NetScaler Console-Dienst

Machine translated content

Disclaimer

Contents

Übersicht

January 26, 2024

Der NetScaler Console Service (früher bekannt als NetScaler ADM Service) ist eine webbasierte Lösung für die Verwaltung aller NetScaler-Bereitstellungen, einschließlich NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler CPX, NetScaler BLX und NetScaler Gateway, die on-premises oder in der Cloud bereitgestellt werden.

Mit dieser Cloud-Lösung können Sie die gesamte globale Anwendungsbereitstellungsinfrastruktur über eine einzige, einheitliche und zentrale cloudbasierte Konsole verwalten, überwachen und beheben. NetScaler Console bietet alle Funktionen, die für die schnelle Einrichtung, Bereitstellung und Verwaltung der Anwendungsbereitstellung in NetScaler-Bereitstellungen erforderlich sind, und bietet umfangreiche Analysen zu Zustand, Leistung und Sicherheit von Anwendungen.

NetScaler Console bietet die folgenden Vorteile:

- **Agilität** —Einfach zu bedienen, zu aktualisieren und zu verwenden. Das Servicemodell von NetScaler Console ist über die Cloud verfügbar, sodass die von NetScaler Console bereitgestellten Funktionen einfach zu bedienen, zu aktualisieren und zu verwenden sind. Die Häufigkeit von Updates in Kombination mit der automatischen Update-Funktion verbessert die NetScaler Bereitstellung schnell.
- **Schnellere Wertschöpfung** —Schnellere Erreichung der Geschäftsziele. Im Gegensatz zur herkömmlichen on-premises Bereitstellung können Sie Ihre NetScaler Console mit wenigen Klicks verwenden. Sie sparen nicht nur die Installations- und Konfigurationszeit, sondern vermeiden auch Zeit- und Ressourcenverschwendung für potenzielle Fehler.
- **Multisite-Management** —Einheitlicher Überblick für Instanzen in Multisite-Rechenzentren. Mit der NetScaler Console können Sie NetScaler verwalten und überwachen, die sich in verschiedenen Bereitstellungstypen befinden. Sie haben eine zentrale Verwaltung für NetScaler, die on-premises und in der Cloud bereitgestellt werden.
- **Betriebseffizienz** —Optimierte und automatisierte Methode zur Erzielung höherer Betriebsproduktivität. Mit der NetScaler Console reduzieren Sie Ihre Betriebskosten, da Sie Zeit, Geld und Ressourcen für die Wartung und Aktualisierung herkömmlicher Hardwarebereitstellungen sparen.
- **Einblick in den Internetverkehr in Echtzeit** —Verbesserte Benutzererfahrung mit der Analyse des Internetverkehrs in Echtzeit. Mit der NetScaler Console können Sie echte Benutzerüberwachungsdaten von Kunden sammeln, die über Clouds, Rechenzentren und CDNs auf Anwendungen zugreifen, und sich ein ganzheitliches Bild des Internetzustands machen. Der Traffic wird an Standorte mit der niedrigsten Latenz und der besten Verfügbarkeit geleitet, um ein optimales Benutzererlebnis zu gewährleisten.

- **Multisite-Anwendungen** —Erstellen, konfigurieren und stellen Sie eine Multisite-Anwendung bereit. Mit der NetScaler Console können Sie Anwendungen in mehreren Cloud-Umgebungen konfigurieren, bereitstellen und verwalten, um eine hohe Verfügbarkeit und Zuverlässigkeit zu gewährleisten.

So funktioniert NetScaler Console

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

Ein Agent ermöglicht die Kommunikation zwischen der NetScaler Console und den verwalteten Instanzen in Ihrem Rechenzentrum. Der Agent sammelt Daten von den verwalteten Instanzen in Ihrem Netzwerk und sendet sie an die NetScaler Console.

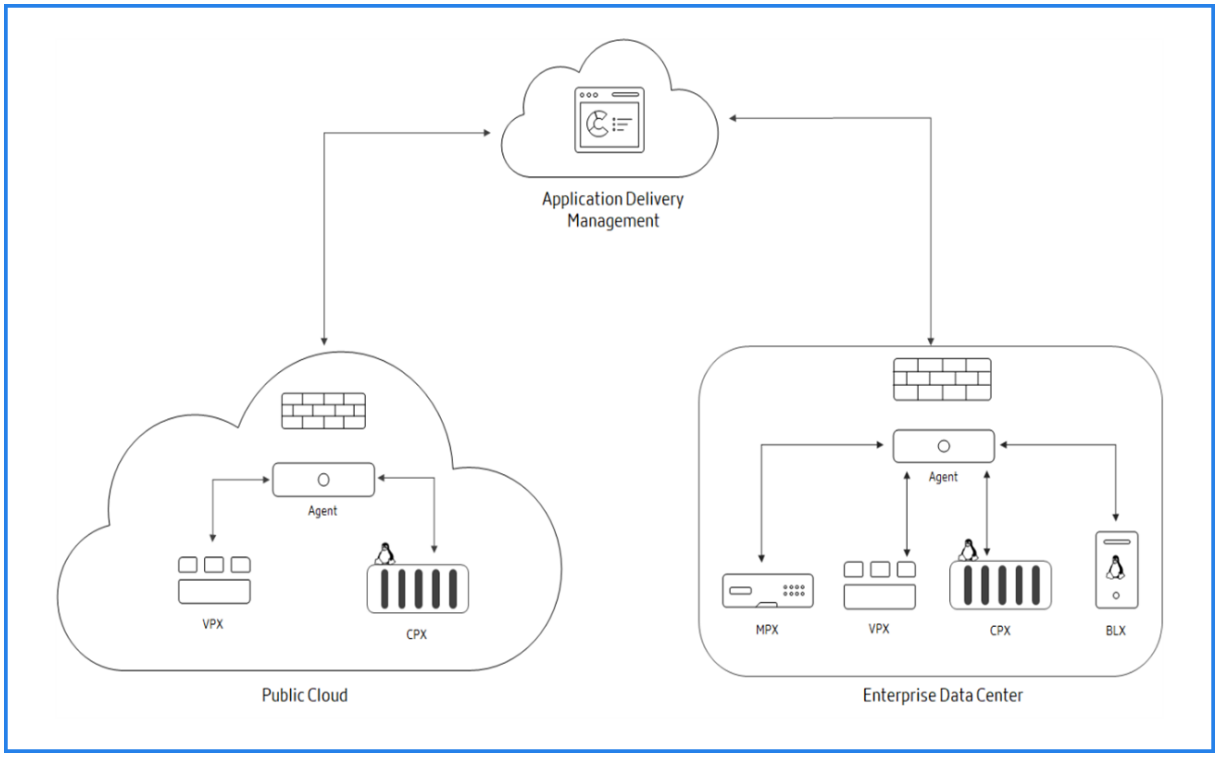
Wenn Sie der NetScaler Console eine Instanz hinzufügen, fügt sie sich implizit selbst als Trap-Ziel hinzu und erfasst ein Inventar der Instanz.

Der Dienst sammelt Instanzdetails wie:

- Hostname
- Softwareversion
- Konfiguration wird ausgeführt und gespeichert
- Zertifikate
- Entitäten, die für die Instanz konfiguriert sind, usw.

NetScaler Console fragt verwaltete Instanzen regelmäßig ab, um Informationen zu sammeln. Weitere Informationen finden Sie unter Data Governance.

Die folgende Abbildung zeigt die Kommunikation zwischen dem Dienst, den Agents und den Instanzen (MPX, VPX, CPX, BLX):



Informationen zur Integration in die NetScaler Console und deren Funktionsweise finden Sie unter Erste Schritte und die zugehörigen Unterthemen.

Features und Lösungen

January 26, 2024

In diesem Dokument werden die Funktionen beschrieben, die von der NetScaler Console unterstützt werden.

Anwendungsanalyse und -management

Die Anwendungsanalyse- und Verwaltungsfunktion der NetScaler Console stärkt den anwendungsorientierten Ansatz und hilft Ihnen dabei, verschiedene Herausforderungen bei der Anwendungsbereitstellung zu bewältigen. Dieser Ansatz gibt Ihnen Einblick in die Integritätsbewertungen von Anwendungen, hilft Ihnen bei der Bestimmung der Sicherheitsrisiken und hilft Ihnen, Anomalien in den Datenverkehrsströmen der Anwendung zu erkennen und Korrekturmaßnahmen zu ergreifen.

- Analyse der Anwendungsleistung: App Score ist das Produkt eines Bewertungssystems, das definiert, wie gut eine Anwendung funktioniert. Es zeigt, ob die Anwendung hinsichtlich der Reaktionsfähigkeit eine gute Leistung erbringt, nicht anfällig für Bedrohungen ist und ob alle Systeme betriebsbereit sind.

- Analyse der 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, kleine Fensterangriffe und DNS-Flutangriffe für die erkannten NetScaler-Instanzen an.
- Intelligente App Analytics: Die Intelligent App Analytics-Funktion bietet eine einfache und skalierbare Lösung für die Überwachung und Fehlerbehebung von Anwendungen, die über NetScaler Appliances bereitgestellt werden. Intelligent App Analytics überwacht nicht nur alle Ebenen von Anwendungstransaktionen, sondern verwendet auch Techniken des maschinellen Lernens, um normale Verkehrsmuster in Ihrem Netzwerk zu definieren und Anomalien zu erkennen. Diese Funktion reduziert die Gesamtdurchlaufzeit und verbessert die Gesamtverfügbarkeit der Anwendung.

StyleBooks

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 ein StyleBook entwerfen, um Konfigurationen für eine Bereitstellung von Unternehmensanwendungen wie Microsoft Exchange oder Skype for Business zu erstellen.

Instanzverwaltung

Ermöglicht das Verwalten der NetScaler-, NetScaler Gateway- und Citrix Secure Web Gateway-Instanzen.

Ereignisverwaltung

Ereignisse stellen Ereignisse oder Fehler in einer verwalteten NetScaler-Instanz dar. Wenn beispielsweise ein Systemausfall oder eine Änderung der Konfiguration auftritt, wird ein Ereignis generiert und in der NetScaler Console aufgezeichnet. Im Folgenden sind die zugehörigen Funktionen aufgeführt, die Sie mithilfe der NetScaler Console konfigurieren oder anzeigen können:

- Erstellen von Ereignisregeln
- Verwenden der NetScaler Console zum Exportieren von Syslog-Meldungen

Zertifikatverwaltung

NetScaler Console optimiert jeden Aspekt der Zertifikatsverwaltung für Sie. Über eine einzige Konsole können Sie automatisierte Richtlinien einrichten, um den richtigen Aussteller, die richtige Schlüsselstärke und korrekte Algorithmen sicherzustellen, während Sie nicht verwendete oder bald ablaufende Zertifikate im Auge behalten.

Konfigurationsverwaltung

Mit NetScaler Console können Sie Konfigurationsjobs erstellen, mit denen Sie Konfigurationsaufgaben wie das Erstellen von Entitäten, das Konfigurieren von Funktionen, das Replizieren von Konfigurationsänderungen, Systemaktualisierungen und andere Wartungsaktivitäten mühelos auf mehreren Instanzen ausführen können. Konfigurationsaufträge und Vorlagen vereinfachen die sich am häufigsten wiederholenden Verwaltungsaufgaben in einer einzigen Aufgabe auf der NetScaler Console.

Konfigurationsaudit

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

- Konfigurationsempfehlung: Ermöglicht es Ihnen, Konfigurationsanomalien zu identifizieren.
- Audit-Vorlage: Ermöglicht es Ihnen, die Änderungen in einer bestimmten Konfiguration zu überwachen.

Verwaltung der Lizenzen

Ermöglicht die Verwaltung von NetScaler-Lizenzen, indem Sie NetScaler Console als Lizenzmanager konfigurieren.

- NetScaler gepoolte Kapazität: Ein gemeinsamer Lizenzpool, aus dem Ihre NetScaler-Instanz eine Instanzlizenz und nur so viel Bandbreite auschecken kann, wie sie benötigt. Wenn die Instanz diese Ressourcen nicht mehr benötigt, werden sie wieder in den gemeinsamen Pool eingecheckt und die Ressourcen anderen Instanzen zur Verfügung gestellt, die sie benötigen.
- NetScaler VPX-Lizenzierung beim Ein- und Auschecken: NetScaler Console weist Lizenzen für NetScaler VPX-Instanzen nach Bedarf zu. Eine NetScaler VPX-Instanz kann die Lizenz von der NetScaler Console auschecken, wenn eine NetScaler VPX-Instanz bereitgestellt wird, oder ihre Lizenz wieder in die NetScaler Console einchecken, wenn eine Instanz entfernt oder zerstört wird.

Netzwerkberichterstellung

Sie können die Ressourcennutzung optimieren, indem Sie Ihre Netzwerkberichte in der NetScaler Console überwachen.

Analytics

Bietet eine einfache und skalierbare Möglichkeit, die verschiedenen Erkenntnisse der Daten der NetScaler-Instanzen zu untersuchen, zu prognostizieren und die Anwendungsleistung zu verbessern. Sie können eine oder mehrere Analysefunktionen gleichzeitig verwenden.

- HDX Insight: Bietet End-to-End-Sichtbarkeit für ICA-Datenverkehr, der durch NetScaler geleitet wird. Mit HDX Insight können Administratoren Client- und Netzwerklatenzmetriken, historische Berichte und End-to-End-Leistungsdaten in Echtzeit anzeigen und Leistungsprobleme beheben.

- Web Insight: Bietet Einblick in Unternehmens-Webanwendungen. Es ermöglicht IT-Administratoren, alle vom NetScaler bereitgestellten Webanwendungen zu überwachen, indem eine integrierte Überwachung von Anwendungen in Echtzeit bereitgestellt wird. Web Insight verarbeitet Daten von NetScaler mithilfe eines Approximationsalgorithmus. Es bietet die 1.000 wichtigsten Datensätze der Metriken, die sich auf die Webanwendungen in Ihrem Unternehmen beziehen.
- Gateway Insight: Bietet Einblick in 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 Lösung aus einem einzigen Bereich, mit der Sie den Sicherheitsstatus Ihrer Anwendung bewerten und Korrekturmaßnahmen ergreifen können, um Ihre Anwendungen zu schützen.
- SSL Insight: Bietet Einblick in sichere Transaktionen im Internet (HTTPs). Es ermöglicht IT-Administratoren, alle vom NetScaler bereitgestellten Webanwendungen zu überwachen, indem eine integrierte Echtzeit- und historische Überwachung von Webtransaktionen bereitgestellt wird. SSL Insight verarbeitet Daten von NetScaler mithilfe eines Näherungsalgorithmus. Es bietet die 1.000 wichtigsten Datensätze der Metriken im Zusammenhang mit den Webtransaktionen in Ihrem Unternehmen.

Rollenbasierte Zugriffssteuerung

Mit der rollenbasierten Zugriffssteuerung (RBAC) können Sie Zugriffsberechtigungen basierend auf den Rollen einzelner Benutzer in Ihrem Unternehmen erteilen. Der erste Benutzer einer Organisation, der sich mit Citrix Cloud-Anmeldeinformationen anmeldet, hat die Super-Admin-Rolle, der standardmäßig über alle Zugriffsberechtigungen verfügt. Den anderen Benutzern dieser Organisation, die später vom Administrator erstellt werden, werden Nicht-Administratorrollen zugewiesen.

Subscriptions

Bietet eine Dashboard-Ansicht der Abonnements, die Sie gekauft haben.

Sie sind standardmäßig einem Express-Konto zugewiesen. Mit diesem Konto können Sie begrenzte NetScaler Console-Ressourcen verwalten. Weitere Informationen finden Sie unter NetScaler Console-Ressourcen mithilfe des Express-Kontos verwalten .

Die folgenden NetScaler Console-Funktionen sind derzeit nicht verfügbar:

- Bereitstellung
  - Migration von Citrix Insight Center zur NetScaler Console
  - Integration von NetScaler Console in Citrix Virtual Desktop Director

- Analytik: TCP Insight und Video Insight
- Eingeschränkte Systemeinstellungen
- Orchestrierung
  - Integration mit OpenStack und VMware NSX Manager
  - NetScaler-Automatisierung im Hybridmodus von Cisco ACI
  - Container Orchestration: Integration mit Mesos/Marathon und Kubernetes

Versionshinweise

January 26, 2024

In den Versionshinweisen zur NetScaler Console (früher bekannt als NetScaler ADM Service) werden die neuen Funktionen, Verbesserungen vorhandener Funktionen, behobene Probleme und bekannte Probleme beschrieben, die in einem Service Release verfügbar sind.

Weitere Informationen:

- Was ist neu
- Frühere Veröffentlichungen

Der NetScaler Agent wird standardmäßig automatisch auf den neuesten Build der NetScaler Console aktualisiert. Sie können die Agentdetails auf der Seite **Infrastruktur > Instanzen > Agents** anzeigen. Sie können auch den Zeitpunkt angeben, zu dem die Agent-Upgrades durchgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren der Agent-Upgrade-Einstellungen.

Was ist neu

September 2, 2024

July 25, 2024

Behobenes Problem

Infrastruktur Wenn Sie **unter Infrastruktur > Upgrade-Jobs** eine NetScaler-Instanz aktualisieren, die klassische Richtlinien hat, listet die Validierung vor dem Upgrade die Instanz als **Instanzen auf, die für das Upgrade gesperrt sind**, und das Upgrade findet nicht statt.

Problemumgehung: Bevor Sie eine Instanz aktualisieren, empfehlen wir, die klassischen Richtlinien in erweiterte Richtlinien für die Funktionen zu konvertieren, die vom NSPEPI-Tool unterstützt werden. Weitere Informationen finden Sie unter Überlegungen zum Upgrade für Konfigurationen mit klassischen Richtlinien.

[NSADM-113851]

Telemetrie Als Teil des NetScaler-Telemetrieprogramms prüft NetScaler Console nicht mehr alle 24 Stunden, ob die folgende Konfiguration vorhanden ist, oder überträgt sie an NetScaler-Instanzen. Zuvor wurde die Konfiguration alle 24 Stunden überprüft und auf NetScaler-Instanzen übertragen, falls sie fehlte:

```
enable ns feature AppFlow
add analytics profile telemetry_metrics_profile -type timeseries -
    outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "
    ./telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency
    300
```

[NSADM-114375]

July 15, 2024

Infrastruktur

NetScaler-eigene IP-Adressen in der NetScaler Console-GUI anzeigen und exportieren Sie können jetzt NetScaler-eigene IP-Adressen (**Infrastruktur > Instanzen > NetScaler-eigene IPs) in der NetScaler Console-GUI** anzeigen und exportieren.

Weitere Informationen finden Sie unter NetScaler-eigene IP-Adressen anzeigen.

[NSADM-88798, NSADM-91769]

Lizenzierung

Details für VPX-Instanzen, die auf einer SDX-Instanz bereitgestellt wurden, im Flexed-Lizenzierungs-Dashboard anzeigen Im Flexed-Lizenzierungs-Dashboard (**NetScaler Licensing > Flected Licensing > Dashboard**) unter **Licensed NetScalers** können Sie die Anzahl der VPX-Instanzen einsehen, die für NetScaler SDX ausgecheckt sind. Sie können jetzt auf die Anzahl klicken, um die bereitgestellten VPX-Instanzdetails für dieses SDX anzuzeigen, z. B. Instanzname, IP-Adresse, Durchsatz (MBPS) und Edition.

Zuvor konnten Sie nur die Gesamtzahl der VPX-Instanzen anzeigen, die für dieses SDX ausgecheckt wurden.

[NSADM-105358]

Details zur MPX/SDX-Host-ID und Seriennummer unter Nullkapazitätslizenzen anzeigen Unter **NetScaler Licensing > Zero-Capacity-Lizenzen** können Sie jetzt Details zur **Host-ID** und **Seriennummer** für die MPX- und SDX-Instanzen anzeigen.

[NSADM-100327]

Behobene Probleme

Die Probleme, die im Build am 15. Juli 2024 behoben wurden.

Infrastruktur

- Wenn Sie eine Instanz in NetScaler Console (Infrastruktur > Instances > NetScaler) ändern, z. B. die Site oder das Admin-Profil ändern, werden die Schlüssel-Wert-Paare der mit der Instanz verknüpften Tags umgekehrt.

  [NSHELP-38083]

- Wenn Sie in Config Job die ShowConfiguration-Vorlage gleichzeitig auf dem primären und dem sekundären NetScaler in einem HA-Paar ausführen, wird durch Klicken auf Ergebnisdateien herunterladen die Datei nur für die sekundäre Instanz heruntergeladen.

  [NSHELP-37831]

- Wenn in Network Reporting (Infrastruktur > Network Reporting) kein Dashboard vorhanden ist, wird die folgende Fehlermeldung angezeigt:

  “Sie haben keinen Zugriff auf diese Seite”

  Diese Fehlermeldung kann ignoriert werden und hindert Sie nicht daran, Dashboards zu erstellen.

  [NSADM-113332]

- Die SNMP-Traps werden im NetScaler Console-Dienst nicht empfangen, wenn er mit dem integrierten Agenten konfiguriert wird.

  [NSHELP-38191]

StyleBooks Wenn Sie in der NetScaler Console-GUI ein Config Pack bearbeiten, um ein anderes StyleBook zu verwenden, funktioniert das Upgrade nicht wie erwartet.

[NSADM-110351]

July 09, 2024

Unterstützung bei der Identifizierung und Behebung von CVE-2024-5491 und CVE-2024-5492

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2024-5491 und CVE-2024-5492.

- Die Identifizierung für CVE-2024-5491 erfordert eine Kombination aus Versions- und Konfigurationsscan.
- Für die Identifizierung von CVE-2024-5492 ist ein Versionsscan erforderlich.

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 Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Jobs zum Upgrade von NetScaler-Instanzen.

Weitere Informationen finden Sie im Sicherheitsbulletin.

> **Hinweis:**
>
> Es kann einige Stunden dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2024-5491 und CVE-2024-5492 im Sicherheitsberatungsmodul reflektiert werden. Um die Auswirkungen früher zu erkennen, können Sie einen Scan auf Anforderung starten, indem Sie auf **Jetzt scannen** klicken.

18. Juni 2024

Telemetrie

NetScaler Telemetrieprogramm Als bestehender NetScaler Console-Kunde müssen Sie die Anforderungen des NetScaler Telemetrie-Programms erfüllen, für das die Erfassung von Telemetriedaten zur Lizenz- und Funktionsnutzung erforderlich ist. Die Telemetriedaten werden alle 24 Stunden automatisch hochgeladen, sodass Sie nichts unternehmen müssen.

- Weitere Informationen finden Sie unter NetScaler Telemetrie-Programm.
- Weitere Informationen zu den Telemetrieparametern finden Sie unter Data Governance.

[NSADM-113300]

11. Juni 2024

Analytics

Metrics Collector und Lean Period-Nutzungsanalysen sind auf virtueller Serverebene aktiviert Der Metriksammler und die Lean-Nutzungsanalyse sind jetzt auf virtueller Serverebene statt auf Instanzebene aktiviert. Mit dieser Erweiterung bleiben der Metriksammler und die Lean-Nutzungsanalyse nur auf Ihren aktiven virtuellen Servern mit hohem Traffic aktiviert.

Sie können Ihre virtuellen Server überprüfen und den **Metrics Collector** aktivieren und die Nutzung auf anderen virtuellen Servern überprüfen, indem Sie zu **Einstellungen > Analytics-Konfiguration** navigieren und unter **Zusammenfassung der virtuellen Server-Metriken auf Messobjektekonfigurieren** klicken.

Weitere Informationen finden Sie unter Konfigurieren von Intelligent App Analytics.

[NSADM-111609]

Weisen Sie in NetScaler-Instanzen ein Netzprofil für die Erfassung von Metriken zu Wenn Sie den Messobjektsammler für die virtuellen Server in NetScaler Console aktivieren, werden die Messobjektdaten von NetScaler über die NetScaler-Subnetz-IP-Adresse (SNIP) in die NetScaler Console exportiert. In einigen Szenarien kann das SNIP aufgrund der Firewall im Netzwerk blockiert werden. In solchen Szenarien müssen Sie möglicherweise eine andere IP-Adresse verwenden. Weitere Informationen zum Netzprofil finden Sie unter Verwenden einer angegebenen Quell-IP für die Back-End-Kommunikation.

Sie können der NetScaler-Instanz jetzt ein Netzprofil für die Erfassung von Metriken zuweisen. Metrics Collector überträgt die NetScaler-Leistungsindikatordaten an die NetScaler Console, die zur Erkennung von Anwendungsproblemen verwendet wird. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**, wählen Sie die Instanz aus und klicken Sie in der Liste **Aktion auswählen** auf **Netzprofile für Metrics Collector konfigurieren**.

Weitere Informationen zum Zuweisen eines Netzprofils finden Sie unter Netzprofil für die verwaltete NetScaler-Instanz zuweisen.

[NSADM-111138]

Observability Integration —Details für ein fehlgeschlagenes NetScaler-Abonnement anzeigen Wenn Sie in **Observability Integration**ein Abonnement für NetScaler für Splunk oder Prometheus konfigurieren, können Sie jetzt detaillierte Protokolle für die fehlgeschlagenen Abonnements anzeigen. Als Administrator können Sie anhand dieser Protokolle den Grund für den Abonnementfehler analysieren.

Weitere Informationen finden Sie unter Protokolle für fehlgeschlagene Konfigurationen anzeigen

[NSADM-109022]

Entfernung der periodischen Exportoption für WAF- und Bot-Insights in der Observability Integration Die periodische Exportoption für WAF- und Bot-Insight wird jetzt entfernt, wenn Sie den Export von Erkenntnissen von NetScaler Console in Observability-Tools (wie Splunk, New Relic und Microsoft Sentinel) konfigurieren. Da WAF- und Bot-Verstöße von entscheidender Bedeutung sind, wird empfohlen, die Echtzeit-Exportoption zu verwenden, um Erkenntnisse in Echtzeit zu exportieren, wann immer sie auftreten.

Jedes bestehende Abonnement mit regelmäßiger Exportkonfiguration für WAF und Bot wird automatisch auf Echtzeitexport umgestellt.

[NSADM-109019]

Infrastruktur

Unterstützung für "App-basierte"Bereitstellung Der NetScaler Console Service führt die "App-basierte"Bereitstellung für AWS und Azure ein. Diese Funktion optimiert und vereinfacht NetScaler-Bereitstellungen in Cloud-Rechenzentren und ermöglicht eine effiziente Anwendungsbereitstellung aus diesen Umgebungen.

Weitere Informationen finden Sie unter App-basierte Bereitstellung in AWS und App-basierte Bereitstellung in Azure.

[NSADM-108491]

Behobene Probleme

Die Probleme, die in Build am 11. Juni 2024 behoben wurden.

Analytics

- Ein Prozess in NetScaler Console/Agent kann aufgrund einer Speicherbeschädigung abstürzen.

  [NSHELP-38032]

- In **Web Insight**sind die Details für den virtuellen Lastausgleichsserver, der hinter dem virtuellen Content Switching-Server konfiguriert ist, für tägliche, wöchentliche und monatliche Berichte nicht sichtbar.

  [NSHELP-37713]

Infrastruktur

- Wenn Benutzer ohne Administratorrechte versuchen, Statistiken für die virtuellen Server in der NetScaler Console (**Infrastruktur > Netzwerkfunktionen**) anzuzeigen, wird die folgende Fehlermeldung angezeigt:

  “Nicht zugriffsberechtigt ”

  [NSHELP-37977]

- Wenn Sie in einem HA-Setup den integrierten Agenten „Mastools“zusammen mit den Partitionen verwenden, lautet der Status der sekundären NetScaler-Instanz im SSL-Dashboard (**Infrastruktur >SSL-Dashboard**) und im Load Balancing (**Infrastruktur > Netzwerkfunktionen > Load Balancing**) „unbekannt“.

  [NSHELP-37902]

StyleBooks

- Wenn Sie die Konfigurationspakete bearbeiten, werden alle Änderungen, die Sie an ACLs oder Policy-Based Routing (PBR) -Regeln wie Hinzufügen, Aktualisieren oder Löschen vornehmen, nicht angewendet.

  [NSHELP-37656]

5. Juni 2024

Analytics

Integrieren Sie NetScaler Console in Microsoft Sentinel In **Observability Integration** können Sie jetzt die Integration von NetScaler Console mit Microsoft Sentinel konfigurieren, um Erkenntnisse in Microsoft Sentinel zu exportieren und anzuzeigen. Stellen Sie für eine erfolgreiche Integration sicher, dass die folgenden Voraussetzungen erfüllt sind:

- **Azure-Abonnement** —Ein Azure-Abonnement für die Bereitstellung und Verwendung von Microsoft Sentinel.
- **Log Analytics Workspace** —Ein Workspace ist erforderlich, um die gesammelten Daten zu speichern und zu analysieren.
- **IAM-Rollen** —Berechtigungsstufen wie Leser, Mitwirkender müssen für den Workspace festgelegt werden.
- **Benutzerdefinierte Tabellen** —Zum Speichern und Senden der NetScaler Console-Daten an den Workspace.

Weitere Informationen finden Sie unter Integration mit Microsoft Sentinel

[NSADM-108930]

Plattform

Unterstützung für OpenSSH Version 9.x Die OpenSSH-Version auf NetScaler wurde jetzt von 8.x auf 9.x aktualisiert.

[NSPLAT-29640]

StyleBooks

Option Als Entwurf speichern in Konfigurationspaketen Sie können das Konfigurationspaket jetzt als Entwurf speichern. Gehen Sie wie folgt vor, um die Konfiguration als Entwurf zu speichern:

1. Navigieren Sie zu **Anwendungen > Konfiguration > Config Packs**.
2. Klicken Sie auf der Seite **Konfigurationen** auf **Hinzufügen**.
3. Wählen Sie ein Stylebook aus und klicken Sie auf **Auswählen**.
4. Klicken Sie auf der Seite **Konfiguration erstellen** auf **Als Entwurf speichern**.

Die gespeicherten Entwürfe werden auf der Registerkarte **Entwurfskonfigurationen** unter **Ausstehende Konfigurationen** angezeigt.

Weitere Informationen finden Sie unter Konfigurationspakete als Entwurf speichern.

[NSADM-110734]

Zeitplanoption in Konfigurationspaketen Sie können jetzt die Bereitstellung neu erstellter Konfigurationspakete planen. Gehen Sie wie folgt vor, um einen Zeitplan für ein neues Config Pack zu erstellen:

1. Navigieren Sie zu **Anwendungen > Konfiguration > Config Packs**.
2. Klicken Sie auf der Seite **Konfigurationen** auf **Hinzufügen**.
3. Wählen Sie das Stylebook aus und klicken Sie auf **Auswählen**.
4. Wählen Sie auf der Seite **Konfiguration erstellen** unter **Ausführung** in der Liste **Ausführungsmodus** die Option **Später** aus.
5. Wählen Sie die gewünschte Uhrzeit und das gewünschte Datum für die Planung aus.

Für bereitgestellte Config Packs können Sie planen, wann die Updates veröffentlicht und wann das Config Pack gelöscht werden soll. Die Planungsoptionen sind verfügbar, wenn Sie ein bereitgestelltes Konfigurationspaket bearbeiten.

Weitere Informationen finden Sie unter Zeitplan für ein Konfigurationspaket erstellen.

[NSADM-110728]

Behobene Probleme

Die Probleme, die in Build vom 5. Juni 2024 behoben wurden.

Analytics

- Die Details zum **Anwendungsstatus** im **Übersichts-Dashboard** zeigen nicht dieselben Details an, die unter **Application Score** im **App-Dashboard** verfügbar sind.

  [NSHELP-37720]

- Wenn mehr als 25000 virtuelle Server über NetScaler Console verwaltet werden, benötigt App Dashboard möglicherweise mehr Zeit, um Details zu laden.

  [NSADM-111705]

Infrastruktur

- Die Ereignisregeln generieren nicht die erwarteten Aktionen, wenn sich der Status der Dienstgruppe ändert.

  [NSHELP-37616]

StyleBooks

- Wenn Sie der benutzerdefinierten Datenquelle in StyleBooks Sammlungsdaten mit leeren Werten für Felder vom Typ IP-Adresse, Ganzzahl oder Boolean hinzufügen, schlägt der Vorgang möglicherweise fehl.

  [NSHELP-37826]

- Wenn Sie ein Konfigurationspaket über die NetScaler Console-GUI erstellen, gibt das System möglicherweise eine leere Liste für die Parameter zurück, die sich auf die integrierte verwaltete ADC-Datenquelle beziehen.

  [NSHELP-37824]

- Wenn Sie versuchen, ein Konfigurationspaket zu erstellen oder einen Probelauf durchzuführen, schlagen die Operationen möglicherweise fehl, wenn die beiden folgenden Bedingungen erfüllt sind:

  - Die StyleBook-Definition verweist auf ein anderes StyleBook im Komponentenabschnitt.
  - Wenn Sie Eigenschaften zwischen dem aktuellen StyleBook und dem referenzierten StyleBook Parameter vom Typ “Datum”zuweisen.

  [NSHELP-37793]

22. Mai 2024

Analytics

Massenupgrade virtueller SSL-Server mithilfe der Upgrade-Aufgabe für die Bewertung SSL A+ Unter **Aufgaben** können Sie jetzt die **Upgrade-Aufgabe für die SSL A+-Rating** anzeigen. Der bestehende Upgrade-Prozess zur SSL-Bewertung auf A+ im **App Dashboard** ermöglicht es Ihnen, jeweils nur eine Anwendung zu aktualisieren. Mithilfe der **Upgrade-Aufgabe für die SSL A+-Rating** können Sie ein Bulk-Upgrade durchführen.

NetScaler Console überprüft die SSL-Konfiguration des virtuellen Anwendungsservers mit dem NetScaler Secure Front-End-Profil und identifiziert die Anwendungen, die nicht mit A+ bewertet wurden. Die **Upgrade-Aufgabe für die SSL-Bewertung A+** zeigt die Anwendungen an, die nicht mit A+ bewertet wurden. Als Administrator können Sie Anwendungen auswählen und ein Massen-Upgrade durchführen, um die SSL-Konformität zu erreichen.

Weitere Informationen finden Sie unter Umsetzbare Aufgaben und Empfehlungen.

[NSADM-108164]

Lizenzierung

Tatsächliche Nutzungsdetails in der Flexed-Lizenzberichterstattung Im **Flected License Reporting**-Dashboard (**NetScaler Licensing > Flected Licensing > Reporting**) können Sie jetzt die tatsächliche Bandbreiten-/Durchsatznutzung einsehen, sodass Sie die Nutzungsdetails (Spitzenauslastungund durchschnittliche Nutzung) einsehen können. Zuvor wurden auf dem Dashboard nur die Zuordnungs- und Anspruchsdetails angezeigt.

Darüber hinaus sind die folgenden Verbesserungen auch im Flexed-Lizenzberichts-Dashboard verfügbar:

- Filtern Sie, um Details für ausgewählte NetScaler-Instanzen anzuzeigen.
- Option zum Exportieren von Details im PDF-, PNG- und JPEG-Format.
- Bandbreite wird in Durchsatzkapazität umbenannt.

Weitere Informationen finden Sie unter Flexed-Lizenzberichte.

[NSADM-97093]

StyleBooks

Erstellen Sie NetScaler-Richtlinienausdrücke in StyleBooks Mit der StyleBooks-GUI können Sie jetzt NetScaler-Richtlinienausdrücke erstellen, indem Sie Elemente aus Listen auswählen, sodass Sie Ausdrücke schneller und genauer erstellen können. Um den Editor für Richtlinienausdrücke für einen

Parameter verfügbar zu machen, geben Sie das GUI-Attribut `is_policy_expression` in der Parameterdefinition von StyleBooks an.

Weitere Informationen finden Sie unter Richtlinienausdrücke in StyleBooks.

[NSADM-12651]

Behobene Probleme

Die Probleme, die in Build am 22. Mai 2024 behoben wurden.

Infrastruktur Wenn Sie in **Config Job** die **ShowConfiguration**-Vorlage gleichzeitig auf dem primären und dem sekundären NetScaler in einem HA-Paar ausführen, wird durch Klicken auf **Ergebnisdateien herunterladen** die Datei nur für die sekundäre Instanz heruntergeladen.

[NSHELP-37831]

StyleBooks Wenn Sie eine NetScaler-Instanz löschen, die eine Subnetz-IP-Adresse (SNIP) für den Verwaltungszugriff von der NetScaler Console verwendet, und die Instanz dann erneut hinzufügen, schlagen die vor dem Löschen der Instanz erstellten Konfigurationspakete möglicherweise fehl.

[NSHELP-37786]

April 23, 2024

Analytics

Unterstützung für den Export periodischer Daten für benutzerdefinierte NetScaler-Instanzen Wenn Sie ein Abonnement für den Datenexport von NetScaler Console nach Splunk oder New Relic erstellen, können Sie jetzt den **Periodischen Export** (täglich oder stündlich) auswählen und ihn auf die benutzerdefinierten Instanzen anwenden. Zuvor wurde der periodische Insights-Datenexport in die benutzerdefinierten Instanzen nicht unterstützt.

[NSADM-109020]

Infrastruktur

Zusätzliche Ereigniswarnung bei Datenträgerauslastung NetScaler Console ermöglicht es Ihnen jetzt, einen zusätzlichen Schwellenwert für Alarme zur Datenträgerauslastung festzulegen. Mit diesem Schwellenwert können Sie einen unteren Grenzwert festlegen, um Benachrichtigungen zu erhalten, bevor ein oberer Schwellenwert überschritten wird. Um den Schwellenwert auf niedrigerer

Ebene zu konfigurieren, navigieren Sie zu **Einstellungen > SNMP > Bearbeiten** und aktivieren Sie die Option **Unteren Schwellenwert konfigurieren**.

Weitere Informationen finden Sie unter Systemalarme konfigurieren und anzeigen.

[NSADM-97285]

Behobene Probleme

Die Probleme, die im Build April 23, 2024 behoben wurden.

Infrastruktur

- Wenn Sie versuchen, den NetScaler Console-Bericht als Snapshot unter **Infrastruktur > Instanzen > NetScaler** zu exportieren, reagiert die Seite nicht mehr.

  [NSHELP-37689]

- Wenn mehr als 10 NetScaler-Instanzen über einen Agenten in der NetScaler Console verwaltet werden, schlägt das Agenteninventarsubsystem fehl. Daher ruft die NetScaler Console nicht die neuesten NetScaler-Konfigurationsdaten ab.

  [NSHELP-37749]

Lizenzierung

- Die Anzahl der im Flexed-License-Dashboard angezeigten Instanzen ist falsch.

  [NSHELP-37733]

Sicherheit

- Wenn Sie Verstoßdatensätze in tabellarischer Form über die Optionen **Jetzt exportieren** oder **Export planen** unter **Sicherheit > Sicherheitsverletzungen > Alle Verstöße > Verstoßdetails** exportieren, werden nur die in der aktuellen Seitenansicht sichtbaren Datensätze in den Bericht aufgenommen, unabhängig von der Anzahl der Datensätze, die unter **Anzahl der zu exportierenden Datensätze** ausgewählt wurden.

  [NSHELP-37562]

April 10, 2024

Analytics

Integration der Beobachtbarkeit – Unterstützung für die Konfiguration des Exports von NetScaler-Metriken und Auditprotokolle nach Splunk Unter **Einstellungen > Integration der Beobachtbarkeit** können Sie jetzt den Export von NetScaler Metrics und Audit-Logs nach Splunk konfigurieren.

Weitere Informationen finden Sie unter Export von NetScaler-Metriken und Auditprotokollen nach Splunk konfigurieren.

[NSADM-108858]

Infrastruktur

Mit Hostnamen auf die NetScaler-GUI zugreifen Wenn Sie über **Infrastruktur > Instanzen > NetScaler** eine Verbindung zu NetScaler herstellen, wird durch Klicken auf den Hostnamen nun die Verbindung zur NetScaler-GUI über den Hostnamen hergestellt. Zuvor wurde durch Klicken auf den Hostnamen oder die IP-Adresse die Verbindung zur NetScaler-GUI über das NSIP initiiert.

[NSADM-108790]

Diskrepanzen zwischen Hochverfügbarkeitsknoten während des Upgrades anzeigen Sie können jetzt Konfigurationsunterschiede zwischen dem primären Knoten und dem sekundären Knoten anzeigen, während Sie die NetScaler-Hochverfügbarkeitsbereitstellung aktualisieren. Sie können die Unstimmigkeiten überprüfen und entscheiden, ob Sie das Upgrade fortsetzen oder beenden möchten. Um diese Funktion zu verwenden, navigieren Sie zu **Infrastruktur > Upgrade-Jobs** und sehen Sie sich die Abweichungen auf der Registerkarte **Validierung vor dem Upgrade** an.

Weitere Informationen finden Sie unter Upgrade-Jobs.

[NSADM-103826]

Behobene Probleme

Die Probleme, die in Build April 10, 2024 behoben wurden.

Infrastruktur

- Die Seite **Infrastruktur > Ereignisse > Syslog-Meldungen** erscheint leer, wenn die Syslog-Meldungen Sonderzeichen wie hochgestellte Zeichen enthalten.

[NSHELP-37551]

- Die Anzahl der verwendeten und unbenutzten Zertifikate, die unter **Infrastruktur > SSL-Dashboard > Verwendung** angezeigt wird, ist falsch, wenn die SSL-Zertifikate Zertifikatsketten haben.

  [NSHELP-37469, NSADM-106867]

Lizenzierung

- Die Ports 27000 und 7279, die auf dem Agenten für gepoolte oder Flexed-Lizenzen erforderlich sind, sind nach dem Neustart der Agentenprozesse möglicherweise nicht mehr verfügbar. In solchen Szenarien kann es vorkommen, dass die NetScaler-Instanzen, die Pool- oder Flexed-Lizenzen verwenden, in die Kulanzphase übergehen.

  [NSADM-110461]

Sicherheit

- Wenn Sie zu **Sicherheit > WAF-Empfehlung**navigieren, wird möglicherweise die folgende Fehlermeldung angezeigt:

  "**HTTP Error 500 ([object Object]) while accessing the data endpoint: "apps"**"

  [NSHELP-37598]

26. März 2024

Behobene Probleme

Die Probleme, die in Build am 26. März 2024 behoben wurden.

Infrastruktur

- Wenn Sie beim Erstellen oder Aktualisieren eines Upgrade-Jobs versuchen, eine Instanz unter **Infrastruktur > Upgrade-Jobs > Job erstellen > Instanz auswählen > Instanzen hinzufügen** auszuwählen, wird auf der Seite **Instanzen hinzufügen** die Registerkarte **Partitionen** angezeigt, die für den Workflow nicht gilt. Wenn Sie eine Partition auswählen, reagiert die Seite nicht mehr und Sie können nicht fortfahren.

  [NSADM-110118]

- Wenn Sie Slack-Benachrichtigungen unter **Einstellungen > Benachrichtigungen > Slack > Slack-Benachrichtigungen erstellen** erstellen und **Benachrichtigungen mit Anlage auswählen**, werden die Benachrichtigungen nicht angezeigt und die folgende Fehlermeldung wird angezeigt:

  ```
  Invalid token
  ```

  [NSHELP-37313]

StyleBooks

- Wenn die Option **Nur sicherer Zugriff** unter **Einstellungen > Verwaltung > Systemkonfigurationen > Grundeinstellungen** ausgewählt ist und Sie versuchen, einen Geräte-API-Proxyvorgang auszuführen, schlägt der Vorgang fehl.

  [NSHELP-37368]

12. März 2024

Lizenzierung

Unterstützung für die manuelle Auswahl eines NetScaler Agents als LSA im NetScaler Console Service Sie können jetzt manuell einen NetScaler Agent als Lizenzserver-Agent (LSA) für die NetScaler Pooled- oder NetScaler Flexed-Lizenzierung auswählen.

Wenn ein LSA ausgefallen ist, wartet der NetScaler Console-Dienst 24 Stunden, bevor er automatisch den nächsten LSA auswählt. Der Administrator kann den neuen LSA in der Zwischenzeit mit diesem Feature manuell auswählen. Der Administrator muss jedoch sicherstellen, dass der Status des ausgewählten neuen LSA **AKTIV** und sein Diagnosestatus **OK** ist.

Weitere Informationen finden Sie unter Verhalten des NetScaler Agents bei Flexed- oder gepoolter Lizenzierung.

[NSADM-105168]

Behobene Probleme

Die Probleme, die in Build am 12. März 2024 behoben wurden.

Analytics

- Wenn Sie **Gateway Insight** für die virtuellen Gateway-Server aktivieren, wird in der Spalte **Analytics-Status** unter **Einstellungen > Analytics-Konfiguration > Alle virtuellen Server Deaktiviert** angezeigt.

[NSHELP-37400]

- Unter **Gateway > Gateway Insight** werden auf der Registerkarte **Authentifizierung** keine Benutzerdetails für die fehlgeschlagenen Authentifizierungen angezeigt.

  [NSHELP-37465]

Infrastruktur

- Wenn eine benutzerdefinierte Richtlinie erstellt und ein Benutzer zu dieser Richtlinie hinzugefügt wird, treten bei GET-API-Anfragen für bestimmte Ressourcen Berechtigungsprobleme auf und der folgende Fehler wird angezeigt:

  "Nicht autorisiert, da die erforderlichen Berechtigungen nicht erteilt wurden."

  [NSHELP-37331]

28. Februar 2024

Infrastruktur

Aktualisierungen der VIP-Lizenzierung und des NetScaler Console Service-Speichers

- **Unbegrenzte Anzahl von VIPs im NetScaler Console-Dienst**: Ab NetScaler Console Service Release 14.1-21.x wurde das Konzept der lizenzierten VIPs entfernt. Eine unbegrenzte Anzahl von VIPs ist jetzt im NetScaler Console-Dienst verfügbar. Sie müssen keine virtuellen NetScaler Console-Serverlizenzen mehr erwerben, da die VIP-Lizenz-SKU in Kürze End of Sale (EOS) & End of Renewal (EOR) lauten wird.
- **NetScaler Console-Dienstspeicher**:
  - Die NetScaler Console Service Storage-SKU wird in Kürze "End of Sale"(EOS) und "End of Renewal"(EOR) lauten.
  - Die Standardspeicherberechtigung für den NetScaler Console-Dienst beträgt jetzt 5 GB.
  - Alle in der Vergangenheit gekauften NetScaler Console Service Storage-Lizenzen werden bis zum Ende der Laufzeit eingelöst.
  - Alle NetScaler Console VIP-Lizenzen, die Sie in der Vergangenheit erworben haben und die Sie zu einem anteiligen Anspruch auf NetScaler Console Service-Speicher berechtigen, werden bis zum Ende der Laufzeit eingelöst.
  - Wenn Sie ein anderes Lizenzpaket erwerben, das Sie zu einer höheren NetScaler Console-Speicherberechtigung berechtigt, werden die standardmäßigen 5 GB entsprechend der Berechtigung geändert.

[NSADM-108300]

Aktualisierungen des Analytics- und Metrik-Collectors

- Mit unbegrenzter VIPs-Unterstützung ab 14.1 21.x Build werden alle vorhandenen und neuen virtuellen Server jetzt automatisch lizenziert. Sie können Analysen auf den virtuellen Servern aktivieren, ohne sie explizit zu lizenzieren.
- Metrics Collector ist jetzt standardmäßig für alle NetScaler-Lizenztypen in den neuen NetScaler-Instanzen deaktiviert, die in NetScaler Console ab 14.1 21.x Build hinzugefügt wurden. Die Konfiguration des Metrik-Collectors für die vorhandenen verwalteten Instanzen bleibt unverändert.

[NSADM-108803]

Analytics

Aktionsrichtlinien – Benachrichtigungen für die Anwendungsnutzung konfigurieren Unter Aktionsrichtlinien (**Einstellungen > Aktionen > Aktionsrichtlinien**) können Sie jetzt eine Aktionsrichtlinie für die Anwendungsnutzung konfigurieren und die Optionen **Anforderungen pro Sekunde**, **Durchsatz**und **Datenvolumen** auswählen. Mit diesen Optionen können Sie Benachrichtigungen für durchschnittliche Anforderungen pro Sekunde, Anomalien pro Sekunde, Durchsatzdurchschnitt, Durchsatzanomalien, Gesamtdatenvolumen und Datenvolumenanomalien konfigurieren und empfangen. Weitere Informationen finden Sie unter Konfigurieren einer Aktionsrichtlinie für den Empfang von Benachrichtigungen über Anwendungsereignisse.

[NSADM-104833]

Integration der Beobachtbarkeit Der Konfigurationsworkflow für die Integration mit Splunk und New Relic wurde für eine bessere Benutzererfahrung verbessert und ist unter **Settings > Observability Integration** verfügbar. Zuvor war der Konfigurationsworkflow für die Integration mit Splunk und New Relic unter **Settings > Ecosystem Integration** verfügbar.

Weitere Informationen finden Sie unter Observability Integration.

[NSADM-104702]

Observability Integration – Unterstützung für die Konfiguration des Exports von NetScaler-Metriken nach Prometheus Unter **Settings > Observability Integrations** können Sie jetzt den Export von NetScaler-Metriken nach Prometheus konfigurieren, indem Sie das Standardschema auswählen.

Weitere Informationen finden Sie unter Prometheus Integration und Observability Integration.

[NSADM-101426]

Gateway Insight – Verbesserungen beim Exportieren von Berichten Unter **Gateway > Gateway Insight**können Sie jetzt Berichte nur mit den ausgewählten Optionen exportieren, indem Sie das Einstellungssymbol in allen Tabellen unter jeder Metrik verwenden (EPA, Authentifizierung, Autorisierungsfehler, SSO und Anwendungsstart). Zuvor wurden im exportierten Bericht alle Informationen unabhängig von den ausgewählten Optionen angezeigt.

[NSADM-96821]

StyleBooks

Aktualisierungen der Standard-StyleBooks Standard-StyleBooks, die auf der NetScaler-Version 10.5 basieren, werden in kommenden Versionen veraltet sein. Ein neuer Satz von Standard-StyleBooks ist jetzt unter **Applications > Configuration > StyleBooks > Default StyleBooks**verfügbar, basierend auf NetScaler Version 13.0.

[NSADM-105513]

Option zum Klonen eines StyleBook NetScaler Console ermöglicht es Administratoren jetzt, ein Duplikat eines StyleBook zusammen mit ihren Abhängigkeiten zu erstellen. Administratoren können dieses Paket dann für zusätzliche Anpassungen wie das Aktualisieren von `parameters` und `components`verwenden.

Um diese Funktion zu verwenden, navigieren Sie zu **Anwendungen > Konfiguration > Stylebooks**, wählen Sie ein standardmäßiges oder benutzerdefiniertes StyleBook aus und klicken Sie auf **Clone**.

Weitere Informationen finden Sie unter StyleBook klonen.

[NSADM-92376]

Behobene Probleme

Die Probleme, die in Build am 28. Februar 2024 behoben wurden.

Infrastruktur

- Die Migration von NetScaler Console zum NetScaler Console-Dienst schlägt fehl und bestimmte Azure Active Directory-Gruppen sind im NetScaler Console-Dienst nicht verfügbar. Dieses Problem tritt auf, weil in den Azure Active Directory-Gruppennamen, die in NetScaler Console erstellt wurden, Leerzeichen enthalten.

  [NSHELP-37006]

- Benutzer können nicht auf NetScaler Console zugreifen, wenn sie mehreren Azure Active Directory-Gruppen angehören.

  [NSHELP-37005]

- In **Web Insight** und **Security Violations** wurde der Workflow für den Schedule-Export in der GUI verbessert, um die Benutzererfahrung zu verbessern.

  [NSADM-106624]

- Unter **Infrastruktur > Netzwerkberichterstattung** enthält der tabellarische Exportbericht keine Details wie Dienst, Dienstgruppe, virtueller Server und Schnittstellenname.

  [NSHELP-37224]

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

  [NSADM-106497]

06. Februar 2024

Analytics

App-Dashboard – Unterstützung zum Anzeigen von Anwendungsmetriken aus der NetScaler Admin-Partition Im **App Dashboard** können Sie jetzt Metrikdetails für Anwendungen anzeigen, die aus den NetScaler Admin-Partitionen erstellt wurden. Bisher konnten Sie nur Anwendungen von den Admin-Partitionen ohne Metriken anzeigen.

[NSADM-105343]

Infrastruktur

Umbenennung von NetScaler ADM in Citrix Cloud Ab Build 14.1 16.x wurde der NetScaler ADM Service in NetScaler Console Service umbenannt. In Fortsetzung wird Application Delivery Management jetzt an den folgenden Stellen in NetScaler Console umbenannt:

- Die Kachel unter **Meine Dienste** auf der Citrix Cloud-Startseite.
- Der Dienstname im **Citrix Cloud-Menü > Meine Dienste**.
- Der Produktname im Workflow Administrator hinzufügen unter **Zugriff einrichten > Benutzerdefinierter Zugriff** aus dem **Citrix Cloud-Menü > Identitäts- und Zugriffsmanagement > Administratoren > Administrator/Gruppe hinzufügen**.

Standardvalidierungsskripten in Upgrade-Aufträgen ausführen NetScaler Console enthält jetzt eine Option für Standard-Validierungsskripts im Upgrade-Job-Workflow. Diese Standardskripts werden sowohl vor als auch nach einem Upgrade-Job ausgeführt und generieren einen Diff-Bericht. Sie haben weiterhin die Möglichkeit, benutzerdefinierte Standardskripts auszuführen.

Weitere Informationen finden Sie unter Upgrade von NetScaler-Instanzen.

[NSADM-100803]

Bereitstellung von Radarobjekt für NetScaler Console Sites automatisieren NetScaler unterstützt die Automatisierung der Bereitstellung von Radarobjekten für NetScaler Console-Sites, sodass keine manuelle Bereitstellung auf den NetScaler-Instanzen erforderlich ist.

Diese Erweiterung ist nur verfügbar, wenn Sie eine NetScaler-Instanz bearbeiten, und sie gilt nur für den Standorttyp **Rechenzentrum** (mit dem Typ **Privat**) oder **Branch.**

Wenn Sie in der Liste **Real User Measurements** die Option **Auf NetScaler bereitstellen** auswählen, wird die Liste der **NetScaler-Instanzen** automatisch gefüllt, sodass Sie die spezifische Instanz für die Bereitstellung des Radarobjekts (r20.png) auswählen können.

Weitere Informationen finden Sie unter Bereitstellung von Radarobjekt automatisieren.

[NSADM-104691]

Behobene Probleme

Folgende Probleme wurden im Build vom 06. Februar 2024 behoben.

Analytics

- Der **XML-SQL-Angriff** wird nicht sowohl im Sicherheits-Dashboard (**Sicherheit > Sicherheits-Dashboard**) als auch im Dashboard für Sicherheitsverletzungen (**Sicherheit > Sicherheitsverletzungen**) gemeldet.

  [NSHELP-37159]

Lizenzierung

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

  [NSADM-106497]

Verwaltung und Überwachung

- Wenn ein Konfigurationsjob erstellt wird, wird der Status unter **Infrastruktur > Konfiguration > Jobs** als **Abgeschlossen** angezeigt, aber unter **Details > Ausführungsübersicht** wird “0% abgeschlossen”angezeigt.

  [NSHELP-37176]

- Ein zweistufiger Upgrade-Jobstatus für eine NetScaler HA zeigt “Geplant”an, obwohl das NetScaler HA-Upgrade abgeschlossen ist. Der primäre Knoten wird als abgeschlossen angezeigt (**Status Phase 1: Abgeschlossen)**, während der sekundäre Knoten als geplant (**Phase 2: Geplant**) angezeigt wird.

  [NSHELP-36943]

- Wenn eine Konfigurationsüberwachungsvorlage mit Sonderzeichen im Namen unter **Infrastruktur > Konfiguration > Konfigurationsüberprüfung > Auditvorlagen > Hinzufügen** erstellt wird, wird die Vorlage erfolgreich generiert. Während der Abfrage kann jedoch kein Differenzbericht für die Vorlage im **Configuration Audit-Dashboard** generiert werden.

  Dieses Problem tritt auf, wenn andere Sonderzeichen als - (Bindestrich) und ‘_’(Unterstrich) verwendet werden.

  [NSHELP-36438]

24. Januar 2024

Analytics

Details zur Upgradeempfehlung unter Aufgaben anzeigen Unter **Aufgaben** können Sie jetzt die umsetzbare Aufgabe der **Upgrade Advisory** anzeigen. Wenn Ihre NetScaler-Instanzen das Ende der Nutzungsdauer (EOL) oder das Ende der Wartung (EOM) bereits innerhalb von 90 Tagen erreicht haben oder kurz davor stehen, das Ende der Wartung (EOM) erreicht zu haben, zeigt die **Upgrade Advisory-Aufgabe** auf der Grundlage Ihrer aktuellen Auslastung die Details dieser Instances an. Sie können auf **Take Action** klicken und diese Instanzen auf einen empfohlenen Build aktualisieren.

[NSADM-104715]

Infrastruktur

Verbesserte Berechtigungen für schreibgeschützte Benutzer Benutzer mit Leseberechtigungen für die folgenden Funktionen können jetzt NetScaler-Instanzen abfragen:

- SSL-Zertifikate (**Infrastruktur > SSL-Dashboard > Jetzt abfragen**)
- Netzwerkfunktionen (**Infrastruktur > Netzwerkfunktionen > Jetzt abfragen**)

- Konfigurationsaudits (**Infrastruktur > Konfiguration > Konfigurationsüberprüfung > Jetzt abfragen**)

[NSADM-104710]

Behobene Probleme

Die Probleme, die in Build am 24. Januar 2024 behoben wurden.

- Bei der integrierten Agentregistrierung in NetScaler SDX wird eine Erfolgsmeldung angezeigt, die SDX-Instanz wird jedoch nicht unter **Infrastruktur > Instanzen-Dashboard** angezeigt.

  [NSHELP-37137, NSHELP-37128]

- Unter **Infrastruktur > Netzwerkfunktionen > Load Balancing** gibt die Registerkarte **Server** die Anzahl der Server an, es werden jedoch keine Tabelleneinträge für Benutzer angezeigt, die keine Standardbenutzer sind.

  [NSHELP-36964]

16. Januar 2024

Unterstützung bei der Identifizierung und Behebung von CVE-2023-6548 und CVE-2023-6549

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2023-6548 und CVE-2023-6549.

- Für die Identifizierung von CVE-2023-6548 ist ein Versionsscan erforderlich.
- Die Identifizierung für CVE-2023-6549 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.

> **Hinweis:**
>
> Es kann einige Stunden dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2023-6548 und CVE-2023-6549 im Sicherheitsberatungsmodul reflektiert werden. Um die Auswirkungen früher zu erkennen, können Sie einen Anforderungsscan starten, indem Sie auf **Jetzt scannen**klicken.

[NSADM-104763]

09. Januar 2024

Analytics

Unterstützung, um ein benutzerdefiniertes Dashboard mit anderen Benutzern zu teilen Als Administrator können Sie das benutzerdefinierte Dashboard jetzt mit anderen Benutzern teilen. Wählen Sie unter **Übersicht > Benutzerdefiniertes Dashboard** ein Dashboard aus und klicken Sie auf **Teilen**. Geben Sie den Nutzernamen ein und klicken Sie auf **Einladen**, um das Dashboard zu teilen. Die zugewiesenen Benutzer können das Dashboard im schreibgeschützten Modus anzeigen.

[NSADM-100879]

Infrastruktur

ITM Radar in NetScaler Console Sites konfigurieren Das ITM Radar verbessert die Netzwerküberwachungsfunktionen. Die in Rechenzentren, virtuellen Maschinen oder Cloud-Anbietern bereitgestellten Websites können jetzt das Radarobjekt (r20.png) hosten und so Einblicke in Leistungskennzahlen bieten. Das ITM-Radar-Objekt sammelt aktiv wertvolle Anwendungsstatistiken für Endbenutzer und versorgt die Standorte mit robuster ITM-Radartelemetrie für eine effektivere Netzwerküberwachung und fundierte Verkehrsmanagemententscheidungen.

Weitere Informationen finden Sie unter ITM-Radar konfigurieren.

[NSADM-91686]

Gateway-Insights in Splunk und New Relic anzeigen Wenn Sie unter **Einstellungen > Ökosystemintegration ein neues Abonnement für die Integration** des NetScaler Console-Dienstes mit Splunk und New Relic erstellen, können Sie jetzt die Option **Gateway Insights** auswählen. Nachdem Sie das Abonnement mit der Option **Gateway Insights** konfiguriert haben, können Sie die Gateway-Insights -Daten in Splunk und New Relic einsehen.

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

[NSADM-101036]

Exportieren Sie SSL-Daten sofort nach Splunk und New Relic Die SSL-Daten werden jetzt sofort nach Splunk und New Relic exportiert, nachdem ein Administrator ein Abonnement erstellt hat, indem er **SSL Certificate Insight** in Splunk und New Relic auswählt. Zuvor mussten die Admins auf **Jetzt abfragen** (**Infrastruktur > SSL-Dashboard**) klicken, um die Daten zum ersten Mal zu exportieren.

[NSADM-101035]

Details zur Upgradeempfehlung unter Aufgaben anzeigen Unter **Aufgaben** können Sie jetzt die umsetzbare Aufgabe der **Upgrade Advisory** anzeigen. Wenn Ihre NetScaler-Instanzen das Ende der Nutzungsdauer (EOL) oder das Ende der Wartung (EOM) bereits innerhalb von 90 Tagen erreicht haben oder kurz davor stehen, das Ende der Wartung (EOM) erreicht zu haben, zeigt die Upgrade Advisory-Aufgabe auf der Grundlage Ihrer aktuellen Auslastung die Details dieser Instances an. Sie können auf **Take Action** klicken und diese Instanzen auf einen empfohlenen Build aktualisieren.

[NSADM-104715]

Aktionsrichtlinie – Konfigurieren Sie Benachrichtigungen für Anfragen, Bandbreite und Antwortzeit Wenn Sie unter **Aktionsrichtlinien** (**Einstellungen > Aktionen > Aktionsrichtlinien**) eine Aktionsrichtlinie unter Anwendungsleistung konfigurieren, können Sie jetzt die Optionen **Anforderungen**, **Bandbreite** und **Antwortzeit** auswählen. Mit diesen Optionen können Sie Benachrichtigungen für die Gesamtzahl der Anfragen, die Gesamtbandbreite, die durchschnittliche Antwortzeit und Anomalien bei der Antwortzeit konfigurieren und empfangen. Weitere Informationen finden Sie unter Konfigurieren einer Aktionsrichtlinie für den Empfang von Benachrichtigungen über Anwendungsereignisse.

Darüber hinaus können Sie jetzt auch eine Aktionsrichtlinie aus dem Grafiktrend in **Web Insight** für diese Metriken konfigurieren. Wenn Sie als Administrator ein ungewöhnliches Verkehrsmuster oder einen plötzlichen Anstieg dieser Metriken für eine Anwendung feststellen, können Sie mit dieser Erweiterung eine Richtlinie für relative Aktionen erstellen, indem Sie auf **Aktionsrichtlinie erstellen** klicken, nachdem Sie sie an einem bestimmten Punkt im Diagramm platziert haben.

[NSADM-101273]

Behobene Probleme

Im Build vom 9. Januar 2024 wurden folgende Probleme behoben.

Lizenzierung

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

  [NSADM-106665]

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

  [NSADM-106561]

- Unter **NetScaler Licensing > License Management** funktioniert die Konfiguration für die Schwellenwertüberschreitung per E-Mail-Benachrichtigung nicht wie erwartet.

  [NSHELP-36895]

13. Dezember 2023

Infrastruktur

Umbenennung des NetScaler ADM Service NetScaler Application Delivery Management Service (ADM Service) wurde jetzt in NetScaler Console Service umbenannt.

Andere Terminologien, die umbenannt wurden, lauten wie folgt:

- ADM Agent wird jetzt in NetScaler Agent umbenannt
- ADM Service Connect wurde jetzt in Console Advisory Connect umbenannt

> **Hinweis:**
>
> Die Benutzeroberfläche und die Dokumentation unseres NetScaler Console-Serviceprodukts werden derzeit aktualisiert, um diesen Änderungen Rechnung zu tragen. Während dieser Zeit stoßen Sie möglicherweise auf frühere und umbenannte Namen, auf die synonym verwiesen wird. Wir danken Ihnen für Ihr Verständnis während dieses Übergangs.

[NSADM-105125]

Lizenzierung

NetScaler Flexed-Lizenzierung NetScaler Flexed 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 auf den NetScaler Console-Dienst oder NetScaler ADM on-premises 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 on-premises bereitgestellt werden.

> **Hinweis:**
>
> Stellen Sie sicher, dass auf Ihren NetScaler Agents Version 16.x oder höher ausgeführt wird.

Weitere Informationen finden Sie unter Flexed-Lizenz .

[NSADM-98483]

Analytics

Flexed-Lizenz – Metrics Collector ist standardmäßig für die neuen NetScaler-Instanzen deaktiviert, die in der NetScaler Console hinzugefügt wurden Wenn Sie die Flexed-Lizenz verwenden, ist der Metrics Collector jetzt standardmäßig für die neuen NetScaler-Instanzen deaktiviert, die in der NetScaler Console hinzugefügt wurden. Sie müssen diese Option manuell aktivieren, um die NetScaler-Metriken und Zählerdaten an die Konsole zu übertragen. Die Konfiguration des Metrik-Collectors für die vorhandenen verwalteten Instanzen bleibt unverändert.

> **Hinweis:**
>
> Der Metrics Collector muss aktiviert sein, damit die Daten im Anwendungs-Dashboard und den zugehörigen Registerkarten wie Performance, SSL und Key Metrics für alle lizenzierten virtuellen Server auf dieser Instanz angezeigt werden.

Weitere Informationen finden Sie unter Konfigurieren von Intelligent App Analytics.

[NSADM-106193]

Die Video- und TCP-Insight-Funktionen sind veraltet Mit der neuesten Version sind **Video Insight** - und **TCP Insight**-Berichtsdaten nicht mehr für die Visualisierung in der NetScaler Console verfügbar.

[NSADM-106597]

Infrastruktur

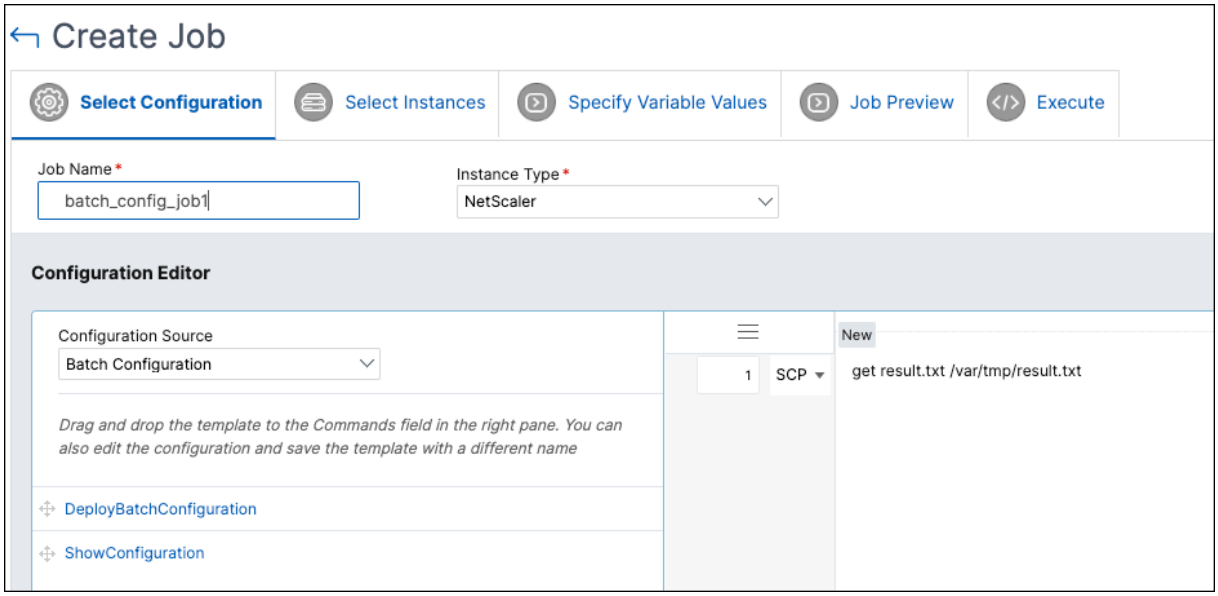
Laden Sie Dateien für Batch-Konfigurationsaufträge herunter Mit den Konfigurationsjobs können Sie jetzt mithilfe der NetScaler ADM-GUI Dateien aus einem Verzeichnis auf einer NetScaler-Instanz in ein Verzeichnis auf Ihrem lokalen Computer herunterladen.

Um diese Funktion zu verwenden, navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsaufträge , wählen Sie einen Job aus und klicken Sie auf Ergebnisdateien herunterladen** .**

Die Schaltfläche Ergebnisdateien herunterladen ist nur verfügbar, wenn die folgenden Bedingungen erfüllt sind:

- Der Konfigurationsauftrag, der erstellt wird, ist ein Batch-Konfigurationsauftrag. Um einen Batch-Konfigurationsauftrag zu erstellen, gehen Sie zu **Auftrag erstellen > Konfiguration auswählen** und wählen Sie i**m Konfigurationseditor Konfigurationsquelle > Batch-Konfiguration** aus**
- Ein `scp get`Befehl wird im Konfigurationseditor **verwendet**

Für mehrere NetScaler-Instanzen sind die heruntergeladenen Ergebnisdateien in separaten Ordnern verfügbar, die jeweils einer einzelnen Instanz entsprechen.



[NSADM-105442]

Einen geplanten Upgrade-Job anhalten und fortsetzen NetScaler ADM bietet jetzt die Option, Ihren geplanten Upgrade-Job anzuhalten. Um diese Funktion zu verwenden, navigieren Sie zu **Infrastruktur > Upgrade-Jobs** , wählen Sie einen vorhandenen geplanten Upgrade-Job aus und klicken Sie auf **Stopp** , um den Job anzuhalten. Um den geplanten Upgrade-Job fortzusetzen, klicken Sie auf **Fortsetzen** .

> **Hinweis:**
>
> Wenn die geplante Zeit für den Upgrade-Job abgelaufen ist, nachdem Sie beschlossen haben, ihn fortzusetzen, müssen Sie den Upgrade-Job erneut erstellen.

Weitere Informationen finden Sie unter Upgrade-Jobs

[NSADM-100807, NSADM-97280]

Behobene Probleme

Die Probleme, die in Build am 13. Dezember 2023 behoben wurden.

Analytics

- Unter **Anwendungen > Dashboard** werden beim Export von Transaktionsprotokolldaten in das Tabellen- oder CSV-Format keine Daten angezeigt. Dieses Problem tritt auf, wenn NetScaler ADM mit Nicht-UTC-Zeitzonen konfiguriert ist.

  [NSHELP-36817]

- Unter Sicherheit > Sicherheitsverstöße > Verstoßdetails erkennt der Suchfilter die "Client-IP! =" Abfrage.**

  [NSHELP-36675]

- Geplante Snapshot-Berichte, die unter **Sicherheit > Sicherheitsverletzungen > Berichte exportieren > Export planen** mit dem als JPEG ausgewählten Dateiformat exportiert wurden, zeigen den folgenden Fehler an:

  "Please provide query parameters in the report context or csv_export_arr."

  [NSHELP-36657]

Infrastruktur

- Bestimmte Benutzer sehen auf den Karten auf der Seite **Infrastruktur > Instanzen** das Wasserzeichen "Nur für Entwicklungszwecke".

  [NSHELP-36863]

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]

Sicherheit

- Nach der Konfiguration der Schutzmaßnahmen im Unified **Security Dashboard (Sicherheit > Security Dashboard > Anwendung verwalten**) werden die Schutzmaßnahmen nicht auf dem virtuellen Content Switching-Server bereitgestellt.

  [NSADM-105544]

29. November 2023

Infrastruktur

Verwenden Sie Tags, um Instanzen für Benutzergruppen zu autorisieren Als Administrator können Sie jetzt Benutzer anhand der zugehörigen Tags für bestimmte Instanzen autorisieren. Navigieren Sie beim Erstellen von Benutzergruppen zu **Einstellungen > Benutzer und Rollen > Hinzufügen > Autorisierungseinstellungen > Tags auswählen** und autorisieren Sie dann Benutzer anhand von Stichwörtern für Instanzen.

Weitere Informationen finden Sie unter Konfiguration der rollenbasierten Zugriffskontrolle.

[NSADM-104798]

Behobene Probleme

Die Probleme, die in Build vom 29. November 2023 behoben wurden.

- 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]

09. November 2023

Analytics

Gateway-Sitzungstimeout konfigurieren Unter **Einstellungen > Analytics-Einstellungen > ICA/Gateway-Sitzungstimeout konfigurieren**können Sie jetzt eine Timeout-Sitzung für Gateway Insight konfigurieren. Standardmäßig ist der Wert 30 Minuten. Wenn NetScaler ADM bei dieser Konfiguration innerhalb der konfigurierten Dauer keinen Sitzungsbeendigungsdatensatz empfängt, wird die Sitzung als beendet aufgezeichnet.

[NSADM-101271]

Update im NetScaler-Backup-Prozess und Firewallzugriff NetScaler-Instanz-Backups werden jetzt direkt vom NetScaler Agent zum NetScaler ADM Service und dann zu Amazon S3 hochgeladen. Sie müssen also den Zugriff auf S3-URLs in Ihrer Firewall für den NetScaler-Backup-Service nicht mehr zulassen.

[NSADM-98267]

Unterstützung für intelligentes Verkehrsmanagement Der NetScaler ADM Service unterstützt jetzt intelligentes Verkehrsmanagement, das Ihnen hilft, das Benutzererlebnis zu verbessern, indem der Internetverkehr in Echtzeit analysiert und Ihr Datenverkehr automatisch an die optimalen Standorte gelenkt wird.

Intelligentes Verkehrsmanagement ermöglicht Ihnen:

- Stellen Sie Anwendungen an mehreren Standorten bereit, um die Reaktionszeit der Anwendungen zu verkürzen und die Anwendungsverfügbarkeit auf der Grundlage von Servicedaten in Echtzeit zu maximieren.
- Konfigurieren Sie das autoritative DNS für die Verwaltung Ihrer Zonen.
- Sehen Sie sich Einblicke in die Rechenzentren oder Bereitstellungsplattformen und Anwendungen der Kunden an.
- Identifizieren Sie die besten Plattformen und Standorte.

Klicken Sie im linken Navigationsbereich auf **Intelligent Traffic Management**, um loszulegen. Weitere Informationen finden Sie unter Intelligentes Verkehrsmanagement.

[NSADM-91677]

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]

Behobene Probleme

Die Probleme, die in Build vom 09. November 2023 behoben wurden.

Infrastruktur

- Beim Einrichten des integrierten NetScaler-Agents zur Verwaltung von Instanzen bleibt die Konfiguration auf der Seite **Instanzen hinzufügen** hängen, obwohl die Registrierung erfolgreich ist und der Agent auf der Seite **Instanz-Dashboard** angezeigt werden kann.

  [NSHELP-36614]

StyleBooks

- 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 Fehler für unvollständige Konfigurationen, die auf Sonderzeichen in der Configpack-Definition zurückzuführen sind, korrekt an.

  [NSADM-104423]

25. Oktober 2023

Analytics

Benutzerdefinierte Dashboards ertellen, um die wichtigsten Kennzahldetails der Instanz anzuzeigen Ähnlich wie beim vereinheitlichten Dashboard (**Übersicht > Dashboard**) können Sie jetzt die Metrikdetails Ihrer Instanz nach Ihrer Wahl anzeigen, indem Sie benutzerdefinierte Dashboards erstellen. Wenn Sie beispielsweise die wichtigsten Kennzahlen für Anwendungen und Anwendungssicherheit überwachen möchten, können Sie ein benutzerdefiniertes Dashboard erstellen, indem Sie nur diese beiden Kategorien auswählen. Sie können bis zu 20 Dashboards erstellen, indem Sie für jedes Dashboard einen eindeutigen Namen verwenden. Als Administrator können Sie mit dieser Erweiterung mehrere Dashboards erstellen und nur die erforderlichen Instanzinformationen überwachen.

Um loszulegen, navigieren Sie zu **Übersicht > Benutzerdefiniertes Dashboard**.

Weitere Informationen finden Sie unter Benutzerdefinierte Dashboards erstellen, um die wichtigsten Kennzahldetails der Instanz anzuzeigen.

[NSADM-91875]

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. Sie können diese umsetzbaren Aufgaben auch basierend auf dem Schweregrad der Probleme (Kritisch und Mittel) anzeigen.
- 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.

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.

[NSADM-101303]

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]

Behobene Probleme

Die Probleme, die in Build vom 25. Oktober 2023 behoben wurden.

- 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]

10. Oktober 2023

Verwaltung und Überwachung

Unterstützung bei der Identifizierung und Behebung von CVE-2023-4966 und CVE-2023-4967
Die NetScaler Console 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]

26. September 2023

Analytics

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 die NetScaler-Instanzen auswählen. Wenn Sie ein Abonnement mit bestimmten Instanzen erstellen, werden die Daten nur von den ausgewählten NetScaler-Instanzen nach Splunk und New Relic exportiert.

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

[NSADM-94371]

Infrastruktur

On-premises ADM-Instanzen, die mithilfe von Cloud Connector mit dem ADM Service verbunden sind In den **Einstellungen**können Sie jetzt eine neue Option namens **ADM On-Prem**anzeigen.

Auf dieser Seite können Sie Details der on-premises ADM-Instanzen anzeigen, die über ADM On-Prem Cloud Connector mit dem ADM-Dienstmandanten verbunden sind.

Weitere Informationen finden Sie unter On-premises ADM-Instanzen, die mithilfe von Cloud Connector mit dem ADM Service verbunden sind.

[NSADM-94576]

Behobene Probleme

Die Probleme, die in Build vom 26. September 2023 behoben wurden.

Analytics

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

  [NSHELP-36184]

13. September 2023

Infrastruktur

Authentifizierungstoken zum Hochladen des Pakets für technischen Support Sie benötigen jetzt ein Authentifizierungstoken, um das auf Ihrem NetScaler generierte Paket für den technischen Support auf den Server für den technischen Support von Citrix hochzuladen. Zuvor haben Sie das Paket für den technischen Support mit dem Citrix-Benutzernamen und -Kennwort hochgeladen. Weitere Informationen finden Sie unter So generieren Sie ein technisches Support-Paket für eine NetScaler-Instanz.

[NSADM-93351]

Behobene Probleme

Die Probleme, die in Build vom 13. September 2023 behoben wurden.

Analytics

- Wenn NetScaler Console 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**zeigt die X-Achse des Diagramms Datum statt Uhrzeit an.

  [NSHELP-36043]

Verwaltung und Überwachung

- Berichte, die aus **Infrastruktur > Netzwerkberichterstattung > Export** exportiert wurden, werden gekürzt oder unvollständig angezeigt.

  [NSHELP-36252]

- Azure Active Directory (AD) -Benutzer, die vielen Azure-Gruppen angehören, können nicht auf NetScaler Console zugreifen, selbst wenn die AD-Gruppen ADM-Gruppen zugeordnet sind.

  [NSHELP-35456]

31. August 2023

Infrastruktur

Rufen Sie die Seite mit dem Zertifikatsspeicher unter SSL-Dashboard auf Sie können jetzt zu **Infrastruktur > SSL-Dashboard > Zertifikatsspeicher** navigieren, um die Seite mit dem **Zertifikatsspeicher** aufzurufen.

[NSADM-97858]

Unterstützung der SNMP-Funktionalität für die Agents Unter **Infrastruktur > Agents > Aktionen > SNMP verwalten** können Sie jetzt SNMP-Manager, SNMP-Benutzer und SNMP-Ansichten für Agents erstellen.

Weitere Informationen zu SNMP-Managern und Benutzern finden Sie unter Erstellen von SNMP-Managern und Benutzern für den NetScaler ADM Agent.

[NSADM-94923]

Verbesserungen der Benutzererfahrung und der Funktionalität des Data Storage Management-Dashboards Um die Benutzererfahrung zu verbessern und die Datenspeicherverwaltung effizienter zu gestalten, sind jetzt die folgenden Verbesserungen für das **Data Storage Management-Dashboard** verfügbar:

- Neues UI-Design für das Dashboard:

  - Die Kacheln **Data Ingestion**, **Storage Consumption**, **Data Pruning** und **Actions** wurden hinzugefügt
  - Die Kachel **Actions** bietet Optionen, um mehr Speicherplatz hinzuzufügen, die Datenaufbewahrungsrichtlinie zu überprüfen, Daten zu bereinigen und Ihre Systembenachrichtigungen zu überprüfen

- Suchfunktionen im Bereich **Speicherverbrauchstrends**:

  Sie können jetzt nicht nur die Speichertrends anzeigen, sondern auch nach bestimmten Funktionen und Trends suchen.

- Führen Sie eine Datenbereinigung durch:
  - Sie können jetzt eine oder mehrere Funktionen auswählen und deren Daten bereinigen, um Speicherplatz freizugeben
  - Sie haben Anspruch auf 10 Datenbereinigt pro Monat

Weitere Informationen zum Datenspeichermanagement-Dashboard finden Sie unter Datenspeicherverwaltung.

[NSADM-93202]

Sicherheit

API Gateway wurde in API Security umbenannt **API Gateway** wurde jetzt in **API Security** umbenannt. Sie können die Änderungen auf den folgenden Seiten einsehen:

- **Sicherheit > API-Sicherheit**
- **Sicherheit > API-Sicherheit > API-Analyse > Hilfe anfordern > API-Sicherheitsdokumente**
- **Einstellungen > Benutzer und Rollen > Gruppen > Autorisierungseinstellungen > API-Sicherheit**
- **Einstellungen > Benutzer und Rollen > Zugriffsrichtlinien > Berechtigungen > Sicherheit > API-Sicherheit**

[NSADM-102384]

Behobene Probleme

Die Probleme, die in Build am 31. August 2023 behoben wurden.

Verwaltung und Überwachung

- Unter **Infrastruktur > Network Reporting** zeigt das Network Reporting-Dashboard keine historischen Daten in den Berichten der virtuellen Server an. Dieses Problem tritt auf, wenn Sie beim Erstellen des Dashboards in Select **Entities ein NetScaler HA-Paar auswählen** .

[NSHELP-36228]

11. August 2023

Verwaltung und Überwachung

Sicherheitsempfehlung – Überwachung der Dateiintegrität Mit der NetScaler Console Security Advisory können Sie jetzt die NetScaler-Build-Dateien scannen und die Ergebnisse aller Änderungen oder Ergänzungen der ursprünglichen NetScaler-Builddateien anzeigen.

In der Sicherheitsempfehlung (**Infrastruktur > Instanzberatung > Sicherheitsempfehlung**) können Sie mit der Option **Jetzt scannen** die Optionen **CVEs scannen**, **Dateien scannen**oder **Beide scannen** auswählen. Nachdem Sie "**Dateien scannen** "oder "**Beide scannen** "ausgewählt haben, vergleicht NetScaler Console den Binär-Hash für verwaltete NetScaler-Builddateien mit den ursprünglichen binären Hashwerten und hebt auf der Registerkarte "Überwachung der Dateiintegrität"hervor, ob Dateiänderungen oder Dateierweiterungen vorliegen. **

Die Scanergebnisse zeigen die NetScaler-Instanzen, die potenzielle Änderungen an den Originaldateien und/oder andere Dateiergänzungen aufweisen. Für weitere Untersuchungen zu den Scanergebnissen können Sie sich an die digitale Forensik Ihres Unternehmens wenden.

Weitere Informationen finden Sie unter Sicherheitsempfehlung.

[NSADM-91856]

09. August 2023

Infrastruktur

Details zur Virtualisierungsplattform für NetScaler VPX anzeigen Unter **Infrastruktur > Instanzen > NetScaler > VPX** können Sie jetzt die Plattform anzeigen, auf der NetScaler VPX gehostet wird, indem Sie **Einstellungen > Cloud Platform** auswählen.

[NSADM-97319]

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]

Sicherheit

Bestehende API-Definition aktualisieren Unter **Sicherheit > API Gateway > API Discovery** können Sie jetzt eine bestehende API-Definition mit ausgewählten API-Ressourcen aktualisieren.

Weitere Informationen finden Sie unter Vorhandene API-Definition mit erkannten API-Endpunkten aktualisieren.

[NSADM-97433]

Behobene Probleme

Die Probleme, die in Build vom 09. August 2023 behoben werden.

Provisioning

- Die NetScaler VPX-Bereitstellung auf VMware vCenter (**Infrastruktur > Instanz > Citrix ADC > VPX > Bereitstellung**) schlägt aufgrund desselben Namens fehl, der in der zuvor gelöschten VPX-Instanz verwendet wurde.

  [NSHELP-35983]

StyleBooks

- 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:

  Kein Job gefunden.

  [NSADM-97948]

- Wenn Sie ein Configpack aus einer StyleBook-Definition erstellen, die über einen virtuellen Authentifizierungsserver und integrierte Cache-Richtlinienbindungen verfügt, und dann das Configpack löschen, ist das Löschen erfolgreich. Wenn Sie jedoch erneut versuchen, das Configpack mit denselben Parametern zu erstellen, erscheint die folgende Fehlermeldung:

  Ressource ist bereits vorhanden.

  [NSHELP-35646]

26. Juli 2023

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 Überwachen der NetScaler-Konsole, der Anwendungen und der Anwendungssicherheit mit Prometheus.

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]

Weisen Sie den verwalteten NetScaler-Instanzen von der NetScaler Console aus ein Net-Profil zu Wenn Sie Analysen für die virtuellen Server in NetScaler Console aktivieren, werden die AppFlow-Daten von NetScaler über die NetScaler Subnetz-IP-Adresse (SNIP) in die NetScaler Console 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 jetzt über die NetScaler Console Netzprofile zuweisen. Navigieren Sie zu **Infrastruktur > Instanzen > Citrix 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 zur NetScaler Console zuweisen.

[NSADM-91836]

Infrastruktur

Verbesserte Benutzererfahrung bei der Verwendung der CLI zur Konfiguration des NetScaler Agents als Proxy Wenn Sie versuchen, einen NetScaler Agent beim NetScaler Console-Dienst zu registrieren, werden Sie von der CLI nun mit (J/N) Fragen zur Proxynutzung gefragt.

Sie haben auch die Möglichkeit, den Proxy bei Bedarf im selben Skript zu konfigurieren.

[NSADM-96921]

CLI-Unterstützung zum Anzeigen von Endpunkt-URLs bei der Registrierung eines NetScaler Agents Nachdem Sie eine Dienst-URL in CLI eingegeben haben, während Sie einen NetScaler Agent beim NetScaler Console-Dienst registrieren, können Sie die Liste aller Endpunkt-URLs anzeigen, denen der Zugriff gewährt werden muss.

[NSADM-96920]

StyleBooks

Unterstützung für zusätzliche Attribute in StyleBooks Analytics Der Analysebereich von StyleBooks wurde jetzt erweitert um:

- Akzeptieren von Parametern, um Transport Mode (`transport-mode`) zu konfigurieren
- Konfiguration von HDX Insight für verschiedene Arten von Datenverkehr (`enable-hdxinsight-for`)
  - Aktivieren der Option HTTP X-Forwarded-For (`http-x-forwarded-for`)
  - Clientseitige Messungen aktivieren (`client-side-measurements`)

Weitere Informationen finden Sie unter StyleBooks Analytics.

[NSADM-97839]

18. Juli 2023

Verwaltung und Überwachung

Unterstützung für die Identifizierung und Behebung von CVE-2023-3519, CVE-2023-3466 und CVE-2023-3467 NetScaler Console Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2023-3519, CVE-2023-3466 und CVE-2023-3467.

Identifizierung von:

- CVE-2023-3519 erfordert eine Kombination aus Versions- und Konfigurationsscan.
- CVE-2023-3466 und CVE-2023-3467 erfordern einen Versionsscan.

Die Korrektur für CVE-2023-3519, CVE-2023-3466 und CVE-2023-3467 erfordert ein Upgrade der anfälligen NetScaler-Instanz auf eine Version und einen Build, die den Fix enthalten.

> **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 Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Jobs zum Upgrade von NetScaler-Instanzen.

Weitere Informationen zur Behebung von CVE-2023-3519, CVE-2023-3466 und CVE-2023-3467 finden Sie im Security Bulletin.

> **Hinweis:**
>
> Es kann einige Stunden dauern, bis der Scan des Sicherheitsempfehlungssystems abgeschlossen ist und die Auswirkungen von CVE-2023-3519, CVE-2023-3466 und CVE-2023-3467 im Sicherheitsempfehlungsmodul berücksichtigt werden. Um die Auswirkungen früher zu erkennen, können Sie einen Scan auf Anforderung starten, indem Sie auf **Jetzt scannen** klicken.

[NSADM-100103]

12. Juli 2023

Behobene Probleme

Die Probleme, die in Build vom 12. Juli 2023 behoben werden.

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

[NSHELP-35724]

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

  [NSHELP-35588]

03. Juli 2023

Analytics

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.

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

Weitere Informationen finden Sie unter Job für die Konfiguration des Exports von Metriken von NetScaler nach Prometheus planen.

[NSADM-97251]

Infrastruktur

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

> **Hinweis:**
>
> Dies gilt nur für NetScaler, die mithilfe des NetScaler Agents hinzugefügt werden.

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

[NSADM-76343]

Behobene Probleme

- Wenn Sie in Web Insight eine Metrik aufschlüsseln, um Details anzuzeigen, und dann eine Metrik weiter aufschlüsseln, bleibt das Diagramm 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]

- 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, NSADM-97727]

- Wenn Sie im **App-Dashboard**eine Anwendung auswählen und zur Registerkarte **SSL** navigieren, um ein Zertifikat zu binden, wird die Fehlermeldung "**Zertifikat nicht in der Datenbank gefunden**"angezeigt.

  [NSHELP-35654]

14. Juni 2023

Sicherheit

Unterstützung für die Erstellung von API-Definitionen ohne Auswahl von Endpunkten Auf der Seite **Sicherheit > API Gateway > API Discovery** > **Vserver** können Sie jetzt eine API-Definition erstellen, ohne einen Endpunkt auszuwählen. Wenn Sie auf **API-Definition erstellen**klicken, erscheint ein Popup-Fenster, in dem Sie bestätigen können, ob eine API-Definition für alle erkannten Endpunkte erstellt werden muss. Klicken Sie auf **Ja**, um die API-Definition mit allen Endpunkten zu erstellen, oder klicken Sie auf **Nein**.

Weitere Informationen finden Sie unter Discover API-Endpoints.

[NSADM-94318]

StyleBooks

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

- `string`
- `ipaddress`
- `tcp-port`
- `number`

- `boolean`

Weitere Informationen finden Sie unter replace ().

[NSADM-96802]

Behobene Probleme

Die Probleme, die in Build vom 14. Juni 2023 behoben wurden.

- Wenn Sie unter Upgrade-Jobs (**Infrastruktur > Upgrade-Jobs**) die Instanz auswählen, bei der die Überprüfung vor dem Upgrade fehlgeschlagen ist, und auf **Erneut validieren**klicken, wird eine Fehlermeldung angezeigt.

  [NSADM-98329]

- MPX-Instanzen fehlen auf der Seite **Infrastruktur > Citrix ADC-Inventar > Citrix ADC (MPX/VPX/CPX/BLX**).

  [NSHELP-35593]

- Wenn Sie die SSL-Ablaufberichte für wöchentlich, 30 Tage oder 90 Tage unter **Infrastruktur > SSL-Dashboard > SSL-Zertifikate > Berichte exportieren 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]

- In NetScaler Version 13.1 und höher werden die ISSU-Befehle während des NetScaler-Upgrades nicht ausgeführt.

  [NSHELP-35391]

- Wenn Sie bei mehreren Cluster-IP-Adressen (CLIPs) in einem Cluster unter **Infrastruktur > Instanzen > Citrix ADC > Hinzufügen einen CLIP in Klammern hinzufügen** , schlägt die Konfiguration fehl und der CLIP wird nicht zur NetScaler Console hinzugefügt.

  [NSHELP-35323]

31. Mai 2023

Analytics

Gepoolte Lizenzierungsempfehlungen in der Aufgabenfunktion In **Tasks** können Sie jetzt Empfehlungen und Guide Me-Workflows für gepoolte Lizenzberechtigungen einsehen. Als Admin-

istrator stellen diese gepoolten Lizenzierungsempfehlungen sicher, dass Sie alle Funktionen der NetScaler Console nutzen.

Weitere Informationen finden Sie unter Empfehlungen anzeigen und Ihre ADCs und Anwendungen effizient verwalten.

[NSADM-93988]

Exportieren Sie SSL-Insights-Daten nach Splunk und New Relic Wenn Sie unter **Einstellungen > Ökosystemintegration** ein neues Abonnement für die Integration von Citrix ADM mit Splunk und New Relic erstellen, können Sie jetzt die Option **SSL Certificate Insights** auswählen. Nachdem Sie das Abonnement mit der Option **SSL Certificate Insights** konfiguriert haben, können Sie die SSL-Daten (SSL-vserver- und SSL-Zertifikatsdaten) im Splunk- und New Relic-Dashboard anzeigen.

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

[NSADM-92047]

Behobene Probleme

Die Probleme, die in Build vom 31. Mai 2023 behoben wurden.

- Wenn Sie unter **Gateway > HDX Insight > Instanzen** eine Instanz auswählen und die Daten exportieren, waren die Benutzernameninformationen für Desktop-Benutzer nicht verfügbar. Mit diesem Fix sind die Informationen zum Benutzernamen auch im Bericht verfügbar.

  [NSADM-96024]

- Wenn Sie unter **Infrastruktur > Instanzen > Citrix ADC > SDX** für eine SDX-Instanz die Option **SNMP konfigurieren** auswählen, wird eine Fehlermeldung angezeigt. Dieses Problem tritt auf, wenn das SDX-Profil mit SNMP v3 und **NoAuthNoPriv** als Sicherheitsstufe konfiguriert ist.

  [NSHELP-35324]

- Wenn Sie unter **Infrastruktur > Konfiguration > Konfigurationsaufträge > Auftrag erstellen > Konfiguration auswählen** eine Kennwortvariable ($password$) eingeben und als **Typ** das **Textfeld** beibehalten statt **Kennwortfeld** zu wählen und dann auf **Weiter** klicken, wird die Seite nicht geladen.

  [NSHELP-35266]

- Wenn Sie in Web Insight Daten mit der Snapshot-Option exportieren, werden die Diagramme im Bericht leer angezeigt.

  [NSHELP-35147]

- Analytics ist in HDX Insight nicht sichtbar. Selbst wenn Citrix ADM neu gestartet wird, sind die Analysen nur für kurze Zeit sichtbar und werden später unsichtbar.

  [NSHELP-35128]

- Wenn für eine SDX-Instanz unter **Infrastructure > Instanzen > Citrix ADC > SDX > Dasboard** die verwendeten und freien Werte für eine Ressource Null sind, zeigt das Diagramm zur **Systemressourcenauslastung** ein Leerzeichen und leere Wertfelder an.

  Mit diesem Fix wird die Zahl Null neben dem Ressourcennamen angezeigt, wenn der verwendete und der freie Wert Null sind.

  [NSHELP-35069]

18. Mai 2023

Analytics

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]

Infrastruktur

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**.

[NSADM-52467]

Unterstützung für die Protokollierung von Ereignissen unabhängig vom Alter des Ereignisses
NetScaler Console ermöglicht es Ihnen jetzt, alle Ereignisse unabhängig vom in den Eventregeln festgelegten Event-Alter aufzuzeichnen.

Um diese Option einzustellen, navigieren Sie zu **Infrastruktur > Regeln > Hinzufügen > Ereignisalter konfigurieren** und aktivieren Sie das Kontrollkästchen **Ereignisse sofort unabhängig von der Dauer des Ereignisses protokollieren** .

[NSHELP-19914]

Behobene Probleme

Die Probleme, die in Build vom 18. Mai 2023 behoben wurden.

- Wenn Sie unter **Infrastruktur > Upgrade-Jobs > Hinzufügen > Aufgabe planen** die Option **Zweistufiges Upgrade für Knoten in HA ausführen** auswählen und in den beiden Feldern **Startzeit** dieselbe Uhrzeit auswählen, wird die folgende Fehlermeldung angezeigt, wenn Sie fortfahren:

  "common.date_diff_error:There should be atleast 1 hour difference between upgrade time"

  Selbst wenn Sie die Startzeit in den Feldern ändern, wird auf der Registerkarte **Job erstellen** eine leere Seite angezeigt.

  [NSHELP-35016]

- Unter **Infrastruktur > Instanzberatung > Upgrade-Empfehlung** sind die Informationen zum Ende der Wartung (EOM) und zum Ende der Lebensdauer (EOL) für Version 13.0 falsch.

  [NSHELP-34953]

- In der E-Mail-Benachrichtigung für jedes Ereignis wurde die Region falsch angezeigt. Mit diesem Fix wird die Region in den E-Mail-Benachrichtigungen für Ereignisse nicht angezeigt.

  [NSHELP-34913]

09. Mai 2023

Verwaltung und Überwachung

Unterstützung bei der Identifizierung und Behebung von CVE-2023-24488 und CVE-2023-24487
Die NetScaler Console Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2023-24488 und CVE-2023-24487.

Identifizierung von:

- CVE-2023-24488 erfordert eine Kombination aus Versions- und Konfigurationsscan.

- CVE-2023-24487 erfordert einen Versionsscan.

Die Behebung für CVE-2023-24487 und CVE-2023-24488 erfordert ein Upgrade der anfälligen ADC-Instanz auf eine Version und einen Build, die den Fix enthalten.

Weitere Informationen zu den festen Build-Versionsdetails für CVE-2023-24487 und CVE-2023-24488 finden Sie im Security Bulletin.

> **Hinweis:**
>
> ADC-Build 13.1–45.63 ersetzt Build 13.1–45.61.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von ADC-Instanzen finden Sie unter Erstellen eines ADC-Upgrade-Jobs .

> **Hinweis:**
>
> Es kann einige Stunden dauern, bis der Scan des Sicherheitsempfehlungssystems abgeschlossen ist und die Auswirkungen von CVE-2023-24488 und CVE-2023-24487 im Modul zur Sicherheitsempfehlung berücksichtigt werden. Um die Auswirkungen früher zu erkennen, können Sie einen Scan auf Anforderung starten, indem Sie auf **Jetzt scannen** klicken.

[NSADM-93570]

25. April 2023

Die Verbesserungen und Änderungen, die in Build am 25. April 2023 verfügbar sind.

Analytics

Web Insight - Unterstützung für die Anzeige von Nullwerten in Diagrammen Wenn Sie in **Web Insight**eine Metrik unter Applications, Clients, URLs oder Instanzen 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]

StyleBooks

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**.

[NSADM-92374]

Behobene Probleme

Die Probleme, die in Build vom 25. April 2023 behoben wurden.

- Wenn Sie unter **Anwendungen > Konfiguration > Config Packs**eine Suchabfrage mithilfe der Suchkriterien von **Eigenschaften > Schlüssel anzeigen**eingeben, wird das Suchergebnis angezeigt, aber in der Suchleiste wird die Indexnummer des Ergebnisses angezeigt.

  Mit diesem Fix zeigt die Suchleiste die Suchabfrage in Text statt in einer Zahl an.

  [NSADM-96859]

Analytics

- Die Bandbreitendaten in **HDX Insight** und **Gateway Insight** werden falsch in Byte pro Sekunde statt in Bits pro Sekunde angezeigt.

  [NSHELP-34836]

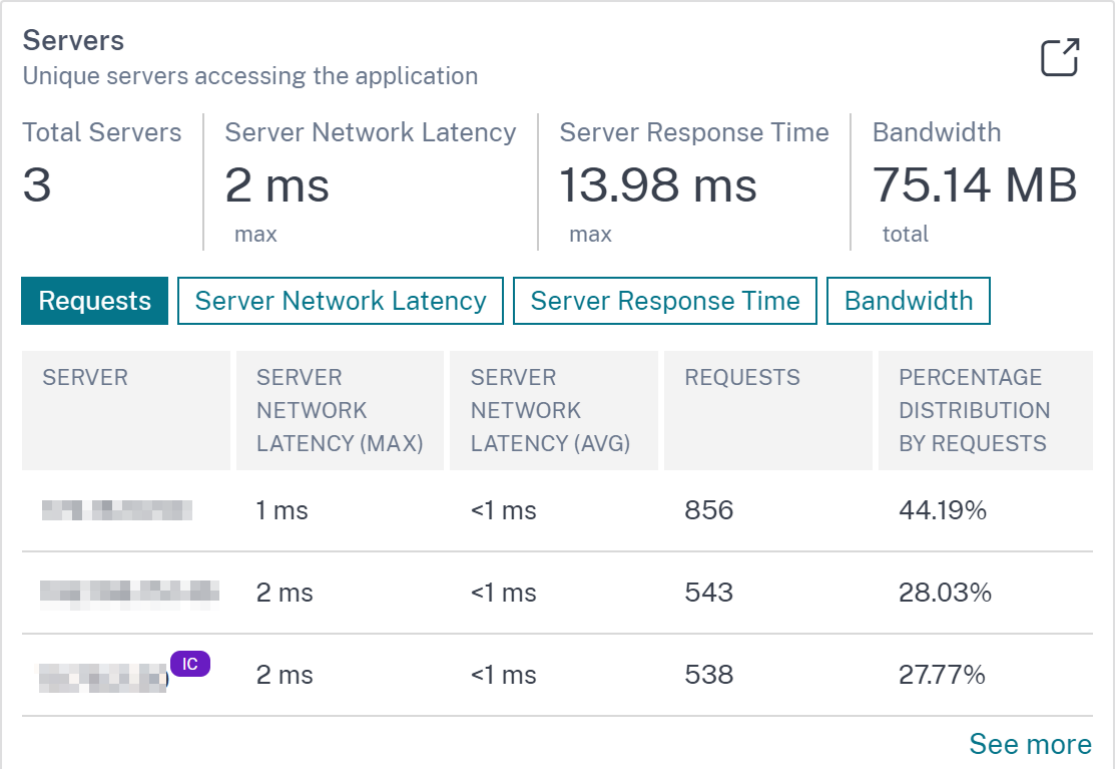
13. April 2023

Die Verbesserungen und Änderungen, die in Build am 13. April 2023 verfügbar sind.

Analytics

Integrierte Cache-Benachrichtigung in Web Insight Nachdem Sie den integrierten Cache in der NetScaler-Instanz aktiviert haben, werden die berechtigten Anfragen verarbeitet, ohne dass ein Roundtrip zu einem Ursprungsserver erforderlich ist. In **Web Insight**sind diese integrierten Cache-Anforderungen derzeit unter **Servern** mit virtueller Server-IP-Adresse statt unter der tatsächlichen Server-IP-Adresse sichtbar.

Für eine bessere Sichtbarkeit dieser integrierten Cache-Anfragen können Sie jetzt eine IC-Benachrichtigung neben der IP-Adresse des virtuellen ADC-Servers unter **Server**anzeigen.



Für die Anfragen, die nicht mit Integrated Cache verarbeitet werden, ist die tatsächliche IP-Adresse des Ursprungsservers sichtbar.

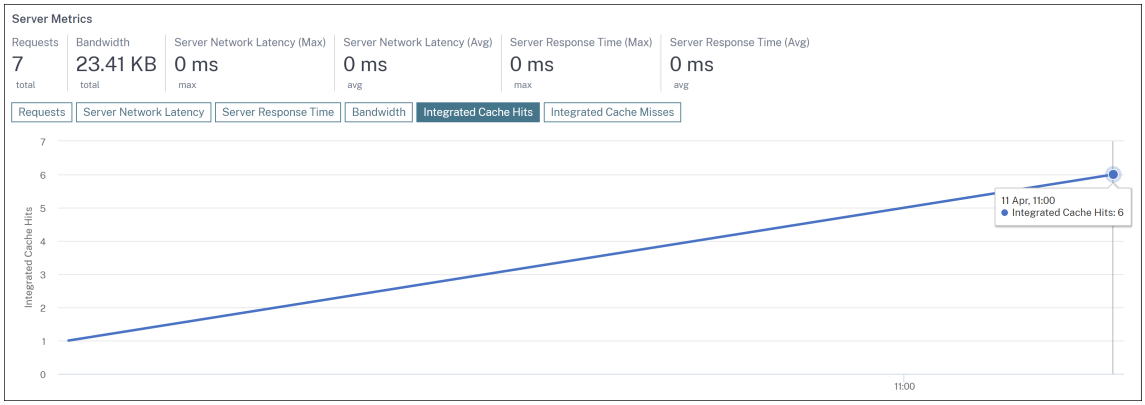
Als Administrator können Sie anhand dieser Benachrichtigung schnell feststellen, dass die ADC-Instanz die Integrated Cache-Anforderungen verarbeitet hat.

[NSADM-91864]

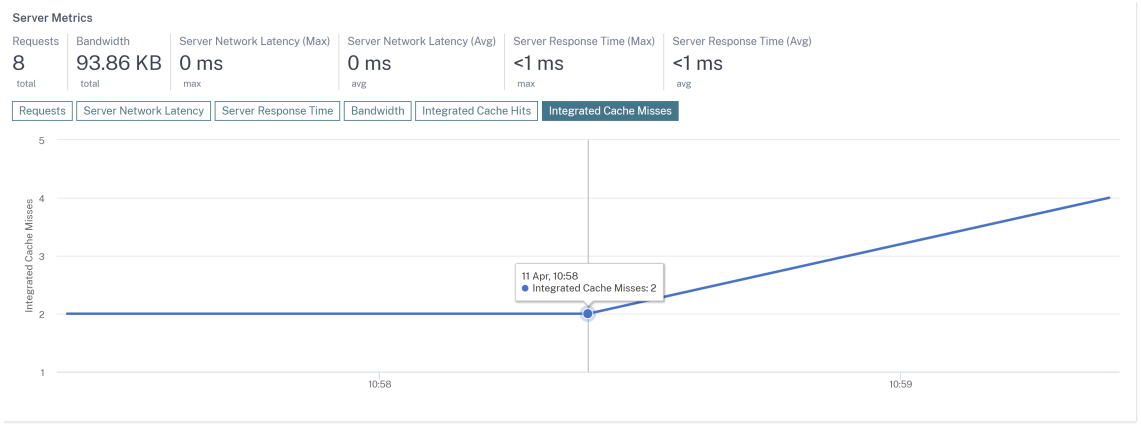
Integriertes Diagramm mit Cache-Treffern und -Fehlschlägen in Web Insight Wenn Sie in **Web Insight einen**Drilldown für einen Server durchführen, werden in den **Servermetriken** jetzt die Registerkarten **Integrierte Cache-Treffer** und **Integrierte Cachefehler** angezeigt.

Als Administrator wird das Diagramm angezeigt in:

- Auf der Registerkarte **Integrated Cache Hits** können Sie die gesamten Antworten anzeigen, die die NetScaler Appliance aus dem Cache bereitstellt.



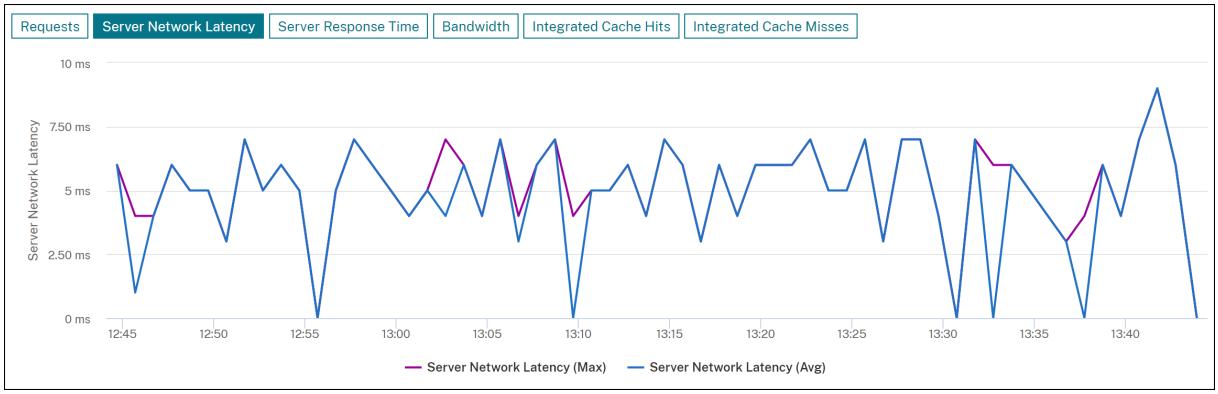
- Auf der Registerkarte **Integrated Cache** Misses können Sie die gesamten Antworten anzeigen, die die NetScaler Appliance vom Originalserver bereitstellt.



[NSADM-93952]

Web Insight - Zeigen Sie sowohl Durchschnitts- als auch Höchstwerte in Grafiken an Ab 13.1 45.47 oder höheren Versionen wird **Web Insight** in NetScaler Console unterstützt, wobei die maximalen Latenzwerte unter **Server** und **Clients** sichtbar sind.

Zusätzlich zu dieser Unterstützung können Sie beim Drilldown eines Servers oder eines Clients nun sowohl Durchschnitts- als auch Höchstwerte im Übersichtsbereich anzeigen. Sie können diese Werte auch anzeigen, indem Sie in den Bereichen **Server-Netzwerklatenz**, **Serverantwortzeit** und **Client-Netzwerklatenz** mit dem Mauszeiger auf das Diagramm zur Zeitreihenanalyse zeigen.



Als Administrator können Sie mit dieser Erweiterung die maximale Latenz in Diagrammen für die gewählte Dauer visualisieren.

[NSADM-93816]

Infrastruktur

Zeigen Sie Datenspeichertrends in der NetScaler Console-GUI an Unter **Einstellungen > Datenspeicherverwaltung**können Sie jetzt die Datenspeicherinformationen für die verschiedenen Funktionen in Ihrer aktuellen Bereitstellung einsehen. Das **Data Storage Management** Dashboard hilft Ihnen zu visualisieren, wie die Daten gespeichert werden und ob die Funktionen innerhalb ihrer Speicheransprüche funktionieren.

> **Hinweis**
>
> Die Datenspeicherrichtlinien werden sich voraussichtlich in den kommenden Versionen ändern. Mit diesen Änderungen können Sie historische Daten nicht speichern, nachdem sie das Speicherlimit überschritten haben.

Weitere Informationen finden Sie unter Datenspeicher verwalten.

[NSADM-94623]

Behobene Probleme

Die Probleme, die in Build vom 12. April 2023 behoben wurden.

Infrastruktur

- In Bereitstellungen mit hoher Verfügbarkeit gibt es keine Option, Build-Image-Dateien nur auf den sekundären Knoten hochzuladen.

Als Teil des Updates können Sie jetzt Build-Image-Dateien über **Infrastruktur > Upgrade-Jobs > Registerkarte**Job erstellen**Nur auf sekundären Knoten hochladen auf den sekundären Knoten**hochladen.

[NSADM-96079]

- Die aus **Infrastruktur > Instanzen > NetScaler** exportierten Berichte zeigen nicht die Seriennummer der sekundären Knoten an.

  In den Berichten werden jetzt die Seriennummern der primären und sekundären Knoten der NetScaler-Instanzen angezeigt. Sie können die Berichte auch unter **Infrastruktur > NetScaler Inventory**einsehen.

  [NSHELP-18816]

05. April 2023

Die Verbesserungen und Änderungen, die in Build vom 05. April 2023 verfügbar sind.

Sicherheit

Erstellen Sie API-Definitionen aus erkannten API-Endpunkten in der NetScaler Console-GUI Sie können jetzt API-Definitionen aus erkannten API-Endpunkten unter **Sicherheit > API Gateway > API Discovery**erstellen.

[NSADM-85957]

Einheitliches Dashboard – Wichtige Kennzahlen für API-Analysen anzeigen Im vereinheitlichten Dashboard (Übersicht **> Dashboard**) sehen Sie jetzt wichtige Metriken für die API-Endpunkte, die über NetScaler Console konfiguriert wurden.

Weitere Informationen finden Sie unter Ein einheitliches Dashboard zum Anzeigen der Details der Instanzschlüsselmetrik.

[NSADM-85954]

Behobene Probleme

Die Probleme, die in Build vom 05. April 2023 behoben wurden.

- Die Option **“Gerät auswählen** “für die Felder “**Zertifikatsdatei** “und “**Schlüsseldatei** “wird auf den folgenden Seiten angezeigt:
  - **Infrastruktur > SSL-Dashboard > Zertifikatsspeicher verwalten > Hinzufügen**

- **Infrastruktur > SSL-Dashboard > SSL-Zertifikate > Update**

Als Fix wurde die Option **“Gerät auswählen** “jetzt entfernt.

[NSHELP-34566]

- Wenn NetScaler über eine on-premises NetScaler Console als Lizenzserver verfügt und ein Agent unter **Infrastruktur > Instanzen > Agents** geändert wird, tritt das folgende Problem auf:

  `The IP address of the license server on NetScaler changes from the IP address of the on-premises NetScaler Console to the IP address of one of the NetScaler agents`.

  [NSHELP-34483]

- Wenn Sie das Kennwort für ein mit SNMPv3 konfiguriertes SDX-Administratorprofil unter **Infrastruktur > Instanzen > NetScaler > Registerkarte SDX**Profil bearbeiten, wird die folgende Fehlermeldung angezeigt:

  `Please provide valid authentication protocol. The possible values are MD5, SHA`.

  [NSHELP-34372]

14. März 2023

Behobene Probleme

Das folgende Problem wurde in Build vom 14. März 2023 behoben:

Wenn Sie **unter Infrastruktur > SSL-Dashboard > Zertifikate installieren**eine Zertifikatskette hochladen, die dasselbe Stammzertifikat wie eine vorhandene Zertifikatskette hat, schlägt die Zertifikatinstallation fehl. Der folgende Text wird unter **Infrastruktur > SSL-Dashboard > SSL-Auditprotokolle > Geräteprotokoll > Befehlsprotokoll**angezeigt:

`Resource Already Exists`

[NSHELP-34233]

Wenn Sie eine E-Mail-Verteilerliste unter **Einstellungen > Benachrichtigungen > E-Mail**löschen, wird der folgende Fehler angezeigt:

`Error: Bad Gateway`

Dieses Problem tritt auf, weil der Name der E-Mail-Verteilerliste ein Leerzeichen enthält.

Als Teil des Fixes können Sie in NetScaler Console jetzt E-Mail-Verteilerlisten mit Leerzeichen löschen.

[NSHELP-34545]

02. März 2023

Analytics

Verbesserungen bei Web Insight In Web Insight können Sie sich jetzt die folgenden Verbesserungen unter **Application Metrics** ansehen:

- Eine neue Registerkarte **Zusammenfassung** wird eingeführt, auf der Sie einen Überblick über die Anwendungsleistung wie Reaktionszeit, Anfragen und Bandbreite visualisieren können. Als Administrator erhalten Sie so einen Einblick in die Anwendungsleistung für die gewählte Dauer. Sie können die Umschaltoption verwenden und die Ansicht anpassen.
- Auf der Registerkarte **Anfragen** können Sie neben der Gesamtzahl der Anfragen auch die Anfragen der fünf wichtigsten Clients auf der Grundlage der Gesamtzahl der Anfragen anzeigen. Als Administrator erhalten Sie auf diese Weise einen Einblick in die Clients, die für die gewählte Dauer auf die Anwendung zugreifen.
- Auf der Registerkarte **Bandbreite** können Sie den Bandbreitenverbrauch der fünf wichtigsten Server auf der Grundlage des gesamten Bandbreitenverbrauchs einsehen. Als Administrator erhalten Sie auf diese Weise einen Einblick in die Server, die für die gewählte Dauer mehr Bandbreite verbrauchen.
- Auf der Registerkarte **Antwortzeit** können Sie auch die Client-Netzwerklatenz, die Servernetzwerklatenz und die Serververarbeitungszeit in derselben Grafik anzeigen. Als Administrator erhalten Sie auf diese Weise einen Einblick in die Latenz, die von Client, Server und Anwendung für die gewählte Dauer auftritt. Sie können die Umschaltoption verwenden und die Ansicht anpassen.

  [NSADM-87792]

Infrastruktur

Löschen inaktiver NetScaler Console Express-Konten Wenn Ihr NetScaler Console Express-Konto 45 Tage lang inaktiv bleibt, wird das Konto gelöscht. Citrix sendet nach 30 Tagen Inaktivität eine Erinnerung.

[NSADM-93203]

Verwaltung und Überwachung

Änderung der Ausführungszusammenfassung für das NetScaler Hochverfügbarkeitsupgrade In der NetScaler Console GUI werden in der Ausführungsübersicht unter Infrastruktur > Upgrade-Jobs > Ausführungsübersicht nicht mehr die Befehle für die Hochverfügbarkeitssynchronisierung angezeigt.**

Dies liegt daran, dass NetScaler während des NetScaler-Hochverfügbarkeitsupgrades die Hochverfügbarkeitssynchronisierung zwischen den Knoten deaktiviert, wenn sich die primären und sekundären NetScaler-Knoten in unterschiedlichen Versionen befinden. NetScaler Console führt diesen Vorgang nicht aus.

[NSADM-93441]

Schwellenwert für einzelne Entitäten in Netzwerkberichten festlegen Unter **Infrastruktur > Netzwerkberichterstattung > Schwellenwerte** können Sie jetzt bei der Konfiguration des Schwellenwerts den Schwellenwert für bestimmte Entitäten festlegen.

Weitere Informationen finden Sie unter Netzwerkberichte.

[NSADM-91727]

Unterstützung für die Planung einzelner Agent-Upgrades Unter **Infrastruktur > Instanzen > Agents > Einstellungen** können Sie jetzt das Upgrade jedes NetScaler Agents planen. Sie können wählen, ob Sie einen Agent entweder automatisch auf den nächsten Build aktualisieren oder eine Uhrzeit und Zeitzone angeben möchten, um ein Upgrade zu planen.

Weitere Informationen finden Sie unter Einstellungen für das Agent-Upgrade.

[NSADM-91719]

Verbesserungen beim Upgrade der NetScaler-Instanz Die folgenden Änderungen sind jetzt auf der Registerkarte **Pre-upgrade validation** verfügbar:

- Abschnitt **Instanzen blocked from upgrade** – In diesem neuen Abschnitt werden die Instanzen aufgeführt, für die das Upgrade aufgrund von Validierungsfehlern vor dem Upgrade gesperrt wurde.
- Schaltfläche **Quick Cleanup** – Diese Schaltfläche ist im Bereich **Disk Space Details** verfügbar und ermöglicht es Ihnen, schnell Speicherplatz in mehreren Ordnern freizugeben.

Weitere Informationen finden Sie unter So aktualisieren Sie eine ADC-Instanz.

[NSADM-91505]

NetScaler BLX-Images jetzt in der Bildbibliothek verfügbar Beim Upgrade von NetScaler BLX über **Infrastruktur > Upgrade-Jobs > Upgrade NetScaler BLX > Image auswählen**können Sie jetzt die **NetScaler BLX-Images** aus der Bildbibliothek auswählen.

[NSADM-86864]

Sicherheit

Sehen Sie sich die Versionen von NetScaler Web App Firewall und Bot-Signaturen für eine NetScaler-Instanz an Sie können jetzt die Versionen von NetScaler Web App Firewall und Bot-Signaturen für eine NetScaler-Instanz anzeigen. Die neuesten Signaturversionen schützen Ihre Instanz vor den CVEs. Weitere Informationen finden Sie in den Artikeln zu Signaturwarnungen und Artikeln zu Bot-Signaturwarnungen.

[NSADM-92378]

Analyse der Anwendungsleistung

Verbesserungen bei Web Insight In **Web Insight** können Sie jetzt die maximalen Netzwerklatenzwerte sowohl im **Server** als auch im **Client** anzeigen. Als Administrator können Sie mit dieser Erweiterung genau den Server oder Client ermitteln, der mit maximaler Latenz arbeitet.

Bisher gab Web Insight den Maximalwert nur auf der Grundlage der durchschnittlichen Latenzwerte für alle Server und Clients an.

[NSADM-91834]

Sonstiges

Filter im vereinheitlichten Dashboard erstellen und anwenden Im vereinheitlichten Dashboard (**Übersicht > Dashboard**) können Sie jetzt Filter erstellen und anwenden in:

- Anwendungen
- ADC-Infrastruktur
- Anwendungssicherheit

Als Administrator können Sie Filter anwenden und Erkenntnisse nur für die ausgewählten Instanzen oder Anwendungen anzeigen.

Weitere Informationen finden Sie unter Ein einheitliches Dashboard zum Anzeigen der Details der Instanzschlüsselmetrik.

[NSADM-91873]

Behobene Probleme

Die Probleme, die in Build 02. März 2023 behoben wurden.

- Wenn Sie unter **Infrastruktur > Upgrade-Jobs**einen abgeschlossenen Job auswählen, der den Namen der Skriptdatei vor oder nach dem Upgrade mit Sonderzeichen enthält, und dann die Ausgabeskripts aus der Liste **Aktion auswählen** herunterladen, wird die Fehlermeldung **Datei nicht gefunden** angezeigt.

[NSHELP-33854]

07. Februar 2023

Analytics

Bei Sicherheitsverstößen werden OWASP-Tags angezeigt In der NetScaler Console-GUI zeigen die Sicherheitsverletzungen jetzt OWASP-Tags an. Es unterstützt die Listen OWASP 2017 und OWASP 2021. Anhand dieser Tags können Sie feststellen, ob der Verstoß zur OWASP-Top-10-Liste gehört.

Wählen Sie einen Verstoß aus, um weitere Details zu sehen. Zu den Details gehören jetzt die Spalten OWASP 2017 und OWASP 2021. In diesen Spalten werden die OWASP-Codes angezeigt. Sie können sie verwenden, um auf der OWASP-Websitemehr über den Verstoß zu erfahren.

[NSADM-92999]

Verwaltung und Überwachung

Unterstützung für das Ändern des Agentkennworts ohne aktuelles Kennwort Als Superadministrator können Sie jetzt zulassen, dass Agentkennwörter ohne die aktuellen Kennwörter geändert werden.

Navigieren Sie zu **Einstellungen** > **Allgemeine Einstellungen** > **Systemkonfigurationen** > **Agent und Zeitzone > Agent** und aktivieren Sie das Kontrollkästchen **Aktuelle Kennwortvoraussetzung für Agentkennwortänderung entfernen**. Auf der Seite **Agentkennwort ändern** wird das Feld **Aktuelles Kennwort** nicht mehr angezeigt.

Um das Feld **Aktuelles Kennwort** erneut anzuzeigen, deaktivieren Sie das Kontrollkästchen **Aktuelle Kennwortvoraussetzung für die Änderung des Agentkennworts entfernen**.

[NSADM-91826]

Das Intervall für die Visualisierung von Zeitreihendaten für NetScaler Console Express-Konten wurde überarbeitet Für virtuelle Server, die mit dem Express-Konto verwaltet werden, wurde die Zeitreihendatenvisualisierung in Analysediagrammen und Network Reporting-Diagrammen für die Dauer **Letzte Stunde** überarbeitet.

Feature	Bestehendes Datenvisualisierungsintervall	Neues Datenvisualisierungsintervall
Anwendungsdashboard	1 Minute	5 Minuten
Netzwerkberichterstellung	5 Minuten	10 Minuten
Web Insight, HDX Insight, Gateway Insight, Security Insights, BOT Insights, detaillierte Transaktionen	1 Minute	5 Minuten

[NSADM-93200]

Behobene Probleme

Die folgenden Probleme wurden im Build vom 07. Februar 2023 behoben.

Wenn Sie die Syslog-Einstellungen für die ADC-Instanz aktivieren oder deaktivieren, speichert ADM die Konfiguration nicht in der ADC-Instanz. Daher werden Ereignisse mit Konfigurationsänderungen nicht in NetScaler Console gespeichert.

[NSHELP-33264]

Nachdem Sie unter **Infrastruktur > Instanzen > Agent** das SSL-Zertifikat mit einem kennwortverschlüsselten Schlüssel installiert haben, schlägt die Verbindung zum Agent auf Port 443 fehl.

[NSHELP-33614]

24. Januar 2023

Behobene Probleme

Die folgenden Probleme wurden im Build vom 24. Januar 2023 behoben.

Eine Fehlermeldung wird angezeigt, wenn Sie SNMP v3 auf einer NetScaler SDX-Instanz über die NetScaler Console-GUI aktivieren, indem Sie zu **Infrastruktur > Instanzen > NetScaler > SDX > Select Action > Configure SNMP** navigieren.

[NSHELP-33852]

10. Januar 2023

Verwaltung und Überwachung

Sehen Sie sich Empfehlungen an und verwalten Sie Ihre ADCs und Apps effizient als umsetzbare Aufgaben mit Guide Me-Workflows In der NetScaler Console-GUI wurde eine neue **Task**-Option eingeführt, in der Sie jetzt Empfehlungen basierend auf Ihrem Abonnement und Ihrer aktuellen Auslastung anzeigen können. Als Administrator können Sie:

- **To-Do-Aufgaben** als umsetzbare Empfehlungen für Lizenzierung, Analysen, Ereignisse, SSL-Zertifikate und vieles mehr anzeigen
- Schließen Sie die Aufgabe mithilfe der Option **Guide Me** ab, die Hilfestellungen und Tooltips enthält, mit denen Sie die Aufgabe erfolgreich abschließen können.
- Bestätigen Sie die Aufgaben und verschieben Sie sie ins Archiv
- Gehe zu **Archivierte Aufgaben** und verwende die geführten Tooltips für wiederkehrende Aufgaben

Diese Empfehlungen stellen sicher, dass Sie alle Funktionen der NetScaler Console nutzen, ermöglichen die Produkterkennung und die vom Produkt empfohlenen Funktionen für eine effiziente Verwaltung der Bereitstellung.

Weitere Informationen finden Sie unter Empfehlungen anzeigen und Ihre ADCs und Anwendungen effizient verwalten.

[NSADM-68719]

StyleBooks

Aktivieren oder deaktivieren Sie die Netzmaskenlänge in der StyleBook-Konfigurations-GUI Wenn Sie ein Konfigurationspaket aus StyleBooks mit dem`type: ipnetwork` Attribut erstellen, zeigt die StyleBook-Konfigurations-GUI jetzt die Schaltfläche **Netmask Length** neben dem **IP-Adressfeld** an.

Sie können eine der folgenden Aktionen ausführen:

- Aktiviert die Eingabe der Netzmaskenlänge
- Deaktiviert die Eingabe der Netzwerkmasken-IP-Adresse

[NSADM-80696]

13. Dezember 2022

Verwaltung und Überwachung

Unterstützung bei der Identifizierung und Behebung von CVE-2022-27518 Die Sicherheitsempfehlung von NetScaler Console unterstützt jetzt die Identifizierung und Behebung von CVE-2022-27518.

Die Identifizierung von CVE-2022-27518 erfordert eine Kombination aus einem Versionsscan und einem Konfigurationsscan, und für die Behebung ist ein Upgrade der anfälligen ADC-Instanzen auf eine Version und einen Build erforderlich, die den Fix enthalten.

Weitere Informationen zur Behebung von CVE-2022-27518 finden Sie in der Sicherheitsempfehlung.

> **HINWEIS**
>
> Es kann einige Stunden dauern, bis der Scan des Sicherheitsempfehlungssystems abgeschlossen ist und die Auswirkungen von CVE-2022-27518 im Sicherheitsempfehlungsmodul berücksichtigt werden. Um die Auswirkungen früher zu erkennen, können Sie einen Scan auf Anforderung starten, indem Sie auf **Jetzt scannen** klicken.

09. Dezember 2022

Analytics

Einstellung von Advanced Security Analytics für die Premium-lizenzierten ADC-Instanzen NetScaler Console unterstützt **Advanced Security Analytics** für die lizenzierten ADC-Instanzen der Premiumklasse nicht mehr. Mit diesem Upgrade in der NetScaler Console-GUI:

- Die vorhandenen Konfigurationen in Advanced Security Analytics und die damit verbundenen verhaltensbasierten Verstöße sind jetzt nicht sichtbar.
- Die Sichtbarkeit der anderen Bot- und WAF-Verstöße bleibt unverändert. Weitere Informationen finden Sie in den Kategorien von Verstößen.
- Der Splunk- und New Relic-Export wird nur bei WAF- und Bot-Verstößen unterstützt.

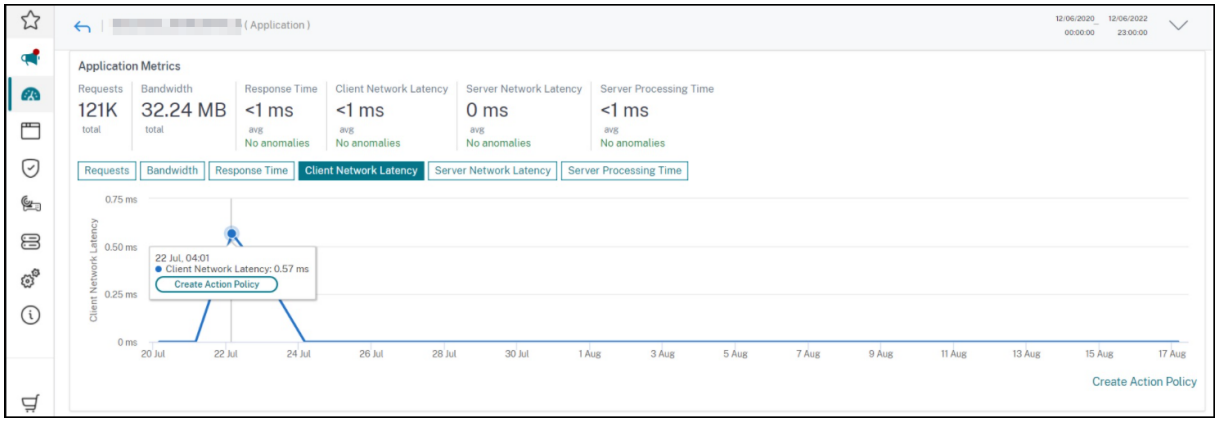
[NSADM-92342]

Konfigurieren Sie eine Aktionsrichtlinie von Web Insight In **Web Insight**können Sie jetzt anhand eines Diagrammtrends eine Aktionsrichtlinie für die folgenden Metriken konfigurieren:

- **Latenz im Client-Netzwerk**
- **Server-Netzwerk-Latenz**

- **Verarbeitungszeit des Servers**

Wenn Sie als Administrator ein ungewöhnliches Verkehrsmuster oder einen plötzlichen Anstieg dieser Metriken für eine Anwendung feststellen, können Sie mit dieser Erweiterung eine Richtlinie für relative Aktionen erstellen, indem Sie auf **Aktionsrichtlinie erstellen** klicken, nachdem Sie sie an einem bestimmten Punkt im Diagramm platziert haben.



[NSADM-88682]

Aktionsrichtlinie – Fügen Sie mehrere Anwendungen hinzu Wenn Sie eine Aktionsrichtlinie für **Clientnetzwerklatenz**, **Server-Netzwerklatenz** und **Serververarbeitungszeit** konfigurieren, können Sie jetzt mehrere Anwendungen mit dem **IN**-Operator auswählen und sie in einer einzigen Richtlinie anwenden.

Weitere Informationen finden Sie unter Aktionsrichtlinien.

[NSADM-88680]

29. November 2022

Infrastruktur

Z Informationen zum Ablauf der Lizenz werden in der NetScaler Console angezeigt Sie können jetzt Informationen zum Ablauf der Z-Lizenz von MPX- und SDX-Instanzen in der NetScaler Console anzeigen, indem Sie zu **Infrastruktur > Pooled Licensing > Pooled Capacity Z-Lizenzen** navigieren.

[NSADM-80202]

Verwaltung und Überwachung

Nicht mehr verfügbare SD-WAN- und HAProxy-Funktionen in NetScaler Console NetScaler Console unterstützt keine SD-WAN- und HAProxy-Funktionen mehr. Daher sind die zugehörigen Funktionen für SD-WAN und HAProxy jetzt nicht in der NetScaler Console-GUI verfügbar.

[NSADM-90549]

Verbesserungen beim SDX-Upgrade – Unterstützung für die Auswahl eines SDX-Images aus der Ressourcenbibliothek Wenn Sie einen Wartungsauftrag zum Upgrade einer SDX-Instanz in NetScaler Console planen, haben Sie jetzt die Möglichkeit, aus der für ein Upgrade erforderlichen Image-Bibliothek auszuwählen. Navigieren Sie zu **Infrastruktur > Upgrade-Jobs > Job erstellen**, wählen Sie **NetScaler SDX aktualisieren**und klicken Sie auf **Weiter**, um eine SDX-Instanz zu aktualisieren.

[NSADM-88832]

Behobene Probleme

Die Probleme, die in Build am 29. November 2022 behoben wurden.

- Benutzer von Azure AD können sich nicht bei ADM anmelden, wenn ein Administrator sie vor ADM zu DaaS oder anderen NetScaler-Produkten hinzugefügt hat.

  [NSHELP-32556]

- Unter **Infrastruktur > Netzwerkfunktionen > Lastenausgleich > Dienste**werden für die Gesamtzahl der konfigurierten Dienste nur 5000 gezählt, selbst wenn die Gesamtzahl der konfigurierten Dienste auf den ADC-Instanzen mehr als 5000 beträgt.

  [NSHELP-32299]

16. November 2022

Analytics

Integration mit New Relic Sie können NetScaler Console jetzt in New Relic integrieren, um Analysen zu WAF-, Bot- und verhaltensbasierten 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 Console erfasst Bot-, WAF- und verhaltensbasierte Ereignisse und sendet sie je nach Wahl entweder in Echtzeit oder in regelmäßigen Abständen an New Relic. Als Administrator können Sie den Bot, die WAF und andere verhaltensbasierte Ereignisse auch in Ihrem New Relic-Dashboard einsehen.

Weitere Informationen finden Sie unter Integration mit New Relic.

[NSADM-83119]

Infrastruktur

Automatisiertes Upgrade von Autoscale-Gruppen Der Upgrade-Vorgang von Autoscale-Gruppen ist jetzt automatisiert. Navigieren Sie zu **Infrastruktur > Public Cloud > Autoscale Groups** und wählen Sie die Autoscale-Gruppe aus, die Sie aktualisieren möchten. NetScaler Console führt die erforderlichen Prüfungen durch und aktualisiert die Autoscale-Gruppe.

Weitere Informationen finden Sie unter Autoscale-Gruppen ändern.

[NSADM-84955]

Verwaltung und Überwachung

Metriken zur Krypto-Auslastung sind im ADM Service Network Reporting-Dashboard verfügbar Sie können jetzt die Metriken zur Krypto-Auslastung im Network Reporting Dashboard hinzufügen und anzeigen. Navigieren Sie zu **Infrastruktur > Network Reporting > Dashboard erstellen**. Wählen Sie **SSL Crypto Utilization** als Entität aus und erstellen Sie ein Dashboard für Network Reporting.

[NSADM-88416]

Behobene Probleme

Die Probleme, die in Build am 16. November 2022 behoben wurden.

Asymmetrische Kryptoeinheiten und **symmetrische Kryptoeinheiten sind jetzt bearbeitbare Felder in der NetScaler Console-GUI. Sie können die Anzahl der ASUs und SCUs eingeben, während Sie eine NetScaler VPX-Instanz auf der NetScaler SDX-Appliance mit Intel Coleto (COL) -Chips bereitstellen.

Navigieren Sie zu **Infrastruktur** > **Instanzen** > **NetScaler** und wählen Sie auf der Registerkarte **SDX** eine SDX-Instanz aus, für die Sie eine NetScaler VPX-Instanz bereitstellen möchten. Wählen Sie unter **Aktion auswählen** die Option **Bereitstellung VPX** aus und geben Sie auf der angezeigten Seite die Kryptokapazität unter **Crypto Allocation** ein.

[NSHELP-33297]

8. November 2022

Verwaltung und Überwachung

Unterstützung bei der Identifizierung und Behebung von CVE-2022-27510, CVE-2022-27513 und CVE-2022-27516 Die Sicherheitsempfehlung von NetScaler Console unterstützt jetzt die Identifizierung und Behebung von drei neuen CVEs: CVE-2022-27510, CVE-2022-27513 und CVE-2022-27516.

- Die Identifizierung von CVE-2022-27510 erfordert eine Kombination aus Konfigurationsscan und Versionsscan, und die Behebung erfordert ein Upgrade der anfälligen ADC-Instanzen auf eine Version und einen Build, die den Fix enthalten.
- Die Identifizierung von CVE-2022-27513 erfordert eine Kombination aus einem Konfigurationsscan und einem Versionsscan, und die Behebung erfordert ein Upgrade der anfälligen ADC-Instanzen auf eine Version und einen Build, die den Fix enthalten.
- Die Identifizierung von CVE-2022-27516 erfordert eine Kombination aus einem Konfigurationsscan und einem Versionsscan, und die Behebung erfordert ein Upgrade der anfälligen ADC-Instanzen auf eine Version und einen Build, die den Fix enthalten.

Weitere Informationen zur Behebung von CVE-2022-27510, CVE-2022-27513 und CVE-2022-27516 finden Sie in der Sicherheitsempfehlung.

> **Hinweis**
>
> Es kann einige Stunden dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2022-27510, CVE-2022-27513 und CVE-2022-27516 im Modul für Sicherheitsberatung berücksichtigt werden. Um die Auswirkungen früher zu erkennen, können Sie einen Scan auf Anforderung starten, indem Sie auf **Jetzt scannen** klicken.

Zusammen mit dem Bulletin wird auch ein Sicherheitsartikel für Angriffe zum Schmuggeln von HTTP-Anfragen veröffentlicht. Informationen zu Angriffen auf den Schmuggel von HTTP-Anfragen finden Sie unter CTX472830.

> **Hinweis**
>
> Die Sicherheitsempfehlung von NetScaler Console unterstützt nur die Identifizierung und Behebung der CVEs. Die Sicherheitsbedenken, die im Artikel Sicherheit hervorgehoben werden, werden nicht unterstützt. Daher unterstützen wir nicht die Identifizierung und Behebung von Angriffen zum Schmuggeln von HTTP-Anfragen.

[NSADM-88525]

28. Oktober 2022

Infrastruktur

Zeitzone für das Agent-Upgrade angeben Unter **Infrastruktur > Instanzen > Agents > Einstellungen > Upgrade**verwendet die Startzeit die Zeitzone, die Sie **unter Allgemeine Einstellungen > Systemkonfiguration**ausgewählt haben.

Weitere Informationen zum Einstellen der Zeitzone finden Sie unter Einstellen der NetScaler Console-Zeitzone.

[NSADM-88417]

Behobene Probleme

Die Probleme, die in Build am 28. Oktober 2022 behandelt werden.

Unter **Einstellungen > Lizenzierung & Analytics-Konfiguration > Analytics konfigurieren**werden die Ergebnisse auf der Seite **Alle virtuellen Server** ausgeblendet, wenn Sie die folgenden Filter anwenden:

- Name
- Status
- Typ

[NSHELP-32807]

Wenn Sie eine zweite Netzwerkkarte konfigurieren, um den Verwaltungszugriff auf NetScaler Console zu isolieren, wird der zweiten NIC-IP-Adresse fälschlicherweise dieselbe IP-Adresse wie die primäre Netzwerkkarte zugewiesen.

[NSHELP-32567]

12. Oktober 2022

Analytics

WAF-Sicherheitsverletzungen – Analysen für Command Injection Grammar anzeigen Unter **Sicherheit > Sicherheitsverletzungen**unter **WAF**können Sie jetzt Protokolle und Analysen für Verstöße gegen die **Grammatik von Command Injection** anzeigen. Weitere Informationen:

- Überprüfung für HTML-Befehlseinschleusungsschutz
- Sicherheitsverstöße

[NSADM-85792]

Infrastruktur

Validieren Sie Ihr Cloud Access-Profil mit zusätzlichen Berechtigungen Das vorhandene Cloud-Zugriffsprofil der Autoscale-Gruppe, die eine Verbindung zu AWS herstellt, benötigt zusätzliche IAM-Berechtigungen. Derzeit hat der NetScaler Console-Dienst die Cloud Access-Profile aufgrund fehlender Berechtigungen ungültig gemacht. Gehen Sie wie folgt vor, um IAM-Berechtigungen zu validieren:

1. Kopieren Sie die neuesten IAM-Berechtigungen, die unter Erstellen von IAM-Rollenerwähnt werden.
2. Gehen Sie zur AWS-Konsole und validieren Sie die Rolle des Cloud Access Profils mit den neuesten IAM-Berechtigungen.

[NSADM-90096]

27. September 2022

Analytics

WAF-Sicherheitsverletzungen – Analysen für Block-Keyword anzeigen Unter **Sicherheit > Sicherheitsverletzungen**unter **WAF**können Sie jetzt Protokolle und Analysen für Verstöße gegen **Blockschlüsselwörter** und **JSON-Block-Keywords** anzeigen.

Weitere Informationen:

- Unterstützung benutzerdefinierter Keywords für HTML-Nutzlast
- Sicherheitsverstöße

[NSADM-86225]

Konfigurieren der Bot-Verwaltung auf den Platin-ADC-Instanzen In NetScaler Console können Sie jetzt:

- Konfigurieren Sie Bot-Erkennungstechniken und stellen Sie sie auf den ADC-Instanzen Build 13.0 36.27 oder höher mit Premium-Lizenz bereit.
- Zeigen Sie Bot-Analysen an, indem Sie die Option **Bot-Sicherheitsverletzungen** für die vorhandenen virtuellen Server aktivieren, die mit Bot-Erkennungstechniken konfiguriert sind, entweder über StyleBook oder direkt von der ADC-Instanz aus.

Zusammen mit der vorhandenen StyleBook-Konfiguration vereinfacht diese Erweiterung den Prozess zur Konfiguration der Bot-Erkennungstechniken und zur Bereitstellung auf den ADC-Instanzen weiter.

Weitere Informationen finden Sie unter Konfigurieren von Bot-Erkennungstechniken in NetScaler Console .

[NSADM-80413]

Infrastruktur

Neue Option zum Erstellen eines Konfigurationsauftrags für Autoscale-Anwendungen In **Autoscale-Gruppen > Konfigurationen**können Sie jetzt zu Konfigurationsjobs navigieren, indem Sie eine Autoscale-Anwendung auswählen. Auf der Seite **Job erstellen** werden Beispielbefehle basierend auf den Konfigurationsdetails der ausgewählten Anwendung angezeigt. Sie können Werte oder Befehle bearbeiten. Fügen Sie außerdem Befehle hinzu oder entfernen Sie sie.

> **Hinweis**
>
> Sie können Konfigurationsaufträge nur für Anwendungen verwenden, die im ADC CLI-Befehlsmodus erstellt wurden.

Weitere Informationen finden Sie unter Bereitstellen einer Autoscale-Anwendung mithilfe von Konfigurationsjobs.

[NSADM-85939]

NetScaler Console plant die Jobs neu, wenn unvorhergesehene Ereignisse eintreten Manchmal kann es beim Ausführen einer Konfiguration oder eines Upgrade-Auftrags zu folgenden Ereignissen kommen:

- Das Upgrade des NetScaler Console-Dienstes ist im Gange.
- Ein ADM-Agent geht aus. Es kann passieren, wenn das Agent-Upgrade läuft.

In solchen Fällen verschiebt NetScaler Console die Jobs auf die nächste Stunde.

Zuvor war NetScaler Console nicht in der Lage, das ADM-Dienst-Upgrade oder den Agent-Status zu identifizieren. Infolgedessen scheiterten Jobs nach dem Timeout.

[NSADM-85554]

Nutzungs- und Lizenzinformationen für nicht verwaltete CICO ADC-Instanzen anzeigen Sie können jetzt zu **Infrastruktur > Pool-Lizenzierung > Bandbreitenlizenzen > CICO** navigieren, um die Nutzungs- und Lizenzinformationen für nicht verwaltete CICO ADC-Instanzen im ADM Service anzuzeigen.

[NSADM-85452]

Verwaltung und Überwachung

Generieren Sie ein Tech-Support-Paket für die sekundäre ADC-Instanz In einem ADC-Paar mit hoher Verfügbarkeit können Sie jetzt auch ein Tech-Support-Bundle für den sekundären Knoten über die ADM-GUI generieren. Zuvor konnten Sie ein Tech-Support-Paket nur für den primären Knoten generieren.

[NSADM-88905]

Datenpunkte für Netzwerkberichte für jeden Tag des Monats anzeigen Wenn Sie **unter Infrastruktur > Netzwerkberichterstattung**eine Monatsdauer im Dashboard auswählen, werden die Datenpunkte für jeden Tag angezeigt. Zuvor wurden die Datenpunkte für jede Woche angezeigt.

[NSADM-88875]

StyleBooks

StyleBooks unterstützen NetScaler BLX-Instanzen Beim Erstellen eines Konfigurationspakets können Sie jetzt NetScaler BLX-Instanzen als Zielinstanzen auswählen. Zuvor unterstützten StyleBooks NetScaler MPX-, SDX-, VPX- und CPX-Instanzen.

[NSADM-86253]

13. September 2022

StyleBooks

Verbesserte Standard-StyleBooks zum Konfigurieren eines virtuellen Lastenausgleichsservers Mit den verbesserten Standard-StyleBooks können Sie jetzt alle unterstützten Optionen in ADC für einen virtuellen Lastausgleichsserver konfigurieren. Beispielsweise können Sie jetzt IP-Muster, IP-Maske, IP-Bereich und mehr festlegen. Zuvor konnten Sie nur weniger Optionen von StyleBooks konfigurieren. Wir haben die folgenden StyleBooks in NetScaler Console mit ihren verbesserten Versionen hinzugefügt:

Name	Version
lb	2.0
lb-mon	2.0

[NSADM-80663]

Behobene Probleme

Die Probleme, die in Build am 13. September 2022 behandelt werden.

- Beim Einladen einer IAM-Gruppe durch Auswahl von Azure AD als Identitätsanbieter werden die ADM-Rollen nicht unter **Benutzerdefinierter Zugriff** angezeigt, wenn sie Leerzeichen enthalten.

  [NSHELP-32557]

- Benutzer von Azure AD können sich nicht bei ADM anmelden, wenn ein Administrator sie vor ADM zu DaaS oder anderen NetScaler-Produkten hinzugefügt hat.

  [NSHELP-32556]

29. August 2022

Automatische Aktivierung von Gateway Insight und Kontoübernahme für NetScaler Gateway

Alle lizenzierten virtuellen NetScaler Gateway-Server werden jetzt automatisch mit **Account Takeover for NetScaler Gateway und GatewayInsight**aktiviert. In der NetScaler Console können Sie auf diese Weise Einblicke für Folgendes anzeigen:

- Account-Takeover-Angriffe für NetScaler Gateway unter **Sicherheit > Sicherheitsverletzungen**. Die Verfügbarkeit der NetScaler Gateway-Anmeldeseite wird für böswillige Bots zum einfachen Ziel, Benutzeranmeldeinformationen zu stehlen und Cyberangriffe wie das Ausfüllen von Anmeldeinformationen und das Sprühen Als Administrator möchten Sie möglicherweise analysieren, ob böswillige Bots versucht haben, das NetScaler Gateway-Konto zu übernehmen. Weitere Informationen finden Sie unter Kontoübernahme für NetScaler Gateway.
- Probleme im Zusammenhang mit virtuellen NetScaler Gateway-Servern in **Gateway > Gateway Insight**. Als Administrator möchten Sie möglicherweise die Gateway-Instanzen auf Erkenntnisse wie Benutzeranmeldeaktivitäten, Gründe für Anmeldefehler, aktive Benutzer, verfügbare Benutzer, Bot-Angriffe usw. überwachen. Weitere Informationen finden Sie unter Gateway Insight.

> **Hinweis**
>
> Die automatische Aktivierung für Gateway Insight und Account Takeover for NetScaler Gateway wird den Kunden schrittweise zur Verfügung gestellt.
>
> - In Ihrer NetScaler Console müssen ein oder mehrere externe NetScaler Agents konfiguriert sein und über ein oder mehrere Premium- oder Advanced Gateway-Geräte verfügen.
> - Nachdem diese Funktion in Ihrer NetScaler Console veröffentlicht wurde, werden alle

vorhandenen lizenzierten virtuellen NetScaler Gateway-Server und die nachfolgenden lizenzierten virtuellen NetScaler Gateway-Server automatisch mit Gateway Insight und Account Takeover for NetScaler Gateway aktiviert.

- Für alle virtuellen NetScaler Gateway-Server, die manuell mit der Option Gateway Insight deaktiviert wurden, wird Gateway Insight für diese virtuellen Server nicht automatisch aktiviert.
- So deaktivieren Sie die Option **Gateway Insight** :
  1. Navigieren Sie zu **Einstellungen > Lizenzierung und Analytics-Konfiguration**.
  2. Klicken Sie unter **Virtual Server Analytics-Zusammenfassung**auf **Analytics konfigurieren**.
  3. Wählen Sie auf der Seite **Alle virtuellen Server** den virtuellen NetScaler Gateway-Server aus und klicken Sie auf **Analytics bearbeiten**.
  4. Deaktivieren Sie die Option **Gateway Insight** und klicken Sie auf **Speichern**.
- Die **Kontoübernahme für NetScaler Gateway** wird automatisch deaktiviert, nachdem die Option **Gateway Insight** deaktiviert wurde.

[NSADM-82732]

Verbesserungen am einheitlichen Dashboard

Das einheitliche Dashboard unter **Übersicht > Dashboard** wurde jetzt mit kleineren Widgets für alle wichtigen Metriken in jeder Kategorie hinzugefügt. Wenn Sie auf **Dashboard bearbeiten**klicken, können Sie:

- 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.

Mit dieser Erweiterung können Sie die Dashboard-Ansicht anpassen, indem Sie die erforderlichen Widgets unter jeder Kategorie hinzufügen oder entfernen.

[NSADM-86337]

Wählen Sie ein Land aus der ausgewählten Region

Wenn Sie sich zum ersten Mal beim NetScaler Console-Dienst anmelden, können Sie jetzt ein Land auswählen, das Ihren Geschäftsanforderungen entspricht. Die Länder werden basierend auf der von

Ihnen ausgewählten Region angezeigt. Zuvor konnten Sie nur Regionen auswählen.

Wenn Sie beispielsweise die **EMEA-Region** auswählen, listet die GUI die folgenden Länder auf:

- Frankreich
- Vereinigtes Königreich
- Deutschland

Ebenso können Sie ein geeignetes Land aus anderen Regionen auswählen.

[NSADM-83643]

Web Insight – Details zu Problemen im Zusammenhang mit der Verschlüsselung anzeigen

Unter **Anwendungen > Web Insight**können Sie jetzt unter **SSL-Fehler**einen Drilldown der **Chiffrier-abweichung** durchführen, um Details wie den Namen der SSL-Verschlüsselung, die empfohlenen Aktionen und die Details der betroffenen Anwendungen und Clients anzuzeigen.

Weitere Informationen finden Sie unter Web Insight.

SNMP Version 3-Unterstützung für SDX-Konfiguration auf ADM

Sie können jetzt über die ADM-GUI ein SNMP v3-Profil für die NetScaler SDX-Instanz erstellen. Navigieren Sie zur Registerkarte **Infrastruktur > Instanzen > NetScaler > SDX**, und klicken Sie dann auf **Profile**. Sie können alle Profilparameter hinzufügen, **v3** als SNMP-Profiltyp auswählen und dann auf **Erstellen** klicken, um ein NetScaler SDX-Profil zu erstellen.

[NSADM-84828]

16. August 2022

Analytics

App-Dashboard – Zeigen Sie detaillierte Einblicke an, um Anwendungsprobleme zu beheben
Wenn Sie im **App-Dashboard**einen Drilldown einer Anwendung durchführen, können Sie jetzt die **empfohlenen Aktionen** für die folgenden Anwendungsprobleme anzeigen, mit denen Sie detaillierte Einblicke zur Behebung der Probleme anzeigen können:

- Reaktionszeit
- Aktive Dienste
- Instabiler Server
- Serviceklappen

Weitere Informationen finden Sie unter Leistungsindikatoren (Probleme).

[NSADM-84811]

Infrastruktur

Duale NIC-Unterstützung für ADM-Agent Sie können eine zweite Netzwerkkarte auf dem ADM-Agent konfigurieren, um den Zugriff auf die NetScaler Console zu verwalten. Mit der Dual-NIC-Architektur kann der ADM-Agent nun:

- Stellen Sie die Kommunikation zwischen ADM-Agent und ADC-Instanzen her
- Stellen Sie die Kommunikation zwischen dem ADM-Agent und dem ADM Service her

Weitere Informationen finden Sie unter Dual-NIC-Unterstützung in der NetScaler Console .

[NSADM-85781]

Erstellen Sie einen Cluster neu, der Teil der Google Cloud Autoscale-Gruppe ist Um die ADC-Cluster anzuzeigen und Fehler zu beheben, die Teil einer Google Cloud (GCP) Autoscale-Gruppe sind, können Sie jetzt zu **Infrastruktur > Public Cloud > Autoscale-Gruppe**navigieren und auf **Cluster anzeigen**klicken.

Sie können den **GCP-Cluster** auswählen und auf **Neu erstellen** klicken, um den vorhandenen Cluster zu löschen und durch einen neuen Cluster zu ersetzen. Alle Anwendungskonfigurationen werden auf den neuen ADC-Cluster übertragen.

Weitere Informationen finden Sie unter Anzeigen und Problembehandlung von ADC-Clustern.

[NSADM-75731]

Verwaltung und Überwachung

ADM-Agentdetails im einheitlichen Dashboard anzeigen Im vereinheitlichten Dashboard können Sie jetzt eine Übersicht der ADM-Agentdetails visualisieren. Unter **Übersicht > Dashboard**können Sie neben dem **ADM-Agentstatus**die Agents anzeigen, die verfügbar/nicht verfügbar sind.

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.

Weitere Informationen finden Sie unter Übersicht über das einheitliche Dashboard.

[NSADM-83096]

Behobene Probleme

- Nachdem Sie Analytics aktiviert oder Analysen für virtuelle NetScaler Gateway-Server bearbeitet haben, die über das HA-Paar konfiguriert wurden, werden die **Optionen auf Instanzebene** unter **Erweiterte Einstellungen (optional)** auch nach Aktivierung dieser Optionen deaktiviert angezeigt.

  [NSHELP-32188]

- Wenn Sie **unter Gateway > HDX Insight > Benutzer** einen Benutzer auswählen, zeigt ADM Details für alle Benutzer an, anstatt Details für den ausgewählten Benutzer anzuzeigen.

  [NSHELP-32181]

- Wenn Sie unter **Gateway > HDX Insight > Instanzen** auf ein Land klicken, um einen Drilldown für weitere Details durchzuführen, werden die Daten unter **Aktuelle Sitzungen** nicht angezeigt.

  [NSHELP-32125]

13. Juli 2022

Verwaltung und Überwachung

Unterstützung bei der Identifizierung und Behebung von CVE-2022-27509 Die Sicherheitsempfehlung von NetScaler Console unterstützt jetzt die Identifizierung und Behebung von CVE-2022-27509.

Die Identifizierung von CVE-2022-27509 erfordert eine Kombination aus Versionsscan und benutzerdefiniertem Scan, und die Behebung erfordert ein Upgrade der anfälligen ADC-Instanzen auf eine Version und einen Build, für die das Update vorhanden ist. Wenn Ihre anfälligen ADC-Instanzen die Datei `/etc/httpd.conf` in das Verzeichnis `/nsconfig` kopiert haben, lesen Sie Upgrade-Überlegungen zu benutzerdefinierten ADC-Konfigurationen, bevor Sie ein ADC-Upgrade planen.

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 .

Weitere Informationen dazu, wie ADM ADCs identifiziert, die für CVE-2022-27509 anfällig sind, und zu Schritten zur Behebung finden Sie unter Identifizieren und Korrigieren von Schwachstellen für CVE-2022-27509.

> **Hinweis**
>
> Es kann einige Stunden dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2022-27509 im Sicherheitsberatungsmodul berücksichtigt werden. Um die Auswirkungen früher zu erkennen, können Sie einen Anforderungsscan starten, indem Sie auf **Jetzt scannen**klicken.

[NSADM-85549]

Konfigurieren einer Zugriffsrichtlinie für Upgrade-Jobs Als Superadministrator können Sie jetzt eine Zugriffsrichtlinie konfigurieren, die Berechtigungen (Anzeigen/Bearbeiten) für die Upgrade-Jobs festlegen und die Richtlinie auf Ihre NetScaler Console-Benutzer anwenden. Klicken Sie unter **Einstellungen > Benutzer und Rollen > Zugriffsrichtlinien** auf **Hinzufügen**, um eine Zugriffsrichtlinie zu konfigurieren, indem Sie unter **Berechtigungen** die Option **Infrastruktur > Upgrade-Aufträge** auswählen.

Weitere Informationen finden Sie unter Konfigurieren von Zugriffsrichtlinien auf der NetScaler Console .

[NSADM-82494]

Unterstützung für Konfigurationsüberprüfung in NetScaler BLX-Instanzen im freigegebenen Modus Sie können jetzt Konfigurationsüberprüfungsvorlagen mit bestimmten Konfigurationen erstellen und die Konfigurationsänderungen in NetScaler BLX-Instanzen im freigegebenen Modus überwachen. Weitere Informationen finden Sie unter Erstellen von Überwachungsvorlagen.

[NSADM-82323]

Unterstützung für CSV-Format und Zeitplanexport in Web-Transaktionsanalysen In der **Web-Transaktionsanalyse**können Sie jetzt die folgenden Verbesserungen sehen, wenn Sie auf das **Exportsymbol** klicken:

- In **Jetzt exportieren**können Sie Daten im CSV-Format exportieren.
- Die Option **Export planen** wird eingeführt, mit der du die Daten im CSV-Format per E-Mail und Slack planen und exportieren kannst.

Weitere Informationen finden Sie unter Webtransaktionsanalyse.

Behobenes Problem

Wenn Sie im NetScaler Console Service zu **Infrastruktur > Instanzen > Agents** navigieren und auf Einstellungen klicken**,**um die Agent-Upgrade-Einstellungen zu ändern, wird eine Bestätigungsmeldung

Geänderte Agent-Upgrade-Einstellungen angezeigt, sobald die Einstellungen geändert wurden.

[NSHELP-32099]

29. Juni 2022

Anwendungen

Anwendung für mehrere benutzerdefinierten Anwendungen konfigurieren und zuordnen Im **Application Dashboard**können Sie jetzt eine Anwendung konfigurieren und sie mehreren benutzerdefinierten Anwendungen zuordnen. Mit dieser Funktion können Sie dieselbe Anwendung für mehrere benutzerdefinierte Anwendungen wiederverwenden, anstatt für jede benutzerdefinierte App eine separate Anwendung zu erstellen.

Weitere Informationen finden Sie unter Konfigurieren und Zuordnen einer Anwendung zu mehreren benutzerdefinierten Anwendungen.

[NSADM-82040]

Verwaltung und Überwachung

Unterstützte Browser für den Zugriff auf die NetScaler Console-GUI Auf die NetScaler Console-GUI kann jetzt nur von den folgenden kompatiblen Browserversionen aus zugegriffen werden:

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

[NSADM-83943]

15. Juni 2022

Infrastruktur

Überwachen Sie die Nutzung der NetScaler Agent-Systemparameter und beheben Sie Probleme mithilfe des Self-Heal-Daemons Der NetScaler Agent überwacht jetzt seine Systemressourcen

(CPU, Arbeitsspeicher und Datenträger), indem er den Self-Heal-Daemon automatisch im Hintergrund ausführt. Der Self-Heal-Daemon prüft in den folgenden Szenarien auf Schwellenwerte und wendet Aktionen automatisch an:

- Wenn die Datenträgernutzung für einen bestimmten Zeitraum 80% oder mehr übersteigt, wird die Aktion zum Bereinigen von Speicherplatz (Protokolle, Backupprotokolle, Kerndateien, Absturzdateien usw.) angewendet, um den Speicherplatz zurückzugewinnen.
- Wenn die Arbeitsspeicher- und CPU-Auslastung für eine bestimmte Dauer 90% oder mehr übersteigt, werden ADM-Prozesse neu gestartet, um die CPU und den Arbeitsspeicher zurückzugewinnen.

> **Hinweis**
>
> Der Self-Heal-Daemon überwacht die unter **Infrastruktur > Instanzen > Agents > Einstellungen > Benachrichtigung**konfigurierten Schwellenwerte nicht.

[NSADM-82558]

07. Juni 2022

Analytics

Bot- und WAF-Analysen für benutzerdefinierte Apps anzeigen Unter **Sicherheit > Sicherheitsverletzungen**können Sie jetzt unter **WAF** und **Bot**eine benutzerdefinierte App auswählen und die konsolidierten Anwendungsdetails anzeigen, die für eine benutzerdefinierte App gelten. Sie können auch eine Anwendung aus der Liste auswählen und Details für eine bestimmte Anwendung der benutzerdefinierten App anzeigen.

Weitere Informationen finden Sie unter Sicherheitsverletzungen.

[NSADM-77375]

Verwaltung und Überwachung

Importieren und installieren Sie das SSL-Zertifikatspaket (mit Zertifikatskette) über den Zertifikatsspeicher Wenn Sie unter **Infrastruktur > SSL-Dashboard**die Option **Zertifikatspeicher verwalten** aus der Liste neben **Einstellungen**auswählen, haben Sie folgende Möglichkeiten:

- Klicken Sie auf **ADC-Zertifikate importieren > Abfrage starten**. Das SSL-Zertifikatpaket wird zusammen mit der Zertifikatkette, die das Serverzertifikat mit seinem Aussteller (der Zwischenzertifizierungsstelle) verknüpft, aus der ADC-Instanz in den Zertifikatsspeicher importiert.

- Zeigen Sie die Zertifikate im Zertifikatspeicher an, wählen Sie ein Zertifikat aus und klicken Sie auf **Installieren**, um das Zertifikat zusammen mit der Zertifikatkette auf den ausgewählten ADC-Instanzen zu installieren.

[NSADM-82727]

Upgrade-Unterstützung für NetScaler BLX-Instanzen Unter **Infrastruktur > Upgrade-Jobs**können Sie jetzt einen Auftrag zum Upgrade von NetScaler BLX-Instanzen erstellen. Sie müssen das entsprechende Build-Image (gilt für Ubuntu oder Red Hat) für ein erfolgreiches Upgrade auswählen. Weitere Informationen finden Sie unter Wartungsaufträge.

[NSADM-82324]

Behobenes Problem

Unter **Infrastruktur > Ereigniszusammenfassung > Syslog-Meldungen**wurden die Daten nur für die letzten 30 Tage angezeigt. Mit diesem Fix werden die Daten bis zu 180 Tage lang angezeigt.

[NSHELP-30961]

10. Mai 2022

Analytics

Exportieren Sie Echtzeitdaten nach Splunk Die Integration von NetScaler Console mit Splunk ermöglicht es Ihnen jetzt, Echtzeitdaten nach Splunk zu exportieren. Wenn Sie in der ADM-GUI die Option **Realtime Export** auswählen und konfigurieren, werden die ausgewählten Verstöße in der NetScaler Console sofort an Splunk übertragen.

Weitere Informationen finden Sie unter Integration mit Splunk.

[NSADM-84529]

Verbesserungen der WAF-Lernmaschine In NetScaler Console können Sie jetzt ein Lernprofil konfigurieren und die Entspannungsregeln für die folgenden zusätzlichen Sicherheitsüberprüfungen bereitstellen oder überspringen:

- **JSON SQL**
- **JSON-Befehlseinschleusung**
- **JSON XSS**

> **Hinweis**
>
> Um ein Lernprofil mithilfe dieser Sicherheitsüberprüfungen zu konfigurieren, muss die NetScaler-Instanz 13.1–14.10 oder höher sein.

Weitere Informationen finden Sie unter WAF Learning Engine.

[NSADM-80921]

Anwendungen

Verbesserungen am einheitlichen Dashboard Das vereinheitlichte **Dashboard unter Übersicht > Dashboard** ermöglicht es Ihnen jetzt, es nach Ihren Wünschen anzupassen. Mit der Option **Dashboard bearbeiten** können Sie:

- Widgets ziehen
- Widgets entfernen
- Widgets hinzufügen
- Auf Standard zurücksetzen

Klicken Sie nach den Änderungen auf **Speichern**.

> **Hinweis**
>
> Standardmäßig werden alle Widgets angezeigt. Wenn Sie das Dashboard angepasst, die Änderungen gespeichert und die Option Auf Standard zurücksetzen verwenden, wird das zuletzt gespeicherte angepasste Dashboard wiederhergestellt.

[NSADM-52144]

Infrastruktur

Verbesserungen der ADM-GUI Sie können jetzt das ADM-GUI-Navigationsmenü einzeln erweitern oder reduzieren. Diese Verbesserung ermöglicht es Ihnen, alle Optionen in jedem Abschnitt anzuzeigen.

[NSADM-85480]

Unterstützung bei der Identifizierung und Behebung von CVE-2022-27507 und CVE-2022-22508
Die Sicherheitsempfehlung von NetScaler Console unterstützt jetzt die Identifizierung und Behebung von zwei neuen CVEs: **CVE-2022-27507** und **CVE-2022-22508**.

- Die Identifizierung von **CVE-2022-27507** erfordert eine Kombination aus einem Versionsscan und einem Konfigurationsscan, und die Behebung erfordert ein Upgrade der anfälligen ADC-Instanzen auf eine Version und einen Build, die das Update enthalten.

  ADM Security Advisory unterstützt keine Risikominderung. Wenn Sie die Schadensbegrenzung (temporäre Problemumgehung) auf die ADC-Instanz angewendet haben, identifiziert ADM den ADC weiterhin als anfällig, bis Sie die Standardisierung abgeschlossen haben.

  Für **CVE-2022-27507**identifiziert ADM Security Advisory den ADC weiterhin als anfällig, selbst wenn Sie die Risikominderung angewendet und HDX Insight for EDT-Datenverkehr vorübergehend deaktiviert haben (siehe Security Bulletin), bis Sie die Standardisierung abgeschlossen haben (Upgrade auf eine Version und den Build, der reparieren).

- Die Identifizierung von **CVE-2022-27508** erfordert eine Kombination aus einem Versionsscan und einem Konfigurations-Scan, und die Behebung erfordert ein Upgrade der anfälligen ADC-Instanzen auf eine Version und einen Build, die das Update enthalten.

  Weitere Informationen zur Behebung von CVE-2022-27507 und CVE-2022-22508 finden Sie in der Sicherheitsempfehlung.

  > **Hinweis**
  >
  > Es kann einige Stunden dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von **CVE-2022-27507** und **CVE-2022-27508** im Sicherheitsberatungsmodul widerspiegelt. Um die Auswirkungen früher zu erkennen, können Sie einen Anforderungsscan starten, indem Sie auf **Jetzt scannen**klicken.

[NSADM-85673]

Behobenes Problem

Wenn Sie unter **Infrastruktur > Instanzen > NetScaler** ein Administratorprofilkennwort ändern und % in das Kennwort aufnehmen, wird eine Fehlermeldung angezeigt.

[NSHELP-31392]

27. April 2022

Verwaltung und Überwachung

ADC-Downgrade über ADM GUI mit der richtigen Datei `ns.conf` Wenn Sie unter **Infrastruktur > Upgradejobs** einen Upgradejob erstellen, um die ADC-Instanz auf eine niedrigere Version zu aktualisieren, wählt ADM jetzt die kompatible Datei `ns.conf` aus, aus der die Konfiguration auf die ADC-Instanz angewendet wird. Die ausgewählte Datei `ns.conf` muss dieselbe oder eine niedrigere Ver-

sion als die vom Benutzer ausgewählte Version haben. Wenn in der ADC-Instanz keine geeignete Datei `ns.conf` vorhanden ist, ist ein Downgrade nicht zulässig und die entsprechende Fehlermeldung wird angezeigt.

[NSADM-81421]

Behobene Probleme

- Wenn Sie **Advanced Security Analytics**aktivieren, ein Profil mit einer oder mehreren verhaltensbasierten Verstößen anwenden und auf **Speichern**klicken, werden die Details in der Tabelle nicht **unter Einstellungen > Lizenzierung & Analytics-Konfiguration > Alle virtuellen Server**angezeigt.

  Hinweis: Die verhaltensbasierten Verstöße sind übermäßige Clientverbindungen, ungewöhnlich große Upload-Transaktionen, ungewöhnlich große Download-Transaktionen und ungewöhnlich hohe Anforderungsraten.

  [NSADM-85020]

- Unter **Infrastruktur > Ereigniszusammenfassung > Syslog-Meldungen**wurden die Daten nur für die letzten 30 Tage angezeigt. Mit diesem Fix werden die Daten bis zu 180 Tage lang angezeigt.

  [NSHELP-30961]

12. April 2022

Analytics

Neue Verstöße für Bot-Verstöße gegen Ratenbegrenzung hinzugefügt Die Ratenbegrenzungsregel erkennt mehrere Anfragen, die vom selben Client kommen. Unter **Sicherheit > Sicherheitsverletzungen > Anwendungsübersicht** unter **Bot** können Sie nun die folgenden Verstoßdetails anzeigen:

- **URL**
- **Quell-IP**
- **Geo-Standort**
- **Sitzungsfortbestehen**

Klicken Sie auf **Protokolle**, um Details wie Uhrzeit, Client-IP, Bot-Typ, Bot-Erkennung usw. anzuzeigen. Weitere Informationen finden Sie unter Details zu Bot-Verstößen anzeigen.

[NSADM-80925]

Unterstützung für Headless-Browserverletzungen bei Bot-Ver Unter **Sicherheit > Sicherheitsverletzungen > Anwendungsübersicht**unter **Bot**können Sie jetzt Details zu **Headless-Browserverletzungen** anzeigen. Klicken Sie auf **Protokolle**, um Details wie Uhrzeit, Client-IP, Bot-Typ, Bot-Erkennung usw. anzuzeigen.

Weitere Informationen finden Sie unter Details zu Bot-Verstößen anzeigen.

[NSADM-89027]

Verwaltung und Überwachung

CVE-2022-21827 fällt nicht in den Anwendungsbereich der NetScaler Console Security Advisory CVE-2022-21827 wirkt sich auf die unterstützten Versionen des NetScaler Gateway-Plug-Ins für Windows vor 21.9.1.2 aus.

Die Erkennung und Behebung von Sicherheitslücken, die sich auf das NetScaler Gateway-Plug-In für Windows auswirken, wird von der NetScaler Console 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 fallen die Erkennung und Behebung dieser Sicherheitsanfälligkeit nicht in den Geltungsbereich der NetScaler Console Security Advisory.

Weitere Informationen finden Sie unter Nicht unterstützte CVEs in Security Advisory.

Abmeldeoption in an Kunden gesendeten Produkt-E-Mails verfügbar Kunden (Neukunden und Inaktive) haben jetzt die Möglichkeit, alle E-Mail-Benachrichtigungen in den von NetScaler Console gesendeten Produkt-E-Mails abzubestellen. Weitere Informationen zum An- oder Abbestellen finden Sie unter E-Mail-Abonnements.

[NSADM-83272]

Filter im App-Dashboard beibehalten Wenn Sie unter **Anwendungen > Dashboard** Filter über die Suchleiste und wichtige Metriken anwenden, werden die Filter jetzt beibehalten. Sie können dieselben Filter auch dann anzeigen, wenn:

- Sie kehren von einer anderen Navigation innerhalb der ADM-GUI zu **Anwendungen > Dashboard** zurück.
- Sie schließen den Browser und öffnen eine neue Sitzung im selben Browser.

> **Hinweis**
>
> Die Filter werden nicht beibehalten, wenn Sie eine neue Sitzung in einem anderen Browser oder in einem Inkognito-Modus öffnen.

[NSADM-82038]

StyleBooks

Automatische Aktualisierung von Konfigurationspaketen Wenn ein SSL-Zertifikat im NetScaler Console-Zertifikatsspeicher aktualisiert wird, werden die mit dem SSL-Zertifikat verknüpften Konfigurationspakete automatisch aktualisiert.

[NSADM-80694]

31. März 2022

Analytics

Verbesserungen an erweiterten Sicherheitsanalysen bei Sicherheitsverletzungen Als Verbesserung der Funktion Advanced Security Analytics wurde der Prozess, zuerst **Advanced Security Analytics** zu aktivieren und dann ein Profil mithilfe des Symbols **Einstellungen** zu erstellen, jetzt vereinfacht. Sie können jetzt **Advanced Security Analytics**aktivieren, ein Profil erstellen und das Profil den virtuellen Servern in einem einzigen Workflow zuweisen.

Weitere Informationen finden Sie unter Aktivieren erweiterter Sicherheitsanalysen.

[NSADM-81383]

Verbesserungen am einheitlichen Dashboard Unter **Übersicht > Dashboard**können Sie jetzt die folgenden Verbesserungen anzeigen:

- Sie können auf die Anzahl der Schlüsselmetriken unter allen Kategorien klicken, um Details der betroffenen ADC-Instanz/Anwendung/Gateway anzuzeigen.
- Unter **Anwendungen**wurden geringfügige GUI-Änderungen an SSL-Schlüsselmetriken vorgenommen, um mehr Informationen zu visualisieren.
- Unter **Gateway**zeigt die **Users Geo Distribution** die drei wichtigsten Länder basierend auf den Benutzerzahlen an.

[NSADM-82758]

Verwaltung und Überwachung

Unterstützung des ECDSA-Algorithmus im SSL-Dashboard Wenn Sie eine Unternehmensrichtlinie im **SSL-Dashboard > Einstellungen > Unternehmensrichtlinie**konfigurieren, können Sie jetzt **ECDSA** im **empfohlenen Signaturalgorithmus**auswählen.

Weitere Informationen zu ECDSA finden Sie unter ECDSA Cipher Suites support.

Weitere Informationen zur Konfiguration von Unternehmensrichtlinien finden Sie unter Konfigurieren einer Unternehmensrichtlinie.

[NSADM-71321]

Onboarding

ADM-Unterstützung für Kubernetes Version 1.23 NetScaler Console unterstützt jetzt das Hinzufügen und Verwalten von Clustern mit Kubernetes Version 1.23.

[NSADM-83683]

16. März 2022

Onboarding

Testen Sie die Onboarding-Bereitschaft von ADC-Instanzen Wenn Sie eine ADC-Instanz mithilfe der Standard-Built-Agent-Option in die NetScaler Console einbinden möchten, können Sie einen Testlauf durchführen, um sicherzustellen, dass die ADC-Instanz für das Onboarding bereit ist. Weitere Informationen finden Sie unter Testen der Onboarding-Bereitschaft von ADC-Instanzen.

[NSADM-80502]

01. März 2022

Verwaltung und Überwachung

Laden Sie Benutzer oder Gruppen aus Azure AD zu ADM ein Als Superadministrator können Sie jetzt Benutzer oder Gruppen vom verbundenen Azure AD zur NetScaler Console zur NetScaler Console einladen. Stellen Sie zuvor sicher, dass Azure AD mit Citrix Cloud verbunden ist. Weitere Informationen finden Sie unter Verbinden von Azure Active Directory mit Citrix Cloud. Zuvor konnten Sie nur Benutzer mit Citrix Identity einladen.

Wenn Sie Azure AD als Identitätsanbieter auswählen, können Sie nur benutzerdefinierten Zugriff für den ausgewählten Benutzer oder die ausgewählte Gruppe angeben. Die Benutzer können sich mit

ihren Azure AD-Anmeldeinformationen bei NetScaler Console anmelden. Mit dieser Funktion müssen Sie keine Citrix Identity für die Benutzer erstellen, die Teil des ausgewählten Azure AD sind. Wenn ein Benutzer zur eingeladenen Gruppe hinzugefügt wird, müssen Sie keine Einladung für den neu hinzugefügten Benutzer senden. Dieser Benutzer kann mit den Azure AD-Anmeldeinformationen auf NetScaler Console zugreifen.

[NSADM-81039]

In ADC hochgeladene Zertifikate und Schlüsseldateien werden von ADM gespeichert und die Informationen werden in der ADM-Datenbank gespeichert Wenn Sie Zertifikate und Schlüsseldateien über das **SSL-Dashboard** in der ADM Service-GUI in den Cert Store hochladen, werden nur die Metadaten und der verschlüsselte Inhalt der Zertifikatsdatei in der ADM-Datenbank gespeichert. Der Schlüssel und das Kennwort, mit denen der Inhalt entschlüsselt wurde, werden in Cloud Wallet gespeichert.

[NSADM-72475]

Neue Netzwerkberichte in ADM Die folgenden neuen Netzwerkberichte werden als Gesamtzähler hinzugefügt:

- **Authentifizierung erfolgreich im Vergleich zu Fehlern**
- **HTTP-Authentifizierungserfolg gegenüber Fehlern**
- **Erfolg der Nicht-HTTP-Authentifizierung im Vergleich zu Fehlern**
- **AAA-Sitzungen**
- **Aktuelle AAA-Sitzungen**
- **Aktuelle ICAOnly-Sitzungen**
- **Aktuelle ICAOnly-Verbindungen**
- **Aktuelle ICA-Verbindungen (Smart Access)**

Sie können diese Zähler verwenden, um Schwellenwerte hinzuzufügen und Benachrichtigungen zu erhalten. Weitere Informationen finden Sie unter Netzwerkberichte.

[NSADM-62239]

Aktionsrichtlinie – Konfiguration von Bot- und WAF-Benachrichtigungen mit Transaktionsdetails Wenn Sie in **Aktionsrichtlinien**eine Aktionsrichtlinie konfigurieren, können Sie jetzt die Optionen **Bot-Verletzung pro Client** und **WAF-Verletzung pro Client** auswählen. Mit diesen Optionen können Sie Benachrichtigungen mit Transaktionsdetails wie Client-IP, Gesamtzahl der Angriffe, Verstoßart usw. konfigurieren und empfangen.

Weitere Informationen finden Sie unter Konfigurieren einer Aktionsrichtlinie für den Empfang von Benachrichtigungen über Anwendungsereignisse.

[NSADM-80630]

Deaktivieren Sie benutzerdefinierte Scans von Security Advisory Mit der Benutzeroberfläche des NetScaler Application Delivery Management Service können Sie jetzt benutzerdefinierte Scans mit Sicherheitsempfehlungen deaktivieren. Wenn Sie diese benutzerdefinierten Scans von Security Advisory deaktivieren, werden die Auswirkungen der CVEs, die einen benutzerdefinierten Scan benötigen, für Ihre ADC-Instanzen im Security Advisory nicht bewertet.

Informationen zum Deaktivieren benutzerdefinierter Scans von Security Advisory finden Sie unter Benutzerdefinierte Sucheinstellungen.

[NSADM-80288]

StyleBooks

Verwenden Sie HTML-Formatierungs-Tags in der StyleBook-Beschreibung und in In der **StyleBook-Definition** können Sie jetzt ein Header-Feld einbinden und HTML-Formatierungs-Tags für den Text verwenden. Sie können auch Bilder als Teil der Kopfzeile hinzufügen. Diese werden oben im Konfigurationsformular wiedergegeben. Mit dieser Funktion können Sie Infografiken für StyleBook-Benutzer hinzufügen, die das Verständnis der StyleBook-Konfiguration erleichtern. Wenn Sie Bilder in der Kopfzeile verwenden, stellen Sie sicher, dass das base64-codierte Bildformat im `image`-Tag verwendet wird.

```
name: app-stylebook-with-HTML-tags
namespace: com.examples.stylebooks
version: `1.0`
display-name: `Example App StyleBook`
header: 'This <b> StyleBook </b> defines all the app configuration for
    <i>Load Balanced Application </i>. The following image describes the
     target deployment for the app <img id=`b64img` src=`data:image/png;
    base64,` />'
```

[NSADM-80699]

Stellen Sie Autoscale-Anwendungen bereit, die sich außerhalb des virtuellen Netzwerks oder der VPC der ADC-Instanzen befinden Wenn sich Anwendungsserver und ADC-Instanzen in verschiedenen virtuellen Netzwerken, VPC-Netzwerken und Subnetzen befinden, stellen Sie den CIDR-Block eines Subnetzes oder einer VPC bereit, in dem sich Anwendungsserver befinden. Geben Sie den CIDR-Block im Feld **Ursprungsserver** an, während Sie die Bereitstellungsparameter konfigurieren. Auf diese Weise können Sie Apps von den Anwendungsservern bereitstellen, die sich außerhalb des virtuellen Netzwerks oder VPC-Netzwerks der ADC-Instanzen befinden.

Früher war diese Funktion nur für die Autoscale-Gruppen in AWS verfügbar. Jetzt können Sie diese Funktion auch in Azure und Google Cloud verwenden.

Weitere Informationen:

- Microsoft Azure.
- Google Cloud.

[NSADM-78617]

10. Februar 2022

Verwaltung und Überwachung

Unterstützung für die ShowConfiguration-Vorlage Wenn Sie im Konfigurationseditor **Batch-Konfiguration** auswählen, können Sie jetzt die Vorlage **ShowConfiguration** verwenden. Ziehen Sie die Vorlage **ShowConfiguration** in den rechten Bereich und geben Sie die show-Befehle ein, die auf NetScaler-Instanzen ausgeführt werden sollen.

Sie können beispielsweise Befehle wie `sh ns info`, `sh node`, `sh ns stats`, `sh interface` und `shell ls /var/tmp` eingeben und die Ausgabe anzeigen.

Sie können die Ausgabe der Befehle als Textdatei herunterladen.

[NSADM-66132]

Konfigurieren einer Aktionsrichtlinie, um Benachrichtigungen über Anwendungsereignisse Neben der vorhandenen Analyseansicht von Anwendungsereignissen können Sie eine Aktionsrichtlinie konfigurieren, um Benachrichtigungen über Anwendungsereignisse über Slack, E-Mail, PagerDuty oder ServiceNow zu erhalten. Zu den Anwendungsereignissen gehören Leistungsprobleme, Bot- und WAF-Verstöße sowie Service-Graph-Verstöße. Als Administrator können Sie mithilfe der Aktionsrichtlinie Ereignisbenachrichtigungen in Echtzeit erhalten.

Mit der Aktionsrichtlinie können Sie:

- Definieren Sie bestimmte Bedingungen für die Anwendungsereignisse.
- Lassen Sie sich über Slack, E-Mail, PagerDuty und ServiceNow über die folgenden Ereignisse benachrichtigen:
  - **WAF-SQL-Verstoß**
  - **Verstoß gegen WAF XSS**
  - **WAF-Infer-XML-Verletzung**

> **Hinweis**
>
> Um die Benachrichtigung über einen WAF-Verstoß zu erhalten, müssen die Mindesttransaktionen bei Verstößen 20% betragen. Beispielsweise müssen von 100 Transaktionen mindestens 20 Verstöße gegen Transaktionen sein.

- **Die 3 häufigsten Verstöße gegen die WAF**

  (Die Gesamtzahl der Verstöße, die von SQL, XSS und XML zusammen verursacht wurden, muss 30% betragen. Beispielsweise müssen von 100 Transaktionen 30 oder mehr Transaktionen eine Kombination aus SQL-, XSS- und Infer-XML-Verstößen sein.)

- **Bot-Verstöße**

  (Weitere Informationen zur Liste der Bot-Verstöße finden Sie unter Kategorien von Verstößen.)

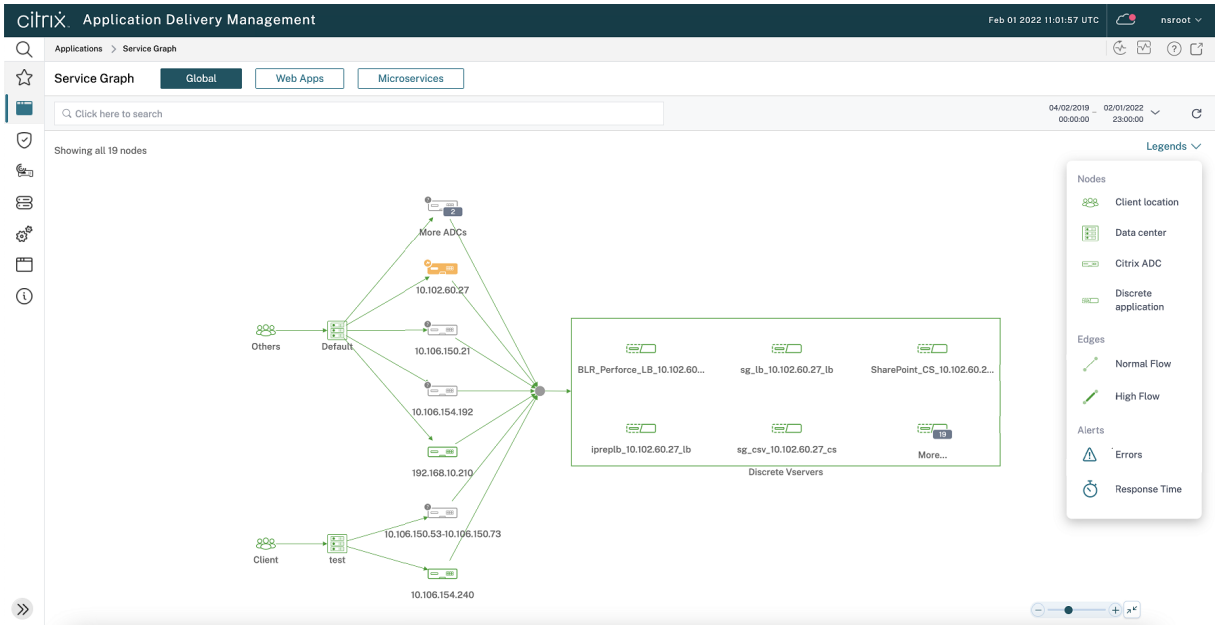
- **Verstoß gegen App-Score**
- **Netzwerklatenz des Clients**
- **Servernetzwerklatenz**
- **Verarbeitungszeit des Servers**
- **Verstoß gegen das Service-Diagramm**

Weitere Informationen finden Sie unter Konfigurieren einer Aktionsrichtlinie für den Empfang von Benachrichtigungen über Anwendungsereignisse.

[NSADM-70968], [NSADM-76588], [NSADM-72799]

Anwendungen

Verbesserungen des Service-Graphen Im globalen Service-Graph und im Microservices-Servicegraph können Sie jetzt die Legende anzeigen, die die Beschreibung der im Servicegraphen verfügbaren Symbole enthält.



[NSADM-82077]

Onboarding

Einstellungen für berührungslose Onboarding-Workflow-E-Mails konfigurieren Als Teil des auf ADM Service Connect basierenden Low-Touch-Onboarding-Workflows erhalten Sie produktinitiierte E-Mails vom NetScaler Console-Dienst. Sie können die E-Mails, die Sie im Rahmen dieses Workflows erhalten, auf folgende Weise konfigurieren und verwalten:

- E-Mails für alle Admins aktivieren
- E-Mails für ausgewählte Admins aktivieren/deaktivieren
- E-Mails für alle Admins deaktivieren

Weitere Informationen zum Konfigurieren und Verwalten von E-Mails finden Sie unter E-Mail-Einstellungen.

[NSADM-80289]

Sehen Sie sich die NetScaler Agent-Diagnose an und erhalten Sie Warnmeldungen für die Endpunktverifizierung NetScaler Console führt jetzt in regelmäßigen Abständen (alle eine Stunde) eine Diagnoseüberprüfung für den NetScaler Agent durch und stellt die folgenden Informationen bereit:

- **Erreichbarkeit der End**
- **Sonde zur Gesundheitsprüfung**

- **Agent-Proxy**

Wenn sich der Erreichbarkeitsstatus des Agentendpunkts ändert (von **OK** zu **Needs Review**), erhält der Superadministrator eine E-Mail-Benachrichtigung mit den Details zum Problem.

Weitere Informationen finden Sie unter Anzeigen der Agentdiagnose und Empfangen von Warnungen für die Endpunktüberprüfung.

[NSADM-69407]

StyleBooks

Aktualisierungen des StyleBook-Konfigurationspakets werden automatisch abgeglichen Manchmal kann das Aktualisieren eines StyleBook-Konfigurationspakets, das auf einer ADC-Instanz bereitgestellt wird, Unterschiede zum bereitgestellten Status aufweisen. In solchen Fällen schlägt das Update des Konfigurationspakets fehl. Die StyleBook-Engine gleicht diese Unterschiede nun automatisch aus und aktualisiert das Konfigurationspaket. Zuvor wurde auf der GUI eine Meldung angezeigt, die Ihre Bestätigung benötigte, um die Änderungen abzugleichen, bevor das Konfigurationspaket aktualisiert wurde.

[NSADM-80660]

Datenquellen in ADM verwalten Das Definieren einer Datenquelle in NetScaler Console hilft Ihnen, Daten aus externen Quellen als Eingabe beim Erstellen oder Aktualisieren von StyleBook-Konfigurationen zu verwenden. Andernfalls müssen Sie jede vom StyleBook benötigte Eingabe explizit angeben. In NetScaler Console können Sie jede verwaltete ADC-Instanz als Datenquelle für die Eingabe in eine StyleBook-Konfiguration verwenden. In NetScaler Console können Sie die verwalteten ADC-Instanzen als Datenquellen verwenden. Sie können auch benutzerdefinierte Datenquellen definieren, die als Eingabe beim Erstellen oder Aktualisieren von Konfigurationen dienen können. Um benutzerdefinierte Datenquellen anzuzeigen, gehen Sie zu **Anwendungen > Konfiguration > Datenquellen**.

Verwenden Sie den integrierten Typ `datum` in der StyleBook-Definition, um eine Datenquelle zu definieren.

Beispiel:

```
parameters:
  -
    name: selected-lb
    label: Select an existing ADC
    type: datum
    required: true
    data-source:
      type: managed-adc
```


In diesem Beispiel wird der Parameter `datum` verwendet, um die Datenquelle `managed-adc` zu definieren. Mit dieser Datenquelle können Sie Daten von den ADC-Instanzen abrufen, die von NetScaler Console verwaltet werden.

[NSADM-80659]

Überprüfen Sie die StyleBook-Kompatibilität für ein Konfigurationspaket Wenn Sie das StyleBook für ein Konfigurationspaket in der ADM-GUI ändern, können Sie die Änderungen nun anhand der neu ausgewählten StyleBook-Definition ermitteln. Und wie sich diese Änderungen auf das Konfigurationspaket auswirken. Mit diesen Informationen können Sie die StyleBook-Definition aktualisieren, bevor Sie sie ändern. Sie können auch entscheiden, mit dem vorhandenen StyleBook fortzufahren.

Wenn Sie beispielsweise das StyleBook für ein Konfigurationspaket ändern, kann das vorhandene StyleBook einen zulässigen Port HTTPS haben, während das neu ausgewählte StyleBook SSL haben kann. In diesem Fall müssen Sie möglicherweise dieselben HTTPS-Werte auch für den SSL-Port bearbeiten.

[NSADM-80664]

25. Januar 2022

ADC Low-Touch-Onboarding in ADM – Automatische Diagnose anzeigen

Die folgenden Informationen gelten nur für die ADC-Instanzen, die über die ADM-Dienstverbindungsfunktion mit dem ADM Service verbunden sind.

Zuvor gab es einen manuellen Prozess zur Verwendung des Diagnosetools zur Behebung der Low-Touch-Onboarding-Probleme. Jetzt können Sie auch Diagnoseinformationen zu den ADC-Instanzen, die Probleme beim Low-Touch-Onboarding haben, auf der ADM-GUI anzeigen.

Wenn Sie sich im ADM Service Connect-basierten Low-Touch-Onboarding-Workflow befinden, können Sie auf der Seite **Asset-Inventar** die neu hinzugefügte Option **Onboarding Readiness** sehen, die den Onboarding-Bereitschaftsstatus der ADC-Instanz wie **Needs Review** oder **OK**bereitstellt.

Sie können diese Ansicht auch anzeigen, indem Sie zu **Infrastruktur > Instanzen > NetScaler** navigieren und auf die Option **Asset-Inventar** klicken.

Sie können diese Informationen dann verwenden, um die Probleme zu verstehen und zu lösen.

Weitere Informationen finden Sie unter Problembehandlung mit dem Diagnosetool oder der ADM-GUI.

[NSADM-77245]

Unterstützung für Low-Touch-Onboarding von Kunden, die noch nicht in der Citrix Cloud

Im Rahmen des Low-Touch-Onboardings von NetScaler-Instanzen mithilfe des ADM Service Connect-Workflows können sich Kunden, die noch nicht in der Citrix Cloud sind, jetzt bei der Citrix Cloud anmelden und ihre ADC-Instanzen problemlos in ADM Service integrieren. Diese Kunden erhalten eine E-Mail vom NetScaler Console Service, in der sie zum **Onboard to ADM Service** weitergeleitet werden. Durch Klicken auf diese Schaltfläche können sie sich dann bei Citrix Cloud anmelden und ihre ADC-Instanzen mithilfe des Low-Touch-Onboarding-Workflows beim ADM Service integrieren. Weitere Informationen finden Sie unter Low-Touch-Onboarding von NetScaler-Instanzen mithilfe von Service Connect.

[NSADM-76466]

Infrastructure Analytics – Benachrichtigungen für bestimmte Probleme konfigurieren

In **Infrastructure Analytics**können Sie jetzt die erforderlichen Probleme auswählen, Benachrichtigungen für Probleme aktivieren, die die konfigurierten Schwellenwerte überschreiten, und Benachrichtigungen nur für die ausgewählten Probleme erhalten. Zuvor gingen Benachrichtigungen für alle Probleme ein. Diese Erweiterung ermöglicht es Ihnen, Benachrichtigungen nur für die ausgewählten Probleme zu erhalten, die Sie überwachen möchten.

Weitere Informationen finden Sie unter Benachrichtigungen konfigurieren.

[NSADM-76361]

17. Januar 2022

ADM-Unterstützung für BLX-Cluster

Sie können jetzt den BLX-Cluster in ADM hinzufügen. In der ADM-GUI wird die Cluster-IP-Adresse (CLIP) hinzugefügt und die Anzahl der Clusterknoten ist jetzt im Dashboard sichtbar.

[NSADM-78588]

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 Ein einheitliches Dashboard zum Anzeigen der Details der Instanzschlüsselmetrik.

[NSADM-74075]

Sicherheitsverletzung - JSON SQL Injection Grammar

Unter **Sicherheit > Sicherheitsverletzungen**unter **WAF**können Sie jetzt die **JSON-SQL-Injection-Grammatikverletzung** für die ausgewählte Anwendung anzeigen. Weitere Informationen finden Sie unter Details zu Verstößen.

[NSADM-62909]

Verwenden Sie die reservierten Schlüsselwörter des StyleBook für Parameter und Ausdrücke

Sie können jetzt die reservierten Schlüsselwörter verwenden, wenn Sie Parameter und Ausdrücke in einer StyleBook-Definition definieren. Die reservierten Schlüsselwörter lauten wie folgt:

```
"and", "false", "in", "not", "true", "or"
```

Zum Beispiel ist ein Parameter namens `not` jetzt ein gültiger Parameter (`$parameters.not`).

[NSADM-80657]

StyleBooks unterstützen verschachtelte Parameterbedingungen

In einer StyleBook-Definition können Sie jetzt eine Parameterbedingung innerhalb einer Parameterbedingung angeben. Diese Bedingungen werden als verschachtelte Parameterbedingungen bezeichnet und verwenden ein Wiederholungskonstrukt, um diese Bedingungen zu definieren. Die Bedingungen für verschachtelte Parameter sind nützlich, wenn Sie eine Aktion auf jedes Element eines Listenparameters anwenden möchten.

Beispiel:

```
parameters-conditions:
  -
    repeat: $parameters.lbvservers
    repeat-item: lbvserver
    parameters-conditions:
      -
        target: $lbvserver.port
```



```
8           action: set-allowed-values
9           condition: $lbvserver.protocol == "HTTPS"
10          value: $parameters.ssl-ports
```

In diesem Beispiel werden die Portwerte dynamisch aufgefüllt, wenn der Benutzer das HTTPS-Protokoll für einen virtuellen Lastausgleichsserver auswählt. Und es gilt für jeden virtuellen Lastausgleichsserver in der Liste.

Weitere Informationen finden Sie unter Bedingungen für verschachtelte Parameter.

[NSADM-62747]

Behobenes Problem

Wenn Sie in einem GSLB-Setup denselben Domänennamen für mehrere ADC-Instanzen haben, aktualisiert die Entitätsabfrage die Datenbank falsch.

[NSHELP-29885]

Bekannte Probleme

July 17, 2024

Bei NetScaler Application Delivery Management (NetScaler Console) sind die folgenden Probleme bekannt:

Verwaltung und Überwachung

Wenn Sie unter **Infrastruktur > SSL-Dashboard > Zertifikatsspeicher verwalten auf**NetScaler-Zertifikate**importieren** klicken, importiert NetScaler Console keine NetScaler-Zertifikate im PFX-Format.

[NSHELP-34803]

Infrastruktur

- 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]

- Wenn eine Ereignisregel erstellt wird und einige Entitäten unter **Infrastruktur > Ereignisse > Regeln > Regel erstellen > Fehlerobjekte auswählen** ausgewählt wurden, werden nicht alle ausgewählten Entitäten angezeigt. Dieses Problem tritt auf, wenn eine große Anzahl virtueller Server, Dienste oder Dienstgruppen vorhanden ist.

  Umgehung: Wenden Sie sich an das NetScaler Support-Team, um Unterstützung bei diesem Problem zu erhalten.

  [NSADM-110553]

Datencompliance

January 26, 2024

PCI-DSS-Compliance

Der Payment Card Industry (PCI) Data Security Standard (DSS) ist ein Sicherheitsstandard der Kreditkartenbranche, der ein erforderliches Sicherheitsniveau für Personen, Prozesse und Technologien definiert, das bei der Speicherung, Verarbeitung oder Übertragung von Kreditkartendaten vorhanden sein muss. PCI DSS gilt für Händler, Prozessoren und Dienstleister sowie für alle anderen Unternehmen, die Kreditkartendaten speichern, verarbeiten oder übertragen. Die PCI DSS Attestation of Compliance (AOC) ist letztlich eine Bescheinigung eines Unternehmens, dass ein bestimmtes Sicherheitsniveau erforderlich ist und besteht.

PCI Security Standards Council ™
PARTICIPATING ORGANIZATION

PCI-DSS-Konformität mit dem NetScaler Application Delivery Management Service

Der NetScaler Application Delivery Management (ADM) -Service hat die PCI DSS-Konformität erfolgreich erreicht. Die Bewertung erfolgte anhand der PCI-DSS-Compliance-Kontrolldomänen für Kunden. Der NetScaler Console-Dienst speichert, verarbeitet und überträgt keine Kunden-PCI-Daten. NetScaler Console Service wird außerdem jährlich einer PCI DSS-Bewertung durch einen Qualified Security Assessor (QSA) unterzogen, um unsere Services und Kontrollen zu bewerten.

Citrix unterstützt zwar die PCI-DSS-Konformität des Kunden, die Verwendung von NetScaler-Produkten und -Diensten allein reicht jedoch nicht aus, um die PCI-DSS-Konformität zu erreichen. Die Kunden sind dafür verantwortlich, sicherzustellen, dass sie über ein angemessenes Compliance-Programm, interne Prozesse und Kontrollen verfügen, um ihre PCI-DSS-Compliance-Anforderungen zu erfüllen und aufrechtzuerhalten.

Klicken Sie auf NetScaler Console Service PCI Attestation of Compliance (AOC) , um einen Offline-Bericht herunterzuladen.

NetScaler Telemetrieprogramm

September 2, 2024

Das NetScaler Telemetrieprogramm ist ein erforderliches Datenerfassungsprogramm, das das Hochladen der erforderlichen Lizenz- und Funktionsnutzungsdaten ermöglicht, die Kunden benötigen, um ihre Wartungs- und Supportlizenzverpflichtungen einzuhalten. Citrix sammelt grundlegende Lizenztelemetriedaten und Telemetriedaten zur NetScaler-Bereitstellung und Feature-Nutzung für seine legitimen Interessen, einschließlich der Einhaltung von Lizenzbestimmungen. Daten zur Konfiguration und Nutzung der Funktionen von NetScaler Console werden ebenfalls erfasst, um die Produkte und Dienste von Citrix zu verwalten, zu messen und zu verbessern.
Das NetScaler Telemetrie-Programm wird ab dem Build 14.1-28.x automatisch aktiviert.

> **Hinweise:**
>
> - Der Telemetrie-Upload erfolgt automatisch alle 24 Stunden.
> - Um die Telemetriemetriken in Ihren NetScaler-Instanzen zu erfassen und zu speichern, wurde die folgende Konfiguration im Rahmen des am 18. Juni 2024 veröffentlichten NetScaler-Telemetrieprogramms über NetScaler Console auf Ihre NetScaler-Instances übertragen.

```
enable ns feature AppFlow
add analytics profile telemetry_metrics_profile -type timeseries -
    outputMode prometheus -metrics ENABLED -serveMode Pull -
    schemaFile "./telemetry_collect_ns_metrics_schema.json" -
    metricsExportFrequency 300
```

> - Die Datei `/nsconfig/.telemetry.conf` wird mit dem folgenden Befehl für die Gateway-Telemetrie aktualisiert. NetScaler Console sucht jede Stunde nach diesem Befehl und fügt ihn hinzu, falls dieser Befehl fehlt. Dieser Befehl wird nur an die NetScaler-Instanzen übertragen, die über eine virtuelle VPN-Serverkonfiguration verfügen:


```
ns_telemetry_server,<Console IP>,5140
```

- Einige Telemetrieparameter werden über Skripts erfasst, die von NetScaler Console an NetScaler-Instanzen übertragen werden. Diese Skripts sind schreibgeschützt und ändern nichts in NetScaler.
- Die durch Telemetrie gesammelten Informationen, wie E-Mail-Adressen, Benutzernamen und IP-Adressen, werden sicher pseudonymisiert, indem die Informationen an der Quelle mithilfe von Einweg-Hashing-Algorithmen gehasht werden. Daher kann Citrix nicht auf diese Werte zugreifen oder sie lesen. Diese Telemetriedaten werden ausschließlich für logische Asset-Matching-Zwecke verwendet.

Die folgende Tabelle enthält die Parameterdetails, die im Rahmen des NetScaler Telemetrie-Programms erfasst werden:

Kategorien	Beschreibung	Wofür verwenden wir es
Lizenz- und NetScaler-Bereitstellungs- und Nutzungstelemetrie	Informationen zu Lizenzanspruch, Zuweisung, Nutzung und allgemeinen NetScaler-Bereitstellungsdaten sowie zur Nutzung der NetScaler-Funktionen.	Einhaltung der Lizenzbestimmungen und zur Verwaltung, Messung und Verbesserung des Dienstes.
Telemetrie zur Bereitstellung und Nutzung von Funktionen in der NetScaler Console	Informationen zur Bereitstellung und Nutzung der Funktionen auf der Konsole.	Um den Service zu verwalten, zu messen und zu verbessern.

Weitere Informationen zur Liste der Telemetrieparameter finden Sie unter Data Governance.

Data Governance

July 17, 2024

Der NetScaler Console-Dienst ist Teil der Citrix Cloud-Dienste und verwendet Citrix Cloud als Plattform für Registrierung, Onboarding, Authentifizierung, Verwaltung und Lizenzierung. Citrix sammelt und speichert Daten in Citrix Cloud als Teil des NetScaler Console-Dienstes. Dieses Dokument beschreibt, welche Daten gesammelt werden und wie Daten gesammelt, gespeichert und übertragen werden.

Weitere Informationen zu den Datenschutzpraktiken bei Citrix finden Sie unter Überblick über den Datenschutz bei Citrix Cloud Services.

Diese Informationen richten sich an Sicherheitsbeauftragte, Compliance-Beauftragte, Informationsprüfer, Administratoren für Netzwerkinfrastruktur und -betrieb sowie Inhaber von Geschäftsbereichen.

NetScaler Telemetrieprogramm

Das NetScaler Telemetrieprogramm ist im NetScaler Console Service von Build **14.1-28.x** aktiviert. Mit diesem Programm werden die benötigten Daten automatisch hochgeladen. Weitere Informationen zu den gesammelten erforderlichen Telemetriedaten finden Sie unter Data Governance for NetScaler Telemetry.

Wie sammeln, speichern und übertragen wir Daten?

Der NetScaler Console-Dienst sammelt Daten von den verwalteten Instanzen und Agents. Diese Instanzen werden beim Kunden bereitgestellt und die Daten werden vom Agenten (der beim Kunden vor Ort eingesetzt wird) sicher über einen mit dem TLS 1.2-Protokoll verschlüsselten SSL-Kanal in die Cloud übertragen.

Die Daten werden in einer relationalen Datenbank mit mehrinstanziger Datenisolierung auf der Datenbankebene und als Dateien im Elastic File System (EFS) gespeichert, das in der AWS-Cloud in den USA, EMEA (Frankfurt) und APJ (Sydney) gehostet wird —je nach dem vom Kunden ausgewählten Point of Presence (POP). Alle POPs werden in kommerziellen AWS-Regionen gehostet.

Kennwörter, SNMP-Community-Strings, SSL-Zertifikate und NetScaler-Konfigurations-Backups werden mit einem eindeutigen AES-256-Schlüssel pro Mandant verschlüsselt und sicher in der Datenbank gespeichert. Weitere Informationen zu den kommerziellen Regionen, die Citrix Cloud verwendet, und zum Vorhandensein des NetScaler Console-Dienstes in jeder Region finden Sie unter Geografische Überlegungen.

Datenkategorien

Für die Datenverarbeitungspraktiken werden die Daten in folgende Kategorien unterteilt:

- **Kundeninhalte** —Alle Daten, die zur Speicherung auf das Konto des Kunden hochgeladen werden, oder Daten in der Computerumgebung des Kunden, auf die NetScaler Zugriff erhält, um bestimmte Dienste auszuführen.
- **Protokolle** —Beinhaltet Aufzeichnungen über Dienste, einschließlich, aber nicht beschränkt auf:
  - Daten und Informationen zu Leistung, Stabilität, Nutzung, Sicherheit, Support
  - Technische Informationen über Geräte, Systeme

Inhalt der Kunden

Der NetScaler Console Service sammelt Informationen aus verschiedenen Quellen:

- NetScaler
- NetScaler Gateway
- NetScaler Web App Firewall (WAF) und Bot-Management

NetScaler Console Service sammelt zusätzlich zu den in den Protokollen genannten Informationen auch Informationen über die Sitzungs- und Aktivitätsdetails des Administrators.

Protokolle

Protokolle werden verwendet, um die Bereitstellung von Softwareupdates, Lizenzauthentifizierung, Support, Analysen und andere Zwecke gemäß den Citrix Benutzervereinbarungenzu erleichtern.

Zu den gesammelten Metadaten und Telemetrieprotokollen gehören:

- NetScaler Service Agent, Hypervisor oder Public-Cloud-Plattform oder beides, Agent-Hypervisor und Public-Cloud-Plattform
- Geografischer Standort des Agenten
- NetScaler-Version
- NetScaler-Produkttyp
- Informationen zur Lizenzierung (Express und Abonnement)
- Nutzung des Cloud-Dienstes durch den NetScaler Console-Administrator (wodurch die Benutzererfahrung für Administratoren verbessert wird).

Detaillierte Kundeninhalte und Protokolle

- **Event Management (Login > Infrastructure > Events)**
  - SNMP-Traps geben Warnmeldungen zum Status und zur Leistung des NetScaler-Netzwerks aus.
  - Syslog von Webtransaktionen, die NetScaler-Netzwerkstatusinformationen durchlaufen.
  - SMS-Server-, Slack- und PagerDuty-Profildetails zum Auslösen von SMS/Slack-Benachrichtigungen über Ereignisse.
  - SMTP-Serverdetails für die E-Mail-Konfiguration.
  - ServiceNow-Profildetails für die Erstellung von Tickets in ServiceNow.

- **SSL-Zertifikatsverwaltung (Anmeldung > Infrastruktur > SSL-Dashboard)**
  - SSL-Zertifikate, SSL-Schlüssel, SSL CSR, CA Issuer und Signaturalgorithmen der von der NetScaler-Instanz optimierten Web-Apps.
- **Konfigurationsaudit (Anmeldung > Infrastruktur > Konfiguration > Konfigurationsaudit)**
  - Änderungen der Datenverfolgung für NetScaler Configuration Audit, die sich auf die NetScaler-Instanzen beziehen, einschließlich der IP-Adresse des Web-App-Servers und der NetScaler-IP-Adressdetails.
- **Konfigurationsaufträge (Anmeldung > Infrastruktur > Konfiguration > Konfigurationsaufträge)**
  - NetScaler-Konfigurationsdetails, Instanz-IP-Adresse und Web-App-Server-IP-Adressdetails.
- **StyleBooks (Anmeldung > Anwendungen > Konfiguration > StyleBooks)**
  - Als Vorlage gespeicherte NetScaler-Konfigurationen, die IP-Adressdetails des Web-App-Servers enthalten.
- **Instanzverwaltung (Anmeldung > Infrastruktur > Instanzen)**
  - IP-Adresse der NetScaler-Instanzen, NetScaler-Instanztyp, NetScaler-Konfigurations-Backup, kritische NetScaler-Ereignisse und Geolocation des Rechenzentrums, in dem die NetScaler-Instanz bereitgestellt wird (falls konfiguriert).
- **Infrastrukturanalysen (Anmeldung > Infrastruktur > Infrastrukturanalyse)**
  - IP-Adresse der NetScaler-Instanzen, NetScaler-Instanztyp, kritische NetScaler-Ereignisse, Anzahl der zugehörigen Apps und Geolocation des Rechenzentrums, in dem die NetScaler-Instanz bereitgestellt wird (falls konfiguriert).
- **Applications (Login > Applications)**
  - App-Dashboard: Anwendungs-URL, Anforderungsmethode, Antwortcode, Gesamtzahl der Byte, Web-App-Serverdetails, IP-Adressen des virtuellen Servers, Clientdetails, Browser, Client-Betriebssystem, Client-Gerät, SSL-Protokoll, SSL-Verschlüsselungsstärke, SSL-Schlüsselstärke, IP-Adresse der NetScaler-Instanz, Zeitstempel der Server-Flaps und Inhaltstyp der Antwort.
- **Analytics (AppFlow/ Logstream)**
  - **Web Insights (Anmeldung > Anwendungen)**: IP-Adresse des virtuellen Servers, Clients, URLs, Browser, Betriebssysteme, Anforderungsmethoden, Antwortstatus, Domänen, IP-Adresse des Web-App-Servers, SSL-Zertifikate, ausgehandelte SSL-Verschlüsselung, SSL-Schlüsselstärke, SSL-Protokoll und SSL-Fehler-Frontend.

- **HDX Insight (Anmeldung > Gateway)**: ICA-Benutzerdetails, ICA-Anwendungsdetails, VDA-Serverdetails, Desktopdetails in HDX Insight, Geolokalisierungsdetails des App-Clients, Details zur aktiven HDX-Sitzung, VPN-Lizenzen für HDX, NetScaler-IP-Adresse, Clienttyp und Version.
- **Gateway Insight (Anmeldung > Gateway)**: Benutzerdetails, Anwendungsdetails, Browser, Betriebssysteme, Sitzungsmodi, Gateway-Lizenzen, AAA-Serverdetails und AAA-Richtlinie, die auf Gateway konfiguriert sind.
- **Sicherheitsverstöße (Anmeldung > Sicherheit)**: Client-IP, URL, Sicherheitsverletzungen (WAF und Bot), Geolocation des Angriffs, Zeitstempel des Angriffs, Transaktions-ID, WAF und NetScaler-Sicherheitskonfigurationsstatus.
- **API-Analysen (Anmeldung > Sicherheit > API-Gateway)**: Informationen zu API-Instanzen, API-Endpunkten, Gesamtbandbreite, API-Leistungsinformationen, Gesamtanfrage, Antwortzeit, Fehlern. Möglichkeit, jede API-Instanz genauer zu untersuchen, um einen Überblick über die einzelnen API-Endpunkte und die Leistung zu erhalten. Sicherheit in Bezug auf erfolgreiche Authentifizierung, Fehlschläge, Ratenbegrenzung, SSL-Verschlüsselung, Protokollinformationen und SSL-Fehler.

- **Sicherheitsempfehlung (Anmeldung > Infrastruktur > Instanzempfehlung > Sicherheitsempfehlung)**
  - **Versionsscan : Für diesen Scan ist NetScaler Console erforderlich, um die Version einer**NetScaler-Instanz mit den Versionen und Builds zu vergleichen, für die der Fix verfügbar ist. Dieser Versionsvergleich hilft der Sicherheitsempfehlung von NetScaler Console dabei, festzustellen, ob der NetScaler für das CVE anfällig ist. Die diesem Scan zugrundeliegende Logik lautet: Wenn ein CVE auf NetScaler-Version und Build xx.yy repariert ist, gelten alle NetScaler-Instanzen in Builds, die kleiner als xx.yy sind, als anfällig. Versionsscans werden heute in der Sicherheitsempfehlung unterstützt.
  - **Konfigurationsscan : Für diesen Scan muss NetScaler Console ein für den CVE-Scan spezifisches Muster mit der NetScaler-Konfigurationsdatei**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.

    Der Konfigurationsscan wird heute in der Sicherheitsempfehlung unterstützt.
  - **Benutzerdefinierter Scan**: Für diesen Scan ist der NetScaler Console-Dienst erforderlich, um eine Verbindung mit der verwalteten NetScaler-Instanz herzustellen, ein Skript darauf zu übertragen und das Skript auszuführen. Anhand der Skriptausgabe kann NetScaler Console 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.

Sicherheit

Die Ausstellung zur Sicherheit von Citrix Services beschreibt ausführlich die Sicherheitskontrollen, die auf Citrix Cloud Services angewendet werden, einschließlich Zugriff und Authentifizierung, Systementwicklung und Wartung, Verwaltung von Sicherheitsprogrammen, Bestandsmanagement, Verschlüsselung, Betriebsmanagement, Personalsicherheit, physische Sicherheit, Geschäftskontinuität und Vorfallmanagement.

Die Sicherheit der Citrix Cloud-Produkte wird durch Verschlüsselungs- und Schlüsselverwaltungsrichtlinien gesteuert. Weitere Informationen darüber, wie Citrix Sicherheit während des gesamten Produktentwicklungszyklus einsetzt, finden Sie im Whitepaper zu Sicherheitsentwicklungsprozessen .

Datenaufbewahrungsrichtlinie für NetScaler Console Service

Daten wie statistische Kennzahlen, Dashboards, Berichte, Warnungen, Ereignisse und Protokolle in der NetScaler Console sowie Anmeldedaten werden für den Zeitraum aufbewahrt, für den der Kunde den Service abonniert. Das Benutzerkonto wird dann in ein Express-Konto umgewandelt, in dem der Benutzer nur zwei virtuelle Server verwalten kann.

Das Express-Konto hat eine Kapazität von 500 MB oder Analytics-/Reporting-Daten für einen Tag, je nachdem, welches Limit das Konto zuerst erreicht. Wenn ein Express-Konto nicht verwendet wird oder sich der Kunde länger als 30 Tage nicht in das Konto einloggt, werden das Konto und alle zugehörigen Kundeninhalte automatisch gelöscht.

Weitere Informationen zur Aufbewahrung und Löschung von Daten für Citrix Cloud Services-Konten finden Sie in der Übersicht über den Datenschutz von Citrix Cloud Services.

> **Hinweis**
>
> Alle Analytics-Daten in NetScaler Console werden für einen Zeitraum von maximal 30 Tagen aufbewahrt.

Dienste von Drittanbietern

Der NetScaler Console Service wird in Amazon Web Service (AWS) -Rechenzentren in den Regionen USA, EMEA (Frankfurt) und APJ (Sydney) gehostet —je nachdem, welchen Point of Presence (POP) der Kunde gewählt hat.

Derzeit verwendet der NetScaler Console Service Dienste und APIs verschiedener Technologien von Drittanbietern:

- Dienste, die für die Produktfunktionalität verwendet werden:
  - Google Maps, AWS EFS, AWS RDS, AWS Elastic Cache, AWS ALB, AWS Route 53, AWS EKS, AWS Secret Manager, AWS ECR-Repository und AWS MSK.
- Zu den Diensten und Tools von Drittanbietern, die für die Überwachung und den Betrieb von NetScaler Console verwendet werden, gehören:
  - PagerDuty für Rotation auf Abruf
  - Protokollanalyse mit Splunk
  - Fluentd für die Protokollaggregation
  - Slack für Kommunikation und Alarmierung
  - AWS Cloudwatch, SQS
  - S3 als Speicherbereich in AWS —zum Speichern von Kerndateien und Metriken
  - Prometheus und Grafana zur Überwachung (im Honeycomb-Einsatz)

Referenzen

- Weitere Informationen darüber, wie wir auf die gesammelten Daten zugreifen, finden Sie unter Citrix Services Security Exhibit.
- Weitere Informationen darüber, wie lange die gesammelten Daten aufbewahrt werden, finden Sie unter Übersicht über den Datenschutz von Citrix Cloud Services.
- Überblick über die technische Sicherheit von Citrix Cloud.
- Citrix Cloud Technische und organisatorische Datensicherheitsmaßnahmen.

Erste Schritte

January 26, 2024

In diesem Dokument erfahren Sie, wie Sie mit dem Onboarding und der ersten Einrichtung von NetScaler Console beginnen. Dieses Dokument richtet sich an Netzwerk- und Anwendungsadministratoren, die Citrix Netzwerkgeräte (NetScaler, NetScaler Gateway, Citrix Secure Web Gateway usw.) verwalten. Folgen Sie den Schritten in diesem Dokument unabhängig vom Gerätetyp, den Sie mit NetScaler Console verwalten möchten.

Bevor Sie mit dem Onboarding beginnen, stellen Sie sicher, dass Sie die Browseranforderungen, die Agentinstallationsanforderungen und die Portanforderungen überprüfen.

Schritt 1: Melden Sie sich für Citrix Cloud an

Um NetScaler Console verwenden zu können, müssen Sie zunächst ein Citrix Cloud-Unternehmenskonto erstellen oder einem vorhandenen Konto beitreten, das eine andere Person in Ihrem Unternehmen erstellt hat. Detaillierte Verfahren und Anweisungen zum weiteren Vorgehen finden Sie unter Registrierung für Citrix Cloud.

Schritt 2: NetScaler Console mit einem Express-Konto verwalten

Nachdem Sie sich bei Citrix Cloud angemeldet haben, gehen Sie wie folgt vor:

1. Gehen Sie zum Abschnitt **Verfügbare Dienste**.
2. Klicken Sie auf der Kachel **Application Delivery Management** auf **Verwalten**.

   Die Kachel **Application Delivery Management** wird in den Abschnitt **Meine Dienste** verschoben
3. Wählen Sie eine Region aus, die Ihren Geschäftsanforderungen entspricht.

   > **Wichtig**
   >
   > Die Region kann später nicht geändert werden.

4. Wählen Sie Rollen und Anwendungsfälle aus, die auf Sie zutreffen.

Sie können sich vom Browser abmelden, während die Initialisierung im Hintergrund abgeschlossen ist. Dies kann einige Zeit in Anspruch nehmen.

> **Hinweis**
>
> Citrix weist ein Express-Konto zur Verwaltung der NetScaler Console-Ressourcen zu. Wenn Ihr NetScaler Console Express-Konto 45 Tage lang inaktiv bleibt, wird das Konto gelöscht. Weitere Informationen finden Sie unter NetScaler Console mit dem Express-Konto verwalten .

Wenn Sie sich wieder bei Ihrem Citrix Cloud-Konto anmelden, wird der **NetScaler Console-GUI**-Bildschirm angezeigt. Klicken **Sie auf Erste Schritte**, um den Dienst zum ersten Mal einzurichten.

Schritt 3: Wählen Sie einen NetScaler-Bereitstellungstyp

Wählen Sie eine der folgenden Bereitstellungsoptionen aus, die Ihren Geschäftsanforderungen entspricht:

- **Intelligente Bereitstellung**—Bei dieser Option handelt es sich um ein automatisiertes Umgebungs-Setup zur Bereitstellung neuer NetScaler-Instanzen. Es installiert automatisch einen Agenten, um die Kommunikation zwischen der NetScaler Console und den verwalteten Instanzen zu ermöglichen.

  Diese Option unterstützt AWS-, Microsoft Azure- und Google Cloud-Umgebungen . In drei Schritten können Sie mithilfe von NetScaler-Instanzen eine Anwendung bereitstellen, die in der Cloud vorhanden ist.

- **Benutzerdefinierte Bereitstellung** —Diese Option ist eine mehrstufige Bereitstellung. Sie können jede Umgebungsoption auswählen und NetScaler-Instanzen bereitstellen oder erkennen.

Wählen Sie Smart Deployment für AWS

Diese Bereitstellungsoption schafft die folgende Infrastruktur in AWS:

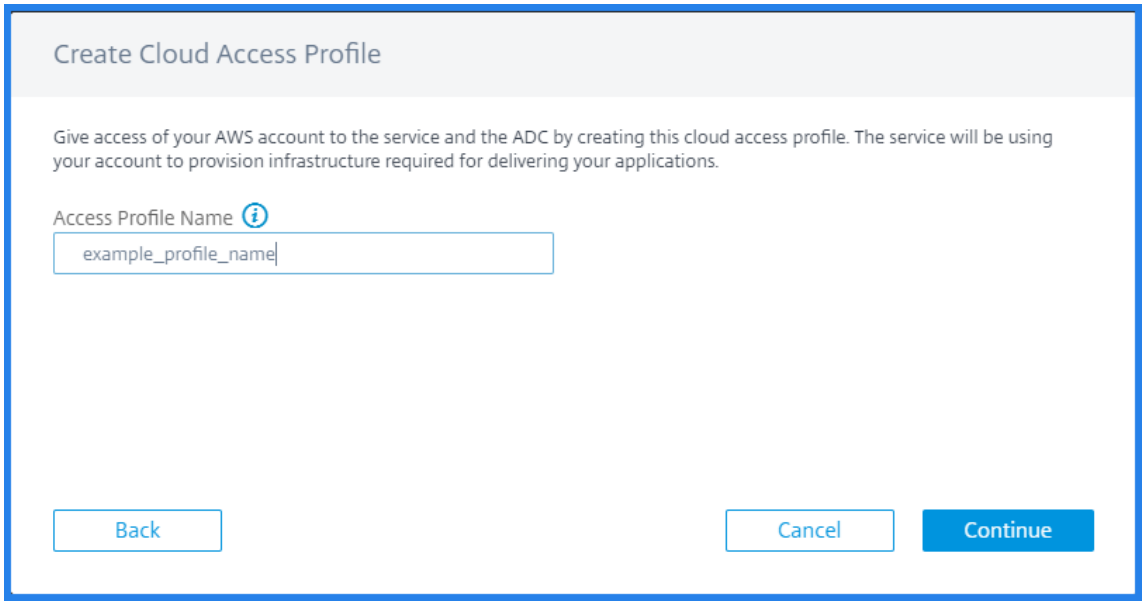
- Ein CloudFormation-Stack in AWS zum Erstellen der erforderlichen Infrastruktur, die Subnetze, Sicherheitsgruppen, NAT-Gateways usw. umfasst.
- Ein Agent in der VPC zur Verwaltung von NetScaler-Instanzen.
- Eine NetScaler Autoscale-Gruppe. Sie können diese Gruppe später auf der Seite **Infrastruktur > Public Cloud > Autoscale-Gruppen** anpassen.

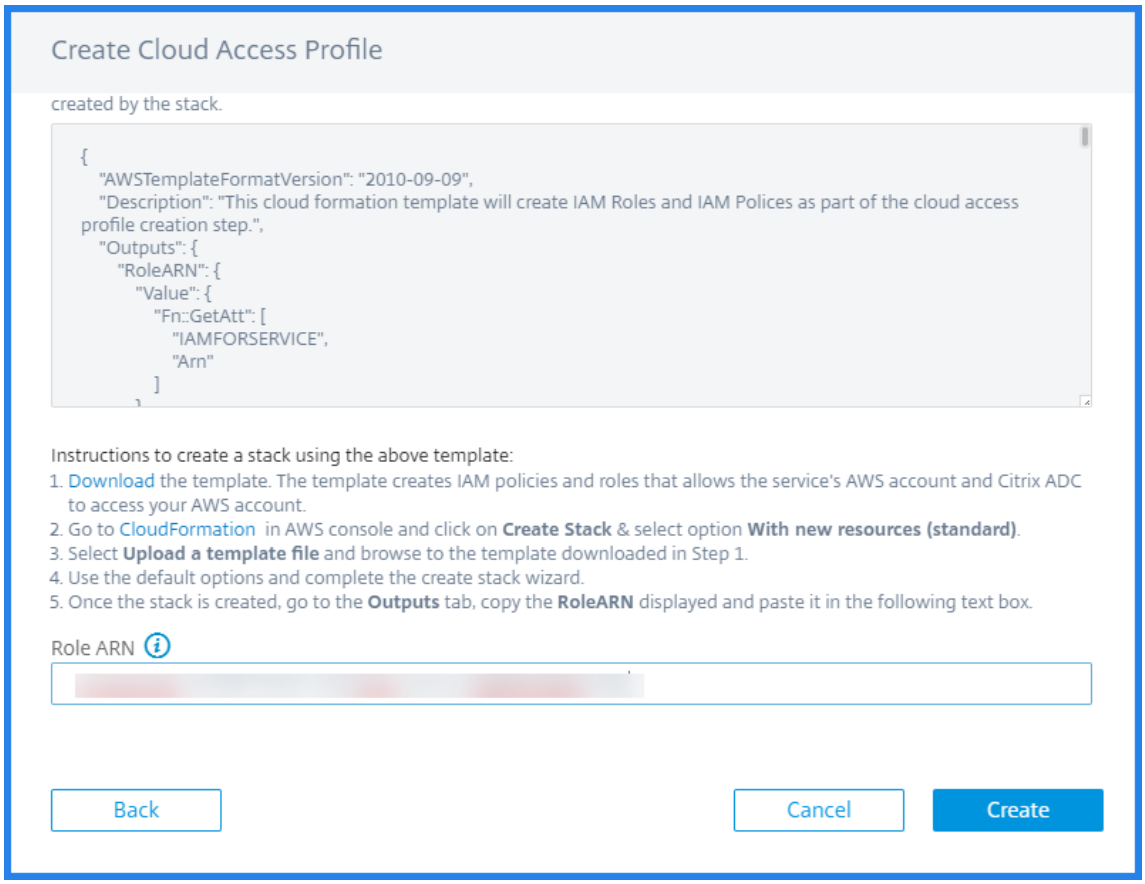
Stellen Sie vor der Bereitstellung von NetScaler-Instanzen Folgendes sicher:

1. Sie besitzen bereits ein AWS-Konto.
2. Sie haben einen IAM-Benutzer mit allen Administratorberechtigungen erstellt.

Gehen Sie wie folgt vor, um NetScaler-Instanzen bereitzustellen:

1. Wählen **Sie unter Create Cloud Access Profile**die Option **AWS** als Bereitstellungsumgebung aus. Geben Sie **den Zugriffsprofilnamen und denRollen-ARN** an, um ein Cloud Access-Profil zu erstellen





Die NetScaler Console verwendet das Cloud Access Profile, um auf ein AWS-Konto zuzugreifen.

2. Geben Sie die folgenden Details an, um die AWS-Umgebung vorzubereiten:

   a) ****Wählen Sie unter Rechenzentrumsdetails die **AWS-Region** und die **AWS-VPC** aus, in der Sie NetScaler-Instanzen bereitstellen möchten.

AWS VPC listet die in der ausgewählten **AWS-Region** vorhandenen VPCs auf.

b) Geben Sie in den NetScaler AutoScale-Gruppendetails Folgendes an, um NetScaler-Instanzen in der AWS-Cloud zu skalieren:**

- **AutoScale Group Name** - Ein Name zur Identifizierung einer Autoscale-Gruppe.
- **Availability Zones** - Wählen Sie die Zonen aus, in denen Sie die Autoscale-Gruppen erstellen möchten.

  Sie können mehrere Zonen aus der Liste auswählen.
- **Bereitstellungstyp** - Wählen Sie entweder die Option **Bewertung** oder **Produktion** aus.

  Wenn Sie die NetScaler Console Autoscale-Lösung vor dem Kauf der Produktionslizenz testen möchten, wählen Sie die **Option**Evaluierung.

  > **Wichtig!**
  >
  > – Die Evaluierungsoption unterstützt nur eine Availability Zone.
  > – Mit der Auswertungsoption können Sie nur NetScaler VPX Express auswählen. Und die NetScaler Console Autoscale-Lösung kann auf bis zu drei NetScaler-Instanzen skaliert werden.

- **NetScaler VPX-Produkt**—Wählen Sie Lizenzen für die Bereitstellung von NetScaler-Instanzen aus.

  Abonnieren Sie die ausgewählte Lizenz auf der AWS-Marketplace-Site und kehren Sie zu dieser Seite zurück.

  Überprüfen Sie die Einwilligungsnachricht des Benutzers und wählen
- **Instanz-Typ** - Wählen Sie den erforderlichen Instanz-Typ aus.

c) Klicken Sie auf **Weiter**.

Klicken Sie nach erfolgreicher Validierung auf **Erstellen** , um NetScaler-Instanzen in AWS bereitzustellen und eine Autoscale-Gruppe zu erstellen.

3. Klicken Sie nach der erfolgreichen NetScaler-Bereitstellung auf **Deploy Application**.

   Geben Sie unter **Configure Application** die erforderlichen Details an und klicken Sie auf **Submit**.

   Weitere Informationen finden Sie unter Konfigurieren einer Anwendung für die Autoscale-Gruppe.

Intelligente Bereitstellung für Microsoft Azure auswählen

Diese Bereitstellungsoption erstellt die folgende Infrastruktur in Azure:

- Eine Azure Resource Manager (ARM) -Vorlage zum Erstellen der erforderlichen Infrastruktur, die Subnetze, Sicherheitsgruppen, NAT-Gateways usw. umfasst.
- Ein Agent in der VPC zur Verwaltung von NetScaler-Instanzen.
- Eine NetScaler Autoscale-Gruppe. Sie können diese Gruppe später auf der Seite **Infrastruktur > Public Cloud > Autoscale-Gruppen** anpassen.

Stellen Sie vor der Bereitstellung von NetScaler-Instanzen Folgendes sicher:

- Sie besitzen ein Microsoft Azure-Konto, das das Azure Resource Manager-Bereitstellungsmodell unterstützt
- Sie haben eine Ressourcengruppe in Microsoft Azure.

Weitere Informationen zum Erstellen eines Kontos und zu anderen Aufgaben finden Sie in der Microsoft Azure-Dokumentation.

Gehen Sie wie folgt vor, um NetScaler-Instanzen bereitzustellen:

1. Wählen **Sie unter Cloud-Zugriffsprofil erstellen**die Option **Microsoft Azure** als Bereitstellungsumgebung aus. Geben Sie NetScaler Console- und NetScaler Cloud-Zugriffsprofildetails an.

   Die NetScaler Console verwendet das NetScaler Console Cloud Access Profile, um auf ein Microsoft Azure-Konto zuzugreifen. Und ein NetScaler Cloud Access Profile wird verwendet, um NetScaler VPX-Instanzen bereitzustellen.

2. Geben Sie die folgenden Details an, um die Azure-Umgebung vorzubereiten:

   a) Geben Sie unter **Details zur Anwendungsumgebung**einen Namen für Ihre Bereitstellung an. Stellen Sie außerdem sicher, dass das richtige Cloud-Zugriffsprofil ausgewählt ist.

   b) Geben Sie unter **Data Center Details** die Region, die Ressourcengruppe und die virtuellen Netzwerkdetails an, in denen Sie NetScaler-Instanzen bereitstellen möchten.

   c) Geben Sie in NetScaler AutoScale-Gruppendetails Folgendes an:**

      - **Verfügbarkeit** —Wählen Sie die Availability Zone oder das Set aus, in dem Sie die Autoscale-Gruppen erstellen möchten. Abhängig vom ausgewählten Cloud-Zugriffsprofil werden Availability Zones in der Liste angezeigt.
      - **Bereitstellungstyp** - Wählen Sie entweder die Option **Bewertung** oder **Produktion** aus.

        Wenn Sie die NetScaler Console Autoscale-Lösung vor dem Kauf der Produktionslizenz testen möchten, wählen Sie die **Option**Evaluierung.

> **Wichtig!**
>
> - Die Evaluierungsoption unterstützt nur eine Availability Zone oder einen Satz.
> - Mit der Auswertungsoption können Sie nur NetScaler VPX Express auswählen. Und die NetScaler Console Autoscale-Lösung kann auf bis zu drei NetScaler-Instanzen skaliert werden.

- **NetScaler VPX-Produkt**auswählen —Wählen Sie Lizenzen für die Bereitstellung von NetScaler-Instanzen aus.

  Abonnieren Sie diese Azure Marketplace-Lizenz und kehren Sie zur Seite zurück.

  Überprüfen Sie die Einwilligungsnachricht des Benutzers und wählen
- **VM-Größe auswählen** —Wählen Sie die erforderliche Größe der virtuellen Maschine aus.

d) Klicken Sie auf **Weiter**.

Klicken Sie nach erfolgreicher Validierung auf **Erstellen** , um NetScaler-Instanzen in Microsoft Azure bereitzustellen und eine Autoscale-Gruppe zu erstellen.

3. Klicken Sie nach der erfolgreichen NetScaler-Bereitstellung auf **Deploy Application**.

   Geben Sie unter **Configure Application** die erforderlichen Details an und klicken Sie auf **Submit**.

   Weitere Informationen finden Sie unter Konfigurieren einer Anwendung für die Autoscale-Gruppe.

Wählen Sie eine intelligente Bereitstellung für Google Cloud

Diese Bereitstellungsoption erstellt die folgende Infrastruktur in Google Cloud:

- Ein Google Cloud Deployment Manager zum Erstellen der erforderlichen Infrastruktur, die VPC-Netzwerke, Subnetze, Cloud-NAT, Cloud Router-Gateways und Firewallregeln umfasst.
- Ein Agent in der VPC zur Verwaltung von NetScaler-Instanzen.
- Eine NetScaler Autoscale-Gruppe. Sie können diese Gruppe später auf der Seite **Infrastruktur > Public Cloud > Autoscale-Gruppen** anpassen.

Stellen Sie vor der Bereitstellung von NetScaler-Instanzen sicher, dass Sie bereits über ein Google Cloud-Konto verfügen. Weitere Informationen zum Erstellen eines Kontos finden Sie in der Google Cloud-Dokumentation.

Gehen Sie wie folgt vor, um NetScaler-Instanzen bereitzustellen:

1. Wählen **Sie unter Cloud-Zugriffsprofil erstellen**die Option **Google Cloud** als Bereitstellungsumgebung aus.

   Geben Sie **den Cloud Access-Profilnamen** und **den Dienstkontoschlüssel**an

   Die NetScaler Console verwendet das Cloud Access Profile, um auf ein Google Cloud-Konto zuzugreifen.

2. Geben Sie die folgenden Details an, um die Google Cloud-Umgebung vorzubereiten:

   a) Geben Sie unter **Details zur Anwendungsumgebung**einen Namen für Ihre Bereitstellung an. Stellen Sie außerdem sicher, dass das richtige Cloud-Zugriffsprofil ausgewählt ist.

   b) ****Wählen Sie unter Rechenzentrumsdetails die **Google Cloud-Region** aus, in der Sie NetScaler-Instanzen bereitstellen möchten.

   c) Geben Sie in den NetScaler AutoScale-Gruppendetails Folgendes an, um NetScaler-Instanzen in Google Cloud automatisch zu skalieren:**

      - **Subnetz-CIDR des VPC-Netzwerks** : Geben Sie ein VPC-Netzwerk an, das für Verwaltungs-, Client- und Serverdatenverkehr erstellt wurde. Sie können jedoch das vorhandene Netzwerk für den Server auswählen.
      - **Zonen** —Wählen Sie die Zonen aus, in denen Sie Autoscale-Gruppen erstellen möchten.

        Sie können mehrere Zonen aus der Liste auswählen.
      - **Bereitstellungstyp** - Wählen Sie entweder die Option **Bewertung** oder **Produktion** aus.

        Wenn Sie die NetScaler Console Autoscale-Lösung vor dem Kauf der Produktionslizenz testen möchten, wählen Sie die **Option**Evaluierung.

        > **Wichtig!**
        >
        > – Die Evaluierungsoption unterstützt nur eine Availability Zone.
        > – Mit der Auswertungsoption können Sie nur NetScaler VPX Express auswählen. Und die NetScaler Console Autoscale-Lösung kann auf bis zu drei NetScaler-Instanzen skaliert werden.

      - **NetScaler VPX-Produkt**—Wählen Sie Lizenzen für die Bereitstellung von NetScaler-Instanzen aus.
      - **Maschinentyp** —Wählen Sie den erforderlichen Instanztyp aus.

   d) Klicken Sie auf **Weiter**.

      Klicken Sie nach erfolgreicher Validierung auf **Erstellen** , um NetScaler-Instanzen in Google Cloud bereitzustellen und eine Autoscale-Gruppe zu erstellen.

3. Klicken Sie nach der erfolgreichen NetScaler-Bereitstellung auf **Deploy Application**.

   Geben Sie unter **Configure Application** die erforderlichen Details an und klicken Sie auf **Submit**.

   Weitere Informationen finden Sie unter Konfigurieren einer Anwendung für die Autoscale-Gruppe.

Wählen Sie eine benutzerdefinierte Bereitstellung

Diese Option bietet eine mehrstufige Bereitstellung. Wählen Sie diese Option, um NetScaler-Instanzen aus verschiedenen Umgebungen zu ermitteln. Mit dieser Option können Sie auch neue Instanzen bereitstellen, indem Sie benutzerdefinierte Umgebungsoptionen angeben.

Führen Sie die folgenden Schritte aus, um NetScaler-Instanzen bereitzustellen oder zu ermitteln:

1. Wählen Sie eine der folgenden Umgebungen aus:

   - **AWS**
   - **Microsoft Azure**
   - **Google Cloud Platform**
   - **On-Premises**

2. Installieren Sie den Agenten, um die Kommunikation zwischen der NetScaler Console und den verwalteten Instanzen in Ihrem Rechenzentrum oder Ihrer Cloud zu ermöglichen.

   Der Schritt **Agenttyp auswählen** variiert die Agentinstallationsoptionen je nach ausgewählter Umgebung.

   - **Lokal** —Wenn Sie **Lokal**auswählen, können Sie einen Agent auf den folgenden Hypervisoren installieren:
     - Citrix Hypervisor
     - VMware ESXi
     - Microsoft Hyper-V
     - Linux KVM-Server
   - **Öffentliche Clouds** —Wenn Sie **AWS**, **Microsoft Azure**oder **Google Cloud Platform**auswählen, können Sie einen Agent extern in der ausgewählten Cloud installieren.

     Es folgt ein Beispiel für die AWS-Umgebung.
   - **Als Microservice** - Um einen Agent als Kubernetes-Anwendung bereitzustellen.
   - **Eingebauter Agent** - Um integrierte Agents zu ermitteln, die mit NetScaler Version 12.0 oder höher verfügbar sind.

3. Klicken Sie auf **Weiter**.

   Die Schritte zur Installation eines Agents sind bei jeder Option unterschiedlich. Die folgenden Links führen Sie zu den spezifischen Schritten zur Installation eines Agents:

   - Hypervisor
   - Externer Agent
   - Als Microservice
   - Eingebauter Agent

Installieren eines Agents auf einem Hypervisor

Gehen Sie wie folgt vor, um einen Agenten auf einem Hypervisor einzurichten:

1. Wählen Sie den Hypervisor aus und klicken Sie auf **Image herunterladen**, um das Agentimage auf Ihr lokales System herunterzuladen.

   Eine Service-URL und ein Aktivierungscode werden generiert und auf der GUI angezeigt.

2. Kopieren Sie die Service-URL und einen Aktivierungscode.
3. Geben Sie die kopierte Dienst-URL und den Aktivierungscode an, während Sie den Agent auf Ihrem Hypervisor installieren.

   Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren. Eine ausführliche Anleitung zur Installation eines Agenten auf Ihrem lokalen Hypervisor finden Sie unter Installieren eines Agenten on-premises.

4. Kehren Sie nach erfolgreicher Agentinstallation zur Seite **Agent einrichten** zurück und klicken Sie auf **Agent registrieren**.

Nächster Schritt: Instanzen hinzufügen.

> **Hinweis**
>
> Wenn Sie bei der Ersteinrichtung keine Agenten hinzufügen möchten, klicken Sie auf **Überspringen** , um die von NetScaler Console bereitgestellten Funktionen zu überprüfen. Sie können die Agents und Instanzen später hinzufügen. Um später Agenten hinzuzufügen, navigieren Sie zu **Einstellungen > Agenten einrichten**. Anweisungen zum späteren Hinzufügen von Instanzen finden Sie unter Hinzufügen von Instanzen.

Installieren eines Agents in einer öffentlichen Cloud

Sie müssen das Agentimage nicht von der Seite **Agent einrichten** herunterladen. Das Agentimage ist auf dem jeweiligen Cloud-Marktplatz verfügbar.

1. Kopieren und speichern Sie die Service-URL und den Aktivierungscode, der während der Agentinstallation verwendet werden soll.

   Wenn Sie einen neuen Aktivierungscode wünschen, klicken Sie auf **Neuen Aktivierungscode erstellen**, kopieren und speichern Sie dann den Code, der während der Agentinstallation verwendet werden soll.

   - Eine ausführliche Anleitung zur Installation eines Agenten in der Microsoft Azure Cloud finden Sie unter Installieren eines Agenten in der Microsoft Azure Cloud .
   - Eine ausführliche Anleitung zur Installation eines Agenten auf AWS finden Sie unter Einen Agenten auf AWS installieren .
   - Eine ausführliche Anleitung zur Installation eines Agenten in Google Cloud finden Sie unter Installieren eines Agenten auf der GCP .

2. Kehren Sie nach erfolgreicher Agentinstallation zur Seite **Agent einrichten** zurück und klicken Sie auf **Agent registrieren**.

Nächster Schritt: Instanzen hinzufügen.

Installieren eines Agent als Microservice

**Sie können einen Agenten als Microservice im Kubernetes-Cluster bereitstellen, um das Dienstdiagramm in NetScaler Console anzuzeigen.

Weitere Informationen zu den ersten Schritten mit Service Graph finden Sie unter Service Graph einrichten.

1. Geben Sie 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) **Agent-Kennwort**—Geben Sie ein Kennwort für CPX an, um dieses Kennwort zu verwenden, um CPX über den Agent in NetScaler Console zu integrieren.

   c) **Kennwort bestätigen** —Geben Sie dasselbe Kennwort zur Bestätigung an.

   d) Klicken Sie auf **Submit**.

2. Nachdem Sie auf **Senden** geklickt haben, können Sie die YAML- oder Helm-Karte herunterladen.
3. Klicken Sie auf **Schließen**.

   Weitere Informationen finden Sie unter Installieren eines Agent im Kubernetes-Cluster.

Integrierten Agent verwenden

Die NetScaler-Instanzen in Ihrer Umgebung enthalten einen integrierten Agent. Sie können den integrierten Agenten initiieren und ihn verwenden, um die Kommunikation zwischen der Instanz und NetScaler Console herzustellen.

1. Kopieren Sie die generierte **Service-URL** und den **Aktivierungscode**. Speichern Sie sie, um sie beim Initiieren des integrierten Agents auf Ihrer NetScaler-Instanz zu verwenden.

   Detaillierte Anweisungen zum Initiieren des integrierten Agents auf Ihrer NetScaler-Instanz finden Sie unter Initiieren des integrierten Agents auf der NetScaler-Instanz.

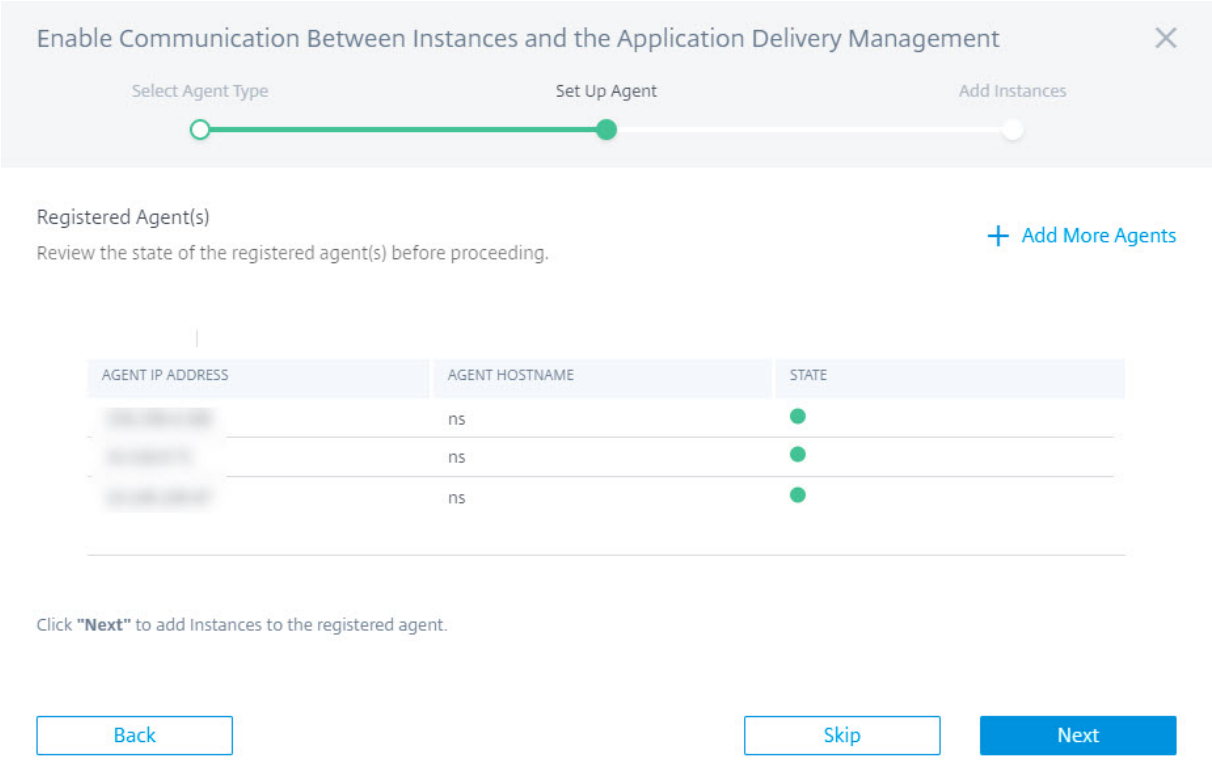
2. Nachdem der integrierte Agent initiiert wurde, kehren Sie zur Seite **Agent einrichten** zurück und klicken Sie auf **Instanz registrieren**.

Nächster Schritt: Instanzen hinzufügen.

Instanzen hinzufügen

Instanzen sind Netzwerk-Appliances oder virtuelle Appliances, die Sie von der NetScaler Console aus erkennen, verwalten und überwachen möchten. Um diese Instanzen zu verwalten und zu überwachen, müssen Sie die Instanzen dem Dienst hinzufügen.

Nach der erfolgreichen Agentinstallation und -registrierung werden die Agents auf der Seite “**Agent einrichten** “angezeigt. Wenn sich der Agent-Status im Status UP befindet, der mit einem grünen Punkt daneben gekennzeichnet ist, klicken Sie auf **Weiter**, um Instanzen zum Dienst hinzuzufügen.



1. Sehen Sie sich auf der Seite „ **Instanzen hinzufügen** “die NetScaler-Instanzen an, die mit dem registrierten Agenten verbunden sind. Stellen Sie sicher, dass sich die Instanz im Status **Up** befindet, und klicken Sie auf **Weiter**.
2. Klicken Sie auf **Fertig**, um die Erstinstallation abzuschließen und mit der Verwaltung der Bereitstellung zu beginnen.

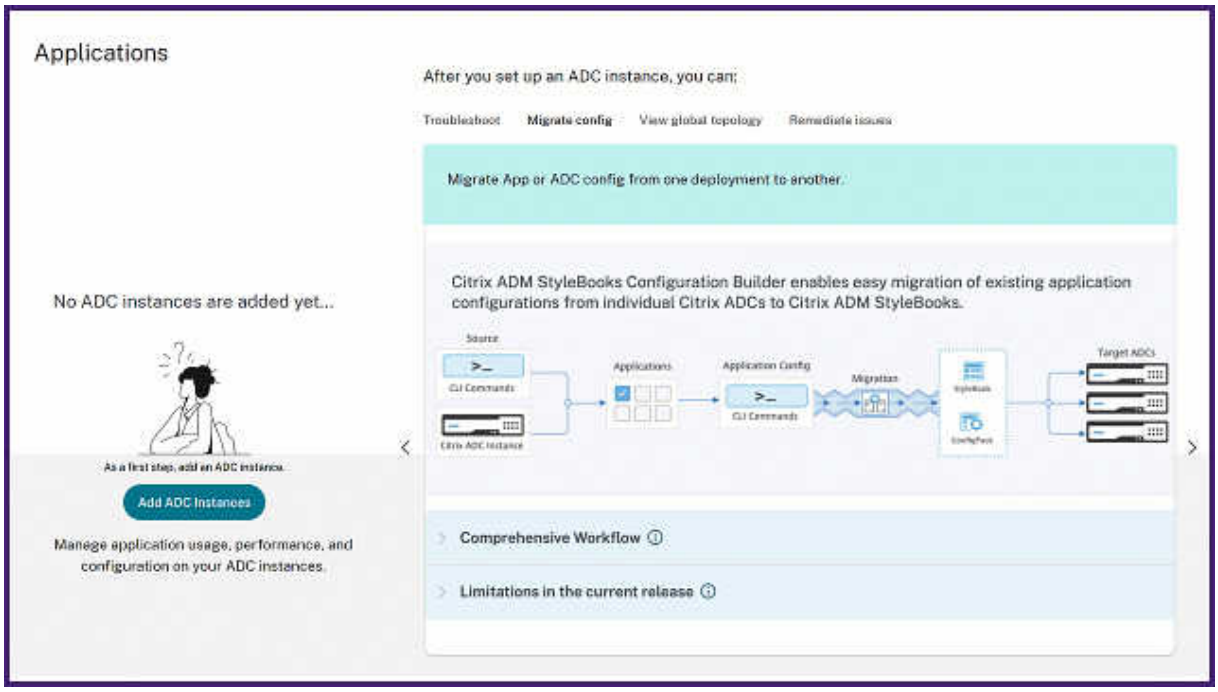
> **Hinweis**
>
> Wenn Sie bei der Ersteinrichtung keine Instanzen hinzufügen möchten, können Sie auf **Fertig** klicken, um das Setup abzuschließen und die Instanzen später hinzuzufügen. Anweisungen zum späteren Hinzufügen von Instanzen zur NetScaler Console finden Sie unter Hinzufügen von Instanzen.

Integrieren Sie NetScaler-Instanzen mithilfe des NetScaler Console-GUI-Dashboards

Wenn Sie beim ersten Einrichten der NetScaler Console das Onboarding der NetScaler-Instanzen im **Getting** Started-Workflow übersprungen haben, können Sie die Instanzen über das NetScaler Console-GUI-Dashboard einbinden. Wenn die NetScaler-Instanzen noch nicht hinzugefügt wurden, werden Sie von der GUI aufgefordert, die Instanzen hinzuzufügen.

Wenn Sie in der linken Navigationsleiste auf ein Modul klicken, wird auf der rechten Seite eine tabellarische Vorschau der Funktionen und Vorteile dieses Moduls angezeigt. Diese Funktionen und Vorteile

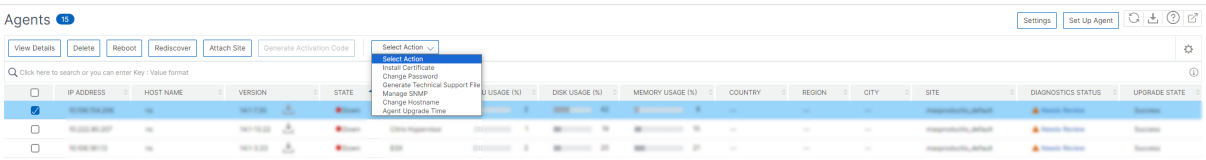
helfen Ihnen, NetScaler-Instanzen mithilfe der NetScaler Console besser zu verwalten.



Klicken Sie auf **NetScaler-Instanzen hinzufügen**, um die Instanzen zu integrieren. Der Arbeitsablauf **Erste Schritte** wird neu gestartet. Folgen Sie den in diesem Dokument angegebenen Schritten ab Schritt 3: Wählen Sie einen NetScaler-Bereitstellungstyp, um die Instanzen einzubinden.
Wenn die NetScaler-Instanzen bereits integriert sind, wird nach der Anmeldung an der NetScaler Console nur die NetScaler Console-Landingpage mit der Navigationsleiste auf der linken Seite angezeigt.

Agent-Aktionen

Nachdem Sie Ihre NetScaler Console eingerichtet haben, können Sie verschiedene Aktionen auf einen Agenten anwenden. Navigieren Sie zu **Infrastruktur > Instanzen > Agents**.



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 Agentkennwort**: Um die Sicherheit Ihrer Infrastruktur zu gewährleisten, ändern Sie das Standardkennwort eines Agents.

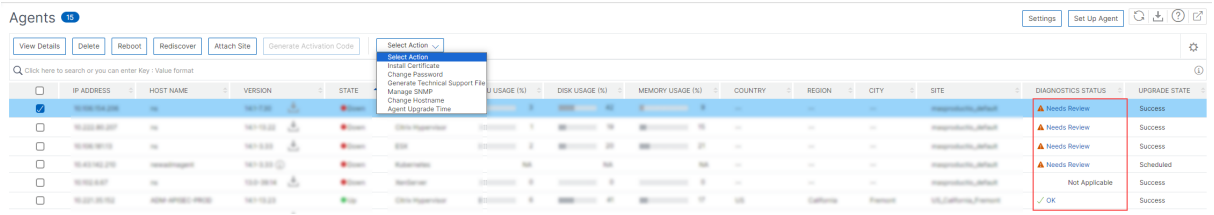
- **Generieren Sie eine Datei**für den technischen Support : Generieren Sie eine Datei für den technischen Support für einen ausgewählten Agenten. Sie können diese Datei herunterladen und an den technischen Support von Citrix zur Untersuchung und Fehlerbehebung senden.

Agentdiagnosen anzeigen und Warnmeldungen für Endpunktverifizierung

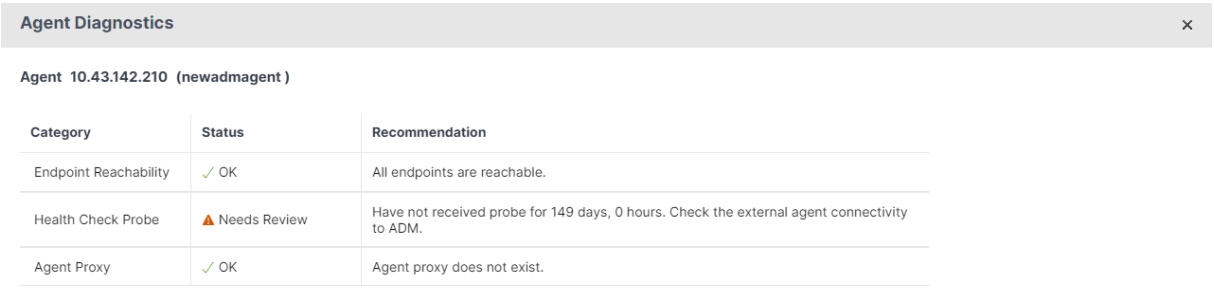
NetScaler Console führt in regelmäßigen Abständen (alle eine Stunde) eine Diagnoseüberprüfung für den Agenten durch und stellt die folgenden Informationen bereit:

- **Erreichbarkeit von Endpunkten** —Prüft, ob alle Endpunkte erreichbar sind. Der Agent verwendet verschiedene Endpunkte für die Kommunikation zwischen NetScaler Console und NetScaler-Instanzen. Weitere Informationen finden Sie unter Softwareanforderungen.
- **Health Check Probe** —Stellt den Zeitstempel der letzten Integritätsprüfung bereit.
- **Agentproxy** —Prüft, ob der Agentproxy existiert.

Wenn sich der Erreichbarkeitsstatus des Agentendpunkts ändert (von **OK** zu **Needs Review**), erhält der Superadministrator eine E-Mail-Benachrichtigung mit den Details zum Problem. Navigieren Sie zu **Infrastruktur > Instanzen > Agents**, um die neu hinzugefügte **Diagnosestatus-Option** anzuzeigen, die den Status wie **Bedarfsüberprüfung** oder **OK**bereitstellt.



Klicken Sie hier, um die Diagnoseinformationen eines Agents anzuzeigen.

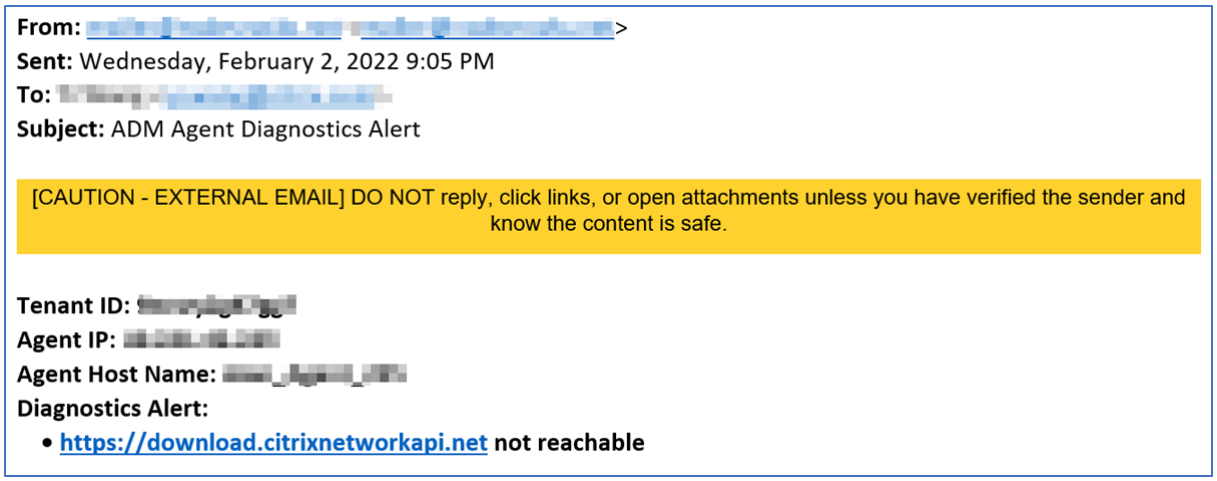


- **Kategorie**. Stellt die Problemkategorie bereit.
- **Status**. Zeigt den Problemstatus an, z. B. **Überprüfung erforderlich** oder **OK**.
- **Empfehlung**. Stellt die erforderliche Empfehlung zur Behebung des Problems bereit.

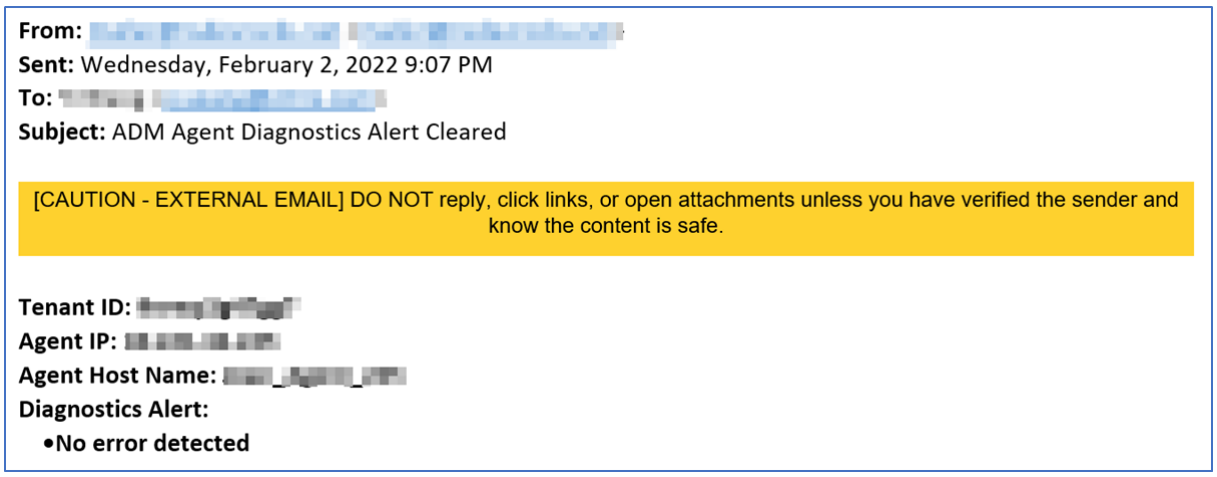
Nachdem Sie die Fehlerbehebung durchgeführt haben und der Status der Erreichbarkeit des Endpunkts von **Needs Review** in **OK**geändert wurde, erhält der Superadministrator eine E-Mail-Benachrichtigung, dass das Problem behoben wurde.

E-Mail-Benachrichtigung

Das folgende Beispiel ist eine E-Mail-Benachrichtigung, nachdem sich der Erreichbarkeitsstatus des Endpunkts von **OK in NeedsReview**geändert hat:



Das folgende Beispiel ist eine E-Mail-Benachrichtigung, nachdem sich der Erreichbarkeitsstatus des Endpunkts von **Needs Review** in **OK**geändert hat:



Konfigurieren Sie den integrierten Agenten für die Verwaltung von Instanzen

January 26, 2024

Ein integrierter Agent ist auf NetScaler MPX, VPX, Gateway-Instanzen verfügbar, auf denen die Version `12.1.48.13` ausgeführt wird, und später sowie auf NetScaler SDX-Instanzen mit Version 13.0 61.x und höher sowie 12.1 58.x und höher. Sie können diesen Agenten auf der NetScaler-Instanz initiieren, anstatt einen dedizierten Agenten in Ihrem Rechenzentrum oder Ihrer Public Cloud zu installieren. Der integrierte Agent ermöglicht die Kommunikation zwischen der Instanz und NetScaler Console.

> **Hinweis:**
>
> Der integrierte Agent ist nur für die folgenden NetScaler-Instanztypen verfügbar:
>
> - NetScaler MPX
> - NetScaler VPX
> - NetScaler SDX
> - NetScaler Gateway

Der integrierte Agent ist ideal für kleinere NetScaler Standalone- oder HA-Paar-Bereitstellungen. Wenn Sie mehrere NetScaler-Instanzen haben, verwenden Sie einen dedizierten Agenten für Bereitstellungen. Dieser Agent stellt sicher, dass Sie über bessere Datenaggregationsfunktionen verfügen als der integrierte Agent. Weitere Informationen finden Sie unter Installieren eines Agents on-premises.

NetScaler Console unterstützt die Verwaltung und Überwachung von NetScaler-Instanzen mithilfe integrierter Agenten. Die folgenden Funktionen werden jedoch vom integrierten Agent nicht unterstützt:

- Anwendungsdashboard
- Web Insight
- SSL-Einblick
- HDX Insight
- Gateway-Einblick
- Einblicke in die Sicherheit
- Fortschrittliche Analytik
- Zusammengefasste Lizenzierung

Sie können von einem integrierten Agent zu einem externen Agent wechseln. Weitere Informationen finden Sie unter Übergang von einem integrierten Agent zu einem externen Agent.

Voraussetzungen

Bevor Sie einen integrierten Agent in der NetScaler-Instanz konfigurieren, stellen Sie Folgendes sicher:

- Die NetScaler (MPX, VPX oder Gateway) -Instanz wird auf der Version `12.1.48.13` oder höher ausgeführt. Die SDX-Instanz läuft Version `13.0.61.x` und höher.
- Ein DNS-Namenserver wird auf der NetScaler-Instanz hinzugefügt.

  Weitere Informationen finden Sie unter Hinzufügen eines Namenservers.
- Sie haben ein Citrix Cloud-Konto. Weitere Informationen finden Sie unter Für Citrix Cloud anmelden.

> **Hinweis:**
>
> Alle Informationen zu Ports und anderen Systemanforderungen finden Sie unter Systemanforderungen.

Integrierten Agent konfigurieren

Führen Sie die folgenden Aufgaben aus, um den integrierten NetScaler Agent zu konfigurieren:

1. Wählen Sie die Option Integrierter Agent, wie unter Erste Schritte beschrieben.
2. Kopieren Sie die **Service-URL** und den **Aktivierungscode**.

   Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren. Überspringen Sie Schritt 7, wenn Sie ein MPX- oder Gateway-Kunde sind.
3. Initiieren Sie den integrierten Agent mit einem SSH-Client. Gateway-Benutzer müssen diesen Schritt überspringen.

   a) Melden Sie sich bei der NetScaler-Instanz an. Weitere Informationen finden Sie unter Zugriff auf einen NetScaler.

   b) Navigieren Sie zum Verzeichnis `/var/mastools/scripts`, und geben Sie den folgenden Befehl ein:

   Auf der SDX-Instanz

	Registrierung mit NetScaler-Profil	Registrierung ohne NetScaler-Profil
Voraussetzung	Erstellen Sie vor der Registrierung ein NetScaler-Profil. Weitere Informationen finden Sie unter So erstellen Sie ein NetScaler-Profil.		**Diesen Befehl ausführen**

| |./mastools_init.sh <device-profile-name> <service-url> <activation-code> -sdx -profile./mastools_init.sh <user_name> <service-url> <activation-code> -sdx
|Benutzeranmeldeinformationen**|Geben Sie ein. nsroot<device_profile_name> Alternativ können Sie einen Benutzernamen verwenden, der dieselben Zugriffsrechte wie nsroot hat. |Geben Sie nsroot unter <user_name> ein. Alternativ können Sie einen Benutzernamen verwenden, der dieselben Zugriffsrechte wie nsroot hat. |

> **Hinweis:**
>
> NetScaler Console erkennt alle VPX-Instanzen, die auf diesem SDX ausgeführt werden, und Sie müssen die VPX-Instanzen nicht einzeln registrieren.

Bei VPX-Instanzen, die nicht auf einer SDX-Appliance ausgeführt werden, sowie bei MPX- und Gateway-Instanzen:

Wenn die NetScaler-Image-Version niedriger als 13.0 61.x oder 12.1 57.x ist, müssen Sie die mastoolsVersion überprüfen, indem Sie den Befehl cat /var/mastools/version.txteingeben. Wenn die Ausgabe 0.0-0.0 ist, ist es das erste Mal.

Geben Sie je nach Softwareversion einen der folgenden Befehle ein.

> **Hinweis:**
>
> Bevor Sie sich mit einem NetScaler-Profil registrieren, müssen Sie das Profil erstellen. Weitere Informationen finden Sie unter So erstellen Sie ein NetScaler-Profil.

NetScaler-Image-Version	Ist mastools_version 0.0-0.0?	Befehl zur Registrierung mit Profil	Befehl zur Registrierung ohne Profil
Unter 13,0 61.xx und 12,1 57,xx	Ja	./mastools_init.sh < device_profile_name> <service_url> "MAS;<activation_code>"-profile	./mastools_init.sh <user_name><pwd> <service_url> "MAS;<activation_code>"

NetScaler-Image-Version	Ist mastools_version 0.0-0.0?	Befehl zur Registrierung mit Profil	Befehl zur Registrierung ohne Profil
Unter 13,0 61.xx und 12,1 57,xx	Nein	./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile	./mastools_init.sh <user_name><pwd> <service_url> <activation_code>
Höher als 13,0 61.x und 12.1 57,xx	Nicht zutreffend	./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile	./mastools_init.sh <user_name><pwd> <service_url> <activation_code>

> **Hinweis:**
>
> - Geben Sie <device_profile_name><user_name>oder ein nsroot. Alternativ können Sie einen Benutzernamen verwenden, der dieselben Zugriffsrechte wie nsroot hat.
> - Schließen Sie in einem HA-Paar die Registrierung auf dem primären Knoten ab. Wenn Sie die Registrierungsbefehle auf dem sekundären Knoten ausführen, wird die folgende Meldung angezeigt: **Bitte führen Sie den Registrierungsbefehl auf dem primären Knoten**aus.

4. Kehren Sie zur NetScaler Console-Seite zurück und klicken Sie auf **Instanz registrieren**.
5. Zeigen **Sie unter Instanzen hinzufügen**die Instanz an, in der Sie den integrierten Agent initiiert haben. Stellen Sie sicher, dass sich die Instanz im Status **Up** befindet, und klicken Sie auf **Weiter**.
6. Klicken Sie auf **Fertig**.

Nach erfolgreicher integrierter Agentenkonfiguration können Sie auf die Funktionen der NetScaler Console zugreifen, wie z. B.:

- **Virtueller Server und Analytik**—Wenden Sie Lizenzen auf Ihren virtuellen Server an, um NetScaler-Instanzen zu verwalten. Weitere Informationen finden Sie unter Abonnements verwalten.

- **Anwendungsdashboard** —Um alle Anwendungen auf ganzheitliche Weise anzuzeigen. Weitere Informationen finden Sie unter Anwendungsverwaltung und Dashboard.
- **Infrastrukturanalyse** —Mit dieser Funktion können Sie die Faktoren visualisieren, die zu einem Problem in den Instanzen geführt haben oder dazu führen könnten. Weitere Informationen finden Sie unter Infrastructure Analytics.

> Hinweis:
>
> Sie können den integrierten Agent auch konfigurieren, indem Sie zur Seite **Infrastruktur > Instanzen > Agents > Aktivierungscode generieren** navigieren. Kopieren Sie die URL und den Aktivierungscode, fügen Sie sie in eine NetScaler-Instanz ein und suchen Sie nach dieser Instanz.

Nachdem der integrierte Agent initiiert wurde, navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**. Auf dieser Seite werden die Details zur verwalteten Instanz angezeigt, die mit dem integrierten Agent ermittelt wurde.

Problembehandlung

Sie können die Protokolle überprüfen, wenn die Registrierung fehlschlägt oder wenn die Registrierung erfolgreich ist, der integrierte Agent jedoch nicht in der NetScaler Console-GUI angezeigt wird.

- Wenn die Registrierung fehlschlägt, checken Sie die Login `/var/mastools/logs/mastools_reg.py.log`
- Wenn die Registrierung erfolgreich ist, der integrierte Agent jedoch nicht in der NetScaler Console-GUI angezeigt wird, überprüfen Sie:
  - **mastools_Upgrade** meldet sich an `/var/mastools/logs/mastools_upgrade.log`
  - **Binär meldet** sich an `/var/log/mastoolsd.log`.

Installieren Sie einen NetScaler Agent on-premises

January 26, 2024

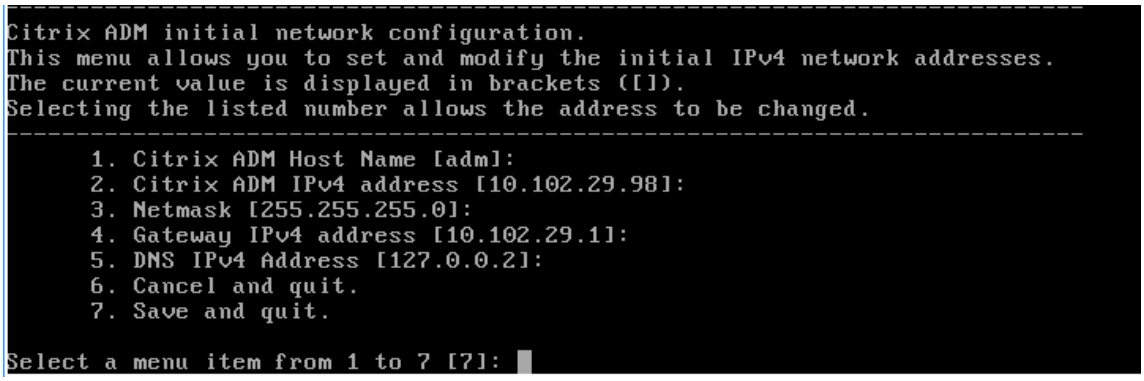
Der Agent fungiert als Vermittler zwischen der NetScaler Console und den erkannten Instanzen im Rechenzentrum.

Stellen Sie vor der Installation des Agents sicher, dass Sie über die erforderlichen virtuellen Computerressourcen verfügen, die der Hypervisor für jeden Agent bereitstellen muss. Weitere Informationen finden Sie unter Anforderungen für die Agentinstallation und Lightweight Agent für die Pool-Lizenzierung.

> **Hinweis**
>
> Alle Informationen zu Ports und anderen Anforderungen finden Sie unter Unterstützte Ports.

So installieren Sie den NetScaler Agent:

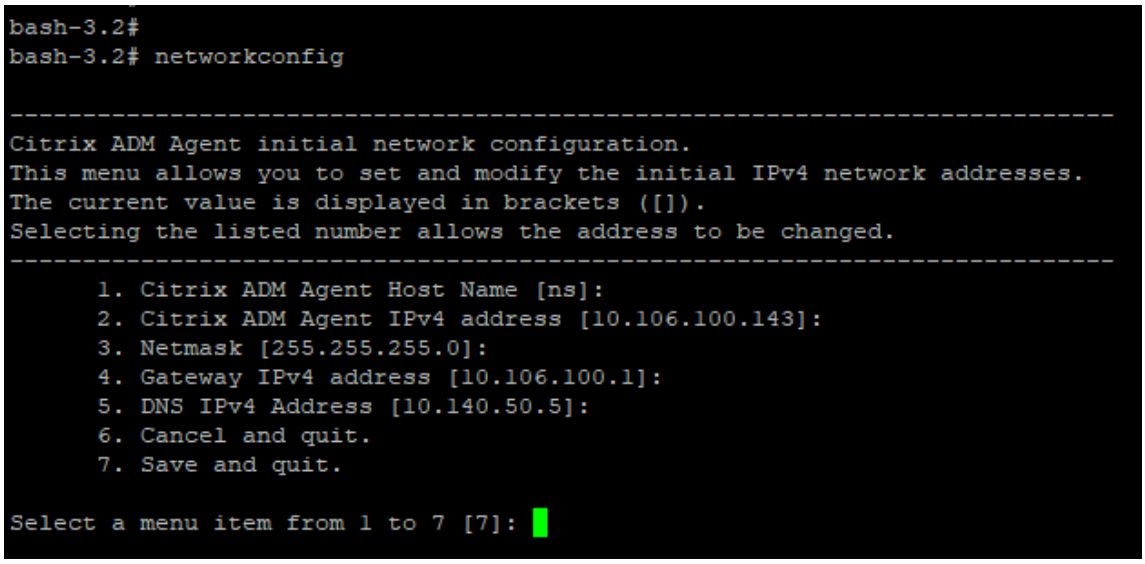
1. Laden Sie das Agentimage wie unter Erste Schrittebeschrieben herunter.
2. Importieren Sie die Agentimagedatei in Ihren Hypervisor.
3. Konfigurieren Sie auf der Registerkarte **Konsole** die anfänglichen Netzwerkkonfigurationsoptionen wie im folgenden Beispiel gezeigt:



> **Hinweis** Stellen Sie sicher, dass Sie Ihr DNS so konfigurieren, dass Ihr NetScaler Agent auf das Internet zugreifen kann.

4. Nach Abschluss der anfänglichen Netzwerkkonfiguration speichern Sie die Konfigurationseinstellungen. Wenn Sie dazu aufgefordert werden, melden Sie sich mit den Standardanmeldeinformationen()`nsrecover`/`nsroot` an.

   Wenn Sie die konfigurierten Netzwerkeinstellungen auf dem Agent ändern möchten, geben Sie den Befehl `networkconfig` ein und folgen Sie den Anweisungen in der CLI.

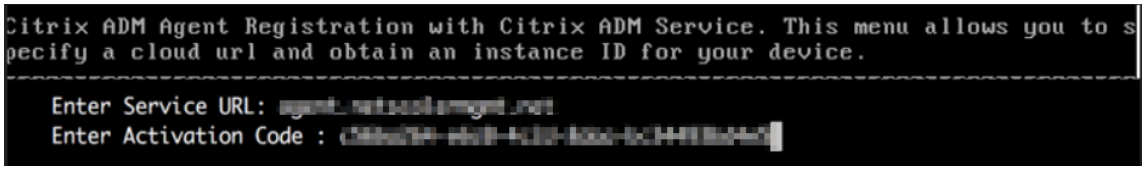


5. Wenn Sie nicht aufgefordert werden, die Service-URL einzugeben, navigieren Sie im NetScaler Agent zu /mps und führen Sie dann eines der folgenden Skripts aus:

```
deployment_type.py
```

```
register_agent_cloud.py
```

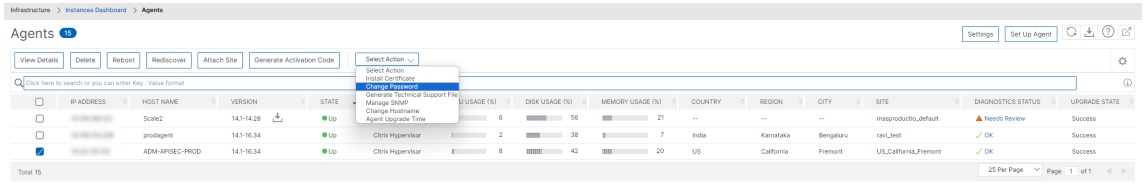
6. Geben Sie die **Service-URL** und den **Aktivierungscode** ein, die Sie gespeichert haben, als Sie das Agentimage heruntergeladen haben. Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.



7. Nach erfolgreicher Agentregistrierung wird der Agent neu gestartet, um den Installationsvorgang abzuschließen.

Rufen Sie nach dem Neustart des Agents die NetScaler Console-GUI auf und navigieren Sie zu **Infrastruktur > Instanzen > Agents**, um den Status des Agenten zu überprüfen. Nachdem der Agent konfiguriert wurde, müssen Sie das Kennwort ändern.

1. Navigieren Sie zu **Infrastruktur > Instanzen > Agents**
2. Wählen Sie den Agent aus und klicken Sie in der Liste **Aktion auswählen** auf **Kennwort ändern**.



3. Geben Sie das aktuelle Kennwort (`nsroot`) ein, geben Sie ein neues Kennwort ein und klicken Sie auf **OK**, um das Kennwort zu ändern.

   Das Kennwort muss:

   - Mindestens sechs Zeichen lang sein
   - Mindestens ein Sonderzeichen haben
   - Mindestens einen Großbuchstaben haben
   - Mindestens einen Kleinbuchstaben haben
   - Mindestens ein numerisches Zeichen haben

Installieren Sie einen NetScaler Agent in der Microsoft Azure Cloud

January 26, 2024

Der Agent fungiert als Vermittler zwischen der NetScaler Console und den verwalteten Instanzen im Unternehmensrechenzentrum oder in der Cloud.

Um den NetScaler Agent in der Microsoft Azure Cloud zu installieren, müssen Sie eine Instanz des Agenten im virtuellen Netzwerk erstellen. Rufen Sie das NetScaler Agent-Image vom Azure Marketplace ab und verwenden Sie dann das Azure Resource Manager-Portal, um den Agenten zu erstellen.

Bevor Sie mit der Erstellung der NetScaler Agent-Instanz beginnen, stellen Sie sicher, dass Sie ein virtuelles Netzwerk mit den erforderlichen Subnetzen erstellt haben, in denen sich die Instanz befindet. Sie können während des VM-Provisionings virtuelle Netzwerke erstellen, jedoch ohne die Flexibilität, verschiedene Subnetze einzurichten. Hinweise zum Erstellen virtueller Netzwerke finden Sie unter http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network.

Konfigurieren Sie die DNS-Server- und VPN-Konnektivität, die es einer virtuellen Maschine ermöglicht, auf Internetressourcen zuzugreifen.

Voraussetzungen

Stellen Sie sicher, dass Sie Folgendes haben:

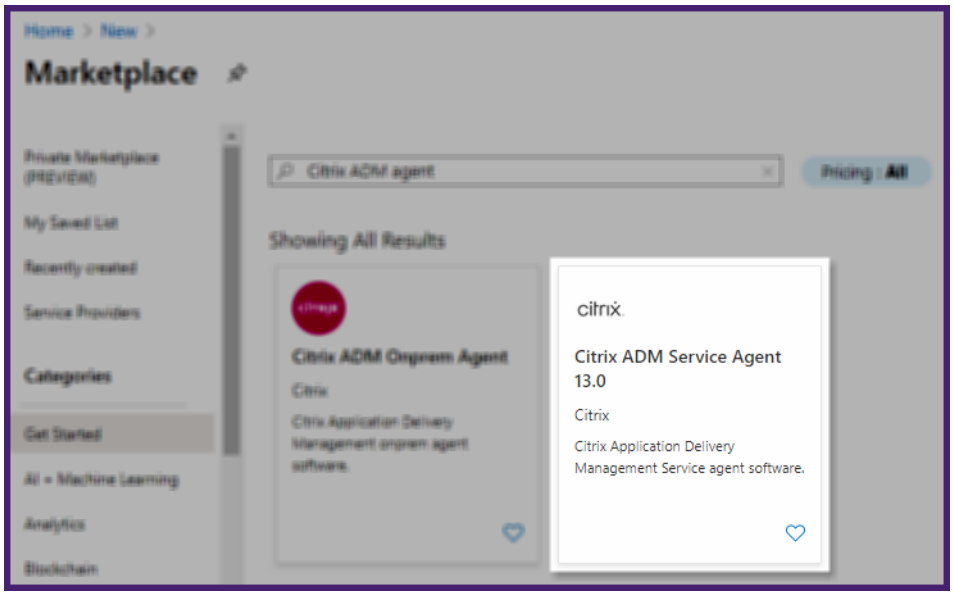
- Ein Microsoft Azure-Benutzerkonto
- Zugriff auf Microsoft Azure Resource Manager

> **Hinweis**
>
> - Es wird empfohlen, eine Ressourcengruppe, eine Netzwerksicherheitsgruppe, ein virtuelles Netzwerk und andere Entitäten zu erstellen, bevor Sie die virtuelle NetScaler Agent-Maschine bereitstellen, damit die Netzwerkinformationen während der Bereitstellung verfügbar sind.
> - Stellen Sie sicher, dass die empfohlenen Ports geöffnet sind, damit der NetScaler Agent mit der NetScaler Console und den NetScaler-Instanzen kommunizieren kann. Vollständige Informationen zu den Port-Anforderungen für den NetScaler Agent finden Sie unter Ports.

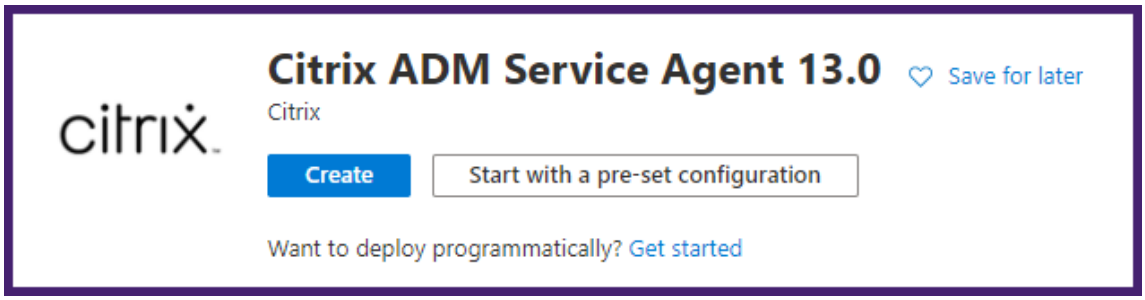
So installieren Sie den NetScaler Agent in der Microsoft Azure Cloud:

1. Melden Sie sich mit Ihren Microsoft Azure-Anmeldeinformationen beim Azure-Portal (https://portal.azure.com) an.
2. Klicken Sie auf **+Eine Ressource erstellen**.

3. Geben Sie `NetScaler agent`in die Suchleiste ein und wählen Sie **NetScaler Agent** aus.



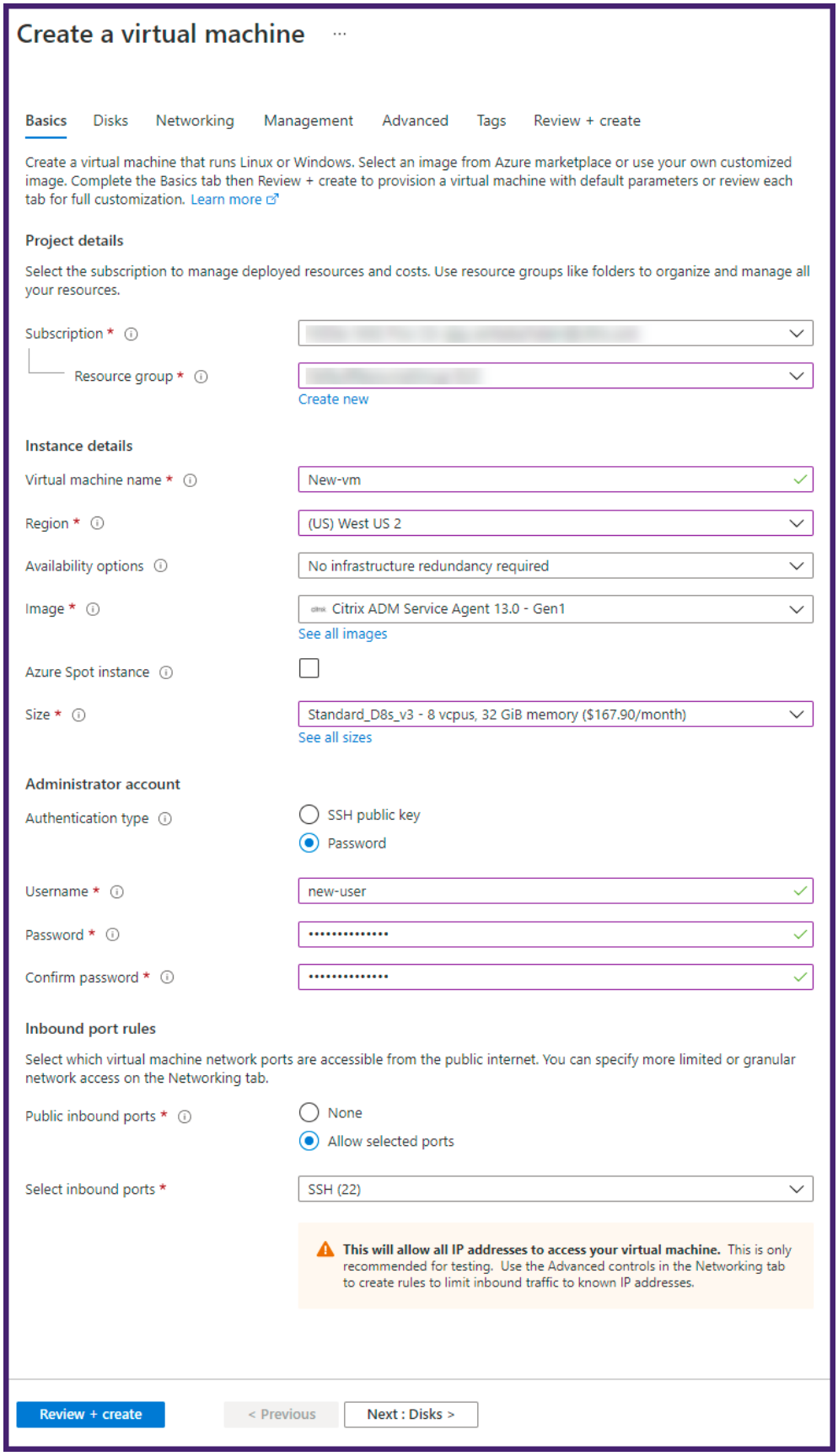
4. Klicken Sie auf **Erstellen**.



5. Geben Sie im Bereich **Virtuelle Maschine erstellen** in jedem Abschnitt die erforderlichen Werte an, um eine virtuelle Maschine zu erstellen.

   Grundlagen:

   Geben Sie auf dieser Registerkarte **Projektdetails**, **Instanzdetails**und **Administratorkonto**an.



- **Ressourcengruppe** —Wählen Sie die Ressourcengruppe, die Sie erstellt haben, aus der Dropdownliste aus.

  > Hinweis: Sie können an dieser Stelle eine Ressourcengruppe erstellen, wir empfehlen jedoch, im Azure Resource Manager eine Ressourcengruppe aus Ressourcengruppen zu erstellen und dann die Gruppe aus der Dropdownliste auszuwählen.**

- **Name**der virtuellen Maschine —Geben Sie einen Namen für die NetScaler Agent-Instanz an.
- **Region** - Wählen Sie die Region aus, in der Sie einen Agent ausbringen möchten.
- **Verfügbarkeitsoptionen** —Wählen Sie den Verfügbarkeitssatz aus der Liste aus.
- **Bild** - In diesem Feld wird das bereits ausgewählte Agentimage angezeigt. Wenn Sie zu einem anderen Agentimage wechseln möchten, wählen Sie das gewünschte Image aus der Liste aus.
- **Größe**—Geben Sie den Typ und die Größe des virtuellen Laufwerks für die Bereitstellung Ihres NetScaler Agents an.

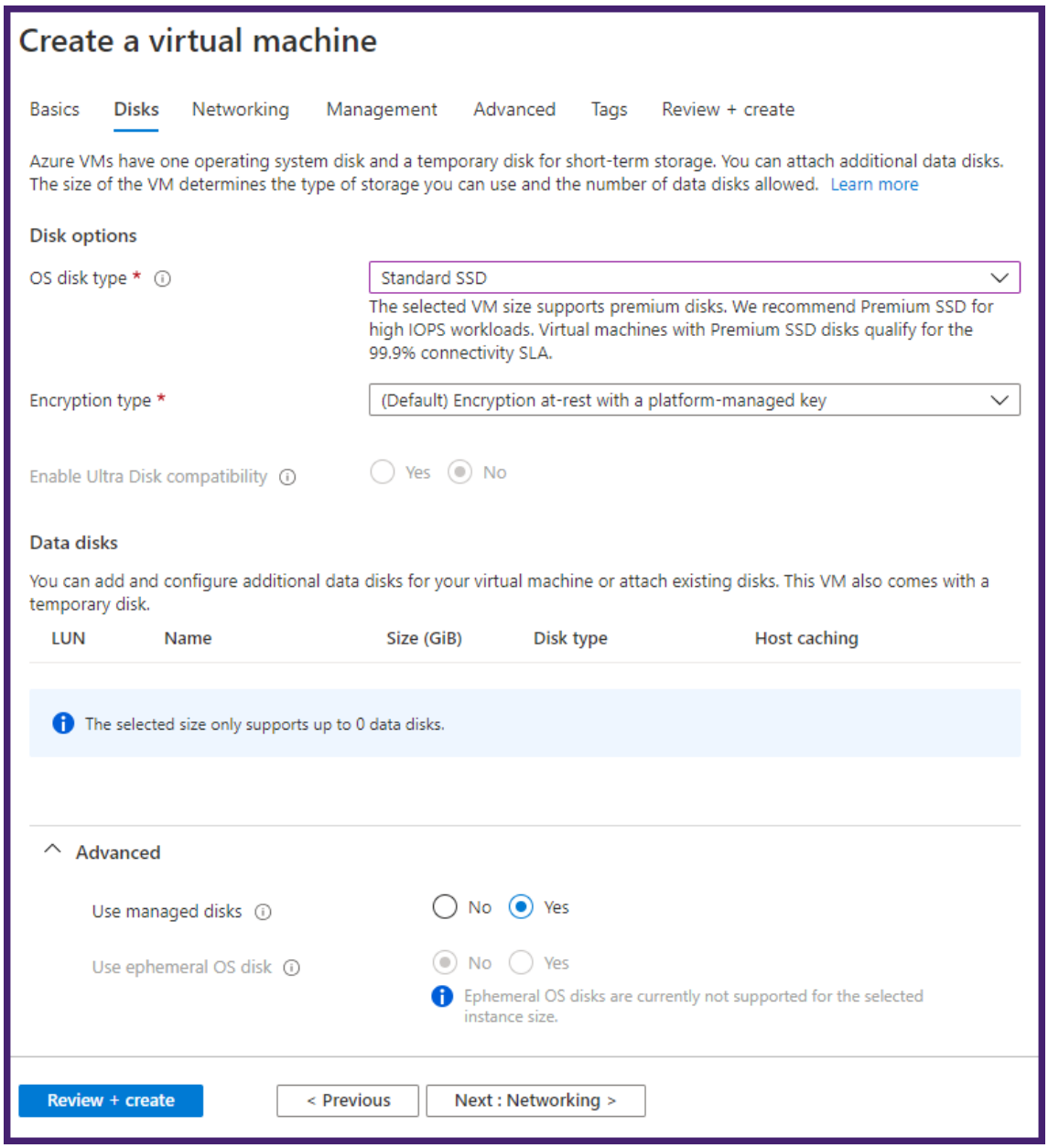
  Wählen Sie den Typ Unterstützte virtuelle Laufwerke (**HDD** oder **SSD**) aus der Liste aus.

  Weitere Informationen zu unterstützten virtuellen Laufwerksgrößen finden Sie unter Anforderungen für die Agentinstallation und Lightweight Agent für die Pool-Lizenzierung.
- **Authentifizierungstyp** —Wählen Sie Kennwort aus.
- **Benutzername und Kennwort** —Geben Sie einen Benutzernamen und ein Kennwort an, um auf die Ressourcen in der von Ihnen erstellten Ressourcengruppe zuzugreifen.

  > **Wichtig**
  >
  > Wir empfehlen Ihnen, Ihren eigenen Benutzernamen und Ihr Kennwort für Ihren Agenten anzugeben. Verwenden Sie `nsrecover` oder `nsroot` nicht als Benutzernamen, da diese für Agentbenutzer reserviert sind.

Datenträger:

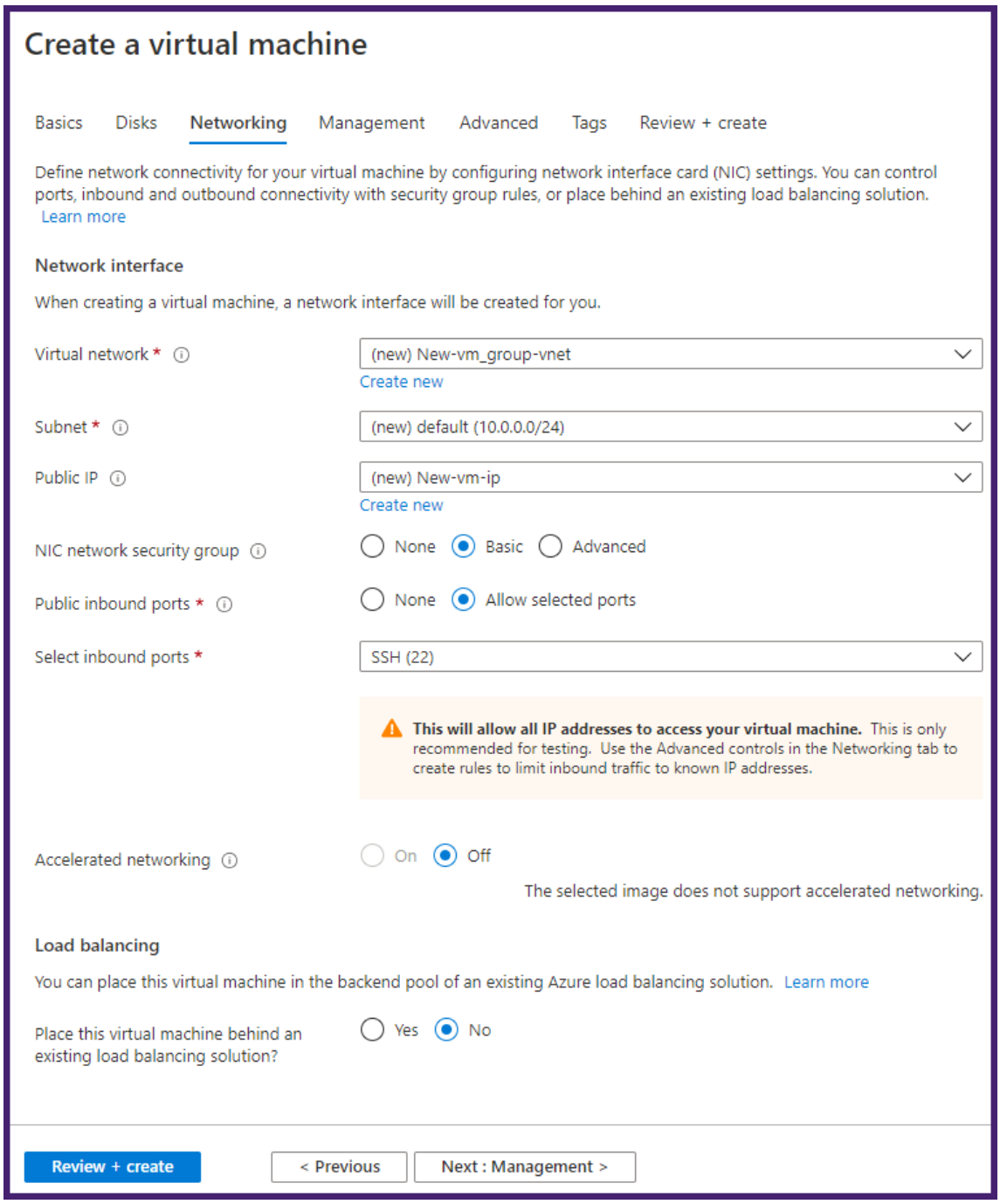
Auf dieser Registerkarte geben Sie **Datenträgeroptionen** und **Datendatenträger**an.



- **Betriebssystemdatenträgertyp** - Wählen Sie den Typ des virtuellen Laufwerks (HDD oder SSD) aus.

Vernetzung:

Geben Sie die erforderlichen Netzwerkdetails an:



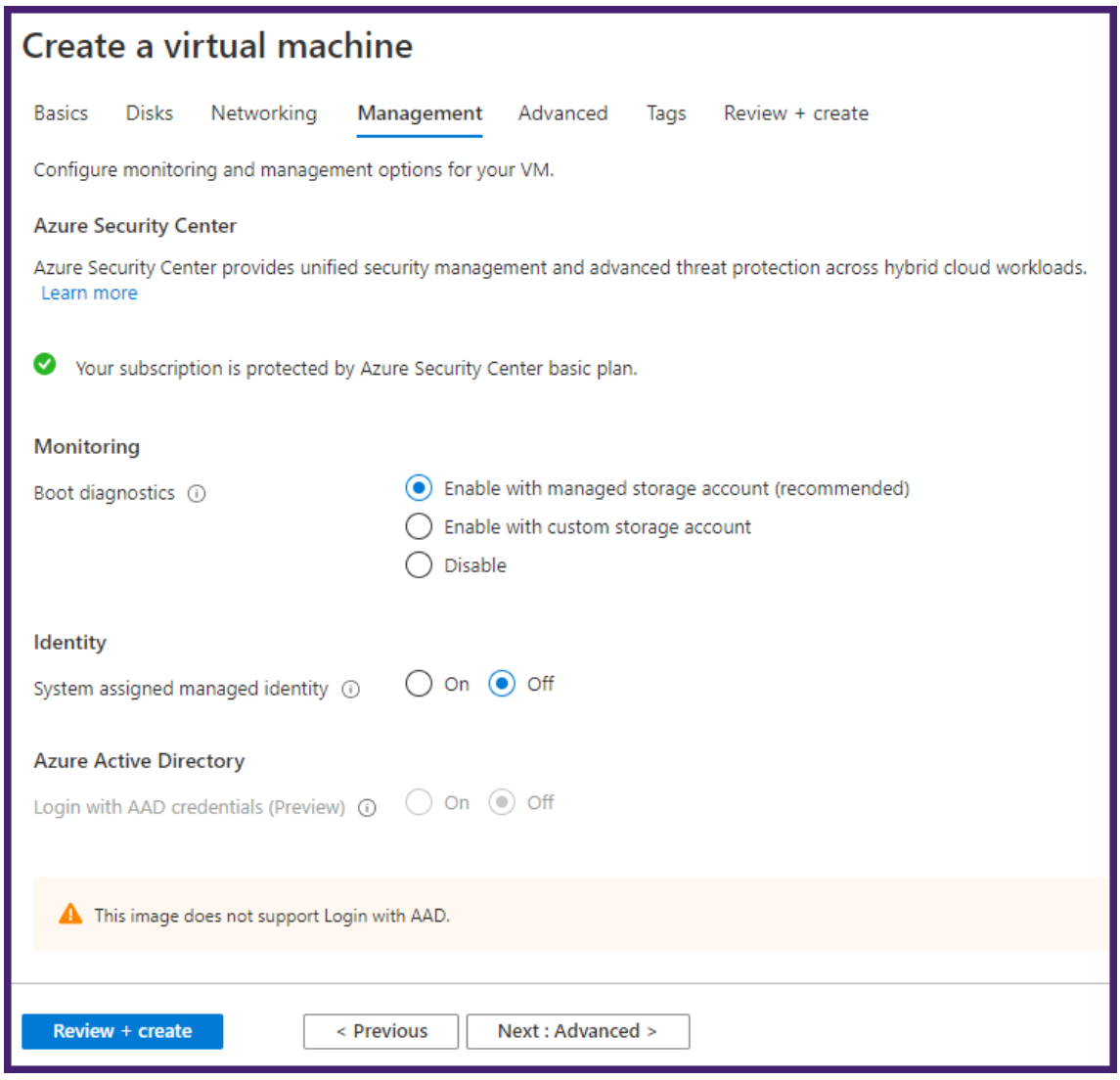
- **Virtuelles Netzwerk** —Wählen Sie das virtuelle Netzwerk aus.
- **Subnet** —Legen Sie die Subnetzadresse fest.
- **Öffentliche IP-Adresse** —Wählen Sie optional die IP-Adresse aus.
- **Netzwerksicherheitsgruppe** —Wählen Sie optional die Sicherheitsgruppe aus, die Sie erstellt haben.
- **Eingehende Ports auswählen** - Wenn Sie öffentliche eingehende Ports zulassen, stellen Sie sicher, dass die eingehenden und ausgehenden Regeln in der Sicherheitsgruppe kon-

figuriert sind. Wählen Sie dann die eingehenden Ports aus der Liste aus. Weitere Einzelheiten finden Sie unter Voraussetzungen.

> **Hinweis Stellen Sie**
>
> sicher, dass der Agent über Internetzugang verfügt.

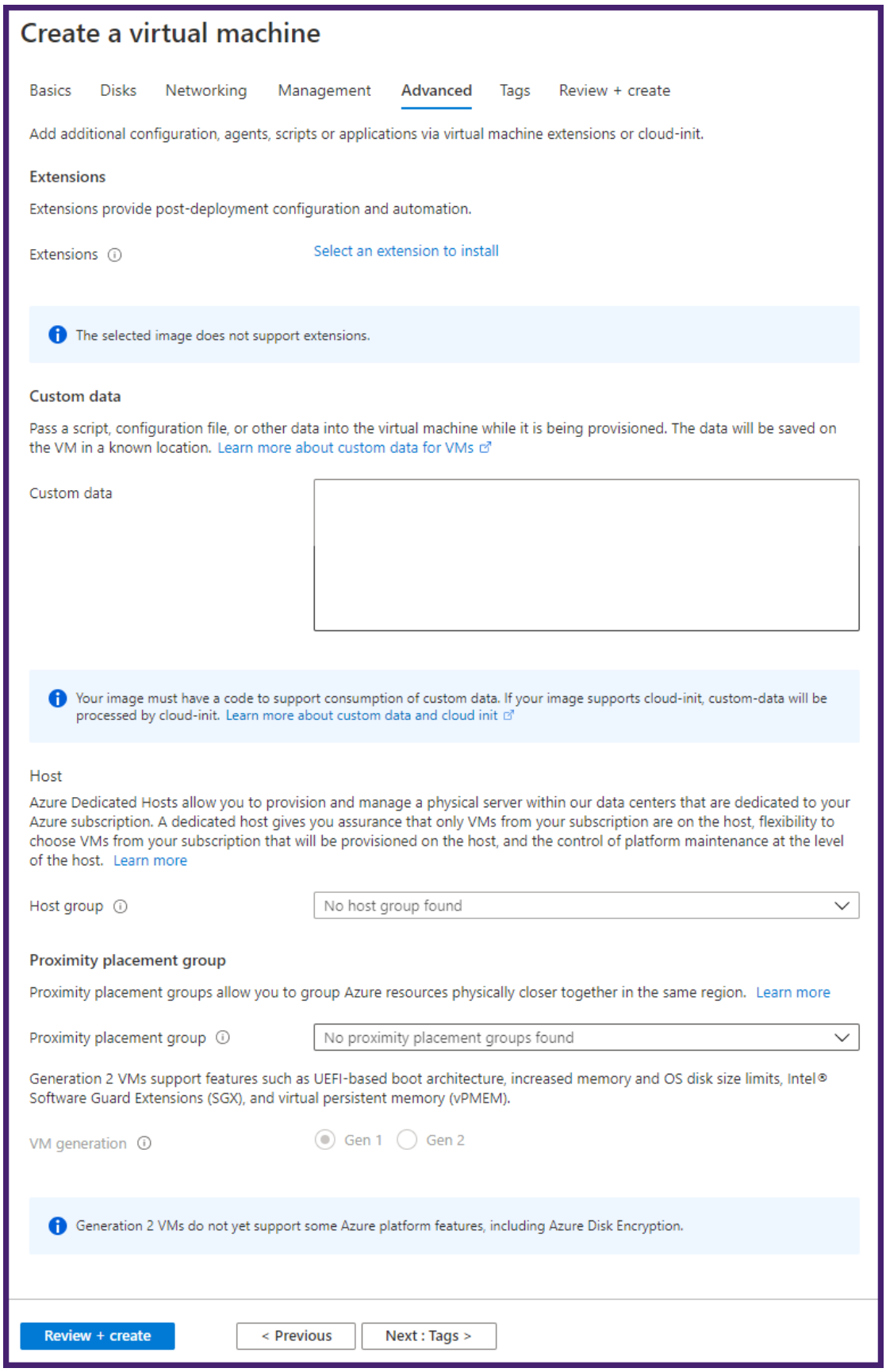
Verwaltung:

Geben Sie **Azure Security Center**, **Überwachung**und **Identität**an.



Fortgeschritten:

Optional geben Sie **Erweiterungen**, **benutzerdefinierte Daten**und **Proximity-Platzierungsgruppe**an.

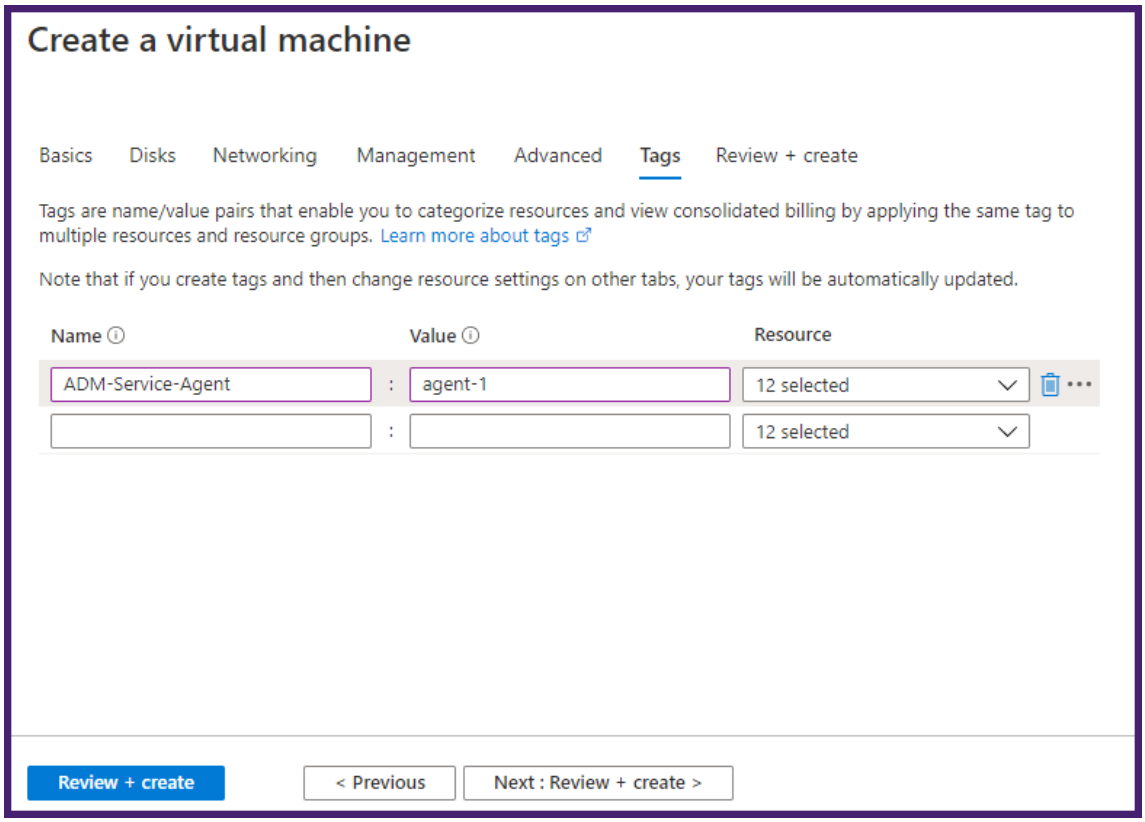


> **Hinweis**
>
> Geben Sie unter **Benutzerdefinierte Daten** die **Service-URL** und **den Aktivierungscode**an, die Sie von der Seite „ **Agenten einrichten** “in NetScaler Console kopiert haben, wie unter Erste Schritte beschrieben. Geben Sie die Details im folgenden Format ein:
>
> ```
> registeragent -serviceurl <apigatewayurl> -activationcode <
>    activationcodevalue>
> ```
>
> Der Agent verwendet diese Informationen, um sich beim Booten automatisch bei der NetScaler Console zu registrieren.

Wenn Sie dieses Skript für die automatische Registrierung angeben, überspringen Sie Schritt 7 und 8.

