NetScaler SDX 13.1

Machine translated content

Disclaimer

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

Contents

Einführung

November 23, 2023

Die NetScaler SDX-Appliance ist eine Multi-Tenant-Plattform, auf der Sie mehrere virtuelle NetScaler-Maschinen (Instanzen) bereitstellen und verwalten können. Die SDX-Appliance erfüllt Cloud-Computing- und Multitenancy-Anforderungen, indem sie es einem einzelnen Administrator ermöglicht, die Appliance zu konfigurieren und zu verwalten und die Verwaltung jeder gehosteten Instanz an Mandanten zu delegieren. Mit der SDX-Appliance kann der Appliance-Administrator jedem Mandanten die folgenden Vorteile bieten:

- Eine vollständige Instanz. Jede Instanz hat die folgenden Berechtigungen:
  - Dedizierte CPU- und Speicherressourcen
  - Ein separater Raum für Entitäten
  - Die Unabhängigkeit, das Release und den Build ihrer Wahl zu leiten
  - Unabhängigkeit des Lebenszyklus
- Ein vollständig isoliertes Netzwerk. Datenverkehr, der für eine bestimmte Instanz bestimmt ist, wird nur an diese Instanz gesendet.

Die SDX-Appliance stellt einen Management Service bereit, der auf der Appliance vorab bereitgestellt ist. Der Management Service bietet eine Benutzeroberfläche (HTTP- und HTTPS-Modi) und eine API zum Konfigurieren, Verwalten und Überwachen der Appliance, des Management Service und der Instanzen. Ein selbstsigniertes Citrix Zertifikat ist für die HTTPS-Unterstützung vorverpackt. Citrix empfiehlt, den HTTPS-Modus zu verwenden, um auf die Management Service-Benutzeroberfläche zuzugreifen.

Versionshinweise

November 23, 2023

In den Versionshinweisen werden die Verbesserungen, Änderungen, Bugfixes und bekannten Probleme für eine bestimmte Version oder einen bestimmten Build der NetScaler-Software beschrieben. Die NetScaler SDX-Versionshinweise werden als Teil der ADC-Versionshinweise behandelt.

Detaillierte Informationen zu den Verbesserungen von SDX 13.1, bekannten Problemen und Bugfixes finden Sie in denADC-Versionshinweisen.

Erste Schritte mit der Management Service-Benutzeroberfläche

November 23, 2023

Um mit der Konfiguration, Verwaltung und Überwachung der Appliance, des Management Service und der virtuellen Instanzen zu beginnen, stellen Sie mithilfe eines Browsers eine Verbindung zur Management Service-Benutzeroberfläche her. Stellen Sie dann die virtuellen Instanzen auf der Appliance bereit.

Sie können eine Verbindung zur Management Service-Benutzeroberfläche herstellen, indem Sie einen der folgenden unterstützten Browser verwenden:

- Internet Explorer
- Google Chrome
- Apple Safari
- Mozilla Firefox

Melden Sie sich an der Management Service-Benutzeroberfläche an

1. Geben Sie in das Adressfeld Ihres Web-Browsers eine der folgenden Optionen ein:

   `http://Management Service IP Address`

   oder

   `https://Management Service IP Address`

2. Geben Sie auf der Anmeldeseite unter **Benutzername** und **Kennwort** den Benutzernamen und das Kennwort des Management Service ein. Der standardmäßige Benutzername lautet `nsroot`. Wenn das Standardkennwort nicht funktioniert, versuchen Sie, die Seriennummer der Appliance einzugeben. Der Seriennummern-Barcode ist auf der Rückseite der Appliance verfügbar. Nachdem Sie sich zum ersten Mal mit den Standardanmeldeinformationen angemeldet haben, müssen Sie Ihr `nsroot`-Standardkennwort ändern. Informationen zum Ändern des Administratorkennworts finden Sie unter Ändern des Kennworts des Standardbenutzerkontos.

3. Klicken Sie auf Optionen anzeigen, und führen Sie dann die folgenden Schritte aus:

   a) Wählen Sie **in der Liste Starten in** die Seite aus, die unmittelbar nach der Anmeldung an der Benutzeroberfläche angezeigt werden muss. Die verfügbaren Optionen sind Home, Überwachung, Konfiguration, Dokumentation und Downloads. Wenn Sie beispielsweise möchten, dass der Management Service bei der Anmeldung die Seite Konfiguration anzeigt, wählen Sie **Konfiguration** in der Liste **Starten in** aus.

   b) Geben Sie im Feld **Timeout**die Zeitspanne (in Minuten, Stunden oder Tagen) ein, nach der die Sitzung ablaufen soll. Der minimale Timeout-Wert beträgt 15 Minuten.

Die Einstellungen **Start in** und **Timeout** bleiben sitzungsübergreifend erhalten. Ihre Standardwerte werden erst wiederhergestellt, nachdem Sie den Cache geleert haben.

4. Klicken Sie auf **Anmelden**, um sich an der Management Service-Benutzeroberfläche anzumelden.

Assistent für die Ersteinrichtung

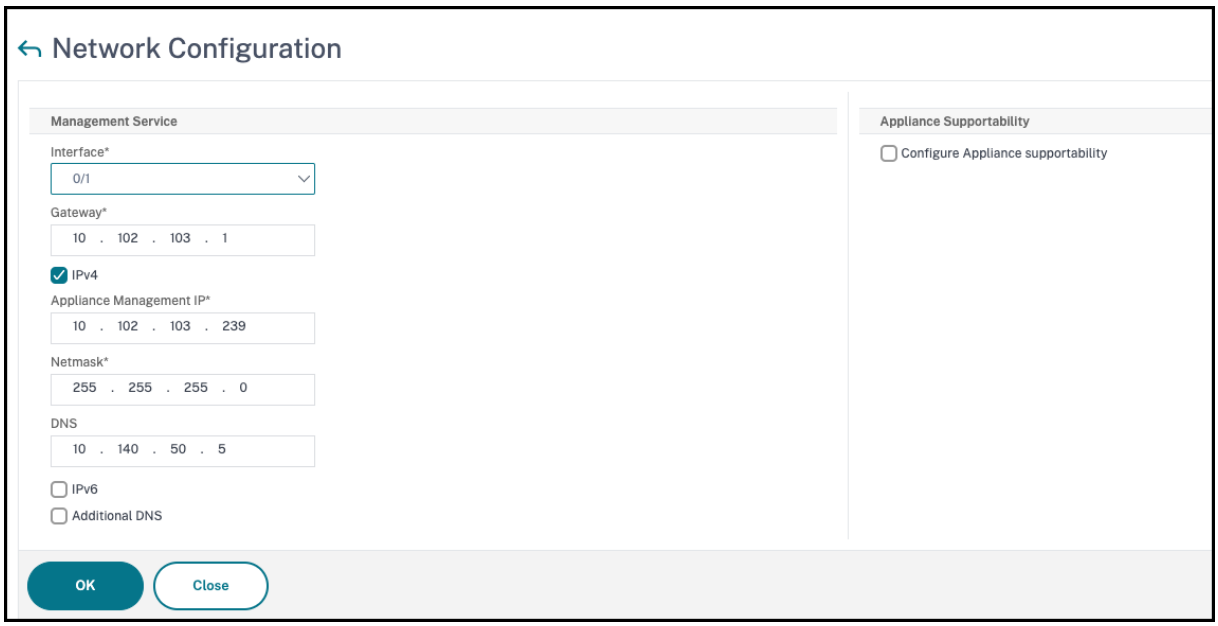
Sie können den Setup-Assistenten verwenden, um alle Erstkonfigurationen in einem einzigen Schema abzuschließen.

Sie können den Assistenten verwenden, um Netzwerkkonfigurationsdetails und Systemeinstellungen zu konfigurieren, das standardmäßige Administratorkennwort zu ändern und Lizenzen zu verwalten und zu aktualisieren.

Sie können diesen Assistenten auch verwenden, um die Netzwerkkonfigurationsdetails zu ändern, die Sie bei der Erstkonfiguration für die SDX-Appliance angegeben haben.

Um auf den Assistenten zuzugreifen, navigieren Sie zu **Konfiguration > System** und klicken Sie unter **Appliance einrichten**auf **Setup-Assistent**. Geben Sie Werte für die folgenden Parameter ein.

- **Schnittstelle:** Verwaltungsschnittstelle, die die Appliance mit einer Verwaltungsarbeitsstation oder einem Netzwerk verbindet. Mögliche Werte: 0/1, 0/2. Standard: 0/1.
- **Gateway:** Die IP-Adresse des Routers, der den Datenverkehr aus dem Subnetz der Appliance weiterleitet.
- Aktivieren Sie das Kontrollkästchen IPv4, wenn Sie die IPv4-Adresse für den Management Service verwenden möchten, und geben Sie die Details für die folgenden Parameter ein:
  - **Appliance Management IP:** Die IPv4-Adresse, die für den Zugriff auf den Management Service mithilfe eines Web-Browsers verwendet wird.
  - **Netzwerkmaske:** Die Subnetzmaske, in der sich die SDX-Appliance befindet.
- **DNS:** IPv4-Adresse des primären DNS-Servers. IPv6-Adressen werden für den primären DNS-Server nicht unterstützt.
- Aktivieren Sie das Kontrollkästchen IPv6, wenn Sie die IPv6-Adresse für den Management Service verwenden möchten, und geben Sie die Details für die folgenden Parameter ein:
  - **IP-Adresse des Management Service:** Die IPv6-Adresse, die für den Zugriff auf den Management Service mithilfe eines Web-Browsers verwendet wird.
  - **Gateway-IPv6-Adresse:** Die IPv4-Adresse des Routers, der den Datenverkehr aus dem Subnetz der Appliance weiterleitet.
- Wählen Sie **Zusätzliches DNS** aus, um DNS-Server-IP-Adressen als zusätzlichen DNS-Server neben dem primären DNS-Server hinzuzufügen. Die IP-Adressen können entweder IPv4 oder IPv6 sein.



> **Wichtig!**
>
> Citrix empfiehlt, die Appliance-Unterstützbarkeit für eine verbesserte Sicherheit deaktiviert zu lassen. Um die Geräteunterstützung zu deaktivieren, navigieren Sie zu **System > Netzwerkkonfiguration** und deaktivieren **Sie das Kontrollkästchen Appliance-Unterstützung konfigurieren** .

Unter **Systemeinstellungen**können Sie festlegen, dass der Management Service und eine NetScaler-Instanz nur über einen sicheren Kanal miteinander kommunizieren dürfen. Sie können auch den Zugriff auf die Management Service-Benutzeroberfläche einschränken. Clients können sich nur mit https an der Management Service-Benutzeroberfläche anmelden.

Sie können die Zeitzone des Management Service und des Citrix Hypervisor ändern. Die Standardzeitzone ist UTC. Sie können das Administratorkennwort ändern, indem Sie das Kontrollkästchen **Kennwort ändern** aktivieren und das neue Kennwort eingeben.

Unter Lizenzen verwalten können Sie Lizenzen verwalten und zuweisen. Sie können Ihre Hardware-Seriennummer (HSN) oder Ihren Lizenzzugangscode verwenden, um Ihre Lizenzen zuzuweisen. Wenn auf Ihrem lokalen Computer bereits eine Lizenz vorhanden ist, können Sie sie alternativ auf die Appliance hochladen.

Wählen Sie die Lizenzen auf der Appliance aus und klicken Sie auf **Fertig**, um die Erstkonfiguration abzuschließen.

Bereitstellen von Instanzen auf einer SDX-Appliance

Sie können eine oder mehrere NetScaler- oder Drittanbieter-Instanzen auf der SDX-Appliance mithilfe des Management Service bereitstellen. Die Anzahl der Instanzen, die Sie installieren können, hängt

von der Lizenz ab, die Sie erworben haben. Wenn die Anzahl der hinzugefügten Instanzen der in der Lizenz angegebenen Anzahl entspricht, erlaubt der Management Service die Bereitstellung weiterer Instanzen nicht.

Informationen zum Bereitstellen von Instanzen von Drittanbietern finden Sie unter Virtuelle Maschinen von Drittanbietern.

Zugriff auf die Konsole

Sie können über die Management Service-Schnittstelle auf die Konsole der NetScaler-Instanzen, den Management Service, Citrix Hypervisor und virtuelle Maschinen von Drittanbietern zugreifen. Dieser Zugriff ist hilfreich beim Debuggen und bei der Fehlerbehebung der auf der SDX-Appliance gehosteten Instanzen.

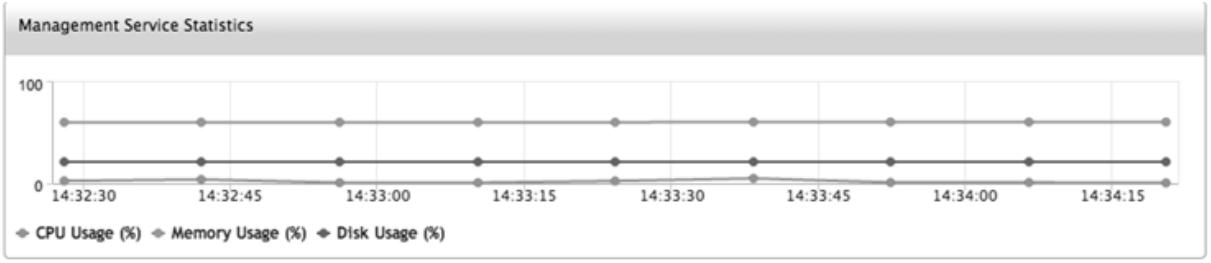
Um auf die Konsole von VMs zuzugreifen, navigieren Sie zur Instanzliste, wählen Sie die VM aus der Liste aus und klicken Sie in der Liste **Aktion** auf **Konsolenzugriff**.

Um auf die Konsole von Management Service oder Citrix Hypervisor zuzugreifen, navigieren Sie zu **Konfiguration > System**, und klicken Sie unter **Konsolenzugriff**auf **Management Service** oder **Citrix Hypervisor** Link.

Hinweis: Der Internet Explorer-Browser unterstützt keinen Konsolenzugriff. Citrix empfiehlt, die Konsolenzugriffsfunktion nur über HTTPS-Sitzungen des Management Service zu verwenden

Statistiken des Management Service

Das Dashboard enthält jetzt Management Service Statistics zur Überwachung der Verwendung von Speicher-, CPU- und Datenträgerressourcen durch den Management Service auf der SDX-Appliance.



Single Sign-On für den Management Service und die NetScaler-Instanzen

Nachdem Sie sich mit Ihren Benutzeranmeldeinformationen beim Management Service angemeldet haben, müssen Sie die Benutzeranmeldeinformationen nicht erneut angeben, um sich bei einer Instanz anzumelden. Standardmäßig ist der **Timeout-Wert** auf 30 Minuten festgelegt und die Konfigurationsregisterkarte wird in einem neuen Browserfenster geöffnet.

Verwalten Sie die Homepage

Auf der Homepage des Management Service erhalten Sie eine allgemeine Ansicht der Leistung der SDX-Appliance und der auf Ihrer Appliance bereitgestellten Instanzen. Die Informationen zur SDX-Appliance und -Instanz werden in Gadgets angezeigt, die Sie je nach Anforderung hinzufügen und entfernen können.

Die folgenden Minianwendungen sind standardmäßig auf der Homepage verfügbar.

- **Systemressourcen:** Zeigt die Gesamtzahl der CPU-Kerne, die Gesamtzahl der SSL-Chips, die Anzahl der freien SSL-Chips, den Gesamtspeicher und den freien Speicher auf der Appliance an.

**System-CPU	Speicherauslastung (%):** Zeigt den Prozentsatz der CPU- und Speicherauslastung der Appliance in grafischem Format an.

-

- **System-WAN-/LAN-Durchsatz (Mbit/s):** Zeigt den Gesamtdurchsatz der SDX-Appliance für eingehenden und ausgehenden Datenverkehr in einem Diagramm an, das in Echtzeit geplottet und in regelmäßigen Abständen aktualisiert wird.
- **NetScaler-Instanzen:** Zeigt die Eigenschaften der NetScaler-Instanzen an. Die angezeigten Eigenschaften sind Name, VM-Status, Instanzstatus, IP-Adresse, Rx (Mbit/s), Tx (Mbit/s), HTTP-Req/s und CPU-Auslastung (%) und Speicherauslastung (%).
  Hinweis: Bei der ersten Anmeldung werden auf der Startseite keine Daten zu den NetScaler-Instances angezeigt, da Sie keine Instances auf Ihrer Appliance bereitgestellt haben.
- **Health Monitoring-Ereignisse:** Zeigt die letzten 25 Ereignisse mit Schweregrad, Meldung sowie Datum und Uhrzeit des Ereignisses an.

Auf der Homepage können Sie Folgendes tun:

- NetScaler-Instanzdetails anzeigen und ausblenden

  Sie können die Details einer bestimmten NetScaler-Instanz anzeigen und ausblenden, indem Sie in der Spalte Name auf den Namen der Instanz klicken.
  Sie können auch auf Alle erweitern klicken, um alle Instanzknoten zu erweitern, und Alle reduzieren, um alle Instanzknoten zu reduzieren.

- Minianwendungen hinzufügen und entfernen

  Sie können auch Minianwendungen hinzufügen, um andere Systeminformationen anzuzeigen.

  Um diese Minianwendungen hinzuzufügen, klicken Sie auf den Pfeil («) in der oberen rechten Ecke der Homepage, geben Sie Schlüsselwörter in das Suchfeld ein und klicken Sie dann auf

Los. Die zulässigen Zeichen sind: a-z, A-Z, 0—9, ^, $, * und _. Klicken Sie auf Los, ohne Zeichen in das Suchfeld einzugeben, um alle verfügbaren Minianwendungen anzuzeigen. Nachdem das Gadget angezeigt wurde, klicken Sie auf Zum Dashboard hinzufügen.

Derzeit können Sie der Homepage die folgenden Minianwendungen hinzufügen:

- **Hypervisor-Details:** Das Gadget "Hypervisor-Details"zeigt Details zu Citrix Hypervisor Verfügbarkeit, Edition, Version, iSCSI Qualified Name (IQN), Produktcode, Seriennummer, Erstellungsdatum und Buildnummer an.
- **Lizenzen:** Das Lizenzen-Gadget zeigt die folgenden Details an: die SDX-Hardwareplattform, die maximale Anzahl der auf der Plattform unterstützten Instanzen, den maximal unterstützten Durchsatz in Mbit/s und den verfügbaren Durchsatz in Mbit/s.

Wenn Sie ein Gadget entfernen, das standardmäßig auf der Homepage verfügbar ist, können Sie es wieder zur Homepage hinzufügen, indem Sie nach dem Gadget suchen.

Ports

Die folgenden Ports müssen auf der SDX-Appliance geöffnet sein, damit sie ordnungsgemäß funktioniert.

Typ	Port	Details
TCP	80	Wird für eingehende HTTP-Anfragen (GUI und NITRO) verwendet Eine der primären Schnittstellen für den Zugriff auf die SDX Management Service-Schnittstelle.
TCP	443	Wird für eingehende sichere HTTP-Anfragen (GUI und NITRO) verwendet Eine der primären Schnittstellen für den Zugriff auf die SDX Management Service-Schnittstelle.
TCP	22	Wird für den SSH- und SCP-Zugriff auf die SDX Management Service-Schnittstelle verwendet.

Typ	Port	Details
UDP	162	Die SDX Management Service-Schnittstelle wartet auf SNMP-Traps von den NetScaler-Instanzen, die auf der SDX-Appliance gehostet werden.
UDP	161	Die SDX Management Service-Schnittstelle wartet auf SNMP-Walks/Get-Anforderungen.

Data Governance

November 23, 2023

Was ist ein NetScaler ADM Service Connect?

NetScaler Application Delivery Management (ADM) Service Connect ist eine Funktion, die eine nahtlose Integration von NetScaler SDX-Appliances in den NetScaler ADM Service ermöglicht. Mit dieser Funktion kann die NetScaler SDX-Appliance automatisch eine sichere Verbindung mit dem NetScaler ADM Service herstellen und System-, Nutzungs- und Telemetriedaten an diesen senden. Basierend auf diesen Daten erhalten Sie Erkenntnisse und Empfehlungen für Ihre NetScaler-Infrastruktur auf dem NetScaler ADM Service.

Mithilfe der NetScaler ADM Service Connect-Funktion und der Integration Ihrer NetScaler SDX-Appliances in den NetScaler ADM Service können Sie all Ihre NetScaler- und NetScaler Gateway-Ressourcen verwalten, egal ob on-premises oder in der Cloud. Darüber hinaus profitieren Sie vom Zugriff auf eine Vielzahl von Sichtbarkeitsfunktionen, die Ihnen helfen, Leistungsprobleme, hohe Ressourcennutzung, kritische Fehler usw. schnell zu erkennen. Der NetScaler ADM Service bietet eine Vielzahl von Funktionen für Ihre NetScaler-Instanzen und -Anwendungen. Weitere Informationen zum NetScaler ADM Service finden Sie unter NetScaler Application Delivery ManagementService.

> **Wichtig**
>
> - Dieses Dokument bezieht sich auf NetScaler SDX-Appliances. Weitere Informationen zur

> NetScaler-Appliance finden Sie unter Einführung in NetScaler ADM Service Connect für NetScalerAppliances.
>
> - NetScaler Gateway unterstützt auch die NetScaler ADM Service Connect-Funktion. Der Einfachheit halber wird die NetScaler Gateway-Appliance in den nachfolgenden Abschnitten nicht explizit aufgerufen.

Hinweis:
Die NetScaler ADM Service Connect-Funktion wurde für NetScaler-Instances und NetScaler Gateway-Instanzen veröffentlicht. Die entsprechende Funktionalität des NetScaler ADM Service ist jedoch in der kommenden Version verfügbar. Der Nutzen dieser Funktion wird in Kürze mit dem NetScaler ADM Service Release ausgeschöpft. Citrix wird diesen Hinweis aktualisieren, wenn es passiert.
Die Vorteile dieser neuen Funktion können genutzt werden, sobald sie im NetScaler ADM Service veröffentlicht wurden.

Was ist der NetScaler ADM Service?

Der NetScaler ADM Service ist eine cloudbasierte Lösung, die Sie bei der Verwaltung, Überwachung, Orchestrierung, Automatisierung und Fehlerbehebung Ihrer NetScaler SDX-Instances unterstützt, indem sie Ihnen analytische Erkenntnisse und kuratierte, auf maschinellem Lernen basierende Empfehlungen zu NetScaler SDX-Instances sowie zur Integrität, Leistung und Sicherheit von Anwendungen bietet. Weitere Informationen finden Sie unter NetScaler ADMService Overview.

Wie wird die NetScaler ADM Service Connect aktiviert?

NetScaler ADM Service Connect ist standardmäßig aktiviert, nachdem Sie NetScaler SDX auf Version 13.1 installiert oder aktualisiert haben.

Welche Daten werden mit NetScaler ADM Service Connect erfasst?

Die folgenden Details werden mithilfe von NetScaler ADM Service Connect erfasst:

- **Einzelheiten zu NetScaler SDX**
  - Verwaltungs-IP-Adresse
  - Beschreibung der Plattform
  - Plattformtyp
  - Hostname
  - System-ID
  - Codierte serielle ID
  - Version

  - Seriennummer
  - Host-ID
  - Typ
  - Buildtyp

- **Wichtige Nutzungsmetriken**
  - Prozentsatz der Verwaltungs-C
  - Prozentsatz der Speicherauslastung
  - CPU-Nutzung in Prozent
  - Systemverfügbarkeit
  - Datum und Uhrzeit des Systems

Wie werden die Daten verwendet?

Durch die Erfassung der Daten kann NetScaler zeitnahe und detaillierte Einblicke in Ihre NetScaler SDX-Installationen liefern, die Folgendes beinhalten:

- **Die wichtigsten Kennzahlen**. Einzelheiten zu den wichtigsten Kennzahlen in Bezug auf CPU, Arbeitsspeicher, Durchsatz und SSL-Durchsatz sowie Hinweise auf anomales Verhalten auf NetScaler SDX-Instances.
- **Kritische Fehler**. Alle kritischen Fehler, die möglicherweise auf Ihren NetScaler-Instances aufgetreten sind.
- **Beratung zur Bereitstellung**. Identifizieren Sie NetScaler-Instanzen, die im Standalone-Modus bereitgestellt werden, aber einen hohen Durchsatz aufweisen und anfällig für einen einzigen Fehlerpunkt sind.

Wie lange werden die gesammelten Daten aufbewahrt?

Alle gesammelten Daten werden nicht länger als 13 Monate aufbewahrt.

Wenn Sie beschließen, die Nutzung des Dienstes zu beenden, indem Sie die NetScaler ADM Service Connect-Funktion von NetScaler aus deaktivieren, werden alle zuvor gesammelten Daten nach einem Zeitraum von 30 Tagen gelöscht.

Wo werden die Daten gespeichert und wie sicher sind sie?

Alle von NetScaler ADM Service Connect gesammelten Daten werden in einer der drei Regionen gespeichert: Vereinigte Staaten, Europäische Union sowie Australien und Neuseeland (ANZ). Weitere Informationen finden Sie unter Geografische Überlegungen.

Die Daten werden sicher mit strenger Tenant-Isolation auf der Datenbankebene gespeichert.

Wie deaktiviere ich NetScaler ADM Service Connect?

Informationen zum Deaktivieren der Datenerfassung über NetScaler ADM Service Connect finden Sie unter So aktivieren und deaktivieren Sie die NetScaler ADM Service Connect.

Einführung in NetScaler ADM Service Connect für NetScaler SDX-Appliances

November 23, 2023

Der NetScaler ADM Service ist eine cloudbasierte Lösung, mit der Sie Ihre NetScaler SDX-Appliances verwalten, überwachen, orchestrieren, automatisieren und Fehler beheben können. Es bietet auch analytische Erkenntnisse und kuratierte auf maschinellem Lernen basierende Empfehlungen für den Zustand, die Leistung und die Sicherheit Ihrer Anwendungen. Weitere Informationen finden Sie unter NetScaler ADM Service.

NetScaler Application Delivery Management (ADM) Service Connect ist eine Funktion, die eine nahtlose Integration von NetScaler SDX-Appliances in den NetScaler ADM Service ermöglicht. Diese Funktion trägt dazu bei, dass NetScaler SDX-Appliances und der NetScaler ADM Service als ganzheitliche Lösung funktionieren, die den Kunden vielfältige Vorteile bietet.

Mit der NetScaler ADM Service Connect-Funktion kann die NetScaler SDX-Instanz automatisch eine Verbindung zum NetScaler ADM Service herstellen und System-, Nutzungs- und Telemetriedaten an ihn senden. Anhand dieser Daten bietet Ihnen der NetScaler ADM Service einige Einblicke und Empfehlungen zu Ihrer NetScaler SDX-Infrastruktur, z. B. die schnelle Identifizierung von Leistungsproblemen und eine hohe Ressourcennutzung.

Um die Leistungsfähigkeit des NetScaler ADM-Dienstes zu nutzen, können Sie sich dafür entscheiden, Ihre NetScaler SDX-Appliances in den NetScaler ADM Service zu integrieren. Der Onboarding-Prozess verwendet ADM Service Connect und macht das Erlebnis für Sie nahtlos und schneller.

> **Wichtige Hinweise**
>
> - NetScaler ADM Service Connect ist jetzt auf NetScaler MPX-, SDX- und VPX-Instanzen sowie NetScaler Gateway-Appliances verfügbar.
> - NetScaler ADM Service Connect ist für den NetScaler ADM Service noch nicht verfügbar.

Weitere Informationen finden Sie unter Data Governance.

Wie verbindet der NetScaler ADM Service den Support mit dem NetScaler ADM Service?

Im Folgenden finden Sie einen allgemeinen Arbeitsablauf, der zeigt, wie die NetScaler ADM Service Connect-Funktion auf NetScaler mit dem NetScaler ADM Service interagiert.

1. Die NetScaler ADM-Dienstverbindungsfunktion der NetScaler SDX-Appliance stellt mithilfe einer regelmäßigen Testanforderung automatisch eine Verbindung zum NetScaler ADM Service her.
2. Diese Anfrage enthält System-, Nutzungs- und Telemetriedaten. Anhand dieser Daten gibt Ihnen der NetScaler ADM Service einige Einblicke und Empfehlungen zu Ihrer NetScaler-Infrastruktur, z. B. die schnelle Identifizierung von Leistungsproblemen und eine hohe Ressourcennutzung.
3. Sie können sich die Erkenntnisse und Empfehlungen ansehen und entscheiden, Ihre NetScaler SDX-Appliances in den NetScaler ADM Service zu integrieren, um mit der Verwaltung Ihrer NetScaler SDX-Appliances zu beginnen.
4. Wenn Sie sich für ein Onboarding entscheiden, hilft Ihnen die NetScaler ADM Service Connect-Funktion dabei, das Onboarding nahtlos abzuschließen.

Auf welchen Versionen von NetScaler wird NetScaler ADM Service Connect unterstützt?

NetScaler ADM Service Connect wird auf allen NetScaler-Plattformen und allen Appliance-Modellen (MPX, VPX und SDX) unterstützt. Ab NetScaler Version 13.0 Build 64.xx ist NetScaler ADM Service Connect standardmäßig für NetScaler SDX-Appliances aktiviert.

Wie aktiviere ich NetScaler ADM Service Connect?

Wenn Sie bereits NetScaler-Kunde sind und ein Upgrade auf NetScaler Version 13.0 Build 64.xx durchführen, ist NetScaler ADM Service Connect standardmäßig als Teil des Upgrade-Vorgangs aktiviert.

Wenn Sie ein neuer NetScaler-Kunde sind und NetScaler Version 13.0 Build 64.xx installieren, ist NetScaler ADM Service Connect standardmäßig als Teil des Installationsvorgangs aktiviert.

> **Hinweis**
>
> Im Gegensatz zu den neuen NetScaler-Appliances finden bestehende NetScaler SDX-Appliances die Route über Citrix Insight Service (CIS) oder Call Home.

Wie aktiviere und deaktiviere ich NetScaler ADM Service Connect?

Sie können die NetScaler ADM Service Connect über CLI-, GUI- oder NITRO-API-Methoden aktivieren und deaktivieren.

Verwenden der CLI

Um den NetScaler ADM Service zu aktivieren, stellen Sie eine Verbindung mit der CLI her

Geben Sie in der Befehlszeile Folgendes ein:

```
set autoreg_setting autoreg=true
```

Um den NetScaler ADM Service zu deaktivieren, stellen Sie eine Verbindung mit der CLI her.

Geben Sie in der Befehlszeile Folgendes ein:

```
set autoreg_setting autoreg=false
```

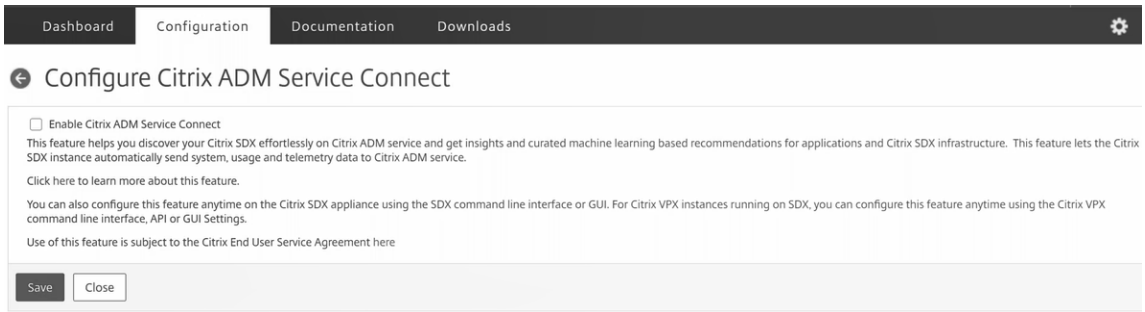
Um die NetScaler ADM-Dienstverbindungseinstellungen mithilfe der CLI anzuzeigen

```
show autreg_setting

                autoreg: true

     is_banner_displayed: true

Done
```

Verwenden der GUI

Um den NetScaler ADM Service zu deaktivieren, stellen Sie eine Verbindung mit der NetScaler-GUI her.

1. Navigieren Sie zu **System**. Klicken Sie auf der **Systemseite** im Abschnitt **Systemeinstellungen** auf **NetScaler ADM Service Connect konfigurieren** .
2. Deaktivieren Sie auf der Seite **ADM-Parameter konfigurieren** die Option **NetScaler ADM Service Connect aktivieren**und klicken Sie auf **OK**.



Verwenden der NITRO-API

Sie können NetScaler ADM Service Connect mit dem Befehl NITRO deaktivieren.


```
curl -X PUT -H "Content-Type:application/json"http://192.0.2.10/nitro
/v1/config/sdx_autoreg -d '{ "sdx_autoreg":{ "autoreg":"false" } } '
-u nsroot:Test@1
```

Verhalten des integrierten NetScaler ADM-Agenten

Ab NetScaler Version 13.0 Build 61.xx und höher verfügen NetScaler SDX-Instances über einen integrierten Agenten mit ADM Service Connect-Funktionalität. Der in NetScaler ADM integrierte Agent, der auf NetScaler SDX-Instanzen verfügbar ist, startet wie ein aktiver Daemon und kommuniziert mit dem ADM Service. Nachdem die Kommunikation mit dem ADM-Dienst hergestellt wurde, aktualisiert sich der eingebaute Agent regelmäßig automatisch auf die neueste Softwareversion.

Referenzen

Weitere Informationen zu NetScaler ADM Service Connect finden Sie in den folgenden Themen:

- Data Governance: Data Governance.
- NetScaler ADM Service: NetScaler Application Delivery ManagementService.

Einzelbündel-Upgrade

November 23, 2023

Hinweis: Die NetScaler ADM Service Connect ist standardmäßig aktiviert, nachdem Sie die NetScaler SDX-Appliance auf Version 13.1 installiert oder aktualisiert haben. Weitere Informationen finden Sie unter Data Governance und NetScaler ADMService Connect.

Das Single-Bundle-Upgrade, das ab Version 11.0 verfügbar ist, kombiniert alle Komponenten außer dem NetScaler VPX-Instanz-Image und der LOM-Firmware in einer einzigen Image-Datei. Diese Datei wird SDX-Image genannt.

> **Hinweis**
>
> Ab Version 12.0 Build 57.19 wird die Lights Out Management (LOM)-Firmware zum SBI hinzugefügt, und Citrix Kunden müssen LOM nicht separat aktualisieren. Die LOM-Firmware wurde nicht von Citrix geschrieben.

Mit diesem Image können Sie alle Komponenten in einem einzigen Schritt aktualisieren, wodurch die Gefahr einer Inkompatibilität zwischen verschiedenen Komponenten ausgeschlossen wird. Ein

einzelnes Bundle-Upgrade stellt außerdem sicher, dass auf Ihrer Appliance immer eine Version ausgeführt wird, die Citrix getestet hat und unterstützt. Da alle SDX-Komponenten in einer einzigen Datei zusammengefasst sind, ist die SDX-Imagedatei größer als die Management Service-Imagedatei.

Der Dateiname des Images hat das Format `build-sdx-13.1-<build_number>.tgz`. Nachdem der Management Service auf SDX 13.1 aktualisiert wurde, zeigt die neue GUI nicht die Optionen zum Hochladen der Citrix Hypervisor Imagedatei, zusätzlicher Packs oder Hotfixes an. Die Optionen fehlen, da SDX 13.1 das Upgrade einzelner Komponenten nicht unterstützt.

Wichtige Hinweise

- Das Upgrade eines einzelnen Pakets ist ein mehrstufiger Vorgang, der bis zu 90 Minuten dauern kann.
- Zunächst wird der Management Service auf die neuere, bereitgestellte Version aktualisiert. Während des Upgrades geht die Konnektivität zum Management Service möglicherweise verloren. Stellen Sie erneut eine Verbindung zum Management Service her, um den Status des Upgrades zu überwachen.
- Als Nächstes aktualisiert der neue Management Service den Citrix Hypervisor und schließt den Rest des Appliance-Upgrades ab. Der Management Service ab Version 11.0 und höher kann das vollständige Citrix Hypervisor Upgrade durchführen.
- Starten Sie das Gerät während des Citrix Hypervisor-Upgrades nicht neu.
- Citrix empfiehlt, dass Sie eine serielle Citrix Hypervisor-Konsole (oder LOM-Konsole) verwenden, um das Citrix Hypervisor Upgrade zu überwachen.

Aktualisieren Sie die gesamte Appliance auf 13.1

Hinweis: Der Upgrade-Vorgang startet die gesamte SDX-Appliance, einschließlich aller VPX-Instanzen, mehrmals neu. Wenn sich die VPX-Instanzen in einem HA-Setup befinden, führen Sie vor der Durchführung dieses Verfahrens einen Failover aller primären HA-Knoten zum sekundären Knoten durch. Wenn Sie keine HA-Bereitstellung haben, planen Sie die Ausfallzeit entsprechend ein.

Aktualisieren der Appliance:

1. Laden Sie die einzelne Bundle-Imagedatei hoch, navigieren Sie zu **Konfiguration > Management Service > Software-Images**, und klicken Sie dann auf **Hochladen**.
2. Navigieren Sie zu **Konfiguration > System > Systemadministration**.
3. Klicken Sie in der Gruppe Systemadministration auf **Appliance aktualisieren**.
   Der Upgrade-Vorgang dauert einige Minuten.

Vor dem Upgrade zeigt der Management Service die folgenden Informationen an:

- Einzelbündel-Imagedateiname.

- Die aktuelle Version von SDX, die auf Ihrer Appliance ausgeführt wird.
- Die ausgewählte Version, auf die die Appliance aktualisiert werden soll.
- Ungefähre Zeit für das Upgrade der Appliance.
- Verschiedene Informationen.

Bevor Sie auf **Appliance aktualisieren**klicken, vergewissern Sie sich, dass Sie alle auf dem Bildschirm angezeigten Informationen überprüft haben. Sie können den Upgrade-Vorgang nicht abbrechen, sobald er gestartet wurde.

Unterstützte Upgradepfade

	11.1	12.0	12.1	13.0	13.1	14.1
10.5 oder 11.0	J	J	J	N*	N*	N*
11.1—65.x und höher	Nicht verfügbar	Nicht zu empfehlen	12.1-56.x und höher	J	J	J
12.1	Nicht verfügbar	Nicht verfügbar	Nicht zu empfehlen	J	J	J

*Von älteren Builds der Versionen 10.5, 11.0 und 11.1 müssen Sie zuerst auf Version 11.1 oder 12.1 und dann auf Version 13.0, 13.1 oder 14.1 aktualisieren.

Verwandte Informationen

NetScaler SDX-Kompatibilitätsmatrix für Hardware und Software

Entmystifizierung des Upgrade-Prozesses der NetScaler SDX-Appliance

NetScaler-Instanz aktualisieren

November 23, 2023

> **Hinweise**
>
> - Die NetScaler ADM Service Connect ist standardmäßig aktiviert, nachdem Sie die NetScaler SDX-Appliance auf Version 13.1 installiert oder aktualisiert haben. Weitere Informationen finden Sie unter Data Governance und NetScaler ADMService Connect.
> - Der Upgrade-Prozess der NetScaler SDX-Appliance erfordert einen einzigen Neustart statt

> zwei Neustarts ab Version 13.1 Build 37.x.

Beim Aktualisieren der NetScaler-Instanzen wird die Build-Datei hochgeladen und anschließend die NetScaler-Instanz aktualisiert.

> **Wichtig**
>
> Das Herabstufen einer ADC-Instanz über den Management Service wird nicht unterstützt. Verwenden Sie zum Downgrade die Instanz-CLI.

Laden Sie die NetScaler-Software-Images auf die NetScaler SDX-Appliance hoch, bevor Sie die NetScaler-Instanzen aktualisieren. Für die Installation einer neuen Instanz benötigen Sie die NetScaler XVA-Datei.

Im Bereich **Software-Images** können Sie die folgenden Details anzeigen.

- **Name:** Name der Image-Datei der NetScaler-Instanzsoftware. Der Dateiname enthält die Release-Nummer und die Buildnummer. Beispielsweise bezieht sich der Dateiname build-10-53.5_nc.tgz auf Release 10 Build 53.5.
- **Letzte Änderung:** Datum, an dem die Datei zuletzt geändert wurde.
- **Größe:** Größe der Datei in MB.

So laden Sie ein Software-Image hoch

1. Erweitern Sie im Navigationsbereich NetScaler, und klicken Sie dann auf **Software-Images**.
2. Klicken Sie im Bereich **Software-Images** auf **Upload**.
3. Klicken **Sie im Dialogfeld NetScaler Software-Image hochladen** auf **Durchsuchen** und wählen Sie die NetScaler-Imagedatei aus, die Sie hochladen möchten.
4. Klicken Sie auf **Upload**. Die Imagedatei wird im Bereich NetScaler Software Images angezeigt.

So erstellen Sie eine Backup durch Herunterladen einer Build-Datei

1. Wählen Sie im Bereich Software-Images die Datei aus, die Sie herunterladen möchten, und klicken Sie dann auf **Herunterladen**.
2. Wählen Sie im Meldungsfeld in der Liste **Speichern** die Option **Speichern unter** aus.
3. Navigieren Sie im Meldungsfeld Speichern unter zu dem Speicherort, an dem Sie die Datei speichern möchten, und klicken Sie dann auf **Speichern**.

So laden Sie eine XVA-Datei hoch

1. Erweitern Sie im Navigationsbereich NetScaler, und klicken Sie dann auf **Software-Images**.

2. Klicken Sie im Bereich Software-Images auf der Registerkarte **XVA-Dateien** auf **Hochladen**.
3. Klicken **Sie im Dialogfeld NetScaler XVA-Datei hochladen** auf **Durchsuchen** und wählen Sie die NetScaler XVA-Datei aus, die Sie hochladen möchten.
4. Klicken Sie auf **Upload**. Die XVA-Datei wird im Bereich **XVA-Dateien** angezeigt.

So erstellen Sie eine Backup durch Herunterladen einer XVA-Datei

1. Wählen Sie im Bereich XVA-Dateien die Datei aus, die Sie herunterladen möchten, und klicken Sie dann auf **Herunterladen**.
2. Wählen Sie im Meldungsfeld in der Liste Speichern die Option **Speichern unter** aus.
3. Navigieren Sie im Meldungsfeld **Speichern unter** zu dem Speicherort, an dem Sie die Datei speichern möchten, und klicken Sie dann auf **Speichern**.

NetScaler VPX-Instanzen aktualisieren

Sie können den Management Service verwenden, um eine oder mehrere der VPX-Instanzen zu aktualisieren, die auf der Appliance ausgeführt werden. Stellen Sie vor dem Upgrade einer Instanz sicher, dass Sie den richtigen Build auf die SDX-Appliance hochgeladen haben.

Bevor Sie mit dem Upgrade einer Instanz beginnen, sollten Sie sich mit dem Lizenzierungsrahmen und den Lizenztypen vertraut machen. Für ein Upgrade der Software-Edition (z. B. von einer Standard Edition auf die Enterprise Edition oder von einer Enterprise Edition auf die Platin-Edition) sind möglicherweise neue Lizenzen erforderlich. Beachten Sie außerdem Folgendes:

- Um einen Konfigurationsverlust zu verhindern, speichern Sie die Konfiguration auf jeder Instanz, bevor Sie ein Upgrade von Instanzen durchführen.
- Sie können eine einzelne Instanz auch vom Knoten Instanzen aus aktualisieren. Wählen Sie dazu die Instanz im Knoten Instanzen aus. Wählen Sie im Detailbereich die Instanz aus, und klicken Sie dann im Dropdown-Menü Aktionen auf Upgrade.

> **Wichtig**
>
> Wenn Sie den SDX Management Service und nicht die VPX-GUI verwenden, um VPX-Instanzen zu aktualisieren, sind die Upgrade-Images Teil der Backup-Datei und ermöglichen Ihnen eine reibungslose Wiederherstellung der Instanz.

So aktualisieren Sie VPX-Instanzen

1. Klicken Sie auf der Registerkarte **Konfiguration** im Navigationsbereich auf **NetScaler**.
2. Klicken Sie im Detailbereich unter **NetScaler Configuration**auf **Upgrade**.

3. Wählen Sie im Dialogfeld **NetScaler aktualisieren** in **Software-Image**die NetScaler-Upgrade-Build-Datei der Version aus, auf die Sie aktualisieren möchten.
4. Wählen Sie in der Dropdownliste **Instanz-IP-Adresse** die IP-Adressen der Instanzen aus, die Sie aktualisieren möchten.
5. Klicken Sie auf **OK** und dann auf Schließen.

Verwandte Informationen

NetScaler SDX-Kompatibilitätsmatrix für Hardware und Software

Entmystifizierung des Upgrade-Prozesses der NetScaler SDX-Appliance

Verwalten und Überwachen der SDX-Appliance

February 15, 2024

Nachdem Ihre NetScaler SDX-Appliance betriebsbereit ist, können Sie verschiedene Aufgaben ausführen, um die Appliance über die Management Service-Benutzeroberfläche zu verwalten und zu überwachen.

Ändern der Netzwerkkonfiguration der SDX-Appliance

Sie können die Netzwerkkonfigurationsdetails ändern, die Sie bei der Erstkonfiguration für die SDX-Appliance angegeben haben.

Um die Netzwerkkonfiguration der SDX-Appliance zu ändern, klicken Sie auf **System**. Klicken Sie im Bereich **System** unter der Gruppe **Setup-Appliance** auf **Netzwerkkonfiguration** und geben Sie die Details in den Assistenten ein.

> **Hinweis:** Wenn Sie in der **Netzwerkkonfiguration**den Zugriff auf den Citrix Hypervisor aktivieren, wird die Warnmeldung „Der Zugriff wird nach sechs Stunden automatisch deaktiviert “angezeigt.

Ändern Sie das Kennwort des Standardbenutzerkontos

Das Standardbenutzerkonto bietet vollständigen Zugriff auf alle Funktionen der NetScaler SDX-Appliance. Um die Sicherheit zu gewährleisten, verwenden Sie das Standardadministratorkonto nur bei Bedarf. Nur Personen, deren Aufgaben vollen Zugriff erfordern, müssen das Kennwort für das Standardadministratorkonto kennen. Citrix empfiehlt, das standardmäßige Administratorkennwort

häufig zu ändern. Wenn Sie das Kennwort verlieren, können Sie das Kennwort auf den Standardwert zurücksetzen, indem Sie die Appliance-Einstellungen auf die Werkseinstellungen zurücksetzen, und Sie können dann das Kennwort ändern.

Um das Kennwort des Standardbenutzerkontos zu ändern, klicken Sie auf **System** > **Benutzerverwaltung** > **Benutzer**. Wählen Sie einen Benutzer und klicken Sie auf **Bearbeiten**, um das Kennwort zu ändern.

Ändern der Zeitzone auf der Appliance

Sie können die Zeitzone des Management Service und des Citrix Hypervisor ändern. Die Standardzeitzone ist UTC.

Um die Zeitzone zu ändern, klicken Sie auf **System** und klicken Sie in der Gruppe **Systemeinstellungen** auf **Zeitzone ändern**.

Hostnamen der Appliance ändern

Sie können den Hostnamen des Management Service ändern, indem Sie zu **System > Systemeinstellungen > Hostname ändern** navigieren.
Der Citrix Hypervisor-Hostname wird während des Backup-/Wiederherstellungsvorgangs gesichert und wiederhergestellt. Beim Zurücksetzen der Konfiguration wird der Citrix Hypervisor-Hostname auf den Standardwert “netscaler-sdx”zurückgesetzt.

VLAN-Filterung

Die VLAN-Filterung ermöglicht die Trennung von Daten zwischen VPX-Instanzen, die sich einen physischen Port teilen. Wenn Sie beispielsweise zwei VPX-Instanzen auf zwei verschiedenen VLANs konfiguriert haben und die VLAN-Filterung aktivieren, kann eine Instanz den Datenverkehr der anderen Instanz nicht anzeigen. Wenn die VLAN-Filterung deaktiviert ist, können alle Instanzen die markierten oder nicht getaggten Broadcast-Pakete sehen, aber die Pakete werden auf Softwareebene verworfen. Wenn die VLAN-Filterung aktiviert ist, erreicht jedes markierte Broadcast-Paket nur die Instanz, die zum entsprechenden markierten VLAN gehört. Wenn keine der Instanzen zum entsprechenden markierten VLAN gehört, wird das Paket auf Hardwareebene (NIC) verworfen.

Wenn die VLAN-Filterung auf einer Schnittstelle aktiviert ist, kann eine begrenzte Anzahl von getaggten VLANs auf dieser Schnittstelle verwendet werden. 63 getaggte VLANs auf einer 10G-Schnittstelle und 32 getaggte VLANs auf einer 1G-Schnittstelle. Eine VPX-Instanz empfängt nur die Pakete mit den konfigurierten VLAN-IDs. Starten Sie die mit einer Schnittstelle verknüpften VPX-Instanzen neu, wenn Sie den Status des VLAN-Filters auf dieser Schnittstelle von DISABLED in ENABLED ändern.

Die VLAN-Filterung ist standardmäßig auf der SDX-Appliance aktiviert. Wenn Sie die VLAN-Filterung auf einer Schnittstelle deaktivieren, können Sie bis zu 4096 VLANs auf dieser Schnittstelle konfigurieren.

Hinweis: Die VLAN-Filterung kann nur auf einer SDX-Appliance deaktiviert werden, auf der Citrix Hypervisor Version 6.0 ausgeführt wird.

Um die VLAN-Filterung auf einer Schnittstelle zu aktivieren, klicken Sie auf **System** > **Schnittstellen**. Wählen Sie eine Schnittstelle aus und klicken Sie auf **VLAN-Filter** und geben Sie die Details ein, um die VLAN-Filterung zu

Konfigurieren der Uhrsynchronisierung

Wenn Sie die Network Time Protocol (NTP) -Synchronisierung aktivieren, wird der Management Service neu gestartet. Sie können Ihre SDX-Appliance so konfigurieren, dass sie ihre lokale Uhr mit einem NTP-Server synchronisiert. Daher hat die Uhr auf der SDX-Appliance dieselben Datums- und Uhrzeiteinstellungen wie die anderen Server in Ihrem Netzwerk. Die Konfiguration der Uhrsynchronisierung ändert sich nicht, wenn die Appliance neu gestartet, aktualisiert oder heruntergestuft wird. In einem Hochverfügbarkeits-Setup wird die Konfiguration jedoch nicht an die sekundäre NetScaler-Instanz weitergegeben.

Die Uhr wird sofort synchronisiert, wenn Sie einen NTP-Server hinzufügen oder einen der Authentifizierungsparameter ändern. Sie können die NTP-Synchronisierung auch explizit aktivieren und deaktivieren.

Hinweis: Wenn Sie keinen lokalen NTP-Server haben, finden Sie eine Liste der öffentlichen NTP-Server mit offenem Zugriff auf der offiziellen NTP-Website http://www.ntp.org. Bevor Sie Ihren NetScaler für die Verwendung eines öffentlichen NTP-Servers konfigurieren, lesen Sie unbedingt die Seite Rules of Engagement (Link finden Sie auf allen Public Time Server-Seiten).

Um einen NTP-Server zu konfigurieren, klicken Sie auf **System > NTP-Server**.

So aktivieren Sie NTP-Synchronisierung

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **NTP-Server**.
2. Klicken Sie im Detailbereich auf **NTP-Synchronisierung**.
3. Wählen Sie im Dialogfeld **NTP-Synchronisierung** die Option **NTP-Synchronisierung aktivieren**.
4. Klicken Sie auf **OK**und dann auf **Schließen**.

So ändern Sie Authentifizierungsoptionen

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **NTP-Server**.

2. Klicken Sie im Detailbereich auf **Authentication Parameters**.
3. Legen **Sie im Dialogfeld "Authentifizierungsoptionen ändern** "die folgenden Parameter fest:

    - **Authentifizierung**—NTP-Authentifizierung aktivieren. Mögliche Werte: YES, NO. Standard: YES.
    - **Vertrauenswürdige Schlüsselkennungen**—Die vertrauenswürdigen Schlüsselkennungen Beim Hinzufügen eines NTP-Servers wählen Sie eine Schlüsselkennung aus dieser Liste aus. Mindestwert: 1. Maximaler Wert: 65534
    - **Revoke-Intervall**—Das Intervall zwischen der Neuzuordnung bestimmter kryptografischer Werte, die vom Autokey-Schema verwendet werden, als Potenz von 2 in Sekunden. Standardwert: 17 (2^17=36 Stunden).
    - **Automax-Intervall**—Das Intervall zwischen der Regenerierung der mit dem Autokey-Protokoll verwendeten Sitzungsschlüsselliste mit einer Potenz von 2 in Sekunden. Standardwert: 12 (2^12=1,1 Stunden).

4. Klicken Sie auf **OK**und dann auf **Schließen**.

Zeigen Sie die Eigenschaften der SDX-Appliance an

Zeigen Sie Systemeigenschaften wie die Anzahl der CPU-Kerne und SSL-Chips, den gesamten verfügbaren Speicher und freien Speicher sowie verschiedene Produktdetails auf der Registerkarte **Konfiguration** an.

Um die Eigenschaften der SDX-Appliance anzuzeigen, klicken Sie auf die Registerkarte **Konfiguration** .

Sie können die folgenden Informationen zu Systemressourcen, Hypervisor, Lizenz und System anzeigen:

Systemressourcen:

- **Gesamtzahl der CPU-Kerne;** Die Anzahl der CPU-Kerne auf der SDX-Appliance.
- **SSL-Chips insgesamt:** Die Gesamtzahl der SSL-Chips auf der SDX-Appliance.
- **Kostenlose SSL-Chips:** Die Gesamtzahl der SSL-Chips, die keiner Instanz zugewiesen wurden.
- **Gesamtspeicher (GB): Gesamter** Gerätespeicher in GB.
- **Freier Speicher (GB):** Freier Gerätespeicher in GB.

Hypervisor-Informationen:

- **Betriebszeit:** Zeit seit dem letzten Neustart der Appliance in Tagen, Stunden und Minuten.
- **Ausgabe:** Die Edition des Citrix Hypervisor, die auf der SDX-Appliance installiert ist.
- **Version:** Die Version des Citrix Hypervisor, die auf der SDX-Appliance installiert ist.

- **iSCSI-IQN:** Der qualifizierte iSCSI-Name.
- **Produktcode:** Produktcode von Citrix Hypervisor.
- **Seriennummer:** Seriennummer von Citrix Hypervisor.
- **Erstellungsdatum:** Erstellungsdatum von Citrix Hypervisor.
- **Buildnummer:** Buildnummer von Citrix Hypervisor.
- **Zusatzpaket:** Version des Zusatzpakets, das auf der SDX-Appliance installiert ist.

Informationen zur Lizenz:

- **Plattform:** Modellnummer der Hardwareplattform, basierend auf der installierten Lizenz.
- **Maximale Instanzen:** Die maximale Anzahl von Instanzen, die Sie auf der SDX-Appliance basierend auf der installierten Lizenz einrichten können.
- **Verfügbare Instanzen (gemeinsam genutzt):** Die Anzahl der Instanzen, die abhängig von der Anzahl der noch verfügbaren CPU-Kerne konfiguriert werden können.
- **Maximaler Durchsatz (Mbit/s):** Der maximale Durchsatz, der auf der Appliance basierend auf der installierten Lizenz erreicht werden kann.
- **Verfügbarer Durchsatz (Mbit/s):** Der verfügbare Durchsatz basierend auf der installierten Lizenz.

Informationen zur Anlage:

- **Plattform:** Modellnummer der Hardwareplattform.
- **Produkt:** Typ des NetScaler-Produkts.
- **Build:** NetScaler Release und Build läuft auf der SDX-Appliance.
- **IP-Adresse:** Die IP-Adresse des Management Service.
- **Host-ID:** Citrix Hypervisor Host-ID.
- **Systemkennung:** Citrix Hypervisor-Systemkennung.
- **Seriennummer:**Citrix Hypervisor Seriennummer.
- **Systemzeit:** Systemzeit angezeigt im Format Tag Monat Datum Stunden:Min:Sek Zeitzone Jahresformat.
- **Betriebszeit:** Zeit seit dem letzten Neustart des Management Service in der Anzahl der Tage, Stunden und Minuten.
- **BIOS-Version:** BIOS-Version.

Gerätedurchsatz in Echtzeit anzeigen

Der Gesamtdurchsatz der SDX-Appliance für eingehenden und ausgehenden Datenverkehr wird in Echtzeit in einem Diagramm dargestellt, das in regelmäßigen Abständen aktualisiert wird. Standardmäßig werden Durchsätze für eingehenden und ausgehenden Verkehr zusammen in der Grafik dargestellt.

Um den Durchsatz der SDX-Appliance anzuzeigen, klicken Sie in der GUI auf **Dashboard** und überprüfen Sie**Systemdurchsatz (Mbit/s)**.

CPU- und Speicherauslastung in Echtzeit anzeigen

Sie können ein Diagramm der CPU- und Speicherauslastung der Appliance anzeigen. Das Diagramm wird in Echtzeit geplottet und in regelmäßigen Abständen aktualisiert.

Um die CPU- und Speicherauslastung der SDX-Appliance anzuzeigen, klicken Sie in der GUI auf **Dashboard** und überprüfen Sie **Management Service Statistics**.

CPU-Auslastung für alle Kerne anzeigen

Sie können die Verwendung jedes CPU-Kerns auf der SDX-Appliance anzeigen.

Im Bereich "**CPU-Kernauslastung** "werden folgende Details angezeigt:

- **Kernnummer:** Die CPU-Kernnummer auf der Appliance.
- **Physische CPU:** Die physische CPU-Nummer dieses Kerns.
- **Hyper-Threads:** Die Hyper-Threads, die diesem CPU-Kern zugeordnet sind.
- **Instanzen:** Die Instanzen, die diesen CPU-Kern verwenden.
- **Durchschnittliche Kernauslastung:** Die durchschnittliche Kernauslastung, ausgedrückt als Prozentsatz.

Um die CPU-Auslastung für alle Kerne auf der SDX-Appliance anzuzeigen, klicken Sie in der GUI auf **Dashboard** und überprüfen Sie die**System-CPU-Auslastung (%)**.

Installieren Sie ein SSL-Zertifikat auf der SDX-Appliance

Die SDX-Appliance wird mit einem Standard-SSL-Zertifikat geliefert. Aus Sicherheitsgründen möchten Sie dieses Zertifikat möglicherweise durch Ihr eigenes SSL-Zertifikat ersetzen. Dazu müssen Sie zuerst Ihr SSL-Zertifikat in den Management Service hochladen und dann das Zertifikat installieren. Durch die Installation eines SSL-Zertifikats werden alle aktuellen Clientsitzungen mit dem Management

Service beendet. Melden Sie sich für zusätzliche Konfigurationsaufgaben beim Management Service an.

Um ein SSL-Zertifikat zu installieren, klicken Sie auf **System**. Klicken Sie in der Gruppe "**Appliance einrichten** "auf **SSL-Zertifikat installieren** und geben Sie die Details im Assistenten ein.

Zeigen Sie das SSL-Zertifikat im Management Service an

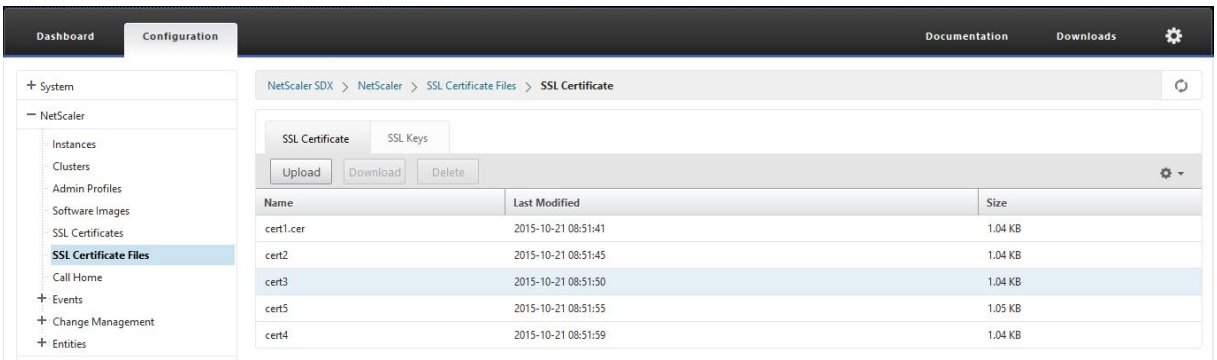
Der Management Service verwendet ein SSL-Zertifikat für sichere Clientverbindungen. Zeigen Sie die Details dieses Zertifikats an, wie Gültigkeitsstatus, Aussteller, Betreff, Tage bis zum Ablauf, gültig ab- und bis Datum, Version und Seriennummer.

Um das SSL-Zertifikat anzuzeigen, klicken Sie auf **System** und klicken Sie in der Gruppe **Gerät einrichten** auf **SSL-Zertifikat anzeigen**.

SSL-Zertifikate und Schlüssel für NetScaler-Instanzen

Separate Ansichten von SSL-Zertifikaten und Schlüsseln für NetScaler-Instances sorgen für eine verbesserte Benutzerfreundlichkeit. Verwenden Sie einen neuen Management Service-Knoten, SSL Certificate Files, um die SSL-Zertifikate und die entsprechenden öffentlichen und privaten Schlüsselpaare hochzuladen und zu verwalten, die auf NetScaler-Instances installiert werden können.

Um auf die SSL-Zertifikate und Schlüssel für NetScaler-Instanzen zuzugreifen, navigieren Sie zu **Konfiguration > NetScaler**SSL-Zertifikatsdateien.



Systemeinstellungen ändern

Aus Sicherheitsgründen können Sie angeben, dass der Management Service und eine VPX-Instanz nur über einen sicheren Kanal miteinander kommunizieren dürfen. Sie können auch den Zugriff auf die Management Service-Benutzeroberfläche einschränken. Clients können sich nur mit https an der Management Service-Benutzeroberfläche anmelden.

Um die Systemeinstellungen zu ändern, klicken Sie auf **Konfiguration > System** und klicken Sie in der Gruppe Systemeinstellungen auf **Systemeinstellungen ändern**.

Starten Sie das Gerät neu

Der Management Service bietet eine Option zum Neustart der SDX-Appliance. Während des Neustarts fährt die Appliance alle gehosteten Instanzen herunter und startet dann den Citrix Hypervisor neu. Wenn der Citrix Hypervisor neu gestartet wird, werden alle gehosteten Instanzen zusammen mit dem Management Service gestartet.

Um das Gerät neu zu starten, klicken Sie auf **Konfiguration > System** und klicken Sie in der Gruppe Systemadministration auf **Gerät neu starten.**

Gerät herunterfahren

Sie können die SDX-Appliance über den Management Service herunterfahren.

Um die Appliance herunterzufahren, klicken Sie auf **Konfiguration > System**, und klicken Sie in der Gruppe Systemadministration auf **Gerät herunterfahren**.

SDX-Verwaltungsdomänen

November 23, 2023

Mit der SDX-Funktion für administrative Domänen können Sie mehrere administrative Domänen erstellen. Sie können die administrativen Domänen verwenden, um Ressourcen für verschiedene Abteilungen zu trennen. Administrative Domänen können daher die Kontrolle über Ressourcen verbessern, und die Ressourcen können zur optimalen Nutzung auf verschiedene Domänen verteilt werden.

Eine SDX-Appliance wird mit festen Ressourcen wie CPU-Kernen, Datendurchsatz, Arbeitsspeicher, Speicherplatz, SSL-Chips und einer bestimmten Anzahl von Instanzen geliefert, die bereitgestellt werden können. Die Anzahl der Instanzen, die Sie erstellen können, hängt von der Lizenz ab.

Eine SDX-Appliance unterstützt bis zu drei Ebenen von Verwaltungsdomänen. Wenn die Appliance ausgeliefert wird, werden alle Ressourcen dem Besitzer zugewiesen.

Alle administrativen Domänen, die Sie erstellen, sind Unterdomänen der Eigentümerdomäne. In jedem Fall werden die Ressourcen der Subdomain aus dem Ressourcenpool der übergeordneten Domäne zugewiesen. Die Benutzer in einer Verwaltungsdomäne haben Zugriff auf die Ressourcen dieser Domäne. Sie haben weder Zugriff auf die Ressourcen anderer Domänen auf derselben

Hierarchieebene noch auf die übergeordneten Domänenressourcen, die ihrer Domäne nicht zugewiesen wurden. Benutzer in einer übergeordneten Domäne können jedoch auf die Ressourcen der Subdomänen dieser Domäne zugreifen.

Beispiele für die Zuweisung von Ressourcen zu Subdomänen

Tabelle 1 listet die Ressourcen der standardmäßigen Stammdomäne auf. Der SDX-Administrator kann diese Ressourcen Subdomänen zuweisen. In diesem Fall kann der Administrator beispielsweise maximal 10 CPU-Kerne und 840 GB Speicherplatz zuweisen.

Tabelle 1. Ressourcen für Besitzer

Prozessor-Kern	10
Durchsatz (Mbit/s)	18500
Arbeitsspeicher (MB)	87300
Speicherplatz (GB)	840
SSL-Chips	36
Instanzen	36

Tabelle 2 listet die Ressourcen auf, denen eine Subdomain namens *Test*zugewiesen wurde. Dieser Subdomain wurden 5 der 10 CPU-Kerne ihrer übergeordneten Domäne zugewiesen, sodass 5 Kerne übrig blieben, die anderen Subdomänen des Eigentümers zugewiesen werden können.

Tabelle 2. Testen der Ressourcen der Domäne

Prozessor-Kern	5
Durchsatz (Mbit/s)	1024
Arbeitsspeicher (MB)	2048
Speicherplatz (GB)	40
SSL-Chips	8
Instanzen	4

Beim Erstellen von Subdomänen kann der Administrator der *Testdomäne* nur die in Tabelle 2 aufgeführten Ressourcen zuweisen. Die *Testdomäne* kann nur eine Ebene von Unterdomänen haben, da nur drei Ebenen von Domänen erstellt werden können.

Die folgende Abbildung zeigt ein weiteres Beispiel für die Ressourcenzuweisung zwischen Subdomänen, wobei andere Werte als die in den Tabellen 1 und 2 aufgeführten verwendet werden.

Um eine Administratordomäne zu erstellen, navigieren Sie zu **Konfiguration > System > Administrative Domäne** und wählen Sie die gewünschten Optionen aus. Befolgen Sie die Anweisungen auf dem Bildschirm. Sobald eine neue Domäne erstellt wurde, melden Sie sich über die Anmeldeseite des Management Service bei dieser Domäne an und geben Sie den Domainnamen und den Benutzernamen an. Wenn Sie beispielsweise eine Domäne mit dem Namen NewDomain mit dem Benutzer NewUser erstellt haben, melden Sie sich als NewDomain\ NewUser an.

Weisen Sie Benutzer Domains zu

Wenn eine Subdomain erstellt wird, werden automatisch zwei Benutzergruppen erstellt: eine Admin-Gruppe und eine schreibgeschützte Gruppe. Standardmäßig ist jeder Benutzer Teil der Admin-Gruppe. Ein Benutzer kann zu mehreren Gruppen hinzugefügt werden.

Verwalten der RAID-Datenträgerzuweisung auf der SDX 22000-Plattform

November 23, 2023

Die NetScaler SDX 22040/22060/22080/22100/22120-Appliances verfügen jetzt über einen RAID-Controller (Redundant Array of Independent Disks), der bis zu acht physische Festplatten unterstützen kann. Mehrere Datenträger bieten nicht nur Leistungssteigerungen, sondern auch eine höhere Zuverlässigkeit. Zuverlässigkeit ist für eine SDX-Appliance besonders wichtig, da die Appliance viele virtuelle Maschinen hostet und ein Datenträgerausfall mehrere virtuelle Maschinen betrifft. Der RAID-Controller im Management Service unterstützt die RAID 1-Konfiguration, die die Datenträgerspiegelung implementiert. Das heißt, zwei Datenträger enthalten dieselben Daten. Wenn ein Datenträger im RAID 1-Array ausfällt, liefert der Spiegel sofort alle benötigten Daten.

Bei der RAID-1-Datenträgerspiegelung werden zwei physische Laufwerke in einem logischen Laufwerk kombiniert. Die nutzbare Kapazität eines logischen Laufwerks entspricht der Kapazität eines seiner physikalischen Laufwerke. Durch die Kombination von zwei 1-Terabyte-Laufwerken entsteht beispielsweise ein einziges logisches Laufwerk mit einer nutzbaren Gesamtkapazität von 1 Terabyte. Diese Kombination von Laufwerken wird der Appliance als ein einziges logisches Laufwerk angezeigt.

Die SDX-Appliance wird mit einer Konfiguration geliefert, die das logische Laufwerk 0 und das logische Laufwerk 1 umfasst. Das logische Laufwerk 0 ist dem Management Service und dem Citrix Hy-

pervisor zugewiesen, und das logische Laufwerk 1 ist den NetScaler-Instanzen zugewiesen, die Sie bereitstellen. Um mehr physische Laufwerke zu verwenden, müssen Sie neue logische Laufwerke erstellen.

