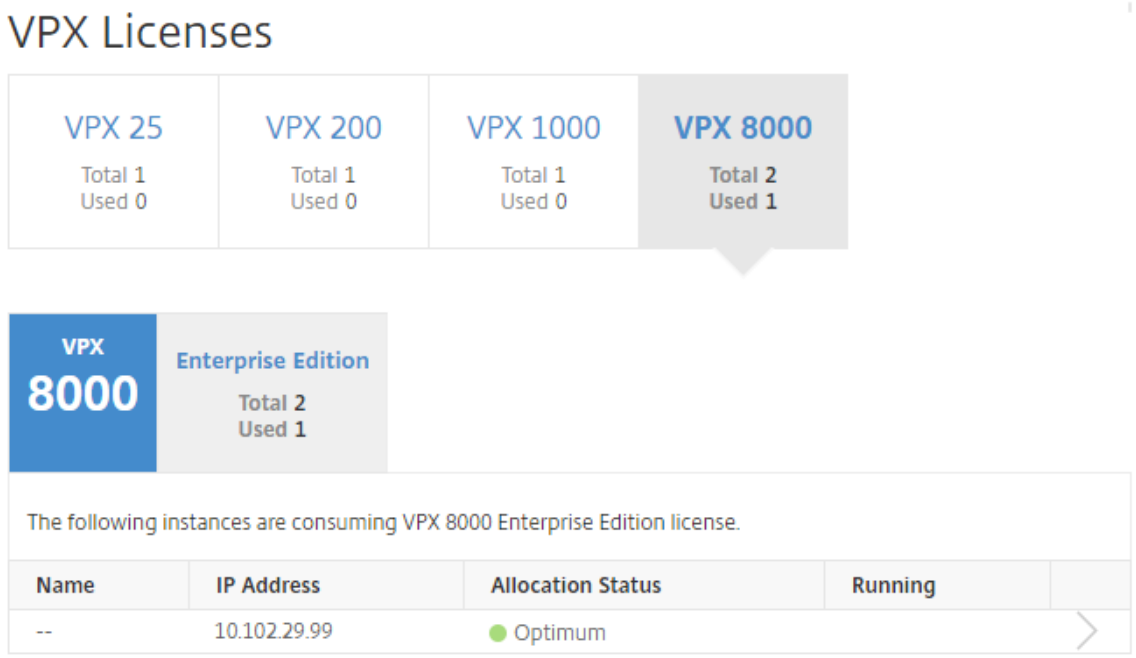
Auf der Seite mit den **Lizenzeinstellungen** können Sie dem NetScaler ADM jederzeit weitere Lizenzen hinzufügen.

Verifizierung

Sie können die verfügbaren und zugewiesenen Lizenzen in der NetScaler ADM-GUI einsehen.

Um die Lizenzen anzuzeigen:

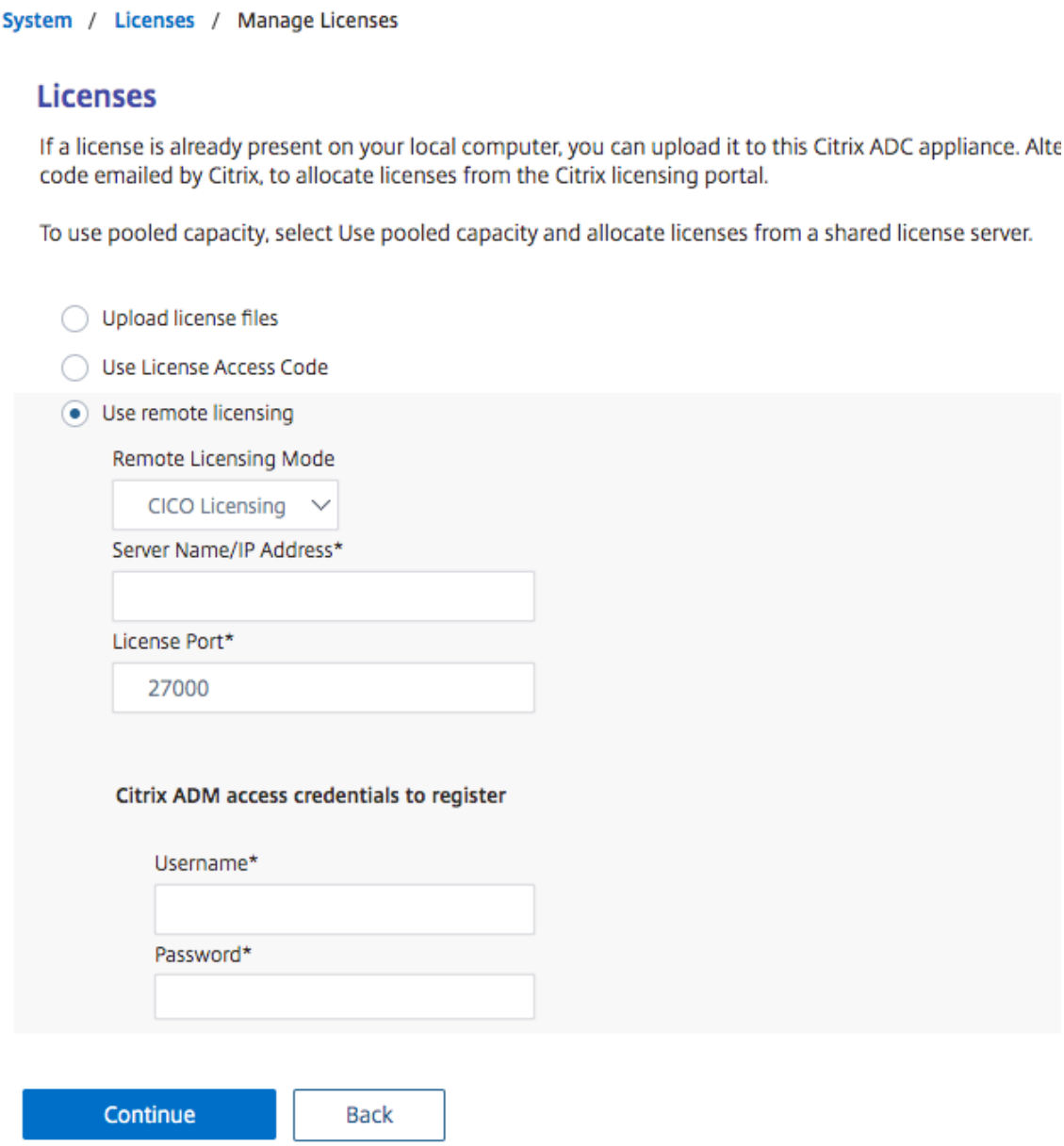
1. Geben Sie in einem Webbrowser die IP-Adresse von NetScaler ADM ein (z. B.http://192.168.100.1).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte Konfiguration zu **Infrastruktur > Gepoolte Lizenzierung > VPX-Lizenzen**.



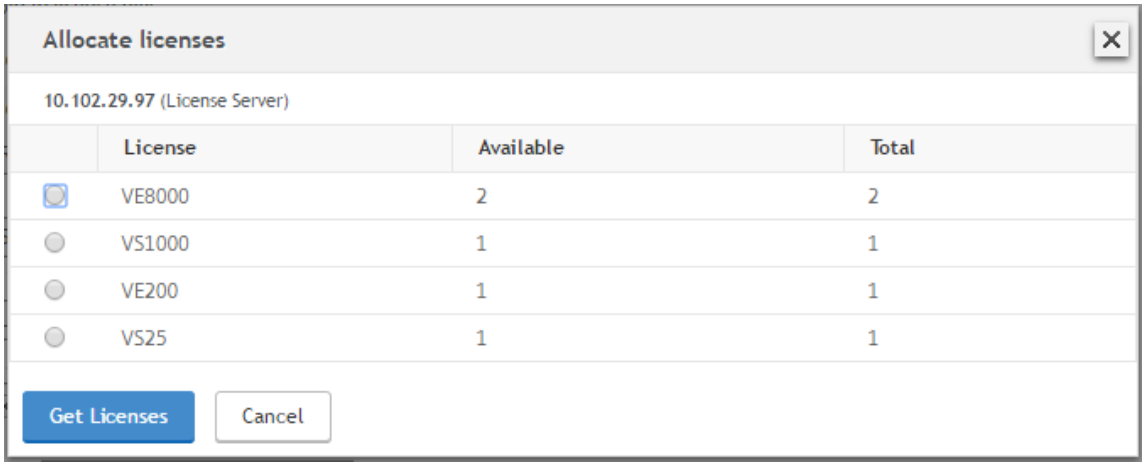
4. Sie können die zugewiesenen Lizenzen in der Tabelle im Abschnitt Verfügbare Lizenzen anzeigen.

NetScaler VPX- und NetScaler BLX-Lizenzen mit der NetScaler-GUI einer NetScaler-Instanz zuweisen

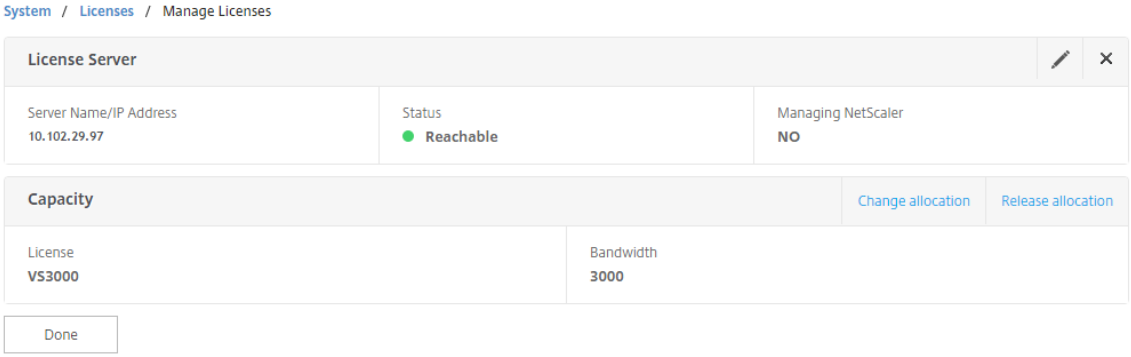
1. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler Instanz ein (z. B. http://192.168.100.1).
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte Konfiguration zu **Einstellungen > Lizenzen > Lizenzen verwalten**, klicken Sie auf **Neue Lizenz hinzufügen**und wählen Sie **Remotelizenzierung verwenden > CICO-Lizenzierung**aus.
4. Geben Sie die Details des Lizenzservers in das Feld **Servername/IP-Adresse** ein.
5. Geben Sie unter **Benutzername** und **Kennwort** die NetScaler ADM-Anmeldeinformationen ein und klicken Sie auf **Weiter**.



6. Wählen Sie die Lizenzedition mit der erforderlichen Bandbreite aus, und klicken Sie auf **Lizenzen abrufen**.



7. Klicken Sie auf **Neustart**, Ihre NetScaler-Instanz wird neu gestartet.
8. Sie können die Lizenzzuweisung ändern oder freigeben, indem Sie zu **System > Lizenzen > Lizenzen verwalten** navigieren und **Zuordnung ändern** oder **Zuordnung freigeben** auswählen.



9. 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**.

NetScaler VPX- und NetScaler BLX-Lizenzen mithilfe der NetScaler-CLI einer NetScaler-Instanz zuweisen

1. Geben Sie in einem SSH-Client die IP-Adresse der NetScaler-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. Um der NetScaler Appliance eine Lizenz zuzuweisen, geben Sie den folgenden Befehl ein:

```
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
```

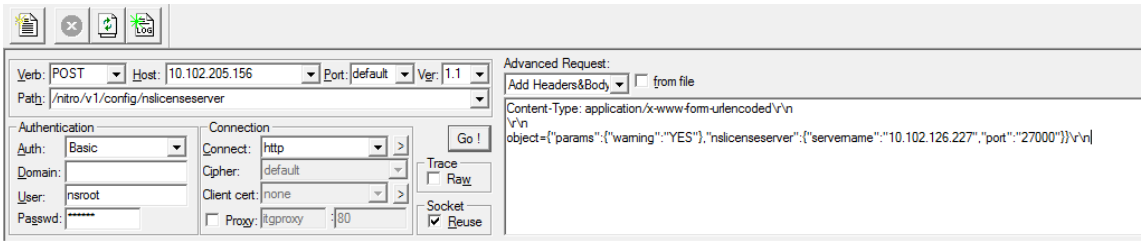

NetScaler VPX- und NetScaler BLX-Lizenzen mithilfe der API einer NetScaler-Instanz zuweisen

Melden Sie sich in einem Webbrowser oder einem API-Client mit den Administratoranmeldeinformationen bei der NetScaler-Instanz an.

So fügen Sie einen Lizenzserver hinzu:

1. Legen Sie den Anforderungstyp auf **Post**fest.
2. Legen Sie den Pfad zu /nitro/v1/config/nslicensingserver fest.
3. Legen Sie die Nutzlast wie folgt fest:

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
object= {
  " params " ;{
 warning " : " yes "  }
 , " nslicensing server " ;{
 servername " : " <NetScaler ADM IP> " , " port " : " 27000 "  }
  }
 \r\n
<!--NeedCopy-->
```



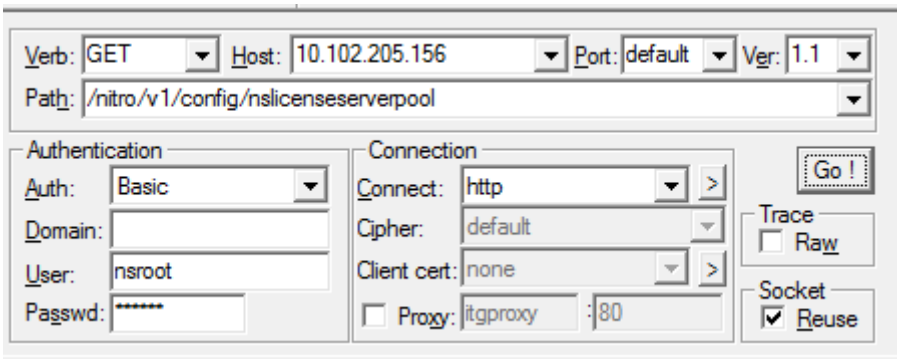
NetScaler ADM antwortet auf die Anforderung. Die folgende Beispielantwort zeigt Erfolg.

```
RESPONSE: **********\n
HTTP/1.1 201 Created\r\n
Date: Fri, 06 Jan 2017 19:03:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

So zeigen Sie die verfügbaren Lizenzen auf dem Lizenzserver an:

1. Stellen Sie den Anforderungstyp auf **Get ein**.

2. Legen Sie den Pfad zu /nitro/v1/config/nslicenseserverpool fest



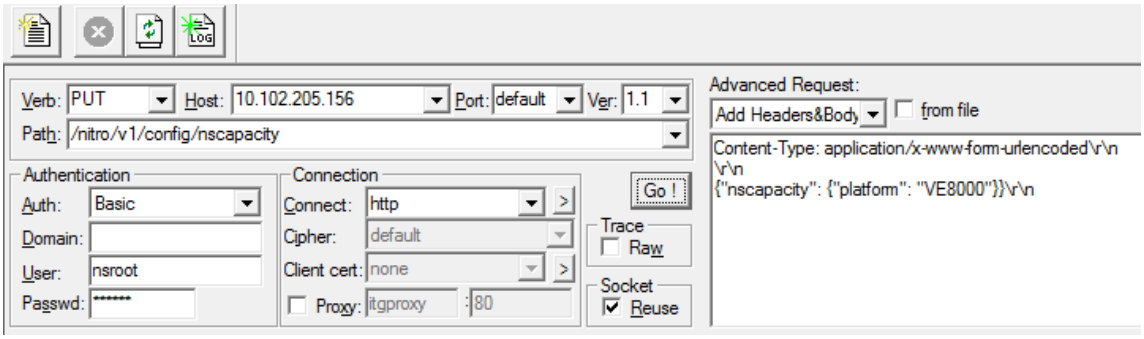
NetScaler ADM antwortet auf die Anforderung. Die folgende Beispielantwort zeigt den Erfolg und die Liste der verfügbaren Lizenzen auf dem Lizenzserver.

RESPONSE: **********\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:18:54 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 1874\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE", "nslicenseserverpool": { "instancetotal": 0, "instanceavailable": 0, "standardbandwidthtotal":
0, "standardbandwidthavailable": 0, "enterprisebandwidthtotal": 0, "enterprisebandwidthavailable": 0, "platinumbandwidthtotal": 0, "platinumbandwidthav
ailable": 0, "cpxinstancetotal": 0, "cpxinstanceavailable": 0, "vpx1stotal": 0, "vpx1savailable": 0, "vpx1ptotal": 0, "vpx1pavailable": 0, "vpx5stotal"
: 0, "vpx5savailable": 0, "vpx5ptotal": 0, "vpx5pavailable": 0, "vpx10stotal": 0, "vpx10savailable": 0, "vpx10etotal": 0, "vpx10eavailable": 0, "vpx10p
total": 0, "vpx10pavailable": 0, "vpx25stotal": 0, "vpx25savailable": 0, "vpx25etotal": 0, "vpx25eavailable": 0, "vpx25ptotal": 0, "vpx25pavailable": 0
, "vpx50stotal": 0, "vpx50savailable": 0, "vpx50etotal": 0, "vpx50eavailable": 0, "vpx50ptotal": 0, "vpx50pavailable": 0, "vpx100stotal": 0, "vpx100sav
ailable": 0, "vpx100etotal": 0, "vpx100eavailable": 0, "vpx100ptotal": 0, "vpx100pavailable": 0, "vpx200stotal": 0, "vpx200savailable": 0, "vpx200etota
l": 0, "vpx200eavailable": 0, "vpx200ptotal": 0, "vpx200pavailable": 0, "vpx500stotal": 0, "vpx500savailable": 0, "vpx500eto
tal": 0, "vpx500eavailable": 0, "vpx500ptotal": 0, "vpx500pavailable": 0, "vpx1000stotal": 0, "vpx1000savailable": 0, "vpx1000etotal": 0, "vpx1000eavail
able": 0, "vpx1000ptotal": 0, "vpx1000pavailable": 0, "vpx2000ptotal": 0, "vpx2000pavailable": 0, "vpx3000stotal": 0, "vpx3000savailable": 0, "vpx3000e
total": 0, "vpx3000eavailable": 0, "vpx3000ptotal": 0, "vpx3000pavailable": 0, "vpx4000ptotal": 0, "vpx4000pavailable": 0, "vpx5000stotal": 0, "vpx5000
savailable": 0, "vpx5000etotal": 0, "vpx5000eavailable": 0, "vpx5000ptotal": 0, "vpx5000pavailable": 0, "vpx8000stotal": 1, "vpx8000savailable": 1, "vp
x8000etotal": 2, "vpx8000eavailable": 1, "vpx8000ptotal": 1, "vpx8000pavailable": 1 } }
finished.

So weisen Sie der NetScaler Appliance eine Lizenz zu:

1. Legen Sie den Anforderungstyp auf **Post**fest.
2. Stellen Sie den Pfad zu /nitro/v1/config/nscapacity.
3. Legen Sie die Nutzlast wie folgt fest:

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
{
  “ nscapacity:{
  “ platform ” : ” VE8000 ”  }
   }
 \r\n
<!--NeedCopy-->
```

NetScaler ADM antwortet auf die Anforderung. Die folgende Beispielantwort zeigt Erfolg.

```
RESPONSE: **************\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:16:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

Aktualisieren der IP-Adresse eines Lizenzservers

Sie können die IP-Adresse des Lizenzservers in den NetScaler VPX- und NetScaler BLX-Instanzen aktualisieren, ohne dass dies Auswirkungen auf die zugewiesene Lizenzbandbreite auf der Instanz hat und Datenverlust entsteht.

Update mit der CLI: Um die IP-Adresse des Lizenzservers mithilfe der CLI zu aktualisieren, geben Sie den folgenden Befehl in der Instanz ein:

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

Dieser Befehl stellt eine Verbindung zum neuen Server her und gibt die Ressourcen frei, die dem vorherigen Lizenzserver zugeordnet waren.

Mit der GUI aktualisieren: Um die IP-Adresse des Lizenzservers mithilfe der GUI zu aktualisieren, navigieren Sie zu **System > Lizenzen > Lizenzen verwalten** und klicken Sie auf **Neue Lizenz hinzufügen**. Weitere Informationen finden Sie unter NetScaler VPX- und NetScaler BLX-Lizenzen mit der NetScaler-GUI einer NetScaler-Instanz zuweisen.

Ablaufprüfungen für NetScaler VPX- und NetScaler BLX Ein- und Auschecklizenzen konfigurieren

Sie können jetzt den Schwellenwert für Lizenzablaufzeiten für NetScaler VPX- und NetScaler BLX-Lizenzen konfigurieren. Durch Festlegen von Schwellenwerten sendet NetScaler ADM Benachrichtigungen per E-Mail oder SMS, wenn eine Lizenz abläuft. Ein SNMP-Trap und eine Benachrichtigung werden ebenfalls gesendet, wenn die Lizenz auf NetScaler ADM abgelaufen ist.

Ein Ereignis wird generiert, wenn eine Benachrichtigung über den Ablauf der Lizenz gesendet wird und dieses Ereignis in NetScaler ADM angezeigt werden kann.

So konfigurieren Sie Lizenzablaufprüfungen:

1. Navigieren Sie zu**Infrastruktur > Gepoolte Lizenzierung**.
2. Auf der Seite**Lizenzeinstellungen**finden Sie im Abschnitt**Lizenzablaufinformationen**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 Warnschwellenwert an. Sie können einen Prozentsatz der gepoolten Lizenzkapazität festlegen, der zur Benachrichtigung von Administratoren verwendet werden soll.
4. Wählen Sie die Art der Benachrichtigung, die Sie senden möchten, indem Sie das entsprechende Kontrollkästchen auswählen. Die Benachrichtigungstypen sind wie folgt:
   a) **E-Mail-Profil**: Geben Sie einen Mailserver und Profildetails an. Eine E-Mail wird ausgelöst, wenn Ihre Lizenzen bald ablaufen.
   b) **SMS-Profil**: Geben Sie einen Short Message Service (SMS) -Server und Profildetails an. Eine SMS-Nachricht wird ausgelöst, wenn Ihre Lizenzen ablaufen.
5. Geben Sie dann an, wann Sie die Benachrichtigung senden möchten, und zwar anhand der Anzahl der Tage vor Ablauf der Lizenz.
6. Klicken Sie auf **Speichern**.

NetScaler virtuelle CPU-Lizenzierung

February 5, 2024

Rechenzentrumsadministratoren wie Sie wechseln zu neueren Technologien, die Netzwerkfunktionen vereinfachen und gleichzeitig niedrigere Kosten und größere Skalierbarkeit bieten. Neuere Rechenzentrumsarchitekturen müssen mindestens die folgenden Funktionen enthalten:

- Softwaredefiniertes Netzwerk (SDN)
- Virtualisierung von Netzwerkfunktionen (NFV)
- Netzwerkvirtualisierung (NV)
- Mikro-Services

Für eine solche Entwicklung müssen auch die Softwareanforderungen dynamisch, flexibel und agil sein, um den sich ständig ändernden Geschäftsanforderungen gerecht zu werden. Es wird erwartet, dass Lizenzen von einem zentralen Management-Tool verwaltet werden, das volle Einblick in die Nutzung bietet.

Virtuelle CPU-Lizenzierung für NetScaler VPX

Zuvor wurden NetScaler VPX-Lizenzen basierend auf dem Bandbreitenverbrauch der Instanzen zugewiesen. Ein NetScaler VPX ist auf die Verwendung einer bestimmten Bandbreite und anderer Leistungsmetriken beschränkt, die auf der Lizenzedition basieren, an die er gebunden ist. Um die verfügbare Bandbreite zu erhöhen, müssen Sie ein Upgrade auf eine Lizenzedition durchführen, die mehr Bandbreite bietet. In bestimmten Szenarien ist die Bandbreitenanforderung möglicherweise geringer, für andere L7-Leistungen wie SSL TPS und Komprimierungsdurchsatz ist die Anforderung jedoch höher. Ein Upgrade der NetScaler 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. NetScaler ADM unterstützt jetzt die Zuweisung von Lizenzen für die NetScaler-Instanz auf der Grundlage der virtuellen CPU-Anforderungen.

In der virtuellen CPU-Usage-basierten Lizenzierungsfunktion gibt die Lizenz die Anzahl der CPUs an, auf die ein bestimmtes NetScaler VPX berechtigt ist. NetScaler VPX kann daher Lizenzen nur für die Anzahl der virtuellen CPUs, die auf dem Server ausgeführt werden, vom Lizenzserver auschecken. NetScaler VPX checkt Lizenzen abhängig von der Anzahl der im System ausgeführten CPUs aus. NetScaler VPX berücksichtigt die Leerlauf-CPUs beim Auschecken der Lizenzen nicht.

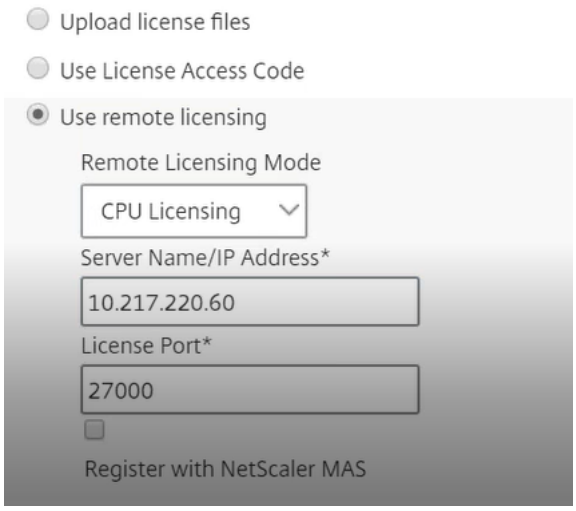
Ähnlich wie bei der gepoolten Lizenzkapazität und den CICO-Lizenzfunktionen verwaltet der NetScaler ADM-Lizenzserver einen separaten Satz virtueller CPU-Lizenzen. Auch hier sind die drei Editionen, die für virtuelle CPU-Lizenzen verwaltet werden, Standard, Advanced und Premium. Diese Editionen entsperren 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 einem solchen Fall müssen Sie die Instanz immer herunterfahren, bevor Sie eine Anforderung für

einen neuen Satz von Lizenzen initiieren. Starten Sie NetScaler VPX nach dem Auschecken der Lizenzen neu.

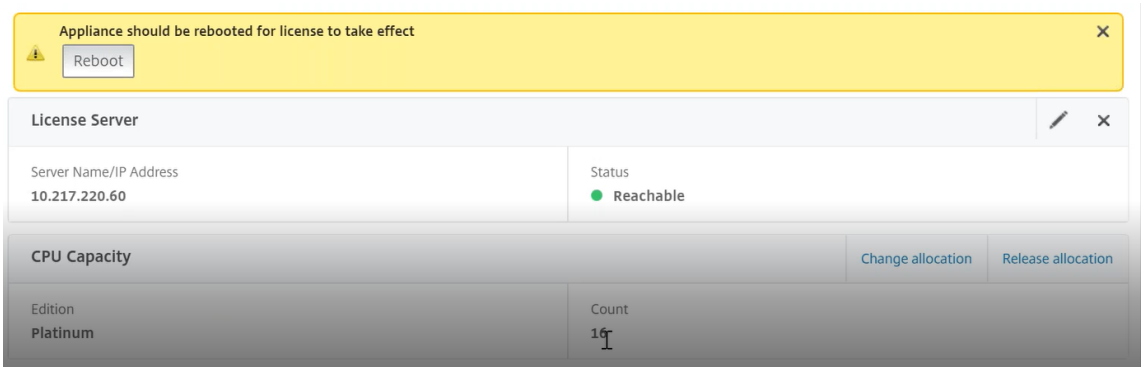
So konfigurieren Sie den Lizenzierungsserver in NetScaler VPX mit der GUI:

1. Navigieren Sie in NetScaler 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** .
4. Wählen Sie **CPU-Lizenzierung** aus der Liste **Remote-Lizenzierungsmodus** aus.
5. Geben Sie die IP-Adresse des Lizenzservers und die Portnummer ein.
6. Klicken Sie auf **Weiter**.



> **Hinweis** Sie müssen die NetScaler VPX-Instanz immer bei NetScaler ADM registrieren. Falls noch nicht geschehen, aktivieren Sie die Option **Bei NetScaler ADM registrieren und geben Sie die NetScaler ADM-Anmeldeinformationen** ein.

7. Wählen Sie im Fenster **Lizenzen zuweisen** den Lizenztyp aus. Das Fenster zeigt die Gesamtzahl und die verfügbaren virtuellen CPUs sowie die CPUs an, die zugewiesen werden können. Klicken Sie auf **Get Licenses**.
8. Klicken Sie auf der nächsten Seite auf **Reboot** , um die Lizenz zu beantragen.



> **Hinweis**
>
> Sie können auch die aktuelle Lizenz freigeben und aus einer anderen Edition auschecken. Beispielsweise führen Sie bereits eine Standard Edition-Lizenz auf Ihrer Instance aus. Sie können diese Lizenz freigeben und dann aus der Advanced Edition auschecken.

Konfiguration eines Lizenzservers in der NetScaler VPX-Lizenz mithilfe der CLI

Geben Sie in der NetScaler VPX-Konsole die folgenden Befehle für die folgenden zwei Aufgaben ein:

1. Um den Lizenzserver zum NetScaler VPX hinzuzufügen:

```
1 add licenseserver <IP address of the license server>
2 <!--NeedCopy-->
```

2. So beantragen Sie die Lizenzen:

```
1 set capacity -vcpu - edition premium
2 <!--NeedCopy-->
```

   Wenn Sie dazu aufgefordert werden, starten Sie die Instanz neu, indem Sie den folgenden Befehl eingeben:

```
1 reboot -w
2 <!--NeedCopy-->
```

Aktualisieren der IP-Adresse eines Lizenzservers

Sie können die IP-Adresse des Lizenzservers in der NetScaler VPX-Instanz aktualisieren, ohne dass dies Auswirkungen auf die der Instanz zugewiesene Lizenzbandbreite und Datenverlust hat. Um die IP-Adresse des Lizenzservers zu aktualisieren, geben Sie den folgenden Befehl auf der NetScaler VPX-Instanz ein:

```
add licenseserver <licensing server IP address> -forceUpdateIP
```


Dieser Befehl stellt eine Verbindung zum neuen Server her und gibt die Ressourcen frei, die dem vorherigen Lizenzserver zugeordnet waren.

Verwalten virtueller CPU-Lizenzen auf NetScaler ADM

1. Navigieren Sie in NetScaler ADM zu **Infrastruktur > Gepoolte Lizenzierung > Gepoolte VCPU**.
2. Auf der Seite werden die Lizenzen angezeigt, die für jeden Lizenzausgabetyp zugewiesen sind.
3. Klicken Sie auf die Zahl in jedem Donut, um die NetScaler-Instanzen anzuzeigen, die diese Lizenz verwenden.

Virtuelle CPU-Lizenzierung für NetScaler CPX

Während der Bereitstellung der NetScaler CPX-Instanz können Sie die NetScaler CPX-Instanz so konfigurieren, dass je nach CPU-Auslastung der Instanz Lizenzen vom Lizenzserver ausgecheckt werden.

NetScaler CPX verwendet den Lizenzserver, der auf NetScaler ADM läuft, um die Lizenzen zu verwalten. NetScaler CPX checkt die Lizenzen vom Lizenzserver aus, wenn dieser gestartet wird. Die Lizenzen werden beim Herunterfahren des NetScaler CPX wieder auf den Lizenzserver eingecheckt.

Sie können das NetScaler CPX-Image mit dem Befehl ‘docker pull’aus der Quay-Container-Registry herunterladen und in Ihrer Umgebung bereitstellen.

Für die NetScaler CPX-Lizenzierung sind drei Lizenztypen verfügbar:

1. Virtuelle CPU-Abonnementlizenzen werden für NetScaler CPX und VPX unterstützt
2. Lizenzen für gepoolte Kapazität
3. CP1000-Lizenzen, die einzelne bis mehrere vCPUs unterstützen, nur für NetScaler CPX

So konfigurieren Sie vCPU-Abonnementlizenzen während der Provisioning der NetScaler CPX-Instanz:

Geben Sie die Anzahl der vCPU-Lizenzen an, die die NetScaler CPX-Instanz verwendet.

- Dieser Wert wird als Umgebungsvariable über Docker, Kubernetes oder Mesos/Marathon eingegeben.
- Die Zielvariable lautet “CPX_CORES”. Der NetScaler CPX kann 1 bis 16 Kerne unterstützen.

Um 2 Kerne anzugeben, können Sie den Befehl docker run wie folgt ausführen:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2
2 <!--NeedCopy-->
```

Definieren Sie bei der Bereitstellung einer NetScaler CPX-Instanz den NetScaler Lizenzserver als Umgebungsvariable im Befehl **docker run**, wie unten gezeigt:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
     LS_PORT> cpx:11.1
2 <!--NeedCopy-->
```

Hierbei gilt:

- *<LS_IP_ADDRESS>* ist die IP-Adresse des NetScaler Lizenzservers.
- *<LS_PORT>* ist der Port des NetScaler Lizenzservers. Standardmäßig ist der Port 27000.

> **Hinweis:**
>
> Standardmäßig checkt die NetScaler CPX-Instanz die Lizenz aus dem vCPU-Abonnementpool aus. Die NetScaler CPX-Instanz checkt eine „n“Anzahl von Lizenzen aus, wenn die Instanz mit „n“CPUs ausgeführt wird.

So konfigurieren Sie NetScaler Pooled Capacity oder CP1000-Lizenzen bei der Bereitstellung der NetScaler CPX-Instanz:

Wenn Sie die Lizenz für die NetScaler CPX-Instanz mithilfe der gepoolten Lizenzierung (bandbreitenbasiert) oder des privaten NetScaler CPX-Pools (CP1000 oder privatpoolbasiert) auschecken möchten, müssen Sie die Umgebungsvariablen entsprechend angeben.

Beispiel:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
     LS_PORT> -e PLATFORM=CP1000 cpx:11.1
2 <!--NeedCopy-->
```

CP1000. Dieser Befehl löst das Auschecken aus dem CP1000-Pool (privater NetScaler CPX-Pool) aus. Die NetScaler CPX-Instanz ruft dann die Anzahl der Instanzen “n”für die Anzahl der für CPX_CORES angegebenen Kerne ab. Der häufigste Anwendungsfall ist, n = 1 für ein Auschecken einer einzelnen Instanz anzugeben. Bei NetScaler CPX-Anwendungsfällen mit mehreren Kernen werden „n“vCPUs überprüft (wobei „n“zwischen 1 und 7 steht).