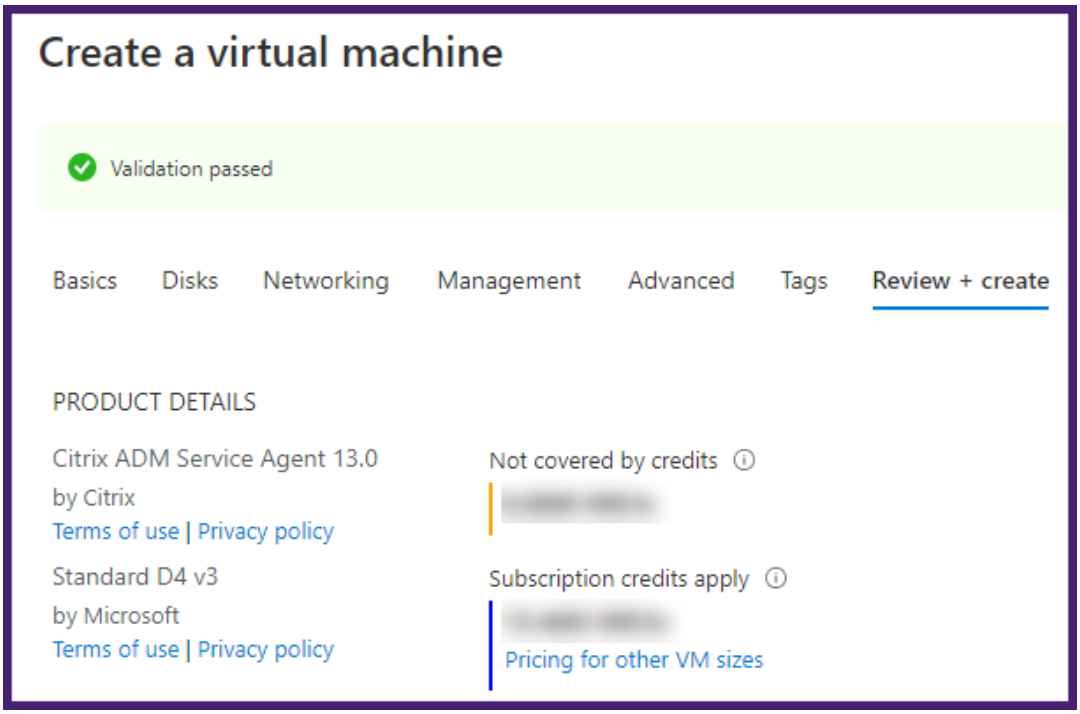
Tags:

Geben Sie das Schlüssel-Wert-Paar für die NetScaler Agent-Tags ein. Ein Tag besteht aus einem Schlüssel-Wert-Paar, das zwischen Groß- und Kleinschreibung unterschieden wird. Mit diesen Tags können Sie den Agent einfach organisieren und identifizieren. Die Tags werden sowohl auf Azure als auch auf NetScaler Console angewendet.

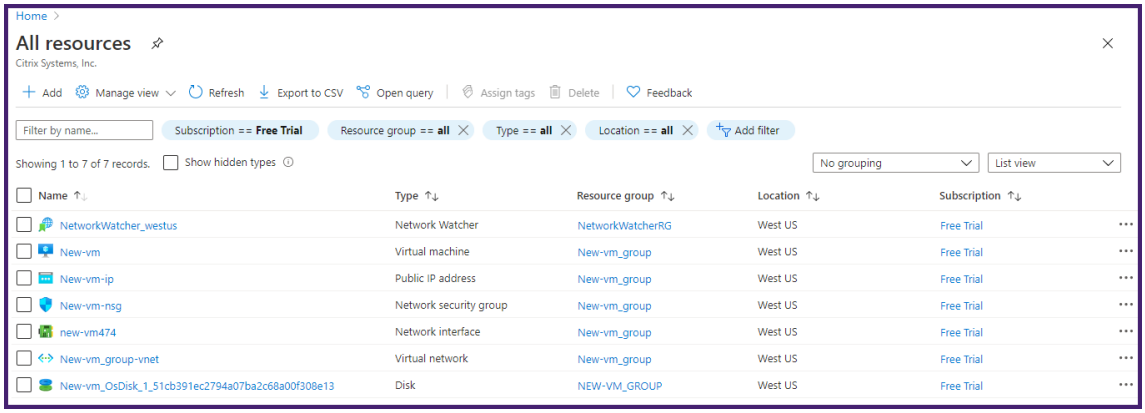


Die Konfigurationseinstellungen werden überprüft, und auf der Registerkarte **Überprüfen und erstellen** wird das Ergebnis der Validierung angezeigt.

- Wenn die Validierung fehlschlägt, zeigt diese Registerkarte den Grund für den Fehler an. Gehen Sie zurück zum jeweiligen Abschnitt und nehmen Sie ggf. Änderungen vor.
- Wenn die Validierung erfolgreich ist, klicken Sie auf **Erstellen**. Der Prozess der Agentbereitstellung beginnt.

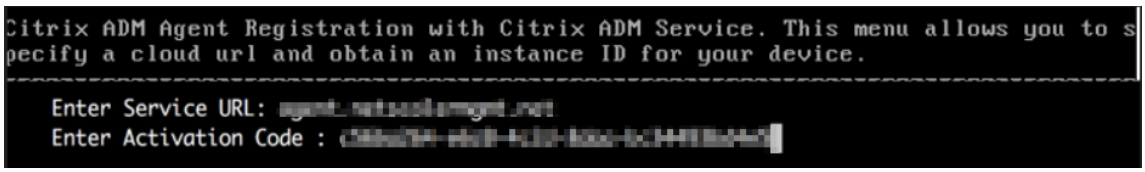


Der Bereitstellungsprozess kann etwa 10 bis 15 Minuten dauern. Sobald die Bereitstellung erfolgreich abgeschlossen ist, können Sie Ihre virtuelle NetScaler Agent-Maschine in Ihrem Microsoft Azure-Konto anzeigen.



6. Sobald der Agent betriebsbereit ist, verwenden Sie einen SSH-Client, um sich bei Ihrem NetScaler Agent anzumelden. Verwenden Sie den Benutzernamen und das Kennwort, die bei der Erstellung der virtuellen Maschine angegeben wurden.
7. Führen Sie das Bereitstellungsskript aus, indem Sie den Befehl an der Shell-Eingabeaufforderung eingeben: **deployment_type.py**.

8. Geben Sie die **Service-URL** und den **Aktivierungscode ein**, den Sie auf der Seite „ **Agenten einrichten** “in NetScaler Console kopiert und gespeichert haben, wie unter Erste Schritte beschrieben. Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.



Nach erfolgreicher Agentregistrierung wird der Agent neu gestartet, um den Installationsvorgang abzuschließen.

Rufen Sie nach dem Neustart des Agents die NetScaler Console auf und überprüfen Sie auf der Seite „ **Agent** einrichten “unter **Discovered Agents** den Status des Agents.

Installieren Sie einen NetScaler Agent auf Amazon Web Services (AWS)

January 26, 2024

Der NetScaler Agent fungiert als Vermittler zwischen der NetScaler Console und den erkannten Instanzen im Rechenzentrum oder in der Cloud.

Voraussetzungen

Um ein NetScaler Agent-AMI in einer Amazon Web Services (AWS) Virtual Private Cloud (VPC) mithilfe der Amazon-GUI zu starten, benötigen Sie:

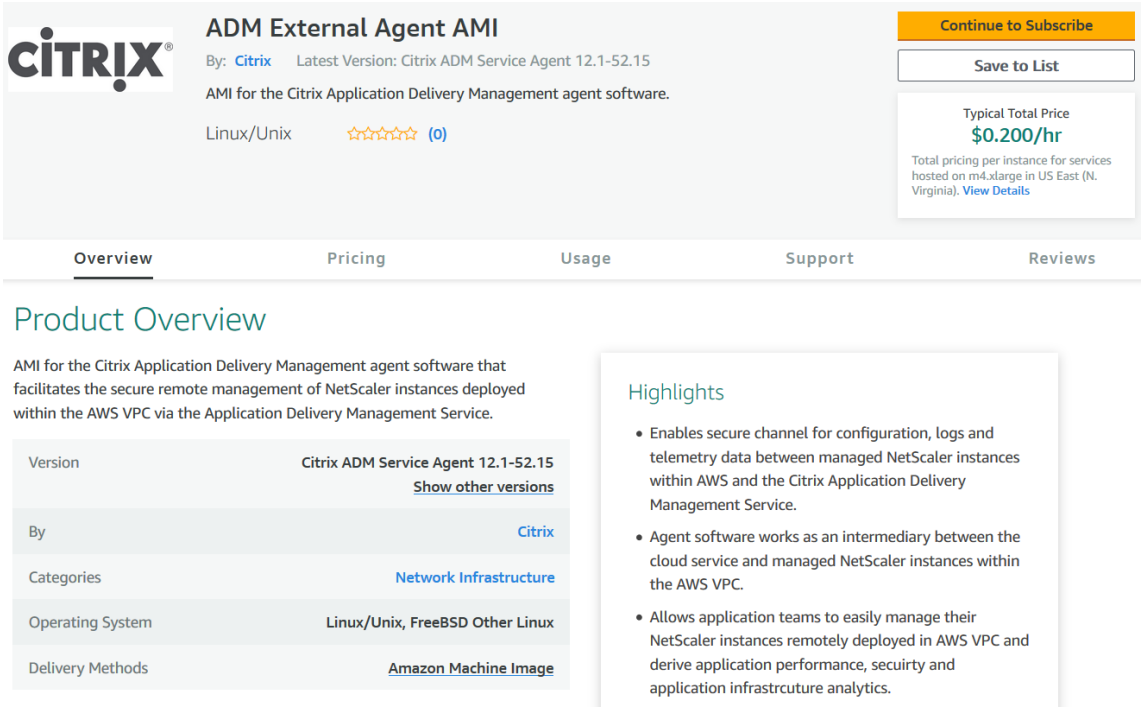
- Ein AWS-Konto
- Eine virtuelle Private Cloud (VPC) von AWS
- Ein IAM-Konto

> **Hinweis**
>
> - Bevor Sie eine virtuelle NetScaler Agent-Maschine bereitstellen, empfiehlt Citrix, eine Sicherheitsgruppe, ein virtuelles privates Netzwerk, ein Schlüsselpaar, ein Subnetz und andere Entitäten zu erstellen. Daher stehen die Netzwerkinformationen während der Provisioning zur Verfügung.
> - Damit ein NetScaler Agent mit der NetScaler Console und den NetScaler-Instanzen kommunizieren kann, stellen Sie sicher, dass die empfohlenen Ports geöffnet sind. Vollständige

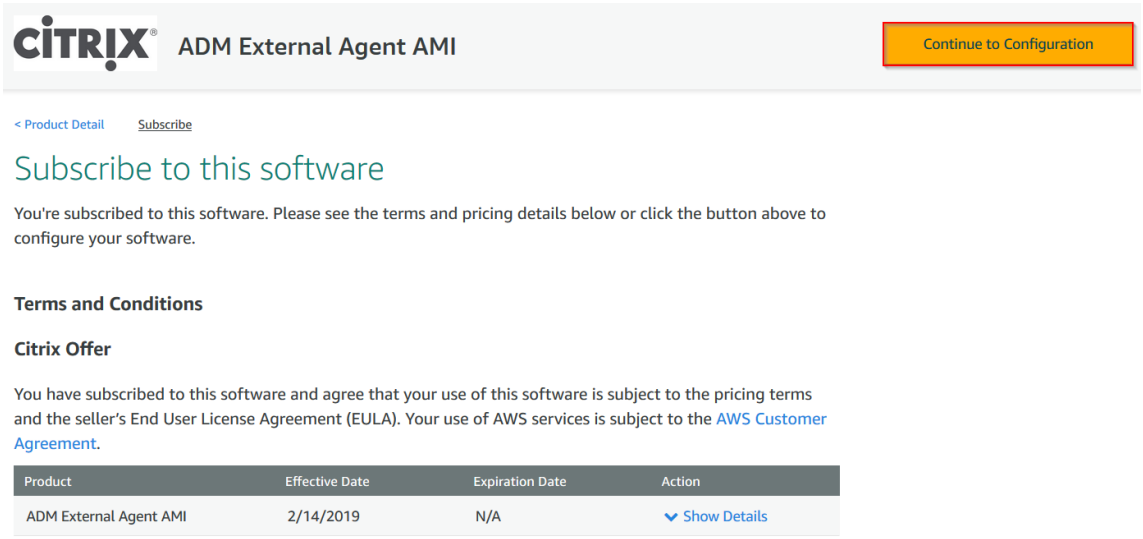
> Informationen zu den Portanforderungen für einen NetScaler Agent finden Sie unter Ports.

So installieren Sie den NetScaler Agent auf AWS:

1. Melden Sie sich mit Ihren AWS-Anmeldeinformationen am AWS-Marketplace an .
2. Geben Sie in das Suchfeld **NetScaler Agent** ein, um nach dem NetScaler Agent-AMI zu suchen, und klicken Sie auf **Los**.
3. Klicken Sie auf der Suchergebnisseite in der verfügbaren Liste auf das **NetScaler Console External Agent AMI** .
4. Klicken Sie auf der Seite **NetScaler Console External Agent AMI** auf **Continue to Subscribe**.



5. Nachdem das Abonnement erfolgreich war, klicken Sie auf **Weiter zur Konfiguration**.



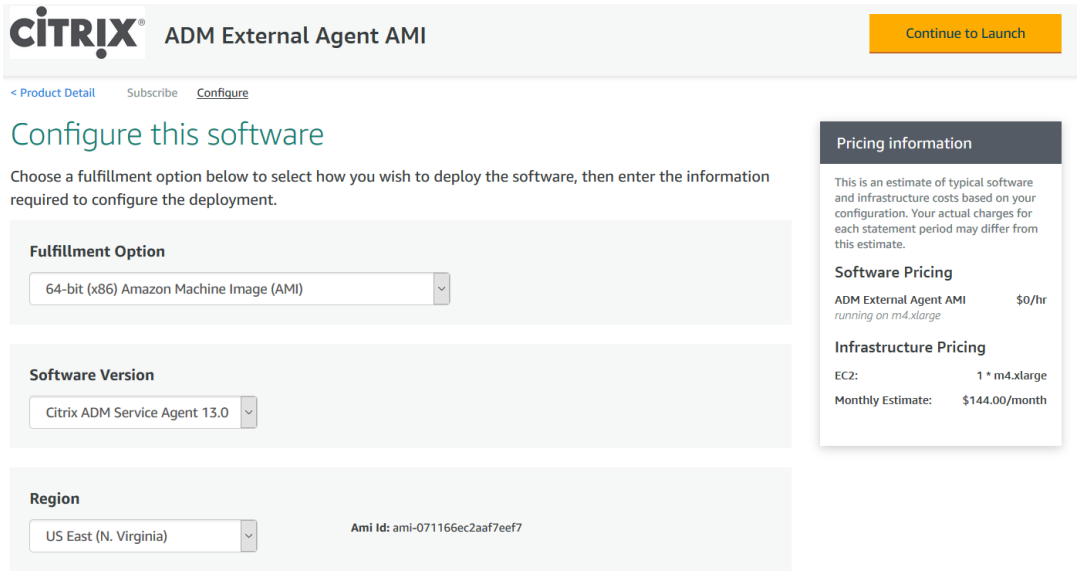
6. Auf der Seite **Diese Software konfigurieren** :

   a) Wählen Sie das AMI aus der **Optionsliste Fulfillment** aus.

   b) Wählen Sie die neueste NetScaler Agent-Version aus der Liste der Softwareversionen aus.**

   c) Wählen Sie Ihre Region aus der Liste **Region** aus.

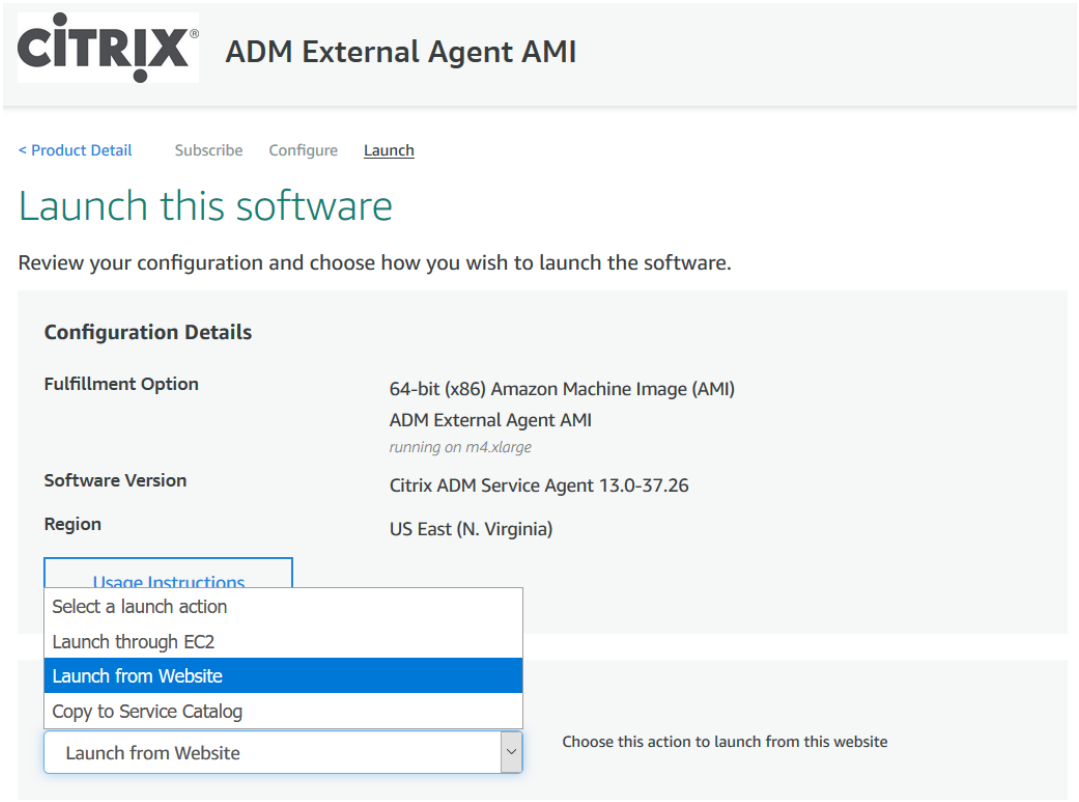
   d) Klicken Sie auf **Weiter zum Starten**



7. Auf der Seite **Diese Software starten** haben Sie zwei Möglichkeiten, den NetScaler Agent zu registrieren:

   a) **Von der Website aus starten**

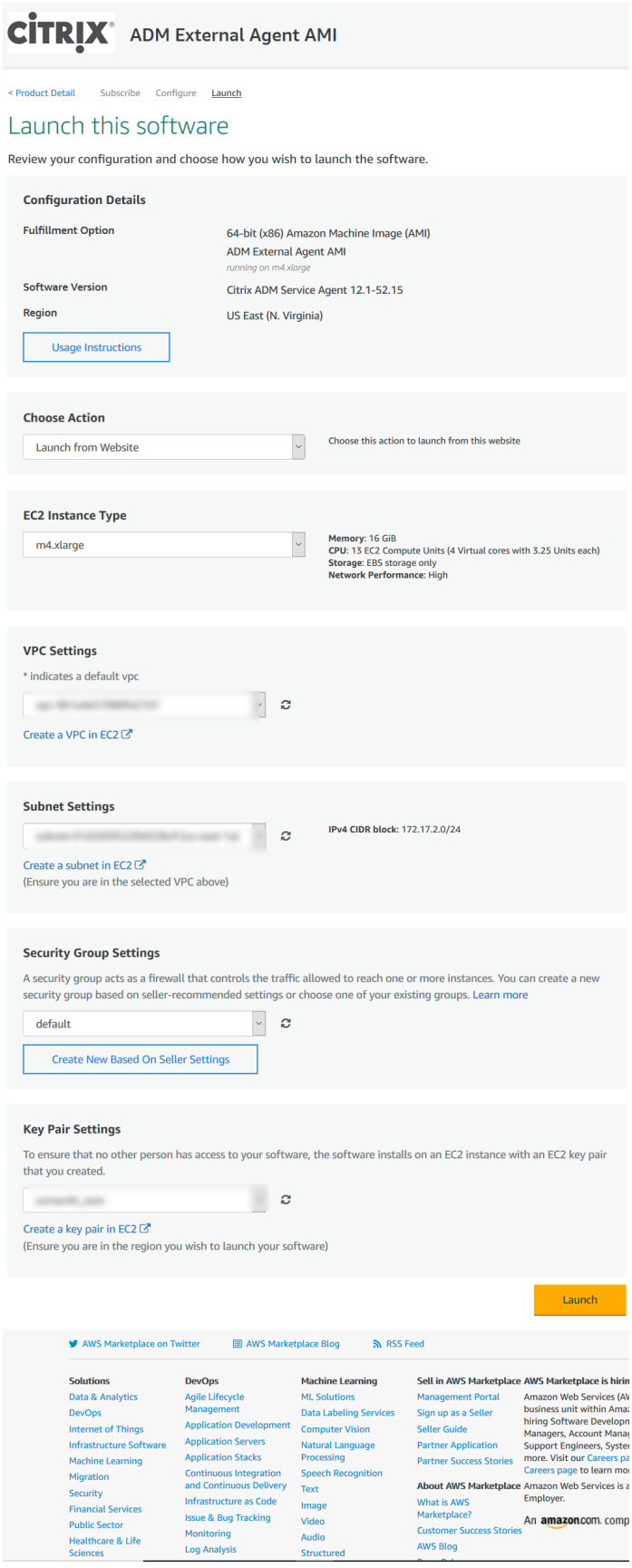
   b) **Starten Sie mit EC2**



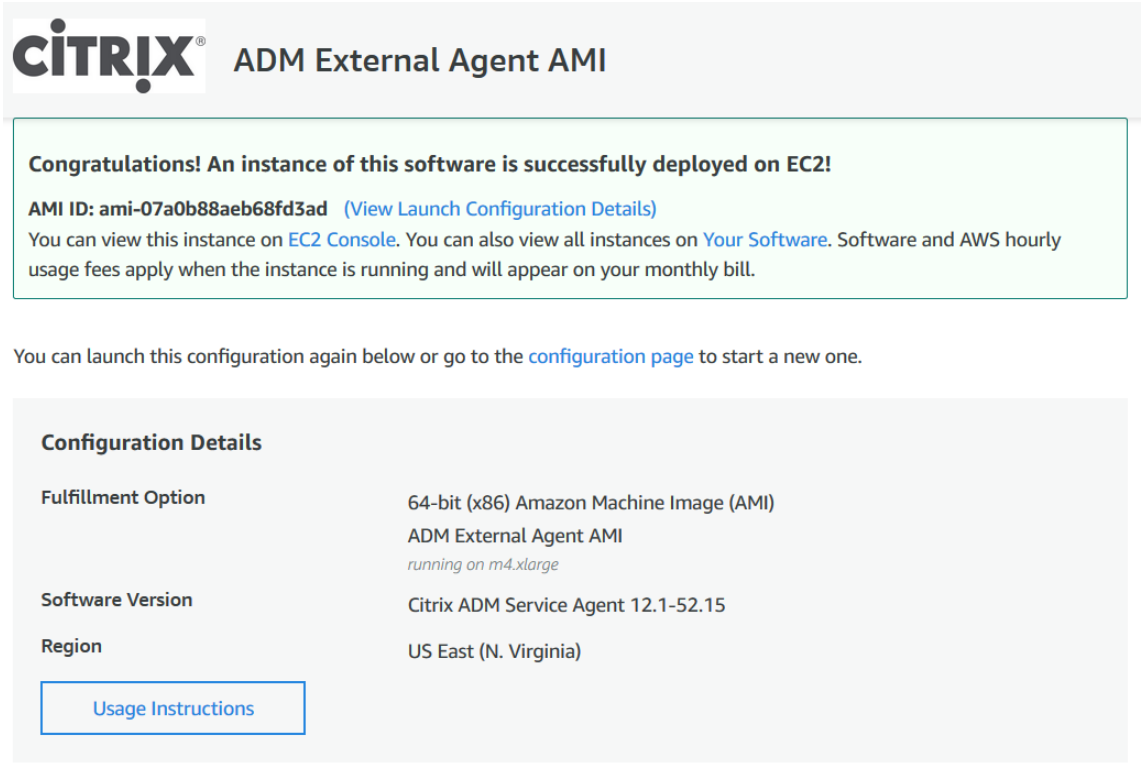
Von einer Website aus starten

Um von einer Website aus zu starten, wählen Sie:

1. Ein EC2-Instanztyp aus der Liste **EC2-Instanztyp**
2. Eine VPC aus der Liste der **VPC-Einstellungen** . Klicken Sie auf **Create a VPC in EC2**, um eine VPC für Ihre Software zu erstellen.
3. Ein Subnetz aus der Liste **Subnetzeinstellungen** . Klicken Sie auf **Subnetz erstellen in EC2**, um ein Subnetz zu erstellen, nachdem Sie die VPC ausgewählt haben.
4. Eine Sicherheitsgruppe für die Firewall aus der Liste **Sicherheitsgruppeneinstellungen** . Klicken Sie auf **Basierend auf Verkäufereinstellungen neu erstellen**, um eine Sicherheitsgruppe zu erstellen.
5. Ein Schlüsselpaar zur Gewährleistung der Zugriffssicherheit aus der Liste **Schlüsselpaareinstellungen** . Klicken Sie auf **Create a key pair in EC2**, um ein Schlüsselpaar für Ihre Software zu erstellen.
6. Klicken Sie auf **Starten**



7. Der Start von einer Website ist erfolgreich.



> **Hinweis**
>
> Der Bereitstellungsprozess kann etwa 10 bis 15 Minuten dauern. Nachdem die Bereitstellung erfolgreich abgeschlossen wurde, können Sie Ihre virtuelle NetScaler Agent-Maschine in Ihrem AWS-Konto anzeigen.

8. Sobald der Agent bereitgestellt ist, weisen Sie Ihrem NetScaler Agent einen Namen zu.
9. Sobald der Agent betriebsbereit ist, weisen Sie Ihrem NetScaler Agent eine elastische IP-Adresse zu.

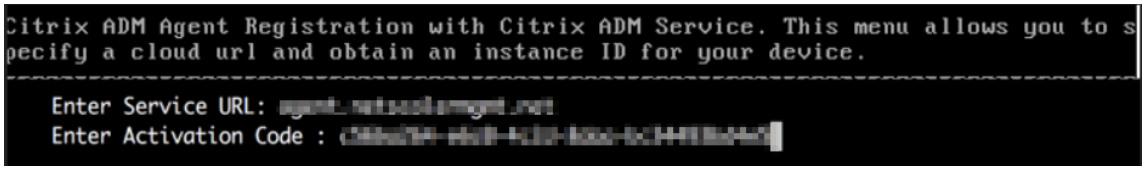
> **Hinweis**
>
> Die elastische IP-Adresse ermöglicht es dem NetScaler Agent, mit der NetScaler Console zu kommunizieren. Eine elastische IP-Adresse ist jedoch möglicherweise nicht erforderlich, wenn Sie NAT Gateway so konfiguriert haben, dass der Datenverkehr an das Internet weitergeleitet wird.

10. Melden Sie sich mit einem SSH-Client bei Ihrem NetScaler Agent an.

> **Hinweis** Sie können sich auf eine der folgenden Arten am NetScaler Agent anmelden:
>
> - Verwenden Sie `nsrecover` als Benutzernamen und AWS-Instanz-ID als Kennwort.

> • Verwenden Sie `nsroot` als Benutzernamen und ein gültiges Schlüsselpaar als Kennwort.

11. Geben Sie den folgenden Befehl ein, um den Bereitstellungsbildschirm aufzurufen: **deployment_type.py**
12. Geben Sie die **Service-URL** und den **Aktivierungscode ein**, den Sie auf der Seite „ **Agenten einrichten** “in NetScaler Console kopiert und gespeichert haben, wie unter Erste Schritte beschrieben. Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.



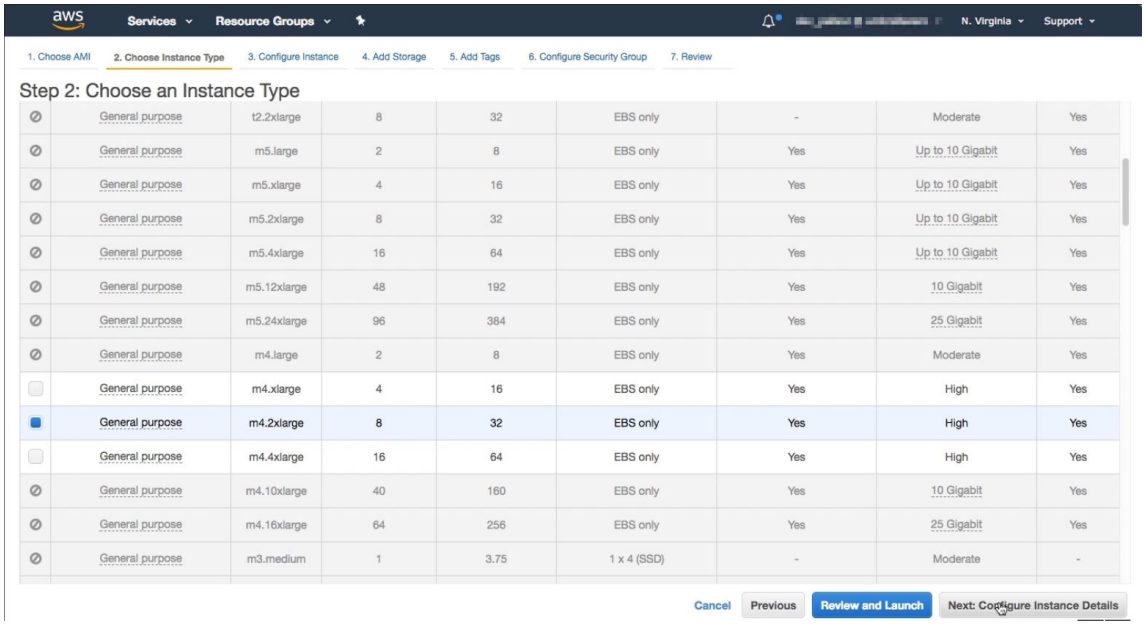
Nach erfolgreicher Agentregistrierung wird der Agent neu gestartet, um den Installationsvorgang abzuschließen.

Rufen Sie nach dem Neustart des Agents die NetScaler Console auf und überprüfen Sie auf der Seite „ **Agent** einrichten “unter **Discovered Agents** den Status des Agents.

Starten Sie mit EC2

Um mit EC2 zu starten, wählen Sie **Start über EC2** aus der Liste **Aktion auswählen** aus, und klicken Sie dann auf **Starten**.

1. **Wählen Sie auf der Seite Choose an Instanz Type** die Instanz aus und klicken Sie auf **Next: Configure Instanz Details**.



2. Geben Sie auf der Seite **Configure Instanz Details** die erforderlichen Parameter an.

   Im Abschnitt **Erweiterte Details** können Sie einen Zero-Touch-Agent aktivieren, indem Sie Authentifizierungsdetails oder ein Skript im Feld **Benutzerdaten** angeben.

   - **Authentifizierungsdetails**—Geben Sie die **Service-URL** und **den Aktivierungscode**an, die Sie von der Seite „ **Agenten einrichten** “in NetScaler Console kopiert haben, wie unter Erste Schritte beschrieben. Geben Sie die Details im folgenden Format ein.

     ```
     registeragent -serviceurl <apigatewayurl> -activationcode <
         activationcodevalue>
     ```

     Der Agent verwendet diese Informationen, um sich beim Booten automatisch bei der NetScaler Console zu registrieren.

   - **Skript** - Geben Sie ein Skript zur automatischen Registrierung des Agent als Benutzerdaten an. Das Folgende ist ein Beispielskript:

     ```
     #!/var/python/bin/python2.7
     import os
     import requests
     import json
     import time
     import re
     import logging
     import logging.handlers
     import boto3

     '''
     Overview of the Script:
     The script helps to register a NetScaler agent with NetScaler
         Console. Pass it in userdata to make NetScaler agent in
     ```



```
    AWS to autoregister on bootup. The workflow is as follows
14  1)  Fetch the NetScaler Console API credentials (ID and
    secret) from AWS secret store (NOTE: you have to assign
    IAM role to the NetScaler agent that will give permission
    to fetch secrets from AWS secret store)
15  2)  Login to NetScaler Console with credentials fetched in
    step 1
16  3)  Call NetScaler Console to fetch credentials (serviceURL
    and token) for agent registration
17  4)  Calls registration by using the credentials fetched in
    step 3
18  '''
19
20  '''
21  These are the placeholders which you need to replace
    according to your setup configurations
22  aws_secret_id: Id of the AWS secret where you have stored
    NetScaler Console Credentials
23  The secrets value should be in the following json format
24  {
25   "adm_user_id_key": "YOUR_ID", " adm_user_secret_key": "
        YOUR_SECRET" }
26
27  '''
28
29  aws_secret_id = "<AWS_secret_id>"
30  adm_ip_or_hostname = "<YOUR_ADM_POP>.adm.cloud.com"
31
32  '''
33  Set up a specific logger with your desired output level and
    log file name
34  '''
35  log_file_name_local = os.path.basename(\_\_file\_\_)
36  LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'
37  LOG_MAX_BYTE = 50\*1024\*1024
38  LOG_BACKUP_COUNT = 20
39
40  logger = logging.getLogger(\_\_name\_\_)
41  logger.setLevel(logging.DEBUG)
42  logger_handler = logging.handlers.RotatingFileHandler(
    LOG_FILENAME, maxBytes=LOG_MAX_BYTE, backupCount=
    LOG_BACKUP_COUNT)
43  logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%(
    funcName)30s:%(lineno)4d: [%(levelname)s] %(message)s',
    datefmt="%Y-%m-%d %H:%M:%S")
44  logger_handler.setFormatter(logger_fortmater)
45  logger.addHandler(logger_handler)
46
47  class APIHandlerException(Exception):
48      def \_\_init\_\_(self, error_code, message):
49          self.error_code = error_code
50          self.message = message
51
```



```
52      def \_\_str\_\_(self):
53          return self.message + ". Error code '" + str(self.
               error_code) + "'"
54
55  def parse_response(response, url, print_response=True):
56      if not response.ok:
57          if "reboot" in url:
58              logger.debug('No response for url: reboot')
59              resp = {
60  "errorcode": "500", "message": "Error while reading response.
       " }
61
62              return resp
63
64          if print_response:
65              logger.debug('Response text for %s is %s' % (url,
                    response.text))
66
67          response = json.loads(response.text)
68          logger.debug("ErrorCode - " + str(response['errorcode
               ']) + ". Message -" + str(response['message']))
69          raise APIHandlerException(response['errorcode'], str(
               response['message']))
70      elif response.text:
71          if print_response:
72              logger.debug('Response text for %s is %s' % (url,
                    response.text))
73
74          result = json.loads(response.text)
75          if 'errorcode' in result and result['errorcode'] > 0:
76              raise APIHandlerException(result['errorcode'],
                   str(result['message']))
77          return result
78
79  def _request(method, url, data=None, headers=None, retry=3,
       print_response=True):
80      try:
81          response = requests.request(method, url, data=data,
               headers=headers)
82          result = parse_response(response, url, print_response
               =print_response)
83          return result
84      except [requests.exceptions.ConnectionError, requests.
           exceptions.ConnectTimeout]:
85          if retry > 0:
86              return _request(method, url, data, headers, retry
                   -1, print_response=print_response)
87          else:
88              raise APIHandlerException(503, 'ConnectionError')
89      except requests.exceptions.RequestException as e:
90          logger.debug(str(e))
91          raise APIHandlerException(500, str(e))
92      except APIHandlerException as e:
```



```
93            logger.debug("URL: %s, Error: %s, Message: %s" % (url
                  , e.error_code, e.message))
94            raise e
95        except Exception as e:
96            raise APIHandlerException(500, str(e))
97
98    try:
99        '''Get the AWS Region'''
100       client = boto3.client('s3')
101       my_region = client.meta.region_name
102       logger.debug("The rgion is %s" % (my_region))
103
104       '''Creating a Boto cleint session'''
105       session = boto3.session.Session()
106       client = session.client(
107           service_name='secretsmanager',
108           region_name=my_region
109       )
110
111       '''Getting the values stored in the secret with id: <
              aws_secret_id>'''
112       get_id_value_response = client.get_secret_value(
113           SecretId = aws_secret_id
114       )
115       adm_user_id = json.loads(get_id_value_response["
              SecretString"])["adm_user_id_key"]
116       adm_user_secret = json.loads(get_id_value_response["
              SecretString"])["adm_user_secret_key"]
117
118   except Exception as e:
119       logger.debug("Fetching of NetScaler Console credentials
              from AWS secret failed with error: %s" % (str(e)))
120       raise e
121
122   '''
123   Initializing common NetScaler Console API handlers
124   '''
125   mas_common_headers = {
126
127       'Content-Type': "application/json",
128       'Accept-type': "application/json",
129       'Connection': "keep-alive",
130       'isCloud': "true"
131    }
132
133
134   '''
135   API to login to the NetScaler Console and fetch the Session
          ID and Tenant ID
136   '''
137   url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/
          config/login"
138   payload = 'object={
```

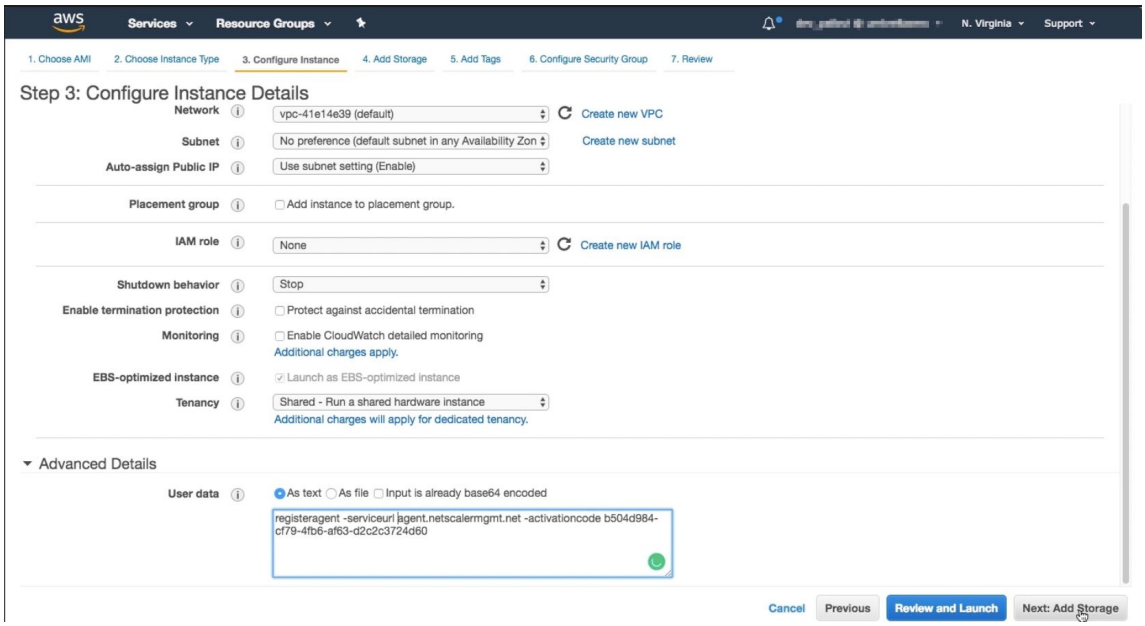


```
"login":{
"ID":"' + adm_user_id + '","Secret":"' + adm_user_secret + '"
    }
 }
'
try:
    response = _request("POST", url, data=payload, headers=
       mas_common_headers)
    sessionid = response["login"][0]["sessionid"]
    tenant_id = response["login"][0]["tenant_name"]
except Exception as e:
    logger.debug("Login call to the NetScaler Console failed
       with error: %s" % (str(e)))
    raise e

'''
API to fetch the service URL and Token to be used for
   registering the agent with the NetScaler Console
'''
mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)
url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/
   config/trust_preauthtoken/" + tenant_id +"?customer="+
   tenant_id
logger.debug("Fetching Service URL and Token.")
try:
    response = _request("GET", url, data=None, headers=
       mas_common_headers)
    service_name  = response["trust_preauthtoken"][0]["
       service_name"]
    token = response["trust_preauthtoken"][0]["token"]
    api_gateway_url = response["trust_preauthtoken"][0]["
       api_gateway_url"]
except Exception as e:
    logger.debug("Fetching of the Service URL Passed with
       error. %s" % (str(e)))
    raise e

'''
Running the register agent command using the values we
   retrieved earlier
'''
try:
    registeragent_command = "registeragent -serviceurl "+
       api_gateway_url+" -activationcode "+service_name+";"+
       token
    file_run_command = "/var/python/bin/python2.7 /mps/
       register_agent_cloud.py "+registeragent_command
    logger.debug("Executing registeragent command: %s" % (
       file_run_command))
    os.system(file_run_command)
except Exception as e:
    logger.debug("Agent Registeration failed with error: %s"
       % (str(e)))
```



```
176             raise e
```

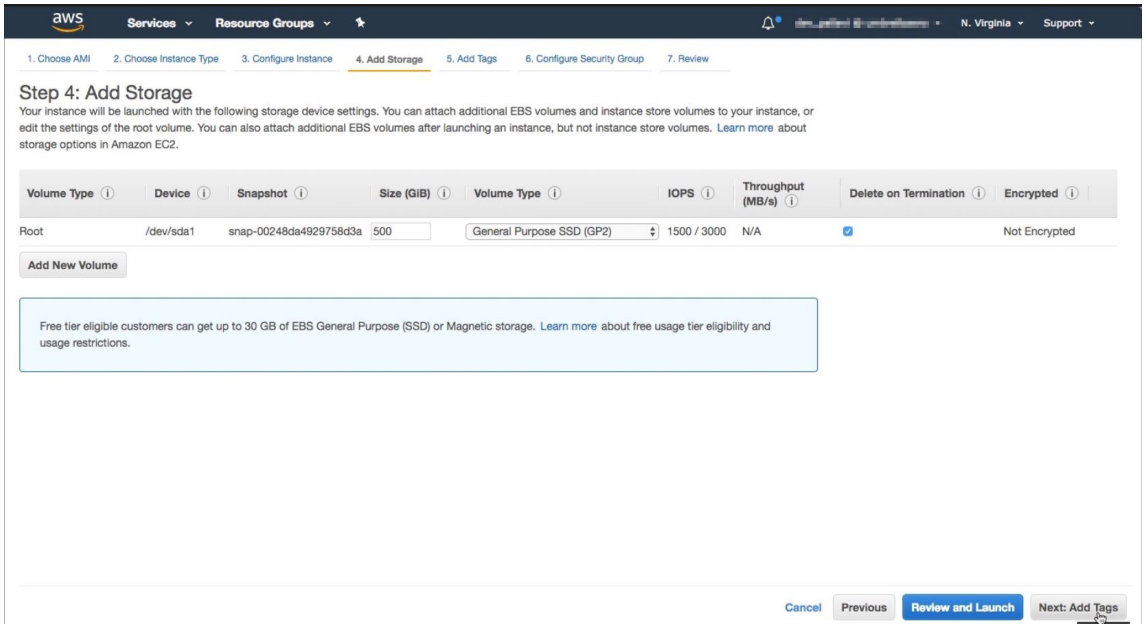
Dieses Skript ruft die Authentifizierungsdetails vom AWS Secrets Manager ab und führt das `deployment.py`Skript aus, um den Agenten bei der NetScaler Console zu registrieren.



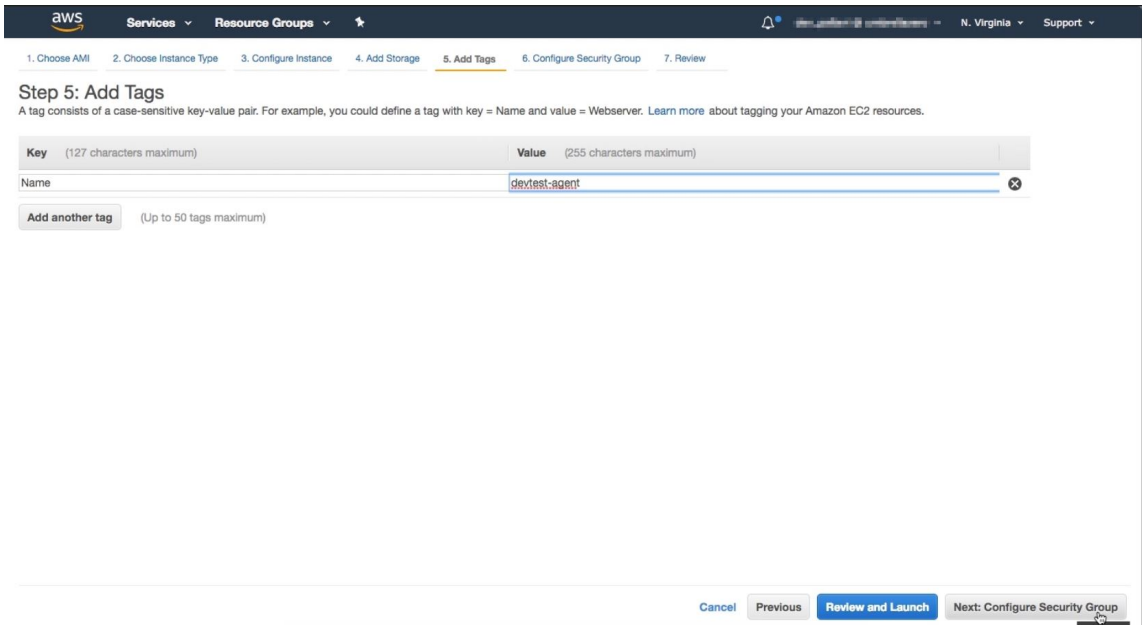
> **Hinweis**
>
> Während Sie öffentliche IP-Adressen automatisch zuweisen können, können Sie auch elastische IP-Adressen zuweisen. Das Zuweisen einer elastischen IP-Adresse ist erforderlich, wenn NAT-Gateway nicht konfiguriert ist.
>
> Wenn die Elastic IP-Adresse in diesem Schritt nicht festgelegt ist, können Sie dies weiterhin auf der EC2-Konsole tun. Sie können eine neue elastische IP-Adresse erstellen und diese mithilfe der Instanz-ID oder ENI-ID dem NetScaler Agent zuordnen.

Klicken Sie auf "**Speicher hinzufügen**"

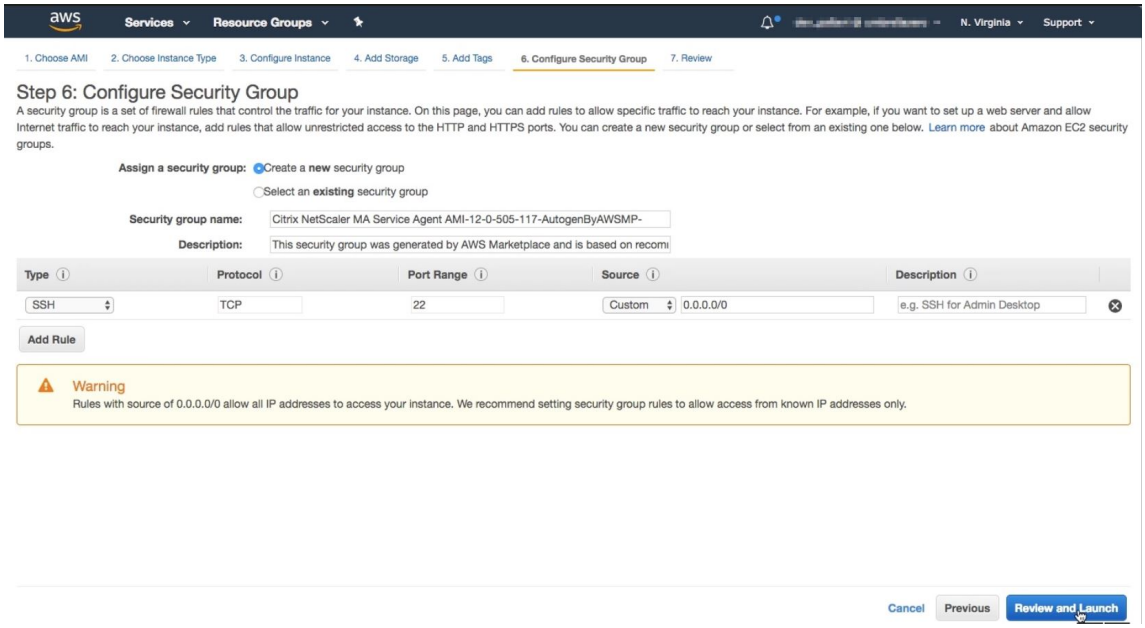
3. Konfigurieren Sie auf der Seite "**Speicher hinzufügen** "die Einstellungen des Speichergeräts für die Instanz und klicken Sie auf **Weiter: Tags hinzufügen**.



4. Definieren Sie auf der Seite **Add Tags** das Tag für die Instanz und klicken Sie auf **Weiter: Security Group konfigurieren**.

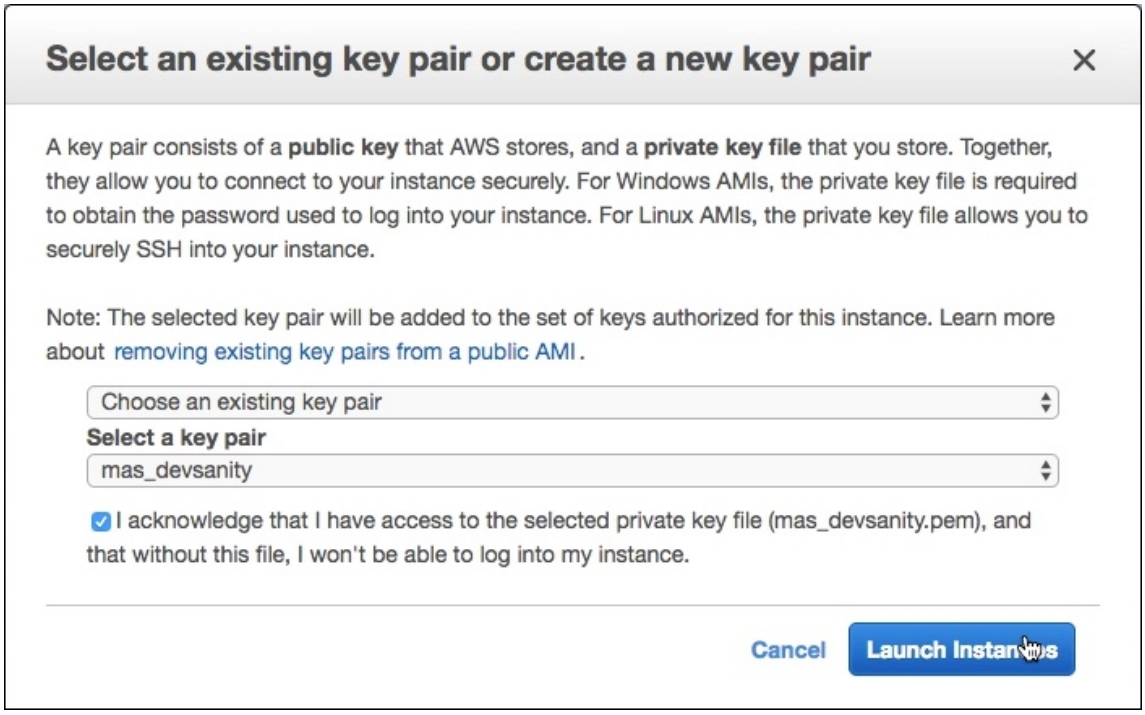


5. Fügen Sie auf der Seite **Configure Security Group** Regeln hinzu, um bestimmten Traffic zu Ihrer Instanz zu erlauben, und klicken Sie auf **Review and Launch**



6. Überprüfen Sie auf der Seite **Review Instanz Launch** die Instanz-Einstellungen und klicken Sie auf **Starten**.
7. Erstellen **Sie im Dialogfeld Wählen Sie ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues** Schlüsselpaar ein Schlüsselpaar. Sie können auch aus den vorhandenen Schlüsselpaaren wählen.

   Akzeptieren Sie die Bestätigung und klicken Sie auf **Launch Instanzen**.



Der Bereitstellungsprozess kann etwa 10 bis 15 Minuten dauern. Nachdem die Bereitstellung erfolgre-

ich abgeschlossen wurde, können Sie Ihre virtuelle NetScaler Agent-Maschine in Ihrem AWS-Konto anzeigen.

Installieren Sie einen NetScaler Agent auf GCP

January 26, 2024

Der NetScaler Agent fungiert als Vermittler zwischen der NetScaler Console und den erkannten Instanzen im Rechenzentrum oder in der Cloud. Sie können den Agenten auf der Google Cloud Platform (GCP) bereitstellen, um die sichere Remoteverwaltung von NetScaler-Instanzen zu ermöglichen, die im virtuellen Google Cloud-Netzwerk über NetScaler Console bereitgestellt werden. Weitere Informationen finden Sie im Google Cloud Platform Marketplace.

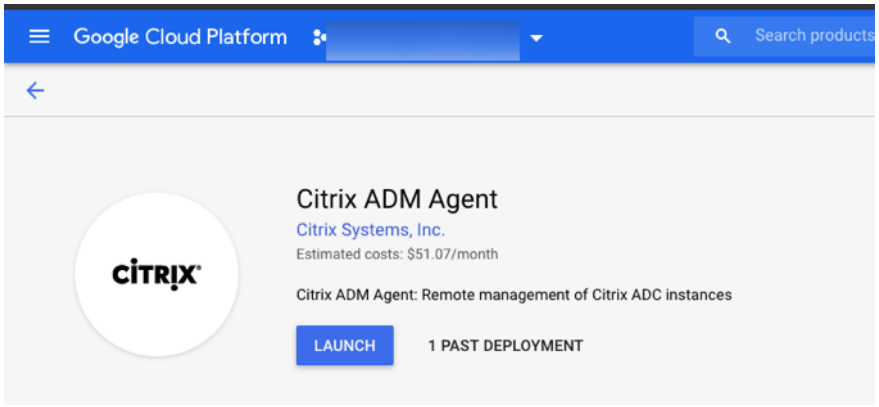
Voraussetzungen

Um einen NetScaler Agent auf GCP zu installieren, benötigen Sie ein GCP-Konto.

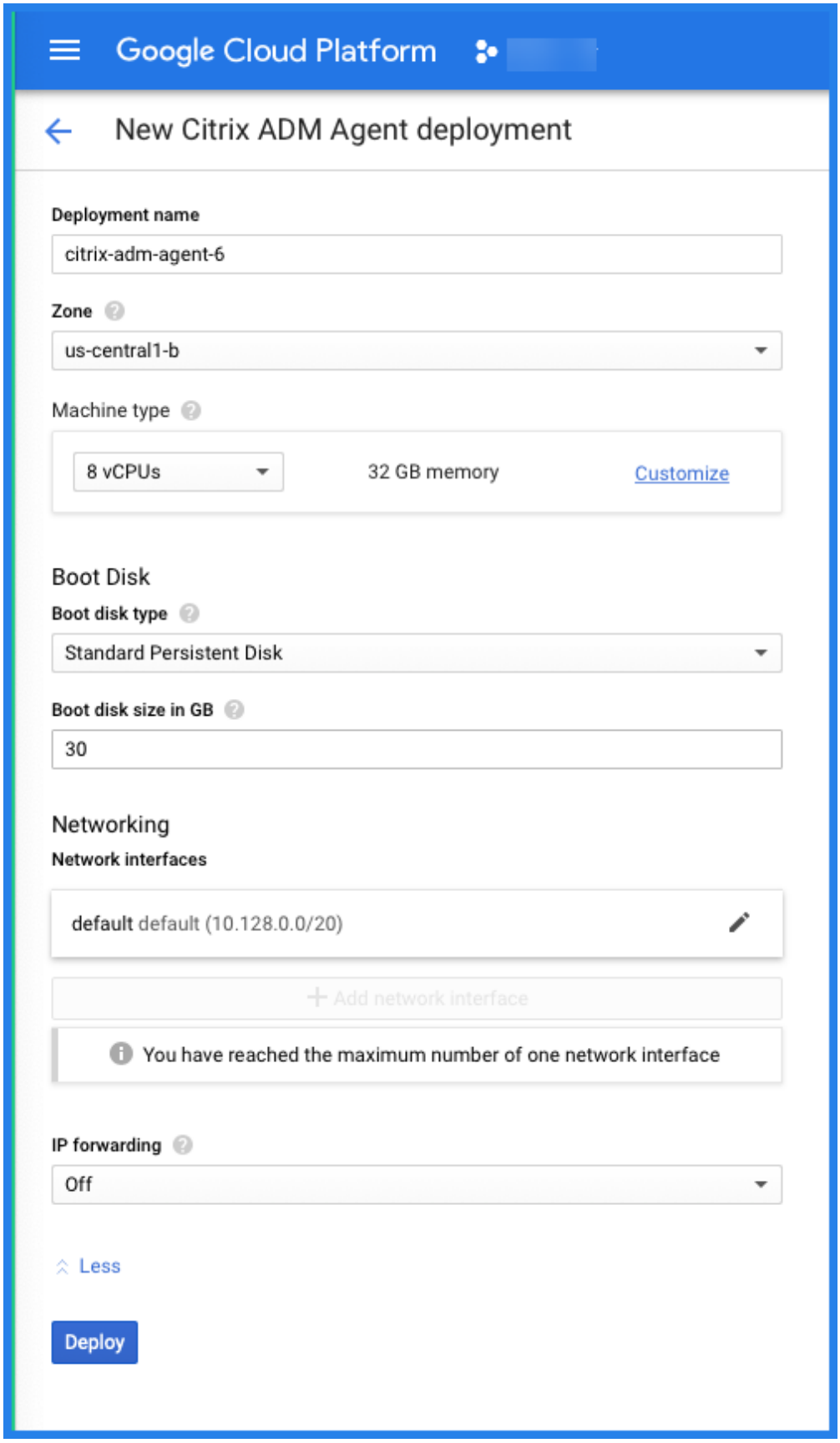
Installieren Sie den NetScaler Agent auf GCP

Gehen Sie wie folgt vor, um einen NetScaler Agent auf der GCP zu installieren.

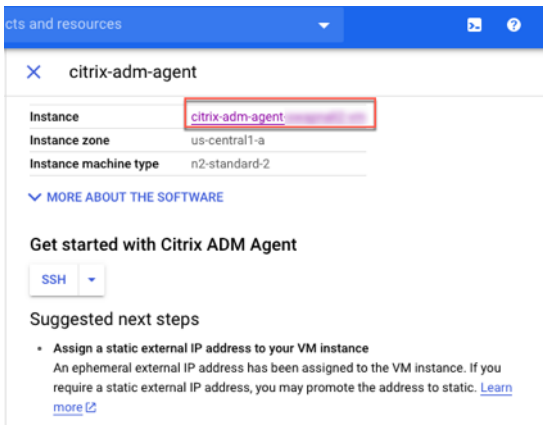
1. Melden Sie sich mit Ihren Anmeldeinformationen bei der GCP-Konsole (console.cloud.google.com) an und gehen Sie zum Marktplatz.
2. Geben Sie **NetScaler Agent** in das Suchfeld ein.
3. Klicken Sie im Ergebnisfeld auf **NetScaler Agent** und dann auf **Starten**.



4. Auf der Seite „ **New NetScaler Agent Deployment** “sind die meisten Optionen standardmäßig festgelegt. Sie können die Standardkonfigurationen nach Bedarf ändern und auf **Bereitstellen** klicken.



5. Nachdem der Agent bereitgestellt wurde, klicken Sie auf den Link Instanz und überprüfen Sie die Details auf der **Detailseite der VM-Instanz**.

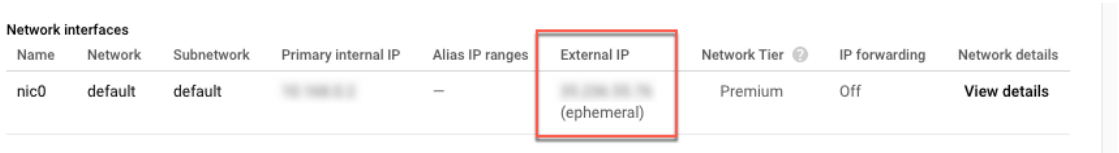


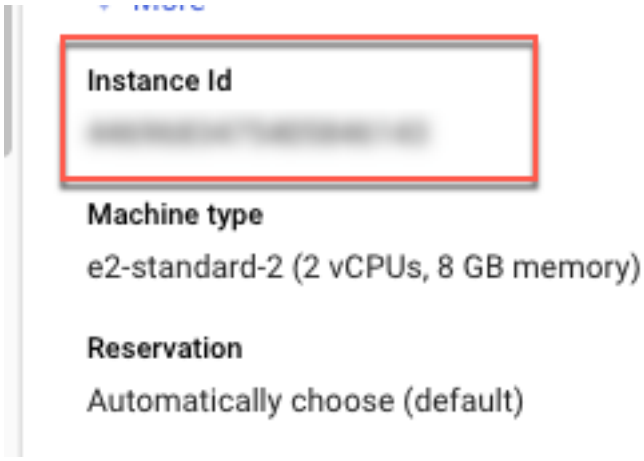
6. Melden Sie sich über einen SSH-Client mit der externen IP-Adresse des Agent beim Agent an. Verwenden Sie die folgenden Befehle:

   ```
   ssh nsrecover@<external IP address of the agent>
   ```

   Kennwort: Instanz-ID

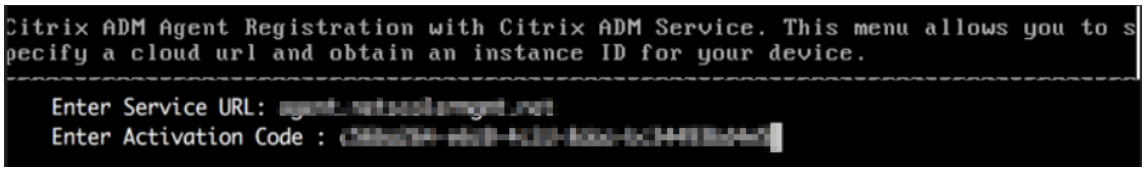
   Können Sie die externe IP-Adresse und die Instanz-ID auf der **Detailseite der VM-Instanz finden** ?





7. Geben Sie den folgenden Befehl ein, um den Bereitstellungsbildschirm aufzurufen: **deployment_type.py**
8. Geben Sie die **Service-URL** und den **Aktivierungscode ein**, den Sie auf der Seite „ **Agenten einrichten** “in NetScaler Console kopiert und gespeichert haben, wie unter Erste Schritte

beschrieben. Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.



Nach erfolgreicher Agentregistrierung wird der Agent neu gestartet, um den Installationsvorgang abzuschließen.

Rufen Sie nach dem Neustart des Agents die NetScaler Console auf und überprüfen Sie auf der Seite „ **Agent** einrichten “unter **Discovered Agents** den Status des Agents.

Installieren Sie den NetScaler Agent mithilfe von YAML im Kubernetes-Cluster

January 26, 2024

> **Hinweis**
>
> Das Verfahren zum Installieren eines Agent als Microservice finden Sie im Abschnitt Erste Schritte .

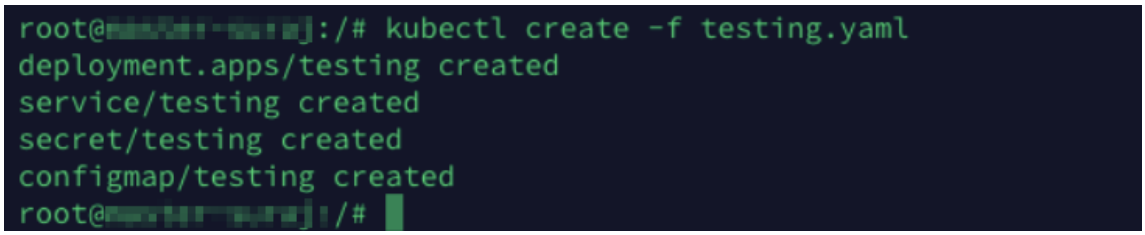
Im Kubernetes-Masterknoten:

1. Speichern Sie die heruntergeladene YAML-Datei
2. Führen Sie den folgenden Befehl aus:

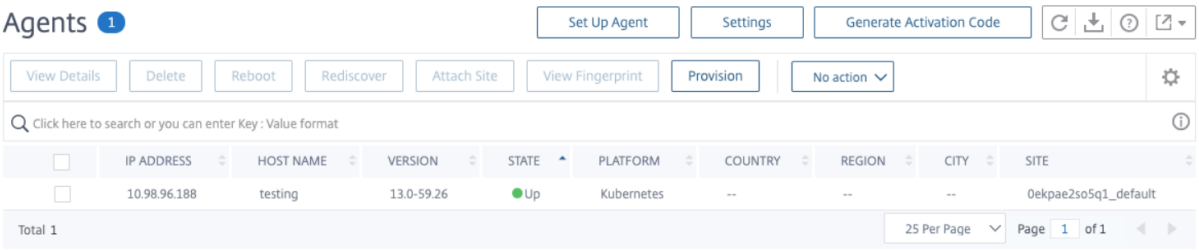
   `kubectl create -f <yaml file>`

   Beispiel: `kubectl create -f testing.yaml`

   Der Agent wurde erfolgreich erstellt.



Navigieren Sie in der NetScaler Console zu **Infrastruktur > Instanzen > Agents** , um den Agentenstatus zu sehen.



> **Hinweis:**
>
> Der im Kubernetes-Cluster mithilfe von YAML konfigurierte NetScaler-Agent unterstützt das automatische Agenten-Upgrade (Evergreen-Upgrade).

Installieren Sie einen NetScaler Agent-Operator mithilfe der OpenShift-Konsole

April 10, 2024

Ein Operator ist ein Open-Source-Toolkit, mit dem Sie die Kubernetes-Anwendungen auf effektive, automatisierte und skalierbare Weise bereitstellen und verwalten können. Als Administrator können Sie mithilfe des **NetScaler ADM Agent Operators** einen Agent im OpenShift-Cluster bereitstellen.

> **Hinweis:**
>
> Ein im OpenShift-Cluster konfigurierter Agent wird standardmäßig nicht automatisch aktualisiert.

Voraussetzungen

Stellen Sie vor der Bereitstellung sicher, dass:

- Sie verfügen über die privilegierten Sicherheitskontextbeschränkungen, um die Berechtigungen für Pods zu steuern. Führen Sie für den Agent den folgenden Befehl aus, um die Rechtesicherheitskontextbeschränkungen für das Dienstkonto abzurufen:

  ```
  oc adm policy add-scc-to-user privileged -z adm-agent-serviceaccount
  ```

- Führen Sie den folgenden Befehl aus, um ein Agent-Login-Geheimnis zu erstellen:

  ```
  kubectl create secret generic admlogin --from-literal=username=
  nsroot --from-literal=password=<adm-agent-password> -n <namespace
  >
  ```


> **Hinweis:**
>
> - `<adm-agent-password>` ist ein Beispielkennwort. Sie müssen ein Kennwort für den Agent festlegen und NetScaler CPX verwendet diese Anmeldeinformationen, um sich beim Agent zu registrieren.
> - Geben Sie **admlogin** für `loginSecret` in der YAML des Agent an, während Sie die Instanz erstellen.

Wenn Sie NetScaler CPX und Agent in verschiedenen Namespaces bereitstellen, stellen Sie Folgendes sicher:

- Benennen Sie den Namespace, in dem der NetScaler CPX bereitgestellt wurde, mit `citrix-cpx=enabled`.
- Legen Sie beim Installieren des Agentoperators den Parameter `helper.required` mit True oder False fest.

  > **Hinweis:**
  >
  > Standardmäßig ist `helper.required` auf **false** gesetzt. Wenn dieser Parameter auf False gesetzt ist, müssen Sie sicherstellen, dass in jedem Namespace ein geheimer Schlüssel für **Admlogin** erstellt wird, wenn sich NetScaler CPX und Agent in unterschiedlichen Namespaces befinden.

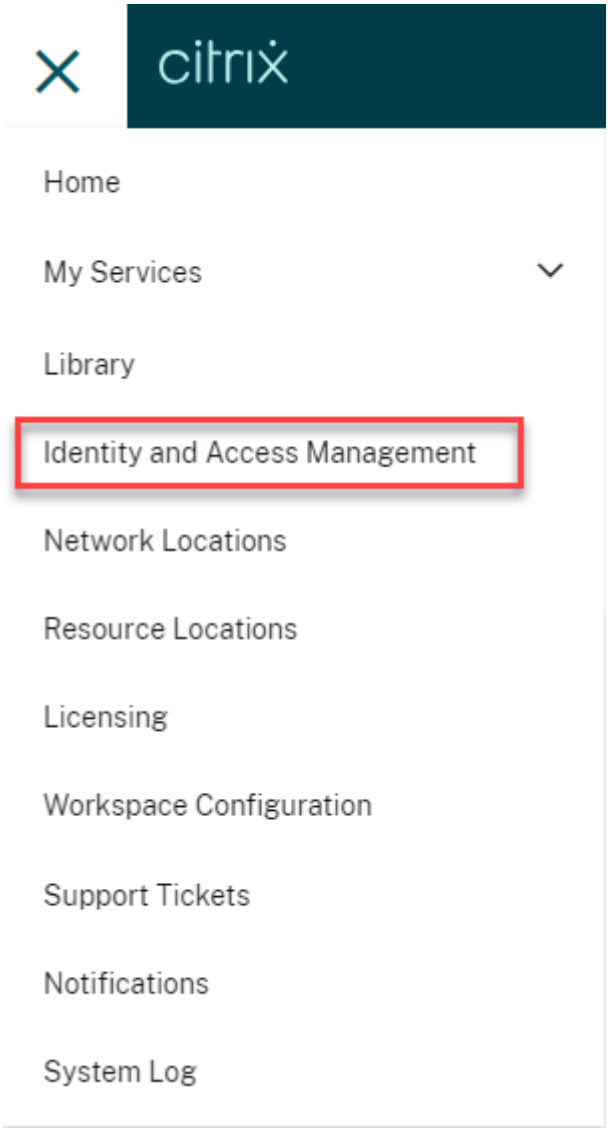
- Sie haben den geheimen Schlüssel `accessSecret`, der im Agent YAML benötigt wird. Diese Anmeldeinformationen sind erforderlich, damit der Agent eine Verbindung mit dem NetScaler Console-Dienst herstellen kann.

  ```
  kubectl create secret generic <secretname> --from-literal=accessid
  =<ID> --from-literal=accesssecret=<Secret> -n namespace
  ```

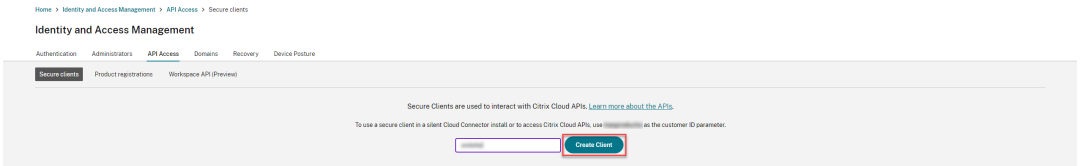
  > **Hinweis:**
  >
  > Geben Sie beim Erstellen der Instanz einen geheimen Namen für AccessSecret in Agent-YAML an.

  Die Zugriffs-ID und den Schlüssel für den Zugriff auf die NetScaler Console erhalten Sie mit dem folgenden Verfahren:

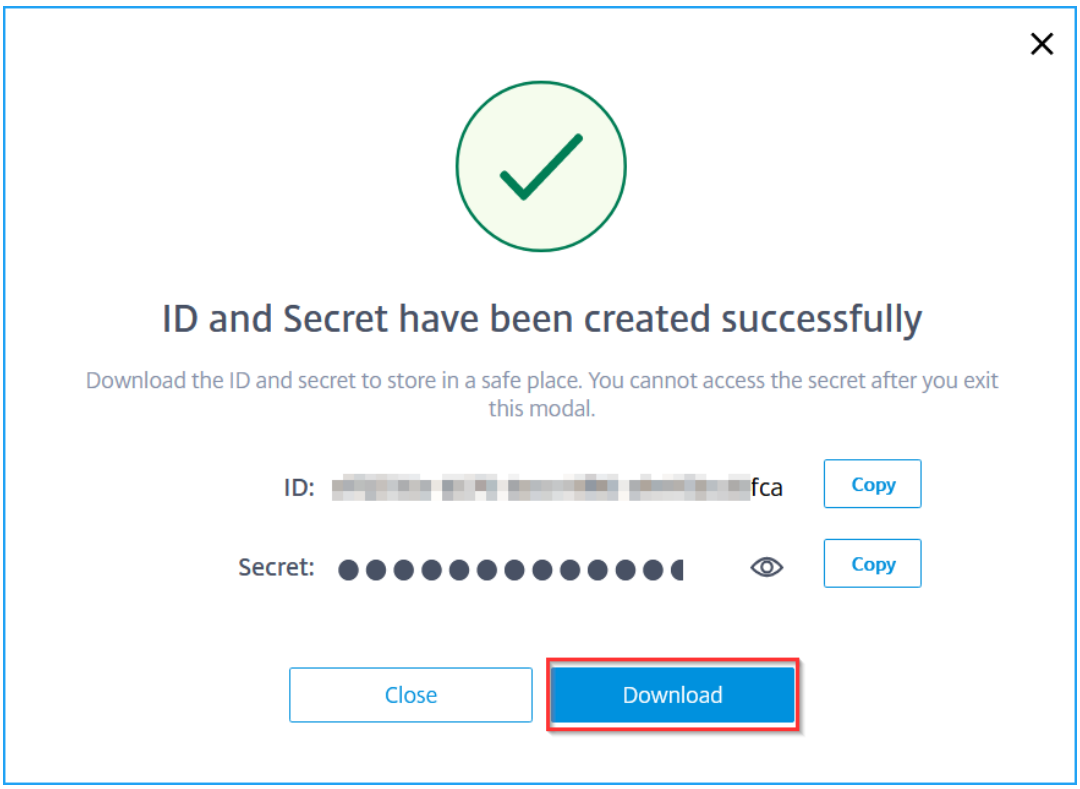
  1. Melden Sie sich an der Citrix Cloud-Managementkonsole an.
  2. Klicken Sie im Menü “Citrix Cloud”auf **Identitäts- und Zugriffsverwaltung**.



3. Geben Sie auf der Registerkarte **API-Zugriff** einen sicheren Client-Namen ein und klicken Sie auf **Client erstellen**.

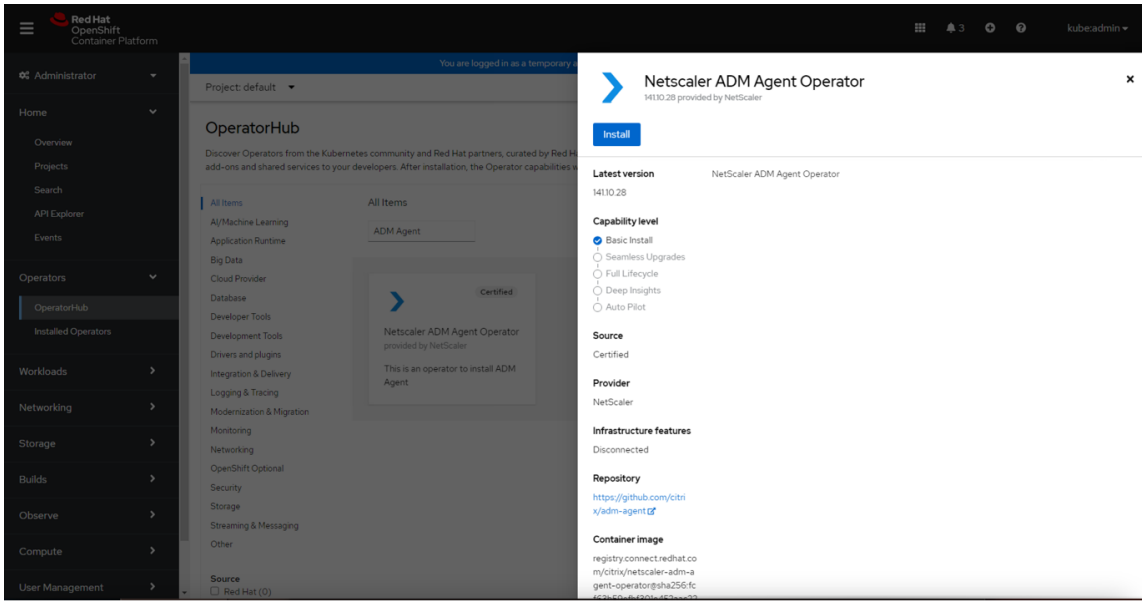


4. ID und Secret werden generiert. Klicken Sie auf **Herunterladen** und speichern Sie die CSV-Datei.



Installieren Sie den Agent Operator

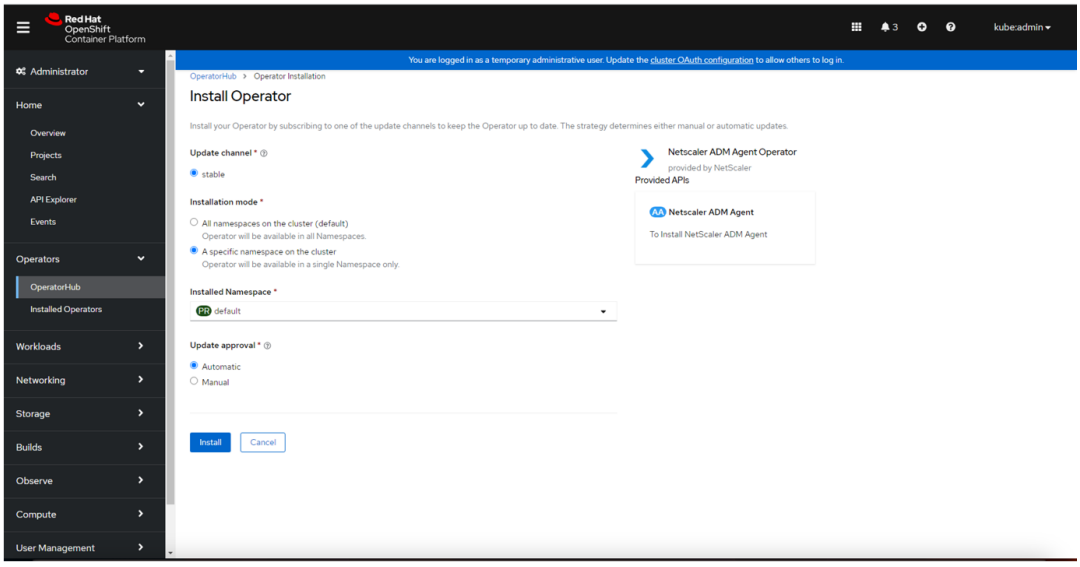
1. Melden Sie sich an der OpenShift-Cluster-Konsole an.
2. Navigieren Sie zu **Operators > OperatorHub**.
3. Geben Sie in der Suchleiste den Namen des Agent ein, wählen Sie den **NetScaler ADM Agent Operator** aus und klicken Sie dann auf **Installieren**.



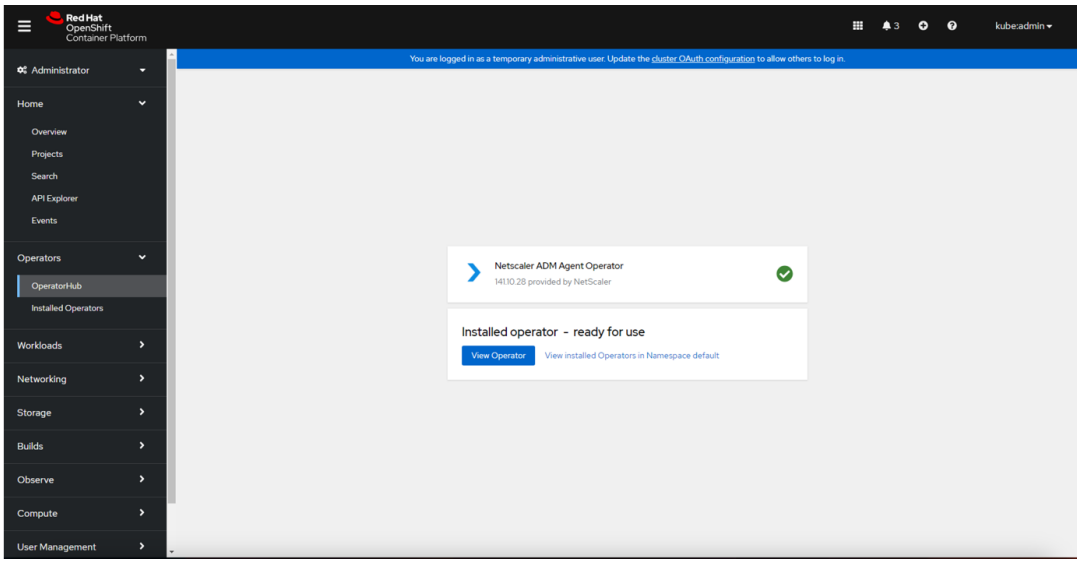
4. Auf der Seite **Operator installieren** haben Sie zwei Optionen:

   - **Alle Namespaces im Cluster (Standard)**—Ermöglicht dem Agent-Operator, alle im Cluster verfügbaren Namespaces zu abonnieren, und ermöglicht es Ihnen, die Instanz des Agent-Operators von einem beliebigen Namespace im Cluster aus zu initiieren.
   - **Ein bestimmter Namespace auf dem Cluster**—Ermöglicht dem Agent-Operator, einen ausgewählten Namespace im Cluster zu abonnieren, und Sie können die Instanz des Agent-Operators nur vom ausgewählten Namespace aus initiieren.

     In diesem Beispiel wird der Agent-Operator einem Namespace namens **Default** zugewiesen. Wählen Sie unter **Genehmigung von Updates** die Option **Automatisch** aus und klicken Sie auf **Installieren**.

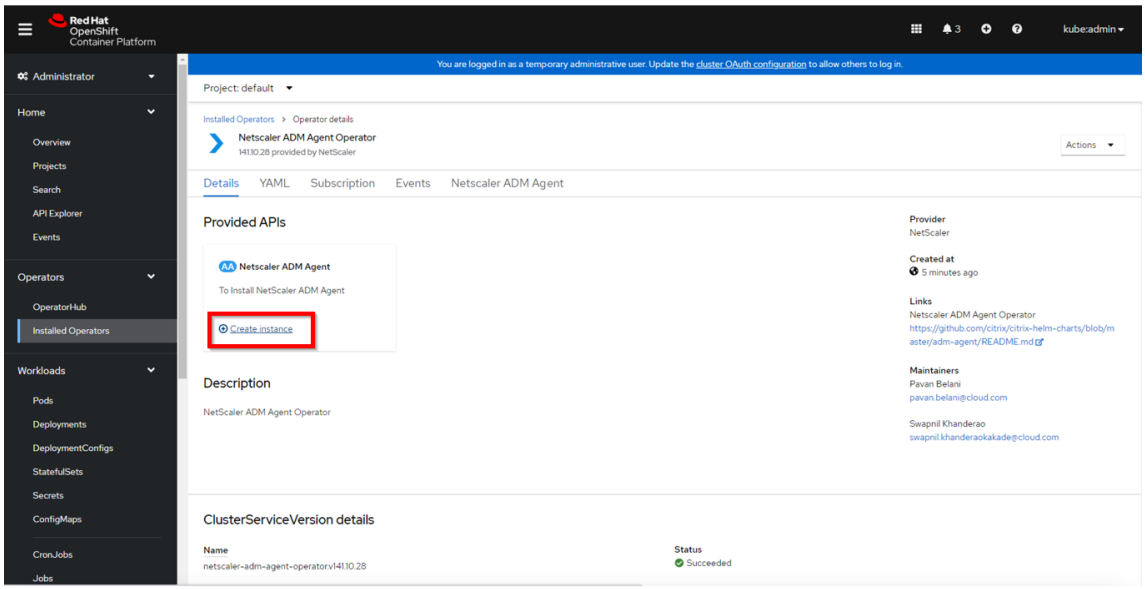


Warten Sie, bis der Agent-Operator erfolgreich abonniert wurde.



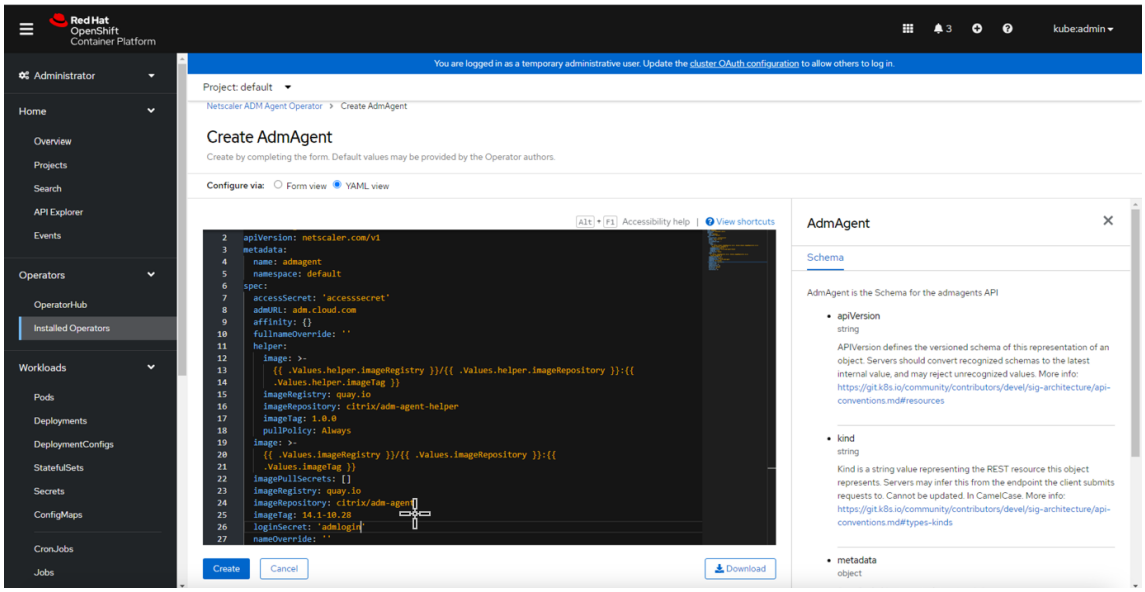
5. Navigieren Sie zu **Workloads > Pods** und überprüfen Sie, ob der Pod `netscaler-adm-agent-operator-controller` betriebsbereit ist.

6. Nachdem der Pod betriebsbereit ist, klicken Sie auf **Create Instance**.

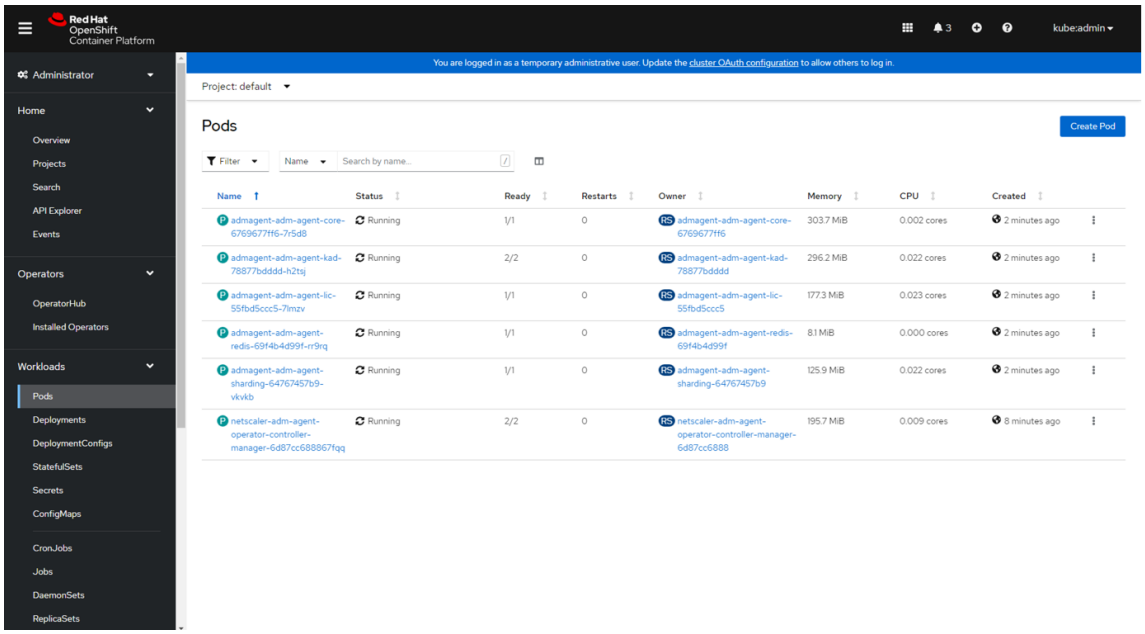


7. Wählen Sie die **YAML-Ansicht** aus, um alle Parameter zu aktualisieren, und klicken Sie dann auf **Erstellen**.

> **Hinweis:**
>
> Stellen Sie sicher, dass pro OpenShift-Cluster nur eine Agentinstanz vorhanden sein darf.

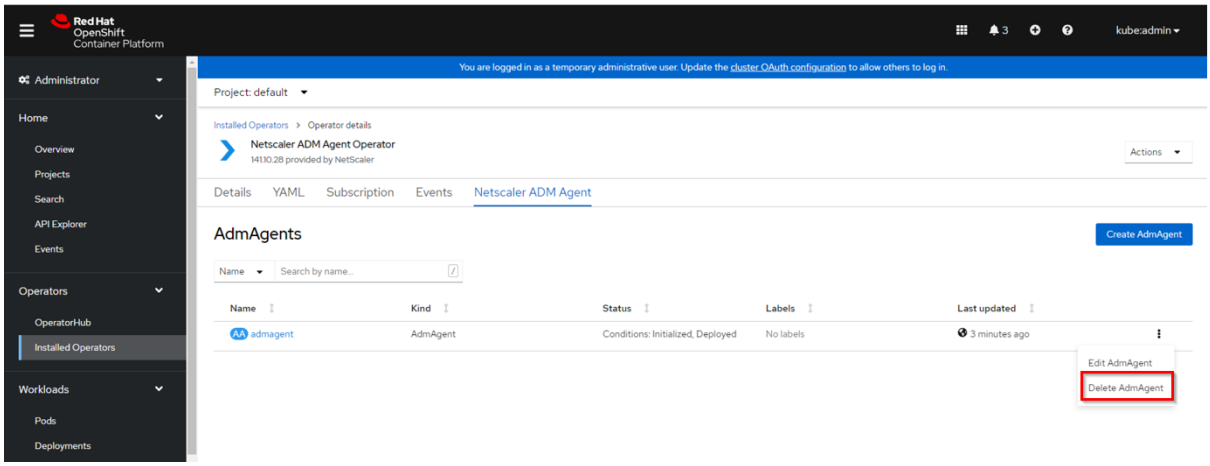


8. Navigieren Sie zu **Workloads > Pods** und stellen Sie sicher, dass die Agent-Pods betriebsbereit sind.



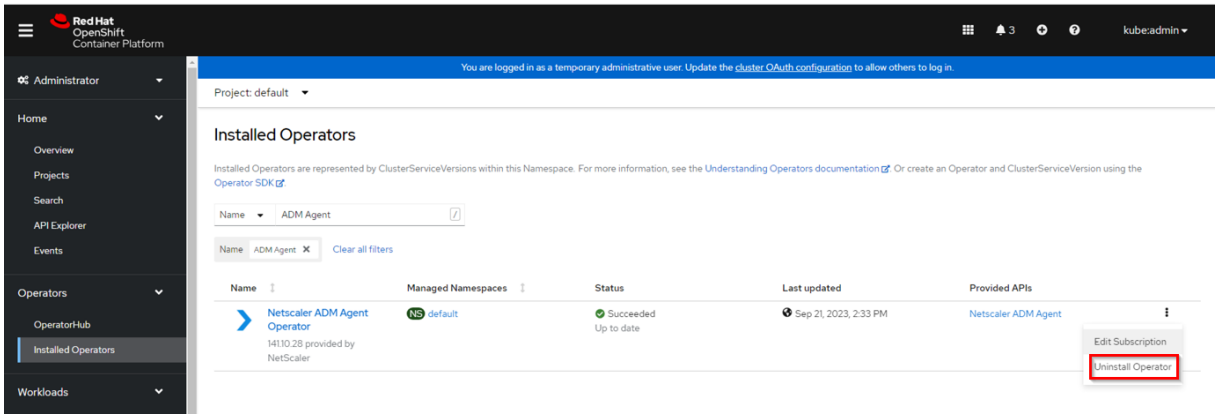
Eine Agentinstanz löschen

Sie können die Agentinstanz aus dem Cluster löschen, indem Sie zu **Operatoren > Installierte Operatoren** navigieren. Wählen Sie auf der Registerkarte **NetScaler ADM Agent Operator** die Instanz aus und wählen Sie **AdmAgent löschen** aus der Liste aus.



Deinstallieren Sie den Agent-Operator

Wenn Sie den Agent-Operator-Pod aus dem Cluster deinstallieren möchten, navigieren Sie zu Operatoren **> Installierte** Operatoren und wählen Sie dann **Operator deinstallieren** aus der Liste aus.



Containerbasierten Agent mit dem Helm Chart installieren

January 26, 2024

Sie können einen containerbasierten Agenten bereitstellen, um NetScaler CPX mit der NetScaler Console zu verbinden, um den NetScaler CPX zu verwalten und zu überwachen. Folgen Sie dem in diesem Dokument beschriebenen Verfahren, um einen containerbasierten Agent bereitzustellen.

> **Hinweis:**
>
> Der containerbasierte Agent wird standardmäßig nicht automatisch aktualisiert (Evergreen-Upgrade).

Hilfe und Support

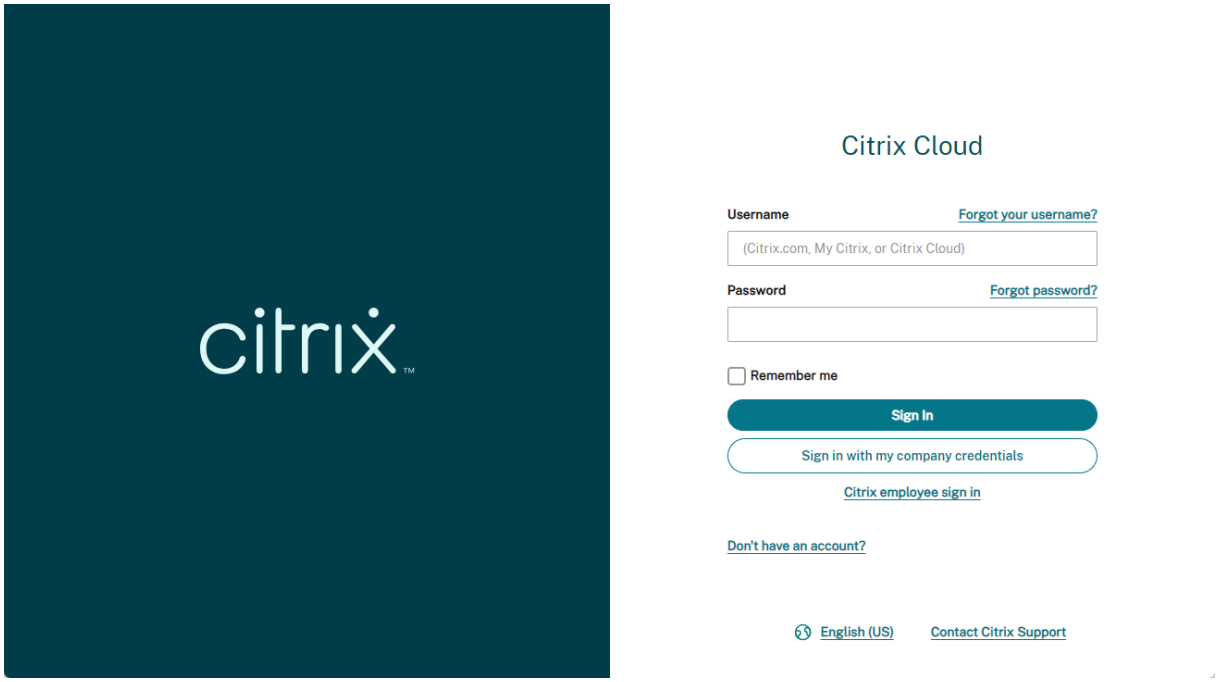
July 17, 2024

Als Citrix Cloud-Benutzer benötigen Sie manchmal Hilfe bei der Sicherstellung eines reibungslosen Funktionierens unserer Infrastruktur. In diesem Thema finden Sie weitere Informationen zu den verschiedenen Hilfe- und Unterstützungsoptionen sowie zum Zugriff auf diese Optionen.

Erstellen eines Citrix Cloud-Kontos

Falls bei der Registrierung für ein Citrix Cloud-Konto ein Fehler auftritt, wenden Sie sich bitte an den Citrix Customer Service.

Loggen Sie sich in Ihr Konto ein



Falls beim Anmelden an Ihrem Citrix Cloud-Konto Probleme auftreten:

- Stellen Sie sicher, dass Sie die E-Mail-Adresse und das Kennwort verwenden, die Sie bei der Registrierung angegeben haben.
- Citrix Cloud fordert Sie automatisch auf, Ihr Kennwort zurückzusetzen, bevor Sie sich anmelden können, wenn:
  - Sie haben sich seit einiger Zeit nicht mehr bei Citrix Cloud angemeldet

  - Ihr Kennwort entspricht nicht den Anforderungen von Citrix Cloud

- Weitere Informationen finden Sie in diesem Artikel unter Ändern des Kennworts.
- Wenn Ihr Unternehmen es Benutzern ermöglicht, sich auch mit den Firmenanmeldeinformationen an Citrix Cloud anzumelden, klicken Sie auf **Mit Firmenanmeldeinformationen anmelden** und geben Sie die Anmelde-URL Ihres Unternehmens ein. Sie können dann Ihre Firmenanmeldeinformationen eingeben, um auf das Citrix Cloud-Konto Ihres Unternehmens zuzugreifen. Wenden Sie sich an Ihren Administrator, wenn Sie die Anmelde-URL Ihres Unternehmens nicht kennen.

Ändern Sie Ihr Kennwort

Wenn Sie Ihr Citrix Cloud-Kontokennwort **vergessen haben, klicken Sie auf Benutzernamen oder Kennwort vergessen?**, und Sie können die E-Mail-Adresse Ihres Kontos eingeben. Sie erhalten eine E-Mail, um Ihr Kennwort zurückzusetzen. Wenn Sie keine E-Mail zum Zurücksetzen des Kennworts erhalten oder weitere Unterstützung benötigen, wenden Sie sich an den Citrix Customer Service.

Zum Schutz Ihres Kontokennworts fordert Citrix Cloud Sie beim Anmelden möglicherweise auf, Ihr Kennwort zurückzusetzen. Diese Aufforderung wird in folgenden Situationen angezeigt:

- Ihr Kennwort entspricht nicht den Komplexitätsvorgaben von Citrix Cloud. Kennwörter müssen mindestens 8 Zeichen lang sein und Folgendes enthalten:
  - Mindestens eine Zahl
  - Mindestens einen Großbuchstaben
  - Mindestens ein Symbol: ! @ # $ % ^ * ? + = –
- Ihr Kennwort enthält im Wörterbuch enthaltene Wörter.
- Ihr Kennwort wird in einer bekannten Datenbank mit gefährdeten Kennwörtern aufgeführt.
- Sie haben sich in den vergangenen sechs Monaten nicht bei Citrix Cloud angemeldet.

Wenn Sie dazu aufgefordert werden, wählen Sie **Kennwort zurücksetzen**, um ein neues sicheres Kennwort für Ihr Konto zu erstellen.

Supportforen für Citrix Cloud

In den Supportforen für Citrix Cloud können Sie Hilfe erhalten, Feedback und Verbesserungsvorschläge hinterlassen, Unterhaltungen anderer Benutzer anzeigen oder selbst ein Thema diskutieren.

Die Mitarbeiter des NetScaler-Supports verfolgen diese Foren und sind bereit, Ihre Fragen zu beantworten. Andere Mitglieder der Citrix Cloud-Community bieten möglicherweise ebenfalls Hilfe an oder nehmen an der Diskussion teil.

Sie müssen sich nicht anmelden, um Forumsbeiträge zu lesen. Um selbst einen Kommentar zu posten oder auf ein Thema zu antworten, müssen Sie jedoch angemeldet sein. Verwenden Sie zur Anmeldung die Anmeldeinformationen für Ihr Citrix Konto oder die E-Mail-Adresse und das Kennwort, die Sie beim Erstellen Ihres Citrix Cloud-Kontos angegeben haben. Um ein Citrix-Konto zu erstellen, gehen Sie zu Konto erstellen oder anfordern.

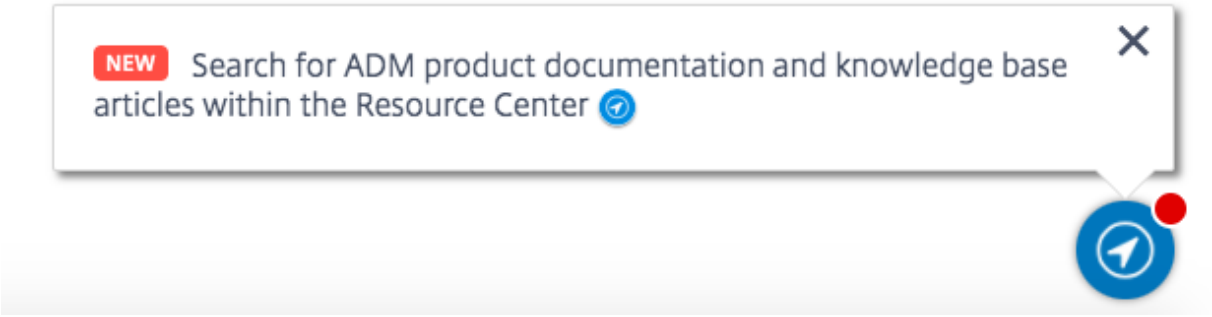
Supportartikel und Dokumentation

NetScaler bietet eine Fülle von Produkt- und Support-Inhalten, die Ihnen helfen, das Beste aus Citrix Cloud herauszuholen und viele Probleme zu lösen, die möglicherweise mit NetScaler-Produkten auftreten.

Citrix Cloud-Ressourcencenter

Das Citrix Cloud Resource Center bietet verschiedene Ressourcen, die Ihnen den Einstieg in die Citrix Cloud-Dienste erleichtern, mehr über Funktionen erfahren und Probleme lösen. Die angezeigten Ressourcen beziehen sich auf das Feature oder den Dienst in Citrix Cloud, mit dem Sie gerade arbeiten. Wenn Sie sich beispielsweise in der Virtual Apps and Desktops Service Management Console befinden, werden Ihnen im Resource Center die folgenden Ressourcen angezeigt.

Greifen Sie jederzeit auf das Resource Center zu, indem Sie unten rechts in der Citrix Cloud-Konsole auf das blaue Kompasssymbol klicken.



- **Erste Schritte**: Bietet eine kurze Anleitung zu den wichtigsten Aufgaben speziell für den Service, mit dem Sie gerade arbeiten. Sie finden auch Links zu Schulungs- und Onboarding-Ressourcen, die Ihnen helfen, mehr über die Servicefunktionen zu erfahren und Ihre Endbenutzer auf Erfolgskurs zu bringen.
- **Ankündigungen**: Bietet Benachrichtigungen über neu veröffentlichte Features und Links zu wichtigen Mitteilungen von Citrix. Klicken Sie auf eine Feature-Benachrichtigung, um eine kurze Anleitung zur Funktion zu erhalten.

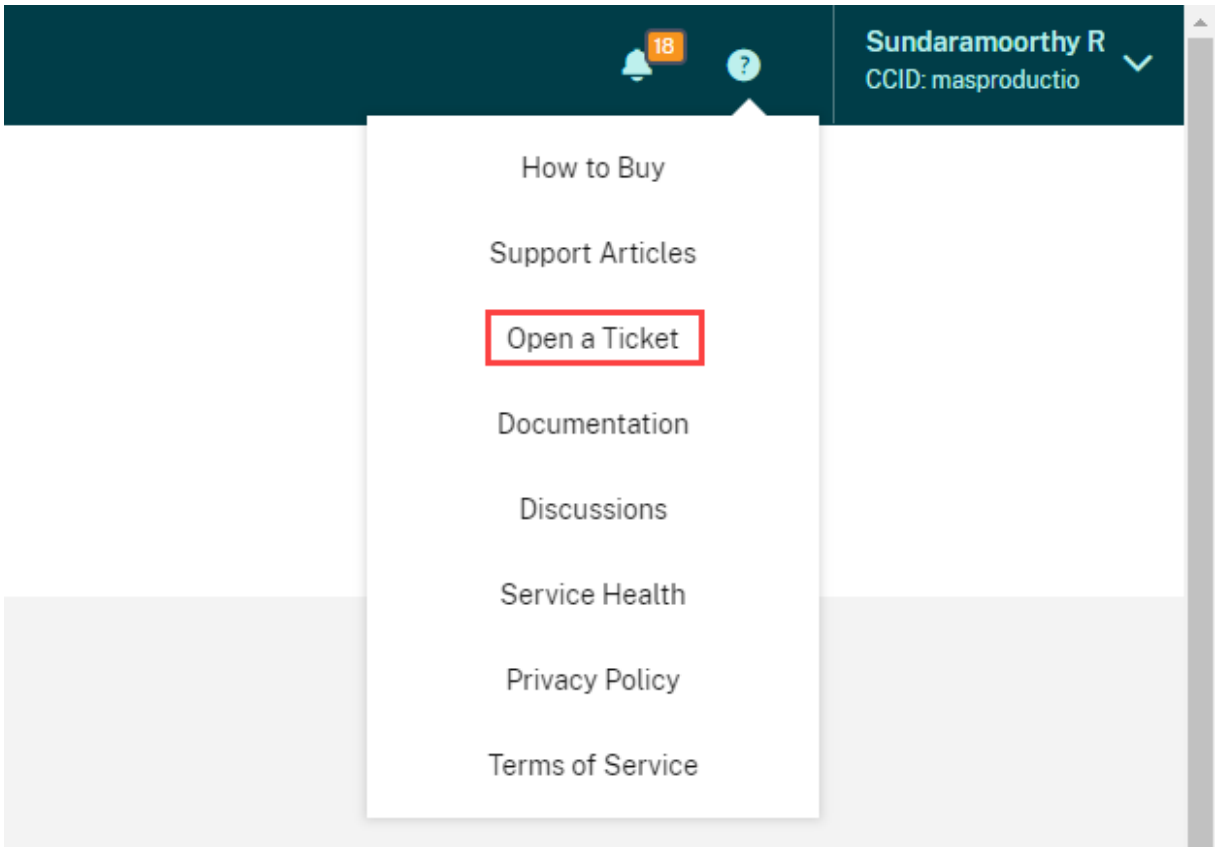
- **Artikel durchsuchen**: Enthält eine Liste mit Produktdokumentation und Knowledge Center-Artikeln für häufige Aufgaben und hilft Ihnen, weitere Artikel zu finden, ohne Citrix Cloud zu verlassen. Geben Sie eine Suchabfrage in das Feld **How do I ...** ein, um eine gefilterte Liste von Artikeln für den Service anzuzeigen, mit dem Sie arbeiten. Im Allgemeinen werden Supportartikel zuerst in der Liste angezeigt, gefolgt von Artikeln in der Produktdokumentation.

Citrix Tech Zone

Citrix Tech Zone enthält eine Fülle von Informationen, mit denen Sie mehr über Citrix Cloud und andere NetScaler-Produkte erfahren können. Hier finden Sie Referenzarchitekturen, Diagramme, Videos und technische Dokumente, die Einblicke in den Entwurf, die Entwicklung und den Einsatz von Citrix-Technologien bieten.

Technischer Support

Wenn Sie bei einem Problem technische Hilfe benötigen, klicken Sie rechts oben im Bildschirm auf das Symbol **Feedback und Support**, und wählen Sie **Ticket erstellen**.

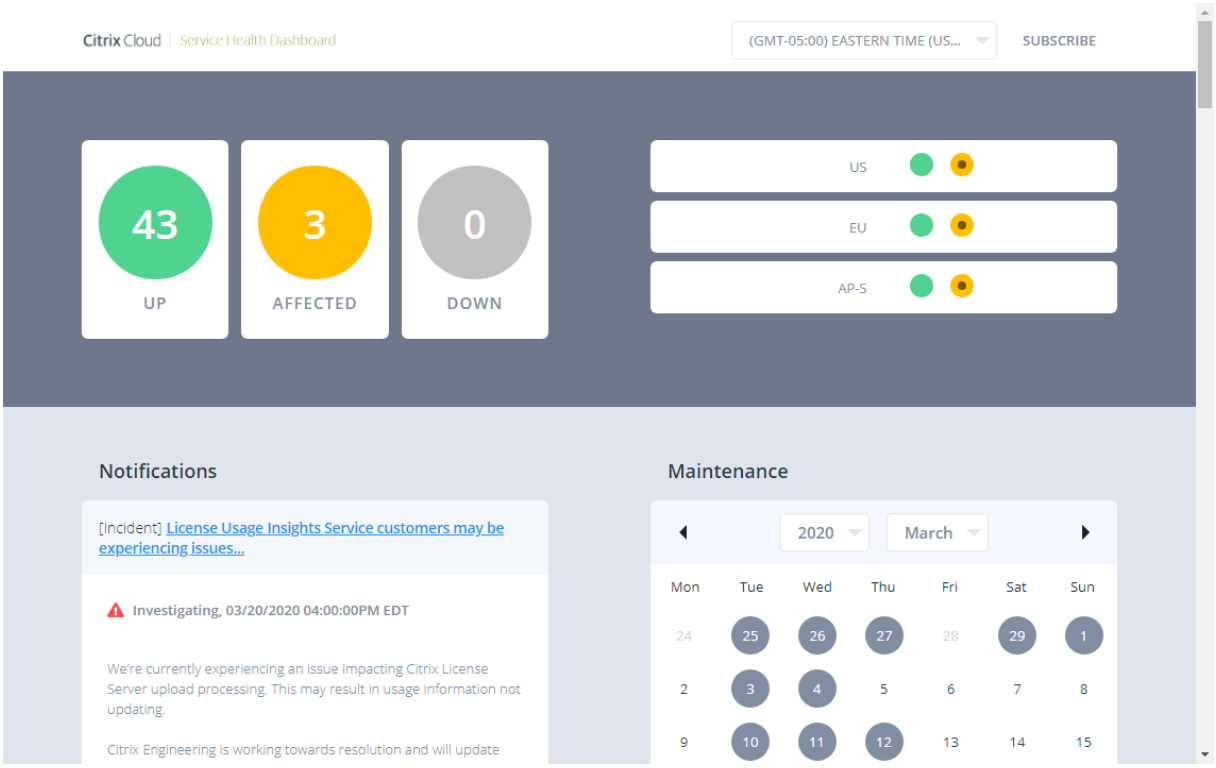


Klicken Sie auf **Zu My Support** und dann auf **My Support**, um ein Ticket im My Support-Portal zu erstellen. Im My Support-Portal können Sie außerdem bestehende Tickets verfolgen und aktuelle Pro-

duktansprüche anzeigen.

Service Health Dashboard

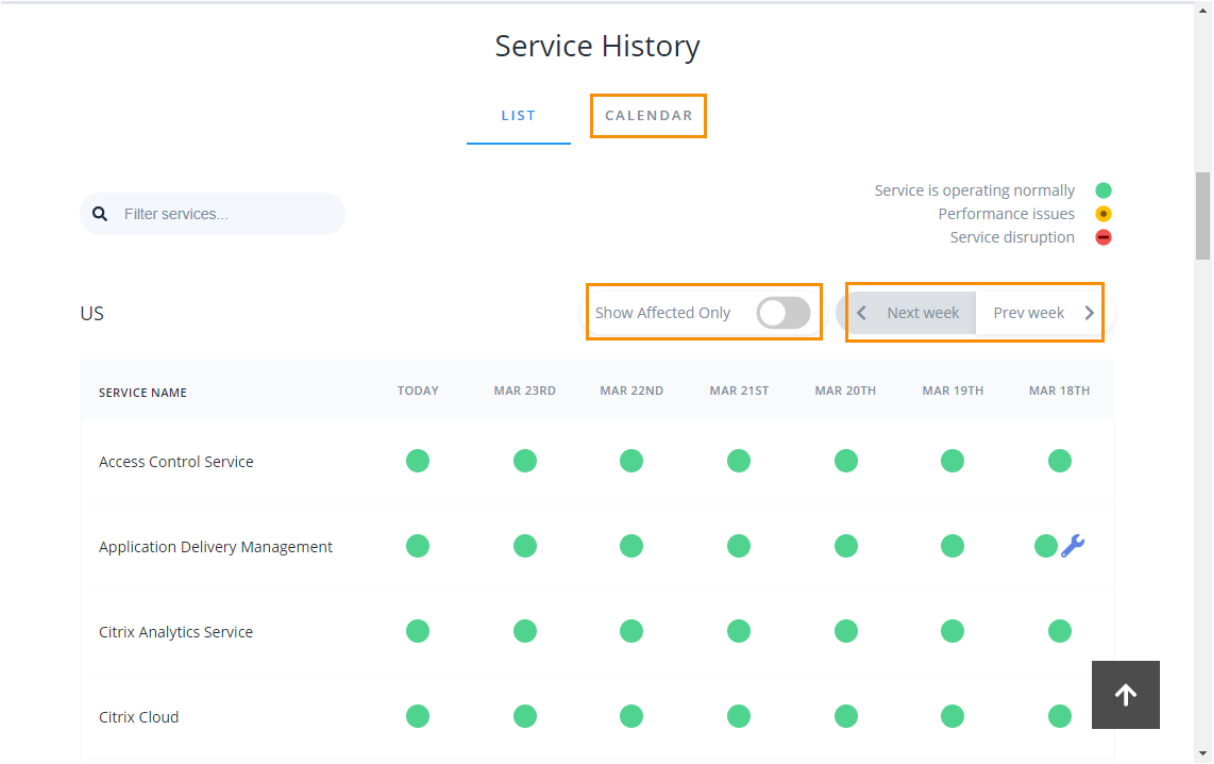
Das Citrix Cloud Service Health Dashboard bietet einen Überblick über die Verfügbarkeit der Citrix Cloud-Plattform und der Dienste in jeder geografischen Region in Echtzeit. Wenn Sie Probleme mit Citrix Cloud haben, überprüfen Sie im Service Health Dashboard, ob Citrix Cloud oder bestimmte Dienste normal funktionieren.



Über das Dashboard erhalten Sie Informationen zu folgenden Elementen:

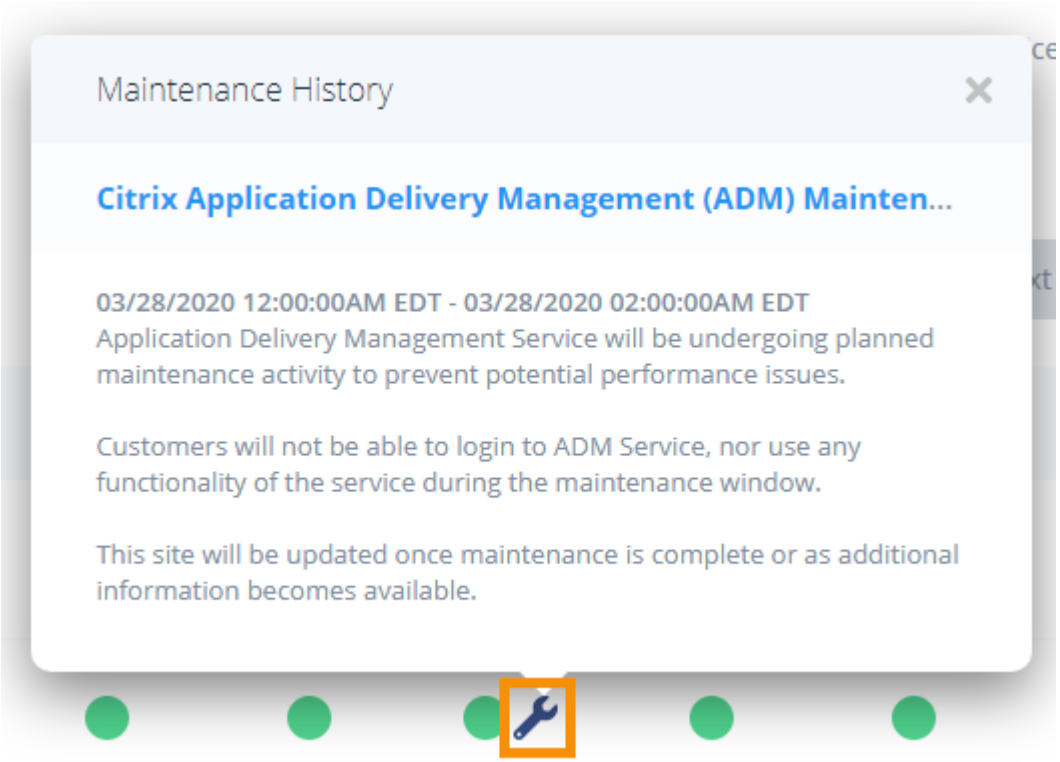
- Der aktuelle Verfügbarkeitsstatus aller Citrix Cloud-Dienste, gruppiert nach geografischer Region
- Die Dienstintegritätshistorie jedes Dienstes für die letzten sieben Tage (Standard) oder für die vorherigen 7-Tage-Inkremente
- Wartungsfenster für bestimmte Services

Standardmäßig wird der Dienststatus als Liste angezeigt, Sie können den Status jedoch auch in einer Kalenderansicht anzeigen. Wählen Sie **Weiter** oder **Zurück** aus, um in Schritten von sieben Tagen durch den Servicestatus zu blättern. Sie können die Liste auch filtern, um nur die betroffenen Dienste anzuzeigen.

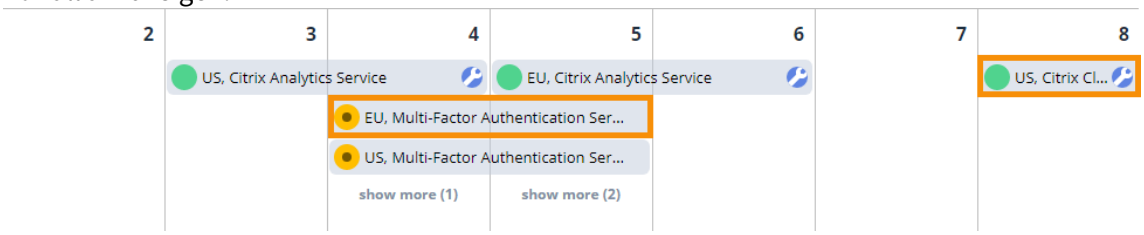


Zum Anzeigen detaillierter Informationen zu einem Service-Incident gehen Sie folgendermaßen vor:

- Klicken Sie in der Listenansicht auf das Symbol neben dem Serviceindikator, um detailliertere Informationen über den Service-Integritätsvorfall anzuzeigen.

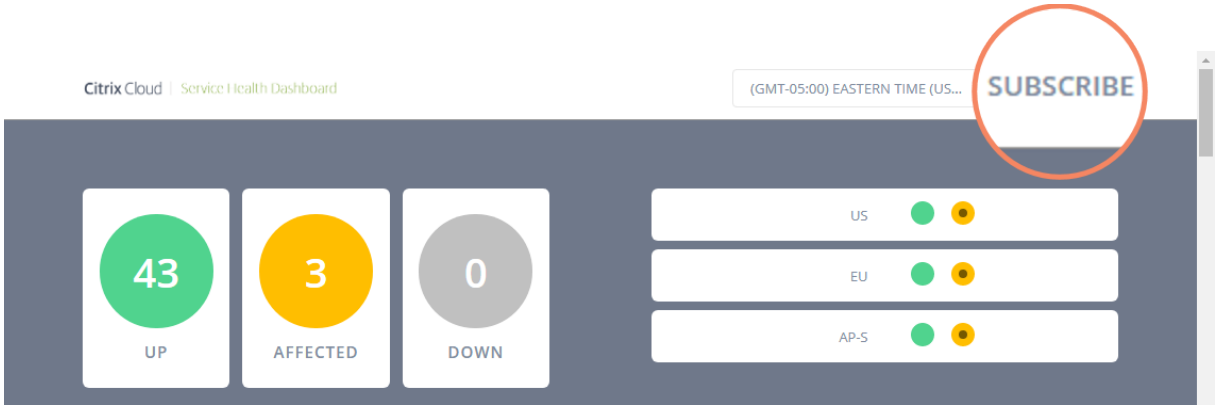


- Klicken Sie in der Kalenderansicht auf den Diensteintrag, um den Status für den Service-Health-Vorfall anzuzeigen.

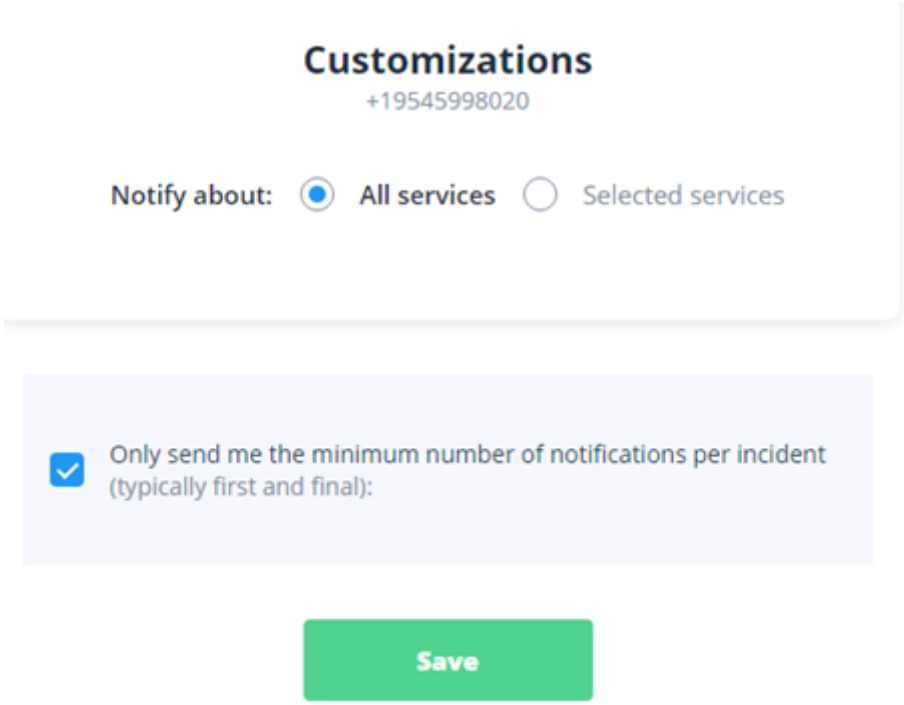


Service Health-Abonnements

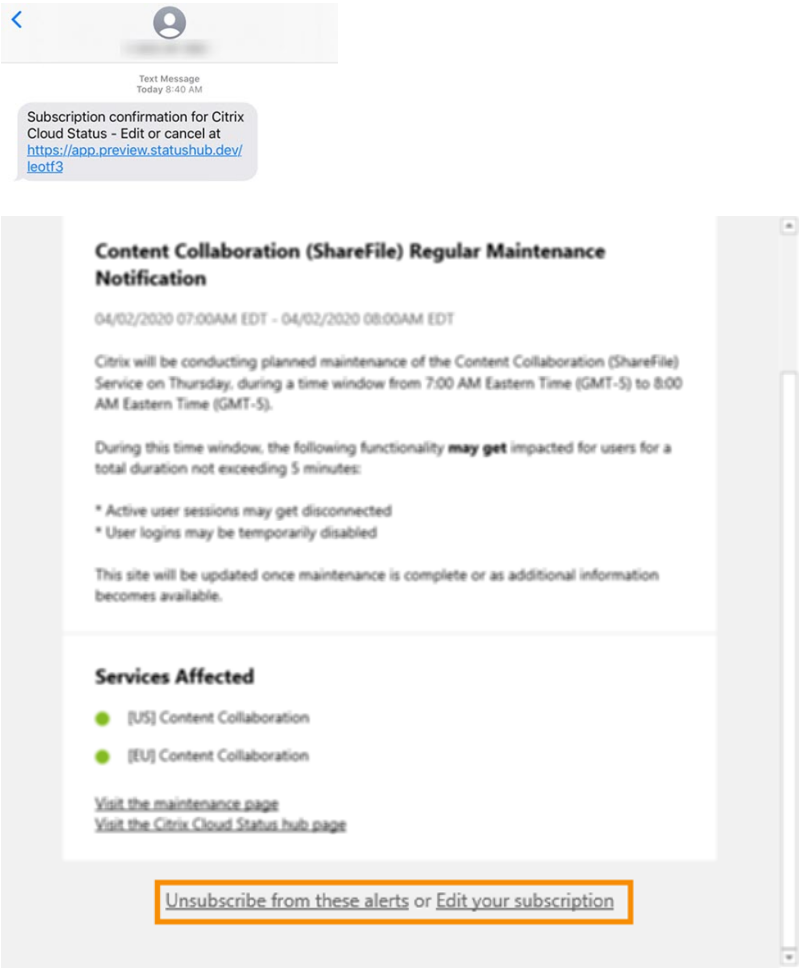
Um Benachrichtigungen zum Dienststatus zu erhalten, klicken Sie oben rechts im Dashboard auf **Abonnieren** und wählen Sie die Benachrichtigungsmethode aus, die Sie verwenden möchten.



Sie können Benachrichtigungen für alle Dienste oder nur für die von Ihnen ausgewählten Dienste abonnieren. Standardmäßig erhalten Sie alle Benachrichtigungen über einen Service-Integritätsvorfall. Um die Häufigkeit von Benachrichtigungen während eines Vorfalls zu begrenzen, können Sie wählen, ob Sie nur die erste und die letzte Benachrichtigung erhalten möchten.



Je nach Abonnementmethode sind Links zum Abbestellen und Ändern Ihrer Einstellungen in der Abonnementbestätigungsnachricht enthalten, die Sie erhalten (z. B. wenn Sie Telefonbenachrichtigungen abonnieren) oder in jeder Benachrichtigung (z. B. wenn Sie E-Mail-Benachrichtigungen abonnieren).



Um sich abzumelden oder Ihre Abonnementeinstellungen zu ändern:

1. Suchen Sie nach einer vorhandenen Benachrichtigung und wählen Sie den Link aus, um sich abzumelden oder Ihre Benachrichtigungseinstellungen zu ändern.
2. Wenn Sie sich abmelden, wählen Sie **Abbestellen** und dann die Benachrichtigungsmethode aus, die Sie kündigen möchten. Um sich von allen Benachrichtigungsmethoden aus zu abonnieren, wählen Sie **Alle Abonnements entfernen**aus.
3. Wenn Sie die Einstellungen ändern, wählen Sie die Benachrichtigungsmethode aus, nehmen Sie die entsprechenden Änderungen an den Diensten und minimalen Vorfallbenachrichtigungen vor, und wählen Sie dann **Speichern**aus.

Low-Touch-Onboarding von NetScaler-Instanzen mithilfe von Console Advisory Connect

January 26, 2024

Wenn Ihre hybride Multi-Cloud (HMC) -Infrastruktur wächst, werden die Herausforderungen bei der Verwaltung, Überwachung, Analyse und Fehlerbehebung von NetScaler-Instanzen vielfältig. Ein zentralisierter Controller, der Einblick in Ihre gesamte Infrastruktur und alle darauf ausgeführten Anwendungen bietet, wird zum Bedarf der Stunde.

In der heutigen Welt muss das Onboarding Ihrer Instanzen auf einem zentralen Controller schnell, einfach und berührungslos erfolgen. Unter Berücksichtigung dieser Anforderung startet NetScaler Console einen neuen Onboarding-Workflow, der Ihnen eine schnellere Möglichkeit bietet, einen vollständigen Überblick über Ihre HMC-Bereitstellung zu erhalten.

Überblick: Komponenten des NetScaler Console-Onboarding-Workflows

Die Bausteine dieses Workflows sind zwei ADC-seitige Komponenten: NetScaler Service Connect und Call Home.

- **Console Advisory Connect**: Es handelt sich um eine neue Funktion in NetScaler, die ein nahtloses Onboarding von NetScaler-Instanzen in die NetScaler Console ermöglicht. Mit dieser Funktion kann die NetScaler-Instanz automatisch eine Verbindung mit NetScaler Console herstellen und System-, Nutzungs- und Telemetriedaten an NetScaler Console senden. Auf der Grundlage dieser Daten bietet Ihnen die NetScaler Console Einblicke und Empfehlungen zu Ihrer NetScaler-Infrastruktur. Zum Beispiel die schnelle Identifizierung von Performance-Problemen, eine hohe Ressourcennutzung und kritische Fehler.

  Console Advisory Connect ist in den folgenden NetScaler-Versionen verfügbar:

  - NetScaler MPX und VPX Image Version 12.1 57.18 und höher und 13.0 61.48 und höher. Weitere Informationen finden Sie unter Einführung in NetScaler Console Connect für NetScaler Appliances.
  - NetScaler SDX Version Image 12.1 58.14 und höher und 13.0 61.48 und höher. Weitere Informationen finden Sie unter Einführung in NetScaler Console Connect für NetScaler SDX-Appliances.

- **Call Home**: Es handelt sich um eine vorhandene Funktion in ADC, die die Instanzen regelmäßig überwacht und Daten automatisch auf den Citrix Technical Support Server hochlädt. Weitere Informationen finden Sie unter Call Home. Die von Call Home gesammelten Daten werden ebenfalls an NetScaler Console weitergeleitet, um diesen neuen Workflow zu ermöglichen.

Alle NetScaler-Instanzen mit Internetkonnektivität oder Call Home oder Instanzen, die mit NetScaler Console Connect aktiviert sind, sind mit NetScaler Console verbunden. NetScaler Console beginnt mit der Erfassung relevanter Metriken von diesen NetScaler-Instanzen über die Call Home-Route, die NetScaler Console-Connect-Route oder beide. Weitere Informationen finden Sie unter Data Governance für MPX- und VPX-Instanzen und Data Governance für SDX-Instanzen.

Anhand dieser Daten erstellt NetScaler Console ein Inventar der NetScaler-Instanzen für jeden Kunden (eindeutige Organisations-ID), das Ihnen eine konsolidierte Liste Ihrer NetScaler-Instanzen anzeigt. NetScaler Console verwendet diese Daten auch, um Einblicke in Ihre NetScaler- und Gateway-Instanzen zu gewinnen, die aussagekräftige Einblicke in Ihre HMC-Bereitstellungen geben, Probleme identifizieren und Maßnahmen zur Minderung der Probleme empfehlen. Bevor Sie die Probleme beheben können, müssen Sie die NetScalerInstanzen in die NetScaler Console integrieren.

Sie können **NetScaler- und Gateway-Instanzen zum Onboarding auswählen aktivieren** und die NetScaler-Instanzen auswählen, die Sie in die NetScaler Console einbinden möchten. Nach dem Start werden Sie zum Onboarding-Prozess geführt.

Der automatische Onboarding-Prozess verwendet Console Advisory Connect, wodurch das Erlebnis automatisiert, nahtlos und schneller wird. Für NetScaler-Instanzen auf Versionen, die Console Advisory Connect und Auto-Onboarding nicht unterstützen, bietet NetScaler Console skriptbasiertes Onboarding, bei dem es sich um einen halbautomatischen Prozess handelt.

> **Hinweise**
>
> - Das automatische und skriptbasierte Onboarding verwendet einen integrierten Agent. Dieser Workflow bietet Ihnen jedoch auch die Flexibilität, einen externen Agent für das Onboarding zu verwenden. Sie können das externe agentenbasierte Onboarding verwenden, wenn Sie die gepoolte Lizenzierung oder die komplette Analytics-Suite in NetScaler Console verwenden möchten. Oder wenn Sie sowohl die gepoolte Lizenzierung als auch die komplette Analytics-Suite verwenden möchten. Der integrierte Agent unterstützt nur Verwaltung und Überwachung.
> - Die von Console Advisory Connect gesammelten Metriken werden direkt an den NetScaler Console-Dienstendpunkt gesendet. Selbst wenn der NetScaler ein verwalteter/erkannter NetScaler auf der NetScaler Console ist und ein externer Agent für diesen ADC konfiguriert wurde, werden die Metriken direkt von NetScaler an den NetScaler Console-Dienstendpunkt gesendet und nicht über den externen Agenten weitergeleitet.

Eine kurze Tour durch das Onboarding

Ihr erster Touchpoint auf der Onboarding-Reise ist eine vom Produkt initiierte E-Mail. Hier ist ein kurzer Überblick über die Onboarding-Reise:

1. Eine vom **NetScaler-Produkt initiierte E-Mail** : Sie erhalten eine E-Mail von NetScaler Console, die einige wichtige Einblicke in Ihre NetScaler-Infrastruktur enthält und Sie dazu einlädt, mit NetScaler Console zu beginnen. Klicken Sie in der E-Mail **auf Onboard to ADM Service** . Die Seite **Citrix Cloud** wird angezeigt.
2. Auf der **Citrix Cloud-Anmeldeseite** :

- Wenn Sie bereits Kunde von Citrix Cloud sind, melden Sie sich mit Ihren Anmeldeinformationen von **Citrix.com**, **My Citrix oder Citrix**Cloud bei **Citrix Cloud**an.
- Wenn Sie noch kein Citrix Cloud-Kunde sind, melden Sie sich bei Citrix Cloud an. Weitere Informationen finden Sie unter Anmelden für Citrix Cloud.

> **Hinweise**
>
> - Wenn Sie Teil mehrerer Organisations-IDs sind und sich eine der Organisations-IDs in Citrix Cloud befindet, melden Sie sich mit Ihren vorhandenen Anmeldeinformationen an. Schließen Sie dann den Onboarding-Workflow für die neue Organisations-ID ab.
> - Sie können die E-Mail-Benachrichtigungen, die Sie im Rahmen des auf Console Advisory Connect basierenden Low-Touch-Onboarding-Workflows erhalten, aktivieren oder deaktivieren. Weitere Informationen finden Sie unter E-Mail-Einstellungen.

3. **NetScaler Console-Willkommensseite**: Sie erhalten einen Überblick über NetScaler Console und ihre Vorteile.
4. **Insights on your NetScaler and Gateway instances**: Sie erhalten detaillierte Einblicke in Ihre gesamte NetScaler-Infrastruktur, einschließlich Sicherheitsratschlägen (Beratung zu aktuellen NetScaler-CVEs), Upgrade-Ratschlägen (Empfehlungen auf der Grundlage von EOM/EOL-Zeitplänen), wichtigen Kennzahlen und Trends. Außerdem werden die Probleme hervorgehoben, die sich auf die Leistung und den Zustand von NetScaler auswirken, und Empfehlungen zur Behebung der Probleme gegeben.
5. **Wählen Sie NetScaler- und Gateway-Instanzen für das Onboarding aus**: Sie erhalten eine konsolidierte Ansicht Ihres NetScalerInventory. Sie können auswählen, welche NetScalerInstanzen Sie in die NetScaler Console integrieren möchten.
6. **Integrieren Sie NetScaler-Instanzen in die NetScaler Console**: Basierend auf den NetScalerInstanzen , die für das Onboarding ausgewählt wurden, führt Sie NetScaler Console durch den Onboarding-Prozess. Standardmäßig ist der integrierte Agent für das automatische Onboarding ausgewählt.
7. **NetScaler Console-GUI-Dashboard**: Nach Abschluss des Onboardens werden Sie zum Instanz-Dashboard der NetScaler Console weitergeleitet.

Weitere Informationen zu jeder dieser Onboarding-Methoden finden Sie unter Onboarding von NetScaler-Instanzen mithilfe von NetScaler Console Connect.

Integrieren Sie NetScaler-Instanzen mithilfe von Console Advisory Connect

January 26, 2024

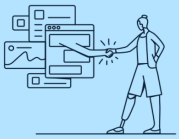
Dieses Dokument enthält eine schrittweise Anleitung, die Ihnen den Einstieg in NetScaler Console erleichtert. Bevor Sie beginnen, lesen Sie, wie die NetScaler Console einen neuen Onboarding-Workflow einleitet, der Ihnen eine schnellere Möglichkeit bietet, einen vollständigen Überblick über Ihre Hybrid-Multi-Cloud-Bereitstellung (HMC) zu erhalten. Weitere Informationen finden Sie unter Low-Touch-Onboarding von NetScaler-Instanzen mithilfe von NetScaler Console Connect .

Schritt 1: Loslegen

Sie erhalten eine E-Mail von der NetScaler Console, die einige wichtige Einblicke in Ihre NetScaler-Infrastruktur enthält und Sie dazu einlädt, mit der NetScaler Console zu beginnen.

citrix

Onboard to Citrix ADM Service for Security Advisory



Hello [redacted] Org ID - [redacted]

As a valued Citrix customer, your application delivery infrastructure security is our top concern. To help keep your infrastructure secure, we just launched **security advisory and upgrade advisory** for your Citrix ADCs.

These new features can identify outdated software deployed in your ADC fleet, notify you of known vulnerabilities in these releases, and suggest steps you can take to remediate these issues.

Below, you'll see a preview of these advisories and other key insights customized to your infrastructure. More information and recommended actions are available when you onboard to Citrix ADM service. You can get started with Citrix ADM Service Express account at no additional cost.

Insights on your ADC & Gateway infrastructure

These insights are based on data provided via Call Home and/or Citrix ADM Service Connect.

ADC instances by platforms

30	20	5	5
Total	VPX	SDX	MPX

Security Advisory

5 ADC instances are on versions with known common vulnerability exposures (CVEs).
This advisory is based on ADC build version scan only & more conclusive & exhaustive security advisory insights can be seen after onboarding all your ADCs to ADM Svc

Upgrade Advisory

2 ADC instances are on versions that have reached end of life in last 365 days or earlier.

1 ADC instance is on a version that will reach end of life in next 365 days.

3 ADC instances are on versions that have reached end of maintenance in last 365 days or earlier.

4 ADC instances are on versions that will reach end of maintenance in next 365 days.

2 ADC instances are on older builds and releases.

Recent events

4 ADC instances encountered SSL card failure.
2 ADC instances encountered hard disk failure.

Resource utilization

2 ADC instances CPU usage exceeded 50%
3 ADC instances memory usage exceeded 50%

ADC deployment

5 ADC instances are not deployed as High Availability (HA) pair. Citrix ADM recommends HA pair for production ADC instances.

To get more details and recommendations on these insights, **onboard your ADC instances to Citrix ADM service, today.**

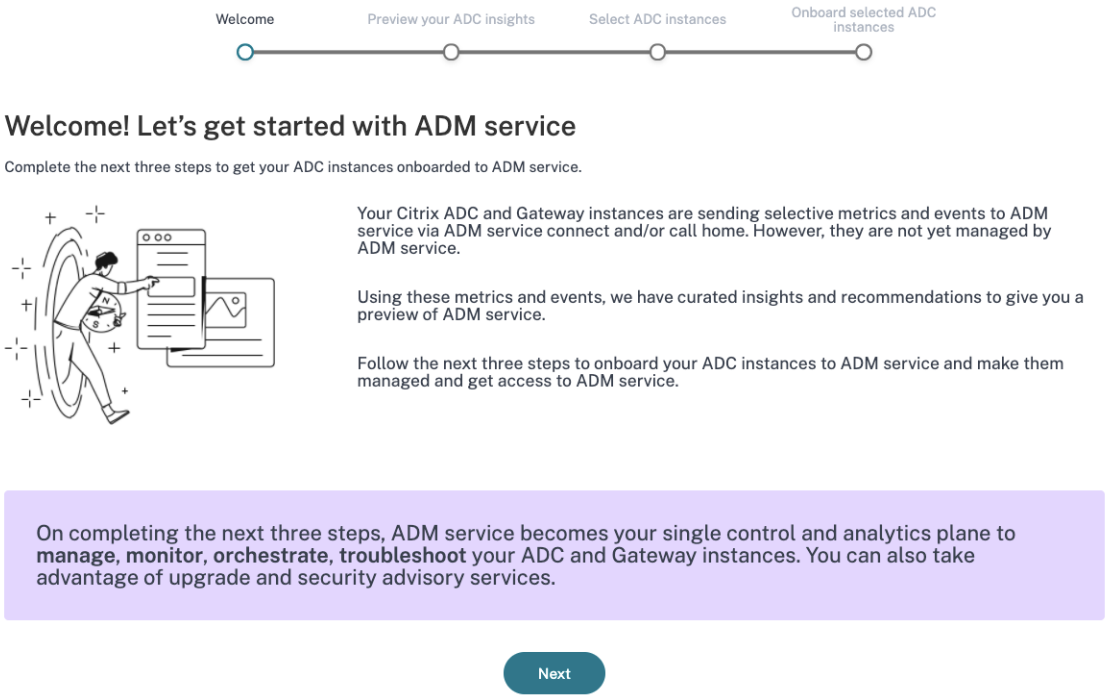
As a first step, you will need to create Citrix Cloud account by clicking on the button below.

Onboard to ADM Service

1. Klicken Sie in der E-Mail auf **Onboard to ADM Service**. Die Seite **Citrix Cloud** wird angezeigt.
2. Auf der **Citrix Cloud-Anmeldeseite** :
   - Wenn Sie bereits Kunde von Citrix Cloud sind, melden Sie sich mit Ihren Anmeldeinformationen von **Citrix.com**, **My Citrix oder Citrix**Cloud bei **Citrix Cloud**an.
   - Wenn Sie noch kein Citrix Cloud-Kunde sind, melden Sie sich bei Citrix Cloud an. Weitere Informationen finden Sie unter Anmelden für Citrix Cloud.

   > **Hinweise**
   >
   > - Wenn Sie Teil mehrerer Organisations-IDs sind und sich eine der Organisations-IDs in Citrix Cloud befindet, melden Sie sich mit Ihren vorhandenen Anmeldeinformationen an. Schließen Sie dann den Onboarding-Workflow für die neue Organisations-ID ab.
   > - Sie können die E-Mail-Benachrichtigungen, die Sie im Rahmen des auf Consolve Advisory Connect basierenden Low-Touch-Onboarding-Workflows erhalten, aktivieren oder deaktivieren. Weitere Informationen finden Sie unter E-Mail-Einstellungen.

3. Nehmen Sie sich auf der NetScaler Console-Landingpage einen Moment Zeit, um zu erfahren, warum Sie dort sind und welche Vorteile die Verwendung von NetScaler Console mit sich bringt.



> **Hinweis**
>
> Die Sicherheitshinweise in der E-Mail basieren ausschließlich auf dem NetScaler Build-Versionsscan. Nach dem Onboarding Ihrer NetScaler-Instanzen in NetScaler Console erhalten

> Sie aussagekräftigere und umfassendere Einblicke in Sicherheitsratgeber.

1. Klicken Sie auf **Weiter**. Die Seite **Insights on your NetScaler and Gateway instances** wird geöffnet.

Die nächsten Schritte dienen als geführter Workflow, der Ihnen eine Vorschau auf das bietet, was NetScaler Console bieten kann, und Ihnen dabei hilft, Ihre NetScaler-Instanzen nahtlos in NetScaler Console zu integrieren.

Schritt 2: Einblicke in Ihre NetScaler- und Gateway-Instanzen

Diese Insights-Seite verwendet die Daten, die über Call Home oder NetScaler Console Connect oder sowohl Call Home als auch NetScaler Console Connect gesammelt wurden, um Einblicke in Ihre NetScaler-Instanzen bereitzustellen. Auf dieser Seite erhalten Sie Einblicke in Ihre gesamte NetScaler-Infrastruktur, einschließlich Sicherheitsempfehlungen (Beratung zu aktuellen NetScaler-CVEs), Upgrade-Ratschlägen (Empfehlungen auf der Grundlage von EOM/EOL-Zeitplänen), wichtigen Kennzahlen und Trends. Außerdem werden die Probleme hervorgehoben, die sich auf die Leistung und den Zustand von NetScaler auswirken, und es wird empfohlen, diese Probleme zu beheben. Diese Erkenntnisse und Empfehlungen sind nur eine kleine Vorschau auf die zahlreichen Vorteile und den Mehrwert, die NetScaler Console zu bieten hat. Um viele weitere Vorteile und detaillierte Einblicke zu erhalten und die empfohlenen Aktionen ausführen zu können, müssen Sie die NetScaler-Instanzen in die NetScaler Console integrieren.

Die Erkenntnisse und Empfehlungen sind in folgende Typen unterteilt:

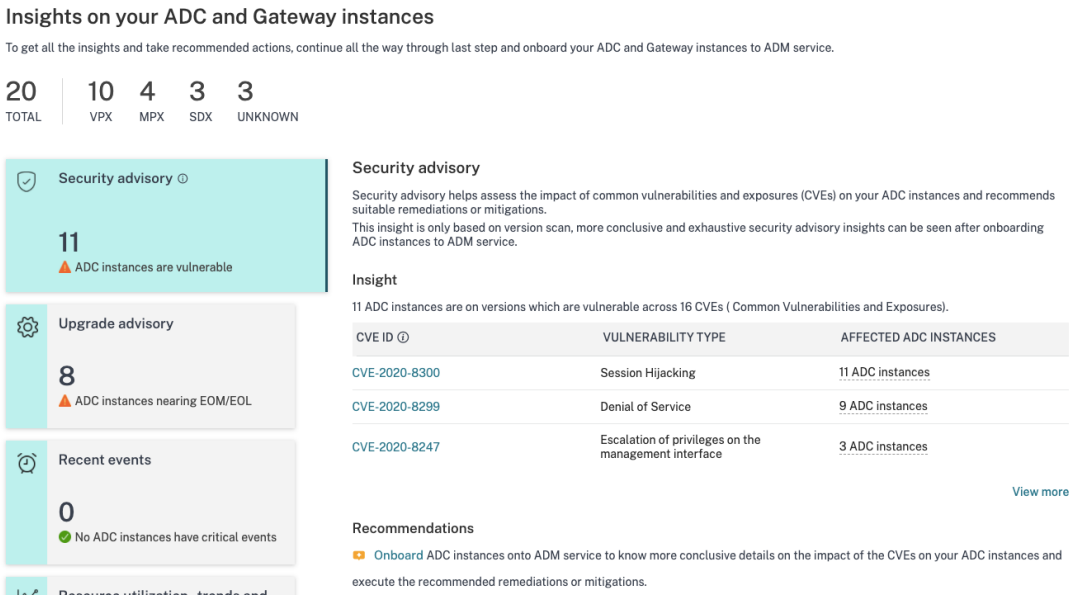
- **Sicherheitshinweis**: Integrieren Sie NetScaler-Instanzen, um die CVE-Auswirkungen auf Ihre NetScaler-Instanzen abzurufen und die empfohlenen Abhilfemaßnahmen oder Abhilfemaßnahmen durchzuführen.
- **Upgrade-Empfehlung**: Integrieren Sie NetScaler-Instanzen in die NetScaler Console und aktualisieren Sie Ihre NetScaler-Instanzen, die EOM/EOL erreicht haben oder gerade erreichen oder auf älteren Versionen/Builds laufen.
- **Aktuelle Ereignisse**: Integrieren Sie NetScaler-Instanzen in die NetScaler Console, um regelmäßig über 200 Ereignisse zu überwachen und Regeln zu erstellen, um per E-Mail benachrichtigt zu werden. PagerDuty, Slack, ServiceNow, ergreifen Sie die entsprechenden Maßnahmen.
- **Ressourcenauslastung —Trends und Anomalien**: Integrieren Sie NetScaler-Instanzen in die NetScaler Console, um einen umfassenden Überblick über den Zustand und die Leistungsprobleme der NetScaler-Instanz zu erhalten und Empfehlungen zur Behebung dieser Probleme zu erhalten. Sie können auch die vorhergesagte CPU- und Speicherauslastung für Ihre NetScaler-Instanzen bewerten.

- **Anleitung**zur NetScaler-Bereitstellung : Integrieren Sie NetScaler-Instanzen in die NetScaler Console und konfigurieren Sie sie mithilfe von Konfigurationsaufträgen auf der NetScaler Console als HA-Paar.

1. **Sicherheitshinweis**: Die NetScaler Console Security Advisory warnt Sie vor Sicherheitslücken, die Ihre NetScaler-Instanzen gefährden, und empfiehlt Abhilfemaßnahmen und Abhilfemaßnahmen.

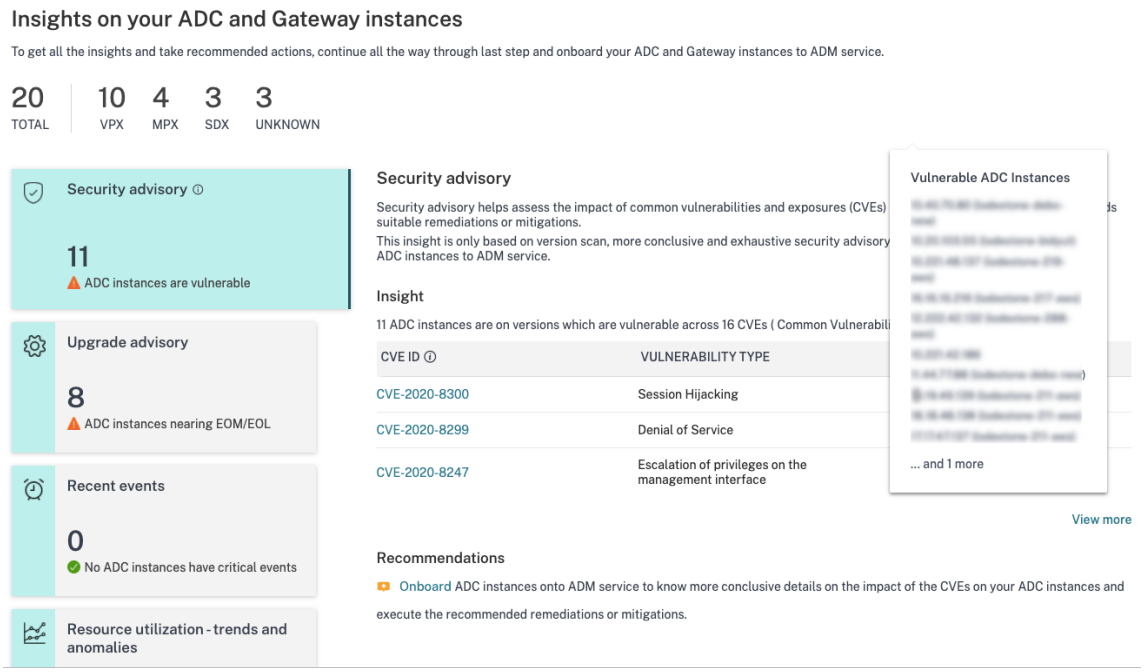
   > **Hinweis:**
   >
   > Die Erkenntnisse der Sicherheitshinweise in der Onboarding-E-Mail und im geführten Workflow basieren ausschließlich auf dem NetScaler-Build-Versionsscan. Nach dem Onboarding Ihrer NetScaler-Instanzen in die NetScaler-Konsole erhalten Sie aussagekräftige und umfassende Einblicke in die Sicherheitsempfehlungen. **Beispiel** : Wenn ein CVE zur Schwachstellenanalyse sowohl einen Versionsscan als auch einen Konfigurationsscan benötigt, zeigen die Onboarding-E-Mail und der geführte Workflow die Ergebnisse auf der Grundlage des Versionsscans. Es könnte also falsch positive Ergebnisse geben. Um eine aussagekräftigere und genauere Bewertung der Auswirkungen zu erhalten, integrieren Sie NetScaler in NetScaler Console. Nach dem Onboarding zeigt die Sicherheitsempfehlung von NetScaler Console die Folgenabschätzung. Dabei handelt es sich um eine anfällige NetScaler-Bewertung, die auf Versionsscan und Konfigurationsscan basiert.

   Sie können die CVE-ID, den Schwachstellentyp und die betroffenen NetScaler-Instanzen überprüfen. Der CVE-ID-Link geht zum Artikel im Sicherheitsbulletin.



   Die Empfehlung leitet Sie an, Ihre NetScaler-Instanzen in die NetScaler Console zu integrieren, um weitere Informationen über die Auswirkungen von CVE auf Ihre NetScaler-Instanzen zu erhalten und die empfohlenen Abhilfemaßnahmen oder Abhilfemaßnahmen durchzuführen.

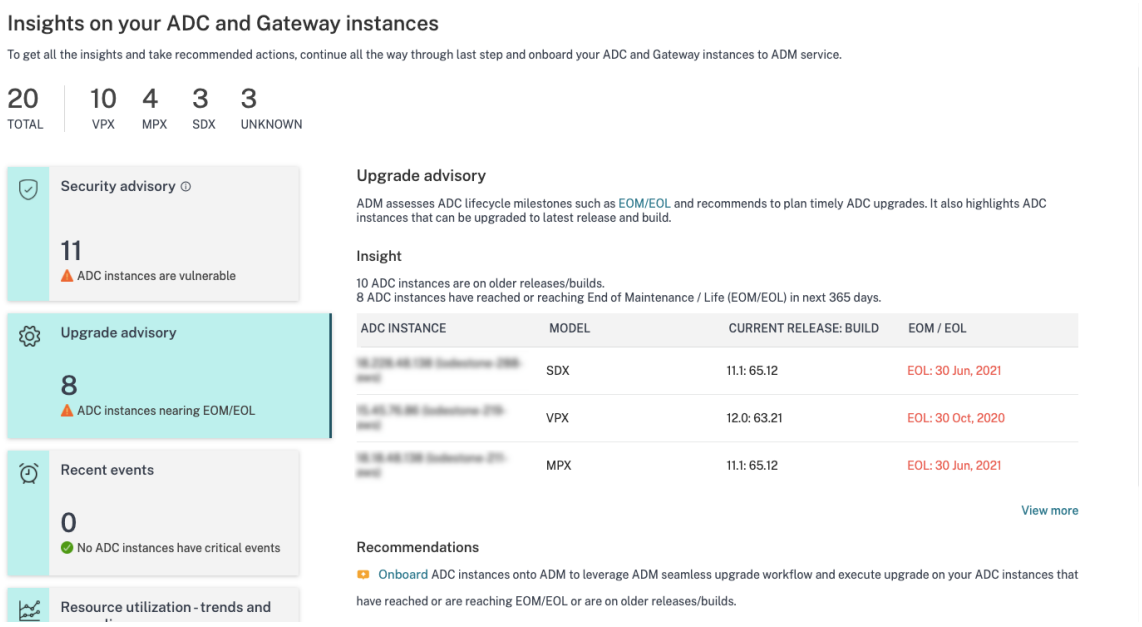
Klicken Sie auf die betroffenen NetScaler-Instanzen, um die IP-Adressen der betroffenen Instanzen anzuzeigen.



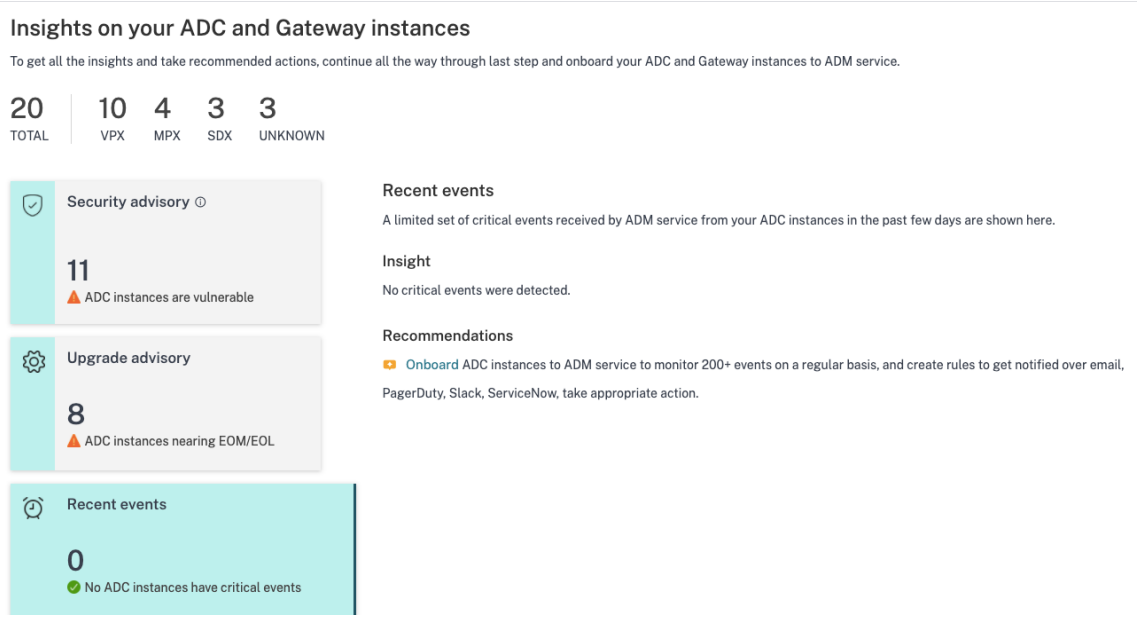
2. **Upgrade-Empfehlung**: Verwenden Sie diese Empfehlung, um zu überprüfen, welche NetScaler-Instanzen kurz vor EOM/EOL stehen oder sich auf älteren Builds befinden.

   Basierend auf diesen Erkenntnissen empfiehlt NetScaler Console, vor EOM/EOL ein zeitnahes Upgrade zu planen oder von den neuesten Funktionen und Fixes zu profitieren.

   Um das Upgrade durchzuführen, müssen Sie Ihre NetScaler-Instanzen in die NetScaler Console einbinden.

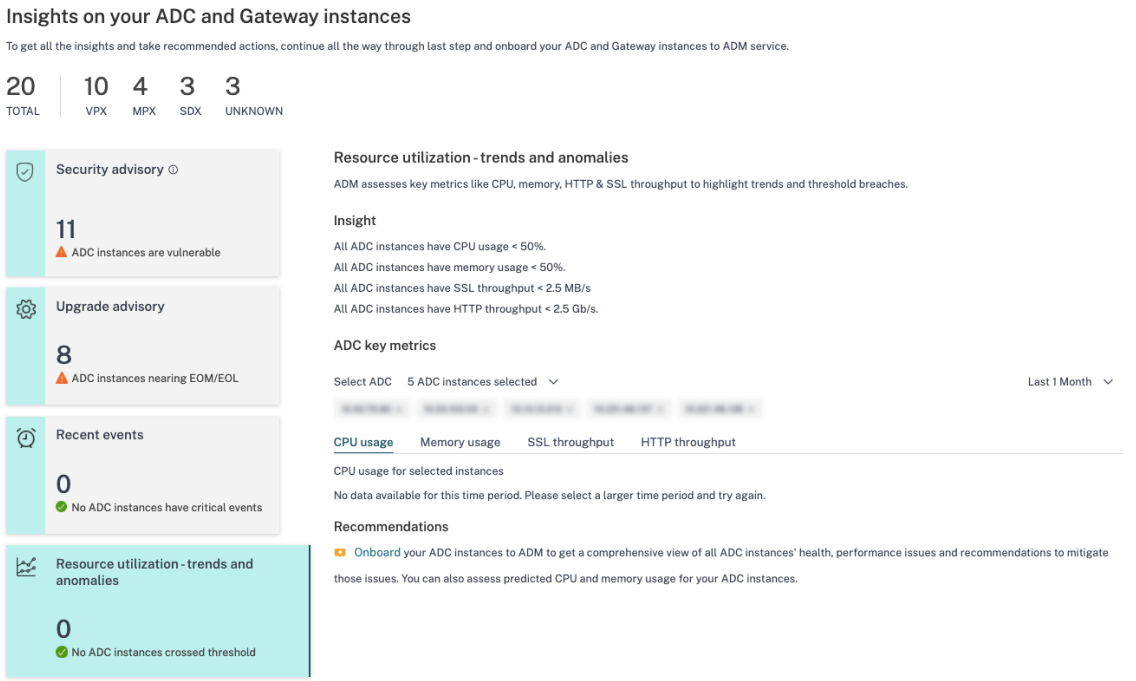


3. **Aktuelle Ereignisse**: Rufen Sie Details zu einigen kritischen Fehlern ab, die auf den NetScaler-Instanzen aufgetreten sind, sowie eine Liste der NetScaler-Instanzen, auf denen die Fehler aufgetreten sind.

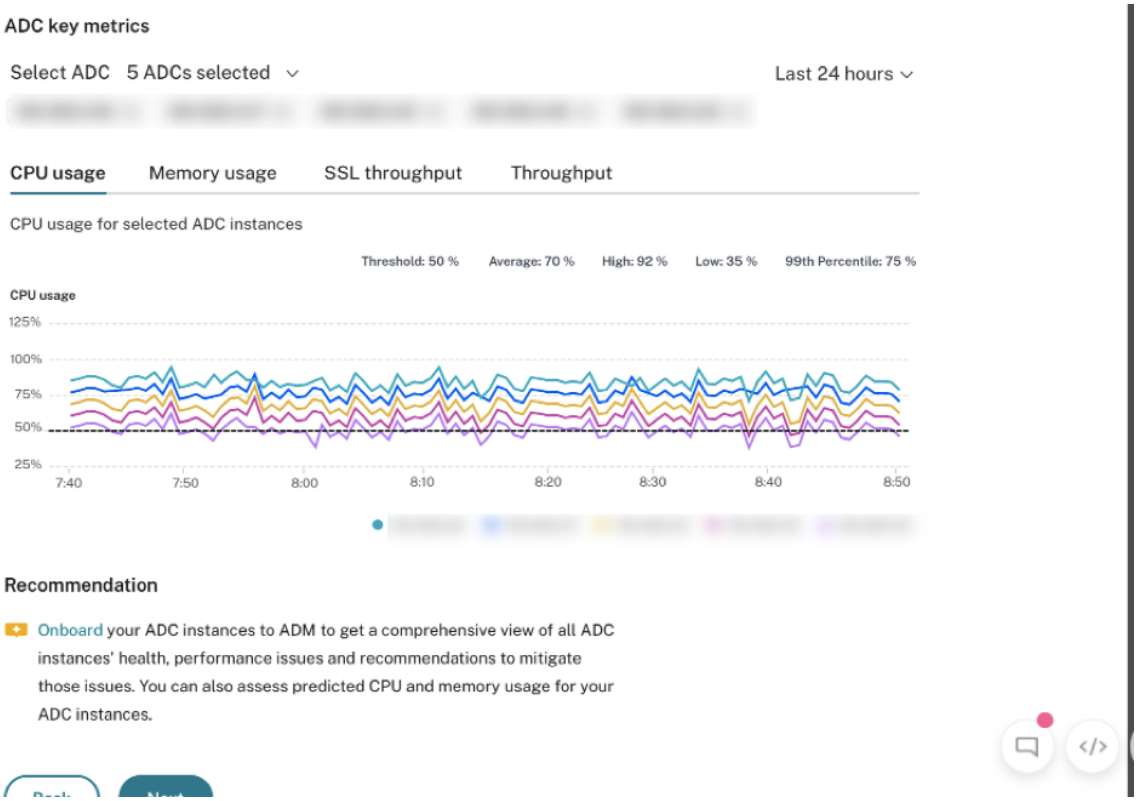


4. **Ressourcennutzung - Trends und Anomalien**: Hier finden Sie Einblicke in eine hohe Ressourcenauslastung für CPU-, Speicher-, HTTP-Durchsatz und SSL-Durchsatz. Für jeden Einblick schlägt NetScaler Console Handlungsempfehlungen vor. Um einen besseren Einblick in diese Erkenntnisse und Empfehlungen zu erhalten, müssen Sie Ihre NetScaler-Instanzen in die NetScaler Console integrieren. Einige Vorteile nach dem Onboarding sind:

    - CPU: Prognostizieren Sie die CPU-Auslastung für die nächsten 24 Stunden auf der NetScaler Console.
    - Arbeitsspeicher: Prognostizieren Sie die Speicherauslastung für die nächsten 24 Stunden auf der NetScaler Console.
    - SSL-Durchsatz: Sehen Sie sich die SSL-Echtzeitoptimierung mit intelligenten App Analytics auf der NetScaler Console an.
    - HTTP-Durchsatz: Beheben Sie NetScaler-Durchsatzkapazitätsprobleme mit Infrastructure Analytics.

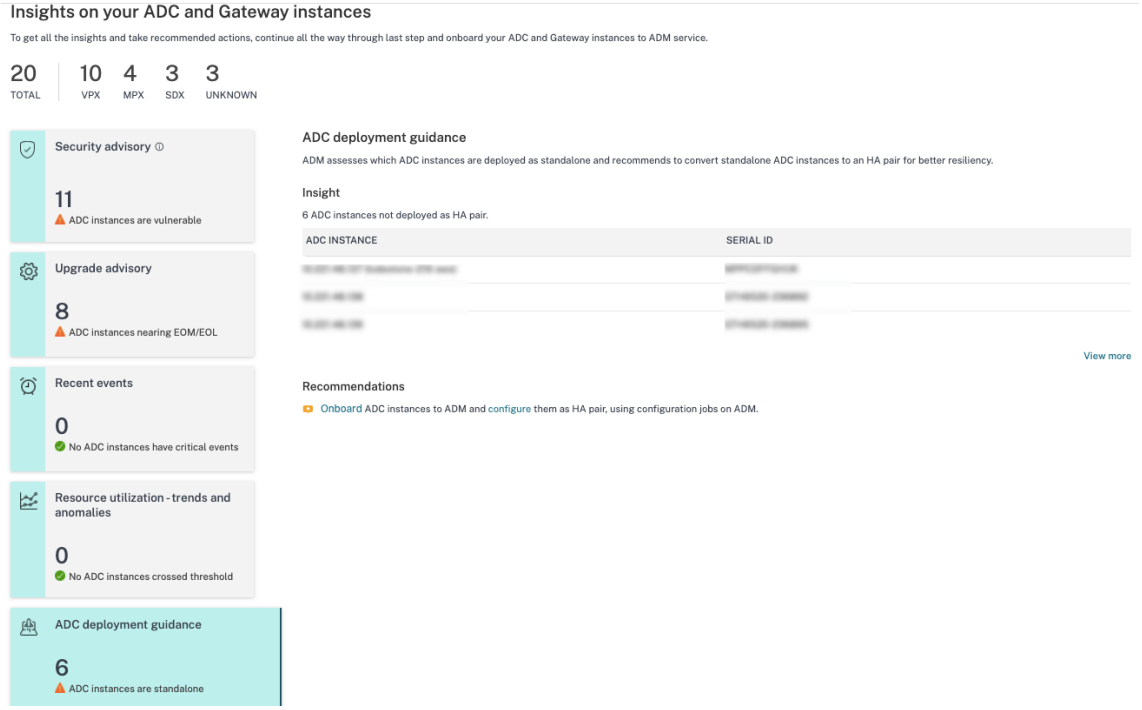


- **Wichtige Metriken**: Erhalten Sie Details zu wichtigen Metriken in Bezug auf CPU, Speicher, HTTP-Durchsatz, SSL-Durchsatz und decken Sie anomale Trends in den Metriken auf.



5. **Anleitung**zur Bereitstellung : Verschaffen Sie sich einen Überblick über NetScaler-Instanzen, die als eigenständiges NetScaler bereitgestellt werden. NetScaler Console empfiehlt, diese

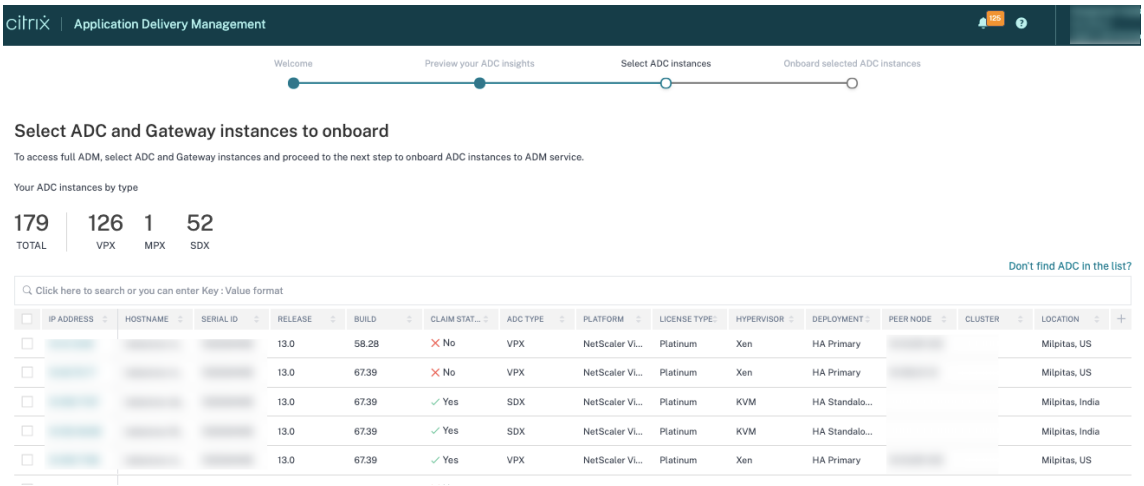
NetScaler-Instanzen für eine bessere Stabilität als HA-Paar zu konfigurieren. Dazu müssen Sie Ihre NetScaler-Instanzen in die NetScaler Console einbinden und dann Wartungsaufträge verwenden, um die Instanzen als HA-Paar zu konfigurieren.



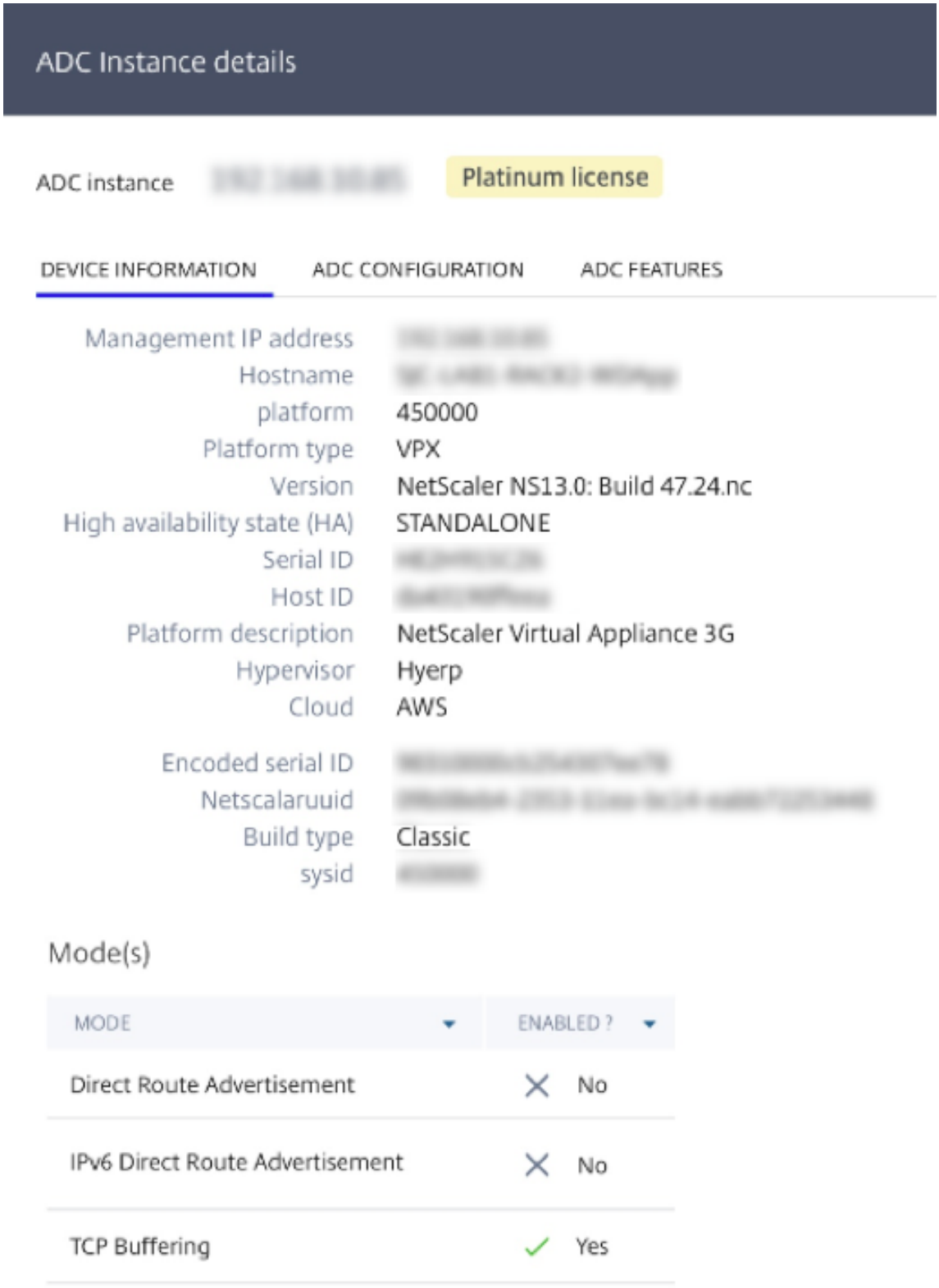
Schritt 3: Wählen Sie NetScaler- und Gateway-Instanzen für das Onboarding aus

Auf dieser Seite werden alle NetScaler- und Gateway-Instanzen in Ihrer Umgebung angezeigt. Zeigen Sie die NetScaler- und Gateway-Instanzen an, die Sie in die NetScaler Console einbinden möchten, wählen Sie sie aus und klicken Sie auf **Weiter**.

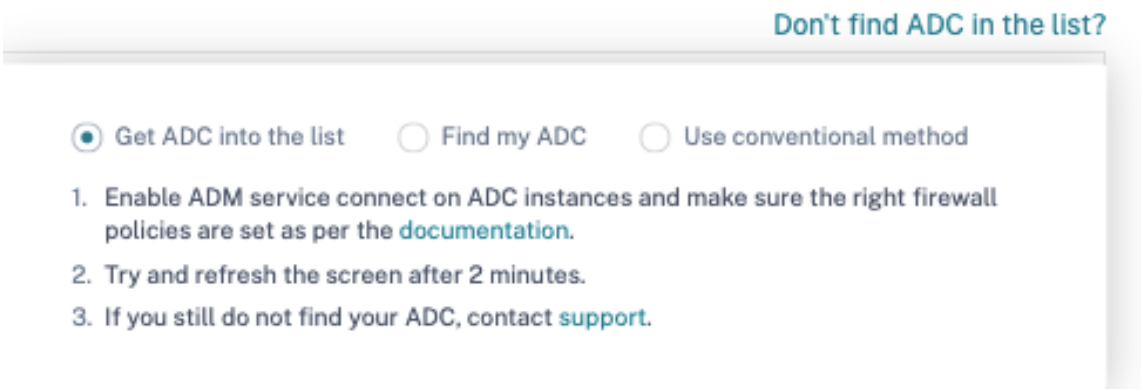
1. Zeigen Sie die NetScaler-Instanzen an, die Sie in die NetScaler Console einbinden möchten, und wählen Sie sie aus.



Wenn Sie Details zu einer Instanz wie Geräteinformationen, NetScaler-Konfiguration, verfügbare NetScaler-Funktionen oder Lizenzinformationen benötigen, klicken Sie unter der NetScaler-Instanz auf die Instanz-IP-Adresse.

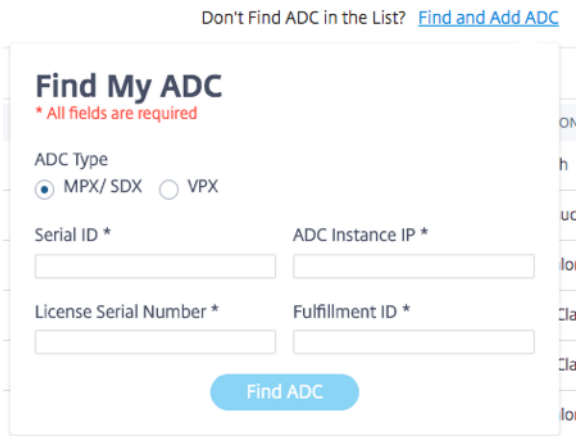


Wenn Ihre Instance nicht aufgeführt ist, verwenden Sie Don't find **NetScaler in der** Liste in der oberen rechten Ecke.



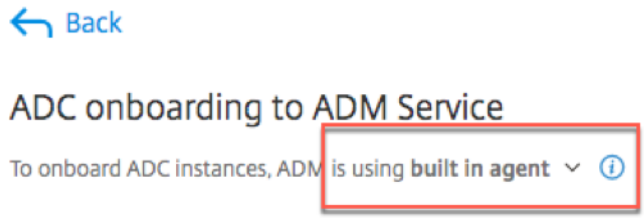
Sie können auf drei Arten vorgehen: Folgen Sie den Schritten unter **NetScaler in die Liste aufnehmen** oder verwenden Sie die **Option Find my NetScaler** . Wenn diese beiden Schritte nicht helfen, klicken Sie auf **Konventionelle Methode verwenden**. Dadurch wird der Workflow übersprungen und Sie werden durch die herkömmliche Methode zum Onboarding von NetScaler-Instanzen geführt.

Geben Sie für die **Option Find my NetScaler** die Details in die Pflichtfelder ein (Seriennummer, NetScaler-Instanz-IP-Adresse, Lizenzseriennummer und Fulfillment-ID) und suchen Sie.



Schritt 4: Integrieren von NetScaler-Instanzen in NetScaler Console

Sie können Ihre Instanzen mit dem integrierten Agent (Standardoption) oder einem externen Agent einbinden.



Integrieren NetScaler-Instanzen mithilfe eines integrierten Agenten

Automatisches und skriptbasiertes Onboarding verwenden den integrierten Agent, der standardmäßig eingestellt ist.

Auto-Onboarding: Es wird nur in den folgenden NetScaler-Versionen unterstützt:

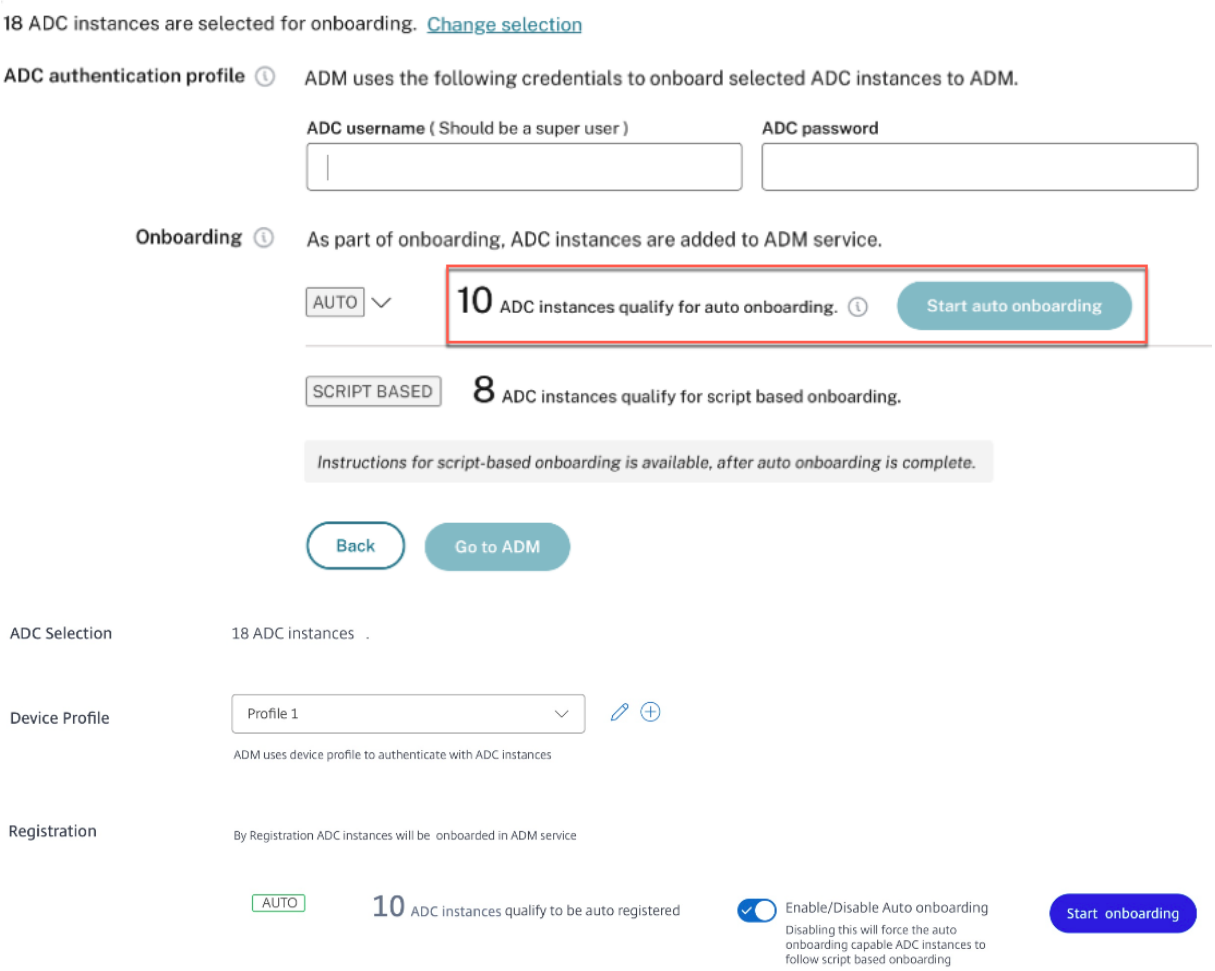
- NetScaler MPX und VPX Image-Version 12.1 57.18 und höher sowie 13.0 61.48 und höher
- SDX-Image Version 13.0 61.48 und höher und 12.1 58.14 und höher

Um eine andere NetScaler-Instanz auszuwählen, klicken Sie auf **Auswahl ändern** .

Von den insgesamt ausgewählten NetScaler-Instanzen kommen einige Instanzen möglicherweise für das automatische Onboarding in Frage (basierend auf Mindestversionskriterien). Sie können die Instanzen sehen, die sich für das automatische Onboarding qualifizieren.

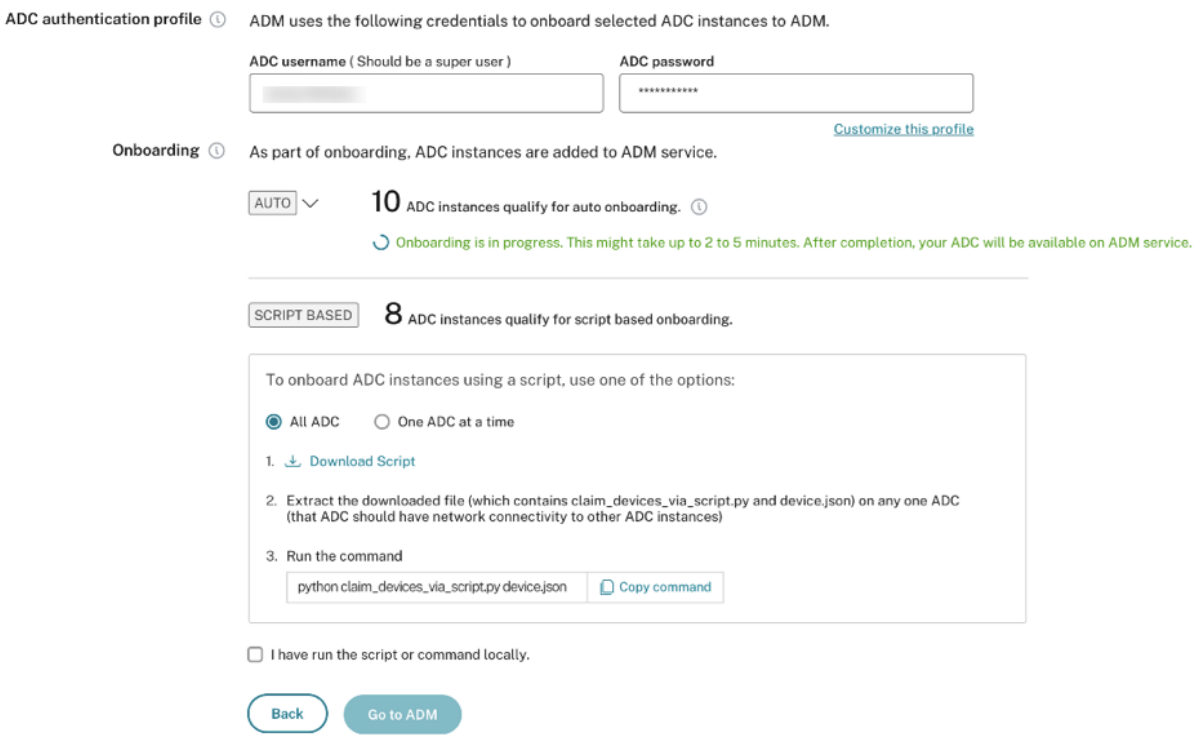
Sie können einen Onboarding-Testlauf durchführen, um sicherzustellen, dass die NetScaler-Instanz bereit für das Onboarding ist. Klicken Sie auf **Test**, um den Testlauf zu starten. Weitere Informationen finden Sie unter Testen der Onboarding-Bereitschaft von NetScaler-Instanzen .

Wenn Sie das Onboard ohne den Testlauf durchführen möchten, geben Sie den NetScaler-Benutzernamen und das Kennwort ein. Bei den Anmeldeinformationen muss es sich um NetScaler-Benutzeradministratoranmeldeinformationen handeln, und NetScaler Console verwendet diese Anmeldeinformationen für das Onboarding von NetScaler. Klicken Sie auf **Auto Onboarding starten**, um Ihre NetScaler-Instanzen in der NetScaler Console zu integrieren.



> **Hinweis**
>
> Nachdem Sie die NetScaler-Anmeldeinformationen angegeben und das Geräteprofil erstellt haben, fordert die ADM-GUI nicht erneut zur Eingabe des Benutzernamens und des Kennworts für jede NetScaler-Instanz auf. Sie können das Profil jedoch aus der Dropdownliste **Geräteprofil** auswählen, um die NetScaler-Instanzen zu authentifizieren.

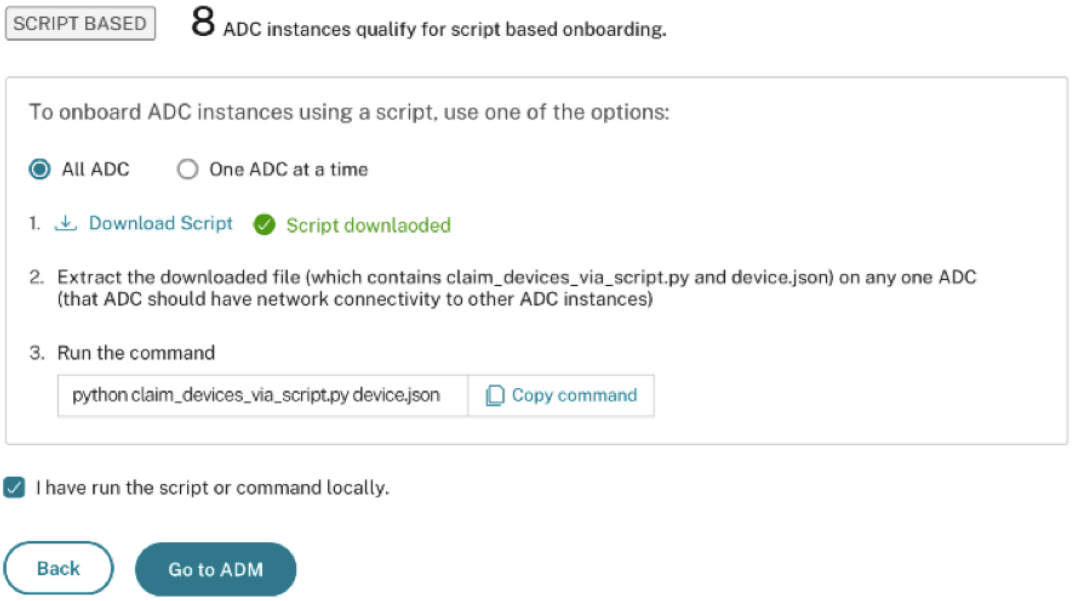
Das automatische Onboarding kann bis zu 2-5 Minuten in Anspruch nehmen.



> **Hinweis:**
>
> Wenn Sie nicht möchten, dass die NetScaler-Instanzen automatisch in die NetScaler Console eingebunden werden, können Sie das automatische Onboarding deaktivieren und die skriptbasierte Option für das Onboarding verwenden.

Skriptbasiertes Onboarding: Nachdem das automatische Onboarding abgeschlossen ist, können Sie die restlichen Instanzen mithilfe des skriptbasierten Onboarding einbinden. Verwenden Sie eine der folgenden Optionen:

- **Option 1**: Laden Sie das Skript herunter, extrahieren Sie die TAR-Datei und führen Sie sie auf einer der NetScaler-Instanzen aus, indem Sie den auf der Benutzeroberfläche angegebenen Befehl verwenden. Stellen Sie sicher, dass die NetScaler-Instanz, auf der Sie dieses Skript ausführen, über Netzwerkkonnektivität zu allen anderen ausgewählten NetScaler-Instanzen verfügt.
- **Option 2**: Melden Sie sich bei der CLI-Konsole jeder NetScaler-Instanz an und führen Sie die auf der Benutzeroberfläche angegebenen Befehle aus. Weitere Informationen finden Sie in Schritt 7 im Dokument Konfigurieren Sie den integrierten NetScaler-Agenten zur Verwaltung von Instanzen . Stellen Sie sicher, dass Sie für jede NetScaler-Instanz einen neuen eindeutigen Aktivierungscode generieren.

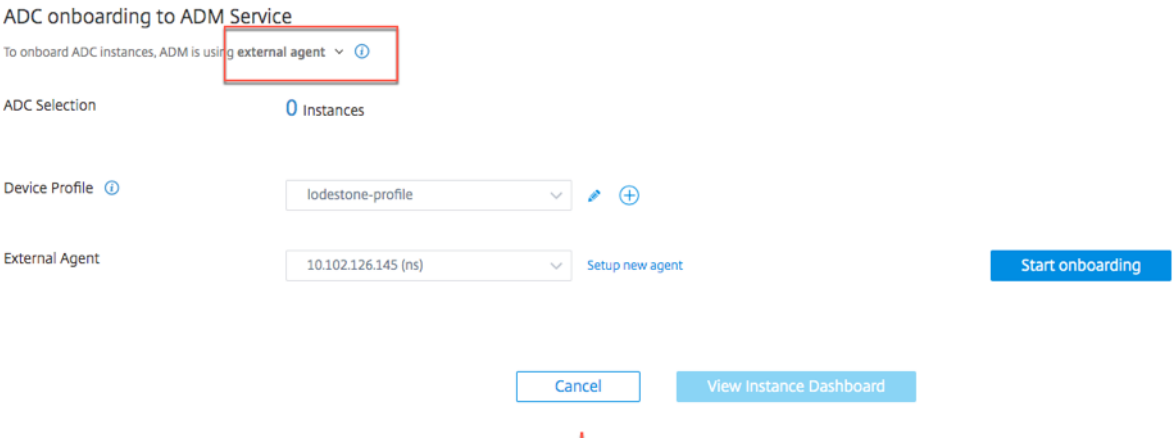


Nachdem Sie alle Ihre Instanzen integriert haben, klicken Sie auf Gehe **zu NetScaler Console**, um zum Dashboard der NetScaler Console-Instanzverwaltungs-Benutzeroberfläche zu wechseln und die verschiedenen Funktionen zu erkunden.

> **Hinweis** Wenn Sie ein neuer Kunde von NetScaler Console ohne NetScaler Console-Lizenz sind, ist Ihr Citrix-Dienstkonto standardmäßig ein Express-Konto. Weitere Informationen zur Kontoberechtigung für NetScaler Console finden Sie unter NetScaler Console-Ressourcen mithilfe des Express-Kontos verwalten .

Integrieren NetScaler-Instanzen mithilfe eines externen Agenten

Sie können externes agentenbasiertes Onboarding verwenden, wenn Sie die gepoolte Lizenzierung oder die komplette Analytics-Suite in NetScaler Console verwenden möchten oder beide die gepoolte Lizenzierung und die komplette Analytics-Suite verwenden möchten.



Führen Sie hierzu die folgenden Schritte aus:

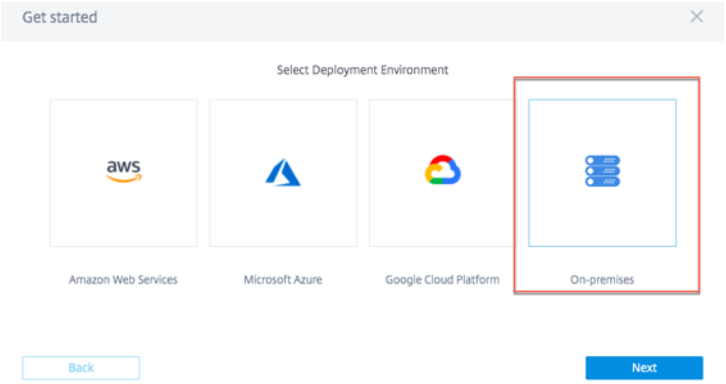
1. Wählen Sie ein Geräteprofil aus.

   > **Hinweis** Aus Sicherheitsgründen können Sie die Standard-NetScaler-Anmeldeinformationen (nsroot/nsroot) nicht für das Onboarding verwenden.

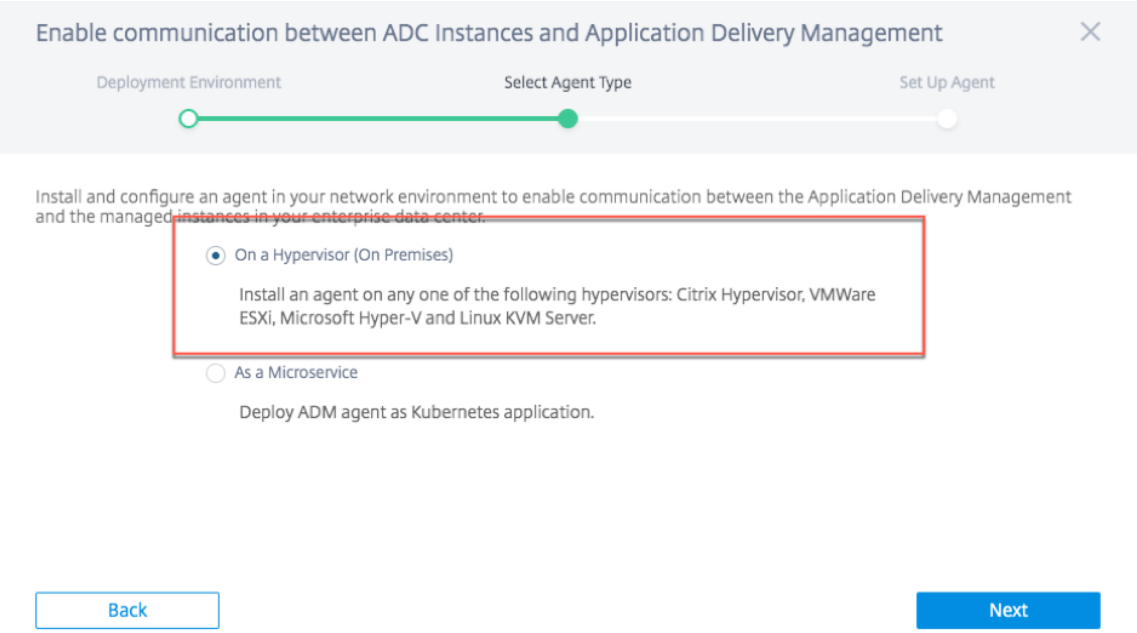
2. Wählen Sie einen externen Agent aus und klicken Sie auf **Neuen Agent einrichten**.
3. Wählen Sie eine der folgenden Umgebungen aus:

   - Amazon Web Services
   - Microsoft Azure
   - Google Cloud Platform
   - On-Premises

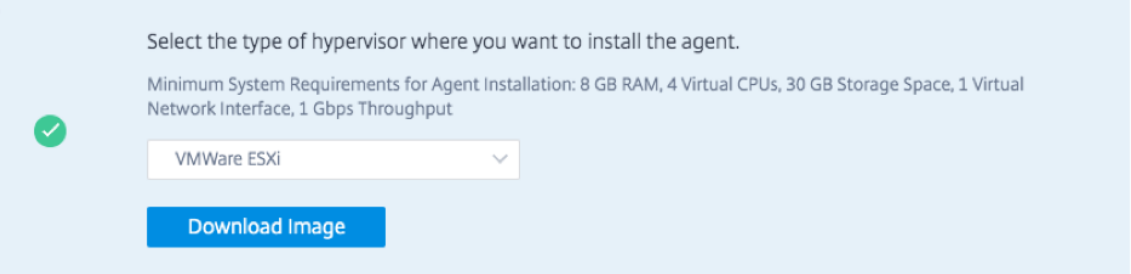
Installieren Sie einen Agent auf Ihrem on-premises Hypervisor Wenn Sie **On-Premises**auswählen, können Sie den Agent auf den folgenden Hypervisoren installieren: Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V, Linux KVM Server.



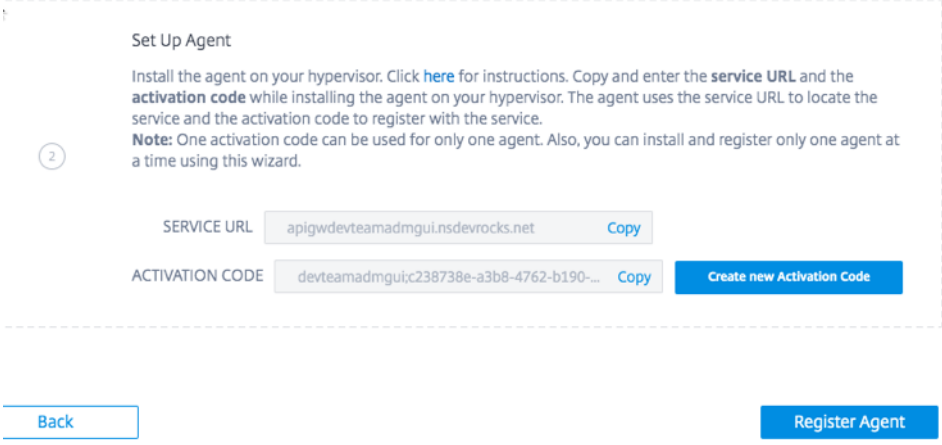
1. Wählen Sie **On a Hypervisor (On Premises)** aus und klicken Sie auf **Weiter**.



2. Wählen Sie den Hypervisortyp aus und laden Sie das Image herunter, zum Beispiel VMware ESXi.

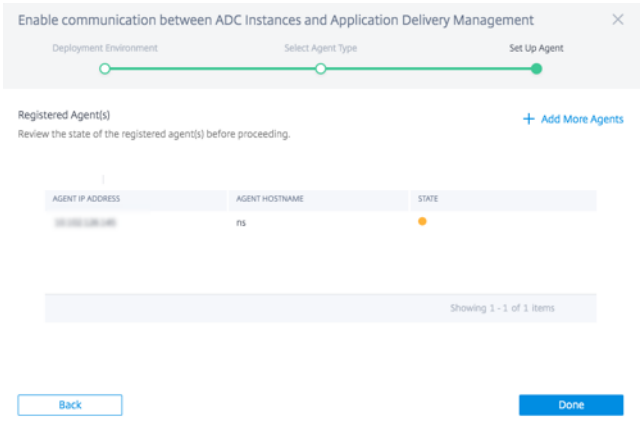


3. Verwenden Sie die Dienst-URL und den Aktivierungscode, um den Agent zu konfigurieren.

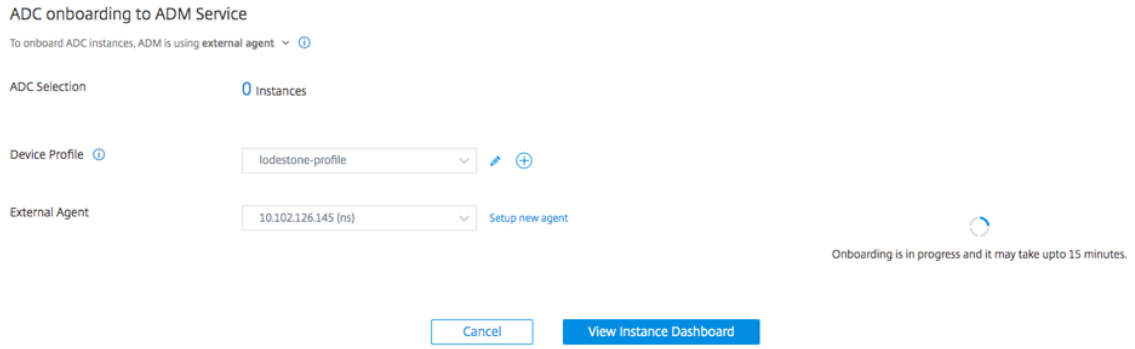


Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren. Eine ausführliche Anleitung zur Installation eines Agents auf Ihrem on-premises Hypervisor finden Sie unter Lokales Installieren eines NetScaler Agents

4. Klicken Sie auf **Agent registrieren**. Wenn Sie fertig sind, klicken Sie auf **Fertig** , um zur NetScaler Onboarding NetScaler Console-Seite zurückzukehren.



5. Klicken Sie auf **Onboarding starten**. Nachdem Sie alle Ihre Instanzen integriert haben, klicken Sie auf Instanz-Dashboard **anzeigen, um zum Dashboard** der NetScaler Console-Instanzverwaltungs-Benutzeroberfläche zu wechseln und die verschiedenen Funktionen zu erkunden.



Installieren eines Agents in einer öffentlichen Cloud

Sie können den Agent in einer der folgenden Cloud-Umgebungen installieren:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

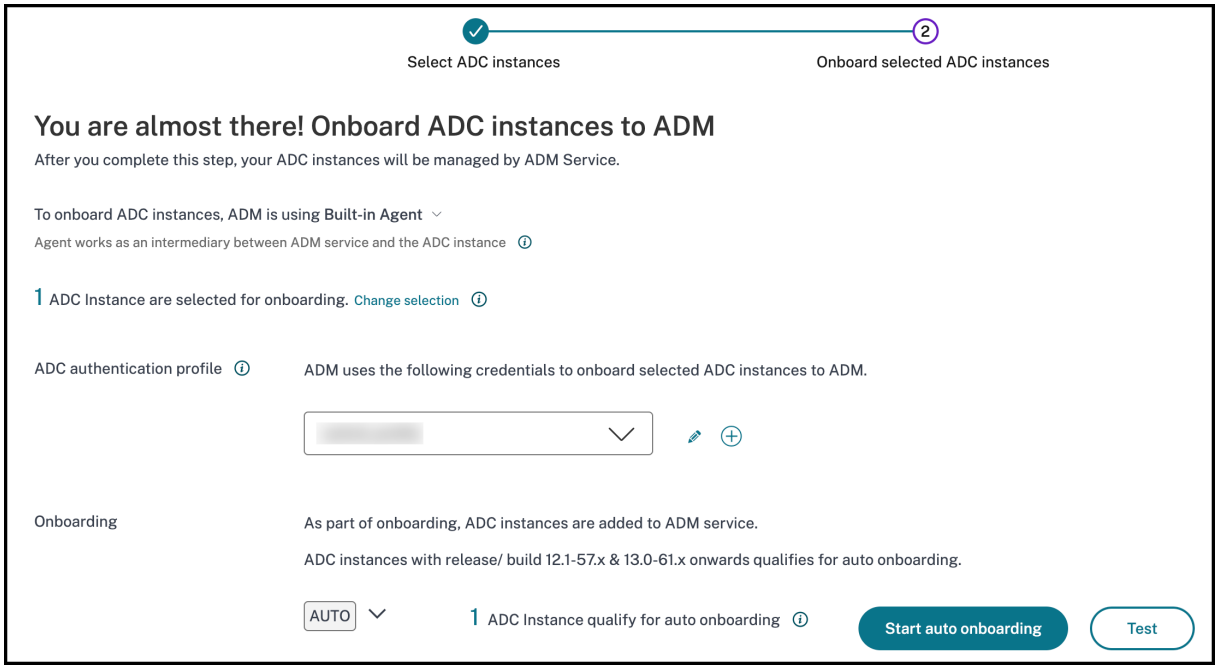
Weitere Informationen finden Sie in den folgenden Dokumenten:

- Installieren Sie einen Agent in der Microsoft Azure Cloud
- Installieren Sie einen Agenten auf AWS
- Agent auf der GCP installieren

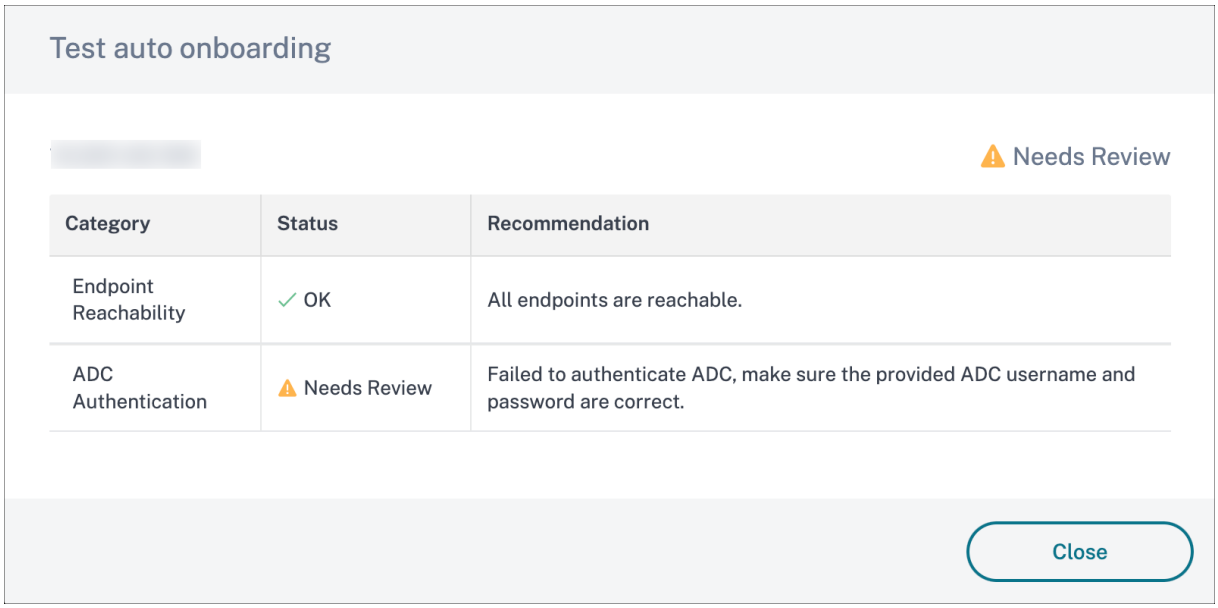
Testen Sie die Onboarding-Bereitschaft von NetScaler-Instanzen

September 2, 2024

Wenn Sie eine NetScaler-Instanz in die NetScaler Console einbinden möchten, können Sie testen, ob die Instanzen für das Onboarding bereit sind. Der Testlaufstatus zeigt an, ob die Instanzen bereit sind oder überprüft werden müssen.



Klicken Sie auf **Test**, um den Diagnosetest zu starten. Auf der Seite „**Automatisches Onboarding testen** “werden die Problemkategorie, der Status und die Empfehlung angezeigt.



Weitere Informationen finden Sie unter Anzeigen von NetScaler-Diagnoseinformationen in der NetScaler Console-GUI .

Wenn der NetScaler-Testlaufstatus den Status „ Überprüfung **erforderlich** “hat, dann:

- Überprüfen Sie die NetScaler-Anmeldeinformationen im Geräteprofil.
- Die folgenden Endpunkte sind nicht erreichbar:
  - `adm.cloud.com`
  - `agent.adm.cloud.com`
  - `trust.citrixnetworkapi.net`
  - `download.citrixnetworkapi.net`

Wenn beim Ausführen des Tests auf Onboarding-Bereitschaft Probleme auftreten, finden Sie unter Fehlerbehebung Empfehlungen.

E-Mail-Einstellungen

January 26, 2024

Der NetScaler Console-Dienst ermöglicht das Onboarding von NetScaler-Instanzen mithilfe des auf Advisory Concole Connect basierenden Low-Touch-Onboarding-Workflows. Im Rahmen dieses Workflows erhalten Kunden produktinitiierte E-Mails vom NetScaler Console-Dienst . Sie können die E-Mail-Benachrichtigungen, die Sie im Rahmen des auf Advisory Console Connect basierenden Low-Touch-Onboarding-Workflows erhalten, aktivieren oder deaktivieren. Sie können die E-Mail-Benachrichtigungen auf folgende Weise konfigurieren und verwalten:

- **E-Mails für alle Admins aktivieren** —Sie können die E-Mails für alle Admins in Ihrer Organisation aktivieren. Standardmäßig sind die E-Mails für alle Administratoren in der Organisation aktiviert.
- **E-Mails für ausgewählte Administratoren aktivieren/deaktivieren** - Sie können die E-Mail-Einstellungen so anpassen, dass nur bestimmte Administratoren in der Organisation E-Mails erhalten und die anderen Administratoren nicht.
- **E-Mails für alle Administratoren deaktivieren**- Sie können die E-Mails für alle Administratoren in Ihrer Organisation deaktivieren und beenden.

E-Mail-Einstellungen konfigurieren

Sie können die E-Mail-Einstellungen konfigurieren und die E-Mails aktivieren oder deaktivieren, die Sie im Rahmen des auf Console Advisory Connect basierenden Low-Touch-Onboarding-Workflows erhalten. So konfigurieren Sie die **E-Mail-Einstellungen**:

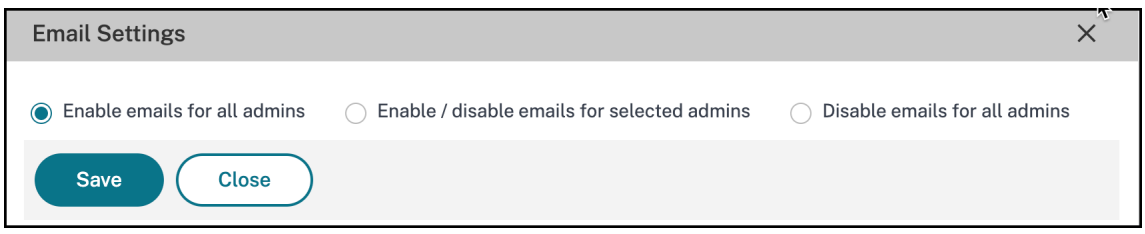
1. Klicken Sie in der vom Produkt initiierten E-Mail auf **Onboard to ADM Service** . Die Seite **Citrix Cloud** wird angezeigt.
2. Auf der **Citrix Cloud-Anmeldeseite** :
   - Wenn Sie bereits Kunde von Citrix Cloud sind, melden Sie sich mit Ihren Anmeldeinformationen von Citrix.com, My Citrix oder CitrixCloud bei Citrix Cloudan.
   - Wenn Sie noch kein Citrix Cloud-Kunde sind, melden Sie sich bei Citrix Cloud an. Weitere Informationen finden Sie unter Registrieren für Citrix Cloud.

     > **Hinweis:**
     >
     > Wenn Sie Teil mehrerer Org-IDs sind und sich eine der Org-IDs in Citrix Cloud befindet, melden Sie sich mit Ihren vorhandenen Anmeldeinformationen an.

   Die NetScaler Console-Landingpage wird angezeigt und bietet Ihnen einen Überblick über NetScaler Console und ihre Vorteile.
3. Klicken Sie auf der NetScaler Console-Landingpage auf **Weiter**.

   Die Seite **Insights on your NetScaler and Gateway instances** wird angezeigt, auf der Sie Einblicke in Ihre gesamte NetScaler-Infrastruktur mit Empfehlungen erhalten.
4. Klicken Sie auf der Seite **Insights on your NetScaler and Gateway instances** auf **Weiter**.

   Die Seite **NetScaler- und Gateway-Instances für Onboarding auswählen** wird angezeigt. Dort finden Sie eine Liste der zu integrierenden NetScaler-Instanzen sowie zusätzliche Optionen wie **E-Mail-Einstellungen**.
5. Klicken Sie auf **E-Mail-Einstellungen**. Der Bereich **E-Mail-Einstellungen** wird angezeigt.

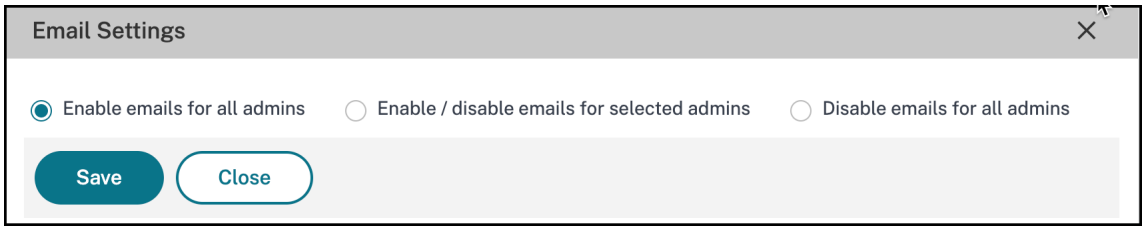
   Sie können jetzt die E-Mail-Einstellungen so konfigurieren, dass E-Mails aktiviert oder deaktiviert werden.

> **Hinweis:**
>
> Wenn Sie nur eine NetScaler-Instanz eingebunden haben, erhalten Sie diese E-Mails nicht.

Wenn Sie sich bereits auf der NetScaler Console-GUI befinden und die E-Mail-Einstellungen konfigurieren möchten:

1. Navigieren Sie in der NetScaler Console GUI zu **Infrastruktur > Instanzen**, und klicken Sie dann auf **NetScaler**. Die Seite **NetScaler** wird angezeigt.
2. Klicken Sie auf der Seite **NetScaler** auf **Asset Inventory**.

   Die Seite **NetScaler- und Gateway-Instanzen für Onboarding auswählen** wird angezeigt. Sie enthält eine Liste der NetScaler-Instanzen, die integriert sind, sowie zusätzliche Optionen wie E-**Mail-Einstellungen**.
3. Klicken Sie auf **E-Mail-Einstellungen**. Der Bereich **E-Mail-Einstellungen** wird angezeigt.



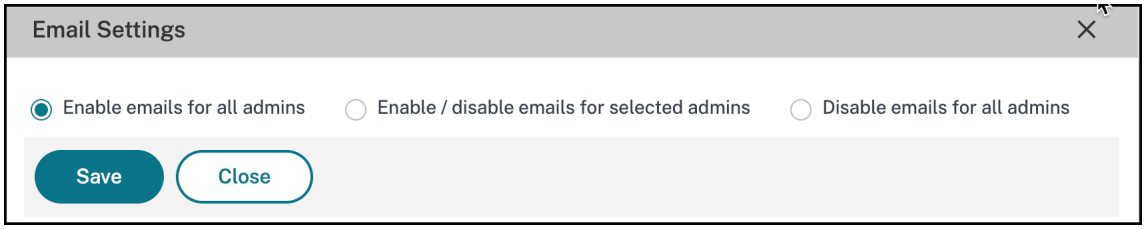
   Sie können jetzt die E-Mail-Einstellungen so konfigurieren, dass E-Mails aktiviert oder deaktiviert werden.

E-Mails für alle Admins aktivieren

Standardmäßig sind die E-Mails für alle Administratoren in der Organisation aktiviert.

Um die E-Mail-Benachrichtigungen als Teil des Console Advisory Connect-basierten Workflows zu aktivieren oder zu abonnieren:

1. Wählen Sie im Bereich **E-Mail-Einstellungen** die Option **E-Mails für alle Administratoren aktivieren** aus.



2. Klicken Sie auf **Speichern** und **Schließen**.

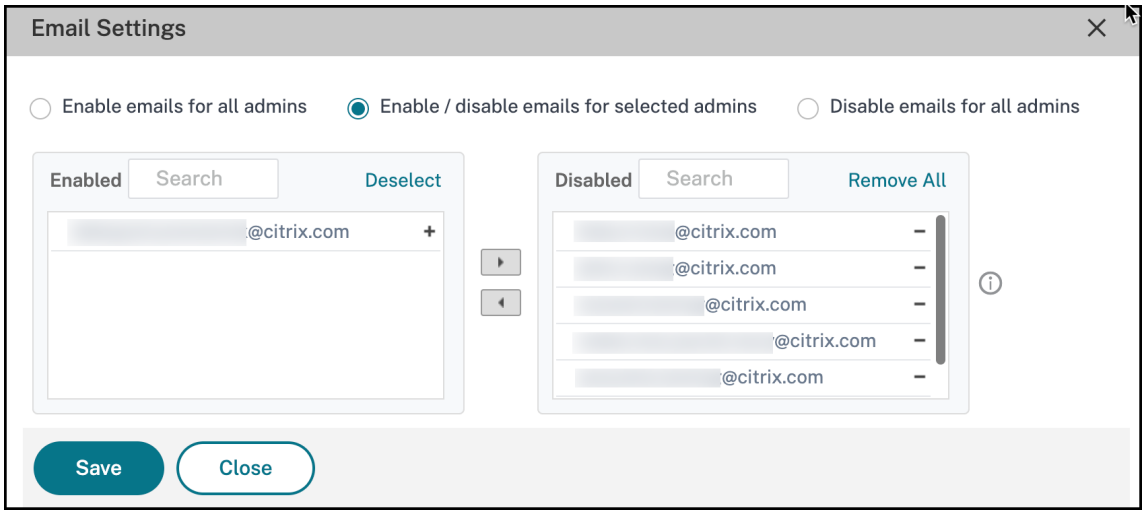
   Alle Administratoren in der Organisation sind jetzt abonniert und erhalten im Rahmen des auf Console Advisory Connect basierenden Workflows E-Mail-Benachrichtigungen.

Aktivieren/Deaktivieren von E-Mails für bestimmte Admins in der Organisation

Sie können die E-Mail-Einstellungen so anpassen, dass nur bestimmte Administratoren in der Organisation E-Mails erhalten. Sie sehen links die Liste der Administratoren, für die die E-Mails aktiviert sind, und die Liste der Administratoren, für die die E-Mails deaktiviert sind, auf der rechten Seite.

So deaktivieren Sie E-Mails für bestimmte Administratoren in der Organisation:

1. Suchen Sie die Admin-E-Mail-Adresse in der Liste **Aktiviert** .
2. Klicken Sie auf die Schaltfläche Hinzufügen (**+**).



   Sie sehen, dass die Admin-E-Mail-Adresse zur Liste der **Deaktivierten** hinzugefügt wurde.

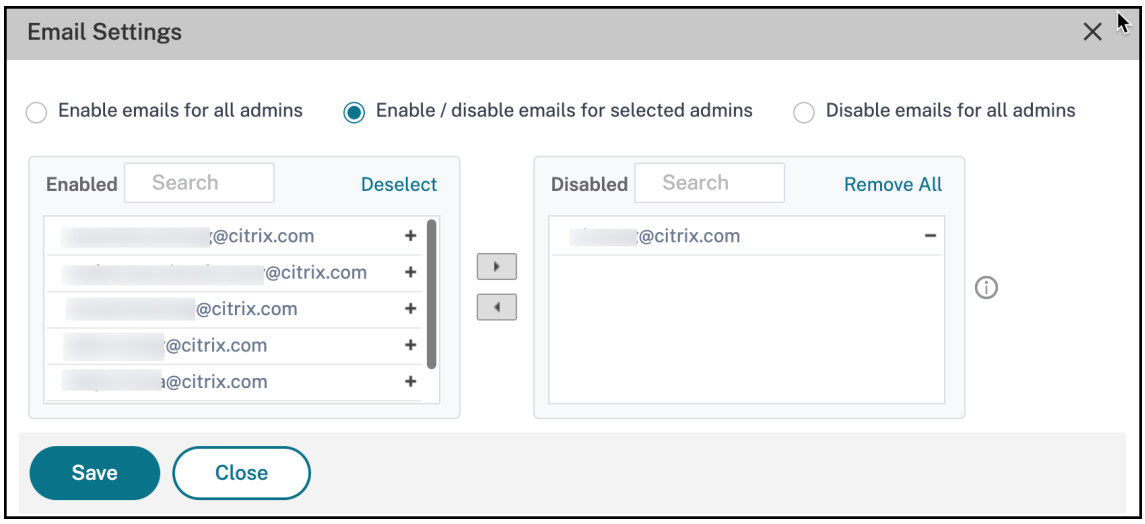
3. Klicken Sie auf **Speichern** und **Schließen**.

   Der Administrator hat sich jetzt abgemeldet, um im Rahmen des Console Advisory Connect-basierten Workflows keine E-Mail-Benachrichtigungen zu erhalten.

   > **Hinweis:**
   >
   > Wenn Sie E-Mails für mehrere Administratoren deaktivieren möchten, wählen Sie alle ihre E-Mail-IDs in der E-Mail-Liste **Aktiviert** aus und klicken Sie auf die Schaltfläche Hinzufügen (**+**), um die E-Mail-IDs zur Liste **Deaktiviert** hinzuzufügen. Klicken Sie auf **Speichern** und **Schließen**.

Wenn Sie zuvor E-Mails für bestimmte oder alle Administratoren in Ihrer Organisation deaktiviert haben, können Sie E-Mails für alle Administratoren aktivieren. So aktivieren Sie E-Mails für bestimmte Administratoren in der Organisation:

1. Suchen Sie die E-Mail-Adresse des Administrators in der Liste **Deaktiviert** .
2. Klicken Sie auf die Schaltfläche Entfernen (-). Sie sehen, dass die E-Mail-Adresse des Administrators aus der Liste der **Deaktivierten** entfernt wurde.



3. Klicken Sie auf **Speichern** und **Schließen**.

   Der Administrator erhält nun E-Mails im Zusammenhang mit dem Onboarding. Der Administrator ist jetzt abonniert, um E-Mail-Benachrichtigungen zu erhalten.

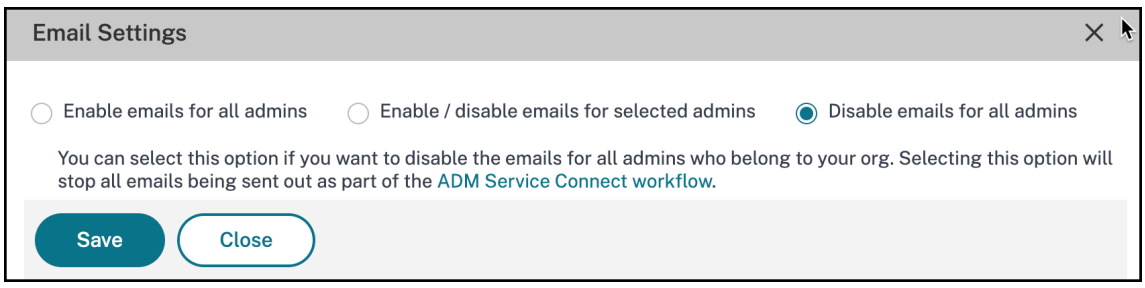
   > **Hinweis:**
   >
   > Wenn Sie E-Mails für mehrere Administratoren aktivieren möchten, wählen Sie alle ihre E-Mail-IDs in der Liste **Deaktivierte** E-Mails aus und klicken Sie auf die Schaltfläche zum Entfernen (**-**), um die E-Mail-IDs zur Liste **Aktiviert** hinzuzufügen. Klicken Sie auf **Speichern** und **Schließen**.

E-Mails für alle Admins deaktivieren

Sie können diese Option auswählen, wenn Sie die E-Mails für alle Administratoren, die zu Ihrer Organisation gehören, deaktivieren oder beenden möchten.

So deaktivieren oder kündigen Sie den Empfang von E-Mails ab:

1. Wählen Sie im Bereich **E-Mail-Einstellungen** die Option **E-Mails für alle Administratoren deaktivieren**aus.



2. Klicken Sie auf **Speichern** und **Schließen**.

Alle Administratoren in der Organisation sind jetzt abgemeldet und erhalten keine E-Mail-Benachrichtigungen.

Beheben Sie Probleme mithilfe des Diagnosetools oder der NetScaler Console-GUI

January 26, 2024

> Hinweis
>
> Das Diagnosetool gilt nur für die NetScaler-Instanzen, die mithilfe des auf Console Advisory Connect basierenden Low-Touch-Onboarding eingebunden wurden oder noch eingebunden werden sollen.
>
> Weitere Informationen finden Sie unter Low-Touch-Onboarding von NetScaler-Instanzen mithilfe von NetScaler Console Connect .

Wenn Sie eine NetScaler-Instanz in die NetScaler Console einbinden, treten möglicherweise einige Probleme auf, die ein erfolgreiches Onboarding der NetScaler-Instanz verhindern. Als Administrator müssen Sie den Grund für den Fehler beim Onboarding kennen. Sie können Diagnoseprüfungen mit dem Diagnosetool durchführen, wenn Sie:

- Probleme beim Auto-Onboarding oder beim skriptbasierten Onboarding
- Sie möchten sicherstellen, dass die NetScaler-Instanz bereit für das Onboarding ist
- Sie möchten Probleme für die bereits integrierten NetScaler-Instanzen analysieren, für die in der NetScaler Console-GUI der Status „Heruntergefahren“angezeigt wird?

Wenn Console Advisory Connect auf der NetScaler-Instanz aktiviert ist, werden die Diagnosedetails automatisch an Citrix gesendet und Sie können Details in der NetScaler Console-GUI anzeigen. Wenn Console Advisory Connect nicht aktiviert ist, können Sie das Diagnosetool manuell verwenden .

Verwenden Sie das Diagnosetool manuell

Das Diagnosetool ist im Rahmen des `mastools`-Upgrades (13.1-2.x oder höher) verfügbar und kann unter `/var/mastools/scripts` abgerufen werden. Sie können die `mastools`Version überprüfen, indem Sie den `cat /var/mastools/version.txt`Befehl in der NetScaler-Instanz ausführen.

So führen Sie das Diagnosetool aus:

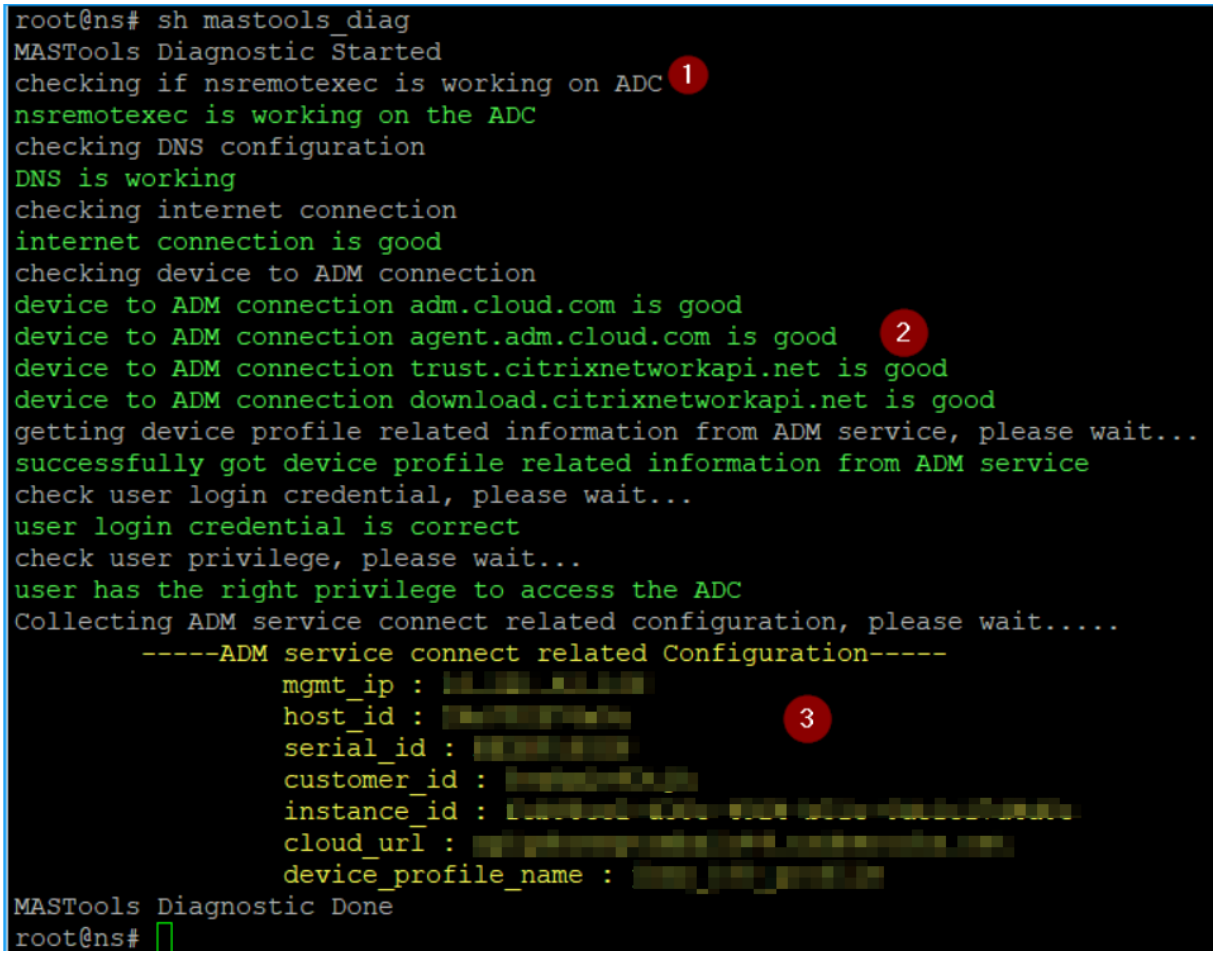
1. Melden Sie sich mit einem SSH-Client bei der NetScaler-Instanz an.
2. Geben Sie shell ein und drücken Sie die Eingabetaste, um in den Bash-Modus zu wechseln.
3. Geben Sie `cd /var/mastools/scripts` ein.
4. Geben Sie `sh mastools_diag` ein.

Das Tool wird gestartet und zeigt die Ergebnisse für die folgenden Diagnoseprüfungen an:

- **nscli**
- **DNS-Konfiguration**
- **Internetverbindung**
- **Verbindung zwischen Instanz und ADM**
- **Benutzerberechtigung**

Wenn die Probleme auch nach der Fehlerbehebung weiterhin bestehen, können Sie sich an den Support wenden. Wenn Sie den Support kontaktieren, müssen Sie die Konfigurationsinformationen angeben, die nach dem Ausführen des Diagnosetools angezeigt werden.

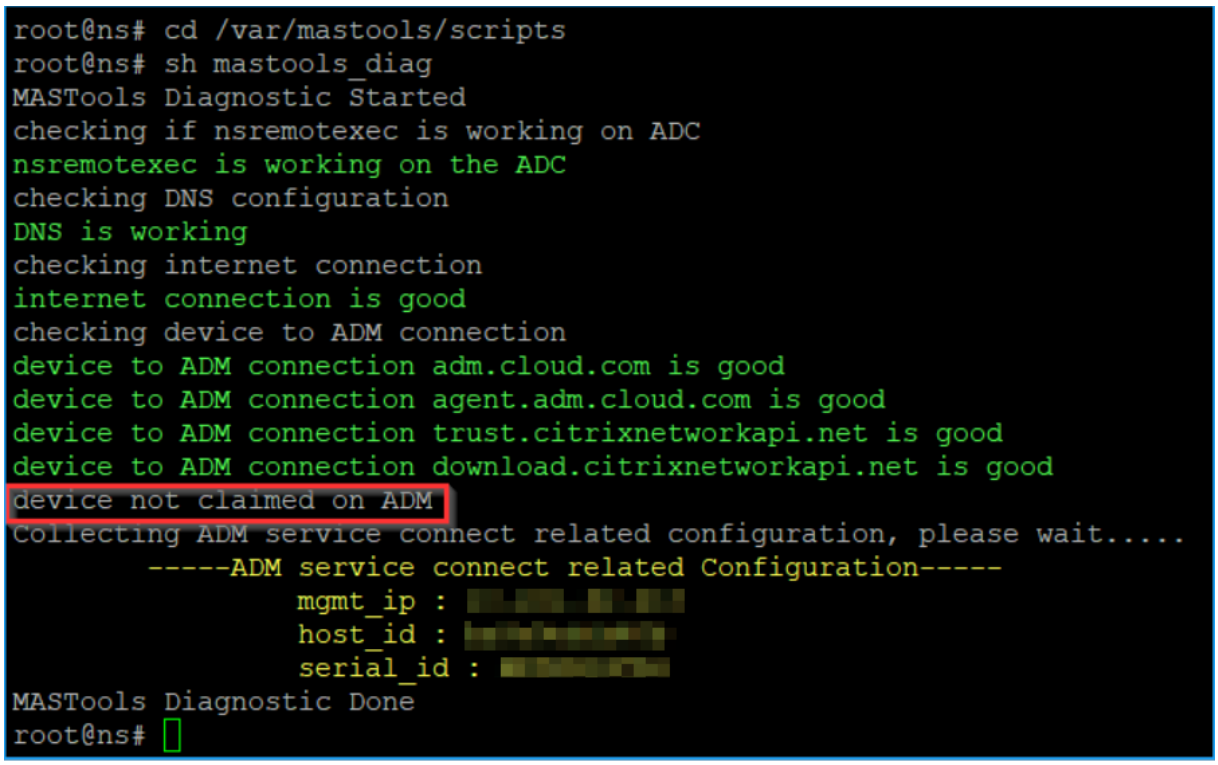
Das Folgende ist ein Beispiel für Diagnoseergebnisse für eine NetScaler-Instanz, die keine Probleme hat:



- **1** —Zeigt die Art der Diagnoseprüfung an
- **2** —Zeigt die Ergebnisse der Diagnoseprüfung entweder grün oder rot an. Grün bedeutet, dass das Ergebnis erfolgreich ist, und Rot zeigt an, dass das Ergebnis nicht erfolgreich ist.
- **3**—Zeigt die NetScaler Console-Konfigurationsinformationen bei jeder Ausführung des Diagnosetools gelb an. Wenn Sie den NetScaler-Support kontaktieren möchten, müssen Sie diese Informationen angeben.

Überprüfen Sie die Bereitschaft der NetScaler-Instanz für das Onboarding mithilfe des Diagnosetools

Bevor Sie die NetScaler-Instanz in die NetScaler Console einbinden, können Sie die Bereitschaft der NetScaler-Instanz überprüfen, indem Sie das Diagnosetool auf der NetScaler-Instanz ausführen. Wenn die NetScaler-Instanz keine Probleme hat und bereit für das Onboarding ist, zeigt das Tool die **ADM-Nachricht an, dass das Gerät nicht beansprucht wurde** .



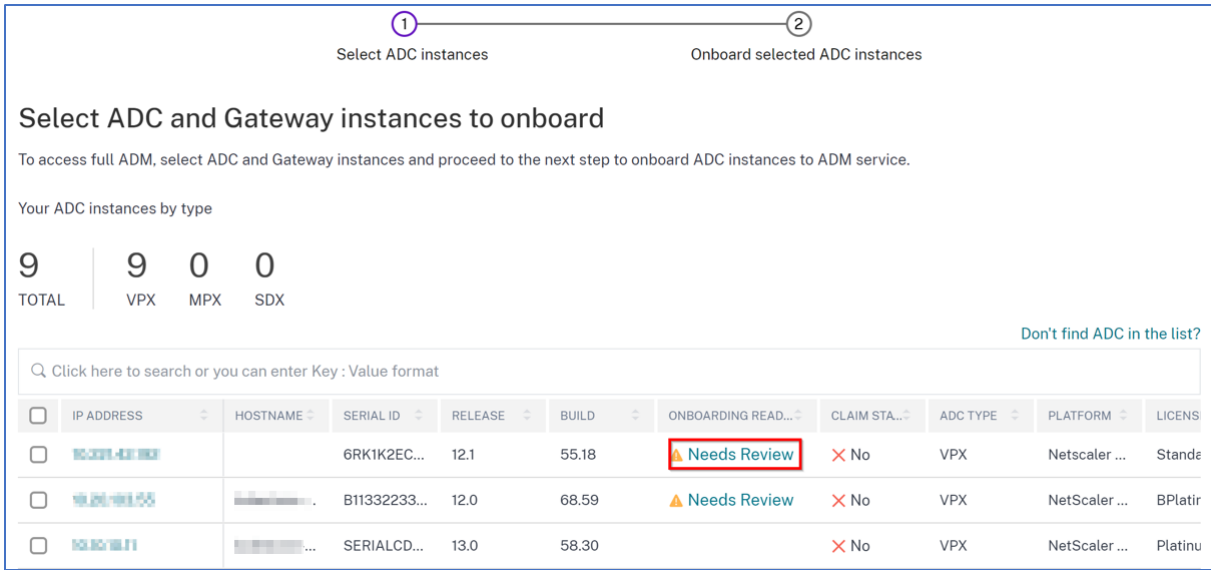
NetScaler-Diagnoseinformationen in der NetScaler Console-GUI anzeigen

Navigieren Sie zu **Infrastruktur > Instances > NetScaler** und klicken Sie auf **Asset Inventory** , um die neu hinzugefügte Option **Onboarding Readiness** anzuzeigen, die den Onboarding-Bereitschaftsstatus der NetScaler-Instanz wie **Needs Review** oder **OK** anzeigt.

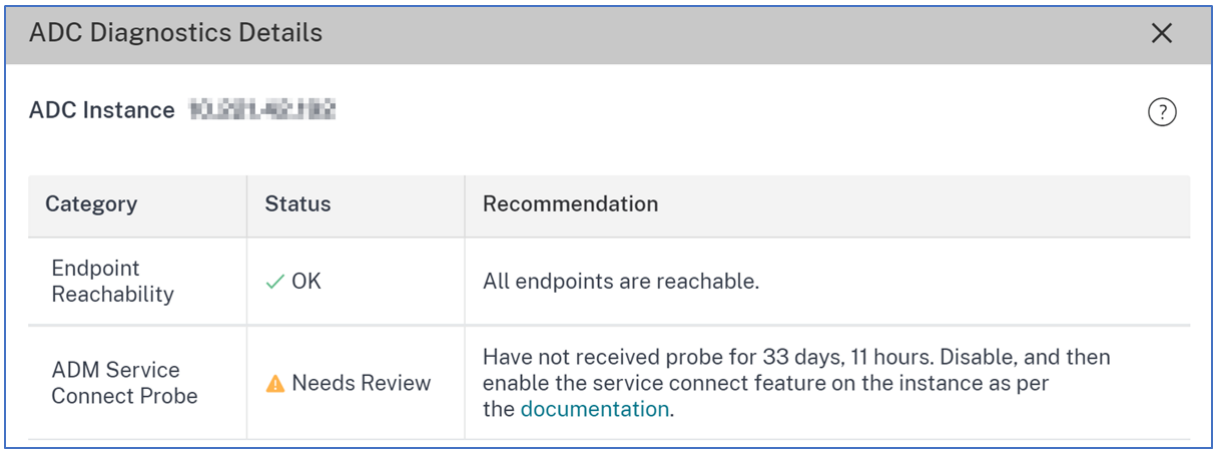
- **Muss überprüft werden**. Die NetScaler-Instanz weist Probleme auf, die behoben werden müssen.
- **OKAY**. Die NetScaler-Instanz ist bereit für das Onboarding.

> **Hinweis:**
>
> Wenn das Feld **Onboarding Readiness** leer erscheint, bedeutet das, dass die NetScaler-Instanz nicht mit dem neuesten Image läuft, das Diagnoseunterstützung bietet.

Wenn bei der NetScaler-Instanz Probleme auftreten, wird die Option „ **Überprüfung erforderlich** “angezeigt, und Sie können klicken, um weitere Details anzuzeigen.



Nachdem Sie auf Überprüfung **erforderlich** geklickt haben, werden auf der Seite **NetScaler Diagnostics Details** die Problemdetails angezeigt.



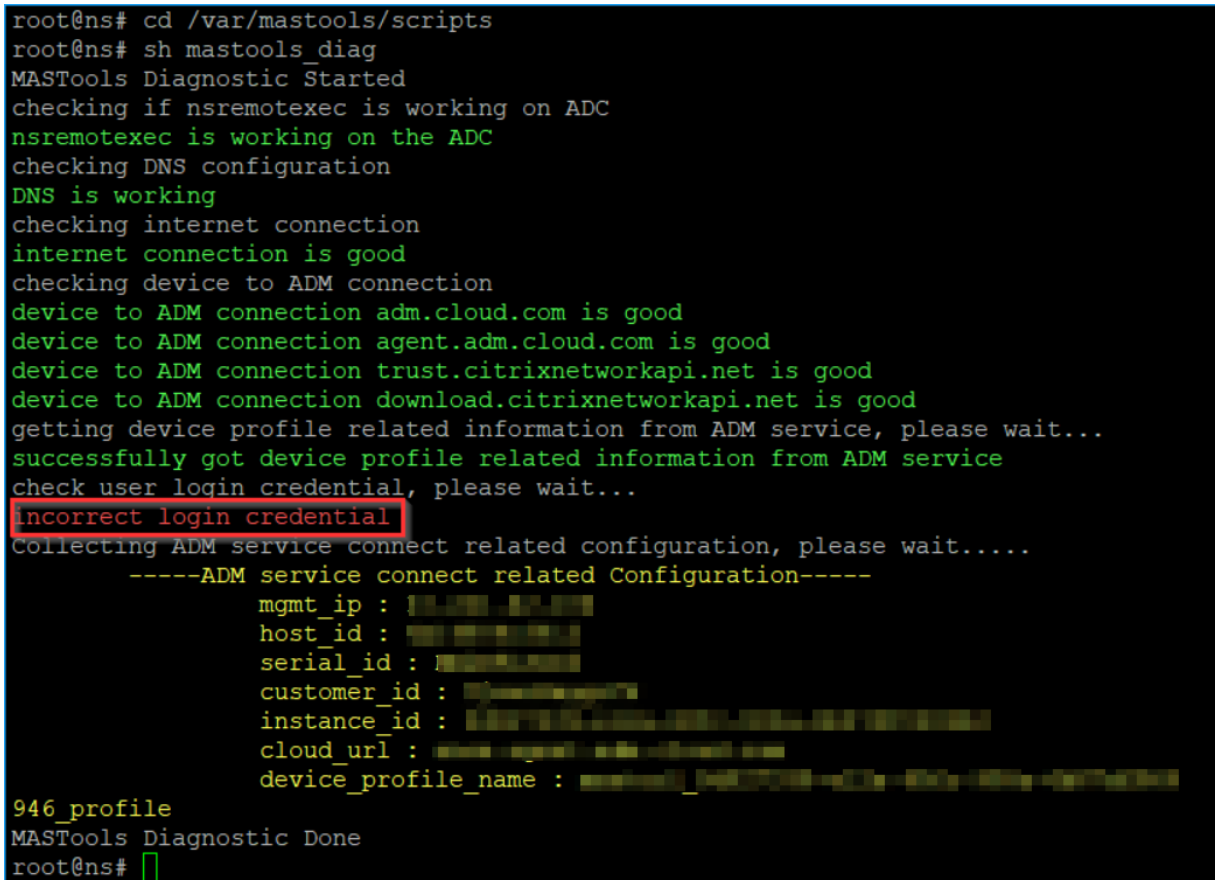
- **Kategorie**. Stellt die Problemkategorie bereit.
- **Status**. Zeigt den Problemstatus an, z. B. **Überprüfung erforderlich**, **OK**oder **Nicht zutreffend**.
- **Empfehlung**. Stellt die erforderliche Empfehlung zur Behebung des Problems bereit.

Nachdem Sie das Problem behoben haben, wird der Status in der Onboarding-Bereitschaft auf **OK**geändert.

Problembehandlung

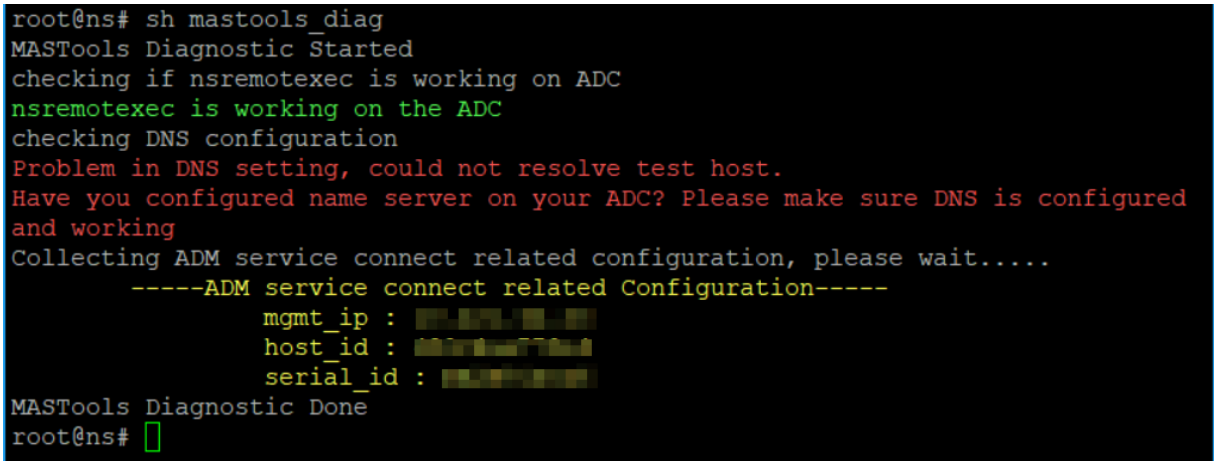
Im Folgenden sind einige der Probleme mit der NetScaler-Instanz und deren Schritte zur Problembehandlung aufgeführt:

Ungültiger Benutzername oder Kennwort



Problemumgehung: Stellen Sie sicher, dass der im Admin-Profil angegebene Benutzername und das Kennwort korrekt sind. Wenn Sie das NetScaler-Instanzkennwort geändert haben, müssen Sie die Admin-Profile der Instanzen ändern. Weitere Informationen finden Sie unter Ändern des Admin-Profils.

DNS-Konfigurationsfehler



Problemumgehung: Stellen Sie sicher, dass der DNS konfiguriert ist oder die DNS-IP-Adresse gültig ist. Weitere Informationen finden Sie unter DNS-Konfiguration.

Keine Internetverbindung

Problemumgehung: Stellen Sie sicher, dass die Firewalleinstellung den Internetzugang nicht blockiert und der erforderliche Proxy konfiguriert ist.

Keine Verbindung zum NetScaler Console-Endpunkt

** Problemumgehung : Stellen Sie sicher, dass die Firewalleinstellungen überprüft werden und die folgenden NetScaler Console-Endpunkte nicht in der Firewall blockiert sind:

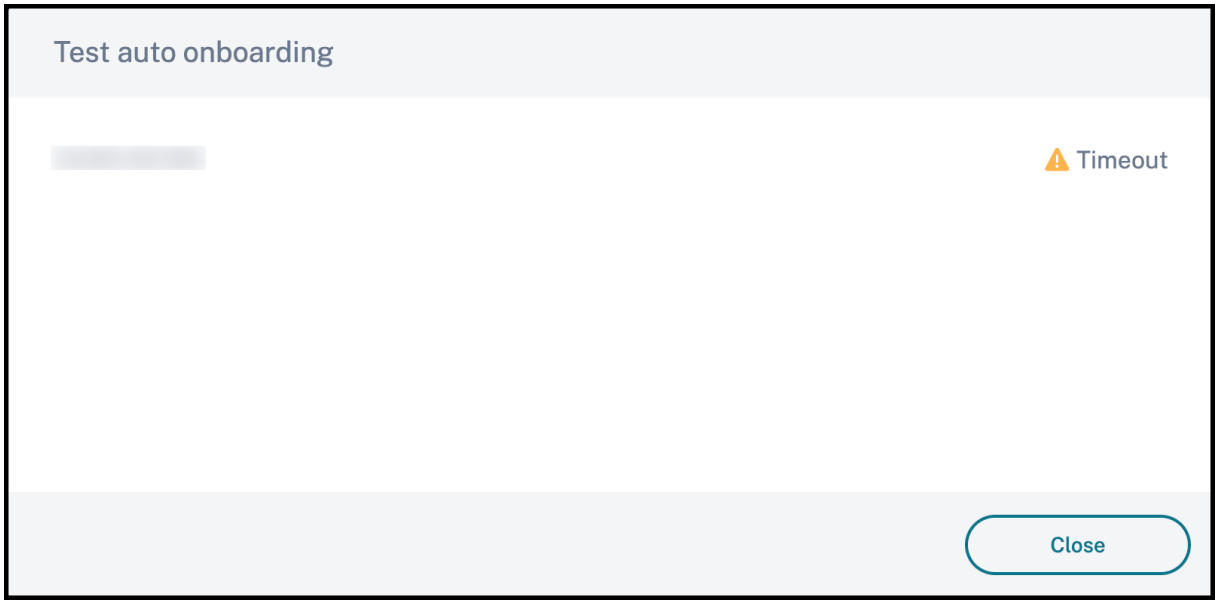
```
ADM_GRP_EP = "adm.cloud.com"

ADM_AGENT_EP = "agent.adm.cloud.com"

ADM_TRUST_EP = "trust.citrixnetworkapi.net"

ADM_DOWNLOAD_EP = "download.citrixnetworkapi.net"
```

Wenn bei den Diagnosetests kein Problem festgestellt wurde und das Problem „Keine Verbindung “weiterhin besteht, notieren Sie sich die Konfigurationsinformationen der NetScaler Console (in gelb verfügbar) und wenden Sie sich an den NetScaler-Support.

Wenn Sie einen Testlauf durchführen, um sicherzustellen, dass die NetScaler-Instanz bereit für das Onboarding ist, treten möglicherweise die folgenden Probleme auf:

Integrierte Zeitüberschreitung für den Trockenlauf

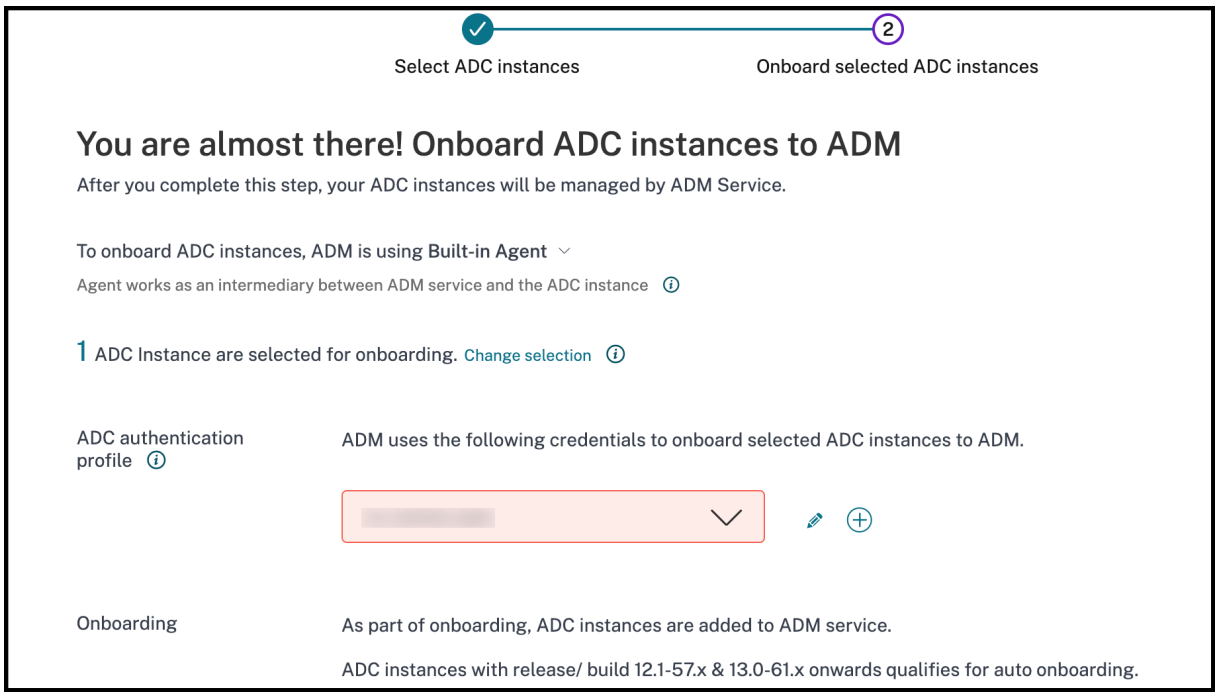
Wenn die Ergebnisse des Probelaufs nicht innerhalb von 5 Minuten abgerufen werden, wird eine Timeout-Meldung angezeigt.



Empfehlung: Es wird empfohlen, zu überprüfen, ob die NetScaler-Instanz mit dem neuesten Image ausgeführt wird, das Diagnoseunterstützung bietet. Außerdem wird in der Tabelle Asset-Auswahl die Spalte Onboarding Readiness leer angezeigt.

Roter Umriss im Dropdownmenü des Geräteprofils

Die NetScaler-Authentifizierung schlägt während des Probelaufs fehl und in der Dropdownliste des Geräteprofils wird ein roter Umriss angezeigt.



Empfehlung: Geben Sie die NetScaler-Benutzeradministrator-Anmeldeinformationen erneut ein, erstellen Sie das Geräteprofil und klicken Sie auf Testen, um den Probelauf erneut auszuführen.

Übergang von einem integrierten Agent zu einem externen Agent

January 26, 2024

Möglicherweise haben Sie mit der NetScaler Console nur zur Verwaltung und Überwachung begonnen, und später möchten Sie möglicherweise andere Funktionen wie gepoolte Lizenzierung und Analysen verwenden. Dazu müssen Sie vom integrierten Agenten zu einem externen Agenten wechseln.

Der integrierte Agent unterstützt nur Verwaltungs- und Überwachungsfunktionen. Für andere NetScaler Console-Funktionen wie gepoolte Lizenzierung und Analysen benötigen Sie einen externen Agenten. Dieses Dokument behandelt die Schritte für den Übergang von einem vorhandenen in NetScaler Console integrierten Agenten zu einem externen Hypervisor-basierten Agenten.

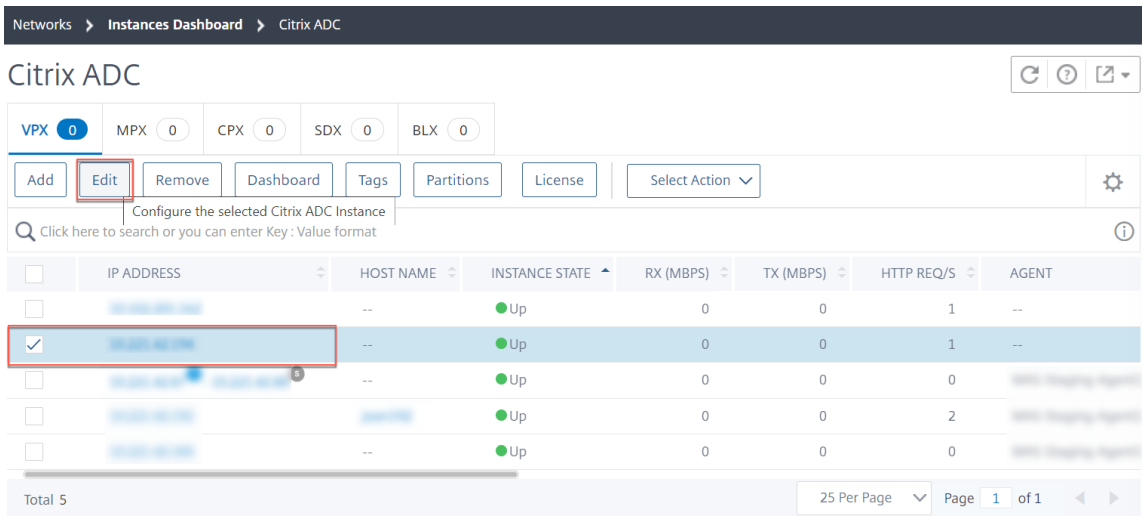
Vorbereitung

Installieren Sie einen externen Agent, bevor Sie mit dem Umstieg beginnen. Folgen Sie den Anweisungen im Thema on-premises Installation eines NetScaler Agents .

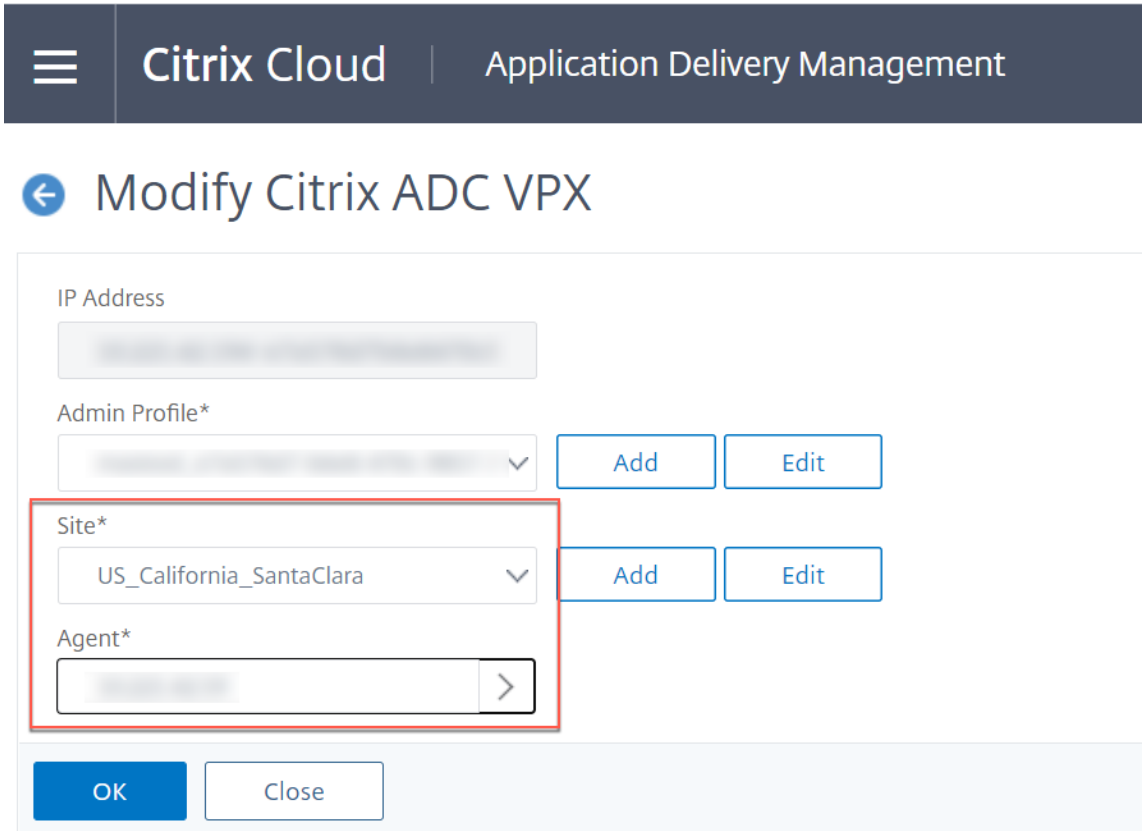
Übergang von einem integrierten Agent zu einem externen Agent

Befolgen Sie diese Schritte, um von einem integrierten Agent zu einem externen Agent zu wechseln:

1. Wählen Sie in der NetScaler Console-GUI unter **Infrastructure > Instances Dashboard > NetScaler** die NetScaler-Instanz aus und klicken Sie auf **Bearbeiten**.



2. Wählen Sie die Site und den Agent aus und klicken Sie auf **OK**.



3. Wählen Sie die Instanz erneut aus und klicken **Sie auf Aktion auswählen > Wiederentdecken**.

Informationen zum Erstellen einer Site in der NetScaler Console und zum Hinzufügen des Agenten zur Site finden Sie unter Instanzen hinzufügen

SAML als Identitätsanbieter mit NetScaler Console verbinden

January 26, 2024

NetScaler Console unterstützt die Verwendung von SAML (Security Assertion Markup Language) als Identitätsanbieter zur Authentifizierung von Administratoren und Abonnenten, die sich bei ihrer NetScaler Console anmelden. Sie können den SAML 2.0-Anbieter Ihrer Wahl mit Ihrem On-Premises-Active Directory (AD) verwenden.

Bei den meisten SAML-Anbietern können Sie die SAML-Authentifizierung gemäß den Informationen in diesem Artikel einrichten. Wenn Sie die SAML-Authentifizierung mit Ihrem Azure AD verwenden möchten, können Sie die Citrix Cloud-SAML-SSO-App aus der Azure AD-App-Galerie verwenden.

Voraussetzungen

Für die SAML-Authentifizierung mit NetScaler Console gelten die folgenden Anforderungen:

- SAML-Anbieter, der SAML 2.0 unterstützt
- On-Premises-AD-Domäne
- Zwei Cloud Connectors, an einem Ressourcenstandort bereitgestellt und mit Ihrer On-Premises-AD-Domäne verbunden. Die Cloud Connectors werden verwendet, um sicherzustellen, dass Citrix Cloud mit Ihrem Ressourcenstandort kommunizieren kann.
- AD-Integration mit Ihrem SAML-Anbieter.

Cloud Connectors

Sie benötigen mindestens zwei (2) Server, auf denen Sie die Citrix Cloud Connector-Software installieren können. Es wird empfohlen, mindestens zwei Server für die hohe Verfügbarkeit von Cloud Connector zu haben. Die Server müssen die folgenden Anforderungen erfüllen:

- Die unter Technische Daten zu Citrix Cloud Connector beschriebenen Systemanforderungen müssen erfüllt sein.
- Es dürfen keine anderen Komponenten von Citrix installiert sein. Die Server dürfen keine AD-Domänencontroller oder Maschinen sein, die für Ihre Ressourcenstandortinfrastruktur kritisch sind.

- Sie müssen mit der Domäne verbunden sein, in der sich Ihre Ressourcen befinden. Wenn Benutzer auf Ressourcen in mehreren Domänen zugreifen, müssen Sie in jeder Domäne mindestens zwei Cloud Connectors installieren.
- Es muss eine Verbindung zum Netzwerk bestehen, das die Ressourcen abrufen kann, auf die Abonnenten über Citrix Workspace zugreifen.
- Mit dem Internet verbunden.

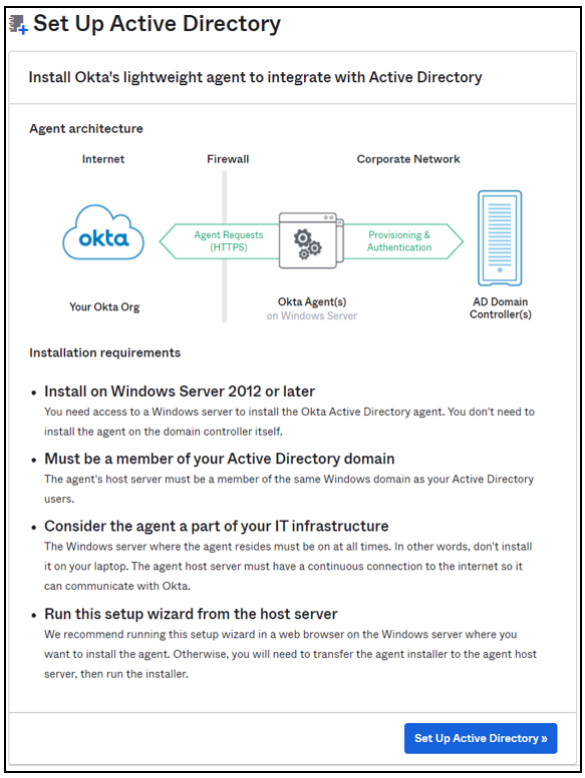
Active Directory

Führen Sie vor dem Konfigurieren der SAML-Authentifizierung die folgenden Aufgaben aus:

- Die Felder Vorname, Nachname und E-Mail sind für die Benutzer in Active Directory erforderlich, um Benutzer in Okta Instance zu importieren.
- Stellen Sie sicher, dass Ihre Workspace-Abonnenten über Benutzerkonten in Active Directory (AD) verfügen. Abonnenten ohne AD-Konten können sich nicht erfolgreich in ihren Workspaces anmelden, wenn die SAML-Authentifizierung konfiguriert ist.
- Stellen Sie sicher, dass die Benutzereigenschaften in den AD-Konten Ihrer Abonnenten gefüllt sind. Citrix Cloud benötigt diese Eigenschaften, um den Benutzerkontext bei der Anmeldung von Abonnenten bei Citrix Workspace zu erfassen. Wenn diese Eigenschaften nicht ausgefüllt sind, können sich Abonnenten nicht anmelden. Zu diesen Eigenschaften gehören:
  - E-Mail-Adresse
  - Anzeigename (optional)
  - Allgemeiner Name
  - SAM-Kontoname
  - Benutzerprinzipalname
  - Objekt-GUID
  - SID
- Verbinden Sie Ihr Active Directory (AD) mit Ihrem Citrix Cloud-Konto, indem Sie Cloud Connectors in Ihrem On-Premises-AD bereitstellen.
- Synchronisieren Sie Ihre AD-Benutzer mit dem SAML-Anbieter. Citrix Cloud benötigt die AD-Benutzerattribute Ihrer Workspace-Abonnenten, damit diese sich erfolgreich anmelden können.

SAML SSO-Konfiguration

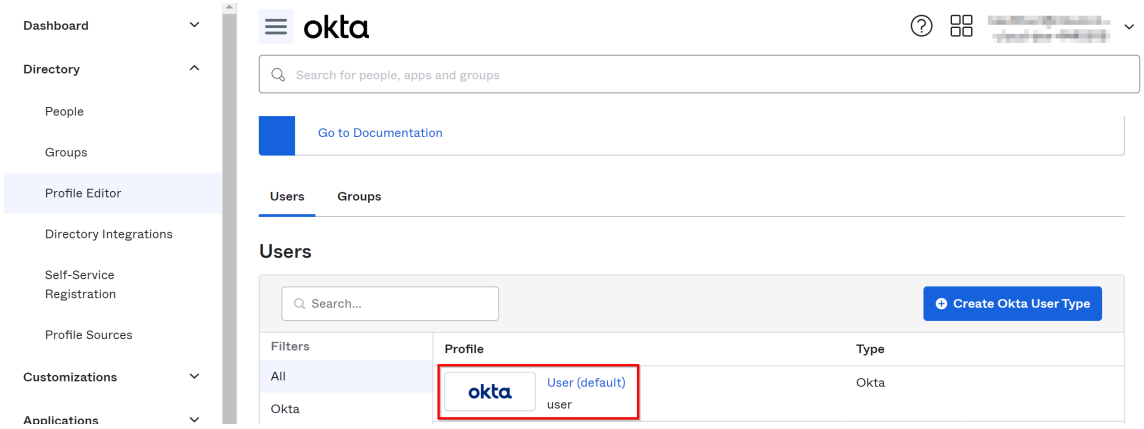
Navigieren Sie in einer Okta-Instanz zu **Verzeichnisintegrationen > Active Directory hinzufügen**.



Für eine erfolgreiche Integration muss der SAML-Identitätsanbieter Citrix Cloud bestimmte Active Directory-Attribute des Benutzers in der SAML-Assertion übergeben. Konkret

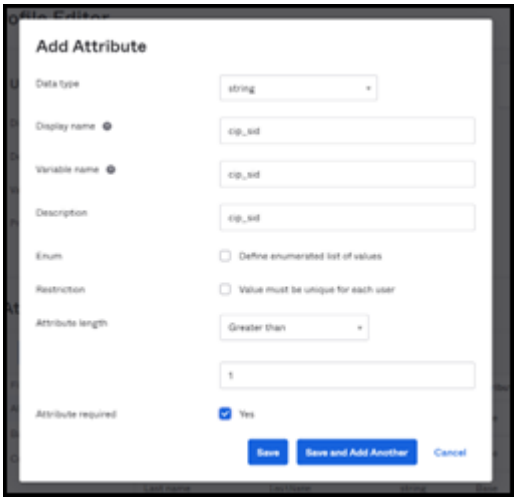
- Sicherheitskennung (SID)
- objectGUID (OID)
- Benutzerprinzipalname (UPN)
- E-Mail (E-Mail)

1. Melden Sie sich mit Administratoranmeldedaten bei Okta an.
2. Wählen Sie **Verzeichnis > Profileditor** und wählen Sie das **Okta-Benutzerprofil (Standard)** aus. Okta zeigt die Profilseite User an.



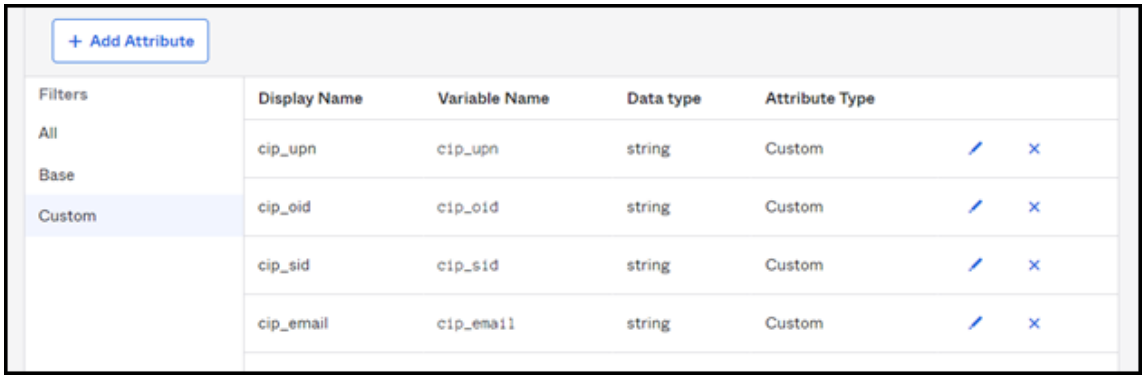
3. Wählen Sie unter **Attribute**die Option **Attribute hinzufügen** aus und fügen Sie die benutzerdefinierten Felder hinzu.

   - `cip_sid`
   - `cip_upn`
   - `cip_oid`
   - `cip_email`



Klicken Sie auf **Speichern und weitere hinzufügen** und wiederholen Sie den Vorgang, um 4 benutzerdefinierte Attribute zu erstellen.

Sie können die folgenden Details anzeigen, nachdem Sie 4 benutzerdefinierte Attribute erstellt haben:

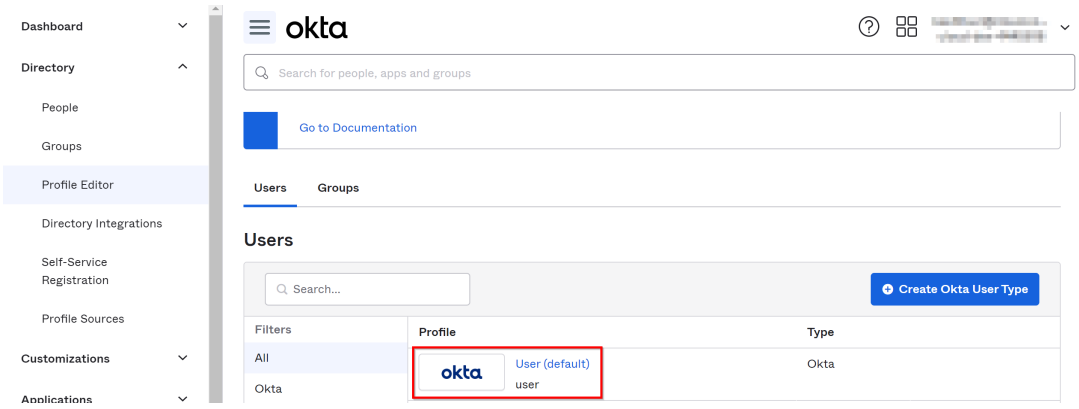


4. Ordnen Sie Active Directory-Attribute den benutzerdefinierten Attributen zu. Wählen Sie unter **Benutzer > Verzeichnisse**das von Ihnen verwendete Active Directory aus.
5. Bearbeiten Sie die Attributzuordnungen:

   a) Navigieren Sie in der Okta-Konsole zu **Verzeichnis > Profileditor**.

   b) Suchen Sie das `active_directory` Profil für Ihr AD. Dieses Profil kann mit dem Format MyDomain User beschriftet werden, wobei MyDomain der Name Ihrer integrierten AD-Domain ist.

   c) Wählen Sie **Mappings** aus. Die Seite **Benutzerprofilzuordnungen** für Ihre AD-Domain wird angezeigt und die Registerkarte für die Zuordnung Ihres AD zu Okta-Benutzern wird ausgewählt.



   d) Ordnen Sie in der Spalte Okta-Benutzerprofil die Active Directory-Attribute den benutzerdefinierten Attributen zu, die Sie erstellt haben:**

      i. Wählen Sie für `cip_email`E-Mail in der Spalte Benutzerprofil für Ihre Domain aus. Bei dieser Auswahl wird die Zuordnung als `appuser.email` angezeigt.

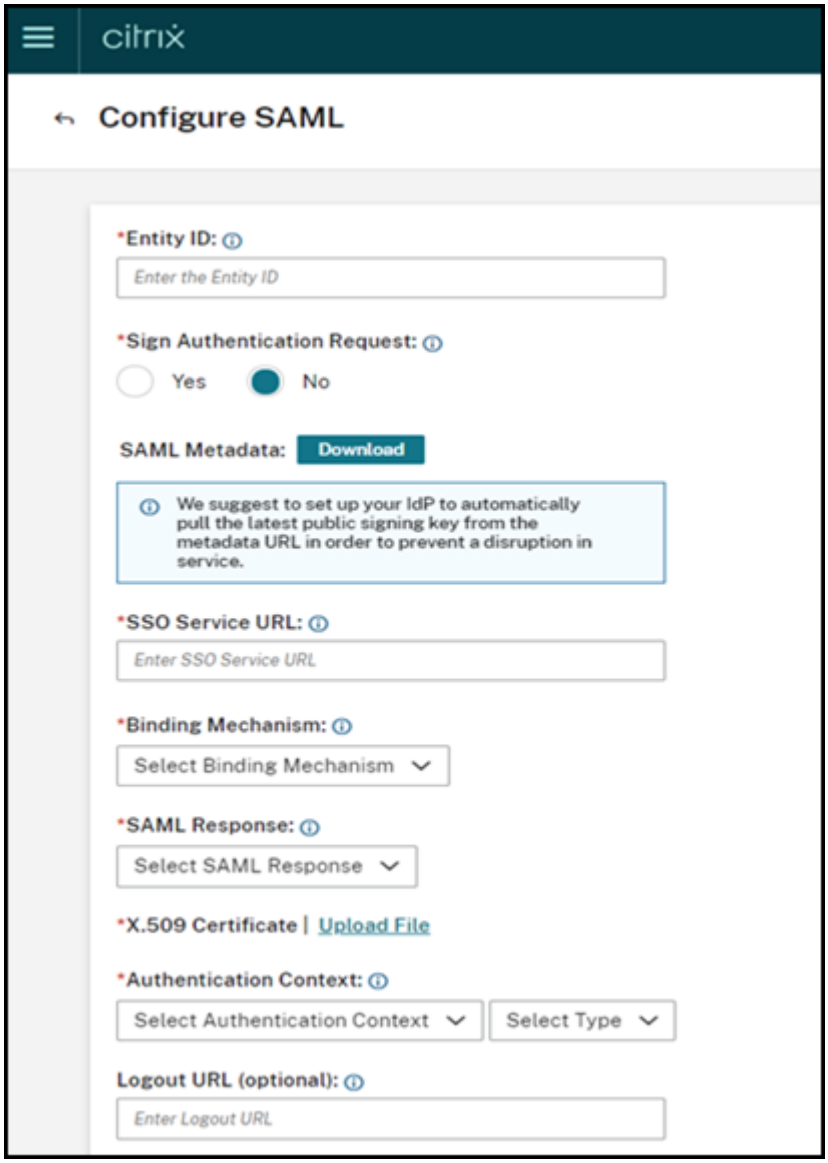
      ii. Wählen Sie für `cip_sid`Ihre Domain in der Spalte Benutzerprofil die Option **objectSID** aus. Bei dieser Auswahl wird die Zuordnung als `appuser.objectSid` angezeigt.

iii. **Wählen `userName`Sie aus der Spalte Benutzerprofil für Ihre Domain aus`cip_upn`. Bei dieser Auswahl wird die Zuordnung als `appuser.userName` angezeigt.

iv. **Wählen `externalId`Sie aus der Spalte Benutzerprofil für Ihre Domain aus`cip_oid`. Bei dieser Auswahl wird die Zuordnung als `appuser.externalId` angezeigt.

6. Melden Sie sich bei Citrix Cloud auf `https://citrix.cloud.com` an.
7. Klicken Sie im Menü “Citrix Cloud”auf **Identitäts- und Zugriffsverwaltung**.
8. Suchen Sie **SAML 2.0** und klicken Sie auf **Verbinden**.

   Die Seite **SAML konfigurieren** wird angezeigt.



Laden Sie die `xml` Datei herunter und öffnen Sie sie mit einem beliebigen Dateieditor. Nach Abschluss der weiteren Konfiguration in Okta müssen Sie erneut zu dieser Seite zurückkehren.

9. Navigieren Sie in Okta zu **Anwendung > App-Integration erstellen**.
10. Klicken Sie auf der Seite „ **Anwendung hinzufügen** “auf **Neue App erstellen** .
11. Wählen Sie auf der Seite „ **Neue Anwendungsintegration erstellen** “**SAML 2.0** aus und klicken Sie auf **Erstellen** .
12. Geben Sie Details wie den Namen der App und das App-Logo (optional) ein, legen Sie die Sichtbarkeit der App fest und klicken Sie dann auf **Weiter**.
13. Auf der Registerkarte **Configuration SAML** müssen Sie die Details aus der heruntergeladenen `xml` Datei verwenden:

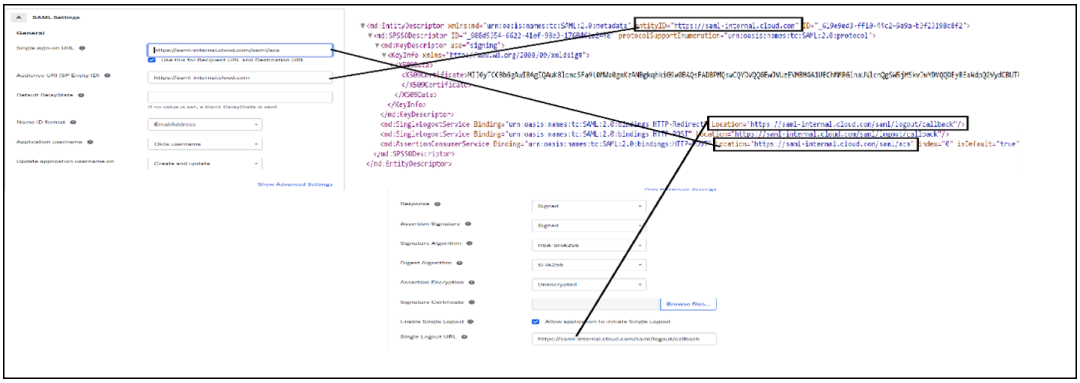
a) Geben Sie die URL-Details für **Single Sign-On-URL** als `https://saml-internal.cloud.com/saml/acs` und **Zielgruppen-URI (SP-Entitäts-ID)** als `https://saml-internal.cloud.com`ein.

> **Hinweis:**
>
> Wenn es sich um eine externe Citrix Cloud handelt, muss die URL `https://saml.cloud.com/saml/acs` und `https://saml.cloud.com` anstelle von `https://saml-internal.cloud.com` Domain lauten.

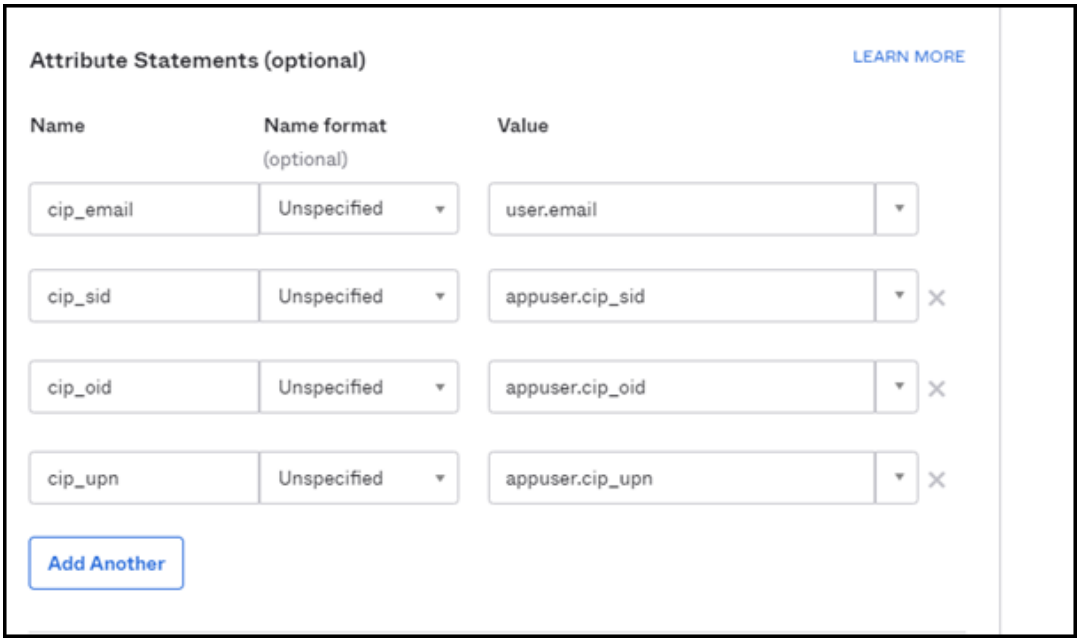
b) Wählen Sie **Unspezifiziert** für das **Name-ID-Format** aus.

c) ****Wählen Sie Okta-Benutzername als Anwendungsbenutzername aus.****

d) Klicken Sie auf **Erweiterte Einstellungen anzeigen** und stellen Sie sicher, dass **Antwort** und **Assertion** mit **Signiert**ausgewählt sind.



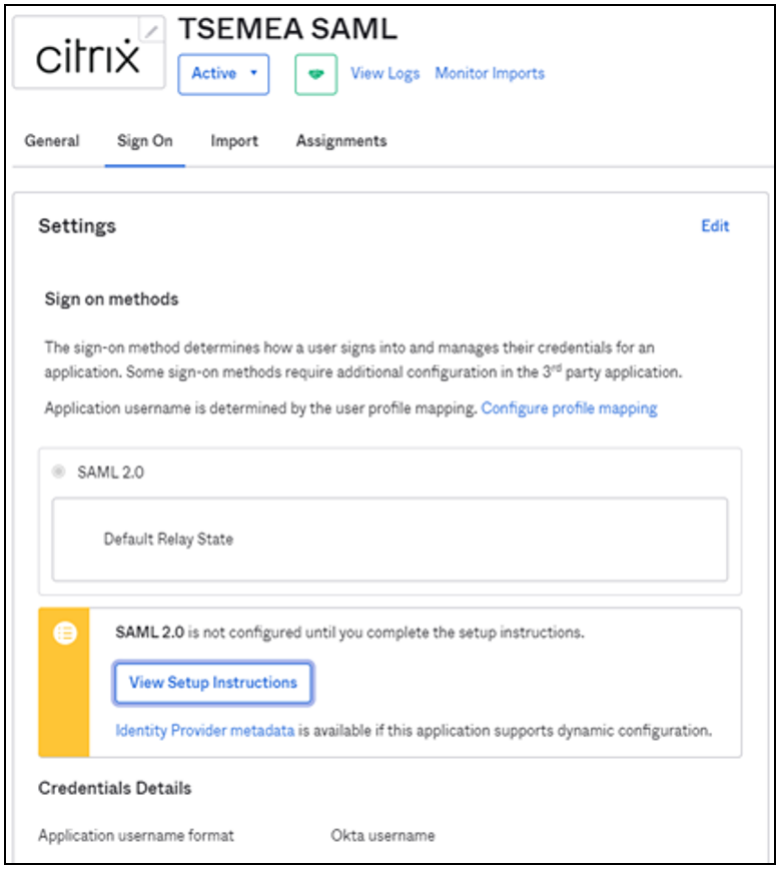
e) Fügen Sie **Attributanweisungen** hinzu, wie in der folgenden Abbildung gezeigt.



f) Sie können alle anderen Optionen standardmäßig belassen und auf **Weiter**klicken.

g) Wählen Sie Ich bin **Okta-Kunde und füge eine interne App hinzu** und klicken Sie dann auf **Fertig** stellen.

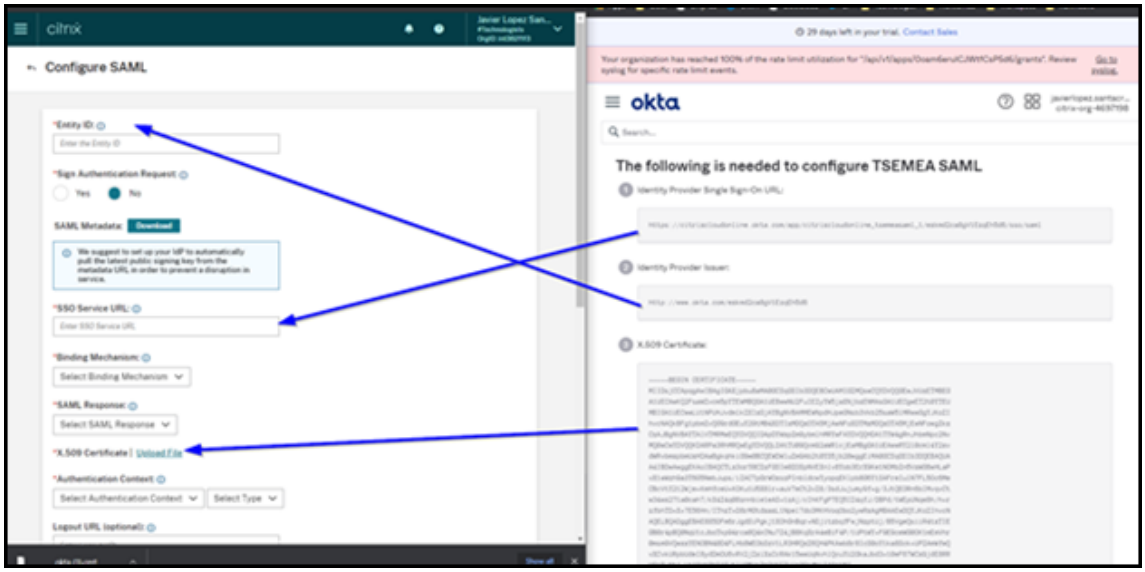
14. Die Okta-Anwendung ist jetzt erstellt und klicken Sie auf **Einrichtungsanweisungen anzeigen**.



Die Seite **So konfigurieren Sie SAML 2.0 für Testanwendungen** wird mit Informationen angezeigt, die Sie erneut in der Citrix Cloud hinzufügen müssen.

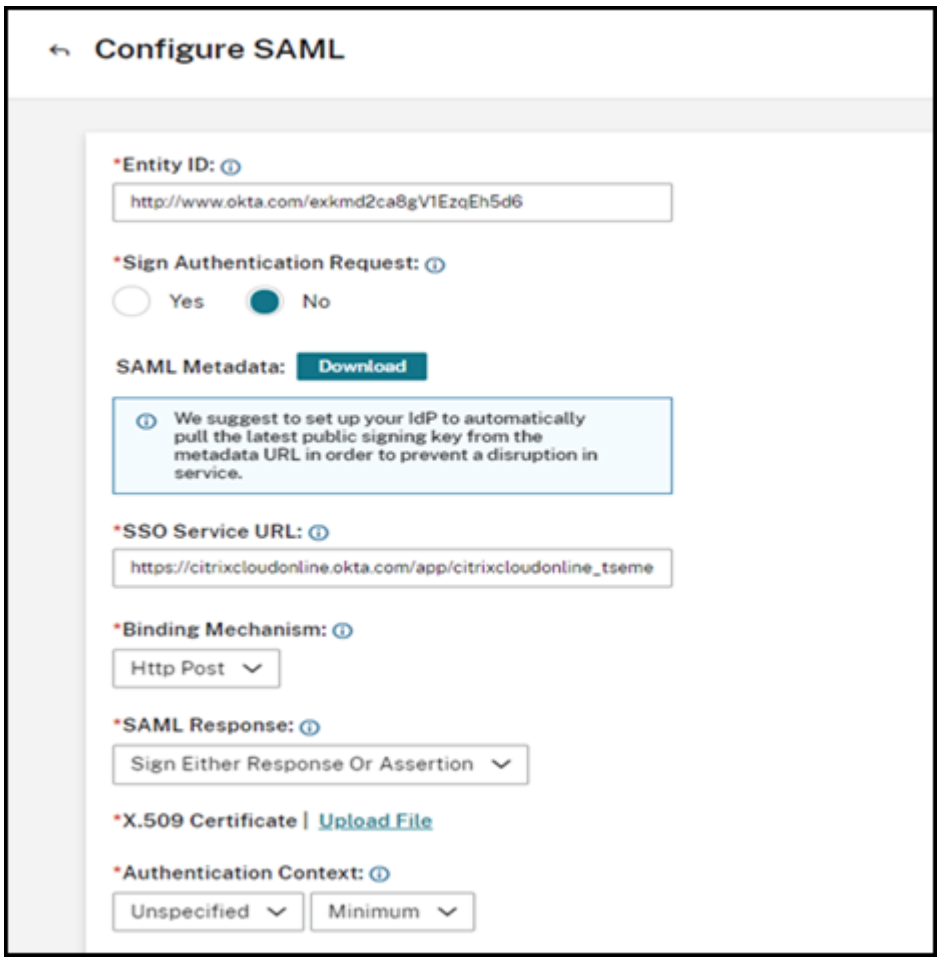
Laden Sie das Zertifikat herunter, um es in Citrix Cloud hochzuladen.

15. Sie müssen jetzt zur Seite **SAML konfigurieren** in Citrix Cloud zurückkehren und die verbleibende Konfiguration wie im Folgenden beschrieben abschließen:

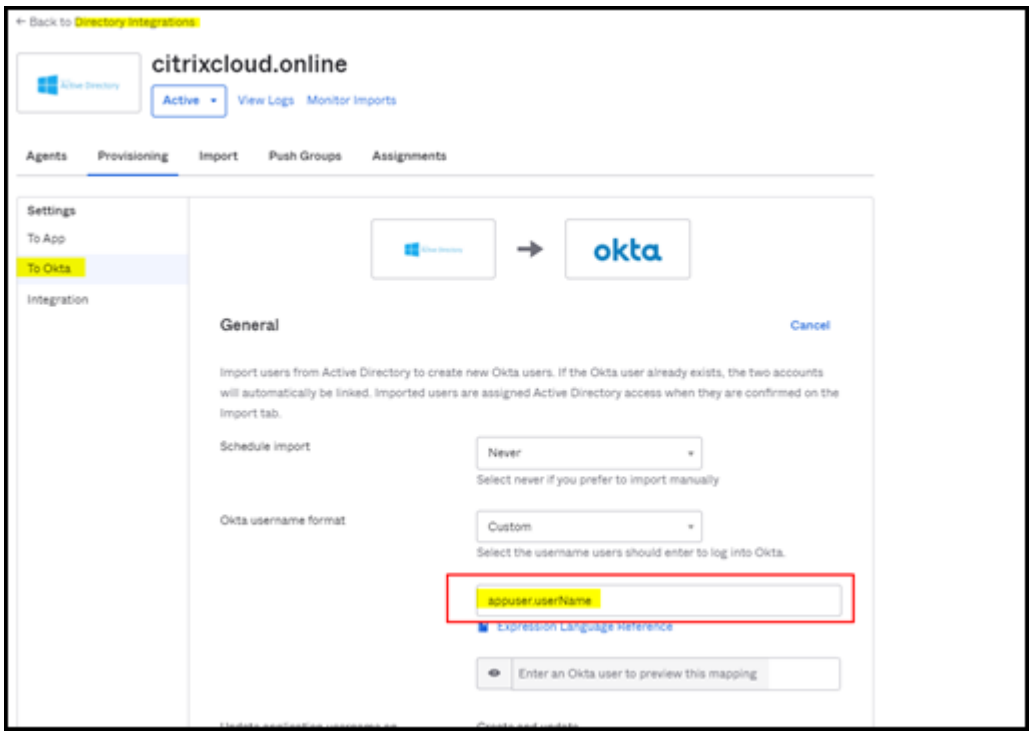


Verwenden Sie das heruntergeladene Zertifikat und benennen Sie die Dateinamenerweiterung von `.cert`in um `.crt`, um es in Citrix Cloud hochzuladen.

16. Nachdem Sie das Zertifikat hochgeladen haben, verwenden Sie alle anderen Optionen, die standardmäßig sind:



17. Als Nächstes müssen Sie sicherstellen`appuser.userName`, dass es unter **Directory-Integrations > Active Directory -> Provisioning > To** Okta definiert ist.



> **Hinweis:**
>
> Manchmal müssen Sie `user.cip_upn`stattdessen verwenden `appuser.cip_upn`. Stellen Sie sicher, dass Sie die Definition Ihrer Anwendung in der OKTA-Integration überprüfen, wie in diesem Bild gezeigt.

18. Sie müssen jetzt versuchen, Benutzer in Okta zu dieser SAML-Anwendung hinzuzufügen. Sie können Benutzer auf verschiedene Arten zuweisen.

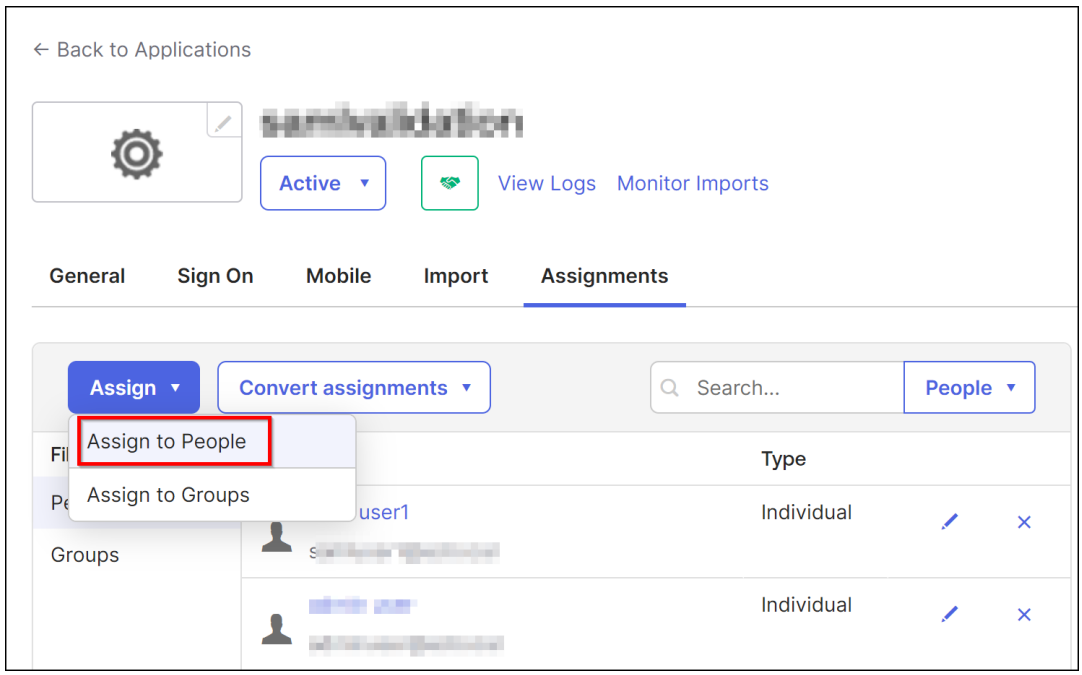
    Methode 1:

    a) Melden Sie sich mit Administratoranmeldedaten bei Okta an

    b) Navigieren Sie zu **Anwendungen > Anwendungen**

    c) Wählen Sie die SAML-Anwendung, die Sie erstellt haben

    d) Klicken Sie auf **Zuweisen > Personen zuweisen**



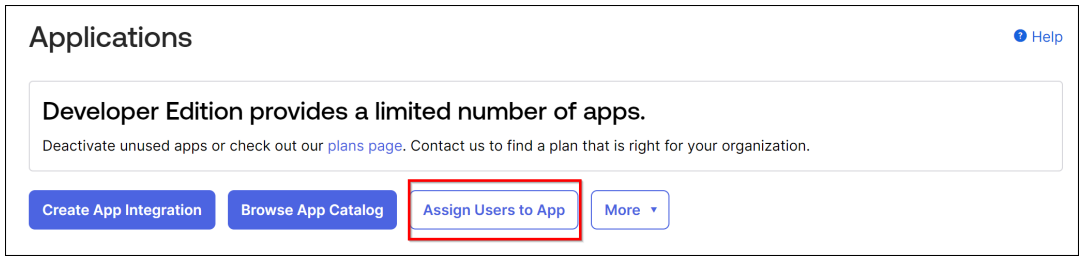
e) Klicken Sie auf **Zuweisen** und wählen Sie dann **Speichern und zurück** .

f) Klicken Sie auf **Fertig**.

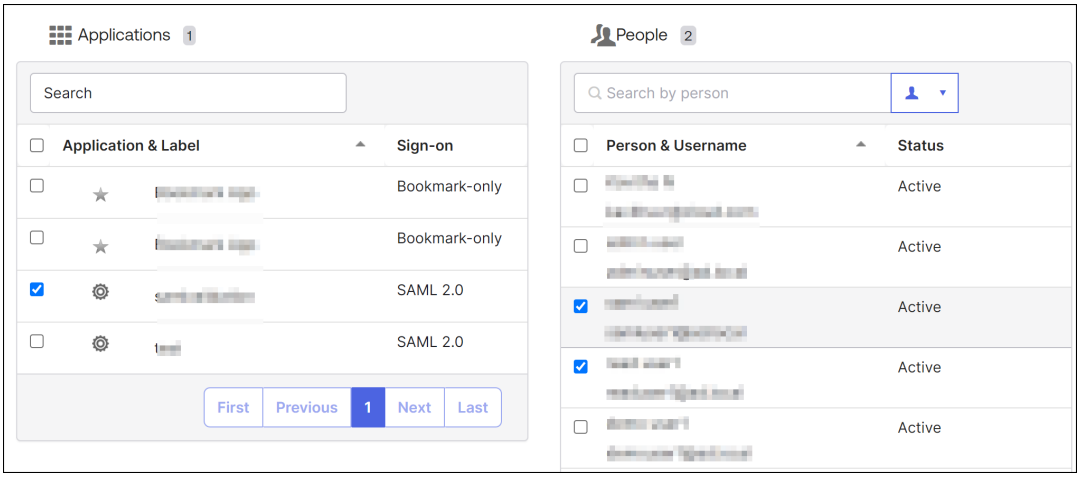
Methode 2:

a) Navigieren Sie zu **Anwendungen > Anwendungen**.

b) Klicken Sie auf **Benutzer der App zuweisen**.



c) Wählen Sie die Anwendung und die Benutzer aus, und klicken Sie dann auf **Weiter**.



d) Klicken Sie auf **Zuweisungen bestätigen**.

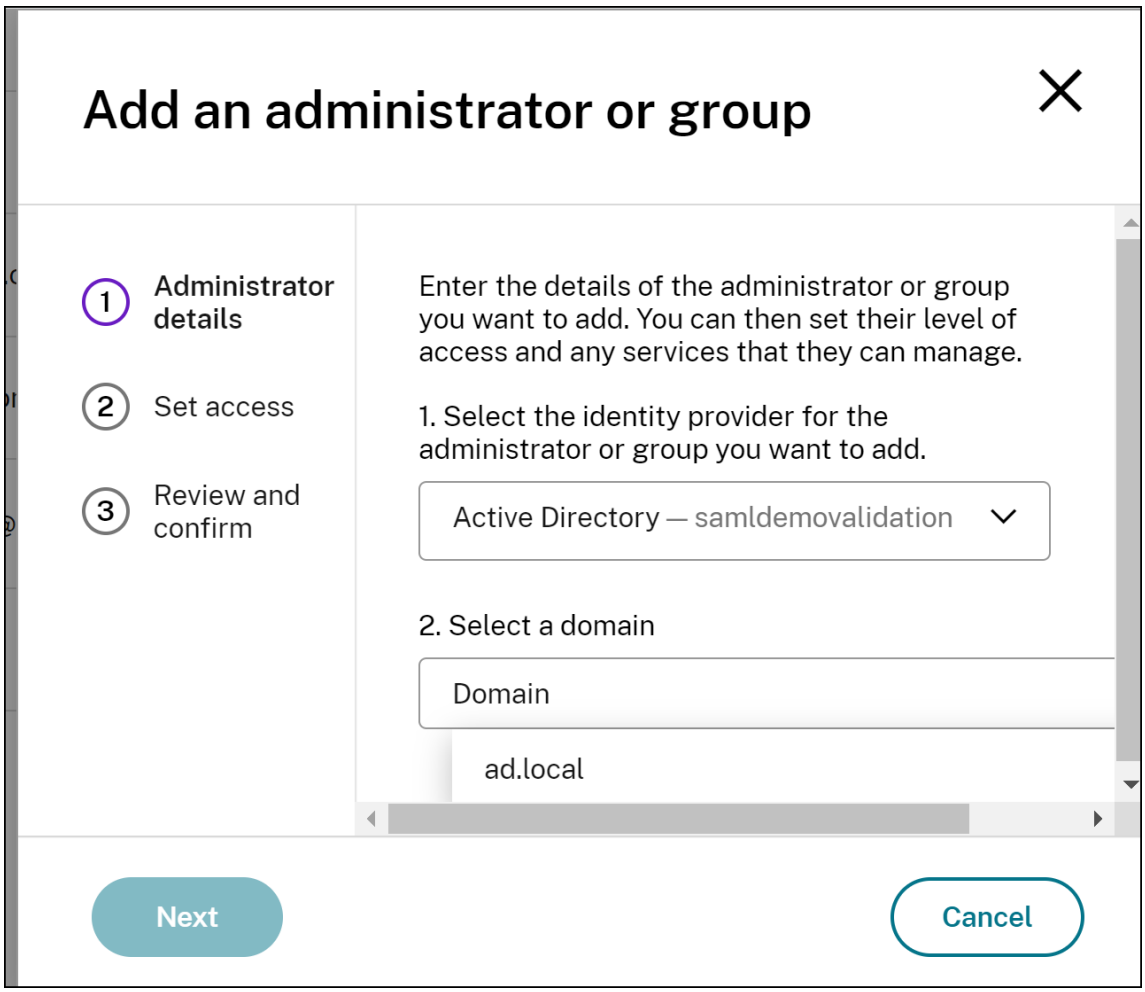
Methode 3:

a) Navigieren Sie zu **Verzeichnis > Personen**.

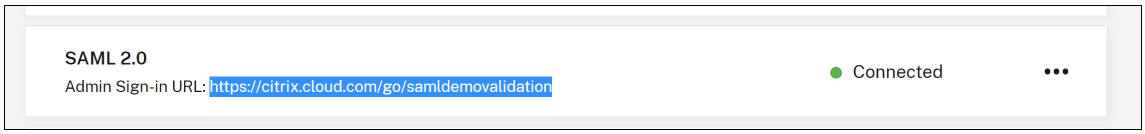
b) Wählen Sie einen beliebigen Benutzer aus.

c) Klicken Sie auf **Anwendungen zuweisen** und weisen Sie die SAML-Anwendung dem Benutzer zu.

19. Nachdem Sie Benutzer zugewiesen haben, melden Sie sich bei Citrix Cloud an.
20. Klicken Sie im Menü “Citrix Cloud”auf **Identitäts- und Zugriffsverwaltung**.
21. Klicken Sie auf der Registerkarte **Administratoren** auf **Administrator/Gruppe hinzufügen**.
22. Wählen Sie **Active Directory** —**[Ihr SAML-App-Name]** aus der Liste aus, wählen Sie die Domain aus und klicken **Sie**dann auf Weiter .



23. Geben Sie die Zugriffsberechtigungen an.
24. Prüfen Sie, ob alles korrekt ist, und klicken Sie auf **Einladung senden**.
25. Auf der Registerkarte **Authentifizierung** können Sie die Anmelde-URL für SAML 2.0 anzeigen. Ein Beispiel:



Systemanforderungen

July 17, 2024

Bevor Sie NetScaler Console verwenden, müssen Sie die Softwareanforderungen, Browseranforderungen, Portinformationen, Lizenzinformationen und Einschränkungen überprüfen.

Unterstützte Browser

Für den Zugriff auf NetScaler Console muss Ihre Workstation über einen unterstützten Webbrowser verfügen.

Die folgenden Browser werden unterstützt.

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

Installationsanforderungen für den Agent

Installieren und konfigurieren Sie einen Agenten in Ihrer Netzwerkumgebung, um die Kommunikation zwischen der NetScaler Console und den verwalteten Instanzen in Ihrem Rechenzentrum zu ermöglichen. In Ihrem lokalen Rechenzentrum können Sie einen Agent auf Citrix XenServer, VMware ESXi, Microsoft Hyper-V und Linux KVM-Server installieren.

Die Agentenanforderungen sind die virtuellen Computerressourcen, die der Hypervisor für jeden Agenten bereitstellen muss. In der folgenden Tabelle sind die Agentenanforderungen aufgeführt, um alle Funktionen der NetScaler Console nutzen zu können:

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

Die Agentanforderungen, um nur die gepoolte Lizenzierungsfunktion nutzen zu können, siehe Lightweight agent für gepoolte Lizenzierung.

Sie können auch einen Agent in Microsoft Azure oder AWS oder Google Cloud installieren. Citrix empfiehlt, die folgenden virtuellen Maschinentypen aus den jeweiligen Cloud-Marktplätzen zu verwenden, um alle Funktionen der NetScaler Console nutzen zu können:

Cloud	Anforderungen an Agents	Bevorzugter Typ der virtuellen
AWS	8 virtuelle CPUs, 32 GB RAM und 30 GB Speicherplatz	`m4.2xlarge`
Microsoft Azure	8 virtuelle CPUs, 32 GB RAM und 30 GB Speicherplatz	`Standard_D8s_v3`
Google Cloud	8 virtuelle CPUs, 32 GB RAM und 30 GB Speicherplatz	`e2-standard-8`

> **Hinweise:**
>
> Azure unterstützt das Scaling Out für Agenten mit den Basisinstallationsversionen 13.0 und 13.1 nach dem 23. Juli 2024 nicht mehr.
>
> Für NetScaler Agents:
>
> - NetScaler Agents mit 8 virtuellen CPUs, 32 GB RAM und 30 GB Speicherplatz bleiben davon unberührt. Diese Agenten können ohne Unterbrechungen aktualisiert werden.
> - Bereitstellungen, die mit Version 14.1 gestartet wurden, bleiben ebenfalls unberührt.
>
> Für Lightweight Agents:
>
> - Lightweight Agents mit 4 virtuellen CPUs, 8 GB RAM und 30 GB Speicherplatz, die die Basisinstallationsversionen 13.0 oder 13.1 verwenden, können nach dem Verfallsdatum nicht mehr hochskalieren (CPU oder RAM erhöhen).
> - Um die Lightweight Agents in Zukunft zu skalieren, stellen Sie einen neuen Agenten mit der neuesten Version bereit.

Anweisungen zur Installation eines Agents finden Sie unter den folgenden Links:

- Installieren Sie einen Agenten in Microsoft Azure Cloud.
- Installieren Sie einen Agenten auf AWS.
- Installieren Sie einen Agenten in Google Cloud.

Lightweight Agent für gepoolte Lizenzierung

Wenn Sie die NetScaler Console nur für gepoolte Lizenzen verwenden möchten, können Sie einen Agenten mit niedrigeren Spezifikationen verwenden, wie in der folgenden Tabelle aufgeführt:

Komponente	Voraussetzung
RAM	8 GB

Komponente	Voraussetzung
Virtuelle CPU	4
Speicherplatz	30 GB

Solche Agents mit niedrigeren Spezifikationen (Lightweight) werden nur auf der NetScaler Console unterstützt.

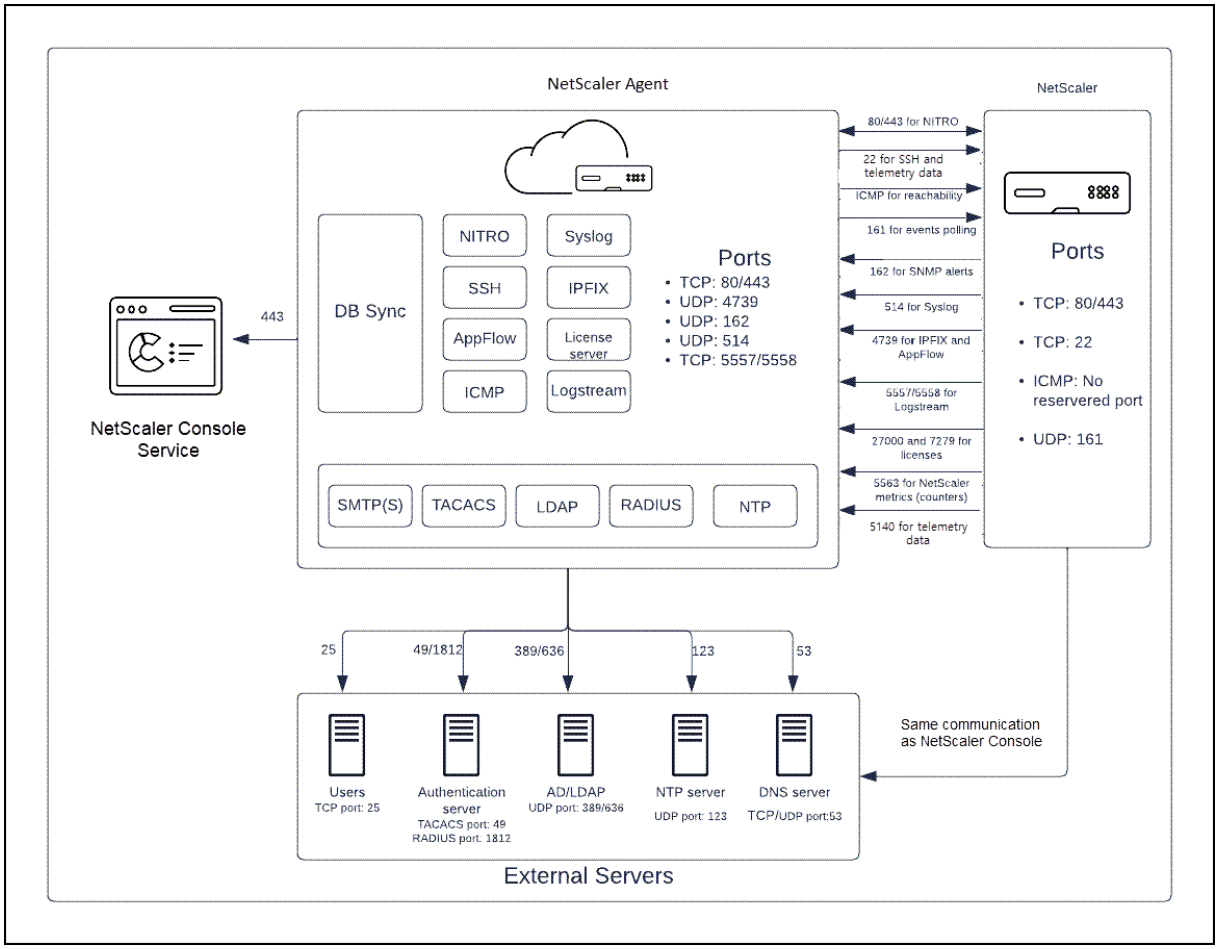
Citrix empfiehlt, die folgenden Typen virtueller Maschinen der jeweiligen Cloud-Marktplätze zu verwenden, um nur die gepoolte Lizenzierungsfunktion zu nutzen:

Cloud	Anforderungen an Agents	Bevorzugter Typ der virtuellen
AWS	4 virtuelle CPUs, 8 GB RAM und 30 GB Speicherplatz	`m4.xlarge`. Dieser Instanz-Typ bietet 4 virtuelle CPUs, 16 GB RAM und 30 GB Speicherplatz. Citrix empfiehlt diesen Instanz-Typ, da er den meisten Agentanforderungen unter vorhandenen Instanz-Typen entspricht.
Microsoft Azure	4 virtuelle CPUs, 8 GB RAM und 30 GB Speicherplatz	`Standard_F4s_v2`
Google Cloud	4 virtuelle CPUs, 8 GB RAM und 30 GB Speicherplatz	`e2-standard-4`

> **Hinweis**
>
> Sie müssen die Standardplanungsjobs deaktivieren, indem Sie zu **Einstellungen > Globale Einstellungen > Konfigurierbare Funktionen**navigieren.