Laufwerkseigenschaften und -vorgänge anzeigen

Eine SDX-Appliance unterstützt maximal acht Steckplätze für physische Laufwerke, d. h. ein Paar von vier Steckplätzen auf jeder Seite der Einheit. Sie können physische Laufwerke in die Steckplätze einlegen. Bevor Sie ein physisches Laufwerk verwenden können, müssen Sie es zu einem logischen Laufwerk machen.

Im Management Service enthält der Bildschirm **Konfiguration > System > RAID** Registerkarten für logische Laufwerke, physische Laufwerke und Speicher-Repositorys.

Logische Laufwerke

Auf der Registerkarte **Konfiguration > System > RAID > Logische Laufwerke** können Sie den Namen, den Status, die Größe jedes logischen Laufwerks und Informationen zu seinen physikalischen Komponentenlaufwerken anzeigen. In der folgenden Tabelle werden die Zustände des virtuellen Laufwerks beschrieben.

Status	Beschreibung
Optimale	Der Betriebszustand des virtuellen Laufwerks ist gut. Alle konfigurierten Laufwerke sind online.
Abgebaut	Der Betriebszustand des virtuellen Laufwerks ist nicht optimal. Eines der konfigurierten Laufwerke ist ausgefallen oder ist offline.
Fehlgeschlagen	Das virtuelle Laufwerk ist ausgefallen.
Offline	Das virtuelle Laufwerk ist für den RAID-Controller nicht verfügbar.

Sie können auch die Details der physikalischen Laufwerke anzeigen, die mit dem logischen Laufwerk verknüpft sind, indem Sie das logische Laufwerk auswählen und auf **Physikalisches Laufwerk anzeigen**klicken.

So erstellen Sie ein neues logisches Laufwerk

1. Navigieren Sie zu **Konfiguration** > **System** > **RAID**, und wählen Sie die Registerkarte **Logische Laufwerke** aus.

2. Klicken Sie auf **Hinzufügen**.
3. Wählen **Sie im Dialogfeld Logisches Laufwerk erstellen** zwei Steckplätze aus, die physische Betriebslaufwerke enthalten, und klicken Sie dann auf **Erstellen**.

Physische Laufwerke

Eine SDX-Appliance unterstützt maximal acht physische Steckplätze, d. h. ein Paar von vier Steckplätzen auf jeder Seite der Appliance. Auf der Registerkarte
Konfiguration > System > RAID > Physische Laufwerke können Sie die folgenden Informationen anzeigen:

- **Steckplatz:**—Physischer Steckplatz, der dem physischen Laufwerk zugeordnet ist
- **Größe:**—Größe des physikalischen Laufwerks.
- **Firmware-Status:**—Status der Firmware. Mögliche Werte:
  - **Online, hochgefahren:**—Physisches Laufwerk ist aktiv und wird von RAID gesteuert.
  - **Nicht konfiguriert (gut):**—Physisches Laufwerk ist in gutem Zustand und kann als Teil des logischen Laufwerkspaars hinzugefügt werden.
  - **Nicht konfiguriert (schlecht):**—Physisches Laufwerk ist nicht in gutem Zustand und kann nicht als Teil eines logischen Laufwerks hinzugefügt werden.
- **Foreign State:**—Zeigt an, ob der Datenträger leer ist.
- **Logisches Laufwerk:**—Assoziiertes logisches Laufwerk.

Im Bereich **Physikalische Laufwerke** können Sie die folgenden Aktionen für die physischen Laufwerke ausführen:

- **Initialize:**—Initialisiert den Datenträger. Sie können das physische Laufwerk initialisieren, wenn es sich nicht in einem guten Zustand befindet und als Teil des logischen Laufwerkspaars hinzugefügt werden muss.
- **Rebuild:**—Startet einen Neuaufbau des Laufwerks. Wenn ein Laufwerk in einer Laufwerksgruppe ausfällt, können Sie das Laufwerk neu erstellen, indem Sie die Daten, die vor dem Ausfall auf dem Laufwerk gespeichert waren, neu erstellen. Der RAID-Controller erstellt die auf den anderen Laufwerken in der Laufwerksgruppe gespeicherten Daten neu.
- **Lokalisieren:**—Suchen Sie das Laufwerk auf dem Gerät, das dadurch angezeigt wird, dass die dem Laufwerk zugeordnete Laufwerks-Aktivitäts-LED blinkt.
- **Lokalisieren beenden:**—Beenden Sie die Suche nach dem Laufwerk auf der Appliance.
- **Vorbereiten zum Entfernen:**—Deaktiviert das ausgewählte physische Laufwerk, damit es entfernt werden kann.

Speicherrepository

Auf der Registerkarte **Konfiguration > System > RAID > Speicher-Repository** können Sie den Status der Speicher-Repositories auf der SDX-Appliance anzeigen. Sie können auch Informationen zu einem Speicher-Repository-Laufwerk anzeigen, das nicht angeschlossen ist, und Sie können ein solches Laufwerk entfernen, indem Sie es auswählen und dann auf **Entfernen**klicken. Auf der Registerkarte **Speicherrepository** werden die folgenden Informationen zu jedem Speicherrepository angezeigt:

- **Name:**—Name des Speicher-Repository-Laufwerks.
- **Ist Laufwerk angeschlossen:**—Ob das Speicher-Repository angeschlossen ist oder nicht. Wenn das Laufwerk nicht angeschlossen ist, können Sie zum Löschen auf **Entfernen** klicken.
- **Größe:**—Größe des Speicher-Repositorys.
- **Verwendet:** —**Menge des verwendeten**Speicher-Repository-Speichers.

Hinzufügen eines logischen Laufwerks zur SDX 22000-Appliance So fügen Sie der SDX 22000-Plattform ein zusätzliches logisches Laufwerk hinzu:

1. Melden Sie sich beim Management Service an.
2. Navigieren Sie zu **Konfiguration > System > RAID**.
3. Setzen Sie auf der Rückseite der SDX 22000-Einheit die beiden leeren SSDs in die Steckplätze 4 und 5 ein. Sie können die SSDs in einem laufenden System hinzufügen.
   Hinweis: Stellen Sie sicher, dass die SSDs NetScaler-zertifiziert sind.
4. Navigieren Sie im Management Service zu**Konfiguration > System > RAID** und zur Registerkarte **Physikalische Laufwerke**. Sie würden die SSDs sehen, die Sie hinzugefügt haben.
5. Navigieren Sie zur Registerkarte **Logisches Laufwerk** und klicken Sie auf **Hinzufügen**.
6. Auf der Seite **Logischen Datenträger erstellen** :
   a) Wählen Sie in der Dropdownliste **Erster Steckplatz**4 aus.
   b) Wählen Sie in der Dropdownliste **Zweiter Steckplatz**5 aus.
   c) Klicken Sie auf **Erstellen**.
      Hinweis: In Management Service beginnt die Steckplatznummer mit Null. Daher unterscheidet sich die Steckplatznummerierung im Management Service von der Steckplatznummerierung auf der physischen Appliance.

Das logische Laufwerk wird erstellt und auf der
Registerkarte Logisches Laufwerkaufgeführt. Klicken Sie auf das Aktualisierungssymbol, um die Reihenfolge der logischen Laufwerke zu aktualisieren.

Hinzufügen eines zweiten logischen Laufwerks auf der SDX 22000-Appliance Um ein weiteres logisches Laufwerk hinzuzufügen, legen Sie die SSDs in die Steckplätze 6 und 7 ein. Wählen Sie auf

der Seite
Logisches Laufwerk erstellenin der Liste **Erster Steckplatz** 6 aus und wählen Sie 7 aus der Liste **Zweiter Steckplatz** aus.

Ersetzen Sie ein defektes SSD-Laufwerk mit einem leeren SSD-Laufwerk Ersetzen eines defekten SSD-Laufwerks durch ein leeres SSD-Laufwerk:

1. Navigieren Sie zu **Konfiguration > System > RAID**.
2. Wählen Sie auf der Registerkarte **Physikalische Laufwerke** das defekte Laufwerk aus, das Sie ersetzen möchten.
3. Klicken Sie auf **Zum Entfernen vorbereiten**, um das Laufwerk zu entfernen.
4. Klicken Sie auf das Aktualisierungssymbol, um die Liste der physischen Laufwerke zu aktualisieren.
5. Nehmen Sie das defekte Laufwerk physisch aus dem Steckplatz.
6. Stecken Sie die neue Citrix verifizierte SSD in den Steckplatz, aus dem Sie die defekte SSD entfernt
7. Navigieren Sie im Management Service zu **Konfiguration > System > RAID**. Die neue SSD ist im Abschnitt**Physikalische Laufwerke** aufgeführt. Der Neuaufbau des Laufwerks wird automatisch gestartet.

Klicken Sie auf das Aktualisierungssymbol, um den Status des Neuaufbaus zu überprüfen. Wenn der Neuaufbau abgeschlossen ist, können Sie den Status Online, Spun Up in der Spalte **Firmware-Status** sehen.

SDX Lizenzierung —Überblick

February 15, 2024

Im NetScaler SDX Management Service können Sie Ihre Hardware-Seriennummer (HSN) oder Ihren Lizenzzugriffscode verwenden, um Ihre Lizenzen zuzuweisen. Die Management Service-Software ruft intern die Seriennummer Ihrer Appliance ab, und Citrix sendet den Lizenzzugangscode beim Kauf einer Lizenz per E-Mail.

Wenn auf Ihrem lokalen Computer bereits eine Lizenz vorhanden ist, können Sie sie alternativ auf die Appliance hochladen.

Für alle anderen Funktionen, wie die Rückgabe oder Neuzuweisung Ihrer Lizenz, müssen Sie das Lizenzportal verwenden. Optional können Sie weiterhin das Lizenzportal für die Lizenzzuweisung verwenden. Weitere Informationen finden Sie unter Verwalten von Lizenzen auf citrix.com.

Informationen zu SDX-Lizenzierungsoptionen finden Sie unter:

- Auswahl der richtigen Plattform und Editionsoptionen.
- Lizenzierung von Modellen

Hinweis: Für die Installation einer unbefristeten oder gepoolten Lizenz ist kein Neustart der SDX-Appliance erforderlich.

Voraussetzungen

So verwenden Sie die Hardwareseriennummer oder den Lizenzzugriffscode, um Ihre Lizenzen zuzuweisen:

1. Sie müssen über die Appliance auf öffentliche Domains zugreifen können. Das Gerät muss beispielsweise auf www.citrix.comzugreifen können. Die Lizenzzuweisungssoftware greift intern auf das Citrix Lizenzierungsportal für Ihre Lizenz zu. Um auf eine Public Domain zuzugreifen, müssen Sie die IP-Adresse des Management Service konfigurieren und einen DNS-Server einrichten.
2. Ihre Lizenz muss mit Ihrer Hardware verknüpft sein, oder Sie müssen über einen gültigen Lizenzzugangscode verfügen.

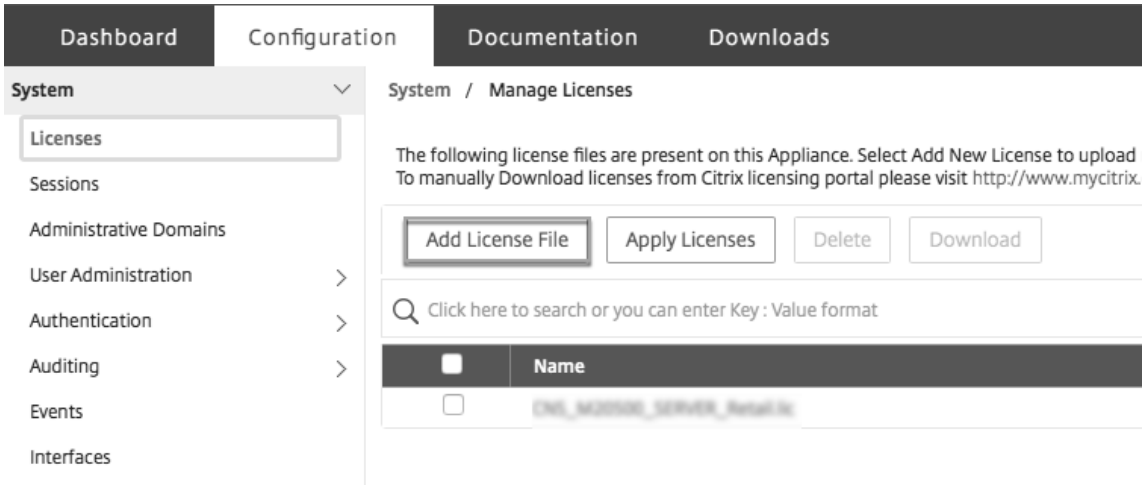
Zuweisen Ihrer Lizenz mit dem Management Service

Wenn Ihre Lizenz bereits mit Ihrer Hardware verknüpft ist, kann der Lizenzzuweisungsprozess die Hardware-Seriennummer verwenden. Andernfalls müssen Sie den Lizenzzugangscode eingeben.

Sie können nach Bedarf für Ihre Bereitstellung teilweise Lizenzen zuweisen. Wenn Ihre Lizenzdatei beispielsweise 10 Lizenzen enthält, Ihre aktuelle Anforderung jedoch nur sechs Lizenzen umfasst, können Sie jetzt sechs Lizenzen zuweisen und später weitere Lizenzen zuweisen. Sie können nicht mehr als die Gesamtzahl der in Ihrer Lizenzdatei enthaltenen Lizenzen zuweisen.

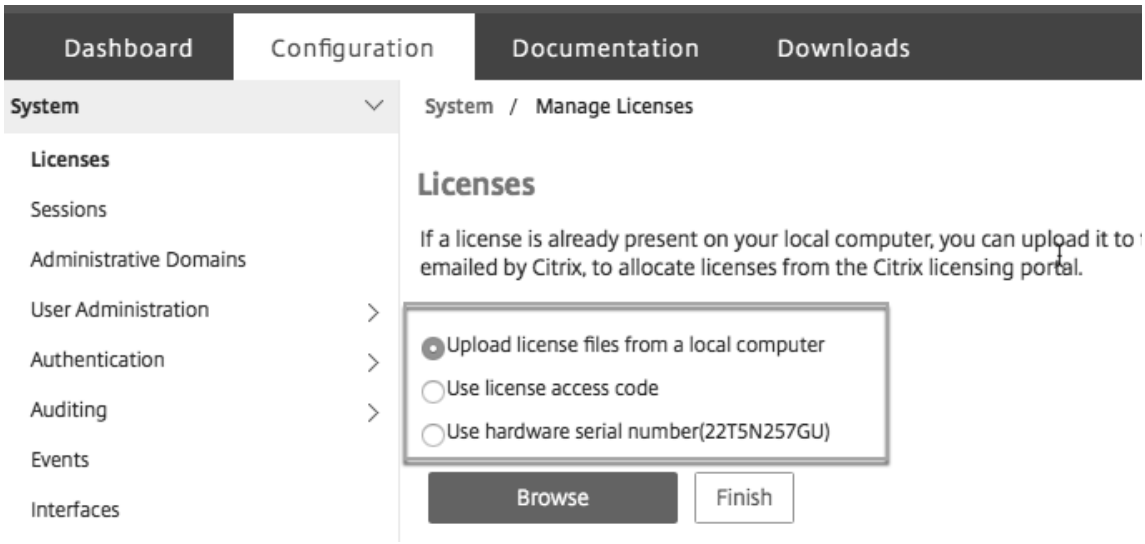
So weisen Sie Ihre Lizenz zu

1. Geben Sie in einem Webbrowser die IP-Adresse des Management Service der SDX-Appliance ein (z. B. http://10.102.126.251).
2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte **Configuration** zu **System > Licenses**.
4. Klicken Sie im Detailbereich auf **Lizenzdatei hinzufügen**.



5. Wählen Sie als Nächstes eine der Optionen aus:

   - Laden Sie Lizenzdateien von einem lokalen Computer hoch (diese Option ist standardmäßig ausgewählt)
   - Mit Lizenzzugangscode
   - Hardware-Seriennummer verwenden



- **Laden Sie Lizenzdateien von einem lokalen Computer**hoch: Wenn Sie diese Option wählen, klicken Sie auf **Durchsuchen**, um die Lizenz ohne Kapazität von Ihrem lokalen Computer auszuwählen. Klicken Sie dann auf **Finish**.

  1. Nachdem die Lizenz ohne Kapazität erfolgreich angewendet wurde, wird der Abschnitt **Lizenzmodus** auf der Seite **Lizenzen** angezeigt.
  2. Sie können entweder **Pool-Lizenzen** oder **Self Managed Pool-Lizenzen**wählen.
  3. Geben Sie im Feld **Lizenzservername oder IP-Adresse** die Details des Lizenzservers ein.
  4. Geben Sie im Feld **Portnummer** den Lizenzserverport ein. Standardwert: 27000.

5. Klicken Sie auf **Get Licenses**.
6. Geben Sie im Fenster **Lizenzen zuweisen** die erforderlichen Instanzen und die Bandbreite an und klicken Sie auf **Allocate**.
7. 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:**
>
> Ab NetScaler Version 13.1 Build 30.x unterstützt die NetScaler SDX-Appliance die Self Managed Pool-Lizenz. Mit dieser Lizenz können Sie das Hochladen von Lizenzdateien auf den Lizenzserver vereinfachen und automatisieren. Sie können NetScaler ADM verwenden, um ein Lizenzierungsframework zu erstellen, das eine gemeinsame Bandbreite oder vCPU und einen Instanzpool umfasst.

- **Lizenzzugangscode verwenden**: Wenn Sie diese Option auswählen, geben Sie entweder den **LAC** im Feld **Lizenzzugangscode** an oder aktivieren Sie das Kontrollkästchen, um eine Verbindung über einen Proxy-Server herzustellen. Klicken Sie anschließend auf **Lizenzen abrufen**.

  - Wählen Sie die Lizenzdatei aus, mithilfe derer Sie Lizenzen zuteilen möchten.
  - Geben Sie in der Spalte **Zuweisen** die Anzahl der zuzuordnenden Lizenzen ein. Klicken Sie anschließend auf **Herunterladen**.

  Wenn die Lizenz heruntergeladen wurde, wird sie unter **Lizenzdateien**angezeigt. Wählen Sie die Lizenzdatei aus und klicken Sie auf**Lizenzen anwenden**.

- **Hardware-Seriennummer verwenden**: Wenn Sie diese Option wählen, ruft die Software intern die Seriennummer Ihres Geräts ab und verwendet diese Nummer, um Ihre Lizenzen anzuzeigen.

  - Klicken Sie auf **Lizenzen abrufen**, oder aktivieren Sie das Kontrollkästchen **Verbindung über Proxy-Server** herstellen, und klicken Sie dann auf **Lizenzen abrufen**.

  Nachdem Sie die Lizenzdatei heruntergeladen haben, wählen Sie die Lizenzdatei aus und klicken Sie auf **Lizenzen anwenden**.

Informationen zur gepoolten Lizenzierung finden Sie unter Aktualisieren einer unbefristeten Lizenz in einem NetScaler SDX auf NetScaler-Poolkapazität.

SDX-Ressourcen-Visualizer

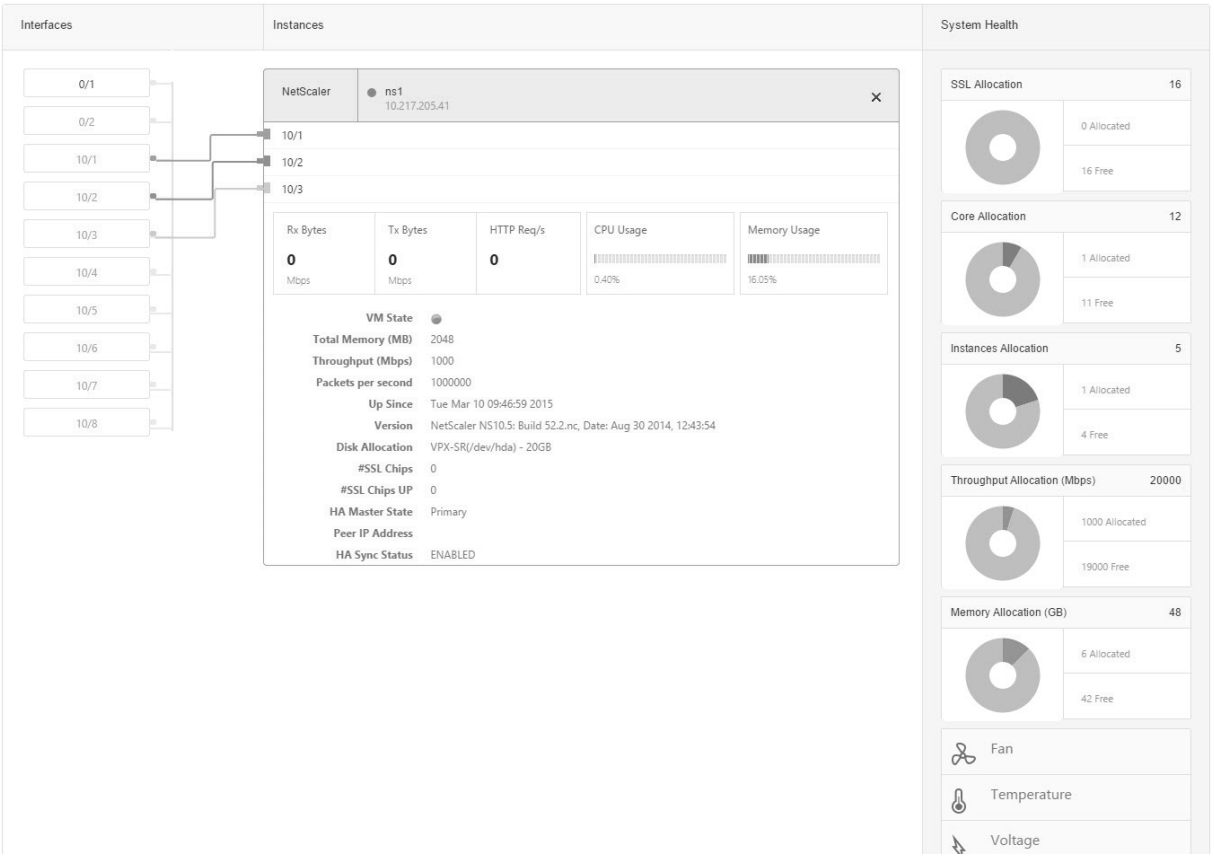
February 15, 2024

Wenn eine NetScaler-Instanz auf einer NetScaler SDX-Appliance bereitgestellt wird, müssen einer Instanz verschiedene Ressourcen wie CPU, Durchsatz und Arbeitsspeicher zugewiesen werden. Mit dem aktuellen SDX werden die Informationen zu verschiedenen verfügbaren Ressourcen nicht angezeigt.

Mit dem Ressourcen-Visualizer werden alle verfügbaren Ressourcen, die zur Bereitstellung einer Instanz verwendet werden können, in einem einzigen Dashboard angezeigt. Alle verfügbaren und verwendeten Ressourcen werden in einem grafischen Format angezeigt. Der Resource Visualizer zeigt neben den Ressourcen, die zugewiesen werden können, auch andere Parameter wie den Status der Stromversorgung und die Temperatur an.

Der Ressourcen-Visualizer zeigt auch die verschiedenen Ressourcen an, die eine Instanz verwendet. Um die verschiedenen Ressourcen anzuzeigen, die mit einer Instanz verknüpft sind, klicken Sie im Visualizer auf den Instanznamen. Auf der rechten Seite des Visualizers werden alle verfügbaren und verwendeten Ressourcen in einem grafischen Format angezeigt.

Die folgende Abbildung zeigt die im Ressourcen-Visualizer erfassten Details:



Schnittstellen verwalten

November 23, 2023

Im Bereich **Schnittstellen** können Sie die Zuordnung der virtuellen Schnittstellen in den VPX-Instanzen zur SDX-Appliance anzeigen und den Schnittstellen MAC-Adressen zuweisen.

Hinweis: Autonegotiation wird auf einer Schnittstelle nicht unterstützt, an die ein Direct Attach-Kabel (DAC) angeschlossen ist.

In der Liste der Schnittstellen im Bereich **Schnittstellen** in der Spalte **Status** zeigt UP an, dass die Schnittstelle normal Datenverkehr empfängt. DOWN zeigt ein Netzwerkproblem an, aufgrund dessen die Schnittstelle keinen Datenverkehr senden oder empfangen kann.

Wichtig: Die Flusskontrolle wird von Verbindungen über 1 GB nicht empfohlen.

Konfigurieren einer Schnittstelle

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **System**, und klicken Sie dann auf **Schnittstellen**.
2. Klicken Sie im Bereich **Schnittstellen** auf die Schnittstelle, die Sie konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**.
3. Geben **Sie im Fenster Interface konfigurieren** Werte für die folgenden Parameter an:
    - **Auto Negotiation**—Aktiviert automatische Absprache. Mögliche Werte: ON, OFF. Standardeinstellung: ON.
    - **Geschwindigkeit**—Ethernet-Geschwindigkeit für die Schnittstelle in MB/s. Mögliche Werte: 10, 100, 1000 und 10000.
    - **Duplex** — Art des Duplexbetriebs der Schnittstelle. Mögliche Werte: Full, Half, NONE. Standard: NONE.
    - **Automatische Absprache der Flusssteuerung**—Verhandeln Sie automatisch Flusskontrollparameter. Mögliche Werte: ON, OFF. Standard: ON
    - **Rx Flow Control**—Rx-Flusskontrolle aktivieren. Mögliche Werte: ON, OFF. Standard: ON
    - **Tx Flow Control**—Tx-Flusskontrolle aktivieren. Mögliche Werte: ON, OFF. Standard: ON
4. Klicken Sie auf **OK** und dann auf **Schließen**.

So setzen Sie die Parameter einer Schnittstelle auf ihre Standardwerte zurück

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **System**, und klicken Sie dann auf **Schnittstellen**.

2. Klicken Sie im Bereich **Schnittstellen** auf die Schnittstelle, die Sie zurücksetzen möchten, und klicken Sie dann auf **Zurücksetzen**.

Zeigen Sie die Zuordnung der virtuellen Schnittstellen auf der VPX-Instanz zu den physischen Schnittstellen an

In der NetScaler VPX-Instanz zeigen die GUI und die CLI die Zuordnung der virtuellen Schnittstellen auf der Instanz zu den physischen Schnittstellen auf der Appliance an.

Nachdem Sie sich bei der VPX-Instanz angemeldet haben, navigieren Sie im Konfigurationsprogramm zu **Netzwerk**, und klicken Sie dann auf **Schnittstellen.** Die virtuelle Schnittstellennummer auf der Instanz und die entsprechende physische Schnittstellennummer auf der Appliance werden im Feld **Beschreibung** angezeigt, wie in der folgenden Abbildung dargestellt:

Geben Sie in der CLI den Befehl `show interface` ein. Beispiel:

```
> show interface
1) Interface 10/3 (10G VF Interface, PF 10/4) #2
flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
MTU=1500, native vlan=1, MAC=6e:b6:f5:21:5d:db, uptime 43h03m35s
Actual: media FIBER, speed 10000, duplex FULL, fctl NONE, throughput
    10000
RX: Pkts(2547925) Bytes(287996153) Errs(0) Drops(527183) Stalls(0)
TX: Pkts(196) Bytes(8532) Errs(0) Drops(0) Stalls(0)
NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
Bandwidth thresholds are not set.
...
<!--NeedCopy-->
```

Zuweisen einer MAC-Adresse zu einer Schnittstelle

Während Sie eine ADC-Instanz auf einer SDX-Appliance bereitstellen, weist der Citrix Hypervisor intern einer virtuellen Schnittstelle, die dieser Instanz zugeordnet ist, eine MAC-Adresse zu. Dieselbe MAC-Adresse kann einer virtuellen Schnittstelle zugewiesen werden, die mit einer anderen Instanz auf derselben Appliance oder auf einer anderen Appliance verknüpft ist. Um die Zuweisung doppelter MAC-Adressen zu verhindern, können Sie eindeutige MAC-Adressen erzwingen.

Es gibt zwei Möglichkeiten, einer Schnittstelle eine MAC-Adresse zuzuweisen:

1. Weisen Sie einer Schnittstelle eine Basis-MAC-Adresse und einen Bereich zu: Der Management Service weist mithilfe der Basisadresse und des Bereichs eine eindeutige MAC-Adresse zu.
2. Weisen Sie eine globale Basis-MAC-Adresse zu: Eine globale Basis-MAC-Adresse gilt für alle Schnittstellen. Der Management Service generiert dann die MAC-Adressen für alle Schnittstellen. Wenn Sie die globale Basis-MAC-Adresse festlegen, wird der Bereich für eine 1G-Schnittstelle auf 8 festgelegt. Der Bereich für eine 10G-Schnittstelle ist auf 64 eingestellt.

In der folgenden Tabelle finden Sie Beispiele für Basis-MAC-Adressen, wenn die globale Basis-MAC-Adresse auf 00:00:00:00:00:00 festgelegt ist.

Physische Schnittstelle	Basis-MAC-Adresse
0/1	00:00:00:00:00:00
0/2	00:00:00:00:00:08
1/1	00:00:00:00:00:10
1/2	00:00:00:00:00:18
1/3	00:00:00:00:00:20
1/4	00:00:00:00:00:28
1/5	00:00:00:00:00:30
1/6	00:00:00:00:00:38
1/7	00:00:00:00:00:40
1/8	00:00:00:00:00:48
10/1	00:00:00:00:00:50
10/2	00:00:00:00:00:90

Tabelle 1. Beispiel für aus einer globalen Basis-MAC-Adresse generierte Basis-MAC-Adressen

Die Basis-MAC-Adresse für die Management-Ports dient nur als Referenz. Der Management Service generiert MAC-Adressen, basierend auf der Basis-MAC-Adresse, nur für 1/x- und 10/x-Ports.

Hinweis: Sie können einem Kanal keine Basis-MAC-Adresse zuweisen.

Um die verschiedenen Vorgänge mit der MAC-Adresse durchzuführen, klicken Sie auf **System > Schnittstellen**. Wählen Sie eine Schnittstelle aus und klicken Sie dann auf **Bearbeiten**. Führen Sie den MAC-Adressvorgang im Fenster **Schnittstelle konfigurieren** aus.

Deaktivieren oder aktivieren Sie die physischen Schnittstellen auf der SDX-Appliance

Wenn Sie keine der physischen Schnittstellen auf der SDX-Appliance verwenden, können Sie die physische Schnittstelle mithilfe des Management Service deaktivieren. Diese Aktion ist aus Sicherheitsgründen hilfreich.

Hinweis: Standardmäßig sind alle physischen Schnittstellen auf der SDX-Appliance aktiviert. Wenn eine Schnittstelle von einem VPX oder Kanal verwendet wird, können Sie die Schnittstelle nicht deaktivieren.

Um die physische Schnittstelle zu deaktivieren:

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **System**, und klicken Sie dann auf **Schnittstellen**.
2. Wählen Sie im Bereich **Schnittstellen** die Schnittstelle aus, die Sie deaktivieren möchten.
3. Klicken Sie in der Dropdownliste **Aktion** auf **Deaktivieren**.

Wenn Sie die deaktivierte physische Schnittstelle verwenden möchten, können Sie die Schnittstelle mit dem Management Service aktivieren.

Um die deaktivierte physische Schnittstelle zu aktivieren:

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **System**, und klicken Sie dann auf **Schnittstellen**.
2. Wählen Sie im Bereich **Interfaces** die Deaktivierungsschnittstelle aus, die Sie aktivieren möchten.
3. Klicken Sie in der Dropdownliste **Aktion** auf **Aktivieren**.

Jumbo Frames auf SDX-Appliances

November 23, 2023

NetScaler SDX-Appliances unterstützen das Empfangen und Senden von Jumbo-Frames mit bis zu 9216 Byte an IP-Daten. Jumbo-Frames können große Dateien effizienter übertragen als dies mit der standardmäßigen IP-MTU-Größe von 1500 Byte möglich ist.

Eine NetScaler SDX-Appliance kann Jumbo-Frames in den folgenden Bereitstellungsszenarien verwenden:

- **Jumbo zu Jumbo**: Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als Jumbo-Frames.
- **Non-Jumbo zu Jumbo**: Die Appliance empfängt Daten als Nicht-Jumbo-Frames und sendet sie als Jumbo-Frames.
- **Jumbo zu Non-Jumbo**: Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als Nicht-Jumbo-Frames.

Die auf der SDX-Appliance bereitgestellten NetScaler-Instanzen unterstützen Jumbo-Frames in einer Load-Balancing-Konfiguration für die folgenden Protokolle:

- TCP
- Jedes andere Protokoll über TCP
- SIP

Weitere Informationen zu Jumbo-Frames finden Sie in den Anwendungsfällen.

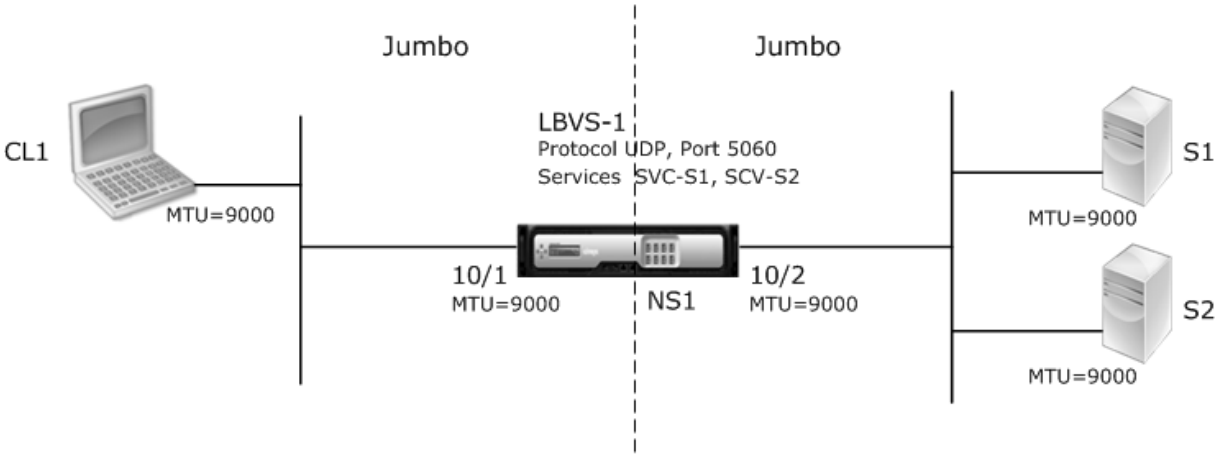
Anwendungsfall: Jumbo zum Jumbo-Setup

Stellen Sie sich ein Beispiel für ein Jumbo-zu-Jumbo-Setup vor, bei dem der virtuelle SIP-Lastenausgleichsserver LBVS-1, der auf der NetScaler-Instanz NS1 konfiguriert ist, verwendet wird, um den SIP-Verkehr zwischen den Servern S1 und S2 auszugleichen. Die Verbindung zwischen Client CL1 und NS1 und die Verbindung zwischen NS1 und den Servern unterstützen Jumbo-Frames.

Die Schnittstelle 10/1 von NS1 empfängt oder sendet Datenverkehr vom oder zum Client CL1. Die Schnittstelle 10/2 von NS1 empfängt oder sendet Datenverkehr vom oder zum Server S1 oder S2. Die Schnittstellen 10/1 und 10/2 von NS1 sind Teil von VLAN 10 bzw. VLAN 20.

Für die Unterstützung von Jumbo-Frames ist die MTU für die Schnittstellen 10/1, 10/2 und VLANs VLAN 10, VLAN 20 auf 9216 eingestellt.

Alle anderen Netzwerkgeräte, einschließlich CL1, S1, S2, sind in diesem Setup-Beispiel ebenfalls für die Unterstützung von Jumbo-Frames konfiguriert.



In der folgenden Tabelle sind die im Beispiel verwendeten Einstellungen aufgeführt.

Entität	Name	Details
Die IP-Adresse des Clients CL1	CL1	192.0.2.10
Die IP-Adresse der Server	S1	198.51.100.19
		S2
Für Schnittstellen (mithilfe der Management Service-Schnittstelle) und VLANs auf NS1 (mithilfe der CLI) angegebene MTU.	10/1	9000
		10/2

Entität	Name	Details
		VLAN 10 VLAN 20
Dienste auf NS1, die Server darstellen	SVC-S1	IP-Adresse: 198.51.100.19; Protokoll: SIP; Port: 5060
Dienste auf NS1, die Server darstellen	SVC-S2	IP-Adresse: 198.51.100.20; Protokoll: SIP; Port: 5060
Virtueller Lastausgleichsserver auf VLAN 10	LBVS-1	IP-Adresse: 203.0.113.15; Protokoll: SIP; Anschluss: 5060; SVC-S1, SVC-S2

Im Folgenden ist der Verkehrsfluss der Anfrage von CL1 an NS1:

1. CL1 erstellt eine 20000-Byte-SIP-Anforderung für LBVS1.
2. CL1 sendet die Anforderungsdaten in IP-Fragmenten an LBVS1 von NS1. Die Größe jedes IP-Fragments ist entweder gleich oder kleiner als die MTU (9000), die auf der Schnittstelle festgelegt ist, von der CL1 diese Fragmente an NS1 sendet.
    - Größe des ersten IP-Fragments = [IP-Header + UDP-Header + SIP-Datensegment] = [20 + 8 + 8972] = 9000
    - Größe des zweiten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 8980] = 9000
    - Größe des letzten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 2048] = 2068
3. NS1 empfängt die IP-Fragmente der Anforderung an Schnittstelle 10/1. NS1 akzeptiert diese Fragmente, da die Größe jedes dieser Fragmente gleich oder kleiner als die MTU (9000) der Schnittstelle 10/1 ist.
4. NS1 setzt diese IP-Fragmente wieder zusammen, um die 27000-Byte-SIP-Anforderung zu bilden. NS1 verarbeitet diese Anfrage.
5. Der Load-Balancing-Algorithmus von LBVS-1 wählt Server S1 aus.
6. NS1 sendet die Anforderungsdaten in IP-Fragmenten an S1. Die Größe jedes IP-Fragments ist entweder gleich oder kleiner als die MTU (9000) der Schnittstelle 10/2, von der NS1 diese Fragmente an S1 sendet. Die IP-Pakete werden mit einer SNIP-Adresse von NS1 bezogen.
    - Größe des ersten IP-Fragments = [IP-Header + UDP-Header + SIP-Datensegment] = [20 + 8 + 8972] = 9000
    - Größe des zweiten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 8980] = 9000
    - Größe des letzten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 2048] = 2068

Es folgt der Verkehrsfluss der Antwort von S1 auf CL1 in diesem Beispiel:

1. Server S1 erstellt eine 30000-Byte-SIP-Antwort zum Senden an die SNIP-Adresse von NS1.

2. S1 sendet die Antwortdaten in IP-Fragmenten an NS1. Die Größe jedes IP-Fragments ist entweder gleich oder kleiner als die MTU (9000), die auf der Schnittstelle festgelegt ist, von der S1 diese Fragmente an NS1 sendet.
    - Größe des ersten IP-Fragments = [IP-Header + UDP-Header + SIP-Datensegment] = [20 + 8 + 8972] = 9000
    - Größe des zweiten und dritten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 8980] = 9000
    - Größe des letzten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 3068] = 3088
3. NS1 empfängt die Antwort-IP-Fragmente an Schnittstelle 10/2. NS1 akzeptiert diese Fragmente, da die Größe jedes Fragments gleich oder kleiner als die MTU (9000) der Schnittstelle 10/2 ist.
4. NS1 setzt diese IP-Fragmente wieder zusammen, um die 27000-Byte-SIP-Antwort zu bilden. NS1 verarbeitet diese Antwort.
5. NS1 sendet die Antwortdaten in IP-Fragmenten an CL1. Die Größe jedes IP-Fragments ist entweder gleich oder kleiner als die MTU (9000) der Schnittstelle 10/1, von der NS1 diese Fragmente an CL1 sendet. Die IP-Fragmente werden mit der IP-Adresse von LBVS-1 beschafft. Diese IP-Pakete werden von der IP-Adresse von LBVS-1 bezogen und an die IP-Adresse von CL1 bestimmt.
    - Größe des ersten IP-Fragments = [IP-Header + UDP-Header + SIP-Datensegment] = [20 + 8 + 8972] = 9000
    - Größe des zweiten und dritten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 8980] = 9000

Größe des letzten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 3068] = 3088

Aufgaben der Konfiguration:

Navigieren Sie im SDX Management Service zur Seite **Konfiguration > System > Schnittstellen** . Wählen Sie die gewünschte Schnittstelle aus und klicken Sie auf **Bearbeiten**. Setzen Sie den MTU-Wert und klicken Sie auf **OK**.

Beispiel:

Stellen Sie den MTU-Wert für das Interface 10/1 auf 9000 und für das Interface 10/2 auf 9000 ein.

Melden Sie sich bei der NetScaler-Instanz an und verwenden Sie die ADC-Befehlszeilenschnittstelle, um die verbleibenden Konfigurationsschritte abzuschließen.

In der folgenden Tabelle sind die Aufgaben, Befehle und Beispiele für die Erstellung der erforderlichen Konfiguration auf den NetScaler-Instanzen aufgeführt.

Aufgaben	ADC-Befehlssyntax	Beispiele
Erstellen Sie VLANs und legen Sie die MTU der gewünschten VLANs für die Unterstützung von Jumbo-Frames fest.	`add vlan <id> -mtu <positive_integer>;show vlan <id>`	`add vlan 10 -mtu 9000; add vlan 20 -mtu 9000`
Binden Sie Schnittstellen an VLANs.	`bind vlan <id> -ifnum <interface_name>; show vlan <id>`	`bind vlan 10 -ifnum 10/1; bind vlan 20 -ifnum 10/2`
Fügen Sie eine SNIP-Adresse hinzu.	`add ns ip <IPAddress> <netmask> -type SNIP; show ns ip`	`add ns ip 198.51.100.18 255.255.255.0 -type SNIP`
Erstellen Sie Dienste, die SIP-Server darstellen	`add service <serviceName> <ip> SIP_UDP <port>; show service <name>`	Dienst hinzufügen SVC-S1 198.51.100.19 SIP_UDP 5060; Dienst SVC-S2 198.51.100.20 SIP_UDP 5060 hinzufügen
Erstellen Sie virtuelle SIP-Lastausgleichsserver und binden Sie die Dienste daran	`add lb vserver <name> SIP_UDP <ip> <port> ;bind lb vserver <vserverName> <serviceName>; show lb vserver <name>`	`add lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060;bind lb vserver LBVS-1 SVC-S1;bind lb vserver LBVS-1 SVC-S2`
`bind lb vserver LBVS -1 SVC-S2`	`save ns config; show ns config`	

Anwendungsfall: Nicht-Jumbo-zu-Jumbo-Setup

Stellen Sie sich ein Beispiel für ein Setup ohne Jumbo zu Jumbo vor, bei dem der virtuelle Lastausgleichsserver LBVS1, der auf einer NetScaler-Instanz NS1 konfiguriert ist, für den Lastenausgleich des Datenverkehrs zwischen den Servern S1 und S2 verwendet wird. Die Verbindung zwischen Client CL1 und NS1 unterstützt Nicht-Jumbo-Frames, und die Verbindung zwischen NS1 und den Servern unterstützt Jumbo-Frames.

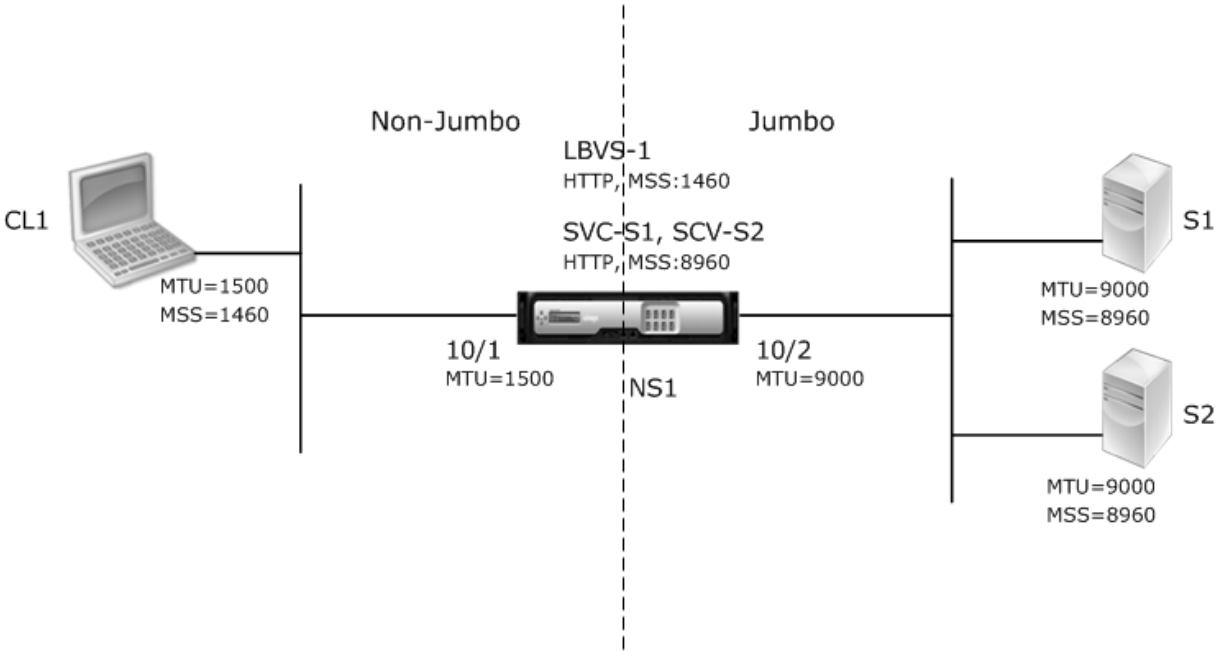
Die Schnittstelle 10/1 von NS1 empfängt oder sendet Datenverkehr vom oder zum Client CL1. Die Schnittstelle 10/2 von NS1 empfängt oder sendet Datenverkehr vom oder zum Server S1 oder S2.

Die Schnittstellen 10/1 und 10/2 von NS1 sind Teil von VLAN 10 bzw. VLAN 20. Um nur Nicht-Jumbo-Frames zwischen CL1 und NS1 zu unterstützen, ist die MTU sowohl für die Schnittstelle 10/1 als auch für VLAN 10 auf den Standardwert 1500 festgelegt.

Für die Unterstützung von Jumbo-Frames zwischen NS1 und den Servern ist die MTU für die Schnittstelle 10/2 und VLAN 20 auf 9000 eingestellt.

Server und alle anderen Netzwerkgeräte zwischen NS1 und den Servern sind ebenfalls für die Unterstützung von Jumbo-Frames konfiguriert. Da der HTTP-Verkehr auf TCP basiert, werden MSSs an jedem Endpunkt entsprechend für die Unterstützung von Jumbo-Frames festgelegt:

- Für die Verbindung zwischen CL1 und dem virtuellen Server LBVS1 von NS1 wird die MSS auf NS1 in einem TCP-Profil festgelegt, das dann an LBVS1 gebunden wird.
- Für die Verbindung zwischen einer SNIP-Adresse von NS1 und S1 wird die MSS auf NS1 in einem TCP-Profil festgelegt, das dann an den Dienst (SVC-S1) gebunden ist, der S1 auf NS1 darstellt.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt:

Entität	Name	Details
Die IP-Adresse des Clients CL1	CL1	192.0.2.10
Die IP-Adresse der Server	S1	198.51.100.19
		S2
MTU für die Schnittstelle 10/1 (mithilfe der Management Service-Schnittstelle).		1500

Entität	Name	Details
Die MTU wurde für die Schnittstelle 10/2 festgelegt (mithilfe der Management Service-Schnittstelle).		9000
MTU für VLAN 10 auf NS1 (mithilfe der ADC-Befehlszeilenschnittstelle).		1500
Die MTU wurde für VLAN 20 auf NS1 festgelegt (mithilfe der ADC-Befehlszeilenschnittstelle).		9000
Dienste auf NS1, die Server darstellen	SVC-S1	IP-Adresse: 198.51.100.19; Protokoll: HTTP; Port: 80; MSS: 8960 SVC-S2
Virtueller Lastausgleichsserver auf VLAN 10	LBVS-1	IP-Adresse: 203.0.113.15; Protokoll: HTTP; Port: 80. Gebundene Dienste: SVC-S1, SVC-S2; MSS: 1460

Es folgt der Verkehrsfluss von CL1s Anfrage an S1 in diesem Beispiel:

1. Der Client CL1 erstellt eine 200-Byte-HTTP-Anforderung zum Senden an den virtuellen Server LBVS-1 von NS1.
2. CL1 öffnet eine Verbindung zu LBVS-1 von NS1. CL1 und NS1 tauschen beim Verbindungsaufbau ihre jeweiligen TCP-MSS-Werte aus.
3. Da der MSS von NS1 größer ist als die HTTP-Anforderung, sendet CL1 die Anforderungsdaten in einem einzigen IP-Paket an NS1.
   1.

```
<div id="concept_57AEA1C9D3DA47948B6D834341388D29__d978e142">

Size of the request packet = [IP Header + TCP Header + TCP Request
    ] = [20 + 20 + 200] = 240

</div>
```

4. NS1 empfängt das Anforderungspaket an der Schnittstelle 10/1 und verarbeitet dann die HTTP-Anforderungsdaten im Paket.
5. Der Load Balancing-Algorithmus von LBVS-1 wählt Server S1 aus, und NS1 öffnet eine Verbindung zwischen einer seiner SNIP-Adressen und S1. NS1 und CL1 tauschen beim Verbindungsaufbau ihre jeweiligen TCP-MSS-Werte aus.
6. Da der MSS von S1 größer ist als die HTTP-Anforderung, sendet NS1 die Anforderungsdaten in

einem einzigen IP-Paket an S1.

a) Größe des Anforderungspakets = [IP-Header + TCP-Header + [TCP-Anforderung] = [20 + 20 + 200] = 240

Es folgt der Verkehrsfluss der Antwort von S1 auf CL1 in diesem Beispiel:

1. Server S1 erstellt eine 18000-Byte-HTTP-Antwort, die an die SNIP-Adresse von NS1 gesendet wird.
2. S1 segmentiert die Antwortdaten in Vielfache des MSS von NS1 und sendet diese Segmente in IP-Paketen an NS1. Diese IP-Pakete werden von der IP-Adresse von S1 bezogen und an die SNIP-Adresse von NS1 bestimmt.
   - Größe der ersten beiden Pakete = [IP-Header + TCP-Header + (TCP-Segment = MSS-Größe von NS1)] = [20 + 20 + 8960] = 9000
   - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 2080] = 2120
3. NS1 empfängt die Antwortpakete an Schnittstelle 10/2.
4. Aus diesen IP-Paketen setzt NS1 alle TCP-Segmente zu den HTTP-Antwortdaten von 18000 Byte zusammen. NS1 verarbeitet diese Antwort.
5. NS1 segmentiert die Antwortdaten in Vielfache des MSS von CL1 und sendet diese Segmente in IP-Paketen von der Schnittstelle 10/1 an CL1. Diese IP-Pakete werden von der IP-Adresse von LBVS-1 bezogen und an die IP-Adresse von CL1 bestimmt.
   - Größe des gesamten Pakets außer dem letzten = [IP-Header + TCP-Header + (TCP-Nutzlast = CL1s MSS-Größe)] = [20 + 20 + 1460] = 1500
   - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 480] = 520

Aufgaben der Konfiguration:

Navigieren Sie im SDX Management Service zur Seite **Konfiguration > System > Schnittstellen** . Wählen Sie die gewünschte Schnittstelle aus und klicken Sie auf **Bearbeiten**. Setzen Sie den MTU-Wert und klicken Sie auf **OK**.

Beispiel:

Stellen Sie die folgenden MTU-Werte ein:

- Für 10/1-Schnittstelle wie 1500
- Für 10/2-Schnittstelle als 9000

Melden Sie sich bei der NetScaler-Instanz an und verwenden Sie die ADC-Befehlszeilenschnittstelle, um die verbleibenden Konfigurationsschritte abzuschließen.

In der folgenden Tabelle sind die Aufgaben, Befehle und Beispiele für die Erstellung der erforderlichen Konfiguration auf den NetScaler-Instanzen aufgeführt.

Aufgaben	ADC-Befehlszeilensyntax	Beispiel
—	—	—
Erstellen Sie VLANs und legen Sie die MTU der gewünschten VLANs für die Unterstützung von Jumbo-Frames fest.	`add vlan <id> -mtu <positive_integer>; show vlan <id>`	`add vlan 10 -mtu 1500; add vlan 20 -mtu 9000`
Binden Sie Schnittstellen an VLANs.	`bind vlan <id> -ifnum <interface_name>; show vlan <id>`	`bind vlan 10 -ifnum 10/1; bind vlan 20 -ifnum 10/2`
Fügen Sie eine SNIP-Adresse hinzu.	`add ns ip <IPAddress> <netmask> -type SNIP; show ns ip`	`add ns ip 198.51.100.18 255.255.255.0 -type SNIP`
Dienste erstellen, die HTTP-Server darstellen	`add service <serviceName> <ip> HTTP <port>; show service <name>`	`add service SVC-S1 198.51.100.19 http 80; add service SVC-S2 198.51.100.20 http 80`
Erstellen Sie virtuelle HTTP-Lastausgleichsserver und binden Sie die Dienste daran	`add lb vserver <name> HTTP <ip> <port>;bind lb vserver <vserverName> <serviceName>; show lb vserver <name>`	`add lb vserver LBVS-1 http 203.0.113.15 80; bind lb vserver LBVS-1 SVC-S1`
Erstellen Sie ein benutzerdefiniertes TCP-Profil und legen Sie dessen MSS für die Unterstützung von Jumbo-Frames fest	`add tcpProfile <name> -mss <positive_integer>; show tcpProfile <name>`	`add tcpprofile NS1-SERVERS-JUMBO -mss 8960`
Binden Sie das benutzerdefinierte TCP-Profil an die gewünschten Dienste.	`set service <Name > -tcpProfileName <string>; show service <name>`	`set service SVC-S1 -tcpProfileName NS1-SERVERS-JUMBO; set service SVC-S2 -tcpProfileName NS1-SERVERS-JUMBO`
Konfiguration speichern	`save ns config; show ns config`

Anwendungsfall: Koexistenz von Jumbo- und Nicht-Jumbo-Flows auf demselben Satz von Schnittstellen

Stellen Sie sich ein Beispiel vor, in dem die virtuellen Lastausgleichsserver LBVS1 und LBVS2 auf der NetScaler-Instanz NS1 konfiguriert sind. LBVS1 wird zum Lastenausgleich des HTTP-Datenverkehrs über die Server S1 und S2 verwendet, und global wird zum Lastenausgleich des Datenverkehrs zwischen den Servern S3 und S4 verwendet.

CL1 ist auf VLAN 10, S1 und S2 sind auf VLAN20, CL2 ist auf VLAN 30 und S3 und S4 sind auf VLAN 40. VLAN 10 und VLAN 20 unterstützen Jumbo-Frames, und VLAN 30 und VLAN 40 unterstützen nur Nicht-Jumbo-Frames.

Mit anderen Worten, die Verbindung zwischen CL1 und NS1 und die Verbindung zwischen NS1 und

Server S1 oder S2 unterstützen Jumbo-Frames. Die Verbindung zwischen CL2 und NS1 und die Verbindung zwischen NS1 und Server S3 oder S4 unterstützen nur Nicht-Jumbo-Frames.

Die Schnittstelle 10/1 von NS1 empfängt oder sendet Datenverkehr von oder zu Clients. Die Schnittstelle 10/2 von NS1 empfängt oder sendet Datenverkehr von oder zu den Servern.

Die Schnittstelle 10/1 ist sowohl an VLAN 10 als auch an VLAN 20 als getaggte Schnittstelle gebunden. Die Schnittstelle 10/2 ist sowohl an VLAN 30 als auch an VLAN 40 als getaggte Schnittstelle gebunden.

Für die Unterstützung von Jumbo-Frames ist die MTU für die Schnittstellen 10/1 und 10/2 auf 9216 eingestellt.

Auf NS1 ist die MTU für VLAN 10 auf 9000 und für die Unterstützung von Jumbo-Frames auf VLAN 30 eingestellt. Die MTU ist auf den Standardwert 1500 für VLAN 20 und VLAN 40 für die Unterstützung von Nicht-Jumbo-Frames festgelegt.

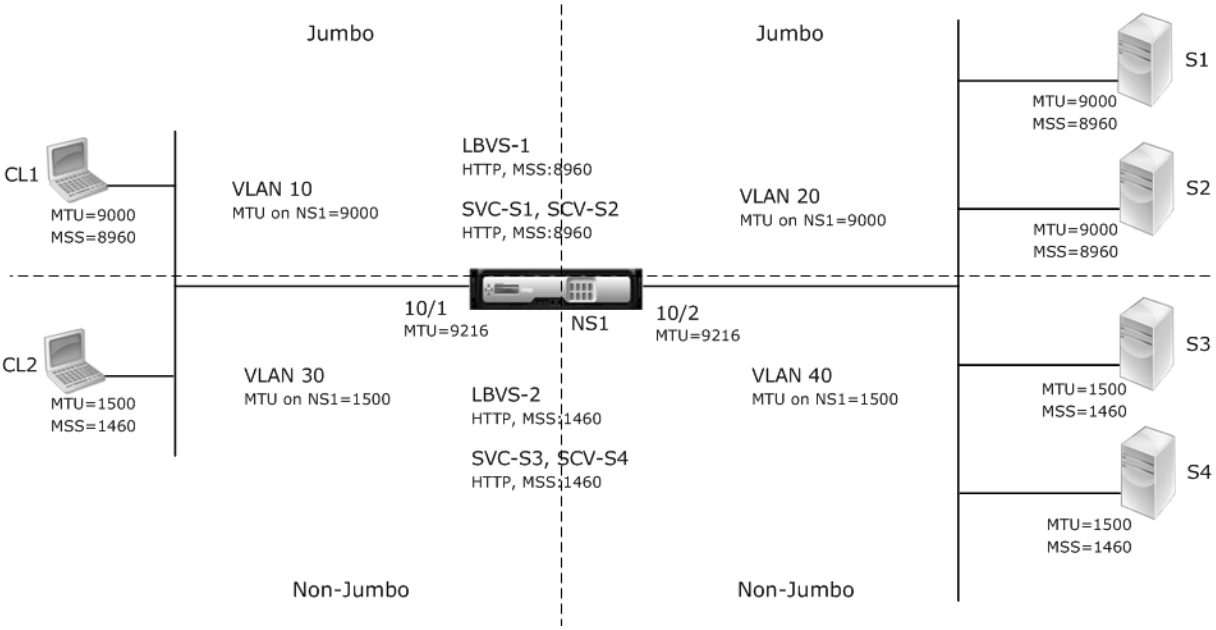
Die effektive MTU auf einer ADC-Schnittstelle für mit VLAN markierte Pakete entspricht der MTU der Schnittstelle oder der MTU des VLAN, je nachdem, welcher Wert niedriger ist. Beispiel:

- Die MTU der Schnittstelle 10/1 ist 9216. Die MTU von VLAN 10 ist 9000. Auf der Schnittstelle 10/1 beträgt die MTU der mit VLAN 10 markierten Paketen 9000.
- Die MTU der Schnittstelle 10/2 ist 9216. Die MTU von VLAN 20 ist 9000. Auf der Schnittstelle 10/2 beträgt die MTU der mit VLAN 20 markierten Paketen 9000.
- Die MTU der Schnittstelle 10/1 ist 9216. Die MTU von VLAN 30 beträgt 1500. Auf der Schnittstelle 10/1 beträgt die MTU der mit VLAN 30 markierten Paketen 1500.
- Die MTU der Schnittstelle 10/2 ist 9216. Die MTU von VLAN 40 beträgt 1500. Auf der Schnittstelle 10/2 beträgt die MTU der mit VLAN 40 markierten Paketen 9000.

CL1, S1, S2 und alle Netzwerkgeräte zwischen CL1 und S1 oder S2 sind für Jumbo-Frames konfiguriert.

Da der HTTP-Verkehr auf TCP basiert, werden MSSs an jedem Endpunkt entsprechend für die Unterstützung von Jumbo-Frames festgelegt.

- Für die Verbindung zwischen CL1 und dem virtuellen Server LBVS-1 von NS1 wird die MSS auf NS1 in einem TCP-Profil festgelegt, das dann an LBVS1 gebunden wird.
- Für die Verbindung zwischen einer SNIP-Adresse von NS1 und S1 wird die MSS auf NS1 in einem TCP-Profil festgelegt, das dann an den Dienst (SVC-S1) gebunden ist, der S1 auf NS1 darstellt.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

|Entität|Name|Details|
|—|—|—|
|Die IP-Adresse der Clients|CL1|192.0.2.10
||CL2|192.0.2.20
|Die IP-Adresse der Server|S1|198.51.100.19
||S2|198.51.100.20
||S3|198.51.101.19
||S4|198.51.101.20
|SNIP-Adressen auf NS1||198,51.100.18; 198,51.101.18
|MTU für Schnittstellen und VLANs auf NS1 spezifiziert|10/1|9216
||10/2|9216
|VLAN 10|9000
|VLAN 20|9000
|VLAN 30|9000
|VLAN 40|1500
|Default TCP profile|nstcp_default_profile|MSS: 1460
|Custom TCP profile|ALL-JUMBO|MSS: 8960
|Services on NS1 representing servers|SVC-S1|IP address: 198.51.100.19; Protocol: HTTP; Port: 80; TCP profile: ALL-JUMBO (MSS: 8960)
||SVC-S2|IP address: 198.51.100.20; Protocol: HTTP; Port: 80; TCP profile: ALL-JUMBO (MSS: 8960)
||SVC-S3|IP address: 198.51.101.19; Protocol: HTTP; Port: 80; TCP profile: nstcp_default_profile (MSS: 1460)
||SVC-S4|IP address: 198.51.101.20; Protocol: HTTP; Port: 80; TCP profile: nstcp_default_profile (MSS:

1460)
|Load balancing virtual servers on NS1|LBVS-1|IP address = 203.0.113.15; Protocol: HTTP; Port: 80. Bound services: SVC-S1, SVC-S2; TCP profile: ALL-JUMBO (MSS: 8960)
||LBVS-2|IP address = 203.0.114.15; Protocol: HTTP; Port: 80. Gebundene Dienste: SVC-S3, SVC-S4; TCP-Profil: nstcp_default_profile (MSS: 1460)

Es folgt der Verkehrsfluss der Anfrage von CL1 an S1:

1. Der Client CL1 erstellt eine 20000-Byte-HTTP-Anforderung zum Senden an den virtuellen Server LBVS-1 von NS1.
2. CL1 öffnet eine Verbindung zu LBVS-1 von NS1. CL1 und NS1 tauschen beim Verbindungsaufbau ihre TCP-MSS-Werte aus.
3. Da der MSS-Wert von NS1 kleiner ist als die HTTP-Anforderung, segmentiert CL1 die Anforderungsdaten in Vielfaches von NS1 MSS und sendet diese Segmente in IP-Paketen, die als VLAN 10 gekennzeichnet sind, an NS1.
    - Größe der ersten beiden Pakete = [IP-Header + TCP-Header + (TCP-Segment=NS1 MSS)] = [20 + 20 + 8960] = 9000
    - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 2080] = 2120
4. NS1 empfängt diese Pakete an Schnittstelle 10/1. NS1 akzeptiert diese Pakete, da die Größe dieser Pakete gleich oder kleiner ist als die effektive MTU (9000) der Schnittstelle 10/1 für mit VLAN 10 getaggte Pakete.
5. Aus den IP-Paketen stellt NS1 alle TCP-Segmente zur 20000-Byte-HTTP-Anforderung zusammen. NS1 verarbeitet diese Anfrage.
6. Der Load Balancing-Algorithmus von LBVS-1 wählt Server S1 aus, und NS1 öffnet eine Verbindung zwischen einer seiner SNIP-Adressen und S1. NS1 und CL1 tauschen beim Verbindungsaufbau ihre jeweiligen TCP-MSS-Werte aus.
7. NS1 segmentiert die Anforderungsdaten in Vielfaches des MSS von S1 und sendet diese Segmente in IP-Paketen, die als VLAN 20 an S1 gekennzeichnet sind.
    - Größe der ersten beiden Pakete = [IP-Header + TCP-Header + (TCP-Nutzlast = S1 MSS)] = [20 + 20 + 8960] = 9000
    - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 2080] = 2120

Es folgt der Verkehrsfluss der Antwort von S1 auf CL1:

1. Server S1 erstellt eine 30000-Byte-HTTP-Antwort, die an die SNIP-Adresse von NS1 gesendet wird.
2. S1 segmentiert die Antwortdaten in ein Vielfaches des MSS von NS1 und sendet diese Segmente in IP-Paketen, die als VLAN 20 an NS1 gekennzeichnet sind. Diese IP-Pakete werden von der IP-Adresse von S1 bezogen und an die SNIP-Adresse von NS1 bestimmt.

- Größe der ersten drei Pakete = [IP-Header + TCP-Header + (TCP-Segment = MSS-Größe von NS1)] = [20 + 20 + 8960] = 9000
- Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 3120] = 3160

3. NS1 empfängt die Antwortpakete an Schnittstelle 10/2. NS1 akzeptiert diese Pakete, da ihre Größe dem effektiven MTU-Wert (9000) der Schnittstelle 10/2 für mit VLAN 20 getaggte Pakete entspricht oder kleiner ist.
4. Aus diesen IP-Paketen stellt NS1 alle TCP-Segmente zur 30000-Byte-HTTP-Antwort zusammen. NS1 verarbeitet diese Antwort.
5. NS1 segmentiert die Antwortdaten in Vielfache des MSS von CL1 und sendet diese Segmente in IP-Paketen, die als VLAN 10 gekennzeichnet sind, von der Schnittstelle 10/1 an CL1. Diese IP-Pakete werden von der IP-Adresse von LBVS bezogen und zur IP-Adresse von CL1 bestimmt.

   - Größe der ersten drei Pakete = [IP-Header + TCP-Header + [(TCP-Nutzlast = MSS-Größe von CL1)] = [20 + 20 + 8960] = 9000
   - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 3120] = 3160

Aufgaben der Konfiguration:

Navigieren Sie im SDX Management Service zur Seite **Konfiguration > System > Schnittstellen** . Wählen Sie die gewünschte Schnittstelle aus und klicken Sie auf **Bearbeiten**. Setzen Sie den MTU-Wert und klicken Sie auf **OK**.

Beispiel:

Stellen Sie die folgenden MTU-Werte ein:

- Für 10/1-Schnittstelle wie 9216
- Für 10/2-Schnittstelle wie 9216

Melden Sie sich bei der NetScaler-Instanz an und verwenden Sie die ADC-Befehlszeilenschnittstelle, um die verbleibenden Konfigurationsschritte abzuschließen.

In der folgenden Tabelle sind die Aufgaben, Befehle und Beispiele für die Erstellung der erforderlichen Konfiguration auf den NetScaler-Instanzen aufgeführt.