```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> -e BANDWIDTH=2000 cpx:11.1
<!--NeedCopy-->
```

Kapazität gepoolt. Dieser Befehl checkt eine Lizenz aus dem Instance-Pool aus und verbraucht 1000 Mbit/s Bandbreite aus dem Premium-Bandbreitenpool, ermöglicht NetScaler CPX jedoch, bis zu 2000 Mbit/s auszuführen. Bei der Pool-Lizenzierung werden die ersten 1000 Mbit/s nicht berechnet.

> **Hinweis**
>
> Geben Sie beim Auschecken aus dem Bandbreitenpool die entsprechende Anzahl von vCPUs für die gewünschte Zielbandbreite an, wie in der folgenden Tabelle beschrieben:

Anzahl der Kerne (vCPU)	Maximale Bandbreite
1	1000 MBit/s
2	2000 Mbit/s
3	3500 Mbit/s
4	5000 Mbit/s
5	6500 Mbit/s
6	8000 Mbit/s
7	9300 Mbit/s

Systemeinstellungen verwalten

February 5, 2024

In der folgenden Tabelle wird die Liste der Optionen beschrieben, die unter **Einstellungen** > **Verwaltung**verfügbar sind:

Netzwerkkonfigurationen

Netzwerkkonfigurationen	Optionen	Beschreibung
IP-Adresse, zweite Netzwerkkarte, Hostname und Proxyserver	IP-Adresse	Zeigt die IP-Adressdetails der NetScaler ADM-Netzwerkkonfiguration an, die für die Bereitstellung von NetScaler ADM verwendet werden
	Zweiter NIC	Ermöglicht die Konfiguration einer zweiten NIC zur Isolierung des NetScaler ADM Verwaltungszugriffs. Weitere Informationen finden Sie unter Konfigurieren einer dualen Netzwerkkarte für den Zugriff auf NetScaler ADM
	Hostname	Ermöglicht das Zuweisen eines Hostnamens zu NetScaler ADM. Weitere Informationen finden Sie unter Zuweisen eines Hostnamens zu einem NetScaler ADM-Server
	Proxyserver	Ermöglicht die Konfiguration von ADM als Proxyserver. Weitere Informationen finden Sie unter NetScaler ADM als API-Proxyserver
Statische Routen		Ermöglicht die Konfiguration statischer Routen, um eine Verbindung zwischen NetScaler ADM- und NetScaler VPX-Instanzen herzustellen
NTP-Server		Stellt sicher, dass die NetScaler ADM Uhr dieselben Datums- und Uhrzeiteinstellungen hat wie die anderen Server im Netzwerk. Weitere Informationen finden Sie unter Konfigurieren des NTP-Servers

Netzwerkkonfigurationen	Optionen	Beschreibung
ADM-Port-Informationen		Ermöglicht es Ihnen zu verstehen, welcher Port für die Kommunikation zwischen ADM- und ADC-Instanzen geöffnet sein muss. Weitere Informationen finden Sie unter Unterstützte Ports

Systemkonfigurationen

Systemkonfigurationen	Optionen	Beschreibung
System, Zeitzone, erlaubte URLs und Nachricht des Tages	Grundeinstellungen	Ermöglicht es Ihnen, Systemeinstellungen wie das Aktivieren der `nsrecover` Anmeldung, das Aktivieren des Sitzungstimeouts usw. zu ändern
	Zeitzone	Ermöglicht es Ihnen, die Zeitzone zu ändern, die in NetScaler ADM verwendet werden soll. Die Standardzeitzone ist UTC
	Liste der zulässigen URLs	Ermöglicht die Konfiguration von URLs zum Senden ununterbrochener Anforderungen an ADM. Sie können es mit dem Wert “none”konfigurieren, wenn keine URL hinzugefügt werden soll

Systemkonfigurationen	Optionen	Beschreibung
	Botschaft des Tages	Ermöglicht das Erstellen einer Willkommensnachricht in NetScaler ADM. Mit dieser Funktion können Sie Erinnerungsmeldungen für sich selbst oder den Benutzer festlegen, der sich bei NetScaler ADM anmeldet. Klicken Sie auf **Nachricht aktivieren**, geben Sie die Nachricht in das Nachrichtenfeld ein und klicken Sie auf **Speichern**
ADM-Fingerabdruck anzeigen		Ermöglicht das Kopieren der eindeutigen NetScaler ADM-Fingerabdruck-ID, um mit dem Servicediagramm zu beginnen
Kundenidentität konfigurieren		Ermöglicht es Ihnen, die Netzwerkressourcen zu schützen, indem nur authentifizierte Kunden oder Benutzer auf das Netzwerk zugreifen können. Weitere Informationen finden Sie unter Daten-Governance
CUXIP-Einstellungen		Wenn Sie dieses Kontrollkästchen aktivieren, werden Nutzungsstatistiken ausschließlich zum Zweck der Verbesserung der GUI gesammelt. Die empfangenen Daten werden nur von Citrix-Technikern verwendet und an niemanden weitergegeben

System-Pflege

System-Pflege	Beschreibung
Upgrade von NetScaler ADM	Ermöglicht Ihnen das Upgrade von NetScaler ADM über die GUI. Weitere Informationen finden Sie unter Upgrade
Starten Sie NetScaler ADM neu	Ermöglicht den Neustart von NetScaler ADM
Fahren Sie NetScaler ADM herunter	Ermöglicht das Herunterfahren von NetScaler ADM
Notfallwiederherstellung	Ermöglicht Ihnen das Anzeigen von Knoteninformationen zur Notfallwiederherstellung. Weitere Informationen finden Sie unter Konfigurieren der Notfallwiederherstellung

Datenbereinigung

Datenbereinigung	Optionen	Beschreibung
Bereinigung von System- und Instanzdaten	System	Ermöglicht die Begrenzung der Berichtsdaten, die in der NetScaler ADM -Serverdatenbank gespeichert werden. Weitere Informationen finden Sie unter Konfigurieren der System-Prune-Einstellungen
	Instanz-Ereignisse	Ermöglicht es Ihnen, die in NetScaler ADM gespeicherten Ereignismeldungen zu beschränken, die Daten melden

Datenbereinigung	Optionen	Beschreibung
	Instanz Syslog	Ermöglicht es Ihnen, die Menge der in der Datenbank gespeicherten Syslog-Daten zu begrenzen. Weitere Informationen finden Sie unter Konfigurieren der Syslog-Einstellungen für Instanz-Prune-Einstellungen
	Netzwerkberichterstattung	Ermöglicht es Ihnen, die in NetScaler ADM gespeicherten Netzwerkberichtsdaten zu begrenzen

Backup

Backup	Optionen	Beschreibung
System- und Instanz-Backup konfigurieren	System	Ermöglicht es Ihnen, die anfänglichen Backupeinstellungen zu konfigurieren, bevor Sie eine Systembackup durchführen. Weitere Informationen finden Sie unter Systembackupeinstellungen
	Instanz	Ermöglicht das Konfigurieren von Einstellungen in NetScaler ADM zum Sichern einer ausgewählten NetScaler Instanz oder mehrerer Instanzen. Weitere Informationen finden Sie unter Konfigurieren der Instanzbackupeinstellungen

Ereignisbenachrichtigungen

Ereignisbenachrichtigungen	Optionen	Beschreibung
Ereignisbenachrichtigung und Zusammenfassung konfigurieren	Benachrichtigung über das Ereignis	Sie können Benachrichtigungen für verschiedene systembezogene Funktionen an ausgewählte Benutzergruppen senden. Diese Systemfunktionen sind in Ereigniskategorien wie SystemReboot, StatusPoll, SystemState usw. unterteilt. Sie können NetScaler Application Delivery Management (ADM) so konfigurieren, dass Sie Benachrichtigungen entweder per E-Mail, SMS oder Slack erhalten. Dadurch wird sichergestellt, dass Sie über alle Aktivitäten auf Systemebene informiert werden, z. B. über eine Überschreitung des Datenspeichers oder über Backup-Fehler.
	Ereigniszusammenfassung	Ermöglicht es Ihnen, einen konsolidierten Bericht über wichtige System- und Funktionsereignisse zu erhalten

SSL-Einstellungen

SSL-Einstellungen	Beschreibung
Installieren Sie das SSL-Zertifikat	Ermöglicht die Installation des SSL-Zertifikats und der SSL-Schlüsseldatei
SSL-Zertifikat anzeigen	Ermöglicht das Anzeigen der SSL-Zertifikatsdetails
Konfigurieren von SSL-Einstellungen	Weitere Informationen finden Sie unter Konfigurieren von SSL-Einstellungen
SSL-Zertifikate	Ermöglicht das Hochladen, Herunterladen oder Löschen eines SSL-Zertifikats oder einer SSL-Schlüsseldatei
Chiffriergruppen	Weitere Informationen finden Sie unter Konfigurieren einer Verschlüsselungsgruppe

Funktionen konfigurieren

Funktionen konfigurieren	Beschreibung
Funktionen deaktivieren oder aktivieren	Sie können Funktionen in NetScaler ADM aktivieren oder deaktivieren. Weitere Informationen finden Sie unter ADM-Funktionen aktivieren oder deaktivieren

Einstellungen für das Systembackup konfigurieren

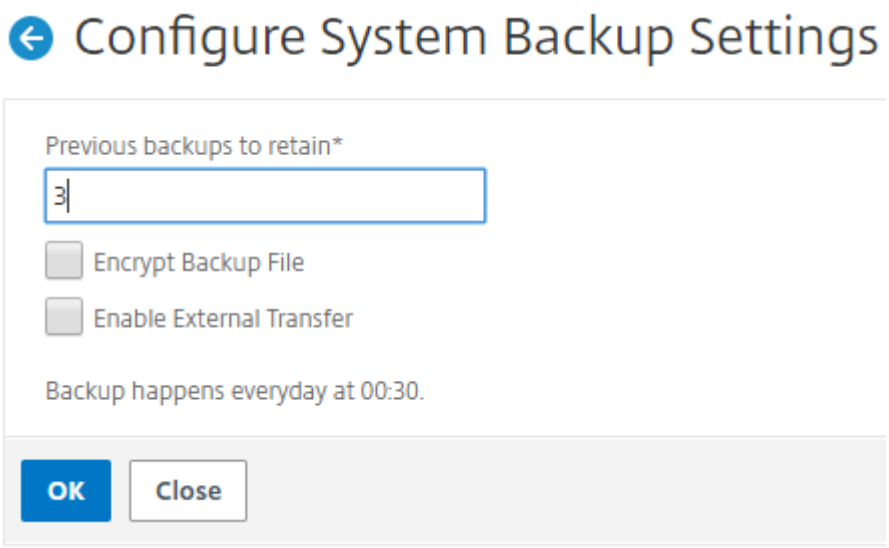
February 5, 2024

Richten Sie Ihre ersten Systembackupeinstellungen ein, bevor Sie ein Backup und eine Wiederherstellung des NetScaler Application Delivery Management (ADM)-Systems ausführen müssen.

1. Navigieren Sie zu **Einstellungen > Administration** . Klicken Sie unter **Backup** auf **System- und Instanz-Backup konfigurieren** .
2. Geben Sie auf der Seite **Backup > System** Folgendes an:
    - Frühere Backups, die aufbewahrt werden sollen. Sie können nur bis zu 10 Backups behalten.
    - Wählen Sie **Encrypt Backup File** aus, um die Backupdateien zu verschlüsseln.

- Wählen Sie **Externe Übertragung aktivieren**, um eine Kopie Ihrer Backupdatei auf ein anderes System zu übertragen. Wenn Sie die Konfiguration wiederherstellen möchten, müssen Sie zuerst die Datei auf den NetScaler ADM-Server hochladen und dann den Wiederherstellungsvorgang ausführen. Geben Sie den Server, den Benutzernamen und das Kennwort, den Port, das zu verwendende Übertragungsprotokoll und den Verzeichnispfad an. Weitere Informationen zur externen Übertragung finden Sie unter Übertragen einer NetScaler ADM-Backupdatei auf ein externes System.

3. Klicken Sie auf **OK**.



Konfigurieren eines NTP-Servers

February 5, 2024

Sie können einen NTP-Server (Network Time Protocol) in NetScaler Application Delivery Management (ADM) so konfigurieren, dass er seine Uhr mit dem NTP-Server synchronisiert. Durch die Konfiguration eines NTP-Servers wird sichergestellt, dass die NetScaler ADM Uhr dieselben Datums- und Uhrzeiteinstellungen wie die anderen Server im Netzwerk aufweist.

So konfigurieren Sie einen NTP-Server auf NetScaler ADM:

1. Navigieren Sie zu **Einstellungen> NTP-Server**, und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie auf der Seite **NTP-Server erstellen** die folgenden Details ein:

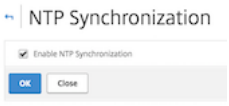
   - **Servername/IP-Adresse** —Geben Sie den Domainnamen oder die IP-Adresse des NTP-Servers ein. Der Name oder die IP-Adresse können nicht geändert werden, nachdem Sie den NTP-Server hinzugefügt haben.

- **Minimales Abfrageintervall** —Geben Sie den Mindestwert für das Intervall zwischen übertragenen NTP-Nachrichten in Sekunden als Trennschärfe von 2. Wenn Sie beispielsweise möchten, dass das minimale Abfrageintervall 64 Sekunden beträgt, was als 2 ^ 6 ausgedrückt werden kann, geben Sie 6 ein.
- **Maximales Abfrageintervall** —Geben Sie den Maximalwert für das Intervall zwischen übertragenen NTP-Nachrichten in Sekunden als Trennschärfe von 2. Wenn Sie beispielsweise möchten, dass das maximale Abfrageintervall 256 Sekunden beträgt, was als 2^8 ausgedrückt werden kann, geben Sie 8 ein.
- **Schlüssel-ID**—Geben Sie die Schlüssel-ID ein, die für die symmetrische Schlüsselauthentifizierung mit dem NTP-Server verwendet werden kann. Fügen Sie keine Schlüssel-ID hinzu, wenn Sie Autokey auswählen.
- **Autokey** —Wählen Sie **Autokey** aus, wenn Sie die Authentifizierung mit öffentlichen Schlüsseln für den NTP-Server verwenden möchten. Wählen Sie nicht aus, ob Sie eine Schlüssel-ID hinzufügen möchten.
- **Bevorzugt** —Wählen Sie diese Option, wenn Sie diesen NTP-Server als bevorzugten Server für die Uhrsynchronisierung angeben möchten. Dies gilt nur, wenn mehr als ein Server konfiguriert ist.

3. Klicken Sie auf **Erstellen**.

So aktivieren Sie die NTP-Synchronisierung auf NetScaler ADM:

1. Navigieren Sie zu **Einstellungen> NTP-Server**.
2. Klicken Sie auf **NTP-Synchronisierung** und **aktivieren Sie das Kontrollkästchen NTP-Synchronisierung** aktivieren.
3. Klicken Sie auf **OK**.



> Hinweis Die NTP-Protokollmeldungen finden
>
> Sie im Verzeichnis /var/log in der `/var/log/ntpd.log` Dateidatei.

Aktualisieren Sie NetScaler Application Delivery Management (ADM)

February 5, 2024

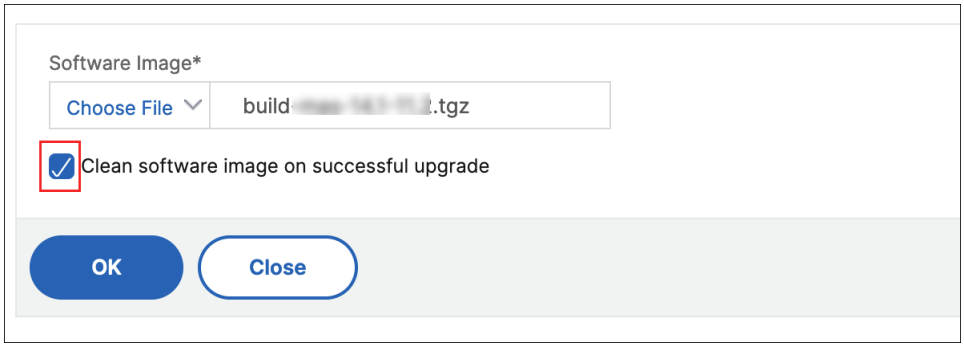
Jede NetScaler ADM-Version bietet neue und aktualisierte Funktionen mit erweiterter Funktionalität. Eine umfassende Liste von Verbesserungen ist in den Versionshinweisen aufgeführt, die der Release-Ankündigung beigefügt sind. Nehmen Sie sich einen Moment Zeit, um die Versionshinweise zu lesen, bevor Sie die Software aktualisieren. Es ist wichtig, dass Sie den Lizenzrahmen und die Lizenztypen verstehen, bevor Sie mit dem Upgrade beginnen.

Um NetScaler ADM zu aktualisieren:

1. Navigieren Sie zu **Einstellungen > Administration**. Klicken Sie unter **Systemwartung** auf **NetScaler ADM aktualisieren**.
2. Laden Sie auf der Seite NetScaler ADM aktualisieren eine neue Image-Datei hoch, indem Sie entweder **Lokal** (Ihr lokaler Computer) oder **Appliance**auswählen.

   > **Hinweis**
   >
   > Wenn Sie **Appliance**auswählen, stellen Sie sicher, dass das Upgrade-Image `/var/mps/mps_images` in NetScaler ADM verfügbar ist.

   Standardmäßig wird das Softwareimage nach einem erfolgreichen Upgrade bereinigt.
3. Klicken Sie auf **OK**.



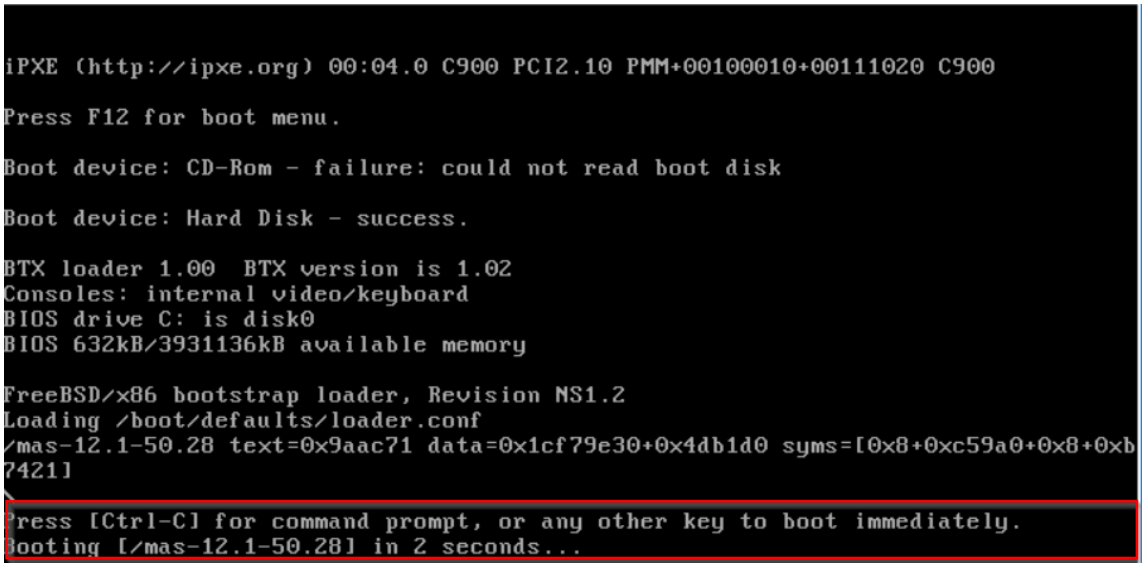
Kennwort für NetScaler ADM zurücksetzen

February 5, 2024

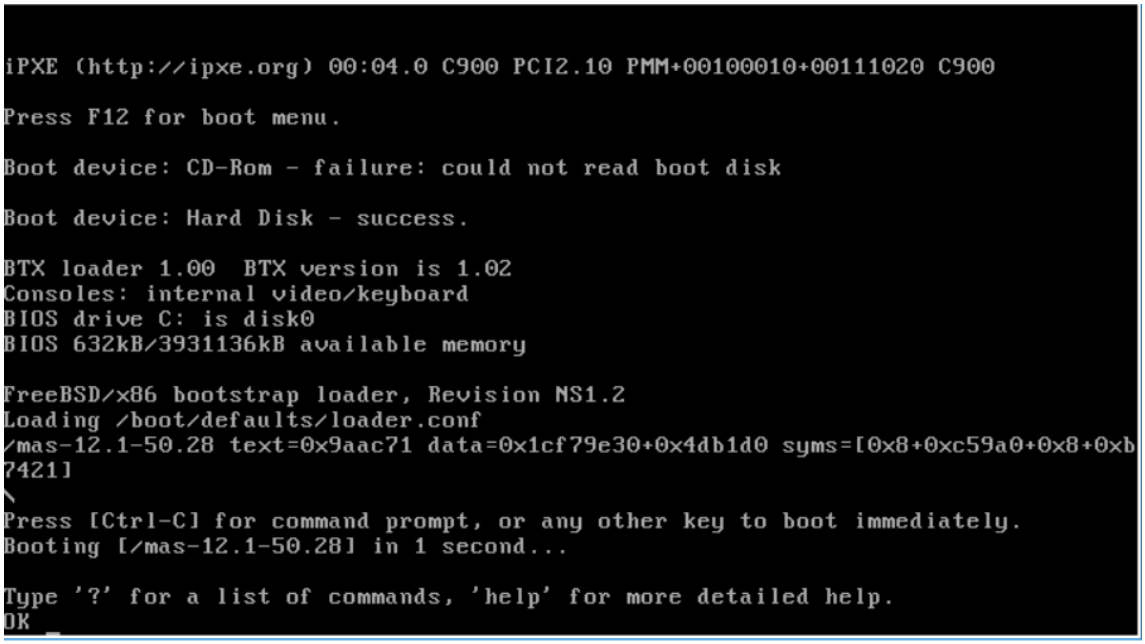
Das Verfahren zum Zurücksetzen des Kennworts für NetScaler ADM kann auf Hypervisoren, auf denen es gehostet wird, unterschiedlich sein. Wenn Sie Ihr Standardkennwort geändert haben und auf das Standardkennwort zurücksetzen möchten, können Sie das Kennwort zurücksetzen, indem Sie den NetScaler ADM-Knoten neu starten.

Citrix Hypervisor mit XenCenter:

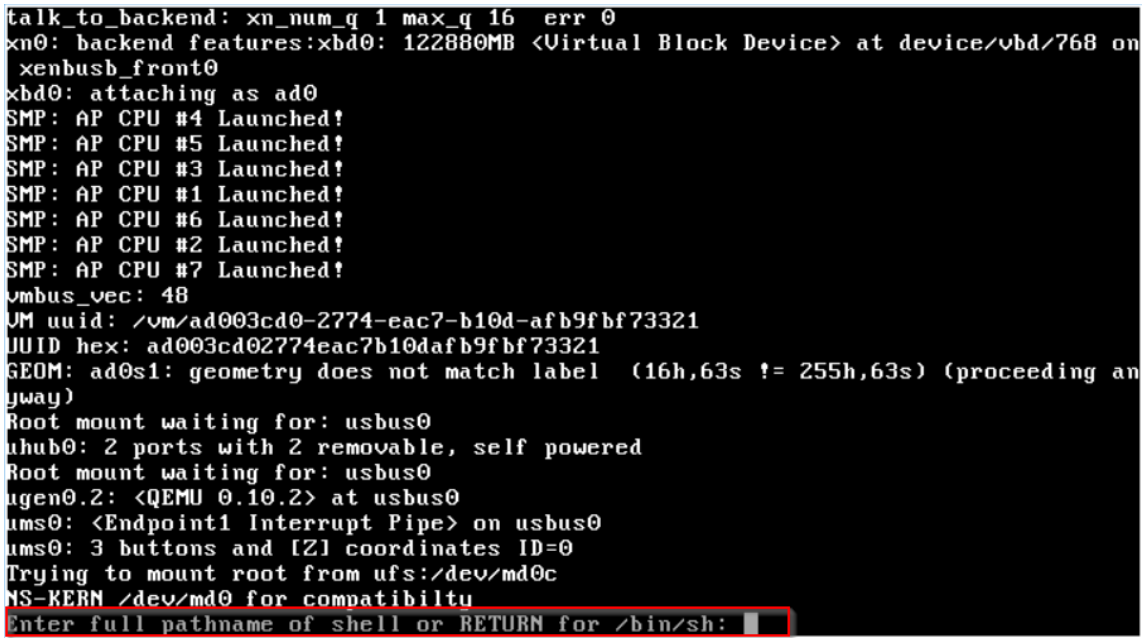
1. Melden Sie sich mit XenCenter bei Citrix Hypervisor an.
2. Wählen Sie den Knoten NetScaler ADM aus, klicken Sie mit der rechten Maustaste und wählen Sie **Neustart**
3. Auf der Registerkarte **Konsole** drücken Sie **CTL + C**, um die Startsequenz zu unterbrechen.



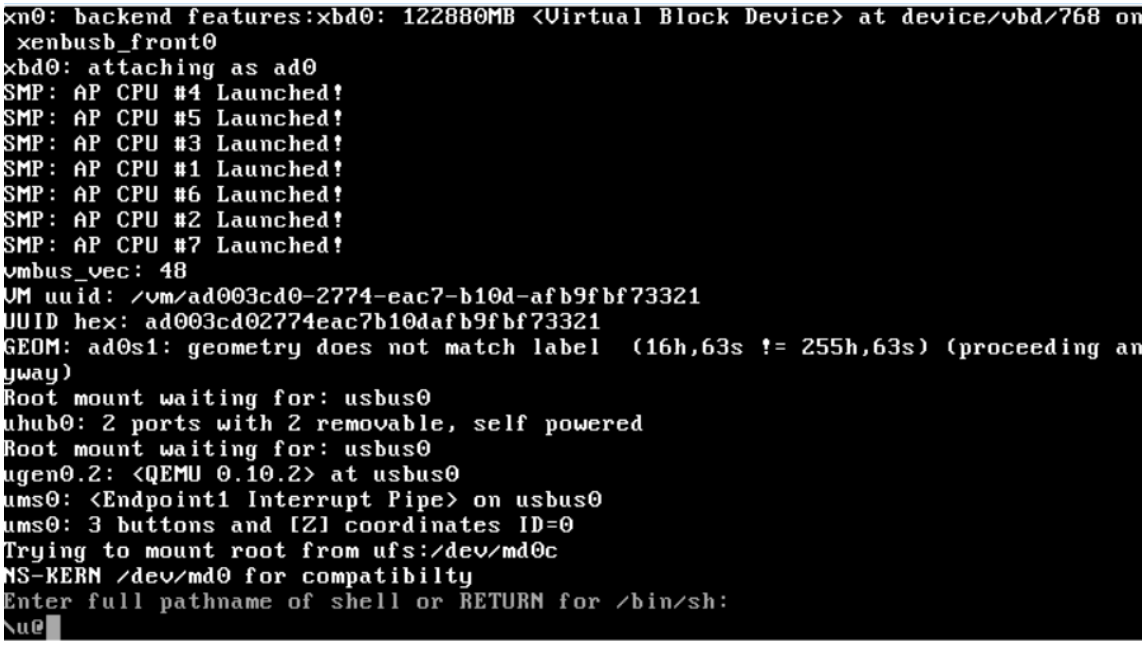
4. Führen Sie den Befehl **boot -s** an der Eingabeaufforderung OK



NetScaler ADM wird neu gestartet und zeigt die folgende Meldung an:

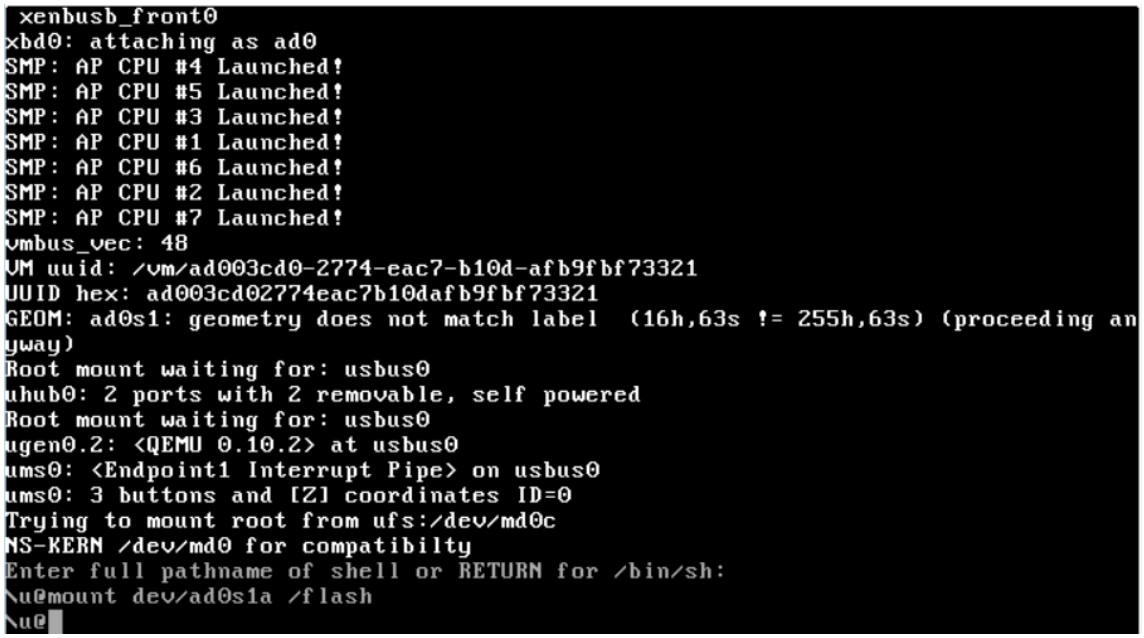


5. Drücken Sie die **Eingabetaste**, um die Eingabeaufforderung /u @ zu erhalten.



6. Mounten Sie die Flash-Partition mit dem folgenden Befehl:

   ```
   mount /dev/da0s1a /flash
   ```



7. Erstellen Sie eine Datei mit dem folgenden Befehl:

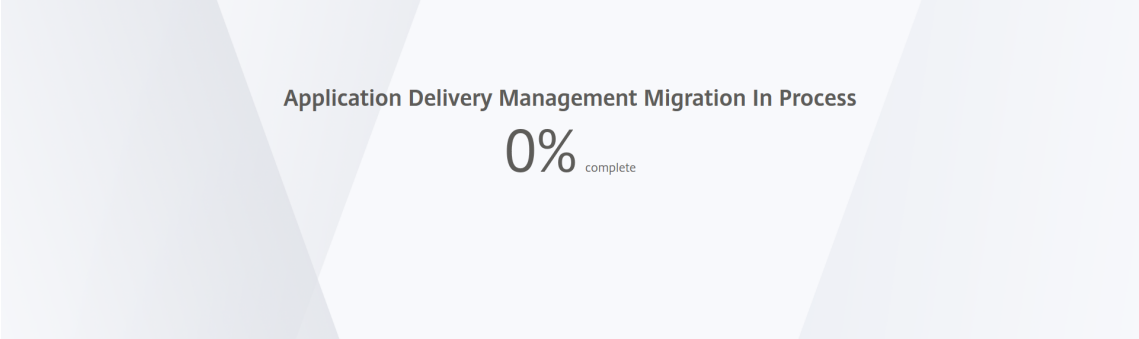
   ```
   touch /flash/mpsconfig/.recover
   ```

   Das Kennwort wird nun auf das Standardkennwort zurückgesetzt.

8. Führen Sie den Befehl **Neustart** aus, um NetScaler ADM neu zu starten.