Unterstützte Ports

Für die Kommunikation zwischen NetScaler-Instanzen und Agent öffnen Sie die erforderlichen Ports.



Ports für den NetScaler Agent

In dieser Tabelle werden die erforderlichen Ports erklärt, die auf dem Agenten geöffnet sein müssen.

Port	Typ	Details	Richtung der Kommunikation
80/443	TCP	Für die NITRO-Kommunikation vom NetScaler Console-Dienst zu NetScaler.	NetScaler Agent zu NetScaler und NetScaler zu NetScaler Agent
4739	UDP	Für die AppFlow-Kommunikation von NetScaler zum NetScaler Console-Dienst.	NetScaler zu NetScaler Agent

Port	Typ	Details	Richtung der Kommunikation
162	UDP	Um SNMP-Ereignisse von der NetScaler-Instanz an den NetScaler Console-Dienst zu empfangen.	NetScaler zu NetScaler Agent
514	UDP	Um Syslog-Meldungen von der NetScaler-Instanz an den NetScaler Console-Dienst zu empfangen.	NetScaler zu NetScaler Agent
5563	TCP	Dieser Port ist für die Ausführung des NetScaler Console Collector-Dienstes erforderlich. Um NetScaler-Metriken (Zähler) von der NetScaler-Instanz an die NetScaler Console zu empfangen.	NetScaler zu NetScaler Console
5557/5558	TCP	Für die Logstream-Kommunikation (für WAF-Sicherheitsverstöße, Web Insight und HDX Insight) von NetScaler zum NetScaler Console-Dienst.	NetScaler zum NetScaler Agent

Port	Typ	Details	Richtung der Kommunikation
27000 und 7279	TCP	Lizenzports für die Kommunikation zwischen NetScaler Agent und NetScaler-Instanz. Diese Ports werden auch für NetScaler-Poollizenzen verwendet.	NetScaler zu NetScaler Agent
443	TCP	Ports für die Kommunikation zwischen NetScaler Agent und NetScaler Console Service	NetScaler Agent zum NetScaler Console-Dienst
5140	UDP	Port zum Empfangen von NetScaler Gateway-Telemetriedaten	NetScaler zu NetScaler Console

Ports für NetScaler-Instanzen

In dieser 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 der NetScaler-Konsole zur NetScaler-Instanz.	NetScaler Agent zu NetScaler und NetScaler zu NetScaler Agent

Port	Typ	Details	Richtung der Kommunikation
22	TCP	Für die SSH-Kommunikation zwischen dem Agenten und NetScaler. **Hinweis:** Dieser Port wird auch für NetScaler-Telemetrie verwendet.	NetScaler Agent zu NetScaler
Kein reservierter Port	ICMP	Um die Netzwerkerreichbarkeit zwischen NetScaler Agent und NetScaler-Instanzen zu erkennen.	NetScaler Agent zu NetScaler
161	UDP	Um Ereignisse von NetScaler-Instanzen abzufragen.	NetScaler Agent zu NetScaler

Ports für den integrierten NetScaler-Agent

In dieser Tabelle werden die erforderlichen Ports erläutert, die für den integrierten NetScaler-Agent erforderlich sind.

Port	Typ	Details	Richtung der Kommunikation
443	TCP	Für die NITRO-Kommunikation von der NetScaler-Konsole zur NetScaler-Instanz.	NetScaler Console auf den integrierten NetScaler Agent und den integrierten NetScaler Agent auf die NetScaler Console

> **Hinweis**
>
> Der Endpunkt des NetScaler Console-Dienstes entspricht der "Service-URL", die beim Versuch, den Agenten zu registrieren, generiert wurde. Der Agent verwendet die Service-URL, um die NetScaler Console zu finden.

Stellen Sie sicher, dass die folgenden Endpunkt-URLs Zugriff haben:

- Download-Service:

```
https://download.citrixnetworkapi.net
```

- Treuhand-Service:

```
*.citrixnetworkapi.net
```

- Service-URLs:

```
*.agent.adm.cloud.com
*.adm.cloud.com
adm.cloud.com
```

- Citrix Cloud-Konnektivität:

```
citrix.cloud.com
accounts.cloud.com
```

Veraltete FQDNs

Einige FQDNs sind für die folgende Verwendung der NetScaler Console veraltet. Damit Sie ohne Unterbrechung zu den neuen FQDNs wechseln können, funktionieren die veralteten FQDNs für einige Zeit weiter und werden langsam auslaufen.

NetScaler Console-Endpunkte	Alter FQDN	Neuer FQDN
Zugriff auf die NetScaler Console UI	`netscalermas.cloud.com`	`adm.cloud.com`
Dienst-URL	`agent.netscalermgmt.net`	`*.agent.adm.cloud.com` **Hinweis**: Der Wert von * hängt davon ab, in welcher PoP (Point of Presence) Ihre Daten verfügbar sind.
API-Interaktionen	`netscalermas.cloud.com`	`api.adm.cloud.com`

Minimale NetScaler-Versionen erforderlich

> Hinweis
>
> Die NetScaler-Versionen 10.5, 11.0 und 12.0 haben bereits End Of Life (EOL) erreicht. Weitere Informationen finden Sie in der Produktmatrix. Die empfohlene NetScaler-Version ist 12.1.

NetScaler Console-Funktion	NetScaler-Softwareversion
StyleBooks	10.5 und höher
Überwachen/Reporting und Konfiguration mithilfe von Jobs Analytics	10.5 und höher
HDX Insight	10.1 und höher
Gateway Insight	11.0.65.31 und höher
Security Insight	11.0.65.31 und höher

Anforderungen an die NetScaler Console Analytics-Lösung

Erforderliche Mindestversionen von Citrix Virtual Apps and Desktops

NetScaler Console-Funktion	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 Console unterstützt keine eigenständigen Access Gateway Standard-Geräte.

NetScaler Console kann Berichte für Anwendungen generieren, die auf einer Citrix Virtual App oder einem Desktop veröffentlicht sind und auf die über Citrix Workspace zugegriffen wird. Diese Funktion hängt jedoch vom Betriebssystem ab, auf dem der Citrix 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

NetScaler Console unterstützt die folgenden Thin Clients zur Überwachung von NetScaler-Instanzen, die auf Softwareversion 11.0 Build 65.31 und höher ausgeführt werden:

- Dell Wyse Windows basierte Thin Clients
- Dell Wyse Linux-basierte Thin Clients
- Dell Wyse ThinOS-basierte Thin Clients
- 10ZiG Ubuntu-basierte Thin Clients

NetScaler-Instanzlizenz für HDX Insight erforderlich

Die von NetScaler Console für HDX Insight gesammelten Daten hängen von der Version und den installierten Lizenzen der NetScaler-Instanzen ab, die überwacht werden. HDX Insight-Berichte werden nur für NetScaler Premium- und Enterprise-Appliances angezeigt, die auf Softwareversion 10.5 und höher ausgeführt werden.

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 Betriebssysteme und Citrix Workspace-Versionen

In der folgenden Tabelle sind die von NetScaler Console unterstützten Betriebssysteme und die aktuell von jedem System unterstützten Citrix Workspace-Versionen aufgeführt:

Betriebssystem	Citrix 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

Lizenzen

March 12, 2024

Ab NetScaler Console Service Release 14.1-21.x wurde das Konzept der lizenzierten VIPs entfernt. Eine unbegrenzte Anzahl von VIPs ist jetzt im NetScaler Console-Dienst verfügbar. Sie müssen keine virtuellen NetScaler Console-Serverlizenzen mehr erwerben, da die VIP-Lizenz-SKU in Kürze End of Sale (EOS) und End of Renewal (EOR) lauten.

Die Änderungen am NetScaler Console-Dienstspeicher lauten wie folgt:

- Die NetScaler Console Service Storage-SKU wird in Kürze "End of Sale"(EOS) und "End of Renewal"(EOR) lauten.
- Die Standardspeicherberechtigung für den NetScaler Console-Dienst beträgt jetzt 5 GB.
- Jeder NetScaler Console-Servicespeicher, der in der Vergangenheit gekauft wurde, wird bis zum Ende der Laufzeit berücksichtigt.
- Alle NetScaler Console-VIP-Lizenzen, die in der Vergangenheit erworben wurden und die Sie zu einem anteiligen Anspruch auf NetScaler Console-Servicespeicher berechtigen, werden bis zum Ende der Laufzeit anerkannt.
- Wenn Sie ein anderes Paket erwerben, das Sie zu einer höheren NetScaler Console-Speicherberechtigung berechtigt, werden die standardmäßigen 5 GB entsprechend der Berechtigung geändert.

> **Hinweis:**
>
> Wenn Sie zuvor einen virtuellen Server gekauft haben, fallen bis zum Ende der Abonnementlaufzeit 500 MB Speicherplatz pro virtuellem Server an.

Für die Funktionen der NetScaler Console ist eine NetScaler-Lizenzierung erforderlich

In der folgenden Tabelle sind die NetScaler-Lizenzen aufgeführt, die für die Nutzung einiger Funktionen der NetScaler Console erforderlich sind.

NetScaler Console-Funktionsgruppe	Funktionen der NetScaler Console	Lizenzanforderungen für NetScaler und Gateway
Analytics	HDX Insight	Advanced (Reporting < 1 Stunde) Premium (Reporting = Unbegrenzt)
Analytics	Security Insight	Premium (oder) Advanced mit App Firewall-Lizenz

NetScaler Console-Funktionsgruppe	Funktionen der NetScaler Console	Lizenzanforderungen für NetScaler und Gateway
Analytics	Gateway Insight	Advanced (Reporting < 1 Stunde) Premium (Reporting = Unbegrenzt)
Anwendungen	Anwendungsstatistiken (App-Dashboard, App-Sicherheitsdashboard)	Für Informationen zur NetScaler Web App Firewall im App-Dashboard und im App-Sicherheitsdashboard ist eine Premium (oder) Advanced mit App Firewall-Lizenz erforderlich
Anwendungen	API-Gateway	Premium (oder) Advanced-Lizenz
Anwendungen	StyleBooks	–
Anwendungen	Inventarverwaltung — Infrastruktur-Dashboard, Instanzgruppen, Instanz-Dashboards und Sites	–
Anwendungen	Eventmanagement und Syslog	–
Anwendungen	Konfigurationsjobs, Konfigurationsaudit und Konfigurationsempfehlungen	–
Anwendungen	Netzwerk-Reporting (Instanzebene)	–
Anwendungen	Netzwerkberichte (virtuelle Serverebene)	–
Anwendungen	Netzwerkfunktionen (Einfache Sichtbarkeit und Verwaltung von virtuellen Servern, Diensten, Servicegruppen, Servern)	–
Anwendungen	SSL-Zertifikatsverwaltung (Instanzebene)	–
Anwendungen	SSL-Zertifikatsverwaltung (virtuelle Serverebene)	–

NetScaler Console-Funktionsgruppe	Funktionen der NetScaler Console	Lizenzanforderungen für NetScaler und Gateway
System	RBAC und externe Authentifizierung (Instanzebene)	–
System	RBAC und externe Authentifizierung (virtuelle Serverebene)	–

Ablaufprüfungen für virtuelle Serverabonnements anzeigen

Sie können den Status der installierten Lizenzen mit Ablauf und dem zulässigen Speicherlimit für die Lizenzen in NetScaler Console anzeigen.

So zeigen Sie den Status der Lizenzen an:

1. Navigieren Sie zu **Konto** > **Abonnements**.
2. Im Abschnitt **Ansprüche** können Sie die Details der lizenzierten virtuellen Server und die Tage bis zum Ablauf anzeigen:
    - **Berechtigte virtuelle Server:** Anzahl der virtuellen Server, die lizenziert werden können.
    - **Berechtigte virtuelle Server von Drittanbietern:** Anzahl der virtuellen Server von Drittanbietern, die Sie mit der Lizenz verwalten können.
    - **Berechtigter Speicher:** Speicherlimit der Lizenz.
    - **Tage bis zum Ablauf:** Anzahl der verbleibenden Tage bis zum Ablauf der Lizenz.

Zeigen Sie die Art der auf den virtuellen Servern aktivierten Analysen an

Nachdem Sie AppFlow auf den ausgewählten virtuellen Servern aktiviert haben, können Sie den Analysetyp, der auf den lizenzierten virtuellen Servern oder virtuellen Servern von Drittanbietern aktiviert ist, auf der Seite **Abonnements** anzeigen.

1. Navigieren Sie zu **Konto > Abonnements**.
2. Wählen Sie im Abschnitt **Zusammenfassung der Virtual Server Analytics** den Typ der lizenzierten virtuellen Server aus.
3. Auf der Seite Lizenzierte virtuelle Server wird die Liste der lizenzierten virtuellen Server angezeigt. Auf dieser Seite zeigt die Spalte **Analytics-Status** den Typ der auf den virtuellen Servern aktivierten Analysen an.

Upgrade-Empfehlungen

January 26, 2024

Als Netzwerkadministrator verwalten Sie möglicherweise viele NetScaler-Instanzen, die auf verschiedenen NetScaler-Versionen ausgeführt werden, in der NetScaler Console. Die Überwachung des Lebenszyklus jeder NetScaler-Instanz kann eine umständliche Aufgabe sein. Sie müssen die NetScaler-Produktmatrix aufrufen und die NetScaler-Instanzen identifizieren , die das Ende des Lebenszyklus (EOL) oder das Ende der Wartung (EOM) erreichen oder erreicht haben. Planen Sie dann ihr Upgrade.

Um diesen Vorgang zu vereinfachen, hilft Ihnen die Upgrade-Empfehlung von NetScaler Console dabei, den Lebenszyklus Ihrer NetScaler-Instanzen auf folgende Weise zu überwachen:

- Identifiziert Instanzen, die EOL oder EOM erreichen oder erreicht haben. Sie können NetScaler-Upgrades also vor dem EOL- oder EOM-Datum planen.
- Hebt die Instanzen hervor, die nicht auf der neuesten Version oder dem neuesten Build Sie können diese Instanzen auf die neueste Version oder den neuesten Build aktualisieren. Mit diesem Upgrade erhalten Sie Updates zu neuen Funktionen und behobenen Problemen.
- Hebt die Instanzen hervor, die sich nicht auf bevorzugten NetScaler-Builds befinden. Einige Organisationen haben möglicherweise bevorzugte NetScaler-Builds für ihre Instanzen. In NetScaler Console können Sie je nach Buildstabilität, Funktionen und anderen Überlegungen den bevorzugten Build für Ihre Organisation festlegen . Überprüfen und aktualisieren Sie dann die Instanzen, die nicht auf bevorzugten Builds sind. Instanzen, auf denen die bevorzugten Builds ausgeführt werden, sind mit einem Sternsymbol gekennzeichnet.
- Hebt Instanzen hervor, die in den beliebtesten Versionen oder Builds ausgeführt werden. Instanzen, auf denen die beliebten Builds ausgeführt werden, werden durch ein Ribbon-Symbol gekennzeichnet

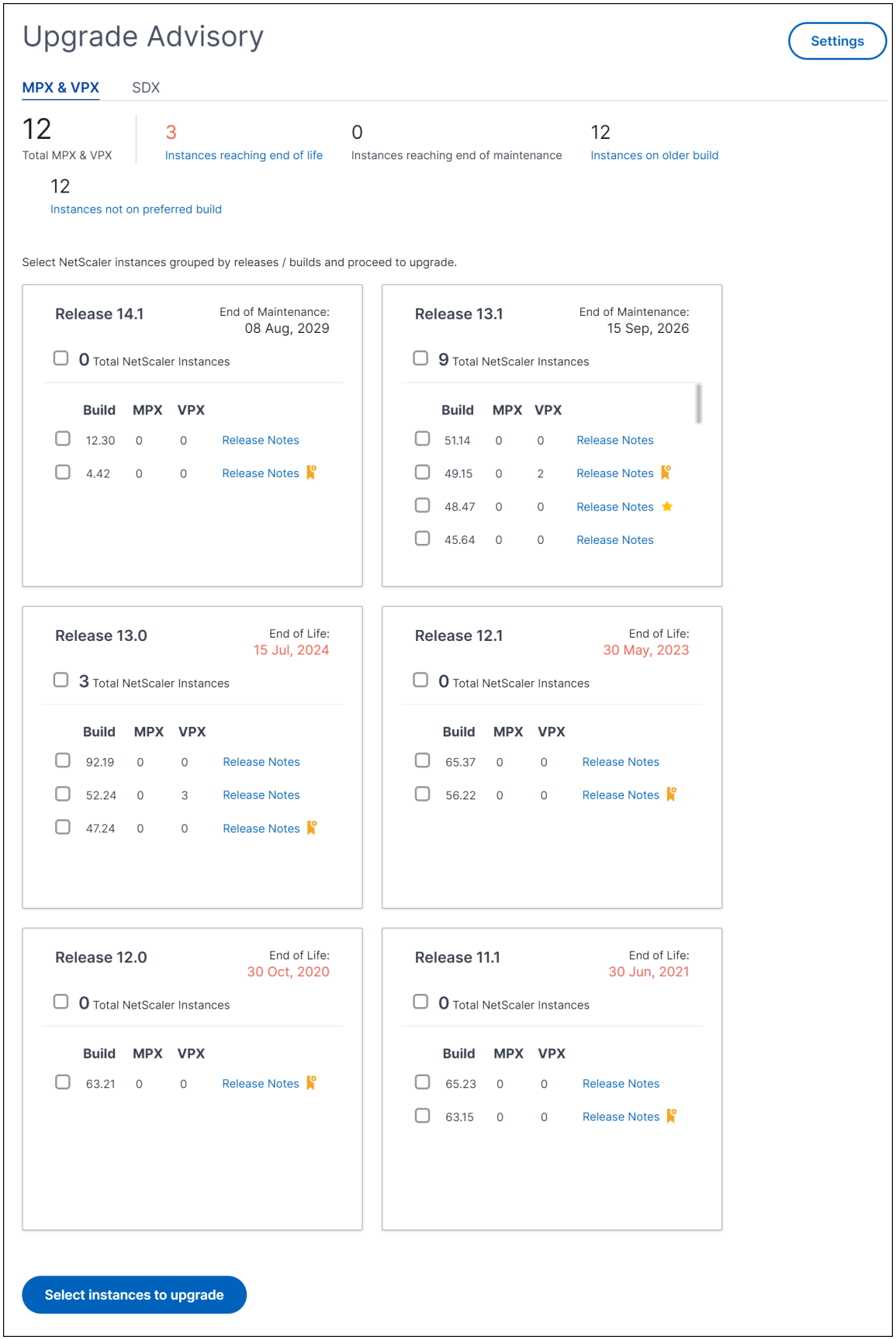
Der Upgrade-Advisory bietet Links zu entsprechenden Versionshinweisen. Anhand dieser Informationen können Sie einen NetScaler-Build für ein Upgrade überprüfen und entscheiden. Sie können mit der Erstellung eines Wartungsauftrags zum Upgrade von NetScaler-Instanzen von der Seite mit der Upgrade-Empfehlung aus fortfahren.

> **Wichtig**
>
> Die Upgradeempfehlung überwacht nur die EOL von NetScaler-Softwareversionen. Die EOL von NetScaler Appliances wird nicht überprüft.

Upgrade-Advisory anzeigen

Navigieren Sie zu **Infrastruktur > Instanz Advisory > Upgrade Advisory**, und zeigen Sie die folgenden

- Gesamtzahl der NetScaler-Instanzen.
- Instanzen, die das Lebensende erreichen.
- Instanzen, die das Ende der Wartung erreichen.
- Instanzen in älteren Builds.
- Instanzen, die sich nicht im bevorzugten Buil
- Daten zum Ende der Lebensdauer und zum Ende der Wartung für die verschiedenen NetScaler-Versionen.

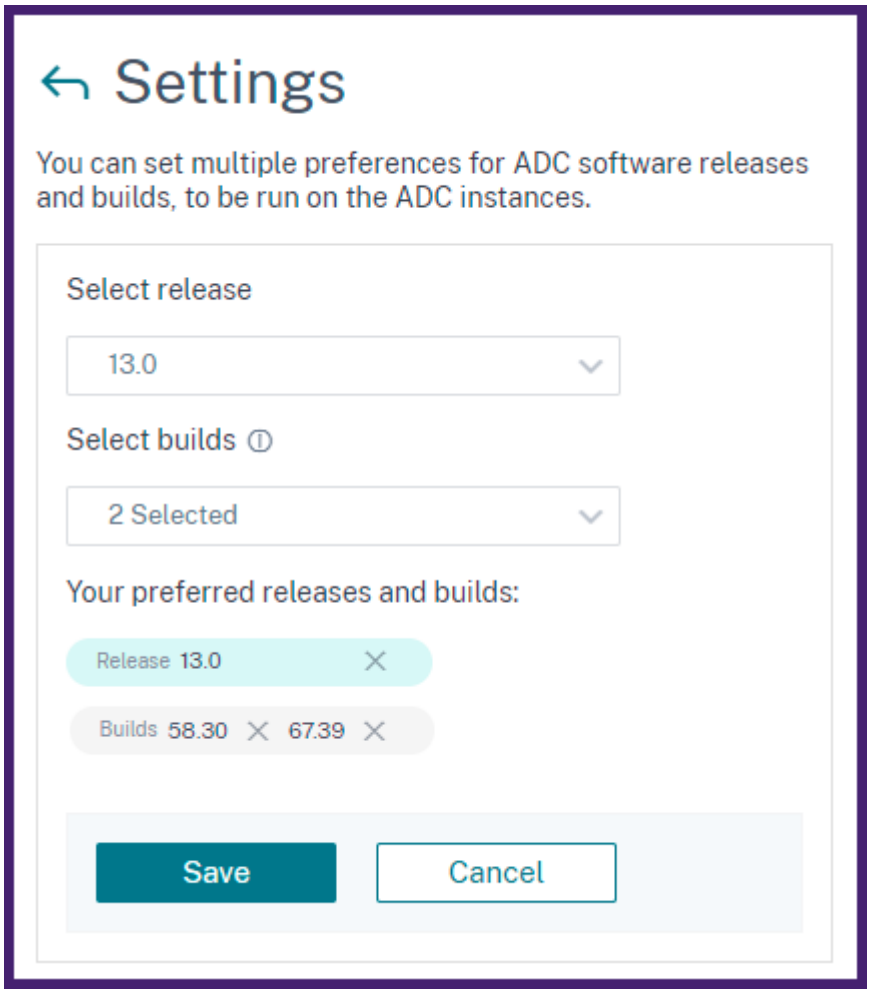


Auf der Seite „ **Upgrade Advisory** “werden die NetScaler-Instanzen nach ihren Versionen gruppiert. **Der Link Versionshinweise führt Sie zu den spezifischen NetScaler-Versionshinweisen. Überprüfen Sie neue Funktionen, behobene und bekannte Probleme, bevor Sie sich für ein Upgrade entscheiden. Sie können mehrere NetScaler-Instanzen in verschiedenen Versionen für ein gleichzeitiges Upgrade auswählen. Wenn Sie mit einem Upgrade fortfahren, wird ein Upgrade-Job erstellt. Siehe NetScaler-Instanzen aktualisieren .

Festlegen der bevorzugten Builds

Als Administrator können Sie einen bevorzugten NetScaler-Build für die Organisation definieren. Führen Sie folgende Schritte aus, um den bevorzugten Build festzulegen:

1. Klicken Sie unter **Infrastruktur > Instanz Advisory > Upgrade Advisory**auf **Einstellungen**.
2. Wählen Sie das bevorzugte Release und Build.



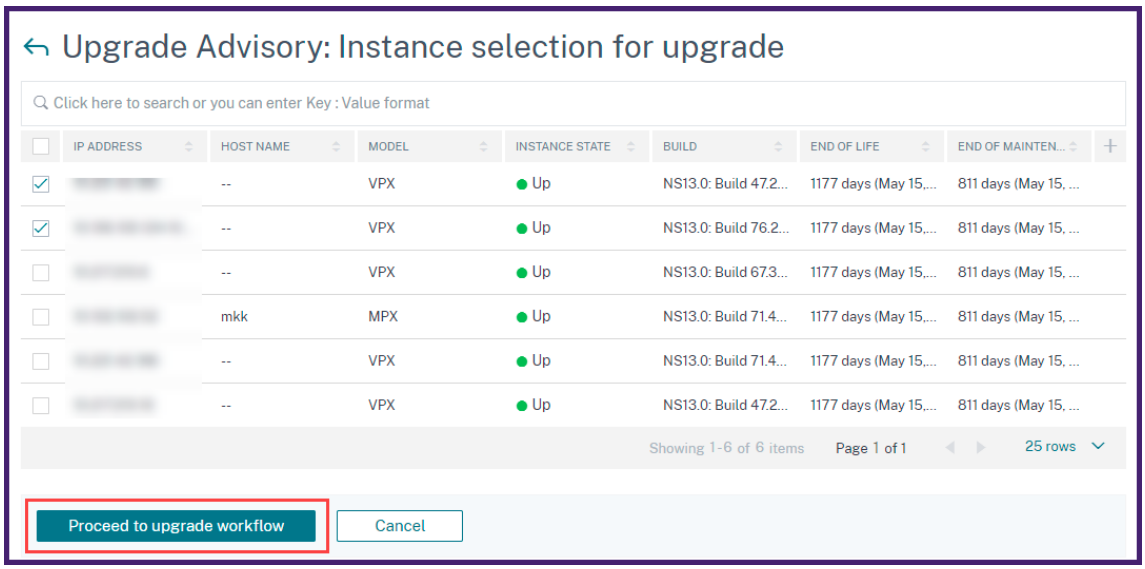
   In diesem Beispiel sind die bevorzugten Builds `13.0-58.30` und `13.0-67.39`.

3. Klicken Sie auf **Speichern**.

Upgrade von NetScaler-Instanzen

Führen Sie nach Ihrer Überprüfung auf der Seite mit den **Upgrade**-Hinweisen die folgenden Schritte aus, um die erforderlichen NetScaler-Instanzen zu aktualisieren:

1. Wählen Sie die Instanz-Builds aus, die Sie aktualisieren möchten, und klicken Sie auf **Instanzen auswählen, um ein Upgrade durchzuführen**
2. Wählen Sie die NetScaler-Instanz aus, die Sie aktualisieren möchten, und klicken Sie auf **Weiter zum Upgrade-Workflow** .



   Dieser Workflow erstellt einen Upgrade-Auftrag.

3. Auf der Registerkarte **Select Instanz**

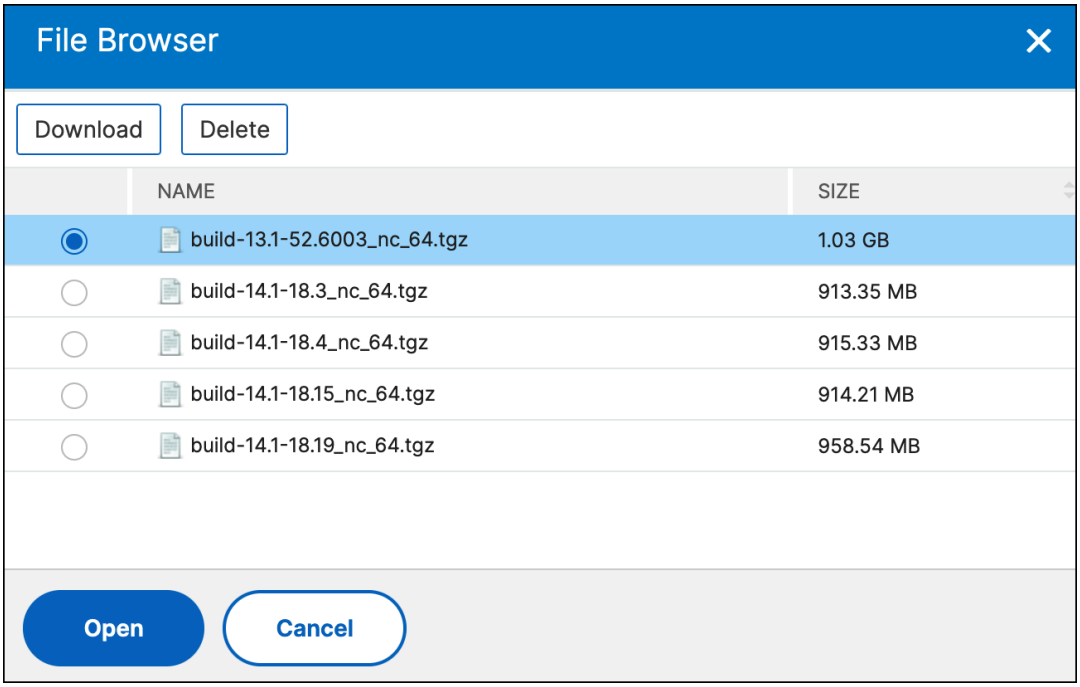
   a) Geben Sie einen Namen für den Upgrade-Auftrag an.

   b) (Optional) wenn Sie weitere Instanzen hinzufügen möchten, klicken Sie auf **Instanzen hinzufügen**.

   c) Klicken Sie auf **Weiter**.

4. Wählen Sie auf der Registerkarte **Select Image** ein NetScaler-Image aus der Image-Bibliothek oder lokal oder Appliance aus.

   - **Aus Bildbibliothek**auswählen : Wählen Sie ein NetScaler-Image aus der Liste aus. Diese Option listet alle NetScaler-Images auf, die auf der NetScaler-Download-Website verfügbar sind.



Die NetScaler-Software-Images zeigen die bevorzugten Builds mit dem Sternsymbol an. Und die meisten heruntergeladenen Builds mit dem Lesezeichen-Symbol.

- **Wählen Sie zwischen lokal oder Appliance**: Sie können das Image von Ihrem lokalen Computer oder der NetScaler Appliance hochladen. Wenn Sie NetScaler Appliance auswählen, zeigt die NetScaler Console-GUI die Instanzdateien an, die in `/var/mps/mps_images`enthalten sind. Wählen Sie das Image in der NetScaler Console-GUI aus.
- **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.

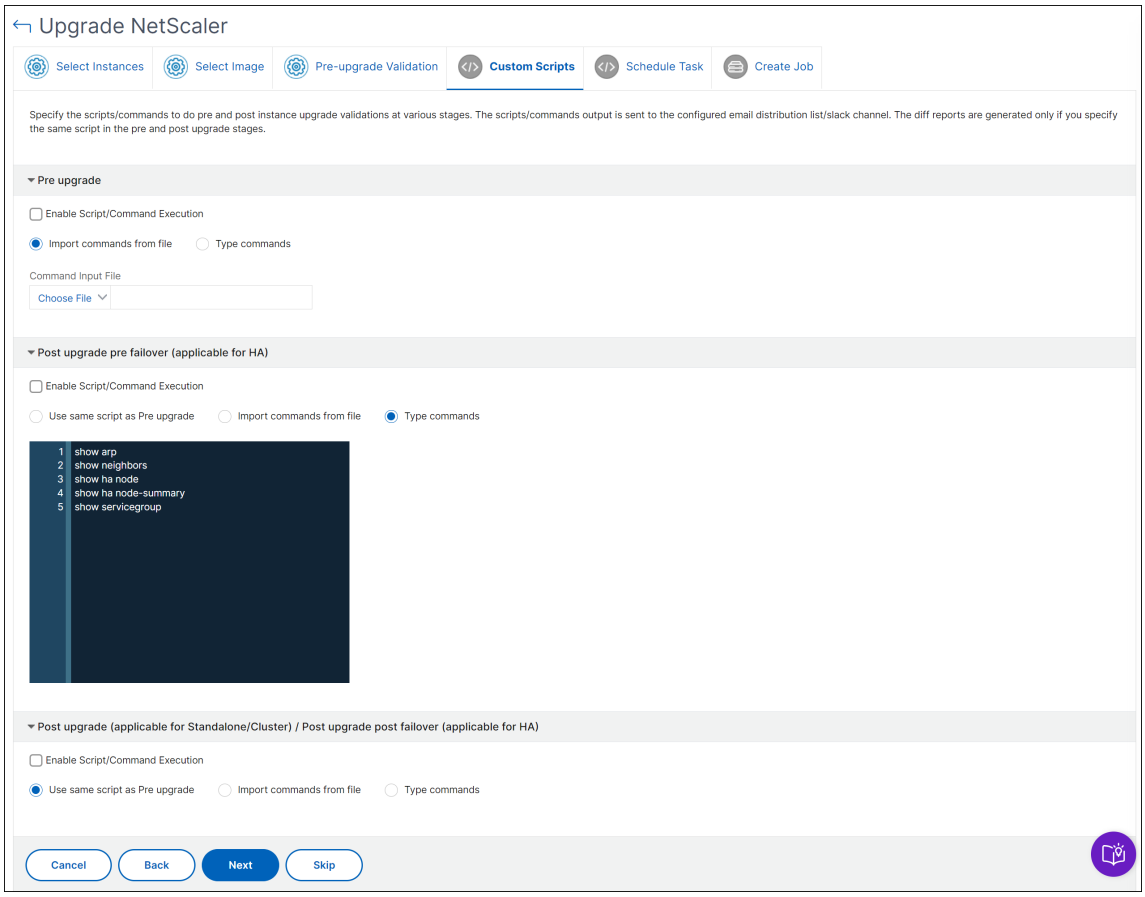
5. Auf der Registerkarte **Validierung vor dem Upgrade** werden die fehlgeschlagenen Instanzen angezeigt. Sie können die fehlgeschlagenen Instanzen entfernen und auf **Weiter**klicken.

   - **Speicherplatzprüfung**: Wenn auf einer Instanz nicht genügend Speicherplatz vorhanden ist, können Sie den Speicherplatz überprüfen und bereinigen. Siehe NetScaler-Speicherplatz bereinigen.

- **Richtlinien-Check**: Wenn NetScaler Console nicht unterstützte klassische Richtlinien findet, können Sie diese Richtlinien entfernen, um einen Upgrade-Job zu erstellen.

> **Hinweis:**
>
> Wenn Sie eine Cluster-IP-Adresse angeben, führt die NetScaler Console die Validierung vor dem Upgrade nur auf der angegebenen Instanz durch, nicht auf den anderen Clusterknoten.

6. Optional geben Sie auf der Registerkarte **Benutzerdefinierte Skripts** die Scripts an, die vor und nach einem Instanz-Upgrade ausgeführt werden sollen.

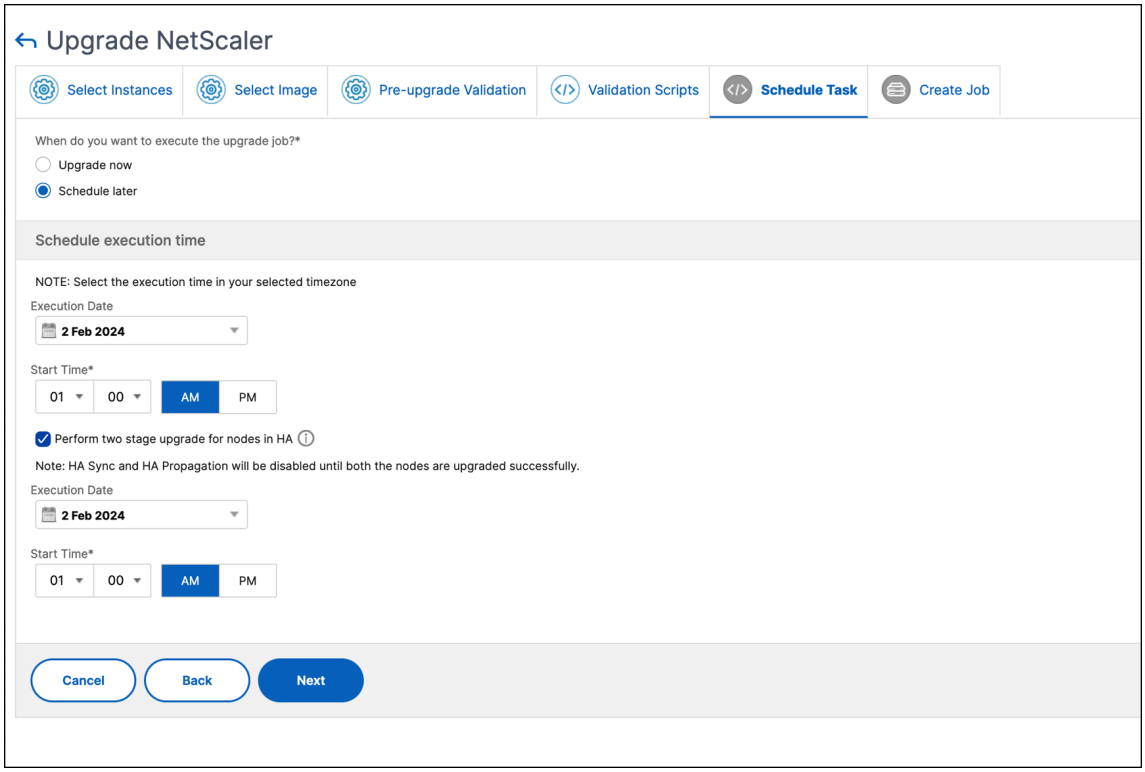


Weitere Informationen finden Sie unter Verwenden benutzerdefinierter Skripts.

7. Wählen Sie im **Task planen**eine der folgenden Optionen aus:

   - **Jetzt upgraden** - Der Upgrade-Auftrag wird sofort ausgeführt.
   - **Später planen** - Wählen Sie diese Option, um diesen Upgrade-Auftrag später auszuführen. Geben Sie das **Ausführungsdatum** und die **Startzeit** an, wenn Sie die Instanzen aktualisieren möchten.

   Wenn Sie ein NetScaler-Hochverfügbarkeitspaar in zwei Schritten aktualisieren möchten, wählen Sie Zweistufiges Upgrade für Knoten in HA durchführen aus.



Weitere Informationen finden Sie unter Upgrade des NetScaler-Hochverfügbarkeitspaars .

8. Geben Sie auf der Registerkarte **Job erstellen** die folgenden Details an:

   Wenn Sie den Upgrade-Auftrag planen, können Sie angeben, wann Sie das Image in eine Instanz hochladen möchten:

   - **Jetzt hochladen**: Wählen Sie diese Option, um das Image sofort hochzuladen. Der Upgrade-Auftrag wird jedoch zum geplanten Zeitpunkt ausgeführt.
   - **Zum Zeitpunkt des Ausführens hochladen**: Wählen Sie diese Option, um das Image hochzuladen, wenn der Upgradejob ausgeführt wird.

Weitere Informationen zu den anderen Optionen finden Sie unter NetScaler-Upgrade-Optionen .

Sicherheitsempfehlungen

January 26, 2024

Eine sichere und belastbare Infrastruktur ist die Lebensader jeder Organisation. Höhepunkte der Sicherheitsempfehlungen für NetScaler Console:

- **Erkennung und Behebung von Common Vulnerabilities and Exposures (CVEs)** —Ermöglicht

es Ihnen, die CVEs zu identifizieren, die Ihre NetScaler-Instanzen gefährden, und empfiehlt Abhilfemaßnahmen.

- **Dateiintegritätsüberwachung** —Ermöglicht es Ihnen, festzustellen, ob Änderungen oder Ergänzungen an Ihren NetScaler-Builddateien vorgenommen wurden.

Als Administrator müssen Sie Folgendes sicherstellen:

- Verfolgen Sie alle neuen Common Vulnerabilities and Exposures (CVEs), bewerten Sie die Auswirkungen von CVEs, verstehen Sie die Behebung und beheben Sie die Sicherheitslücken.
- Untersuchen Sie die Integrität Ihrer NetScaler-Build-Dateien.

Funktionen zur Sicherheitsberatung

Die folgenden Sicherheitsfunktionen helfen Ihnen beim Schutz Ihrer Infrastruktur.

CVEs:

Features	Beschreibung
Systemscan	Scannt standardmäßig alle verwalteten Instanzen einmal pro Woche. NetScaler Console entscheidet über Datum und Uhrzeit von Systemscans, und Sie können sie nicht ändern.
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.
CVE-Berichte	Speichert Kopien der letzten fünf Scans. Sie können diese Berichte im CSV-Format herunterladen und analysieren.

Features	Beschreibung
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.

Überwachung der Dateiintegrität:

Features	Beschreibung
Scannen auf Anforderung	Sie müssen einen Scan auf Anforderung ausführen, um Ergebnisse für alle Dateiänderungen zu erhalten, die in NetScaler-Builddateien erkannt wurden.
Scan zur Überwachung der Dateiintegrität	Vergleicht den binären Hashwert Ihrer aktuellen NetScaler-Build-Dateien mit dem ursprünglichen binären Hash und hebt hervor, ob Dateiänderungen oder Dateiergänzungen vorgenommen wurden. Sie können die Scanergebnisse auf der Registerkarte **Dateiintegritätsüberwachung** einsehen.

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.
- Für die Dateiintegritätsüberwachung unterstützte Instanzen: MPX-, VPX-Instanzen und Gateway.
- Unterstützte CVEs: Alle CVEs nach Dezember 2019.

> **Hinweis:**
>
> Die Erkennung und Behebung von Sicherheitslücken, die das NetScaler Gateway-Plug-in für Windows betreffen, wird von der NetScaler Console Security Advisory nicht unterstützt. Informationen zu CVEs, die nicht unterstützt werden, finden Sie unter Nicht unterstützte CVEs in Security Advisory.

- Die Sicherheitsempfehlung von NetScaler Console berücksichtigt bei der Identifizierung der Sicherheitsanfälligkeit keinerlei Fehlkonfigurationen von Funktionen.
- Die Sicherheitsempfehlung von NetScaler Console 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 ist NetScaler Console erforderlich, um die Version einer**NetScaler-Instanz mit den Versionen und Builds zu vergleichen, für die der Fix verfügbar ist. Dieser Versionsvergleich hilft der Sicherheitsempfehlung von NetScaler Console 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 Console 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 benötigt NetScaler Console, um eine Verbindung mit der verwalteten NetScaler-Instanz herzustellen, ein Skript darauf zu übertragen und das Skript auszuführen. Anhand der Skriptausgabe kann NetScaler Console 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.

- Der folgende Scan ist für die Dateiintegritätsüberwachung verfügbar:
  - ** Scan zur Überwachung der Dateiintegrität : Für diesen Scan ist die NetScaler Console erforderlich, um eine Verbindung mit der verwalteten NetScaler-Instanz herzustellen. NetScaler Console führt einen Vergleich der Hashwerte durch, indem sie ein Skript in NetScaler ausführt und die aktuellen binären Hashwerte für die NetScaler-Build-Dateien sammelt. Nach dem Vergleich liefert NetScaler Console das Ergebnis mit der Gesamtzahl der vorhandenen, geänderten Dateien und der Gesamtzahl der neu hinzugefügten Dateien. Als Administrator können Sie sich an die digitale Forensik Ihres Unternehmens wenden, um weitere Untersuchungen zu den Scanergebnissen zu erhalten.

    Die folgenden Dateien werden gescannt:

    * `/netscaler`
    * `/bin`, `/sbin`, `/usr/bin`, `/usr/sbin`, `/usr/local/bin`, `/usr/local/sbin`
    * `/lib`, `/libexec`, `/usr/lib`, `/usr/libexec`, `/usr/local/lib`, `/usr/lib32`, `/compat`
    * `/etc`
    * Der Rest von `/usr`
    * `/root`, `/home`, `/mnt`

- Scans wirken sich nicht auf den Produktionsdatenverkehr auf NetScaler aus und ändern keine NetScaler-Konfiguration auf NetScaler.
- Die NetScaler Console Security Advisory unterstützt keine CVE-Abwehr. Wenn Sie auf die NetScaler-Instanz eine Risikominderung (temporäre Problemumgehung) angewendet haben, identifiziert die NetScaler Console den NetScaler weiterhin als anfälligen NetScaler, bis Sie die Standardisierung abgeschlossen haben.
- Für die FIPS-Instanzen wird der CVE-Scan nicht unterstützt, aber der File Integrity Monitoring-Scan wird unterstützt.
- Einige Dateiänderungen können im Rahmen des normalen Betriebs des Geräts vorgenommen werden, während andere möglicherweise weitere Untersuchungen erfordern. Bei der Überprüfung von Dateiänderungen kann Folgendes hilfreich sein:

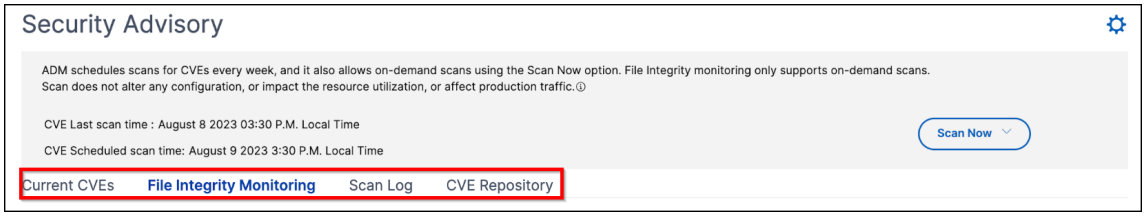
- Änderungen im `/netscaler` Verzeichnis (in **HTML** - und **JS-Dateien**) können durch die Verwendung von Skripten oder Plug-ins auftreten.
- Das `/etc` Verzeichnis enthält Konfigurationsdateien, die durch unerwartete Eingriffe nach dem Booten des Systems geändert werden können.
- Es wäre ungewöhnlich, wenn es:
  * Berichte in den Verzeichnissen `/bin`, `/sbin` oder `/lib`
  * Neue .php-Dateien im Verzeichnis `/netscaler`

So verwenden Sie das Sicherheits-Advisory-Dashboard

Um auf das **Security Advisory** Dashboard zuzugreifen, navigieren Sie von der NetScaler Console aus zu **Infrastructure > Instance Advisory > Security Advisory** .

Das Dashboard umfasst vier Registerkarten:

- Aktuelle CVEs
- Überwachung der Dateiintegrität
- 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. Um dieses Problem zu umgehen, klicken Sie auf **Jetzt scannen > CVEs scannen**, um einen Scan auf Anforderung auszuführen. Nachdem der Scan abgeschlossen ist, werden alle CVEs im Bereich (ungefähr 15) in der Benutzeroberfläche oder im Bericht angezeigt.

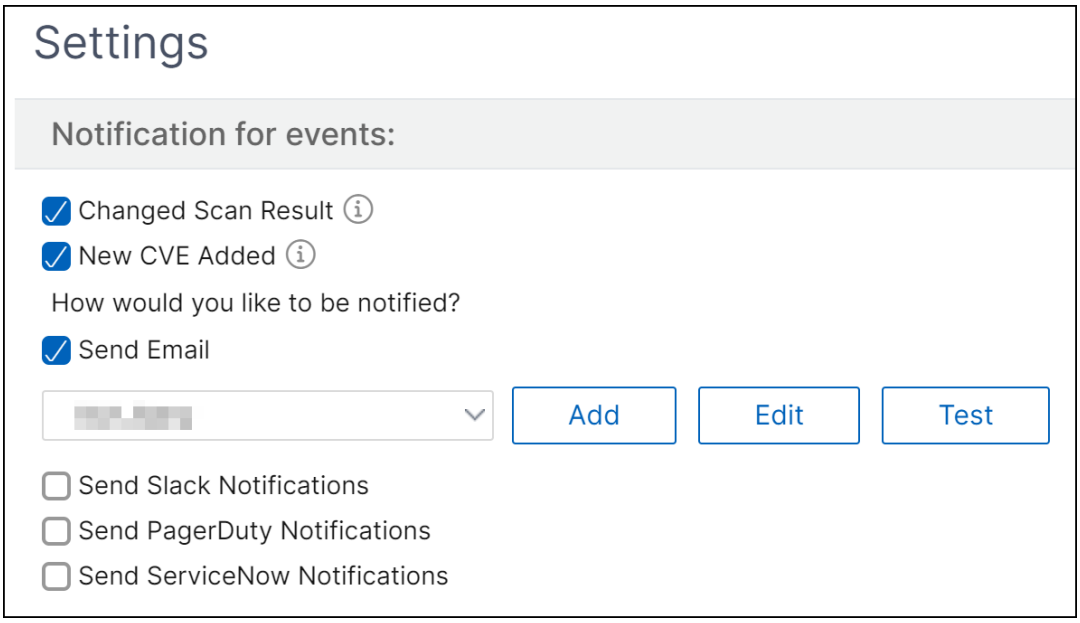
In der oberen rechten Ecke des Dashboards befindet sich das Einstellungssymbol, mit dem Sie:

- Benachrichtigungen aktivieren und deaktivieren (gilt nur für die CVE-Erkennung).

  Sie können die folgenden Benachrichtigungen über die Auswirkungen von CVE erhalten.

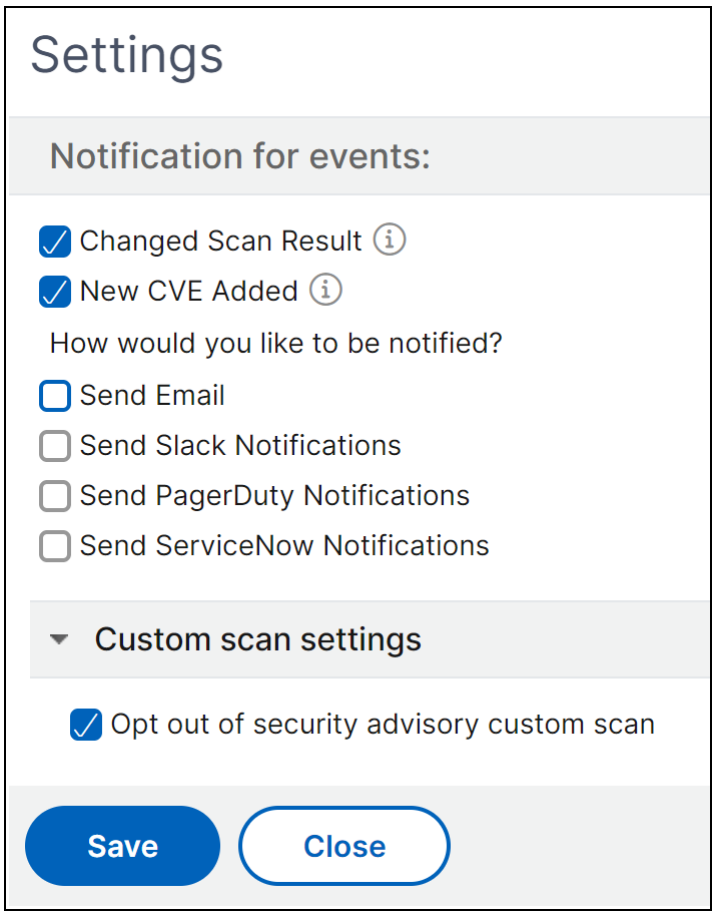
  - E-Mail-, Slack-, PagerDuty- und ServiceNow-Benachrichtigungen für Änderungen der CVE-Scanergebnisse und neue CVEs, die dem CVE-Repository hinzugefügt wurden.

- Cloud-Benachrichtigung für Änderungen der CVE-Impact-Scanergebnisse.



- Benutzerdefinierte Scaneinstellungen konfigurieren (gilt nur für CVEs)

  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.

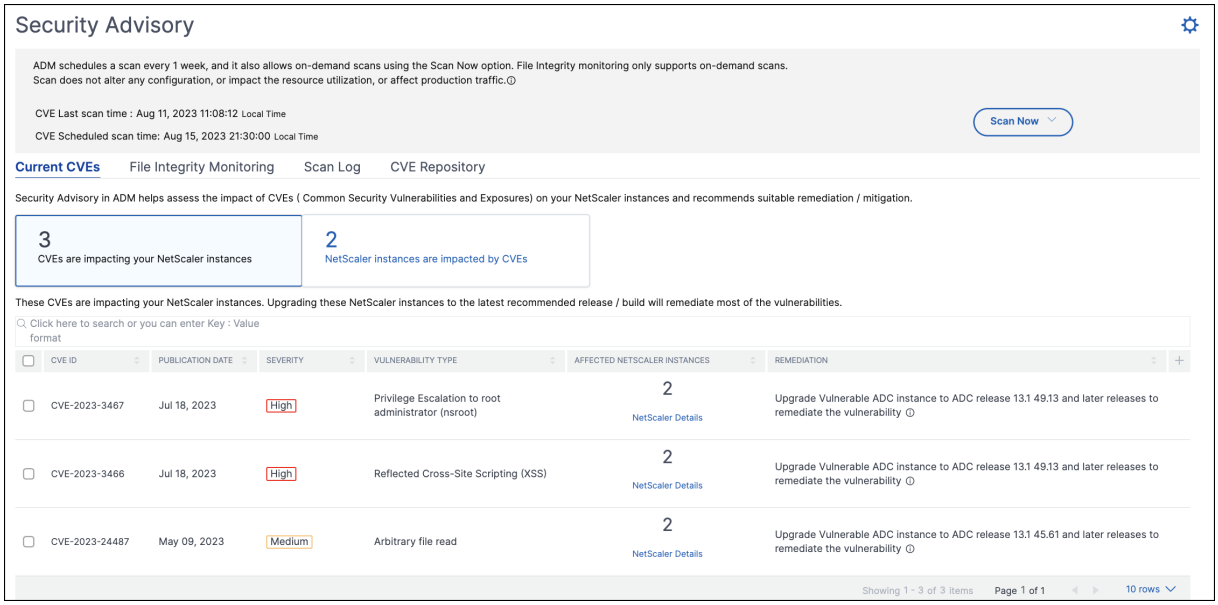
Schwachstellentyp: Die Art der Sicherheitsanfälligkeit für dieses CVE.

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.

Standardisierung: Die verfügbaren Standardisierungen, 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.

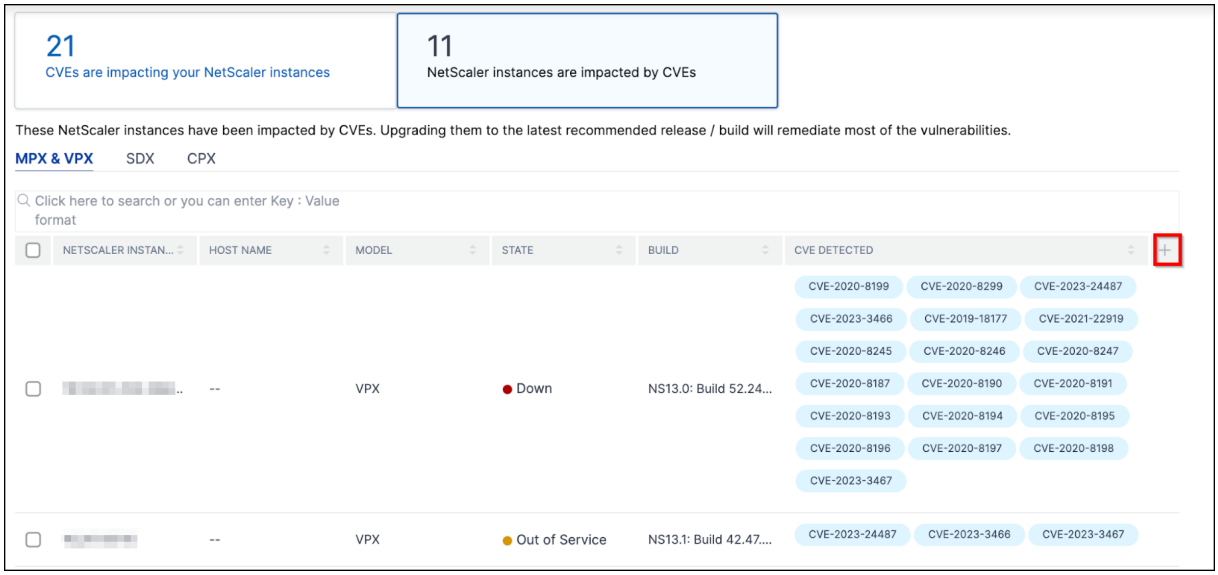
In diesem Bildschirm beträgt die Anzahl der CVEs, die sich auf Ihre Instanzen auswirken, 3 CVEs und die Anzahl der Instanzen, die von diesen CVEs betroffen sind, ist zwei.



Auf der Registerkarte **<number of>NetScaler-Instanzen sind von CVEs** betroffen werden alle betroffenen NetScaler Console NetScaler-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.

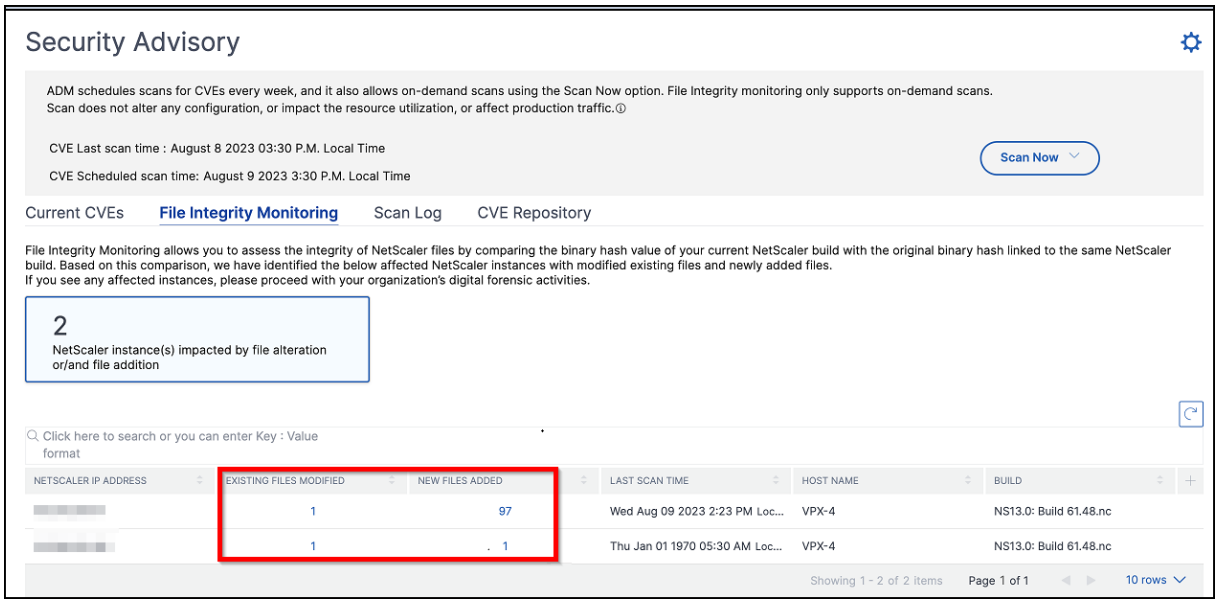
Der Upgrade-Workflow beginnt. Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Jobs zum Upgrade von NetScaler-Instanzen.

> **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.

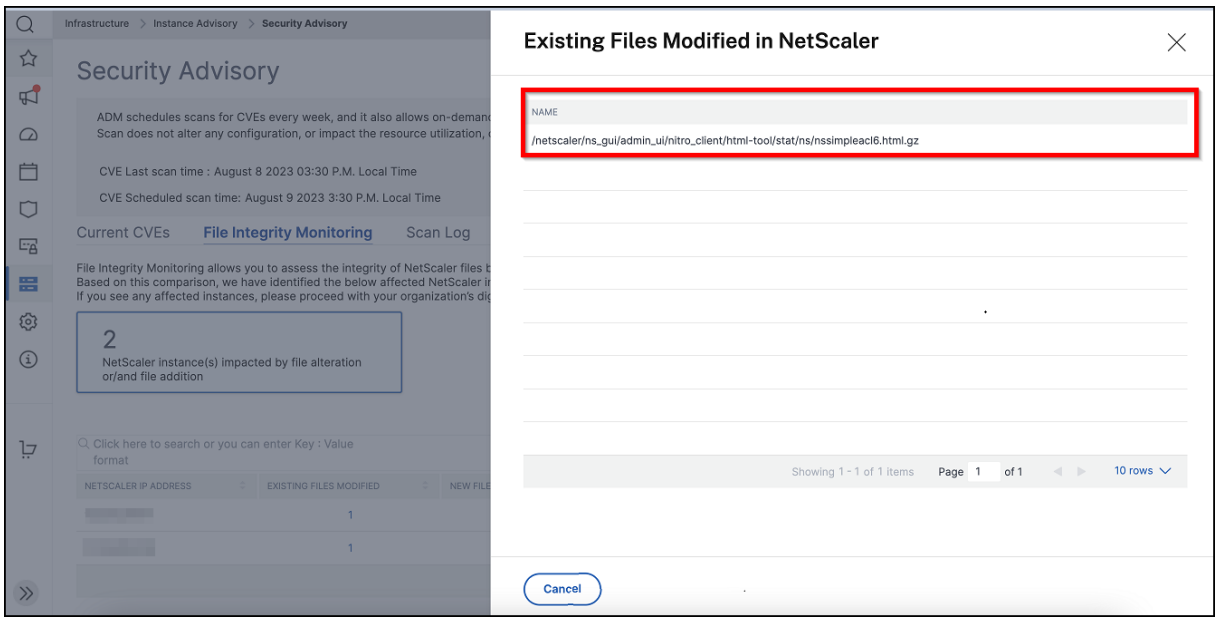
Überwachung der Dateiintegrität

Auf dieser Registerkarte wird das Ergebnis des File Integrity Monitoring-Scans mit NetScaler-Instanzen angezeigt, die Änderungen oder Ergänzungen zu den ursprünglichen NetScaler-Build-Dateien aufweisen.

Das folgende Beispiel zeigt das Scanergebnis für zwei betroffene NetScaler-Instanzen, bei denen vorhandene Dateien geändert und den ursprünglichen Build-Dateien neue Dateien hinzugefügt wurden.

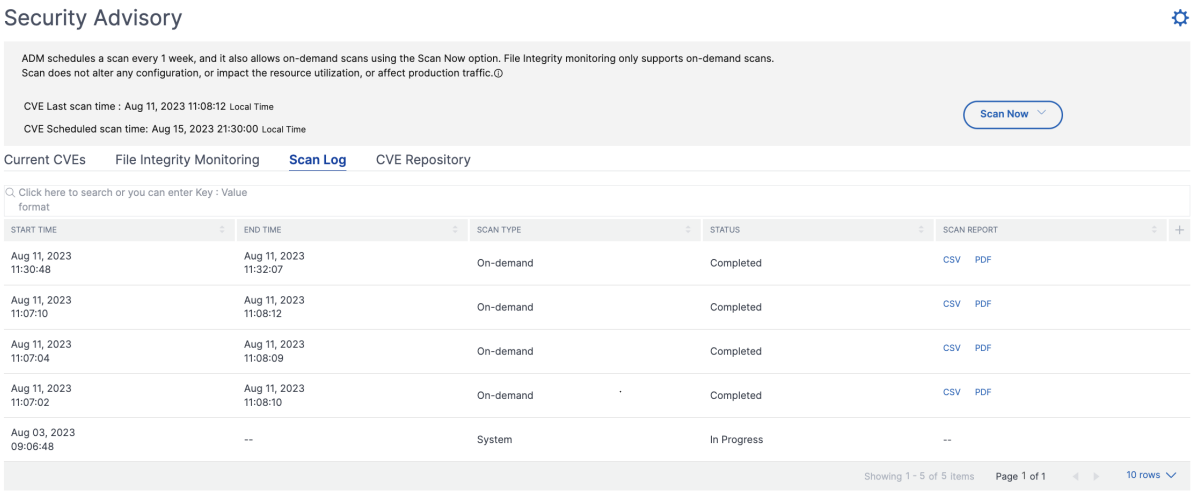


Klicken Sie auf die Zahlen unter **Bestehende Dateien geändert** und **Neue Dateien hinzugefügt**, um Details anzuzeigen.



Scanprotokoll (gilt nur für CVEs)

Auf der Registerkarte werden Berichte der letzten fünf CVE-Scans angezeigt, die sowohl Standardsystemscans als auch benutzerinitiierte On-Demand-Scans enthalten. Sie können den Bericht jedes Scans im CSV-Format herunterladen. Wenn ein Anforderungsscan läuft, können Sie den Abschlussstatus hier einsehen. Wenn ein Scan fehlgeschlagen ist, zeigt der Status dies an.

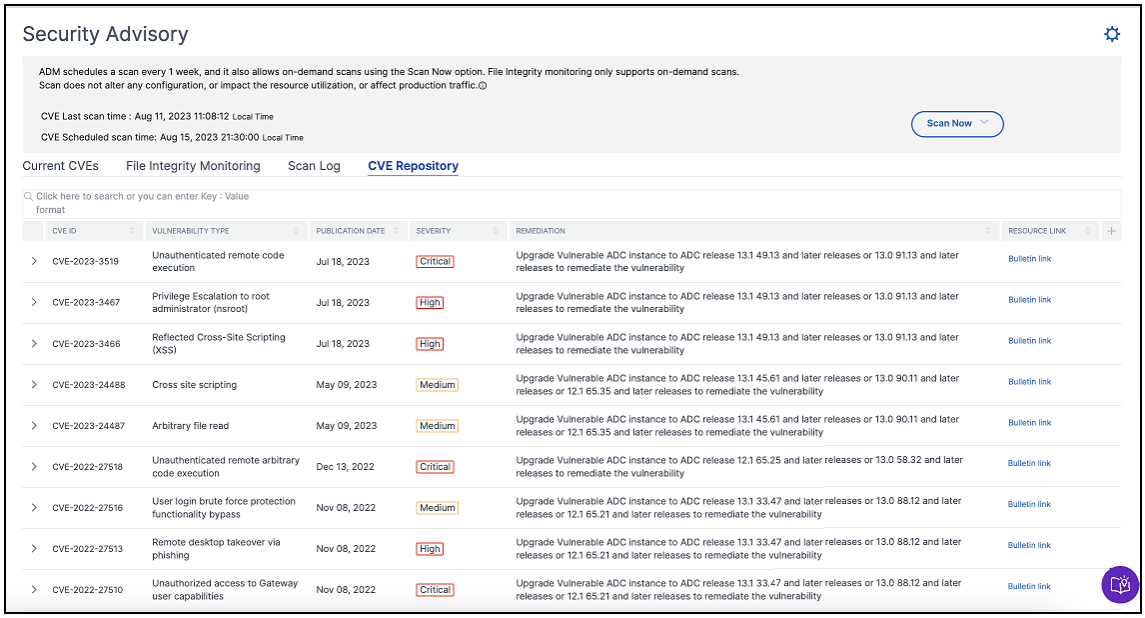


CVE-Repository

Diese Registerkarte enthält die neuesten Informationen aller CVEs ab Dezember 2019 sowie die folgenden Details:

- CVE-IDs

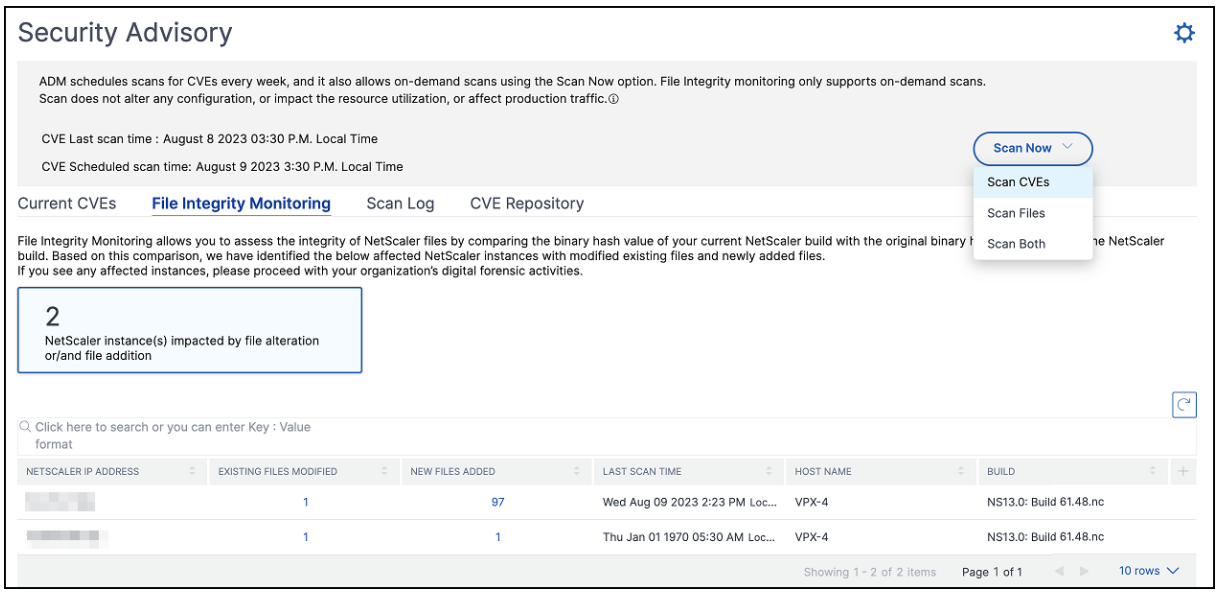
- Art der Sicherheitslücke
- Datum der Veröffentlichung
- Schweregrad
- Sanierung
- Links zu Sicherheitsbulletins



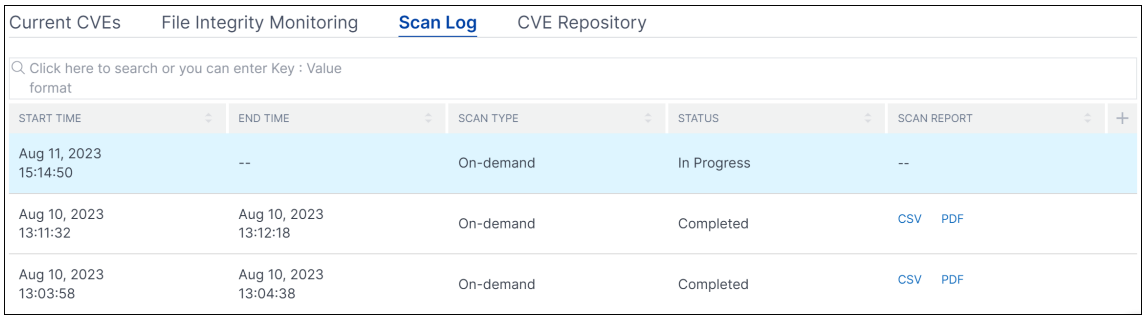
Jetzt durchsuchen

Sie können die Instanzen jederzeit nach Ihren Bedürfnissen scannen.

Klicken Sie auf **Jetzt scannen**und wählen Sie **CVEs scannen**, **Dateien scannen** oder **Beide scannen** aus, um den neuesten Sicherheitsbericht Ihrer Instanzen zu erhalten.



- **CVEs scannen** —Scannt nur nach CVEs, die sich auf Ihre NetScaler-Instanzen auswirken. Sobald der Scan abgeschlossen ist, werden die überarbeiteten Sicherheitsdetails in der Benutzeroberfläche für Sicherheitsempfehlungen angezeigt. Sie finden den Bericht auch unter **Scan-Protokoll**, das Sie auch herunterladen können.



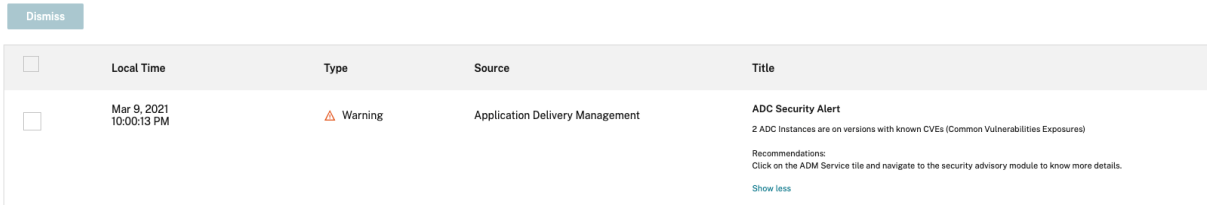
- **Dateien scannen** —Scannt nur nach der Dateiintegritätsüberwachung und zeigt das Ergebnis auf der Registerkarte **Dateiintegritätsüberwachung** an.
- **Beide scannen** —Scannt sowohl auf die CVE-Erkennung als auch auf die Überwachung der Dateiintegrität

Die NetScaler Console benötigt einige Minuten, um den Scan abzuschließen.

> **Hinweis**
>
> Das Scanprotokoll zeigt nur die Protokolle der letzten fünf CVE-Scans an, die sowohl geplant als auch auf Anfrage durchgeführt werden können.

Benachrichtigung (gilt nur für CVEs)

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 Console-GUI.

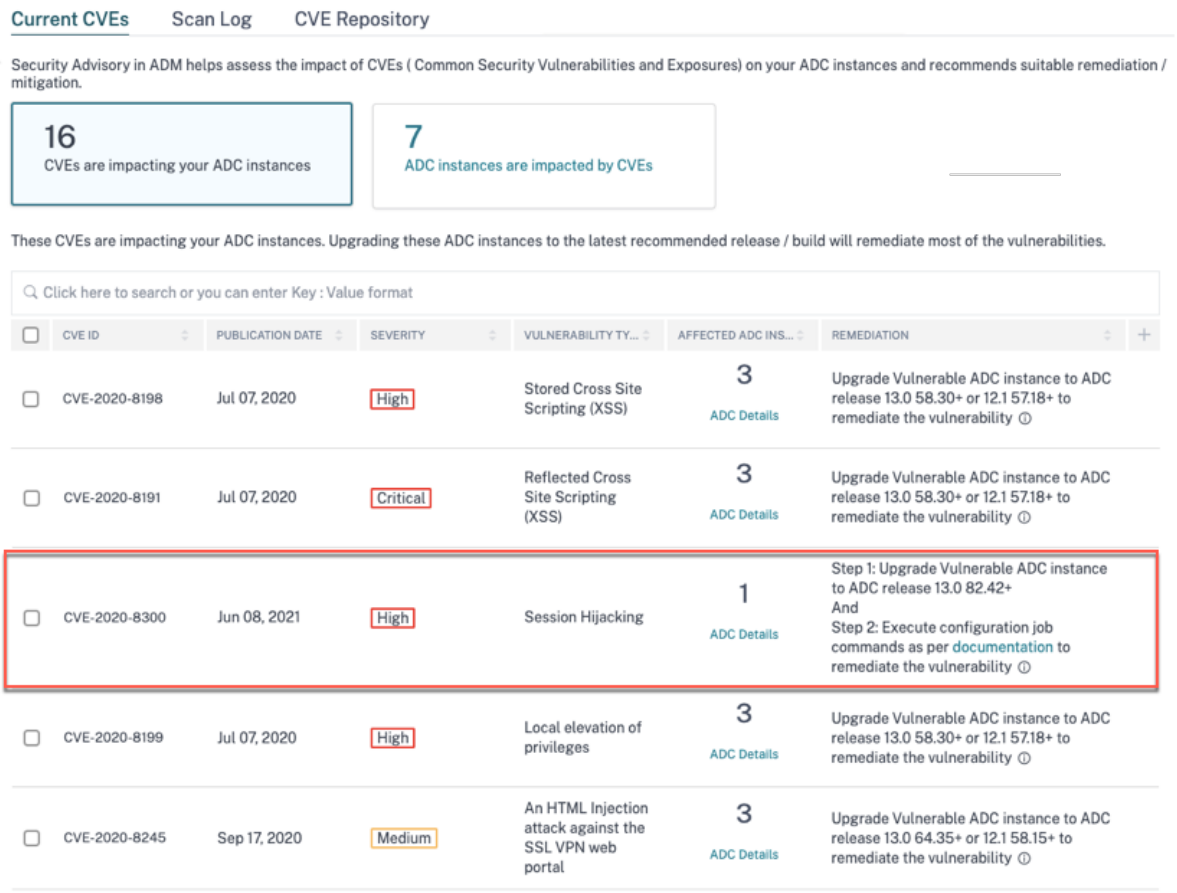


> **Haftungsausschluss:**
>
> Bitte beachten Sie, dass NetScaler File Integrity Monitoring ("das Feature") nicht in der Lage ist, alle Techniken, Taktiken oder Verfahren (TTPs) zu erkennen, die Bedrohungsakteure möglicherweise verwenden, um relevante Umgebungen ins Visier zu nehmen. Bedrohungsakteure ändern häufig TTPs und Infrastruktur, weshalb die Funktion in Bezug auf bestimmte Bedrohungen möglicherweise von begrenztem bis gar keinem forensischen Wert ist. Es wird dringend empfohlen, die Dienste erfahrener forensischer Ermittler in Anspruch zu nehmen, um Ihre Umgebung im Zusammenhang mit möglichen Bedrohungen zu bewerten.
>
> Dieses Dokument und die darin enthaltenen Informationen werden unverändert zur Verfügung gestellt. Cloud Software Group, Inc. gibt keine ausdrücklichen oder stillschweigenden Garantien oder Zusicherungen in Bezug auf das Dokument oder seinen Inhalt ab, einschließlich, aber nicht beschränkt auf die Tatsache, dass dieses Dokument oder die darin enthaltenen Informationen fehlerfrei sind oder irgendwelche Bedingungen der Marktgängigkeit oder Eignung für einen bestimmten Zweck erfüllen.

Sicherheitsrisiko CVE-2020-8300 korrigieren

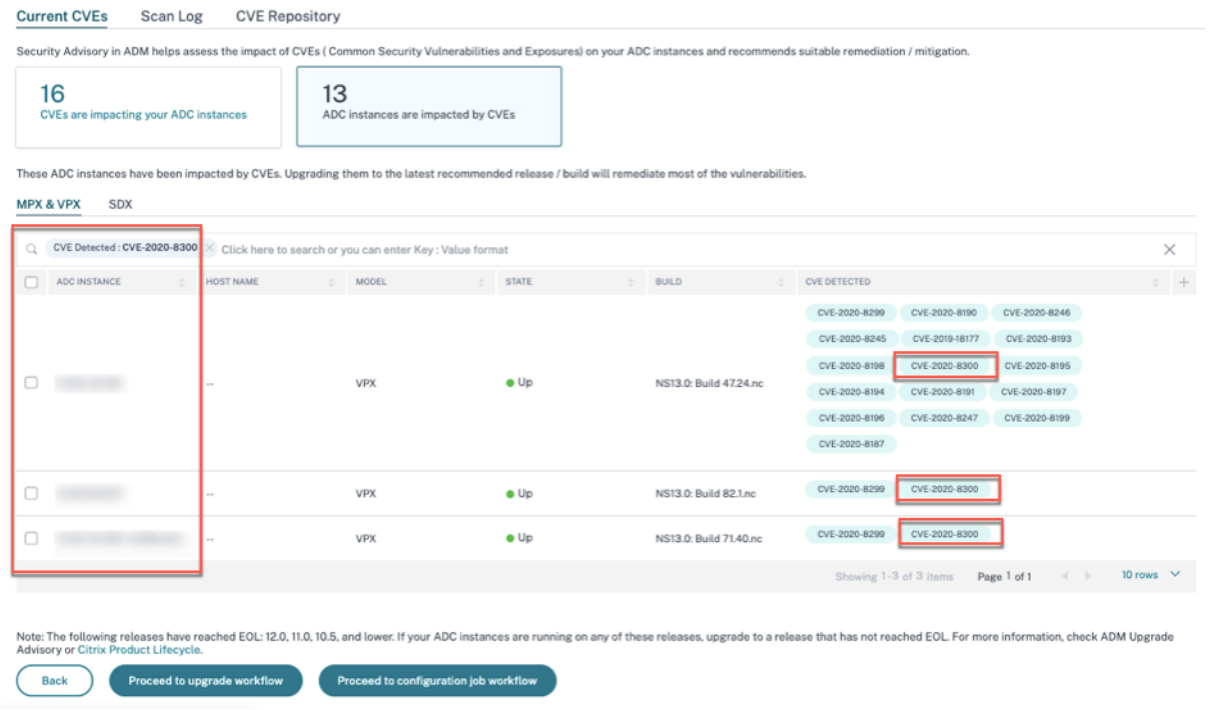
January 26, 2024

Im NetScaler Console Security Advisory Dashboard können Sie unter **Aktuelle CVEs > <`number of`> NetScaler-Instanzen sind von CVEs betroffen** alle Instanzen sehen, die aufgrund dieser spezifischen 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**.



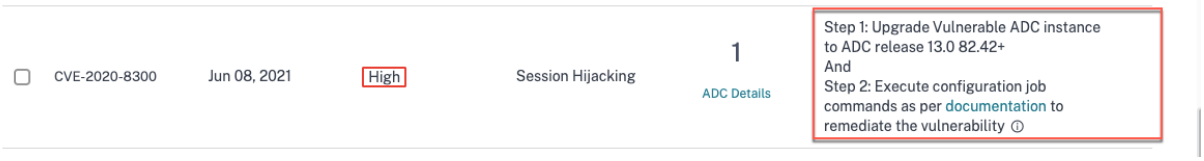
> **Hinweis**
>
> Weitere Informationen zum Security Advisory Dashboard finden Sie unter Security Advisory.

Das Fenster **<number of>NetScaler-Instanzen, die von CVEs betroffen** sind, wird angezeigt. Hier sehen Sie die Anzahl und Details der NetScaler-Instanzen, die von CVE-2020-8300 betroffen sind.



CVE-2020-8300 korrigieren

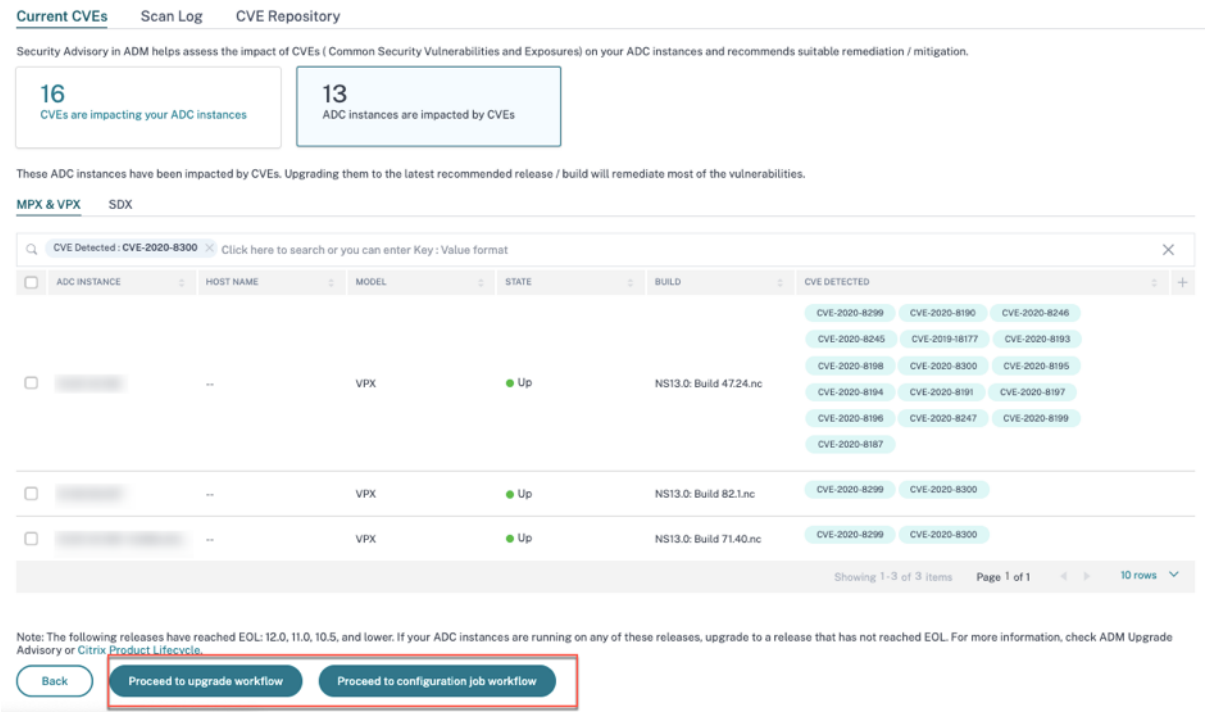
Für NetScaler-Instanzen, die von CVE-2020-8300 betroffen sind, besteht die Behebung aus zwei Schritten. In der GUI können Sie unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen** die Schritte 1 und 2 sehen.



Die zwei Schritte beinhalten:

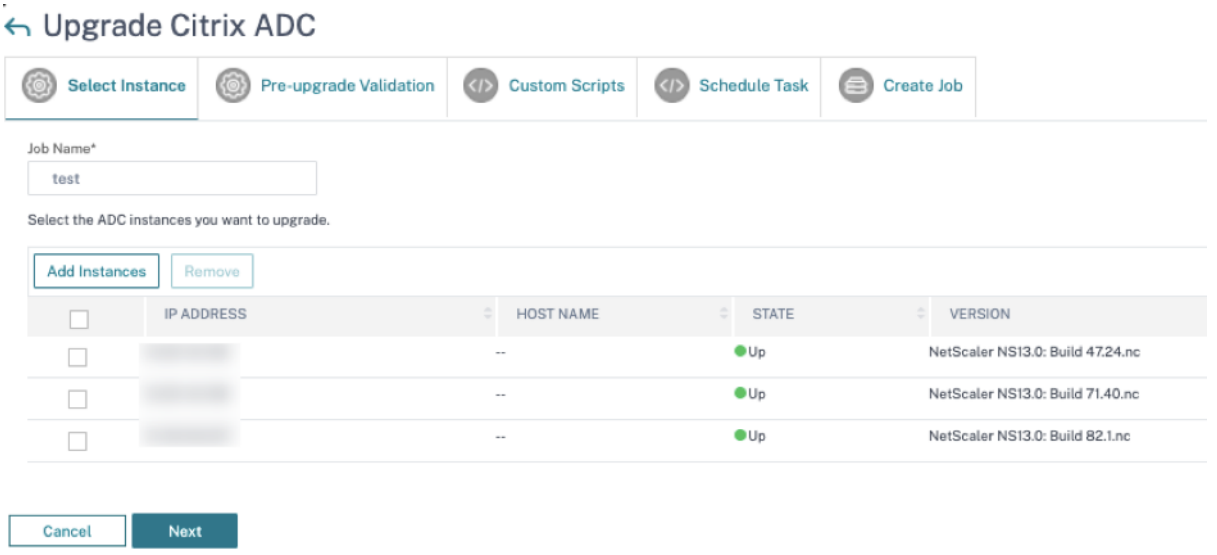
1. Aktualisierung der anfälligen NetScaler-Instanzen auf eine Version und einen Build, die den Fix enthalten.
2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen. Folgen Sie diesen Schritt für jeden anfälligen NetScaler nacheinander und schließen Sie alle SAML-Aktionen und SAML-Profile für diesen NetScaler ein.

Unter **Aktuelle CVEs > NetScaler-Instanzen, die von CVEs betroffen** sind, sehen Sie zwei separate Workflows für diesen zweistufigen Korrekturprozess: **Weiter zum Upgrade-Workflow** und **Weiter zum Konfigurationsjob-Workflow**.



Schritt 1: Aktualisieren Sie die anfälligen NetScaler-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 anfälligen NetScaler-Instanzen geöffnet, die bereits gefüllt sind.



Weitere Informationen zur Verwendung der NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Jobs.

> **Hinweis**
>
> Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig ausgeführt werden.

Schritt 2: Anwenden von Konfigurationsbefehlen

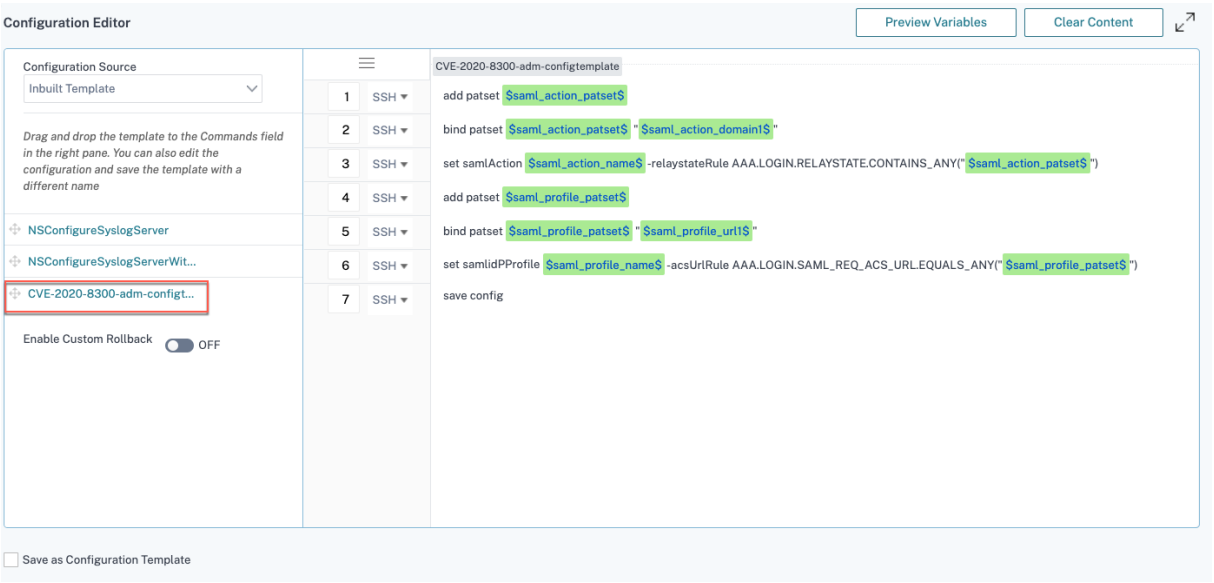
Nachdem Sie die betroffenen Instanzen aktualisiert haben, wählen Sie im Fenster **<number of> NetScaler-Instanzen, die von CVEs betroffen** sind, eine Instance aus, die von CVE-2020-8300 betroffen ist, und klicken Sie auf **Weiter zum Konfigurationsjob-Workflow**. Der Workflow umfasst die folgenden Schritte.

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 NetScaler-Instanz, die von mehreren CVEs betroffen ist (wie CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 und CVE-2021-22956): Wenn Sie die Instanz auswählen und auf Weiter zum Konfigurationsauftrags-Workflow** 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.
- Nur für mehrere NetScaler-Instanzen, die von CVE-2021-22956 betroffen sind: Sie können Konfigurationsaufträge auf allen Instanzen gleichzeitig ausführen. Sie haben beispielsweise NetScaler 1, NetScaler 2 und NetScaler 3, und alle 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.
- **Für mehrere NetScaler-Instanzen, die von CVE-2021-22956 und einer oder mehreren anderen CVEs betroffen sind (wie CVE-2020-8300, CVE-2021-22927 und CVE-2021-22920), die eine Korrektur erfordern, um auf jedem NetScaler gleichzeitig angewendet zu werden: Wenn Sie diese Instanzen auswählen und auf Weiter zum Konfigurationsauftrags-Workflow** klicken, wird eine Fehlermeldung angezeigt, die Sie auffordert, den Konfigurationsjob auf jedem NetScaler gleichzeitig auszuführen.

Schritt 1: Konfiguration wählen Im Workflow des Konfigurationsauftrags wird die integrierte Konfigurationsvorlage automatisch unter **Konfiguration auswählen**ausgefüllt.



Führen Sie für jede betroffene NetScaler-Instanz nacheinander einen separaten Konfigurationsjob aus und schließen Sie alle SAML-Aktionen und SAML-Profile für diesen NetScaler ein. Wenn Sie beispielsweise zwei anfällige NetScaler-Instanzen mit jeweils zwei SAML-Aktionen und zwei SAML-Profilen haben, müssen Sie diesen Konfigurationsjob zweimal ausführen. Einmal pro NetScaler, der alle SAML-Aktionen und SAML-Profile abdeckt.

NetScaler 1	NetScaler 2
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.

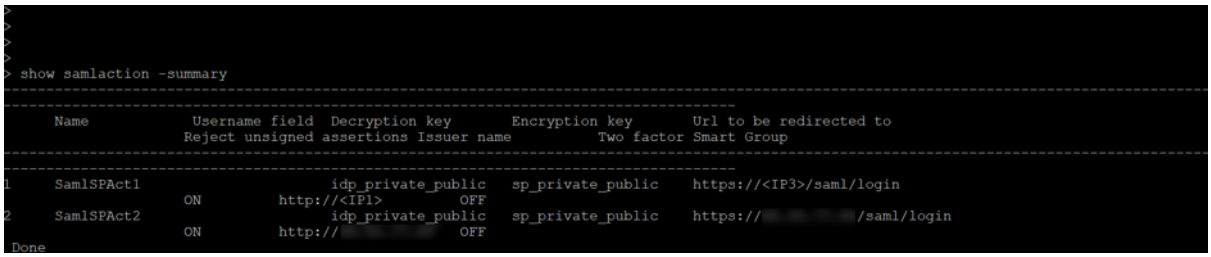
1	SSH	add patset $saml_action_patset$
2	SSH	bind patset $saml_action_patset$ " $saml_action_domain1$ "
3	SSH	set samlAction $saml_action_name$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY(" $saml_action_patset$ ")
4	SSH	add patset $saml_profile_patset$
5	SSH	bind patset $saml_profile_patset$ " $saml_profile_url1$ "
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-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:

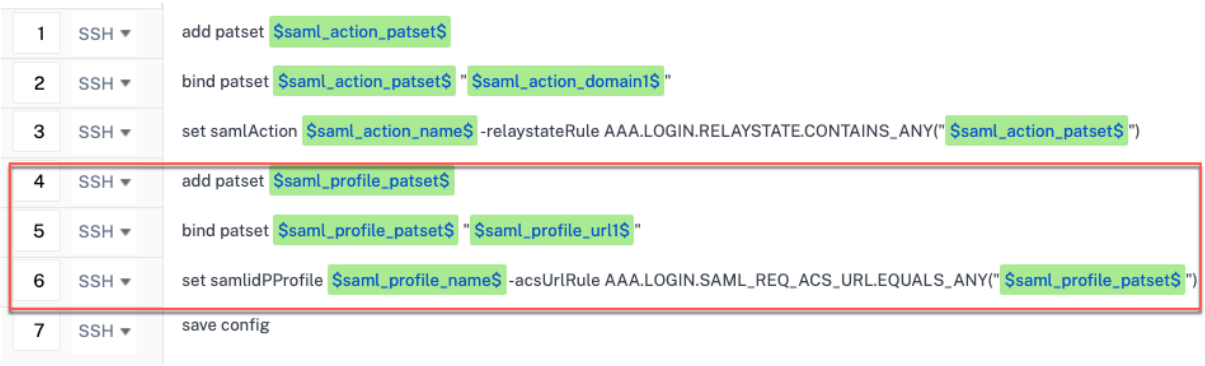
- `saml_action_patset`: ist die Konfigurations-Template-Variable und stellt den Wert des Namens des Mustersatzes (patset) für die SAML-Aktion dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsjob-Workflows angeben. Weitere Informationen finden Sie im Abschnitt Schritt 3: Variablenwerte 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`.



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.



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.

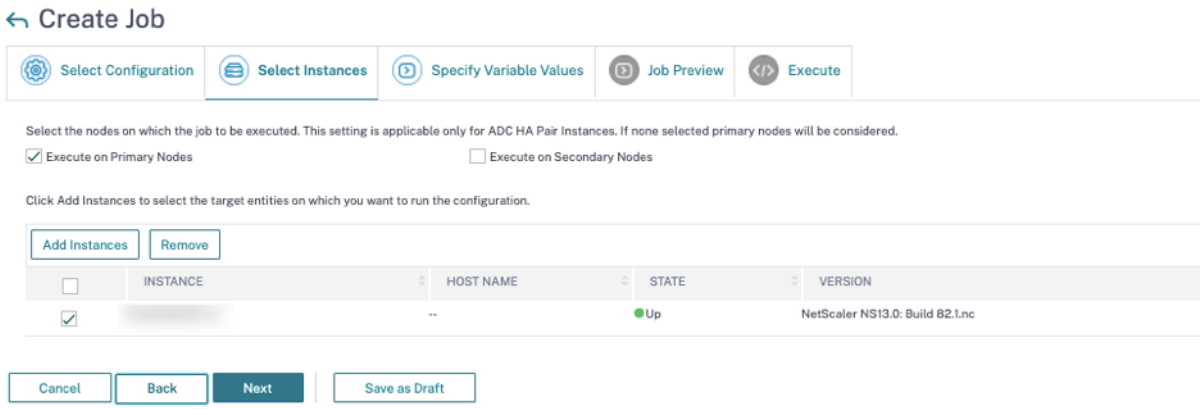
Und wenn Sie N Domänen für eine SAML-Aktion haben, müssen Sie die Zeile `bind patset $saml_profile_patset$ “$saml_profile_url1$”` mehrmals manuell eingeben, um sicherzustellen, dass die Zeile N Mal für dieses SAML-Profil angezeigt wird. Und ändern Sie die folgenden Variablendefinitionsnamen:

- `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

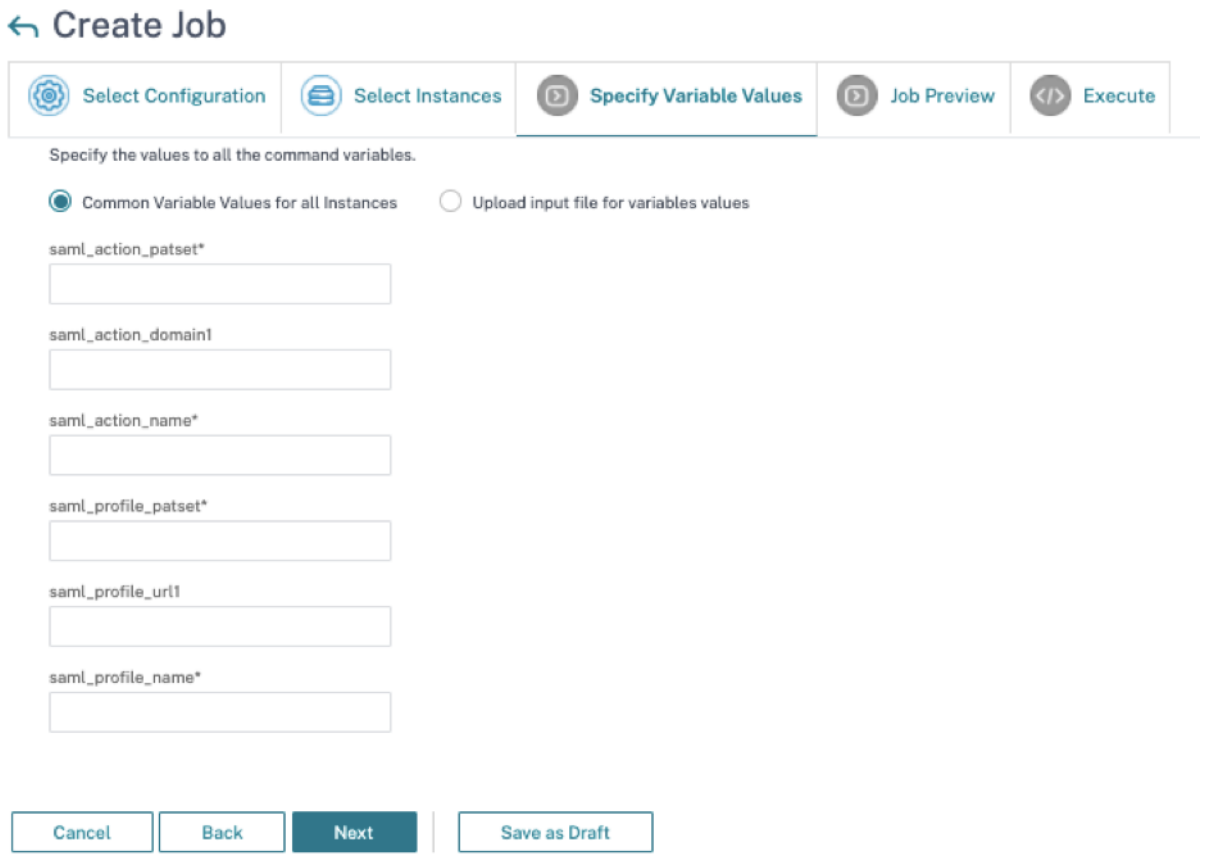
Die betroffene Instanz wird automatisch unter **Ausgewählte Instanzen**aufgefüllt. Wählen Sie die Instanz und klicken Sie auf **Weiter**.



Schritt 3: Variablenwerte angeben Geben Sie die Werte der Variablen ein.

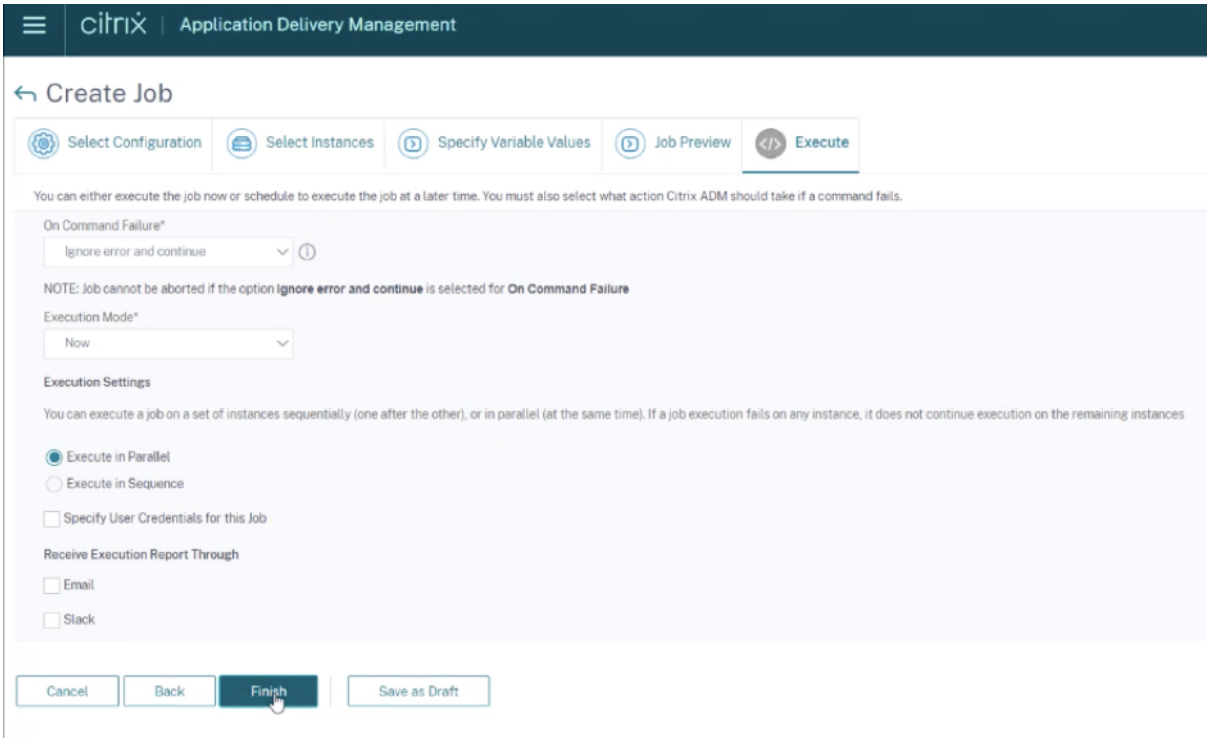
- `saml_action_patset`: Namen für die SAML-Aktion hinzufügen
- `saml_action_domain1`: Domäne im Format `https://<example1.com>/` eingeben
- `saml_action_name`: Dieselbe SAML-Aktion eingeben, für die Sie den Job konfigurieren
- `saml_profile_patset`: Namen für das SAML-Profil hinzufügen
- `saml_profile_url1`: 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 Schritte zur Behebung aller anfälligen NetScaler-Instanzen abgeschlossen haben, können Sie einen On-Demand-Scan ausführen, um die überarbeitete Sicherheitslage zu überprüfen.

Zu beachtende Punkte für das NetScaler Console Express-Konto

Das NetScaler Console Express-Konto verfügt über eingeschränkte Funktionen, einschließlich der Beschränkung auf nur zwei Konfigurationsaufträge. Weitere Informationen zum NetScaler Console Express-Konto finden Sie unter NetScaler Console-Ressourcen mithilfe des Express-Kontos verwalten
.

Für die CVE-2020-8300-Wiederherstellung müssen Sie so viele Konfigurationsaufträge ausführen, wie die Anzahl Ihrer anfälligen NetScaler-Instanzen entspricht. Wenn Sie also ein Express-Konto haben und mehr als zwei Konfigurationsaufträge ausführen müssen, befolgen Sie diese Problemumgehung.

**** Problemumgehung : Führen Sie zwei Konfigurationsaufträge für zwei anfällige NetScaler-Instanzen aus und löschen Sie dann beide Jobs, um die nächsten beiden Jobs für die nächsten beiden anfälligen NetScaler-Instanzen fortzusetzen. 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**

> Jobsdie Jobs aus und klicken Sie unter **Aktionen** auf **Herunterladen**.

Beispiel: Wenn Sie sechs anfällige NetScaler-Instanzen haben, führen Sie zwei Konfigurationsaufträge auf jeweils 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 NetScaler-Instanzen ausgeführt. In der NetScaler Console-Benutzeroberfläche unter **Infrastruktur > Jobs** werden nur die letzten beiden Konfigurationsaufträge angezeigt.

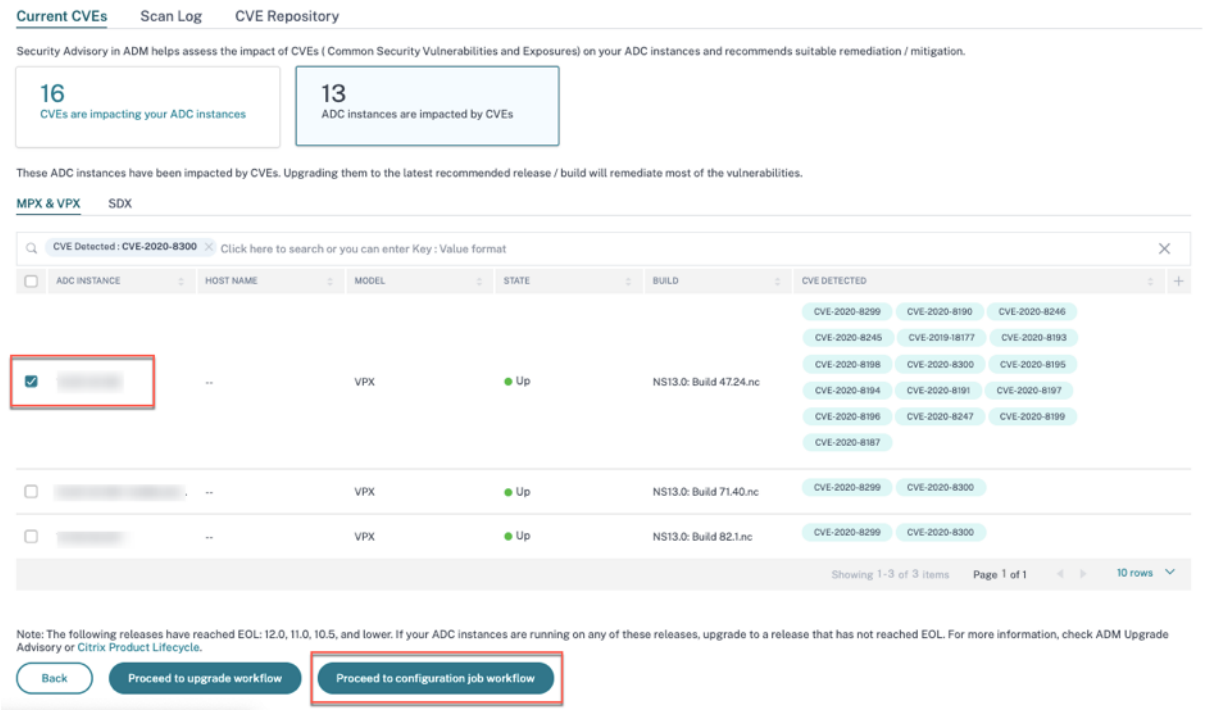
Szenario

In diesem Szenario sind drei NetScaler-Instanzen anfällig für CVE-2020-8300, und Sie müssen alle Instanzen reparieren. Führen Sie die folgenden Schritte aus:

1. Führen Sie ein Upgrade aller drei NetScaler-Instanzen durch, indem Sie die Schritte im Abschnitt **Eine Instanz** aktualisieren in diesem Dokument befolgen.
2. Wenden Sie den Konfigurationspatch mithilfe des Konfigurationsauftragsworkflows jeweils auf einen NetScaler an. Sehen Sie sich die Schritte an, die im Abschnitt **Konfigurationsbefehle anwenden** in diesem Dokument beschrieben werden.

Der anfällige NetScaler 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 NetScaler 1 aus und klicken Sie auf Weiter zum Workflow für den Konfigurationsauftrag .** 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

NetScaler-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

NetScaler-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** die Option NetScaler 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.

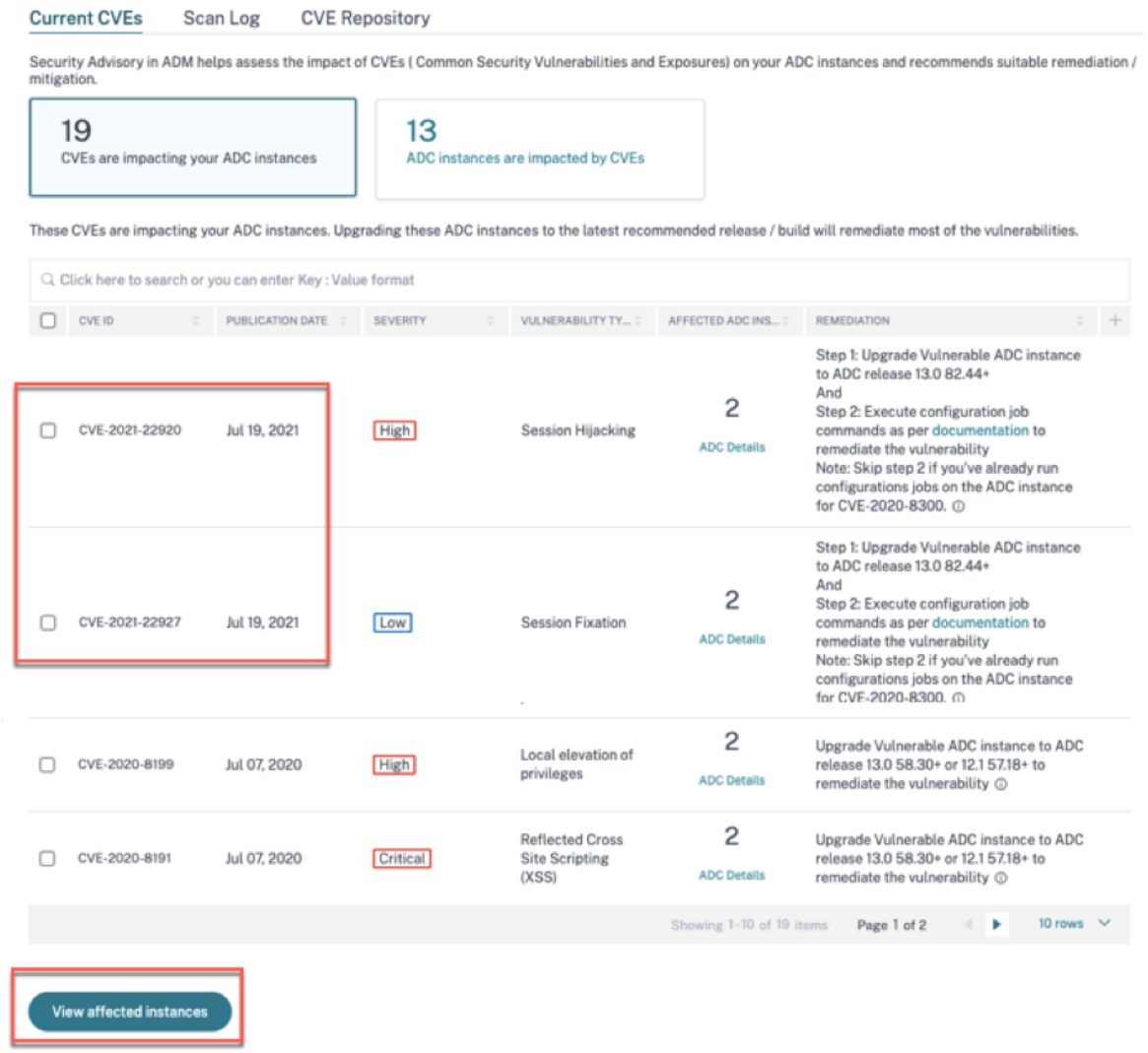
Nachdem der Job ausgeführt wurde, wird er unter **Infrastruktur > Konfiguration > Konfigurationsjobs**angezeigt.

Nachdem Sie die beiden Standardisierungsschritte für NetScaler 1 abgeschlossen haben, führen Sie dieselben Schritte aus, um NetScaler 2 und NetScaler 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

January 26, 2024

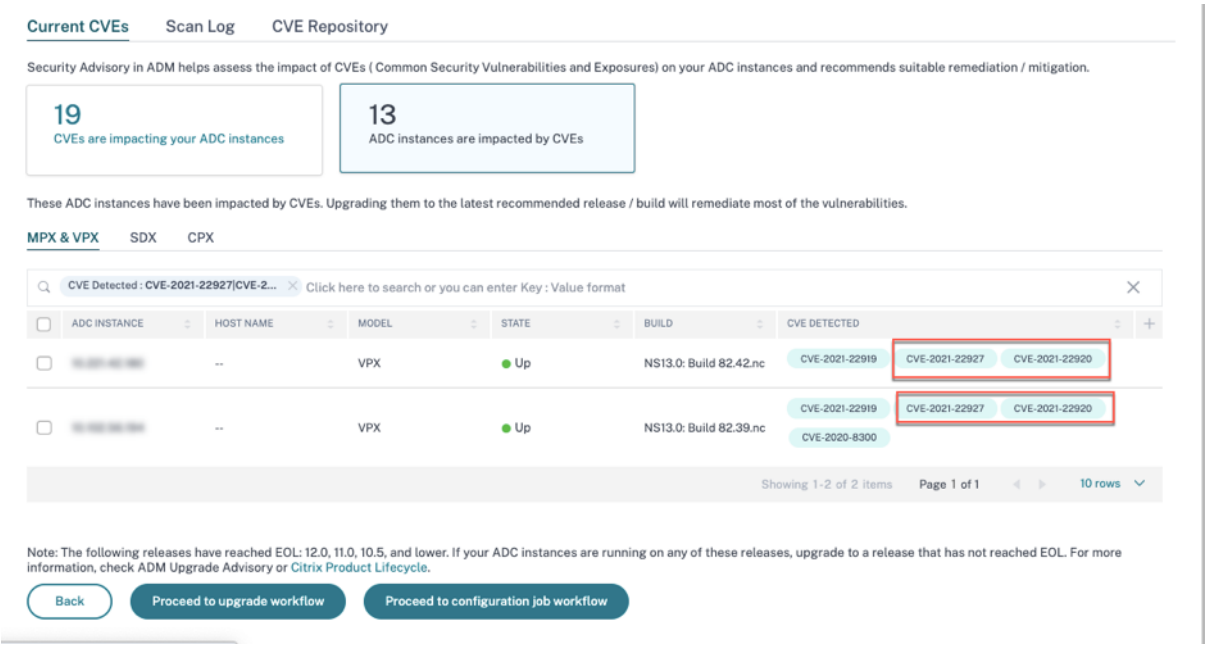
Im NetScaler Console Security Advisory Dashboard können Sie unter **Aktuelle CVEs > <number of >NetScaler-Instanzen sind von CVEs betroffen** alle Instanzen sehen, die aufgrund von CVE-2021-22927 und CVE-2021-22920 anfällig sind. Um die Details der Instanzen zu überprüfen, die von diesen beiden CVEs betroffen sind, wählen Sie mindestens eine CVEs aus und klicken Sie auf **Betroffene Instanzen anzeigen**.



Hinweis

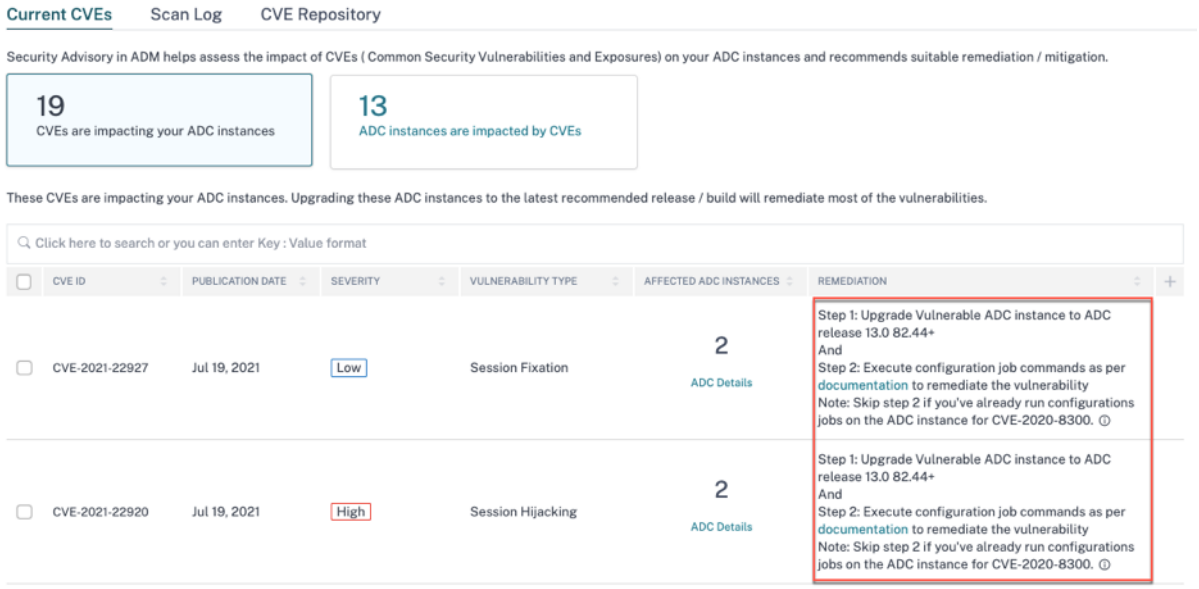
Es kann einige Stunden dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2021-22927 und CVE-2021-22920 im Sicherheitsberatungsmodul widerspiegelt. Um die Auswirkungen früher zu erkennen, starten Sie einen Anforderungsscan, indem Sie auf **Jetzt scannen**klicken.
Weitere Informationen zum Security Advisory Dashboard finden Sie unter Security Advisory .

Das Fenster **<number of>NetScaler-Instanzen, die von CVEs betroffen** sind, wird angezeigt. In der folgenden Bildschirmaufnahme sehen Sie die Anzahl und Details der NetScaler-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 NetScaler-Instanzen erfolgt die Behebung in zwei Schritten. In der GUI können Sie unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen** die Schritte 1 und 2 sehen.



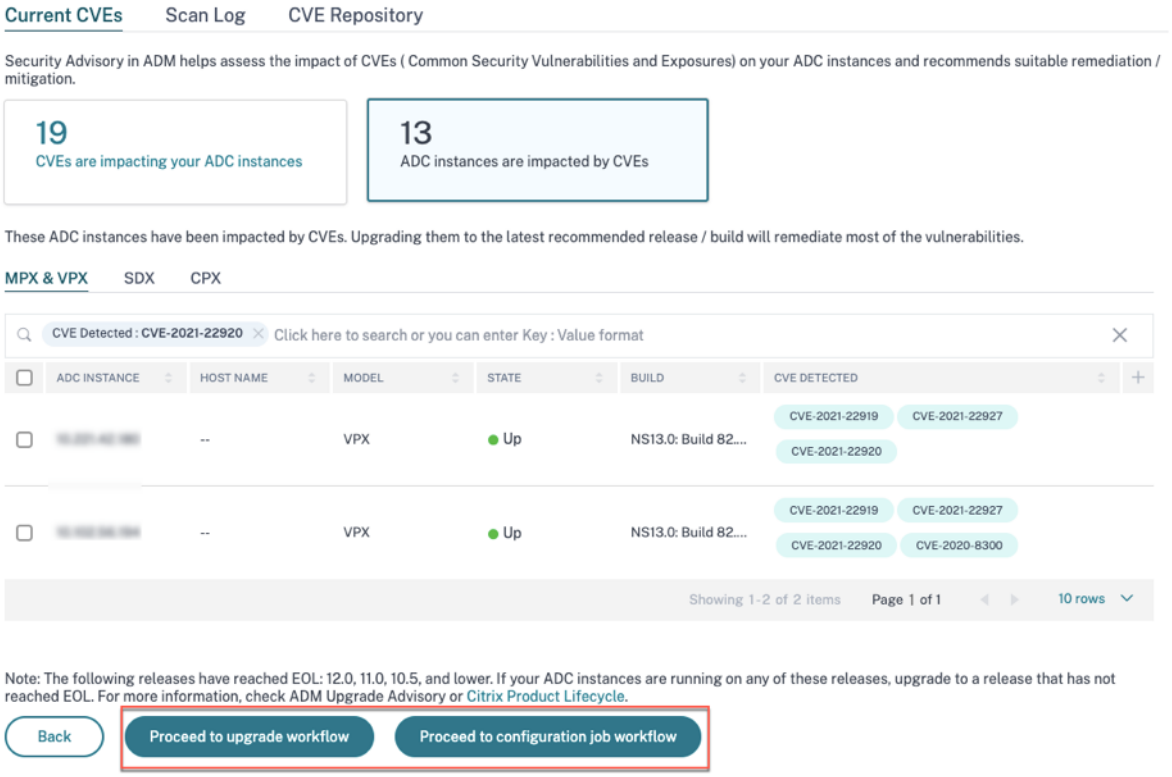
Die zwei Schritte beinhalten:

1. Aktualisierung der anfälligen NetScaler-Instanzen auf eine Version und einen Build, die den Fix enthalten.

2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen. Folgen Sie diesen Schritt für jeden anfälligen NetScaler nacheinander und schließen Sie alle SAML-Aktionen für diesen NetScaler ein.

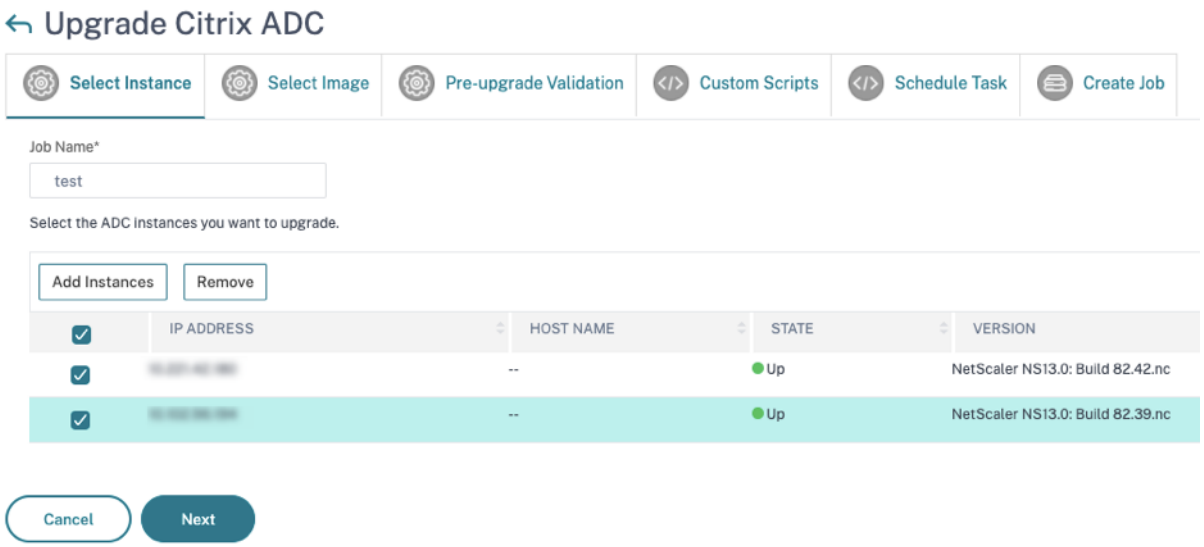
> **Hinweis**
>
> Überspringen Sie Schritt 2, wenn Sie bereits Konfigurationsaufträge auf der NetScaler-Instanz für CVE-2020-8300 ausgeführt haben.

Unter **Aktuelle CVEs > NetScaler-Instanzen, die von CVEs betroffen** sind, sehen Sie zwei separate Workflows für diesen zweistufigen Korrekturprozess: **Weiter zum Upgrade-Workflow** und **Weiter zum Konfigurationsjob-Workflow**.



Schritt 1: Aktualisieren Sie die anfälligen NetScaler-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 anfälligen NetScaler-Instanzen geöffnet, die bereits gefüllt sind.



Weitere Informationen zur Verwendung der NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Jobs.

> **Hinweis**
>
> Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig ausgeführt werden.
>
> **Hinweis**
>
> Nachdem Sie Schritt 1 für alle NetScaler-Instanzen abgeschlossen haben, die für CVE-2021-22920 und CVE-2021-22927 anfällig sind, führen Sie einen On-Demand-Scan durch. Die aktualisierte Sicherheitslage unter **Aktuelle CVEs** hilft Ihnen zu verstehen, ob die NetScaler-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 Konfigurationsaufträge auf die NetScaler-Instanz für CVE-2020-8300 angewendet haben und jetzt die NetScaler-Instanz aktualisiert haben, wird die Instanz nach dem On-Demand-Scan 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> NetScaler-Instanzen, die von CVEs betroffen** sind, eine Instance aus, die von CVE-2021-22927 und CVE-2021-22920 betroffen ist, und klicken Sie auf **Weiter zum Konfigurationsjob-Workflow**. Der Workflow umfasst die folgenden Schritte.

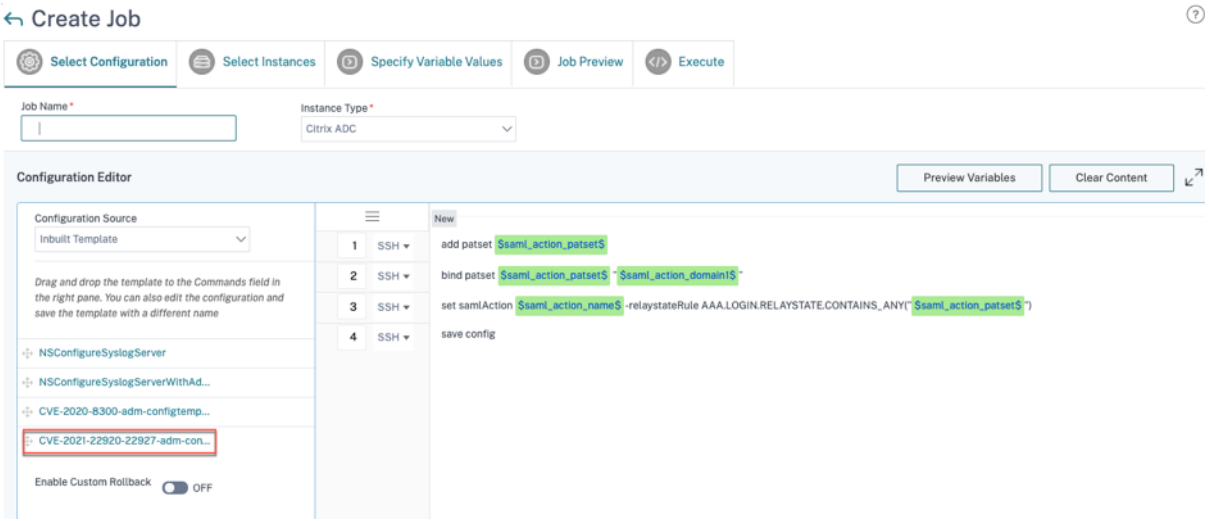
1. Anpassen der Konfiguration.
2. Überprüfung der automatisch ausgefüllten betroffenen Instanzen.
3. Angabe von Eingaben für Variablen für den Job.

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 NetScaler-Instanz, die von mehreren CVEs betroffen ist (wie CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 und CVE-2021-22956): Wenn Sie die Instanz auswählen und auf Weiter zum Konfigurationsauftrags-Workflow** 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.
- Nur für mehrere NetScaler-Instanzen, die von CVE-2021-22956 betroffen sind: Sie können Konfigurationsaufträge auf allen Instanzen gleichzeitig ausführen. Sie haben beispielsweise NetScaler 1, NetScaler 2 und NetScaler 3, und alle 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.
- **Für mehrere NetScaler-Instanzen, die von CVE-2021-22956 und einer oder mehreren anderen CVEs betroffen sind (wie CVE-2020-8300, CVE-2021-22927 und CVE-2021-22920), die eine Korrektur erfordern, um auf jedem NetScaler gleichzeitig angewendet zu werden: Wenn Sie diese Instanzen auswählen und auf Weiter zum Konfigurationsauftrags-Workflow** klicken, wird eine Fehlermeldung angezeigt, die Sie auffordert, den Konfigurationsjob auf jedem NetScaler 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 NetScaler-Instanz anfällig für CVE-2021-22927, CVE-2021-22920 und auch CVE-2020-8300 ist, wird die Basisvorlage für CVE-2020-8300 automatisch gefüllt. Die Vorlage CVE-2020-8300 ist ein Supersatz der Konfigurationsbefehle, die für alle drei CVEs erforderlich sind. Passen Sie diese Basisvorlage an die Bereitstellung und die Anforderungen Ihrer NetScaler-Instanz an.

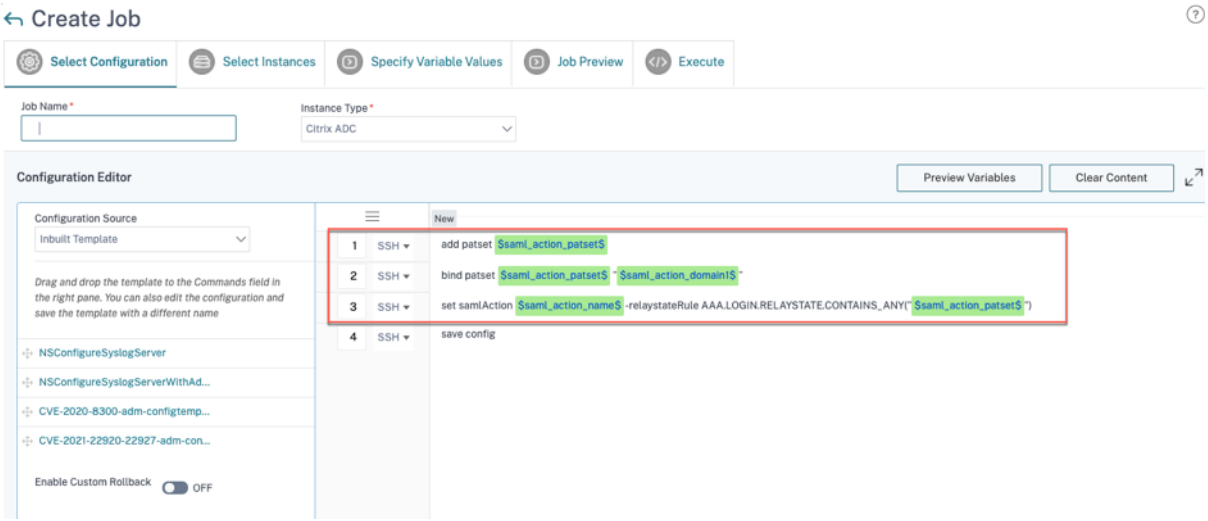
Sie müssen für jede betroffene NetScaler-Instanz nacheinander einen separaten Konfigurationsjob ausführen und alle SAML-Aktionen für diesen NetScaler einbeziehen. Wenn Sie beispielsweise zwei anfällige NetScaler-Instanzen mit jeweils zwei SAML-Aktionen haben, müssen Sie diesen Konfigurationsjob zweimal ausführen. Einmal pro NetScaler, der alle SAML-Aktionen abdeckt.

NetScaler 1	NetScaler 2
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:

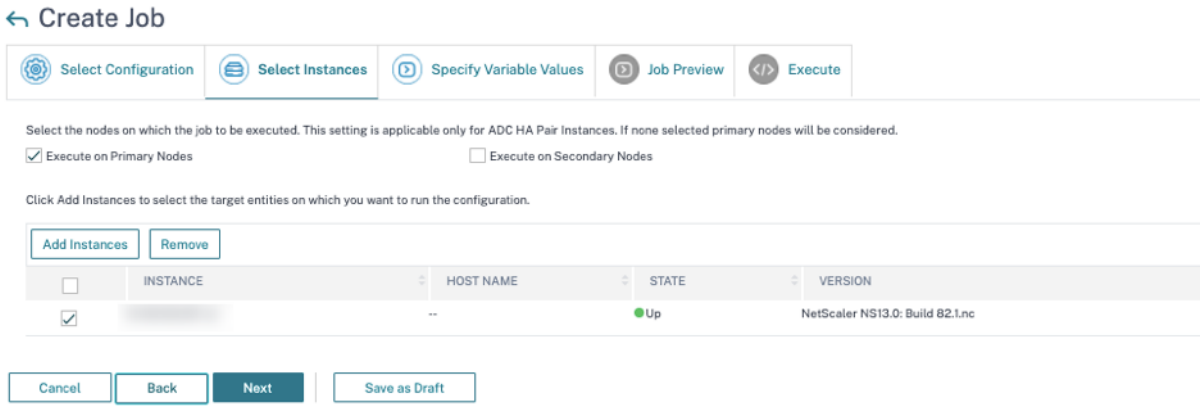
- `saml_action_patset`: ist die Konfigurations-Template-Variable und stellt den Wert des Namens des Mustersatzes (patset) für die SAML-Aktion dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsjob-Workflows angeben. Weitere Informationen finden Sie im Abschnitt Schritt 3: Variablenwerte 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`.

```
> 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
```

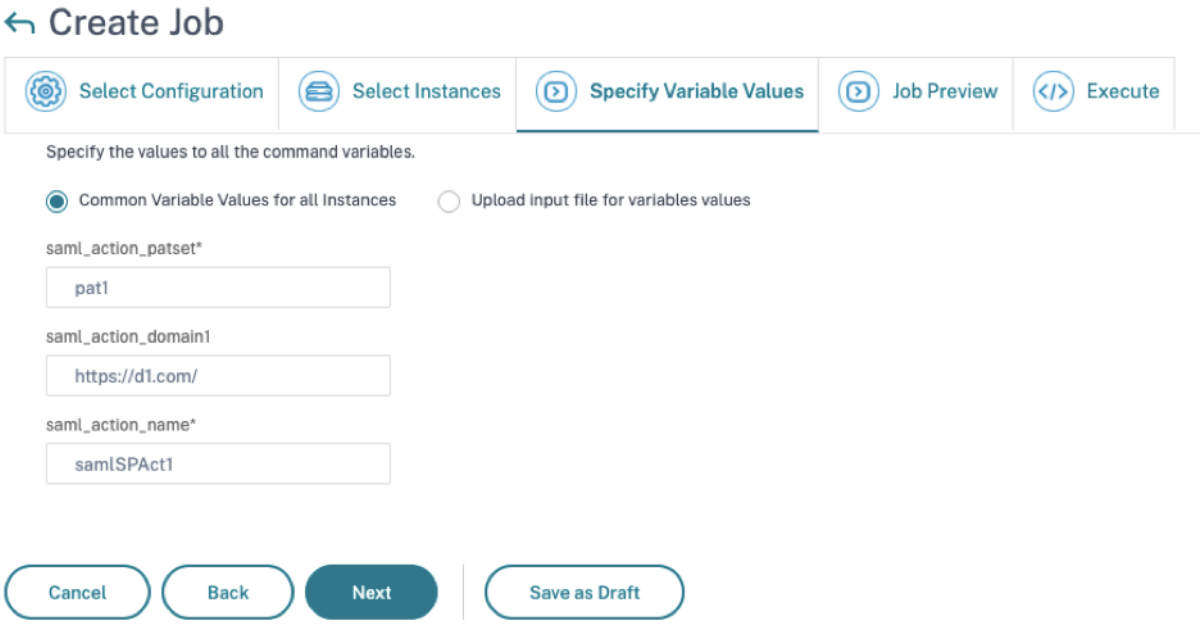

Schritt 2: Wählen Sie die Instanz aus

Die betroffene Instanz wird automatisch unter **Ausgewählte Instanzen**aufgefüllt. Wählen Sie die Instanz und klicken Sie auf **Weiter**.

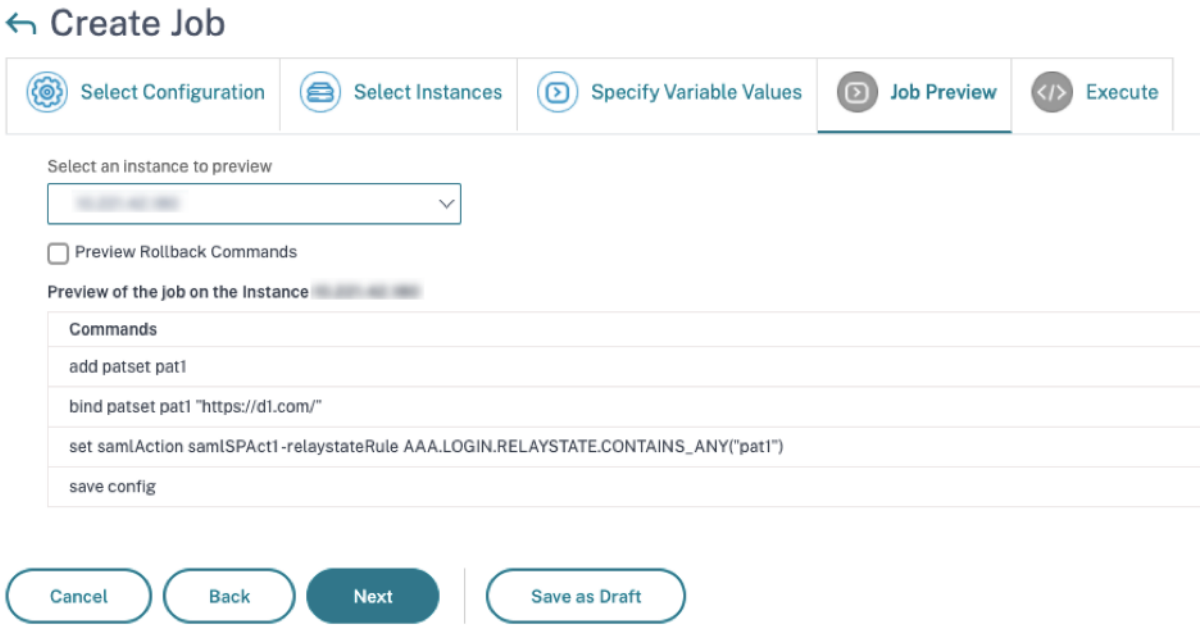


Schritt 3: Variablenwerte angeben Geben Sie die Werte der Variablen ein.

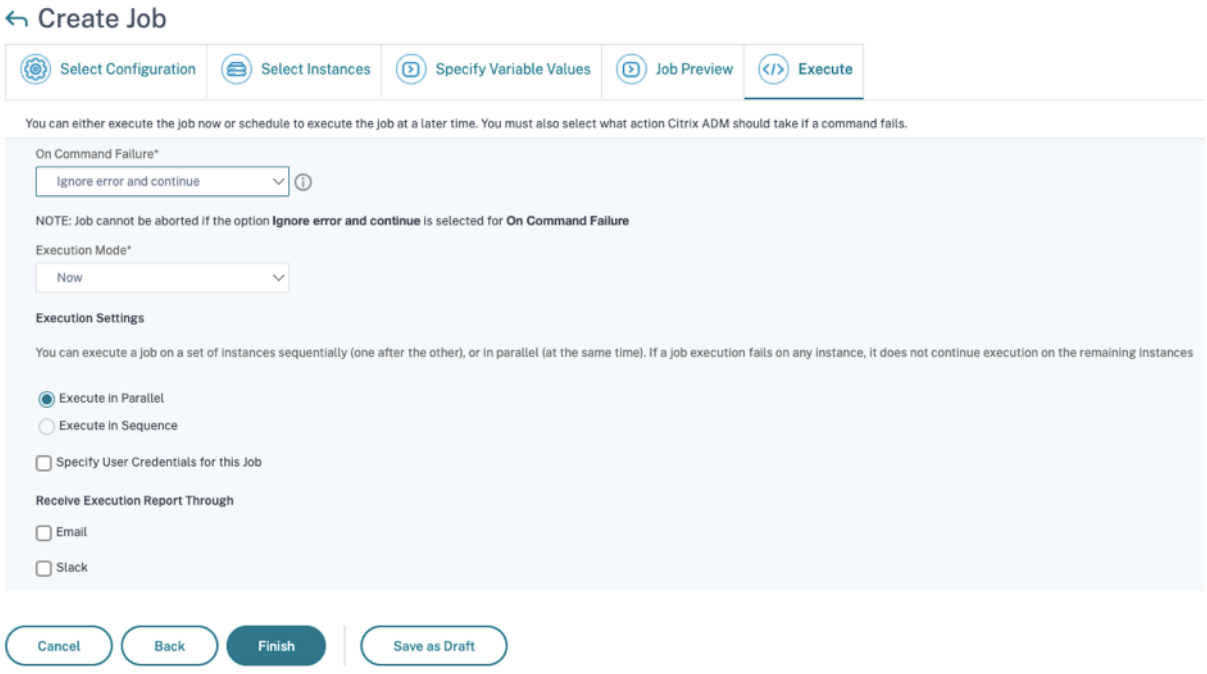
- `saml_action_patset`: Namen für die SAML-Aktion hinzufügen
- `saml_action_domain1`: Domäne im Format `https://<example1.com>/` eingeben
- `saml_action_name`: Dieselbe SAML-Aktion eingeben, für die Sie den Job konfigurieren



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 Schritte zur Behebung aller anfälligen NetScaler-Instanzen abgeschlossen haben, können Sie einen On-Demand-Scan ausführen, um die überarbeitete Sicherheitslage zu überprüfen.

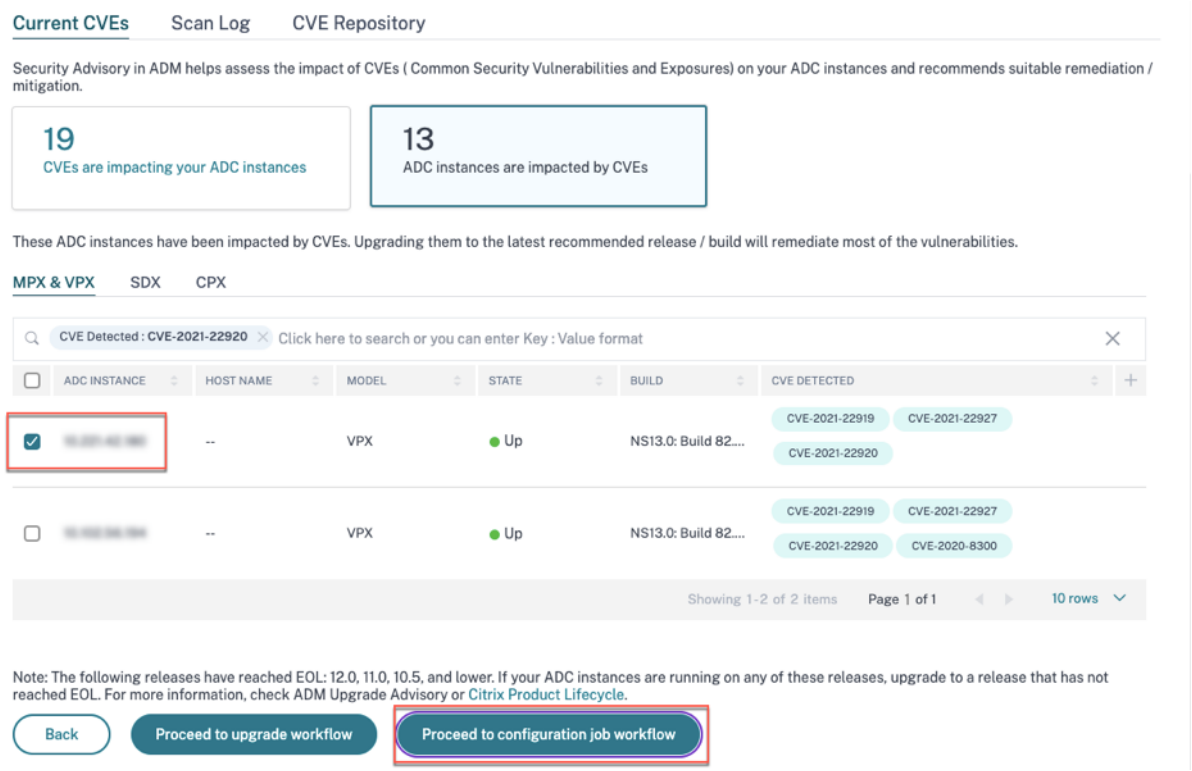
Szenario

In diesem Szenario sind zwei NetScaler-Instanzen anfällig für CVE-2021-22920, und Sie müssen alle Instanzen reparieren. Führen Sie die folgenden Schritte aus:

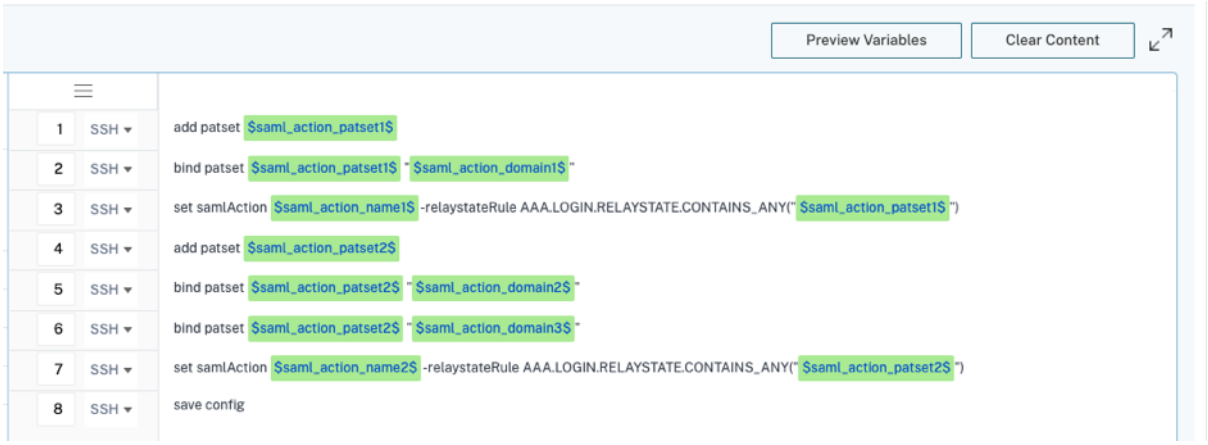
1. Führen Sie ein Upgrade aller drei NetScaler-Instanzen durch, indem Sie die Schritte im Abschnitt „Eine Instanz aktualisieren“in diesem Dokument befolgen.
2. Wenden Sie den Konfigurationspatch mithilfe des Konfigurationsauftragsworkflows jeweils auf einen NetScaler an. Lesen Sie die Schritte, die im Abschnitt “Konfigurationsbefehle anwenden” in diesem Dokument beschrieben werden.

Das anfällige NetScaler 1 hat zwei SAML-Aktionen:

- SAML action 1 hat eine Domain
- SAML-Aktion 2 hat zwei Domänen



Wählen Sie NetScaler 1 aus und klicken Sie auf Weiter zum Workflow für den Konfigurationsauftrag .** Die integrierte Basisvorlage wird automatisch ausgefüllt. Geben Sie als Nächstes einen Auftragsnamen an und passen Sie die Vorlage entsprechend der angegebenen Konfiguration an.

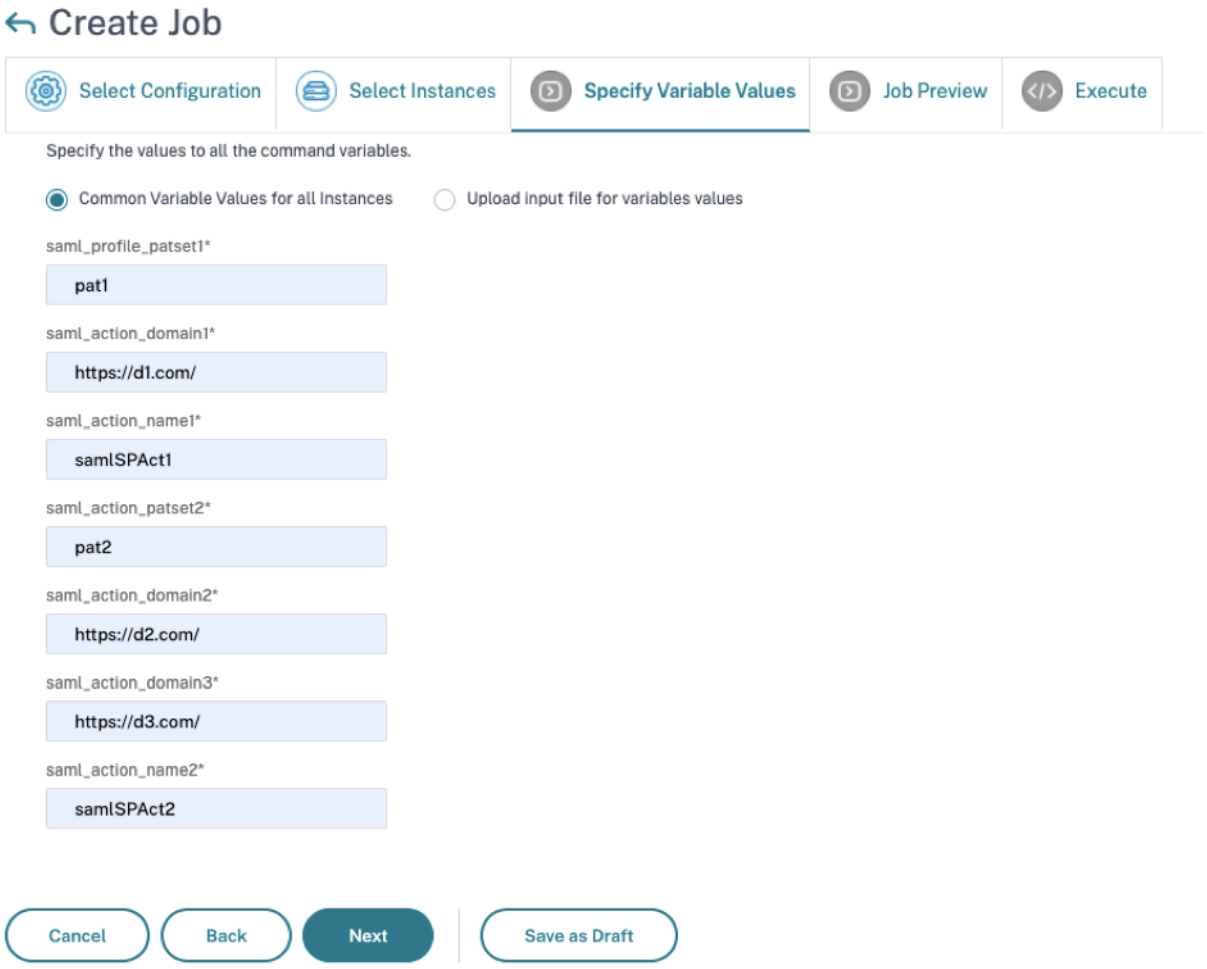


In der folgenden Tabelle sind die Variablendefinitionen für benutzerdefinierte Parameter aufgeführt.

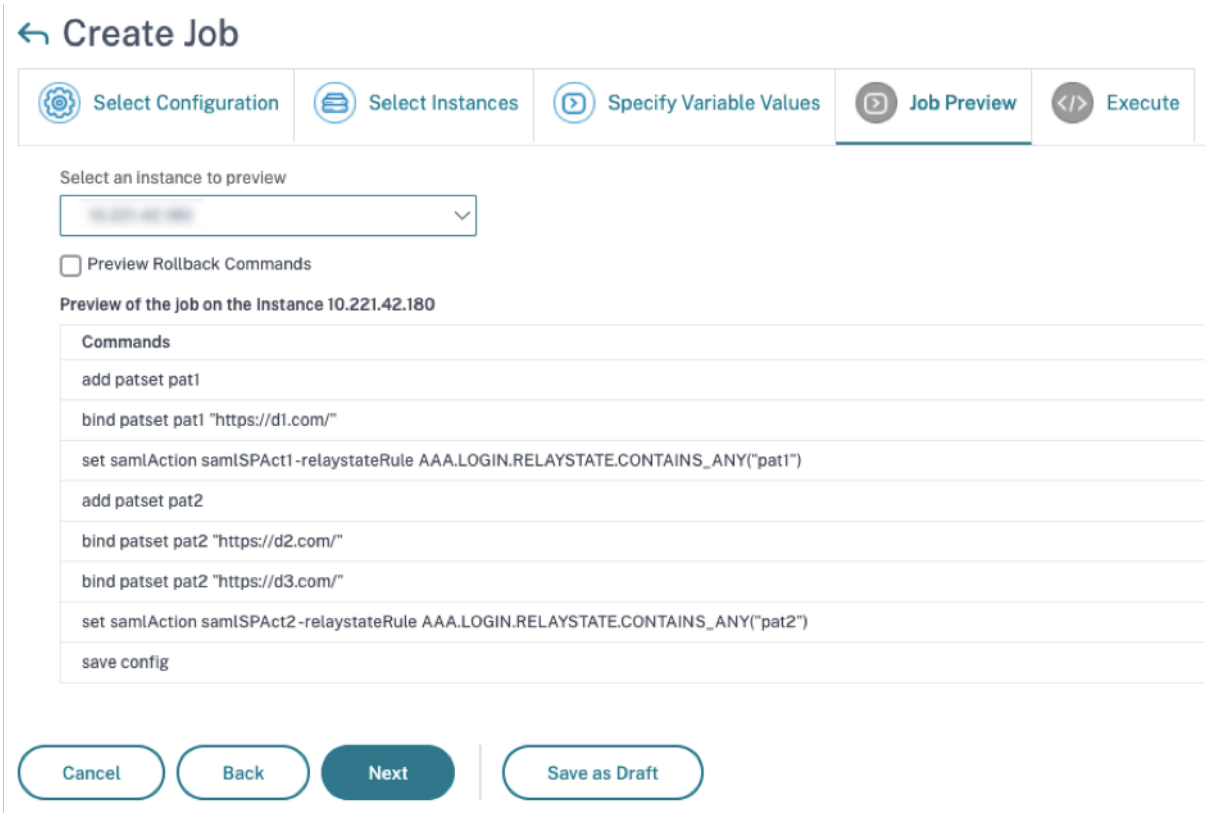
Tabelle. Variablendefinitionen für SAML-Aktionen

NetScaler-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** die Option NetScaler 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.

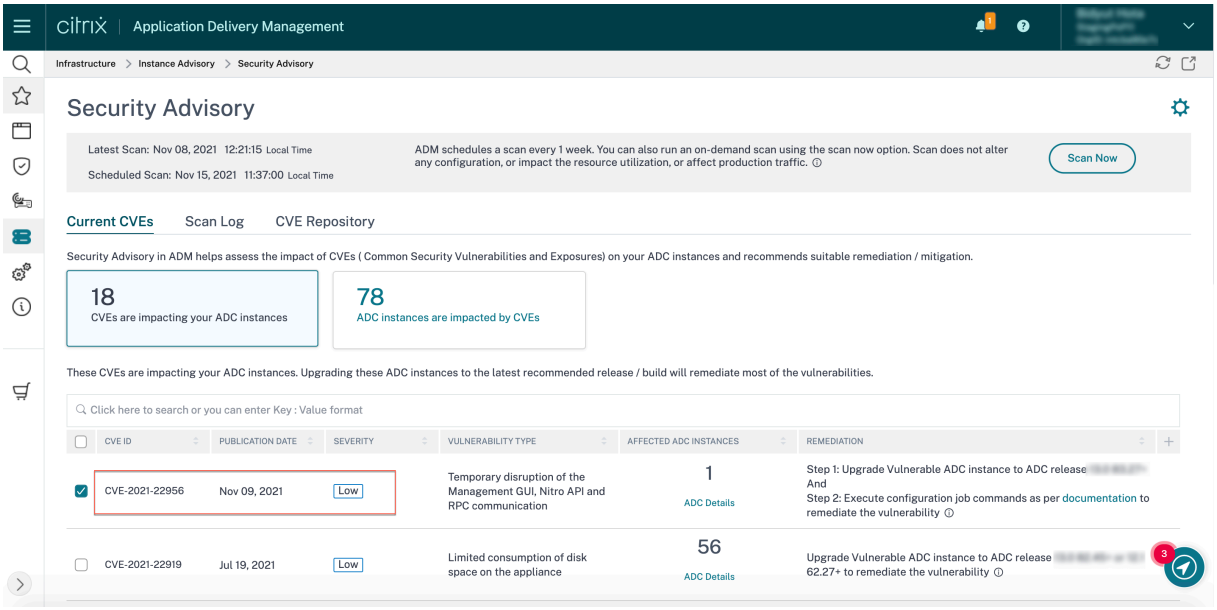
Nachdem der Job ausgeführt wurde, wird er unter **Infrastruktur > Konfiguration > Konfigurationsjobs**angezeigt.

Nachdem Sie die beiden Standardisierungsschritte für NetScaler 1 abgeschlossen haben, führen Sie dieselben Schritte aus, um NetScaler 2 und NetScaler 3 zu standardisieren. Nach Abschluss der Standardisierung können Sie einen Anforderungsscan ausführen, um die überarbeitete Sicherheitslage zu überprüfen.

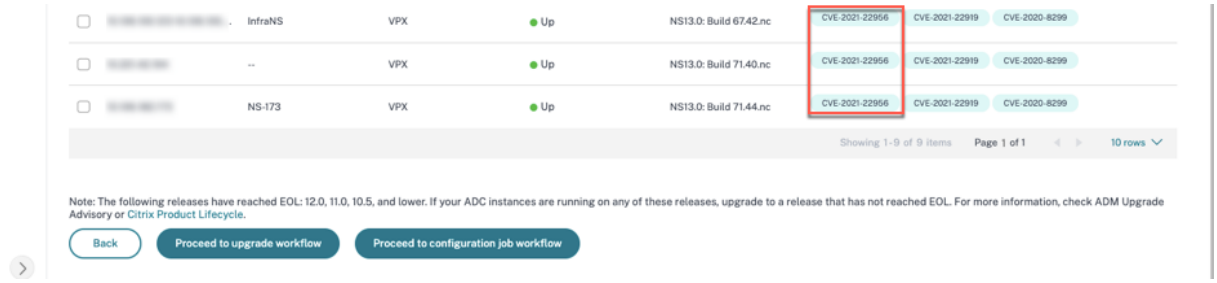
Sicherheitsrisiko CVE-2021-22956 identifizieren und korrigieren

January 26, 2024

Im NetScaler Console Security Advisory Dashboard können Sie unter **Aktuelle CVEs > NetScaler< number of>**-Instanzen sind von Common Vulnerabilities and Exposures (CVEs) betroffen alle Instanzen sehen, die aufgrund dieser spezifischen 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 <number of>Fenster NetScaler-Instanzen, die von CVEs betroffen sind, wird angezeigt. Hier sehen Sie die Anzahl und Details der NetScaler-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 Anforderungsscan, indem Sie auf **Jetzt scannen**klicken.

Identifizieren von CVE-2021-22956 betroffenen Instanzen

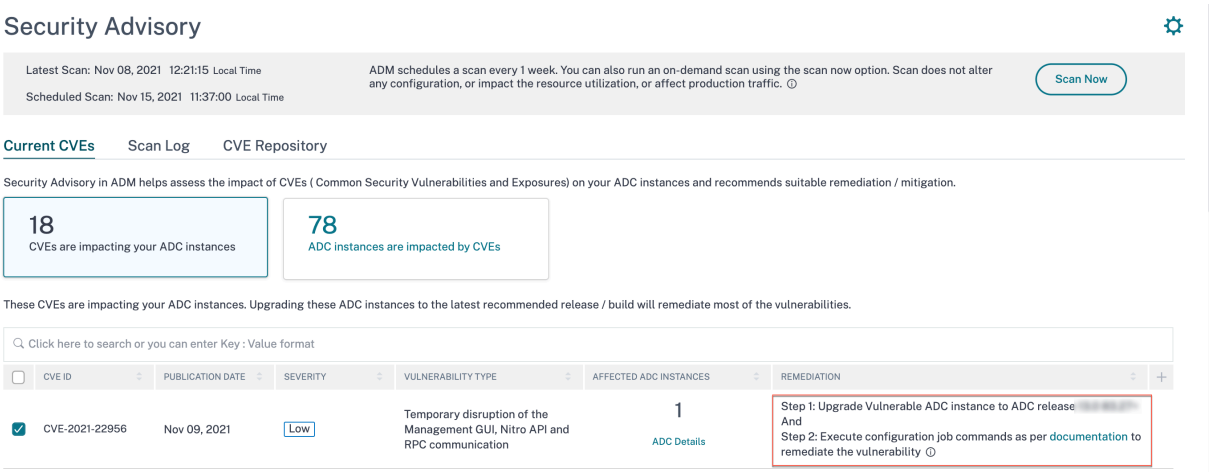
CVE-2021-22956 erfordert einen benutzerdefinierten Scan, bei dem die NetScaler Console eine Verbindung mit der verwalteten NetScaler-Instanz herstellt und ein Skript an die Instanz überträgt. Das Skript wird auf der NetScaler-Instanz ausgeführt und überprüft die Parameter der Apache-Konfigurationsdatei (`httpd.conf file`) und die maximalen Client-Verbindungen (`maxclient`), um festzustellen, ob eine Instanz anfällig ist oder nicht. Die Informationen, die das Skript mit NetScaler Console teilt, sind der Schwachstellenstatus in Boolean (wahr oder falsch). Das Skript

gibt der NetScaler Console auch eine Liste mit Zählungen für max_clients für verschiedene Netzwerkschnittstellen zurück, z. B. für lokalen Host, NSIP und SNIP mit Verwaltungszugriff. Sie können einen detaillierten Bericht zu dieser Liste in der CSV-Datei sehen, die Sie auf der Registerkarte **Scan-Protokolle** auf der Seite **Sicherheitsempfehlung** herunterladen können.

Dieses Skript wird jedes Mal ausgeführt, wenn Ihre geplanten Scans auf Anforderung ausgeführt werden. Nach Abschluss des Scans wird das Skript aus der NetScaler-Instanz gelöscht.

Korrigieren CVE-2021-22956

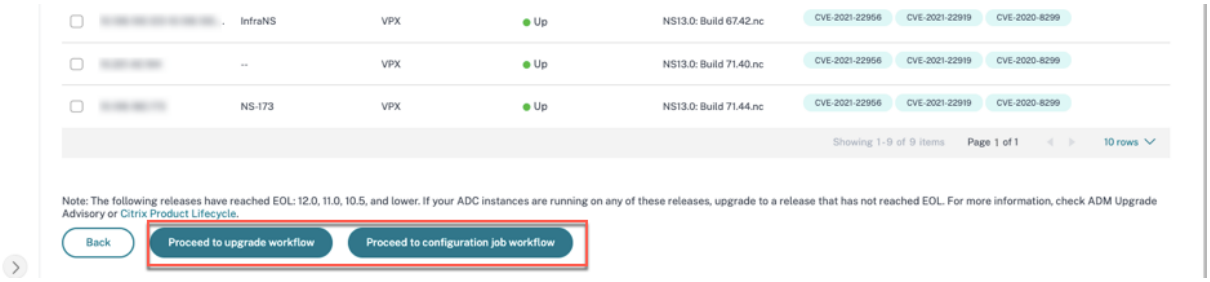
Für NetScaler-Instanzen, die von CVE-2021-22956 betroffen sind, besteht die Behebung aus zwei Schritten. In der GUI können Sie unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen** die Schritte 1 und 2 sehen.



Die zwei Schritte beinhalten:

1. Aktualisierung der anfälligen NetScaler-Instanzen auf eine Version und einen Build, die den Fix enthalten.
2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen.

Unter Aktuelle CVEs > NetScaler-Instanzen, die von CVEs betroffen sind, sehen Sie zwei separate Workflows für diesen zweistufigen Korrekturprozess: Weiter zum Upgrade-Workflow und Weiter zum Konfigurationsjob-Workflow.



Schritt 1: Aktualisieren Sie die anfälligen NetScaler-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 anfälligen NetScaler-Instanzen geöffnet, die bereits gefüllt sind.

Weitere Informationen zur Verwendung der NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Jobs.

> **Hinweis**
>
> Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig ausgeführt werden.

Schritt 2: Anwenden von Konfigurationsbefehlen

Nachdem Sie die betroffenen Instanzen aktualisiert haben, wählen Sie im Fenster **<number of> NetScaler-Instanzen, die von CVEs betroffen** sind, die Instance aus, die von CVE-2021-22956 betroffen ist, und klicken Sie auf **Weiter zum Konfigurationsjob-Workflow**. Der Workflow umfasst die folgenden Schritte.

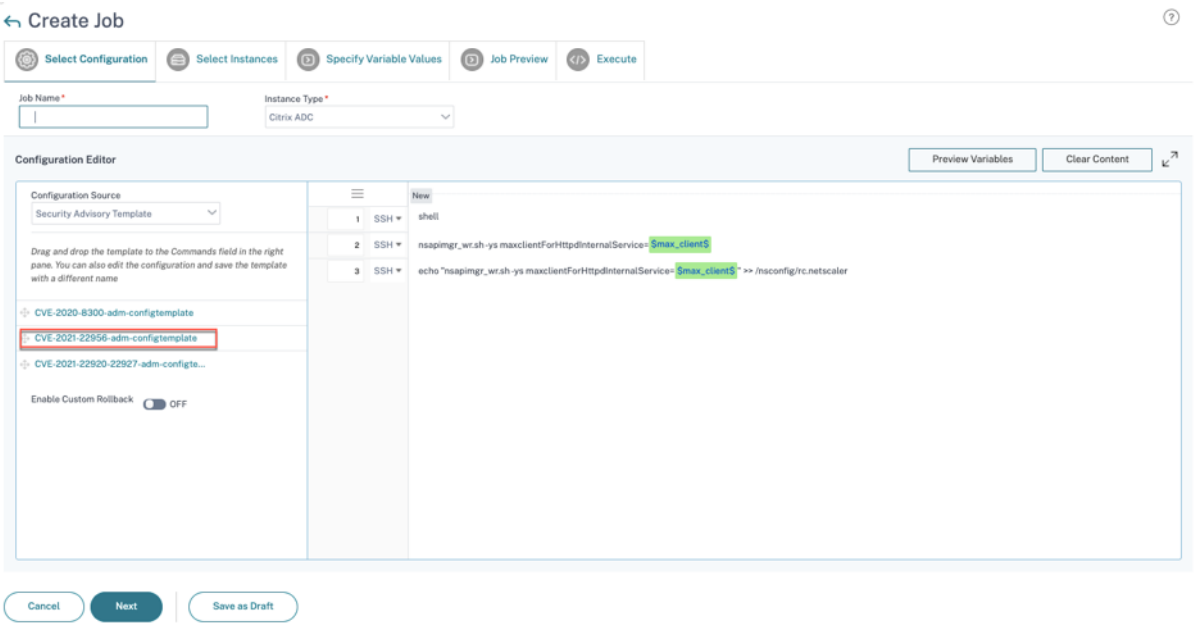
1. Anpassen der Konfiguration.
2. Überprüfung der automatisch ausgefüllten betroffenen Instanzen.
3. Angabe von Eingaben für Variablen für den Job.
4. Überprüfung der endgültigen Konfiguration mit aufgefüllten Variableneingaben.
5. Den Job ausführen.

Beachten Sie die folgenden Punkte, bevor Sie eine Instanz auswählen und auf **Weiter zum Workflow des Konfigurationsauftrags**klicken:

- **Für eine NetScaler-Instanz, die von mehreren CVEs betroffen ist (wie CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 und CVE-2021-22956): Wenn Sie die Instanz auswählen und auf Weiter zum Konfigurationsauftrags-Workflow** 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.

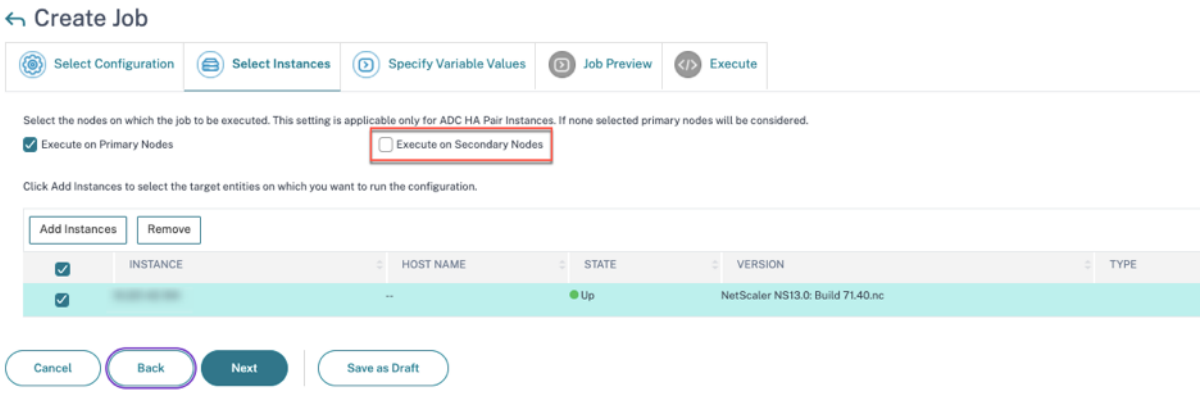
- Nur für mehrere NetScaler-Instanzen, die von CVE-2021-22956 betroffen sind: Sie können Konfigurationsaufträge auf allen Instanzen gleichzeitig ausführen. Sie haben beispielsweise NetScaler 1, NetScaler 2 und NetScaler 3, und alle sind nur von CVE-2021-22956 betroffen. Wählen Sie alle diese Instanzen 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.
- **Für mehrere NetScaler-Instanzen, die von CVE-2021-22956 und einer oder mehreren anderen CVEs betroffen sind (wie CVE-2020-8300, CVE-2021-22927 und CVE-2021-22920), die eine Korrektur erfordern, um auf jedem NetScaler gleichzeitig angewendet zu werden: Wenn Sie diese Instanzen auswählen und auf Weiter zum Konfigurationsauftrags-Workflow** klicken, wird eine Fehlermeldung angezeigt, die Sie auffordert, den Konfigurationsjob auf jedem NetScaler 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

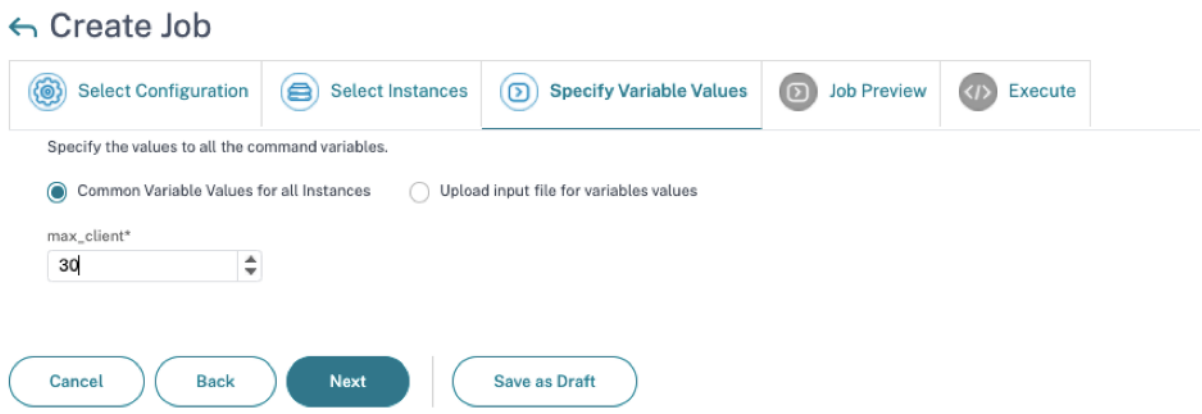
Die betroffene Instanz wird automatisch unter **Ausgewählte Instanzen**aufgefüllt. Wählen Sie die Instanz aus. Wenn diese Instanz Teil eines HA-Paars ist, wählen Sie **Auf sekundären Knoten ausführen**aus. Klicken Sie auf **Weiter**.



> **Hinweis**
>
> Für NetScaler-Instanzen im Clustermodus unterstützt die NetScaler Console unter Verwendung der Sicherheitsempfehlung die Ausführung des Konfigurationsauftrags nur auf dem Cluster Configuration Coordinator (CCO) -Knoten. 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.



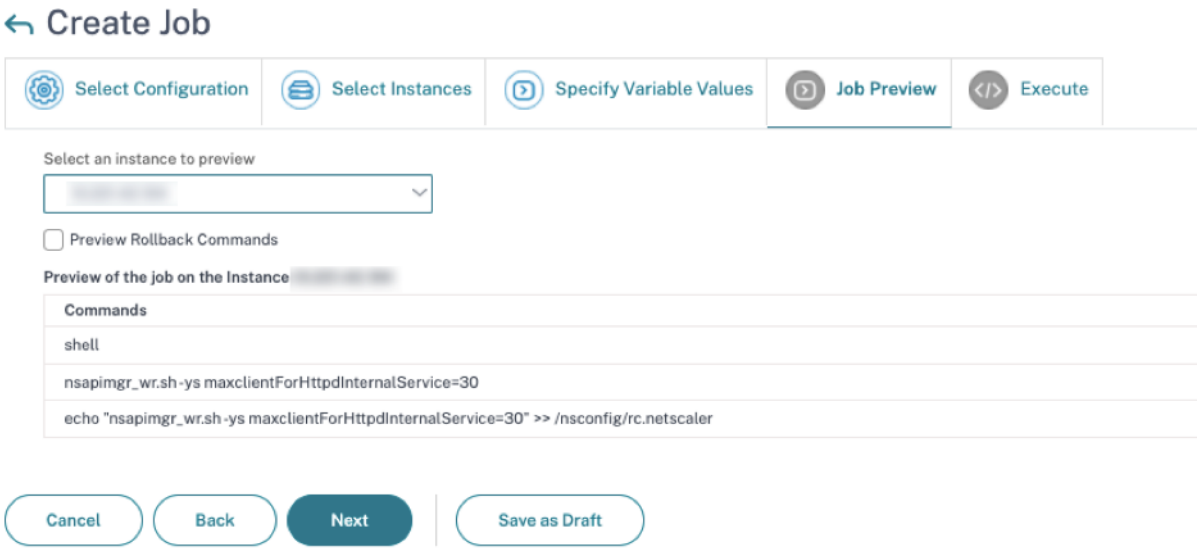
Wählen Sie eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:

Gemeinsame Variablenwerte für alle Instanzen: Geben Sie einen gemeinsamen Wert für die Variable ein `max_client`.

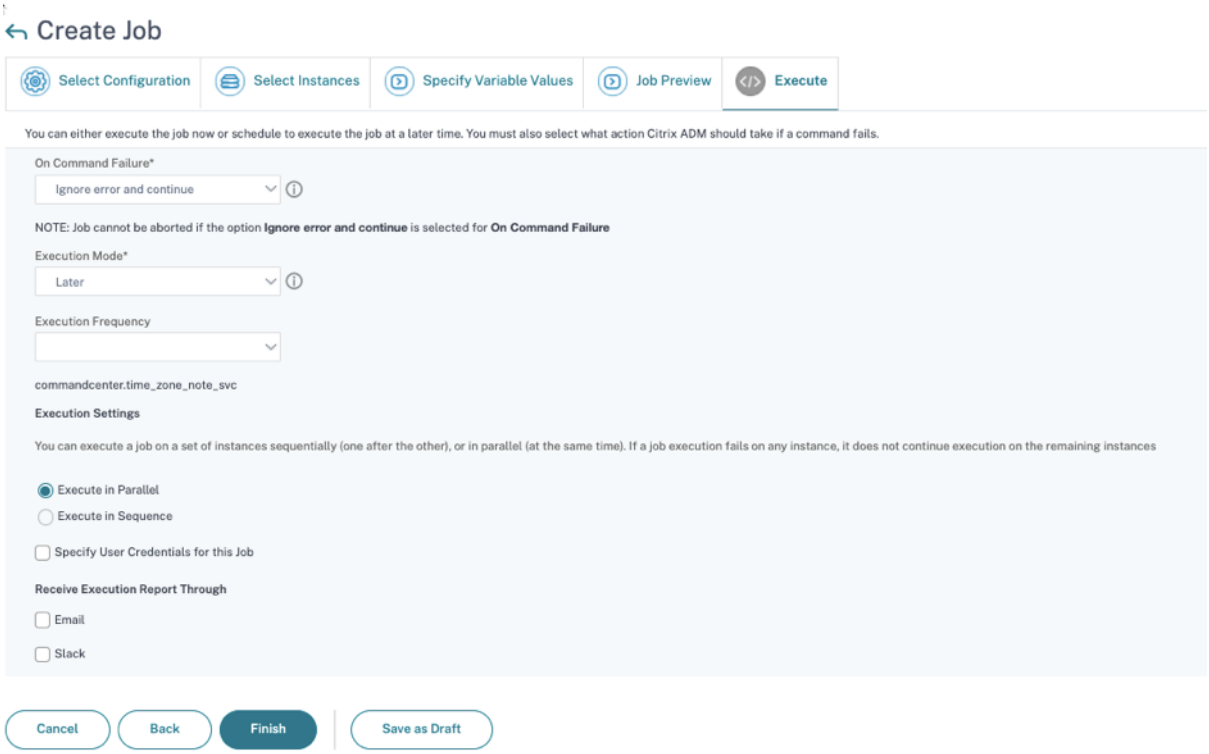
Eingabedatei für Variablenwerte hochladen: Klicken Sie auf **Eingabeschlüsseldatei herunterladen**, um eine Eingabedatei herunterzuladen. Geben Sie in der Eingabedatei Werte für die Variable `max_client`ein und laden Sie die Datei dann auf den NetScaler Console-Server hoch. Lesen Sie das bekannte Problem 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. `MaxClients`Sie können den aktuellen Wert überprüfen, der in der Apache HTTP Server-Konfigurationsdatei `/etc/httpd.conf`festgelegt ist , indem Sie die Zeichenfolge in der NetScaler-Instanz durchsuchen.

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.



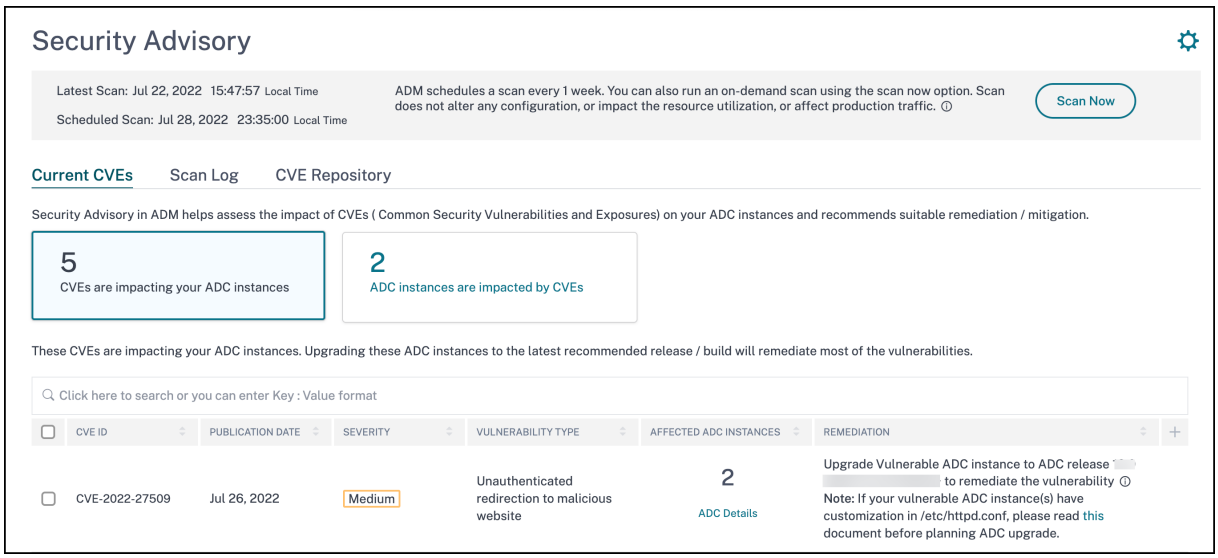
Nachdem der Job ausgeführt wurde, wird er unter **Infrastruktur > Konfiguration > Konfigurationsjobs**angezeigt.

Nachdem Sie die beiden Schritte zur Behebung aller anfälligen NetScaler-Instanzen abgeschlossen haben, können Sie einen On-Demand-Scan ausführen, um die überarbeitete Sicherheitslage zu überprüfen.

Sicherheitsrisiko CVE-2022-27509 identifizieren und korrigieren

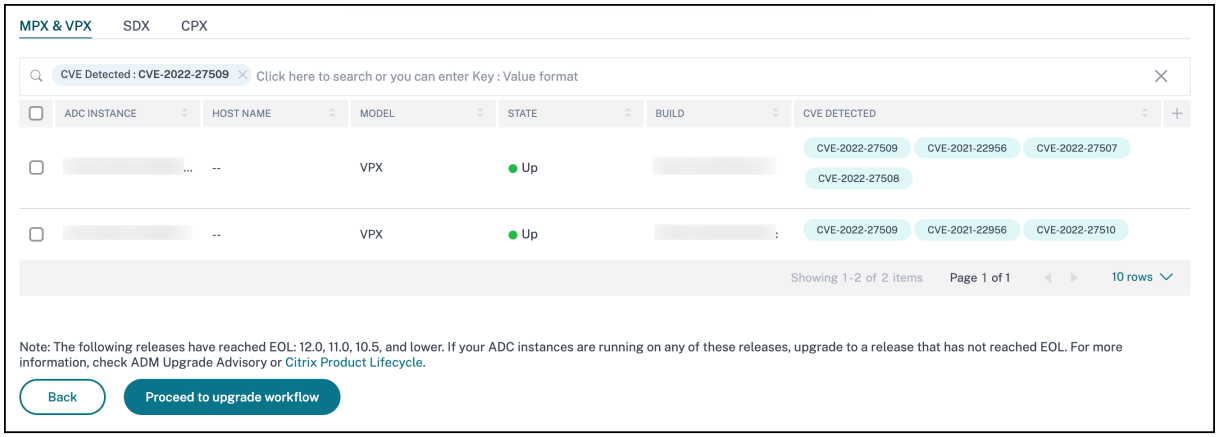
January 26, 2024

Im NetScaler Console Security Advisory Dashboard können Sie unter **Aktuelle CVEs <`number of`>NetScaler-Instanzen sind von CVEs betroffen** alle Instanzen sehen, 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 NetScaler-Schwachstelle zu verstehen, laden Sie den CSV-Bericht auf der Registerkarte Scanprotokolle in der Sicherheitsempfehlung herunter.

Das Fenster **<number of>NetScaler-Instanzen, die von CVEs betroffen** sind, wird angezeigt. In der folgenden Bildschirmaufnahme sehen Sie die Anzahl und Details der NetScaler-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 die NetScaler Console eine Verbindung mit der verwalteten NetScaler-Instanz her und überträgt ein Skript an die Instanz. Das Skript wird auf der NetScaler-Instanz ausgeführt und bestimmt, ob die Instanz anfällig ist. Dieses Skript wird jedes Mal ausgeführt, wenn Ihr geplanter Scan oder ein Scan auf Anforderung

Nach Abschluss des Scans wird das Skript aus der NetScaler-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

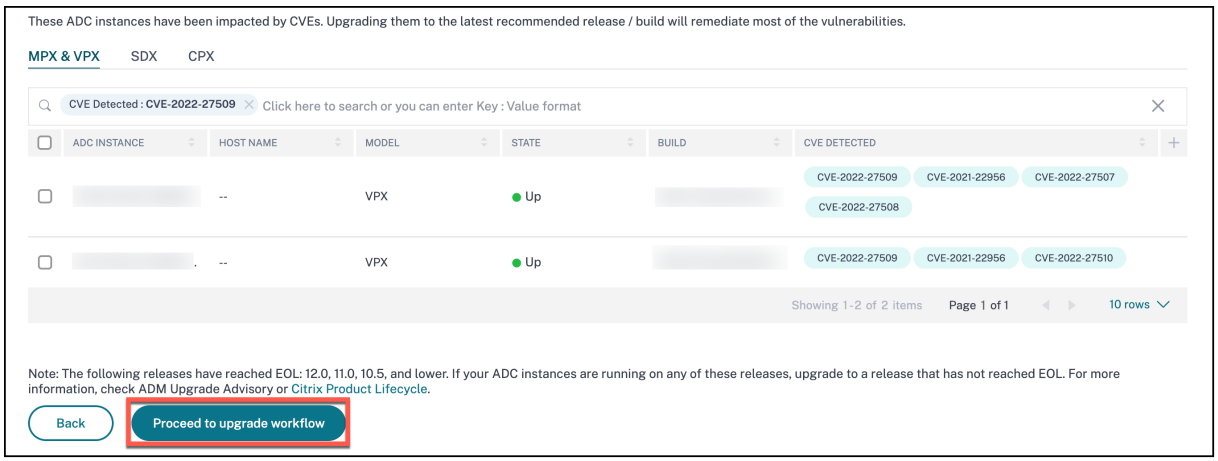
Bei NetScaler-Instanzen, die von CVE-2022-27509 betroffen sind, erfolgt die Behebung in einem einzigen Schritt, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, die den Fix enthalten. In der GUI können Sie unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen** den Schritt zur Behebung sehen.

Unter **Aktuelle CVEs > NetScaler-Instanzen, die von CVEs betroffen** sind, sehen Sie den folgenden Arbeitsablauf für diesen einstufigen Behebungsprozess, nämlich **Proceed to 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 anfälligen NetScaler-Instanzen geöffnet, die bereits gefüllt sind.

> **WICHTIG**
>
> Wenn auf Ihren anfälligen NetScaler-Instanzen die Datei /etc/httpd.conf in das Verzeichnis /nsconfig kopiert wurde, finden Sie weitere Informationen unter Überlegungen zum Upgrade für benutzerdefinierte NetScaler-Konfigurationen, bevor Sie ein NetScaler-Upgrade planen .

Weitere Informationen zur Verwendung der NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Jobs.



Nicht unterstützte CVEs in den Sicherheitsempfehlungen

January 26, 2024

Die Sicherheitsempfehlung von NetScaler Console 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 Sicherheitslücken fallen nicht in den Geltungsbereich der NetScaler Console 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 der NetScaler Console nicht unterstützt. Außerdem können Sicherheitslücken im NetScaler Gateway-Plug-In nicht untersucht werden, indem irgendwelche Prüfungen auf der NetScaler-Seite durchgeführt, die NetScaler-Version überprüft oder die NetScaler-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 fallen die Erkennung und Behebung dieser Sicherheitsanfälligkeit nicht in den Geltungsbereich der NetScaler Console Security Advisory.

einrichten

January 26, 2024

Nachdem Ihre Ersteinrichtung abgeschlossen ist, müssen Sie bestimmte Einstellungen konfigurieren, um mit der vollständigen Verwaltung Ihrer Bereitstellung zu beginnen.

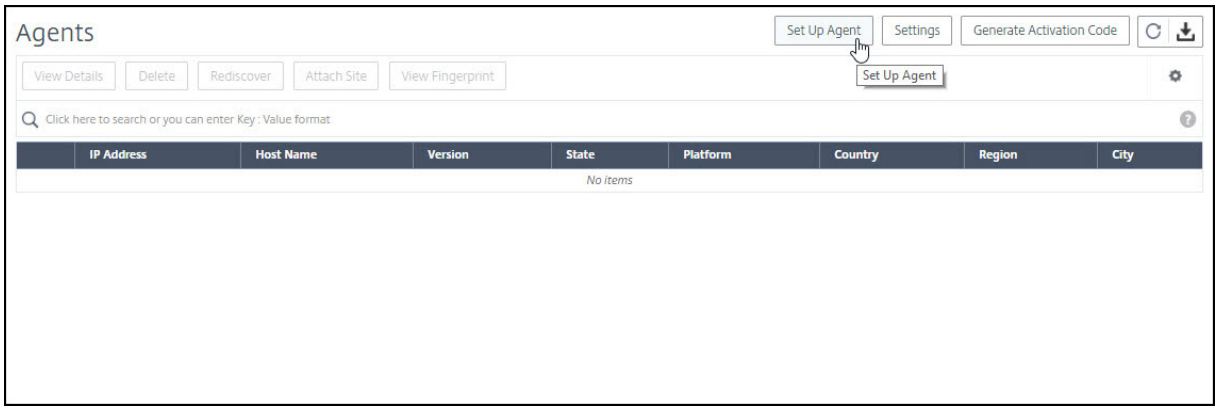
- Hinzufügen mehrerer Agents. Die Anzahl der zu installierenden Agents hängt von der Anzahl der verwalteten Instanzen in einem Rechenzentrum oder einer Cloud und dem Gesamtdurchsatz ab. Citrix empfiehlt, mindestens einen Agent für jedes Datencenter zu installieren.
- Hinzufügen von Instanzen. Sie können Instanzen entweder beim ersten Einrichten der NetScaler Console oder zu einem späteren Zeitpunkt hinzufügen. Sie müssen dem Service Instanzen hinzufügen, um sie zu verwalten und zu überwachen. Nachdem Sie mehrere Agents installiert haben, müssen Sie Instanzen hinzufügen und sie den Agents zuordnen.
- Analytics aktivieren. Um Analysedaten für den Datenverkehr Ihrer Anwendung anzuzeigen, müssen Sie die Analytics-Funktion auf den virtuellen Servern aktivieren, die Datenverkehr für die jeweiligen Anwendungen empfangen.
- Syslog auf Instanzen konfigurieren. Sie können die auf Ihren NetScaler-Instanzen generierten Syslog-Ereignisse überwachen, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Meldungen an NetScaler Console umgeleitet werden. Um Syslog-Ereignisse zu überwachen, müssen Sie zunächst NetScaler Console als Syslog-Server für Ihre NetScaler-Instanz konfigurieren.
- Konfiguration der rollenbasierten Zugriffskontrolle. NetScaler Console bietet eine detaillierte, rollenbasierte Zugriffskontrolle (RBAC), mit der Sie Zugriffsberechtigungen auf der Grundlage der Rollen einzelner Benutzer in Ihrem Unternehmen gewähren können.
- Analytics-Einstellungen konfigurieren Sie können bestimmte Einstellungen konfigurieren, um eine optimale Erfahrung mit der Analytics-Funktion zu gewährleisten. Sie können beispielsweise die Dauer angeben, in der historische Analysedaten gespeichert werden sollen, und Sie können auch Schwellenwerte und Warnungen festlegen, um die gewünschten Analysemetriken zu überwachen.

Hinzufügen mehrerer Agents

January 26, 2024

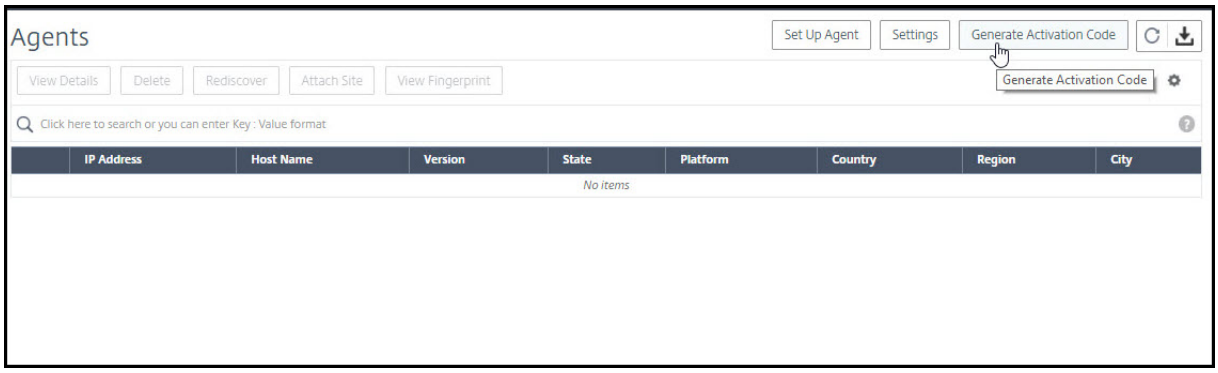
Die Anzahl der zu installierenden Agents hängt von der Anzahl der verwalteten Instanzen in einem Rechenzentrum und dem Gesamtdurchsatz ab. Citrix empfiehlt, mindestens einen Agent für jedes Datencenter zu installieren.

Sie können nur einen Agent installieren, wenn Sie sich zum ersten Mal beim Dienst anmelden. Um mehrere Agents hinzuzufügen, führen Sie zuerst die Ersteinrichtung durch, navigieren Sie zu **Infrastruktur > Instanzen > Agents** und klicken Sie auf **Agent einrichten.**



Laden Sie das Image für den erforderlichen Hypervisor herunter und installieren Sie den Agent, indem Sie den Anweisungen unter Erste Schritte folgen. Stellen Sie sicher, dass Sie die Dienst-URL und den Aktivierungscode, die auf dem Bildschirm angezeigt werden, kopieren, da Sie bei der Installation des Agents auf Ihrem Hypervisor die Dienst-URL und den Aktivierungscode eingeben müssen. Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.

Sie können dasselbe Image verwenden, um mehrere Agents in Ihrem Hypervisor zu installieren. Sie können jedoch nicht denselben Aktivierungscode auf mehreren Agents verwenden. Nachdem Sie einen Agent installiert haben, generieren Sie den Aktivierungscode erneut für den nächsten Agent. Sie können einen neuen Aktivierungscode generieren, indem Sie zu **Infrastruktur > Instanzen > Agents**navigieren und auf **Aktivierungscode generieren**klicken.



Nachdem der Agent erfolgreich installiert und registriert wurde, überprüfen Sie den Agent-Status auf der Dienst-GUI und fügen Sie Instanzen hinzu.

Hinweis

Sie können auch einen Agenten in der Microsoft Azure-Cloud oder der AWS-Cloud installieren. Das Agentimage ist auf dem jeweiligen Cloud-Marktplatz verfügbar.

- Anweisungen zur Installation eines Agenten in der Microsoft Azure-Cloud finden Sie unter Installieren eines NetScaler-Agenten in der Microsoft Azure Cloud.
- Anweisungen zur Installation eines Agenten auf AWS finden Sie unter Installieren eines NetScaler-Agenten auf AWS.

Agents für die Bereitstellung an mehreren Standorten konfigurieren

January 26, 2024

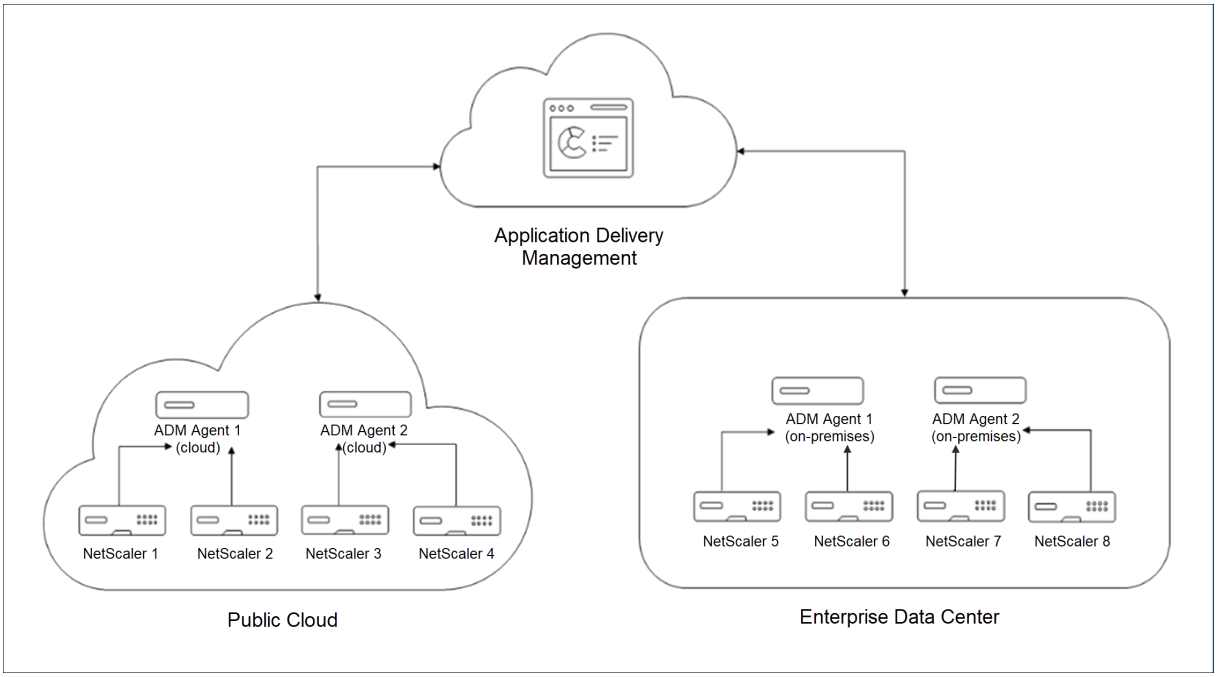
Agenten fungieren als Vermittler zwischen der NetScaler Console und den erkannten Instanzen in verschiedenen Rechenzentren und öffentlichen Clouds. NetScaler Console unterstützt Agenten-Failover innerhalb eines Rechenzentrums oder einer öffentlichen Cloud.

Im Folgenden sind die Vorteile der Installation von Agents aufgeführt:

- Die konfigurierten Instanzen an einen Agenten senden die unverarbeiteten Daten direkt an den Agenten statt an NetScaler Console. Der Agent führt die erste Ebene der Datenverarbeitung durch und sendet die verarbeiteten Daten im komprimierten Format zur Speicherung an die NetScaler Console.
- Agents und Instanzen befinden sich in demselben Rechenzentrum oder derselben Cloud, 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, wechselt der Datenverkehr von NetScaler-Instanzen zu einem anderen verfügbaren Agent an derselben Site.

Architektur

Die folgende Abbildung zeigt NetScaler-Instanzen, die auf mehreren Agents in einem Rechenzentrum und einer Public Cloud konfiguriert sind, um ein Agent-Failover zu erzielen:



Die Public Cloud hat vier NetScaler-Instanzen und zwei Agenten. Das Unternehmensrechenzentrum verfügt außerdem über vier NetScaler-Instanzen und zwei Agenten. Jeder Agent ist mit zwei NetScaler-Instanzen konfiguriert.

Die Agents erhalten Daten direkt von den konfigurierten Instanzen. Nachdem der Agent die Daten empfangen hat, verarbeitet der Agent die Daten und sendet sie in einem komprimierten Format an die NetScaler Console. Agents kommunizieren mit dem NetScaler Console-Server über einen sicheren Kanal.

Wenn **Agent 1** in der Public Cloud inaktiv wird (DOWN-Status), erfolgt ein Agenten-Failover. NetScaler Console verteilt die NetScaler-Instanzen von **Agent 1** mit **Agent 2**. Die Umverteilung der Instanzen erfolgt in einem Unternehmensrechenzentrum, wenn einer der Agents im Rechenzentrum ausfällt.

Informationen zur Installation eines Agents finden Sie unter Installieren eines NetScaler Agents.

Agenten-Failover

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

> **Wichtig!**
>
> - Beim Agenten-Failover werden CPX-Instanzen nicht berücksichtigt.
> - Stellen Sie sicher, dass die Agent-Failover-Funktion für Ihr Konto aktiviert ist. Informationen

> zum Aktivieren dieser Funktion finden Sie unter Aktivieren oder Deaktivieren der NetScaler Console-Funktionen .
>
> - 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.

So hängen Sie in der NetScaler Console-GUI eine Site an einen Agenten an:

1. Navigieren Sie zu **Infrastruktur > Instanzen > Agents**.
2. Wählen Sie einen Agent aus, den Sie einer Site zuordnen möchten.
3. Geben Sie die Site aus der Liste an. Wenn Sie eine neue Website hinzufügen möchten, klicken Sie auf **Hinzufügen**.
4. Klicken Sie auf **Speichern**.

Um einen Agenten-Failover zu erreichen, wählen Sie die Agenten nacheinander aus und verbinden Sie sie mit derselben Site.

Beispielsweise sind zwei Agents 10.106.1xx.2x und 10.106.1xx.7x am Standort Bangalore angeschlossen und betriebsbereit. Wenn ein Agent inaktiv wird, erkennt NetScaler Console ihn und zeigt den Status als inaktiv an.

Wenn ein Agent an einer Site inaktiv wird (Status Heruntergefahren), wartet NetScaler Console einige Minuten, bis der Agent aktiv wird (Status Aktiv). Wenn der Agent inaktiv bleibt, verteilt NetScaler Console die Instanzen automatisch auf die verfügbaren Agents an derselben Site neu. Diese Umverteilung kann etwa 10 bis 15 Minuten dauern.

NetScaler Console löst alle 30 Minuten eine Neuverteilung der Instanzen aus, um die Last zwischen den aktiven Agents in der Site auszugleichen.

Die Instanzen, die für Trap-Ziel, Syslog-Server und Analysen an Agents am selben Standort angehängt und automatisch neu konfiguriert wurden.

Agent-Upgradeeinstellungen konfigurieren

January 26, 2024

In NetScaler Console werden Agents, die auf der Softwareversion 12.0 Build 507.110 und höher ausgeführt werden, von NetScaler Console automatisch auf neuere und empfohlene Versionen aktualisiert. Der Agent wird entweder aktualisiert, wenn eine neue Version verfügbar ist, oder zu einem von Ihnen angegebenen Zeitpunkt.

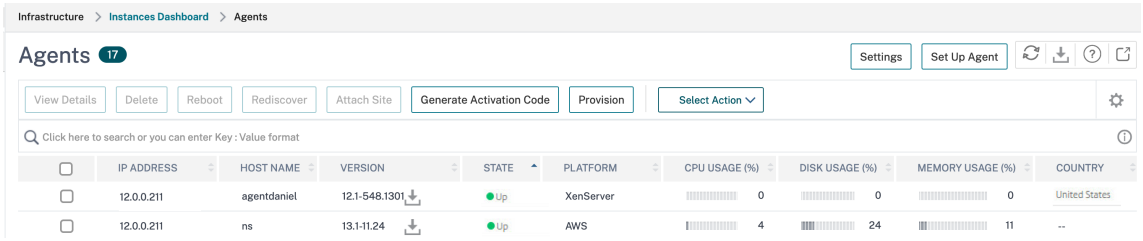
Sie können die aktuelle Version und die empfohlene Version Ihrer Agents anzeigen, indem Sie zu **Infrastruktur > Instanzen > Agents** navigieren.

Standardmäßig wird ein Agent automatisch aktualisiert, wenn eine neuere Version verfügbar ist. Sie können jedoch für jeden der Agents ein Upgrade planen.

Während des Upgrades kann es zu einer Ausfallzeit von etwa fünf Minuten kommen.

So konfigurieren Sie Agent-Upgrade-Einstellungen:

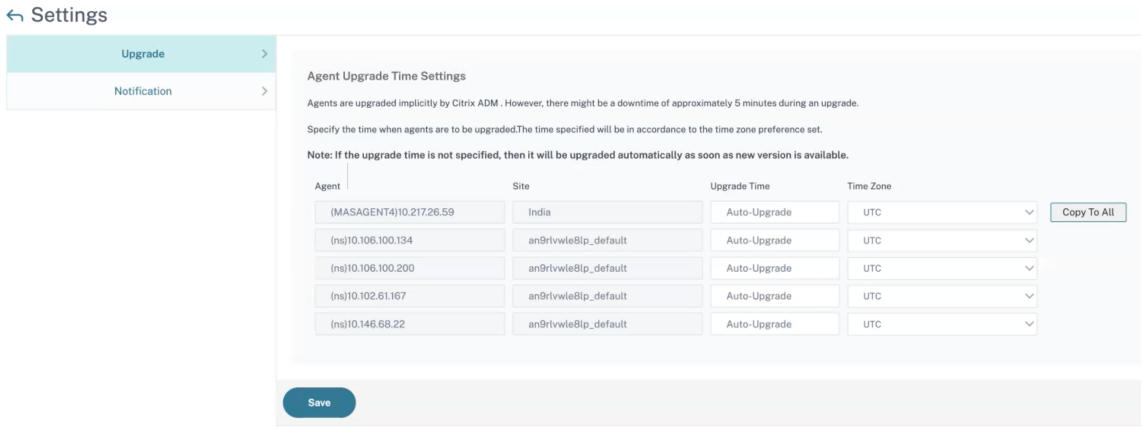
1. Navigieren Sie zu **Infrastruktur > Instanzen > Agents** und klicken Sie auf **Einstellungen**.



2. Geben Sie an, wann das Upgrade für jeden Agent beginnen soll.

   Sie können eine der folgenden Optionen verwenden, um den Agent zu aktualisieren:

   - Automatisches Upgrade —Wählen Sie **Auto-Upgrade**, damit der Agent aktualisiert werden soll, wenn ein neues Agent-Image verfügbar ist. Wenn Sie keinen Wert eingeben, ist **Auto-Upgrade** standardmäßig ausgewählt.
   - Stellen Sie eine bestimmte Uhrzeit ein: Geben Sie die Uhrzeit (im Format hh:mm) ein und wählen Sie die Zeitzone aus, in der NetScaler Console den Agenten automatisch aktualisieren soll.



   Sie können auf **An alle kopieren** klicken, um dieselbe Upgrade-Zeit auf alle Agents anzuwenden.

3. Klicken Sie auf **Speichern**.

   Diese Einstellungen bleiben für zukünftige Agent-Upgrades bestehen, bis Sie die Einstellungen ändern.

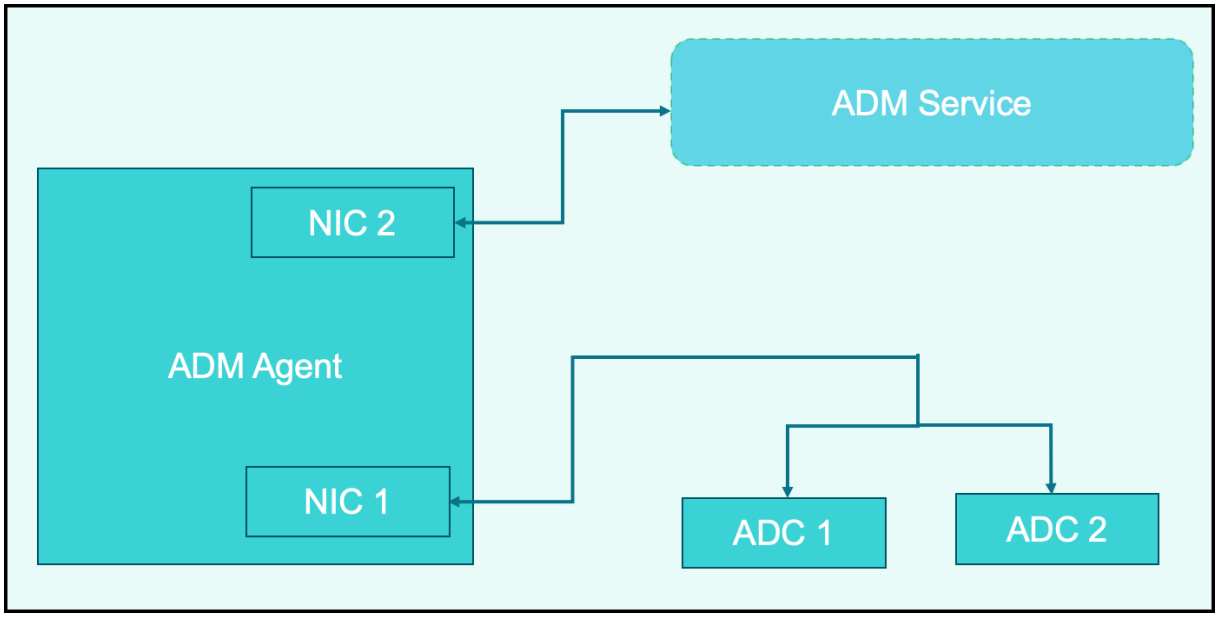
Dual-NIC-Unterstützung auf der NetScaler Console

January 26, 2024

Sie können zwei NICs auf einem Agenten konfigurieren. Mithilfe der Dual-NIC-Architektur kann der Agent:

- Stellen Sie die Kommunikation zwischen dem Agenten und den NetScaler-Instanzen her —Sie können die erste Netzwerkkarte verwenden, um den über die NetScaler Console empfangenen und gesendeten Datenverkehr zu isolieren und auch um zwischen NetScaler Console und den verwalteten NetScaler-Instanzen in einem anderen Netzwerk zu kommunizieren.
- Stellen Sie die Kommunikation zwischen dem Agenten und der NetScaler Console her —Sie können die zweite NIC verwenden, um die NetScaler Console in einem Netzwerk zu verwalten und Verwaltungsaufgaben auszuführen.

> **Hinweis**
>
> Sie können die Funktionalität und Konfiguration der beiden NICS nicht austauschen.



In diesem Szenario können Sie als Administrator:

- Konfigurieren Sie die IP-Adresse für den Datenverkehr zwischen NetScaler Console und ihren verwalteten NetScaler-Instanzen.
- Konfigurieren Sie die IP-Adresse für die Verwaltung der NetScaler Console-Software, um alle Verwaltungsaufgaben in der Software auszuführen.

> **Hinweis**
>
> Es ist nicht zwingend erforderlich, zwei NICs für einen Agenten zu konfigurieren. Sie ist optional und nur erforderlich, wenn der Datenverkehr zwischen Agent, NetScaler Console Service und NetScaler-Instanzen getrennt werden muss.

Voraussetzungen

- Stellen Sie sicher, dass Sie den NetScaler Agent 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.

Ändern der IPV4-NIC-Netzwerkadressen

1. Öffnen Sie mithilfe eines SSH-Clients wie PuTTY eine SSHConnection zur NetScaler 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 Agent und NetScaler Communication
    - NIC 2 —Für die Kommunikation zwischen Agent und NetScaler Console


```
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.

Hinzufügen von Instanzen

January 26, 2024

Sie können Instanzen entweder beim ersten Einrichten der NetScaler Console oder später hinzufügen.

Instanzen sind NetScaler Appliances oder virtuelle Appliances, die Sie von der NetScaler Console aus erkennen, verwalten und überwachen möchten. Sie können die folgenden NetScaler Appliances und virtuellen Appliances zur NetScaler Console hinzufügen:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway
- Citrix Secure Web Gateway

Um Instanzen hinzuzufügen, müssen Sie entweder den Hostnamen oder die IP-Adresse jeder NetScaler-Instanz oder einen Bereich von IP-Adressen angeben.

Geben Sie ein Instanzprofil an, das NetScaler Console für den Zugriff auf die Instanz verwenden kann. Dieses Instanzprofil enthält den Benutzernamen und das Kennwort der Instanzen, die Sie dem Dienst hinzufügen möchten. Für jeden Instanztyp ist ein Standardprofil verfügbar. Beispielsweise ist das ns-root-Profil das Standardprofil für NetScaler-Instanzen. Die standardmäßigen NetScaler-Administratoranmeldeinformationen definieren dieses Profil. Wenn Sie die standardmäßigen Administratoranmeldeinformationen Ihrer Instanzen geändert haben, können Sie benutzerdefinierte Instanzprofile für diese Instanzen definieren. Wenn Sie die Anmeldeinformationen einer Instanz ändern, nachdem die Instanz erkannt wurde, müssen Sie das Instanzprofil bearbeiten oder ein Profil erstellen und dann die Instanz neu ermitteln.

Sie können von der NetScaler Console aus auf die GUIs von NetScaler-Instanzen zugreifen, nachdem Sie die Instanzen in der NetScaler Console hinzugefügt haben. Um von der NetScaler Console aus auf die NetScaler-Instanzen zuzugreifen, müssen Sie mit dem Citrix-Netzwerk verbunden sein.

> **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 der NetScaler Console steht die Cluster-IP-Adresse jedoch für den Cluster.
> - Für die NetScaler-Instanzen, die als HA-Paar eingerichtet sind, wird beim Hinzufügen einer

> Instanz automatisch die andere Instanz im Paar hinzugefügt.
>
> - Um sicherzustellen, dass der NetScaler-Benutzer über alle Berechtigungen verfügt, weisen Sie dem Benutzer in NetScaler Superuser-Berechtigungen zu. Weitere Informationen finden Sie unter Benutzer-, Benutzergruppen und Befehlsrichtlinien

Erstellen eines NetScaler Profils

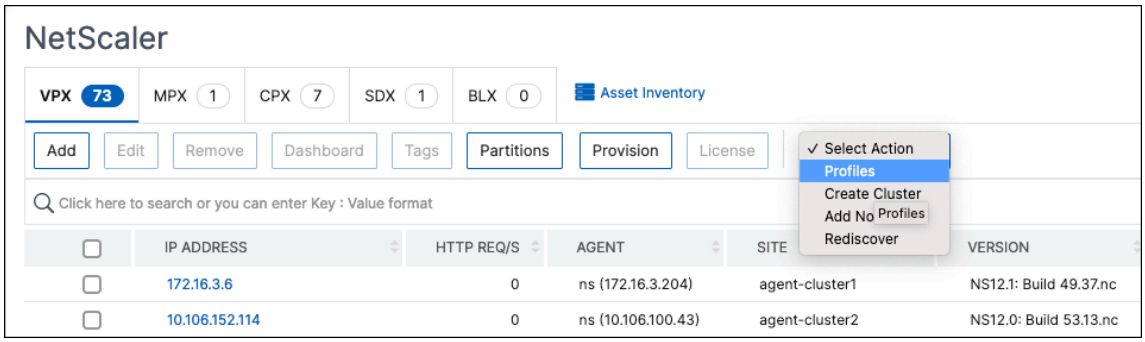
Das NetScaler-Profil enthält den Benutzernamen, das Kennwort, die Kommunikationsports und die Authentifizierungstypen der Instanzen, die Sie zur NetScaler Console hinzufügen möchten. Für jeden Instanztyp ist ein Standardprofil verfügbar. Zum Beispiel ist `nsroot` das Standardprofil für NetScaler-Instanzen. 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.

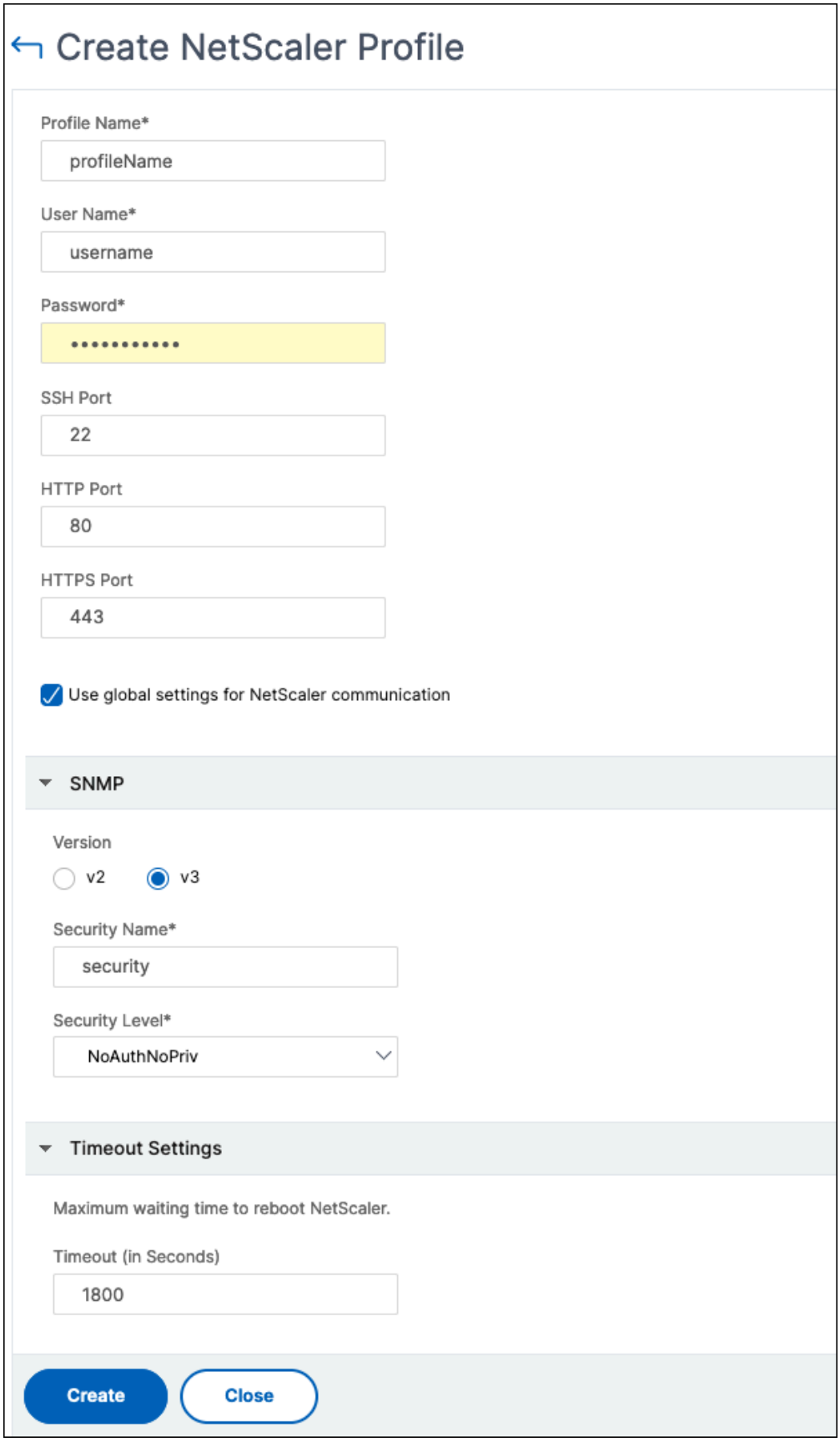
So erstellen Sie ein NetScaler Profil auf der Instanzseite:

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 Console und der NetScaler-Instanz an.

e) **HTTP-Port**: Geben Sie den Port für die HTTP-Kommunikation zwischen NetScaler Console 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 Console und NetScaler CPX verwendet werden.

f) **HTTPS-Port**: Geben Sie den Port für die HTTPS-Kommunikation zwischen NetScaler Console 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 benutzerdefinierte HTTPS-Port kann nur für die Kommunikation zwischen NetScaler Console 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 Console und NetScaler-Instanz verwenden möchten, andernfalls wählen Sie entweder HTTP oder https.

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 Console warten muss, bevor nach einem Neustart eine Verbindungsanforderung an die NetScaler-Instanz gesendet wird.

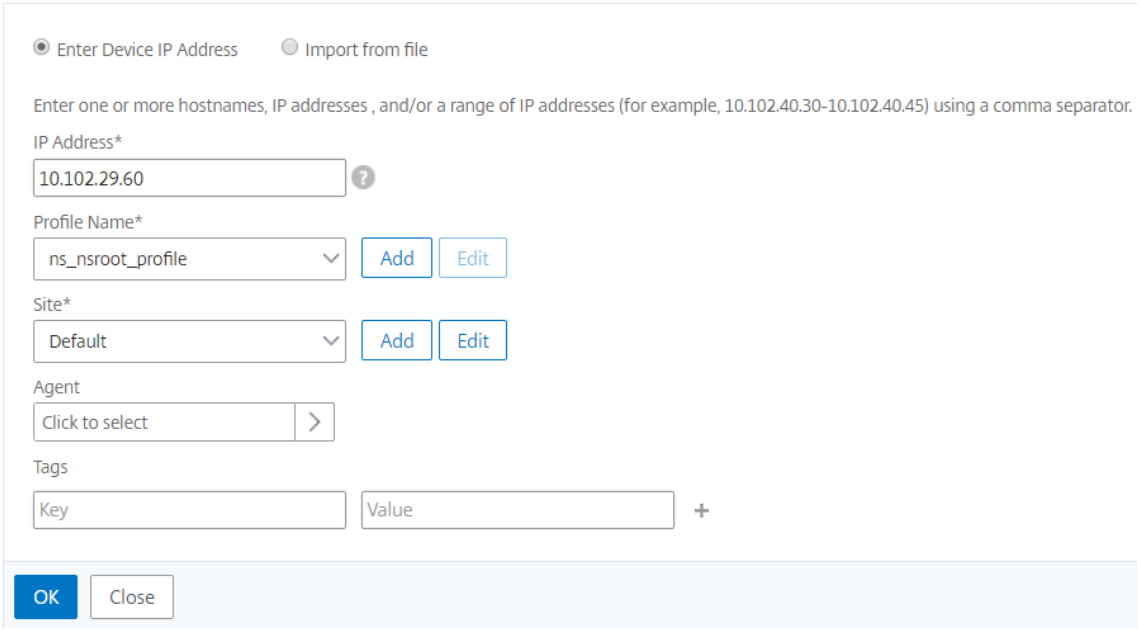
j) Wählen Sie **Create**.

So fügen Sie der NetScaler Console eine NetScaler-Instanz hinzu

> **Hinweis**
>
> Führen Sie diese Aufgabe aus, um alle anderen NetScaler-Instanzen mit Ausnahme der NetScaler CPX-Instanz hinzuzufügen.

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**. Wählen Sie unter Instanzen den Instanztyp aus, den Sie hinzufügen möchten (z. B. NetScaler VPX), und klicken Sie auf **Hinzufügen**.
2. Wählen Sie eine der folgenden Optionen:
   - **Geben Sie die Geräte-IP-Adresse** ein —Geben Sie für NetScaler-Instanzen entweder den Hostnamen oder die IP-Adresse jeder Instanz oder einen Bereich von IP-Adressen an.
   - **Aus Datei importieren** —Laden Sie von Ihrem lokalen System eine Textdatei hoch, die die IP-Adressen aller Instanzen enthält, die Sie hinzufügen möchten.
3. (Optional) Wählen Sie **Gerätezusatz beim ersten Anmeldefehler aktivieren**aus. Mit dieser Option können Sie die Instanz auch ohne gültige Anmeldeinformationen hinzufügen.
4. Wählen Sie unter **Profilname** das entsprechende Instanzprofil aus, oder erstellen Sie ein Profil, indem Sie auf das Symbol **+** klicken.
5. Wählen Sie unter **Site**die Site aus, zu der die Instanz hinzugefügt werden soll.
6. Wählen Sie **unter Agent**den Agent aus, dem Sie die Instanzen zuordnen möchten, und klicken Sie dann auf **OK**.

   Wenn auf Ihrer NetScaler Console nur ein Agent konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.



So fügen Sie eine NetScaler CPX-Instanz in der NetScaler Console hinzu

1. Navigieren Sie zu **Infrastruktur > Instanzen**. Wählen Sie unter **Instanzen**die Option **NetScaler** und wählen Sie die Registerkarte CPX.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie eine der folgenden Optionen:
   - **Geben Sie die Geräte-IP-Adresse**ein. Geben Sie entweder den Hostnamen oder die IP-Adresse jeder Instanz oder einen Bereich von IP-Adressen an.
   - **Aus einer Datei importieren**. Laden Sie von Ihrem lokalen System eine Textdatei hoch, die die IP-Adressen aller Instanzen enthält, die Sie hinzufügen möchten.
4. (Optional) Wählen Sie **Gerätezusatz beim ersten Anmeldefehler aktivieren**aus. Mit dieser Option können Sie die Instanz auch ohne gültige Anmeldeinformationen hinzufügen.
5. Geben Sie im Feld **Routable IP/Docker IP** die IP-Adresse ein. Die IP-Adresse kann entweder die NetScaler CPX-Instanz (falls sie erreichbar ist) oder der Docker-Host sein.
6. Wählen Sie im Feld **Profilname** das entsprechende Instanzprofil aus, oder erstellen Sie ein Profil, indem Sie auf das +-Symbol klicken.

   > **Hinweis:**
   >
   > Stellen Sie beim Erstellen eines Profils sicher, dass Sie die HTTP-, HTTPS-, SSH- und SNMP-Port-Details des Hosts angeben. Sie können auch den Port-Bereich angeben, der vom Host

> veröffentlicht wird, im Feld Startport und Anzahl der Ports.

7. Wählen Sie optional die Site aus, an der Sie die CPX-Instanz bereitstellen möchten. Sie können eine Site auch erstellen, indem Sie auf **Hinzufügen**klicken.
8. Falls verfügbar, wählen Sie den Agenten aus der Agentenliste aus.
9. Klicken Sie auf **OK** , um das Hinzufügen von Instanzen zur NetScaler Console zu starten.

> **Hinweis**
>
> Wenn Sie eine Instanz wiederfinden möchten, führen Sie die folgenden Schritte aus:
>
> a) Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** > **CPX**.
> b) Wählen Sie die Instanz aus, die Sie wiederentdecken möchten.
> c) Klicken **Sie in der Liste Aktion auswählen** auf **Erneut ermitteln**.

So fügen Sie eine eigenständige NetScaler BLX-Instanz in NetScaler Console 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. (Optional) Wählen Sie **Gerätezusatz beim ersten Anmeldefehler aktivieren**aus. Mit dieser Option können Sie die Instanz auch ohne gültige Anmeldeinformationen hinzufügen.
4. Wählen Sie in der Liste **Instanztyp** die Option **Standalone** aus.
5. Geben Sie im Feld **IP-Adresse** die IP-Adresse der BLX-Instanz an.
6. Geben Sie im Feld **Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die BLX-Instanz gehostet wird.
7. Wählen Sie in der Liste **Profilname** das entsprechende Profil für eine BLX-Instanz aus, oder erstellen Sie ein Profil.

   Um ein Profil zu erstellen, klicken Sie auf **Hinzufügen**.

   > **Wichtig**
   >
   > Stellen Sie sicher, dass Sie den richtigen Host-Benutzernamen und das richtige Kennwort des Linux-Servers im Profil angegeben haben.

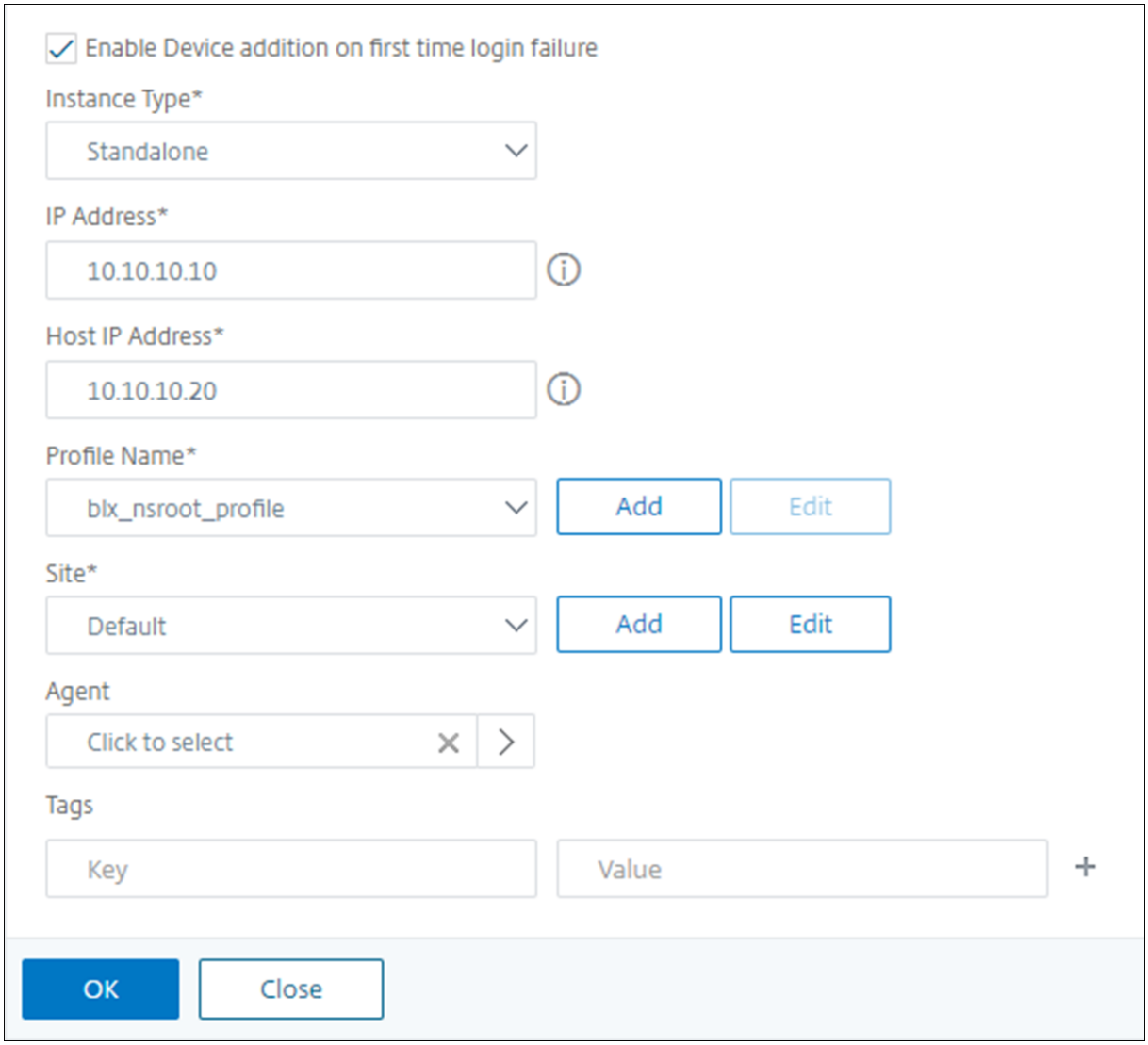
8. Wählen Sie in der Liste **Site** die Site aus, der Sie eine Instanz hinzufügen möchten.

   Wenn Sie eine Site hinzufügen möchten, klicken Sie auf **Hinzufügen**.

9. **Wählen Sie in der Agentenliste den Agenten aus, dem Sie die Instanz zuordnen möchten.

   Wenn auf Ihrer NetScaler Console nur ein Agent konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.

10. Klicken Sie auf **OK**.



So fügen Sie hochverfügbare NetScaler BLX-Instanzen in NetScaler Console hinzu

Die hochverfügbaren NetScaler BLX-Instanzen, die auf verschiedenen Host-Linux-Servern ausgeführt werden. Ein Linux-Server kann nicht mehr als eine BLX-Instanzen hosten.

1. Klicken Sie auf der Registerkarte **BLX** auf **Hinzufügen**.
2. (Optional) Wählen Sie **Gerätezusatz beim ersten Anmeldefehler aktivieren**aus. Mit dieser Option können Sie die Instanz auch ohne gültige Anmeldeinformationen hinzufügen.

3. Wählen Sie die Option **Hochverfügbarkeit** aus der Liste **Instanztyp** aus.
4. Geben Sie im Feld **IP-Adresse** die IP-Adresse der BLX-Instanz an.
5. Geben Sie im Feld **Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die BLX-Instanz gehostet wird.
6. Geben Sie im Feld **Peer-IP-Adresse** die IP-Adresse der Peer-BLX-Instanz an.
7. Geben Sie im Feld **Peer-Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die Peer-BLX-Instanz gehostet wird.
8. Wählen Sie in der Liste **Profilname** das entsprechende Profil für eine BLX-Instanz aus, oder erstellen Sie ein Profil.

   Um ein Profil zu erstellen, klicken Sie auf **Hinzufügen**.

   > **Wichtig**
   >
   > Stellen Sie sicher, dass Sie den richtigen Host-Benutzernamen und das richtige Kennwort des Linux-Servers im Profil angegeben haben.

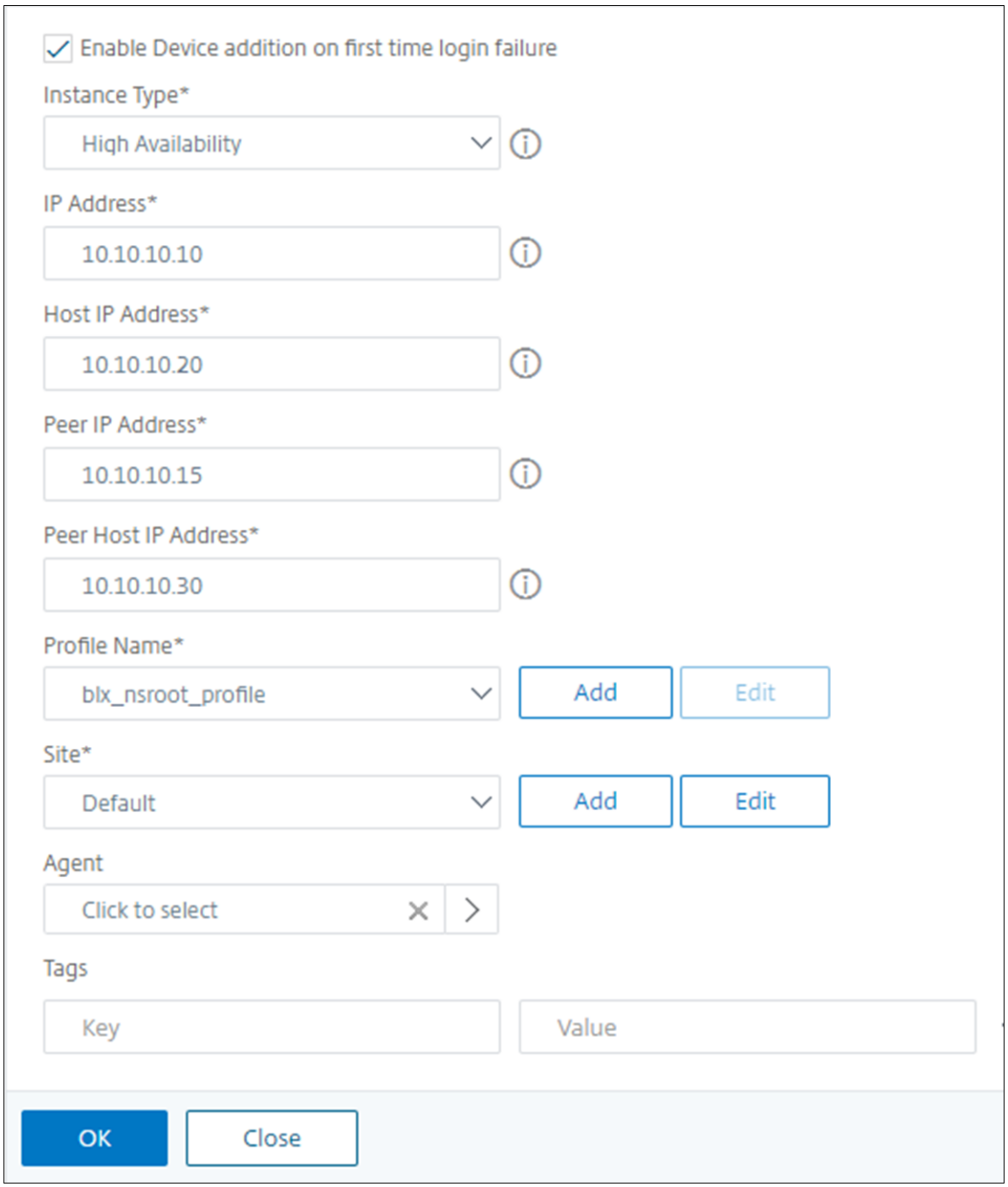
9. Wählen Sie in der Liste **Site** die Site aus, der Sie eine Instanz hinzufügen möchten.

   Wenn Sie eine Site hinzufügen möchten, klicken Sie auf **Hinzufügen**.

10. **Wählen Sie in der Agentenliste den Agenten aus, dem Sie die Instanz zuordnen möchten.

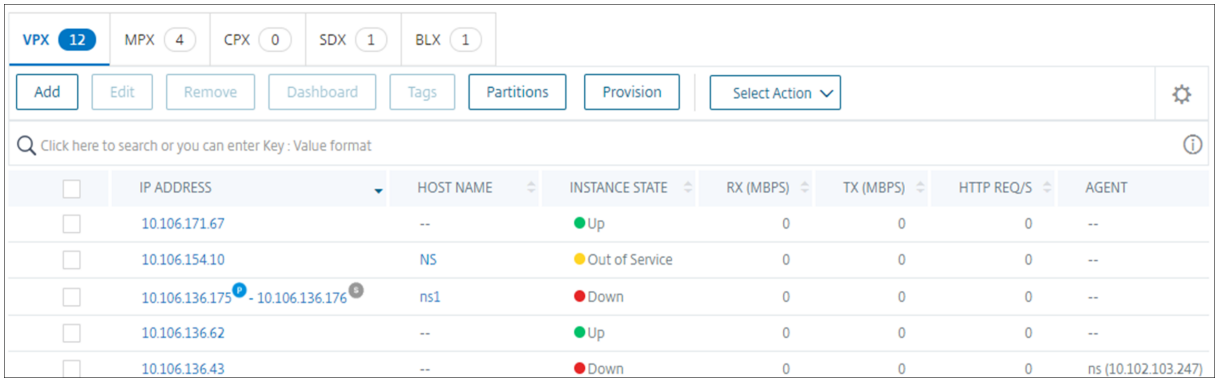
    Wenn auf Ihrer NetScaler Console nur ein Agent konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.

11. Klicken Sie auf **OK**.



So greifen Sie von der NetScaler Console aus auf eine Instanz-GUI zu

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 IP-Adressen der Instanz geben den Bereitstellungstyp mit den folgenden Notationen an:

- Beim Hochverfügbarkeitspaar **P** —Primärserver und **S** —Sekundärserver.
- **C**-Cluster
- **A**-Autoscale-Gruppe

Wenn eine Instanz keine Notation hat, zeigt dies die eigenständige Bereitstellung an.

Die GUI der ausgewählten Instanz wird in einem Popup-Fenster angezeigt.

Lösen Sie Instanzwarnungen

Ein Warnzeichen wird aus folgenden Gründen auf der Instanz angezeigt:

- **Anmeldung fehlgeschlagen** - Wenn Sie eine Instanz ohne gültige Anmeldeinformationen hinzufügen, wird sie im Status DOWN mit einer Warnung bei Anmeldung fehlgeschlagen angezeigt. Geben Sie die richtigen Anmeldeinformationen an, um die Instanz in NetScaler Console zu verwalten.

  Wenn die Instanz nicht lizenziert ist, wird die Option **Lizenz** angezeigt, wenn Sie die Instanz auswählen. Klicken Sie auf **Lizenz**, um die Lizenz auf eine Instanz aus dem Lizenzpool anzuwenden.
- **Unlizenzierte Instanz mit HTTPS-Profil**—Wenn eine unlizenzierte Instanz nur eine HTTPS-Verbindung verwendet, wenden Sie die Lizenz über die NetScaler-GUI auf eine Instanz an.

Syslog auf Instanzen konfigurieren

July 17, 2024

Das Syslog-Protokoll bietet einen Transport, der es den NetScaler-Instanzen ermöglicht, Ereignisbenachrichtigungen an die NetScaler Console zu senden, die als Collector oder Syslog-Server für diese Nachrichten konfiguriert ist.

Sie können die auf Ihren NetScaler-Instanzen generierten Syslog-Ereignisse überwachen, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Meldungen an NetScaler Console umgeleitet werden. Um Syslog-Ereignisse zu überwachen, müssen Sie zunächst NetScaler Console als Syslog-Server für Ihre NetScaler-Instanz konfigurieren. Nach der Konfiguration der Instanz werden alle Syslog-Meldungen an NetScaler Console umgeleitet, sodass diese Protokolle dem Benutzer strukturiert angezeigt werden können.

Syslog verwendet das User Datagram Protocol (UDP), Port 514, für die Kommunikation, und da UDP ein verbindungsloses Protokoll ist, gibt es keine Rückmeldung an die Instanzen. Die Syslog-Paketgröße ist auf 1024 Byte begrenzt und enthält die folgenden Informationen:

- Einrichtung
- Schweregrad
- Hostname
- Zeitstempel
- Meldung

In NetScaler Console müssen Sie die Facility- und Log-Schweregrade für die Instanzen konfigurieren.

- **Einrichtung** - Syslog-Nachrichten werden anhand der Quellen, die sie generieren, grob kategorisiert. Diese Quellen können das Betriebssystem, der Prozess oder eine Anwendung sein. Diese Kategorien werden als Einrichtungen bezeichnet und durch ganze Zahlen dargestellt. Beispielsweise wird 0 von Kernel-Nachrichten verwendet, 1 wird von Nachrichten auf Benutzerebene verwendet, 2 wird vom Mailsystem verwendet usw. Die lokalen Nutzungsmöglichkeiten (von local0 bis local7) sind nicht reserviert und stehen für den allgemeinen Gebrauch zur Verfügung. Daher können die Prozesse und Anwendungen, für die keine vorab zugewiesenen Anlagenwerte vorhanden sind, an eine der acht Einrichtungen für den lokalen Einsatz geleitet werden.
- **Schweregrad** - Die Quelle oder Einrichtung, die die Syslog-Nachricht generiert, gibt auch den Schweregrad der Nachricht mit einer einstelligen Ganzzahl an, wie unten dargestellt:

```
1 - Emergency: System is unusable.

2 - Alert: Action must be taken immediately.

3 - Critical: Critical conditions.

4 - Error: Error conditions.