Aufgabe	Syntax	Beispiel
—	—	—
Erstellen Sie VLANs und legen Sie die MTU der gewünschten VLANs für die Unterstützung von Jumbo-Frames fest.	`add vlan <id> -mtu <positive_integer>; show vlan <id>`	`add vlan 10 -mtu 9000add vlan 20 -mtu 9000;add vlan 30 -mtu 1500;add vlan 40 -mtu 1500`

Binden Sie Schnittstellen an VLANs.	bind vlan <id> -ifnum <interface_name>;show vlan <id>	bind vlan 10 -ifnum 10/1 -taggedbind vlan 20 -ifnum 10/2 -tagged;bind vlan 30 -ifnum 10/1 -tagged;bind vlan 40 -ifnum 10/2 -tagged
Fügen Sie eine SNIP-Adresse hinzu.	add ns ip <IPAddress> <netmask> -type SNIP;show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP;add ns ip 198.51.101.18 255.255.255.0 -type SNIP
Erstellen Sie Dienste, die HTTP-Server darstellen	add service <serviceName> <ip> HTTP <port>;show service <name>	add service SVC-S1 198.51.100.19 http 80add service SVC-S2 198.51.100.20 http 80;add service SVC-S3 198.51.101.19 http 80;add service SVC-S4 198.51.101.20 http 80
Erstellen Sie virtuelle HTTP-Lastausgleichsserver und binden Sie die Dienste daran	add lb vserver <name> HTTP <ip> <port>; bind lb vserver <vserverName> <serviceName>;show lb vserver <name>	add lb vserver LBVS-1 http 203.0.113.15 80; bind lb vserver LBVS-1 SVC-S1;bind lb vserver LBVS-1 SVC-S2
		add lb vserver LBVS-2 http 203.0.114.15 80; bind lb vserver LBVS-2 SVC-S3;bind lb vserver LBVS-2 SVC-S4
Erstellen Sie ein benutzerdefiniertes TCP-Profil und legen Sie dessen MSS für die Unterstützung von Jumbo-Frames fest	add tcpProfile <name> -mss <positive_integer>;show tcpProfile <name>	add tcpprofile ALL-JUMBO -mss 8960
Binden Sie das benutzerdefinierte TCP-Profil an den gewünschten virtuellen Lastausgleichsserver und die Dienste.	set service <Name> -tcpProfileName <string>;show service <name>	set lb vserver LBVS-1 - tcpProfileName ALL-JUMBO; set service SVC-S1 - tcpProfileName ALL-JUMBO;set service SVC-S2 - tcpProfileName ALL-JUMBO
Save the configuration	save ns config; show ns config

SNMP auf SDX-Appliances konfigurieren

November 23, 2023

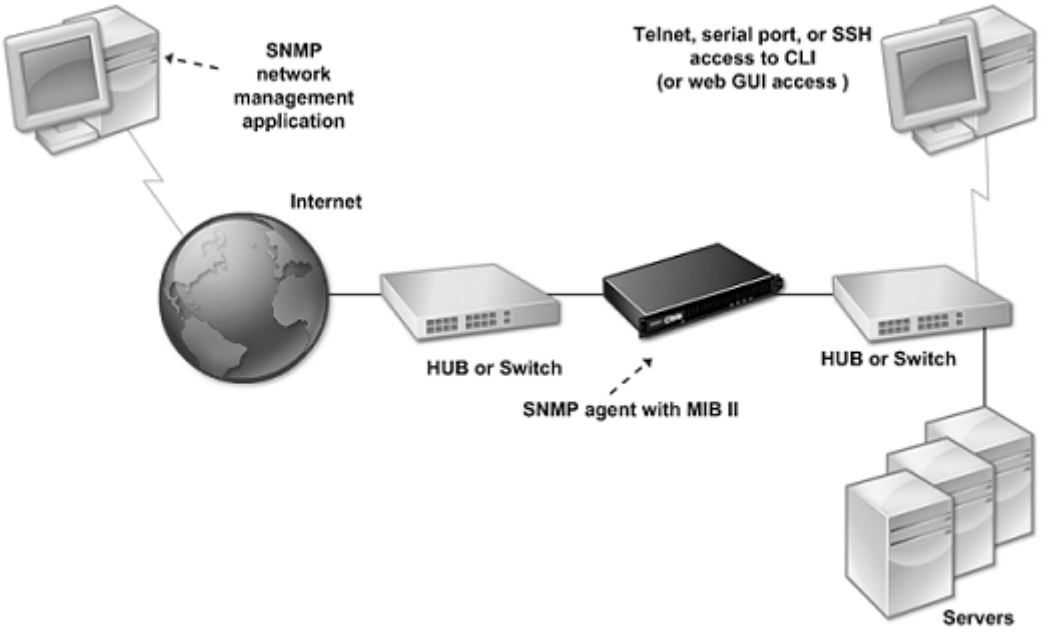
Sie können einen SNMP-Agenten auf der NetScaler SDX-Appliance konfigurieren, um asynchrone Ereignisse zu generieren, die als Traps bezeichnet werden. Die Traos werden immer dann generiert, wenn ungewöhnliche Bedingungen auf der SDX-Appliance vorliegen. Die Traps werden dann an ein Remotegerät gesendet, das als *Trap-Listener*bezeichnet wird und den abnormalen Zustand auf der SDX-Appliance signalisiert.

Neben der Konfiguration eines SNMP-Trap-Ziels, dem Herunterladen von MIB-Dateien und der Kon-

figuration eines oder mehrerer SNMP-Manager können Sie die NetScaler SDX-Appliance für SNMPv3-Abfragen konfigurieren.

Die folgende Abbildung zeigt ein Netzwerk mit einer SDX-Appliance, für die SNMP aktiviert und konfiguriert ist. In der Abbildung verwendet jede SNMP-Netzwerkverwaltungsanwendung SNMP, um mit dem SNMP-Agenten auf der SDX-Appliance zu kommunizieren.

Abbildung 1. *SDX-Appliance unterstützt SNMP*



Der SNMP-Agent auf der SDX-Appliance generiert Traps, die nur mit SNMPv2 kompatibel sind. Die unterstützten Traps können in der SDX MIB-Datei angezeigt werden. Sie können diese Datei von der Downloads-Seite in der SDX-Benutzeroberfläche herunterladen.

So fügen Sie ein SNMP-Trap-Ziel hinzu

1. Erweitern Sie auf der Registerkarte Konfiguration im Navigationsbereich **System > SNMP**, und klicken Sie dann auf SNMP-Trap-Ziele.
2. Klicken Sie im Bereich SNMP-Trap-Ziele auf Hinzufügen.
3. Geben Sie auf der Seite "SNMP-Trap-Ziel konfigurieren"Werte für die folgenden Parameter an:
    - Zielserver —IPv4-Adresse des Trap-Listeners, an den die SNMP-Trap-Nachrichten gesendet werden sollen.
    - Port —UDP-Port, an dem der Trap-Listener auf Trap-Meldungen wartet. Muss mit der Einstellung auf dem Trap-Listener übereinstimmen, sonst lässt der Listener die Nachrichten fallen. Mindestwert: 1. Standardeinstellung: 162.

- Community —Kennwort (Zeichenfolge), das mit den Trap-Nachrichten gesendet wird, damit der Trap-Listener sie authentifizieren kann. Kann Buchstaben, Zahlen und Bindestriche (-), Punkt (.) Hash (#), Leerzeichen (), At (@), Gleichheitszeichen (=), Doppelpunkt (:) und Unterstriche (_) enthalten.
  Hinweis: Geben Sie dieselbe Community-Zeichenfolge auf dem Trap-Listener-Gerät an, oder der Listener verwirft die Nachrichten. Standardeinstellung: öffentlich.

4. Klicken Sie auf Hinzufügenund dann auf Schließen. Das hinzugefügte SNMP-Trap-Ziel wird im Bereich SNMP-Traps angezeigt.

   Um die Werte der Parameter eines SNMP-Trap-Ziels zu ändern, wählen Sie im Bereich SNMP-Trap-Ziele das Trap-Ziel aus, das Sie ändern möchten, und klicken Sie dann auf Ändern. Ändern Sie im Dialogfeld SNMP-Trap-Ziel ändern die Parameter.

   Um einen SNMP-Trap zu entfernen, wählen Sie im Bereich SNMP-Trap-Ziele das Trap-Ziel aus, das Sie entfernen möchten, und klicken Sie dann auf Löschen. Klicken Sie im Feld Meldung bestätigen auf, um das Ziel des SNMP-Traps zu entfernen.

MIB-Dateien werden heruntergeladen

Sie müssen die folgende Datei herunterladen, bevor Sie mit der Überwachung einer SDX-Appliance beginnen.

SDX-MIB-smiv2.mib. Diese Datei wird von SNMPv2-Managern und SNMPv2-Trap-Listenern verwendet.

Die Datei enthält eine NetScaler Enterprise-MIB, die SDX-spezifische Ereignisse bereitstellt.

So laden Sie MIB-Dateien herunter

1. Melden Sie sich auf der Downloads-Seite der SDX-Appliance-Benutzeroberfläche an.
2. Klicken Sie unter SNMP-Dateien auf SNMP v2 - MIB-Objektdefinitionen. Sie können die Datei mit einem MIB-Browser öffnen.

Hinzufügen einer SNMP Manager-Community

Konfigurieren Sie SNMP-Manager auf der SDX-Appliance für die Abfrage und Überwachung der Appliance und der verwalteten Geräte, die auf der Appliance gehostet werden Außerdem müssen Sie dem SNMP-Manager die erforderlichen gerätespezifischen Informationen zur Verfügung stellen. Für einen IPv4-SNMP-Manager können Sie anstelle der IP-Adresse des Managers einen Hostnamen angeben. In diesem Fall müssen Sie einen DNS-Nameserver hinzufügen, der den Hostnamen des SNMP-Managers in seine IP-Adresse auflöst.

Konfigurieren Sie mindestens einen SNMP-Manager. Wenn Sie keinen SNMP-Manager konfigurieren, akzeptiert oder beantwortet die Appliance keine SNMP-Abfragen von einer IP-Adresse im Netzwerk. Wenn Sie einen oder mehrere SNMP-Manager konfigurieren, akzeptiert die Appliance und antwortet nur auf SNMP-Abfragen von diesen spezifischen IP-Adressen.

So konfigurieren Sie einen SNMP-Manager

1. Erweitern Sie auf der Registerkarte Konfiguration im Navigationsbereich System, und erweitern Sie dann SNMP.
2. Klicken Sie auf Manager.
3. Klicken Sie im Detailbereich auf "Hinzufügen".
4. Stellen Sie auf der Seite SNMP-Manager-Community erstellen die folgenden Parameter ein:
    - SNMP-Manager—IPv4-Adresse des SNMP-Managers. Anstelle einer IPv4-Adresse können Sie auch einen Hostnamen angeben, der einem SNMP-Manager zugewiesen wurde. In diesem Fall müssen Sie einen DNS-Nameserver hinzufügen, der den Hostnamen des SNMP-Managers in seine IP-Adresse auflöst.
    - Community—Die SNMP-Community-Zeichenfolge. Kann aus 1 bis 31 Zeichen bestehen, die Groß- und Kleinbuchstaben, Zahlen und den Bindestrich (-), Punkt (.) Pfund (#), At (@), Gleichheitszeichen (=), Doppelpunkt (:) und Unterstrich (_) enthalten.
    - Markieren Sie das Kontrollkästchen **Verwaltungsnetzwerk aktivieren**, um die SNMP-Manager mithilfe der Netzmaske anzugeben.
    - Geben Sie im Feld **Netzwerkmaske** die Netzmaske der SNMP-Community ein.
5. Klicken Sie auf Hinzufügenund dann auf Schließen.

Konfigurieren der SDX-Appliance für SNMPv3-Abfragen

SNMPv3 basiert auf der Grundstruktur und Architektur von SNMPv1 und SNMPv2. SNMPv3 erweitert jedoch die Basisarchitektur, um Verwaltungs- und Sicherheitsfunktionen wie Authentifizierung, Zugriffskontrolle, Datenintegritätsprüfung, Überprüfung des Datenursprungs, Überprüfung der Aktualität von Nachrichten und Datenvertraulichkeit zu integrieren.

Die NetScaler SDX-Appliance unterstützt die folgenden Entitäten, mit denen Sie die Sicherheitsfunktionen von SNMPv3 implementieren können:

- SNMP-Ansichten
- SNMP-Benutzer

Diese Entitäten arbeiten zusammen, um die SNMPv3-Sicherheitsfunktionen zu implementieren. Views werden erstellt, um den Zugriff auf Teilbäume der MIB zu ermöglichen.

Hinzufügen eines SNMP-Managers

Konfigurieren Sie die SDX-Appliance so, dass die entsprechenden SNMP-Manager sie abfragen können. Stellen Sie dem SNMP-Manager außerdem die erforderlichen gerätespezifischen Informationen zur Verfügung. Für einen IPv4-SNMP-Manager können Sie anstelle der IP-Adresse des Managers einen Hostnamen angeben. In diesem Fall müssen Sie einen DNS-Nameserver hinzufügen, der den Hostnamen des SNMP-Managers in seine IP-Adresse auflöst.

Konfigurieren Sie mindestens einen SNMP-Manager. Wenn Sie keinen SNMP-Manager konfigurieren, akzeptiert oder beantwortet die Appliance keine SNMP-Abfragen von einer IP-Adresse im Netzwerk. Wenn Sie einen oder mehrere SNMP-Manager konfigurieren, akzeptiert die Appliance und antwortet nur auf SNMP-Abfragen von diesen spezifischen IP-Adressen.

So konfigurieren Sie einen SNMP-Manager:

1. Navigieren Sie zur Seite **System > Konfiguration** .
2. Erweitern Sie auf der Registerkarte Konfiguration im Navigationsbereich System, und erweitern Sie dann SNMP.
3. Klicken Sie auf Manager.
4. Klicken Sie im Detailbereich auf “Hinzufügen”.
5. Legen Sie im Dialogfeld SNMP Manager-Community hinzufügen die folgenden Parameter fest:
    - **SNMP-Manager**—IPv4-Adresse des SNMP-Managers. Anstelle einer IPv4-Adresse können Sie auch einen Hostnamen angeben, der einem SNMP-Manager zugewiesen wurde. In diesem Fall müssen Sie einen DNS-Nameserver hinzufügen, der den Hostnamen des SNMP-Managers in seine IP-Adresse auflöst.
    - **Community**—Die SNMP-Community-Zeichenfolge. Kann aus 1 bis 31 Zeichen bestehen, die Groß- und Kleinbuchstaben, Zahlen und den Bindestrich (-), Punkt (.) Pfund (#), At (@), Gleichheitszeichen (=), Doppelpunkt (:) und Unterstrich (_) enthalten.
6. Klicken Sie auf Hinzufügenund dann auf Schließen.

Konfigurieren einer SNMP-Ansicht

SNMP-Ansichten beschränken den Benutzerzugriff auf bestimmte Teile der MIB. SNMP-Ansichten werden verwendet, um die Zugriffssteuerung zu implementieren.

So konfigurieren Sie eine Ansicht

1. Erweitern Sie auf der Registerkarte Konfiguration im Navigationsbereich System, und erweitern Sie dann SNMP.
2. Klicken Sie auf Ansichten.

3. Klicken Sie im Detailbereich auf "Hinzufügen".
4. Stellen Sie im Dialogfeld SNMP-Ansicht hinzufügen die folgenden Parameter ein:

    - Name —Name für die SNMPv3-Ansicht. Kann aus 1—31 Zeichen bestehen, die Groß- und Kleinbuchstaben, Zahlen und den Bindestrich (-), Punkt (.) Pfund (#), At (@), Gleichheitszeichen (=), Doppelpunkt (:) und Unterstrich (_) enthalten. Wählen Sie einen Namen, mit dessen Hilfe die SNMPv3-Ansicht identifiziert werden kann.
    - Teilbaum —Ein bestimmter Zweig (Teilbaum) des MIB-Baums, den Sie dieser SNMPv3-Ansicht zuordnen möchten. Geben Sie den Teilbaum als SNMP-OID an.
    - Typ —Schließt den durch den Teilbaum-Parameter angegebenen Teilbaum in oder aus dieser Ansicht ein. Diese Einstellung kann nützlich sein, wenn Sie einen Teilbaum wie A in eine SNMPv3-Ansicht aufgenommen haben und einen bestimmten Teilbaum von A, z. B. B, aus der SNMPv3-Ansicht ausschließen möchten.

Konfigurieren eines SNMP-Benutzers

Nachdem Sie eine SNMP-Ansicht erstellt haben, fügen Sie SNMP-Benutzer hinzu. SNMP-Benutzer haben Zugriff auf die MIBs, die für die Abfrage der SNMP-Manager erforderlich sind.

So konfigurieren Sie einen Benutzer

1. Erweitern Sie auf der Registerkarte Konfiguration im Navigationsbereich System, und erweitern Sie dann SNMP.
2. Klicken Sie auf Benutzer.
3. Klicken Sie im Detailbereich auf "Hinzufügen".
4. Stellen Sie auf der Seite SNMP-Benutzer erstellen die folgenden Parameter ein:

    - Name —Name für den SNMPv3-Benutzer. Kann aus 1—31 Zeichen bestehen, die Groß- und Kleinbuchstaben, Zahlen und den Bindestrich (-), Punkt (.) Pfund (#), At (@), Gleichheitszeichen (=), Doppelpunkt (:) und Unterstrich (_) enthalten.
    - Sicherheitsstufe —Sicherheitsstufe, die für die Kommunikation zwischen der Appliance und den SNMPv3-Benutzern erforderlich ist. Wählen Sie eine der folgenden Optionen:
        - noAuthNoPriv —erfordert weder Authentifizierung noch Verschlüsselung.
        - authNoPriv —Authentifizierung erforderlich, aber keine Verschlüsselung.
        - authPriv —Authentifizierung und Verschlüsselung erforderlich.
    - Authentifizierungsprotokoll —Authentifizierungsalgorithmus, der von der Appliance und dem SNMPv3-Benutzer zur Authentifizierung der Kommunikation zwischen ihnen verwendet wird. Geben Sie denselben Authentifizierungsalgorithmus an, wenn Sie den SNMPv3-Benutzer im SNMP-Manager konfigurieren.

- Authentifizierungskennwort —Passphrase, die vom Authentifizierungsalgorithmus verwendet werden soll. Kann aus 1—31 Zeichen bestehen, die Groß- und Kleinbuchstaben, Zahlen und den Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), At (@), Gleich (=), Doppelpunkt (:) und Unterstrich (_) enthalten.
- Datenschutzprotokoll —Verschlüsselungsalgorithmus, der von der Appliance und dem SNMPv3-Benutzer zum Verschlüsseln der Kommunikation zwischen ihnen verwendet wird. Geben Sie denselben Verschlüsselungsalgorithmus an, wenn Sie den SNMPv3-Benutzer im SNMP-Manager konfigurieren.
- Anzeigename —Name der konfigurierten SNMPv3-Ansicht, die Sie an diesen SNMPv3-Benutzer binden möchten. Ein SNMPv3-Benutzer kann auf die Teilbäume zugreifen, die an diese SNMPv3-Ansicht gebunden sind, als Typ INCLUDED, kann jedoch nicht auf die Teilbäume zugreifen, die vom Typ EXCLUDED sind.

Konfigurieren eines SNMP-Alarms

Die Appliance stellt einen vordefinierten Satz von Bedingungseinheiten bereit, die als SNMP-Alarme Wenn die für einen SNMP-Alarm festgelegte Bedingung erfüllt ist, generiert die Appliance SNMP-Trap-Nachrichten, die an die konfigurierten Trap-Listener gesendet werden. Wenn beispielsweise der DeviceAdded-Alarm aktiviert ist, wird eine Trap-Nachricht generiert und an den Trap-Listener gesendet, wenn ein Gerät (eine Instanz) auf der Appliance bereitgestellt wird. Sie können einem SNMP-Alarm einen Schweregrad zuweisen. Wenn Sie dies tun, wird den entsprechenden Trap-Nachrichten dieser Schweregrad zugewiesen.

Im Folgenden sind die auf der Appliance definierten Schweregrade in absteigender Reihenfolge des Schweregrads aufgeführt:

- Kritisch
  - Hauptfach
- Minor
- Warnung
- Informativ (Standard)

Wenn Sie beispielsweise einen Warnschweregrad für den SNMP-Alarm mit dem Namen DeviceAdded festlegen, werden den Trap-Nachrichten, die beim Hinzufügen eines Geräts generiert werden, der Schweregrad Warnung zugewiesen.

Sie können auch einen SNMP-Alarm konfigurieren, um die entsprechenden Trap-Meldungen zu protokollieren, die generiert werden, wenn die Bedingung für diesen Alarm erfüllt ist.

Um einen vordefinierten SNMP-Alarm zu ändern, klicken Sie auf **System > SNMP > Alarme**.

Konfigurieren von Syslog-Benachrichtigungen

November 23, 2023

SYSLOG ist ein Standard-Protokollierungsprotokoll. Es besteht aus zwei Komponenten: dem SYSLOG-Auditing-Modul, das auf der NetScaler SDX-Appliance ausgeführt wird, und dem SYSLOG-Server, der auf einem Remote-System ausgeführt werden kann. SYSLOG verwendet UDP für die Datenübertragung.

Wenn Sie einen SYSLOG-Server ausführen, stellt er eine Verbindung zur SDX-Appliance her. Die Appliance beginnt dann, alle Protokollinformationen an den SYSLOG-Server zu senden, und der Server kann die Protokolleinträge filtern, bevor er sie in einer Protokolldatei speichert. Ein SYSLOG-Server kann Protokollinformationen von mehr als einer SDX-Appliance empfangen, und eine SDX-Appliance kann Protokollinformationen an mehr als einen SYSLOG-Server senden.

Die Protokollinformationen, die ein SYSLOG-Server von einer
SDX-Appliance sammelt, werden in einer Protokolldatei in Form von Nachrichten gespeichert. Diese Meldungen enthalten normalerweise die folgenden Informationen:

- Die IP-Adresse der SDX-Appliance, die die Protokollnachricht generiert hat
- Zeitstempel
- Meldungstyp
- Die Protokollebene (Kritisch, Fehler, Hinweis, Warnung, Information, Debug, Warnung oder Notfall)
- Meldungstext

Sie können anhand dieser Informationen die Ursache einer Warnung analysieren und ggf. Maßnahmen ergreifen. Konfigurieren Sie zunächst einen Syslog-Server, an den die Appliance Protokollinformationen sendet, und geben Sie dann das Daten- und Zeitformat für die Aufzeichnung der Protokollmeldungen an.

Konfigurieren eines Syslog-Servers

1. Navigieren Sie zu **System > Benachrichtigungen > Syslog-Server**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie auf der Seite "Syslog-Server erstellen** "Werte für die Syslog-Serverparameter an. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Feld.
4. Klicken Sie auf **Hinzufügen**und dann auf **Schließen**.

Konfigurieren der Syslog-Parameter

1. Navigieren Sie zu **System > Benachrichtigungen > Syslog-Server**.
2. Klicken Sie im Detailbereich auf **Syslog-Parameter**.
3. Geben **Sie auf der Seite Syslog-Parameter konfigurieren** das Datums- und Uhrzeitformat an.
4. Klicken Sie auf **OK** und dann auf **Schließen**.

E-Mail-Benachrichtigungen konfigurieren

November 23, 2023

Konfigurieren Sie einen SMTP-Server so, dass er jedes Mal, wenn eine Warnung ausgelöst wird, eine E-Mail-Nachricht empfängt. Konfigurieren Sie zunächst einen SMTP-Server und anschließend ein E-Mail-Profil. Verwenden Sie im E-Mail-Profil Kommas, um die Adressen der Empfänger zu trennen.

So konfigurieren Sie einen SMTP-Server

1. Navigieren Sie zu **System > Benachrichtigungen > E-Mail**.
2. Klicken Sie im Detailbereich auf die Registerkarte **E-Mail-Server**, und klicken Sie dann auf **Hinzufügen**.
3. Geben Sie auf der Seite **E-Mail-Server erstellen** Werte für die Serverparameter an.
    - **Servername/IP-Adresse**: Geben Sie den Servernamen oder die IP-Adresse des SMTP-Mailservers ein.
    - **Port**: Geben Sie die Portnummer ein. Der Standardwert ist 25.
    - **Authentifizierung**: Wählen Sie diese Option, um den Zugriff auf den E-Mail-Server zu authentifizieren.
    - **Sicher**: Wählen Sie diese Option, um eine sichere E-Mail-Verbindung herzustellen. Standardmäßig wird TLS 1.2 verwendet, um die E-Mail-Kommunikation zu verschlüsseln.
4. Klicken Sie auf **Erstellen**.

So konfigurieren Sie ein E-Mail-Profil

1. Navigieren Sie zu **System > Benachrichtigungen > E-Mail**.
2. Klicken Sie im Detailbereich auf die Registerkarte **E-Mail**, und klicken Sie dann auf **Hinzufügen**.

3. Geben **Sie auf der Seite E-Mail-Verteilerliste erstellen** Werte für die Parameter an. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Feld.
4. Klicken Sie auf **Erstellen**.

Konfigurieren von SMS-Benachrichtigungen

November 23, 2023

Konfigurieren Sie einen SMS-Server (Short Message Service) für den Empfang einer SMS-Nachricht bei jeder Warnmeldung. Konfigurieren Sie zunächst einen SMS-Server und anschließend ein SMS-Profil. Verwenden Sie im SMS-Profil Kommas, um die Adressen der Empfänger zu trennen.

Konfigurieren eines SMS-Servers

1. Navigieren Sie zu **System > Benachrichtigungen > SMS**.
2. Klicken Sie im Detailbereich auf **SMS-Server**, und klicken Sie dann auf **Hinzufügen**.
3. Geben **Sie auf der Seite SMS-Server erstellen** die Werte für die SMS-Serverparameter an. Die Werte für diese Parameter werden vom Anbieter bereitgestellt.
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

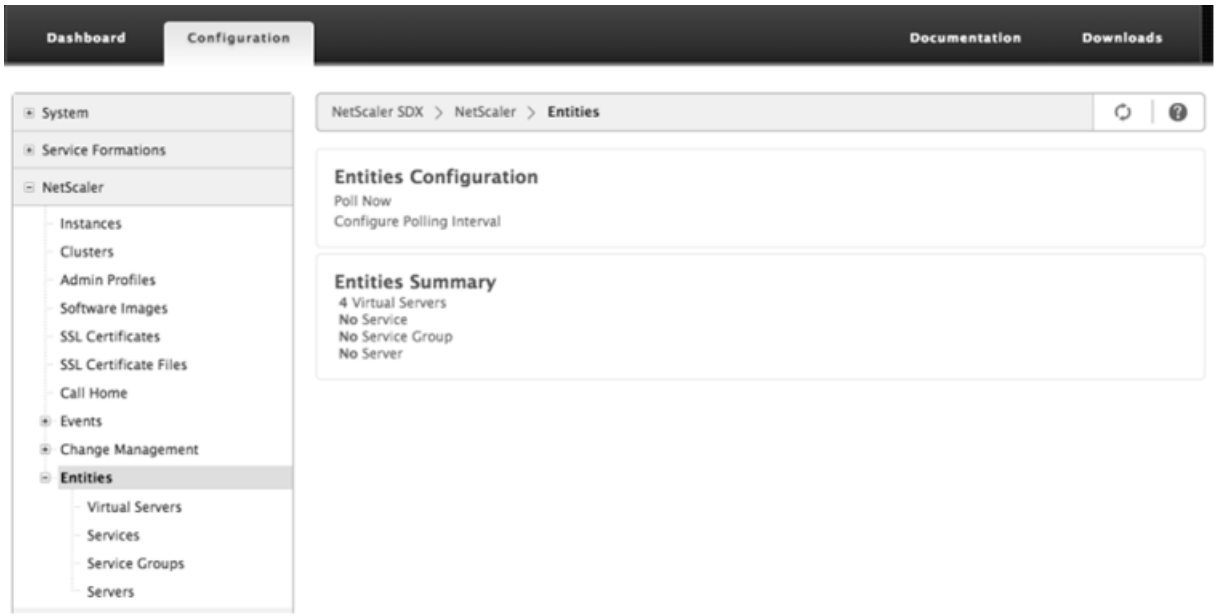
Konfigurieren eines SMS-Profils

1. Navigieren Sie zu **System > Benachrichtigungen > SMS**.
2. Klicken Sie im Detailbereich auf **SMS-Verteilerliste**, und klicken Sie dann auf **Hinzufügen**.
3. Geben **Sie auf der Seite SMS-Verteilerliste erstellen** die Werte für die E-Mail-Profilparameter an. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Feld.
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Überwachung und Verwaltung des Echtzeitstatus von Entitäten, die auf einer SDX-Appliance konfiguriert

February 15, 2024

Die NetScaler SDX-Appliance kann den Status virtueller Server, Dienste, Dienstgruppen und Server auf den virtuellen Appliances überwachen und verwalten, die auf der SDX-Appliance gehostet werden. Sie können Werte überwachen, z. B. den Zustand eines virtuellen Servers und die Zeit, die seit der letzten Statusänderung eines Dienstes oder einer Dienstgruppe vergangen ist. Diese Überwachung gibt Ihnen Einblick in den Echtzeitstatus der Entitäten und erleichtert die Verwaltung dieser Entitäten, wenn Sie viele Entitäten auf Ihren NetScaler-Instances konfiguriert haben.



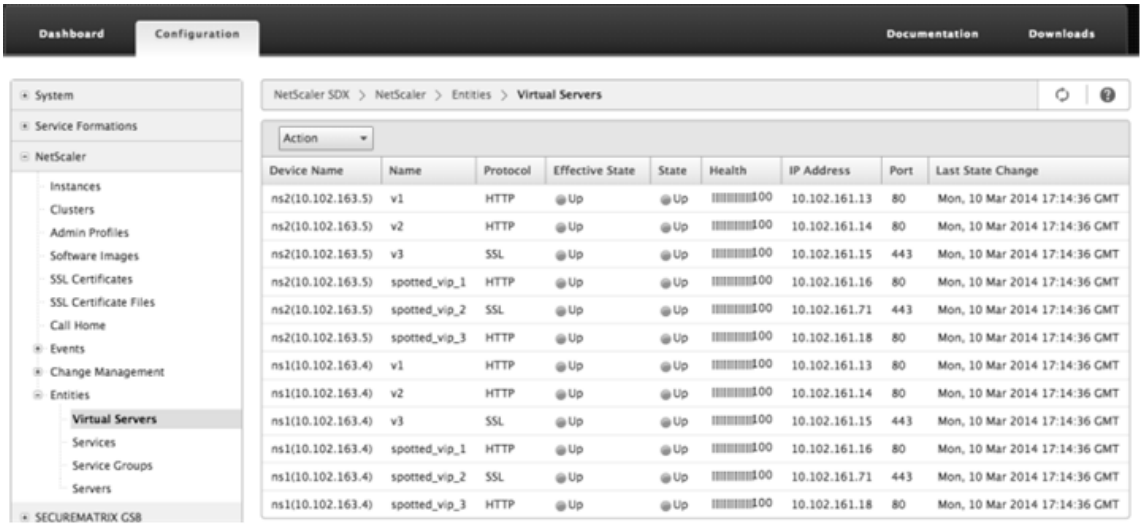
Zeigen Sie den Status virtueller Server an

Sie können die Echtzeitwerte des Status und des Zustands eines virtuellen Servers überwachen. Sie können auch die Attribute eines virtuellen Servers wie Name, IP-Adresse und Typ des virtuellen Servers anzeigen.

- So zeigen Sie den Status eines virtuellen Servers an

  1. Klicken Sie auf der Registerkarte Konfiguration im Navigationsbereich auf **NetScaler > Entitäten > Virtuelle Server**.
  2. Zeigen Sie im rechten Bereich unter Virtuelle Server die folgenden Statistiken an:
     - Gerätename —Name des VPX, auf dem der virtuelle Server konfiguriert ist.
     - Name —Name des virtuellen Servers.
     - Protokoll —Diensttyp des virtuellen Servers. Zum Beispiel HTTP, TCP und SSL.
     - Gültigkeitsstatus —Gültigkeitsstatus des virtuellen Servers, basierend auf dem Status der virtuellen Backupserver. Zum Beispiel UP, DOWN oder OUT OF SERVICE.
     - Status —Aktueller Status des virtuellen Servers. Zum Beispiel UP, DOWN oder OUT OF SERVICE.

- Integrität —Prozentsatz der Dienste, die sich im Status “UP”befinden und an den virtuellen Server gebunden sind. Die folgende Formel wird verwendet, um den prozentualen Gesundheitszustand zu berechnen: (Anzahl der gebundenen UP-Dienste * 100)/Gebundene Dienste insgesamt
- IP-Adresse —Die IP-Adresse des virtuellen Servers. Clients senden Verbindungsanfragen an diese IP-Adresse.
- Port —Port, an dem der virtuelle Server auf Clientverbindungen wartet.
- Letzte Statusänderung —Verstrichene Zeit (in Tagen, Stunden, Minuten und Sekunden) seit der letzten Änderung des Status des virtuellen Servers. Das heißt, die Zeitdauer, für die sich der virtuelle Server im aktuellen Zustand befand. Diese Informationen sind nur für virtuelle Server verfügbar, die mit NetScaler Version 9.0 und höher konfiguriert sind.

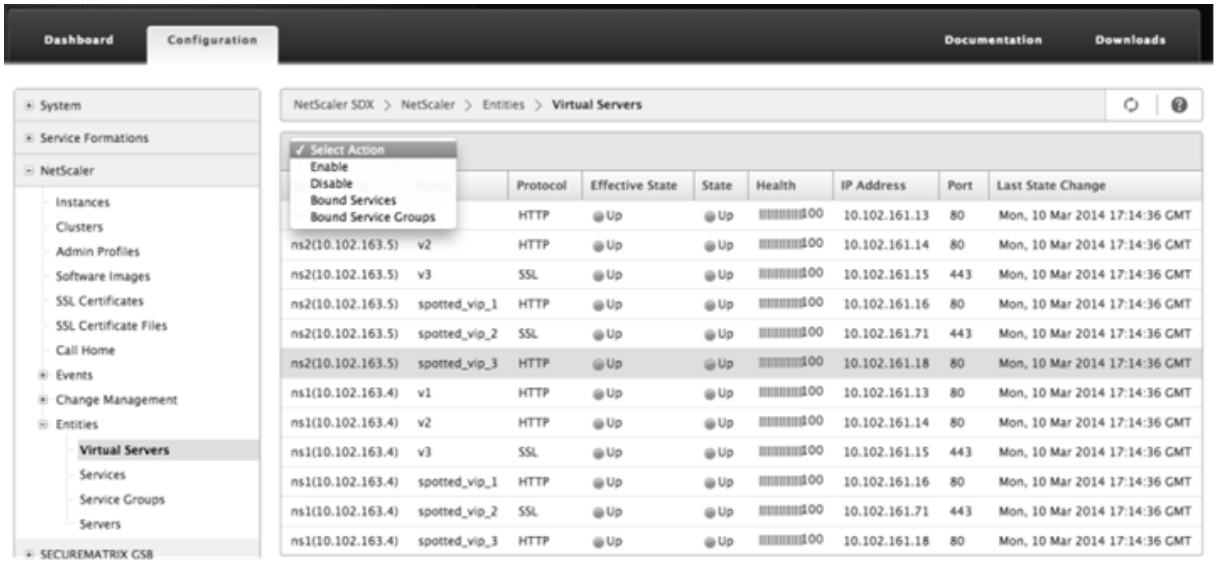


- An einen virtuellen Server gebundene Dienste und Dienstgruppen anzeigen

  Sie können den Echtzeitstatus der Dienste und Dienstgruppen überwachen, die an einen virtuellen Server gebunden sind. Mit dieser Überwachung können Sie den Status der Dienste überprüfen, die dazu führen könnten, dass der Integritätsprozentsatz eines virtuellen Servers niedrig wird, sodass Sie geeignete Maßnahmen ergreifen können.

  So zeigen Sie die an einen virtuellen Server gebundenen Dienste und Dienstgruppen an

  1. Klicken Sie auf der Registerkarte Konfiguration im linken Bereich auf **NetScaler > Entitäten > Virtuelle Server**.
  2. Klicken Sie im Detailbereich unter Virtuelle Server auf den Namen des virtuellen Servers, für den Sie die gebundenen Dienste und Dienstgruppen anzeigen möchten, und klicken Sie unter Aktionen auf Gebundene Dienste oder Gebundene Dienstgruppen. Klicken Sie alternativ mit der rechten Maustaste auf den Namen des virtuellen Servers, und klicken Sie dann auf Gebundene Dienste oder Gruppen für gebundene Dienste.



Zeigen Sie den Status der Dienste an

Sie können die Echtzeitwerte des Status eines Dienstes und die Dauer überwachen, für die sich der Dienst im aktuellen Zustand befand.

So zeigen Sie den Status virtueller Server an

1. Klicken Sie auf der Registerkarte Konfiguration im Navigationsbereich auf **NetScaler > Entities > Service**.
2. Zeigen Sie im Detailbereich unter Dienste die folgenden Statistiken an:

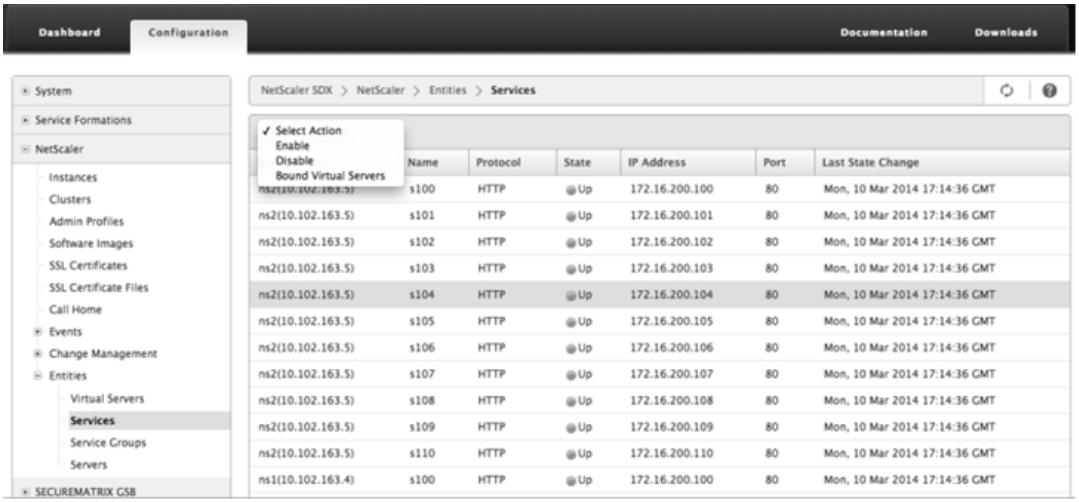
    - Gerätename —Name des Geräts, auf dem der Dienst konfiguriert ist.
    - Name —Name des Dienstes.
    - Protokoll —Diensttyp, der das Verhalten des Dienstes bestimmt. Zum Beispiel HTTP, TCP, UDP oder SSL.
    - State —Aktueller Status des Dienstes. Zum Beispiel UP, DOWN oder OUT OF SERVICE.
    - IP-Adresse —Die IP-Adresse des Dienstes.
    - Port —Port, auf dem der Dienst lauscht.
    - Letzte Statusänderung —Verstrichene Zeit (in Tagen, Stunden, Minuten und Sekunden) seit der letzten Änderung des Status des Dienstes. Das heißt, die Dauer, für die sich der Dienst im aktuellen Zustand befindet.

- Anzeigen der virtuellen Server, an die ein Dienst gebunden ist

  Sie können die virtuellen Server anzeigen, an die ein Dienst gebunden ist, und den Echtzeitstatus der virtuellen Server überwachen.

  So zeigen Sie die virtuellen Server an, an die ein Dienst gebunden ist

1. Klicken Sie auf der Registerkarte Konfiguration im Navigationsbereich auf **NetScaler > Entities > Service**.
2. Klicken Sie im Detailbereich unter Dienste auf den Namen des Dienstes, für den Sie die gebundenen virtuellen Server anzeigen möchten. Wählen Sie dann im Menü Aktion die Option Gebundene virtuelle Server aus. Sie können auch mit der rechten Maustaste auf den Dienst klicken und dann auf Gebundene virtuelle Server



Status von Dienstgruppen anzeigen

Sie können den Echtzeitstatus eines Dienstgruppenmitglieds über die SDX-Schnittstelle überwachen.

So zeigen Sie den Status von Dienstgruppen an

1. Klicken Sie auf der Registerkarte Konfiguration im Navigationsbereich auf **NetScaler > Entities > Service**Groups.
2. Zeigen Sie im Detailbereich unter Service Groups die folgenden Statistiken an:
   - Gerätename —Name des Geräts, auf dem die Dienstgruppe konfiguriert ist.
   - Name —Name der Dienstgruppe.
   - IP-Adresse —Die IP-Adresse jedes Dienstes, der Mitglied der Dienstgruppe ist.
   - Port —Ports, auf denen die Mitglieder der Dienstgruppe zuhören.
   - Protokoll —Diensttyp, der das Verhalten der Dienstgruppe bestimmt. Zum Beispiel HTTP, TCP, UDP oder SSL.
   - Gültigkeitsstatus —Gültigkeitsstatus der virtuellen Servergruppe, basierend auf dem Status der virtuellen Backupserver. Zum Beispiel UP, DOWN oder OUT OF SERVICE
   - State —Gültiger Status der Dienstgruppe, der auf dem Status des Mitglieds der Dienstgruppe basiert. Zum Beispiel UP, DOWN oder OUT OF SERVICE.
   - Letzte Statusänderung —Verstrichene Zeit (in Tagen, Stunden, Minuten und Sekunden) seit der letzten Änderung des Status des Dienstgruppenmitglieds. Das heißt, die Dauer,

für die sich das Mitglied der Servicegruppe im aktuellen Zustand befindet. Diese Informationen sind nur für Mitglieder der Dienstgruppe verfügbar, die mit NetScaler Version 9.0 und höher konfiguriert sind.

- Anzeigen der virtuellen Server, an die ein Dienst gebunden ist

  Sie können die virtuellen Server anzeigen, an die ein Dienst gebunden ist, und den Echtzeitstatus der virtuellen Server überwachen.

  So zeigen Sie die virtuellen Server an, an die der Dienst gebunden ist

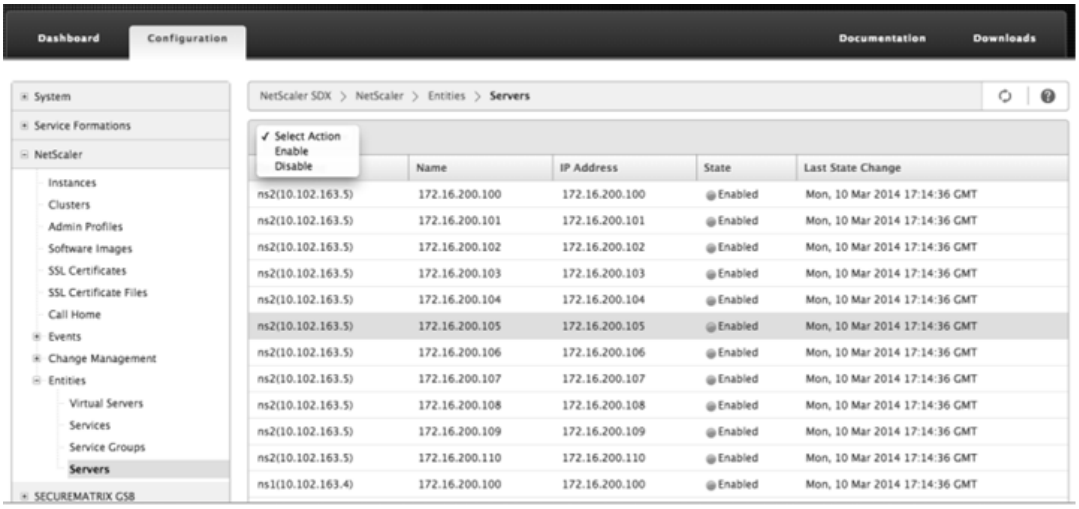
  1. Klicken Sie auf der Registerkarte Konfiguration im linken Bereich auf **NetScaler > Entitäten > Server**.
  2. Wählen Sie im rechten Bereich unter Server den Server aus der Liste aus, und klicken Sie im Menü Aktionen auf Gebundene virtuelle Dienste. Klicken Sie alternativ mit der rechten Maustaste auf den Dienst und klicken Sie auf Gebun

Zeigen Sie den Status von Servern an

Sie können den Status der Server in den NetScaler-Instanzen überwachen und verwalten. Diese Überwachung gibt Ihnen Einblick in den Echtzeitstatus der Server und erleichtert die Verwaltung dieser Server, wenn Sie über viele Server verfügen.

So zeigen Sie den Status von Servern an

1. Klicken Sie auf der Registerkarte Konfiguration im Navigationsbereich auf **NetScaler > Entitäten > Server**.
2. Zeigen Sie im Detailbereich unter Server die folgenden Statistiken an:
   - Gerätename: Gibt den Namen des Geräts an, auf dem der Server konfiguriert ist.
   - Name: Gibt den Namen des Servers an.
   - IP-Adresse: Gibt die IP-Adresse des Servers an. Clients senden Verbindungsanfragen an diese IP-Adresse.
   - Status: Gibt den aktuellen Status des Servers an. Zum Beispiel UP, DOWN und OUT OF SERVICE.
   - Letzte Statusänderung: Gibt die Zeit an, die seit der letzten Änderung des Serverstatus (in Tagen, Stunden, Minuten und Sekunden) vergangen ist. Das heißt, die Zeitdauer, für die sich der Server im aktuellen Zustand befindet.



Konfigurieren des Abrufintervalls

Sie können das Zeitintervall festlegen, für das die SDX-Appliance die Echtzeitwerte der virtuellen Server, Dienste, Dienstgruppen und Server abfragen soll. Standardmäßig fragt die Appliance die Werte alle 30 Minuten ab.

- Konfigurieren des Abfrageintervalls für virtuelle Server, Dienste, Dienstgruppen und Server.

    1. Klicken Sie auf der Registerkarte Konfiguration auf **NetScaler > Entitäten**und klicken Sie im rechten Bereich auf Configure Polling Interval.
    2. Geben Sie im Dialogfeld Abfrageintervall konfigurieren die Anzahl der Minuten ein, die Sie als Zeitintervall festlegen möchten, für das SDX den Entitätswert abfragen muss. Der Mindestwert des Abrufintervalls beträgt 30 Minuten. Klicken Sie auf OK.

Überwachen und Verwalten von Ereignissen, die auf NetScaler-Instanzen generiert wurden

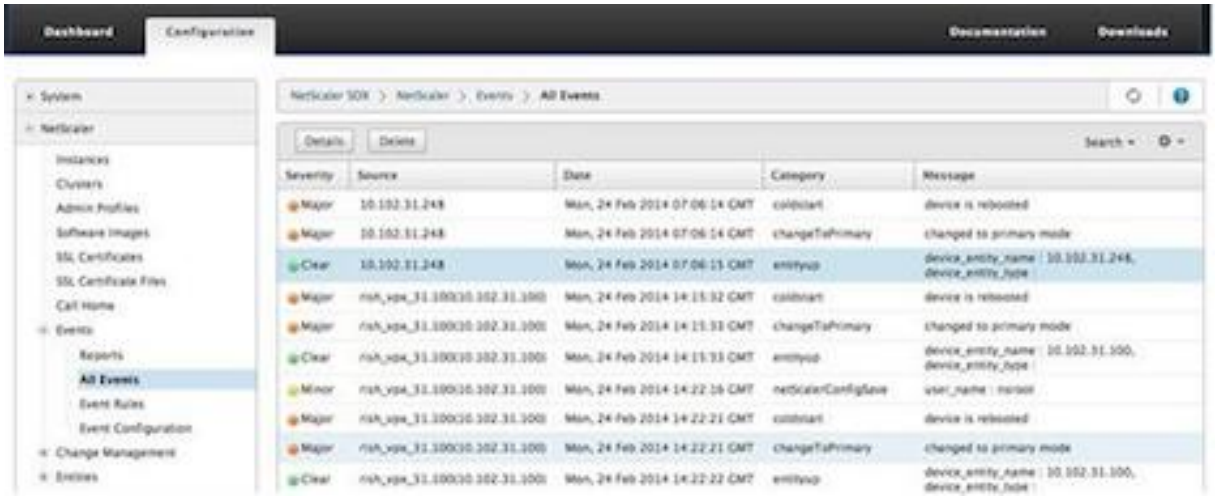
February 15, 2024

Verwenden Sie die Funktion Ereignisse, um die auf den NetScaler-Instanzen generierten Ereignisse zu überwachen und zu verwalten. Der Management Service identifiziert Ereignisse in Echtzeit und hilft Ihnen so, Probleme sofort zu beheben, und sorgt dafür, dass die NetScaler-Instanzen effektiv laufen. Sie können auch Ereignisregeln konfigurieren, um die generierten Ereignisse zu filtern und benachrichtigt zu werden, um Maßnahmen in der gefilterten Ereignisliste zu ergreifen.

Alle Ereignisse anzeigen

Sie können alle Ereignisse anzeigen, die auf den NetScaler-Instanzen generiert wurden, die auf der NetScaler SDX-Appliance bereitgestellt wurden. Sie können die Details wie Schweregrad, Kategorie, Datum, Quelle und Meldung für jedes der Ereignisse anzeigen.

Um die Ereignisse anzuzeigen, navigieren Sie zu **Konfiguration > NetScaler > Ereignisse > Alle**Ereignisse.



Sie können den Ereignisverlauf und die Entitätsdetails anzeigen, indem Sie das Ereignis auswählen und auf die Schaltfläche **Details** klicken. Sie können auch nach einem bestimmten Ereignis suchen oder es von dieser Seite löschen.

Hinweis: Nachdem Sie die Ereignisse gelöscht haben, können Sie sie nicht mehr wiederherstellen.

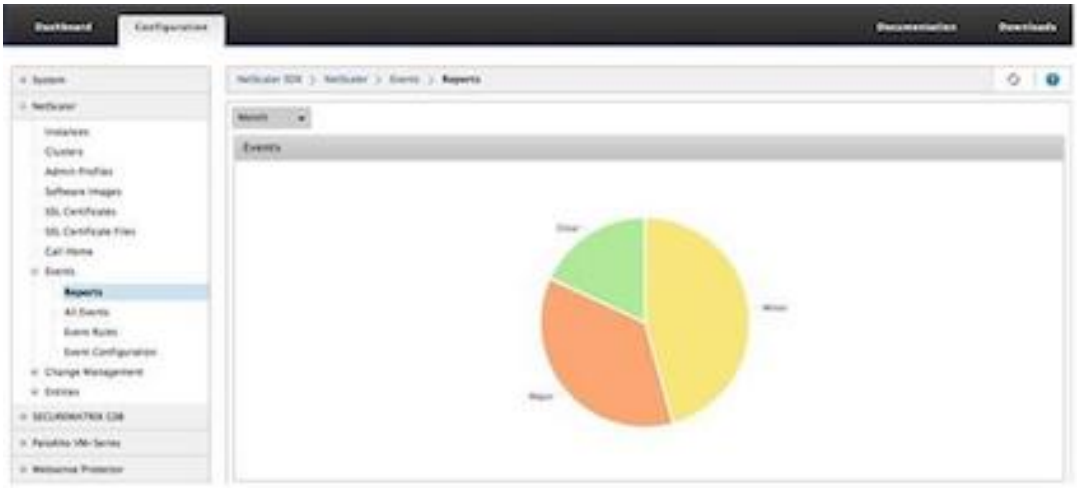
- Anzeigen von Berichten

  Auf der Seite “Berichte”wird die Zusammenfassung der Ereignisse in einem grafischen Format angezeigt. Ihre Ansicht der Berichte kann auf verschiedenen Zeitskalen basieren. Standardmäßig ist die Zeitskala Tag.

  Um die Berichte anzuzeigen, navigieren Sie zu **Konfiguration > NetScaler > Ereignisse**Berichte. Im Folgenden finden Sie die grafischen Berichte, die vom Management Service unterstützt werden

  - **Ereignisse**

    Der Ereignisbericht ist eine Tortendiagrammdarstellung der Anzahl der Ereignisse, segmentiert und basierend auf ihrem Schweregrad farbcodiert.

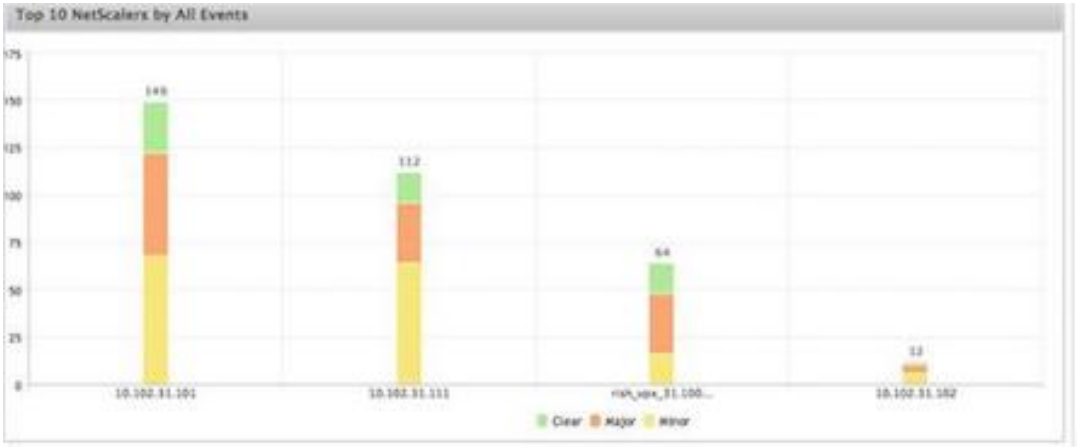


Um die Details der Ereignisse mit einem bestimmten Schweregrad anzuzeigen, klicken Sie auf dieses Segment des Tortendiagramms. Sie können die folgenden Details anzeigen:

* Quelle: Systemname, Hostname oder die IP-Adresse, für die das Ereignis generiert wurde.
* Datum: Datum und Uhrzeit, zu der der Alarm generiert wurde.
* Kategorie: Ereigniskategorie (z. B. `entityup`).
* Meldung: Ereignisbeschreibung.

– **Die 10 besten NetScaler-Instanzen nach allen Ereignissen**

Bei diesem Bericht handelt es sich um ein Balkendiagramm, in dem die 10 wichtigsten NetScaler-Instanzen entsprechend der Anzahl der Ereignisse für die ausgewählte Zeitskala angezeigt werden.



– **Die 10 wichtigsten NetScaler-Instanzen nach Entity State Change-Ereignissen**

Bei diesem Bericht handelt es sich um ein Balkendiagramm, in dem die 10 wichtigsten NetScaler-Instanzen entsprechend der Anzahl der Entitätsstatusänderungen für die

ausgewählte Zeitskala angezeigt werden. Die Änderungen des Entitätsstatus spiegeln Ereignisse nach oben, Entity Down oder Out of Service wider.

- **Die 10 NetScaler-Instanzen mit den meisten Schwellenwertverstößen**

  Bei diesem Bericht handelt es sich um ein Balkendiagramm, in dem die 10 wichtigsten NetScaler-Instances entsprechend der Anzahl der Ereignisse zur Verletzung des Schwellenwerts für die ausgewählte Zeitskala angezeigt werden. Die Ereignisse der Schwellenwertverletzung spiegeln die folgenden Ereignisse wider:

  * cpuUtilization
  * memoryUtilization
  * diskUsageHigh
  * temperatureHigh
  * voltageLow
  * voltageHigh
  * fanSpeedLow
  * temperatureCpuHigh
  * interfaceThroughputLow
  * interfaceBWUseHigh
  * aggregateBWUseHigh

- **Top 10 NetScaler-Instanzen nach Hardwarefehlerereignissen Bei**
  diesem Bericht handelt es sich um ein Balkendiagramm, in dem die 10 wichtigsten NetScaler-Instances entsprechend der Anzahl der Hardwarefehlerereignisse für die gewählte Zeitskala angezeigt werden. Die Hardwarefehlereignisse spiegeln die folgenden Ereignisse wider:

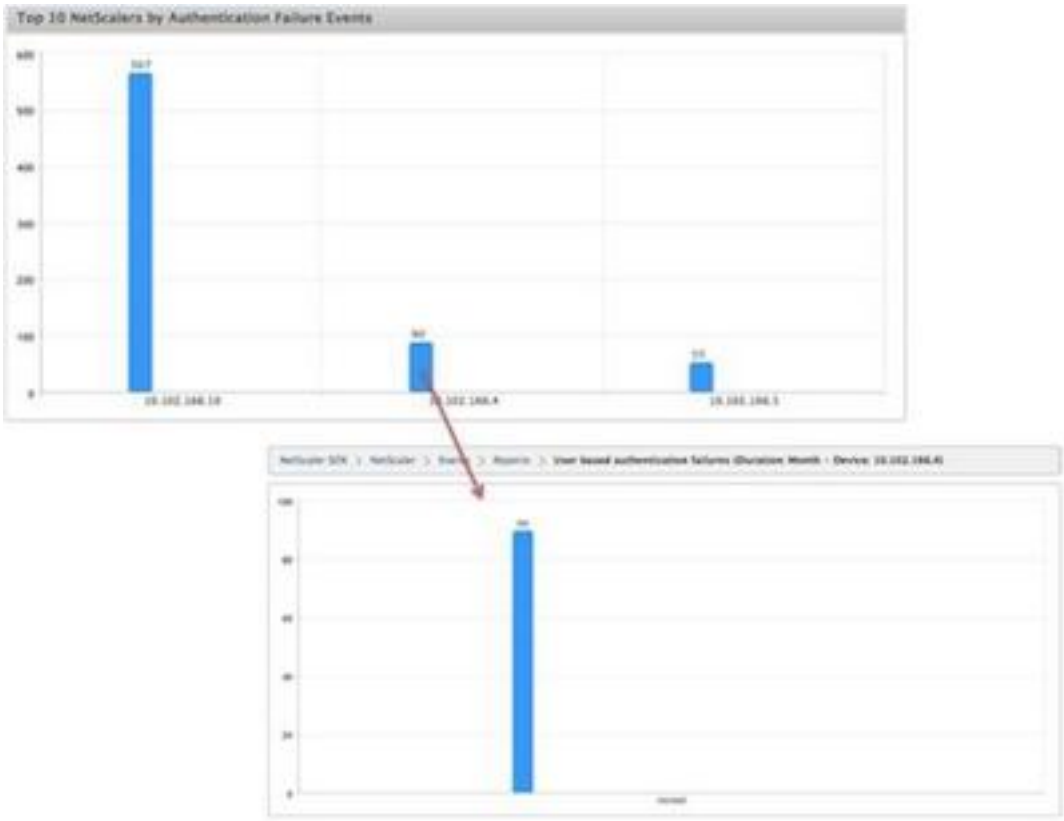
  * hardDiskDriveErrors
  * compactFlashErrors
  * powerSupplyFailed
  * “sslCardFailed”

– **Die 10 wichtigsten NetScaler-Instanzen nach Ereignissen mit Konfigurationsänderungen**

Bei diesem Bericht handelt es sich um ein Balkendiagramm, das die 10 wichtigsten NetScaler-Instances entsprechend der Anzahl der Konfigurationsänderungsereignisse für die ausgewählte Zeitskala wiedergibt. Sie können auf das Diagramm klicken, um einen Drilldown durchzuführen und die benutzerbasierten Konfigurationsänderungen für eine Instanz anzuzeigen. Sie können die Autorisierungs- und Ausführungsstatusdetails weiter anzeigen, indem Sie auf dieses Diagramm klicken.

– <**Die 10 häufigsten NetScaler-Instanzen nach Authentifizierungsfehlerereignissen**

Bei diesem Bericht handelt es sich um ein Balkendiagramm, in dem die 10 wichtigsten NetScaler-Instanzen entsprechend der Anzahl der Authentifizierungsfehlerereignisse für die ausgewählte Zeitskala angezeigt werden. Sie können auf das Diagramm klicken, um einen Drilldown durchzuführen und die benutzerbasierten Authentifizierungsfehler für eine Instanz anzuzeigen.



- Konfigurieren von Ereignisregeln

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 Bedingun-

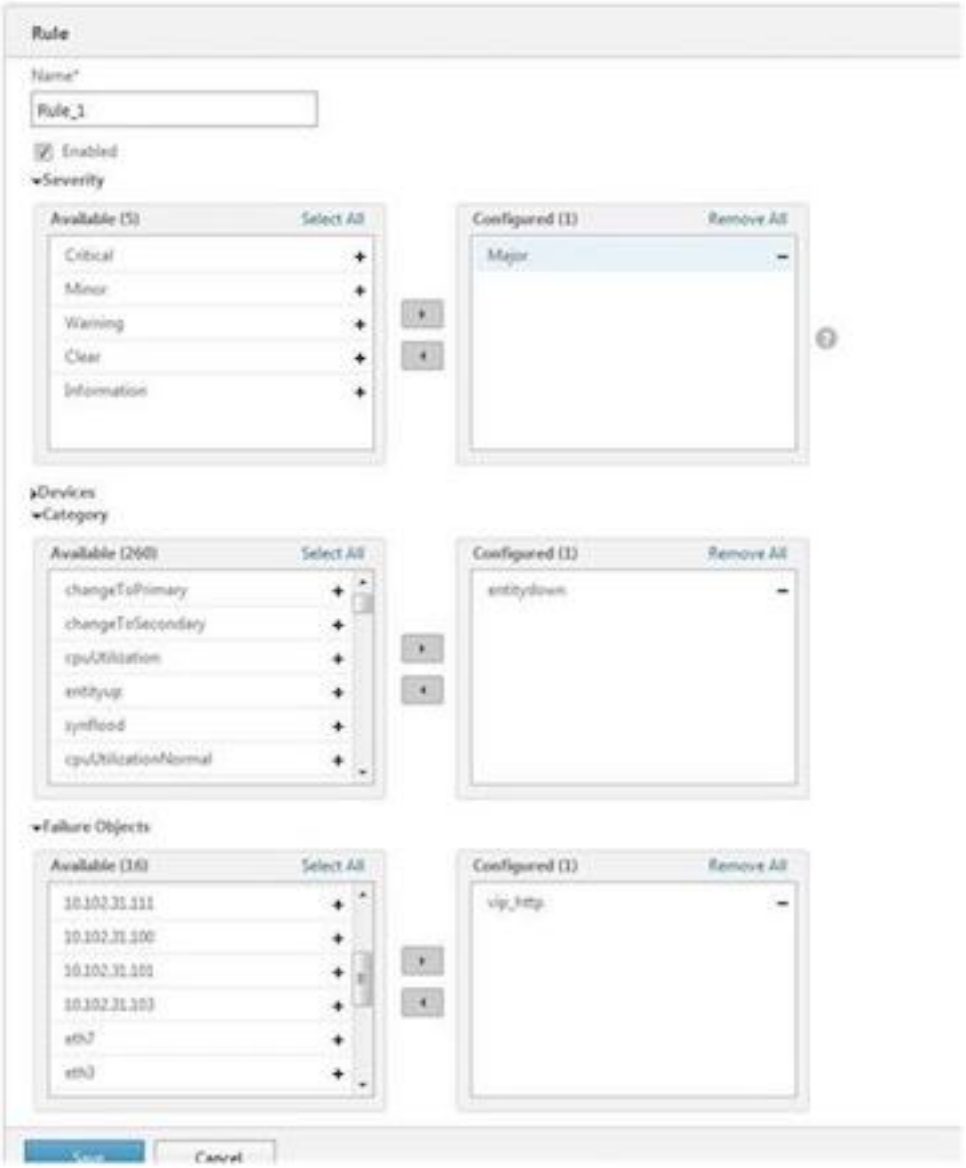
gen, für die Sie Filter erstellen können, sind: Schweregrad, Geräte, Fehlerobjekte und Kategorie.

Sie können den Ereignissen die folgenden Aktionen zuweisen:

- **E-Mail senden Aktion** Sendet eine E-Mail mit den Ereignissen, die den Filterkriterien entsprechen.
- **Aktion "SMS senden"** Sendet einen Short Message Service (SMS) für die Ereignisse, die den Filterkriterien entsprechen.

So fügen Sie Ereignisregeln hinzu

1. Navigieren Sie zu **Konfiguration > NetScaler > Ereignisse > Ereignisregeln**und klicken Sie auf Hinzufügen.
2. Stellen Sie auf der Seite Regel die folgenden Parameter ein:
   - Name —Name der Ereignisregel.
   - Aktiviert —Aktiviert die Ereignisregel.
   - Schweregrad —Schweregrad der Ereignisse, für die Sie die Ereignisregel hinzufügen möchten.
   - Geräte —IP-Adressen der NetScaler-Instanzen, für die Sie eine Ereignisregel definieren möchten.
   - Kategorie —Kategorie oder Kategorien der von den NetScaler-Instanzen generierten Ereignisse.
   - Ausfallobjekte —Entity-Instanzen oder Leistungsindikatoren, für die ein Ereignis generiert wurde.

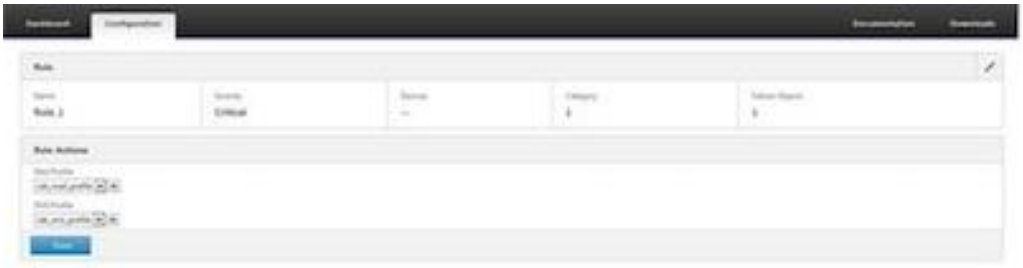


Hinweis: Diese Liste kann Leistungsindikatornamen für alle Ereignisse im Zusammenhang mit Schwellenwerten, Entitätsnamen für alle entitätsbezogenen Ereignisse und Zertifikatsnamen für zertifikatsbezogene Ereignisse enthalten.

3. Klicken Sie auf Speichern.
4. Unter Regelaktionen können Sie die Benachrichtigungsaktionen für das Ereignis zuweisen.

   a) E-Mail-Profil —Details des Mailservers und des E-Mail-Profils. Eine E-Mail wird ausgelöst, wenn die Ereignisse die definierten Filterkriterien erfüllen.

   b) SMS-Profil —SMS-Server- und SMS-Profildetails. Eine SMS wird ausgelöst, wenn die Ereignisse die definierten Filterkriterien erfüllen.

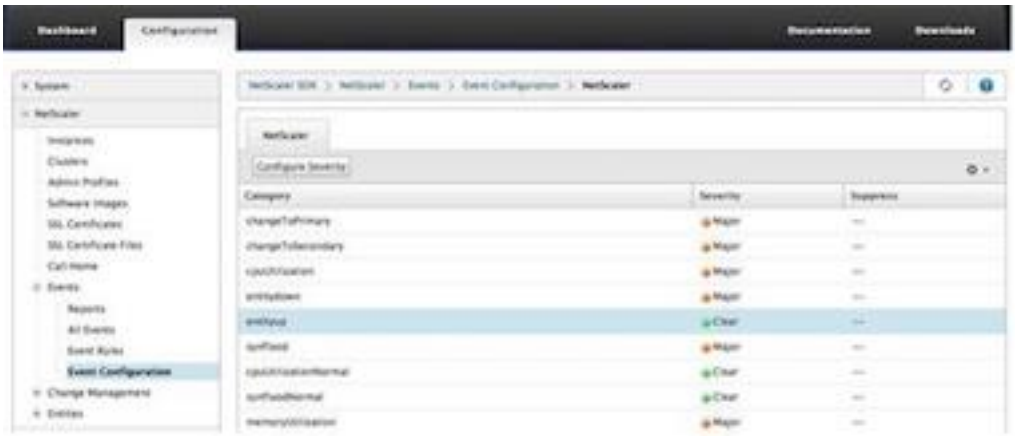


5. Klicken Sie auf Fertig.

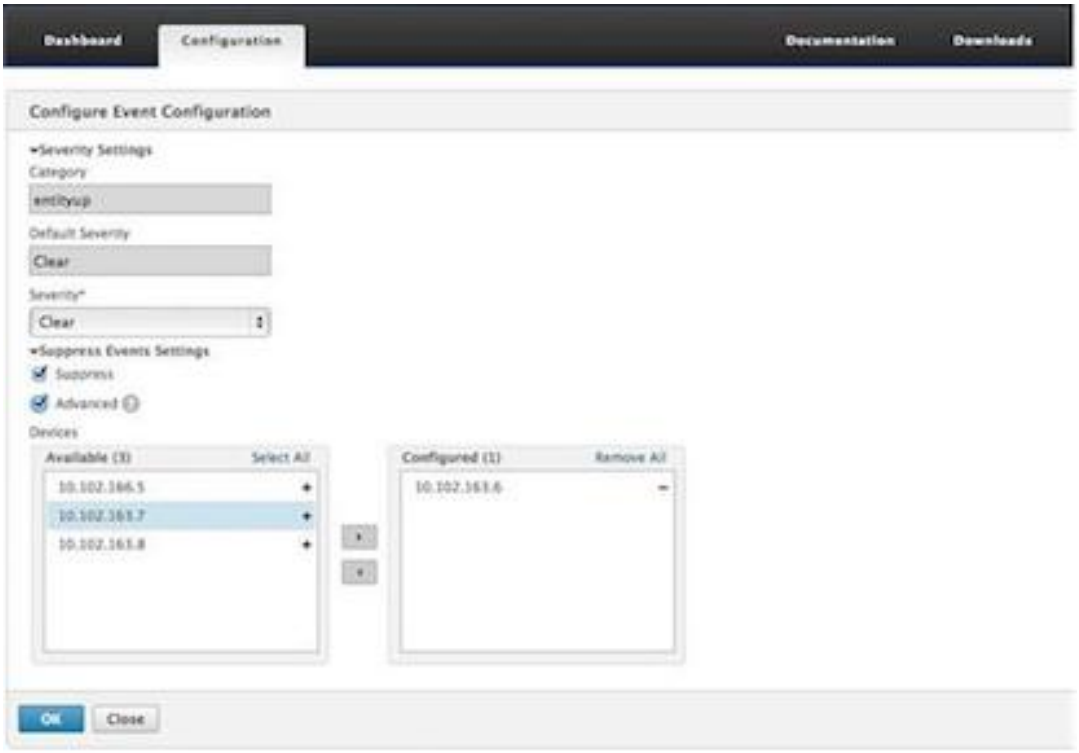
- Ereignisse konfigurieren

  Sie können Ereignissen, die für die NetScaler-Instanzen auf der SDX-Appliance generiert werden, Schweregrade zuweisen. Sie können die folgenden Typen von Schweregrad definieren: Kritisch, Major, Minor, Warnung, Löschen und Information. Sie können die Ereignisse auch für eine bestimmte Zeit unterdrücken.
  Konfigurieren des Schweregrads:

  1. Navigieren Sie zu **Konfiguration > NetScaler > Ereignisse > Ereigniskonfiguration**, wählen Sie das Ereignis aus der Liste aus und klicken Sie dann auf Schweregrad konfigurieren.