```
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
\u@mount dev/ad0s1a /flash
\u@touch /flash/mpsconfig/.recover
\u@reboot
```

9. Greifen Sie auf die NetScaler ADM GUI zu und warten Sie, bis der Neustart abgeschlossen ist.



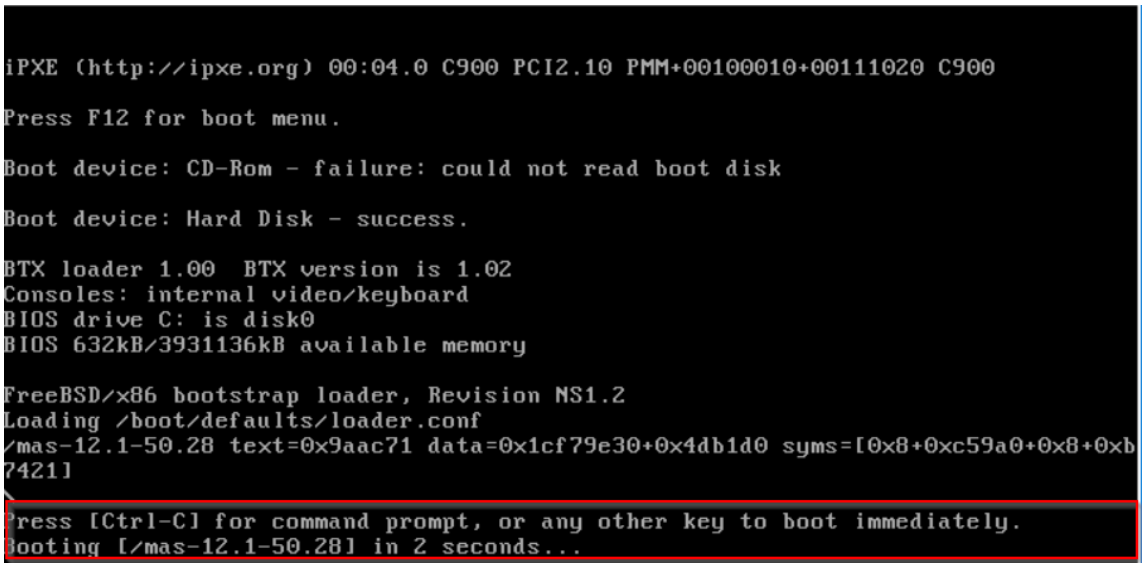
Sie können jetzt *nsroot/nsroot* Anmeldeinformationen verwenden, um sich von der GUI anzumelden, und *nsrecover/nsroot*, um sich vom Hypervisor anzumelden.

> Hinweis
>
> Wenn das Kennwort nach dem Neustart nicht auf das Standardkennwort zurückgesetzt wurde, wiederholen Sie den Vorgang (Schritt 1 bis Schritt 7). Führen Sie dann die folgenden Befehle aus und starten Sie NetScaler ADM neu:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Esx mit vSphere:

1. Melden Sie sich mit vSphere bei ESX an.
2. Wählen Sie den NetScaler ADM Knoten aus, klicken Sie mit der rechten Maustaste, und wählen Sie dann **Neustart** aus.

3. Auf der Registerkarte **Konsole** drücken Sie **CTL + C**, um die Startsequenz zu unterbrechen.



4. Führen Sie den Befehl **boot -s** in der Eingabeaufforderung OK

   NetScaler ADM wird neu gestartet.

5. Drücken Sie die **Eingabetaste**, um die Eingabeaufforderung /u @ zu erhalten.
6. Mounten Sie die Flash-Partition mit dem folgenden Befehl:

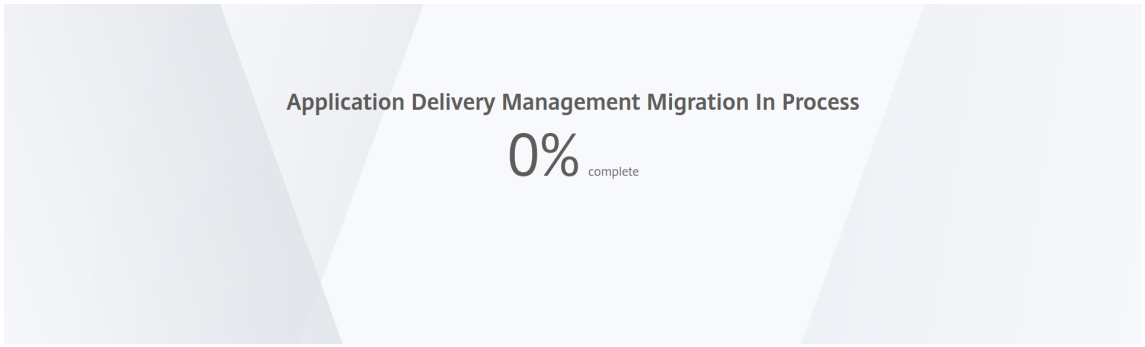
   ```
   mount dev/da0s1a /flash
   ```

7. Erstellen Sie eine Datei mit dem folgenden Befehl:

   ```
   touch /flash/mpsconfig/.recover
   ```

   Das Kennwort wird nun auf das Standardkennwort zurückgesetzt.

8. Führen Sie den Befehl **Neustart** aus, um NetScaler ADM neu zu starten.
9. Greifen Sie auf die NetScaler ADM GUI zu und warten Sie, bis der Neustart abgeschlossen ist.

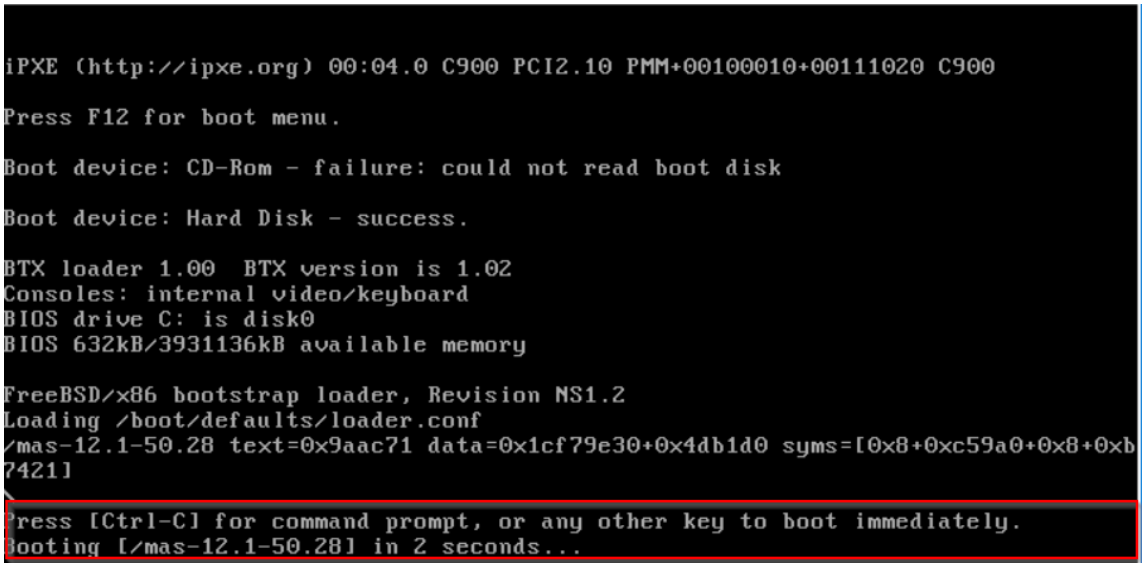


   Sie können jetzt *nsroot/nsroot* Anmeldeinformationen verwenden, um sich von der GUI anzumelden, und *nsrecover/nsroot*, um sich vom ESX-Server anzumelden.

> Hinweis
>
> Wenn das Kennwort nach dem Neustart nicht auf das Standardkennwort zurückgesetzt wurde, wiederholen Sie den Vorgang (Schritt 1 bis Schritt 7). Führen Sie dann die folgenden Befehle aus und starten Sie NetScaler ADM neu:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Hyper-V mit Hyper-V-Manager:

1. Melden Sie sich mit dem Hyper-V-Manager bei Hyper-V an.
2. Wählen Sie den NetScaler ADM Knoten aus, klicken Sie mit der rechten Maustaste, und wählen Sie dann **Neustart** aus.
3. Auf der Registerkarte **Konsole** drücken Sie **CTL + C**, um die Startsequenz zu unterbrechen.



4. Führen Sie den Befehl **boot -s** an der Eingabeaufforderung OK aus

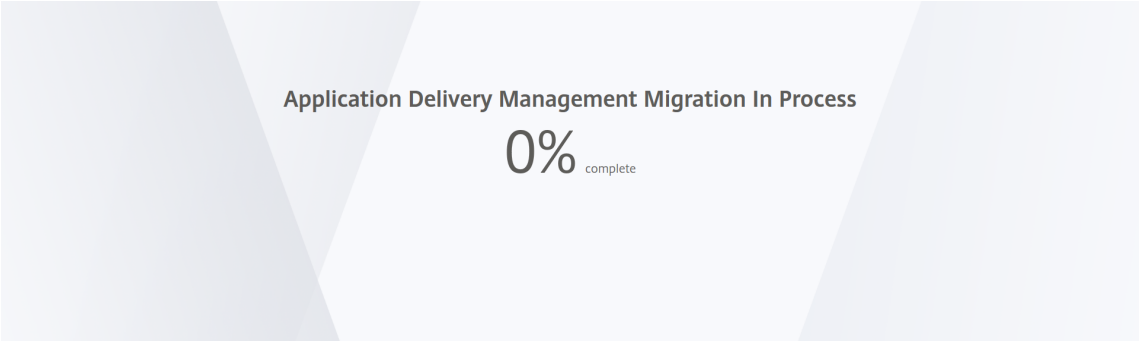
   NetScaler ADM wird neu gestartet.
5. Drücken Sie die **Eingabetaste**, um die Eingabeaufforderung /u @ zu erhalten.
6. Mounten Sie die Flash-Partition mit dem folgenden Befehl:

   ```
   mount dev/ad0s1a /flash
   ```
7. Erstellen Sie eine Datei mit dem folgenden Befehl:

   ```
   touch /flash/mpsconfig/.recover
   ```

   Das Kennwort wird nun auf das Standardkennwort zurückgesetzt.
8. Führen Sie den Befehl **Neustart** aus, um NetScaler ADM neu zu starten.

9. Greifen Sie auf die NetScaler ADM GUI zu und warten Sie, bis der Neustart abgeschlossen ist.



Sie können jetzt *nsroot/nsroot* Anmeldeinformationen verwenden, um sich von der GUI anzumelden, und *nsrecover/nsroot*, um sich vom hyper-v Manager anzumelden.

> Hinweis
>
> Wenn das Kennwort nach dem Neustart nicht auf das Standardkennwort zurückgesetzt wurde, wiederholen Sie den Vorgang (Schritt 1 bis Schritt 7). Führen Sie dann die folgenden Befehle aus und starten Sie NetScaler ADM neu:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Linux KVM-Server (SSH zu KVM-Server unter Verwendung eines beliebigen SSH-Clients):

1. Melden Sie sich mit einem SSH-Client bei NetScaler ADM am KVM-Server an.
2. Starten Sie NetScaler ADM neu.
3. Drücken Sie **CTL + C**, um die Startsequenz kurz nachdem die Meldung **Loading /boot/defaults/loader.conf** angezeigt wird, zu unterbrechen.
4. Führen Sie an der Eingabeaufforderung OK den folgenden Befehl aus:

   ```
   set console='comconsole,vidconsole'
   ```

5. Führen Sie den Befehl **boot -s** aus, um NetScaler ADM neu zu starten.
6. Nachdem die Meldung **Enter full path of shell oder RETURN for /bin/sh:** angezeigt wird, drücken Sie die **Eingabetaste**, um die Eingabeaufforderung /u@ zu erhalten.
7. Mounten Sie die Flash-Partition mit dem folgenden Befehl:

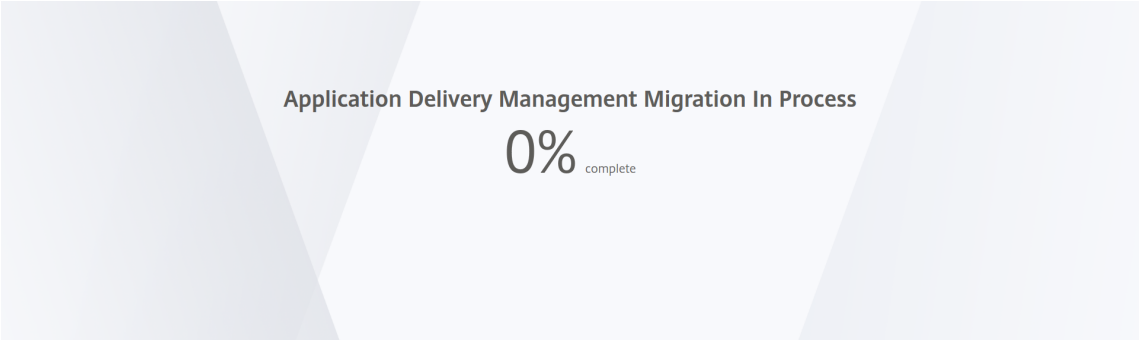
   ```
   mount dev/vtbd0s1a /flash
   ```

8. Erstellen Sie eine Datei mit dem folgenden Befehl:

   ```
   touch /flash/mpsconfig/.recover
   ```

   Das Kennwort wird nun auf das Standardkennwort zurückgesetzt.

9. Führen Sie den Befehl **Neustart** aus, um NetScaler ADM neu zu starten.
10. Greifen Sie auf die NetScaler ADM GUI zu und warten Sie, bis der Neustart abgeschlossen ist.



Sie können jetzt *nsroot/nsroot* Anmeldeinformationen verwenden, um sich von der GUI anzumelden, und *nsrecover/nsroot*, um sich von der SSH-Konsole aus anzumelden.

> Hinweis
>
> Wenn das Kennwort nach dem Neustart nicht auf das Standardkennwort zurückgesetzt wurde, wiederholen Sie den Vorgang (Schritt 1 bis Schritt 7). Führen Sie dann die folgenden Befehle aus und starten Sie NetScaler ADM neu:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Konfigurieren einer sekundären Netzwerkkarte für den Zugriff auf NetScaler ADM

February 5, 2024

Sie können eine zweite Netzwerkkarte konfigurieren, um den Verwaltungszugriff auf NetScaler ADM zu isolieren. Mit dieser zweiten NIC-Funktion können Sie je nach Anforderung auswählen, wie Sie den über NetScaler ADM empfangenen und gesendeten Datenverkehr isolieren möchten.

Stellen Sie sich ein Szenario vor, in dem Sie den Datenverkehr isolieren möchten, um:

- Führen Sie die gesamte Kommunikation zwischen NetScaler ADM und seinen verwalteten NetScaler-Instanzen in einem Netzwerk durch.
- Haben Sie Verwaltungszugriff auf NetScaler ADM in einem anderen Netzwerk.

In diesem Szenario können Sie als Administrator:

- Konfigurieren Sie eine IP-Adresse für den Datenverkehr zwischen NetScaler ADM und seinen verwalteten NetScaler-Instanzen.
- Konfigurieren Sie eine andere IP-Adresse für die Verwaltung der NetScaler ADM-Software, um alle administrativen Aufgaben in der Software auszuführen.

> **Hinweis**
>
> Wenn NetScaler ADM als HA-Paar konfiguriert ist, wird die auf der zweiten Netzwerkkarte konfigurierte Verwaltungs-IP-Adresse dem primären Knoten zugeordnet.

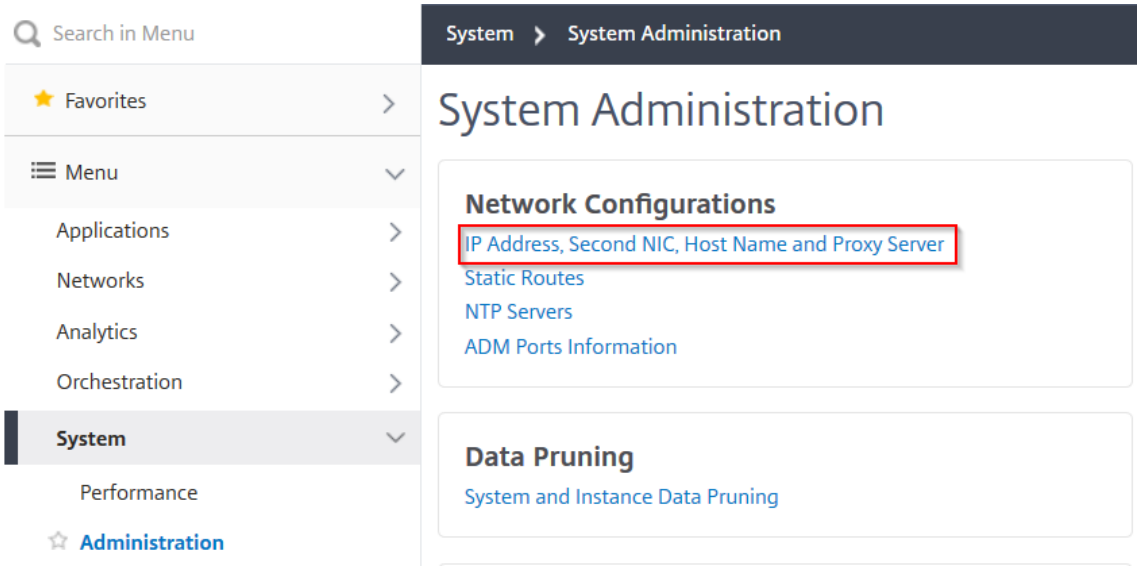
Voraussetzungen

- Stellen Sie sicher, dass Sie **NetScaler ADM 13.0 Build 47.x oder höher** auf dem Hypervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM oder VMware ESXi) bereitgestellt und konfiguriert haben.
- Stellen Sie sicher, dass Sie die zweite Netzwerkkarte auf dem Hypervisor hinzugefügt haben (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM oder VMware ESXi).

Informationen zum Zuweisen einer IP-Adresse zu einer Netzwerkkarte auf einem Citrix Hypervisor und zum Erstellen einer sekundären Schnittstelle finden Sie unter Zuweisen einer IP-Adresse zu einer Netzwerkkarte.

Konfigurieren Sie eine zweite Netzwerkkarte in NetScaler ADM

1. Melden Sie sich bei ADM GUI an.
2. Navigieren Sie zu **Einstellungen > Administration**.
3. Klicken Sie unter **Netzwerkkonfiguration**auf **IP-Adresse, Zweite Netzwerkkarte, Hostname und Proxyserver**.



Die Seite **Netzwerkkonfiguration** wird angezeigt.

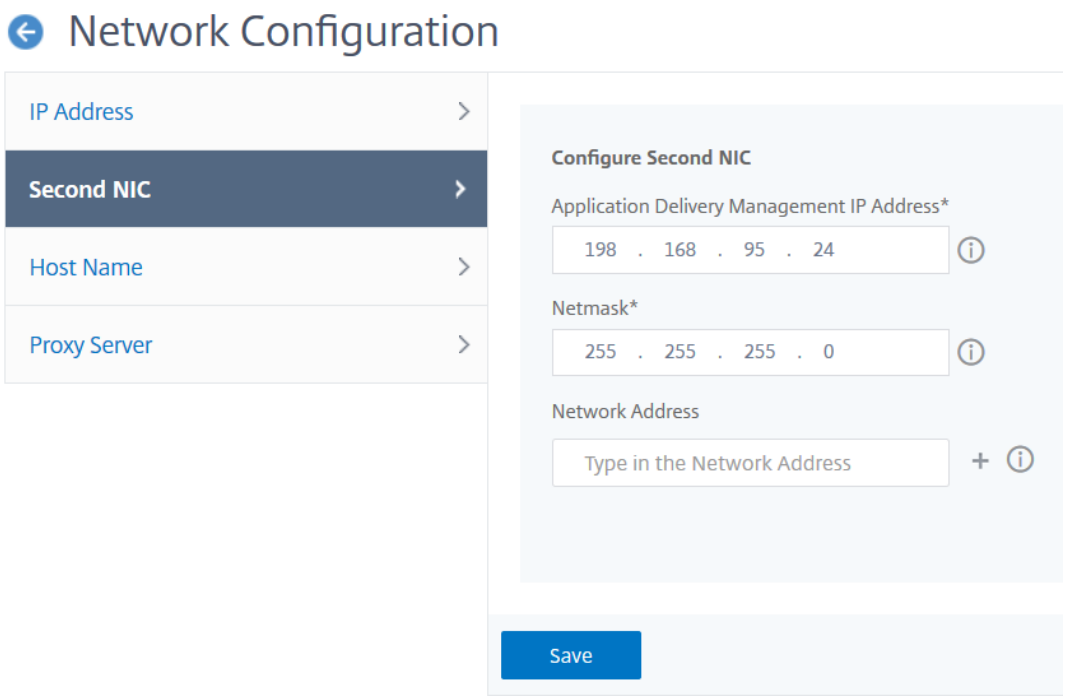
4. Klicken Sie auf die Registerkarte Zweite NIC und konfigurieren Sie die folgenden Parameter:

   a) **IP-Adresse für Application Delivery Management** —Geben Sie eine gültige IP-Adresse für den Zugriff auf NetScaler ADM ein. Sie können diese IP-Adresse für den Zugriff auf NetScaler ADM verwenden, abgesehen von der vorhandenen Verwaltungs-IP-Adresse.

   b) **Netzmaske** —Geben Sie die Netzmaskenadresse ein, um den Netzwerk-Host anzugeben. Die Standardadresse ist 255.255.255.0.

   c) **Netzwerkadresse** —Geben Sie eine IP-Adresse ein, um einen Routeneintrag für NetScaler ADM hinzuzufügen. Klicken Sie auf **+**, um weitere IP-Adressen hinzuzufügen. Das Feld ist optional.

   d) Klicken Sie auf **Speichern**.



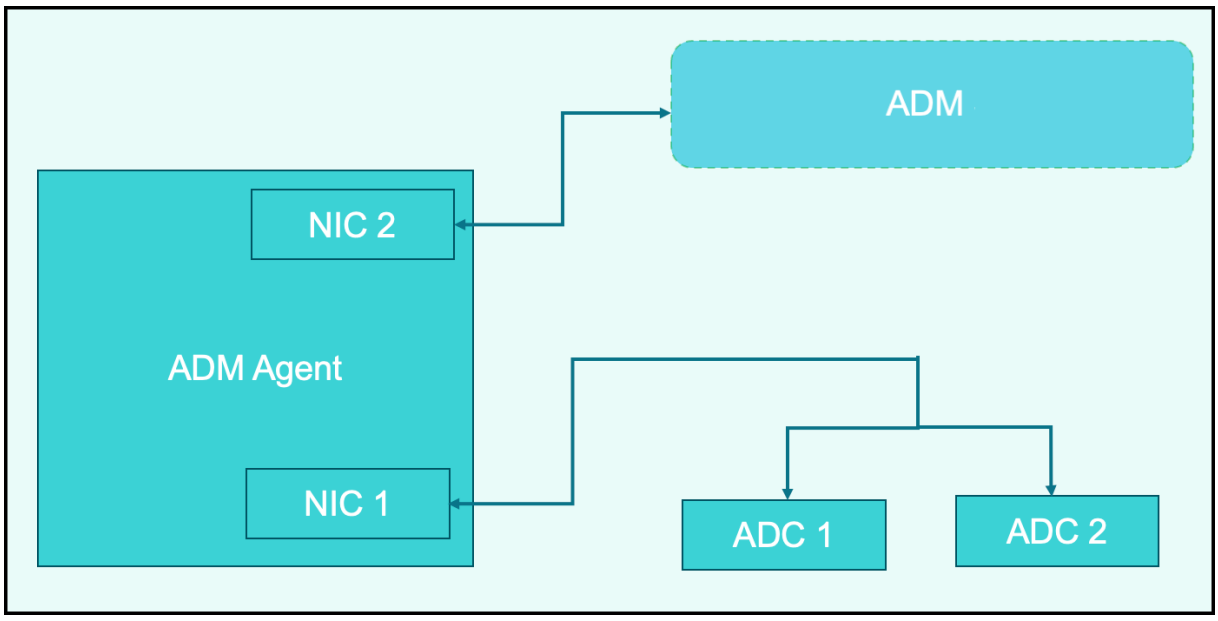
Konfigurieren einer sekundären Netzwerkkarte für den Zugriff auf ADM-Agenten

February 5, 2024

Sie können zwei Netzwerkkarten auf einem ADM-Agent konfigurieren. Mit der Dual-NIC-Architektur kann der ADM-Agent:

- Stellen Sie die Kommunikation zwischen ADM-Agent und ADC-Instanzen her - Sie können die erste Netzwerkkarte verwenden, um den über NetScaler ADM empfangenen und gesendeten Datenverkehr zu isolieren und um zwischen NetScaler ADM und seinen verwalteten NetScaler-Instanzen in einem anderen Netzwerk zu kommunizieren.
- Stellen Sie die Kommunikation zwischen dem ADM-Agenten und NetScaler ADM her - Sie können die zweite Netzwerkkarte verwenden, um den NetScaler ADM in einem Netzwerk zu verwalten und administrative Aufgaben auszuführen

> **Hinweis**
>
> Sie können die Funktionalität und Konfiguration der beiden Netzwerkkarten nicht austauschen.



In diesem Szenario können Sie als Administrator:

- Konfigurieren Sie die IP-Adresse für den Datenverkehr zwischen NetScaler ADM und seinen verwalteten NetScaler-Instanzen.
- Konfigurieren Sie die IP-Adresse für die Verwaltung der NetScaler ADM-Software, um alle administrativen Aufgaben in der Software auszuführen.

> **Hinweis**
>
> Es ist nicht zwingend erforderlich, Dual-NICs für einen ADM-Agent zu konfigurieren. Es ist optional und nur erforderlich, wenn der Datenverkehr zwischen ADM-Agent, NetScaler ADM und ADCs getrennt werden muss.

IPV4-NIC-Netzwerkadressen über die CLI ändern

1. Öffnen Sie mit einen SSH-Client wie PuTTY eine SSH-Verbindung zur NetScaler ADM Agent-Konsole.
2. Melden Sie sich mit den **nsrecover/nsroot-Anmeldeinformationen** an und wechseln Sie zur Shell-Eingabeaufforderung.
3. Führen Sie den Befehl **ifconfig** aus. Sie können die Details der beiden Netzwerkkarten sehen, die Sie konfiguriert haben -
    - NIC 1 —Für die Kommunikation zwischen ADM-Agent und ADC
    - NIC 2 —Für die Kommunikation zwischen ADM Agent und NetScaler ADM


```
bash-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
pflog0: flags=0<> metric 0 mtu 33152
        groups: pflog
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether a2:56:cd:d2:f8:8c
        hwaddr a2:56:cd:d2:f8:8c
        inet6 fe80::a056:cdff:fed2:f88c%1/1 prefixlen 64 scopeid 0x3
        inet 10.102.103.247 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
1/2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 32:89:fe:8c:8f:45
        hwaddr 32:89:fe:8c:8f:45
        inet6 fe80::3089:feff:fe8c:8f45%1/2 prefixlen 64 scopeid 0x4
        inet 10.102.103.250 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
```

4. Führen Sie den Befehl **networkconfig** aus. Es erscheint ein Menü, in dem Sie die IPV4-Netzwerkadressen festlegen oder ändern können.

```
bash-3.2# /mps/networkconfig

------------------------------------------------------------------------------
Citrix ADM Agent initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
------------------------------------------------------------------------------
     1. Citrix ADM Agent Host Name [ns]:
     2. Citrix ADM Agent IPv4 address [10.102.103.247]:
     3. Netmask [255.255.255.0]:
     4. Gateway IPv4 address [10.102.103.1]:
     5. DNS IPv4 Address [10.102.166.70]:
     6. Second NIC IPv4 address [10.102.103.250]:
     7. Second NIC Netmask [255.255.255.0]:
     8. Second NIC Network address [10.102.103.251,10.102.103.252,10.102.103.252]:
     9. Second NIC Gateway IPv4 address [10.102.103.2]:
    10. Cancel and quit.
    11. Save and quit.
```

> **Hinweis**
>
> Die zweite Netzwerkadresse der Netzwerkkarte kann mehrere IP-Werte annehmen.

5. Wählen Sie einen zu ändernden Menüpunkt aus. Speichern und beenden Sie die Einstellungen.

Syslog-Löschintervall konfigurieren

February 5, 2024

Syslog ist ein Standardprotokoll für die Protokollierung. Es besteht aus zwei Komponenten: dem Syslog-Auditing-Modul, das auf der Citrix Application Delivery Controller (ADC) -Instanz läuft, und dem Syslog-Server, der entweder auf dem zugrunde liegenden FreeBSD-Betriebssystem (OS) der NetScaler-Instanz oder auf einem Remote-System ausgeführt werden kann. SYSLOG verwendet das User Datagram Protocol (UDP) für die Datenübertragung.

Syslog ermöglicht die Isolierung des Systems, das Informationen generiert, und des Systems, in dem die Informationen gespeichert werden. Sie können Protokollinformationen konsolidieren und Erkenntnisse aus den gesammelten Daten gewinnen. Sie können syslog auch so konfigurieren, dass verschiedene Arten von Ereignissen protokolliert werden.

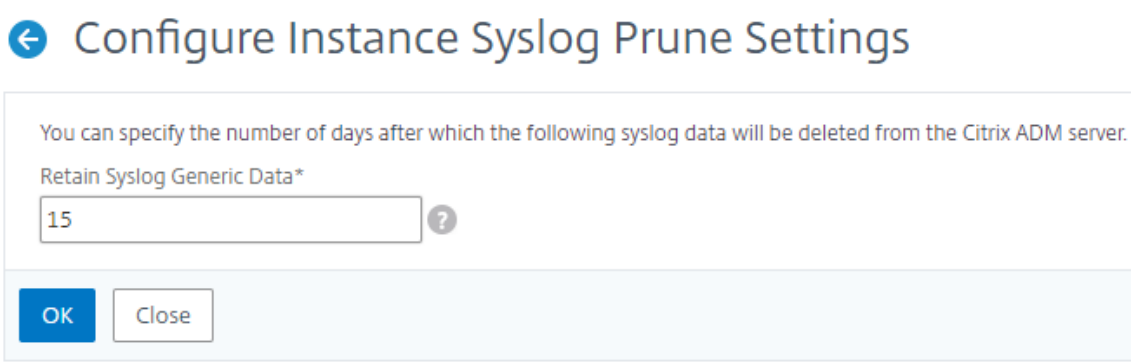
Um die Menge der in der Datenbank gespeicherten Syslog-Daten zu begrenzen, können Sie das Intervall angeben, in dem Sie Syslog-Daten löschen möchten. Sie können die Anzahl der Tage angeben, nach denen die folgenden Syslog-Daten aus NetScaler Application Delivery Management (ADM) gelöscht werden:

- Generische Syslog-Daten
- AppFirewall-Daten
- NetScaler Gateway Daten

Sie können das NetScaler Gateway-Bereinigen auch anhand des Syslog-Typs konfigurieren. Dieses Bereinigen hat Vorrang vor dem Runenintervall, das für die Aufbewahrung von NetScaler Gateway-Daten konfiguriert ist.

So konfigurieren Sie die Einstellungen für das Syslog-Prune-Intervall für NetScaler ADM:

1. Navigieren Sie zu **Einstellungen > Administration**.Klicken Sie unter **Datenbereinigung**auf **System- und Instanzdatenbereinigung**, und klicken Sie dann auf **Instanzsyslog**.
2. Geben Sie auf der Seite **Einstellungen für Instanz Syslog-Bereinigung konfigurieren** die Option **Generische Syslog-Daten (Tage) beibehalten**an. Geben Sie die Anzahl der Tage ein, für die NetScaler ADM generische Syslog-Nachrichten aufbewahrt.



Konfigurieren der Einstellungen für Systembeschneidung und Event-Prune

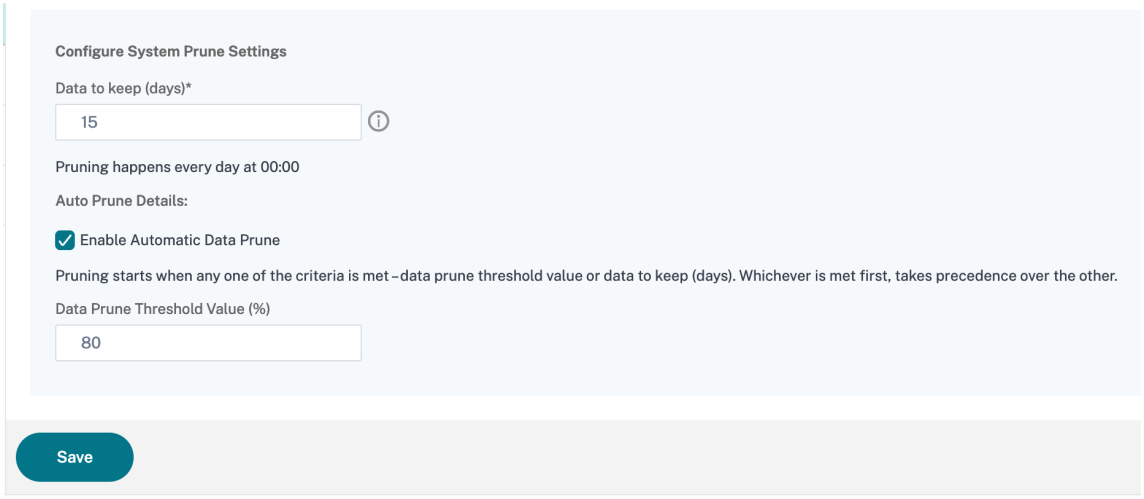
February 5, 2024

Um die Menge der Berichtsdaten zu begrenzen, die in Ihrer NetScaler Application Delivery Management (ADM) -Softwaredatenbank gespeichert werden, können Sie sie bereinigen. Sie können das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle beibehalten soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00.00 Uhr) bereinigt.

> **Hinweis**
>
> Der angegebene Wert darf nicht länger als 30 Tage oder weniger als 15 Tage sein.

So konfigurieren Sie Systembereinigungseinstellungen für Leistungsberichte:

1. Navigieren Sie zu **Einstellungen** > **Administration** . Klicken Sie unter **Datenbereinigung** auf **System- und Instanzdatenbereinigung**.
2. Geben Sie auf der Seite **Configure System Prune Settings** Folgendes an:
   - Anzahl der Tage für die Aufbewahrung der Daten
   - Prozentsatz des Speicherplatzes (Bereinigungsschwellenwert)
3. Klicken Sie auf **OK**.



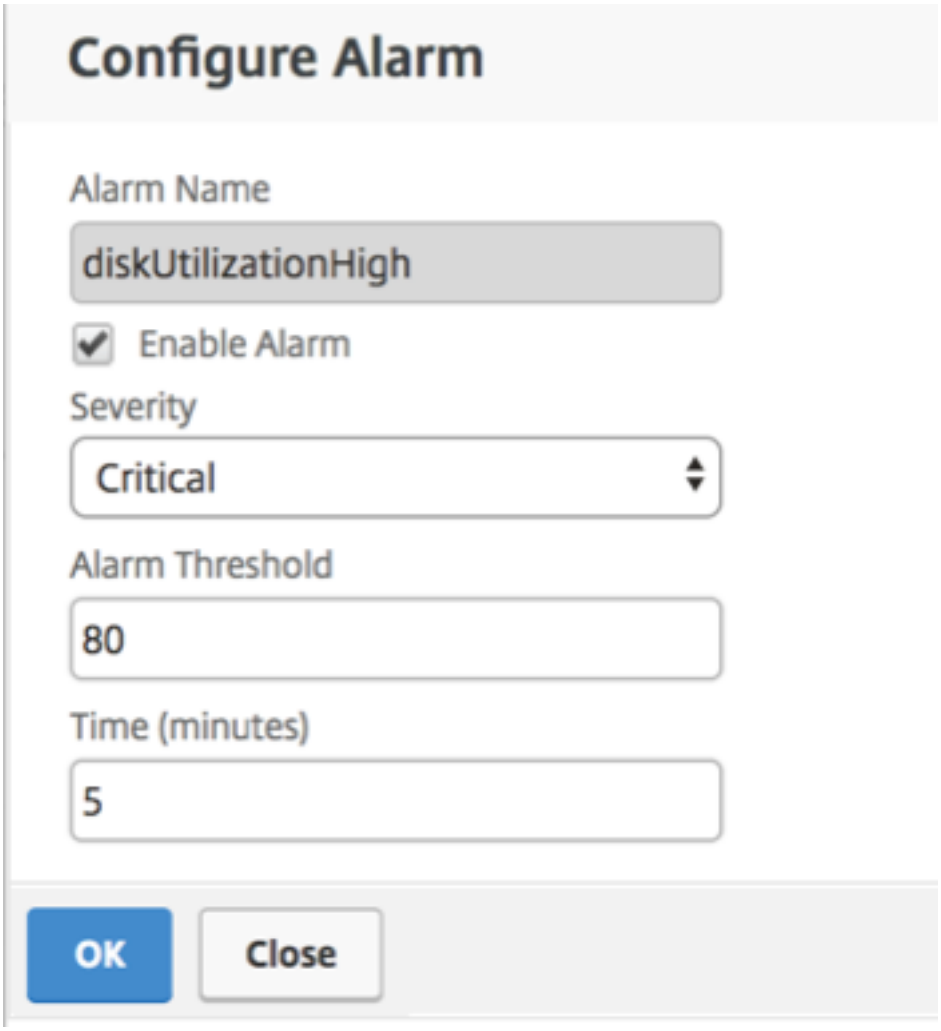
Sie können das automatische Bereinigen aktivieren, indem Sie das Kontrollkästchen **Automatische Datenbereinigung aktivieren** aktivieren. Ein Alarm wird ausgelöst und eine E-Mail wird gesendet, wenn die Datenträgernutzung den konfigurierten **Schwellenwert für Datenbereinigung** verletzt.

> **Hinweis**
>
> Die Bereinigung beginnt, wenn eines der Kriterien erfüllt ist —Schwellenwert für Datenbereinigung oder aufzubewahrende Daten (Tage). Was zuerst getroffen wird, hat Vorrang vor dem anderen.

So konfigurieren und aktivieren Sie Alarmeinstellungen:

1. Navigieren Sie zu **Einstellungen** > **SNMP** . Klicken Sie in der oberen rechten Ecke auf **Alarme**.
2. Wählen Sie den Alarm aus, den Sie konfigurieren möchten (z. B. diskUtilizationHigh) und klicken Sie auf **Bearbeiten**.
3. Geben Sie auf der Seite **Alarm konfigurieren** Folgendes an:

- **Schweregrad**—Wählen Sie den Schweregrad
- **Alarmschwelle**—Geben Sie den Wert ein, für den die Schwere des Ereignisses berechnet wird.
- **Zeit**—Geben Sie die Zeit (in Minuten) ein, nach der Sie den Alarm auslösen möchten.



Konfigurieren von Einstellungen für die Ereignisbereinigung mit NetScaler ADM

Um die Menge der in Ihrer NetScaler ADM-Datenbank gespeicherten Ereignisnachrichten zu begrenzen, können Sie das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Audit-Logs und Task-Protokolle speichern soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00.00 Uhr) bereinigt.

1. Navigieren Sie zu **Einstellungen > Verwaltung > Datenbereinigung**, und klicken Sie auf **System- und Instanzdatenbereinigung**. Klicken Sie auf **Instanzereignisse**.
2. Geben Sie das Zeitintervall in Tagen ein, für das Sie die Daten auf dem NetScaler ADM Server behalten möchten, und klicken Sie auf **Speichern**.

Shell-Zugriff für nicht standardmäßige Benutzer aktivieren

February 5, 2024

In NetScaler Application Delivery Management (ADM) können Sie den Shell-Zugriff für Benutzer aktivieren, die keine Standardbenutzer sind. Sie können diese Funktion verwenden, um den Kommunikationsmodus mit Instanzen zu aktivieren und einzurichten.

> **Hinweis**
>
> Standardmäßig ist der Shell-Zugriff für Nicht-Standardbenutzer deaktiviert.

Gehen Sie wie folgt vor, um den Shell-Zugriff für Nicht-Standardbenutzer in NetScaler ADM zu aktivieren:

1. Navigieren Sie in NetScaler ADM zu **Einstellungen > Administration**.
2. Klicken Sie unter **Systemkonfigurationen**auf **System, Zeitzone, Zulässige URLs und Agenteneinstellungen**.
3. Konfigurieren Sie auf der Seite **Systemkonfigurationen** die folgenden Parameter:

    - **Kommunikation mit Instanzen** —Wählen Sie das Kommunikationsprotokoll aus.
    - **Sicherer Zugriff** —Aktivieren Sie den sicheren Zugriff für NetScaler ADM.
    - **Sitzungs-Timeout aktivieren** —Geben Sie den Zeitraum an, für den eine inaktive Sitzung beibehalten werden soll.
    - **Standardauthentifizierung zulassen** - Zulassen, dass der Verwaltungsdienst Anmeldeinformationen akzeptiert, die mit dem Standardauthentifizierungsprotokoll angegeben wurden.
    - **Nsrecover Login** aktivieren - `nsrecover` Anmeldung bei Management Service aktivieren.
    - **Zertifikatdownload aktivieren** : Ermöglicht das Herunterladen von Zertifikaten aus dem hinzugefügten NetScaler.
    - **Shell-Zugriff für Nicht-nsroot-Benutzer** aktivieren —Aktivieren Sie den Shell-Zugriff für Nicht-Standardbenutzer in NetScaler ADM.
    - **Benutzeranmeldedaten für Instanzanmeldung anfordern** —Erlauben Sie Benutzern, ihre Benutzeranmeldeinformationen einzugeben, während sie sich von NetScaler ADM aus an Instanzen anmelden.
        - **Eingabeaufforderung für Stylebooks-Operationen** —Erlaubt Benutzern, ihre Benutzeranmeldeinformationen einzugeben, während sie StyleBook- und Config Pack-Operationen auf NetScaler-Instanzen verwenden.

> **Hinweis:**
> Wenn **Prompt Credentials for Instance Login** ausgewählt ist und **Prompt Credentials for Stylebook Operations** deaktiviert ist, werden Benutzer nicht aufgefordert, Anmeldeinformationen für StyleBook- und Config Pack-Operationen auf NetScaler-Instanzen einzugeben.

4. Klicken Sie auf **OK**.

Nicht zugängliche NetScaler ADM-Server wiederherstellen

February 5, 2024

NetScaler Application Delivery Management (ADM) bietet jetzt ein Tool zur Datenbankverwaltung, mit dem die Systemdatenbank bereinigt werden kann. Sie können jetzt das NetScaler ADM Utility Tool starten, um eine Verbindung zum Dateisystem herzustellen, einige Komponenten zu löschen und die Datenbank zugänglich zu machen. Das NetScaler ADM-Wiederherstellungsskript ist ein Tool, mit dem Speicherplatz im Dateisystem wiederhergestellt werden kann, indem alte oder ungenutzte Datenbanktabellen und -dateien gelöscht werden. Das Tool unterstützt Sie dabei, in aufeinanderfolgenden Schritten durch die Datenbanktabellen und -dateien zu navigieren, und zeigt den aktuellen Speicherplatz, der von den jeweiligen Elementen im Dateisystem belegt wird. Nachdem Sie die zu löschenden Datenbanktabellen und Dateien ausgewählt haben, löscht das Tool diese nach Bestätigung aus dem Dateisystem.

So verwenden Sie das NetScaler ADM Database Recovery Script für eine eigenständige NetScaler ADM-Bereitstellung

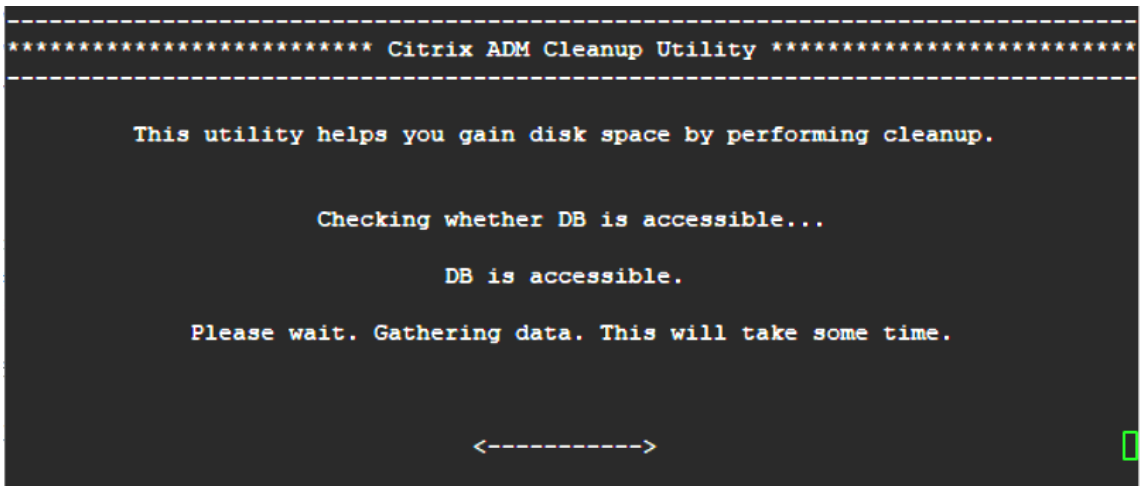
Verwenden Sie das folgende Verfahren in einer NetScaler ADM Bereitstellung für einen Server, um eine Verbindung mit dem Dateisystem herzustellen, einige Komponenten zu löschen, die Datenbank zugänglich zu machen und dann die Wiederherstellungsvorgänge durchzuführen.

1. Melden Sie sich mit einem SSH-Client oder der Konsole Ihres Hypervisors bei NetScaler ADM an und geben Sie den folgenden Befehl ein:

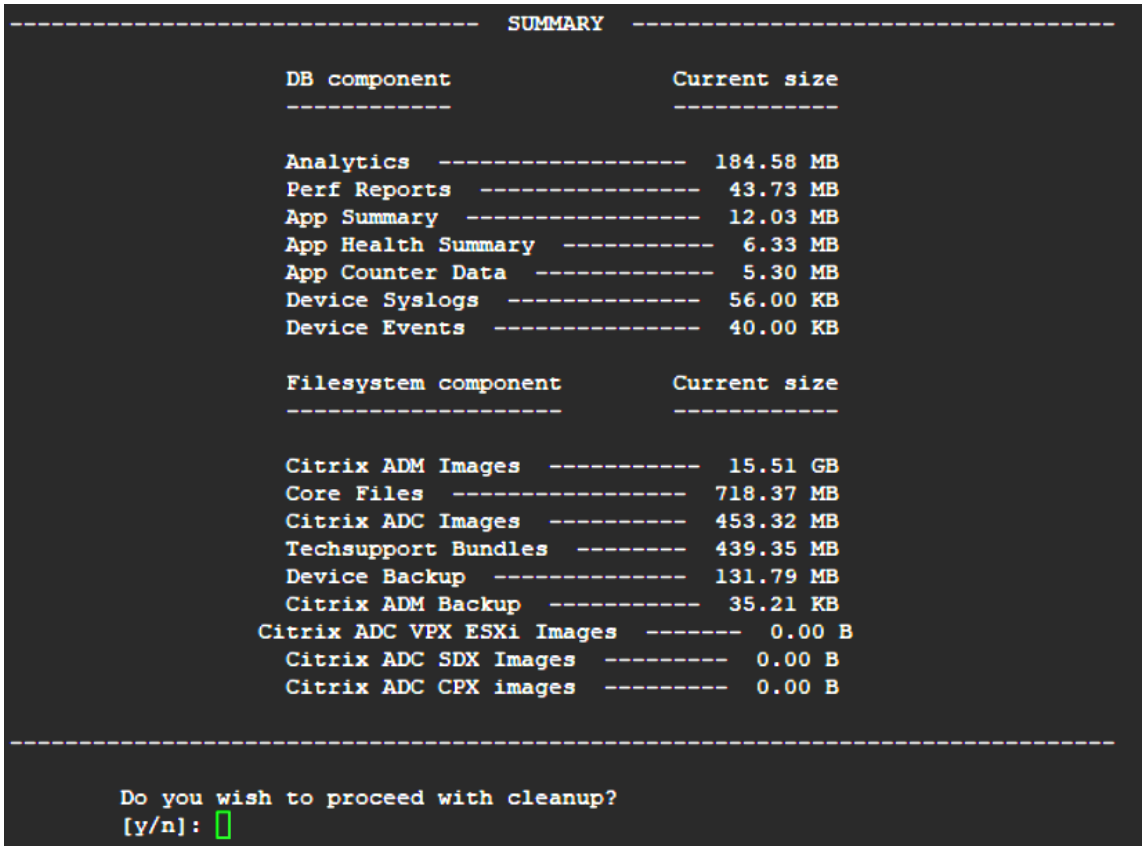
```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

2. Wenn auf dem Bildschirm eine Warnmeldung zum Beenden einiger NetScaler ADM Prozesse angezeigt wird, geben Sie “y”ein, und drücken **Sie die Eingabetaste**.

   Der folgende Bildschirm wird angezeigt, während das System bestimmt, welche Komponenten der Datenbank Sie löschen können, ohne dass sich auf die Kerndateien des Systems auswirkt.