5 - Warning: Warning conditions.
```



```
10
11   6 - Notice: Normal but significant condition.
12
13   7 - Informational: Informational messages.
14
15   8 - Debug: Debug-level messages.
```

So konfigurieren Sie Syslog auf NetScaler-Instanzen:

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Instanzen** .
2. Wählen Sie die NetScaler-Instanz aus, von der die Syslog-Meldungen erfasst und in der NetScaler Console angezeigt werden sollen.
3. Wählen Sie in der Dropdownliste **Aktion** die Option **Syslog konfigurieren**aus.
4. Klicken Sie auf **Aktivieren**.
5. Wählen Sie in der Dropdownliste **Einrichtung** eine Einrichtung auf lokaler Ebene oder auf Benutzerebene aus.
6. Wählen Sie die erforderliche Protokollebene für die Syslog-Meldungen aus.
7. Klicken Sie auf **OK**.

Dadurch werden alle Syslog-Befehle in der NetScaler-Instanz konfiguriert, und die NetScaler Console beginnt, die Syslog-Meldungen zu empfangen. Sie können die Meldungen anzeigen, indem Sie zu **Infrastruktur > Ereignisse > Syslog-Meldungen**navigieren.

Übersicht über den Logstream

March 12, 2024

NetScaler-Instanzen generieren AppFlow Datensätze und stellen einen zentralen Kontrollpunkt für den gesamten Anwendungsdatenverkehr im Rechenzentrum dar. **IPFIX**und **Logstream** sind die Protokolle, die diese AppFlow-Datensätze von NetScaler-Instanzen zur NetScaler Console transportieren. Weitere Informationen finden Sie unter AppFlow.

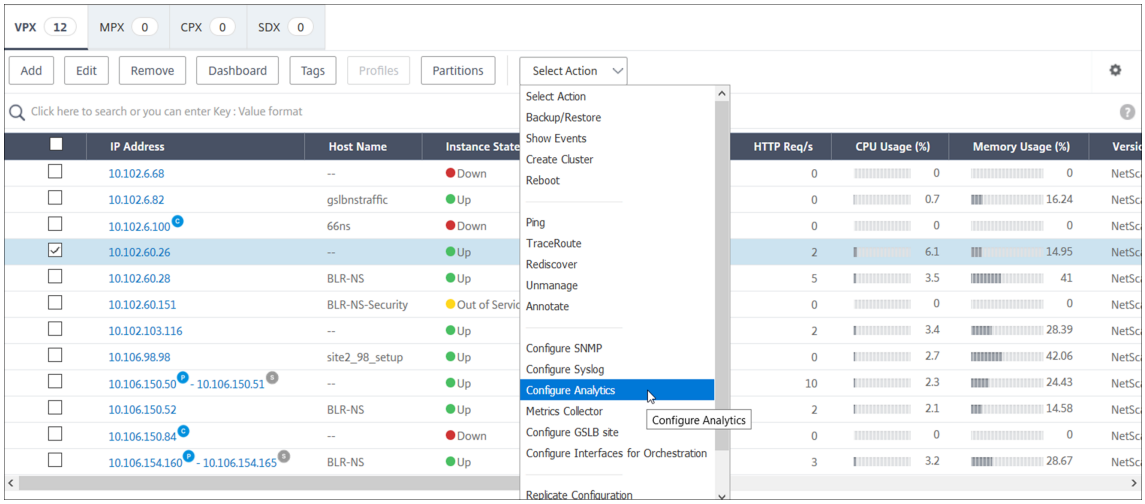
- **IPFIX** ist ein offener Standard der Internet Engineering Task Force (IETF), der in RFC 5101 definiert ist. **IPFIX** verwendet das UDP-Protokoll, ein unzuverlässiges Transportprotokoll, das für den Datenfluss in eine Richtung verwendet wird. Da IPFIX das UDP-Protokoll verwendet, führt die Einhaltung des IPFIX-Standards dazu, dass mehr Ressourcen in NetScaler Console verarbeitet werden.
- **Logstream**ist ein Citrix-eigenes Protokoll, das als einer der Transportmodi verwendet wird, um die Analytics-Protokolldaten effizient von NetScaler-Instanzen zur NetScaler Console zu übertragen. **Logstream** verwendet ein zuverlässiges TCP-Protokoll und benötigt weniger Ressourcen bei der Verarbeitung der Daten.

Für NetScaler zwischen **11.1 Build 47.14 und 11.1 Build 62.8** ist **Logstream** der Standardtransportmodus für die Aktivierung von Web Insight (HTTP) und IPFIX der einzige Transportmodus für die Aktivierung anderer Erkenntnisse. Für NetScaler Version ab **12.0 bis zur neuesten Version** können Sie entweder **Logstream**oder **IPFIX** als Transportmodus auswählen.

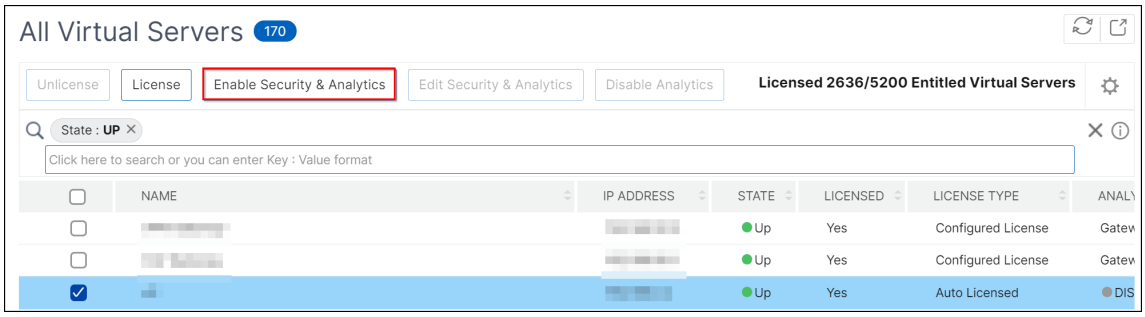
> **Hinweis**
>
> Die Version und der Build der NetScaler Console müssen Ihrer NetScaler-Version und Ihrem Build entsprechen oder **höher** sein. Wenn Sie beispielsweise NetScaler 12.1 Build 50.28/50.31 installiert haben, stellen Sie sicher, dass Sie NetScaler Console 12.1 Build 50.39 oder höher installiert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

Logstream als Transportmodus aktivieren

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 die virtuellen Server aus und klicken Sie dann auf **Security & Analytics aktivieren**.



4. Gehen Sie im Fenster **Enable Security & Analytics** wie folgt vor:

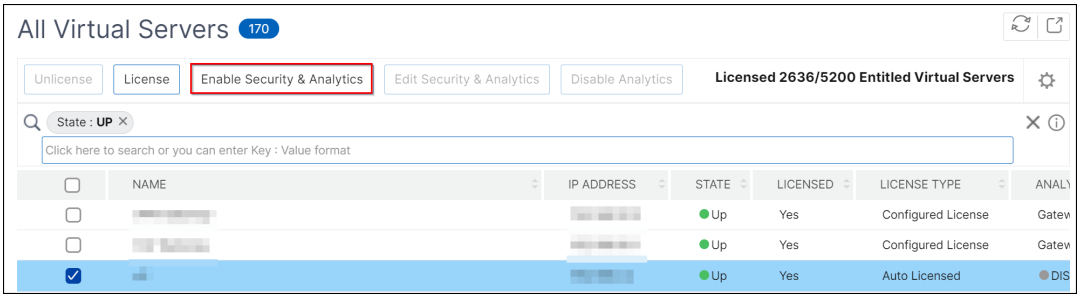
a) Wählen Sie die Insight-Typen aus (Web Insight- oder WAF-Sicherheitsverletzungen oder Bot-Sicherheitsverletzungen)

b) Wählen Sie **Logstream** als Transportmodus

> **Hinweis**
>
> Für NetScaler zwischen **11.1 Build 47.14 und 11.1 Build 62.8** ist **Logstream** der Standardtransportmodus für die Aktivierung von Web Insight (HTTP) und IPFIX der einzige Transportmodus für die Aktivierung anderer Erkenntnisse. Für NetScaler Version ab **12.0 bis zur neuesten Version** können Sie entweder **Logstream**oder **IPFIX** als Transportmodus auswählen.

c) Der Ausdruck ist standardmäßig wahr

d) Klicken Sie auf **Analytics speichern**



> **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.

In der folgenden Tabelle werden die Funktionen der NetScaler Console beschrieben, die **Logstream** als Transportmodus unterstützt:

Feature	**IPFIX**	**Logstream**
Web Insight	•	•
Bot-Sicherheitsverstöße	Nicht unterstützt	•
Sicherheitsverletzungen der WAF	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Nicht unterstützt	•

Feature	IPFIX	Logstream
CR-Einblick	•	•
IP-Reputation	•	•
AppFirewall	•	•
Kundenseitige Messung	•	•
Syslog/Auditlog	•	•

So weisen Sie delegierten Admin-Benutzern weitere Berechtigungen zu

January 26, 2024

Wenn sich der erste Benutzer Ihrer Organisation anmeldet und sich bei NetScaler Console anmeldet, werden diesem Benutzer die Superadmin-Rechte zugewiesen. Jedem nachfolgenden Benutzer, der sich anmeldet, wird standardmäßig eine delegierte Administratorrolle zugewiesen. Ein delegierter Administrator verfügt nicht über die Berechtigung zum Anzeigen und Ausführen von Aufgaben im Zusammenhang mit der Benutzerverwaltung oder RBAC-Einstellungen.

Sie können jedoch einem delegierten Administrator Superadmin-Berechtigungen oder bestimmte Nicht-Super-Admin-Rollen zuweisen, damit der Administrator Aufgaben im Zusammenhang mit der Benutzerverwaltung ausführen kann.

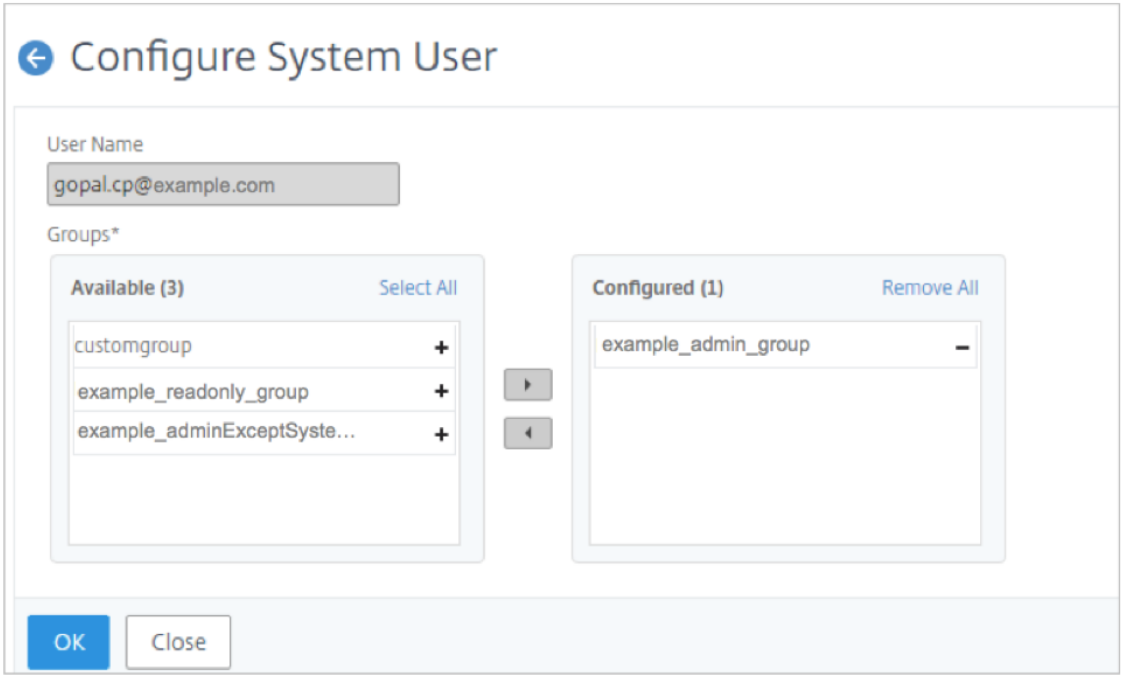
Detaillierte Informationen zur rollenbasierten Zugriffssteuerung finden Sie unter Konfigurieren der rollenbasierten Zugriffssteuerung.

Zuweisen von Super-Admin-Berechtigungen an einen delegierten Administrator

Um einem delegierten Administrator Super-Admin-Berechtigungen zuzuweisen, muss ein Superadministrator die Standardadministratorgruppe einem delegierten Admin-Benutzer zuweisen. Führen Sie die folgenden Aufgaben aus:

1. Melden Sie sich als Superadmin bei NetScaler Console an.
2. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Benutzer**.
3. Wählen Sie den Benutzernamen des delegierten Administrators aus und klicken Sie auf **Bearbeiten**.

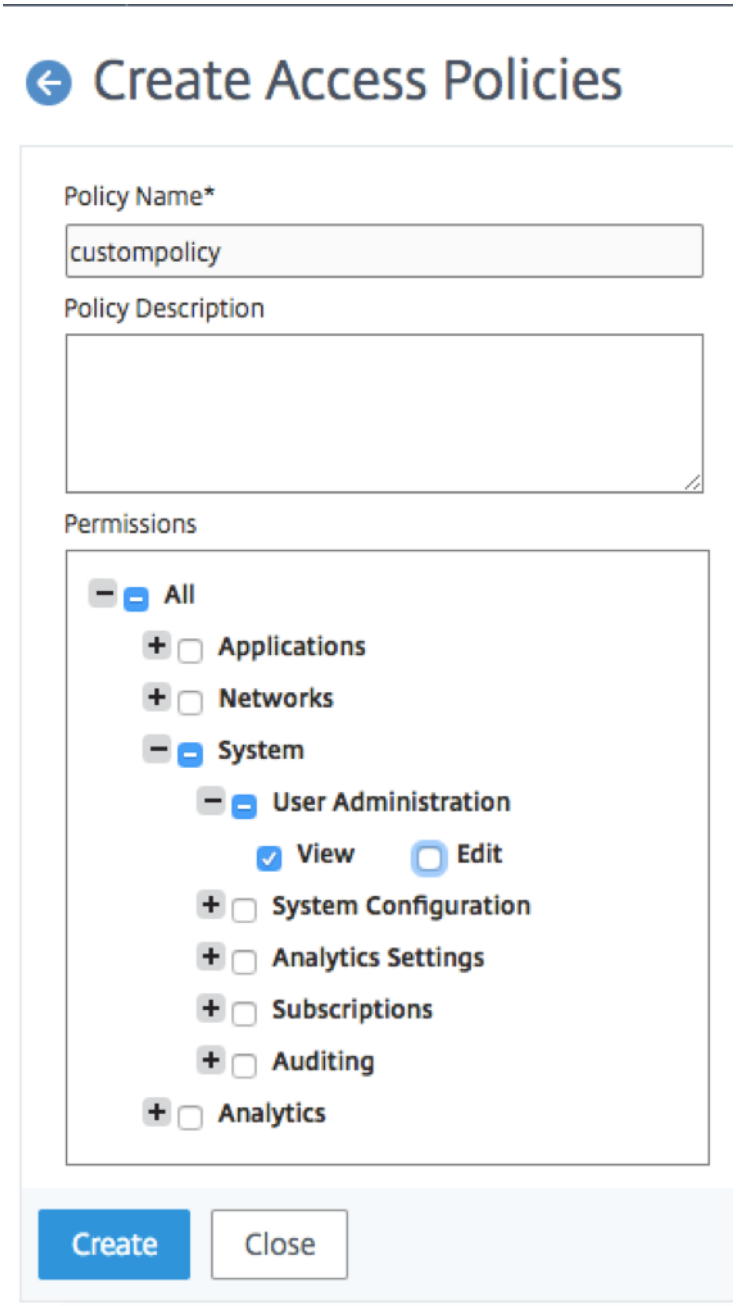
4. Assign the group ***<tenant_name>*_admin_group** to the delegated admin and click **OK**. In der folgenden Abbildung wird beispielsweise “example_admin_group”einem delegierten Admin-Benutzer zugewiesen.



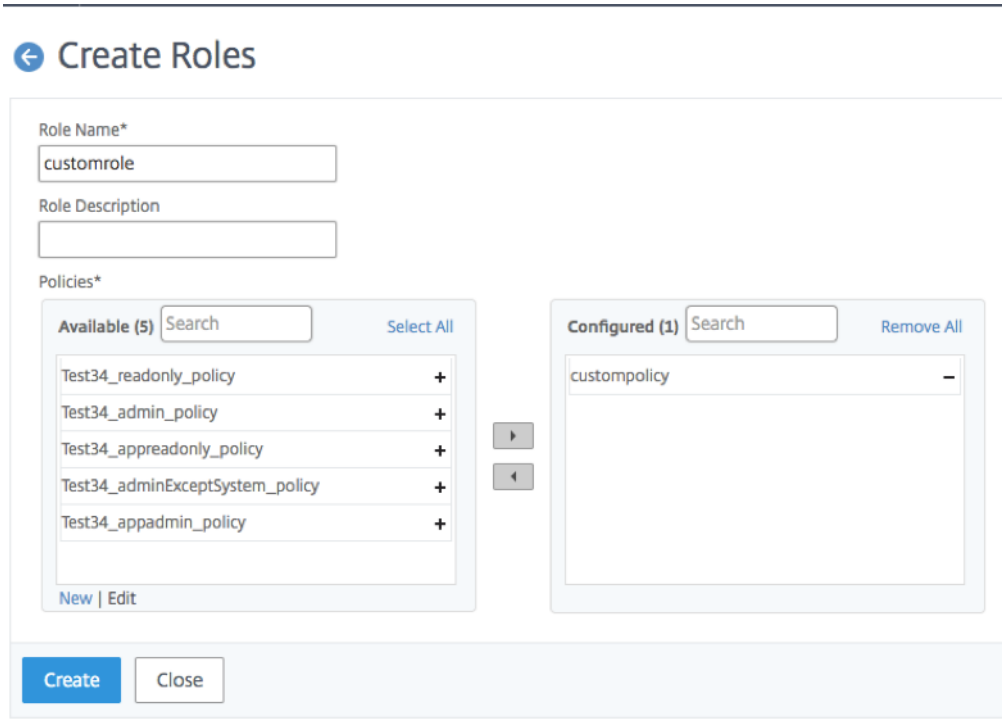
Zuweisen einer benutzerdefinierten Rolle zu einem delegierten Administrator

Um eine beliebige benutzerdefinierte Rolle einem delegierten Administrator zuzuweisen, muss der Superadmin eine Gruppe, Rolle und Richtlinie erstellen und dem delegierten Administratorbenutzer zuweisen. Dadurch wird sichergestellt, dass der delegierte Administrator nur über die erforderlichen Berechtigungen verfügt. Führen Sie die folgenden Aufgaben aus:

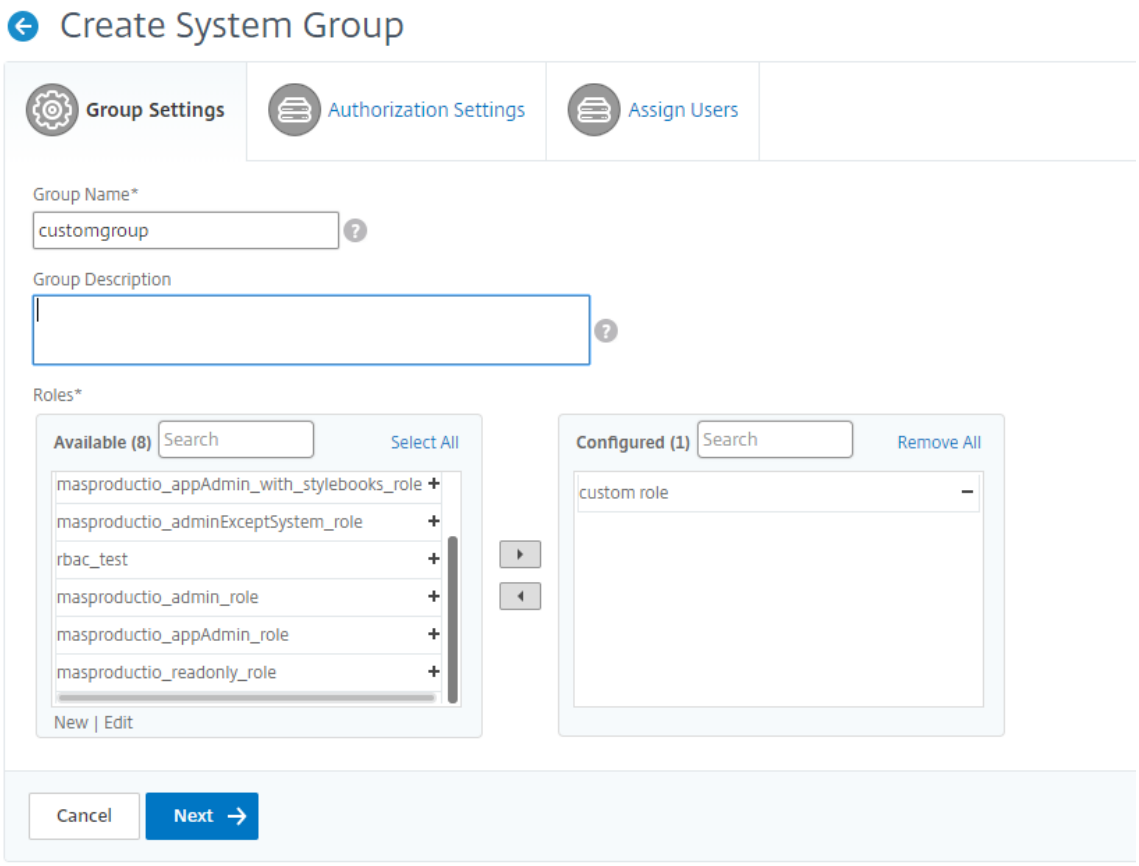
1. Melden Sie sich als Superadmin bei NetScaler Console an.
2. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Zugriffsrichtlinien**. Wählen Sie **Hinzufügen** aus, um eine Zugriffsrichtlinie mit den erforderlichen Berechtigungen für den delegierten Administrator zu erstellen. In diesem Beispiel `custompolicy` wird eine Zugriffsrichtlinie erstellt, die den Zugriff auf die Einstellungen der Benutzerverwaltung ermöglicht.



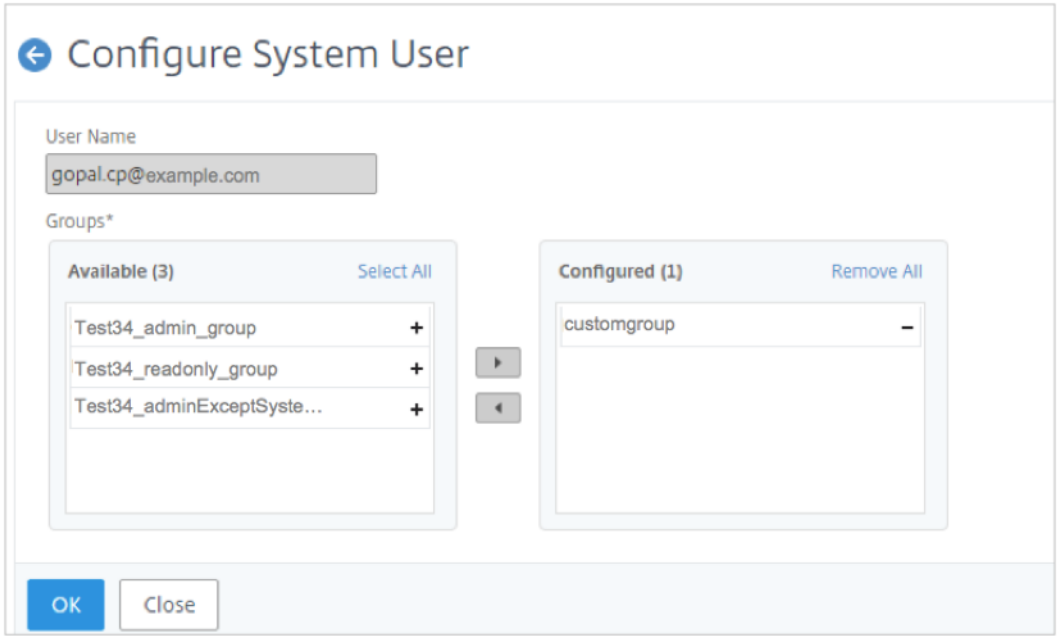
3. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Rollen**. Wählen Sie **Hinzufügen** aus, um eine Rolle zu erstellen und diese Rolle an die im vorherigen Schritt erstellte Zugriffsrichtlinie zu binden. In diesem Beispiel `customrole` wird eine Rolle erstellt und an die `custompolicy` Zugriffsrichtlinie gebunden.



4. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Gruppen**. Wählen Sie **Hinzufügen** aus, um eine Gruppe zu erstellen und diese Gruppe an die Rolle zu binden, die Sie im vorherigen Schritt erstellt haben. In diesem Beispiel wird die Gruppe “benutzerdefinierte Gruppe”erstellt und an die Rolle “benutzerdefinierte Rolle”gebunden.



5. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Benutzer**
6. Wählen Sie den Benutzernamen des delegierten Administrators aus und klicken Sie auf **Bearbeiten**.
7. Weisen Sie die Gruppe, die Sie im vorherigen Schritt erstellt haben, dem delegierten Admin-Benutzer zu. In diesem Beispiel wird dem delegierten Admin-Benutzer die Gruppe zugewiesen `customgroup`.



Integration mit der ServiceNow-Instanz

January 26, 2024

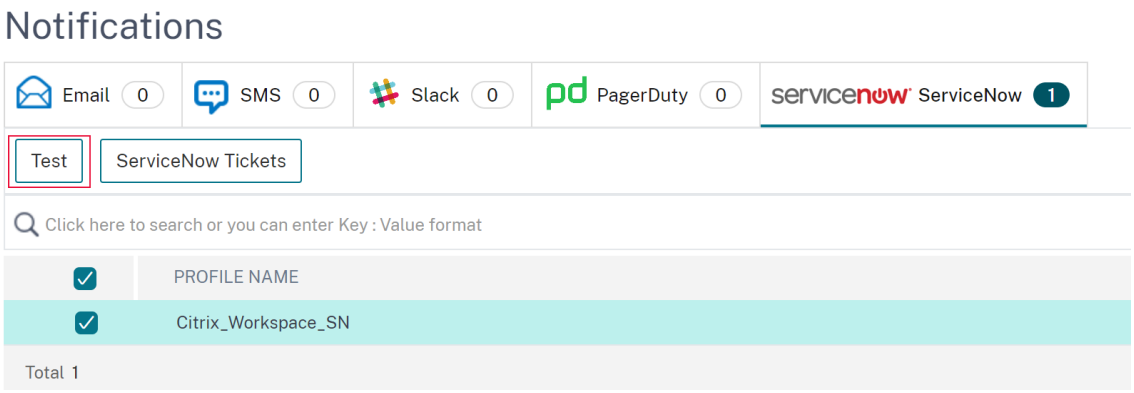
Als NetScaler-Administrator können Sie ServiceNow als primäres IT-Anforderungs- und Supportsystem verwenden. Sie müssen Tickets oder Vorfälle für die kritischen NetScaler-Ereignisse erstellen, um sie zu untersuchen, zu verfolgen und zu beheben.

Sie können die Ticketerstellung in ServiceNow mithilfe der NetScaler Console und des Citrix ITSM Connectors für ServiceNow automatisieren. Um diese Automatisierung zu starten, integrieren Sie den Citrix ITSM-Adapterdienst, um Ereignisse zu empfangen und relevante Vorfälle in ServiceNow zu erstellen. Weitere Informationen zu Vorbereitungs- und Integrationsschritten finden Sie unter Erste Schritte im Citrix ITSM-Adapterdienst.

Konfigurieren Sie nach der erfolgreichen Integration die automatische Generierung von ServiceNow-Incidents in NetScaler Console. Führen Sie die Schritte aus, um zu überprüfen, ob ServiceNow-Tickets automatisch generiert werden.

1. Melden Sie sich bei NetScaler Console an.
2. Navigieren Sie zu **Einstellungen > 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 Console-GUI anzeigen möchten, wählen Sie **ServiceNow-Tickets** aus.



Wenn Sie NetScaler Console in ServiceNow integrieren, können Sie die Generierung von ServiceNow-Incidents für Folgendes automatisieren:

- Alle NetScaler-Ereignisse
- SSL-Zertifikate, die bald ablaufen
- Die Ereignisse zum Ablauf der NetScaler Console-Lizenz

Außerdem können Sie die NetScaler Console-Ereignisrichtlinien anpassen.

Generieren Sie ServiceNow-Vorfälle für alle NetScaler-Ereignisse

In NetScaler Console können Sie Regeln konfigurieren, um automatisch ein Ticket in ServiceNow für bestimmte Ereignisse zu erstellen. NetScaler Console generiert automatisch ein ServiceNow-Ticket für Ereignisse wie:

- Virtuelle Server fallen aus oder sind außer Betrieb.
- Der Ressourcenverbrauch überschreitet den Schwellenwert.
- Die Lizenz läuft auf einer NetScaler-Instanz ab.

Das automatisch generierte Ticket in ServiceNow enthält die erforderlichen Details, um das Problem zu verfolgen und zu beheben. Sie können die Benachrichtigungen über ein oder mehrere Netzwerkgeräte hinweg von einer einzigen ServiceNow-Konsole aus verwalten. Weisen Sie dann den Administrator zur weiteren Analyse zu.

Sie können eine Ereignisregel in der NetScaler Console erstellen, indem Sie zu **Infrastruktur > Ereignisse Regeln** navigieren. Weitere Informationen finden Sie unter ServiceNow-Benachrichtigungen senden.

Generieren Sie ServiceNow-Vorfälle für SSL-Zertifikate, die bald ablaufen

Wenn ein SSL-Zertifikat auf NetScaler-Instanzen bald abläuft, generiert NetScaler Console automatisch ein ServiceNow-Ticket. Auf diese Weise können Sie die bevorstehenden Ablauftickets für SSL-Zertifikate im Voraus in Ihrem ServiceNow-Dashboard überprüfen.

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

Generieren Sie ServiceNow-Vorfälle für den Ablauf der NetScaler Console-Lizenz

In NetScaler Console können Sie die Regeln so konfigurieren, dass in ServiceNow automatisch ein Ticket für bestimmte Ereignisse zum Ablauf der NetScaler Console-Lizenz erstellt wird.

Informationen zum Senden von ServiceNow-Benachrichtigungen für den Ablauf der NetScaler Console-Lizenz finden Sie unter Ablauf der NetScaler Console-Lizenz.

Passen Sie die NetScaler Console-Ereignisrichtlinien an

Sie können Richtlinien definieren, um zu steuern, wie ServiceNow die NetScaler Console-Ereignisse auf der Grundlage von Ereignisattributen verarbeitet. Legen Sie die NetScaler Console-Ereignisrichtlinien im Citrix ITSM Connector fest. Sie können entscheiden, wie ein Vorfall in ADM generiert, verarbeitet und gemeldet werden muss. Führen Sie dann die folgenden Aktionen über ITSM aus:

- Ignoriere Vorfälle
- Vorfälle auf dem Dashboard anzeigen
- Vorfälle erstellen

Weitere Informationen finden Sie unter Anpassen der NetScaler Console-Ereignisrichtlinien .

Umsetzbare Aufgaben und Empfehlungen

June 7, 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** .

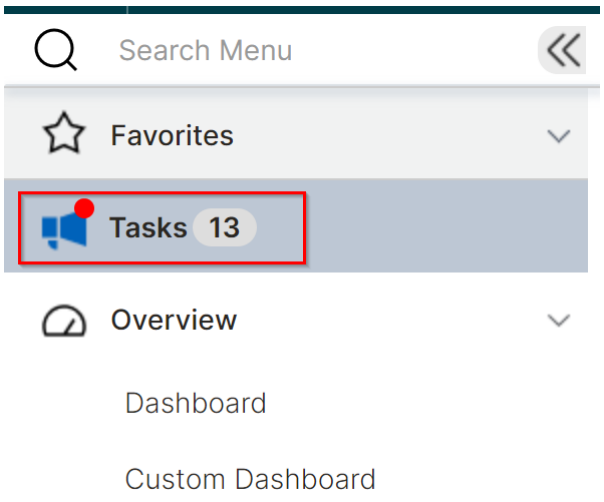
Möglicherweise haben Sie Hunderte von NetScaler-Instanzen erkannt und mehrere virtuelle Server (Anwendungen) von jeder Instanz aus konfiguriert. Als Administrator müssen Sie sicherstellen, dass alle NetScaler-Instanzen und Ihre Anwendungen effizient verwaltet werden, um Erkenntnisse für eine bessere 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 Console-Bereitstellung effizient, sicher und konform ist. Basierend auf Ihrer aktuellen Auslastung und Ihrem Abonnement können Sie mit der **Tasks**-Funktion in NetScaler Console sowohl umsetzbare **Aufgaben**, die Sie sofort ergreifen müssen, als auch **Empfehlungen** für eine effiziente Bereitstellung anzeigen.

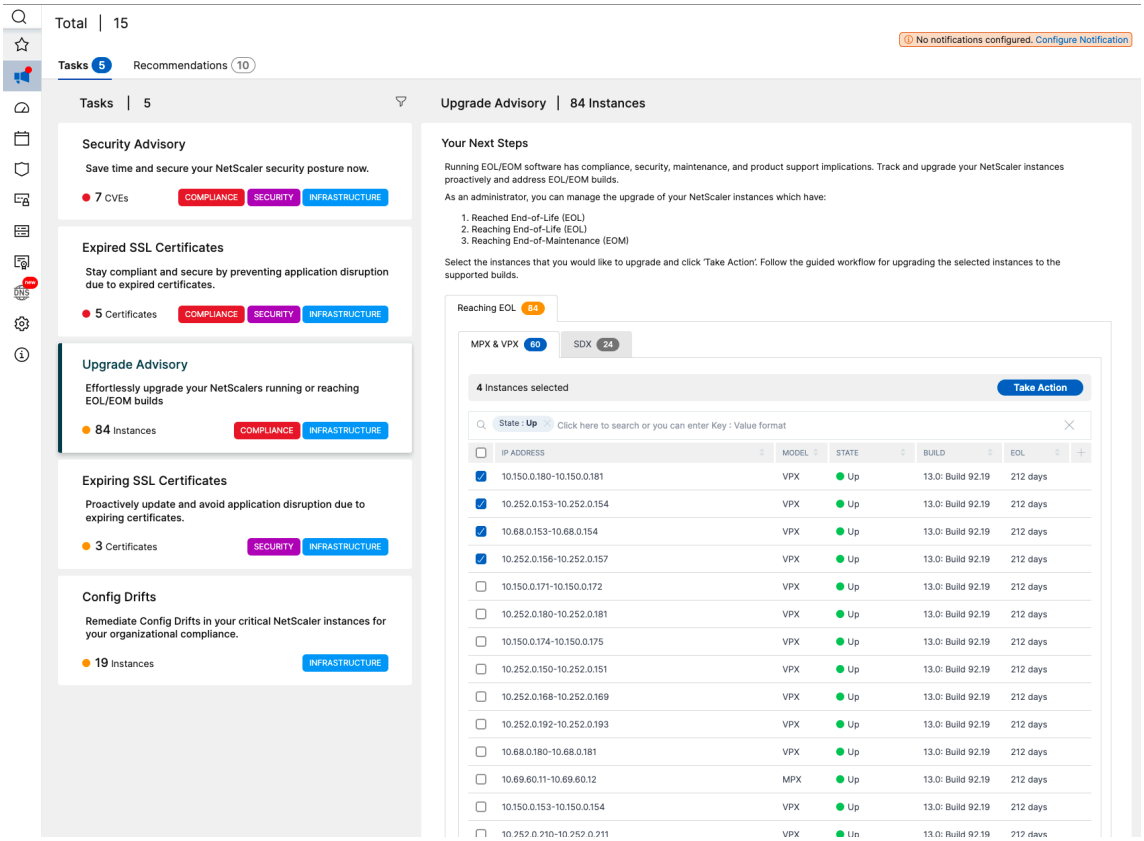
Als Administrator können Sie mithilfe dieser umsetzbaren **Aufgaben** und **Empfehlungen**:

- Verschaffen Sie sich einen sofortigen Überblick über alle Beobachtungen oder Probleme, die Ihr sofortiges Handeln erfordern.
- Konfigurieren Sie Benachrichtigungen so, dass Sie benachrichtigt werden, wenn NetScaler Console Aufgaben erkennt, und proaktiv Maßnahmen ergreifen.
- Sorgen Sie für eine effiziente Bereitstellung von NetScaler Console und NetScaler-Instanzen.
- Reduzieren Sie den entscheidenden Zeit- und Arbeitsaufwand bei der Identifizierung der kritischen Probleme.
- Stellen Sie sicher, dass Sie alle Funktionen der NetScaler Console nutzen, aktivieren Sie die Produkterkennung und die vom Produkt empfohlenen Funktionen für eine effiziente Verwaltung der Bereitstellung.

Klicken Sie in der NetScaler Console-GUI auf **Aufgaben** , um sowohl **Aufgaben** als auch **Empfehlungen** anzuzeigen.

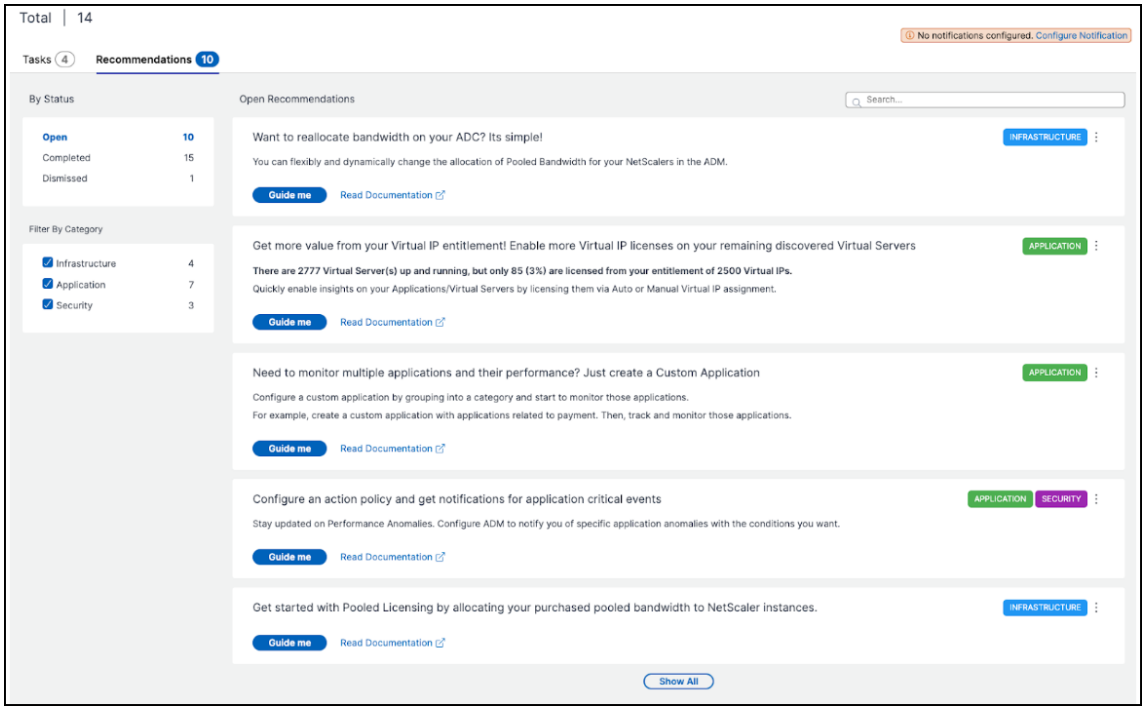


- **Aufgaben** —Ermöglicht es Ihnen, eine Liste von Aufgaben anzuzeigen, die Ihre sofortige Aufmerksamkeit und Aktion erfordern. Wenn Sie Ihre Infrastruktur erweitern, können einige kritische Probleme unbemerkt bleiben und zu Sicherheitslücken führen. NetScaler-Instanzen mit CVEs erfordern beispielsweise 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 5 Aufgaben anzeigen. Die Aufgaben werden basierend auf dem Schweregrad (Kritisch und Mittel) angezeigt.



- **Empfehlungen**—Enthält bestimmte Empfehlungen, die auf Ihrer aktuellen Auslastung basieren, um Ihre NetScaler Console-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 NetScaler Console-Bereitstellung die folgenden 4 Aufgaben anzeigen.

- **Abgelaufene SSL-Zertifikate**—Stellt Informationen zu den abgelaufenen SSL-Zertifikaten bereit, die in Ihrer NetScaler Console 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:

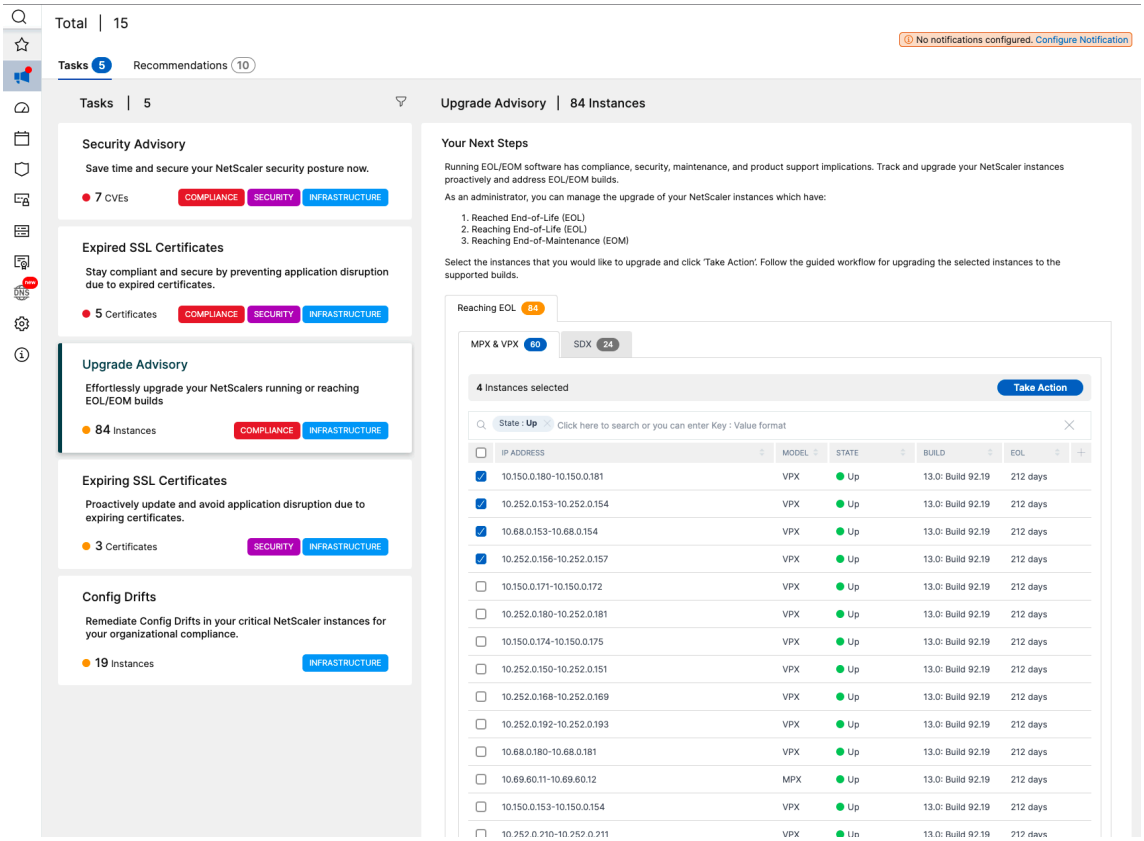
  - Entdeckte**CVEs: Zeigt die erkannten**CVEs und die NetScaler-Instanzen an, die sich auf die CVEs auswirken. Um diese Aufgabe abzuschließen, wählen Sie eine CVE aus und klicken Sie auf **Anzeigen und korrigieren.**

    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.**

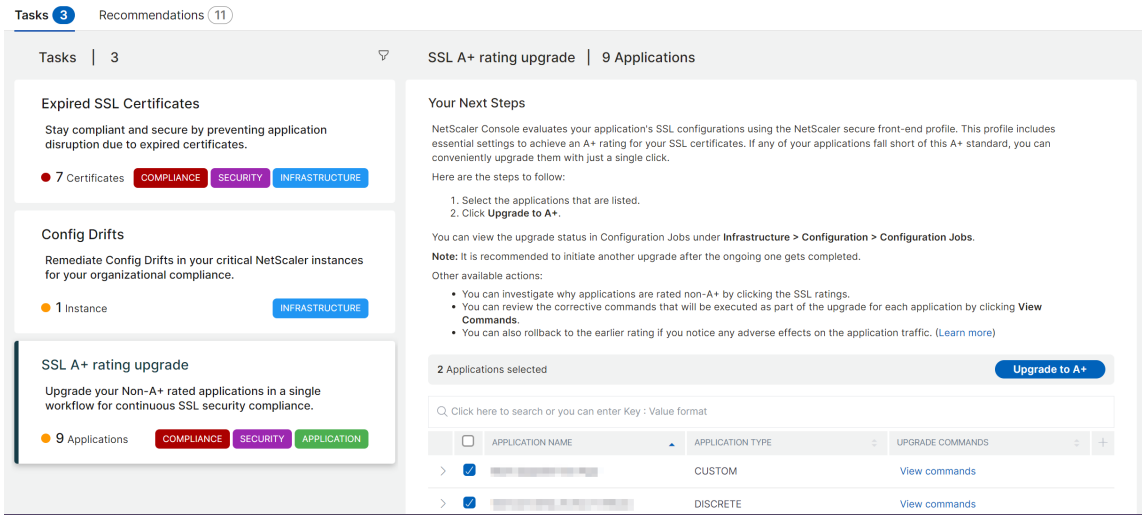
  Empfohlene Maßnahme: Sie werden unter **Infrastruktur > Instanzempfehlung >**Sicherheitsempfehlung**zur Seite mit Sicherheitshinweisen**weitergeleitet. Folgen Sie der Dokumentation, um die Aufgabe abzuschließen.

- **Upgrade-Empfehlung**: Enthält Informationen zu Ihren NetScaler-Instanzen, die das End of Life (EOL) oder das Ende der Wartung (EOM) bereits erreicht haben oder demnächst innerhalb von 90 Tagen erreichen werden.



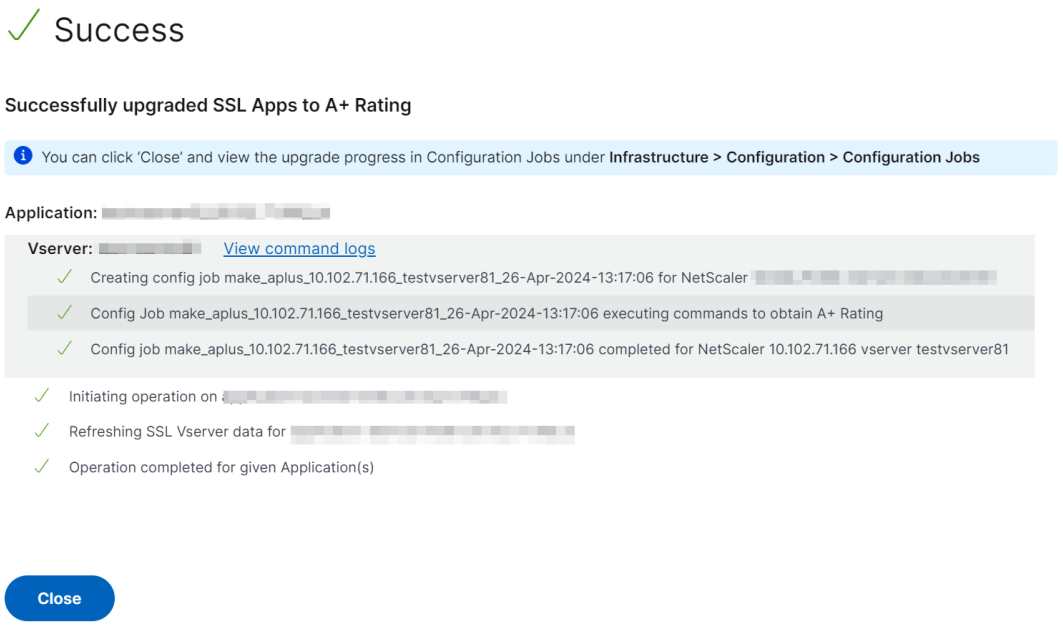
Empfohlene Aktion: Klicken Sie auf **Take Action** und aktualisieren Sie die Instanzen auf einen empfohlenen Build.

- **Upgrade der SSL-Bewertung A+**: Stellt Informationen zu Ihren Anwendungen bereit, die nicht mit einer A+-Bewertung konform sind.



Empfohlene Aktion: Wählen Sie die Anwendungen aus der Liste aus und klicken Sie auf **Auf A+ aktualisieren**.

Nach erfolgreichem Upgrade können Sie die folgende Erfolgsmeldung erhalten:



Nach Abschluss des Upgrades werden die Anwendungsdetails aus der Aufgabe entfernt.

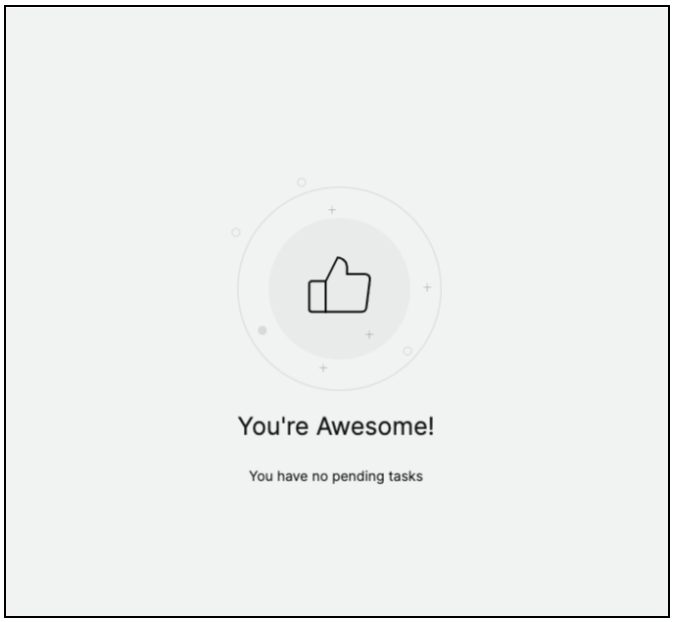
Zu beachtende Punkte:

- Je nach Anzahl der ausgewählten Anwendungen kann die Dauer des Upgrade-Vorgangs variieren.
- Nachdem Sie einen Upgrade-Vorgang gestartet haben, wird empfohlen, einen weiteren Upgrade-Vorgang einzuleiten, nachdem der laufende Upgrade-Vorgang abgeschlossen ist.

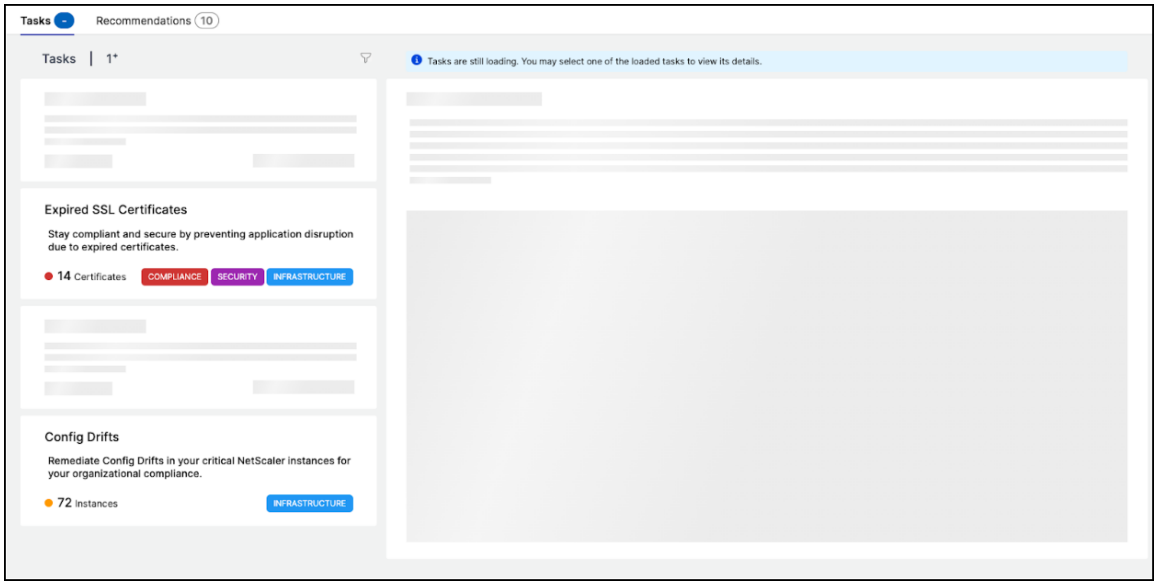
- Sie können den Status des Upgrade-Vorgangs auch unter **Infrastruktur > Konfiguration > Konfigurationsaufträge** einsehen.
- Wenn der Upgrade-Vorgang nicht erfolgreich ist, können Sie den Status unter **Infrastruktur > Konfiguration > Konfigurationsaufträge** einsehen. Sie können den Upgrade-Vorgang erneut von der Aufgabe aus starten.
- Wenn Sie ein Massen-Upgrade durchführen und eine oder mehrere Anwendungen nicht aktualisiert werden können, können Sie in der Aufgabe nur die Details der fehlgeschlagenen Anwendungen anzeigen. Sie können den Upgrade-Vorgang erneut einleiten, um ihn abzuschließen.

Hinweis:

- Sie können die folgende Seite anzeigen, wenn Ihre NetScaler Console 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 Console-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?
Fügen Sie eine NetScaler-Instanz hinzu	Nach dem Onboarding in die NetScaler Console und wenn keine NetScaler-Instanz erkannt wurde.
Fügen Sie einen externen Agenten hinzu, um das Maximum an Funktionen in NetScaler Console 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.

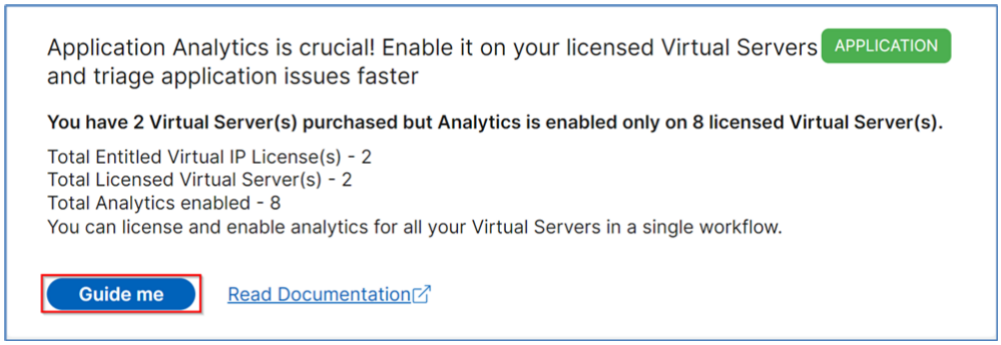
Name der Empfehlung	Wann ist die Aufgabe in der GUI sichtbar?
Registrieren Sie einen NetScaler von einem integrierten Agenten für einen externen Agenten	Nachdem Sie mithilfe des Service Connect-Workflows in NetScaler Console eingebunden sind, werden die NetScaler-Instanzen mithilfe des integrierten Agenten eingebunden. Sie können diese NetScaler-Instanzen bei einem externen Agenten registrieren, um alle Funktionen wie Analysen, gepoolte Lizenzierung usw. nutzen zu können.
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 NetScaler neu zuweisen? Es ist ganz einfach!	Wenn die gepoolten Lizenzen in der NetScaler-GUI zugewiesen werden und diese NetScaler-Instanzen in der NetScaler Console erkannt werden, können Sie die Neuzuweisung mithilfe der NetScaler Console 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 Console noch nicht konfiguriert ist.
Konfigurieren Sie Regeln und verpassen Sie keine kritischen Ereignisse auf Ihren NetScaler-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.

Name der Empfehlung	Wann ist die Aufgabe in der GUI sichtbar?
Sicherheitsempfehlung —Halten Sie Ihre NetScaler-Instanzen mit CVEs und Gegenmaßnahmen auf dem neuesten Stand	Wenn die NetScaler-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 NetScaler-Instanzen an	Wenn die **Config-Job-Task** noch nicht konfiguriert ist.
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 Console 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 Console noch nicht konfiguriert ist.

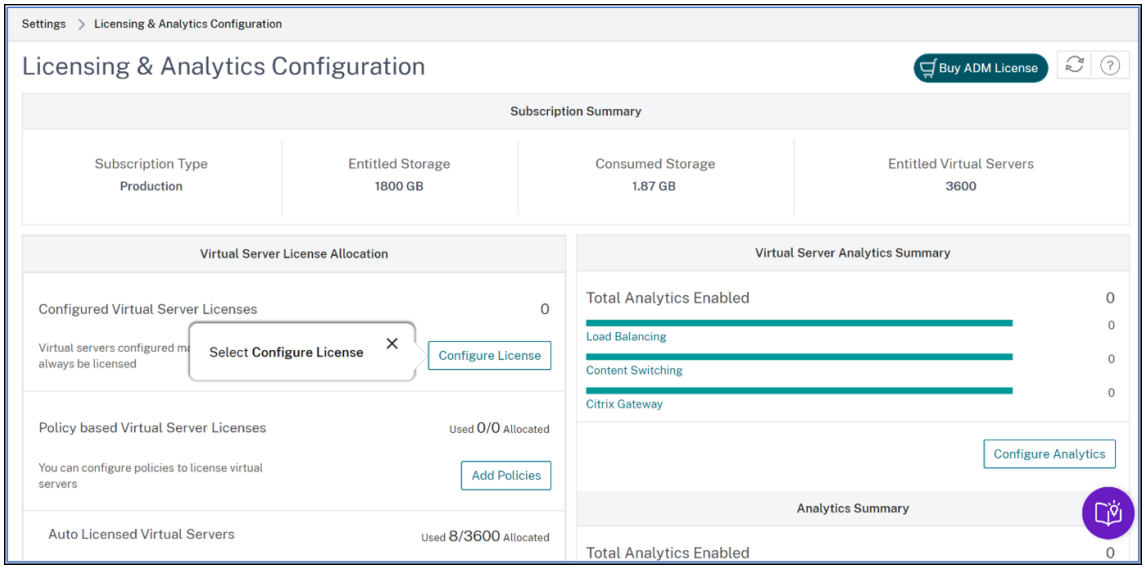
Name der Empfehlung	Wann ist die Aufgabe in der GUI sichtbar?
Automatisieren Sie die Verwaltung von SSL-Zertifikaten mit Venafi und ADM	Wenn der Venafi-Server noch nicht in NetScaler Console konfiguriert ist.
Erneuern Sie Ihre Pool-Lizenz, bevor sie abläuft.	Wenn Ihre bestehende Lizenz in 30 Tagen abläuft.
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.
Ihr aktueller Anspruch auf gepoolte Bandbreite wird nicht ausreichend genutzt. Prüfen und erwägen Sie, mehr zuzuweisen	Wenn Ihre gepoolte Lizenzzuweisung weniger als 70% beträgt.

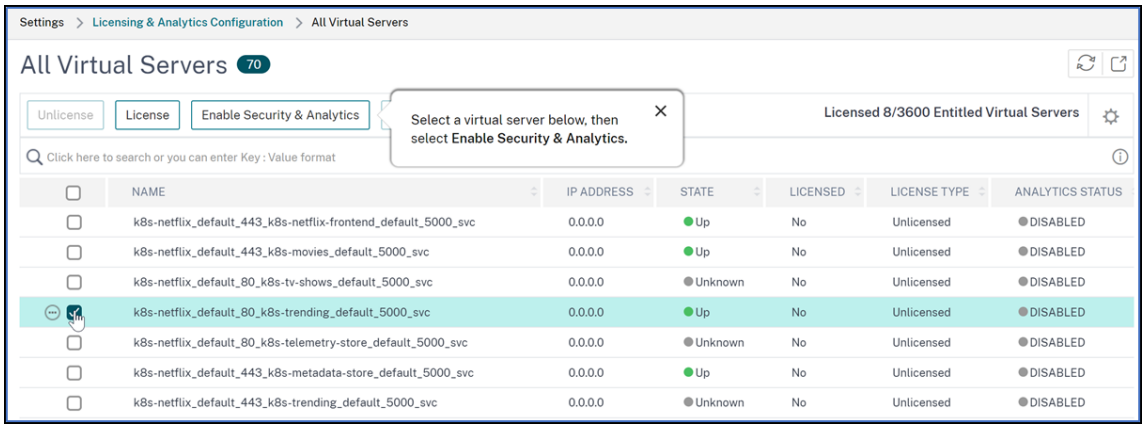
Wie verwende ich den Guide me-Workflow und vervollständige die Empfehlung?

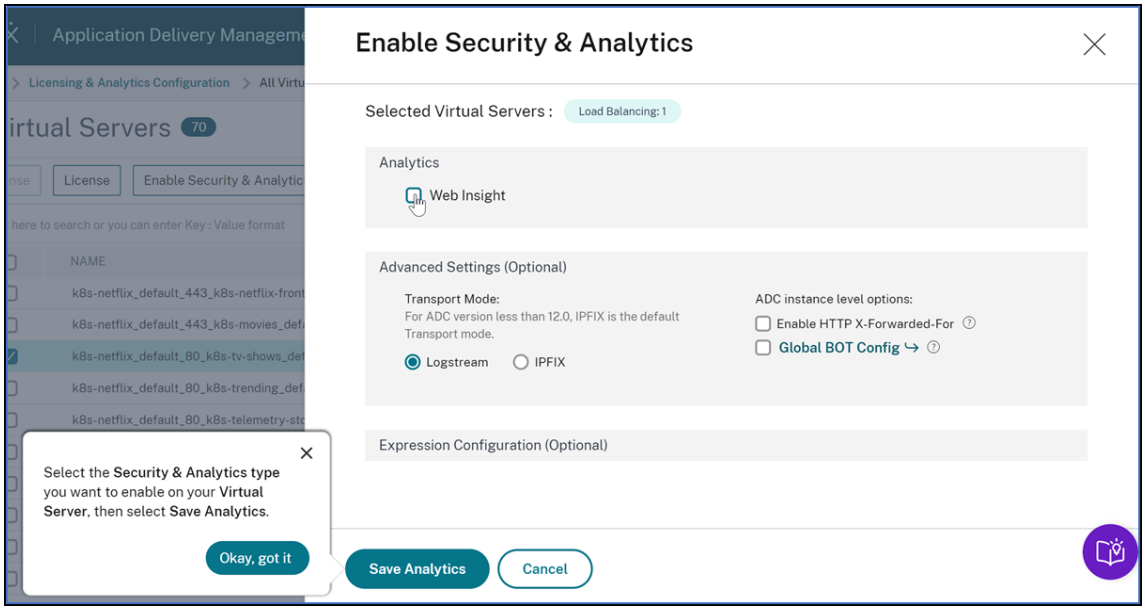
Bedenken Sie, dass Sie Analysen für alle virtuellen Server aktivieren möchten. Klicken Sie für die folgende Aufgabe auf **Guide me**:



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:

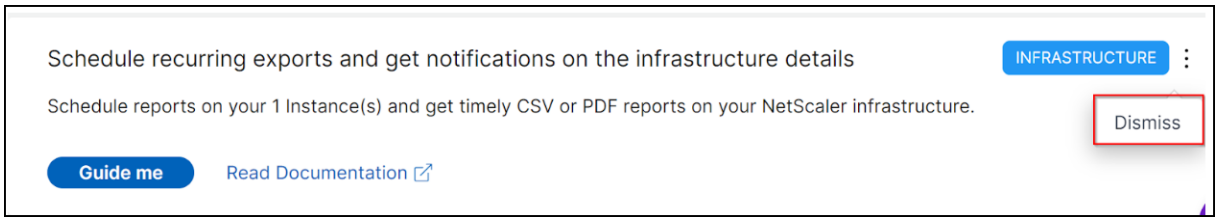
1. 

2. 

3. 

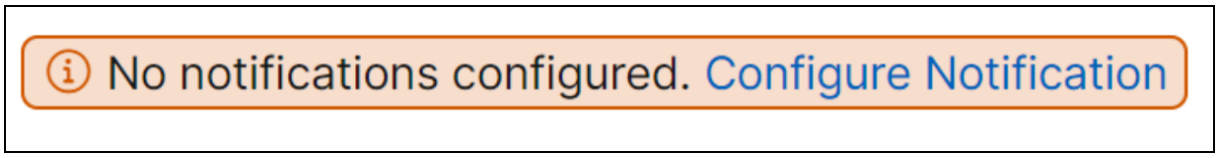
Nachdem Sie den Analysetyp ausgewählt und auf **Analytics speichern** geklickt haben, ist die Empfehlung abgeschlossen und wird in den Status Abgeschlossen verschoben.

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 konfigurieren und Benachrichtigungen erhalten, wenn NetScaler Console offene Aufgaben identifiziert, die Ihre sofortige Aktion erfordern. Wenn Sie keine Benachrichtigungen konfiguriert 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 Console-GUI die konfigurierte Verteilerliste oder das konfigurierte Profil an. Die NetScaler Console sendet Benachrichtigungen an die ausgewählte Verteilerliste oder das ausgewählte Profil.

Häufig gestellte Fragen

1. **Guide Me** zeigt keinen Tooltip und nur die Umleitung der Benutzeroberfläche? Was muss ich tun, um das zu beheben?

   Dieses Problem kann auftreten, wenn Ihre Firewall den Pendo FQDN blockiert. Weitere Informationen finden Sie unter Enable Pendo for your enterprise und stellen Sie sicher, dass der FQDN in der Firewall zugelassen ist. Wenn Sie Pendo FQDN zulassen, kann der **Guide me** Tooltips anzeigen. Sie können den **Guide me** Workflow nur dann von seiner besten Seite erleben, wenn Pendo verfügbar ist.

2. 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 Produktermittlung, und Administratoren können wissen, was eine Aufgabe bewirkt und wie sie helfen kann, ohne dass sie vorher wissen oder wissen müssen, ob die Funktion in NetScaler Console vorhanden ist oder nicht.

3. Was passiert, wenn ich eine Empfehlung ablehne?

   Die Empfehlungen, die Sie ablehnen, werden in den Bereich **Abgewiesen**verschoben. Sie können diese Empfehlungen später vervollständigen.

4. 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.

5. 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.

6. 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.

7. Werden alle umsetzbaren Aufgaben und mehr als 20 Empfehlungen angezeigt, auch wenn ich keine NetScaler-Instanzen in der NetScaler Console hinzugefügt habe?

   Nein. In der NetScaler Console müssen sowohl die NetScaler-Instanz als auch die virtuellen Server verfügbar sein, um alle Aufgaben und Empfehlungen anzeigen zu können.

8. 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

January 26, 2024

In der NetScaler Console können Sie verschiedene Einblicke in die Nutzung und Leistung von Anwendungen, zur NetScaler-Infrastruktur, zu Sicherheitsverletzungen (Bot und WAF) usw. einsehen. Als Administrator müssen Sie möglicherweise zu verschiedenen Optionen in der NetScaler Console-GUI navigieren, um mehrere Einblicke anzuzeigen. Um beispielsweise die virtuellen Server (Anwendungen) und NetScaler-Instanzinformationen zu überprüfen:

- Sie müssen zuerst zu **Anwendungen > Dashboard** navigieren, um Einblicke in Anwendungen anzuzeigen.

- Anschließend müssen Sie zu Infrastruktur > Infrastrukturanalysen navigieren, um Einblicke für NetScaler-Instanzen anzuzeigen.**

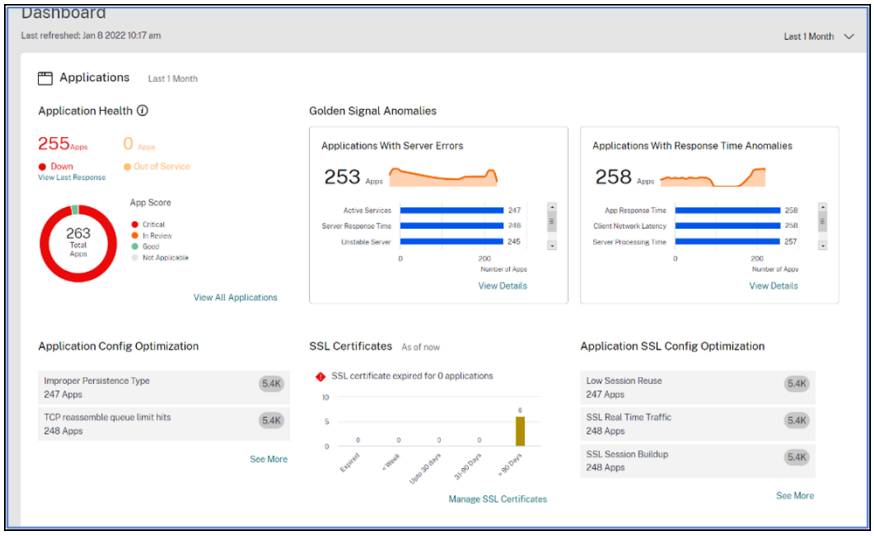
Für eine bessere Überwachungserfahrung ist es erforderlich, dass Sie über ein Privileg verfügen, das einen Überblick über alle erforderlichen Erkenntnisse enthält. Navigieren Sie zu **Übersicht > Dashboard**, um ein Einzelbereichs-Dashboard mit einer Übersicht der wichtigsten Metrikdetails basierend auf den folgenden Kategorien zu visualisieren:

- Anwendungen
- NetScaler-Infrastruktur
- Anwendungssicherheit
- Gateway
- API-Analytik

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.



NetScaler-Infrastruktur

Unter **NetScaler Infrastructure** können Sie die folgenden wichtigen Metriken zur NetScaler-Instanz anzeigen:

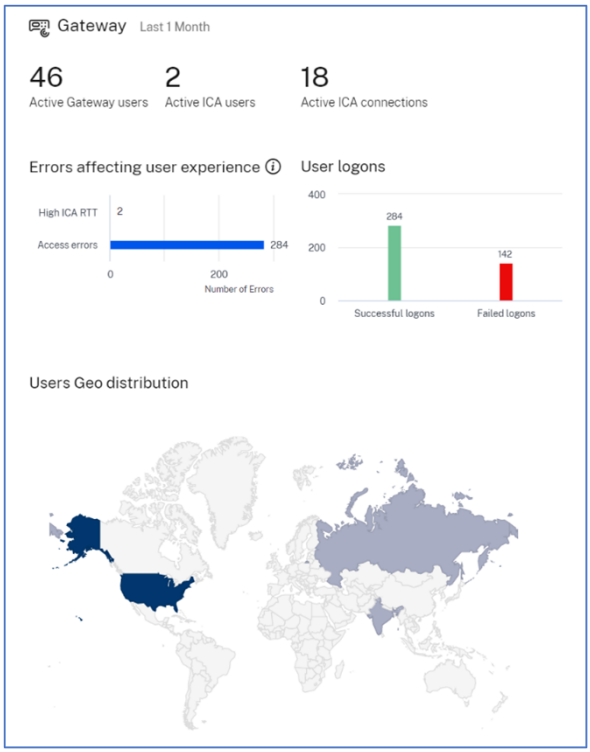
- **NetScaler Instance Health**—Bietet einen Überblick über die Gesamtzahl der NetScaler-Instanzen auf der Grundlage der Instanzbewertung.
- **Von CVEs betroffene NetScaler-Instanzen** —Bietet einen Überblick über die Gesamtzahl der NetScaler-Instances, die von Common Vulnerabilities and Exposures (CVEs) betroffen sind. Weitere Informationen finden Sie unter Sicherheitsempfehlung.
- **Probleme**mit NetScaler-Instanzen —Bietet einen Überblick über NetScaler-Instanzprobleme je nach Problemkategorie. Weitere Informationen finden Sie unter Infrastructure Analytics.
- **Zusammenfassung**des NetScaler-Instanz-Upgrades —Bietet einen Überblick über die Gesamtzahl der NetScaler-Instanzen, die nicht auf dem neuesten Build sind. Klicken Sie auf **NetScaler Instances Dashboard** anzeigen , 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

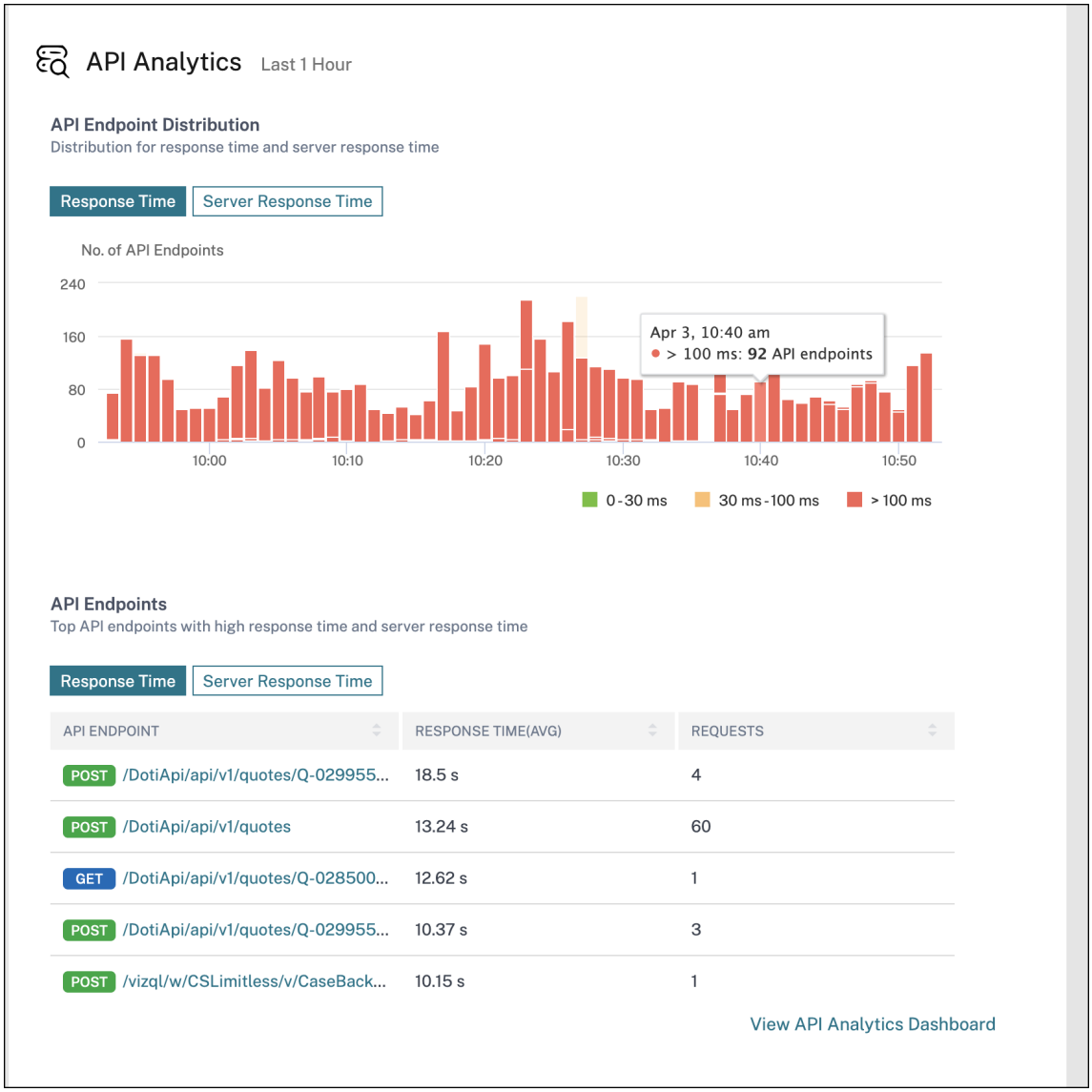
Bietet einen Überblick über die Gesamtzahl aktiver Gateway-Benutzer, die Gesamtzahl der aktiven ICA-Benutzer und die Gesamtzahl der aktiven ICA-Verbindungen. Sie können sich auch Fehler, Benutzeranmeldedetails und eine Geokarte anzeigen lassen, die Details zu den Benutzerstandorten enthält.



API-Analytik

Bietet einen Überblick über die Leistung und Nutzung der API-Endpunkte, die über NetScaler Console konfiguriert wurden. Sie können Folgendes einsehen:

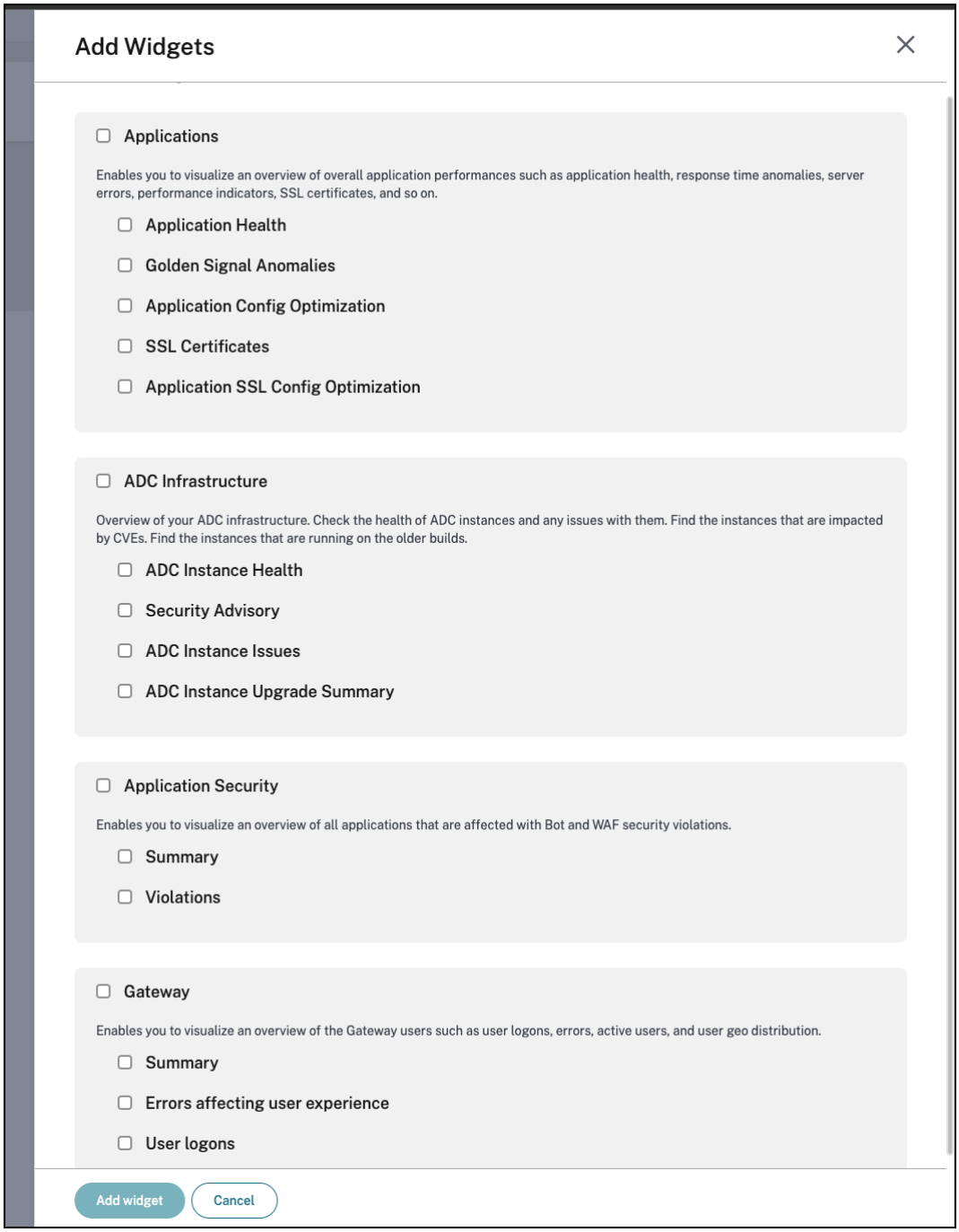
- Verteilung der Anwendungs- und Serverreaktionszeit für API-Endpunkte.
- Endpunkte mit hoher Anwendungs- und Serverreaktionszeit.



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, NetScaler Infrastructure, Gateway oder Application Security).
- 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-

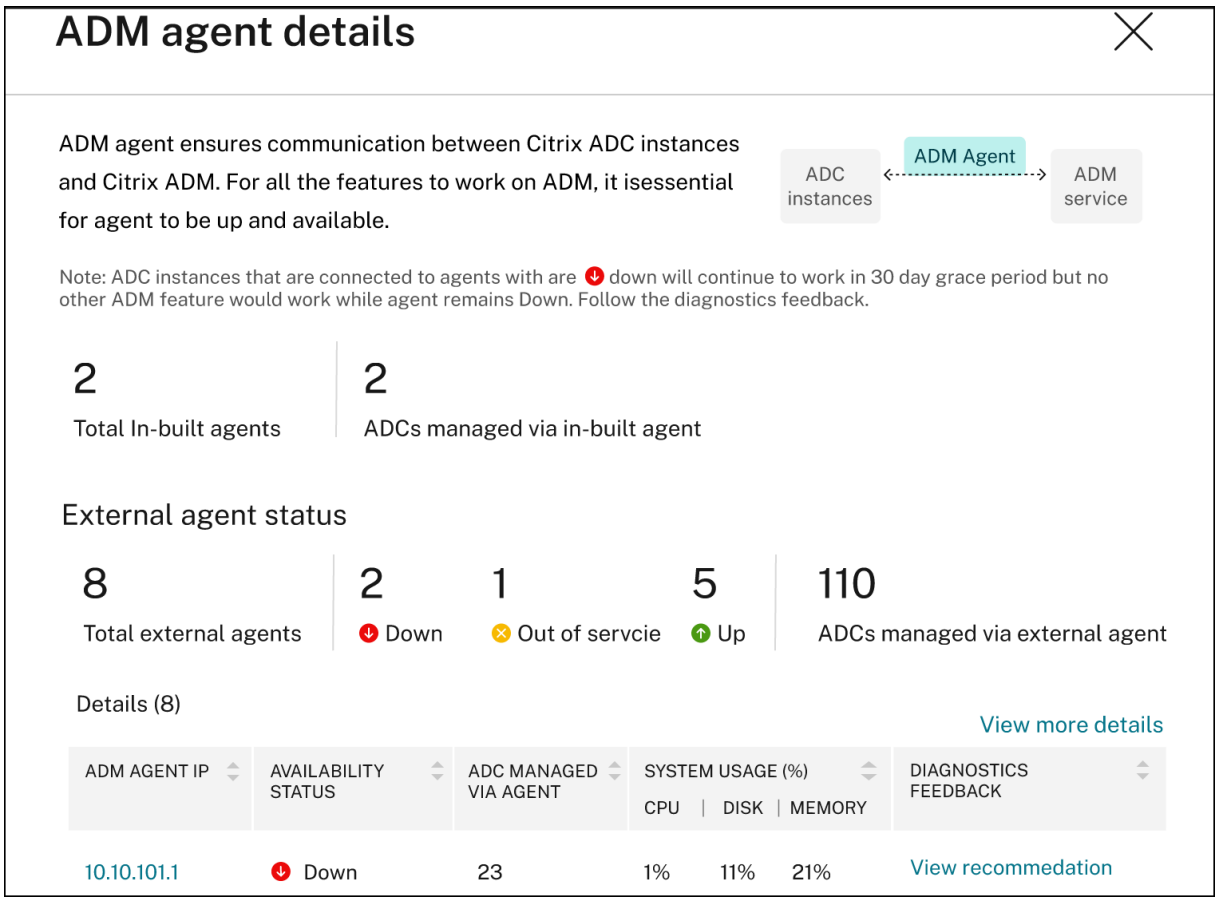
> derungen speichern und erneut die Option Auf **Standard zurücksetzen** verwenden, werden alle Widgets zum Dashboard hinzugefügt.
>
> - Die Option Auf **zuletzt gespeichert zurücksetzen** lädt die zuvor gespeicherte Konfiguration.

Agentdetails anzeigen

Im einheitlichen Dashboard können Sie sich einen Überblick über die Agentendetails verschaffen. ****Unter Übersicht **> Dashboard** können Sie neben dem Agentenstatus den folgenden Status einsehen, mit dem Sie die Gesamtverfügbarkeit der Agenten 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 einen Überblick über Agentendetails wie Gesamtzahl der integrierten Agenten, Gesamtzahl der externen Agenten, Agenten-IP, Status, Systemnutzung, Diagnosetests usw. zu erhalten.



Filter erstellen und anwenden

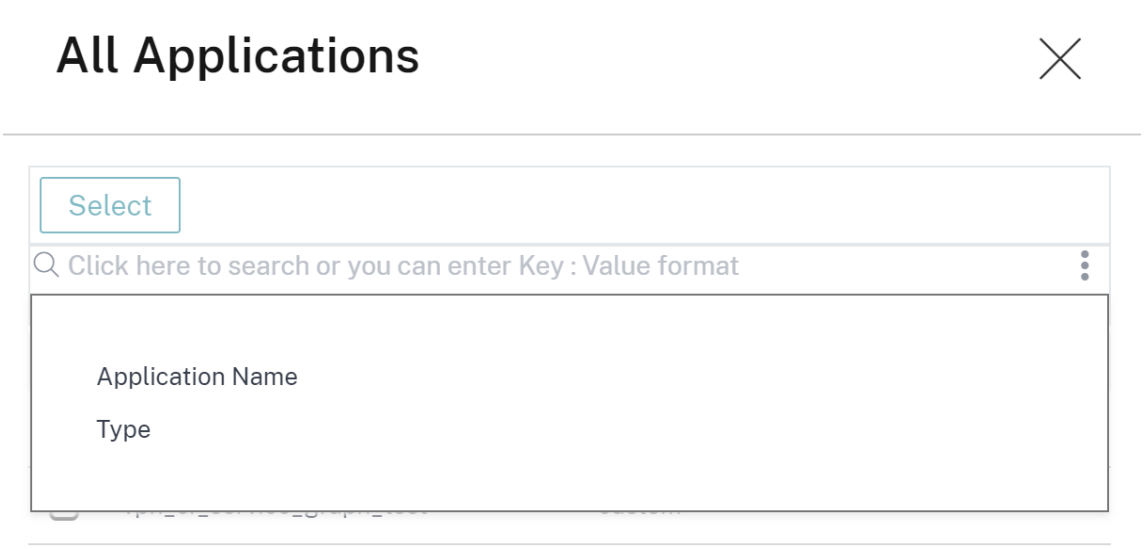
In den folgenden Fällen können Sie Filter anwenden und Erkenntnisse nur für die ausgewählten Instanzen oder Anwendungen anzeigen:

- Anwendungen
- NetScaler-Infrastruktur
- Anwendungssicherheit

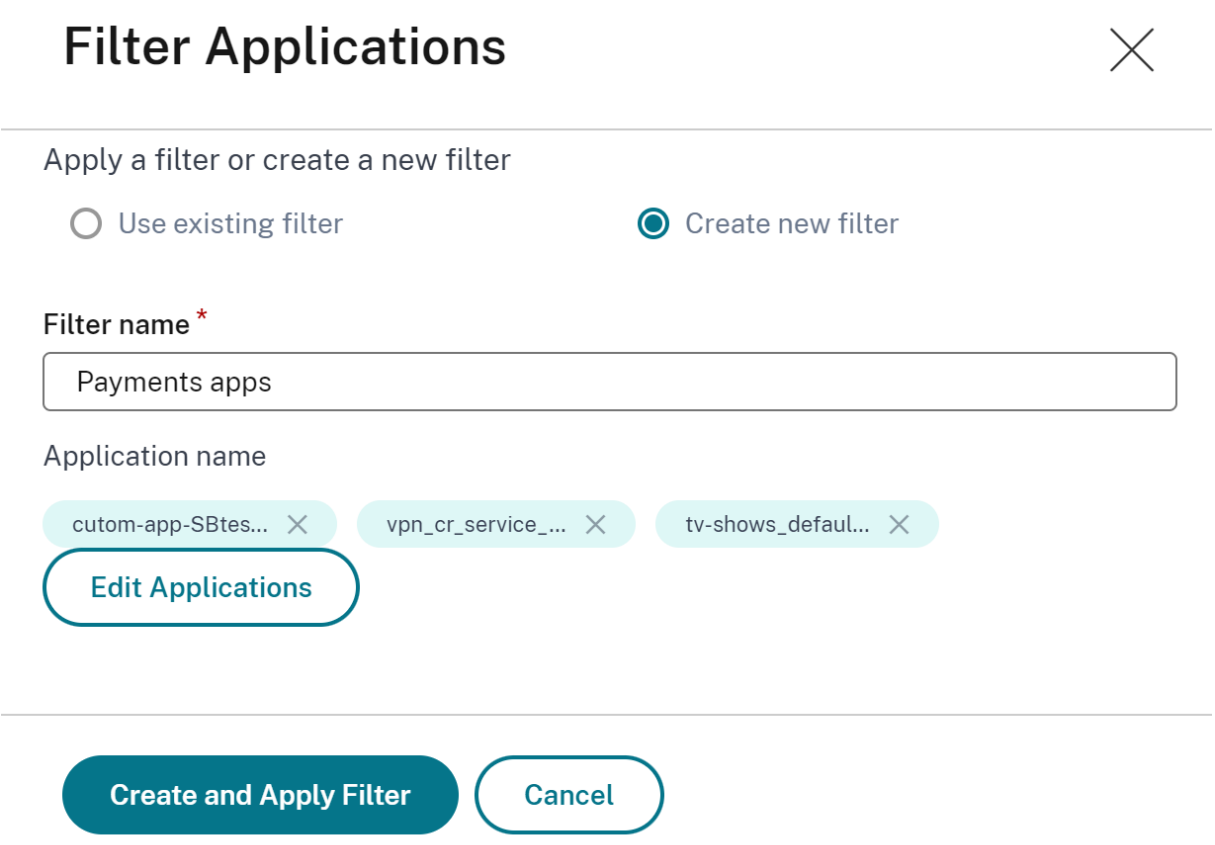
Standardmäßig sind alle Anwendungen ausgewählt. Sie können vom Dashboard aus einen benutzerdefinierten Filter erstellen, indem Sie auf das Filtersymbol in der Kachel klicken.

Im Fenster **Anwendungen filtern**:

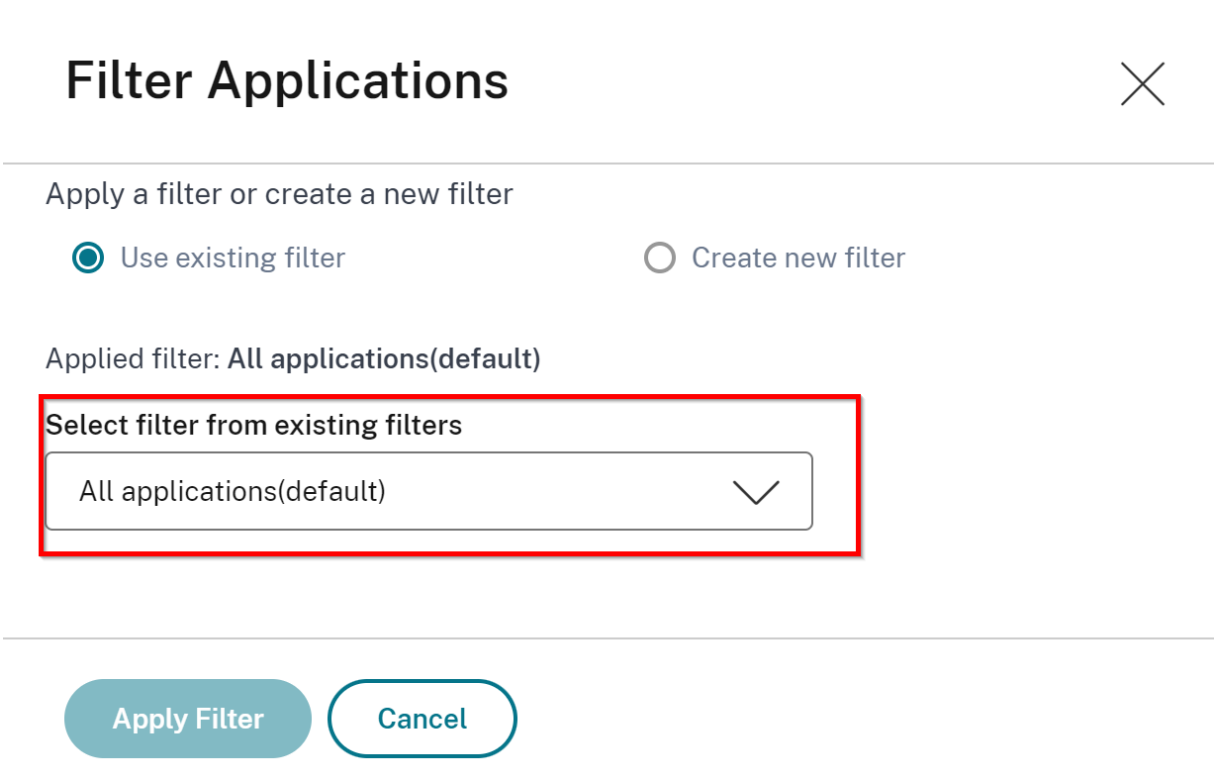
1. Wählen Sie **Neuen Filter erstellen** aus.
2. Geben Sie einen Filternamen ein, der Ihrer Wahl entspricht.
3. Klicken **Sie auf Anwendungen auswählen** und fügen Sie alle erforderlichen Anwendungen für den Filter hinzu. Wenn Sie Anwendungen auswählen, können Sie auch die Filter (**Anwendungsname** und **Typ**) verwenden und dann Anwendungen auswählen.



4. Klicken Sie auf **Filter erstellen und anwenden**.

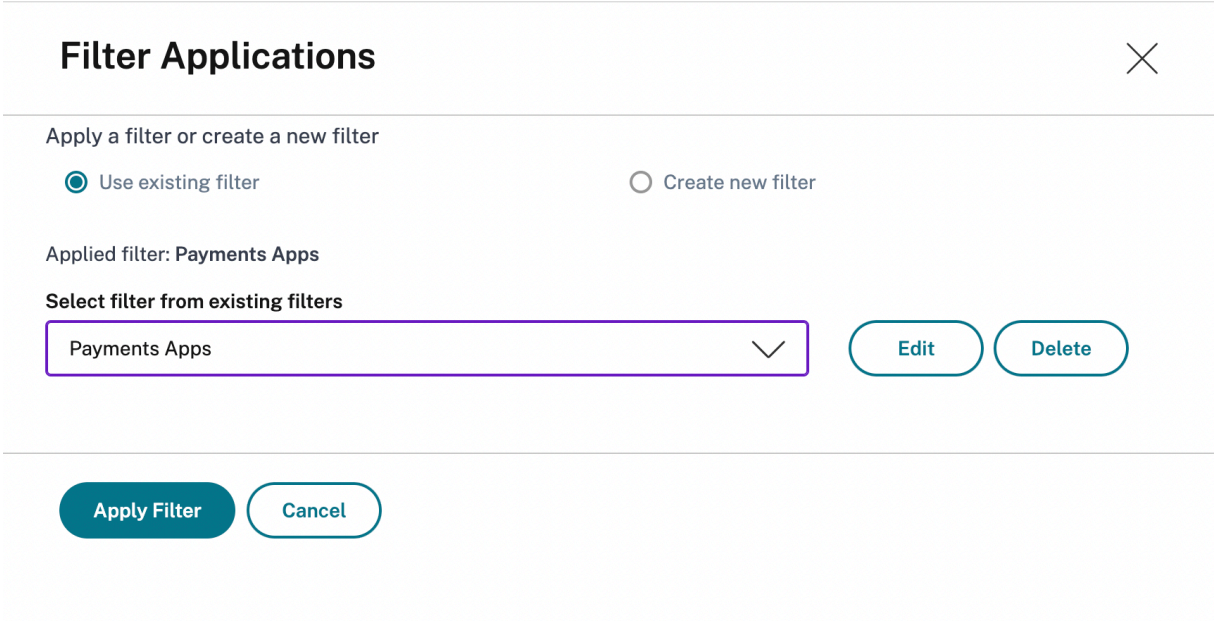


Der Filter ist jetzt erstellt und angewendet. Sie können weitere Filter erstellen, indem Sie dasselbe Verfahren befolgen. Nachdem Sie Filter erstellt haben, können Sie über die Liste **Filter aus vorhandenen Filtern auswählen** und anwenden.



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.

Benutzerdefinierte Dashboards ertellen, um die wichtigsten Kennzahldetails der Instanz anzuzeigen

January 26, 2024

Ähnlich wie beim vereinheitlichten Dashboard (**Übersicht > Dashboard**) können Sie die Metrikdetails Ihrer Instanz nach Ihrer Wahl anzeigen, indem Sie benutzerdefinierte Dashboards erstellen. Sie können bis zu 20 Dashboards erstellen, indem Sie für jedes Dashboard einen eindeutigen Namen verwenden. Als Administrator können Sie mit dieser Erweiterung mehrere Dashboards erstellen und nur die erforderlichen Instanzinformationen überwachen.

Denken Sie zunächst daran, dass Sie die wichtigsten Kennzahlen für **Anwendungen** und **Anwendungssicherheit**überwachen möchten:

1. Navigieren Sie zu **Übersicht > Benutzerdefiniertes Dashboard**.
2. Klicken Sie auf **+**, um ein neues Dashboard zu erstellen.

   Gehen Sie auf der Seite **Benutzerdefiniertes Dashboard erstellen** wie folgt vor:

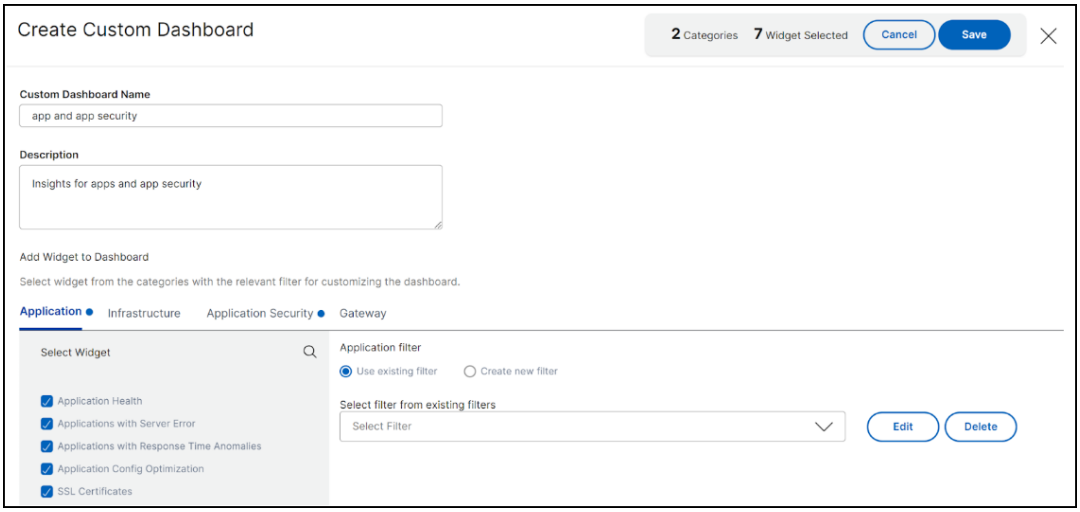
   a) **Benutzerdefinierter Dashboard-Name** —Geben Sie einen eindeutigen Namen für das Dashboard an.

   b) **Beschreibung** —Geben Sie eine kurze Beschreibung ein, um weitere Informationen zu erhalten.

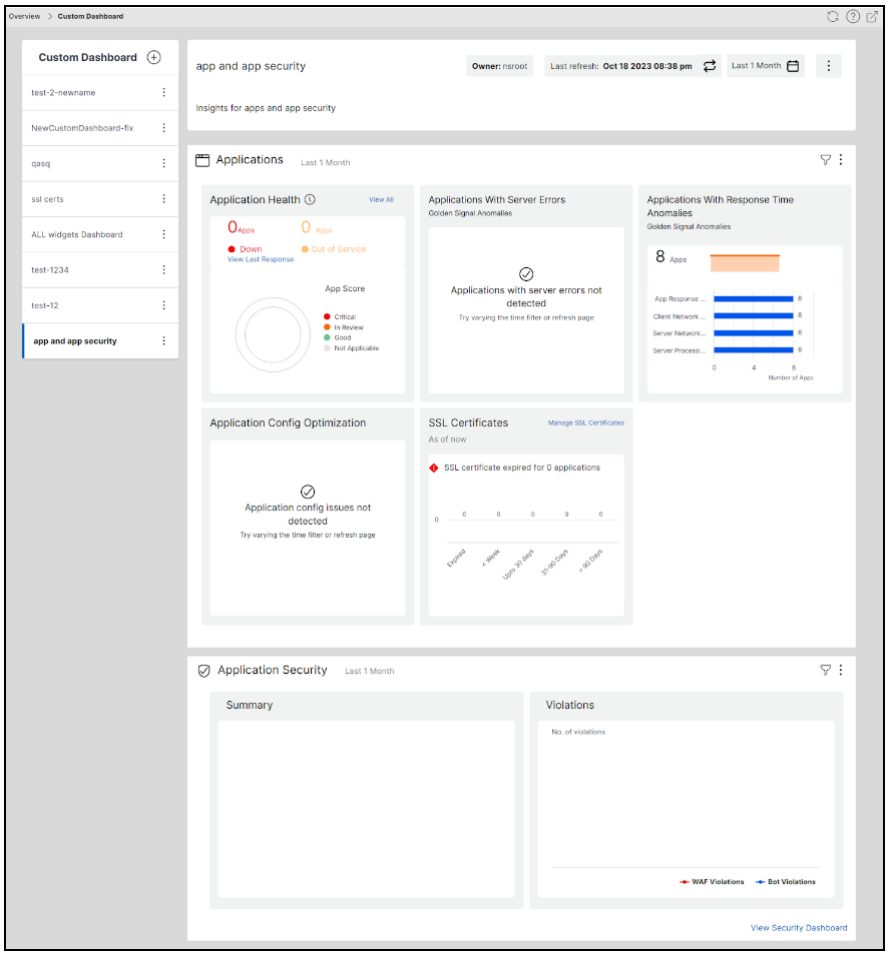
   c) **Widget zum Dashboard hinzufügen** —In diesem Beispiel müssen Widgets für Anwendungen und Anwendungssicherheit hinzugefügt werden. Wählen Sie aus den Kategorien **Anwendung und**Anwendungssicherheit** die Widgets aus, die Sie überwachen möchten.

   d) **Anwendungsfilter** —Standardmäßig wird der Filter auf alle Anwendungen angewendet. Sie können auch einen Filter erstellen und nur bestimmte Anwendungen auswählen. Weitere Informationen finden Sie unter Filter erstellen und anwenden.

   e) Klicken Sie auf **Speichern**.



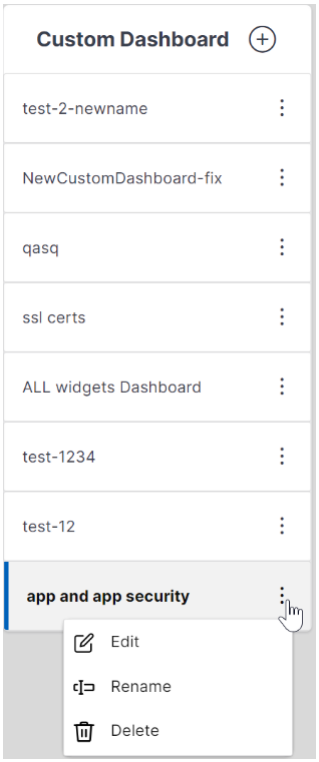
Das Dashboard wurde erfolgreich erstellt. In ähnlicher Weise können Sie bis zu 20 Dashboards erstellen und Kategorien nach Ihrer Wahl auswählen, indem Sie für jedes Dashboard einen eindeutigen Namen angeben.



Sie können die folgenden Optionen verwenden, nachdem Sie ein benutzerdefiniertes Dashboard er-

stellt haben:

- **Bearbeiten**: Sie können das Dashboard bearbeiten, indem Sie weitere Widgets hinzufügen oder entfernen, Filter anwenden usw.
- **Umbenennen**: Sie können den Dashboard-Namen ändern.
- **Löschen**: Sie können das Dashboard löschen.

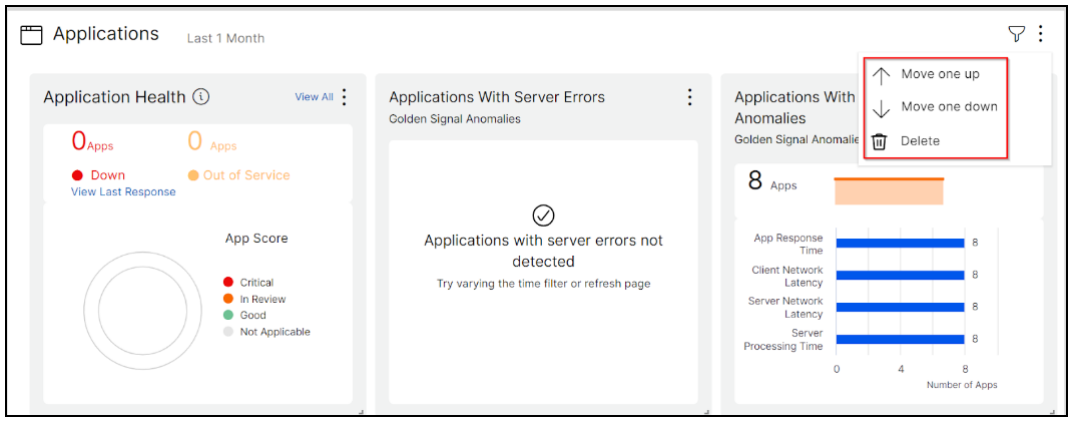


Mehr Optionen im Dashboard

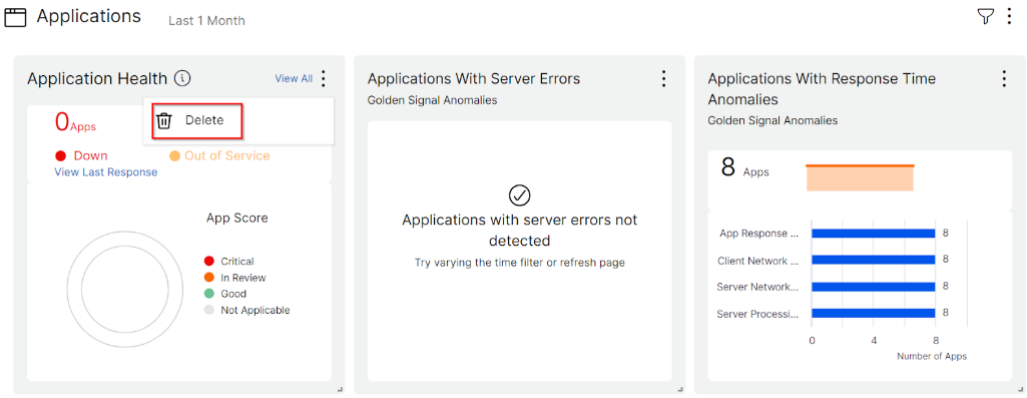
In dem von Ihnen erstellten benutzerdefinierten Dashboard können Sie die folgenden Optionen verwenden:

- **Konfiguration bearbeiten**: Sie können diese Option auch verwenden, um das Dashboard zu bearbeiten, indem Sie weitere Widgets hinzufügen oder Widgets entfernen, Filter anwenden usw.
- **Layout bearbeiten**: Mit dieser Option können Sie das Dashboard zusätzlich anpassen.

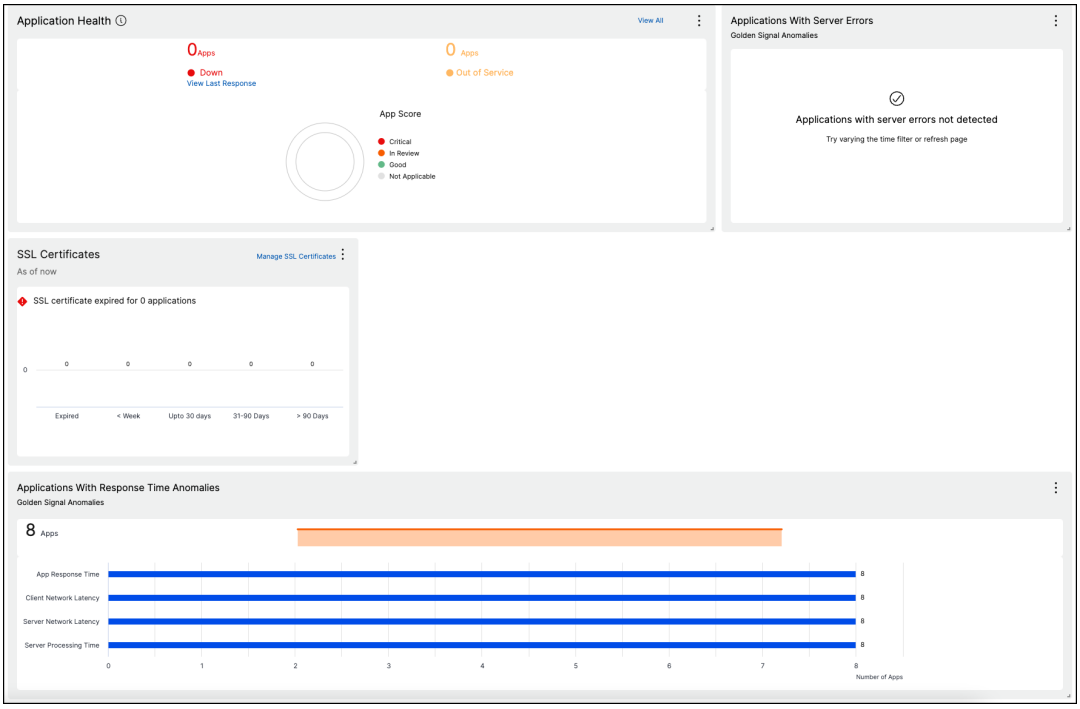
- Sie können wählen, ob Sie nach oben, unten oder löschen möchten.



- In den Widgets können Sie jedes Widget löschen, indem Sie die Option Löschen auswählen.



- Platzieren Sie die Widgets per Drag-and-Drop an einer beliebigen Stelle.
- Erhöhen oder verringern Sie die Größe des Widgets, um bestimmte Erkenntnisse besser sichtbar zu machen.



Nachdem Sie die Änderungen vorgenommen haben, klicken Sie auf **Speichern**, um das aktualisierte Dashboard anzuzeigen.

Dashboard mit anderen Benutzern teilen

Sie können das Dashboard für andere Benutzer freigeben. Wählen Sie ein vorhandenes Dashboard aus und klicken Sie auf **Teilen**. Geben Sie den Benutzernamen ein und klicken Sie auf **Einladen**, um das Dashboard zu teilen. Der zugewiesene Benutzer kann das Dashboard im schreibgeschützten Modus anzeigen.

API-Sicherheit

January 26, 2024

APIs oder Application Programming Interfaces sind Sätze von Regeln, Protokollen und Tools, die es verschiedenen Softwareanwendungen oder Systemen ermöglichen, miteinander zu kommunizieren. APIs spielen eine wichtige Rolle beim Schutz sensibler Daten, indem sie Zugriffskontrollen, Authentifizierung und Verschlüsselung durchsetzen und so sicherstellen, dass nur autorisierte Stellen auf vertrauliche Informationen zugreifen und diese sicher übertragen können.

APIs dienen als Backend-Framework für Mobil- und Webanwendungen. Daher ist es wichtig, die vertraulichen Daten, die sie übertragen, zu schützen. API-Sicherheit bezieht sich auf die Praxis, Angriffe

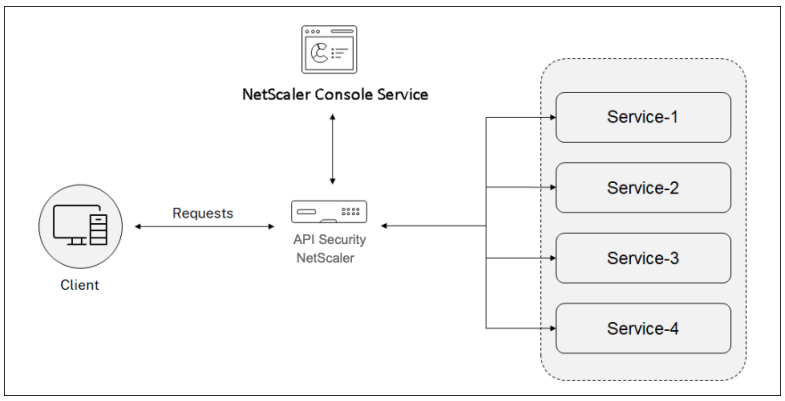
auf APIs zu verhindern oder abzuschwächen.

Bei der API-Sicherheit fungiert ein Gateway als Einstiegspunkt für alle Anfragen an Ihre API-Endpunkte. Und gewährleistet einen sicheren und zuverlässigen Zugriff auf alle API-Endpunkte und Microservices in Ihrem System.

Gehen Sie wie folgt vor, um Ihre APIs zu sichern:

- API-Definition erstellen und hochladen
- Bereitstellen einer API-Instanz
- Richtlinien zu einer API-Bereitstellung hinzufügen

Die folgende Abbildung beschreibt, wie die API-Sicherheit in NetScaler Console die Client-Anfrage empfängt und die Antwort von den Back-End-API-Diensten sendet:



> **Hinweis:**
>
> In NetScaler Console ist diese Funktion für Benutzer mit Premium- oder Advanced-Lizenzen verfügbar.

Vorteile der API-Sicherheit

Die API-Sicherheit bietet Ihnen die folgenden Vorteile:

- Schützt**Ihre API-Endpunkte**: Die API-Sicherheit fügt eine Sicherheitsebene hinzu und schützt Ihre API-Endpunkte und Backend-API-Server vor Angriffen wie:
  - Pufferüberlauf
  - SQL-Einschleusung
  - Cross-Site Scripting
  - Denial-of-Service (Dos)
- **Überwacht und verbessert die API-Leistung**: Die API-Sicherheit bietet Dienste wie SSL-Offloading, Authentifizierung, Autorisierung, Ratenbegrenzung und mehr. Diese Dienste erhöhen die API-Performance und ihre Verfügbarkeit.

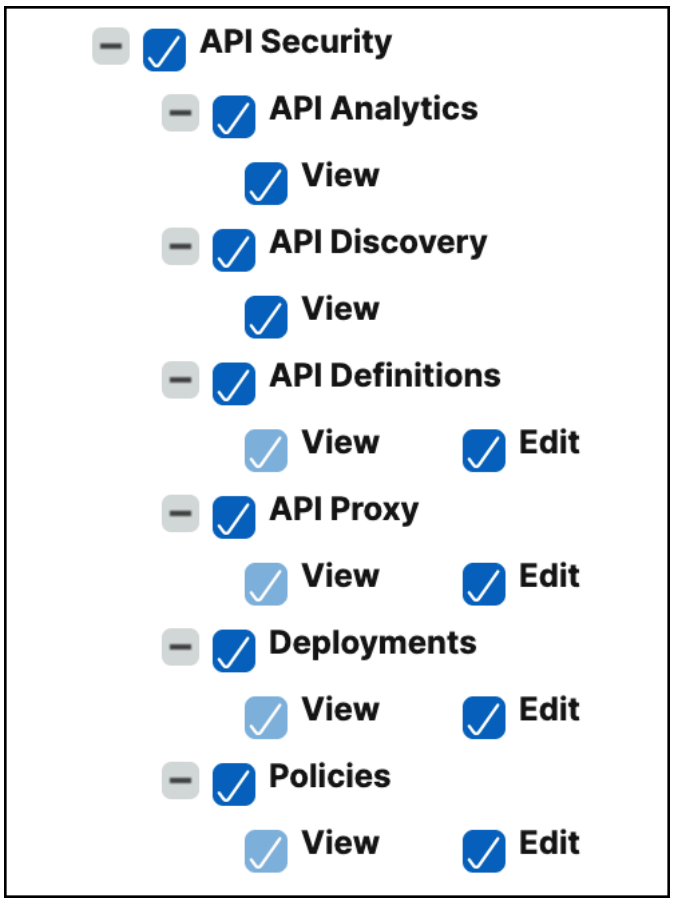
Die API-Analytik bietet Ihnen die Einblicke in Ihre API-Performance-Metriken und Bedrohungen für Ihre API-Endpunkte. Weitere Informationen finden Sie unter Anzeigen von API-Analysen.

- **Verwaltet den API-Verkehr**: Die API-Sicherheit abstrahiert die Komplexität Ihrer Backend-API-Infrastruktur.
- **Erkennt API-Endpunkte**: Die API-Sicherheit erkennt die API-Endpunkte, die sich in Ihrer Organisation befinden, und fügt sie der Seite **API Discovery** hinzu.

API-Sicherheitskonfigurations- und Verwaltungsberechtigungen gewähren

Als Administrator können Sie eine Zugriffsrichtlinie erstellen, um Benutzerberechtigungen für die Konfiguration und Verwaltung der API-Sicherheit zu gewähren. Die Benutzerberechtigungen können Anzeigen, Hinzufügen, Bearbeiten und Löschen sein. Führen Sie Folgendes aus, um Berechtigungen zu erteilen:

1. Navigieren Sie zu **Einstellungen > Benutzer und Rollen > Zugriffsrichtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie unter **Zugriffsrichtlinien erstellen**einen Richtliniennamen und die Beschreibung an.
4. Erweitern Sie im Feld **Berechtigungen** die Optionen **Anwendungen** und dann **API-Sicherheit**.
5. Wählen Sie die erforderlichen **API-Sicherheitsseiten** aus. Wählen Sie dann die Berechtigungen aus, die Sie gewähren möchten.



Wichtig:

Stellen Sie sicher, dass Sie Berechtigungen für die Funktionen gewähren, die für die Verwendung einer API-Sicherheit erforderlich sind. Wenn Sie beispielsweise Benutzern Zugriff auf die Seite "**Bereitstellungen** "gewähren, erfordern die folgenden Funktionen auch Benutzerzugriff:

- StyleBooks
- IPAM
- Load Balancing (unter **Netzwerkfunktionen**)
- Content Switching (unter **Netzwerkfunktionen**)
- Geräte-API-Proxy (unter **API**)

Weitere Informationen zu Zugriffsrichtlinien finden Sie unter Konfigurieren von Zugriffsrichtlinien in der NetScaler Console .

API-Definition erstellen und hochladen

January 26, 2024

Eine API-Definition ist ein Dokument, das eine API beschreibt, die die OpenAPI-Spezifikationsstandards (Swagger 2.0, OpenAPI 3.0.x) verwendet. Diese Definition kann API-Ressourcenpfade und -methoden enthalten, um sie zu bedienen. Sie können API-Definitionen zur NetScaler Console hinzufügen und sie dann auf einem API-Gateway (NetScaler) bereitstellen.

Sie können API-Definitionen auf eine der folgenden Arten erstellen:

- Laden Sie die Swagger OAS-Spezifikationsdatei hoch
- Erstellen Sie Ihre eigene API-Definition

> **Hinweis:**
>
> Derzeit unterstützt NetScaler Console das Parsen von OAS-Spezifikationsdateien, die **Swagger 2.0** oder **openapi 3.0.1** verwenden.

Laden Sie die OAS-Spezifikation hoch

Sie können die OAS-Spezifikation auf die NetScaler Console-GUI hochladen.

1. Navigieren Sie zu **Sicherheit > API-Sicherheit > API-Definitionen**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie **OAS-Spezifikation hochladen**aus.

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass die OAS-Spezifikationsdatei im YAML- oder JSON-Format vorliegt. Und diese Datei darf keine externen Referenzen enthalten. Derzeit unterstützt NetScaler Console Swagger Version 2.0.

4. Durchsuchen Sie eine OAS-Spezifikation von Ihrem lokalen Computer aus und laden Sie sie auf NetScaler Console hoch.

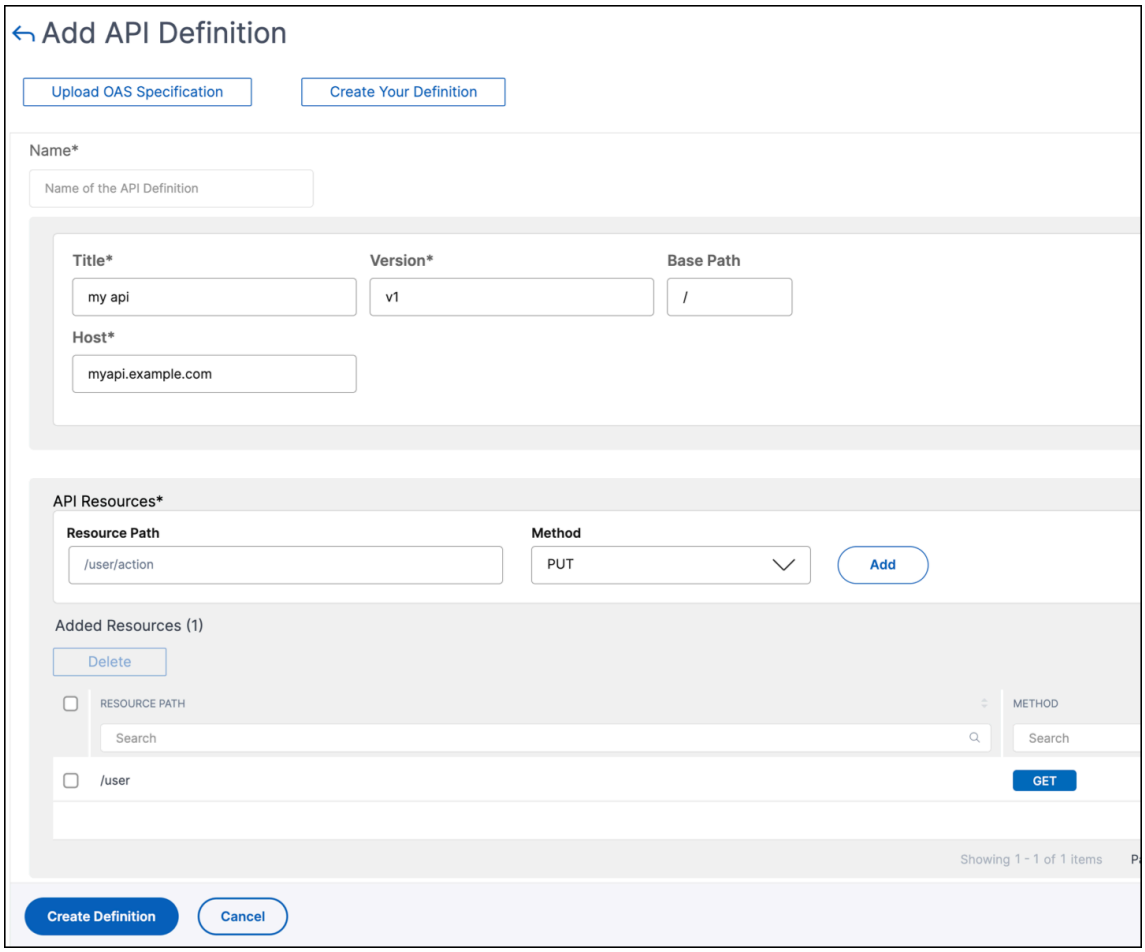
Erstellen einer API-Definition

Sie können Ihre eigene API-Definition in der NetScaler Console-GUI erstellen.

1. Navigieren Sie zu **Sicherheit > API-Sicherheit > API-Definitionen**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie **Create Your Definition** und geben Sie Folgendes an:

   - **Name** - Ein Name für die API-Definition.

- **API-Definition** - Eine Definition muss Titel, Version, Basispfad und Host enthalten. Sie können einen Domänennamen oder eine IP-Adresse im Feld **Host** angeben.
- **API-Ressourcen** - Fügen Sie Ihrer Definition mehrere API-Ressourcen hinzu. Jede Ressource hat einen Pfad und eine unterstützte Methode. Klicken Sie auf **Hinzufügen**. Die Ressource wird der Tabelle **Hinzugefügte Ressourcen hinzugefügt** . Klicken Sie auf **Löschen**, um eine API-Ressource zu löschen.



4. Klicken Sie auf **Erstellen**.

API-Definitionen anzeigen

Auf der Seite “**API-Definitionen** “wird die hochgeladene Definition aufgeführt. Klicken Sie auf **Ansicht**, um die folgenden API-Definitionsdetails anzuzeigen:

- **Name** —Zeigt den Namen einer API-Definition an.
- **API-Definition** —Zeigt Titel, Version, Basispfad und Host einer Definition an.

- **API-Ressourcen** —Listet die API-Ressourcen in einer API-Definition und ihre Methoden zum Betrieb auf.

Bereitstellen einer API-Instanz

January 26, 2024

Um eine API-Instanz bereitzustellen, benötigen Sie einen API-Proxy. Ein API-Proxy ist ein virtueller Front-End-Server, auf dem die API-Sicherheit (NetScaler-Instanz) den API-Verkehr von API-Clients empfängt. Die API-Clients können Browser, mobile Anwendungen usw. sein.

Sie können einen API-Proxy für verschiedene API-Bereitstellungen freigeben. In einer Organisation, in der Sie über viele API-Dienste verfügen, können Sie für jeden API-Dienst einen separaten API-Proxy erstellen. Sie können auch einen API-Proxy erstellen und mit API-Instanzen für verschiedene API-Dienste teilen.

Beispielsweise werden die beiden API-Dienste `app1` und `app2` auf derselben API-Sicherheit bereitgestellt und verwenden denselben virtuellen Front-End-Server. Sie möchten beiden API-Diensten dieselbe virtuelle IP-Adresse und dieselben SSL-Zertifikatsinformationen zur Verfügung stellen. In diesem Fall können Sie einen API-Proxy mit den erforderlichen Informationen hinzufügen und für separate Bereitstellungen freigeben. So können API-Dienste in verschiedenen Bereitstellungen mithilfe des gemeinsam genutzten API-Proxys Anfragen empfangen.

Führen Sie als Administrator die folgenden Schritte aus, um eine API-Instanz bereitzustellen:

1. Einen API-Proxyhinzufügen.
2. Stellen Sie eine API-Instanz mithilfe des API-Proxybereit

Einen API-Proxy hinzufügen

Folgen Sie den Schritten, um einen API-Proxy hinzuzufügen:

1. Gehen Sie zu **Sicherheit > API-Sicherheit > API-Proxy > Hinzufügen**.
2. Geben Sie Folgendes an:
    - **Proxyname** —Ein Name für einen API-Proxy.
    - **NetScaler-Zielinstanz** —Wählen Sie eine NetScaler-Instanz aus, die als API-Gateway fungiert.
    - **IP-Adresse** —Eine IP-Adresse des virtuellen Servers, der API-Dienste hostet.
    - **Port** —Eine Portnummer des virtuellen Servers, der API-Dienste hostet.

- **Protokoll** —Legen Sie ein Protokoll fest, das von der Art des Datenverkehrs abhängt, den Sie auf dem API-Proxy empfangen möchten (HTTP oder HTTPS).
- **TLS-Sicherheitsprofil** —Wählen Sie Hoch oder Mittel aus der Liste aus. Wenn Sie Hoch auswählen, wird es dem SSL-Profil mit A+-Rating auf einer NetScaler-Instanz zugeordnet.
- **Zertifikatsspeicher** —Wählen Sie das SSL-Zertifikat für die API-Sicherheit aus. Der NetScaler Agent-Zertifikatsspeicher hilft Ihnen, Ihre SSL-Zertifikate an einem Ort zu speichern und zu verwalten.

  Im NetScaler Agent-Zertifikatsspeicher können Sie SSL-Zertifikate im NetScaler Agent speichern und sie während der NetScaler-Konfiguration wiederverwenden.

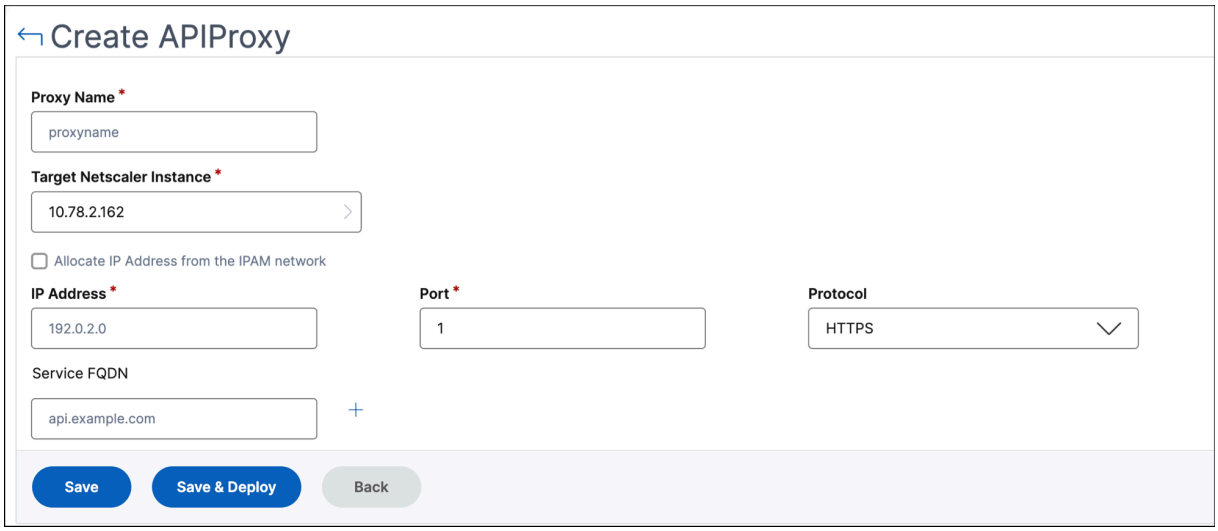
  > **Hinweis:**
  >
  > Wenn Ihre vorhandenen Bereitstellungen das SSL-Zertifikat oder den SSL-Schlüssel verwenden, die sich nicht im NetScaler Agent-Zertifikatsspeicher befinden, müssen Sie das Zertifikat und den Schlüssel dem Speicher mit demselben Namen hinzufügen.

- **Dienst-FQDN** —Ein vollqualifizierter Domänenname, in dem Ihre API-Services gehostet werden. Beispiel: `api.example.com`

Alternativ können Sie ein IPAM-Netzwerk auswählen, um die IP-Adresse zuzuweisen. Um die zugewiesene IP-Adresse aus dem IPAM-Netzwerk anzuzeigen, navigieren Sie zu **Einstellungen > IPAM**. Weitere Informationen zu IPAM finden Sie unter IPAM konfigurieren.

3. Klicken Sie auf **Speichern**, um die Bereitstellungskonfiguration zu speichern.

   Wenn Sie diesen API-Proxy auf der API-Sicherheit bereitstellen möchten, klicken Sie auf **Speichern und bereitstellen**.



Stellen Sie nach dem Hinzufügen eines API-Proxy eine API-Instanz bereit.

Bereitstellen einer API-Instanz mit dem API-Proxy

Führen Sie die Schritte aus, um eine API-Instanz bereitzustellen:

1. Navigieren Sie zu **Sicherheit > API-Sicherheit > Bereitstellungen**.
2. Klicken Sie auf **Hinzufügen**.
3. In den **Basisinformationen zur Bereitstellung** :
   a) Geben Sie den **Namen der Bereitstellung**an.
   b) Wählen Sie unter **API-Definitionen**die erforderliche API-Definition aus.
   c) Wählen Sie den **API-Proxy** aus, den Sie mit dieser Bereitstellung verwenden möchten.
4. Klicken Sie in **Upstream Services**auf **Hinzufügen**, um Back-End-API-Server (Ursprungsserver) hinzuzufügen, auf denen Sie den API-Datenverkehr ausleiten möchten. Sie können einen Upstream-Dienst mit seinem Domänennamen oder seiner IP-Adresse konfigurieren.

   Sie können SNIP-Adresse und Netzwerkmaskendetails angeben, während Sie eine API-Instanz bereitstellen. Die NetScaler-Instanz verwendet die angegebene SNIP-Adresse, um mit den Upstream-Diensten (Backend) zu kommunizieren. Die angegebene SNIP-Adresse wird zur Quell-IP-Adresse für den ausgehenden Datenverkehr, der an Upstream-Dienste gesendet wird. Sie können IPAM auch verwenden, um die SNIP-Adresse und Netzwerkmaske zu konfigurieren. Wenn Sie die SNIP-Adresse nicht konfigurieren, wird die Standard-SNIP-Adresse der NetScaler-Instanz zur Quell-IP-Adresse für die Upstream-Dienste.

   > **Hinweis:**
   >
   > Standardmäßig sind die Optionen SNIP-Adresse und Netzmaske optional. Wenn Sie jedoch eine dieser Optionen angeben, müssen Sie auch eine andere Option angeben.

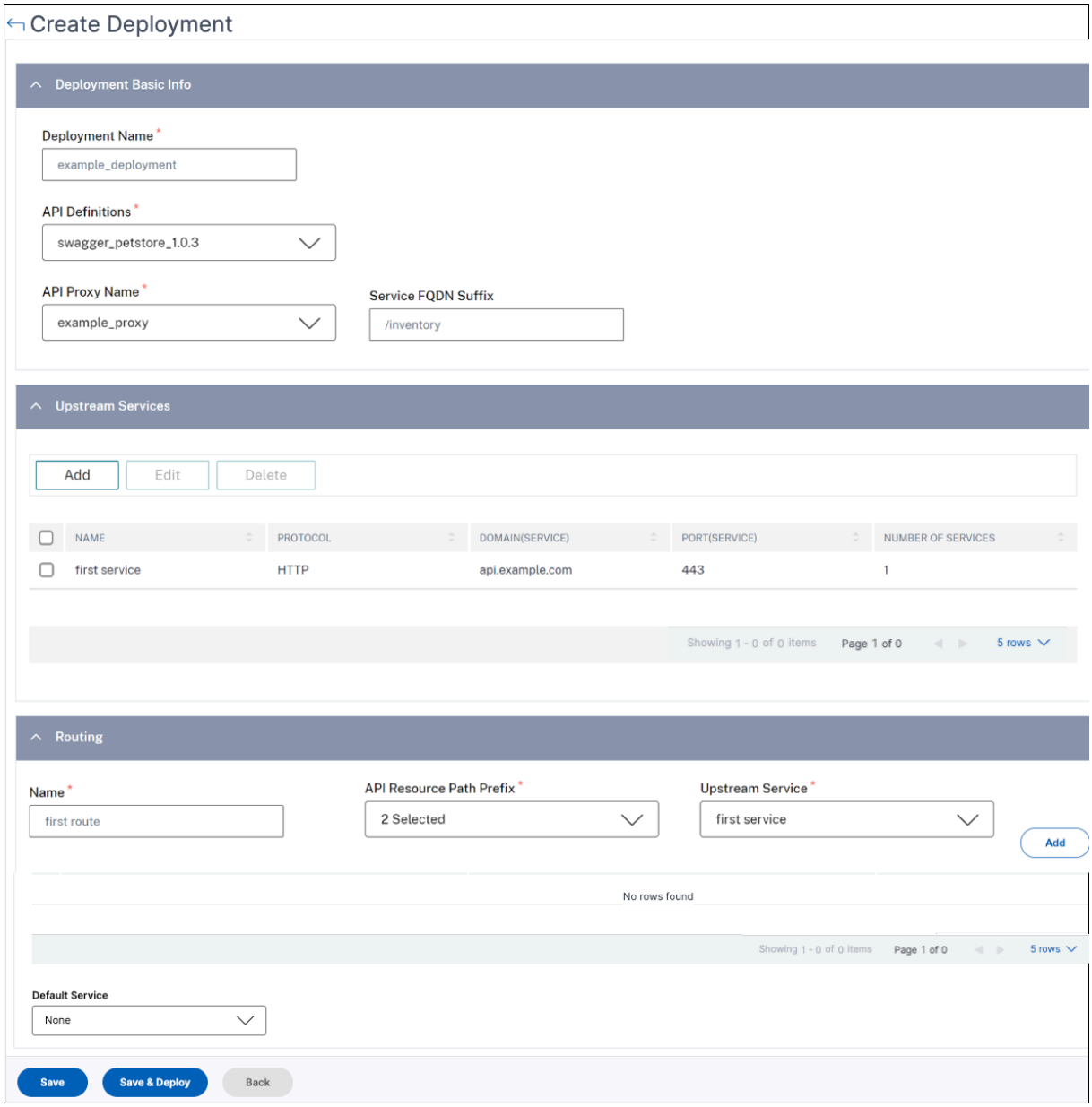
   a) Geben Sie einen Namen für einen Upstream-Dienst an.
   b) Geben Sie die Domäne an.
   c) Geben Sie unter **Dienste**eine IP-Adresse und einen Portwert an. Um weitere IP-Adressen hinzuzufügen, klicken Sie auf **Neue Zeile hinzufügen**.
   d) Klicken Sie auf **Hinzufügen**.
5. Geben Sie unter **Routing**die folgenden Details an, um eingehenden API-Datenverkehr basierend auf dem Ressourcenpfadpräfix weiterzuleiten:
   a) Geben Sie den Routennamen an.
   b) Wählen Sie eine **API-Ressource**, um eine API-Anfrage zu erhalten.

> **Hinweis:**
>
> Sie können auch den benutzerdefinierten Pfad oder das Pfadpräfix angeben.

c) Wählen Sie einen **Upstream-Dienst** aus der Liste aus, in den Sie den API-Datenverkehr übertragen möchten.

6. Klicken Sie auf **Speichern**, um die Bereitstellungskonfiguration zu speichern.

   Wenn Sie die Konfiguration für die API-Sicherheit bereitstellen möchten, klicken Sie auf **Speichern und bereitstellen**.



Aktivieren der API-Analytik

Im Folgenden sind die Voraussetzungen aufgeführt, um Analysen für eine Bereitstellung zu ermöglichen:

- Sicherstellen, dass virtuelle Server **lizenziert** sind
- Stellen Sie sicher, dass Analysestatus **Deaktiviert**
- Stellen Sie sicher, dass virtuelle Server im Status **UP** sind

Um die API-Analyse für eine Bereitstellung zu aktivieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie **unter Sicherheit > API-Sicherheit > Bereitstellungen**die Bereitstellung aus, für die Sie die API-Analyse aktivieren möchten.
2. Klicken Sie auf **Analytics aktivieren**.
3. Wählen Sie auf der Seite **Configure Analytics for deployment** den virtuellen Server aus und klicken Sie auf **Analytics aktivieren**.
4. Gehen Sie im Fenster **Enable Analytics** wie folgt vor:
    a) Wählen Sie den Einsichtstyp aus (Web Insight, Security Insight, Bot Insight)
    b) Wählen Sie **Logstream** oder **IPFIX** als Transportmodus aus.

    Weitere Informationen zu IPFIX und Logstream finden Sie unter Logstream-Übersicht .

    Der Ausdruck ist standardmäßig “true”.
    c) Klicken Sie auf **OK**.

NetScaler Console ermöglicht Analysen auf den ausgewählten virtuellen Servern.

Richtlinien zu einer API-Bereitstellung hinzufügen

January 26, 2024

Sie können verschiedene Sicherheitsrichtlinien für Ihren API-Verkehr konfigurieren. Bei dieser Konfiguration müssen Sie die Auswahlkriterien für den Datenverkehr und die für eine Richtlinie erforderlichen Parameter angeben. Führen Sie die folgenden Schritte aus, um einer API-Definition eine Richtlinie hinzuzufügen:

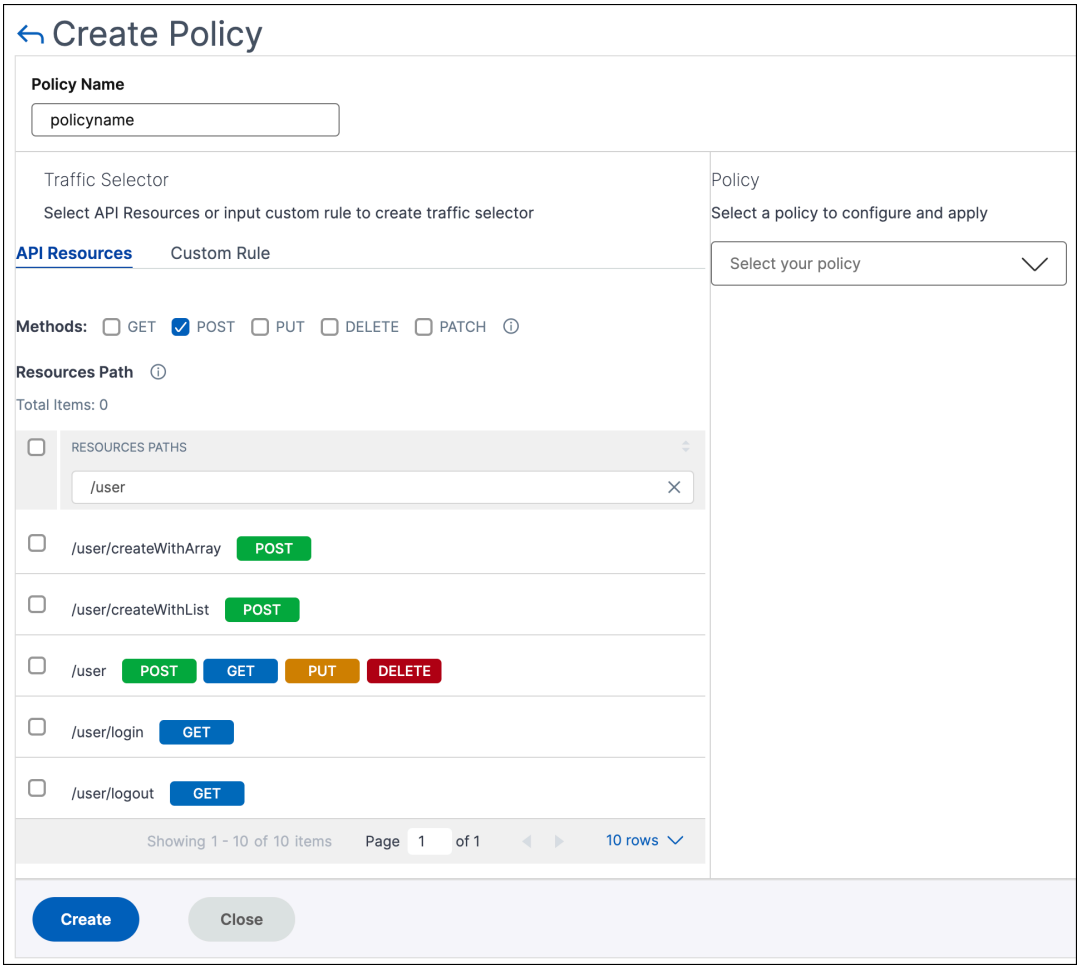
1. Navigieren Sie zu **Sicherheit > API-Sicherheit > Richtlinien**.
2. Klicken Sie auf **Hinzufügen**.

3. Geben Sie den Namen für eine Richtliniengruppe an.
4. Wählen Sie eine **Bereitstellung** aus der Liste aus.
5. Wählen Sie einen **Upstream-Dienst** aus der Liste aus, für den Sie Richtlinien konfigurieren möchten.
6. Klicken Sie auf **Hinzufügen**, um Datenverkehrsmarkierer und einen Richtlinientyp auszuwählen.

   Traffic-Selektor - Die Kriterien zur Auswahl des Datenverkehrs umfassen API-Ressourcenpfade oder Pfadpräfixe, Methoden und Richtlinien.

   Sie können eine der folgenden Optionen verwenden, um Kriterien für die Verkehrsauswahl festzulegen:

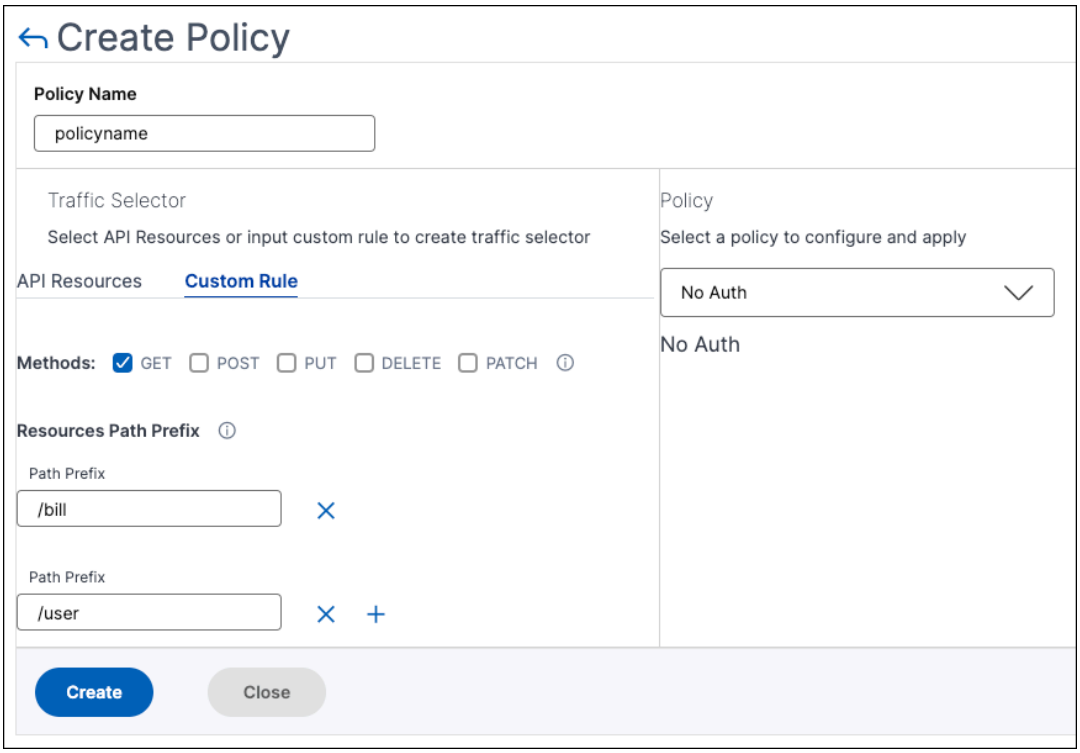
   - **API-Ressourcen** —Wählen Sie eine API-Ressource und ihre Methoden aus, für die Sie eine Richtlinie anwenden möchten. Sie können API-Ressourcen und -Methoden mit einem Schlüsselwort durchsuchen.



   In diesem Beispiel werden die API-Ressourcen mit `/user` der `POST` Methode aufgelistet.

- **Benutzerdefinierte Regel** —Auf dieser Registerkarte können Sie benutzerdefinierte Pfadpräfixe und mehrere Methoden angeben.

  Die konfigurierte Richtlinie gilt für eine eingehende API-Anforderung, die der benutzerdefinierten Regel für die Auswahl des API-Datenverkehrs entspricht.



  In diesem Beispiel gilt die **No-Auth-Richtlinie** für die API-Ressourcen, die das Präfix `/bill` und die Methode `GET` haben.

Wählen Sie unter **Richtlinie**eine Richtlinie aus der Liste aus, die Sie auf die ausgewählte API-Ressource und -Methode anwenden möchten. Weitere Informationen zu den einzelnen Richtlinien finden Sie unter Richtlinientypen.

7. Optional können Sie Richtlinientypen verschieben, um eine Priorität festzulegen. Die Richtlinientypen mit höherer Priorität gelten zuerst.
8. Klicken Sie auf **Speichern**, um eine Richtlinie hinzuzufügen. Wenn Sie die Richtlinie sofort anwenden möchten, klicken Sie auf **Speichern und Anwenden**.

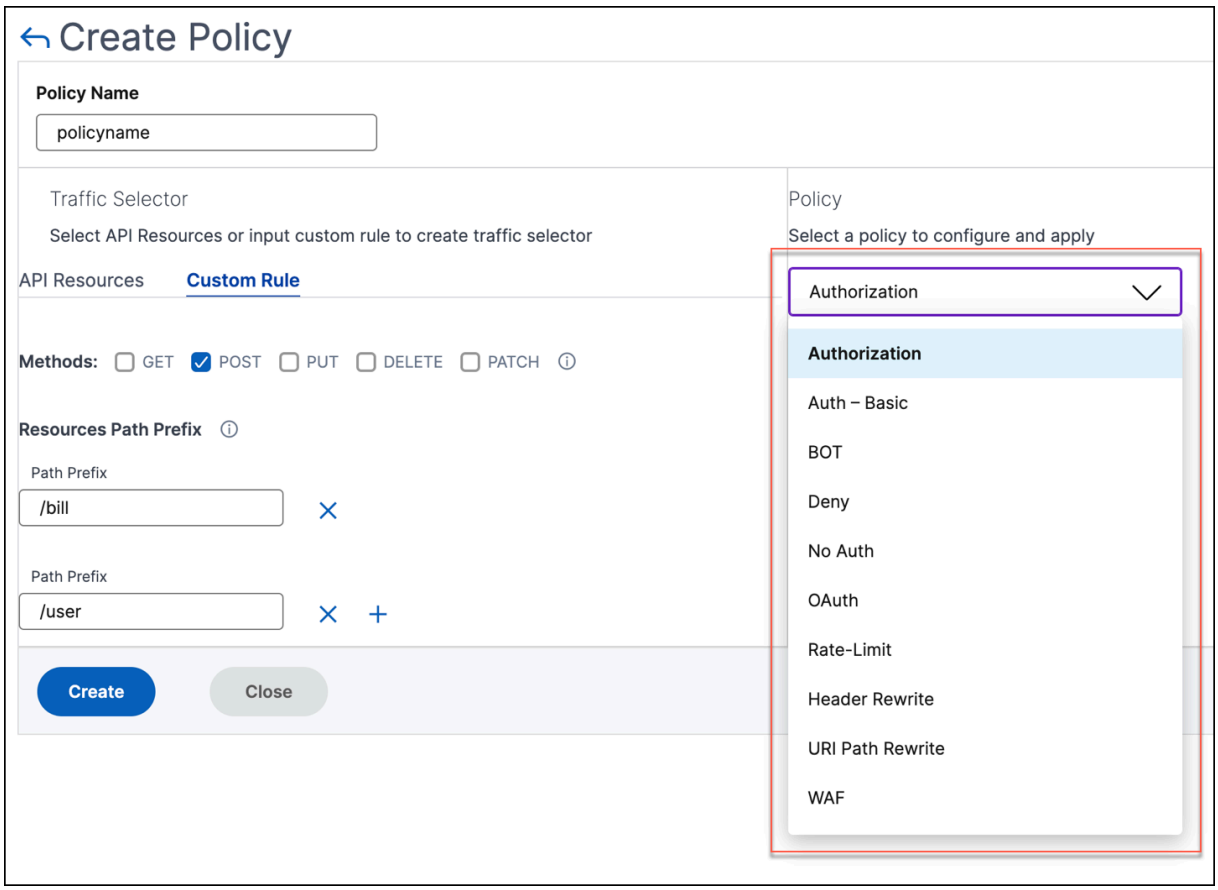
Arten von Richtlinien

Wenn Sie eine API-Richtlinie konfigurieren, können Sie die folgenden Richtlinien auswählen, die Sie auf die API-Ressource und -Methode anwenden möchten:

- **Authentifizierung und Autorisierung**

- **Ratenlimit**
- **WAF**
- **BOT**
- **Header Rewrite**
- **URI Path Rewrite**
- **Verweigern**

> **Hinweis:**
>
> Informationen zur Verwaltung der API-Sicherheit mithilfe von APIs finden Sie unter APIs zum Verwalten der API-Sicherheit verwenden.



Authentifizierung und Autorisierung

API-Ressourcen werden auf einer Anwendung oder einem API-Server gehostet. Wenn Sie Zugriffsbeschränkungen für solche API-Ressourcen durchsetzen möchten, können Sie die Authentifizierungs-

und Autorisierungsrichtlinien verwenden. Diese Richtlinien überprüfen, ob die eingehende API-Anfrage über die erforderliche Berechtigung für den Zugriff auf die Ressource verfügt.

Verwenden Sie die folgenden Richtlinien, um die Authentifizierung und Autorisierung für die ausgewählten API-Ressourcen zu definieren:

`No-Auth` Verwenden Sie diese Richtlinie, um die Authentifizierung für den ausgewählten Datenverkehr zu überspringen.

`Auth-Basic` Diese Richtlinie legt fest, dass die lokale Authentifizierung mit dem HTTP-Standardauthentifizierungsschema verwendet wird. Um die lokale Authentifizierung zu verwenden, müssen Sie Benutzerkonten auf dem NetScaler erstellen.

`OAuth` OAuth erfordert, dass ein externer Identitätsanbieter einen Client mit OAuth2 authentifiziert und ein Zugriffstoken ausgibt. Wenn der Client dieses Token als Zugriffs-Berechtigung für ein API-Gateway bereitstellt, wird das Token basierend auf den konfigurierten Werten validiert.

- **JWKS URI** - Die URL eines Endpunkts mit JWKs (JSON Web Key) für JWT (JSON Web Token) Verifizierung
- **Issuer** —Die Identität (normalerweise eine URL) des Authentifizierungsservers.
- **Zielgruppe** : Die Identität des Dienstes oder der Anwendung, für die das Token anwendbar ist.
- **Ansprüche auf Speichern** - Die Zugriffsberechtigungen werden als eine Reihe von Ansprüchen und erwarteten Werten dargestellt. Geben Sie die Anspruchswerte im CSV-Format an.
- **Introspect URI** - Eine Introspektions-Endpunkt-URL des Authentifizierungsservers. Diese URL wird verwendet, um undurchsichtige Zugriffstoken zu überprüfen. Weitere Informationen zu diesen Token finden Sie unter OAuth-Konfiguration für undurchsichtige Zugriffstoken.

  Nachdem Sie **Introspect-URI**angegeben haben, geben Sie die **Client-ID** und den **Client Secret** für den Zugriff auf den Authentifizierungsserver an.
- **Zulässige Algorithmen** - Mit dieser Option können Sie bestimmte Algorithmen in den eingehenden Token einschränken. Standardmäßig sind alle unterstützten Methoden zulässig. Sie können jedoch die erforderlichen Algorithmen für den ausgewählten Datenverkehr überprüfen.

Nach erfolgreicher Validierung gewährt API Security dem Client Zugriff.

> **Wichtig:**
>
> Wenn Sie eine OAuth- oder **Auth-Basic-Richtlinie** für die ausgewählten API-Ressourcen konfigurieren, konfigurieren Sie die Richtlinie „ **Keine Authentifizierung“für die verbleibenden** API-Ressourcen. Diese Konfiguration zeigt explizit an, dass Sie die Authentifizierung für die übrigen

> Ressourcen überspringen möchten.

Autorisierung Diese Richtlinie überprüft die erforderlichen Berechtigungen für den Zugriff auf eine API-Ressource. Die Zugriffsberechtigungen werden als eine Reihe von Ansprüchen und erwarteten Werten dargestellt. Um diese Richtlinie zu konfigurieren, wählen Sie **Neuen Anspruch hinzufügen** aus und geben Sie Folgendes an:

- Bezeichnung des Antrags
- Werte einfordern

> **Wichtig:**
>
> API-Sicherheit erfordert sowohl Authentifizierungs- als auch Autorisierungsrichtlinien für den API-Verkehr. Daher müssen Sie eine Autorisierungsrichtlinie mit einer Authentifizierungsrichtlinie konfigurieren. Die Authentifizierungsrichtlinie kann OAuth oder sein. `Auth-Basic`
>
> Auch wenn Sie über keine Autorisierungsprüfungen verfügen, müssen Sie eine Autorisierungsrichtlinie mit leeren Ansprüchen erstellen. Andernfalls wird die Anfrage mit einem 403-Fehler abgelehnt.

Ratenlimit

Geben Sie die maximale Belastung an, die der ausgewählten API-Ressource zugewiesen wird. Mit dieser Richtlinie können Sie die API-Datenverkehrsrate überwachen und vorbeugende Maßnahmen ergreifen. Um diese Richtlinie zu konfigurieren, geben Sie Folgendes an:

- **HTTP-Header-Name** - Es ist ein Traffic-Selektorschlüssel, der den Datenverkehr filtert, um die API-Anfragen zu identifizieren. Und die Ratenlimit-Richtlinie gilt und überwacht nur solche API-Anfragen.
- **Header-Werte** - Diese Header-Werte werden durch Kommas für den genannten Header-Namen getrennt.
- **Schwellenwert** - Die maximale Anzahl von Anfragen, die im angegebenen Intervall zulässig sind. Wenn Sie **Header-Werte**angegeben haben, gilt dieser Schwellenwert für jeden Header-Wert.

  Beispiel-1:

  Wenn Sie Header-Werte (`"key1","key2","key3"`) für den Header-Namen `x-api-key` angeben und den Schwellenwert auf `80` festlegen, gilt der festgelegte Schwellenwert für jeden Header-Wert.

  Beispiel-2:

  Wenn Sie für jeden Header-Wert unterschiedliche Schwellenwerte angeben möchten, erstellen Sie separate Richtlinien für Ratenbegrenzungen mit demselben HTTP-Header-Namen.

  - **Policy-1**: Geben Sie Header-Werte (`"key1"`,`"key2"`) für den Header-Namen `x-api-key` an und legen Sie den Schwellenwert auf `80` fest.
  - **Policy-2**: Geben Sie Header-Werte (`"key3"`) für den Header-Namen `x-api-key` an und legen Sie den Schwellenwert auf `30` fest.

  Wenn Sie keinen Header-Wert angeben, gilt der Schwellenwert für den angegebenen HTTP-Headernamen.

- **Zeitscheibe** - Das in Mikrosekunden angegebene Intervall. Während dieses Intervalls werden die Anforderungen anhand der konfigurierten Limits überwacht. Standardmäßig ist er auf 1000 Mikrosekunden (1 Millisekunde) eingestellt.
- **Limit-Typ** - Der Modus, in dem Sie die Ratenlimit-Richtlinie anwenden möchten. Sie können den Grenztyp **Burst** oder **Smooth** auswählen.
- **Aktion** - Definiert eine Aktion, die Sie für den Traffic ausführen möchten, der den Schwellenwert überschreitet. Sie können eine der folgenden Aktionen festlegen:
  - **DROP**: Löscht die Anfragen, die die konfigurierten Datenverkehrslimits überschreiten.
  - **RESET**: Setzt die Verbindung für die Anfragen zurück.
  - **REDIRECT**: Leitet den Datenverkehr auf die konfigurierte redirect_url um.
  - **RESPOND**: Reagiert mit der Standardantwort (`429 Too many requests`).

WAF

Diese Richtlinie verhindert Sicherheitsverletzungen, Datenverlust und mögliche unbefugte Änderungen an Websites, die auf sensible Geschäfts- oder Kundeninformationen zugreifen.

Bevor Sie eine WAF-Richtlinie konfigurieren, erstellen Sie mit StyleBooks ein WAF-Profil in NetScaler Console.

Wählen Sie in **WAF-Profilname**das von Ihnen erstellte WAF-Profil aus oder geben Sie es an.

Bot

Diese Richtlinie identifiziert schlechte Bots und schützt Ihre Appliance vor erweiterten Sicherheitsangriffen.

Bevor Sie eine BOT-Richtlinie konfigurieren, erstellen Sie mit StyleBooks ein BOT-Profil in NetScaler Console.

Geben Sie unter **Bot-Profilname** das BOT-Profil an, das Sie erstellt haben.

Header Rewrite

Diese Richtlinie hilft Ihnen, den Header von API-Anfragen und -Antworten zu ändern. Wenn Sie den Wert im HTTP-Header ersetzen möchten, geben Sie Folgendes an:

- **HTTP-Header-Name**: Der abgerufene Name, den Sie im Anforderungsheader ändern möchten.

  Beispiel:`Host`

- **Header-Wert**: Optional ist die Wertzeichenfolge, die Sie im angegebenen Header-Namen ändern möchten.

  Beispiel:`sample.com`

- **Header neuer Wert**: Der neue Wert, der den angegebenen Header-Wert ersetzt.

  Wenn kein **Header-Wert** angegeben wird, ersetzt es jeden empfangenen Wert durch den angegebenen Wert für den **HTTP-Header-Namen**.

  Beispiel:`example.com`

In diesem Beispiel wird die Richtlinie `sample.com` zum Umschreiben von Kopfzeilen `example.com` im `Host` Feld einer API-Anforderung ersetzt.

URI Path Rewrite

Diese Richtlinie hilft Ihnen, den URI-Pfad von API-Anfragen und -Antworten zu ändern. Wenn Sie ein Segment im URI-Pfad ersetzen möchten, fügen Sie eine Regel hinzu, um einen der folgenden Schritte auszuführen:

- **Pfadsegment ersetzen** —Wenn Sie diesen Aktionstyp auswählen, geben Sie Folgendes an:
  - **Aktuelles Pfadsegment** —Das Pfadsegment, das Sie ersetzen möchten.
  - **Neues Pfadsegment** —Neues Pfadsegment, das nur das aktuelle Pfadsegment ersetzt.

  Um beispielsweise ein Gebietsschema im URI-Pfad von Englisch in Chinesisch zu ändern, geben Sie `/en-us/` in **Current Path Segment** an. Und geben Sie unter `/zh-zh`**Neues Pfadsegment**an. Es ersetzt nur das Pfadsegment und behält den verbleibenden URI-Pfad bei.

- **Vollständigen Pfad ersetzen** —Dieser Aktionstyp ersetzt den URI-Pfad von API-Anfragen und -Antworten vollständig durch den angegebenen Pfad. Wenn Sie unter **Neues Pfadsegment**angeben `/example.html`, wird der URI-Pfad einer API-Anfrage oder -Antwort in den angegebenen Pfad geändert.

- **Pfadsegment entfernen** —Diese Aktion entfernt das angegebene Segment aus dem URI. Um beispielsweise das englische Gebietsschema aus dem URI-Pfad zu entfernen, geben Sie `/en-us/` in **Current Path Segment**an.

- **Pfadsegment einfügen** —Mit dieser Aktion wird das angegebene Segment in den URI-Pfad eingefügt. Um diese Regel anzuwenden, geben Sie die Position an, an der Sie das Segment einfügen möchten. Und welches Segment Sie einfügen möchten.

  Wenn Sie beispielsweise ein Segment direkt nach einem Text einfügen möchten, gehen Sie wie folgt vor:

  1. Geben Sie die Position an, an der Sie ein neues Segment einfügen möchten.
  2. Geben Sie **unter Aktuelles Pfadsegment**den Text an, nach dem ein neues Segment hinzugefügt werden soll.
  3. Geben Sie **unter Neues Pfadsegment**das Segment an, das Sie hinzufügen möchten.

Verweigern

Mit dieser Richtlinie können Sie verhindern, dass API-Anfragen Ihre API-Ressourcen erreichen.

API-Analysen anzeigen

January 26, 2024

API-Analysen ermöglichen Transparenz im API-Datenverkehr. Diese Analyse ermöglicht es IT-Administratoren, API-Instanzen und Endpunkte zu überwachen, die von einem API-Gateway bereitgestellt werden. Es bietet eine integrierte periodische Überwachung von API-Anfragen.

Bevor Sie API-Analysen überwachen, stellen Sie sicher, dass Sie Folgendes ausführen:

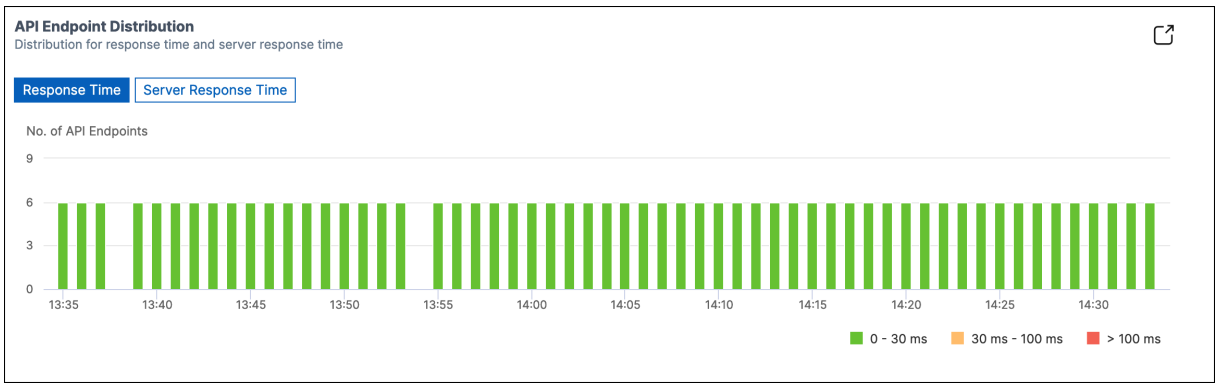
1. Hinzufügen einer API-Definition
2. Bereitstellen einer API-Definition
3. Hinzufügen einer Richtlinie zu einer API-Definition
4. Lizenz auf API-Instanzen anwenden
5. Aktivieren von Web Insight für API-Instanzen

In **API Analytics** können Sie die Antwortzeit von API-Instanzen und Endpunkten überwachen, die als Teil von API-Definitionen hinzugefügt werden. Es zeigt auch die Bandbreite an, die von API-Instanzen und Endpunkten verbraucht wird.

Standardmäßig zeigt das Dashboard API-Analysen für die letzte Stunde an. Sie können eine Dauer auswählen, um API-Analysen für dieses Intervall anzuzeigen. Klicken Sie auf **Mehr** anzeigen auf jeder Kachel, um die gesamte Liste anzuzeigen. In dieser Ansicht können Sie API-Instanzen und Endpunkte anhand ihrer Teilnamen mit Ausnahme der Kachel **Geo Locations** durchsuchen.

API-Endpunktverteilung

Dieses Diagramm zeigt die Verteilung der Anwendungs- und Serverantwortzeit für API-Endpunkte an. Sie können einen API-Endpunkt identifizieren, der eine enorme Reaktionszeit hat, und die erforderlichen Maßnahmen ergreifen.

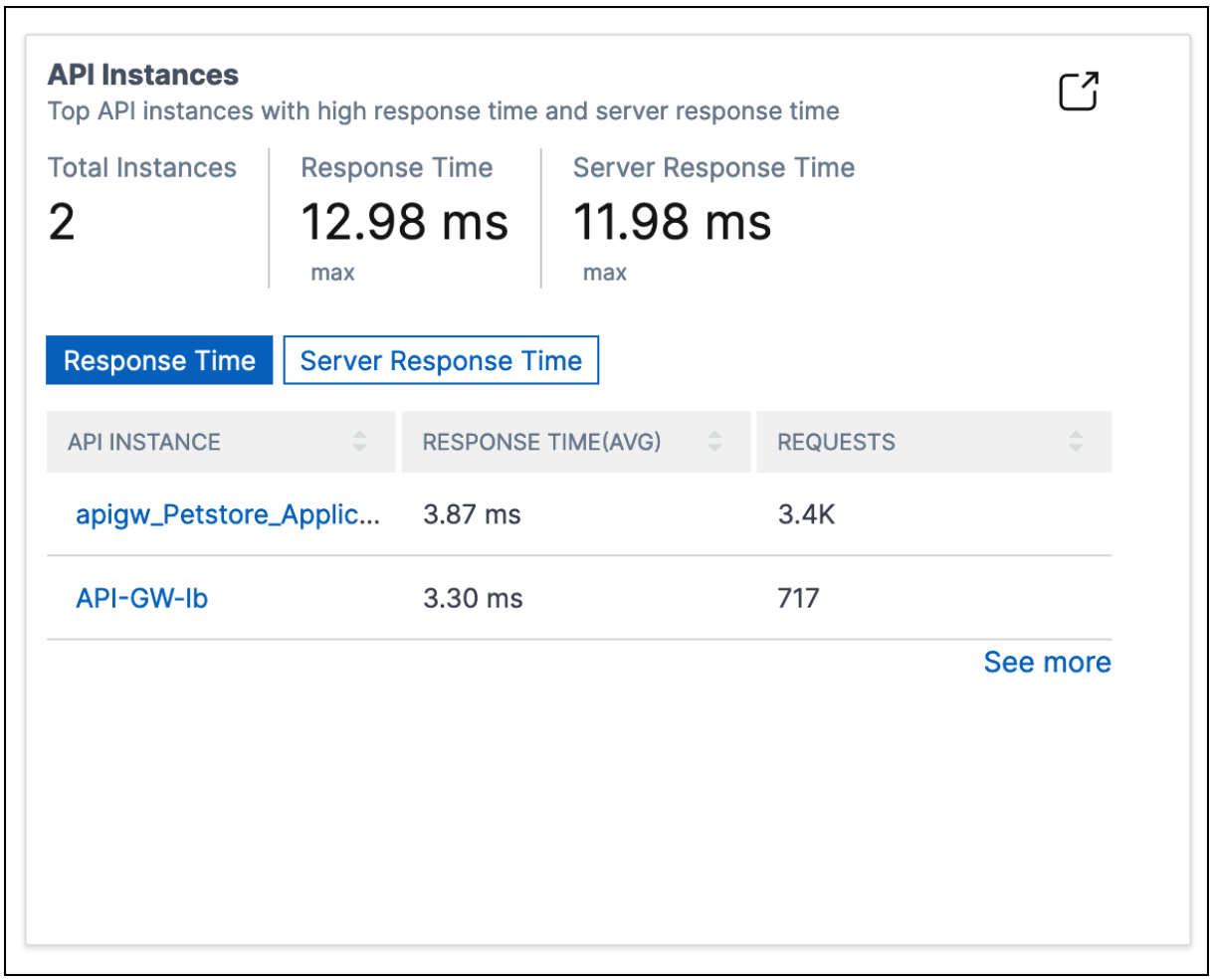


Die API-Endpunkte werden abhängig von ihren Antwortzeitlimits in einer der folgenden Farben angezeigt:

- **Grün** —Wenn die Reaktionszeit weniger als 30 Millisekunden beträgt.
- **Orange** —Wenn die Reaktionszeit zwischen 30—100 Millisekunden liegt.
- **Rot** —Wenn die Reaktionszeit mehr als 100 Millisekunden beträgt.

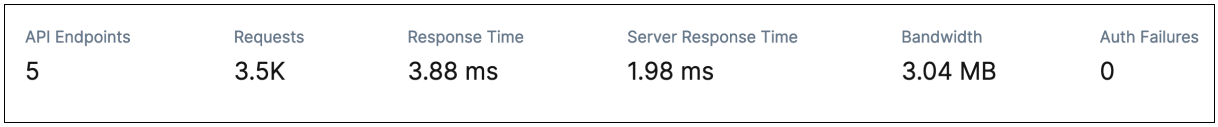
API-Instanzen

Die Kachel "**API-Instanzen** "zeigt die wichtigsten API-Instanzen mit hoher Anwendungs- und



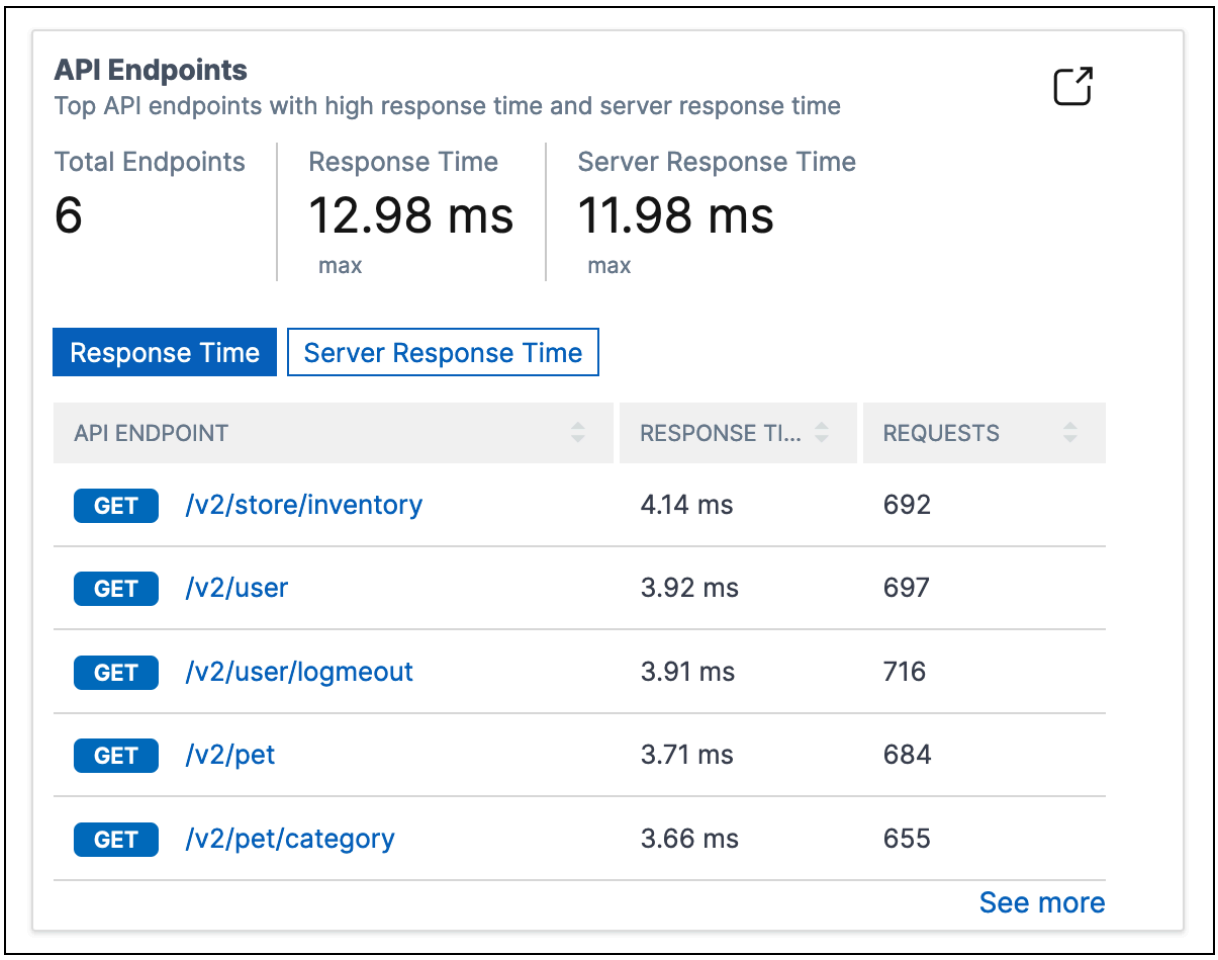
Wählen Sie eine API-Instanz, um deren Leistungs-, Nutzungs- und Sicherheitsdetails anzuzeigen. Die ausgewählte API-Instanz zeigt die folgenden Informationen an:

- Anzahl API-Endpunkte
- Anfragen zählen
- Anwendungs- und Serverantwortzeit
- Verbrauchte Bandbreite
- Authentifizierungsfehler



API-Endpunkte

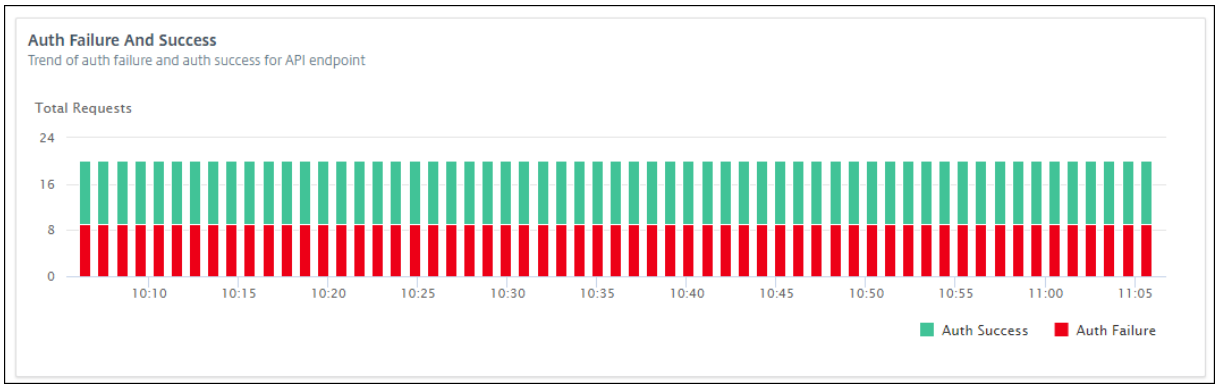
Die Kachel **API-Endpunkte** zeigt die obersten Endpunkte mit hoher Anwendungs- und Serverantwortzeit an.



Wählen Sie einen API-Endpunkt, um Leistungs-, Nutzungs- und Sicherheitsdetails anzuzeigen

Authentifizierungsfehler

Die Kachel **Authentifizierungsfehler** zeigt die wichtigsten API-Endpunkte an, die mehr Authentifizierungsfehler aufweisen. Der Authentifizierungsfehler oder der Erfolg der Authentifizierung erfolgt basierend auf der Richtlinie, die einer API-Definition hinzugefügt wurde.



Wenn Sie Authentifizierungsfehler und Erfolgsrate in einem API-Endpunkt anzeigen möchten, gehen Sie wie folgt vor:

1. Wählen Sie einen Endpunkt von **API-Endpunkten** aus.
2. Klicken Sie auf die Registerkarte **Sicherheit**. Auf dieser Registerkarte werden die Authentifizierungsfehler und -erfolge auf dem ausgewählten Endpunkt angezeigt.

Wenn Sie den Authentifizierungsfehler und die Erfolgsrate in den API-Endpunkten einer Instanz anzeigen möchten, gehen Sie wie folgt vor:

1. Wählen Sie eine Instanz aus **API-Instanz**aus.
2. Klicken Sie auf die Registerkarte **Sicherheit**. Auf dieser Registerkarte werden die Authentifizierungsfehler und -erfolge in den Endpunkten der ausgewählten Instanz angezeigt.

Verschiedene API-Einblicke anzeigen

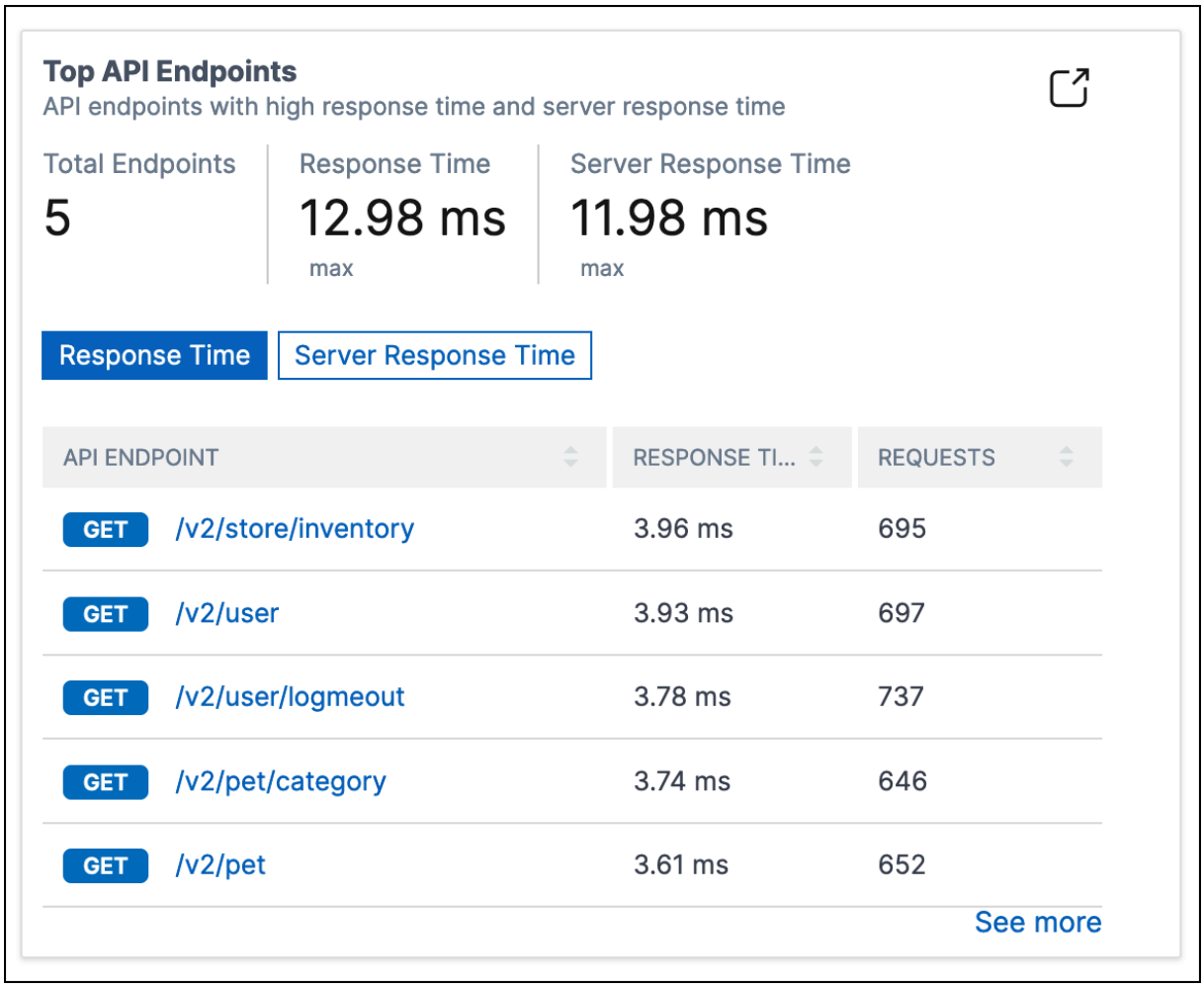
Navigieren Sie durch API Analytics, um spezifische Informationen zu folgenden Themen anzuzeigen:

- Top-API-Endpunkte in einer Instanz
- APIs auf die meisten
- Geolokalisierung eines Endpunkts
- HTTPS-Antwortstatus
- Trend bei API-Anfragen
- Bandbreitenverbrauch eines Endpunkts
- SSL-Fehler und Verwendung

Zeigen Sie die wichtigsten API-Endpunkte in einer Instanz an

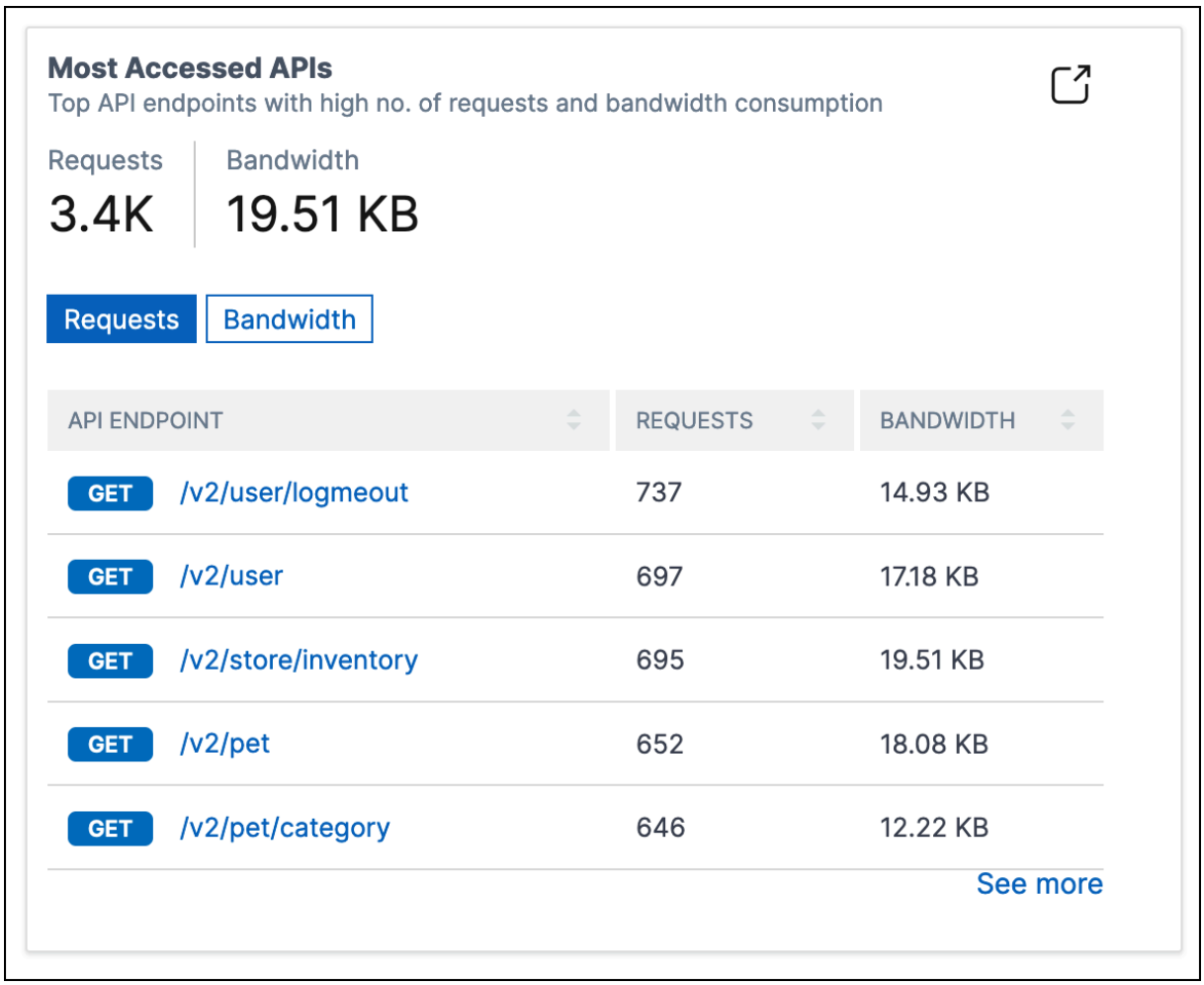
Auf der Seite **API Analytics** werden die wichtigsten Endpunkte angezeigt, die eine hohe Reaktionszeit haben. Wenn Sie ähnliche Endpunkte einer Instanz anzeigen möchten, wählen Sie eine Instanz aus **API-Instanzen**aus.

Die Kachel **Top API Endpoints** zeigt die Endpunkte an, die eine hohe Anwendungs- und Serverantwortzeit aufweisen.



APIs anzeigen, auf die

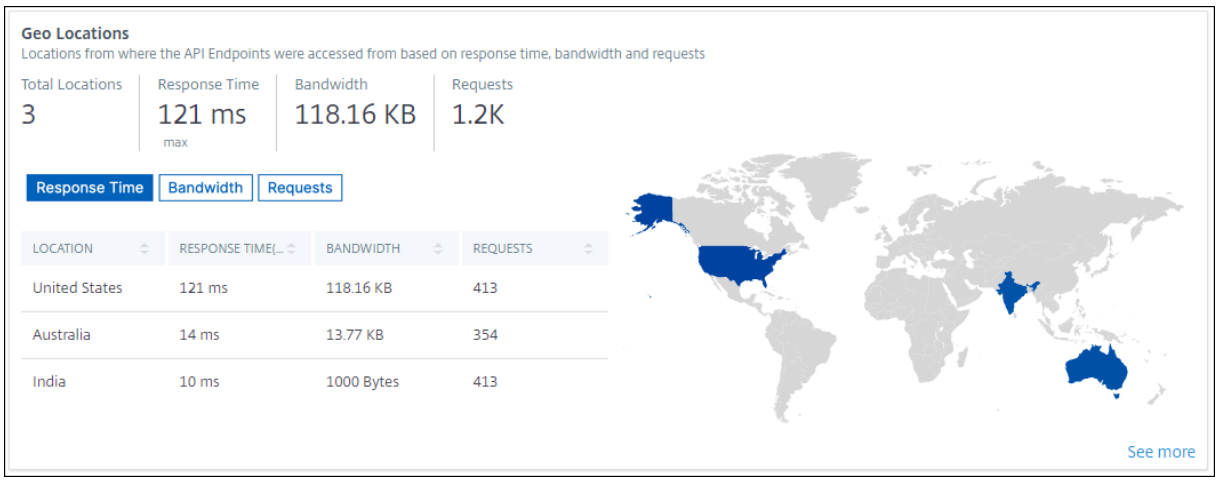
Wählen Sie in **API Analytics**eine API-Instanz aus API-Instanzen aus. Die Kachel **APIs mit den meisten Zugriffen** zeigt die obersten Endpunkte an, die mehr Anforderungen und Bandbreite haben



Geolocation eines Endpunkts anzeigen

1. Wählen Sie in **API Analytics**eine der folgenden Optionen aus:
   - Wählen Sie eine Instanz aus **API-Instanzen** aus, um die Standorte anzuzeigen, von denen die Endpunkte der ausgewählten Instanz Anforderungen erhalten haben.
   - Wählen Sie einen Endpunkt unter **API-Endpoints** aus, um Standorte anzuzeigen, von denen der Endpunkt Anfragen erhalten hat
2. Unter **Leistung und Nutzung**wird die Kachel **Geostandorte** angezeigt.

   Sie können Standorte nach Antwortzeit, Bandbreite und Anforderungen sortieren.

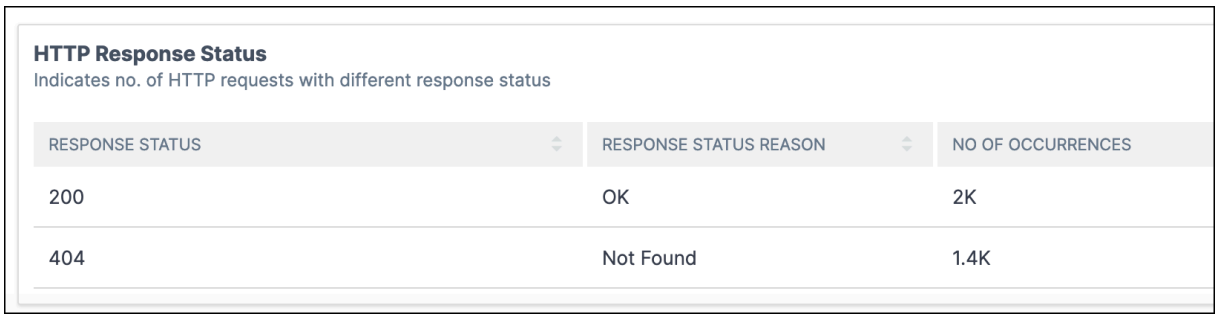


HTTPS-Antwortstatus anzeigen

Die Kachel **HTTPS-Antwortstatus** zeigt den Antwortstatus mit seinen Gründen und Vorkommen an. Sie können den HTTPS-Antwortstatus auf eine der folgenden Arten anzeigen:

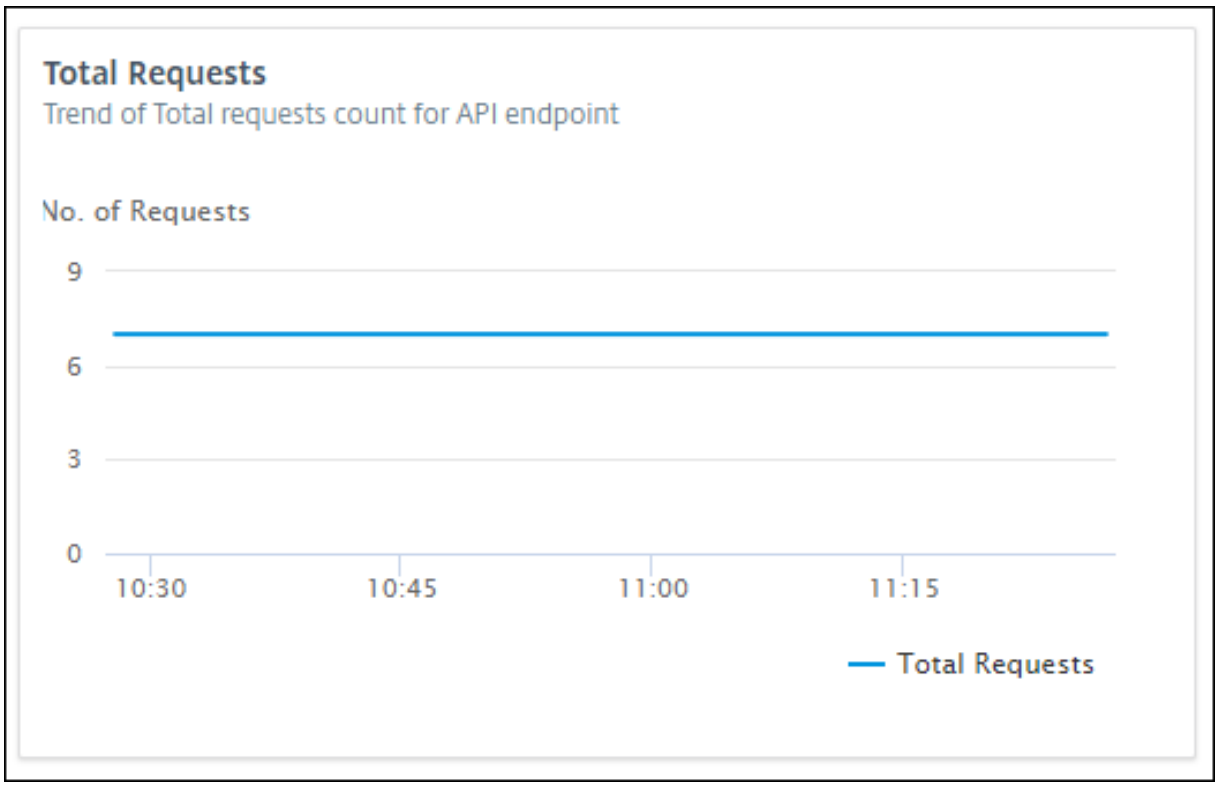
- Wählen Sie eine Instanz aus **API-Instanzen** aus.
- Wählen Sie einen Endpunkt von **API-Endpunkten** aus.

Diese Kachel wird auf der Registerkarte **Leistung und Nutzung** angezeigt.

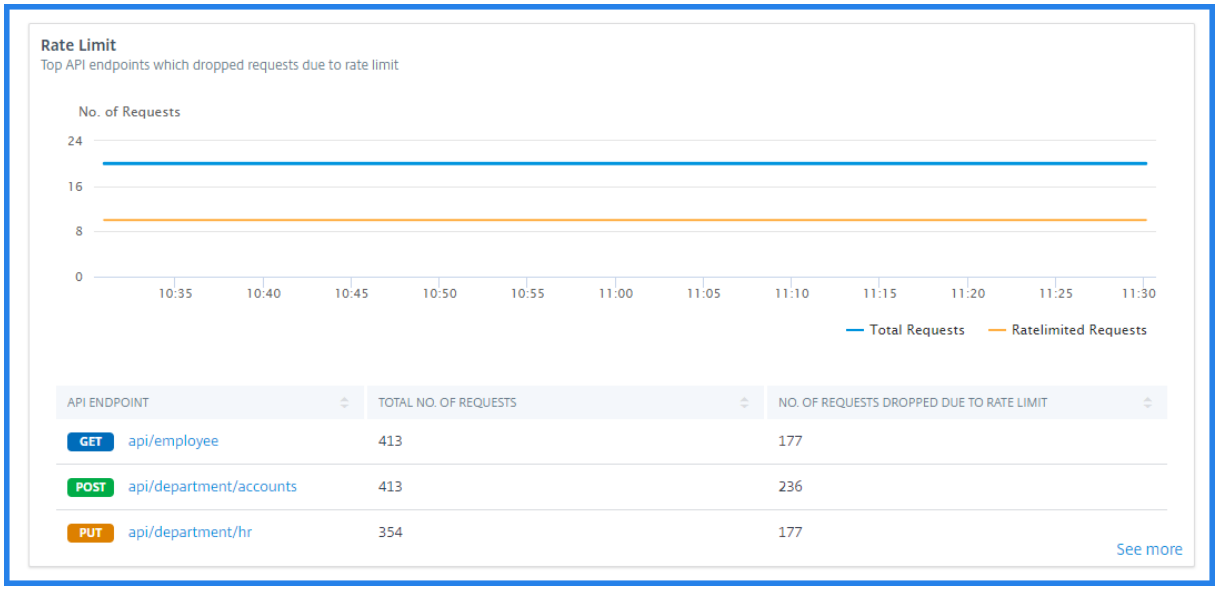


Trend der API-Anfragen anzeigen

Wählen Sie einen Endpunkt von **API-Endpunkten** aus. Unter **Leistung und Nutzung**zeigt die Kachel **Anfragen insgesamt** den Trend der Gesamtzahl der von einem Endpunkt empfangenen Anforderungen an.



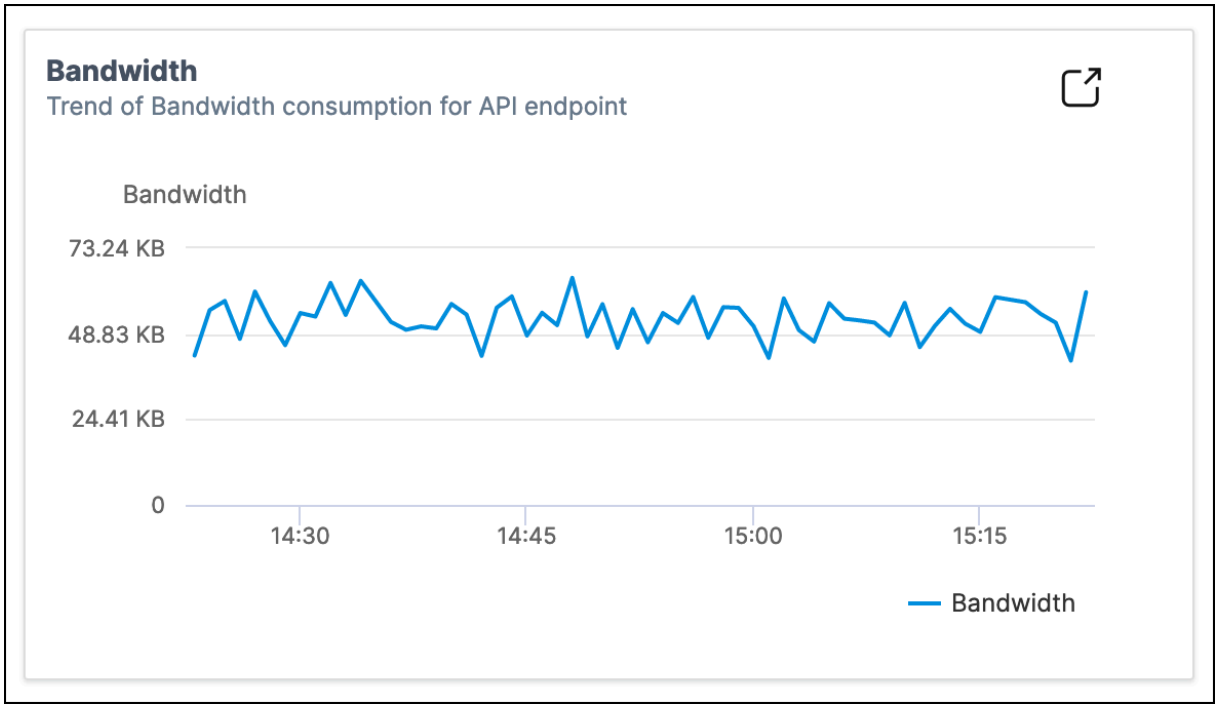
Wenn Sie den Trend zu verworfenen Anforderungen aufgrund einer Ratenbegrenzung anzeigen möchten, wählen Sie eine Instanz aus **API-Instanzen**aus. In **Sicherheit**zeigt die Kachel **Ratenlimit** den Trend zu verworfenen Anfragen an. Es zeigt auch den Trend der Gesamtzahl der an einem Endpunkt eingegangenen Anfragen an.



Mit diesem Vergleich können Sie ermitteln, wie viele Anfragen aufgrund einer Ratenbegrenzung unter den Gesamtanforderungen verworfen wurden.

Bandbreitenverbrauch eines Endpunkts anzeigen

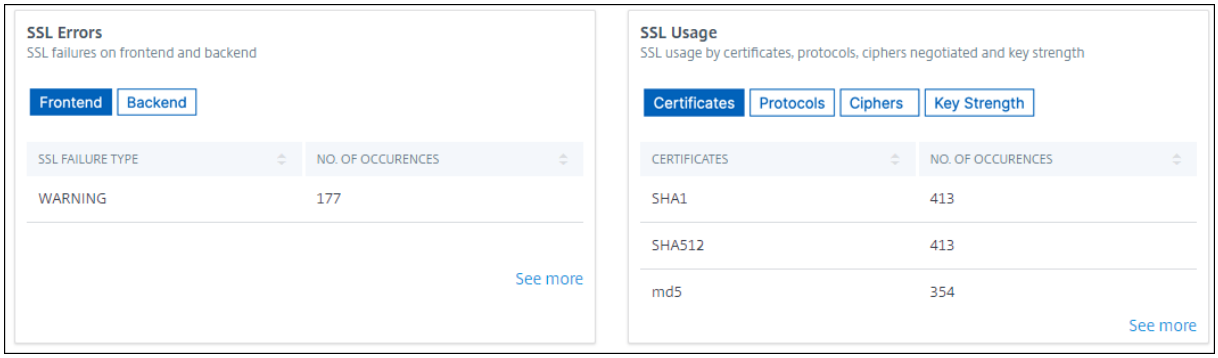
Um den Trend des Bandbreitenverbrauchs nach einem Endpunkt anzuzeigen, wählen Sie einen Endpunkt aus den API-Endpunkten aus. Die Kachel **Bandbreite** zeigt ein Diagramm zum Bandbreitenverbrauch



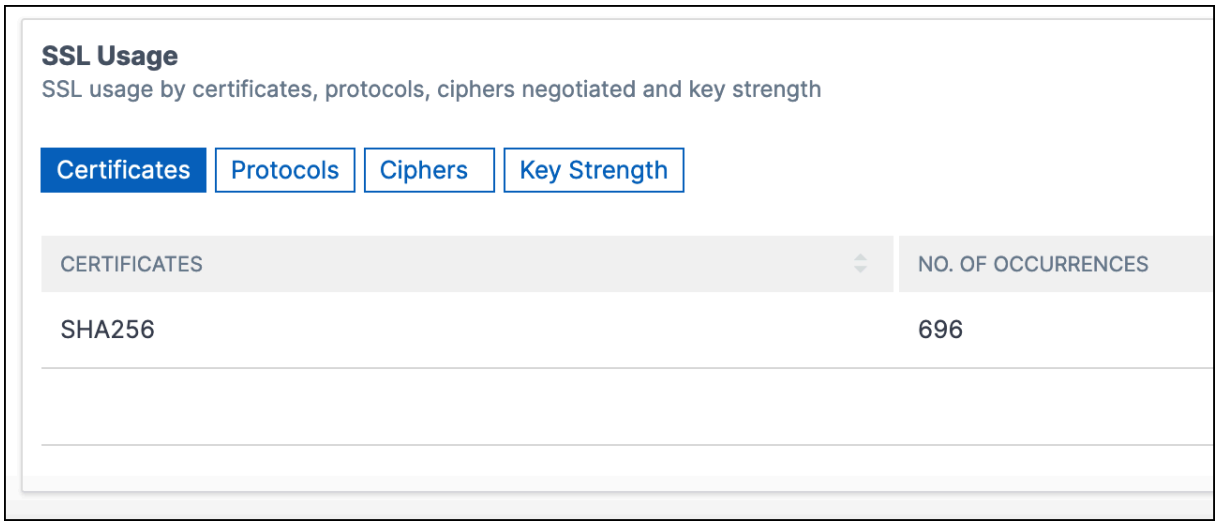
SSL-Fehler und -Nutzung anzeigen

Wählen Sie eine Instanz aus **API-Instanzen** aus. In **Sicherheit**werden die folgenden Kacheln angezeigt:

- **SSL-Fehler** —Zeigt auf Clients und Anwendungsservern aufgetretene SSL-Fehler an.
- **SSL-Verwendung** —Zeigt SSL-Zertifikate, Protokolle, Verschlüsselung und wichtige Stärken mit ihren Vorkommen an.



Um die SSL-Nutzung in einem Endpunkt anzuzeigen, wählen Sie einen Endpunkt aus den API-Endpunkten aus. Die Kachel **SSL-Nutzung** wird auf der Registerkarte **Sicherheit** angezeigt.



Discovery von API-Endpunkten

July 17, 2024

Mit API Security können Sie die erkannten API-Endpunkte in Ihrer Organisation anzeigen. NetScaler Console erkennt die API-Endpunkte auf der Grundlage des API-Datenverkehrs, der auf NetScaler-Instanzen und API-Bereitstellungen empfangen wird.

In NetScaler Console werden auf der Seite **Sicherheit > API-Sicherheit > API**-Erkennung die erkannten API-Endpunkte angezeigt.

- **Virtuelle Server**—Auf der Registerkarte **vServer** werden die virtuellen Server Ihrer NetScaler-Instanzen angezeigt. Die virtuellen Server werden auf dieser Registerkarte angezeigt, wenn sie die API-Anfragen für den angegebenen Zeitraum erhalten.
- **API-**Bereitstellungen —Auf dieser Registerkarte werden die API-Bereitstellungen angezeigt, die mithilfe einer API-Definition von NetScaler Console aus bereitgestellt werden. Auf dieser Registerkarte werden die API-Endpunkte erkundet, wenn API-Bereitstellungen die API-Anfragen für den angegebenen Zeitraum erhalten. Informationen zum Hinzufügen und Bereitstellen einer API-Definition finden Sie unter Hinzufügen einer API-Definition und Bereitstellen von API-Definitionen.

> **Hinweis:**
>
> - Stellen Sie sicher, dass Sie Analysen konfigurieren und Web Insights auf virtuellen Servern

aktivieren. Siehe Web Insight auf API-Instanzen aktivieren.

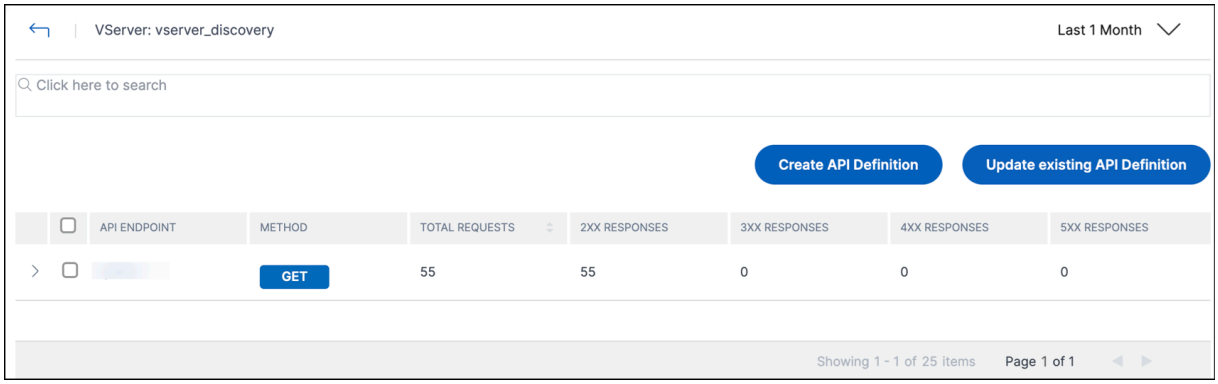
- Sie können nur Richtlinien zu den API-Endpoints hinzufügen, die auf der Registerkarte **API-Bereitstellungen** erkannt werden.

Anzeigen von API-Endpunkten

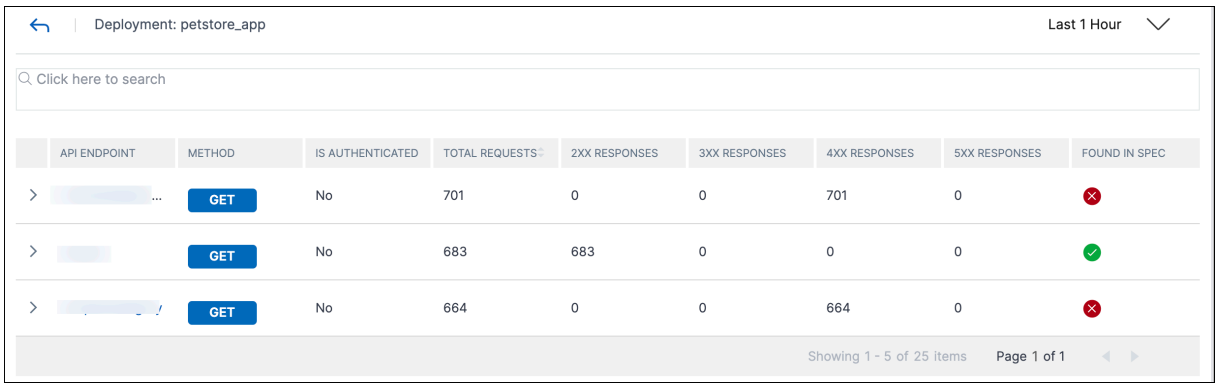
Wenn Sie in **API Discovery** einen virtuellen Server oder eine API-Bereitstellung auswählen, zeigt die NetScaler Console-GUI die API-Endpunkte und ihre Details an, z. B.:

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

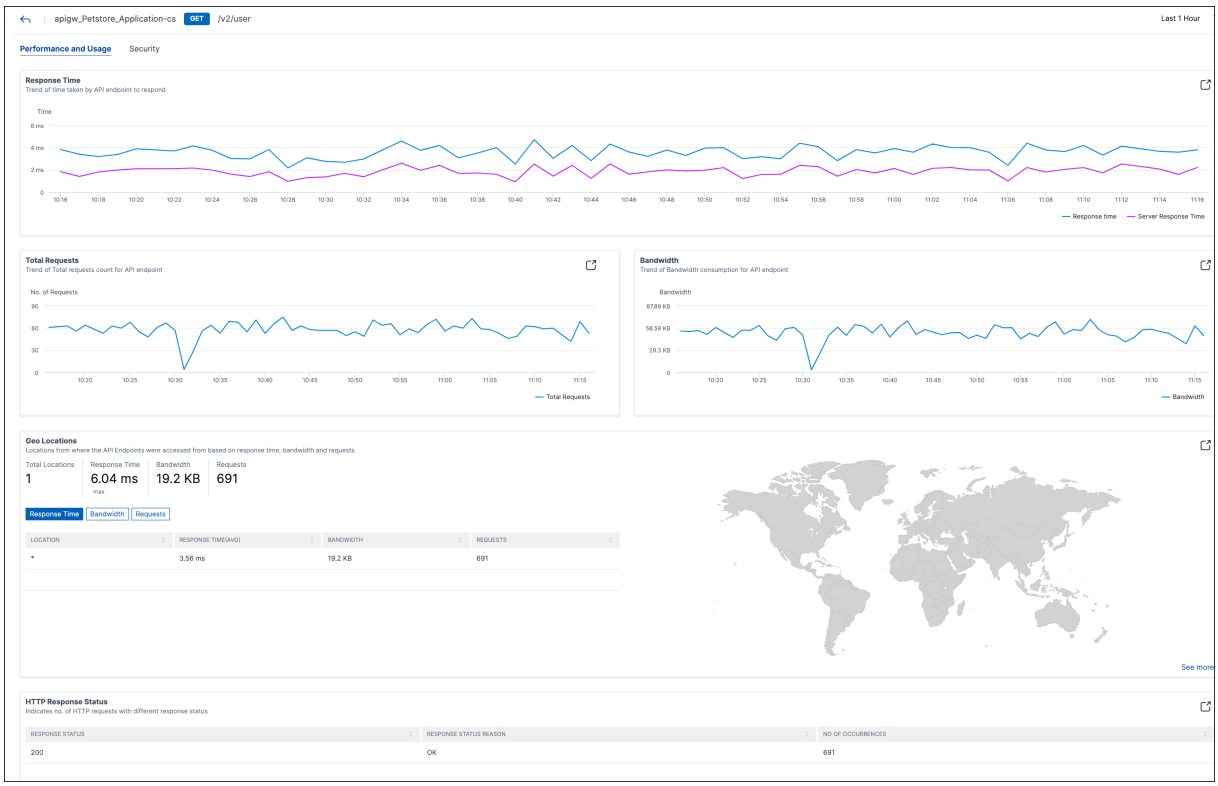
Die API-Endpunkte in einem virtuellen Server sind wie folgt verfügbar:



Die API-Endpunkte in API-Bereitstellungen sind wie folgt verfügbar:



Sie können auch den erforderlichen API-Endpunkt auswählen, um den detaillierten Analysebericht anzuzeigen.



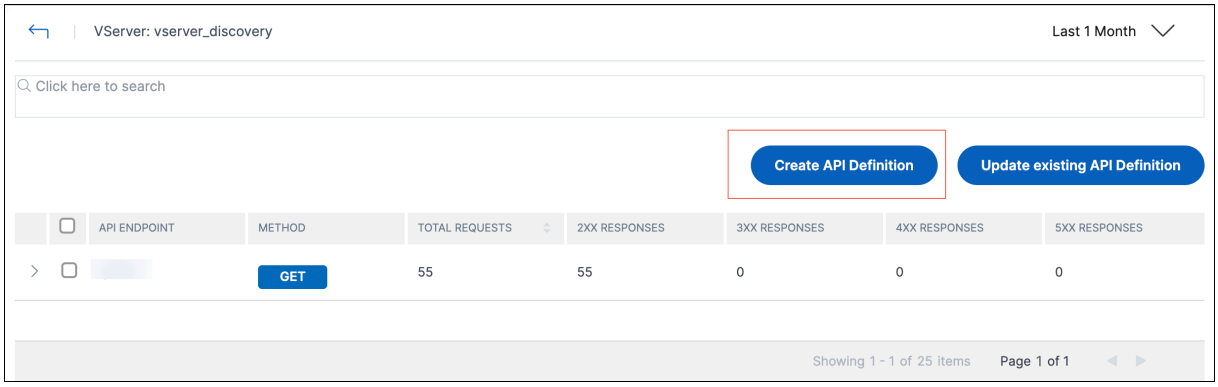
Weitere Informationen zu den einzelnen Abschnitten finden Sie unter Anzeigen von API-Analysen.

API-Definitionen aus erkannten API-Endpunkten erstellen

So erstellen Sie API-Definitionen aus erkannten API-Endpunkten (API-Ressourcen und -Methoden):

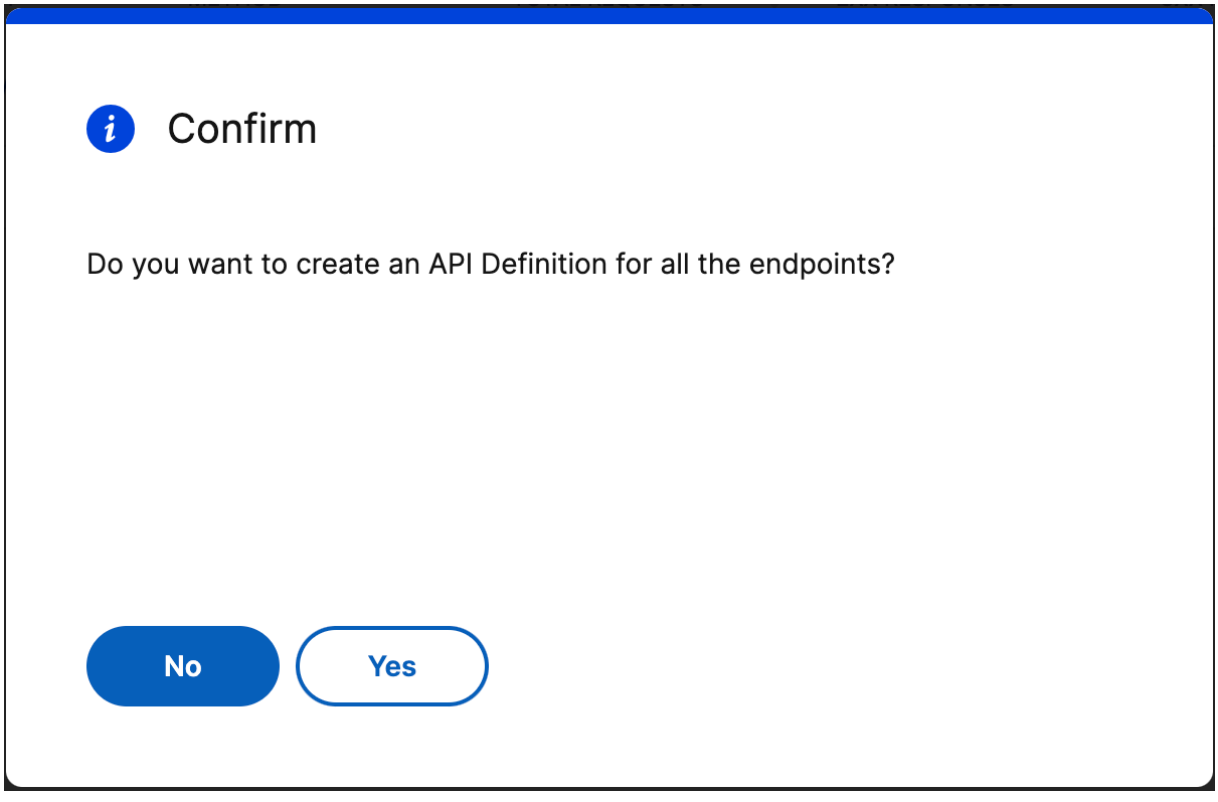
1. Navigieren Sie zu **Sicherheit > API-Sicherheit > API Discovery**, um die Liste der virtuellen Server und API-Bereitstellungen anzuzeigen.
2. Klicken Sie auf der Registerkarte **vServer** auf einen beliebigen virtuellen Server.

3. Auf der Seite des virtuellen Servers wird die Liste der erkannten Endpunkte angezeigt. Wählen Sie einen beliebigen Endpunkt aus und klicken Sie auf **API-Definition erstellen**.



Hinweis:

Wenn Sie keinen Endpunkt auswählen und auf **API-Definition erstellen**klicken, wird ein Popup-Fenster angezeigt, in dem Sie bestätigen können, ob Sie eine API-Definition für alle Endpunkte erstellen möchten. Klicken Sie auf **Ja**, um die API-Definition mit allen Endpunkten zu erstellen, oder klicken Sie auf **Nein**.



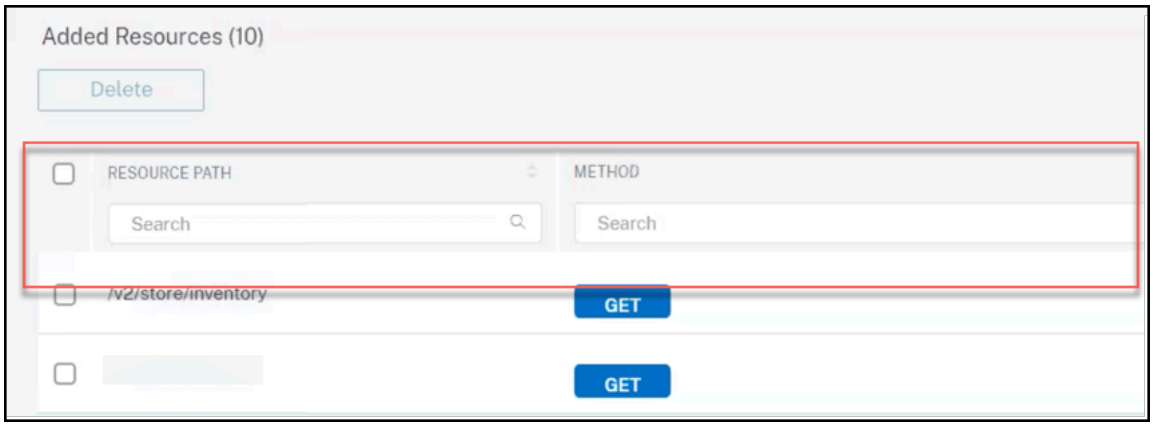
1. Geben Sie unter **API-Definition erstellen**Folgendes an:

   - **Name** - Ein Name für die API-Definition.

- **API-Definition** - Eine Definition muss Titel, Version, Basispfad und Host enthalten. Sie können einen Domänennamen oder eine IP-Adresse im Feld **Host** angeben.
- **API-Ressourcen** - Fügen Sie Ihrer Definition mehrere API-Ressourcen hinzu. Jede Ressource hat einen Pfad und eine unterstützte Methode.

2. Klicken Sie auf **Definition erstellen**, um die API-Definition zu erstellen.

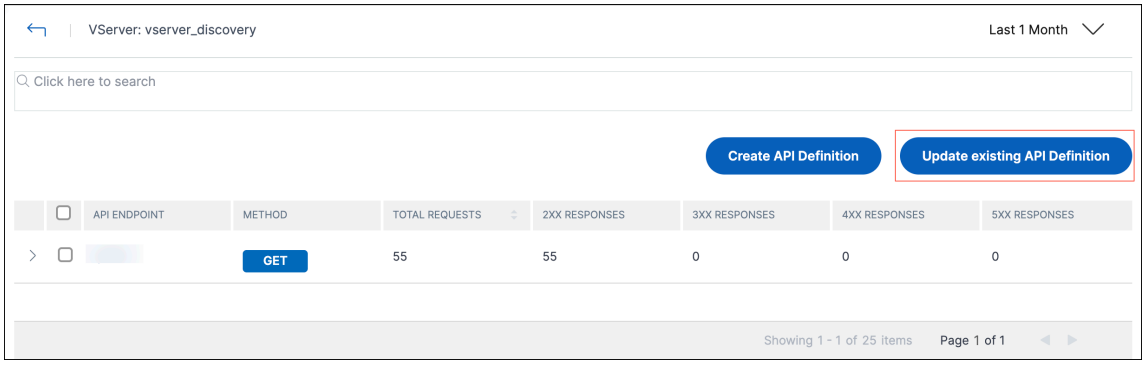
> **Hinweis:**
>
> Wenn Sie einen API-Ressourcenpfad bearbeiten möchten, bevor Sie ihn zur API-Definition hinzufügen, verwenden Sie die Sortier- oder Suchfunktion für die API-Ressourcen auf dem API-Definitionsbildschirm.
>
> Stellen Sie sich beispielsweise eine API-Ressource mit dem Namen "/api/products/123-3243-2344334/reviews"vor, wobei das Pfadsegment "123-3243-2344334"eine variable Produkt-ID ist. Sie können jetzt die API-Ressourcen sortieren, den Ressourcenpfad als "/api/products/{id}/reviews"hinzufügen und alle API-Endpunkte mit IDs wie "/api/products/123-3243-2344334/reviews"löschen.



Vorhandene API-Definition mit erkannten API-Endpunkten aktualisieren

So aktualisieren Sie eine vorhandene API-Definition mit API-Endpunkten (API-Ressourcen und -Methoden):

1. Navigieren Sie zu **Sicherheit > API-Sicherheit > API Discovery**, um die Liste der virtuellen Server und API-Bereitstellungen anzuzeigen.
2. Klicken Sie auf der Registerkarte **vServer** auf einen beliebigen virtuellen Server.
3. Auf der Seite des virtuellen Servers wird die Liste der erkannten Endpunkte angezeigt. Wählen Sie den Endpunkt aus, den Sie einer vorhandenen API-Definition hinzufügen möchten. Klicken Sie auf **Bestehende API-Definition aktualisieren**.



4. Wählen Sie aus der Dropdownliste **Vorhandene API-Definition auswählen** die API-Definition aus, die Sie aktualisieren möchten. Klicken Sie auf **Definition aktualisieren**.
5. Die Seite **Bestehende API-Definition aktualisieren** wird angezeigt. Im Abschnitt **API-Ressourcen** werden die folgenden Tabellen angezeigt:
   - **Hinzugefügte Ressourcen** —Die von Ihnen ausgewählten API-Endpunkte
   - **Bestehende Ressourcen** —Die API-Endpunkte, die bereits in der API-Definition verfügbar sind

   > **Hinweis:**
   >
   > Wenn derselbe API-Endpunkt in **Added Resources** und **Existing Resources** verfügbar ist, wird der Endpunkt nur einmal zur API-Definition hinzugefügt.

6. Klicken Sie auf **Definition aktualisieren**.

Bereitstellung einer API-Instanz aufheben

January 26, 2024

Sie können die Option Undeploy verwenden, wenn Sie die API-Instanzkonfiguration aus einer NetScaler-Instanz entfernen möchten, die API-Instanzobjekte jedoch als Entwurf in der NetScaler Console beibehalten möchten. Diese Aktion setzt den Bereitstellungsstatus auf In Entwurf. Und es kann nur auf die bereitgestellten API-Instanzkonfigurationen angewendet werden.

> **Wichtig:**
>
> - Bevor Sie die Bereitstellung einer API-Bereitstellung aufheben, stellen Sie sicher, dass alle zugehörigen API-Richtlinien nicht bereitgestellt oder gelöscht wurden. Weitere Informationen finden Sie unter Bereitstellen einer API-Richtlinie.
> - Bevor Sie die Bereitstellung eines API-Proxys aufheben, stellen Sie sicher, dass alle zuge-

> hörigen API-Bereitstellungen nicht bereitgestellt oder gelöscht wurden. Weitere Informationen finden Sie unter Bereitstellen einer API-Bereitstellung.

Bereitstellung einer API-Richtlinie aufheben

Führen Sie die Schritte aus, um die Bereitstellung einer API-Richtlinie aufzuheben:

1. Wählen Sie unter **Sicherheit > API-Sicherheit > Richtlinien** die Richtlinie aus, deren Bereitstellung Sie rückgängig machen möchten.
2. Klicken Sie **auf Bereitstellen**.

Durch diese Aktion wird der **Richtlinienstatus** auf Im Entwurf festgelegt.

Bereitstellung einer API-Bereitstellung aufheben

Führen Sie die Schritte aus, um die Bereitstellung einer API-Bereitstellung aufzuheben:

1. Wählen Sie unter **Sicherheit > API-Sicherheit > API**-Bereitstellungen die API-Bereitstellung aus, deren Bereitstellung Sie rückgängig machen möchten.

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass alle zugehörigen Richtlinien der ausgewählten Bereitstellung aufgehoben oder gelöscht wurden.

2. Klicken Sie **auf Bereitstellen**.

Diese Aktion setzt den **Bereitstellungsstatus** auf In Entwurf.

Bereitstellung eines API-Proxy aufheben

Folgen Sie den Schritten, um die Bereitstellung eines API-Proxys aufzuheben

1. Wählen Sie unter **Sicherheit > API-Sicherheit > API-Proxys** den API-Proxy aus, dessen Bereitstellung Sie rückgängig machen möchten.

   > **Hinweis:**
   >
   > Sie können einen API-Proxy mit verschiedenen API-Bereitstellungen teilen. Stellen Sie daher sicher, dass alle zugehörigen Bereitstellungen des ausgewählten Proxys nicht bereitgestellt oder gelöscht wurden.

2. Klicken Sie **auf Bereitstellen**.

Diese Aktion setzt den **Proxy-Status** auf In Entwurf.

APIs zum Verwalten der API-Sicherheit verwenden

January 26, 2024

Sie können auf die APIs zugreifen, um eine API-Sicherheit zu erstellen, zu konfigurieren und bereitzustellen.

> **Hinweis:**
>
> Informationen zur Verwendung von API-Sicherheits-APIs zur Konfiguration der Funktion finden Sie in der Nitro-API-Dokumentation.

	Schritte	Ressourcen-URL
1	Erstellen Sie eine API-Definition	`https://adm.cloud.com/{ customerid } /apisec/nitro/v1/config/apidefs`
2	Einen API-Proxy hinzufügen	`https://adm.cloud.com/apiproxies`
3	Stellen Sie eine API-Instanz mithilfe des API-Proxys bereit	`https://adm.cloud.com/apiproxies/{ customerid } /deployments`
4	API-Richtlinien hinzufügen	`https://adm.cloud.com/{ customerid } /apisec/nitro/v1/config/policies/{ id }`

Jede API-Richtlinie hat ein anderes `config_spec`-Objekt. Es ist ein undurchsichtiges Objekt, das ein JSON-Wörterbuch enthält, um einen `policytype` mit bestimmten Werten zu konfigurieren.

In diesem Objekt können Sie eine API-Ressource und ihre Methoden mithilfe der folgenden Optionen auswählen:

- `api-resource-paths` - Geben Sie die API-Ressourcenpfade und -Methoden an, die in einer API-Definition definiert sind.

  Beispiel:

  ```
  {

  "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
      "get": true,
      "post": false,
      "put": false,
      "delete": false
   }
  ```

- `custom-rules` - Geben Sie die benutzerdefinierten API-Ressourcenpfade und -Methoden an, die in einer API-Definition möglicherweise nicht vorhanden sind.

  Beispiel:

  ```
  {

   "endpoints": ["/pet/categories", "/pet/findByName"],
      "get": true,
      "post": false,
      "put": false,
      "delete": false
   }
  ```

Bei dieser Konfiguration filtert die Richtlinie die eingehenden Verkehrsanfragen, die den angegebenen API-Ressourcenpfaden entsprechen.

Informationen zu den `config_spec` für die einzelnen Richtlinientypen finden Sie in den API-Beispielen für Richtlinientypen.

API-Beispiele für Richtlinientypen

In diesem Abschnitt werden die unterstützten API-Richtlinientypen und ihre Konfiguration beschrieben:

- Ratenlimit
- OAuth
- Grundlegende Authentifizierung
- Keine Authentifizierung
- Bot
- WAF
- Header Rewrite
- URI Path Rewrite

- Autorisierung
- Verweigern

Ratenlimit

Im Folgenden finden Sie eine Beispielkonfiguration für den Richtlinientyp `Ratelimit`. Geben Sie die folgende Konfiguration im `config_spec`-Objekt an:

```
{

    "policytype": "Ratelimit",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": false,
            "put": false,
            "delete": false
         }
 ,
        "custom-rules": {
  }
 ,
        "threshold": "10",
        "timeslice": "20000",
        "limittype": "BURSTY",
        "api-respondertype": "DROP",
        "header_name": "x-api-key",
        "per_client_ip": true
     }
 ,
    "order_index": 1,
    "policy_name": "ratelimit_policy"
 }
```

Weitere Informationen zu den einzelnen Attributen finden Sie unter Ratenbegrenzungsrichtlinie.

OAuth

Im Folgenden finden Sie ein Beispiel für eine API-Konfiguration für den Richtlinientyp `JWT Auth validation`. Geben Sie die folgende Konfiguration im `config_spec`-Objekt an:

```
{

    "policytype": "JWT Auth Validation",
    "config_spec": {
```



```
5
6           "api-resource-paths": {
7
8               "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                    "],
9               "get": true,
10              "post": true,
11              "put": false,
12              "delete": false
13           }
14  ,
15          "custom-rules": {
16   }
17  ,
18          "jwks-uri": "https://uri.petstore.com",
19          "issuer": "https://issuer.petstore.com",
20          "audience": "petstore",
21          "introspect-uri": "https://introspect.uri.com",
22          "clientid": "client",
23          "clientsecret": "clientsecret",
24          "claims-to-save": ["scope", "scope2"],
25          "allowed-algorithms": {
26
27              "hs256": true,
28              "rs256": true,
29              "rs512": true
30           }
31
32       }
33  ,
34     "order_index": 2,
35     "policy_name": "Jwt_auth_policy"
36  }
```

Weitere Informationen zu den einzelnen Attributen finden Sie in der OAuth-Richtlinie

Grundlegende Authentifizierung

Im Folgenden finden Sie ein Beispiel für eine API-Konfiguration für den Richtlinientyp `BasicAuth`:

```
1  {
2
3      "config_spec": {
4
5          "api-resource-paths": {
6
7              "delete": false,
8              "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                    "],
9              "get": true,
10             "post": true,
11             "put": false
```



```
          }
  ,
        "custom-rules": {
   }

      }
  ,
     "order_index": 3,
     "policy_name": "Auth_BaSIC",
     "policytype": "BasicAuth"
  }
```

Weitere Informationen zu den einzelnen Attributen finden Sie unter Grundlegende Authentifizierungsrichtlinie.

Keine Authentifizierung

Im Folgenden finden Sie ein Beispiel für eine API-Konfiguration für den Richtlinientyp `NoAuth`:

```
{

    "config_spec": {

        "api-resource-paths": {

            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": false,
            "put": false
         }
  ,
        "custom-rules": {
   }

      }
  ,
     "order_index": 4,
     "policy_name": "no_auth_policy",
     "policytype": "NoAuth"
  }
```

Bot

Im Folgenden finden Sie ein Beispiel für eine API-Konfiguration für den Richtlinientyp `Bot`:

```
{

```



```
    "config_spec": {

        "api-resource-paths": {

            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": false,
            "post": false,
            "put": false
         }
,
        "bot-prof-name": "apisec_test_profile",
        "custom-rules": {
 }

    }
,
    "order_index": 5,
    "policy_name": "bot_policy",
    "policytype": "Bot"
}
```

Weitere Informationen zu den einzelnen Attributen finden Sie unter Bot-Richtlinie.

WAF

Im Folgenden finden Sie ein Beispiel für eine API-Konfiguration für den WAF-Richtlinientyp:

```
{

    "config_spec": {

        "api-resource-paths": {

            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": false,
            "post": false,
            "put": false
         }
,
        "waf-prof-name": "apisec_waf_profile",
        "custom-rules": {
 }

    }
,
    "order_index": 6,
    "policy_name": "waf_policy",
    "policytype": "WAF"
```



```
23   }
```

Weitere Informationen zu den einzelnen Attributen finden Sie in der WAF-Richtlinie.

Header Rewrite

Im Folgenden finden Sie ein Beispiel für eine API-Konfiguration für den Richtlinientyp Header Rewrite. Geben Sie diese Konfiguration im `config_spec`-Objekt an:

```
{

    "policytype": "Header Rewrite",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
               "],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
         }
 ,
        "custom-rules": {
  }
 ,
        "rewrite-policy-header-field-name": "org",
        "rewrite-policy-header-field-val": "Citrix",
        "rewrite-policy-header-field-new-val": "Citrite"
     }
 ,
    "order_index": 7,
    "policy_name": "header_rewrite_pol"
 }
```

Weitere Informationen zu den einzelnen Attributen finden Sie unter Header Rewrite-Richtlinie.

URI Path Rewrite

Im Folgenden finden Sie ein Beispiel für eine API-Konfiguration für den Richtlinientyp URI Path Rewrite:

```
{

    "config_spec": {

        "api-resource-paths": {

```



```
            "endpoints": ["/store/order", "/store/inventory"],
            "delete": false,
            "get": true,
            "post": true,
            "patch": false,
            "put": false
         }
,
       "custom-rules": {

            "delete": false,
            "endpoints": [],
            "get": false,
            "post": false,
            "patch": false,
            "put": true
         }
,
       "path-rewrite-params": [
       {

            "insert-segment-position": "beginning",
            "new-path-value": "v3",
            "old-path-value": "v2",
            "action-type": "replace path segment"
         }
,
       {

            "insert-segment-position": "beginning",
            "new-path-value": "begin",
            "action-type": "insert path segment"
         }
,
       {

            "insert-segment-position": "end",
            "new-path-value": "end",
            "action-type": "insert path segment"
         }
,
       {

            "insert-segment-position": "before",
            "new-path-value": "before",
            "old-path-value": "store",
            "action-type": "insert path segment"
         }
,
       {

            "insert-segment-position": "after",
            "new-path-value": "after",
```



```
60              "old-path-value": "store",
61              "action-type": "insert path segment"
62           }
63
64           ]
65       }
66   ,
67           "order_index": 24,
68           "policy_name": "eats_uripathrewrite",
69           "policytype": "URI Path Rewrite ”
70   }
```

Weitere Informationen zu den einzelnen Attributen finden Sie unter URI Path Rewrite-Richtlinie.

Autorisierung

Im Folgenden finden Sie ein Beispiel für eine API-Konfiguration für den Richtlinientyp `Authorization`. Geben Sie die folgende Konfiguration im `config_spec`-Objekt an:

```
1  {
2
3      "policytype": "Authorization",
4      "config_spec": {
5
6          "api-resource-paths": {
7
8              "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                   "],
9              "get": true,
10             "post": true,
11             "put": false,
12             "delete": false
13          }
14   ,
15         "custom-rules": {
16    }
17   ,
18         "claims": [{
19
20             "name": "scope",
21             "values": ["value1", "value2"]
22          }
23   ]
24       }
25   ,
26      "order_index": 8,
27      "policy_name": "authorization"
28   }
```

Weitere Informationen zu den einzelnen Attributen finden Sie unter Autorisierungsrichtlinie.

Verweigern

Im Folgenden finden Sie ein Beispiel für eine API-Konfiguration für den Richtlinientyp `Deny`. Geben Sie die folgende Konfiguration im `config_spec`-Objekt an:

```
{

    "policytype": "Deny",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
         }
 ,
        "custom-rules": {
  }
 ,
        "api-denytype": "RESPONDWITH"
     }
 ,
    "order_index": 9,
    "policy_name": "deny_policy"
 }
```

In `api-denytype` können Sie einen der folgenden Werte angeben:

- RESPONDWITH
- RESET

Weitere Informationen zu den einzelnen Attributen finden Sie unter Regel ablehnen.

WAF- und BOT-Profile mit StyleBooks erstellen

January 26, 2024

Wenn Sie eine Richtlinie für eine API-Ressource in **API Gateway**auswählen können, können Sie die Kriterien zur Verkehrsauswahl definieren, um eine API-Anfrage zu authentifizieren. Außerdem können Sie API-Sicherheitsrichtlinien für den API-Datenverkehr konfigurieren. Weitere Informationen finden Sie unter API-Sicherheit.

Sie können WAF- und BOT-Richtlinien für eine API-Ressource konfigurieren. Bevor Sie eine Richtlinie

konfigurieren, stellen Sie sicher, dass Sie ihr Profil in NetScaler Console erstellen. Verwenden Sie die folgenden Standard-StyleBooks, um ein Profil zu erstellen:

- API WAF Erkennung StyleBook
- API BOT Erkennung StyleBook

WAF-Profil mit StyleBooks erstellen

Führen Sie Folgendes aus, um ein WAF-Profil zu erstellen:

1. Navigieren Sie in der NetScaler Console zu **Anwendungen** > **Konfigurationen** > **StyleBooks** . Suchen Sie nach dem StyleBook, indem Sie den Namen als eingeben `api-waf-profile`. Klicken Sie auf **Konfiguration erstellen**.

   Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

2. Geben Sie Werte für die folgenden Parameter an:

   - **API WAF-Profilname** - Ein Name zur Identifizierung eines WAF-Profils.
   - **Anwendungstyp** - Fügen Sie dem Profil Anwendungstypen hinzu. Das WAF-Profil unterstützt JSON- und XML-Anwendungstypen.

3. Optional: Aktivieren Sie **Sicherheitseinstellungen**, um HTTP-, JSON- oder XML-Schutzprüfungen anzugeben. Sie können auch eine Fehler-URL für die NetScaler Web App Firewall angeben. Weitere Informationen finden Sie unter Erstellen eines Web App Firewall-Profils.

4. Wählen Sie die NetScaler-Zielinstanz oder Instanzgruppe aus, auf der Sie diese Konfiguration bereitstellen möchten.

5. Klicken Sie auf **Erstellen**.

Informationen zum Konfigurieren einer WAF-Richtlinie finden Sie unter Hinzufügen von Richtlinien zu einer API-Bereitstellung.

Erstellen Sie ein BOT-Profil mit dem StyleBook

Führen Sie Folgendes aus, um ein BOT-Profil zu erstellen:

1. Navigieren Sie in der NetScaler Console zu **Anwendungen** > **Konfigurationen** > **StyleBooks** . Suchen Sie nach dem StyleBook, indem Sie den Namen als eingeben `api-bot-profile`. Klicken Sie auf **Konfiguration erstellen**.

   Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

2. Geben Sie in **BOT Profile Name**einen Namen zur Identifizierung eines BOT-Profils an.
3. Optional können Sie die folgenden Optionen basierend auf Ihren Anforderungen aktivieren:
    - **Überprüfung der IP-Reputation aktivieren** - Diese Option identifiziert die IP-Adresse, die unerwünschte Anfragen sendet. Sie können die IP-Reputationsliste verwenden, um Anforderungen vorbeugend abzulehnen, die von der IP mit der schlechten Reputation stammen.
    - **Aktivieren von BOT-Signaturen** - Geben Sie den Namen der BOT-Sig Es blockiert die Anfragen von der angegebenen Signatur.
    - **Liste zulassen** - Geben Sie die IPv4- oder Subnetzadresse (CIDR) an. Diese Option ermöglicht es dem BOT-Profil, Anfragen von der angegebenen IPv4- oder Subnetzadresse zu Bypass.
    - **Liste ablehnen** - Geben Sie die IPv4- oder Subnetzadresse (CIDR) an. Diese Option ermöglicht es dem BOT-Profil, Anfragen von der angegebenen IPv4- oder Subnetzadresse zu blockieren.
4. Wählen Sie die NetScaler-Zielinstanz oder Instanzgruppe aus, auf der Sie diese Konfiguration bereitstellen möchten.
5. Klicken Sie auf **Erstellen**.

Informationen zum Konfigurieren einer BOT-Richtlinie finden Sie unter Hinzufügen von Richtlinien zu einer API-Bereitstellung.

Anwendungen

April 10, 2024

Mit der Anwendungsanalyse- und Verwaltungsfunktion der NetScaler Console können Sie die Anwendungen mithilfe eines anwendungsorientierten Ansatzes überwachen. Dieser Ansatz hilft Ihnen dabei:

- Score überprüfen und Gesamtleistung der Anwendungen analysieren
- Nach weiteren Problemen mit Server oder Client suchen
- Anomalien in den Datenverkehrsströmen der Anwendung erkennen und Korrekturmaßnahmen ergreifen

> **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 der NetScaler Console hinzugefügt haben.
- Stellen Sie sicher, dass Sie über eine gültige Lizenz für Ihre NetScaler-Instanzen verfügen. Weitere Informationen finden Sie unter Lizenzierung.

Anwendungsüberblick

Anwendungen können sein:

- Diskrete Anwendungen
- Benutzerdefinierte Anwendungen
- Microservices-Anwendungen (k8s_discrete)

Diskrete Anwendungen

Alle virtuellen Server, die in NetScaler Console erkannt werden, werden als separate 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 NetScaler-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.

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

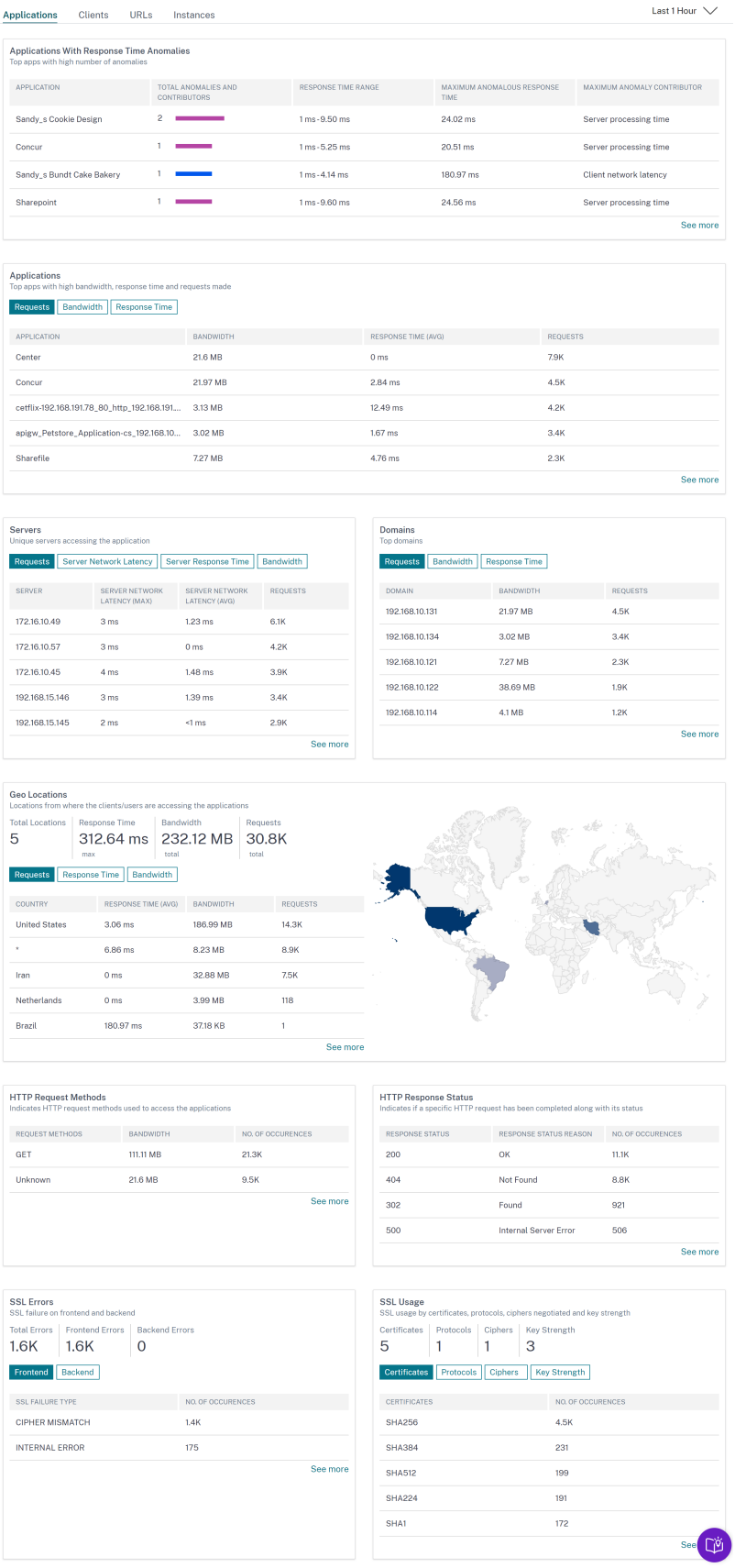
January 26, 2024

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	Clients	URLs	Instanzen
Anwendung mit Anomalien der Reaktionszeit	Clients	URLs	Instanzmetriken
Anwendungen	Geo Standorte		Anwendungen
Server	HTTP-Anforderungsmethoden		Domänen
Domänen	HTTP-Antwortstatus		URLs

Anwendungen	Clients	URLs	Instanzen
Geo Standorte	URLs		HTTP-Anforderungsmethoden
URLs	Betriebssystem		HTTP-Antwortstatus
HTTP-Anforderungsmethoden	Browser		Clients
HTTP-Antwortstatus	SSL-Fehler		Server
SSL-Fehler	SSL-Nutzung		Betriebssystem
SSL-Nutzung			Browser



In jeder Metrik können Sie die Top-5-Ergebnisse anzeigen. Sie können klicken, um weitere Drilldowns durchzuführen, um das Problem zu analysieren und schneller Fehlerbehebungsmaßnahmen durchzuführen.

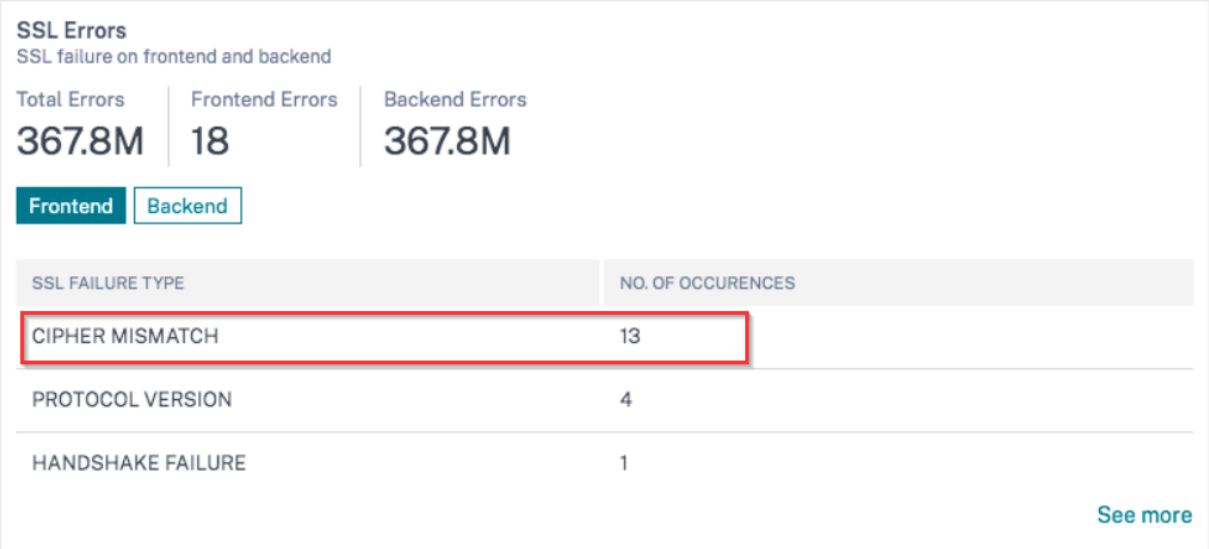
> **Hinweis**
>
> - Ab Version **14.1-1.16** oder einer späteren Version werden beim Drilldown einer Metrik in der Analyseansicht im Zeitreihendiagramm Nullwerte (z. B. 0 ms und 0 Anfrage) für die gewählte Dauer angezeigt. Wenn früher für die gewählte Dauer kein Traffic oder keine Transaktion einging, 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 Console die RTT-Werte wie folgt an:
>
>   - **NA**—Wird angezeigt, wenn die NetScaler-Instanz den RTT nicht berechnen kann.
>   - **< 1 ms**—Wird angezeigt, wenn die NetScaler-Instanz den RTT in Dezimalzahlen zwischen 0 ms und 1 ms berechnet. Zum Beispiel 0,22 ms.

Details zu Problemen im Zusammenhang mit der Verschlüsselung anzeigen

Unter **SSL-Fehler**können Sie Details für die folgenden SSL-Parameter anzeigen:

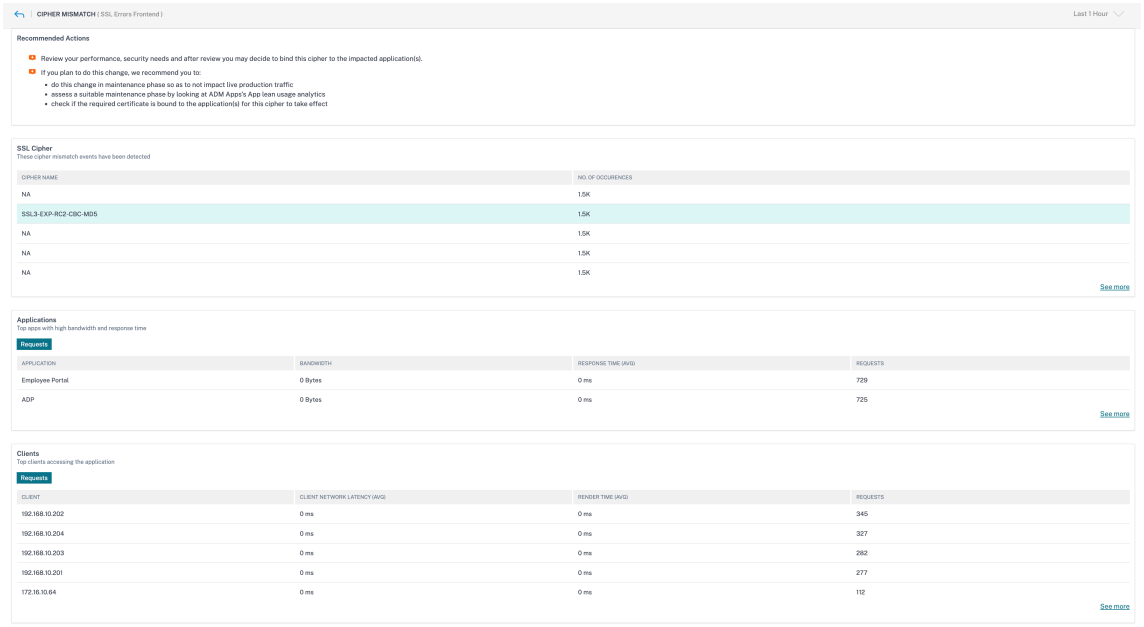
- Nichtübereinstimmung der Verschlüsselung
- Nicht unterstützte Chiffren

Klicken Sie unter **SSL-Fehler**auf einen SSL-Parameter (Cipher Mismatch oder Unsupported Ciphers), um Details wie den SSL-Verschlüsselungsnamen, die empfohlenen Aktionen und die Details der betroffenen Anwendungen und Clients anzuzeigen.

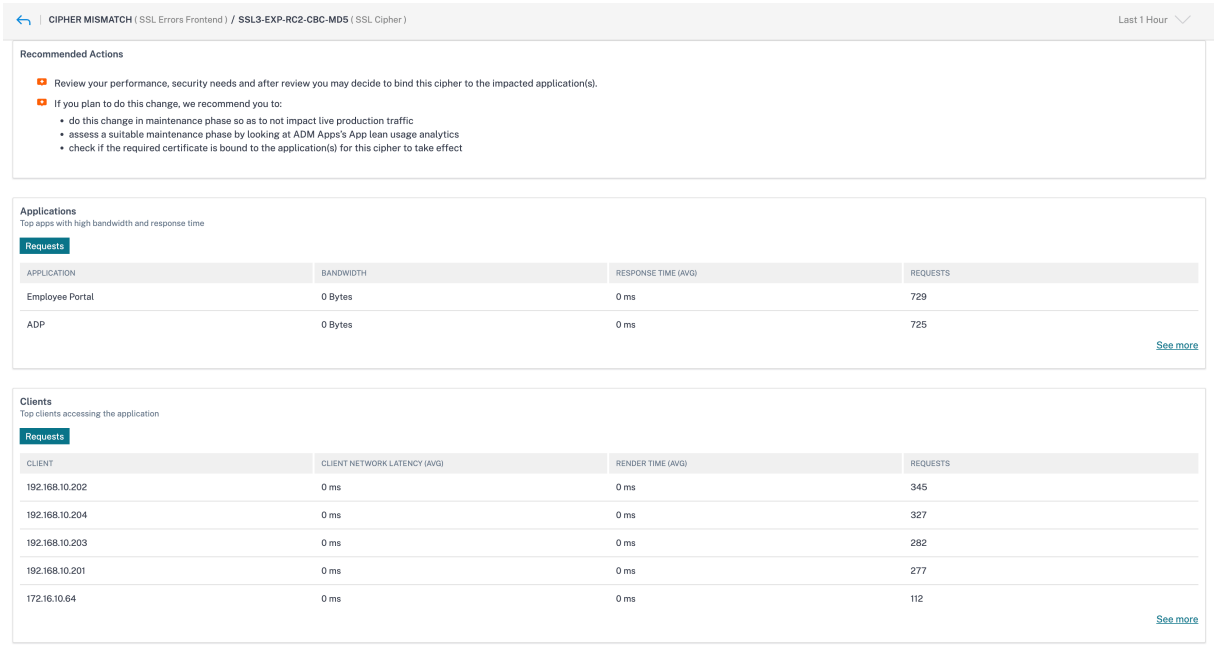


Die Detailseite wird für den ausgewählten SSL-Parameter angezeigt. Sie haben folgende Möglichkeiten:

- Lesen Sie die in den **empfohlenen Maßnahmen enthaltenen Vorschläge durch**.
- Zeigen Sie die Verschlüsselungsnamen und die Anzahl der Vorkommen unter **SSL Cipher an**.
- Zeigen Sie die Gesamtzahl der betroffenen Anwendungen und Clients an.



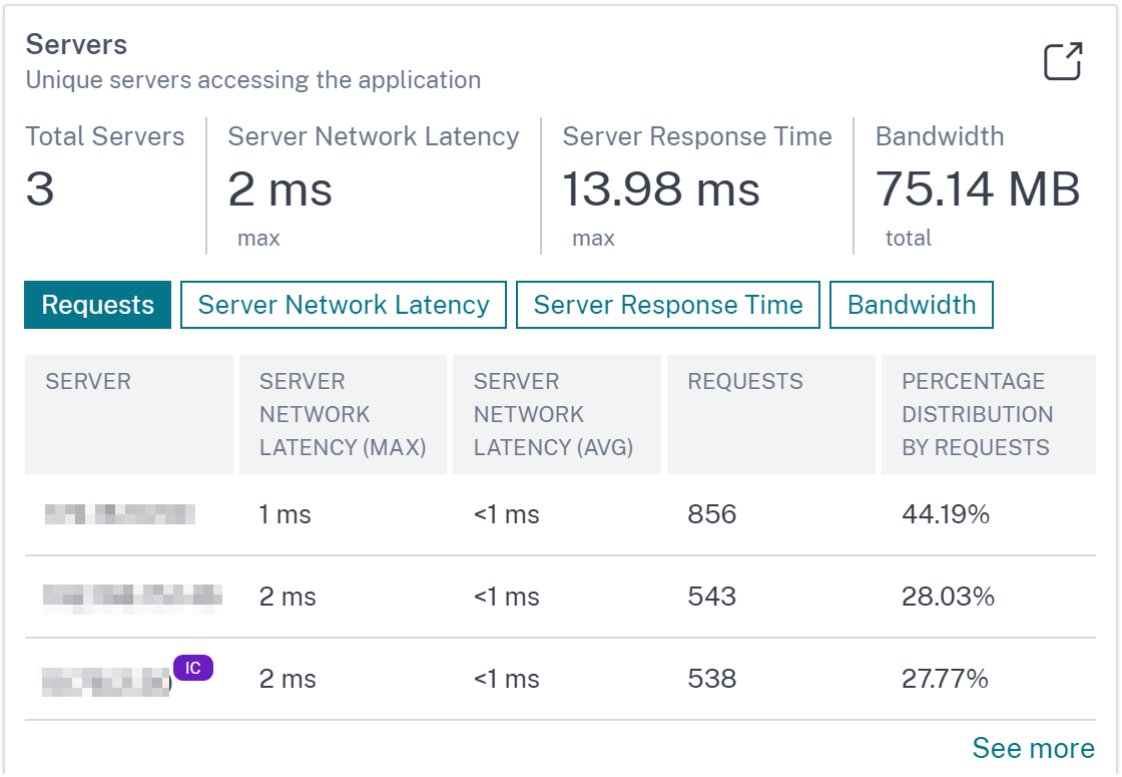
Klicken Sie auf den **Namen der SSL-Verschlüsselung**, um die Anwendungen und Clients anzuzeigen, die von der ausgewählten SSL-Verschlüsselung betroffen sind.



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.

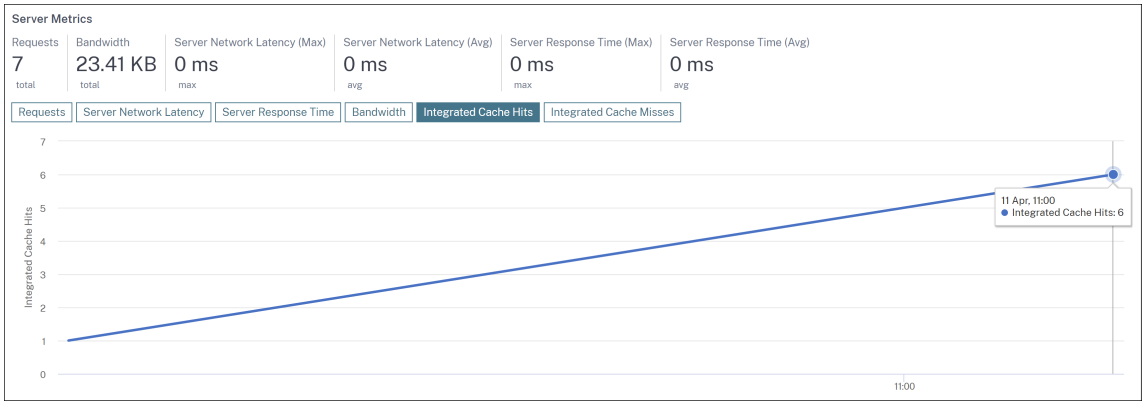
Die Integrationscache-Anforderungen sind derzeit unter Server mit einer IC-Benachrichtigung neben der IP-Adresse des virtuellen NetScaler-**Servers** sichtbar. Alle anderen Anfragen sind mit der IP-Adresse des Ursprungsservers sichtbar.



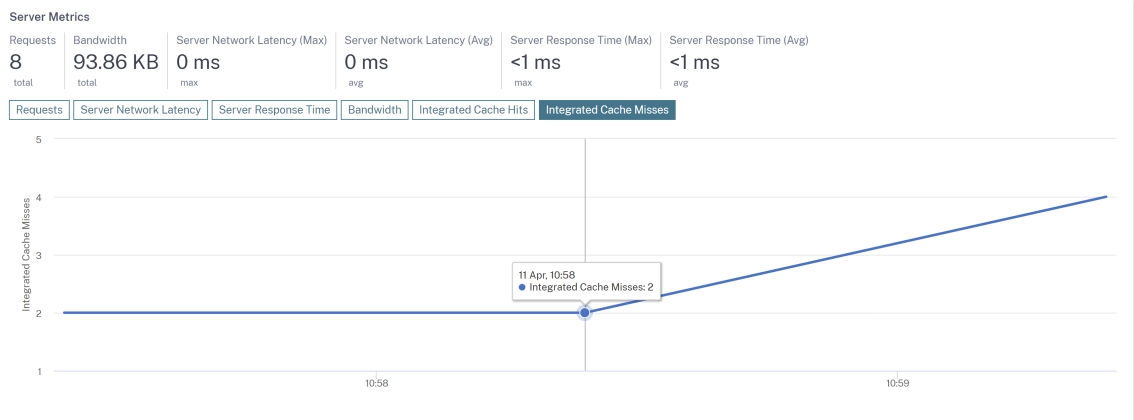
Wenn Sie einen Server aufschlüsseln, um weitere Details anzuzeigen, werden in den **Servermetriken** die Registerkarten „Treffer“und „Fehlschläge“im integrierten Cache angezeigt.

Die Diagrammansicht in:

- Auf der Registerkarte **Integrated Cache Hits** können Sie die gesamten Antworten anzeigen, die die NetScaler Appliance aus dem Cache bereitstellt.



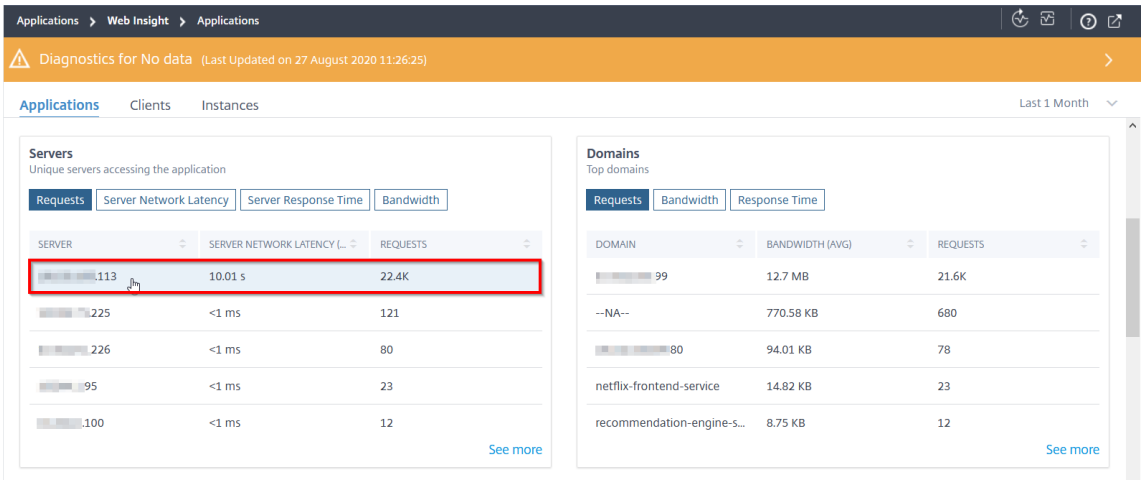
- Auf der Registerkarte **Integrated Cache** Misses können Sie die gesamten Antworten anzeigen, die die NetScaler Appliance vom Originalserver bereitstellt.



Anderer Anwendungsfall

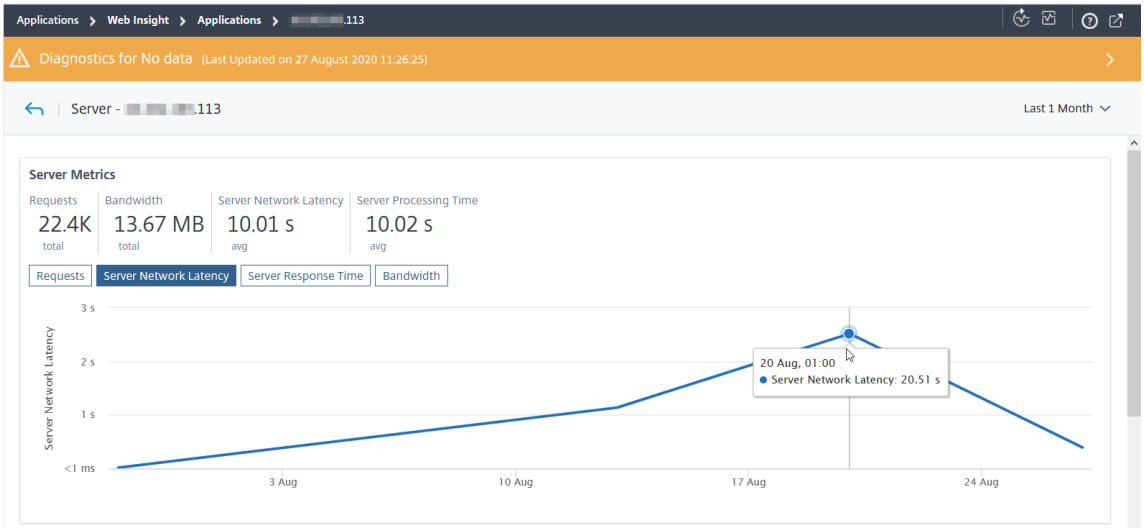
Bedenken Sie, dass Sie die Latenz des Servernetzwerks für einen Zeitraum von einem Monat analysieren und entscheiden möchten, ob Sie die Produktionsumgebung nach oben oder unten skalieren möchten. Um dies zu analysieren:

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 die Entscheidung treffen, die Produktionsumgebung zu skalieren.

Ursache für die Langsamkeit der Anwendung analysieren

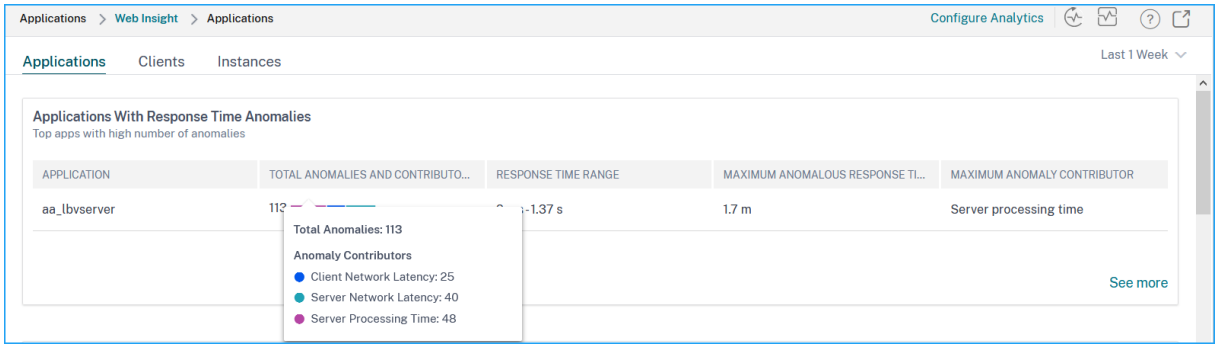
January 26, 2024

Anwendungsverlangsamung ist ein wichtiges Anliegen für jede Organisation, da dies zu geschäftlichen Auswirkungen oder Produktivität führt. Als Administrator müssen Sie sicherstellen, dass alle Anwendungen optimal funktionieren, um geschäftliche Auswirkungen zu vermeiden. Wenn Ihre Benutzer eine langsame Zugriffsart auf die Anwendung haben, müssen Sie sicherstellen, dass das Problem bei folgenden Problemen liegt:

- Netzwerklatenz des Clients
- Servernetzwerklatenz
- Verarbeitungszeit des Servers

NetScaler Console führt jede Stunde Anomalieprüfungen durch und meldet Anomalien für den Datenverkehr der letzten 1 Stunde, sofern bestimmte Voraussetzungen erfüllt sind. Um beispielsweise falsch positive Ergebnisse zu vermeiden, werden die Anomalieprüfungen für diese Ergebnisse übersprungen, wenn die Reaktionszeit < 1 ms beträgt.

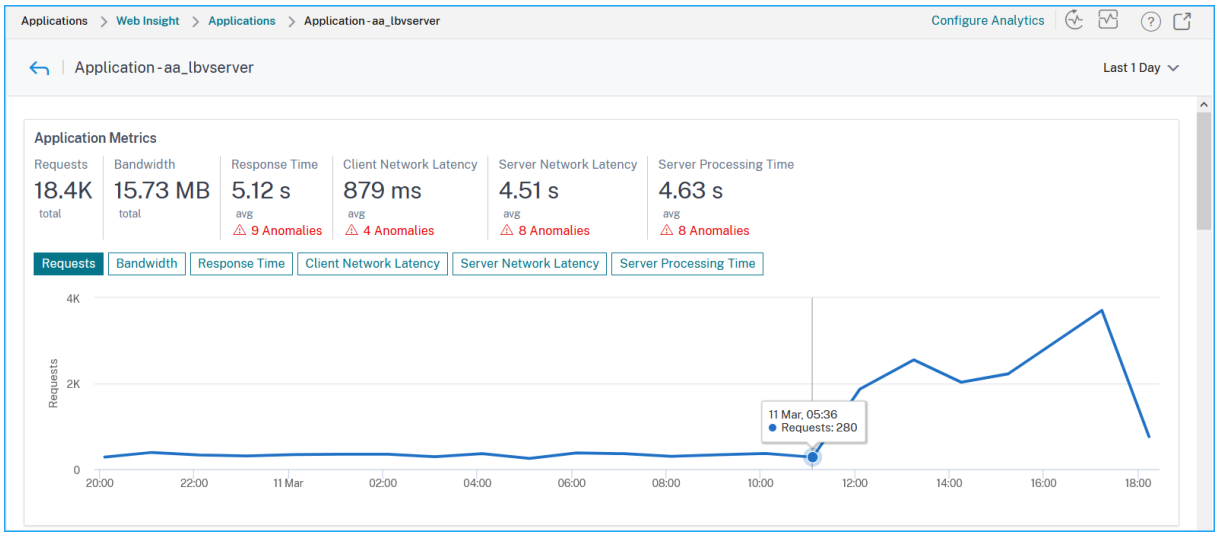
Auf der Seite "**Anwendungen > Web Insight** "können Sie die Anwendungen mit Anomalien der Reaktionszeit für die ausgewählte Dauer anzeigen. Die Metrik "**Anwendungen mit Antwortanomalien** "zeigt die fünf wichtigsten Anwendungen basierend auf den gesamten Anomalien an. Klicken Sie auf **Mehr** anzeigen, 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.



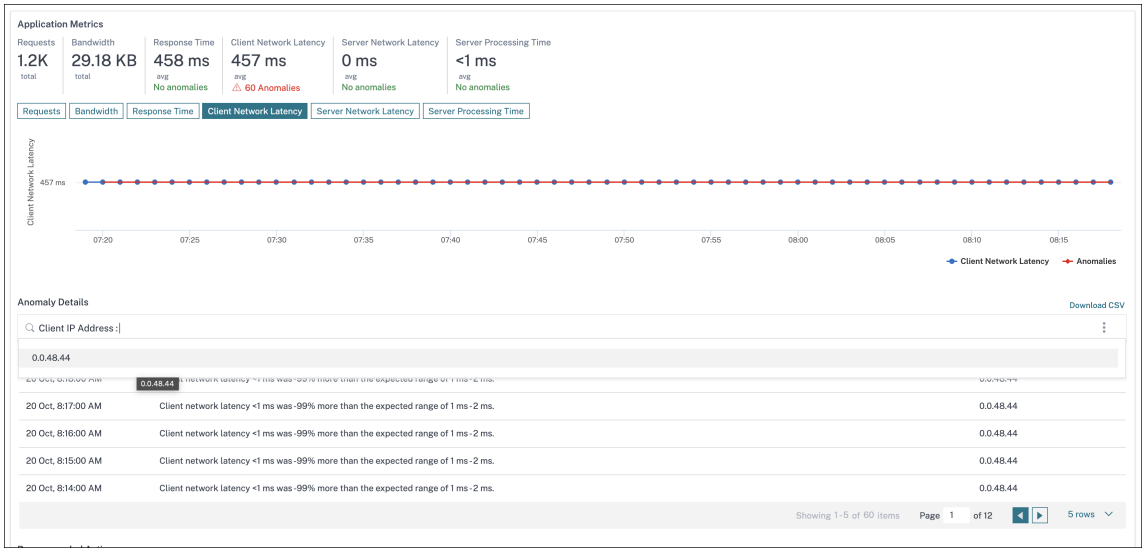
Mit den **Anwendungsmetriken** können Sie Folgendes anzeigen:

- **Zusammenfassung** —Eine Übersicht zur Visualisierung der Anwendungsleistung wie Reaktionszeit, Anfragen und Bandbreite
- **Anfragen** —Die Gesamtzahl der von der Anwendung eingegangenen Anfragen. Sie können sich auch die Anfragen der fünf wichtigsten Clients ansehen, basierend auf der Gesamtzahl der Anfragen
- **Bandbreite** —Die gesamte Bandbreite, die von der Anwendung verarbeitet wird. Sie können sich auch den Bandbreitenverbrauch der fünf wichtigsten Server auf der Grundlage des gesamten Bandbreitenverbrauchs anzeigen lassen.
- **Reaktionszeit** —Eine Übersicht zur Visualisierung der Client-Netzwerklatenz, der Servernetzwerklatenz und der Serververarbeitungszeit in derselben Grafik
- **Client-Netzwerklatenz**—Die durchschnittliche Client-Netzwerklatenz (vom Client bis NetScaler)
- **Servernetzwerklatenz —Die durchschnittliche Servernetzwerklatenz (von NetScaler zum Server**)
- **Serververarbeitungszeit —Die durchschnittliche Serververarbeitungszeit (vom Server zu NetScaler**)

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.

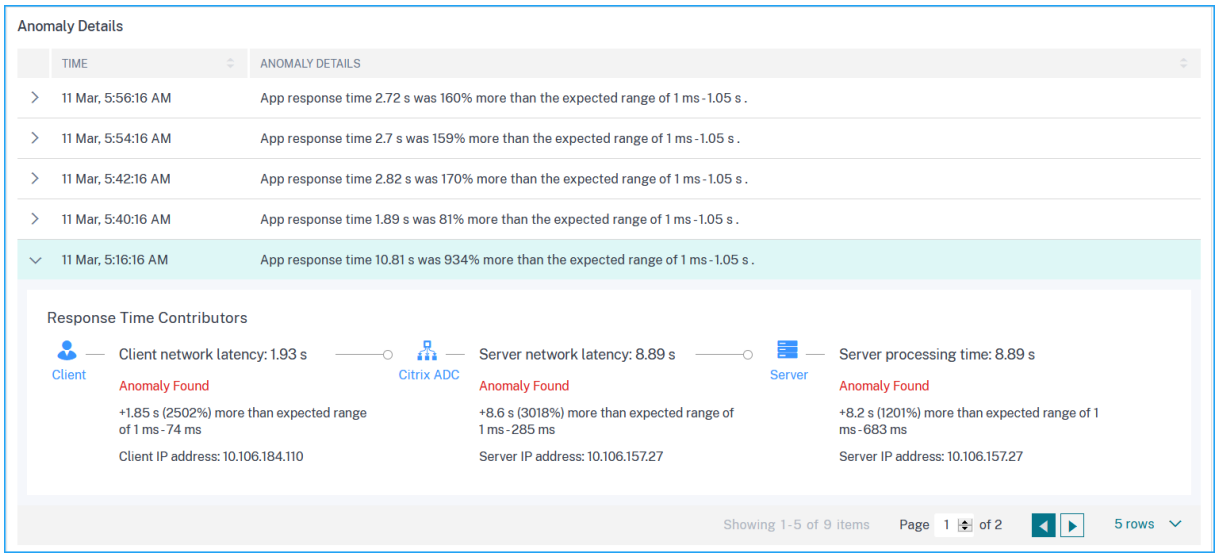
Auf den Registerkarten **Client-Netzwerklatenz** und **Server-Netzwerklatenz** können Sie Folgendes anzeigen:

- **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.

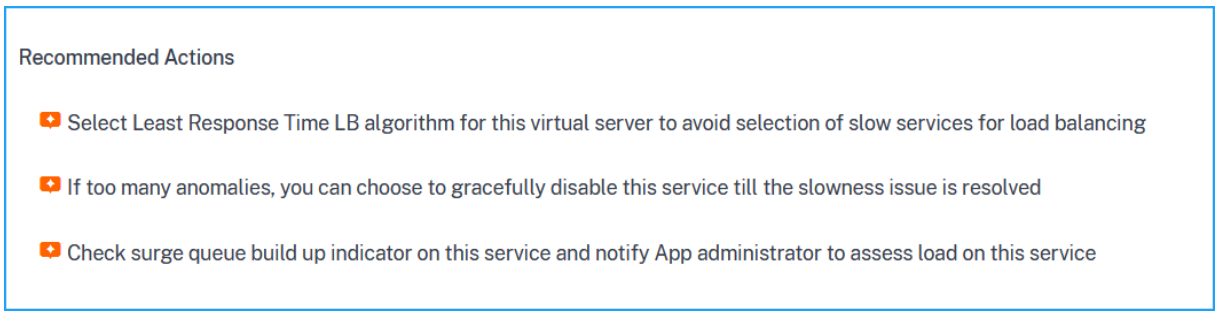


Reaktionszeit

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.



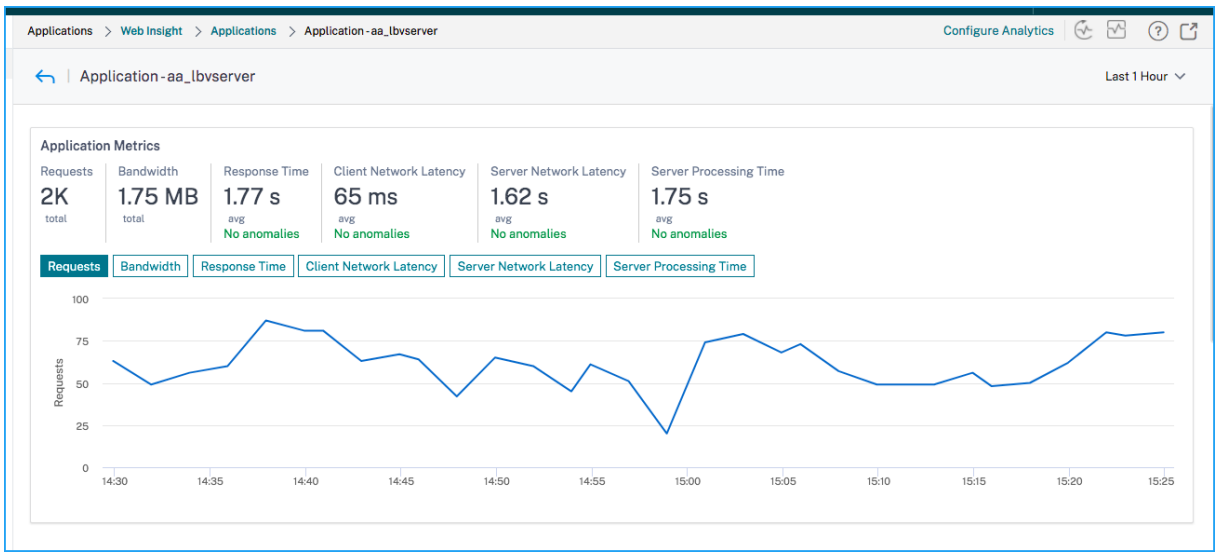
Die **empfohlenen Maßnahmen** schlagen Ihnen die möglichen Lösungen für die Anomalien vor.



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

March 12, 2024

Mit der Service Graph-Funktion in NetScaler Console können Sie alle Kubernetes-Dienste in einer grafischen Darstellung überwachen. Mit dieser Funktion können Sie auch eine detaillierte Analyse und umsetzbare Metriken der Services anzeigen. Navigieren Sie zu **Anwendungen > Servicegrafik**, um das Service-Diagramm anzuzeigen für:

- Für alle 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 **Applications > Service Graph** und klicken Sie auf die Registerkarte **Microservices**, um:

- 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
- Anzeigen von Client-Metriken und zusammenfassenden Kundentransaktionen

Durch die Visualisierung dieser Metriken in NetScaler Console können Sie die Ursache von Problemen analysieren und die erforderlichen Maßnahmen zur Problembehandlung schneller ergreifen. 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 Server für Rechenzentren, NetScaler-Instanzen, CS und LB 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, z. B. **Kritisch**, **Überprüfung** und **Gut**. NetScaler Console zeigt den Dienststatus basierend auf der Antwortzeit des Dienstes und der Fehleranzahl an.
  - **Kritisch (rot)** —Zeigt an, wenn die durchschnittliche Reaktionszeit des Service > 200 ms UND Fehlerzahl > 0
  - **Überprüfung (orange)** —Zeigt an, wenn die durchschnittliche Reaktionszeit des Service > 200 ms ODER Fehlerzahl > 0
  - **Gut (grün)** —Zeigt keinen Fehler an und durchschnittliche Reaktionszeit < 200 ms
- Der Clientstatus, z. B. **Kritisch**, **Überprüfung** und **Gut**. NetScaler Console zeigt den Clientstatus auf der Grundlage der Client-Netzwerklatenz 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 Fehlerzahl > 0
  - **Gut (grün)** —Zeigt keinen Fehler an und durchschnittliche Latenz des Client-Netzwerks < 200 ms
- Der Status des virtuellen Servers, z. B. **Kritisch**, **Überprüfung** und **Gut**. NetScaler Console zeigt den Status des virtuellen Servers auf der Grundlage der App-Punktzahl 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 beachtende 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

January 26, 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.

Mit einem StyleBook können Sie:

- Konfigurieren Sie eine bestimmte Funktion von NetScaler.
- Erstellen Sie Konfigurationen für die Bereitstellung von Unternehmensanwendungen wie Microsoft Exchange oder Lync.

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 darauf konzentrieren, das Ergebnis oder den „gewünschten Zustand“der Konfiguration zu beschreiben, anstatt Schritt für Schritt zu erklären, wie Sie dies auf einer bestimmten NetScaler-Instanz erreichen. NetScaler Console 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 ist, können die Komponenten eines StyleBook in beliebiger Reihenfolge angegeben werden, und NetScaler Console bestimmt die richtige Reihenfolge anhand ihrer 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 Konfigurationsmuster 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 einer oder mehreren NetScaler-Instanzen bereitgestellt und auch zwischen Instanzen verschoben werden.
- ** Automatisch generierte Benutzeroberfläche : NetScaler Console generiert automatisch Benutzeroberflächenformulare, die zum Ausfüllen der StyleBook-Parameter verwendet werden, wenn die Konfiguration über die NetScaler Console-GUI erfolgt. StyleBook-Autoren müssen keine neue GUI-Sprache erlernen oder Benutzeroberflächenseiten und -formulare separat erstellen.
- **API-gesteuert**: Alle Konfigurationsvorgänge werden mithilfe der NetScaler Console-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 andere Konfiguration mit unterschiedlichen Werten zu erstellen und sie auf derselben oder einer anderen Instanz auszuführen. Für diese Konfiguration wird ein neues Konfigurationspaket erstellt. Ein Config Pack wird sowohl auf der NetScaler Console als auch auf der NetScaler-Instanz gespeichert, auf der die Konfiguration ausgeführt wird.

Sie können entweder Standard-StyleBooks verwenden, die mit NetScaler Console geliefert werden, um Konfigurationen für Ihre Bereitstellung zu erstellen, oder Ihre eigenen StyleBooks entwerfen und sie in NetScaler Console importieren. Sie können die StyleBooks verwenden, um Konfigurationen entweder mithilfe der NetScaler Console-GUI oder mithilfe von APIs zu erstellen.

Dieses Dokument enthält die folgenden Abschnitte:

- So zeigen Sie StyleBooks an

- Standard-StyleBooks
- Für Geschäftsanwendungen entwickelte Stylebooks
- Benutzerdefinierte StyleBooks
- APIs in StyleBooks
- StyleBooks Grammatik

Anwendungssicherheitsdashboard

March 12, 2024

Das **App Security** Dashboard bietet Ihnen einen Überblick über die Sicherheitsmetriken für die erkannten Anwendungen. Dieses Dashboard zeigt die Informationen zu Sicherheitsangriffen für die erkannten Anwendungen an, z. B. Sync-Angriffe, Small Window-Angriffe und DNS-Flood-Angriffe.

So zeigen Sie die Sicherheitsmetriken im App-Sicherheitsdashboard an:

1. Navigieren Sie zu **Security > Security 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.

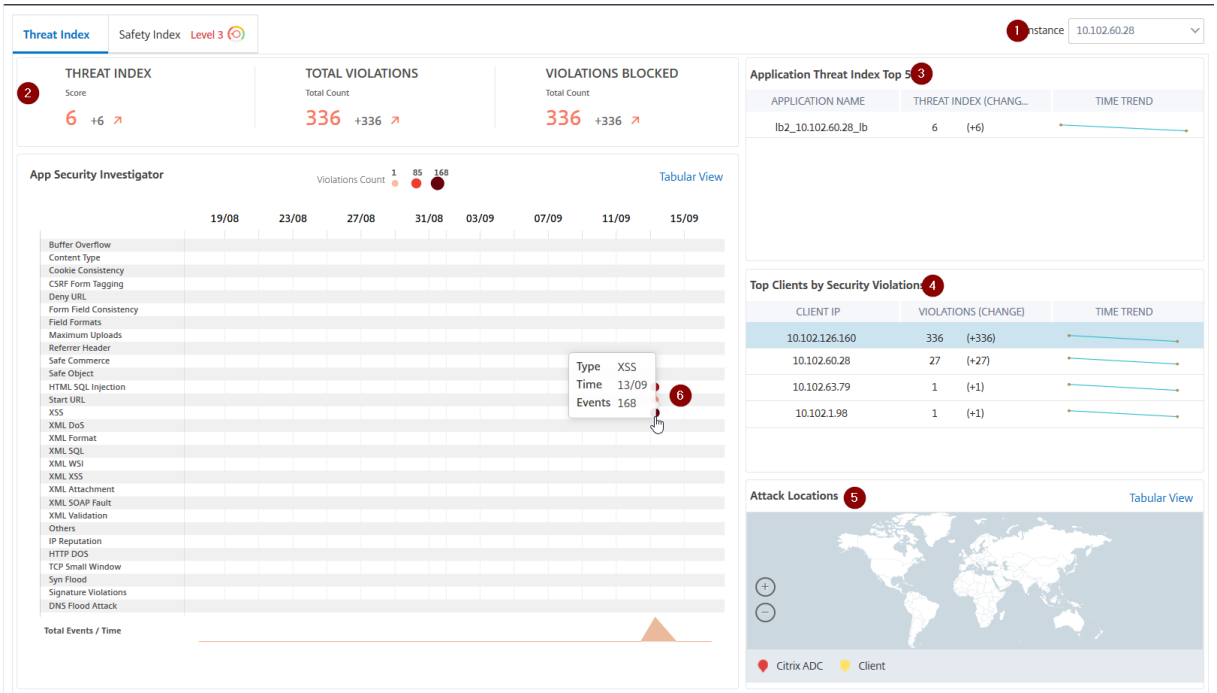
     Der Bedrohungsindex basiert auf Angriffsinformationen. Die angriffsbezogenen Informationen wie Verstoßtyp, Angriffskategorie, Standort und Client-Details geben einen Einblick in die Angriffe auf die Anwendung. Informationen zu Verstößen werden nur dann an NetScaler Console gesendet, wenn es zu einer Verletzung oder einem Angriff kommt. Viele Verstöße und Schwachstellen führen 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 Überprüfungen der Anwendungs-Firewall durchgeführt werden, aber keine Sicherheitsmaßnahmen für das NetScaler-System bereitgestellt werden, z. B. ein sicheres Kennwort für den nsroot-Benutzer, wird Anwendungen ein niedriger Sicherheitsindexwert zugewiesen.

Sie können die im **App Security Investigator**gemeldeten Unstimmigkeiten anzeigen.

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.

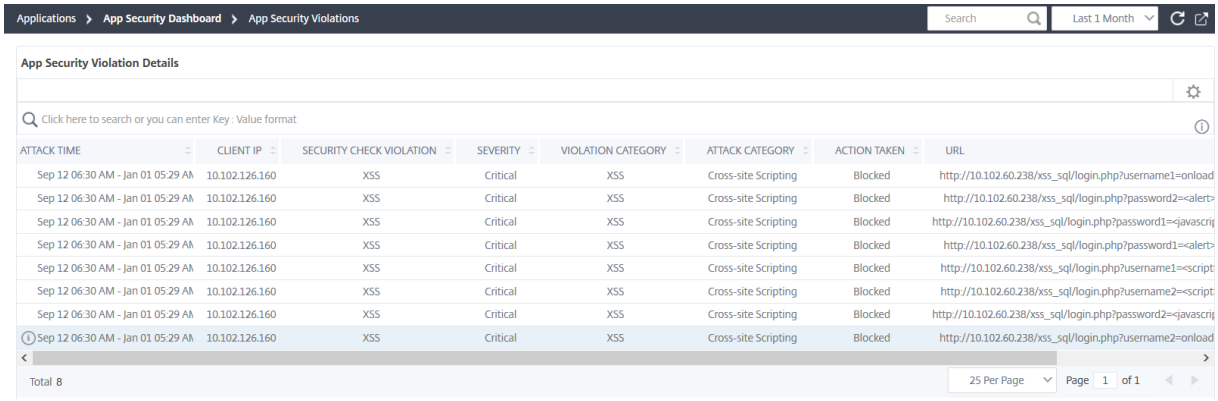
4 - Zeigt die Sicherheitsverletzungen basierend auf Clients an. Das Diagramm App Security Investigator wird für jeden Client angezeigt. Sie können auf jede Client-IP klicken, um Ergebnisse anzuzeigen.

5 - Zeigt die Verstöße in Kartenansicht und Tabellenansicht an.

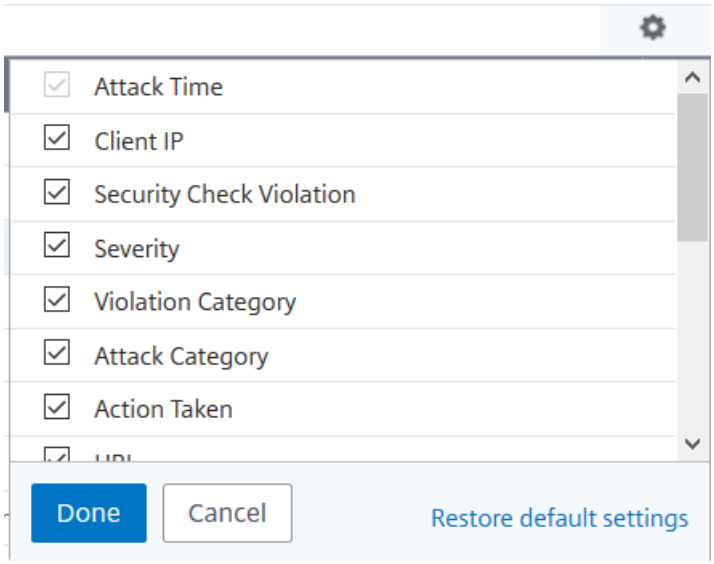
6 - Zeigt die Details des Verstoßes an. Wenn Sie den Mauszeiger auf das Diagramm bewegen, werden die Details wie Verletzungstyp, Zeitpunkt des Angriffs und Gesamtereignisse angezeigt.

Wenn Sie auf ein Blasendiagramm klicken, werden die Details auf der Seite **Details zu App-Sicherheitsverletzungen** angezeigt. Wenn Sie beispielsweise weitere Details für eine siteübergreifende Skriptverletzung anzeigen möchten, klicken Sie in **App Security Investigator** auf das Diagramm, das für **XSS**ausgefüllt wurde.

Die **Details zu App-Sicherheitsverletzungen** werden mit Verstoßdetails wie Angriffszeit, Angriffskategorie, Schweregrad, URL usw. angezeigt.



Sie können auch auf die Option **Einstellungen** klicken, um die Optionen auszuwählen, die angezeigt werden sollen.



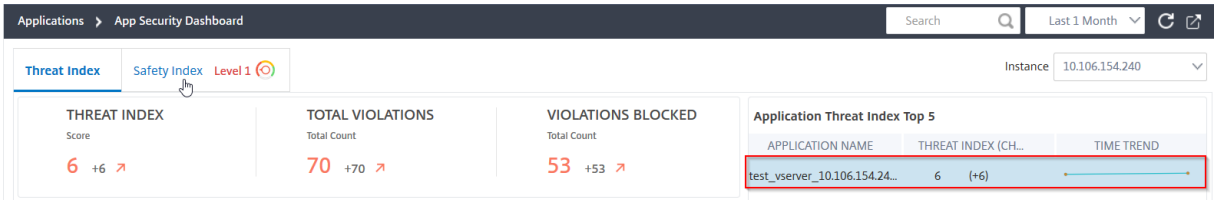
Sicherheitsindex Details

Nachdem Sie die Bedrohungsgefahr einer Anwendung überprüft haben, möchten Sie ermitteln, welche Anwendungssicherheitskonfigurationen vorhanden sind und welche Konfigurationen für diese Anwendung fehlen. Sie können diese Informationen erhalten, indem Sie einen Drilldown in die Zusammenfassung des Anwendungssicherheitsindex durchführen.

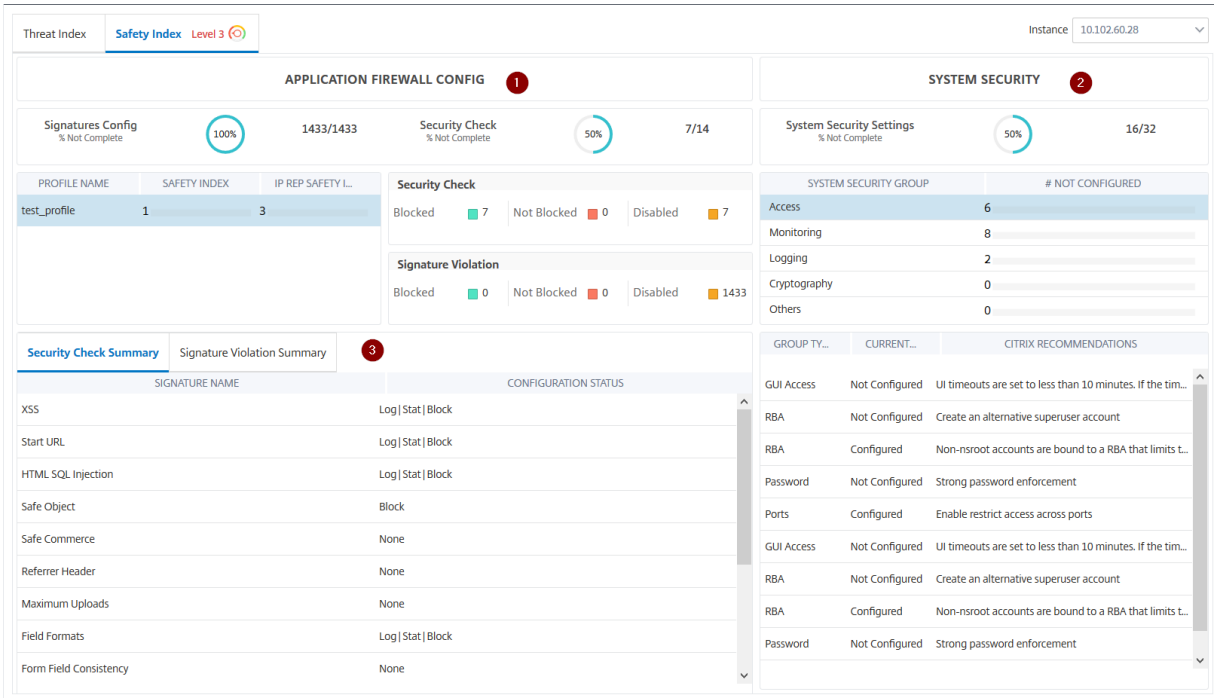
Die Zusammenfassung des Sicherheitsindex gibt Ihnen Informationen über die Wirksamkeit der folgenden Sicherheitskonfigurationen:

- **Konfiguration der Anwendungsfirewall**. Zeigt an, wie viele Signatur- und Sicherheitseinheiten nicht konfiguriert sind.
- **NetScaler Console System Security**. Zeigt an, wie viele Systemsicherheitseinstellungen nicht konfiguriert sind.

Um die Details des **Sicherheitsindex** anzuzeigen, wählen Sie einen virtuellen Server/eine Anwendung aus, und klicken Sie auf die Registerkarte **Sicherheitsindex**.



Die Details werden angezeigt.



1 - Zeigt die detaillierten Informationen für Anwendungs-Firewall-Konfigurationen an.

2 - Zeigt die detaillierten Informationen für Systemsicherheit an. Klicken Sie auf jede Sicherheitsgruppe, um Details zum Status und zu Citrix Empfehlungen zu erhalten.

3 - Zeigt die Zusammenfassung für Sicherheitsprüfung und Signaturverletzung an.

Sie können auch eine Zusammenfassung der Bedrohungsumgebung anzeigen, indem Sie die Sicherheitsinformationen für virtuelle Server aktivieren und dann zu **Sicherheit > Sicherheitsverletzungen**navigieren. Weitere Informationen zum Anwendungsfall des Sicherheitsindex finden Sie unter Sicherheitseinblick.

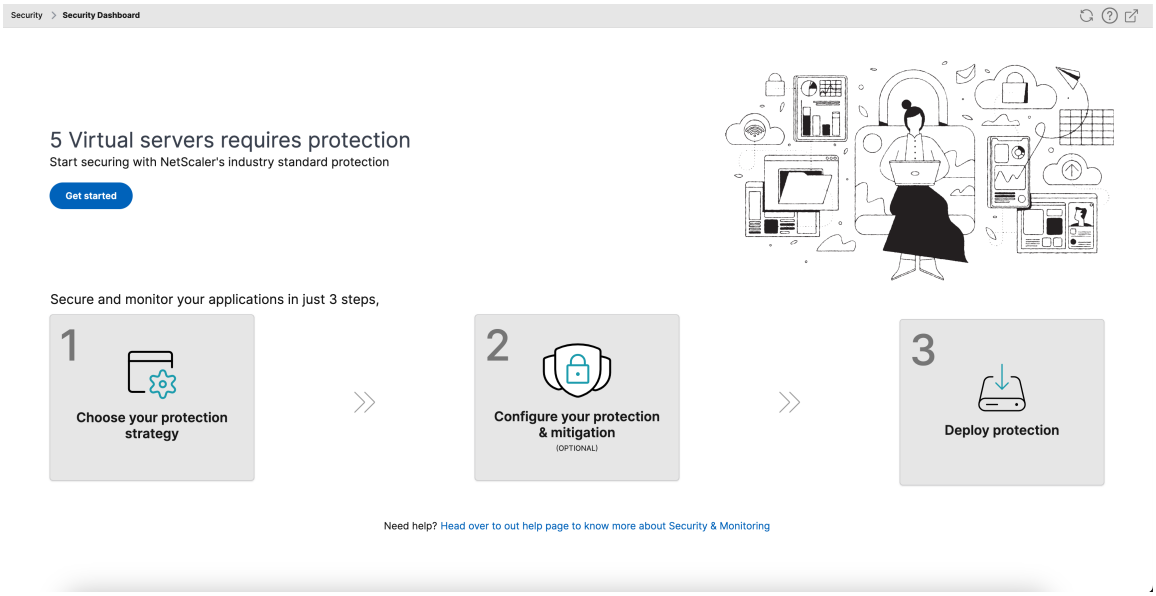
Einheitliches Sicherheitsdashboard

March 12, 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.



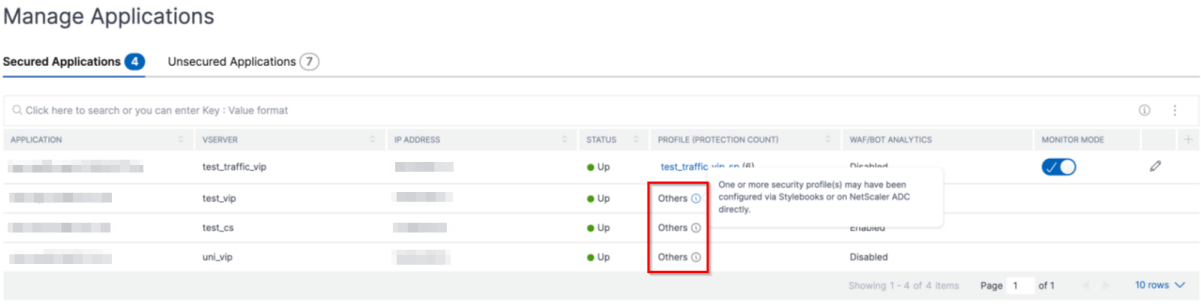
- Sie können die Gesamtzahl der virtuellen Server anzeigen, die geschützt werden müssen. Klicken Sie auf **Erste Schritte**, um Details in **Unsecured Applications**anzuzeigen.
- Die für die Konfiguration von Schutzmaßnahmen in Frage kommenden virtuellen Servertypen sind Load Balancing und Content Switching.

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**

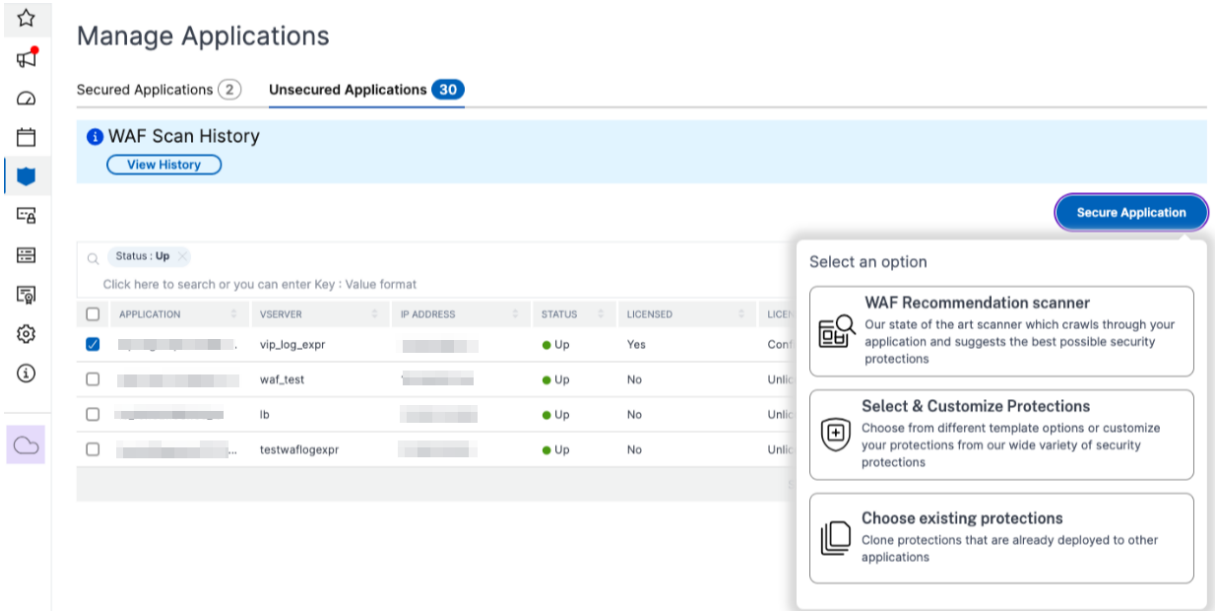
anzeigen, die unter **Profil** als **Andere** markiert sind.



Schutzmaßnahmen für ungesicherte Anwendungen konfigurieren

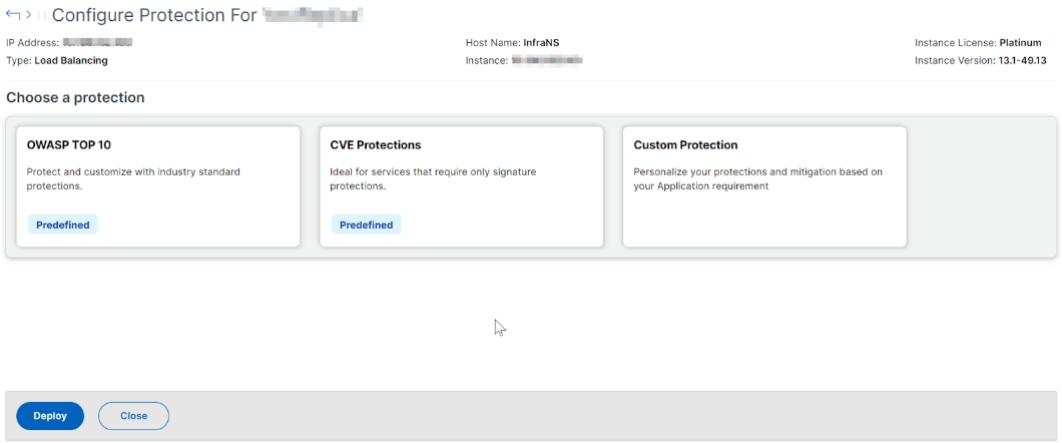
> **Hinweis:**
>
> Die maximale Anzahl unterstützter Konfigurationsentitäten (Regeln) in der Blockliste ist 32.

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:

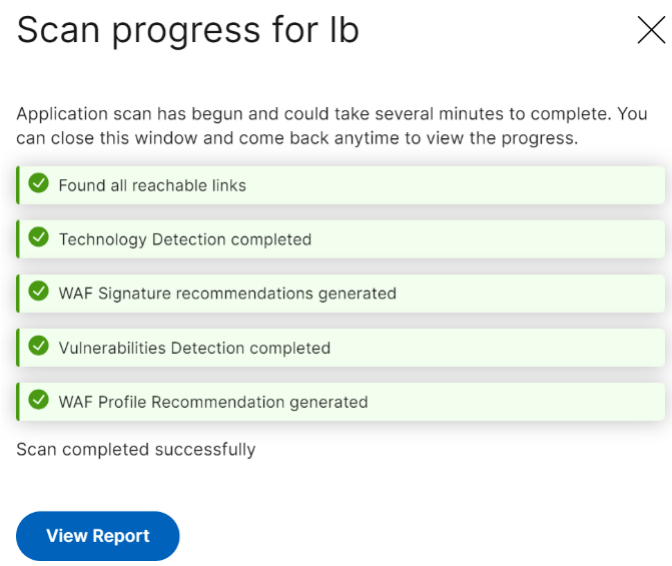
1. Unter **Scanparameter**:
    - **Domain name** —Geben Sie eine gültige, zugängliche IP-Adresse oder den öffentlich erreichbaren Domänennamen an, der der Anwendung zugeordnet ist. Beispiel: `www.example.com`.
    - **HTTP-/HTTPS-Protokoll** —Wählen Sie das Protokoll der Anwendung aus.
    - **Traffic 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 auf die private IP-Adresse von der NetScaler Console-Verwaltungs-IP aus zugegriffen werden kann.
    - **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`.

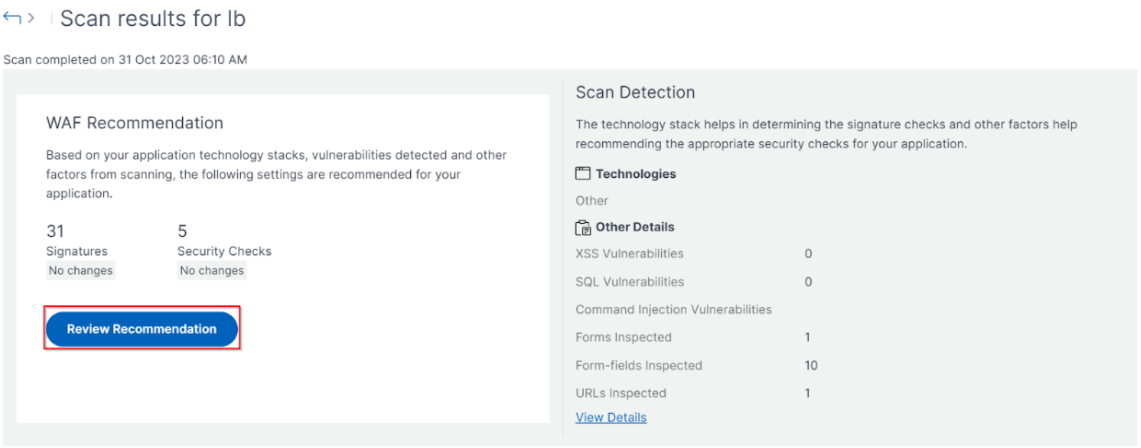
2. Unter **Scankonfigurationen**:

   - **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.

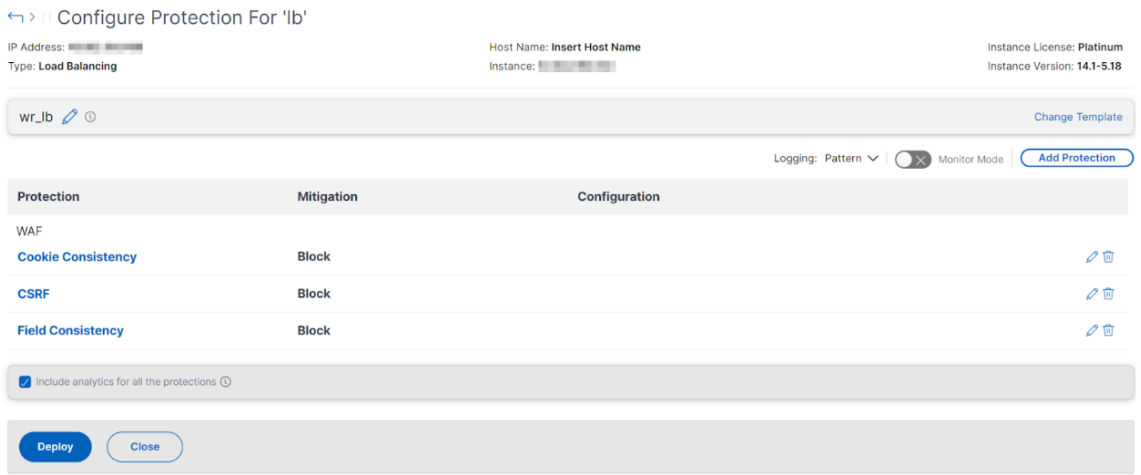
3. Die Konfiguration der WAF-Scaneinstellungen ist abgeschlossen. Sie können auf **Scan starten** klicken, um den Scanvorgang zu starten, und warten, bis der Vorgang abgeschlossen ist. Nachdem der Scan abgeschlossen ist, klicken Sie auf **Bericht anzeigen**.



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**.

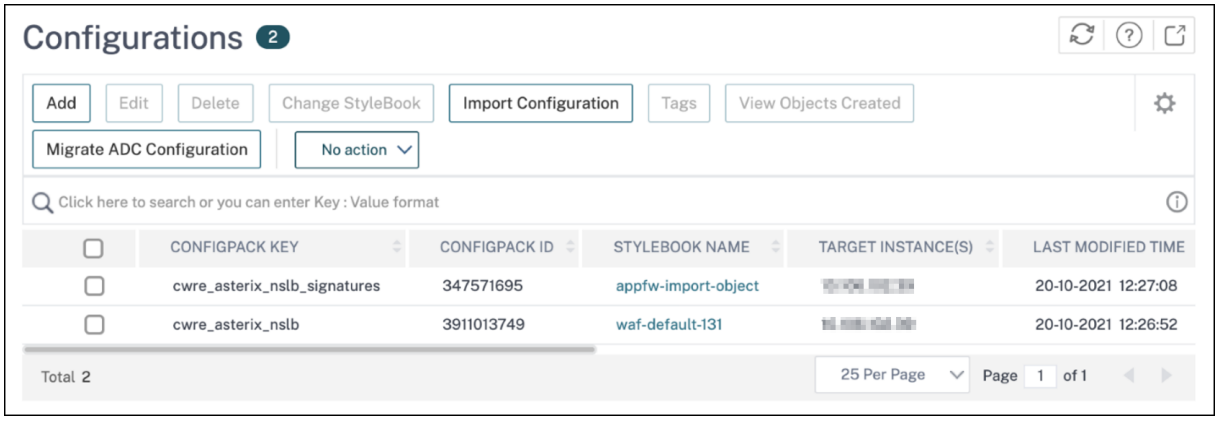


Wenn Sie Sicherheitsüberprüfungen erfolgreich durchführen:

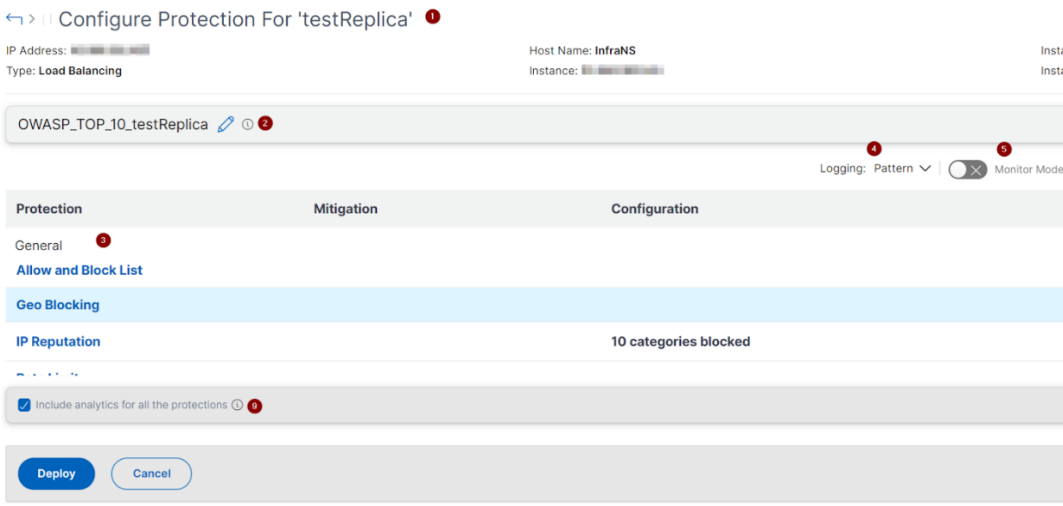
- Die Konfiguration wird je nach Version über StyleBooks auf die NetScaler-Instanz angewendet.
  - Für NetScaler 13.0 wird StyleBook `unified-appsec-protection-130` verwendet.
  - Für NetScaler 13.1 wird StyleBook `unified-appsec-protection-131` verwendet.
  - Für NetScaler 14.1 wird StyleBook `unified-appsec-protection-141` 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.

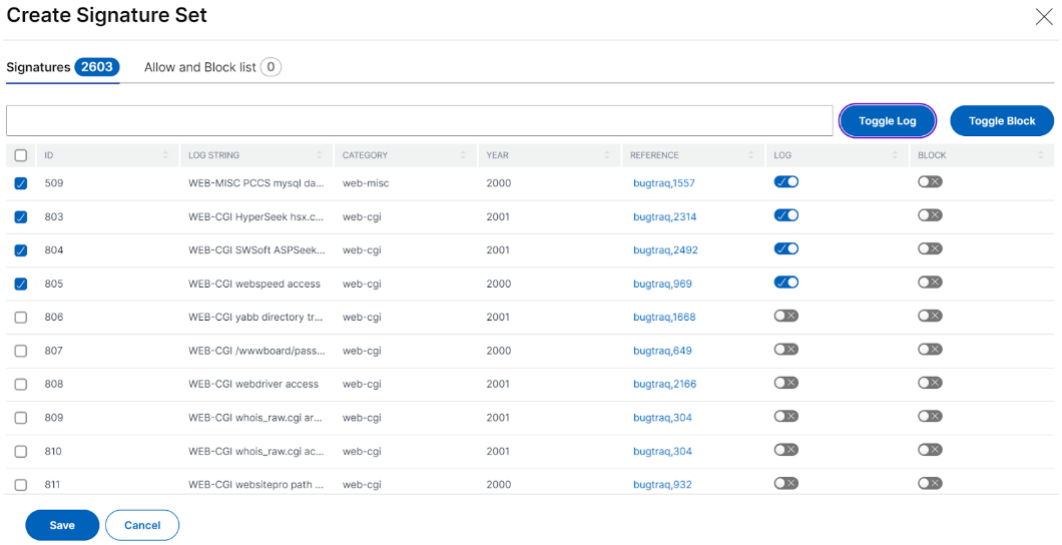
7 —Ermöglicht die Auswahl einer neuen Vorlage mithilfe der Option Vorlage ändern.

8 —Ermöglicht es Ihnen, den Schutz zu bearbeiten oder zu löschen.

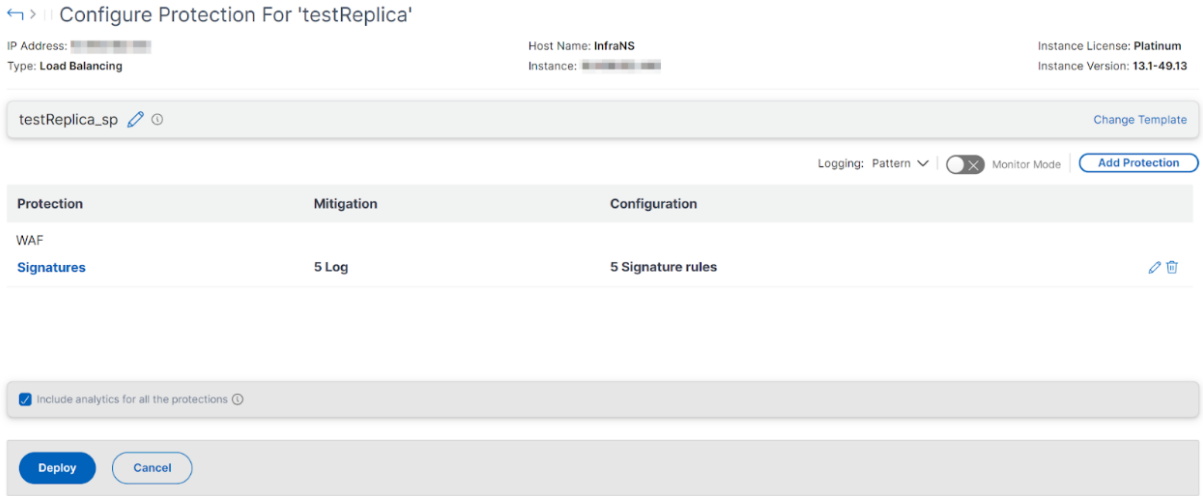
9 —Aktiviert Analysen für die von Ihnen ausgewählten Schutzmaßnahmen. Diese Option ist standardmäßig ausgewählt. Sie können Analysen für die konfigurierten Schutzmaßnahmen unter **Sicherheit > Sicherheitsverletzungen**einsehen.

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**.

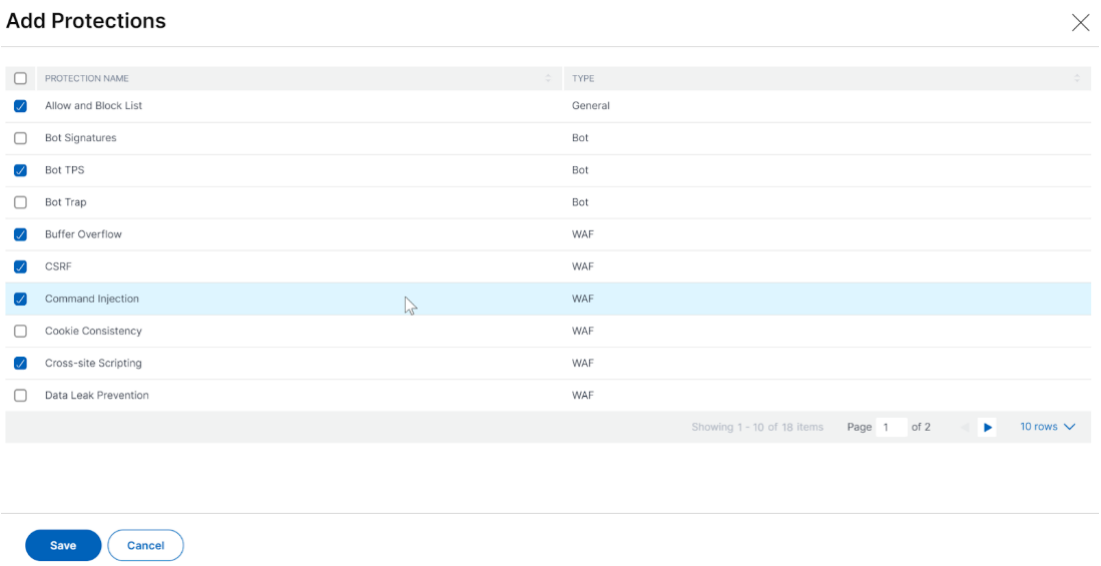


Nachdem Sie auf **Speichern**geklickt haben, können Sie die Signaturen anzeigen, die der Konfigurationsseite hinzugefügt wurden.



Sie können auch auf **Schutz hinzufügen** klicken, um der Anwendung weitere Schutzmaßnahmen hinzuzufügen. Nachdem Sie alle Schutzmaßnahmen konfiguriert haben, klicken Sie auf **Bereitstellen**.

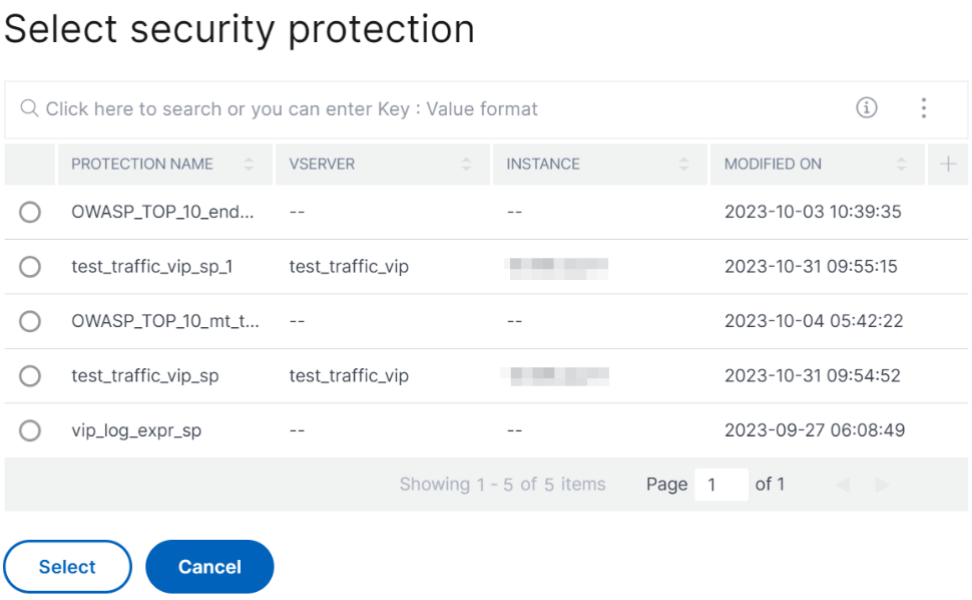
Benutzerdefinierter Schutz Klicken Sie auf **Neuen Schutz erstellen, um die Bereitstellung mit Schutzmaßnahmen**durchzuführen, die Ihren Anforderungen entsprechen. Wählen Sie auf der Seite **Schutzmaßnahmen hinzufügen** die Schutzmaßnahmen aus, die Sie bereitstellen möchten, und klicken Sie auf **Speichern**.



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

March 12, 2024

Webanwendungen, die dem Internet ausgesetzt sind, sind drastisch anfällig für Angriffe geworden. NetScaler Console ermöglicht es Ihnen, verwertbare Verstoßdetails zu 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 in WAF Insight als auch in Bot Insight enthalten sind. Weitere Informationen finden Sie unter Einheitliches Sicherheitsdashboard.
- Greifen Sie auf die Sicherheitsverletzungen der Anwendung anhand ihrer Kategorien wie **Netzwerk**, **Bot**und **WAF** zu.
- Ergreifen Sie Korrekturmaßnahmen, um die Anwendungen zu sichern.

Die Seite "**Sicherheitsverletzungen** "enthält die folgenden Optionen:

- **Anwendungsübersicht** —Zeigt eine Übersicht mit Anwendungen an, die totale Verstöße, totale WAF- und Bot-Verstöße, Verstöße nach Ländern usw. aufweisen. Weitere Informationen finden Sie unter Anwendungsübersicht.
- **Alle Verstöße** —Zeigt die Details zur Verletzung der Anwendungssicherheit an. Weitere Informationen finden Sie unter Alle Verstöße.

einrichten

Um die Verstöße einzusehen, müssen Sie Folgendes sicherstellen:

- Um mit der Konfiguration von Schutzmaßnahmen und der Aktivierung von Analysen in Ihren Anwendungen zu beginnen. Weitere Informationen finden Sie unter Einheitliches Sicherheitsdashboard.

  Wenn Sie Schutzmaßnahmen entweder über StyleBook oder direkt auf der NetScaler-Instanz konfiguriert haben, können Sie das Verfahren zum Aktivieren von **WAF-Sicherheitsverletzungen** und **Bot-Sicherheitsverletzungen** befolgen:

  1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** und wählen Sie den Instanztyp aus. Zum Beispiel VPX.
  2. Wählen Sie die Instanz aus und **wählen Sie in der Liste Aktion** auswählen die Option **Analytics konfigurieren**aus.

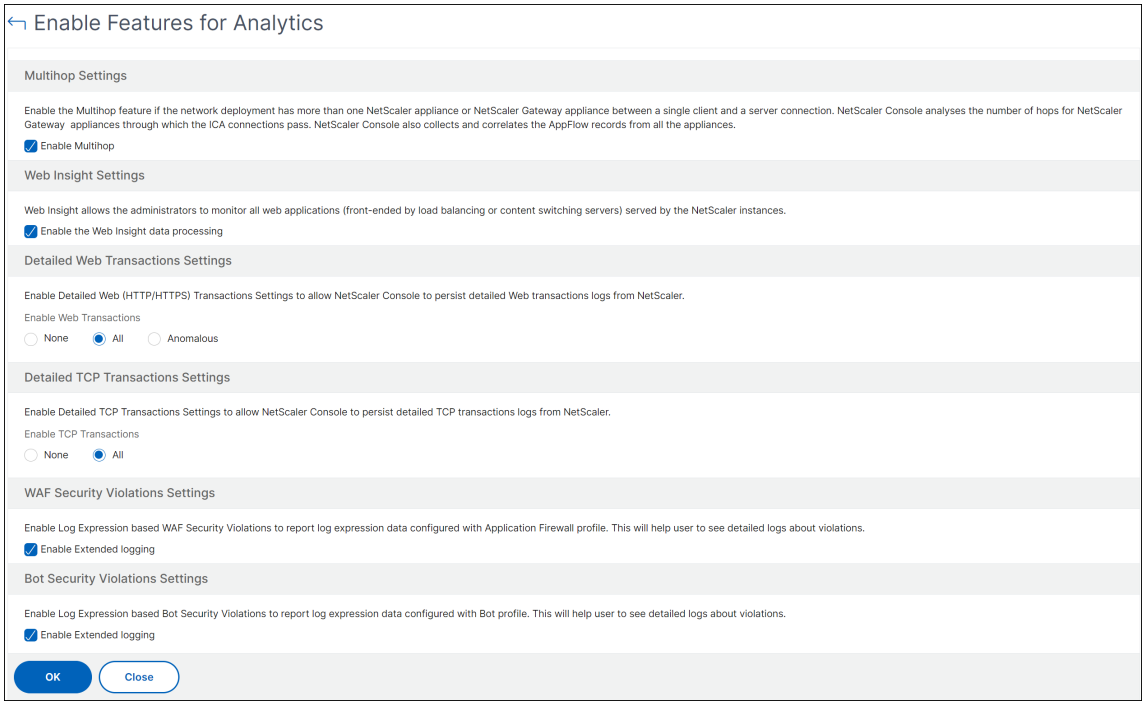
3. Wählen Sie die virtuellen Server aus und klicken Sie auf **Sicherheit und Analysen aktivieren**.
4. Wählen Sie im Fenster **Analysen aktivieren** die Optionen **WAF-Sicherheitsverletzungen** und **Bot-Sicherheitsverletzungen** aus und klicken Sie dann auf **OK**.

- Um detaillierte Web-Transaktionseinstellungen zu konfigurieren.
- Wenn **Metrics Collector** aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren von Intelligent App Analytics.

Webtransaktionseinstellungen aktivieren

1. Navigieren Sie zu **Einstellungen > Analytics-Einstellungen**.

   Die Seite **Analytics-Einstellungen** wird angezeigt.
2. Klicken Sie auf **Features für Analytics aktivieren**.
3. Wählen Sie unter **Detaillierte Webtransaktionseinstellungen**die Option **Alle** aus.

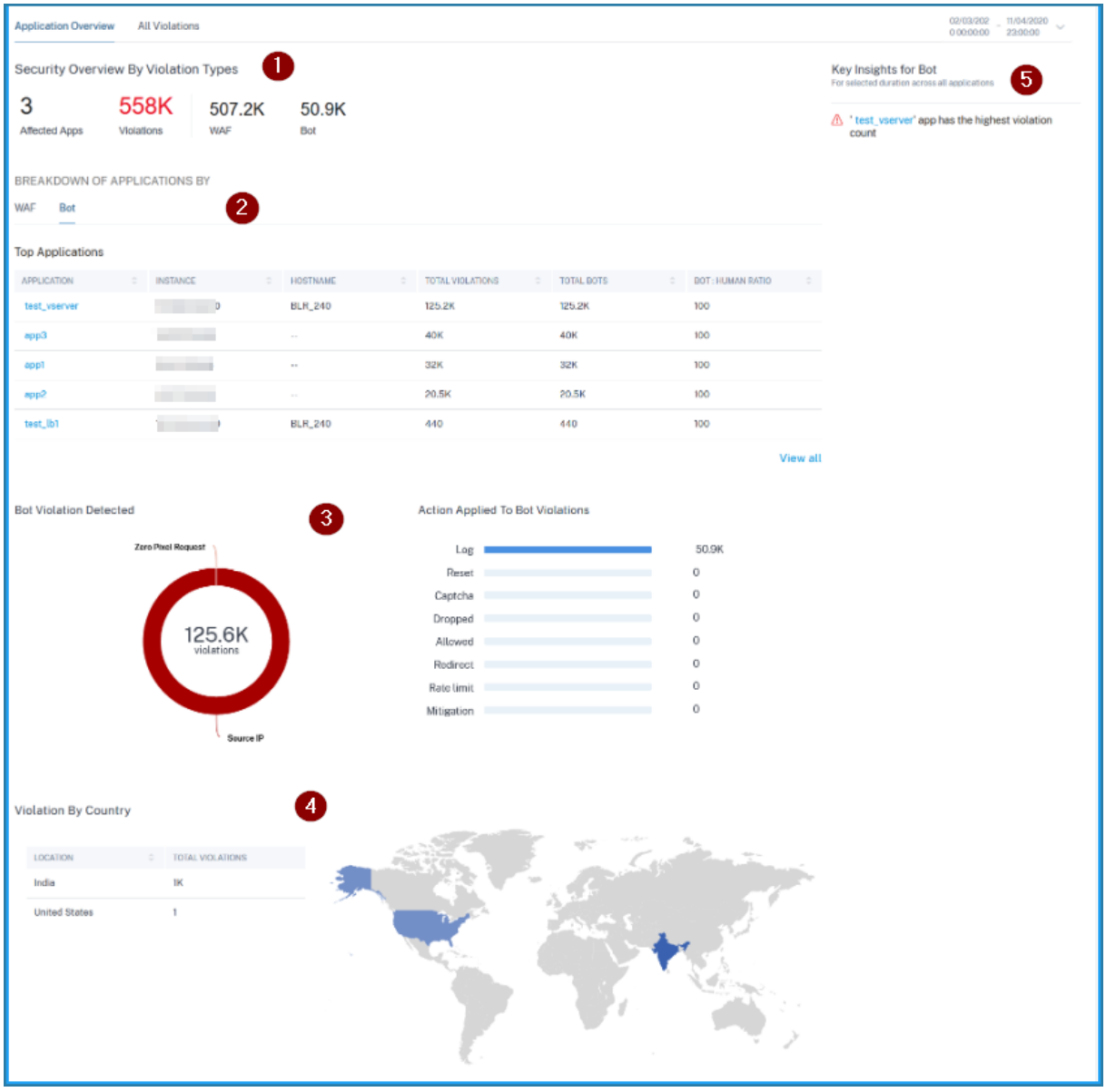


4. Klicken Sie auf **OK**.

Anwendungsüberblick

March 12, 2024

Auf der Seite **Anwendungsübersicht** werden Anwendungen mit vollständiger Einsicht in die Bedrohungsdetails angezeigt, die sowohl mit Security Insight als auch mit Bot Insight verknüpft Sie können auch Informationen wie totale Verstöße, vollständige Verstöße gegen WAF und Bot, Verstöße nach Ländern usw. anzeigen.



1 —Zeigt die Gesamtzahl der betroffenen Anwendungen, die Gesamtzahl von Verstößen, den gesamten WAF-Verstößen und den gesamten Bot-Verstößen für die ausgewählte

2 —Zeigt die Details zu WAF- und Bot-Verstößen an. Klicken Sie auf die Registerkarte **WAF** und **Bot**, um die fünf wichtigsten benutzerdefinierten oder diskreten Anwendungen basierend auf der Gesamtzahl der aufgetretenen Verstöße anzuzeigen. Klicken Sie auf **Alle anzeigen**, um alle Anwendungsdetails anzuzeigen.

3 —Zeigt die wichtigsten Verstöße basierend auf den Vorkommnissen und den angewendeten Aktio-

nen an.

4 —Zeigt eine Geo-Kartenansicht an, die Sichtbarkeit von Orten aus bietet, an denen die Verstöße aufgetreten sind.

5 —Stellt Informationen basierend auf den Verstößen bereit.

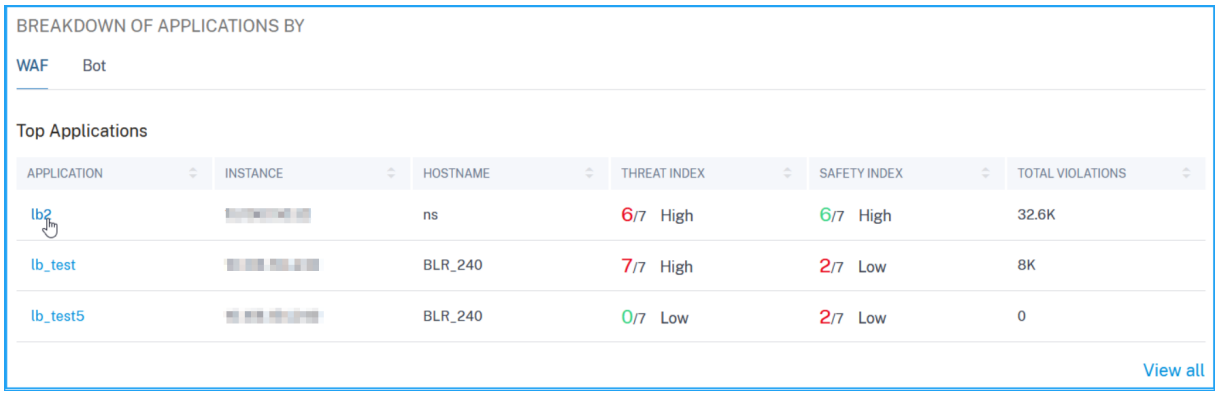
Kategorien von Verstößen

WAF	Bot
Cookie Hijack	Scraper
Infer Content Type XML	Screenshot Creator
Pufferüberlauf	Suchmaschine
Inhaltstyp	Service Agent
Konsistenz von Cookies	Sitemonitor
CSRF-Formular-Tagging	Geschwindigkeitstester
URL verweigern	Nicht kategorisiert
Konsistenz von Formularfeldern	Viren-Scanner
Feld-Formate	Vulnerability Scanner
Maximale Uploads	DeviceFP-Wartezeit überschritten
Referrer Header	Ungültiger DeviceFP
Sicherer Handel	Ungültige Captcha-Antwort
Sicheres Objekt	Tool
HTML SQL Inject	Captcha-Versuche wurden überschritten
Start-URL	Gültige Captcha-Antwort
Cross-Site Scripting	Captcha-Kunde stummgeschaltet
XML DoS	Captcha-Wartezeit überschritten
XML-Format	Größenbeschränkung der Anfrage überschritten
XML WSI	Ratenlimit überschritten
XML SSL	Sperrliste (IP, Subnetz, Richtlinienausdruck)
XML-Anhang	Positivliste (IP, Subnetz, Richtlinienausdruck)
XML-SOAP-Fehler	Null-Pixel-Anfrage

WAF	Bot
XML-Validierung	Quell-IP
Sonstiges	Host
IP-Reputation	Crawler
HTTP DOS	Feed Fetcher
TCP Small Window	Link Checker
Signatur-Verletzung	Marketing
Datei-Upload-Typ	Geo-Standort
JSON Cross-Site Scripting	URL
JSON SQL	
JSON DOS	
Befehlseinschleusung	
Schlüsselwort blockieren	
Schlüsselwort JSON Block	
Befehlseinschleusungsgrammatik	

Details zu WAF-Verstößen anzeigen

Klicken Sie in den **Top-Anwendungen** oder in der Option **Alle anzeigen auf** eine Anwendung, um die WAF-Details anzuzeigen.

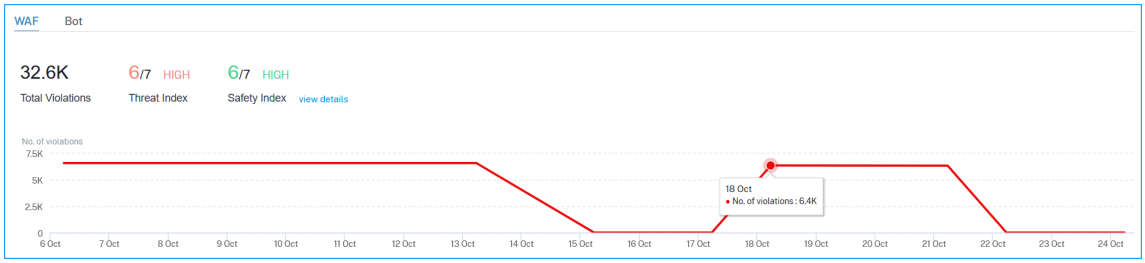


> **Hinweis:**
>
> Wenn Sie eine benutzerdefinierte App auswählen, können Sie die Details der konsolidierten Anwendungen auf der Seite **Sicherheitsübersicht** anzeigen. Wählen Sie aus der Liste eine Anwen-

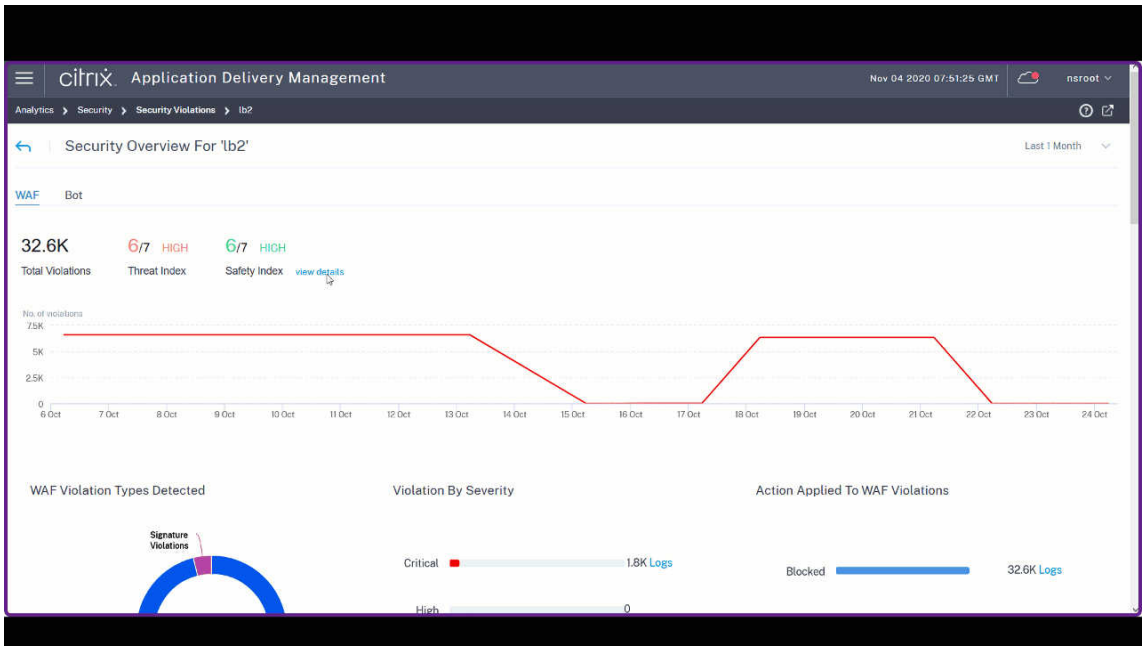
> dung aus, um Details für die ausgewählte Anwendung anzuzeigen.

Die Seite "**Sicherheitsübersicht** "für die ausgewählte Anwendung wird angezeigt. Unter **WAF**können Sie Folgendes sehen:

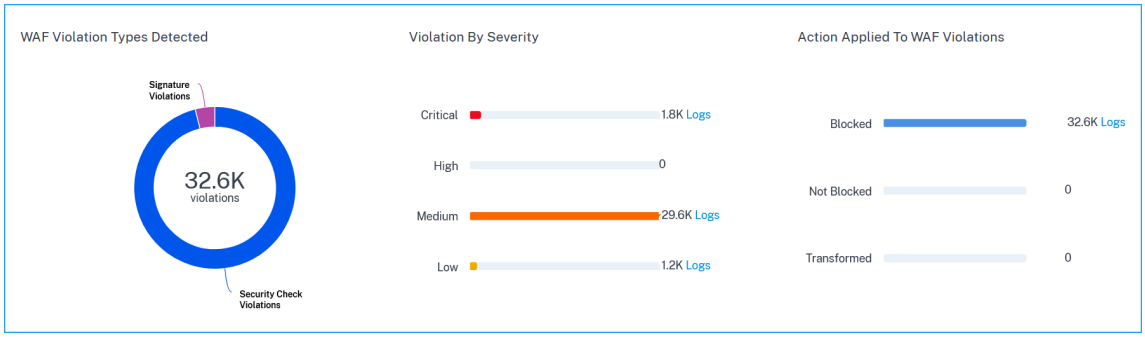
- Eine Diagrammansicht, die die Gesamtzahl der Verstöße, den Bedrohungsindex-Score und den Sicherheitsindex-Score



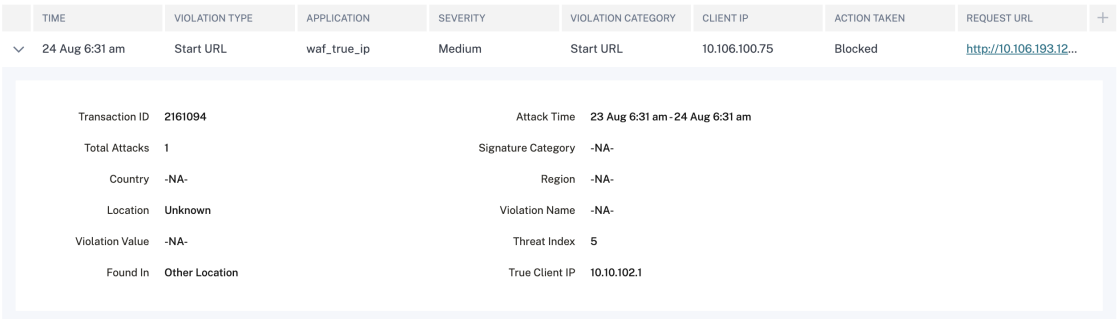
Klicken Sie auf **Details anzeigen**, um die Details zur Konfiguration der Application Firewall und NetScaler System Security anzuzeigen.



- Die Verstöße basieren auf Arten, Schweregrad und angewandten Maßnahmen.



Klicken Sie auf **Protokolle**, um Details basierend auf dem Schweregrad oder den ergriffenen Sie können auch die Client-IP-Adresse anzeigen.



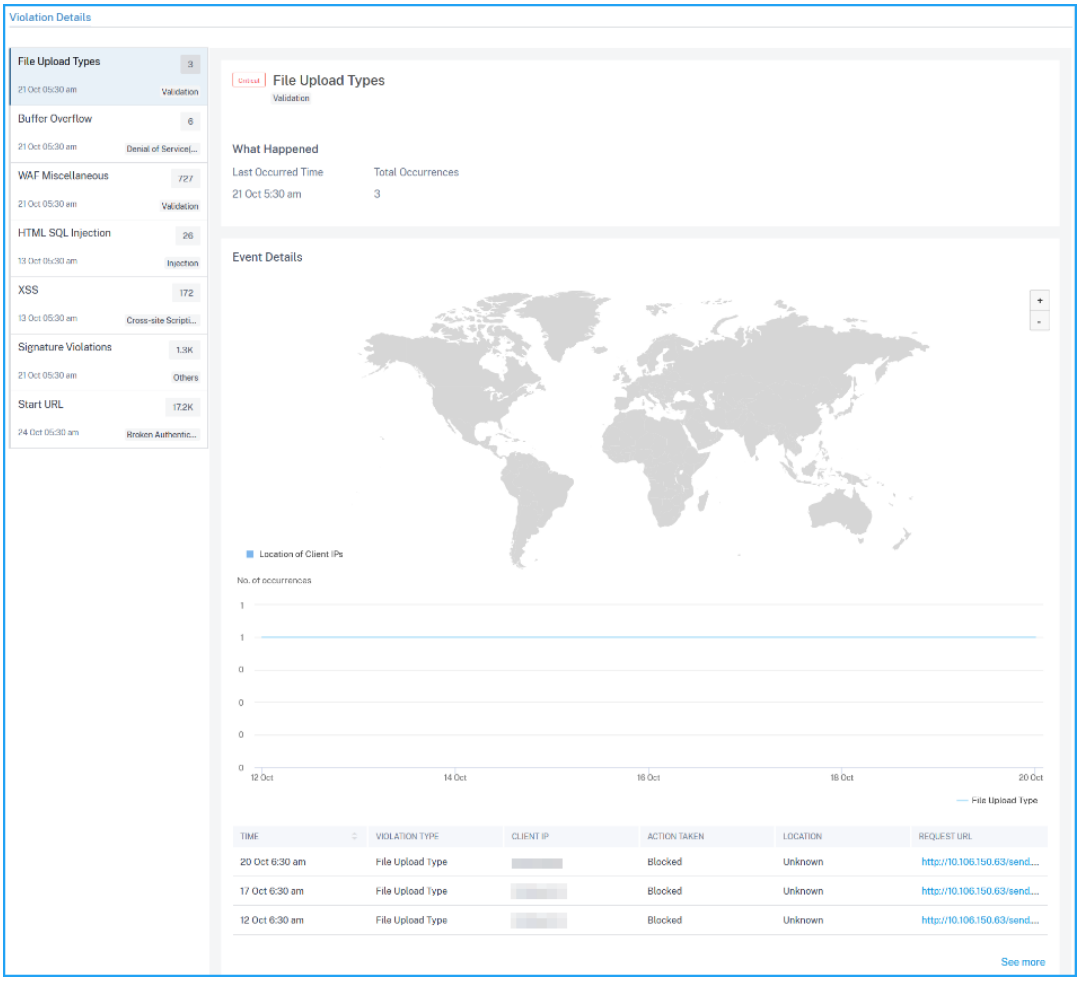
Sie können auch das Suchtextfeld verwenden, in dem Sie Details gemäß Ihren Anforderungen anzeigen können. Wenn Sie auf das Suchfeld klicken, erhalten Sie im Suchfeld eine Liste mit Suchvorschlägen.

- Die von der Anwendung betroffenen Verstöße. Unter **Details zu Verstößen**können Sie die Details des betroffenen Verstoßes anzeigen.

  > **Hinweis**
  >
  > Bei einer benutzerdefinierten App werden Verstöße angezeigt, die für alle Anwendungen gelten. Sie können auf eine Anwendung in der Liste klicken, um die betroffenen Verstöße für die ausgewählte Anwendung anzuzeigen.

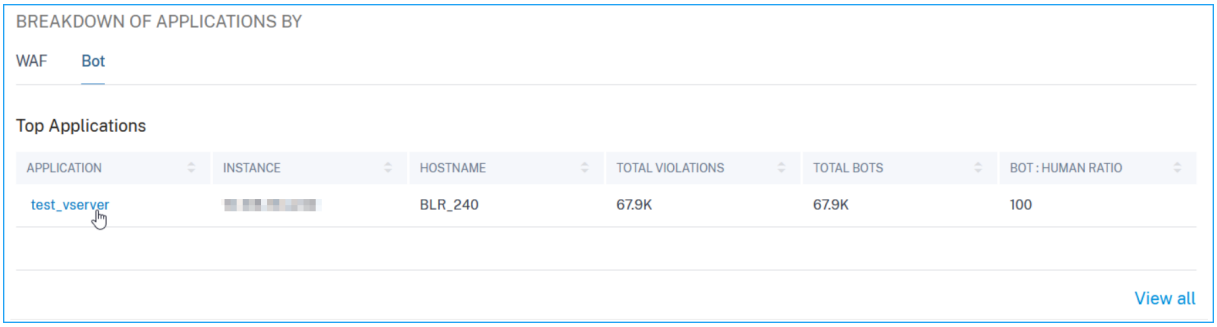
  Klicken Sie auf jeden Verstoß, um Details wie:

  - **Was ist passiert** —Gibt die Gesamtvorkommen und das Datum und die Uhrzeit des letzten aufgetretenen Datums an.
  - **Ereignisdetails** —Zeigt eine Geomap an, die die Client-IP und andere Verstoßdetails wie Verstoßart, Client-IP, Standort usw. angibt.



Details zur Bot-Verletzung anzeigen

Klicken Sie auf der Registerkarte **Bot** in den **Top-Anwendungen** oder in der Option **Alle anzeigen** auf eine Anwendung, um die Bot-Details anzuzeigen.

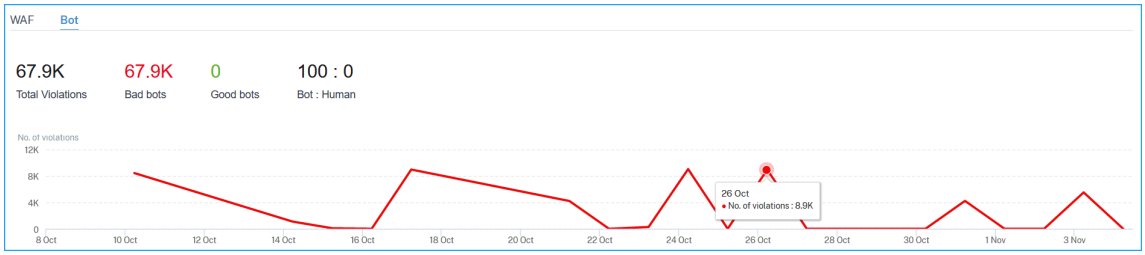


> **Hinweis**
>
> Wenn Sie eine benutzerdefinierte App auswählen, können Sie die Details der konsolidierten An-

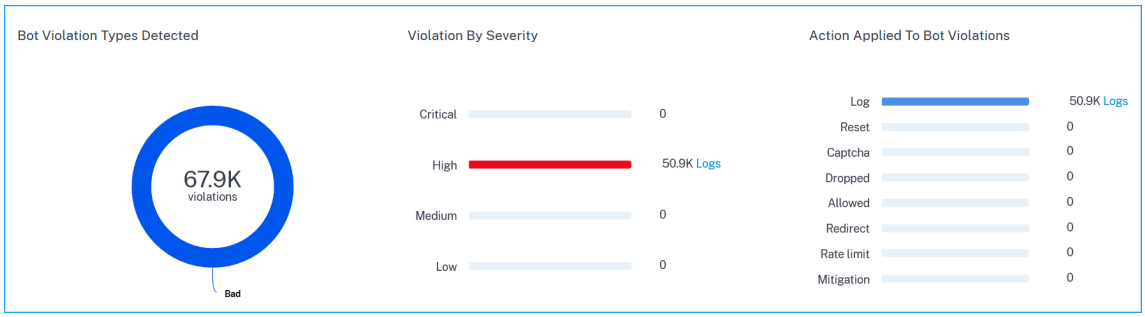
> wendungen auf der Seite **Sicherheitsübersicht** anzeigen. Wählen Sie aus der Liste eine Anwendung aus, um Details für die ausgewählte Anwendung anzuzeigen.

Die Seite "**Sicherheitsübersicht** "für die ausgewählte Anwendung wird angezeigt. Unter **Bot**können Sie Folgendes anzeigen:

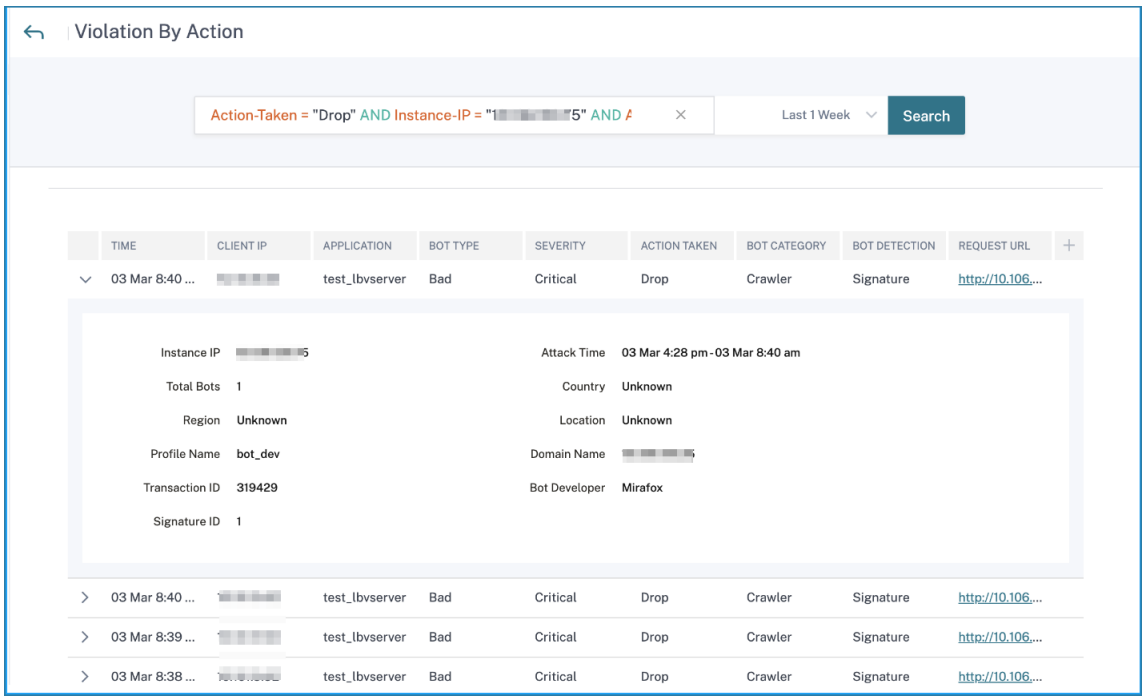
- Eine Grafik, die die Gesamtzahl der Bots, die insgesamt schlechten Bots, die insgesamt guten Bots und das Gesamtverhältnis zwischen menschlichen Benutzern und Bots anzeigt, die auf die Anwendung zugreifen.



- Die Verstöße basieren auf den angewendeten Bot-Typen, dem Schweregrad und den Aktionen.

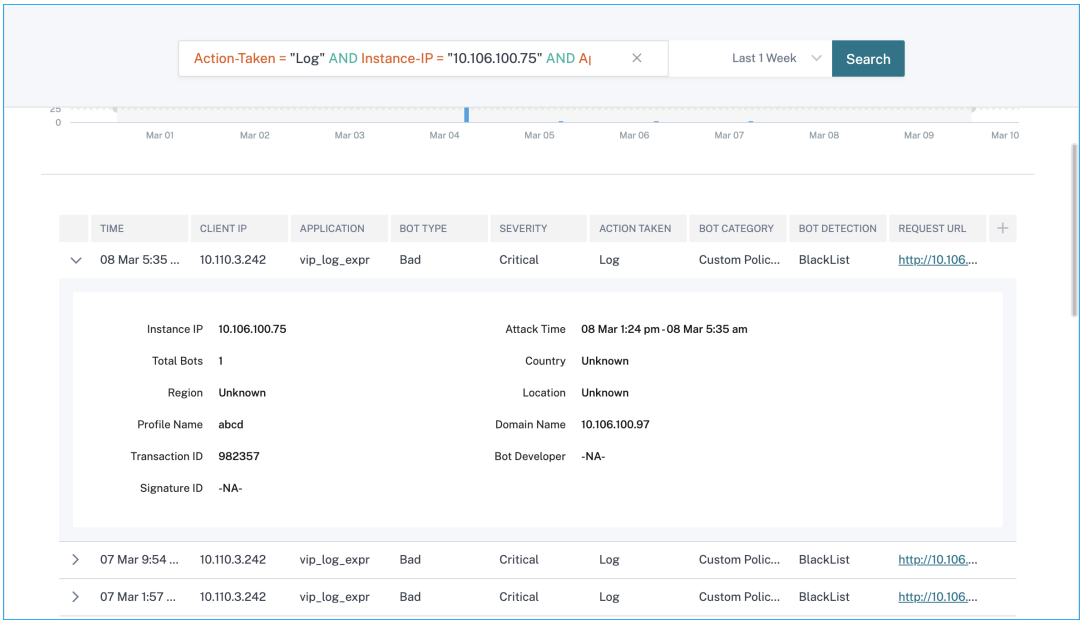


Klicken Sie auf **Protokolle**, um Details basierend auf dem Schweregrad oder den ergriff Wenn ein erkannter Bot ein Bot vom Typ Signature ist, können Sie weitere Details wie Bot-Entwickler und Signature ID anzeigen. Mit der Signature-ID können Sie feststellen, ob der erkannte Bot ein guter Bot oder ein schlechter Bot ist.



Hinweis:

Wenn ein erkannter Bot ein anderer Bot-Typ außer dem Signature-Bot ist, werden die Signature-ID und der Bot-Entwickler als N/A angezeigt.



Sie können auch das Suchtextfeld verwenden, in dem Sie Bot-Details gemäß Ihren Anforderungen anzeigen können. Wenn Sie auf das Suchfeld klicken, erhalten Sie im Suchfeld eine Liste mit Suchvorschlägen.

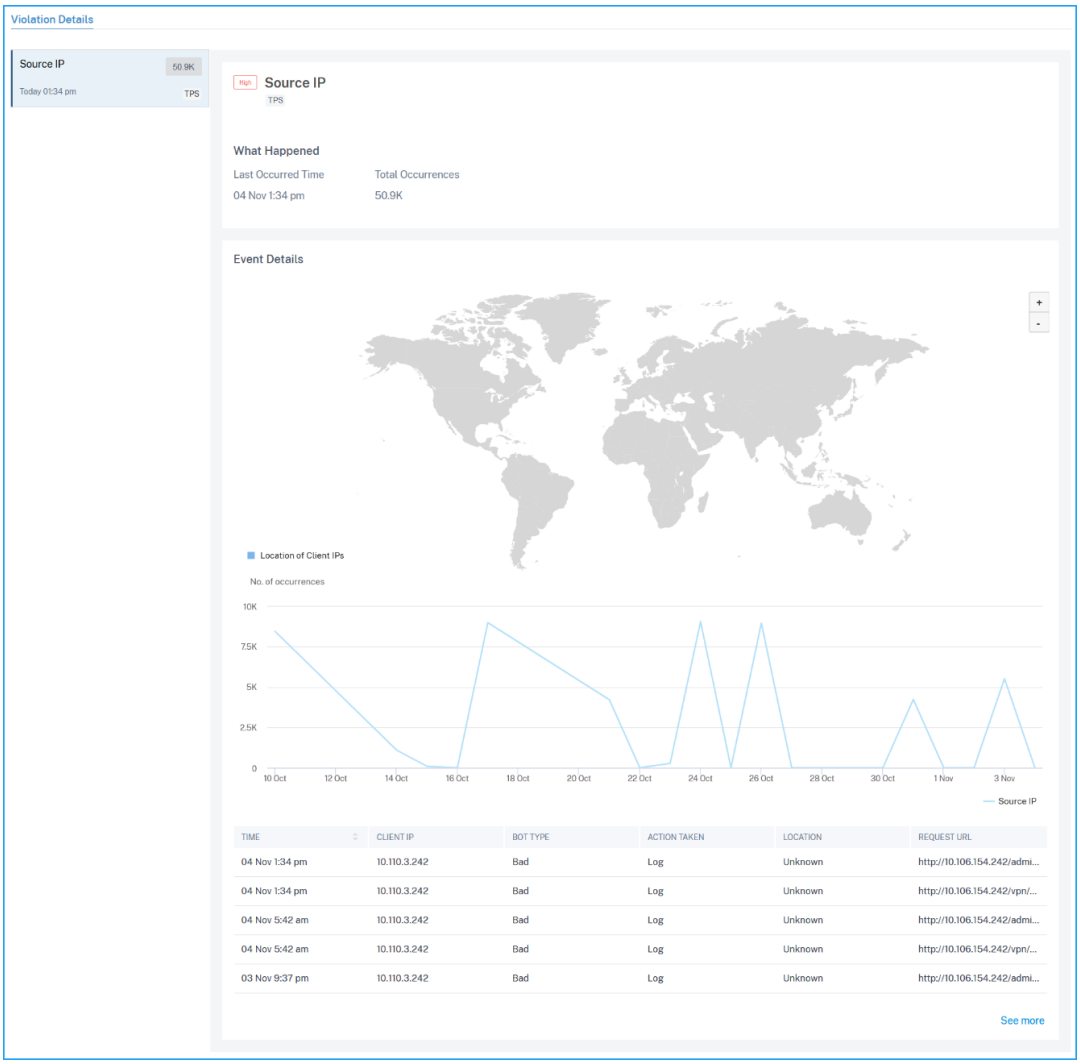
- Die von der Anwendung betroffenen Verstöße. Unter **Details zu Verstößen**können Sie die De-

tails des betroffenen Verstoßes anzeigen.

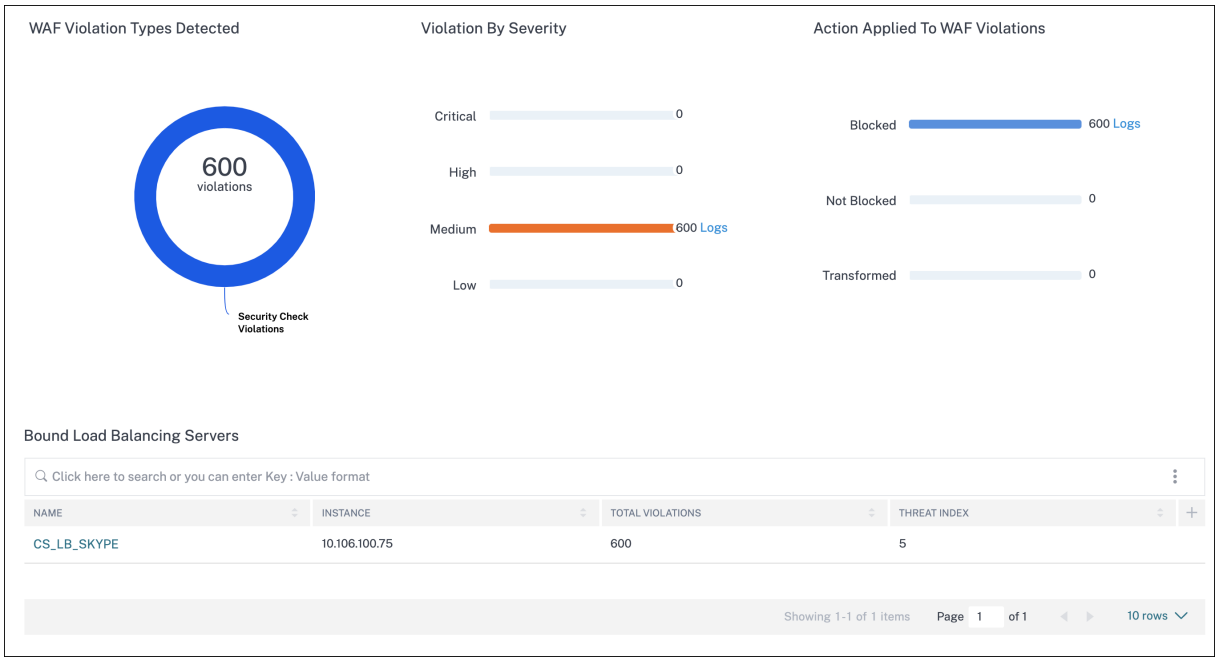
> **Hinweis:**
>
> Bei einer benutzerdefinierten App werden Verstöße angezeigt, die für alle Anwendungen gelten. Sie können auf eine Anwendung in der Liste klicken, um die betroffenen Verstöße für die ausgewählte Anwendung anzuzeigen.

Klicken Sie auf jeden Verstoß, um Details wie:

- **Was ist passiert** —Gibt die Gesamtvorkommen und das Datum und die Uhrzeit des letzten aufgetretenen Datums an.
- **Ereignisdetails** —Zeigt eine Geomap an, die die Client-IP und andere Verstoßdetails wie Verstoßart, Client-IP, Standort usw. angibt.



> **Hinweis:**
>
> Unter **WAF** und **Bot**können Sie Analysen für den virtuellen Server mit Content Switching anzeigen, der an virtuelle Lastausgleichsserver gebunden ist. Klicken Sie auf den virtuellen Content Switching-Server und unter **Bound Load Balancing Server**können Sie die Liste der Load Balancing-Server anzeigen, die an den virtuellen Content Switching-Server gebunden sind.



Ereignisverlauf anzeigen

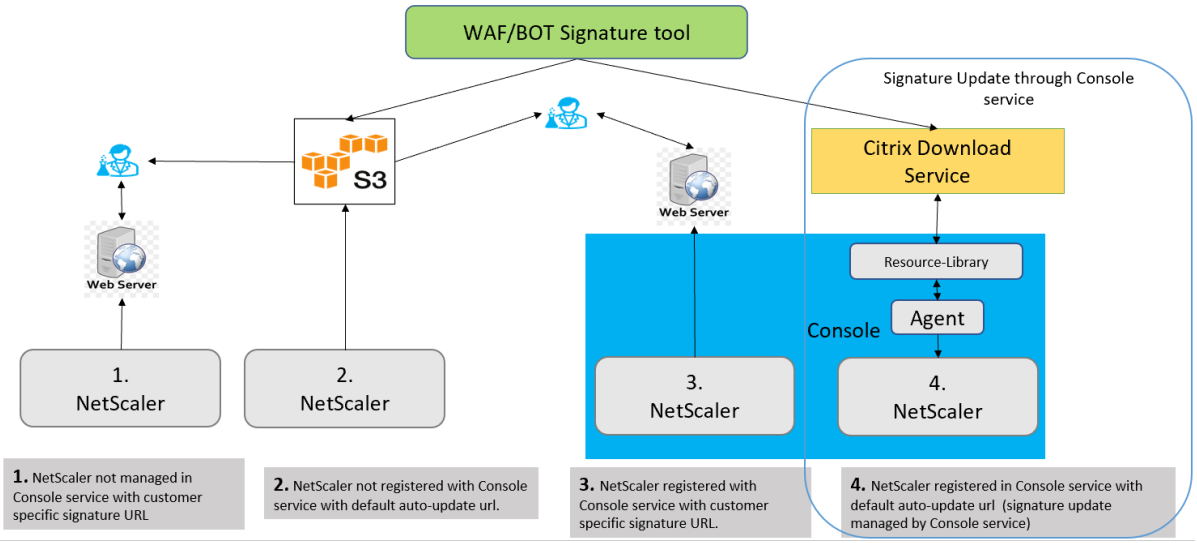
Sie können die Signaturaktualisierungen unter **Ereignisse** einsehen, wenn:

- Neue Signaturen werden in NetScaler-Instanzen hinzugefügt.
- Bestehende Signaturen werden in NetScaler-Instanzen aktualisiert.

Automatische Aktualisierung der Signatur

NetScaler Console sucht automatisch nach neuen Signaturaktualisierungen und wendet sie auf die verwalteten NetScaler-Instanzen an.

Das folgende Diagramm zeigt, wie die Signaturen aus der AWS-Cloud abgerufen, auf NetScaler aktualisiert werden und eine Zusammenfassung der Signaturaktualisierung in der NetScaler Console angezeigt wird.



Alle Verstöße

March 12, 2024

Auf der Seite "**Alle Verstöße** "werden die Details zur Verletzung der Anwendungssicherheit basierend auf den Kategorien **Netzwerk**, **WAF**und **Bot** angezeigt. Stellen Sie sicher, dass Sie alle erforderlichen Einstellungen aktiviert haben, um die Sicherheitsverletzungen in der NetScaler Console anzuzeigen. Weitere Informationen finden Sie in der Vorgehensweise unter Einrichten.

Kategorien von Verstößen

Mit der NetScaler Console können Sie die folgenden Verstöße anzeigen. Unter **Verstoßdetails**können Sie auf jede Registerkarte "Verstoß"klicken, um die Details zum Verstoß anzuzeigen.

Netzwerk	WAF	Bot
HTTP Slow Loris	Infer Content Type XML	Scraper
DNS Slow Loris	Pufferüberlauf	Screenshot Creator
Langsame HTTP-Post	Inhaltstyp	Suchmaschine
NXDomain Flood Attack	Konsistenz von Cookies	Service Agent
HTTP-Desync-Angriff	CSRF-Formular-Tagging	Sitemonitor
Bleichenbacher Angriff	URL verweigern	Geschwindigkeitstester

Netzwerk	WAF	Bot
Segment smack Attack	Konsistenz von Formularfeldern	Tool
SYN-Flood-Angriff	Feld-Formate	Nicht kategorisiert
Angriff auf kleine Fenster	Referrer Header	Viren-Scanner
		Cross-Site Scripting
		XML DoS
		XML-Format
		XML WSI
		XML SSL
		XML-Anhang
		XML-SOAP-Fehler
		XML-Validierung
		Sonstiges
		IP-Reputation
		HTTP DOS
		TCP Small Window
		Signatur-Verletzung
		Datei-Upload-Typ
		JSON Cross-Site Scripting
		JSON SQL
		JSON DOS
		Befehlseinschleusung
	Cookie Hijack	Feed Fetcher
	Schlüsselwort blockieren	Link Checker
	Schlüsselwort JSON Block	Marketing
		Sicherer Handel
		Sicheres Objekt
		HTML SQL Inject
		Start-URL

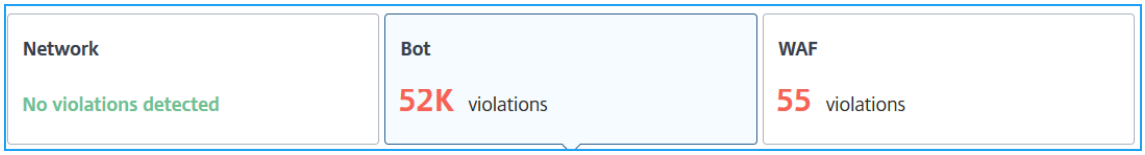
Netzwerk	WAF	Bot
	Befehlseinschleusungsgrammatik JSON SQL Injection	

Dashboard für Sicherheitsverletzungen

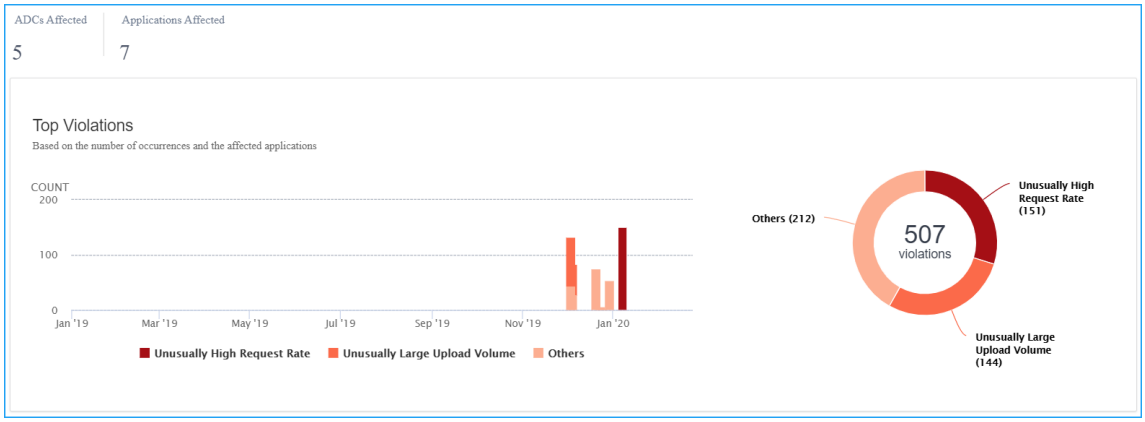
Im Dashboard für Sicherheitsverletzungen können Sie Folgendes anzeigen:

- In allen NetScaler-Instanzen und -Anwendungen kam es insgesamt zu Verstößen. Die Gesamtzahl der Verstöße wird basierend auf der ausgewählten Zeitdauer angezeigt.

- Gesamtzahl der Verstöße in jeder Kategorie.



- Gesamtzahl der betroffenen NetScaler-Instanzen, Gesamtzahl der betroffenen Anwendungen und die häufigsten Verstöße, basierend auf der Gesamtzahl der Vorkommnisse und der betroffenen Anwendungen.



Einzelheiten des Verstoßes

Bei jedem Verstoß überwacht NetScaler Console das Verhalten für einen bestimmten Zeitraum und erkennt Verstöße bei ungewöhnlichen Verhaltensweisen. Klicken Sie auf die einzelnen Registerkarten, um die Verstöße anzuzeigen. Sie können Details anzeigen, z. B.:

- Die Gesamtereignisse, zuletzt aufgetretene und die Gesamtzahl der betroffenen Anwendungen

- Unter Ereignisdetails können Sie Folgendes anzeigen:
  - Die betroffene Anwendung. Sie können die Anwendung auch aus der Liste auswählen, wenn zwei oder mehr Anwendungen mit Verstößen betroffen sind.
  - Das Diagramm, das Verstöße anzeigt.
  - **Empfohlene Maßnahmen**, die darauf hindeuten, dass Sie das Problem beheben.
  - Weitere Einzelheiten zu Verstößen wie Zeit des Auftretens von Gewalt und Erkennungsmeldung.

API-Sicherheit

January 26, 2024

APIs oder Application Programming Interfaces sind Sätze von Regeln, Protokollen und Tools, die es verschiedenen Softwareanwendungen oder Systemen ermöglichen, miteinander zu kommunizieren. APIs spielen eine wichtige Rolle beim Schutz sensibler Daten, indem sie Zugriffskontrollen, Authentifizierung und Verschlüsselung durchsetzen und so sicherstellen, dass nur autorisierte Stellen auf vertrauliche Informationen zugreifen und diese sicher übertragen können.

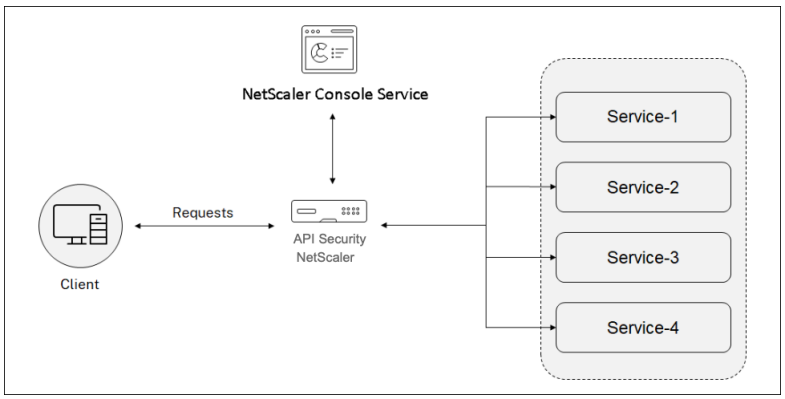
APIs dienen als Backend-Framework für Mobil- und Webanwendungen. Daher ist es wichtig, die vertraulichen Daten, die sie übertragen, zu schützen. API-Sicherheit bezieht sich auf die Praxis, Angriffe auf APIs zu verhindern oder abzuschwächen.

Bei der API-Sicherheit fungiert ein Gateway als Einstiegspunkt für alle Anfragen an Ihre API-Endpunkte. Und gewährleistet einen sicheren und zuverlässigen Zugriff auf alle API-Endpunkte und Microservices in Ihrem System.

Gehen Sie wie folgt vor, um Ihre APIs zu sichern:

- API-Definition erstellen und hochladen
- Bereitstellen einer API-Instanz
- Richtlinien zu einer API-Bereitstellung hinzufügen

Die folgende Abbildung beschreibt, wie die API-Sicherheit in NetScaler Console die Client-Anfrage empfängt und die Antwort von den Back-End-API-Diensten sendet:



> **Hinweis:**
>
> In NetScaler Console ist diese Funktion für Benutzer mit Premium- oder Advanced-Lizenzen verfügbar.

Vorteile der API-Sicherheit

Die API-Sicherheit bietet Ihnen die folgenden Vorteile:

- Schützt**Ihre API-Endpunkte**: Die API-Sicherheit fügt eine Sicherheitsebene hinzu und schützt Ihre API-Endpunkte und Backend-API-Server vor Angriffen wie:
  - Pufferüberlauf
  - SQL-Einschleusung
  - Cross-Site Scripting
  - Denial-of-Service (Dos)
- **Überwacht und verbessert die API-Leistung**: Die API-Sicherheit bietet Dienste wie SSL-Offloading, Authentifizierung, Autorisierung, Ratenbegrenzung und mehr. Diese Dienste erhöhen die API-Performance und ihre Verfügbarkeit.

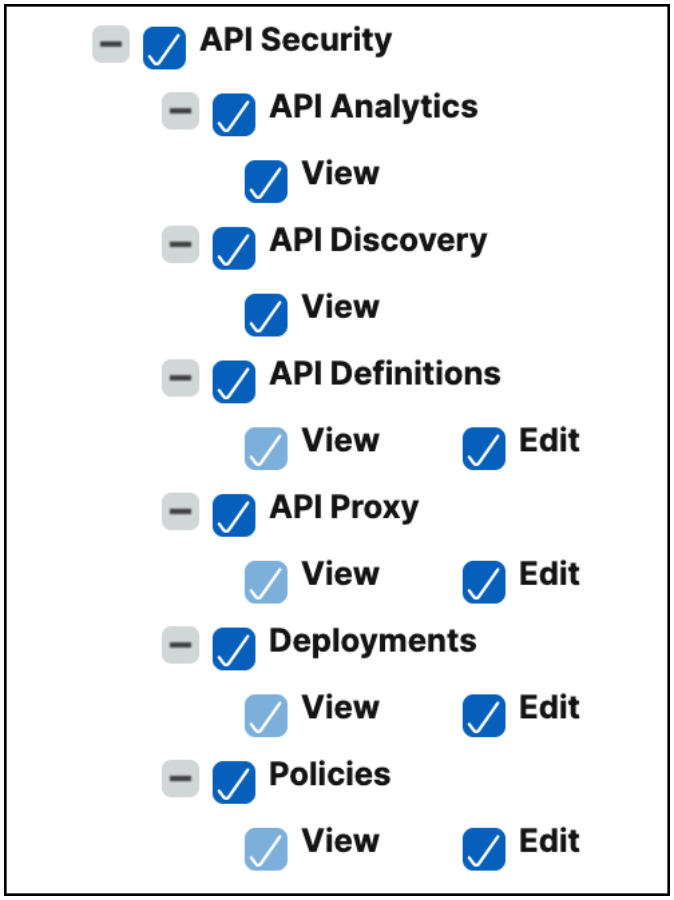
  Die API-Analytik bietet Ihnen die Einblicke in Ihre API-Performance-Metriken und Bedrohungen für Ihre API-Endpunkte. Weitere Informationen finden Sie unter Anzeigen von API-Analysen.
- **Verwaltet den API-Verkehr**: Die API-Sicherheit abstrahiert die Komplexität Ihrer Backend-API-Infrastruktur.
- **Erkennt API-Endpunkte**: Die API-Sicherheit erkennt die API-Endpunkte, die sich in Ihrer Organisation befinden, und fügt sie der Seite **API Discovery** hinzu.

API-Sicherheitskonfigurations- und Verwaltungsberechtigungen gewähren

Als Administrator können Sie eine Zugriffsrichtlinie erstellen, um Benutzerberechtigungen für die Konfiguration und Verwaltung der API-Sicherheit zu gewähren. Die Benutzerberechtigungen können

Anzeigen, Hinzufügen, Bearbeiten und Löschen sein. Führen Sie Folgendes aus, um Berechtigungen zu erteilen:

1. Navigieren Sie zu **Einstellungen > Benutzer und Rollen > Zugriffsrichtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie unter **Zugriffsrichtlinien erstellen**einen Richtliniennamen und die Beschreibung an.
4. Erweitern Sie im Feld **Berechtigungen** die Optionen **Anwendungen** und dann **API-Sicherheit**.
5. Wählen Sie die erforderlichen **API-Sicherheitsseiten** aus. Wählen Sie dann die Berechtigungen aus, die Sie gewähren möchten.



> **Wichtig:**
>
> Stellen Sie sicher, dass Sie Berechtigungen für die Funktionen gewähren, die für die Verwendung einer API-Sicherheit erforderlich sind. Wenn Sie beispielsweise Benutzern Zugriff auf die Seite "**Bereitstellungen** "gewähren, erfordern die folgenden Funktionen auch Benutzerzugriff:
>
> - StyleBooks
> - IPAM

- Load Balancing (unter **Netzwerkfunktionen**)
- Content Switching (unter **Netzwerkfunktionen**)
- Geräte-API-Proxy (unter **API**)

Weitere Informationen zu Zugriffsrichtlinien finden Sie unter Konfigurieren von Zugriffsrichtlinien in der NetScaler Console .

WAF-Lernen

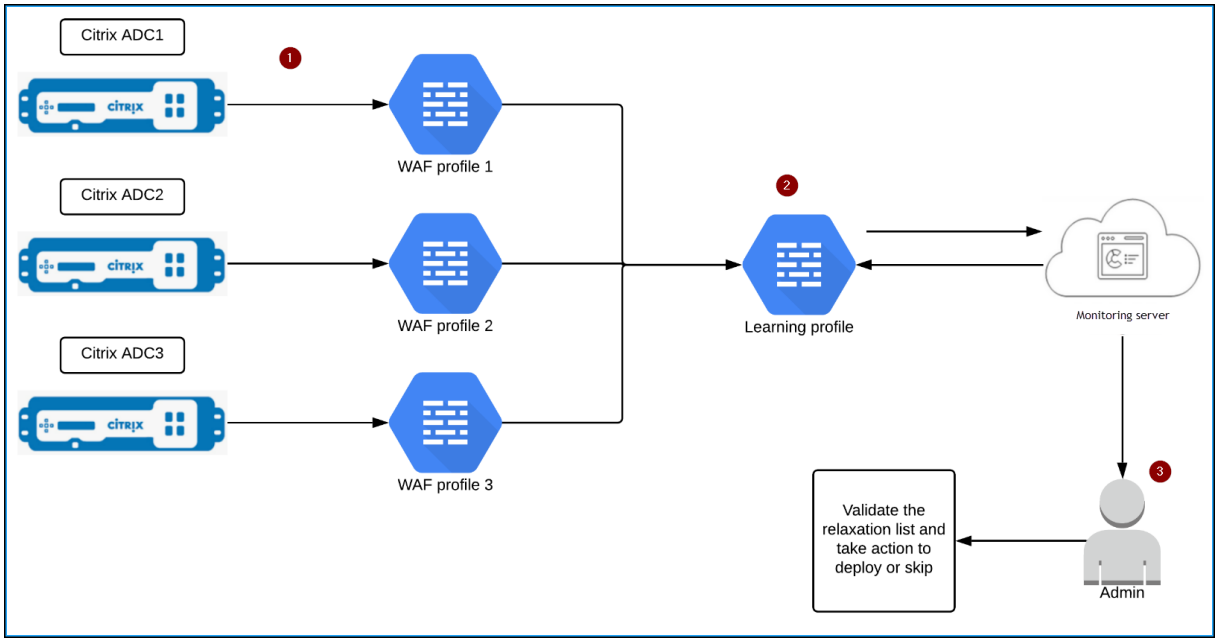
January 26, 2024

NetScaler Web App Firewall (WAF) schützt Ihre Webanwendungen vor böswilligen Angriffen wie SQL-Injection und Cross-Site Scripting. Um Datenschutzverletzungen vorzubeugen und den richtigen Sicherheitsschutz zu bieten, müssen Sie Ihren Datenverkehr auf Bedrohungen und umsetzbare Echtzeitdaten bei Angriffen überwachen. Manchmal können die gemeldeten Angriffe falsch positiv sein und diese müssen ausnahmsweise angegeben werden.

Die Learning-Engine in NetScaler Console ist ein sich wiederholender Musterfilter, der es der WAF ermöglicht, das Verhalten (die normalen Aktivitäten) Ihrer Webanwendungen zu erlernen. Basierend auf der Überwachung generiert die Engine eine Liste mit vorgeschlagenen Regeln oder Ausnahmen für jede Sicherheitsüberprüfung, die auf den HTTP-Verkehr angewendet wird.

Es ist viel einfacher, Relaxationsregeln mithilfe der Lern-Engine bereitzustellen, als sie manuell als notwendige Relaxationen bereitzustellen.

In der folgenden Abbildung werden die allgemeinen Informationen zur Funktionsweise des WAF-Lernens in NetScaler Console erläutert:



1 —NetScaler-Instanzen mit seinen WAF-Profilen

2—Konfigurieren Sie ein Lernprofil in NetScaler Console, fügen Sie die WAF-Profile hinzu und wählen Sie, ob die Entspannungsregeln automatisch oder manuell bereitgestellt werden sollen

3—Der Administrator kann die Relaxationsregeln in der NetScaler Console überprüfen und entscheiden, ob sie bereitgestellt oder übersprungen werden sollen

Erste Schritte

Um die Lernfunktion bereitzustellen, müssen Sie:

- Aktivieren Sie das zentralisierte Lernen in der NetScaler-Instanz. Führen Sie den folgenden Befehl in der NetScaler-Instanz aus:

  ```
  set appfw settings -centralizedLearning ON
  ```

- Stellen Sie sicher, dass die NetScaler-Instanzversion **13.0-76.6** oder höher ist.
- Konfigurieren Sie ein Web App Firewall-Profil (Satz von Sicherheitseinstellungen) auf Ihrer NetScaler Appliance. Weitere Informationen finden Sie unter Erstellen von Web App Firewall-Profilen.

Nachdem Sie das zentrale Lernen aktiviert und das WAF-Profil konfiguriert haben, generiert NetScaler Console eine Liste von Ausnahmen (Relaxationen) für die konfigurierte Sicherheitsüberprüfung. Als Administrator können Sie die Liste der Ausnahmen in NetScaler Console überprüfen und entscheiden, ob Sie sie bereitstellen oder überspringen möchten.

Mit der WAF-Lernfunktion in NetScaler Console können Sie:

- Konfigurieren Sie ein Lernprofil mit den folgenden Sicherheitsüberprüfungen:
  - Start-URL
  - Konsistenz von Cookies
  - Kreditkarte

    > **Hinweis**
    >
    > Für die Kreditkartensicherheitsprüfung müssen Sie die `doSecureCreditCardLogging` in der NetScaler-Instanz konfigurieren und sicherstellen, dass die Einstellung **OFF**ist.

  - Inhaltstyp
  - Konsistenz von Formularfeldern
  - Feld-Formate
  - CSRF-Formular-Tagging
  - Siteübergreifendes HTML-Scripting
  - HTML-SQL-Injektion

    > **Hinweis**
    >
    > Für die HTML-SQL-Einschleusungsprüfung müssen Sie `set -sqlinjectionTransformSpeci ON` und `set -sqlinjectiontype sqlspclcharorkeywords` in der NetScaler-Instanz konfigurieren.

  - HTML-Befehlseinschleusung

    > **Hinweis**
    >
    > Wird nur in der NetScaler-Instanz 13.0-72.12 oder höher unterstützt.

  - JSON SQL

    > **Hinweis**
    >
    > Wird nur in der NetScaler-Instanz 13.1-14.10 oder höher unterstützt.

  - JSON-Befehlseinschleusung

    > **Hinweis**
    >
    > Wird nur in der NetScaler-Instanz 13.1-14.10 oder höher unterstützt.

  - JSON XSS

> **Hinweis**
>
> Wird nur in der NetScaler-Instanz 13.1-14.10 oder höher unterstützt.

- Überprüfen Sie die Relaxationsregeln in der NetScaler Console und entscheiden Sie, ob Sie die erforderlichen Maßnahmen ergreifen möchten (bereitstellen oder überspringen)
- Erhalten Sie die Benachrichtigungen per E-Mail, Slack und ServiceNow
- Verwenden Sie die Seite **Aktionsübersicht**, um Details zur Entspannung anzuzeigen

So verwenden Sie das WAF-Lernen in NetScaler Console:

1. Konfigurieren des Lernprofils
2. Verwalte die Entspannungsregeln
3. Verwenden Sie die Seite Zusammenfassung der WAF-Lernaktion

Empfehlungen der WAF

January 26, 2024

Das Profil der NetScaler Web App Firewall (WAF) und WAF-Signaturen schützen Ihre Webanwendungen vor böswilligen Angriffen. WAF-Signaturen bieten spezifische, konfigurierbare Regeln, um den Schutz Ihrer Websites vor bekannten Angriffen zu vereinfachen. Eine Signatur stellt ein Muster dar, das Bestandteil eines bekannten Angriffs auf ein Betriebssystem, einen Webserver, eine Website, einen XML-basierten Webdienst oder eine andere Ressource ist. Um Ihre Anwendung mithilfe von Signaturen zu schützen, müssen Sie die Regeln überprüfen, aktivieren und konfigurieren, die Sie anwenden möchten.

Um Datenschutzverletzungen zu verhindern und den richtigen Sicherheitsschutz in der Anwendung zu gewährleisten, müssen Sie ebenfalls ein WAF-Profil mit Sicherheitsüberprüfungen erstellen. Wenn Sie ein WAF-Profil in der NetScaler-Instanz erstellen, kann der Datenverkehr:

- Lassen Sie sich mit den genannten Sicherheitsüberprüfungen generieren
- Wird nicht mit den genannten Sicherheitsüberprüfungen generiert

Die Instanz empfängt möglicherweise andere Angriffe, aber Sie haben diese Sicherheitsüberprüfung möglicherweise nicht in den WAF-Profilen aktiviert.

Als Administrator müssen Sie verstehen, um die richtigen Signaturen zu aktivieren und die richtigen WAF-Profile zum Schutz der Webanwendung zu erstellen. Das Identifizieren der richtigen Signaturen und der WAF-Profile kann in einigen Szenarien eine schwierige Aufgabe sein.

Die WAF-Empfehlung von NetScaler Console scannt die Anwendung auf Sicherheitslücken und generiert die folgenden Empfehlungen:

- WAF-Profil
- WAF Signatur

Weitere Informationen finden Sie unter WAF-Profil und WAF-Signaturen.

Die WAF-Empfehlungsdatenbank wird regelmäßig aktualisiert, um neue Schwachstellen aufzunehmen. Sie können scannen und dann auswählen, um die erforderlichen Empfehlungen zu aktivieren. Sie können alle Signaturen und Sicherheitsprüfungen aktivieren, dies kann jedoch zu Fehlalarmen führen und die Leistung der NetScaler-Instanz beeinträchtigen. Daher wird empfohlen, nur die erforderlichen Sicherheitsüberprüfungen und Signaturen auszuwählen. Die WAF-Empfehlungs-Engine erkennt auch automatisch, welche Signaturen und Sicherheitsüberprüfungen für die Anwendung aktiviert werden müssen.

> **Hinweis**
>
> Die NetScaler-Instanz muss **13.0 41.28 oder** höher (für Sicherheitsüberprüfungen) und **13.0 oder** höher (für Signaturen) sein.

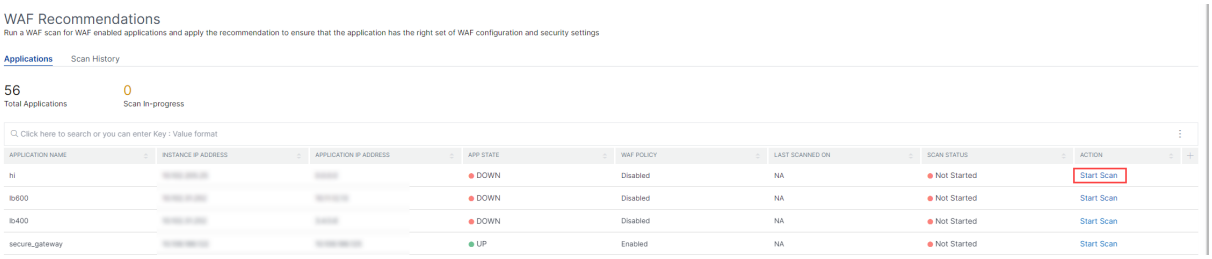
Voraussetzungen

Die Anwendungen:

- Muss die Premium-Lizenz haben.
- Muss der virtuelle Lastausgleichsserver sein.

Konfigurieren der WAF-Scaneinstellungen

Navigieren Sie in der NetScaler Console zu **Sicherheit > WAF-Empfehlung** und klicken Sie unter **Anwendungen** auf **Scan starten** , um die WAF-Scaneinstellungen für eine Anwendung zu konfigurieren.

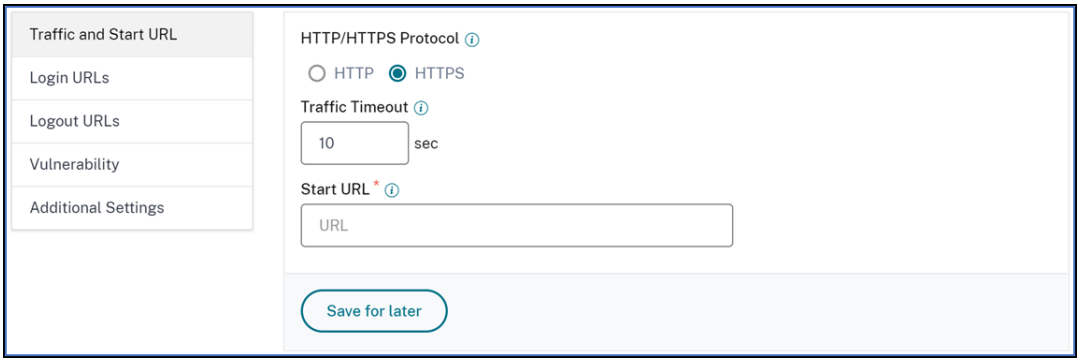


Auf der Seite WAF-Empfehlungen:

- **Domänenname** —Geben Sie den öffentlich zugänglichen/öffentlich erreichbaren Domänennamen an, der mit dem Anwendungs-VIP verknüpft ist. Beispiel: `www.example.com`.

  > Hinweis
  >
  > Start-URL, Anmelde-URL und Abmelde-URL müssen mit der angegebenen Domäne übereinstimmen.

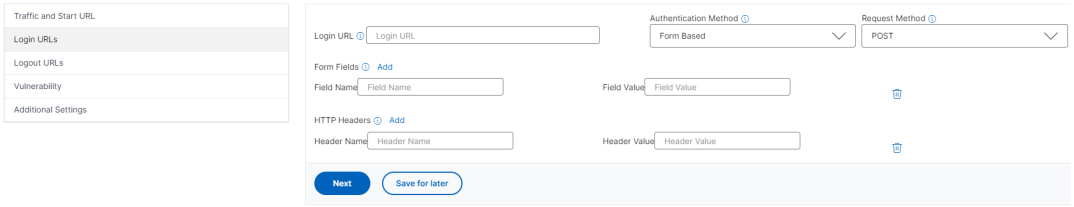
- **Datenverkehr und Start-URL** —Geben Sie die URL-Details der Anwendung (Server) an.
  - **HTTP-/HTTPS-Protokoll** —Wählen Sie das Protokoll der Anwendung aus.
  - **Traffic Timeout** —Die Wartezeit (in Sekunden) für eine einzelne Anfrage während des Scans. Der Wert muss größer als 0 sein.
  - **Start-URL** —Die Startseite der Anwendung, um den Scan zu starten. Beispiel: `https://www.example.com/home`. Die URL muss eine gültige IPv4-Adresse sein. Wenn die IP-Adressen privat sind, müssen Sie sicherstellen, dass auf die private IP-Adresse von der NetScaler Console-Verwaltungs-IP aus zugegriffen werden kann.



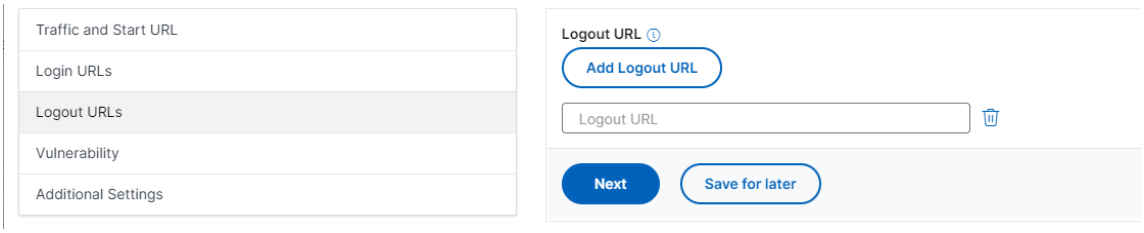
- **Anmelde-URLs** —Geben Sie die Anmeldeinformationen und ggf. URLs für den Zugriff auf die Anwendung an.
  - **Anmelde-URL** —Die URL, an die die Anmeldedaten zur Authentifizierung gesendet werden. In HTML wird diese URL allgemein als Aktions-URL bezeichnet.
  - **Authentifizierungsmethode** —Wählen 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.

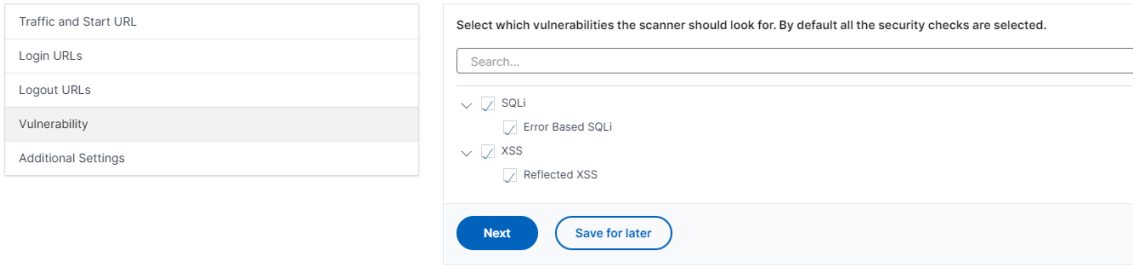
- **Anforderungsmethode** —Wählen Sie die HTTP-Methode, die beim Senden von Formulardaten an die Anmelde-URL Die zulässigen Anforderungsmethoden sind POST, GETund PUT.
- **Formularfelder** —Geben Sie die Formulardaten an, die an die Anmelde-URL gesendet werden sollen Formularfelder sind nur erforderlich, 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 die Schaltfläche Hinzufügen klicken, um mehrere Formularfelder hinzuzufügen. Zum Beispiel Feldname —Benutzername und Feldwert —admin.
- **HTTP-Header** —Die HTTP-Header sind möglicherweise erforderlich, damit die Anmeldung erfolgreich ist. Sie müssen in den Schlüssel-Wert-Paaren angeben, wobei Header-Name der Schlüssel und Header-Wert der Wert ist. Sie können auf die Schaltfläche Hinzufügen klicken, um mehrere HTTP-Header hinzuzufügen. Einer der am häufigsten benötigten HTTP-Header ist der Content-Type-Header.



- **Abmelde-URLs** —Geben Sie die URL an, die die Sitzung nach dem Zugriff beendet. Beispiel: `https://www.example.com/customer/logout`.

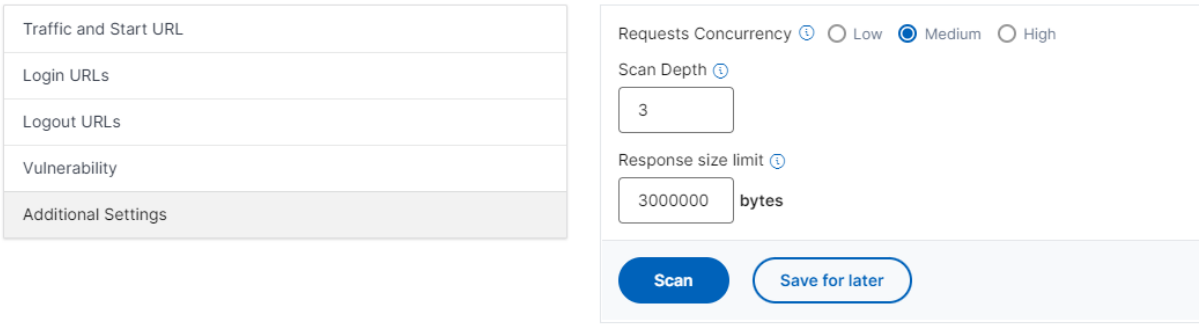


- **Sicherheitsanfälligkeit** —Wählen Sie die Sicherheitslücken aus, die der Scanner erkennen soll. Derzeit wird dies für Verstöße gegen SQL Injection und Cross-Site-Skripting durchgeführt. Standardmäßig sind alle Verstöße ausgewählt. Nach Auswahl der Schwachstellen werden diese Angriffe auf die Anwendung 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.



- **Zusätzliche Einstellungen**
  - **Parallelität** von Anfragen —Die Gesamtzahl der parallel an die Webanwendung gesendeten Anforderungen.
  - **Scantiefe** - Die Tiefe der Webanwendung, bis zu der der Scan fortgesetzt werden muss. Bei einer Scantiefe von Wert 2 werden beispielsweise die Start-URL und alle in dieser URL gefundenen Links gescannt. Sie müssen einen Wert größer oder gleich 1 angeben.
  - **Größenbeschränkung der Antwort** —Die maximale Grenze für die Antwortgröße. Antworten, die über den genannten Wert hinausgehen, werden nicht gescannt. Der empfohlene Grenzwert liegt bei 3 MB (300000 Byte).

Die Konfiguration der WAF-Scaneinstellungen ist abgeschlossen. Sie können auf **Scannen** klicken, um den Scanvorgang zu starten, oder Sie können auf **Für später speichern** klicken, um die Konfigurationen zu speichern und später zu scannen.



Empfehlungsprozess für WAF-Scans

Wenn Sie den Scan starten, führt das WAF-Empfehlungsmodul folgende Schritte aus:

- Scannt die bereitgestellte Webanwendung über die angegebene URL.
- Untersucht die Webanwendung, um die von der Webanwendung verwendeten Technologien zu ermitteln.
- Simuliert Sicherheitsangriffe auf die Webanwendung, um potenzielle Schwachstellen zu erkennen.

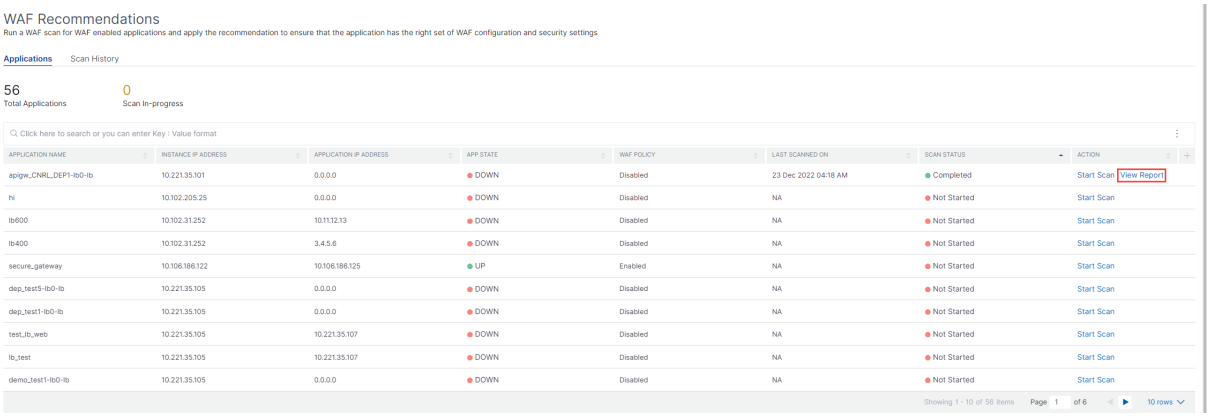
- Empfiehlt Signaturen basierend auf den erkannten Webtechnologien.
- Empfiehlt Sicherheitsüberprüfungen basierend auf gefundenen Schwachstellen und der Analyse des Datenverkehrs.
- Analysiert die Antworten der Webanwendung, um detailliertere Einstellungen zu generieren.

Die folgenden Sicherheitsüberprüfungen werden unterstützt:

- Pufferüberlauf
- Feld-Formate
- Kreditkarte
- Konsistenz von Cookies
- HTML-SQL-Injektion
- Site-übergreifendes HTML-S
- Konsistenz von Formularfeldern
- CSRF-Formular-Tagging

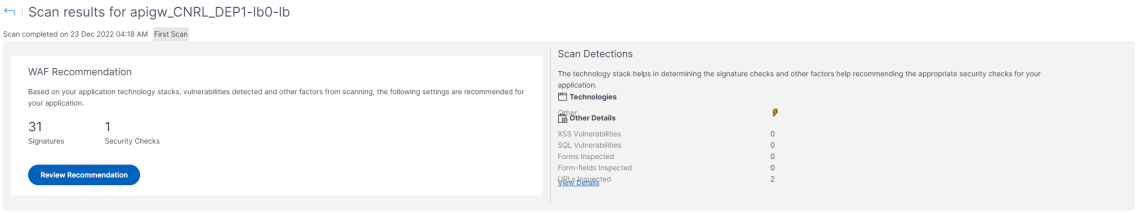
Scan-Bericht anzeigen

Klicken Sie nach Abschluss des Scans auf **Bericht anzeigen**, um die Ergebnisse anzuzeigen.



Das Scan-Ergebnis liefert:

- **WAF-Empfehlung** —Ermöglicht das Anzeigen der Zusammenfassung der gesamten für die Anwendung empfohlenen Signaturen und Sicherheitsüberprüfungen.
- **Scan-Erkennungen** —Ermöglicht das Anzeigen der Sammlung von Informationen wie Technologien und Details zu Verstößen, die in der Anwendung ausgeführt wurden. Klicken Sie auf **Details anzeigen**, um die Informationen zu den Erkennungen und andere Details des Scans anzuzeigen.



Klicken Sie unter **WAF-Empfehlung**auf **Empfehlung überprüfen**, um die Details für **Sicherheitsüberprüfungen** und **Signaturen**anzuzeigen.

Die empfohlenen Sicherheitseinstellungen schlagen die empfohlenen Sicherheitsüberprüfungen und Signaturen für die Anwendung vor. Sie können die Empfehlungen in der Liste bearbeiten und auf **Anzeigen oder Bearbeiten** klicken, um Details anzuzeigen oder Änderungen entsprechend den Anforderungen zu bearbeiten. Mit Auf Standard zurücksetzen werden alle vorgenommenen Änderungen zurückgesetzt und die ursprünglichen Empfehlungen wiederhergestellt.

Klicken Sie nach Überprüfung der Details auf **Empfehlung anwenden**. Die Empfehlungen werden mit den StyleBooks konfiguriert. Sie müssen sicherstellen, dass die Empfehlungen auf den Registerkarten **Sicherheitsüberprüfungen** und **Signatur** separat angewendet werden.

Es wird empfohlen, zuerst die Signaturen und dann die Sicherheitsüberprüfungen anzuwenden. Dadurch werden die Signaturen automatisch an das Profil gebunden.

Wenn Sie Signaturen erfolgreich anwenden:

- Die Konfiguration wird über das StyleBook auf die NetScaler-Instanz angewendet`appfw-import-object`.
- Die Signaturdatei mit den konfigurierten Empfehlungen wird in die NetScaler-Instanz importiert.

> **Hinweis**
>
> Signaturen werden in NetScaler 13.0 oder einer höheren Version unterstützt.

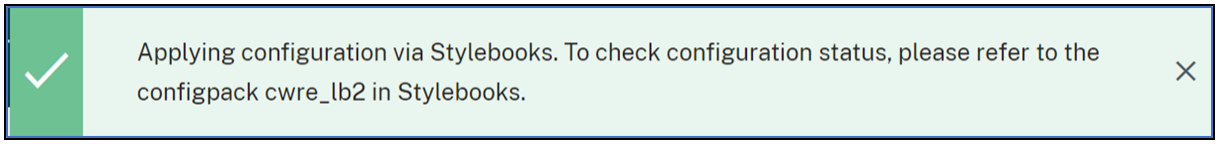
Bevor Sie mit dem Anwenden der **Sicherheitsprüfungsempfehlungen** fortfahren, navigieren Sie zu **Anwendungen > Konfiguration > Konfigurationspakete** und stellen Sie sicher, dass das Signature-Configpack erfolgreich erstellt wurde.

Wenn Sie Sicherheitsüberprüfungen erfolgreich durchführen:

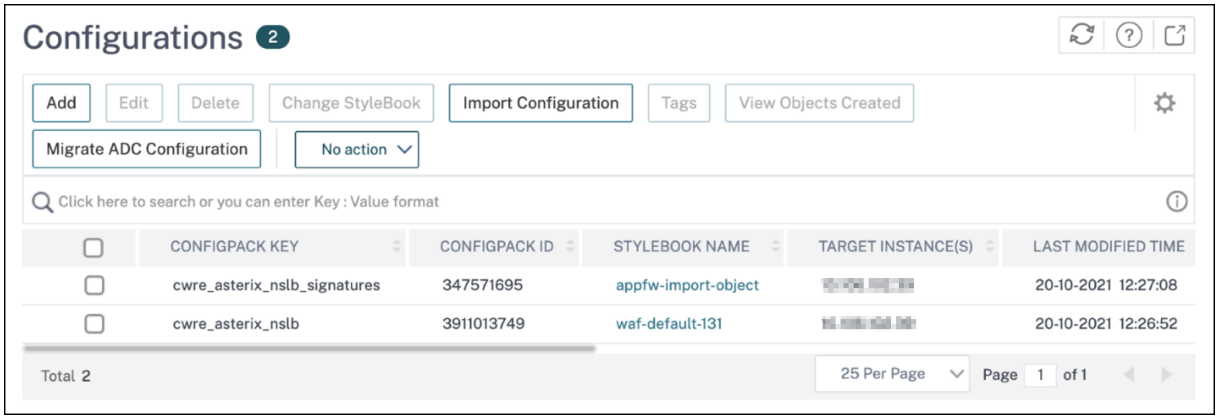
- Die Konfiguration wird je nach NetScaler-Version über StyleBooks auf die NetScaler-Instanz angewendet. Für NetScaler 13.0 wird `waf-default-130`StyleBook verwendet und für NetScaler 13.1 wird `waf-default-131`Stylebook verwendet.
- Das Profil `Appfw` wird auf Ihrem NetScaler erstellt und mithilfe von `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.

Nachdem Sie die Empfehlung (Sicherheitsüberprüfungen und Signaturen) angewendet haben, können Sie die folgende Bestätigungsmeldung anzeigen:



Sie können überprüfen, ob die WAF-Profile und -Signaturen über die Standard-StyleBooks angewendet werden, indem Sie zu **Anwendungen > Konfiguration > Config Packs**navigieren.



Gateway Insight

March 12, 2024

In einer NetScaler Gateway-Bereitstellung ist der Einblick in die Details zum Benutzerzugriff für die Behebung von Zugriffsfehlern unerlässlich Als Netzwerkadministrator möchten Sie wissen, wann ein Benutzer nicht in der Lage ist, sich bei NetScaler Gateway anzumelden, und Sie möchten die Benutzeraktivität und die Gründe für den Anmeldefehler kennen, diese Informationen sind jedoch in der Regel nur verfügbar, wenn der Benutzer eine Anforderung zur Lösung sendet.

Gateway Insight bietet Einblick in die Fehler, die bei der Anmeldung bei 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 Gesamtzahl der Bytes und die von den Anwendungen verbrauchte Bandbreite anzeigen. Sie können Details der Benutzer, Sitzungen, Bandbreite und Startfehler für eine Anwendung anzeigen.

Sie können jederzeit die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die Gesamtzahl der Byte und die Bandbreite anzeigen, die von allen Gateways verwendet werden, die einem NetScaler Gateway-Gerät zugeordnet sind. 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 Console-Datenbank gespeichert, sodass Sie Fehlerdetails für jeden Zeitraum anzeigen können. Sie können auch eine Zusammenfassung der Anmeldefehler anzeigen und feststellen, in welcher Phase des Anmeldevorgangs ein Fehler aufgetreten ist.

Wichtige Hinweise:

- Gateway Insight wird in den folgenden Bereitstellungen unterstützt:
  - Access Gateway
  - Unified Gateway

- Die Version und der Build der NetScaler Console müssen mit der NetScaler Gateway-Appliance identisch oder später sein.
- Eine Stunde Gateway Insight-Berichte können für NetScaler Instanzen mit Advanced-Lizenz angezeigt werden. Eine Premium-Lizenz ist erforderlich, um Berichte von Gateway Insight über eine Stunde hinaus anzuzeigen.

Einschränkungen:

- NetScaler Gateway unterstützt Gateway Insight nicht, wenn die Authentifizierungsmethode als zertifikatbasierte Authentifizierung konfiguriert ist.
- Erfolgreiche Benutzeranmeldungen, Latenz und Details auf Anwendungsebene für virtuelle ICA-Anwendungen und -Desktops sind nur auf dem HDX Insight User-Dashboard sichtbar.
- In einem Double-Hop-Modus sind Fehler auf der NetScaler Gateway-Appliance in der zweiten DMZ nicht sichtbar.
- Probleme mit dem Remotedesktopprotokoll (RDP) -Desktop-Zugriff werden nicht gemeldet.
- Die Gateway Insight-Datensätze für die SAML-Authentifizierung werden nicht gemeldet.
- Gateway Insight wird für die folgenden Authentifizierungstypen unterstützt. Wenn ein anderer Authentifizierungstyp als diese verwendet wird, können Abweichungen in Gateway Insight auftreten.
  - Lokal
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - Natives OTP
  - OAuth

Gateway Insight aktivieren

Um Gateway Insight für Ihr NetScaler Gateway-Gerät zu aktivieren, müssen Sie das NetScaler Gateway-Gerät zuerst zur NetScaler Console hinzufügen. Anschließend müssen Sie AppFlow für den virtuellen Server aktivieren, der die VPN-Anwendung darstellt. Informationen zum Hinzufügen von Geräten zur NetScaler Console finden Sie unter Hinzufügen von Instanzen.

> **Hinweis**
>
> Um EPA-Fehler (Endpoint Analysis) in der NetScaler Console anzuzeigen, müssen Sie die AppFlow-Authentifizierung, Autorisierung und Benutzernamenprotokollierung für die Zugriffskontrolle auf dem NetScaler Gateway-Gerät aktivieren .

Aktivieren Sie AppFlow für einen virtuellen Server in NetScaler Console

1. Navigieren Sie zu **Einstellungen > Lizenzierung und Analytics-Konfiguration**.
2. Klicken Sie unter **Virtual Server Analytics-Zusammenfassung**auf **Analytics konfigurieren**.
3. Wählen Sie auf der Seite **Alle virtuellen Server** den virtuellen NetScaler Gateway-Server aus und klicken Sie auf **Security & Analytics aktivieren**.
4. Wählen Sie **Gateway Insight**.
5. Klicken Sie auf **Speichern**.

Aktivieren Sie die AppFlow-Benutzernamenprotokollierung auf einem NetScaler Gateway-Gerät mithilfe der GUI

1. Navigieren Sie zu **Konfiguration > System > AppFlow > Einstellungen**, und klicken Sie dann auf **AppFlow Einstellungen ändern**.
2. Wählen **Sie im Bildschirm AppFlow-Einstellungen konfigurieren** die Option **AAA-Benutzername**aus, und klicken Sie dann auf **OK**.

Anzeigen von Gateway Insight-Berichten

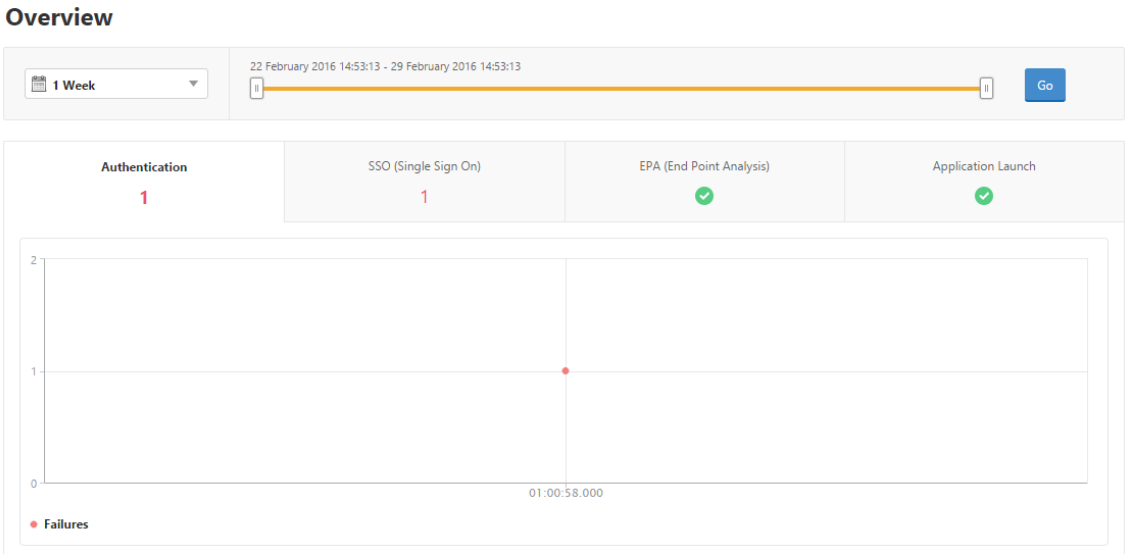
In der NetScaler Console können Sie Berichte für alle Benutzer, Anwendungen und Gateways anzeigen, die den NetScaler Gateway-Geräten zugeordnet sind, und Sie können Details für einen bestimmten Benutzer, eine bestimmte Anwendung oder ein bestimmtes Gateway anzeigen. Im Abschnitt **Überblick** können Sie die Fehler EPA, SSO, Authentifizierung und Application Launch anzeigen. Sie können auch eine Zusammenfassung der verschiedenen Sitzungsmodi anzeigen, die von Benutzern für die Anmeldung verwendet werden, die Clienttypen und die Anzahl der stündlich angemeldeten Benutzer.

> **Hinweis:**
>
> Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, Zugriff auf Anwendungsebene für die Gruppe gewähren und der Gruppe Benutzer zuweisen. Die NetScaler Console-Analytik 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 zu Gruppen finden Sie unter Konfigurieren von Gruppen in der NetScaler Console.

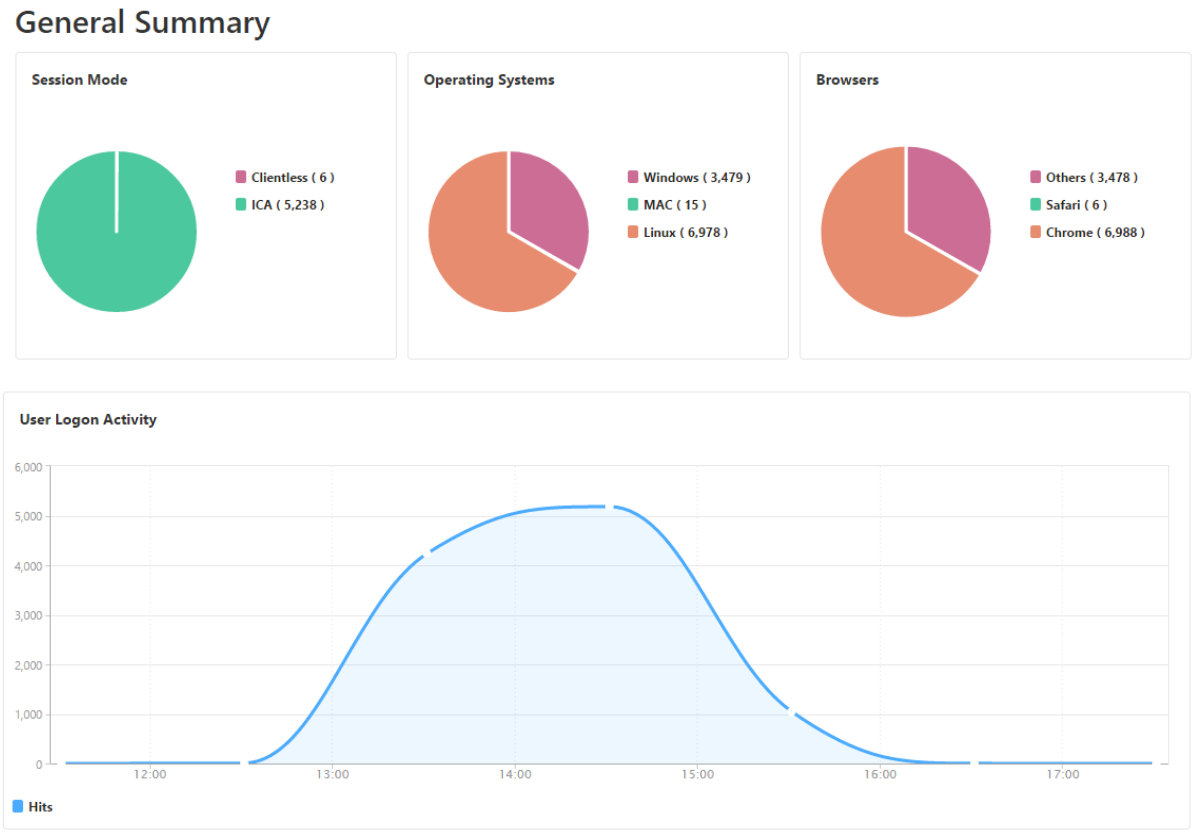
Anzeigen von EPA-, SSO, Authentifizierung, Autorisierung und Anwendungsstartfehlern

1. Navigieren Sie in der NetScaler Console 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.



Zusammenfassung der Sitzungsmodi, Clients und der Anzahl der Benutzer anzeigen

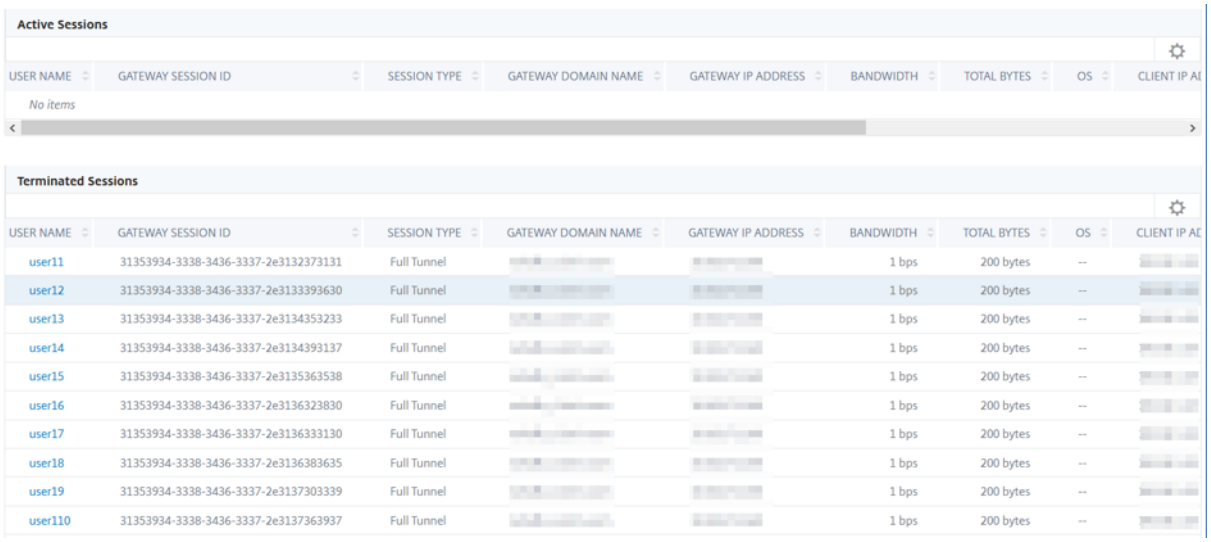
Navigieren Sie in der NetScaler Console zu **Gateway > Gateway Insight** und scrollen Sie nach unten, um die Berichte anzuzeigen.



Benutzer

Sie können einen vollständigen Bericht für die Benutzer anzeigen, die den NetScaler Gateway-Appliances zugeordnet sind. Sie können die EPA, Authentifizierung, SSO, Fehler beim Start von Anwendungen usw. für einen Benutzer anzeigen.

Sie können auch eine konsolidierte Ansicht aller aktiven und beendeten Sitzungen des Benutzers visualisieren.

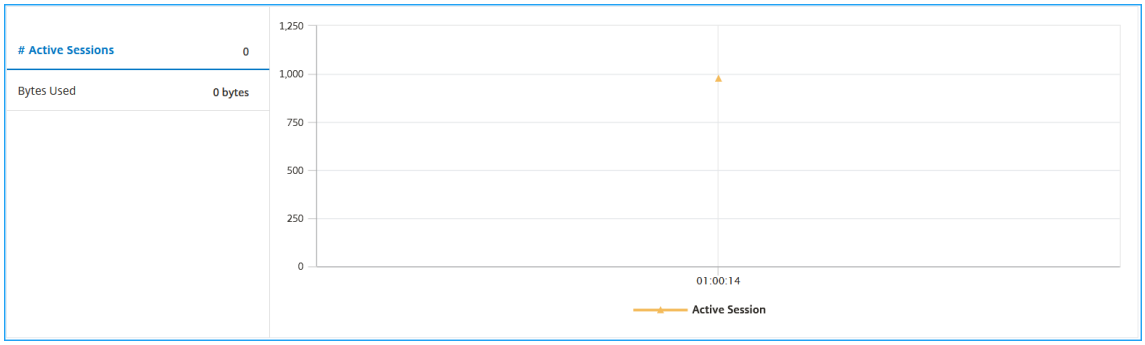


Als Administrator ermöglicht Ihnen diese Ansicht Folgendes:

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

Benutzerdetails anzeigen

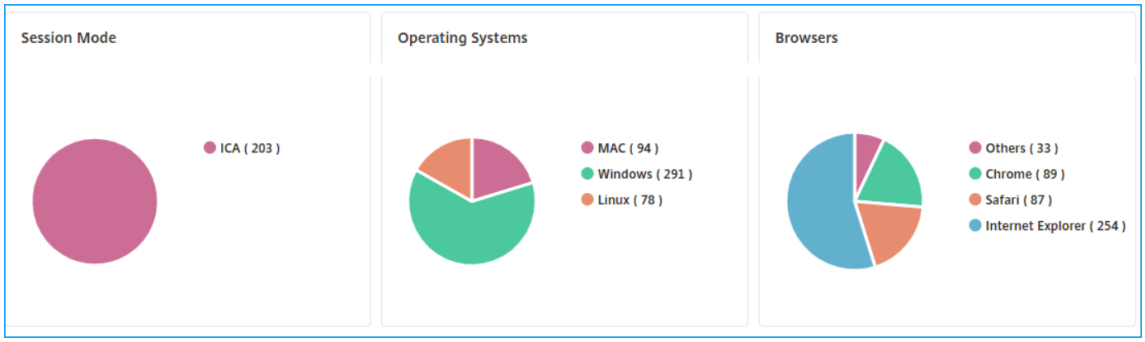
1. Navigieren Sie in der NetScaler Console zu **Gateway > Gateway Insight > Users** .
2. Wählen Sie den Zeitraum aus, für den Sie die Benutzerdetails anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.
3. Sie können die Anzahl der aktiven Benutzer, die Anzahl der aktiven Sitzungen und Bytes von allen Benutzern während des Zeitraums anzeigen.



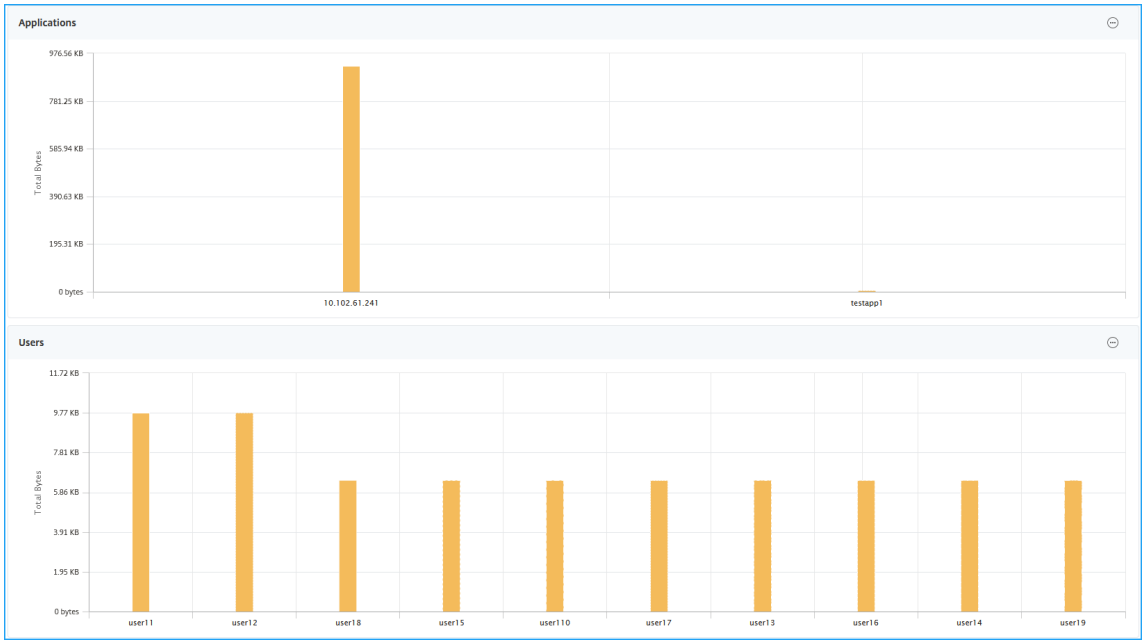
Scrollen Sie nach unten, um eine Liste der verfügbaren Benutzer und aktiven Benutzer anzuzeigen.

Klicken Sie auf der Registerkarte **Benutzer** oder **Aktive Benutzer** auf einen Benutzer, um die folgenden Benutzerdetails anzuzeigen:

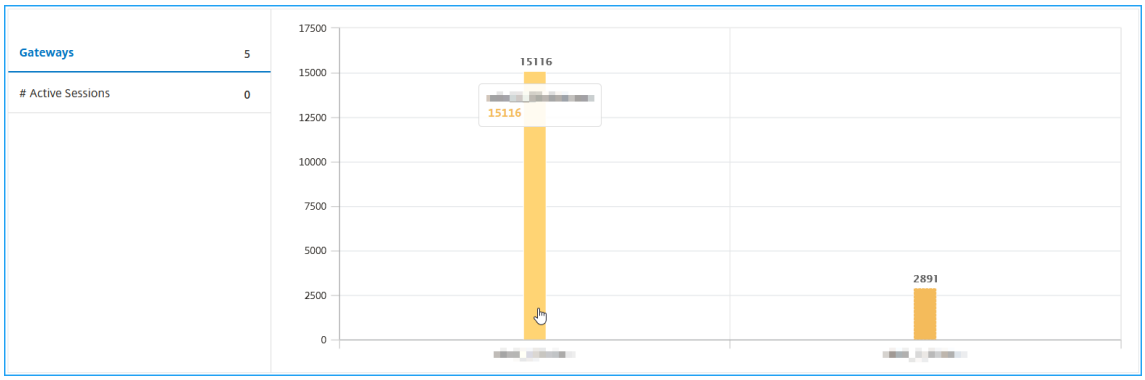
- **Benutzerdetails**—Sie können Einblicke für jeden Benutzer anzeigen, der mit den NetScaler Gateway-Appliances verknüpft ist. Navigieren Sie zu **Gateway** > **Gateway Insight** > **Users** und klicken Sie auf einen Benutzer, um Informationen für den ausgewählten Benutzer wie Sitzungsmodus, Betriebssystem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



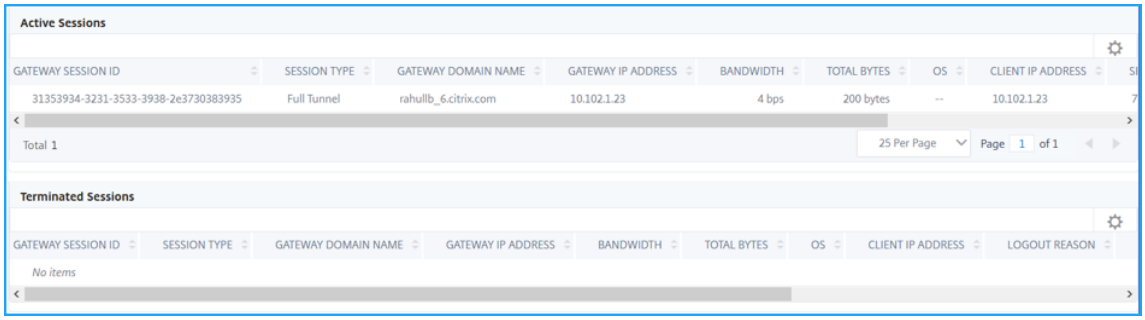
- **Benutzer und Anwendungen für das ausgewählte Gateway** —Navigieren Sie zu **Gateway** > **Gateway Insight** > **Gateway** und klicken Sie auf einen Gateway-Domänennamen, um die Top 10 Anwendungen und Top 10 Benutzer anzuzeigen, die mit dem ausgewählten Gateway verknüpft sind.



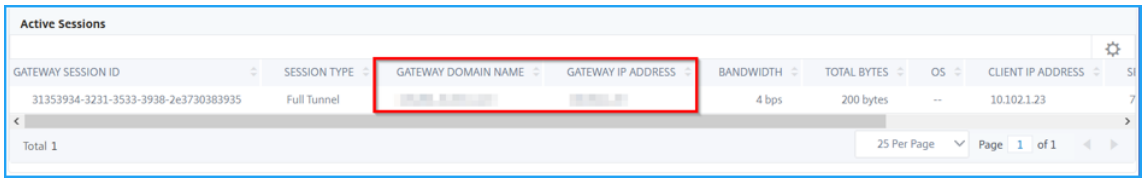
- **Weitere Optionen für Anwendungen und Benutzer anzeigen** —Für mehr als 10 Anwendungen und Benutzer können Sie auf das Mehr-Symbol in Anwendungen und Benutzer klicken, um alle Benutzer- und Anwendungsdetails anzuzeigen, die mit dem ausgewählten Gateway verknüpft sind.
- **Zeigen Sie Details an, indem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



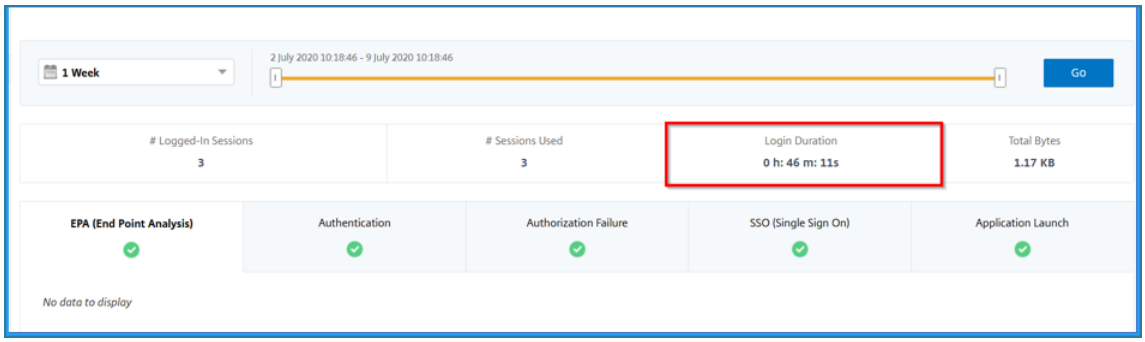
- **Active Sessions** und **Terminated Sessions** der Benutzer.



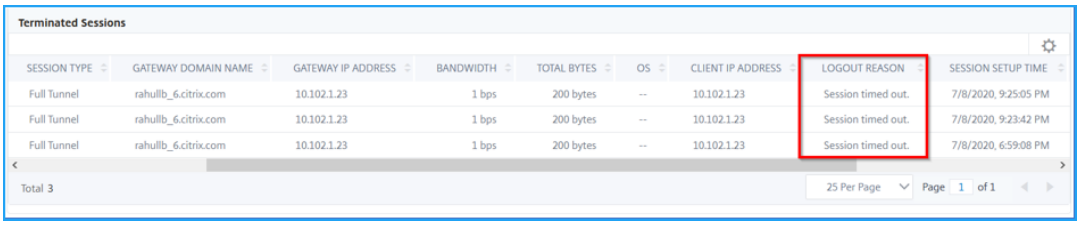
- Der Gateway-Domänenname und die Gateway-IP-Adresse in **Active Sessions**



- Die Dauer der Benutzeranmeldung.



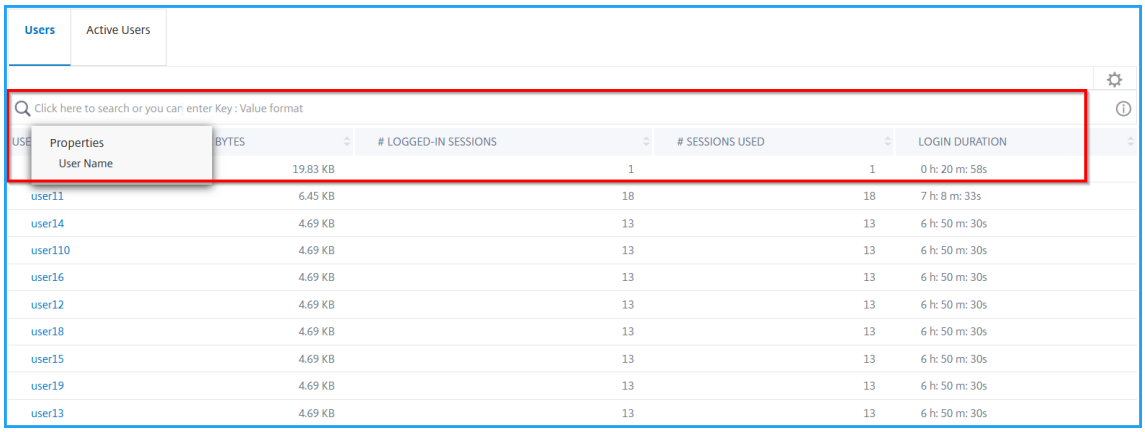
- Der Grund für die Logout-Sitzung des Benutzers. Die Gründe für die Abmeldung können sein:
  - Zeitüberschreitung der Sitzung
  - Ausgeloggt wegen internem Fehler
  - Abgemeldet wegen zeitlich abgelaufenen inaktiven Sitzungen
  - Der Benutzer hat sich abgemeldet
  - Der Administrator hat die Sitzung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



Suchleiste und Geokartenansicht

Sie können Folgendes anzeigen:

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



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

  1. Navigieren Sie zu **Gateway > Gateway Insight**, um die Geokarte anzuzeigen
  2. Klicken Sie auf ein Land. Zum Beispiel United States

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

Anwendungen

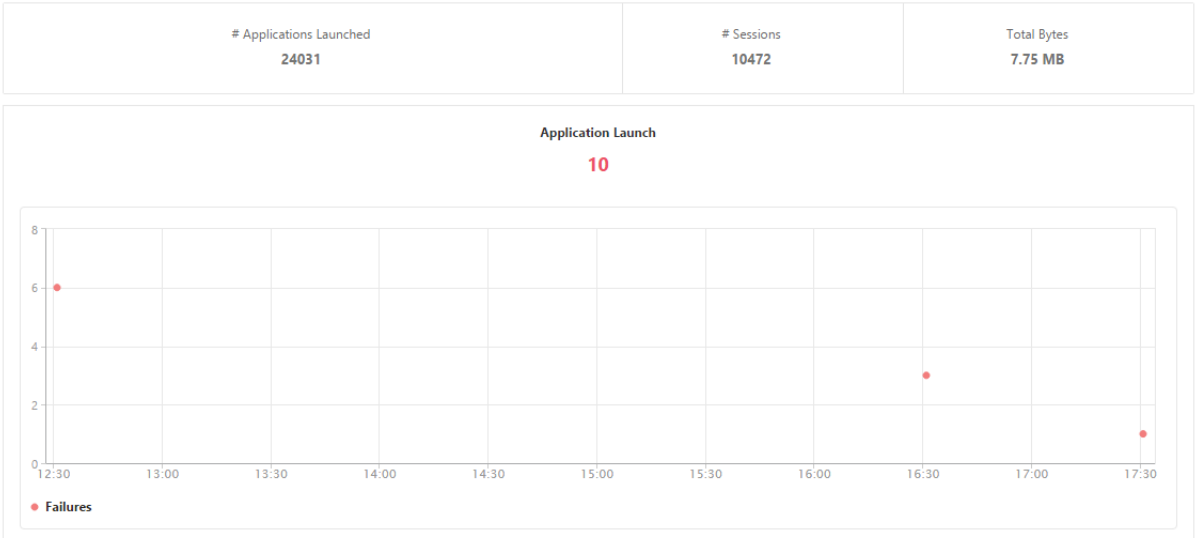
Sie können die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen, die Gesamtzahl der Bytes und die von den Anwendungen verbrauchte Bandbreite anzeigen. Sie können Details der Benutzer, Sitzungen, Bandbreite und Startfehler für eine Anwendung anzeigen.

Anwendungsdetails anzeigen

1. Navigieren Sie in der NetScaler Console 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 nun die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen, die Anzahl der Gesamtbytes und die Bandbreite der Anwendungen anzeigen.



Führen Sie einen Bildlauf nach unten durch, um die Anzahl der Sitzungen, Bandbreite und Gesamtbytes anzuzeigen, die von ICA und anderen Anwendungen belegt werden.

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

Auf der Registerkarte **Andere Anwendungen** können Sie in der Spalte **Name** auf eine Anwendung klicken, um Details zu dieser Anwendung anzuzeigen.

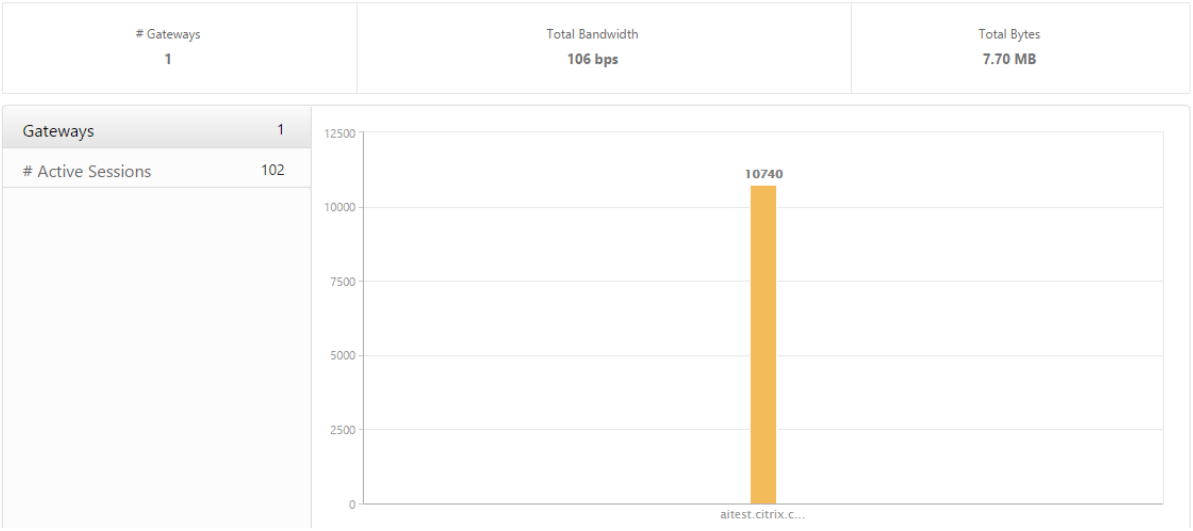
Gateways

Sie können die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die Gesamtzahl der Byte und die Bandbreite anzeigen, die von allen Gateways verwendet werden, die einem NetScaler Gateway-Gerät zugeordnet sind, zu einem bestimmten Zeitpunkt. 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.

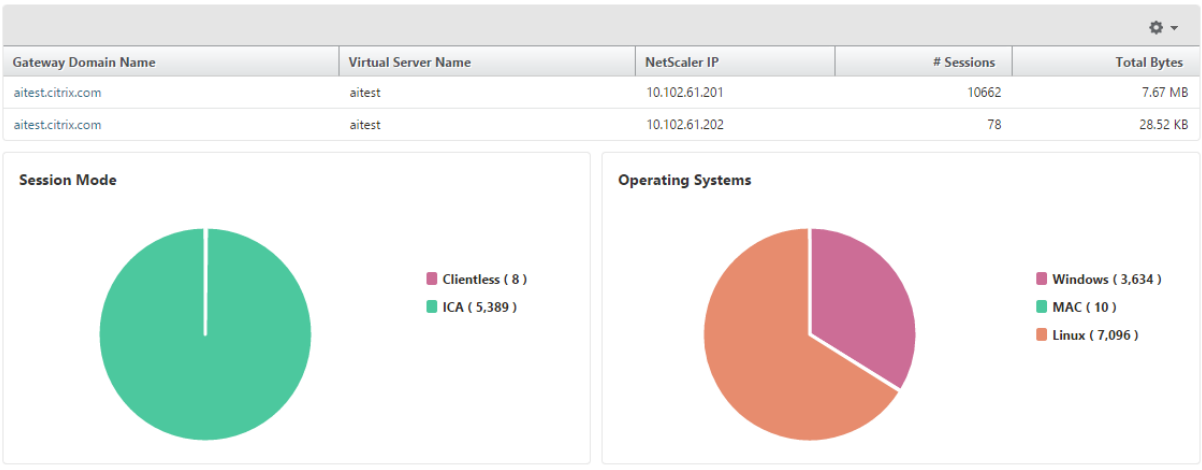
Gatewaydetails anzeigen

1. Navigieren Sie in der NetScaler Console 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 jederzeit die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die Gesamtzahl der Byte und die Bandbreite anzeigen, die von allen Gateways verwendet werden, die einem NetScaler Gateway-Gerät zugeordnet 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.

Sie können auch eine Geomap für Gateways anzeigen, mit der Sie Benutzer basierend auf einem bes-

timmten Standort filtern können.

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

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

Exportieren von Berichten

Sie können die Gateway Insight-Berichte mit allen in der GUI angezeigten Details im PDF-, JPEG-, PNG- oder CSV-Format auf Ihrem lokalen Computer speichern. Sie können auch den Export der Berichte an bestimmte E-Mail-Adressen in verschiedenen Intervallen planen.

> **Hinweis**
>
> - Benutzer mit schreibgeschütztem Zugriff können keine Berichte exportieren.
> - Geomap-Berichte werden nur exportiert, wenn die NetScaler Console über eine Internetverbindung verfügt.

Exportieren eines Berichts

1. Klicken Sie auf der Registerkarte **Dashboard** im rechten Fensterbereich auf die Schaltfläche **Exportieren** .
2. Wählen Sie unter **Jetzt exportieren**das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.

So planen Sie den Export:

1. Klicken Sie auf der Registerkarte **Dashboard** im rechten Fensterbereich auf die Schaltfläche **Exportieren** .
2. Geben Sie unter **Export planen**die Details an und klicken Sie auf **Zeitplan**.

So bearbeiten Sie den Exportzeitplan:

1. Navigieren Sie auf der Registerkarte Konfiguration zu **Konfiguration** > **NetScaler Insight Center** > **Exportzeitpläne**.
2. Wählen Sie einen Bericht aus der verfügbaren Liste aus, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie nach der Bearbeitung auf **Speichern**.

> **Hinweis:**
>
> Konfigurieren Sie die E-Mail-Servereinstellungen, bevor Sie den Bericht planen, indem Sie zu **System** > **Benachrichtigungen** > **E-Mail** navigieren und auf **Hinzufügen**klicken.

So fügen Sie einen E-Mail-Server oder eine E-Mail-Verteilerliste hinzu:

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **Benachrichtigungen** > **E-Mail**.
2. Wählen Sie im rechten Bereich **E-Mail-Server**aus, um einen E-Mail-Server hinzuzufügen, oder wählen Sie **E-Mail-Verteilerliste**, 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.

1. Der Benutzer kann sich nicht am NetScaler Gateway-Gerät oder an den internen Webservern anmelden

Sie sind ein NetScaler Gateway-Administrator, der NetScaler Gateway-Appliances über die NetScaler Console überwacht, und Sie möchten herausfinden, warum sich ein Benutzer nicht anmelden kann oder in welcher Phase des Anmeldevorgangs der Fehler aufgetreten ist.

Mit der NetScaler Console können Sie die Fehlerdetails der Benutzeranmeldung in den folgenden Phasen des Anmeldevorgangs anzeigen:

- Authentifizierung
- Endpunktanalyse (EPA)
- Single Sign-On

In NetScaler Console 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 Console zu **Gateway > Gateway Insight** und geben Sie im Textfeld Nach **Benutzern suchen** den Benutzer an, den Sie suchen möchten.

Fehler bei der Authentifizierung

Sie können Authentifizierungsfehler wie falsche Anmeldeinformationen oder keine Antwort vom Authentifizierungsserver anzeigen. Wenn Sie die zweistufige Authentifizierung eingerichtet haben, können Sie sehen, ob die primäre, sekundäre oder beide Phasen der Authentifizierung fehlgeschlagen sind.

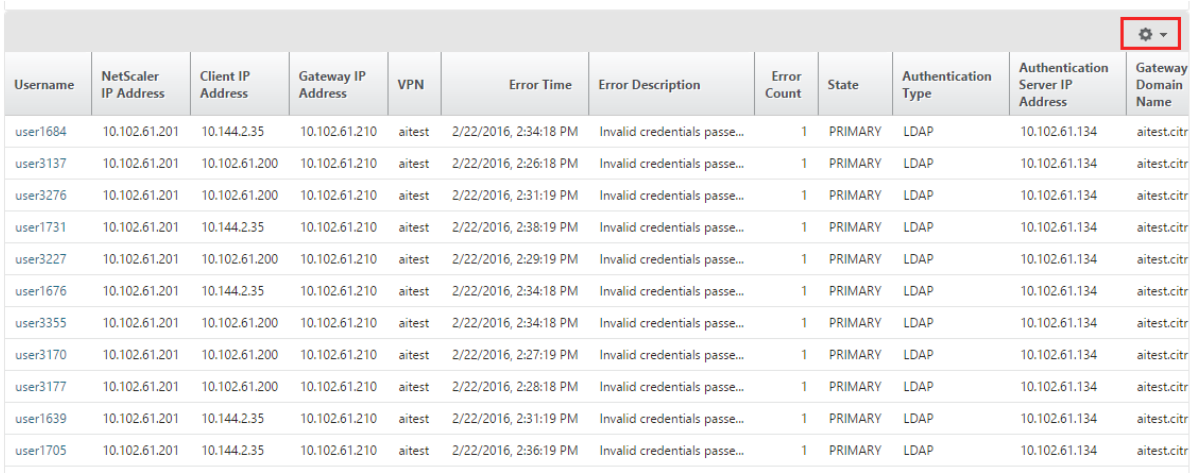
Details zum Authentifizierungsfehler anzeigen

1. Navigieren Sie in der NetScaler Console 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 angezeigt, in welchem Stadium einer zweistufigen Authentifizierung der Fehler aufgetreten ist.

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die Authentifizierungsfehler und andere Details für diesen Benutzer anzuzeigen.

Mithilfe der Einstellungsoption können Sie die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen.



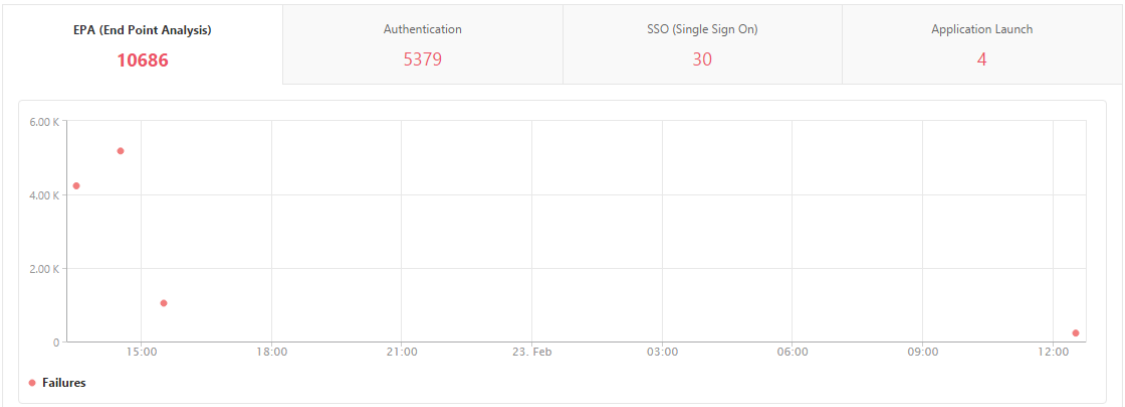
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

EPA-Ausfälle

Sie können EPA-Fehler in der Phase vor oder nach der Authentifizierung anzeigen.

Details zum EPA-Fehler anzeigen

1. Navigieren Sie in der NetScaler Console 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.

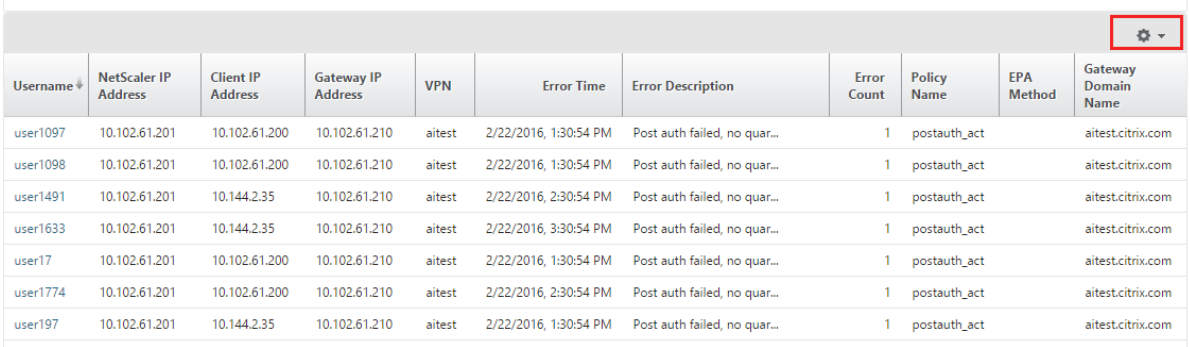


Scrollen Sie nach unten, um Details zu jedem EPA-Fehler wie **Benutzername, NetScaler-IP-Adresse, Gateway-IP-Adresse, VPN, Fehlerzeit, Richtlinienname, Gateway-Domainname** und mehr aus

der Tabelle auf derselben Registerkarte anzuzeigen. In der Spalte **Fehlerbeschreibung** in der Tabelle wird der Grund für den EPA-Fehler angezeigt, und in der Spalte **Richtlinienname** wird die Richtlinie angezeigt, die zum Fehler geführt hat.

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die EPA-Fehler und andere Details für diesen Benutzer anzuzeigen.

Mithilfe der Einstellungsoption können Sie die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

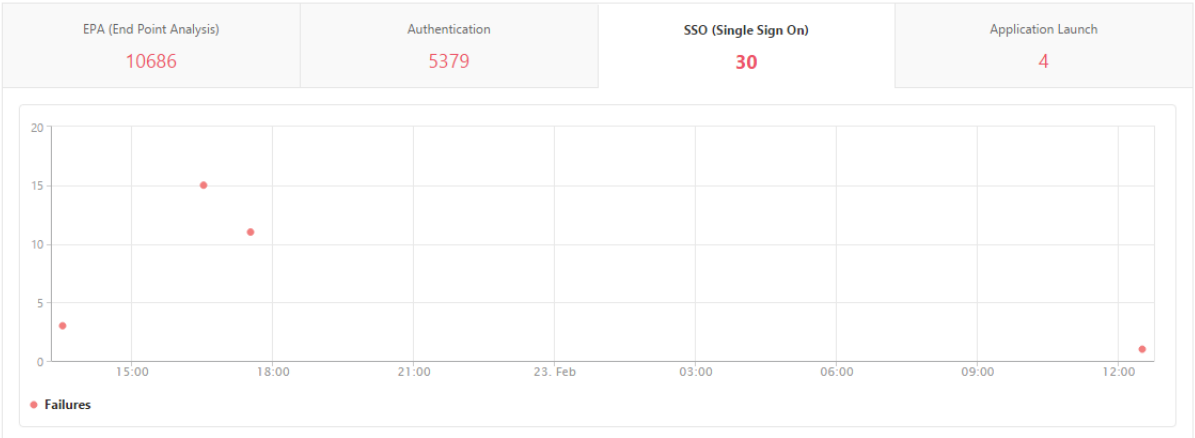
> **Hinweis**
>
> NetScaler Gateway meldet die EPA-Fehler nicht, wenn der Ausdruck "clientSecurity"als VPN-Sitzungsrichtlinienregel konfiguriert ist.

SSO-Fehler

Sie können zu jedem Zeitpunkt alle SSO-Fehler für einen Benutzer einsehen, der über die NetScaler Gateway-Appliance auf beliebige Anwendungen zugreift.

SSO-Fehlerdetails anzeigen

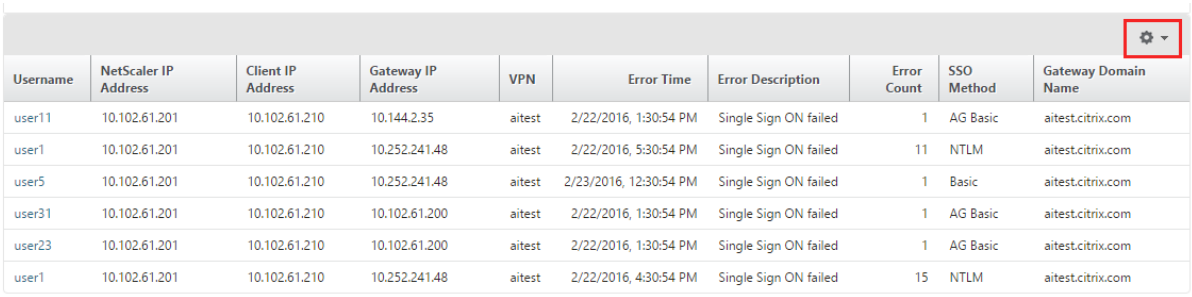
1. Navigieren Sie in der NetScaler Console zu **Gateway > Gateway Insight** .
2. Wählen Sie im Abschnitt Übersicht den Zeitraum aus, für den Sie die SSO-Fehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.
3. Klicken 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.

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die SSO-Fehler und andere Details für diesen Benutzer anzuzeigen.

Mithilfe der Einstellungsoption können Sie die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen.



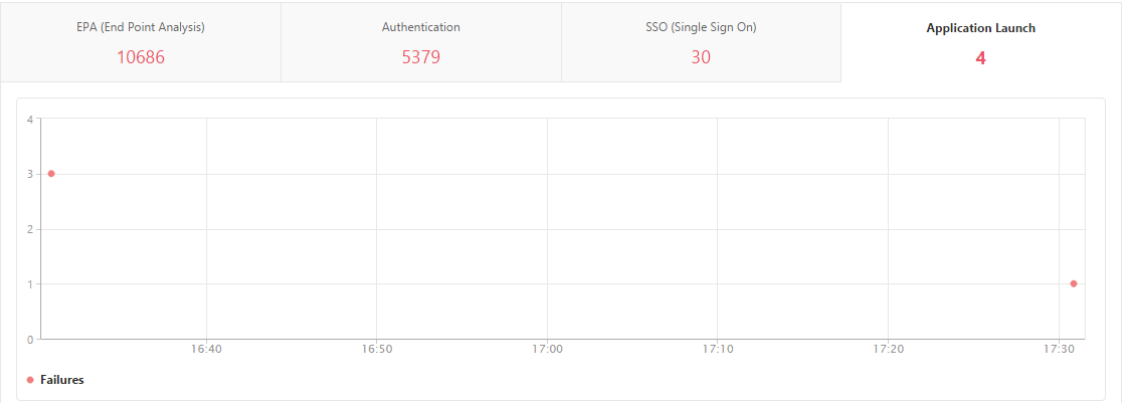
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

2. Nach erfolgreicher Anmeldung bei 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.

Details zum Anwendungsstart anzeigen

1. Navigieren Sie in der NetScaler Console 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**.

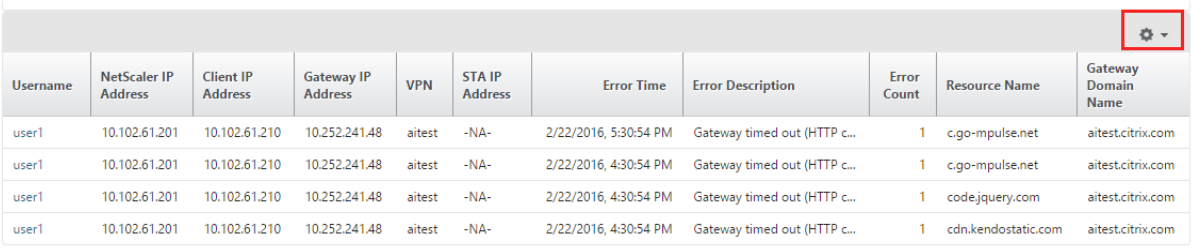
3. Klicken Sie auf die Registerkarte **Anwendungsstart**. Sie können die Anzahl der Anwendungsstartfehler zu einem bestimmten Zeitpunkt im Diagramm **Fehler** anzeigen.



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.

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die Programmstartfehler und andere Details für diesen Benutzer anzuzeigen.

Mithilfe der Einstellungsoption können Sie die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

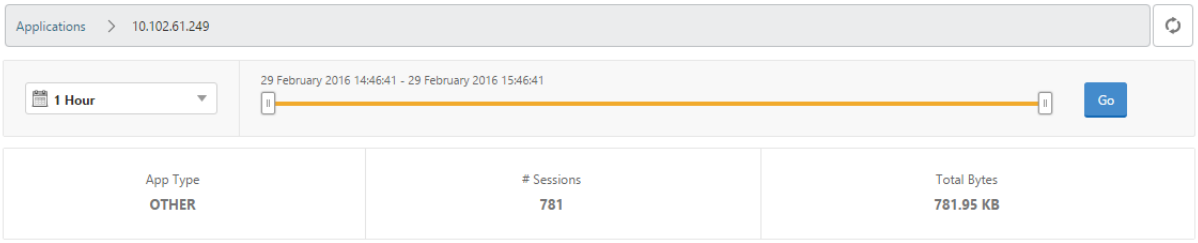
3. Nachdem eine neue Anwendung erfolgreich gestartet wurde, möchte ein Benutzer die Gesamtbytes und Bandbreite anzeigen, die von dieser Anwendung belegt wurden Nachdem Sie erfolgreich eine neue Anwendung gestartet haben, können Sie in NetScaler Console die Gesamtzahl der von dieser Anwendung verbrauchten Byte und Bandbreite anzeigen.

Anzeige der gesamten von einer Anwendung verbrauchten Byte und Bandbreite

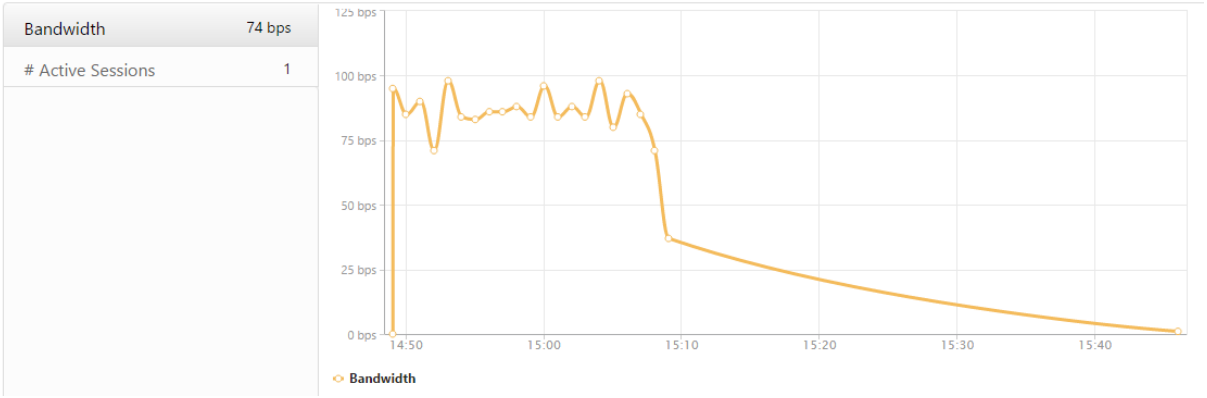
Navigieren Sie in der NetScaler Console zu **Gateway > Gateway Insight > Applications**, scrollen Sie nach unten und klicken Sie auf der Registerkarte **Andere** Anwendungen auf die Anwendung, für die

Sie die Details anzeigen möchten.

Sie können die Anzahl der Sitzungen und die Gesamtanzahl der Bytes anzeigen, die von dieser Anwendung belegt werden.



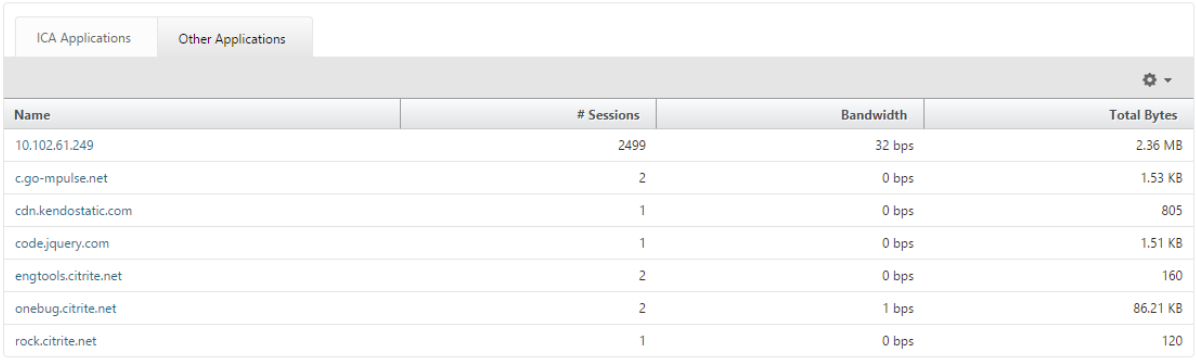
Sie können auch die von dieser Anwendung verbrauchte Bandbreite anzeigen.



4. Ein Benutzer hat sich erfolgreich bei 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.

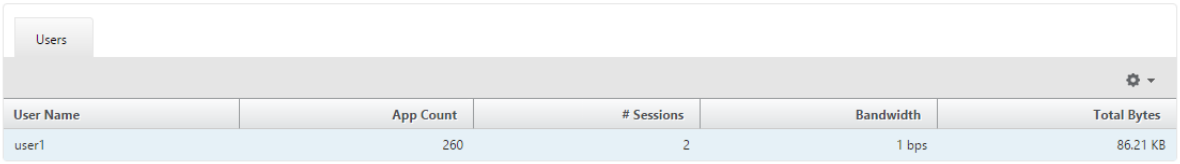
Anzeigen des Benutzerzugriffs für Ressourcen

1. Navigieren Sie in der NetScaler Console zu **Gateway > Gateway Insight > Applications** .
2. Wählen Sie auf dem angezeigten Bildschirm einen Bildlauf nach unten und auf der Registerkarte **Andere Anwendungen** die Anwendung aus, bei der sich der Benutzer nicht anmelden konnte.



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

Scrollen Sie auf dem angezeigten Bildschirm nach unten und in der Tabelle **Benutzer** alle Benutzer, die Zugriff auf diese Anwendung haben, angezeigt.

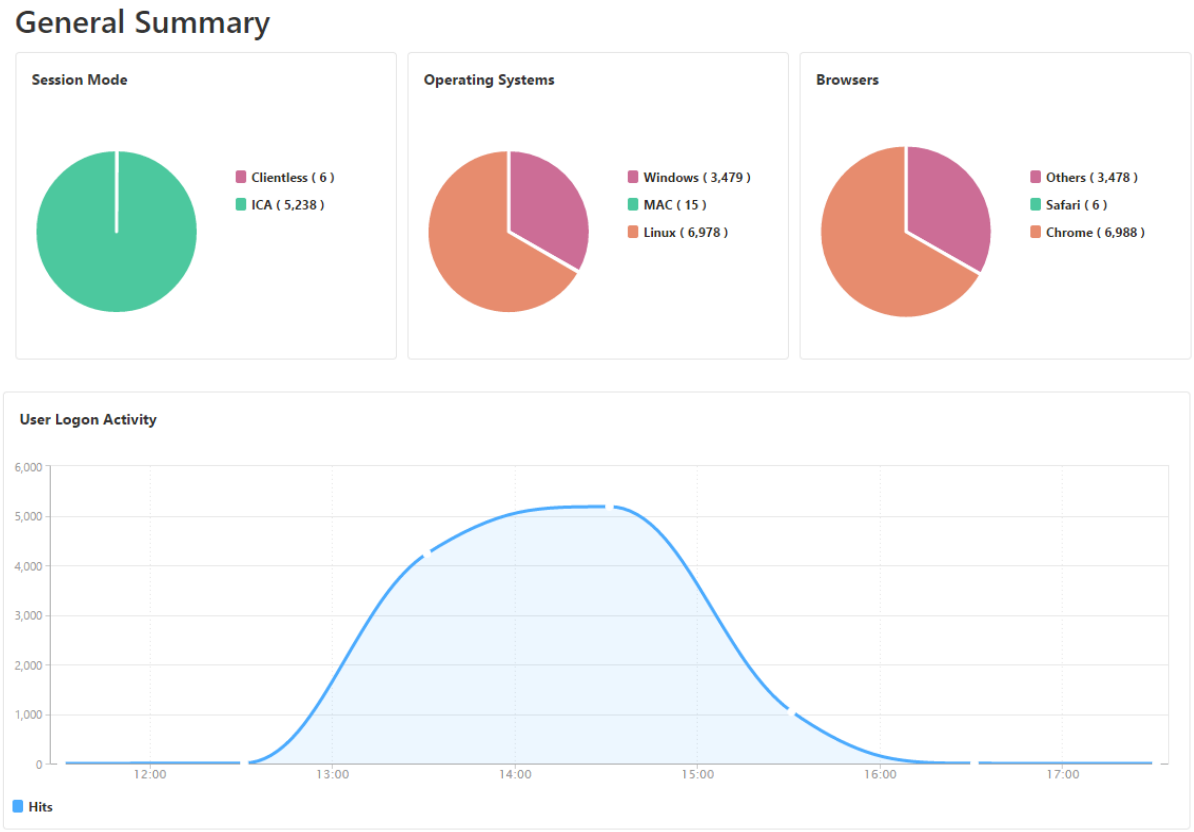


User Name	App Count	# Sessions	Bandwidth	Total Bytes
user1	260	2	1 bps	86.21 KB

5. Verschiedene Benutzer verwenden möglicherweise unterschiedliche 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.

Übersicht der Sitzungsmodi, der Art der Clients und der Anzahl der angemeldeten Benutzer anzeigen

1. Navigieren Sie in der NetScaler Console 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.



HDX Insight

January 26, 2024

HDX Insight bietet End-to-End-Sichtbarkeit für HDX-Datenverkehr zu Citrix Virtual Apps and Desktops, der über NetScaler geleitet wird. Außerdem können Administratoren Client- und Netzwerklatenzmetriken, historische Berichte und End-to-End-Leistungsdaten in Echtzeit anzeigen und Leistungsprobleme beheben. Durch die Verfügbarkeit von Echtzeit- und historischen Sichtbarkeitsdaten kann NetScaler Console eine Vielzahl von Anwendungsfällen unterstützen.

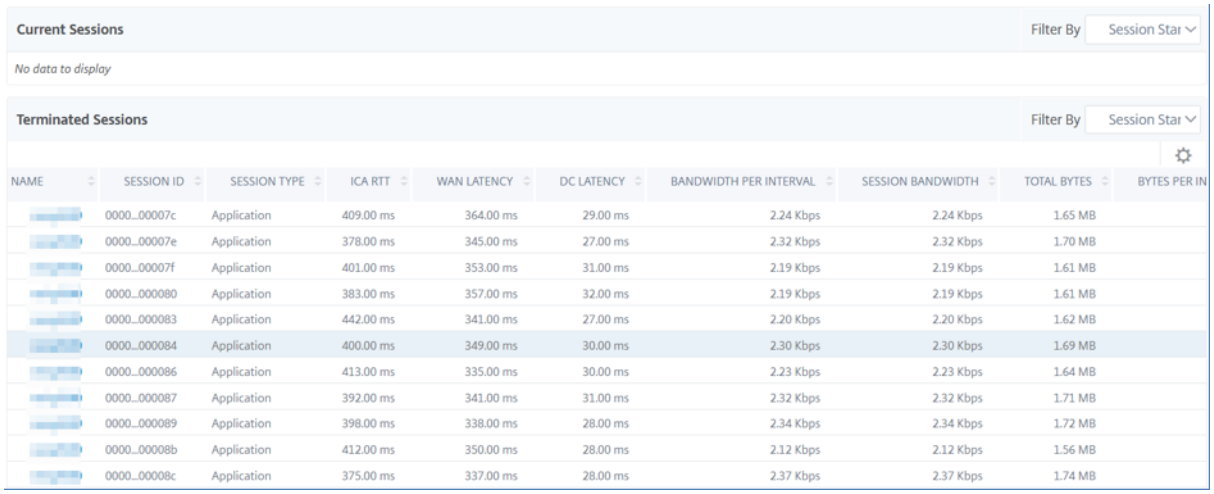
Damit Daten angezeigt werden, müssen Sie AppFlow auf Ihren virtuellen NetScaler Gateway-Servern aktivieren. AppFlow kann über das **IPFIX-Protokoll** oder die **Logstream-Methode** bereitgestellt werden.

> **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 auch Bandbreiteninformationen von einzelnen virtuellen Kanälen wie Audio, Druckerzuordnung und Clientlaufwerkzuordnung abrufen.

Sie können auch eine konsolidierte Ansicht aller aktiven und beendeten Sitzungen des Benutzers visualisieren.



Als Administrator ermöglicht Ihnen diese Ansicht Folgendes:

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

> **Hinweis**
>
> Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, Zugriff auf Anwendungsebene für die Gruppe gewähren und der Gruppe Benutzer zuweisen. Die NetScaler Console-Analytik 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 zu Gruppen finden Sie unter Gruppen auf der NetScaler Console konfigurieren .

Sie können auch zu **HDX Insight** > **Anwendungen** navigieren und auf **Startdauer** klicken, um die Zeit anzuzeigen, die für den Start der Anwendung benötigt wurde. Sie können auch den Benutzeragent aller verbundenen Benutzer anzeigen, indem Sie zu **HDX Insight > Benutzer** navigieren.

> **Hinweis** HDX Insight unterstützt Admin-Partitionen, die in NetScaler-Instanzen konfiguriert sind, die auf Softwareversion 12.0 ausgeführt werden.

Die folgenden Thin Clients unterstützen HDX Insight:

- WYSE Windows-basierte Thin Clients
- WYSE Linux-basierte Thin Clients
- WYSE ThinOS-basierte Thin Clients
- 10ZiG Ubuntu-basierte Thin Clients

Identifizierung der Hauptursache für Probleme mit langsamer Leistung

Szenario 1

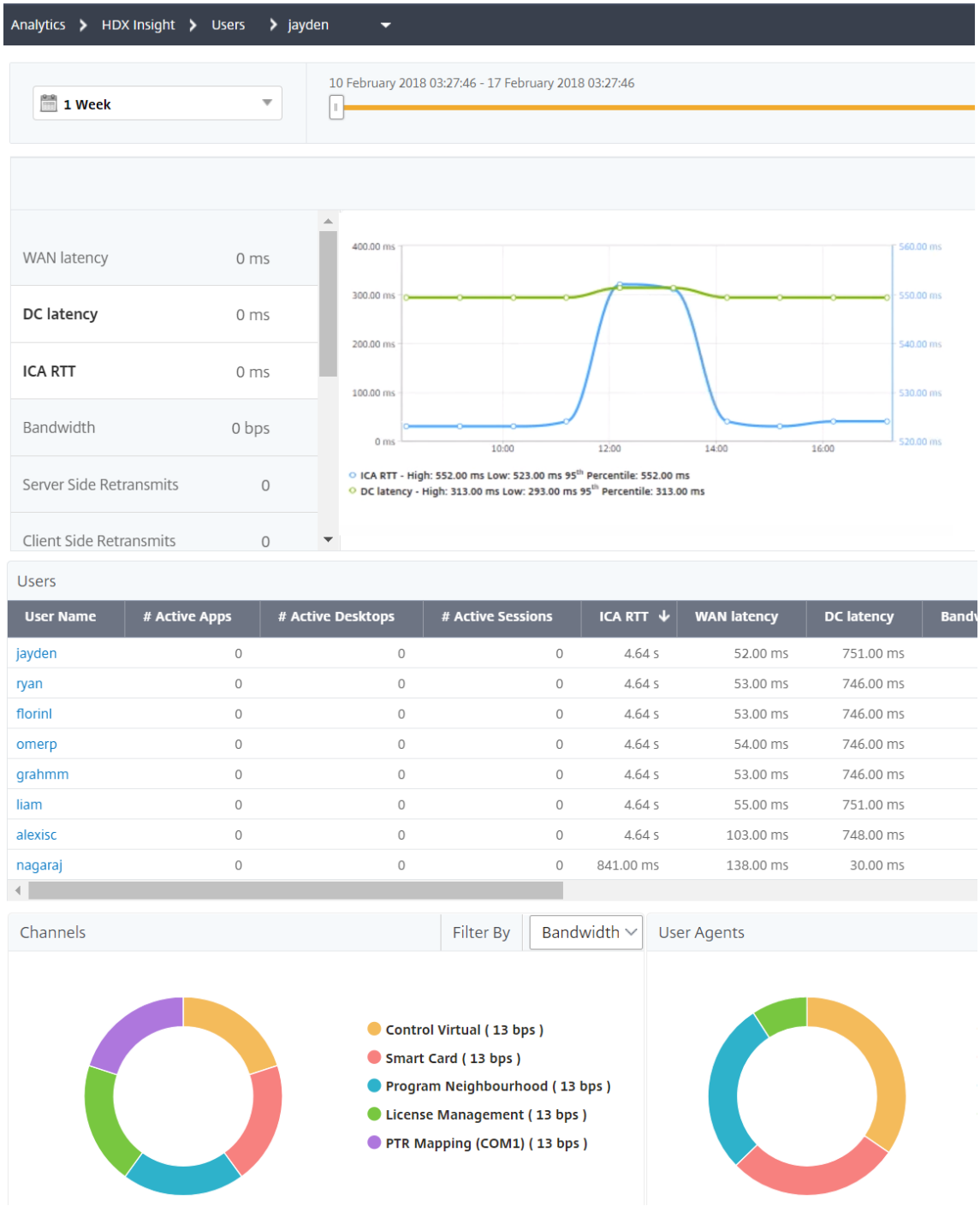
Benutzer haben Verzögerungen beim Zugriff auf Citrix Virtual Apps and Desktops Die Verzögerungen können auf Latenz im Servernetzwerk, durch das Servernetzwerk verursachte ICA-Verkehrsverzögerungen oder Latenz im Client-Netzwerk zurückzuführen sein.

Analysieren Sie die folgenden Metriken, um die Grundursache des Problems zu ermitteln:

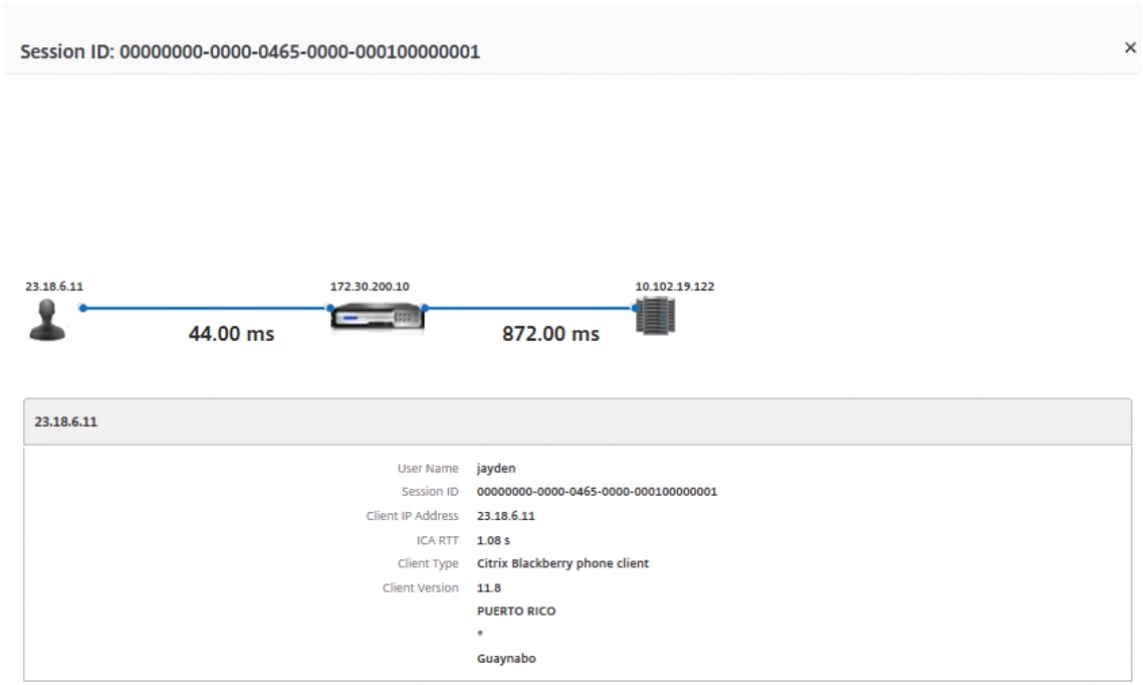
- WAN-Latenz
- DC-Latenz
- Hostverzögerung

So zeigen Sie die Client-Metriken an:

1. Navigieren Sie auf der Registerkarte **Analytics** zu **HDX Insight** > **Benutzer**.
2. Scrollen Sie nach unten, wählen Sie den Benutzernamen aus, und wählen Sie den Zeitraum aus der Liste aus. Der Zeitraum kann ein Tag, eine Woche, 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 Anwendungssitzungen** den Mauszeiger über den **RTT-Wert**, und notieren Sie sich die Hostverzögerung, die DC-Latenz und die WAN-Latenzwerte.
5. Klicken Sie in der Tabelle **Aktuelle Anwendungssitzungen** auf das Hopdiagrammsymbol, um Informationen über die Verbindung zwischen dem Client und dem Server anzuzeigen, einschließlich Latenzwerte.



Zusammenfassung:

In diesem Beispiel beträgt die **DC-Latenz** 751 Millisekunden, die **WAN-Latenz** 52 Millisekunden und **Hostverzögerungen** 6 Sekunden. Dies weist darauf hin, dass es beim Benutzer aufgrund der vom Servernetzwerk verursachten durchschnittlichen Latenz zu Verzögerungen kommt.

Szenario 2

Es kommt zu Verzögerungen beim Starten einer Anwendung auf Citrix Virtual Apps oder Desktops 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.

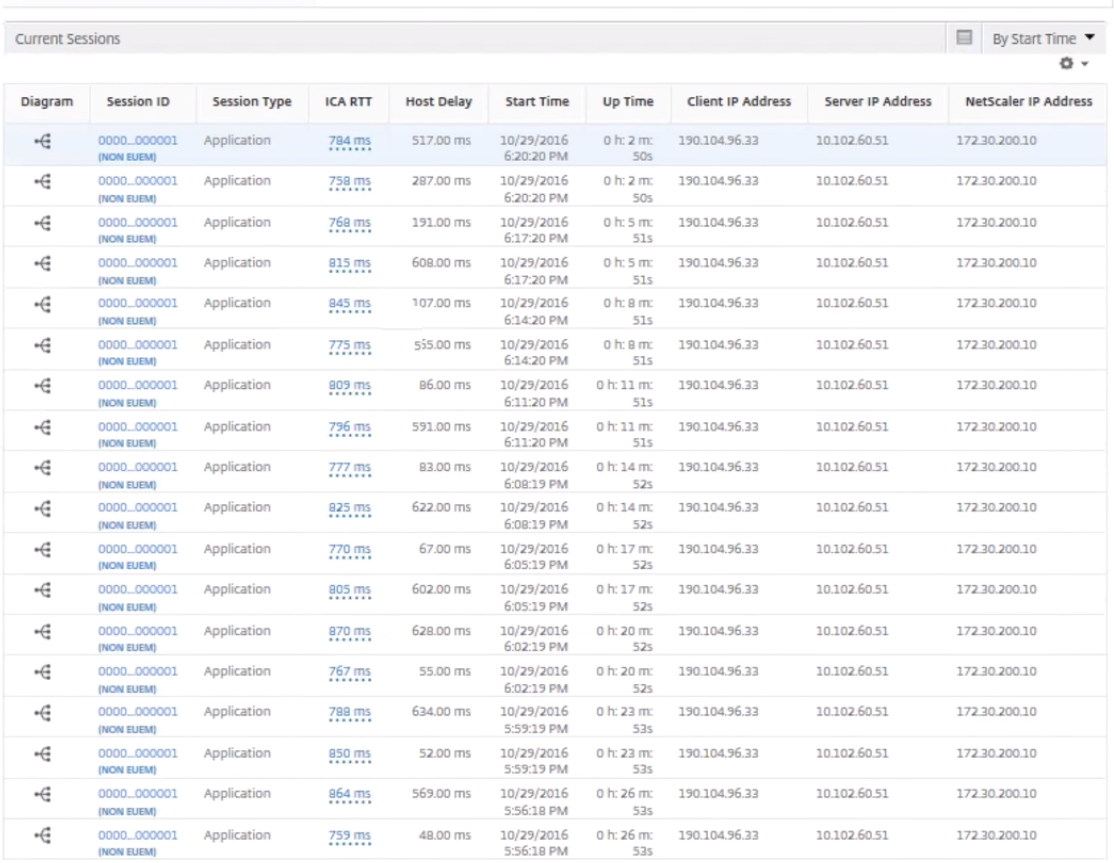
Analysieren Sie die folgenden Metriken, um die Grundursache des Problems zu ermitteln:

- 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. Notieren Sie sich in der grafischen Darstellung die WAN-Latenz-, DC-Latenz- und RTT-Werte für die jeweilige Sitzung.

4. Beachten Sie in der Tabelle **Aktuelle Anwendungssitzungen**, dass die Hostverzögerung hoch ist.



Current Sessions — By Start Time

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001 (NON EUEM)	Application	784 ms	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	758 ms	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	768 ms	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	815 ms	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	845 ms	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	775 ms	555.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	809 ms	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	796 ms	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	777 ms	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	825 ms	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	770 ms	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	805 ms	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	870 ms	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	767 ms	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	788 ms	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	850 ms	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	864 ms	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	759 ms	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

Zusammenfassung:

In diesem Beispiel beträgt die **DC-Latenz** 1 Millisekunde, die **WAN-Latenz** 12 Millisekunden, aber die **Hostverzögerung** 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 Benutzermesswerte an, z. B. WAN-Jitter und serverseitige Neuübertragungen, wenn Sie NetScaler Console verwenden, auf der 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.

Geo-Map für HDX Insight

Die Geokartenfunktion in NetScaler Console zeigt die Nutzung von Webanwendungen an verschiedenen geografischen Standorten auf einer Karte an. Als Administrator können Sie diese Informationen verwenden, um die Trends bei der Anwendungsnutzung und für die Kapazitätsplanung zu verstehen.

Die Geo-Map bietet Informationen zu den folgenden Kennzahlen, die für ein Land, einen Bundesstaat und eine Stadt spezifisch sind:

- Treffer insgesamt: Gesamtzahl der Zugriffe auf eine Anwendung.
- Bandbreite: Gesamtbandbreite, die bei der Bearbeitung von Clientanfragen
- Antwortzeit: Durchschnittliche Zeit für das Senden von Antworten auf Clientanforderungen.

Geo-Map enthält Informationen, die verwendet werden können, um verschiedene Anwendungsfälle wie die folgenden zu behandeln:

- Region mit der maximalen Anzahl von Clients, die auf eine Anwendung zugreifen
- Region mit der höchsten Reaktionszeit
- Region, die die größte Bandbreite verbraucht

NetScaler Console aktiviert **automatisch** Geomaps für private oder öffentliche IP-Adressen, wenn Sie **Web Insight** aktivieren.

Erstellen eines privaten IP-Blocks

NetScaler Console kann den Standort eines Clients erkennen, wenn die private IP-Adresse des Clients zum NetScaler Console-Server hinzugefügt wird. Wenn beispielsweise die IP-Adresse eines Clients in

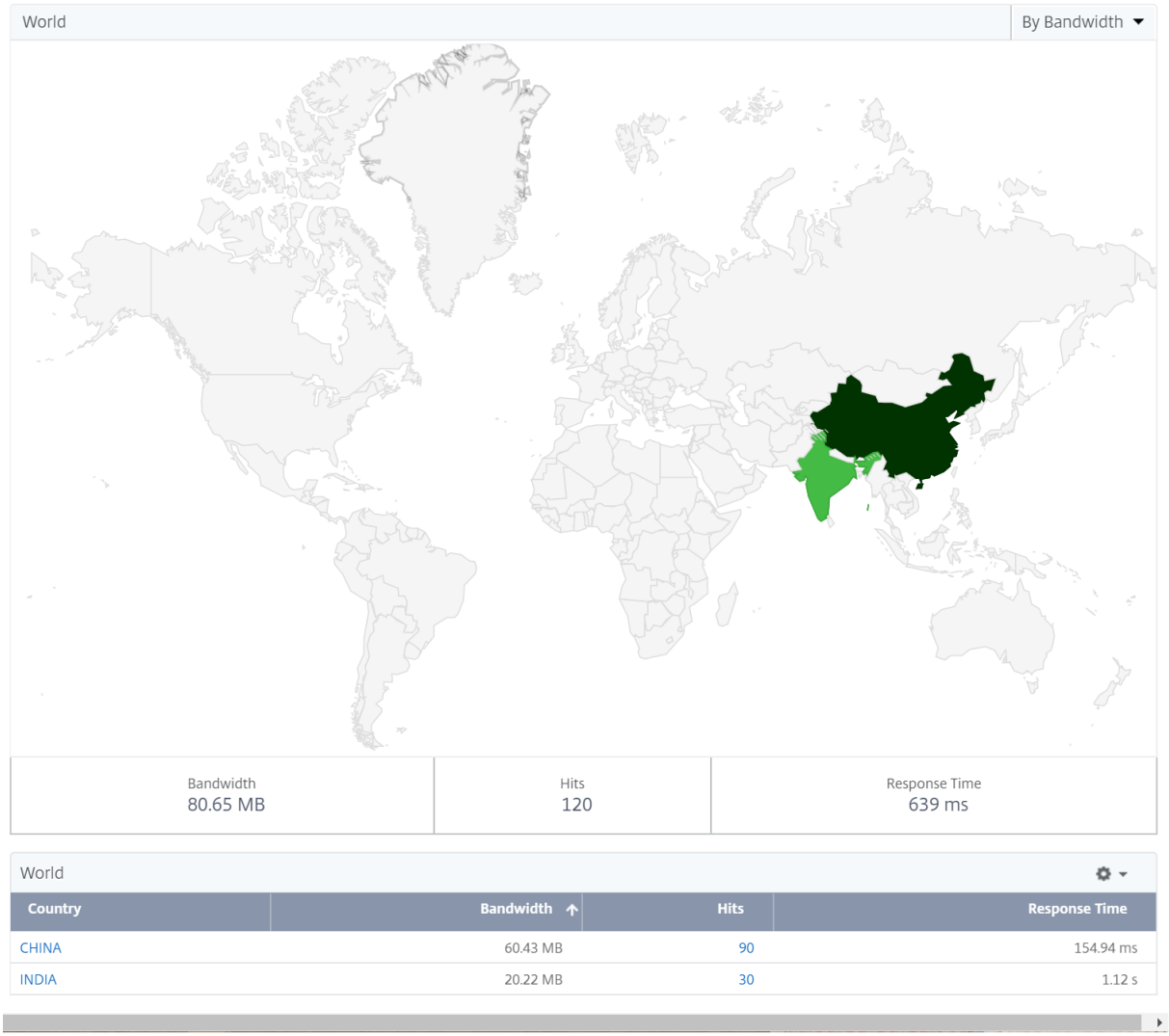
den Bereich eines privaten IP-Adressblocks fällt, der City A zugeordnet ist, erkennt NetScaler Console, dass der Datenverkehr von City A für diesen Client stammt.

So erstellen Sie einen IP-Block:

1. Navigieren Sie in NetScaler Console zu **Einstellungen > Analytics-Einstellungen > IP-Blöcke** , und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie auf der Seite **IP-Blöcke erstellen** die folgenden Parameter an:
    - **Name.** Geben Sie einen Namen für den privaten IP-Block an
    - **Starten Sie die IP-Adresse**. Geben Sie den niedrigsten IP-Adressbereich für den IP-Block an.
    - **IP-Adresse beenden**. Geben Sie den höchsten IP-Adressbereich für den IP-Block an.
    - **Land**. Wählen Sie das Land aus der Liste aus.
    - **Region**. Je nach Land wird die Region automatisch ausgefüllt, Sie können jedoch Ihre Region auswählen.
    - **Stadt**. Je nach Region wird die Stadt automatisch ausgefüllt, Sie können jedoch Ihre Stadt auswählen.
    - **Breitengrad** der **Stadt und Längengrad**der Stadt. Basierend auf der ausgewählten Stadt werden Breiten- und Längengrade automatisch ausgefüllt.
3. Klicken Sie zum Abschluss auf **Erstellen**.

Öffentliche IP-Blöcke NetScaler Console kann den Standort des Clients auch erkennen, wenn der Client eine öffentliche IP-Adresse verwendet. NetScaler Console verfügt über eine integrierte Standort-CSV-Datei, die dem Standort auf der Grundlage des Client-IP-Adressbereichs entspricht. Um den öffentlichen IP-Block verwenden zu können, müssen Sie lediglich die Option **Geodatenerfassung aktivieren** auf der Seite „Insight konfigurieren“aktivieren.

> Hinweis
>
> NetScaler Console benötigt eine Internetverbindung, um die Geomaps für einen bestimmten geografischen Standort anzuzeigen. Eine Internetverbindung ist auch erforderlich, um die GeoMap in den Formaten PDF-, PNG- oder JPG-Format zu exportieren.



So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** . Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu senden.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage

> eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

So konfigurieren Sie eine Geomap für Rechenzentren:

Navigieren Sie auf der Registerkarte **Infrastruktur** zu **Standorte** > **Private IP-Blöcke**, um Geomaps für einen bestimmten Standort zu konfigurieren.

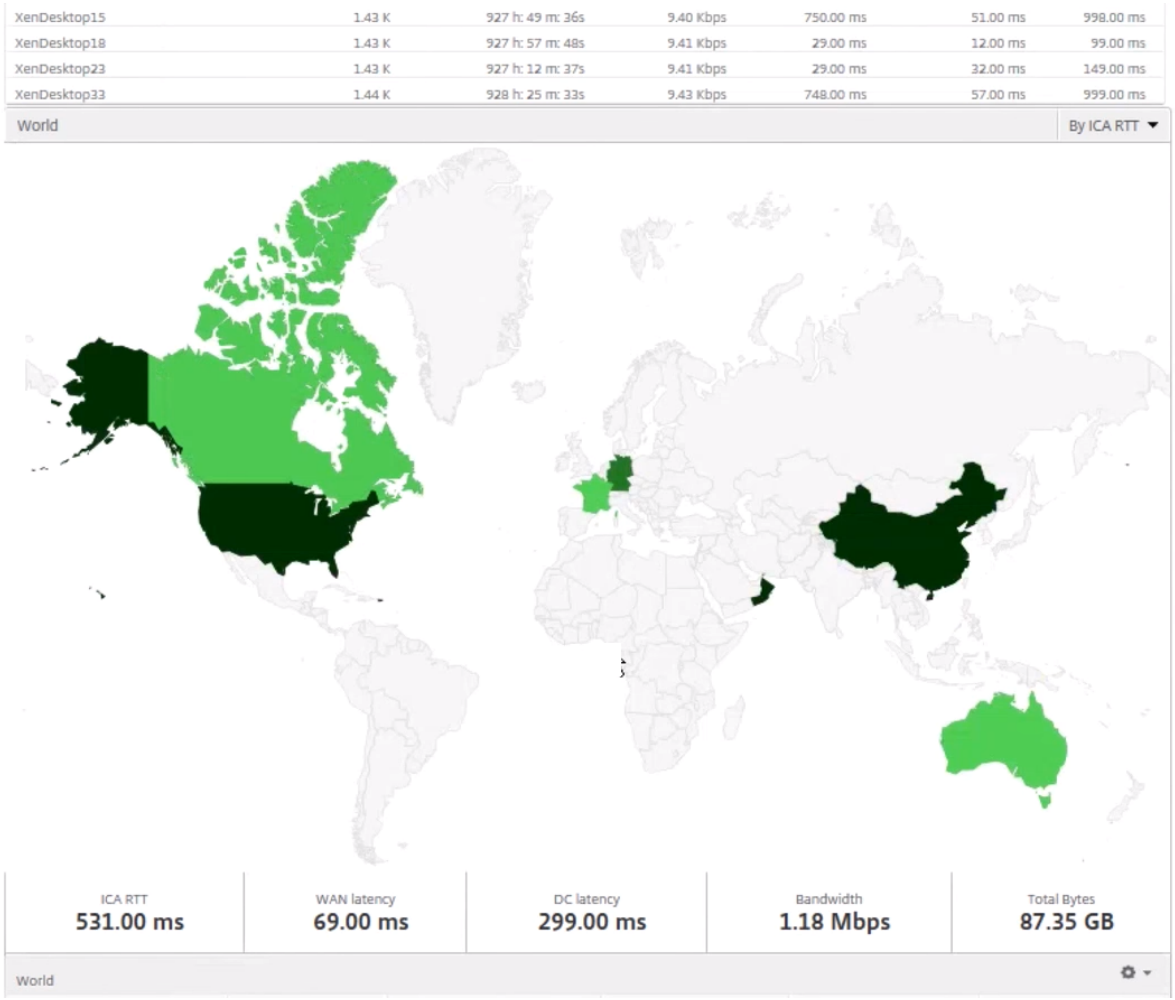
Anwendungsfall

Betrachten Sie ein Szenario, in dem Organisation ABC 2 Niederlassungen hat, eine in Santa Clara und die andere in Indien.

Die Santa Clara-Benutzer verwenden die 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-Instanzen über eine Advanced-Lizenz verfügen, werden in der NetScaler Console für HDX Insight festgelegte Schwellenwerte nicht ausgelöst, da Analysedaten nur 1 Stunde lang erfasst werden.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** . Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu senden.

Hinweis

- Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

HDX Insight-Datenerfassung aktivieren

January 26, 2024

HDX Insight ermöglicht es dem Administrator, eine außergewöhnliche Benutzererfahrung zu bieten, indem End-to-End-Transparenz des ICA-Datenverkehrs bereitgestellt wird, der durch die NetScaler Appliance geleitet wird.

HDX Insight bietet überzeugende und leistungsstarke Business Intelligence- und Fehleranalysefunktionen für Netzwerk, virtuelle Desktops, Anwendungen und Anwendungs-Fabric. HDX Insight kann Benutzerprobleme sofort erfassen, Daten über virtuelle Desktopverbindungen sammeln, AppFlow Datensätze generieren und als visuelle Berichte präsentieren.

Die Konfiguration zur Aktivierung der Datenerfassung in den NetScaler-Instanzen unterscheidet sich je nach Position der Appliance in der Bereitstellungstopologie. Dieses Thema umfasst die folgenden Details:

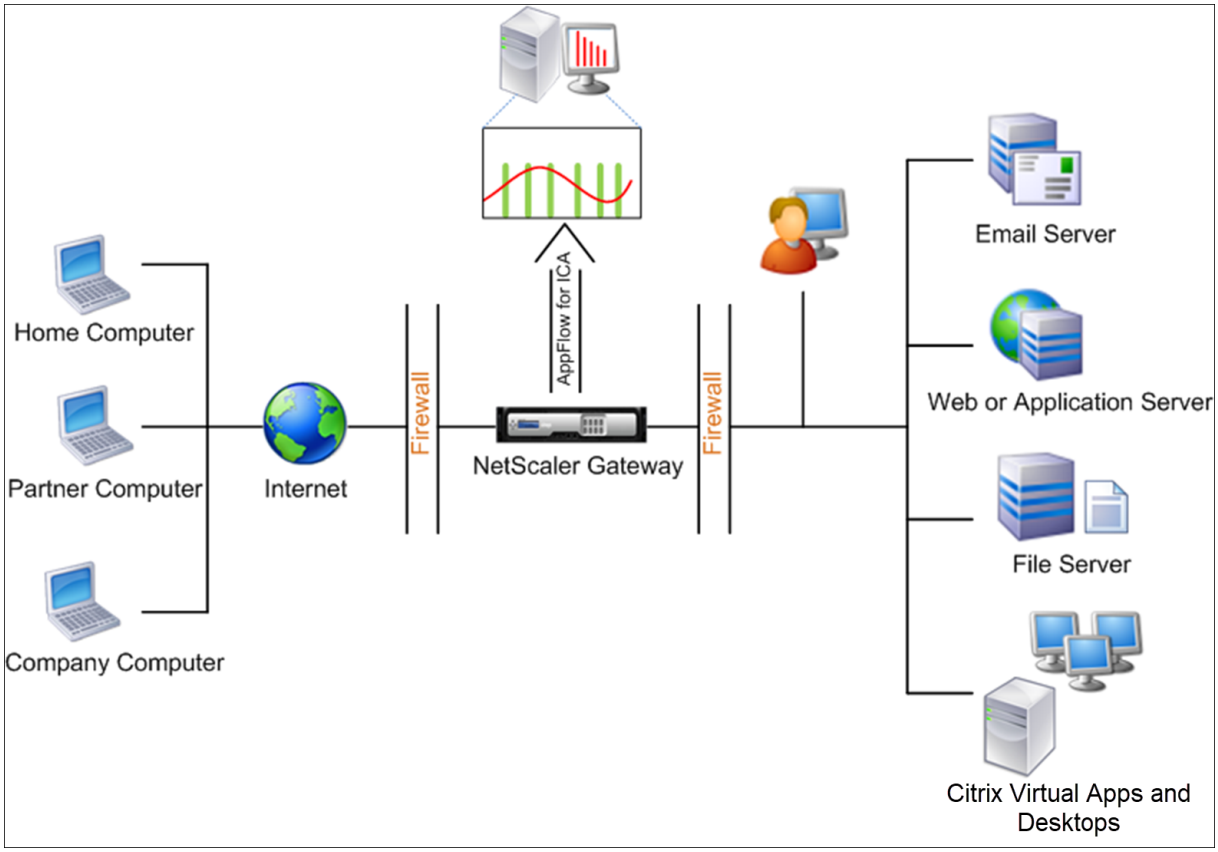
- Aktivieren der Datenerfassung für die Überwachung von NetScaler-Instanzen, die im transparenten Modus bereitgestellt werden
- Aktivieren der Datenerfassung für im Single-Hop-Modus bereitgestellte NetScaler Gateway-Geräte
- Aktivieren der Datenerfassung für im Double-Hop-Modus bereitgestellte NetScaler Gateway-Geräte
- Aktivierung der Datenerfassung für die Überwachung von NetScalern, die im LAN-Benutzermodus eingesetzt werden

Datenerfassung für NetScaler Gateway-Geräte im Single-Hop-Modus aktivieren

January 26, 2024

Wenn NetScaler Gateway im Single-Hop-Modus bereitgestellt wird, befindet sich das NetScaler Gateway am Rand des Netzwerks und leitet ICA-Verbindungen an die Desktop Delivery-Infrastruktur weiter. Diese Bereitstellung ist die einfachste und gebräuchlichste Bereitstellung. Dieser Modus bietet Sicherheit, wenn ein externer Benutzer versucht, auf das interne Netzwerk in einer Organisation zuzugreifen. Im Single-Hop-Modus greifen Benutzer über ein virtuelles privates Netzwerk (VPN) auf die NetScaler-Appliances zu.

Um mit der Erfassung der Berichte zu beginnen, müssen Sie das NetScaler Gateway-Gerät zum Inventar der NetScaler Console hinzufügen und AppFlow auf der NetScaler Console aktivieren. Die folgende Abbildung zeigt eine NetScaler Console, die im Single-Hop-Modus bereitgestellt wird.



Aktivieren Sie die AppFlow-Funktion in der NetScaler Console

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 die virtuellen VPN-Server aus, und klicken Sie auf **Analytics aktivieren**.
4. Wählen Sie **Web Insight** aus.
5. Klicken Sie auf **OK**.

Hinweis

Die folgenden Befehle werden im Hintergrund ausgeführt, wenn Sie AppFlow im Single-Hop-Modus aktivieren. Diese Befehle werden hier explizit zur Fehlerbehebung angegeben.

- `add appflow collector \<name\> -IPAddress \<ip\\_addr\>`
- `add appflow action \<name\> -collectors \<string\>`
- `set appflow param -flowRecordInterval \<secs\>`
- `disable ns feature AppFlow`
- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

Datenerfassung zur Überwachung von NetScalern aktivieren, die im transparenten Modus eingesetzt werden

January 26, 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 eine NetScaler Appliance im transparenten Modus in einer Citrix Virtual Apps and Desktops-Umgebung bereitgestellt wird, wird der ICA-Datenverkehr nicht über ein VPN übertragen.

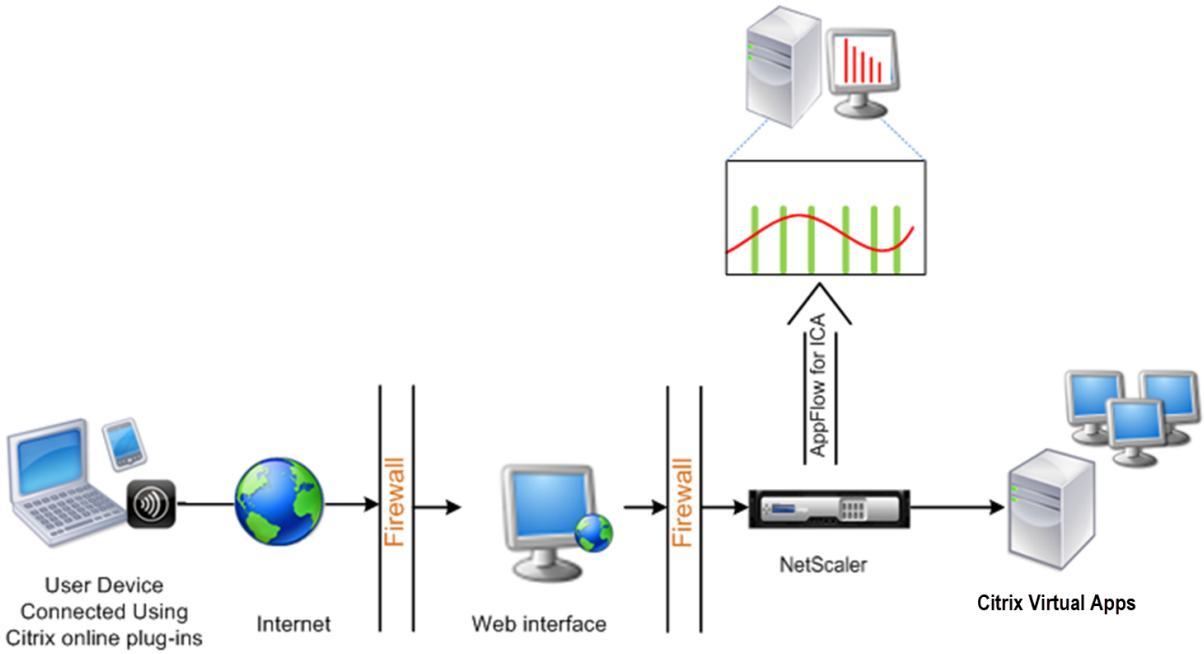
Nachdem Sie den NetScaler zum Inventar der NetScaler Console hinzugefügt haben, müssen Sie AppFlow für die Datenerfassung aktivieren. Die Aktivierung der Datenerfassung hängt vom Gerät und vom Modus ab. In diesem Fall müssen Sie NetScaler Console als AppFlow-Collector auf jeder NetScaler-Appliance hinzufügen, und Sie müssen eine AppFlow-Richtlinie konfigurieren, um den gesamten oder einen 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 Console-Konfigurationsprogramms 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 einer NetScaler Console, wenn ein NetScaler in einem 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, um für den ICA-Verkehr zu gelten.

7. Legen Sie den Wert des Parameters FlowRecordInterval für AppFlow auf 60 Sekunden fest.

```
set appflow param -flowRecordInterval 60
```

8. Speichern Sie die Konfiguration.

```
save ns config
```


Datenerfassung für NetScaler Gateway-Appliances im Double-Hop-Modus aktivieren

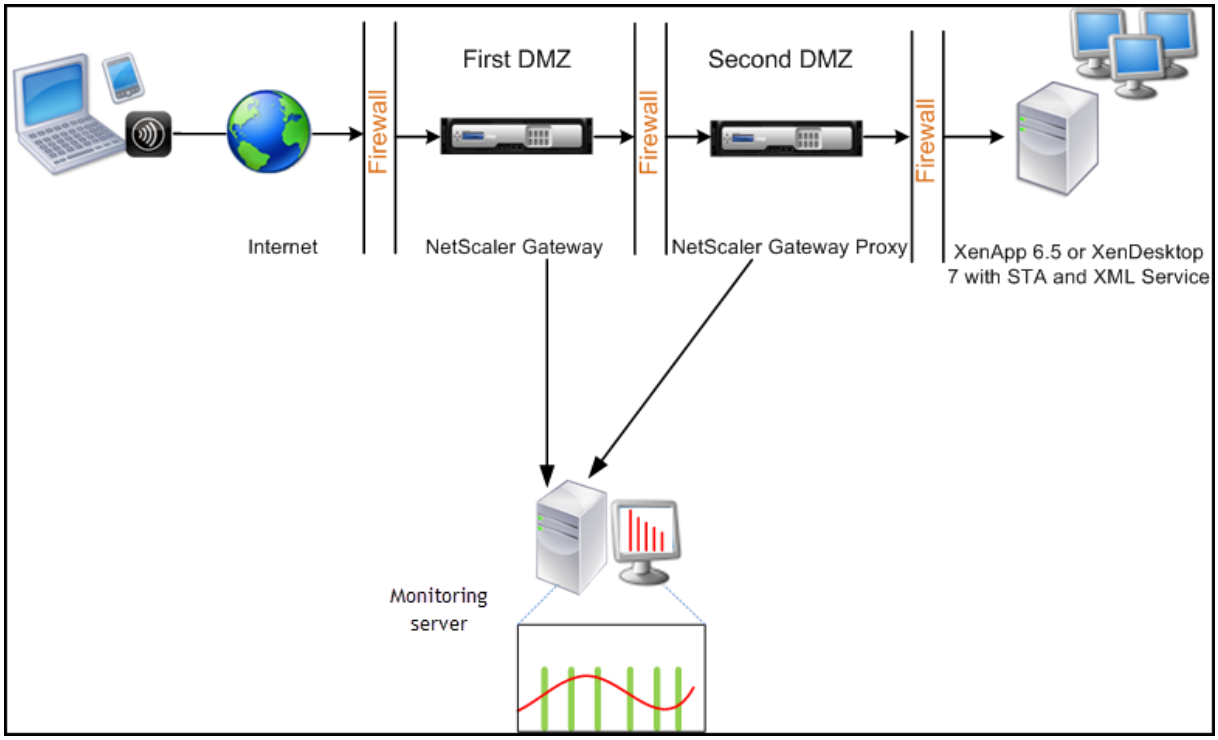
March 12, 2024

Der Doppel-Hop-Modus von NetScaler Gateway bietet zusätzlichen Schutz für ein internes Organisationsnetzwerk, da ein Angreifer mehrere Sicherheitszonen oder Demilitarisierte Zonen (DMZ) durchdringen muss, um die Server im sicheren Netzwerk zu erreichen.

Als Administrator können Sie mithilfe der NetScaler Console Folgendes analysieren:

- Die Anzahl der Hops (NetScaler Gateway-Appliances), über die die ICA-Verbindungen laufen
- Die Details über die Latenz bei jeder TCP-Verbindung und wie sie sich gegen die vom Client wahrgenommene Gesamt-ICA-Latenz auswirkt

Das folgende Bild zeigt, dass die NetScaler Console und NetScaler Gateway in der ersten DMZ im selben Subnetz bereitgestellt werden.



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.

Die NetScaler Console kann entweder im Subnetz des NetScaler Gateway-Geräts in der ersten DMZ oder im Subnetz des NetScaler Gateway-Geräts in der zweiten DMZ bereitgestellt werden.

Im Double-Hop-Modus sammelt NetScaler Console TCP-Datensätze von einer Appliance und ICA-Datensätze von der anderen Appliance. Nachdem Sie die NetScaler Gateway-Appliances zum Inventar der NetScaler Console hinzugefügt und die Datenerfassung aktiviert haben, exportiert jedes Gerät die Berichte, indem es die Anzahl der Hops und die Verbindungsketten-ID verfolgt.

Damit NetScaler Console identifizieren kann, welche Appliance Datensätze exportiert, wird jede Appliance mit einer Hop-Anzahl und jede Verbindung 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 Console verwendet die Hop-Anzahl und die Verbindungsketten-ID, um die Daten der beiden NetScaler Gateway-Appliances miteinander in Beziehung zu setzen und die Berichte zu generieren.

Um NetScaler Gateway-Appliances zu überwachen, die in diesem Modus bereitgestellt werden, müssen Sie zuerst das NetScaler Gateway zum NetScaler Console-Inventar hinzufügen, AppFlow auf der NetScaler Console aktivieren und dann die Berichte im NetScaler Console-Dashboard anzeigen.

Datenerfassung auf der NetScaler Console aktivieren

Wenn Sie NetScaler Console aktivieren, um mit der Erfassung der ICA-Details von beiden Appliances zu beginnen, sind die gesammelten Informationen überflüssig. Um diese Situation zu umgehen, müssen Sie AppFlow für TCP auf der ersten NetScaler Gateway-Appliance aktivieren und dann AppFlow für ICA 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 über die NetScaler Console:

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 die virtuellen Server aus und klicken Sie auf **Security & Analytics aktivieren**.
4. Wählen Sie Web **Insight**
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 die NetScaler Console 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. 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
```

3. Aktivieren Sie Double Hop und AppFlow auf dem NetScaler Gateway in der zweiten DMZ.

---

set vpn vserver [**-** DISABLED)] [**- appflowLog** (DISABLED)]
doubleHop** (ENABLED ENABLED

```
1 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 [**-authentication** (ON 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>]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA_REQUEST
```

7. Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway-Appliances:

set appFlow param [**-connectionChaining** DISABLED)]
(ENABLED

```
set appflow param -connectionChaining ENABLED
```

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 **KonfigurationNetScaler 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 nächsten 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 Bearbeitungssymbol.

c) Erweitern Sie **Mehr**, 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 **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 Bearbeitungssymbol.

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 **KonfigurationNetScaler Gateway**und klicken Sie auf**Virtuelle Server**.

b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe Erweitert die Option Richtlinien.

c) Klicken Sie auf das Symbol + und wählen Sie in der Liste **Choose policy** die Option **AppFlow** aus und wählen Sie in der Liste **Typ auswählen** die Option **Andere TCP-Anforderung** aus.

d) Klicken Sie auf **Weiter**.

e) Fügen Sie eine Richtlinienbindung hinzu und klicken Sie auf **Schließen** .

5. Aktivieren Sie die andere NetScaler Gateway-Appliance zum Exportieren von ICA-Datensätzen:

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 erweitern Sie in der Gruppe **Erweitert** die Option **Richtlinien**.

c) Klicken Sie auf das Symbol + und wählen Sie in der Liste **Choose policy** die Option **AppFlow** aus und wählen Sie in der Liste **Typ auswählen** die Option **Andere TCP-Anforderung** aus.

d) Klicken Sie auf **Weiter**.

e) Fügen Sie eine Richtlinienbindung hinzu und klicken Sie auf **Schließen** .

6. Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway-Appliances.
    a) Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **Appflow**.
    b) Klicken Sie im rechten Bereich in der Gruppe **Einstellungen** auf **Appflow-Einstellungen ändern**.
    c) Wählen Sie **Verbindungsverkettung** aus, und klicken Sie auf **OK**.

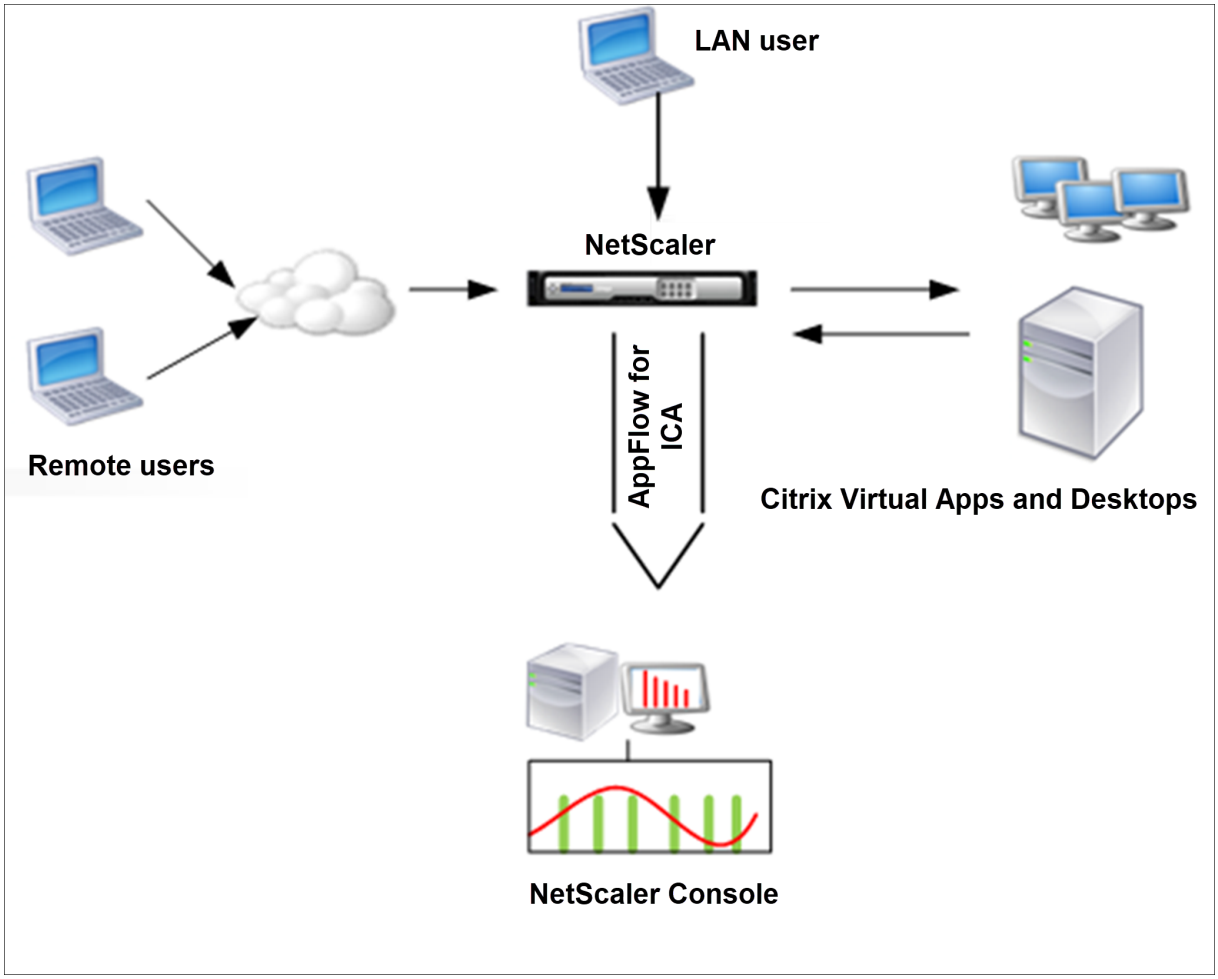
Datenerfassung zur Überwachung von NetScalern aktivieren, die im LAN-Benutzermodus eingesetzt werden

January 26, 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 bewältigen und LAN-Benutzer direkt mit Citrix Virtual Apps and Desktops-Anwendungen verbinden zu können, können Sie die NetScaler Appliance in einem LAN-Benutzermodus bereitstellen, indem Sie einen virtuellen Cache-Umleitungsserver konfigurieren. Der virtuelle Cache-Umleitungsserver fungiert als SOCKS-Proxy auf dem NetScaler Gateway-Gerät.

Die folgende Abbildung zeigt die NetScaler Console, die im LAN-Benutzermodus bereitgestellt wird.**



> **Hinweis**
>
> Das NetScaler Gateway-Gerät muss in der Lage sein, den Agenten zu erreichen.

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 zum Inventar der NetScaler Console 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 Console-Konfigurationsprogramms 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 der NetScaler-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>]
```

Beispiel:

```
add cr vserver cr1 HDX 10.12.2.2 443 – cacheType FORWARD –
    cltTimeout 180
```

> **Hinweis:**
>
> Wenn Sie mit einem NetScaler Gateway-Gerät auf das LAN-Netzwerk zugreifen, fügen Sie eine Aktion hinzu, um eine Richtlinie anzuwenden, die dem VPN-Datenverkehr entspricht.

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]

add vpn trafficPolicy** \<name\> \<rule\> \<action\>
```

Beispiel:

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. Fügen Sie NetScaler Console 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
```

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, um für den ICA-Verkehr zu gelten.

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.

```
save ns config
```

Schwellenwerte erstellen und Warnungen für HDX Insight konfigurieren

January 26, 2024

Mit HDX Insight auf der NetScaler Console können Sie den HDX-Verkehr überwachen, der die NetScaler-Instanzen durchläuft. Mit der NetScaler Console können Sie Schwellenwerte für verschiedene Leistungsindikatoren festlegen, die zur Überwachung des Insight-Datenverkehrs verwendet werden. Sie können in NetScaler Console auch Regeln konfigurieren und Warnungen 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 mehreren Treffern, der von der Anwendung

verbrauchten Bandbreite und der Reaktionszeit des Servers zugeordnet. Eine Benutzerentität kann WAN-Latenz, DC-Latenz, ICA RTT und Bandbreite zugeordnet werden, die von einem Benutzer belegt wird.

Die Schwellenwertverwaltung für HDX Insight in der NetScaler Console 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. In der Entität des Benutzers kann die Schwellenwertgruppe auch mit einer Geolokalisierung verknüpft sein.

In der NetScaler Console wird nur dann eine Warnung 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 beispielsweise die Entität der Anwendung auswählen und dann **Gesamtzahl für den Sitzungsstart oder Anzahl der App-Launch**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 Console ein Ereignis, das auf eine Schwellenwertverletzung hinweist, und für jedes Ereignis wird eine Warnung ausgegeben.

Sie müssen konfigurieren, wie Sie die Warnung erhalten. Sie können die Anzeige der Warnung auf der NetScaler Console aktivieren oder die Warnung als E-Mail oder beides oder als SMS auf Ihrem

Mobilgerät erhalten. Für die letzten beiden Aktionen müssen Sie den E-Mail-Server oder den SMS-Server in der NetScaler Console konfigurieren.

Schwellenwertgruppen können auch an Geolocations gebunden werden, um die geospezifische Überwachung der Benutzerentität zu ermöglichen.

Beispiel-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 mit dem NetScaler Gateway und der GSLB-basierten Umleitung auf die Citrix Virtual Apps and Desktops auf der ganzen Welt zu. Eric, der Citrix Virtual Apps and Desktops Admin für ABC Inc. möchte die Benutzererfahrung für alle ihre Büros verfolgen, um die Apps und die Desktop-Bereitstellung für den Zugriff von überall und jederzeit zu optimieren. Eric möchte auch die 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.

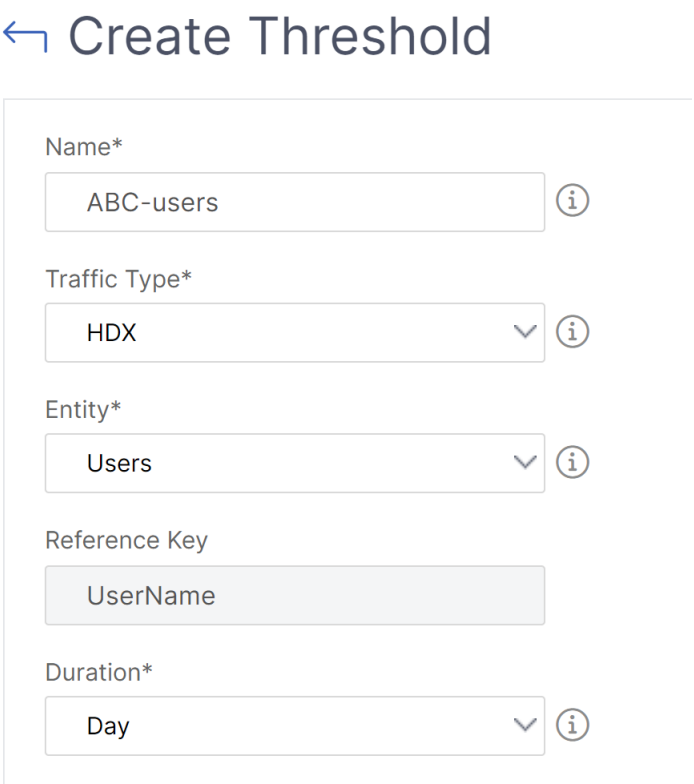
Mit der Verwaltung von Schwellenwertregelgruppen für HDX Insight kann Eric geospezifische Schwellenwertregelgruppen für jeden Standort festlegen und per E-Mail oder SMS bei Verstößen pro Gebiet gewarnt werden. Eric ist auch in der Lage, die Verfolgung mehrerer Metriken innerhalb einer Schwellenwertregelgruppe 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 beim manuellen Durchsuchen aller Citrix Virtual Apps and Desktops for HDX Insight Portfolio-Metriken entsteht.

Erstellen Sie eine Schwellenwertregelgruppe und konfigurieren Sie Warnungen für HDX Insight mithilfe der NetScaler Console

1. Navigieren Sie in der NetScaler Console 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:

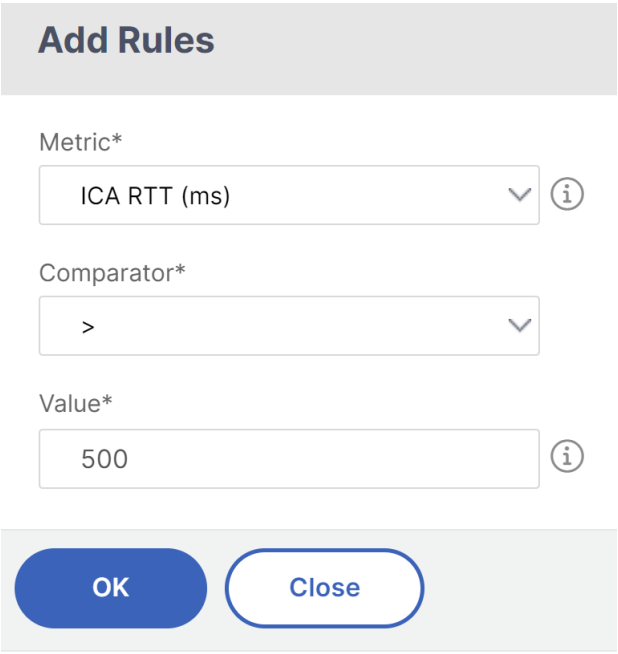
    a) **Name.** Geben Sie einen Namen für die Erstellung eines Ereignisses ein, für das NetScaler Console eine Warnung generiert.

b) **Art des Datenverkehrs**. Wählen Sie in der Liste **HDX**aus.
c) **Entität**. Wählen Sie in der Liste 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 aus der Liste das Zeitintervall aus, für das Sie die Entität überwachen möchten. Sie können die Entitäten für eine Stunde, für einen Tag oder für eine Woche überwachen.

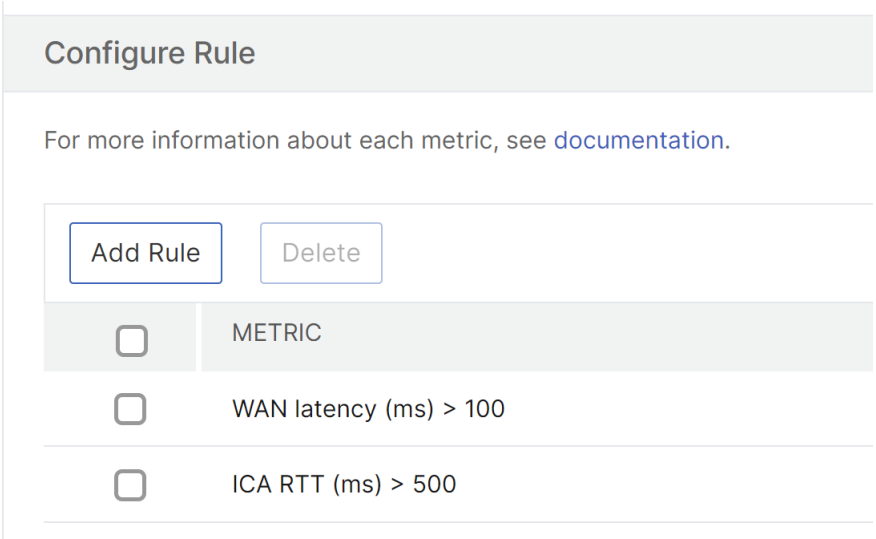


3. **Erstellen von Schwellenwertregelgruppen für alle Entitäten:**

   Für HDX-Verkehr müssen Sie eine Regel erstellen, indem Sie auf **Regel hinzufügen**klicken. Geben Sie die Werte in das sich **öffnende Popup-Fenster Regeln hinzufügen** ein.

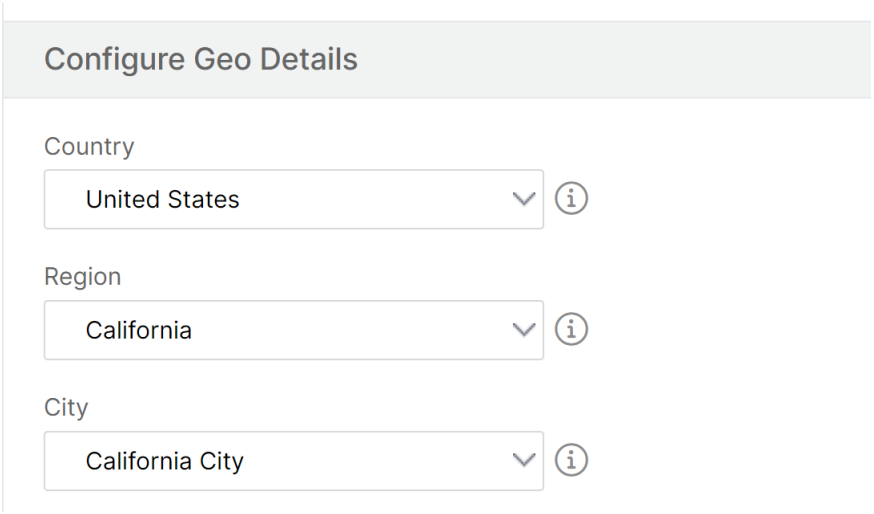


Sie können mehrere Regeln erstellen, um jede Entität zu überwachen. Wenn Sie mehrere Regeln in einer einzigen Gruppe erstellen, können Sie die Entitäten als Gruppe von Schwellenwertregeln anstelle einzelner Regeln überwachen. Klicken Sie auf **OK**, um das Fenster zu schließen.



4. **Konfigurieren von Geolocation-Tagging für Benutzer-Entität:**

   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 Console mit der Überwachung der Entitäten beginnen kann.
6. Optional können Sie Aktionen wie E-Mail- und Slack -Benachrichtigungen konfigurieren.
7. Klicken Sie auf **Erstellen**, um eine Schwellenregelgruppe zu erstellen.

HDX Insight-Berichte und Metriken anzeigen

January 26, 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 Apps and Desktops 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.

Dieses Dokument umfasst Folgendes:

- Berichte und Metriken der Benutzeransicht
- Berichte und Metriken der Anwendungsansicht
- Desktop-View-Berichte und Metriken
- Instanzansichtsberichte und -metriken
- Lizenzansichtsberichte und -metriken

Problemen mit HDX Insight beheben

January 26, 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 Console.
- Datensatzgenerierung für HDX/ICA-Verkehr in NetScaler.
- Auffüllung der Datensätze in NetScaler Console.

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 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.

Checkliste für die Konnektivität zwischen NetScaler und NetScaler Console

- 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 **System > AppFlow > Richtlinien** navigieren, um die AppFlow-Richtlinientreffer zu überprüfen.
- Überprüfen Sie jede Firewall, die AppFlow Ports 4739 oder 5557 blockiert.

Datensatzgenerierung für HDX/ICA-Datenverkehr in der 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 der Citrix Workspace-App

  Lösung: Aktualisieren Sie die Citrix Workspace App auf eine unterstützte Version. Einzelheiten finden Sie unter Citrix Workspace-App.

- Log: **Fehler von Expand Packet - Überspringen der gesamten hdx-Verarbeitung für diesen Flow**

  Ursache: Problem beim Dekomprimieren 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

Code überspringen	Fehlermeldung	Ursache des Fehlers
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
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_COR	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

Code überspringen	Fehlermeldung	Ursache des Fehlers
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
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_NS_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

Code überspringen	Fehlermeldung	Ursache des Fehlers
134	NS_ICA_ERR_IDENT_PROTO	Das ICA- oder CGP-Protokoll kann nicht identifiziert werden, bei falschen Empfängern beobachtet
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 übersteigt 1.460 Byte
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	Das ICA-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_ID	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

Code überspringen	Fehlermeldung	Ursache des Fehlers
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
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 Befehl crypt-Befehl in der Basisverschlüsselung
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	Ungültiger Status für einen crypt-Befehl in der RC5-Verschlüsselung

Code überspringen	Fehlermeldung	Ursache des Fehlers
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	VDA 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
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

Code überspringen	Fehlermeldung	Ursache des Fehlers
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.

Name des HDX-Zählers	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_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

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
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_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 von Hosts abgelehnten Wiederverbindungsanfragen nach Client	Stats/Diagnostik

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_euem_available	Gibt die Anzahl der Verbindungen an, für die der Kanal “Überwachung der Benutzererfahrung”verfügbar ist. Der End User Experience Monitoring-Kanal ist erforderlich, um Statistiken wie ICA RTT zu sammeln.	Stats/Diagnostik
hdx_err_disabled_sr	Die Sitzungszuverlässigkeit ist mit dem `nsapimgr`Drehknopf deaktiviertDie Sitzung funktioniert für diese Sitzung nicht.	Fehler
hdx_err_skip_no_msi	Auf dem XA/XD-Server fehlt die MSI-Fähigkeit. Dies weist auf eine ältere Serverversion hin. HDX Insight überspringt diese Verbindung.	Fehler
hdx_err_skip_old_server	Alte, nicht unterstützte Serverversion	Fehler
hdx_err_clnt_not_whitelist	Clientempfänger nicht in der Zulassungsliste, HDX Insight überspringt diese Verbindung	Fehler
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

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/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_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

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/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.

Auffüllen der Datensätze in der NetScaler Console-Checkliste

- Führen Sie den Befehl `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` aus und überprüfen Sie die Protokolle, um zu bestätigen, dass NetScaler Console AppFlow-Datensätze empfängt.
- Bestätigen Sie, dass die NetScaler-Instanz zur NetScaler Console hinzugefügt wurde.
- Stellen Sie sicher, dass der virtuelle NetScaler Gateway/VPN-Server in der NetScaler Console 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 Console-Versionen.
- Serverversionen von Citrix Virtual Apps and Desktops.
- Versionen des Client-Workspace.
- 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.
- Paket mit technischem Support für NetScaler Console 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 in HDX Insight finden Sie in den NetScaler Versionshinweisen.

Metrikinformationen für Schwellenwerte

January 26, 2024

Sie können Schwellenwerte erstellen und diese benachrichtigen lassen, wenn der Schwellenwert überschritten wird. In einer typischen Bereitstellung können Sie Schwellenwerte wie folgt festlegen:

- Verschiedene Anwendungsmetriken verfolgen
- Erleichtert die Planung
- Lassen Sie sich benachrichtigen, wenn der Metrikwert der Anwendung den festgelegten

So konfigurieren Sie Schwellenwerte:

1. Navigieren Sie zu **Einstellungen > Analytics-Einstellungen > Schwellenwerte**.
2. Klicken Sie auf der Seite **Schwellenwerte** auf **Hinzufügen**.

Web-Site

Metriken	Entität	Beschreibung
Anwendungen	Treffer	Gesamtzahl der von einem virtuellen Server (Anwendung) empfangenen Treffer
	Bandbreite (MB)	Gesamtbandbreite, die vom virtuellen Server (Anwendung) verbraucht wird
	Reaktionszeit (ms)	Die Zeit, die der virtuelle Server benötigt, um zu antworten
Clients	Anfragen	Die gesamte Anfrage, die ein Kunde erhalten hat
	Renderzeit (ms)	Die Zeit, die der Client für das Rendern der Serverantwort benötigt
	Latenz im Client-Netzwerk	Die Zeit, die für Anfragen aus dem Client-Netzwerk benötigt wird
Geräte	Treffer	Gesamtzahl der von einem Gerät empfangenen Treffer. Zum Beispiel: Laptop, Handy
	Bandbreite (MB)	Von einem Gerät verbrauchte Gesamtbandbreite
Domänen	Treffer	Gesamtzahl der von einer Netzwerkdomäne empfangenen Treffer
	Bandbreite (MB)	Von einer Netzwerkdomäne verbrauchte Gesamtbandbreite
	Reaktionszeit (ms)	Die Zeit, die für die Beantwortung von Anfragen einer Netzwerkdomäne benötigt wird

Metriken	Entität	Beschreibung
Betriebssystem	Treffer	Gesamtzahl der von einem Betriebssystem empfangenen Treffer
	Bandbreite (MB)	Gesamtbandbreite, die von einem Betriebssystem verbraucht wird
	Renderzeit (ms)	Die Zeit, die ein Betriebssystem benötigt, um die Serverantwort zu rendern
Methoden der Anfrage	Treffer	Gesamtzahl der Anfragen, die von einer Anforderungsmethode empfangen wurden. Zum Beispiel: GET, POST
	Bandbreite (MB)	Insgesamt von einer Anforderungsmethode verbrauchte Bandbreite
Antwortstatus	Treffer	Gesamtzahl der mit Antwortcodes empfangenen Treffer
	Bandbreite (MB)	Vom Antwortcode verbrauchte Gesamtbandbreite
Server	Treffer	Gesamtzahl der von einem Server empfangenen Anfragen/Treffern
	Bandbreite (MB)	Von einem Server verbrauchte Gesamtbandbreite
	Netzwerklatenz des Servers (ms)	Die Zeit, die für Anfragen vom Servernetzwerk benötigt wird
	Verarbeitungszeit des Servers (ms)	Die Zeit, die ein Server benötigt, um auf Anfragen zu antworten
URLs	Treffer	Gesamtzahl der von einer URL empfangenen Treffer. Zum Beispiel: www.Citrix.com
	Ladezeit (ms)	Die Zeit, die benötigt wird, um eine URL vom Server zu laden
	Renderzeit (ms)	Die Zeit, die die URL zum Rendern und Anzeigen benötigt

Metriken	Entität	Beschreibung
Benutzeragents	Treffer	Gesamtzahl der Anfragen, die von einem Benutzeragenten empfangen wurden. Zum Beispiel: Chrome-Webbrowser
	Bandbreite (MB)	Gesamtbandbreite, die vom Benutzeragent verbraucht wird
	Renderzeit (ms)	Die Zeit, die benötigt wird, um die Serverantwort durch den Benutzeragenten zu geben

Sicherheit

Metrik	Entität	Beschreibung
Anwendungen	Bedrohungsindex	Ein einstelliges Bewertungssystem, das die 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.
	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.

APPANALYTICS

Metrik	Entität	Beschreibung
Anwendungen	AppScore	App Score definiert, wie gut eine Anwendung funktioniert, und zeigt an, ob die Anwendung hinsichtlich der Reaktionsfähigkeit eine gute Leistung erbringt. Die Werte reichen von 0 bis 80.

HDX

Informationen zu HDX-Schwellenwerten finden Sie unter Erstellen von Schwellenwerten und Konfigurieren von Warnungen für HDX Insight.

Infrastrukturanalyse

March 12, 2024

Ein wichtiges Ziel für Netzwerkadministratoren ist die Überwachung von NetScaler-Instanzen. NetScaler-Instanzen bieten interessante Einblicke in die Nutzung und Leistung von Anwendungen und Desktops, auf die über sie zugegriffen wird. Administratoren müssen die NetScaler-Instanz überwachen und die von jeder NetScaler-Instanz verarbeiteten Anwendungsabläufe analysieren. Administratoren müssen außerdem in der Lage sein, mögliche Probleme bei Konfiguration, Einrichtung, Konnektivität, Zertifikaten und anderen Auswirkungen auf die Anwendungsnutzung oder -leistung zu beheben. Beispielsweise kann eine plötzliche Änderung des Anwendungsdatenverkehrsmusters auf eine Änderung der SSL-Konfiguration wie die Deaktivierung eines SSL-Protokolls zurückzuführen sein. 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 mehrere Datenquellen korreliert und zu einem messbaren Wert quantifiziert werden, der die Integrität einer Instanz definiert. Mit dieser Funktion erhalten Administratoren einen einzigen Kontaktpunkt, um das Problem, den Ursprung des Problems und die wahrscheinlichen Abhilfemaßnahmen, die sie durchführen können, zu verstehen.

Infrastrukturanalysen in NetScaler Console

Mit der Funktion Infrastructure Analytics werden alle aus den NetScaler-Instanzen gesammelten Daten zusammengefasst und in einen **Instanz-Score** quantifiziert, der die Integrität der Instanzen definiert. Die Instanzbewertung wird in einer tabellarischen Ansicht oder als Circle-Pack-Visualisierung zusammengefasst. Mit der Funktion Infrastructure Analytics können Sie die Faktoren visualisieren, die zu einem Problem in den Instanzen geführt haben oder 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 NetScaler-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 erklärt

- Indikatoren für Systemressourcen

Im Folgenden sind die kritischen Systemressourcenprobleme aufgeführt, die auf NetScaler-Instanzen auftreten können und von der NetScaler Console überwacht werden.

- **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 NetScaler-Instanz installiert ist.
- **Stromausfall**. Die Stromversorgung ist ausgefallen oder von der NetScaler-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 Instanz-Dashboard.

- Indikatoren für kritische Ereignisse

  Die folgenden kritischen Ereignisse werden durch die Event-Management-Funktion der NetScaler Console identifiziert, die mit kritischem Schweregrad konfiguriert sind.

  - **HA-Synchronisierung fehlgeschlagen**. Die Konfigurationssynchronisierung zwischen den NetScaler-Instanzen mit hoher Verfügbarkeit ist auf dem sekundären Server fehlgeschlagen.
  - **HA kein Herzschlag**. Der Primärserver in einem Paar von NetScaler-Instanzen mit hoher Verfügbarkeit empfängt keine Herzschläge vom sekundären Server.
  - **HA bad secondary state**. Der sekundäre Server in einem Paar von NetScaler-Instanzen mit hoher Verfügbarkeit befindet sich im sekundären Status Down, Unbekannt oder Stay.
  - **Nichtübereinstimmung der HA-Version**. Die Version der NetScaler-Software-Images, die auf einem Paar von NetScaler-Instanzen mit hoher Verfügbarkeit installiert sind, stimmt nicht überein.
  - **Fehler bei der Clustersynchron** Die Konfigurationssynchronisierung zwischen den NetScaler-Instanzen im Clustermodus ist fehlgeschlagen.

- **Nichtübereinstimmung der Clusterversion**. Die Version der NetScaler-Software-Images, die auf den NetScaler-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 kritischer SNMP-Ereignisse erstellen, 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 Console finden Sie unter [Ereignisse.] (/en-us/netscaler-console-service/networks/events.html)

- 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 NetScaler-Instanz installierte SSL-Zertifikat ist abgelaufen.
  - **Ablauf der SSL-Zertifikate ist fällig**. Das in der NetScaler-Instanz installierte SSL-Zertifikat läuft in der nächsten Woche ab.
  - **Nicht empfohlene Algorithmen**. Die Signaturalgorithmen der in der NetScaler-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.

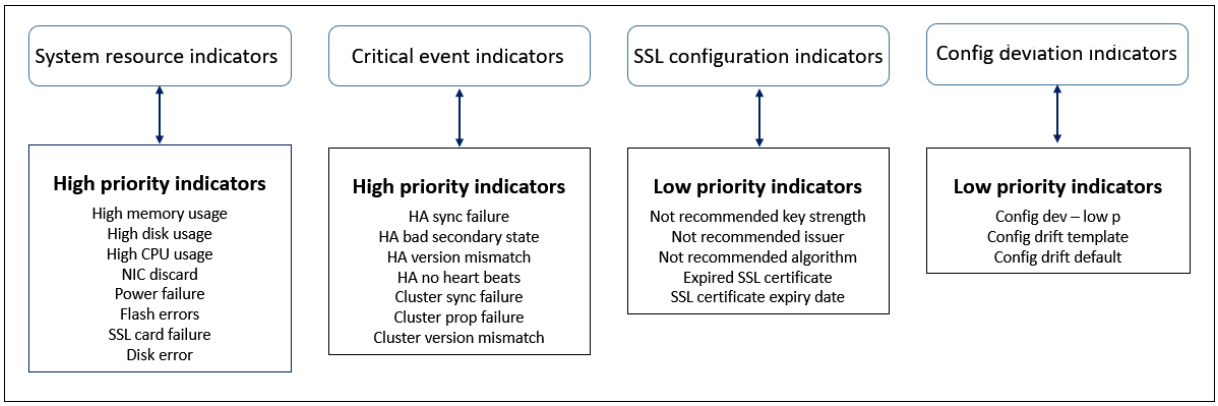
Weitere Informationen zu Konfigurationsabweichungen und zur Ausführung von Auditberichten zur Überprüfung von Konfigurationsabweichungen finden Sie unter Auditberichte anzeigen..

Probleme mit NetScaler Capacity anzeigen

Wenn eine NetScaler-Instanz ihre verfügbare Kapazität am meisten verbraucht hat, kann es bei der Verarbeitung des Client-Datenverkehrs zu einem Paketverlust kommen. Wenn Sie solche NetScaler-Kapazitätsprobleme verstehen, können Sie proaktiv zusätzliche Lizenzen zuweisen, um die NetScaler-Leistung aufrechtzuerhalten. Weitere Informationen finden Sie unter Anzeigen der Kapazitätsprobleme in einer NetScaler-Instanz .

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.

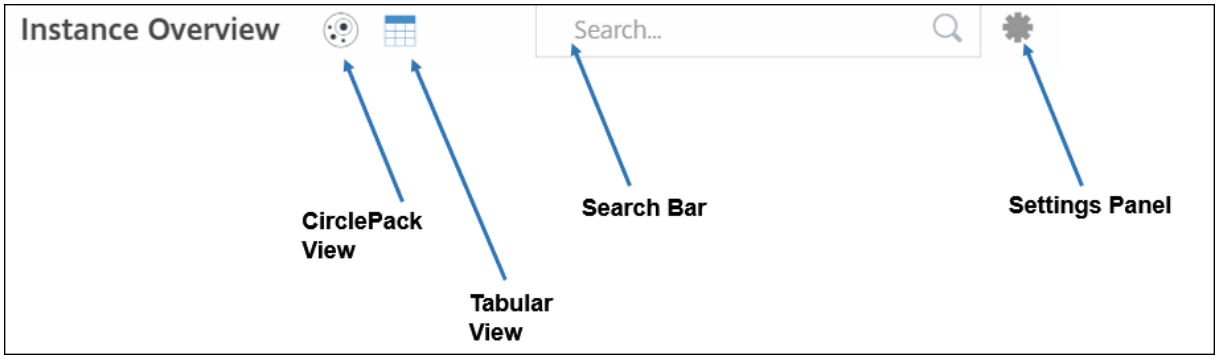
3. **Basierend auf der Verletzung des niedrigen und hohen Schwellenwerts**. Hier kann ein Indikator auf zwei Arten ausgelöst werden:
    - Wenn der Wert des Indikators zwischen niedrigen und hohen Schwellenwerten liegt, wird in diesem Fall eine Teilstrafe auf die Instanzbewertung erhoben.
    - Wenn 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.

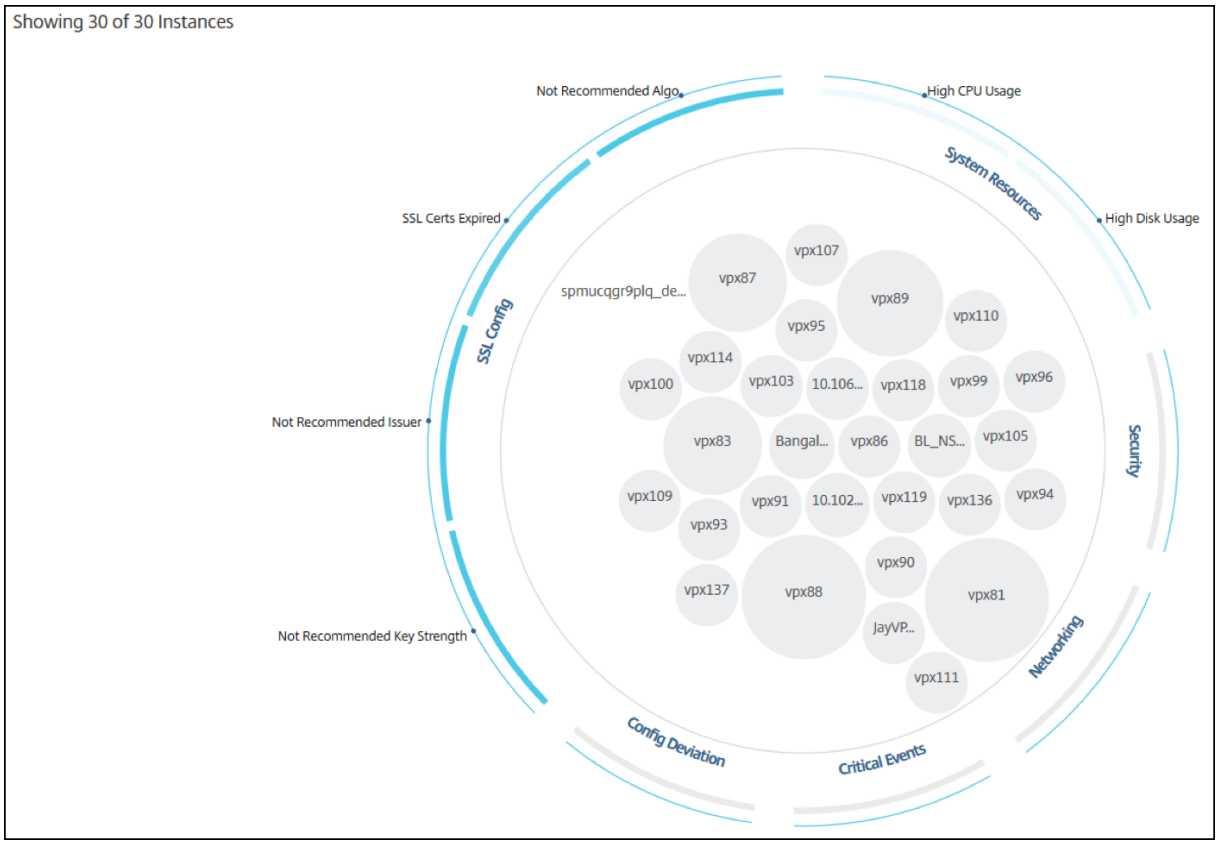


- In der Tabellenansicht können Sie nach einer Instanz suchen, indem Sie den Hostnamen oder die IP-Adresse in die Suchleiste eingeben.
- Standardmäßig wird auf der Seite Infrastructure Analytics rechts auf der Seite das Zusammenfassungsfenster angezeigt.
- Klicken Sie auf das Symbol **Einstellungen**, um die **Einstellungsleiste** anzuzeigen.
- In beiden Ansichtsformaten zeigt das Zusammenfassungsfenster Details aller Instanzen in Ihrem Netzwerk an.

Circle Pack-Ansicht

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.



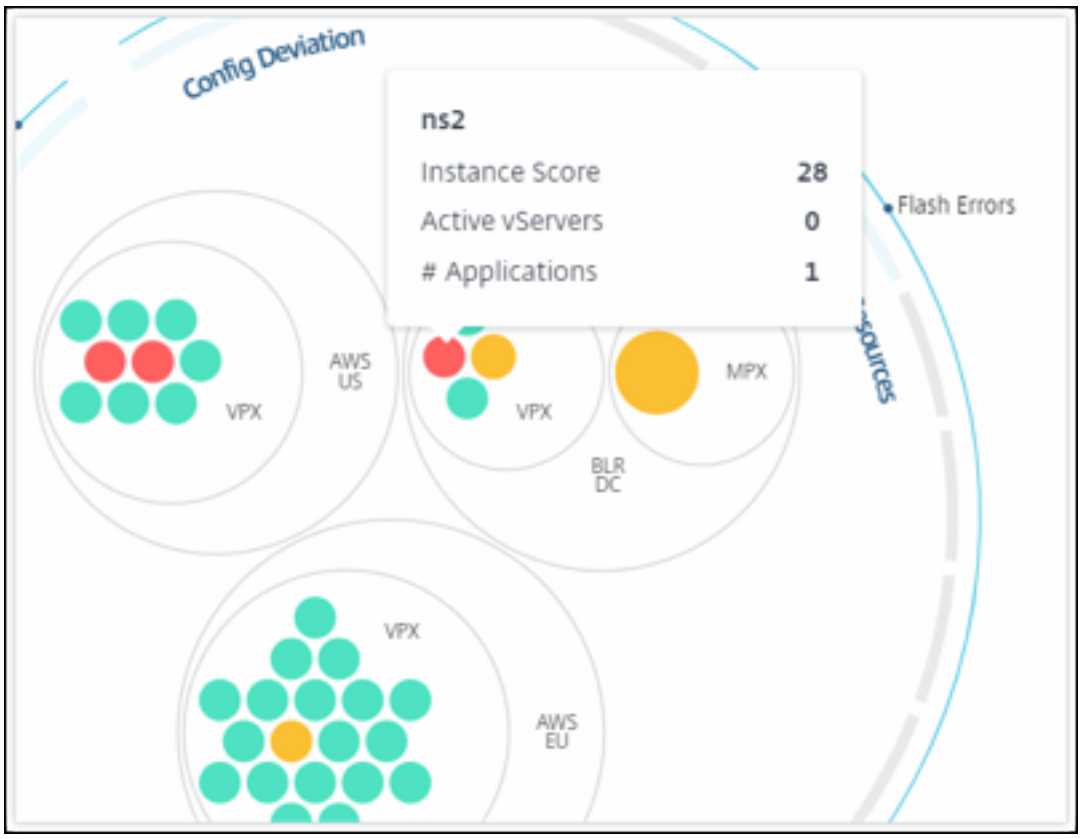
Instanzkreise

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** —Instanz-Score 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.

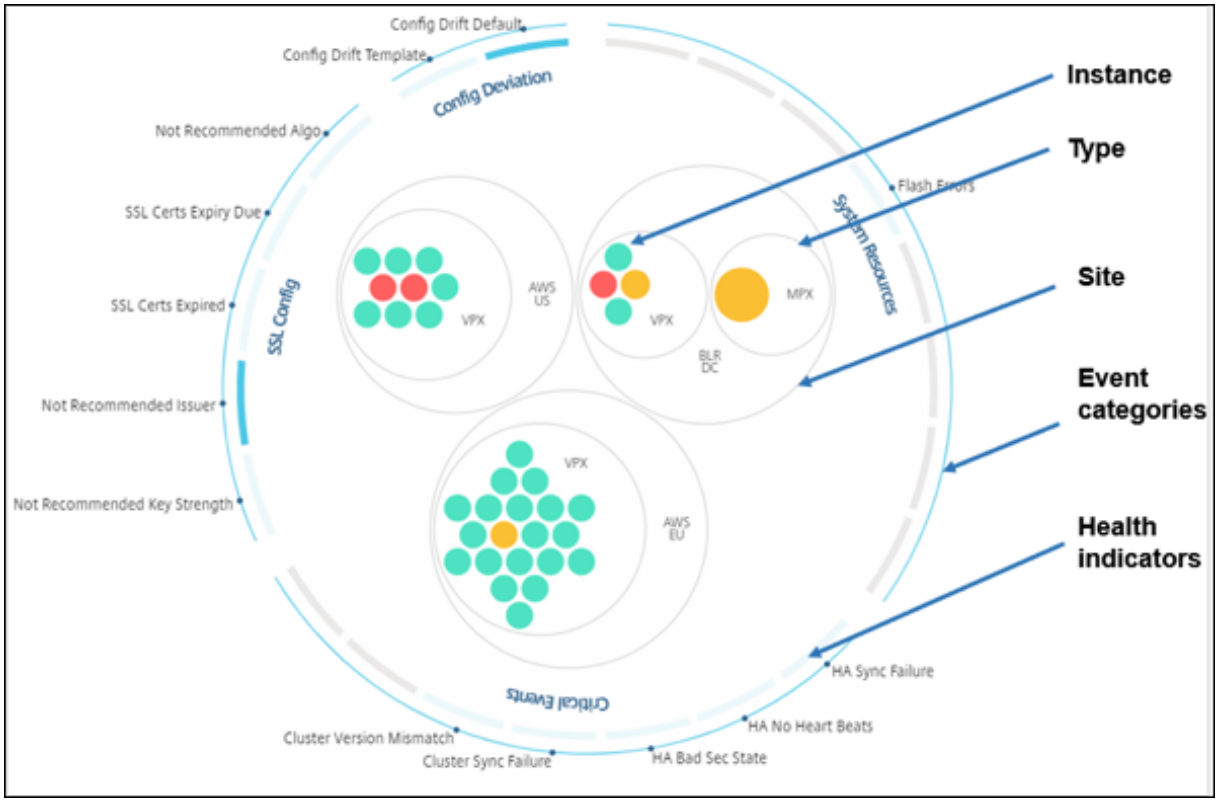


Gruppierte Instanzkreise

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 NetScaler-Instanz
- die auf den Instanzen installierte NetScaler-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.

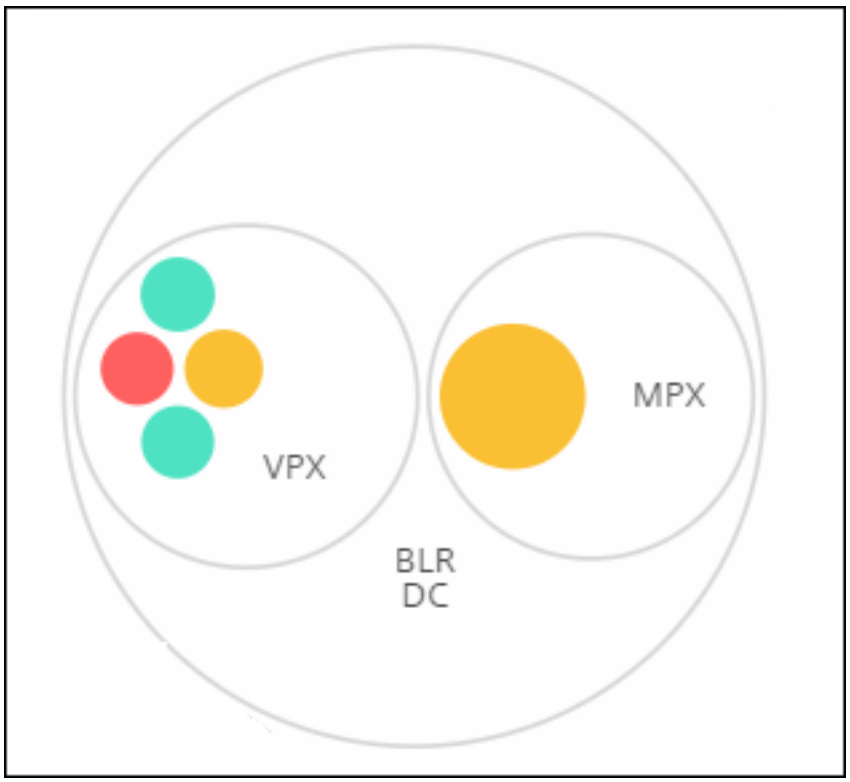


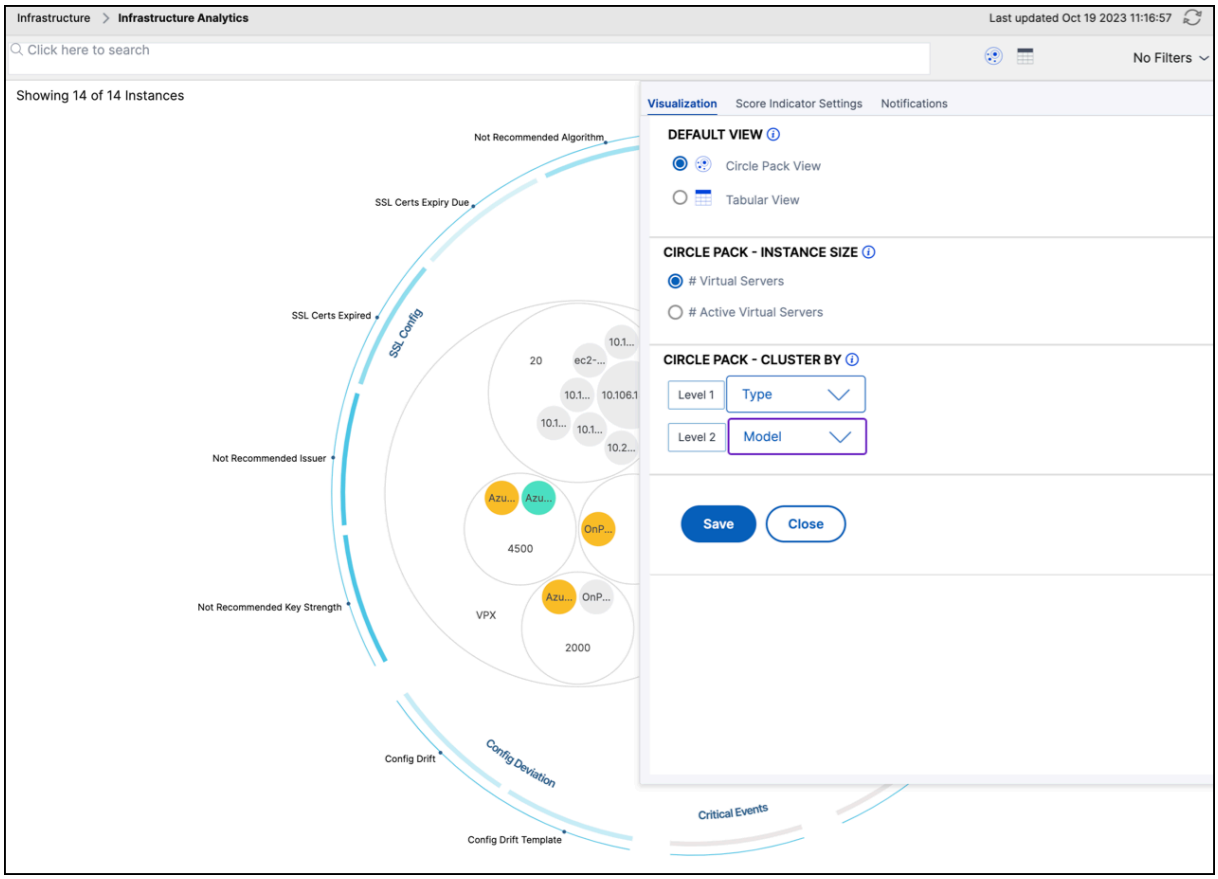
Alle diese verschachtelten Kreise werden von zwei äußersten Kreisen begrenzt. Die äußeren beiden Kreise stehen für die vier Kategorien von Ereignissen, die von der NetScaler Console überwacht werden (Systemressourcen, kritische Ereignisse, SSL-Konfiguration und Konfigurationsabweichung), sowie für die zugehörigen Integritätsindikatoren.

Gruppierte Instanzkreise

NetScaler Console 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.

Das BLR-Rechenzentrum verfügt beispielsweise über zwei Typen von NetScaler-Instanzen —VPX und MPX —, die darin bereitgestellt werden. Sie können die NetScaler-Instanzen zuerst nach ihrem Typ gruppieren und dann alle Instanzen nach der Site gruppieren, auf der sie gruppiert sind. Sie können jetzt leicht erkennen, wie viele Instanztypen in den von Ihnen verwalteten Sites bereitgestellt werden.

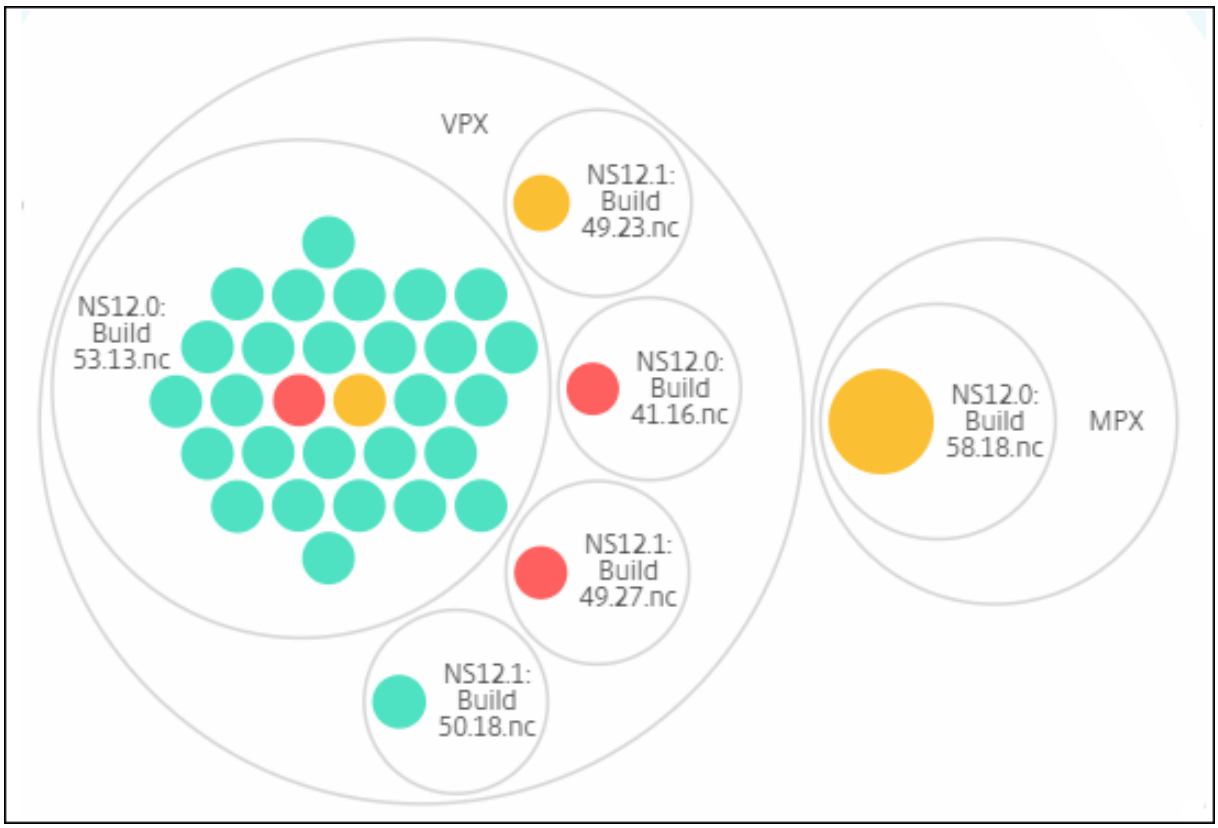




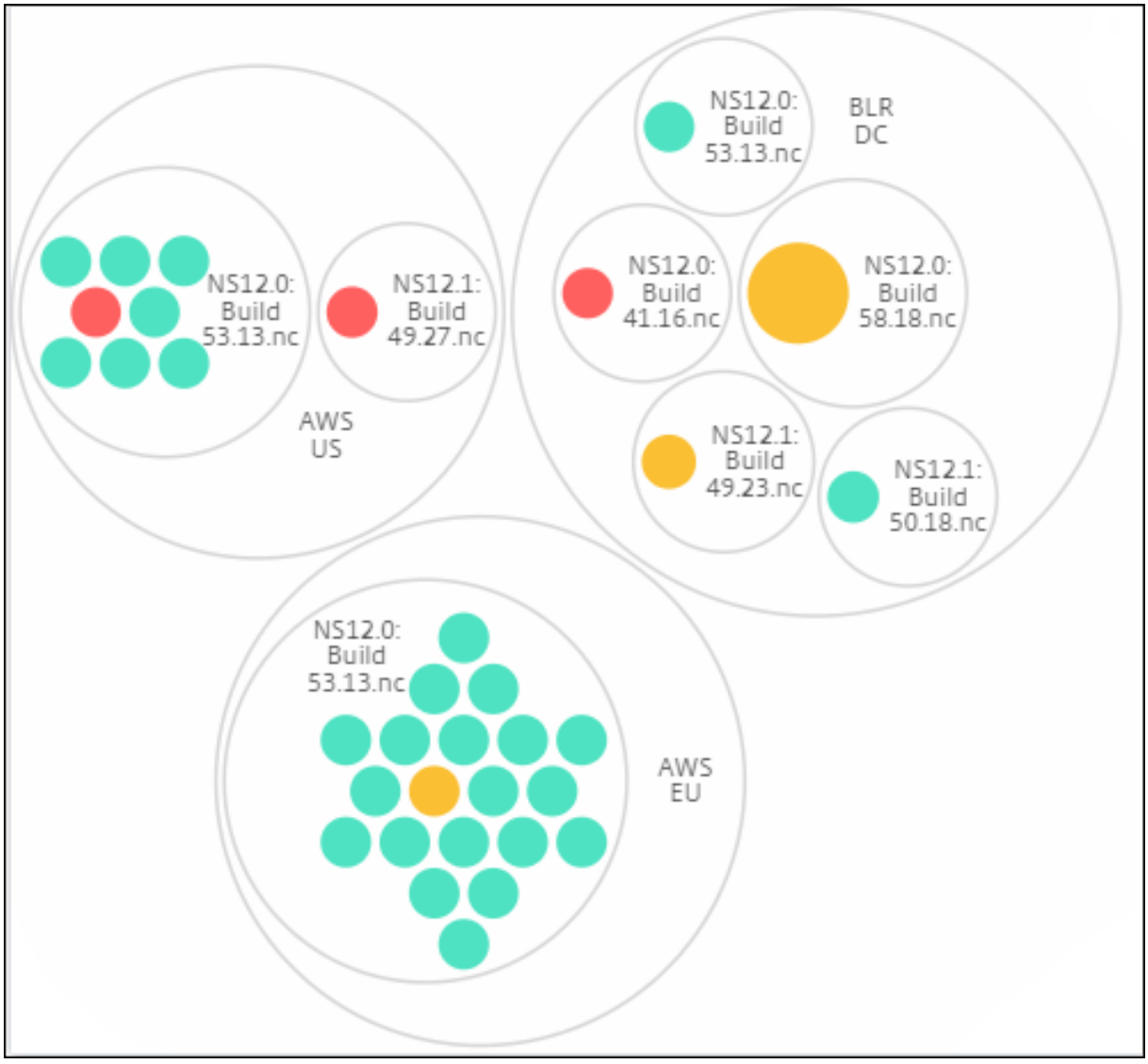
Ein paar weitere Beispiele für zweistufiges Clustering sind wie folgt:

Standort und Modell:

Typ und Ausführung:

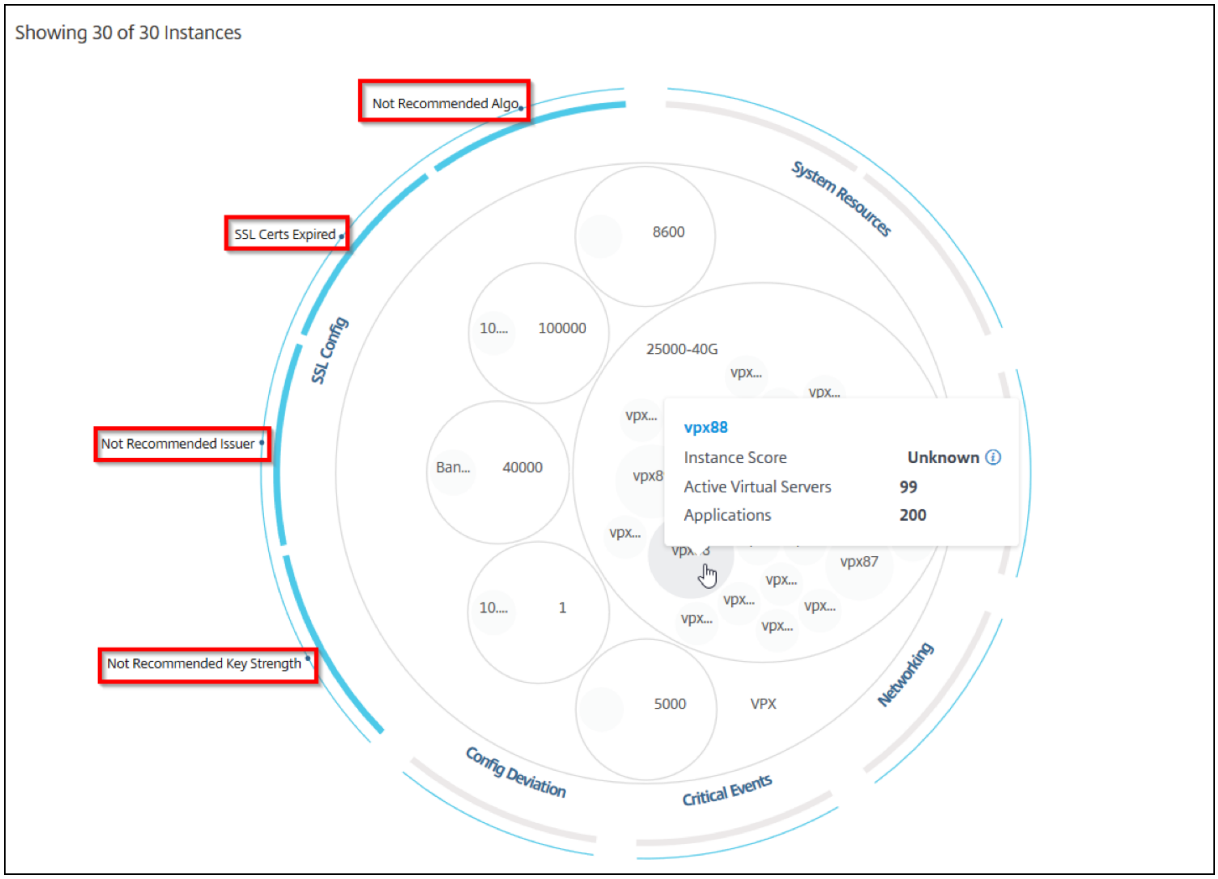


Website und Version:

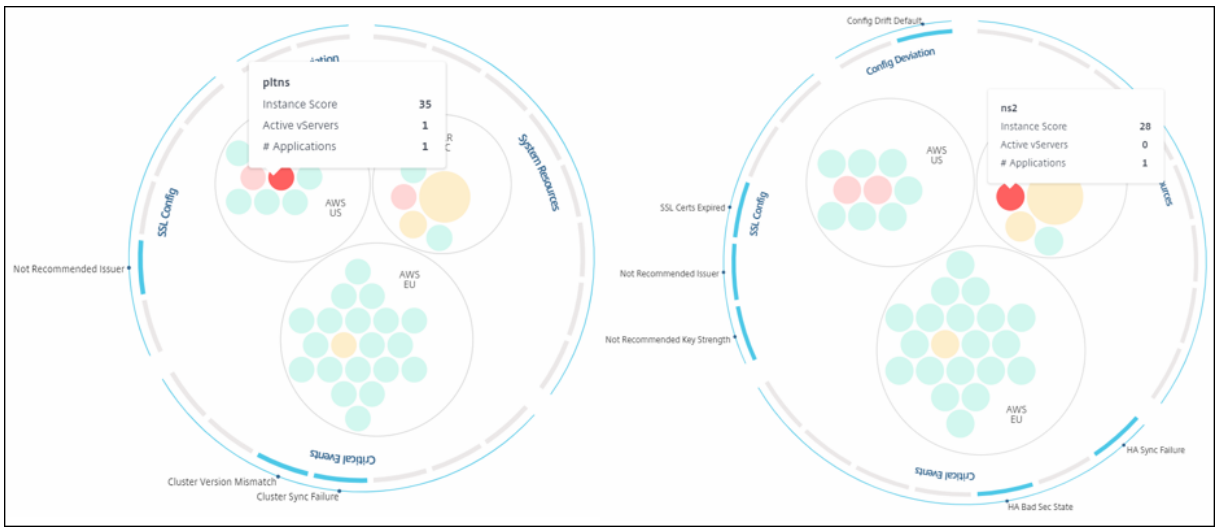


Wie benutzt man Circle Pack

Klicken Sie auf jeden der farbigen Kreise, um diese Instanz hervorzuheben.

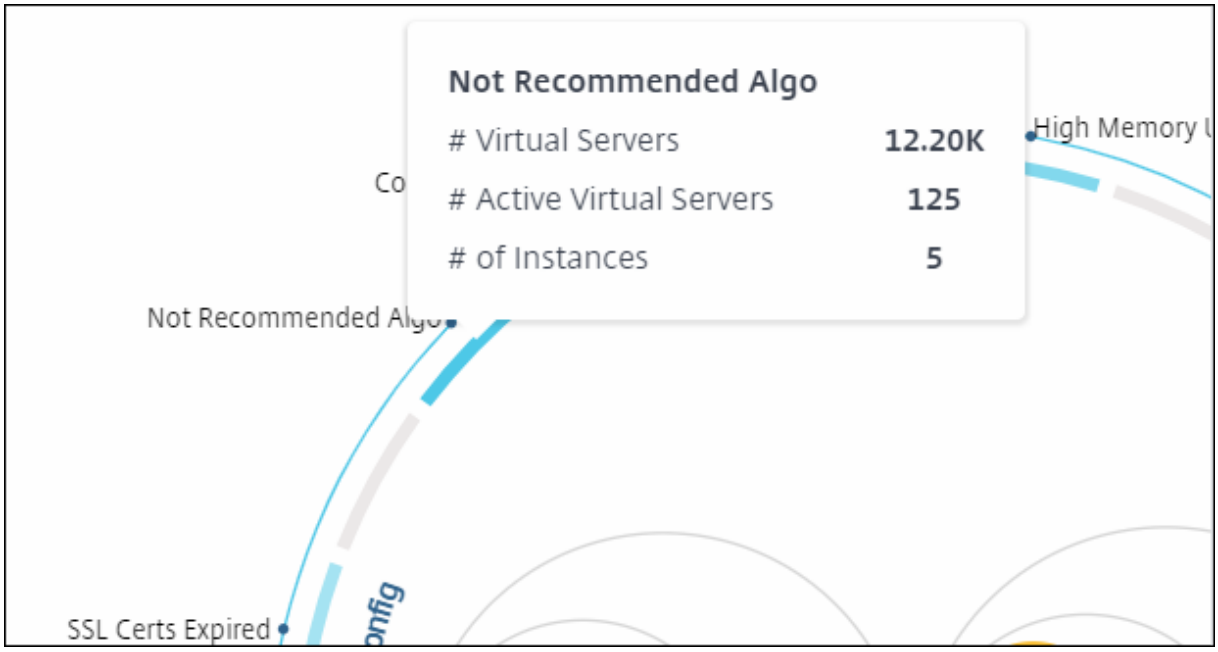


Abhängig von den Ereignissen, die in dieser Instanz aufgetreten sind, werden nur diese Gesundheitsindikatoren auf den äußeren Kreisen hervorgehoben. Die folgenden beiden Bilder des Circle Pack zeigen beispielsweise unterschiedliche Risikoindikatoren, obwohl sich beide Instanzen in einem kritischen Zustand 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.



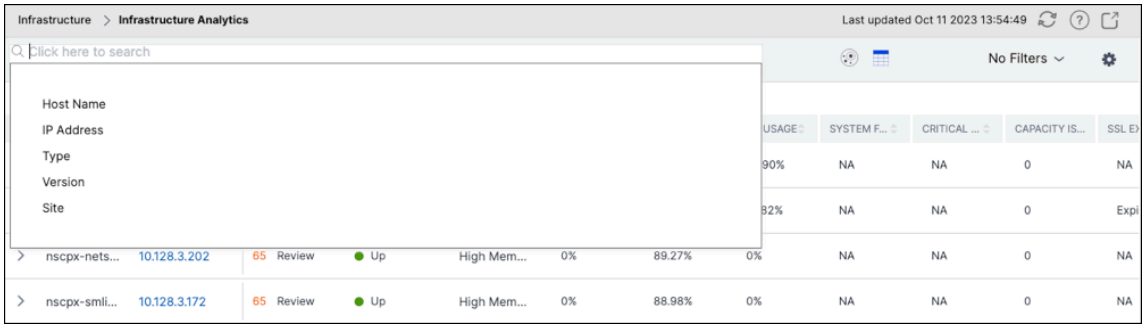
Tabellarische Ansicht

In der tabellarischen Ansicht werden die Instanzen und die Details dieser Instanzen in einem tabellarischen Format angezeigt. Weitere Informationen finden Sie unter Instanzdetails

Suchleiste

Platzieren Sie den Mauszeiger auf die Suchleiste und wählen Sie die folgenden Suchattribute aus, um die Ergebnisse zu filtern:

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



Die Suchergebnisse funktionieren sowohl für die Kreis- als auch für die Tabellenansicht.

So verwenden Sie das Übersichtsfenster

Das **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

Weitere Informationen zu diesen Indikatoren finden Sie unter *Integritätsindikatoren in NetScaler-Instanzen*.

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.

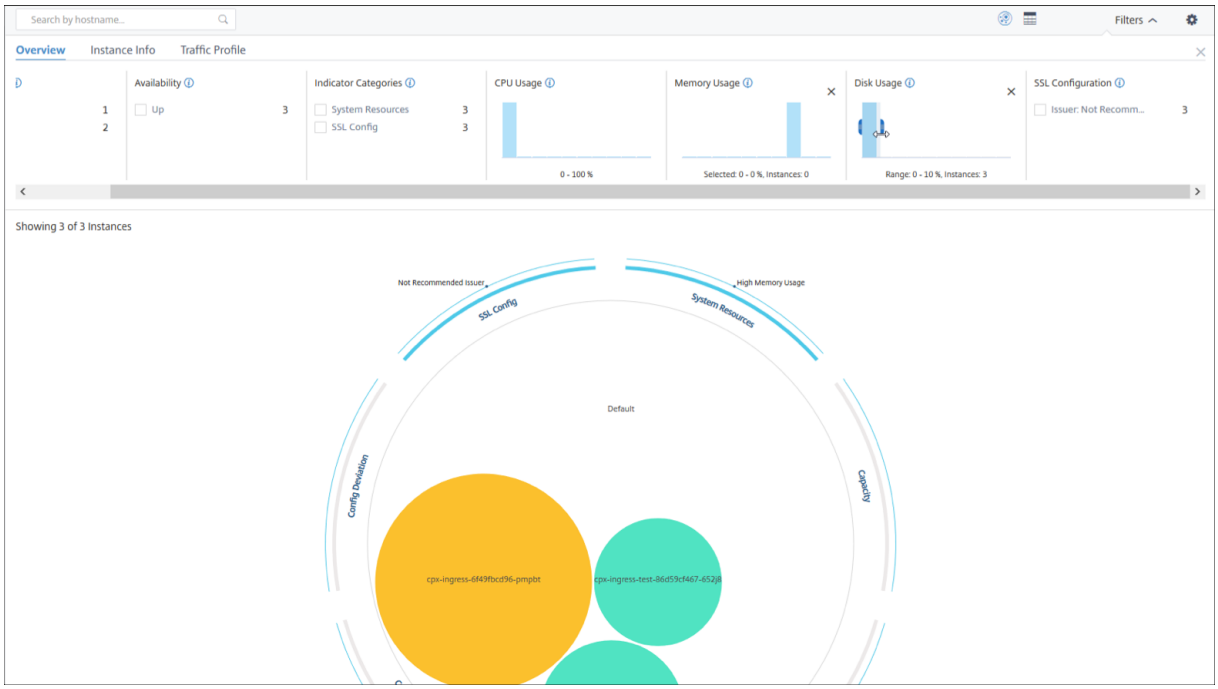
Beispiel 2: Zeigen Sie Instanzen an, die zwischen 10 und 20% des zugewiesenen Speichers verbrauchen:

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: Zeigen Sie Instanzen an, die Speicherplatz in mehreren Bereichen verbrauchen:

Um Instanzen anzuzeigen, die Speicherplatz zwischen 0 und 10% belegt haben, ziehen Sie den Mauszeiger über die beiden Bereiche, wie in der folgenden Abbildung dargestellt.



> **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 Sys-

temfehler, 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:

Aktivieren Sie im Abschnitt **Ablauf von SSL-Zertifikaten** das Kontrollkästchen **Abgelaufen**, um die drei Instanzen anzuzeigen.

1 —Klicken Sie auf die **Filterliste** .

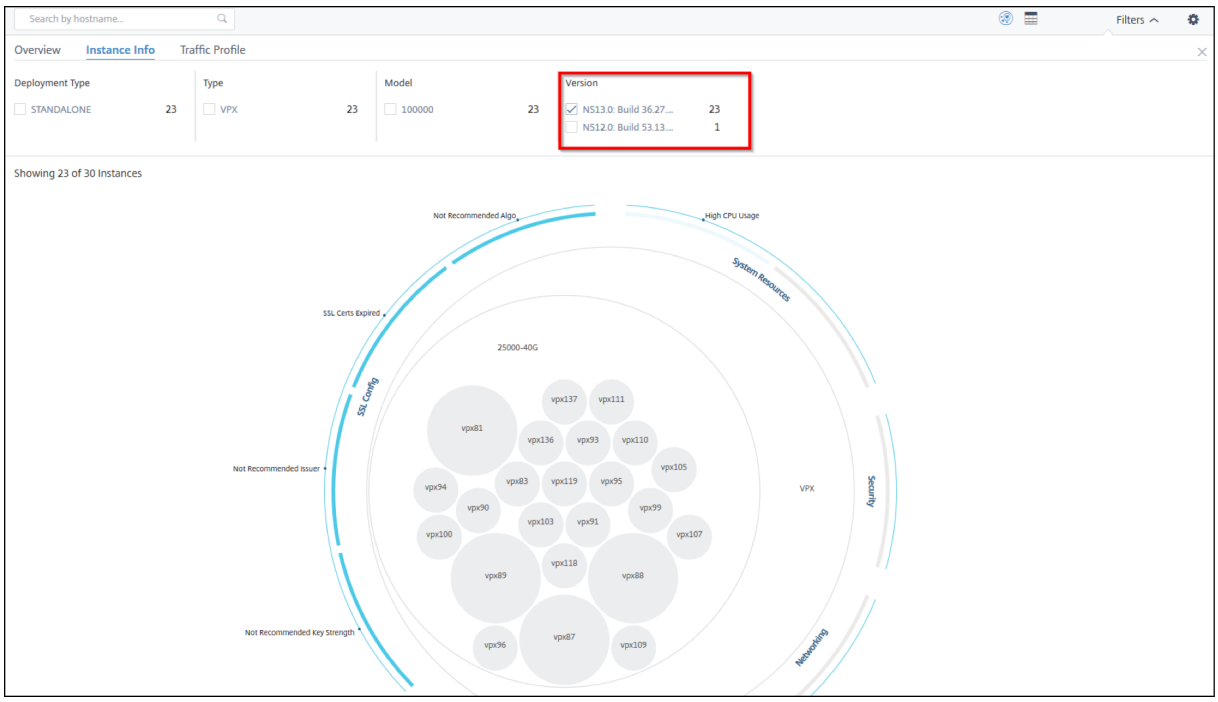
2 —Aktivieren Sie im Abschnitt **Ablauf von SSL-Zertifikaten** das Kontrollkästchen **Abgelaufen**, um die Instanzen anzuzeigen.

Instanz-Info

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.

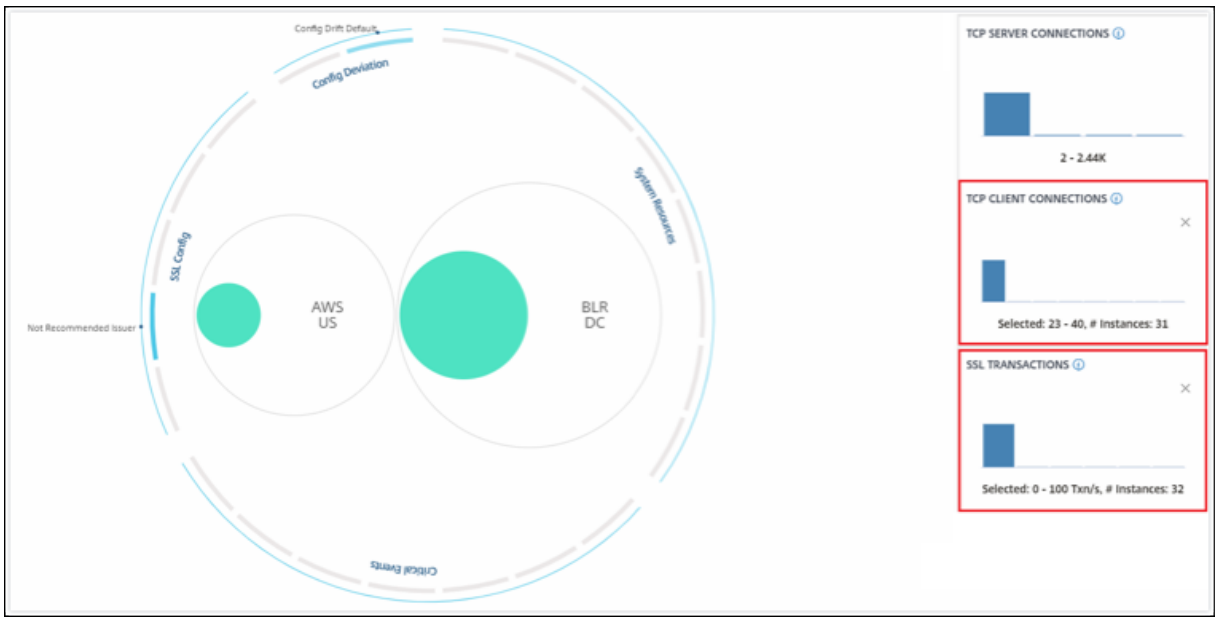


Traffic-Profil

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 zwischen 23 und 40 unterstützen und außerdem bis zu 100 SSL-Transaktionen pro Sekunde verarbeiten.



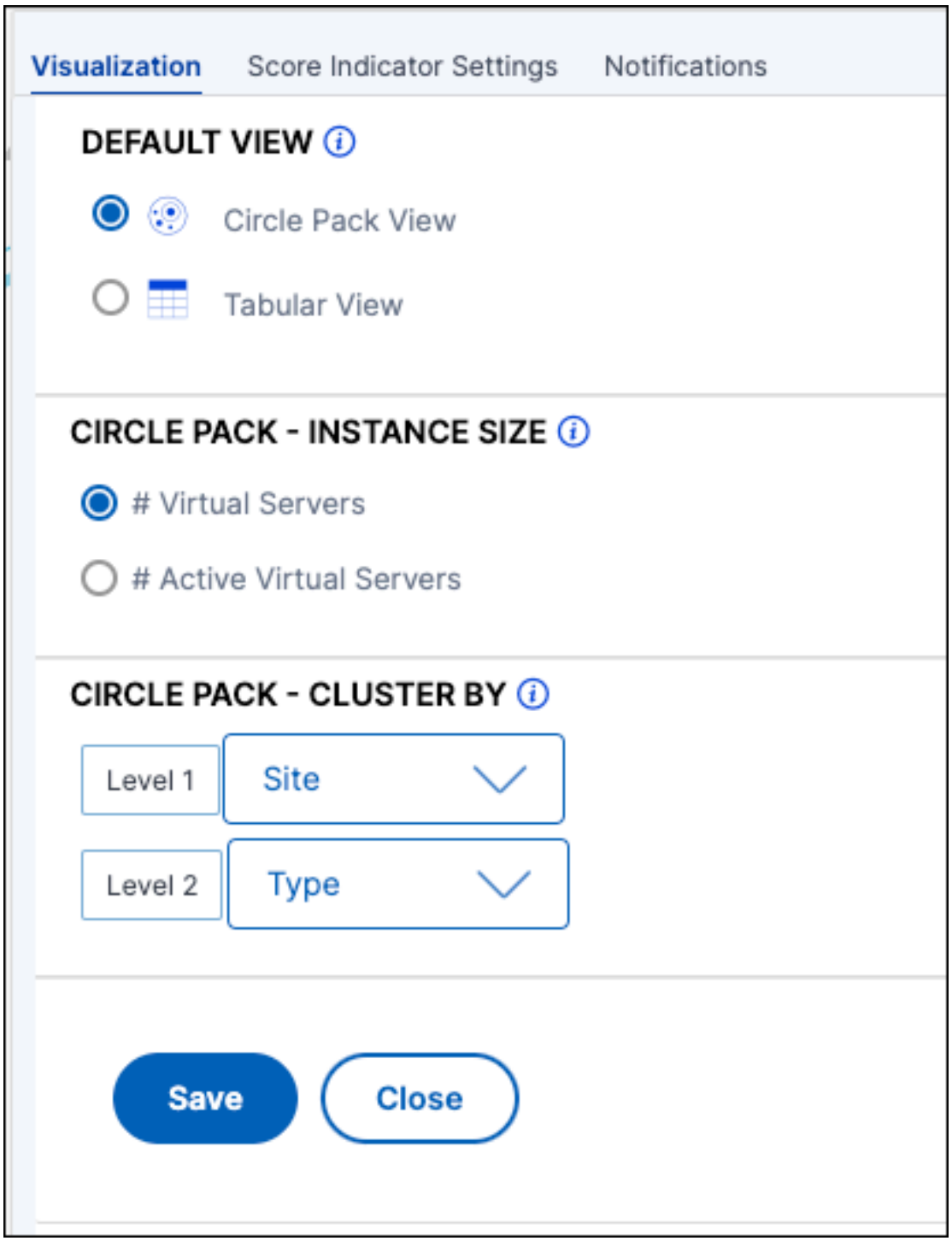
So verwenden Sie das Einstellungsfeld

Das Bedienfeld "**Einstellungen** "ermöglicht Ihnen:

- Legen Sie die Standardansicht der Infrastructure Analytics fest.
- Legen Sie die niedrigen und hohen Schwellenwerte für hohe CPU-Auslastung, hohe Datenträgerauslastung und hohe Speicherauslastung fest.
- Wählen Sie die Instanzmetriken aus, konfigurieren Sie Schwellenwerte und weisen Sie diesen Metriken Gewichtungen zu, um den Instanzwert
- Wählen Sie die erforderlichen Probleme aus, aktivieren Sie Benachrichtigungen für Probleme, die die konfigurierten Schwellenwerte überschreiten, und erhalten Sie Benachrichtigungen nur für die ausgewählten Probleme.

Ansicht

- **Standardansicht**. Wählen Sie **Circle Pack** oder Tabellarisches Format als Standardansicht auf der Analyseseite aus. Das Format, das Sie auswählen, wird angezeigt, wenn Sie die Seite in NetScaler Console aufrufen.
- **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 Instanz-Clustering finden Sie unter Clustered instance circles.



Wählen Sie Metriken und passen Sie die Gewichtung an, z. B. Instanzscoreberechnung

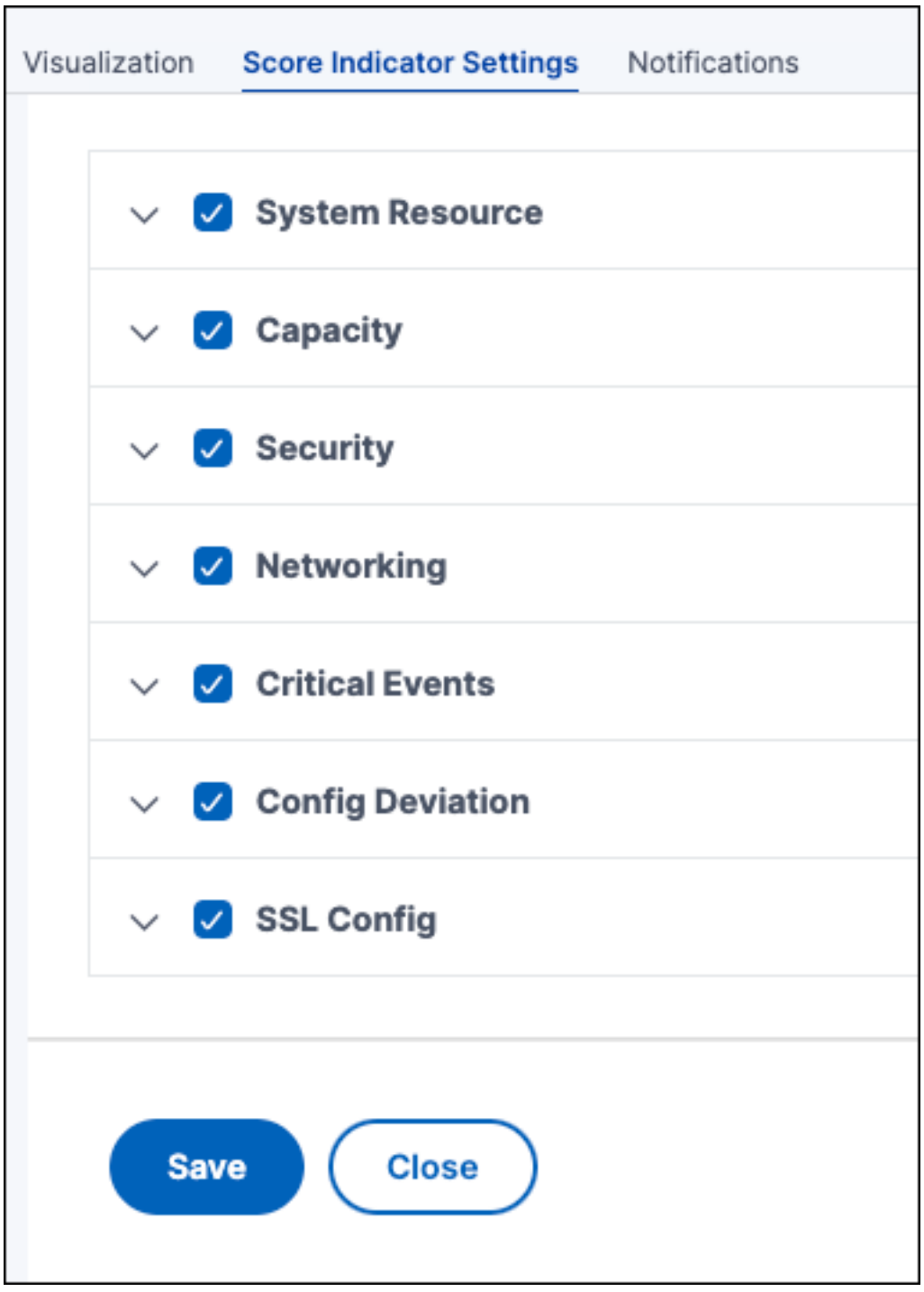
Sie können die Instanzmetriken auswählen, Schwellenwerte konfigurieren und diesen Metriken Gewichtungen zuweisen, um die Instanzbewertung zu berechnen. Standardmäßig sind alle Metriken ausgewählt, und jeder Metrik wird die Standardgewichtung zugewiesen. Sie können Metriken je

nach Anforderung auswählen und eine geeignete Gewichtung zuweisen, um die Berechnung des Instanz-Scores zu bestimmen.

Klicken Sie auf das Symbol **Einstellungen** und wählen Sie die Registerkarte **Score-Indikator-Einstellungen**, um

- Wählen Sie die erforderlichen Metriken und fügen Sie Schwellenwerte
- Weisen Sie die Gewichtung für Kennzahlen zu.

Nachdem Sie Schwellenwerte konfiguriert und Gewichtungen zugewiesen haben, klicken Sie auf **Speichern**. Die Instanzbewertung wird nur basierend auf den ausgewählten Metriken und ihrer Gewichtung aktualisiert.



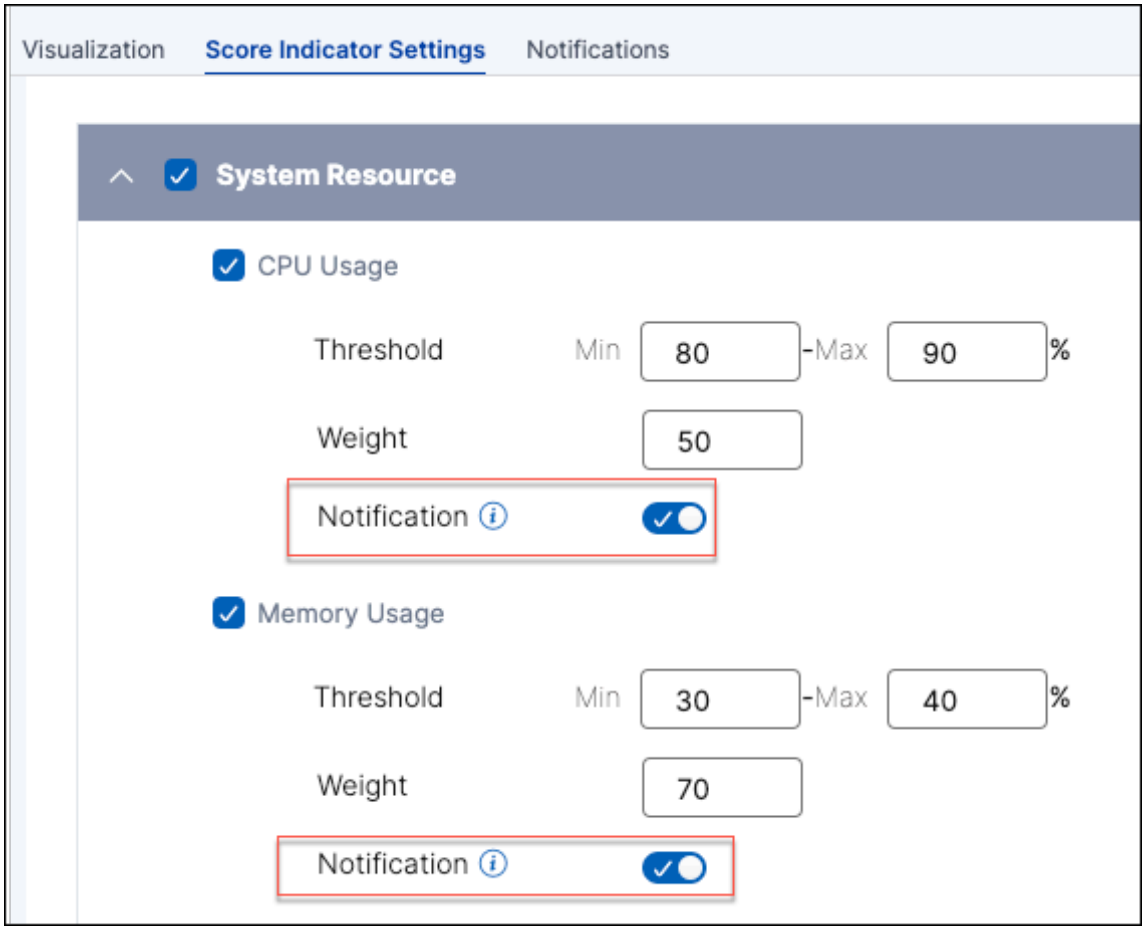
Benachrichtigungen konfigurieren

Sie können die erforderlichen Probleme auswählen, Benachrichtigungen für Probleme aktivieren, die die konfigurierten Schwellenwerte überschreiten, und Benachrichtigungen nur für die ausgewählten Probleme erhalten. Diese Erweiterung ermöglicht es Ihnen, Benachrichtigungen nur für

die ausgewählten Probleme zu erhalten, die Sie überwachen möchten.

> **Hinweis:**
>
> Standardmäßig sind Probleme in allen Kategorien ausgewählt. Sie können Benachrichtigungen nur für die Probleme aktivieren, für die Sie Schwellenwerte konfigurieren können.

1. Klicken Sie auf das Symbol **Einstellungen** und wählen Sie die Registerkarte **Bewertungsindikator-Einstellungen** .
2. Wählen Sie die Probleme aus, für die Sie Benachrichtigungen erhalten möchten.
3. Aktivieren Sie für die Probleme unter den Kategorien **Systemressourcen** und **Kapazität** die **Benachrichtigung**.



4. Klicken Sie auf **Speichern**.

> **Hinweis:**
>
> Sie müssen sicherstellen, dass Sie mindestens ein Profil auf der Registerkarte **Benachrichtigungen** konfigurieren.

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 dies genauer zu verstehen, betrachten wir den Fall von Chris, einem Netzwerkadministrator von ExampleCompany.

Chris unterhält viele NetScaler-Instanzen in seiner Organisation. Einige der Instanzen verarbeiten hohen Datenverkehr, und er muss sie genau überwachen. Er stellt fest, dass einige Instanzen mit hohem Datenverkehr nicht mehr den gesamten Datenverkehr verarbeiten, der durch sie fließt. Um diese Reduzierung zu analysieren, musste er zuvor mehrere Datenberichte aus verschiedenen Quellen lesen. Chris musste mehr Zeit damit verbringen, die Daten manuell zu korrelieren und herauszufinden, welche Instanzen sich nicht im optimalen Zustand befinden und Aufmerksamkeit benötigen. Er 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. Er klickt auf die Instanz, um zu sehen, wo das Problem liegt. In der Instanzzusammenfassung wird angezeigt, dass auf dieser Instanz ein SSL-Kartenfehler vorliegt und diese Instanz daher keinen SSL-Datenverkehr verarbeiten kann (der SSL-Datenverkehr wurde reduziert). Chris extrahiert diese Informationen und sendet einen Bericht an das Team, um das Problem sofort zu untersuchen.

Beispiel 2 - So überwachen Sie Konfigurationsänderungen:

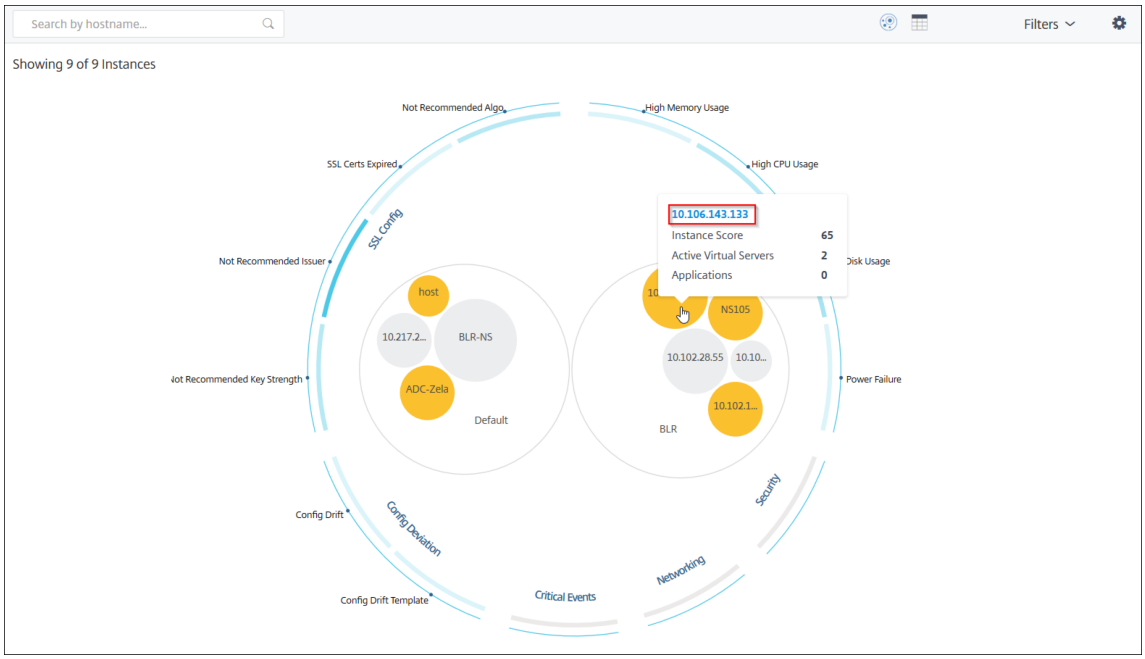
Chris bemerkt auch, dass sich eine andere Instanz im Status “Überprüfung”befindet und dass es in letzter Zeit eine Konfigurationsabweichung gegeben hat. Wenn er auf den Risikoindikator für Konfigurationsabweichungen klickt, bemerkt er, dass Konfigurationsänderungen im Zusammenhang mit RC4 Cipher, SSL v3, TLS 1.0 und TLS 1.1 vorgenommen wurden, die möglicherweise auf Sicherheitsbedenken zurückzuführen sind. Er bemerkt auch, dass das Profil des SSL-Transaktionsverkehrs für diese Instanz ausgefallen ist. Er exportiert diesen Bericht und sendet ihn an den Administrator, um ihn weiter zu erkundigen.

Instanzdetails in Infrastructure Analytics anzeigen

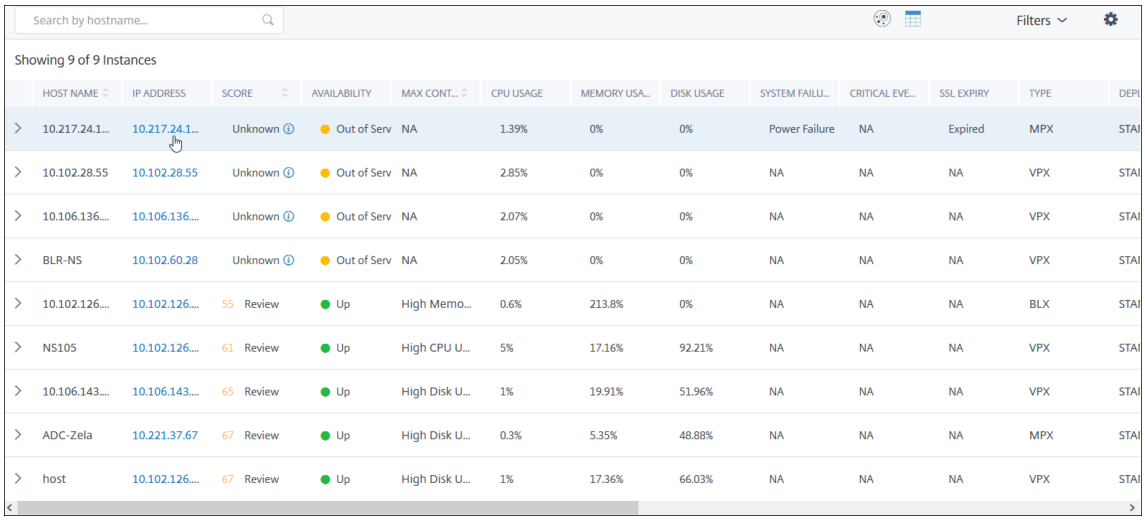
January 26, 2024

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 NetScaler-Instanz zugewiesen ist
- **IP-Adresse**—Bezeichnet die IP-Adresse der NetScaler-Instanz
- **Bewertung —Gibt den NetScaler-Instanz-Score**und den Status wie Kritisch, Gut und Fair an
- **Verfügbarkeit**—Bezeichnet den aktuellen Status der NetScaler-Instanz, z. B. **Up** , **Down** oder **Out of Service**.
- **Max Contribution**—Gibt die Problemkategorie an, in der die NetScaler-Instanz die maximale Fehleranzahl aufweist.

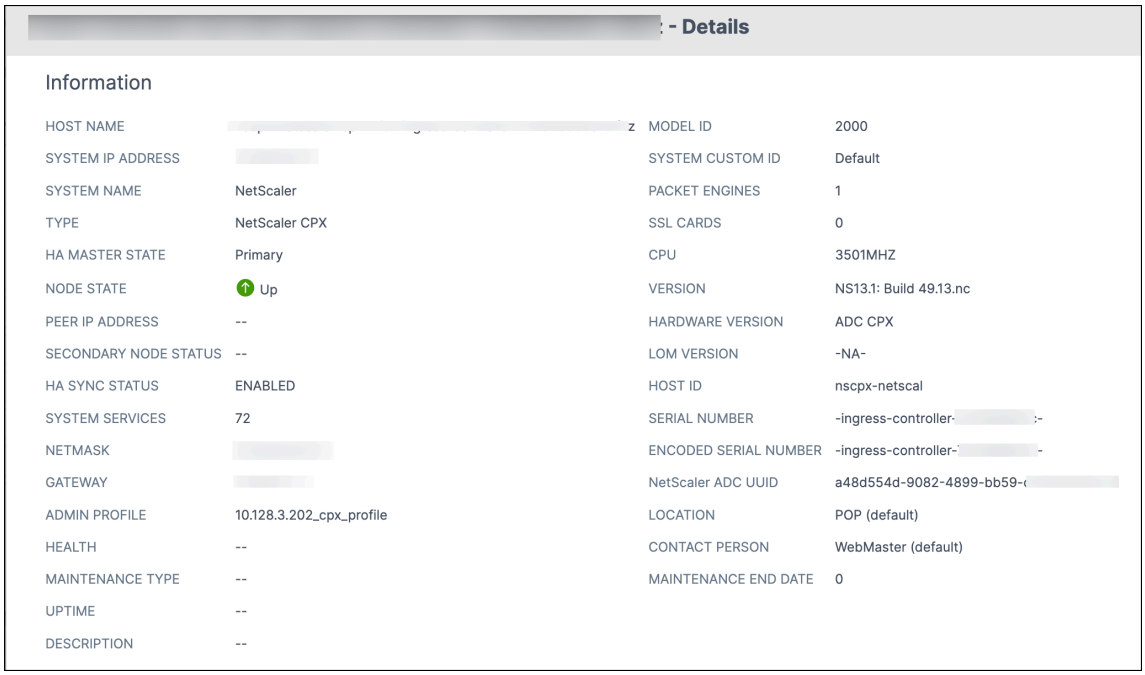
- **CPU-Auslastung** —Gibt den aktuellen CPU-Prozentsatz an, der von der Instanz verwendet wird
- **Speichernutzung** —Gibt den aktuellen Speicherprozentsatz an, der von der Instanz verwendet wird
- **Datenträgernutzung** —Gibt den aktuellen Datenträgerprozentsatz an, der von der Instanz verwendet
- **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**—Bezeichnet den aktuellen Status des auf der NetScaler-Instanz installierten SSL-Zertifikats
- **Typ**—Bezeichnet den NetScaler-Instanztyp wie VPX, SDX, MPX oder CPX
- **Bereitstellung**—Gibt an, ob die NetScaler-Instanz als eigenständige Instanz oder HA-Paar bereitgestellt wird
- **Model**—Bezeichnet die Modellnummer der NetScaler-Instanz
- **Version**—Bezeichnet die Version und Buildnummer der NetScaler-Instanz
- **Durchsatz**—Bezeichnet den aktuellen Netzwerkdurchsatz der NetScaler-Instanz.
- **HTTPS-Anforderung/Sekunde**—Bezeichnet die aktuellen HTTPS-Anforderungen/Sekunde, die von der NetScaler-Instanz empfangen wurden
- **TCP-Verbindung** —Bezeichnet die aktuell aufgebauten TCP-Verbindungen
- **SSL-Transaktion**—Bezeichnet die aktuellen SSL-Transaktionen, die von der NetScaler-Instanz verarbeitet werden
- **Site**—Bezeichnet den Namen der Site, auf der die NetScaler-Instanz bereitgestellt wird.

> **Hinweis:**
>
> Alle 5 Minuten werden die aktuellen Werte für CPU-Auslastung, Speichernutzung, Datenträgerauslastung, Durchsatz usw. aktualisiert.

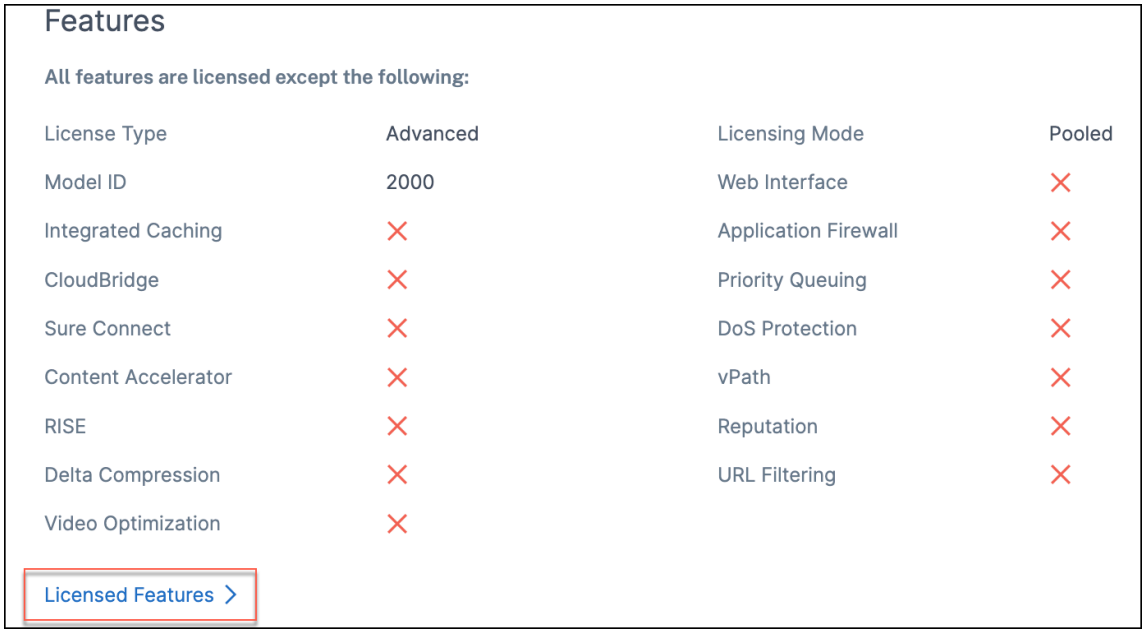
Klicken Sie auf eine IP-Adresse und auf der daraufhin angezeigten Seite auf **Instanzdetails**, um die Instanzdetails anzuzeigen.

Die folgenden Details werden angezeigt:

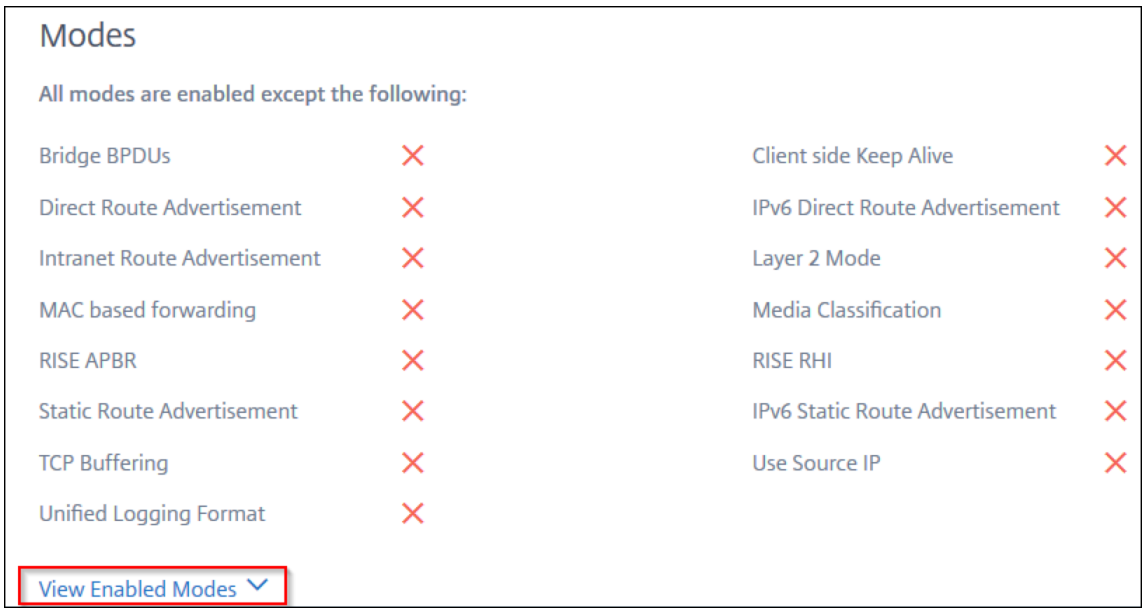
- **Informationen** —Instanzdetails wie Instanztyp, Bereitstellungstyp, Version, Modell usw.



- **Funktionen** —Standardmäßig werden die Funktionen angezeigt, die nicht lizenziert sind. Klicken Sie auf **Lizenzierte Funktionen**, um die lizenzierten Funktionen anzuzeigen.

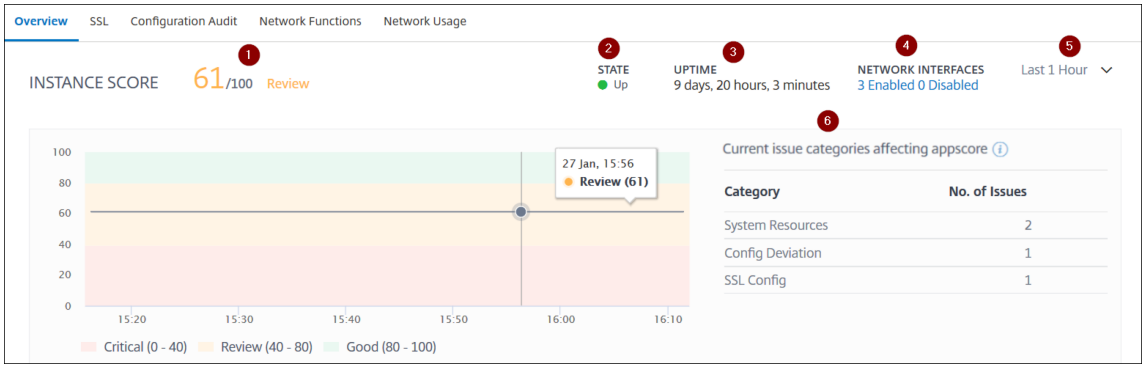


- **Modi** —Standardmäßig werden alle Modi angezeigt, die auf der Instanz deaktiviert sind. Klicken Sie auf **Aktivierte Modi** anzeigen, um die aktivierten Modi auf der Instanz anzuzeigen.



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 —Gibt den aktuellen Status der NetScaler-Instanz an, z. B. **Up-**, **Down-**und **Out-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 auf **Aktiviert** oder **Deaktiviert**, um Details wie den Namen der Netzwerkschnittstelle und den Status (aktiviert oder deaktiviert) anzuzeigen.

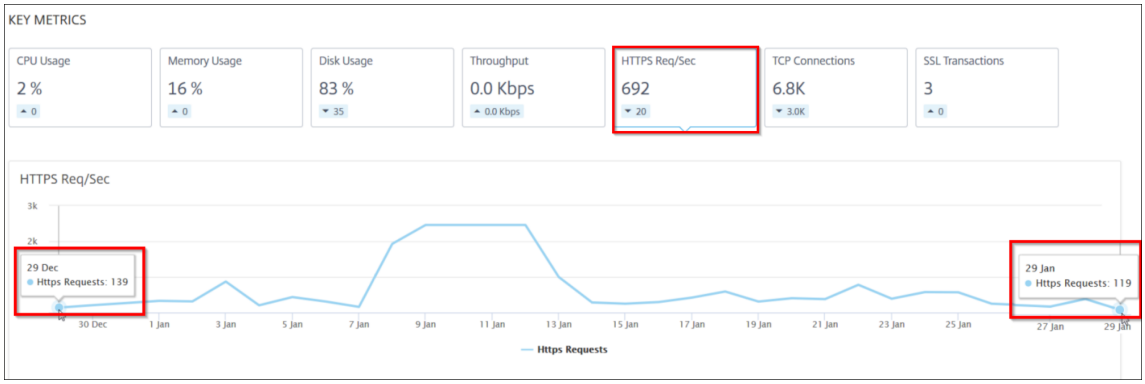
5 —Wählen Sie die Zeitdauer aus der Liste aus, um die Instanzdetails anzuzeigen.

6—Zeigt die Gesamtzahl der Probleme und die Problemkategorie der NetScaler-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.

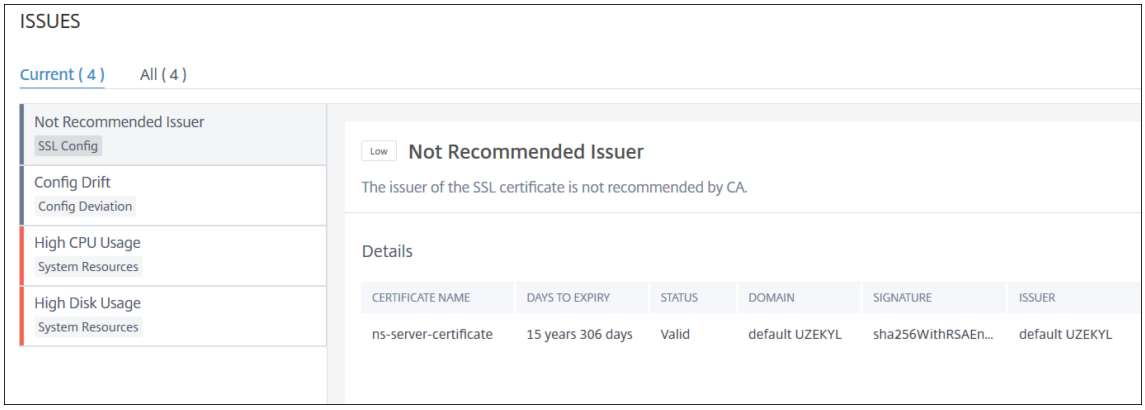
- **Probleme**

  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 an, wie CPU, Arbeitsspeicher, Datenträgernutzung usw.	– 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 empfohlen Algo – 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 – Fehler bei der Cluster

Kategorie der Ausgabe	Beschreibung	Probleme
		– Nicht übereinstimmende Cluster-Versionen – HA Bad Sec State – HA Keine Hitze schlägt – HA-Synchronisierungsfehler – Nichtübereinstimmung der HA-Version
Kapazitätsprobleme	Zeigt NetScaler-Kapazitätsprobleme an. Die NetScaler Console fragt diese Ereignisse alle fünf Minuten von der NetScaler-Instanz ab und zeigt, falls vorhanden, die Paketverluste oder die Erhöhung des Ratenlimits an. Die Probleme sind nach den folgenden Kapazitätsparametern kategorisiert.	– Durchsatzlimit erreicht
Netzwerke	Zeigt die Betriebsprobleme an, die in den Instanzen auftreten.	Weitere Informationen finden Sie unter Verbesserte Infrastrukturanalyse mit neuen Indikatoren.

Klicken Sie auf die einzelnen Registerkarten, um das Problem zu analysieren und zu beheben. 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.

Sehen Sie sich die Kapazitätsprobleme in einer NetScaler-Instanz an

January 26, 2024

Wenn eine NetScaler-Instanz ihre verfügbare Kapazität am meisten verbraucht hat, kann es bei der Verarbeitung des Client-Datenverkehrs zu einem Paketverlust kommen. Dieses Problem führt zu einer niedrigen Leistung in einer NetScaler-Instanz. Wenn Sie solche NetScaler-Kapazitätsprobleme verstehen, können Sie proaktiv zusätzliche Lizenzen zuweisen, um die NetScaler-Leistung aufrechtzuerhalten.

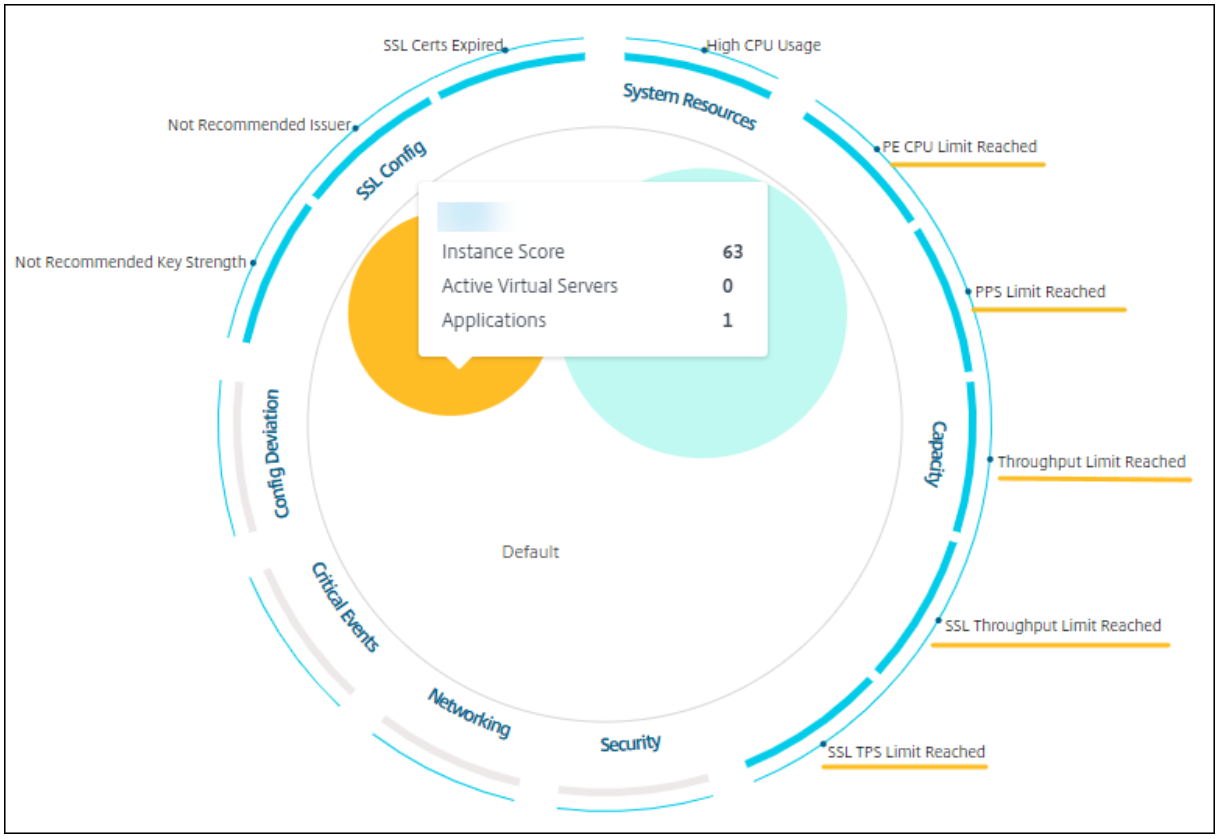
In der **Circle Pack-Ansicht** können Sie die Kapazitätsprobleme der NetScaler-Instanz anzeigen, falls vorhanden.

Um NetScaler-Kapazitätsprobleme anzuzeigen,

1. Navigieren Sie zu **Infrastruktur > Infrastructure Analytics**.
2. Wählen Sie die Ansicht des Kreispakets aus.

> **Hinweis:**
>
> In **Infrastructure Analytics**zeigen die Circle-Pack- und Tabellenansichten 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:



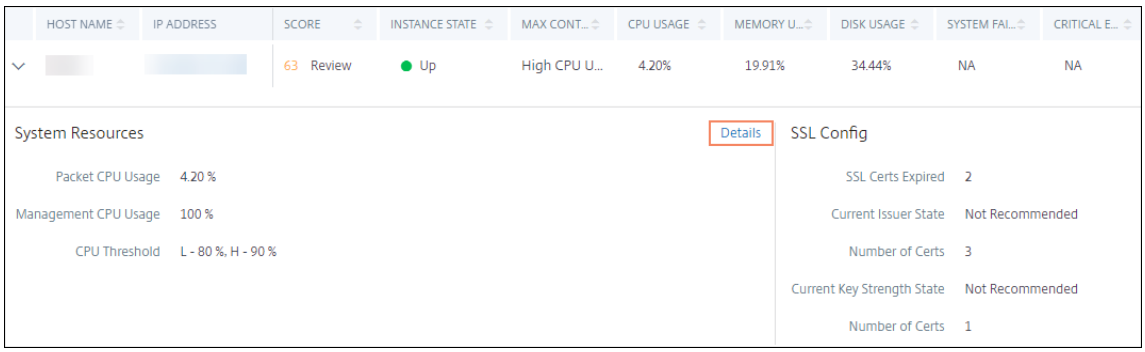
Die Probleme sind nach den folgenden Kapazitätsparametern kategorisiert:

- **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 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.

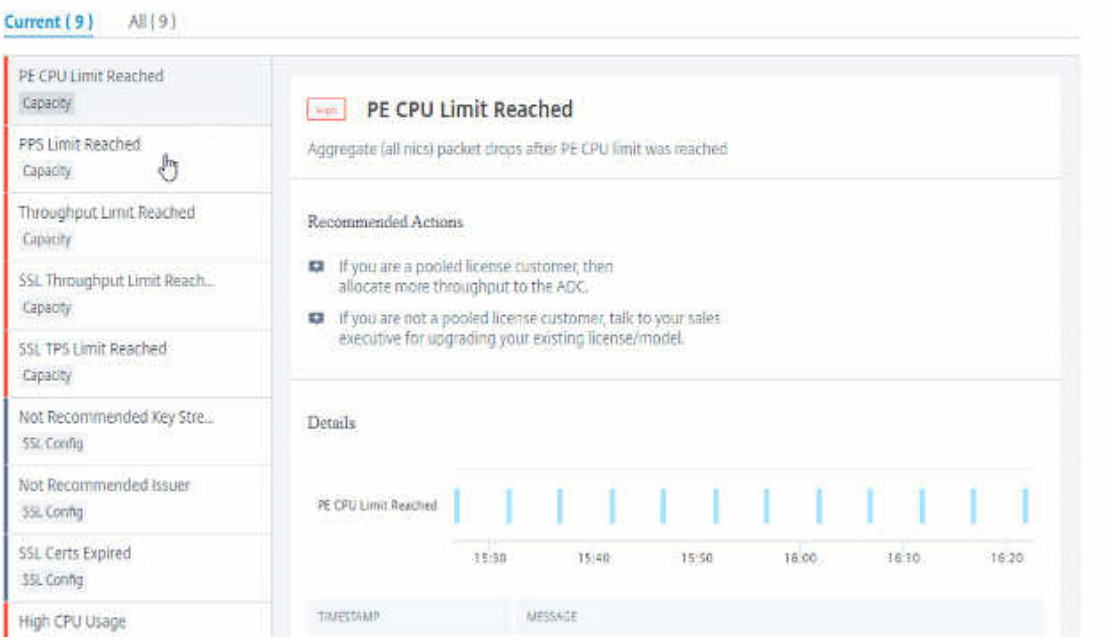
Empfohlene Maßnahmen zur Lösung von Kapazitätsproblemen anzeigen

Die NetScaler Console 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.



Die NetScaler Console fragt diese Ereignisse alle fünf Minuten von der NetScaler-Instanz ab und zeigt, falls vorhanden, die Paketverluste oder die Erhöhung des Ratenlimits an.

Die NetScaler Console berechnet den Instanzwert anhand des definierten Kapazitätsschwellenwerts.

- **Niedriger Schwellenwert** —1 Zählerinkrement für Paketverlust oder Ratenbegrenzung
- **Hoher Schwellenwert** —10.000 Paketverlust oder Erhöhung des Ratenlimit-Zählers

Wenn eine NetScaler-Instanz den Kapazitätsschwellenwert überschreitet, wirkt sich dies daher auf die Instanzbewertung aus.

Wenn Pakete fallen oder der Zähler für die Ratenbegrenzung inkrementiert wird, wird ein Ereignis in der Kategorie `ADCCapacityBreach` generiert. Um diese Ereignisse anzuzeigen, navigieren Sie zu

Einstellungen > Systemereignisse.

Verbesserte Infrastrukturanalyse mit neuen Indikatoren

January 26, 2024

Mit der NetScaler Console **Infrastructure Analytics** können 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.

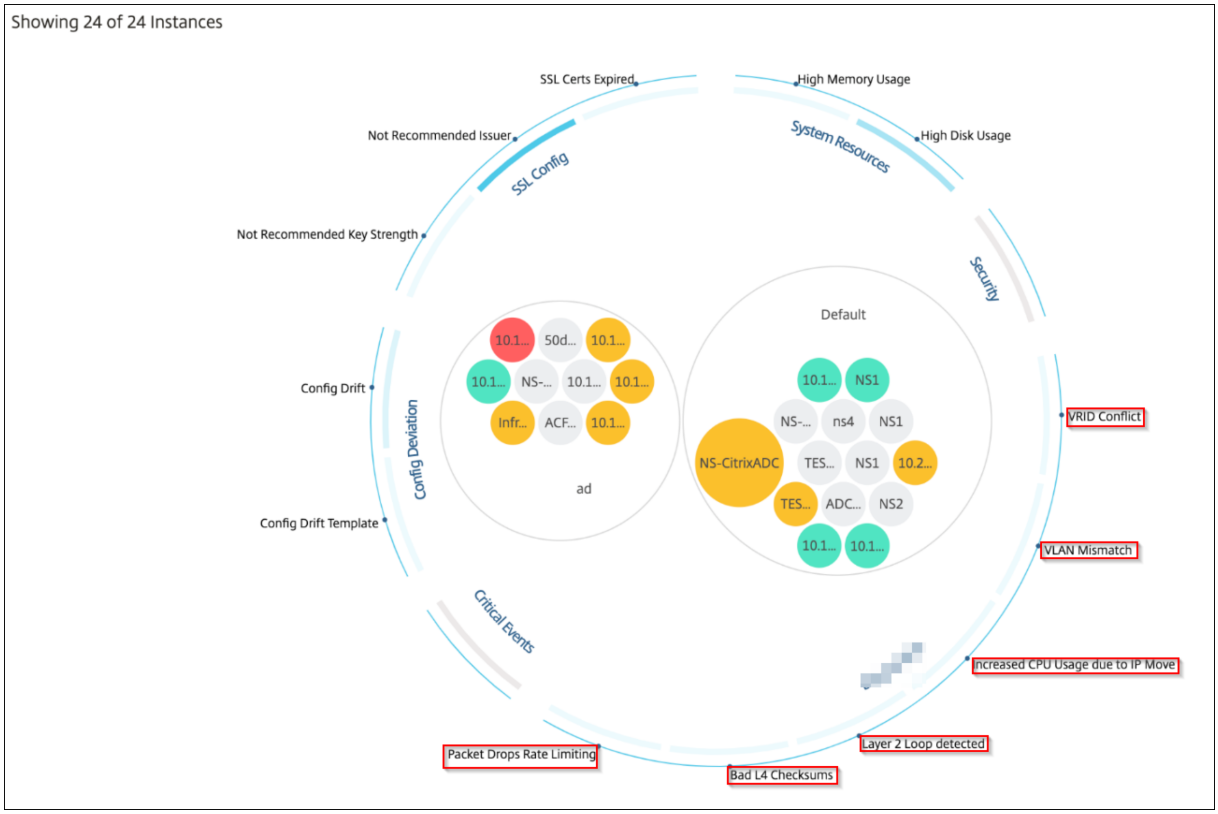
Als Administrator können Sie schnell die Ursachenanalyse von Problemen identifizieren.

> **Hinweis:**
>
> Regelindikatoren werden nicht unterstützt für:
>
> - NetScaler-Instanzen, die im Clustermodus konfiguriert sind.
> - NetScaler-Instanzen, die mit Administratorpartitionen konfiguriert sind.

Navigieren Sie in der NetScaler Console zu **Infrastructure > Infrastructure Analytics** , um Indikatoren für Folgendes anzuzeigen:

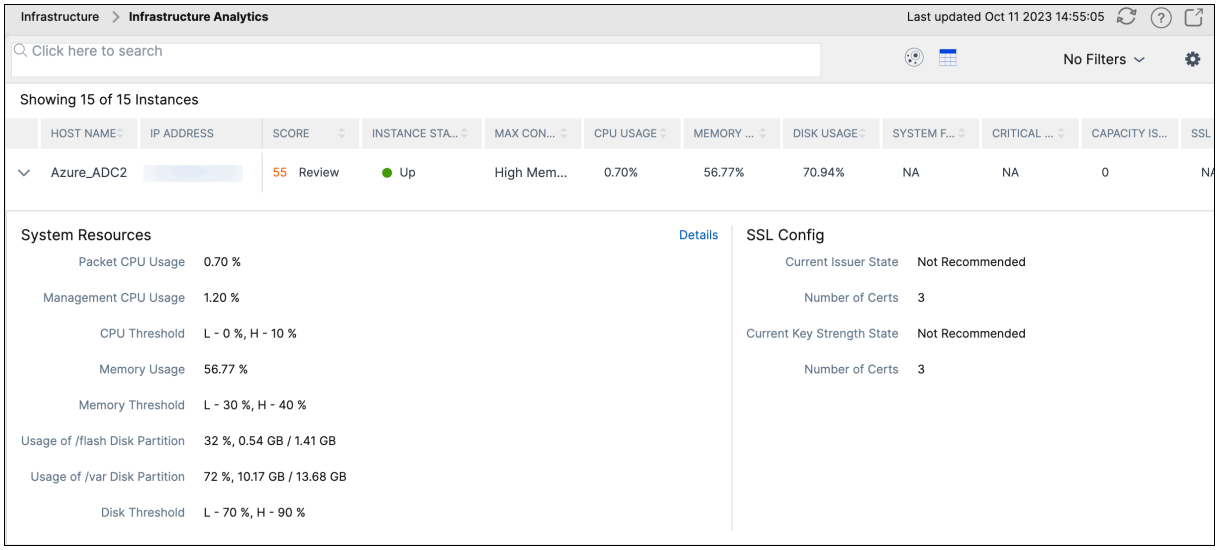
Indikatorname in Infrastructure Analytics	Beschreibung
Fehler bei Portzuweisung	Erkennt, wenn NetScaler SNIP verwendet, um mit einer neuen Serververbindung zu kommunizieren, und die Gesamtzahl der auf diesem SNIP verfügbaren Ports erschöpft ist. Die empfohlene Aktion besteht darin, ein weiteres SNIP im selben Subnetz hinzuzufügen.
Aufbau der Sitzung	Erkennt, wenn NetScaler-Speicher von SSL-Sitzungen gehalten wird.
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.

Indikatorname in Infrastructure Analytics	Beschreibung
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.
TCP-Angriff auf kleine Fenster	Erkennt, wenn möglicherweise ein kleiner Fensterangriff im Gange ist. Diese Warnung dient nur zu Informationszwecken, da NetScaler 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.



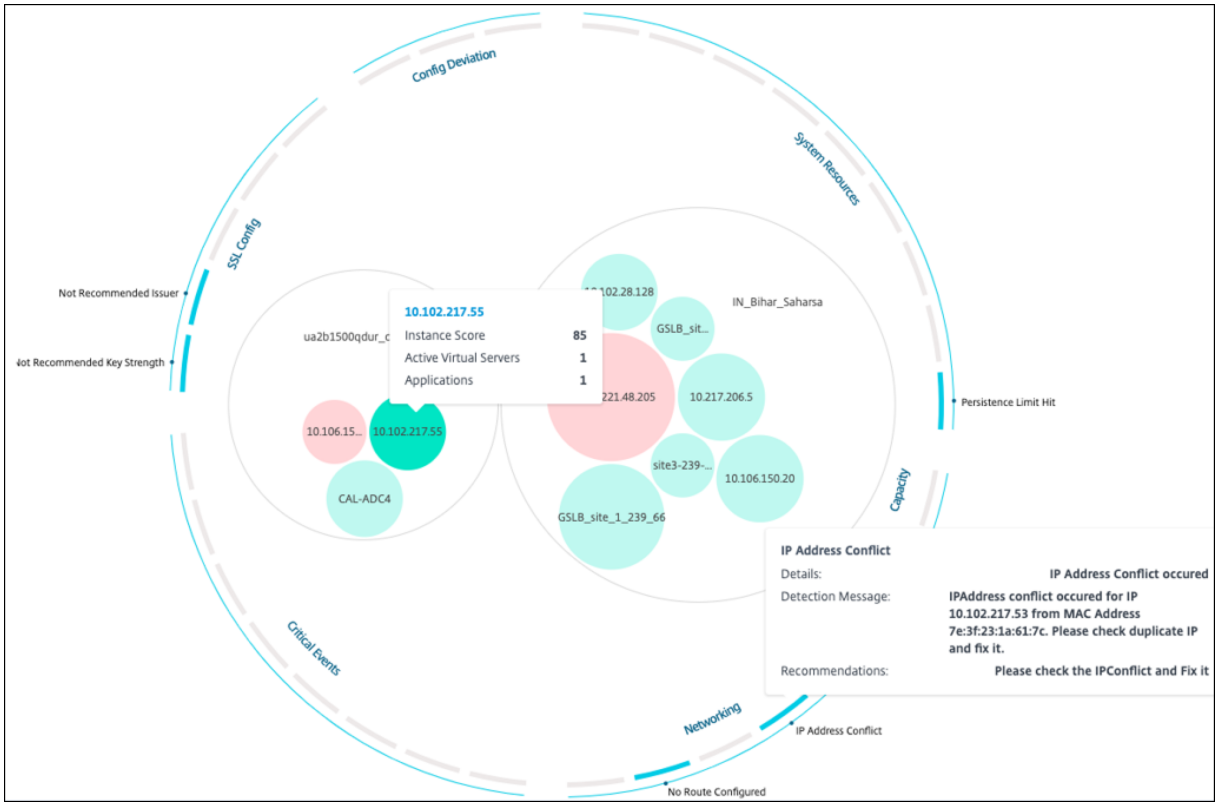
Tabellarische Ansicht

Sie können auch Anomalien anzeigen, indem Sie die Option Tabellenansicht in **Infrastructure Analytics**verwenden. Navigieren Sie zu **Infrastruktur > 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 IP-Adresskonflikte angezeigt wird.



- **Details** - Zeigt an, welche Anomalie festgestellt wurde
- **Erkennungsmeldung** —Zeigt die MAC-Adresse an, für die die IP-Adresse den Konflikt hat
- **Empfehlungen** —Gibt das Verfahren zur Fehlerbehebung an, um diesen IP-Adresskonflikt

Instanzverwaltung

September 2, 2024

Instanzen sind Citrix Application Delivery Controller (ADC) -Appliances, die Sie mit NetScaler Console verwalten, überwachen und Fehler beheben können. Fügen Sie Instanzen zur NetScaler Console hinzu, um sie zu überwachen. Instanzen können hinzugefügt werden, wenn Sie NetScaler Console oder später einrichten. Nachdem Sie Instanzen zur NetScaler Console hinzugefügt haben, werden diese kontinuierlich abgefragt, um Informationen zu sammeln, die später zur Problemlösung oder als Berichtsdaten verwendet werden können.

Instanzen können als statische Gruppe oder als privater IP-Block gruppiert werden. Eine statische Gruppe von Instanzen kann nützlich sein, wenn Sie bestimmte Aufgaben wie Konfigurationsaufträge und andere ausführen möchten. Ein privater IP-Block gruppiert Ihre Instanzen basierend auf ihren geografischen Standorten.

Eine Instanz hinzufügen

Sie können Instanzen entweder beim ersten Einrichten des NetScaler Console-Servers oder später hinzufügen. 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 zur NetScaler Console finden Sie unter Hinzufügen von Instanzen zur NetScaler Console.

Wenn Sie dem NetScaler Console-Server eine Instanz hinzufügen, fügt sich der Server implizit selbst als Trap-Ziel für die Instanz hinzu und erfasst ein Inventar der Instanz. Weitere Informationen finden Sie unter So erkennt NetScaler Console Instanzen .

Nachdem Sie eine Instanz hinzugefügt haben, können Sie sie löschen, indem Sie zu **Infrastruktur > Instanzen** navigieren und die Instanz-Kategorie auswählen. Wählen Sie dann die Instanz aus, die Sie löschen möchten, und klicken Sie auf **Entfernen**.

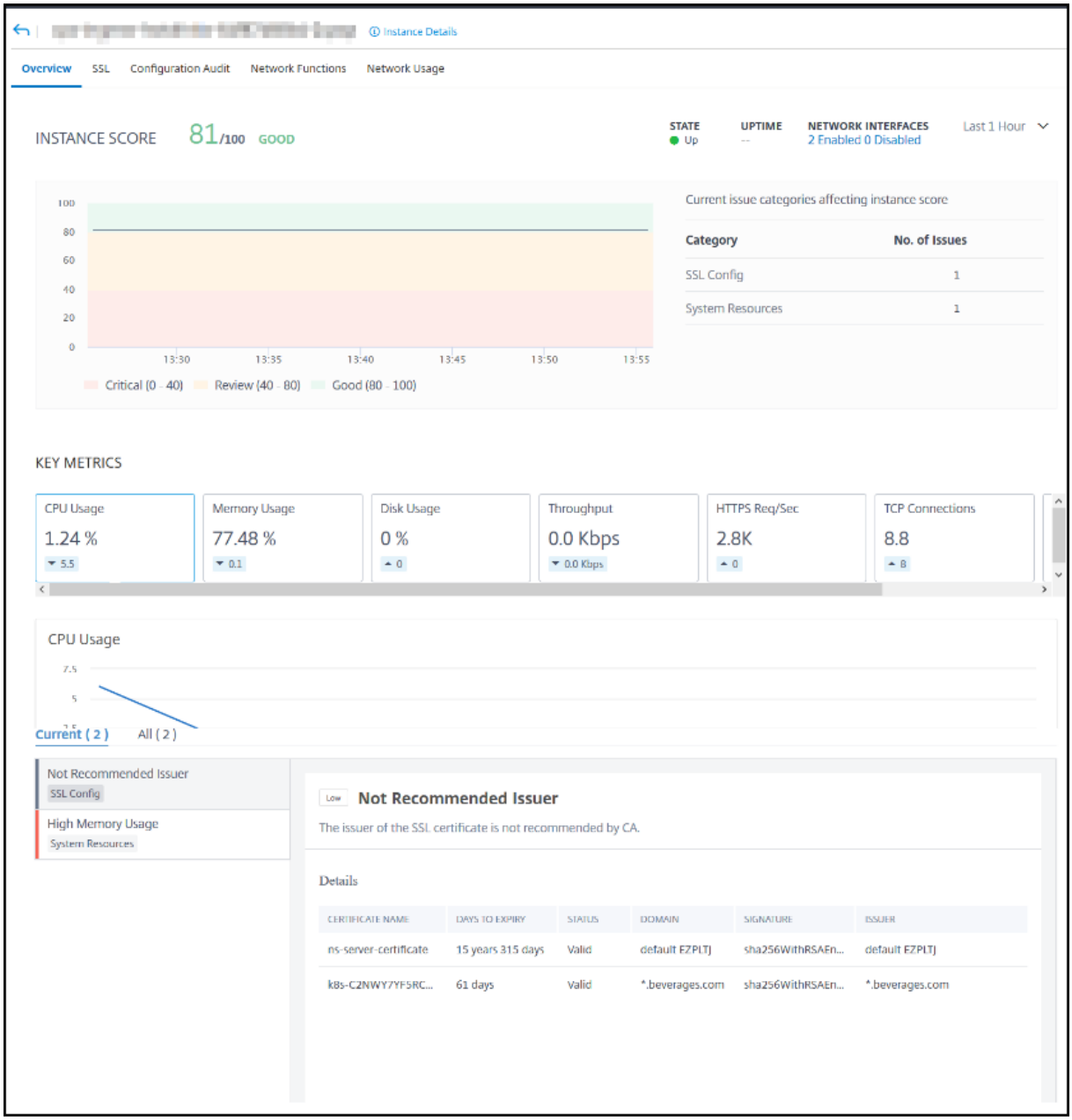
So verwenden Sie das Instanz-Dashboard

Das Dashboard pro Instanz in NetScaler Console zeigt Daten in tabellarischer und grafischer Form 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 > NetScaler**. Wählen Sie auf der Seite NetScaler 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. Hier werden auch instanzspezifische Informationen wie die IP-Adresse, ihre Hardware- und LOM-Versionen, die Profildetails, die Seriennummer, die Kontaktperson und andere angezeigt. Wenn Sie weiter nach unten scrollen, werden die lizenzierten Funktionen, die für die ausgewählte Instanz verfügbar sind, zusammen mit den darauf konfigurierten Modi. Weitere Informationen finden Sie unter Instanzdetails.
- **SSL-Dashboard**. Sie können die Registerkarte SSL im Dashboard pro Instanz verwenden, um die Details der SSL-Zertifikate, virtuellen SSL-Server und SSL-Protokolle Ihrer ausgewählten In-

stanz anzuzeigen 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 zum **gespeicherten Status** der **NetScaler**-Konfiguration und die Driftdiagramme der NetScaler-Konfiguration auf dem Dashboard zeigen allgemeine Details zu Konfigurationsänderungen zwischen gespeicherten Konfigurationen und ungespeicherten Konfigurationen an.
- **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 Pluszeichen unten rechts auf dem Bildschirm klicken, um einen weiteren Leistungsbericht hinzuzufügen.

So überwachen Sie global verteilte Websites

June 7, 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 Console 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.

In den folgenden Abschnitten wird erläutert, wie Sie Rechenzentren in NetScaler Console überwachen können.

Überwachung global verteilter Standorte in NetScaler Console

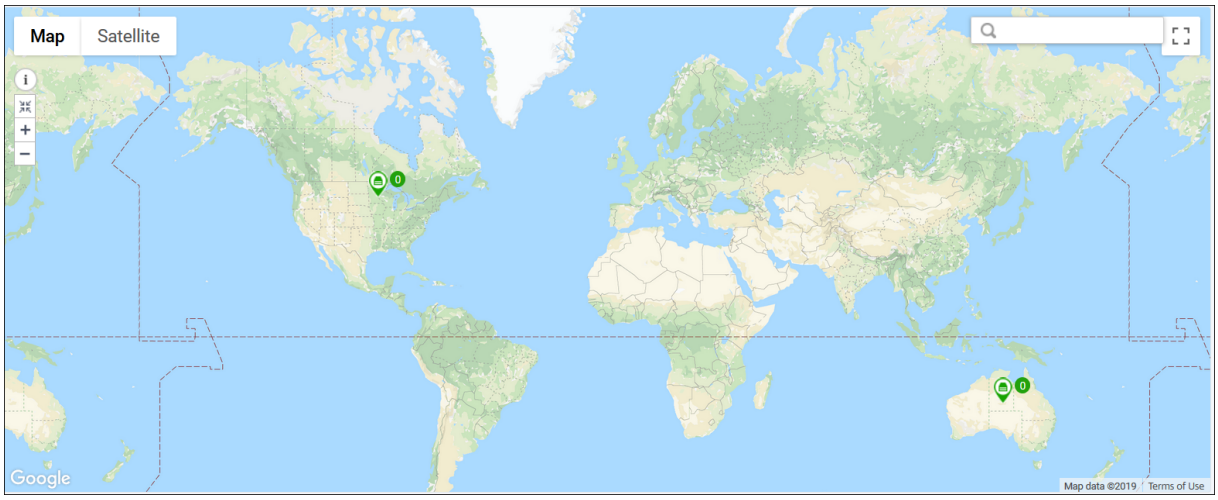
Die NetScaler Console-Site ist eine logische Gruppierung von Citrix Application Delivery Controller (NetScaler) -Instanzen an einem bestimmten geografischen Standort. Zum Beispiel, während ein Stan-

dort Amazon 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 Console verwaltet und überwacht alle NetScaler-Instanzen, die mit allen Sites verbunden sind. Sie können NetScaler Console verwenden, um Syslog-, AppFlow-, SNMP- und ähnliche Daten, die von den verwalteten Instanzen stammen, zu überwachen und zu sammeln.

Geomaps in NetScaler Console bietet 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 im Menü auf **Infrastruktur** klicken. Daraufhin wird das **Instanzen Dashboard** für eine visuelle Darstellung der auf der Weltkarte erstellten Standorte angezeigt.

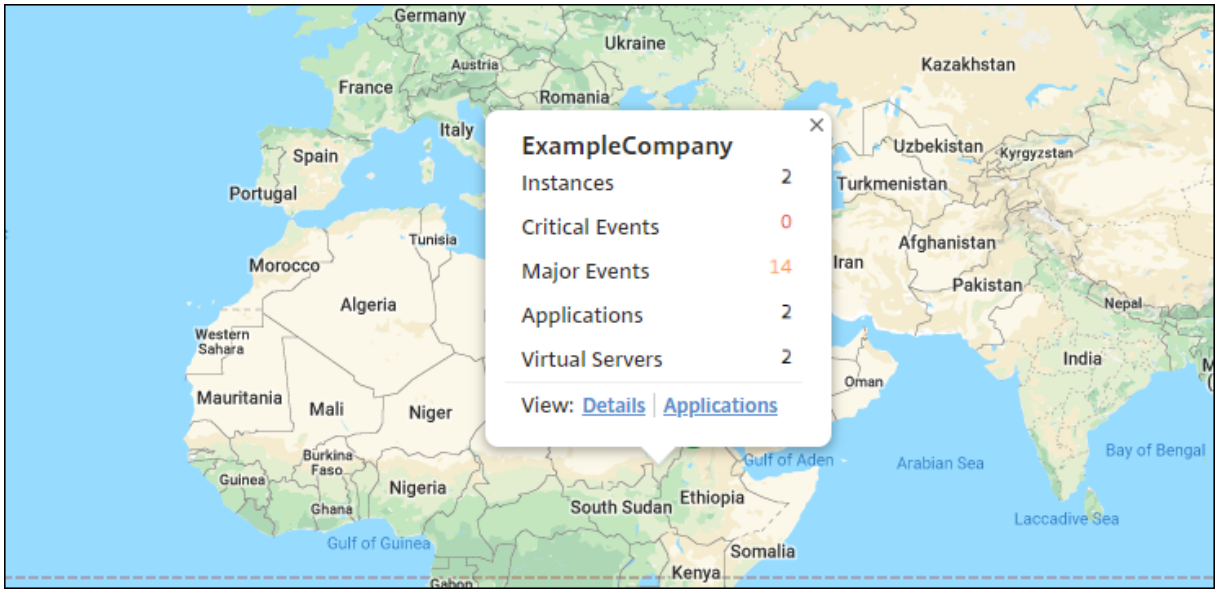
Anwendungsfall

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 die Anzahl der folgenden Komponenten auf der Website an:

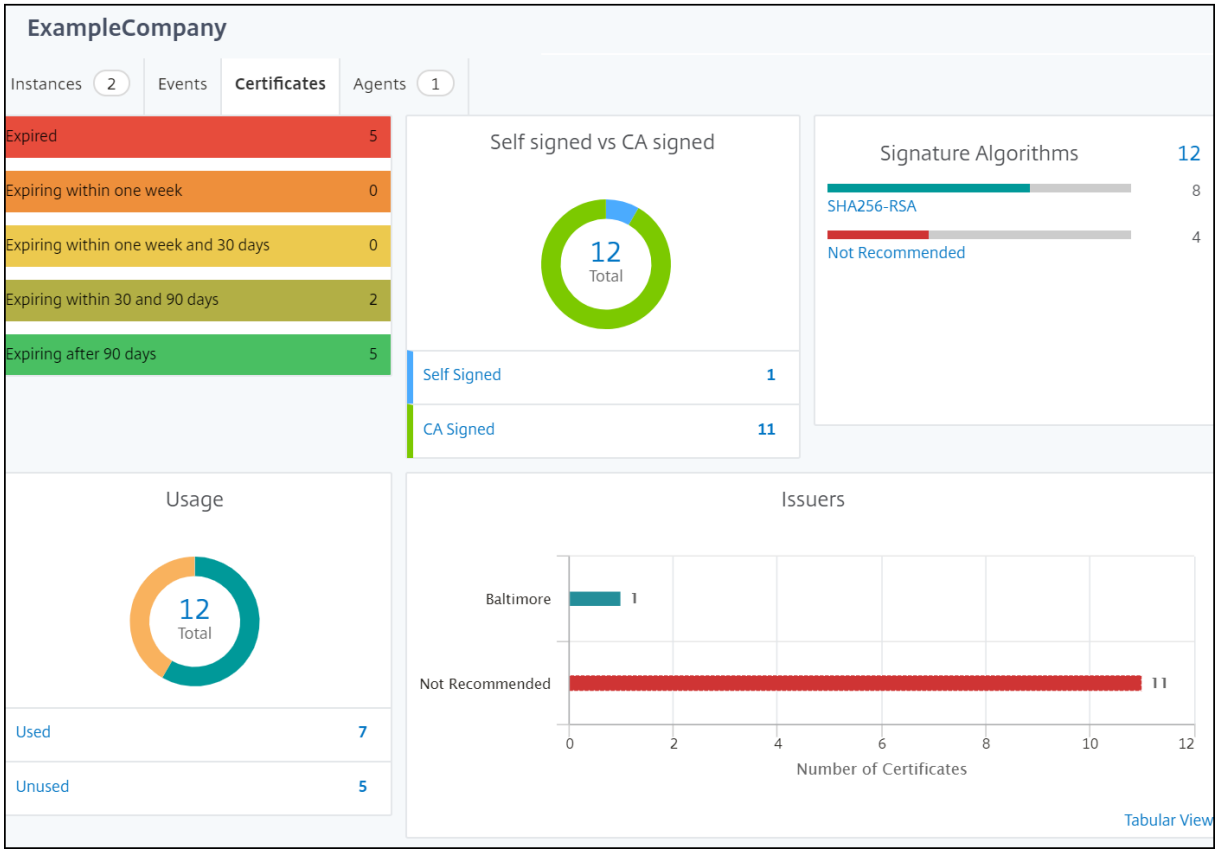
- **Instanzen**: Gibt die Anzahl der verfügbaren Instanzen an.
- **Anwendungen**: Gibt die Anzahl der gehosteten Anwendungen an.
- **Virtuelle Server**: Gibt die Anzahl der verfügbaren virtuellen Server an.
- **Kritische Ereignisse**: Gibt die Anzahl der kritischen Ereignisse an, die auf den Instanzen aufgetreten sind.
- **Hauptereignisse**: Gibt an, dass die Anzahl der Hauptereignisse auf den Instanzen aufgetreten ist.



Klicken Sie auf **Anwendungen**, um alle benutzerdefinierten Anwendungen anzuzeigen, die an den einzelnen Standorten erstellt wurden.

Klicken Sie auf **Details**, um eine Liste der NetScaler-Instanzen anzuzeigen, die an jedem Standort hinzugefügt wurden. 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 NetScaler-Instanz
  - Anzahl kritischer Ereignisse
  - 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 als Nächstes die NetScaler-Instanzen in der NetScaler Console hinzufügen. Sie müssen außerdem die Instanz zur Site hinzufügen, einen Agent hinzufügen und den Agent an die Site binden. NetScaler Console erkennt dann die Site, zu der die NetScaler-Instanz und der Agent gehören.

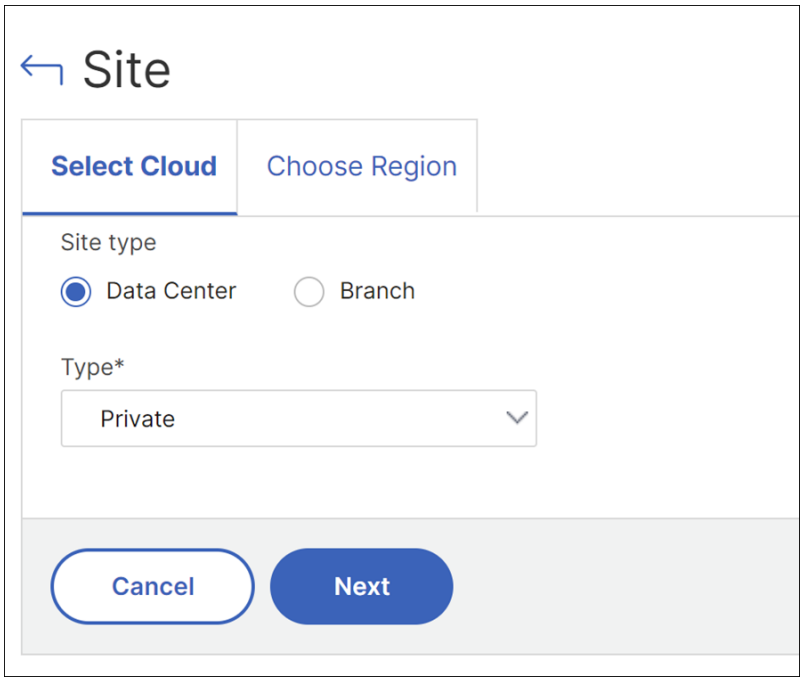
Weitere Informationen zum Hinzufügen von NetScaler-Instanzen finden Sie unter Hinzufügen von Instanzen.

Erstellen einer Site

Erstellen Sie Sites, bevor Sie Instanzen in NetScaler Console hinzufügen. Durch die Angabe von Standortinformationen können Sie die Site genau lokalisieren.

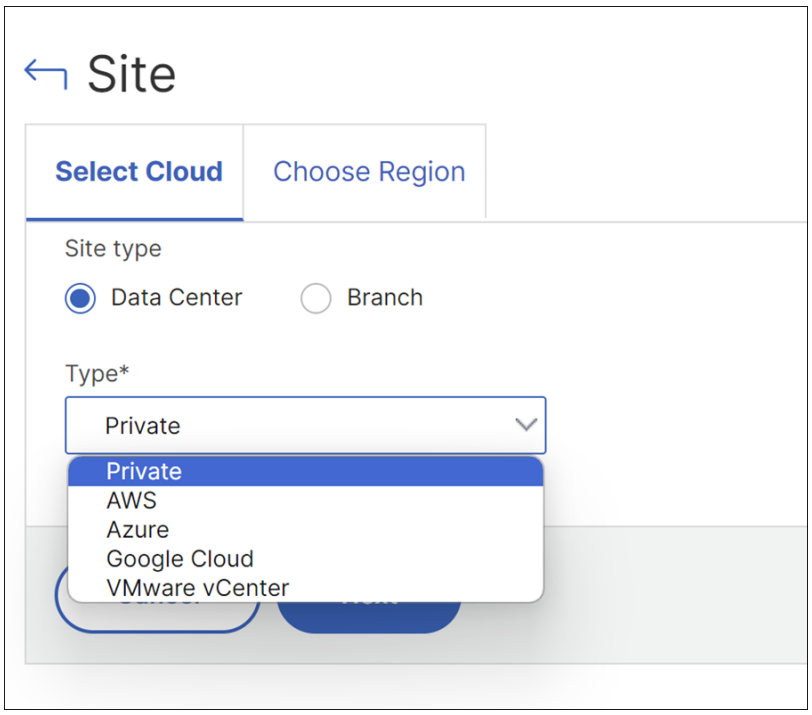
Erstellen einer Site:

1. Navigieren Sie zu **Infrastruktur > Instanzen > Site** . Klicken Sie auf **Hinzufügen**.
2. Wählen Sie auf der Registerkarte **Select Cloud** den **Sitetyp** aus. Sie können eine Site vom Typ **Datencenter** oder **Zweigstelle** erstellen.



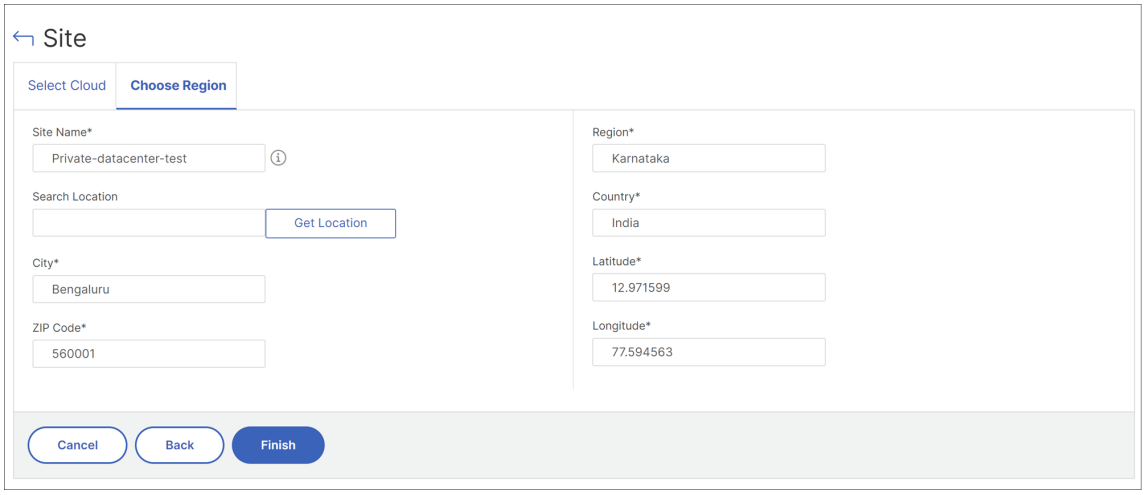
Wählen Sie für den Standorttyp Datencenter den **Typ** aus der Liste aus:

- Privat
- AWS
- Azure
- Google Cloud
- VMware vCenter



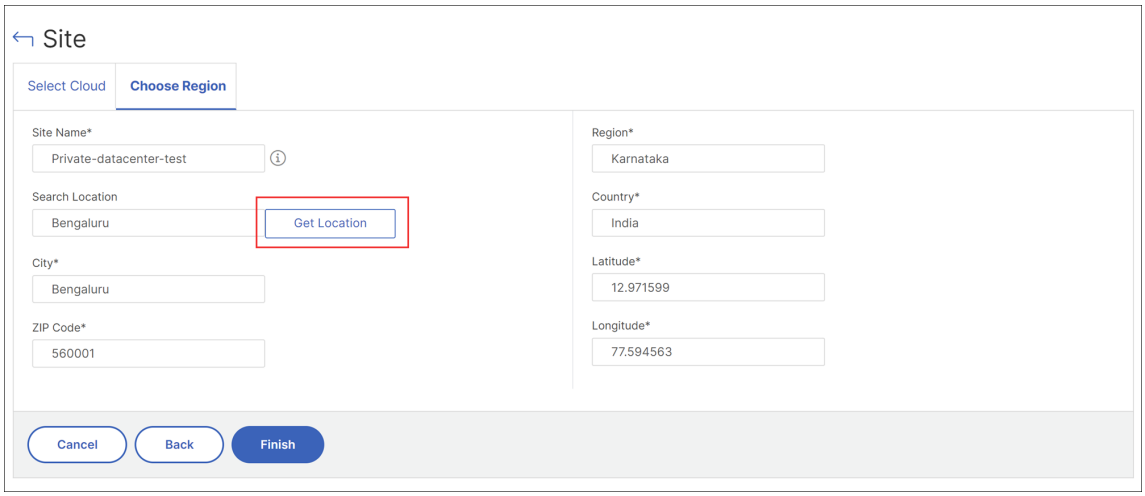
3. Klicken Sie auf **Weiter**.
4. Geben Sie auf der Registerkarte **Region auswählen** die folgenden Details ein:

    - Sitename
    - Ort
    - PLZ
    - Region
    - Land
    - Breitengrad
    - Längengrad



Alternativ können Sie den Standort unter **Standort suchen** eingeben und auf **Standort abrufen**

klicken, um den Standort genau zu lokalisieren. Die Felder Stadt, PLZ, Region, Land, Breitengrad und Längengrad werden automatisch ausgefüllt.



5. Klicken Sie auf **Fertigstellen**.

> **Hinweise:**
>
> Die beschriebenen Schritte gelten für:
>
> - Art des Zweigstellenstandorts.
> - Standorttyp Datencenter mit dem Typ Privat.
> - Wenn die Abruf-Option für die Cloud-Anbietertypen nicht ausgewählt ist.

Erstellen Sie eine Site für Cloud-Anbietertypen

Sie können eine Site mit einem Cloud-Anbietertyp erstellen und wählen, ob Sie die **Fetch**-Option aktivieren oder deaktivieren möchten. Standardmäßig ist die Option **Abrufen** nicht ausgewählt.

Die **Fetch**-Option ist nur für AWS-, Azure- und Google Cloud-Plattformen verfügbar.

Eine detaillierte Anleitung zum Erstellen einer Site für bestimmte Cloud-Anbieter finden Sie in den folgenden Abschnitten:

1. Erstellen Sie eine Site in AWS
2. Erstellen Sie eine Site in Azure
3. Erstellen Sie eine Website in Google Cloud
4. Erstellen Sie eine Site in VMware vCenter

Site bearbeiten

Um eine bestehende Site zu ändern:

1. Wählen Sie die Site aus und klicken Sie auf **Bearbeiten** .
2. Auf der Seite **Site konfigurieren** können Sie den **Site-Typ** aktualisieren. Wenn Sie beispielsweise zuvor **Branch** ausgewählt haben, können Sie auf **Data Center** aktualisieren.
3. Je nach Site-Typ können Sie den **Typ** ändern. Beispielsweise können Sie den Typ von einem privaten Rechenzentrum in eine öffentliche Cloud aus der Liste ändern.

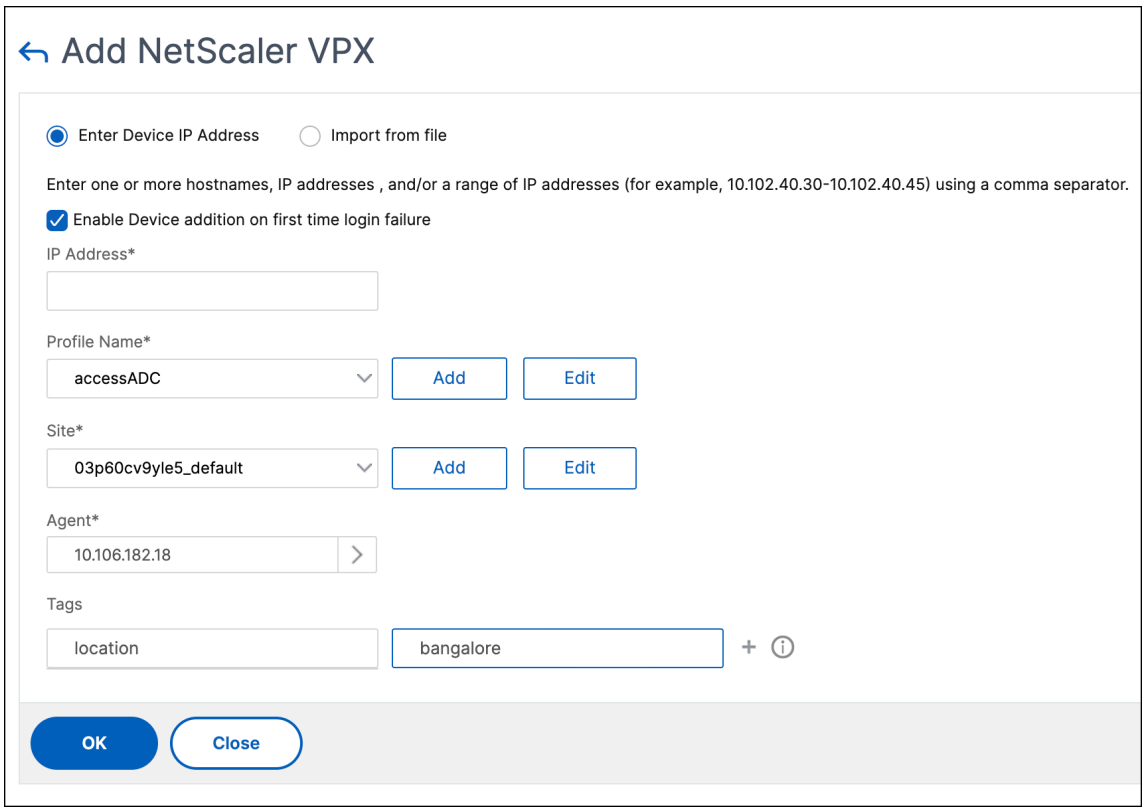
Site löschen

1. Um eine Site zu löschen, wählen Sie die Site aus und klicken Sie auf **Löschen**.
2. Klicken Sie auf der Seite "Bestätigen"auf **Ja**.

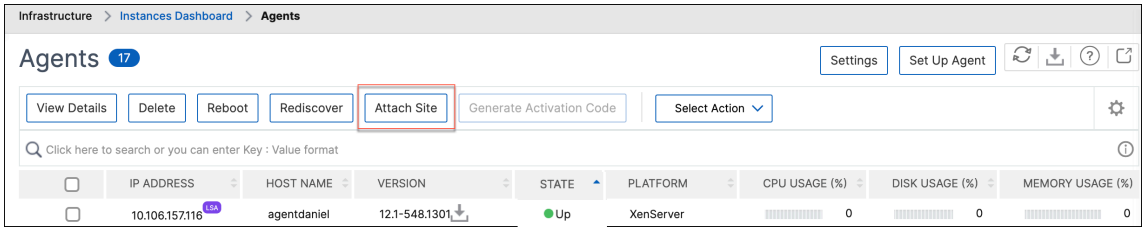
So fügen Sie Instanzen hinzu und wählen Sie Sites aus:

Nach dem Erstellen von Sites müssen Sie Instanzen in NetScaler Console hinzufügen. Sie können die zuvor erstellte Site auswählen, oder Sie können auch eine Site erstellen und die Instanz zuordnen.

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Instanzen NetScaler**.
2. Wählen Sie das **VPX**aus 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 die Schaltfläche **Hinzufügen** neben dem Feld **Site** klicken, um eine Site zu erstellen, oder auf die Schaltfläche **Bearbeiten** klicken, um die Details der Standardsite 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 Agent aus und klicken Sie auf **Site anhängen**.



   a) Wählen Sie die Website aus der Liste aus, und klicken Sie auf **Speichern**.

7. Optional können Sie Schlüssel- und Wertfelder für **Tags**eingeben.
8. Klicken Sie auf **OK**.

Sie können auch einen Agent an eine Site anhängen, indem Sie zu **Infrastruktur > Instanzen > Agents** navigieren.

Um einen Agenten mit der Site zu verknüpfen:

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Instanzen > Agents** .
2. Wählen Sie den Agent aus, und klicken Sie auf **Site anhängen**.

3. Sie können die Website zuordnen und auf **Speichern**klicken.

NetScaler Console beginnt mit der Überwachung der NetScaler-Instanzen, die am Standort Bangalore hinzugefügt wurden, zusammen mit den Instanzen an den beiden anderen Standorten.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** . Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis:**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Tags erstellen und Instanzen zuweisen

January 26, 2024

NetScaler Console ermöglicht es Ihnen jetzt, Ihre NetScaler-Instanzen mit Tags zu verknüpfen. Ein Tag ist ein Schlüsselwort oder ein Begriff mit einem Wort, den 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 Markieren von Instanzen Ihnen hilft, diese besser zu überwachen.

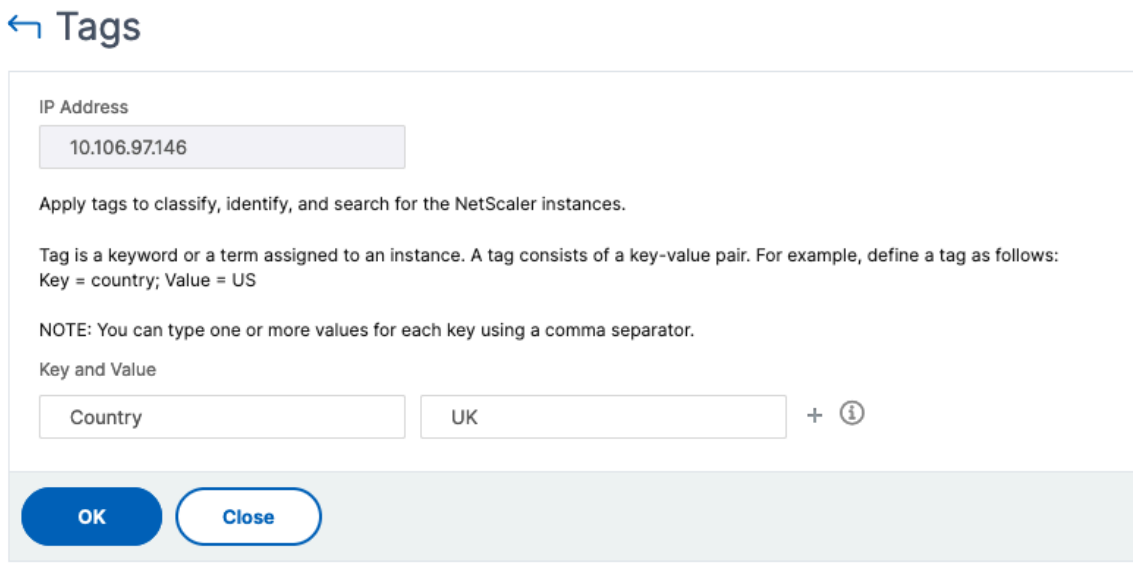
- **Anwendungsfall 1**: Sie können ein Tag erstellen, um alle Instanzen zu identifizieren, die sich im Vereinigten Königreich befinden. Hier können Sie ein Tag mit dem Schlüssel "Country"und dem Wert als "UK"erstellen. Mit diesem Tag können Sie alle Instanzen durchsuchen und überwachen, die sich in Großbritannien befinden.

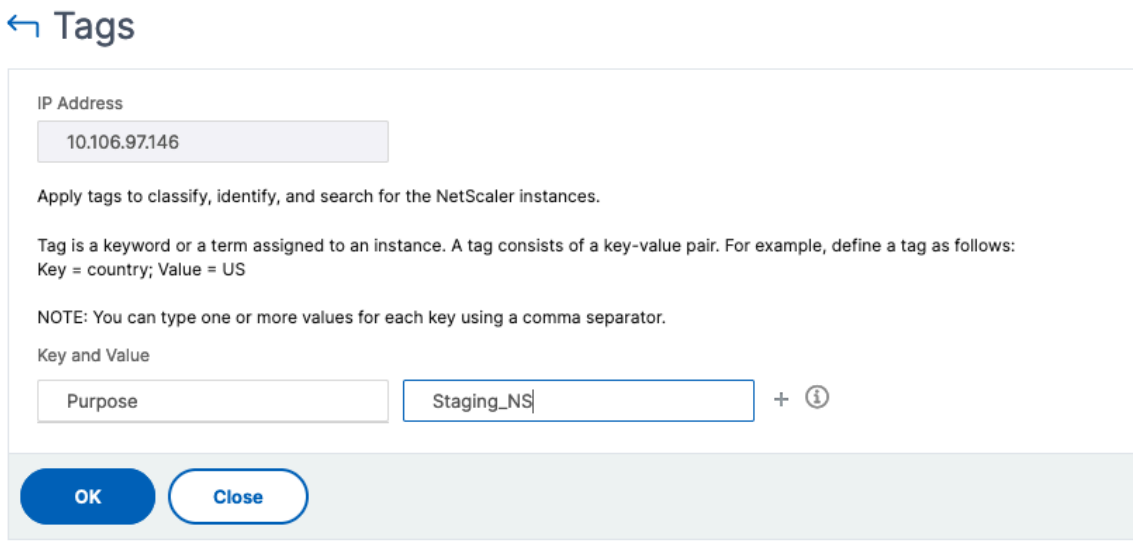
- **Anwendungsfall 2**: Sie möchten nach Instanzen suchen, die sich in der Stagingumgebung befinden. Hier können Sie ein Tag mit dem Schlüssel "Purpose"und einem Wert als "Staging_NS"erstellen. Mit diesem Tag können Sie alle Instanzen, die in der Stagingumgebung verwendet werden, von den Instanzen trennen, die Clientanforderungen durchlaufen.
- **Anwendungsfall 3**: Betrachten Sie eine Situation, in der Sie die Liste der 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:

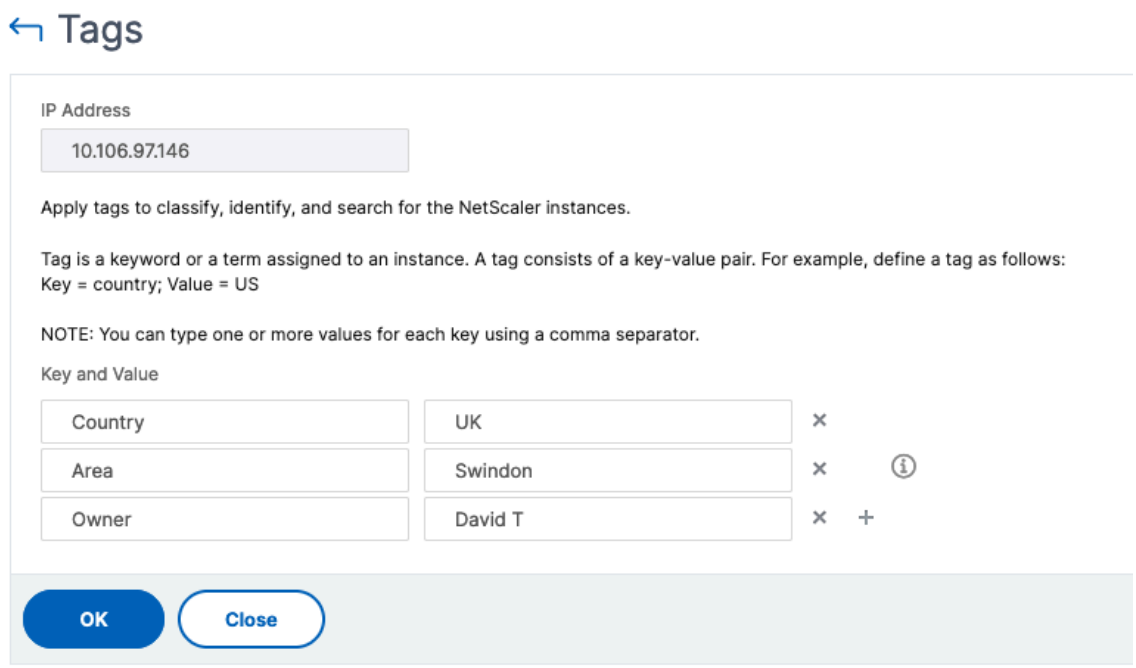
1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Instanzen NetScaler**.
2. Wählen Sie die Registerkarte **VPX** .
3. Wählen Sie die erforderliche VPX-Instanz aus.
4. Klicken Sie **auf Tags**. Im angezeigten **Tags-Fenster** können Sie Ihre eigenen "Schlüssel-Wert" -Paare erstellen, indem 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.





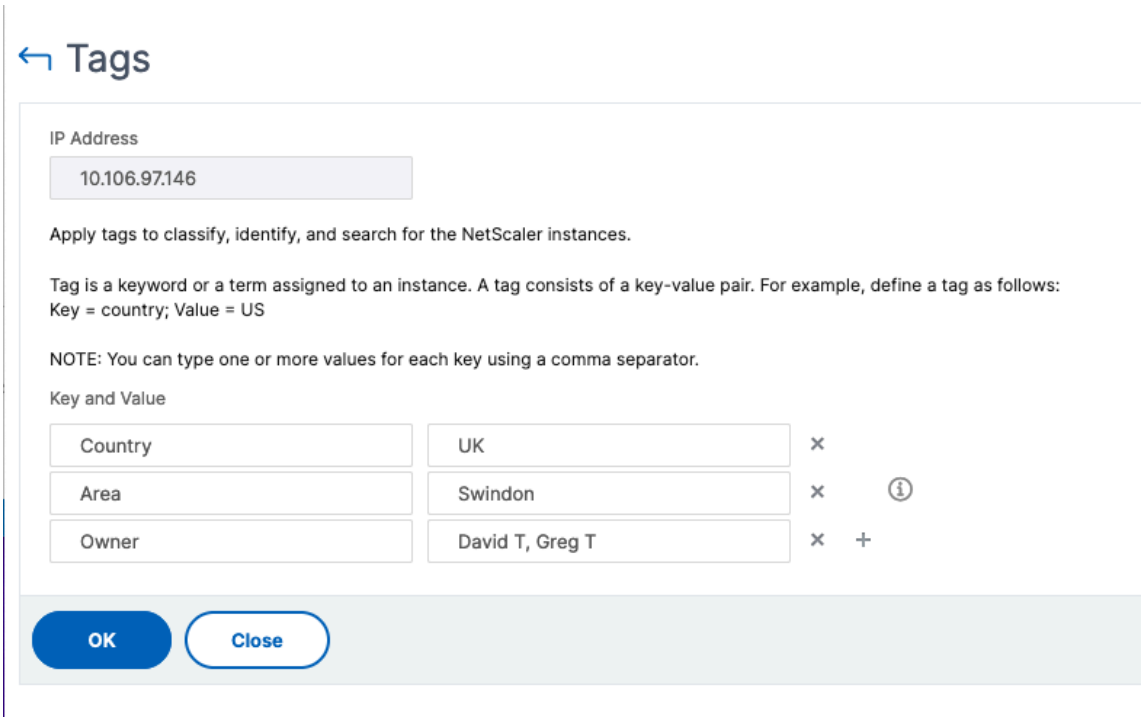
Sie können auch mehrere Tags hinzufügen, indem Sie auf + klicken. Durch das Hinzufügen mehrerer und aussagekräftiger Tags können Sie effizient nach den Instanzen suchen.



Sie können einem Schlüsselwort mehrere Werte hinzufügen, indem Sie sie durch Kommas trennen.

Zum Beispiel weisen Sie die Admin-Rolle einem anderen Mitarbeiter zu, Greg T. Sie können seinen Namen durch ein Komma getrennt hinzufügen. Durch das Hinzufügen mehrerer Namen können Sie entweder nach den Namen oder nach beiden Namen suchen. NetScaler Console

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.

5. Klicken Sie auf **OK**.

> **Hinweis**
>
> Sie können später neue Tags hinzufügen oder vorhandene Tags löschen. Es gibt keine Einschränkung für die Anzahl der Tags, die Sie erstellen.

Instanzen über Werte von Tags und Eigenschaften suchen

January 26, 2024

Es kann vorkommen, dass NetScaler Console viele NetScaler-Instanzen verwaltet. Als Administrator möchten Sie möglicherweise die Flexibilität, die Instanzinventar anhand bestimmter Parameter zu durchsuchen. NetScaler Console bietet jetzt verbesserte Suchfunktionen zum Durchsuchen einer Teilmenge von NetScaler-Instanzen auf der Grundlage der Parameter, 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 von Ihnen einer NetScaler-Instanz zugewiesen werden können, um zusätzliche Beschreibung zur 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 in der NetScaler Console hinzugefügte NetScaler-Instanz hat 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.

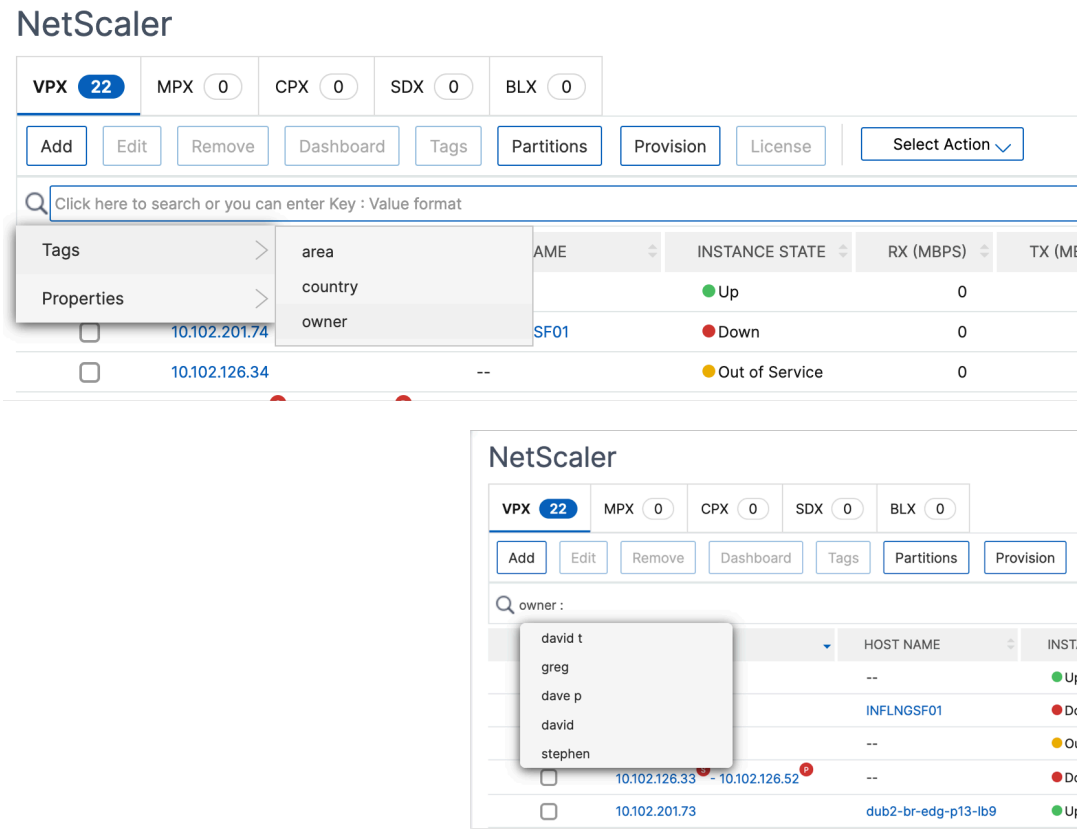
Sie können eine Kombination aus Tags und Eigenschaften verwenden, um eigene Suchkriterien zu erstellen.

So suchen Sie nach NetScaler VPX Instanzen

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Instanzen NetScaler**.
2. Wählen Sie die Registerkarte **VPX** .
3. Klicken Sie auf das Suchfeld. Sie können einen Suchausdruck erstellen, indem Sie Tags oder Eigenschaften verwenden oder beide kombinieren.

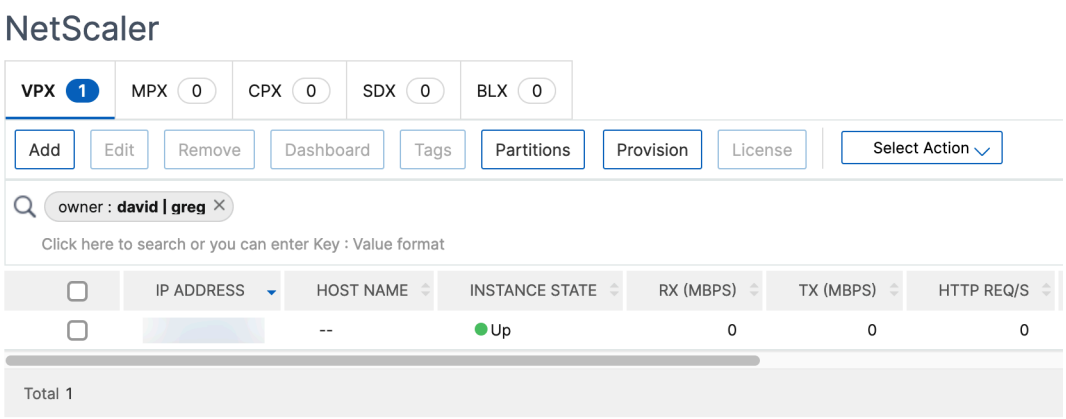
   Die folgenden Beispiele zeigen, wie Sie den Suchausdruck effizient verwenden können, um nach der Instanz zu suchen.

   a) Wählen Sie die Option **Tags** und dann **Besitzer**aus. Wählen Sie David T.

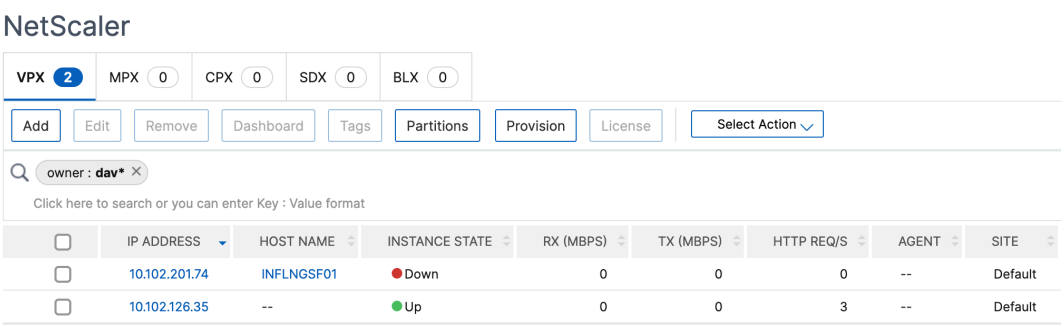


NetScaler Console unterstützt reguläre Ausdrücke und Platzhalterzeichen in den Suchausdrücken.

a) 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.



b) Sie können auch Platzhalterzeichen verwenden, um ein oder mehrere Zeichen zu ersetzen oder darzustellen. Sie können beispielsweise mit Dav* nach allen Instanzen suchen, die sich im Besitz von “David”und “Dave P”befinden.



> **Hinweis:**
>
> Weitere Informationen zu regulären Ausdrücken und Platzhalterzeichen und deren Verwendung finden Sie, wenn Sie in der Suchleiste auf das Symbol „Informationen “klicken.

Adminpartitionen von NetScaler-Instanzen verwalten

January 26, 2024

Sie können Adminpartitionen auf Ihren Citrix Application Delivery Controller (NetScaler) -Instanzen so konfigurieren, dass verschiedenen Gruppen in Ihrer Organisation unterschiedliche Partitionen auf derselben NetScaler-Instanz zugewiesen werden. Sie können einen Netzwerkadministrator zuweisen, um mehrere Partitionen auf mehreren NetScaler-Instanzen zu verwalten.

NetScaler Console 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. Weitere Informationen zum Erstellen einer Gruppe oder eines Benutzers finden Sie unter Benutzer erstellen und Gruppe erstellen.

Ein Benutzer kann nur die Partitionen in der Gruppe anzeigen und verwalten, zu der der Benutzer gehört. Wenn Sie eine NetScaler-Instanz entdecken, werden die für diese NetScaler-Instanz konfigurierten Adminpartitionen automatisch dem System hinzugefügt. Jede Admin-Partition wird in NetScaler Console als Instanz betrachtet.

Administrator-Partitionen anzeigen

Bedenken Sie, dass Sie zwei NetScaler VPX-Instanzen haben und zwei Admin-Partitionen für jede Instanz konfiguriert sind. Beispielsweise hat die NetScaler-Instanz 10.xx.xx.100 Partition-1 und Partition-2 und die 10.xx.xx.101-Instanz hat die erste Partition und die zweite Partition.

Führen Sie die folgenden Schritte aus, um Administratorpartitionen anzuzeigen:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**.
2. Klicken Sie auf der Registerkarte **VPX** auf **Partitionen**.

Wenn Sie beispielsweise eine Gruppe mit den folgenden Bedingungen erstellen:

- In **Settings > Users & Roles > Create Group > Authorization Settings > Select Instances**, you select “10.xx.xx.100-partition-1”and “10.xx.xx.101-first-partition”instances.
- Sie weisen der Gruppe „Benutzer1”zu.

Benutzer1 kann nur die Partitionen anzeigen und verwalten, die der Gruppe hinzugefügt wurden. Die Partitionen, die der Gruppe nicht hinzugefügt werden, sind jedoch auf den Benutzer beschränkt, obwohl sie zu denselben Instanzen gehören.

In diesem Beispiel sind 10.xx.xx.100-partition-2 und 10.xx.xx.101-second-partition eingeschränkt, da die Instanzen nicht zu der Gruppe hinzugefügt werden, der der Benutzer zugewiesen ist.

Wenn Sie möchten, dass ein anderer Benutzer die Admin-Partitionen 10.xx.xx.100-partition-2 und 10.xx.xx.101-second-partition verwaltet, erstellen Sie eine Gruppe mit den folgenden Bedingungen:

- Wählen Sie auf der Registerkarte Autorisierungseinstellungen die Instanzen 10.xx.xx.100-partition-2 und 10.xx.xx.101-Second-Partition aus.**
- Weisen Sie der Gruppe den gewünschten Benutzer zu.

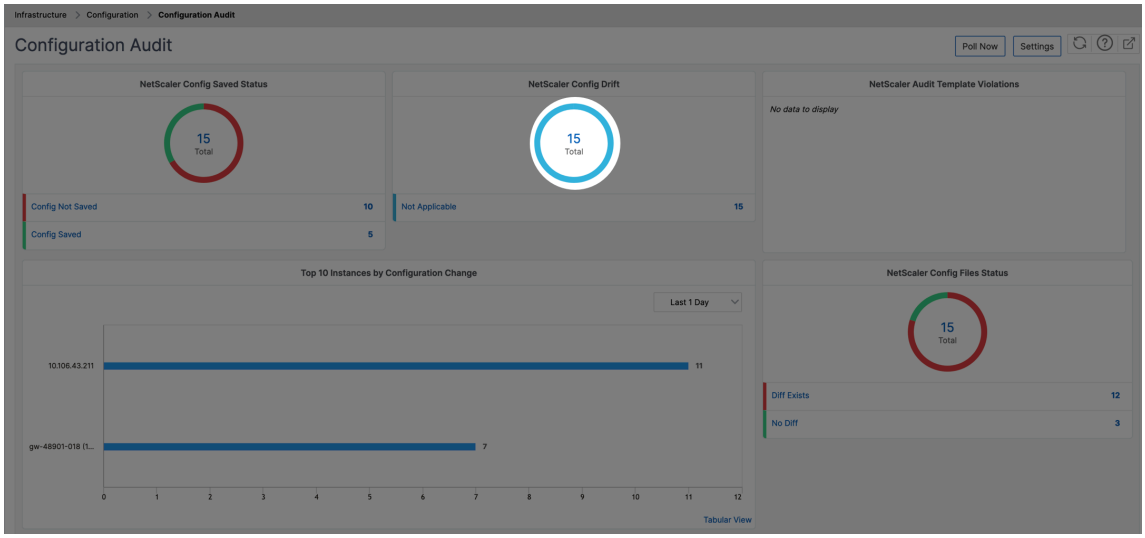
Diese Gruppe ermöglicht es dem zugewiesenen Benutzer, die ausgewählten Admin-Partitionen anzuzeigen und zu verwalten.

Versionsverlaufsunterschied anzeigen

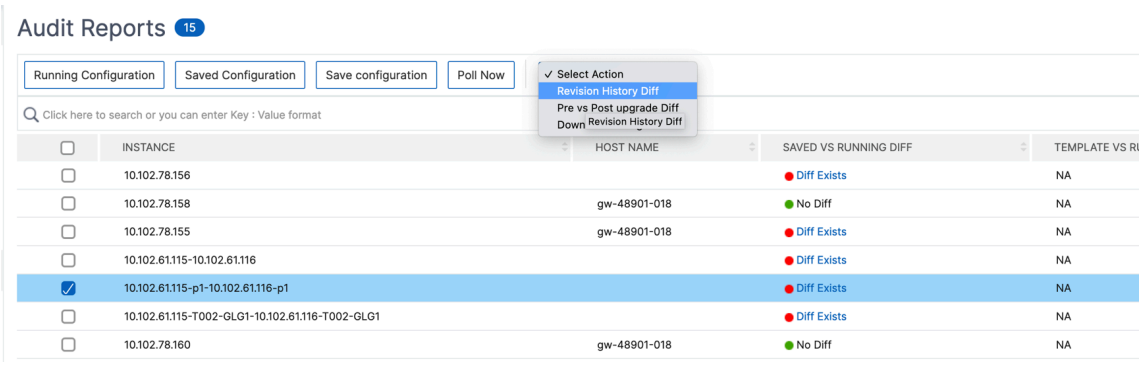
Der Unterschied zum Revisionsverlauf für eine Admin-Partition ermöglicht es Ihnen, den Unterschied zwischen den fünf neuesten Konfigurationsdateien für eine partitionierte NetScaler-Instanz zu sehen. Sie können die Konfigurationsdateien miteinander vergleichen (Beispiel: Konfigurationsversion - 1 mit Konfigurationsversion -2) oder mit der aktuellen laufen/gespeicherten Konfiguration mit Konfigurationsversion. Neben den Unterschieden in der Konfiguration werden auch die Korrekturkonfigurationen angezeigt. Sie können alle Korrekturbefehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.

So zeigen Sie die Differenz der Versionshistorie an:

1. Navigieren Sie zu **Infrastruktur > Konfigurationsprüfung**. Das Konfigurationsüberprüfungs-Dashboard zeigt verschiedene Berichte an. Klicken Sie auf die Zahl, die in der Mitte des Donutdiagramms angezeigt wird.

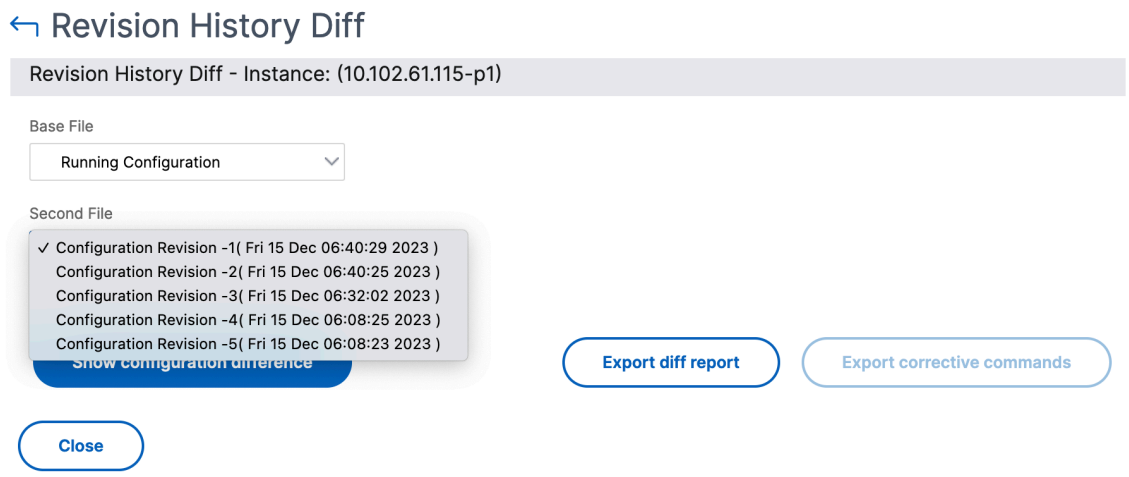


2. Wählen Sie die partitionierte NetScaler-Instanz aus.
3. Klicken Sie im Feld "Aktion"auf **Versionsverlauf Diff**.

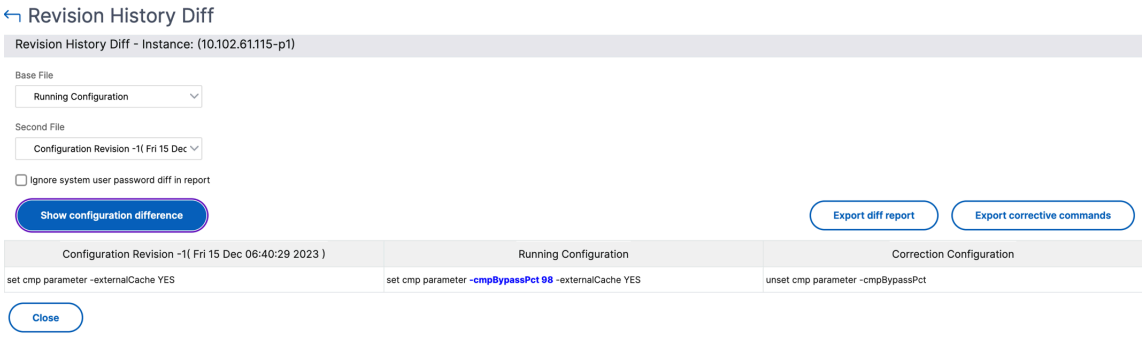


4. Wählen Sie auf der Seite **Versionsverlauf-Diff** die Dateien aus, die Sie vergleichen möchten. Vergleichen Sie beispielsweise die gespeicherte Konfiguration mit Configuration Revision-2, und klicken Sie dann auf **Konfigurationsunterschied anzeigen**.

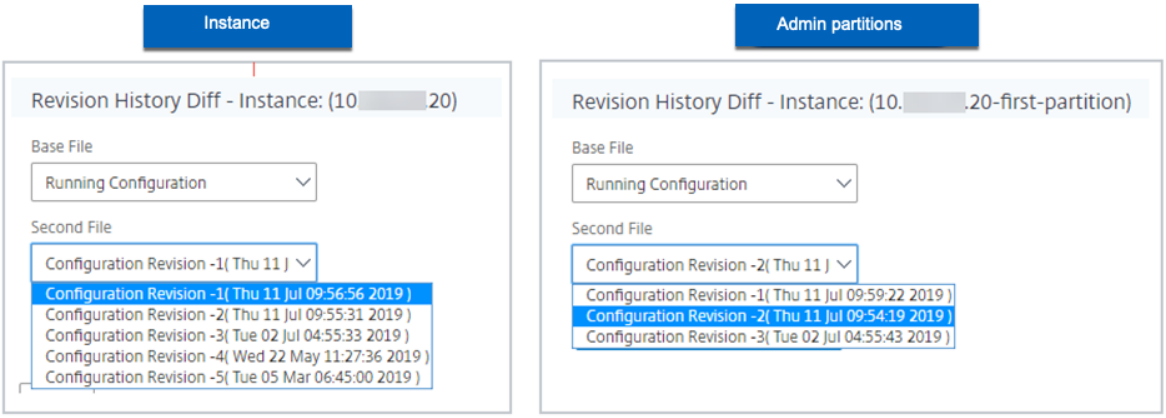
   Anschließend können Sie die Unterschiede zwischen den fünf neuesten Konfigurationsdateien für die ausgewählte partitionierte NetScaler-Instanz anzeigen. Das Folgende ist ein Beispiel für eine Admin-Partition mit fünf gespeicherten Konfigurationen:



Sie können auch die Korrekturkonfigurationsbefehle anzeigen und diese Korrekturbefehle in Ihren lokalen Ordner exportieren. Diese korrigierenden Befehle sind die Befehle, die für die Basisdatei ausgeführt werden müssen, um die Konfiguration in den gewünschten Zustand zu bringen (Konfigurationsdatei, die zum Vergleich verwendet wird).



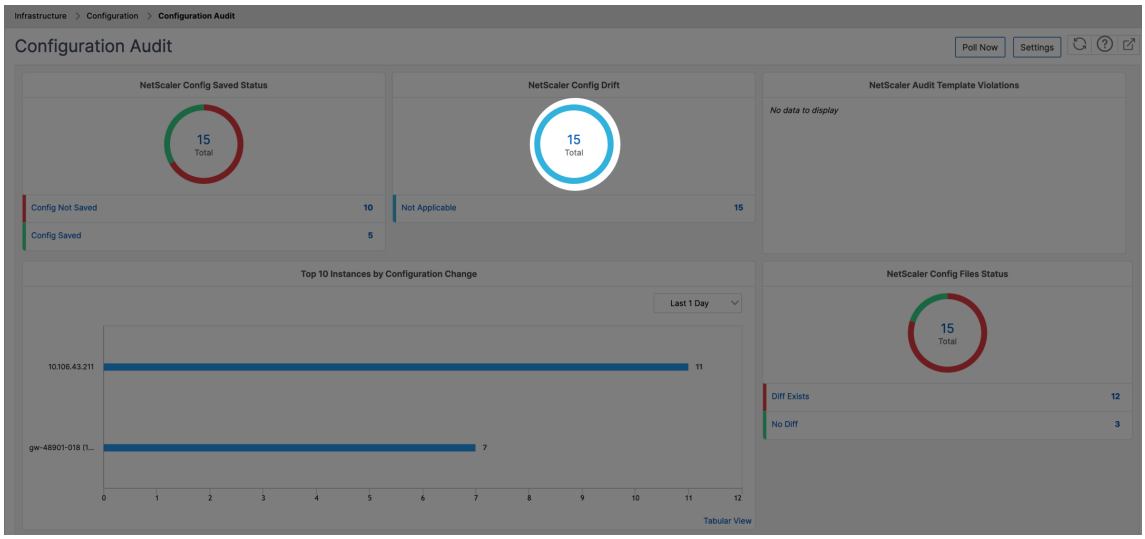
Die gespeicherten Konfigurationen auf einer Admin-Partition und der Instanz sind unterschiedlich. Im folgenden Beispiel verfügt die 10.xx.xx.20-Instanz über fünf gespeicherte Konfigurationen, bei denen die Admin-Partition dieser Instanz drei verschiedene gespeicherte Konfigurationen aufweist:



Anzeigen der Vorlage im Vergleich zu laufenden Differenzen

Überwachungsvorlagen für die Partition ermöglichen es Ihnen, eine benutzerdefinierte Konfigurationsvorlage zu erstellen und sie einer Partitionsinstanz zuzuordnen. Jede Variation in der laufenden Konfiguration der Instanz mit der Audit-Vorlage wird in der Spalte "**Vorlage vs 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.

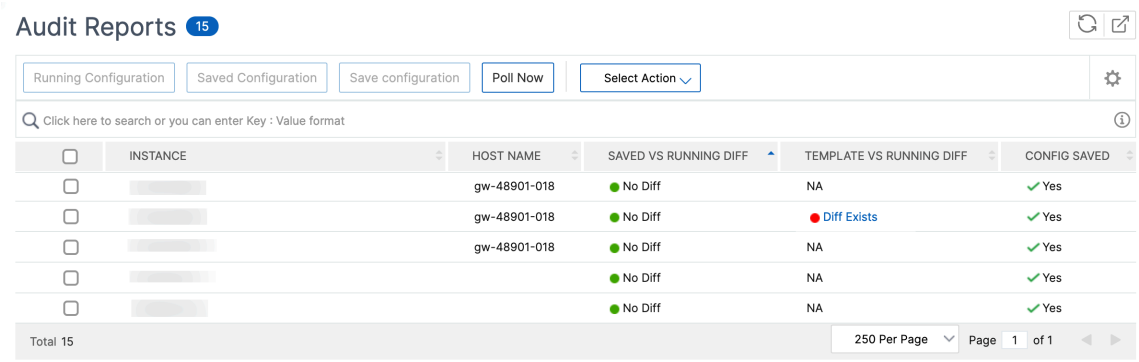
1. Navigieren Sie zu **Infrastruktur > Konfigurationsprüfung**. Das Konfigurationsüberprüfungs-Dashboard zeigt verschiedene Berichte an. Klicken Sie auf die Zahl, die in der Mitte des Donutdiagramms angezeigt wird.



2. Klicken Sie auf der Seite **Überwachungsberichte** auf den Hyperlink **Diff Existiert** in der Spalte Vorlage vs Laufendes Diff.

   Wenn zwischen der Überwachungsvorlage und der laufenden Konfiguration ein Unterschied

besteht, wird der Unterschied als Hyperlink angezeigt. Klicken Sie auf den Hyperlink, um die Unterschiede anzuzeigen, falls vorhanden. Neben den Unterschieden in der Konfiguration werden auch die Korrekturkonfigurationen angezeigt. Sie können auch alle Korrekturbefehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.



So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** . Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis:**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Backup und Wiederherstellen von NetScaler-Instanzen

January 26, 2024

Sie können den aktuellen Status einer Citrix Application Delivery Controller Instanz (NetScaler) sichern und später die gesicherten Dateien verwenden, um die NetScaler-Instanz in demselben Zustand wiederherzustellen. Sie müssen eine Instanz immer sichern, bevor Sie sie aktualisieren oder aus vorsorglichen Gründen. 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 NetScaler-Konfigurationen manuell über die GUI oder CLI Backup und wiederherstellen, oder Sie können NetScaler Console verwenden, um automatische Backups und manuelle Wiederherstellungen durchzuführen. NetScaler Console sichert den aktuellen Status Ihrer verwalteten NetScaler-Instanzen mithilfe von NITRO-Aufrufen und den Protokollen Secure Shell (SSH) und Secure Copy (SCP).

NetScaler Console erstellt ein vollständiges Backup und stellt die folgenden NetScaler-Instanztypen wieder her:

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

Weitere Informationen finden Sie unter Sichern und Wiederherstellen einer NetScaler-Instanz .

> **Hinweis:**
>
> - Von der NetScaler Console 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/tenants/<specify-the-tenant-name>/device_backup/
```

Um Probleme aufgrund der Nichtverfügbarkeit von Speicherplatz zu vermeiden, können Sie maximal drei Backupdateien in diesem Verzeichnis speichern.