  2. Wählen Sie auf der Seite Ereigniskonfiguration konfigurieren in der Dropdownliste den erforderlichen Schweregrad aus.
  3. Sie können die Ereignisse auch unterdrücken, indem Sie das Kontrollkästchen Unterdrücken aktivieren. Sie können auch die NetScaler-Instanzen angeben, für die Sie dieses Ereignis unterdrücken möchten, indem Sie die Option Advanced verwenden.



4. Klicken Sie auf OK.

Call Home-Support für NetScaler-Instanzen auf einer SDX-Appliance

February 15, 2024

Die Call Home-Funktion überwacht Ihre NetScaler-Instances auf häufig auftretende Fehler. Sie können jetzt die Call Home-Funktion auf NetScaler-Instances über die Management Service-Benutzeroberfläche konfigurieren, aktivieren oder deaktivieren.

Hinweis: Die NetScaler-Instanz muss auf dem Server des technischen Supports von Citrix registriert sein, bevor Call Home die Systemdaten auf den Server hochladen kann, wenn vordefinierte Fehlerbedingungen auf der Appliance auftreten. Durch die Aktivierung der Call Home-Funktion auf der NetScaler-Instanz wird der Registrierungsprozess eingeleitet.

- Call Home auf einer NetScaler-Instanz aktivieren und deaktivieren

  Sie können die Call Home-Funktion auf einer NetScaler-Instanz über den Management Service aktivieren. Wenn Sie die Call Home-Funktion aktivieren, registriert der Call Home-Prozess die NetScaler-Instanz beim Citrix Technical Support Server. Die Registrierung dauert einige Zeit. Während dieser Zeit zeigt der Management Service den Fortschritt der Registrierung an.

Um die Call Home-Funktion zu aktivieren, navigieren Sie zu **Konfiguration > NetScaler > Call Home**, wählen Sie die NetScaler-Instanz aus und klicken Sie auf die Schaltfläche Aktivieren. Klicken Sie auf der Bestätigungsseite auf Ja.

Um die Call Home-Funktion zu deaktivieren, navigieren Sie zu **Konfiguration > NetScaler > Call Home**, wählen Sie die NetScaler-Instanz aus und klicken Sie auf die Schaltfläche Deaktivieren. Klicken Sie auf der Bestätigungsseite auf Ja.

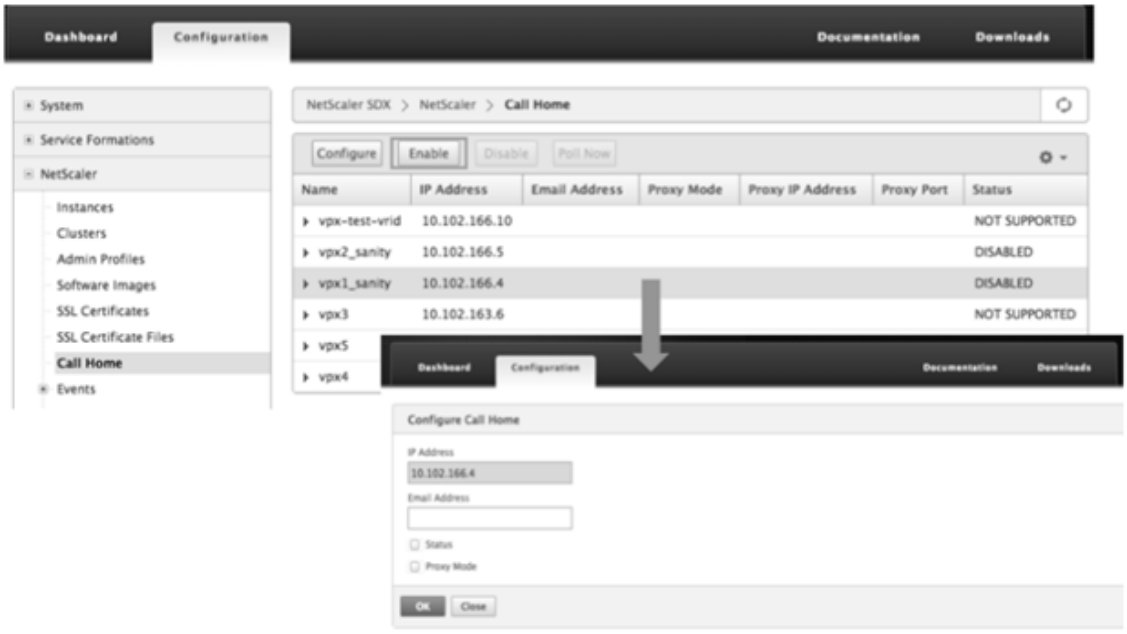
Wenn Sie Call Home aktivieren, können Sie die folgenden Optionen konfigurieren:

1. (Optional) Geben Sie die E-Mail-Adresse des Administrators an. Der Call Home-Prozess sendet die E-Mail-Adresse an den Support-Server, wo sie für zukünftige Korrespondenz zu Call Home gespeichert wird.
2. (Optional) Proxymodus Call Home aktivieren. Call Home kann die Daten Ihrer NetScaler-Instanz über einen Proxyserver auf den Citrix TaaS-Server hochladen. Um diese Funktion zu verwenden, aktivieren Sie sie auf Ihrer NetScaler-Instanz und geben Sie die IP-Adresse und Portnummer eines HTTP-Proxyservers an. Der gesamte Datenverkehr vom Proxy-Server zu den TaaS-Servern (über das Internet) erfolgt über SSL und ist verschlüsselt, sodass Datensicherheit und Datenschutz nicht beeinträchtigt werden.

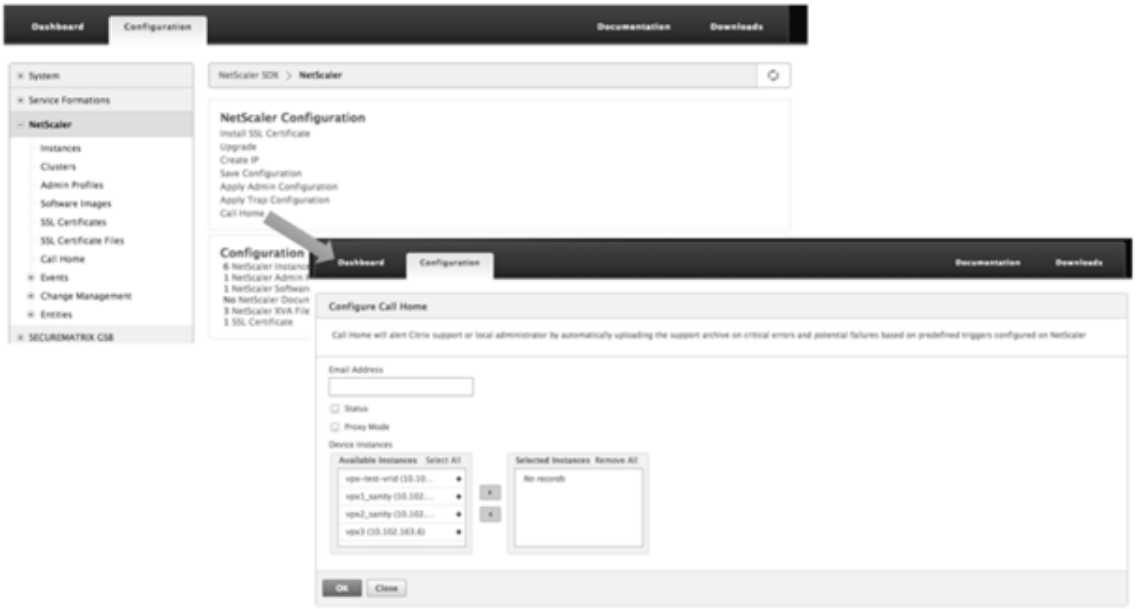
- So konfigurieren Sie Call Home auf der NetScaler-Instanz über den Management Service

  Sie können die Call Home-Funktion auf einer einzelnen Instanz oder auf mehreren Instanzen gleichzeitig konfigurieren.

  Um die Call Home-Funktion auf einer einzelnen NetScaler-Instanz zu konfigurieren, navigieren Sie zu **Konfiguration > NetScaler > Call Home, wählen Sie die NetScaler-Instanz**aus und klicken Sie auf die Schaltfläche Configure. Klicken Sie auf der Seite Call Home konfigurieren auf OK.



Um die Call Home-Funktion auf mehreren NetScaler-Instanzen zu konfigurieren, navigieren Sie zu **Konfiguration**NetScaler. Klicken Sie im rechten Bereich auf Call Home. Wählen Sie auf der Seite Configure Call Home im Abschnitt Verfügbare Instances die NetScaler-Instances aus, geben Sie weitere Details an und klicken Sie auf OK.



– Abfragen der NetScaler-Instanzen

  Um die Call Home-Funktion von allen NetScaler-Instanzen aus abzufragen und den aktuellen Status einzusehen, navigieren Sie zu **Konfiguration > NetScaler > Call Home** und klicken Sie auf **Jetzt abfragen**. Klicken Sie auf der Bestätigungsseite auf **Ja**.

Überwachung des Systemzustands

November 23, 2023

Die Systemzustandsüberwachung erkennt Fehler in den überwachten Komponenten, sodass Sie Korrekturmaßnahmen ergreifen können, um einen Ausfall zu vermeiden. Die folgenden Komponenten werden auf einer NetScaler SDX-Appliance überwacht:

- Hardware- und Software-Ressourcen
- Physische und virtuelle Datenträger
- <Hardwaresensoren wie Lüfter-, Temperatur-, Spannungs- und Stromversorgungssensoren
- Schnittstellen

Klicken Sie auf der Registerkarte **Überwachung** auf **Systemintegrität**. Eine Zusammenfassung aller Komponenten wird angezeigt. Um Details der überwachten Komponenten anzuzeigen, erweitern Sie **Systemzustand**, und klicken Sie dann auf die Komponente, die Sie überwachen möchten.

- Überwachen der Ressourcen auf der SDX-Appliance

  Sie können die Hardware- und Softwarekomponenten auf der SDX-Appliance überwachen und gegebenenfalls Korrekturmaßnahmen ergreifen. Um die überwachten Komponenten anzuzeigen, erweitern Sie auf der Registerkarte Überwachung den Systemzustand, und klicken Sie dann auf Ressourcen. Details zu Hardware- und Softwareressourcen werden angezeigt. Für alle Hardwarekomponenten werden aktuelle und erwartete Werte angezeigt. Für Softwarekomponenten, mit Ausnahme der BMC-Firmware-Version, werden aktuelle und erwartete Werte als nicht zutreffend (NA) angezeigt.

- **Name:** Name der Komponente, z. B. CPU-, Speicher- oder BMC-Firmware-Version.
- **Status:** Zustand (Zustand) der Komponente. Für
  Hardware und für die BMC-Firmware-Version zeigt ERROR eine Abweichung vom erwarteten Wert an. Bei Aufrufen von Citrix Hypervisor zeigt ERROR an, dass der Management Service nicht mit Citrix Hypervisor mithilfe eines API-, HTTP-, PING- oder SSH-Aufrufs kommunizieren kann. Für
  das Health Monitor-Plug-In zeigt ERROR an, dass das Plug-in nicht auf dem Citrix Hypervisor installiert ist.
- **Aktueller Wert:** Aktueller Wert der Komponente. Unter normalen Bedingungen entspricht der aktuelle Wert dem erwarteten Wert.
- **Erwarteter Wert:** Erwarteter Wert für die Komponente. Gilt nicht für Softwareaufrufe an Citrix Hypervisor.

Überwachen Sie die Speicherressourcen auf der SDX-Appliance

Sie können die Datenträger auf der SDX-Appliance überwachen und gegebenenfalls Korrekturmaßnahmen ergreifen. Um die überwachten Komponenten anzuzeigen, erweitern Sie auf der Registerkarte **Überwachung** den **Systemzustand**, und klicken Sie dann auf **Speicher**. Details werden für physische Datenträger und für virtuelle Datenträger oder Partitionen angezeigt, die aus physischen Datenträgern erstellt wurden.

Für Datenträger (Disk) werden die folgenden Details angezeigt:

- **Name** Der Name des physikalischen Datenträgers.
- **Größe:** Größe des Datenträgers in GB.
- **Verwendet:** Datenmenge auf dem Datenträger in GB.
- **Transaktionen/S:** Anzahl der Blöcke, die pro Sekunde gelesen oder geschrieben werden. Diese Zahl wird aus der Ausgabe `iostat` gelesen.
- **Blocks gelesen/s:** Anzahl der pro Sekunde gelesenen Blöcke. Sie können diesen Wert verwenden, um die Ausgangsrate von dem Datenträger zu messen.
- **Geschriebene Blöcke:** Anzahl der pro Sekunde geschriebenen Blöcke. Sie können diesen Wert verwenden, um die Eingangsrate von dem Datenträger zu messen.
- **Gesamtanzahl gelesener Blöcke:** Anzahl der seit dem letzten Start der Appliance gelesenen Blöcke.
- **Gesamtanzahl geschriebener Blöcke:** Anzahl der seit dem letzten Start der Appliance geschriebenen Blöcke.

Für virtuelle Datenträger oder Partitionen (Storage Repository) werden die folgenden Details angezeigt:

- **Laufwerksschacht:** Nummer des Laufwerks im Laufwerksschacht. Sie können die Daten für diesen Parameter sortieren.
- **Status:** Zustand (Zustand) des Laufwerks im Laufwerksschacht. Mögliche Werte:
  - GOOD: Das Laufwerk befindet sich in einem guten Zustand und ist einsatzbereit.
  - FAIL: Das Laufwerk ist ausgefallen und muss ersetzt werden.
  - MISSING: Ein Laufwerk wurde im Laufwerksschacht nicht erkannt.
  - UNKNOWN: Ein neues unformatiertes Laufwerk ist im Laufwerksschacht vorhanden.
- **Name:** Vom System definierter Name des Lagers.
- **Größe:** Größe des Speicher-Repositorys in GB.
- **Verwendet:** Datenmenge im Speicher-Repository in GB.

Überwachen der Hardware-Sensoren auf der SDX-Appliance

Sie können die Hardwarekomponenten auf der SDX-Appliance überwachen und gegebenenfalls Korrekturmaßnahmen ergreifen. Erweitern Sie auf der Registerkarte **Überwachung** den **Systemzustand**, und klicken Sie dann auf **Hardwaresensoren**. Die Überwachungsfunktion zeigt Details über die Geschwindigkeit verschiedener Lüfter, die Temperatur und Spannung verschiedener Komponenten und den Status der Stromversorgung an.

Für die Lüftergeschwindigkeit werden die folgenden Details angezeigt:

- **Name:** Name des Lüfters.
- **Status:** Zustand (Zustand) des Lüfters. ERROR zeigt eine Abweichung vom erwarteten Wert an. NA zeigt an, dass der Lüfter nicht vorhanden ist.
- **Aktueller Wert (U/min):** Aktuelle Umdrehungen pro Minute.

Zu den Temperaturinformationen gehören die folgenden Details:

- **Name:** Name der Komponente, wie CPU oder Speichermodul (z. B. P1-DIMM1A.)
- **Status:** Zustand (Zustand) der Komponente. ERROR zeigt an, dass der aktuelle Wert außerhalb des zulässigen Bereichs liegt.
- **Aktueller Wert (Grad C):** Aktuelle Temperatur des Bauteils in Grad.

Zu den Spannungsinformationen gehören die folgenden Details:

- **Name:** Name der Komponente, z. B. CPU-Kern.
- **Status:** Zustand (Zustand) der Komponente. ERROR zeigt an, dass der aktuelle Wert außerhalb des zulässigen Bereichs liegt.
- **Stromwert (Volt):** Aktuelle Spannungen, die an der Komponente vorhanden sind.

Informationen zur Stromversorgung beinhalten folgende Details:

- **Name:** Name der Komponente.
- **Status:** Zustand (Zustand) der Komponente. Mögliche Werte:
  - **Fehler**: Nur ein Netzteil ist angeschlossen oder funktioniert.
  - **OK**: Beide Netzteile sind angeschlossen und funktionieren wie erwartet.

Überwachen Sie die Schnittstellen auf der SDX-Appliance

Sie können die Schnittstellen auf der SDX-Appliance überwachen und gegebenenfalls Korrekturmaßnahmen ergreifen. Erweitern Sie auf der Registerkarte **Überwachung** den **Systemzustand**, und klicken Sie dann auf **Schnittstellen**. Die Überwachungsfunktion enthält die folgenden Informationen zu jeder Schnittstelle:

- **Schnittstelle:** Schnittstellennummer auf der SDX-Appliance.

- **Status:** Zustand der Schnittstelle. Mögliche Werte: UP, DOWN.
- **Zugewiesene VFs/Insgesamt:** Anzahl der virtuellen Funktionen (VFs), die der Schnittstelle zugewiesen sind, und die Anzahl der auf dieser Schnittstelle verfügbaren virtuellen Funktionen. Verschiedene Plattformen unterstützen eine unterschiedliche Anzahl von VFs.
- **Tx-Pakete:** Anzahl der Pakete, die seit dem letzten Start der Appliance übertragen wurden.
- **Rx-Paket:** Anzahl der Pakete, die seit dem letzten Start der Appliance empfangen wurden.
- **Tx Byte:** Anzahl der Byte, die seit dem letzten Start der Appliance übertragen wurden.
- **Rx Byte:** Anzahl der Byte, die seit dem letzten Start der Appliance empfangen wurden.
- **Tx-Fehler:**Anzahl der Fehler beim Übertragen von Daten seit dem letzten Start der Appliance.
- **Rx-Fehler:** Anzahl der Fehler beim Empfangen von Daten seit dem letzten Start der Appliance.

Systembenachrichtigungseinstellungen konfigurieren

November 23, 2023

Sie können Benachrichtigungen senden, um mit ausgewählten Benutzergruppen für eine Reihe von systembezogenen Funktionen zu kommunizieren. Sie können im SDX Management Service einen Benachrichtigungsserver einrichten, um E-Mail- und Short Message Service (SMS) -Gateway-Server so zu konfigurieren, dass sie E-Mail- und Textbenachrichtigungen (SMS) an Benutzer senden.

> **Hinweis**
>
> Nach dem Upgrade auf SDX Management Service Version 11.1 ist die Systembenachrichtigung für alle Ereigniskategorien aktiviert, und die Benachrichtigungen werden an das vorhandene E-Mail- oder SMS-Profil gesendet.

Konfigurieren der Einstellungen für Systembenachrichtigungen

1. Navigieren Sie zu **System > Benachrichtigungen > Einstellungen,** und klicken Sie dann auf **Benachrichtigungseinstellungen ändern.**
2. Geben Sie auf der Seite **"Systembenachrichtigungseinstellungen konfigurieren** "die folgenden Details ein:
   - **Kategorie** —Kategorie oder Kategorien der vom SDX Management Service generierten Ereignisse.
   - E-Mail —Wählen Sie eine E-Mail-Verteilerliste aus dem Dropdownmenü aus. Sie können auch eine neue E-Mail-Verteilerliste erstellen, indem Sie auf das Symbol **+** klicken und die Details des neuen E-Mail-Servers in die entsprechenden Felder eingeben.
   - SMS (Textnachricht) —Wählen Sie eine SMS-Verteilerliste aus dem Dropdownmenü aus. Sie können auch eine

neue SMS-Verteilerliste erstellen, indem Sie auf das Symbol **+** klicken und die neuen SMS-Serverdetails in die entsprechenden Felder eingeben.

3. Klicken Sie auf **OK.**

Funktionen des Management Service aktivieren und deaktivieren

November 23, 2023

> **Hinweis**:
>
> Diese Funktion ist in Version 13.1 Build 12.x und höher verfügbar.

Auf einer NetScaler SDX-Appliance fragt der Management Service die NetScaler-Instanzen im Hintergrund nach Vorgängen wie SSL-Zertifikaten, Netzwerkfunktionen und Konfigurationsaudits ab. Je nach Anforderung ist eine Option verfügbar, um diese Abfrage zu aktivieren oder zu deaktivieren. Durch Deaktivieren dieser Abfrage wird die Leistung des Management Service und der ADC-Instanzen verbessert.

So aktivieren oder deaktivieren Sie Funktionen mit der GUI

1. Navigieren Sie zu **System > Systemeinstellungen**.
2. Klicken Sie auf **Funktionen konfigurieren**.
3. Wählen Sie eine Funktion und klicken Sie auf **Aktivieren** oder **Deaktivieren**.

Konfigurieren des Management Service

November 23, 2023

Mit dem Management Service können Sie Clientsitzungen verwalten und Konfigurationsaufgaben ausführen, z. B. das Erstellen und Verwalten von Benutzerkonten und das Optimieren von Backup- und Beschneidungsrichtlinien gemäß Ihren Anforderungen. Sie können den Management Service auch neu starten und die Version des Management Service aktualisieren. Sie können weiterhin TAR-Dateien des Management Service und des Citrix Hypervisor erstellen und an den technischen Support senden.

Verwalten von Clientsitzungen

Eine Clientsitzung wird erstellt, wenn sich ein Benutzer beim Management Service anmeldet. Sie können alle Clientsitzungen auf der Appliance im Bereich **Sitzungen** anzeigen.

Im Bereich **Sessions** können Sie die folgenden Details anzeigen:

- **Benutzername:** Das Benutzerkonto, das für die Sitzung verwendet wird.
- **IP-Adresse:** Die IP-Adresse des Clients, von dem aus die Sitzung erstellt wurde.
- **Port:** Der für die Sitzung verwendete Port.
- **Anmeldezeit:** Die Uhrzeit, zu der die aktuelle Sitzung auf der SDX-Appliance erstellt wurde.
- **Zeit der letzten Aktivität:** Der Zeitpunkt, zu dem Benutzeraktivitäten zuletzt in der Sitzung erkannt wurden.
- **Sitzung läuft ab in: Verbleibende** Zeit für den Ablauf der Sitzung.

Um Clientsitzungen anzuzeigen, navigieren Sie auf der Registerkarte **Konfiguration** zu **System > Sitzungen**.

Um eine Clientsitzung zu beenden, klicken Sie im Bereich **Sitzungen** auf die Sitzung, die Sie entfernen möchten, und klicken Sie dann auf **Sitzung beenden**.

Sie können eine Sitzung nicht von dem Client aus beenden, der diese Sitzung initiiert hat.

Richtlinien konfigurieren

Um die Größe der protokollierten Daten innerhalb der verwaltbaren Grenzen zu halten, führt die SDX-Appliance zu einem bestimmten Zeitpunkt Backup- und Datenbeschneidungsrichtlinien automatisch aus.

Die Richtlinie zum Beschneiden wird täglich um 00:00 Uhr ausgeführt und gibt die Anzahl der Tage an, an denen Daten auf der Appliance aufbewahrt werden sollen. Standardmäßig beschneidet die Appliance Daten, die älter als 3 Tage sind, aber Sie können die Anzahl der Tage an Daten angeben, die Sie behalten möchten. Nur Ereignisprotokolle, Überwachungsprotokolle und Aufgabenprotokolle werden beschnitten.

Die Backuprichtlinie wird täglich um 00:30 Uhr ausgeführt und erstellt eine Backup der Protokolle und Konfigurationsdateien. Standardmäßig behält die Richtlinie drei Backups bei, Sie können jedoch die Anzahl der Backups angeben, die Sie behalten möchten. Mit der Backup-Richtlinie können Sie Folgendes:

- Backupdateien verschlüsseln.
- Konfigurieren Sie die SDX-Appliance so, dass die Backupdateien über FTP, SFTP und SCP auf einen externen Backupserver übertragen werden.

So geben Sie die Anzahl der Tage an, für die protokollierte Daten beschnitten werden:

1. Klicken Sie auf der Registerkarte **Konfiguration** im Navigationsbereich auf **System**.
2. Klicken Sie im Bereich **System** unter **Richtlinienverwaltung**auf **Richtlinie bereinigen**.
3. Geben Sie im Dialogfeld **Prune-Richtlinie ändern** unter **Zu speichernde Daten (Tage)**die Anzahl der Tage an Daten an, die die Appliance zu einem bestimmten Zeitpunkt aufbewahren muss.
4. Klicken Sie auf **OK**.

So konfigurieren Sie die Backuprichtlinie:

1. Klicken Sie auf der Registerkarte **Konfiguration** im Navigationsbereich auf **System**.
2. Klicken Sie im Bereich **System** unter **Richtlinienverwaltung**auf **Backuprichtlinie**.
3. Geben **Sie im Dialogfeld Backuprichtlinie ändern** in **Vorherige zu bewahrende Sicherungen** die Anzahl der Sicherungen an, die die Appliance zu einem bestimmten Zeitpunkt aufbewahren muss.
4. Wählen Sie **Backupdatei verschlüsseln** aus, um die Backupdatei zu verschlüsseln.
5. Wählen Sie **Externe Übertragung** und gehen Sie wie folgt vor, um die Backupdatei auf einen externen Sicherungsserver zu übertragen:

    a) Geben Sie im Feld **Server** den Host-Namen oder die IP-Adresse des externen Backupservers ein.
    b) Geben Sie in den Feldern **Benutzername** und **Kennwort** den Benutzernamen und das Kennwort für den Zugriff auf den externen Backupserver ein.
    c) Geben Sie im Feld **Port** die Portnummer ein.
    d) Wählen Sie im Feld **Übertragungsprotokoll** das Protokoll aus, das Sie verwenden möchten, um die Backupdatei auf den externen Sicherungsserver zu übertragen.
    e) Geben Sie im Feld **Verzeichnispfad** den Pfad des Verzeichnisses auf dem externen Sicherungsserver ein, in dem Sie die Backupdateien speichern möchten.

6. **Datei nach der Übertragung aus dem Management Service löschen:** Wählen Sie aus, ob Sie die Backupdatei von der SDX-Appliance löschen möchten, nachdem Sie die Backupdatei auf den externen Sicherungsserver übertragen haben.
7. Klicken Sie auf **OK**.

Starten Sie den Management Service neu

Sie können den Management Service im **Systembereich** neu starten. Ein Neustart des Management Service wirkt sich nicht auf die Arbeit der Instanzen aus. Die Instanzen funktionieren während des Neustarts des Management Service weiter.

So starten Sie den Management Service neu:

1. Klicken Sie auf der Registerkarte **Konfiguration** im Navigationsbereich auf **System**.

2. Klicken Sie im Bereich **System** unter **Systemadministration**auf **Management Service neu starten**.

Entfernen Sie Management Service-Dateien

Sie können alle nicht benötigten Management Service-Build- und Dokumentationsdateien von der SDX-Appliance entfernen.

So entfernen Sie eine Management Service-Datei:

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **Management Service**, und klicken Sie dann auf die Datei, die Sie entfernen möchten.
2. Wählen Sie im **Detailbereich** den Dateinamen aus, und klicken Sie dann auf **Löschen**.

Generieren Sie ein Tar-Archiv für technischen Support

Sie können die Option Technischer Support verwenden, um ein Tar-Archiv mit Daten und Statistiken zu erstellen, das an den technischen Support von Citrix gesendet werden kann. Dieser Teer kann für den Management Service oder den Citrix Hypervisor oder für beide gleichzeitig generiert werden. Sie können die Datei dann auf Ihr lokales System herunterladen und an den technischen Support von Citrix senden.

Im Bereich **Technischer Support** können Sie die folgenden Details anzeigen.

- **Name:** Der Name der Tar-Archivdatei. Der Dateiname gibt an, ob das Teer für den Management Service oder den Citrix Hypervisor-Server bestimmt ist.
- **Letzte Änderung:** Das Datum, an dem diese Datei zuletzt geändert wurde.
- **Größe:** Die Größe der TAR-Datei.

So generieren Sie das Tar-Archiv für den technischen Support:

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Diagnose > Technischer Support**.
2. Wählen Sie im **Detailbereich** in der Liste **Aktion** die Option **Datei für technischen Support generieren**aus.
3. Wählen **Sie im Dialogfeld Datei für technischen Support generieren** in der Liste **Modus** die entsprechende Option aus.
4. Klicken Sie auf **OK**.

So laden Sie das Tar-Archiv für technischen Support herunter:

1. Wählen Sie im Bereich **Technischer Support** die Datei des technischen Supports aus, die Sie herunterladen möchten.
2. Wählen Sie in der Liste **Aktion** die Option **Herunterladen**aus. Die Datei wird auf Ihrem lokalen Computer gespeichert.

CLI-Unterstützung für Management Service

Sie können jetzt die CLI verwenden, um Vorgänge im Management Service durchzuführen. Die folgenden Vorgänge werden unterstützt:

- Hinzufügen, Festlegen, Löschen —Zum Konfigurieren der Ressourcen.
- Tun —Zum Ausführen von Vorgängen auf Systemebene. Zum Beispiel Upgrade oder Shutdown des Management Service oder Neustart.
- Speichern —Zum Hinzufügen von Schnittstellen, die für die Bereitstellung verwendet werden.

Um auf die CLI zuzugreifen, starten Sie den Secure Shell (SSH) -Client von jeder Arbeitsstation aus, die mit der IP-Adresse des Management Service verbunden ist. Melden Sie sich mit den Administratoranmeldeinformationen an.

In den Manpages können Sie auf detaillierte Informationen zur Befehlsverwendung und -syntax zugreifen.

Hinweis: CLI wird nicht über den Konsolenzugriff unterstützt.

Konfigurieren der Authentifizierungs- und Autor

November 23, 2023

Die Authentifizierung mit dem NetScaler SDX Management Service kann lokal oder extern erfolgen. Bei der externen Authentifizierung gewährt der Management Service Benutzerzugriff basierend auf der Antwort eines externen Servers. Der Management Service unterstützt die folgenden externen Authentifizierungsprotokolle:

- DFÜ-Benutzerdienst für Remote-Authentifizierung (RADIUS)
- Zugangskontrollsystem für die Terminalzugriffskontrolle (TACACS)
- Lightweight Directory Access Protocol (LDAP)

Der Management Service unterstützt auch Authentifizierungsanfragen von SSH. Die SSH-Authentifizierung unterstützt nur Anfragen zur interaktiven Authentifizierung über die Tastatur. Die Autorisierung von SSH-Benutzern ist nur auf Administratorrechte beschränkt. Benutzer mit Nur-Lese-Rechten können sich nicht über SSH anmelden.

Um die Authentifizierung zu konfigurieren, geben Sie den Authentifizierungstyp an und konfigurieren Sie einen Authentifizierungsserver.

Die Autorisierung durch den Management Service ist lokal. Der Management Service unterstützt zwei Berechtigungsebenen. Benutzer mit Administratorrechten können jede Aktion im Management Service ausführen. Benutzer mit Nur-Lese-Rechten dürfen nur Lesevorgänge ausführen.

Die Autorisierung von SSH-Benutzern ist nur auf Administratorrechte beschränkt. Benutzer mit Nur-Lese-Rechten können sich nicht über SSH anmelden.

Die Autorisierung für RADIUS und LDAP wird durch Gruppen-Extraktion unterstützt. Sie können die Gruppenextraktionsattribute während der Konfiguration von RADIUS- oder LDAP-Servern im Management Service festlegen. Der extrahierte Gruppenname wird mit den Gruppennamen im Management Service abgeglichen, um die dem Benutzer erteilten Berechtigungen zu ermitteln. Ein Benutzer kann mehreren Gruppen angehören. In diesem Fall verfügt der Benutzer über Administratorrechte, wenn eine Gruppe, zu der der Benutzer gehört, über Administratorrechte verfügt. Während der Konfiguration kann ein Standardauthentifizierungsgruppenattribut festgelegt werden. Diese Gruppe wird zusammen mit den extrahierten Gruppen für die Autorisierung berücksichtigt.

Bei der TACACS-Autorisierung muss der TACACS-Serveradministrator einen speziellen Befehl admin für einen Benutzer mit Administratorrechten zulassen und diesen Befehl Benutzern mit Nur-Lese-Rechten verweigern. Wenn sich ein Benutzer bei einer SDX-Appliance anmeldet, prüft der Management Service, ob der Benutzer über die Berechtigung zum Ausführen dieses Befehls verfügt. Wenn der Benutzer über Berechtigungen verfügt, werden dem Benutzer die Administratorrechte zugewiesen, andernfalls werden dem Benutzer nur Leseberechtigungen zugewiesen.

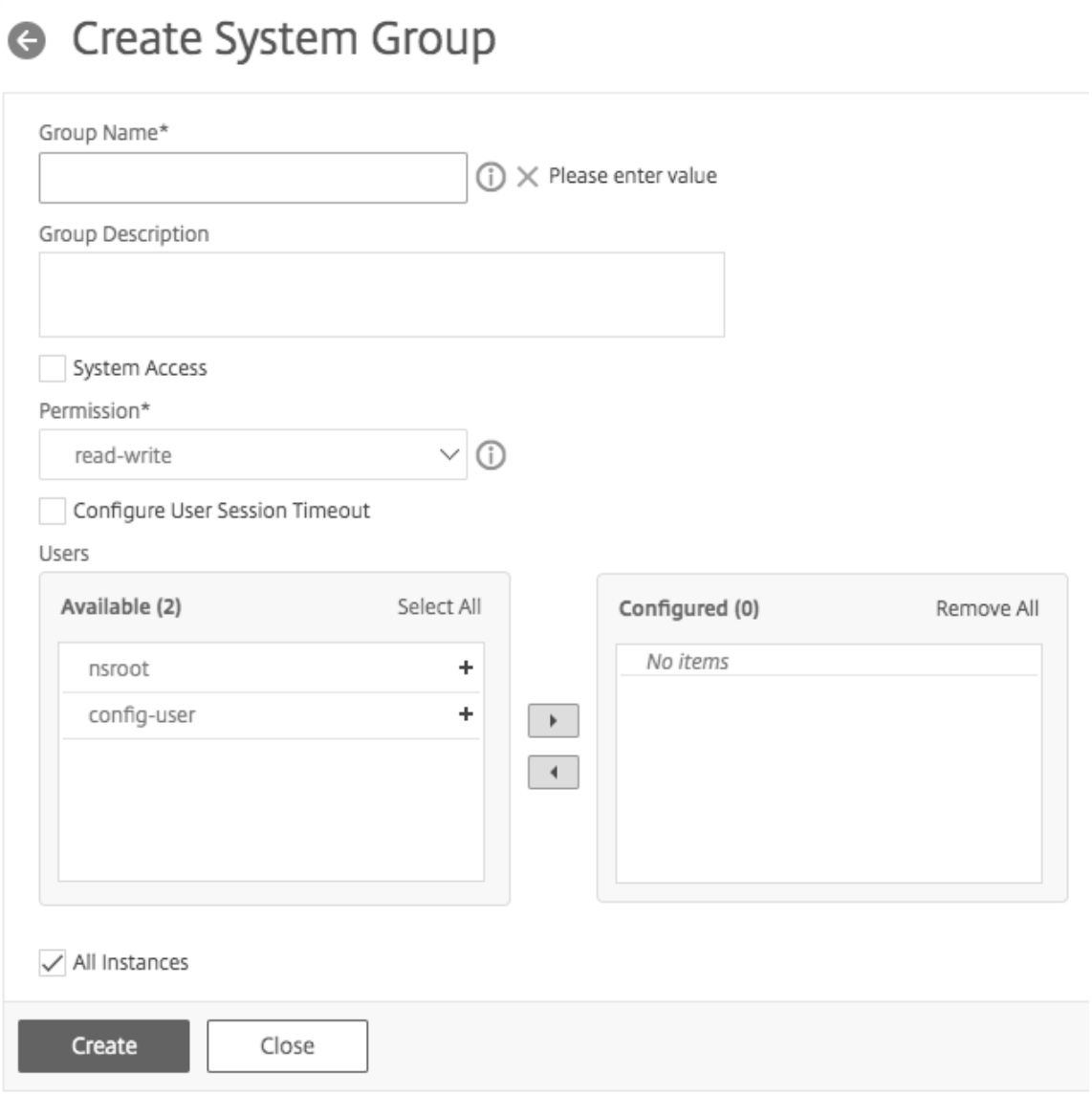
Eine Benutzergruppe hinzufügen

Gruppen sind logische Gruppen von Benutzern, die auf allgemeine Informationen zugreifen oder ähnliche Aufgaben ausführen müssen. Sie können Benutzer in Gruppen einteilen, die durch eine Reihe allgemeiner Vorgänge definiert sind. Indem Sie bestimmte Berechtigungen für Gruppen und nicht für einzelne Benutzer bereitstellen, können Sie beim Erstellen von Benutzern Zeit sparen.

Wenn Sie externe Authentifizierungsserver für die Authentifizierung verwenden, können Gruppen in SDX so konfiguriert werden, dass sie mit Gruppen übereinstimmen, die auf Authentifizierungsservern konfiguriert sind. Wenn sich ein Benutzer, der zu einer Gruppe gehört, deren Name mit einer Gruppe auf einem Authentifizierungsserver übereinstimmt, anmeldet und authentifiziert wird, erbt der Benutzer die Einstellungen für die Gruppe.

So fügen Sie eine Benutzergruppe hinzu

1. Erweitern Sie auf der Registerkarte **Konfiguration** unter **System**den Knoten **Benutzerverwaltung**, und klicken Sie dann auf **Gruppen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.



3. Stellen Sie auf der Seite **Systemgruppe erstellen** die folgenden Parameter ein:

   - Name der Gruppe
   - Beschreibung der Gruppe
   - Systemzugriff: Wählen Sie dieses Feld aus, um Zugriff auf die gesamte SDX-Appliance und die darauf ausgeführten Instanzen zu gewähren. Geben Sie alternativ für den Zugriff auf Instanzebene die Instanzen unter **Instanzen**an.
   - Berechtigung
   - Konfigurieren des Zeitlimits für Benutzersitzung
   - Benutzer: Datenbankbenutzer, die zur Gruppe gehören. Wählen Sie die Benutzer aus, die Sie der Gruppe hinzufügen möchten.

4. Klicken Sie auf **Erstellen** und **Schließen**.

Hinweis: Um eine Gruppe mit Administratorrolle auf einer SDX-Appliance zu erstellen, die von Version 10.5 auf Version 11.1 aktualisiert wurde, aktivieren Sie die Berechtigung "Lese- und Schreibzugriff" und das Kontrollkästchen "Systemzugriff". In SDX 10.5 ist dieses Kontrollkästchen nicht verfügbar und die Werte für Permission sind "admin"und "schreibgeschützt".

Konfigurieren von Benutzerkonten

Ein Benutzer meldet sich bei der SDX-Appliance an, um Appliance-Verwaltungsaufgaben durchzuführen. Um einem Benutzer den Zugriff auf die Appliance zu ermöglichen, müssen Sie ein Benutzerkonto auf der SDX-Appliance für diesen Benutzer erstellen. Benutzer werden lokal auf der Appliance authentifiziert.

Wichtig: Das Kennwort gilt für die
SDX-Appliance, den Management Service und den Citrix Hypervisor. Ändern Sie das Kennwort nicht direkt auf dem Citrix Hypervisor.

Konfigurieren eines Benutzerkontos

1. Erweitern Sie auf der Registerkarte **Konfiguration** unter **System**den Knoten **Verwaltung**, und klicken Sie dann auf **Benutzer**. Im Bereich Benutzer wird eine Liste der vorhandenen Benutzerkonten mit ihren Berechtigungen angezeigt.
2. Führen Sie im Bereich **Benutzer** eine der folgenden Aktionen aus:
   - Um ein Benutzerkonto zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um ein Benutzerkonto zu ändern, wählen Sie den Benutzer aus, und klicken Sie dann auf **Ändern**.
3. Stellen **Sie im Dialogfeld "Systembenutzer erstellen** "oder "**Systembenutzer ändern** "die folgenden Parameter ein:
   - Name* —Der Benutzername des Kontos. Die folgenden Zeichen sind im Namen zulässig: Buchstaben a bis z und A bis Z, Zahlen 0 bis 9, Punkt (.), Leerzeichen und Unterstrich (_). Maximale Länge: 128 Der Name kann nicht geändert werden.
   - Kennwort* —Das Kennwort für die Anmeldung an der Appliance. Maximale Länge: 128
   - Kennwort bestätigen* —Das Kennwort.
   - Berechtigung* —Die Berechtigungen des Benutzers auf der Appliance. Mögliche Werte:
     - admin —Der Benutzer kann alle Verwaltungsaufgaben im Zusammenhang mit dem Management Service ausführen.
     - Schreibgeschützt —Der Benutzer kann nur das System überwachen und das Kennwort des Kontos ändern.
       Standardeinstellung: admin.

- Externe Authentifizierung aktivieren —Ermöglicht die externe Authentifizierung für diesen Benutzer. Der Management Service versucht vor der Datenbankbenutzerauthentifizierung eine externe Authentifizierung. Wenn dieser Parameter deaktiviert ist, ist der Benutzer nicht beim externen Authentifizierungsserver authentifiziert.
  Hinweis: Wenn der Remote-Authentifizierungsserver nicht erreichbar ist, verliert der Benutzer möglicherweise den Zugriff auf die Appliance. In solchen Fällen greift die Authentifizierung auf den standardmäßigen Admin-Benutzer (`nsroot`) zurück.
- Sitzungstimeout konfigurieren —Ermöglicht Ihnen, den Zeitraum zu konfigurieren, wie lange ein Benutzer aktiv bleiben kann. Geben Sie die folgenden Details an:
  - Sitzungs-Timeout —Der Zeitraum, in dem eine Benutzersitzung aktiv bleiben kann.
  - Einheit für Sitzungs-Timeout —Die Zeitüberschreitungseinheit in Minuten oder Stunden.
- Gruppen —Weisen Sie die Gruppen dem Benutzer zu.

* Ein erforderlicher Parameter

4. Klicken Sie auf Erstellen oder OK und dann auf Schließen. Der Benutzer, den Sie erstellt haben, wird im Bereich Benutzer aufgeführt.

So entfernen Sie ein Benutzerkonto

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **System**, erweitern Sie **Administration**, und klicken Sie dann auf **Benutzer**.
2. Wählen Sie im Bereich **Benutzer** das Benutzerkonto aus, und klicken Sie dann auf **Löschen**.
3. Klicken Sie im Feld Meldung bestätigen auf **OK**.

Den Authentifizierungstyp festlegen

Über die Management Service-Schnittstelle können Sie die lokale oder externe Authentifizierung angeben. Die externe Authentifizierung ist für lokale Benutzer standardmäßig deaktiviert. Sie kann aktiviert werden, indem Sie die Option Externe Authentifizierung
aktivieren aktivieren, wenn Sie den lokalen Benutzer hinzufügen oder die Einstellungen für den Benutzer ändern.

Wichtig: Externe Authentifizierung wird erst unterstützt, nachdem Sie einen RADIUS-, LDAP- oder TACACS-Authentifizierungsserver eingerichtet haben.

Festlegen des Authentifizierungstyps

1. Klicken Sie auf der Registerkarte Konfiguration unter System auf Authentifizierung.

2. Klicken Sie im Detailbereich auf Authentication Configuration.
3. Legen Sie die folgenden Parameter fest:
    - Servertyp —Typ des für die Benutzerauthentifizierung konfigurierten Authentifizierungsservers. Mögliche Werte: LDAP, RADIUS, TACACS und Local.
    - Servername —Name des im Management Service konfigurierten Authentifizierungsservers. Das Menü listet alle Server auf, die für den ausgewählten Authentifizierungstyp konfiguriert sind.
    - Lokale Fallback-Authentifizierung aktivieren —Alternativ können Sie einen Benutzer mit der lokalen Authentifizierung authentifizieren, wenn die externe Authentifizierung fehlschlägt. Diese Option ist standardmäßig aktiviert.
4. Klicken Sie auf OK.

Standardauthentifizierung aktivieren oder deaktivieren

Sie können sich mit der Standardauthentifizierung bei der NITRO-Schnittstelle des Management Service authentifizieren. Standardmäßig ist die Standardauthentifizierung in der SDX-Appliance aktiviert. Führen Sie Folgendes aus, um die Standardauthentifizierung mithilfe der Management Service-Schnittstelle zu deaktivieren

Deaktivieren der Basisauthentifizierung

1. Klicken Sie auf der Registerkarte **Konfiguration** auf **System**.
2. Klicken Sie in der Gruppe **Systemeinstellungen** auf **Systemeinstellungen ändern**.
3. Deaktivieren Sie im Dialogfeld “Systemeinstellungen konfigurieren”das Kontrollkästchen **Standardauthentifizierung zulassen** .
4. Klicken Sie auf **OK**.

Konfigurieren des externen Authentifizierungsservers

November 23, 2023

Der NetScaler SDX Management Service kann Benutzer mit lokalen Benutzerkonten oder mithilfe eines externen Authentifizierungsservers authentifizieren. Die Appliance unterstützt die folgenden Authentifizierungstypen:

- Lokal —Authentifiziert sich beim Management Service mithilfe eines Kennworts ohne Bezug zu einem externen Authentifizierungsserver. Benutzerdaten werden lokal im Management Service gespeichert.

- RADIUS —Authentifiziert sich bei einem externen RADIUS-Authentifizierungsserver.
- LDAP —Authentifiziert sich bei einem externen LDAP-Authentifizierungsserver.
- TACACS —Authentifiziert sich bei einem externen Terminal Access Controller Access Control System (TACACS) -Authentifizierungsserver.

Um eine externe Authentifizierung zu konfigurieren, geben Sie den Authentifizierungstyp an und konfigurieren Sie einen Authentifizierungsserver.

Hinzufügen eines RADIUS-Servers

Um die RADIUS-Authentifizierung zu konfigurieren, geben Sie den Authentifizierungstyp als RADIUS an und konfigurieren den RADIUS-Authentifizierungsserver

Der Management Service unterstützt die Authentifizierung von RADIUS-Challenge-Response gemäß den RADIUS RADIUS-Benutzer können mit einem Einmalkennwort auf dem RADIUS-Server konfiguriert werden. Wenn sich der Benutzer bei einer SDX-Appliance anmeldet, wird der Benutzer aufgefordert, dieses Einmalkennwort anzugeben.

So fügen Sie einen RADIUS-Server hinzu

1. Erweitern Sie auf der Registerkarte **Konfiguration** unter **System**den Knoten **Authentifizierung**, und klicken Sie dann auf **Radius**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Radius-Server erstellen** die Werte für die Parameter ein oder wählen Sie sie aus:

    - Name* —Name des Servers.
    - Servername/IP-Adresse* —Vollqualifizierter Domänenname (FQDN) oder Server-IP-Adresse.

      Hinweis: DNS muss in der Lage sein, den angegebenen FQDN in eine IP-Adresse aufzulösen, und nur das primäre DNS wird verwendet, um den FQDN aufzulösen. Informationen zum manuellen Festlegen des primären DNS finden Sie im Abschnitt “Hinzufügen eines primären DNS für die FQDN-Namensauflösung”.
    - **Port*** —Port, auf dem der RADIUS-Server läuft. Standardwert: 1812.
    - Timeout* —Anzahl der Sekunden, die das System auf eine Antwort vom RADIUS-Server wartet. Standardwert: 3.
    - Geheimer Schlüssel* —Schlüssel, der zwischen dem Client und dem Server gemeinsam genutzt wird. Diese Informationen sind für die Kommunikation zwischen dem System und dem RADIUS-Server erforderlich.

- NAS-IP-Adressextraktion aktivieren —Wenn diese Option aktiviert ist, wird die IP-Adresse des Management Service gemäß dem RADIUS-Protokoll als `nasip` an den Server gesendet.
- NASID —Falls konfiguriert, wird diese Zeichenfolge gemäß dem RADIUS-Protokoll als `nasid` an den RADIUS-Server gesendet.
- Gruppenpräfix —Präfix-Zeichenfolge, die den Gruppennamen innerhalb eines RADIUS-Attributs für die RADIUS-Gruppen-Extraktion
- Gruppenhersteller-ID —Hersteller-ID für die Verwendung der RADIUS-Gruppen-Extraktion.
- Gruppenattributtyp —Attributtyp für die RADIUS-Gruppen-Extraktion.
- Gruppentrennzeichen —Gruppentrennzeichenfolge, die Gruppennamen innerhalb eines RADIUS-Attributs für die RADIUS-Gruppen-Extraktion
- IP Address Vendor Identifier —Hersteller-ID des Attributs im RADIUS, das die Intranet-IP angibt. Ein Wert von 0 bedeutet, dass das Attribut nicht vom Hersteller kodiert ist.
- IP-Adressattributtyp —Attributtyp des Remote-IP-Adressattributs in einer RADIUS-Antwort.
- Kennwort-Lieferantenkennung —Lieferanten-ID des Kennworts in der RADIUS-Antwort. Wird verwendet, um das Benutzerkennwort zu extrahieren.
- Kennwort-Attributtyp —Attributtyp des Kennwort-Attributs in einer RADIUS-Antwort.
- Kennwortcodierung —Wie Kennwörter in den RADIUS-Paketen codiert werden müssen, die vom System zum RADIUS-Server übertragen werden. Mögliche Werte: pap, chap, mschapv1 und mschapv2.
- Standardauthentifizierungsgruppe —Standardgruppe, die ausgewählt wird, wenn die Authentifizierung erfolgreich ist, zusätzlich zu den extrahierten Gruppen.
- Buchhaltung —Ermöglichen Sie Management Service, Überwachungsinformationen mit dem RADIUS-Server zu protokollieren.

4. Klicken Sie auf Erstellen, und klicken Sie dann auf Schließen.

Hinzufügen eines LDAP-Authentifizierungsservers

Um die LDAP-Authentifizierung zu konfigurieren, geben Sie den Authentifizierungstyp als LDAP an und konfigurieren den LDAP-Authentifizierungsserver.

So fügen Sie einen LDAP-Server hinzu

1. Erweitern Sie auf der Registerkarte **Konfiguration** unter **System**den Knoten **Authentifizierung**, und klicken Sie dann auf **LDAP**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.

3. Geben Sie im Dialog LDAP-Server erstellen die Werte für die Parameter ein oder wählen Sie sie aus:

   - Name* —Name des Servers.
   - Servername/IP-Adresse* —FQDN oder Server-IP-Adresse.
     Hinweis: DNS muss in der Lage sein, den angegebenen FQDN in eine IP-Adresse aufzulösen, und nur das primäre DNS wird verwendet, um den FQDN aufzulösen.Informationen zum manuellen Festlegen des primären DNS finden Sie im Abschnitt "Hinzufügen eines primären DNS für die FQDN-Namensauflösung".
   - **Port*** —Port, auf dem der LDAP-Server läuft. Standardwert: 389.
   - Timeout* —Anzahl der Sekunden, die das System auf eine Antwort vom LDAP-Server wartet.
   - Basis-DN —Base oder Knoten, an dem die LDAP-Suche beginnen muss.
   - Typ —Typ des LDAP-Servers. Mögliche Werte: Active Directory (AD) und Novell Directory Service (NDS).
   - Administrativer Bind-DN —Vollständiger definierter Name, der für die Bindung an den LDAP-Server verwendet wird.
   - Administratives Kennwort —Kennwort, das für die Bindung an den LDAP-Server verwendet wird.
   - LDAP-Zertifikat validieren —Wählen Sie diese Option, um das vom LDAP-Server empfangene Zertifikat zu überprüfen.
   - LDAP-Hostname —Hostname für den LDAP-Server. Wenn der validateServerCert-Parameter aktiviert ist, gibt dieser Parameter den Hostnamen auf dem Zertifikat vom LDAP-Server an. Eine Nichtübereinstimmung des Hostnamens führt zu einem Verbindungsfehler.
   - Serveranmeldenamen-Attribut —Namensattribut, das vom System zur Abfrage des externen LDAP-Servers oder eines Active Directory verwendet wird.
   - Suchfilter —Zeichenfolge, die mit der standardmäßigen LDAP-Benutzersuchzeichenfolge kombiniert werden soll, um den Wert zu bilden. Zum Beispiel würde vpnallowed=true mit ldaploginame `samaccount` und dem vom Benutzer angegebenen Benutzernamen bob eine LDAP-Suchzeichenfolge mit folgendem Wert ergeben: (& (vpnallowed=true) (samaccount=bob).
   - Gruppenattribut —Attributname für die Gruppen-Extraktion vom LDAP-Server.
   - Subattributname —Name des Unterattributs für die Gruppen-Extraktion vom LDAP-Server.
   - Sicherheitstyp —Verschlüsselungsart für die Kommunikation zwischen der Appliance und dem Authentifizierungsserver. Mögliche Werte:

PLAINTEXT: Keine Verschlüsselung erforderlich.

TLS: Kommunizieren Sie mit dem TLS-Protokoll.

SSL: Kommunizieren mit SSL-Protokoll

- Standardauthentifizierungsgruppe —Standardgruppe, die ausgewählt wird, wenn die Authentifizierung erfolgreich ist, zusätzlich zu den extrahierten Gruppen.
- Verweise: Aktiviert das Verfolgen von LDAP-Verweisen, die vom LDAP-Server empfangen wurden.
- Maximale LDAP-Verweise —Maximale Anzahl an zu befolgenden LDAP-Verweisen.
- Kennwort ändern aktivieren —Erlaubt dem Benutzer, das Kennwort zu ändern, wenn das Kennwort abläuft. Sie können das Kennwort nur ändern, wenn der konfigurierte Sicherheitstyp TLS oder SSL ist.
- Extraktion verschachtelter Gruppen aktivieren —Extraktionsfunktion für verschachtelte Gruppen aktivieren.
- Maximale Verschachtelungsebene —Anzahl der Ebenen, auf denen die Gruppenextraktion zulässig ist.
- Gruppennamen-Identifier —Name, der eine Gruppe im LDAP-Server eindeutig identifiziert.
- Gruppensuchattribut —LDAP-Gruppensuchattribut. Wird verwendet, um zu bestimmen, zu welchen Gruppen eine Gruppe gehört.
- Unterattribut für Gruppensuche —Unterattribut für die LDAP-Gruppensuche Wird verwendet, um zu bestimmen, zu welchen Gruppen eine Gruppe gehört.
- Gruppensuchfilter —Zeichenfolge, die mit der standardmäßigen LDAP-Gruppensuchzeichenfolge kombiniert werden soll, um den Suchwert zu bilden.

4. Klicken Sie auf Erstellenund dann auf Schließen.

SSH-Authentifizierungsunterstützung für öffentliche Schlüssel für LDAP-Benutzer

Die SDX-Appliance kann jetzt die LDAP-Benutzer über die SSH-Authentifizierung mit öffentlichem Schlüssel für die Anmeldung authentifizieren. Die Liste der öffentlichen Schlüssel wird auf dem Benutzerobjekt im LDAP-Server gespeichert. Während der Authentifizierung extrahiert SSH die öffentlichen SSH-Schlüssel vom LDAP-Server. Die Anmeldung ist erfolgreich, wenn einer der abgerufenen öffentlichen Schlüssel SSH unterstützt.

Derselbe Attributname des extrahierten öffentlichen Schlüssels muss sowohl auf dem LDAP-Server als auch in der NetScaler SDX-Appliance vorhanden sein.

> **Wichtig**
>
> Für die schlüsselbasierte Authentifizierung müssen Sie einen Speicherort für die öffentlichen Schlüssel angeben, indem Sie den Wert von `Authorizedkeysfile` in der Datei `/etc/sshd_config` im folgenden Aspekt festlegen:
>
> `AuthorizedKeysFile .ssh/authorized_keys`

Systembenutzer. Sie können den Speicherort von öffentlichen Schlüsseln für jeden Systembenutzer angeben, indem Sie den Wert von `Authorizedkeysfile` in der Datei `/etc/sshd_config`*‘ festlegen.

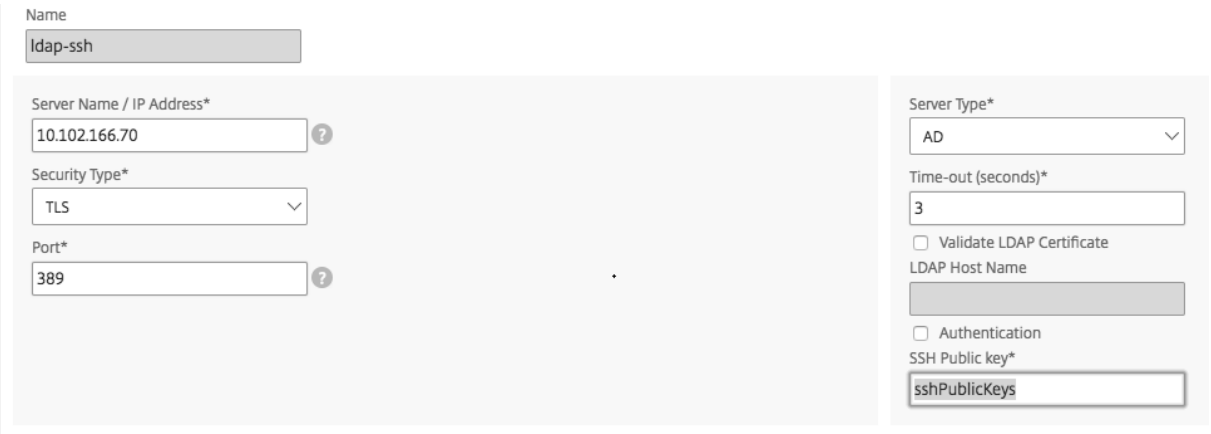
LDAP-Benutzer. Der abgerufene öffentliche Schlüssel wird im Verzeichnis `/var/pubkey/<user_name>/tmp_authorized_keys-<pid>` gespeichert. `pid` ist die eindeutige Nummer, die hinzugefügt wurde, um zwischen gleichzeitigen SSH-Anfragen desselben Benutzers zu unterscheiden. Dieser Ort ist ein temporärer Ort, an dem der öffentliche Schlüssel während des Authentifizierungsvorgangs gespeichert wird. Der öffentliche Schlüssel wird nach Abschluss der Authentifizierung aus dem System entfernt.

Um sich mit dem Benutzer anzumelden, führen Sie den folgenden Befehl an der Shell-Eingabeaufforderung aus:

```
$ ssh –i <private key> <username>@<IPAddress>
```

So konfigurieren Sie den LDAP-Server mit der GUI:

1. Navigieren Sie zu **System > Authentifizierung > LDAP**.
2. Klicken Sie auf der LDAP-Seite auf die Registerkarte ****Server**** .
3. Klicken Sie auf einen der verfügbaren LDAP-Server.
4. Wählen Sie auf der Seite **LDAP-Server für Authentifizierung konfigurieren** die Option **Authentifizierung**aus.



> **Hinweis:**
>
> Deaktivieren Sie das Kontrollkästchen Authentifizierung, um „sshPublicKeys“für die Authentifizierung von LDAP-Benutzern zu verwenden.

Hinzufügen eines primären DNS für die FQDN-Namensauflösung

Wenn Sie einen RADIUS- oder LDAP-Server definieren, indem Sie den FQDN des Servers anstelle seiner IP-Adresse verwenden, legen Sie den primären DNS manuell fest, um den Servernamen aufzulösen. Sie können entweder die GUI oder die CLI verwenden.

Um das primäre DNS mithilfe der GUI festzulegen, gehen Sie zu **System > Netzwerkkonfiguration > DNS**.

Gehen Sie folgendermaßen vor, um das primäre DNS mithilfe der CLI festzulegen.

1. Öffnen Sie eine Secure Shell (SSH) -Konsole.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei der NetScaler SDX-Appliance an.
3. Führen Sie den Befehl `networkconfig` aus.
4. Wählen Sie das entsprechende Menü aus, aktualisieren Sie die DNS-IPv4-Adresse und speichern Sie die Änderungen.

Wenn Sie den Befehl `networkconfig` neu ausführen, wird die aktualisierte DNS-Adresse angezeigt.

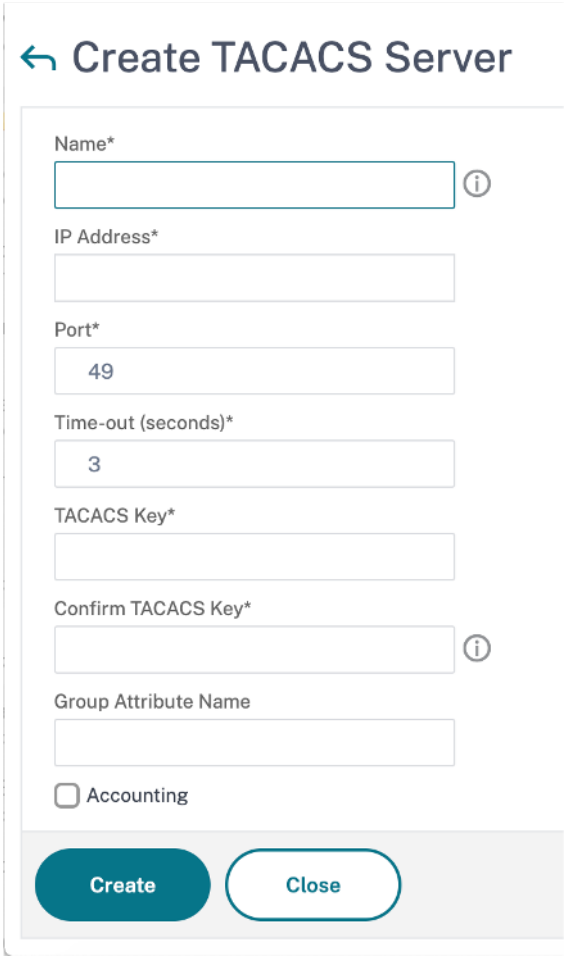
Hinzufügen eines TACACS-Servers

Um die TACACS-Authentifizierung zu konfigurieren, geben Sie den Authentifizierungstyp als TACACS an und konfigurieren Sie den TACACS-Authentifizierungsserver.

So fügen Sie einen TACACS-Server hinzu

1. Erweitern Sie auf der Registerkarte **Konfiguration** unter **System**die Option **Authentifizierung**, und klicken Sie dann auf **TACACS**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Dialog TACACS-Server erstellen die Werte für die Parameter ein oder wählen Sie sie aus:
    - Name —Name des TACAS-Servers
    - IP-Adresse —Die IP-Adresse des TACACS-Servers

- Port —Port, auf dem der TACACS-Server läuft. Standardwert: 49
- Timeout —Maximale Anzahl von Sekunden, die das System auf eine Antwort vom TACACS-Server wartet
- TACACS-Schlüssel —Schlüssel, der zwischen dem Client und dem Server gemeinsam genutzt wird. Diese Informationen sind erforderlich, damit das System mit dem TACACS-Server kommunizieren kann.
- Buchhaltung —Ermöglicht Management Service, Überwachungsinformationen mit dem TACACAS-Server zu protokollieren
- Gruppenattributname —Name des im TACACS+-Server konfigurierten Gruppenattributs



4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Konfigurieren der Linkaggregation über den Management Service

November 23, 2023

Die Link-Aggregation kombiniert mehrere Ethernet-Verbindungen zu einer einzigen Hochgeschwindigkeitsverbindu
Die Konfiguration der Link-Aggregation erhöht die Kapazität und Verfügbarkeit des Kommunikationskanals zwischen der NetScaler SDX-Appliance und anderen angeschlossenen Geräten. Eine aggregierte Verbindung wird auch als "Kanal"bezeichnet.

Wenn eine Netzwerkschnittstelle an einen Kanal gebunden ist, haben die Kanalparameter Vorrang vor den Netzwerkschnittstellenparametern. (Das heißt, die Netzwerkschnittstellenparameter werden ignoriert.) Eine Netzwerkschnittstelle kann nur an einen Kanal gebunden werden.

Wenn eine Netzwerkschnittstelle an einen Kanal gebunden ist, löscht sie ihre VLAN-Konfiguration. Die Schnittstelle wird aus dem VLAN entfernt, zu dem sie ursprünglich gehörte, und zum Standard-VLAN hinzugefügt. Sie können den Kanal jedoch wieder an das alte oder an ein neues VLAN binden. Wenn Sie beispielsweise die Netzwerkschnittstellen 1/2 und 1/3 an ein VLAN mit der ID 2 (VLAN 2) binden und sie dann an Kanal LA/1 binden, werden die Netzwerkschnittstellen in das Standard-VLAN verschoben, aber Sie können den Kanal an VLAN 2 binden.

Hinweis:

- Eine Schnittstelle muss nur Teil eines Kanals sein.
- Für die Konfiguration eines Kanals sind mindestens zwei Schnittstellen erforderlich.
- Die Schnittstellen, die Teil eines Kanals sind, werden in der Ansicht „Netzwerkeinstellungen "nicht aufgeführt, wenn Sie eine NetScaler-Instanz hinzufügen oder ändern. Anstelle der Schnittstellen werden die Kanäle aufgeführt.

Wenn Sie einen Kanal mithilfe von drei Schnittstellen konfigurieren, die einer Instanz zugewiesen sind, und eine zweite Instanz einige dieser Schnittstellen verwendet, fährt der Management Service die zweite Instanz herunter, ändert die Netzwerkeinstellungen und startet die Instanz neu. Nehmen Sie zum Beispiel zwei Instanzen an, Instanz1 und Instanz2. Wenn diese Instanzen bereitgestellt werden, werden die Schnittstellen 10/1, 10/2 und 10/3 Instanz1 und die Schnittstellen 10/1 und 10/2 Instanz2 zugewiesen. Wenn ein LA-Kanal mit den Schnittstellen 10/1, 10/2 und 10/3 erstellt wird, wird Instanz1 nicht neu gestartet. Der Management Service fährt jedoch Instanz2 herunter, weist Instanz2 die Schnittstelle 10/3 zu und startet dann Instanz2 neu.

Wenn Sie eine Schnittstelle aus einem LA-Kanal entfernen, werden die Änderungen in der Datenbank gespeichert, und die Schnittstelle wird in der Ansicht Netzwerkeinstellungen angezeigt, wenn Sie eine Instanz hinzufügen oder ändern. Bevor Sie die Schnittstelle löschen, wird nur der Kanal aufgeführt, zu dem die Schnittstelle gehört.

Konfigurieren eines Kanals über den Management Service

November 23, 2023

Sie können einen Kanal manuell konfigurieren oder das Link Aggregation Control Protocol (LACP) verwenden. Sie können LACP nicht auf einen manuell konfigurierten Kanal anwenden, und Sie können auch keinen von LACP erstellten Kanal manuell konfigurieren. Konfigurieren Sie einen Kanal über den Management Service. Wählen Sie dann den Kanal zum Zeitpunkt der Bereitstellung oder Änderung einer NetScaler-Instanz aus.

Ein LA-Kanal ist eine logische Einheit für Link-Redundanz und Bandbreitenaggregation. Schnittstellen, die Teil eines Kanals sind, können keine separaten IP-Adressen zugewiesen werden.

Hinweis: Eine NetScaler SDX-Appliance unterstützt Link-Aggregation, unterstützt jedoch keine Link-Redundanz. Ab NetScaler Version 13.1 Build 27.x und höher wird die Link-Redundanzkonfiguration auf einer NetScaler VPX-Instanz, die auf einer NetScaler SDX-Appliance gehostet wird, explizit nicht unterstützt.

So konfigurieren Sie einen Kanal über den Management Service

1. Navigieren Sie zu **System > Kanäle**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen **Sie im Dialogfeld Kanal hinzufügen** die folgenden Parameter ein:

    - Kanal-ID —ID für den zu erstellenden LA-Kanal. Geben Sie einen LA-Kanal in LA/x-Notation an, wobei x von 1 bis zu einer Zahl reichen kann, die der halben Anzahl von Schnittstellen entspricht. Kann nicht geändert werden, nachdem der LA-Kanal erstellt wurde.
    - Typ —Typ des Kanals. Mögliche Werte:
        - Statisch —nur auf den Datenschnittstellen konfiguriert.
        - Aktiv-Aktiv —nur auf den Verwaltungsschnittstellen 0/x konfiguriert.
        - Aktiv-Passiv —nur auf den Verwaltungsschnittstellen 0/x konfiguriert.
        - LACP —konfiguriert auf Datenschnittstellen und Verwaltungsschnittstellen 0/x.
    - Durchsatz (gilt nur für einen statischen Kanal und LACP) —Niedriger Schwellenwert für den Durchsatz des LA-Kanals in Mbit/s. In einer HA-Konfiguration wird ein Failover ausgelöst, wenn für den LA-Kanal HA MON aktiviert ist und der Durchsatz unter dem angegebenen Schwellenwert liegt.
    - Bandwidth High (Gilt nur für einen statischen Kanal und LACP) —Hoher Schwellenwert für die Bandbreitennutzung des LA-Kanals in Mbit/s. Die Appliance generiert eine SNMP-Trap-Nachricht, wenn die Bandbreitennutzung des LA-Kanals gleich oder größer als der angegebene hohe Schwellenwert ist.
    - Bandbreite Normal (Gilt nur für einen statischen Kanal und LACP) —Normaler Schwellenwert für die Bandbreitennutzung des LA-Kanals in Mbit/s. Wenn die Bandbreitennutzung des LA-Kanals nach dem Überschreiten des hohen Schwellenwerts dem angegebenen normalen Schwellenwert entspricht oder diesen unterschreitet, generiert die NetScaler SDX-Appliance eine SNMP-Trap-Meldung, die angibt, dass sich die Bandbreitennutzung wieder

normalisiert hat.