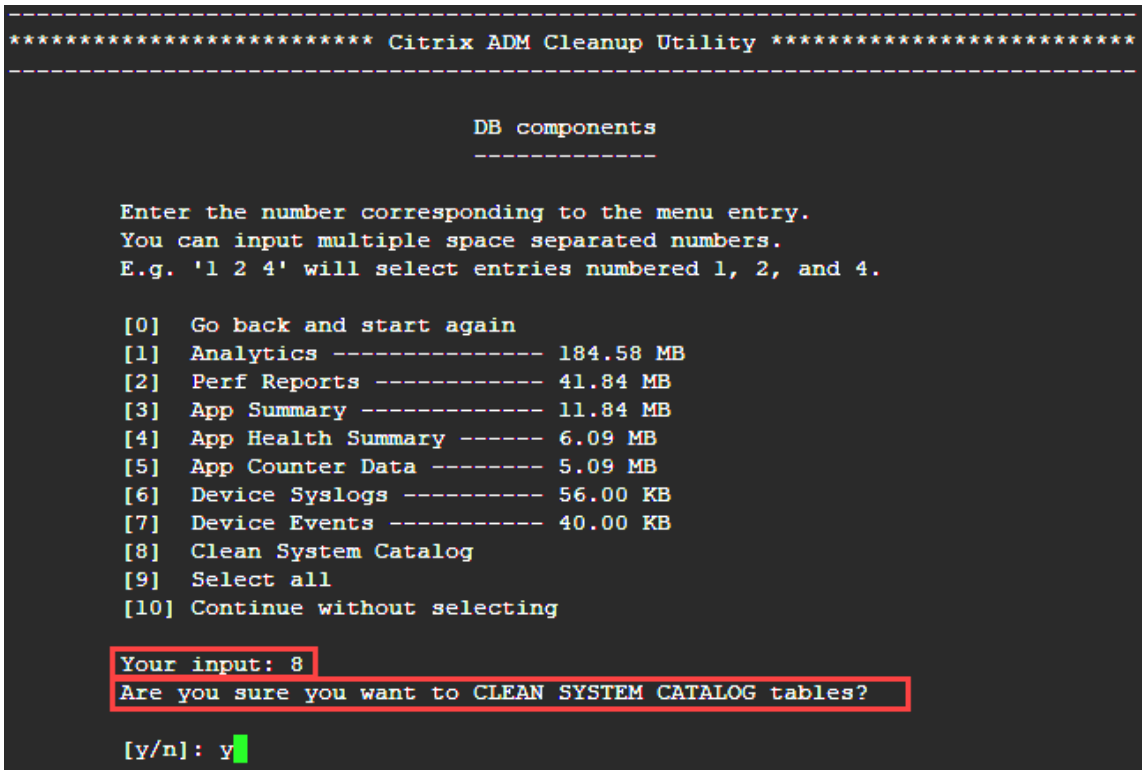
3. Auf dem Bildschirm wird die Liste der Dateien in der Datenbank angezeigt. Geben Sie “y”ein und drücken Sie die Eingabetaste, um den Bereinigungsprozess zu starten.



4. Sie können die spezifische Datenbankkomponente auswählen, die gereinigt werden muss, und die entsprechende Nummer eingeben. Drücken Sie die **Eingabetaste**.

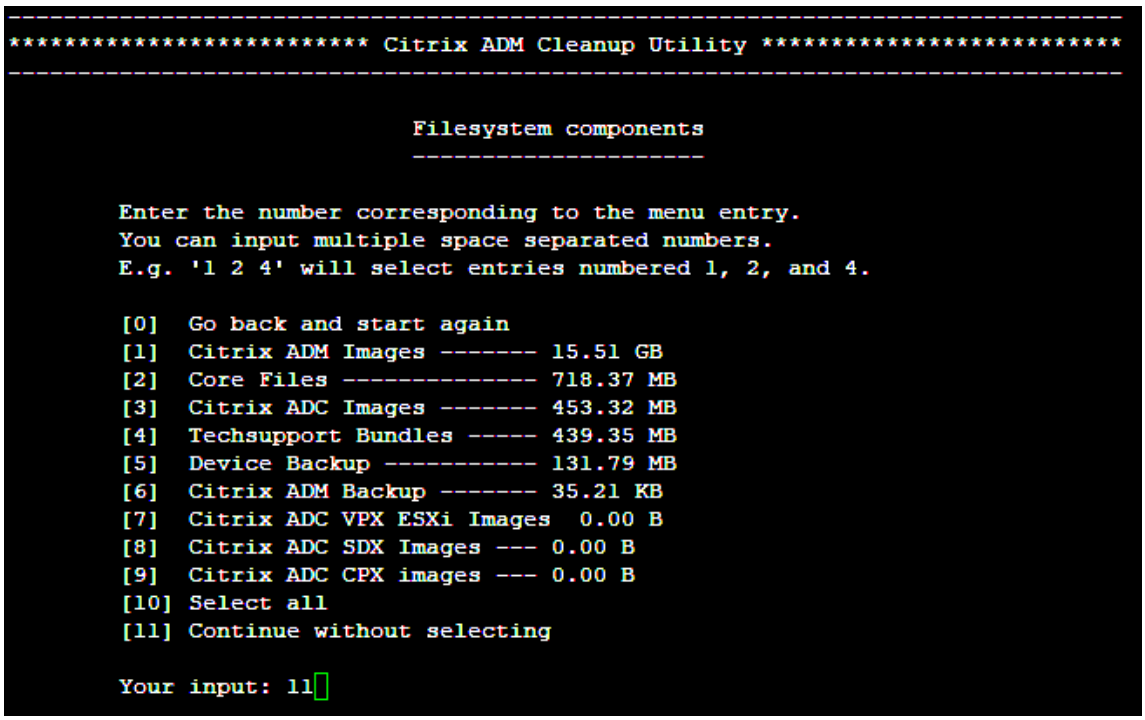
   Um beispielsweise den Systemkatalog zu bereinigen, wählen Sie Option 8 im **DB-Komponentenauswahlme** aus, geben Sie “y”ein und drücken Sie die **Eingabetaste**, um mit der Bereinigung des Systemkatalogs fortzufahren.

> **Hinweis**
>
> NetScaler ADM enthält Benutzertabellen, die als Systemkatalog bezeichnet werden. Der Systemkatalog ist ein Speicherort in der NetScaler ADM-Datenbank, an dem ein relationales Datenbankverwaltungssystem Schematometadaten wie Informationen über Tabellen und Spalten sowie interne Datensätze speichert. Die Tabellen im Systemkatalog sind wie normale Tabellen, in denen sich im Laufe der Zeit überhöhte und tote Zeilen ansammeln können. Daher müssen sie regelmäßig bereinigt werden, um eine optimale Leistung zu erzielen. Es empfiehlt sich, diese Tabellen regelmäßig zu pflegen. Die Aktivität gibt nicht nur Speicherplatz frei, sondern verbessert auch die Gesamtleistung der Datenbank und damit des NetScaler ADM.

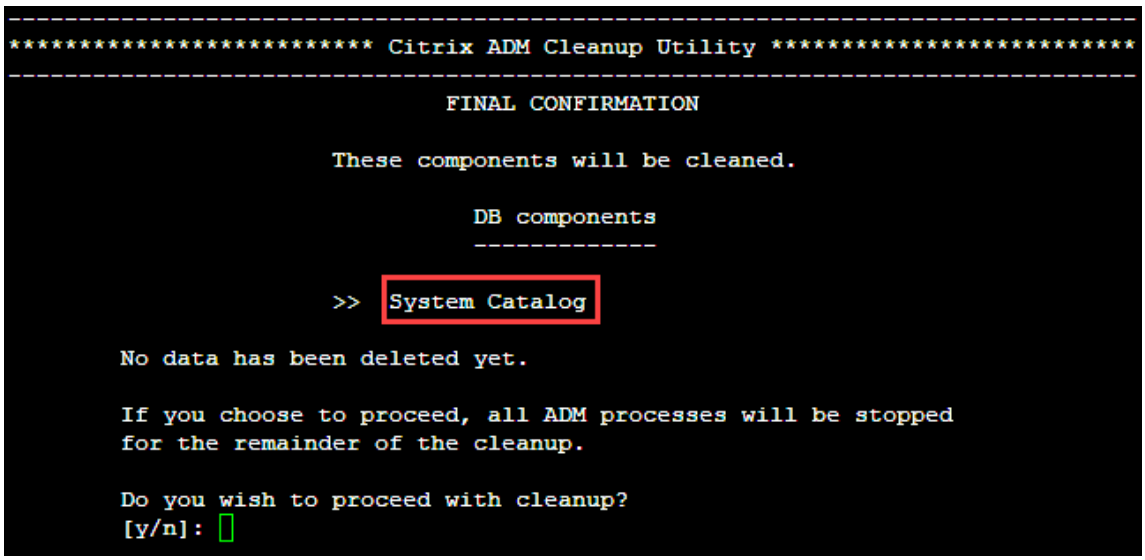


Das Cleanup-Hilfsprogramm bietet Ihnen die Möglichkeit, Datenbankkomponenten und Dateikomponenten zu bereinigen. Sie können eine beliebige Dateikomponente auswählen, indem Sie eine Zahl zwischen „1“und „9“eingeben oder „11”eingeben und die Eingabetaste drücken, um die Datenbankkomponente zu reinigen.

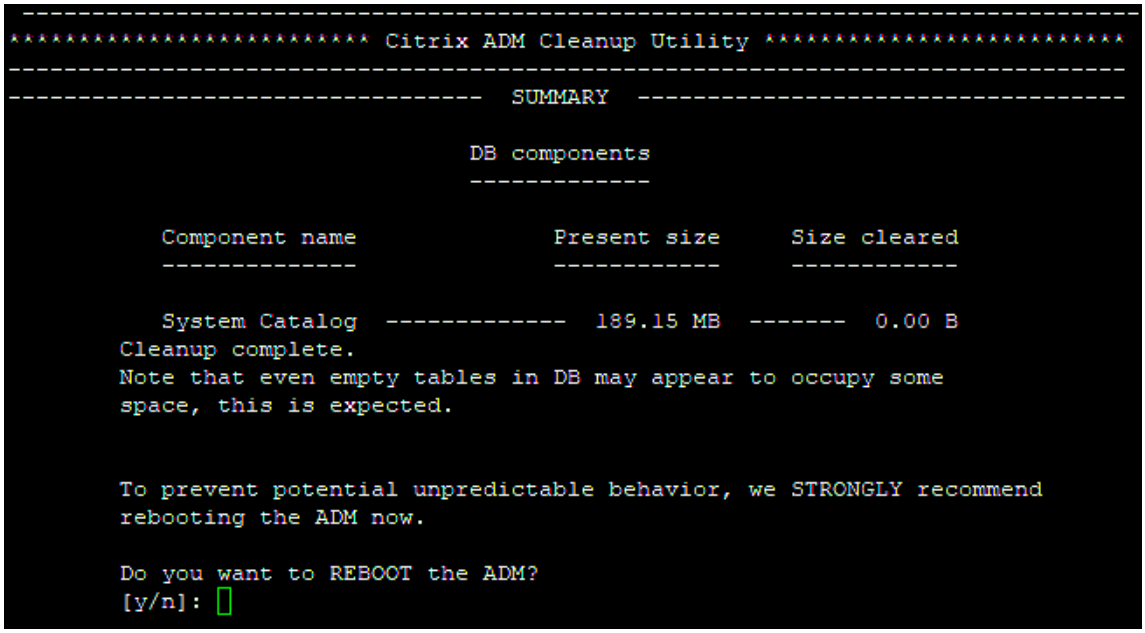
> **Hinweis**
>
> Die Zahl „11”gibt an, dass Sie keine zu reinigende Dateikomponente ausgewählt haben und dass Sie mit der Bereinigung der früheren Datenbankkomponente fortfahren, die Sie zuvor ausgewählt hatten. In diesem Beispiel ist es “Systemkatalog”.



5. Geben Sie “y”ein und drücken Sie im letzten Bestätigungsbildschirm erneut die **Eingabetaste**.



Der Systemkatalog wird bereinigt, was je nach Größe der Tabelle im Systemkatalog einige Zeit in Anspruch nehmen kann. Nach Abschluss des Vorgangs wird ein Übersichtsbildschirm angezeigt.



6. Geben Sie “y”ein und drücken Sie die **Eingabetaste**, um NetScaler ADM neu zu starten.

   Stellen Sie sicher, dass Sie NetScaler ADM nach der Systembereinigung neu starten. Warten Sie etwa 30 Minuten, bis interne Datenbankvorgänge abgeschlossen sind, nachdem NetScaler ADM neu gestartet wurde. Sie sollten dann in der Lage sein, eine Verbindung zur NetScaler ADM-Datenbank herzustellen. Wenn nicht, führen Sie das Wiederherstellungsskript erneut aus, um mehr Speicherplatz freizugeben. Wenn NetScaler ADM läuft, sollte es wie erwartet funktionieren.

   > **Hinweis**
   >
   > Die aktuelle Größe der Systemkatalogtabelle ist nie gleich Null nach dem Bereinigen. Dies liegt daran, dass nur leere Zeilen aus der Tabelle entfernt werden und die Tabelle möglicherweise einige gültige Einträge enthält, auch wenn sie bereinigt wurden.

So verwenden Sie das NetScaler ADM-Datenbankwiederherstellungsskript für eine NetScaler ADM-Hochverfügbarkeitsbereitstellung

Das Datenbanksystem für NetScaler ADM-Server in einer Hochverfügbarkeitsbereitstellung befindet sich im kontinuierlichen Synchronisationsmodus. Wenn Sie das neue Tool zur Datenbankwiederherstellung verwenden, müssen Sie das Verfahren nicht auf beiden NetScaler ADM-Servern replizieren.

1. Melden Sie sich mit einem SSH-Client oder der Hypervisor-Konsole am primären Knoten an.
2. Führen Sie den folgenden Befehl aus:

   ```
   /mps/mas_recovery/mas_recovery.py
   ```


3. Befolgen Sie das Verfahren aus Schritt 2, das für das NetScaler ADM Standalone Deployment Recovery Scriptverfügbar ist

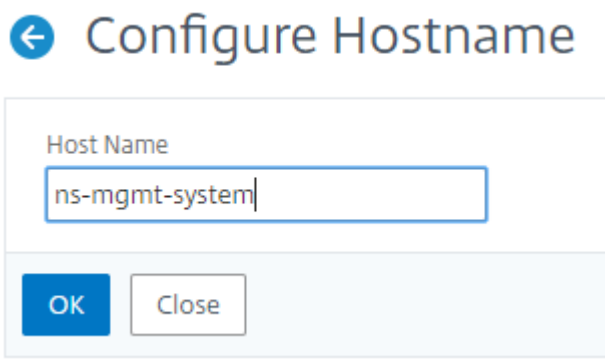
Hostnamen zu einem NetScaler ADM-Server zuweisen

February 5, 2024

Um einen NetScaler Application Delivery Management (ADM) -Server zu identifizieren, können Sie dem Server einen Hostnamen zuweisen. Der Hostname wird in der universellen Lizenz für NetScaler ADM angezeigt.

So weisen Sie einem NetScaler ADM-Server einen Hostnamen zu:

1. Navigieren Sie in NetScaler ADM zu **System** > **Systemadministration**.
2. Klicken Sie unter **Systemeinstellungen** auf **Hostname ändern**.
3. Geben Sie auf der Seite **Hostname konfigurieren** einen Hostnamen ein, und klicken Sie auf **OK**.



> **Hinweis**
>
> Sie können den Befehl `networkconfig` auch in Ihrem Hypervisor verwenden und den Hostnamen ändern.

Backup und Wiederherstellen des NetScaler ADM-Servers

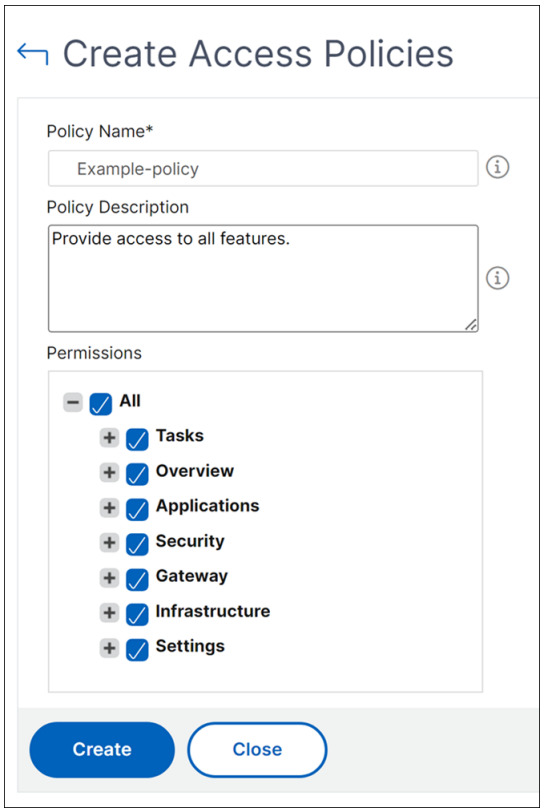
February 5, 2024

Sie können regelmäßige Backups Ihres NetScaler ADM-Servers erstellen. Sie können die Konfigurationsdateien, Instanzdetails, Systemdaten usw. sichern und wiederherstellen.

Wichtig

Citrix empfiehlt, den ADM-Server mit einer Backup derselben Version wiederherzustellen. Wenn die ADM-Version beispielsweise 13.0 ist, verwenden Sie das 13.0-ADM-Backup, um den Server wiederherzustellen.

Der Benutzerzugriff zum Backup und Wiederherstellen des ADM-Servers ist begrenzt. Die Seite **Einstellungen > Backupdateien** wird nur Benutzern angezeigt, die Zugriff auf alle ADM-Funktionen haben. Ein Benutzer kann nur auf diese Seite zugreifen, wenn seine Zugriffsrichtlinie über alle Berechtigungen verfügt. In der Regel haben Superuser Zugriff auf alle ADM-Funktionen.



Weitere Informationen finden Sie unter Konfigurieren von Zugriffsrichtlinien.

Sichern Sie vor dem Upgrade die ADM-Serverkonfigurationsdateien aus Sicherheitsgründen.

Das Backup umfasst die folgenden Komponenten:

- NetScaler ADM-Konfigurationsdateien:
  - SNMP
  - Syslog-Serverkonfigurationsdateien
  - NTP-Dateien
  - SSL-Zertifikate

  - Control Center-Dateien
- Backups von NetScaler-Instanzen, die der NetScaler ADM-Server verwaltet.
- Vorlagen für Konfigurationsprüfungen.
- In der Datenbank gespeicherte Systemdaten:
  - Liste der erstellten Mandanten und Benutzer.
  - Konfiguration des externen Authentifizierungsservers (LDAP, RADIUS und andere).
  - Konfigurationsaufträge und Jobvorlagen wurden erstellt.
- In der Datenbank gespeicherte Infrastruktur- und Anwendungsdaten:
  - Daten von hinzugefügten und verwalteten NetScaler-Instanzen.
  - Instanzprofildetails, Versionsdetails, Instanzgruppendetails usw.
  - Eine statische Anwendung (Gruppe virtueller Server), die vom Administrator erstellt wurde.
- SNMP-Einstellungen.

> **Note**
>
> Analytics-Daten, Ereignisse, ADM-Lizenzen und Syslog-Nachrichten sind vom Backup ausgeschlossen.

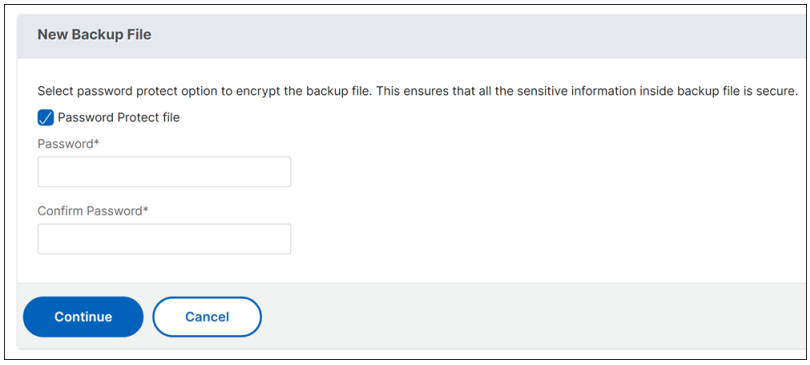
Sichern der NetScaler ADM Konfiguration

Standardmäßig sichert der NetScaler ADM Server die Konfiguration alle 24 Stunden (um 00.30 Uhr). Sie können auch die Uhrzeit für das Backup planen und auswählen. Außerdem können Sie eine Kopie der gesicherten Datei auf ein anderes System verschieben.

Das Backup wird als komprimierte TAR-Datei gespeichert, die auch verschlüsselt werden kann. Standardmäßig werden drei Sicherungsdateien auf dem Server aufbewahrt. Um Probleme mit geringem Speicherplatz zu vermeiden, können Sie maximal 10 Backupdateien auf dem NetScaler ADM -Server speichern. Citrix empfiehlt jedoch, einige Kopien Ihrer Backupdateien auf dem Server zu speichern oder die Dateien vorsorglich auf ein anderes System zu übertragen .

So Backup Sie eine NetScaler ADM-Konfiguration:

1. Navigieren Sie zu **Einstellungen> Backupdateien**, und klicken Sie dann auf **Sichern**.
2. Um die Backupdatei zu verschlüsseln, aktivieren Sie das Kontrollkästchen **Kennwortschutzdatei**, und geben Sie dann ein Kennwort zum Verschlüsseln der Datei ein.

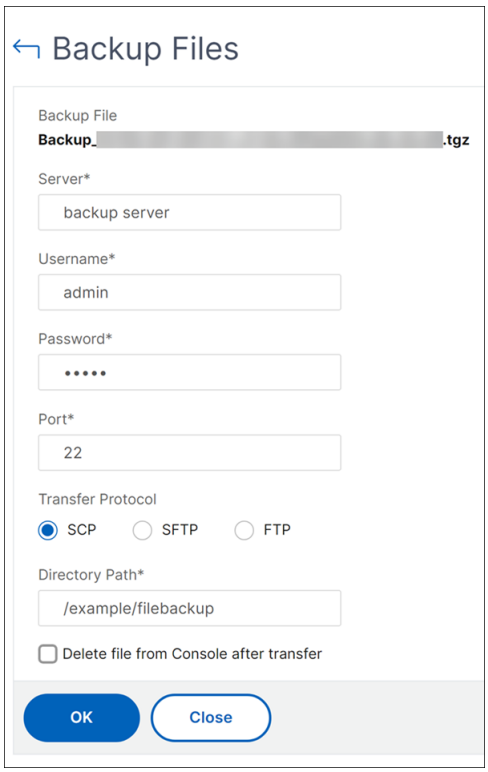


Übertragen einer NetScaler ADM -Backupdatei auf ein externes System

Als Vorsichtsmaßnahme können Sie eine Kopie der Backupdatei auf ein anderes System übertragen. Wenn Sie die Konfiguration wiederherstellen möchten, laden Sie die Datei zuerst auf den NetScaler ADM-Server hoch und führen Sie dann den Wiederherstellungsvorgangdurch.

So übertragen Sie eine NetScaler ADM-Backup-Datei:

1. Navigieren Sie zu**Einstellungen> Backupdateien**.
2. Wählen Sie die Backupdatei aus, die Sie auf ein anderes System verschieben möchten, und klicken Sie dann auf**Übertragen**.
3. Geben Sie auf der Seite **Backup-Dateien** die folgenden Parameter an:
    - **Server** —IP-Adresse des Systems, auf das Sie die gesicherte Datei übertragen möchten.
    - **Benutzername und Kennwort** —Benutzeranmeldedaten des neuen Systems, in das die gesicherten Dateien kopiert werden.
    - **Port** —Portnummer des Systems, auf das die Dateien übertragen werden.
    - **Übertragungsprotokoll** —Protokoll, das für die Übertragung der Sicherungsdatei verwendet wird. Sie können die Protokolle SCP, SFTP oder FTP auswählen, um die gesicherte Datei zu übertragen.
    - **Verzeichnispfad** - Der Speicherort, an den die gesicherte Datei auf dem neuen System übertragen wird.
4. Sie können die Backupdatei nach der Übertragung aus NetScaler ADM löschen, indem Sie das Kontrollkästchen **Datei aus der Anwendungsübermittlungsverwaltung nach der Übertragung löschen** aktivieren.
5. Klicken Sie auf **OK**, um die Übertragung durchzuführen.



> **Hinweis**
>
> Um eine Kopie der Backupdatei in Ihrem lokalen System zu speichern, navigieren Sie zu **Einstellungen > Backupdateien**, wählen Sie die zu kopierende Datei aus und klicken Sie dann auf **Herunterladen**.

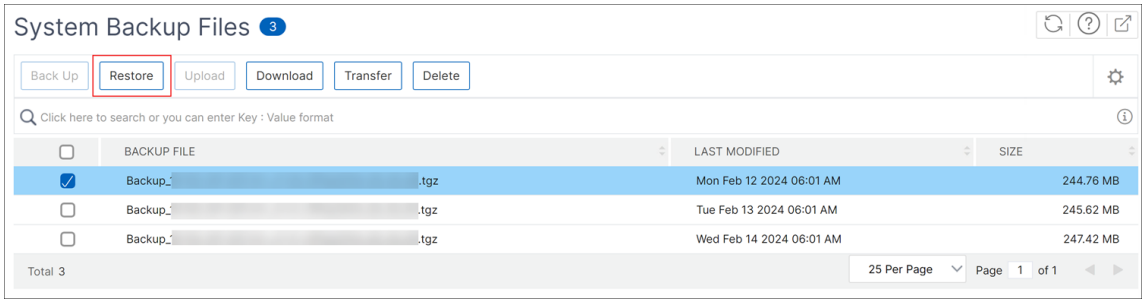
Wiederherstellen der NetScaler ADM Konfiguration aus einer Backupdatei

Wenn Sie die NetScaler ADM-Konfiguration aus einer zuvor gesicherten Datei wiederherstellen, entzieht der Wiederherstellungsvorgang die Sicherungsdatei und stellt dann die Konfiguration wieder her. Der Wiederherstellungsvorgang löscht die vorhandene Konfiguration und ersetzt sie durch die Konfiguration in der Sicherungsdatei.

> **Hinweis**
>
> Der Wiederherstellungsvorgang schlägt fehl, wenn die Sicherungsdatei umbenannt wird oder wenn der Inhalt der Sicherungsdatei geändert wird.

So stellen Sie eine NetScaler ADM Konfiguration aus einer Backupdatei wieder her:

1. Navigieren Sie zu**Einstellungen> Backupdateien**.
2. Wählen Sie die Backupdatei aus, die Sie wiederherstellen möchten, und klicken Sie dann auf **Wiederherstellen**.



3. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

> **Hinweis**
>
> Um die Konfiguration aus einer Backupdatei wiederherzustellen, die in einem externen System gespeichert ist, laden Sie die Backupdatei auf den ADM-Server hoch, bevor Sie den Wiederherstellungsvorgang ausführen. Um die Datei hochzuladen, navigieren Sie zu **Einstellungen > Backupdateien**, und klicken Sie dann auf **Hochladen**.

VM-Snapshots von NetScaler ADM in einer Bereitstellung mit hoher Verfügbarkeit

February 5, 2024

Sie können Snapshots von NetScaler ADM-Servern in der HA-Bereitstellung erstellen, bevor Sie mit dem Upgrade beginnen. Snapshots erfassen den gesamten Zustand der virtuellen Maschine zum Zeitpunkt der Aufnahme.

Erstellen Sie einen Snapshot der NetScaler ADM-Server

Verwenden Sie die folgende Sequenz, um Snapshots der NetScaler ADM-Server zu erstellen:

1. NetScaler ADM sekundärer Server
2. NetScaler ADM-Primärserver

Um einen Snapshot von NetScaler ADM-Servern zu erstellen:

1. Wählen Sie auf Ihrem Hypervisor den sekundären NetScaler ADM-Server aus der Liste der virtuellen Maschinen aus.
2. Erstellen Sie einen VM-Snapshot.

> **Hinweis:**
>
> Wir empfehlen, dass Sie beim Erstellen des Snapshots die Option **VM-Speicher** übernehmen auswählen.

3. Geben Sie dem Snapshot einen aussagekräftigen Namen und geben Sie bei Bedarf eine Beschreibung ein.

   Der Snapshot wird im Standard-VM-Verzeichnis gespeichert.

4. Wiederholen Sie die gleichen Schritte für den Primärserver.

> **Hinweis:**
>
> Sie müssen die VM nicht ausschalten, während Sie einen Snapshot erstellen.

Stellen Sie einen Snapshot von NetScaler ADM-Servern wieder her

Wenn Sie einen Snapshot wiederherstellen, setzen Sie den Arbeitsspeicher, die Einstellungen und den Zustand der Festplatten der virtuellen Maschine in den Zustand zurück, in dem sie sich zum Zeitpunkt der Snapshot-Erstellung befanden.

Verwenden Sie die folgende Sequenz, um Snapshots der NetScaler ADM-Server wiederherzustellen:

1. NetScaler ADM-Primärserver
2. NetScaler ADM sekundärer Server

So stellen Sie den Snapshot von NetScaler ADM-Servern wieder her:

1. Wählen Sie auf Ihrem Hypervisor den NetScaler ADM-Primärserver aus der Liste der virtuellen Maschinen aus.
2. Klicken Sie mit der rechten Maustaste auf die VM und stellen Sie den Snapshot wieder her.

   Die virtuelle Maschine wird auf den neuesten Snapshot zurückgesetzt.

3. Wiederholen Sie die gleichen Schritte für den sekundären NetScaler ADM-Server.

Auditing-Informationen anzeigen

February 5, 2024

Syslog ist ein Standardprotokoll für die Protokollierung. Es besteht aus zwei Komponenten: dem Syslog-Auditing-Modul, das auf der Citrix Application Delivery Controller (ADC) -Instanz läuft, und dem Syslog-Server, der entweder auf dem zugrunde liegenden FreeBSD-Betriebssystem (OS) der

NetScaler-Instanz oder auf einem Remote-System ausgeführt werden kann. SYSLOG verwendet das User Datagram Protocol (UDP) für die Datenübertragung.

Syslog ermöglicht die Isolierung des Systems, das Informationen generiert, und des Systems, in dem die Informationen gespeichert werden. Sie können Protokollinformationen konsolidieren und Erkenntnisse aus den gesammelten Daten gewinnen. Sie können syslog auch so konfigurieren, dass verschiedene Arten von Ereignissen protokolliert werden.

Sie können die Syslog-Meldungen überwachen, die ein NetScaler-Gerät generiert, wenn Sie das Gerät so konfigurieren, dass es Syslog-Meldungen an NetScaler Application Delivery Management (ADM) umleitet. Mithilfe der integrierten Vorlagenfunktion in NetScaler ADM können Sie einen Job planen, um Syslog-Server zu erstellen, die verschiedene Arten von Syslog-Daten generieren.

Konfigurieren Sie zunächst einen Syslog-Server, an den die Instanz Protokollinformationen senden kann. Geben Sie dann das Datums- und Uhrzeitformat für die Aufzeichnung von Protokollmeldungen an.

So konfigurieren Sie einen Syslog-Server auf NetScaler ADM:

1. Navigieren Sie zu**System** > **Überwachung**. Wählen Sie unter **Konfigurationsübersicht**die Option **Syslog-Server**aus. Oder Sie können zu **System** > **Auditing** > **Syslog-Server**navigieren.
2. Klicken Sie auf der Seite **Syslog-Server** auf **Hinzufügen.**
3. Geben Sie auf der Seite **Syslog-Server erstellen** die folgenden Werte ein:
    - **Name** —Name für den Syslog-Server.
    - **IP-Adresse** —IP-Adresse des Syslog-Servers.
    - **Port** —Syslog-Serverport.
4. Wählen Sie die Protokollebenen (Alle, Keine oder Benutzerdefiniert). Wählen Sie entsprechend die Schweregrade aus.
5. Klicken Sie auf **Erstellen**.

Gehen Sie wie folgt vor, um das Syslog-Datums- und Uhrzeitformat auf NetScaler ADM zu konfigurieren:

1. Navigieren Sie zu**System** > **Überwachung**. Wählen Sie unter **Konfigurationsübersicht** die Option **Syslog-Server** aus.
2. Wählen Sie auf der Seite **Syslog-Server** einen Syslog-Server aus, und klicken Sie dann auf **Syslog-Parameter.**
3. Geben Sie auf der Seite **Syslog-Parameter konfigurieren** das Datums- und Uhrzeitformat an.
4. Klicken Sie auf **OK**.

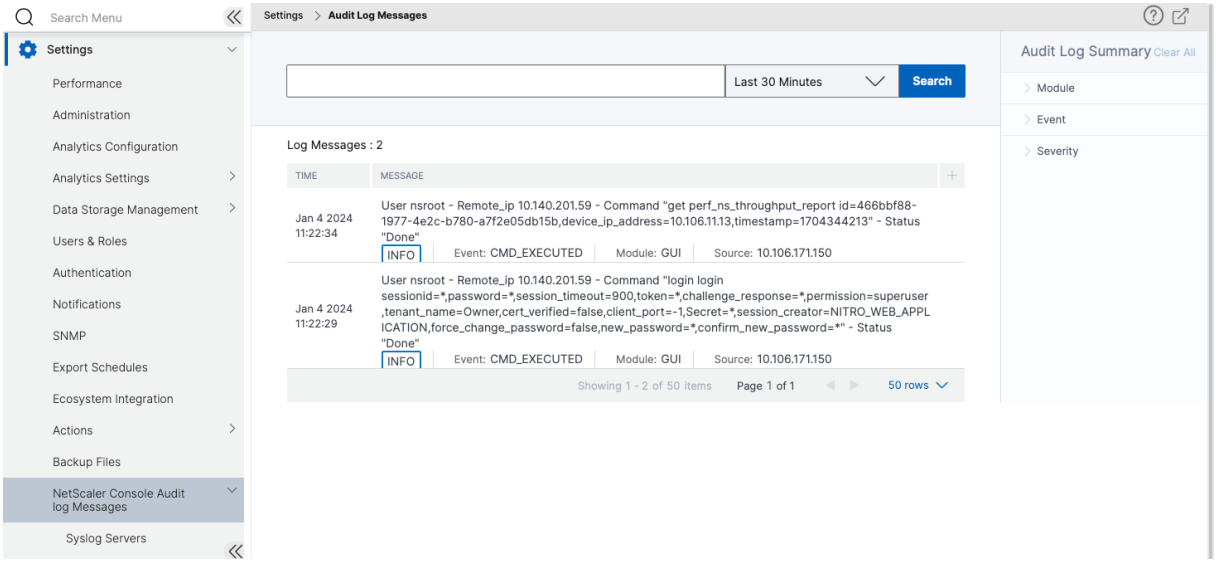
Um Syslog-Meldungen auf NetScaler ADM anzuzeigen:

Sie können jetzt alle Ihre Syslog-Meldungen anzeigen, die auf Ihren verwalteten NetScaler-Instanzen generiert wurden, wenn Sie Ihre Instanz so konfiguriert haben, dass sie die Syslog-Meldungen an

den NetScaler ADM-Server umleitet. Die Syslog-Meldungen werden zentral in der Datenbank des NetScaler ADM Servers gespeichert und zu Prüfungszwecken im Syslog-Viewer verfügbar gemacht. Sie können diese Protokollierungsinformationen konsolidieren und aus den gesammelten Daten Berichte für Analysen ableiten.

Sie können diese Informationen nach Modul, Ereignistyp und Schweregrad filtern. Sie können syslog auch so konfigurieren, dass verschiedene Arten von Ereignissen protokolliert werden.

Um den **Syslog-Viewer** aufzurufen, navigieren Sie zu **System** > **Auditing**. Wählen Sie auf der **Auditing-Seite** unter **Audit-Meldungen** die Option **Syslog-Meldungen** aus. Wählen Sie die entsprechenden Filter, um Ihre Systemprotokollmeldungen anzuzeigen.



SSL-Einstellungen konfigurieren

February 5, 2024

SSL (Secure Socket Layer) und TLS (Transport Layer Security) sind häufig verwendete Sicherheitsnetzwerkprotokolle, die eine verschlüsselte Kommunikation zwischen Benutzern und Servern ermöglichen. Sie können SSL-Einstellungen auf NetScaler Application Delivery Management (ADM) konfigurieren und den Typ der Clients angeben, die eine Verbindung zum System herstellen.

So konfigurieren Sie SSL-Einstellungen für NetScaler ADM:

1. Navigieren Sie zu **System** > **Systemadministration**. Klicken Sie unter **Systemeinstellungen**auf **SSL-Einstellungen konfigurieren**.
2. Überprüfen Sie auf der Seite **SSL-Einstellungen** die aktuellen Protokolleinstellungen und die auf das System angewandten Verschlüsselungssammlungen.

3. Um die Protokolleinstellungen zu ändern, navigieren Sie zu **Einstellungen bearbeiten** > **Protokolleinstellungen** und nehmen Sie die gewünschten Änderungen vor.
4. Um die angewendeten Cipher Suites zu ändern, navigieren Sie zu **Einstellungen bearbeiten** > **Cipher Suites und nehmen** Sie die gewünschten Änderungen vor.
5. Klicken Sie auf **OK**und dann auf **Schließen**.