Um NetScaler-Instanzen zu sichern und wiederherzustellen, müssen Sie zuerst die Backup-Einstellungen in der NetScaler Console 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.

Erstellen Sie mithilfe der NetScaler Console ein Backup für eine ausgewählte NetScaler-Instanz

Führen Sie diese Aufgabe aus, wenn Sie eine ausgewählte NetScaler-Instanz oder mehrere Instanzen sichern möchten:

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Instanzen** . Wählen Sie unter **Instanzen**den Typ der Instanzen (z. B. VPX) aus, die auf dem Bildschirm angezeigt werden sollen.
2. Wählen Sie die Instanz aus, die Sie sichern möchten.
   - Wählen Sie für MPX-, VPX- und BLX-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 **Sichern**.
4. Geben Sie an, ob Sie Ihre Backup-Datei für mehr Sicherheit verschlüsseln möchten. Sie können entweder Ihr Kennwort eingeben oder das globale Kennwort verwenden, das Sie zuvor auf der Seite Instanzbackupeinstellungen angegeben haben.
5. Klicken Sie auf **Weiter**.

Übertragen einer Backupdatei auf ein externes System

Sie können vorsorglich eine Kopie Ihrer Backupdatei auf ein anderes System übertragen. Wenn Sie die Konfiguration wiederherstellen möchten, müssen Sie zuerst die Sicherungsdatei auf den NetScaler Console-Server hochladen und dann den Wiederherstellungsvorgang ausführen.

So übertragen Sie eine NetScaler Console-Backup-Datei:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**, und wählen Sie dann den Instanztyp aus. Zum Beispiel VPX.
2. Wählen Sie die Instanz aus und wählen Sie in der Liste **Aktion auswählen** die Option **Backup/Wiederherstellen**aus.
3. Wählen Sie die Backupdatei aus, und klicken Sie dann auf **Übertragen**.

   Die Seite **Backupdatei übertragen** wird angezeigt. Geben Sie die folgenden Parameter an:

   a) **Server** —IP-Adresse des Systems, in das Sie die Backupdatei übertragen möchten.

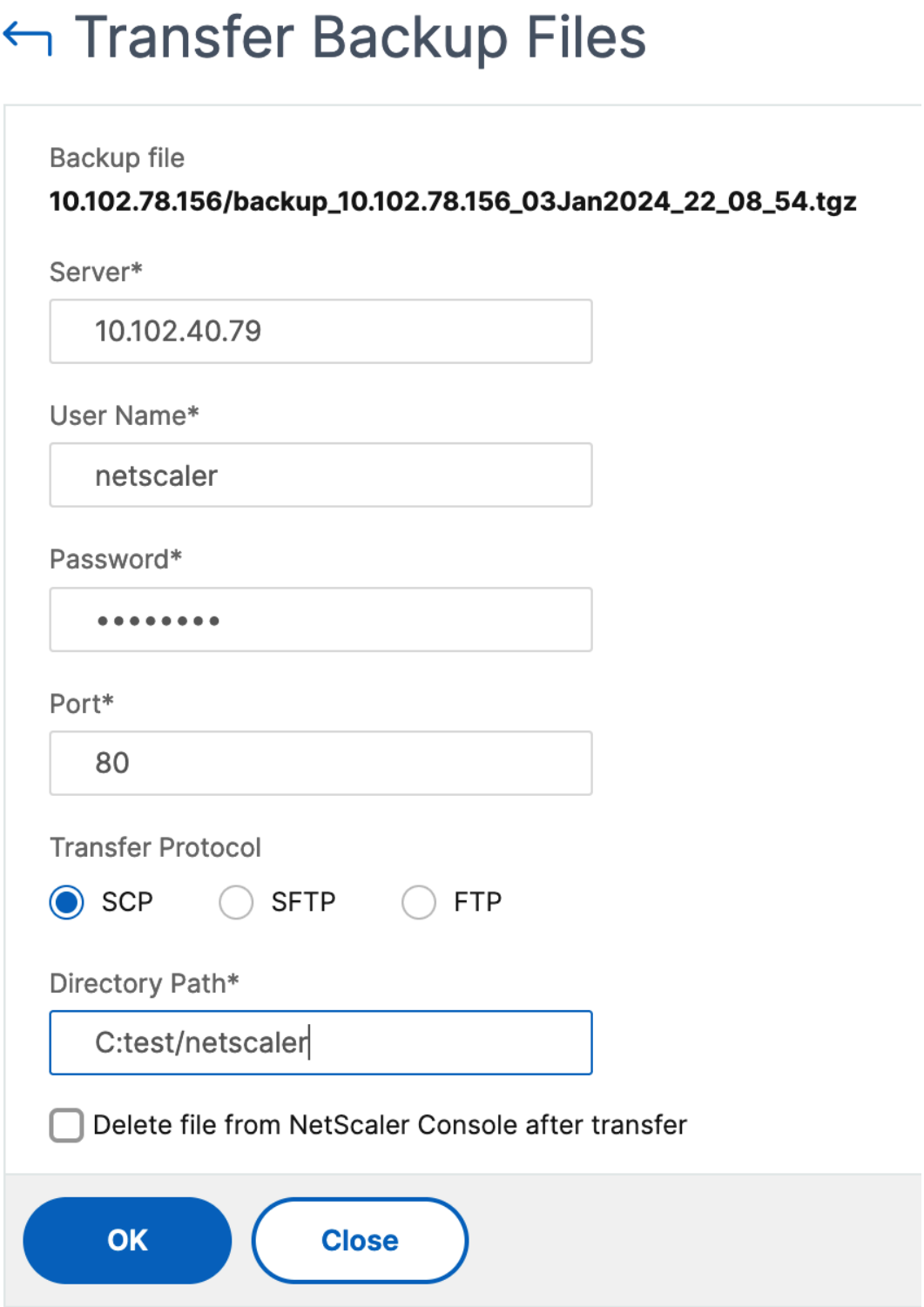
   b) **Benutzername** und **Kennwort** —Benutzeranmeldeinformationen des neuen Systems, in das die gesicherten Dateien kopiert werden.

   c) **Port** —Portnummer des Systems, auf das die Dateien übertragen werden.

   d) **Übertragungsprotokoll** —Protokoll, das für die Übertragung der Backupdatei verwendet wird. Sie können SCP-, SFTP- oder FTP-Protokolle auswählen, um die Backupdatei zu übertragen.

   e) **Verzeichnispfad** —Der Speicherort, an den die gesicherte Datei auf dem neuen System übertragen wird.

f) Klicken Sie auf **OK**.



> **Hinweis:**
>
> Die Sicherungsdateien vom NetScaler Console-Dienst werden über einen Agenten an den externen Server gesendet. Wenn es viele Agenten gibt, wird eine NetScaler-Backup-Datei über denselben Agenten gesendet, der zum Hinzufügen dieser NetScaler-Instanz verwendet wurde. Um mehr über die mit einem Agenten verknüpften Instanzen zu erfahren, navigieren Sie zu **Infrastruktur > NetScaler Agents**.

Stellen Sie eine NetScaler-Instanz mithilfe der NetScaler Console wieder her

> **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 Wiederherstellungsvorgang auf der primären NetScaler-Instanz starten, können Sie nicht auf die primäre Instanz zugreifen und die sekundäre Instanz wird in **STAYSECONDARY** geändert. Sobald der Wiederherstellungsvorgang auf der primären Instanz abgeschlossen ist, wechselt die sekundäre NetScaler-Instanz vom **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 **Backup anzeigen**.
2. Wählen Sie auf der Seite **Sicherungsdateien** die Sicherungsdatei aus, die die Einstellungen enthält, die Sie wiederherstellen möchten, und klicken Sie dann auf **Wiederherstellen**.

Stellen Sie eine NetScaler SDX-Appliance mithilfe der NetScaler Console wieder her

In NetScaler Console umfasst das Backup einer 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)

Sie müssen Ihre NetScaler SDX-Appliance auf die in der Backupdatei verfügbare Konfiguration wiederherstellen. Während der Wiederherstellung der Appliance wird die gesamte aktuelle Konfiguration gelöscht.

Wenn Sie die NetScaler SDX-Appliance mit dem Backup einer anderen NetScaler SDX-Appliance wiederherstellen, stellen Sie sicher, dass Sie die Lizenzen hinzufügen und die Verwaltungsdienst-Netzwerkeinstellungen der Appliance so konfigurieren, dass sie mit denen in der Backupdatei übereinstimmen, bevor Sie den Wiederherstellungsvorgang starten.

Stellen Sie sicher, dass die gesicherte NetScaler SDX-Plattformvariante dieselbe ist wie die, die Sie wiederherstellen möchten. Sie können nicht von einer anderen Plattformvariante wiederherstellen.

> **Hinweis:**
>
> Bevor Sie die SDX RMA-Appliance wiederherstellen, stellen Sie sicher, dass die gesicherte Version entweder dieselbe oder eine höhere als die RMA-Version ist.

So stellen Sie die SDX-Appliance aus der gesicherten Datei wieder her:

1. Navigieren Sie in der NetScaler Console-GUI zu **Infrastruktur > Instances > NetScaler**.
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**.

Exportieren Sie den Bericht dieses Dashboards

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** . Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Failovers auf die sekundäre NetScaler-Instanz erzwingen

January 26, 2024

Möglicherweise möchten Sie ein Failover erzwingen, wenn Sie beispielsweise die primäre Citrix Application Delivery Controller (NetScaler) -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 mithilfe der NetScaler Console ein Failover auf die sekundäre NetScaler-Instanz:

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Instanzen** . Gehen Sie zur Registerkarte **VPX** und wählen Sie eine Instanz aus.
2. Wählen Sie Instanzen in einem HA-Setup aus den Instanzen aus, die unter dem ausgewählten Instanztyp aufgeführt sind.
3. Wählen Sie im Feld **Aktion** die Option **Failover erzwingen aus.**
4. Klicken Sie auf **Ja**, um die Aktion "Failover erzwingen"zu bestätigen.

Erzwingen, dass eine sekundäre NetScaler-Instanz sekundär bleibt

January 26, 2024

In einem Hochverfügbarkeits-Setup (HA) kann der sekundäre Knoten gezwungen werden, unabhängig vom Status des primären Knotens zweitrangig zu bleiben.

Angenommen, der primäre Knoten muss aktualisiert werden und der Prozess dauert einige Sekunden. Während des Upgrades kann der primäre Knoten für einige Sekunden ausfallen, aber Sie möchten nicht, dass der sekundäre Knoten die Kontrolle übernimmt, und Sie möchten, dass er der sekundäre Knoten bleibt, selbst wenn er einen Fehler im primären Knoten erkennt.

Wenn Sie den sekundären Knoten zwingen, sekundär zu bleiben, bleibt er sekundär, selbst wenn der primäre Knoten ausfällt. Wenn Sie erzwingen, dass der Status eines Knotens in einem HA-Paar sekundär bleibt, nimmt er nicht an Übergängen des HA-Zustands der Maschine teil. Der Status des Knotens wird als STAYSECONDARY angezeigt.

> **Hinweis**
>
> Wenn Sie ein System zwingen, sekundär zu bleiben, wird der erzwungene Prozess weder propagiert noch synchronisiert. Sie wirkt sich nur auf den Knoten aus, auf dem Sie den Befehl ausführen.

So konfigurieren Sie eine sekundäre NetScaler-Instanz mithilfe der NetScaler Console so, dass sie sekundär bleibt:

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Instanzen** und wählen Sie dann eine Instanz unter einem Instanztyp (VPX) aus.
2. Wählen Sie Instanzen in einem HA-Setup aus den Instanzen aus, die unter dem ausgewählten Instanztyp aufgeführt sind.
3. Wählen Sie im Feld **Aktion** die Option **Sekundär bleiben**aus.
4. Klicken Sie auf **Ja**, um die Ausführung der Aktion "Secondary bleiben"zu bestätigen.

Instanzgruppen erstellen

January 26, 2024

Um eine Instanzgruppe zu erstellen, müssen Sie zuerst alle Ihre NetScaler-Instanzen zur NetScaler Console 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 Console

1. Navigieren Sie in der NetScaler Console zu Infrastruktur > Instanzen > 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. Wählen Sie unter **Kategorie**die Option **Standard** aus.
4. 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** .
5. Klicken Sie auf **Erstellen**.

Standortgruppen für globalen Serverlastenausgleich

January 26, 2024

Wenn Sie die kontinuierliche Verfügbarkeit und Disaster Recovery für Ihre ADC-Instanzen sicherstellen möchten, können Sie eine GSLB-Standortgruppe konfigurieren. Es gleicht die Last zwischen den Standorten aus, indem Kundenanfragen an den nächstgelegenen oder leistungsstärksten Standort oder an überlebende Standorte weitergeleitet werden, wenn es zu einem Ausfall kommt.

Manchmal versuchen die Konfigurationsobjekte der ADC-Instanzen in einer GSLB-Site-Gruppe, sich gegenseitig zu überschreiben. Es führt zu einer Rennbedingung. Um solche Probleme zu beheben, müssen Sie die Auswahl des primären Knotens in der GSLB-Site-Gruppe steuern. Die Konfiguration im primären Knoten wird auf die verbleibenden ADC-Instanzen angewendet. In NetScaler Console können Sie eine GSLB-Sitegruppe erstellen und wie folgt vorgehen:

- Wählen Sie einen primären Knoten unter den ausgewählten ADC-Instanzen.
- Legen Sie die Prioritätsreihenfolge für die primäre Knotenauswahl fest, wenn der ausgewählte primäre Knoten ausfällt.

Sie können Ihre GSLB-Standortgruppen unter **Infrastruktur > Instanzen > GSLB-Site-Gruppe**anzeigen.

Erstellen einer GSLB-Site-Gruppe

Führen Sie die folgenden Schritte aus, um eine GSLB-Standortgruppe mit ADC-Instanzen zu erstellen:

1. Gehen Sie zu **Infrastruktur > Instanzen > GSLB-Site-Gruppe**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie einen Namen für die GSLB-Site-Gruppe an.
4. Wählen Sie die Instanzen aus, die Sie in der GSLB-Site-Gruppe hinzufügen möchten. Diese Instanzen fungieren als Standorte in der Gruppe.
5. Wählen Sie mindestens eine Site aus und klicken Sie auf **Aktive Site erstellen**.

   Eine Instanz, die auf Priorität 1 gesetzt ist, wird zum primären Knoten. Sie können die Priorität der aktiven Websites neu anordnen. Wählen Sie die Instanz mit niedrigerer Priorität und klicken Sie **auf Priorität nach oben**.
6. Klicken Sie auf **Erstellen**.

Unter **Infrastruktur > Netzwerkfunktionen > GSLB**zeigt die GUI die Entitäten nur vom primären ADC-Knoten der GSLB-Site-Gruppe an.

SNMP-Manager und Benutzer für NetScaler Agent erstellen

January 26, 2024

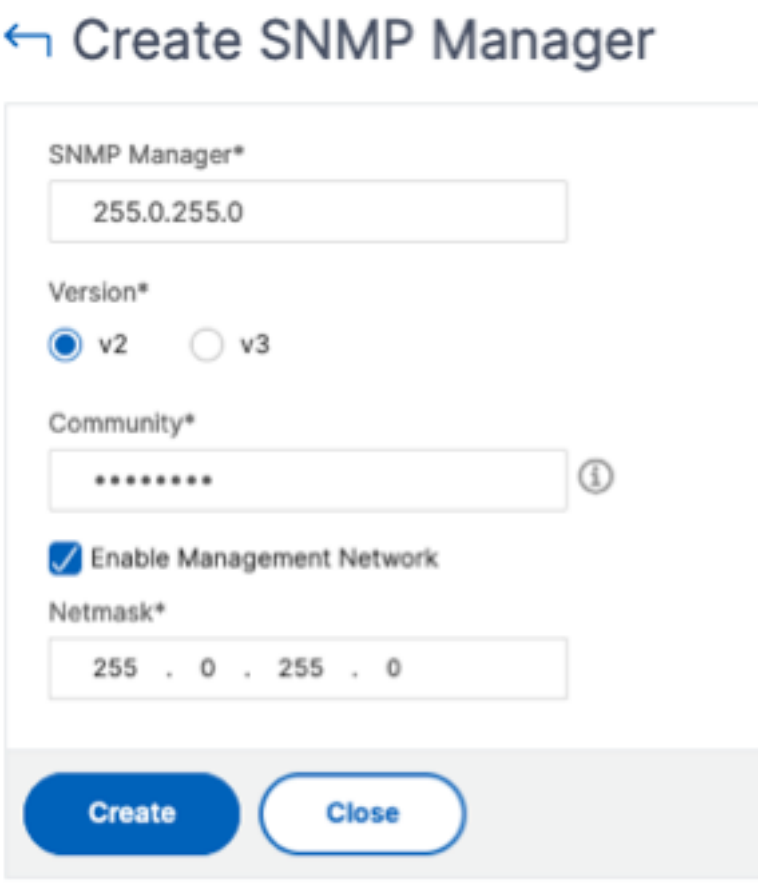
Sie können den SNMP-Agenten über ein Remote-Gerät, das als SNMP-Manager bezeichnet wird, nach systemspezifischen Informationen fragen. Der Agent durchsucht dann die MIB (Management Information Base) nach angeforderten Daten und sendet die Daten an den SNMP-Manager.

Sie können einen SNMP-Manager hinzufügen, um einen NetScaler Agent abzufragen. Der Manager entspricht SNMP V2 und V3. Wenn Sie einen oder mehrere SNMP-Manager angeben, akzeptiert der NetScaler 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 Agent hinzu:

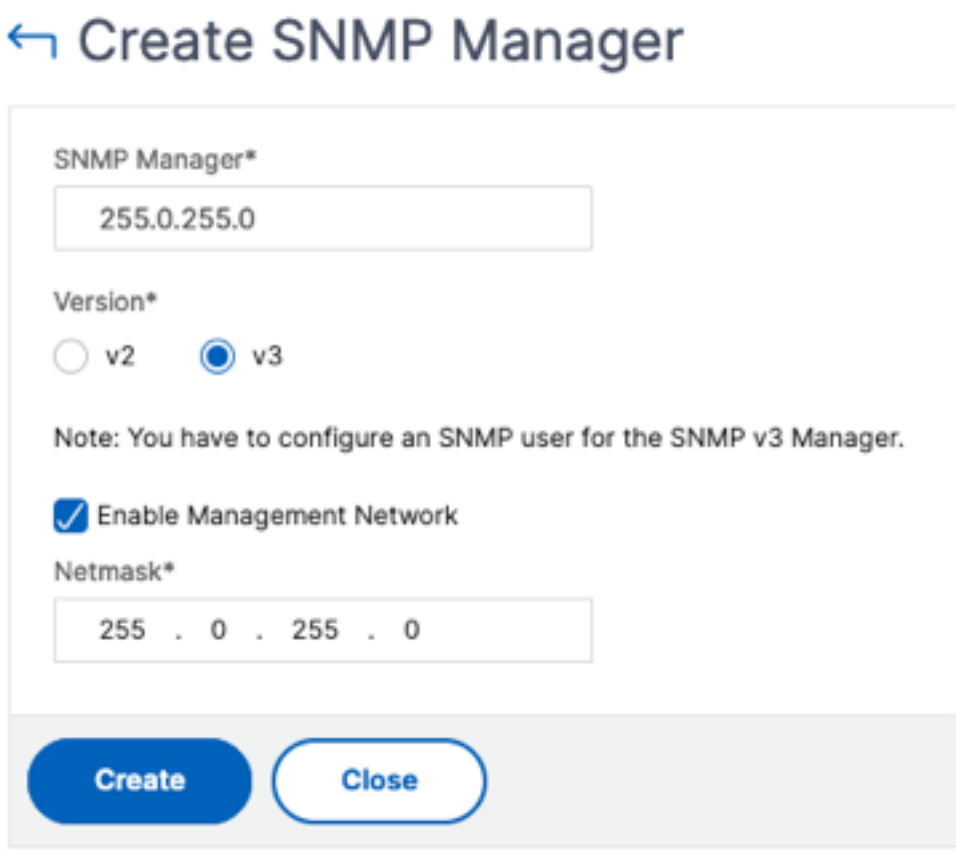
1. Navigieren Sie zu **Infrastruktur > Instanzen > Agents** , wählen Sie einen NetScaler Agent aus und klicken Sie auf **Aktion auswählen > SNMP verwalten** .
2. Klicken Sie auf der Registerkarte **SNMP > SNMP Manager** auf **Hinzufügen**.
3. Geben Sie auf der Seite **SNMP-Manager erstellen** die folgenden 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**: Wählen 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 **Create**.



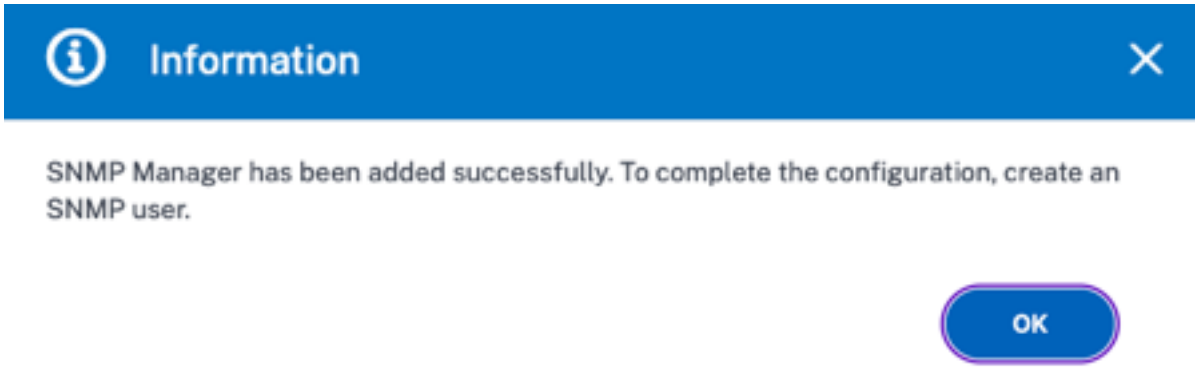
Fügen Sie einen SNMP v3-Manager hinzu

So fügen Sie einen SNMP v3 Manager für den NetScaler Agent hinzu:

1. Navigieren Sie zu **Infrastruktur > Instanzen > Agents** , wählen Sie einen NetScaler 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**: Wählen 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 **Create**.



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

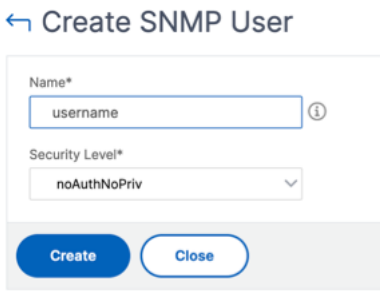
Fügen Sie einen SNMP-Benutzer hinzu, um auf die SNMP v3-Abfragen eines SNMP-Managers zu antworten.

So fügen Sie einen SNMP-Benutzer für den NetScaler Agent hinzu:

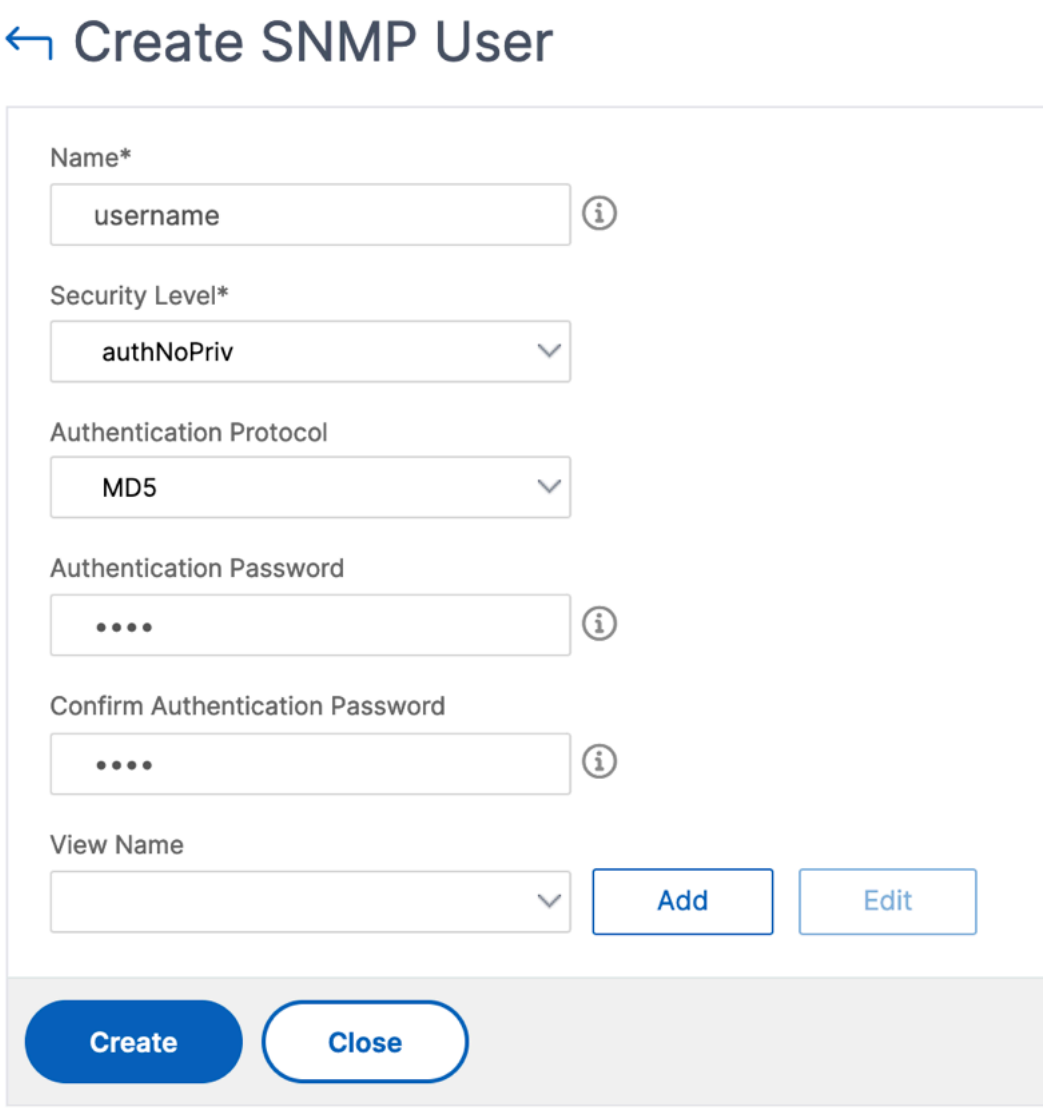
1. Navigieren Sie zu **Infrastruktur > Instanzen > Agents** , wählen Sie einen NetScaler Agent aus und klicken Sie auf **Aktion auswählen > SNMP verwalten** .
2. Klicken Sie auf der Registerkarte **SNMP > SNMP-Benutzer** auf **Hinzufügen**.
3. Fügen Sie auf der Seite **SNMP-Benutzer erstellen** die folgenden Details hinzu:

    - **Name.** Geben Sie den Benutzernamen ein.
    - **Sicherheitsstufe**. Sicherheitsstufe, die für die Kommunikation zwischen dem NetScaler Agent und dem SNMP-Manager erforderlich ist.

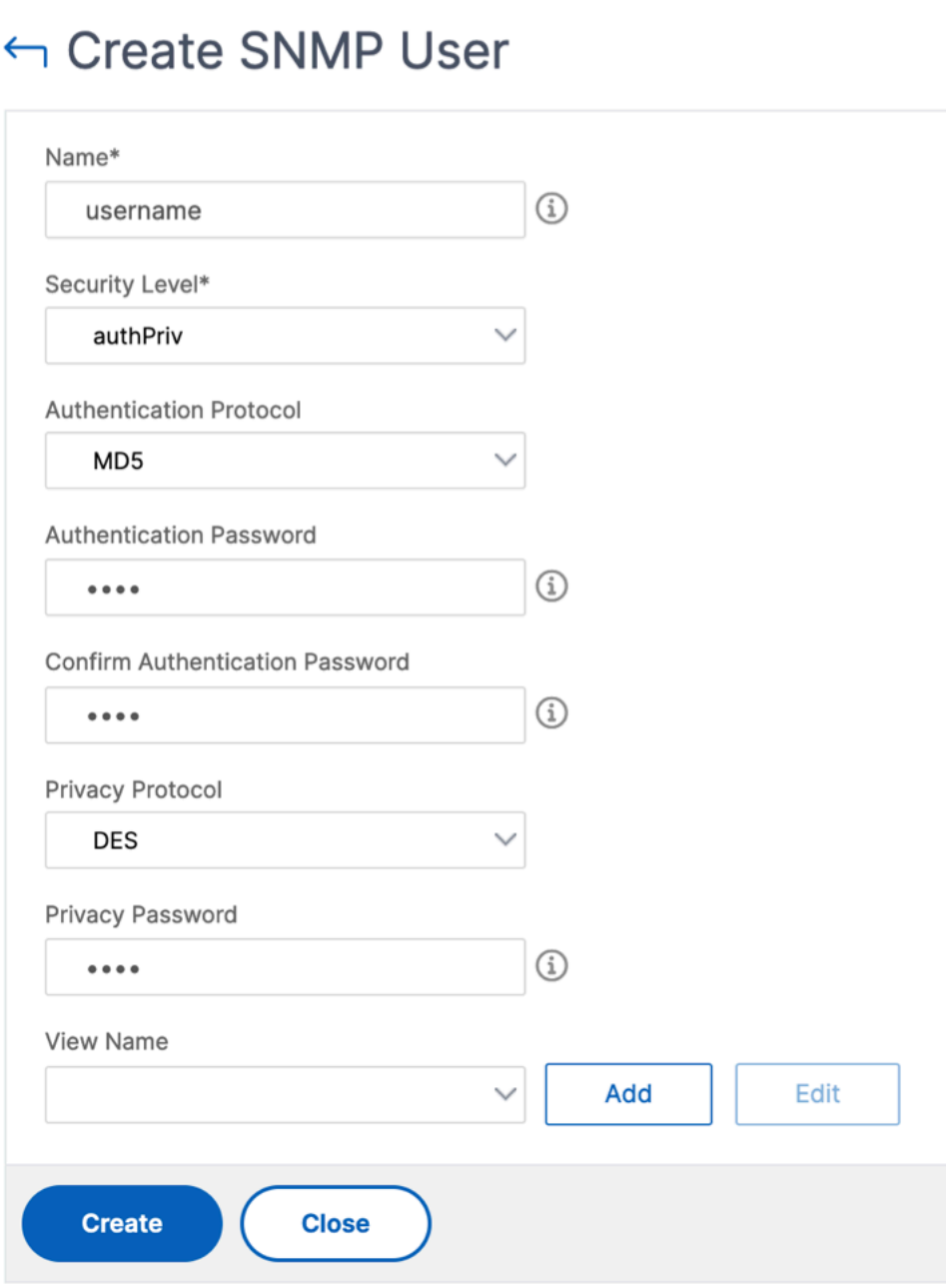
      Wählen Sie eine der folgenden Sicherheitsstufen aus:
    - **noAuthNoPriv**. Erfordert weder Authentifizierung noch Verschlüsselung.



    - **authNoPriv**. Authentifizierung erforderlich, aber keine Verschlüsselung.



- **authPriv**. Authentifizierung und Verschlüsselung erforderlich.



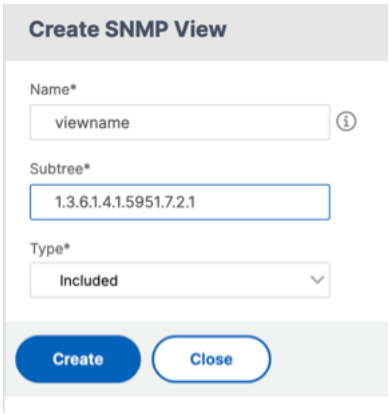
Geben Sie basierend auf der Sicherheitsstufe, die Sie dem Benutzer zugewiesen haben, zusätzliche Authentifizierungsprotokolle an, wie Authentifizierungsprotokolle, Datenschutzkennwörter und Zuweisen von SNMP-Ansichten.

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 Agent zuzulassen oder einzuschränken:

1. Navigieren Sie zu **Infrastruktur > Instanzen > Agents** , wählen Sie einen NetScaler Agent aus und klicken Sie auf **Aktion auswählen SNMP verwalten**.
2. Klicken Sie auf der Registerkarte **SNMP > SNMP-Benutzer** auf **Hinzufügen**.
3. 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.
4. Klicken Sie auf **Create**.



NetScaler VPX-Instanzen auf SDX bereitstellen

January 26, 2024

Sie können eine oder mehrere NetScaler VPX-Instanzen auf der SDX-Appliance mithilfe der NetScaler Console bereitstellen. Die Anzahl der Instanzen, die Sie bereitstellen können, hängt von der erworbenen Lizenz ab. Wenn die Anzahl der hinzugefügten Instanzen der in der Lizenz angegebenen Anzahl entspricht, können Sie mit der NetScaler Console keine weiteren NetScaler-Instanzen bereitstellen.

Bevor Sie beginnen, stellen Sie sicher, dass Sie in der NetScaler Console eine SDX-Instanz hinzufügen, auf der Sie VPX-Instanzen bereitstellen möchten.

Führen Sie die folgenden Schritte aus, um eine VPX-Instanz bereitzustellen:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**.

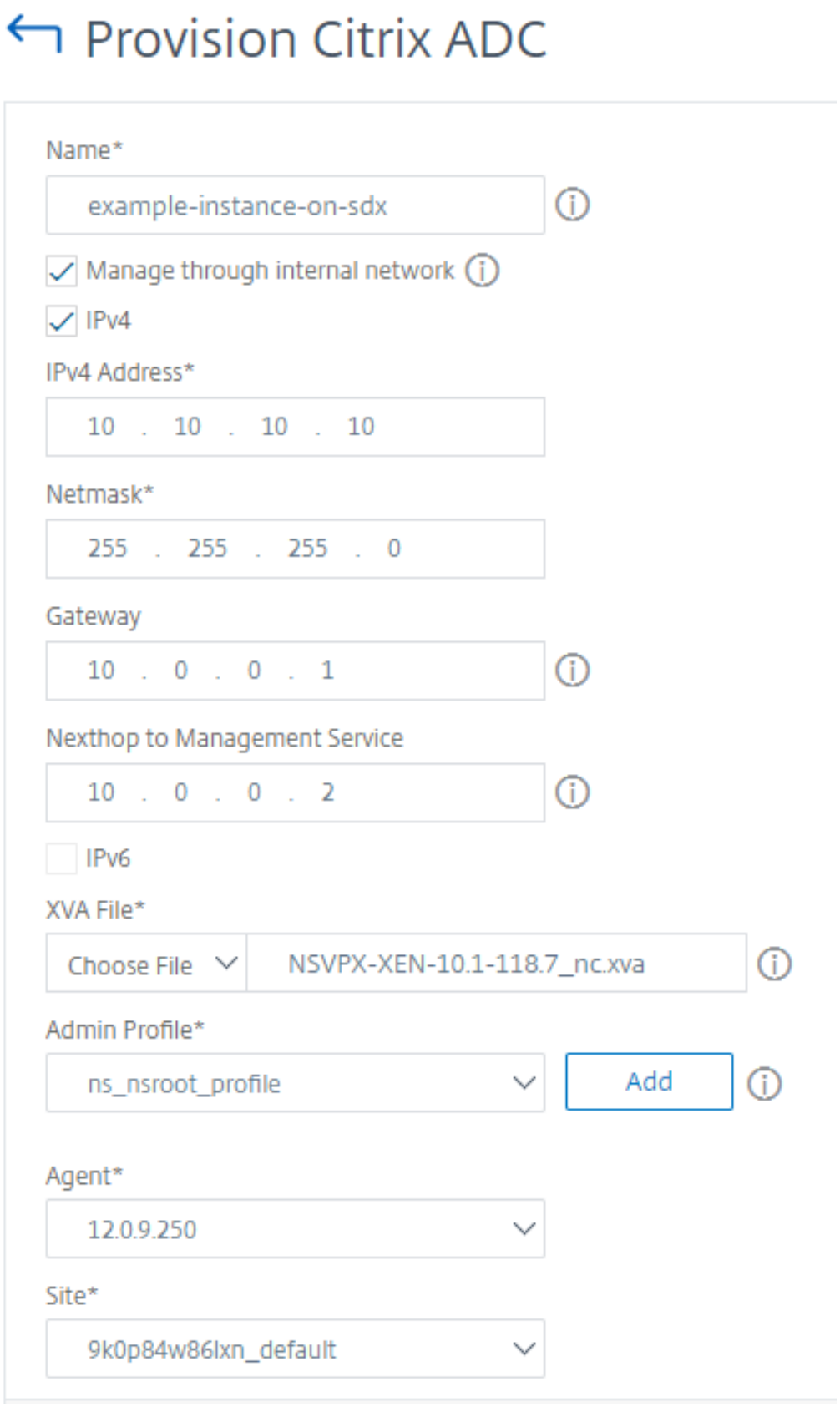
2. Wählen Sie auf der Registerkarte **SDX** eine SDX-Instanz aus, in der Sie eine VPX-Instanz bereitstellen möchten.
3. Wählen Sie unter **Aktion auswählen** die Option **VPX bereitstellen** aus.

Schritt 1 - Hinzufügen einer VPX-Instanz

Die NetScaler Console verwendet die folgenden Informationen, um VPX-Instanzen in einer SDX-Appliance zu konfigurieren:

- **Name**—Geben Sie einen Namen für eine NetScaler-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 —Mit dieser Option wird ein internes Netzwerk für die Kommunikation zwischen der NetScaler Console und einer VPX-Instanz eingerichtet.
  - **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 der NetScaler Console für die IP-Adresse für die ausgewählte Option eine Netzmaske, ein Standard-Gateway und den nächsten Hop 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 NetScaler Console-Dateibrowser aus.
- **Admin-Profil** —Dieses Profil bietet Zugriff auf die Bereitstellung von VPX-Instanzen. Mit diesem Profil ruft NetScaler Console 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

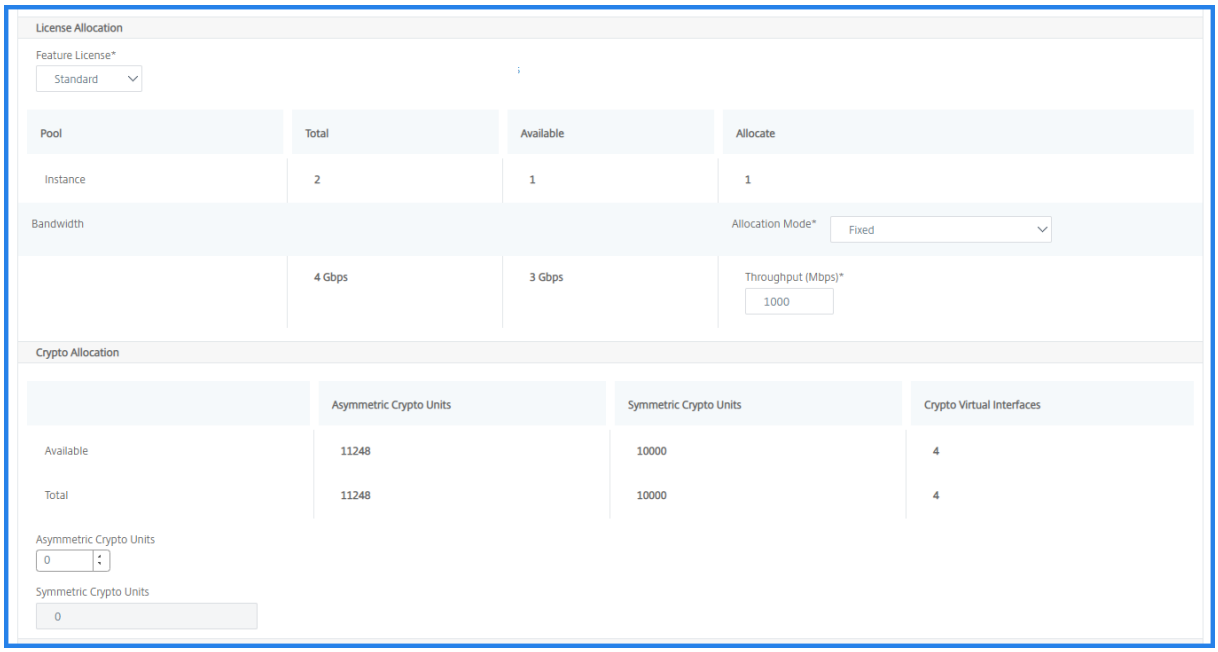
Geben Sie im Abschnitt **Lizenzzuweisung** die VPX-Lizenz an. Sie können Standard-, Advanced- und Premium-Lizenzen verwenden.

- **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.

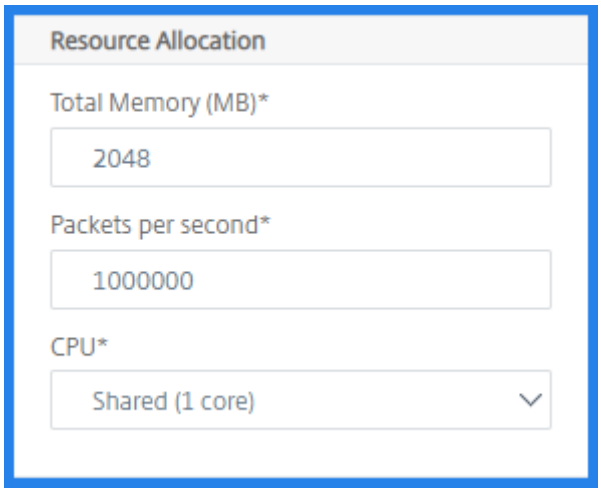
- **Gesamtspeicher (MB)** - Weisen Sie einer Instanz den gesamten Arbeitsspeicher zu. Der Mindestwert ist 2048 MB.
- **Pakete pro Sekunde** - Geben Sie die Anzahl der Pakete an, die pro Sekunde übertragen werden sollen.
- **CPU** —Geben Sie die Anzahl der CPU-Kerne für eine Instanz an. Sie können gemeinsam 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.



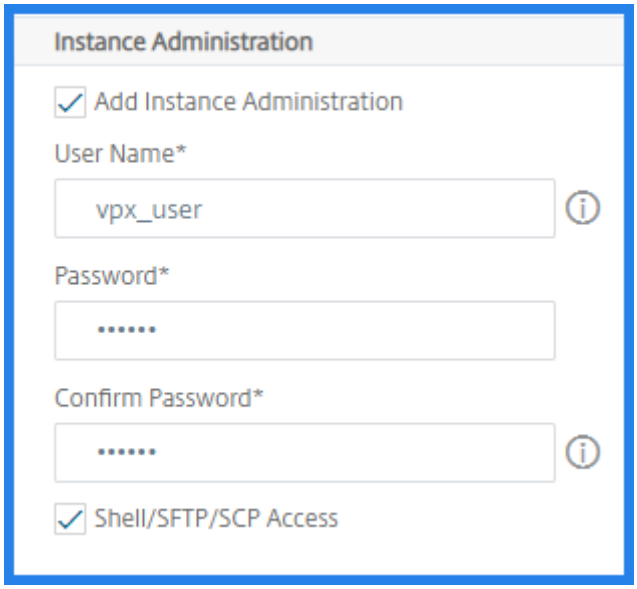
Weitere Informationen finden Sie in der Tabelle unter Bereitstellen von NetScaler-Instanzen, in der die unterstützte VPX, die Einzelpaket-Image-Version und die Anzahl der Kerne aufgeführt sind, die Sie einer Instanz zuweisen können

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:

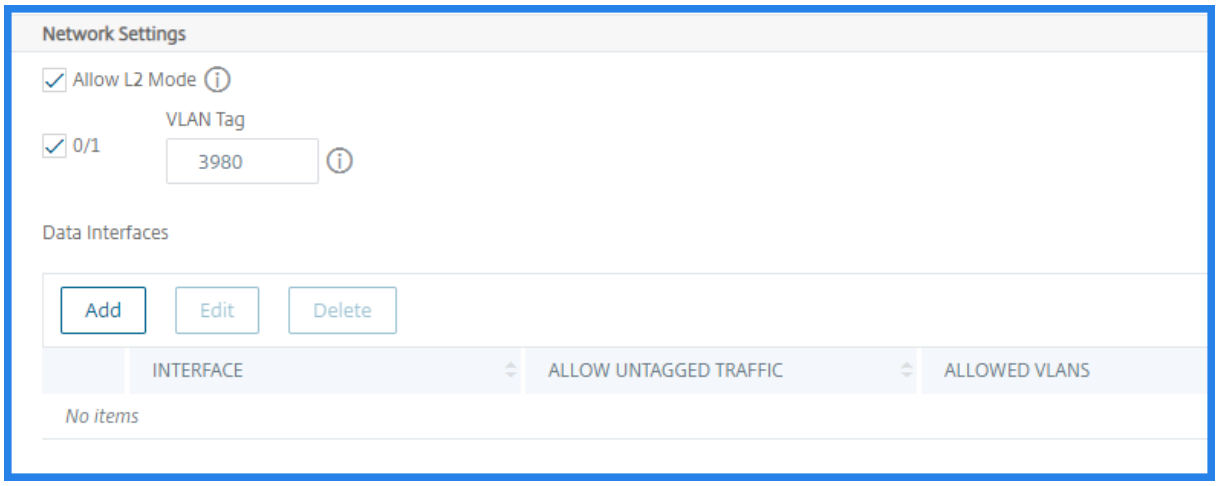
- **L2-Modus unter Netzwerkeinstellungen** zulassen: Sie können den L2-Modus auf der NetScaler-Instanz zulassen. Wählen Sie unter Netzwerkeinstellungen die Option L2-Modus zulassenaus. Bevor Sie sich bei der Instanz anmelden und den L2-Modus aktivieren. Weitere Informationen finden Sie unter Zulassen 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:

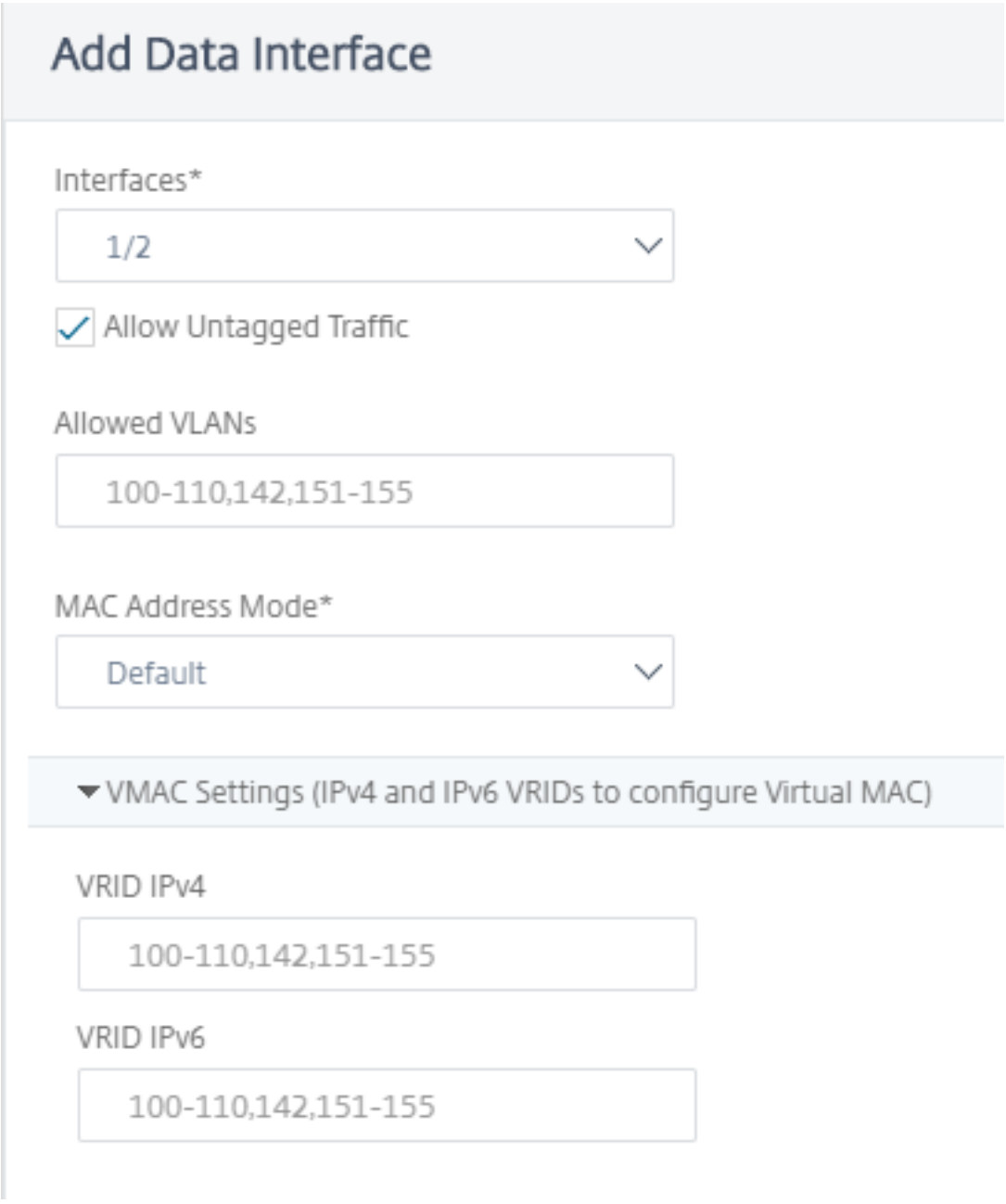
- **Schnittstellen** - Wählen Sie die Schnittstelle aus der Liste aus.

  > **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

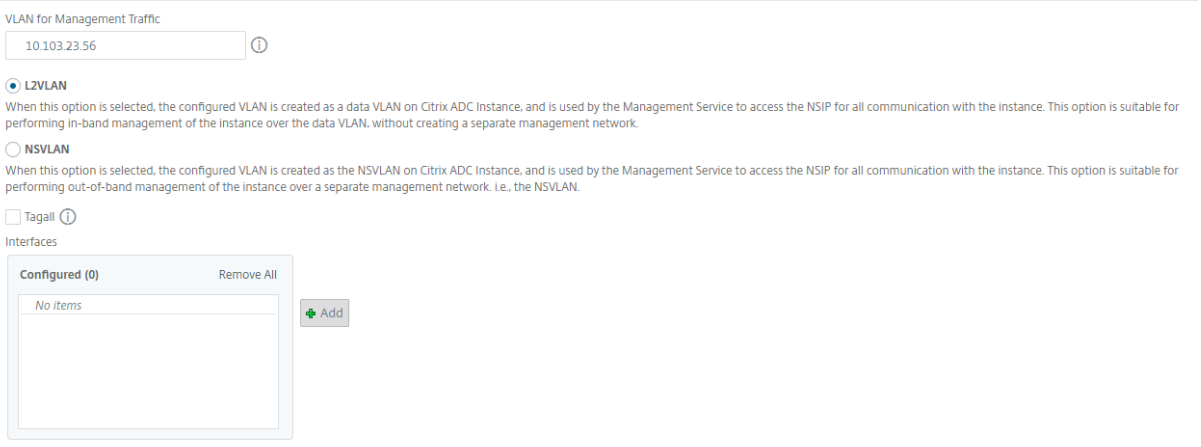
Der Verwaltungsdienst und die Verwaltungsadresse (NSIP) der VPX-Instanz befinden sich im selben Subnetz, und die Kommunikation erfolgt über eine Verwaltungsschnittstelle.

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.

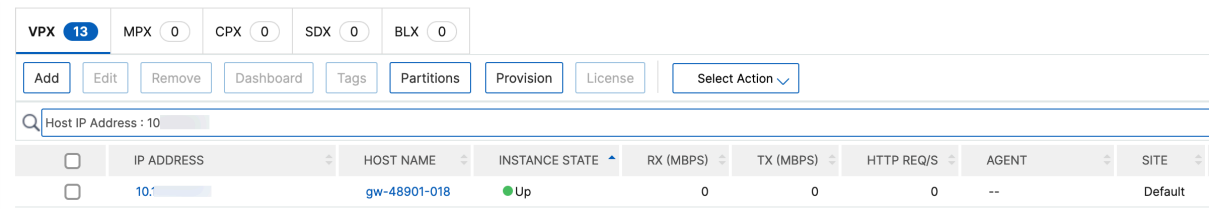


Klicken Sie auf **Fertig**, um eine VPX-Instanz bereitzustellen.

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.



Erkennen Sie mehrere NetScaler-Instanzen erneut

January 26, 2024

Sie können mehrere Citrix Application Delivery Controller (NetScaler) -Instanzen (VPX, MPX, SDX, BLX und CPX) in Ihrem NetScaler Console-Setup wiedererkennen. Nachdem Sie die Instanzen erneut erkannt haben, können Sie die neuesten Status und Konfigurationen dieser Instanzen anzeigen. Der NetScaler Console-Server erkennt alle ADC-Instanzen erneut und prüft, ob die Instanzen erreichbar sind.

So erkennen Sie mehrere NetScaler VPX-Instanzen erneut:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**. Wählen Sie die Registerkarte “Instanz”(VPX, MPX, SDX, BLX und CPX) und wählen Sie die Instanzen aus, die Sie erneut ermitteln möchten.
2. Klicken Sie im Feld **Aktion** auf **Wiederermitteln**. Sie können auch mehrere VPX-Instanzen wiederentdecken.
3. Wenn die Bestätigungsmeldung für die Ausführung des Dienstprogramms Wiederermittlung angezeigt wird, klicken Sie auf **Ja**.

   Auf dem Bildschirm wird der Fortschritt der Wiederentdeckung der einzelnen Instanzen angezeigt.

Übersicht über die Abrufung

January 26, 2024

Polling ist ein Prozess, bei dem NetScaler Console bestimmte Informationen von NetScaler-Instanzen sammelt. Möglicherweise haben Sie weltweit mehrere NetScaler-Instanzen für Ihre Organisation konfiguriert. Um Ihre Instanzen über NetScaler Console zu überwachen, muss NetScaler Console bestimmte Informationen wie CPU-Auslastung, Speicherauslastung, SSL-Zertifikate, lizenzierte Funktionen und Lizenztypen von allen verwalteten NetScaler-Instanzen erfassen. Im Folgenden sind die verschiedenen Abfragetypen aufgeführt, die zwischen NetScaler Console und den verwalteten Instanzen auftreten:

- Instanz-Abfrage
- Lagerbestandsabfrage
- Erfassung von Leistungsdaten
- Instanzbackupabruf
- Abfragen der Konfigurationsüberprüfung
- Abfrage von SSL-Zertifikaten
- Entitätsabfrage

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

Wie NetScaler Console verwaltete Instanzen und Entitäten abfragt

NetScaler Console fragt standardmäßig automatisch in regelmäßigen Intervallen ab. Mit NetScaler Console können Sie auch Abfrageintervalle für einige Abfragetypen konfigurieren und bei Bedarf manuell Abfragen durchführen.

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)	Die Backup-Datei des aktuellen Status der verwalteten NetScaler-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 NetScaler-Instanzen auftreten (z. B. laufende Konfiguration im Vergleich zu gespeicherten Konfigurationen)	SSH, SCP- und NITRO-Anruf	Ja. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsüberprüfung**. Klicken Sie auf der Seite Configuration Audit auf **Einstellungen**, und konfigurieren Sie das Abrufintervall für Configuration Audit Polling.

Abfrage-Typ	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufin
				Sie können Konfigurationsaudits manuell abfragen und alle Konfigurationsaudits der Instanzen sofort zur NetScaler Console hinzufügen. Navigieren Sie dazu zu **Infrastruktur > Konfiguration > Konfigurationsüberprüfung** und klicken Sie auf **Jetzt abfragen**. Auf der Seite **Jetzt abfragen** können Sie alle oder ausgewählte Instanzen im Netzwerk abfragen.
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.

Abfrage-Typ	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufin
				Sie können SSL-Zertifikate manuell abfragen und alle Zertifikate der Instanzen sofort zur NetScaler Console 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 NetScaler-Instanz verknüpft ist. Informationen zum Aktivieren von Entitätsabfragen finden Sie unter Aktivieren oder Deaktivieren der NetScaler Console-Funktionen .	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 zur NetScaler Console 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 Ereignisse, die von verwalteten NetScaler-Instanzen generiert werden, von NetScaler Console 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 Instanz-Backups werden SSL-Dateien, CA-Zertifikatsdateien, NetScaler-Vorlagen, Datenbankinformationen usw. auf die NetScaler Console 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 werden die verschiedenen Polling-Methoden beschrieben, die NetScaler Console auf den verwalteten Instanzen durchführt:

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

Globale Abfrage von Instanzen

NetScaler Console fragt je nach dem von Ihnen konfigurierten Intervall automatisch alle verwalteten Instanzen im Netzwerk ab. Obwohl das Standardabfrageintervall 60 Minuten beträgt, können Sie das Intervall je nach Ihren Anforderungen festlegen, indem Sie zu **Infrastruktur > Netzwerkfunktionen > Einstellungen**navigieren.

Manuelles Abrufen von Instanzen

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

In NetScaler Console gibt es ein Mindestabfrageintervall, in dem kein automatisches Polling stattfindet. Wenn Sie eine neue NetScaler-Instanz hinzufügen oder wenn eine Entität aktualisiert wird, erkennt NetScaler Console 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, können Sie mit NetScaler Console jetzt nur ausgewählte Instanzen und Entitäten gleichzeitig abfragen.

NetScaler Console fragt verwaltete Instanzen automatisch ab, um Informationen zu festgelegten Tageszeiten zu sammeln. Ausgewählte Abfragen reduzieren die Aktualisierungszeit, die NetScaler Console benötigt, um den neuesten Status der Entitäten anzuzeigen, die an diese ausgewählten Instanzen gebunden sind.

So fragen Sie bestimmte Instanzen in der NetScaler Console ab:

1. Navigieren Sie in der NetScaler Console 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 **Umfrage starten**.

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

Manuelles Abrufen von Entitäten

Mit NetScaler Console können Sie auch nur einige ausgewählte Entitäten abfragen, die an eine Instanz gebunden sind. Sie können diese Option beispielsweise verwenden, um den neuesten Status einer bestimmten Entität in einer Instanz zu kennen. In diesem Fall müssen Sie die Instanz nicht als Ganzes abfragen, um den Status einer aktualisierten Entität zu ermitteln. Wenn Sie eine Entität auswählen und abfragen, fragt NetScaler Console nur diese Entität ab und aktualisiert den Status in der NetScaler Console-GUI.

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

Sie können nun die folgenden Entitäten für alle Aktualisierungen in ihrem Status, Diensten, Dienstgruppen, Lastenausgleichsserver, virtuelle Server zur Cache-Reduzierung, virtuelle Content Switching-Server, virtuelle Authentifizierungsserver, virtuelle VPN-Server, virtuelle GSLB-Server und Anwendungsserver abfragen.

> **Hinweis:**
>
> Wenn Sie einen virtuellen Server abfragen, wird nur dieser virtuelle Server abgefragt. Die 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 Console ab:

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

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

Instanzverwaltung aufheben

January 26, 2024

Wenn Sie den Informationsaustausch zwischen NetScaler Console und den Instanzen in Ihrem Netzwerk beenden möchten, können Sie die Verwaltung der Instanzen aufheben.

So heben Sie die Verwaltung einer Instanz auf:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**.
2. Wählen Sie die Registerkarte NetScaler-Instanz aus (z. B. VPX).
3. Klicken Sie in der Liste der Instanzen mit der rechten Maustaste auf eine Instanz, und wählen Sie dann **Aufheben** aus, oder wählen Sie Instanz und aus der Liste **Aktion** die Option **Verwalten aufheben** aus.

   Der Status der ausgewählten Instanz ändert sich in **Out of Service**.

   Die Instanz wird nicht mehr von NetScaler Console verwaltet und tauscht keine Daten mehr mit NetScaler Console aus.

Tracing einer Route zu einer Instanz

January 26, 2024

Indem Sie die Route eines Pakets von der NetScaler Console zu einer Instanz verfolgen, können Sie Informationen wie die Anzahl der Hops finden, die erforderlich sind, um die Instanz zu erreichen. Die Traceroute verfolgt den Pfad des Pakets von der Quelle zum Ziel. Es zeigt die Liste der Netzwerk-Hops zusammen mit dem Hostnamen und der IP-Adresse der einzelnen Entitäten in der Route an.

Traceroute erfasst auch die Zeit, die ein Paket für die Reise von einem Hop zum anderen nimmt. Wenn die Übertragung von Paketen unterbrochen wird, zeigt die Traceroute an, wo das Problem besteht.

So verfolgen Sie die Route einer Instanz:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**.

2. Wählen Sie die Registerkarte NetScaler-Instanz aus (z. B. VPX).
3. Klicken Sie in der Liste der Instanzen mit der rechten Maustaste auf eine Instanz, und wählen Sie dann **TraceRoute**aus, oder wählen Sie die Instanz aus, und klicken Sie in der Liste **Aktion**auf **TraceRoute**.

   Das TraceRoute-Meldungsfeld zeigt die Route zur Instanz und die von jedem Hop verbrauchte Zeit in Millisekunden an.

NetScaler-eigene IP-Adressen anzeigen

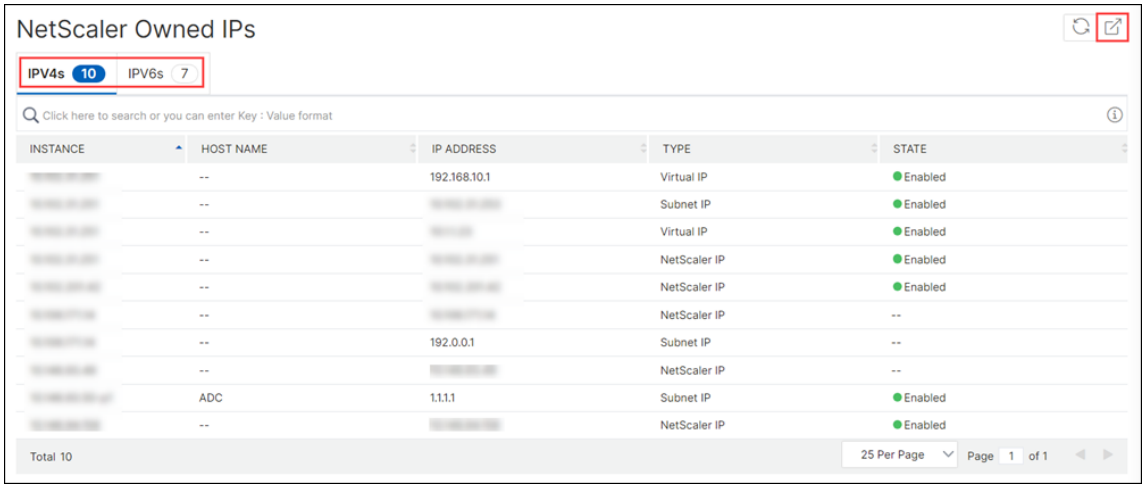
July 17, 2024

Sie können die auf NetScaler-Instanzen konfigurierten IP-Adressen direkt über die NetScaler Console-GUI anzeigen. Bitte beachten Sie, dass die Konfigurationsänderungen und andere Operationen nur auf NetScaler-Instanzen ausgeführt werden können.

Um die NetScaler-eigenen IP-Adressen anzuzeigen, navigieren Sie zu **Infrastruktur > Instanzen > NetScaler-eigene IPs**.

Diese Funktion zeigt sowohl IPv4- als auch IPv6-Adressen an, die auf NetScaler-Instanzen konfiguriert sind. Zu den Arten von IP-Adressen gehören:

- NetScaler IP-Adresse
- Subnetz-IP-Adresse
- Virtuelle IP-Adresse
- IP-Adresse des ADNS-Dienstes
- GSLB-IP-Adresse
- Cluster-IP-Adresse
- Zugeordnete IP-Adresse



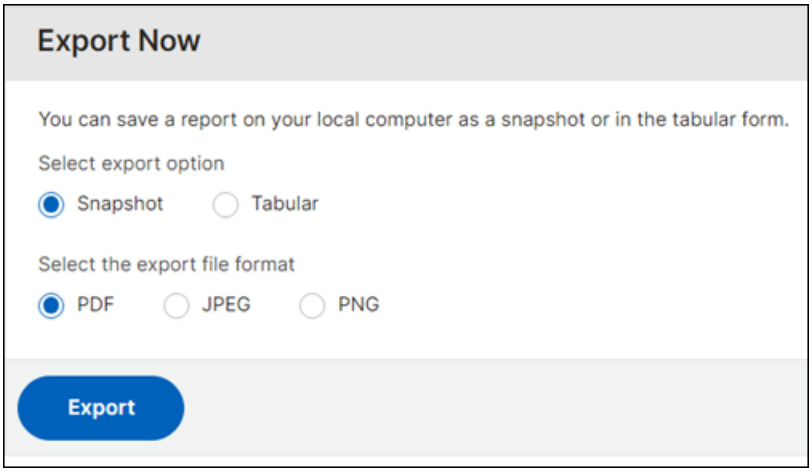
NetScaler-eigene IP-Adressen exportieren

Gehen Sie folgendermaßen vor, um NetScaler-eigene IP-Adressen zu exportieren:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler-eigene IPs**.
2. Klicken Sie auf der Seite **NetScaler Owned IPs** auf das Exportsymbol in der oberen rechten Ecke.
3. Klicken Sie auf der Seite **Berichte exportieren** auf **Jetzt exportieren**.
4. Wählen Sie auf der Seite **Jetzt exportieren** die Exportoption aus:

   Für den **Snapshot**-Export:

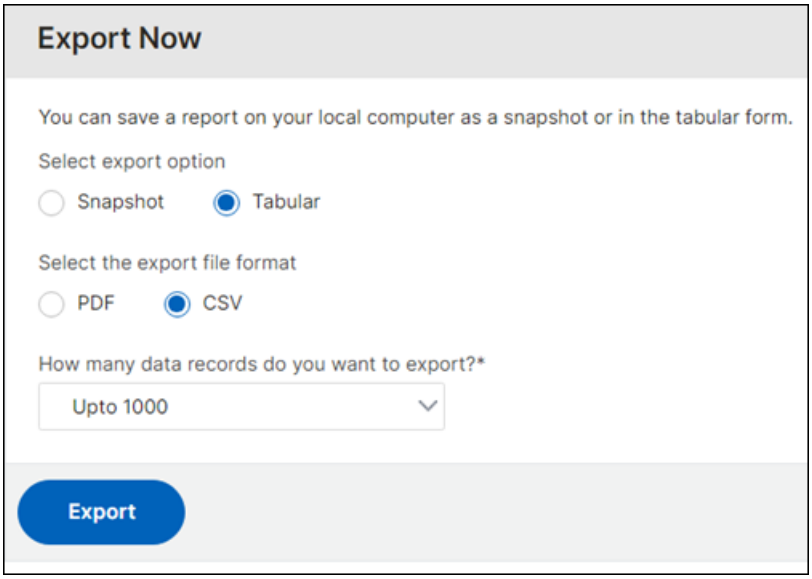
   a) Wählen Sie das Exportdateiformat aus: PDF, JPG oder PNG.



   Für den **tabellarischen** Export:

   a) Wählen Sie das Exportdateiformat: PDF oder CSV.

b) Wählen Sie die Anzahl der zu exportierenden Datensätze aus der Liste aus.



5. Klicken Sie auf **Exportieren**.

Planen Sie den Export von NetScaler-eigenen IP-Adressen

Gehen Sie wie folgt vor, um den Export von NetScaler-eigenen IP-Adressen zu planen:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler-eigene IPs**.
2. Klicken Sie auf der Seite **NetScaler Owned IPs** auf das Exportsymbol in der oberen rechten Ecke.
3. Klicken Sie auf der Seite **Berichte exportieren** auf **Export planen**.
4. Geben Sie auf der Seite **Export planen** die folgenden Details ein:
   a) Geben Sie den Betreff und die Beschreibung ein.
   b) Wählen Sie den Exporttyp aus.

      Für den **Snapshot-Exporttyp**:

      - Wählen Sie das Exportdateiformat aus: PDF, JPG oder PNG.

      Für den **tabellarischen** Exporttyp:

      - Wählen Sie das Exportdateiformat: PDF oder CSV.
      - Wählen Sie die Anzahl der zu exportierenden Datensätze aus der Liste aus.

   c) Wählen Sie die Wiederholung aus: Täglich, Wöchentlich oder Monatlich.
   d) Wählen Sie die Exportzeit aus.

e) Wähle aus, wie die exportierten IP-Adressen gesendet werden sollen: E-Mail, Slack oder beides.

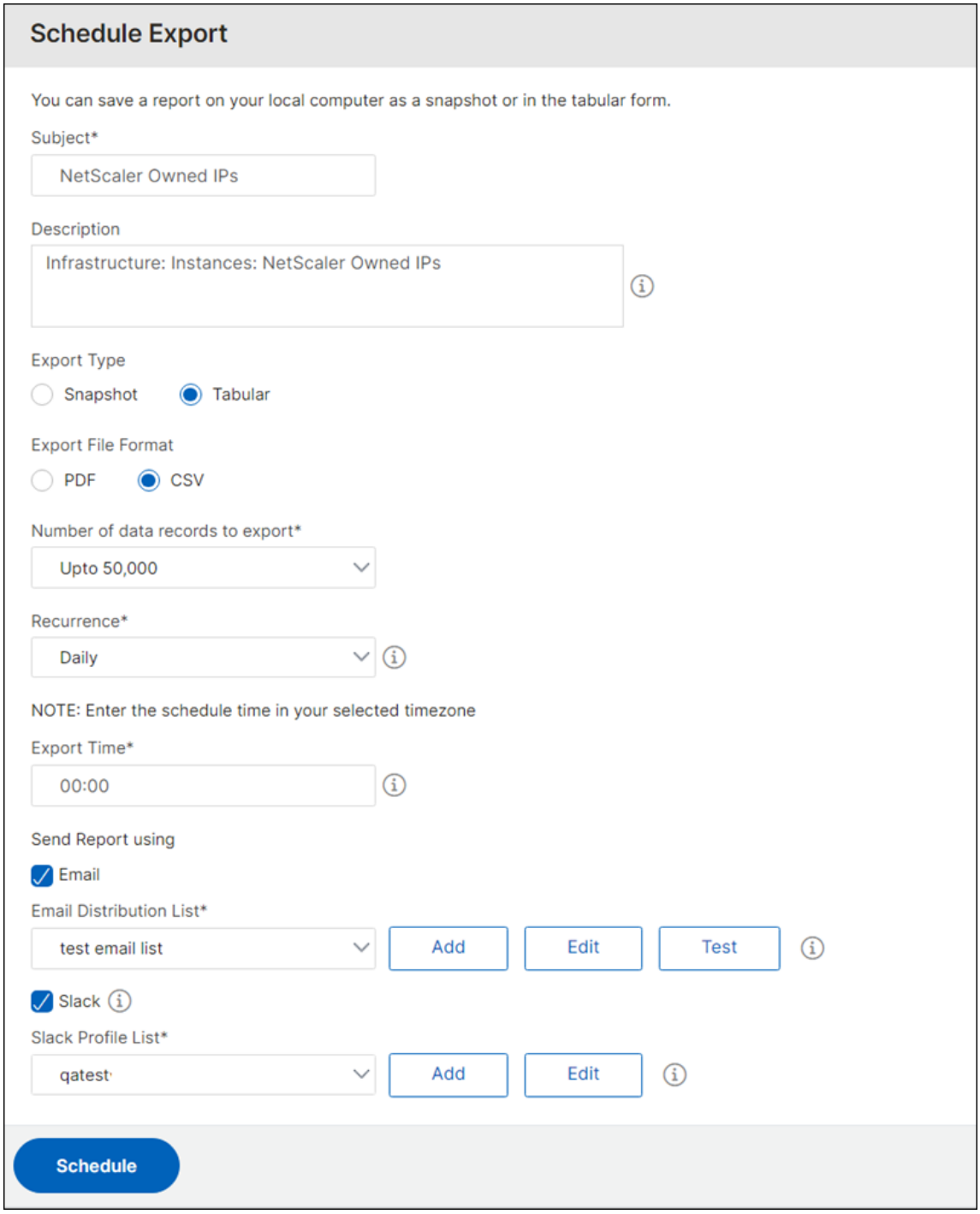
Für E-Mail:

- Wählen Sie **E-Mail** und dann die E-Mail-Verteilerliste aus, um die Liste der NetScaler-eigenen IP-Adressen zu senden.
  - Um eine E-Mail-Verteilerliste hinzuzufügen, klicken Sie auf **Hinzufügen** und geben Sie die E-Mail-Serverdetails an.
  - Um eine E-Mail-Verteilerliste zu bearbeiten, klicken Sie auf **Bearbeiten**.
  - Um zu überprüfen, ob die E-Mail-Verteilerliste funktioniert, klicken Sie auf **Testen**. Dadurch wird eine Test-E-Mail an die ausgewählte E-Mail-Verteilerliste gesendet.

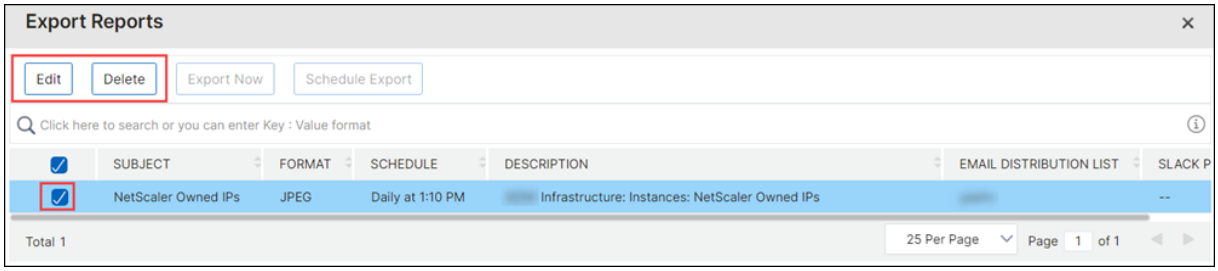
Für Slack:

- Wähle **Slack** und wähle die Slack-Profilliste aus, um die Liste der NetScaler-eigenen IP-Adressen zu senden.
  - Um ein Slack-Profil hinzuzufügen, klicken Sie auf **Hinzufügen** und geben Sie den **Profilnamen**, den **Kanalnamen**und den **Token** des Slack-Channels an.
  - Um einen bestehenden Slack-Kanal zu bearbeiten, klicke auf **Bearbeiten**.

5. Klicken Sie auf **Planen**, um den Export zu planen.



Nach der Planung wird Ihr Exportplan auf der Seite **Berichte exportieren** angezeigt, und Sie können den Zeitplan auswählen, um den Bearbeitungs- oder Löschvorgang durchzuführen.



So ändern Sie das NetScaler MPX oder VPX Root-Kennwort

January 26, 2024

Gelegentlich müssen Sie das Stammkennwort der NetScaler Appliance aus Sicherheitsgründen oder der Einhaltung der Kennwortrotierungsrichtlinie ändern.

In diesem Dokument werden die Schritte beschrieben, die erforderlich sind, um das Root-Kennwort der NetScaler MPX- und VPX-Appliances zu ändern, die über die NetScaler Console Cloud verwaltet werden.

Wenn Sie das NetScaler-Kennwort ändern, müssen Sie das NetScaler Console-Administratorprofil ändern, das dem NetScaler zugeordnet ist. Ein NetScaler Console-Administratorprofil verwaltet die NetScaler-Anmeldeinformationen für die REST-API-, SSH-, SCP- oder SNMP-basierte Kommunikation mit der NetScaler Appliance. Über Administratorprofile verwaltet NetScaler Console NetScaler MPX- und VPX-Appliances.

Kennwort mit Konfigurationsjobs ändern

Mithilfe der Funktion NetScaler Console Configuration Jobs können Sie den sich wiederholenden Kennwortänderungsprozess vereinfachen und die Änderungen auf die NetScaler Appliances anwenden, ohne auf die einzelnen Instanzen zugreifen zu müssen.

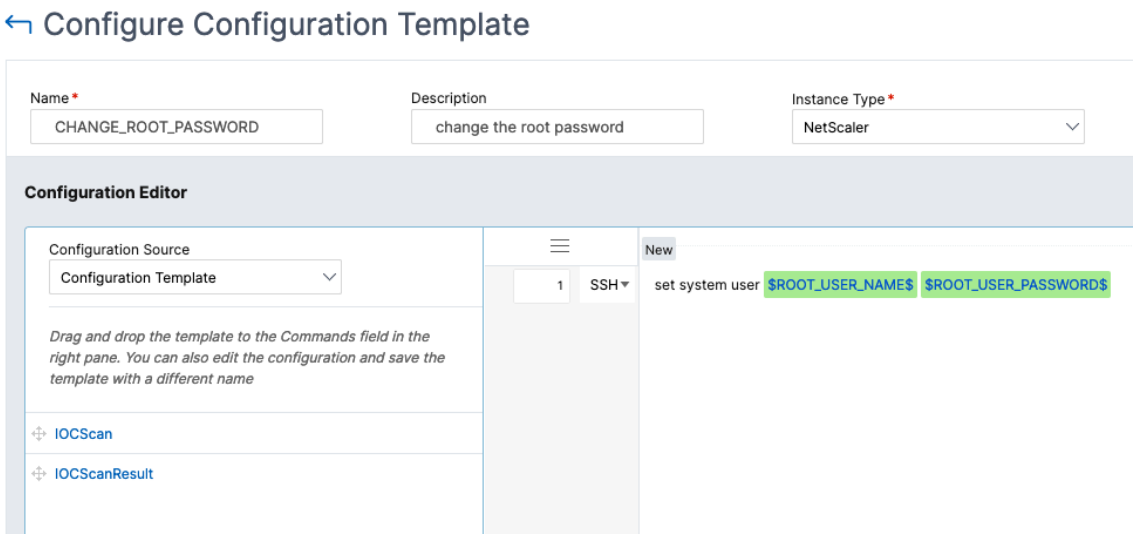
Folgen Sie diesen Schritten, um das Kennwort zu ändern:

- Schritt 1. Erstellen Sie eine Konfigurationsvorlage.
- Schritt 2. Erstellen Sie einen Konfigurationsjob.
- Schritt 3: Erstellen Sie ein Admin-Profil und ändern Sie es.

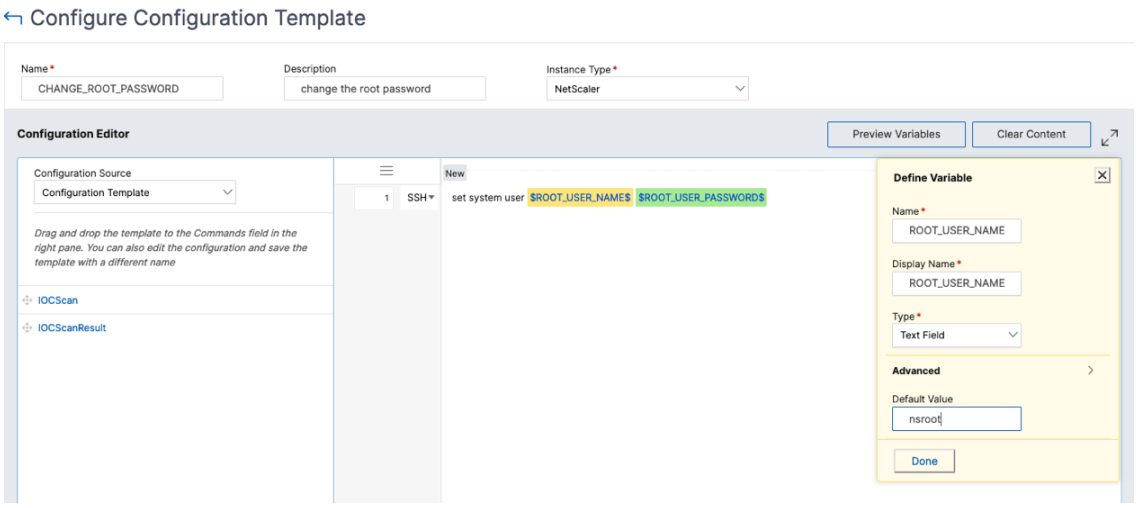
> Hinweis:
>
> Wenn die NetScaler Appliances auch von anderen Tools verwaltet werden, müssen Sie auch die Anmeldeinformationen für diese Tools ändern.

Erstellen einer Konfigurationsvorlage

1. Navigieren Sie in der NetScaler Console-GUI zu Infrastruktur > Konfigurationsaufträge > Konfigurationsvorlagen .**
2. Wählen Sie **Hinzufügen** aus. Erstellen Sie eine Konfigurationsvorlage mit, indem Sie den SSH-Befehl eingeben`set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$`.



3. Wählen Sie die Variable $ROOT_USER_NAME$ aus, und wählen Sie **Textfeld als Typ**aus.
4. Geben Sie optional den Standardwert für den Root-Benutzernamen an. Wählen Sie **Fertig**, um die Variableneinstellungen zu speichern.

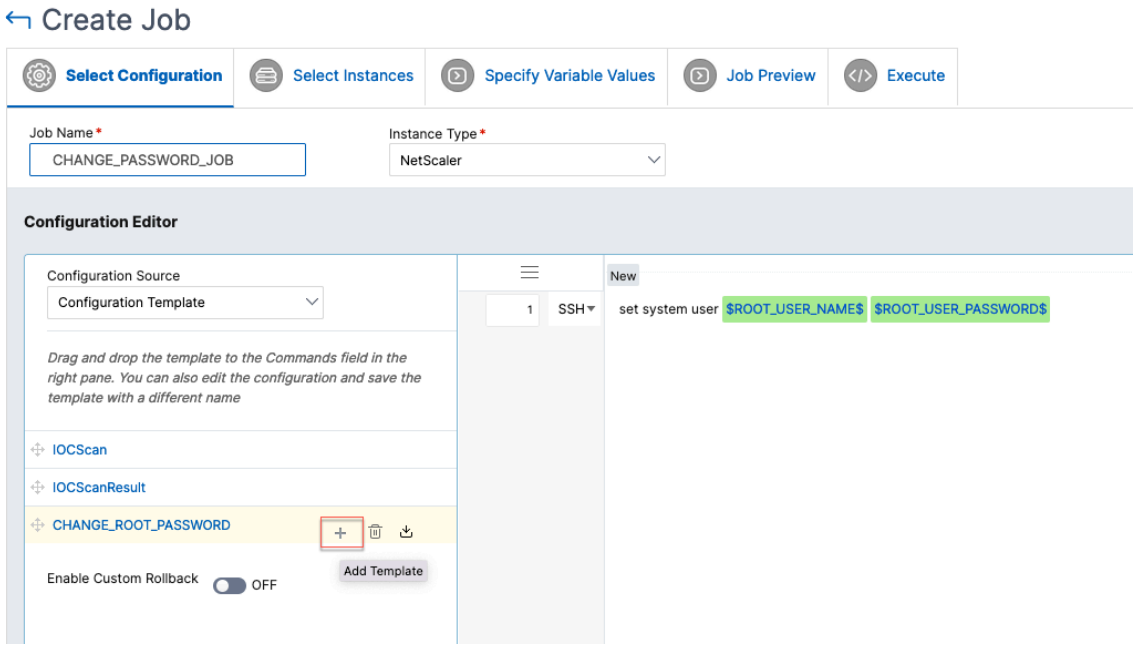


5. Wählen Sie die Variable $ROOT_USER_PASSWORD$ und wählen Sie **Kennwortfeld als Typ**aus. Wählen Sie **Fertig**, um die Variableneinstellungen zu speichern.
6. Wählen Sie **OK**, um die Konfigurationsvorlage zu speichern.

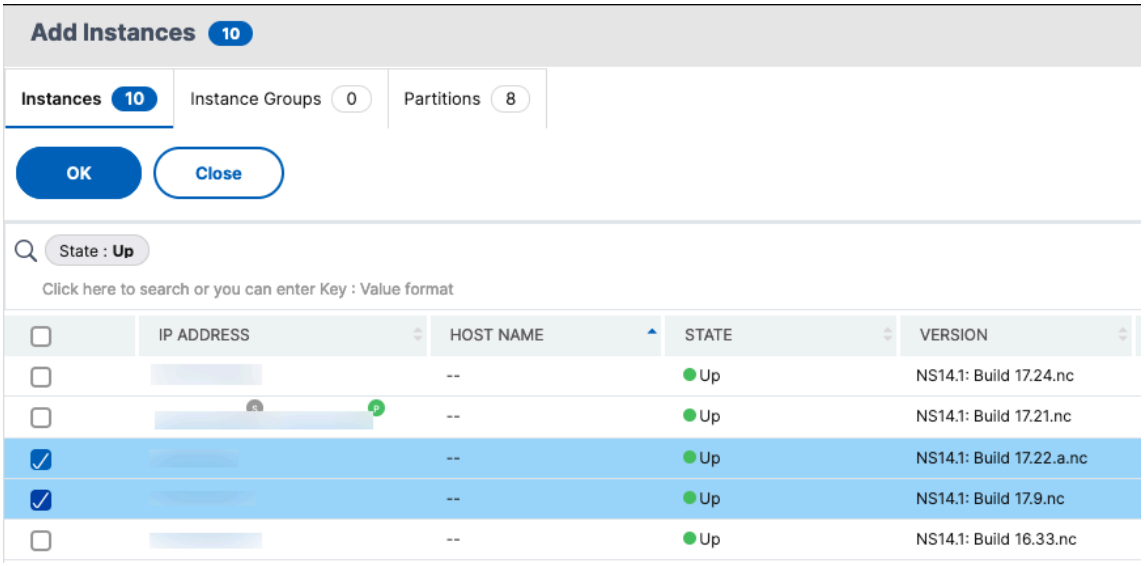
7. Die neue Konfigurationsvorlage wird unter **Konfigurationsvorlagen** angezeigt.

Erstellen eines Konfigurationsauftrags

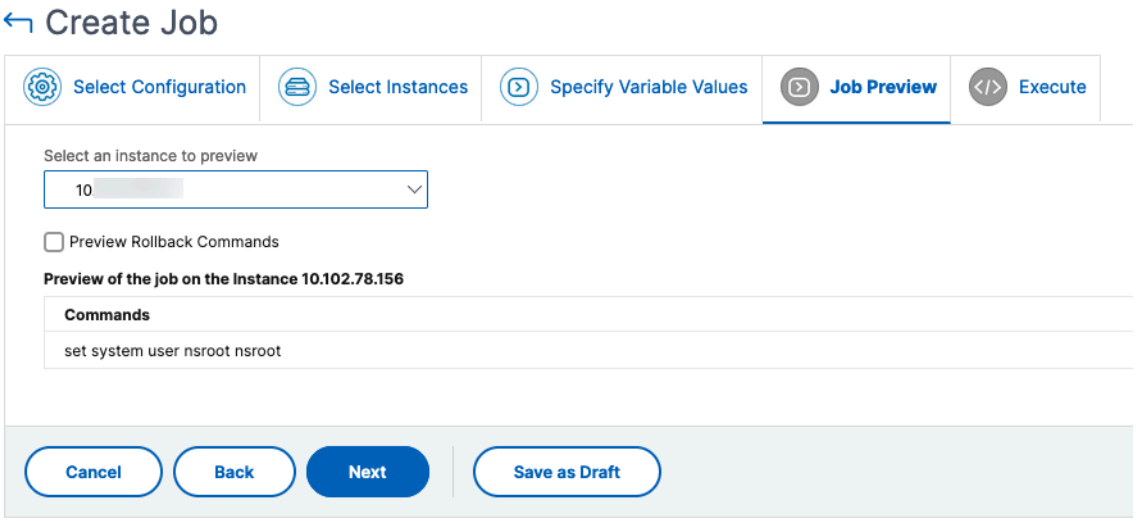
1. Navigieren Sie in der NetScaler Console-GUI zu Infrastruktur > Konfigurationsaufträge .**
2. Wählen Sie **Job erstellen** und klicken Sie auf das “+”-Symbol der neuen Konfigurationsvorlage. Wählen Sie **Weiter**.



3. Wählen Sie die NetScaler-Instanz oder die Instanzen aus, für die das Kennwort geändert werden muss.



4. Wählen Sie im Bereich **Instanzen auswählen** die Instanzen aus, und klicken Sie auf **Weiter**.
5. Geben Sie im Bereich **Variablenwerte angeben** Werte für den Benutzernamen und das Kennwort an und klicken Sie auf **Weiter**.
6. Überprüfen Sie unter **Job Preview** die tatsächlichen CLI-Befehle, die die NetScaler Console auf den NetScaler-Instanzen ausführen wird. Wenn die Vorschau gut aussieht, klicken Sie auf **Weiter**.

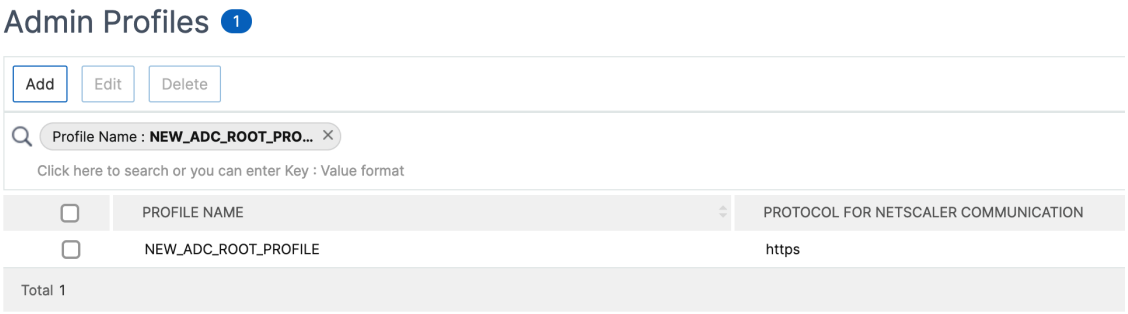


7. Im Bereich **Ausführen** haben Sie die Wahl, den Job sofort auszuführen oder ihn für einen späteren Zeitpunkt zu planen. Sie können den Job auch parallel auf allen ausgewählten Instanzen oder sequentiell ausführen. Wählen Sie Fertig stellen, nachdem Sie die Ausführungsdetails angegeben haben.
8. Konfigurationsauftrag zeigt an, ob die Ausführung erfolgreich war oder fehlgeschlagen ist.
9. Wählen Sie den **Auftrag** aus, und klicken Sie auf **Details**. Die Ausführungsdetails zeigen den Status auf der Ebene der einzelnen Instanzen.

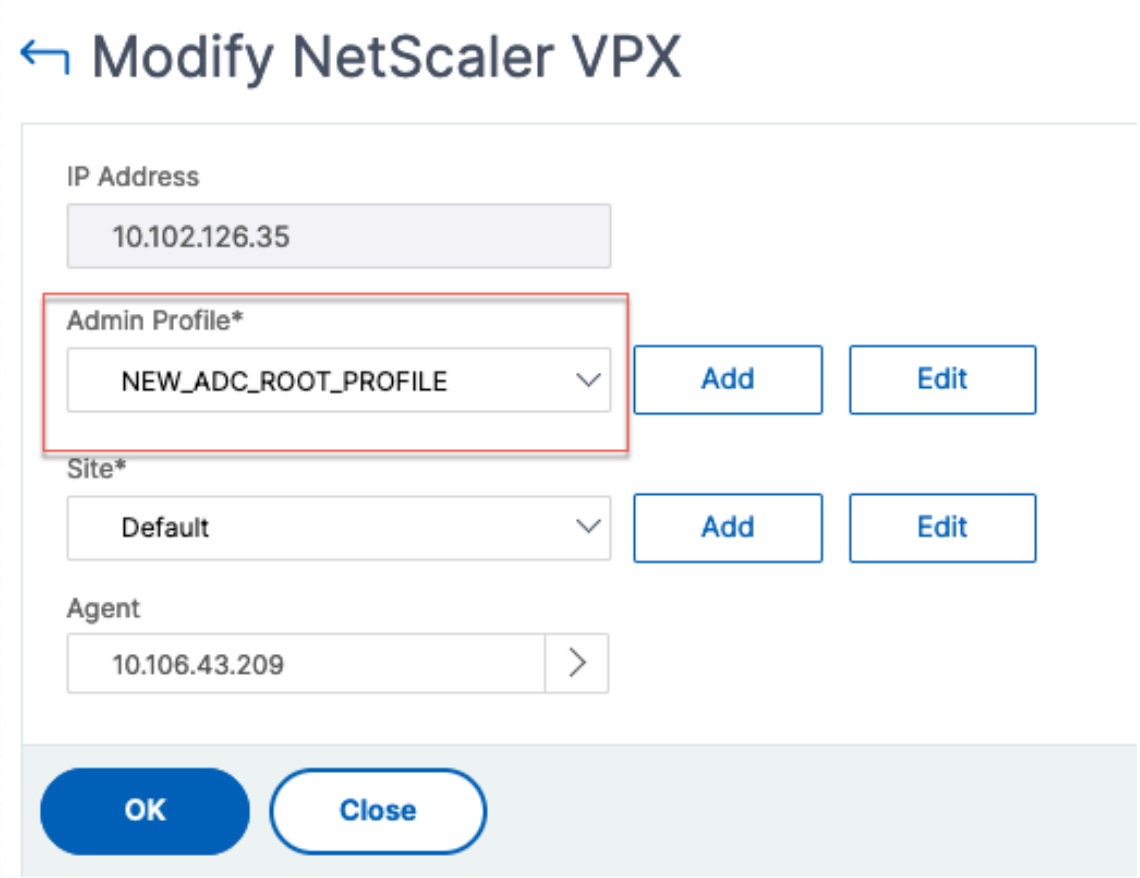
Das Admin-Profil ändern

Nachdem Sie die NetScaler-Kennwörter geändert haben, müssen Sie die Admin-Profile der Instanzen hinzufügen und ändern. Führen Sie die folgenden Schritte aus:

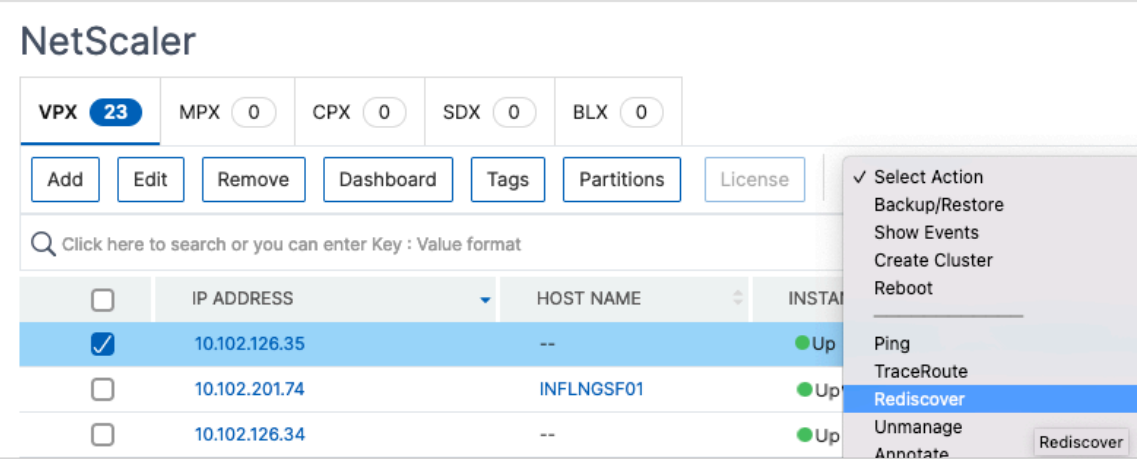
1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**.
2. Klicken Sie auf **Profile**, um alle Admin-Profile anzuzeigen.
3. Wählen Sie **Hinzufügen** aus, um ein Administratorprofil zu erstellen und neue NetScaler Anmeldeinformationen bereitzustellen.



4. Das neu erstellte Profil wird unter **Admin-Profile** angezeigt.
5. Gehen Sie zu **Netzwerk > Instanzen > NetScaler**. Wählen Sie die NetScaler-Instanz aus, für die das Kennwort geändert wurde, und wählen Sie **Bearbeiten**aus.
6. Wählen Sie den neu erstellten Profilnamen aus und klicken Sie auf **OK**.



7. Wählen Sie die Instanz erneut aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Wiedererkennen**aus.



Sie haben das Kennwort erfolgreich geändert.

Informationen zum Ändern des Kennworts einer SDX-Appliance finden Sie unter Ändern eines NetScaler SDX-Root-Kennworts.

So ändern Sie ein NetScaler SDX nsroot-Kennwort

January 26, 2024

Gelegentlich müssen Sie das nsroot-Kennwort der NetScaler Appliance aus Sicherheitsgründen oder der Einhaltung der Kennwortrotationsrichtlinie ändern.

In diesem Dokument werden die Schritte beschrieben, die erforderlich sind, um das nsroot-Kennwort einer NetScaler SDX-Appliance zu ändern, die über die NetScaler Console Cloud verwaltet wird.

Wenn Sie das NetScaler-Kennwort ändern, müssen Sie das NetScaler Console-Administratorprofil ändern, das dem NetScaler zugeordnet ist. Ein NetScaler Console-Administratorprofil verwaltet die NetScaler-Anmeldeinformationen für die REST-API-, SSH-, SCP- oder SNMP-basierte Kommunikation mit der NetScaler Appliance. Über Administratorprofile verwaltet NetScaler Console NetScaler SDX-Appliances.

Kennwort ändern

Folgen Sie diesen Schritten, um das Kennwort zu ändern:

- Schritt 1. Ändern Sie das SDX-Kennwort über die SDX Management Service-GUI.
- Schritt 2. Ändern Sie das NetScaler Console-Administratorprofil, das dem SDX zugeordnet ist.

> Hinweis:
>
> Wenn die SDX-Appliance auch von anderen Tools verwaltet wird, müssen Sie auch die Anmeldeinformationen für diese Tools ändern.

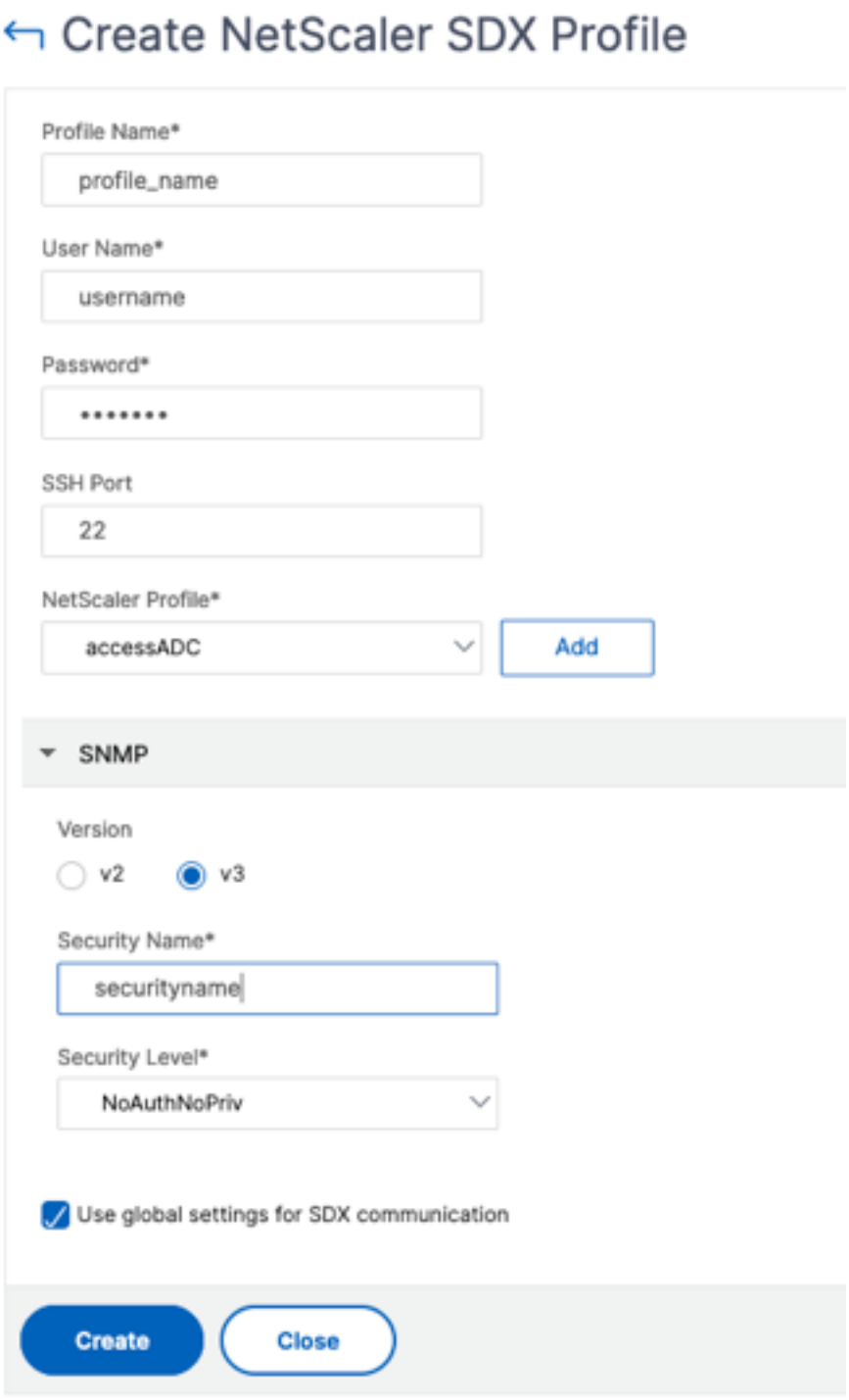
Ändern Sie das SDX-Kennwort über die SDX Management Service-GUI

1. Navigieren Sie im SDX Management Service zu **System > Benutzerverwaltung > Benutzer**.
2. Wählen Sie den Benutzernamen aus, für den Sie das Kennwort ändern möchten, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie **Kennwort ändern** aus.
4. Geben Sie ein neues Kennwort ein und klicken Sie auf **OK**.
5. Das SDX-Kennwort wurde geändert

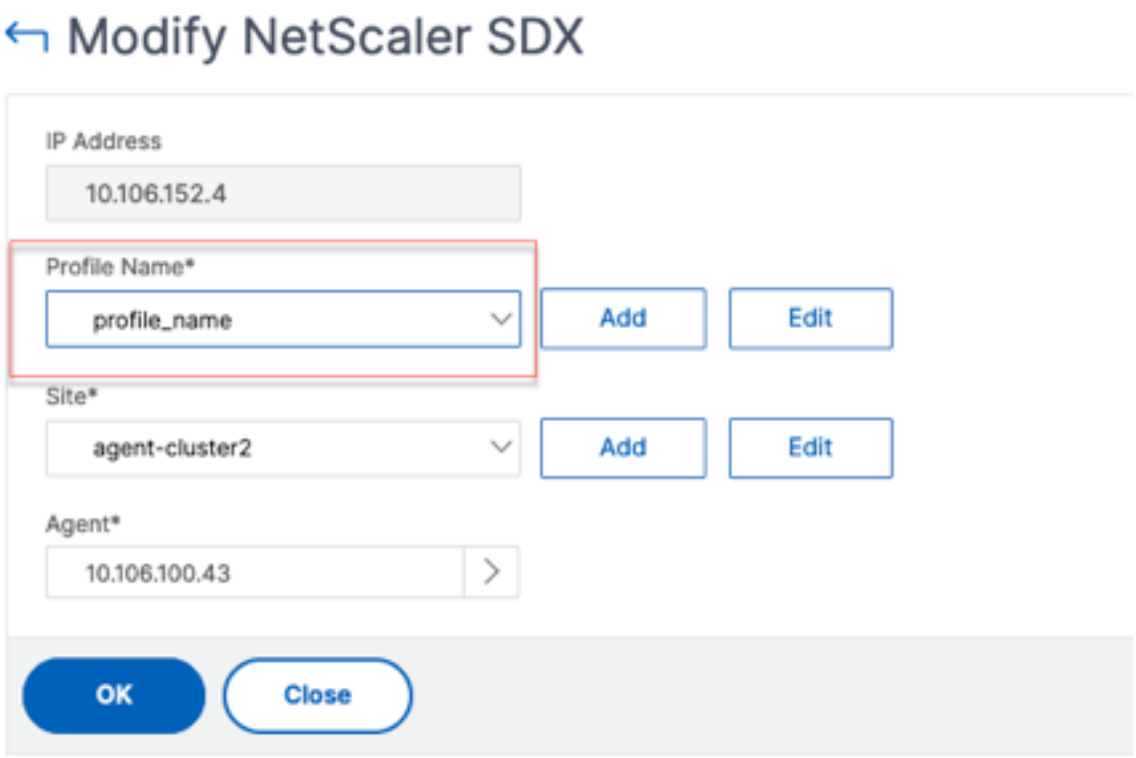
Ändern Sie das NetScaler Console-Administratorprofil

Nachdem Sie die SDX-Kennwörter geändert haben, müssen Sie die Admin-Profile der Instanzen ändern. Führen Sie die folgenden Schritte aus:

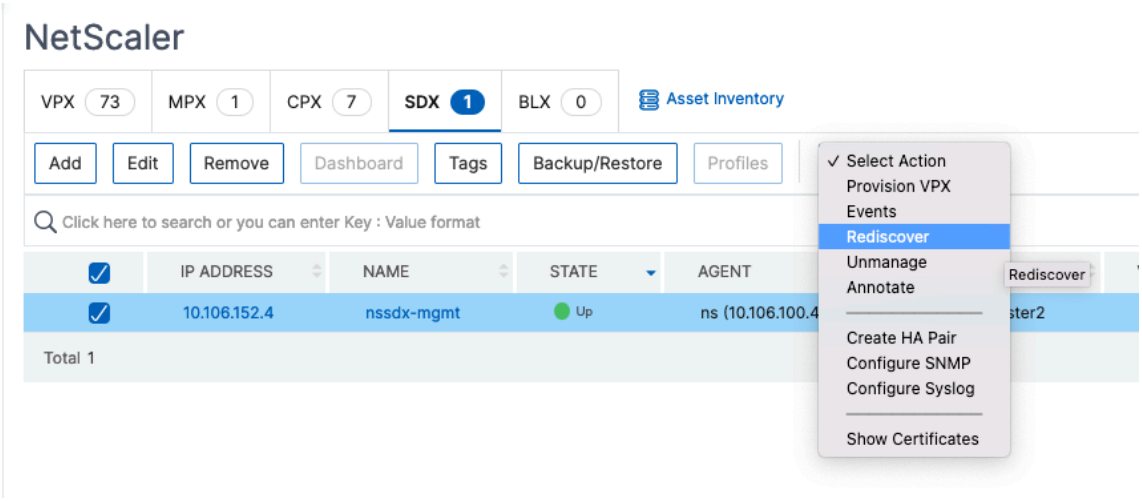
1. Navigieren Sie zu **Infrastruktur > Instanzen Dashboard > NetScaler > SDX**.
2. Wählen Sie **Profile** aus, um alle Admin-Profile anzuzeigen.
3. Wählen Sie **Hinzufügen** aus, um ein Administratorprofil zu erstellen.
4. Geben Sie neue NetScaler-Anmeldeinformationen ein und klicken Sie auf **Erstellen**.



5. Das neu erstellte Profil wird unter **Admin-Profile** angezeigt.
6. Gehen Sie zu **Netzwerk > Instanzen > NetScaler > SDX**. Wählen Sie die Instanz aus, für die das Kennwort geändert wurde, und wählen Sie dann **Bearbeiten**aus.
7. Wählen Sie den neu erstellten Profilnamen aus und klicken Sie auf **OK**.



8. Wählen Sie die Instanz erneut aus, klicken Sie mit der rechten Maustaste auf **Erneut**



Sie haben das Kennwort erfolgreich geändert.

Informationen zum Ändern des Kennworts einer SDX-Appliance finden Sie unter Ändern eines NetScaler MPX- oder VPX-Root-Kennworts.

So generieren Sie ein technisches Support-Paket für eine NetScaler-Instanz

January 26, 2024

Wenn Sie Hilfe bei der Analyse und Lösung von Problemen mit einer NetScaler-Instanz benötigen, können Sie ein Paket für den technischen Support auf der Instanz generieren und das Paket an den technischen Support von Citrix senden. Das Paket für den technischen Support ist ein komprimiertes TAR-Archiv mit Systemkonfigurationsdaten und Statistiken. Das Paket für den technischen Support sammelt die folgenden Daten von der NetScaler-Instanz, auf der Sie das Paket generieren:

- Konfigurationsdateien. Alle Dateien im Verzeichnis /flash/nsconfig.
- `newnslog` Akten. Die aktuell laufende `newnslog` und einige frühere Dateien. Um die Größe der Archivdatei zu minimieren, ist die Sammlung `newnslog` auf 500 MB, 6 Dateien oder 7 Tage beschränkt, je nachdem, was zuerst eintritt. Wenn ältere Daten benötigt werden, ist möglicherweise eine manuelle Erfassung erforderlich.
- Logdateien. Dateien in /var/log/messages, /var/log/ns.log und anderen Dateien unter /var/log und /var/nslog.
- Kerndateien der Anwendung. Dateien, die in der letzten Woche im Verzeichnis /var/core erstellt wurden, falls vorhanden.
- Ausgabe einiger CLI-Show-Befehle.
- Ausgabe einiger CLI-Statbefehle.
- Ausgabe von BSD-Shell-Befehlen.

Sie können das Paket für den technischen Support auch sicher auf den Server für den technischen Support von Citrix hochladen. Ab NetScaler 14.1 Version 8.x Build müssen Sie ein Authentifizierungstoken generieren, bevor Sie das Paket für den technischen Support hochladen. In den vorherigen Builds können Sie das Paket für den technischen Support mit dem Citrix-Benutzernamen und -Kennwort hochladen.

Um das Authentifizierungstoken zu generieren:

1. Starten Sie einen Browser und geben Sie die folgende URL ein: https://cis.citrix.com/auth/api/create_identity_v2/?expiration=3600.
2. Melden Sie sich mit Multifaktor-Authentifizierung an.

   > **Hinweis:**
   >
   > Informationen zur Registrierung für die Multifaktor-Authentifizierung finden Sie unter So registrieren Sie sich bei der Multifaktor-Authentifizierung(MFA).

3. Klicken Sie auf **Kopieren**, um das auf dem Bildschirm angezeigte Authentifizierungstoken zu

kopieren. Das Token ist 3600 Sekunden (1 Stunde) gültig. Die maximal zulässige Länge für das Token beträgt 1023 Zeichen.

Verwenden Sie nach dem Kopieren des Authentifizierungstokens die GUI, um die Datei hochzuladen.

So laden Sie das Paket für technischen Support über die GUI hoch:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**.
2. Wählen Sie eine NetScaler-Instanz aus.
3. Wählen Sie **unter**Aktionen auswählen**die Option Datei für den technischen Support generieren**aus.
4. Klicken Sie auf **Datei für den technischen Support erstellen**.
5. Verwenden Sie die Option **Scope**, um anzugeben, ob Sie Daten auf dem aktuellen Knoten, allen Clusterknoten oder für die angegebenen Partitionen sammeln möchten.
6. Wählen Sie **Collector-Archiv hochladen**aus.
7. Geben Sie im Abschnitt **Mein Citrix-Konto** das Authentifizierungstoken in das Feld **Citrix Authentication Token** ein.
8. Klicken Sie auf **Technischen Support erstellen**.

Ereignisse

January 26, 2024

Wenn die IP-Adresse einer Citrix Application Delivery Controller (NetScaler) -Instanz zur NetScaler Console hinzugefügt wird, sendet NetScaler Console einen NITRO-Aufruf und fügt sich implizit selbst als Trap-Ziel hinzu, damit die Instanz ihre Traps oder Ereignisse empfangen kann.

Ereignisse stellen Ereignisse oder Fehler in einer verwalteten NetScaler-Instanz dar. Wenn beispielsweise ein Systemausfall oder eine Änderung der Konfiguration auftritt, wird ein Ereignis generiert und auf dem NetScaler Console-Server aufgezeichnet. In NetScaler Console empfangene Ereignisse werden auf der Seite „Ereignisübersicht“(**Infrastruktur > Ereignisse**) angezeigt, und alle aktiven Ereignisse werden auf der Seite „ Ereignismeldungen“(Infrastruktur > Ereignisse > Ereignismeldungen) angezeigt.**

NetScaler Console überprüft auch die auf Instanzen generierten Ereignisse, um Alarme mit unterschiedlichem Schweregrad auszulösen, und zeigt sie als Meldungen an, von denen einige möglicherweise sofortige Aufmerksamkeit erfordern. Beispielsweise kann ein Systemausfall als Schweregrad des “kritischen”Ereignisses eingestuft und sofort behoben werden.

Sie können Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Regeln erleichtern die Überwachung verschiedener Ereignisse, die in Ihrer 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 für ein bestimmtes Zeitintervall für ein Ereignis mehrere Benachrichtigungen ausgelöst werden, bis das Ereignis gelöscht wird. Als zusätzliche Maßnahme möchten Sie Ihre E-Mail möglicherweise mit einer bestimmten Betreffzeile, einer Benutzernachricht und einer Anfügung anpassen.

Ereignisdashboard verwenden

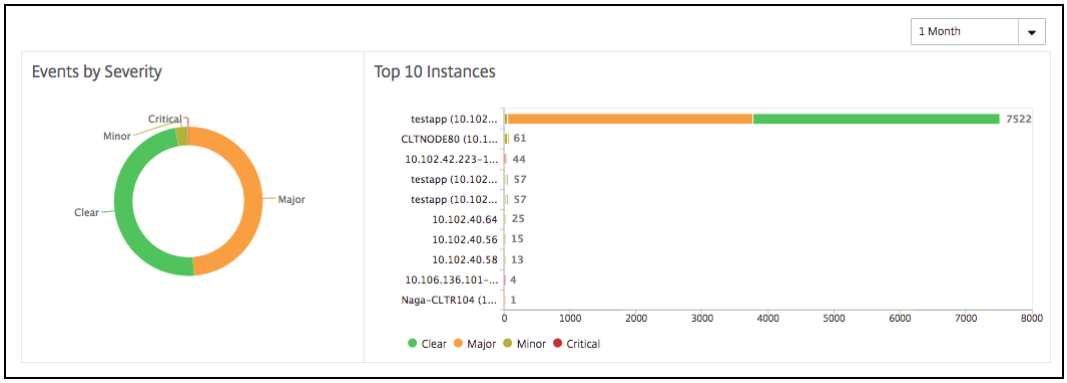
March 12, 2024

Als Netzwerkadministrator können Sie Details wie Konfigurationsänderungen, Anmeldebedingungen, Hardwarefehler, Schwellenwertverletzungen und Änderungen des Entitätsstatus auf Ihren Citrix Application Delivery Controller (NetScaler) -Instanzen sowie Ereignisse und deren Schweregrad für bestimmte Instanzen anzeigen. Sie können das Event-Dashboard der NetScaler Console verwenden, um Berichte anzuzeigen, die für Details zum Schweregrad kritischer Ereignisse für alle Ihre NetScaler-Instanzen generiert wurden.

So zeigen Sie die Details im Ereignis-Dashboard an:

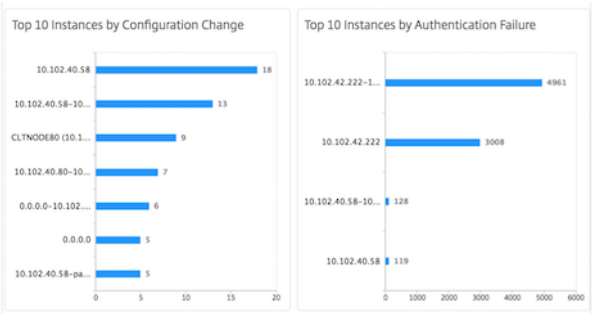
Navigieren Sie zu **Infrastruktur > Ereignisse > Berichte**.

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.

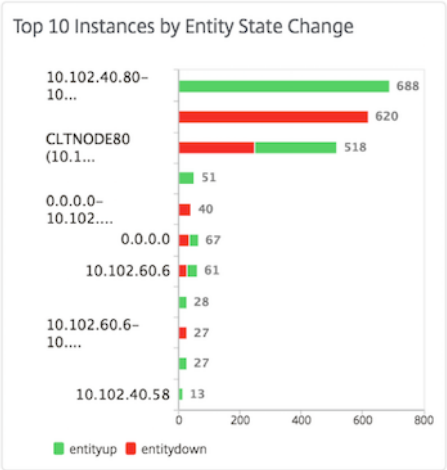


Sie können weitere Details anzeigen, indem Sie zum NetScaler-Instanztyp navigieren (**Infrastruktur > Ereignisse > Berichte** > **NetScaler/ NetScaler SDX/ NetScaler**), um Folgendes anzuzeigen:

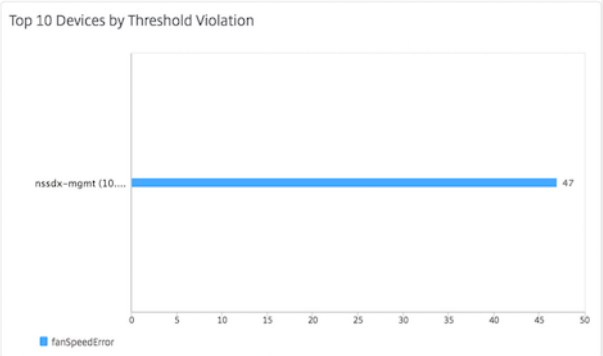
- Top 10 Geräte nach Hardwarefehler
- Top 10 Geräte nach Konfigurationsänderung
- Top 10 Geräte durch Authentifizierungsfehler



- Top 10 Geräte nach Entitätsstatusänderungen



- Top 10 Geräte nach Schwellenverletzung



So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** . Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis:**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Ereignisregeln erstellen

May 9, 2024

Sie können Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Regeln erleichtern das Filtern der Ereignisse, 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.

Sie können Filter für die folgenden Bedingungen erstellen:

- Schweregrad
- Instanzen von Citrix Application Delivery Controller (NetScaler)
- Kategorie
- Fehlerobjekte
- Konfigurationsbefehle
- Nachrichten

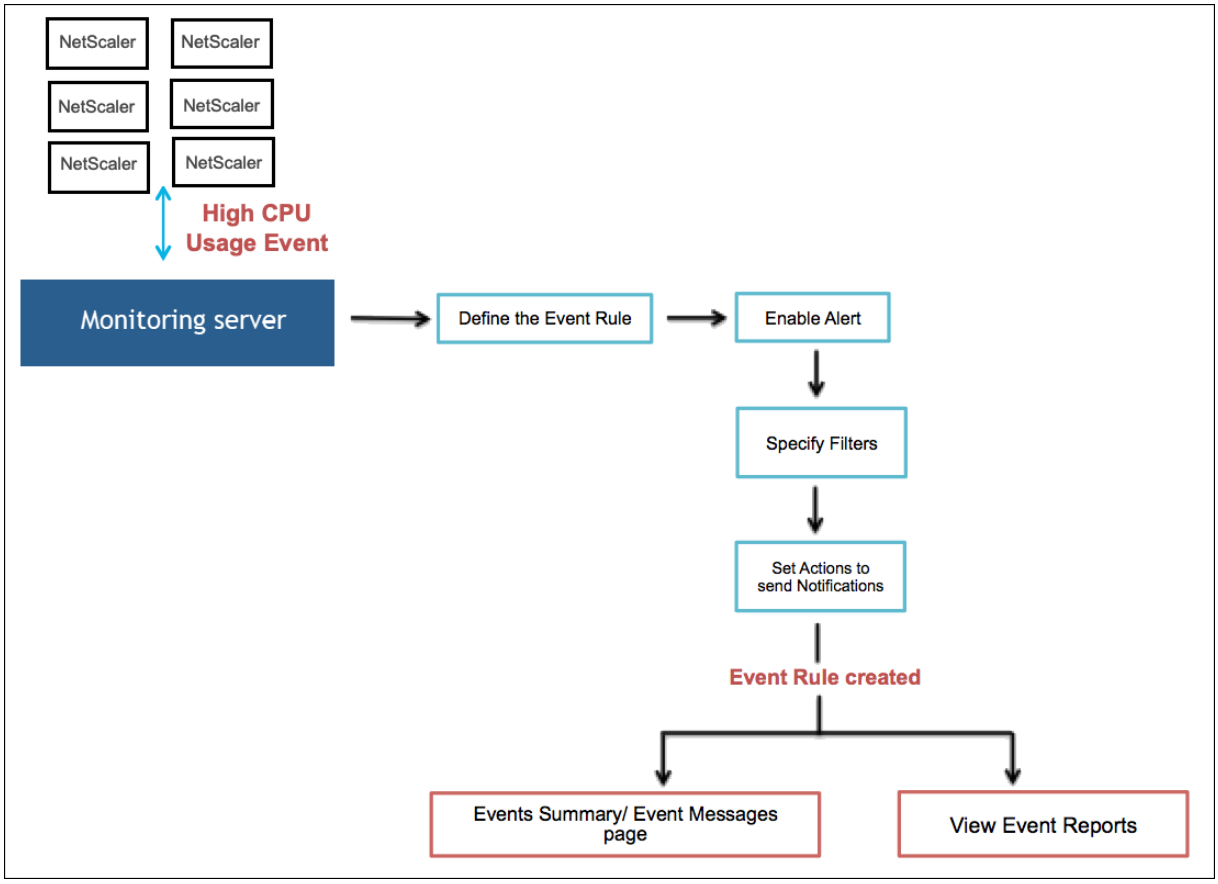
Nachdem Sie Ereignisse erstellt haben, können Sie den Ereignissen Aktionen zuweisen. Weitere Informationen finden Sie unter Aktionen für Ereignisregeln hinzufügen.

Als Administrator möchten Sie beispielsweise Ereignisse mit „hoher CPU-Auslastung“auf NetScaler-Instanzen überwachen, die zu einem Ausfall führen können. Sie können eine der folgenden Aktionen ausführen, um Benachrichtigungen zu erhalten:

- Erstellen Sie eine Regel zur Überwachung von Instanzen und fügen Sie der Regel eine Aktion hinzu, um Benachrichtigungen zu erhalten, wenn solche Ereignisse eintreten.

- Planen Sie eine Regel zur Überwachung von Instanzen in einem bestimmten Intervall. Sie erhalten also Benachrichtigungen, wenn solche Ereignisse innerhalb dieses Intervalls auftreten.

In der folgenden Abbildung wird der Arbeitsablauf zur Funktionsweise von Regeln für Ereignisse erläutert.



Ereignisregel konfigurieren

Um eine Ereignisregel zu konfigurieren, navigieren Sie zu **Infrastruktur > Ereignisse > Regeln** und klicken Sie auf **Hinzufügen**. Führen Sie #auf der Seite **Regel erstellen** die folgenden Aufgaben aus:

1. Namen und Instanzfamilie angeben
2. Ereignisalter konfigurieren
3. Schweregrad des Ereignisses auswählen, das die Regel erkennt
4. Kategorie des Ereignisses angeben
5. NetScaler-Instanzen angeben, für die die Regel gilt
6. Fehlerobjekte auswählen
7. Erweiterte Filter angeben

8. Aktionen angeben, die ausgeführt werden sollen, wenn die Regel ein Ereignis erkennt

Schritt 1 - Namen und Instanzfamilie angeben

1. **Name**. Geben Sie einen Namen für die Ereignisregel ein.
2. **Instanzfamilie**. Wählen Sie in der Dropdownliste **Instanzfamilie** eine Instanzfamilie aus.

   Sie können die Ereignisregeln nach **Instanzfamilie** filtern, um die NetScaler-Instanz zu verfolgen, von der NetScaler Console ein Ereignis empfängt.

Schritt 2 - Ereignisalter konfigurieren

1. **Ereignisalter**. Geben Sie das Zeitintervall (in Sekunden) an, nach dem NetScaler Console eine Ereignisregel aktualisiert.

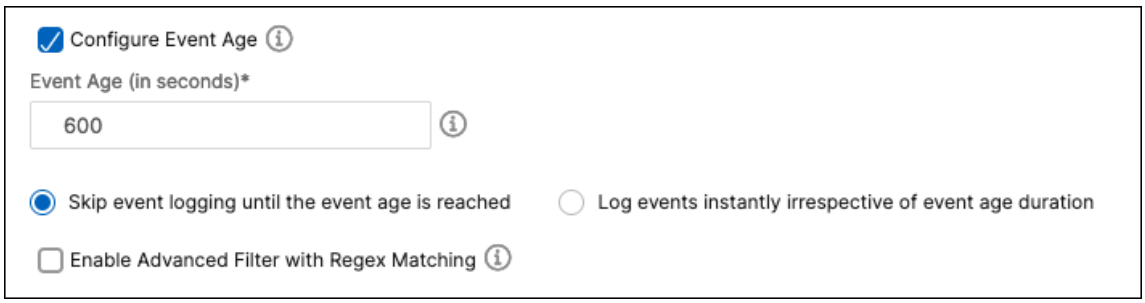
   Sie möchten beispielsweise, dass jedes Mal, wenn Ihre NetScaler-Instanz 60 Sekunden oder länger ein Ereignis mit “hoher CPU-Auslastung”erlebt, eine E-Mail gesendet wird. Sie können das Ereignisalter auf 60 Sekunden festlegen. Sie erhalten immer dann eine E-Mail-Benachrichtigung, wenn Ihre NetScaler-Instanz 60 Sekunden oder länger ein Ereignis mit “hoher CPU-Auslastung”auslöst.

   > **Hinweis:**
   >
   > Das **Ereignisalter** ist ein Pflichtfeld. Der Mindestwert für das Ereignisalter ist 60 Sekunden. Wenn Sie das Feld **Ereignisalter** leer lassen, wird die Ereignisregel unmittelbar nach dem Eintreten des Ereignisses angewendet.

2. Wählen Sie eine der folgenden Optionen, um Ihre Ereignisse zu verfolgen:

   - **Überspringen Sie die Protokollierung von Ereignissen, bis das Ereignisalter erreicht ist**. Ereignisse, die vor dem angegebenen Ereignisalter auftreten, werden nicht in der NetScaler Console-Serverdatenbank protokolliert. Wenn das Ereignisalter erreicht ist, werden Ereignisse in der Datenbank protokolliert und konfigurierte Ereignisaktionen werden ausgelöst.

- **Protokollieren Sie Ereignisse sofort, unabhängig vom Ereignisalter**. Alle Ereignisse werden unabhängig vom angegebenen Ereignisalter in der NetScaler Console-Serverdatenbank protokolliert. Nachdem das Ereignisalter erreicht ist, werden konfigurierte Ereignisaktionen ausgelöst.



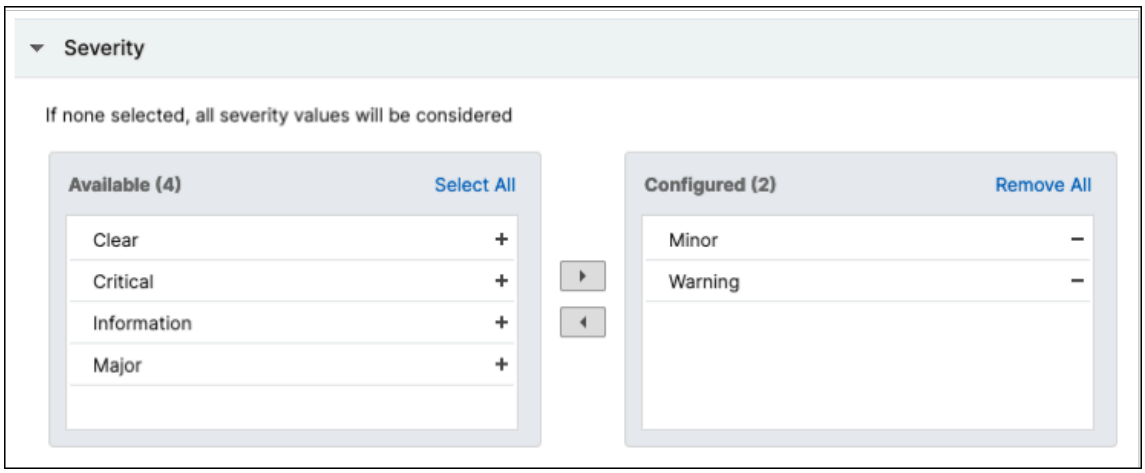
3. **Aktivieren Sie den erweiterten Filter mit Regex-Abgleich**. Wählen Sie diese Option, um einen anderen regulären Ausdruck als den Musterabgleich mit Sternchen (*) einzubeziehen. Diese Option gilt für Fehlerobjekte, Konfigurationsbefehle und Meldungen.

Schritt 3 – Schweregrad des Ereignisses auswählen

- Wählen Sie im Abschnitt **Schweregrad** einen Schweregrad für Ihre Ereignisregel aus.

  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 der NetScaler Console 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**.

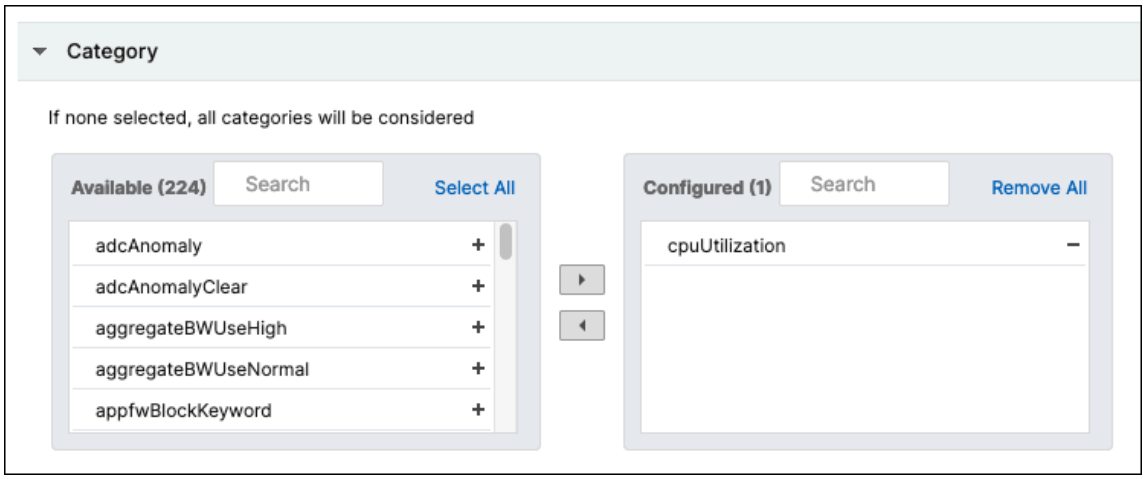


Schritt 4 – Ereigniskategorie angeben

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 der NetScaler Console zugeordnet, die 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**.

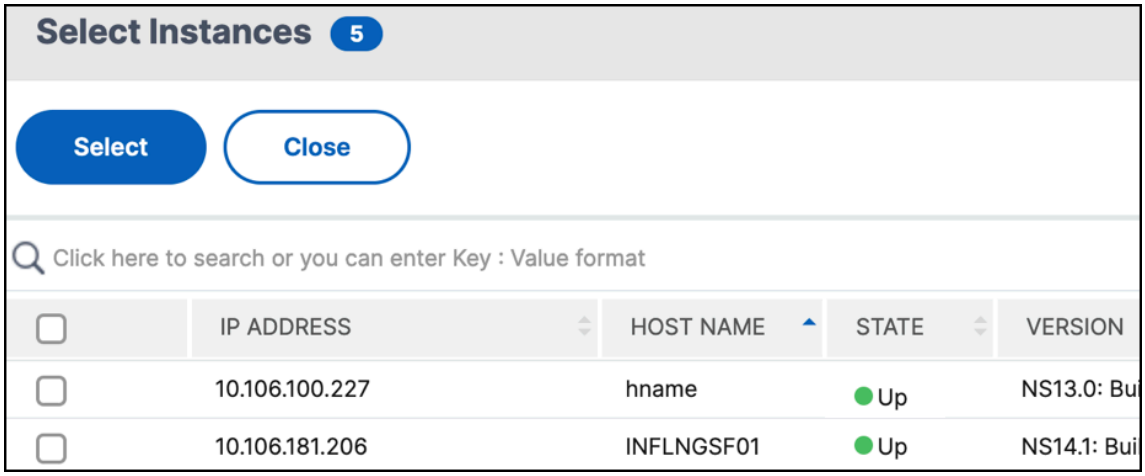
  Im Beispiel müssen Sie “cpuUtilization”als Ereigniskategorie aus der angezeigten Tabelle auswählen.



Schritt 5 - Angeben von NetScaler-Instanzen

Gehen Sie im Abschnitt **Instanzen** wie folgt vor:

1. Klicken Sie auf **Instanz auswählen**. Wählen Sie auf der Seite **Instanzen auswählen** die IP-Adressen der NetScaler-Instanzen aus, für die Sie die Ereignisregel definieren möchten.
2. Klicken Sie auf **Auswählen**.



Schritt 6 - Auswählen von Fehlerobjekten

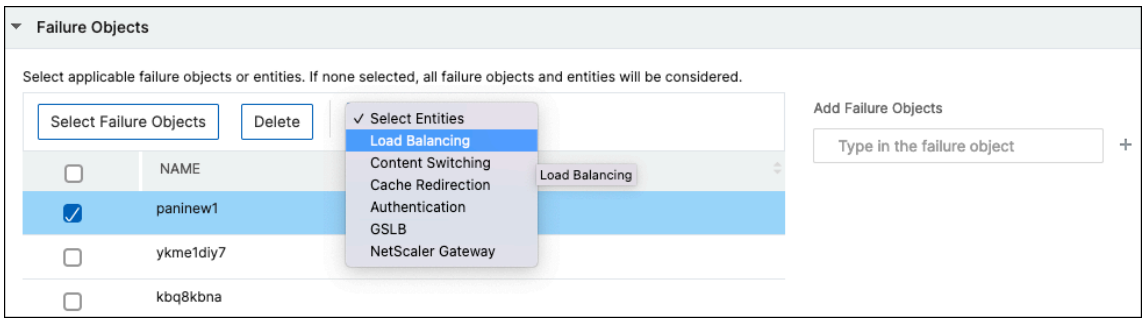
Fehlerobjekte sind Entitätsinstanzen oder Leistungsindikatoren, für die ein Ereignis generiert wurde.

1. Klicken Sie auf **Fehlerobjekte auswählen**.
2. Wählen Sie auf der Seite **Fehlerobjekte** ein Fehlerobjekt aus der Liste aus. Klicken Sie auf **Auswählen**.
3. Um ein Fehlerobjekt hinzuzufügen, geben Sie im Feld **Fehlerobjekte hinzufügen** einen regulären Ausdruck ein. Abhängig vom angegebenen regulären Ausdruck werden die Fehlerobjekte automatisch zur Liste hinzugefügt.

   > **Wichtig:**
   >
   > Um Fehlerobjekte mithilfe regulärer Ausdrücke aufzulisten, wählen Sie in Schritt 1 die Option **Erweiterten Filter mit Regex-Matching aktivieren** aus.

   Der erweiterte Filter ermöglicht es Ihnen, Probleme mit den Fehlerobjekten schnell zu verfolgen und die Ursache für ein Problem zu identifizieren. Wenn ein Benutzer beispielsweise Probleme mit der Anmeldung hat, ist das Fehlerobjekt der Benutzername oder das Kennwort, z. B. `nsroot`.
4. Um Entitäten hinzuzufügen, wählen Sie eine Entität aus **Entitäten auswählen** aus.

   Diese Liste kann Zählernamen für alle schwellenwertbezogenen Ereignisse, Entitätsnamen für alle entitätsbezogenen Ereignisse, Zertifikatsnamen für zertifikatsbezogene Ereignisse usw. enthalten.

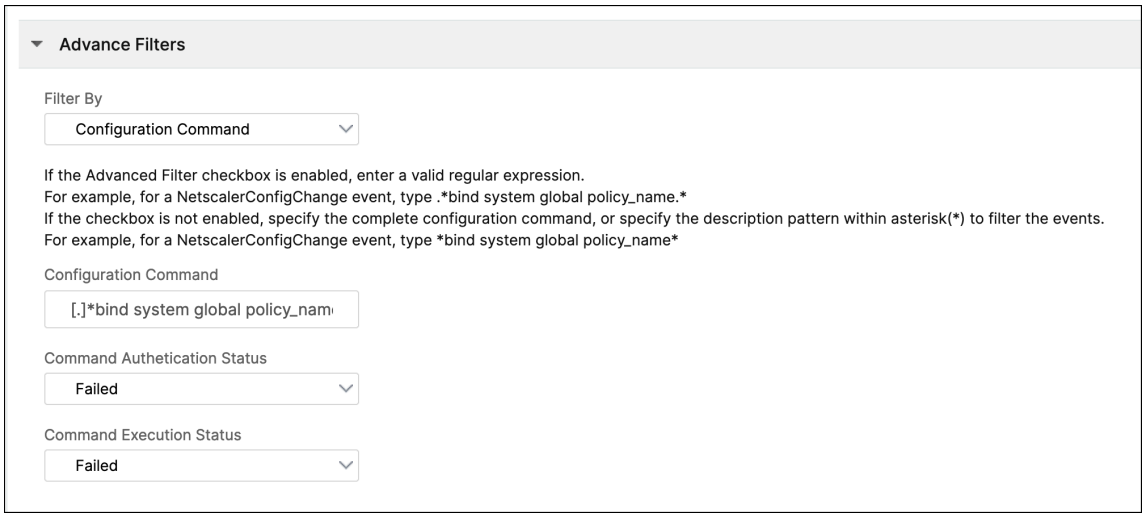


Schritt 7 - Erweiterte Filter angeben

Sie können eine Ereignisregel mit erweiterten Filtern weiter filtern. Wählen Sie einen der folgenden Filter aus:

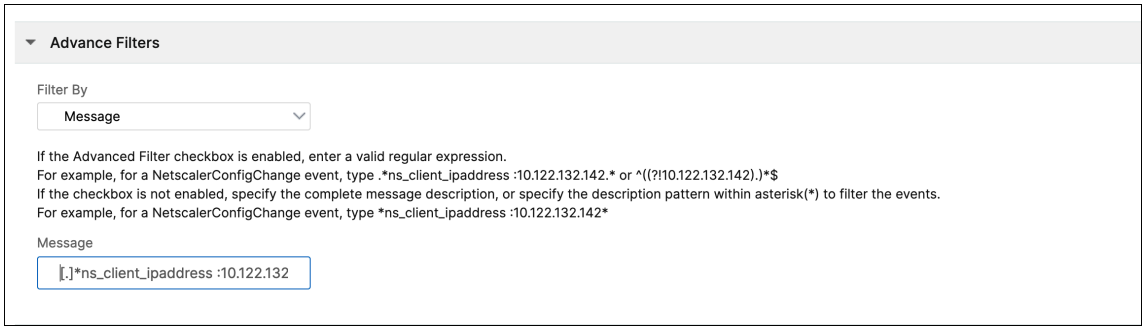
- **Konfigurationsbefehle**: Geben Sie den vollständigen Konfigurationsbefehl oder einen regulären Ausdruck an, um Ereignisse zu filtern.

  Sie können die Ereignisregeln auch nach dem Authentifizierungsstatus und dem Ausführungsstatus des Befehls filtern. Geben Sie beispielsweise für ein `NetscalerConfigChange event` die Regel `[.]*bind system global policy_name[.]*` ein.



- **Nachrichten**: Geben Sie die vollständige Nachrichtenbeschreibung oder einen regulären Ausdruck an, um die Ereignisse zu filtern.

  Geben Sie beispielsweise für ein Ereignis `NetscalerConfigChange` den Ausdruck `[.]* ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)` ein.



> **Wichtig:**
>
> Um Konfigurationsbefehle und Meldungen mit anderen regulären Ausdrücken als dem Musterabgleich mit Sternchen (*) zu filtern, wählen Sie in Schritt 1 die Option **Erweiterten Filter mit Regex-Matching aktivieren** aus.

Schritt 8 – Aktionen für Ereignisregeln hinzufügen

Sie können Ereignisregelaktionen hinzufügen, um Benachrichtigungsaktionen für ein Ereignis zuzuweisen. Diese Benachrichtigungen werden gesendet oder ausgeführt, wenn ein Ereignis die definierten Filterkriterien erfüllt, die Sie in Schritt 7 festgelegt haben.

1. Klicken Sie auf **Aktion hinzufügen**.
2. Auf der Seite **Ereignisaktion hinzufügen** können Sie 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

E-Mail senden Action

Wenn Sie **E-Mail-Aktion senden**wählen, wird eine E-Mail ausgelöst, wenn die Ereignisse die definierten Filterkriterien erfüllen.

1. **E-Mail-Verteilerliste**. Wählen Sie eine E-Mail-Verteilerliste aus. Um eine Verteilerliste hinzuzufügen, klicken Sie auf Hinzufügen.

    a) Gehen Sie auf der Seite **E-Mail-Verteilerliste erstellen** wie folgt vor:

        i. **Name**. Fügen Sie einen Namen für die Verteilerliste hinzu.

        ii. **E-Mail-Server**. Wählen Sie einen E-Mail-Server aus. Sie können auch einen Server hinzufügen oder einen vorhandenen bearbeiten.

        iii. **Von**. Fügen Sie die E-Mail-Adresse des Absenders hinzu.

        iv. **An**. Fügen Sie die E-Mail-Adressen der Empfänger hinzu. Sie können auch die E-Mail-Adressen angeben, die in die CC- und Bcc-Liste aufgenommen werden sollen.

        v. Klicken Sie auf **Erstellen**.

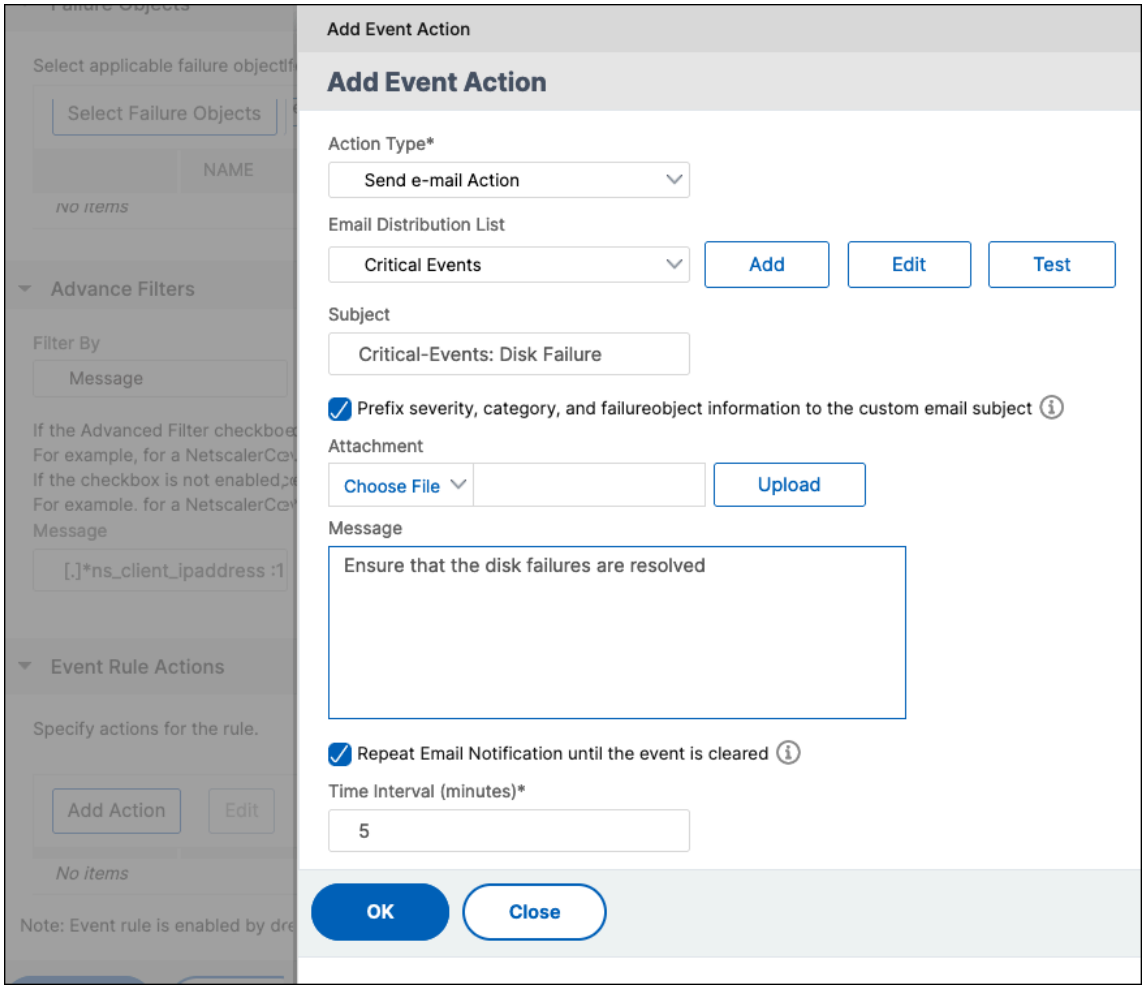
2. **Betreff**:1 Fügen Sie eine Betreffzeile für Ihre E-Mails hinzu, z. B. den Namen der betroffenen Entität, d. h. den Namen des Fehlerobjekts. Diese Betreffzeile enthält Informationen über den virtuellen Server, auf dem diese Ereignisse auftreten.

    > **Hinweis:**
    >
    > Wenn Sie keine Betreffzeile hinzufügen, wird eine Standard-Betreffzeile angezeigt. Die Standard-Betreffzeile enthält nur Informationen über den Schweregrad des Ereignisses, die Kategorie des Ereignisses und das Fehlerobjekt. Der Name des virtuellen Servers, auf dem das Ereignis aufgetreten ist, ist nicht verfügbar.

3. **Anlage**. Laden Sie eine Anlage zu Ihrer E-Mail hoch. Diese Anlage wird gesendet, wenn ein eingehendes Ereignis der konfigurierten Regel entspricht.

4. **Testen**. Klicken Sie auf diese Schaltfläche, um eine Test-E-Mail zu senden, nachdem Sie einen E-Mail-Server, zugehörige Verteilerlisten und andere Einstellungen konfiguriert haben. Mit dieser Option können Sie die konfigurierten Einstellungen testen.

5. **Wiederholen Sie die E-Mail-Benachrichtigung, bis das Ereignis abgeschlossen ist**. Wählen Sie diese Option, um sicherzustellen, dass E-Mail-Benachrichtigungen bei kritischen Ereignissen nicht verpasst werden. Diese Option sendet wiederholt E-Mails für Ereignisregeln, die die von Ihnen ausgewählten Kriterien erfüllen. Sie haben beispielsweise eine Ereignisregel für Instanzen erstellt, bei denen es zu Datenträgerausfällen kommt. Wenn Sie benachrichtigt werden möchten, bis das Problem behoben ist, können Sie sich dafür entscheiden, wiederholt E-Mail-Benachrichtigungen über diese Ereignisse zu erhalten.



6. Klicken Sie auf **OK**.

> **Hinweis:**
>
> Sie können die E-Mail-Verteilerlisten auch hinzufügen, indem Sie zu **Einstellungen** > **Benachrichtigungen** > **E-Mail** navigieren. Klicken Sie auf **Hinzufügen** und erstellen Sie die Liste.

Trap-Aktion senden

Wenn Sie den Ereignistyp **Trap-Aktion senden** auswählen, werden SNMP-Traps an ein externes Trap-Ziel gesendet oder weitergeleitet. Die Trap-Nachrichten werden an den spezifischen Trap-Listener gesendet, wenn Ereignisse die definierten Filterkriterien erfüllen.

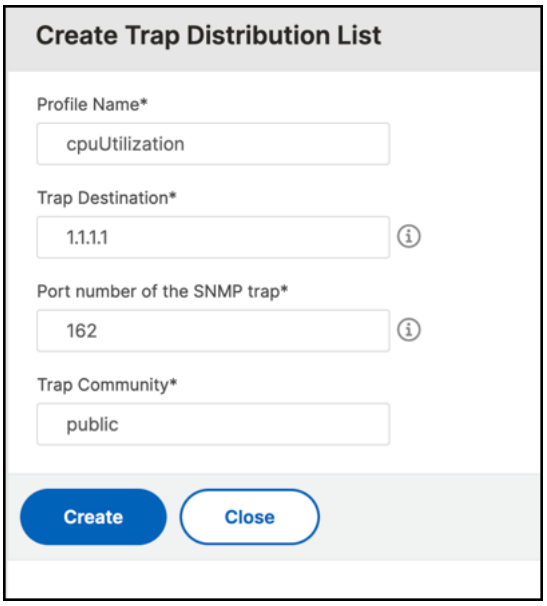
1. **Trap-Verteilerliste**. Wählen Sie eine Trap-Verteilerliste (oder ein Trap-Ziel und Trap-Profildetails) aus. Um eine Trap-Verteilerliste zu erstellen, klicken Sie auf **Hinzufügen**.
2. Gehen Sie auf der Seite **Trap-Verteilerliste erstellen** wie folgt vor:

a) **Profilname**. Geben Sie den Profilnamen ein.

b) **Trap-Ziel**. Geben Sie den Namen oder die IP-Adresse der Instanz ein, die die Trap-Nachrichten empfangen soll.

c) **Portnummer des SNMP-Traps**. Geben Sie die Portnummer ein.

d) **Trap-Gemeinschaft**. Geben Sie die Gruppe ein, zu der die Instanz gehört.



e) Klicken Sie auf **Erstellen**.

3. Klicken Sie auf **OK**.

Befehls-Aktion ausführen

Wenn Sie die Ereignisaktion „Befehlsaktion ausführen“wählen, können Sie einen Befehl oder ein Skript erstellen, das in der NetScaler Console für Ereignisse ausgeführt werden kann, die einem bestimmten Filterkriterium entsprechen.

Sie können auch die folgenden Parameter für das Skript **Befehlsaktion ausführen** festlegen:

Parameter	Beschreibung
$source	Dieser Parameter entspricht der Quell-IP-Adresse des empfangenen Ereignisses.
$category	Dieser Parameter entspricht der Art der Traps, die in der Kategorie des Filters definiert sind

$entity	Dieser Parameter entspricht den Entitätsinstanzen oder Leistungsindikatoren, für die ein Ereignis generiert wurde. 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 beeinflusst die Art und Weise, wie ein Ereignis verarbeitet wird, und stellt sicher, dass das Fehlerobjekt genau das Problem anzeigt, das gemeldet wurde. 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 **Nicht verfügbar** ist. Als Administrator möchten Sie möglicherweise eine schnelle Problemumgehung bereitstellen, indem Sie einen weiteren virtuellen Server hinzufügen. In NetScaler Console können Sie:

- Schreiben Sie eine Skriptdatei (.sh).

  Im Folgenden finden Sie eine Beispielskriptdatei (.sh):

```
#!/bin/sh
source=$1
failureobj=$2
payload='{
"params":{
"warning":"YES" }
,"lbvserver":{
"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","
   port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"
   PASSIVE","appflowlog":"ENABLED","
```



```
bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
 }
'
url="http://$source/nitro/v1/config/lbvserver"
curl --insecure -basic -u nsroot:nsroot -H "Content-type:
   application/json" -X POST -d $payload $url
```

- Speichern Sie die SH-Datei an einem beliebigen dauerhaften Ort auf dem Agent. Beispiel: `/var`.
- Geben Sie den Speicherort der SH-Datei in der NetScaler Console an, die ausgeführt werden soll, wenn die Regelkriterien erfüllt sind.

1. Klicken Sie in der **Befehlsausführungsliste** auf **Hinzufügen**.

   Die Seite “Befehlsverteilerliste erstellen”wird angezeigt.

   a) **Profilname**. Geben Sie einen Namen Ihrer Wahl an.

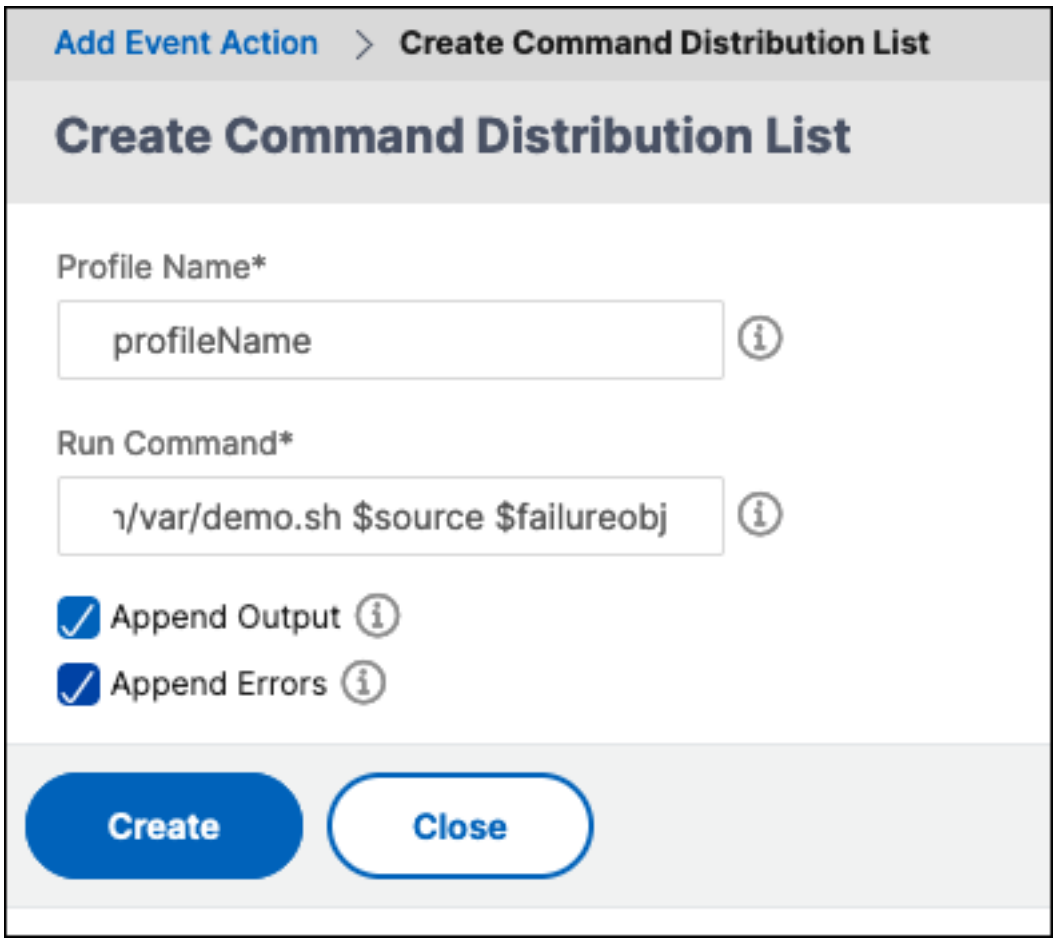
   b) **Befehl ausführen**. Geben Sie den Agentstandort an, an dem das Skript ausgeführt werden muss. Beispiel: `sh/var/demo.sh $source $failureobj`.

   c) Wählen Sie **Ausgabe anhängen** und **Fehler anhängen**.

   > **Hinweis:**
   >
   > Sie können die Optionen Ausgabe **anhängen** und **Fehler anhängen** aktivieren, wenn Sie die Ausgabe und die Fehler (falls vorhanden), die generiert werden, wenn Sie ein Befehlsskript ausführen, in den NetScaler Console-Serverprotokolldateien speichern möchten. Wenn Sie diese Optionen nicht aktivieren, verwirft NetScaler Console alle Ausgaben und Fehler, die bei der Ausführung des Befehlsskripts generiert wurden.

   d) Klicken Sie auf **Erstellen**.

2. Klicken Sie auf der Seite **Ereignisaktion hinzufügen** auf **OK**.



> **Hinweis:**
>
> Sie können die Optionen Ausgabe **anhängen** und **Fehler anhängen** aktivieren, wenn Sie die Ausgabe und die Fehler (falls vorhanden), die generiert werden, wenn Sie ein Befehlsskript ausführen, in den NetScaler Console-Serverprotokolldateien speichern möchten. Wenn Sie diese Optionen nicht aktivieren, verwirft NetScaler Console alle Ausgaben und Fehler, die bei der Ausführung des Befehlsskripts generiert wurden.

Job-Aktion ausführen

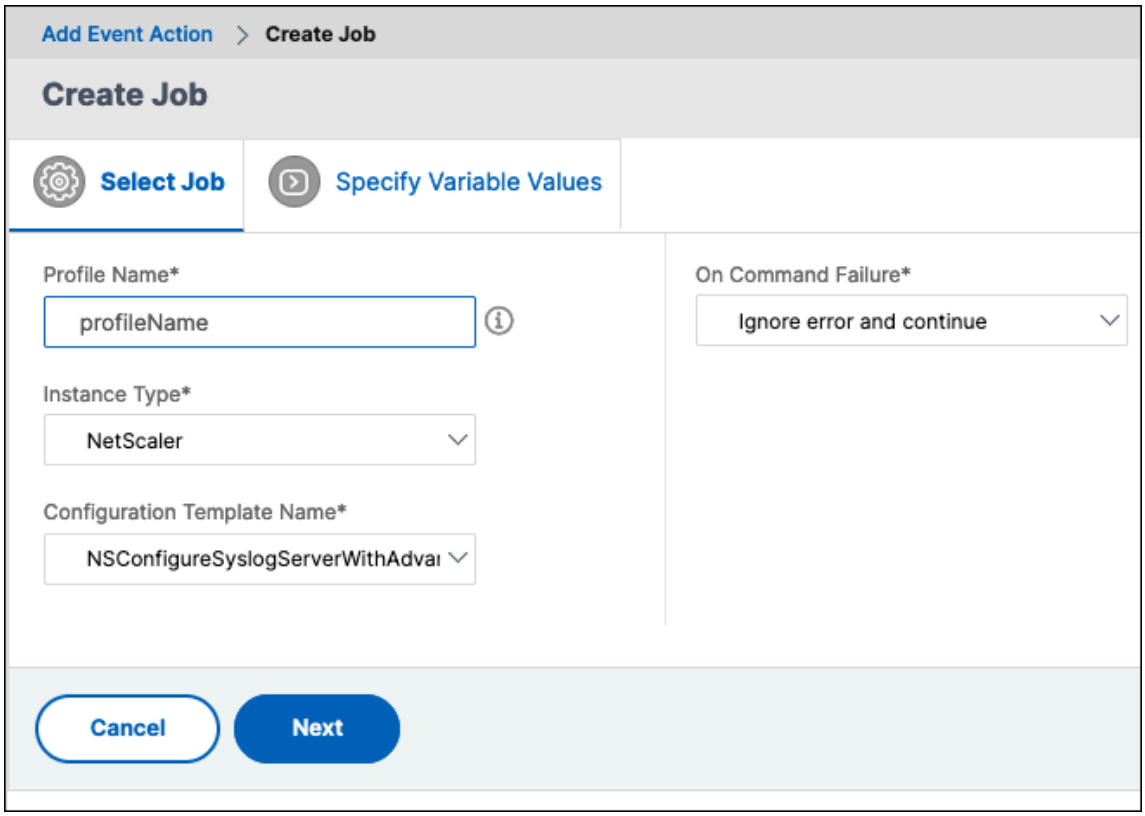
Wenn Sie ein Profil mit Konfigurationsaufträgen erstellen, wird ein Job als integrierter Job oder als benutzerdefinierter Job für NetScaler- und NetScaler SDX-Instanzen für Ereignisse und Alarme ausgeführt, die den von Ihnen angegebenen Filterkriterien entsprechen.

1. Wählen Sie in der **Jobprofilliste** ein Jobprofil aus. Um eine Liste hinzuzufügen, klicken Sie auf **Hinzufügen**.
2. Gehen Sie auf der Seite **Job erstellen** wie folgt vor:

a) **Job auswählen**. Erstellen Sie ein Profil mit einem Job, den Sie ausführen möchten, wenn die Ereignisse die definierten Filterkriterien erfüllen. Geben Sie einen Profilnamen, den Instanztyp, die Konfigurationsvorlage und die Aktion an, die ausgeführt werden soll, wenn die Befehle für den Job fehlschlagen.

b) **Variablenwerte angeben**. Geben Sie Ihre Variablenwerte auf der Grundlage des ausgewählten Instanztyps und der ausgewählten Konfigurationsvorlage an.

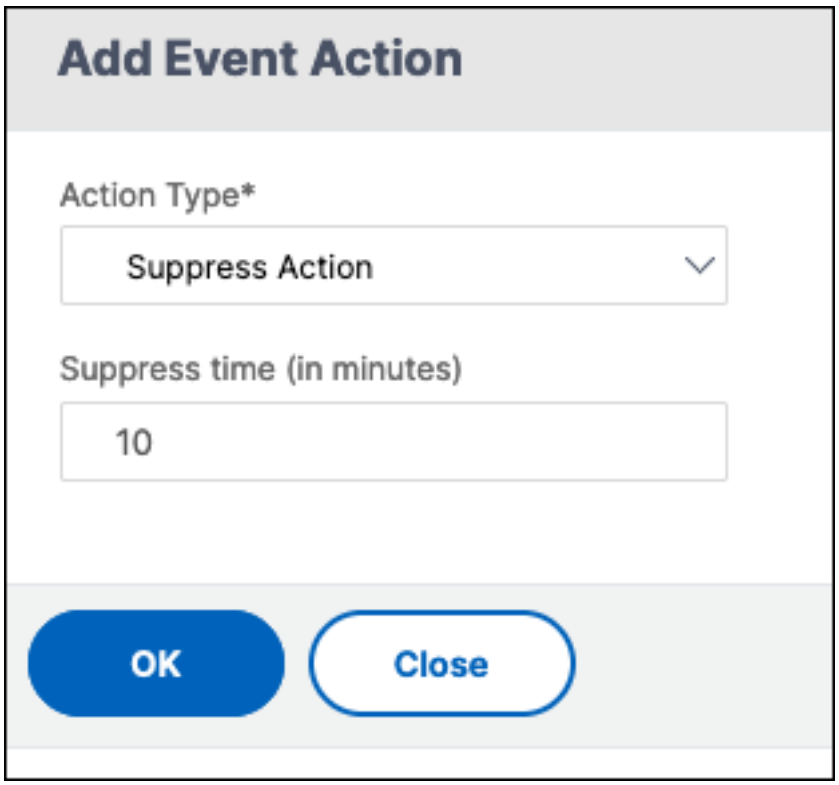
c) Klicken Sie auf **Fertigstellen**, um den Job zu erstellen.



3. Klicken Sie auf **OK**.

Aktion unterdrücken

- Geben Sie im Feld **Zeit unterdrücken** einen Zeitraum in Minuten ein, 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 Console die Unterdrückungszeit als Null und läuft nie ab.

Slack-Benachrichtigungen senden

Beim Konfigurieren eines Slack-Kanals werden die Ereignisbenachrichtigungen an diesen Kanal gesendet. Sie können viele Slack-Kanäle so konfigurieren, dass sie diese Benachrichtigungen erhalten.

1. Wählen Sie in der **Slack-Profilliste** ein Slack-Profil aus. Um ein Slack-Profil hinzuzufügen, klicken Sie auf **Hinzufügen**.
2. Gehen Sie auf der Seite **Slack-Profil erstellen** wie folgt vor:
    a) **Profilname**. Geben Sie einen Namen für die Profilliste ein, die auf der NetScaler Console 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 eingegeben haben. Eingehende Webhooks sind eine einfache Möglichkeit, Nachrichten aus externen Quellen

in Slack zu posten. Die URL ist intern mit dem Kanalnamen verknüpft. Alle Ereignisbenachrichtigungen werden an diese URL gesendet und dann im ausgewählten Slack-Kanal veröffentlicht. Ein Beispiel für einen Webhook ist wie folgt: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK

d) Klicken Sie auf **Erstellen**.

3. Klicken Sie auf **OK**.

> **Hinweis:**
>
> Sie können die Slack-Profile auch hinzufügen, indem Sie zu **Einstellungen** > **Benachrichtigungen** > **Slack-Profile** navigieren. Klicken Sie auf **Hinzufügen** und erstellen Sie das Profil.

PagerDuty-Benachrichtigungen senden

Sie können ein PagerDuty-Profil als Option in NetScaler Console hinzufügen, um die Vorfallbenachrichtigungen auf der Grundlage Ihrer PagerDuty-Konfigurationen zu überwachen. Mit PagerDuty können Sie Benachrichtigungen per E-Mail, SMS, Push-Benachrichtigung und Telefonanruf an einer registrierten Nummer konfigurieren.

1. Wählen Sie in der **PagerDuty-Profilliste** ein PagerDuty-Profil aus. Um ein Profil hinzuzufügen, klicken Sie auf **Hinzufügen**.
2. Auf der Seite **PagerDuty-Profil erstellen** gehen Sie wie folgt vor:

   a) **Profilname**. Geben Sie einen Profilnamen Ihrer Wahl ein.

   b) **Integrationsschlüssel**. Geben Sie den Integrationsschlüssel ein.

   Sie können den Integrationsschlüssel von Ihrem PagerDuty-Portal erhalten.

   c) Klicken Sie auf **Erstellen**.

Bevor Sie ein PagerDuty-Profil in NetScaler Console 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.

Anwendungsfall:

Stellen Sie sich ein Szenario mit folgenden Aufgaben vor:

- Senden von Benachrichtigungen an Ihr PagerDuty-Profil.
- Konfigurieren eines Telefonanruf als Option in PagerDuty, um Benachrichtigungen zu erhalten.
- Erhalten von Telefonanrufbenachrichtigungen für NetScaler-Ereignisse.

Erstellen der PagerDuty-Konfiguration. Nach Abschluss der Konfiguration erhalten Sie jedes Mal, wenn ein neues Ereignis für die NetScaler-Instanz generiert wird, einen Telefonanruf. Aus dem Telefonanruf können Sie entscheiden:

- Bestätigen Sie das Ereignis
- Markiere es als gelöst
- Eskalieren Sie zu einem anderen Teammitglied

ServiceNow-Benachrichtigungen senden

Sie können ServiceNow-Incidents für NetScaler Console-Ereignisse automatisch generieren, indem Sie das ServiceNow-Profil auf der NetScaler Console-GUI auswählen. Sie müssen das **ServiceNow**-Profil in der NetScaler Console auswählen, um eine Ereignisregel zu konfigurieren.

Bevor Sie eine Ereignisregel zur automatischen Generierung von ServiceNow-Incidents konfigurieren, integrieren Sie die NetScaler Console in die ServiceNow-Instanz. Weitere Informationen finden Sie unter Konfigurieren des ITSM-Adapters für ServiceNow.

1. Wählen Sie **ServiceNow-Profil**das Profil **Citrix_Workspace_SN** aus der Liste aus.
2. Klicken Sie auf **OK**.

Ereignisfilter planen

March 12, 2024

Wenn Sie nach dem Erstellen eines Filters für Ihre Regel nicht möchten, dass die NetScaler Console jedes Mal eine Benachrichtigung sendet, wenn das generierte Ereignis die Filterkriterien erfüllt, können Sie den Filter so planen, dass er nur in bestimmten Zeitintervallen ausgelöst wird, z. B. täglich, wöchentlich oder monatlich.

Wenn Sie beispielsweise eine Systemwartungsaktivität für verschiedene Anwendungen auf Ihren Instanzen zu unterschiedlichen Zeiten geplant haben, können die Instanzen mehrere Alarme generieren.

Wenn Sie einen Filter für diese Alarme konfiguriert und E-Mail-Benachrichtigungen für diese Filter aktiviert haben, sendet der Server viele E-Mail-Benachrichtigungen, wenn NetScaler Console 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 mithilfe der NetScaler Console:

1. Navigieren Sie in der NetScaler Console 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.
    - **Geplantes Zeitintervall (Stunden)** —Stunden, zu denen die Regel geplant werden soll (verwenden Sie das 24-Stunden-Format).
4. Klicken Sie auf **Zeitplan**.

Gemeldeten Schweregrad von Ereignissen auf NetScaler-Instanzen ändern

January 26, 2024

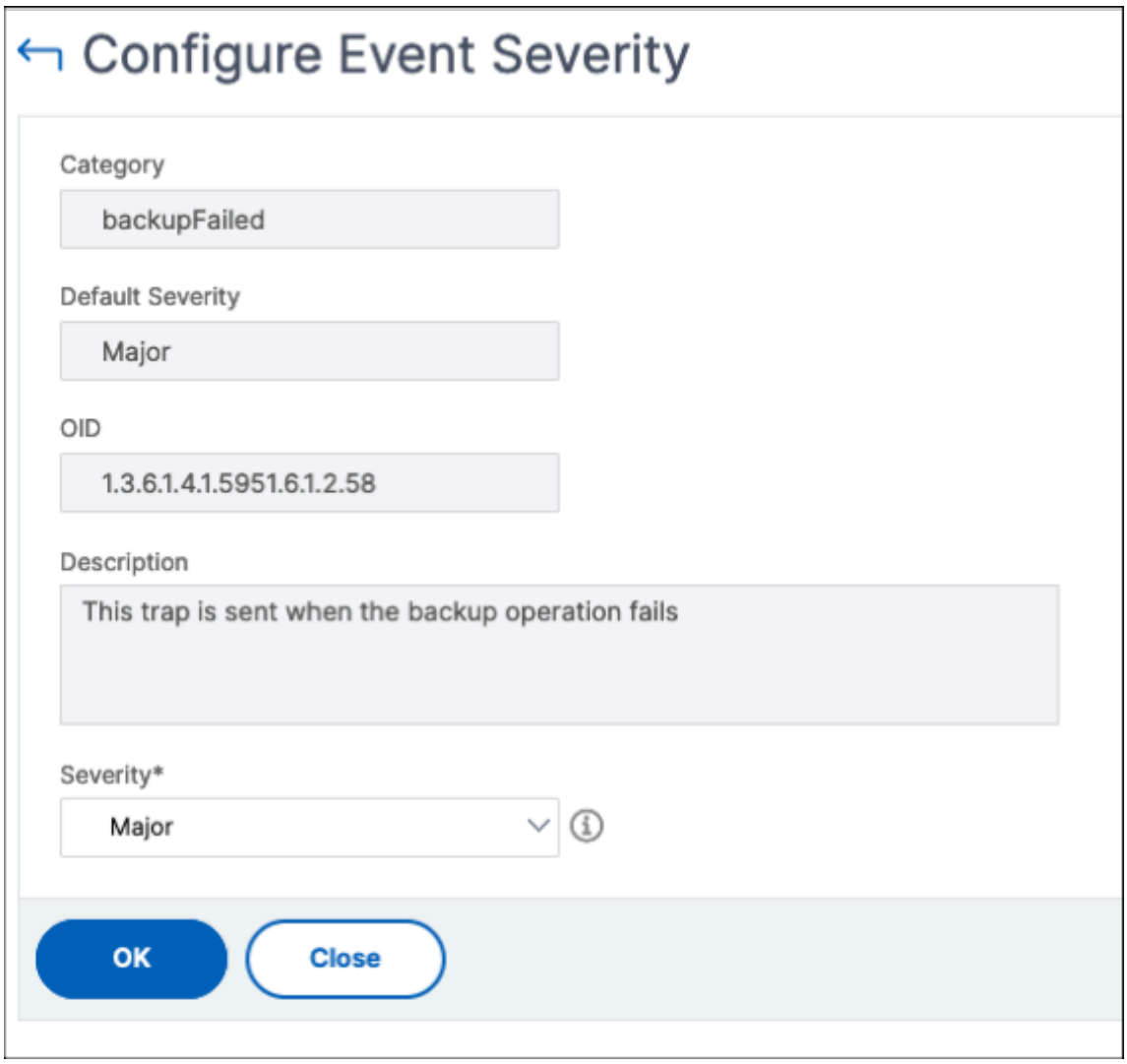
Sie können die Berichterstellung über Ereignisse verwalten, die auf allen Ihren Geräten generiert werden, sodass Sie Ereignisdetails zu einem bestimmten Ereignis in einer Instanz anzeigen und Berichte basierend auf dem Schweregrad des Ereignisses anzeigen können. Sie können auch Ereignisregeln erstellen, die die Standardeinstellungen für den Schweregrad verwenden, und Sie können die Einstellungen für den Schweregrad ändern. Sie können den Schweregrad für allgemeine und unternehmensspezifische Ereignisse konfigurieren.

Sie können die folgenden Schweregrade definieren: Kritisch, 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 NetScaler-Instanztyp, 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**.



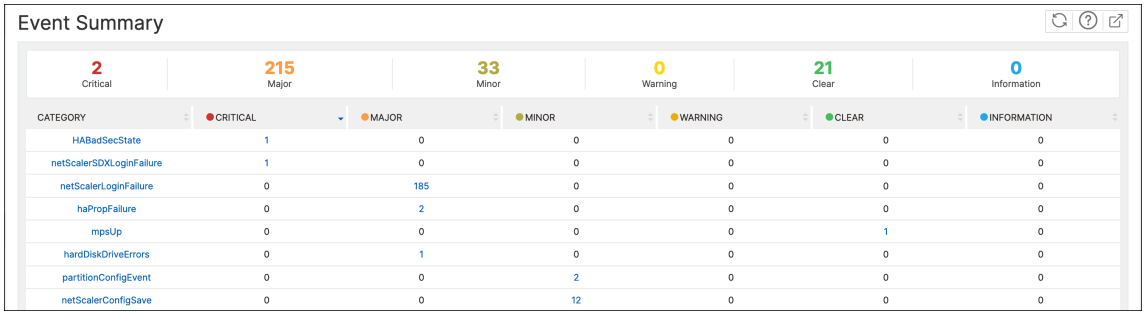
Zusammenfassung der Ereignisse anzeigen

March 12, 2024

Sie können jetzt eine Seite mit der Ereignisübersicht anzeigen, auf der Sie die Ereignisse und Traps überwachen können, die auf Ihrer NetScaler Console empfangen wurden. Navigieren Sie zu **Infrastruktur > Ereignisse**. Auf der Seite Ereignisübersicht werden die folgenden Informationen in einem tabellarischen Format angezeigt:

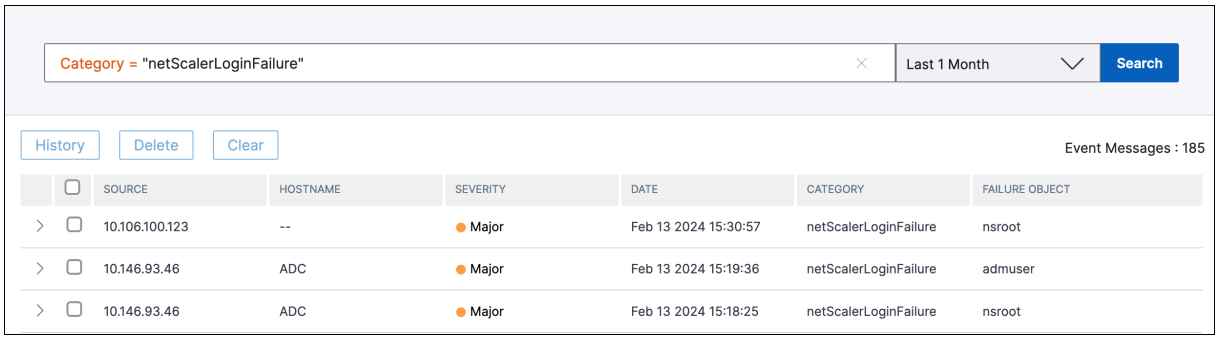
- **Zusammenfassung aller Ereignisse, die von NetScaler Console**empfangen wurden . Die Ereignisse sind nach Kategorien aufgelistet, und die verschiedenen Schweregrade werden in verschiedenen Spalten angezeigt: Kritisch, Schwerwiegend, Gering, Warnung, Unklar

und Information. Ein kritisches Ereignis würde beispielsweise eintreten, wenn eine Citrix Application Delivery Controller (NetScaler) -Instanz ausfällt und das Senden von Informationen an die NetScaler Console beendet. Während des Ereignisses wird eine Benachrichtigung an einen Administrator gesendet, in der der Grund für den Ausfall der Instanz, die Zeit, für die sie ausgefallen war, usw. erläutert wird. Das Ereignis wird dann auf der Seite Ereignisübersicht aufgezeichnet, auf der Sie die Zusammenfassung anzeigen und auf die Details des Ereignisses zugreifen können.



- **Anzahl der empfangenen Traps für jede Kategorie**. Die Anzahl der empfangenen Traps, kategorisiert nach Schweregrad. Standardmäßig hat jeder Trap, der von NetScaler-Instanzen an NetScaler Console gesendet wird, einen zugewiesenen Schweregrad, aber als Netzwerkadministrator können Sie seinen Schweregrad in der NetScaler Console-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 den Hostnamen einer NetScaler-Instanz, das Datum, an dem die Trap empfangen wurde, die Kategorie, die Fehlerobjekte, die Ausführung des Konfigurationsbefehls und die Nachrichtenbenachrichtigung.



Sie können die Anzahl der Tage zwischen 1 und 40 konfigurieren, für die Sie die Ereignisse in NetScaler Console anzeigen möchten. Wenn Sie beispielsweise 30 Tage auswählen, zeigt NetScaler Console die Ereignisse 30 Tage lang an. Nach 30 Tagen werden die Ereignisse gelöscht. Um diese Ereigniseinstellung zu konfigurieren, navigieren Sie zu **Einstellungen > Allgemeine Einstellungen > Datenspeicherungsrichtlinie**. Weitere Informationen finden Sie unter Richtlinie zur Datenaufbewahrung.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** . Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis:**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Ereignisschweregrade und SNMP-Trap-Details anzeigen

March 12, 2024

Wenn Sie ein Ereignis und seine Einstellungen in NetScaler Console erstellen, können Sie das Ereignis sofort auf der Seite mit der Ereignisübersicht anzeigen. Ebenso können Sie den Zustand, die Betriebszeit, die Modelle und die Versionen aller Citrix Application Delivery Controller (NetScaler) -Instanzen, die Ihrem NetScaler Console-Server hinzugefügt wurden, im Infrastructure 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.

In ähnlicher Weise können Sie den Zustand einer NetScaler VPX Instanz auf dem Dashboard anzeigen. Sie können die Zeit maskieren, in der die Instanz gestartet und ausgeführt wurde, und nur die Zeiten

anzeigen, in denen die Instanz außer Betrieb war. Wenn Sie auf das Diagramm klicken, gelangen Sie zur Seite dieser Instanz, auf der der Filter *außerhalb des Dienstes* bereits angewendet wurde, und sehen Details wie den Hostnamen, die Anzahl der pro Sekunde empfangenen HTTP-Anforderungen, die CPU-Auslastung und andere. Sie können auch die Instanz auswählen und das Instanz-Dashboard für weitere Details anzeigen.

So wählen Sie in NetScaler Console bestimmte Ereignisse nach Schweregrad aus:

1. Melden Sie sich mit Ihren Administratoranmeldeinformationen bei NetScaler Console an.
2. Navigieren Sie zu **Infrastruktur > Instanzen**.

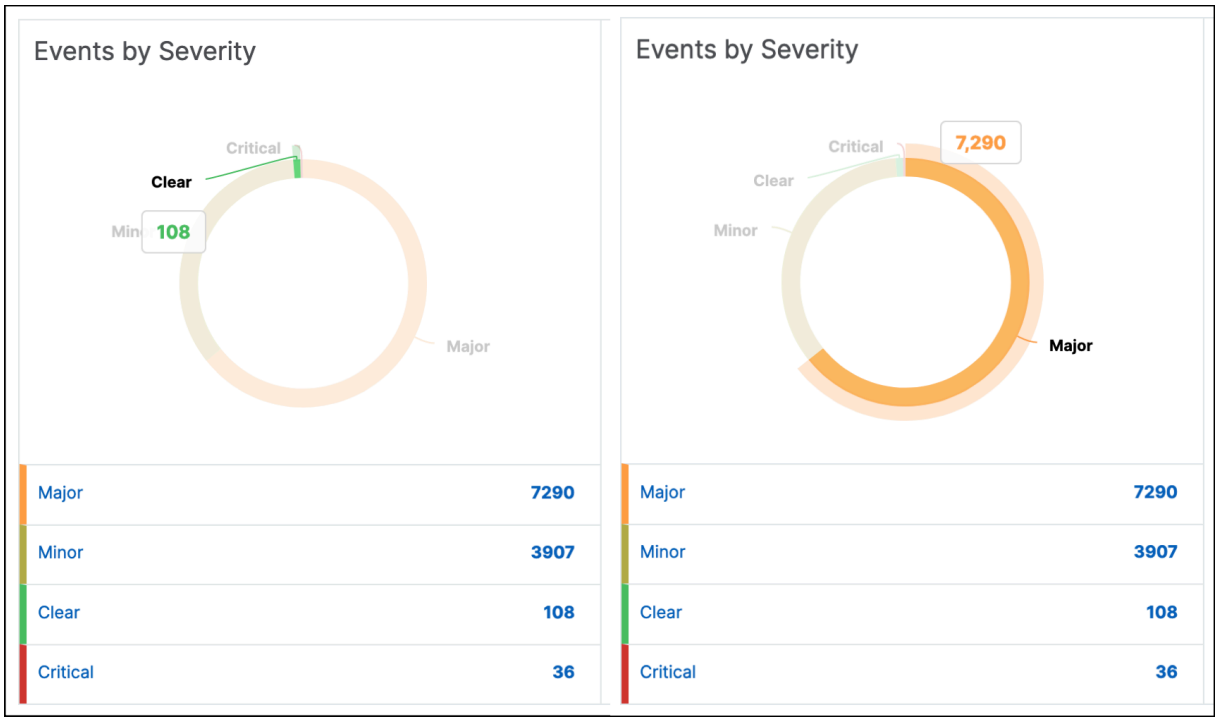
   Oder

   Navigieren Sie zu **Infrastruktur > Ereignisse > Berichte**.
3. Wählen Sie in der Dropdownliste oben rechts auf der Seite die Dauer aus, für die Ereignisse nach Schweregrad angezeigt werden sollen.

4. Das Ringdiagramm **Ereignisse nach Schweregrad** zeigt eine visuelle Darstellung aller Ereignisse nach Schweregrad. 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:**
>
> Unter dem Ringdiagramm sehen Sie eine Liste der Schweregrade, die in der Tabelle dargestellt sind. Standardmäßig werden in einem Donutdiagramm alle Ereignisse aller Schweregradtypen angezeigt. Daher werden alle Schweregradtypen in der Liste hervorgehoben. Bewegen Sie den Mauszeiger über die Schweregradtypen, um den von Ihnen ausgewählten Schweregrad einfacher anzuzeigen und zu überwachen.

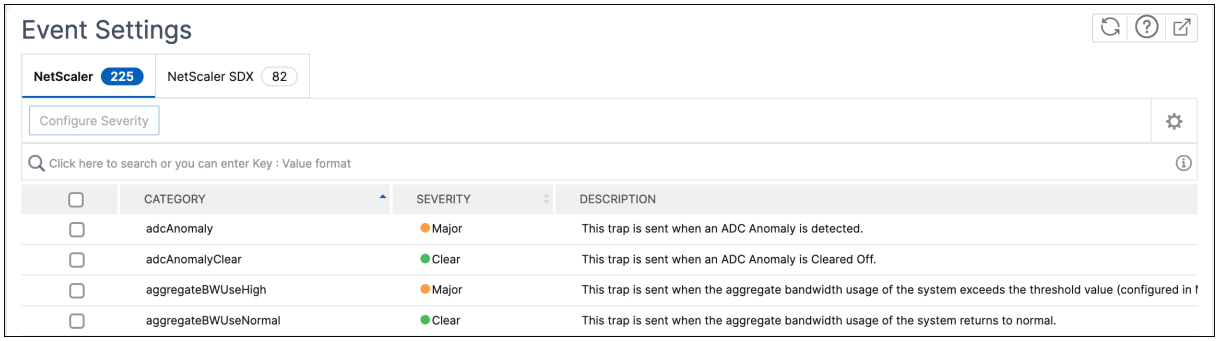


So zeigen Sie NetScaler SNMP-Trap-Details auf der NetScaler Console an:

**** Sie können jetzt die Details zu jedem SNMP-Trap, der von seinen verwalteten NetScaler-Instanzen empfangen wurde, in der NetScaler Console auf der Seite mit den Ereigniseinstellungen anzeigen. 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.

Beispiel: Bei einem Ereignis mit der Trap-Kategorie **aggregateBWUseNormal** wird die Beschreibung des Traps wie folgt angezeigt: “Dieser Trap wird gesendet, wenn die Gesamtbandbreitennutzung des Systems wieder normal ist.”



Syslog-Meldungen anzeigen und exportieren

July 17, 2024

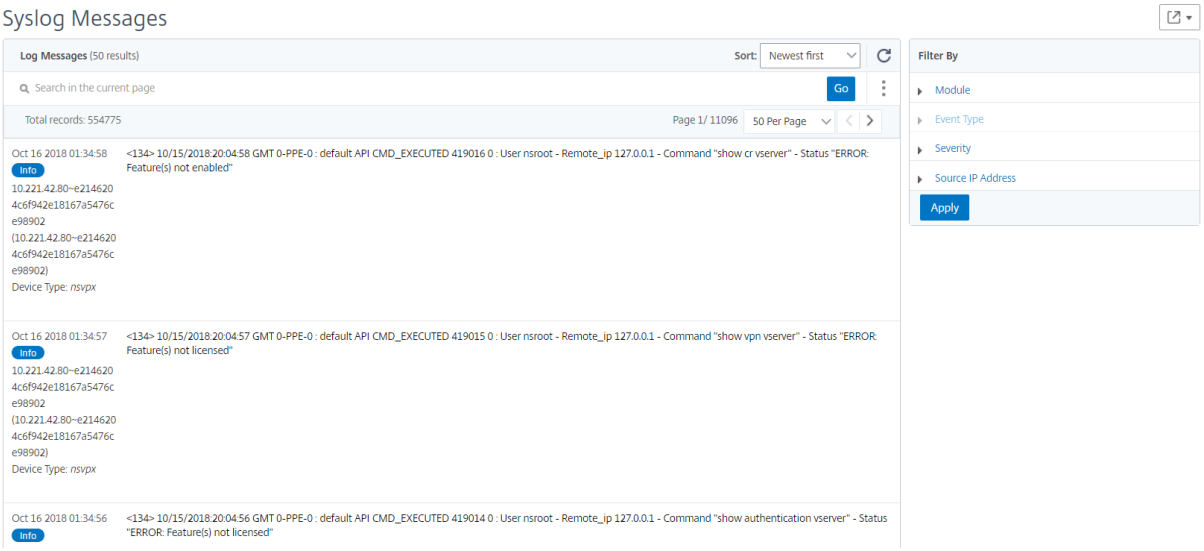
Sie können Syslog-Meldungen anzeigen, ohne sich bei NetScaler Console anzumelden, indem Sie einen Export aller auf dem Server empfangenen Syslog-Meldungen planen. Sie können Syslog-Nachrichten, die auf Ihren Citrix Application Delivery Controller (NetScaler)-Instanzen generiert wurden, in den Formaten PDF, CSV, PNG und JPEG exportieren. Sie können auch den Export dieser Berichte an bestimmte E-Mail-Adressen in verschiedenen Intervallen planen.

Anzeigen von Syslog-Nachrichten

Sie können alle Syslog-Nachrichten anzeigen, die auf Ihren verwalteten NetScaler-Instanzen generiert wurden. Um die Meldungen anzuzeigen, müssen Sie die Instanzen so konfigurieren, dass sie die Syslog-Meldungen an den NetScaler Console-Server umleiten. Die Syslog-Meldungen werden zentral in der Datenbank gespeichert und stehen im Syslog Viewer zu Überwachungszwecken zur Verfügung. Sie können diese Protokollierungsinformationen kombinieren und Berichte für Analysen aus den gesammelten Daten ableiten.

Sie können syslog auch so konfigurieren, dass verschiedene Arten von Ereignissen protokolliert werden.

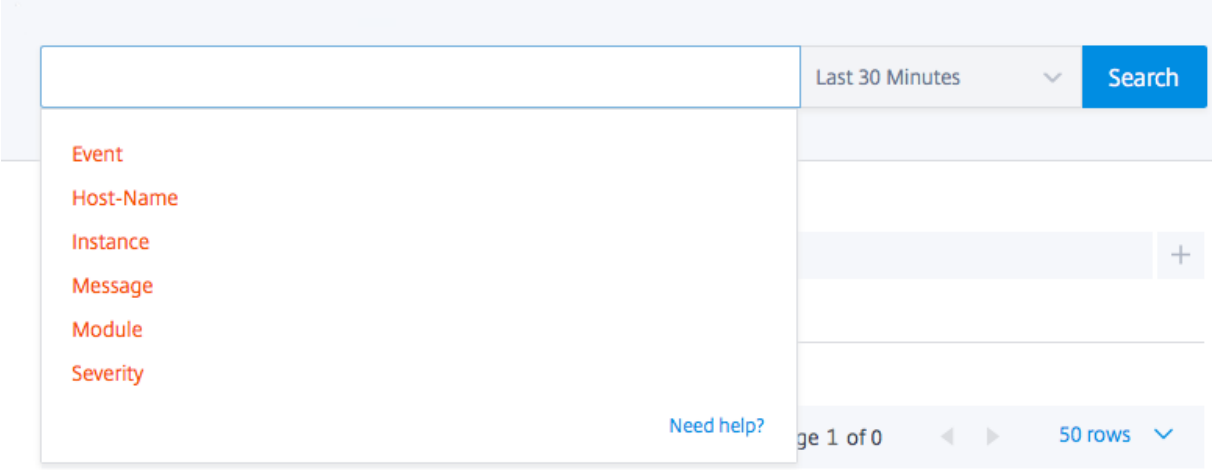
Um den Syslog Viewer anzuzeigen, navigieren Sie zu **Infrastruktur > Ereignisse > Syslog-Meldungen**. Wählen Sie die entsprechenden Filter aus, um Ihre Systemprotokollmeldungen anzuzeigen.



Syslog-Nachrichten durchsuchen

Sie können Filter verwenden, um Syslog-Meldungen und Überwachungsprotokollmeldungen zu durchsuchen, um Ihre Ergebnisse einzugrenzen und in Echtzeit genau das zu finden, wonach Sie suchen.

Um Syslog-Meldungen für alle in der NetScaler Console-Software vorhandenen NetScaler-Instanzen zu durchsuchen, navigieren Sie von der NetScaler Console-GUI aus zu **Infrastruktur > Ereignisse > Syslog-Meldungen**. Die neuen Filterkategorien sind Instanz, Modul, Ereignis, Schweregrad und Nachricht.



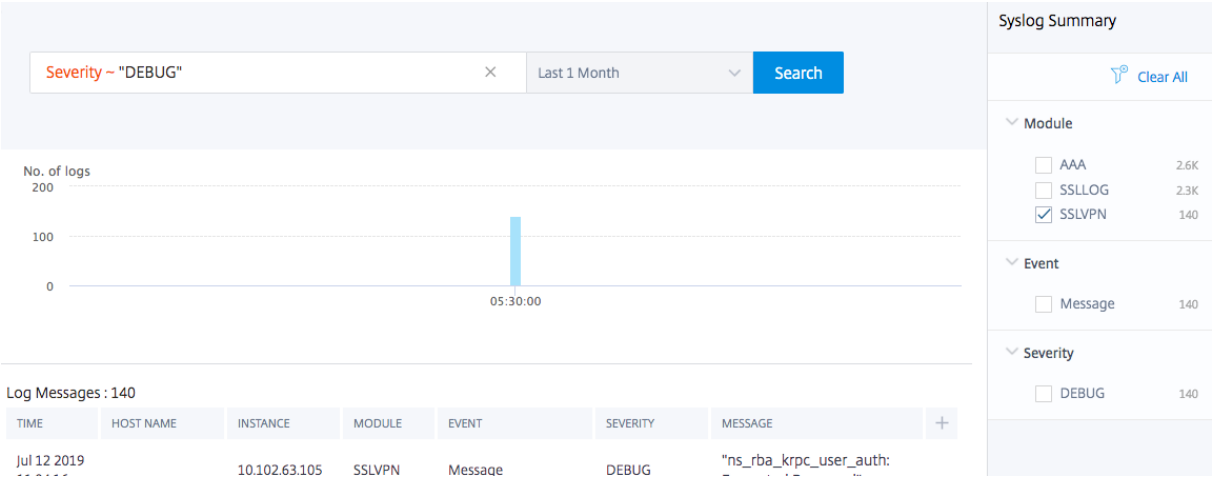
Um alle NetScaler Console-Systemüberwachungsprotokollmeldungen in der NetScaler Console-Software zu durchsuchen, navigieren Sie von der NetScaler Console-GUI aus zu **Einstellungen > Audit-Log-Meldungen**. Die neuen Filterkategorien sind Instanz, Modul, Ereignis, Schweregrad und Nachricht.

Um Audit-Log-Meldungen für alle in der NetScaler Console vorhandenen Anwendungen zu durchsuchen, navigieren Sie von der NetScaler Console-GUI aus zu **Infrastruktur > Netzwerkfunktionen Überwachung**.

Um die Audit-Log-Meldungen für eine bestimmte Anwendung auf der NetScaler Console zu durchsuchen, navigieren Sie von der NetScaler Console-GUI aus zu **Anwendung > Dashboard** und wählen Sie den virtuellen Server aus, für den Sie die Audit-Log-Meldungen durchsuchen möchten. Klicken Sie als Nächstes auf die Registerkarte **Überwachungsprotokoll**.

Nachdem Sie eine Filterkategorie ausgewählt haben, geben Sie an, ob sie dem Suchbegriff entspricht oder diesen enthält.

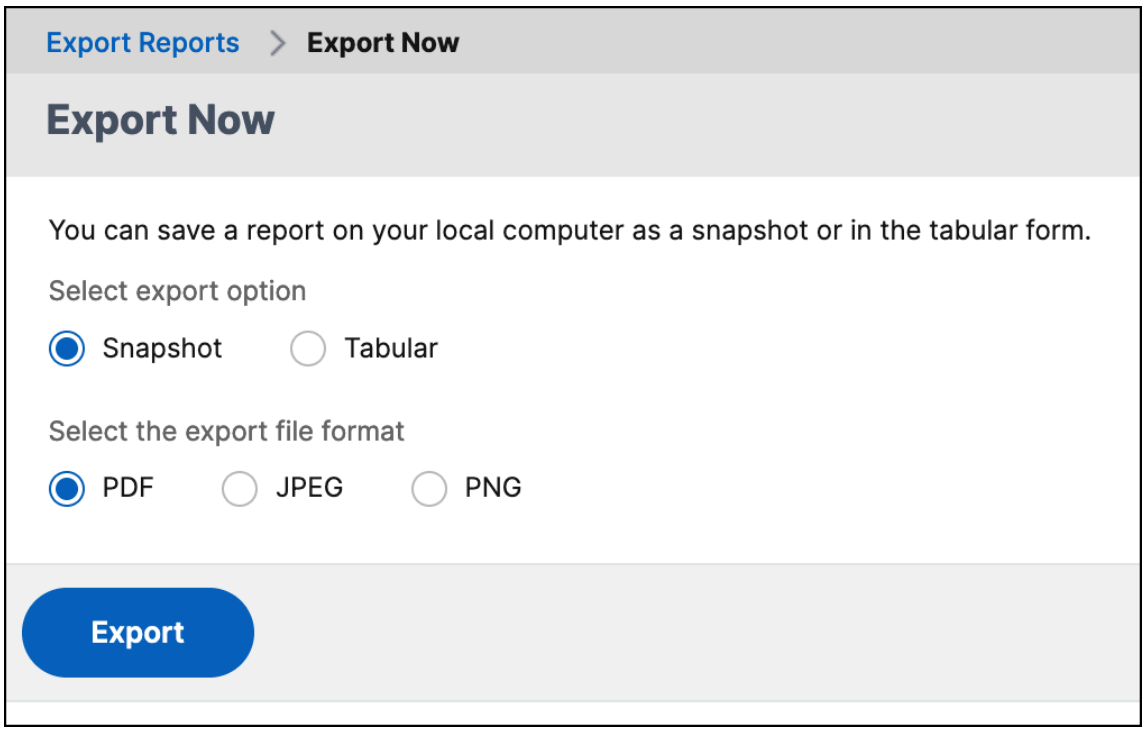
Fügen Sie als Nächstes den Suchbegriff hinzu. Für einige Kategorien wird eine vorausgefüllte Liste mit Suchbegriffen angezeigt. Standardmäßig beträgt die Suchzeit 1 Tag. Sie können den Zeit- und Datumsbereich ändern, indem Sie auf den Pfeil nach unten klicken. Sie können Ihre Suche weiter eingrenzen, indem Sie Optionen im Bereich **Syslog-Zusammenfassung** oder **Überwachungsprotokollzusammenfassung** auswählen.



Syslog-Nachrichten exportieren

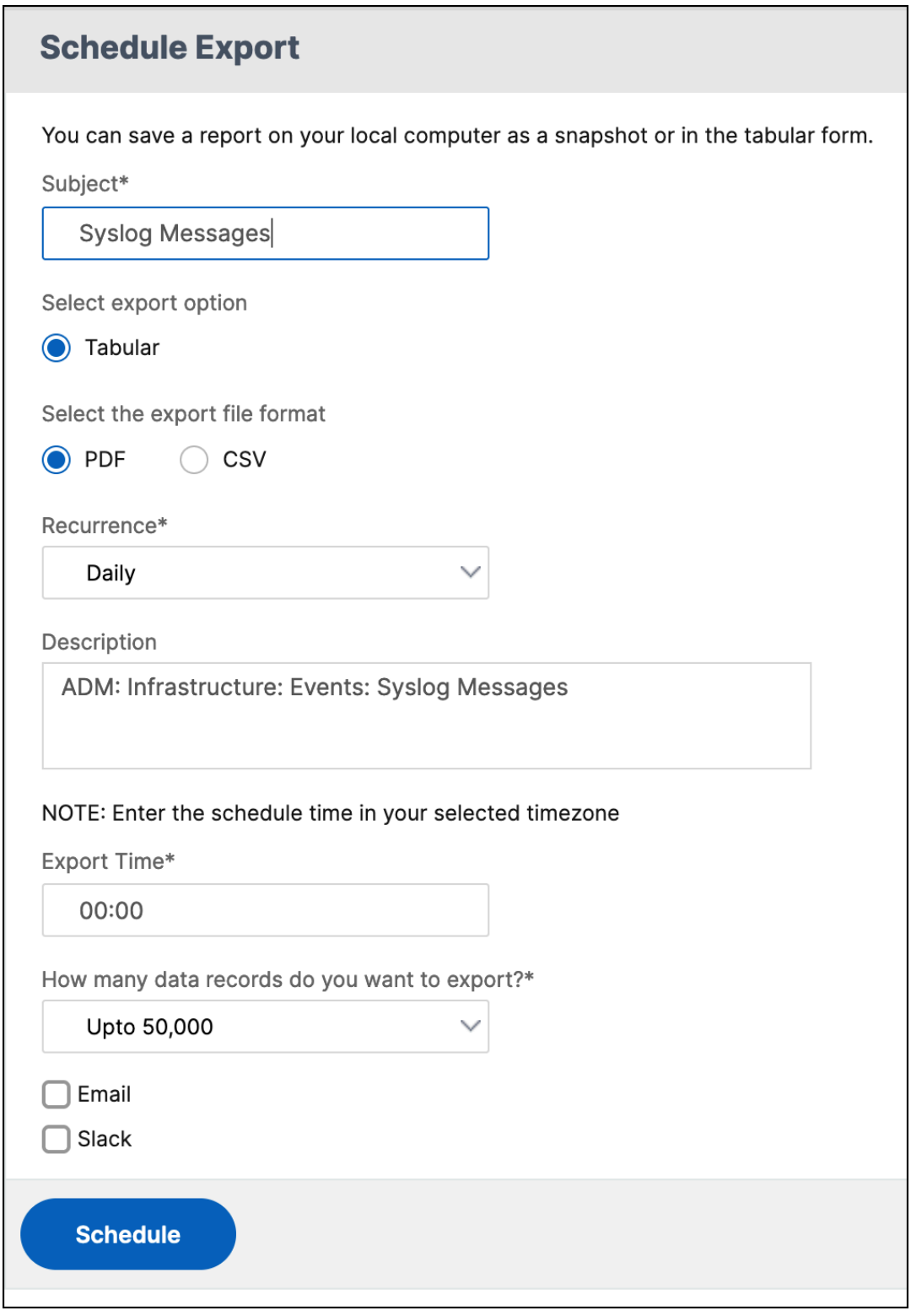
So exportieren Sie einen Syslog-Meldungsbericht mithilfe der NetScaler Console:

1. Navigieren Sie zu **Infrastruktur > Ereignisse > Syslog-Meldungen**.
2. Klicken Sie im rechten Bereich auf die Schaltfläche Exportieren in der oberen rechten Ecke der Seite Syslog-Meldungen.
3. Wählen Sie unter **Jetzt exportieren**das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.



So planen Sie den Export von Syslog-Meldungsberichten mithilfe der NetScaler Console:

1. Navigieren Sie zu **Infrastruktur > Ereignisse > Syslog-Meldungen**.
2. Klicken Sie auf der Seite **Syslog-Meldungen** im rechten Fensterbereich auf **Exportieren**.
3. Legen Sie auf der Registerkarte **Bericht planen** die folgenden Parameter fest:
    - **Beschreibung**: Meldung, die den Grund für den Export des Berichts beschreibt.
    - **Format**: Format, in das der Bericht exportiert werden soll.
    - **Wiederholung**: Intervall, in dem der Bericht exportiert werden soll.
    - **Exportzeit**: Der Zeitpunkt, zu dem die Auswertung exportiert werden soll. Geben Sie die Uhrzeit im 24-Stunden-Format für Ihre lokale Zeitzone ein.
    - **E-Mail-Verteilerliste**: Liste der Empfänger, die den Bericht per E-Mail erhalten sollen. Wählen Sie eine E-Mail-Verteilerliste aus der bereitgestellten Liste aus. Eine E-Mail wird ausgelöst, wenn der Bericht generiert wird und die geplanten Zeitkriterien erfüllt. Wenn Sie eine E-Mail-Verteilerliste erstellen möchten, klicken Sie auf **+** und geben Sie E-Mail-Server- und E-Mail-Profildetails ein.



Syslog-Nachrichten unterdrücken

July 17, 2024

Wenn NetScaler Console als Syslog-Server konfiguriert ist, empfängt sie alle Syslog-Meldungen von den konfigurierten Citrix Application Delivery Controller (NetScaler) -Instanzen. Möglicherweise möchten Sie viele Nachrichten nicht sehen. Zum Beispiel könnten Sie nicht daran interessiert sein, alle Nachrichten auf Informationsebene zu sehen. Sie können nun einige Syslog-Nachrichten verwerfen, die Sie nicht interessieren. Sie können einige der Syslog-Meldungen, die in NetScaler Console eingehen, unterdrücken, indem Sie einige Filter einrichten. NetScaler Console löscht alle Nachrichten, die den Kriterien entsprechen. Diese verworfenen Nachrichten werden nicht auf der NetScaler Console-GUI angezeigt, und diese Meldungen werden auch nicht in der NetScaler Console-Datenbank des Kunden gespeichert.

Sie können einige der protokollierten Syslog-Meldungen, die in NetScaler Console 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 Console angeben, um Nachrichten zu suchen und zu unterdrücken. NetScaler Console löscht alle Nachrichten, die den Kriterien entsprechen. Diese verworfenen Nachrichten werden nicht auf der NetScaler Console-GUI angezeigt, und diese Meldungen 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 der NetScaler Console zu **Infrastruktur > Ereignisse > Syslog-Meldungen** .
2. Klicken Sie auf das Zahnradsymbol, um die Seite **Suppress Filters** anzuzeigen.

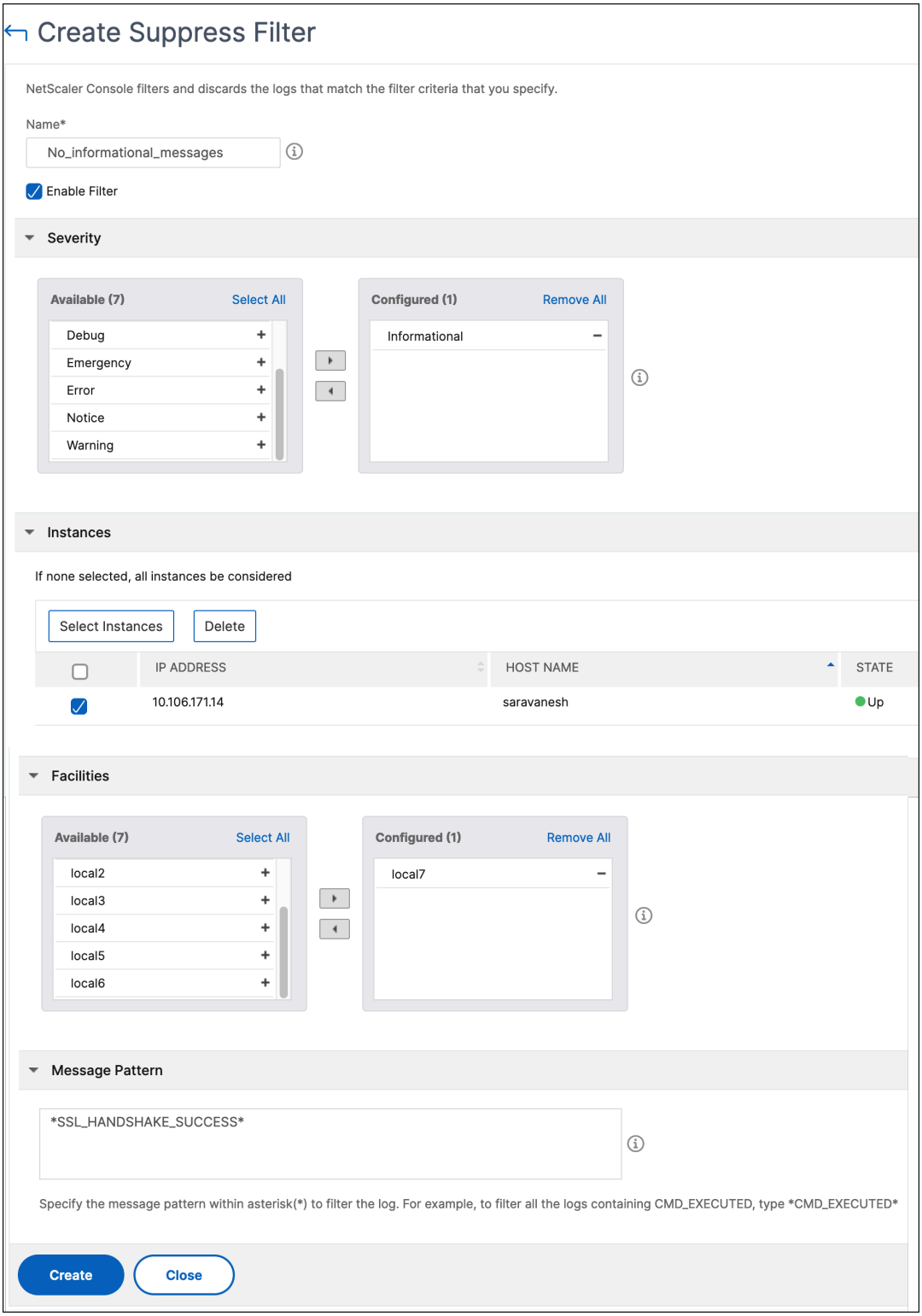
3. Klicken Sie auf der Seite **Suppress Filters** auf **Add**.
4. Aktualisieren Sie in **Create Suppress Filter** die folgenden Informationen:

a) **Name** - geben Sie einen Namen für den Filter ein.

> **Hinweis:**
>
> Wenn verschiedene Benutzer unterschiedlichen Zugriff 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 Möglichkeit aus, um Nachrichten basierend auf der Quelle, die sie generiert, zu unterdrücken.

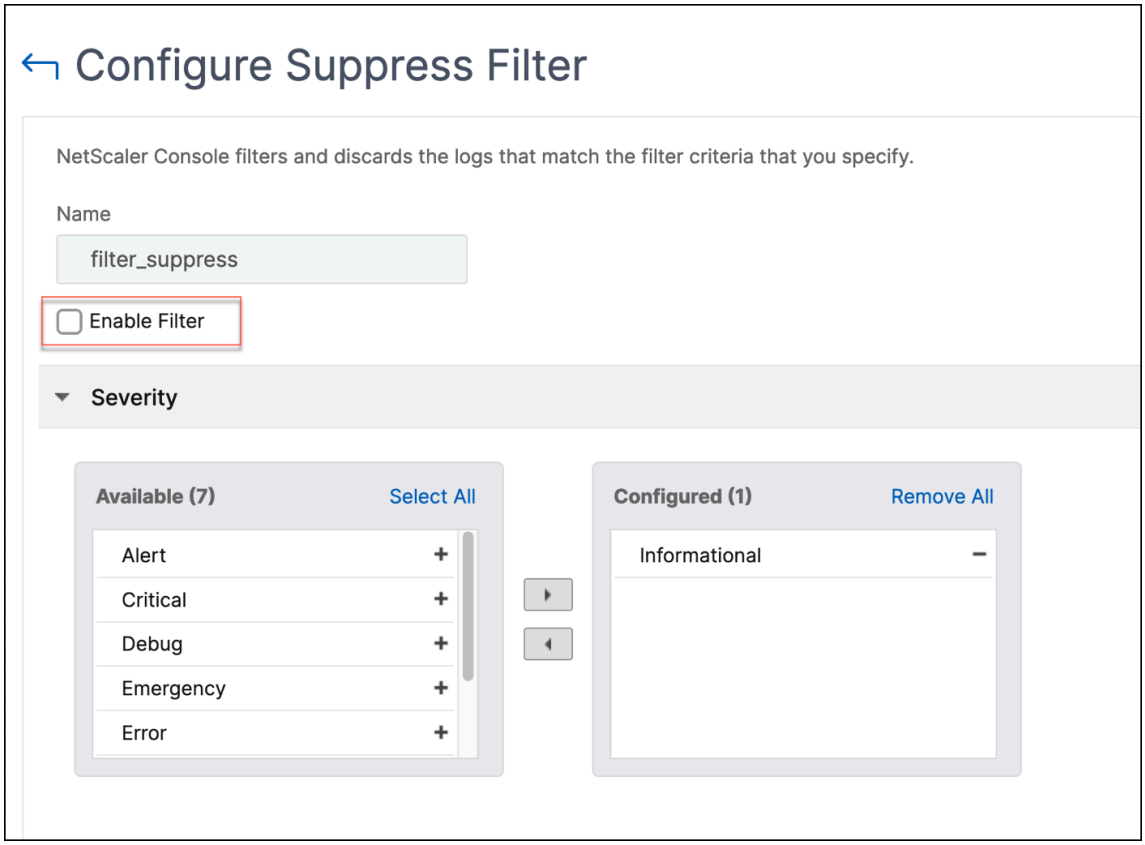
e) **Nachrichtenmuster** - Sie können auch ein Textmuster eingeben, das von Sternchen (*)

umgeben ist, um die Nachrichten zu unterdrücken. Die Nachrichten werden nach der Textmusterzeichenfolge gesucht und die Meldungen, die dieses Muster enthalten, werden unterdrückt.

Deaktivieren des Filters

Damit die Nachrichten auf der NetScaler Console angezeigt werden können, müssen Sie den Filter deaktivieren.

1. Navigieren Sie zu **Infrastruktur > Ereignisse > Syslog-Meldungen**.
2. Klicken Sie auf das Zahnradsymbol, um die Seite **Suppress Filters** anzuzeigen.
3. Wählen Sie auf der Seite **Suppress Filters** den Filter aus und klicken Sie auf **Edit**.
4. Deaktivieren Sie auf der Seite **Filter unterdrücken konfigurieren** das Kontrollkästchen **Filter aktivieren**, um den Filter zu deaktivieren.



SSL Dashboard

May 9, 2024

NetScaler Console optimiert jetzt jeden Aspekt der Zertifikatsverwaltung 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. Bevor Sie das SSL-Dashboard und seine Funktionen von NetScaler Console verwenden können, müssen Sie verstehen, was ein SSL-Zertifikat ist und wie Sie NetScaler Console verwenden können, um Ihre SSL-Zertifikate zu verfolgen.

Ein SSL-Zertifikat (Secure Socket Layer), das Teil einer SSL-Transaktion ist, ist ein digitales Eingabeformular (X509), das ein Unternehmen (Domain) oder eine Person identifiziert. Das Zertifikat verfügt über eine Public-Key-Komponente, die für jeden Client sichtbar ist, der eine sichere Transaktion mit dem Server initiieren möchte. Der entsprechende private Schlüssel, der sich sicher auf der NetScaler-Appliance befindet, wird verwendet, um die Verschlüsselung und Entschlüsselung asymmetrischer Schlüssel (oder öffentlicher Schlüssel) abzuschließen.

Sie können ein SSL-Zertifikat und einen Schlüssel auf eine der folgenden Arten beziehen:

- Von einer autorisierten Zertifizierungsstelle (CA)
- Durch Generieren eines neuen SSL-Zertifikats und eines neuen Schlüssels auf der NetScaler-Appliance

Die NetScaler Console bietet eine zentrale Ansicht der SSL-Zertifikate, die auf allen verwalteten NetScaler-Instanzen installiert sind. Im SSL-Dashboard können Sie Diagramme anzeigen, mit denen Sie Zertifikatsaussteller, wichtige Stärken, Signaturalgorithmen, abgelaufene oder nicht verwendete Zertifikate usw. nachverfolgen können. Sie können auch die Verteilung der SSL-Protokolle sehen, die auf Ihren virtuellen Servern ausgeführt werden, und die Schlüssel, die auf ihnen aktiviert sind.

Sie können auch Benachrichtigungen einrichten, um Sie darüber zu informieren, wann Zertifikate ablaufen werden, und Informationen darüber enthalten, welche NetScaler-Instanzen diese Zertifikate verwenden.

Sie können ein NetScaler-Instanzzertifikat mit einem Zertifizierungsstellenzertifikat verknüpfen. Stellen Sie jedoch sicher, dass die Zertifikate, die Sie mit demselben CA-Zertifikat verknüpfen, dieselbe Quelle und denselben Aussteller haben. Nachdem Sie ein oder mehrere Zertifikate mit einem Zertifizierungsstellenzertifikat verknüpft haben, können Sie die Verknüpfung aufheben.

> **Hinweis:**
>
> Sie können auch einen Venafi Trust Protection Platform-Server mit NetScaler Console verwenden, um die Verwaltung des gesamten Lebenszyklus von SSL-Zertifikaten zu automatisieren.

> Weitere Informationen finden Sie unter Automatisieren der SSL-Zertifikatsverwaltung.

SSL-Dashboard verwenden

May 9, 2024

Sie können das SSL-Zertifikat-Dashboard in NetScaler Console verwenden, um Grafiken anzuzeigen, die Ihnen helfen, den Überblick über Zertifikataussteller, wichtige Stärken und Signaturalgorithmen zu behalten. Das SSL-Zertifikat-Dashboard zeigt außerdem Diagramme an, die Folgendes angeben:

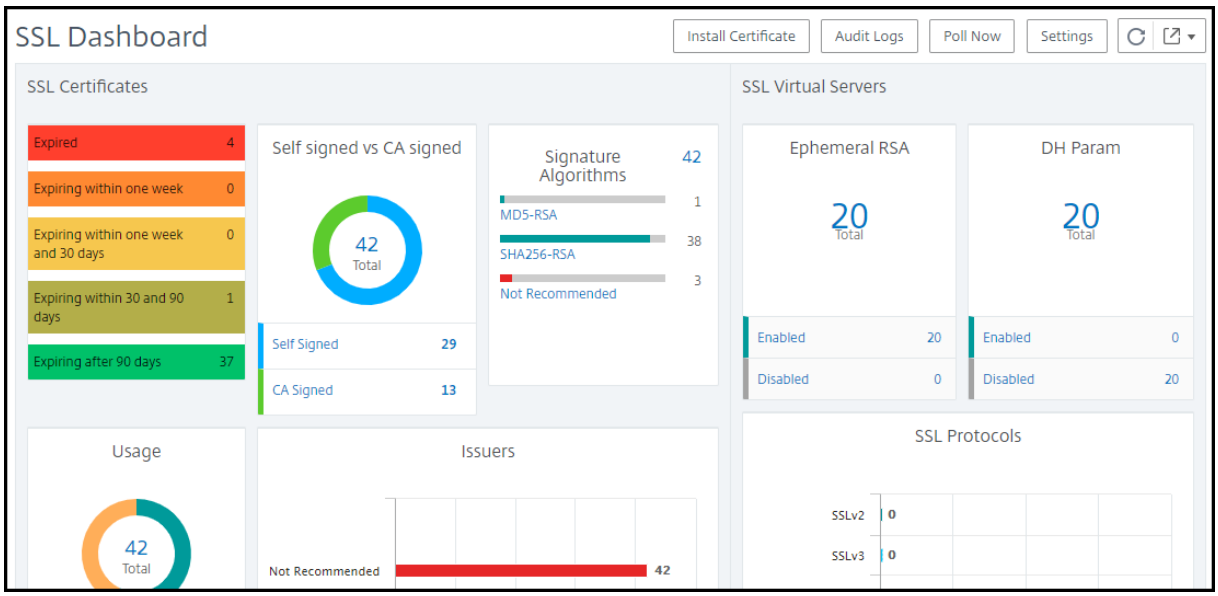
- Anzahl der Tage, nach denen Zertifikate ablaufen
- Anzahl verwendeter und nicht verwendeter Zertifikate
- Anzahl selbstsignierter und von einer Zertifizierungsstelle signierter Zertifikate
- Anzahl der Emittenten
- Signatur-Algorithmen
- SSL-Protokolle
- Top 10 Instanzen nach Anzahl der verwendeten Zertifikate

Überwachen von SSL-Zertifikaten

Verwenden Sie das SSL-Dashboard in der NetScaler Console, um Ihre Zertifikate zu überwachen, wenn Ihr Unternehmen eine SSL-Richtlinie hat, in der Sie bestimmte SSL-Zertifikatsanforderungen definiert haben, z. B. müssen alle Zertifikate eine Mindestschlüsselstärke von 2048 Bit haben und eine vertrauenswürdige Zertifizierungsstelle sie autorisieren muss.

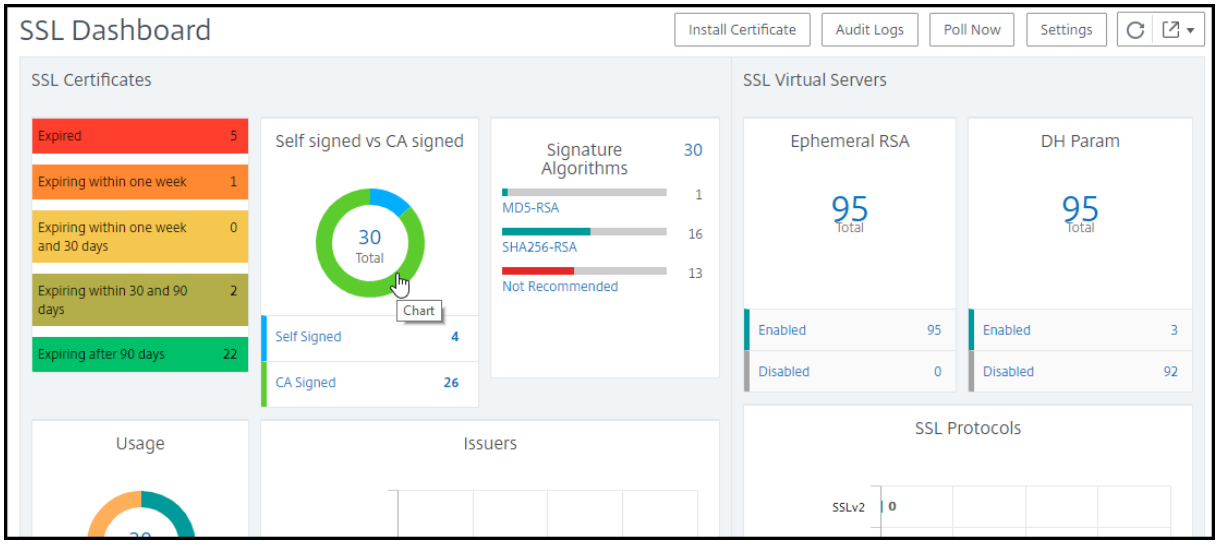
In einem anderen Beispiel haben Sie möglicherweise ein neues Zertifikat hochgeladen, aber vergessen, es an einen virtuellen Server zu binden. Das SSL-Dashboard hebt die verwendeten oder nicht verwendeten SSL-Zertifikate hervor. Im Abschnitt **Verwendung** können Sie die Anzahl der installierten Zertifikate und die Anzahl der verwendeten Zertifikate sehen. Sie können weiter auf das Diagramm klicken, um den Namen der Zertifikate, die Instanz, für die es verwendet wird, ihre Gültigkeit, den Signaturalgorithmus usw. anzuzeigen.

Um SSL-Zertifikate in NetScaler Console zu überwachen, navigieren Sie zu **Infrastruktur > SSL-Dashboard** .

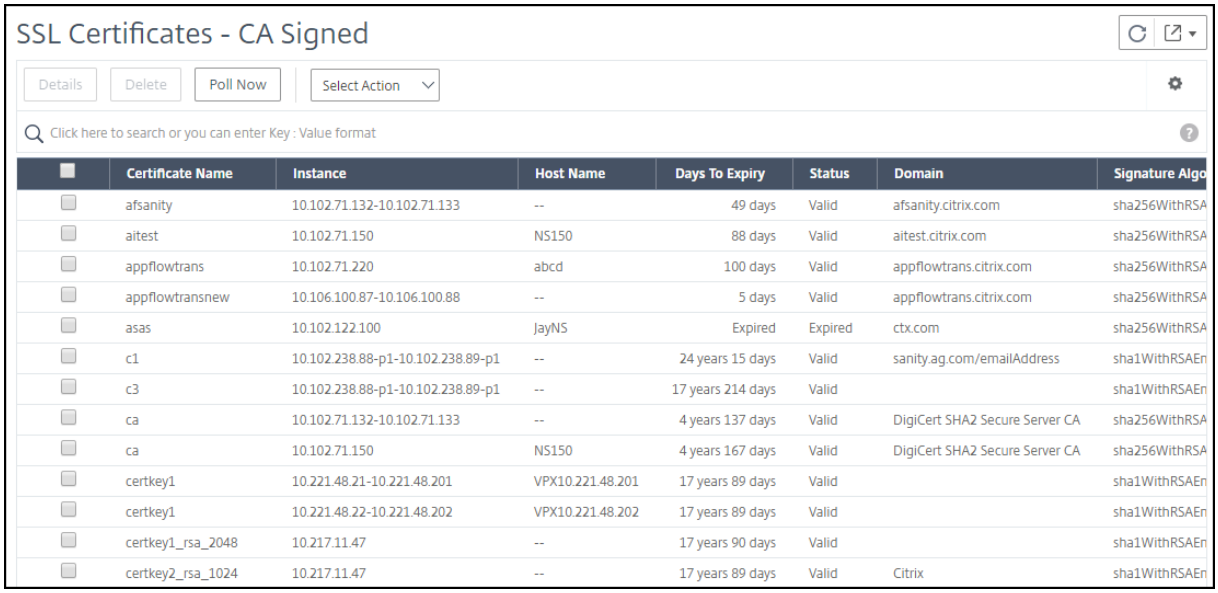


Mit NetScaler Console können Sie SSL-Zertifikate abfragen und alle SSL-Zertifikate der Instanzen sofort zur NetScaler Console hinzufügen. Navigieren Sie dazu zu **Infrastruktur > SSL Dashboard** und klicken Sie auf **Jetzt abfragen**. Die Seite **Jetzt abfragen** wird geöffnet und bietet die Option an, alle NetScaler-Instanzen im Netzwerk abzufragen oder ausgewählte Instanzen abzufragen.

Sie können das NetScaler Console SSL-Dashboard verwenden, um die Details von SSL-Zertifikaten, virtuellen SSL-Servern und SSL-Protokollen anzuzeigen oder zu überwachen. Die Zahlen sind Hyperlinks, auf die Sie klicken können, um Details zu SSL-Zertifikaten, virtuellen SSL-Servern oder SSL-Protokollen anzuzeigen.



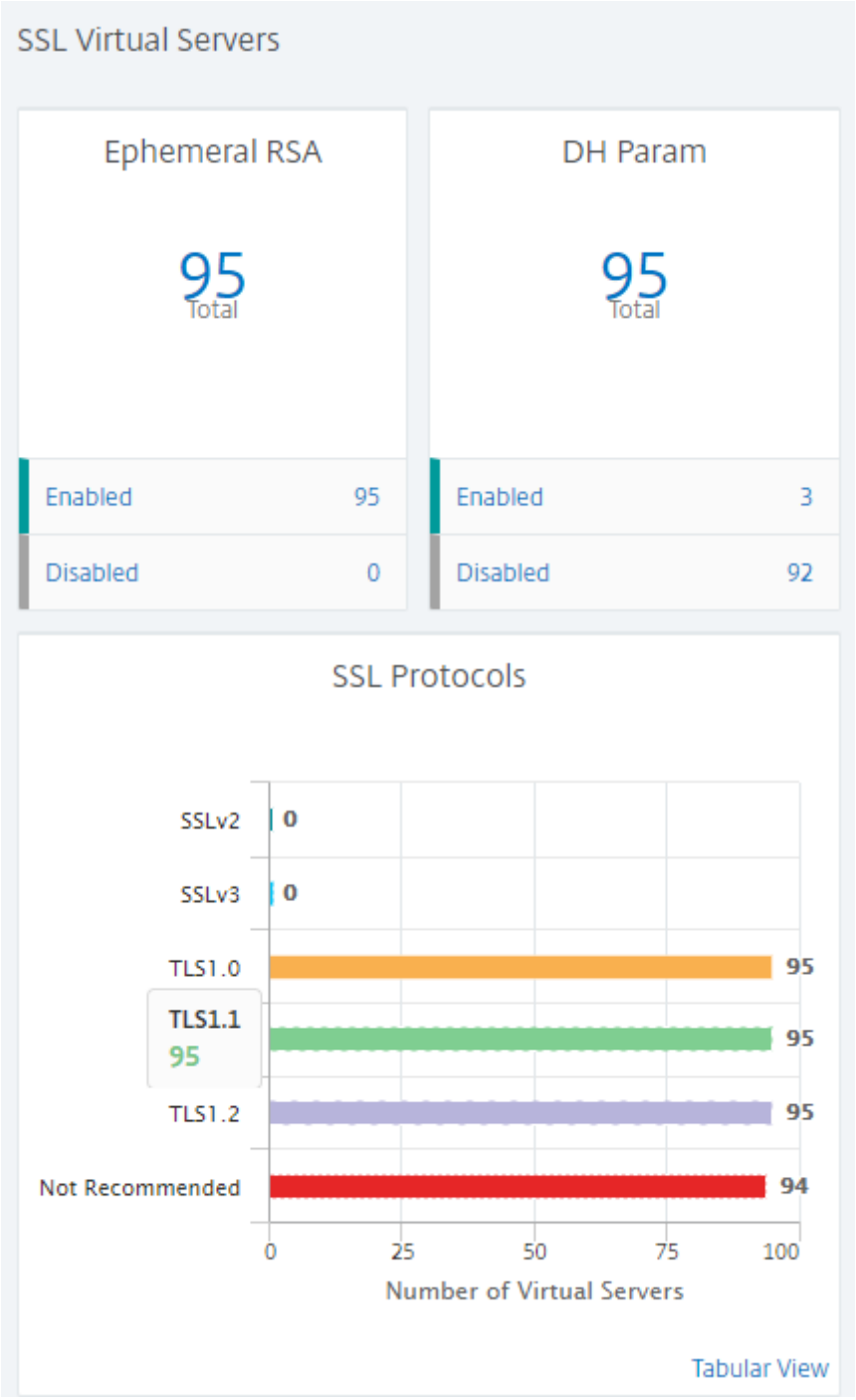
Zum Beispiel, wenn ein Benutzer auf die Zahl 30 klickt unter **Selbstsigniert vs. CA ist**in der obigen Abbildung angemeldet. Ein neues Fenster mit Details zu den 30 SSL-Zertifikaten auf den NetScaler-Instanzen wird angezeigt.



Certificate Name	Instance	Host Name	Days To Expiry	Status	Domain	Signature Algo
afsanity	10.102.71.132-10.102.71.133	--	49 days	Valid	afsanity.citrix.com	sha256WithRSA
aitest	10.102.71.150	NS150	88 days	Valid	aitest.citrix.com	sha256WithRSA
appflowtrans	10.102.71.220	abcd	100 days	Valid	appflowtrans.citrix.com	sha256WithRSA
appflowtransnew	10.106.100.87-10.106.100.88	--	5 days	Valid	appflowtrans.citrix.com	sha256WithRSA
asas	10.102.122.100	JayNS	Expired	Expired	ctx.com	sha256WithRSA
c1	10.102.238.88-p1-10.102.238.89-p1	--	24 years 15 days	Valid	sanity.ag.com/emailAddress	sha1WithRSAEn
c3	10.102.238.88-p1-10.102.238.89-p1	--	17 years 214 days	Valid		sha1WithRSAEn
ca	10.102.71.132-10.102.71.133	--	4 years 137 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
ca	10.102.71.150	NS150	4 years 167 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
certkey1	10.221.48.21-10.221.48.201	VPX10.221.48.201	17 years 89 days	Valid		sha1WithRSAEn
certkey1	10.221.48.22-10.221.48.202	VPX10.221.48.202	17 years 89 days	Valid		sha1WithRSAEn
certkey1_rsa_2048	10.217.11.47	--	17 years 90 days	Valid		sha1WithRSAEn
certkey2_rsa_1024	10.217.11.47	--	17 years 89 days	Valid	Citrix	sha1WithRSAEn

Das NetScaler Console SSL Dashboard zeigt auch die Verteilung der SSL-Protokolle, 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, TLS1.0, TLS1.1 und TLS1.2. 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.



Anzeigen von Überwachungsprotokollen für SSL-Zertifikate

Sie können jetzt die Protokolldetails von SSL-Zertifikaten in der NetScaler Console anzeigen. In den Protokolldetails werden Vorgänge angezeigt, die mit SSL-Zertifikaten in der NetScaler Console ausgeführt wurden, z. B.: Installieren von SSL-Zertifikaten, Verknüpfen und Aufheben der Verknüpfung von SSL-Zertifikaten, Aktualisieren von SSL-Zertifikaten und Löschen von SSL-Zertifikaten. Auditpro-

tokollinformationen sind nützlich, wenn Sie SSL-Zertifikatsänderungen überwachen, die an einer Anwendung mit mehreren Besitzern vorgenommen wurden.

Um ein Audit-Log für einen bestimmten Vorgang anzuzeigen, der auf NetScaler Console mithilfe von SSL-Zertifikaten ausgeführt wurde, navigieren Sie zu **Infrastruktur > SSL-Dashboard** und wählen Sie **Audit-Logs** aus.

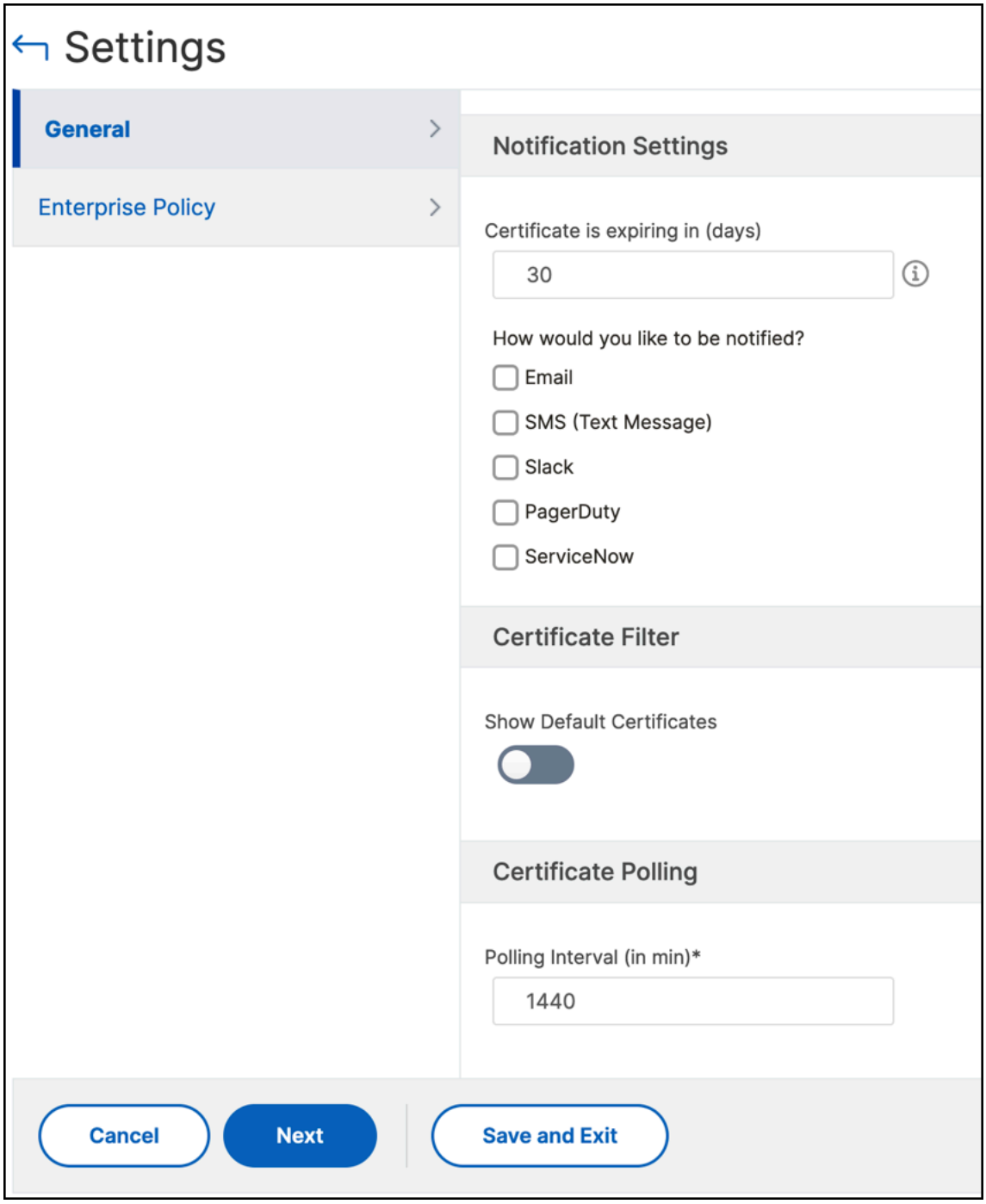
Für einen bestimmten Vorgang, der mit dem SSL-Zertifikat ausgeführt wird, können Sie den Status, die Startzeit und die Endzeit anzeigen. Darüber hinaus können Sie die Instanz anzeigen, für die der Vorgang ausgeführt wurde, und die Befehle, die für diese Instanz ausgeführt werden.

Ausschließen von NetScaler Standardzertifikaten auf dem SSL-Dashboard

Mit NetScaler Console können Sie Standardzertifikate, die in den SSL-Dashboard-Diagrammen angezeigt werden, je nach Ihren Einstellungen ein- oder ausblenden. Standardmäßig werden alle Zertifikate im SSL-Dashboard angezeigt, einschließlich Standardzertifikaten.

So blenden Sie Standardzertifikate auf dem SSL-Dashboard ein oder aus:

1. Navigieren Sie in der NetScaler Console-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. Deaktivieren Sie im Abschnitt **Zertifikatfilter** die **Standardzertifikate anzeigen**, und wählen Sie **Speichern und Beenden** aus.



SSL-Zertifikate herunterladen

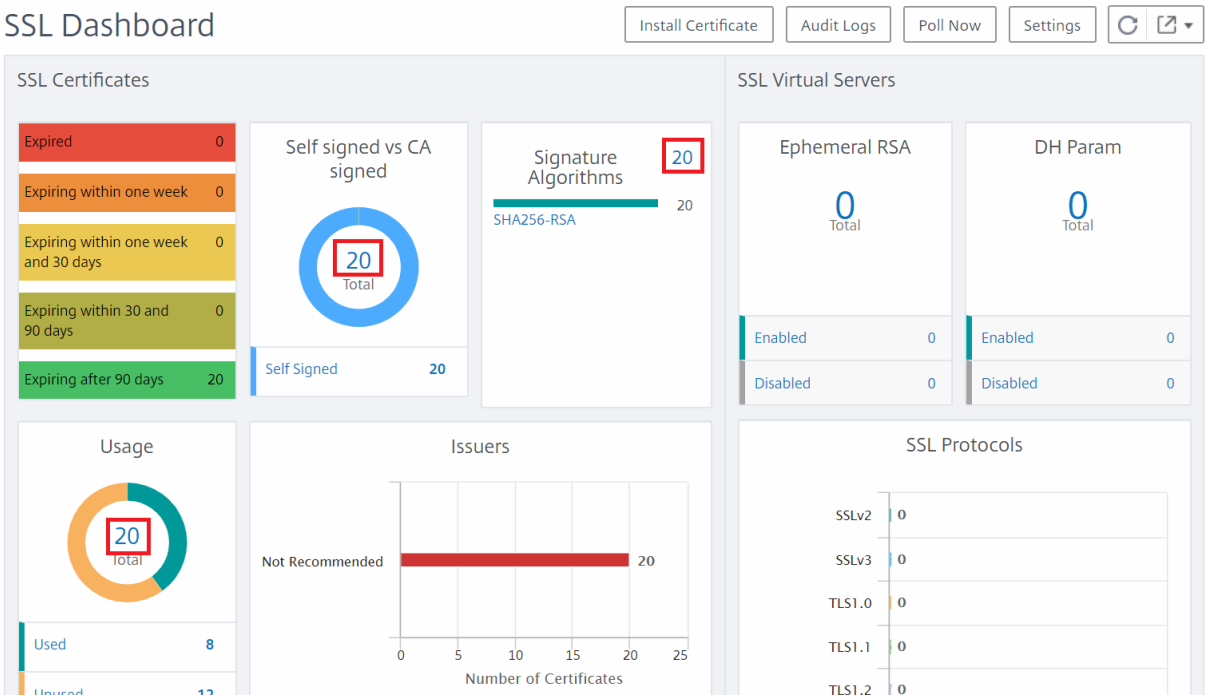
SSL-Zertifikate müssen pro Instanz individuell verwaltet werden. NetScaler Console bietet Einblick in alle Zertifikate, die auf mehreren Instanzen bereitgestellt werden.

- Sie können auswählen, welche Zertifikate ablaufen und Zertifikatverlängerungen automatisieren.

- Richtlinien können für die zulässigen Arten von Zertifikaten und Unterzeichnerbehörden festgelegt und durchgesetzt werden.
- Sie können die SSL-Zertifikate auch zur Verlängerung herunterladen und später hochladen.

So laden Sie SSL-Zertifikate herunter:

1. Navigieren Sie in der NetScaler Console-GUI zu **Infrastruktur > SSL-Dashboard** .
2. Klicken Sie auf der Seite **SSL Dashboard** auf die Gesamtzahl der SSL-Zertifikate in einem der Diagramme.



1. Klicken Sie auf der Seite **SSL-Zertifikate** auf das Zertifikat, das Sie herunterladen möchten. Sie möchten beispielsweise die Datei herunterladen, die in der nächsten Woche abläuft.
2. Wählen Sie im Listenfeld **Aktion auswählen** die Option **Download** aus.
   Das Zertifikat wird auf Ihr System heruntergeladen.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** . Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

Hinweis

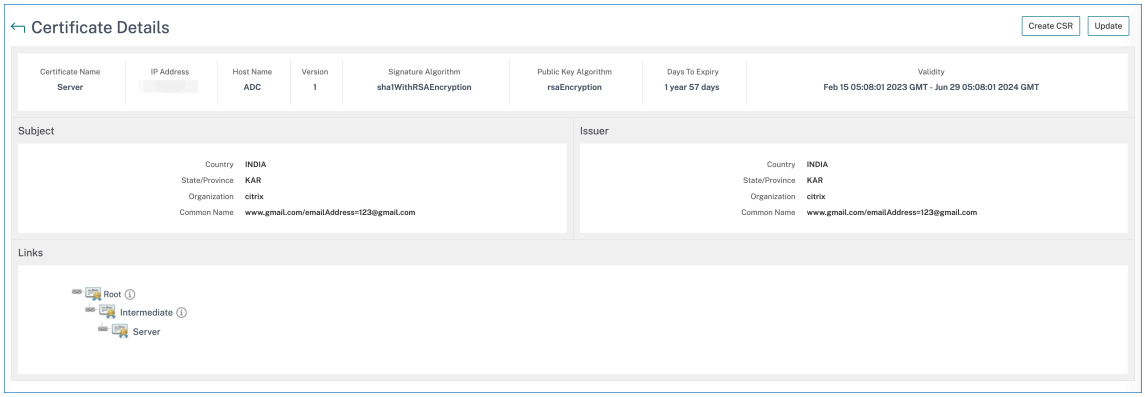
- Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

SSL-Zertifikatskette anzeigen

Sie können die komplette Linkkette für ein Zertifikat einsehen, einschließlich der Zwischenzertifikate bis hin zum Stammzertifikat der Zertifizierungsstelle.

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

May 9, 2024

Als Sicherheitsadministrator können Sie Benachrichtigungen konfigurieren, wenn die Zertifikate ablaufen, und Informationen darüber enthalten, welche NetScaler-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 der NetScaler Console aus ein:

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > SSL-Dashboard** .
2. Klicken Sie auf der Seite **SSL-Dashboard** auf **Einstellungen**.
3. Klicken Sie auf der Seite **Einstellungen** auf **Allgemein**.
4. Geben Sie im Abschnitt **Benachrichtigungseinstellungen** an, wann die Benachrichtigung in Bezug auf die Anzahl der Tage vor dem Ablaufdatum gesendet werden soll.
5. Wählen Sie die Art der Benachrichtigung, die Sie senden möchten. Wählen Sie den Benachrichtigungstyp und die Verteilerliste aus dem 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.
   - **Slack** – Gib ein Slack-Profil an Eine Benachrichtigung wird gesendet, wenn Ihre Zertifikate bald ablaufen.
   - **PagerDuty** - 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 Console integriert ist. Weitere Informationen finden Sie unter Integrieren der NetScaler Console in die ServiceNow-Instanz .
6. Klicken Sie auf **Speichern und Beenden**.

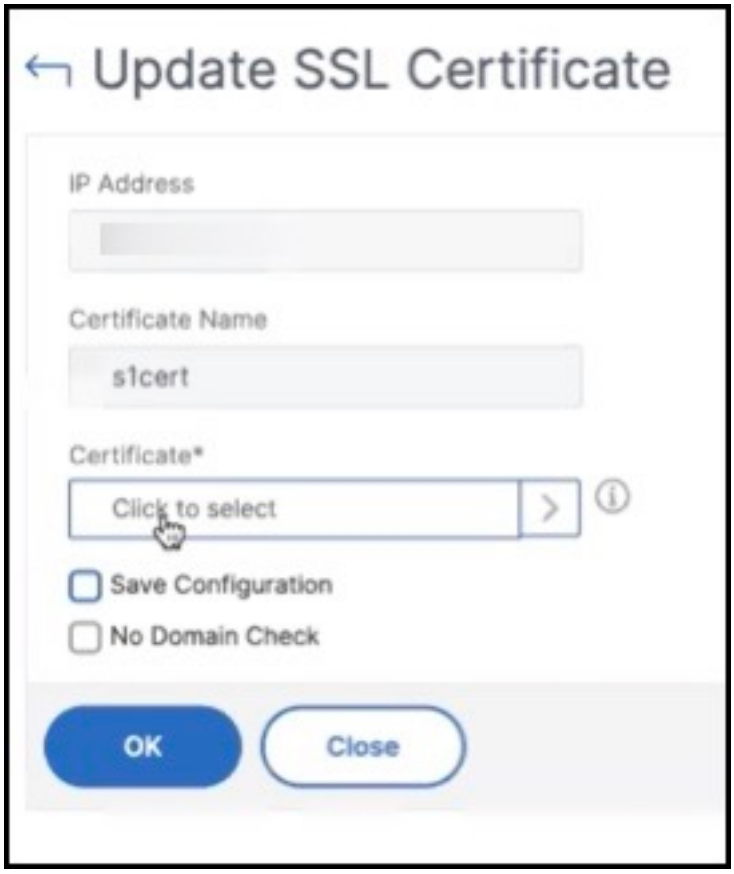
Installiertes Zertifikat aktualisieren

January 26, 2024

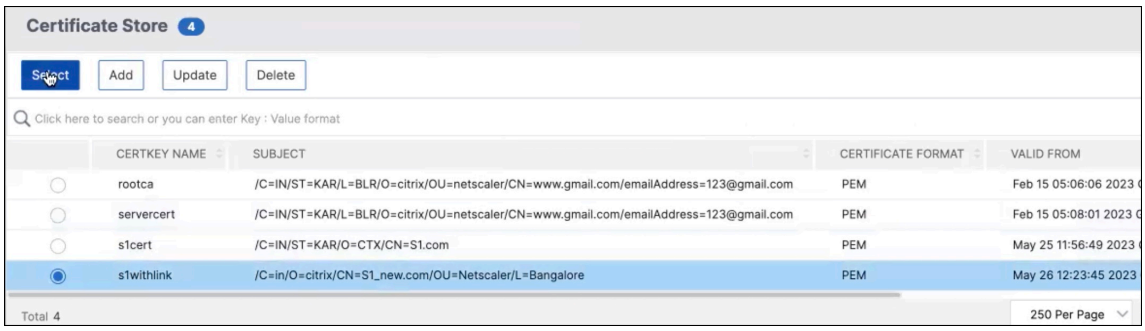
Nachdem Sie ein erneuertes Zertifikat von der Zertifizierungsstelle (CA) erhalten haben, müssen Sie sich nicht bei einzelnen NetScaler-Instanzen anmelden, um die Zertifikate zu aktualisieren. Sie können die vorhandenen Zertifikate in NetScaler Console mit Zertifikaten aus dem Zertifikatsspeicher aktualisieren.

So aktualisieren Sie ein SSL-Zertifikat von der NetScaler Console aus:

1. Navigieren Sie in der NetScaler Console 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.

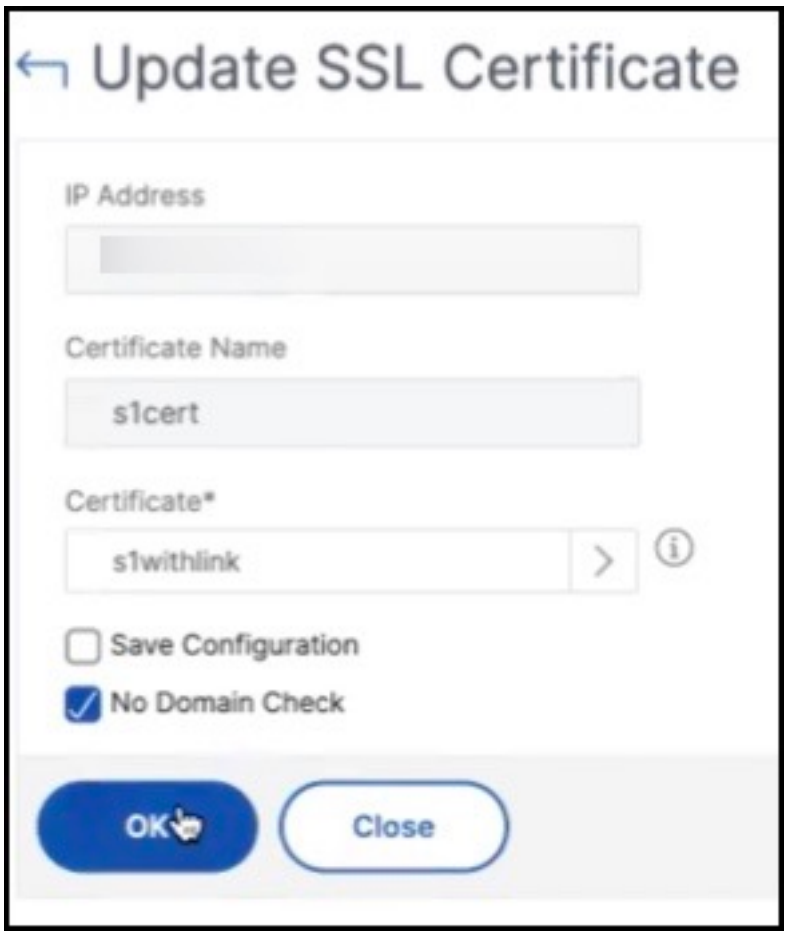


5. Wählen Sie auf der Seite „ **Zertifikatsspeicher** “die Zertifikatsdatei aus, die Sie hinzufügen möchten. Klicken Sie auf **Select**.



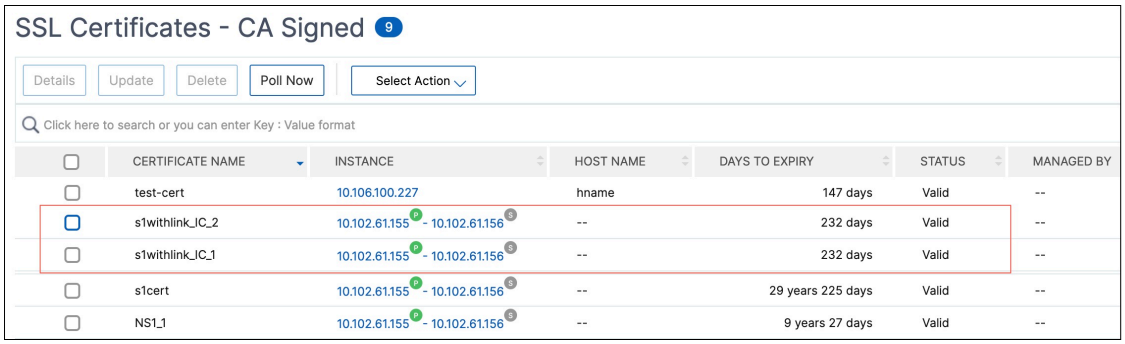
6. Wenn der Domänenname des neuen Zertifikats nicht mit dem alten Zertifikat übereinstimmt

und Sie möchten, dass der Server die neue Domäne hostet, wählen Sie **Keine Domänenprüfung** aus.

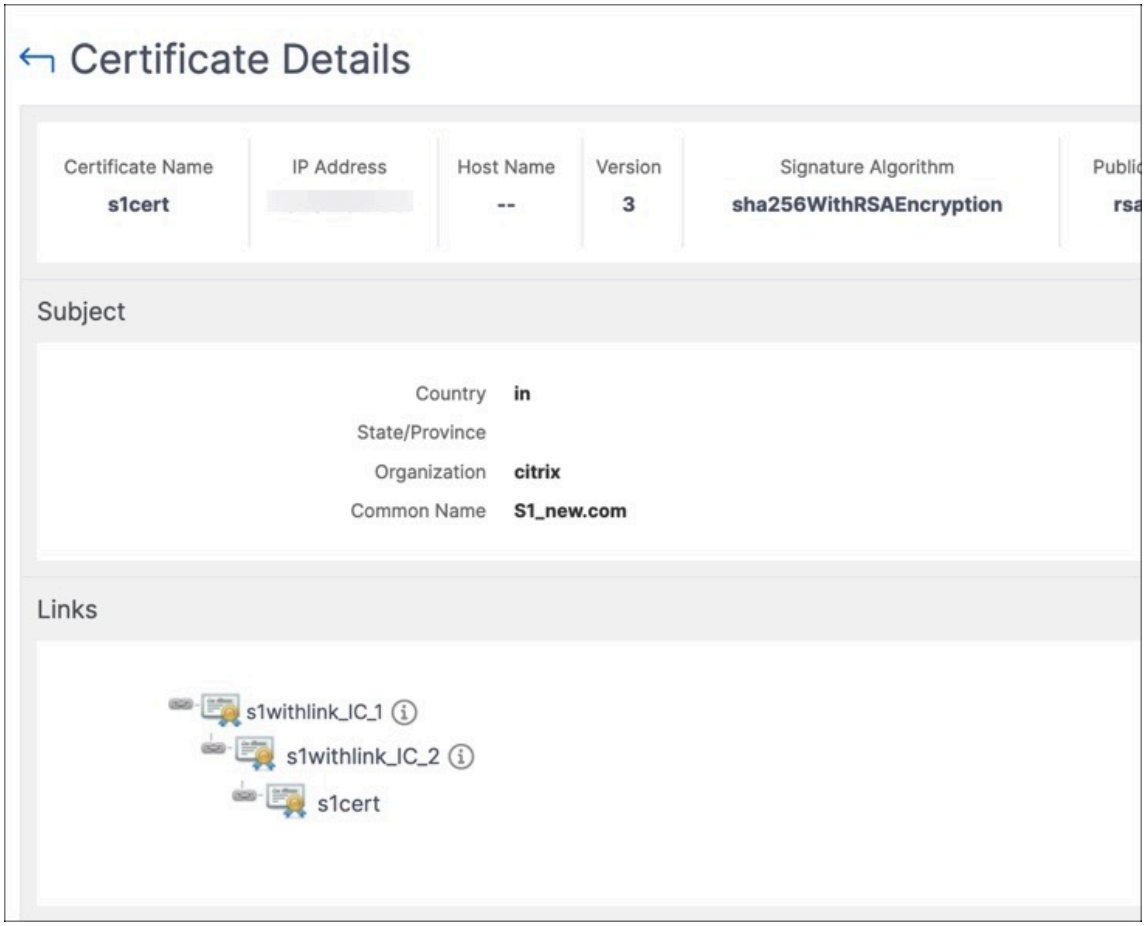


Klicken Sie auf **OK**. Alle virtuellen SSL-Server, an die dieses Zertifikat gebunden ist, werden automatisch aktualisiert.

Wenn Sie ein vorhandenes SSL-Zertifikat mit einer Zertifikatskette aus dem Zertifikatsspeicher 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

May 9, 2024

Stellen Sie vor der Installation von SSL-Zertifikaten auf NetScaler-Instanzen sicher, dass die Zertifikate von vertrauenswürdigen Zertifizierungsstellen ausgestellt werden. Stellen Sie außerdem sicher, dass die Schlüsselstärke der Zertifikatschlüssel 2.048 Bit oder höher beträgt und dass die Schlüssel mit sicheren Signaturalgorithmen signiert sind.

So installieren Sie ein SSL-Zertifikat von einer anderen NetScaler-Instanz:

Sie können auch ein Zertifikat von einer ausgewählten NetScaler-Instanz importieren und es über die NetScaler Console-GUI auf andere NetScaler-Zielinstanzen 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-Instanzen installieren** die folgenden Parameter an:

   a) Quelle des Zertifikats

   Wählen Sie die Option "**Aus Instanz importieren**".

   - 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) Einzelheiten zum Zertifikat

   - **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.

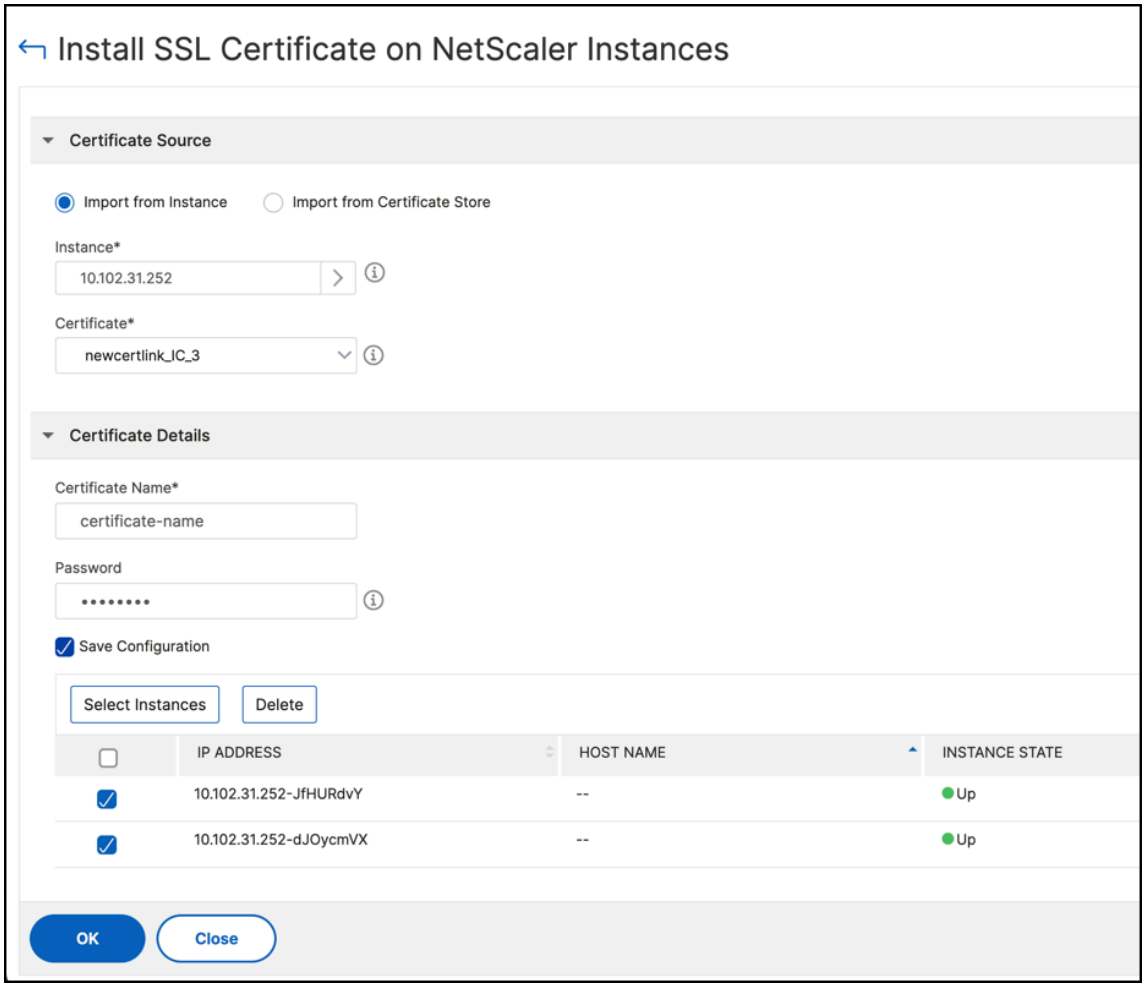
4. Klicken Sie auf **Instanzen auswählen**, um die NetScaler-Instanzen auszuwählen, auf denen Sie Ihre Zertifikate installieren möchten.
5. Klicken Sie auf OK.

So installieren Sie ein SSL-Zertifikat von NetScaler Console aus:

1. Navigieren Sie zu **Infrastruktur > SSL-Dashboard**.
2. Klicken Sie in der oberen rechten Ecke des Dashboards auf **Zertifikat installieren**.
3. Geben Sie auf der Seite **SSL-Zertifikat auf NetScaler-Instanz installieren** die folgenden Parameter an:

   - **Zertifikatdatei** − Laden Sie eine SSL-Zertifikatsdatei hoch, indem Sie entweder **Lokal** (Ihr lokaler Computer) oder **Appliance** auswählen (die Zertifikatdatei muss auf der NetScaler-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-Instanzen 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

May 9, 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. Sie enthält Informationen, die im Zertifikat enthalten sind, z. B. den Namen Ihrer Organisation, den allgemeinen Namen (Domänenname), den Ort und das Land.

So erstellen Sie eine CSR mit NetScaler Console:

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > SSL-Dashboard** .
2. Klicken Sie auf eines der Diagramme, um die Liste der installierten SSL-Zertifikate anzuzeigen, und wählen Sie dann das Zertifikat aus, für das Sie eine CSR erstellen möchten, und wählen Sie **CSR erstellen** aus der Dropdown-Liste **Aktion auswählen** aus.