4. Fügen Sie auf der Registerkarte **Interfaces** die Interfaces hinzu, die Sie in diesen Kanal aufnehmen möchten.
5. Stellen Sie auf der Registerkarte **Einstellungen** die folgenden Parameter ein:
    - Kanalzustand (gilt nur für einen statischen Kanal) —Aktiviert oder deaktiviert den LA-Kanal.
    - LACP-Zeit (gilt nur für LACP) —Zeit, nach der ein Link nicht aggregiert wird, wenn der Link keine LACPDU empfängt. Der Wert muss auf allen Ports übereinstimmen, die an der Link-Aggregation auf der SDX-Appliance und dem Partnerknoten teilnehmen.
    - HA-Überwachung —Überwachen Sie in einer Konfiguration mit hoher Verfügbarkeit (HA) den Kanal auf Ausfallereignisse. Der Ausfall eines LA-Kanals, bei dem HA MON aktiviert ist, löst ein HA-Failover aus.
    - Alle kennzeichnen: Fügen Sie jedem auf diesem Kanal gesendeten Paket ein Vier-Byte-802.1q-Tag hinzu. Die ON-Einstellung wendet Tags für alle VLANs an, die an diesen Kanal gebunden sind. OFF wendet das Tag für alle VLANs außer dem nativen VLAN an.
    - Aliasname —Aliasname für den LA-Kanal. Wird nur zur Verbesserung der Lesbarkeit verwendet. Um irgendwelche Operationen durchzuführen, müssen Sie die LA-Kanal-ID angeben.
6. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

> **Hinweise**
>
> - Sie können keine Verwaltungs-LA erstellen, wenn sowohl 0/1- als auch 0/2-Schnittstellen Teil einer VPX-Instanz sind und diese Instanz Teil eines Clusters ist.
> - Sie können eine Verwaltungs-LA nicht löschen, wenn sie Teil einer VPX-Instanz ist und diese Instanz Teil eines Clusters ist.

Zugriffssteuerungslisten

February 15, 2024

Eine Zugriffssteuerungsliste (ACL) ist eine Reihe von Bedingungen, die Sie auf eine Netzwerk-Appliance anwenden können, um IP-Verkehr zu filtern und Ihre Appliance vor unbefugtem Zugriff zu schützen.

Sie können eine ACL auf Ihrer NetScaler SDX Management Service-GUI konfigurieren, um den Zugriff auf die Appliance einzuschränken und zu kontrollieren.

> **Hinweis:**
>
> ACLs auf SDX-Appliances werden ab Version 12.0 57.19 unterstützt.

Dieses Artikel enthält die folgenden Abschnitte:

- Richtlinien für die Verwendung
- Wie konfiguriert man ACLs
- Andere Aktionen für ACL-Regeln
- Problembehandlung

Richtlinien für die Verwendung

Beachten Sie beim Erstellen von ACLs auf Ihrer Appliance die folgenden Punkte:

- Wenn Sie die SDX-Appliance auf Version 11.0 57.19 aktualisieren, ist die ACL-Funktion standardmäßig deaktiviert.
- SDX-Administratoren können nur eingehende Pakete über ACL auf der SDX-Appliance steuern.
- Wenn Sie NetScaler Application Delivery Management zur Verwaltung Ihrer SDX-Appliance verwenden, müssen Sie entsprechende ACL-Regeln erstellen, um die Kommunikation zwischen MAS und dem SDX Management Service zu ermöglichen.
- Alle anderen Konfigurationen auf der SDX-Appliance wie das Bereitstellen oder Löschen von VPXs, das Hinzufügen/Löschen externer Server und die SNMP-Verwaltung erfordern keine Änderungen an der vorhandenen ACL-Konfiguration. Die Kommunikation mit diesen Stellen wird vom Management Service übernommen.

So konfigurieren Sie eine ACL

Das Konfigurieren einer ACL umfasst die folgenden Schritte:

- Aktivieren der ACL-Funktion
- Erstellen einer ACL-Regel
- Aktivieren der ACL-Regel

> **Hinweis:**
>
> Sie können ACL-Regeln erstellen, ohne die ACL-Funktion zu aktivieren. Wenn die Funktion jedoch nicht aktiviert ist, können Sie eine ACL-Regel nicht aktivieren, nachdem Sie sie erstellt haben.

Aktivieren der ACL-Funktion

1. Um die ACL-Funktion zu aktivieren, melden Sie sich bei der SDX Management Service GUI an und navigieren Sie zu **Konfiguration > System > ACL**.

2. Schalten Sie mit der Umschalttaste die ACL-Funktion ein.

Erstellen einer ACL-Regel

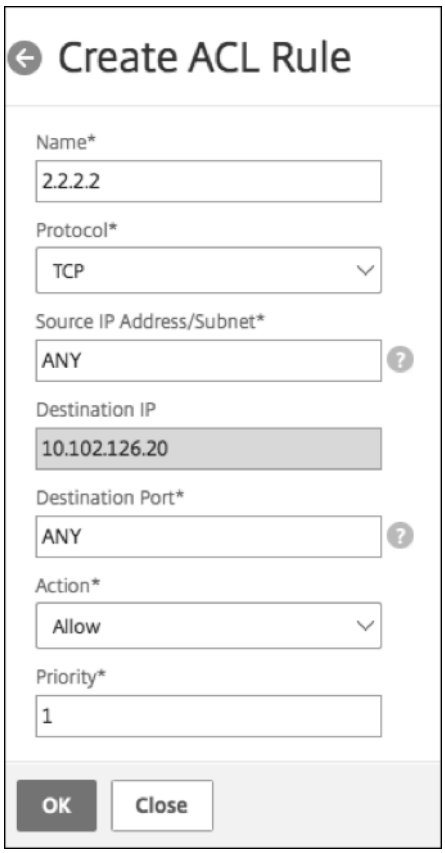
1. Klicken Sie auf der ACL-Seite auf **Regel erstellen**.
2. Das Fenster **Regel erstellen** wird geöffnet. Fügen Sie die in der folgenden Tabelle aufgeführten Details hinzu.

Eigenschaft	Beschreibung
Name	Füge einen Namen hinzu.
Protokoll	Wählen Sie im Menü ein Protokoll aus. Standardmäßig ist TCP ausgewählt. Sie können **ANY** auswählen, um alle Protokolle zuzulassen.
Quell-IP-Adresse/Subnetz	Geben Sie die Quell-IP-Adresse oder das Quellsubnetz an, für das die Regel gilt. Wählen Sie **ANY** aus, wenn die Regel auf den gesamten eingehenden Verkehr angewendet werden muss.
Ziel-IP	Die IP-Adresse des SDX Management Service wird automatisch als Ziel-IP gefüllt. Dieses Feld kann nicht bearbeitet werden.
Destination port	Geben Sie den Zielport an, für den die Regel gilt. Wählen Sie **ANY** aus, wenn die Regel für alle Zielports gilt.
Aktion	Wählen Sie die Aktion für die Regel aus: Zulassen oder Verweigern.

Eigenschaft	Beschreibung
Priorität	Weisen Sie Priorität zu, um die Reihenfolge festzulegen, in der die Regel ausgewertet werden soll. Prioritätsnummern bestimmen die Reihenfolge, in der ACL-Regeln mit einem eingehenden Paket abgeglichen werden. Eine niedrigere Prioritätszahl hat eine höhere Priorität. Beispielsweise hat die Prioritätsnummer 1 eine höhere Priorität als die Prioritätsnummer 1. Wenn keine der Regeln mit dem eingehenden Paket übereinstimmt, ist das Paket gesperrt.

3. Klicken Sie auf **OK**, um die Regel zu erstellen.

   Abbildung: Ein Beispiel für eine ACL-Regel



   Nachdem die Regel erstellt wurde, befindet sie sich im Status Deaktiviert. Um die Regel wirksam zu machen, müssen Sie die Regel aktivieren.

> **Hinweis:**
>
> Um eine Regel zu aktivieren, muss die ACL-Funktion aktiviert sein. Wenn die Funktion deaktiviert ist und Sie versuchen, eine ACL-Regel zu aktivieren, wird die Meldung "ACL wird nicht ausgeführt"angezeigt.

Eine ACL-Regel aktivieren

1. Fahren Sie mit der Maus über die Regel, die Sie aktivieren möchten, und klicken Sie auf den Kreis mit drei Punkten.
2. Wählen Sie im Menü die Option **Aktivieren**aus.
3. Wählen Sie alternativ das Optionsfeld für diese Regel aus und klicken Sie auf die Registerkarte **Aktivieren** .
4. Klicken Sie bei der Eingabeaufforderung zur Bestätigung auf **Ja** .

Andere Aktionen für ACL-Regeln

Sie können die folgenden Aktionen auf die ACL-Regeln anwenden:

1. Deaktivieren einer ACL-Regel
2. Bearbeiten einer ACL-Regel
3. Löschen einer ACL-Regel
4. Nummerieren Sie die Priorität der ACL-Regeln neu

Deaktivieren einer ACL-Regel

1. Bewegen Sie die Maus über die Regel, die Sie deaktivieren möchten, und wählen Sie den Kreis mit drei Punkten aus.
2. Klicken Sie in der Liste auf **Deaktivieren** .
3. Wählen Sie alternativ das Optionsfeld für diese Regel aus und klicken Sie auf die Registerkarte **Deaktivieren** .
4. Klicken Sie zur Bestätigung auf **Ja**.

> **Hinweis:**
>
> Wenn Sie eine Regel deaktivieren, gilt die Regel nicht mehr für eingehenden Datenverkehr. Die

> Regelkonfiguration bleibt jedoch unter den ACL-Einstellungen.

Bearbeiten einer ACL-Regel

1. Bewegen Sie den Mauszeiger über die Regel, die Sie bearbeiten möchten, und wählen Sie den Kreis mit drei Punkten aus.
2. Klicken Sie in der Liste auf **Regel bearbeiten** . Das Fenster **Regel ändern** wird geöffnet.
3. Wählen Sie alternativ das Optionsfeld für diese Regel aus und klicken Sie auf die Registerkarte **Regel bearbeiten** . Das Fenster **Regel ändern** wird geöffnet.
4. Nehmen Sie die Änderungen vor und klicken Sie auf **OK**.

> **Hinweis:**
>
> Sie können eine Regel sowohl im aktivierten als auch im deaktivierten Status bearbeiten. Wenn Sie eine Regel bearbeiten, die bereits aktiviert ist, werden die Änderungen sofort angewendet. Für eine Regel im Status Deaktiviert werden die Änderungen übernommen, wenn Sie die Regel aktivieren.

Löschen einer ACL-Regel

1. Stellen Sie sicher, dass sich die Regel im deaktivierten Zustand befindet.
2. Bewegen Sie den Mauszeiger über die Regel, die Sie löschen möchten, und wählen Sie den Kreis mit drei Punkten aus. Klicken Sie in der Liste auf **Regel löschen** .
3. Wählen Sie alternativ das Optionsfeld für diese Regel aus und klicken Sie auf die Registerkarte **Regel löschen** .
4. Klicken Sie zur Bestätigung auf **Ja**.

> **Hinweis:**
>
> Sie können eine Regel im aktivierten Status nicht löschen.

Nummerieren Sie die Prioritäten der ACL-Regeln neu

1. Bewegen Sie den Mauszeiger über die Regel, für die Sie die Prioritäten neu nummerieren möchten, und wählen Sie den Kreis mit drei Punkten aus. Klicken Sie in der Liste auf **Priorität (n) neu nummerieren** .
2. Wählen Sie alternativ das Optionsfeld für diese Regel aus und klicken Sie auf die Registerkarte **Aktion auswählen** .

3. Wählen Sie **Priorität (n) neu nummerieren**.
4. Der SDX Management Service weist allen vorhandenen Regeln automatisch neue Prioritätsnummern zu, die ein Vielfaches von 10 sind.
5. Bearbeiten Sie die Regeln, um Prioritätsnummern entsprechend Ihrer Anforderung zuzuweisen. Weitere Informationen zum Bearbeiten einer Regel finden Sie im Abschnitt “So bearbeiten Sie eine ACL-Regel”.

Abbildung. Ein Beispiel für vorhandene Prioritätsnummern

	Priority ↑	Name	Source IP Address/Subnet
☐	1	2.2.2.2	ANY
☐	2	test1	1.1.1.1
☐	3	test2	ANY

Abbildung. Ein Beispiel für Prioritätszahlen in Vielfachen von 10, nachdem Prioritäten neu nummeriert wurden

	Priority ↑	Name	Source IP Address/Subnet
☐	10	2.2.2.2	ANY
☐	20	test1	1.1.1.1
☐	30	test2	ANY

Problembehandlung

Wenn ACL-Regeln nicht ordnungsgemäß eingerichtet wurden, kann allen Benutzerkonten der Zugriff verweigert werden. Wenn Sie versehentlich den gesamten Netzwerkzugriff auf den SDX Management Service aufgrund einer falschen ACL-Setup verlieren, gehen Sie folgendermaßen vor, um Zugriff zu erhalten.

1. Melden Sie sich mit SSH und Ihrem “root”-Konto bei der Citrix Hypervisor Management-IP-Adresse an.
2. Melden Sie sich mit Administratorrechten an der Konsole der Management Service-VM an.
3. Führen Sie den Befehl `pfctl –d` aus.
4. Melden Sie sich über die GUI beim Management Service an und konfigurieren Sie die ACL entsprechend neu.

Cluster von NetScaler-Instanzen einrichten

November 23, 2023

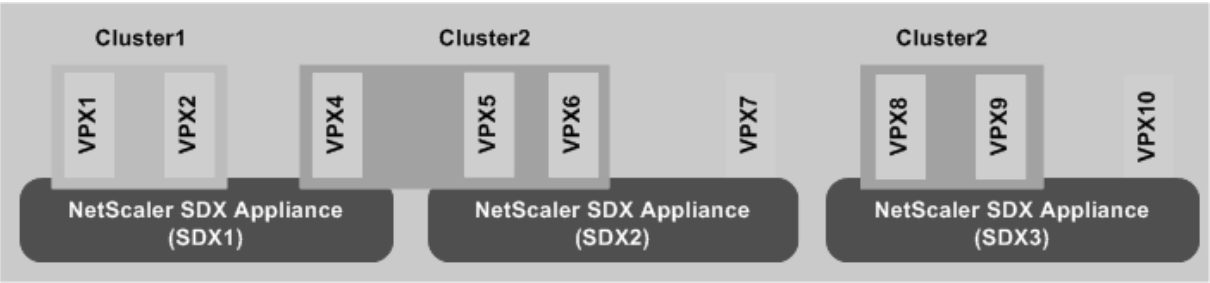
Nachdem Sie NetScaler-Instanzen auf einer oder mehreren SDX-Appliances bereitgestellt haben, können Sie einen Cluster von NetScaler-Instanzen erstellen.

Citrix empfiehlt, dass Sie die Clusterkonfiguration über den Management Service ausführen. Wenn Sie die Cluster-Konfiguration von einer VPX-Instanz aus durchführen, erfährt der Management Service während der automatischen Erkennung alle 30 Minuten von der Konfiguration. Im schlimmsten Fall werden die Clusterinformationen 30 Minuten lang nicht erkannt. Während der Cluster möglicherweise ordnungsgemäß funktioniert, werden einige wichtige Validierungsprüfungen für Cluster-Abhängigkeiten verpasst. Der Management Service führt diese Überprüfungen durch, bevor der Cluster auf ADC-Instanzen konfiguriert wird. Daher müssen Sie jede Clusterkonfiguration über den Management Service ausführen.

Hinweis:

- Um einen Cluster einzurichten, müssen Sie NetScaler-Clustering verstehen. Weitere Informationen finden Sie unter Clustering.
- Für Cluster mit NetScaler-Instanzen auf allen SDX-Appliances empfiehlt Citrix, NetScaler-Instanzen von drei SDX-Appliances zu verwenden. Dieser Prozess stellt sicher, dass die Cluster-Kriterien von mindestens (n/2 +1) Knoten immer erfüllt werden.

Abbildung 1. Cluster von SDX NetScaler-Instanzen



Die vorherige Abbildung zeigt drei SDX-Appliances, SDX1, SDX2 und SDX3, im selben Subnetz. Die NetScaler-Instanzen auf diesen Appliances werden verwendet, um zwei Cluster zu bilden: Cluster1 und Cluster2.

- Cluster1 umfasst zwei Instanzen auf SDX1.
- Cluster2 umfasst eine Instanz auf SDX1, zwei Instanzen auf SDX2 und zwei weitere Instanzen auf SDX3.

Wichtige Punkte

- Die CLAG-Bildung mit Mellanox-Schnittstellen (50G und 100G) wird auf einer SDX-Plattform nicht unterstützt.
- Alle Knoten eines Clusters müssen vom gleichen Typ sein. Sie können mit den folgenden Kombinationen keinen Cluster bilden:
  - Hardware und virtuelle Geräte.
  - NetScaler VPX-Instanzen und NetScaler SDX-Instanzen.
  - ADC-Instanzen auf verschiedenen SDX-Hardwareplattformen.
- Die NetScaler-Instanzen müssen dieselbe Version haben, die Version 10.1 oder höher sein muss.
- Die NetScaler-Instanzen müssen alle über dieselbe Feature-Lizenz verfügen.
- Auf einzelnen NetScaler-Instanzen können keine Konfigurationen aktualisiert werden, nachdem sie dem Cluster hinzugefügt wurden. Alle Änderungen müssen über die Cluster-IP-Adresse durchgeführt werden.
- Die NetScaler-Instanzen müssen alle über dieselben Ressourcen verfügen (Speicher, CPU, Schnittstellen usw.).
- Die Backplane-MTU muss 78 Byte mehr als die MTU der Datenschnittstelle sein.
- Stellen Sie sicher, dass jede Datenschnittstellen-MTU innerhalb von 9138 Byte liegt.
- Ab Version 13.0 Build 82.x werden Sie aufgefordert, eine SNIP-Adresse hinzuzufügen, während Sie einen Knoten zu einem Cluster hinzufügen. Sie können SNIP-Adressen auch dynamisch erstellen, während Sie einen Knoten hinzufügen. Diese Funktion hilft bei der Behebung von Sicherheitsproblemen bei der strengen Überprüfung der Quell-IP-Adresse.
- **Wichtig!** Verwenden Sie die Option **Cluster entfernen** mit Vorsicht. Wenn Sie auf **Cluster entfernen**klicken, wird der Cluster ohne Warnung gelöscht.

Richten Sie einen Cluster auf einer SDX-Appliance ein

1. Melden Sie sich bei der SDX-Appliance an.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **NetScaler > Clusters > Cluster-Instances**.
3. Erstellen Sie den Cluster:
   a) Klicken Sie auf **Cluster erstellen**.
   b) Legen **Sie im Dialogfeld Cluster erstellen** die für den Cluster erforderlichen Parameter fest. Um einen Parameter zu beschreiben, bewegen Sie den Mauszeiger über das entsprechende Feld.
   c) Klicken Sie auf **Weiter**, um die Zusammenfassung der Konfiguration anzuzeigen.

d) Klicken Sie auf **Beenden**, um den Cluster zu erstellen.
Hinweis: Wenn dem Cluster eine NetScaler-Instanz mit konfiguriertem L2-VLAN hinzugefügt wird, wird der Befehl zum
Hinzufügen von VLAN gespeichert, wobei der
`sdxvlan` Parameter auf Ja gesetzt ist. Dieser Parameter ist ein internes Argument und wird verwendet, um den Verlust der Konnektivität während der SDX-Clusterbildung zu vermeiden.

4. Knoten zum Cluster hinzufügen:

a) Klicken Sie auf **Knoten hinzufügen**.
b) Konfigurieren **Sie im Dialogfeld Knoten hinzufügen** die für das Hinzufügen eines Clusterknotens erforderlichen Parameter. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Feld.
c) Klicken Sie auf **Weiter**, um die Zusammenfassung der Konfiguration anzuzeigen.
d) Klicken Sie auf **Fertig stellen**, um den Knoten zum Cluster hinzuzufügen.
e) Wiederholen Sie die Schritte 1 bis 4, um dem Cluster einen weiteren Knoten hinzuzufügen.

Nachdem Sie den Cluster erstellt haben, müssen Sie ihn konfigurieren, indem Sie über die Cluster-IP-Adresse darauf zugreifen.

Wenn die Knoten in einer Cluster-Instanz zu derselben Citix NetScaler SDX-Appliance gehören, verlieren wir möglicherweise das Quorum, wenn eine NetScaler SDX-Appliance ausfällt.

Sie können einen Clusterknoten mithilfe der folgenden Methoden bereitstellen:

1. Erstellen Sie mehrere Cluster-Instanzen mit einer VPX-Instanz von jeder NetScaler SDX-Appliance.

Beispiel:

SDX1	SDX2	Instanz-ID
VPX1	VPX1	1
VPX2	VPX2	2

1. Wenn es mehr als zwei NetScaler SDX-Appliances gibt, erstellen Sie eine einzelne Cluster-Instanz mit VPX-Instanzen von allen Appliances mit. `quorumType Majority` Stellen Sie in diesem Fall sicher, dass die VPX-Instanzen gleichmäßig auf alle NetScaler SDX-Appliances verteilt sind.

Example1:

SDX1	SDX2	SDX3	Instanz-ID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	Nicht verfügbar
VPX3	VPX3	VPX3	Nicht verfügbar

Example2:

SDX1	SDX2	SDX3	Instanz-ID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	Nicht verfügbar
VPX3	VPX3	VPX3	Nicht verfügbar
VPX4	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar

1. Erstellen Sie eine einzelne Cluster-Instanz mit allen VPX-Instanzen von allen NetScaler SDX-Geräten. Aber benutze `quorum type NONE`. Dies hat einige Einschränkungen.

Beispiel:

SDX1	SDX2	Instanz-ID
VPX1	VPX1	1
VPX2	VPX2	2
VPX3	Nicht verfügbar	Nicht verfügbar

Einschränkungen, wenn der Parameter –`quorumType` auf `NONE` gesetzt ist:

- Topologien müssen über redundante Verbindungen zwischen Clusterknoten verfügen, um eine Netzwerkpartition aufgrund einer einzigen Fehlerstelle zu vermeiden.
- Der Cluster kann bei Clustervorgängen wie dem Hinzufügen oder Entfernen von Knoten instabil werden.

> **Hinweis:**
>
> Verwenden Sie die Option **Rediscover**, um eine aktualisierte Liste von NetScaler-Clustern zu erhalten, von denen jeder mindestens eine NetScaler-Instanz der SDX-Appliance enthält.

Fügen Sie eine NetScaler-Instanz, die auf einer SDX-Appliance vorhanden ist, zu einem Cluster hinzu, der auf einer anderen SDX-Appliance konfiguriert ist

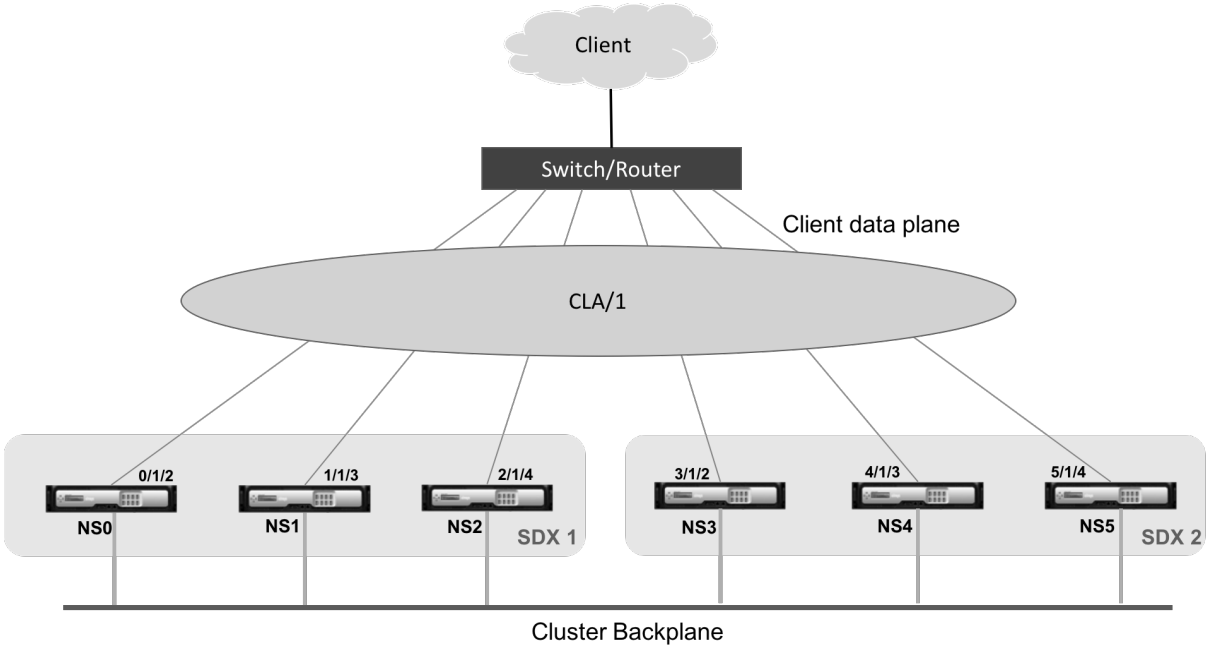
1. Melden Sie sich bei der SDX-Appliance an, von der Sie die NetScaler-Instanz hinzufügen möchten.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **NetScaler**, und klicken Sie dann auf **Cluster**.
3. Klicken Sie auf **Knoten hinzufügen**.
4. Konfigurieren **Sie im Dialogfeld Knoten hinzufügen** die für das Hinzufügen eines Clusterknotens erforderlichen Parameter. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Feld.
   Hinweis: Stellen Sie sicher, dass die Werte der
   Cluster-IP-Adresse und des
   Cluster-IP-Kennworts für den Cluster gelten, dem Sie den Knoten hinzufügen möchten.
5. Klicken Sie auf **Weiter**, um die Zusammenfassung der Konfiguration anzuzeigen.
6. Klicken Sie auf **Fertig stellen**, um den Knoten zum Cluster hinzuzufügen.

Konfigurieren der Cluster-Link-Aggregation

February 15, 2024

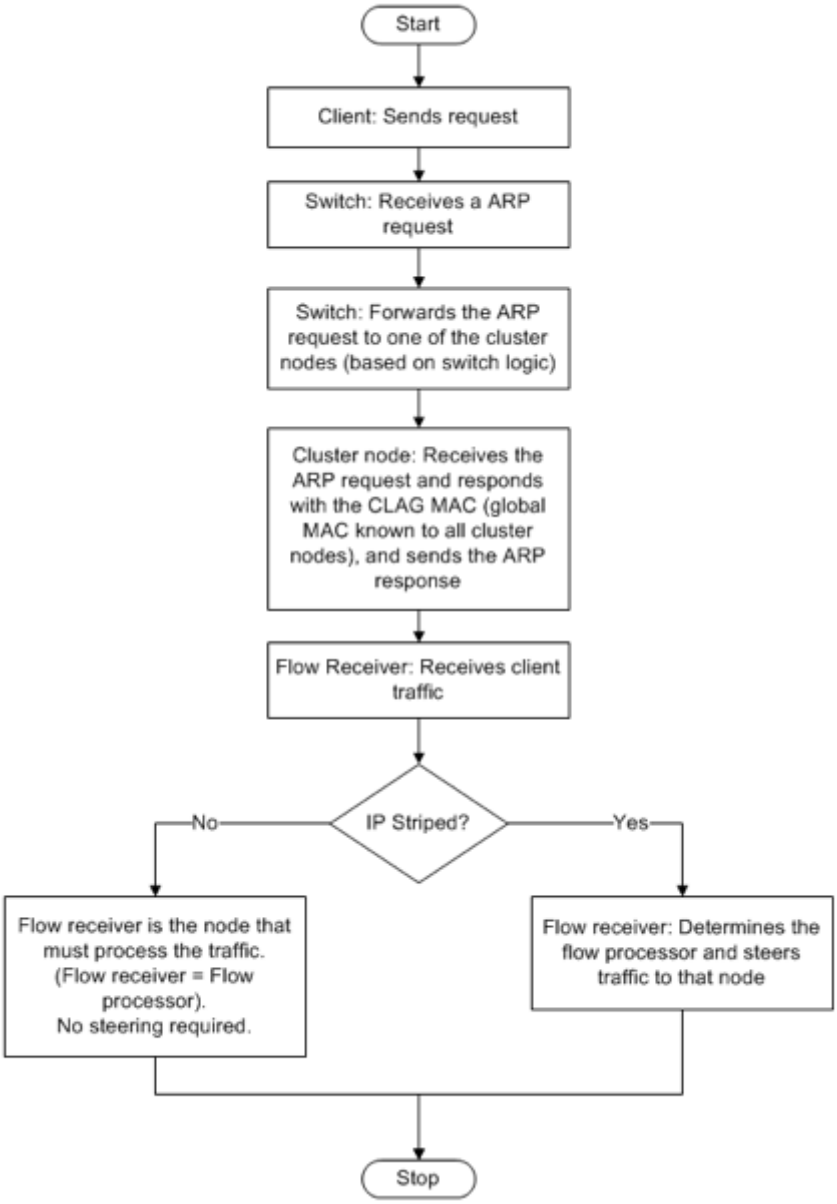
Die Cluster-Link-Aggregation kombiniert, wie der Name schon sagt, eine Gruppe von Cluster-Knoten-Schnittstellen zu einem Kanal. Es ist eine Erweiterung der NetScaler Link Aggregation (LA). Der einzige Unterschied besteht darin, dass sich bei der Linkaggregation die Schnittstellen auf demselben Gerät befinden müssen, sich die Schnittstellen bei der Cluster-Link-Aggregation jedoch auf verschiedenen Knoten des Clusters befinden. Weitere Informationen zur Link-Aggregation finden Sie unter Konfigurieren der Link-Aggregation.

Stellen Sie sich beispielsweise einen Cluster mit sechs Knoten über zwei SDX-Appliances vor, in dem alle sechs Knoten mit einem Upstream-Switch verbunden sind. Ein Cluster-LA-Kanal (CLA/1) wird durch Bindungsschnittstellen 0/1/2, 1/1/3, 2/1/4, 3/1/2, 4/1/3 und 5/1/4 gebildet.



Ein Cluster-LA-Kanal hat folgende Attribute:

- Jeder Kanal hat eine eindeutige MAC-Adresse, auf die sich Clusterknoten einigen.
- Der Kanal kann sowohl lokale als auch Remote-SDX-Knotenschnittstellen binden.
- In einem Cluster werden maximal vier Cluster-LA-Kanäle unterstützt.
- An jeden Cluster-LA-Kanal können maximal 16 Schnittstellen gebunden werden.
- Backplane-Schnittstellen können nicht Teil eines Cluster-LA-Kanals sein.
- Wenn eine Schnittstelle an einen Cluster-LA-Kanal gebunden ist, haben die Kanalparameter Vorrang vor den Netzwerkschnittstellenparametern.
- Eine Netzwerkschnittstelle kann nur an einen Kanal gebunden werden.
- Konfigurieren Sie keinen Verwaltungszugriff auf einen Clusterknoten auf einem Cluster-LA-Kanal (z. B. CLA/1) oder dessen Mitgliedsschnittstellen. Wenn der Knoten INACTIVE ist, wird die entsprechende Cluster-LA-Schnittstelle als POWER OFF gekennzeichnet, wodurch er den Verwaltungszugriff verliert.



Implementieren Sie ähnliche Konfigurationen auf der Cluster-IP-Adresse und auf dem externen Verbindungsgerät. Wenn möglich, konfigurieren Sie den Upstream-Switch so, dass der Datenverkehr basierend auf der IP-Adresse oder dem Port anstelle der MAC-Adresse verteilt wird.

Wichtige Punkte:

- Aktivieren Sie LACP (indem Sie den LACP-Modus entweder als ACTIVE oder PASSIVE angeben). **Hinweis:** Stellen Sie sicher, dass der LACP-Modus sowohl im NetScaler-Cluster als auch auf dem externen Verbindungsgerät nicht als PASSIVE festgelegt ist.
- Zum Erstellen eines Cluster-LA-Kanals kann der LACP-Schlüssel einen Wert von 5 bis 8 haben. Diese LACP-Schlüssel sind CLA/1, CLA/2, CLA/3 und CLA/4 zugeordnet.

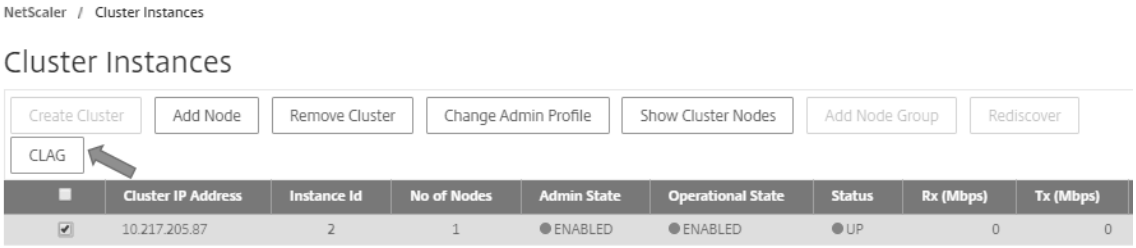
- Auf der SDX-Appliance können die Cluster-Link-Aggregationsgruppen-Mitgliedsschnittstellen (CLAG) nicht mit anderen virtuellen Maschinen gemeinsam genutzt werden.
- Stellen Sie auf dem Upstream-Switch das LACP-Timeout auf “Short”ein, um lange Verkehrsschwächer auf Clusterknoten zu vermeiden. Diese Einstellung ist nützlich, wenn der Upstream-Switch erst nach dem LACP-Timeout über das Herunterfahren des CLAG und seiner Mitgliedsschnittstellen informiert wird.

Voraussetzungen:

Erstellen Sie einen Cluster von NetScaler-Instanzen. Die Knoten des Clusters können NetScaler-Instanzen auf derselben SDX-Appliance oder auf anderen SDX-Appliances sein, die im selben Subnetz verfügbar sind.

So konfigurieren Sie einen Cluster-LA-Kanal mithilfe des Management Service:

1. Melden Sie sich bei der SDX-Appliance an.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **NetScaler ADC**, und klicken Sie dann auf **Cluster**.
3. Wählen Sie auf der Seite **Cluster Instanzen** den Cluster aus und klicken Sie auf **CLAG**.



4. Gehen Sie im Dialogfeld **CLAG erstellen** wie folgt vor:
   a) Wählen Sie in der Dropdownliste **Kanal-ID** die Cluster-LA-Kanal-ID aus.
   b) Wählen Sie im Abschnitt **Schnittstellen** im Auswahlfeld **Verfügbar** die Schnittstellen aus und klicken Sie auf **+**.
   c) Die ausgewählten Schnittstellen werden im Auswahlfeld **Konfiguriert** angezeigt.
5. Gehen Sie im Abschnitt **Einstellung** wie folgt vor:
   a) Geben Sie im Feld **Alias** einen alternativen Namen für den Cluster-LA-Kanal ein.
   b) Wählen Sie im Feld **LACP-Timeout** einen der folgenden Werte aus, um das Intervall zu definieren, nach dem ein Link nicht aggregiert wird, wenn der Link keine LACPDU empfängt.

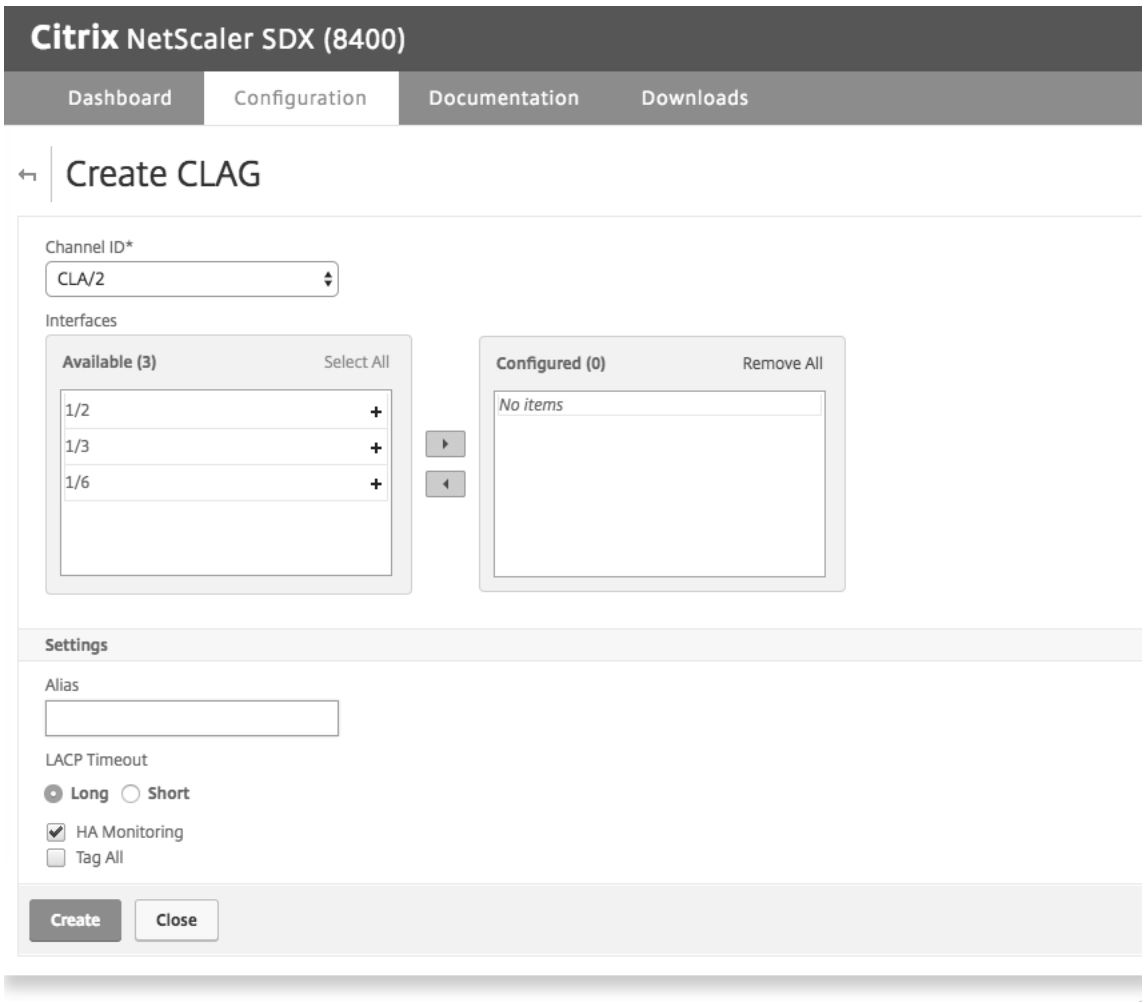
      Der Wert muss auf allen Ports übereinstimmen, die an der Linkaggregation auf der SDX-Appliance und dem Partnerknoten teilnehmen:

- **Lang** —30 Sekunden
- **Kurz** —1 Sekunde

c) Für die Hochverfügbarkeitskonfiguration (HA) aktivieren Sie das Kontrollkästchen **HA-Überwachung**, um den Kanal auf Ausfallereignisse zu überwachen. Der Ausfall eines LA-Kanals, bei dem HA MON aktiviert ist, löst ein HA-Failover aus.

d) Wählen Sie **Alle markieren** aus, um jedem auf diesem Kanal gesendeten Paket ein Vier-Byte-802.1q-Tag hinzuzufügen. Die **ON-Einstellung** wendet Tags für alle VLANs an, die an diesen Kanal gebunden sind. OFF wendet das Tag auf alle VLANs außer dem nativen VLAN an.

6. Klicken Sie auf **Erstellen**, um eine CLAG für eine der SDX-Appliances zu konfigurieren.



7. Klicken Sie im Dialogfeld **Bestätigen** auf **Ja**, um die CLAG-Einstellungen in den anderen SDX-Appliances zu aktualisieren.

> **Hinweise:**
>
> - Wenn Sie **Nein**auswählen, ist die CLAG nicht konfiguriert.
> - Aktualisieren Sie die CLAG-Einstellungen in den anderen SDX-Appliances manuell.
> - Die MTU-Einstellungen müssen auf beiden SDX-Appliances identisch sein. Die MTU-Einstellungen müssen auf einer der SDX-Appliances manuell geändert werden.

8. Gehen Sie wie folgt vor, um die MTU-Einstellungen im **CLAGs-Dialogfeld** zu ändern:
   a) Wählen Sie **CLA/1** aus und klicken Sie auf **Bearbeiten**.
   b) Stellen Sie im Dialogfeld **CLAG konfigurieren** die MTU manuell im Feld **MTU** ein und klicken Sie auf **OK**.
9. Klicken Sie im **Bestätigungsdialogfeld** auf **Ja**.

Konfigurieren von SSL-Verschlüsselungen für den sicheren Zugriff auf den Management Service

February 15, 2024

Sie können SSL-Verschlüsselungssuites aus einer Liste von SSL-Verschlüsselungen auswählen, die von NetScaler SDX-Appliances unterstützt werden. Binden Sie eine beliebige Kombination der SSL-Verschlüsselungen, um über HTTPS sicher auf den SDX Management Service zuzugreifen. Eine SDX-Appliance bietet 37 vordefinierte Verschlüsselungsgruppen, die Kombinationen ähnlicher Verschlüsselungen sind, und Sie können benutzerdefinierte Verschlüsselungsgruppen aus der Liste der unterstützten SSL-Verschlüsselungsgruppen erstellen.

Einschränkungen

- Das Binden von Chiffren mit Schlüsselaustausch = “DH”oder “ECC-DHE”wird nicht unterstützt.
- Das Binden der Verschlüsselungen mit Authentication = “DSS”wird nicht unterstützt.
- Das Binden von Verschlüsselungen, die nicht Teil der Liste der unterstützten SSL-Verschlüsselungen sind, oder das Einbeziehen dieser Verschlüsselungen in einer benutzerdefinierten Verschlüsselungsgruppe wird nicht unterstützt.

Unterstützte SSL-Verschlüsselungen

In der folgenden Tabelle sind die unterstützten SSL-Verschlüsselungen aufgeführt. Der Wert in der Spalte **Protokoll** ist das niedrigste unterstützte Protokoll. Wenn beispielsweise SSLv3 aufgeführt ist,

werden SSLv3/TLSv1/TLSv1.1/TLSv1.2 unterstützt.

Citrix Verschlüsselungsname	OpenSSL CipherName	Hex-Code	Protokoll	Key Exchange-Algorithmus	Authentifizierungsalgorithmus	Algorithmus für Nachrichtenauthentifizierungscode (MAC)
TLS1-AES-256-CBC-SHA	AES256-SHA	0x0035	SSLv3	RSA	RSA	AES(256)
TLS1-AES-128-CBC-SHA	AES128-SHA	0x002F	SSLv3	RSA	RSA	AES(128)
TLS1.2-AES-256-SHA256	AES256-SHA256	0x003D	TLSv1.2	RSA	RSA	AES(256)
TLS1.2-AES-128-SHA256	AES128-SHA256	0x003C	TLSv1.2	RSA	RSA	AES(128)
TLS1.2-AES256-GCM-SHA384	AES256-GCM-SHA384	0x009D	TLSv1.2	RSA	RSA	AES-GCM(256)
TLS1.2-AES128-GCM-SHA256	AES128-GCM-SHA256	0x009C	TLSv1.2	RSA	RSA	AES-GCM(128)
TLS1-ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA	0xC014	SSLv3	ECC-DHE	RSA	AES(256)
TLS1-ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	0xC013	SSLv3	ECC-DHE	RSA	AES(128)
TLS1.2-ECDHE-RSA-AES-256-SHA384	ECDHE-RSA-AES256-SHA384	0xC028	TLSv1.2	ECC-DHE	RSA	AES(256)

Citrix Verschlüsselungsname	OpenSSL CipherName	Hex-Code	Protokoll	Key Exchange-Algorithmus	Authentifizierungsalgorithmus	Algorithmus für Nachrichtenauthentifizierungscode (MAC)
TLS1.2-ECDHE-RSA-AES-128-SHA256	ECDHE-RSA-AES128-SHA256	0xC027	TLSv1.2	ECC-DHE	RSA	AES(128)
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA-AES256-GCM-SHA384	0xC030	TLSv1.2	ECC-DHE	RSA	AES-GCM(256)
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA-AES128-GCM-SHA256	0xC02F	TLSv1.2	ECC-DHE	RSA	AES-GCM(128)
TLS1.2-DHE-RSA-AES-256-SHA256	DHE-RSA-AES256-SHA256	0x006B	TLSv1.2	DH	RSA	AES(256)
TLS1.2-DHE-RSA-AES-128-SHA256	DHE-RSA-AES128-SHA256	0x0067	TLSv1.2	DH	RSA	AES(128)
TLS1.2-DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384	0x009F	TLSv1.2	DH	RSA	AES-GCM(256)
TLS1.2-DHE-RSA-AES128-GCM-SHA256	DHE-RSA-AES128-GCM-SHA256	0x009E	TLSv1.2	DH	RSA	AES-GCM(128)

Citrix Verschlüsselungsname	OpenSSL CipherName	Hex-Code	Protokoll	Key Exchange-Algorithmus	Authentifizierungsalgorithmus	Algorithmus für Nachrichtenauthentifizierungscode (MAC)
TLS1-DHE-RSA-AES-256-CBC-SHA	DHE-RSA-AES256-SHA	0x0039	SSLv3	DH	RSA	AES(256)
TLS1-DHE-RSA-AES-128-CBC-SHA	DHE-RSA-AES128-SHA	0x0033	SSLv3	DH	RSA	AES(128)
TLS1-DHE-DSS-AES-256-CBC-SHA	DHE-DSS-AES256-SHA	0x0038	SSLv3	DH	DSS	AES(256)
TLS1-DHE-DSS-AES-128-CBC-SHA	DHE-DSS-AES128-SHA	0x0032	SSLv3	DH	DSS	AES(128)
TLS1-ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA-DES-CBC3-SHA	0xC012	SSLv3	ECC-DHE	RSA	3DES(168)
SSL3-EDH-RSA-DES-CBC3-SHA	EDH-RSA-DES-CBC3-SHA	0x0016	SSLv3	DH	RSA	3DES(168)
SSL3-EDH-DSS-DES-CBC3-SHA	EDH-DSS-DES-CBC3-SHA	0x0013	SSLv3	DH	DSS	3DES(168)
TLS1-ECDHE-RSA-RC4-SHA	ECDHE-RSA-RC4-SHA	0xC011	SSLv3	ECC-DHE	RSA	RC4(128)
SSL3-DES-CBC3-SHA	DES-CBC3-SHA	0x000A	SSLv3	RSA	RSA	3DES(168)
SSL3-RC4-SHA	RC4-SHA	0x0005	SSLv3	RSA	RSA	RC4(128)

Citrix Verschlüsselungsname	OpenSSL CipherName	Hex-Code	Protokoll	Key Exchange-Algorithmus	Authentifizierungsalgorithmus	Algorithmus für Nachrichtenauthentifizierungscode (MAC)
SSL3-RC4-MD5	RC4-MD5	0x0004	SSLv3	RSA	RSA	RC4(128)
SSL3-DES-CBC-SHA	DES-CBC-SHA	0x0009	SSLv3	RSA	RSA	DES(56)
SSL3-EXP-RC4-MD5	EXP-RC4-MD5	0x0003	SSLv3	RSA (512)	RSA	RC4(40)
SSL3-EXP-DES-CBC-SHA	EXP-DES-CBC-SHA	0x0008	SSLv3	RSA (512)	RSA	DES(40)
SSL3-EXP-RC2-CBC-MD5	EXP-RC2-CBC-MD5	0x0006	SSLv3	RSA (512)	RSA	RC2(40)
SSL2-DES-CBC-MD5	DHE-DSS-AES128-SHA256	0x0040	SSLv2	RSA	RSA	DES(56)
SSL3-EDH-DSS-DES-CBC-SHA	EDH-DSS-DES-CBC-SHA	0x0012	SSLv3	DH	DSS	DES(56)
SSL3-EXP-EDH-DSS-DES-CBC-SHA	EXP-EDH-DSS-DES-CBC-SHA	0x0011	SSLv3	DH(512)	DSS	DES(40)
SSL3-EDH-RSA-DES-CBC-SHA	EDH-RSA-DES-CBC-SHA	0x0015	SSLv3	DH	RSA	DES(56)
SSL3-EXP-EDH-RSA-DES-CBC-SHA	EXP-EDH-RSA-DES-CBC-SHA	0x0014	SSLv3	DH(512)	RSA	DES(40)
SSL3-ADH-RC4-MD5	ADH-RC4-MD5	0x0018	SSLv3	DH	Ohne	RC4(128)
SSL3-ADH-DES-CBC3-SHA	ADH-DES-CBC3-SHA	0x001B	SSLv3	DH	Ohne	3DES(168)

Citrix Verschlüsselungsname	OpenSSL CipherName	Hex-Code	Protokoll	Key Exchange-Algorithmus	Authentifizierungsalgorithmus	Algorithmus für Nachrichtenauthentifizierungscode (MAC)
SSL3-ADH-DES-CBC-SHA	ADH-DES-CBC-SHA	0x001A	SSLv3	DH	Ohne	DES(56)
TLS1-ADH-AES-128-CBC-SHA	ADH-AES128-SHA	0x0034	SSLv3	DH	Ohne	AES(128)
TLS1-ADH-AES-256-CBC-SHA	ADH-AES256-SHA	0x003A	SSLv3	DH	Ohne	AES(256)
SSL3-EXP-ADH-RC4-MD5	EXP-ADH-RC4-MD5	0x0017	SSLv3	DH(512)	Ohne	RC4(40)
SSL3-EXP-ADH-DES-CBC-SHA	EXP-ADH-DES-CBC-SHA	0x0019	SSLv3	DH(512)	Ohne	DES(40)
SSL3-NULL-MD5	NULL-MD5	0x0001	SSLv3	RSA	RSA	Ohne
SSL3-NULL-SHA	NULL-SHA	0x0002	SSLv3	RSA	RSA	Ohne

Vordefinierte Verschlüsselungsgruppen

In der folgenden Tabelle sind die von der SDX-Appliance bereitgestellten vordefinierten Verschlüsselungsgruppen aufgeführt.

Cipher-Gruppenname	Beschreibung
ALL	Alle von der SDX-Appliance unterstützten Verschlüsselungen, ausgenommen NULL-Verschlüsselungen
DEFAULT	Standard-Verschlüsselungsliste mit Verschlüsselungsstärke> = 128 Bit
kRSA	Chiffren mit Key-Ex-Algo als RSA

Cipher-Gruppenname	Beschreibung
kEDH	Chiffren mit Key-Ex-Algo als Ephemeral-DH
DH	Chiffren mit Key-Ex-Algo als DH
EDH	Chiffren mit Key-Ex/Auth Algo als DH
aRSA	Chiffren mit Auth Algo als RSA
aDSS	Chiffren mit Auth Algo als DSS
aNULL	Chiffren mit Auth Algo als NULL
DSS	Chiffren mit Auth Algo als DSS
DES	Chiffren mit Enc Algo als DES
3DES	Chiffren mit Enc Algo als 3DES
RC4	Chiffren mit Enc Algo als RC4
RC2	Chiffren mit Enc Algo als RC2
NULL	Chiffren mit Enc-Algo als NULL
MD5	Chiffren mit MAC-Algo als MD5
SHA1	Chiffren mit MAC-Algo als SHA-1
SHA	Chiffren mit MAC-Algo als SHA
NULL	Chiffren mit Enc-Algo als NULL
RSA	Chiffren mit Key-Ex/Auth Algo als RSA
ADH	Chiffren mit Key-Ex-Algo als DH und Auth Algo als NULL
SSLv2	SSLv2-Protokollchiffren
SSLv3	SSLv3-Protokollchiffren
TLSv1	SSLv3/TLSv1-Protokollchiffren
TLSv1_ONLY	TLSv1-Protokollchiffren
EXP	Chiffren exportieren
EXPORT	Chiffren exportieren
EXPORT40	Exportieren von Chiffren mit 40-Bit-Verschlüsselung
EXPORT56	Exportieren von Chiffren mit 56-Bit-Verschlüsselung
LOW	Verschlüsselungen mit geringer Stärke (56-Bit-Verschlüsselung)

Cipher-Gruppenname	Beschreibung
MEDIUM	Verschlüsselungen mittlerer Stärke (128-Bit-Verschlüsselung)
HIGH	Starke Chiffren (168-Bit-Verschlüsselung)
AES	AES-Chiffren
FIPS	FIPS-zugelassene Verschlüsselungen
ECDHE	Ephemere DH-Chiffren mit elliptischer Kurve
AES-GCM	Chiffren mit Enc-Algo als AES-GCM
SHA2	Chiffren mit MAC-Algo als SHA-2

Zeigen Sie die vordefinierten Verschlüsselungsgruppen an

Um die vordefinierten Verschlüsselungsgruppen anzuzeigen, erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **Management Service**, und klicken Sie dann auf **Verschlüsselungsgruppen**.

Erstellen von benutzerdefinierten Verschlüsselungsgruppen

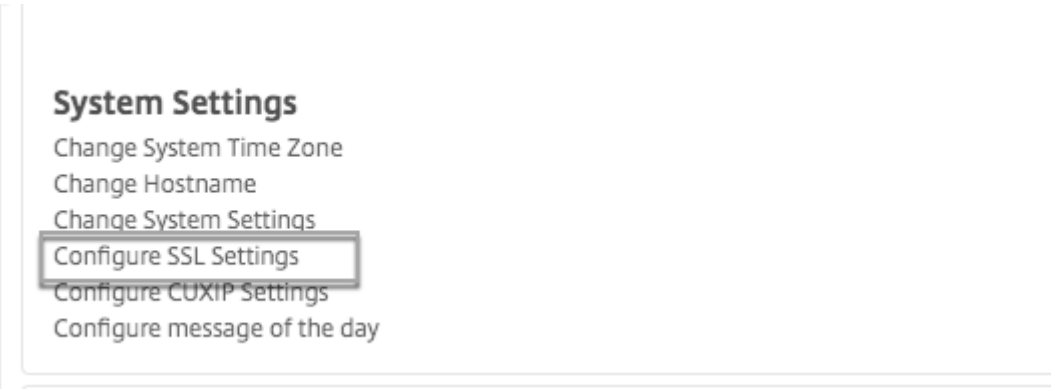
Sie können benutzerdefinierte Verschlüsselungsgruppen aus der Liste der unterstützten SSL-Verschlüsselungen erstellen.

So erstellen Sie benutzerdefinierte Verschlüsselungsgruppen:

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **Management Service**, und klicken Sie dann auf **Verschlüsselungsgruppen**.
2. Klicken Sie im Bereich **Verschlüsselungsgruppen** auf **Hinzufügen**.
3. Führen **Sie im Dialogfeld Verschlüsselungsgruppe erstellen** die folgenden Schritte aus:
    a) Geben Sie im Feld **Gruppenname** einen Namen für die benutzerdefinierte Verschlüsselungsgruppe ein.
    b) Geben Sie im Feld **Beschreibung der Verschlüsselungsgruppe** eine kurze Beschreibung der benutzerdefinierten Verschlüsselungsgruppe ein.
    c) Klicken Sie im Abschnitt **Cipher Suites** auf **Hinzufügen** und wählen Sie die Verschlüsselungen aus, die in die Liste der unterstützten SSL-Verschlüsselungen aufgenommen werden sollen.
    d) Klicken Sie auf **Erstellen**.

Bestehende SSL-Verschlüsselungsbindungen anzeigen

Um die vorhandenen Verschlüsselungsbindungen anzuzeigen, erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **System**, und klicken Sie dann unter **Systemeinstellungen** auf **SSL-Einstellungen konfigurieren**.



> **Hinweis:**
>
> Nach dem Upgrade auf die neueste Version des Management Service werden in der Liste der vorhandenen Verschlüsselungssammlungen die OpenSSL-Namen angezeigt. Sobald Sie die Verschlüsselungen aus dem aktualisierten Management Service gebunden haben, verwendet die Anzeige die Citrix Benennungskonvention.

Binden von Chiffren an den HTTPS-Dienst

1. Klicken Sie auf der Registerkarte **Konfiguration** im Navigationsbereich auf **System**.
2. Klicken Sie im Bereich **System** unter Systemeinstellungen auf **SSL-Einstellungen konfigurieren**.
3. Klicken **Sie im Bereich Einstellungen bearbeiten** auf **Ciphers Suites**.
4. Führen Sie im Bereich **Ciphers Suites** einen der folgenden Schritte aus:
    - Um eine Verschlüsselungsgruppe aus den vordefinierten Verschlüsselungsgruppen auszuwählen, wählen Sie **Verschlüsselungsgruppen**aus, wählen Sie eine Verschlüsselungsgruppe aus der Liste **Verschlüsselungsgruppen** aus, und klicken Sie dann auf **OK**.
    - Um aus der Liste der unterstützten Verschlüsselungen auszuwählen, aktivieren Sie das Kontrollkästchen **Cipher Suites**, klicken Sie auf **Hinzufügen**, um die Verschlüsselungen auszuwählen, und klicken Sie dann auf **OK**.

Sichern und Wiederherstellen der Konfigurationsdaten der SDX-Appliance

February 15, 2024

Der Backup-Prozess der NetScaler SDX-Appliance ist ein einstufiger Prozess, bei dem eine Sicherungsdatei erstellt wird, die Folgendes enthält:

- Einzelbündel-Image:
  - Citrix Hypervisor-Image
  - Hotfixes und ergänzende Packs von Citrix Hypervisor
  - Management Service-Image
- XVA-Image
- Image aktualisieren
- SDX-Konfiguration
- Konfiguration

Der Backup-Ordner ist /var/mps/backup/.

Backup der aktuellen Konfiguration

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **Management Service**, und klicken Sie dann auf **Backupdateien**.
2. Klicken Sie im Bereich **Backupdateien** auf **Backup**.
3. Aktivieren Sie im Dialogfeld **Neue Backupdatei** das Kontrollkästchen **Password Protect file**, um die Backupdatei zu verschlüsseln.
4. Geben Sie in die Felder **Kennwort**und **Kennwort bestätigen** das Kennwort für die Backupdatei ein und bestätigen Sie es.
5. Klicken Sie auf **Weiter**.

Beim Backupvorgang wird eine Backupdatei erstellt. Der Dateiname der Backupdatei enthält die aktuelle IP-Adresse des Management Service und den Zeitstempel, wann die Backup wurde. Um nach Abweichungen in der Backupdatei zu suchen, navigieren Sie in der SDX-GUI zu **Konfiguration > System > Ereignisse/Alarme**.

Geplantes Backup

Standardmäßig erstellt SDX alle 24 Stunden eine Backup über einer Backuprichtlinie. Mithilfe der Backuprichtlinie können Sie die Anzahl der Backupdateien definieren, die Sie in der SDX-Appliance

aufbewahren möchten. Sie können die geplanten Backupdateien auch mit einem Kennwort verschlüsseln, um sicherzustellen, dass die Backupdatei sicher ist.

Bearbeiten der Backuprichtlinie

1. Klicken Sie auf der Registerkarte **Konfiguration** auf **System**.
2. Klicken Sie im Bereich **Richtlinienverwaltung** auf **Backuprichtlinie**.
3. Führen Sie im Bereich **Backuprichtlinie konfigurieren** die folgenden Schritte aus:
    a) Geben Sie im Feld **Vorherige aufzubewahrende Backups** die Anzahl der Backupdateien ein, die Sie behalten möchten.
    b) Um die Backupdateien zu verschlüsseln, aktivieren Sie das Kontrollkästchen **Backupdatei verschlüsseln**.
    c) Geben Sie in die Felder **Kennwort** und **Kennwort bestätigen** das Kennwort zum Verschlüsseln der Backupdatei ein und bestätigen Sie es.

Übertragen Sie die Backupdatei manuell auf einen externen Sicherungsserver

Stellen Sie sicher, dass Sie über die Details des externen Sicherungsservers verfügen, bevor Sie die Backupdatei manuell übertragen.

Übertragen Sie die Backupdatei auf einen externen Sicherungsserver

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **Management Service**, und klicken Sie dann auf **Backupdateien**.
2. Wählen Sie im Bereich **Backupdateien** die Backupdatei aus, und klicken Sie dann auf **Übertragen**.
3. Geben Sie im Feld **Server** den Host-Namen oder die IP-Adresse des externen Backupservers ein.
4. Geben Sie in die Felder **Benutzername** und **Kennwort** den Benutzernamen und das Kennwort für den Zugriff auf den externen Backupserver ein.
5. Geben Sie im Feld **Port** die Portnummer ein.
6. Wählen Sie im Feld **Übertragungsprotokoll** das Protokoll aus, das Sie verwenden möchten, um die Backupdatei auf den externen Sicherungsserver zu übertragen.
7. Geben Sie im Feld **Verzeichnispfad** den Pfad des Verzeichnisses auf dem externen Sicherungsserver ein, in dem Sie die Backupdateien speichern möchten.
8. Wählen Sie **Datei aus Management Service** löschen aus, um die Backupdatei von der SDX-Appliance zu löschen, nachdem Sie die Backupdatei auf den externen Sicherungsserver übertragen haben.
9. Klicken Sie auf **OK**.

Wiederherstellen der Appliance

Sie können die SDX-Appliance auf die in der Backupdatei verfügbare Konfiguration zurücksetzen. Während der Appliance-Wiederherstellung wird die gesamte aktuelle Konfiguration gelöscht.

Zu beachtenswerte Punkte:

- Bevor Sie die SDX-Appliance mit der Backupdatei einer anderen SDX-Appliance wiederherstellen, fügen Sie die Netzwerkeinstellungen des Verwaltungsdienstes gemäß den in der Backupdatei verfügbaren Einstellungen hinzu.
- Stellen Sie sicher, dass die Plattformvariante, auf der die Backup wurde, mit der Sie die Wiederherstellung versuchen, identisch ist. Das Wiederherstellen der Backupdatei zwischen zwei verschiedenen Plattformvarianten wird nicht unterstützt.
- Citrix empfiehlt, das SDX-Backup erst wiederherzustellen, nachdem die Netzwerkkonfiguration festgelegt wurde. Sie können die folgenden Netzwerkeinstellungen für die SVM angeben:
  - SVM-IP-Adresse
  - Hypervisor-IP-Adresse
  - Subnetzmaske
  - Gateway
  - DNS-Server

Stellen Sie die Appliance aus der Backupdatei wieder her

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **Management Service**, und klicken Sie dann auf **Backupdateien**.
2. Klicken Sie im Bereich **Backupdateien** auf die Backupdatei, und klicken Sie dann auf **OK**.
3. Wählen Sie im Dialogfeld**Wiederherstellen**die Option**Gerätewiederherstellung**aus, und klicken Sie dann auf **Fortfahren**.

   Die verschiedenen Komponenten der Anwendungswiederherstellung werden angezeigt:

   - Lizenz
   - SDX-Image
   - XVA-Dateien
   - NetScaler-Konfiguration
   - Zusammenfassung

   Wenn eine der erforderlichen Komponenten in der Backupdatei fehlt, werden Sie aufgefordert, das fehlende Element hochzuladen, bevor Sie fortfahren.

   Informationen darüber, ob eine Backupdatei auf der aktuellen SDX Single Bundle Image-Version wiederhergestellt werden kann, finden Sie in der folgenden Tabelle. Als Faustregel für

Single Bundle Image gilt, dass Backup mit niedrigerer Version nicht auf einer späteren Version wiederhergestellt werden können.

Aktuelle SDX-Einzelpaket-Image-Version	Backupdateiversion
11.1	11.1, 12.0, 12.1, 13.0 unterstützt; 11.0 wird nicht unterstützt
12.0	12.0, 12.1, 13.0 unterstützt; 11.0 und 11.1 werden nicht unterstützt
12.1	12.1, 13.0 unterstützt, 11.0, 11.1, 12.0 nicht unterstützt
13.0	13.0 unterstützt; 11.0, 11.1, 12.0, 12.1 nicht unterstützt
13.1	13.1 unterstützt; 11.0, 11.1, 12.0, 12.1, 13.0 nicht unterstützt

4. Prüfen Sie auf der Seite **Lizenz**, ob eine gültige Lizenz vorhanden ist, und klicken Sie auf **Weiter**.
5. Die **SDX-Image-Seite** wird angezeigt. Wenn für die Wiederherstellung kein SDX-Image erforderlich ist, klicken Sie auf **Weiter**. Andernfalls laden Sie bei Aufforderung ein gültiges SDX-Image hoch und klicken Sie auf **Weiter**.
6. Die Seite **XVA-Datei** wird geöffnet. Klicken Sie auf **Weiter**, wenn XVA-Images für alle Instanzen vorhanden sind.Wenn die XVA-Datei für eine Instanz in der Backupdatei fehlt, können Sie sie entweder hochladen oder die Wiederherstellung dieser Instanz überspringen. Klicken Sie auf **Weiter**, um zur nächsten Seite zu gelangen.
7. Die NetScaler-Konfigurationsseite wird geöffnet. NetScaler-Konfigurationsdateien sind nicht zwingend erforderlich. Sie können die Instanz bereitstellen, ohne ihre Konfiguration wiederherzustellen. Wenn die NetScaler-Konfigurationsdatei in der Backupdatei fehlt, können Sie entweder nur mit der Instanzbereitstellung fortfahren oder die Wiederherstellung der Instanz überspringen. Klicken Sie auf **Weiter**, um zur nächsten Seite zu gelangen.
8. Die Zusammenfassungsseite wird mit den folgenden Details zu allen in der Backupdatei vorhandenen Instanzen angezeigt:
   - IP-Adresse
   - Hostname
   - SDX-Version
   - XVA-Version
   - Version-Bit
   - Wiederherstellen: Wenn die Appliance oder Instanz für die Wiederherstellung bereit ist, wird ein Häkchen angezeigt. Ist dies nicht der Fall, erscheint eine Kreuzmarkierung.

- Fehlermeldungen: Wenn die Appliance oder Instanz nicht für die Wiederherstellung bereit ist, wird eine Fehlermeldung angezeigt, die den Grund erklärt.

9. Klicken Sie auf **Wiederherstellen**, um die Anwendungswiederherstellung abzuschließen.

NetScaler-Instanz wiederherstellen

Sie können die NetScaler-Instanz in der SDX-Appliance auf den NetScaler-Instanzen wiederherstellen, die in der Backupdatei verfügbar sind.

Hinweis: Eine VPX-Instanz kann nicht wiederhergestellt werden, wenn:

- Der Instanz ist keine Management-NIC zugewiesen, und
- Die Instanz wird vom SDX Management Service nur über LACP verwaltet.
  Die Wiederherstellung schlägt fehl, da SDX Management Service die Kanalkonfigurationen nicht automatisch wiederherstellen kann. Um dieses Problem zu vermeiden, stellen Sie die Kanalkonfiguration manuell wieder her, um die VPX-Instanzwiederherstellung abzuschließen.

Gehen Sie wie folgt vor, um die NetScaler-Instanz in der Backupdatei wiederherzustellen:

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **Management Service**, und klicken Sie dann auf **Backupdateien**.
2. Wählen Sie im Bereich **Backupdateien** die Backupdatei aus, und klicken Sie dann auf **Wiederherstellen**.
3. Wählen Sie im Dialogfeld **Wiederherstellen** die Option **Instanzwiederherstellung** aus.
4. Wählen Sie die NetScaler-Instanzen aus, die Sie wiederherstellen möchten, und klicken Sie dann auf **Fortfahren**.
5. (Optional) Wenn die Backupdatei verschlüsselt ist, geben Sie bei Aufforderung das Kennwort ein und klicken Sie dann auf**OK**.

> **Hinweis:**
>
> Stellen Sie sicher, dass auf der SDX-Appliance, auf der die wiederherzustellende Instanz ausgeführt wird, eine entsprechende XVA-, Build-Image- und Kanalkonfiguration vorhanden sind.

Führen Sie einen Gerätereset durch

November 23, 2023

Die NetScaler SDX-Appliance ermöglicht Ihnen:

- Setzen Sie die Konfiguration der Appliance zurück.

> **Hinweis:**
>
> Wenn Sie die Konfiguration zurücksetzen, müssen Sie sich mit der Seriennummer des Geräts als Kennwort anmelden.

- Setzen Sie das Gerät auf die Werksversion zurück.
- Setzen Sie die Appliance auf eine bestimmte Single Bundle-Image-Version zurück.

Bevor Sie einen Appliance-Reset durchführen, sichern Sie alle auf der Appliance gespeicherten Daten, einschließlich der Einstellungen aller auf der Appliance bereitgestellten NetScaler-Instanzen.

Citrix empfiehlt, die Dateien außerhalb der Appliance zu speichern. Durch das Zurücksetzen der Appliance werden alle aktuellen Clientsitzungen mit dem Management Service beendet. Melden Sie sich für zusätzliche Konfigurationsaufgaben wieder beim Management Service an. Wenn Sie bereit sind, die Daten wiederherzustellen, importieren Sie die Backupdateien mithilfe des Management Service.