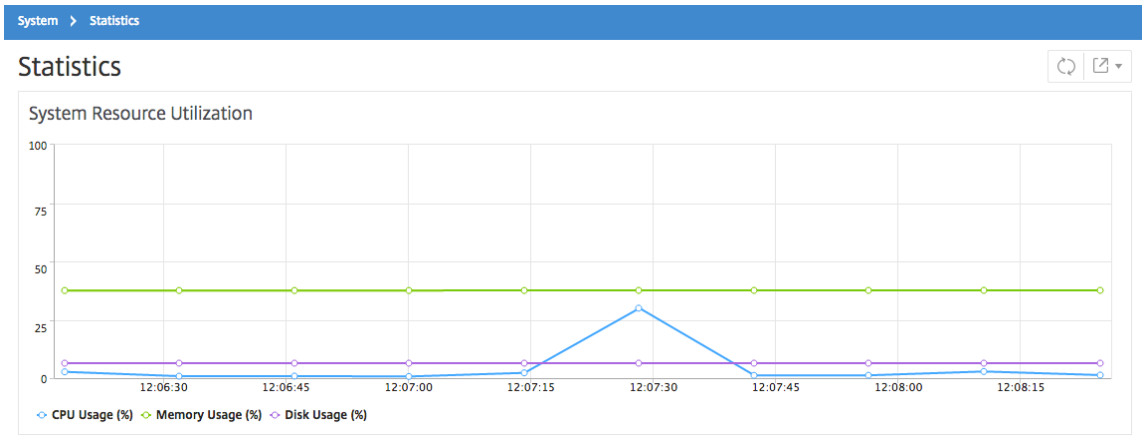
CPU-, Arbeitsspeicher- und Datenträgernutzung überwachen

February 5, 2024

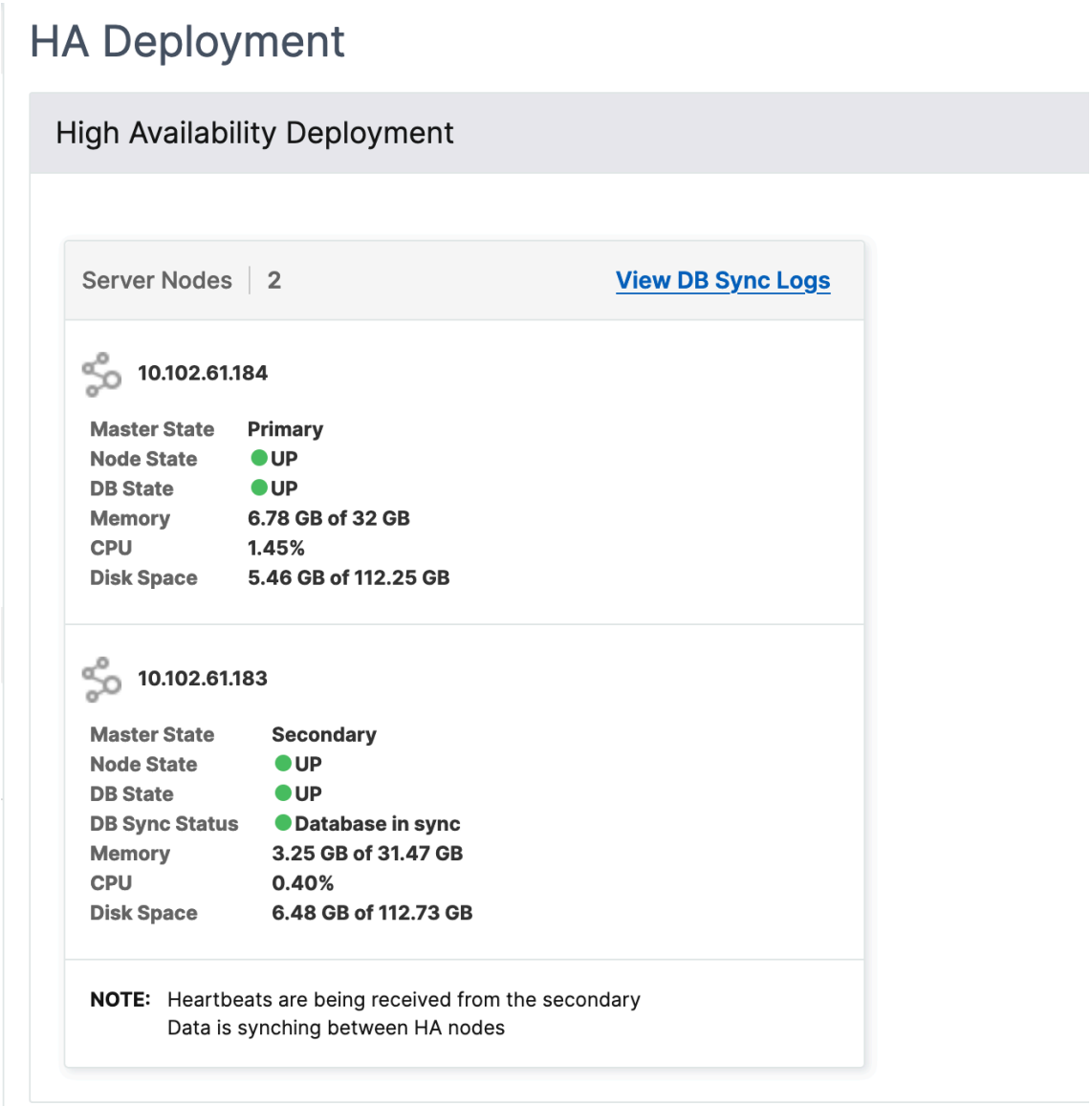
Sie können die in Protokollen und Statistiken gespeicherten Informationen verwenden. Diese Informationen werden auch in Berichten angezeigt, die Ihnen bei der Konfiguration und Wartung von NetScaler Application Delivery Management (ADM) helfen.

So überwachen Sie die CPU-, Speicher- und Datenträgernutzung:

- **Eigenständige Bereitstellung.** Navigieren Sie zu **System** > **Statistik**. Sie können in Echtzeit CPU-, Speicher- und Datenträgerauslastungsdiagramme anzeigen.



- **Bereitstellung mit hoher Verfügbarkeit.** Navigieren Sie zu **Einstellungen> Bereitstellung**. Die Statistiken für Arbeitsspeicher, CPU, Speicherplatz und verwaltete Instanzen werden numerisch angezeigt, wie in der folgenden Abbildung dargestellt:



Benachrichtigungseinstellungen konfigurieren

February 5, 2024

Sie können einen Benachrichtigungstyp auswählen, um Benachrichtigungen für die folgenden Funktionen zu erhalten:

- **Ereignisse** —Liste der Ereignisse, die für NetScaler-Instanzen generiert werden. Weitere Informationen finden Sie unter Aktionen für Ereignisregeln hinzufügen.
- **Lizenzen** —Liste der Lizenzen, die derzeit aktiv sind, bald ablaufen usw. Weitere Informationen finden Sie unter Ablauf der NetScaler ADM-Lizenz.

- **SSL-Zertifikate** —Liste der SSL-Zertifikate, die NetScaler-Instanzen hinzugefügt werden. Weitere Informationen finden Sie unter Ablauf des SSL-Zertifikats

ADM unterstützt die folgenden Benachrichtigungstypen:

- E-Mail
- SMS
- Slack
- PagerDuty
- ServiceNow

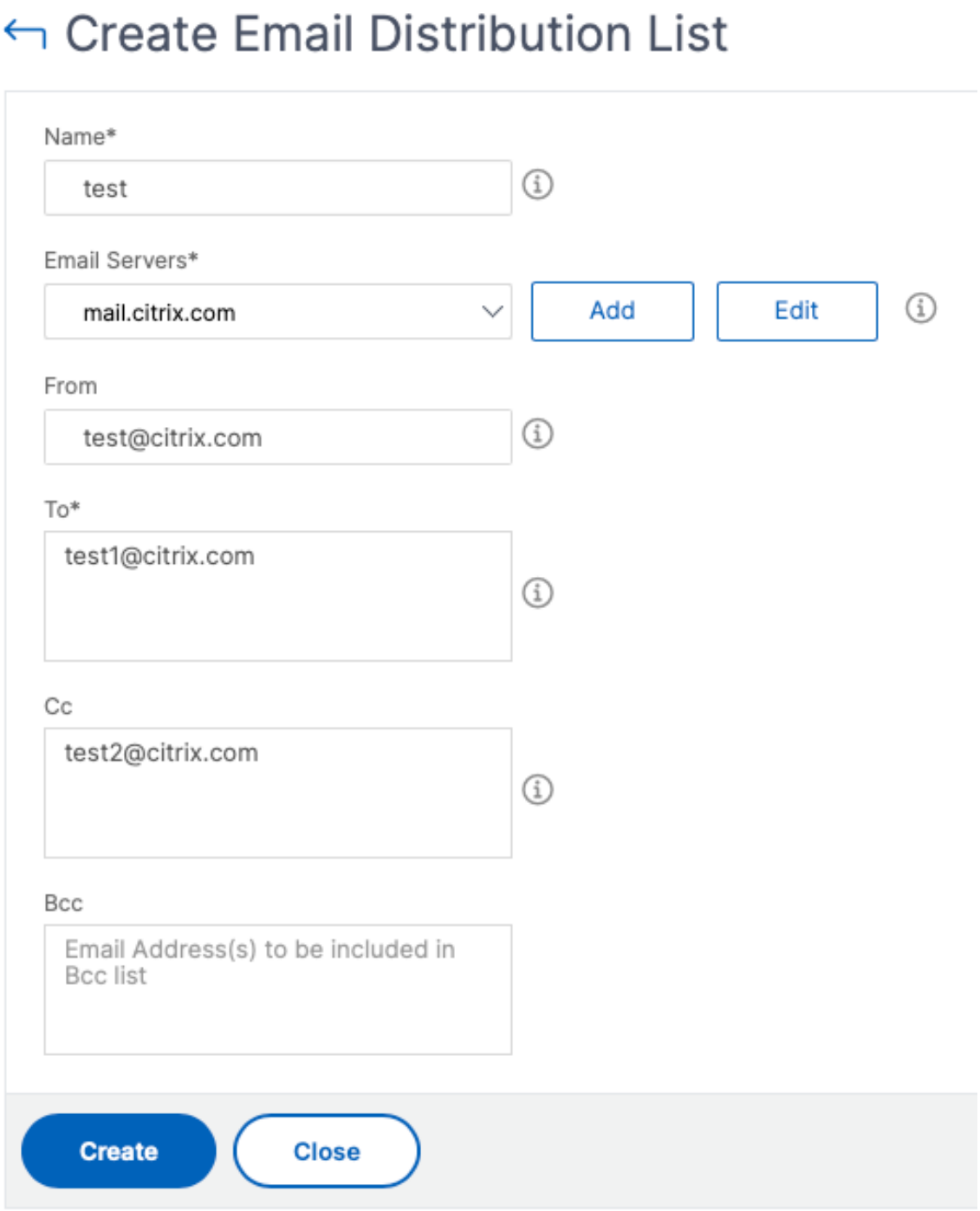
Für jeden Benachrichtigungstyp zeigt die ADM-GUI die konfigurierte Verteilerliste oder das konfigurierte Profil an. Das ADM sendet Benachrichtigungen an die ausgewählte Verteilerliste oder das ausgewählte Profil.

Erstellen einer E-Mail-Verteilerliste

Um E-Mail-Benachrichtigungen für ADM-Funktionen zu erhalten, müssen Sie einen E-Mail-Server und eine Verteilerliste hinzufügen.

Führen Sie die folgenden Schritte aus, um eine E-Mail-Verteilerliste zu erstellen:

1. Navigieren Sie zu **Einstellungen> Benachrichtigungen**.
2. Klicken Sie **unter E-Mail**auf **Hinzufügen**.
3. Geben Sie unter **E-Mail-Verteilerliste erstellen**die folgenden Details an:
    - **Name** - Geben Sie den Namen der Verteilerliste an.
    - **E-Mail-Server** —Wählen Sie den E-Mail-Server aus, der E-Mail-Benachrichtigungen sendet. Wenn Sie einen E-Mail-Server hinzufügen möchten, klicken Sie auf **Hinzufügen**.
    - **Von** —Geben Sie die E-Mail-Adresse an, von der ADM Nachrichten senden muss.
    - **An** - Geben Sie die E-Mail-Adressen an, an die ADM Nachrichten senden soll.
    - **Cc** —Geben Sie die E-Mail-Adressen an, an die ADM Nachrichtenkopien senden muss.
    - **Bcc** —Geben Sie die E-Mail-Adressen an, an die ADM Nachrichtenkopien senden muss, ohne die Adressen anzuzeigen.



4. Klicken Sie auf **Erstellen**.

Wiederholen Sie diesen Vorgang, um mehrere E-Mail-Verteilerlisten zu erstellen. Auf der Registerkarte **E-Mail** werden alle in ADM vorhandenen E-Mail-Verteilerlisten angezeigt.

Erstellen Sie eine SMS-Verteilerliste

Um SMS-Benachrichtigungen für ADM-Funktionen zu erhalten, müssen Sie einen SMS-Server und Telefonnummern hinzufügen.

Führen Sie die folgenden Schritte aus, um die SMS-Benachrichtigungseinstellungen zu konfigurieren:

1. Navigieren Sie zu **Einstellungen> Benachrichtigungen**.
2. Klicken Sie in **SMS**auf **Hinzufügen**.
3. Geben Sie unter **SMS-Verteilerliste erstellen**die folgenden Details an:
    - **Name** - Geben Sie den Namen der Verteilerliste an.
    - **SMS-Server** —Wählen Sie den SMS-Server, der SMS-Benachrichtigungen sendet.
    - **An** —Geben Sie die Telefonnummer an, an die ADM Nachrichten senden muss.
4. Klicken Sie auf **Erstellen**.

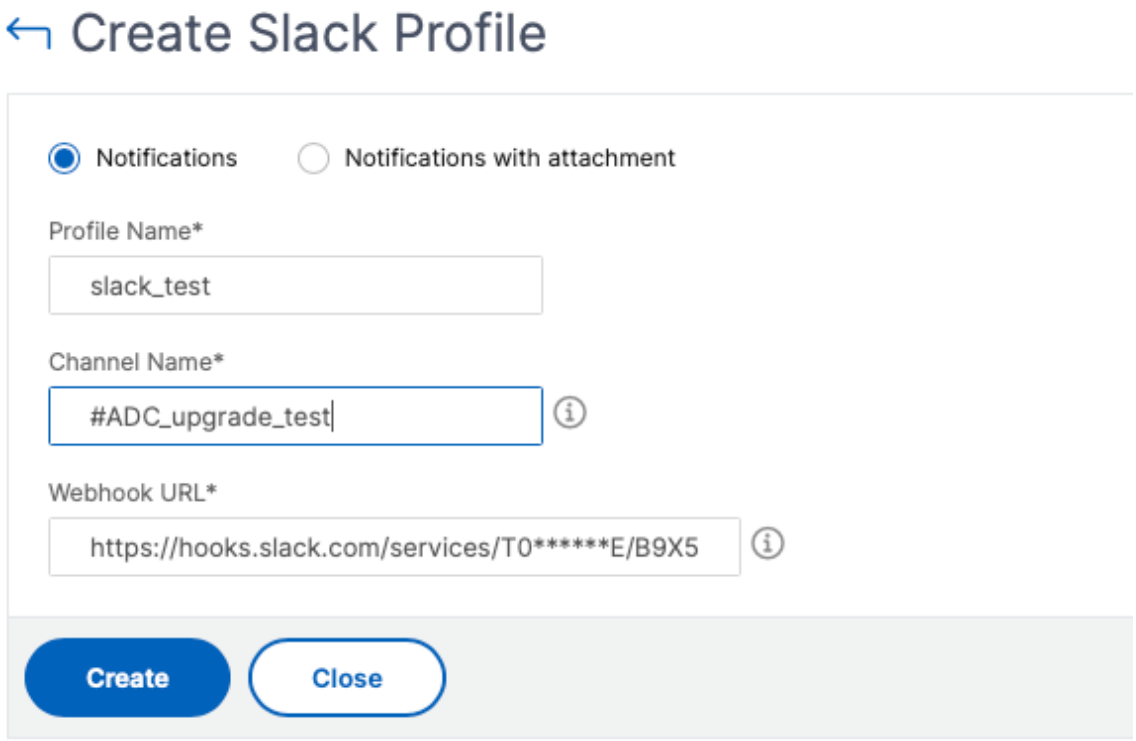
Wiederholen Sie diesen Vorgang zum Erstellen mehrerer SMS-Verteilerlisten. Auf der Registerkarte **SMS** werden alle in ADM vorhandenen SMS-Verteilerlisten angezeigt.

Erstellen eines Slack Profils

Um Slack-Benachrichtigungen für ADM-Funktionen zu erhalten, müssen Sie ein Slack-Profil erstellen.

Führen Sie die folgenden Schritte aus, um ein Slack Profil zu erstellen:

1. Navigieren Sie zu **Einstellungen> Benachrichtigungen**.
2. Klicken Sie in **Slack**auf **Hinzufügen**.
3. Geben Sie unter **“Slack-Profil erstellen**”die folgenden Details an:
    - **Profilname** —Geben Sie den Profilnamen an. Dieser Name wird in der Slack-Profilliste angezeigt.
    - **Kanalname** —Geben Sie den Namen des Slack-Channels an, an den ADM Benachrichtigungen senden muss.
    - **Webhook-URL** —Geben Sie die Webhook-URL des Kanals an. 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 werden, werden auf dem dafür vorgesehenen Slack Kanal veröffentlicht. Ein Beispiel für Webhook lautet wie folgt: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK



4. Klicken Sie auf **Erstellen**.

Wiederhole diesen Vorgang, um mehrere Slack-Profile zu erstellen Auf der Registerkarte **Slack** werden alle in ADM vorhandenen Slack-Profile angezeigt.

Erstellen eines PagerDuty-Profils

Sie können ein PagerDuty-Profil hinzufügen, um die Vorfallbenachrichtigungen basierend auf den PagerDuty-Konfigurationen zu überwachen. Mit PagerDuty können Sie Benachrichtigungen per E-Mail, SMS, Push-Benachrichtigung und Telefonanruf an einer registrierten Nummer konfigurieren.

Bevor Sie ein PagerDuty-Profil in NetScaler ADM hinzufügen, stellen Sie sicher, dass Sie die erforderlichen Konfigurationen in PagerDuty abgeschlossen haben. Um mit PagerDuty zu beginnen, lesen Sie die PagerDuty-Dokumentation.

Führen Sie die folgenden Schritte aus, um ein PagerDuty-Profil zu erstellen:

1. Navigieren Sie zu **Einstellungen> Benachrichtigungen**.
2. Klicken Sie in **PagerDuty**auf **Hinzufügen**.
3. Geben Sie unter **PagerDuty-Profil erstellen**die folgenden Details an:
    - **Profilname** —Geben Sie einen Profilnamen Ihrer Wahl an.

- **Integrationsschlüssel** —Geben Sie den Integrationsschlüssel an. Sie können diesen Schlüssel von Ihrem PagerDuty-Portal erhalten.

4. Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Services und Integrationen in der PagerDuty-Dokumentation.

Wiederholen Sie diesen Vorgang, um mehrere PagerDuty-Profile zu erstellen. Auf der Registerkarte **PagerDuty** werden alle in ADM vorhandenen PagerDuty-Profile angezeigt.

Das ServiceNow-Profil anzeigen

Wenn Sie ServiceNow-Benachrichtigungen für NetScaler-Ereignisse und ADM-Ereignisse aktivieren möchten, müssen Sie NetScaler ADM mit dem ITSM-Connector in ServiceNow integrieren. Weitere Informationen finden Sie unter Integrieren von NetScaler ADM mit der ServiceNow-Instanz.

Führen Sie die folgenden Schritte aus, um das ServiceNow-Profil anzuzeigen und zu überprüfen:

1. Navigieren Sie zu **Einstellungen> Benachrichtigungen**.
2. Wählen Sie in **ServiceNow**das Profil **Citrix_Workspace_SN** aus der Liste aus.
3. Klicken Sie auf **Test**, um automatisch ein ServiceNow-Ticket zu generieren und die Konfiguration zu überprüfen.

   Wenn Sie ServiceNow-Tickets in der NetScaler ADM GUI anzeigen möchten, wählen Sie **ServiceNow Tickets**aus.

Technische Supportdatei generieren

February 5, 2024

Citrix empfiehlt, dass Sie ein Archiv mit NetScaler Application Delivery Management (ADM) -Daten und Statistiken erstellen, bevor Sie sich an den technischen Support wenden, um ein Problem zu beheben. Das Archiv ist eine TAR-Datei, die Sie an das technische Support-Team senden können.

> **Hinweis**
>
> Für NetScaler ADM-Server in einem Hochverfügbarkeitsmodus können Sie von einem der Server eine Datei für den technischen Support generieren. Citrix empfiehlt, die IP-Adresse des virtuellen Lastausgleichsservers nicht zum Generieren der Datei für den technischen Support zu verwenden.

So konfigurieren und senden Sie eine Datei für den technischen Support von NetScaler ADM:

1. Navigieren Sie zu **System** > **Diagnose** > **Technischer Support**, und klicken Sie dann auf **Datei für technischen Support erstellen**.
2. Wählen Sie auf der Seite **Supportdatei generieren** die folgenden Optionen aus:

- **Debug-Protokolle sammeln** —Wählen Sie diese Option, um `afdecoder`-Protokolle zu sammeln.
- **Dauer** —Geben Sie die Dauer ein, für die Debug-Protokolle gesammelt werden müssen. Diese Option wird nur angezeigt, wenn Sie die Option **Debug-Protokolle sammeln** aktivieren.
- **Datenverteilung sammeln** —Wählen Sie diese Option aus, um unterschiedliche Protokolle aus der Datenbank zu sammeln.

```
The archive file is created as a TAR file.

For example, the archive file that is created might be named as
   follows:   Citrix_ADM_<ADM_IP_address>_<DDMMYY>_<time_stamp>.
   tar.gz
```

1. Sie können die technischen Support-Dateien auf zwei Arten an das Support-Team senden:

   a) Sie können die Datei von der ADM-GUI in Ihren lokalen Speicher herunterladen und dann einen Webbrowser verwenden, um sie auf Citrix Insight Services (CIS)hochzuladen.

   b) Sie können die Dateien des technischen Supports auch auf die CIS-Website hochladen, indem Sie ein Skript auf der ADM-Konsole ausführen.

      i. Melden Sie sich mithilfe von SSH an der ADM-Konsole an.

      ii. Wechseln Sie zur Shell-Eingabeaufforderung und geben Sie Folgendes

      /mps/collector_upload.pl

Der vollständige Befehl ist unten mit den Attributen angegeben, die Sie angeben müssen:

```
/mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<
   proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr
    <sr>] [-description <description>] [-debug] <file>
<!--NeedCopy-->
```

Der Vorteil der Ausführung des Perl-Skripts besteht darin, dass Sie die technische Support-Datei nicht von ADM auf Ihr lokales System herunterladen und dann in CIS hochladen müssen. Optional können Sie die Datei direkt in CIS hochladen, indem Sie einen Proxy von der ADM-Konsole verwenden.

Stellen Sie sicher, dass Sie ein Konto bei CIS haben. Sie können die Anmeldeinformationen Ihres Citrix-Kontos verwenden, um Dateien in CIS hochzuladen.

Was passiert, wenn Sie keinen Proxyserver haben? Oder was ist, wenn Sie Probleme mit SSL-Forward-Proxys haben? (Dies kann passieren, wenn das Perl-Skript dem Stammzertifikat des Proxyservers

nicht vertraut.)
Sie können die Datei weiterhin direkt von der ADM-Shell in CIS hochladen.

> **Hinweis:**
>
> Sie können die Datei weiterhin herunterladen und per E-Mail an den technischen Support von Citrix senden, wenn ADM die Datei nicht von der Konsole in CIS hochladen kann. Oder Sie können die Datei von ADM in Ihren lokalen Speicher herunterladen und dann einen Webbrowser zum Hochladen in CIS verwenden.

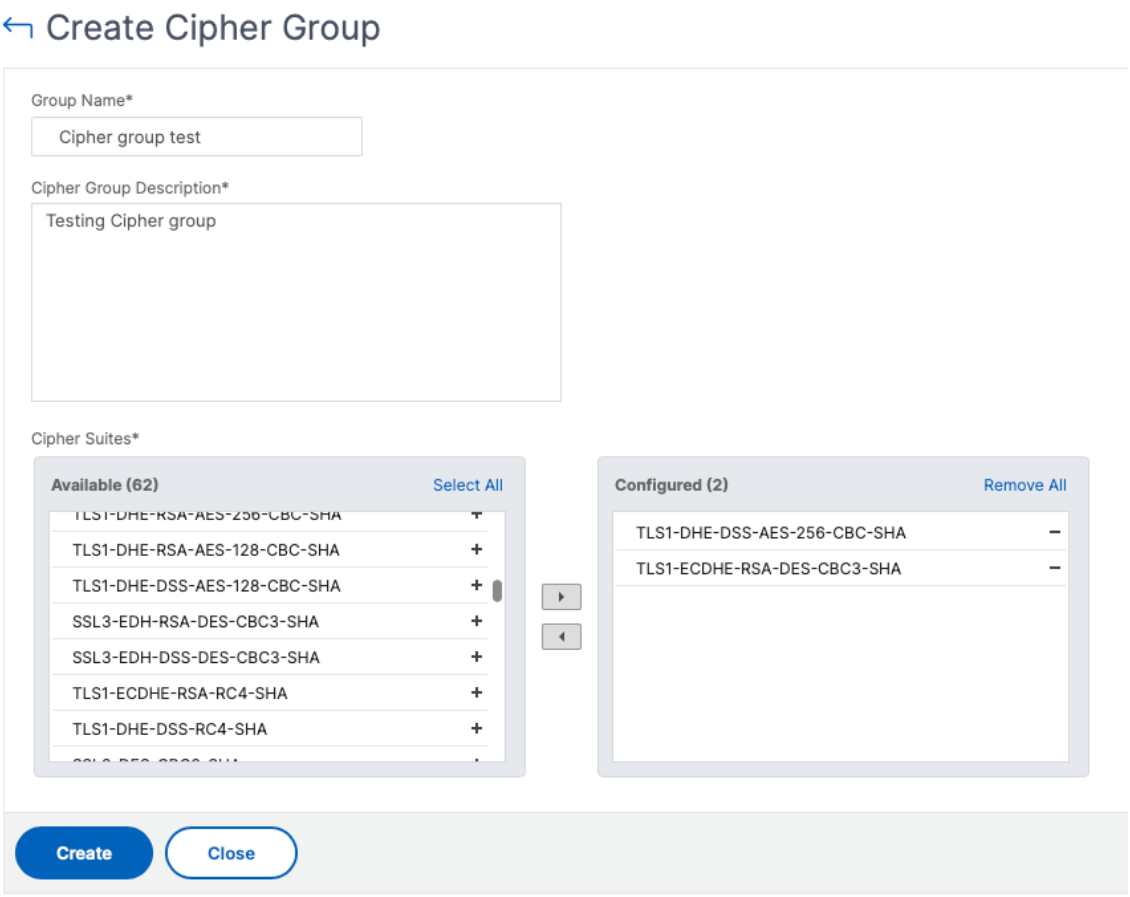
Chiffriergruppe konfigurieren

February 5, 2024

Eine Verschlüsselungsgruppe ist ein Satz von Verschlüsselungssammlungen, die Sie an einen virtuellen SSL-Server, -Dienst oder -Dienstgruppe auf der Citrix Application Delivery Controller (ADC) -Instanz binden. Eine Verschlüsselungssuite besteht aus einem Protokoll, einem Schlüsselaustauschalgorithmus (Kx), einem Authentifizierungsalgorithmus (Au), einem Verschlüsselungsalgorithmus (Enc) und einem Nachrichtenauthentifizierungscode (Mac) -Algorithmus.

So fügen Sie eine Verschlüsselungsgruppe in NetScaler ADM hinzu:

1. Navigieren Sie zu **Einstellungen> Verwaltung**
2. Klicken Sie unter **SSL-Einstellungen**auf **Verschlüsselungsgruppen**
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie auf der Seite **Verschlüsselungsgruppe erstellen** die folgenden Details ein:
    - **Gruppenname** —Name für die Verschlüsselungsgruppe.
    - **Beschreibung der Verschlüsselungsgruppe** —Geben Sie eine Beschreibung für Ihre Verschlüsselungsgruppe ein.
    - **Cipher Suites** —Klicken Sie auf Hinzufügen, um Cipher Suites aus der Liste Verfügbar auszuwählen, und verschieben Sie dann die ausgewählten (oder alle) Cipher Suites in die Liste Konfiguriert.
5. Klicken Sie auf **Erstellen**.



SNMP-Trap-Ziel, Manager-Community und Benutzer erstellen

February 5, 2024

Immer wenn ein abnormaler Zustand auf dem NetScaler ADM auftritt, wird ein SNMP-Trap generiert. Die Traps werden dann an ein Remotegerät gesendet, das Trap-Zielserver oder *SNMP-Trap-Ziel*genannt wird. Hier ist NetScaler ADM als Trap-Ziel konfiguriert. Sie können den SNMP-Agent systemspezifische Informationen von einem Remotegerät abfragen, das *SNMP-Manager*genannt wird. Der Agent durchsucht dann die MIB (Management Information Base) nach angeforderten Daten und sendet die Daten an den SNMP-Manager.

Um ein SNMP-Trap-Ziel auf NetScaler ADM zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **System** > **SNMP** > **Trap-Ziele**.
2. Klicken Sie unter **SNMP-Traps**auf **Hinzufügen**, um einen SNMP-Trap zu erstellen, und geben Sie dann die folgenden Details an:

- **Version.** Wählen Sie die zu verwendende SNMP-Version aus.
- **Zielserver.** Name oder IP-Adresse des Trap-Ziels.
- **Hafen.** Geben Sie den Port des Trap-Ziels ein. Der Port ist standardmäßig auf 162 gesetzt.
- **Gemeinschaft.** Geben Sie die Community-Zeichenfolge an, die verwendet werden soll, wenn eine Trap an den Trap-Listener gesendet wird.

3. Klicken Sie auf **Erstellen**.

> **Hinweis**
>
> Wenn Sie ein SNMP v3-Trap-Ziel erstellen, geben Sie die SNMP-Benutzeranmeldeinformationen an, an die Sie den Trap binden möchten. Um eine SNMP-Benutzeranmeldeinformationen hinzuzufügen, klicken Sie auf **Einfügen** und fügen Sie dann den Benutzer aus der Liste der verfügbaren SNMP-Benutzer hinzu.

So erstellen Sie eine SNMP-Manager-Community:

1. Navigieren Sie zu **System** > **SNMP** > **Manager**.
2. Klicken Sie unter **SNMP Manager**auf **Hinzufügen**, um eine SNMP-Manager-Community zu erstellen, und geben Sie dann die folgenden Details an:
   - **SNMP-Manager.** Geben Sie den Namen oder die IP-Adresse des SNMP-Managers ein.
   - **Gemeinschaft.** Geben Sie die Community-Zeichenfolge an, die verwendet werden soll, wenn Traps an den Trap-Listener gesendet werden.
3. Optional können Sie das Kontrollkästchen **Verwaltungsnetzwerk aktivieren** aktivieren, um die **Netzmaske** anzugeben, die die Subnetzmaske des SNMP-Manager-Netzwerks ist.
4. Klicken Sie auf **Erstellen**.

Um einen SNMP-Benutzer zu erstellen:

1. Navigieren Sie zu **System** > **SNMP** > **Benutzer**.
2. Klicken Sie unter **SNMP-Benutzer**auf **Hinzufügen**.
3. Geben Sie den Benutzernamen ein und weisen Sie dem Benutzer über das Menü eine Sicherheitsstufe zu.
4. Geben Sie basierend auf der Sicherheitsstufe, die Sie dem Benutzer zugewiesen haben, zusätzliche Authentifizierungsprotokolle an, wie Authentifizierungsprotokolle, Datenschutzkennwörter und Zuweisen von SNMP-Ansichten.

Systemalarme konfigurieren und anzeigen

February 5, 2024

Sie können eine Reihe von Alarmen aktivieren und konfigurieren, um den Zustand Ihrer NetScaler Application Delivery Management (ADM) -Server zu überwachen. Sie müssen Systemalarme konfigurieren, um sicherzustellen, dass Sie kritische oder größere Systemprobleme kennen. Sie möchten z. B. benachrichtigt werden, wenn die CPU-Auslastung hoch ist oder wenn mehrere Anmeldefehler auf dem Server auftreten. Für einige Alarmkategorien, wie CPUUsageHigh oder MemoryUsageHigh, können Sie Schwellenwerte festlegen und den Schweregrad (z. B. Critical oder Major) für jede Alarmkategorie definieren. Für einige Kategorien, wie inventoryFailed oder loginFailure, können Sie nur den Schweregrad definieren. Wenn der Schwellenwert für eine Alarmkategorie (z. B. MemoryUsageHigh) überschritten wird oder ein Ereignis eintritt, das der Alarmkategorie entspricht (z. B. **LoginFailure**), wird eine Meldung im System aufgezeichnet und Sie können die Nachricht als Syslog-Nachricht anzeigen. Sie können außerdem Benachrichtigungen einrichten, um eine E-Mail oder SMS zu erhalten, die Ihren Alarmeinstellungen entsprechen.

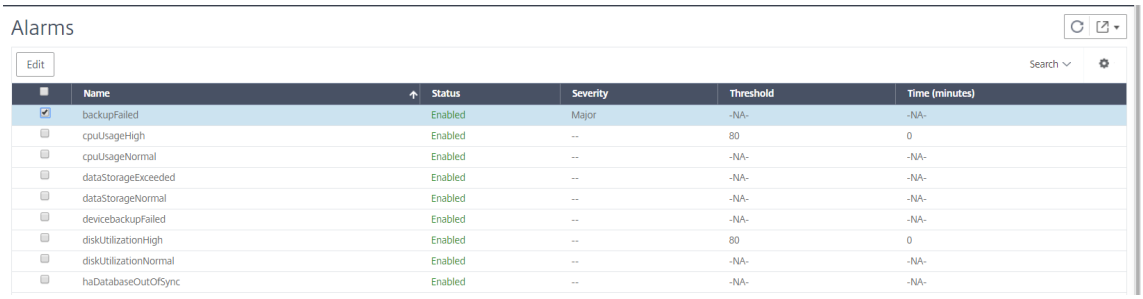
Sie können den Schweregrad eines Alarms zuweisen oder ändern. Die Schweregrade, die Sie zuweisen können, sind Kritisch, Groß, Geringfügig, Warnung und Informativ.

Betrachten Sie ein Szenario, in dem Sie überwachen möchten, wenn ein fehlgeschlagener Backupversuch vorliegt. Sie können den backupFailed Alarm aktivieren und ihm einen Schweregrad wie Major zuweisen. Wenn NetScaler ADM versucht, die Systemdateien zu sichern und der Versuch fehlschlägt, wird ein Alarm ausgelöst. Sie können die Nachricht auf dem NetScaler ADM anzeigen oder Benachrichtigungen per E-Mail oder SMS erhalten.

Um den Alarm zu konfigurieren, müssen Sie den BackupFailed-Alarm auswählen und den Schweregrad als Schweregrad angeben. Der Alarm ist standardmäßig aktiviert.

So konfigurieren und zeigen Sie einen Systemalarm mithilfe von NetScaler ADM an:

1. Navigieren Sie zu **Einstellungen > SNMP**. Klicken Sie in der oberen rechten Ecke auf **Alarme**.



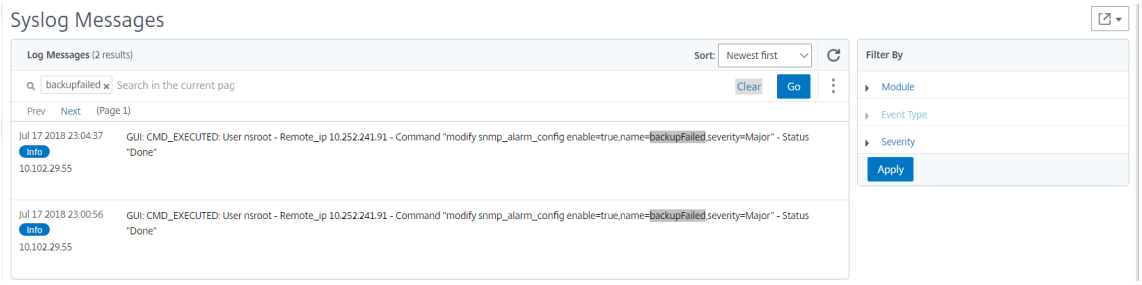
2. Wählen Sie den Alarm aus, den Sie konfigurieren möchten (z. B. BackupFailed), und klicken Sie auf **Bearbeiten**, um die Einstellungen zu ändern.

3. Der Alarm ist standardmäßig aktiviert. Weisen Sie einen Schweregrad zu (Beispiel: Major), und klicken Sie dann auf **OK**.

> **Hinweis**
>
> Für einige Alarme können Sie keinen Schwellenwert festlegen.
> Wenn der Alarm ausgelöst wird, können Sie das generierte Ereignis als Syslog-Meldung anzeigen.

Gehen Sie wie folgt vor, um das durch den BackupFailed-Alarm generierte Ereignis mithilfe von NetScaler ADM anzuzeigen:

1. Navigieren Sie zu**System** > **Überwachung**.
2. Wählen Sie auf der**Auditing-Seite**unter**Audit-Meldungen**die Option**Syslog-Meldungen**aus.
3. Geben Sie in das Suchfeld den Namen des Alarms ein.
   In diesem Beispiel können Sie sehen, dass ein Ereignis für einen fehlgeschlagenen Backupversuch generiert wurde.



   Sie können auch Benachrichtigungen festlegen, um Ihnen entweder eine E-Mail oder einen SMS (Short Message Service) zu senden, wenn ein Alarm ausgelöst wird. Informationen zum Konfigurieren von Systembenachrichtigungen finden Sie unter Konfigurieren der Systembenachrichtigungseinstellungen von NetScaler ADM.