3. Geben Sie auf der Seite **Certificate Signing Request (CSR)** einen Namen für die CSR an.
4. Führen Sie einen der folgenden Schritte aus:
    - **Schlüssel hochladen** − Wählen Sie die Option **Ich habe einen Schlüssel** aus. Um Ihre Schlüsseldatei hochzuladen, wählen Sie entweder **Lokal** (Ihr lokaler Computer) oder **Appliance** (die Schlüsseldatei muss auf der virtuellen NetScaler Console-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 wählen, 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>
```

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

January 26, 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 mit der "Domäne"von Zertifikat B übereinstimmen.

So verknüpfen Sie ein SSL-Zertifikat mit einem anderen Zertifikat mithilfe der NetScaler Console:

1. Navigieren Sie in der NetScaler Console 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 **Link** aus der Dropdown-Liste **Aktion auswählen** 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 der NetScaler Console auf:

1. Navigieren Sie in der NetScaler Console 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 in der Dropdown-Liste **Aktion auswählen die OptionVerknüpfung aufheben** 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

August 8, 2024

Sie können eine Unternehmensrichtlinie konfigurieren und alle vertrauenswürdigen CAs und sicheren Signaturalgorithmen hinzufügen und die empfohlene Schlüsselstärke für Ihre Zertifikatsschlüssel in NetScaler Console auswählen. Wenn eines der auf Ihrer NetScaler-Instanz installierten Zertifikate der Unternehmensrichtlinie nicht hinzugefügt wurde, zeigt das SSL-Zertifikat-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 der NetScaler Console:

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > SSL-Dashboard** , und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf der Seite “**Einstellungen** “auf das Symbol für **Unternehmensrichtlinien**, um alle vertrauenswürdigen Zertifizierungsalgorithmen und sichere Signaturalgorithmen hinzuzufügen und die empfohlene Schlüsselstärke für Ihre Zertifikate und Schlüssel auszuwählen. Unterstützte Hauptstärken sind 512, 1024, 2048, 3072 und 4096 Bit.

- **Empfohlene Schlüsselstärken** - Bezeichnet die Algorithmussicherheit und die Anzahl der Bits in einem Schlüssel.
- **Empfohlene Signaturalgorithmen** - Bezeichnet die signierten Token-Probleme für die Anwendungen.
- **Empfohlene Trusted CA** - Bezeichnet die vertrauenswürdige Entität, die die digitalen Zertifikate ausstellt. Klicken Sie auf das Symbol **+**, um weitere Entitys hinzuzufügen.
- **Empfohlene SSL-Protokolle** - Bezeichnet die TLS/SSL-Versionen.

3. Klicken Sie auf **Fertigstellen** oder **Speichern und Beenden**, um Ihre Unternehmensrichtlinie zu speichern.

> **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

May 9, 2024

NetScaler Console fragt mithilfe von NITRO-Aufrufen und dem Secure Copy (SCP) -Protokoll automatisch alle 24 Stunden SSL-Zertifikate ab. Sie können die SSL-Zertifikate auch manuell abfragen, um neu hinzugefügte SSL-Zertifikate auf den NetScaler-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 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 abzufragen oder ausgewählte Instanzen abzufragen.
    a) Um die SLL-Zertifikate aller NetScaler-Instanzen abzufragen, wählen Sie die Registerkarte **Alle Instanzen**, und klicken Sie auf **Abruf starten**.
4. Um bestimmte Instanzen abzufragen, wählen Sie den Tab **Instanzen auswählen** aus, wählen Sie die Instanzen aus der Liste aus und klicken Sie auf **Jetzt abfragen**.

Verwenden Sie den NetScaler Console-Zertifikatsspeicher, um SSL-Zertifikate zu verwalten

June 7, 2024

Der NetScaler Console-Zertifikatsspeicher hilft Ihnen, Ihre SSL-Zertifikate an einem Ort zu speichern und zu 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 **Löschen**.
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 **NetScaler-Zertifikate importieren**.
2. Auf der Seite **NetScaler-Zertifikate importieren** können Sie eine der folgenden Registerkarten auswählen:

   - **NetScaler-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 **NetScaler-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.

Konfigurationsaufträge

January 26, 2024

Der NetScaler Console-Konfigurationsmanagementprozess gewährleistet die korrekte Replikation von Konfigurationsänderungen, Systemaktualisierungen und anderen Wartungsaktivitäten auf mehreren NetScaler-Instanzen im Netzwerk.

Mit NetScaler Console können Sie Konfigurationsjobs erstellen, mit denen Sie all diese Aktivitäten mühelos auf mehreren Geräten als eine einzige Aufgabe ausführen können. Konfigurationsaufträge und Vorlagen vereinfachen die sich am häufigsten wiederholenden Verwaltungsaufgaben in einer einzigen Aufgabe auf der NetScaler Console. 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 Konfigurationsjob erstellen, indem Sie eine der folgenden vier Optionen in NetScaler Console 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. Weitere Informationen finden Sie unter So verwenden Sie die Masterkonfigurationsvorlage auf der NetScaler Console .

> **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 so planen, dass er zu einem späteren Zeitpunkt ausgeführt wird.

Weitere Informationen finden Sie unter Verwenden von Konfigurationsvorlagen zum Erstellen von Überwachungsvorlagen.

Instanz

Sie können ein Einzelbündel-Upgrade Ihrer NetScaler SDX-Instanzen mit NetScaler Version 11.0 und höher durchführen. Um ein Einzelpaket-Upgrade durchzuführen, verwenden Sie eine integrierte Aufgabe in NetScaler Console. 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. Dieses Upgrade ermöglicht es Ihnen, die Konfiguration einer Instanz auf der anderen zu replizieren.

Datei

Sie können eine Konfigurationsdatei von Ihrem lokalen Computer hochladen und 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 Job ausführen, werden Änderungen in der Datei ns.conf auf der ausgewählten Instanz aufgezeichnet und in die NetScaler Console kopiert. Weitere Informationen finden Sie unter Verwenden von Record and Play zum Erstellen von Konfigurationsaufträgen.

Exportieren Sie den Bericht dieses Dashboards

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** . Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder eine Slack-Nachricht zu senden.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Verwandte Artikel

- Verwendung des SCP (put) -Befehls in Konfigurationsjobs
- So verwenden Sie Variablen in Konfigurationsjobs
- So erstellen Sie Konfigurationsaufträge aus Korrekturbefehlen

Konfigurationsauftrags erstellen

January 26, 2024

Ein Auftrag ist eine Reihe von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen erstellen und ausführen können.

Sie können Jobs erstellen, um Konfigurationsänderungen über Instanzen hinweg vorzunehmen. Sie können Konfigurationen [auf mehreren Instanzen in Ihrem Netzwerk replizieren](/de-de/netscaler-console-service/networks/configuration-jobs/replicate-configuration.html) und Konfigurationsaufgaben mithilfe der NetScaler Console-GUI aufzeichnen und abspielen und in CLI-Befehle konvertieren.

Sie können die Funktion „Konfigurationsaufträge“der NetScaler Console verwenden, um einen Konfigurationsjob zu erstellen, E-Mail-Benachrichtigungen zu senden und die Ausführungsprotokolle der erstellten Jobs zu überprüfen.

So erstellen Sie einen Konfigurationsjob auf der NetScaler Console:

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsjobs**.
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 Auftragsvorlage "Masterkonfiguration bereitstellen"zum ersten Mal hinzufügen und eine Vorlage eines anderen Typs hinzufügen, wird die gesamte Auftragsvorlage zu einem Master-Konfigurationstyp.

Sie können die Befehle auch im Konfigurationseditor neu anordnen und neu anordnen. Sie können den Befehl von einer Zeile in eine andere verschieben, indem Sie die Befehlszeile ziehen und 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 Konfigurationsjobs 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.

b) Klicken Sie auf **Instanzen hinzufügen**, und wählen Sie die Instanzen aus der Liste aus. Klicken Sie auf **OK**.

c) Klicken Sie auf **Weiter**.

6. **Auf der Registerkarte „ Variablenwerte angeben** “haben Sie zwei Optionen:

a) Laden Sie die Eingabedatei herunter, um die Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den NetScaler Console-Server hoch.

b) Geben Sie gemeinsame Werte für die Variablen ein, die Sie für alle Instanzen definiert haben

c) Klicken Sie auf **Weiter**.

7. Bewerten und überprüfen Sie die Befehle, die für jede Instanz auf der Registerkarte **Job-Vorschau** ausgeführt werden sollen. Auf dieser Registerkarte werden auch die Rollback-Befehle angezeigt, wenn sie auf der Registerkarte **Konfiguration auswählen** angegeben sind.
8. Wählen Sie auf der Registerkarte **Ausführen**, ob Sie Ihren Job jetzt ausführen möchten, oder planen Sie, den Job später auszuführen.

   Wählen Sie außerdem eine der folgenden Aktionen aus der Liste **On Command Failure** aus, die NetScaler Console ausführen muss, wenn der Befehl fehlschlägt:

   - **Fehler ignorieren und fortfahren**: NetScaler Console ignoriert den fehlgeschlagenen Befehl und führt die verbleibenden Befehle für die ausgewählte Instanz aus.

     > **Hinweis:**
     >
     > Mit dieser Aktion können Sie einen Konfigurationsauftrag abbrechen, der gerade ausgeführt wird.

   - **Weitere Ausführung**beenden : NetScaler Console stoppt die verbleibenden Befehle, wenn ein Befehl während der Ausführung fehlschlägt.

- **Erfolgreiche Befehle**rückgängig machen : NetScaler Console stellt die erfolgreich ausgeführten Befehle wieder her, wenn ein Befehl während der Ausführung fehlschlägt.

  Wenn das benutzerdefinierte Rollback aktiviert ist, führt die NetScaler Console die entsprechenden Rollback-Befehle für die fehlgeschlagenen Befehle aus.

9. Klicken Sie auf **Fertig stellen**.

So senden Sie eine E-Mail und eine Slack Benachrichtigung für einen Job:

Eine E-Mail- und Slack-Benachrichtigung wird jetzt jedes Mal gesendet, wenn ein Job ausgeführt oder geplant wird. Die Benachrichtigung enthält Details wie den Erfolg oder Misserfolg des Auftrags sowie die relevanten Details.

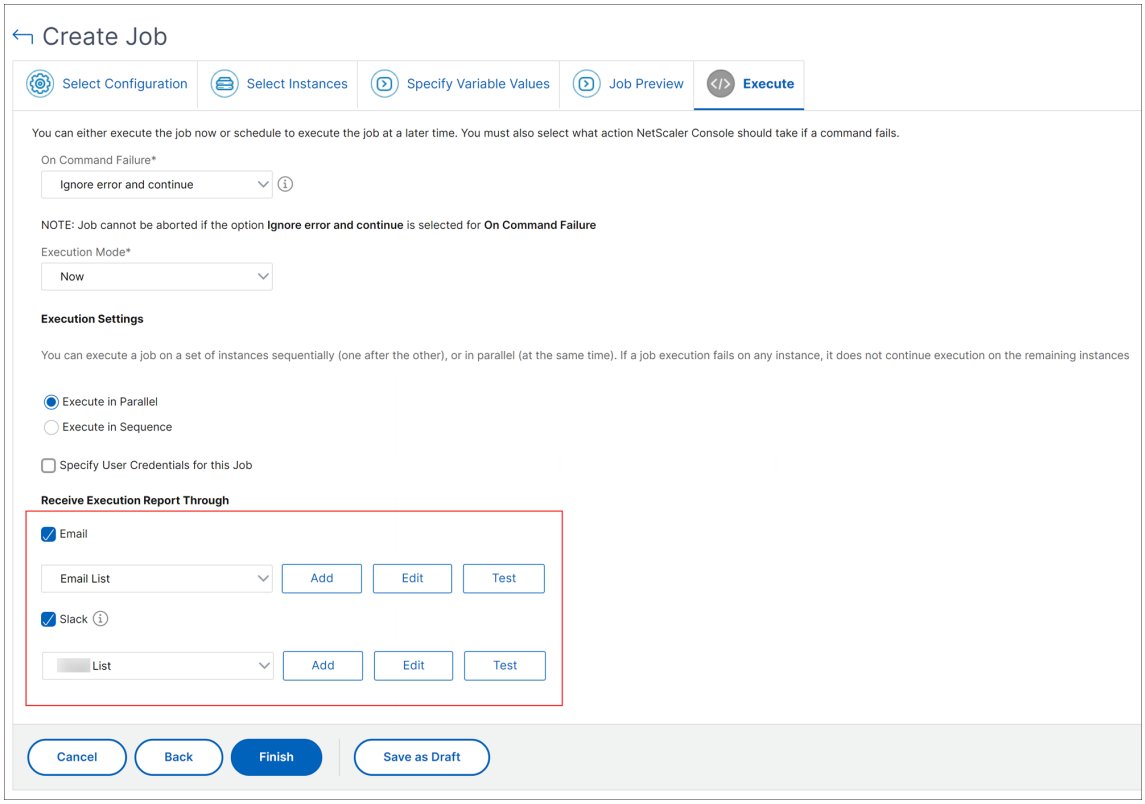
1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsaufträge**.
2. Wählen Sie den Job aus, den Sie E-Mail- und Slack -Benachrichtigung aktivieren möchten, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Registerkarte **Ausführen** zum Bereich **Ausführungsbericht empfangen 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.

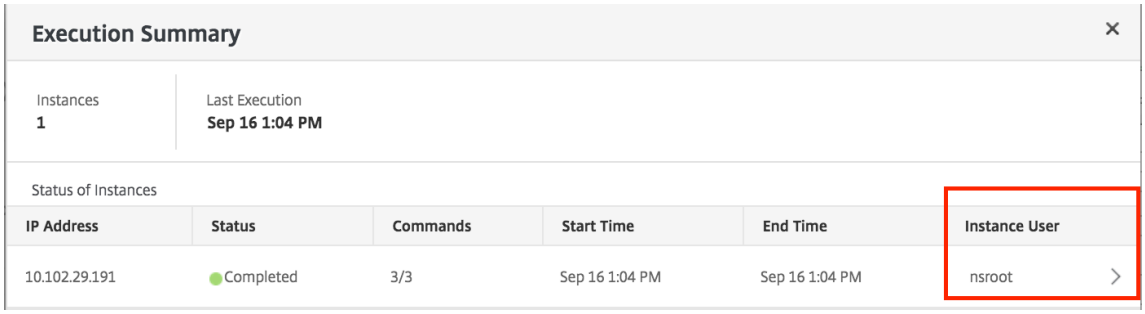
     Wenn Sie ein Slack -Profil hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie den **Profilnamen**, den **Kanalnamen** und das **Token** des erforderlichen Slack-Kanals an.



4. Klicken Sie auf **Fertig stellen**.

So zeigen Sie Details zur Ausführungszusammenfassung an:

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsaufträge**.
2. Wählen Sie den Job aus, den Sie die Ausführungszusammenfassung anzeigen möchten, und klicken Sie auf **Details**.
3. Klicken Sie auf **Ausführungsübersicht**, um Folgendes anzuzeigen:
   - Der Status der Instanz des Jobs, der ausgeführt wurde
   - Die Befehle werden für den Auftrag ausgeführt
   - Die Start- und Endzeit des Auftrags und
   - Der Name des Instanzbenutzers



Konfigurationsaudit

January 26, 2024

Dieses Dokument beinhaltet:

- Audit-Vorlagen erstellen
- Auditberichte anzeigen
- Konfigurationsänderungen über alle Instanzen hinweg überwachen
- Konfigurationshinweise zur Netzwerkkonfiguration erhalten
- So rufen Sie die Konfigurationsüberprüfung von NetScaler Console-Instanzen ab
- Konfigurations-Audit-Diff für ConfigChange SNMP-Traps generieren

Upgradeaufträge

January 26, 2024

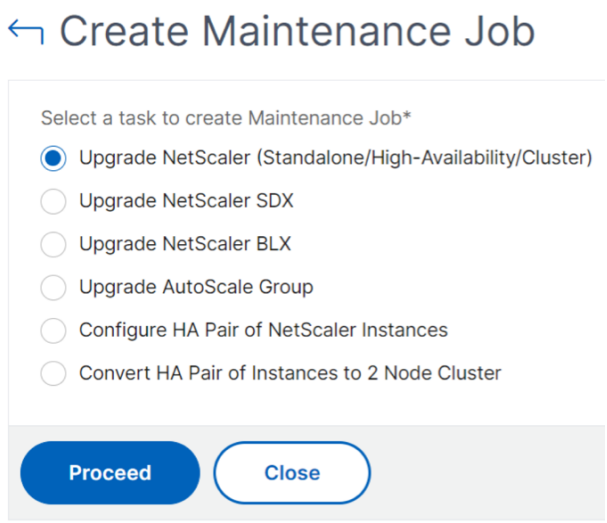
Sie können die folgenden Wartungsaufgaben mit NetScaler Console erstellen. Anschließend können Sie die Wartungsaufgaben zu einem bestimmten Datum und einer bestimmten Uhrzeit planen.

- 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

Planen des Upgrades von NetScaler-Instanzen

1. Navigieren Sie in der NetScaler Console 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 NetScaler-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 Instanz-Upgrade-Datei in einem NetScaler Console-Dateibrowser aus. Die NetScaler Console-GUI zeigt die Instanzdateien an`/var/mps/mps_images`, die unter vorhanden sind.
        - **Das Hochladen von Bildern auf NetScaler überspringen, wenn das ausgewählte Bild bereits verfügbar**ist —Wählen Sie diese Option, wenn das Bild 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 NetScaler-Instanz nach dem Instanzupgrade zu löschen.

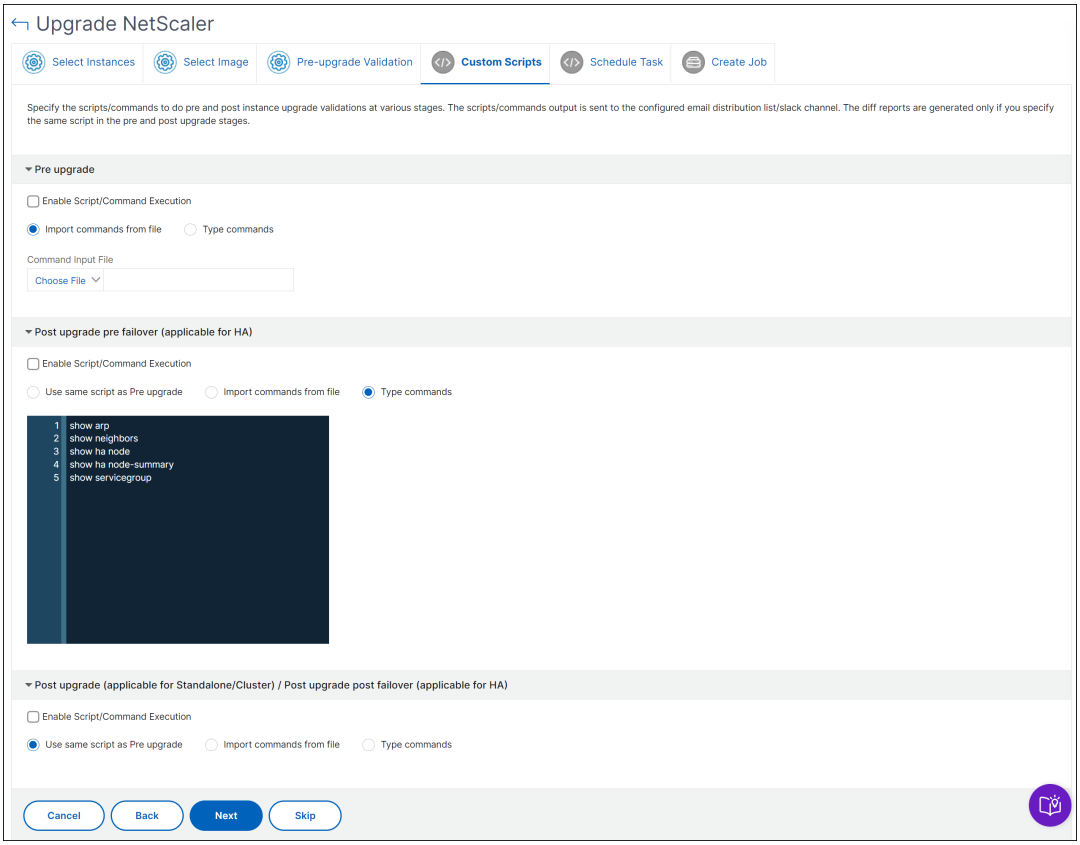
6. Klicken Sie auf **Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten.

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 eine Cluster-IP-Adresse angeben, führt die NetScaler Console die Validierung vor dem Upgrade nur auf der angegebenen 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.

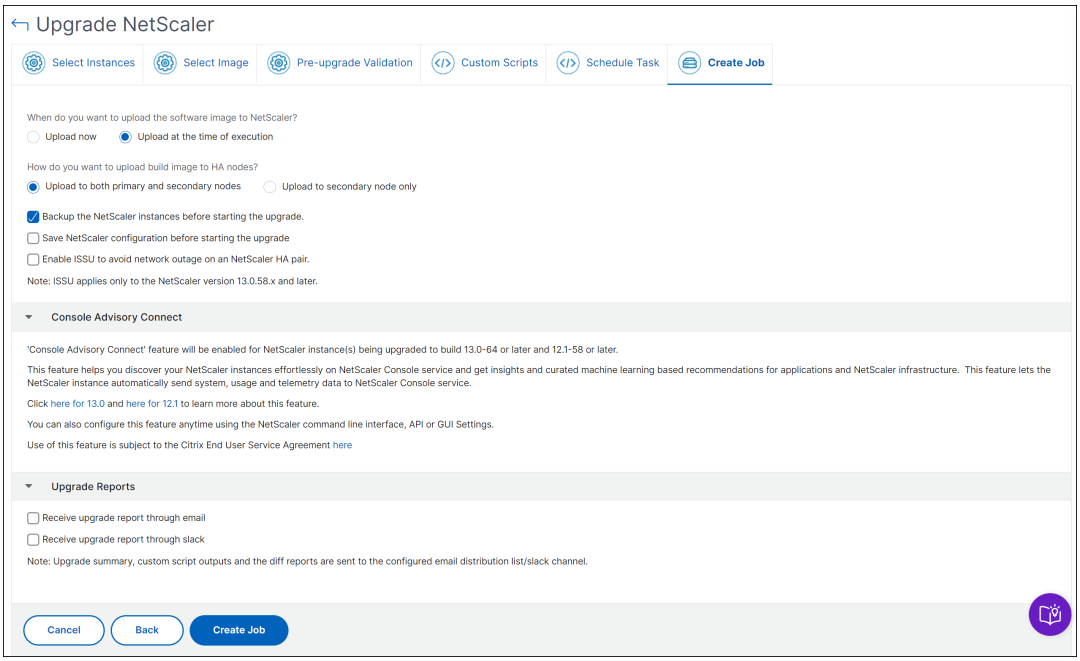
- Der Status von Schnittstellen, Hochverfügbarkeitsknoten, virtuellen Servern und Diensten vor und nach dem Upgrade.
- Die Statistik der virtuellen Server und Dienste.
- Die dynamischen Routen.

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 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. 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 NetScaler-Instanzen, bevor Sie das Upgrade starten.** - Erstellt ein Backup der ausgewählten NetScaler-Instanzen.
      - **NetScaler-Konfiguration vor dem Upgrade**speichern —Speichert die Konfigurationsaufträge, die vor dem Upgrade auf der Instanz konfiguriert wurden.
      - **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. Sie können also ein NetScaler HA-Paar ohne Ausfallzeiten aktualisieren. Geben Sie das Timeout der ISSU Migration in Minuten an.
   - **Console Advisory Connect**—Wenn Sie ein Upgrade auf Build **13.0-64 oder** höher und **12.1-58 oder** höher durchführen, wird Console Advisory Connect automatisch aktiviert. Weitere Informationen finden Sie unter Low-Touch-Onboarding von NetScaler-Instanzen mithilfe von NetScaler Console 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. Navigieren Sie in der NetScaler Console 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** aus (die Build-Datei muss auf der virtuellen NetScaler Console-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. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail** empfangen und **Ausführungsbericht über Pufferzeit** empfangen, um die Benachrichtigungen zu aktivieren.

   Weitere Informationen zum Konfigurieren der E-Mail-Verteilerliste und des Slack-Channels finden Sie in **Schritt 8** unter Planen des Upgrades von NetScaler-Instanzen.

Planen Sie das Upgrade von NetScaler BLX-Instanzen

1. Navigieren Sie in der NetScaler Console 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 Instanz-Upgrade-Datei in einem NetScaler Console-Dateibrowser aus. Die NetScaler Console-GUI zeigt die Instanzdateien an`/var/mps/mps_images`, die unter vorhanden sind.
     - **Das Hochladen von Bildern auf NetScaler überspringen, wenn das ausgewählte Bild bereits verfügbar**ist —Wählen Sie diese Option, wenn das Bild 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 NetScaler-Instanz nach dem Instanzupgrade zu löschen.

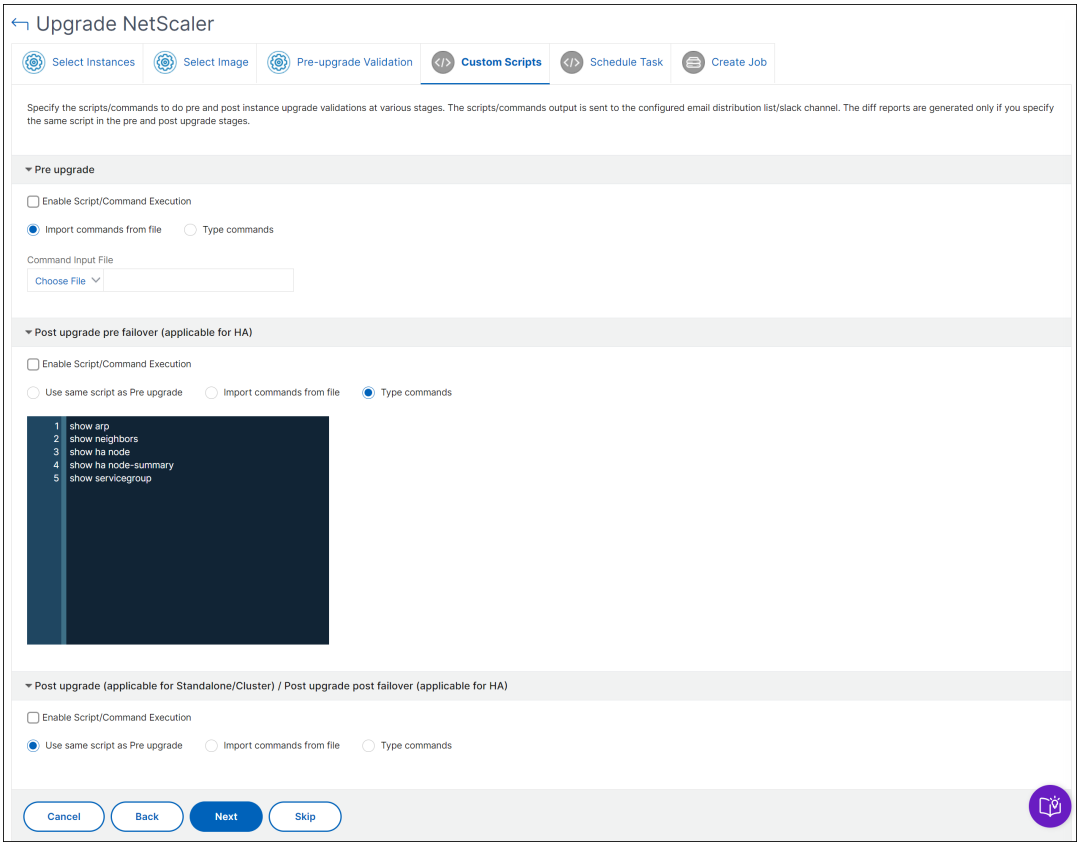
6. Klicken Sie auf **Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten.

   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 eine Cluster-IP-Adresse angeben, führt die NetScaler Console die Validierung vor dem Upgrade nur auf der angegebenen 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.
      - **Sichern Sie die NetScaler-Instanzen, bevor Sie das Upgrade**starten —Erstellt eine Backup der ausgewählten NetScaler-Instanzen.
      - **Speichert die NetScaler-Konfiguration vor dem Start**des Upgrades —Speichert die Konfigurationsaufträge, die vor dem Upgrade auf der Instanz konfiguriert wurden.
      - **Aktivieren Sie ISSU, um Netzwerkausfälle auf dem NetScaler HA-Paar**zu vermeiden —ISSU gewährleistet das Upgrade ohne Ausfallzeiten auf einem NetScaler-Hochverfügbarkeitspaar. Diese Option bietet eine Migrationsfunktionalität, die die vorhandenen Verbindungen während des Upgrades berücksichtigt. Sie können also ein NetScaler HA-Paar ohne Ausfallzeiten aktualisieren. Geben Sie das Timeout der ISSU Migration in Minuten an.

- **Console Advisory Connect**—Wenn Sie ein Upgrade auf Build **13.0-64 oder** höher und **12.1-58 oder** höher durchführen, wird Console Advisory Connect automatisch aktiviert. Weitere Informationen finden Sie unter Low-Touch-Onboarding von NetScaler-Instanzen mithilfe von Console Advisory 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. Navigieren Sie in der NetScaler Console 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. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail** empfangen und **Ausführungsbericht über Pufferzeit** empfangen, um die Benachrichtigungen zu aktivieren.

5. Klicken Sie auf **Fertig stellen**.

Planen der Konfiguration des HA-Paares von NetScaler-Instanzen

1. Navigieren Sie in der NetScaler Console 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) Geben Sie die primäre IP-Adresse ein.
   c) Geben Sie die sekundäre IP-Adresse ein.
   d) Klicken Sie auf **Weiter**.
   e) Klicken Sie hier, um **den INC-Modus (Independent Network Configuration)** zu aktivieren, wenn die HA-Paarinstanzen in zwei Subnetzen vorhanden sind.
4. Wählen Sie auf der Registerkarte **Task planen** in der Liste **Ausführungsmodus** die Option **Jetzt** aus, um eine 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 **Ausführungsmodus** aus. Anschließend können Sie 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 zur Erstellung des NetScaler HA-Paars zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail** empfangen und **Ausführungsbericht über Pufferzeit** 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 .

Planen Sie die Konvertierung von HA-Instanzen in Cluster

1. Navigieren Sie in der NetScaler Console 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. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail** empfangen und **Ausführungsbericht über Pufferzeit** 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

September 2, 2024

In der NetScaler Console können Sie eine oder mehrere NetScaler-Instanzen aktualisieren. Sie müssen das Lizenzierungsframework und die Lizenztypen kennen, bevor Sie eine Instanz aktualisieren.

HINWEIS: Wenn Sie eine Instanz mit klassischen Richtlinien aktualisieren möchten, empfehlen wir Ihnen, die klassischen Richtlinien in erweiterte Richtlinien zu konvertieren, bevor Sie die Instanz mithilfe des NSPEPI-Tools aktualisieren. Dies gilt für die Funktionen, die vom NSPEPI-Tool unterstützt werden. Weitere Informationen finden Sie unter Überlegungen zum Upgrade für Konfigurationen mit klassischen Richtlinien.

Voraussetzungen

NetScaler Console führt die folgenden Vorabvalidierungsprüfungen für die Instanz durch, die Sie aktualisieren möchten:

1. **Speicherplatz prüfen** − Bereinigen Sie den Speicherplatz, damit genügend Datenträgerkapazität für ein Instanz-Upgrade zur Verfügung steht. Beheben Sie etwaige Datenträgerprobleme.
2. **Überprüfen Sie auf Datenträger-Hardwareprobleme** - Beheben Sie ggf. die Hardwareprobleme.
3. Auf**Anpassungen prüfen** - Sichern Sie Ihre Anpassungen, und löschen Sie sie aus den Instanzen. Sie können die gesicherte Anpassung nach dem Instanz-Upgrade erneut anwenden.
4. **Richtlinienprobleme**− NetScaler unterstützt keine klassischen Richtlinien ab Version `13.1`. Bevor Sie eine Instanz auf diese Version aktualisieren, migrieren Sie klassische Richtlinien zu erweiterten Richtlinien.

   Weitere Informationen finden Sie unter Klassische und erweiterte Richtlinien.

Überlegungen zum Upgrade für benutzerdefinierte NetScaler-Konfigurationen

Es ist wichtig, dass sowohl die Upgrade-Änderungen als auch Ihre Anpassungen auf eine aktualisierte NetScaler Appliance angewendet werden. Wenn Sie also benutzerdefinierte Konfigurationsdateien im Verzeichnis /etc haben, lesen Sie die Hinweise zum Upgrade für benutzerdefinierte Konfigurationsdateien, bevor Sie mit dem Upgrade der NetScaler Appliance fortfahren. Im Folgenden sind die wichtigsten Schritte aufgeführt, die Sie ausführen müssen:

1. Schritte vor dem Upgrade in NetScaler
   - Erstellen Sie vor dem Upgrade ein Backup
   - Löschen Sie den Symlink der angepassten Datei vor dem Upgrade
2. Aktualisieren Sie NetScaler mithilfe von ADM. Um ein Upgrade durchzuführen, folgen Sie den Anweisungen am Anfang der Seite.
3. Schritte nach dem Upgrade in NetScaler
   - Stellen Sie Anpassungen nach dem Upgrade wieder her

Sowohl die Schritte vor dem Upgrade als auch nach dem Upgrade müssen auf jeder NetScaler-Instanz ausgeführt werden. In Schritt 2, um NetScaler mithilfe von ADM zu aktualisieren, können jedoch alle anfälligen NetScaler-Instanzen ausgewählt und zusammen aktualisiert werden.

NetScaler Hochverfügbarkeitspaar

Beachten Sie beim Upgrade eines NetScaler-Hochverfügbarkeitspaars Folgendes:

- Der sekundäre Knoten wird zuerst aktualisiert.
- Synchronisation und Weitergabe der Knoten werden deaktiviert, bis beide Knoten erfolgreich aktualisiert wurden.
- Nach dem erfolgreichen Hochverfügbarkeitspaar-Upgrade wird eine Fehlermeldung in der Ausführungshistorie angezeigt. Diese Meldung wird angezeigt, wenn sich Ihre Knoten im Hochverfügbarkeitspaar auf verschiedenen Builds oder Versionen befinden. Es zeigt an, dass die Synchronisation zwischen primären und sekundären Knoten deaktiviert ist.

Sie können ein NetScaler-Hochverfügbarkeitspaar 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.

NetScaler Cluster

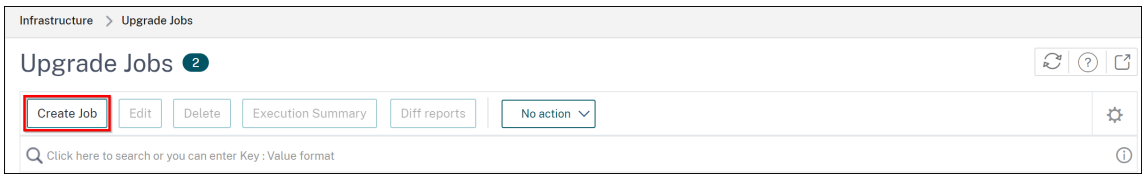
Wenn Sie einen NetScaler-Cluster aktualisieren, validiert die NetScaler Console in der Validierungsphase vor dem Upgrade nur die angegebene Instanz. Überprüfen und beheben Sie daher die folgenden Probleme auf den Clusterknoten:

- Anpassung
- Datenträgernutzung
- Hardware-Probleme

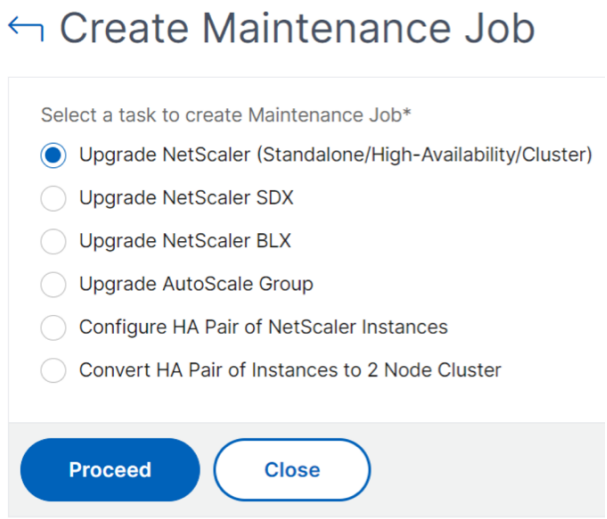
Erstellen Sie einen NetScaler-Upgrade-Job

Gehen Sie wie folgt vor, um einen NetScaler-Upgrade-Job zu erstellen:

1. Gehen Sie zu **Infrastruktur > Upgrade-Jobs**.



2. Wählen Sie unter **Wartungsaufträge erstellen**die Option **NetScaler (Standalone/Hochverfügbarkeit/Cluster) aktualisieren** aus und klicken Sie auf **Fortfahren**.



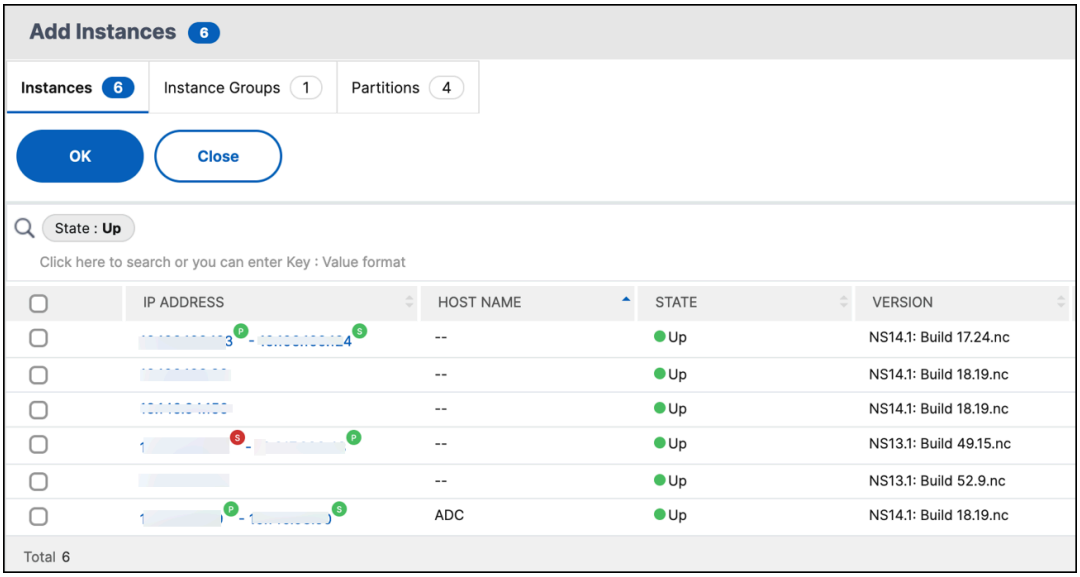
> **Hinweis:**
>
> Informationen zum Upgrade von Autoscale-Gruppen finden Sie unter Aktualisieren einer Autoscale-Gruppe .

3. Auf der Registerkarte **Instanzen auswählen**

   a) Geben Sie für **Job Name einen Namen**Ihrer Wahl an.

   b) Klicken Sie auf **Instanzen hinzufügen**, um NetScaler-Instanzen hinzuzufügen, die Sie aktualisieren möchten.

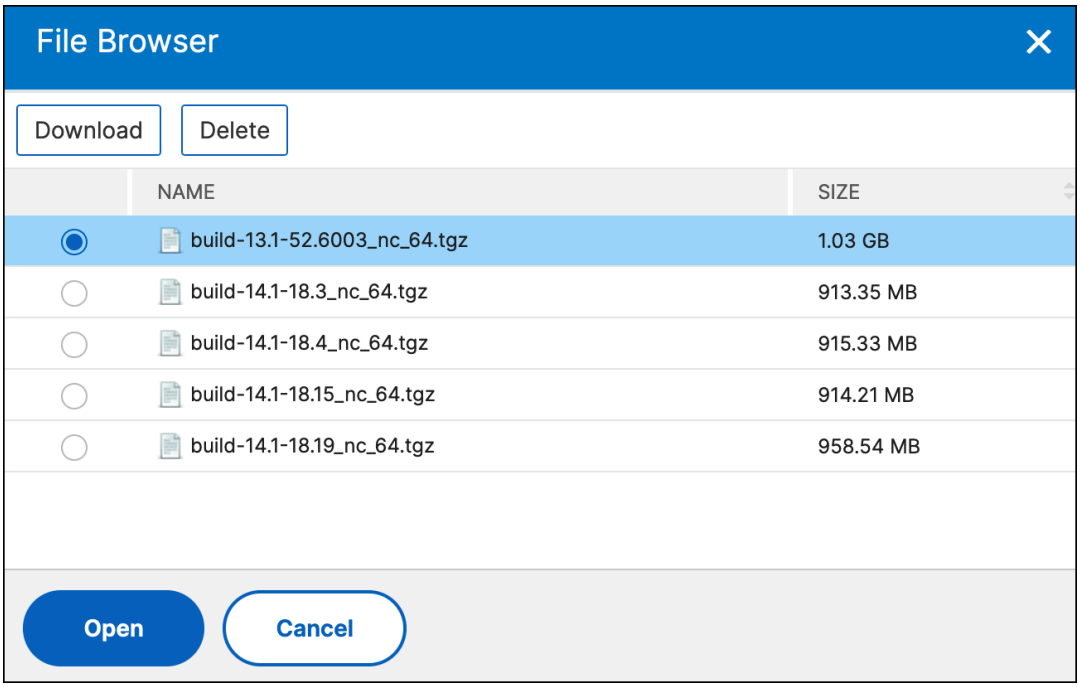
      - Um ein NetScaler-Hochverfügbarkeitspaar zu aktualisieren, wählen Sie die IP-Adressen des Hochverfügbarkeitspaars aus (gekennzeichnet durch das hochgestellte Zeichen ‘S’und ‘P’).
      - Um einen Cluster zu aktualisieren, wählen Sie die Cluster-IP-Adresse aus (gekennzeichnet durch das hochgestellte Zeichen von ‘C’).



c) Klicken Sie auf **OK**.

4. Wählen Sie auf der Registerkarte **Select Image** ein NetScaler-Image aus der Image-Bibliothek oder lokal oder Appliance aus.

   - **Aus Bildbibliothek**auswählen : Wählen Sie ein NetScaler-Image aus der Liste aus. Diese Option listet alle NetScaler-Images auf, die auf der NetScaler-Download-Website verfügbar sind.



Die NetScaler-Software-Images zeigen die bevorzugten Builds mit dem Sternsymbol an. Und die meisten heruntergeladenen Builds mit dem Lesezeichen-Symbol.

- **Wählen Sie zwischen lokal oder Appliance**: Sie können das Image von Ihrem lokalen Computer oder der NetScaler Appliance hochladen. Wenn Sie NetScaler Appliance auswählen, zeigt die NetScaler Console-GUI die Instanzdateien an, die in `/var/mps/ns_images`enthalten sind. Wählen Sie das Image in der NetScaler Console-GUI aus.
- **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.

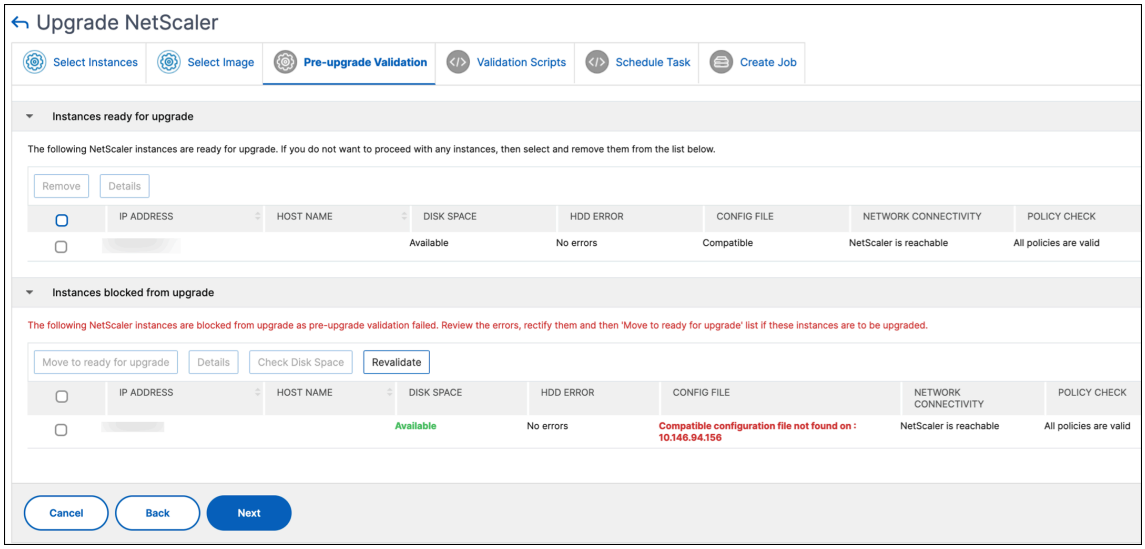
Klicken Sie auf **Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten.

> **Hinweis:**
>
> - Die heruntergeladenen NetScaler-Images werden im Agenten gespeichert und sind in `/var/mps/adcimages`enthalten. Diese zwischengespeicherten Images können für mehrere NetScaler-Upgrades verwendet werden, sodass Sie nicht jedes Mal ein Image für ein Upgrade herunterladen müssen.
> - NetScaler Console löscht die zwischengespeicherten NetScaler-Images alle drei Tage, basierend auf dem Zeitpunkt der letzten Änderung der Images. Nur die letzten beiden Bilddateien werden gleichzeitig im Agenten zwischengespeichert.

5. 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.

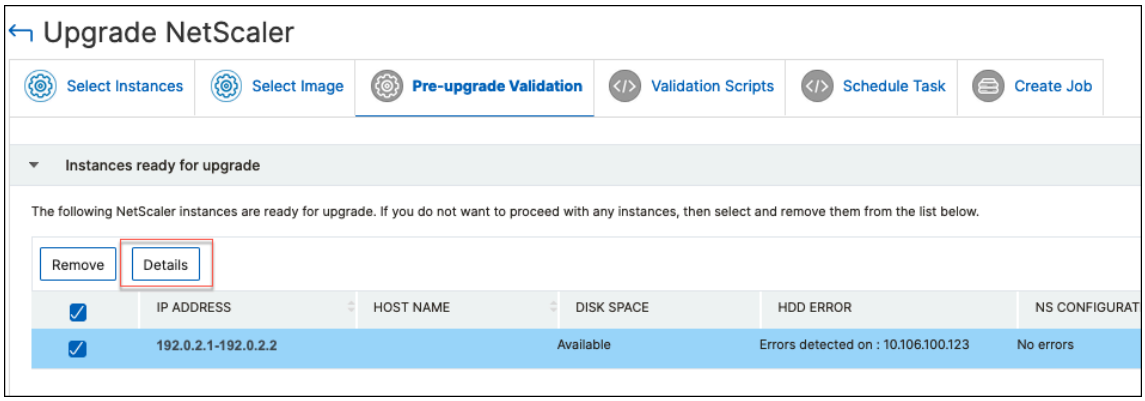
     Sie können die Fehler überprüfen, korrigieren und dann für das Upgrade auf **Move to ready for upgrade** klicken. Wenn Sie auf einer Instanz nicht genügend Speicherplatz haben, können Sie den Speicherplatz überprüfen und bereinigen. Siehe NetScaler-Speicherplatz bereinigen.

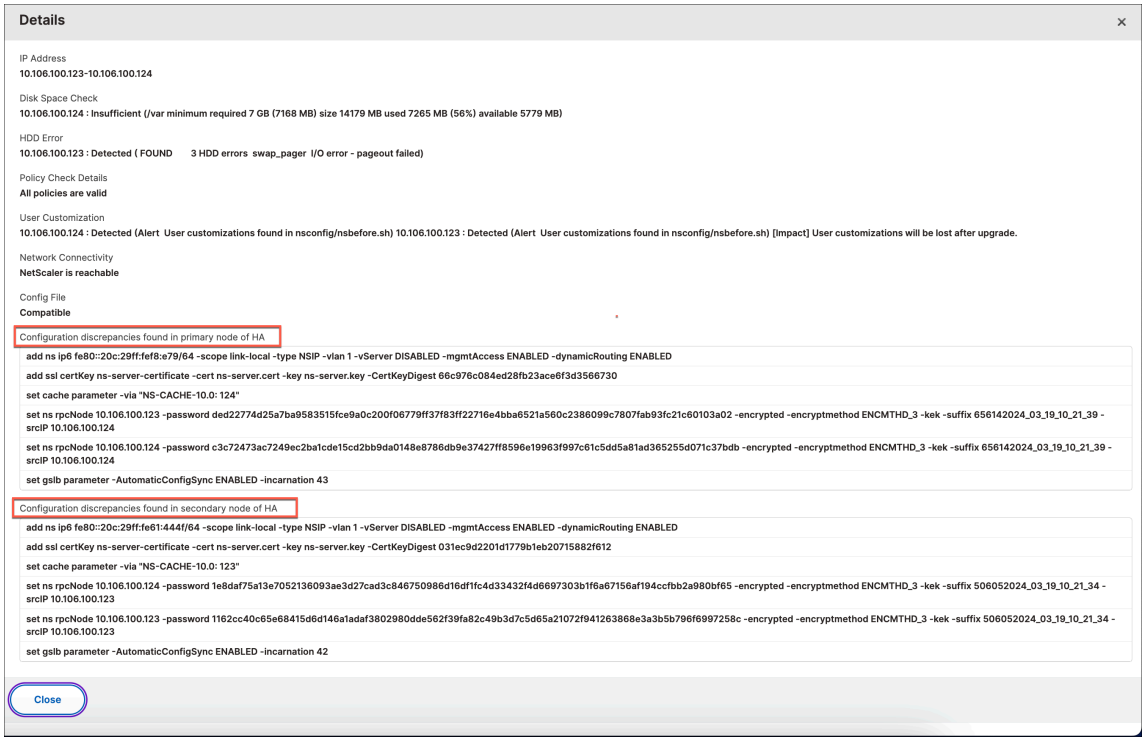


- **Richtlinien-Check**: Wenn NetScaler Console nicht unterstützte klassische Richtlinien findet, können Sie diese Richtlinien entfernen, um einen Upgrade-Job zu erstellen.

> **Wichtig:**
>
> Wenn Sie eine Cluster-IP-Adresse angeben, überprüft NetScaler Console vor dem Upgrade nur die angegebene Instanz und nicht die anderen Clusterknoten.

Um Diskrepanzen zwischen primären und sekundären Knoten während eines Upgrades anzuzeigen, wählen Sie den Hochverfügbarkeitsknoten aus und klicken Sie auf **Details**.





- **Im primären Knoten von HA festgestellte Konfigurationsdiskrepanzen** – Zeigt alle Konfigurationen an, die im sekundären Knoten des NetScaler-Hochverfügbarkeitspaars gefunden wurden, aber im primären Knoten fehlen.
- **Im sekundären Knoten von HA festgestellte Konfigurationsdiskrepanzen** – Zeigt alle Konfigurationen an, die im primären Knoten des NetScaler-Hochverfügbarkeitspaars gefunden wurden, aber im sekundären Knoten fehlen.

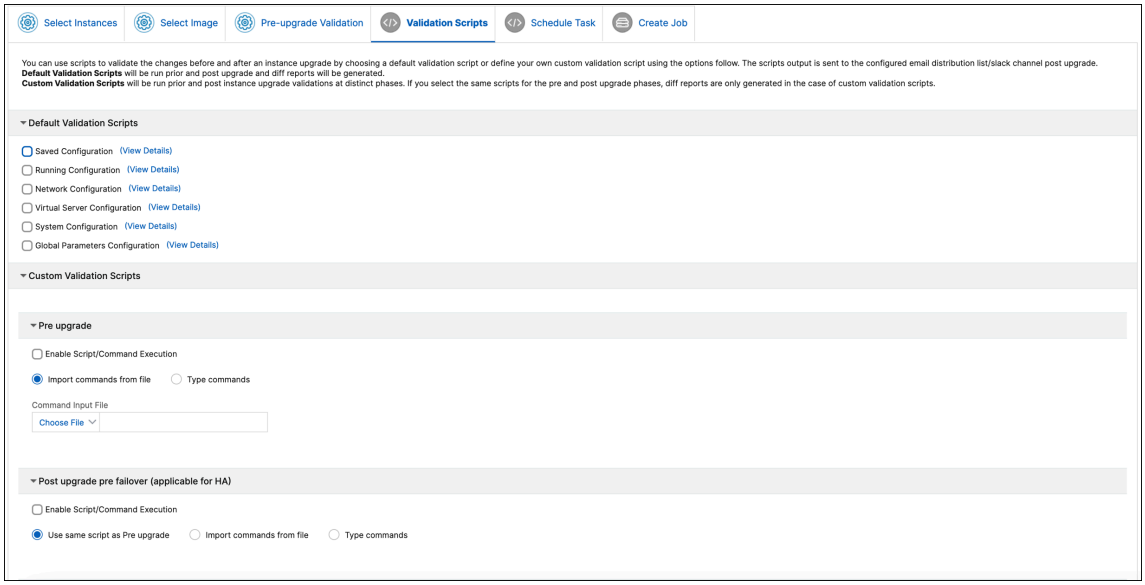
> **Hinweis:**
>
> Sie können die folgenden Abweichungen ignorieren, die in den Abschnitten mit den Konfigurationsabweichungen auftreten können:
>
> - Gerätespezifische Konfigurationen wie IP-Adressen.
> - Verschlüsselte Kennwörter oder Zertifikate, die sich zwischen den Knoten unterscheiden können, auch wenn das Kennwort dasselbe ist.
>
> Sie können die Abweichungen überprüfen und sich dafür entscheiden, sie zu ignorieren, wenn sie nicht relevant sind.

6. Geben Sie in **Validation Scripts**die Skripts an, die vor und nach einem Instanz-Upgrade ausgeführt werden sollen. Sie haben folgende Wahl:
   - **Standard-Validierungsskripten** – Wählen Sie diese Option, um die vordefinierten Validierungsskripts auszuführen. Diese Skripts werden sowohl vor als auch nach dem

Upgrade-Job ausgeführt und generieren einen Diff-Bericht für das Validierungsskript.

> **Hinweis:**
>
> Sie können diesen vordefinierten Befehlssatz nicht ändern oder bearbeiten.

- **Benutzerdefinierte Validierungsskripte** – Wählen Sie diese Option, um Ihr eigenes Validierungsskript auszuführen. Sie können angeben, ob die Skripts vor oder nach dem Upgrade ausgeführt werden sollen. Ein Diff-Bericht wird nur generiert, wenn vor und nach dem Upgrade dieselben Skripts ausgewählt werden.



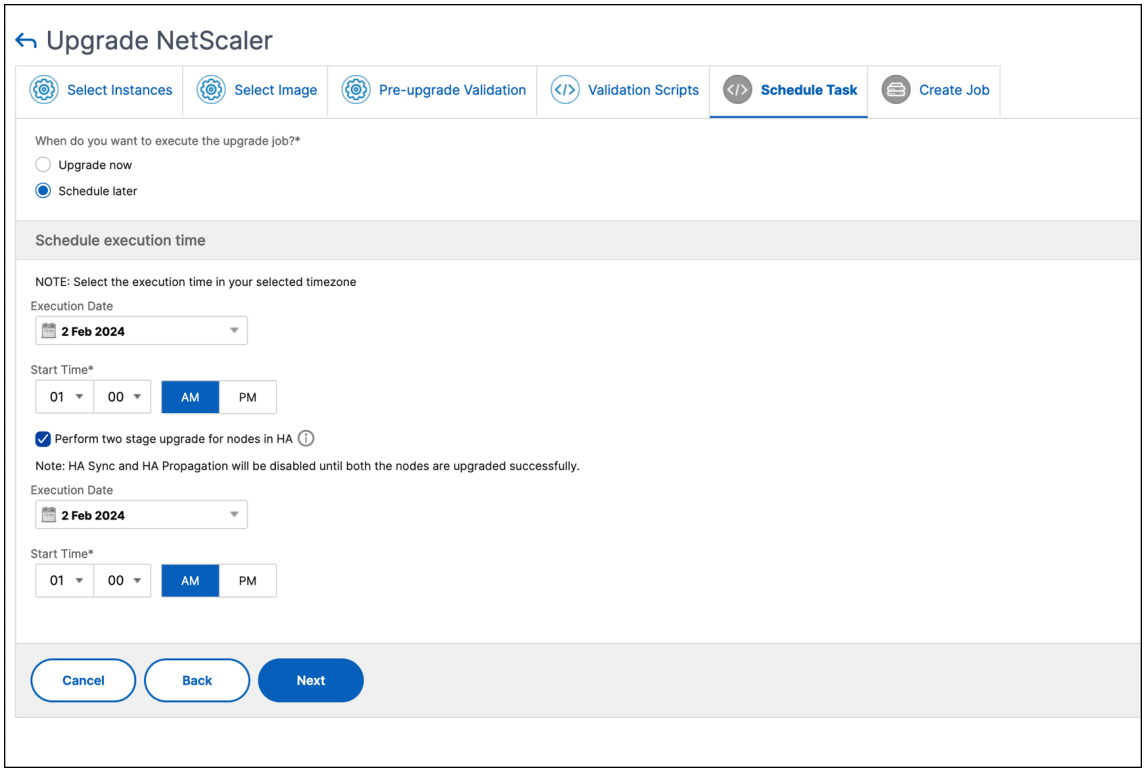
Um den Befehlssatz in jeder Konfiguration zu erfahren, klicken Sie auf **Details anzeigen**. Weitere Informationen finden Sie unter Verwenden benutzerdefinierter Skripts.

7. Wählen Sie unter **Task planen** eine der folgenden Optionen aus:

   - **Jetzt upgraden**: Der Upgrade-Job wird sofort ausgeführt.
   - **Später planen**: Wählen Sie diese Option, um diesen Upgrade-Auftrag später auszuführen. Geben Sie das **Ausführungsdatum** und die **Startzeit** an, wenn Sie die Instanzen aktualisieren möchten.

   Wenn Sie ein NetScaler-Hochverfügbarkeitspaar in zwei Schritten aktualisieren möchten, wählen Sie Zweistufiges **Upgrade für Knoten mit hoher Verfügbarkeit durchführen aus**.

   Geben Sie das **Ausführungsdatum** und die **Startzeit an**, wenn Sie eine andere Instanz im Hochverfügbarkeitspaar upgraden möchten.



Weitere Informationen finden Sie unter NetScaler Hochverfügbarkeitspaar .

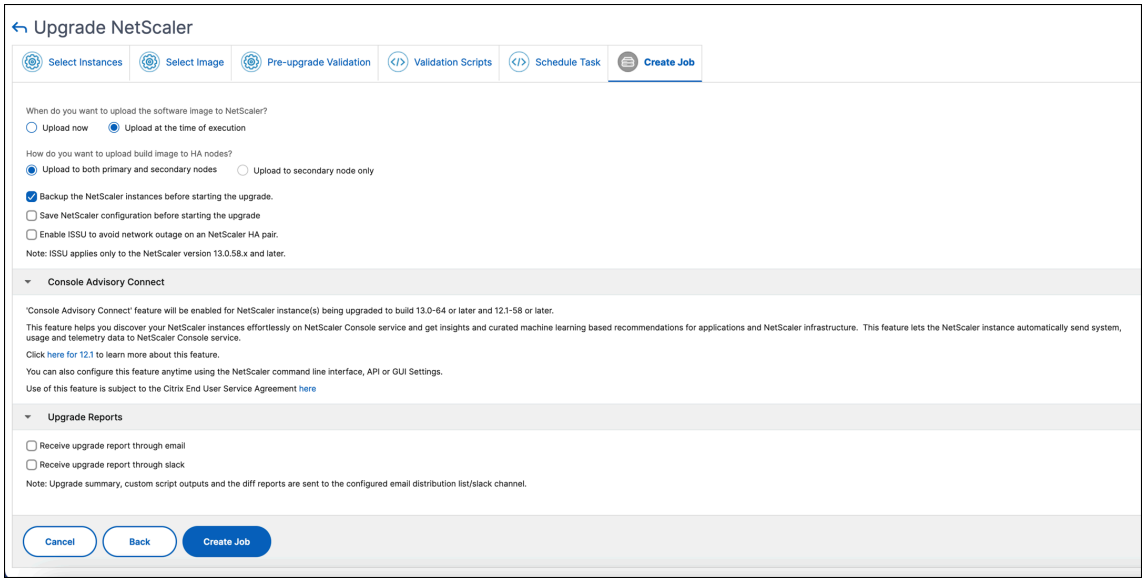
8. Geben Sie unter **Job erstellen** die folgenden Details an:

   Wenn Sie den Upgrade-Auftrag planen, können Sie angeben, wann Sie das Image in eine Instanz hochladen möchten:

   - **Jetzt hochladen**: Wählen Sie diese Option, um das Image sofort hochzuladen. Der Upgrade-Job wird jedoch zur geplanten Zeit ausgeführt.
   - **Zum Zeitpunkt des Ausführens hochladen**: Wählen Sie diese Option, um das Image hochzuladen, wenn der Upgradejob ausgeführt wird.

   Für Paare mit hoher Verfügbarkeit 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 Planen von Upgrade-Aufträgen für ein NetScaler-Hochverfügbarkeitspaar .

Weitere Informationen zu anderen Upgrade-Optionen finden Sie unter NetScaler-Upgrade-Optionen .

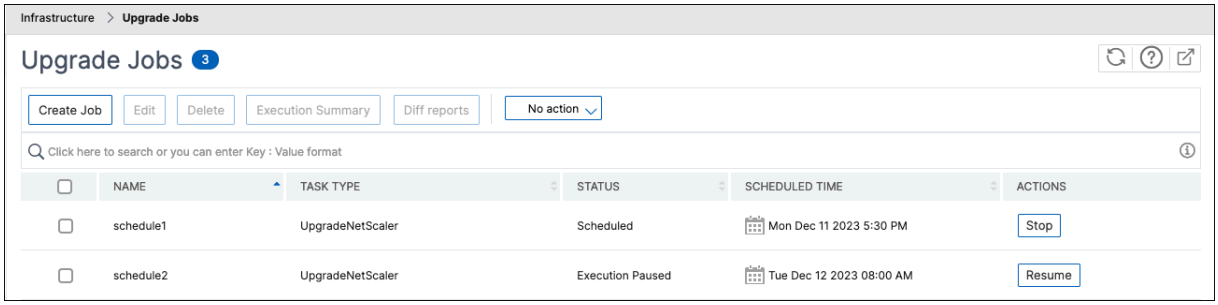
9. Klicken Sie auf **Job erstellen**.

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.

Einen geplanten Upgrade-Job anhalten oder fortsetzen

Sie können Ihren geplanten Upgrade-Job auch unterbrechen.

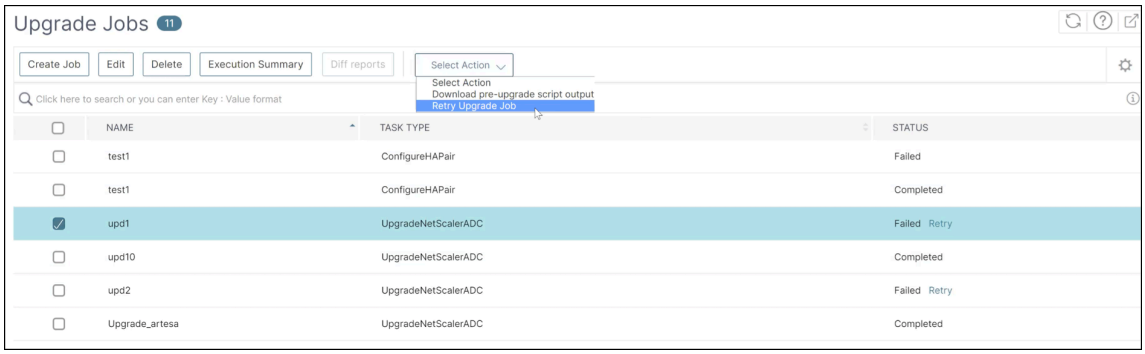
Um diese Funktion zu verwenden, navigieren Sie zu **Infrastruktur > Upgrade-Jobs** , wählen Sie einen vorhandenen geplanten Upgrade-Job aus und klicken Sie auf **Stopp** , um den Job anzuhalten. Um den geplanten Upgrade-Job fortzusetzen, klicken Sie auf **Fortsetzen** .



> **Hinweis:**
>
> Wenn die geplante Zeit für den Upgrade-Job abgelaufen ist, nachdem Sie beschlossen haben, ihn fortzusetzen, müssen Sie den Upgrade-Job erneut erstellen.

Fehlgeschlagene Upgrade-Jobs erneut versuchen

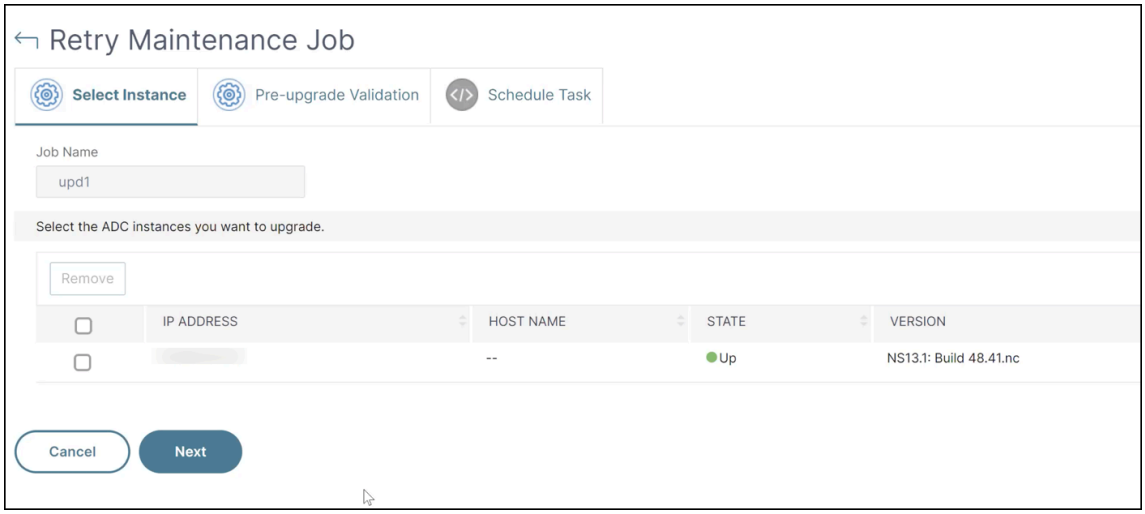
1. Wählen Sie unter **Infrastruktur > Upgrade-Jobs**den fehlgeschlagenen Upgrade-Job aus und klicken Sie auf **Erneut versuchen**. Alternativ können Sie auch zu **Aktion auswählen > Upgrade-Job erneut versuchen** navigieren, um einen fehlgeschlagenen Job erneut zu versuchen.



2. Geben Sie unter **Select Instanz**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**.

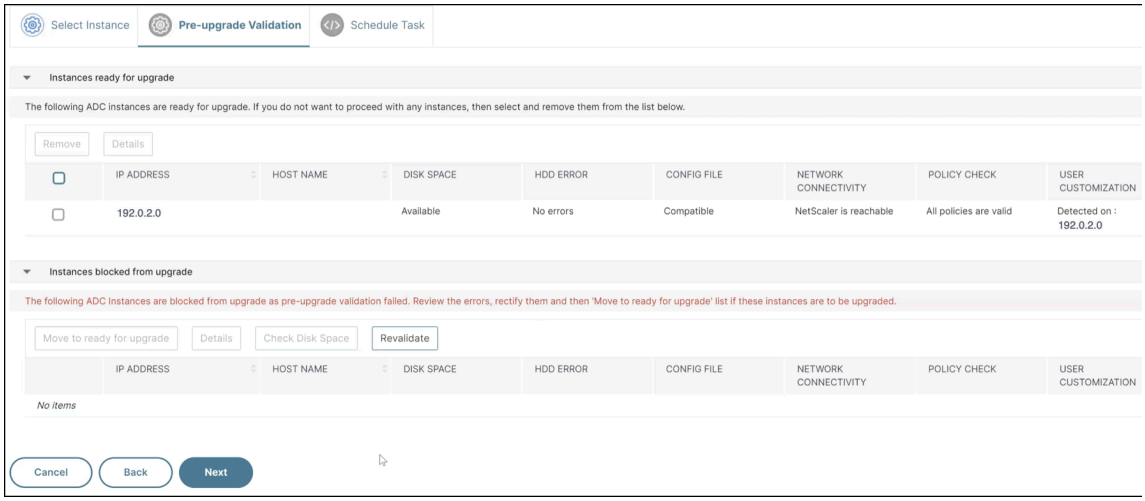
   Klicken Sie auf **Weiter**, um den Validierungsprozess zu starten.



3. Auf der Registerkarte **Pre-upgrade validation** werden die folgenden Abschnitte angezeigt:

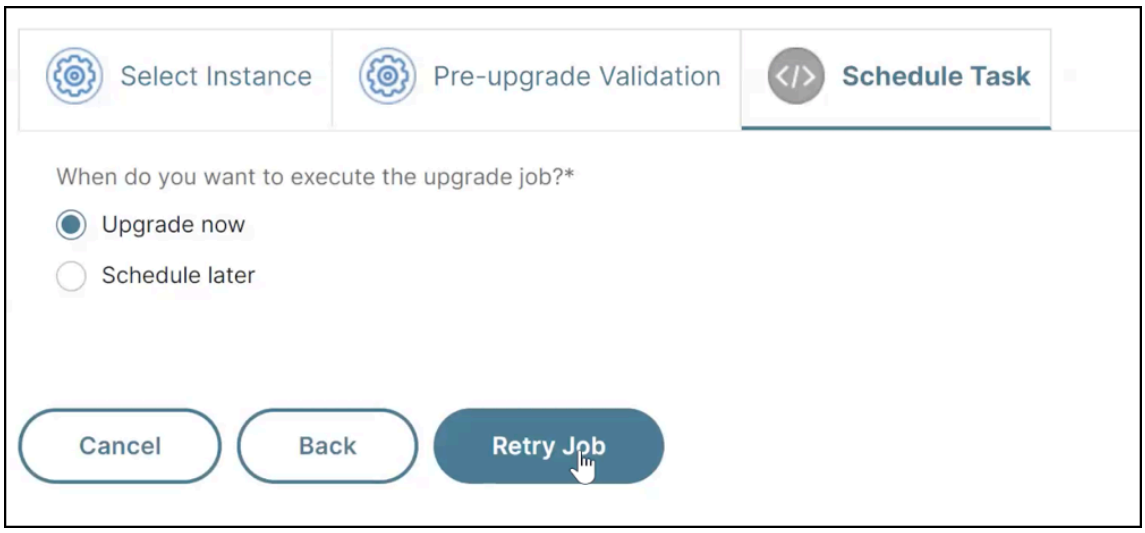
- **Instanzen, die für das Upgrade bereit sind**. Sie können mit dem Upgrade dieser Instanzen fortfahren.
- **Für das Upgrade blockierte Instanzen**. Diese NetScaler-Instanzen sind aufgrund von Validierungsfehlern vor dem Upgrade für das Upgrade gesperrt.

  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. Siehe NetScaler-Speicherplatz bereinigen.
- **Richtlinien-Check**: Wenn NetScaler Console nicht unterstützte klassische Richtlinien findet, können Sie diese Richtlinien entfernen, um einen Upgrade-Job 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.



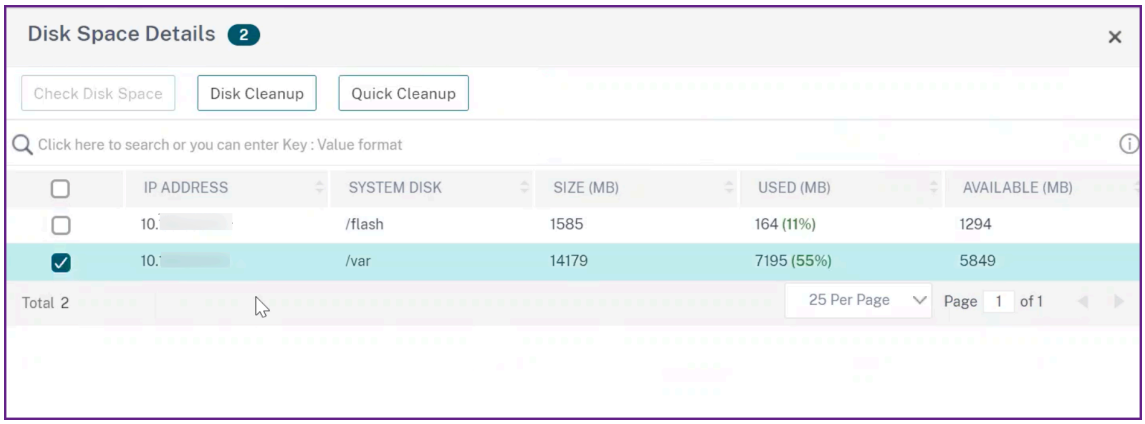
Klicken Sie auf **Wiederholen**.

NetScaler-Speicherplatz bereinigen

Wenn beim Upgrade einer NetScaler-Instanz das Problem mit unzureichendem Speicherplatz auftritt, bereinigen Sie den Speicherplatz über die NetScaler Console-GUI selbst.

1. Auf der Registerkarte **Pre-upgrade validation** werden im Abschnitt **Instanzen 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**.

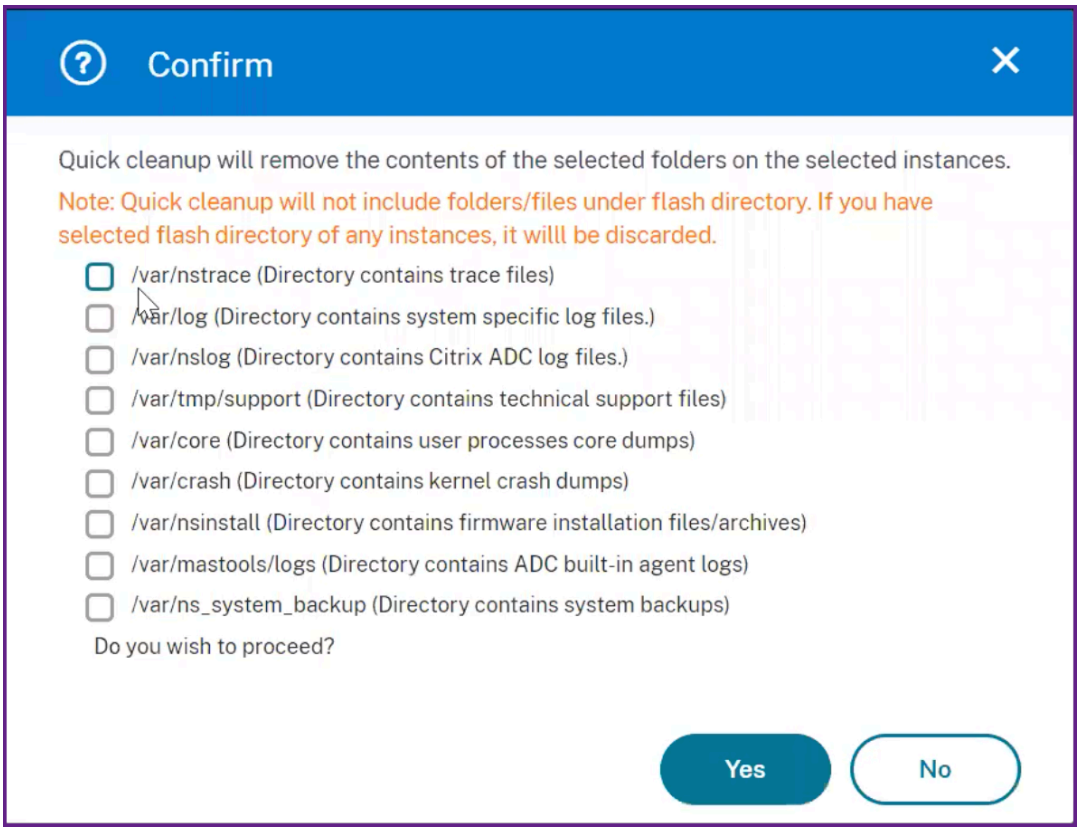
   Ein Bereich mit **Speicherplatzdetails** wird angezeigt. In diesem Bereich werden die Instanzen, der verwendete Speicher und der verfügbare Speicher angezeigt.



3. Wählen Sie im Bereich **Disk Space Details** die Instanz aus, die bereinigt werden muss, und führen Sie einen der folgenden Schritte aus:

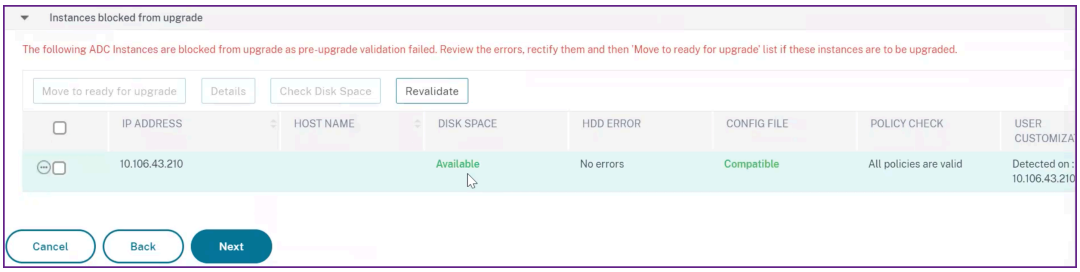
a) **Disk Cleanup** - Navigieren Sie zu den erforderlichen Ordnern oder Verzeichnissen und löschen Sie sie, um Speicherplatz freizugeben.

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 **Instanzen 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.



Verwenden von benutzerdefinierten Skripts

Sie können benutzerdefinierte Skripts angeben, während Sie einen NetScaler-Upgrade-Job erstellen . 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.

Geben Sie die benutzerdefinierten Skripts an, die in den folgenden Phasen ausgeführt werden sollen:

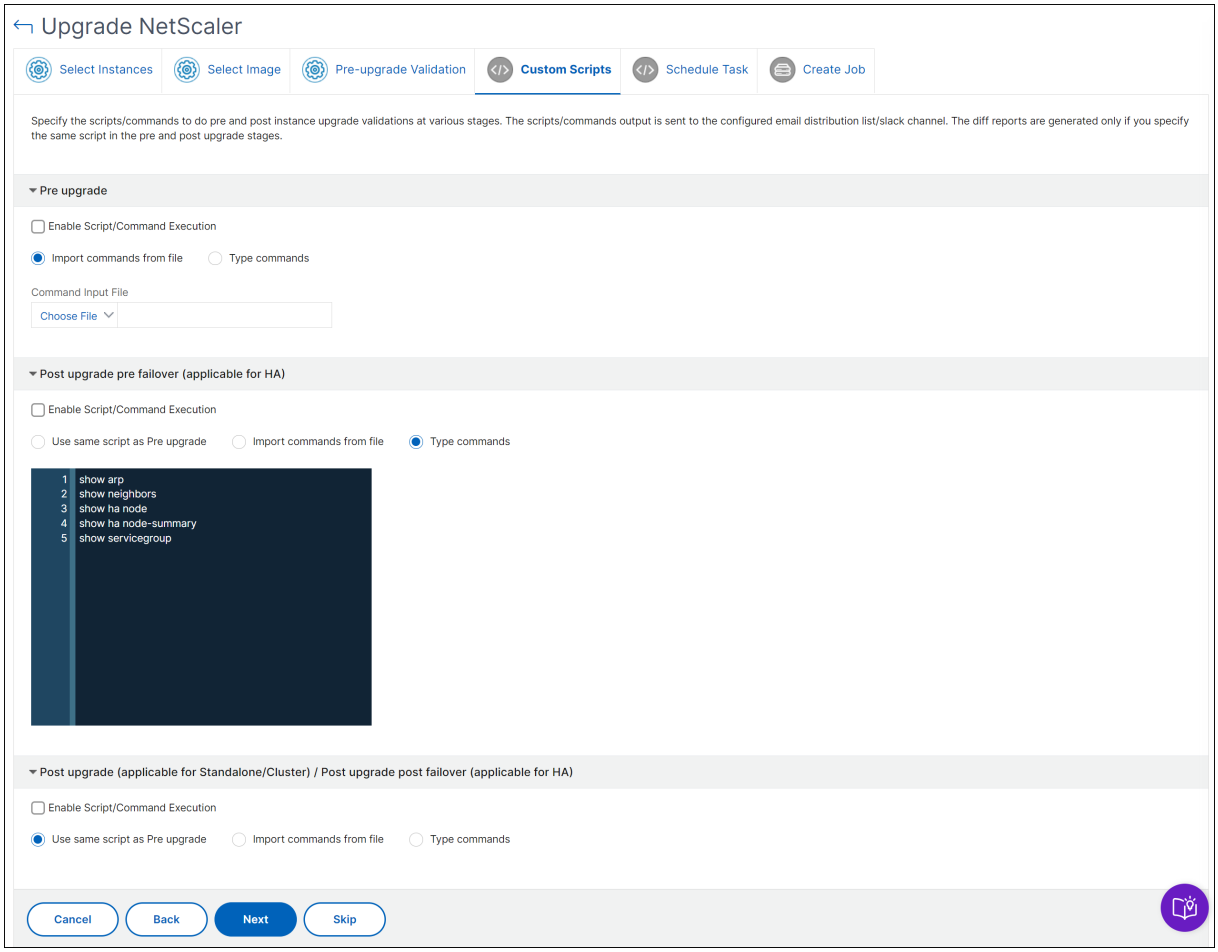
- **Vor dem Upgrade**: Das angegebene Script wird vor dem Upgrade einer Instanz ausgeführt.
- **Vorab-Failover nach dem Upgrade (gilt für HA)**: Diese Phase gilt nur für die Bereitstellung mit hoher Verfügbarkeit. Das angegebene Skript wird nach dem Upgrade der Knoten, jedoch vor ihrem Failover ausgeführt.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

> **Hinweis:**
>
> - Stellen Sie sicher, dass die Skript- oder Befehlsausführung in den erforderlichen Phasen aktiviert ist. Andernfalls werden die angegebenen Skripts nicht ausgeführt.
> - Der Diff-Bericht wird nur generiert, wenn Sie dasselbe Skript in den Phasen vor dem Upgrade und nach dem Upgrade angeben. Stellen Sie daher sicher, dass Sie in den Phasen nach **dem Upgrade dasselbe Skript wie vor dem Upgrade verwenden** auswählen. Siehe Laden Sie einen konsolidierten Vergleichsbericht eines NetScaler-Upgrade-Jobs herunter.

Sie können eine Skriptdatei importieren oder Befehle direkt in die NetScaler Console-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 der Phase nach dem Upgrade können Sie dasselbe Skript verwenden, das in der Phase vor dem Upgrade angegeben wurde.



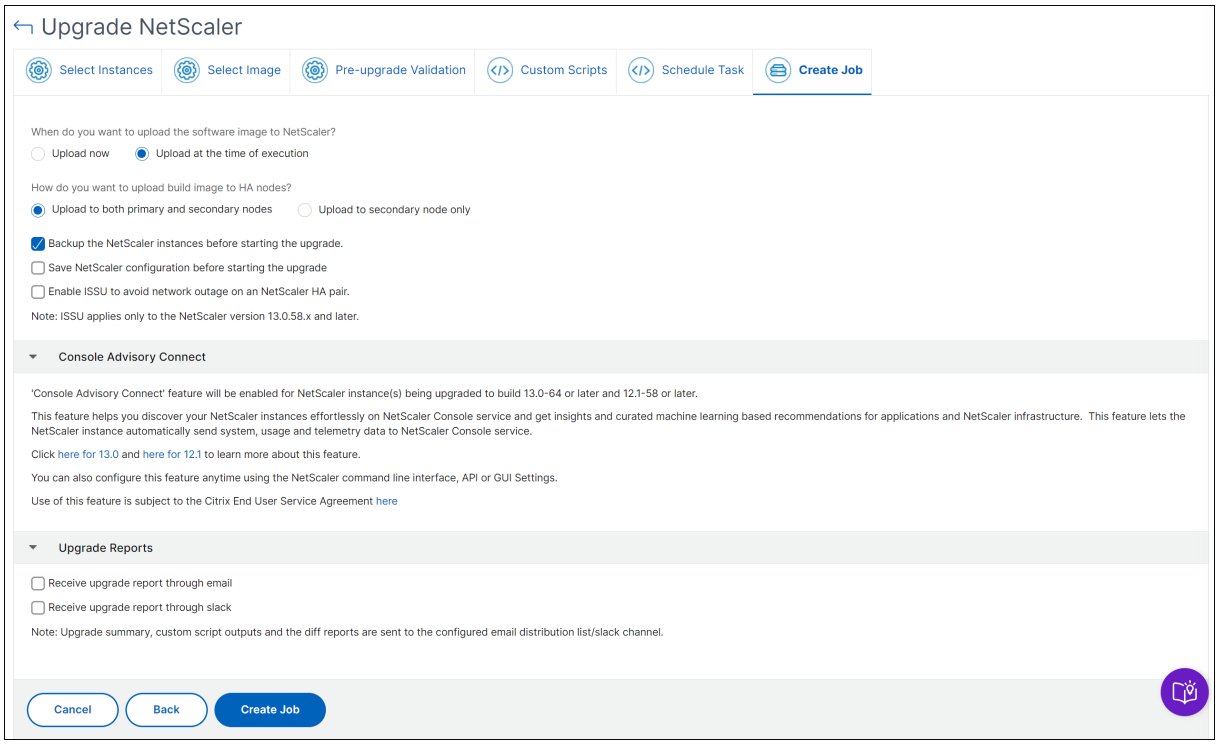
NetScaler-Upgrade-Optionen

Während Sie einen NetScaler-Upgrade-Job erstellen , können Sie auf der Registerkarte „ **Job erstellen** “die folgenden Optionen auswählen:

- **Erstellen Sie ein Backup der NetScaler-Instanzen, bevor Sie das Upgrade starten.**: Erstellt ein Backup der ausgewählten NetScaler-Instanzen.
- **Den primären und sekundären Status von Knoten mit hoher Verfügbarkeit nach dem Upgrade beibehalten**: Wählen Sie diese Option, wenn der Upgrade-Job nach dem Upgrade jedes Knotens ein 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 das Upgrade ohne Ausfallzeiten auf einem NetScaler-Hochverfügbarkeitspaar. Diese Option bietet eine Migrationsfunktionalität, die die vorhandenen Verbindungen während

des Upgrades berücksichtigt. Sie können also ein NetScaler-Hochverfügbarkeitspaar ohne Ausfallzeiten aktualisieren. Geben Sie das Timeout der ISSU Migration in Minuten an.

- **Ausführungsbericht per E-Mail empfangen** - Sendet den Ausführungsbericht per E-Mail. Informationen zum Hinzufügen einer E-Mail-Verteilerliste finden Sie unter Erstellen einer E-Mail-Verteilerliste.
- **Ausführungsbericht über Pufferzeit empfangen** - Sendet den Ausführungsbericht in Pufferzeit. Informationen zum Hinzufügen eines Slack-Profils findest du unter Erstellen eines Slack-Profils.



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 konsolidierten Vergleichsbericht eines NetScaler-Upgrade-Jobs herunter

In der NetScaler Console können Sie einen Vergleichsbericht über einen NetScaler-Upgrade-Auftrag herunterladen. Dazu muss der Upgrade-Job über benutzerdefinierte Skriptsverfügen. 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 in den Phasen vor und nach dem Upgrade dasselbe Skript angeben.

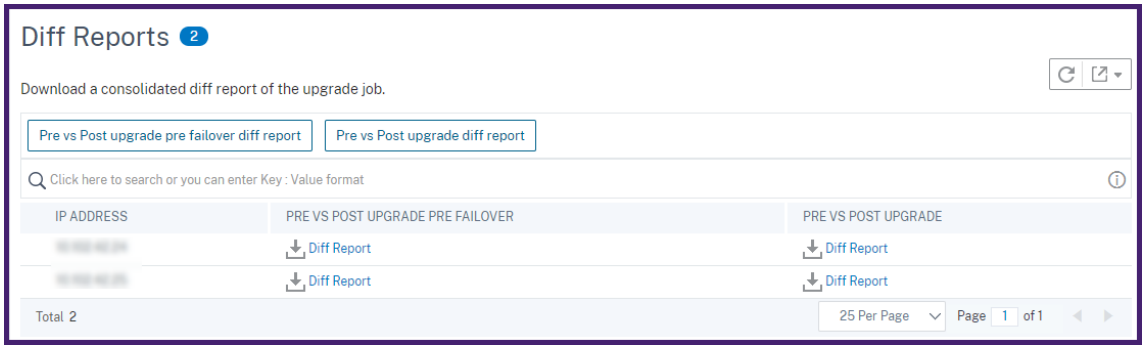
Um einen Diff-Bericht über einen Upgrade-Job herunterzuladen, gehen Sie wie folgt vor:

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**



Netzwerkfunktionen

January 26, 2024

Mit der Funktion Netzwerkfunktionen können Sie den Status der Entitäten überwachen, die auf Ihren verwalteten Citrix Application Delivery Controller (NetScaler) -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

- Load Balancing-Methode
- Load Balancing-Persistenz

Berichte für Lastausgleichseinheiten generieren

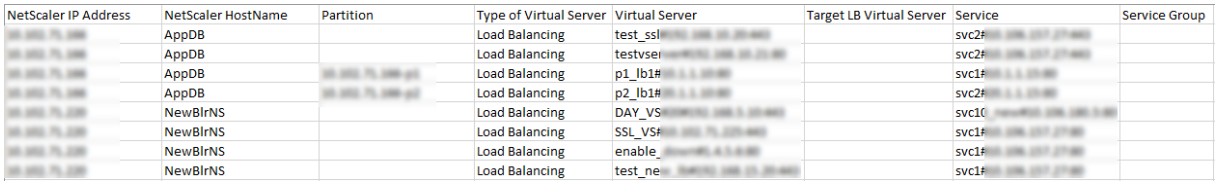
January 26, 2024

Mit der NetScaler Console können Sie die Berichte der Citrix Application Delivery Controller (NetScaler) -Instanzentitäten auf allen Ebenen anzeigen. Es gibt zwei Arten von Berichten, die Sie unter **NetScaler Console > 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]	AppDB		Load Balancing	test_ssl[redacted]		svc2[redacted]	
[redacted]	AppDB		Load Balancing	testvser[redacted]		svc2[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p1_lb1[redacted]		svc1[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p2_lb1[redacted]		svc2[redacted]	
[redacted]	NewBlrNS		Load Balancing	DAY_VS[redacted]		svc1[redacted]	
[redacted]	NewBlrNS		Load Balancing	SSL_VS[redacted]		svc1[redacted]	
[redacted]	NewBlrNS		Load Balancing	enable_[redacted]		svc1[redacted]	
[redacted]	NewBlrNS		Load Balancing	test_ne[redacted]		svc1[redacted]	

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 der NetScaler Console 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 der NetScaler Console zu Infrastruktur > Netzwerkfunktionen .**
2. Klicken Sie auf **Bericht erstellen**.
3. Auf der Seite **Bericht generieren**, die geöffnet wird, haben Sie zwei Optionen, um den Bericht anzuzeigen:

   a) Wählen Sie auf der Registerkarte **Jetzt exportieren** die Option **Load Balancing** und klicken Sie auf **OK**.

   Der konsolidierte Bericht wird auf Ihr System heruntergeladen.

   b) Wählen Sie **Bericht planen**, um einen Zeitplan für die Erstellung und den Export von Berichten in regelmäßigen Abständen zu erstellen. Geben Sie die Einstellungen für die Berichtsgenerierung an, und erstellen Sie ein E-Mail-Profil, in das der Bericht exportiert wird.

      i. Wählen Sie **Zeitplan aktivieren**aus.

      ii. **Wiederholung** - wählen Sie **Täglich**, **Wöchentlich**oder **Monatlich** aus der Liste aus.

      > **Hinweis**
      >
      > Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.

> **Hinweis**
>
> Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie Monatstage mit den Werten zwischen 1 und 31 eingeben.

iii. **Exportzeit** - Geben Sie die Zeit in der Stunde: Minute im 24-Stunden-Format ein.

iv. **E-Mail** - markieren Sie das Kontrollkästchen und wählen Sie dann ein Profil aus der Liste aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

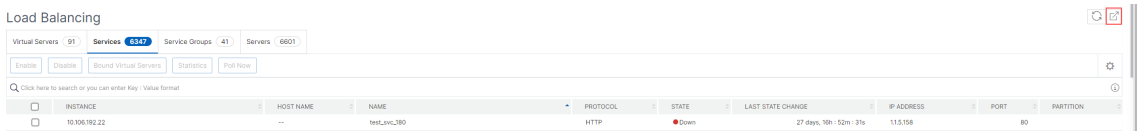
v. **Slack** - Aktivieren Sie das Kontrollkästchen Slack und wählen Sie dann ein Profil aus dem Listenfeld aus oder klicken Sie auf **Hinzufügen**, um ein Slack-Profil zu erstellen.

vi. Klicken Sie auf **Zeitplan**, um den Vorgang abzuschließen.

Erstellen eines individuellen Lastausgleichsentitätsberichts

Sie können einen 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 der NetScaler Console zu **Infrastruktur > Netzwerkfunktionen > Load Balancing > Dienste** .
2. Klicken Sie auf der Seite **Dienste** oben rechts auf die Schaltfläche **Exportieren**.



Wählen Sie die Registerkarte **Jetzt exportieren**, wenn Sie den Bericht in diesem Moment generieren und anzeigen möchten.

> **Hinweis**
>
> Sie können die Berichte nur herunterladen oder als E-Mail-Anhänge exportieren. Sie können die Berichte nicht auf der NetScaler Console-GUI anzeigen.

Netzwerkfunktionenberichte exportieren oder planen

January 26, 2024

Sie können in der NetScaler Console 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 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. Informationen zum Einrichten von E-Mail-Benachrichtigungen finden Sie unter Erstellen von Ereignisregeln.

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 der NetScaler Console keine separate Liste virtueller SSL-Server geführt wird.
- Wenn ein neuer Bericht generiert wird, werden die älteren Berichte automatisch aus Ihrem Konto gelöscht.

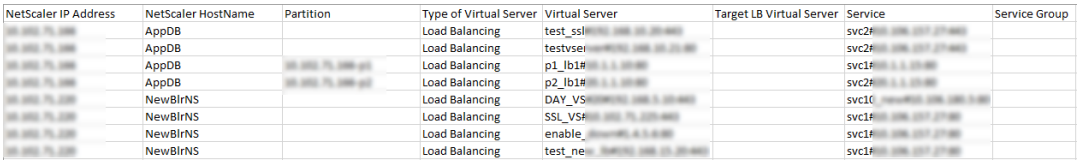
So exportieren und planen Sie Berichte über Netzwerkfunktionen:

1. Navigieren Sie zu **Infrastruktur > Netzwerkfunktionen**.
2. Klicken Sie auf der Seite **Netzwerkfunktionen** im rechten Bereich oben rechts auf der Seite auf **Bericht erstellen** .
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]	AppDB		Load Balancing	test_ssl[redacted]		svc2[redacted]	
[redacted]	AppDB		Load Balancing	testvser[redacted]		svc2[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p1_lb1[redacted]		svc1[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p2_lb1[redacted]		svc2[redacted]	
[redacted]	NewBlrNS		Load Balancing	DAY_VS[redacted]		svc1C[redacted]	
[redacted]	NewBlrNS		Load Balancing	SSL_VS[redacted]		svc1[redacted]	
[redacted]	NewBlrNS		Load Balancing	enable_[redacted]		svc1[redacted]	
[redacted]	NewBlrNS		Load Balancing	test_ne[redacted]		svc1[redacted]	

   b) Wählen Sie **Bericht planen** aus, um einen Zeitplan für die Generierung und den Export von Berichten in regelmäßigen Abständen zu erstellen. Geben Sie die Einstellungen für die Berichtsgenerierung an, und erstellen Sie ein E-Mail-Profil, in das der Bericht exportiert wird.

      i. **Wiederholung** - Wählen Sie **Täglich**, **Wöchentlich** oder **Monatlich** aus dem Dropdownlistenfeld aus.

      ii. **Wiederholzeit** - Geben Sie die Zeit in der Stunde: Minute im 24-Stunden-Format ein.

      iii. **E-Mail** - Aktivieren Sie das Kontrollkästchen, und wählen Sie dann das Profil aus dem Dropdownlistenfeld aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

      iv. **Slack** —Aktiviere das Kontrollkästchen und wähle dann das Profil aus dem Dropdown-Listenfeld aus, oder klicke auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

Klicken Sie auf **Zeitplan aktivieren**, um den Bericht zu planen, und klicken Sie dann auf **OK**. Wenn Sie auf das Kontrollkästchen **Zeitplan aktivieren** klicken, können Sie die ausgewählten Berichte erstellen.

Netzwerkberichterstellung

January 26, 2024

Sie können die Ressourcennutzung optimieren, indem Sie Ihre Netzwerkberichte in der NetScaler Console 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.

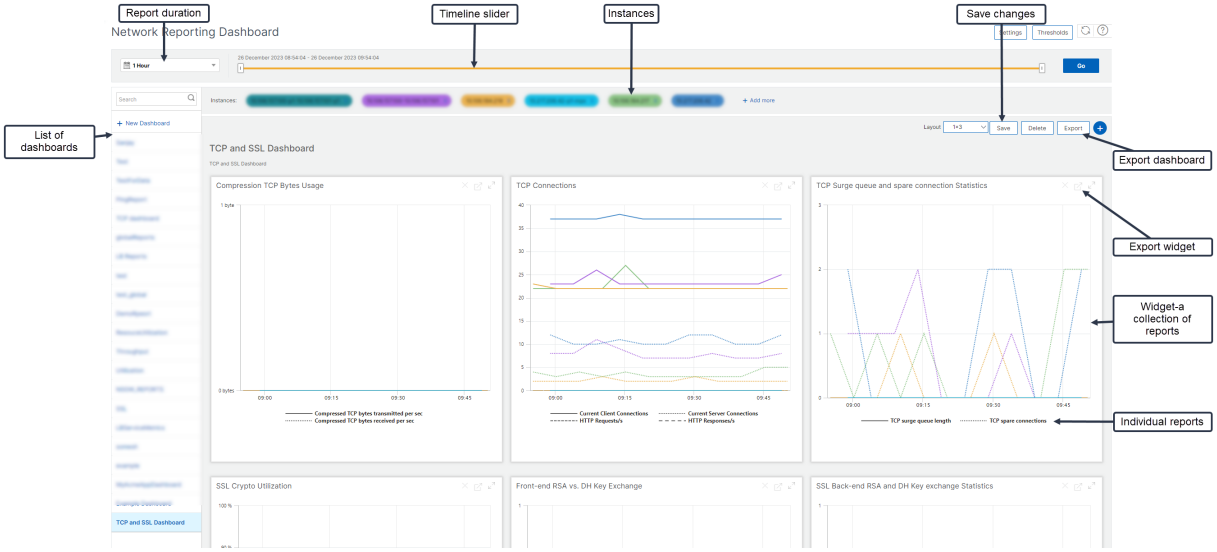
Mit NetScaler Console können Sie Berichte für Instanzen auf globaler Ebene und Entitäten wie virtuelle Server und Netzwerkschnittstellen generieren. Die virtuellen Server, für die Sie Berichte erstellen können, sind wie folgt:

- Load Balancing-Server, Dienste und Dienstgruppen
- Content Switching-Server
- Cache-Umleitungsserver
- Globaler Service Load Balancing (GSLB)
- Authentifizierung
- NetScaler Gateway

Sie können in NetScaler Console mehrere Dashboards für verschiedene Instanzen, virtuelle Server und andere Entitäten erstellen.

Netzwerkberichterstattungs-Dashboard

Das folgende Bild ruft die verschiedenen Funktionen im Dashboard auf:

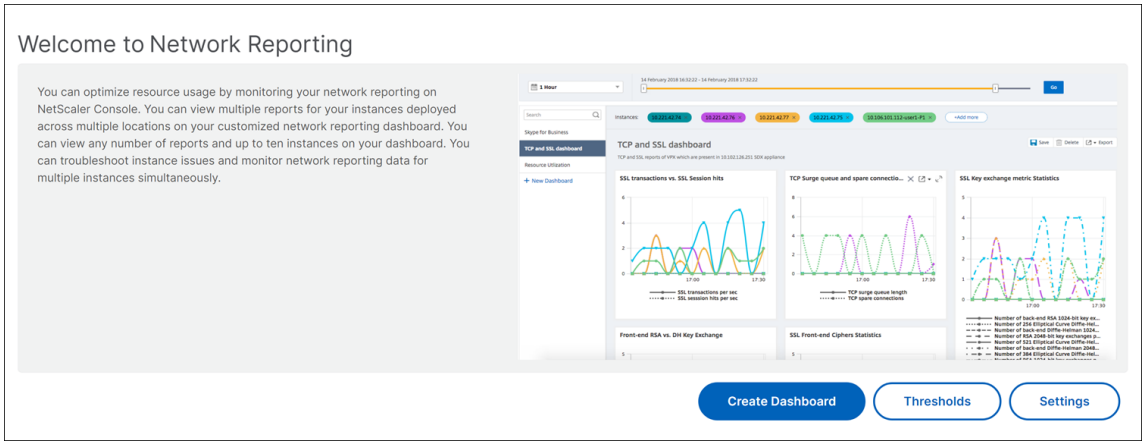


- Im linken Seitenbereich sind alle benutzerdefinierten Dashboards aufgeführt, die in NetScaler Console erstellt wurden. Sie können auf einen von ihnen klicken, um die verschiedenen Berichte anzuzeigen, aus denen das Dashboard besteht. Beispielsweise enthält ein TCP- und SSL-Dashboard verschiedene Berichte, 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. Ein komprimierter TCP-Byte-Nutzungsbericht enthält beispielsweise Berichte über die pro Sekunde übertragenen und empfangenen komprimierten TCP-Bytes.
- Sie können Berichte für eine Stunde, einen Tag, eine Woche oder für einen Monat anzeigen. Sie können die Timeline-Slider-Option verwenden, um die Dauer der Berichte anzupassen, die in der NetScaler Console generiert werden.
- Sie können einen Bericht entfernen, indem Sie auf “X”klicken. Sie können den Bericht auch als PDF-, JPEG-, PNG- oder CSV-Format in Ihr System exportieren. Sie können auch einen Zeitpunkt und eine Wiederholung festlegen, wann der Bericht erstellt werden soll. Sie können auch eine E-Mail-Verteilerliste konfigurieren, an die Sie die Berichte senden möchten.
- Im Abschnitt Instanzen oben im Dashboard werden die IP-Adressen aller Instanzen aufgeführt, für die der Bericht generiert wird.
- Sie können Instanzen entweder entfernen, indem Sie auf X klicken oder weitere Instanzen zu den Berichten hinzufügen. Derzeit können Sie mit NetScaler Console jedoch Berichte für 10 Instanzen anzeigen.
- 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.

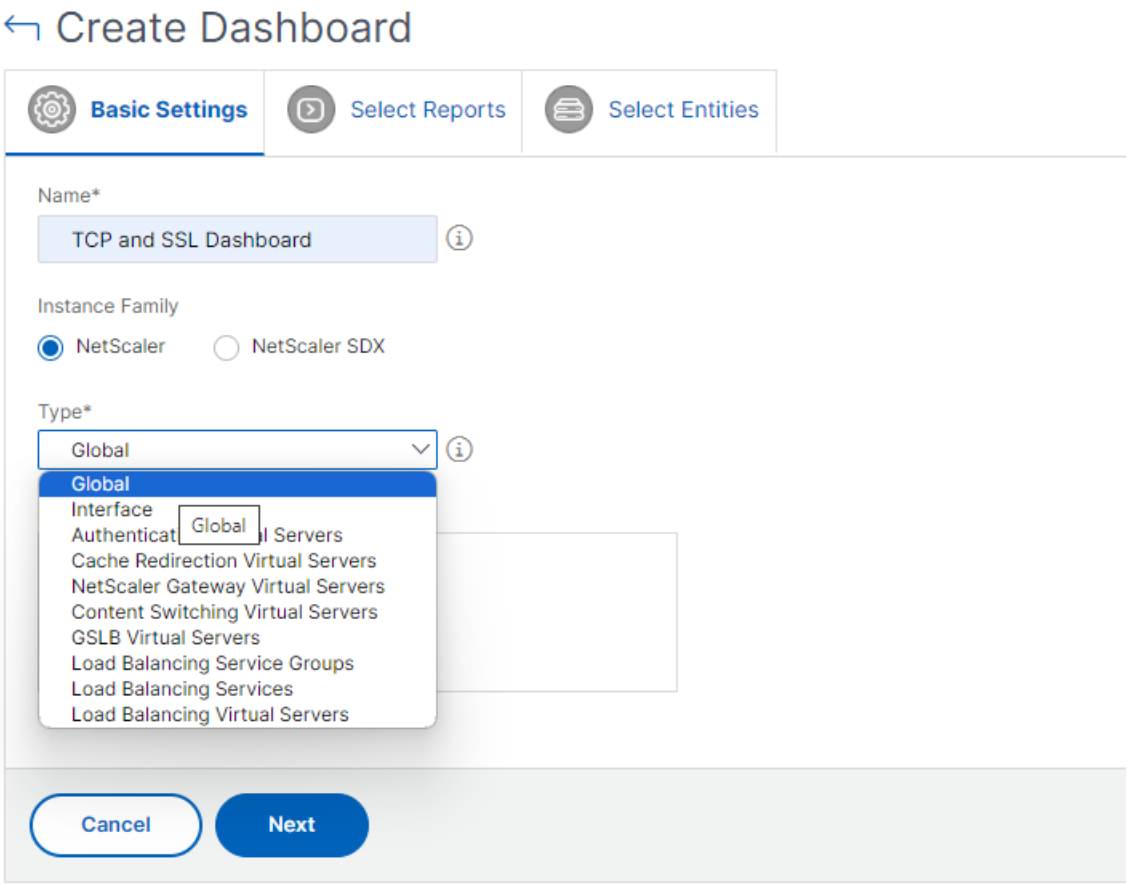
So zeigen Sie ein Dashboard an oder erstellen Sie es:

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > 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. Zum Erstellen eines Dashboards klicken Sie auf **Dashboard erstellen**.

   Die Seite **Dashboard erstellen** wird geöffnet.



4. Geben Sie auf der Registerkarte **Grundeinstellungen** die folgenden Details ein:

   a) **Name.** Geben Sie den Namen des Dashboards ein.

   b) **Instanzfamilie**. Wählen Sie den Instanztyp aus - NetScaler oder NetScaler SDX.

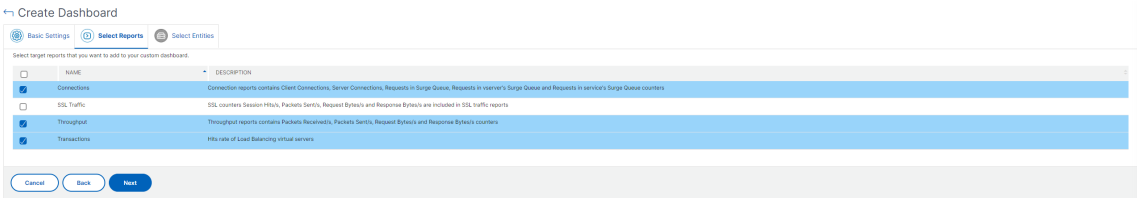
   <!–1. **Instanzfamilie**. Wählen Sie den Instanztyp aus - NetScaler, Citrix SD-WAN oder NetScaler SDX. —>

   a) **Typ**. Wählen Sie den Entitätstyp aus, für den Sie Berichte erstellen möchten. Wählen Sie in diesem Beispiel virtuelle Server für den Lastenausgleich aus.

   b) **Beschreibung**. Geben Sie eine aussagekräftige Beschreibung für das Dashboard ein.

5. Klicken Sie auf **Weiter**.

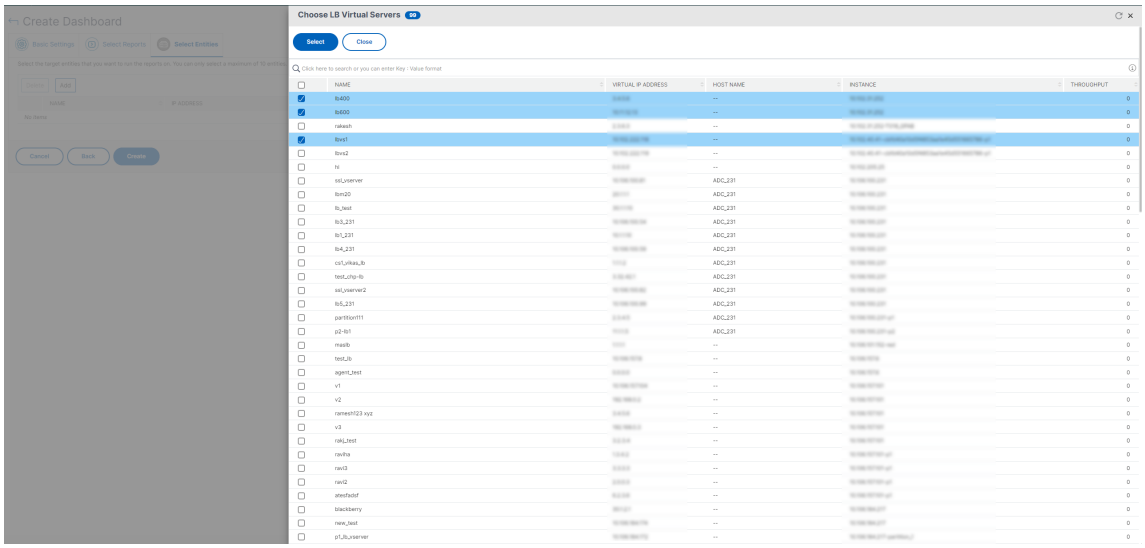
6. **Wählen Sie auf der Registerkarte Berichte** auswählen die erforderlichen Berichte aus. In diesem Beispiel können Sie Transaktionen, Verbindungen und Durchsatz auswählen. Klicken Sie auf **Weiter**.



7. Klicken **Sie auf der Registerkarte Entitäten auswählen** auf **Hinzufügen**.

   Je nach ausgewähltem Entitätstyp auf der Registerkarte **Grundeinstellungen** wird ein Fenster mit der Entitätsliste angezeigt. In diesem Beispiel wird das Fenster **Choose LB Virtual Servers** angezeigt.

8. Wählen Sie die Entitäten aus, die Sie überwachen möchten.



9. Klicken Sie auf **Erstellen**.

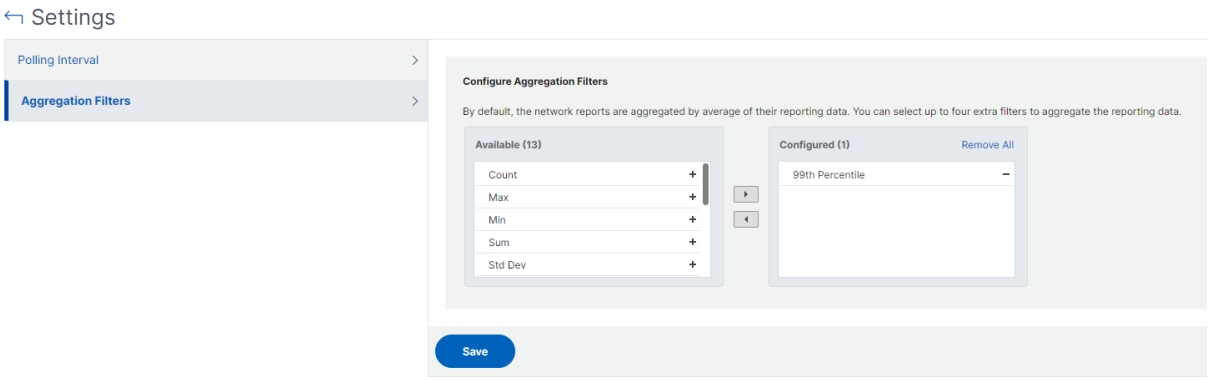
Das Dashboard wird erstellt und zeigt alle von Ihnen ausgewählten Berichte an.

> **Hinweis**
>
> Derzeit können Änderungen, die Sie an Legenden oder Filtern vornehmen, nicht gespeichert werden.

Anzeigen von Netzwerkberichtsdaten durch Anwendung von Aggregationen

Sie können Aggregationen auf die Netzwerkleistungsdaten anwenden und die Anwendungsleistung im Dashboard anzeigen. Sie können die Ergebnisse auch basierend auf Ihren Anforderungen exportieren. Mithilfe dieser auf die Daten angewendeten Aggregationen können Sie analysieren und prüfen, ob 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 Console ungefähr 1 Stunde, um Berichte für die ausgewählten Aggregationsoptionen zu generieren.

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 in NetScaler Console keine Berichte exportieren, wenn Sie nur Leseberechtigungen haben. Sie benötigen eine Bearbeitungsberechtigung, um eine Datei in NetScaler Console zu erstellen und die Datei zu exportieren.

So exportieren Sie Dashboard-Berichte:

1. Navigieren Sie zu **Infrastruktur > Network Reporting**
2. Klicken Sie auf **Dashboards anzeigen**, um alle Dashboards anzuzeigen, die Sie erstellt haben.
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 Seite **Network Reporting Dashboard** auf wiederkehrender Basis planen. Sie können beispielsweise eine Option festlegen, um wöchentlich einen Dashboard-Bericht für die vorherige Stunde zu einem bestimmten Zeitpunkt zu generieren. Der Bericht wird dann 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 wählen, wählen Sie die Wochentage aus, an denen der Bericht geplant werden soll.
> - Wenn Sie Monatliche Wiederholung auswählen, geben Sie alle Tage, an denen der Bericht geplant werden soll, durch Kommas getrennt ein.

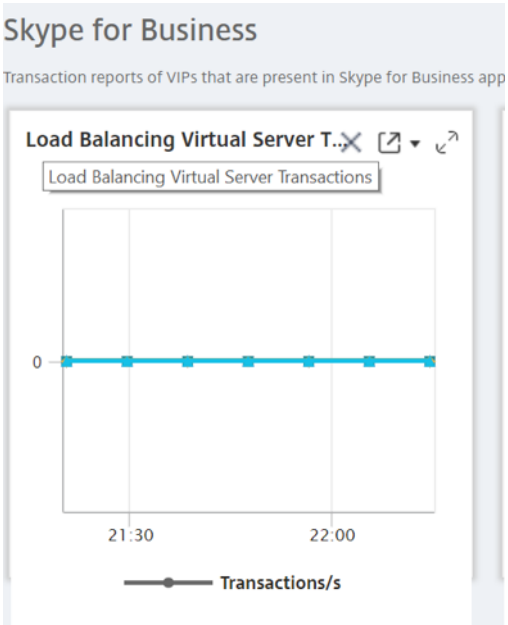
Beim Planen von Netzwerkberichten können Sie die Überschrift des Berichts anpassen, indem Sie eine Textzeichenfolge in das Feld **Betreff** eingeben. Der zum geplanten Zeitpunkt erstellte Bericht hat diese Zeichenfolge als Namen.

Beispielsweise können Sie für Netzwerkberichte, die von einem bestimmten virtuellen Server stammen, den Betreff als “authentication-reports-10.106.118.120”eingeben, wobei 10.106.118.120 die IP-Adresse des überwachten virtuellen Servers ist.

> **Hinweis**
>
> Derzeit ist diese Option nur verfügbar, wenn Sie den Export von Berichten planen. Sie können dem Bericht keine Überschrift hinzufügen, wenn Sie sie sofort exportieren.

So exportieren Sie Widget-Berichte:

1. Navigieren Sie zu **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**.



So verwalten Sie Schwellenwerte für Netzwerkberichte in der NetScaler Console

Um den Status einer NetScaler-Instanz zu überwachen, können Sie Schwellenwerte für Leistungsindikatoren festlegen und Benachrichtigungen erhalten, wenn ein Schwellenwert überschrit-

ten wird. In der NetScaler Console 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 überschreitet oder unterschreitet (wie in der Regel angegeben), wird ein Ereignis mit dem angegebenen Schweregrad generiert, das auf ein leistungsbezogenes Problem hinweist. 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 das Feld **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 der NetScaler Console 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**. Eine NetScaler-Instanz.
    - **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 das Feld **Ereignisse** nach Schweregrad klicken, um Ereignisse nach Schweregrad anzuzeigen.

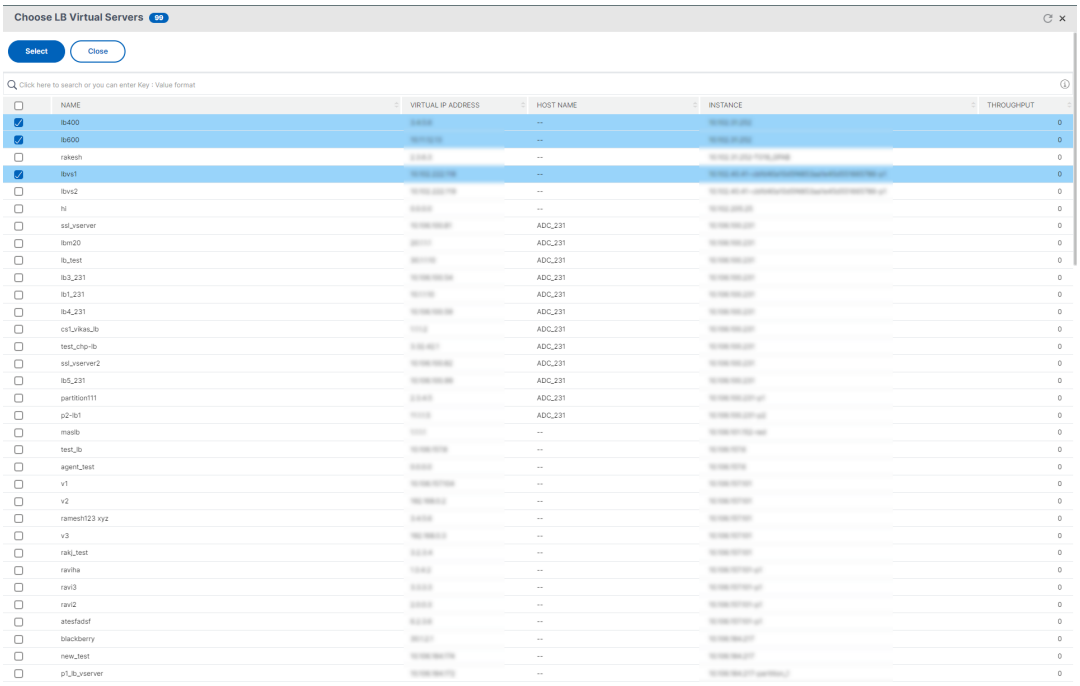
- **Wert löschen**. Geben Sie den Wert ein, der angibt, wann der Wert gelöscht werden soll. Beispielsweise können Sie den Schwellenwert Aktuelle Clientverbindungen löschen, wenn der überwachte Wert 50 Prozent erreicht. Geben Sie in diesem Fall 50 als Löschwert ein.
- **Schwere des Ereignisses**. Wählen 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.



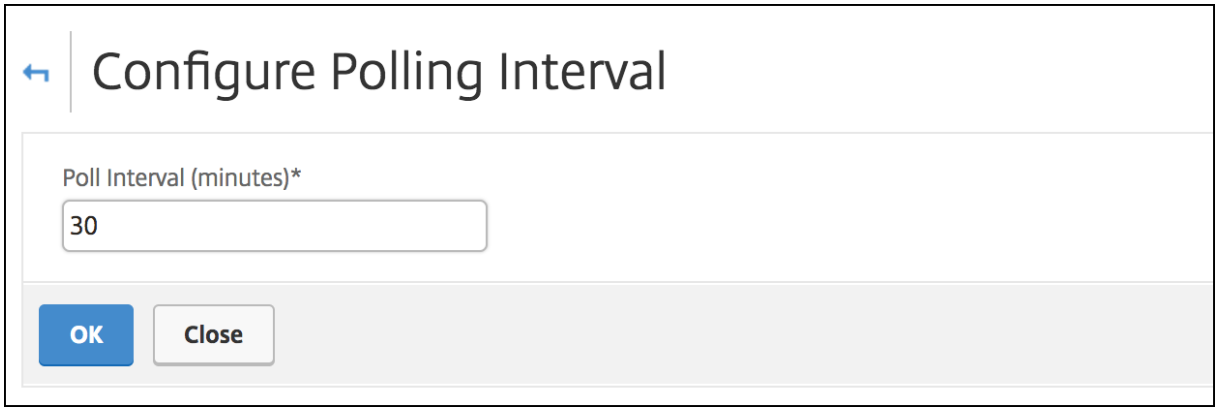
     Wählen Sie die Entitäten aus, für die Sie einen Schwellenwert festlegen möchten. Klicken Sie auf **Select**. Die ausgewählten Entitäten werden im Abschnitt **Instanzen** angezeigt.

5. Sie können wählen, dass eine Meldung angezeigt wird, wenn der Schwellenwert erreicht ist. Geben Sie im Abschnitt **Ereignismeldung** die Nachricht in das Nachrichtenfeld ein. NetScaler Console hängt den überwachten Wert und den Schwellenwert an diese Nachricht an.
6. Wählen Sie im Abschnitt **Benachrichtigungseinstellungen** die Option **Schwellenwert aktivieren** aus, um den Schwellenwert zum Generieren von Alarmen zu aktivieren. Optional können Sie **Per E-Mail benachrichtigen** auswählen, um Benachrichtigungen über verschiedene Kanäle wie E-Mail, Slack, ServiceNow oder PagerDuty zu erhalten, wenn der Schwellenwert erreicht ist.
7. Klicken Sie auf **Erstellen**.

Festlegen des Intervalls für Leistungsabfragen

Standardmäßig erfassen NITRO -Aufrufe alle 5 Minuten Leistungsdaten für das Netzwerk-Reporting. Die NetScaler Console ruft Instanzstatistiken wie Zählerinformationen ab und aggregiert sie 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** Das Abrufintervall darf nicht weniger als 5 Minuten oder mehr als 60 Minuten betragen.



Konfigurieren von Netzwerkberichterstattungseinstellungen

Sie können das Bereinigungsintervall von Netzwerkberichtsdaten in NetScaler Console konfigurieren. Dieses Intervall begrenzt die Menge der Netzwerkberichtsdaten, die in der Datenbank des NetScaler Console-Servers gespeichert werden. Standardmäßig erfolgt die Beschneidung alle 24 Stunden (um 01.00 Uhr) für das Netzwerk, das historische Daten meldet.

> **Hinweis**
>
> Der Wert, den Sie angeben können, darf 90 Tage oder weniger als 1 Tag betragen.

Provisioning von NetScaler VPX Instanzen in AWS

January 26, 2024

Wenn Sie Ihre Anwendungen in die Cloud verlagern, nehmen die Komponenten, die Teil Ihrer Anwendung sind, zu, werden stärker verteilt und müssen dynamisch verwaltet werden.

Mit NetScaler VPX-Instanzen auf AWS können Sie Ihren L4-L7-Netzwerkstack nahtlos auf AWS erweitern. Mit NetScaler VPX wird AWS zu einer natürlichen Erweiterung Ihrer on-premises IT-Infrastruktur. Sie können NetScaler VPX in AWS verwenden, um die Elastizität und Flexibilität der Cloud mit denselben Optimierungs-, Sicherheits- und Kontrollfunktionen zu kombinieren, die auch die anspruchsvollsten Websites und Anwendungen der Welt unterstützen.

Mit der NetScaler Console, die Ihre NetScaler-Instanzen überwacht, erhalten Sie Einblick in den Zustand, die Leistung und die Sicherheit Ihrer Anwendungen. Sie können die Einrichtung, Bereitstellung und Verwaltung Ihrer Anwendungsbereitstellungsinfrastruktur in hybriden Multi-Cloud-Umgebungen automatisieren.

AWS-Terminologie

Der folgende Abschnitt enthält eine kurze Beschreibung der in diesem Dokument verwendeten AWS-Begriffe:

Begriff	Definition
Amazon Machine Image (AMI)	Ein Maschinenimage, das die Informationen bereitstellt, die zum Starten einer Instanz erforderlich sind, bei der es sich um einen virtuellen Server in der Cloud handelt.
Elastic Compute Cloud (EC2)	Ein Webservice, der sichere, skalierbare Rechenkapazität in der Cloud bereitstellt. Es wurde entwickelt, um Web-basierte Cloud Computing für Entwickler einfacher zu machen.
Elastische Netzwerkschnittstelle (ENI)	Eine virtuelle Netzwerkschnittstelle, die Sie an eine Instanz in einer VPC anhängen können.

Begriff	Definition
Instanztyp	Amazon EC2 bietet eine große Auswahl an Instanztypen, die für verschiedene Anwendungsfälle optimiert sind. Instanztypen umfassen unterschiedliche Kombinationen von CPU-, Arbeitsspeicher-, Speicher- und Netzwerkkapazität und bieten Ihnen die Flexibilität, den geeigneten Ressourcenmix für Ihre Anwendungen auszuwählen.
Identitäts- und Zugriffsmanagement (IAM) -Rolle	Eine AWS-Identität mit Berechtigungsrichtlinien, die bestimmen, was die Identität in AWS tun kann und nicht. Sie können eine IAM-Rolle verwenden, um Anwendungen, die auf einer EC2-Instanz ausgeführt werden, den sicheren Zugriff auf Ihre AWS-Ressourcen zu ermöglichen.
Sicherheitsgruppen	Ein benannter Satz zulässiger eingehender Netzwerkverbindungen für eine Instanz.
Subnetze	Ein Segment des IP-Adressbereichs einer VPC, an den EC2-Instanzen angehängt werden können. Sie können Subnetze erstellen, um Instanzen entsprechend den Sicherheits- und Betriebsanforderungen zu gruppieren.
Virtuelle Private Cloud (VPC)	Ein Webservice zum Provisioning eines logisch isolierten Abschnitts der AWS-Cloud, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können.

Voraussetzungen

Dieses Dokument setzt Folgendes voraus:

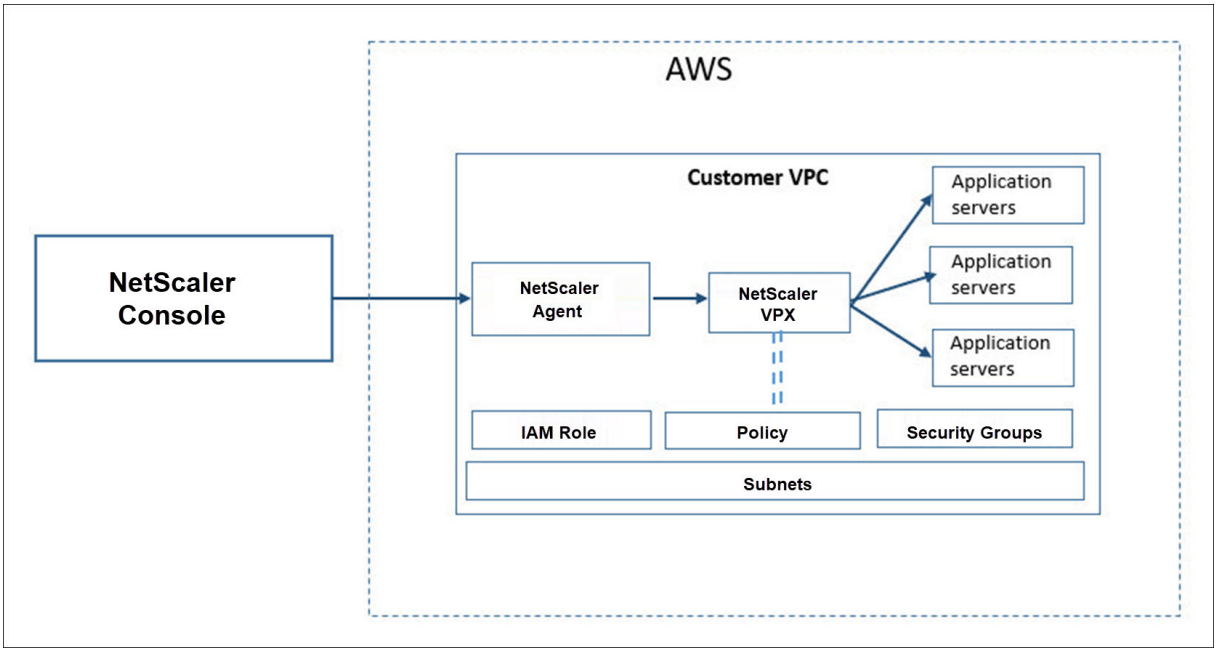
- Sie besitzen ein AWS-Konto.
- Sie haben die erforderliche VPC erstellt und die Availability Zones ausgewählt.
- Sie haben den Agenten in AWS hinzugefügt.

Weitere Informationen zum Erstellen eines Kontos und zu anderen Aufgaben finden Sie in der AWS-Dokumentation.

Weitere Informationen zur Installation eines Agenten auf AWS finden Sie unter Installieren eines NetScaler-Agenten auf AWS.

Architekturdiagramm

Das folgende Bild bietet einen Überblick darüber, wie sich NetScaler Console mit AWS verbindet, um NetScaler VPX-Instanzen in AWS bereitzustellen.



Konfigurationsaufgaben

Führen Sie die folgenden Aufgaben auf AWS aus, bevor Sie NetScaler VPX-Instanzen in der NetScaler Console bereitstellen:

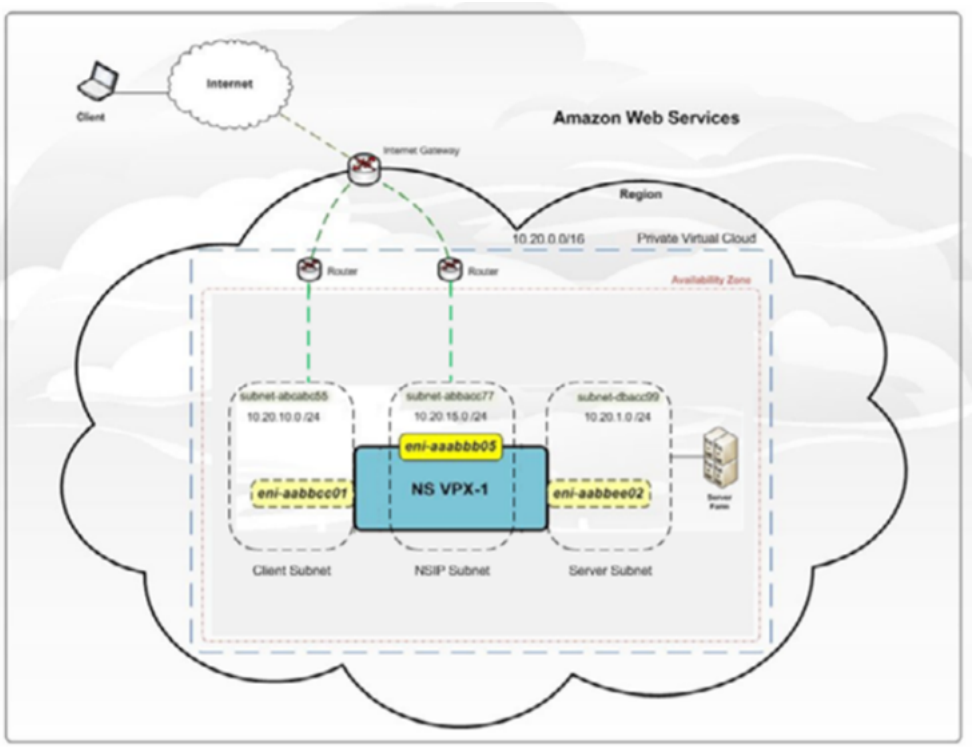
- Subnetze erstellen
- Erstellen von Sicherheitsgruppen
- Erstellen Sie eine IAM-Rolle und definieren Sie eine Richtlinie

Führen Sie die folgenden Aufgaben auf der NetScaler Console aus, um die Instanzen auf AWS bereitzustellen:

- Site erstellen
- Bereitstellen einer NetScaler VPX Instanz auf AWS

So erstellen Sie Subnetze

Erstellen Sie drei Subnetze in Ihrer VPC. Die drei Subnetze, die für die Bereitstellung von NetScaler VPX-Instanzen in Ihrer VPC erforderlich sind, sind Verwaltung, Client und Server. Geben Sie einen IPv4 CIDR-Block aus dem Bereich an, der in Ihrer VPC für jedes der Subnetze definiert ist. Geben Sie die Verfügbarkeitszone an, in der sich das Subnetz befinden soll. Erstellen Sie alle drei Subnetze in derselben Availability Zone. Die folgende Abbildung veranschaulicht die drei in Ihrer Region erstellten Subnetze und deren Konnektivität mit dem Clientsystem.



Weitere Informationen zu VPC und Subnetzen finden Sie unter VPCs und Subnetze.

So erstellen Sie Sicherheitsgruppen

Erstellen Sie eine Sicherheitsgruppe zur Steuerung des eingehenden und ausgehenden Datenverkehrs in der NetScaler VPX Instanz. Eine Sicherheitsgruppe fungiert als virtuelle Firewall für Ihre Instanz. Erstellen Sie Sicherheitsgruppen auf Instanzebene und nicht auf Subnetzebene. Es ist möglich, jede Instanz in einem Subnetz in Ihrer VPC einem anderen Satz von Sicherheitsgruppen zuzuweisen. Fügen Sie Regeln für jede Sicherheitsgruppe hinzu, um den eingehenden Datenverkehr zu steuern, der durch das Clientsubnetz an Instanzen weitergeleitet wird. Sie können auch einen separaten Regelsatz hinzufügen, der den ausgehenden Datenverkehr steuert, der durch das Serversubnetz zu den Anwendungsservern geleitet wird. Obwohl Sie die Standardsicherheitsgruppe für Ihre Instanzen verwenden können, möchten Sie möglicherweise Ihre Gruppen erstellen. Erstellen Sie drei

Sicherheitsgruppen - eine für jedes Subnetz. Erstellen Sie Regeln für eingehenden und ausgehenden Datenverkehr, die Sie steuern möchten. Sie können beliebig viele Regeln hinzufügen.

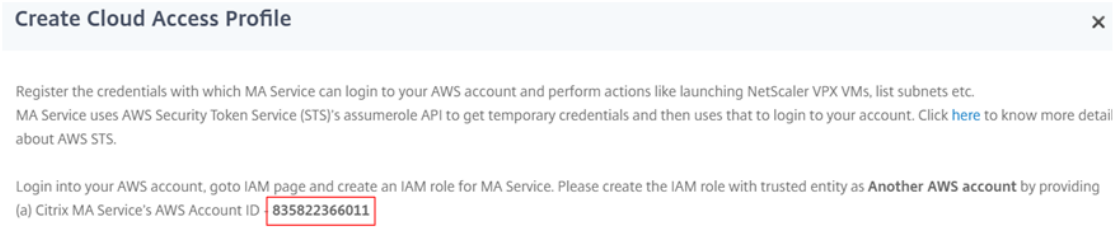
Weitere Informationen zu Sicherheitsgruppen finden Sie unter Sicherheitsgruppen für Ihre VPC.

So erstellen Sie eine IAM-Rolle und definieren eine Richtlinie

Erstellen Sie eine IAM-Rolle, damit Sie eine Vertrauensstellung zwischen Ihren Benutzern und dem vertrauenswürdigen Citrix AWS-Konto einrichten und eine Richtlinie mit Citrix Berechtigungen erstellen können.

1. Klicken Sie in AWS auf **Services** . Wählen Sie im linken Navigationsbereich **IAM > Rollen**, und klicken Sie auf **Rolle erstellen**.
2. Sie verbinden Ihr AWS-Konto mit dem AWS-Konto in NetScaler Console. Wählen Sie also ein **anderes AWS-Konto** aus, damit NetScaler Console Aktionen in Ihrem AWS-Konto ausführen kann.

   Geben Sie die 12-stellige NetScaler Console AWS-Konto-ID ein. Die Citrix ID lautet 835822366011. Sie finden die Citrix ID auch in NetScaler Console, wenn Sie das Cloud-Zugriffsprofil erstellen.

3. Aktivieren Sie **Externe ID erforderlich**, um eine Verbindung mit einem Drittanbieterkonto herzustellen. Sie können die Sicherheit Ihrer Rolle erhöhen, indem Sie eine optionale externe Kennung benötigen. Geben Sie eine ID ein, die eine Kombination aus beliebigen Zeichen sein kann.
4. Klicken Sie auf **Berechtigungen**.
5. Klicken Sie auf der Seite **Berechtigungsrichtlinien anhängen** auf **Richtlinie erstellen**.
6. Sie können eine Richtlinie im visuellen Editor oder mithilfe von JSON erstellen und bearbeiten.

   Die Liste der Berechtigungen von Citrix finden Sie im folgenden Feld:

```
{

"Version": "2012-10-17",
"Statement":
[
    {

```



```
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRegions",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeHosts",
                "ec2:DescribeImages",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeTags",
                "ec2:DescribeVolumeStatus",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumeAttribute",
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:CreateKeyPair",
                "ec2:DeleteKeyPair",
                "ec2:ResetInstanceAttribute",
                "ec2:RunScheduledInstances",
                "ec2:ReportInstanceStatus",
                "ec2:StartInstances",
                "ec2:RunInstances",
                "ec2:StopInstances",
                "ec2:UnmonitorInstances",
                "ec2:MonitorInstances",
                "ec2:RebootInstances",
                "ec2:TerminateInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:CreateNetworkInterface",
                "ec2:AttachNetworkInterface",
                "ec2:DetachNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:ResetNetworkInterfaceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:AssociateAddress",
                "ec2:AllocateAddress",
                "ec2:ReleaseAddress",
                "ec2:DisassociateAddress",
                "ec2:GetConsoleOutput"
            ],
                "Resource": "*"
        }
```



```
61
62  ]
63   }
```

7. Kopieren Sie die Liste der Berechtigungen, fügen Sie sie in die Registerkarte JSON ein und klicken Sie auf **Richtlinie überprüfen**.
8. Geben Sie auf der Seite **Richtlinie überprüfen** einen Namen für die Richtlinie ein, geben Sie eine Beschreibung ein und klicken Sie auf **Richtlinie erstellen**.

So erstellen Sie eine Site in NetScaler Console

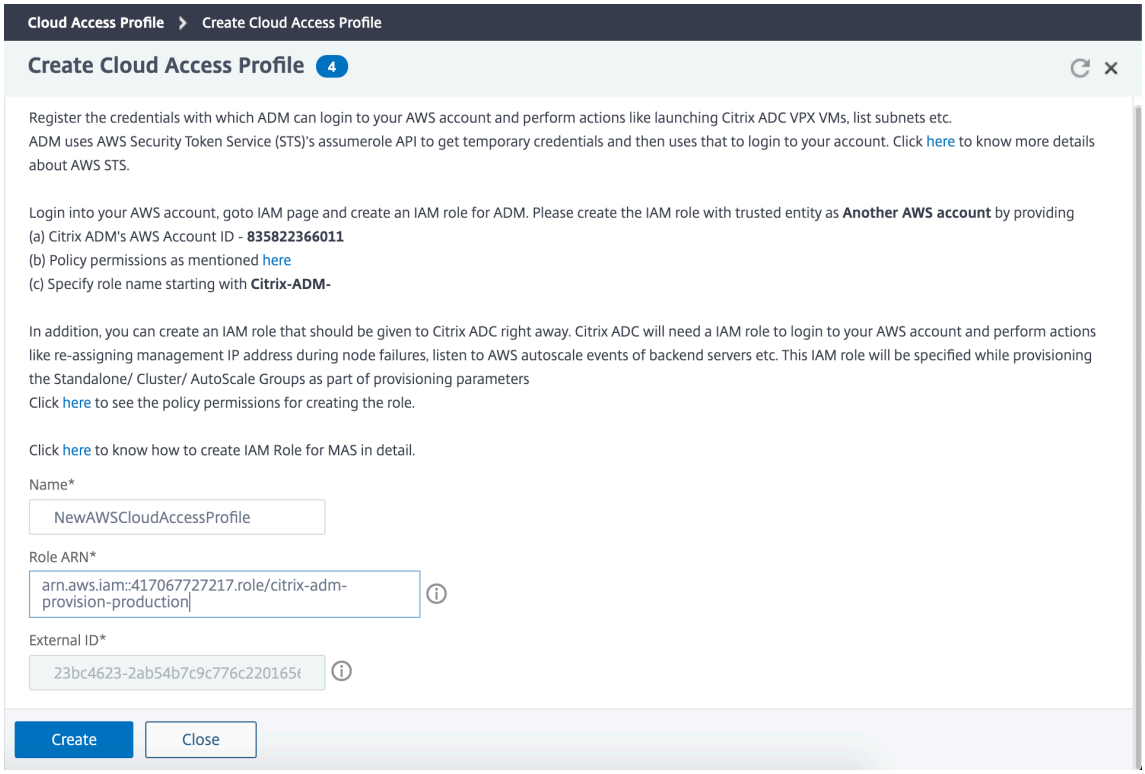
Erstellen Sie eine Site in NetScaler Console und fügen Sie die Details der VPC hinzu, die Ihrer AWS-Rolle zugeordnet ist.

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Sites** .
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie den Servicetyp als AWS aus und aktivieren **Sie Vorhandene VPC als Site verwenden**.
4. Wählen Sie das Cloud-Zugriffsprofil aus.
5. Wenn das Cloud-Zugriffsprofil im Feld nicht vorhanden ist, klicken Sie auf **Hinzufügen**, um ein Profil zu erstellen.

    a) Geben Sie auf der Seite **Cloud-Zugriffsprofil erstellen** den Namen des Profils ein, mit dem Sie auf AWS zugreifen möchten.

    b) Geben Sie den ARN ein, der der Rolle zugeordnet ist, die Sie in AWS erstellt haben.

    c) Geben Sie die externe ID ein, die Sie beim Erstellen einer Identitäts- und Zugriffsmanagementrolle (IAM) in AWS angegeben haben. Siehe Schritt 4 unter So erstellen Sie eine IAM-Rolle und definieren eine Richtlinienaufgabe. Stellen Sie sicher, dass der in AWS angegebene IAM-Rollenname mit Citrix-ADM- beginnt und im Rollen-ARN korrekt angezeigt wird.



Die Details der VPC, wie Region, VPC-ID, Name und CIDR-Block, die Ihrer IAM-Rolle in AWS zugeordnet sind, werden in NetScaler Console importiert.

6. Geben Sie einen Namen für die Site ein.
7. Klicken Sie auf **Erstellen**.

So stellen Sie NetScaler VPX auf AWS bereit

Verwenden Sie die zuvor erstellte Site, um die NetScaler VPX-Instanzen in AWS bereitzustellen. Geben Sie die Agentendetails an, um die Instanzen bereitzustellen, die an diesen Agenten gebunden sind.

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Instanzen NetScaler**.
2. Klicken Sie auf der Registerkarte **VPX** auf **Bereitstellung**.

   Mit dieser Option wird die Seite **NetScaler VPX in der Cloud bereitstellen** angezeigt.
3. Wählen Sie **Amazon Web Services (AWS)** aus und klicken Sie auf **Weiter**.
4. Auf der Registerkarte **Grundlegende Parameter**

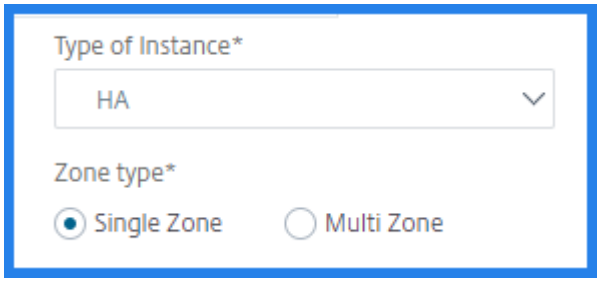
   a) Wählen Sie in der Liste den **Instanztyp** aus.

   - **Standalone:** Diese Option stellt eine eigenständige NetScaler VPX-Instanz in AWS bereit.

- **HA:** Diese Option stellt die hochverfügbaren NetScaler VPX-Instanzen in AWS bereit.

  Um die NetScaler VPX-Instanzen in derselben Zone bereitzustellen, wählen Sie unter **Zonentyp** die Option **Einzelne Zone** aus.

  Um die NetScaler VPX Instanzen über mehrere Zonen hinweg bereitzustellen, wählen Sie unter **Zonentyp** die Option **Multi Zone** aus. Stellen Sie sicher, dass Sie auf der Registerkarte **Bereitstellungsparameter** die Netzwerkdetails für jede Zone angeben, die in AWS erstellt wurde.



b) Geben Sie den Namen einer NetScaler VPX-Instanz an.

c) Wählen Sie unter **Site** die Website aus, die Sie zuvor erstellt haben.

d) Wählen Sie unter **Agent**den Agent aus, der für die Verwaltung der NetScaler VPX-Instanz erstellt wurde.

e) Wählen Sie im **Cloud Access-Profil** das Cloud-Zugriffsprofil aus, das während der Website-Erstellung erstellt wurde.

f) Wählen Sie unter **Geräteprofil** das Profil für die Authentifizierung aus.

   NetScaler Console verwendet das Geräteprofil, wenn eine Anmeldung bei der NetScaler VPX-Instanz erforderlich ist.

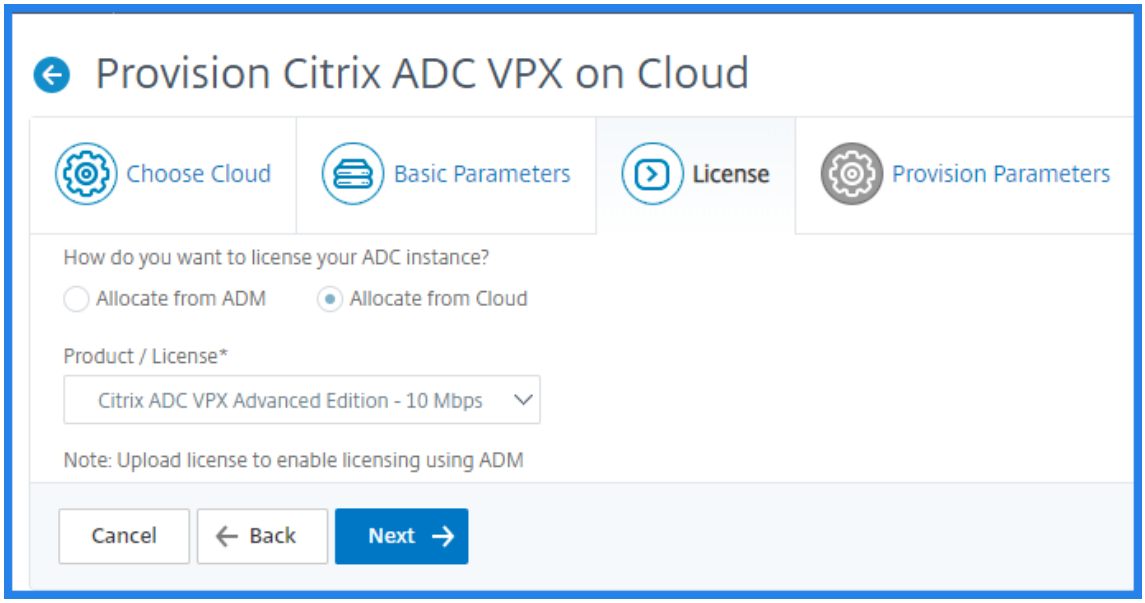
g) Klicken Sie auf **Weiter**.

5. Wählen Sie auf der Registerkarte **Lizenz** einen der folgenden Modi aus, um die Lizenz auf eine NetScaler-Instanz anzuwenden:

   - **NetScaler Console**verwenden : Die Instanz, die Sie bereitstellen möchten, checkt die Lizenzen aus der NetScaler Console aus.
   - **Nutzung der AWS-Cloud**: Die Option **Allocate from Cloud** verwendet die NetScaler-Produktlizenzen, die auf dem AWS-Marketplace verfügbar sind. Die Instanz, die Sie bereitstellen möchten, verwendet die Lizenzen des Marketplace.

     Wenn Sie sich für die Verwendung von Lizenzen aus dem AWS-Marketplace entscheiden, geben Sie das Produkt oder die Lizenz auf der Registerkarte **Bereitstellungsparameter** an.

Weitere Informationen finden Sie unter Lizenzanforderungen.



6. Wenn Sie auf der Registerkarte **Lizenz** die Option Aus der **NetScaler Console zuweisen** auswählen, geben Sie Folgendes an:

   - Lizenztyp - Wählen Sie entweder Bandbreiten- oder virtuelle CPU-Lizenzen aus:

     Bandbreitenlizenzen: Sie können eine der folgenden Optionen aus der Liste **Bandbreitenlizenztypen** auswählen:

     - **Pooled Capacity:** Geben Sie die Kapazität an, die einer Instanz zugewiesen werden soll.

       Aus dem gemeinsamen Pool checkt die NetScaler-Instanz eine Instanzlizenz aus, und es wird nur so viel Bandbreite angegeben.

     - **VPX-Lizenzen:**Wenn eine NetScaler VPX-Instanz bereitgestellt wird, checkt die Instanz die Lizenz von der NetScaler Console aus.

     Virtuelle CPU-Lizenzen: Die bereitgestellte NetScaler VPX-Instanz checkt Lizenzen abhängig von der Anzahl der in der Instanz ausgeführten CPUs aus.

     > **Hinweis** Wenn die bereitgestellten Instanzen entfernt oder zerstört werden, kehren die angewendeten Lizenzen in den NetScaler Console-Lizenzpool zurück. Diese Lizenzen können wiederverwendet werden, um neue Instanzen bereitzustellen.

   a) Wählen Sie in **License Edition** die Lizenzversion aus. Die NetScaler Console verwendet die angegebene Edition zur Bereitstellung von Instanzen.

7. Klicken Sie auf **Weiter**.
8. Auf der Registerkarte **Bereitstellungsparameter**:

a) Wählen Sie die in AWS erstellte **Citrix IAM-Rolle** aus. Eine IAM-Rolle ist eine AWS-Identität mit Berechtigungsrichtlinien, die bestimmen, was die Identität in AWS tun kann und nicht.

b) Wählen Sie im Feld **Produkt** die NetScaler Produktversion aus, die Sie bereitstellen möchten.

c) Wählen Sie den EC2-Instanztyp aus der Liste **Instanztyp** aus.

   In dieser Liste werden die unterstützten AMI-Instanztypen für die ausgewählte NetScaler-Instance angezeigt.

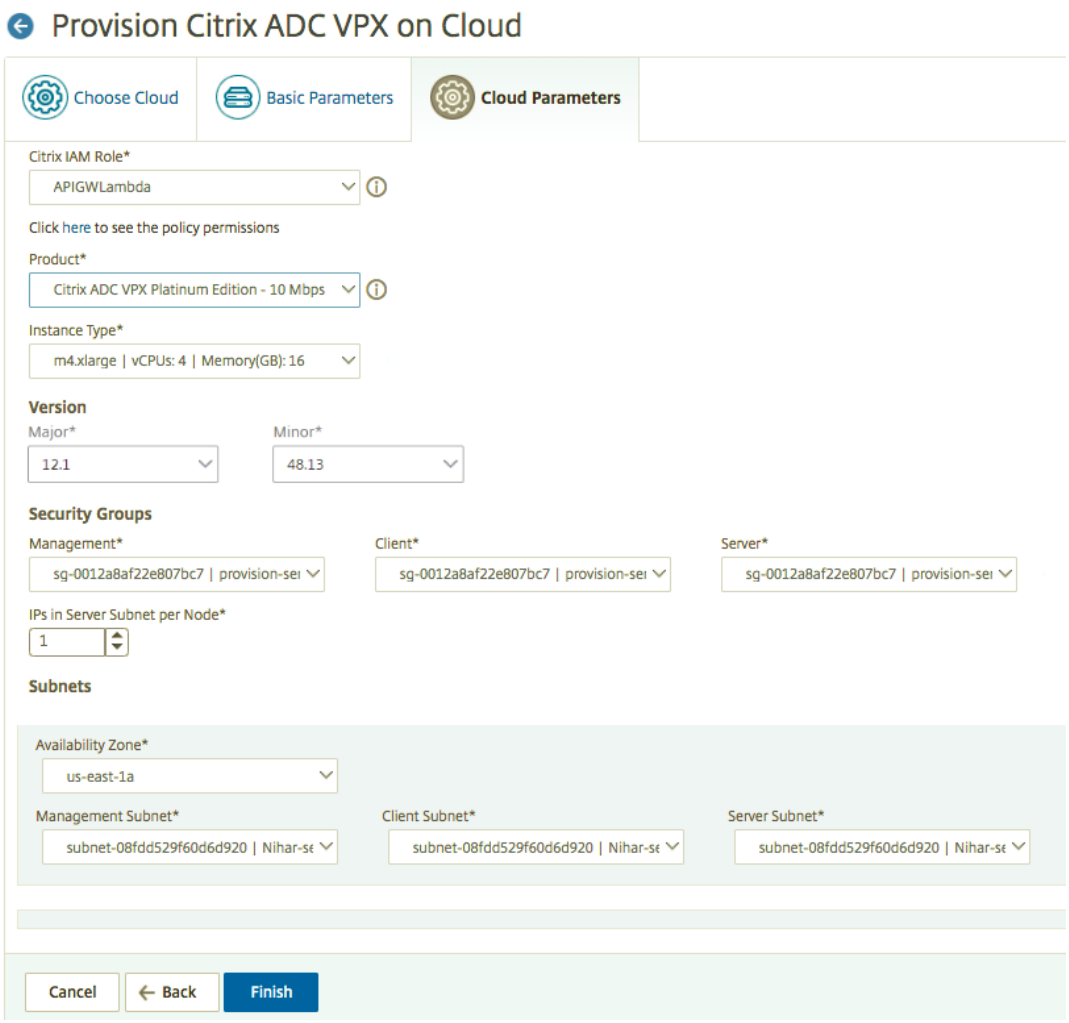
d) Wählen Sie die **Version** von NetScaler aus, die Sie bereitstellen möchten. Wählen Sie sowohl **Major** - als auch **Minor-Version** von NetScaler aus.

e) Wählen Sie **unter Sicherheitsgruppen**die Sicherheitsgruppen Verwaltung, Client und Server aus, die Sie in Ihrem virtuellen Netzwerk erstellt haben.

f) Wählen Sie unter **IPs im Server-Subnetz pro Knoten**die Anzahl der IP-Adressen im Server-subnetz pro Knoten für die Sicherheitsgruppe aus.

g) Wählen Sie **unter Subnetze**die Management-, Client- und Server-Subnetze für jede Zone aus, die in AWS erstellt werden. Sie können die Region auch aus der Liste **Availability Zone** auswählen.

h) Klicken Sie auf **Fertig stellen**.



Die NetScaler VPX Instanz wird jetzt auf AWS bereitgestellt.

> **Hinweis**
>
> Derzeit unterstützt NetScaler Console die Deprovisionierung von NetScaler-Instanzen von AWS nicht.

So zeigen Sie die in AWS bereitgestellte NetScaler VPX an

1. Navigieren Sie auf der AWS-Homepage zu **Services** und klicken Sie auf **EC2**.
2. Klicken Sie auf der Seite **Ressourcen** auf **Laufende Instanzen**.
3. Sie können das in AWS bereitgestellte NetScaler VPX anzeigen.

Der Name der NetScaler VPX-Instanz ist derselbe, den Sie bei der Bereitstellung einer Instanz in der NetScaler Console angegeben haben.

So zeigen Sie das in der NetScaler Console bereitgestellte NetScaler VPX an

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Instanzen NetScaler**.
2. Wählen Sie die Registerkarte **NetScaler VPX** .
3. Die in AWS bereitgestellte NetScaler VPX Instanz wird hier aufgelistet.

NetScaler App Delivery and Security Service Self Managed - Ansprüche

January 26, 2024

NetScaler App Delivery and Security Service Self-Managed ist die neue Methode zur Nutzung gepoolter Lizenzen mit einem hohen Automatisierungsgrad bei Lizenzierung und Kapazitätsmanagement. Kunden müssen Lizenzen nicht manuell verwalten und erhalten Flexibilität bei der Verwaltung ihres Kapazitätsbedarfs über eine hybride Multi-Cloud hinweg.

> **Voraussetzungen**
>
> Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:
>
> - Stellen Sie sicher, dass der NetScaler Agent beim NetScaler Console Service registriert ist
> - Unterstützte NetScaler-Versionen sind:
>   - Version 13.0: Verwenden Sie 13.0 - 88.12 oder höher
>   - Version 13.1: Verwenden Sie 13.1 - 30.x oder höher
> - Sie verwenden einen NetScaler Agent 13.1 - 32.x oder höher

Im Rahmen der Self-Managed-Funktion von NetScaler App Delivery and Security Service werden die Lizenzinformationen automatisch in den NetScaler Console-Service hochgeladen, sobald der Kunde einen Kauf tätigt und einen NetScaler Agent im NetScaler Console Service erstellt. Die Lizenzen werden als Teil der NetScaler Console-Infrastruktur direkt auf den License Server Agent (LSA) oder den Agenten in Ihrem VPC/Rechenzentrum heruntergeladen.

> **Hinweis**
>
> Der NetScaler App Delivery and Security Self Managed Service ist nur im NetScaler Console Service verfügbar.

NetScaler Console kann die vorhandenen Berechtigungen Pooled und NetScaler App Delivery and Security Service Self Managed hosten. Um die erforderliche Lizenz zu verwenden, konfigurieren Sie einen Lizenzserver auf der NetScaler Appliance und checken Sie die Kapazität aus dem entsprechenden Pool aus oder weisen Sie sie zu.

NetScaler App Delivery and Security Service Self Managed bietet die folgenden Funktionen:

- Erhältlich in den Editionen Standard, Advanced und Premium
- NetScaler App Delivery and Security Citrix verwaltete Premium-Anspruch von 100 TB plus 8 Millionen DNS-Abfragen für jeden selbstverwalteten Starterpool im ersten Jahr
- Starter-Pools beinhalten 1 VIP pro 1 Gbit/s oder 1 VIP pro 1 gekaufter vCPU. Zusätzliche VIPs können als Add-Ons erworben werden

Weitere Informationen zu den verfügbaren Self-Managed-Ansprüchen für NetScaler App Delivery and Security Service finden Sie unter **Infrastruktur > Self Managed**.

Sie können die IP-Adresse eines Lizenzservers auf NetScaler wie folgt konfigurieren:

- Verwenden der CLI. Weitere Informationen finden Sie unter Konfigurieren der Lizenz für den Self Managed Pool mithilfe der CLI
- Verwenden der GUI. Weitere Informationen finden Sie unter Konfigurieren der Lizenz für Self Managed Pool mithilfe der GUI

Kunden können auch Informationen wie den Ablauf und die Nutzung der Lizenz im NetScaler Console-Dienst verfolgen.

Weisen Sie NetScaler App Delivery and Security Service Self Managed-Kapazität NetScaler-Instanzen zu

January 26, 2024

Sie können Ansprüche und Kapazitäten für NetScaler App Delivery and Security Service Self Managed auf zwei Arten zuweisen:

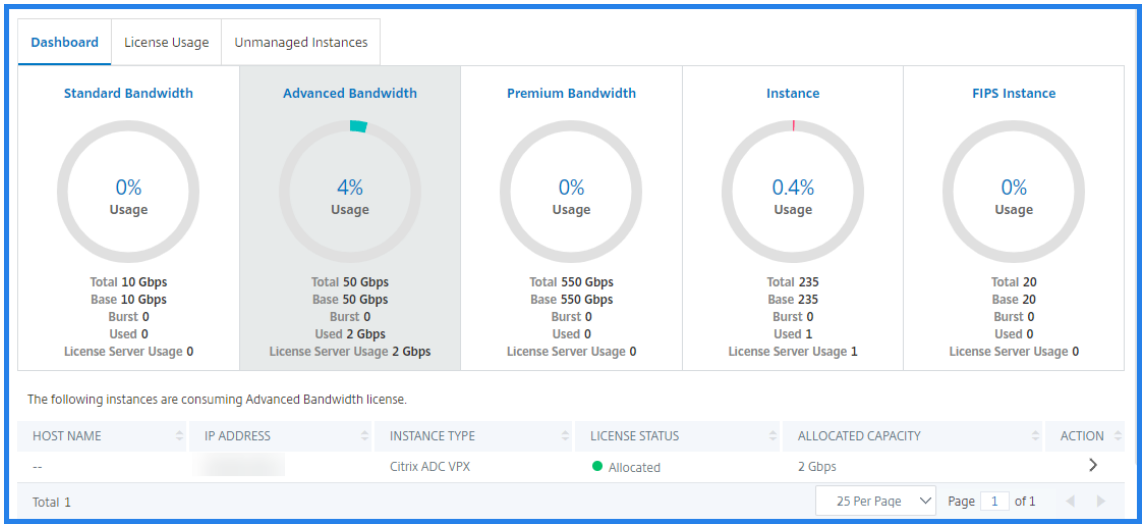
- Verwenden der NetScaler-Instanz
- Verwenden von ADM, wenn NetScaler von ADM verwaltet wird.

So weisen Sie NetScaler App Delivery and Security Service Self Managed-Kapazität über die NetScaler Console-GUI zu:

1. Melden Sie sich bei NetScaler Console an.
2. Navigieren Sie zu **Infrastruktur > Selbstverwaltet > Bandbreitenlizenzen > Selbstverwalteter Pool**
3. Klicken Sie auf den Lizenzpool, den Sie verwalten möchten —Standard, Advanced oder Premium.

> **Hinweis**
>
> Das Feld **Zugeordnete Kapazität** spiegelt die geänderte Bandbreite nicht sofort wider. Die Bandbreitenänderung wird nach dem NetScaler-Warm-Neustart wirksam.
>
> In den **Zuordnungsdetails** werden die Felder **Angefordert** und **Angewendet** aktualisiert, wenn Sie die Bandbreitenzuweisung der Instanz ändern.

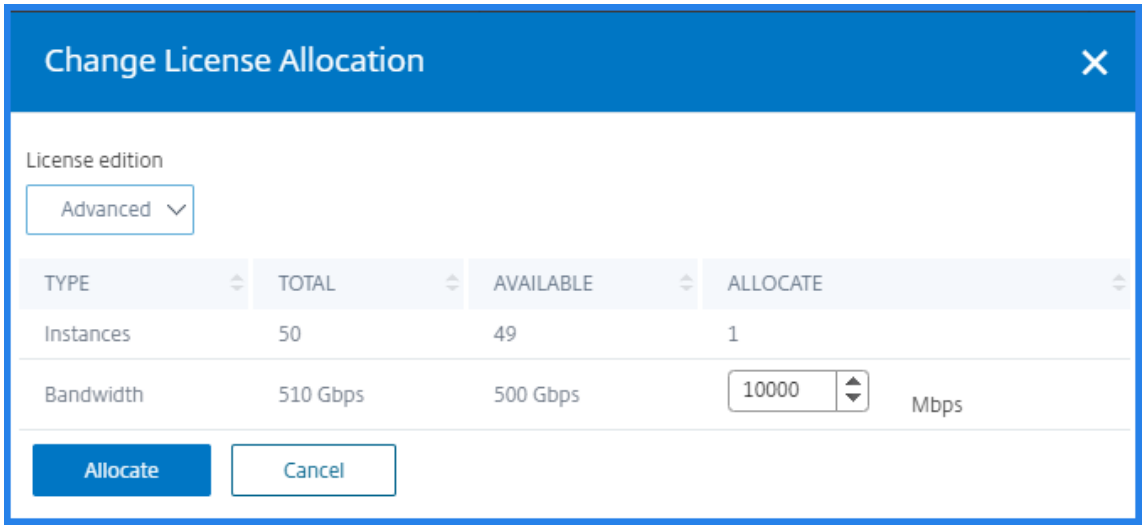
4. Wählen Sie eine NetScaler Instanz aus der Liste der verfügbaren Instanzen aus, indem Sie auf die Schaltfläche **>** klicken.



In der Spalte Lizenzstatus werden entsprechende Statusmeldungen zur Anspruchszuweisung angezeigt.

> **Hinweis** Auf der Registerkarte **Unmanaged Instances** werden die Instanzen angezeigt, die in NetScaler Console 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. Wählen Sie die Bandbreite oder Instanzzuweisung für die Instanz aus, indem Sie die Listenoptionen Zuweisen 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**.



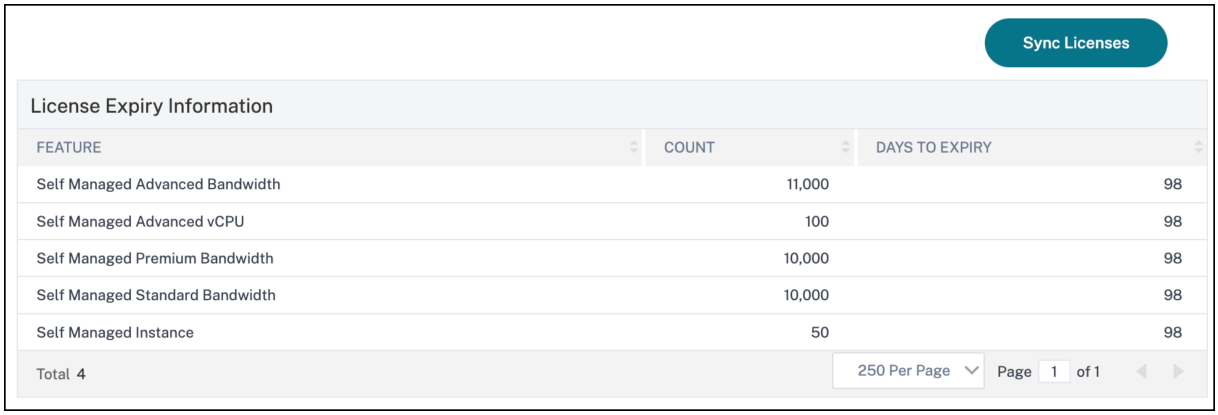
Hinweis

Warm starten Sie eine Instanz neu, wenn Sie die Lizenzversion ändern.

Anspruchsinformationen für NetScaler App Delivery and Security Service Self Managed überprüfen

January 26, 2024

Sie können die NetScaler App Delivery and Security Service Self Managed-Berechtigungen überprüfen, die in der NetScaler Console verfügbar sind, indem Sie zu **Infrastruktur > Self Managed** navigieren.



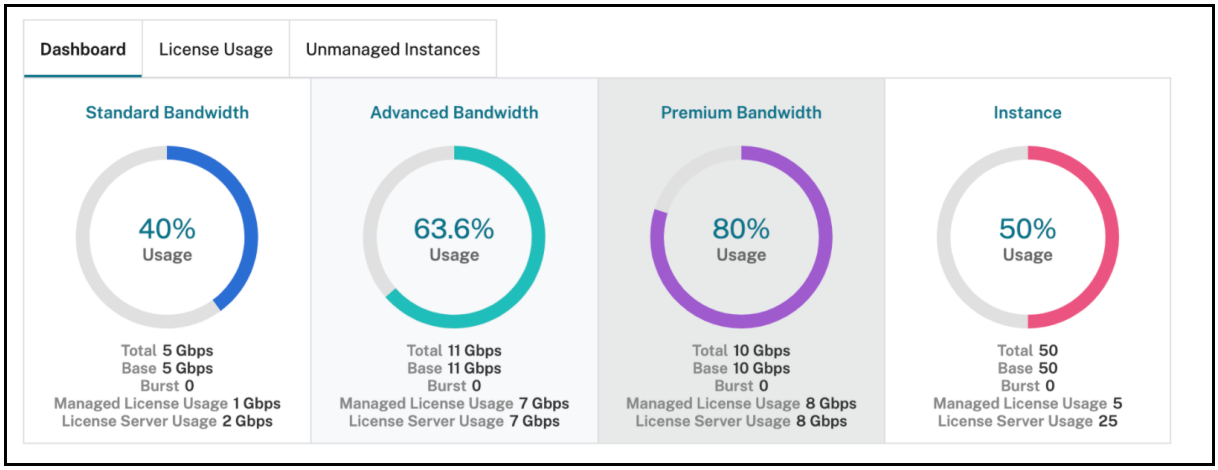
Das Dashboard zeigt die Informationen zu NetScaler App Delivery and Security Service Self Managed-Ansprüche an. Wenn die Anspruchsinformationen nicht im Dashboard angezeigt werden oder es zu Verzögerungen beim Hinzufügen der Anspruchsinformationen kommt, klicken Sie auf die Schaltfläche **Lizenzen synchronisieren**. Daraufhin werden die verfügbaren Bandbreiten-Pools, Anzahl und Ablaufinformationen angezeigt.

Weitere Informationen zum Konfigurieren von Lizenzablaufprüfungen finden Sie unter Konfigurieren von Lizenzablaufprüfungen.

Im Abschnitt **Informationen zum Ablauf der Lizenz** können Sie die Details der Lizenzen anzeigen, die ablaufen werden.

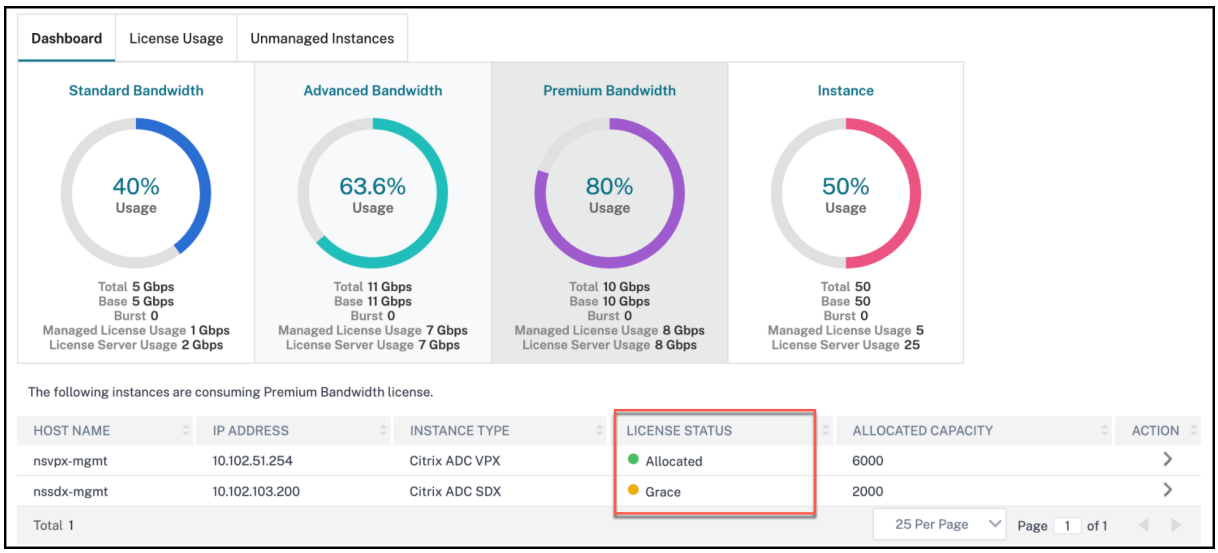
- **Funktion** —Art der Lizenz, die abläuft.
- **Anzahl** —Anzahl der virtuellen Server oder Instanzen, die betroffen sein werden.
- **Tage bis zum Ablauf** —Anzahl der Tage vor Ablauf der Lizenz.

Um die verfügbaren Pools für verschiedene Lizenzeditionen zu überprüfen, navigieren Sie zu **Infrastruktur > Selbstverwaltung > Bandbreitenlizenzen > Self Managed Pool**



Lizenznutzung überprüfen

Wenn Sie NetScaler Console als Lizenzserver für die NetScaler Pool-Capacity-Lizenz konfiguriert haben, können Sie den Status der Lizenz mithilfe der NetScaler Console-GUI überprüfen. Navigieren Sie zu **Infrastruktur > Selbstverwaltete > Gepoolte Kapazität > Lizenznutzung**.



Weitere Informationen zum Lizenzstatustyp und dessen Bedeutung finden Sie unter Überprüfen des Lizenzstatus.

Kubernetes-Cluster für Service Graph verwalten

January 26, 2024

Kubernetes (K8s) ist eine Open Source-Container-Orchestrierungsplattform, die die Bereitstellung, Skalierung und Verwaltung von Cloud-nativen Anwendungen automatisiert.

> **Hinweis**
>
> - NetScaler Console unterstützt die Sichtbarkeit von Clustern für Service Graph mit Kubernetes Version 1.14—1.23.

Sie können die folgenden Aspekte der Kubernetes-Integration in NetScaler Console angeben:

- **Cluster**—Sie können Kubernetes-Cluster registrieren oder die Registrierung aufheben, für die NetScaler Console alle Microservices überwacht und das Service-Diagramm auffüllt. Wenn Sie einen Cluster in NetScaler Console registrieren, geben Sie die Kubernetes-API-Serverinformationen an. Wählen Sie dann einen Agenten aus, der den Kubernetes-Cluster erreichen kann.

Voraussetzungen

Um Ihre Microservices auf Kubernetes-Clustern zu überwachen und zu visualisieren und mit Service Graph loszulegen, stellen Sie sicher, dass Sie über Folgendes

- Kubernetes Cluster an Ort und Stelle.
- Der Agent wurde installiert und konfiguriert, um die Kommunikation zwischen NetScaler Console und Kubernetes-Cluster oder verwalteten Instanzen zu ermöglichen. Sie können die verwalteten Instanzen verwenden, die in Ihrem Rechenzentrum oder Ihrer Cloud vorhanden sind.
- Kubernetes-Cluster, der in NetScaler Console registriert ist.

Konfigurieren Sie den NetScaler Agent für die Registrierung beim Kubernetes-Cluster

Um die Kommunikation zwischen Kubernetes-Cluster und NetScaler Console zu ermöglichen, müssen Sie einen Agenten installieren und konfigurieren. Sie können einen Agent auf den folgenden Plattformen bereitstellen:

- Hypervisor (ESX, XenServer, KVM, Hyper-V)
- Öffentliche Cloud-Dienste (wie Microsoft Azure, AWS)

Folgen Sie den Anweisungen, um einen Agent zu konfigurieren.

> **Hinweis**
>
> Sie können auch einen vorhandenen Agenten verwenden, falls bereits einer bereitgestellt wurde.

Konfigurieren Sie die NetScaler Console mit einem geheimen Token zur Verwaltung eines Kubernetes-Clusters

Damit NetScaler Console Ereignisse von Kubernetes empfangen kann, müssen Sie in Kubernetes für NetScaler Console ein Dienstkonto erstellen. Konfigurieren Sie das Dienstkonto mit den erforderlichen RBAC-Berechtigungen im Cluster.

1. Erstellen Sie ein Dienstkonto für NetScaler Console. 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 Console-Konto 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
   ```

   Nachdem das NetScaler Console-Konto an die `cluster-admin`Rolle gebunden wurde, hat das Dienstkonto 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:

   ```
   1 kubectl describe sa citrixadm-sa
   ```

4. Führen Sie den folgenden Befehl aus, um die geheime Zeichenfolge des Tokens abzurufen:

   ```
   1 kubectl describe secret <token-name>
   ```

Fügen Sie den Kubernetes-Cluster in NetScaler Console hinzu

Nachdem Sie einen Agenten konfiguriert und statische Routen konfiguriert haben, müssen Sie den Kubernetes-Cluster in NetScaler Console registrieren.

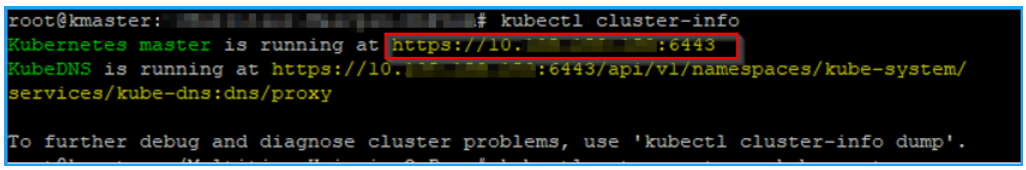
So registrieren Sie den Kubernetes-Cluster:

1. Melden Sie sich mit Administratoranmeldeinformationen an der NetScaler Console an.
2. Navigieren Sie zu **Orchestration** > **Kubernetes** > **Cluster**.
   Die Seite “Cluster”wird angezeigt.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie auf der Seite **Cluster hinzufügen** die folgenden Parameter an:

   a) **Name** - Geben Sie einen Namen Ihrer Wahl an.

   b) **API-Server-URL** —Sie können die API-Server-URL-Details vom Kubernetes-Master-Knoten abrufen.

      i. Führen Sie auf dem Kubernetes-Masterknoten den Befehl aus `kubectl cluster-info`.

      ii. Geben Sie die URL ein, die für **Kubernetes master is running at** angezeigt wird.

   c) **Authentifizierungstoken**—Geben Sie die Zeichenfolge für das Authentifizierungstoken an, die Sie erhalten haben, während Sie NetScaler Console für die Verwaltung eines Kubernetes-Clusters konfigurieren . Das Authentifizierungstoken ist erforderlich, um den Zugriff für die Kommunikation zwischen Kubernetes-Cluster und NetScaler Console zu validieren. So generieren Sie ein Authentifizierungstoken:

      i. Führen Sie auf dem Kubernetes-Masterknoten die folgenden Befehle aus:

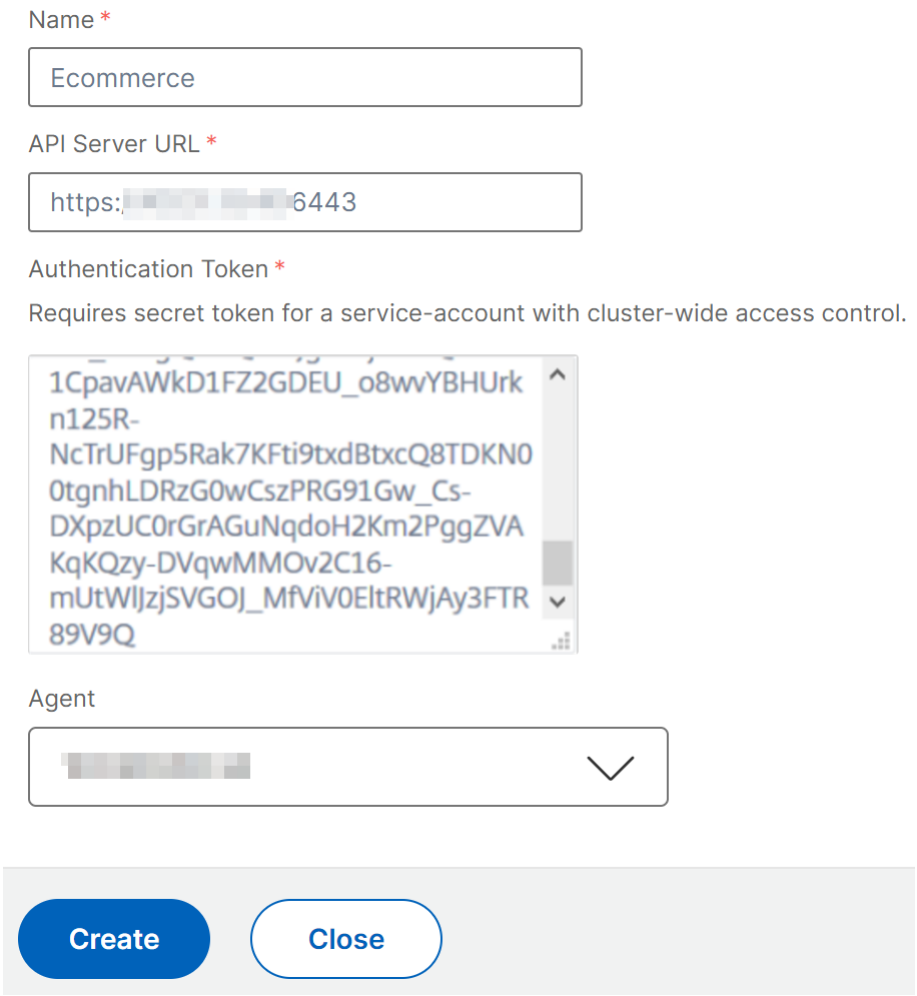

```
kubectl describe secret <token-name>
```

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**.



Lizenzmanagement für flexible und gepoolte Lizenzen

September 2, 2024

> **Hinweis:**
>
> Wenn Sie eine Universal Hybrid Multi-Cloud (UHMC) oder eine Citrix Platform-Lizenz (CPL) erwerben, werden die bereitgestellten NetScaler-Lizenzen als Flexed-Lizenzen bezeichnet.

Lizenzdateien

Die NetScaler Flexed-Lizenz umfasst die folgenden Dateien, die Sie vom MyCitrix-Portal herunterladen müssen. Weitere Informationen zum Übergang von Ihrer aktuellen NetScaler-Lizenzierung zur Flexed-Lizenzierung finden Sie unter Umstellung auf Flexed-Lizenzierung.

Die auf Ihrem NetScaler vorhandenen Lizenzdateien sind in diesem Abschnitt aufgeführt.

Der Dateiname enthält	Beschreibung	Informationen herunterladen	Wo kann die Lizenz hochgeladen/angewendet werden
NetScaler Flexed VPX SW-Instanz	Berechtigt Sie zu VPX/CPX/BLX-Softwareinstanzen	Laden Sie diese Datei mit Ihrer NetScaler Console-Host-ID herunter	Auf der NetScaler Console
NetScaler Flexed MPX SW-Instanz	Berechtigt Sie zu MPX-Softwareinstanzen	Laden Sie diese Datei mit Ihrer NetScaler Console-Host-ID herunter	Auf der NetScaler Console
NetScaler Flexed SDX SW-Instanz	Berechtigt Sie zu SDX-Softwareinstanzen	Laden Sie diese Datei mit Ihrer NetScaler Console-Host-ID herunter	Auf der NetScaler Console
NetScaler Flexed Platinum BW	Berechtigt Sie zur Nutzung der Flexed-Platinum-Durchsatzkapazität	Laden Sie diese Datei mit Ihrer NetScaler Console-Host-ID herunter	Auf der NetScaler Console
NetScaler Flexed VPX FIPS SW-Instanz	Berechtigt Sie zu VPX FIPS-Softwareinstanzen	Laden Sie diese Datei mit Ihrer NetScaler Console-Host-ID herunter	Auf der NetScaler Console

Der Dateiname enthält	Beschreibung	Informationen herunterladen	Wo kann die Lizenz hochgeladen/angewendet werden
MPX-Z-Plattformlizenz ohne Kapazität	Ermächtigt Sie, Ihre NetScaler MPX HW an der Flexed-Lizenzierung teilnehmen zu lassen	Laden Sie diese Datei herunter	Auf NetScaler MPX
SDX-Z-Plattformlizenz ohne Kapazität	Ermächtigt Sie, Ihre NetScaler SDX HW an der Flexed-Lizenzierung teilnehmen zu lassen	Laden Sie diese Datei herunter	Auf NetScaler SDX

Wichtige Punkte, die es zu beachten gilt

1. Wenn Sie ein Pooled-Lizenzkunde sind, der auf Flexed-Lizenzen umstellt, und Ihre MPX- und SDX-Hardware bereits über unbefristete Z-Cap-Lizenzen verfügt, müssen Sie die mit Flexed erhaltenen Z-Cap-Lizenzen nicht anwenden. Wenn jedoch die aktuellen Z-Cap-Lizenzen, die auf NetScaler MPX/NetScaler SDX angewendet werden, für einen bestimmten Zeitraum gültig sind, müssen Sie die mit der Flexed-Lizenz erhaltenen Z-Cap-Lizenzen anwenden. Die Flexed-Softwarelizenz umfasst die NetScaler Flexed MPX/SDX/VPX/VPX FIPS-Softwareinstanz und NetScaler Flexed Platinum-Bandbreitenlizenzen.
2. Sie müssen die Flexed-Lizenzen auf der NetScaler Console für den NetScaler-Formfaktor anwenden, den Sie in Ihrer Bereitstellung verwenden. Beispiel:

   Wenden Sie die folgenden Lizenzen an, wenn Sie den NetScaler SDX-Formfaktor verwenden:

Lizenzdatei	Anzuwenden auf
NetScaler Flexed SDX SW-Instanz	NetScaler-Konsole
NetScaler Flexed VPX SW-Instanz	NetScaler-Konsole
NetScaler Flexed Platinum BW	NetScaler-Konsole
ADC SDX-Z-Plattform mit Nullkapazität	NetScaler SDX

   Wenden Sie die folgenden Lizenzen an, wenn Sie den NetScaler MPX-Formfaktor verwenden:

Lizenzdatei	Anzuwenden auf
NetScaler Flexed MPX SW-Instanz	NetScaler-Konsole
NetScaler Flexed Platinum BW	NetScaler-Konsole
ADC MPX-Z-Plattform mit Nullkapazität	NetScaler MPX

Wenden Sie die folgenden Lizenzen an, wenn Sie den Formfaktor NetScaler VPX, NetScaler BLX oder NetScaler CPX verwenden:

Lizenzdatei	Anzuwenden auf
NetScaler Flexed VPX SW-Instanz	NetScaler-Konsole
NetScaler Flexed Platinum BW	NetScaler-Konsole

Wenden Sie die folgenden Lizenzen an, wenn Sie den NetScaler VPX FIPS-Formfaktor verwenden

Lizenzdatei	Anzuwenden auf
NetScaler Flexed VPX FIPS SW-Instanz	NetScaler-Konsole
NetScaler Flexed Platinum BW	NetScaler-Konsole

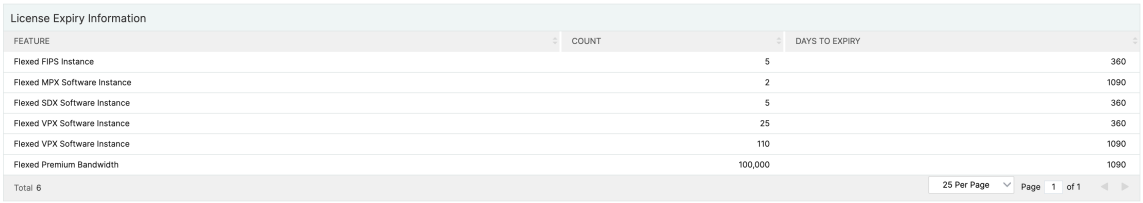
Eine Lizenzdatei anwenden

Sie können Lizenzen hinzufügen, löschen und herunterladen. Sie müssen Lizenzen beantragen, bevor sie verwendet werden können.

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:
   - **Lizenzdateien von einem lokalen Computer hochladen**: Wenn auf Ihrem lokalen Computer bereits eine Lizenzdatei vorhanden ist, können Sie sie in die NetScaler Console 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 zur NetScaler Console hinzugefügt.
   Im Abschnitt **Informationen zum Ablauf der Lizenz** sind die in NetScaler Console vorhandenen Lizenzen, die Anzahl und die verbleibenden Tage bis zum Ablauf aufgeführt.

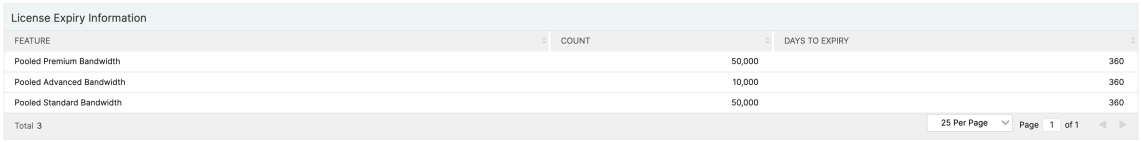
   Der folgende Screenshot zeigt die Anzahl der Flexed NetScaler VPX-, NetScaler MPX-, NetScaler SDX- und NetScaler VPX FIPS-Softwareinstanzlizenzen, die vorhandene Flexed-Premium-Bandbreitenkapazität und die Tage bis zum Ablauf.

   
   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.

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.

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 Console Benachrichtigungen per E-Mail, wenn eine Lizenz bald abläuft. Ein SNMP-Trap und eine Benachrichtigung werden auch gesendet, wenn die Lizenz auf der NetScaler Console abgelaufen ist.

Ein Ereignis wird generiert, wenn eine Benachrichtigung über den Ablauf der Lizenz gesendet wird. Dieses Ereignis kann in der NetScaler Console 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 virtuellen Server oder Instanzen, die betroffen sein werden.
    - **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 Lizenzzuweisung und die Tage bis zum Ablauf versendet werden.

1. Klicken Sie im Abschnitt **Benachrichtigungseinstellungen** auf das Symbol **Bearbeiten** und wählen Sie **Bei Lizenznutzung benachrichtigen** aus. Legen Sie den Alarmschwellenwert als Prozentsatz der flexiblen/gepoolten Lizenzkapazität fest, die für den Versand einer Benachrichtigung zugewiesen werden muss.
2. Wählen Sie die Art der Benachrichtigung aus, die Sie senden möchten, wenn Lizenzen den Schwellenwert erreichen oder bald ablaufen, indem Sie das entsprechende Kontrollkästchen aktivieren. Die Benachrichtigungstypen lauten wie folgt.

- **E-Mail**: E-Mail-Profil oder Verteilerliste für den Versand von Benachrichtigungen. Weitere Informationen finden Sie unter Erstellen einer E-Mail-Verteilerliste.
- **Slack**: Slack-Profildetails zum Senden von Benachrichtigungen.
- **PagerDuty**: PagerDuty-Profil zum Senden von Benachrichtigungen.
- **ServiceNow**: Das Citrix ServiceNow-Profil ist standardmäßig angegeben und ist derzeit die einzige verfügbare Option.
  Weitere Informationen zum Erstellen dieser Profile finden Sie unter Benachrichtigungen konfigurieren

Select a notification type and click **Add** to add details. You can also test each notification system before saving your settings.

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 die 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 die NetScaler Console die Nachricht sendet.
   - **An**—Geben Sie die E-Mail-Adressen an, an die die NetScaler Console die Nachricht sendet.
   - **Cc**—Geben Sie die E-Mail-Adressen an, an die die NetScaler Console die Nachricht kopiert.
   - **Bcc**—Geben Sie die E-Mail-Adressen an, an die die NetScaler Console die Nachricht blind kopiert (ohne die E-Mail-Adresse anzuzeigen).
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 die NetScaler Console 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 Ereignisbenachrichtigungen, 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, Push-Benachrichtigungen und Telefonanrufe unter einer registrierten Nummer konfigurieren. Bevor Sie ein PagerDuty-Profil in NetScaler Console 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 Ereignisregeln 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 die NetScaler-Ereignisse zu aktivieren, müssen Sie NetScaler Console mithilfe des ITSM-Connectors in ServiceNow integrieren. Weitere Informationen finden Sie unter Integrieren der NetScaler Console in die 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.

> **Hinweis:**
>
> Informationen zu den verschiedenen Typen von NetScaler-Lizenzen finden Sie unter Übersicht über die Lizenzierung.

Mindest- und Höchstkapazität für flexible und gepoolte Lizenzen

April 10, 2024

Die NetScaler Flexed-Lizenzierung verwendet NetScaler Console, die als Lizenzserver konfiguriert ist, um Flexed-Lizenzen zu verwalten: Bandbreitenpool-Lizenzen und Instanzpool-Lizenzen.

Beim Auschecken von Lizenzen aus Bandbreite und Instanzpool bestimmen der NetScaler-Formfaktor und die Hardware-Modellnummer auf einer Hardware ohne Kapazität Folgendes:

- 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 Mindestbandbreiteneinheit für jeden jedes Auschecken einer Bandbreite. 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 Mindestbandbreite erreicht ist, kann die Instanz mehr Bandbreite in Vielfachen der Mindestbandbreiteneinheit auschecken.

In den Tabellen 1 bis 5 sind die maximale Bandbreite bzw. die Instanzen, die minimale Bandbreite bzw. Instanzen und die minimale Bandbreiteneinheit für alle unterstützten NetScaler-Instanzen zusammengefasst. Tabelle 6 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 1. 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 2A. 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 2B. 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 2C. 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 3. 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 4. 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 5. 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 6. Lizenzanforderungen ohne Kapazität für verschiedene Formfaktoren

Produkt-Linie	Hardware ohne Kapazität
MPX	Lizenz erforderlich
SDX	Lizenz erforderlich
VPX	-
CPX	-

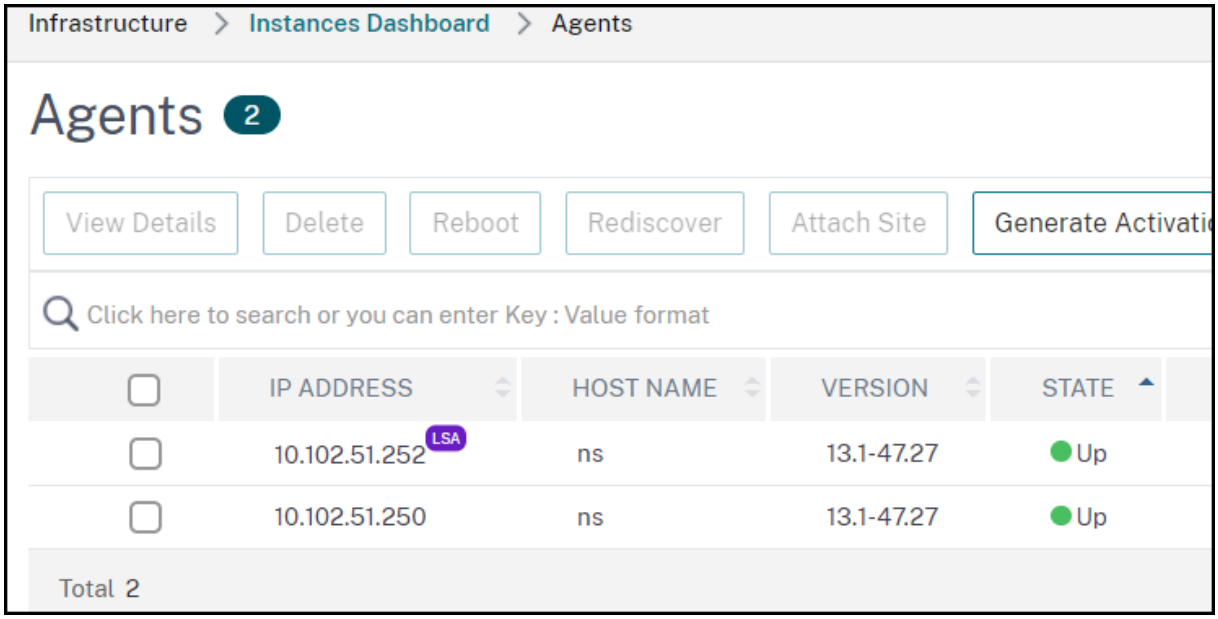
Produkt-Linie	Hardware ohne Kapazität
BLX	-

Verhalten des NetScaler Agents für flexible oder gepoolte Lizenzierung

April 10, 2024

Der NetScaler Agent fungiert als Vermittler zwischen NetScaler Console und den erkannten Instanzen in verschiedenen Rechenzentren und öffentlichen Clouds. Für den NetScaler Console-Dienst ist mindestens ein Agent pro Mandant erforderlich, damit die flexible oder gepoolte Lizenzierung funktioniert. Pro Site oder an mehreren Sites können mehrere NetScaler Agents bereitgestellt werden, aber nur ein Agent kann die Rolle License Server Agent (LSA) für die gesamte Mandantenbereitstellung übernehmen.

Das folgende Beispiel zeigt zwei bereitgestellte Agents, von denen einer die LSA-Rolle hat:



Ein LSA ist ein Agent, der als Lizenzserver in einer auf dem NetScaler Console Service basierenden Bereitstellung gepoolter Lizenzen fungiert. Wenn der LSA ausfällt, wartet der Dienst 24 Stunden, um einen neuen LSA auszuwählen.

Bis dahin gilt für die NetScaler-Instanzen, die eine gepoolte oder flexible Lizenz verwenden, eine Kulanzfrist. Als Administrator können Sie einen LSA auch manuell auswählen.

NetScaler Console-Agent manuell als LSA auswählen

Administratoren können manuell einen NetScaler Console-Agent als LSA für die NetScaler Pooled- oder NetScaler Flexed-Lizenzierung auswählen. Wenn der LSA ausgefallen ist, wartet der NetScaler Console-Dienst 24 Stunden, bevor er automatisch den nächsten LSA auswählt. Der Administrator kann den neuen LSA in der Zwischenzeit mit diesem Feature manuell auswählen. Der Administrator muss jedoch sicherstellen, dass der Status des ausgewählten neuen LSA AKTIV und sein Diagnosestatus OK ist.

Wenn der Administrator manuell einen neuen LSA auswählt, kann es bis zu 5 Minuten dauern, bis die Lizenzierungsfunktion ordnungsgemäß funktioniert. Während dieser Zeit sind die NetScaler-Instanzen in Betrieb und jedes erneute Auschecken einer Lizenz schlägt fehl.

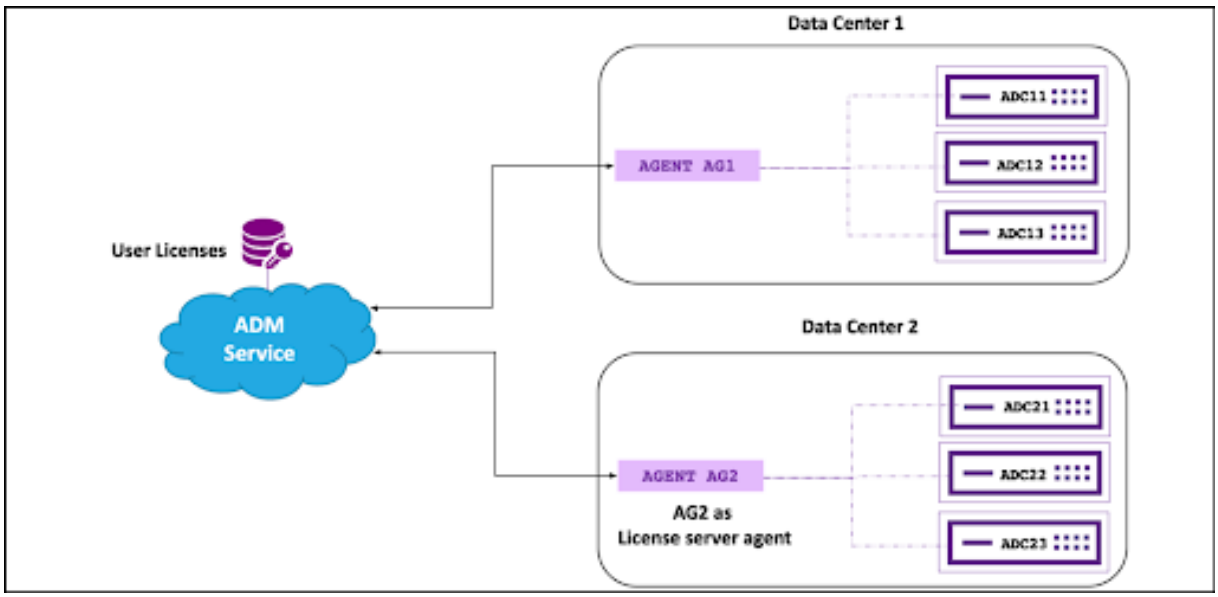
So wählen Sie einen LSA aus:

1. Navigieren Sie zu **Infrastruktur > Instanzen-Dashboard > Agents** und wählen Sie einen Agent aus.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Als LSA festlegen** aus.
3. Klicken Sie zur Bestätigung auf **Ja**. Der ausgewählte Agent übernimmt die LSA-Rolle.

Verhalten mehrerer NetScaler Agents

In einer Bereitstellung mit einer Kombination aus mehreren Agents und mehreren Standorten folgen die NetScaler Agents der Client/Server-Architektur.

Dem ersten/ältesten Agent, der in einem UP-Status registriert ist, wird die LSA-Rolle zugewiesen. Alle anderen Agent, die später hinzugefügt werden, agieren als Proxy und kommunizieren mit dem Agent, der die LSA-Hauptrolle für die Lizenzzuweisung hostet. Jeder Agent, der die Proxyrolle hostet, kommuniziert über den NetScaler Console-Dienst mit dem Agent, der die aktuelle LSA-Rolle hat.



> **Hinweis**
>
> Es gibt keine direkte Kommunikation zwischen dem Agent, der die LSA-Rolle innehat, und den anderen Agents (Nicht-LSA). Alle Verbindungen laufen nur über den NetScaler Console-Dienst.

Failover-Verhalten des NetScaler Agents

Das AgentfFailover funktioniert in einer Multi-Agent-Bereitstellung auf folgende Weise.

Gehen Sie davon aus, dass sich zwei Agents, AG1 und AG2, im selben Rechenzentrum befinden.

- AG1 ist so konfiguriert, dass ADC11, ADC12, ADC13 als Remote-Lizenzhost oder LSA verwendet werden.
- AG2 ist so konfiguriert, dass ADC21, ADC22, ADC23 als Remote-Lizenzhost oder LSA verwendet werden.
- AG2 fungiert als Lizenzserver.
  - Wenn AG1 fehlschlägt, verbinden sich ADC11, ADC12 und ADC13 automatisch über AG2 für den Lizenzabgleich.
    - ADC11, ADC12 und ADC13 bemerken möglicherweise immer noch eine kurze Nachfrist, wenn einige Herzschläge verpasst werden, während die Verbindung wiederhergestellt wird.
  - Wenn AG2 ausfällt, bleiben alle ADCs so lange in Ordnung, bis:
    - Entweder kommt AG2 wieder zurück oder wird wieder hochgefahren, oder AG1 wird entweder automatisch nach 24 Stunden vom NetScaler Console-Dienst oder manuell vom Administrator als neuer LSA ausgewählt.

* Oder AG2 wird aus dem NetScaler Console-Dienst gelöscht. Nach der Abmeldung bestimmt der NetScaler Console-Dienst den AG1 als Agent mit der LSA-Rolle.
* Nachdem die Auswahl abgeschlossen ist, beginnt AG1 mit der Zuweisung und Abstimmung von Ressourcen zu den konfigurierten Instanzen.

Bei Fragen zu LSA lesen Sie die FAQs zum License Server Agent.

Flexible Lizenz

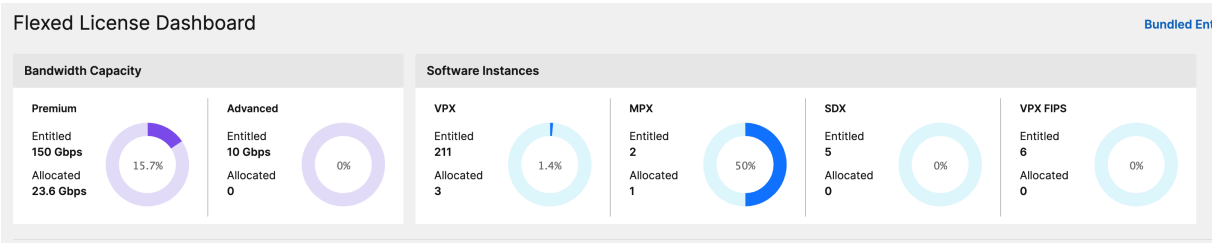
April 10, 2024

NetScaler Flexed 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 on-premises bereitgestellt werden.

Eine Flexed-Lizenz bietet auch Analysen für eine unbegrenzte Anzahl virtueller Server.

Wenn Sie zuvor gepoolte Lizenzen hatten und 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.

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 den Tabellen 1 und 2 unter Mindest- und Höchstkapazität für flexible und gepoolte Lizenzen.

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 auf den folgenden Hypervisors und Cloudplattformen ausgeführt wird, unterstützen die Flexed-Lizenzierung:

- 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 Hypervisors und Cloud-Plattformen ausgeführt werden, unterstützen die Flexed-Lizenzierung:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

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.

Flexed-Lizenzierung konfigurieren

January 26, 2024

> **Hinweis:**
>
> Wenn Sie gepoolte Lizenzen haben und jetzt Flexed-Lizenzen gekauft und angewendet haben, wird die kombinierte Berechtigung jetzt 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.

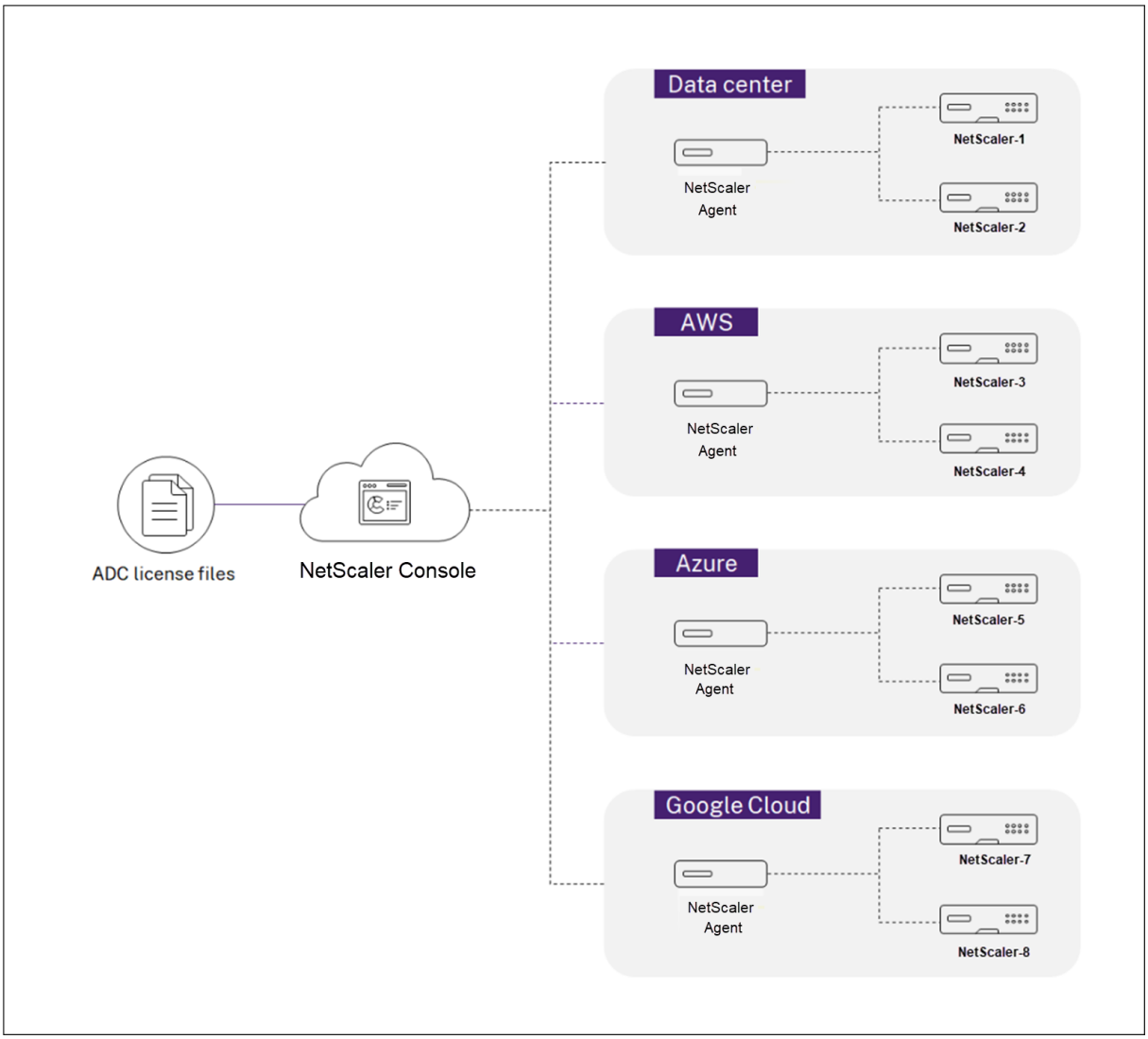
Sie können die Flexed-Lizenzierung verwenden, um die Bandbreitennutzung zu maximieren, indem Sie sicherstellen, dass einer Instance die erforderliche Bandbreite zugewiesen wird und nicht mehr,

als sie benötigt wird. Erhöhen oder verringern Sie die Bandbreite, die einer Instanz zur Laufzeit zugewiesen ist, ohne den Datenverkehr zu beeinträchtigen.

Um die NetScaler Flexed-Lizenzierung zu verwenden, müssen Sie einen NetScaler Console-Agent an eine NetScaler-Instanz anhängen. NetScaler-Instanzen checken Lizenzen von der NetScaler Console über einen Agenten ein und aus.

Sie können die folgenden Aufgaben in NetScaler Console ausführen:

1. Laden Sie die Flexed-Lizenzdateien (Bandbreitenpool oder Software-Instanzpool) auf den Lizenzserver hoch.
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 Console zur Instanz funktioniert nicht.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie die Flexed-Lizenzierung konfigurieren:

- Installieren und registrieren Sie einen Agenten in NetScaler Console. Informationen zum Installieren und Registrieren eines Agents finden Sie unter Erste Schritte.
- Stellen Sie sicher, dass sich alle registrierten Agenten im Status UP befinden, damit die Flexed-Lizenzierung ordnungsgemäß funktioniert. Wenn sich Agents im DOWN-Zustand befinden, aber noch nicht außer Dienst gestellt oder gekündigt wurden, bringen Sie sie in den UP-Status. Wenn DOWN-Agents außer Betrieb genommen oder beendet werden oder nicht mehr verwendet werden, löschen Sie sie aus der NetScaler Console.
- Die `27000`und `7279`-Ports sind verfügbar, um Lizenzen von NetScaler Console an eine Instance auszuchecken. Weitere Informationen finden Sie unter Systemanforderungen.

Schritt 1 —Lizenzen in NetScaler Console anwenden

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 auf NetScaler Console 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 Console jederzeit über die Lizenzeinstellungen weitere Lizenzen**
>
> hinzufügen.

3. Klicken Sie auf **Fertig stellen**.

   Die Lizenzdateien werden zur NetScaler Console hinzugefügt. Im Abschnitt **Informationen zum Ablauf der Lizenz** sind die in der NetScaler Console 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 Console als Lizenzserver registrieren und Lizenzen zuweisen

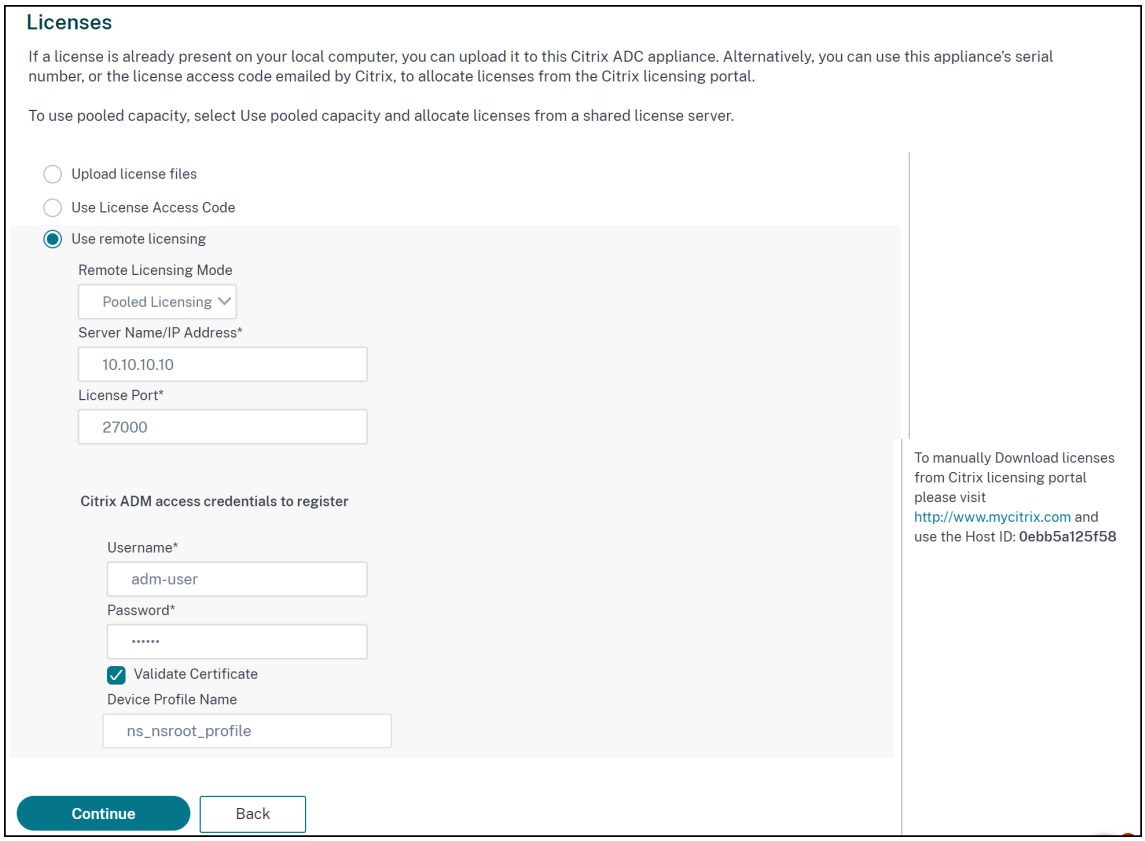
Sie können die NetScaler Console mithilfe eines Agenten als Lizenzserver für eine NetScaler-Instanz registrieren.

Registrieren Sie einen NetScaler Console-Agenten mithilfe der GUI

Registrieren Sie in der NetScaler Console-GUI den NetScaler Console-Agenten, der einer NetScaler-Instanz zugeordnet ist.

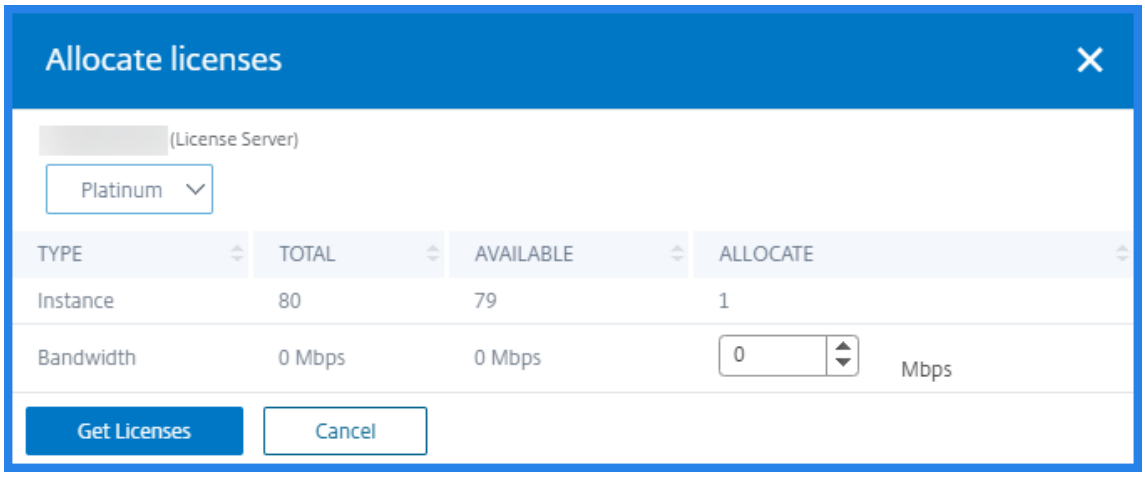
1. Melden Sie sich bei NetScaler GUI an.
2. Navigieren Sie zu **System > Lizenzen > Lizenzen verwalten** .
3. Klicken Sie auf **Neue Lizenz hinzufügen**.
4. Wählen Sie **Remote-Lizenzierung verwenden** und wählen Sie den Remote-Lizenzierungsmodus aus der Liste aus.
5. Geben Sie im Feld **Servername/IP-Adresse** die IP-Adresse des zugehörigen NetScaler Console-Agents an, die bei der NetScaler Console registriert ist.
6. Wählen Sie **Bei NetScaler Console registrieren** aus.

7. Geben Sie Ihre NetScaler Console-Agent-Anmeldeinformationen ein, um eine Instanz bei NetScaler Console zu registrieren, und klicken Sie auf **Weiter**. In NetScaler Console ist einer der Agents 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 über die NetScaler Console-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 Console-Agenten hinzu

Wenn eine NetScaler-Instanz keine GUI hat, verwenden Sie die folgenden CLI-Befehle, um einen NetScaler Console-Agenten hinzuzufügen, der einer Instanz zugeordnet ist:

1. Melden Sie sich bei der NetScaler Konsole an.
2. Fügen Sie die IP-Adresse des zugehörigen NetScaler Console-Agents hinzu, die bei der NetScaler Console registriert ist:

```
> add ns licenseserver <adm-agent-IP-address> -port <adm-agent-license-port-number>
```

3. Zeigen Sie die im Lizenzserver verfügbare Lizenzbandbreite an:

```
> sh ns licenseserverpool
```

4. Weisen Sie die Lizenzbandbreite aus der erforderlichen Lizenzedition zu:

```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth > edition <specify-license-edition>
```

> **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 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 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 Instanzlizenzen werden für den Lizenzserver freigegeben.

Sie können die Bandbreite einer SDX-Z-Instanz ohne Neustart dynamisch 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 Hochverfügbarkeitspaar

Bevor Sie beginnen, stellen Sie sicher, dass der NetScaler Console-Server als Lizenzserver konfiguriert ist. Weitere Informationen finden Sie unter NetScaler Console als Lizenzserver konfigurieren

Wenn Sie die Bandbreite einem NetScaler HA-Paar zuweisen, checkt die NetScaler Console 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.

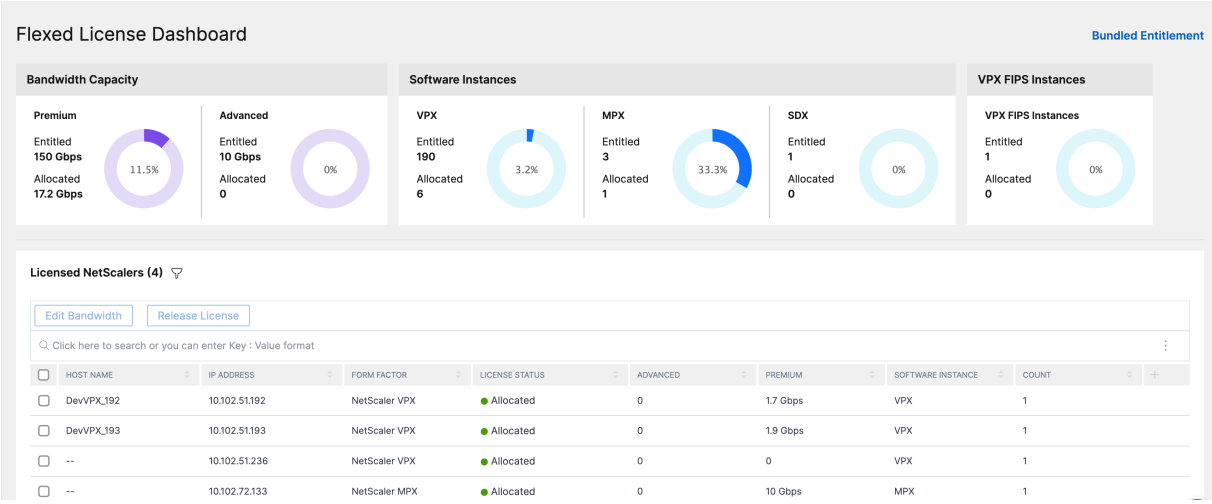
Flexibles Lizenz-Dashboard

April 10, 2024

> **Hinweis:**
>
> Wenn Sie zuvor gepoolte Lizenzen hatten und jetzt Flexed-Lizenzen gekauft und angewendet haben, wird die kombinierte Berechtigung jetzt im Flexed-Lizenz-Dashboard angezeigt.

Das Flexed-Lizenz-Dashboard bietet Ihnen einen umfassenden Überblick über die Bandbreitenkapazität und die von Ihnen gekauften Instanzen.

Bandbreitenkapazität für alle Editionen und Instanzdetails für verschiedene Formfaktoren wie MPX, VPX und SDX werden auf dieser Seite angezeigt. MPX und MPX FIPS haben dieselbe Lizenzdatei. In ähnlicher Weise haben SDX und SDX FIPS dieselbe Lizenzdatei. VPX FIPS hat jedoch eine andere Datei als VPX und wird separat angezeigt. Außerdem benötigen VPX (einschließlich VPX auf SDX), BLX und CPX 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 Standardbandbreitenkapazität oder erweiterte Bandbreitenkapazität gepoolt hatten, werden die Details zur Bandbreitenkapazität (Standard oder Advanced) auch im Flexed-Lizenz-Dashboard aufgeführt.



Für die Formfaktoren VPX (einschließlich VPX auf SDX), BLX und CPX ist eine NetScaler Flexed VPX SW-Instanz-Lizenzdatei erforderlich. Das heißt, diese Formfaktoren sind Teil des Anspruchs und der Zuweisung für Flexed VPX-SW-Instanz-Lizenzen.

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 > Flexed 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

June 7, 2024

In diesem Dashboard können Sie Details zu folgenden Themen einsehen:

- Berechtigung und Zuweisung von Softwareinstanzen (VPX, MPX und SDX sowie VPX FIPs)
- Anspruch, Zuweisung und tatsächliche Nutzung von Bandbreite/Durchsatzkapazität
- Spitzen- und Durchschnittszuweisung für alle verwalteten oder ausgewählten Instanzen
- Spitzen- und Durchschnittsnutzung aller verwalteten oder ausgewählten Instanzen

Funktionen (für NetScaler-Instanzen)	Beschreibung
Anspruch	Die Gesamtzahl der Instanzberechtigungen für Softwareinstanztypen (VPX, SDX, MPX).
Zuteilung	Die gesamte Instanzzuweisung für Software-Instanztypen (VPX, SDX, MPX).

Funktionen (für Bandbreite/Durchsatzkapazität)	Beschreibung
Anspruch	Die gesamten Bandbreiten-/Durchsatzkapazitätsberechtigungen für alle verwalteten NetScaler-Instanzen. Die Gesamtberechtigungen werden anhand der in der Lizenzverwaltung verwendeten Lizenzen berechnet (**NetScaler Licensing > License Management**).
Zuteilung	Die Bandbreite/Durchsatzkapazität, die **lizenzierten NetScalern** im Flected License Dashboard zugewiesen wird (**NetScaler Licensing > Flected Licensing > Flected License Dashboard**).
Verwendung	Der Gesamtdurchsatz, der von den NetScaler-Instanzen verbraucht wird.

> **Hinweis:**
>
> Eine Flexed-Lizenz unterstützt nur die Premium Edition. Wenn Sie jedoch flexible Lizenzen gekauft und angewendet haben und zuvor die Kapazität für Standardbandbreite oder erweiterte Bandbreite gepoolt hatten, werden auch die Details zur Bandbreite/Durchsatzkapazität (Standard oder Advanced) aufgeführt. Wenn Sie beispielsweise eine 1000-Gbit/s-Flexed-Lizenz (Premium-Lizenz) beantragt haben und auch über eine aktive Pool-Lizenz mit 100 Gbit/s Advanced Bandwidth verfügen, werden im Berichts-Dashboard sowohl Premium 1000 Gbps als auch 100 Advanced Bandwidth angezeigt.

Das folgende Beispiel hilft Ihnen zu verstehen, wie das Dashboard die Spitzenauslastung und die durchschnittliche Nutzung anzeigt:

Beachten Sie, dass es 3 verwaltete NetScaler-Instanzen (NetScaler A, NetScaler B und NetScaler C) mit Flexed-Lizenz (Premium-Bandbreite) gibt und die gewählte Dauer 1 Tag beträgt. Bei Berechnungen berücksichtigt NetScaler Console Datenpunkte (in Mbit/s) für jede Stunde pro NetScaler-Instanz. Für einen Tag gibt es 24 Datenpunkte für jede NetScaler-Instanz. Für 3 NetScaler-Instanzen gibt es also (24* 3) Datenpunkte.

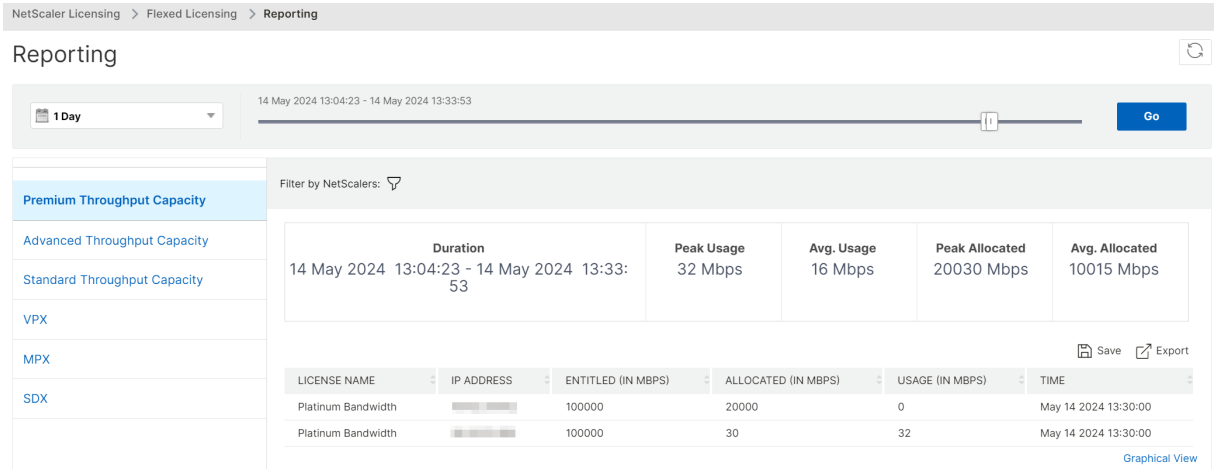
- **Spitzenauslastung** = Die Summe der höchsten Datenpunkte (Mbit/s) aus den 24 Stunden aller NetScaler-Instanzen. Wenn beispielsweise der höchste Datenpunkt aus der 24-Stunden-Dauer für NetScaler A 30 Mbit/s, NetScaler B 45 Mbit/s und NetScaler C 120 Mbit/s beträgt, wird die Spitzenauslastung mit 195 Mbit/s (30 + 45 + 120) angezeigt.

- **Durchschnittliche Nutzung** = Die Summe aller 24-Stunden-Datenpunkte geteilt durch 24 für jede NetScaler-Instanz. Für 3 NetScaler-Instanzen wird also der Gesamtdurchschnitt aller 3 NetScaler-Instanzen geteilt durch 3. Wenn beispielsweise der NetScaler A-Durchschnitt 25 Mbit/s, der NetScaler B-Durchschnitt 20 Mbit/s und der NetScaler C-Durchschnitt 45 Mbit/s beträgt, wird die durchschnittliche Nutzung als 30 Mbit/s angezeigt (25 + 20 + 35 geteilt durch 3).

In ähnlicher Weise werden die Spitzen- und Durchschnittszuordnungsdetails mit derselben Logik angezeigt.

Sie können die Dauer aus der Liste auswählen, angefangen von einer Stunde bis zu einem Jahr, und die Details sowohl in der tabellarischen als auch in der grafischen Ansicht anzeigen.

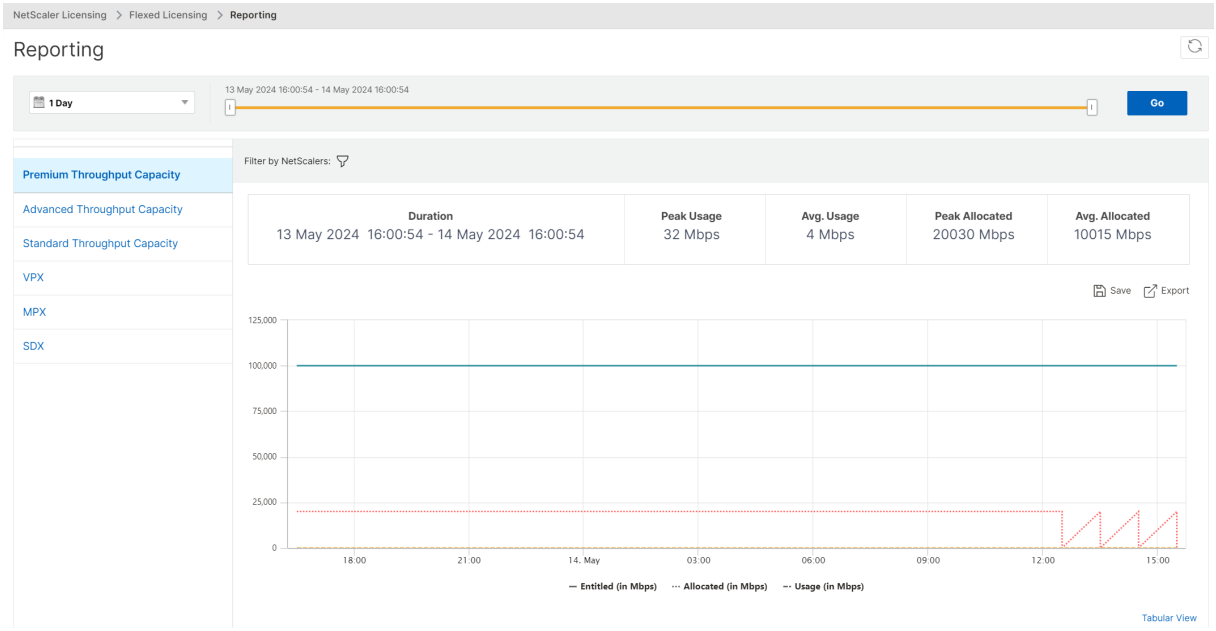
Das folgende Beispiel zeigt die tabellarische Ansicht für die Instanzen, die die Flexed-Lizenz verwenden (Premium-Bandbreite):



Die folgenden Details werden auf dem Dashboard angezeigt:

- **Spitzenauslastung** —Die höchste Auslastung (in Mbit/s) für die gewählte Dauer.
- **Durchschnittliche Nutzung** —Die durchschnittliche Nutzung (in Mbit/s) für die gewählte Dauer.
- **Zugewiesener Höchstwert** —Die höchste Zuteilung für die gewählte Dauer.
- **Durchschnittliche Zuweisung** —Die durchschnittliche Zuweisung für die ausgewählte Dauer.
- **Filter** —Sie können eine oder mehrere Instances auswählen, um die Nutzungs- und Zuordnungsdetails für die jeweiligen Instanzen anzuzeigen.
- **Exportieren** —Sie können Details im PDF-, JPEG- und PNG-Format exportieren.

Das folgende Beispiel zeigt die grafische Ansicht für die Instanzen, die die Flexed-Lizenz verwenden (Premium-Bandbreite):



Umstellung auf Flexed-Lizenzierung

April 10, 2024

> **Hinweis:**
>
> Sie müssen vor Ablauf Ihrer aktuellen Lizenz zur Flexed-Lizenzierung wechseln. Beachten Sie bei der Planung der Umstellung die folgenden Schritte und planen Sie ein Wartungsfenster ein, falls die Schritte eine Neukonfiguration der Lizenz oder einen NetScaler-Neustart beinhalten.

Von der gepoolten Bandbreitenlizenz zur Flexed-Lizenzierung

Einige Schritte sind bei MPX, SDX und VPX üblich. Diese Schritte werden zuerst aufgeführt, gefolgt von den für MPX, SDX oder VPX spezifischen Schritten.

Allgemeine Schritte für VPX/MPX/SDX

1. Laden Sie Flexed-Lizenzen auf NetScaler Console hoch und wenden Sie sie an. Siehe Lizenzdateien.
2. Wenn Sie eine Z-Cap-Softwarelizenz haben, die für einen bestimmten Zeitraum gültig ist, wenden Sie diese Lizenz auf NetScaler-Hardware (MPX/SDX) an.

Für VPX/MPX

Die folgenden zusätzlichen Schritte sind erforderlich:

1. Wenn Sie eine gepoolte Premium-Bandbreitenlizenz (Platinum) haben, wechselt die Lizenz nach Ablauf der alten Lizenz automatisch zu Flexed.
2. Wenn Sie eine gepoolte Standard- oder Advanced-Bandbreitenlizenz haben, checken Sie die Premium-Bandbreite manuell aus und starten Sie NetScaler im Warmmodus neu.

Für SDX

> **Hinweis:**
>
> Achten Sie darauf, dass Sie vor Ablauf Ihrer aktuellen Lizenz zur Flexed-Lizenzierung wechseln.

Die folgenden zusätzlichen Schritte sind erforderlich:

1. Schauen Sie sich die erforderliche Instanz- und Bandbreitenlizenz von Flexed-Lizenzierung zu SDX an. Ein SDX-Neustart ist nicht erforderlich.
2. Wenn alle VPX auf SDX über eine Premium-Edition verfügen, wechselt die Lizenz nach Ablauf der alten Lizenz automatisch zu Flexo.
3. Ändern Sie die Edition für alle VPX (auf SDX) mit Standard oder Advanced auf Premium. Diese VPX-Instanzen werden automatisch neu gestartet.
4. Reduzieren Sie die Standard- und Advanced-Bandbreitenkapazität auf SDX auf Null.

Gepoolte vCPU zur Flexed-Lizenzierung

Für VPX

1. Laden Sie Flexed-Lizenzen auf NetScaler Console hoch und wenden Sie sie an. Siehe Lizenzdateien.
2. Entfernen Sie den vorhandenen Lizenzserver mithilfe der NetScaler-GUI. NetScaler ist nicht lizenziert, bis alle Schritte abgeschlossen sind.
3. Fügen Sie den Lizenzserver mit der Option Flexed/Pooled hinzu.
4. Informieren Sie sich über die erforderlichen Instanz- und Bandbreitenlizenzen für NetScaler.
5. Starten Sie NetScaler im Warmmodus neu.

Festes Abonnement oder unbefristete Lizenz für Flexed-Lizenzen

Einige Schritte sind bei MPX, SDX und VPX üblich. Diese Schritte werden zuerst aufgeführt, gefolgt von den für MPX, SDX oder VPX spezifischen Schritten.

Allgemeine Schritte für VPX/MPX/SDX

1. Onboarding in der NetScaler Console.
2. Stellen Sie den NetScaler Agent bereit.
3. Laden Sie Flexed-Lizenzen auf NetScaler Console hoch und wenden Sie sie an. Siehe Lizenzdateien.
4. Wenden Sie die Z-Cap-Softwarelizenz auf NetScaler-Hardware (MPX/SDX) an.

Für VPX/MPX

Die folgenden zusätzlichen Schritte sind erforderlich:

1. Informieren Sie sich über die erforderlichen Instanz- und Bandbreitenlizenzen für NetScaler.
2. Starten Sie NetScaler im Warmmodus neu.
3. Löschen Sie die feste Abonnementlizenz nach dem Neustart von NetScaler.

Für SDX

Die folgenden zusätzlichen Schritte sind erforderlich:

1. Sehen Sie sich die erforderliche Instanz- und Bandbreitenlizenz unter Flexed-Lizenzierung auf SDX an.
2. Wenn alle VPX auf SDX über die Premium Edition verfügen, ist kein SDX-Neustart erforderlich.
3. Wenn ein VPX die Advanced- oder Standard-Edition hat, muss dieses VPX auf die Premium-Edition umgestellt werden. VPX wird automatisch neu gestartet.
4. Wenden Sie die Z-Cap-Softwarelizenz auf NetScaler SDX an.
5. Sehen Sie sich die erforderliche Instanz- und Bandbreitenlizenz unter Flexed-Lizenzierung auf SDX an.
6. Löschen Sie die feste Abonnementlizenz nach dem Neustart von NetScaler.

Von fester vCPU zur Flexed-Lizenzierung

Für VPX

1. Onboarding in der NetScaler Console.
2. Stellen Sie den NetScaler Agent bereit.
3. Laden Sie Flexed-Lizenzen auf NetScaler Console hoch und wenden Sie sie an. Siehe Lizenzdateien.
4. Konfigurieren Sie den Lizenzserver auf NetScaler im Flexed/Pooled-Modus.
5. Informieren Sie sich über die erforderlichen Instanz- und Bandbreitenlizenzen für NetScaler.

6. Starten Sie NetScaler im Warmmodus neu.
7. Löschen Sie die feste Lizenz nach dem Neustart von NetScaler.

Lizenzierung von CICO zu Flexed

Für VPX

1. Laden Sie Flexed-Lizenzen auf NetScaler Console hoch und wenden Sie sie an. Siehe Lizenzdateien.
2. Entfernen Sie den vorhandenen Lizenzserver mithilfe der NetScaler-GUI. NetScaler ist nicht lizenziert, bis alle Schritte abgeschlossen sind.
3. Fügen Sie den Lizenzserver mit der Option Flexed/Pooled hinzu.
4. Informieren Sie sich über die erforderlichen Instanz- und Bandbreitenlizenzen für NetScaler.
5. Starten Sie NetScaler im Warmmodus neu.

Selbstverwaltete Bandbreitenlizenz zur Flexed-Lizenzierung

Einige Schritte sind bei MPX, SDX und VPX üblich. Diese Schritte werden zuerst aufgeführt, gefolgt von den für MPX, SDX oder VPX spezifischen Schritten.

Allgemeine Schritte für VPX/MPX/SDX

1. Laden Sie Flexed-Lizenzen auf NetScaler Console hoch und wenden Sie sie an. Siehe Lizenzdateien.
2. Wenn Sie eine Z-Cap-Softwarelizenz haben, die für einen bestimmten Zeitraum gültig ist, wenden Sie diese Lizenz auf NetScaler-Hardware (MPX/SDX) an.

Für VPX/MPX

1. Wenn Sie eine selbstverwaltete Premium-Lizenz haben, ändern Sie den Lizenzmodus über die NetScaler-GUI von selbstverwaltete gepoolte Lizenz in Flexed/Pooled.
2. Ein NetScaler-Neustart ist nicht erforderlich.
3. Wenn Sie eine selbstverwaltete Standard- oder Advanced-Lizenz haben, entfernen Sie den vorhandenen Lizenzserver über die NetScaler-GUI.
4. Fügen Sie den Lizenzserver mit der Option Flexed/Pooled hinzu.
5. Schauen Sie sich die Flexed-Premium-Bandbreitenkapazität für VPX/MPX an.
6. Starten Sie NetScaler im Warmmodus neu.

Für SDX

1. Wenn alle VPX auf SDX über eine selbstverwaltete Premium-Lizenz verfügen, ändern Sie den Lizenzmodus über die NetScaler-GUI von selbstverwalteter gepoolter Lizenz auf Flexed/Pooled.
2. Ein NetScaler-Neustart ist nicht erforderlich.
3. Wenn einige VPX auf SDX über eine selbstverwaltete Standard- oder Advanced-Lizenz verfügen, wenden Sie sich an den Citrix Support.

Selbstverwaltete vCPU-Flexed-Lizenzierung

Für VPX

1. Laden Sie Flexed-Lizenzen auf NetScaler Console hoch und wenden Sie sie an. Siehe Lizenzdateien.
2. Entfernen Sie den vorhandenen Lizenzserver mithilfe der NetScaler-GUI. NetScaler ist nicht lizenziert, bis alle Schritte abgeschlossen sind.
3. Fügen Sie den Lizenzserver mit der Option Flexed/Pooled hinzu.
4. Informieren Sie sich über die erforderlichen Instanz- und Bandbreitenlizenzen für NetScaler.
5. Starten Sie NetScaler im Warmmodus neu.

Gepoolte Kapazität

January 26, 2024

Die gepoolte Kapazität in NetScaler ist ein Lizenzierungsframework, das einen gemeinsamen Bandbreiten- und Instanzpool umfasst, der auf der NetScaler Console gehostet und von dieser bereitgestellt wird. Aus diesem gemeinsamen Pool wird jede NetScaler-Instanz in Ihrem Rechenzentrum unabhängig von der Plattform oder dem Formfaktor eine Instanzlizenz und nur die erforderliche Bandbreite ausgecheckt. Die Lizenzdatei und die Bandbreite sind nicht an die Instanz gebunden. Wenn die Instanz diese Ressourcen nicht mehr benötigt, werden sie wieder in den gemeinsamen Pool eingecheckt und die Ressourcen anderen Instanzen zur Verfügung gestellt, die sie benötigen.

> **Hinweis**
>
> In NetScaler Console ist einer der Agents der Lizenzserver.

Dieses Lizenzierungsframework maximiert die Bandbreitenauslastung, indem sichergestellt wird, dass Instanzen nicht mehr Bandbreite zugewiesen wird als ihre Anforderung. Die Fähigkeit der NetScaler-Instanzen, Lizenzen und Bandbreite in einen gemeinsamen Pool ein- und auszuchecken, ermöglicht es Ihnen auch, die Instanzbereitstellung zu automatisieren.

Sie können die einer Instanz zugewiesene Bandbreite zur Laufzeit erhöhen oder verringern, ohne den Datenverkehr zu beeinträchtigen. Sie können die Lizenzen im Pool auch von einer Instanz auf eine andere übertragen.

Gebündelte Kapazität konfigurieren

January 26, 2024

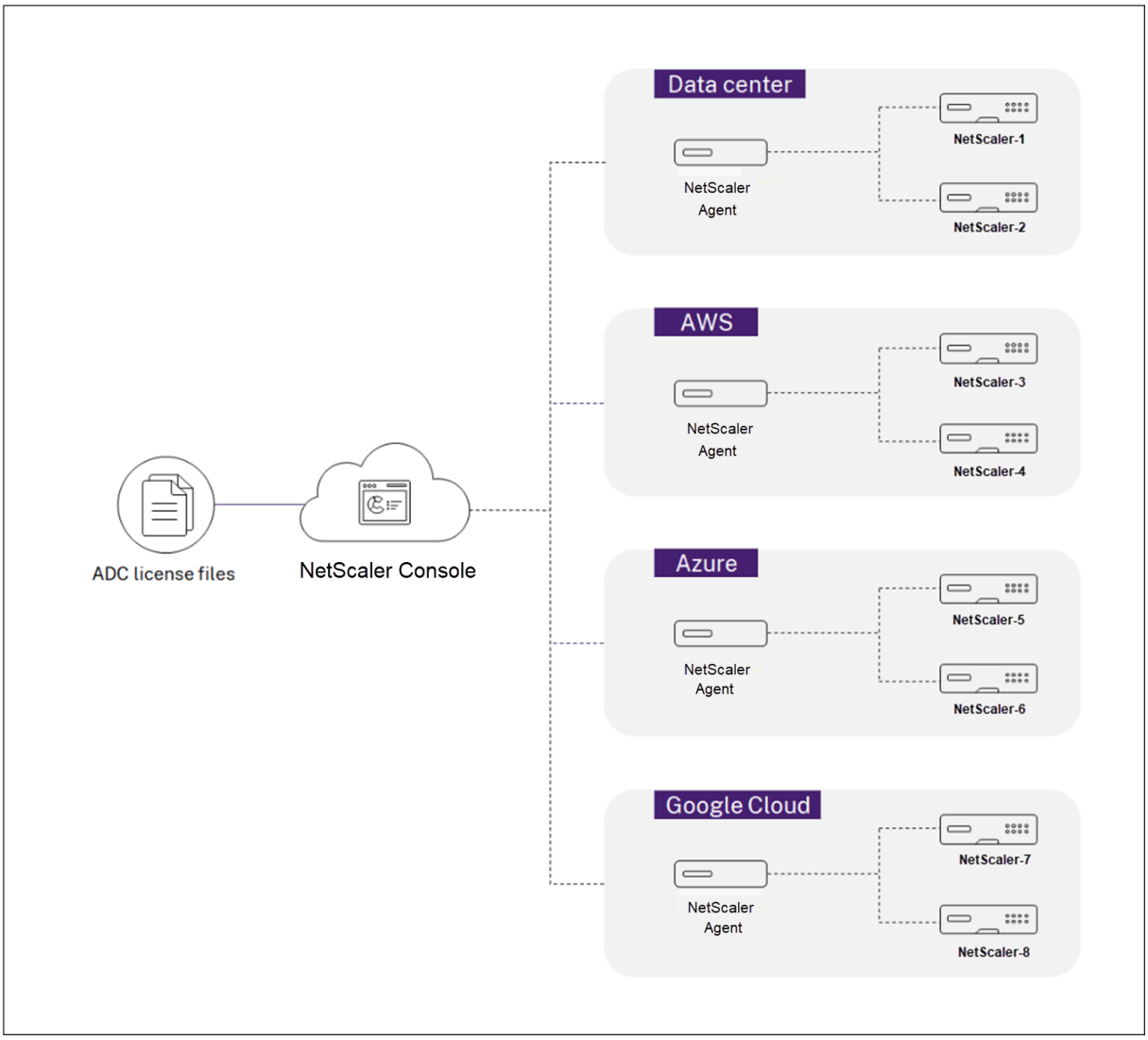
Die NetScaler Pooled-Kapazität ermöglicht es Ihnen, Bandbreiten- oder Instanzlizenzen für verschiedene NetScaler-Formfaktoren gemeinsam zu nutzen. Für Instanzen, die auf virtuellen CPU-Abos basieren, können Sie die virtuelle CPU-Lizenz für Verwenden Sie diese gepoolte Kapazität für die Instanzen, die 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.

Um NetScaler Pooled Capacity nutzen zu können, müssen Sie einen NetScaler Console-Agent an eine NetScaler-Instanz anhängen. NetScaler-Instanzen checken Lizenzen von der NetScaler Console über einen Agenten ein und aus.

Sie können auch gepoolte Kapazitätslizenzen für NetScaler FIPS-Instanzen verwenden. Sie können die folgenden Aufgaben in NetScaler Console ausführen:

1. Laden Sie die Lizenzdateien für gepoolte Kapazitäten (Bandbreitenpool oder Instanzpool) auf den Lizenzserver hoch.
2. 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.



Sie können gepoolte Lizenzen, einschließlich Bandbreite, Instanz und Z-Cap-Lizenzen, von citrix.com herunterladen. Weitere Informationen finden Sie im Lizenzierungsleitfaden für NetScaler.

Kapazitätsprobleme mit NetScaler Pooled

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 für die Verwaltung bei NetScaler Console registriert, oder die NITRO-Kommunikation von der NetScaler Console zu den Instanzen funktioniert nicht.
- **Nicht zugewiesen**: Die Lizenz wird in der Instanz nicht zugewiesen.

Voraussetzungen

Stellen Sie Folgendes sicher, bevor Sie die gepoolte Kapazität konfigurieren:

- Installieren und registrieren Sie einen Agenten in NetScaler Console. Informationen zum Installieren und Registrieren eines Agents finden Sie unter Erste Schritte.
- Stellen Sie sicher, dass sich alle registrierten Agenten im Status UP befinden, damit die Pool-Lizenzierung ordnungsgemäß funktioniert. Wenn sich Agents im DOWN-Zustand befinden, aber noch nicht außer Dienst gestellt oder gekündigt wurden, bringen Sie sie in den UP-Status. Wenn DOWN-Agents außer Betrieb genommen oder beendet werden oder nicht mehr verwendet werden, löschen Sie sie aus der NetScaler Console.
- Die `27000`und `7279`-Ports sind verfügbar, um Lizenzen von NetScaler Console an eine Instance auszuchecken. Weitere Informationen finden Sie unter Systemanforderungen.

Schritt 1 —Lizenzen in NetScaler Console anwenden

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > 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 auf NetScaler Console 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 Console jederzeit über die Lizenzeinstellungen weitere Lizenzen**
>
> hinzufügen.

3. Klicken Sie auf **Fertig stellen**.

   Die Lizenzdateien werden zur NetScaler Console hinzugefügt. Auf der Registerkarte **Informationen zum Ablauf** der Lizenz sind die in der NetScaler Console 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 gepoolte Kapazität zu verwenden.

Schritt 2 —Registrieren Sie die NetScaler Console als Lizenzserver

Sie können die NetScaler Console mithilfe eines Agenten als Lizenzserver für eine NetScaler-Instanz registrieren.

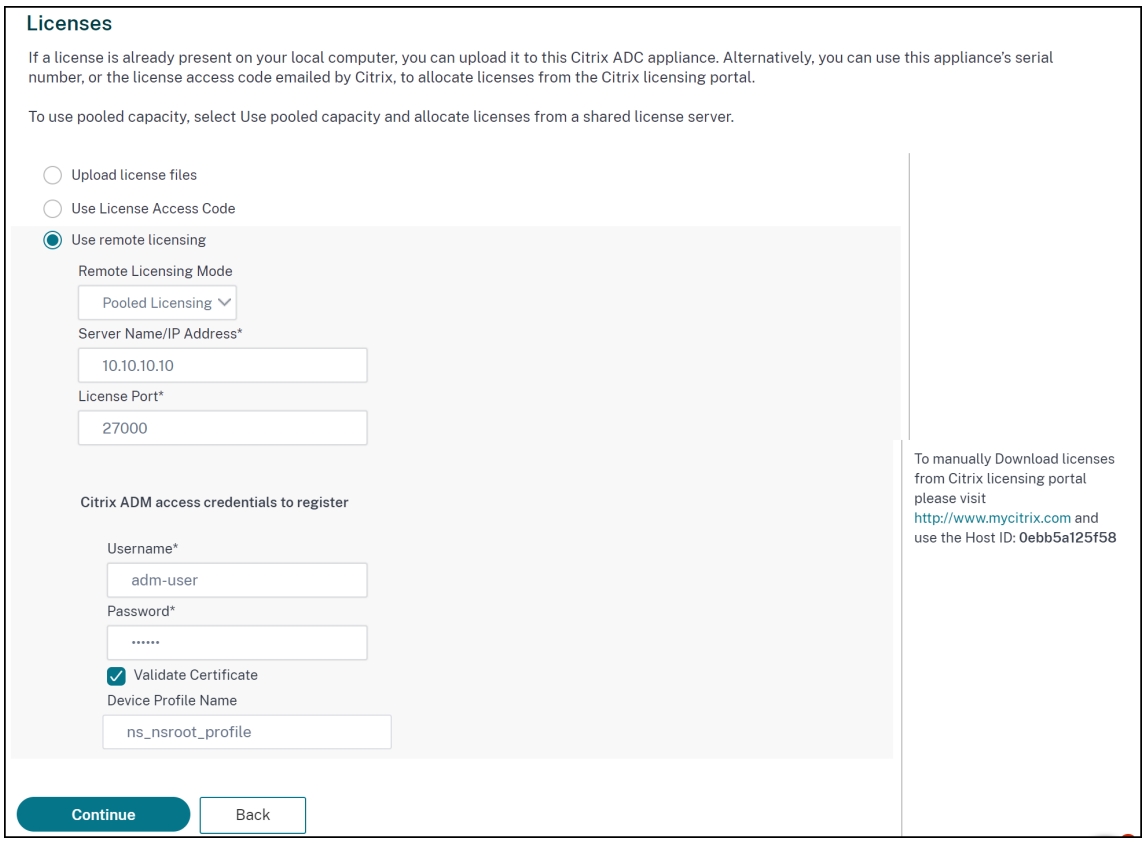
Verwenden Sie eines der folgenden Verfahren, um die NetScaler Console als Lizenzserver zu registrieren:

- GUI verwenden

Verwenden Sie die GUI, um einen Agenten zu registrieren

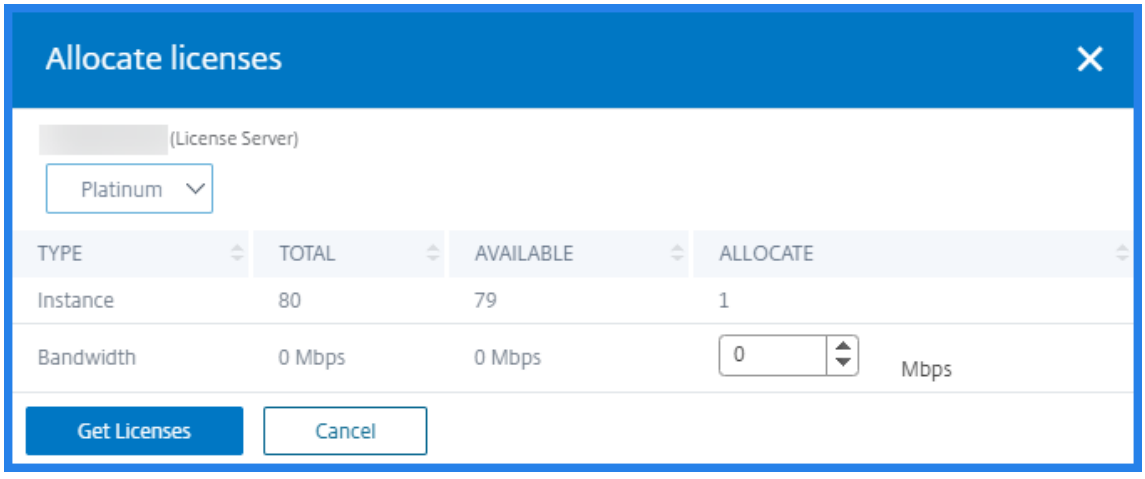
Registrieren Sie in der NetScaler Console-GUI den Agenten, der einer NetScaler-Instanz zugeordnet ist.

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 Agents an, die bei der NetScaler Console registriert ist.
6. Wählen Sie **Bei NetScaler Console registrieren** aus.
7. Geben Sie Ihre Agent-Anmeldeinformationen ein, um eine Instanz bei NetScaler Console zu registrieren, und klicken Sie auf **Weiter**. In NetScaler Console ist einer der Agents 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 über die NetScaler Console-GUI ändern oder freigeben.



9. Klicken Sie auf **Get Licenses**.

> **Wichtig!**

> Starten Sie die Instanz warm neu, wenn Sie die Lizenzversion ändern. Die Konfigurationsänderungen werden erst wirksam, wenn Sie die Instanz neu starten.

Verwenden Sie CLI, um einen Agenten hinzuzufügen

Wenn eine NetScaler-Instanz keine GUI hat, verwenden Sie die folgenden CLI-Befehle, um einen Agenten hinzuzufügen, der einer Instanz zugeordnet ist:

1. Melden Sie sich bei der NetScaler Konsole an.
2. Fügen Sie die IP-Adresse des zugehörigen Agents hinzu, die bei der NetScaler Console registriert ist:

```
> add ns licenseserver <adm-agent-IP-address> -port <adm-agent-license-port-number>
```

3. Zeigen Sie die im Lizenzserver verfügbare Lizenzbandbreite an:

```
> sh ns licenseserverpool
```

4. Weisen Sie die Lizenzbandbreite aus der erforderlichen Lizenzedition zu:

```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth > edition <specify-license-edition>
```

   Die Lizenzausgabe kann **Standard** oder **Advanced** oder **Premium**sein.

   > **Wichtig**
   >
   > Warm starten Sie die Instanz neu, wenn Sie die Lizenzversion ändern.
   >
   > `reboot -w`
   >
   > Die Konfigurationsänderungen werden erst wirksam, wenn Sie die Instanz neu starten.

Schritt 3 —Zuweisen von gepoolten Lizenzen zu NetScaler-Instanzen

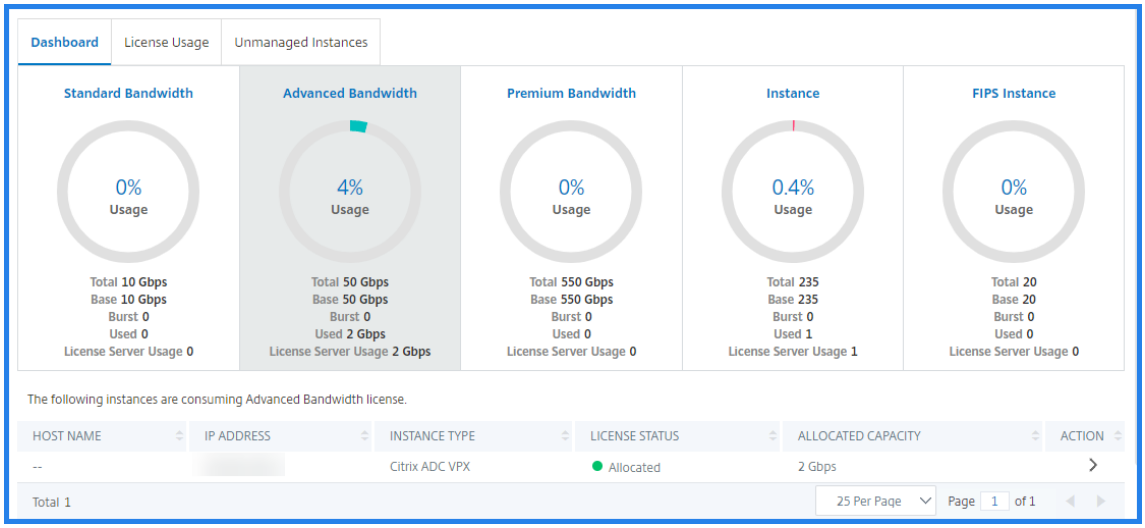
So weisen Sie gepoolte Kapazitätslizenzen über die NetScaler Console-GUI zu:

1. Melden Sie sich bei NetScaler Console an.
2. Navigieren Sie zu **Infrastruktur > Pool-Lizenzierung > Bandbreitenlizenzen > Poolkapazität**.

   Die FIPS-Instanzkapazität wird nur angezeigt, wenn Sie FIPS-Instanzlizenzen auf NetScaler Console hochladen.
3. Klicken Sie auf den Lizenzpool, den Sie verwalten möchten.

> **Hinweis:**
>
> Das Feld **Zugewiesene 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.

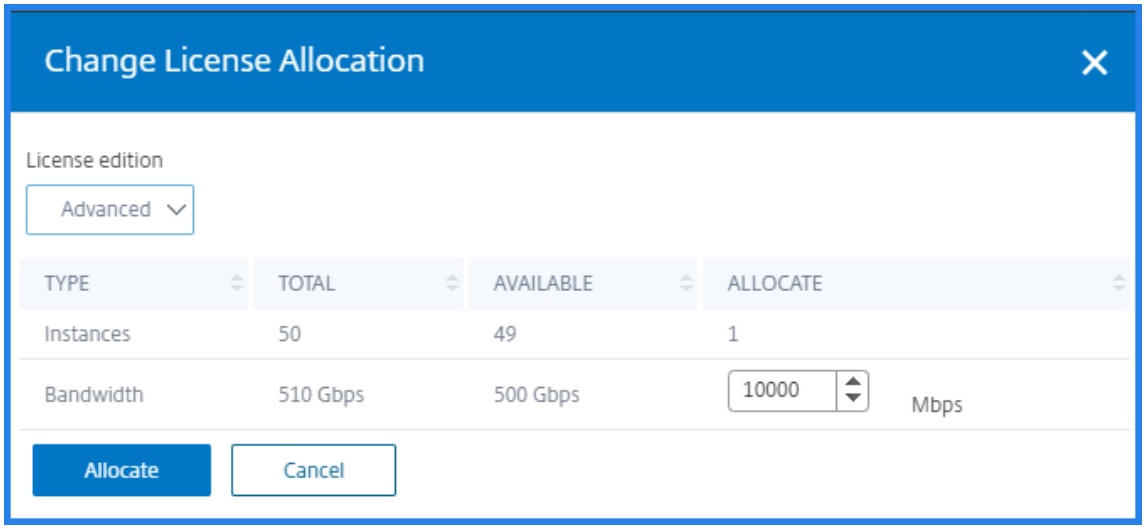


In der Spalte Lizenzstatus werden die entsprechenden Statusmeldungen zur Lizenzzuweisung angezeigt.

> **Hinweis:**
>
> Auf der Registerkarte **Unmanaged Instances** werden die Instanzen angezeigt, die in NetScaler Console 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 bei einem Warmstart neu, wenn Sie die Lizenzedition ändern.

Konfiguration der gepoolten Kapazität auf NetScaler-Instanzen

Sie können gepoolte Kapazitätslizenzen auf den folgenden NetScaler-Instanzen konfigurieren:

- NetScaler MPX-Z-Instanzen
- NetScaler SDX-Z-Instanzen
- NetScaler VPX-Instanzen
- NetScaler Hochverfügbarkeitspaar

NetScaler MPX-Z-Instanzen

MPX-Z ist die NetScaler MPX-Appliance mit gepoolter Kapazität. MPX-Z unterstützt Bandbreiten-Pooling für Premium-, Advanced- oder Standard 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, ist die Funktion für 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 SDX-Z-Instanzen

SDX-Z ist die NetScaler SDX-Appliance mit gepoolter Kapazität. SDX-Z unterstützt Bandbreite und Instanz-Pooling für Premium-, Advanced- oder Standard 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, ist die Funktion für gepoolte Kapazität deaktiviert. Die Instanzlizenzen werden für den Lizenzserver freigegeben.

Sie können die Bandbreite einer SDX-Z-Instanz ohne Neustart dynamisch 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-Instanzen

Eine NetScaler VPX-Instanz mit aktivierter Kapazität kann Lizenzen aus einem Bandbreitenpool auschecken (Premium/Advanced/Standard-Editionen). 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 Console-Server ausgecheckt.

NetScaler Hochverfügbarkeitspaar

Bevor Sie beginnen, stellen Sie sicher, dass der NetScaler Console-Server als Lizenzserver konfiguriert ist. Weitere Informationen finden Sie unter NetScaler Console als Lizenzserver konfigurieren

Wenn Sie die Bandbreite einem NetScaler HA-Paar zuweisen, checkt die NetScaler Console dieselbe Bandbreite für primäre und sekundäre Instanzen aus. Wenn Sie einem NetScaler HA-Paar eine Bandbreite von 10 Mbit/s zuweisen, geht NetScaler Console wie folgt vor:

1. Prüft 20 Mbit/s Bandbreite für das HA-Paar aus.
2. Ordnet jeder Instanz im HA-Paar 10 Mbit/s zu.

Informationen zum Zuweisen einer Poollizenz zu einem NetScaler HA-Paar finden Sie unter Zuweisen von gepoolten Lizenzen zu NetScaler-Instanzen.

Auf der Seite "**Pooled Capacity** "werden die Instanzen und ihre zugewiesene Kapazität separat angezeigt. Wenn Sie die Bandbreite der primären Instanz ändern oder freigeben, wird die Bandbreite der sekundären Instanz automatisch mit der primären Instanz synchronisiert. Die Synchronisierung erfolgt jedoch nicht, wenn Sie die Bandbreite der sekundären Instanz ändern oder freigeben.

Aktualisieren Sie eine unbefristete Lizenz in NetScaler MPX auf NetScaler Pooled Capacity

Die NetScaler MPX-Appliance mit unbefristeter Lizenz kann auf eine NetScaler Pooled-Kapazitätslizenz aktualisiert werden. Durch ein Upgrade auf die NetScaler Pooled Capacity License können Sie NetScaler Appliances bei Bedarf Lizenzen aus dem Lizenzpool zuweisen. NetScaler kann jeweils eine Lizenz verwenden, d. h. entweder eine unbefristete Lizenz oder eine gepoolte Lizenz verwenden. Ein Kunde kann von einer gepoolten Lizenz zu einer unbefristeten Lizenz wechseln. Solange die unbefristete Lizenz gültig ist, können Sie den NetScaler neu konfigurieren und die gepoolte Lizenzierungskonfiguration entfernen. Wenn ein Kunde von einer unbefristeten Lizenz zur Poollizenz oder von einer gepoolten zur unbefristeten Lizenz wechselt, werden alle NetScaler-Instanzen neu gestartet.

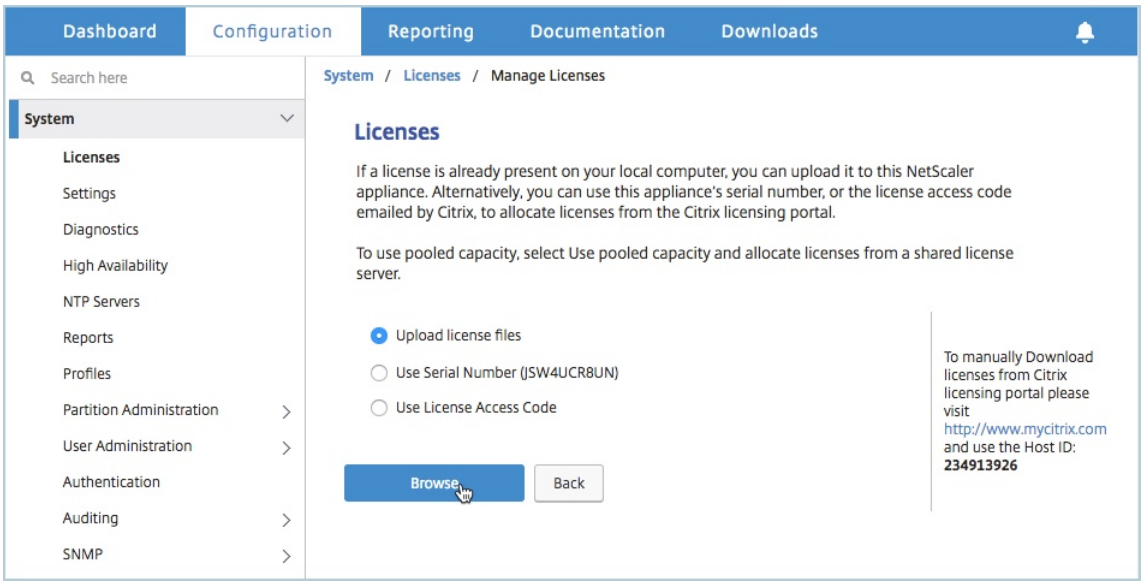
Sie können auch die NetScaler Pooled-Kapazitätslizenz für NetScaler-Instanzen konfigurieren, die im Hochverfügbarkeitsmodus konfiguriert sind. Informationen zum Konfigurieren der NetScaler Pooled-Kapazitätslizenz für NetScaler MPX-Instanzen im Hochverfügbarkeitsmodus finden Sie unter Upgrade der unbefristeten Lizenz im NetScaler MPX-Hochverfügbarkeitspaar auf NetScaler Pooled-Kapazität.

> **Hinweis**
>
> Um die NetScaler MPX-Appliance auf eine NetScaler Pooled-Kapazitätslizenz zu aktualisieren,

müssen Sie die MPX-Z-Lizenz auf die Appliance hochladen.

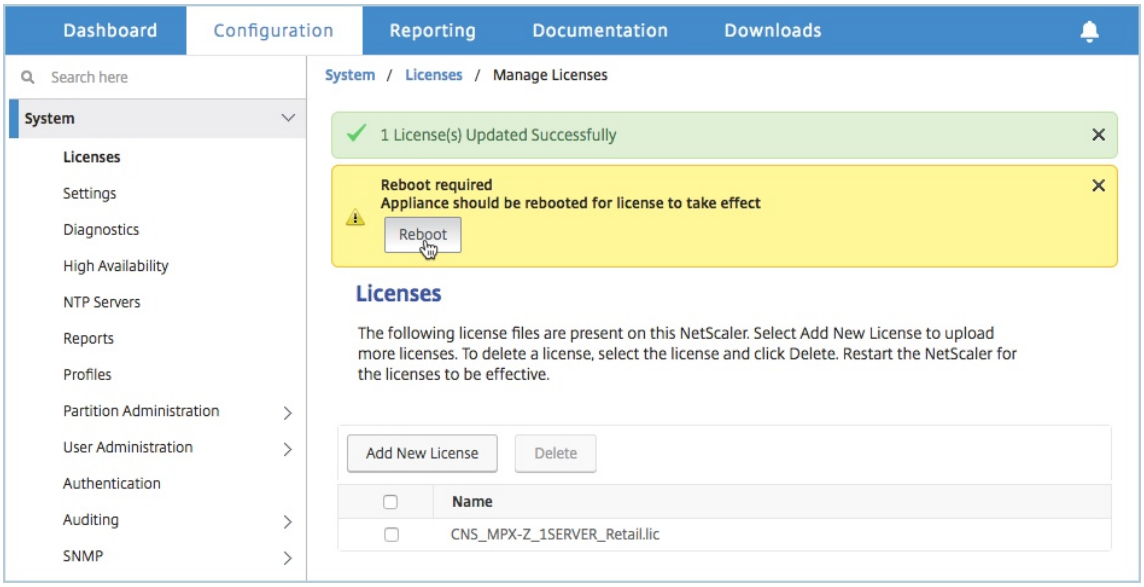
So führen Sie ein Upgrade auf NetScaler Pooled-Kapazität durch:

1. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler Appliance ein, http://192.168.100.1z.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** 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.

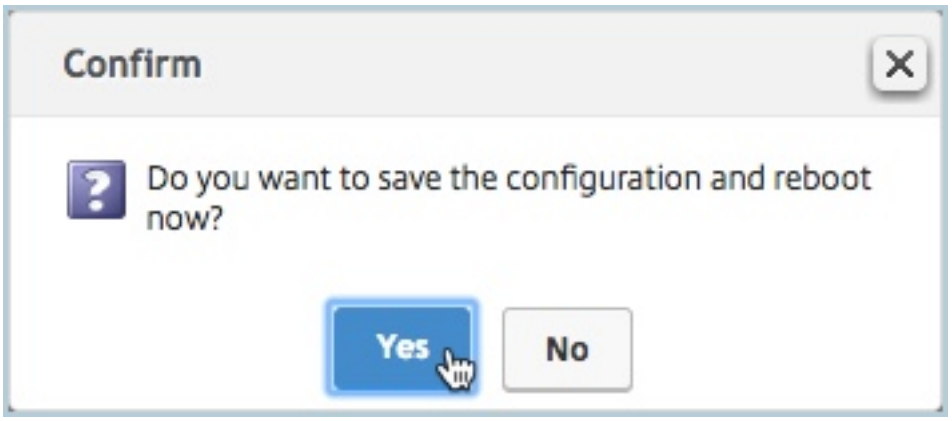


7. Klicken Sie nach dem Hochladen der Lizenz auf **Neu starten**, um die Appliance neu zu starten.

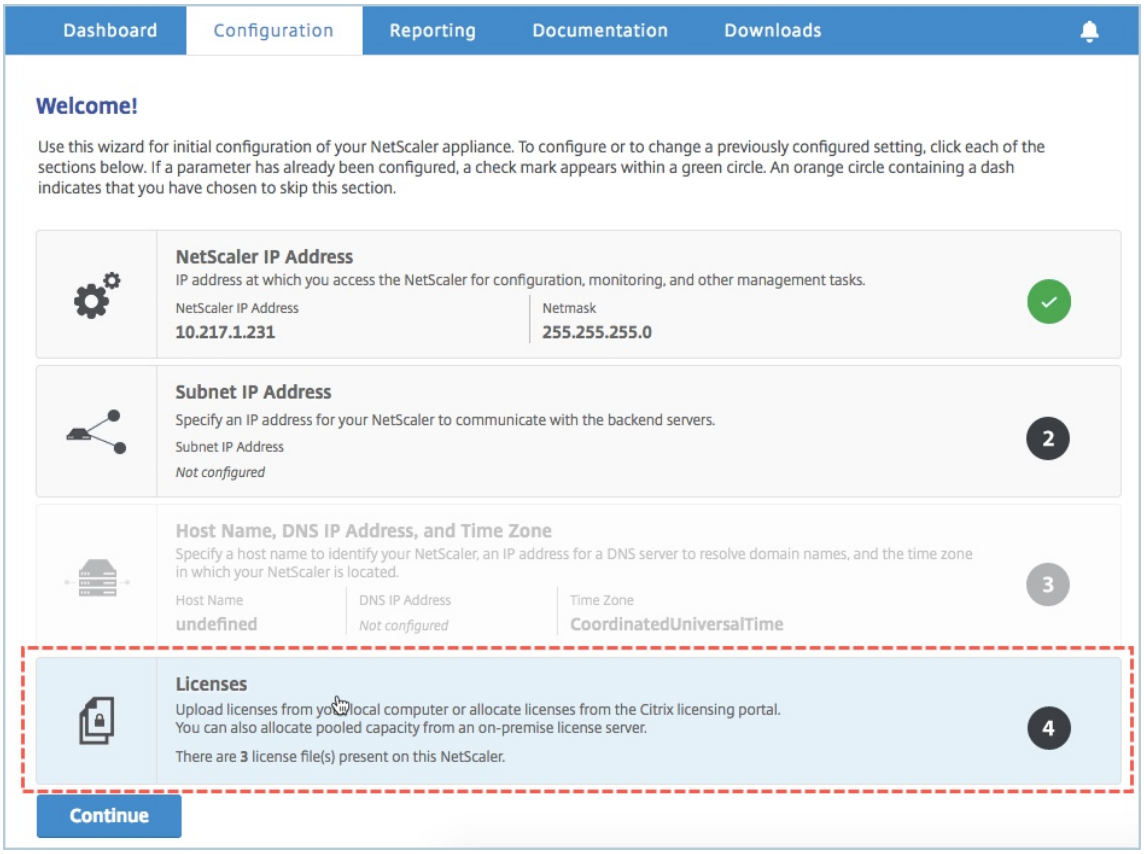
> **Warnung**
>
> Nach der Anwendung der MPX-Z-Lizenz werden die Funktionen, einschließlich SSL-Offloading auf der Appliance, nicht lizenziert. Die Appliance beendet die Verarbeitung von HTTPS-Anforderungen.
>
> Wenn die Option **Nur sicherer Zugriff** auf der Appliance vor dem Upgrade aktiviert ist, können Sie über die NetScaler Console-GUI mithilfe von HTTPS keine Verbindung zur Appliance herstellen.



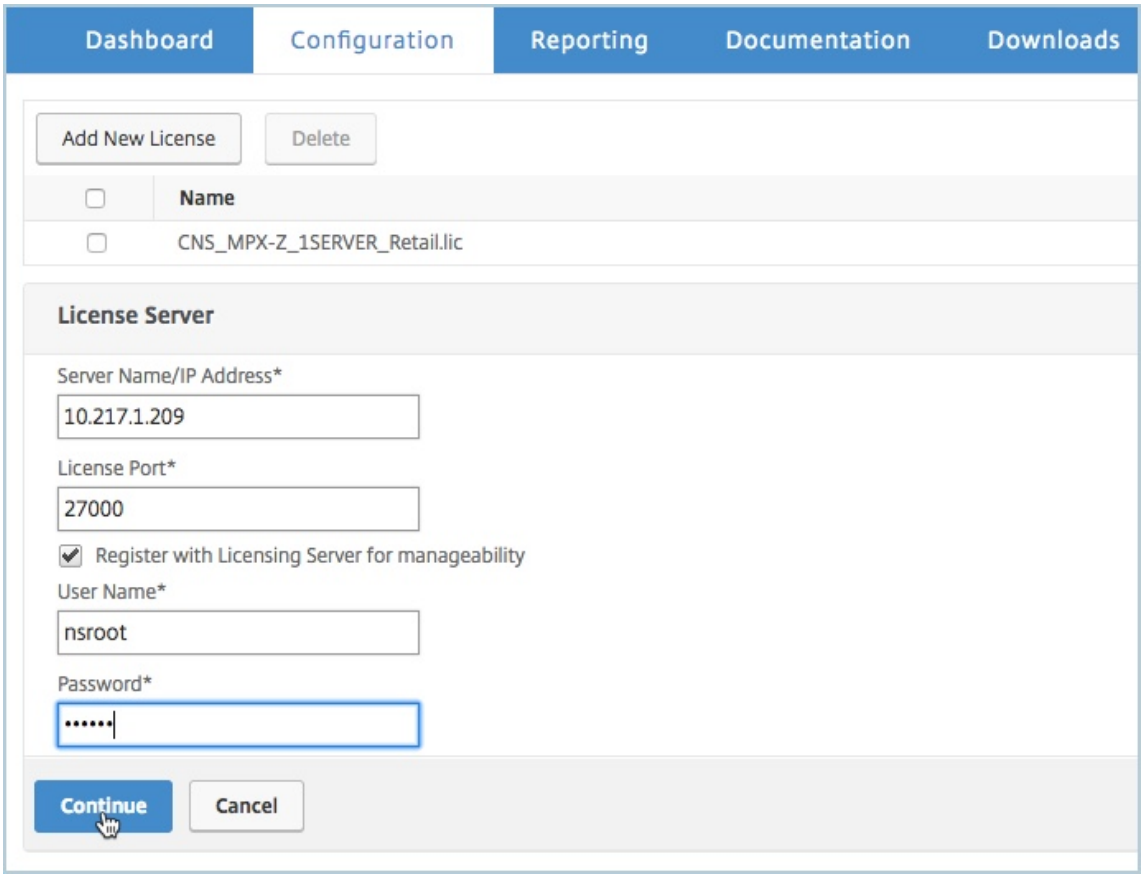
8. Klicken Sie auf der Seite **Bestätigen** auf **Ja**.



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.

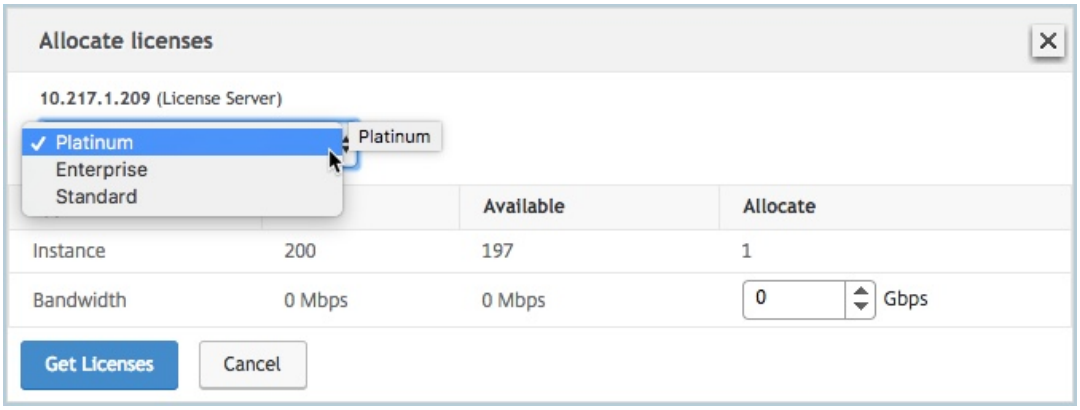
b) Geben Sie im Feld **Lizenzport** den Lizenzserver-Port ein. Standardwert: 27000.

c) Wenn Sie die Poollizenzen Ihrer Instanz über NetScaler Console verwalten möchten, aktivieren Sie das Kontrollkästchen **Für Verwaltbarkeit beim Lizenzserver registrieren** und geben Sie die NetScaler Console-Anmeldeinformationen ein.

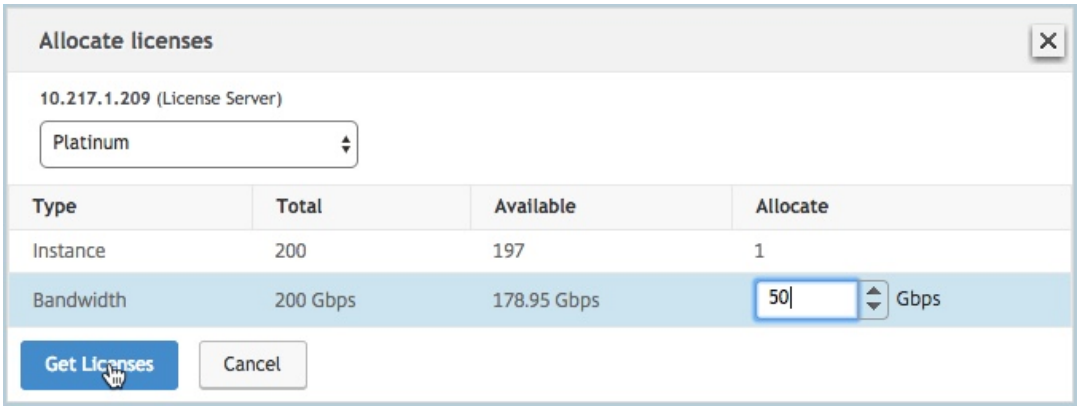
d) Klicken Sie auf **Weiter**.

12. Gehen Sie im Fenster Lizenzen zuweisen wie folgt vor:

a) Wählen Sie die Lizenzversion aus der Dropdownliste aus.

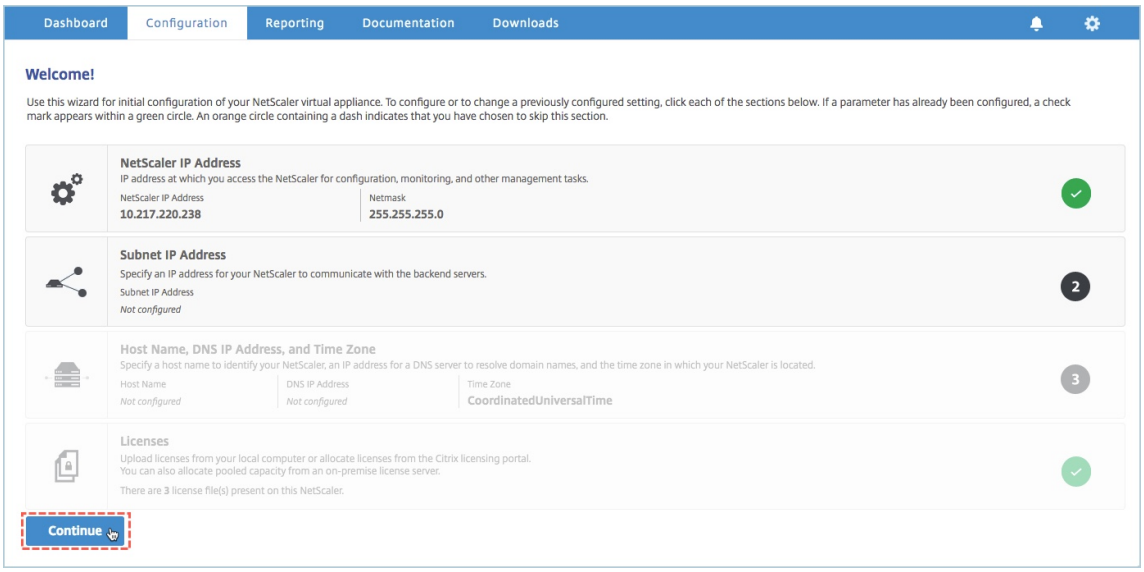


b) Weisen Sie der NetScaler Appliance im Menü **Zuweisen** die Bandbreite zu, und klicken Sie auf **Lizenzen abrufen**.

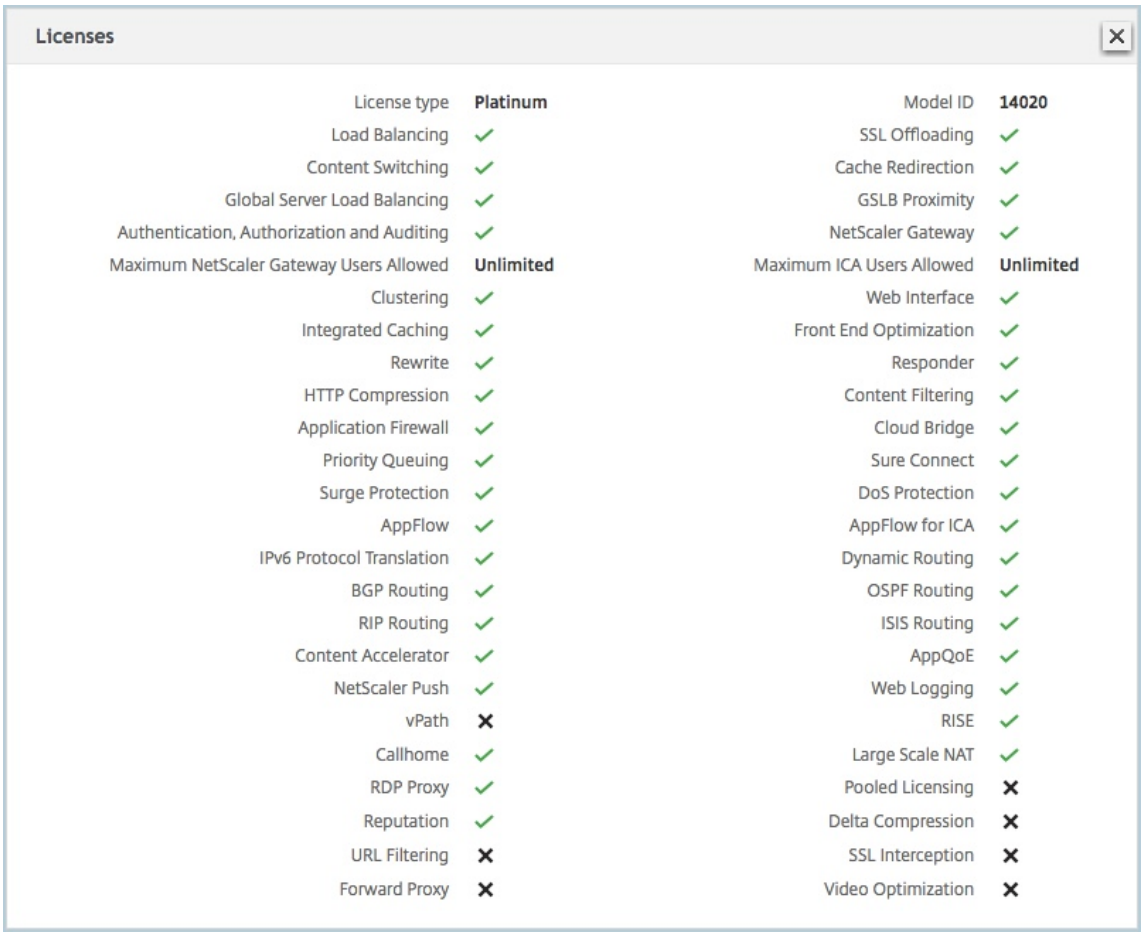


c) Wenn Sie dazu aufgefordert werden, klicken Sie auf **Neu starten**, um die Appliance neu zu starten.

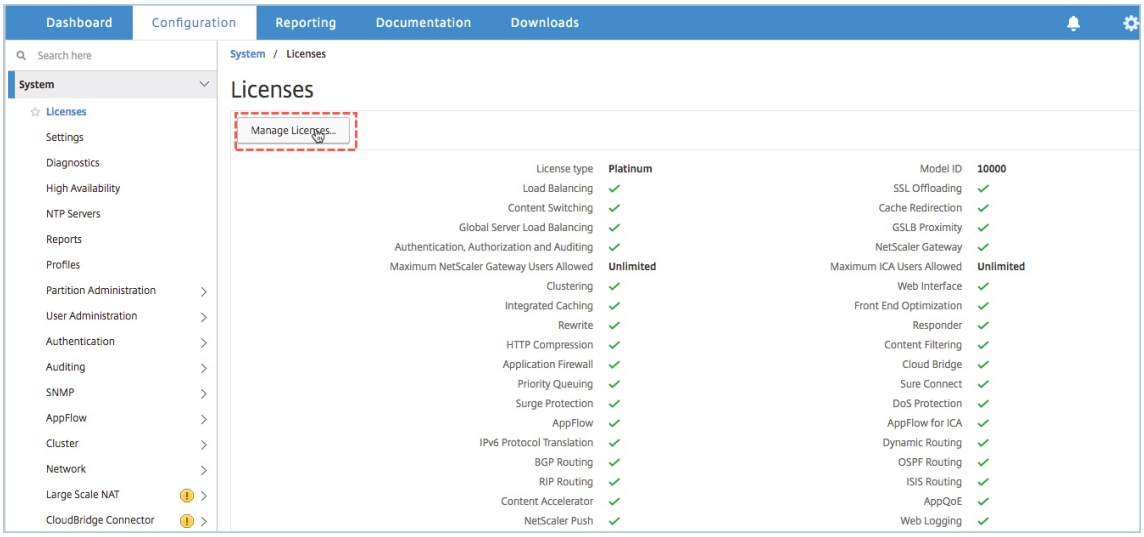
13. Melden Sie sich nach dem Neustart der NetScaler MPX-Appliance bei der NetScaler MPX-Appliance an. Klicken Sie auf der **Willkommensseite** auf **Weiter**.



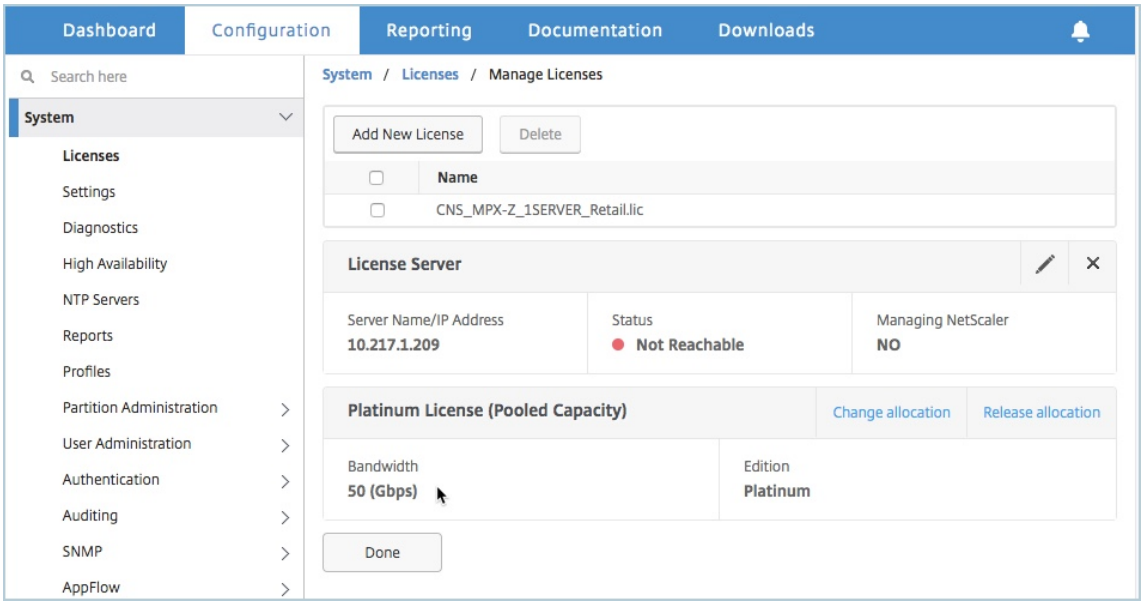
Auf der Seite **Lizenzen** werden alle lizenzierten Funktionen aufgelistet.



14. Navigieren Sie zu **System > Pool-Lizenzierung** 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 NetScaler MPX-Appliances, die im Hochverfügbarkeitsmodus konfiguriert sind, müssen Sie die NetScaler Pooled-Kapazität sowohl auf der primären als auch auf der sekundären NetScaler-Instanz im HA-Paar konfigurieren. Sie müssen Lizenzen mit derselben Kapazität sowohl den primären als auch den sekundären NetScaler Instanzen im HA-Paar zuweisen. Wenn Sie beispielsweise eine Kapazität von 1 Gbit/s von jeder Instanz im HA-Paar benötigen, müssen Sie 2 Gbit/s Kapazität aus dem gemeinsamen Pool zuweisen, damit Sie je 1 Gbit/s den primären und sekundären NetScaler Instanzen im HA-Paar zuweisen können.

> **Wichtig!**
>
> Um die NetScaler MPX-Appliance für die Verwendung der NetScaler Pooled-Kapazitätslizenz zu aktualisieren, müssen Sie die MPX-Z auf die Appliance hochladen.

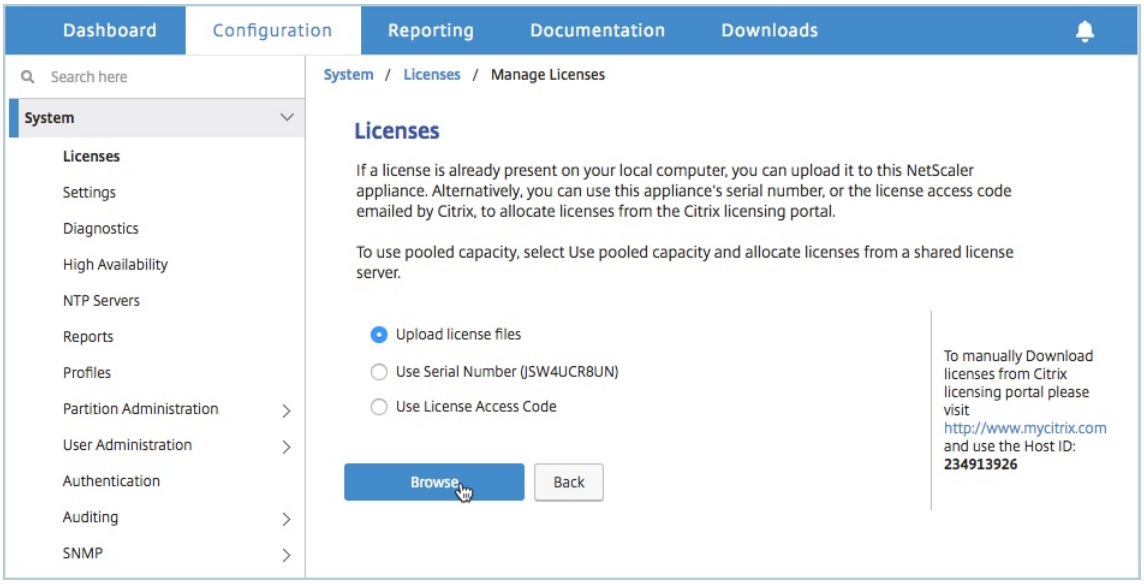
Voraussetzungen

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:

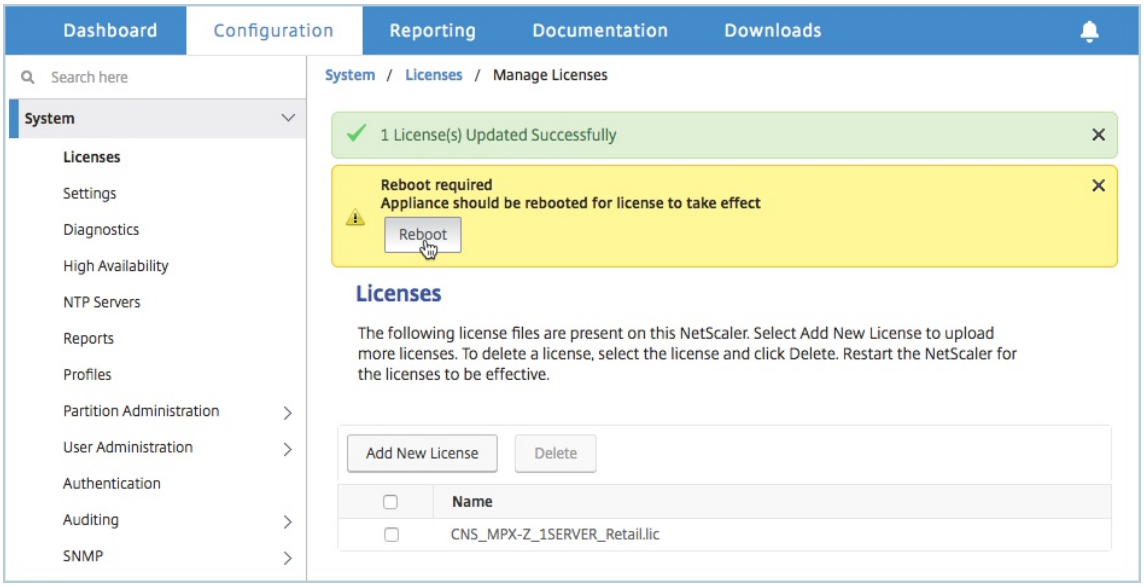
1. Geben Sie in einem Webbrowser die IP-Adresse der Appliance ein, z. http://192.168.100.1B.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.

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.

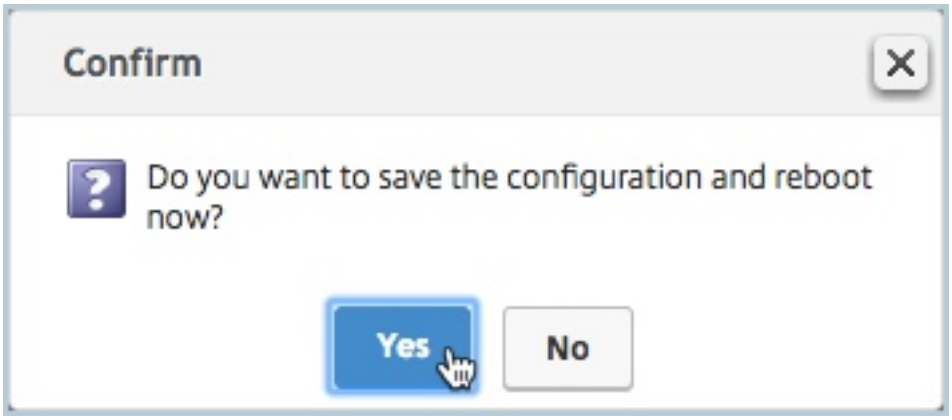


Nach dem Hochladen der Lizenz werden Sie aufgefordert, die Appliance neu zu starten.

7. Klicken Sie auf **Neu starten**, um die Appliance neu zu starten.

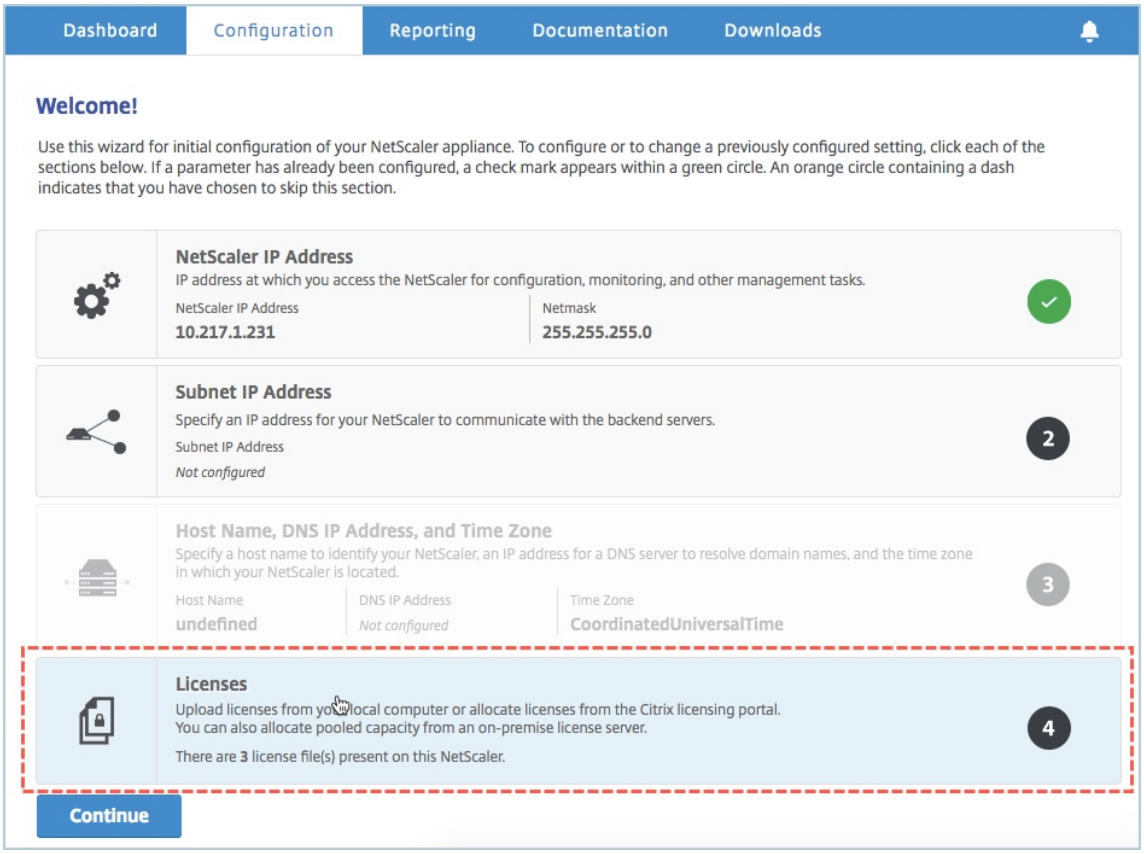


8. Klicken Sie auf der Seite **Bestätigen** auf **Ja**.

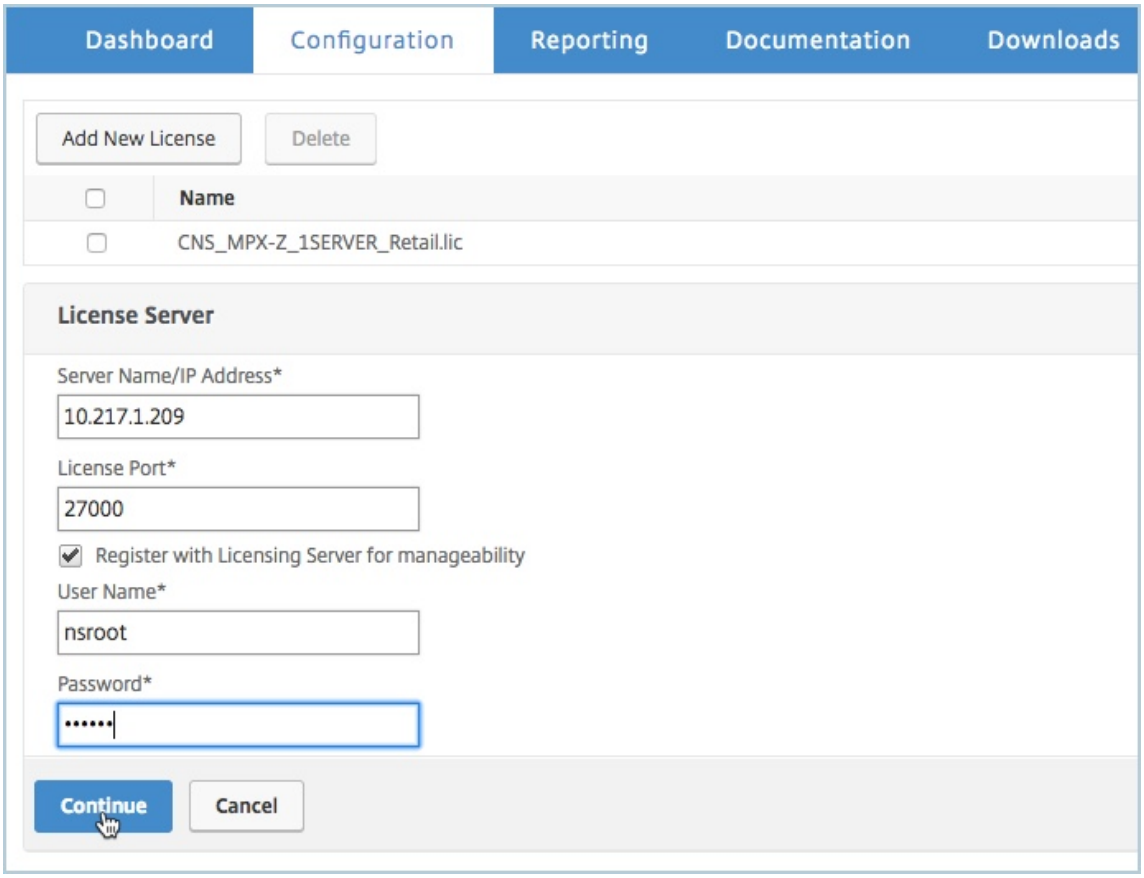


So aktualisieren Sie ein vorhandenes HA-Setup auf NetScaler Pooled-Kapazität:

1. Melden Sie sich bei der sekundären NetScaler MPX-Instanz an. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler Appliance ein, http://192.168.100.1z.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** 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.

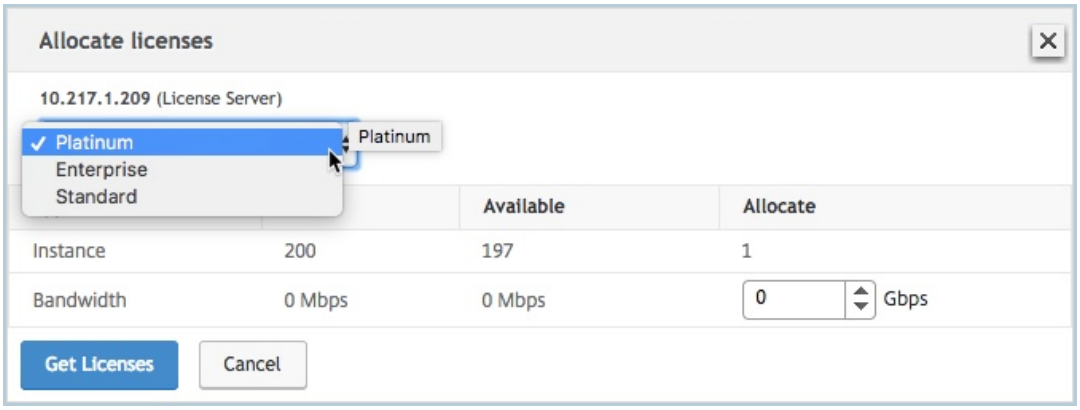
b) Geben Sie im Feld **Lizenzport** den Lizenzserver-Port ein. Standardwert: 27000.

c) Wenn Sie die Poollizenzen Ihrer Instanz über NetScaler Console verwalten möchten, aktivieren Sie das Kontrollkästchen **Für Verwaltbarkeit beim Lizenzserver registrieren** und geben Sie die NetScaler Console-Anmeldeinformationen ein.

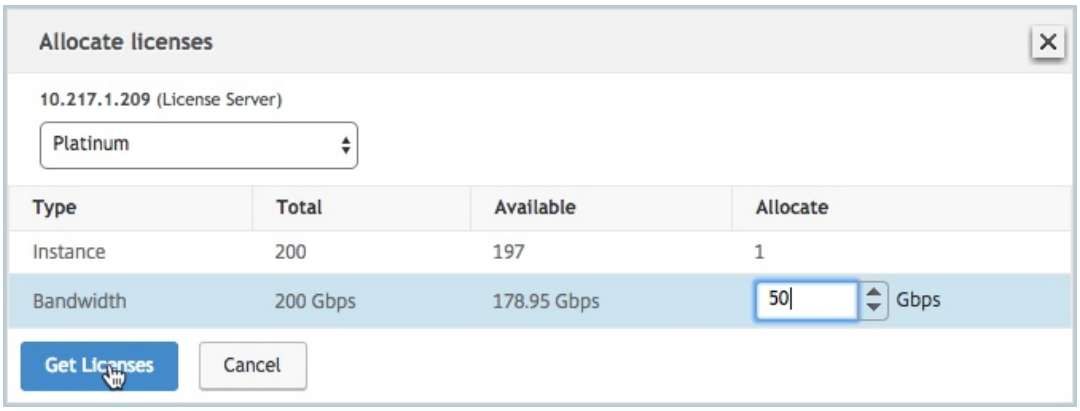
d) Klicken Sie auf **Weiter**.

5. Gehen Sie im Fenster **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 **Neu starten**, um die Appliance neu zu starten.

Nachdem die sekundäre NetScaler MPX-Appliance neu gestartet wurde, wird sie zur primären NetScaler MPX-Appliance im HA-Paar.

6. Melden Sie sich bei der vorhandenen primären NetScaler MPX Appliance an und starten Sie die Appliance neu. Führen Sie folgende Schritte aus:

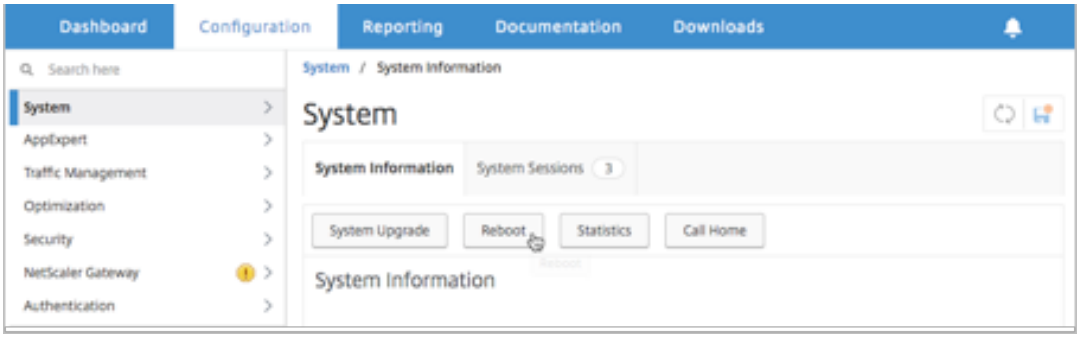
a) Geben Sie in einem Webbrowser die IP-Adresse der NetScaler Appliance ein, http://192.168.100.1z.

b) Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.

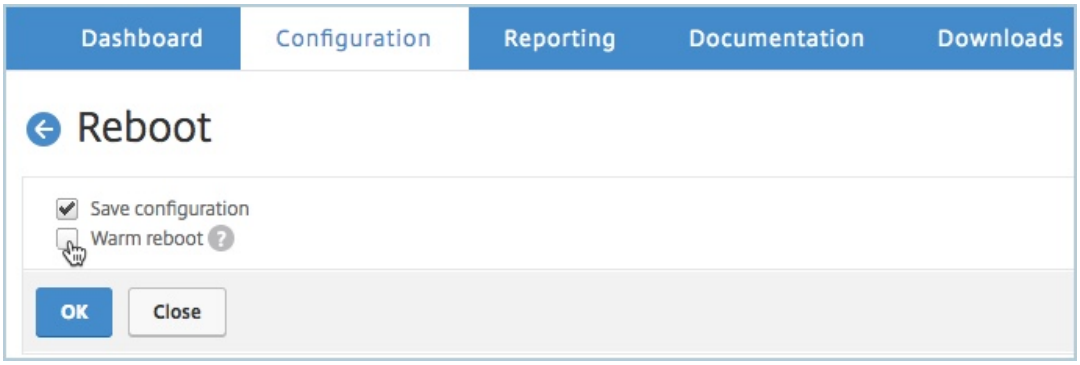
c) Klicken Sie auf der **Willkommensseite** auf **Weiter**.

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**.



Nachdem die primäre NetScaler MPX-Appliance neu gestartet wurde, wird sie zur sekundären NetScaler MPX-Appliance im HA-Paar. Bei Bedarf können Sie die primären und sekundären Instanzen im HA-Paar auf Ihre ursprüngliche HA-Paarkonfiguration ändern, indem Sie den folgenden Befehl für jede Instance im HA-Paar verwenden:

```
1 > force ha failover
```

Aktualisieren Sie eine unbefristete Lizenz in einem NetScaler SDX auf NetScaler Pooled Capacity

January 26, 2024

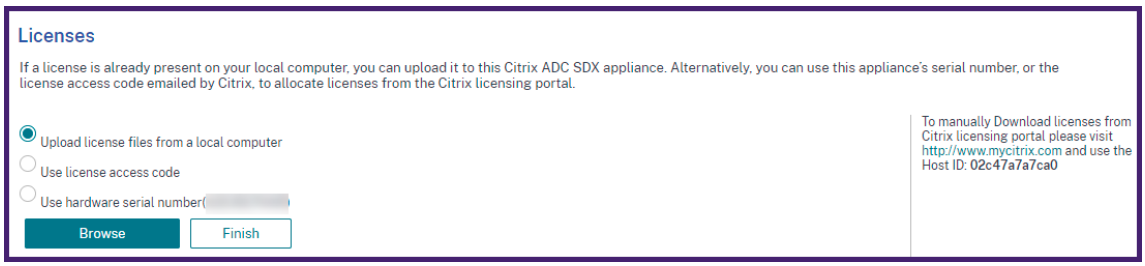
Ein NetScaler SDX mit unbefristeter Lizenz kann auf eine NetScaler Pooled-Kapazitätslizenz aktualisiert werden. Durch ein Upgrade auf die NetScaler Pooled Capacity License können Sie NetScaler Appliances bei Bedarf Lizenzen aus dem Lizenzpool zuweisen. NetScaler kann jeweils eine Lizenz verwenden, d. h. entweder eine unbefristete Lizenz oder die gepoolte Lizenz verwenden. Ein Kunde kann von einer Pool-Lizenz zu einer unbefristeten Lizenz wechseln. Solange die unbefristete Lizenz gültig ist, kann ein Kunde den NetScaler neu konfigurieren und die gepoolte Lizenzkonfiguration entfernen. Wenn ein Kunde von einer unbefristeten Lizenz zur Poollizenz oder von einer gepoolten zur unbefristeten Lizenz wechselt, werden alle NetScaler-Instanzen neu gestartet.

Sie können auch die NetScaler Pooled-Kapazitätslizenz für NetScaler-Instanzen konfigurieren, die in einem Hochverfügbarkeitsmodus konfiguriert sind.

> **Hinweis**
>
> Um die SDX-Appliance auf eine NetScaler Pooled-Kapazitätslizenz zu aktualisieren, müssen Sie die SDX-Z-Lizenz auf die Appliance hochladen.
>
> Stellen Sie sicher, dass Sie über die Berechtigung zum Hinzufügen von NetScaler-Instanzen in der NetScaler Console verfügen.

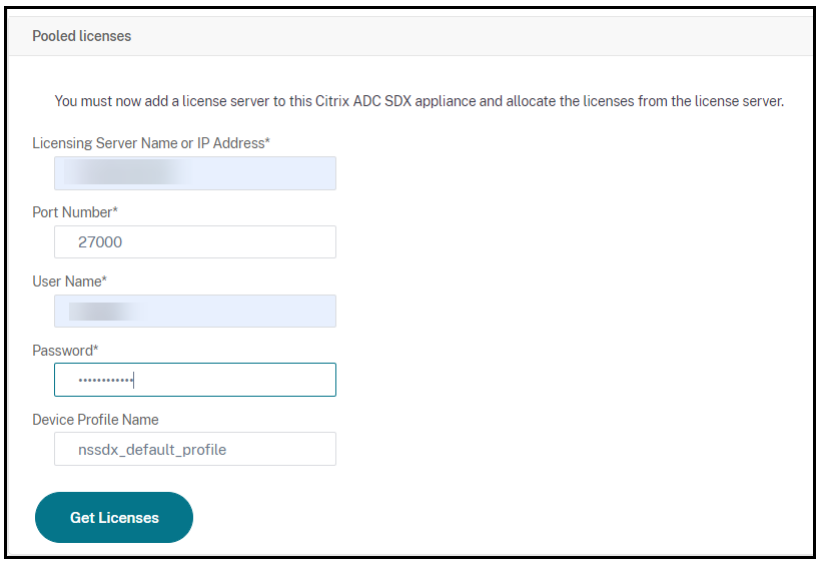
So aktualisieren Sie auf NetScaler gepoolte Kapazität:

1. Geben Sie in einem Webbrowser die IP-Adresse der SDX-Appliance ein, z. B. http://192.168.100.1
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** 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 auf der Seite „**Lizenzen “der Abschnitt „ GepoolteLizenzen** “angezeigt.

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.

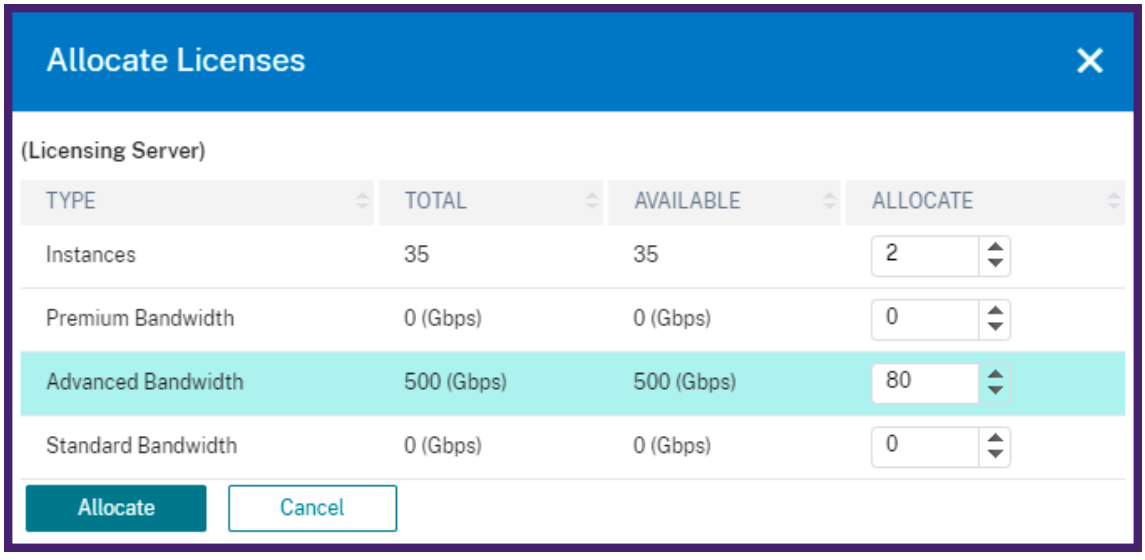
   Wenn Sie den NetScaler Console-Server als Lizenzserver konfigurieren möchten, geben Sie die IP-Adresse des NetScaler Console-Servers an.

   Wenn Sie einen Agenten für die Kommunikation mit dem NetScaler Console-Server verwenden, geben Sie die IP-Adresse des Agenten an.

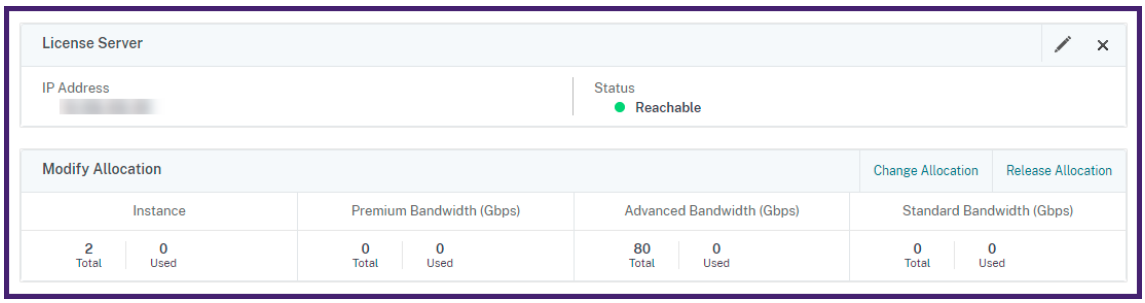
b) Geben Sie im Feld **Portnummer** den Lizenzserverport ein. Standardwert: 27000.

c) 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.

Szenarien für den Ablauf von flexiblen oder gepoolten Lizenzen und das Verhalten bei Verbindungsproblemen

January 26, 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 erklären das Verhalten, wenn eine neue Lizenz vor und nach Ablauf der Laufzeit auf NetScaler Console 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 erklären das Verhalten, wenn eine neue Lizenz vor und nach Ablauf der Laufzeit auf NetScaler Console 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 erklären das Verhalten, wenn eine neue Lizenz vor und nach Ablauf der Laufzeit auf NetScaler Console 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 auf der NetScaler Console 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 Agent oder zwischen Agent und NetScaler Console Service 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 Console-Server nur als Flexe- oder Pool-Lizenzserver

January 26, 2024

Als Administrator können Sie die NetScaler Console nur für die Funktion Pooled Licensing konfigurieren. Bei dieser Konfiguration empfängt die NetScaler Console 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 eines NetScaler Console-Servers in Ihrer regulatorischen Zone bereitstellen, um die Verwaltungs-, Überwachungs- und Analysefunktionen zu nutzen. Wenn Sie die Funktion für gepoolte Lizenzen auf dieselbe Weise verwenden, müssen Sie die gepoolten Lizenzen auf ver-

schiedene NetScaler Console-Lizenzserver aufteilen. Dieser Ansatz bietet Ihnen nicht die Flexibilität, Pool-Lizenzen Ihren global bereitgestellten NetScaler-Instanzen zuzuweisen.

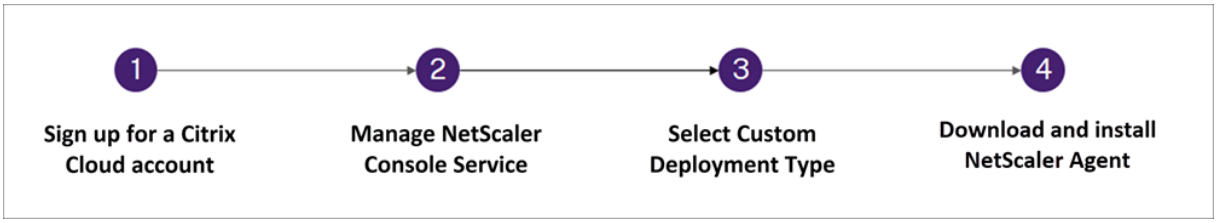
Konfigurieren Sie die NetScaler Console daher nur für die Funktion Pooled Licensing. Die NetScaler Console empfängt nur Lizenzdaten von allen NetScaler-Instanzen. So können Sie die regulatorischen Vorgaben einhalten und gepoolte Kapazitätslizenzen dynamisch auf global eingesetzte NetScaler-Instanzen verteilen.

In diesem Dokument wird erklärt, wie Sie die NetScaler Console nur für die Funktion Pooled Licensing konfigurieren.

Voraussetzungen

Bevor Sie die NetScaler Console nur für die Funktion Pooled Licensing konfigurieren, führen Sie das erste Onboarding und die Einrichtung der NetScaler Console durch. Stellen Sie sicher, dass Sie die Agentspezifikationen unter Systemanforderungenüberprüfen.

> **Wichtig**
>
> Wenn Sie die NetScaler Console zum ersten Mal einbinden oder einrichten, stellen Sie Folgendes sicher:
>
> - Die Option “Benutzerdefinierte Bereitstellung”ist ausgewählt.
> - NetScaler-Instanzen, die hinzugefügt werden müssen, nachdem Sie Schritt 4 in diesem Konfigurationsverfahren abgeschlossen haben



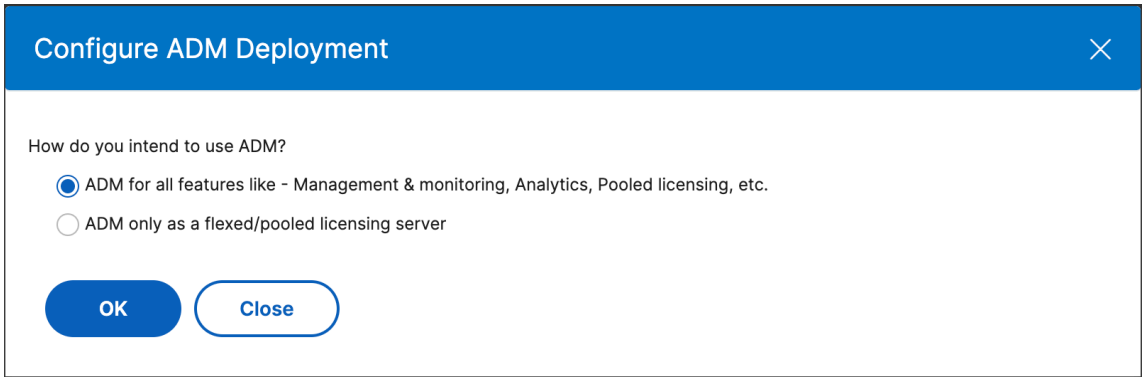
Weitere Informationen zum Onboarding und Einrichten der NetScaler Console finden Sie unter Erste Schritte.

Nachdem Sie die Onboarding-Schritte abgeschlossen haben, konfigurieren Sie die NetScaler Console nur für die Funktion Pooled Licensing.

So konfigurieren Sie NetScaler Console nur als Flexe- oder Pool-Lizenzserver

Gehen Sie wie folgt vor, um die NetScaler Console nur für die Lizenzierungsfunktion zu konfigurieren:

1. Navigieren Sie zu **Einstellungen > Allgemeine Einstellungen > Systemkonfigurationen > Systembereitstellung**.
2. Wählen Sie unter **NetScaler Console Deployment** die Option **NetScaler Console only als flexiblen oder gepoolten** Lizenzserver aus.



3. Klicken Sie auf **OK**.

   Diese Aktion behält nur die Pool-Lizenzierungsfunktion bei und deaktiviert die folgenden NetScaler Console-Funktionen:

   - NetScaler Console-Sicherung
   - Ereignisverwaltung
   - SSL Zertifikatsverwaltung
   - Netzwerkberichterstellung
   - Netzwerkfunktionen
   - Konfigurationsaudit

   > **Hinweis** Die NetScaler Console-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 Console-GUI zeigt jetzt nur noch die Funktion Pooled Licensing an. Und die übrigen Funktionen werden nicht angezeigt.

4. Nachdem Sie NetScaler Console nur für die Lizenzierungsfunktion konfiguriert haben, fügen Sie NetScaler-Instanzen auf der Seite **Infrastruktur > Instanzen** hinzu.

> **Hinweis**
>
> - Sie können eine NetScaler-Instanz auch in der NetScaler Console und auf anderen NetScaler Console-Servern hinzufügen. Wenn Sie das Kennwort solcher NetScaler-Instanzen ändern, stellen Sie sicher, dass Sie das Kennwort auf allen NetScaler Console-Servern aktualisieren, auf denen die Instanz erkannt wurde. Dieser Hinweis gilt, wenn

> die NetScaler Console nur für die Verwendung der gepoolten Lizenzierungsfunktion konfiguriert ist.
>
> - Ein Benutzer kann immer noch einige Operationen der deaktivierten Funktionen in der NetScaler Console-GUI ausführen. Zum Beispiel Event-Polling und NetScaler-Backup. Wenn Sie solche Vorgänge einschränken möchten, deaktivieren Sie als Superadministrator die Benutzerzugriffe für andere Administratoren mithilfe einer entsprechenden Zugriffsrichtlinie. Weitere Informationen finden Sie unter Konfigurieren von Zugriffsrichtlinien auf der NetScaler Console .

NetScaler VPX Ein- und Auschecken Lizenzierung

January 26, 2024

Sie können NetScaler VPX-Lizenzen NetScaler VPX-Instanzen bei Bedarf von der NetScaler Console aus zuweisen. Die Lizenzen werden von der NetScaler Console gespeichert und verwaltet, die über ein Lizenzierungsframework verfügt, das eine skalierbare und automatisierte Lizenzbereitstellung ermöglicht. Eine NetScaler VPX-Instanz kann, wenn sie bereitgestellt wird, die Lizenz über die NetScaler Console auschecken oder ihre Lizenz wieder in die NetScaler Console einchecken, wenn eine Instanz entfernt oder zerstört wird.

Installieren Sie Lizenzen in NetScaler Console

So installieren Sie Lizenzdateien auf der NetScaler Console:

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 in die Konsole 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 zur NetScaler Console hinzugefügt.

> **Hinweis**
>
> Stellen Sie sicher, dass Sie mit dem Internet verbunden sind, bevor Sie den Lizenzzugangscode für die Installation der Lizenzen verwenden.

Weisen Sie einer NetScaler VPX-Instanz mithilfe der NetScaler GUI eine NetScaler VPX-Lizenz zu

1. Melden Sie sich bei der NetScaler VPX-Instanz an und navigieren Sie zu **System > Lizenzen > Lizenzen verwalten**, klicken Sie auf **Neue Lizenz hinzufügen**und wählen Sie **Remote-Lizenzierung verwenden**aus.
2. Geben Sie die Details des Lizenzservers in das Feld **Servername/IP-Adresse** ein.

   > **Hinweis** Wenn Sie die NetScaler VPX-Lizenzen Ihrer Instanz über die NetScaler Console verwalten möchten, aktivieren Sie das Kontrollkästchen Beim **NetScaler MA Service registrieren** und geben Sie die NetScaler Console-Anmeldeinformationen ein.

3. Klicken Sie auf **Weiter**.
4. 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**.
5. 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.

6. Sie können die Lizenzzuweisung ändern oder freigeben, indem Sie zu **System > Lizenzen > Lizenzen verwalten** navigieren und Zuordnung **ändern oder Zuordnungfreigeben** auswählen.
7. Wenn Sie auf **Zuweisung ändern**klicken, werden in einem Popup-Fenster die auf dem Lizenzserver verfügbaren Lizenzen angezeigt. Wählen Sie die erforderliche Lizenz aus, klicken Sie auf **Lizenzen abrufen**.