Der Management Service bietet die folgenden Optionen zum Zurücksetzen der Appliance:

- Konfiguration zurücksetzen
- Zurücksetzen auf Werkseinstellungen
- Saubere Installation

Setzen Sie die Konfiguration der Appliance zurück

Der Management Service bietet die Option Config Reset, um die Konfiguration der Appliance zurückzusetzen. Die Option Config Reset führt Folgendes aus:

- Löscht VPX-Instanzen.
- Löscht SSL-Zertifikat und Schlüsseldateien.
- Löscht Lizenz- und technische Archivdateien.
- Löscht die NTP-Konfiguration auf der Appliance.
- Stellt die Zeitzone auf UTC wieder her.
- Stellt die Richtlinien zum Beschneiden und Backup auf ihre Standardeinstellungen zurück.
- Löscht das Image des Management Service.
- Löscht das NetScaler SDX-Image.
- Löscht alle XVA-Images mit Ausnahme der letzten Imagedatei, auf die auf der Appliance zugegriffen wurde.
- Stellt die Standard-Schnittstelleneinstellungen wieder her.
- Stellt die Standardkonfiguration der Appliance wieder her, einschließlich Standardprofile, Benutzer und Systemeinstellungen.
- Stellt die Standardkennwörter für Citrix Hypervisor und den Management Service wieder her.
- Startet den Management Service neu.

Setzen Sie die Konfiguration der Appliance zurück

1. Navigieren Sie zu **Konfiguration > System > Gruppe Systemadministration**.
2. Klicken Sie auf**Gerät zurücksetzen**.
3. Wählen Sie im Dialogfeld**Appliance Reset** in der Liste**Reset Type die Option ConfigReset** aus.
4. Klicken Sie auf **OK**.

Setzen Sie das Gerät auf die Werksversion zurück

Der Management Service bietet die Option zum Zurücksetzen auf Werkseinstellungen, um die Appliance auf die Werksversion zurückzusetzen. Die Option Factory Reset setzt die aktuellen IP-Adressen des Management Service und des Citrix Hypervisor auf die Standard-IP-Adressen des Management Service und des Citrix Hypervisor zurück.

Stellen Sie sicher, dass Sie alle auf der Appliance gespeicherten Daten sichern, einschließlich der Einstellungen aller auf der Appliance bereitgestellten NetScaler-Instanzen. Citrix empfiehlt, die Dateien außerhalb der Appliance zu speichern. Durch das Zurücksetzen auf die Werkseinstellungen werden alle aktuellen Clientsitzungen mit dem Management Service beendet. Melden Sie sich für zusätzliche Konfigurationsaufgaben wieder beim Management Service an. Wenn Sie bereit sind, die Daten wiederherzustellen, importieren Sie die Backupdateien mithilfe des Management Service.

> **Wichtig**
>
> Schließen Sie vor dem Zurücksetzen auf die Werkseinstellungen unbedingt ein serielles Konsolenkabel an das Gerät an.

Setzen Sie das Gerät auf die Werksversion zurück

1. Navigieren Sie zu **Konfiguration > System > Systemadministration**.
2. Klicken Sie auf**Gerät zurücksetzen**.
3. Wählen Sie im Dialogfeld **Geräte-Reset** in der Liste **Reset-Typ die Option FactoryReset** .
4. Klicken Sie auf **OK**.

Zurücksetzen der Appliance auf eine Image-Version mit einem einzelnen Bund

Der Management Service bietet die Option zur sauberen Installation, mit der Sie eine beliebige Version eines einzelnen Bundle-Images auf der Appliance installieren können. Sie können damit eine Neuinstallation des einzelnen Bundle-Images als neues Standard-Boot-Image durchführen. Durch die Neuinstallation wird die vorhandene Konfiguration, mit Ausnahme der Netzwerkeinstellungen, in der SDX-Appliance entfernt.

> **Hinweis:**
>
> Wenn Ihre SDX-Appliance mit der Softwareversion 11.0 oder früher geliefert wurde, schlägt die Neuinstallation auf Version 13.1 oder höher fehl.

Die Clean-Install-Option wird in folgenden Bereichen unterstützt:

Image-Version mit einem Paket	SDX-Plattformen
11.0.xx	SDX 14xxx, SDX 25xxx. **Hinweis**: Die Option zur sauberen Installation wird auf anderen SDX-Plattformen unterstützt, wenn sie über eine 10G-Werkspartition verfügen.
11.1.xx	SDX 14xxx, SDX 25xxx. **Hinweis**: Die Clean-Install-Option wird auf anderen SDX-Plattformen unterstützt, wenn sie über eine 10G-Werkspartition verfügen
11.1.51.x	Alle SDX-Plattformen.
12.1.xx	Alle SDX-Plattformen.
13.0.xx	Alle SDX-Plattformen.
13.1.xx	Alle SDX-Plattformen.

Voraussetzungen

Stellen Sie sicher, dass:

- Sie führen ein Failover aller primären Hochverfügbarkeitsknoten zu einer anderen SDX-Appliance durch. Wenn Sie nicht über Hochverfügbarkeitsfunktionen verfügen, sollten Sie die Ausfallzeit entsprechend planen.
- Laden Sie das einzelne Bundle-Image auf Ihren lokalen Computer herunter.

> **Wichtig:**
>
> Stellen Sie sicher, dass Sie das Gerät nicht neu starten oder wieder einschalten, während Sie die Option Clean Install verwenden.
> Die Appliance wird mehrfach neu gestartet.

Zurücksetzen der Appliance auf eine Image-Version mit einem einzelnen Bund

1. Navigieren Sie zu **Konfiguration > System > Gruppe Systemadministration**.

2. Klicken Sie auf**Gerät zurücksetzen**.
3. Wählen Sie im Dialogfeld **Appliance Reset** in der Liste **Reset Type** die Option **Clean Install** aus.
4. Klicken Sie auf **OK**.

Externe Authentifizierungsserver kaskadieren

February 15, 2024

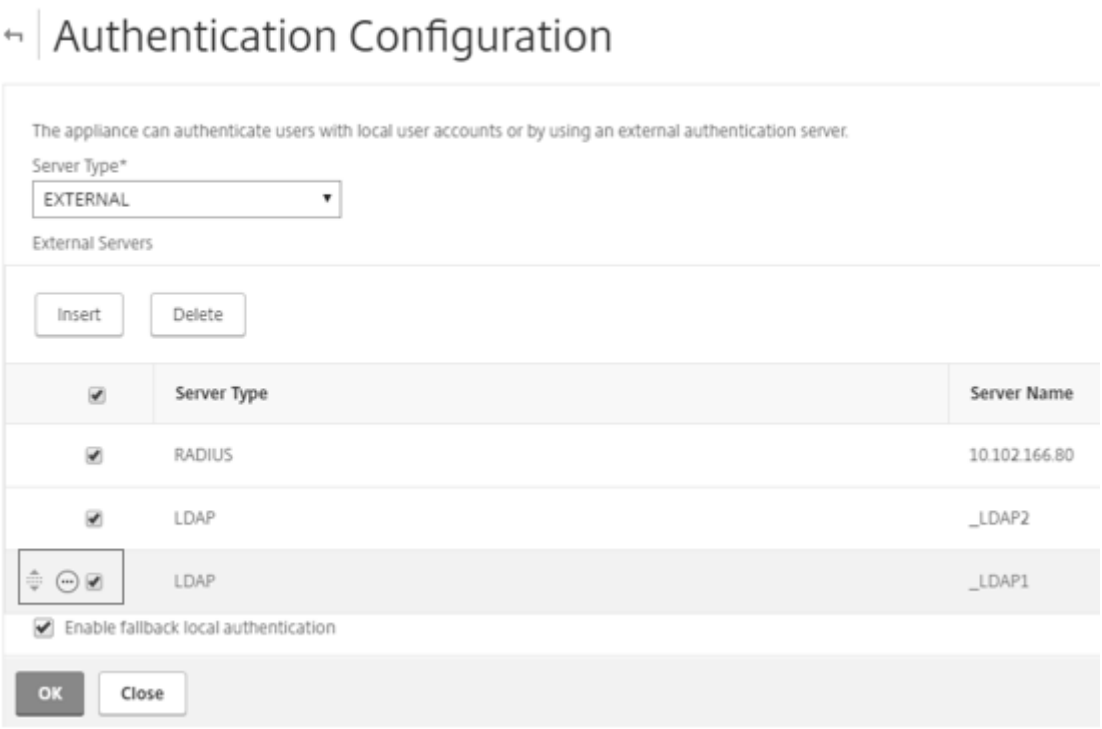
Das Kaskadieren mehrerer externer Authentifizierungsserver bietet einen kontinuierlichen, zuverlässigen Prozess zur Authentifizierung und Autorisierung externer Benutzer. Wenn die Authentifizierung auf dem ersten Authentifizierungsserver fehlschlägt, versucht der Management Service, den Benutzer mithilfe des zweiten externen Authentifizierungsservers zu authentifizieren.

Um die kaskadierende Authentifizierung zu aktivieren, fügen Sie die externen Authentifizierungsserver zum Management Service hinzu. Weitere Informationen finden Sie unter Konfigurieren der externen Authentifizierung. Sie können jeden Typ der unterstützten externen Authentifizierungsserver (RADIUS, LDAP und TACACS) hinzufügen. Um beispielsweise vier externe Authentifizierungsserver für die kaskadierende Authentifizierung hinzuzufügen, können Sie eine beliebige Kombination von RADIUS-, LDAP- und TACACS-Servern hinzufügen. Sie können auch alle vier Server desselben Typs hinzufügen. In NetScaler Application Delivery Management können Sie bis zu 32 externe Authentifizierungsserver konfigurieren.

Kaskadieren externer Authentifizierungsserver

1. Erweitern Sie auf der Registerkarte **Konfiguration** unter **System** den Knoten **Authentifizierung**.
2. Klicken Sie auf der Seite **Authentifizierung** auf **Authentifizierungskonfiguration**.
3. Wählen Sie auf der Seite **Authentifizierungskonfiguration** in der Dropdownliste **Servertyp** die Option **EXTERNAL** aus (Sie können nur externe Server kaskadieren).
4. Klicken Sie auf **Einfügen**, und wählen Sie auf der Seite **Externe Server**, die geöffnet wird, einen oder mehrere Authentifizierungsserver aus, die Sie kaskadieren möchten.
5. Klicken Sie auf **OK**.

Die ausgewählten Server werden auf der Seite **Authentication Servers** angezeigt, wie in der folgenden Abbildung dargestellt. Um die Reihenfolge der Authentifizierung zu ändern, verwenden Sie das Symbol neben einem Servernamen, um den Server in der Liste nach oben oder unten zu verschieben.



Benutzer entsperren

November 23, 2023

Ein NetScaler SDX-Administrator kann einen Benutzer entsperren, bevor das Sperrintervall abläuft. Lockout ist nicht anwendbar, wenn sich ein Benutzer über die Konsole beim Management Service anmeldet. Das Sperrintervall wird ebenfalls von Sekunden auf Minuten geändert. Mindestwert = 1 Minute. Maximalwert = 30 Minuten.

Entsperren eines Benutzers mit der GUI

1. Navigieren Sie zu **Konfiguration > System > Benutzerverwaltung > Benutzer**.
2. Wähle den zu entsperrenden Benutzer aus.
3. Klicken Sie auf **Entsperren**

Entsperren eines Benutzers mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set systemuser id=<ID> unlock=true
```


NetScaler-Instanzen bereitstellen

November 23, 2023

> **Hinweis**
>
> Die NetScaler ADM Service Connect ist standardmäßig aktiviert, nachdem Sie die NetScaler SDX-Appliance auf Version 13.1 installiert oder aktualisiert haben. Weitere Informationen finden Sie unter Data Governance und NetScaler ADMService Connect.

Sie können eine oder mehrere NetScaler-Instanzen auf der SDX-Appliance bereitstellen, indem Sie den Management Service verwenden. Die Anzahl der Instanzen, die Sie installieren können, hängt von der Lizenz ab, die Sie erworben haben. Wenn die Anzahl der hinzugefügten Instanzen der in der Lizenz angegebenen Anzahl entspricht, erlaubt der Management Service die Bereitstellung weiterer NetScaler-Instanzen nicht.

> **Hinweis:**
>
> Sie können bis zu 20 VPX-Instanzen auf einer Netzwerkschnittstelle unabhängig von der zugrunde liegenden Hardwareplattform konfigurieren.

Die Provisioning einer NetScaler VPX-Instanz auf der SDX-Appliance umfasst die folgenden Schritte.

1. Definieren Sie ein Admin-Profil, das an die NetScaler-Instanz angehängt werden soll. Dieses Profil gibt die Benutzeranmeldeinformationen an, die vom Management Service für die Bereitstellung der ADC-Instanz und später für die Kommunikation mit der Instanz zum Abrufen von Konfigurationsdaten verwendet werden. Sie können auch das Standard-Admin-Profil verwenden.
2. Laden Sie die XVA-Imagedatei in den Management Service hoch.
3. Fügen Sie mithilfe des Bereitstellung NetScaler-Assistenten im Management Service eine NetScaler-Instanz hinzu. Der Management Service stellt implizit die NetScaler-Instanz auf der SDX-Appliance bereit und lädt dann die Konfigurationsdetails der Instanz herunter.

> **Warnung**
>
> Stellen Sie sicher, dass Sie die bereitgestellten Netzwerkschnittstellen oder VLANs einer Instanz über den Management Service ändern, anstatt die Änderungen direkt auf der Instanz durchzuführen.

Erstellen Sie ein Administratorprofil

Administratorprofile geben die Benutzeranmeldeinformationen an, die vom Management Service bei der Bereitstellung der NetScaler-Instanzen verwendet werden. Diese Anmeldeinformationen werden

später bei der Kommunikation mit den Instanzen zum Abrufen von Konfigurationsdaten verwendet. Die in einem Administratorprofil angegebenen Benutzeranmeldeinformationen werden auch vom Client verwendet, wenn er sich über die CLI oder GUI bei den NetScaler-Instanzen anmeldet.

Mit Admin-Profilen können Sie auch angeben, dass der Management Service und eine VPX-Instanz nur über einen sicheren Kanal oder über HTTP miteinander kommunizieren.

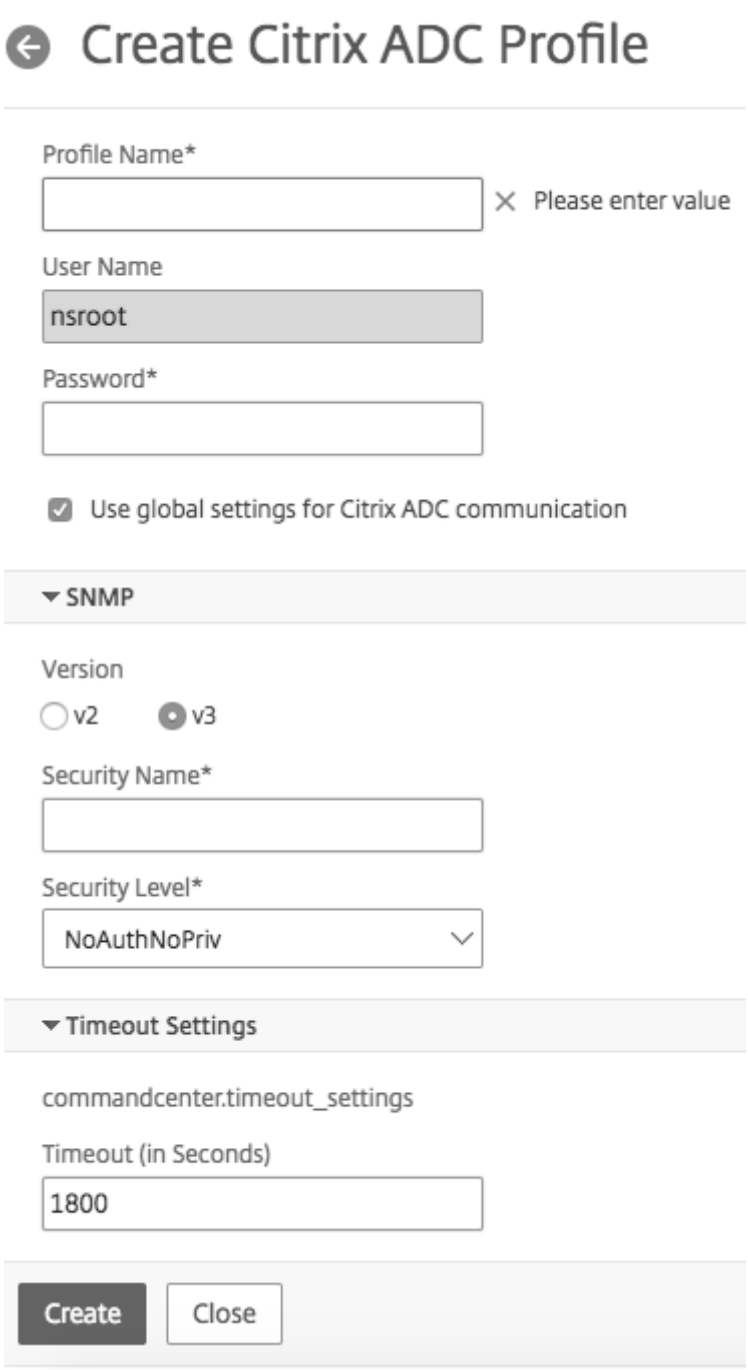
Das standardmäßige Admin-Profil für eine Instanz gibt den standardmäßigen Admin-Benutzernamen an. Dieses Profil kann nicht geändert oder gelöscht werden. Sie müssen jedoch das Standardprofil überschreiben, indem Sie ein benutzerdefiniertes Administratorprofil erstellen und es bei der Bereitstellung der Instanz an die Instanz anhängen. Der Management Service-Administrator kann ein benutzerdefiniertes Administratorprofil löschen, wenn es keiner NetScaler-Instanz angehängt ist.

> **Wichtig**
>
> Ändern Sie das Kennwort nicht direkt in der VPX-Instanz. Wenn Sie dies tun, ist die Instanz über den Management Service nicht mehr erreichbar. Um ein Kennwort zu ändern, erstellen Sie zunächst ein Admin-Profil und ändern Sie dann die NetScaler-Instanz, indem Sie dieses Profil aus der Liste der Admin-Profile auswählen.

Um das Kennwort von NetScaler-Instances in einem Hochverfügbarkeits-Setup zu ändern, ändern Sie zunächst das Kennwort auf der Instanz, die als sekundärer Knoten bezeichnet ist. Ändern Sie dann das Kennwort für die Instanz, die als primärer Knoten bestimmt ist. Denken Sie daran, die Kennwörter nur mit dem Management Service zu ändern.

Erstellen Sie ein Administratorprofil

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich die **NetScaler-Konfiguration**, und klicken Sie dann auf **Admin-Profile**.
2. Klicken Sie im Bereich **Admin-Profile** auf **Hinzufügen**.
3. Das Dialogfeld **Admin-Profil erstellen** wird angezeigt.



Legen Sie die folgenden Parameter fest:

- Profilname: Name des Admin-Profils. Der Standardprofilname lautet `nsroot`. Sie können benutzerdefinierte Profilnamen erstellen.
- Kennwort: Das Kennwort, mit dem Sie sich bei der NetScaler-Instanz anmelden. Maximale Länge: 31 Zeichen.
- SSH-Port: Stellen Sie den SSH-Port ein. Der Standardanschluss ist 22.

- **Globale Einstellungen für die NetScaler-Kommunikation verwenden:** Wählen Sie aus, ob die Einstellung in den Systemeinstellungen für die Kommunikation zwischen dem Management Service und der NetScaler-Instanz definiert werden soll. Sie können dieses Feld löschen und das Protokoll auf HTTP oder HTTPS ändern.
  - Wählen Sie die **HTTP-Option**, um das HTTP-Protokoll für die Kommunikation zwischen dem Management Service und der NetScaler-Instanz zu verwenden.
  - Wählen Sie die Option **https**, um den sicheren Kanal für die Kommunikation zwischen dem Management Service und der NetScaler-Instanz zu verwenden.

4. Wählen Sie unter **SNMP**die Version aus. Wenn Sie v2 wählen, fahren Sie mit Schritt 5 fort. Wenn Sie v3 auswählen, fahren Sie mit Schritt 6 fort.

5. Fügen Sie unter SNMP v2 den Namen der **SNMP-Community** hinzu.

6. Fügen Sie unter SNMP v3 **Sicherheitsname** und **Sicherheitsstufe**hinzu.

7. Geben Sie unter **Timeout-Einstellungen**den Wert an.

8. Klicken Sie auf **Erstellen**und dann auf **Schließen**. Das von Ihnen erstellte Administratorprofil wird im Bereich **Admin-Profile** angezeigt.

Wenn der Wert in der Spalte **Standard** wahr ist, ist das Standardprofil das Admin-Profil. Wenn der Wert false ist, ist ein benutzerdefiniertes Profil das Admin-Profil.

Wenn Sie kein benutzerdefiniertes Administratorprofil verwenden möchten, können Sie es aus dem Management Service entfernen. Um ein benutzerdefiniertes Administratorprofil zu entfernen, wählen Sie im Bereich **Admin-Profile** das Profil aus, das Sie entfernen möchten, und klicken Sie dann auf **Löschen**.

Laden Sie ein NetScaler.xva-Image hoch

Zum Hinzufügen einer NetScaler VPX-Instanz ist eine .xva-Datei erforderlich.

Laden Sie die NetScaler SDX .xva-Dateien auf die SDX-Appliance hoch, bevor Sie die VPX-Instanzen bereitstellen. Sie können auch eine XVA-Imagedatei als Backup auf einen lokalen Computer herunterladen. Das XVA-Imagedateiformat ist: `NSVPX-XEN-ReleaseNumber-BuildNumber_nc`.xva.

Im Bereich **NetScaler XVA-Dateien** können Sie die folgenden Details anzeigen.

- **Name:** Name der XVA-Imagedatei. Der Dateiname enthält das Release und die Buildnummer. Der Dateiname `NSVPX-XEN-12.1-56.22.xva.gz` bezieht sich beispielsweise auf Version 12.1 Build 56.22.
- **Letzte Änderung:** Datum, an dem die XVA-Imagedatei zuletzt geändert wurde.
- **Größe:** Größe der XVA-Imagedatei in MB.

So laden Sie eine NetScaler-.xva-Datei hoch

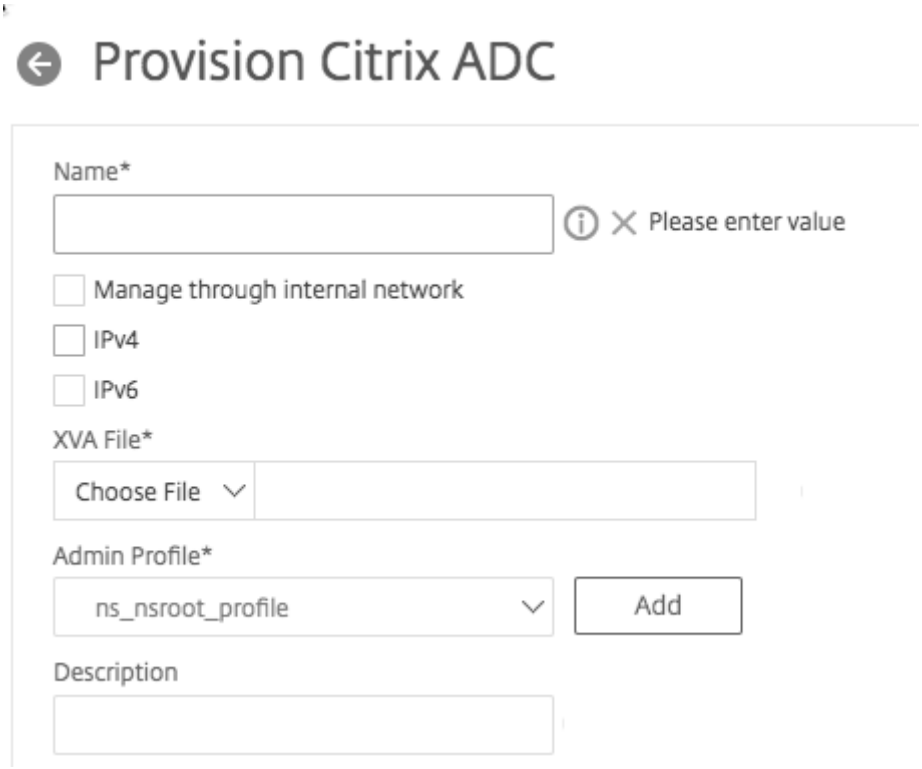
1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich **NetScaler-Konfiguration**, und klicken Sie dann auf **XVA-Dateien**.
2. Klicken Sie im Bereich **NetScaler XVA-Dateien** auf **Hochladen**.
3. Klicken **Sie im Dialogfeld NetScaler-Instanz hochladen** auf **Durchsuchen** und wählen Sie die XVA-Imagedatei aus, die Sie hochladen möchten.
4. Klicken Sie auf **Upload**. Die XVA-Imagedatei wird nach dem Hochladen im Bereich **NetScaler XVA-Dateien** angezeigt.

So erstellen Sie eine Backup durch Herunterladen einer NetScaler-.xva-Datei

1. Wählen Sie im Bereich **NetScaler Build Files** die Datei aus, die Sie herunterladen möchten, und klicken Sie dann auf **Herunterladen**.
2. Klicken Sie im Meldungsfeld **Dateidownload** auf **Speichern**.
3. Navigieren Sie im Meldungsfeld **Speichern unter** zu dem Speicherort, an dem Sie die Datei speichern möchten, und klicken Sie dann auf **Speichern**.

Fügen Sie eine NetScaler-Instanz hinzu

Wenn Sie NetScaler-Instanzen aus dem Management Service hinzufügen, müssen Sie Werte für einige Parameter angeben. Der Management Service konfiguriert diese Einstellungen implizit auf den NetScaler-Instanzen.



- **Name**: Weisen Sie der NetScaler-Instanz einen Namen zu.
- Wählen Sie **Über ein internes Netzwerk verwalten** aus, um eine unabhängige interne Always-On-Konnektivität zwischen dem SDX Management Service und der VPX-Instanz zu aktivieren. Diese Funktion wird in den Versionen 13.0-36.27 und höheren Versionen von VPX-Instanzen unterstützt, die auf der SDX-Appliance ausgeführt werden.
- Wählen Sie eine IPv4- oder IPv6-Adresse oder sowohl IPv4- als auch IPv6-Adressen aus, um zu Verwaltungszwecken auf die NetScaler VPX-Instanz zuzugreifen. Eine NetScaler-Instanz kann nur eine Management-IP (NSIP) haben. Sie können eine NSIP-Adresse nicht entfernen.
- Weisen Sie dem Management Service eine Netzwerkmaske, ein Standard-Gateway und Nexthop für die IP-Adresse zu.
- Die Felder **Gateway** und **Nexthop to Management Service** sind unter einer der folgenden Bedingungen optional, wenn VPX mit Version 13.0—88.9 oder 13.1—37.8 und ihren höheren Versionen bereitgestellt wird:
  - Wenn **Über internes Netzwerk verwalten** aktiviert ist.
  - Wenn sich die konfigurierte IPv4-Adresse im selben Subnetz wie die Management Service-IP-Adresse befindet.

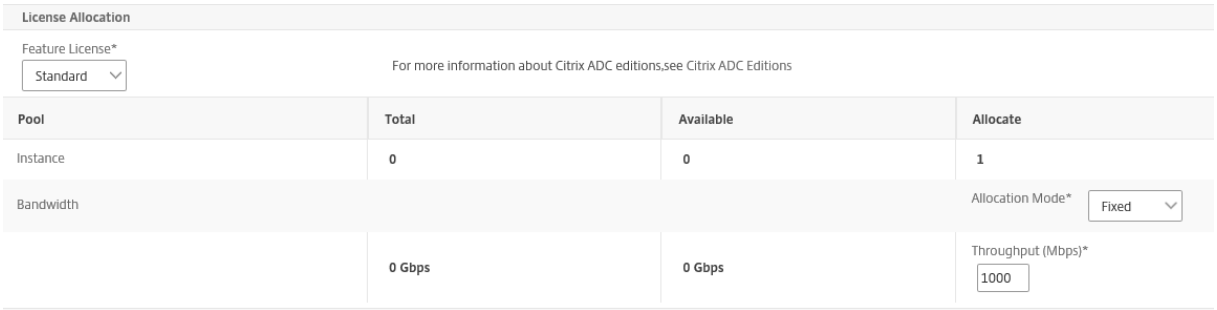
Als Nächstes fügen Sie die XVA-Datei, das Admin-Profil und eine Beschreibung für die Instanz hinzu.

Hinweis: Für ein Hochverfügbarkeits-Setup (Active-Active oder Active-Standby) empfiehlt Citrix, die beiden NetScaler VPX-Instanzen auf verschiedenen SDX-Appliances zu konfigurieren. Stellen Sie sicher, dass die Instanzen im Setup über identische Ressourcen wie CPU, Speicher, Schnittstellen, Pakete pro Sekunde (PPS) und Durchsatz verfügen.

Lizenzzuteilung

Geben Sie in diesem Abschnitt die Lizenz an, die Sie für den NetScaler erworben haben. Die Lizenz kann Standard, Enterprise und Platin sein.

Hinweis: Ein Sternchen zeigt Pflichtfelder an.



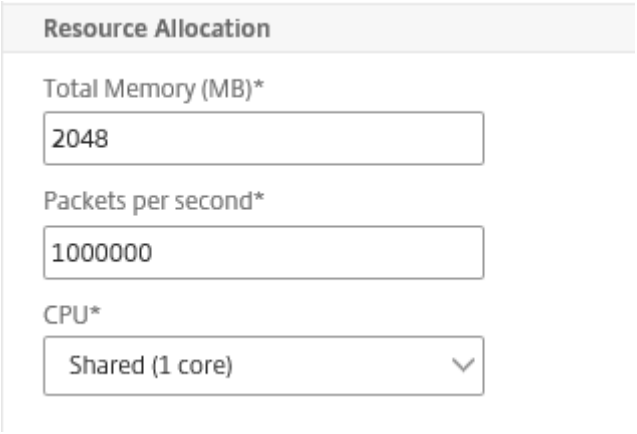
Wenn Sie Bandbreiten-Bursting-Fähigkeit benötigen, wählen Sie unter **Zuweisungsmodus** die Option **Burstable** aus. Weitere Informationen finden Sie unter Bandbreitenmessung in SDX.

Krypto-Zuweisung

Ab Version 12.1 48.13 hat sich die Schnittstelle zur Verwaltung der Kryptokapazität geändert. Weitere Informationen finden Sie unter Verwalten der Krypto-Kapazität.

Ressourcen Allokation

Weisen Sie unter Ressourcenzuweisung Gesamtspeicher, Pakete pro Sekunde und CPU zu.



CPU

Weisen Sie der Instanz einen oder mehrere dedizierte Kerne zu, oder die Instanz teilt sich einen Kern mit anderen Instanzen. Wenn Sie Shared auswählen, wird der Instanz ein Core zugewiesen, der Core wird jedoch möglicherweise mit anderen Instanzen gemeinsam genutzt, wenn Ressourcen knapp sind. Starten Sie betroffene Instanzen neu, wenn CPU-Kerne neu zugewiesen wurden Starten Sie die Instanzen neu, auf denen die CPU-Kerne neu zugewiesen wurden, um Leistungseinbußen

Ab SDX Version 11.1.x.x (MR4) können Sie einer Instanz maximal 16 Kerne zuweisen, wenn Sie die SDX 25000xx-Plattform verwenden. Wenn Sie die SDX 2500xxx-Plattform verwenden, können Sie einer Instanz außerdem maximal 11 Kerne zuweisen.

Hinweis: Für eine Instanz beträgt der maximale Durchsatz, den Sie konfigurieren, 180 Gbit/s.

In der folgenden Tabelle sind die unterstützte VPX, die Single Bundle-Image-Version und die Anzahl der Kerne aufgeführt, die Sie einer Instanz zuweisen können:

Plattformname	Kerne insgesamt	Gesamtzahl der für VPX-Provisioning verfügbaren Kerne	Maximale Kerne, die einer einzelnen Instanz zugewiesen werden können
SDX 8015, SDX 8400 und SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500 und SDX 20500	12	10	5

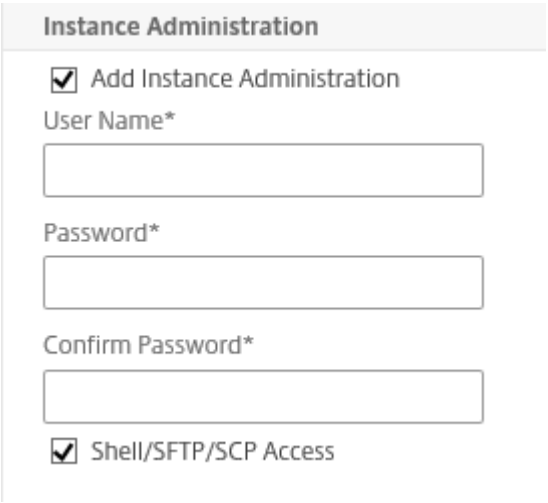
Plattformname	Kerne insgesamt	Gesamtzahl der für VPX-Provisioning verfügbaren Kerne	Maximale Kerne, die einer einzelnen Instanz zugewiesen werden können
SDX 11515, SDX 11520, SDX 11530, SDX 11540 und SDX 11542	12	10	5
SDX 17500, SDX 19500 und SDX 21500	12	10	5
SDX 17550, SDX 19550, SDX 20550 und SDX 21550	12	10	5
SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 und SDX 14100	12	10	5
SDX 22040, SDX 22060, SDX 22080, SDX 22100 und SDX 22120	16	14	7
SDX 24100 und SDX 24150	16	14	7
SDX 14020 40 G, SDX 14030 40 G, SDX 14040 40 G, SDX 14060 40 G, SDX 14080 40 G und SDX 14100 40 G	12	10	10
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS und SDX 14100 FIPS	12	10	5
SDX 14040 40S, SDX 14060 40S, SDX 14080 40S und SDX 14100 40S	12	10	10
SDX 25100A, 25160A, 25200A	20	18	9

Plattformname	Kerne insgesamt	Gesamtzahl der für VPX-Provisioning verfügbaren Kerne	Maximale Kerne, die einer einzelnen Instanz zugewiesen werden können
SDX 25100-40 G, 25160-40 G, 25200-40 G	20	18	16 (wenn Version 11.1-51.x oder höher ist); 9 (wenn Version 11.1-50.x oder niedriger ist; alle Versionen von 11.0 und 10.5)
SDX 26100, 26160, 26200, 26250	28	26	16
SDX 26100-50S, 26160-50S, 26200-50S, 26250-50S	28	26	16
SDX 26100-100 G, 26160-100 G, 26200-100 G, 26250-100 G	28	26	25
SDX 15000	16	14	14
SDX 15000-50 G	16	14	14
SDX 9100	10	9	9
SDX 16000	32	30	16

> **Hinweis:**
>
> Dedizierte Kerne werden der Anzahl der Paket-Engines zugeordnet, die auf der Instanz ausgeführt werden. Für eine VPX-Instanz, die mit dedizierten Kernen erstellt wurde, wird eine zusätzliche CPU für die Verwaltung zugewiesen.

Instanz-Verwaltung

Sie können einen Admin-Benutzer für die VPX-Instanz erstellen, indem Sie **Instanzverwaltung hinzufügen** unter **Instanzverwaltung**auswählen.



Fügen Sie die folgenden Details hinzu:

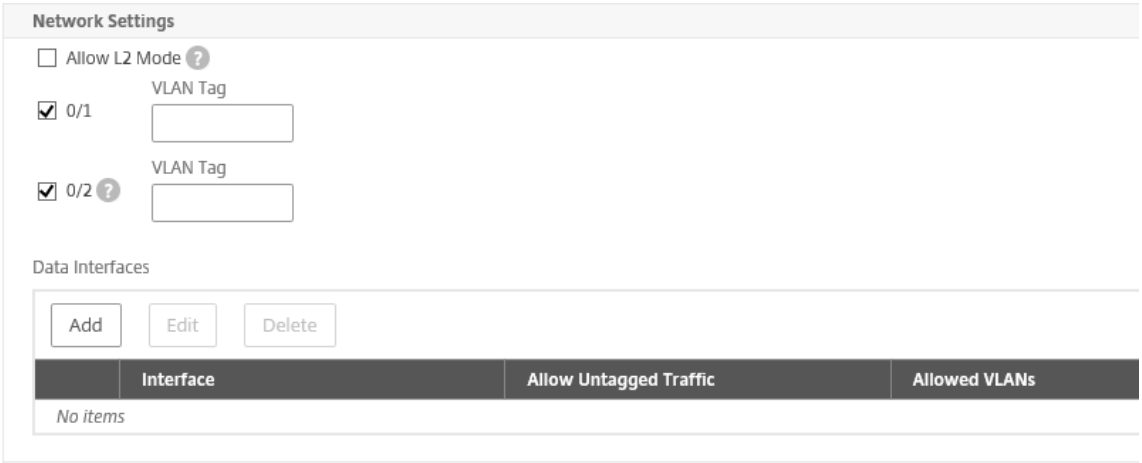
Benutzername: Der Benutzername für den NetScaler-Instanzadministrator. Dieser Benutzer hat Superuser-Zugriff, hat aber keinen Zugriff auf Netzwerkbefehle zum Konfigurieren von VLANs und Schnittstellen.

Kennwort: Das Kennwort für den Benutzernamen.

Shell/Sftp/Scp Access: Der Zugriff, der dem NetScaler-Instanzadministrator gewährt wird. Diese Option ist standardmäßig ausgewählt.

Netzwerkeinstellungen

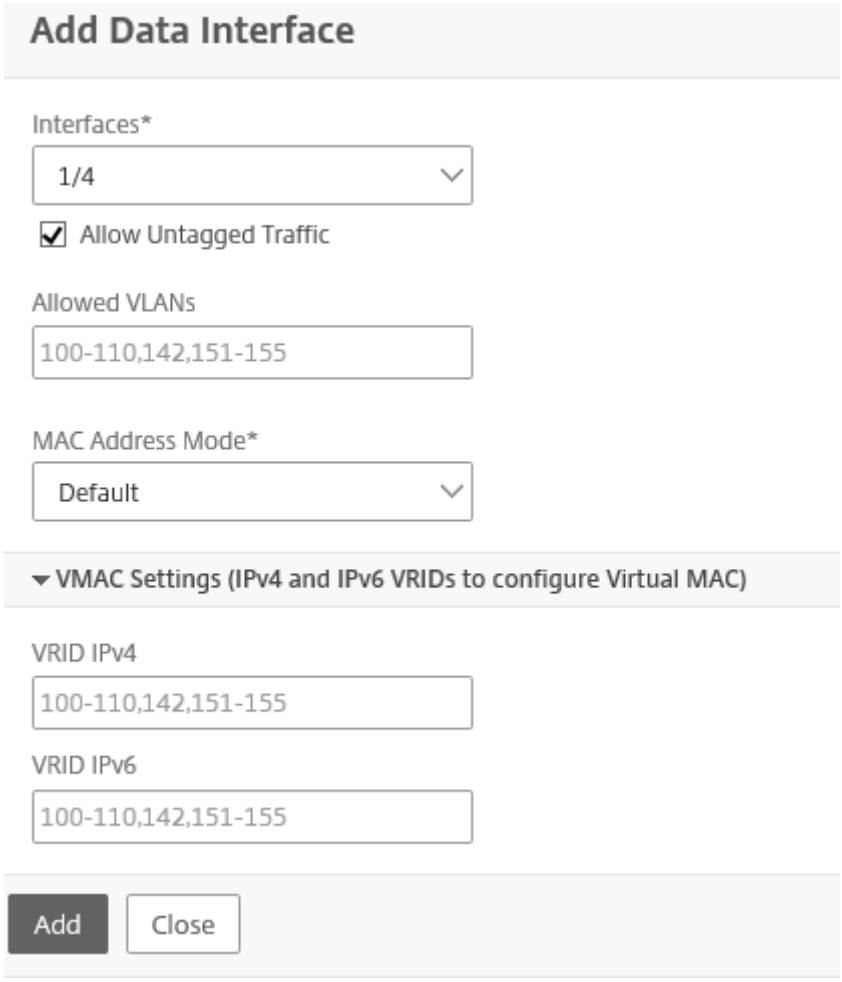
- **L2-Modus zulassen:** Sie können den L2-Modus auf der NetScaler-Instanz zulassen. Wählen Sie unter **Netzwerkeinstellungen** die Option **L2-Modus zulassen**aus. Bevor Sie sich bei der Instanz anmelden und den L2-Modus aktivieren. Weitere Informationen finden Sie unter Zulassen des L2-Modus auf einer NetScaler-Instanz.



> **Hinweis:**
>
> – Wenn Sie den L2-Modus für eine Instanz über den Management Service deaktivieren, müssen Sie sich bei der Instanz anmelden und den L2-Modus von dieser Instanz aus deaktivieren. Andernfalls werden möglicherweise alle anderen NetScaler-Modi nach dem Neustart der Instanz deaktiviert
> – Nachdem eine ADC-Instanz auf SDX bereitgestellt wurde, können Sie keine Schnittstelle oder einen Kanal aus der ADC-Instanz löschen. Sie können der ADC-Instanz jedoch eine Schnittstelle oder einen Kanal hinzufügen.

- **Schnittstelle 0/1 und 0/2:** Standardmäßig sind die Schnittstellen 0/1 und 0/2 für Management-LA ausgewählt.
- **VLAN-Tag:** Geben Sie eine VLAN-ID für die Managementschnittstelle an. Als Nächstes fügen Sie Datenschnittstellen hinzu.

> **Hinweis**:
>
> Die Schnittstellen-IDs von Schnittstellen, die Sie einer Instanz hinzufügen, entsprechen nicht unbedingt der physischen Schnittstellennummerierung auf der SDX-Appliance. Wenn das erste Interface, das Sie mit Instanz 1 verknüpfen, das Interface 1/4 ist, wird es als Schnittstelle 1/1 angezeigt, wenn Sie die Schnittstelleneinstellungen auf der Instanz anzeigen. Die Nummerierung ändert sich, da es sich um die erste Schnittstelle handelt, die Sie mit Instanz 1 verknüpft haben.



- Verkehr**ohne Tags zulassen: Aktivieren Sie das Kontrollkästchen Verkehrohne Tags zulassen, damit die NetScaler-Instanz den unmarkierten** Datenverkehr verarbeiten kann.

  > **Hinweis:**
  >
  > Wenn die SDX-Appliance-Version 13.1-24.x oder höher ist und die NetScaler-Instanzversion vor 13.1-24.x liegt, verarbeitet die ADC-Instanz den unmarkierten Verkehr auf den Mellanox-Schnittstellen, auch wenn das Kontrollkästchen **Allow untagged traffic** deaktiviert ist.

- **Zulässige VLANs:** Geben Sie eine Liste von VLAN-IDs an, die einer NetScaler-Instanz zugeordnet werden können.
- **MAC-Adressmodus:** Weisen Sie eine MAC-Adresse zu. Wählen Sie eine der folgenden Optionen:
  - **Standard:** Citrix Hypervisor weist eine MAC-Adresse zu.
  - **Benutzerdefiniert:** Wählen Sie diesen Modus, um eine MAC-Adresse anzugeben, die die generierte MAC-Adresse überschreibt.
  - **Generiert:** Generieren Sie eine MAC-Adresse mit der zuvor eingestellten Basis-MAC-Adresse. Informationen zum Festlegen einer MAC-Basisadresse finden Sie unter Zuweisen

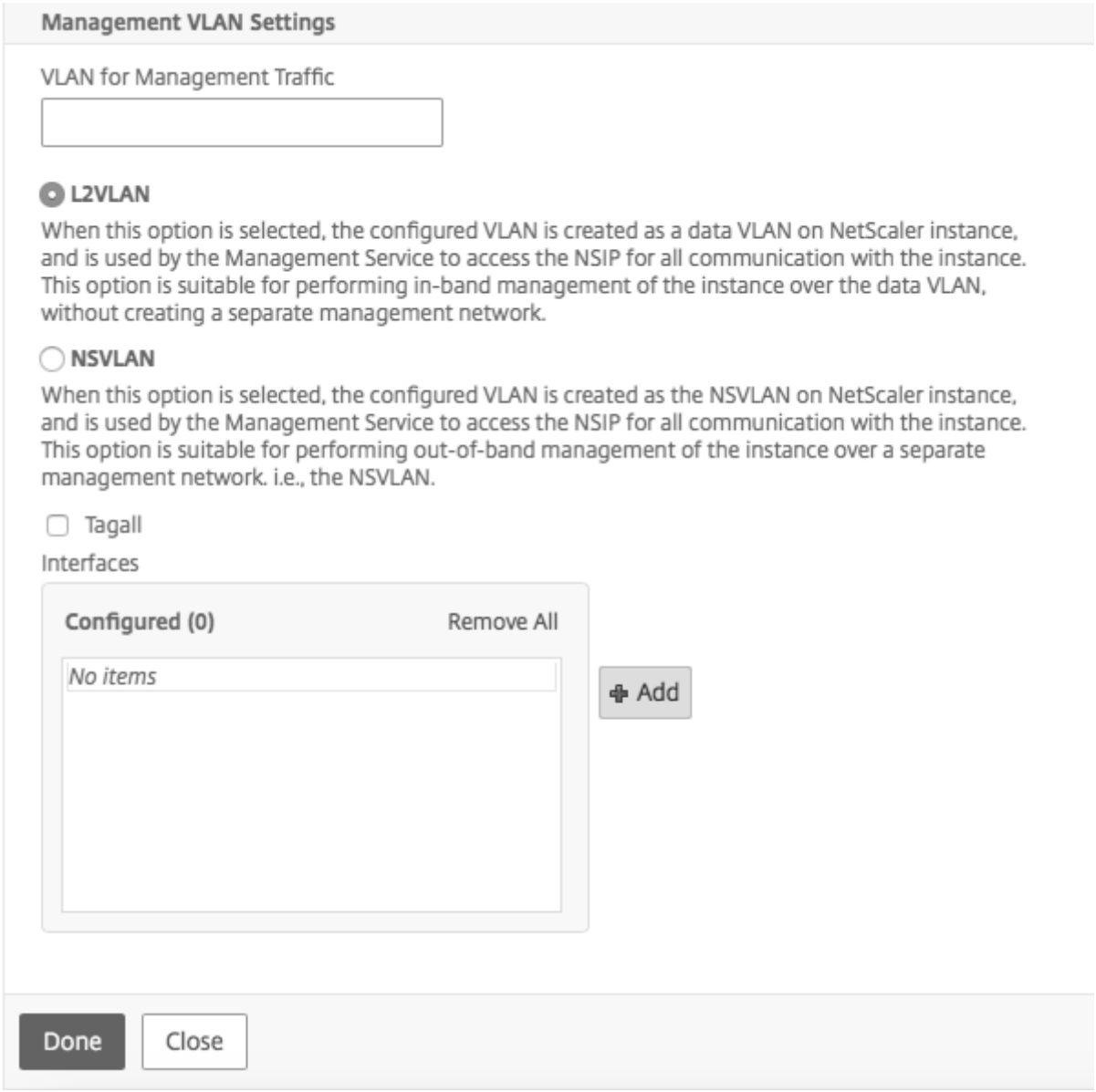
einer MAC-Adresse zu einer Schnittstelle.

- 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 den VMAC identifiziert. Mögliche Werte: 1—255. Weitere Informationen finden Sie unter Konfigurieren von VMACs auf einer Schnittstelle.

Management-VLAN-Einstellungen

In der Regel befinden sich der Management Service und die Verwaltungsadresse (NSIP) der VPX-Instanz im selben Teilnetz, und die Kommunikation erfolgt über eine Verwaltungsschnittstelle. Wenn sich der Management Service und die Instanz jedoch in unterschiedlichen Teilnetzen befinden, müssen Sie zum Zeitpunkt der Bereitstellung einer VPX-Instanz eine VLAN-ID angeben. Diese ID ist erforderlich, damit die Instanz beim Start über das Netzwerk erreicht werden kann. Wenn Ihre Bereitstellung erfordert, dass das NSIP nur über die Schnittstelle zugänglich ist, die zum Zeitpunkt der Bereitstellung der VPX-Instanz ausgewählt wurde, wählen Sie die Option NSVLAN aus.

Wenn die **NSVLAN-Option** ausgewählt ist, können Sie diese Einstellung nicht ändern, nachdem Sie die NetScaler-Instanz bereitgestellt haben.



Hinweis:

- HA-Heartbeats werden nur auf den Schnittstellen gesendet, die Teil des NSVLAN sind.
- Sie können ein NSVLAN nur von VPX XVA Build 9.3 53.4 und höher aus konfigurieren.

Wichtig: Wenn NSVLAN nicht ausgewählt ist, wird durch Ausführen des Befehls „clear config full“auf der VPX-Instanz die VLAN-Konfiguration gelöscht.

Klicken Sie auf **Fertig**, um die NetScaler VPX-Appliance bereitzustellen.

Ändern einer NetScaler-Instanz

Um die Parameterwerte einer bereitgestellten ADC-Instanz zu ändern, wählen Sie im Bereich **NetScaler-Instanzen** die Instanz aus, die Sie ändern möchten, und klicken Sie dann auf **Ändern**. Ändern Sie im ADC-Änderungsassistenten die Parameter.

Zu beachtende Punkte:

- Wenn Sie die folgenden Parameter ändern: Anzahl der SSL-Chips, Schnittstellen, Speicher und Feature-Lizenz, wird die NetScaler-Instanz implizit angehalten und neu gestartet, damit diese Parameter wirksam werden.
- Sie können die Image- und Benutzername-Parameter nicht ändern.
- Schnittstellen oder Kanäle können nicht aus der ADC-Instanz gelöscht werden. Der ADC-Instanz können jedoch neue Schnittstellen oder Kanäle hinzugefügt werden.
- Um eine auf der SDX-Appliance bereitgestellte ADC-Instanz zu entfernen, wählen Sie im Bereich **NetScaler-Instanzen** die Instanz aus, die Sie entfernen möchten, und klicken Sie dann auf **Löschen**. Klicken **Sie im Feld Meldung bestätigen** auf **Ja**, um die NetScaler-Instanz zu entfernen.

Beschränken Sie VLANs auf bestimmte virtuelle Schnittstellen

Der SDX-Appliance-Administrator kann bestimmte 802.1Q-VLANs auf den virtuellen Schnittstellen erzwingen, die mit NetScaler-Instanzen verknüpft sind. Diese Funktion ist besonders hilfreich, um die Verwendung von 802.1Q-VLANs durch die Instanzadministratoren einzuschränken. Wenn zwei Instanzen, die zu zwei verschiedenen Unternehmen gehören, auf einer SDX-Appliance gehostet werden, können Sie die Verwendung derselben VLAN-ID durch die beiden Unternehmen einschränken. Auf diese Weise sieht ein Unternehmen den Verkehr des anderen Unternehmens nicht. Wenn ein Instanzadministrator versucht, einem 802.1Q-VLAN eine Schnittstelle zuzuweisen, wird eine Validierung durchgeführt, um zu überprüfen, ob die angegebene VLAN-ID Teil der zulässigen Liste ist.

Standardmäßig kann jede VLAN-ID auf einer Schnittstelle verwendet werden. Um die markierten VLANs auf einer Schnittstelle einzuschränken, geben Sie die VLAN-IDs bei der Bereitstellung einer NetScaler-Instanz in den Netzwerkeinstellungen an. Sie können es auch später angeben, indem Sie die Instanz ändern. Um einen Bereich anzugeben, trennen Sie die IDs durch einen Bindestrich (z. B. 10—12). Wenn Sie anfänglich einige VLAN-IDs angeben, aber später alle aus der zulässigen Liste löschen, können Sie eine beliebige VLAN-ID auf dieser Schnittstelle verwenden. In der Tat haben Sie die Standardeinstellung wiederhergestellt.

Nach dem Erstellen einer Liste zulässiger VLANs muss sich der SDX-Administrator nicht bei einer Instanz anmelden, um die VLANs zu erstellen. Der Administrator kann VLANs für bestimmte Instanzen aus dem Management Service hinzufügen und löschen.

Wichtig: Wenn der L2-Modus aktiviert ist, muss der Administrator darauf achten, dass sich die VLAN-IDs auf verschiedenen NetScaler-Instanzen nicht überschneiden.

So geben Sie die zulässigen VLAN-IDs an

1. Geben Sie im ADC-Assistenten bereitstellen oder im ADC-Assistenten ändern auf der Seite Netzwerkeinstellungen unter **Zulässige VLANs**eine oder mehrere auf dieser Schnittstelle zulässige VLAN-IDs an. Verwenden Sie einen Bindestrich, um einen Bereich anzugeben. Zum Beispiel 2—4094.
2. Folgen Sie den Anweisungen des Assistenten.
3. Klicken Sie auf **Fertig stellen** und dann auf **Schließen**.

So konfigurieren Sie VLANs für eine Instanz aus dem Management Service

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu NetScaler > Instances.
2. Wählen Sie eine Instanz aus, und klicken Sie dann auf **VLAN**.
3. Klicken Sie im Detailbereich auf **Hinzufügen**.
4. Geben **Sie im Dialogfeld NetScaler-VLAN erstellen** die folgenden Parameter an:
    - VLAN-ID —Eine Ganzzahl, die das VLAN, zu dem ein bestimmter Frame gehört, eindeutig identifiziert. Der NetScaler unterstützt maximal 4094 VLANs. ID 1 ist für das Standard-VLAN reserviert.
    - IPV6 Dynamisches Routing —Aktiviert alle dynamischen IPv6-Routing-Protokolle in diesem VLAN. Hinweis: Damit die **ENABLED-Einstellung** funktioniert, müssen Sie sich bei der Instanz anmelden und die dynamischen IPv6-Routingprotokolle über die VTYSH-Befehlszeile konfigurieren.
5. Wählen Sie die Schnittstellen aus, die Teil des VLAN sein müssen.
6. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Verwalten der Kryptokapazität

November 23, 2023

Ab Version 12.1 48.13 hat sich die Schnittstelle zur Verwaltung der Kryptokapazität geändert. Der Management Service stellt asymmetrische Kryptoeinheiten (ACUs), symmetrische Kryptoeinheiten (SCUs) und virtuelle Kryptoschnittstellen zur Angabe der SSL-Kapazität auf der NetScaler SDX-Appliance bereit. Frühere Kryptokapazität wurde in Einheiten von SSL-Chips, SSL-Kernen und virtuellen SSL-Funktionen zugewiesen. Weitere Informationen darüber, wie Legacy-SSL-Chips in ACU-

und SCU-Einheiten zugeordnet werden, finden Sie in der Konvertierungstabelle für Legacy-SSL-Chips in ACU und SCU.

Mit der Management Service-GUI können Sie der NetScaler VPX-Instanz Kryptokapazität in Einheiten von ACU und SCU zuweisen.

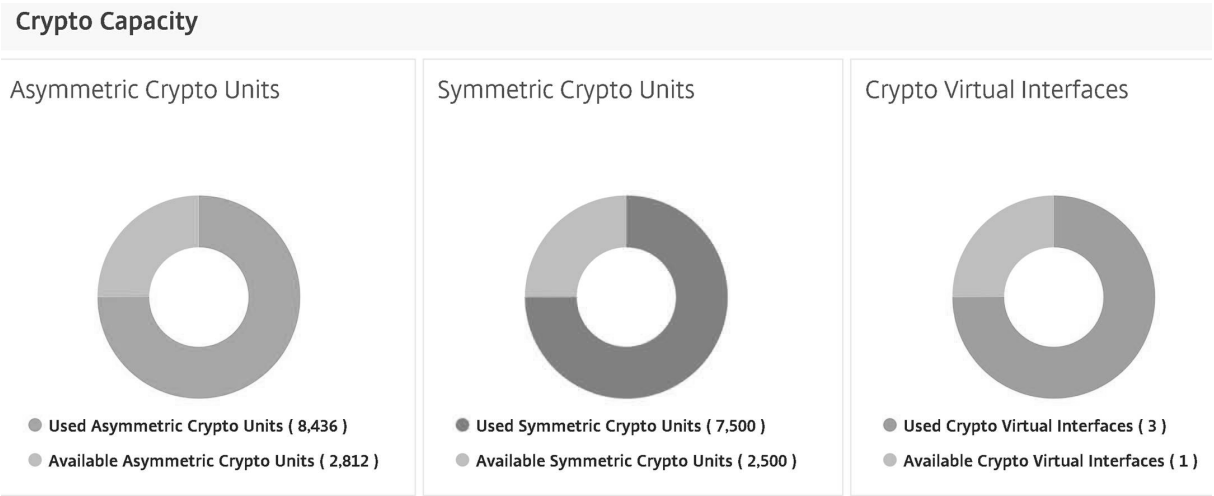
Die folgende Tabelle enthält kurze Beschreibungen zu ACUs, SCUs und virtuellen Krypto-Instanzen.

Tabelle. Krypto-Einheiten

Neue Krypto-Einheiten	Beschreibung
Asymmetrische Kryptoeinheit (ACU)	1 ACU = 1 Vorgang pro Sekunde (ops) der Entschlüsselung mit 2 K (2048-Bit-Schlüsselgröße) (RSA). Weitere Einzelheiten finden Sie unter ACU zu PKE-Ressourcenumrechnungstabelle.
Symmetrische Kryptoeinheit (SCU)	1 SCU = 1 Mbit/s AES-128-CBC + SHA256-HMAC bei 1024 B. Diese Definition gilt für alle SDX-Plattformen.
Virtuelle Krypto-Schnittstellen	Virtuelle Krypto-Schnittstellen, auch virtuelle Funktionen genannt, stellen die Grundeinheit der SSL-Hardware dar. Nachdem diese Schnittstellen erschöpft sind, kann die SSL-Hardware nicht weiter einer VPX-Instanz zugewiesen werden. Virtuelle Krypto-Schnittstellen sind schreibgeschützte Entitäten, und die SDX-Appliance weist diese Entitäten automatisch zu.

Kryptokapazität der SDX-Appliance anzeigen

Sie können die Kryptokapazität der SDX-Appliance im Dashboard der SDX-GUI anzeigen. Das Dashboard zeigt die verwendeten und verfügbaren ACUs, SCUs und virtuellen Schnittstellen auf der SDX-Appliance an. Um die Krypto-Kapazität anzuzeigen, navigieren Sie zu **Dashboard > Krypto-Kapazität**.



Weisen Sie Kryptokapazität zu, während Sie die VPX-Instanz bereitstellen

Bei der Bereitstellung einer VPX-Instanz auf der SDX-Appliance können Sie unter **Crypto Allocation**die Anzahl der ACUs und SCUs für die VPX-Instanz zuweisen. Anweisungen zur Bereitstellung einer VPX-Instanz finden Sie unter Provisioning NetScaler-Instanzen.

Gehen Sie folgendermaßen vor, um während der Bereitstellung einer VPX-Instanz Kryptokapazität zuzuweisen.

1. Melden Sie sich beim Management Service an.
2. Navigieren Sie zu **Konfiguration > NetScaler > Instanzen**, und klicken Sie auf **Hinzufügen**.
3. Unter **Crypto Allocation**können Sie die verfügbaren ACUs, SCU und virtuellen Krypto-Schnittstellen anzeigen. Die Art der Zuweisung von ACUs und SCUs ist je nach SDX-Appliance unterschiedlich:

   a. Für die unter Mindestwert eines für verschiedene SDX-Appliances verfügbaren ACU-Zählers aufgeführten Applianceskönnen Sie ACUs in Vielfachen einer angegebenen Anzahl zuweisen. SCUs werden automatisch zugewiesen und das SCU-Zuweisungsfeld kann nicht bearbeitet werden. Sie können die ACU-Zuweisung um das Vielfache der für dieses Modell verfügbaren Mindest-ACU erhöhen. Wenn die minimale ACU beispielsweise 4375 beträgt, beträgt das ACU-Inkrement 8750, 13125 usw.

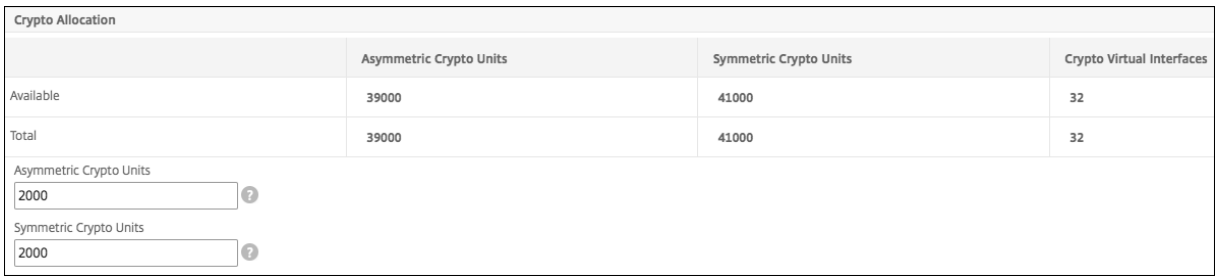
   Beispiel. Krypto-Zuweisung, bei der SCUs automatisch zugewiesen werden und ACUs in Vielfachen einer bestimmten Anzahl zugewiesen werden.

Mindestwert eines ACU-Zählers für verschiedene SDX-Appliances

SDX-Plattform	Minimalwert des ACU-Zählers
22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 Anschlüsse	2187
8400, 8600, 8010, 8015	2812
17500, 19500, 21500	2812
17550, 19550, 20550, 21550	2812
11500, 13500, 14500, 16500, 18500, 20500	2812
11515, 11520, 11530, 11540, 11542	4375
14xxx	4375
14xxx 40S	4375
14xxx 40G	4375
14xxx FIPS	4375
25xxx	4375
25xxx A	4575

b. Für die übrigen SDX-Plattformen, die in der vorherigen Tabelle nicht aufgeführt sind, können Sie ACUs und SCUs frei zuweisen. Die SDX-Appliance weist automatisch virtuelle Krypto-Schnittstellen zu.

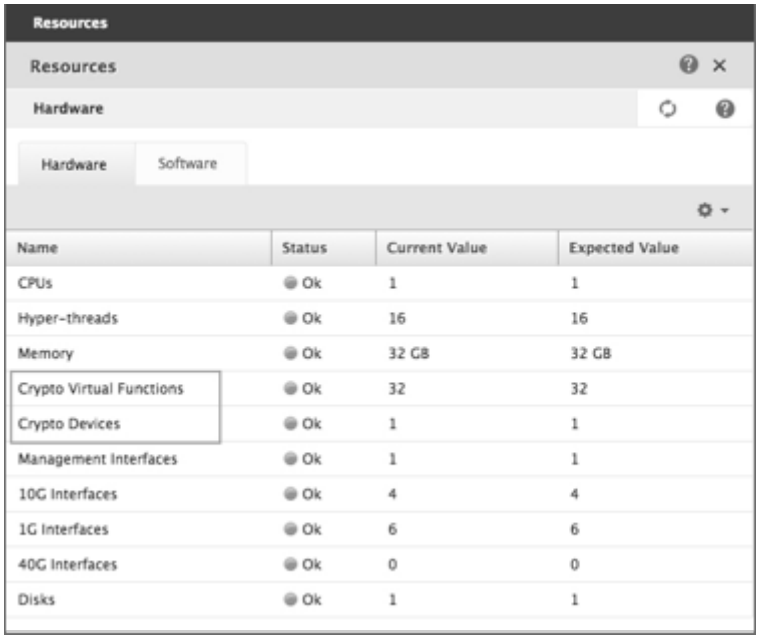
Beispiel. Krypto-Zuweisung, bei der sowohl ACU als auch SCUs frei zugewiesen sind



4./ Führen Sie alle Schritte zum Bereitstellen der VPX-Instanz aus und klicken Sie auf **Fertig**. Weitere Informationen finden Sie unter Provisioning NetScaler-Instances.

Zustand der Krypto-Hardware anzeigen

Im Management Service können Sie den Zustand der mit der SDX-Appliance bereitgestellten Krypto-Hardware anzeigen. Der Zustand der Krypto-Hardware wird als Crypto Devices und Crypto Virtual Functions dargestellt. Um den Zustand der Krypto-Hardware anzuzeigen, navigieren Sie zu **Dashboard > Ressourcen**.



Wichtige Hinweise

Beachten Sie die folgenden Punkte, wenn Sie die SDX-Appliance auf die neueste Version aktualisieren.

- Nur die SDX-Benutzeroberfläche wird aktualisiert, die Hardwarekapazität der Appliance bleibt jedoch unverändert.
- Der Krypto-Zuweisungsmechanismus bleibt derselbe, und nur die Darstellung auf der SDX-GUI ändert sich.
- Die Krypto-Schnittstelle ist abwärtskompatibel und hat keinen Einfluss auf vorhandene Automatisierungsmechanismen, die die NITRO-Schnittstelle zur Verwaltung der SDX-Appliance verwenden.
- Bei einem Upgrade der SDX-Appliance ändert sich das Krypto, das den vorhandenen VPX-Instanzen zugewiesen ist, nicht; es ändert sich nur die Darstellung im Management Service.

ACU zu PKE-Ressourcenumrechnungstabelle

SDX-Plattform	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 Anschlüsse)	2187	12497	2187	312	256	190
8400, 8600, 8010, 8015	2812	17000	2812	424	330	–
11515, 11520, 11530, 11540, 11542	4375	25000	4375	625	512	381
22040, 22060, 22080.22100, 22120 (24 Anschlüsse)	4375	25000	4375	625	512	381
17500, 19500, 21500	2812	17000	2812	424	330	–
17550, 19550, 20550, 21550	2812	17000	2812	424	330	–
11500, 13500, 14500, 16500, 18500, 20500	2812	17000	2812	424	330	–

SDX-Plattform	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
14000, 14000-40G, 25000, 25000A	4375	25000	4375	625	512	381
14000 FIPS	4375	25000	4375	625	512	381
14000-40S	4375	25000	4375	625	512	381
*8900 (8910, 8920, 8930)	1000	4615	1000	136	397	494
*9100 (9110, 9120, 9130)	1000	4615	1000	136	397	494
*26000-100G (26100, 26160, 26200 und 26250)	1000	4615	1000	136	397	494
*15000	1000	4615	1000	136	397	494
*15000-50G	1000	4615	1000	136	397	494
*16000	1000	4615	1000	136	397	494
*26000-50S	1000	4615	1000	136	397	494

*Auf diesen Plattformen sind die PKE-Zahlen die garantierten Mindestwerte.

Wie liest man die ACU zu PKE-Ressourcenumrechnungstabelle

Die ACU in PKE-Ressourcenumrechnungstabelle basiert auf den folgenden Punkten:

- Der Management Service hilft bei der Zuweisung von Crypto-Ressourcen zu jedem einzelnen VPX. Der Management Service kann keine Leistung zuweisen oder versprechen.
- Die tatsächliche Leistung variiert je nach Paketgröße, verwendeter Verschlüsselung/Keyex/H-MAC (oder deren Varianten) usw.

Das folgende Beispiel hilft Ihnen zu verstehen, wie Sie die ACU lesen und auf die PKE-Ressourcenumrechnungstabel anwenden.

Beispiel. ACU auf PKE-Ressourcenumwandlung für die SDX 22040-Plattform

Die Zuweisung von 2187 ACUs zu einer VPX-Instanz auf einer SDX 22040-Plattform weist Kryptoressourcen zu, die 256 ECDHE-RSA-Operationen oder 2187 RSA-2K-Operationen usw. entsprechen.

Legacy-SSL-Chips in ACU- und SCU-Konvertier

Weitere Informationen darüber, wie ältere SSL-Chips in ACU und SCU umgewandelt werden, finden Sie in der folgenden Tabelle.

ACU- und SCU-Umrechnungstabelle

Bereitstellen virtueller Maschinen von Drittanbietern

November 23, 2023

> **Warnung:**
>
> Die Unterstützung **von Drittanbieter-Instances** ist in der NetScaler SDX-GUI ab Version 13.1 Build 37.x veraltet. Wenn Sie weiterhin die Instanzen von Drittanbietern verwenden möchten, empfiehlt Citrix, dass Sie die folgenden Vorgänge ausführen:
>
> - Melden Sie sich bei der Management Service Shell an.
> - Erstellen Sie eine Datei `.thirdPartyVM` im Verzeichnis `/mpsconfig`.
> - Starten Sie den Management Service neu, indem Sie den Befehl `svmd restart` ausführen.

Die SDX-Appliance unterstützt die Bereitstellung der folgenden virtuellen Maschinen (Instanzen) von Drittanbietern:

- SECUREMATRIX GSB
- InterScan Web Security
- Websense Protektor
- BlueCat DNS-/DHCP-Server
- CA Access Gateway
- PaloAlto VM-Serie

SECUREMATRIX GSB bietet ein hochsicheres Kennwortsystem, das den Transport von Token-Geräten überflüssig macht. Websense Protector bietet Überwachungs- und Blockierungsfunktionen, um Datenverlust und den Verlust vertraulicher Informationen zu verhindern. BlueCat DNS/DHCP-Server liefert DNS und DHCP für Ihr Netzwerk. Die PaloAlto VM-Serie auf NetScaler SDX ermöglicht die Konsolidierung erweiterter Sicherheits- und ADC-Funktionen auf einer einzigen Plattform für sicheren und zuverlässigen Zugriff auf Anwendungen für Unternehmen und Service Provider-Kunden. Die

Kombination der VM-Serie auf NetScaler SDX bietet außerdem eine vollständige, validierte und sichere ADC-Lösung für Citrix Virtual Apps and Desktops-Bereitstellungen.

Sie können eine Instanz über den Management Service bereitstellen, überwachen, verwalten und Fehler beheben. Alle vorhergehenden Instanzen von Drittanbietern verwenden den `SDXTools`-Daemon, um mit dem Management Service zu kommunizieren. Der Daemon ist auf der bereitgestellten Instanz vorinstalliert. Sie können den Daemon aktualisieren, wenn neue Versionen verfügbar sind.

Wenn Sie virtuelle Maschinen von Drittanbietern konfigurieren, werden SR-IOV-Schnittstellen (1/x und 10/x), die Teil eines Kanals sind, nicht in der Liste der Schnittstellen angezeigt. Die Schnittstellen fehlen, da Kanäle auf virtuellen Maschinen von Drittanbietern nicht unterstützt werden.

> **Hinweis:**
>
> Die Gesamtzahl der Instanzen, die Sie auf einer SDX-Appliance bereitstellen können, hängt von der auf der Appliance installierten Lizenz ab.

Wichtig: Sie müssen Ihre Citrix Hypervisor Version auf Version 6.1.0 aktualisieren, bevor Sie eine Instanz eines Drittanbieters installieren.

SECUREMATRIX GSB

November 23, 2023

SECUREMATRIX ist eine hochsichere, tokenlose Einmalkennwort-Authentifizierungslösung (OTP), die einfach zu bedienen und kostengünstig ist. Es verwendet eine Kombination aus Position, Sequenz und Bildmuster aus einer Matrixtabelle, um ein Einwegkennwort zu generieren. Der SECUREMATRIX GSB-Server mit SECUREMATRIX Authentication Server verbessert die Sicherheit von VPN/SSL-VPN-Endpunkten, Cloud-basierten Anwendungen und Ressourcen, Desktop-/virtueller Desktop-Anmeldung und Webanwendungen (Reverse-Proxy mit OTP) erheblich. Es bietet eine Lösung, die mit PCs, virtuellen Desktops, Tablets und Smartphones kompatibel ist.

Unter Verwendung der NetScaler SDX-Plattformarchitektur für mehrere Mandanten in einem softwaredefinierten Netzwerk kann die starke Authentifizierungsfunktion von SECUREMATRIX in andere Mandanten oder Cloud-Dienste integriert werden, die über den NetScaler bereitgestellt werden, wie z. B. das Webinterface, Citrix Virtual Apps and Desktops und viele andere Anwendungsdienste, die eine Authentifizierung erfordern.

Weitere Informationen finden Sie unter SECUREMATRIX.

Bereitstellen einer SECUREMATRIX GSB-Instanz

SECUREMATRIX GSB erfordert einen SECUREMATRIX Authentifizierungsserver, der außerhalb der SDX-Appliance konfiguriert werden muss Wählen Sie genau eine Schnittstelle aus und geben Sie die Netzwerkeinstellungen nur für diese Schnittstelle an.