SNMP-Manager und Benutzer für den NetScaler ADM Agent erstellen

February 5, 2024

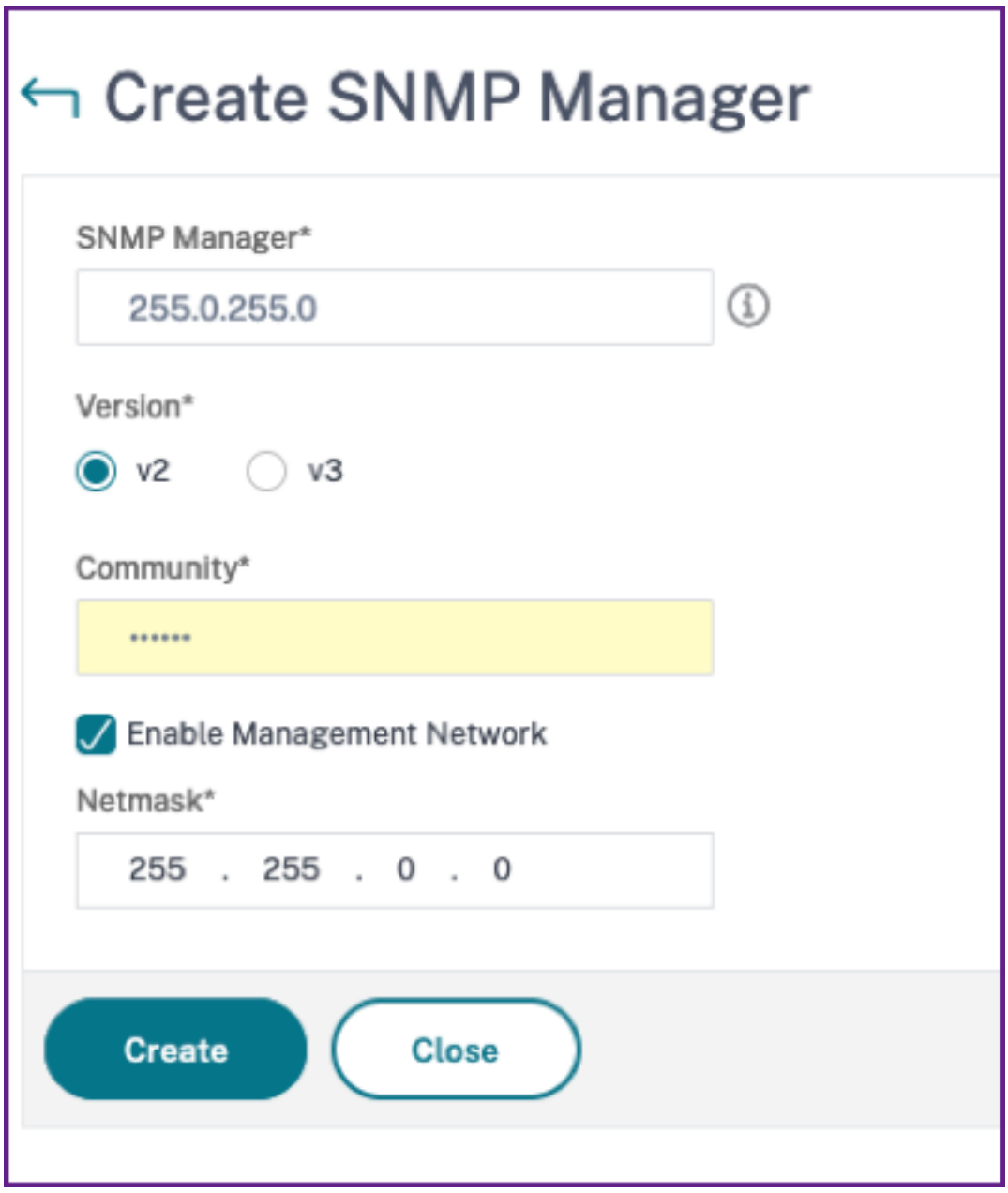
Sie können den SNMP-Agenten über ein Remote-Gerät, das als SNMP-Manager bezeichnet wird, nach systemspezifischen Informationen fragen. Der Agent durchsucht dann die MIB (Management Information Base) nach angeforderten Daten und sendet die Daten an den SNMP-Manager.

Sie können einen SNMP-Manager hinzufügen, um einen NetScaler ADM-Agenten abzufragen. Der Manager entspricht SNMP V2 und V3. Wenn Sie einen oder mehrere SNMP-Manager angeben, akzeptiert der NetScaler ADM Agent keine SNMP-Abfragen von Hosts außer den angegebenen SNMP-Managern.

Fügen Sie einen SNMP v2-Manager hinzu

So fügen Sie einen SNMP v2-Manager für den NetScaler ADM Agent hinzu:

1. Navigieren Sie zu **Infrastruktur > Agents**, wählen Sie einen NetScaler ADM Agent aus und klicken Sie auf **Aktion auswählen**> SNMP verwalten.
2. Klicken Sie auf der Registerkarte **SNMP > SNMP Manager** auf **Hinzufügen**.
3. Geben Sie auf der Seite **SNMP-Manager erstellen** die folgenden Details an:
    - **SNMP-Manager**. Geben Sie den Namen oder die IP-Adresse des SNMP-Managers ein.
    - **Ausführung**. Wählen Sie v2 aus.
    - **Community**. Geben Sie einen Community-Namen ein. Eine SNMP-Community-Konfiguration authentifiziert SNMP-Abfragen von SNMP-Managern.
    - **Verwaltungsnetzwerk aktivieren**: Aktivieren Sie dieses Kontrollkästchen, um die Netzmaske des SNMP-Manager-Netzwerks anzugeben.
    - **Netzmaske**: Geben Sie die Subnetzmaske ein, die einer IP-Adresse zugeordnet ist.
4. Klicken Sie auf **Erstellen**.



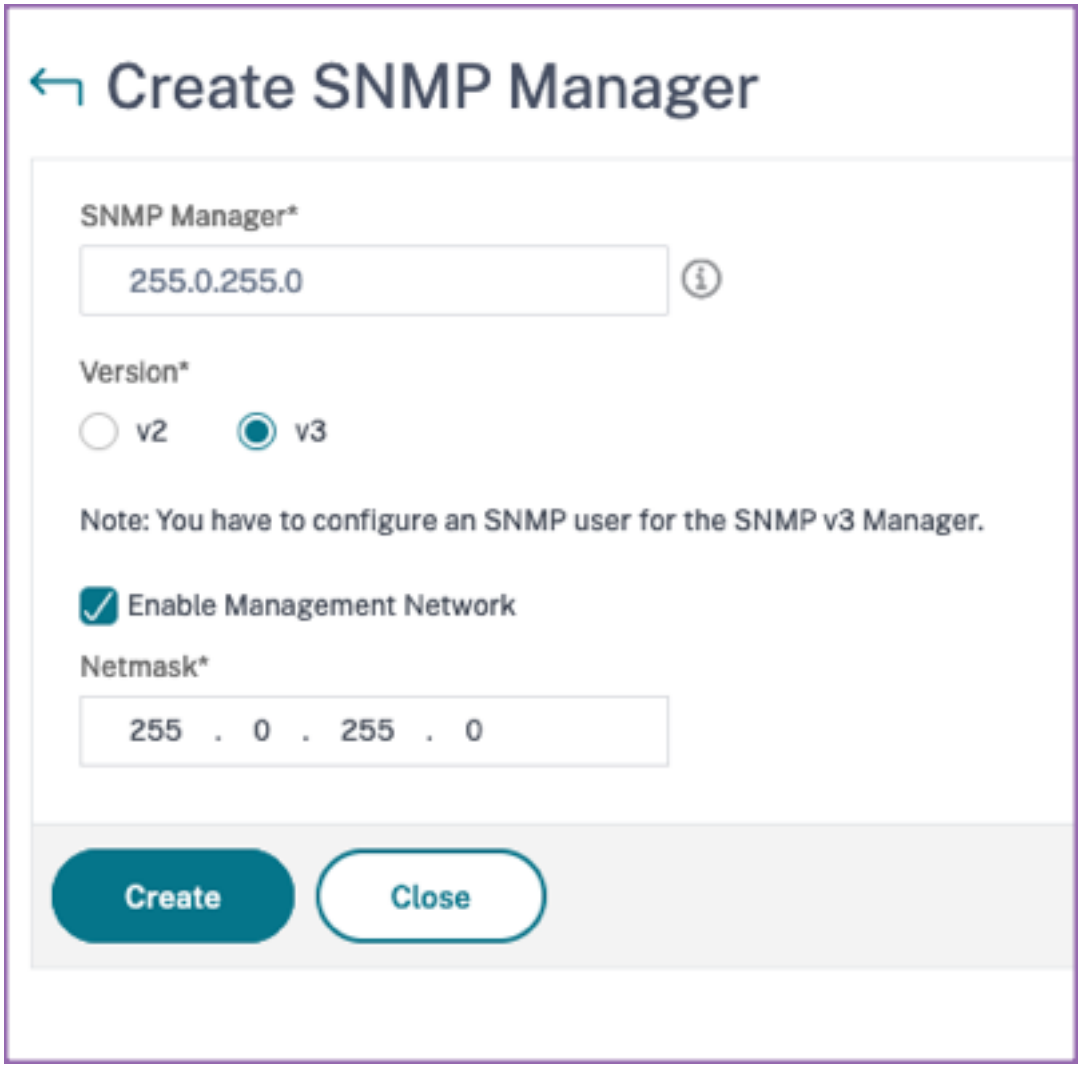
Fügen Sie einen SNMP v3-Manager hinzu

So fügen Sie einen SNMP v3-Manager für den NetScaler ADM Agent hinzu:

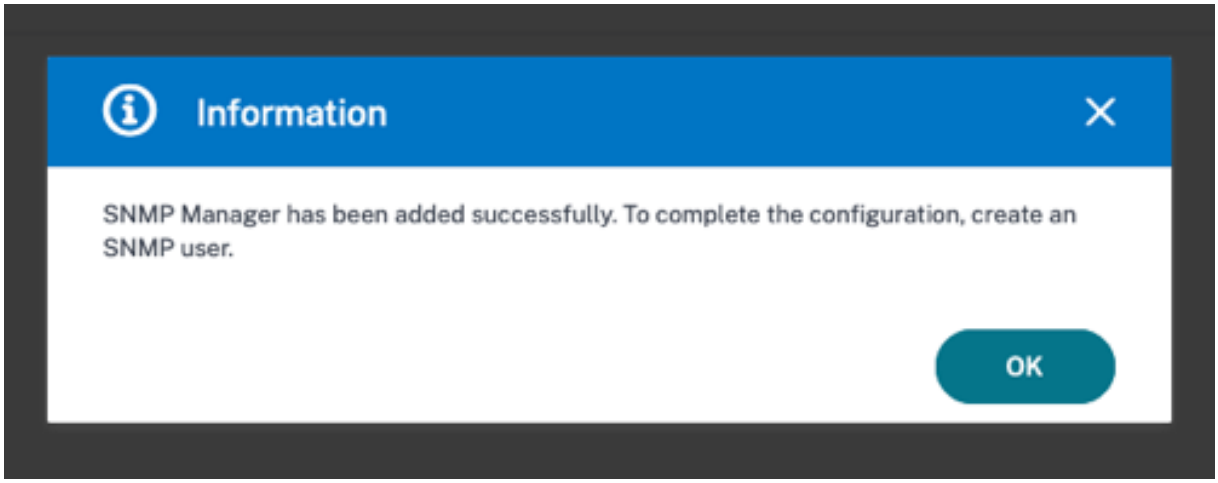
1. Navigieren Sie zu **Infrastruktur > Agents**, wählen Sie einen NetScaler ADM Agent aus und klicken Sie auf **Aktion auswählen**> SNMP verwalten.
2. Klicken Sie auf der Registerkarte **SNMP > SNMP Manager** auf **Hinzufügen**.
3. Geben Sie auf der Seite **SNMP-Manager erstellen** die folgenden Details an:

- **SNMP-Manager**. Geben Sie den Namen oder die IP-Adresse des SNMP-Managers ein.
- **Ausführung**. Wählen Sie v3 aus.
- **Verwaltungsnetzwerk aktivieren**: Aktivieren Sie dieses Kontrollkästchen, um die Netzmaske des SNMP-Manager-Netzwerks anzugeben.
- **Netzmaske**: Geben Sie die Subnetzmaske ein, die einer IP-Adresse zugeordnet ist.

4. Klicken Sie auf **Erstellen**.



In einem Dialogfeld wird bestätigt, dass ein SNMP-Manager erstellt wurde, und in dem Sie aufgefordert werden, einen SNMP-Benutzer zu konfigurieren.



> **Hinweis**
>
> Sie müssen einen SNMP-Benutzer für einen SNMP v3-Manager konfigurieren. Um den SNMP-Benutzer zu konfigurieren, gehen Sie zu **SNMP > SNMP-Benutzer**.

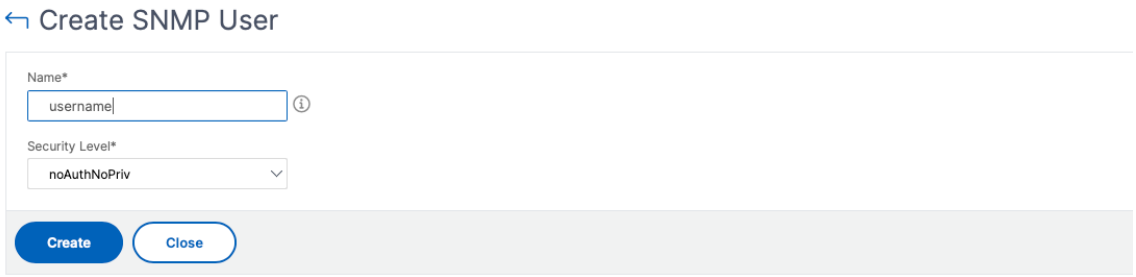
Einen SNMP-Benutzer hinzufügen

Fügen Sie einen SNMP-Benutzer hinzu, um auf die SNMP v3-Abfragen eines SNMP-Managers zu antworten.

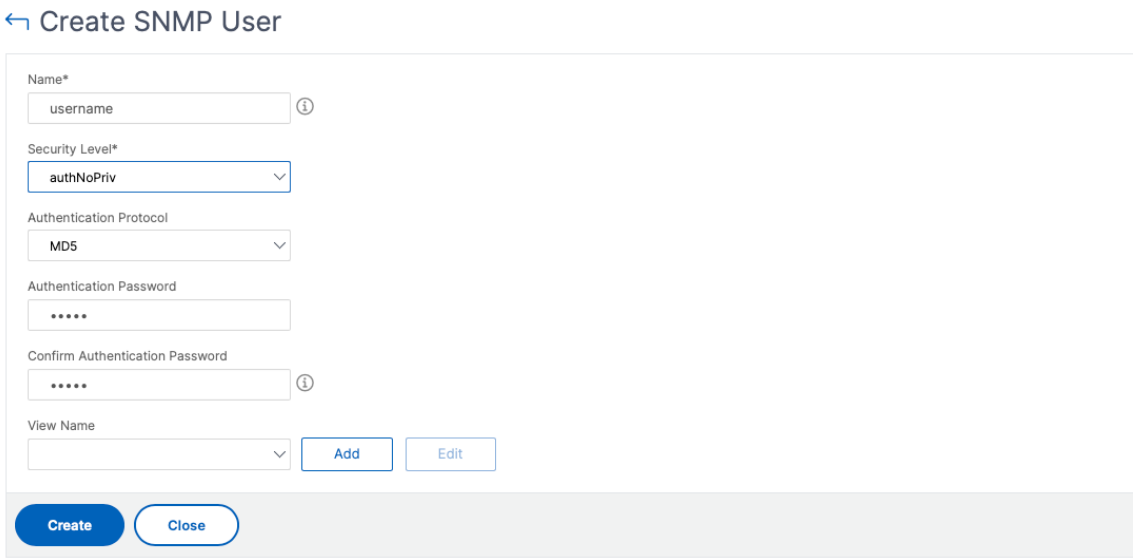
Um einen SNMP-Benutzer für den NetScaler ADM Agent hinzuzufügen:

1. Navigieren Sie zu **Infrastruktur > Agents**, wählen Sie einen NetScaler ADM Agent aus und klicken Sie auf **Aktion auswählen**> SNMP verwalten.
2. Klicken Sie auf der Registerkarte **SNMP > SNMP-Benutzer** auf **Hinzufügen**.
3. Fügen Sie auf der Seite **SNMP-Benutzer erstellen** die folgenden Details hinzu:
    - **Name**. Geben Sie den Benutzernamen ein.
    - **Sicherheitsstufe**. Sicherheitsstufe, die für die Kommunikation zwischen dem NetScaler ADM Agent und dem SNMP-Manager erforderlich ist.

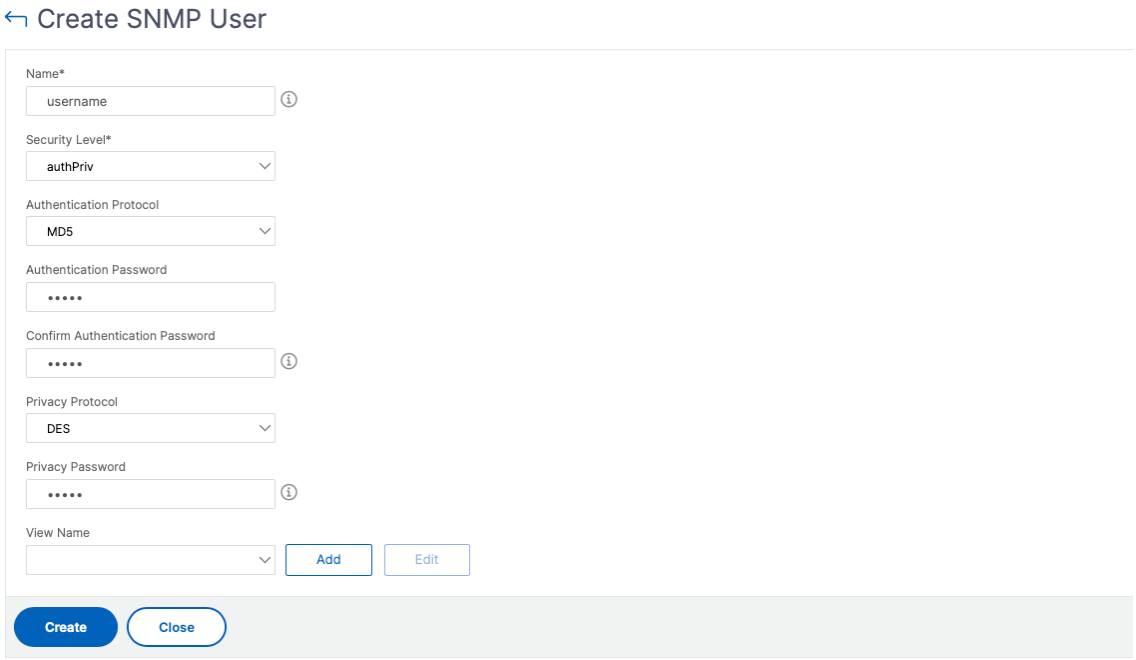
      Wählen Sie eine der folgenden Sicherheitsstufen aus:
    - **noAuthNoPriv**. Erfordert weder Authentifizierung noch Verschlüsselung.



- **authNoPriv**. Authentifizierung erforderlich, aber keine Verschlüsselung.



- **authPriv**. Authentifizierung und Verschlüsselung erforderlich.



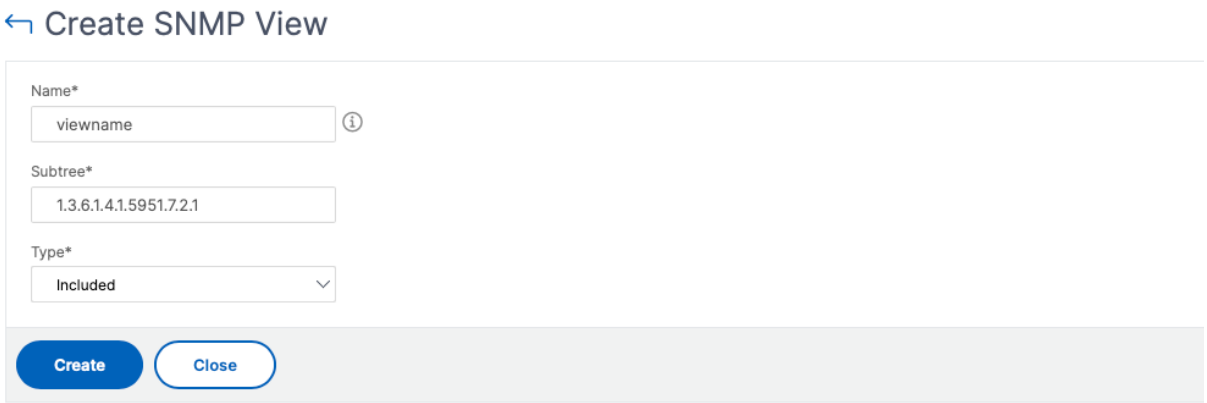
Geben Sie basierend auf der Sicherheitsstufe, die Sie dem Benutzer zugewiesen haben, zusätzliche Authentifizierungsprotokolle an, wie Authentifizierungsprotokolle, Datenschutzkennwörter und Zuweisen von SNMP-Ansichten.

Verwaltung von SNMP-Ansichten

SNMP-Ansichten werden verwendet, um die Zugriffskontrolle für einen SNMP-Benutzer zu implementieren. Die SNMP-Ansichten beschränken den Benutzerzugriff auf bestimmte Teile der MIB.

Gehen Sie wie folgt vor, um eine SNMP-OID für den NetScaler ADM Agent zuzulassen oder einzuschränken:

1. Navigieren Sie zu **Infrastruktur > Agents > SNMP** verwalten und klicken Sie auf der Registerkarte **SNMP-Ansicht** auf **Hinzufügen**.
2. Geben Sie in **SNMP Ansicht erstellen** die folgenden Details ein:
    - **Name der Ansicht**: Ein Name für die SNMP-Ansicht. Eine Instanz kann viele SNMP-Ansichten mit demselben Namen haben, die sich durch die Einstellungen der Teilbaum-Parameter unterscheiden.
    - **Unterbaum**: Ein bestimmter Zweig (Unterbaum) des MIB-Baums, den Sie dieser SNMP-Ansicht zuordnen möchten. Sie müssen den Teilbaum als SNMP-OID angeben.
    - **Typ**: In diesem Feld können Sie Teilbäume in eine Ansicht ein- oder ausschließen.
3. Klicken Sie auf **Erstellen**.



Agenteneinstellungen konfigurieren

February 5, 2024

Sie können das Keep-Alive-Intervall und die Kennwortänderungsanforderungen des NetScaler ADM Agents ändern.

Keep-Alive-Intervall des Agenten festlegen

NetScaler 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 NetScaler ADM Server zu senden.

1. Navigieren Sie zu **Einstellungen > Administration**.
2. Wählen Sie unter **Systemkonfigurationen** die Optionen **System, Zeitzone, Zulässige URLs und Agenteinstellungen** aus.
3. Geben Sie unter **Grundeinstellungen > Agenteneinstellungen**das Keep-Alive-Intervall zwischen 30 und 120 Sekunden an.
4. Klicken Sie auf **Speichern**.

Ändern Sie das Kennwort des Agent ohne das aktuelle Kennwort

Sie können zulassen, dass Agentenkennwörter ohne ihr aktuelles Kennwort geändert werden.

1. Navigieren Sie zu **Einstellungen > Administration**.
2. Wählen Sie unter **Systemkonfigurationen** die Optionen **System, Zeitzone, Zulässige URLs und Agenteinstellungen** aus.
3. Unter **Basic Settings > Agent Settings > Remove current password prerequisite for agent password change** können Sie Folgendes tun:
    - Markieren Sie das Kontrollkästchen, um das Feld **Aktuelles Kennwort** auf der Seite **Agentkennwort ändern** zu entfernen.
    - Deaktivieren Sie das Kontrollkästchen, um das Feld **Aktuelles Kennwort** auf der Seite **Agentkennwort ändern** beizubehalten.
4. Klicken Sie auf **Speichern**.

> **Hinweis**
>
> Um die Seite **Agentkennwort ändern** aufzurufen, navigieren Sie zu **Infrastruktur > Instances > Agents**, wählen Sie einen Agenten aus und klicken Sie auf **Aktion auswählen > Kennwort ändern**.

Data Storage Management-Dashboard verwenden

February 5, 2024

Es ist wichtig zu wissen, welche Funktionen in NetScaler ADM verwendet werden und wie die Daten jeder dieser Funktionen verwendet werden. Das **Data Storage Management-Dashboard** dient diesem Zweck und dient als Visualisierungstool, mit dem Sie die Gesamtmenge der in der NetScaler ADM-Datenbank gespeicherten Daten über verschiedene Funktionen hinweg verstehen können. Das Dashboard zeigt auch an, ob der verbrauchte Speicherplatz innerhalb der angegebenen Grenzwerte liegt oder ob er den berechtigten Speicherplatz übersteigt.

Als Administrator können Sie im **Data Storage Management-Dashboard** die folgenden Aufgaben ausführen:

- Den Datenspeicherverbrauch der letzten 30 Tage anzeigen —Datenspeichertrends werden in der NetScaler ADM-Datenbank für die letzten 30 Tage gespeichert. Diese Trends sind in grafischer oder tabellarischer Form verfügbar. Diese Trends zeigen, wie viele Daten eingegangen sind und wie viele Daten nach den geplanten Bereinigungszyklen in NetScaler ADM gespeichert werden.
- Datenaufnahmestatus anzeigen —Die Datenaufnahmeaktivität findet statt, solange der verbrauchte Speicherplatz innerhalb der Grenzen des berechtigten Speichers liegt. Wenn der verbrauchte Speicherplatz mehr als der berechtigte Speicherplatz ist, wird die Datenaktivität angehalten.
- Benachrichtigungen senden —Sie können festlegen, dass Benachrichtigungen gesendet werden, wenn der verbrauchte Speicherplatz 75% oder 100% des berechtigten Speichers erreicht, sodass Benutzer ihren Speicherplatz verwalten können.
- Flexibilität bei der Verwaltung des Datenspeicherplatzes —Sie können mehr Speicherplatz innerhalb der gespeicherten Daten schaffen, indem Sie Daten löschen, die Sie für geeignet halten, um sie zu entfernen oder zu reduzieren.

Navigieren Sie zu **Einstellungen > Datenspeicherverwaltung**, um Ihr Datenspeicher-Dashboard aufzurufen.

In den folgenden Abschnitten wird beschrieben, wie Sie das **Data Storage Management-Dashboard** für eine effektive Datenspeicherverwaltung verwenden können:

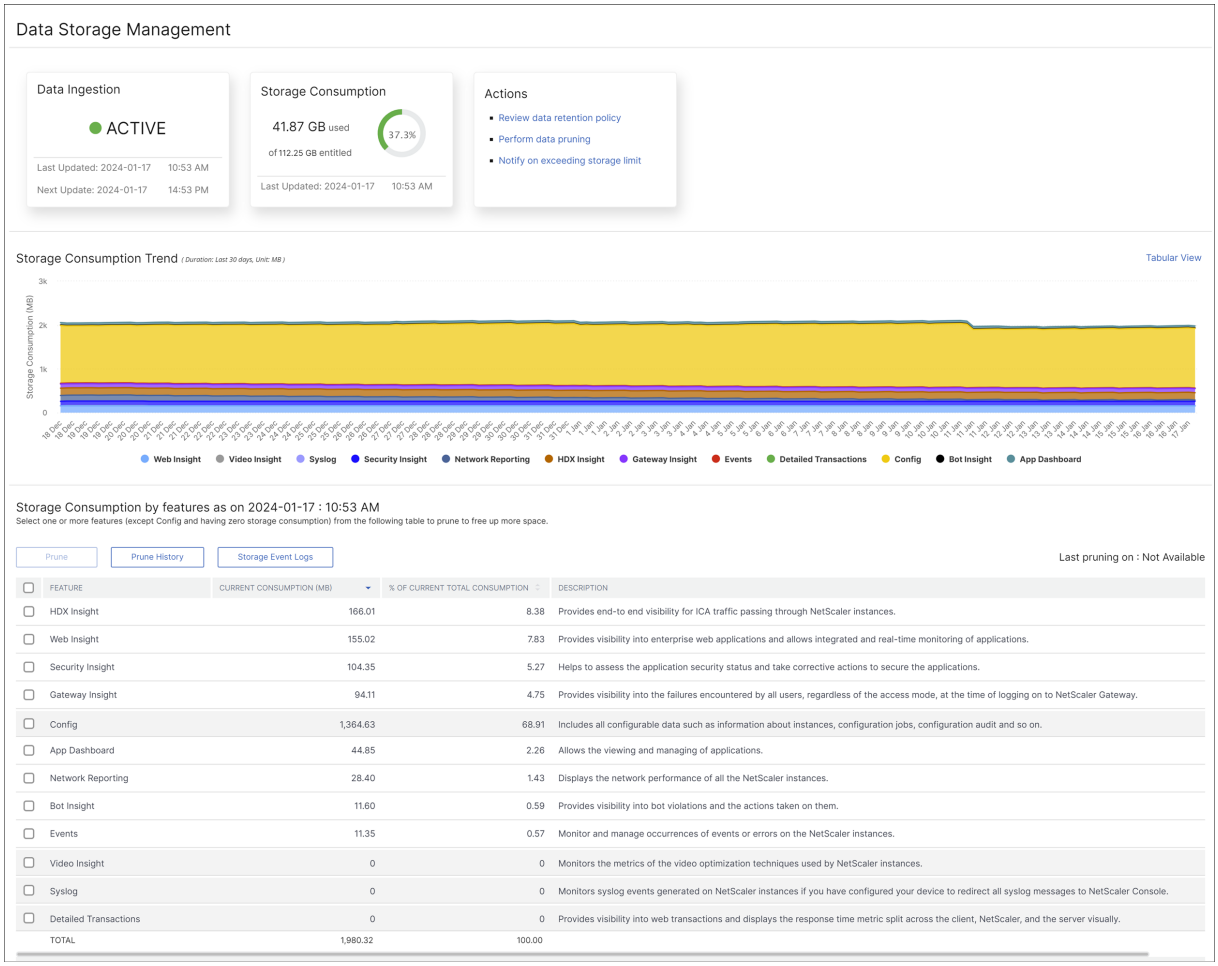
- Verstehen Sie Ihren Datenspeicher —In diesem Abschnitt erfahren Sie, wie Sie das Dashboard verwenden können, um Informationen zu Ihrem Datenspeicher anzuzeigen.
- Datenspeicher verwalten —Dieser Abschnitt enthält Informationen darüber, welche Aktionen Sie im Dashboard ergreifen können, um Ihren Datenspeicher zu verwalten.

Datenspeicher verstehen

February 5, 2024

Sie können das **Data Storage Management-Dashboard** in NetScaler ADM verwenden, um Daten und Diagramme anzuzeigen, mit denen Sie Ihre Datenspeichernutzung verfolgen können.

Um Ihren Datenspeicherverbrauch zu überwachen, navigieren Sie zu **Einstellungen > Datenspeicherverwaltung**.



Das Data Storage Management-Dashboard enthält die folgenden Informationen:

- Status Ihrer Datenaufnahmeaktivität
- Gesamter Speicherverbrauch
- Trends beim Speicherverbrauch
- Speicherverbrauch nach Funktionen

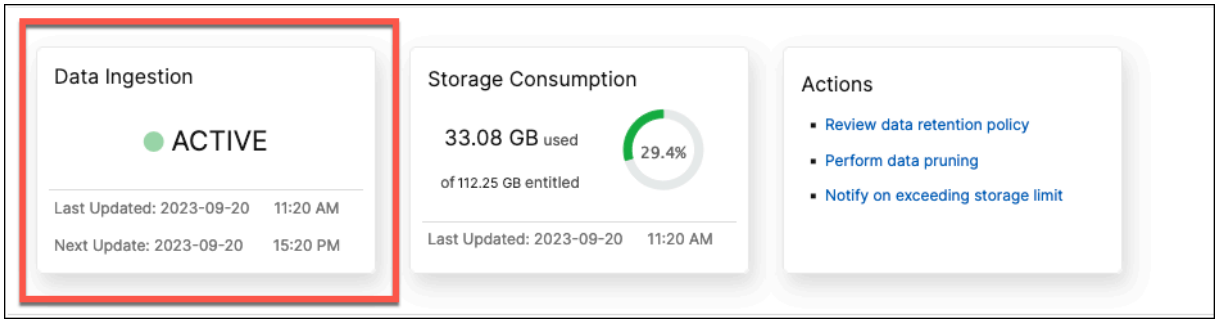
Status Ihrer Datenaufnahmeaktivität

Datenaufnahme bezieht sich auf den Prozess des Imports großer und verschiedener Daten aus allen verwalteten NetScaler-Instanzen über verschiedene Funktionen wie Ereignisse, Syslogs, Network Reporting usw. in den NetScaler ADM-Speicher.

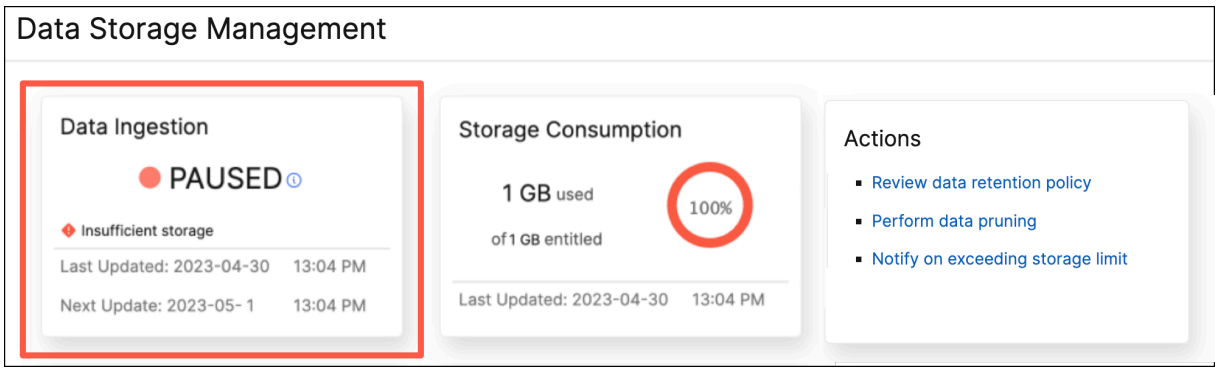
Der Datenaufnahmestatus gibt an, ob NetScaler ADM Statistiken von NetScaler-Instanzen sammelt. Die Datenaufnahmeaktivität wird fortgesetzt, solange sich der verbrauchte Speicherplatz innerhalb des berechtigten Speichers befindet. Wenn der Verbrauch den berechtigten Speicherplatz übertrifft, wird die Datenaufnahme angehalten.

Sehen Sie sich die Kachel **Datenaufnahme** an, um den aktuellen Status der Datenaufnahme zu verstehen. Diese Kachel zeigt einen der folgenden zwei Zustände an:

- **Aktiv** —Die Datenaufnahmeaktivität ist im Gange.



- **Angehalten** —Die Datenaufnahmeaktivität wurde angehalten, da der verbrauchte Speicherplatz den berechtigten Speicherplatz übersteigt.

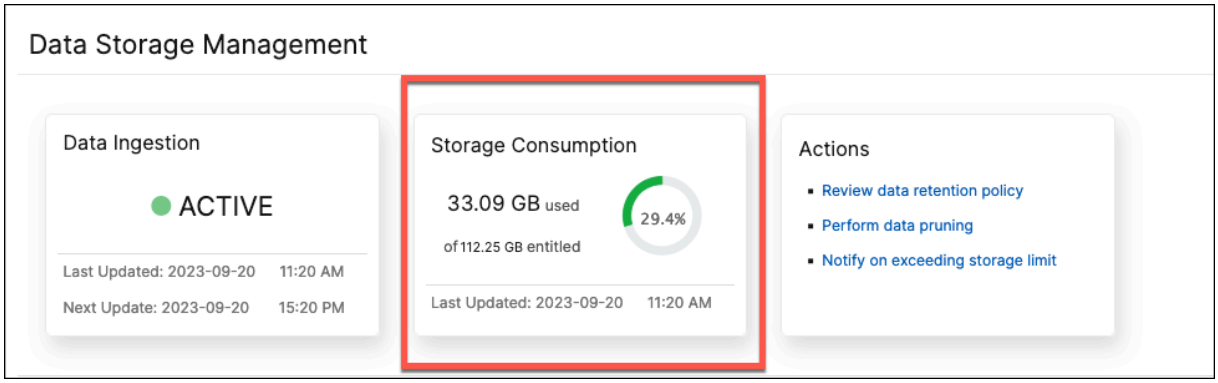


So setzen Sie Ihre unterbrochene Datenaufnahme fort

Um Ihre Datenaufnahmeaktivität wieder aufzunehmen, können Sie Daten bereinigen. Weitere Informationen finden Sie unter Durchführen von Datenbereinigungen.

Gesamter Speicherverbrauch

Einen schnellen Überblick über Ihren Datenspeicher finden Sie in der Kachel **Speicherverbrauch** .



In der Kachel **Speicherverbrauch** wird der gesamte Speicherplatz angezeigt, der von allen Funktionen in der Bereitstellung verwendet wird.

Bewegen Sie den Mauszeiger über das Ringdiagramm, um Folgendes anzuzeigen:

Berechtigter Speicher

Der berechtigte Speicherplatz ist der gesamte Speicherplatz, der Ihnen gemäß Ihrer Lizenz zur Verfügung steht. Wenn Sie über eine Express-Lizenz verfügen, erhalten Sie 500 MB berechtigten Speicherplatz. Wenn Sie über eine Advanced-Lizenz verfügen, erhalten Sie die Summe von 500 MB Speicherplatz pro gekauftem VIP und allen zusätzlichen Speicherplatz, der direkt gekauft wurde, ohne VIPs zu kaufen.

Betrachten Sie die folgenden Szenarien:

- Du hast 20 VIPs gekauft. Sie erhalten 500 MB kostenlosen Speicherplatz für jeden VIP. Ihr berechtigter Speicherplatz beträgt 20*500 = 10 GB.
- Sie haben 20 VIPs und einen zusätzlichen Speicher von 5 GB gekauft. Sie erhalten 500 MB kostenlosen Speicherplatz für jeden VIP. Ihr berechtigter Speicherplatz beträgt 20*500 + 5 = 15 GB.

Verbrauchter Speicherplatz

Der verbrauchte Speicherplatz ist der gesamte Speicherplatz, der von allen Funktionen in der Bereitstellung verwendet wird. Die folgenden Farbcodierungskriterien geben die Menge an Speicherplatz an, die von den Funktionen verwendet wird:

- **Grün** —Der verbrauchte Speicherplatz macht weniger als 75% des berechtigten Speichers aus.
- **Gelb** —Der verbrauchte Speicherplatz macht zwischen 75 und 99% des berechtigten Speichers aus.

- **Rot** —Das verbrauchte Speicherlimit hat den aktuell berechtigten Speicherplatz erreicht oder liegt darüber.