Weisen Sie einer NetScaler VPX-Instanz mithilfe der NetScaler CLI eine NetScaler VPX-Lizenz zu

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 >]
```

```
> 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
```

```
> 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 einer NetScaler VPX-Instanz eine Lizenz zuzuweisen, geben Sie den folgenden Befehl ein:

```
set capacity  –platform V[S/E/P][Bandwidth]
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

Ablaufprüfungen für NetScaler VPX Check-In/Check-Out-Lizenzen konfigurieren

Sie können jetzt den Schwellenwert für Lizenzablaufzeiten für NetScaler VPX-Lizenzen konfigurieren. Durch das Festlegen von Schwellenwerten sendet NetScaler Console Benachrichtigungen per E-Mail oder SMS, wenn eine Lizenz bald abläuft. Ein SNMP-Trap und eine Benachrichtigung werden auch gesendet, wenn die Lizenz auf der NetScaler Console abgelaufen ist.

Ein Ereignis wird generiert, wenn eine Benachrichtigung über den Ablauf der Lizenz gesendet wird. Dieses Ereignis kann in der NetScaler Console angezeigt werden.

Weitere Informationen finden Sie unter Lizenzverwaltung .

NetScaler virtuelle CPU-Lizenzierung

January 26, 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

Eine solche Bewegung muss auch, dass die Softwareanforderungen dynamisch, flexibel und agil sind, um die sich ständig ändernden Geschäftsanforderungen zu erfüllen. Es wird erwartet, dass Lizenzen von einem zentralen Management-Tool verwaltet werden, das volle Einblick in die Nutzung bietet.

Virtuelle CPU-Lizenzierung für 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, die Anforderung gilt jedoch eher für andere L7-Leistungen wie SSL-TPS, Komprimierungsdurchsatz usw. 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 Console unterstützt jetzt die Zuweisung von Lizenzen an 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 gepoolter Lizenzkapazität und CICO-Lizenzfunktionen verwaltet der NetScaler Console-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 Lizenzserver in NetScaler VPX mithilfe 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** Registrieren Sie die NetScaler VPX-Instanz immer bei NetScaler Console. Wenn Sie noch nicht fertig sind, aktivieren Sie Bei NetScaler Console registrieren und geben Sie die NetScaler Console-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**.

   > **Hinweis** Weisen Sie für ein NetScaler HA-Paar jedem Knoten separat virtuelle CPU-Lizenzen zu.

8. Klicken Sie auf der nächsten Seite auf **Neustart**, um die Lizenzen zu beantragen.

   > **Hinweis**
   >
   > Sie können auch die aktuelle Lizenz freigeben und aus einer anderen Edition auschecken. Beispielsweise führen Sie bereits die Standard Edition-Lizenz für Ihre Instanz aus. Sie können diese Lizenz freigeben und dann aus der Advanced Edition auschecken.

FAQs und andere Ressourcen

April 10, 2024

In diesem Abschnitt sind die Referenzdokumentationen zur Konfiguration und zum Betrieb der Pool-Lizenzierung aufgeführt. Sie können sich auf diese Dokumente beziehen, um Unterstützung in Bezug auf Konfigurations- und Betriebsprobleme zu erhalten.

Konfiguration

1. Wo finde ich Informationen zur Übersicht und zu den Funktionen von Pooled Capacity?

   Antwort: Siehe Poolkapazität konfigurieren .

2. Wie konvertiere oder migriere ich unbefristete Lizenzen in Pool-Lizenzen und umgekehrt?

   Antwort: 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.

3. Wie stelle ich den NetScaler Console-Server bereit?

   Antwort: Folgen Sie dem Dokument Erste Schritte .

4. Wie füge ich einer bestehenden Pool-Lizenz eine Lizenz hinzu und weise sie zu?

   Antwort: Folgen Sie dem Dokument zur Lizenzverwaltung .

5. Wie ordne ich Kapazität und Bandbreite für Instanzen zu bzw. erhöhen?

   Antwort: Folgen Sie dem Dokument zur Lizenzverwaltung .

Lizenzserver-Agent

1. Wie weise ich die LSA-Rolle einem bestimmten Agent zu?

   Antwort: Dem ersten eingesetzten Agent wird die LSA-Rolle zugewiesen. Wenn der LSA-Agent ausfällt, beginnt für alle NetScaler-Instanzen, die für die Poollizenzierung mit der NetScaler Console verbunden sind, eine Kulanzfrist von einem Tag. Am nächsten Tag wählt NetScaler Console einen neuen Agent als LSA aus. Dieses Verhalten ist standardmäßig aktiviert.

   Administratoren können einen NetScaler Agent innerhalb von 24 Stunden manuell als LSA auswählen, anstatt darauf zu warten, dass der NetScaler Console-Dienst nach dem Ablauf von 24 Stunden, nachdem der LSA ausgefallen ist, automatisch einen Agent auswählt.

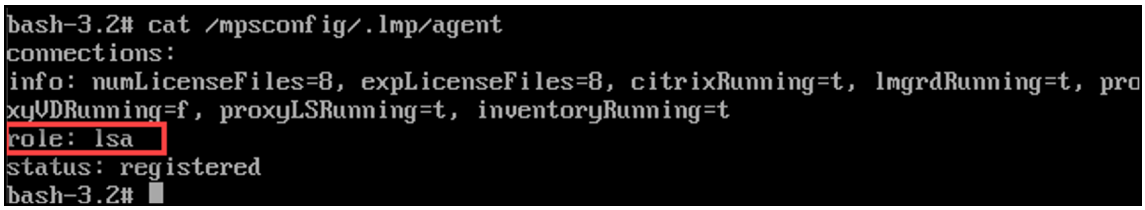
> **Hinweis:**
>
> Während dieses Übergangs wird die NetScaler-Funktionalität nicht beeinträchtigt.

2. Wie können wir feststellen, welcher Agent die Lizenzserverrolle hostet?

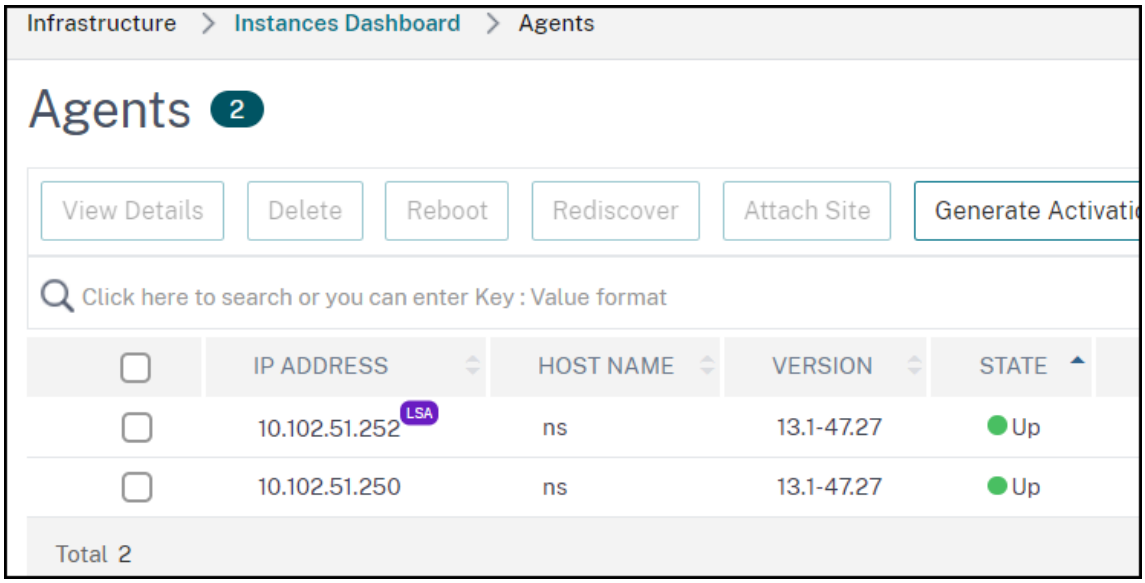
   Antwort: Um zu erfahren, welcher Agent die LSA-Rolle hostet, können Sie den folgenden Befehl in der Shell ausführen:

   ```
   cat /mpsconfig/.lmp/agent
   ```

   Wenn der Ausgabewert für „Rolle“**lsa**ist, hostet dieser Agent die Lizenzserverrolle.

   In der NetScaler Console-GUI wird LSA neben der IP-Adresse des designierten Agents angezeigt.

3. Was passiert, wenn der Agent, der die LSA-Rolle hostet, ausfällt?

   Antwort: Wenn der Agent, der die LSA-Rolle hostet, offline ist, wird für alle bereitgestellten NetScaler-Geräte, die für die Lizenzierung mit gepoolter Kapazität konfiguriert sind, die Kulanzfrist aktiviert. Die Kulanzfrist dauert 30 Tage, und die den NetScaler-Geräten zugewiesenen Ressourcen bleiben während dieses Zeitraums bestehen. NetScaler-Instanzen in diesem Status können die Lizenzzuweisung nicht zuweisen oder ändern, bis der Agent, der die LSA-Rolle hostet, wieder online ist oder ein neuer Agent mit der LSA-Rolle benannt wurde.

4. Wird es eine Wiederwahl geben, wenn der Agent, der die LSA-Rolle hostet, für einen längeren Zeitraum offline geht?

Antwort: Wenn der Administrator innerhalb von 24 Stunden keinen neuen LSA auswählt, wählt der NetScaler Console-Dienst automatisch den nächsten Agent, der aktiv ist, als neuen LSA aus, nachdem der LSA-Agent 24 Stunden ausgefallen ist. Die Kulanzfrist der NetScaler-Geräte endet, nachdem der neue LSA gewählt wurde.

Häufige Probleme

1. Instanzen, die aufgrund von Verbindungsfehlern, Upgrades, Split-Brain usw. im Grace-Modus ausgeführt werden.

   Antwort: Weitere Informationen zum Verhalten des NetScaler Console-Lizenzservers finden Sie unter Konfiguration der NetScaler Pooled-Kapazität.

2. Lizenzen, die keine Instanzen anwenden oder reflektieren.

   Antwort: Weitere Informationen finden Sie unter Problembehandlung bei Lizenzproblemen mit gepoolter Kapazität .

3. Die Lizenzzuweisung befindet sich im ‘‘Sync in Prognose-Bearbeitung’’.

   Antwort: Weitere Informationen finden Sie unter Problembehandlung bei Lizenzproblemen mit gepoolter Kapazität .

4. Fehler aufgrund einer falschen Host-ID in der Lizenzdatei.

   Antwort: Um einen NetScaler Console-Server zu identifizieren, können Sie dem Server einen Hostnamen zuweisen. Der Hostname wird auf der Universallizenz für NetScaler Console angezeigt. Weitere Informationen finden Sie unter Zuweisen eines Hostnamens zu einem NetScaler Console-Server .

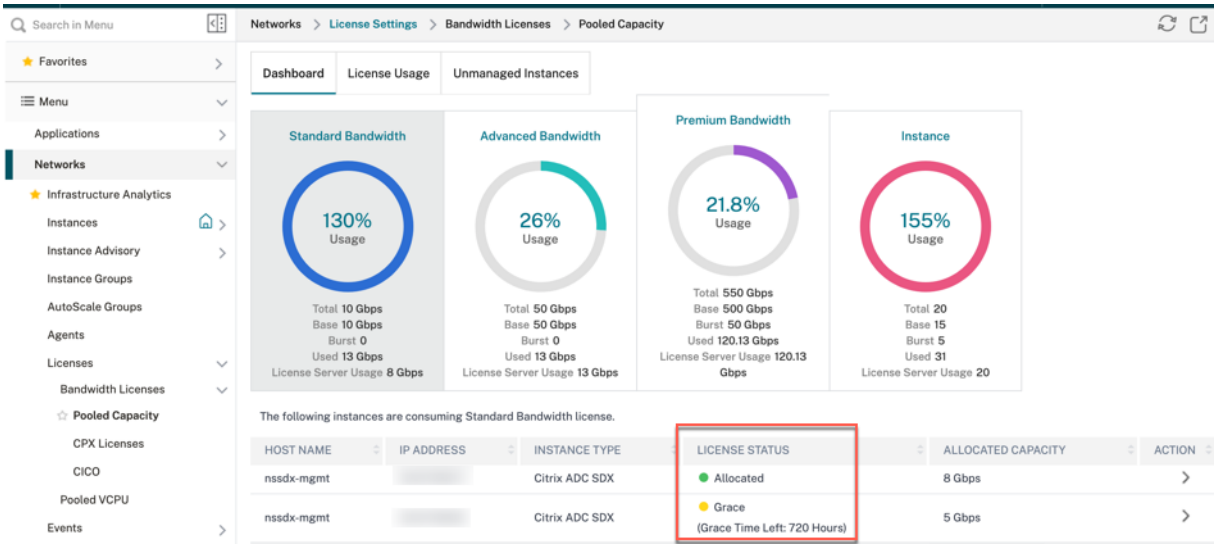
Problembehandlung bei Lizenzproblemen mit gepoolter Kapazität

January 26, 2024

In diesem Abschnitt wird beschrieben, wie häufig auftretende Probleme mit gepoolter Kapazität analysiert und behoben werden.

Überprüfen Sie den Lizenzstatus

Die NetScaler Console fungiert als Lizenzserver für Ihre NetScaler Pooled-Kapazitätslizenz. Sie können die NetScaler Console-GUI verwenden, um den Status der Lizenz zu überprüfen. Navigieren Sie zu **Infrastruktur > Pool-Lizenzierung > Gepoolte Kapazität > Lizenznutzung**.



In der folgenden Tabelle sind die Arten des Lizenzstatus aufgeführt und was sie bedeuten

Status	was es bedeutet
Zugeteilt	Der Lizenzstatus ist in Ordnung.
Zugeteilt: nicht auf NetScaler angewendet	NetScaler erfordert möglicherweise einen Neustart, wenn die Lizenz von NetScaler aus- oder eingecheckt ist, NetScaler jedoch noch nicht neu gestartet wurde.
Nicht zugeteilt	Die Lizenz wird in der NetScaler-Instanz nicht zugewiesen.
Kulanzzeitraum	Die NetScaler-Instanz befindet sich 30 Tage lang in der Kulanzzeit der Lizenz
Synchronisierung wird ausgeführt	NetScaler Console ruft in Intervallen von 2 Minuten Informationen von NetScaler ab. Das Synchronisieren von Lizenzen zwischen NetScaler Console und NetScaler kann bis zu 15 Minuten dauern. Die NetScaler Console wurde möglicherweise neu gestartet oder der NetScaler Console HAS-Failover wird ausgelöst.

Status	was es bedeutet
Teilweise zugeordnet	NetScaler kann die zugewiesene Kapazität nicht akzeptieren, da sie möglicherweise mit ihrer maximalen Zuweisung ausgeführt wird. NetScaler wird beispielsweise mit einer Kapazität von 10 Gbit/s -Lizenzpools ausgeführt. Wenn NetScaler neu gestartet wird, werden die 10 Gbit/s wieder auf den NetScaler Console-Lizenzserver eingecheckt. Wenn NetScaler wieder online kommt, versucht er, die zuvor zugewiesenen 10 Gbit/s automatisch auszuchecken. In der Zwischenzeit haben andere NetScaler-Instanzen diese Bandbreite möglicherweise ausgecheckt. Teilweise zugewiesen wird angezeigt, wenn der Lizenzpool nicht über genügend Kapazität verfügt, um diesem NetScaler vollständige 10 Gbit/s oder sogar einen Teil der Kapazität zuzuweisen.
Nicht verwaltet	NetScaler wurde aus Gründen der Verwaltbarkeit nicht zur NetScaler Console hinzugefügt. Dies hat keine Auswirkungen auf die NetScaler-Lizenzierung, kann sich jedoch auf die Lizenzüberwachung von NetScaler Console aus auswirken.
Nicht verwaltet	NetScaler wurde aus Gründen der Verwaltbarkeit nicht zur NetScaler Console hinzugefügt. Dies hat keine Auswirkungen auf die NetScaler-Lizenzierung, kann sich jedoch auf die Lizenzüberwachung von NetScaler Console aus auswirken.

Status	was es bedeutet
Verbindung unterbrochen	NetScaler ist aus Gründen der Verwaltbarkeit nicht von der NetScaler Console aus erreichbar. Beispielsweise gibt es Netzwerkkonnektivitätsprobleme, NITRO funktioniert nicht oder NetScaler-Kennwörter nicht übereinstimmen. Wenn NITRO nicht funktioniert oder das NetScaler-Kennwort nicht übereinstimmt, hat dies keine Auswirkungen auf die NetScaler-Lizenzierung. Dies kann sich jedoch auf die Lizenzüberwachung von NetScaler Console aus auswirken.

Überprüfen Sie den Serverstatus

In diesem Abschnitt werden die allgemeinen Probleme mit dem Serverstatus und mögliche Gründe und Korrekturen beschrieben.

Problem: NetScaler zeigt den Lizenzserver als nicht erreichbar an und der Lizenzstatus ändert sich in Grace.

- Die Verbindung zum Lizenzserver (NetScaler Console oder Agent) wurde für mehr als 15 Minuten unterbrochen. Überprüfen Sie, ob der Lizenzserver betriebsbereit und erreichbar ist.
- NetScaler befindet sich im Grace-Modus.

Problem: NetScaler zeigt den Lizenzserverstatus als erreichbar an, aber der Versuch des Benutzers, die Zuordnung zu ändern, hat keine Auswirkung. Wenn Sie auf **Zuordnung ändern** klicken, wird 0 0 zurückgegeben Dieser Wert könnte den Anschein erwecken, dass die konfigurierte Kapazität verloren gegangen ist.

- Die Verbindung zum Lizenzserver ist kürzlich unterbrochen worden, aber der NetScaler hat den zweiten Heartbeat immer noch nicht verpasst. Daher ist es (noch) nicht in Grace. Überprüfen Sie, ob der Lizenzserver betriebsbereit und erreichbar ist.

Problem: NetScaler zeigt Kapazität und Anzahl der Instanzen an, aber der Lizenzserver ist **erreichbar/nicht erreichbar**. Wenn Sie auf **Zuordnung ändern** klicken, werden einige Zahlen zurückgegeben, die konfigurierte Kapazität wird jedoch nicht berücksichtigt.

- Die Verbindung zum Lizenzserver wurde wiederhergestellt, aber der NetScaler verpasst immer noch den zweiten Heartbeat oder sendet den Reconnect-Test.

Problem: NetScaler sagt, dass keine Verbindung zum Lizenzserver hergestellt werden kann, wenn die gepoolte Lizenzierung mit NetScaler Console konfiguriert wird

- Überprüfen Sie die Firewallregeln, um sicherzustellen, dass die Ports 27000 und 7279 geöffnet sind.
- Der Agent ist nicht registriert. Weitere Informationen finden Sie unter Erste Schritte.
- NetScaler Console hat keine Lizenzdateien hochgeladen. Weitere Informationen finden Sie unter NetScaler Pooled Capacity konfigurieren
- NetScaler Console hat die falsche Lizenzdatei.

Überprüfen Sie den Nutzungsbericht der Lizenz

Unter **NetScaler Licensing > Pooled Licensing > Bandwidth Licenses > Pooled Capacity > License Usage** in der NetScaler Console GUI können Sie den monatlichen Spitzenwert Ihrer Lizenznutzung sehen. Sie können diesen Bericht verwenden, um Ihre Lizenznutzung zu erhöhen oder den Kauf einer zusätzlichen Lizenz zu planen.

Im Folgenden finden Sie einige Details, wie der Bericht generiert wird und verwendet werden kann.

Polling: Lizenzdaten werden alle 15 Minuten von den NetScaler-Instanzen abgefragt.

Aufrechterhaltung von Spitzenwerten pro Stunde: NetScaler Console behält nur die maximale Lizenznutzung in einer Stunde pro Gerät bei.

** Berichterstattung : Sie können für jede Instanz einen GUI-Bericht für einen bestimmten Zeitraum generieren.

Exportieren: Sie können Berichte entweder im CSV-Format oder im XLS-Format exportieren.

Bereinigen: NetScaler Console löscht Daten am ersten Tag jedes Monats um 12:10 Uhr. Der Löschzeitraum ist konfigurierbar (der Standardzeitraum beträgt zwei Monate).

Zähler und Statistiken für gepoolte Kapazitätslizenzen

Die folgenden Leistungsindikatoren, Protokolle und Befehle enthalten die NetScaler Pooled-Lizenzierungsmetriken, die das Verhalten von NetScaler Console und NetScaler-Instanzen im gepoolten Lizenzierungsmodus angeben.

- **SNMP-Traps**: verfügbar ab NetScaler Version 13.xx.
- **NSCONMSG -Zähler zur Ratenbegrenzung**: verfügbar ab NetScaler Version 12.1 57.xx.
- **NetScaler Console-Zähler**Die Befehlsaktionen der NetScaler Console sind im NetScaler Cloud-Dienst verfügbar.

SNMP-Traps

Sie können die folgenden SNMP-Traps v.13 Pool-Lizenzalarme konfigurieren

- `POOLED-LICENSE-CHECKOUT-FAILURE`
- `POOLED-LICENSE-ONGRACE`
- `Configure POOLED-LICENSE-PARTIAL`

Weitere Informationen zu diesen Alarmen finden Sie unter NetScaler SNMP OID Reference.

NSCONMSG Zähler

Überprüfen Sie die folgenden `NCCONMSG`-Leistungsindikatoren und was sie bedeuten:

- `allnic_err_rl_cpu_pkt_drops`: Aggregat (alle NICs) Paket sinkt, nachdem das CPU-Limit erreicht wurde
- `allnic_err_rl_pps_pkt_drops`: Aggregatpaket fällt systemweit nach pps-Limit
- `allnic_err_rl_rate_pkt_drops`: Aggregatrate sinkt systemweit
- `allnic_err_rl_pkt_drops`: Kumulierte ratenbegrenzende Drops aufgrund von Rate, pps und CPU
- `rl_tot_ssl_rl_enforced`: Anzahl der Male, mit der SSL RL angewendet wurde (bei neuen SSL-Verbindungen)
- `rl_tot_ssl_rl_data_limited`: Häufigkeit, mit der das SSL-Durchsatzlimit erreicht wurde
- `rl_tot_ssl_rl_sess_limited`: Häufigkeit, mit der das SSL-TPS-Limit erreicht wurde

Leistungsindikatoren für NetScaler Console

Wenn Sie die Ereignisaktion „Befehlsaktion ausführen“wählen, können Sie einen Befehl oder ein Skript erstellen, das in der NetScaler Console für Ereignisse ausgeführt werden kann, die einem bestimmten Filterkriterium entsprechen.
Sie können auch die folgenden Parameter für das Skript „ Befehlsaktion ausführen“festlegen:

Parameter	Beschreibung
$source	Dieser Parameter entspricht der Quell-IP-Adresse des empfangenen Ereignisses.
$category	Dieser Parameter entspricht der Art der Traps, die in der Kategorie des Filters definiert sind.

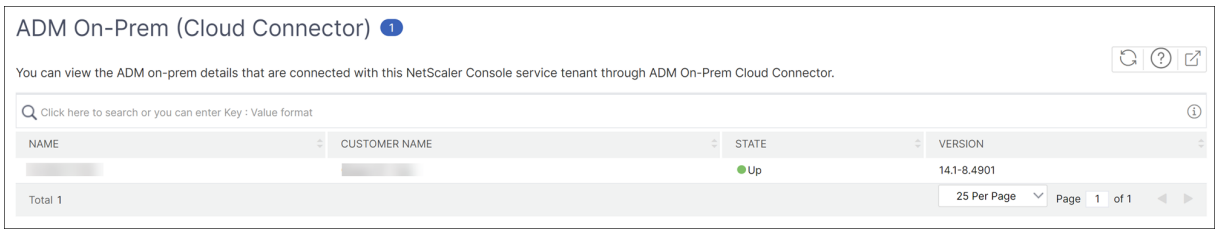
Parameter	Beschreibung
$entity	Dieser Parameter entspricht den Entitätsinstanzen oder Leistungsindikatoren, für die ein Ereignis generiert wurde. Sie kann die Leistungsindikatornamen für alle Ereignisse im Zusammenhang mit dem Schwellenwert, Entitätsnamen für alle entitätsbezogenen Ereignisse und Zertifikatsnamen 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. Dieser Parameter kann verwendet werden, um Probleme schnell aufzuspüren und den Grund für den Ausfall zu identifizieren, anstatt nur Rohereignisse zu melden.

> **Hinweis**
>
> Während der Befehlsausführung werden diese Parameter durch tatsächliche Werte ersetzt.

On-premises Konsoleninstanzen, die mithilfe von Cloud Connect mit dem Konsolendienst verbunden sind

March 12, 2024

Unter **Einstellungen > NetScaler Console On-Prem** können Sie Details der on-premises Console-Instanzen anzeigen, die über Cloud Connect mit dem Console-Dienstmandanten verbunden sind.



- **Name** —Die IP-Adresse der on-premises NetScaler Console
- **Kundenname**—Der Name des NetScaler Console-Dienstmandanten
- **Status** —Der Konnektivitätsstatus zwischen der on-premises NetScaler Console-Instanz und dem NetScaler Console-Dienst
- **Version** —Die Build-Version der on-premises NetScaler Console-Instanz

On-Prem-Upload über die Konsole

July 17, 2024

Diese Seite gilt nur für lokale NetScaler-Benutzer, die den manuellen Modus gewählt haben, um ihre Telemetriedaten in den NetScaler Console-Dienst hochzuladen. Stellen Sie sicher, dass Sie die Telemetriedaten von Ihrer NetScaler Console vor Ort heruntergeladen haben (klicken Sie auf der **NetScaler Telemetrie-Homepage** auf **Telemetrie herunterladen**, um die Bundle-Datei (.tgz) herunterzuladen, die die erforderlichen Telemetriedaten enthält).

So laden Sie Ihre Datentelemetrie in den NetScaler Console-Dienst hoch:

1. Klicken Sie auf der **lokalen Upload-Seite der NetScaler Console** auf **Telemetrie hochladen** und wählen Sie die heruntergeladene Datei (.tgz) aus, um den Upload-Vorgang abzuschließen.
2. Schließen Sie den ersten Upload innerhalb von 30 Tagen ab, nachdem Sie den manuellen Modus ausgewählt haben. Wiederholen Sie den Vorgang und laden Sie die Telemetriedatei danach alle 90 Tage hoch.

> **Hinweise:**
>
> - Der Upload schlägt fehl, wenn die Datei kein gültiges Format (.tgz) hat oder die Datei die Integritätsprüfungen nicht besteht. Es wird empfohlen, den Download erneut durchzuführen und den Upload erneut zu versuchen. Wenn das Problem weiterhin besteht, wenden Sie sich an den Kundendienst.
> - Sie können die optionalen Telemetriedaten deaktivieren. Um dies zu deaktivieren, müssen Sie in NetScaler Console vor Ort zunächst die **Sicherheitsempfehlung** auf der **NetScaler Telemetrieseite** deaktivieren, dann zu **Einstellungen > Administration > Gemeinsame Nutzung der Konsolenfunktion aktivieren oder deaktivieren** und das Kontrollkästchen **Ich stimme zu, die Nutzungsdaten der Konsolenfunktion zu teilen**, deaktivieren.

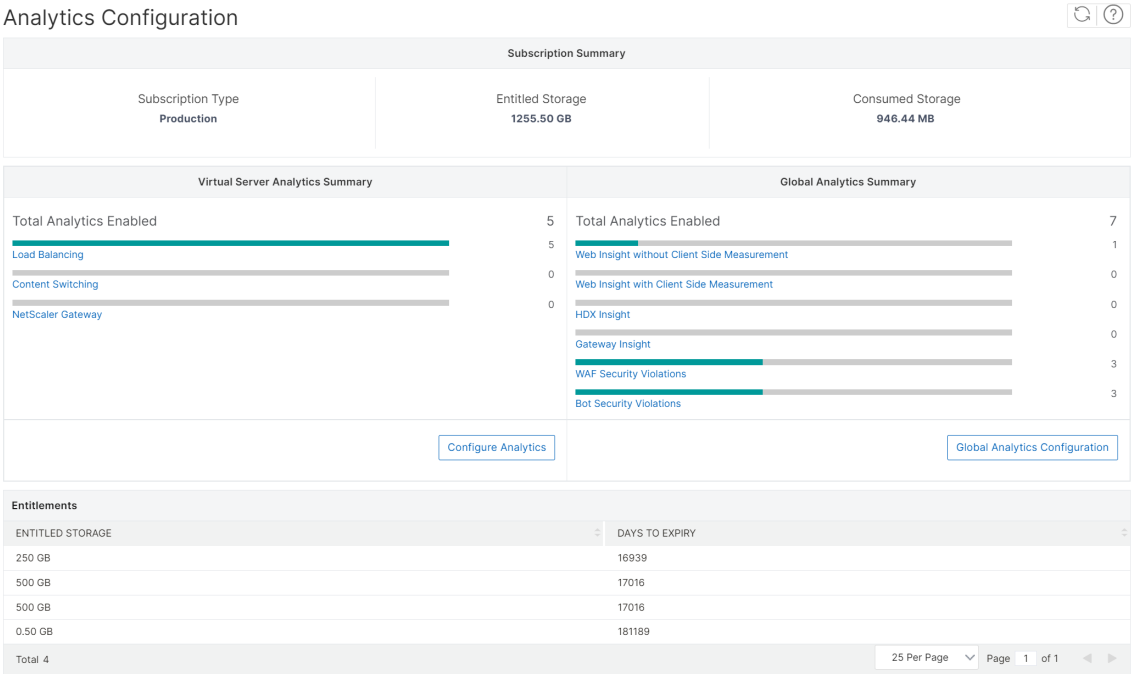
Analytik auf virtuellen Servern konfigurieren

March 12, 2024

Ab Build 14.1-21.x werden alle erkannten 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 es Ihnen, Analysen auf den erkannten virtuellen Servern zu konfigurieren.
- **Globale Analyseübersicht** —Ermöglicht die Konfiguration von Analysen sowohl auf erkannten als auch auf nachfolgenden virtuellen Servern.



Analytik auf den erkannten 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 **Security & 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.
> 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 **Security & Analytics aktivieren**.
> ```

3. Gehen Sie im Fenster **Enable Security & 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 Console, um Analysen auf den ausgewählten virtuellen Servern zu aktivieren.

> **Hinweis**
>
> NetScaler Console verwendet NetScaler SNIP für Logstream und NSIP für IPFIX . Wenn zwischen NetScaler Agent und NetScaler-Instanz eine Firewall aktiviert ist, stellen Sie sicher, dass Sie den folgenden Port öffnen, damit NetScaler Console AppFlow-Datenverkehr 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 **Security & Analytics bearbeiten**.
   > ```

2. Klicken Sie auf **Sicherheit und Analytik 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** .

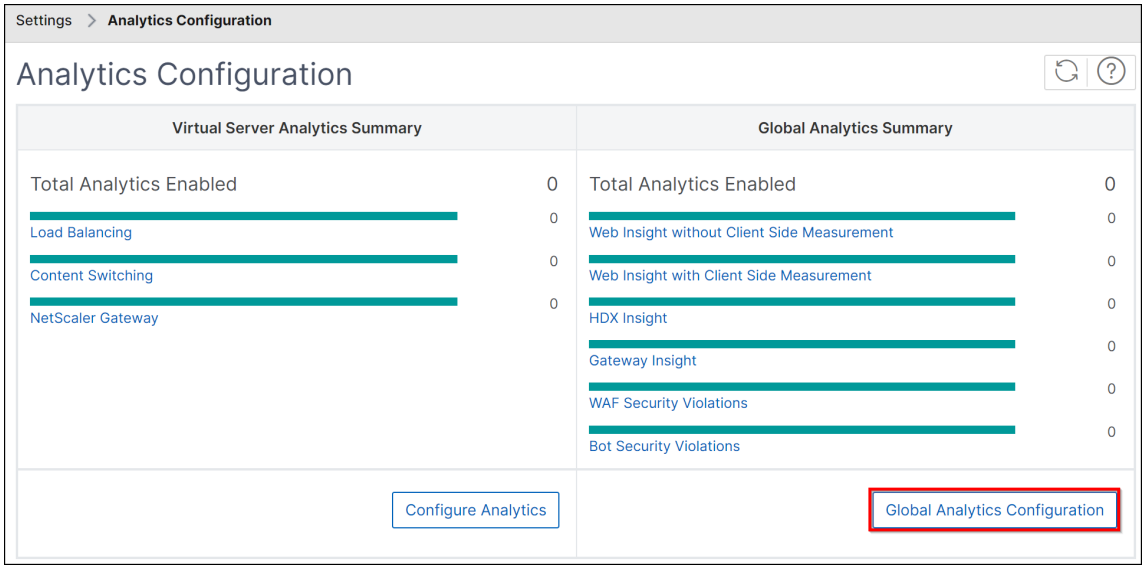
NetScaler Console deaktiviert die Analysen auf den ausgewählten virtuellen Servern.

In der folgenden Tabelle werden die Funktionen der NetScaler Console beschrieben, die IPFIX und Logstream als Transportmodus unterstützt:

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 erkannten 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 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.
- Stellen Sie sich vor, Sie haben 10 virtuelle Server und Sie haben Analysen für zwei virtuelle Server manuell deaktiviert. 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.

Konfiguration der rollenbasierten Zugriffskontrolle

March 12, 2024

NetScaler Console bietet eine detaillierte, rollenbasierte Zugriffskontrolle (RBAC), mit der Sie Zugriffsberechtigungen auf der Grundlage der Rollen einzelner Benutzer in Ihrem Unternehmen gewähren können.

In NetScaler Console werden alle Benutzer in Citrix Cloud hinzugefügt. Als erster Benutzer Ihrer Organisation müssen Sie zuerst ein Konto in Citrix Cloud erstellen und sich dann mit den Citrix Cloud-Anmeldeinformationen an der NetScaler Console-GUI anmelden. Ihnen wird die Superadmin-Rolle zugewiesen, und standardmäßig verfügen Sie über alle Zugriffsberechtigungen in NetScaler Console. Später können Sie andere Benutzer in Ihrer Organisation in Citrix Cloud erstellen.

Benutzer, die später erstellt werden und sich als reguläre Benutzer bei NetScaler Console anmelden, werden als delegierte Administratoren bezeichnet. Diese Benutzer haben standardmäßig alle Berechtigungen außer Benutzeradministrationsberechtigungen. Sie können jedoch bestimmten Benutzerverwaltungsberechtigungen gewähren, indem Sie entsprechende Richtlinien erstellen und sie diesen delegierten Benutzern zuweisen. Die Benutzeradministrationsberechtigungen befinden sich unter **Einstellungen** > **Benutzer und Rollen**.

Weitere Informationen zum Zuweisen bestimmter Berechtigungen finden Sie unter So weisen Sie delegierten Administratorbenutzern zusätzliche Berechtigungen zu.

Weitere Informationen zum Erstellen von Richtlinien, Rollen und Gruppen sowie zum Binden der Benutzer an Gruppen finden Sie in den folgenden Abschnitten.

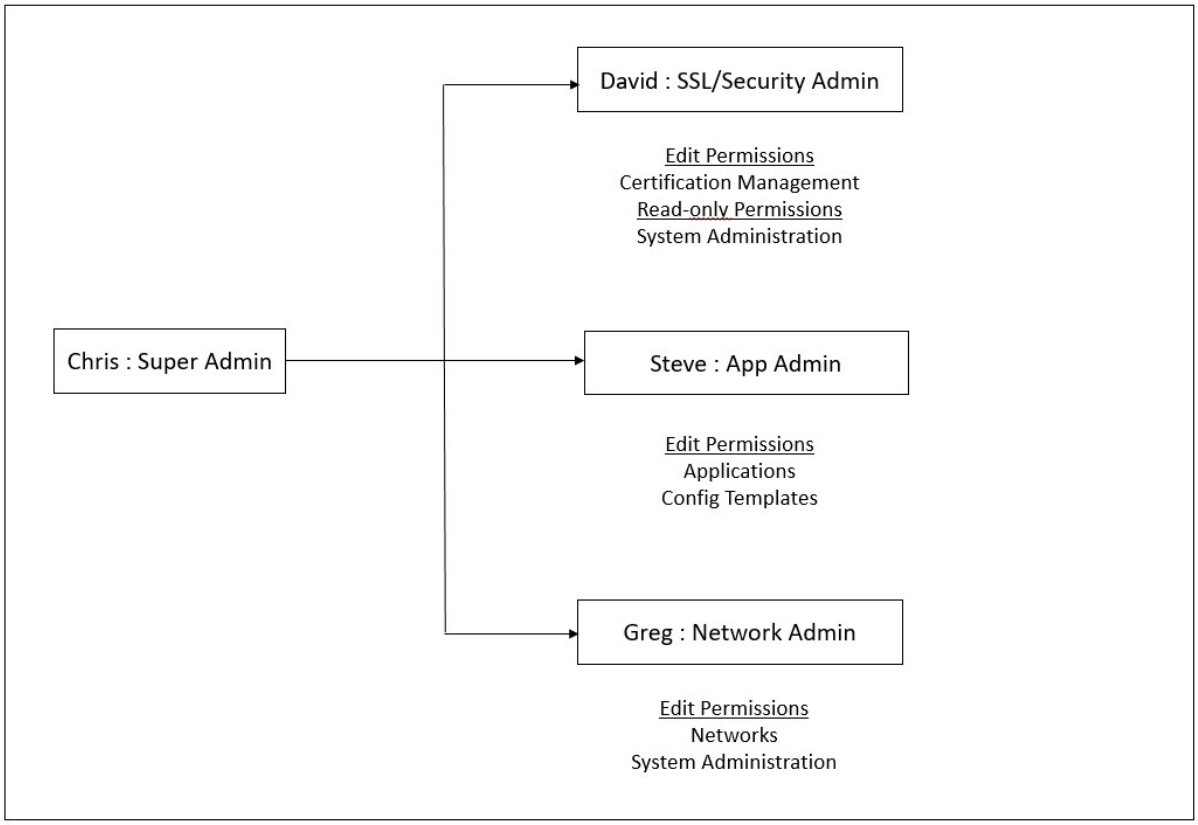
Beispiel:

Das folgende Beispiel veranschaulicht, wie RBAC in NetScaler Console erreicht werden kann.

Chris, der NetScaler-Gruppenleiter, ist der Superadministrator von NetScaler Console in seiner Organisation. Er erstellt drei Administratorrollen: Sicherheitsadministrator, Anwendungsadministrator und Netzwerkadministrator.

- David, der Sicherheitsadministrator, muss über vollständigen Zugriff auf die Verwaltung und Überwachung von SSL-Zertifikaten verfügen, muss jedoch über schreibgeschützten Zugriff für den Systemverwaltungsbetrieb verfügen.
- Steve, ein Anwendungsadministrator, benötigt nur Zugriff auf bestimmte Anwendungen und nur bestimmte Konfigurationsvorlagen.
- Greg, ein Netzwerkadministrator, benötigt Zugriff auf System- und Netzwerkadministration.
- Chris muss auch RBAC für alle Benutzer bereitstellen, unabhängig davon, dass sie lokal oder extern sind.

Das folgende Bild zeigt die Berechtigungen, die Administratoren und andere Benutzer haben und ihre Rollen in der Organisation.



Um seinen Benutzern eine rollenbasierte Zugriffskontrolle zu bieten, muss Chris zuerst Benutzer in Citrix Cloud hinzufügen und erst danach kann er die Benutzer in NetScaler Console sehen. Chris muss je nach Rolle Zugriffsrichtlinien für jeden Benutzer erstellen. Zugriffsrichtlinien sind eng an Rollen gebunden. Chris muss also auch Rollen erstellen, und dann muss er Gruppen erstellen, da Rollen nur Gruppen und nicht einzelnen Benutzern zugewiesen werden können.

Zugriff ist die Fähigkeit, eine bestimmte Aufgabe auszuführen, z. B. eine Datei anzuzeigen, zu erstellen, zu ändern oder zu löschen. Rollen werden entsprechend der Autorität und Verantwortung der Benutzer innerhalb des Unternehmens definiert. Beispielsweise kann ein Benutzer alle Netzwerkoperationen ausführen, während ein anderer Benutzer den Verkehrsfluss in Anwendungen beobachten und beim Erstellen von Konfigurationsvorlagen helfen kann.

Richtlinien bestimmen die Benutzerrollen. Nach dem Erstellen von Richtlinien können Sie Rollen erstellen, jede Rolle an eine oder mehrere Richtlinien binden und Benutzern Rollen zuweisen. Sie können auch Benutzergruppen Rollen zuweisen. Eine Gruppe ist eine Sammlung von Benutzern, die über gemeinsame Berechtigungen verfügen. Beispielsweise können Benutzer, die ein bestimmtes Rechenzentrum verwalten, einer Gruppe zugewiesen werden. Eine Rolle ist eine Identität, die Benutzern gewährt wird, indem sie bestimmten Gruppen basierend auf bestimmten Bedingungen hinzugefügt werden. In NetScaler Console 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. Anwendungsadministratoren können nur auf die Ressourcen in ihrem Geltungsbereich zugreifen.

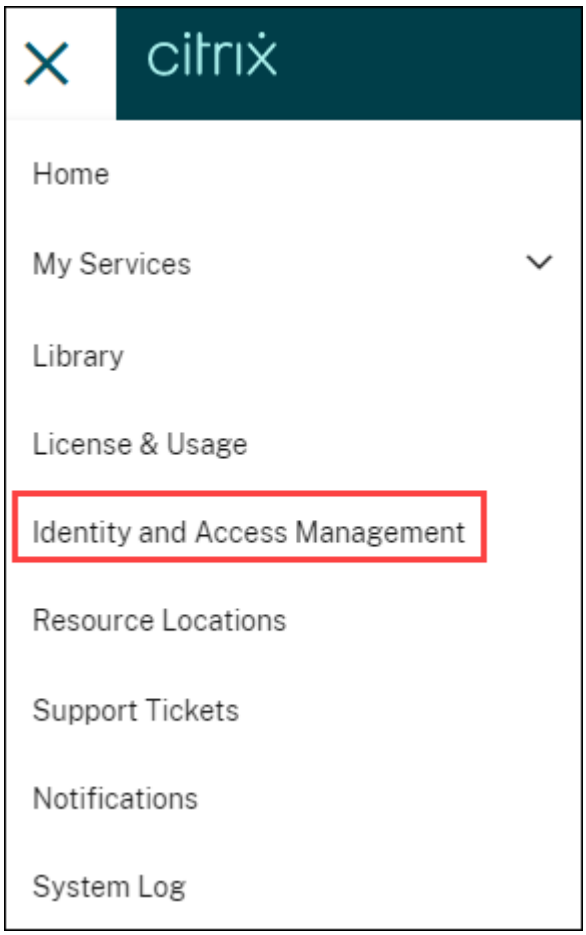
Führen Sie daher in Ihrer Rolle als Chris, der Superadmin, die folgenden Beispielaufgaben in NetScaler Console aus, um Zugriffsrichtlinien, Rollen und Benutzergruppen für David, den Sicherheitsadministrator in Ihrer Organisation, zu konfigurieren.

Benutzer auf der NetScaler Console konfigurieren

Als Superadmin können Sie mehr Benutzer erstellen, indem Sie Konten für sie in Citrix Cloud und nicht in NetScaler Console konfigurieren. Wenn die neuen Benutzer zur NetScaler Console hinzugefügt werden, können Sie ihre Berechtigungen nur definieren, indem Sie dem Benutzer die entsprechenden Gruppen zuweisen.

So fügen Sie neue Benutzer in Citrix Cloud hinzu:

1. Klicken Sie in der NetScaler Console-GUI oben links auf das Hamburger-Symbol und wählen Sie **Identity and Access Management** aus.

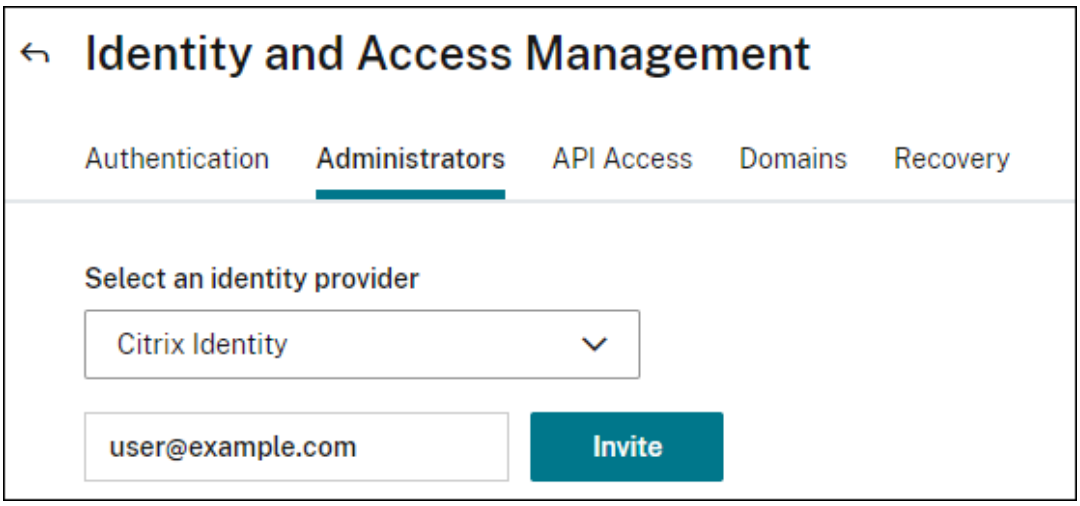


2. Wählen Sie auf der Seite Identitäts- und Zugriffsmanagement die Registerkarte **Administratoren** aus.

   Auf dieser Registerkarte werden die Benutzer aufgeführt, die in Citrix Cloud erstellt wurden.

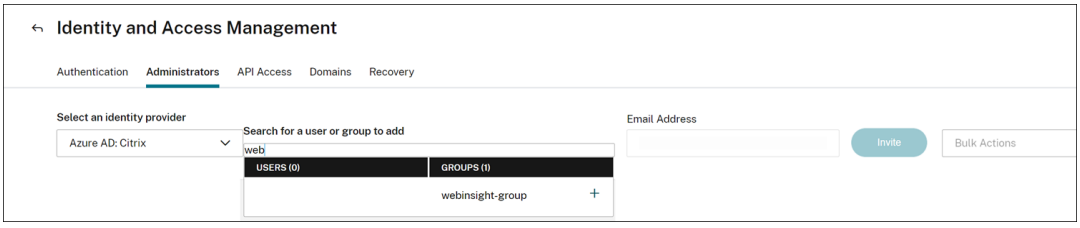
3. Wählen Sie den Identitätsanbieter aus der Liste aus.

   - **Citrix Identity**: Geben Sie die E-Mail-Adresse des Benutzers ein, den Sie in NetScaler Console hinzufügen möchten, und klicken Sie auf **Einladen**.



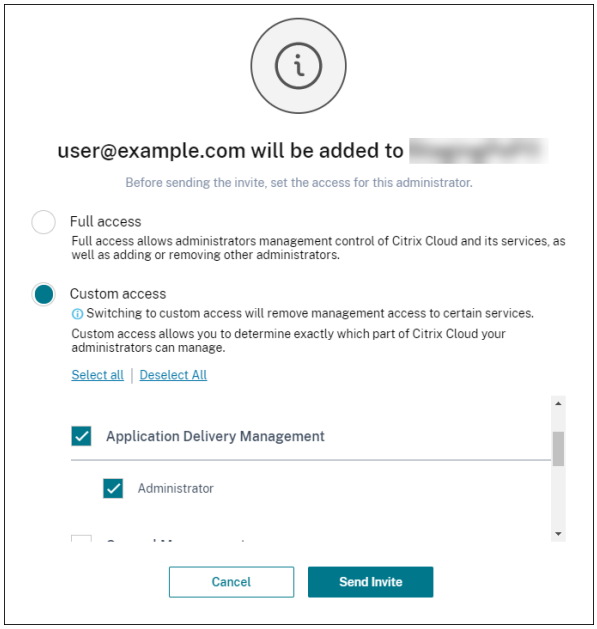
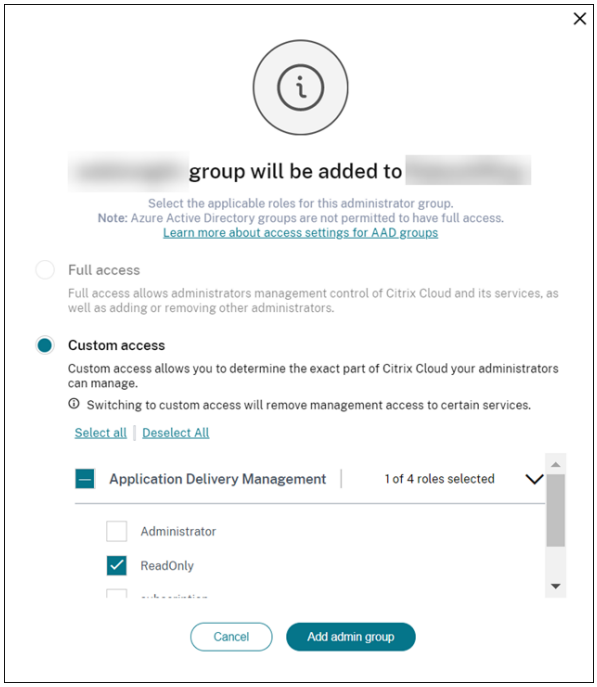
> **Hinweis:**
>
> Der Benutzer erhält eine E-Mail-Einladung von Citrix Cloud. Der Benutzer muss auf den Link in der E-Mail klicken, um den Registrierungsvorgang abzuschließen, indem er seinen vollständigen Namen und sein Kennwort angibt. Später muss er sich mit seinen Anmeldeinformationen bei NetScaler Console anmelden.

- **Azure Active Directory (AD)**: Diese Option wird nur angezeigt, wenn Ihr Azure AD mit Citrix Cloud verbunden ist. Weitere Informationen finden Sie unter Verbinden von Azure Active Directory mit Citrix Cloud. Wenn Sie diese Option auswählen, um Benutzer oder Gruppen einzuladen, können Sie nur **Benutzerdefinierten Zugriff** für den ausgewählten Benutzer oder die ausgewählte Gruppe angeben. Die Benutzer können sich mit ihren Azure AD-Anmeldeinformationen bei NetScaler Console anmelden. Außerdem müssen Sie keine Citrix Identity für die Benutzer erstellen, die Teil des ausgewählten Azure AD sind. Wenn ein Benutzer zur eingeladenen Gruppe hinzugefügt wird, müssen Sie keine Einladung für den neu hinzugefügten Benutzer senden. Dieser Benutzer kann mit den Azure AD-Anmeldeinformationen auf NetScaler Console zugreifen.



4. Wählen Sie **Benutzerdefinierter Zugriff** für den angegebenen Benutzer oder die angegebene Gruppe.
5. Wählen Sie **Management für die Anwendungsbereitstellung**aus.

   Diese Option listet die in NetScaler Console erstellten Benutzergruppen auf. Wählen Sie die Gruppe aus, zu der Sie den Benutzer hinzufügen möchten.

Citrix-Identität	Azure AD
	
Klicken Sie auf **Einladung senden**.	Klicken Sie auf **Admin-Gruppe**hinzufügen.

Als Administrator sehen Sie den neuen Benutzer erst in der NetScaler Console-Benutzerliste, nachdem sich der Benutzer bei NetScaler Console angemeldet hat.

So konfigurieren Sie Benutzer in NetScaler Console:

1. Navigieren Sie in der NetScaler Console-GUI zu **Einstellungen** > **Benutzer und Rollen** > **Benutzer**.
2. Der Benutzer wird auf der Seite **Benutzer** angezeigt.
3. Sie können die Berechtigungen bearbeiten, die dem Benutzer zur Verfügung gestellt werden, indem Sie den Benutzer auswählen und auf **Bearbeiten**klicken. Sie können Gruppenberechtigungen auch auf der Seite **Gruppen** unter dem Knoten **Einstellungen** bearbeiten.

   > **Hinweis:**
   >
   > - Die Benutzer werden in NetScaler Console nur aus der Citrix Cloud hinzugefügt. Daher können Sie in der NetScaler Console-GUI keine Benutzer hinzufügen oder löschen, obwohl Sie über Administratorberechtigungen verfügen. Sie können nur die Gruppenberechtigungen bearbeiten. Benutzer können in der Citrix Cloud hinzugefügt oder gelöscht werden.

> • Die Benutzerdetails werden erst auf der Service-GUI angezeigt, nachdem sich der Benutzer mindestens einmal an der NetScaler Console angemeldet hat.

Konfigurieren Sie Zugriffsrichtlinien auf der NetScaler Console

Zugriffsrichtlinien definieren Berechtigungen. Eine Richtlinie kann auf eine Benutzergruppe oder auf mehrere Gruppen angewendet werden, indem Rollen erstellt werden. Richtlinien bestimmen die Benutzerrollen. Nach dem Erstellen von Richtlinien müssen Sie Rollen erstellen, jede Rolle an eine oder mehrere Richtlinien binden und Benutzergruppen Rollen zuweisen. NetScaler Console bietet fünf vordefinierte Zugriffsrichtlinien:

- **admin_policy**. Gewährt Zugriff auf alle NetScaler Console-Knoten. Der Benutzer hat sowohl Anzeige- als auch Bearbeitungsberechtigungen, kann den gesamten NetScaler Console-Inhalt anzeigen und alle Bearbeitungsvorgänge ausführen. Das heißt, der Benutzer kann Vorgänge für die Ressourcen hinzufügen, ändern und löschen.
- **adminExceptSystem_policy**. Gewährt Benutzern Zugriff auf alle Knoten in der NetScaler Console-GUI, mit Ausnahme des Zugriffs auf den Knoten „Einstellungen“.
- **readonly_policy**. Gewährt schreibgeschützte Berechtigungen. Der Benutzer kann den gesamten Inhalt auf der NetScaler Console anzeigen, ist jedoch nicht berechtigt, Operationen auszuführen.
- **appadmin_policy**. Gewährt Administratorberechtigungen für den Zugriff auf die Anwendungsfunktionen in NetScaler Console. Ein Benutzer, der an diese Richtlinie gebunden ist, kann:
  - Benutzerdefinierte Anwendungen hinzufügen, ändern und löschen
  - Aktivieren oder deaktivieren Sie Dienste, Dienstgruppen und die verschiedenen virtuellen Server, z. B. Content Switching und Cache-Umleitung
- **appreadonly_policy**. 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.

Obwohl Sie diese vordefinierten Richtlinien nicht bearbeiten können, können Sie eigene (benutzerdefinierte) Richtlinien erstellen.

Wenn Sie zuvor Rollen Richtlinien zugewiesen und die Rollen an Benutzergruppen gebunden haben, können Sie Berechtigungen für die Benutzergruppen auf Knotenebene in der NetScaler Console-GUI bereitstellen. Beispielsweise können Sie nur Zugriffsberechtigungen für den gesamten **Load Balancing-Knoten** bereitstellen. Ihre Benutzer waren berechtigt, auf alle entitätsspezifischen Unterknoten unter **Load Balancing** zuzugreifen (z. B. virtuelle Server, Dienste und andere), oder sie hatten keine Berechtigung, auf einen Knoten unter **Load Balancing** zuzugreifen.

In NetScaler Console 507.x Build und späteren Versionen wurde das Zugriffsrichtlinienmanagement erweitert, um auch Berechtigungen für Unterknoten bereitzustellen. Zugriffsrichtlinieneinstellungen

können für alle Unterknoten wie virtuelle Server, Dienste, Dienstgruppen und Server konfiguriert werden.

Derzeit können Sie eine solche granulare Zugriffsberechtigung nur für Unterknoten unter einem **Load Balancing-Knoten** und auch für Unterknoten unter dem **GSLB**-Knoten bereitstellen.

Als Administrator möchten Sie dem Benutzer beispielsweise möglicherweise nur eine Zugriffsberechtigung geben, um virtuelle Server anzuzeigen, nicht jedoch die Back-End-Dienste, Dienstgruppen und Anwendungsserver im **Load Balancing-Knoten** . Die Benutzer, denen eine solche Richtlinie zugewiesen ist, können nur auf die virtuellen Server zugreifen.

So erstellen Sie benutzerdefinierte Zugriffsrichtlinien:

1. ****Navigieren Sie in der NetScaler Console-GUI zu **Einstellungen** > **Benutzer und Rollen** > Zugriffsrichtlinien .
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **Zugriffsrichtlinien erstellen** im Feld **Richtlinienname** den Namen der Richtlinie und die Beschreibung in das Feld **Richtlinienbeschreibung** ein.

   Im Abschnitt „ **Berechtigungen** “sind alle Funktionen der NetScaler Console mit Optionen zum Angeben von Schreibschutz, Aktivieren/Deaktivieren oder Bearbeiten aufgeführt.

   a) Klicken Sie auf das Symbol (+), um jede Funktionsgruppe in viele Funktionen zu erweitern.

   b) Aktivieren Sie das Berechtigungskästchen neben dem Funktionsnamen, um den Benutzern die Berechtigung zu erteilen.

      - **Ansicht:**Mit dieser Option kann der Benutzer die Funktion in NetScaler Console anzeigen.
      - ** Aktivieren-Deaktivieren: **Diese Option ist nur für die Netzwerkfunktions-Funktionen verfügbar, mit denen Aktionen in der NetScaler Console aktiviert oder deaktiviert werden können. Der Benutzer kann die Funktion aktivieren oder deaktivieren. 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.

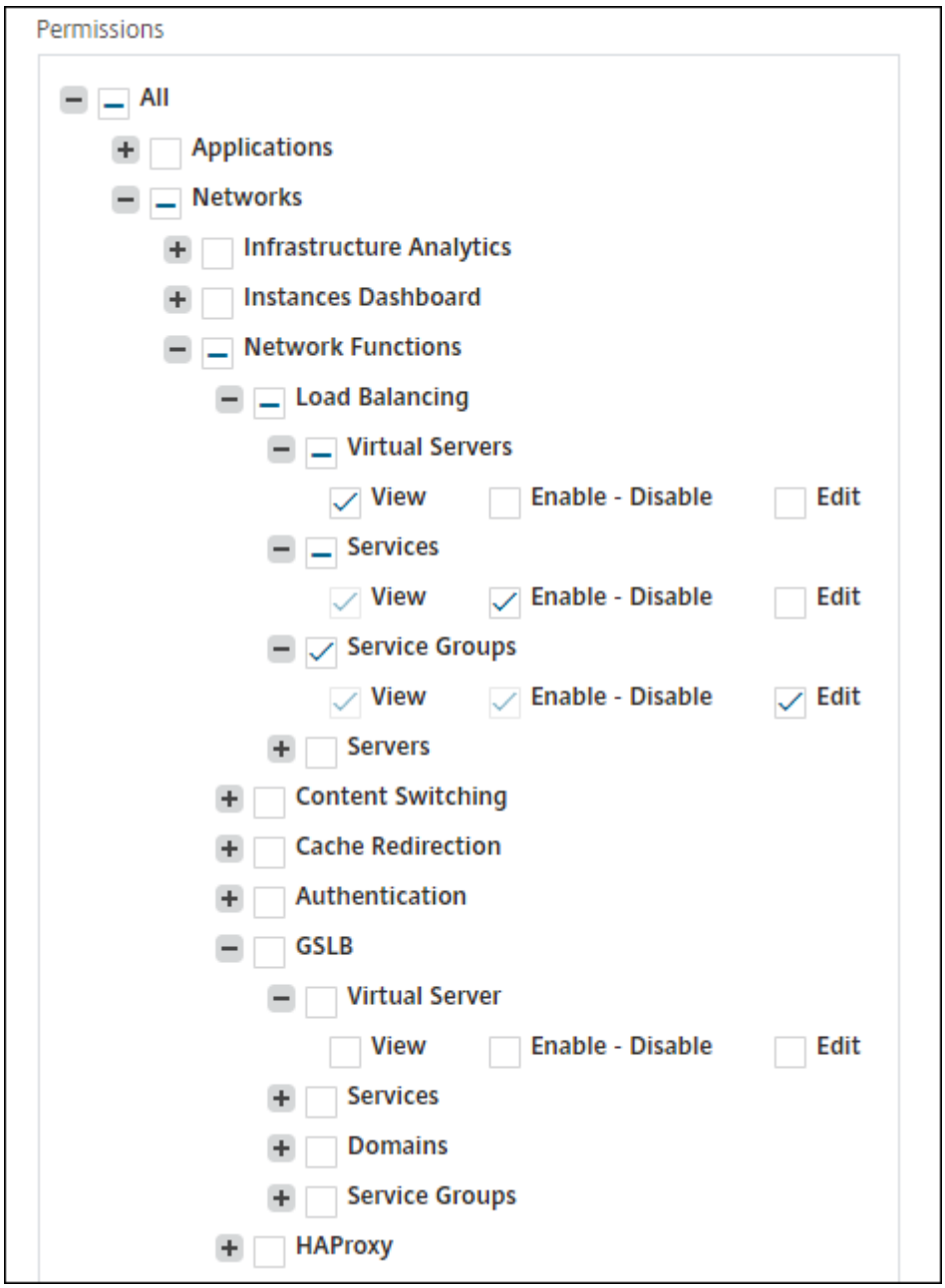
      - **Bearbeiten:** Diese Option gewährt dem Benutzer vollen Zugriff. Der Benutzer kann das Feature und seine Funktionen ändern.

        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 Funktionsfeld auswählen, 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. Der Benutzer kann die virtuellen Lastausgleichsserver in der NetScaler Console 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. Der Benutzer kann die Dienste aktivieren oder deaktivieren, die an einen virtuellen Lastausgleichsserver gebunden sind. Außerdem kann der Benutzer eine **Jetzt abfragen**-Aktion für Dienste ausführen. Um Dienste zu aktivieren oder zu deaktivieren, navigieren Sie zu **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.

4. Klicken Sie auf **Erstellen**.

> **Hinweis:**
>
> Wenn Sie **Bearbeiten** auswählen, können intern abhängige Berechtigungen zugewiesen werden, die im Abschnitt Berechtigungen nicht als aktiviert angezeigt werden. Wenn Sie beispielsweise Bearbeitungsberechtigungen für das Fehlermanagement aktivieren, erteilt NetScaler Console intern die Berechtigung zum Konfigurieren eines E-Mail-Profils oder zum Erstellen von SMTP-Server-Setups, sodass der Benutzer den Bericht als E-Mail senden kann.

Erteilen von StyleBook-Berechtigungen für Benutzer

Sie können eine Zugriffsrichtlinie erstellen, um StyleBook-Berechtigungen wie Importieren, Löschen, Herunterladen und mehr zu erteilen.

> **Hinweis:**
>
> Die View-Berechtigung wird automatisch aktiviert, wenn Sie andere StyleBook-Berechtigungen gewähren.

Rollen auf der NetScaler Console konfigurieren

In NetScaler Console 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 gewährt möglicherweise die Erlaubnis, NetScaler-Instanzen in der NetScaler Console hinzuzufügen, und die andere Richtlinie erteilt möglicherweise die Erlaubnis, ein StyleBook zu erstellen und bereitzustellen und NetScaler-Instanzen zu konfigurieren.

Wenn mehrere Richtlinien die Bearbeitungs- und Schreibschutzberechtigungen für ein einzelnes Feature definieren, haben die Bearbeitungsberechtigungen Priorität gegenüber schreibgeschützten Berechtigungen.

NetScaler Console bietet fünf vordefinierte Rollen:

- **admin_role**. Hat Zugriff auf alle NetScaler Console-Funktionen. (Diese Rolle ist gebunden an `adminpolicy`.)
- **adminExceptSystem_role**. Hat Zugriff auf die NetScaler Console-GUI mit Ausnahme der Einstellungsberechtigungen. (Diese Rolle ist an adminExceptSystem_policy gebunden)
- **readonly_role**. Schreibgeschützter Zugriff. (Diese Rolle ist gebunden an `readonlypolicy`.)
- **appAdmin_role**. Hat nur Administratorzugriff auf die Anwendungsfunktionen in NetScaler Console. (Diese Rolle ist an appAdminPolicy gebunden).
- **appReadonly_role**. Hat nur Lesezugriff auf die Anwendungsfunktionen. (Diese Rolle ist an appReadOnlyPolicy gebunden.)

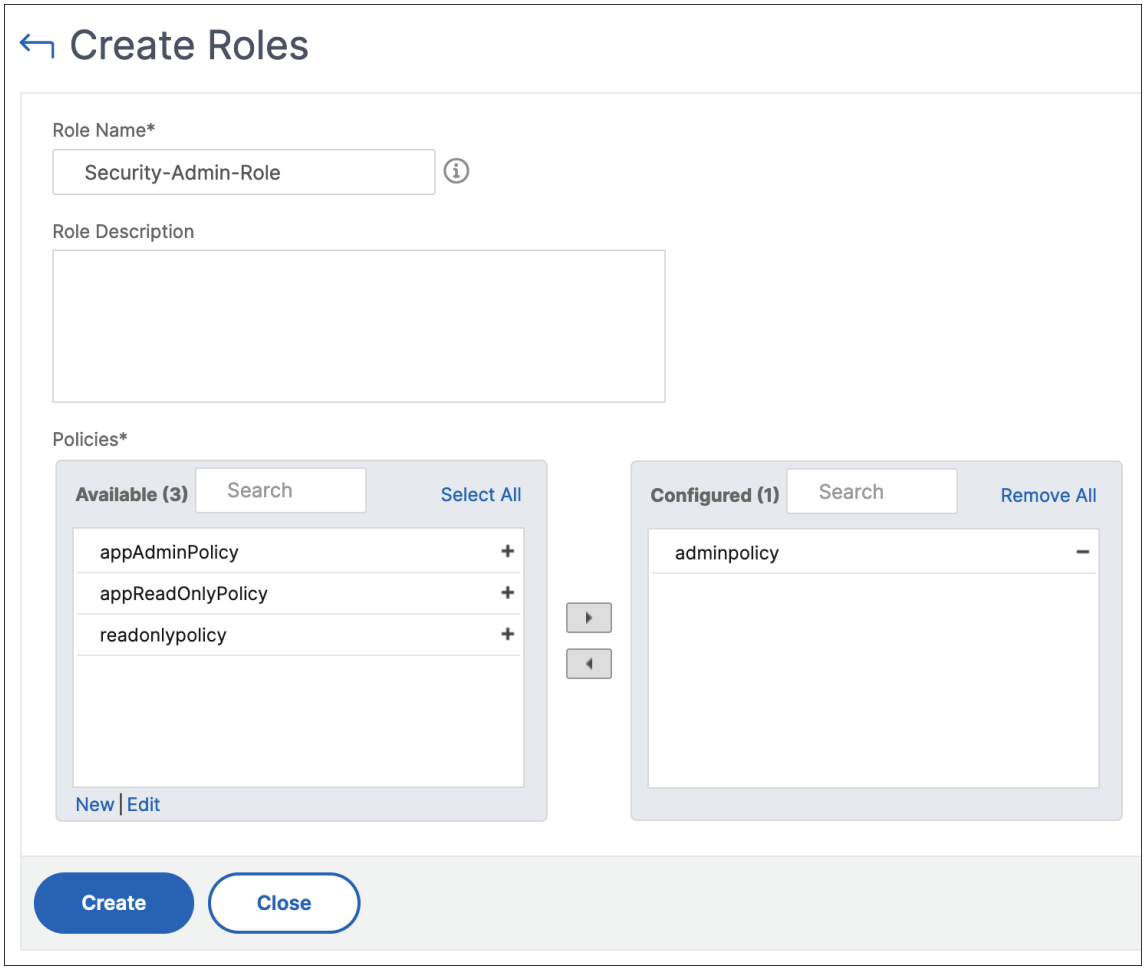
Sie können die vordefinierten Rollen zwar nicht bearbeiten, aber Sie können Ihre eigenen (benutzerdefinierten) Rollen erstellen.

So erstellen Sie Rollen und weisen ihnen Richtlinien zu:

1. Navigieren Sie in der NetScaler Console-GUI zu **Einstellungen** > **Benutzer und Rollen** > **Rollen** .
2. Klicken Sie auf **Hinzufügen**.

3. Geben **Sie auf der Seite Rollen erstellen** im Feld **Rollenname** den Namen der Rolle ein und geben Sie die Beschreibung in das Feld **Rollenbeschreibung** ein (optional).
4. Fügen Sie im Abschnitt **Richtlinien** eine oder mehrere Richtlinien zur Liste **Konfiguriert** hinzu.

> **Hinweis:**
>
> Den Richtlinien wird eine Mandanten-ID vorangestellt (z. B. `maasdocfour`), die für alle Mandanten eindeutig ist.



> **Hinweis:**
>
> ****Sie können eine Zugriffsrichtlinie erstellen, indem Sie auf **Neu** klicken, oder Sie können zu **Einstellungen** > **Benutzer und Rollen** > Zugriffsrichtlinien navigieren und Richtlinien erstellen.

5. Klicken Sie auf **Erstellen**.

Gruppen auf der NetScaler Console konfigurieren

In NetScaler Console kann eine Gruppe sowohl Zugriff auf Funktionsebene als auch auf Ressourcenebene haben. 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 Console dieselben Zugriffsrechte zugewiesen.

Sie können den Benutzerzugriff in NetScaler Console auf der einzelnen Ebene der Netzwerkfunktionsentitäten verwalten. Sie können dem Benutzer oder der Gruppe auf Entitätsebene dynamisch bestimmte Berechtigungen zuweisen.

NetScaler Console behandelt virtuelle Server, Dienste, Dienstgruppen und Server als Netzwerkfunktionsentitäten.

- **Virtueller Server (Anwendungen)** - Load Balancing (`lb`), GSLB, Context Switching (`CS`), Cache-Umleitung (`CR`), Authentifizierung (`Auth`) und NetScaler Gateway (`vpn`)
- **Services** - Lastenausgleich und GSLB-Dienste
- **Servicegruppe** —Lastenausgleich und GSLB-Dienstgruppen
- **Server** —Load Balancing-Server

So erstellen Sie eine Gruppe:

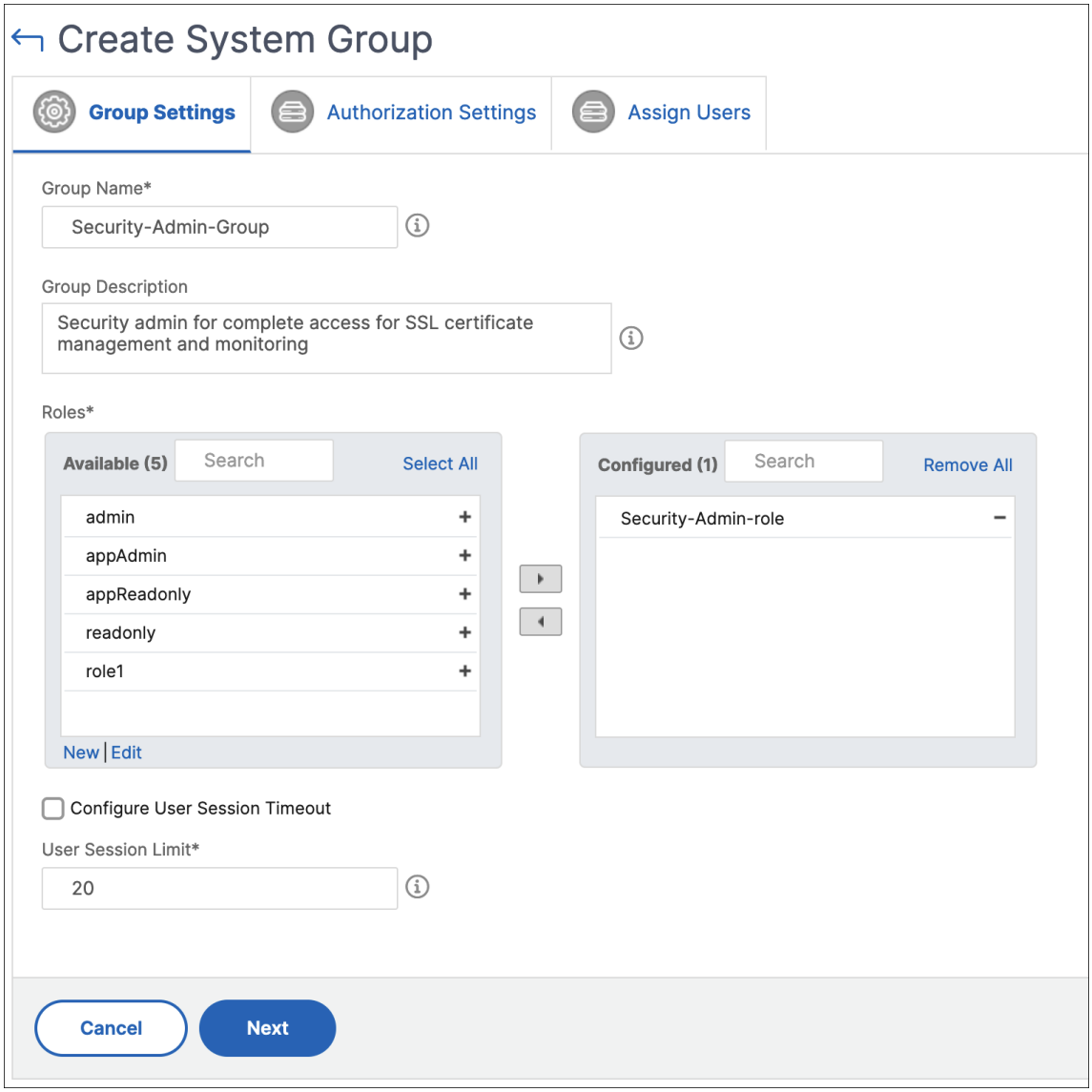
1. Navigieren Sie in der NetScaler Console zu **Einstellungen** > **Benutzer und Rollen** > **Gruppen** .
2. Klicken Sie auf **Hinzufügen**.

   Die Seite **Systemgruppe erstellen** wird angezeigt.
3. Geben Sie im Feld **Gruppenname** den Namen der Gruppe ein.
4. Geben Sie im Feld **Gruppenbeschreibung** eine Beschreibung Ihrer Gruppe ein. Eine gute Beschreibung hilft Ihnen, die Rolle und Funktion der Gruppe zu verstehen.
5. Verschieben Sie im Abschnitt **Rollen** eine oder mehrere Rollen in die Liste **Konfiguriert** .

   > **Hinweis:**
   >
   > Den Rollen wird eine Mandanten-ID vorangestellt (z. B. `maasdocfour`), die für alle Mandanten eindeutig ist.

6. In der Liste **Verfügbar** können Sie auf **Neu** oder **Bearbeiten** klicken und Rollen erstellen oder ändern.

   Alternativ können Sie zu **Einstellungen > Benutzer und Rollen > Benutzer**navigieren und Benutzer erstellen oder ändern.



7. Klicken Sie auf **Weiter**.
8. Auf der Registerkarte **Autorisierungseinstellungen** können Sie Ressourcen aus den folgenden Kategorien auswählen:

   - **Autoscale-Gruppen**
   - **Instanzen**
   - **Anwendungen**
   - **Konfigurationsvorlagen**
   - **IPAM-Anbieter und Netzwerke**
   - **StyleBooks**
   - **Konfigurationspakete**
   - **Domänennamen**

Wählen Sie bestimmte Ressourcen aus den Kategorien aus, auf die Benutzer Zugriff haben können.

Autoscale-Gruppen:

So wählen Sie die spezifischen Autoscale-Gruppen aus, die ein Benutzer anzeigen oder verwalten kann:

a) Deaktivieren Sie das Kontrollkästchen **Alle AutoScale-Gruppen** und klicken Sie auf **AutoScale-Gruppen hinzufügen**.

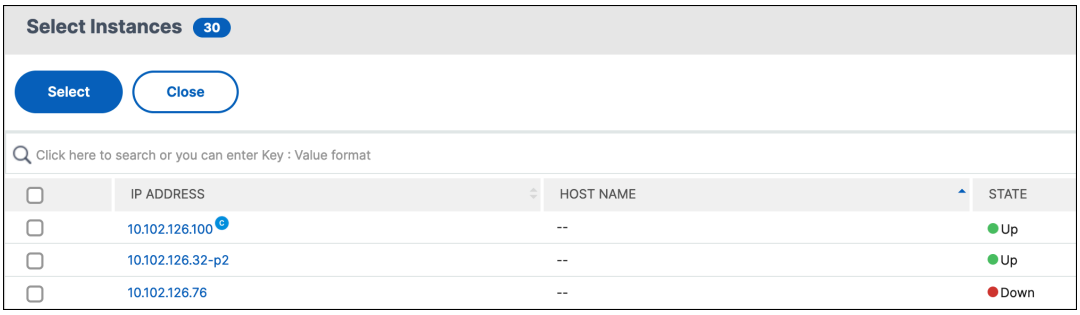
b) Wählen Sie die erforderlichen Autoscale-Gruppen aus der Liste aus, und klicken Sie auf **OK**.

Instanzen:

So wählen Sie die spezifischen Instanzen aus, die ein Benutzer anzeigen oder verwalten kann:

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**.

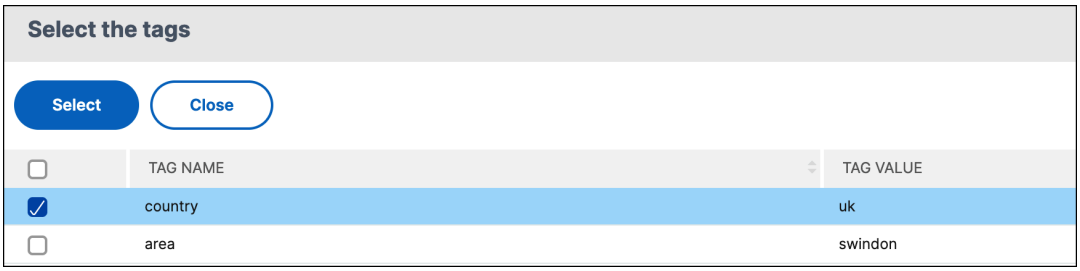


Tags:

So autorisieren Sie Benutzer, bestimmte Instanzen auf der Grundlage der zugehörigen Tags anzuzeigen oder zu verwalten:

a) Deaktivieren Sie das Kontrollkästchen **Alle Instanzen** und klicken Sie auf **Tags auswählen**.

b) Wählen Sie die erforderlichen Tags aus der Liste aus und klicken Sie auf **OK**.



Später, wenn Sie den ausgewählten Tags weitere Instanzen zuordnen, erhalten die autorisierten Benutzer automatisch Zugriff auf die neuen Instanzen.

Weitere Informationen über Tags und das Zuordnen von Tags zu Instanzen finden Sie unter So erstellen Sie Tags und weisen sie Instanzen zu.

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. Weil Anwendungen unabhängig von ihren Instanzen sind, um Benutzerzugriff zu gewähren.

Wenn Sie einem Benutzer Zugriff auf eine Anwendung gewähren, ist der Benutzer berechtigt, unabhängig von der Instanzauswahl nur auf diese Anwendung zuzugreifen.

Diese Liste bietet Ihnen die folgenden Optionen:

- **Alle Anwendungen:** Diese Option ist standardmäßig ausgewählt. Es fügt alle Anwendungen hinzu, die in der NetScaler Console 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.
- **Einzelner Entitätstyp auswählen:** Mit dieser Option können Sie den spezifischen Typ der Netzwerkfunktionsentität und die entsprechenden Entitäten auswählen.

  Sie können entweder einzelne Entitäten hinzufügen oder alle Entitäten unter dem erforderlichen Entitätstyp auswählen, um einem Benutzer den Zugriff zu gewähren.

  Die Option **Auch auf gebundene Entitäten anwenden** autorisiert die Entitäten, die an den ausgewählten Entitätstyp gebunden sind. Wenn Sie beispielsweise eine Anwendung auswählen und **Auf gebundene Entitäten anwenden** auswählen, autorisiert NetScaler Console alle Entitäten, die an die ausgewählte Anwendung gebunden sind.

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

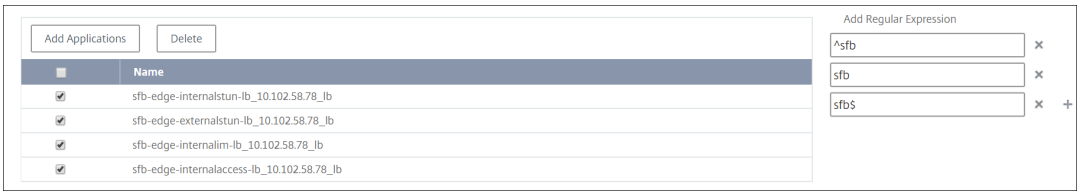
Sie können reguläre Ausdrücke verwenden, um die Netzwerkfunktionsentitäten zu suchen und hinzuzufügen, die die Regex-Kriterien für die Gruppen erfüllen. Der angegebene Regex-

Ausdruck wird in der NetScaler Console beibehalten. Gehen Sie wie folgt vor, um einen regulären Ausdruck hinzuzufügen:

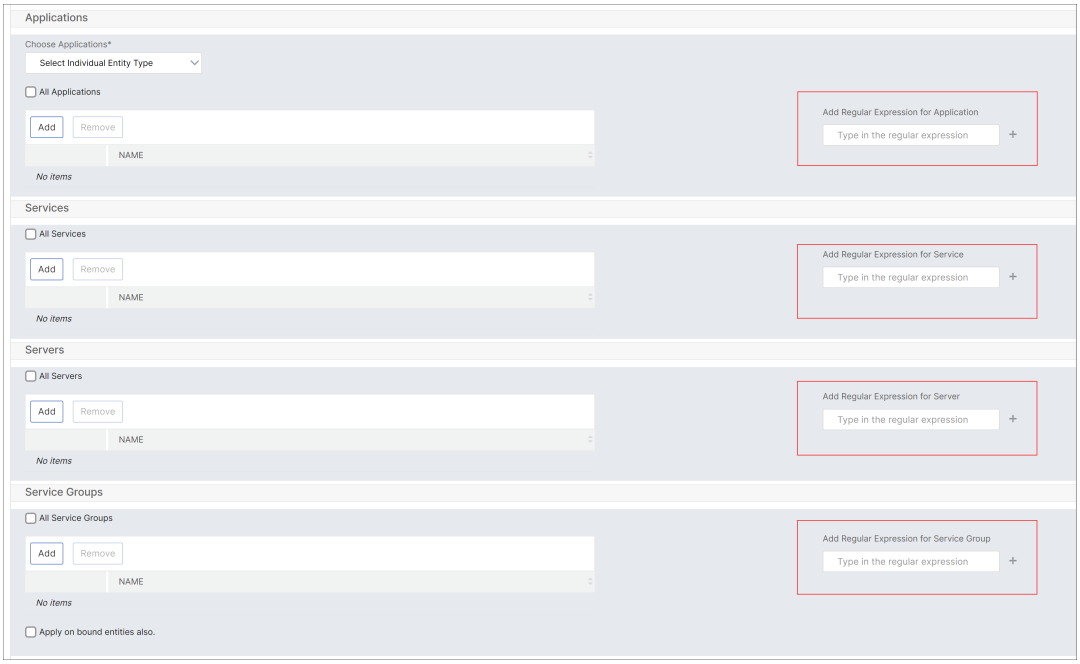
a) Klicken Sie auf **Regulären Ausdruck hinzufügen**.

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 erklärt, wie Sie mithilfe eines regulären Ausdrucks Netzwerkfunktionsentitäten hinzufügen, wenn Sie die Option **Individuellen Entitätstyp auswählen** wählen:



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.

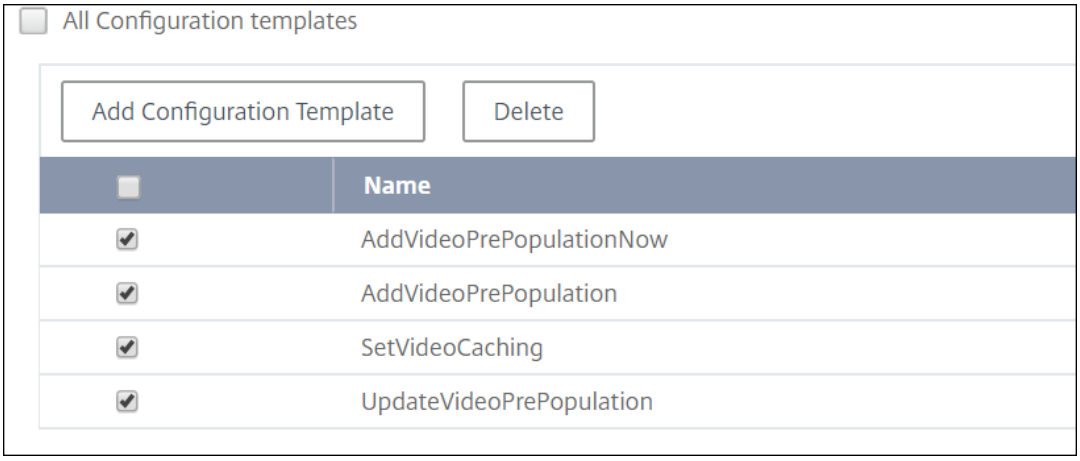
Der reguläre Ausdruck wird im System gespeichert, um den Autorisierungsbereich zu aktualisieren. Wenn die neuen Entitäten dem regulären Ausdruck ihres Entitätstyps entsprechen, aktualisiert NetScaler Console den Autorisierungsbereich auf die neuen Entitäten.

Vorlagen für die Konfiguration:

Wenn Sie die spezifische Konfigurationsvorlage auswählen möchten, die ein Benutzer anzeigen oder verwalten kann, gehen Sie wie folgt vor:

a) Löschen Sie **alle Konfigurationsvorlagen** und klicken Sie auf **Konfigurationsvorlage hinzufügen**.

b) Wählen Sie die gewünschte Vorlage aus der Liste aus und klicken Sie auf **OK**.



IPAM-Anbieter und Netzwerke:

Wenn Sie die spezifischen IPAM-Anbieter und -Netzwerke hinzufügen möchten, die ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

- **Anbieter hinzufügen** —**Alle Anbieter** löschen und auf **Anbieter hinzufügen**klicken. Sie können die erforderlichen Anbieter auswählen und auf **OK**klicken.
- **Netzwerke hinzufügen** —**Alle Netzwerke** löschen und auf **Netzwerke hinzufügen**klicken. Sie können die erforderlichen Netzwerke auswählen und auf **OK**klicken.

StyleBooks:

Wenn Sie das spezifische StyleBook auswählen möchten, das ein Benutzer anzeigen oder verwalten kann, gehen Sie wie folgt vor:

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 auch reguläre Ausdrücke als Werte verwenden, um StyleBooks zu suchen und hinzuzufügen, die 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
```

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

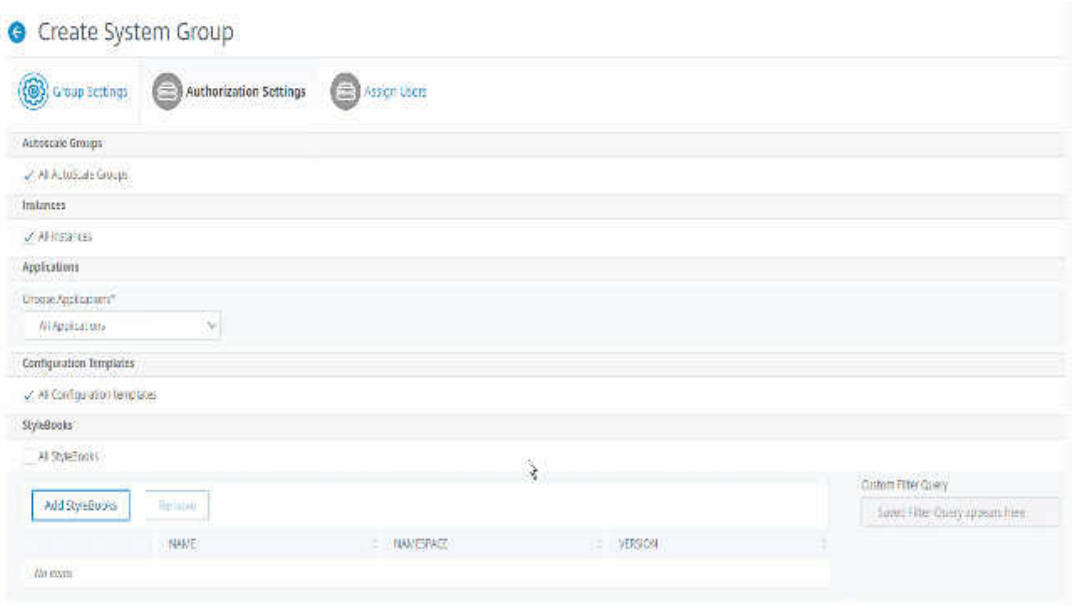
- StyleBook-Name ist entweder `lb-mon` oder `lb`.
- StyleBook Namespace ist `com.citrix.adc.stylebooks`.
- StyleBook-Version ist `1.0`.

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 die NetScaler Console 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 den Konfigurationspaketen eine der folgenden Optionen aus:

- **Alle Konfigurationen**: Diese Option ist standardmäßig ausgewählt. Es ermöglicht Benutzern, alle Konfigurationen in ADM zu verwalten.
- **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:

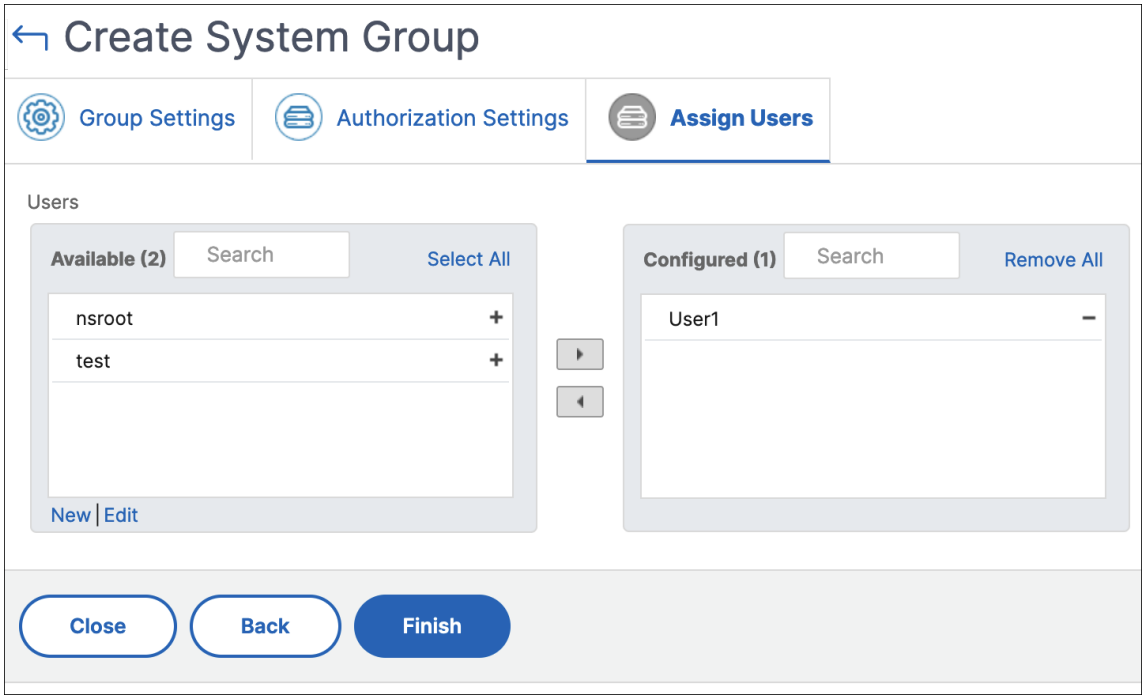
a) Deaktivieren Sie das Kontrollkästchen **Alle Domänennamen** und klicken Sie auf **Domänennamen hinzufügen**.

b) Wählen Sie die erforderlichen Domänennamen aus der Liste aus und klicken Sie auf **OK**.

c) Klicken Sie auf **Gruppe erstellen**.

d) Wählen Sie im Abschnitt **Benutzer zuweisen** den Benutzer in der Liste **Verfügbar** aus und fügen Sie ihn der Liste **Konfiguriert** hinzu.

> **Hinweis:**
>
> Sie können auch neue Benutzer hinzufügen, indem Sie auf **Neu**klicken.



a) Klicken Sie auf **Fertig stellen**.

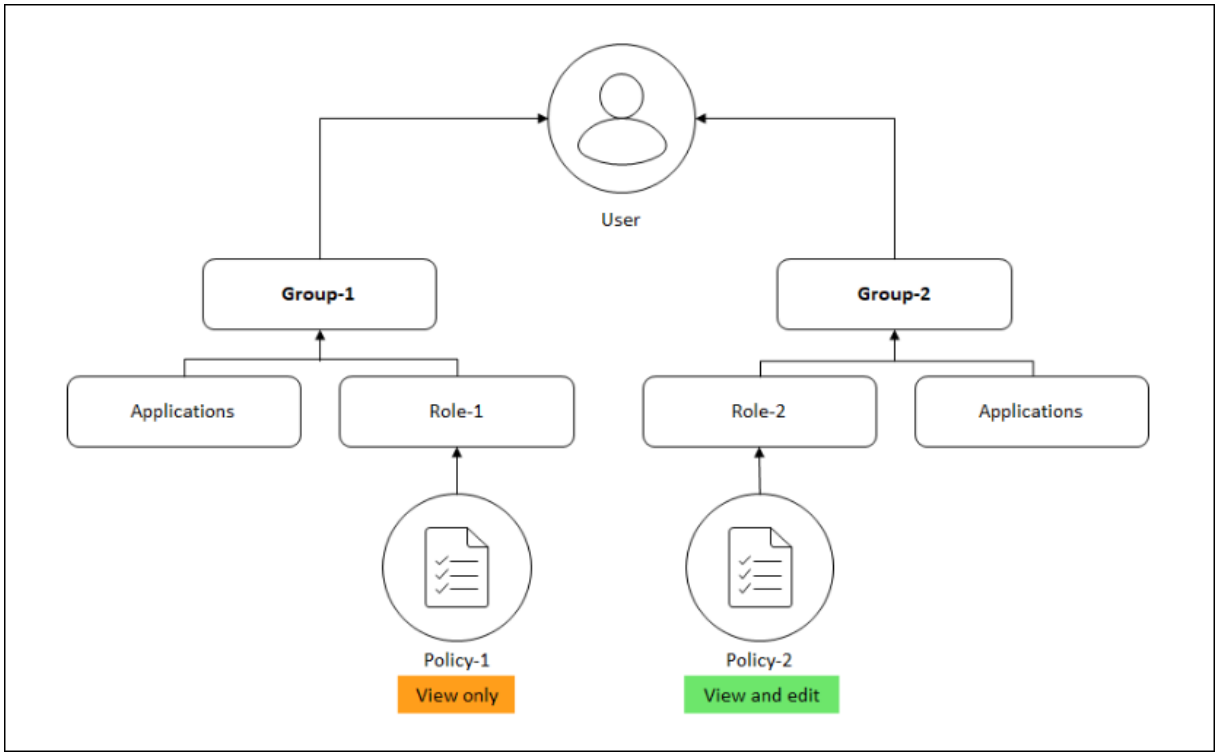
Wie sich der Benutzerzugriff basierend auf dem Berechtigungsumfang ändert

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 die NetScaler Console dem Benutzer je nach dem spezifischen Autorisierungsbereich 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.

Einschränkungen

Die folgenden NetScaler Console-Funktionen unterstützen RBAC nicht vollständig:

- **Analytics** —Die Analysemodule unterstützen RBAC nicht vollständig. Die RBAC-Unterstützung ist auf Instanzebene beschränkt und gilt nicht auf Anwendungsebene in den Analysemodulen Gateway Insight, HDX Insight und Security Insight.
  - Beispiel 1: Instanzbasierte RBAC (unterstützt). Ein Administrator, dem einige Instanzen zugewiesen wurden, kann nur diese Instanzen unter **HDX Insight** > **Geräte**und nur die entsprechenden virtuellen Server unter **HDX Insight** > **Applications** 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 **HDX Insight** > **Anwendungen** sehen, aber nicht darauf zugreifen, da RBAC auf Anwendungsebene nicht unterstützt wird.

- **StyleBooks** —RBAC wird für StyleBooks nicht vollständig unterstützt.
  - Stellen Sie sich eine Situation vor, in der viele Benutzer Zugriff auf ein einzelnes StyleBook haben, aber Zugriffsberechtigungen für verschiedene NetScaler-Instanzen haben. Benutzer können Konfigurationspakete auf ihren eigenen Instanzen erstellen und aktualisieren, da sie keinen Zugriff auf andere Instanzen als ihre eigenen haben. Sie können jedoch weiterhin die Konfigurationspakete und Objekte anzeigen, die auf NetScaler-Instanzen erstellt wurden.

Netzprofil der verwalteten NetScaler-Instanz zuweisen

July 17, 2024

Wenn Sie den Analyse- oder Metrik-Collector für die virtuellen Server in NetScaler Console aktivieren, werden die AppFlow- oder Messobjektdaten von NetScaler über die NetScaler Subnetz-IP-Adresse (SNIP) in die NetScaler Console exportiert. In einigen Szenarien kann das SNIP aufgrund der Firewall im Netzwerk blockiert werden. In solchen Szenarien müssen Sie möglicherweise eine andere IP-Adresse 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 Console ein Netzprofil zuweisen, um AppFlow-Daten von NetScaler nach NetScaler Console 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 Console zu:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** .
2. Wählen Sie die Instanz aus und aus der Liste **Aktion auswählen**:
   - Klicken Sie auf **Netzwerkprofile konfigurieren**, um AppFlow ein Netzprofil zuzuweisen.

- Klicken Sie auf **Netzprofile für den Metrik-Kollektor konfigurieren**, um ein Netzprofil für den Metrik-Kollektor zuzuweisen.

3. Wählen Sie ein Netzprofil aus der Liste aus und klicken Sie auf **Anwenden**.

> **Hinweis:**
>
> - Stellen Sie für AppFlow sicher, dass Sie Analysen für alle virtuellen Server deaktivieren, bevor Sie der Instanz ein Netzprofil zuweisen.
> - Stellen Sie für Metrics Collector sicher, dass Sie Messobjekte für alle virtuellen Server deaktivieren, bevor Sie der Instanz ein Netzprofil zuweisen.

Verwaltung der Datenspeicherung

January 26, 2024

Es ist wichtig zu wissen, welche Funktionen in NetScaler Console verwendet werden und wie die Datennutzung der einzelnen Funktionen ist. Das **Data Storage Management** Dashboard dient diesem Zweck und dient als Visualisierungstool, mit dem Sie die Gesamtdaten, die in der NetScaler Console-Datenbank gespeichert sind, anhand verschiedener Funktionen nachvollziehen 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 Console-Datenbank der 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 Console gespeichert wurden.
- 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:

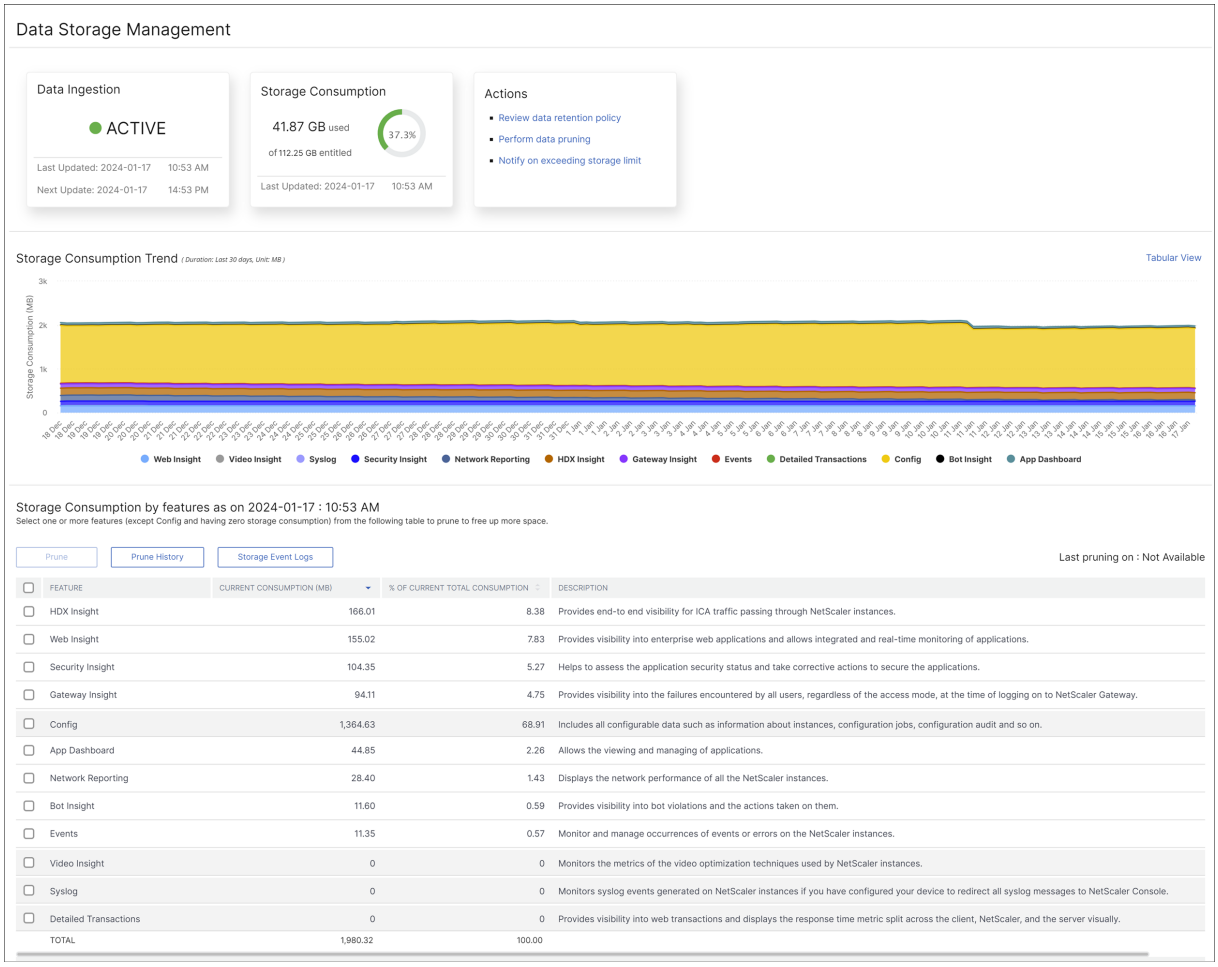
- Verstehen Sie Ihren Datenspeicher —In diesem Abschnitt erfahren Sie, wie Sie das Dashboard verwenden können, um Informationen zu Ihrem Datenspeicher anzuzeigen.
- Datenspeicher verwalten —Dieser Abschnitt enthält Informationen darüber, welche Aktionen Sie im Dashboard ergreifen können, um Ihren Datenspeicher zu verwalten.

Datenspeicher verstehen

May 9, 2024

Sie können das **Data Storage Management**-Dashboard in NetScaler Console verwenden, um Daten und Grafiken 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
- Status der Datenbereinigung
- Trends beim Speicherverbrauch
- Speicherverbrauch nach Funktionen

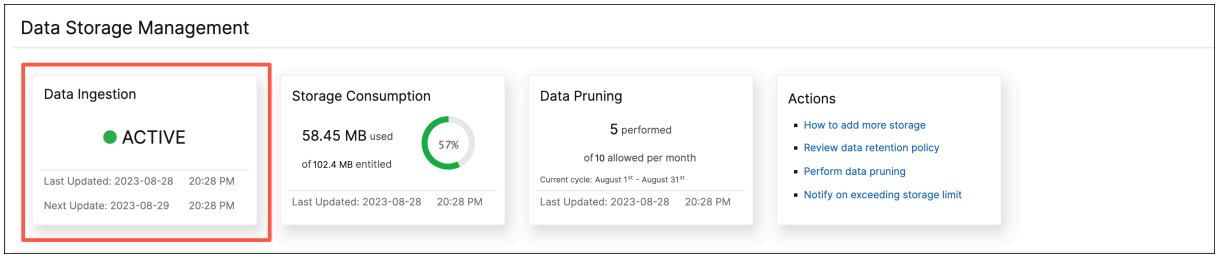
Status Ihrer Datenaufnahmeaktivität

Unter Datenaufnahme versteht man den Import großer und sortierter Daten aus allen verwalteten NetScaler-Instanzen mithilfe verschiedener Funktionen wie Events, Syslogs, Network Reporting usw. in den NetScaler Console-Speicher.

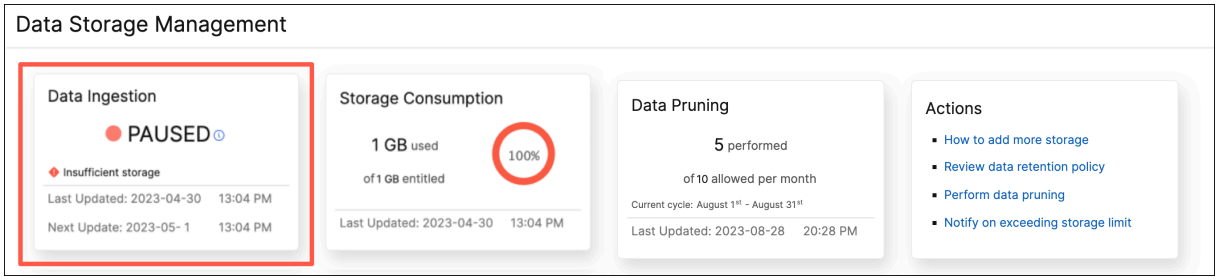
Der Datenaufnahmestatus gibt an, ob NetScaler Console Statistiken von NetScaler-Instanzen sammelt. Die Datenaufnahmeaktivität wird fortgesetzt, solange sich der verbrauchte Speicherplatz innerhalb des berechtigten Speichers befindet. Wenn der Verbrauch den berechtigten Speicherplatz übertrifft, wird 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.



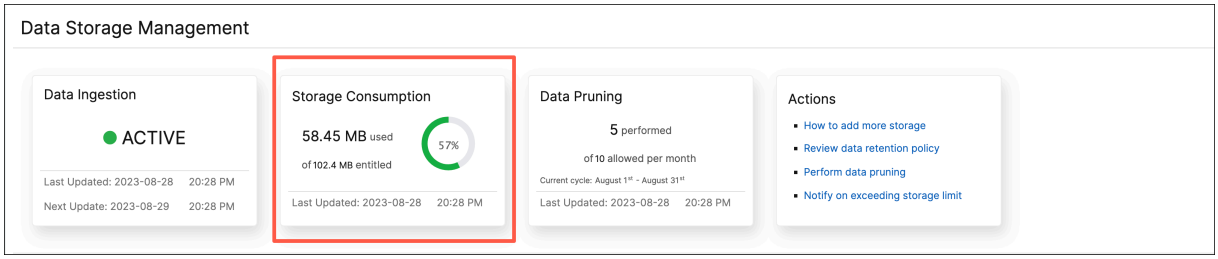
So setzen Sie Ihre unterbrochene Datenaufnahme fort

Um Ihre Datenaufnahme fortzusetzen, können Sie eine der folgenden Aktionen ausführen:

- Fügen Sie mehr Datenspeicher hinzu.
- Führen Sie eine Datenbereinigung durch.

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.

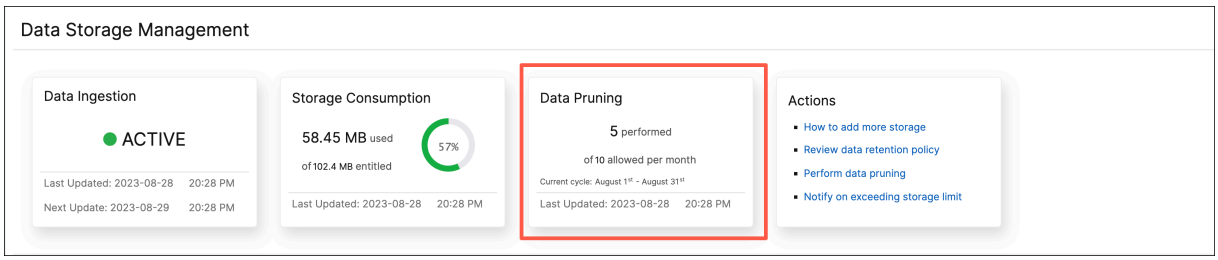
Verbrauchter Speicherplatz

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.

Status der Datenbereinigung

Beim Bereinigen werden Daten manuell gelöscht und Speicherplatz freigegeben. In jedem Kalendermonat sind 10 Datenpflaumen erlaubt. Beispielsweise können Sie Ihre Daten vom 1. bis 31. Juli zehnmal löschen.



Um zu erfahren, wie viele Datenlöschungen Sie bereits verbraucht haben und wie viele noch übrig sind, sehen Sie sich die Kachel **Datenbereinigung an**.

> **Hinweis:**
>
> Jede Schnittaktivität wird unabhängig von der Anzahl der ausgewählten Merkmale als eine Datenbereinigung gezählt.

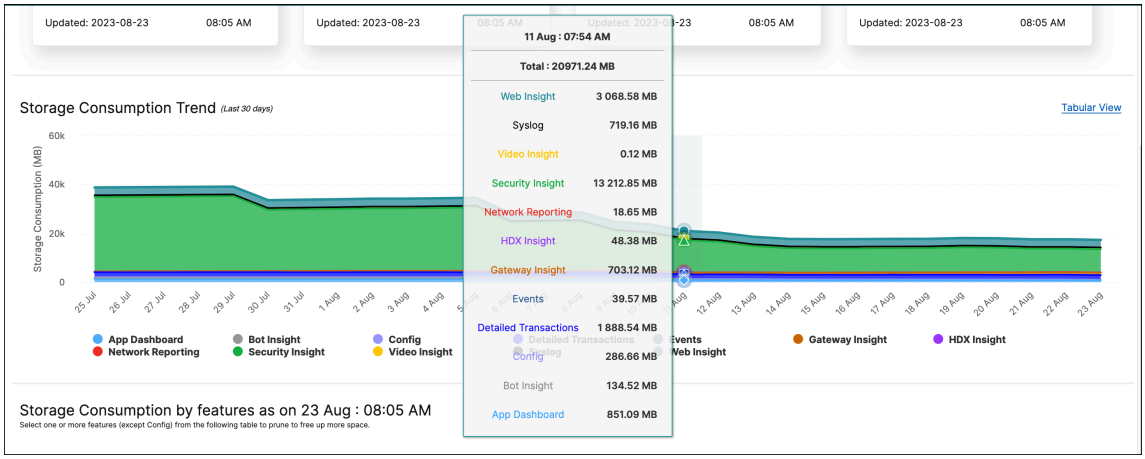
Trends beim Speicherverbrauch

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:

- **Grafische Ansicht**– Zeigt an, wie der Datenspeicher auf die verschiedenen Funktionen der NetScaler Console 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.

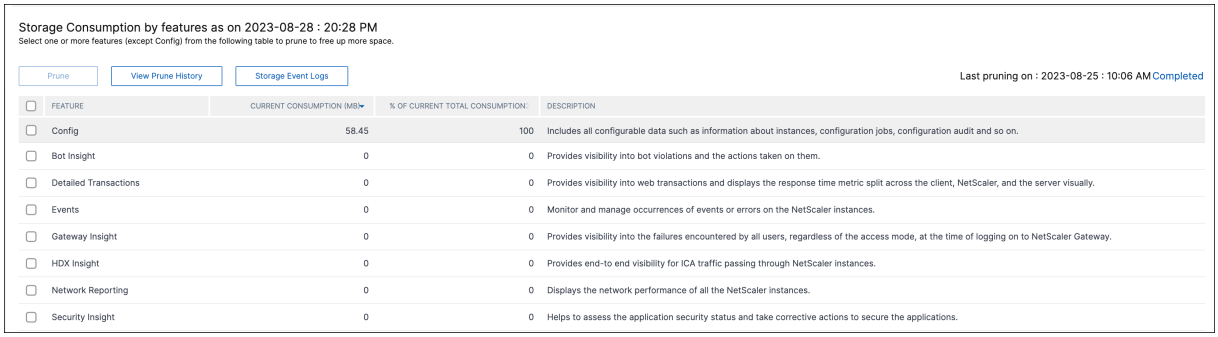
FEATURE	BESCHREIBUNG
Gateway Insight	Bietet Einblick in die Fehler, auf die alle Benutzer unabhängig vom Zugriffsmodus zum Zeitpunkt der Anmeldung bei NetScaler Gateway gestoßen sind.
Ereignisse	Überwachen und verwalten Sie das Auftreten von Ereignissen oder Fehlern auf den NetScaler-Instanzen.
App-Dashboard	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 werden, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Meldungen an NetScaler Console 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 Console verwendet wird
- Der Prozentsatz des Speicherplatzes, den die Features an einem bestimmten Tag beanspruchen



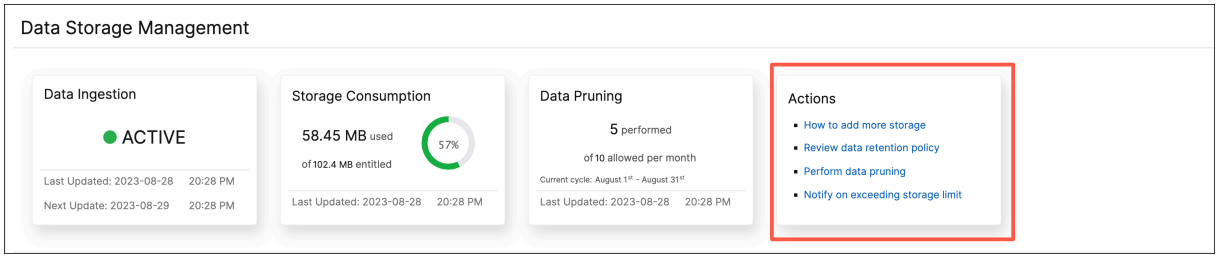
Wenn Sie die Tabelleneinträge sortieren möchten, die Kopfzeilen der Tabelle. NetScaler Console sortiert die Tabelle auf der Grundlage der Daten in der ausgewählten Spalte alphanumerisch von oben nach unten. Um die Tabelle in umgekehrter Reihenfolge zu sortieren, klicken Sie erneut auf die Spaltenüberschrift.

Informationen zum Bereinigen Ihrer Daten, zum Bereinigen des Verlaufs und zu Speicherereignisprotokollen finden Sie unter Datenspeicher verwalten.

Verwalte deinen Speicherplatz

July 17, 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

Wenn Ihr verbrauchter Speicher 100% des lizenzierten Speichers erreicht, wird die Datenaufnahme unterbrochen und die Daten werden nicht mehr in NetScaler Console gespeichert.

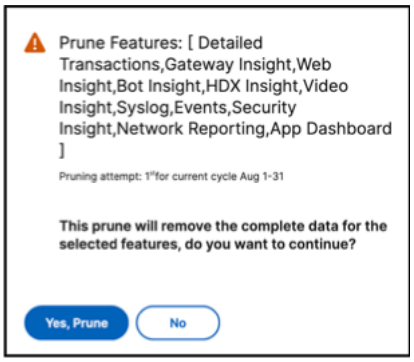
Führen Sie eine Datenbereinigung durch

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 vernünftig eingesetzt werden und NetScaler Console 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.

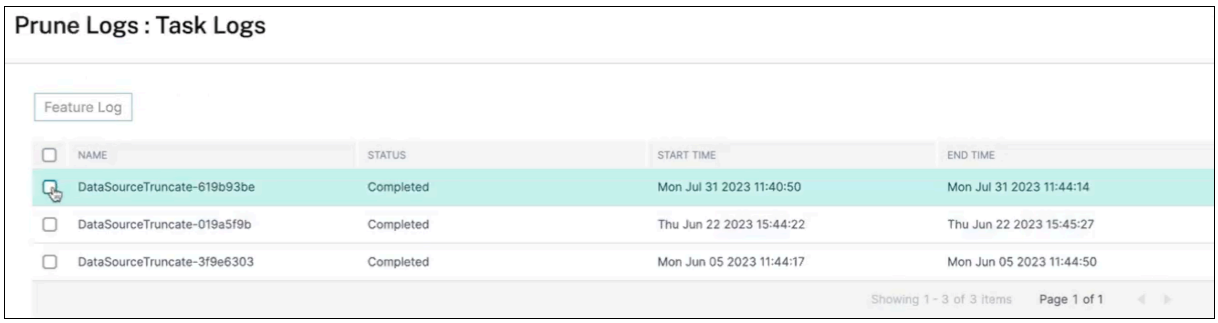
   In einem Popup-Fenster werden Sie aufgefordert zu bestätigen, ob Sie alle Daten für die ausgewählten Features löschen möchten. Klicken Sie auf **Ja, Prune**.



> **Hinweis:**
>
> Im Popup-Fenster werden auch Informationen zu Ihrem aktuellen Bereinigungsversuch angezeigt.

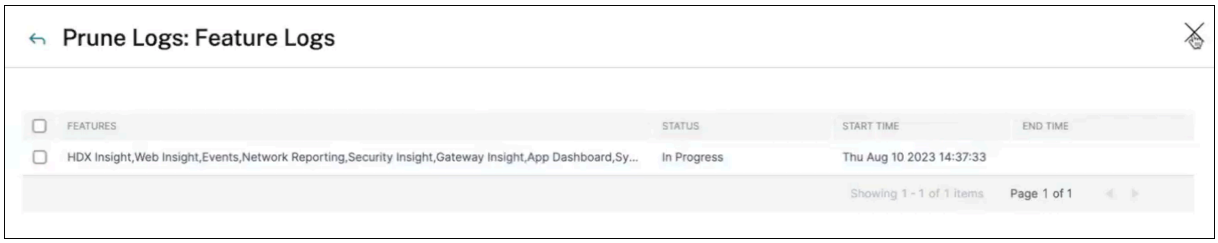
Geschichte der Pflaumen anzeigen

Klicken Sie auf **Prune-Verlauf** anzeigen , um Details zu allen Prune-Aktivitäten zu erhalten, die Sie in NetScaler Console ausgeführt haben.



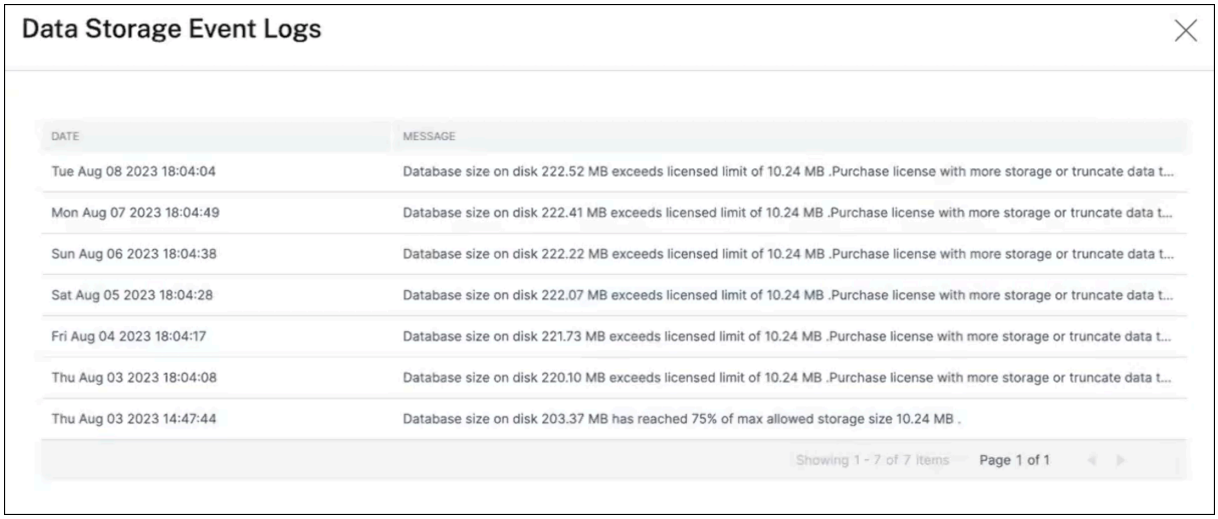
Auf der Seite **Prune Logs: Task Logs** wird die Liste aller Prune-Aufgaben angezeigt, einschließlich ihres jeweiligen Status, ihrer Start- und Endzeit.

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 Console 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 von den verschiedenen Funktionen verwendeten Speicherplatz reduzieren möchten, können Sie ändern, wie lange Daten in NetScaler Console 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 Console 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.

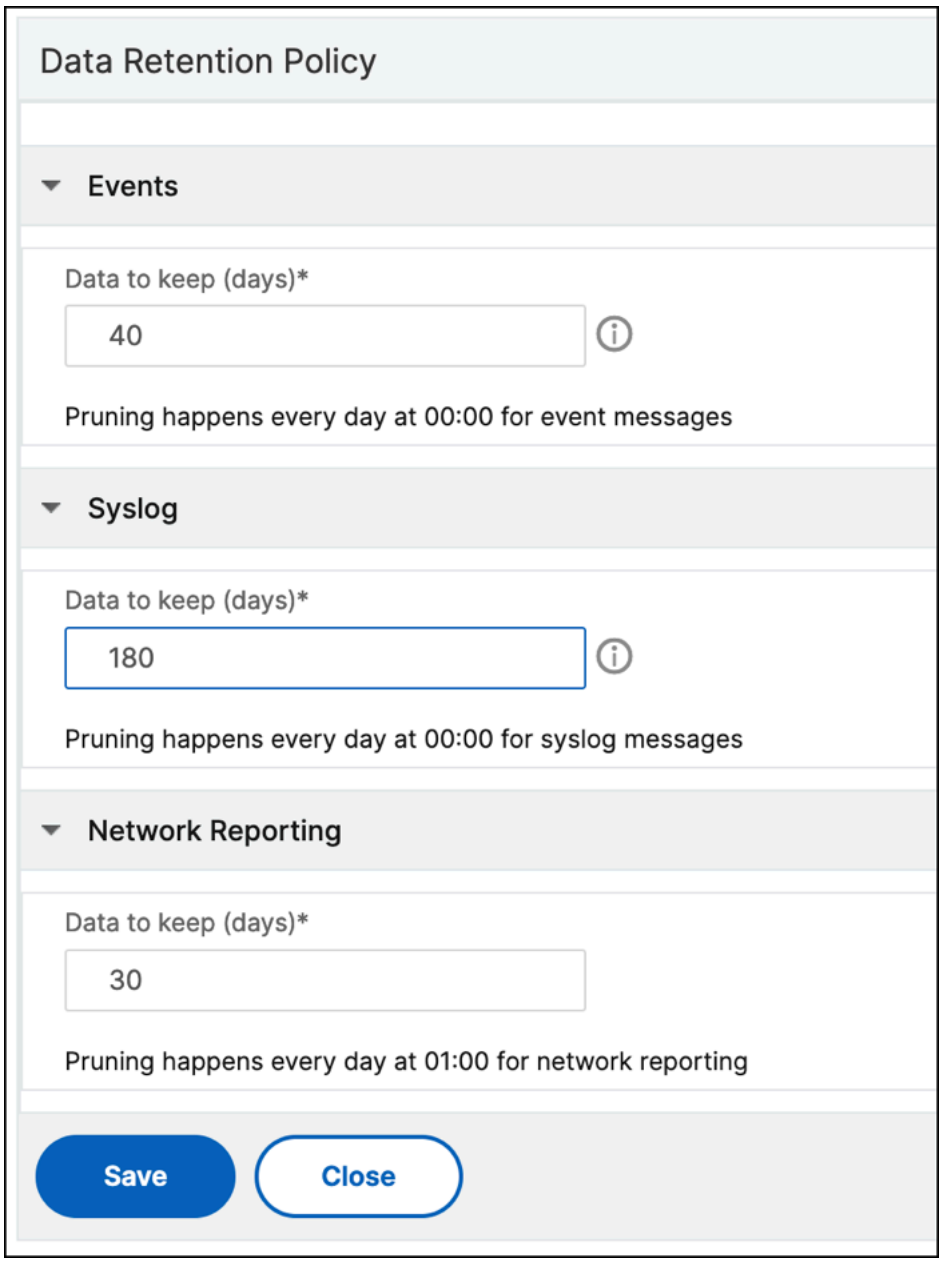
Datenaufbewahrungsrichtlinie

January 26, 2024

In NetScaler Console können Sie für eine bestimmte Dauer auf Systemereignisse, Syslog-Meldungen und Netzwerkberichtsdaten zugreifen.

1. Navigieren Sie zu **Einstellungen > Datenspeicherverwaltung > Datenaufbewahrungsrichtlinie**, um die Datenspeicherung zu konfigurieren.
2. Klicken Sie auf die Schaltfläche Bearbeiten.
3. Geben Sie für jede der folgenden Optionen die Anzahl der Tage ein, für die die Daten in NetScaler Console aufbewahrt werden sollen:

Optionen	Beschreibung
Ereignisse	Ermöglicht es Ihnen, die in NetScaler Console gespeicherten Ereignismeldungen auf bis zu 40 Tage zu beschränken. Die Ereignisse werden aus der NetScaler Console gelöscht, nachdem die Aufbewahrungsrichtlinie abgelaufen ist. Die gelöschten Ereignisse werden nach einem Tag gelöscht.
Syslog	Ermöglicht es Ihnen, die Menge der in der Datenbank gespeicherten Syslog-Daten auf bis zu 180 Tage zu begrenzen.
Netzwerkberichterstattung	Ermöglicht es Ihnen, die in NetScaler Console gespeicherten Netzwerkberichtsdaten auf bis zu 30 Tage zu beschränken.



Wichtig:

Sie können die Datenaufbewahrungsrichtlinie nicht mit einem Express-Konto bearbeiten.

Wenn Ihr Konto in ein Express-Konto umgewandelt wird, speichert die NetScaler Console die Speicherdaten bis zu 500 MB oder Tagesdaten, je nachdem, welcher Wert niedriger ist. Weitere Informationen finden Sie unter NetScaler Console-Ressourcen mithilfe des Express-Kontos verwalten .

Systemalarme konfigurieren und anzeigen

May 9, 2024

Sie können eine Reihe von Alarmen aktivieren und konfigurieren, um den Zustand Ihrer NetScaler Console-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 überschritten wird (z. B. MemoryUsageHigh) oder wenn ein Ereignis eintritt, das der Alarmkategorie entspricht (z. B. LoginFailure), wird eine Meldung im System aufgezeichnet, und Sie können die Nachricht als Syslog-Meldung 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.

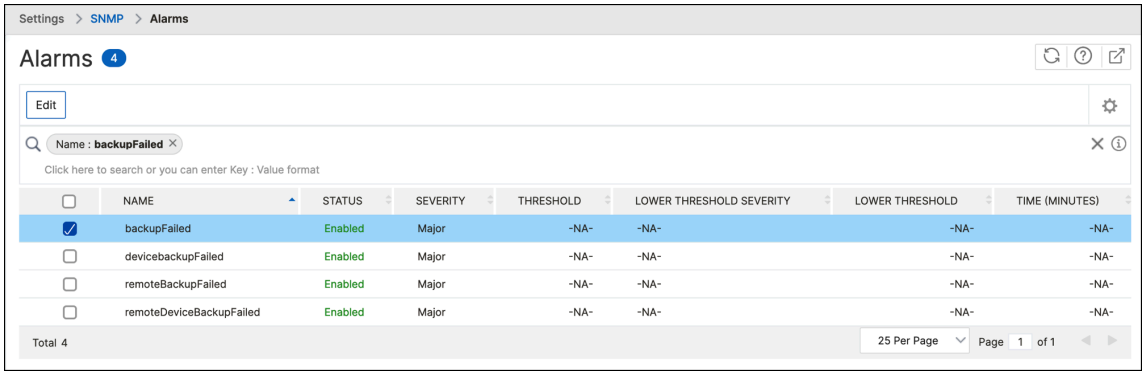
Einen Alarm konfigurieren

Stellen Sie sich ein Szenario vor, in dem Sie einen fehlgeschlagenen Backupversuch überwachen möchten. Sie können den backupFailed Alarm aktivieren und ihm einen Schweregrad wie Major zuweisen. Immer wenn NetScaler Console versucht, die Systemdateien zu sichern, und wenn der Versuch fehlschlägt, wird ein Alarm ausgelöst. Sie können die Nachricht auf der NetScaler Console-Protokollmeldungsseite anzeigen oder Benachrichtigungen per E-Mail oder SMS erhalten.

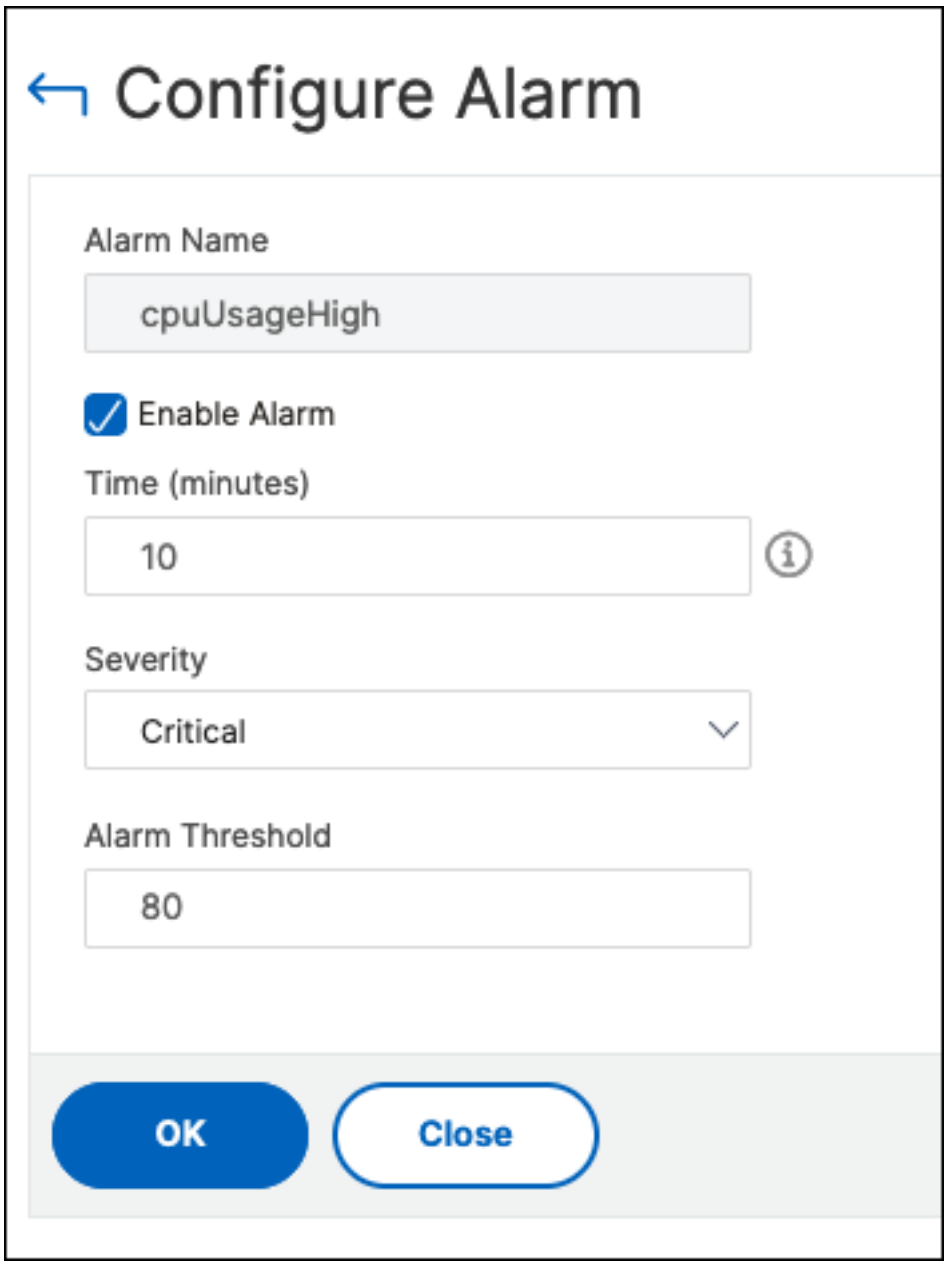
Um den Alarm zu konfigurieren, müssen Sie den backupFailed-Alarm auswählen und den Schweregrad als Schweregrad angeben. Der Alarm ist standardmäßig aktiviert.

So konfigurieren und zeigen Sie einen Systemalarm mithilfe der NetScaler Console 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. cpuUsageHigh), und klicken Sie auf **Bearbeiten, um die Einstellungen zu ändern**.



3. Wählen Sie auf der Seite **Alarm konfigurieren** die Option **Alarm aktivieren** aus, um Warnmeldungen zu erstellen, und geben Sie dann Folgendes an:

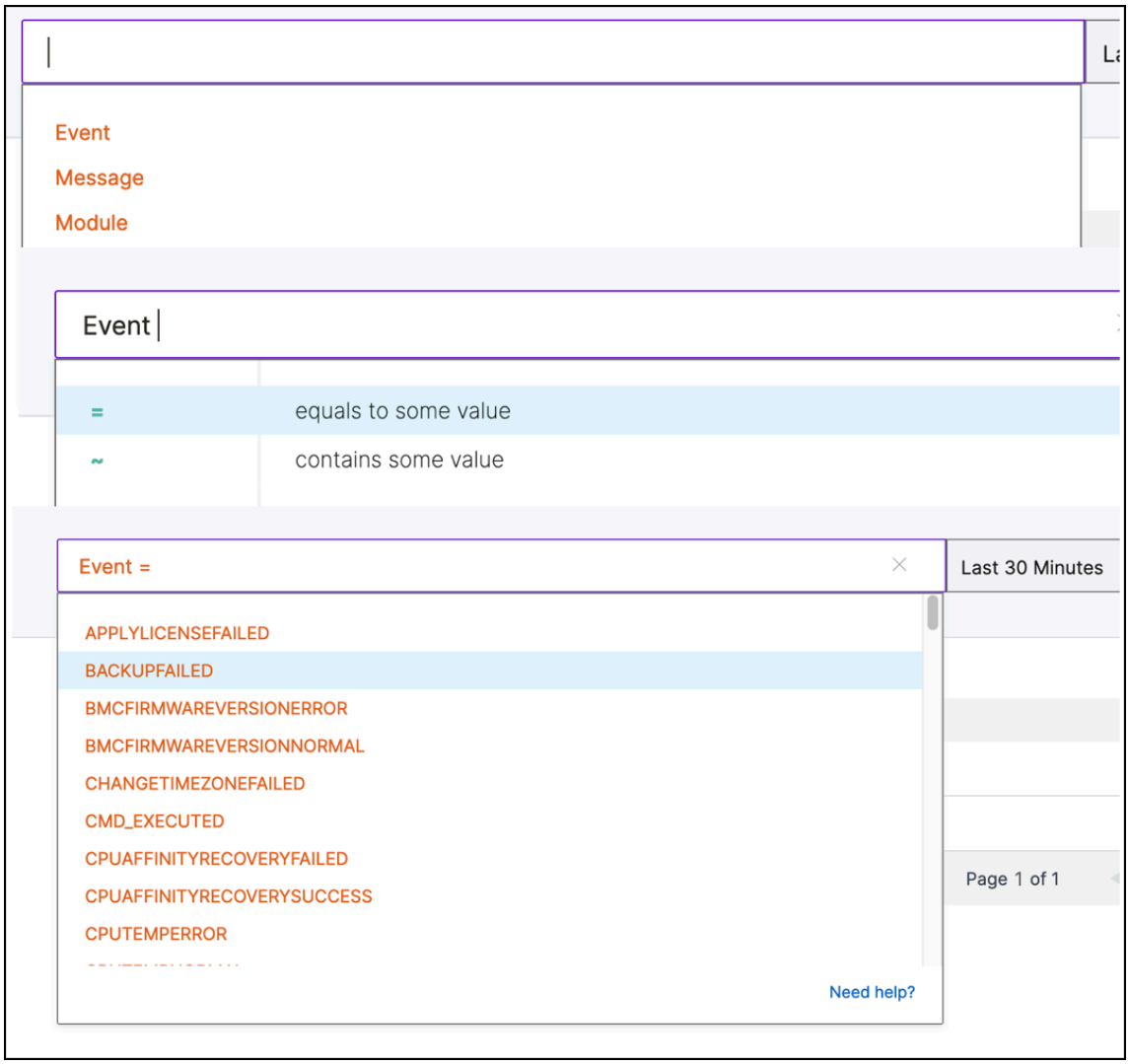
   - **Zeit**. Geben Sie die Zeit (in Minuten) ein, nach der Sie den Alarm auslösen möchten.
   - **Schweregrad**. Wählen Sie den Schweregrad aus.
   - **Alarmschwelle**. Geben Sie den Wert ein, für den der Alarm ausgelöst und die Alarme an Sie gesendet werden sollen.

   Klicken Sie auf **OK**.

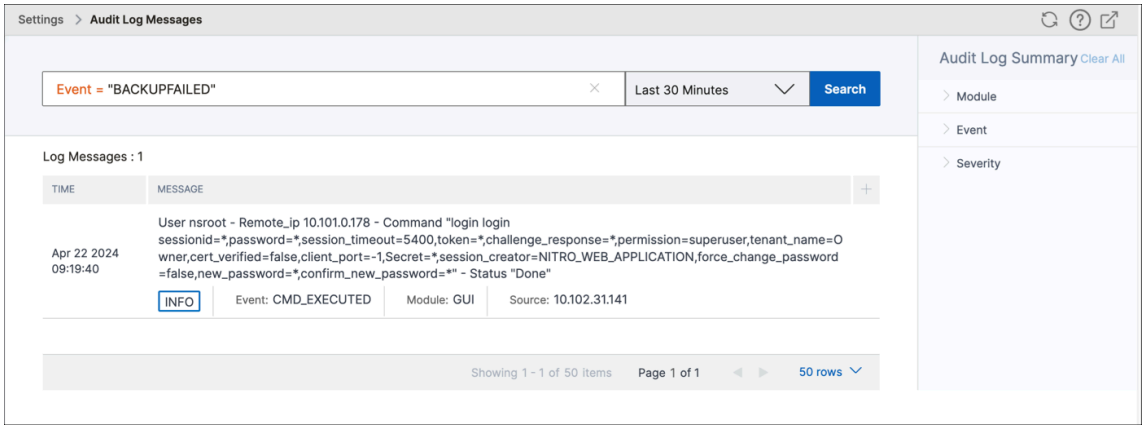
> **Hinweis:**
>
> Für einige Alarme, z. B. backupFailed, können Sie den Schwellenwert nicht festlegen. Wenn der Alarm ausgelöst wird, können Sie das generierte Ereignis als Syslog-Meldung anzeigen.

So zeigen Sie das durch einen Alarm generierte Ereignis an (z. B. backupFailed):

1. Navigieren Sie zu **Einstellungen** > **Auditprotokollmeldungen**.
2. Wählen Sie im Suchfeld die Art des Alarms aus. Wählen Sie in diesem Beispiel **Event**, **=** (entspricht einem Wert) und dann **BACKUPFAILED** aus.



Das Ereignis, das für ein fehlgeschlagenes Backup generiert wurde, wird angezeigt.



Sie können auch Benachrichtigungen so einrichten, dass Sie entweder eine E-Mail oder einen SMS-Text (Short Message Service) erhalten, wenn ein Alarm ausgelöst wird.

Schwellenwerte zu Alarmen zur Datenträgerauslastung hinzufügen

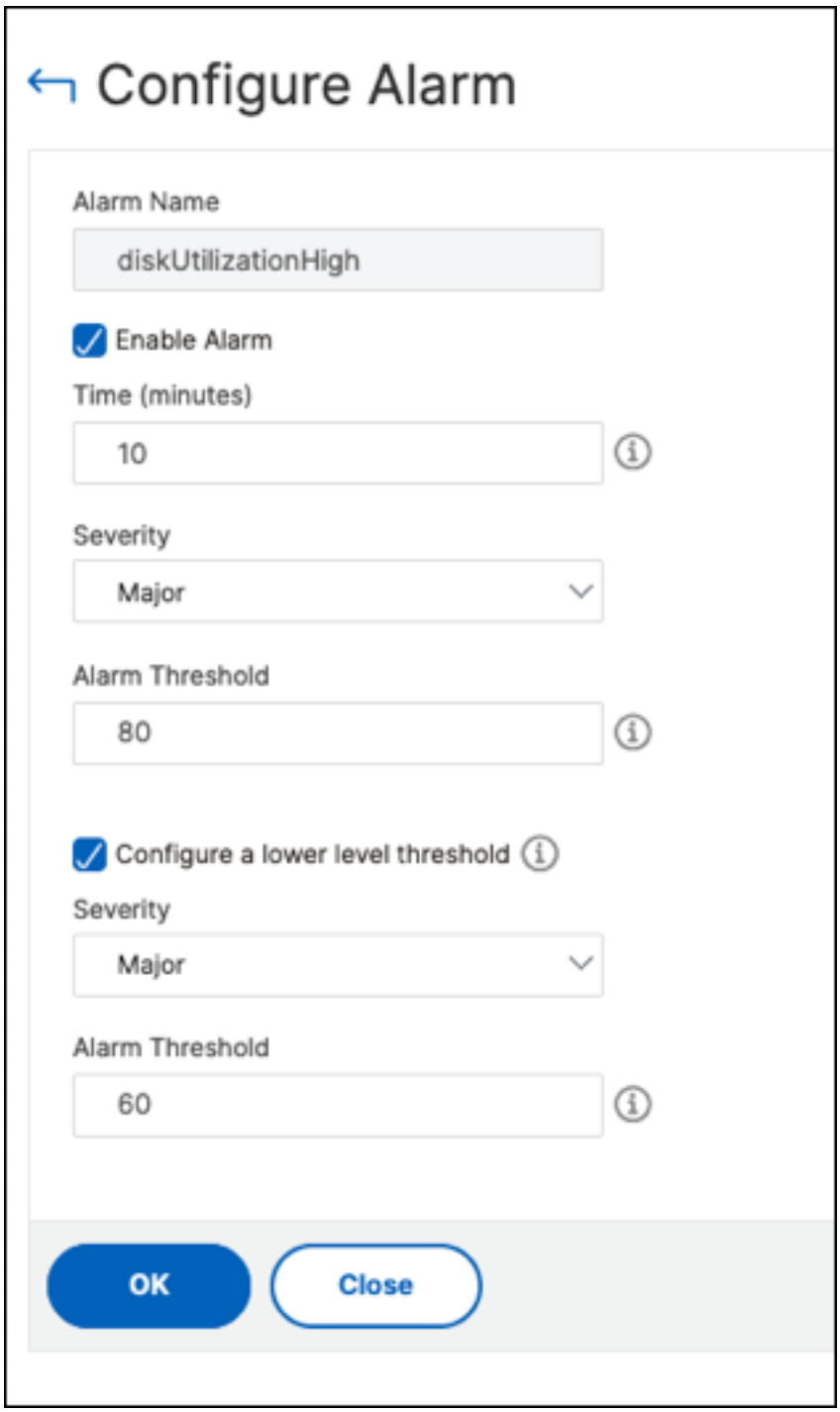
Alarme zur Datenträgerauslastung werden ausgelöst, wenn der auf dem NetScaler Console-Server verwendete Speicherplatz einen vordefinierten Schwellenwert überschreitet.

Wenn Sie als Administrator Benachrichtigungen erhalten, können Sie wählen, ob Sie nicht benötigte Daten löschen oder zusätzliche Speicherressourcen zuweisen möchten, um Serviceunterbrechungen oder Leistungseinbußen zu verhindern.

Ab Version 14.1 Build 25x können Sie auch einen niedrigeren Schwellenwert für Alarme zur Datenträgerauslastung hinzufügen. Mit diesem Schwellenwert können Sie einen unteren Grenzwert festlegen, um Benachrichtigungen zu erhalten, bevor ein oberer Schwellenwert überschritten wird.

So konfigurieren Sie einen Schwellenwert auf niedrigerer Ebene:

1. Navigieren Sie zu **Einstellungen > SNMP > Alarme** und geben Sie in das Suchfeld diskUtilizationHigh ein, um die Alarme zur Datenträgerauslastung anzuzeigen.
2. Wählen Sie den Alarm aus und klicken Sie auf **Bearbeiten**.
3. Wählen Sie auf der Seite **Alarm konfigurieren** die Option **Schwellenwert auf niedrigerer Ebene konfigurieren** aus. Geben Sie den unteren Schwellenwert ein.



Wenn Sie beispielsweise einen unteren Schwellenwert für die Datenträgerauslastung von 60 und einen oberen Schwellenwert von 80 festlegen, erhalten Sie eine Warnung, wenn die Datenträgernutzung 60 % der Datenträgerkapazität überschreitet. Mit dieser Einstellung können Sie Korrekturmaßnahmen ergreifen, bevor die Datenträgerauslastung 80 % erreicht.

Integration der Beobachtbarkeit

July 17, 2024

Aufgrund der zunehmenden Komplexität moderner Anwendungen stehen Administratoren vor folgenden Herausforderungen:

- Überwachung und Problembehandlung von Anwendungen.
- Verschaffen Sie sich einen Überblick über das Verhalten von Infrastruktur und Anwendungen.

Observability überbrückt diese Lücke, indem sie diese Einblicke in die gesamte Infrastruktur bietet. Mit der Observability-Integrationsfunktion in NetScaler Console können Sie:

- NetScaler Console mit Splunk integrieren.
- NetScaler Console mit New Relic integrieren.
- Integrieren Sie NetScaler Console in Microsoft Sentinel
- NetScaler-Instanzen für den Export von Erkenntnissen nach Prometheus mit dem Standardschema konfigurieren.

Integration mit Splunk

July 17, 2024

Sie können NetScaler Console jetzt in Splunk integrieren, um Analysen für Folgendes anzuzeigen:

- Verstöße gegen die WAF
- Bot-Verstöße
- SSL Certificate Insights
- Gateway Insights

Das Splunk-Add-on ermöglicht Ihnen:

- Kombinieren Sie alle anderen externen Datenquellen.
- Bieten Sie eine bessere Sichtbarkeit von Analysen an einem zentralen Ort.

NetScaler Console 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:

- Konfigurieren Sie Splunk für den Empfang von Daten von NetScaler Console
- NetScaler Console so konfigurieren, dass Daten nach Splunk exportiert werden
- Dashboards in Splunk anzeigen

Konfigurieren Sie Splunk für den Empfang von Daten von NetScaler Console

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

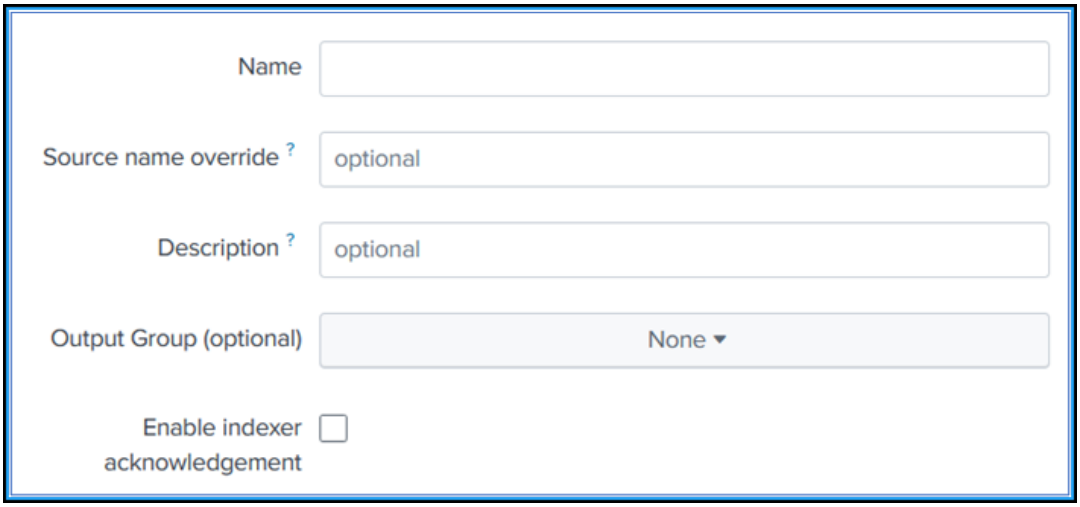
Splunk HTTP Event Collector-Endpunkt einrichten und ein Token generieren

Sie müssen zuerst den HTTP-Event-Collector in Splunk einrichten. Dieses Setup ermöglicht die Integration zwischen der NetScaler Console und Splunk, um die WAF- oder Bot-Daten zu senden. Als Nächstes müssen Sie in Splunk ein Token generieren, um:

- Aktivieren Sie die Authentifizierung zwischen NetScaler Console und Splunk.
- Empfangen Sie Daten über den Event Collector-Endpunkt.

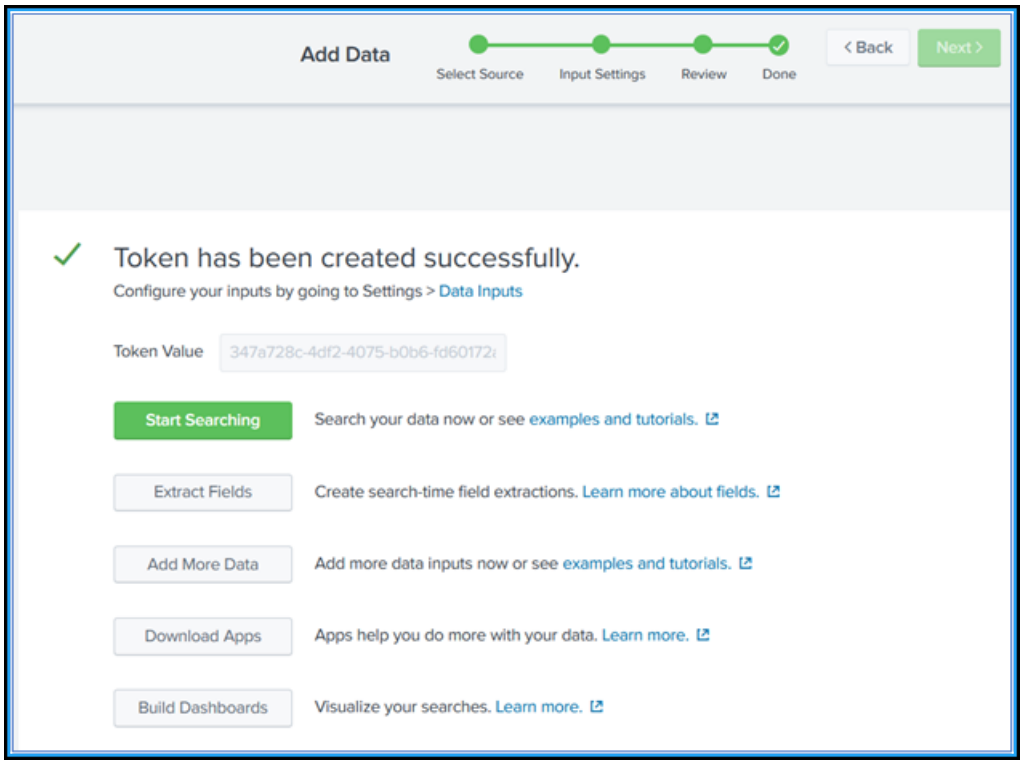
1. Melden Sie sich bei Splunk an.
2. Navigieren Sie zu **Einstellungen > Dateneingaben > HTTP-Event-Collector** und klicken Sie auf **Neu hinzufügen**.
3. Geben Sie die folgenden Parameter an:
    a) **Name**: Geben Sie einen Namen Ihrer Wahl an.
    b) **Quellnamenüberschreibung (optional)**: Wenn Sie 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**: NetScaler Console unterstützt diese Option nicht. Die Auswahl dieser Option wird nicht empfohlen.



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 Console hinzufügen.

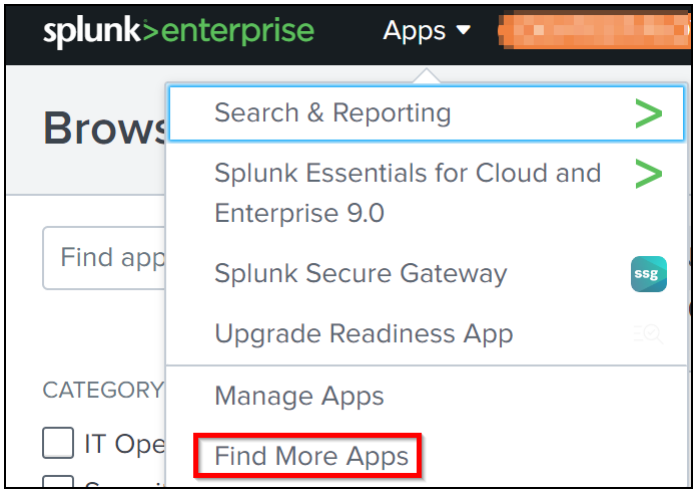


Splunk Common Information Model installieren

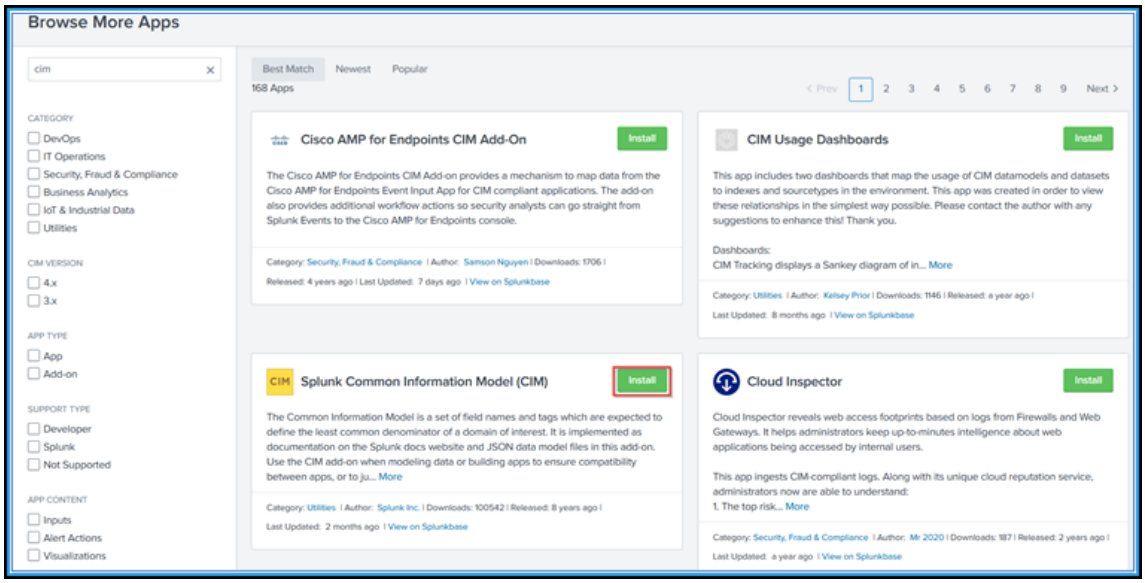
In Splunk müssen Sie das Splunk CIM-Add-on installieren. Dieses Add-on stellt sicher, dass die von NetScaler Console empfangenen Daten die aufgenommenen Daten normalisieren und einem gemeinsamen Standard entsprechen, wobei dieselben Feldnamen und Event-Tags für äquivalente Ereignisse verwendet werden.

> **Hinweis**
>
> Sie können diesen Schritt ignorieren, wenn Sie das Splunk CIM-Add-on bereits installiert haben.

1. Melden Sie sich bei Splunk an.
2. Navigieren Sie zu **Apps > Weitere Apps suchen**.



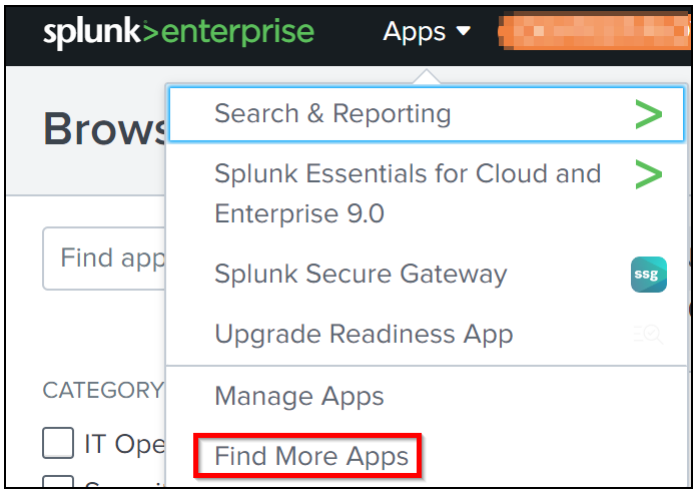
3. Geben Sie **CIM** in die Suchleiste ein und drücken **Sie die Eingabetaste**, um das **Splunk Common Information Model (CIM)** -Add-on aufzurufen, und klicken Sie auf **Installieren**.



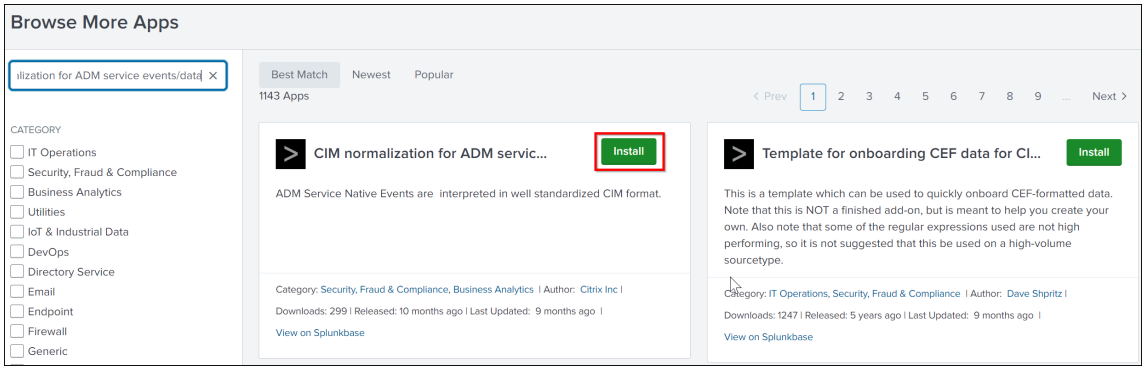
Installieren Sie den CIM-Normalizer

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

Nachdem Sie Splunk CIM installiert haben, müssen Sie ein Beispieldashboard mit einer Vorlage für WAF und Bot sowie SSL Certificate Insights vorbereiten. 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.

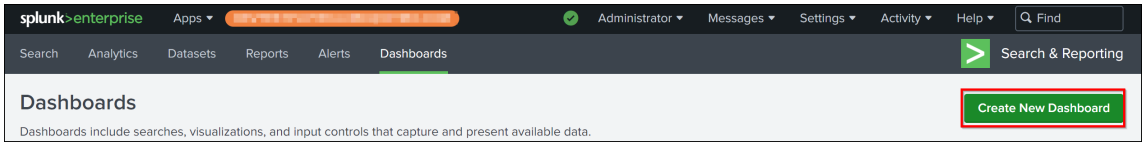
> **Hinweis:**

> Das folgende Verfahren zur Erstellung eines Beispiel-Dashboards gilt sowohl für WAF als auch für Bot und SSL Certificate Insights. 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 Observability Integration verfügbar ist.
2. Extrahieren Sie die Datei, öffnen Sie die `json`-Datei mit einem beliebigen Editor und kopieren Sie die Daten aus der Datei.

   > **Hinweis:**
   >
   > Nach dem Extrahieren erhalten Sie zwei `json`-Dateien. Verwenden Sie `adm_splunk_security_viol.json`, um das WAF- und Bot-Beispieldashboard zu erstellen, und verwenden Sie `adm_splunk_ssl_certificate.json`, um das Beispieldashboard für SSL Certificate Insights 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:

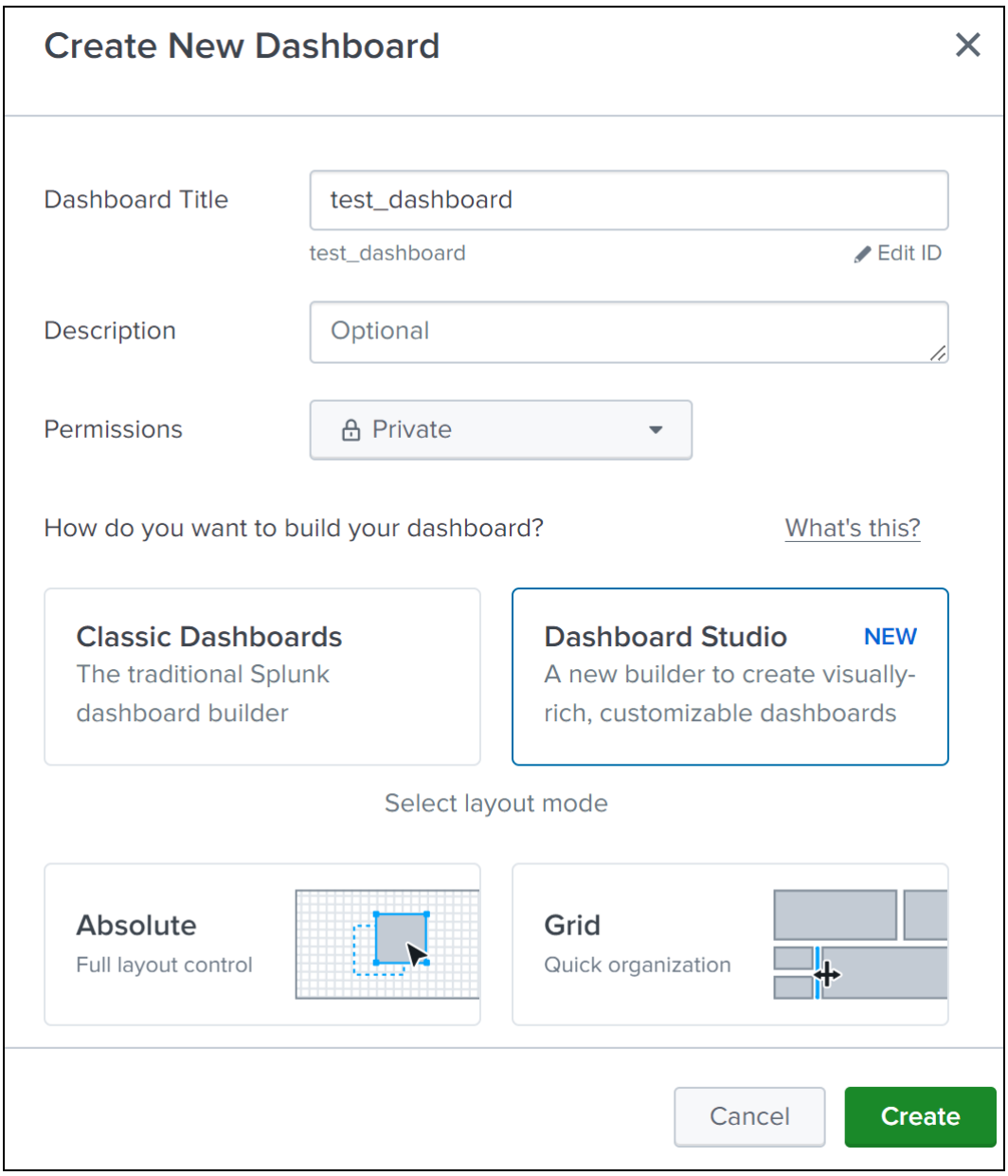
   a) **Dashboard-Titel** – Geben Sie einen Titel Ihrer Wahl ein.

   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.

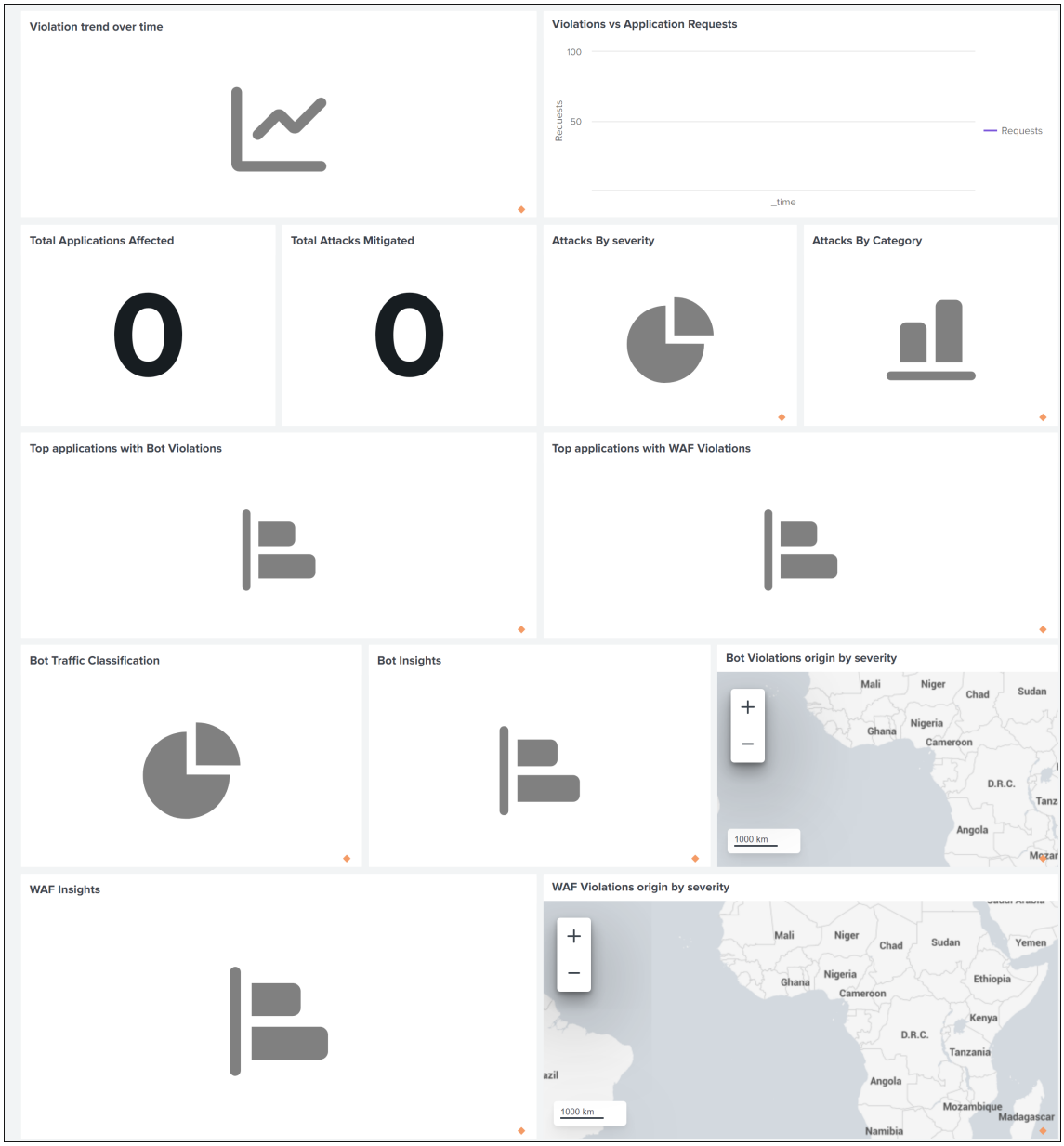
   e) Wählen Sie ein beliebiges Layout (**Absolute** oder **Grid**) aus, und klicken Sie dann auf **Erstellen**.



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 sich das folgende Beispiel-Dashboard in Ihrem Splunk ansehen.



NetScaler Console so konfigurieren, dass Daten nach Splunk exportiert werden

In Splunk haben Sie jetzt alles bereit. Der letzte Schritt besteht darin, NetScaler Console zu konfigurieren, indem Sie ein Abonnement erstellen und das Token hinzufügen.

Nach Abschluss des folgenden Verfahrens können Sie das aktualisierte Dashboard in Splunk anzeigen, das derzeit in Ihrer NetScaler Console verfügbar ist:

1. Melden Sie sich bei NetScaler Console an.
2. Navigieren Sie zu **Einstellungen > Observability Integration**.

3. Klicken Sie auf der Seite **Integrationen** auf **Hinzufügen**.
4. Geben Sie auf der Seite **Abonnement erstellen** die folgenden Details an:

   a) Geben Sie im Feld **Abonnementname einen Namen** Ihrer Wahl ein.

   b) Wählen Sie **NetScaler Console** als **Quelle** aus und klicken Sie auf **Weiter**.

   c) Wählen Sie **Splunk** aus und klicken Sie auf **Konfigurieren**. Auf der Seite **Endpunkt konfigurieren**:

      i. **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.

      ii. **Authentifizierungstoken** − Kopieren Sie das Authentifizierungstoken von Splunk und fügen Sie es ein.

      iii. Klicken Sie auf **Submit**.

   d) Klicken Sie auf **Weiter**.

   e) Klicken Sie auf **Insights hinzufügen**. Auf der Registerkarte **Funktion auswählen** können Sie die Funktionen auswählen, die Sie exportieren möchten, und auf **Ausgewählte hinzufügen** klicken.

   f) Klicken Sie auf **Weiter**.

   g) 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.

   h) Klicken Sie auf **Submit**.

> **Hinweis:**
>
> Die Daten für die ausgewählten Insights werden sofort an Splunk übertragen, nachdem die Verstöße in der NetScaler Console erkannt wurden.

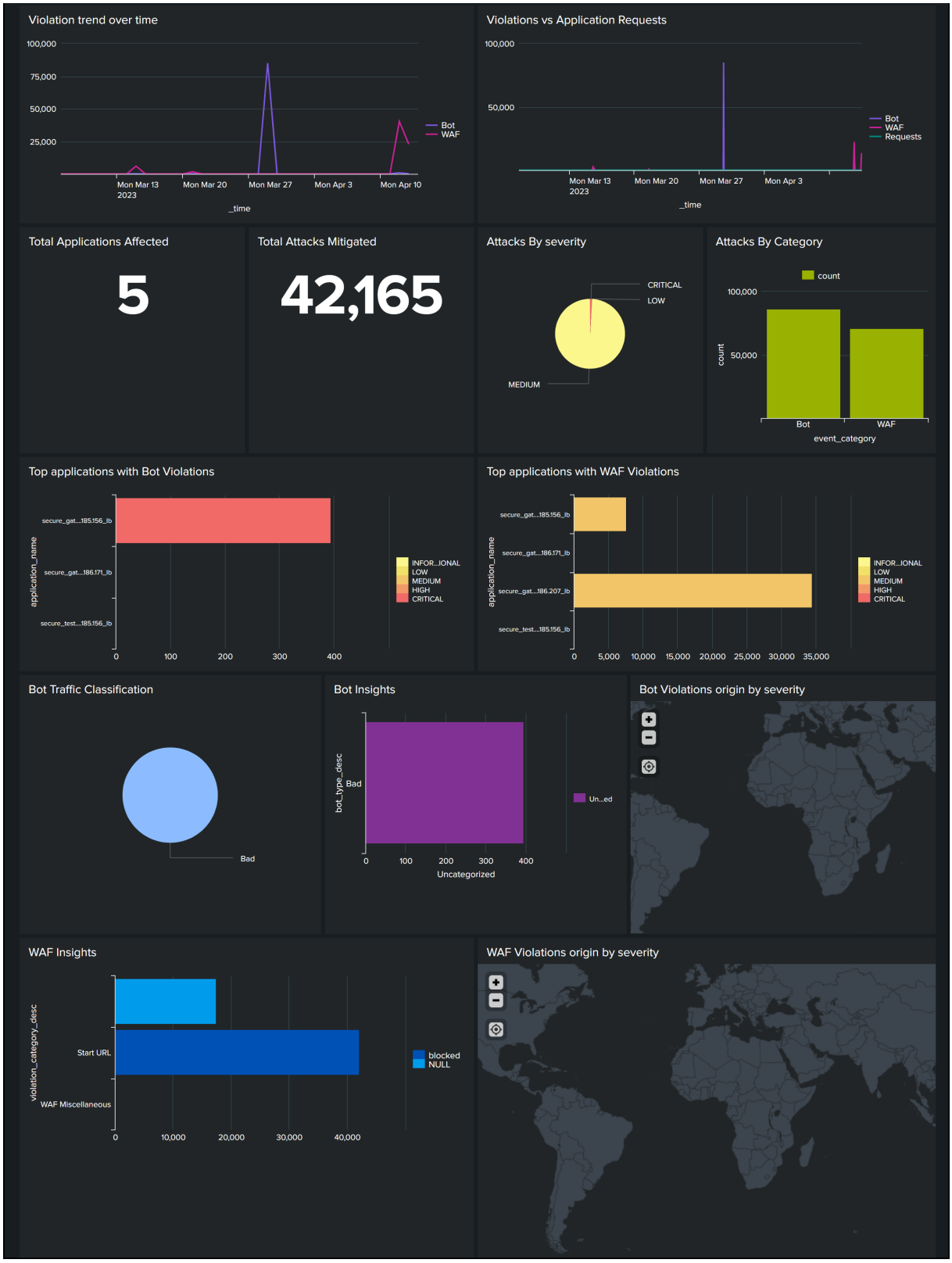
Dashboards in Splunk anzeigen

Nachdem Sie die Konfiguration in NetScaler Console abgeschlossen haben, werden die Ereignisse in Splunk angezeigt.

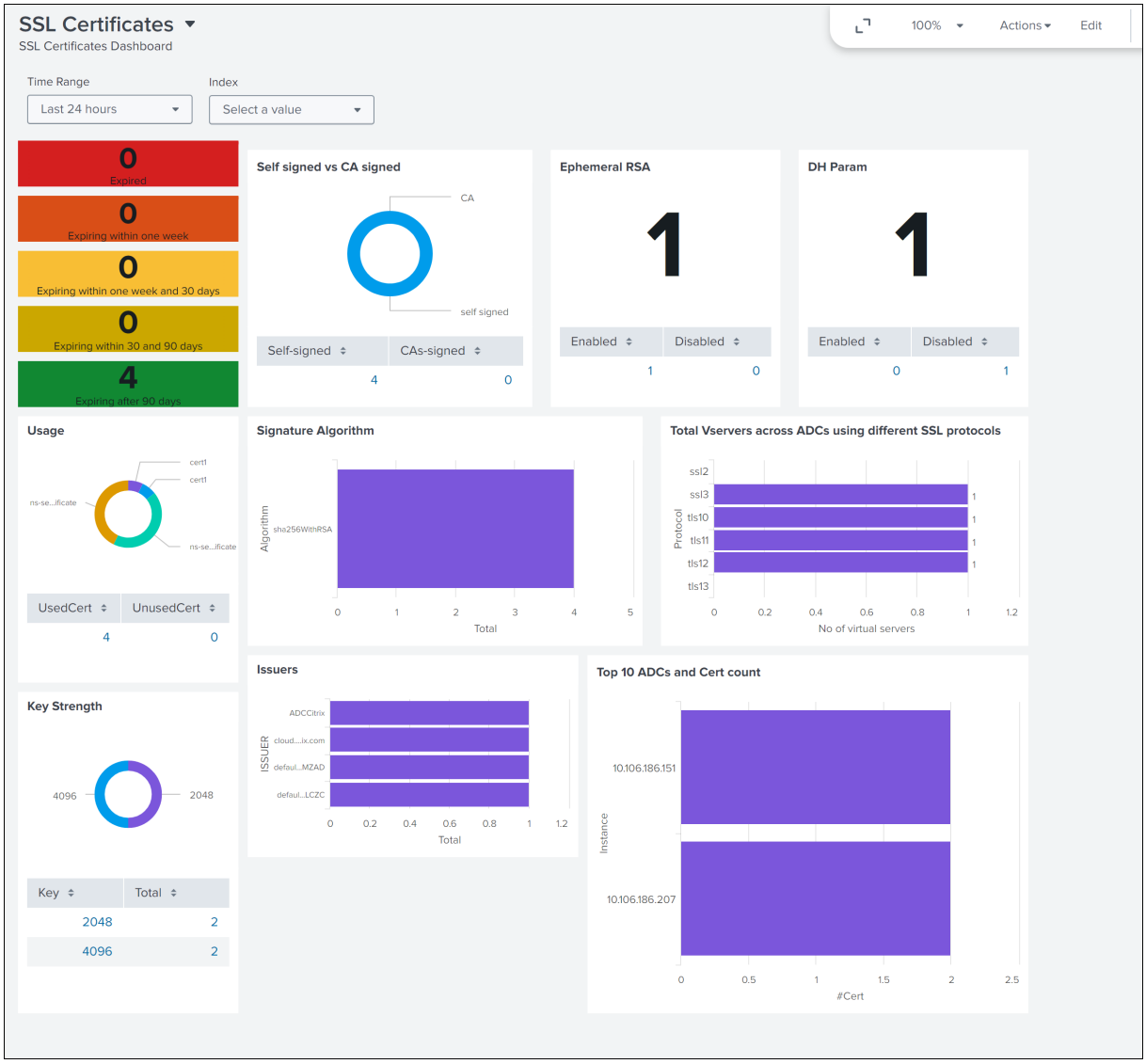
Sie sind bereit, das aktualisierte Dashboard in Splunk ohne weitere Schritte anzuzeigen.

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.



Neben dem Dashboard können Sie auch Daten in Splunk anzeigen, nachdem Sie das Abonnement erstellt haben

1. Klicken Sie in Splunk auf **Search & Reporting**.
2. In der Suchleiste:
    - 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.
    - Geben Sie `sourcetype="gateway_insights"` ein und wählen Sie die Dauer aus der Liste aus, um die Gateway Insights-Daten anzuzeigen.

Integration mit New Relic

July 17, 2024

Sie können NetScaler Console 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 Console erfasst Bot- und WAF-Ereignisse und sendet sie je nach 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.
- Fügen Sie die Schlüsseldetails in NetScaler Console hinzu

Fügen Sie die Schlüsseldetails in NetScaler Console hinzu

Nachdem Sie ein Token generiert haben, müssen Sie zur Integration mit New Relic Details in NetScaler Console hinzufügen.

1. Melden Sie sich bei NetScaler Console an.
2. Navigieren Sie zu **Einstellungen > Observability Integration**.
3. Klicken Sie auf der Seite **Integrationen** auf **Hinzufügen**.
4. Geben Sie auf der Seite **Abonnement erstellen** die folgenden Details an:

a) Geben Sie im Feld **Abonnementname einen Namen** Ihrer Wahl ein.

b) Wählen Sie **NetScaler Console** als **Quelle** aus und klicken Sie auf **Weiter**.

c) Wählen Sie **New Relic** aus und klicken Sie auf **Konfigurieren**. Auf der Seite **Endpunkt konfigurieren**:

   i. **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.

d) **Authentifizierungstoken** —Kopieren Sie das Authentifizierungstoken von New Relic und fügen Sie es ein.

   i. Klicken Sie auf **Submit**.

e) Klicken Sie auf **Weiter**.

f) Klicken Sie auf **Insights hinzufügen**. Auf der Registerkarte **Funktion auswählen** können Sie die Funktionen auswählen, die Sie exportieren möchten, und auf **Ausgewählte hinzufügen** klicken.

g) Klicken Sie auf **Weiter**.

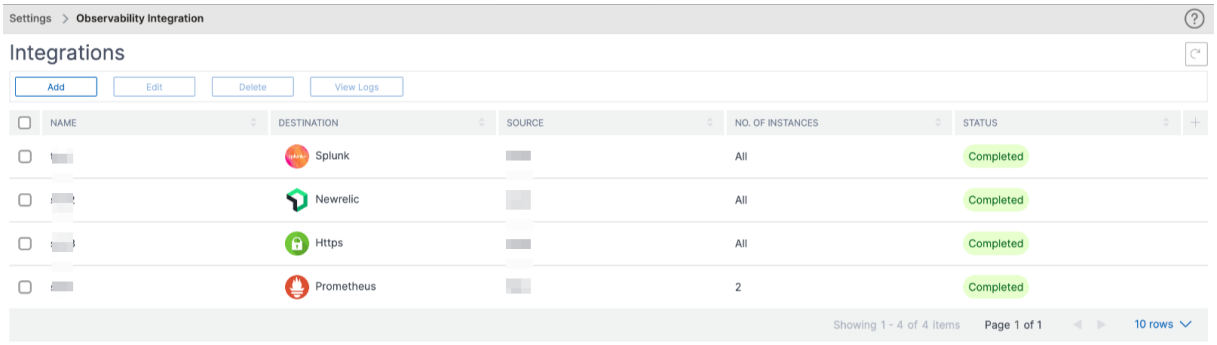
h) Auf der Registerkarte **Instanz auswählen** können Sie entweder **Alle Instanzen auswählen** oder **Benutzerdefiniert auswählen**und dann auf **Weiter**klicken.

- **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.

i) Klicken Sie auf **Submit**.

> **Hinweis:**
>
> - Die Daten für die ausgewählten Erkenntnisse werden sofort an New Relic übertragen, nachdem die Verstöße in der NetScaler Console erkannt wurden.

Die Konfiguration ist abgeschlossen. Einzelheiten können Sie auf der Seite **Abonnements** einsehen.

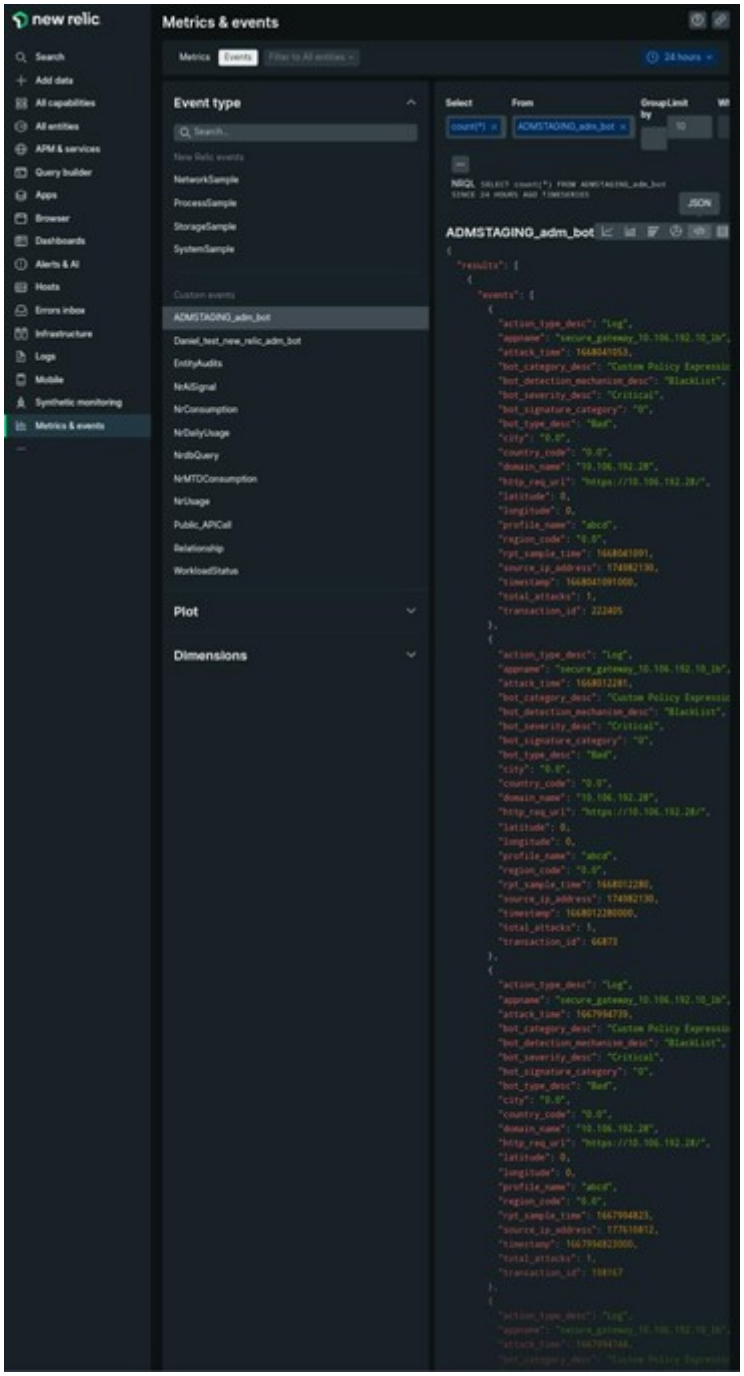


New Relic Dashboard

Wenn die Ereignisse in New Relic exportiert werden, können Sie die Ereignisdetails unter **Metriken und Ereignisse** im folgenden JSON-Format anzeigen:

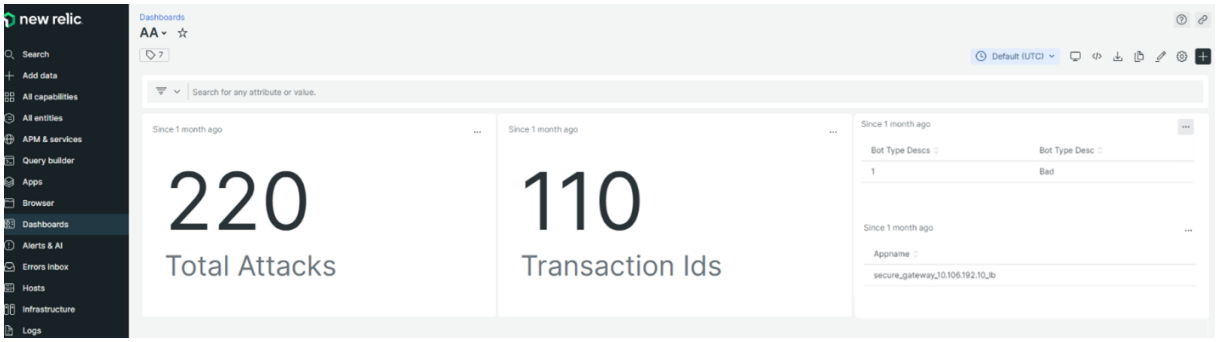
<subsription_name>_adm_<event name> wobei der Eventname Bot, WAF usw. sein kann.

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
  ```

Integration mit Microsoft Sentinel

September 2, 2024

Sie können NetScaler Console in Microsoft Sentinel integrieren, um die folgenden Analysen von NetScaler Console nach Microsoft Sentinel zu exportieren:

- Verstöße gegen die WAF
- Bot-Verstöße
- Einblicke in SSL-Zertifikate
- Gateway insight

Microsoft Sentinel bietet eine zentralisierte Datenerfassung, bei der Daten aus verschiedenen Quellen wie Anwendungen, Servern usw. erfasst werden. Als Administrator können Sie Daten einsehen und Entscheidungen treffen, nachdem die Erkenntnisse oder Verstöße in Microsoft Sentinel gemeldet wurden.

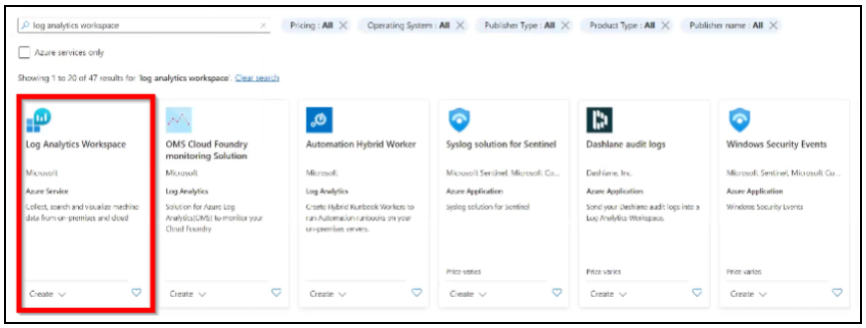
Stellen Sie für eine erfolgreiche Integration sicher, dass Sie über ein aktives Azure-Abonnement verfügen, und folgen Sie dann den Anweisungen in den einzelnen Abschnitten:

Den Log Analytics-Arbeitsbereich konfigurieren

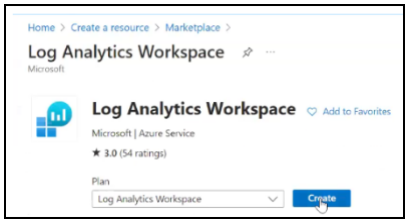
Ein Log Analytics Workspace ist erforderlich, um die gesammelten Daten zu speichern und zu analysieren.

1. Melden Sie sich bei Azure an.
2. Klicken Sie auf **Eine Ressource erstellen**.

3. Geben Sie in der Suchleiste Log Analytics Workspace ein und klicken Sie unter **Log Analytics Workspace** auf **Erstellen**.



4. Klicken Sie auf der Hauptseite von **Log Analytics Workspace** auf **Erstellen**.



5. Gehen **Sie im Workspace "Log Analytics erstellen"** wie folgt vor:

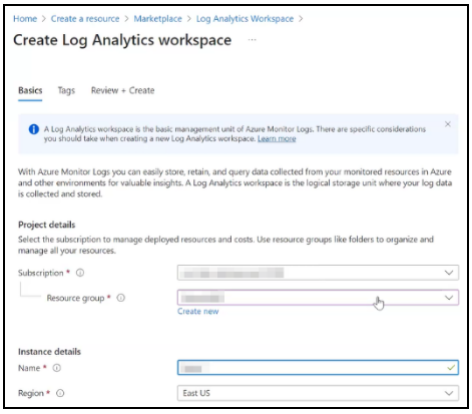
   a) Wählen Sie das aktive Abonnement und die Ressourcengruppe aus.

   > **Hinweis:**
   >
   > Sie können auch auf **Neu erstellen** klicken, um eine Ressourcengruppe hinzuzufügen, sofern Sie über die entsprechende Berechtigung verfügen.

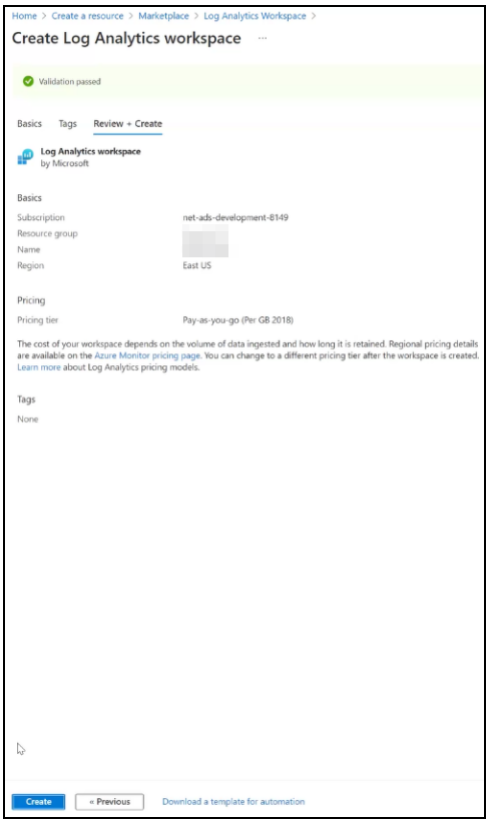
   b) Geben Sie einen Namen Ihrer Wahl an.

c) Wählen Sie Ihre Region aus der Liste aus.

d) Klicken Sie auf **Überprüfen und Erstellen**.



e) Eine Meldung über bestandene Überprüfung wird angezeigt. Klicken Sie auf **Erstellen**, um den Workspace bereitzustellen.



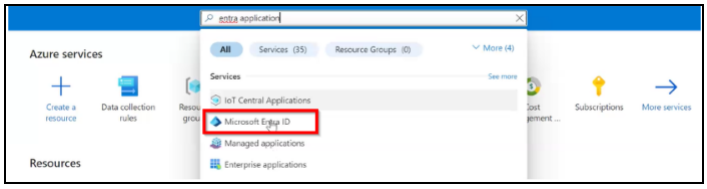
f) Sie können die Meldung "Bereitstellung läuft"sehen. Nachdem die Meldung "Bereitstellung abgeschlossen"angezeigt wird, klicken Sie auf **Gehe zur Ressource**.

Der Workspace wurde erfolgreich erstellt.

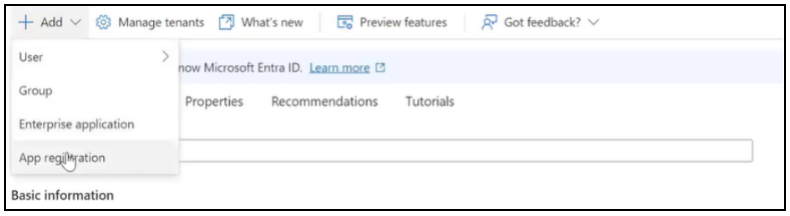
Erstellen Sie eine Microsoft Entra-Anwendung

Sie müssen eine Entra-Anwendung erstellen, die Ihrem Azure-Abonnement zugeordnet ist, um im Namen von Log Analytics Workspace zu kommunizieren. Nachdem Sie die Anwendung erstellt haben, müssen Sie auch die Berechtigung für die **Microsoft Sentinel Contributor-Rolle** erteilen. Die Anwendung enthält auch Details wie **Kunden-ID**, **Mandanten-ID** und **Kundengeheimnis**. Wir empfehlen Ihnen, sich diese Angaben zu notieren. Diese Angaben sind erforderlich, wenn Sie in NetScaler Console ein Abonnement erstellen, um den Integrationsprozess abzuschließen.

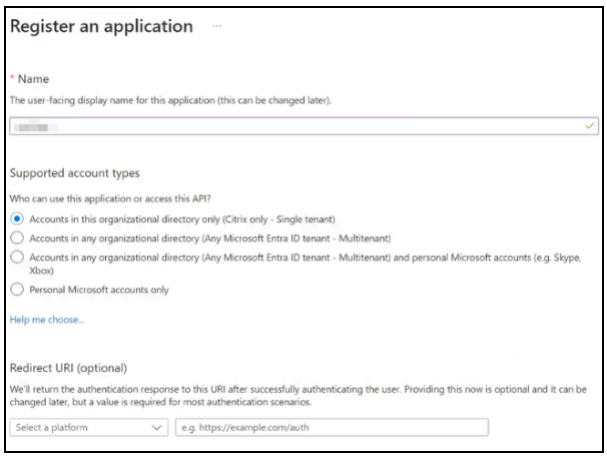
1. Geben Sie in Ihrem Azure-Portal das Schlüsselwort in die Suchleiste ein.
2. Klicken Sie auf **Microsoft Entra ID**.



3. Klicken Sie auf **Hinzufügen** und wählen Sie **App-Registrierung** aus.

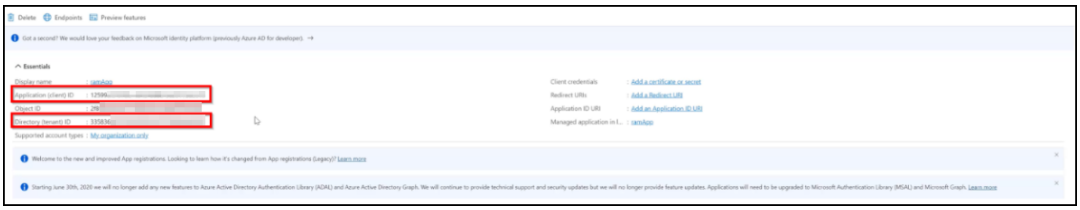


4. Geben Sie einen Namen für die App an, wählen Sie die Standardoption unter **Unterstützte Kontotypen** aus, und klicken Sie dann auf **Registrieren**.



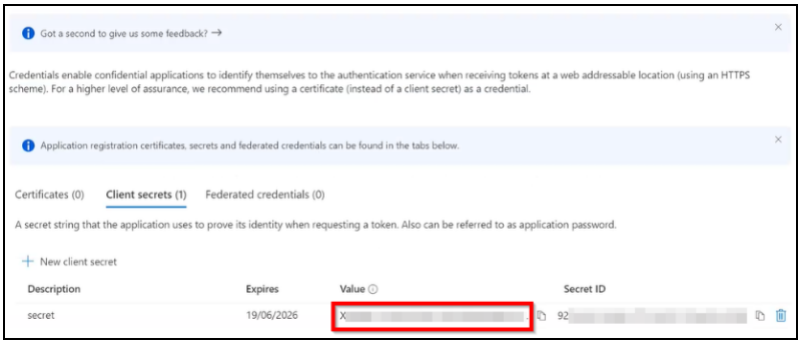
5. Nachdem Sie die Anwendung registriert haben:

   a) Notieren Sie sich die **Kunden-ID** und die **Mandanten-ID**.



   b) Erstellen Sie eine geheime ID für Ihre Anwendung. Klicken Sie auf **Zertifikate und Geheimnisse** und unter **Kundengeheimnisse** auf **Neues Kundengeheimnis**. Geben Sie eine Beschreibung und Gültigkeit ein und klicken Sie dann auf **Hinzufügen**, um eine geheime ID für Ihre Anwendung zu erstellen.

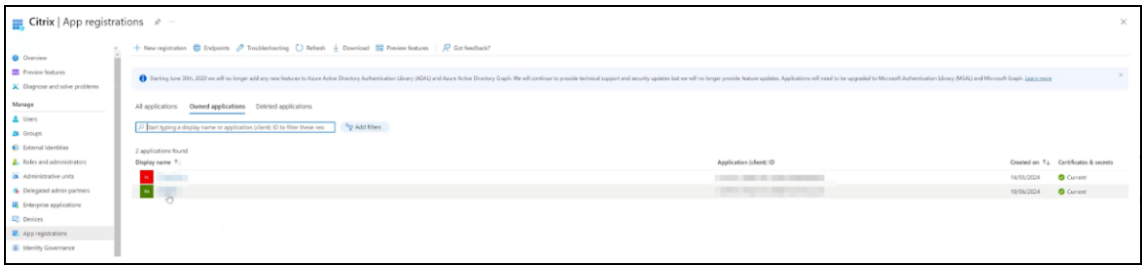
   c) Die Details werden für Ihre Anwendung angezeigt. Stellen Sie sicher, dass Sie sich die unter **Wert** angezeigte ID sofort nach der Erstellung des Geheimnisses notieren. Dieser Wert wird ausgeblendet, wenn Sie zu einer anderen GUI-Option navigieren.



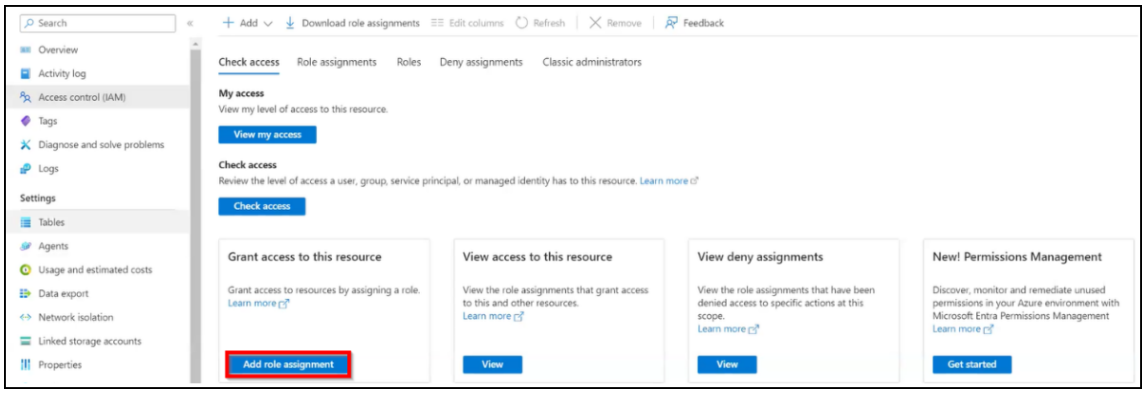
Erteilen Sie die Erlaubnis für die Entra-Anwendung

Sie müssen der Anwendung die Microsoft Sentinel Contributor-Rolle zuweisen. Um eine Genehmigung zu erteilen:

1. Navigieren Sie in Ihrem Azure-Portal zur Microsoft Entra-ID.
2. Klicken Sie auf **App-Registrierungen** und wählen Sie dann Ihre Anwendung aus.



3. Klicken Sie **auf Zugriffskontrolle (IAM)** und dann auf **Rollenzuweisung hinzufügen**.

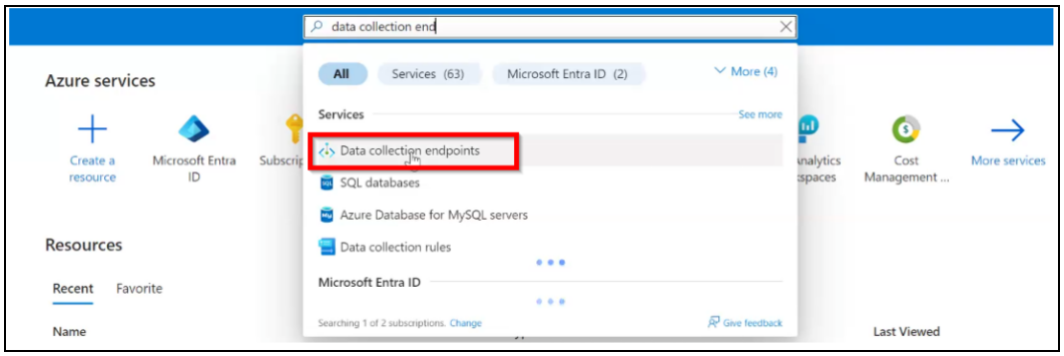


4. Geben Sie in der Suchleiste das Schlüsselwort Sentinel ein, wählen Sie **Microsoft Sentinel Contributor** aus und klicken Sie auf **Weiter**.
5. Klicken Sie auf der Registerkarte **Mitglieder** auf **Mitglieder auswählen** und wählen Sie die Entra-App aus, die Sie erstellt haben.
6. Klicken Sie auf **Überprüfen und Zuweisen**.

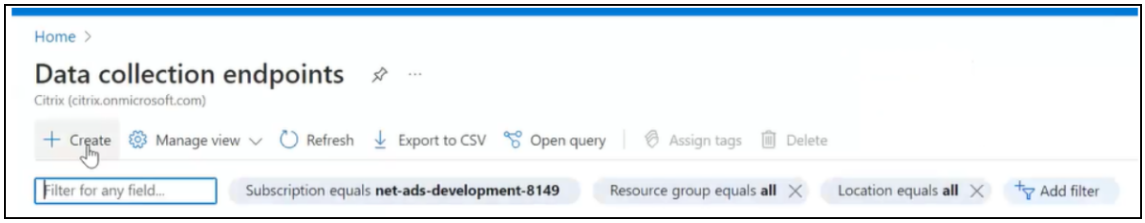
Datenerfassungsendpunkt konfigurieren

Sie müssen einen Datenerfassungsendpunkt erstellen, um die Endpunkt-URL abzurufen. Dies ist erforderlich, wenn Sie ein Abonnement in NetScaler Console erstellen.

1. Wählen Sie in Ihrem Azure-Portal unter **Azure-Dienste** die Option **Datenerfassungsendpunkte** aus, oder geben Sie das Schlüsselwort in die Suchleiste ein.



2. Klicken Sie auf der Seite **Datenerfassungsendpunkte** auf **Erstellen**.



3. Unter **Datenerfassungsendpunkt erstellen**:

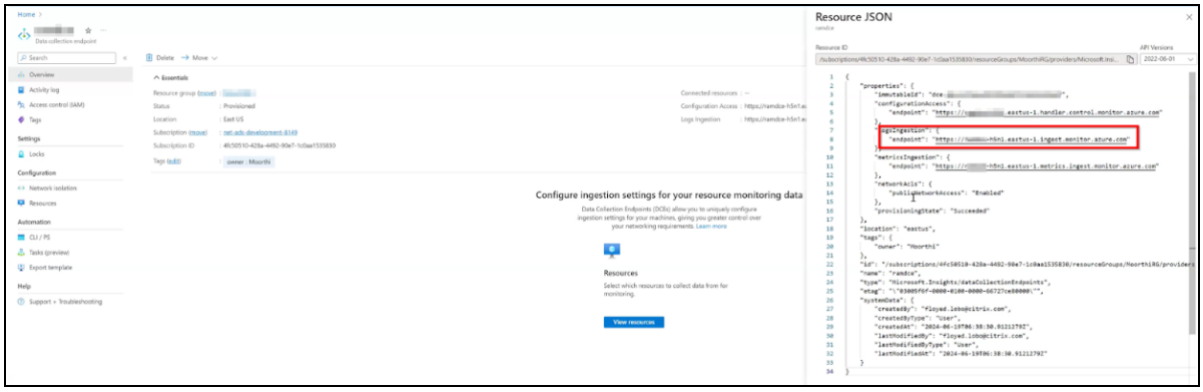
   a) Geben Sie einen Endpunktnamen Ihrer Wahl an

   b) Wählen Sie das **Abonnement, die Ressourcengruppe** und die **Region** aus.

   c) Klicken Sie auf **Überprüfen und Erstellen**.

   d) Nachdem die Meldung “Validierung bestanden”angezeigt wird, klicken Sie auf **Erstellen**.

Sie müssen sich die Endpunkt-URL notieren. Wählen Sie auf der Hauptseite des **Datenerfassungsendpunkts** den erstellten Endpunkt aus, klicken Sie auf **JSON-Ansicht** und notieren Sie sich die Endpunkt-ID.



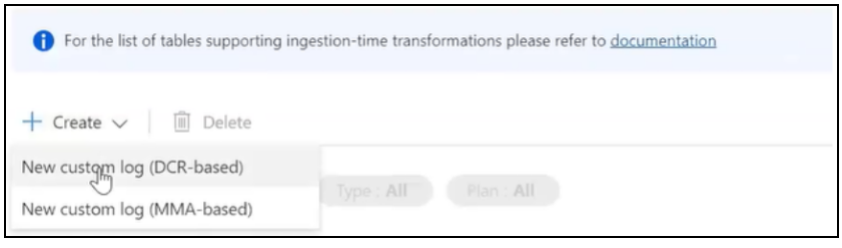
Erstellen Sie Tabellen zum Exportieren von Daten

Sie müssen eine Tabelle erstellen und die JSON-Informationen für jeden Einblick angeben, den Sie von NetScaler Console nach Microsoft Sentinel exportieren möchten. Sie können sich auf die folgenden Details zu den Tabellenanforderungen für jeden Einblick beziehen:

Insights	Gesamtzahl der benötigten Tabellen
Einblicke in SSL	3
WAF	1
Bot	1
Gateway Insights	5

Für jeden Workspace können Sie maximal 10 Tabellen erstellen. Bei mehr als 10 Tabellen müssen Sie einen weiteren Workspace erstellen.

1. Navigieren Sie im Azure-Portal zu Ihrem Workspace und klicken Sie unter **Einstellungen** auf **Tabellen**.
2. Klicken Sie auf **Erstellen** und wählen Sie **Neues benutzerdefiniertes Protokoll (DCR-basiert)**



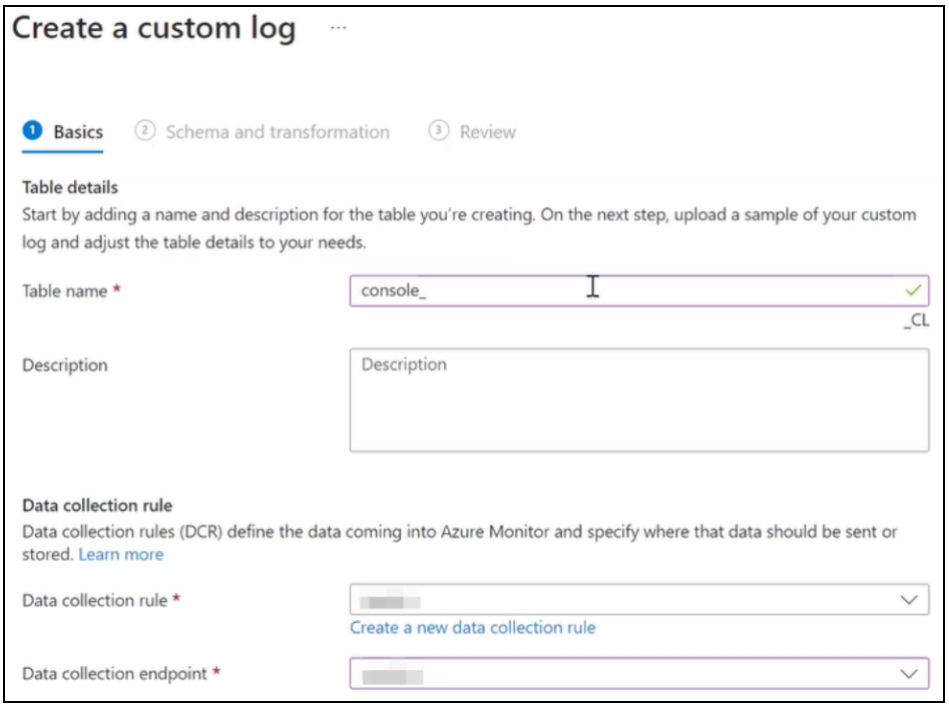
3. In **Benutzerdefiniertes Protokoll erstellen**:

a) Geben Sie einen Tabellennamen an. Der Tabellenname muss das Format **console_insightname** haben. Zum Beispiel: **console_ns_sslvserver**, **console_ns_ssl_certkey**. In Schritt 4 finden Sie die Tabellennamen, die für jeden Insight gelten.

b) Geben Sie eine Beschreibung ein, um weitere Informationen zum Tabellennamen hinzuzufügen. Dies ist optional.

c) Erstellen Sie eine neue Datenerfassungsregel und fügen Sie sie hinzu.

d) Wählen Sie den Datenerfassungsendpunkt aus der Liste aus.



e) Klicken Sie auf **Weiter**.

4. Auf der Registerkarte **Schema und Transformation** müssen Sie die JSON-Beispielprotokolle für die Erkenntnisse hochladen, die Sie exportieren möchten. Sie können das folgende JSON-Beispiel für jeden Insight verwenden und eine JSON-Datei zum Hochladen erstellen:

Insights	JSON	Zu verwendender Tabellenname

Insights	JSON	Zu verwendender Tabellenname
SSL (1)	{ "id": "3eb05733-c326-493c-9aa0-f7db3a6b4277", " ns_ip_address": " 10.106.186.141", " name": " zeta_192_168_110_250" , "vsvr_ip_address": "", "vsvr_port": -1, "vsvr_type": "", " state": "", " partition_name": "", "display_name": " 10.106.186.141", " poll_time": 1716539986, "managed" : "f", "ssl2": "f", " ssl3": "t", "tls10": "t", "tls11": "t", " tls12": "t", "dh": "f ", "ersa": "t", " sslprofile": "", " tls13": "f", " dhkeyexpsizelimit": " DISABLED", " pushenctriggertimeout ": 1, "sessionticket" : "", " includesubdomains": " f", " sessionticketkeyrefresh ": "", "ssllogprofile ": "", "serverauth": "", " ssltriggertimeout": 100, "ersacount": 0, "strictcachecks": "NO ", "dhfile": "", " sessreuse": "ENABLED" , " redirectportrewrite":	console_ns_sslvserver

Insights	JSON	Zu verwendender Tabellenname
SSL (2)	{ "id": "a6673ab2-0b59-47b9-b530-bc30fb2b937c", "ssl_certificate": "/nsconfig/ssl/ca-cert.pem", "ssl_key": "/nsconfig/ssl/ca-key.pem", "certkeypair_name": "athul-ca", "cert_format": "PEM", "days_to_expiry": 281, "ns_ip_address": "10.106.186.141", "status": "Valid", "device_name": "10.106.186.141", "file_location_path": "", "certificate_data": "", "key_data": "", "poll_time": 1717434335, "no_domain_check": "f", "version": 3, "serial_number": "7B34B6A6A1A79E0FF168242D7BCFF78F04C9EE66", "signature_algorithm": "sha256WithRSAEncryption", "issuer": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "valid_from": "Mar 12 08:51:11 2024 GMT", "valid_to": "Mar 12 08:51:11 2025 GMT", "subject": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "public_key_algorithm": "rsaEncryption", "public_key_size":	console_ns_ssl_certkey

Insights	JSON	Zu verwendender Tabellenname
SSL (3)	{ "id": "2baffd1a-7ed6-4035-91e8-ad3a3125bff4", "certkeypair_name": "cert1", "ns_ip_address": "10.106.186.127", "poll_time": 1715671567, "partition_name": "", "display_name": "10.106.186.127", "hostname": "", "entity_name": "secure_gateway", "entity_type": "sslvserver", "table_name": "ns_sslcertkey_binding"}	console_ns_sslcertkey_binding

Insights	JSON	Zu verwendender Tabellenname
WAF	[{ "ip_address": "10.106.185.156", "ctnsappname": "vserver_1", "severity": 2, "violation_type": 19, "violation_type_desc": "Start URL", "block_flags": 1, "transformed_flags": 0, "not_blocked_flags": 0, "country_code": "-NA-", "region_code": "-NA-", "city": "-NA-", "latitude": 200.0, "longitude": 200.0, "signature_category": "", "attack_category": 2, "attack_category_desc": "Broken Authentication and Session Management", "total_attacks": 1, "rpt_sample_time": 1704783773, "source_ip_address": 174766492, "attack_time": 1704783538, "profile_name": "appfw_cs_lb_prof", "session_id": "", "http_req_url": "https://10.106.192.54/csrf_ffc/ffc.html?field10=asfasd", "violation_name": "-NA-", "violation_value": "-NA-", "violation_location": 4, "	console_af_threat_exporter_data_l2

Insights	JSON	Zu verwendender Tabellenname
Bot	{ "ip_address": "10.106.186.122", "ctnsappname": "secure_gateway", "bot_type": "2", "bot_type_desc": "Bad", "action_type": "6", "action_type_desc": "Log", "country_code": "0.0", "region_code": "0.0", "city": "0.0", "bot_severity": "0", "bot_severity_desc": "Critical", "latitude": "0", "longitude": "0", "bot_detection_mechanism": "6", "bot_detection_mechanism_desc": "BlackList", "bot_category": "0", "bot_category_desc": "Uncategorized", "source_ip_address": "174758625", "bot_signature_category": "Custom Policy Expression", "appname": "secure_gateway_10.106.186.122_lb", "backend_vserver": "", "backend_appname": "", "total_attacks": "2", "rpt_sample_time": "1718783216", "table_name": "af_bot_attack_details_l2"}	console_af_bot_attack_details_l2

Insights	JSON	Zu verwendender Tabellenname
Gateway Insight (1)	{ "adc_ip_address": "10.106.186.141", "auth_server": "", "client_ip": 174766732, "epa_method_type": 0, "error_count": 14, "error_details": "Invalid credentials passed", "error_type": 1, "gateway_name": "vpn_vserver_142_6", "req_url": "", "resource": "", "rpt_sample_time": 1713505215, "sso_method_type": 0, "sta_ip": "", "table_name": "af_vpn_error_details", "username": "John"}	console_af_vpn_error_details
Gateway Insight (2)	{ "adc_ip_address": "10.102.71.166", "display_name": "10.102.71.166", "gateway_name": "firsthop", "ip_address": "10.102.71.168", "rpt_sample_time": "1718812158", "state": "Up", "table_name": "ns_vpnvserver"}	console_ns_vpnvserver

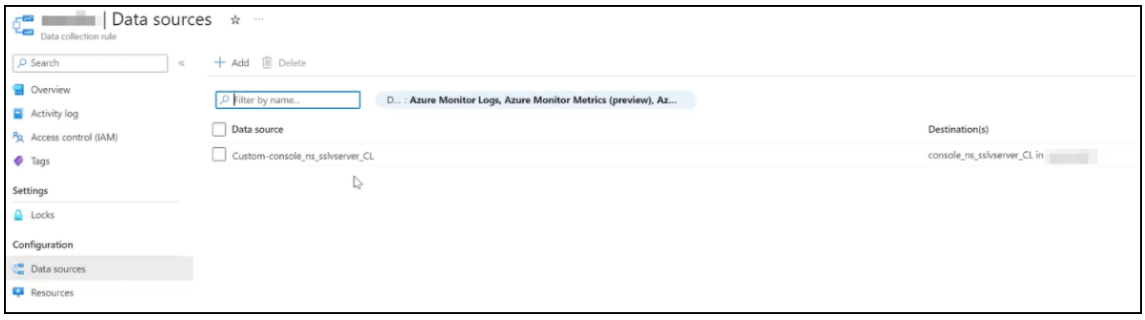
Insights	JSON	Zu verwendender Tabellenname
Gateway Insight (3)	{ "adc_ip_address": "10.106.186.141", "gateway_name": "vpn_vserver_141_7", "rpt_sample_time": 1702011308, "sessions": 1, "table_name": "af_vpn_session_details", "users": 1 }	console_af_vpn_session_details
Gateway Insight (4)	{ "active_sessions": 59, "active_users": 1, "adc_ip_address": "10.106.186.136", "gateway_name": "vpnathul2", "rpt_sample_time": 1698919848, "table_name": "af_vpn_active_session_1"}	console_af_vpn_active_session_1
Gateway Insight (5)	{ "adc_ip_address": "10.106.186.136", "entity_type": 3, "gateway_name": "vpnathul2", "hits": 3, "rpt_sample_time": 1698052438, "table_name": "af_vpn_error_reports" }	console_af_vpn_error_reports

Nach dem Hochladen der JSON-Datei können Sie die folgenden Details einsehen:

Klicken Sie auf **Transformationseditor**, geben Sie die folgende Abfrage ein, die für den entsprechenden Einblick gilt, und klicken Sie auf **Ausführen**, um die Daten ab der Abfragezeit in NetScaler Console zu akzeptieren.

- **SSL** - `source | extend TimeGenerated = todatetime(poll_time)| project-rename sslvserver_id = id`
- **WAF** und **Bot** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`
- **Gateway Insight** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`

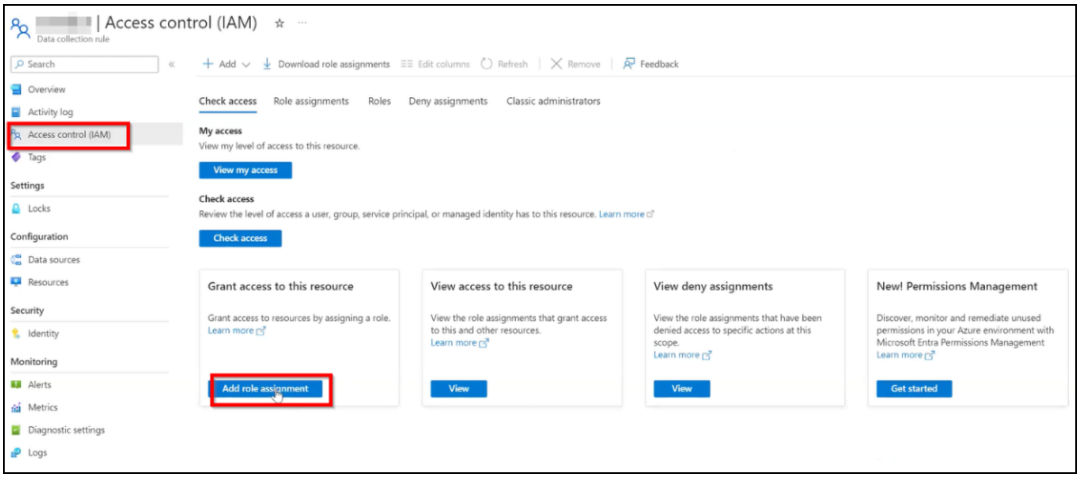
5. Klicken Sie auf **Weiter** und dann auf **Erstellen**, um den Vorgang abzuschließen.
6. Navigieren Sie zu **Datenerfassungsregeln** und klicken Sie auf den DCR, den Sie erstellt haben.
7. Klicken Sie unter **Konfiguration** auf **Datenquellen**, um die erstellte Tabelle anzuzeigen.



Die DCR (Data Collection Rule) erfordert Zugriff auf die Rolle **Monitoring Metrics Publisher**.

a) Navigieren Sie zu Ihrem DCR, auf den Sie in Ihrem Azure-Portal unter **Zuletzt verwendet** zugreifen können.

b) Klicken Sie auf Ihrer DCR-Seite auf **Zugriffskontrolle (IAM)** und dann auf **Rollenzuweisung hinzufügen**.



c) Geben Sie in der Suchleiste den Keyword-Monitor ein, um **Monitoring Metrics Publisher** auszuwählen, und klicken Sie auf **Weiter**.

d) Klicken Sie auf der Registerkarte **Mitglieder** auf **Mitglieder auswählen** und wählen Sie die Entra-App aus, die Sie erstellt haben.

e) Klicken Sie auf **Überprüfen und Zuweisen**.

Sie müssen sich die ID der Datenerfassungsregeln notieren. Navigieren Sie zur Seite mit den Datenerfassungsregeln, wählen Sie Ihren DCR aus und klicken Sie auf die JSON-Ansicht, um sich die ID zu notieren.

Abonnement in NetScaler Console erstellenm

Sie sind jetzt bereit. Der letzte Schritt besteht darin, NetScaler Console zu konfigurieren, indem Sie ein Abonnement erstellen und die erforderlichen Details hinzufügen. Um ein Abonnement in NetScaler Console zu erstellen, benötigen Sie die folgenden Details, die Sie notiert haben:

- Endpunkt-URL
- ID der Datenerfassungsregeln

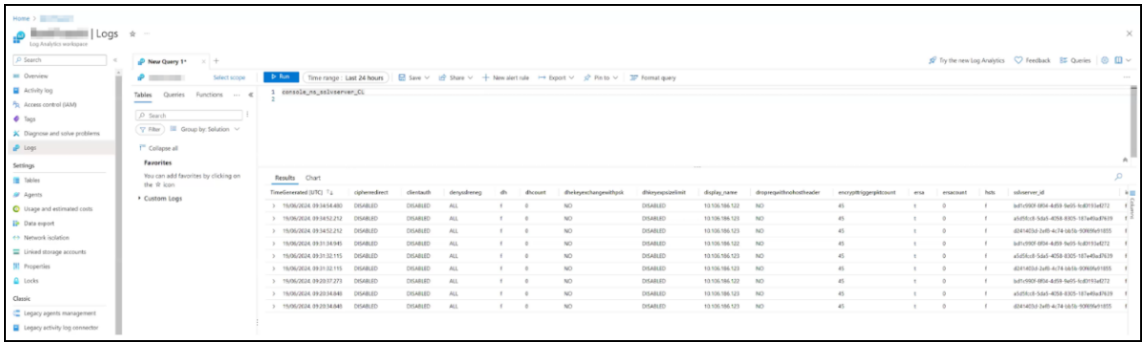
- Mandanten-ID
- Client-ID
- Geheimer Clientschlüssel

1. Melden Sie sich bei NetScaler Console an.
2. Navigieren Sie zu **Einstellungen > Observability Integration**.
3. Klicken Sie auf der Seite **Integrationen** auf **Hinzufügen**.
4. Geben Sie auf der Seite **Abonnement erstellen** die folgenden Details an:
    a) Geben Sie im Feld Abonnementname einen Namen Ihrer Wahl ein.
    b) Wählen Sie **NetScaler Console** als **Quelle** aus und klicken Sie auf **Weiter**.
    c) Wählen Sie **Microsoft Sentinel** aus und klicken Sie auf **Konfigurieren**. Geben Sie auf der Seite **Endpunkt konfigurieren** alle Details ein und klicken Sie auf **Senden**.
    d) Klicken Sie auf **Weiter**.
5. Klicken Sie auf **Insights hinzufügen** und wählen Sie auf der Registerkarte **Feature auswählen**, abhängig von den Tabellen, die Sie in Microsoft Azure hinzugefügt haben, die Features aus, die Sie exportieren möchten, und klicken Sie auf **Ausgewählte hinzufügen** und dann auf **Weiter**.
6. 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 Microsoft Sentinel.
    - **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 Microsoft Sentinel exportiert.
7. Klicken Sie auf **Submit**.

Protokolle in Microsoft Azure anzeigen

Nachdem Sie alles konfiguriert haben, empfehlen wir Ihnen, bis zu 30 Minuten zu warten, um die Details in Microsoft Azure anzuzeigen.

1. Navigieren Sie in Ihrem Azure-Portal zu Ihrem **Log Analytics-Arbeitsbereich**.
2. Klicken Sie auf **Protokolle**, geben Sie den Tabellennamen ein und klicken Sie auf **Ausführen**, um die Ergebnisse anzuzeigen.



NetScaler-Instanzen für den Export von Insights nach Prometheus mit dem Standardschema konfigurieren

September 2, 2024

NetScaler unterstützt den direkten Export von Metriken nach Prometheus. Sie können den umfangreichen Satz von Metriken verwenden, die von der NetScaler-Instanz bereitgestellt werden, um den NetScaler-Zustand und den Anwendungszustand zu überwachen. Sie können beispielsweise Metriken zur CPU- und Speichernutzung sammeln, um den Zustand von NetScaler zu ermitteln. In ähnlicher Weise können Sie Metriken wie die Anzahl der pro Sekunde empfangenen HTTP-Anfragen oder die Anzahl der aktiven Clients verwenden, um den Zustand der Anwendung zu überwachen.

Um die Metriken nach Prometheus zu exportieren, müssen Sie ein Analyseprofil mit dem Typ Zeitreihe konfigurieren. Weitere Informationen finden Sie unter Überwachen von NetScaler, Anwendungen und Anwendungssicherheit mit Prometheus.

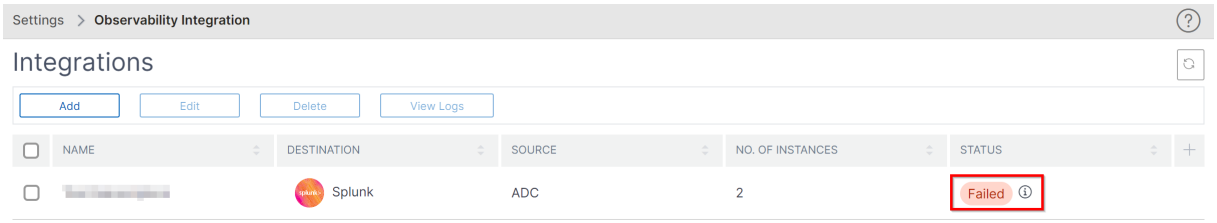
Mit der Observability-Integrationsfunktion in NetScaler Console können Sie den Export von Erkenntnissen nach Prometheus mithilfe des Standardschemas konfigurieren.

1. Navigieren Sie zu **Einstellungen > Observability Integration**.
2. Klicken Sie auf der Seite **Integrationen** auf **Hinzufügen**.
3. Geben Sie auf der Seite **Abonnement erstellen** die folgenden Details an:
    a) Geben Sie im Feld **Abonnementname einen Namen** Ihrer Wahl ein.
    b) Wählen Sie **NetScaler** als **Quelle** aus und klicken Sie auf **Weiter**.
    c) Wählen Sie **Prometheus** als Ziel aus.
    d) Wählen Sie **Standard** für die Standard-Einblicke in die exportierten Daten aus.
    e) Klicken Sie auf **Instanzen hinzufügen** und wählen Sie die Instances aus, für die Sie Erkenntnisse nach Prometheus exportieren möchten.

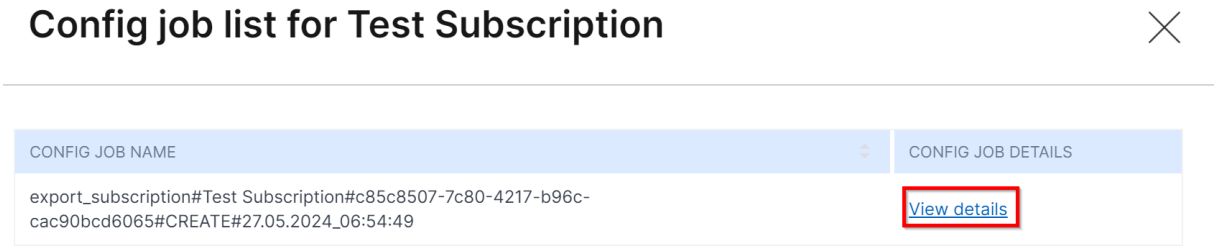
f) Klicken Sie auf **Submit**.

Protokolle für fehlgeschlagene Konfigurationen anzeigen

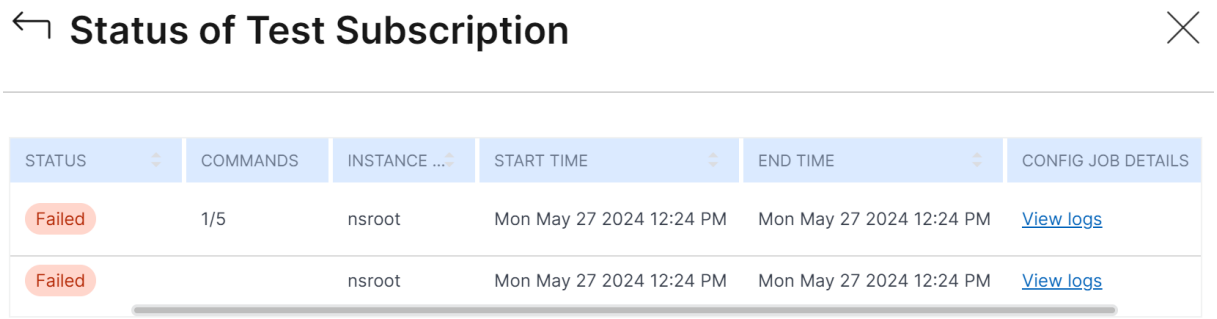
Nachdem Sie ein Abonnement erstellt haben, können Sie den Status des erstellten Abonnements unter **Settings > Observability Integration**einsehen. Wenn der Status **Fehlgeschlagen** lautet, klicken Sie hier, um Details anzuzeigen.



Klicken Sie unter **Auftragsdetails konfigurieren** auf **Details anzeigen**.



Klicken Sie auf **Protokolle anzeigen**, um Details zum Problem anzuzeigen.



Export von NetScaler-Metriken und Auditprotokollen nach Splunk konfigurieren

September 2, 2024

NetScaler unterstützt den direkten Export von Metriken nach Splunk im JSON-Format. NetScaler bietet umfangreiche Metriken zur Überwachung des Zustands Ihrer Anwendungen und der Anwen-

dungssicherheit. Durch den Export der von NetScaler bereitgestellten Metriken nach Splunk können Sie die Metriken visualisieren und aussagekräftige Einblicke gewinnen.

Mithilfe der Prüfprotokollierung können Sie die NetScaler-Zustände und Statusinformationen protokollieren, die von verschiedenen Modulen in NetScaler gesammelt wurden. Durch die Überprüfung der Protokolle können Sie Probleme oder Fehler beheben und beheben.

Weitere Informationen:

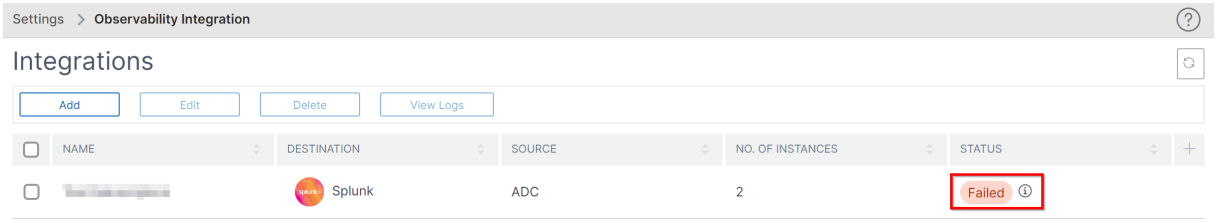
- Auditprotokolle direkt von NetScaler nach Splunk exportieren
- Metriken direkt von NetScaler nach Splunk exportieren

So konfigurieren Sie den Export von Metriken und Audit-Logs nach Splunk über NetScaler Console:

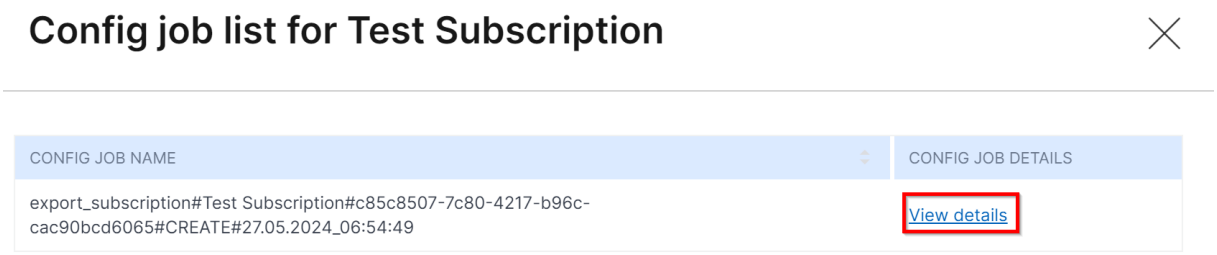
1. Navigieren Sie zu **Einstellungen > Observability Integration**.
2. Klicken Sie auf der Seite **Integrationen** auf **Hinzufügen**.
3. Geben Sie auf der Seite **Abonnement erstellen** die folgenden Details an:
    a) Geben Sie im Feld **Abonnementname einen Namen** Ihrer Wahl ein.
    b) Wählen Sie **NetScaler** als **Quelle** aus und klicken Sie auf **Weiter**.
    c) Wählen Sie **Splunk** als **Ziel** aus und klicken Sie auf **Konfigurieren**. Unter Endpunkt konfigurieren:
        - **Endpunkt-URL** – Geben Sie die Splunk-Endpunktdetails an. Der Endpunkt muss das Format `<https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event>` haben.
        - **Authentifizierungstoken** – Kopieren Sie das Authentifizierungstoken von Splunk und fügen Sie es ein.
        - Klicken Sie auf **Submit**.
    d) Klicken Sie auf **Weiter**.
    e) Klicken Sie auf **Insights hinzufügen** und wählen Sie **NetScaler Metrics** und **NetScaler-Auditprotokolle** aus, und klicken Sie dann auf **Ausgewählte hinzufügen**.
    f) Klicken Sie auf **Weiter**.
    g) Klicken Sie auf **Instanzen hinzufügen** und wählen Sie die Instanzen aus.
    h) Klicken Sie auf **Submit**.

Protokolle für fehlgeschlagene Konfigurationen anzeigen

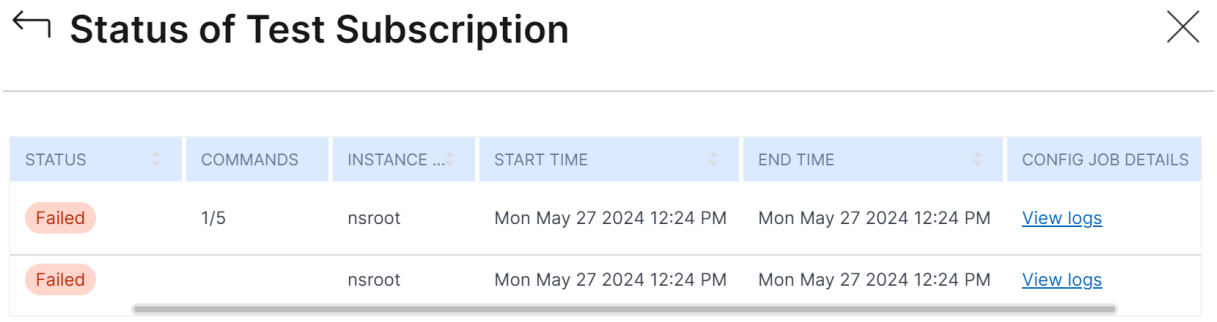
Nachdem Sie ein Abonnement erstellt haben, können Sie den Status des erstellten Abonnements unter **Settings > Observability Integration**einsehen. Wenn der Status **Fehlgeschlagen** lautet, klicken Sie hier, um Details anzuzeigen.



Klicken Sie unter **Auftragsdetails konfigurieren** auf **Details anzeigen**.



Klicken Sie auf **Protokolle anzeigen**, um Details zum Problem anzuzeigen.



Analytics-Einstellungen konfigurieren

January 26, 2024

Bevor Sie beginnen, die Analytics-Funktion in der NetScaler Console zu verwenden, um Einblick in Ihre Instanz- und Anwendungsdaten zu erhalten, wird empfohlen, einige Analyseeinstellungen zu konfigurieren, um eine optimale Nutzung dieser Funktion zu gewährleisten.

Schwellenwerte und Warnungen für Analytics erstellen

Sie können Schwellenwerte und Warnungen festlegen, um die Analytics-Metriken der verwalteten virtuellen Server zu überwachen, die auf den erkannten Instanzen konfiguriert sind. Wenn der Wert einer Metrik den Schwellenwert überschreitet, generiert NetScaler Console ein Ereignis, das auf eine Schwellenwertverletzung hinweist.

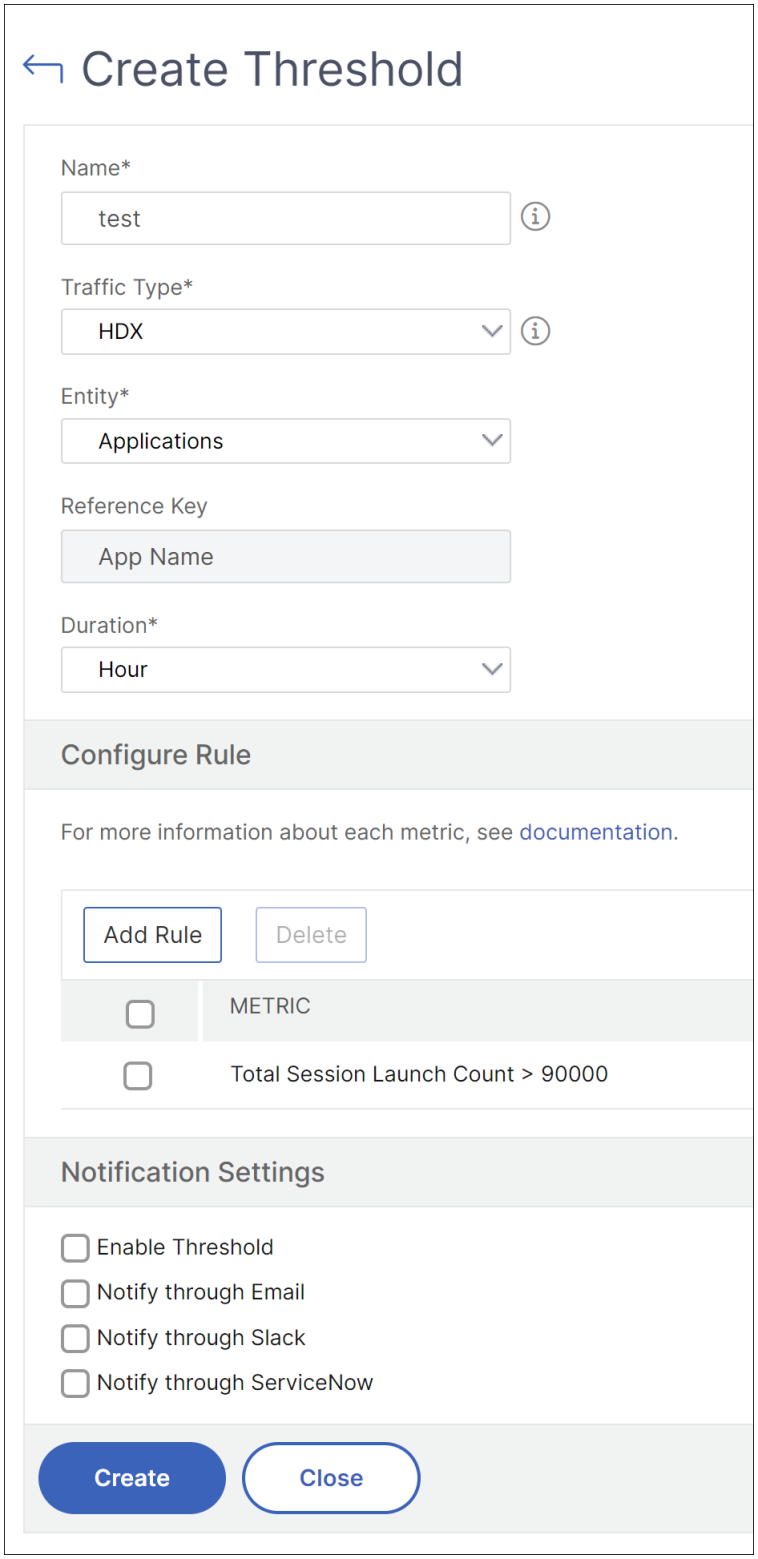
Sie können Aktionen auch den festgelegten Schwellenwerten zuordnen. Zu den Aktionen gehören das Anzeigen einer Warnung auf der GUI und das Senden von E-Mails wie konfiguriert.

Sie können beispielsweise einen Schwellenwert festlegen, um ein Ereignis für HDX Insight zu generieren, wenn der ICA-RTT-Wert eines Benutzers 1 Sekunde überschreitet. Sie können auch Warnungen für das generierte Ereignis aktivieren und die Informationen zur Verletzung des Schwellenwerts an eine konfigurierte E-Mail-Liste senden.

So erstellen Sie Schwellenwerte und Warnungen für Analysen:

1. Navigieren Sie zu **Einstellungen** > **Analytics-Einstellungen** > **Schwellenwerte**.
2. Klicken Sie im Bildschirm **Schwellenwerte** auf **Hinzufügen**, um einen neuen Schwellenwert hinzuzufügen und Alarme für die festgelegten Schwellenwerte zu konfigurieren.
3. Geben Sie auf der Seite **Schwellenwerte und Warnungen erstellen** die folgenden Details an:
    - **Name** —Name für die Konfiguration des Schwellenwerts.
    - **Traffic-Typ** —Art des Analytics-Datenverkehrs, für den Sie den Schwellenwert konfigurieren möchten. Zum Beispiel: HDX Insight, Security Insight.
    - **Entität** —Kategorie oder Ressourcentyp, für die Sie den Schwellenwert konfigurieren möchten.
    - **Referenzschlüssel** —Automatisch generierter Wert basierend auf dem ausgewählten Traffic-Typ und der ausgewählten Entität.
    - **Dauer** —Intervall, für das Sie den Schwellenwert konfigurieren möchten.
4. Um E-Mail-Benachrichtigungen zu konfigurieren, aktivieren Sie das Kontrollkästchen für die festgelegten Schwellenwerte.
5. Geben Sie im Abschnitt **Regeln** Folgendes an:
    - **Metrik** —Metrik für den ausgewählten Traffic-Typ zum Konfigurieren des Schwellenwerts.
    - **Komparator** —Vergleicher zur ausgewählten Metrik (zum Beispiel: <, > =).
    - **Wert** —Wert für die Metrik zum Festlegen des Schwellenwerts und zum Aufrufen von Alerts.

6. Klicken Sie auf **Erstellen**.



Benachrichtigungen konfigurieren

January 26, 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 Console-Lizenz .
- **SSL-Zertifikate** —Liste der SSL-Zertifikate, die NetScaler-Instanzen hinzugefügt werden. Weitere Informationen finden Sie unter Ablauf des SSL-Zertifikats

NetScaler Console unterstützt die folgenden Benachrichtigungstypen:

- E-Mail
- SMS
- Slack
- PagerDuty
- ServiceNow

Für jeden Benachrichtigungstyp zeigt die NetScaler Console-GUI die konfigurierte Verteilerliste oder das konfigurierte Profil an. Die NetScaler Console sendet Benachrichtigungen an die ausgewählte Verteilerliste oder das ausgewählte Profil.

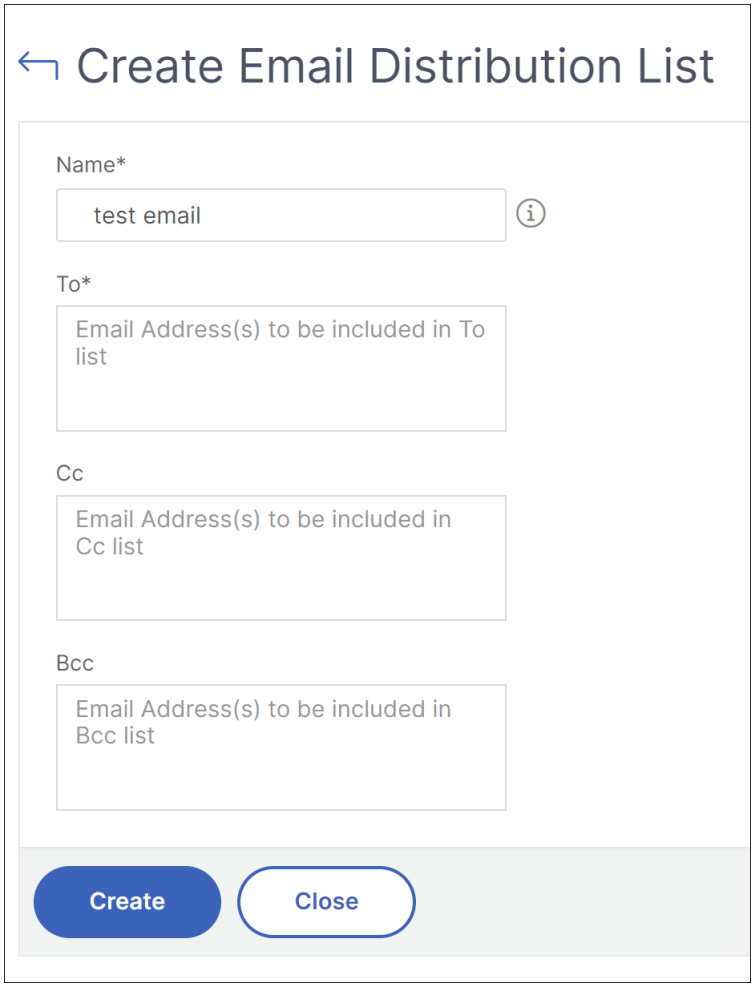
Erstellen einer E-Mail-Verteilerliste

Um E-Mail-Benachrichtigungen für NetScaler Console-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.
    - **An**—Geben Sie die E-Mail-Adressen an, an die NetScaler Console Nachrichten senden muss.

- **Cc**—Geben Sie die E-Mail-Adressen an, an die NetScaler Console Nachrichtenkopien senden muss.
- **Bcc**—Geben Sie die E-Mail-Adressen an, an die NetScaler Console 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 E-Mail-Verteilerlisten angezeigt, die in NetScaler Console vorhanden sind.

Erstellen Sie eine SMS-Verteilerliste

Um SMS-Benachrichtigungen für NetScaler Console-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 NetScaler Console Nachrichten senden muss.
4. Klicken Sie auf **Erstellen**.

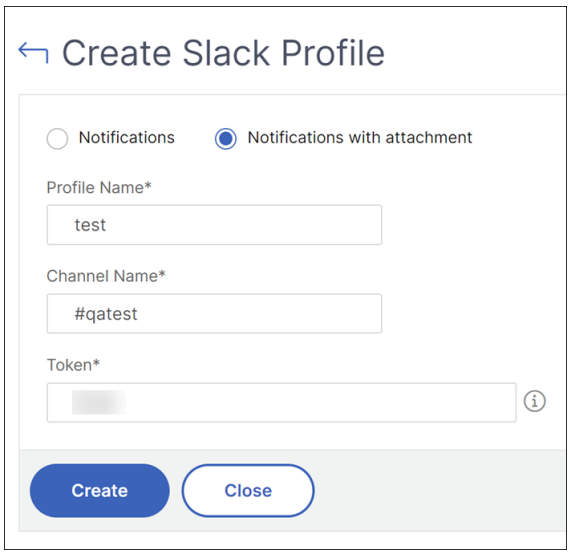
Wiederholen Sie diesen Vorgang zum Erstellen mehrerer SMS-Verteilerlisten. Auf der Registerkarte **SMS** werden alle SMS-Verteilerlisten angezeigt, die in NetScaler Console vorhanden sind.

Erstellen eines Slack Profils

Um Slack-Benachrichtigungen für NetScaler Console-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-Kanals an, an den NetScaler Console 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 einen Webhook ist 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 Slack-Profile angezeigt, die in NetScaler Console vorhanden sind.

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 Console 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 der NetScaler Console vorhandenen PagerDuty-Profile angezeigt.

Das ServiceNow-Profil anzeigen

Wenn Sie ServiceNow-Benachrichtigungen für NetScaler-Ereignisse und NetScaler Console-Ereignisse aktivieren möchten, müssen Sie NetScaler Console mithilfe des ITSM-Connectors in ServiceNow integrieren. Weitere Informationen finden Sie unter Integrieren der NetScaler Console in die 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 Console-GUI anzeigen möchten, wählen Sie **ServiceNow-Tickets** aus.

Exportberichte exportieren oder planen

January 26, 2024

In NetScaler Console können Sie einen umfassenden Bericht für die ausgewählte NetScaler Console-Funktion exportieren. Dieser Bericht bietet Ihnen einen Überblick über die Zuordnung zwischen den Instanzen, Partitionen und entsprechenden Details.

NetScaler Console zeigt funktionsspezifische geplante Exportberichte unter den einzelnen NetScaler Console-Funktionen an, die Sie anzeigen, bearbeiten oder löschen können. Um beispielsweise die Exportberichte von NetScaler-Instanzen anzuzeigen, navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** und klicken Sie auf das Exportsymbol. Sie können diese Berichte im PDF-, JPEG-, PNG- und CSV-Dateiformat exportieren.

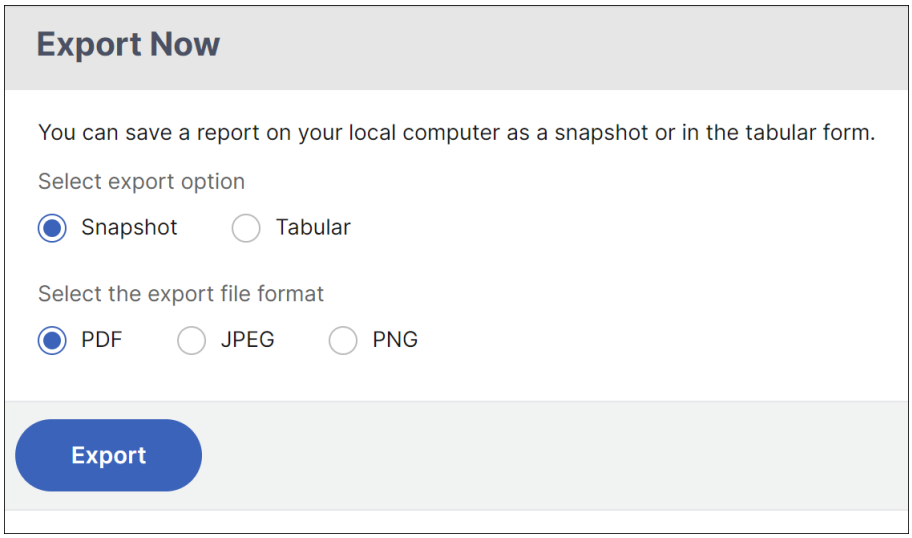
In **Berichte exportieren**können Sie die folgenden Aktionen ausführen:

- Exportieren eines Berichts auf einen lokalen Computer
- Exportberichte planen
- Anzeigen, Bearbeiten oder Löschen der geplanten Exportberichte

Exportieren eines Berichts

Gehen Sie wie folgt vor, um einen Bericht von der NetScaler Console auf den lokalen Computer zu exportieren:

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**—Mit dieser Option werden NetScaler Console-Berichte als Snapshot exportiert.
    - **Tabellarisch**—Mit dieser Option werden NetScaler Console-Berichte in einem tabellarischen Format exportiert. 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**.

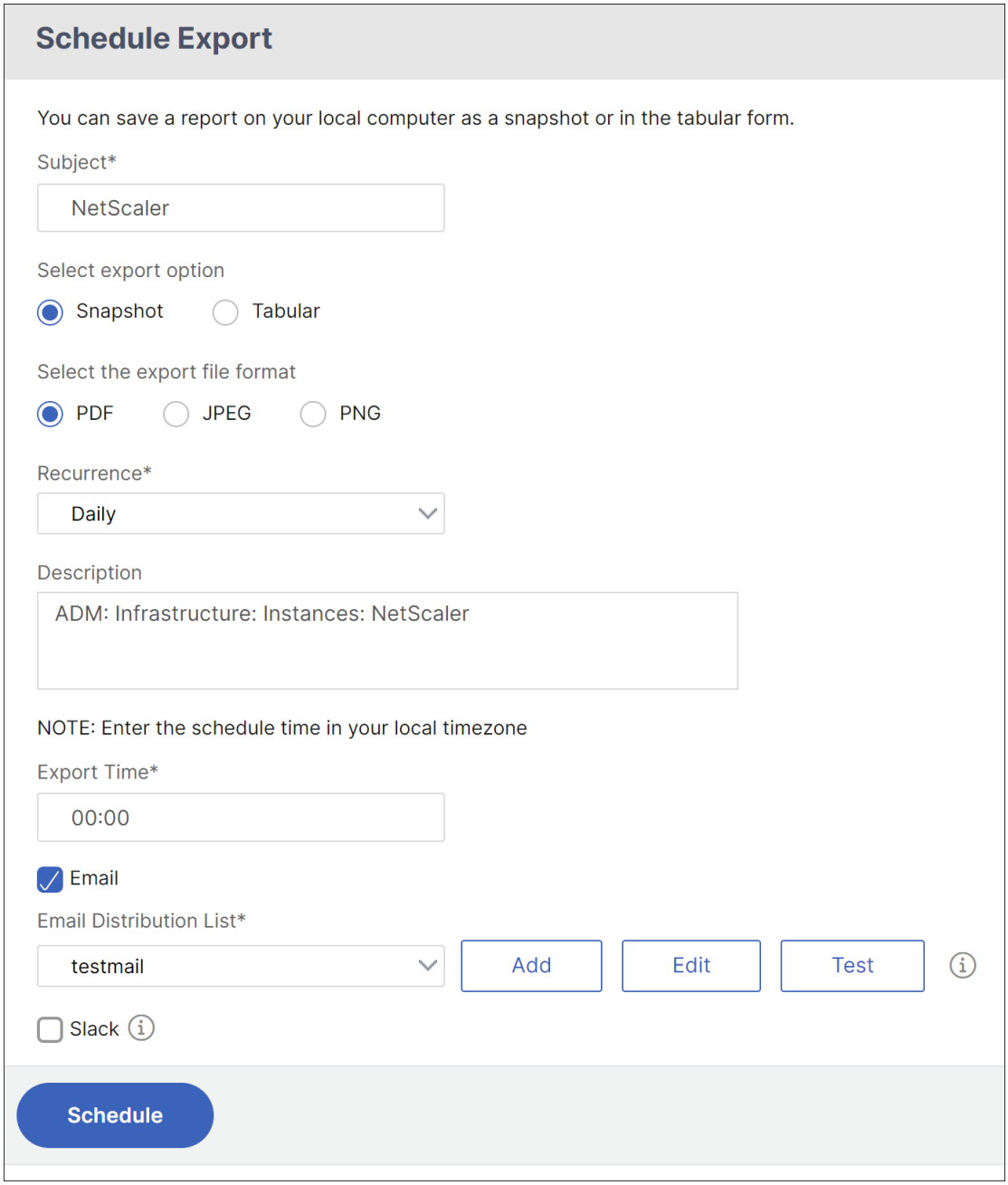
Exportbericht planen

Um den Exportbericht in regelmäßigen Intervallen zu planen, geben Sie das Wiederholungsintervall an. NetScaler Console 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 NetScaler Console-Berichte in einem Snapshot- oder 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**.

Instanzeinstellungen

January 26, 2024

Sie können die erkannten Instanzen in NetScaler Console verwalten und die Einstellungen für das Instanz-Backup konfigurieren.

Instanzkonfiguration verwalten

Unter **Einstellungen > Globale Einstellungen > Instanzeinstellungen > Instanzverwaltung**können Sie die folgenden Instanzkonfigurationen ändern:

- **Kommunikation mit Instanz (en)**—Sie können einen HTTP- oder HTTPS-Kommunikationskanal zwischen NetScaler Console und den erkannten Instanzen wählen.
- **Zertifikatsdownload aktivieren** —Ermöglicht das Herunterladen der SSL-Zertifikate von einer erkannten Instanz.
- **Anmeldedaten für die Instanzanmeldung**abfragen —Wenn Sie über die NetScaler Console-GUI auf die Instanz zugreifen, wird die Instanz-Anmeldeseite angezeigt. Geben Sie Ihre Anmeldeinformationen für den Zugriff auf eine Instanz an.

Konfigurieren der Einstellungen für das Instanzbackup

Unter **Einstellungen > Allgemeine Einstellungen > Instanzeinstellungen > Instanzsicherung können Sie die Backup**-Einstellungen für die erkannten NetScaler-Instanzen in der NetScaler Console konfigurieren.

Wählen Sie unter **Instanzbackupeinstellungen konfigurieren** die Option **Instanzbackup aktivieren**.

- **Anzahl der beizubehaltenden Sicherungsdateien : Geben**Sie die Anzahl der Sicherungsdateien an, die in der NetScaler Console aufbewahrt werden sollen. Sie können bis zu 3 Sicherungsdateien pro NetScaler-Instanz aufbewahren. Die Standardeinstellung ist 1 Sicherungsdatei.
- **Backup-Planungseinstellungen**—Sie können ein Instanz-Backup auf zwei Arten planen:
  - **Intervallbasiert** —**Nach Ablauf des angegebenen Intervalls wird**in NetScaler Console eine Sicherungsdatei erstellt. Das Standardintervall für Backups ist 12 Stunden.
  - **Zeitbasiert**—Geben Sie die Uhrzeit im Format `hours:minutes` an, zu der NetScaler Console das Instanz-Backup durchführen soll.

- **NetScaler-Einstellungen** —Mit dieser Option können Sie ein Backup basierend auf dem Trap initiieren und GeoDB-Dateien in das Backup einbeziehen. Diese Einstellung gilt für MPX-, VPX-, CPX- und BLX-Instanzen.

  - **Instanzsicherung durchführen, wenn der NetScalerConfigSave-Trap empfangen**wird —Standardmäßig erstellt NetScaler Console keine Sicherungsdatei, wenn sie den Trap „NetScalerConfigSave“empfängt. Sie können jedoch die Option aktivieren, eine Sicherungsdatei zu erstellen, wenn eine NetScaler-Instanz einen `NetScalerConfigSave`Trap an NetScaler Console sendet.

    Eine NetScaler-Instanz sendet `NetScalerConfigSave`jedes Mal, wenn die Konfiguration auf der Instanz gespeichert wird.

    Geben Sie die **Verzögerung von Backup bei Trap** in Minuten an Wenn der empfangene `NetScalerConfigSave`Trap für die angegebenen Minuten auf der NetScaler Console bestehen bleibt, sichert NetScaler Console die Instanz.

  - **GeoDB-Dateien**einbeziehen —Standardmäßig erstellt NetScaler Console keine Sicherungskopien der GeoDatabase-Dateien. Sie können die Option aktivieren, um ein Backup dieser Dateien auch zu erstellen.

- **NetScaler SDX-Einstellungen - Um SDX-Instanzen** zu sichern, geben Sie das **Backup-Timeout** in Minuten an. Während einer SDX-Instanzsicherung wird die Verbindung zwischen NetScaler Console und SDX für den angegebenen Zeitraum aufrechterhalten.

  Halten Sie bei großen SDX-Backupdateien die Verbindung zwischen NetScaler Console und SDX-Instanz für einen längeren Zeitraum aufrecht, um den Abschluss der Backup sicherzustellen.

  > **Wichtig:**
  >
  > Das Backup schlägt fehl, wenn bei der Verbindung ein Timeout auftritt.

- **Externe Übertragung**—NetScaler Console ermöglicht es Ihnen, die Backup-Dateien der NetScaler-Instanz an einen externen Speicherort zu übertragen:

  1. Geben Sie die IP-Adresse des Standorts an.
  2. Geben Sie den Benutzernamen und das Kennwort des externen Servers an, auf den Sie die Backupdateien übertragen möchten.
  3. Geben Sie das Übertragungsprotokoll und die Portnummer an.
  4. Geben Sie den Verzeichnispfad an, in dem die Datei gespeichert werden muss.
  5. Wenn Sie die Backupdatei löschen möchten, nachdem Sie die Datei auf einen externen Server übertragen haben, wählen Sie **Datei nach der Übertragung aus Anwendungsbereitstellungsverwaltung löschen**aus.

Instanzeinstellungen

January 26, 2024

Sie können die erkannten Instanzen in NetScaler Console verwalten und die Einstellungen für das Instanz-Backup konfigurieren.

Instanzkonfiguration verwalten

Unter **Einstellungen > Globale Einstellungen > Instanzeinstellungen > Instanzverwaltung**können Sie die folgenden Instanzkonfigurationen ändern:

- **Kommunikation mit Instanz (en)**—Sie können einen HTTP- oder HTTPS-Kommunikationskanal zwischen NetScaler Console und den erkannten Instanzen wählen.
- **Zertifikatsdownload aktivieren** —Ermöglicht das Herunterladen der SSL-Zertifikate von einer erkannten Instanz.
- **Anmeldedaten für die Instanzanmeldung**abfragen —Wenn Sie über die NetScaler Console-GUI auf die Instanz zugreifen, wird die Instanz-Anmeldeseite angezeigt. Geben Sie Ihre Anmeldeinformationen für den Zugriff auf eine Instanz an.

Konfigurieren der Einstellungen für das Instanzbackup

Unter **Einstellungen > Allgemeine Einstellungen > Instanzeinstellungen > Instanzsicherung können Sie die Backup**-Einstellungen für die erkannten NetScaler-Instanzen in der NetScaler Console konfigurieren.

Wählen Sie unter **Instanzbackupeinstellungen konfigurieren** die Option **Instanzbackup aktivieren**.

- **Anzahl der beizubehaltenden Sicherungsdateien : Geben**Sie die Anzahl der Sicherungsdateien an, die in der NetScaler Console aufbewahrt werden sollen. Sie können bis zu 3 Sicherungsdateien pro NetScaler-Instanz aufbewahren. Die Standardeinstellung ist 1 Sicherungsdatei.
- **Backup-Planungseinstellungen**—Sie können ein Instanz-Backup auf zwei Arten planen:
  - **Intervallbasiert** —**Nach Ablauf des angegebenen Intervalls wird**in NetScaler Console eine Sicherungsdatei erstellt. Das Standardintervall für Backups ist 12 Stunden.
  - **Zeitbasiert**—Geben Sie die Uhrzeit im Format `hours:minutes` an, zu der NetScaler Console das Instanz-Backup durchführen soll.

- **NetScaler-Einstellungen** —Mit dieser Option können Sie ein Backup basierend auf dem Trap initiieren und GeoDB-Dateien in das Backup einbeziehen. Diese Einstellung gilt für MPX-, VPX-, CPX- und BLX-Instanzen.

  - **Instanzsicherung durchführen, wenn der NetScalerConfigSave-Trap empfangen**wird —Standardmäßig erstellt NetScaler Console keine Sicherungsdatei, wenn sie den Trap „NetScalerConfigSave“empfängt. Sie können jedoch die Option aktivieren, eine Sicherungsdatei zu erstellen, wenn eine NetScaler-Instanz einen `NetScalerConfigSave`Trap an NetScaler Console sendet.

    Eine NetScaler-Instanz sendet `NetScalerConfigSave`jedes Mal, wenn die Konfiguration auf der Instanz gespeichert wird.

    Geben Sie die **Verzögerung von Backup bei Trap** in Minuten an Wenn der empfangene `NetScalerConfigSave`Trap für die angegebenen Minuten auf der NetScaler Console bestehen bleibt, sichert NetScaler Console die Instanz.

  - **GeoDB-Dateien**einbeziehen —Standardmäßig erstellt NetScaler Console keine Sicherungskopien der GeoDatabase-Dateien. Sie können die Option aktivieren, um ein Backup dieser Dateien auch zu erstellen.

- **NetScaler SDX-Einstellungen - Um SDX-Instanzen** zu sichern, geben Sie das **Backup-Timeout** in Minuten an. Während einer SDX-Instanzsicherung wird die Verbindung zwischen NetScaler Console und SDX für den angegebenen Zeitraum aufrechterhalten.

  Halten Sie bei großen SDX-Backupdateien die Verbindung zwischen NetScaler Console und SDX-Instanz für einen längeren Zeitraum aufrecht, um den Abschluss der Backup sicherzustellen.

  > **Wichtig:**
  >
  > Das Backup schlägt fehl, wenn bei der Verbindung ein Timeout auftritt.

- **Externe Übertragung**—NetScaler Console ermöglicht es Ihnen, die Backup-Dateien der NetScaler-Instanz an einen externen Speicherort zu übertragen:

  1. Geben Sie die IP-Adresse des Standorts an.
  2. Geben Sie den Benutzernamen und das Kennwort des externen Servers an, auf den Sie die Backupdateien übertragen möchten.
  3. Geben Sie das Übertragungsprotokoll und die Portnummer an.
  4. Geben Sie den Verzeichnispfad an, in dem die Datei gespeichert werden muss.
  5. Wenn Sie die Backupdatei löschen möchten, nachdem Sie die Datei auf einen externen Server übertragen haben, wählen Sie **Datei nach der Übertragung aus Anwendungsbereitstellungsverwaltung löschen**aus.

Systemkonfigurationen

January 26, 2024

Sie können das Keep-Alive-Intervall des NetScaler Console-Agents und die NetScaler Console-Serverzeitzone ändern.

Keep-Alive-Intervall des Agenten festlegen

NetScaler Console-Server und -Agent behalten für das angegebene Keep-Alive-Intervall dieselbe TCP-Verbindung bei. Ein Agent verwendet diese Verbindung, um die Daten der verwalteten Instanzen an den NetScaler Console-Server zu senden.

1. Navigieren Sie zu **Einstellungen > Allgemeine Einstellungen**.
2. Wählen Sie unter **Systemkonfigurationen** die Option **Agent und Zeitzone** aus.
3. Geben Sie in **Agent**das Keep-Alive-Intervall zwischen 30 und 120 Sekunden an.
4. Klicken Sie auf **Speichern**.

Stellen Sie die NetScaler Console-Zeitzone ein

Sie können die Zeitzone auswählen, in der Sie die Uhrzeit auf der NetScaler Console-Webseite, in Benachrichtigungen und Berichten anzeigen möchten.

1. Navigieren Sie zu **Einstellungen > Allgemeine Einstellungen**.
2. Wählen Sie unter **Systemkonfigurationen** die Option **Agent und Zeitzone** aus.
3. **Wählen Sie unter Zeitzone die lokale oder GMT-Zeitzone aus, um die Uhrzeit in der NetScaler Console anzuzeigen.
4. Klicken Sie auf **Speichern**.

E-Mail-Abonnements

January 26, 2024

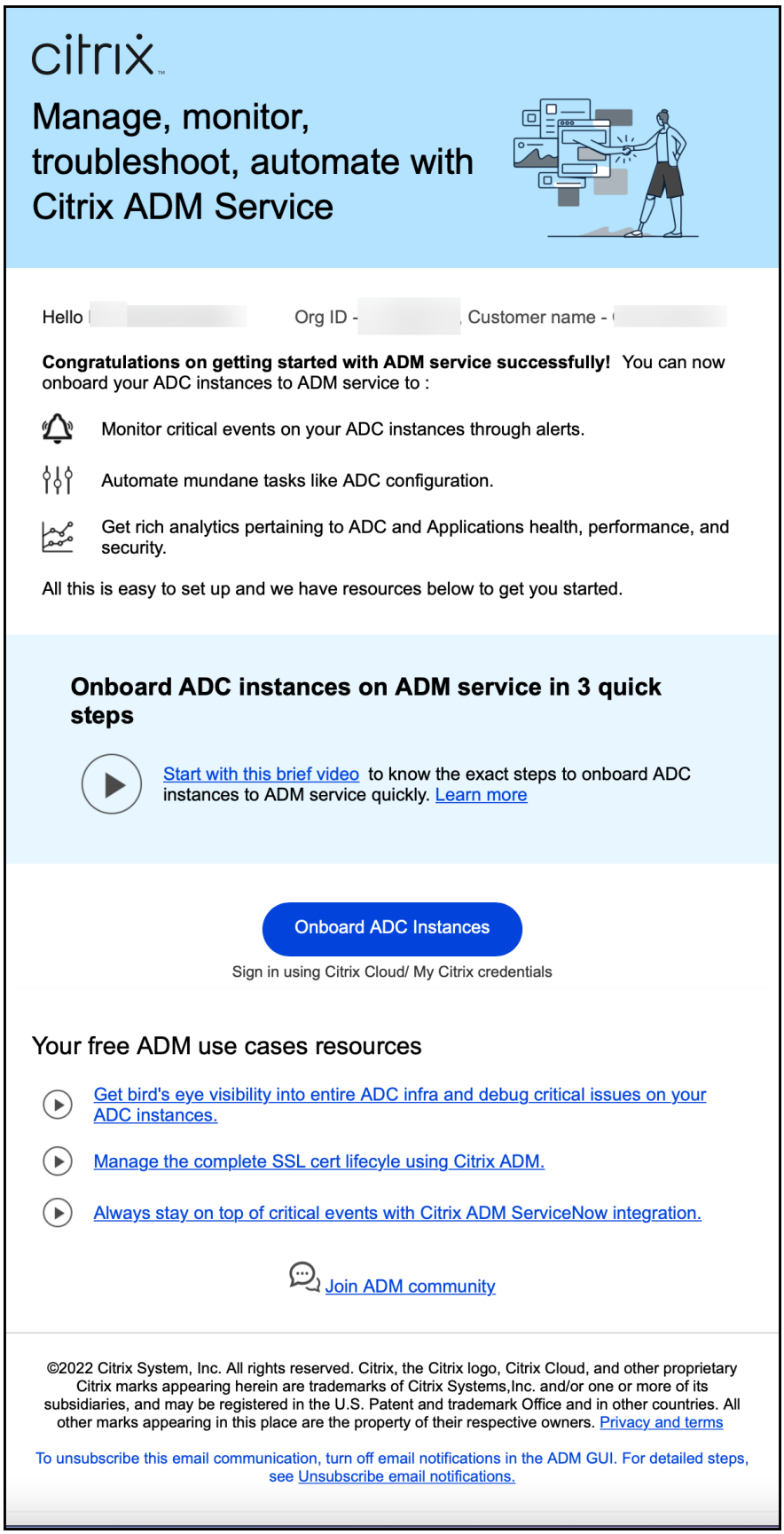
NetScaler Console sendet E-Mail-Benachrichtigungen an alle inaktiven und neuen Benutzer.

Inaktive Kunden erhalten eine E-Mail-Benachrichtigung, wenn:

- NetScaler-Instanzen sind nicht konfiguriert
- Die Mandantenlizenz läuft in weniger als 30 Tagen ab

> **Hinweis:**
>
> Standardmäßig erhalten alle inaktiven Kunden eine E-Mail-Benachrichtigung.

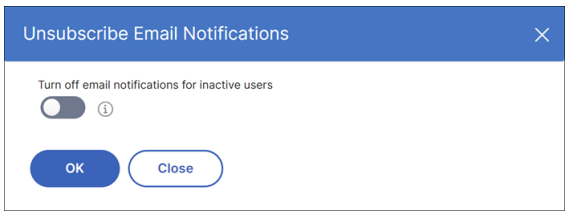
Neukunden erhalten eine E-Mail von NetScaler Console, in der sie aufgefordert werden, die NetScaler-Instanzen in den NetScaler Console-Dienst einzubinden, wo sie kritische Ereignisse auf NetScaler-Instanzen verwalten und überwachen, Fehler beheben und Aufgaben wie die NetScaler-Konfiguration automatisieren können.



E-Mail-Benachrichtigungen abbestellen

Sie können die E-Mail-Benachrichtigungen, die Sie vom NetScaler Console-Dienst erhalten, abonnieren oder abbestellen. So meldest du dich von E-**Mail-Benachrichtigungen** ab :

1. Navigieren Sie in NetScaler Console zu Einstellungen > Allgemeine Einstellungen > Systemkonfigurationen , und klicken Sie dann auf E-**Mail-Abonnements** .** Das Fenster **E-Mail-Benachrichtigungen abbestellen** wird angezeigt.



> **Hinweis:**
>
> Standardmäßig ist die Umschaltfläche zum Deaktivieren von E-Mail-Benachrichtigungen deaktiviert und die E-Mail-Benachrichtigungen sind für alle inaktiven Benutzer aktiviert.

2. Aktivieren Sie im Fenster **E-Mail-Benachrichtigungen abbestellen** die Umschaltfläche. Klicken Sie auf **OK**.

Sie haben die E-Mail-Benachrichtigungen jetzt abgemeldet und erhalten keine E-Mails an Onboard NetScaler-Instanzen.

Aktivieren oder Deaktivieren von Features

July 17, 2024

Als Administrator können Sie die folgenden Funktionen auf der Seite **Einstellungen > Allgemeine Einstellungen > 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 die NetScaler Console die NetScaler-Instanzen des inaktiven Agenten zusammen mit anderen aktiven Agents neu. Weitere Informationen finden Sie unter Konfigurieren von NetScaler Agent-Agents für die Bereitstellung an mehreren Standorten .
- **Netzwerkfunktion**zur Entitätsabfrage —Eine Entität ist entweder eine Richtlinie, ein virtueller Server, ein Dienst oder eine Aktion, die mit einer NetScaler-Instanz verknüpft ist. Standardmäßig fragt NetScaler Console alle 60 Minuten automatisch konfigurierte Netzwerkfunktionsentitäten ab. Weitere Informationen finden Sie unter Überblick über Statusabruf.

- **Instanz-Backup**—Sichern Sie den aktuellen Status einer NetScaler-Instanz und verwenden Sie später die gesicherten Dateien, um die NetScaler-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 Console empfangene Ereignisse werden auf der Seite "Ereignisübersicht "(****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 Console bietet eine zentrale Ansicht der SSL-Zertifikate, die auf allen verwalteten NetScaler-Instanzen installiert sind. Weitere Informationen finden Sie unter SSL-Dashboard.
- **Instance Syslog**—Sie können die auf Ihren NetScaler-Instanzen generierten Syslog-Ereignisse überwachen, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Meldungen an NetScaler Console umgeleitet werden. Weitere Informationen finden Sie unter Syslog auf Instanzen konfigurieren.

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 Operationen nicht ausführen.

Konfigurieren einer Aktionsrichtlinie, um Benachrichtigungen über Anwendungsereignisse

March 12, 2024

Neben der vorhandenen Analyseansicht von Anwendungsereignissen können Sie eine Aktionsrichtlinie konfigurieren, um Benachrichtigungen über Anwendungsereignisse über Slack, E-Mail, PagerDuty oder ServiceNow zu erhalten. Zu den Anwendungsereignissen gehören Leistungsprobleme, Bot- und WAF-Verstöße sowie Service-Graph-Verstöße. Als Administrator können Sie mithilfe der Aktionsrichtlinie Ereignisbenachrichtigungen in Echtzeit erhalten.

Mit der Aktionsrichtlinie können Sie:

- Definieren Sie bestimmte Bedingungen für die Anwendungsereignisse.
- Lassen Sie sich über Slack, E-Mail, PagerDuty und ServiceNow über die folgenden Ereignisse benachrichtigen:

Ereigniskategorien	Ereignisunterkategorien	Ereignisse
Sicherheitsverletzungen	Alle Sicherheitsverstöße	Alle Bot-Verstöße (Weitere Informationen zur Liste der Bot-Verstöße finden Sie unter Verstoßkategorien). Alle WAF-Verstöße (WAF-SQL-Verstöße, WAF-XSS-Verstöße und WAF-Infer-XML-Verstöße)
	Alle Sicherheitsverletzungen pro Kunde	Bot-Verstöße pro Kunde Verstöße gegen WAF pro Kunde **Hinweis:** Um die WAF-Verstoßbenachrichtigung zu erhalten, müssen die Mindesttransaktionen bei Verstößen 20% betragen. Beispielsweise müssen von 100 Transaktionen mindestens 20 Verstöße gegen Transaktionen sein.
Leistung der Anwendung		Verstoß gegen App-Score Netzwerklatenz des Clients Servernetzwerklatenz Verarbeitungszeit des Servers

Ereigniskategorien	Ereignisunterkategorien	Ereignisse
Verwendung der Anwendung		Reaktionszeit Anfragen Bandbreite Verstoß gegen das Service-Diagramm Anfragen pro Sekunde Durchsatz Datenvolume

Eine Aktionsrichtlinie konfigurieren

1. Navigieren Sie zu **Einstellungen > Aktion > Aktionsrichtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Auf der Seite **Aktionsrichtlinie erstellen** :
   a) **Richtlinienname** —Geben Sie einen Policy-Namen Ihrer Wahl an.
   b) **Aktiviert** —Diese Option ist standardmäßig ausgewählt.
   c) Wenn das **folgende Ereignis eintritt** —Wählen Sie in der Liste ein Ereignis aus.
   d) **Und die folgende Bedingung ist erfüllt** —Wählen Sie aus der Liste aus, um eine Bedingung zu definieren, für die Sie benachrichtigt werden möchten. Sie können auf **+** klicken, um weitere Bedingungen hinzuzufügen. Um eine Bedingung zu entfernen, klicken Sie auf —.

      Sie können die Aktionsrichtlinie mit den folgenden Operatoren konfigurieren. Die Operatoren werden basierend auf den von Ihnen ausgewählten Bedingungen angezeigt.

Betreiber	Beschreibung
Entspricht	Entspricht einem definierten Wert
Nicht gleich	Entspricht nicht einem definierten Wert
Größer als	Größer als ein definierter Wert
Größer als oder gleich	Größer als oder gleich einem definierten Wert
Weniger als	Kleiner als ein definierter Wert

Betreiber	Beschreibung
Kleiner als oder gleich	Kleiner als oder gleich einem definierten Wert
Enthält	Enthält den definierten Begriff oder Wert
Beginnt mit	Beginnt mit einem definierten Begriff oder Wert
Endet mit	Endet mit einem definierten Begriff oder Wert
IN	Ermöglicht die Auswahl mehrerer Werte

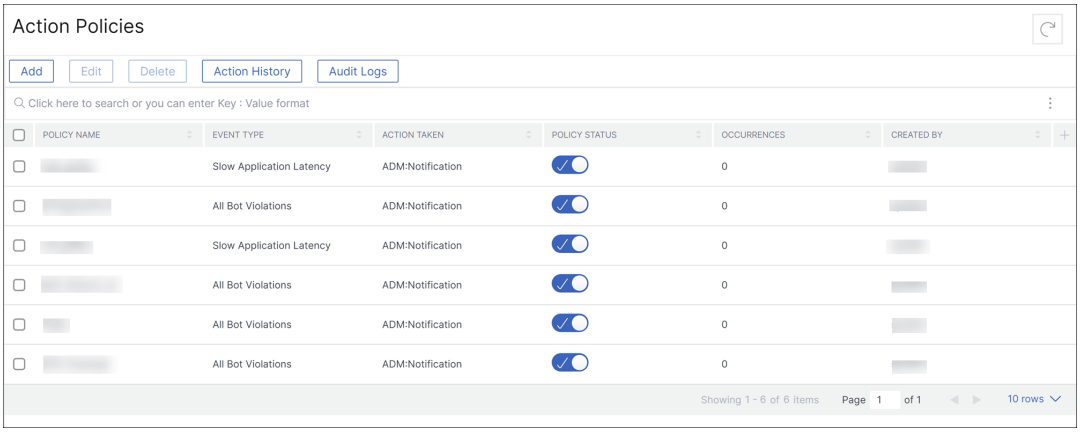
e) **Gehen Sie dann wie folgt** vor —Wählen Sie **Benachrichtigen**. Nachdem Sie **Benachrichtigen**ausgewählt haben, wird die Option Benachrichtigungstyp angezeigt.

f) **Benachrichtigungstyp** —Wählen Sie den Benachrichtigungstyp E-Mail, Slack, PagerDuty oder ServiceNow aus. Abhängig vom ausgewählten Benachrichtigungstyp wird die entsprechende Option (Verteilerliste, Slack-Profil, PagerDuty-Profil oder ServiceNow-Profil) angezeigt. Wählen Sie ein Profil aus der Liste aus.

Wenn Sie ein neues Profil erstellen möchten, klicken Sie auf **Hinzufügen**.

g) Klicken Sie auf **Richtlinie erstellen**.

Die Richtlinie ist konfiguriert. Sie können die konfigurierten Richtliniendetails anzeigen.



Nachdem Sie die Richtlinie konfiguriert haben, können Sie die Richtlinie auswählen und auf Folgendes klicken:

- **Bearbeiten**, um die Aktionsrichtlinie zu aktualisieren oder zu ändern. Klicken Sie nach dem Update auf Richtlinie aktualisieren.
- **Löschen**, um die Aktionsrichtlinie zu entfernen. Sie können mehrere Richtlinien auswählen und auf **Löschen** klicken, um sie zu entfernen.
- **Aktionsverlauf**, um Details wie Uhrzeit, durchgeführte Aktion, Richtlinienname, Warnungstyp und Warnmeldung anzuzeigen.

In der folgenden Tabelle werden die Details der Konfiguration der Aktionsrichtlinie beschrieben.

Name des Verstoßes	Bedingung	Beschreibung
Alle Sicherheitsverstöße	Instanz-IP	IP-Adresse der NetScaler-Instanz. Wählen Sie die IP-Adresse aus der Liste aus.
	Anzahl der Verstöße	Die Anzahl der Verstöße, für die Sie benachrichtigt werden möchten. Wenn Sie beispielsweise die Anzahl der Verstöße als kleiner oder gleich 10 konfigurieren, werden Sie benachrichtigt, wenn 10 oder weniger Bot-Verstoßtransaktionen eingehen.
	Verhältnis von Verstößen	Dieser Wert gibt die Gesamtzahl der Verstöße durch bestimmte Transaktionen an und der Wert muss zwischen 0 und 1 liegen. Beispielsweise handelt es sich bei 20 von 100 Transaktionen um Verstöße, und wenn Sie für ein solches Szenario benachrichtigt werden möchten, müssen Sie 0,2 eingeben.
Alle Bot-Verstöße	Bot-Profil	Der Bot-Profilname, der für die Konfiguration der Bot-Verwaltung auf der NetScaler-Instanz verwendet wird.
	Instanz-IP	IP-Adresse der NetScaler-Instanz. Wählen Sie die IP-Adresse aus der Liste aus.

Name des Verstoßes	Bedingung	Beschreibung
	Anzahl der Verstöße	Die Anzahl der Verstöße, für die Sie benachrichtigt werden möchten. Wenn Sie beispielsweise die Anzahl der Verstöße als kleiner oder gleich 10 konfigurieren, werden Sie benachrichtigt, wenn 10 oder weniger Bot-Verstoßtransaktionen eingehen.
	Verhältnis von Verstößen	Dieser Wert gibt die Gesamtzahl der Verstöße durch bestimmte Transaktionen an und der Wert muss zwischen 0 und 1 liegen. Beispielsweise handelt es sich bei 20 von 100 Transaktionen um Verstöße, und wenn Sie für ein solches Szenario benachrichtigt werden möchten, müssen Sie 0,2 eingeben.
Alle WAF-Verstöße, WAF-SQL-Verletzung, WAF-XSS-Verletzung, WAF Infer XML-Verletzung	WAF-Profil	Der WAF-Profilname, der für die Konfiguration der WAF-Sicherheitseinstellungen auf der NetScaler-Instanz verwendet wird.
	Instanz-IP	IP-Adresse der NetScaler-Instanz. Wählen Sie die IP-Adresse aus der Liste aus.
	Anzahl der Verstöße	Die Anzahl der Verstöße, für die Sie benachrichtigt werden möchten. Die Mindestanforderung für die Benachrichtigung der WAF-Verstöße beträgt 20%.

Name des Verstoßes	Bedingung	Beschreibung
	Verhältnis von Verstößen	Dieser Wert gibt die Gesamtzahl der Verstöße durch bestimmte Transaktionen an und der Wert muss zwischen 0 und 1 liegen. Beispielsweise handelt es sich bei 20 von 100 Transaktionen um WAF-SQL-Verletzungstransaktionen, und wenn Sie für ein solches Szenario benachrichtigt werden möchten, müssen Sie 0,2 eingeben.
Alle Sicherheitsverletzungen pro Kunde	Anwendungsname	Der Name der benutzerdefinierten Anwendung. Wählen Sie die Anwendung aus der Liste aus. Wenn Sie diese Bedingung nicht hinzufügen, werden alle Anwendungen aus der NetScaler-Instanz berücksichtigt.
	Instanz-IP	IP-Adresse der NetScaler-Instanz. Wählen Sie die IP-Adresse aus der Liste aus.
	Client-IP	Die Quelle, aus der der Bot stammt. Geben Sie die IP-Adresse an.
	Angriffe insgesamt	Die Gesamtzahl der Angriffe, für die Sie benachrichtigt werden möchten.
	URL anfragen	Die URL, die Sie zum Blockieren konfigurieren möchten. Geben Sie die URL an.

Name des Verstoßes	Bedingung	Beschreibung
	Vserver-Name	Die zugehörigen Anwendungen, die für benutzerdefinierte Anwendungen konfiguriert sind. Wählen Sie die Anwendung aus der Liste aus. Wenn Sie diese Bedingung nicht hinzufügen, werden alle Anwendungen aus der NetScaler-Instanz berücksichtigt.
Bot-Verstöße pro Kunde	Anwendungsname	Der Name der benutzerdefinierten Anwendung. Wählen Sie die Anwendung aus der Liste aus. Wenn Sie diese Bedingung nicht hinzufügen, werden alle Anwendungen aus der NetScaler-Instanz berücksichtigt.
	Instanz-IP	IP-Adresse der NetScaler-Instanz. Wählen Sie die IP-Adresse aus der Liste aus.
	Client-IP	Die Quelle, aus der der Bot stammt. Geben Sie die IP-Adresse an.
	Angriffe insgesamt	Die Gesamtzahl der Angriffe, für die Sie benachrichtigt werden möchten.
	Art der Verletzung	Wählen Sie den Bot-Verstoß aus der Liste aus.
	URL anfragen	Die URL, die Sie zum Blockieren konfigurieren möchten. Geben Sie die URL an.

Name des Verstoßes	Bedingung	Beschreibung
	Vserver-Name	Die zugehörigen Anwendungen, die für benutzerdefinierte Anwendungen konfiguriert sind. Wählen Sie die Anwendung aus der Liste aus. Wenn Sie diese Bedingung nicht hinzufügen, werden alle Anwendungen aus der NetScaler-Instanz berücksichtigt.
Verstöße gegen WAF pro Kunde	Anwendungsname	Der Name der benutzerdefinierten Anwendung. Wählen Sie die Anwendung aus der Liste aus. Wenn Sie diese Bedingung nicht hinzufügen, werden alle Anwendungen aus der NetScaler-Instanz berücksichtigt.
	Instanz-IP	IP-Adresse der NetScaler-Instanz. Wählen Sie die IP-Adresse aus der Liste aus.
	Client-IP	Die Quelle, aus der der Bot stammt. Geben Sie die IP-Adresse an.
	Angriffe insgesamt	Die Gesamtzahl der Angriffe, für die Sie benachrichtigt werden möchten.
	Art der Verletzung	Wählen Sie den WAF-Verstoß aus der Liste aus.
	URL anfragen	Die URL, die Sie zum Blockieren konfigurieren möchten. Geben Sie die URL an.

Name des Verstoßes	Bedingung	Beschreibung
	Vserver-Name	Die zugehörigen Anwendungen, die für benutzerdefinierte Anwendungen konfiguriert sind. Wählen Sie die Anwendung aus der Liste aus. Wenn Sie diese Bedingung nicht hinzufügen, werden alle Anwendungen aus der NetScaler-Instanz berücksichtigt.
Verstoß gegen App-Score	Leistungsindikator	Die App-Score-Komponenten und deren Schwellenwerte. Wählen Sie die App-Score-Komponente aus der Liste aus. Weitere Informationen finden Sie unter App-Score-Komponenten auswählen und Schwellenwerte festlegen.
	Anzahl der Verstöße	Die Anzahl der Verstöße, für die Sie benachrichtigt werden möchten. Wenn Sie beispielsweise die Anzahl der Sicherheitsverletzungen gleich 5 für die Antwortzeit konfigurieren, werden Sie benachrichtigt, wenn der Schwellenwert für die Antwortzeit fünfmal überschritten wird.
	Anwendungsname	Klicken **Sie auf Anwendungen** auswählen, um die Anwendungen auszuwählen, bei denen der Verstoß benachrichtigt werden soll.

Name des Verstoßes	Bedingung	Beschreibung
Latenz im Client-Netzwerk	Durchschnittliche Latenz im Client-Netzwerk	Geben Sie den Wert für die Clientlatenz (Client zu NetScaler) in Millisekunden an, für den Sie benachrichtigt werden möchten.
	Latenzanomalien im Client-Netzwerk	Geben Sie die Anzahl der Anomalien für die Netzwerklatenz an, über die Sie benachrichtigt werden möchten.
	Anwendungsname	Klicken **Sie auf Anwendungen** auswählen, um die Anwendungen auszuwählen, bei denen der Verstoß benachrichtigt werden soll.
Server-Netzwerk-Latenz	Durchschnittliche Latenz im Servernetzwerk	Geben Sie den Wert für die Serverlatenz (Server zu NetScaler) in Millisekunden an, für den Sie benachrichtigt werden möchten.
	Anomalien bei der Latenz im Servernetzwerk	Geben Sie die Anzahl der Anomalien für die Netzwerklatenz an, über die Sie benachrichtigt werden möchten.
	Anwendungsname	Klicken **Sie auf Anwendungen** auswählen, um die Anwendungen auszuwählen, bei denen der Verstoß benachrichtigt werden soll.
Reaktionszeit	Durchschnittliche Reaktionszeit	Geben Sie den Wert (in Millisekunden) an, für den Sie benachrichtigt werden möchten.
	Auffälligkeiten bei der Reaktionszeit	Geben Sie die Anzahl der Anomalien an, für die Sie benachrichtigt werden möchten.

Name des Verstoßes	Bedingung	Beschreibung
	Anwendungsname	Klicken Sie auf **Anwendungen** auswählen, um die Anwendungen auszuwählen, über die Sie benachrichtigt werden möchten. Wenn Sie keine Anwendung auswählen, wird sie in allen Anwendungen angewendet.
Anfragen	Gesamtzahl der Anfragen	Geben Sie die Gesamtzahl der Anfragen an, für die Sie benachrichtigt werden möchten.
	Anwendungsname	Klicken Sie auf **Anwendungen** auswählen, um die Anwendungen auszuwählen, über die Sie benachrichtigt werden möchten. Wenn Sie keine Anwendung auswählen, wird sie in allen Anwendungen angewendet.
Bandbreite	Gesamtbandbreite	Geben Sie die Bandbreite (MB) an, für die Sie benachrichtigt werden möchten.
	Anwendungsname	Klicken Sie auf **Anwendungen** auswählen, um die Anwendungen auszuwählen, über die Sie benachrichtigt werden möchten. Wenn Sie keine Anwendung auswählen, wird sie in allen Anwendungen angewendet.
Verarbeitungszeit des Servers	Durchschnittliche Verarbeitungszeit des Servers	Geben Sie den Wert für die Serververarbeitung (Server zu NetScaler) in Millisekunden an, für den Sie benachrichtigt werden möchten.

Name des Verstoßes	Bedingung	Beschreibung
	Anomalien bei der Serververarbeitungszeit	Geben Sie die Anzahl der Anomalien für die Serververarbeitungszeit an, über die Sie benachrichtigt werden möchten.
	Anwendungsname	Klicken **Sie auf Anwendungen** auswählen, um die Anwendungen auszuwählen, bei denen der Verstoß benachrichtigt werden soll.
Verstoß gegen das Service-Diagramm		Microservices, die die konfigurierten Schwellenwerte überschreiten. Weitere Informationen finden Sie unter Konfigurieren von Schwellenwerten im Servicegraphen.
Anfragen pro Sekunde	Durchschnittlich Anfragen pro Sekunde	Die Anzahl der Anfragen, die die Anwendung pro Sekunde erhält. Geben Sie den Durchschnittswert an, der benachrichtigt werden soll.
	Durchschnittliche Auffälligkeiten bei Anfragen pro Sekunde	Geben Sie die durchschnittliche Anzahl der Anomalien an, für die Sie benachrichtigt werden möchten. **Hinweis:** Wenn Sie für dieses Ereignis die UND-Bedingung verwenden, können Sie entweder den Durchschnitt der Anfragen pro Sekunde und den Anwendungsnamen oder den Durchschnitt der Anfragen pro Sekunde für Anomalien und den Anwendungsnamen konfigurieren.

Name des Verstoßes	Bedingung	Beschreibung
	Anwendungsname	Klicken **Sie auf Anwendungen** auswählen, um die Anwendungen auszuwählen, bei denen der Verstoß benachrichtigt werden soll.
Durchsatz	Durchsatz (durchschnittlich)	Die Gesamtdaten, die für einen bestimmten Zeitraum übertragen wurden. Geben Sie den Durchschnittswert (in MB) an, um benachrichtigt zu werden.
	Durchsatzanomalien	Geben Sie die durchschnittliche Anzahl der Anomalien an, für die Sie benachrichtigt werden möchten. **Hinweis:** Wenn Sie die UND-Bedingung für dieses Ereignis verwenden, können Sie entweder den durchschnittlichen Durchsatz und den Anwendungsnamen oder die durchschnittliche Durchsatzanomalie und den Anwendungsnamen konfigurieren.
	Anwendungsname	Klicken **Sie auf Anwendungen** auswählen, um die Anwendungen auszuwählen, bei denen der Verstoß benachrichtigt werden soll.
Datenvolume	Gesamtes Datenvolumen	Die Gesamtdaten, die in einer bestimmten Dauer übertragen werden sollen. Geben Sie den Wert (in MB) an, der benachrichtigt werden soll.

Name des Verstoßes	Bedingung	Beschreibung
	Anomalien beim Datenvolumen	Geben Sie die Anzahl der Anomalien an, für die Sie benachrichtigt werden möchten. **Hinweis:** Wenn Sie die AND-Bedingung für dieses Ereignis verwenden, können Sie entweder Gesamtdatenvolumen und Anwendungsname oder Datenvolumenanomalien und Anwendungsname konfigurieren.
	Anwendungsname	Klicken **Sie auf Anwendungen** auswählen, um die Anwendungen auszuwählen, bei denen der Verstoß benachrichtigt werden soll.

Verwenden Sie die Suchleiste

Über die Suchleiste können Sie Ergebnisse filtern. Wenn Sie auf die Suchleiste klicken, erhalten Sie eine Liste mit Suchvorschlägen. Sie können die Komponente auswählen und die Ergebnisse nach Ihren Anforderungen filtern.

Auditprotokolloption verwenden

Klicken **Sie auf**Auditprotokolle und wählen Sie die Dauer aus der Liste aus, um die Aktionsrichtlinien anzuzeigen, die für die ausgewählte Dauer erstellt, geändert und gelöscht wurden, und klicken Sie auf **Suchen** .

> **Hinweis**
>
> Die Datenspeicherrichtlinien werden sich voraussichtlich in den kommenden Versionen ändern. Mit diesen Änderungen können Sie historische Daten nicht speichern, nachdem sie das Speicherlimit überschritten haben. Vorerst wird empfohlen, mehr Speicherplatz hinzuzufügen oder den Speicherplatz innerhalb der Lizenzberechtigungsgrenzen zu halten.

Auditprotokolle für die Verwaltung und Überwachung der Infrastruktur verwenden

March 12, 2024

Sie können die NetScaler Console verwenden, um alle Ereignisse auf der NetScaler Console und die auf den NetScaler-Instanzen generierten Syslog-Ereignisse zu verfolgen. Diese Meldungen können Ihnen bei der Verwaltung und Überwachung Ihrer Infrastruktur helfen. Protokollnachrichten sind jedoch nur dann eine gute Informationsquelle, wenn Sie sie überprüfen, und NetScaler Console vereinfacht die Überprüfung von Protokollnachrichten.

Sie können Filter verwenden, um Syslog- und Audit-Log-Meldungen von NetScaler Console zu durchsuchen. 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 über die NetScaler Console-GUI überprüfen:

- Auditprotokolle, die sich auf die NetScaler-Instanz beziehen
- Auditprotokolle im Zusammenhang mit NetScaler Console
- Audit-Protokolle für Anwendungen

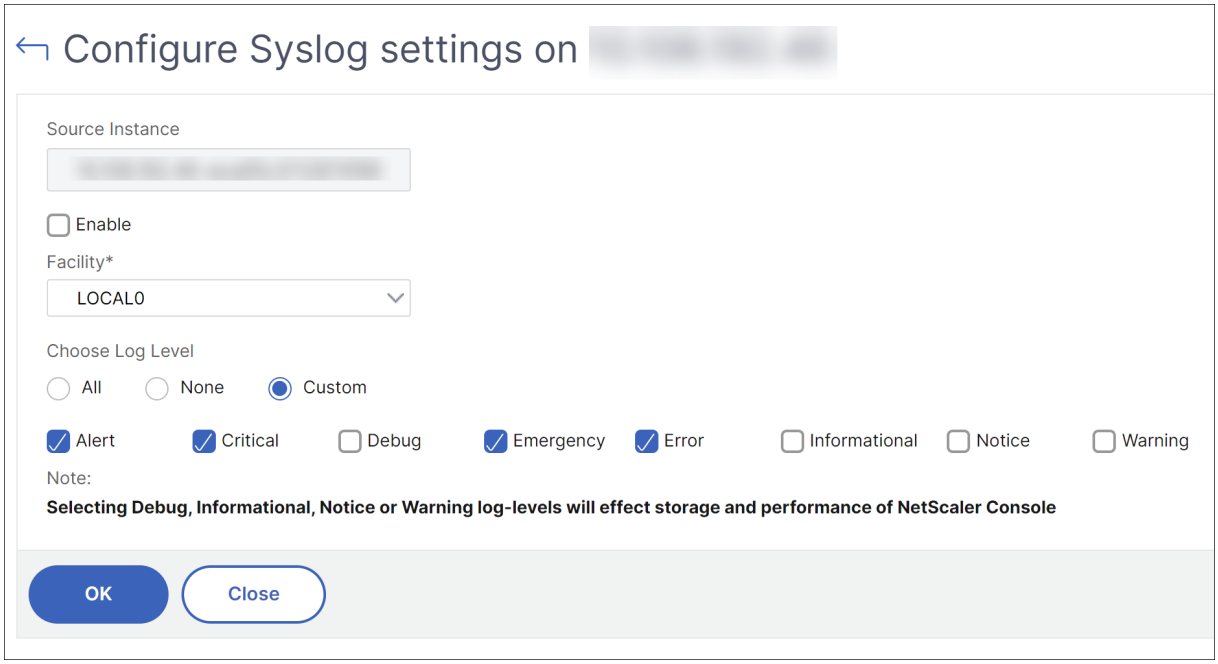
Auditprotokolle, die sich auf die NetScaler-Instanz beziehen

Bevor Sie Syslog-Meldungen zur NetScaler-Instanz in der NetScaler Console anzeigen können, konfigurieren Sie die NetScaler Console als Syslog-Server für Ihre NetScaler-Instanz. Nach Abschluss der Konfiguration werden alle Syslog-Meldungen von der Instanz zur NetScaler Console umgeleitet.

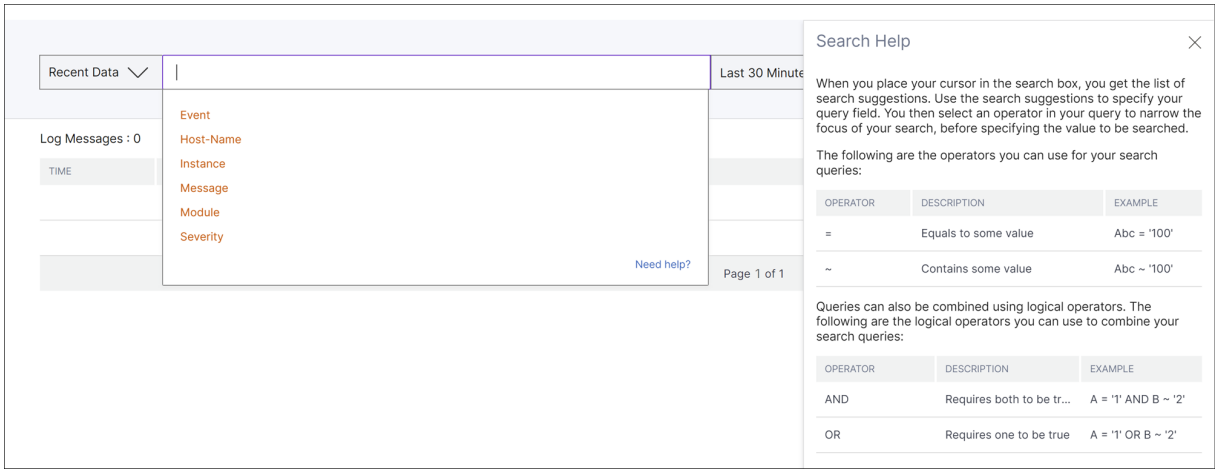
NetScaler Console als Syslog-Server konfigurieren

Gehen Sie wie folgt vor, um NetScaler Console als Syslog-Server zu konfigurieren:

1. Navigieren Sie in der NetScaler Console-GUI zu **Infrastruktur > Instanzen** .
2. Wählen Sie die NetScaler-Instanz aus, von der die Syslog-Meldungen erfasst und in der NetScaler Console 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 Console beginnt, die Syslog-Meldungen zu empfangen. 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-Meldungen.



Um die Protokollmeldungen zu exportieren, klicken Sie auf das Pfeilsymbol in der oberen rechten Ecke.

Klicken Sie als Nächstes auf **Jetzt exportieren** oder **Export planen**. Weitere Informationen finden Sie unter Exportieren von Syslog-Nachrichten.

Auditprotokolle im Zusammenhang mit NetScaler Console

Basierend auf vorkonfigurierten Regeln generiert NetScaler Console Audit-Log-Meldungen für alle Ereignisse, sodass Sie den Zustand Ihrer Infrastruktur überwachen können. Um alle in der NetScaler Console vorhandenen Audit-Log-Meldungen anzuzeigen, navigieren Sie zu **Einstellungen->Audit-Log-Meldungen** .

Um die Protokollmeldungen zu exportieren, klicken Sie auf das Pfeilsymbol in der oberen rechten Ecke.

Anwendungsbezogene Audit-Logs

Sie können die Audit-Log-Meldungen für alle NetScaler Console-Anwendungen oder für eine bestimmte Anwendung anzeigen.

- Um alle Audit-Log-Meldungen für alle in der NetScaler Console vorhandenen Anwendungen anzuzeigen, navigieren Sie zu **Infrastruktur > Netzwerkfunktionen Überwachung**.
- Um Audit-Log-Meldungen für eine bestimmte Anwendung in der NetScaler Console anzuzeigen, navigieren Sie zu **Anwendungen > Dashboard > doppelklicken Sie auf den virtuellen Server > Audit-Log** .

> **Hinweis** Sie können die Audit-Log-Meldungen der NetScaler Console an einen externen Server weiterleiten. Einzelheiten finden Sie unter Anzeigen von Auditing-Informationen.

Konfigurieren der IP-Adressverwaltung (IPAM)

January 26, 2024

Mit NetScaler Console IPAM können Sie IP-Adressen in von NetScaler Console verwalteten Konfigurationen automatisch zuweisen und freigeben. Sie können IPs aus Netzwerken oder IP-Bereichen zuweisen, die mit den folgenden IP-Anbietern definiert wurden:

- In NetScaler Console integrierter IPAM-Anbieter.
- Infoblox IPAM-Lösung.

Sie können NetScaler Console 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 im IP-Bereich verfolgen, der von NetScaler Console verwaltet wird.

Einen externen IP-Adressanbieter hinzufügen

NetScaler Console verfügt über einen integrierten IPAM-Anbieter zur Verwaltung von IPs und IP-Bereichen. Sie können auch einen externen IP-Adressanbieter für NetScaler Console 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 Console 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 Namen des IP-Anbieters an, der in NetScaler Console 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 Console-Umgebung zuweist. Stellen Sie sicher, dass Sie die URL im folgenden Format angeben:

  ```
  https://<host name>
  ```

  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 Console Infoblox DDI als externen Anbieter.

Sie können NetScaler Console 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 Console IPAM-Netzwerk mithilfe des Infoblox-Providers zu erstellen, muss auf Infoblox ein Netzwerk mit demselben CIDR-IP-Bereich vorhanden sein.

Wenn Sie ein IPAM-Netzwerk in der NetScaler Console erstellen, registrieren Sie nur die Verwendung des Infoblox-Netzwerks in der NetScaler Console. Die NetScaler Console arbeitet dann mit Infoblox zusammen, um die vom Netzwerk zugewiesenen IP-Adressen zu verwalten. Das InfoBlox-Netzwerk kann weiterhin außerhalb der NetScaler Console verwendet werden.

Ebenso deregistriert die NetScaler Console das Infoblox-Netzwerk, wenn Sie das NetScaler Console-IPAM-Netzwerk löschen. Das bedeutet, dass die NetScaler Console nicht mehr mit Infoblox für die IP-Adressverwaltung in diesem Netzwerk interagiert.

DDI-APIs von Infoblox NetScaler Console IPAM verwendet die folgenden Infoblox-APIs, um die entsprechenden 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

> **Hinweis:**
>
> - Die IP-Adresse und der Port des Infoblox DNS-, DHCP- und IP Address Management (DDI) -Servers müssen vom öffentlichen Netzwerk aus zugänglich sein, damit der NetScaler Console-Dienst den Infoblox-Server erreichen und eine Verbindung zu ihm herstellen kann.
> - Das auf der NetScaler Console konfigurierte Infoblox-Benutzerkonto muss über die erforderlichen Berechtigungen verfügen, um die Infoblox-APIs verwenden zu können.

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 von NetScaler Console verwalteten 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 der NetScaler Console zu identifizieren.
   - **Anbieter** —Wählen Sie den Anbieter aus der Liste aus.

     In dieser Liste werden die in NetScaler Console 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 Console IPAM unterstützt nur IPv4-Adressen.

     Geben Sie für **IP-Bereich**den Netzwerkwert im folgenden Format an:


```
<first-IP-address>-<last-IP-address>
```

Beispiel:

```
10.0.0.20-10.0.0.100
```

Geben Sie für **CIDR**den Netzwerkwert im folgenden Format an:

```
<IP-address>/<subnet-mask>
```

Beispiel:

```
10.70.124.0/24
```

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

> **Hinweis:**
>
> Wenn Sie die IP-Adresse freigeben möchten, wählen Sie die IP-Adresse aus, die Sie freigeben möchten, und klicken Sie auf Zugeordnete **IPs freigeben**.

Anleitungsartikel

August 8, 2024

Die „How-to Articles“von NetScaler Console sind einfache, relevante und leicht zu implementierende Artikel zu den im Service verfügbaren Funktionen. Diese Artikel enthalten Informationen zu einigen der beliebten NetScaler Console-Funktionen wie Instanzverwaltung, Konfigurationsverwaltung, Eventverwaltung, Anwendungsverwaltung, StyleBooks und Zertifikatsverwaltung.

Klicken Sie in der folgenden Tabelle auf einen Feature-Namen, um die Liste der Anleitungsartikel für diese Funktion anzuzeigen.

Artikel		
Instanzverwaltung	Konfigurationsverwaltung	Zertifikatverwaltung
StyleBooks	Ereignisverwaltung	

Instanzverwaltung

So überwachen Sie global verteilte Websites

Verwalten von Adminpartitionen von NetScaler-Instanzen

So fügen Sie Instanzen zur NetScaler Console hinzu

So erstellen Sie Instanzgruppen in der NetScaler Console

So fragen Sie NetScaler-Instanzen und -Entitäten in der NetScaler Console ab

So konfigurieren Sie Sites für Geomaps in NetScaler Console

Erzwingen eines Failovers auf die sekundäre NetScaler-Instanz

Wie erzwingen Sie, dass eine sekundäre NetScaler-Instanz sekundär bleibt

NetScaler MPX- oder VPX-Stammkennwort ändern

NetScaler SDX-Stammkennwort ändern

Konfigurationsverwaltung

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

So aktualisieren Sie NetScaler SDX-Instanzen mithilfe der NetScaler Console

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

Zertifikatverwaltung

StyleBooks

So erstellen Sie ein StyleBook zum Hochladen von SSL-Zertifikats- und Zertifikatsschlüsseldateien auf NetScaler Console

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

So verwenden Sie Microsoft ADFS Proxy StyleBook

So verwenden Sie Oracle e-Business StyleBook

So verwenden Sie SSO Office 365 StyleBook

So verwenden Sie SSO Google Apps StyleBook

Ereignisverwaltung

So legen Sie das Ereignisalter für Ereignisse in der NetScaler Console fest

So planen Sie einen Ereignisfilter mithilfe der NetScaler Console

So richten Sie wiederholte E-Mail-Benachrichtigungen für Ereignisse von der NetScaler Console aus ein

So unterdrücken Sie Ereignisse mithilfe der NetScaler Console

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

So erstellen Sie Ereignisregeln in der NetScaler Console

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

So zeigen Sie die Zusammenfassung der Ereignisse in NetScaler Console an

So zeigen Sie die Schweregrade und Verzerrungen von SNMP-Traps auf der NetScaler Console an

So exportieren Sie Syslog-Nachrichten mit NetScaler Console

So unterdrücken Sie Syslog-Meldungen in der NetScaler Console

Häufig gestellte Fragen

June 7, 2024

Wie viele Agents muss ich installieren?

Die Anzahl der Agents hängt von der Anzahl der verwalteten Instanzen in einem Rechenzentrum und dem Gesamtdurchsatz ab. Citrix empfiehlt, mindestens einen Agent für jedes Datencenter zu installieren.

Wie kann ich mehrere Agents installieren?

Sie können nur einen Agent installieren, wenn Sie sich zum ersten Mal beim Dienst anmelden. Um mehrere Agents hinzuzufügen, schließen Sie zuerst die Erstinstallation ab und navigieren Sie zu **Einstellungen** > **Setup-Agents**.

Unterstützt NetScaler Agent AMD-Prozessoren?

Ja.

Kann ich von einem integrierten Agent auf einen externen Agent umsteigen?

Ja, das kannst du. Weitere Informationen finden Sie unter Übergang von einem integrierten Agent zu einem externen Agent.

Wie erhalte ich einen neuen Aktivierungscode, wenn ich ihn verliere?

Wenn Sie zum ersten Mal ein Onboarding durchführen, greifen Sie auf die Service-GUI zu, navigieren Sie zum Bildschirm **Agent einrichten** und klicken Sie auf **Aktivierungscode generieren**.

Wenn Sie versuchen, einen zweiten Agent zu installieren, navigieren Sie zum Generieren eines neuen Aktivierungscodes zu **Infrastruktur > Instanzen > Agents > Aktivierungscode generieren.**

Wie melde ich mich bei der Agent-VM an? Was sind die Standardanmeldeinformationen?

Wenn Ihr Agent auf einem Hypervisor oder einer Microsoft Azure-Cloud installiert ist, lauten die Standardanmeldeinformationen für den Agenten , `nsrecover`/`nsroot`wodurch die Shell-Eingabeaufforderung des Agenten geöffnet wird.

Wenn Ihr Agent auf AWS installiert ist, lauten die Standardanmeldeinformationen für die Anmeldung am `nsrecover`/`instance id`Agenten .

Was sind die Ressourcenanforderungen, um einen Agent on-premises auf einem Hypervisor zu installieren?

32 GB RAM, 8 virtuelle CPU, 500 GB Speicher, 1 virtuelle Netzwerkschnittstellen, 1 Gbit/s Durchsatz

Muss ich dem Agent während der Provisioning einen zusätzlichen Datenträger zuweisen?

Nein, Sie müssen keinen zusätzlichen Datenträger hinzufügen. Der Agent wird nur als Vermittler zwischen der NetScaler Console und den Instanzen in Ihrem Unternehmensrechenzentrum oder in der Cloud verwendet. Es speichert keine Inventar- oder Analysedaten, für die ein zusätzlicher Datenträger erforderlich wäre.

Kann ich meinen Aktivierungscode mit mehreren Agents wiederverwenden?

Nein, das geht nicht.

Wie erstelle ich die Netzwerkeinstellungen erneut, wenn ich einen falschen Wert eingegeben habe?

Greifen Sie auf die Agentkonsole auf Ihrem Hypervisor zu, melden Sie sich mit den Anmeldeinformationen nsrecover/nsroot bei der Shell-Eingabeaufforderung an, und führen Sie dann den Befehl aus `networkconfig`.

Was mache ich, wenn meine Agentregistrierung fehlschlägt?

Stellen Sie Folgendes sicher:

- Ihr Agent hat Zugriff auf das Internet (DNS konfigurieren).
- Sie haben den Aktivierungscode korrekt kopiert.
- Sie haben die Service-URL korrekt eingegeben.
- Sie haben die erforderlichen Ports geöffnet.

Die Registrierung war erfolgreich, aber woher weiß ich, ob der Agent gut läuft?

Nachdem der Agent erfolgreich registriert wurde, greifen Sie auf NetScaler Console zu und navigieren Sie zum Bildschirm „**Agent einrichten**“. Sie können den entdeckten Agent auf dem Bildschirm sehen. Wenn der Agent einwandfrei läuft, wird ein grünes Symbol angezeigt. Wenn es nicht läuft, wird ein rotes Symbol angezeigt.

Wie kann ich Agenten mithilfe eines Proxyservers mit NetScaler Console verbinden?

Sie können Agents mithilfe eines Proxyservers mit NetScaler Console verbinden. Das Skript ist im Ordner `/mps` im Agent verfügbar. Die Agents leiten alle ihre Daten an den Proxyserver weiter, der die Daten dann über das Internet an die NetScaler Console sendet.

Um Daten über den Proxyserver weiterzuleiten, geben Sie die Proxyserver-Details auf dem Agent mithilfe des folgenden Skripts ein: `proxy_input.py`, und folgen Sie den Anweisungen des Skripts, um weitere Informationen einzugeben. Der Agent ruft diese Informationen ab, während er über den Proxyserver eine Verbindung zur NetScaler Console herstellt.

Sie können Ihren Proxy-Server authentifizieren, indem Sie Ihren Benutzernamen und Ihr Kennwort angeben. Wenn der Agent die Daten sendet, authentifiziert der Proxyserver die Benutzeranmeldeinformationen, bevor er sie an NetScaler Console weiterleitet.

Weitere Informationen finden Sie unter NetScaler Console als API-Proxyserver .

> **Hinweis**
>
> NetScaler Console unterstützt Proxyserver mit aktivierter Standardauthentifizierung. NetScaler Console unterstützt auch Proxyserver, auf denen die Authentifizierung deaktiviert ist.

Meine Analytics-Berichte werden nicht angezeigt

Ermöglichen Sie Einblicke in Ihre virtuellen Server, um die Analytics-Berichte anzuzeigen. Einzelheiten finden Sie unter Aktivieren von Analytics.

Welche Versionen von NetScaler-Instanzen werden in NetScaler Console unterstützt?

Für Verwaltungs- und Überwachungsfunktionen werden NetScaler-Instanzen mit 10.5 und höher unterstützt. Einige Funktionen werden nur in bestimmten NetScaler-Versionen unterstützt. Weitere Informationen finden Sie unter Systemanforderungen.

Wie exportiere ich Dashboard-Berichte in NetScaler Console?

****Um den Bericht eines beliebigen Dashboards in NetScaler Console zu exportieren, klicken Sie oben rechts auf dieser Seite auf das Exportsymbol . Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** . Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
   Der Bericht wird auf Ihr System heruntergeladen.

2. Wählen Sie **Bericht planen**, um Zeitpläne für das Generieren und Exportieren von Berichten in regelmäßigen Abständen einzurichten. Geben Sie die Einstellungen für die Berichtsgenerierung an, und erstellen Sie ein E-Mail-Profil, in das der Bericht exportiert wird.

   a) **Wiederholung** - Wählen Sie **Täglich**, **Wöchentlich** oder **Monatlich** aus dem Dropdownlistenfeld aus.

   > **Hinweis**
   >
   > - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
   > - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

   b) **Wiederholzeit** - Geben Sie die Zeit wie `Hour : Minute` im 24-Stunden-Format ein.

   c) **E-Mail** - Aktivieren Sie das Kontrollkästchen, und wählen Sie dann das Profil aus dem Dropdownlistenfeld aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

   d) **Slack** —Aktiviere das Kontrollkästchen und wähle dann das Profil aus dem Dropdown-Listenfeld aus, oder klicke auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

   Klicken Sie auf **Zeitplan aktivieren**, um den Bericht zu planen, und klicken Sie dann auf **OK**. Wenn Sie auf das Kontrollkästchen **Zeitplan aktivieren** klicken, können Sie die ausgewählten Berichte erstellen.

Was bewirkt die Aktivierung clientseitiger Messungen?

Wenn clientseitige Messungen aktiviert sind, erfasst NetScaler Console Ladezeit- und Renderzeitmetriken für HTML-Seiten durch HTML-Injection. Mit diesen Metriken können Administratoren Probleme mit der L7-Latenz identifizieren.

Wird SSL-Verkehr vom Agenten zum NetScaler Console-Dienst einer SSL-Überprüfung unterzogen?

Wir empfehlen Ihnen, die SSL-Prüfung für den SSL-Verkehr vom Agent zum NetScaler Console-Dienst zu Bypass.