Hinweis: SR-IOV-Schnittstellen (1/x und 10/x), die Teil eines Kanals sind, werden nicht in der Liste der Schnittstellen angezeigt. Kanäle werden auf einer SECUREMATRIX GSB-Instanz nicht unterstützt.

Laden Sie ein XVA-Image von der SECUREMATRIX Website herunter und laden Sie es auf die SDX-Appliance hoch, bevor Sie mit der Bereitstellung der Instanz beginnen. Weitere Informationen zum Herunterladen eines XVA-Images finden Sie auf der SECUREMATRIX-Website. Stellen Sie sicher, dass Sie Management Service Build 118.7 oder höher auf der SDX-Appliance verwenden.

Navigieren Sie auf der Registerkarte **Konfiguration** zu **SECUREMATRIX GSB > Software-Images**.

So laden Sie ein XVA-Image auf die SDX-Appliance hoch:

1. Klicken Sie im Detailbereich unter **XVA Files > Action**auf **Hochladen**.
2. Klicken Sie in dem daraufhin angezeigten Dialogfeld auf **Durchsuchen**und wählen Sie dann die XVA-Datei aus, die Sie hochladen möchten.
3. Klicken Sie auf **Upload**. Die XVA-Datei wird im Bereich XVA-Dateien angezeigt.

Bereitstellen einer SECUREMATRIX-Instanz

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **SECUREMATRIX GSB > Instanzen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Folgen Sie im **Assistenten SECUREMATRX GSB bereitstellen**den Anweisungen auf dem Bildschirm.
4. Klicken Sie auf **Fertig stellen** und dann auf **Schließen**.

Nachdem Sie die Instanz bereitgestellt haben, melden Sie sich bei der Instanz an und führen Sie eine detaillierte Konfiguration durch. Weitere Informationen finden Sie auf der SECUREMATRIX-Website
.

Um die Einstellungen einer bereitgestellten SECUREMATRIX-Instanz zu ändern, wählen Sie im Bereich **SECUREMATRIX Instanzen** die Instanz aus, die Sie ändern möchten, und klicken Sie dann auf **Ändern**. Ändern Sie im Assistenten SECUREMATRIX GSB ändern die Parameter.

Hinweis: Wenn Sie einen der Schnittstellenparameter oder den Namen der Instanz ändern, wird die Instanz gestoppt und neu gestartet, damit die Änderungen wirksam werden.

Generieren Sie ein Tar-Archiv für die Einreichung an den technischen Support. Informationen zum Generieren einer Datei für den technischen Support finden Sie unter Generieren eines Tar-Archivs für den technischen Support.

Erstellen Sie ein Backup der Konfiguration einer SECUREMATRIX GSB-Instanz und verwenden Sie später die Backupdaten, um die Konfiguration der Instanz auf der SDX-Appliance wiederherzustellen. Informationen zum Backup und Wiederherstellen einer Instanz finden Sie unter Backup und Wiederherstellen der Konfigurationsdaten der SDX-Appliance.

Überwachen einer SECUREMATRIX GSB-Instanz

Die SDX-Appliance sammelt Statistiken wie die Version von `SDXTools`, die Zustände von SSH- und CRON-Daemons und den Webserver-Status einer SECUREMATRIX GSB-Instanz.

So zeigen Sie die Statistiken zu einer SECUREMATRIX GSB-Instanz an:

1. Navigieren Sie zu **SECUREMATRIX GSB > Instanzen**
2. Klicken Sie im Detailbereich auf den Pfeil neben dem Namen der Instanz.

Verwalten einer SECUREMATRIX GSB-Instanz

Sie können eine SECUREMATRIX GSB-Instanz über den Management Service starten, stoppen, neu starten, stoppen oder einen Neustart erzwingen.

Erweitern Sie auf der Registerkarte **KonfigurationSECUREMATRIX GSB**.

So starten, stoppen, starten, beenden oder erzwingen Sie einen Neustart einer Instanz:

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, für die Sie den Vorgang ausführen möchten, und wählen Sie dann eine der folgenden Optionen aus:
   - Starten
   - Herunterfahren
   - Neu starten
   - Herunterfahren erzwingen
   - Neustart erzwingen
3. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Aktualisieren Sie die SDX Tools-Datei für eine SECUREMATRIX GSB-Instanz

`SDXTools`, ein Daemon, der auf der SECUREMATRIX GSB-Instanz läuft, wird für die Kommunikation zwischen dem Management Service und der Instanz verwendet.

Beim Upgrade von `SDXTools` wird die Datei auf die SDX-Appliance hochgeladen und nach Auswahl einer Instanz wird das Upgrade von `SDXTools` durchgeführt. Sie können eine `SDXTools`-Datei von einem Clientcomputer auf die SDX-Appliance hochladen.

So laden Sie eine SDXTools-Datei hoch:

1. Erweitern Sie im Navigationsbereich **Management Service** und klicken Sie dann auf **SDXTools Files**.
2. Wählen Sie im Detailbereich in der Liste **Aktion** die Option **Hochladen**aus.
3. Klicken Sie im Dialogfeld **SDXTools-Dateien hochladen** auf **Durchsuchen**, navigieren Sie zu dem Ordner, der die Datei enthält, und doppelklicken Sie dann auf die Datei.
4. Klicken Sie auf **Upload**.

Um SDXTools zu aktualisieren:

Erweitern Sie auf der Registerkarte **KonfigurationSECUREMATRIX GSB**.

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich eine Instanz aus.
3. Wählen Sie in der Liste **Aktion** die Option **SDXTools aktualisieren**aus.
4. Wählen Sie im Dialogfeld **SDXTools aktualisieren** eine Datei aus, klicken Sie auf **OK**, und klicken Sie dann auf **Schließen**.

Upgrade und Downgrade einer SECUREMATRIX GSB-Instanz

Beim Aktualisieren der SECUREMATRIX GSB-Instanz wird das Software-Image des Ziel-Builds auf die SDX-Appliance hochgeladen und anschließend die Instanz aktualisiert. Beim Downgrade wird eine frühere Version der Instanz geladen.

Erweitern Sie auf der Registerkarte **KonfigurationSECUREMATRIX GSB**.

So laden Sie das Software-Image hoch:

1. Klicken Sie auf **Software-Images**.
2. Wählen Sie im Detailbereich in der Liste **Aktion** die Option **Hochladen**aus.
3. Klicken Sie im Dialogfeld auf **Durchsuchen**, navigieren Sie zu dem Ordner, der die Build-Datei enthält, und doppelklicken Sie dann auf die Build-Datei.
4. Klicken Sie auf **Upload**.

So aktualisieren Sie die Instanz:

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich eine Instanz aus.
3. Wählen Sie in der Liste **Aktion** die Option **Upgrade**aus.
4. Wählen Sie im daraufhin angezeigten Dialogfeld eine Datei aus, klicken Sie auf **OK**, und klicken Sie dann auf **Schließen**.

So stufen Sie eine Instanz herunter:

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich eine Instanz aus.
3. Wählen Sie in der Liste **Aktion** die Option **Herabstufen**aus.
4. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Problembehandlung bei einer SECUREMATRIX GSB-Instanz

Pingen Sie eine SECUREMATRIX GSB-Instanz über den Management Service an, um zu überprüfen, ob das Gerät erreichbar ist. Sie können die Route eines Pakets vom Management Service zu einer Instanz verfolgen, um die Anzahl der Hops zu ermitteln, die zum Erreichen der Instanz erforderlich sind.

Ermitteln Sie eine Instanz erneut, um den neuesten Status und die Konfiguration einer Instanz anzuzeigen. Während der Wiedererkennung ruft der Management Service die Konfiguration und die Version des SECUREMATRIX GSB ab, die auf der SDX-Appliance ausgeführt wird. Standardmäßig plant der Management Service alle 30 Minuten Instanzen für die erneute Erkennung.

Erweitern Sie auf der Registerkarte **KonfigurationSECUREMATRIX GSB**.

So pingen Sie eine Instanz:

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, die Sie pingen möchten, und klicken Sie in der Liste **Aktion** auf **Ping**. Das Feld Pingmessage zeigt an, ob der Ping erfolgreich war.

So verfolgen Sie die Route einer Instanz:

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, für die Sie die Route verfolgen möchten, und klicken Sie in der Liste **Aktion** auf **TraceRoute**. Das Traceroute-Meldungsfeld zeigt die Route zur Instanz an.

Rediscovery einer Instanz:

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, die Sie erneut ermitteln möchten, und klicken Sie in der Liste **Aktion** auf **Rediscover**.
3. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Trend Micro InterScan Web Security

November 23, 2023

Trend Micro InterScan Web Security ist eine virtuelle Software-Appliance, die dynamisch vor traditionellen und neuen Internet-Bedrohungen am Internet-Gateway schützt. Es integriert Anwendungssteuerung, Anti-Malware-Scan, Web Reputation in Echtzeit, flexible URL-Filterung und erweiterten Bedrohungsschutz. Dadurch bietet es überragenden Schutz und bessere Transparenz und Kontrolle über die zunehmende Nutzung von Cloud-basierten Anwendungen im Netzwerk. Echtzeitberichte und zentrales Management bieten Ihren Administratoren ein proaktives Entscheidungstool, das das Risikomanagement vor Ort ermöglicht.

InterScan Web Security:

- Ermöglicht tieferen Einblick in die Internetaktivitäten der Endbenutzer
- Zentralisiert das Management für maximale Kontrolle
- Überwacht die Internetnutzung wie es passiert
- Ermöglicht eine Sanierung vor Ort
- Reduziert die Geräteausbreitung und die Energiekosten
- Bietet optionalen Schutz vor Datenverlust und Sandbox-Ausführungsanalyse

Bevor Sie eine InterScan Web Security-Instanz bereitstellen können, müssen Sie ein XVA-Image von der Trend Micro Website herunterladen. Nachdem Sie das XVA-Image heruntergeladen haben, laden Sie es auf die NetScaler SDX-Appliance hoch.

Hinweis: SR-IOV-Schnittstellen (1/x und 10/x), die Teil eines Kanals sind, werden nicht in der Liste der Schnittstellen angezeigt. Kanäle werden auf einer InterScan Web Security-Instanz nicht unterstützt.

So laden Sie ein XVA-Image auf die SDX-Appliance hoch:

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **TrendMicro IWSVA > Software-Images**.
2. Klicken Sie im Detailbereich unter der Registerkarte **XVA-Dateien** auf **Hochladen**.
3. Klicken Sie in dem daraufhin angezeigten Dialogfeld auf **Durchsuchen**und wählen Sie dann die XVA-Datei aus, die Sie hochladen möchten.
4. Klicken Sie auf **Upload**. Die XVA-Datei wird im Bereich XVA-Dateien angezeigt.

So stellen Sie eine TrendMicro IWSVA-Instanz bereit:

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **TrendMicro IWSVA > Instanzen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Befolgen Sie im **Provisioning TrendMicro IWSVA-Assistenten** die Anweisungen auf dem Bildschirm.
4. Klicken Sie auf **OK** und dann auf **Schließen**.

Nachdem Sie die Instanz bereitgestellt haben, melden Sie sich bei der Instanz an und führen Sie die detaillierte Konfiguration durch.

Um die Werte der Parameter einer bereitgestellten Instanz zu ändern, wählen Sie im Detailbereich die Instanz aus, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**. Stellen **Sie im Assistenten TrendMicro IWSVA modifizieren** die Parameter auf Werte ein, die für Ihre Umgebung geeignet sind.

Websense Protektor

November 23, 2023

Der Websense (jetzt als Forcepoint bekannt) Data Security Protector ist eine virtuelle Maschine, die ausgehenden HTTP-Verkehr (Posts) abfängt. Anschließend analysiert es den Datenverkehr, um Datenverlust und das Eindringen sensibler Daten über das Internet zu verhindern. Der Schutz kommuniziert mit einem dedizierten Windows-Server, um DLP-Richtlinieninformationen zu erhalten, und kann die Veröffentlichung von Daten überwachen oder blockieren, wenn eine Übereinstimmung erkannt wird. Die Inhaltsanalyse wird auf der Box durchgeführt, sodass während dieses Vorgangs keine sensiblen Daten den Schutz verlassen.

Gehen Sie wie folgt vor, um die Funktionen des Protectors Data Loss Prevention (DLP) zu nutzen:

- Websense Data Security kaufen und installieren
- Konfigurieren von Web-DLP-Richtlinien im Datensicherheitsmanager
- Führen Sie die Ersteinrichtung über den Management Service durch.

Weitere Informationen finden Sie auf der Websense Protector-Website .

Bereitstellen einer Websense Protector-Instanz

Für den Websense© Protector ist ein Data Security Management Server erforderlich, der außerhalb der SDX-Appliance konfiguriert werden muss. Wählen Sie genau eine Verwaltungsschnittstelle und zwei Datenschnittstellen aus. Für die Datenschnittstellen müssen Sie L2-Modus zulassen auswählen. Stellen Sie sicher, dass auf den Data Security Management Server über das Verwaltungsnetzwerk des Websense-Schutzes zugegriffen werden kann. Geben Sie für den Nameserver die IP-Adresse des Domainnamenservers (DNS) ein, der diesen Schutz bedient.

Hinweis: SR-IOV-Schnittstellen (1/x und 10/x), die Teil eines Kanals sind, werden nicht in der Liste der Schnittstellen angezeigt. Kanäle werden auf einer Websense-Protector-Instanz nicht unterstützt.

Laden Sie ein Protector-Image von der Websense-Website herunter und laden Sie es auf die SDX-Appliance hoch, bevor Sie mit der Bereitstellung der Instanz beginnen. Weitere Informationen zum Herunterladen eines Protector-Images finden Sie auf der [Websense]-Website. Stellen Sie sicher, dass Sie Management Service Build 118.7 oder höher auf der SDX-Appliance verwenden.

Navigieren Sie auf der Registerkarte **Konfiguration** zu **Websense Protector > Software-Images**.

So laden Sie ein XVA-Image auf die SDX-Appliance hoch

1. Klicken Sie im Detailbereich unter **XVA Files > Action**auf **Hochladen**.
2. Klicken Sie in dem daraufhin angezeigten Dialogfeld auf Durchsuchenund wählen Sie dann die XVA-Datei aus, die Sie hochladen möchten.
3. Klicken Sie auf **Upload**. Die XVA-Datei wird im Bereich XVA-Dateien angezeigt.

So stellen Sie eine Websense Protector-Instanz bereit

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Websense Protector > Instanzen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Folgen Sie im Assistenten **Websense Protector bereitstellen** den Anweisungen auf dem Bildschirm.
4. Klicken Sie auf **Fertig stellen** und dann auf **Schließen**.

Nachdem Sie die Instanz bereitgestellt haben, melden Sie sich bei der Instanz an und führen Sie die detaillierte Konfiguration durch.

Um die Einstellungen einer bereitgestellten Websense Protector-Instanz zu ändern, wählen Sie im Bereich Websense Protector-Instanzen die Instanz aus, die Sie ändern möchten, und klicken Sie dann auf **Ändern**. Stellen Sie im Assistenten Websense Protector ändern die Parameter ein. Ändern Sie nicht die Schnittstellen, die zum Zeitpunkt der Bereitstellung einer Websense-Instanz ausgewählt wurden. Die XVA-Datei kann erst geändert werden, nachdem Sie die Instanz gelöscht und eine neue bereitgestellt haben.

Sie können ein Tar-Archiv erstellen, das Sie beim technischen Support einreichen können. Informationen zum Generieren einer Datei für den technischen Support finden Sie unter Generieren eines Tar-Archivs für den technischen Support.

Überwachen einer Websense Protector-Instanz

Die SDX-Appliance sammelt Statistiken wie die Version von `SDXTools`, den Status der Websense©-Datensicherheitsrichtlinien-Engine und den Proxy-Status der Datensicherheit.

So zeigen Sie die Statistiken zu einer Websense Protector-Instanz an:

1. Navigieren Sie zu **Websense Protector > Instanzen**.
2. Klicken Sie im Detailbereich auf den Pfeil neben dem Namen der Instanz.

Verwalten einer Websense Protector-Instanz

Sie können eine Websense© Protector-Instanz über den Management Service starten, stoppen, neu starten, stoppen oder einen Neustart erzwingen.

Erweitern Sie auf der Registerkarte **KonfigurationWebsense Protector**.

So starten, stoppen, starten, beenden oder erzwingen Sie einen Neustart einer Websense Protector-Instanz

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, für die Sie den Vorgang ausführen möchten, und wählen Sie dann eine der folgenden Optionen aus:
   - Starten
   - Herunterfahren
   - Neu starten
   - Herunterfahren erzwingen
   - Neustart erzwingen
3. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Aktualisieren Sie die SDX Tools-Datei für eine Websense Protector-Instanz

`SDXTools`, ein Daemon, der auf der Drittanbieterinstanz läuft, wird für die Kommunikation zwischen dem Management Service und der Drittanbieter-Instanz verwendet.

Beim Upgrade von `SDXTools` wird die Datei auf die SDX-Appliance hochgeladen und nach Auswahl einer Instanz wird das Upgrade von `SDXTools` durchgeführt. Sie können eine `SDXTools`-Datei von einem Clientcomputer auf die SDX-Appliance hochladen.

So laden Sie eine SDX Tools-Datei hoch

1. Erweitern Sie im Navigationsbereich **Management Service** und klicken Sie dann auf **SDXTools Files**.
2. Wählen Sie im Detailbereich in der Liste **Aktion** die Option **Hochladen**aus.
3. Klicken Sie im Dialogfeld **SDXTools-Dateien hochladen** auf **Durchsuchen**, navigieren Sie zu dem Ordner, der die Datei enthält, und doppelklicken Sie dann auf die Datei.
4. Klicken Sie auf **Upload**.

So aktualisieren Sie SDX-Tools

Erweitern Sie auf der Registerkarte **Konfiguration**
Websense Protector.

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich eine Instanz aus.
3. Wählen Sie in der Liste **Aktion** die Option **SDXTools aktualisieren**aus.
4. Wählen Sie im Dialogfeld **SDXTools aktualisieren** eine Datei aus, klicken Sie auf **OK**, und klicken Sie dann auf **Schließen**.

Aktualisieren Sie die Websense Protector-Instanz auf eine neuere Version

Beim Aktualisieren der Websense© Protector-Instanz wird das Software-Image des Ziel-Builds auf die SDX-Appliance hochgeladen und anschließend die Instanz aktualisiert.

Erweitern Sie auf der Registerkarte **KonfigurationWebsense Protector**.

So laden Sie das Software-Image hoch

1. Klicken Sie auf **Software-Images**.
2. Wählen Sie im Detailbereich in der Liste **Aktion** die Option **Hochladen**aus.
3. Klicken Sie im Dialogfeld auf **Durchsuchen**, navigieren Sie zu dem Ordner, der die Build-Datei enthält, und doppelklicken Sie dann auf die Build-Datei.
4. Klicken Sie auf **Upload**.

So aktualisieren Sie die Instanz

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich eine Instanz aus.
3. Wählen Sie in der Liste **Aktion** die Option **Upgrade**aus.
4. Wählen Sie im daraufhin angezeigten Dialogfeld eine Datei aus, klicken Sie auf **OK**, und klicken Sie dann auf **Schließen**.

Problembehandlung bei einer Websense Protector-Instanz

Pingen Sie eine Websense Protector-Instanz über den Management Service an, um zu überprüfen, ob das Gerät erreichbar ist. Sie können die Route eines Pakets vom Management Service zu einer Instanz verfolgen, um die Anzahl der Hops zu ermitteln, die zum Erreichen der Instanz erforderlich sind.

Ermitteln Sie eine Instanz erneut, um den neuesten Status und die Konfiguration einer Instanz anzuzeigen. Während der Wiedererkennung ruft der Management Service die Konfiguration und die Version des Websense-Schutzes ab, der auf der SDX-Appliance ausgeführt wird. Standardmäßig plant der Management Service alle 30 Minuten Instanzen für die erneute Erkennung.

Erweitern Sie auf der Registerkarte **KonfigurationWebsense Protector**.

So pingen Sie eine Instanz

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, die Sie pingen möchten, und klicken Sie in der Liste **Aktion** auf **Ping**. Das Feld Pingmessage zeigt an, ob der Ping erfolgreich war.

So verfolgen Sie die Route einer Instanz

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, für die Sie die Route verfolgen möchten, und klicken Sie in der Liste **Aktion** auf **TraceRoute**. Das Traceroute-Meldungsfeld zeigt die Route zur Instanz an.

So entdecken Sie eine Instanz

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, die Sie erneut ermitteln möchten, und klicken Sie in der Liste **Aktion** auf **Rediscover**.
3. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

BlueCat DNS/DHCP

November 23, 2023

BlueCat DNS/DHCP Server™ ist eine Softwarelösung, die von der NetScaler SDX-Appliance unterstützt wird. Es wird auf der NetScaler SDX-Plattform gehostet, um zuverlässige, skalierbare und sichere DNS- und DHCP-Kernnetzwerkdienste bereitzustellen, ohne dass zusätzliche Verwaltungskosten oder Speicherplatz im Rechenzentrum anfallen. Kritische DNS-Dienste können über mehrere DNS-Knoten innerhalb eines einzigen Systems oder über mehrere SDX-Appliances verteilt werden, ohne dass mehr Hardware erforderlich ist.

Virtuelle Instanzen von BlueCat DNS/DHCP Server™ können auf SDX gehostet werden, um mobile Geräte, Anwendungen, virtuelle Umgebungen und Clouds intelligenter zu verbinden.

Um mehr über BlueCat und Citrix zu erfahren, besuchen Sie die BlueCat-Website unter https://citrixready.citrix.com/bluecat-networks.html.

Wenn Sie bereits BlueCat Kunde sind, können Sie Software und Dokumentation über das BlueCat-Supportportal unter herunterladen https://care.bluecatnetworks.com/.

Provisioning einer BlueCat DNS/DHCP-Instanz

Laden Sie ein XVA-Image vom BlueCat Customer Care unter herunter https://care.bluecatnetworks.com. Nachdem Sie das XVA-Image heruntergeladen haben, laden Sie es auf die SDX-Appliance hoch, bevor Sie mit der Bereitstellung der Instanz beginnen. Stellen Sie sicher, dass Sie Management Service Build 118.7 oder höher auf der SDX-Appliance verwenden.

Verwaltungskanal über 0/1- und 0/2-Schnittstellen werden auf BlueCat DNS/DHCP-VMs unterstützt. Weitere Informationen finden Sie unter Kanal über den Management Service konfigurieren.

Hinweis: SR-IOV-Schnittstellen (1/x und 10/x), die Teil eines Kanals sind, werden nicht in der Liste der Schnittstellen angezeigt, da Kanäle auf einer BlueCat DNS/DHCP-Instanz nicht unterstützt werden.

Navigieren Sie auf der Registerkarte **Konfiguration** zu **BlueCat DNS/DHCP > Software-Images**.

Um ein XVA-Image auf die SDX-Appliance hochzuladen:

1. Klicken Sie im Detailbereich unter **XVA Files > Action**auf **Hochladen**.
2. Klicken Sie in dem daraufhin angezeigten Dialogfeld auf **Durchsuchen**und wählen Sie dann die XVA-Datei aus, die Sie hochladen möchten.
3. Klicken Sie auf **Upload**. Die XVA-Datei wird im Bereich XVA-Dateien angezeigt.

So stellen Sie eine BlueCat DNS/DHCP-Instanz bereit:

1. Navigieren Sie auf der Registerkarte Konfiguration zu BlueCat DNS/DHCP > Instanzen.
2. Klicken Sie im Detailbereich auf “Hinzufügen”. Die Seite BlueCat DNS/DHCP-Server bereitstellen wird geöffnet.
3. Folgen Sie im Assistenten BlueCat DNS/DHCP bereitstellen den Anweisungen auf dem Bildschirm.

    - Geben Sie unter Instanzerstellung im Feld Name einen Namen für die Instanz ein und wählen Sie das hochgeladene Image aus dem Dropdown-Menü XVA-Datei aus. Klicken Sie dann auf Weiter. Geben Sie optional im Feld Domainname einen Domainnamen für die Instanz ein.
      Hinweis: Der Name darf keine Leerzeichen enthalten.

- Wählen Sie unter Netzwerkeinstellungen im Dropdown-Menü Verwaltungsschnittstelle die Schnittstelle aus, über die die Instanz verwaltet werden soll, und legen Sie die IP-Adresse und das Gateway für diese Schnittstelle fest. Sie können Schnittstellen explizit für Hochverfügbarkeit und Service zuweisen. Wählen Sie die Parameter aus und klicken Sie dann auf **Weiter**.

  Hinweis: Achten Sie beim Zuweisen von Schnittstellen für Management, Hochverfügbarkeit und Service darauf, dass Sie die Schnittstellen basierend auf der unterstützten Schnittstellenkombination zuweisen:

Sie können für alle drei dieselbe Schnittstelle wählen.
Sie können für alle drei eine andere Schnittstelle wählen.
Sie können dieselbe Schnittstelle für Verwaltung und Service auswählen, aber eine andere Schnittstelle für Hochverfügbarkeit auswählen.
Klicken Sie auf **Fertig stellen** und dann auf **Schließen**. Die Instanz wird erstellt, gebootet und mit der ausgewählten IP-Adresse konfiguriert.

Nachdem Sie die Instanz bereitgestellt haben, melden Sie sich über SSH bei der Instanz an, um die Konfiguration abzuschließen. Einzelheiten zur Konfiguration des BlueCat DNS/DHCP-Servers oder zum Platzieren unter der Kontrolle des BlueCat Address Managers finden Sie in der BlueCat-Dokumentation unter https://care.bluecatnetworks.com.

Um die Einstellungen einer BlueCat DNS/DHCP-Server-Instanz zu ändern, wählen Sie im Bereich **BlueCat DNS/DHCP-Instanzen** die Instanz aus, die Sie ändern möchten, und klicken Sie dann auf **Ändern**. Ändern Sie im Assistenten BlueCat DNS/DHCP ändern die Parametereinstellungen.

Hinweis: Wenn Sie einen der Schnittstellenparameter oder den Namen der Instanz ändern, wird die Instanz angehalten und neu gestartet, damit die Änderungen wirksam werden.

Überwachen einer BlueCat DNS/DHCP-Instanz

Die SDX-Appliance sammelt Statistiken, z. B. die Version von `SDXTools`, das auf der Instanz ausgeführt wird, einer BlueCat DNS/DHCP-Instanz.

So zeigen Sie die Statistiken zu einer BlueCat DNS/DHCP-Instanzan:

1. Navigieren Sie zu BlueCat DNS/DHCP > Instanzen.
2. Klicken Sie im Detailbereich auf den Pfeil neben dem Namen der Instanz.

Verwalten einer BlueCat DNS/DHCP-Instanz

Sie können eine BlueCat DNS/DHCP-Instanz über den Management Service starten, stoppen, neu starten, stoppen oder einen Neustart erzwingen.

Erweitern Sie auf der Registerkarte **Konfiguration** den Bereich **BlueCat DNS/DHCP**.

Um eine BlueCat DNS/DHCP-Instanz zu starten, zu stoppen, neu zu starten, zu stoppen, zu erzwingen oder einen Neustartzu erzwingen:

1. Klicke auf Instanzen.
2. Wählen Sie im Detailbereich die Instanz aus, für die Sie den Vorgang ausführen möchten, und wählen Sie dann eine der folgenden Optionen aus:
   - Starten
   - Herunterfahren
   - Neu starten
   - Herunterfahren erzwingen
   - Neustart erzwingen
3. Klicken Sie im Feld Meldung bestätigen auf Ja.

Aktualisieren Sie die Datei SDXTools für eine BlueCat DNS/DHCP-Instanz

SDXTools, ein Daemon, der auf der Drittanbieterinstanz läuft, wird für die Kommunikation zwischen dem Management Service und der Drittanbieter-Instanz verwendet.

Beim Upgrade von SDXTools wird die Datei auf die SDX-Appliance hochgeladen und nach Auswahl einer Instanz wird das Upgrade von SDXTools durchgeführt. Sie können eine SDXTools-Datei von einem Clientcomputer auf die SDX-Appliance hochladen.

Um eine SDXTools-Datei hochzuladen:

1. Erweitern Sie im Navigationsbereich **Management Service** und klicken Sie dann auf **SDXTools Files**.
2. Wählen Sie im Detailbereich in der Liste **Aktion** die Option **Hochladen**aus.
3. Klicken Sie im Dialogfeld **SDXTools-Dateien hochladen** auf **Durchsuchen**, navigieren Sie zu dem Ordner, der die Datei enthält, und doppelklicken Sie dann auf die Datei.
4. Klicken Sie auf **Upload**.

Um SDXTools zu aktualisieren:

Erweitern Sie auf der Registerkarte **Konfiguration** den Bereich **BlueCat DNS/DHCP**.

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich eine Instanz aus.
3. Wählen Sie in der Aktionsliste die Option **SDXTools aktualisieren**aus.
4. Wählen Sie im Dialogfeld **SDXTools aktualisieren** eine Datei aus, klicken Sie auf **OK**, und klicken Sie dann auf **Schließen**.

Entdecken Sie eine BlueCat DNS/DHCP-Instanz neu

Sie können eine Instanz erneut entdecken, um den neuesten Status und die Konfiguration einer Instanz anzuzeigen. Während der Wiederermittlung ruft der Management Service die Konfiguration ab. Standardmäßig plant der Management Service Instanzen für die erneute Erkennung aller Instanzen alle 30 Minuten.

Erweitern Sie auf der Registerkarte **Konfiguration** den Bereich **BlueCat DNS/DHCP**.

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, die Sie erneut ermitteln möchten, und klicken Sie in der Liste **Aktion** auf **Rediscover**.
3. Klicken **Sie im Feld Meldung bestätigen** auf **Ja**.

CA Access Gateway

November 23, 2023

CA Access Gateway ist ein skalierbarer, verwaltbarer und erweiterbarer Standalone-Server, der eine proxybasierte Lösung für die Zugriffssteuerung bietet. CA Access Gateway verwendet eine Proxy-Engine, die ein Netzwerk-Gateway für das Unternehmen bereitstellt und mehrere Sitzungsschemata unterstützt, die nicht auf herkömmlicher Cookie-basierter Technologie basieren.

Der eingebettete Webagent ermöglicht Single Sign-On (SSO) im gesamten Unternehmen. CA Access Gateway bietet Zugriffssteuerung für HTTP- und HTTPS-Anfragen und SSO ohne Cookies. Das Produkt speichert außerdem Sitzungsinformationen im In-Memory-Sitzungsspeicher. Proxy-Regeln definieren, wie das CA Access Gateway Anforderungen an Ressourcen auf Zielservern innerhalb des Unternehmens weiterleitet oder umleitet.

Durch die Bereitstellung eines einzigen Gateways für Netzwerkressourcen trennt CA Access Gateway das Unternehmensnetzwerk und zentralisiert die Zugriffssteuerung.

Hinweis: SR-IOV-Schnittstellen (1/x und 10/x), die Teil eines Kanals sind, werden nicht in der Liste der Schnittstellen angezeigt, da Kanäle auf einer CA Access Gateway-Instanz nicht unterstützt werden. Weitere Informationen zu den Funktionen von CA Access Gateway finden Sie in der Dokumentation zu diesem Produkt.

Bereitstellen einer CA Access Gateway-Instanz

Bevor Sie eine CA Access Gateway-Instanz bereitstellen können, müssen Sie ein XVA-Image herunterladen. Nachdem Sie das XVA-Image heruntergeladen haben, laden Sie es auf die SDX-Appliance hoch.

Stellen Sie sicher, dass Sie Management Service Version 10.5 Build 52.3.e oder höher auf der SDX-Appliance verwenden. Um ein CA Access Gateway bereitzustellen, müssen Sie zuerst das XVA-Image auf die SDX-Appliance hochladen und dann eine Instanz bereitstellen.

So laden Sie ein XVA-Image auf die SDX-Appliance hoch:

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **CA Access Gateway** > **Software-Images**.
2. Klicken Sie im Detailbereich unter **XVA-Dateien**in der Dropdownliste **Aktion** auf **Hochladen**.
3. Klicken Sie in dem daraufhin angezeigten Dialogfeld auf **Durchsuchen**und wählen Sie dann die XVA-Datei aus, die Sie hochladen möchten.
4. Klicken Sie auf **Upload**. Die XVA-Datei wird im Bereich **XVA-Dateien** angezeigt.

Bereitstellen einer CA Access Gateway-Instanz:

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **CA Access Gateway**> **Instanzen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Befolgen Sie im Assistenten “CA Access Gateway bereitstellen”die Anweisungen auf dem Bildschirm.
4. Klicken Sie auf **Fertig stellen** und dann auf **Schließen**.

Nachdem Sie die Instanz bereitgestellt haben, melden Sie sich bei der Instanz an und führen Sie die detaillierte Konfiguration durch.

Um die Werte der Parameter einer bereitgestellten Instanz zu ändern, wählen Sie im Detailbereich die Instanz aus, die Sie ändern möchten, und klicken Sie dann auf **Ändern**. Stellen Sie im Assistenten CA Access Gateway modifizieren die Parameter auf Werte ein, die für Ihre Umgebung geeignet sind.

Hinweis:

Wenn Sie einen der Schnittstellenparameter oder den Namen der Instanz ändern, wird die Instanz angehalten und neu gestartet, um die Änderung in Kraft zu setzen.

Eine CA Access Gateway-Instanz überwachen

Die SDX-Appliance sammelt Statistiken, z. B. die Version von, die auf der Instanz `SDXTools` ausgeführt wird, einer CA Access Gateway-Instanz.

So zeigen Sie die Statistiken zu einer CA Access Gateway-Instanz an:

1. Navigieren Sie zu **CA Access Gateway > Instanzen**.
2. Klicken Sie im Detailbereich auf den Pfeil neben dem Namen der Instanz.

Verwalten einer CA Access Gateway-Instanz

Sie können eine CA Access Gateway-Instanz über den Management Service starten, stoppen, neu starten, beenden oder einen Neustart erzwingen. Gehen Sie folgendermaßen vor, um diese Aufgaben abzuschließen:

1. Erweitern Sie auf der Registerkarte **KonfigurationCA Access Gateway**.
2. Navigieren Sie zu **CA Access Gateway > Instanzen**.
3. Wählen Sie im Detailbereich die Instanz aus, für die Sie den Vorgang ausführen möchten, und wählen Sie dann eine der folgenden Optionen aus:
    - Starten
    - Herunterfahren
    - Neu starten
    - Herunterfahren erzwingen
    - Neustart erzwingen
4. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Palo Alto Networks VM-Series

November 23, 2023

Die virtuellen Firewalls der VM-Serie von Palo Alto Networks verwenden denselben PAN-OS-Funktionsumfang, der in den physischen Sicherheitsgeräten des Unternehmens verfügbar ist und alle wichtigen Netzwerksicherheitsfunktionen bereitstellt. Die VM-Serie auf NetScaler SDX ermöglicht die Konsolidierung erweiterter Sicherheits- und ADC-Funktionen auf einer einzigen Plattform für sicheren und zuverlässigen Zugriff auf Anwendungen für Unternehmen, Geschäftsbereiche und Service Provider-Kunden. Die Kombination der VM-Serie auf NetScaler SDX bietet außerdem eine vollständige, validierte Sicherheits- und ADC-Lösung für Citrix Virtual Apps and Desktops-Bereitstellungen.

Sie können eine Instanz über den Management Service bereitstellen, überwachen, verwalten und Fehler beheben.

Zu beachtende Punkte:

- Die Gesamtzahl der Instanzen, die Sie auf einer SDX-Appliance bereitstellen können, hängt von den verfügbaren SDX-Hardwareressourcen ab.
- SR-IOV-Schnittstellen (1/x und 10/x), die Teil eines Kanals sind, werden nicht in der Liste der Schnittstellen angezeigt, da Kanäle von einer Instanz der Palo Alto VM-Serie nicht unterstützt

werden. Weitere Informationen zur Palo Alto Network VM-Serie finden Sie in der Palo Alto Network-Dokumentation.

Bereitstellen einer Instanz der Palo Alto VM-Serie

Bevor Sie eine Instanz der Palo Alto VM-Serie bereitstellen können, müssen Sie ein XVA-Image von der Palo Alto Networks-Websiteherunterladen. Nachdem Sie das XVA-Image heruntergeladen haben, laden Sie es auf die SDX-Appliance hoch.

So laden Sie ein XVA-Image auf die SDX-Appliance hoch:

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **PaloAlto VM-Series > Software-Images**.
2. Klicken Sie im Detailbereich unter **XVA-Dateien**in der Dropdownliste **Aktion** auf **Hochladen**.
3. Klicken Sie in dem daraufhin angezeigten Dialogfeld auf **Durchsuchen**und wählen Sie dann die XVA-Datei aus, die Sie hochladen möchten.
4. Klicken Sie auf **Upload**. Die XVA-Datei wird im Bereich **XVA-Dateien** angezeigt.

So stellen Sie eine Instanz der Palo Alto VM-Serie bereit:

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **PaloAlto VM-Series > Instances**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Folgen Sie im Assistenten PaloAlto VM-Serie bereitstellen den Anweisungen auf dem Bildschirm.
4. Klicken Sie auf **Fertig stellen** und dann auf **Schließen**.

Nachdem Sie die Instanz bereitgestellt haben, melden Sie sich bei der Instanz an und führen Sie die detaillierte Konfiguration durch.

Um die Werte der Parameter einer bereitgestellten Instanz zu ändern, wählen Sie im Detailbereich die Instanz aus, die Sie ändern möchten, und klicken Sie dann auf **Ändern**. Stellen Sie im Assistenten PaloAlto VM-Serie ändern die Parameter auf Werte ein, die für Ihre Umgebung geeignet sind.

Hinweis: Wenn Sie einen der Schnittstellenparameter oder den Namen der Instanz ändern, wird die Instanz angehalten und neu gestartet, um die Änderung in Kraft zu setzen.

Überwachen einer Instanz der Palo Alto VM-Serie

Die SDX-Appliance sammelt Statistiken, z. B. die Version von `SDXTools`, das auf der Instanz ausgeführt wird, einer Instanz der Palo Alto VM-Serie.

So zeigen Sie die Statistiken zu einer Instanz der Palo Alto VM-Serie an:

1. Navigieren Sie zu **PaloAlto VM-Series > Instanzen**.
2. Klicken Sie im Detailbereich auf den Pfeil neben dem Namen der Instanz.

Verwalten einer PaloAlto Instanz der VM-Serie

Sie können eine Instanz der PaloAlto VM-Serie über den Management Service starten, stoppen, neu starten, stoppen oder einen Neustart erzwingen.

Erweitern Sie auf der Registerkarte **Konfiguration** die Option **PaloAlto VM-Series**.

1. Navigieren Sie zu **PaloAlto VM-Series > Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, für die Sie den Vorgang ausführen möchten, und wählen Sie dann eine der folgenden Optionen aus:
   - Starten
   - Herunterfahren
   - Neu starten
   - Herunterfahren erzwingen
   - Neustart erzwingen
3. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Problembehandlung bei einer Instanz der PaloAlto VM-Serie

Pingen Sie eine Instanz der PaloAlto VM-Serie über den Management Service an, um zu überprüfen, ob das Gerät erreichbar ist. Sie können die Route eines Pakets vom Management Service zu einer Instanz verfolgen, um die Anzahl der Hops zu ermitteln, die zum Erreichen der Instanz erforderlich sind.

Ermitteln Sie eine Instanz erneut, um den neuesten Status und die Konfiguration einer Instanz anzuzeigen. Während der Wiedererkennung ruft der Management Service die Konfiguration und die Version der PaloAlto VM-Serie ab, die auf der SDX-Appliance ausgeführt wird. Standardmäßig plant der Management Service alle 30 Minuten Instanzen für die erneute Erkennung.

Erweitern Sie auf der Registerkarte **Konfiguration** die Option **PaloAlto VM-Series**.

So pingen Sie eine Instanz:

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, die Sie pingen möchten, und klicken Sie in der Liste **Aktion** auf **Ping**. Das Feld **Pingmessage** zeigt an, ob der Ping erfolgreich war.

So verfolgen Sie die Route einer Instanz:

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, die Sie pingen möchten, und klicken Sie in der Liste **Aktion** auf **TraceRoute**. Das **Traceroute-Meldungsfeld** zeigt die Route zur Instanz an.

Rediscovery einer Instanz:

1. Klicke auf **Instanzen**.
2. Wählen Sie im Detailbereich die Instanz aus, die Sie erneut ermitteln möchten, und klicken Sie in der Liste **Aktion** auf **Rediscover**.
3. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Citrix SD-WAN VPX-Instanz auf einer NetScaler SDX-Appliance bereitstellen

November 23, 2023

Die Citrix SD-WAN-Technologie wendet softwaredefinierte Netzwerkkonzepte (SDN) auf WAN-Verbindungen an. Die Technologie abstrakt das Verkehrsmanagement und die Überwachung von Netzwerkhardware und wendet sie auf einzelne Anwendungen an. Das Ergebnis ist eine verbesserte Leistung, eine qualitativ hochwertige Benutzererfahrung über geografisch verteilte Standorte und eine vereinfachte Bereitstellung von Wide-Area- und Cloud-Zugriffsnetzwerken. Weitere Informationen finden Sie unter Citrix SD-WAN.

> **Hinweis:** Nur die SD-WAN VPX Standard Edition wird unterstützt. Weitere Informationen finden Sie unter SD-WAN VPX-Editionen.

Das Bereitstellen einer Citrix SD-WAN VPX-Instanz auf einer SDX-Appliance umfasst die folgenden Aufgaben:

- Installieren der Hardware: Stellen Sie sicher, dass die SDX-Hardware ordnungsgemäß installiert ist. Weitere Informationen finden Sie unter Installieren der Hardware.
- Einrichten und Konfigurieren des SDX Management Service. Weitere Informationen finden Sie unterErste Schritte mit der Management Service-Benutzeroberfläche und Konfigurieren des Management Service.
- Provisioning der SD-WAN VPX-Instanz auf der SDX-Appliance. Weitere Informationen finden Sie unter Bereitstellung der Citrix SD-WAN VPX-Instanz auf einem NetScaler SDX.
- Konfiguration der SD-WAN VPX-Instanz. Weitere Informationen finden Sie in den Dokumentationen zur Konfiguration und Konfigurieren des virtuellen Pfaddienstes zwischen dem MCN und Client-Sites.

Voraussetzungen

Stellen Sie sicher, dass Sie über folgende Lizenzen verfügen:

- Citrix SD-WAN VPX-Lizenz
- NetScaler SDX-Plattformlizenz

Anforderungen für Citrix SD-WAN VPX

Das Citrix SD-WAN VPX auf der SDX-Plattform kann sowohl als Site als auch als MCN fungieren. Der MCN kann einen bidirektionalen Durchsatz von 1 Gbit/s und 64 Standorte verarbeiten.

Unterstützter Durchsatz für MCN und Standort

- 250 MB/s bis 1 GB/s bidirektionaler Durchsatz
- MCN unterstützt 64 Standorte

Hardwareanforderung für unterstützten Durchsatz Site

- 4 CPUs bis 16 CPUs
- 4 GB bis 16 GB RAM
- 60 GB bis 250 GB Speicherplatz
- Mindestens 4 Netzwerkkarten: eine für die Verwaltung und die verbleibenden mindestens 3 Netzwerkkarten für den Datenpfad

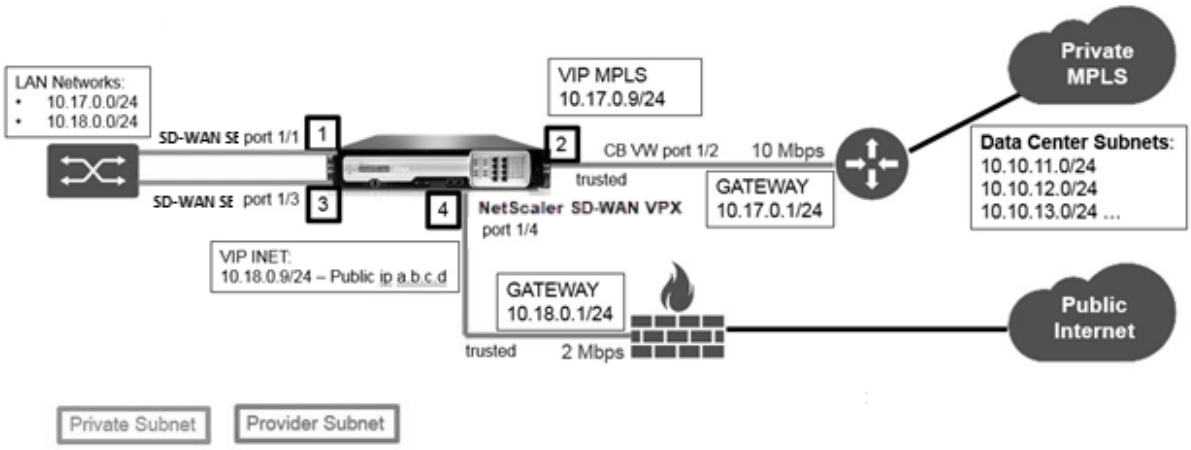
Master-Steuerknoten (MCN)

- 4, 8 und 16 CPUs
- 16 GB RAM
- 250 GB Speicherplatz
- Mindestens 4 Netzwerkkarten: eine für die Verwaltung und die restlichen 3 Netzwerkkarten für den Datenpfad, mit dedizierten NICs für den Datenpfad

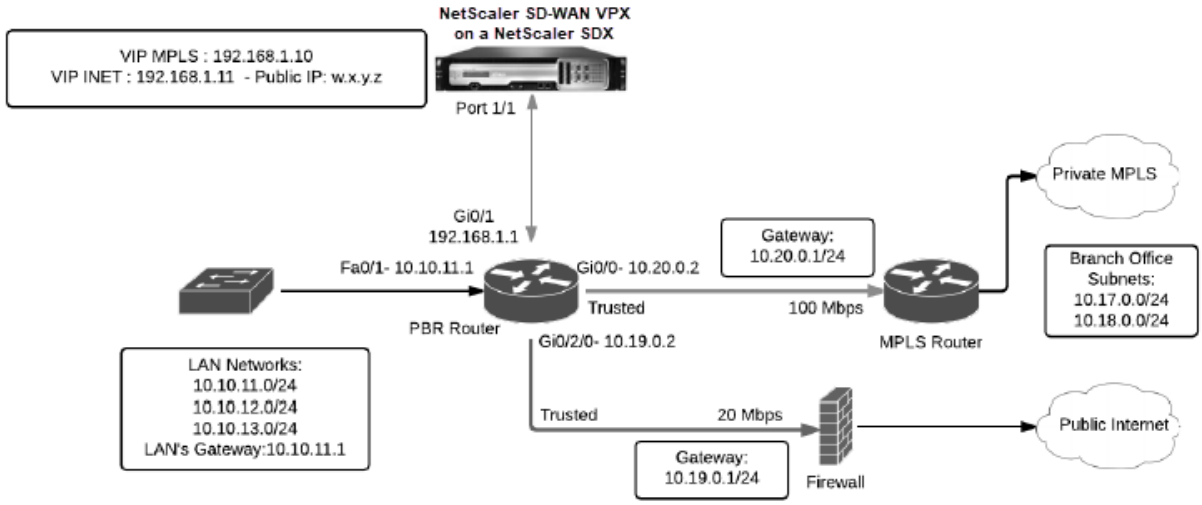
Topologie des Rechenzentrums

Sie können eine Citrix SD-WAN VPX-Appliance auf einem NetScaler SDX im PBR-Modus (Policy-Based Route) oder im Inline-Modus bereitstellen. In Szenario 1 und 2 finden Sie die Topologie des Rechenzentrums für diese beiden unterstützten Modi. Weitere Informationen finden Sie unter Bereitstellen von SD-WAN im virtuellen Inline-Modus).

Szenario 1: Inlinemodus



Szenario 2: PBR-Modus oder virtueller Inline-Modus

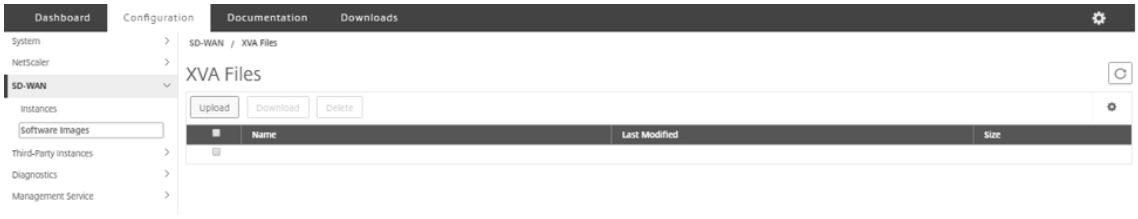


Stellen Sie die Citrix SD-WAN VPX-Instanz auf einem NetScaler SDX bereit

Bevor Sie die Citrix SD-WAN VPX-Appliance bereitstellen, laden Sie das SD-WAN VPX-Image von der NetScaler-Produkt-Download-Site herunter:.
https://www.citrix.com/downloads/netscaler-sd-wan/

Folgen Sie diesen Schritten, um die Citrix SD-WAN VPX-Appliance bereitzustellen.

1. Melden Sie sich bei der NetScaler SDX-Appliance an.
2. Navigieren Sie zu **Konfiguration > SD-WAN > Instanzen**.
3. Wählen Sie **Software-Images > Hochladen** und laden Sie die SD-WAN XVA-Datei hoch.



4. Wählen Sie **Instanzen > Hinzufügen**aus. Die Seite **SD-WAN-Instanz bereitstellen** wird angezeigt.
5. Geben Sie auf der Seite „ **SD-WAN-Instanz bereitstellen** “Folgendes ein:

   a. Name

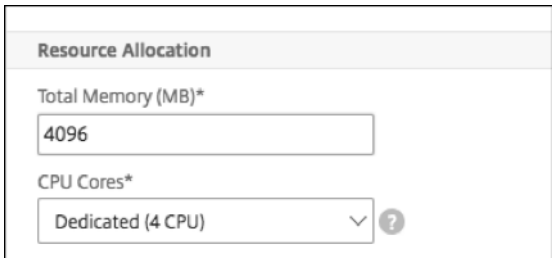
   b. IP-Adresse

   c. Netzmaske

   d. Gateway-Adresse

   e. Laden Sie die XVA-Datei hoch

   f. Weisen Sie unter **Ressourcenzuweisung**Ressourcen zu.



   g. Stellen Sie unter **Netzwerkeinstellungen**Verwaltungsschnittstellen bereit und wählen Sie **OK** zum Erstellen aus, um die SD-WAN VPX-Instanz auf der SDX-Appliance bereitzustellen.

> **Hinweis:** Der SDX Management Service bindet Schnittstellen in aufsteigender Reihenfolge von Schnittstellennamen an die VPX-Instanz. Wenn Sie beispielsweise 1/4 und 1/1 hinzufügen, ordnet Management Service sie als 1/1, 1/4 an.
> Wenn Sie neue Schnittstellen hinzufügen, wird die vorhandene Sequenz beibehalten und eine neue Sequenz wird erstellt. Zum Beispiel fügen Sie die Schnittstellen 1/2, 10/1, 1/3 hinzu. Die neue Sequenz wäre 1/1, 1/4; 1/2, 1/3, 10/1.

6. Die SD-WAN VPX-Instanz wird auf der **Seite Instanz**angezeigt. Hier ist ein Beispiel.