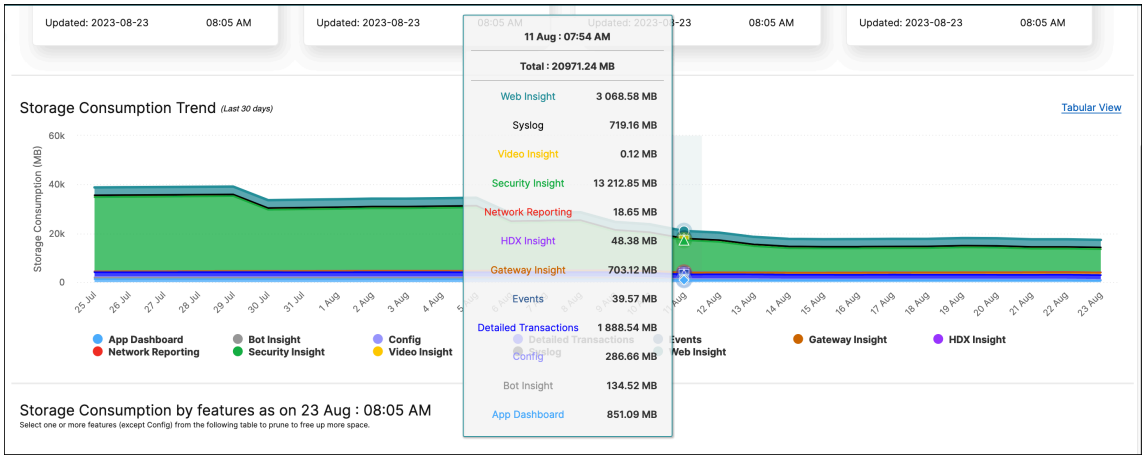
Trends beim Speicherverbrauch

Informationen darüber, wie Daten in den letzten 30 Tagen verbraucht wurden, finden Sie im Abschnitt **Trend zum Speicherverbrauch** .

Der Speicherverbrauchstrend gibt Aufschluss darüber, welche Funktionen über einen bestimmten Zeitraum am meisten oder am wenigsten Speicherplatz beanspruchen, und hilft Ihnen, Ihren Datenspeicherverbrauch effektiv zu verwalten.

Sie können die Speicherdatentrends in einer der folgenden Formen anzeigen:

- **Graphische Ansicht** —Zeigt an, wie der Datenspeicher auf die verschiedenen NetScaler ADM-Funktionen verteilt ist. Zeigen Sie mit der Maus auf die Zeitleiste, um die Datenspeicherinformationen für jeden Tag des Monats anzuzeigen.



> **Hinweis:**
>
> Die **grafische Ansicht** ist die Standardansicht.

- **Tabellarische Ansicht** —Klicken Sie auf **Tabellarische Ansicht**, um die Datenspeicherinformationen in tabellarischer Form anzuzeigen.

> **Hinweis:**
>
> In der tabellarischen Ansicht können Sie die Daten mithilfe des Suchfeldes filtern.

In der folgenden Tabelle werden die Felder beschrieben, die im Abschnitt **Speicherverbrauchstrend** angezeigt werden:

FEATURE	BESCHREIBUNG
Config	Beinhaltet alle konfigurierbaren Daten wie Informationen über Instanzen, Konfigurationsaufträge, Konfigurationsaudits usw.
HDX Insight	Bietet End-to-End-Transparenz für ICA-Verkehr, der durch NetScaler geleitet wird.
Netzwerkberichterstattung	Zeigt die Netzwerkleistung aller NetScaler-Instanzen an.
Web Insight	Bietet Einblick in Unternehmens-Webanwendungen und ermöglicht eine integrierte Überwachung von Anwendungen in Echtzeit.
Security Insight	Hilft dabei, den Sicherheitsstatus der Anwendung zu beurteilen und Korrekturmaßnahmen zu ergreifen, um die Anwendungen zu schützen.

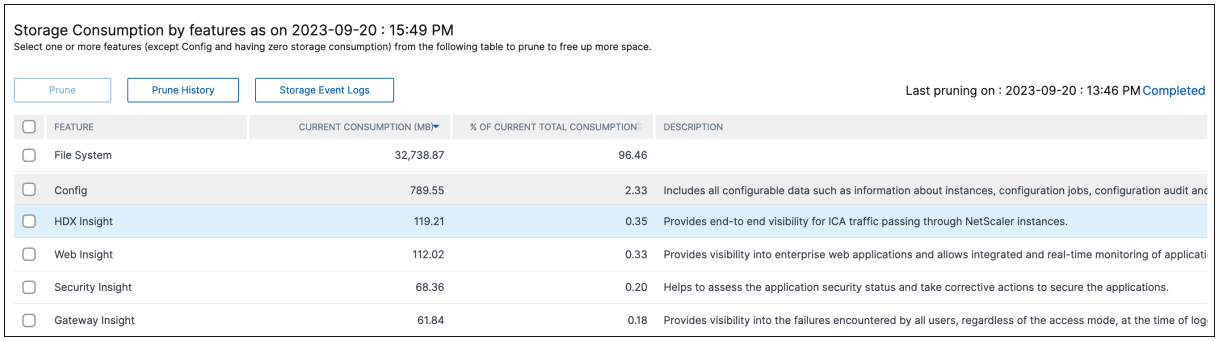
FEATURE	BESCHREIBUNG
Gateway Insight	Bietet Einblick in die Fehler, auf die alle Benutzer unabhängig vom Zugriffsmodus zum Zeitpunkt der Anmeldung bei NetScaler Gateway gestoßen sind.
Ereignisse	Überwachen und verwalten Sie das Auftreten von Ereignissen oder Fehlern auf den NetScaler-Instanzen.
App-Dashboard	Ermöglicht das Anzeigen und Verwalten von Anwendungen.
Bot Insight	Bietet Einblick in Bot-Verstöße und die daraufhin ergriffenen Maßnahmen.
Syslog	Überwacht Syslog-Ereignisse, die auf NetScaler-Instanzen generiert wurden, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Nachrichten an NetScaler ADM umgeleitet werden.
Video Insight	Überwacht die Metriken der Videooptimierungstechniken, die von NetScaler-Instanzen verwendet werden.
Detaillierte Transaktionen	Bietet Einblick in Webtransaktionen und zeigt die Antwortzeitmetrik, aufgeteilt auf den Client, NetScaler und den Server, visuell an.

Speicherverbrauch nach Funktionen

Weitere Informationen darüber, wie der Datenspeicher auf die verschiedenen Funktionen verteilt ist, finden Sie im **Abschnitt Speicherverbrauch nach Funktionen unter *dd mmm***.

Der Speicherverbrauch nach Funktionen wie in *dd mmm* hilft Ihnen zu verstehen:

- Der Speicherplatz, der von den verschiedenen Funktionen in NetScaler ADM verwendet wird
- Der Prozentsatz des Speicherplatzes, den die Features an einem bestimmten Tag beanspruchen



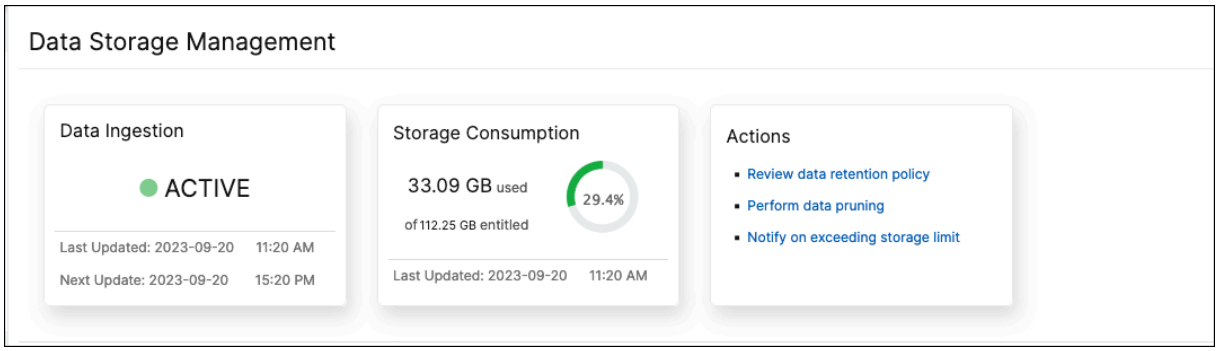
Wenn Sie die Tabelleneinträge sortieren möchten, die Kopfzeilen der Tabelle. NetScaler ADM sortiert die Tabelle anhand der Daten in der ausgewählten Spalte alphanumerisch von oben nach unten. Um die Tabelle in umgekehrter Reihenfolge zu sortieren, klicken Sie erneut auf die Spaltenüberschrift.

Informationen zum Bereinigen Ihrer Daten, zum Bereinigen des Verlaufs und zu Speicherereignisprotokollen finden Sie unter Datenspeicher verwalten

Verwalte deinen Speicherplatz

February 5, 2024

Sie können das **Datenspeichermanagement-Dashboard** verwenden, um Ihre Datenspeichernutzung zu beobachten und die erforderlichen Maßnahmen zu ergreifen, um Speicherplatz freizugeben oder Speicherplatz zu erhöhen, wenn Ihr Datenspeicher das lizenzierte Limit überschreitet.



Auf der Kachel **Aktionen** wird die Liste der empfohlenen Schritte angezeigt, die Sie zur Verwaltung Ihrer Speicherkapazität ergreifen können:

- Überprüfen Sie die Richtlinie zur Datenspeicherung
- Führen Sie eine Datenbereinigung durch
- Bei Überschreitung des Speicherlimits benachrichtigen

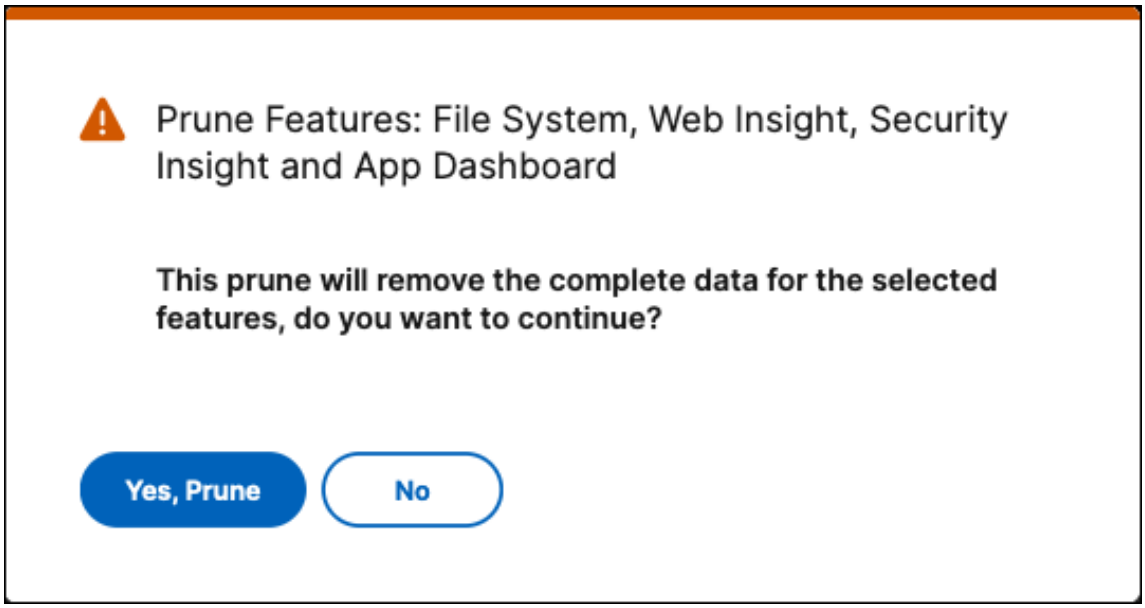
Führen Sie eine Datenbereinigung durch

Überarbeiten Sie Ihre Daten, um die Speicherressourcen zu optimieren und mehr Speicherplatz zu erhalten. Das Bereinigen von Daten spart nicht nur Speicherplatz, sondern verbessert auch die Datenqualität und beschleunigt die Verarbeitungszeiten. Wir empfehlen Ihnen, nicht benötigte Daten in regelmäßigen Abständen zu überprüfen und zu löschen. Dieser Prozess stellt sicher, dass Ihre Ressourcen sinnvoll eingesetzt werden und NetScaler ADM agil und reaktionsschnell ist.

So bereinigen Sie Ihre Daten:

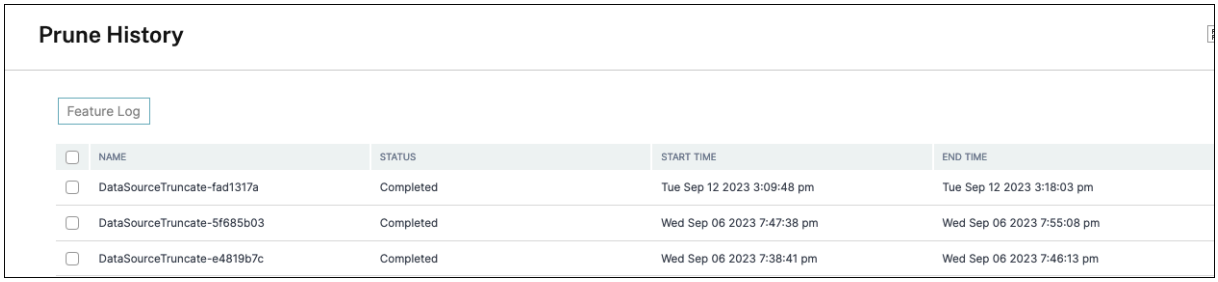
1. Scrollen Sie auf der Seite **Datenspeicherverwaltung** nach unten zum Abschnitt ***Speicherverbrauch nach Funktionen wie auf yyyy-mm-dd***.
2. Wählen Sie eine oder mehrere Funktionen aus und klicken Sie auf „**Ausschneiden**“. Sie können **Config** nicht auswählen, da es alle Systemkonfigurationen enthält.

   In einem Popup-Fenster werden Sie aufgefordert zu bestätigen, ob Sie alle Daten für die ausgewählten Features löschen möchten. Klicken Sie auf **Ja, Prune**.



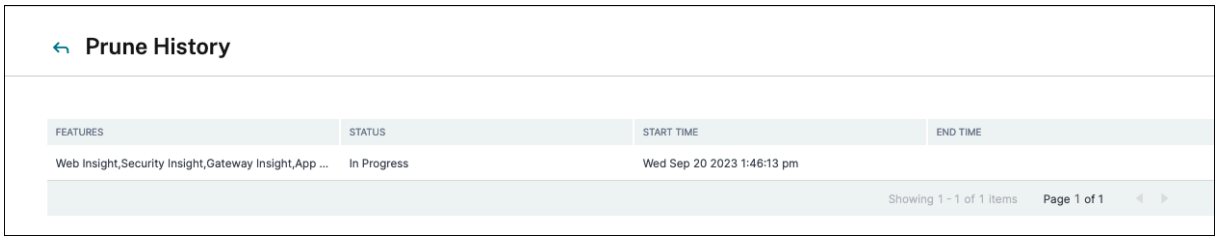
Geschichte der Pflaumen anzeigen

Klicken Sie auf **Prune-Verlauf anzeigen**, um Details zu allen Prune-Aktivitäten zu erhalten, die Sie in NetScaler ADM durchgeführt haben.



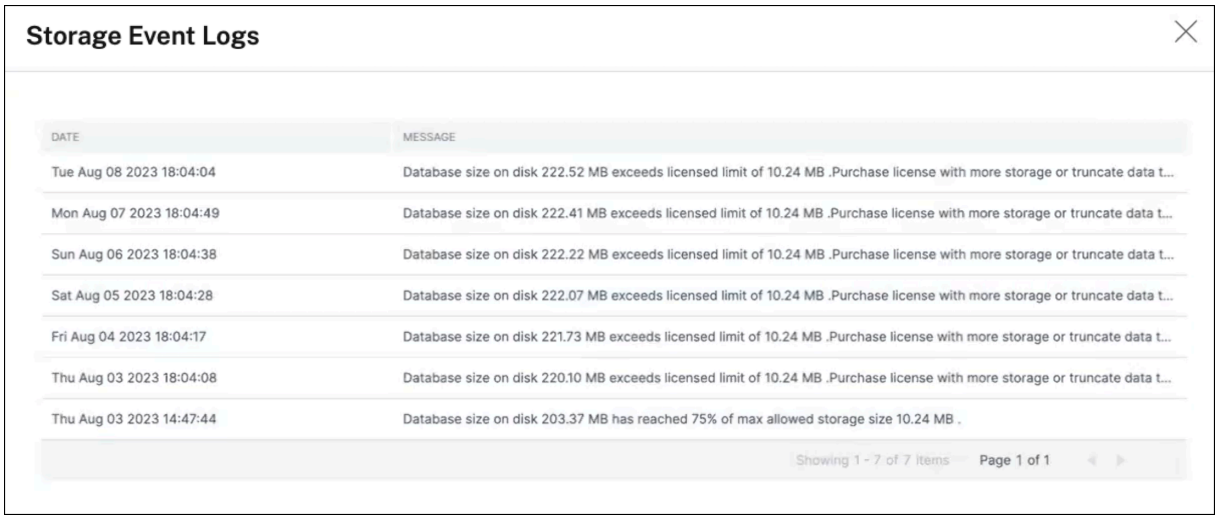
Auf der Seite **Prune Logs: Task Logs** wird die Liste aller Prune-Aufgaben angezeigt, einschließlich ihres jeweiligen Status, ihrer Start- und Endzeit.

Um zu erfahren, welche Features bei den einzelnen Prune-Vorgängen entfernt wurden, wählen Sie eine Aufgabe aus und klicken Sie auf **Feature-Log**.



Speicherereignisprotokolle anzeigen

Klicken Sie auf **Storage Event Logs**, um Informationen darüber zu erhalten, wie oft Ihre Daten 75% Ihres lizenzierten Limits überschritten oder erreicht haben.



Überprüfen Sie die Richtlinie zur Datenspeicherung

Die Datenaufbewahrungsrichtlinie bezieht sich auf eine Reihe von Regeln und Konfigurationen, die festlegen, wie NetScaler ADM historische Daten im Laufe der Zeit verwaltet und verwaltet. Diese

Richtlinie legt fest, wie lange Daten gespeichert werden, bevor sie automatisch gelöscht werden.

Wenn Sie den Speicherplatz reduzieren möchten, der von all den verschiedenen Funktionen verwendet wird, können Sie ändern, wie lange Daten in NetScaler ADM aufbewahrt werden.

Verwenden Sie die **Richtlinienseite zur Datenspeicherung**, um die Datenspeichereinstellungen zu bearbeiten für:

- Ereignismeldungen
- Syslog-Nachrichten
- Daten zur Netzwerkberichterstattung

Weitere Informationen zu den Datenspeichereinstellungen finden Sie unter Datenaufbewahrungsrichtlinie.

Bei Überschreitung des Speicherlimits benachrichtigen

Sie können Benachrichtigungen für NetScaler ADM einrichten, um Ihnen Benachrichtigungen zu senden, wenn Ihre Datenspeicherkapazität die angegebenen Grenzwerte überschreitet.

So können Sie Ihre Systembenachrichtigungen anzeigen und konfigurieren:

1. Klicken Sie in der Kachel **Aktionen** auf **Bei Überschreitung des Speicherlimits benachrichtigen**.
2. Stellen Sie auf der Seite **Systembenachrichtigungen konfigurieren** unter der Kategorie **Systemereignis sicher, dass die KategorieDataStorageExceeded** ausgewählt ist, um Benachrichtigungen zu erhalten.

Sie können verschiedene Parameter angeben, die sich darauf beziehen, wie und wann Benachrichtigungen an Sie oder andere Benutzer gesendet werden. Wählen Sie die bevorzugte Kommunikationsmethode aus (z. B. E-Mail-, Slack-, PagerDuty- und ServiceNow-Benachrichtigungen) und definieren Sie die Empfänger für die Benachrichtigungen.

Weitere Informationen zum Einrichten der Profile und zum Senden von Benachrichtigungen finden Sie unter Benachrichtigungen konfigurieren.

Datenaufbewahrungsrichtlinie

February 5, 2024

Um die Menge der Berichtsdaten zu begrenzen, die in der Datenbank Ihres NetScaler ADM-Servers gespeichert werden, können Sie das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten,

Ereignisse, Prüfprotokolle und Taskprotokolle speichern soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00.00 Uhr) bereinigt.

So konfigurieren Sie die Einstellung für Systemausfall:

1. Navigieren Sie zu **Einstellungen > Datenspeicherverwaltung > Datenaufbewahrungsrichtlinie**.
2. Klicken Sie auf der **Seite Datenbereinigung** auf **System**.
3. Geben Sie auf der Seite **System** die folgenden Details ein:
    - **Zu bewahrende Daten (Tage)** —Geben Sie die Anzahl der Tage ein, für die die Daten aufbewahrt werden müssen. Sie müssen einen Wert zwischen 1 und 30 angeben.
    - **Schwellenwert für Datenbereinigung (%)** —Geben Sie einen Schwellenwert (in Prozent) ein, der als Bedingung für Datenbereinigungs- oder Datenbereinigungsprozesse festgelegt werden soll. Wenn die Daten in der Datenbank diesen angegebenen Prozentsatz der Speicherkapazität erreichen, werden Datenbereinigungsverfahren ausgelöst, um Daten zu entfernen und Speicherplatz freizugeben.
    - **Automatische Bereinigung von Details** —Wählen Sie **Automatische Datenbereinigung aktivieren,** wenn die Datenbereinigung gestartet werden soll, wenn eines der folgenden Kriterien erfüllt ist:
        - Der in Data **Prune Threshold Value (%) angegebene Datenschwellenwert** ist erreicht.
        - Die im Wert Zu speichende **Daten (Tage) angegebene Anzahl von Tagen** wurde erreicht.
    - **Einstellung für Datenaufnahme** —Geben Sie einen Schwellenwert (in Prozent) ein, der als Bedingung für die Datenaufnahme festgelegt werden soll. Wenn die Daten in der Datenbank diesen angegebenen Prozentsatz erreichen, wird die Datenaufnahmeaktivität angehalten. Sie müssen einen Grenzwert zwischen 50 und 80% angeben.
4. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Konfigurieren der Einstellungen für die Instanz Syslog-Ausschneiden

Um die Menge der in der Datenbank gespeicherten Syslog-Daten zu begrenzen, können Sie das Intervall angeben, in dem Syslog-Daten gelöscht werden sollen. Sie können die Anzahl der Tage angeben, nach denen die generischen Syslog-Daten aus NetScaler ADM gelöscht werden.

So konfigurieren Sie die Einstellungen zum Löschen von Instanzsyslog-Einstellungen:

1. Navigieren Sie zu **Einstellungen > Datenspeicherverwaltung > Datenaufbewahrungsrichtlinie**.
2. Klicken Sie auf der Seite **Datenbereinigung** auf **Instanzereignisse**.

3. Geben Sie im Feld **Generische Syslog-Daten beibehalten** die Anzahl der Tage zwischen 1 und 180 an.
4. Klicken Sie auf **Speichern**.

Einstellungen für das Ausschneiden von Instanzereignissen konfigurieren

Um die Anzahl der Ereignismeldungsdaten zu begrenzen, die in der Datenbank Ihres NetScaler ADM-Servers gespeichert werden, können Sie das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle aufbewahren soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00:00 Uhr) beschnitten.

So konfigurieren Sie die Einstellungen für das Ausschneiden von Instanzereignissen:

1. Navigieren Sie zu **Einstellungen > Datenspeicherverwaltung > Datenaufbewahrungsrichtlinie**.
2. Klicken Sie auf der Seite **Datenbereinigung** auf **Instanzereignisse**.
3. **Geben**Sie im Feld Zu speichernde Daten (Tage)**das Zeitintervall in Tagen ein, für das Sie Daten auf dem NetScaler ADM-Server speichern möchten, und klicken Sie auf Speichern.**

Konfiguration der Bereinigungseinstellungen für Netzwerkberichte

Um die in NetScaler ADM gespeicherten Netzwerkberichtsdaten einzuschränken, können Sie das Intervall angeben, für das Sie die historischen Netzwerkberichtsdaten beibehalten möchten.

So konfigurieren Sie die Einstellungen für das Ausschneiden von Instanzereignissen:

1. Navigieren Sie zu **Einstellungen > Datenspeicherverwaltung > Datenaufbewahrungsrichtlinie**.
2. Klicken Sie auf der **Seite Datenbereinigung** auf **Network Reporting**.
3. Geben Sie im Feld **Zu bewahrende Daten (Tage)** die Anzahl der Tage zwischen 1 und 30 an.
4. Klicken Sie auf **Speichern**.

NetScaler ADM als API-Proxyserver

February 5, 2024

NetScaler Application Delivery Management (NetScaler ADM) kann nicht nur NITRO REST-API-Anfragen für seine eigenen Management- und Analysefunktionen empfangen, sondern auch als REST-API-Proxyserver für seine verwalteten Instanzen fungieren. Anstatt API-Anfragen direkt an die verwalteten Instanzen zu senden, können REST-API-Clients die API-Anfragen an NetScaler ADM

senden. NetScaler ADM kann zwischen den API-Anfragen, auf die es antworten muss, und den API-Anfragen, die es unverändert an eine verwaltete Instanz weiterleiten muss, unterscheiden.

Als API-Proxyserver bietet Ihnen NetScaler ADM die folgenden Vorteile:

- **Validierung von API-Anfragen**. NetScaler ADM validiert alle API-Anfragen anhand der konfigurierten Sicherheits- und rollenbasierten Zugriffskontrollrichtlinien (RBAC). NetScaler ADM ist auch mandantenorientiert und stellt sicher, dass API-Aktivitäten keine Mandantengrenzen überschreiten.
- **Zentralisiertes Audit.** NetScaler ADM führt ein Prüfprotokoll aller API-Aktivitäten im Zusammenhang mit seinen verwalteten Instanzen.
- **Sitzungsverwaltung**. NetScaler ADM befreit API-Clients von der Aufgabe, Sitzungen mit verwalteten Instanzen zu verwalten.

So funktioniert NetScaler ADM als API-Proxyserver

Wenn NetScaler ADM eine Anforderung an eine verwaltete Instanz weiterleiten soll, konfigurieren Sie den API-Client so, dass er einen der folgenden HTTP-Header in die API-Anforderung einschließt:

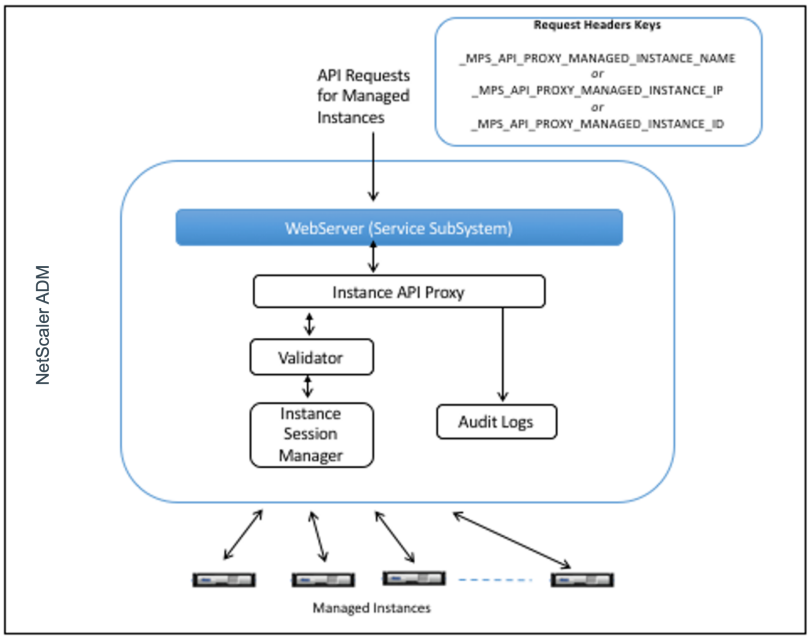
Header-Werte	Beschreibung
_MPS_API_PROXY_MANAGED_INSTANCE_NAME	Name der verwalteten Instanz.
_MPS_API_PROXY_MANAGED_INSTANCE_IP	IP-Adresse der verwalteten Instanz.
_MPS_API_PROXY_MANAGED_INSTANCE_ID	ID der verwalteten Instanz.
_MPS_API_PROXY_TIMEOUT	Timeout-Wert für eine NITRO-API-Anfrage. Legen Sie den Timeout-Wert in Sekunden fest. Wenn Sie ein Proxy-Timeout festlegen, wartet ADM auf die angegebene Dauer, bevor die Anforderung abgegeben wird.
_MPS_API_PROXY_MANAGED_INSTANCE_USERNAME	Benutzername für den Zugriff auf die verwaltete ADC-Instanz.
_MPS_API_PROXY_MANAGED_INSTANCE_PASSWORD	Kennwort für den Zugriff auf die verwaltete ADC-Instanz.
_MPS_API_PROXY_MANAGED_INSTANCE_SESSID	Sitzungs-ID für den Zugriff auf die verwaltete Instanz.

> **Hinweis**
>
> Wenn Sie **unter Einstellungen > Administration > Systemkonfigurationen > Grundeinstel-**

> **lungen**die Option **Anmeldeinformationen für Instanzenanmeldung auffordern**auswählen, müssen Sie den Benutzernamen und das Kennwort einer verwalteten Instanz konfigurieren. Alternativ können Sie auch die Instanzsitzungs-ID angeben.

Das Vorhandensein eines dieser HTTP-Header hilft NetScaler ADM, eine API-Anforderung als eine Anforderung zu identifizieren, die an eine verwaltete Instanz weitergeleitet werden muss. Der Wert des Headers hilft NetScaler ADM dabei, die verwaltete Instanz zu identifizieren, an die es die Anfrage weiterleiten muss.

Dieser Fluss ist in der folgenden Abbildung dargestellt:



Wie in der obigen Abbildung gezeigt, verarbeitet NetScaler ADM die Anforderung wie folgt, wenn einer dieser HTTP-Header in einer Anforderung angezeigt wird:

1. Ohne die Anfrage zu ändern, leitet NetScaler ADM die Anfrage an die Instanz-API-Proxy-Engine weiter.
2. Die Instanz-API-Proxy-Engine leitet die API-Anfrage an einen Validator weiter und protokolliert die Details der API-Anfrage im Audit-Protokoll.
3. Der Validator stellt sicher, dass die Anfrage nicht gegen konfigurierte Sicherheitsrichtlinien, RBAC-Richtlinien, Mandantengrenzen usw. verstößt. Es führt zusätzliche Prüfungen durch, z. B. eine Prüfung, um festzustellen, ob die verwaltete Instanz verfügbar ist.

Wenn die API-Anfrage gültig ist und an die verwaltete Instanz weitergeleitet werden kann, identifiziert NetScaler ADM eine Sitzung, die vom Instanz Session Manager verwaltet wird, und sendet dann die Anfrage an die verwaltete Instanz.

> **Hinweis:**
>
> Stellen Sie sicher, dass die Option **Anmeldeinformationen für Instanzanmeldung anfordern** deaktiviert ist. Vorgehensweise:
>
> 1. Navigieren Sie zu **Einstellungen > Administration**.
> 2. Wählen Sie in **Systemkonfigurationen** die Optionen **System, Zeitzone, Zulässige URLs und Meldung des Tages** aus.

Verwenden von NetScaler ADM als API-Proxyserver

Die folgenden Beispiele zeigen REST-API-Anfragen, die ein API-Client an einen NetScaler ADM-Server mit einer IP-Adresse von 192.0.2.5 sendet. NetScaler ADM ist erforderlich, um die Anfragen unverändert an eine verwaltete Instanz mit der IP-Adresse 192.0.2.10 weiterzuleiten. Alle Beispiele verwenden den _MPS_API_PROXY_MANAGED_INSTANCE_IP-Header.

Bevor NetScaler ADM die API-Anfragen sendet, muss der API-Client:

- Melden Sie sich bei NetScaler ADM an
- Besorgen Sie sich eine Sitzungs-ID
- Fügen Sie die Sitzungs-ID in nachfolgende API-Anfragen ein.

Die Anmelde-API-Anforderung hat das folgende Format:

```
    POST /nitro/v1/config/login
    Content-Type: application/json

    {

        "login": {

            "username":"nsroot",
            "password":"nsroot"
          }

     }

<!--NeedCopy-->
```

NetScaler ADM antwortet auf die Anmeldeanforderung mit einer Antwort, die die Sitzungs-ID enthält. Der folgende Beispielantworttext zeigt eine Sitzungs-ID:

```
{


  "errorcode": 0,

  "message": "Done",
```



```
 7
 8   "operation": "add",
 9
10   "resourceType": "login",
11
12   "username": "***********",
13
14   "tenant_name": "Owner",
15
16   "resourceName": "nsroot",
17
18   "login": [
19
20     {
21
22
23       "tenant_name": "Owner",
24
25       "permission": "superuser",
26
27       "session_timeout": "36000",
28
29       "challenge_token": "",
30
31       "username": "",
32
33       "login_type": "",
34
35       "challenge": "",
36
37       "client_ip": "",
38
39       "client_port": "-1",
40
41       "cert_verified": "false",
42
43       "sessionid": "##
     D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
44
45       "token": "b2f3f935e93db6a"
46      }
47
48
49    ]
50
51  }
52
53 <!--NeedCopy-->
```


Beispiel 1: Rufen Sie die Statistiken für virtuelle Load-Balancing-Server ab

Der Client muss NetScaler ADM eine API-Anforderung mit folgendem Formular senden:

```
1     GET /nitro/v1/stat/lbvserver
2     Content-type: application/json
3     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4     SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5  <!--NeedCopy-->
```

Wobei der Wert des Cookie-Headers die Sitzungs-ID ist, die vom Login-API-Aufruf zurückgegeben wird. Und der Wert von _MPS_API_PROXY_MANAGED_INSTANCE_IP ist die IP-Adresse des ADC.

Beispiel 2: Erstellen eines virtuellen Lastausgleichsservers

Der Client muss NetScaler ADM eine API-Anforderung mit folgendem Formular senden:

```
1     POST /nitro/v1/config/lbvserver/sample_lbvserver
2     Content-type: application/json
3     Accept-type: application/json
4     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5     SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
6
7     {
8
9          "lbvserver":{
10
11             "name":"sample_lbvserver",
12             "servicetype":"HTTP",
13             "ipv46":"10.102.1.11",
14             "port":"80"
15          }
16
17      }
18
19 <!--NeedCopy-->
```

Beispiel 3: Ändern Sie einen virtuellen Lastausgleichsserver

Der Client muss NetScaler ADM eine API-Anforderung mit folgendem Formular senden:

```
1     PUT /nitro/v1/config/lbvserver
2     Content-type: application/json
3     Accept-type: application/json
4     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5     SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```



```
6
7      {
8
9         "lbvserver":{
10
11              "name":"sample_lbvserver",
12              "appflowlog":"DISABLED"
13           }
14
15       }
16
17 <!--NeedCopy-->
```

Beispiel 4: Löschen eines virtuellen Load-Balancing-Servers

Der Client muss NetScaler ADM eine API-Anforderung mit folgendem Formular senden:

```
1      DELETE /nitro/v1/config/lbvserver/sample_lbvserver
2      Accept-type: application/json
3      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4      SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6  <!--NeedCopy-->
```

Beispiel 5: Laden Sie die CLI running Config auf dem ADC herunter

Der Client muss NetScaler ADM eine API-Anforderung mit folgendem Formular senden:

```
1      GET /nitro/v1/config/nsrunningconfig
2      Accept-type: application/json
3      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4      SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6  <!--NeedCopy-->
```

Häufig gestellte Fragen

February 5, 2024

Dieser Abschnitt enthält häufig gestellte Fragen zu den folgenden Funktionen von NetScaler Application Delivery Management (NetScaler ADM). Klicken Sie in der folgenden Tabelle auf einen Funktionsnamen, um die Liste der FAQs für diese Funktion anzuzeigen.

Analytics	Authentifizierung	Konfigurationsverwaltung
Zertifikatverwaltung	Bereitstellung	Bereitstellung (Disaster Recovery)
Event-Management	Instanz-Verwaltung	StyleBooks
Systemverwaltung		

Analytics

Ist es erforderlich, den virtuellen EUEM-Kanal auf NetScaler Gateway-Instanzen zu aktivieren, die im Single-Hop-Modus bereitgestellt werden

Virtuelle EUEM-Kanaldaten sind Teil von HDX Insight Daten, die NetScaler ADM von Gateway-Instanzen erhält. Der virtuelle EUEM-Kanal stellt die Daten über ICA-RTT bereit. Wenn der virtuelle EUEM-Kanal nicht aktiviert ist, werden die restlichen HDX Insight-Daten weiterhin auf NetScaler ADM angezeigt.

Der virtuelle EUEM-Kanal ist ein Standarddienst, der auf Citrix Virtual Desktop-Anwendungen (VDA) ausgeführt wird. Wenn es nicht ausgeführt wird, starten Sie den Prozess "Citrix End User Experience Monitoring"in VDA-Diensten.

Wie aktiviere ich NetScaler ADM, um Webanwendungs- und Virtual-Desktop-Datenverkehr zu überwachen?

1. Navigieren Sie zu **Infrastruktur** > **Instances** > **NetScaler** und wählen Sie die NetScaler-Instanz aus, auf der Sie Analytics aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
3. Wählen Sie auf der Seite "**Analytics konfigurieren** "alle virtuellen Server aus, auf denen Sie Analytics aktivieren möchten, und klicken Sie auf **AppFlow aktivieren**. Weitere Informationen finden Sie unter So aktivieren Sie Analytics für Instanzen.

> Hinweis
>
> Für NetScaler-Instanzen der Version 11.0, Version 65.30 und höher gibt es in NetScaler ADM keine Option, Security Insight explizit zu aktivieren. Stellen Sie sicher, dass Sie die AppFlow Parameter auf den NetScaler-Instanzen konfigurieren, damit NetScaler ADM den Security Insight-Datenverkehr zusammen mit dem Web Insight-Datenverkehr empfängt. Weitere Informationen zum Festlegen der AppFlow-Parameter auf NetScaler-Instanzen finden Sie unterSo legen Sie die AppFlow-Parameter mithilfe des Konfigurationsdienstprogrammsfest.

Wird NetScaler ADM nach dem Hinzufügen der NetScaler-Instanzen automatisch analytische Informationen gesammelt?

Nein. Aktivieren Sie Analysen auf den virtuellen Servern, die in NetScaler-Instanzen gehostet werden und von NetScaler ADM verwaltet werden. Weitere Informationen finden Sie unter So aktivieren Sie Analytics für Instanzen.

Ist es erforderlich, auf die einzelne NetScaler-Appliance zuzugreifen, um Analysen zu aktivieren?

Nein. Alle Konfigurationen erfolgen über die NetScaler ADM-Benutzeroberfläche, auf der die virtuellen Server aufgeführt sind, die auf der bestimmten NetScaler-Instanz gehostet werden. Weitere Informationen finden Sie unter So aktivieren Sie Analytics für Instanzen.

Welche Typen virtueller Server können in einer NetScaler-Instanz aufgeführt werden, um Analysen zu aktivieren?

Derzeit listet die NetScaler ADM-Benutzeroberfläche die folgenden virtuellen Server für die Aktivierung von Analysen auf:

- Virtueller Lastausgleichsserver
- Virtuelle Content Switching-Server
- Virtueller VPN-Server
- Virtueller Server für die Cache-Umleitung

Wie stelle ich einen zusätzlichen Datenträger für NetScaler ADM bereit?

So stellen Sie einen zusätzliche Datenträger für NetScaler ADM bereit:

1. Fahren Sie die virtuelle NetScaler ADM Maschine herunter.
2. Stellen Sie im Hypervisor einen zusätzliche Datenträger mit der erforderlichen Datenträgergröße für die virtuelle NetScaler ADM-Maschine bereit.

   Zum Beispiel, Betrachten wir, dass Sie den Speicherplatz auf 200 GB erhöhen möchten, in einer virtuellen NetScaler ADM Maschine von 120 GB. In diesem Szenario müssen Sie einen Datenträgerspeicher von 200 GB anstelle von 80 GB bereitstellen. Neu zugeordnete 200 GB Speicherplatz werden zum Speichern von Datenbankdaten und NetScaler ADM Protokolldateien verwendet. Der vorhandene 120 GB Datenträgerspeicher wird zum Speichern von Kerndateien, Betriebssystemprotokolldateien usw. verwendet.
3. Starten Sie die virtuelle NetScaler ADM Maschine.

Was meinen Sie mit Collectors sind nicht auf NetScaler-Instanzen konfiguriert?

Ein Collector empfängt AppFlow-Datensätze, die von der NetScaler-Appliance generiert wurden.

NetScaler ADM empfängt Security Insight- und Web Insight-Datenverkehr von den NetScaler-Instanzen, wenn die AppFlow-Funktion aktiviert ist. Wenn Sie die AppFlow-Funktion auf einer NetScaler-Instanz aktivieren, müssen Sie mindestens einen Collector angeben, an den die AppFlow-Datensätze gesendet werden. Wenn die Collectors nicht auf den NetScaler-Instanzen konfiguriert sind, empfängt NetScaler ADM den Datenverkehr nicht von den Instanzen.

Beispielsweise werden fünf NetScaler-Instanzen zu NetScaler ADM hinzugefügt. Wenn Collectors nicht für zwei Instanzen angegeben sind, fließt kein Datenverkehr an NetScaler ADM. Die Self-Service-Diagnose erkennt das Problem und zeigt das Problem als “Collectors sind nicht auf 2 Instanzen konfiguriert. “

Weitere Informationen zum Konfigurieren der AppFlow-Funktion finden Sie unter Konfigurieren der AppFlow-Funktion.

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.

Authentifizierung

Was ist Load Balancing von Authentifizierungsanfragen?

Mit der Load Balancing-Funktion des Authentifizierungsservers kann NetScaler ADM die Authentifizierungsanforderungen ausgleichen, die an die externen Authentifizierungsserver gerichtet sind. Der Lastenausgleich der Authentifizierungsserver stellt sicher, dass die Authentifizierungslast auf mehrere Authentifizierungsserver aufgeteilt wird, und verhindert so, dass ein Authentifizierungsserver überlastet wird. Sie können einen Authentifizierungsdienst erstellen, um sich mit Ihrem vorhandenen externen Authentifizierungsserver zu verbinden und Benutzerinformationen von diesem abzurufen, indem Sie die Authentifizierungsprotokolle wie LDAP, RADIUS oder TACACS verwenden.

Warum müssen wir externe Authentifizierungsserver kaskadieren?

Kaskadierte externe Authentifizierungsserver bieten eine unterbrechungsfreie Authentifizierungsverarbeitung und ermöglichen legitimen Benutzern den Zugriff, wenn ein Authentifizierungsserver aus-

fällt. Es gibt keine Beschränkung, welche Arten von Authentifizierungsservern Sie kaskadieren können. Sie können alle RADIUS-Server oder alle LDAP-Server oder eine Kombination aus RADIUS- und LDAP-Servern haben.

Wie viele externe Authentifizierungsserver kann ich kaskadieren?

Sie können bis zu 32 externe Authentifizierungsserver in NetScaler ADM kaskadieren.

Habe ich eine Alternative, wenn die externe Authentifizierung fehlschlägt?

Es kann vorkommen, dass die externe Authentifizierung vollständig fehlschlägt, selbst wenn Sie mehrere Server kaskadiert haben. Beispielsweise können die externen Server nicht mehr erreichbar sein, oder die Anmeldeinformationen eines neuen Benutzers wurden möglicherweise in keinem der externen Authentifizierungsserver eingegeben. Um zu verhindern, dass Benutzer in einer solchen Situation gesperrt werden, können Sie die lokale Fallback-Authentifizierung aktivieren. Weitere Einzelheiten finden Sie unterLokale Fallback-Authentifizierung.

Was ist die lokale Fallback-Authentifizierung?

Die lokale Fallback-Authentifizierung ist eine Option, um Ihre Benutzer lokal zu authentifizieren, wenn die externe Authentifizierung fehlschlägt. Wenn die externe Authentifizierung fehlschlägt, greift NetScaler ADM auf die lokale Benutzerdatenbank zu, um Ihre Benutzer zu authentifizieren.

Navigieren Sie in NetScaler ADM zu **Einstellungen > Authentifizierung > Authentifizierungskonfiguration**. Auf dieser Seite können Sie mehrere externe Authentifizierungsserver in einer Kaskade hinzufügen, und Sie können die Option **Enable fallback local authentication** auswählen.

Was ist eine Extraktion von externen Benutzergruppen?

Wenn Sie externe Server zur Authentifizierung der Benutzer hinzugefügt haben, können Sie vorhandene Benutzergruppen in NetScaler ADM importieren (extrahieren). Sie müssen Benutzergruppen einmal importieren und einer Benutzergruppe eine Gruppenberechtigung erteilen, anstatt einzelne Benutzer zu importieren und ihnen individuelle Berechtigungen zu erteilen. Sie müssen die Benutzer in NetScaler ADM nicht neu erstellen.

Warum müssen wir Gruppenberechtigungen zuweisen?

Wenn Sie die Lastenausgleichsfunktion von NetScaler verwenden, können Sie NetScaler ADM mit externen Authentifizierungsservern integrieren und Benutzergruppeninformationen von den Authen-

tifizierungsservern importieren. Melden Sie sich bei NetScaler ADM an, erstellen Sie dieselben Gruppeninformationen manuell in NetScaler ADM und weisen Sie diesen Gruppen die Berechtigung zu. Die Benutzer- und Benutzergruppenberechtigung wird in NetScaler ADM und nicht auf dem externen Server verwaltet. Die Benutzer haben unterschiedliche rollenbasierte Zugriffsberechtigungen auf den externen Servern. Konfigurieren Sie dieselben Berechtigungen auch für die Benutzer in NetScaler ADM. Anstatt die Berechtigungen für jeden Benutzer einzeln zu konfigurieren, können Sie eine Berechtigung auf Gruppenebene konfigurieren, sodass die Mitglieder der Benutzergruppe auf bestimmte Dienste auf den virtuellen Servern mit Lastausgleich zugreifen können. Die typischen Berechtigungen, die Sie vergeben können, sind Berechtigungen zur Verwaltung von NetScaler-Instanzen, NetScaler SDX-Instanzen, virtuellen Servern usw., sodass die Benutzer dieser Gruppe nur diese Instanzen oder virtuellen Server verwalten können. Sie können später die Berechtigungen bearbeiten, die den Benutzern auf Gruppenebene erteilt wurden. Sie können sogar eine oder mehrere Benutzergruppen entfernen. Andere Gruppenbenutzer funktionieren weiterhin in NetScaler ADM.

Konfigurationsverwaltung

Kann ich mit NetScaler ADM die Konfiguration über mehrere NetScaler-Instanzen hinweg gleichzeitig durchführen?

Ja, Sie können Konfigurationsaufträge verwenden, um die Konfiguration über mehrere NetScaler-Instanzen hinweg durchzuführen.

Was sind Konfigurationsjobs auf NetScaler ADM?

Ein Job ist ein Satz von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen erstellen und ausführen können. Sie können Jobs erstellen, um Konfigurationsänderungen über Instanzen hinweg vorzunehmen, Konfigurationen auf mehreren Instanzen in Ihrem Netzwerk zu replizieren und Konfigurationsaufgaben mit der NetScaler ADM-GUI aufzuzeichnen und abzuspielen. Sie können die aufgezeichneten Aufgaben auch in CLI-Befehle konvertieren.

Mit der Funktion Konfigurationsaufträge von NetScaler ADM können Sie einen Konfigurationsauftrag erstellen, E-Mail-Benachrichtigungen senden und Ausführungsprotokolle der erstellten Aufträge überprüfen.

Kann ich Jobs mit integrierten Vorlagen in NetScaler ADM planen?

Ja! Sie können einen Job planen, indem Sie die integrierte Vorlagenoption verwenden. Ein Job ist ein Satz 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 wählen, ob Sie den Job sofort ausführen oder den Job so planen, dass er später ausgeführt wird.

Sie können die Konfiguration eines zuvor erstellten Auftrags speichern und den Auftrag erneut ausführen, nachdem Sie die Befehle, die Parameter, die Konfigurationsquelle und die Zielinstanzen geändert haben. Dies 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.

Zertifikatverwaltung

Führt das Löschen von SSL-Zertifikaten aus NetScaler ADM zum Löschen von Zertifikaten aus NetScaler-Instanzen?

Nein

Bereitstellung

Was ist der Standardbenutzername und das Standardkennwort?

- Nachdem Sie die anfängliche Netzwerkkonfiguration abgeschlossen haben, können Sie sich über den Hypervisor oder die SSH-Konsole mit dem Standardbenutzernamen und dem Standardkennwort (nsrecover/nsroot) bei NetScaler ADM anmelden.
- Der Standardbenutzername und das Standardkennwort für die Anmeldung über die GUI sind *nsroot/nsroot*.

Wie ändere ich das Standardkennwort?

So ändern Sie das Kennwort:

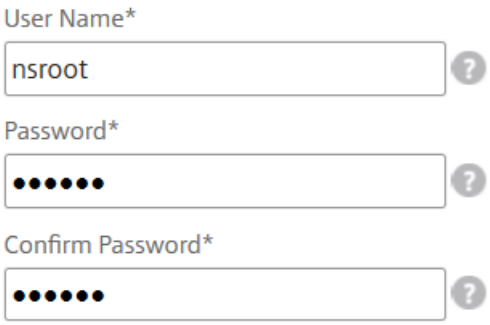
1. Navigieren Sie in NetScaler ADM zu **Einstellungen > Benutzerverwaltung > Benutzer**.

   Die Seite **Benutzer** wird angezeigt.

2. Wählen Sie den Benutzernamen **nsroot** aus, und klicken Sie auf **Bearbeiten**.

   Die Seite **“Systembenutzer konfigurieren** “wird angezeigt.

3. Wählen Sie **Kennwort ändern** aus und erstellen Sie ein Kennwort Ihrer Wahl.



4. Klicken Sie auf **OK**.

   Sie können jetzt das neue Kennwort verwenden, um sich von der GUI, dem Hypervisor oder der SSH-Konsole aus anzumelden.

   > Hinweis
   >
   > Sie können den Benutzernamen nicht ändern.

Wie setze ich das Kennwort zurück?

In dieser Dokumentation können Sie das Kennwort zurücksetzen.

Was ist in einem HA-Paar, wenn das Kennwort im primären Knoten geändert wird und wenn die Option HA-Paar brechen später ausgewählt ist, wie ist das Verhalten?

Sie können sich mit Ihrem neuen Kennwort an beiden eigenständigen Knoten anmelden.

Welche Auswirkungen hat die Bereitstellung dieser beiden Server in HA-Paaren, wenn zwei eigenständige Server unterschiedliche Kennwörter haben?

Es wird empfohlen, für beide Server ein Standardkennwort zu verwenden, wenn Sie zwei eigenständige Server für ein HA-Paar bereitstellen.

Die HA-Konfiguration ist abgeschlossen, aber auf die GUI des primären Knotens kann nicht zugegriffen werden. Was kann der Grund sein?

Es dauert ein paar Minuten, bis die Konfiguration wirksam wird. Sie können nach einigen Minuten erneut versuchen, darauf zuzugreifen.

Die HA-Konfiguration ist abgeschlossen, aber auf die grafische Benutzeroberfläche der Floating-IP kann nicht zugegriffen werden. Was kann der Grund sein?

Nach der HA-Konfiguration müssen Sie zuerst auf die GUI des primären Knotens zugreifen und die Bereitstellung abschließen. Weitere Informationen finden Sie unter Bereitstellen des primären und sekundären Knotens als Paar mit hoher Verfügbarkeit. Nach Abschluss der Bereitstellung wird der Server neu gestartet und für die Bereitstellung mit hoher Verfügbarkeit vorbereitet. Sie können dann auf die grafische Benutzeroberfläche der Floating-IP zugreifen.

Welche DB wird in NetScaler ADM Standalone und NetScaler ADM HA unterstützt?

Sowohl NetScaler ADM Standalone als auch NetScaler ADM HA unterstützen PostgreSQL.

Was ist der potenzielle Datenverlust für den sekundären Knoten?

Der sekundäre Knoten hört die Heartbeat-Nachrichten ab, die der primäre Knoten über die NetScaler ADM-Datenbank sendet. Wenn der sekundäre Knoten die Heartbeats länger als 180 Sekunden nicht empfängt, führt der sekundäre Knoten eine SSH-basierte Prüfung des primären Knotens durch. Wenn der Heartbeat und die SSH-basierte Prüfung fehlschlagen, wird der primäre Knoten als ausgefallen betrachtet.

In diesem Szenario übernimmt der sekundäre Knoten die Position des primären Knotens, und der 180-Sekunden-Zeitrahmen kann als möglicher Datenverlust für den sekundären Knoten betrachtet werden.

Was passiert, wenn der primäre Knoten ausgefallen ist?

Der sekundäre Knoten übernimmt und wird zum primären Knoten.

Wie installiere ich den ausgefallenen Knoten neu?

Es wird empfohlen, einen neuen VM-Build zu installieren. So installieren Sie es erneut:

1. Brechen Sie das HA-Paar. Navigieren Sie zu **Einstellungen> Bereitstellung**

   Die Seite “Bereitstellung”wird angezeigt. Klicken Sie auf **HA aufheben**
2. Löschen Sie den fehlgeschlagenen Knoten vom Hypervisor.
3. Importieren Sie die XVA-Imagedatei in den Hypervisor.

4. Konfigurieren Sie auf der Registerkarte Konsole NetScaler ADM mit den anfänglichen Netzwerkkonfigurationen. Weitere Informationen finden Sie unter Registrieren und Bereitstellen des ersten Servers (primärer Knoten) und Registrieren und Bereitstellen des zweiten Servers (sekundärer Knoten).
5. Stellen Sie das HA-Paar erneut bereit.

Unterstützt NetScaler ADM SAN-Speicher?

Citrix empfiehlt, die NetScaler ADM VHD auf einem lokalen Speicher zu hosten. Wenn NetScaler ADM auf Speichergeräten in einem SAN gehostet wird, funktioniert es möglicherweise nicht wie erwartet. Daher wird die ADM-Bereitstellung auf SAN nicht unterstützt.

Unterstützt NetScaler ADM einen zusätzlichen Datenträger?

Ja. Bei einer Neuinstallation des NetScaler ADM HA-Paars werden standardmäßig 120 GB Speicher zugewiesen. Für mehr als 120 GB Speicher können Sie einen zusätzlichen Datenträger für maximal 3 TB Speicher hinzufügen. Das Hinzufügen von mehr als einem zusätzlichen Datenträger wird nicht unterstützt.

Was passiert nach dem Deaktivieren des HA-Paares mit der konfigurierten Floating-IP-Adresse?

Auf die Floating-IP kann nicht mehr zugegriffen werden, und Sie müssen das Hochverfügbarkeitspaar erneut bereitstellen.

Kann ich während der erneuten Bereitstellung eine andere schwebende IP-Adresse angeben?

Ja. Sie können eine neue Floating-IP konfigurieren.

Warum ist die GUI des sekundären Knotens nicht zugänglich?

Der sekundäre Knoten ist nur ein Read-Replica-Server und fungiert nur dann als primärer Knoten, wenn der primäre Knoten aus irgendeinem Grund ausgefallen ist. Citrix empfiehlt, entweder auf die GUI für den primären Knoten oder die Floating-IP zuzugreifen.

Wenn der primäre Knoten über einen längeren Zeitraum ausgefallen ist, können die Konfigurationen weiterhin mit der Floating-IP-Adress-GUI durchgeführt werden?

Ja. Sie können weiterhin Konfigurationen durchführen und die Konfigurationen werden im sekundären Knoten gespeichert. Nachdem der primäre Knoten wieder da ist, werden alle Konfigurationen synchronisiert.

Was sind die empfohlenen Lösungen, wenn die IP-Adresse des primären Knotens oder die IP-Adresse des sekundären Knotens oder die Floating-IP in Zukunft geändert werden muss (z. B. die Änderung in IPv6)?

Das Ändern der IP-Adressen im HA-Paar wird nicht unterstützt, ohne das HA-Paar zu unterbrechen.

So aktualisieren Sie die IP-Adresse des primären Knotens oder des sekundären Knotens:

1. Brechen Sie das HA-Paar. Navigieren Sie zu **Einstellungen> Bereitstellung**.

   Die Seite Bereitstellung wird angezeigt. Klicken Sie auf **HA aufheben**

   a) Melden Sie sich mit einem SSH-Client oder vom Hypervisor am primären Knoten an.

   b) Verwenden Sie `nsrecover` als Benutzernamen und geben Sie das von Ihnen festgelegte Kennwort ein.

   c) Geben Sie **networkconfig ein**. Führen Sie den Vorgang aus **Schritt 3** unter Registrieren und bereitstellen des ersten Servers (Primärknoten) aus.

      Während der anfänglichen Netzwerkkonfiguration können Sie eine andere IP-Adresse angeben.

   d) Führen Sie dasselbe Verfahren für den sekundären Knoten aus, und fahren Sie mit dem Verfahren aus **Schritt 3** fort, das unter Registrieren und Bereitstellen des zweiten Servers (sekundärer Knoten)verfügbar ist.

So aktualisieren Sie die Floating-IP-Adresse:

1. Navigieren Sie zu **Einstellungen> Bereitstellung**.

   Die Seite Bereitstellung wird angezeigt.

   a) Klicke auf **HA-Einstellungen**.

   b) Klicken Sie auf **Floating-IP-Adresse für Hochverfügbarkeitsmodus konfigurieren**.

   c) Geben Sie die schwebende IP-Adresse ein und klicken Sie auf **OK**.

Unterstützt ADM AMD-Prozessoren?

AMD-Prozessor wird unterstützt in:

- **NetScaler ADM 13.1 Build 4.43 oder höher**.
- **NetScaler ADM Agent 13.1 Build 17.42 oder höher**.

Bereitstellung (Notfallwiederherstellung)

Wie häufig findet die Replikation zwischen dem primären Standort und dem Disaster Recovery-Standort statt?

Die Replikation zwischen dem primären Standort und dem Notfallwiederherstellungsstandort erfolgt in Echtzeit.

Wird der DR-Standort nach dem Initiieren des Backupskripts am DR-Standort zum temporären primären Standort, bis der primäre Standort wiederhergestellt und voll funktionsfähig ist?

Nein. Der DR-Standort wird nun zum primären Standort. Informationen zum Zurücksetzen des HA-Paars als primären Standort finden Sie unter Wiederherstellen von Konfigurationen auf den ursprünglichen primären Standort

Wenn die Option HA-Paar aufheben ausgewählt ist, arbeiten beide Knoten als eigenständiger Server. Da DR-Unterstützung für eigenständige Server nicht verfügbar ist, was passiert mit dem DR-Standort, wenn HA-Paar brechen ausgewählt wird?

Wenn Sie die Option HA-Paar brechen auswählen, wird die Replikation zwischen dem primären Standort und dem DR-Standort beendet. Sie müssen die DR-Website im Rahmen der erneuten Bereitstellung des HA-Paars neu konfigurieren.

Event-Management

Wie kann ich alle Ereignisse verfolgen, die mit NetScaler ADM auf meinen verwalteten NetScaler-Instanzen generiert wurden?

Als Netzwerkadministrator können Sie Details wie Konfigurationsänderungen, Anmeldebedingungen, Hardwarefehler, Schwellenverletzungen und Änderungen des Entitätsstatus in Ihren NetScaler-Instanzen sowie Ereignisse und deren Schweregrad bei bestimmten Instanzen anzeigen. Sie können das NetScaler ADM-Ereignis-Dashboard verwenden, um Berichte anzuzeigen, die für Details zum Schweregrad kritischer Ereignisse in allen Ihren NetScaler-Instanzen generiert wurden.

Was sind Event-Regeln?

Mit NetScaler ADM können Sie Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Ereignisregeln erleichtern die Überwachung vieler Ereignisse, die in Ihrer NetScaler ADM-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 Sie Filter erstellen können, sind Schweregrad, NetScaler-Instanzen, Kategorie- und Fehlerobjekte. Die Aktionen, die Sie den Ereignissen zuweisen können, sind das Senden einer E-Mail-Benachrichtigung, das Weiterleiten von SNMP-Traps von verwalteten NetScaler-Instanzen an den NetScaler ADM und das Senden einer SMS-Benachrichtigung.

Instanz-Verwaltung

Was passiert, wenn eine ADC-Instanz nach der Bandbreitenzuweisung keine Verbindung zu ADM herstellen kann, wenn Sie die gepoolte Kapazitätslizenzierung von NetScaler verwenden?

Wenn der Heartbeat zwischen der ADC-Instanz und ADM ausfällt, tritt die Instanz in eine Nachfrist von 30 Tagen ein. Und nachdem die Kommunikation wiederhergestellt ist, funktioniert die Lizenzierung gepoolter Kapazitäten. In der Nachfrist sind ADC-Funktionen nicht betroffen. Nach 30 Tagen Nachfrist startet die ADC-Instanz einen Warm-Neustart und ist nicht lizenziert.

Was sind Rechenzentren in NetScaler ADM?

Ein NetScaler ADM-Rechenzentrum ist eine logische Gruppierung der NetScaler-Instanzen an einem bestimmten geografischen Standort. Jeder Server kann mehrere NetScaler-Instanzen in einem Rechenzentrum überwachen und verwalten. Sie können den NetScaler ADM-Server verwenden, um Daten wie Syslog, Anwendungsdatenverkehr und SNMP-Traps aus den verwalteten Instanzen zu verwalten. Weitere Informationen zum Konfigurieren von Rechenzentren finden Sie unter Konfigurieren von Rechenzentren für Geomaps in NetScaler ADM.

Welche verschiedenen NetScaler ADC-Appliances werden von NetScaler ADM unterstützt?

Instanzen sind die NetScaler ADC-Appliances oder virtuellen Appliances, die Sie von NetScaler ADM aus erkennen, verwalten und überwachen möchten. Sie müssen diese Instanzen dem NetScaler ADM-Server hinzufügen. Sie können die folgenden NetScaler ADC-Appliances und virtuellen Appliances zu NetScaler ADM hinzufügen:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway

Sie können Instanzen hinzufügen, wenn Sie den NetScaler ADM-Server zum ersten Mal oder später einrichten.

Was ist ein Instanzprofil?

Ein Instanzprofil wird von NetScaler ADM verwendet, um auf eine Instanz zuzugreifen.

Ein Instanzprofil enthält den Benutzernamen und das Kennwort für den Zugriff auf eine oder mehrere Instanzen. Für jeden Instanztyp ist ein Standardprofil verfügbar. Beispielsweise ist das ns-root-Profil das Standardprofil für NetScaler-Instanzen. Es enthält die standardmäßigen NetScaler-Administratoranmeldeinformationen. Wenn Sie die für den Zugriff auf Instances erforderlichen Anmeldeinformationen ändern, können Sie benutzerdefinierte Instanzprofile für diese Instances definieren.

Kann ich mehrere NetScaler VPX-Instances in NetScaler ADM wiederentdecken?

Ja, Sie können mehrere Citrix **VPX-Instanzen** in NetScaler ADM wiederfinden, um die neuesten Zustände und Konfigurationen der Instanzen zu erfahren.

Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler > VPX**, wählen Sie die Instanzen aus, die Sie erneut ermitteln möchten, und klicken Sie in der Liste **Aktion** auf **Erneut ermitteln**. Weitere Informationen finden Sie unter Wiederentdecken mehrerer VPX-Instanzen.

Kann NetScaler ADM auf NetScaler SDX installiert werden?

Nein

Kann ich eine NetScaler-Instanz zur ADM-Software hinzufügen, indem ich eine öffentliche IP-Adresse verwende?

Ja, das können Sie mithilfe der Netzwerkadressübersetzung (NAT).

- Um eine einzelne Instanz hinzuzufügen: Verwenden Sie NAT-IP der öffentlichen IP-Adresse der ADC-Instanz.

- Um ein ADC-HA-Paar hinzuzufügen: Fügen Sie die NAT-IP-Adressen des HA-Paares in diesem Format hinzu:

  <NAT **public** IP of the primary instance>#<NAT **public** IP of the secondary instance>

- Zum Hinzufügen eines ADC-Clusters: Fügen Sie alle öffentlichen NAT-IP-Adressen aller Instanzen im Cluster hinzu, jeweils durch ein Komma getrennt, und fügen Sie die NAT-IP der CLUSTER-IP in Klammern oder runden Klammern hinzu. Ein Beispielformat: NAT1, NAT2, NAT3, (NATIP von CLUSTERIP).

Weitere Informationen finden Sie in den folgenden Artikeln:

- Instanzen zu NetScaler ADM hinzufügen
- Konfigurieren der Netzwerkadressübersetzung

Wie registriere ich einen Notfallwiederherstellungsknoten, wenn die Anmeldeinformationen für den DR-Knoten geändert werden?

Setzen Sie die Anmeldeinformationen des Notfallwiederherstellungsknotens (DR) auf `nsrecover` /`nsroot` zurück, indem Sie den folgenden Befehl verwenden:

```
./mps/change_freebsd_password.sh <username> <password>
<!--NeedCopy-->
```

Um einen DR-Knoten zu registrieren, führen Sie die Schritte unter Bereitstellen aus und registrieren Sie den NetScaler ADM DR-Knoten mithilfe der DR-Konsole.

StyleBooks

Können StyleBooks verwendet werden, um verschiedene NetScaler-Instanzen zu konfigurieren, die auf verschiedenen Versionen der NetScaler-Software ausgeführt werden?

Ja, Sie können StyleBooks verwenden, um verschiedene NetScaler-Instanzen zu konfigurieren, die auf verschiedenen Versionen ausgeführt werden, wenn keine Diskrepanz zwischen den Befehlen in verschiedenen Versionen besteht.

Was passiert, wenn ein StyleBook zum gleichzeitigen Konfigurieren mehrerer NetScaler-Instanzen verwendet wird und die Konfiguration einer NetScaler-Instanz fehlschlägt?

Wenn das Anwenden der Konfiguration auf eine NetScaler-Instanz fehlschlägt, wird die Konfiguration nicht auf weitere Instanzen angewendet, und bereits angewendete Konfigurationen werden zurück-

gesetzt.

Umfassen NetScaler-Backups, die über NetScaler erstellt wurden, Konfigurationen, die über StyleBooks angewendet werden?

Ja

Systemverwaltung

Kann ich meinem NetScaler ADM-Server einen Hostnamen zuweisen?

Ja, Sie können einen Hostnamen zuweisen, um den NetScaler ADM-Server zu identifizieren. Um einen Hostnamen zuzuweisen, navigieren Sie zu **System**> **Systemadministration** > **Systemeinstellungen**und klicken Sie auf **Hostnamen ändern**.

Der Hostname wird in der universellen Lizenz für NetScaler ADM angezeigt. WeitereInformationen finden Sie unter Zuweisen eines Hostnamens zu einem NetScaler ADM-Server.

Kann ich meine NetScaler ADM Konfiguration sichern und wiederherstellen?

Ja, Sie können Konfigurationsdateien (NTP-Dateien und SSL-Zertifikate), Systemdaten, Infrastruktur- und Anwendungsdaten sowie alle Ihre **SNMP-Einstellungen** sichern. Wenn NetScaler ADM jemals instabil wird, können Sie die gesicherten Dateien verwenden, um NetScaler ADM in einen stabilen Zustand wiederherzustellen.

Um Ihre NetScaler ADM-Konfiguration zu sichern und wiederherzustellen, navigieren Sie zu **System** > **Erweiterte Einstellungen** > **Backupdateien**und klicken Sie gegebenenfalls auf **Sichern** oder **Wiederherstellen** . Weitere Informationen finden Sie unterSichern und Wiederherstellen der Konfiguration auf NetScaler ADM.

Citrix empfiehlt, diese Funktion vor der Durchführung eines Upgrades oder aus Vorsichtsgründen zu verwenden.

Was sind Schwellenwerte und Alerts in NetScaler ADM?

Sie können Schwellenwerte und Warnungen festlegen, um den Status einer NetScaler-Instanz zu überwachen und Entitäten auf verwalteten Instanzen zu überwachen.

Wenn der Wert eines Zählers den Schwellenwert überschreitet, generiert NetScaler ADM eine Warnung, um auf ein leistungsbezogenes Problem hinzuweisen. Wenn der Zählerwert zu dem im Schwellenwert angegebenen Löschwert zurückkehrt, wird das Ereignis gelöscht.

Kann ich eine Datei für den technischen Support für NetScaler ADM generieren?

Ja. Citrix empfiehlt, dass Sie ein Archiv mit NetScaler ADM-Daten und Statistiken erstellen, bevor Sie sich an den technischen Support wenden, um ein Problem zu beheben. Das Archiv ist eine TAR-Datei, die Sie an das technische Support-Team senden können.

Sie können eine technische Supportdatei erstellen, die Debug-Protokolle, die Dauer, für die Debug-Protokolle gesammelt wurden, sowie unterschiedliche Protokolle aus der NetScaler ADM-Datenbank enthält.

Um eine Datei für den technischen Support zu konfigurieren und zu senden, navigieren Sie zu **System** > **Diagnose** > **Technischer Support** und klicken Sie dann auf **Datei für technischen Support generieren** . Weitere Informationen finden Sie unterGenerieren einer Tech Support-Datei für NetScaler ADM.

Was ist Syslog Säuberung?

Syslog ist ein Standardprotokoll für die Protokollierung. Syslog ermöglicht die Isolierung des Systems, das Informationen generiert, und des Systems, in dem die Informationen gespeichert werden. Sie können Protokollinformationen konsolidieren und Erkenntnisse aus den gesammelten Daten gewinnen. Sie können syslog auch so konfigurieren, dass verschiedene Arten von Ereignissen protokolliert werden.

Um die Menge der in der Datenbank gespeicherten Syslog-Daten zu begrenzen, können Sie das Intervall angeben, in dem Syslog-Daten gelöscht werden sollen. Sie können die Anzahl der Tage angeben, nach denen alle generischen Syslog-Daten, AppFirewall-Daten und NetScaler Gateway-Daten aus NetScaler ADM gelöscht werden.

Kann ich den NTP-Server auf NetScaler ADM konfigurieren?

Sie können einen Network Time Protocol (NTP) -Server in NetScaler ADM so konfigurieren, dass die NetScaler ADM-Uhr mit dem NTP-Server synchronisiert wird. Durch die Konfiguration eines NTP-Servers wird sichergestellt, dass die NetScaler ADM Uhr dieselben Datums- und Uhrzeiteinstellungen wie die anderen Server im Netzwerk aufweist.

Um einen NTP-Server zu konfigurieren, navigieren Sie zu **System** > **NTP-Server**, und klicken Sie dann auf **Hinzufügen**. Weitere Informationen finden Sie unterKonfigurieren des NTP-Servers auf NetScaler ADM.

Ab welcher Version wird die NetScaler ADM Active-Passiv-HA-Bereitstellung unterstützt?

Der Aktiv-Passiv-HA-Bereitstellungsmodus von NetScaler ADM wird ab NetScaler ADM Version 12.0 Build 51.24 unterstützt.

Ich hatte ein aktiv-aktives NetScaler ADM HA-Setup und hatte eine NetScaler-Appliance mit virtuellem Lastausgleichsserver für den einheitlichen GUI-Zugriff konfiguriert. Wie aktualisiere ich diese Konfiguration?

Nachdem Sie das NetScaler ADM HA-Paar in den Aktiv-Passiv-Modus aktualisiert haben, müssen Sie den folgenden Befehl auf der NetScaler-Appliance ausführen, um die Load Balancing-Konfiguration zu aktualisieren:

add lb monitor MAS_Monitor **TCP-ECV -send "GET /mas_health HTTP/1.1\r\nAccept-Encoding: identity\r\nUser-Agent: NetScaler-Monitor\r\nConnection: close\r\n\r\n"" -recv "{\"status-code\":0, \"is_passive\":0}"-LRTM DISABLED**

Kann ich den Lastausgleich des NetScaler ADM HA-Paars auf einer NetScaler-Instanz über Port 443 konfigurieren?

Nein, Sie können den Lastenausgleich des NetScaler ADM HA-Paars auf einer NetScaler-Instanz nicht über Port 443 konfigurieren.

Wenn Sie die `http-ecv` und `https-ecv` Monitore auf NetScaler konfigurieren, werden die NetScaler ADM HA-Knoten nicht ordnungsgemäß überwacht.

Kann eine NetScaler ADM-Serverbackupdatei verwendet werden, um die Konfiguration eines anderen NetScaler ADM-Servers wiederherzustellen?

Ja

Kann diese Backupdatei verwendet werden, um die Konfiguration einer anderen NetScaler-Instanz über NetScaler ADM wiederherzustellen, nachdem NetScaler ADM ein Backup einer NetScaler-Instanz erstellt hat?

Ja. Laden Sie die NetScaler ADM-Backupdatei herunter, laden Sie sie in das Backup-Repository einer anderen NetScaler-Instanz hoch und stellen Sie diese Instanz wieder her. Stellen Sie sicher, dass die Netzwerkinformationen und Authentifizierungsinformationen nicht in Konflikt stehen. Prüfen Sie beispielsweise auf IP-Adressen- oder Portkonflikte, nicht übereinstimmende Kennwortprofile. Stellen

Sie außerdem sicher, dass die wiederhergestellte VPX-Instanz dieselbe NSIP-Adresse und NetScaler Lizenz hat wie die gesicherte.

Stellen Sie vor dem Wiederherstellen einer Instanz in einem Hochverfügbarkeitspaar sicher, dass die IP-Adressen und der Status (primär oder sekundär), die in der Backupdatei gespeichert sind, mit denen der ursprünglichen HA-Konfiguration übereinstimmen. Stellen Sie außerdem sicher, dass die neue primäre und sekundäre NetScaler Lizenz denselben Typ haben.

Können wir NetScaler ADM zwingen, eine SNIP-Adresse für die Kommunikation mit den NetScaler-Instanzen zu verwenden, anstatt die NSIP-Adresse des NetScaler ADM-Servers zu verwenden?

Ja, Sie können eine SNIP-Adresse (mit aktivierter Verwaltung) in NetScaler ADM für die Kommunikation mit NetScaler-Instanzen hinzufügen.

Wenn ich ein Backup der NetScaler-Instanzen in NetScaler ADM erstelle, ist das Ergebnis eine vollständiges Backup oder nur ein einfaches Backup?

Backups von NetScaler-Instanzen von NetScaler ADM sind vollständige Backups.

Gibt es eine Anleitung zur Fehlerbehebung für NetScaler ADM?

Ja. Siehe https://support.citrix.com/article/CTX224502.

Wie werden NetScaler-Instanzen verwaltet, wenn ein NetScaler ADM HA-Failover auftritt?

Wenn die Heartbeat- und SSH-basierte Prüfung fehlschlägt, wird der primäre Knoten als ausgefallen betrachtet und der sekundäre Knoten übernimmt die Position des primären Knotens. Alle NetScaler-Instanzen werden standardmäßig mit den neuesten primären Knotendetails als SNMP-Trap-Ziel aktualisiert.

Der neue primäre (aktive) NetScaler ADM-Knoten prüft, ob der zuvor aktive Knoten als AppFlow-Collector oder Syslog-Server konfiguriert wurde. Falls dies der Fall war, fügt der neue Primärserver den an die Instanzen gesendeten Informationen die AppFlow-Collector- oder Syslog-Serverdetails hinzu.

Für Syslog ersetzt es die alten Serverdetails.

Was passiert, wenn der heruntergegangene NetScaler ADM HA-Knoten wieder hochgefahren wird?

Nach der Rückkehr in den Dienst bleibt der NetScaler ADM-Knoten passiv, es sei denn, der aktive Knoten schlägt fehl

Wie werden NetScaler-Instanzen über NetScaler ADM HA-Knoten verteilt?

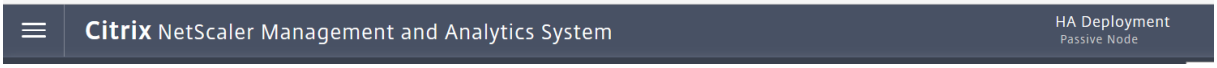
Alle NetScaler-Instanzen werden vom primären NetScaler ADM Knoten verwaltet.

Wie werden virtuelle Serverlizenzen verwaltet, wenn es ein NetScaler ADM HA-Failover gibt?

Wenn der primäre NetScaler ADM Knoten, auf dem virtuelle Serverlizenzen angewendet werden, ausfällt, verwaltet der neue primäre Knoten die virtuellen Serverlizenzen für einen Kulanzzeitraum von 30 Tagen. Wenden Sie die Lizenzen vor Ablauf der Nachfrist erneut auf die neue Grundschule an. Für Alternativen wenden Sie sich an den NetScaler-Support.

Ist ein Load Balancer für ein NetScaler ADM HA-Setup obligatorisch?

Nein, aber wenn kein Load Balancer vorhanden ist, muss auf NetScaler ADM Knoten über ihre eigenen IP-Adressen zugegriffen werden. Der passive Knoten ist mit dem Tag "Passiv"gekennzeichnet, und Citrix empfiehlt, keine Konfigurationen auf dem passiven Knoten zu erstellen.



Unterstützt NetScaler ADM eine externe Datenbank?

Nein

Kann eine NetScaler-Instanz, die von NetScaler ADM verwaltet wird, als Load Balancer für NetScaler ADM HA verwendet werden?

Ja

Welche Daten werden zwischen NetScaler ADM HA-Knoten synchronisiert?

Die vollständige NetScaler ADM-Datenbank wird synchronisiert und die folgenden Ordner werden synchronisiert:

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/