```
1 ![Image](/en-us/sdx/media/sd-wan-vpx-example.png)
```

Um die Instanz zu bearbeiten, navigieren Sie zu **Konfiguration > SD-WAN > Instanzen**. Wählen Sie und klicken Sie auf die Instanz. Wenn Sie die Bearbeitung abgeschlossen haben, klicken Sie auf **OK**, um die Änderungen zu speichern.

Konfigurieren der Citrix SD-WAN VPX-Instanz

Nachdem Sie eine SD-WAN-Instanz auf der SDX-Appliance erstellt haben, konfigurieren Sie die SD-WAN-Instanz, indem Sie die beiden Aufgaben ausführen:

1. Wenden Sie die Konfiguration sowohl für MCN- als auch für Standortgeräte an
2. Konfigurieren Sie den virtuellen Pfad und übertragen Sie den Verkehr.

Weitere Informationen finden Sie in den folgenden Artikeln:

- Konfiguration
- Konfigurieren des virtuellen Pfaddienstes zwischen MCN und Clientsites

Verwandte Informationen

Weitere Informationen zu den ersten Schritten mit einer Citrix SD-WAN-Appliance finden Sie unter Citrix SD-WAN.

Weitere Informationen zur NetScaler SDX Appliance finden Sie unter NetScaler SDX.

Bandbreitenmessung in SDX

February 15, 2024

Die NetScaler SDX-Bandbreitenmessung bietet Ihnen ein genaues, zuverlässiges und benutzerfreundliches Messschema, mit dem Sie Verarbeitungskapazität effizient zuweisen und die Bandbreitennutzung monetarisieren können. Ein Messschema ist erforderlich, um die Bandbreite optimal auf verschiedene Ressourcen zuzuweisen, wobei zu berücksichtigen ist, dass alle Benutzer jederzeit die zugewiesene Bandbreite erhalten.

Die Bandbreitenzuweisung kann in den folgenden zwei Modi erfolgen:

- Dedizierte Bandbreite mit einer festen Durchsatzrate
- Dedizierte Bandbreite mit minimalem gesichertem Durchsatz und Bandbreiten-Burstingfähigkeit

Dedizierte Bandbreite mit einer festen Durchsatzrate

Bei der Bandbreitenzuweisungsmethode wird jeder VPX-Instanz eine dedizierte Bandbreite zugewiesen. Die Instanz darf die Bandbreite bis zum festgelegten Limit nutzen. Im dedizierten Modus sind die zugewiesene minimale und maximale Bandbreite identisch. Wenn die VPX-Instanz während eines Zeitraums mehr Bandbreite als zugewiesen benötigt, kann die Instanz im dedizierten

Modus ihren Durchsatz nicht erhöhen. Dieses Problem kann ein Nachteil sein, wenn eine VPX-Instanz kritische Anforderungen erfüllt.

Wenn eine SDX-Appliance über einige VPX-Instanzen verfügt und einige von ihnen die zugewiesene Bandbreite nicht nutzen, können Sie ihre ungenutzte Bandbreite nicht im dedizierten Modus freigeben. Um all diese Herausforderungen zu bewältigen, ist eine dedizierte Bandbreite mit einer garantierten Mindestrate und der Möglichkeit, die Bandbreite dynamisch zu erhöhen, nützlich.

Dedizierte Bandbreite mit minimalem gesichertem Durchsatz und Bandbreiten-Burstingfähigkeit

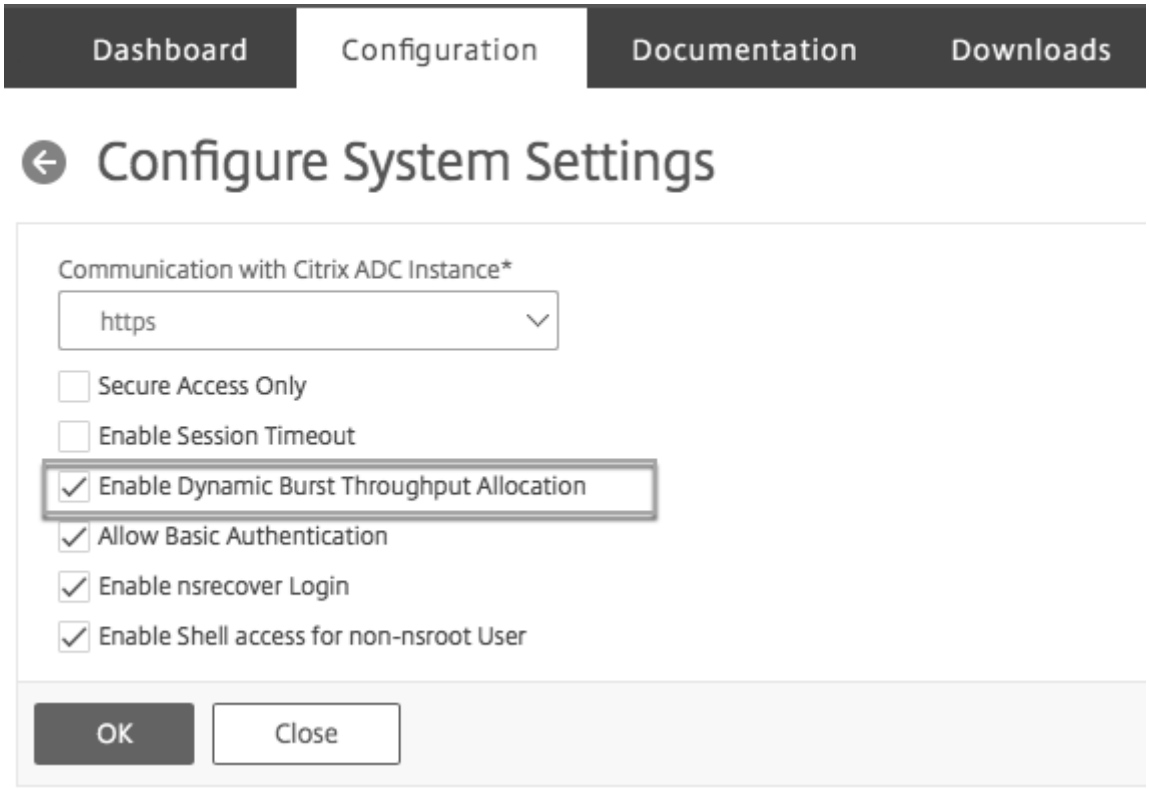
Bei dieser Bandbreitenzuweisungsmethode wird einem VPX eine garantierte Mindestbandbreite mit der Flexibilität zugewiesen, seine Bandbreite bis zu einem vorgegebenen Limit zu erhöhen. Die zusätzliche Bandbreite, die ein VPX nutzen kann, wird als Burst-Kapazität bezeichnet.

Der Vorteil der Burst-Kapazität zeigt sich, wenn Sie einige Instanzen mit zusätzlicher Kapazität und einige VPX mit ungenutzter Kapazität haben. Die zusätzliche Kapazität dieser VPX-Instanzen kann anderen VPX-Instanzen zugewiesen werden, die ihre zugewiesene Bandbreite vollständig genutzt haben und für einige Zeit mehr benötigen. Verschiedene Dienstleister sind auch daran interessiert, ihren Kunden verschiedene Zusatzdienste anzubieten, die dedizierte Kapazität benötigen. Gleichzeitig wollen sie die Bandbreite nicht übertreiben. Eine Burstable-Bandbreite hilft in solchen Szenarien, in denen die Kunden eine bestimmte Bandbreite mit der Option erhalten, die Bandbreite in Zeiten hoher Nachfrage zu erhöhen.

Auswahl des Bandbreitenzuweisungsmodus

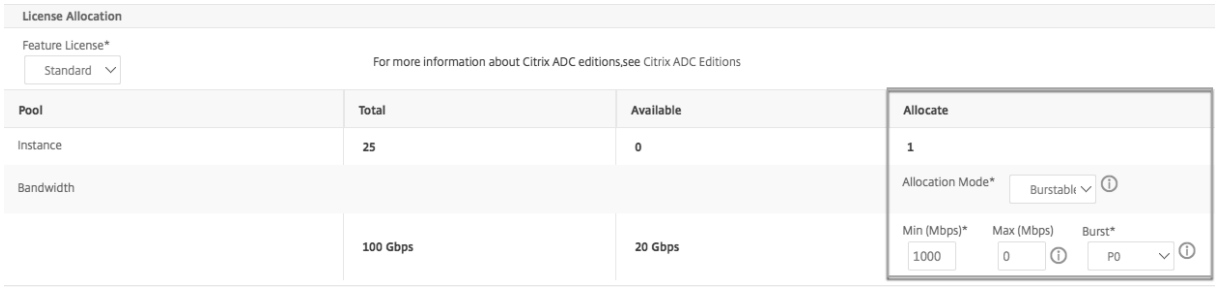
Bevor Sie den Burstable-Durchsatz wählen, müssen Sie die dynamische Burst-Durchsatzzuweisung aktivieren. Gehen Sie folgendermaßen vor, um diese Option zu aktivieren.

1. Navigieren Sie in der SDX Management Console zu **Konfiguration > System**.
2. Wählen Sie in der Gruppe **Systemeinstellungen** die Option **Systemeinstellungen ändern**aus.
3. Klicken Sie auf das Kontrollkästchen **Dynamische Burst-Durchsatzzuweisung** aktivieren, um den dynamischen



Wenn Sie ein VPX bereitstellen, können Sie zwischen Bandbreiten-Burst oder dynamischem Durchsatz wählen.

1. Klicken Sie im **SDX Management Service**auf **Konfiguration > NetScaler > Instances > Hinzufügen**.
2. Die Seite „ **Bereitstellung NetScaler** “wird geöffnet. Wählen Sie unter **Lizenzzuweisung**die Option **Burstable** aus **Zuweisungsmodus**.



Weitere Informationen zur Bereitstellung einer NetScaler-Instanz finden Sie unter Provisioning NetScaler-Instances.

Wenn Sie eine feste Durchsatzrate verwenden möchten, wählen Sie **Fest**aus. Standardmäßig ist der feste Modus für die Bandbreitenzuweisung festgelegt. Es ist nicht erforderlich, dass alle VPX-Instanzen im gleichen Modus arbeiten. Jede VPX-Instanz kann in einem anderen Modus konfiguriert werden.

Hinweis: Wenn Sie SDX von 10.5.e und früheren Versionen migrieren, befinden sich standardmäßig alle VPX-Instanzen im festen Zuweisungsmodus.

Bestimmen der maximalen Burst-Bandbreite für eine VPX-Instanz

Das Ausmaß, in dem jeder VPX platzen darf, wird durch einen Algorithmus berechnet. Wenn Sie ein VPX mit Burstable-Bandbreite bereitstellen, muss jedem dieser VPX eine Priorität eingeräumt werden. Die Zuweisung der Burstable-Bandbreite hängt von dieser Burstpriorität ab Die Priorität variiert von P0 bis P4, wobei P0 die höchste Priorität und P4 die niedrigste ist.

Nehmen wir einen Fall, in dem es 2 VPX gibt, nämlich VPX1 und VPX2. Die minimale Bandbreite, die VPX1 und VPX2 zugewiesen wird, beträgt 4 Gbit/s bzw. 2 Gbit/s mit einer Burstab-Bandbreite von 2 Gbit/s und jeweils 1 Gbit/s. In der folgenden Tabelle sind die Parameter dargestellt:

|VPX-Name|Parameter|Wert|
|–|–|–|
|VPX1|Garantierte Mindestbandbreite|4 Gbit/s
|-|-|Maximale Burstable-Bandbreite|2 Gbit/s
|-|-|Priorität|P0
|VPX2|Minimale garantierte Bandbreite|2 Gbit/s
|-|-|Maximale Burstable-Bandbreite|1 Gbit/s
|-|-|Priorität|P1

Nehmen wir in diesem Fall an, dass die gesamte lizenzierte Bandbreite 8 Gbit/s beträgt. Wenn beide VPX-Instanzen ihre maximalen Burstable-Grenzen erreichen, heißt das:

1. VPX1 verwendet seine maximale Burstable-Bandbreite, dh 2 Gbit/s, dann verwendet es insgesamt 4 + 2 = 6 Gbit/s
2. VPX2 verwendet seine maximale Burstable-Bandbreite, dh 1 Gbit/s, dann verwendet es insgesamt 2 +1 = 3 Gbit/s

In diesem Fall beträgt die maximal genutzte Bandbreite mehr als die lizenzierte Kapazität von 8 Gbit/s. Um die Nutzung auf eine Bandbreite innerhalb der lizenzierten Kapazität zu reduzieren, müsste einer der VPX seine Burstab-Bandbreite aufgeben. Da VPX2 in diesem Fall eine niedrigere Priorität als VPX1 hat, gibt es seine Burstab-Bandbreite von 1 Gbit/s auf. VPX1 würde weiter platzen, da es eine höhere Priorität als VPX2 hat. In all diesen Szenarien wird sichergestellt, dass die garantierte Mindestbandbreite immer eingehalten wird.

Durchsatz- und Datenverbrauchsstatistiken überprüfen

Für jedes VPX können Sie den Durchsatz und die Datenverbrauchsstatistiken in den Diagrammen überprüfen. Gehen Sie folgendermaßen vor, um auf die Diagramme zuzugreifen:

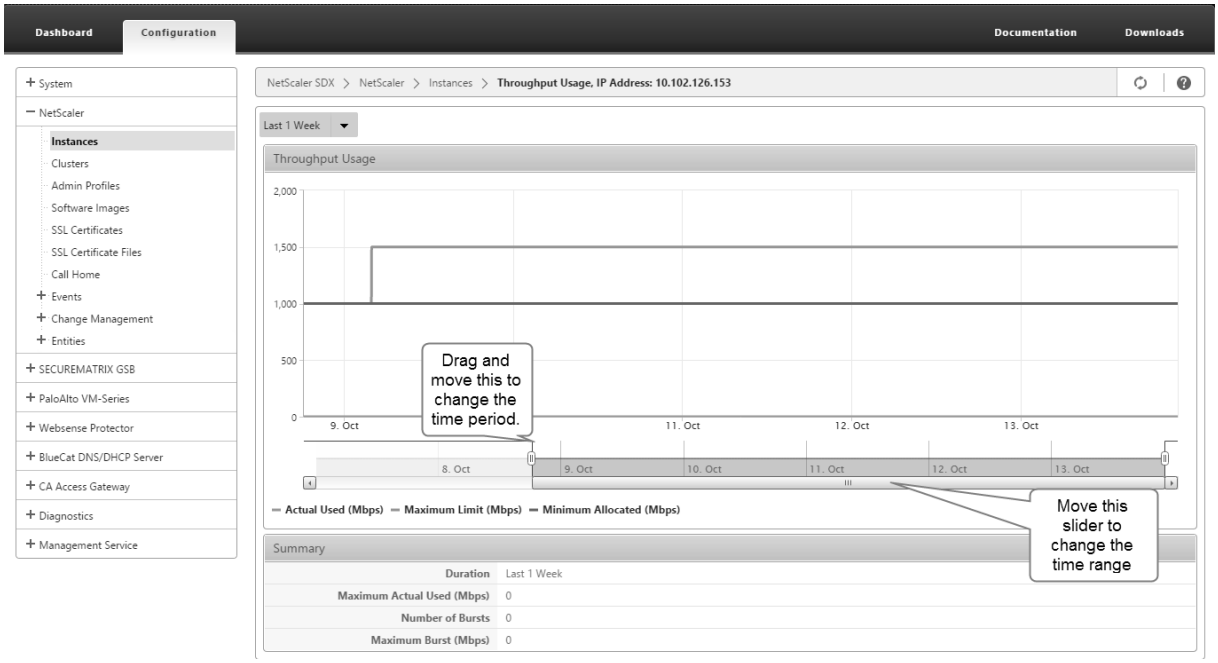
1. Gehen Sie im SDX Management Service zur Seite **Konfiguration > NetScaler > Instanzen**.
2. Wählen Sie eine VPX-Instanz aus und klicken Sie dann auf die **Dropdownliste Aktion** .
3. Wählen Sie in der Liste entweder **Durchsatzstatistiken** oder **Datennutzungsstatistiken**.

In den Diagrammen können Sie den Datenverbrauch und die Durchsatzstatistiken für verschiedene Zeiträume überprüfen, z. B.:

- Letzte Stunde
- Letzter Tag
- Letzte 1 Woche
- In den letzten 1 Monat und
- Voriger Monat

Sie können auch einen bestimmten Zeitraum in der Grafik auswählen, indem Sie den Schieberegler unten im Diagramm anpassen. Bewegen Sie die Maus über die Linien im Diagramm, um den Datenverbrauch oder die Durchsatzdaten für eine bestimmte Zeit zu überprüfen.

Die folgende Abbildung zeigt ein Beispieldiagramm mit Durchsatzdaten für eine Woche:



Konfiguration und Verwaltung von NetScaler-Instanzen

November 23, 2023

Nachdem Sie NetScaler-Instanzen auf Ihrer Appliance bereitgestellt haben, können Sie die Instanzen konfigurieren und verwalten. Erstellen Sie zunächst eine Subnetz-IP-Adresse (SNIP) und speichern

Sie dann die Konfiguration. Sie können dann grundlegende Verwaltungsaufgaben für die Instanzen ausführen. Prüfen Sie, ob Sie die Verwaltungskonfiguration anwenden müssen.

Warnung: Stellen Sie sicher, dass Sie die bereitgestellten Netzwerkschnittstellen oder VLANs einer Instanz mithilfe des Management Service ändern, anstatt die Änderungen direkt an der Instanz durchzuführen.

Erstellen Sie eine SNIP-Adresse auf einer NetScaler-Instanz

Sie können den NetScaler-Instanzen eine SNIP-Adresse zuweisen, nachdem sie auf der SDX-Appliance bereitgestellt wurde.

Ein SNIP wird in der Verbindungsverwaltung und der Serverüberwachung verwendet. Es ist nicht zwingend erforderlich, ein SNIP anzugeben, wenn Sie die NetScaler SDX-Appliance zum ersten Mal konfigurieren. Sie können der NetScaler-Instanz vom Management Service aus SNIP zuweisen.

So fügen Sie einer NetScaler-Instanz eine SNIP-Adresse hinzu

1. Klicken Sie auf der Registerkarte **Konfiguration** im Navigationsbereich auf **NetScaler**.
2. Klicken Sie im Detailbereich unter **NetScaler Configuration**auf **Create**IP.
3. Geben **Sie im Dialogfeld NetScaler-IP erstellen** Werte für die folgenden Parameter an.
    - **IP-Adresse:** Geben Sie die als SNIP-Adresse zugewiesene IP-Adresse an.
    - **Netzwerkmaske:** Geben Sie die Subnetzmaske an, die mit der SNIP-Adresse verknüpft ist.
    - **Typ:** Standardmäßig ist der Wert SNIP.
    - **Konfiguration speichern:** Wählen Sie diese Option, um die Konfiguration auf dem NetScaler zu speichern. Der Standardwert ist falsch.
    - **Instanz-IP-Adresse:** Geben Sie die IP-Adresse der NetScaler-Instanz an.
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Speichern Sie die Konfiguration

Sie können die laufende Konfiguration
einer NetScaler-Instanz vom Management Service aus speichern.

Um die Konfiguration auf einer NetScaler-Instanz zu speichern

1. Klicken Sie auf der Registerkarte **Konfiguration** im Navigationsbereich auf **NetScaler**.
2. Klicken Sie im Detailbereich unter **NetScaler-Konfiguration**auf Konfiguration **speichern**.

3. Wählen **Sie im Dialogfeld Konfiguration speichern unterInstanz-IP-Adresse**die IP-Adressen der NetScaler-Instanzen aus, deren Konfiguration Sie speichern möchten.
4. Klicken Sie auf **OK** und dann auf **Schließen**.

Eine NetScaler-Instanz verwalten

Mit dem Management Service können Sie die folgenden Operationen auf den NetScaler-Instanzen ausführen. Sie können diese Operationen über den Bereich **NetScaler-Instanzen** auf der Registerkarte **Konfiguration** oder über das NetScaler-Instanzen-Gadget auf der Startseite ausführen.

Starten Sie eine NetScaler-Instanz: Starten Sie eine beliebige NetScaler-Instanz über die Management Service-Benutzeroberfläche. Wenn die Management Service-Benutzeroberfläche diese Anfrage an den Management Service weiterleitet, startet sie die NetScaler-Instanz.

Eine NetScaler-Instanz herunterfahren: Fahren Sie jede NetScaler-Instanz über die Management Service-Benutzeroberfläche herunter. Wenn die Management Service-Benutzeroberfläche diese Anfrage an den Management Service weiterleitet, stoppt sie die NetScaler-Instanz.

Starten Sie eine NetScaler-Instanz neu: Starten Sie die NetScaler-Instanz neu.

Löschen Sie eine NetScaler-Instanz: Wenn Sie keine NetScaler-Instanz verwenden möchten, können Sie diese Instanz mithilfe des Management Service löschen. Durch das Löschen einer Instanz werden die Instanz und die zugehörigen Details dauerhaft aus der Datenbank der SDX-Appliance entfernt.

Um eine NetScaler-Instanz zu starten, zu beenden, zu löschen oder neu zu starten

1. Klicken Sie auf der Registerkarte **Konfiguration** im Navigationsbereich auf **NetScaler-Instances**.
2. Wählen Sie die NetScaler-Instanz aus, auf der Sie den Vorgang ausführen möchten, und klicken Sie dann auf **Starten** oder **Herunterfahren** oder **Löschen** oder **Neustarten**.
3. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

NetScaler-Instanzdateien entfernen

Sie können alle NetScaler-Instanzdateien, wie XVAs, Builds, Dokumentation, SSL-Schlüssel oder SSL-Zertifikate, von der Appliance entfernen.

So entfernen Sie NetScaler-Instanzdateien

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich die **NetScaler-Konfiguration**, und klicken Sie dann auf die Datei, die Sie entfernen möchten.

2. Wählen Sie im Detailbereich den Dateinamen aus, und klicken Sie dann auf **Löschen**.

Wenden Sie die Verwaltungskonfiguration an

Zum Zeitpunkt der Bereitstellung einer VPX-Instanz erstellt der Management Service einige Richtlinien, ein Instanzverwaltungsprofil (Admin) und andere Konfigurationen auf der VPX-Instanz. Wenn der Management Service die Admin-Konfiguration nicht anwendet, können Sie die Konfiguration explizit vom Management Service zur VPX-Instanz übertragen. Ein Grund für den Ausfall könnte sein, dass sich der Management Service und die VPX-Instanz in verschiedenen Subnetzen befinden und der Router ausgefallen ist. Ein weiterer Grund könnte sein, dass sich beide im selben Subnetz befinden, der Datenverkehr jedoch einen externen Switch durchlaufen muss und eine der Verbindungen ausgefallen ist.

So wenden Sie die Admin-Konfiguration auf eine NetScaler-Instanz an

1. Klicken Sie auf der Registerkarte **Konfiguration** im Navigationsbereich auf **NetScaler**.
2. Klicken Sie im Detailbereich unter **NetScaler-Konfiguration**auf **Admin-Konfiguration anwenden**.
3. Wählen **Sie im Dialogfeld Admin-Konfiguration anwenden** unter **Instanz-IP-Adresse**die IP-Adresse der VPX-Instanz aus, auf die Sie die Admin-Konfiguration anwenden möchten.
4. Klicken Sie auf **OK**.

Installieren und Verwalten von SSL-Zertifikaten

November 23, 2023

Bei der Installation von SSL-Zertifikaten werden zunächst das Zertifikat und die Schlüsseldateien auf die NetScaler SDX-Appliance hochgeladen. Installieren Sie dann das SSL-Zertifikat auf den NetScaler-Instanzen. Wenn Sie ein SSL-Zertifikat auf der SDX-Appliance installieren oder aktualisieren, wird der Management Service neu gestartet.

Laden Sie die Zertifikatsdatei auf die SDX Appliance hoch

Für jede SSL-Transaktion benötigt der Server ein gültiges Zertifikat und das entsprechende private und öffentliche Schlüsselpaar. Die Zertifikatsdatei muss auf der SDX-Appliance vorhanden sein, wenn Sie das SSL-Zertifikat auf den NetScaler-Instanzen installieren. Sie können die SSL-Zertifikatsdateien auch als Backup auf einen lokalen Computer herunterladen.

Im Bereich **SSL-Zertifikate** können Sie die folgenden Details anzeigen.

- **Name**

Der Name der Zertifikatsdatei.

- **Letzte Änderung**

Das Datum, an dem die Zertifikatsdatei zuletzt geändert wurde.

- **Größe**

Die Größe der Zertifikatsdatei in Byte.

Hochladen von SSL-Zertifikatsdateien auf die SDX-Appliance

1. Erweitern Sie im Navigationsbereich Management Service, und klicken Sie dann auf SSL-Zertifikatsdateien.
2. Klicken Sie im Bereich SSL-Zertifikate auf Hochladen.
3. Klicken Sie im Dialogfeld SSL-Zertifikat hochladen auf Durchsuchen und wählen Sie die Zertifikatsdatei aus, die Sie hochladen möchten.
4. Klicken Sie auf Upload. Die Zertifikatsdatei wird im Bereich SSL-Zertifikate angezeigt.

So erstellen Sie eine Backup durch Herunterladen einer SSL-Zertifikatsdatei

1. Wählen Sie im Bereich SSL-Zertifikate die Datei aus, die Sie herunterladen möchten, und klicken Sie dann auf Herunterladen.
2. Wählen Sie im Meldungsfeld in der Liste Speichern die Option Speichern unter aus.
3. Navigieren Sie im Meldungsfeld Speichern unter zu dem Speicherort, an dem Sie die Datei speichern möchten, und klicken Sie dann auf Speichern.

Hochladen von SSL-Schlüsseldateien auf die SDX-Appliance

Für jede SSL-Transaktion benötigt der Server ein gültiges Zertifikat und das entsprechende private und öffentliche Schlüsselpaar. Die Schlüsseldatei muss auf der SDX-Appliance vorhanden sein, wenn Sie das SSL-Zertifikat auf den NetScaler-Instanzen installieren. Sie können die SSL-Schlüsseldateien auch als Backup auf einen lokalen Computer herunterladen.

Im Bereich SSL-Schlüssel können Sie die folgenden Details anzeigen.

- **Name**

Der Name der Schlüsseldatei.

- **Letzte Änderung**

Das Datum, an dem die Schlüsseldatei zuletzt geändert wurde.

- **Größe**

Die Größe der Schlüsseldatei in Byte.

So laden Sie SSL-Schlüsseldateien auf die SDX-Appliance hoch

1. Erweitern Sie im Navigationsbereich Management Service, und klicken Sie dann auf SSL-Zertifikatsdateien.
2. Klicken Sie im Bereich SSL-Zertifikat auf der Registerkarte SSL-Schlüssel auf Hochladen.
3. Klicken Sie im Dialogfeld SSL-Schlüsseldatei hochladen auf Durchsuchen und wählen Sie die Schlüsseldatei aus, die Sie hochladen möchten.
4. Klicken Sie auf Hochladen, um die Schlüsseldatei auf die SDX-Appliance hochzuladen. Die Schlüsseldatei wird im Bereich SSL-Schlüssel angezeigt.

So erstellen Sie eine Backup durch Herunterladen einer SSL-Schlüsseldatei

1. Wählen Sie im Bereich SSL-Zertifikat auf der Registerkarte SSL-Schlüssel die Datei aus, die Sie herunterladen möchten, und klicken Sie dann auf Herunterladen.
2. Wählen Sie im Meldungsfeld in der Liste Speichern die Option Speichern unter aus.
3. Navigieren Sie im Meldungsfeld Speichern unter zu dem Speicherort, an dem Sie die Datei speichern möchten, und klicken Sie dann auf Speichern.

Installation eines SSL-Zertifikats auf einer NetScaler-Instanz

Mit dem Management Service können Sie SSL-Zertifikate auf einer oder mehreren NetScaler-Instanzen installieren. Bevor Sie mit der Installation des SSL-Zertifikats beginnen, stellen Sie sicher, dass Sie das SSL-Zertifikat und die Schlüsseldateien auf die SDX-Appliance hochgeladen haben.

So installieren Sie SSL-Zertifikate auf einer NetScaler-Instanz

1. Klicken Sie im Navigationsbereich auf NetScaler.
2. Klicken Sie im Detailbereich unter NetScaler Configuration auf SSL-Zertifikate installieren.
3. Geben Sie im Dialogfeld SSL-Zertifikate installieren Werte für die folgenden Parameter an. (*) zeigt erforderliche Felder an.

- Zertifikatsdatei: Geben Sie den Dateinamen des gültigen Zertifikats an. Die Zertifikatsdatei muss auf der SDX-Appliance vorhanden sein.
- Schlüsseldatei: Geben Sie den Dateinamen des privaten Schlüssels an, der zum Erstellen des Zertifikats verwendet wurde. Die Schlüsseldatei muss auf der SDX-Appliance vorhanden sein.
- Zertifikatsname: Geben Sie den Namen des Zertifikatsschlüsselpaars an, das dem NetScaler hinzugefügt werden soll. Maximale Länge: 31
- Zertifikatsformat: Geben Sie das Format des SSL-Zertifikats an, das auf dem NetScaler unterstützt wird. Eine NetScaler SDX-Appliance unterstützt die Formate PEM und DER für SSL-Zertifikate.
- Kennwort: Geben Sie die Passphrase an, die zum Verschlüsseln des privaten Schlüssels verwendet wurde. Diese Option kann verwendet werden, um verschlüsselte private Schlüssel zu laden. Max. Länge: 32.

  Hinweis: Der kennwortgeschützte private Schlüssel wird nur für das PEM-Format unterstützt.
- Konfiguration speichern: Geben Sie an, ob die Konfiguration auf dem NetScaler gespeichert werden muss. Der Standardwert ist falsch.
- Instanz-IP-Adresse: Geben Sie die IP-Adressen der NetScaler-Instanzen an, auf denen Sie das SSL-Zertifikat installieren möchten.

4. Klicken Sie auf OK und dann auf Schließen.

Aktualisierung eines SSL-Zertifikats auf einer NetScaler-Instanz

Sie können einige Parameter aktualisieren, z. B. die Zertifikatsdatei, die Schlüsseldatei und das Zertifikatsformat eines SSL-Zertifikats, das auf einer NetScaler-Instanz installiert ist. Sie können die IP-Adresse und den Zertifikatsnamen nicht ändern.

So aktualisieren Sie das SSL-Zertifikat auf einer NetScaler-Instanz

1. Erweitern Sie im Navigationsbereich NetScaler, und klicken Sie dann auf SSL-Zertifikate.
2. Klicken Sie im Bereich SSL-Zertifikate auf Aktualisieren.
3. Legen Sie im Dialogfeld SSL-Zertifikat ändern die folgenden Parameter fest:

   - Zertifikatsdatei: Der Dateiname des gültigen Zertifikats. Die Zertifikatsdatei muss auf der SDX-Appliance vorhanden sein.
   - Schlüsseldatei: Der Dateiname des privaten Schlüssels, der zum Erstellen des Zertifikats verwendet wurde. Die Schlüsseldatei muss auf der SDX-Appliance vorhanden sein.

- Zertifikatsformat: Das Format des SSL-Zertifikats, das auf der NetScaler SDX-Appliance unterstützt wird. Die Appliance unterstützt die PEM- und DER-Formate für SSL-Zertifikate.
- Kennwort: Die Passphrase, die zur Verschlüsselung des privaten Schlüssels verwendet wurde. Diese Option kann verwendet werden, um verschlüsselte private Schlüssel zu laden. Maximale Länge: 32 Zeichen.

  Hinweis: Der kennwortgeschützte private Schlüssel wird nur für das PEM-Format unterstützt.
- Konfiguration speichern: Geben Sie an, ob die Konfiguration auf der SDX-Appliance gespeichert werden muss. Der Standardwert ist falsch.
- Keine Domainprüfung: Überprüfen Sie den Domainnamen nicht, während Sie das Zertifikat aktualisieren.

4. Klicken Sie auf OK und dann auf Schließen.

Abfragen von SSL-Zertifikaten auf den NetScaler-Instances

Wenn Sie ein SSL-Zertifikat direkt auf einer NetScaler-Instanz hinzufügen, nachdem Sie sich an dieser Instanz angemeldet haben, kennt der Management Service dieses neue Zertifikat nicht. Um dieses Szenario zu vermeiden, geben Sie ein Abfrageintervall an, nach dem der Management Service alle NetScaler-Instanzen abfragt, um nach neuen SSL-Zertifikaten zu suchen. Sie können auch jederzeit vom Management Service aus eine Umfrage durchführen. Zum Beispiel, wenn Sie sofort eine Liste der SSL-Zertifikate von allen NetScaler-Instanzen erhalten möchten.

So konfigurieren Sie ein Abrufintervall

1. Erweitern Sie im Navigationsbereich NetScaler, und klicken Sie dann auf SSL-Zertifikate.
2. Klicken Sie im Bereich SSL-Zertifikate auf Polling-Intervall konfigurieren.
3. Stellen Sie im Dialogfeld Polling-Intervall konfigurieren die folgenden Parameter ein:
   - Abfrageintervall: Die Zeit, nach der der Management Service die NetScaler-Instanzen abfragt.
   - Intervall-Einheit: Die Zeiteinheit. Mögliche Werte: Stunden, Minuten. Standard: Stunden.
4. Klicken Sie auf OK und dann auf Schließen.

So führen Sie eine sofortige Umfrage durch

1. Erweitern Sie im Navigationsbereich NetScaler, und klicken Sie dann auf SSL-Zertifikate.
2. Klicken Sie im Bereich SSL-Zertifikate auf Jetzt abfragen.

3. Klicken Sie im Dialogfeld „Bestätigen ‘‘auf Ja. Der Bereich SSL-Zertifikate wird aktualisiert und neue Zertifikate, falls vorhanden, werden in der Liste angezeigt.

L2-Modus auf einer NetScaler-Instanz zulassen

November 23, 2023

Im Layer-2-Modus (L2) fungiert eine NetScaler-Instanz als Lernbrücke und leitet alle Pakete weiter, für die sie nicht das Ziel ist. Für einige Funktionen, wie z. B. Citrix CloudBridge, muss der L2-Modus auf der NetScaler-Instanz aktiviert sein. Wenn der L2-Modus aktiviert ist, kann die Instanz Pakete für andere MAC-Adressen als ihre eigene MAC-Adresse empfangen und weiterleiten. Um den L2-Modus auf einer NetScaler-Instanz zu aktivieren, die auf einer NetScaler SDX-Appliance ausgeführt wird, muss der Administrator jedoch zuerst den L2-Modus auf dieser Instanz zulassen. Wenn Sie den L2-Modus zulassen, müssen Sie Vorkehrungen treffen, um eine Überbrückung von Schleifen zu vermeiden.

Vorsichtsmaßnahmen:

1. Auf einer bestimmten 1/x-Schnittstelle dürfen Pakete ohne Tags nur auf einer Instanz zulässig sein. Für alle anderen Instanzen, die auf derselben Schnittstelle aktiviert sind, müssen Sie Tagged auswählen.

   Hinweis:

   Citrix empfiehlt, dass Sie für alle Schnittstellen, die Instanzen im L2-Modus zugewiesen sind, Tagged auswählen. Wenn Sie Tagged auswählen, können Sie auf dieser Schnittstelle keine Pakete ohne Tags empfangen.

   Wenn Sie Tagged für eine Schnittstelle ausgewählt haben, die einer Instanz zugewiesen ist, melden Sie sich bei dieser Instanz an und konfigurieren Sie ein 802.1q VLAN, um Pakete auf dieser Schnittstelle zu empfangen.

2. Stellen Sie für 1/x- und 10/x-Schnittstellen, die von NetScaler-Instanzen gemeinsam genutzt werden, auf denen der L2-Modus zulässig ist, sicher, dass die folgenden Bedingungen erfüllt sind:

   - Die VLAN-Filterung ist auf allen Schnittstellen aktiviert.
   - Jede Schnittstelle befindet sich in einem anderen 802.1q VLAN.
   - Nur eine Instanz kann unmarkierte Pakete auf der Schnittstelle empfangen. Wenn diese Schnittstelle anderen Instanzen zugewiesen ist, müssen Sie für diese Instanzen Tagged auf dieser Schnittstelle auswählen.

3. Wenn Sie Pakete ohne Tags auf einer 1/x-Schnittstelle für eine Instanz zulassen, auf der der L2-Modus zulässig ist, kann keine andere Instanz Pakete ohne Tags auf dieser Schnittstelle empfan-

gen. Diese Bedingung gilt unabhängig davon, ob der L2-Modus für die andere Instanz zulässig oder nicht zulässig ist.

4. Wenn Sie unmarkierte Pakete auf einer 1/x-Schnittstelle für eine Instanz mit deaktiviertem L2-Modus zulassen, kann eine Instanz mit erlaubtem L2-Modus keine unmarkierten Pakete auf dieser Schnittstelle empfangen.
5. Wenn der im L2-Modus bereitgestellten Instanz1 eine 0/x-Schnittstelle zugewiesen ist und diese Schnittstelle auch Instanz2 zugewiesen ist, wählen Sie Tagged für alle anderen Schnittstellen aus, die Instanz2 zugewiesen sind.

Hinweis: Wenn beide Verwaltungsschnittstellen einer Instanz mit dem L2-Modus zugewiesen sind, kann nur eine dieser Schnittstellen einer anderen ADC-Instanz mit aktiviertem L2-Modus zugewiesen werden. Das heißt, Sie können beide Verwaltungsschnittstellen nicht mehr als einer NetScaler-Instanz zuordnen, auf der der L2-Modus aktiviert ist.

So lassen Sie den L2-Modus auf einer Instanz zu

1. Wählen Sie im ADC-Assistenten bereitstellen oder im Assistenten zum Ändern des ADC auf der Seite **Netzwerkeinstellungen** die Option **L2-Modus zulassen**aus.
   Hinweis: Sie können die Einstellung L2-Modus zulassen für eine Instanz aktivieren, wenn Sie die Instanz bereitstellen oder während die Instanz ausgeführt wird.
2. Folgen Sie den Anweisungen des Assistenten.
3. Klicken Sie auf **Fertig stellen** und dann auf **Schließen**.

Konfigurieren eines virtuellen MAC auf einer Schnittstelle

November 23, 2023

Eine NetScaler-Instanz verwendet einen virtuellen MAC (VMAC) für Hochverfügbarkeitskonfigurationen (Active-Active oder Active-Standby). Eine virtuelle MAC-Adresse (VMAC) ist eine Floating-Entity, die von den primären und sekundären Knoten in einem Hochverfügbarkeits-Setup gemeinsam genutzt wird.

In einem Hochverfügbarkeits-Setup besitzt der primäre Knoten alle Floating-IP, z. B. die MIP-, SNIP- und VIP-Adressen. Der primäre Knoten reagiert auf Anfragen des Address Resolution Protocol (ARP) für diese IP-Adressen mit einer eigenen MAC-Adresse. Infolgedessen wird die ARP-Tabelle eines externen Geräts (z. B. eines Upstream-Routers) mit der Floating-IP und der MAC-Adresse des primären Knotens aktualisiert.

Wenn ein Failover auftritt, übernimmt der sekundäre Knoten den neuen primären Knoten. Anschließend verwendet es Gratuitous ARP (GARP), um die Floating-IP anzukündigen, die es vom primären System erworben hat. Die MAC-Adresse, die der neue Primärserver ankündigt, ist jedoch die MAC-Adresse seiner eigenen Schnittstelle.

Einige Geräte (insbesondere einige Router) akzeptieren die von der NetScaler SDX-Appliance generierten GARP-Nachrichten nicht. Solche Geräte behalten die alte IP-zu-MAC-Zuordnung bei, die vom alten primären Knoten angekündigt wurde, und eine Site kann infolgedessen ausfallen.

Sie können dieses Problem lösen, indem Sie einen VMAC auf beiden Knoten eines HA-Paars konfigurieren. Beide Knoten besitzen dann identische MAC-Adressen. Daher bleibt die MAC-Adresse des sekundären Knotens bei einem Failover unverändert, und die ARP-Tabellen auf den externen Geräten müssen nicht aktualisiert werden.

Die Konfiguration eines VMAC erfolgt in zwei Schritten:

1. Konfigurieren Sie VMAC im SDX Management Service. Sie fügen eine VRID für eine Schnittstelle oder einen LA-Kanal hinzu. Konfigurieren Sie VMAC im SDX Management Service.
2. Konfigurieren Sie VMAC auf der Citrix Instanz. Weitere Informationen finden Sie im Artikel Configure VMAC on Channel Group Support.

Konfigurieren von VMAC im SDX Management Service

Um VMAC zu konfigurieren, fügen Sie einer Schnittstelle oder einem LA-Kanal aus dem Management Service eine IPv4- oder IPv6-VRID hinzu. Der Management Service generiert intern einen VMAC. Geben Sie dieselbe VRID an, wenn Sie den Active-Active-Modus auf der NetScaler-Instanz konfigurieren. Diese Active-Active-Konfiguration wird auf Mellanox-Schnittstellen nicht unterstützt.

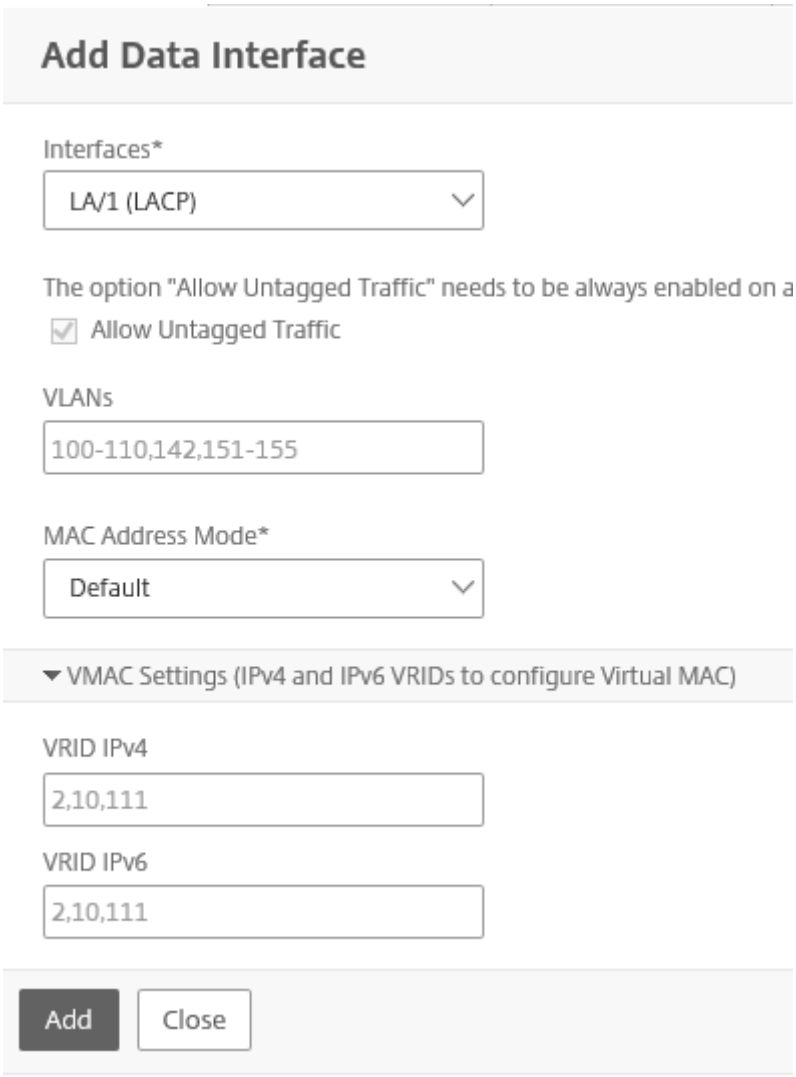
Beachten Sie die folgenden Punkte:

1. Fügen Sie eine VRID aus dem Management Service hinzu und geben Sie dieselbe VRID in der NetScaler-Instanz an. Wenn Sie eine VRID direkt in der NetScaler-Instanz hinzufügen, kann die Instanz kein Paket empfangen, das eine VMAC-Adresse als Ziel-MAC-Adresse hat.
2. Sie können dieselbe VRID nicht auf verschiedenen Instanzen verwenden, die in derselben SDX-Appliance ausgeführt werden.
3. Sie können die VRIDs für eine Schnittstelle hinzufügen oder löschen, die einer Instanz zugewiesen ist, während die Instanz ausgeführt wird.
4. In einer aktiv-aktiven Konfiguration können Sie mehr als eine VRID für eine Schnittstelle angeben, die einer Instanz zugewiesen ist. Die aktive und aktive Bereitstellung wird auf Mellanox-Schnittstellen nicht unterstützt.
5. Auf einer 10G-Schnittstelle sind maximal 86 VMACs und auf einer 1G-Schnittstelle maximal 16 VMACs zulässig. Wenn keine VMAC-Filter mehr verfügbar sind, reduzieren Sie die Anzahl der VRIDs auf einer anderen Instanz.

Sie können beim Hinzufügen einer NetScaler VPX-Instanz eine VRID hinzufügen, oder Sie können eine vorhandene NetScaler-Instanz ändern, um eine VRID hinzuzufügen.

So fügen Sie eine IPv4- oder IPv6-VRID zu einer Schnittstelle oder einem LA-Kanal hinzu

1. Wählen Sie beim Hinzufügen einer VPX-Instanz auf SDX unter **NetzwerkeinstellungenDaten-schnittstellen**aus. Weitere Informationen zum Hinzufügen einer VPX-Instanz auf SDX finden Sie unter Hinzufügen einer NetScaler-Instanz.
2. Wählen Sie im Dropdown-Menü **Schnittstellen** die Schnittstelle oder den LA-Kanal aus.
3. Stellen Sie unter VMAC-Einstellungen einen oder beide der folgenden Werte ein:
    - VRID IPv4 —Die IPv4-VRID, die den VMAC identifiziert. Mögliche Werte: 1—255.
    - VRID IPv6 —Die IPv6-VRID, die den VMAC identifiziert. Mögliche Werte: 1—255.
      Hinweis: Trennen Sie mehrere VRIDs mit einem Komma. Zum Beispiel 12,24.
4. Klicken Sie auf **Hinzufügen**, um die **VMAC-Einstellungen** zur Oberfläche hinzuzufügen.
5. Klicken Sie auf **Fertig stellen** und dann auf **Schließen**.



Wenn die Instanz bereits bereitgestellt ist, gehen Sie folgendermaßen vor, um eine IPv4- oder IPv6-VRID hinzuzufügen.

1. Gehen Sie im SDX Management Service zu **Konfiguration > NetScaler > Instances**.
2. Wählen Sie die Instanz aus und klicken Sie auf **Bearbeiten**.
3. Wählen Sie unter **Datenschnittstellen**die Schnittstelle aus und klicken Sie auf Bearbeiten.
4. Stellen Sie unter VMAC-Einstellungen die VRID-Werte ein. Klicken Sie auf **Hinzufügen** und dann auf **Fertig**.

Generieren Sie Partitions-MAC-Adressen, um eine Admin-Partition auf einer NetScaler-Instanz in der SDX-Appliance zu konfigurieren

November 23, 2023

Eine NetScaler-Instanz auf einer NetScaler SDX-Appliance kann in logische Entitäten partitioniert werden, die als Admin-Partitionen bezeichnet werden. Jede Partition kann konfiguriert und als separate NetScaler-Instanz verwendet werden. Weitere Informationen zu Administratorpartitionen finden Sie unter Admin-Partitionierung.

Um Admin-Partitionen mit einer gemeinsam genutzten VLAN-Konfiguration verwenden zu können, benötigen Sie für jede Partition eine virtuelle MAC-Adresse. Eine solche virtuelle MAC-Adresse wird als Partitions-MAC-Adresse (PMAC) bezeichnet und zur Klassifizierung des in einem gemeinsam genutzten VLAN empfangenen Datenverkehrs verwendet. Diese PMAC-Adresse wird in allen gemeinsam genutzten VLANs verwendet, die an diese Partition gebunden sind.

Generieren und konfigurieren Sie die PMAC-Adresse mithilfe der Management Service-Benutzeroberfläche, bevor Sie die Admin-Partition verwenden. Mit dem Management Service können Sie Partitions-MAC-Adressen generieren, indem Sie:

- Verwenden einer Basis-MAC-Adresse
- Benutzerdefinierte MAC-Adressen angeben
- Zufällige Generierung von MAC-Adressen

Hinweis: Nachdem Sie
die MAC-Adressen der Partition generiert haben, müssen Sie die NetScaler-Instanz neu starten, bevor Sie die Admin-Partitionen konfigurieren.

So generieren Sie die MAC-Adressen der Partition mit einer Basis-MAC-Adresse:

1. Erweitern Sie auf der Registerkarte **Konfiguration** im linken Bereich **NetScaler**, und klicken Sie dann auf **Instanzen**.
2. Wählen Sie im Bereich **Instances** die NetScaler-Instanz aus, für die Sie die Partition-MAC-Adressen generieren möchten.
3. Klicken Sie in der Dropdownliste **Aktion** auf **MACs partitionieren**.
4. Klicken Sie im Bereich **Partitions-MACs** auf **Generieren**.
5. Wählen Sie im Dialogfeld **Partitions-MACs generieren** im Abschnitt **Erstellungsmethode** die Option **Basisadresse verwenden** aus.
6. Geben Sie im Feld **Basis-MAC-Adresse** die Basis-MAC-Adresse ein.
7. Geben Sie im Feld **Inkrement By** den Wert ein, um den die Basis-MAC-Adresse für jede nachfolgende MAC-Adresse erhöht werden muss.
   Wenn Sie beispielsweise die Basis-MAC-Adresse als 00:A1:C9:11:C8:11 und den Inkrementwert als 2 angegeben haben, wird die nächste MAC-Adresse als 00:A1:C9:11:C8:13 generiert.

8. Geben Sie im Feld **Anzahl** die Anzahl der Partitions-MAC-Adressen ein, die Sie generieren möchten.
9. Klicken Sie **Generieren**.

So generieren Sie die MAC-Adressen der Partition durch Angabe benutzerdefinierter MAC-Adressen:

1. Erweitern Sie auf der Registerkarte **Konfiguration** im linken Bereich **NetScaler**, und klicken Sie dann auf **Instanzen**.
2. Wählen Sie im Bereich **Instances** die NetScaler-Instanz aus, für die Sie die Partition-MAC-Adressen generieren möchten.
3. Klicken Sie in der Dropdownliste **Aktion** auf **MACs partitionieren**.
4. Klicken Sie im Bereich **Partitions-MACs** auf **Generieren**.
5. Wählen Sie im Dialogfeld **Partitions-MACs generieren** im Abschnitt **Erstellungsmethode** die Option **Benutzerdefiniert**aus.
6. Geben Sie im Feld **MAC-Adressen** eine MAC-Adresse ein.
7. Klicken Sie auf das Symbol **+** und geben Sie dann die nächste MAC-Adresse ein. Wiederholen Sie dies, um weitere benutzerdefinierte MAC-Adressen anzugeben.
8. Klicken Sie **Generieren**.

Um die MAC-Adressen der Partition zufällig zu generieren:

1. Erweitern Sie auf der Registerkarte **Konfiguration** im linken Bereich **NetScaler**, und klicken Sie dann auf **Instanzen**.
2. Wählen Sie im Bereich **Instances** die NetScaler-Instanz aus, für die Sie die Partition-MAC-Adressen generieren möchten.
3. Klicken Sie in der Dropdownliste **Aktion** auf **MACs partitionieren**.
4. Klicken Sie im Bereich **Partitions-MACs** auf **Generieren**.
5. Wählen Sie im Dialogfeld **Partitions-MACs generieren** im Abschnitt **Generierungsmethode** die Option **Zufällig** aus.
6. Geben Sie im Feld **Anzahl** die Anzahl der Partitions-MAC-Adressen ein, die Sie generieren möchten.
7. Klicken Sie **Generieren**.

Nachdem Sie Partitions-MAC-Adressen in einer SDX-Appliance generiert haben, verwenden Sie die generierten Partitions-MAC-Adressen, um Admin-Partitionen auf der NetScaler-Instanz zu konfigurieren.

Änderungsmanagement für VPX-Instanzen

November 23, 2023

Sie können alle Änderungen an der Konfiguration auf einer NetScaler VPX-Instanz über den Management Service verfolgen. Im Detailbereich wird der Gerätename mit IP-Adresse, Datum und Uhrzeit der letzten Aktualisierung aufgeführt. Es wird auch aufgeführt, ob es einen Unterschied zwischen der gespeicherten Konfiguration und der laufenden Konfiguration gibt. Wählen Sie ein Gerät aus, um seine laufende Konfiguration, die gespeicherte Konfiguration, den Verlauf der Konfigurationsänderungen und alle Unterschiede zwischen den Konfigurationen vor und nach einem Upgrade anzuzeigen. Sie können die Konfiguration einer VPX-Instanz auf Ihren lokalen Computer herunterladen. Standardmäßig fragt der Management Service alle Instanzen alle 24 Stunden ab, aber Sie können dieses Intervall ändern. Sie können eine Überwachungsvorlage erstellen, indem Sie die Befehle aus einer vorhandenen Konfigurationsdatei kopieren. Sie können diese Vorlage später verwenden, um Änderungen in der Konfiguration einer Instanz zu finden und gegebenenfalls Korrekturmaßnahmen zu ergreifen.

So zeigen Sie Änderungsmanagement für VPX-Instanzen an

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **NetScaler > Change Management**.
2. Wählen Sie im Bereich **Change Management** eine VPX-Instanz aus, und wählen Sie dann aus der Liste **Aktion** eine der folgenden Optionen aus:
    - Konfiguration wird ausgeführt —Zeigt die laufende Konfiguration der ausgewählten VPX-Instanz in einem neuen Fenster an.
    - Gespeicherte Konfiguration —Zeigt die gespeicherte Konfiguration der ausgewählten VPX-Instanz in einem neuen Fenster an.
    - Gespeichert Vs. Ausführende Diff: Zeigt die gespeicherte Konfiguration, die laufende Konfiguration und den fehlerbehebenden Befehl (den Unterschied) an.
    - Revisionshistorie-Diff —Zeigt den Unterschied zwischen der Basiskonfigurationsdatei und der zweiten Konfigurationsdatei an.
    - Pre-vs. Diff nach dem Upgrade —Zeigt den Unterschied in der Konfiguration vor und nach einem Upgrade sowie den fehlerbehebenden Befehl (den Unterschied) an.
    - Template-Diff —Zeigt den Unterschied zwischen der gespeicherten oder laufenden Konfiguration und der Vorlage an. Sie können diesen Unterschied als Batch-Datei speichern. Um die Konfiguration aus der Vorlage auf die Instanz anzuwenden, wenden Sie diese Batch-Datei auf die Instanz an.
    - Herunterladen —Lädt die Konfiguration der ausgewählten VPX-Instanz herunter und speichert sie auf einem lokalen Gerät.

Um die Konfiguration einer beliebigen NetScaler-Instanz nach Aktualisierungen abzufragen

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **NetScaler > Change Management**.

2. Wählen Sie im Bereich **Änderungsverwaltung** in der Liste **Aktion** eine der folgenden Optionen aus:

    - Jetzt abfragen —Der Management Service führt eine sofortige Abfrage nach Aktualisierungen der Konfiguration (ns.conf) einer der auf der Appliance installierten VPX-Instanzen durch.
    - Abfrageintervall konfigurieren —Zeit, nach der der Management Service Aktualisierungen der Konfiguration (ns.conf) einer der auf der Appliance installierten VPX-Instanzen abfragt. Das standardmäßige Abrufintervall beträgt 24 Stunden.

So konfigurieren Sie eine Audit-Vorlage für eine NetScaler-Instanz

1. Öffnen Sie eine vorhandene Konfigurationsdatei und kopieren Sie deren Befehlsliste.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **NetScaler > Change Management > Audit Templates**.
3. Klicken Sie im Detailbereich auf **Hinzufügen**.
4. **Fügen Sie im Dialogfeld Vorlage** hinzufügen einen Namen und eine Beschreibung für die Vorlage hinzu.
5. Fügen Sie in das Textfeld **Befehl** die Liste der Befehle ein, die Sie aus der Konfigurationsdatei kopiert haben.
6. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

NetScaler-Instanzen überwachen

November 23, 2023

Eine allgemeine Ansicht der Leistung der Appliance und der auf der Appliance bereitgestellten VPX-Instanzen wird auf der Seite Überwachung der Management Service-Benutzeroberfläche angezeigt. Nach der Bereitstellung und Konfiguration der NetScaler-Instanz können Sie verschiedene Aufgaben ausführen, um die NetScaler-Instanz zu überwachen.

Zeigen Sie die Eigenschaften von VPX-Instanzen an

Auf der Management Service-Benutzeroberfläche werden die Liste und Beschreibung aller VPX-Instanzen angezeigt, die auf der SDX-Appliance bereitgestellt wurden. Verwenden Sie den Bereich **NetScaler-Instanzen**, um Details wie den Instanznamen und die IP-Adresse, die CPU- und Speicherauslastung, den Durchsatz und den der Instanz zugewiesenen Gesamtspeicher anzuzeigen.

Durch Klicken auf die IP-Adresse der VPX-Instanz wird das Konfigurationsdienstprogramm (GUI) dieser Instanz in einer neuen Registerkarte oder einem neuen Browser geöffnet.

So zeigen Sie die Eigenschaften von VPX-Instanzen an

1. Erweitern Sie auf der Registerkarte Konfiguration im linken Bereich die NetScaler-Konfiguration, und klicken Sie dann auf Instances.
   Hinweis: Sie können die Eigenschaften einer VPX-Instanz auch auf der Registerkarte Home anzeigen.
2. Im Bereich NetScaler-Instanz können Sie die folgenden Details für die NetScaler-Instanz anzeigen:
   - **Name:** Der Hostname, der der NetScaler-Instanz bei der Bereitstellung zugewiesen wurde.
   - **VM-Zustand:** Der Status der virtuellen Maschine.
   - **NetScaler State:** Der Status der NetScaler-Instanz.
   - **IP-Adresse: Die** IP-Adresse der NetScaler-Instanz. Durch Klicken auf die IP-Adresse wird die GUI dieser Instanz in einem neuen Tab oder Browser geöffnet.
   - **Rx (Mbit/s):** Die auf der NetScaler-Instanz empfangenen Pakete.
   - **Tx (Mbit/s):** Die von der NetScaler-Instanz übertragenen Pakete.
   - **HTTP-Req/s:** Die Gesamtzahl der HTTP-Anfragen, die pro Sekunde auf der NetScaler-Instanz empfangen werden.
   - **CPU-Auslastung (%):** Der Prozentsatz der CPU-Auslastung auf dem NetScaler.
   - **Speichernutzung (%):** Der Prozentsatz der Speicherauslastung auf dem NetScaler.
3. Klicken Sie auf den Pfeil neben dem Namen einer NetScaler-Instanz, um die Eigenschaften dieser Instanz anzuzeigen. Sie können auch auf **Alle erweitern** klicken, um die Eigenschaften aller NetScaler-Instanzen anzuzeigen. Sie können die folgenden Eigenschaften anzeigen:
   - **Netzmaske:** Die Netzmask-IP-Adresse der NetScaler-Instanz.
   - **Gateway:** Die IP-Adresse des Standard-Gateways, des Routers, der Datenverkehr außerhalb des Subnetzes weiterleitet, in dem die Instanz installiert ist.
   - **Pakete pro Sekunde:** Die Gesamtzahl der Pakete, die jede Sekunde übergeben werden.
   - **NICs:** Die Namen der NICs, die von der NetScaler-Instanz verwendet werden, zusammen mit der virtuellen Funktion, die jeder Schnittstelle zugewiesen ist.
   - **Version:** Die Build-Version, das Build-Datum und die Uhrzeit der NetScaler-Software, die derzeit auf der Instanz ausgeführt wird.
   - **Hostname:** Der Hostname der NetScaler-Instanz.
   - **Gesamtspeicher (GB):** Der Gesamtspeicher, der der NetScaler-Instanz zugewiesen wird.
   - **Durchsatz (Mbit/s):** Der Gesamtdurchsatz der NetScaler-Instanz.
   - **Seit:** Das Datum und die Uhrzeit, seit wann sich die Instanz kontinuierlich im Status UP befindet.

- **SSL-Chips:** Die Gesamtzahl der SSL-Chips, die der Instanz zugewiesen sind.
- **Peer-IP-Adresse: Die** IP-Adresse des Peers dieser NetScaler-Instanz, falls sie sich in einem HA-Setup befindet.
- **Status:** Der Status der Operationen, die auf einer NetScaler-Instanz ausgeführt werden, z. B. der Status, ob die Inventarisierung der Instanz abgeschlossen ist.
- **HA Master State:** Der Zustand des Geräts. Der Status gibt an, ob die Instanz in einem eigenständigen oder primären Setup konfiguriert ist oder Teil eines Hochverfügbarkeits-Setups ist. In einem Hochverfügbarkeits-Setup zeigt der Status auch an, ob er sich im primären oder sekundären Modus befindet.
- **HA-Sync-Status:** Der Modus des HA-Synchronisierungsstatus, z. B. aktiviert oder deaktiviert.
- **Beschreibung:** Die Beschreibung, die bei der Bereitstellung der NetScaler-Instanz eingegeben wurde.

> **Hinweise:**
>
> Wenn eine ADC-Instanz aufgrund eines Authentifizierungsfehlers außer Betrieb geht, ändert sich die Farbe des Instanzstatus in Grau, wenn die folgenden Bedingungen erfüllt sind:
>
> - Das ADC-Instanzkennwort wird direkt mit der Instanz-CLI geändert.
> - Das Kennwort stimmt nicht mit dem im Management Service gespeicherten Instanz-Admin-Profilkennwort überein.
> - Die vorherige Sitzung geht verloren, nachdem Sie die Instanz zum ersten Mal neu gestartet haben.
>
> Wenn eine Instanz außer Betrieb genommen wird, ist die Farbe des Instanzstatus normalerweise gelb.
>
> Um die Instanz wiederherzustellen, führen Sie einen der folgenden Schritte aus:
>
> - Ändern Sie in der Instanz-CLI das Kennwort der Instanz so, dass es mit dem Kennwort im Admin-Profil der Instanz übereinstimmt. Entdecken Sie dann die Instanz im Management Service erneut.
> - Erstellen Sie ein Admin-Profil mit demselben Kennwort wie das aktuelle Kennwort der ADC-Instanz. Aktualisieren Sie dann die ADC-Instanz mit dem neuen Admin-Profil.

Die laufende und gespeicherte Konfiguration einer NetScaler-Instanz anzeigen

Mithilfe des Management Service können Sie die aktuell ausgeführte Konfiguration einer NetScaler-Instanz einsehen. Sie können auch die gespeicherte Konfiguration einer NetScaler-Instanz und den Zeitpunkt, zu dem die Konfiguration gespeichert wurde, einsehen.

Um die laufende und gespeicherte Konfiguration einer NetScaler-Instanz anzuzeigen

1. Erweitern Sie auf der Registerkarte Konfiguration im linken Bereich die NetScaler-Konfiguration, und klicken Sie dann auf Instances.
2. Klicken Sie im Bereich NetScaler-Instanzen auf die NetScaler-Instanz, für die Sie die laufende oder gespeicherte Konfiguration anzeigen möchten.
3. Um die laufende Konfiguration anzuzeigen, klicken Sie auf Konfiguration ausführen, und um die gespeicherte Konfiguration anzuzeigen, klicken Sie auf Gespeicherte Konfiguration.
4. Im Fenster NetScaler Running Config oder NetScaler Saved Config können Sie die laufende oder gespeicherte Konfiguration der NetScaler-Instanz anzeigen.

Pingen Sie eine NetScaler-Instanz

Sie können eine NetScaler-Instanz vom Management Service aus anpingen, um zu überprüfen, ob das Gerät erreichbar ist.

Um eine NetScaler-Instanz anzupingen

1. Erweitern Sie auf der Registerkarte Konfiguration im linken Bereich die NetScaler-Konfiguration, und klicken Sie dann auf Instances.
2. Klicken Sie im Bereich NetScaler-Instanzen auf die NetScaler-Instanz, die Sie pingen möchten, und klicken Sie dann auf Ping. Im Feld Ping-Nachricht können Sie anzeigen, ob der Ping erfolgreich war.

Verfolgen Sie die Route einer NetScaler-Instanz

Sie können die Route eines Pakets vom Management Service zu einer NetScaler-Instanz verfolgen, indem Sie die Anzahl der Hops ermitteln, über die die Instanz erreicht wurde.

Um die Route einer NetScaler-Instanz nachzuverfolgen

1. Erweitern Sie auf der Registerkarte Konfiguration im linken Bereich die NetScaler-Konfiguration, und klicken Sie dann auf Instances.
2. Klicken Sie im Bereich NetScaler-Instanzen auf die NetScaler-Instanz, die Sie verfolgen möchten, und klicken Sie dann auf TraceRoute. Im Meldungsfeld Traceroute können Sie die Route zum NetScaler anzeigen.

Entdecken Sie eine NetScaler-Instanz neu

Sie können eine NetScaler-Instanz wiederfinden, wenn Sie den neuesten Status und die neueste Konfiguration einer NetScaler-Instanz einsehen möchten.

Während der Wiederermittlung ruft der Management Service die Konfiguration ab. Standardmäßig plant der Management Service Geräte für die erneute Erkennung alle 30 Minuten.

Um eine NetScaler-Instanz wiederzuentdecken

1. Erweitern Sie auf der Registerkarte **Konfiguration** im linken Bereich die **NetScaler-Konfiguration**, und klicken Sie dann auf **Instances**.
2. Klicken Sie im Bereich **NetScaler-Instanzen** auf die NetScaler-Instanz, die Sie erneut ermitteln möchten, und klicken Sie dann auf **Rediscover.**
3. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Verwenden Sie Protokolle, um Vorgänge und Ereignisse zu überwachen

November 23, 2023

Verwenden Sie Prüf- und Aufgabenprotokolle, um die auf dem Management Service und auf den NetScaler SDX-Instanzen ausgeführten Vorgänge zu überwachen. Sie können das Ereignisprotokoll auch verwenden, um alle Ereignisse für Aufgaben zu verfolgen, die im Management Service und im Citrix Hypervisor ausgeführt werden.

Die Überwachungsprotokolle anzeigen

Alle mit dem Management Service ausgeführten Vorgänge werden in der Appliance-Datenbank protokolliert. Verwenden Sie Überwachungsprotokolle, um die Vorgänge anzuzeigen, die ein Verwaltungsdienstbenutzer ausgeführt hat, Datum und Uhrzeit sowie den Erfolgs- oder Fehlschlagstatus jedes Vorgangs. Sie können die Details auch nach Benutzer, Vorgang, Prüfzeit, Status usw. sortieren, indem Sie auf die entsprechende Spaltenüberschrift klicken.

Die Paginierung wird im Bereich Überwachungsprotokoll unterstützt. Wählen Sie die Anzahl der Datensätze aus, die auf einer Seite angezeigt werden sollen. Standardmäßig werden 25 Datensätze auf einer Seite angezeigt.

Gehen Sie folgendermaßen vor, um Überwachungsprotokolle anzuzeigen:

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

2. Im Bereich Überwachungsprotokoll können Sie die folgenden Details anzeigen.

    - **Benutzername:** Der Verwaltungsdienstbenutzer, der den Vorgang ausgeführt hat.
    - **IP-Adresse:** Die IP-Adresse des Systems, auf dem der Vorgang ausgeführt wurde.
    - **Port:** Der Port, an dem das System lief, als der Vorgang ausgeführt wurde.
    - **Ressourcentyp:** Der Typ der Ressource, die zur Ausführung des Vorgangs verwendet wird, z. B. xen_vpx_image und Anmeldung.
    - **Ressourcenname:** Der Name der Ressource, die zum Ausführen des Vorgangs verwendet wird, z. B. vpx_image_name und der Benutzername, der für die Anmeldung verwendet wird.
    - **Überwachungszeit:** Der Zeitpunkt, zu dem das Überwachungsprotokoll generiert wurde.
    - **Vorgang:** Die ausgeführte Aufgabe, z. B. Hinzufügen, Löschen und Abmelden.
    - **Status:** Der Status der Prüfung, z. B. erfolgreich oder fehlgeschlagen.
    - **Meldung:** Eine Meldung, die die Ursache des Fehlers beschreibt, wenn der Vorgang fehlgeschlagen ist, und den Status der Aufgabe, z. B. Fertig, wenn der Vorgang erfolgreich war.

3. Um die Protokolle nach einem bestimmten Feld zu sortieren, klicken Sie auf die Überschrift der Spalte.

Aufgabenprotokolle anzeigen

Verwenden Sie Aufgabenprotokolle, um Aufgaben wie das Aktualisieren von Instanzen und das Installieren von SSL-Zertifikaten, die vom Management Service auf den NetScaler-Instanzen ausgeführt werden, einzusehen und zu verfolgen. Im Aufgabenprotokoll können Sie anzeigen, ob eine Aufgabe in Bearbeitung ist oder fehlgeschlagen ist oder erfolgreich war.

Die Paginierung wird im Bereich **Aufgabenprotokoll** unterstützt. Wählen Sie die Anzahl der Datensätze aus, die auf einer Seite angezeigt werden sollen. Standardmäßig werden 25 Datensätze auf einer Seite angezeigt.

Gehen Sie folgendermaßen vor, um das Aufgabenprotokoll anzuzeigen:

1. Erweitern Sie im Navigationsbereich Diagnose, und klicken Sie dann auf Task-Protokoll.
2. Im Bereich Aufgabenprotokoll können Sie die folgenden Details anzeigen.

    - **Name:** Der Name der Aufgabe, die gerade ausgeführt wird oder bereits ausgeführt wurde.
    - **Status:** Der Status der Aufgabe, z. B. In Bearbeitung, Abgeschlossen oder Fehlgeschlagen.
    - **Ausgeführt von:** Der Verwaltungsdienstbenutzer, der den Vorgang ausgeführt hat.
    - **Startzeit:** Die Zeit, zu der die Aufgabe begann.
    - **Endzeit:** Die Zeit, zu der die Aufgabe endete.

Geräteprotokolle für Aufgaben anzeigen

Verwenden Sie Aufgabengeräteprotokolle, um Aufgaben anzuzeigen und zu verfolgen, die auf jeder SDX-Instanz ausgeführt werden. Im Aufgabengeräteprotokoll können Sie anzeigen, ob eine Aufgabe gerade ausgeführt wird oder fehlgeschlagen ist oder erfolgreich war. Es zeigt auch die IP-Adresse der Instanz an, auf der die Aufgabe ausgeführt wird.

Gehen Sie folgendermaßen vor, um das Aufgabengeräteprotokoll anzuzeigen:

1. Erweitern Sie im Navigationsbereich **Diagnose**, und klicken Sie dann auf **Task-Protokoll**.
2. Doppelklicken Sie im Bereich **Aufgabenprotokoll** auf die Aufgabe, um die Details des Aufgabengeräts anzuzeigen.
3. Klicken Sie im Bereich **Aufgabengeräteprotokoll** auf die Überschrift der Spalte, um die Protokolle nach einem bestimmten Feld zu sortieren.

Befehlsprotokolle für Aufgaben anzeigen

Verwenden Sie Task-Befehlsprotokolle, um den Status jedes Befehls einer Aufgabe einzusehen, die auf einer NetScaler-Instanz ausgeführt wird. Im Task-Befehlsprotokoll können Sie anzeigen, ob ein Befehl erfolgreich ausgeführt wurde oder fehlgeschlagen ist. Es zeigt auch den ausgeführten Befehl und den Grund, warum ein Befehl fehlgeschlagen ist.

Gehen Sie folgendermaßen vor, um das Task-Befehlsprotokoll anzuzeigen:

1. Erweitern Sie im Navigationsbereich **Diagnose**, und klicken Sie dann auf **Task-Protokoll**.
2. Doppelklicken Sie im Bereich **Aufgabenprotokoll** auf die Aufgabe, um die Details des Aufgabengeräts anzuzeigen.
3. Doppelklicken Sie im Bereich **Aufgabengeräteprotokoll** auf die Aufgabe, um die Details des Aufgabenbefehls anzuzeigen.
4. Klicken Sie im Bereich **Task-Befehlsprotokoll** auf die Überschrift der Spalte, um die Protokolle nach einem bestimmten Feld zu sortieren.

Ereignisse anzeigen

Verwenden Sie den Bereich **Ereignisse** in der Management Service-Benutzeroberfläche, um die vom Management Service generierten Ereignisse für Aufgaben zu überwachen, die im Management Service ausgeführt werden.

Gehen Sie folgendermaßen vor, um die Ereignisse anzuzeigen:

1. Navigieren Sie zu **System > Ereignisse**.
2. Im Bereich **Ereignisse** können Sie die folgenden Details anzeigen.

- **Schweregrad:** Der Schweregrad eines Ereignisses, der kritisch, schwerwiegend, geringfügig, eindeutig und informativ sein kann.
- **Source:** Die IP-Adresse, für die das Ereignis generiert wird.
- **Date:** Das Datum, an dem das Ereignis generiert wird.
- **Category:** Die Kategorie des Ereignisses, z. B. PolicyFailed und DeviceConfigChange.
- **Message:** Die Nachricht, die das Ereignis beschreibt.

3. Um die Ereignisse nach einem bestimmten Feld zu sortieren, klicken Sie auf die Überschrift der Spalte.

Anwendungsfälle für NetScaler SDX-Appliances

November 23, 2023

Für Netzwerkkomponenten (wie Firewalls und Application Delivery Controller) umfasste die Unterstützung von Mehrmandantenfähigkeit in der Vergangenheit die Möglichkeit, ein einzelnes Gerät in mehrere logische Partitionen aufzuteilen. Dieser Ansatz ermöglicht die Implementierung verschiedener Richtliniensätze für jeden Mandanten, ohne dass zahlreiche separate Geräte erforderlich sind. Traditionell ist es jedoch in Bezug auf den erreichten Isolationsgrad stark eingeschränkt.

Die SDX-Appliance unterliegt nicht denselben Einschränkungen. In der SDX-Architektur wird jede Instanz als separate virtuelle Maschine (VM) mit eigenem dedizierten NetScaler-Kernel, CPU-Ressourcen, Speicherressourcen, Adressraum und Bandbreitenzuweisung ausgeführt. Netzwerk-E/A auf der SDX-Appliance behalten nicht nur die gesamte Systemleistung bei, sondern ermöglichen auch die vollständige Trennung der Datenebene und des Datenverkehrs auf Verwaltungsebene jedes Mandanten. Die Managementebene umfasst die 0/x-Schnittstellen. Die Datenebene umfasst die 1/x- und 10/x-Schnittstellen. Eine Datenebene kann auch als Verwaltungsebene verwendet werden.

Die Hauptanwendungsfälle für eine SDX-Appliance beziehen sich auf die Konsolidierung, wodurch die Anzahl der erforderlichen Netzwerke reduziert wird, während die Managementisolierung aufrechterhalten wird. Es folgen die grundlegenden Konsolidierungsszenarien:

- Konsolidierung, wenn sich der Management Service und die NetScaler-Instanzen im selben Netzwerk befinden.
- Konsolidierung, wenn sich der Management Service und die NetScaler-Instanzen in unterschiedlichen Netzwerken befinden, aber alle Instanzen sich im selben Netzwerk befinden.
- Konsolidierung über Sicherheit hinweg.
- Konsolidierung mit dedizierten Schnittstellen für jede Instanz.
- Konsolidierung mit der gemeinsamen Nutzung eines physischen Port durch mehr als eine Instanz.

Konsolidierung - Management Service und die NetScaler-Instanzen sind im selben Netzwerk

November 23, 2023

Ein einfacher Konsolidierungsfall auf der SDX-Appliance ist die Konfiguration des Management Service und der NetScaler-Instanzen als Teil desselben Netzwerks. Dieser Anwendungsfall ist anwendbar, wenn:

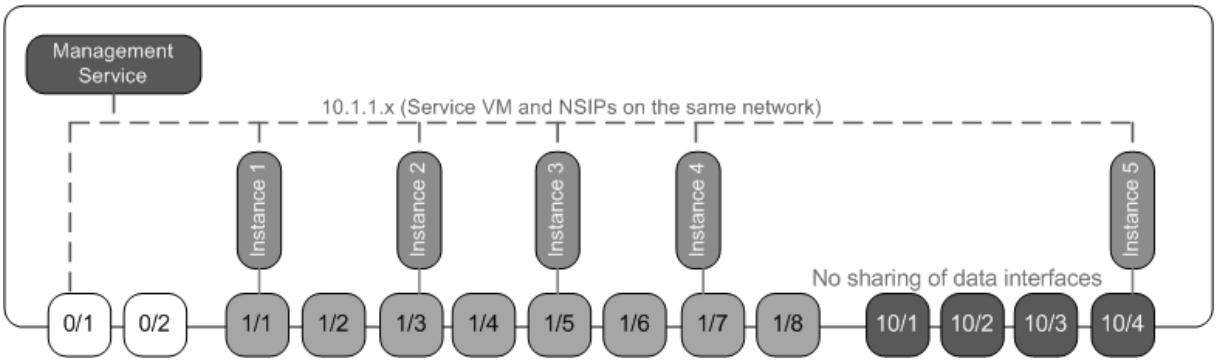
- Der Appliance-Administrator ist auch der Instanzadministrator.
- Die Konformitätsanforderung Ihres Unternehmens legt nicht fest, dass separate Verwaltungsnetzwerke für den Management Service und die NSIP-Adressen der verschiedenen Instanzen erforderlich sind.

Die Instanzen können im selben Netzwerk bereitgestellt werden (für Verwaltungsverkehr). Die VIP-Adressen können in verschiedenen Netzwerken (für den Datenverkehr) und damit in verschiedenen Sicherheitsbereichen konfiguriert werden.

Im folgenden Beispiel sind der Management Service und die NetScaler-Instanzen Teil des 10.1.1.x-Netzwerks. Die Schnittstellen 0/1 und 0/2 sind die Verwaltungsschnittstellen, 1/1 bis 1/8 sind 1G-Datenschnittstellen und 10/1 bis 10/4 sind 10G-Datenschnittstellen. Jede Instanz hat ihre eigene dedizierte physische Schnittstelle. Daher ist die Anzahl der Instanzen auf die Anzahl der physikalischen Schnittstellen beschränkt, die auf der Appliance verfügbar sind. Standardmäßig ist die VLAN-Filterung auf jeder Schnittstelle der SDX-Appliance aktiviert. Die Anzahl der VLANs ist auf 32 auf einer 1G-Schnittstelle und 63 auf einer 10G-Schnittstelle beschränkt. Die VLAN-Filterung kann für jede Schnittstelle aktiviert und deaktiviert werden. Deaktivieren Sie die VLAN-Filterung, um bis zu 4096 VLANs pro Schnittstelle auf jeder Instanz zu konfigurieren. In diesem Beispiel ist eine VLAN-Filterung nicht erforderlich, da jede Instanz über eine eigene dedizierte Schnittstelle verfügt. Weitere Informationen zur VLAN-Filterung finden Sie im Abschnitt **VLAN-Filterung** unter Verwalten und Überwachen der SDX-Appliance.

Die folgende Abbildung veranschaulicht den vorhergehenden Anwendungsfall.

Abbildung 1. Netzwerktopologie einer SDX-Appliance mit Management Service und NSIPs für Instanzen im selben Netzwerk



In der folgenden Tabelle sind die Namen und Werte der Parameter aufgeführt, die im vorherigen Beispiel für die Bereitstellung der NetScaler-Instanz 1 verwendet wurden.

Parametername	Werte für Instanz 1
Name	vpx8
IP-Adresse	10.1.1.2
Netzmaske	255.255.255.0
Gateway	10.1.1.1
XVA-Datei	NS-VPX-XEN-10.0-51.308.a_nc.xva
Feature-Lizenz	Platinum
Admin-Profil	ns_nsroot_profile
Benutzername	vpx8
Kennwort	Sdx1
Confirm Password	Sdx1
Shell/Sftp/Scp Access	True
Gesamter Speicher (MB)	2048
#SSL -Chips	1
Durchsatz (Mbit/s)	1000
Pakete pro Sekunde	1000000
CPU	Freigegeben
Schnittstelle	0/1 und 1/1

Stellen Sie NetScaler-Instanz 1 bereit, wie in diesem Beispiel gezeigt

1. Erweitern Sie auf der Registerkarte Konfiguration im Navigationsbereich die NetScaler-Konfiguration und klicken Sie dann auf Instances.
2. Klicken Sie im Bereich NetScaler-Instanzen auf Hinzufügen.
3. Befolgen Sie im Citrix Provision-Assistenten die Anweisungen des Assistenten, um die in der vorherigen Tabelle aufgeführten Parameterwerte anzugeben.
4. Klicken Sie auf Erstellenund dann auf Schließen. Die NetScaler-Instanz, die Sie bereitgestellt haben, wird im Bereich NetScaler-Instanzen angezeigt.

Konsolidierung - Management Service und die NetScaler-Instanzen sind in unterschiedlichen Netzwerken

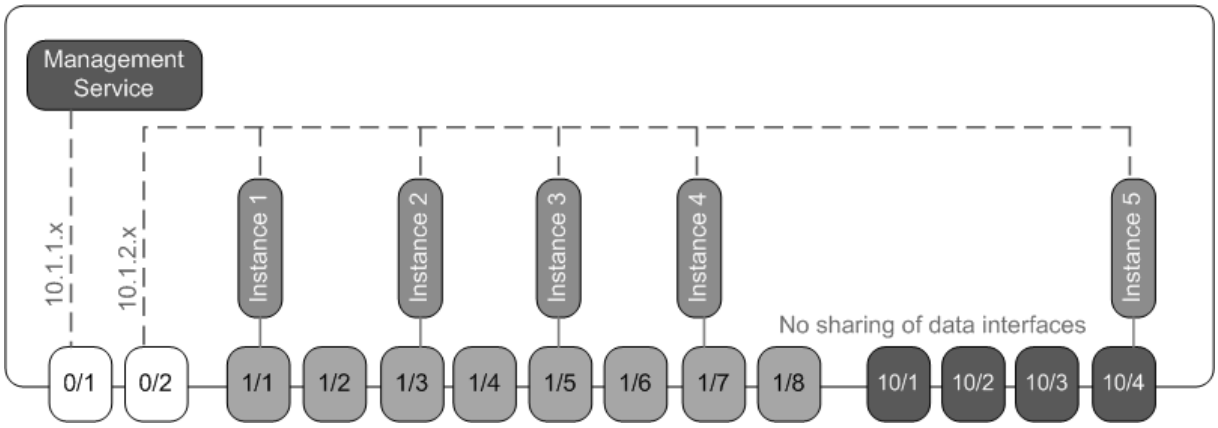
November 23, 2023

In bestimmten Fällen kann der Appliance-Administrator anderen Administratoren erlauben, Verwaltungsaufgaben für einzelne Instanzen durchzuführen. Dies kann sicher erfolgen, indem einem einzelnen Instanzadministrator nur für diese Instanz Anmelderechte erteilt werden. Aus Sicherheitsgründen möchte der Appliance-Administrator jedoch möglicherweise nicht zulassen, dass sich die Instanz im selben Netzwerk wie der Management Service befindet. Dies ist ein gängiges Szenario in Service-Provider-Umgebungen und wird in Unternehmen immer häufiger eingesetzt, da sie Virtualisierung und Cloud-Architekturen einsetzen.

Im folgenden Beispiel befindet sich der Management Service im 10.1.1.x-Netzwerk und die NetScaler-Instanzen befinden sich im 10.1.2.x-Netzwerk. Die Schnittstellen 0/1 und 0/2 sind die Verwaltungsschnittstellen, 1/1 bis 1/8 sind 1G-Datenschnittstellen und 10/1 bis 10/4 sind 10G-Datenschnittstellen. Jede Instanz hat ihren eigenen dedizierten Administrator und ihre eigene dedizierte physische Schnittstelle. Daher ist die Anzahl der Instanzen auf die Anzahl der physikalischen Schnittstellen beschränkt, die auf der Appliance verfügbar sind. Eine VLAN-Filterung ist nicht erforderlich, da jede Instanz über eine eigene dedizierte Schnittstelle verfügt. Deaktivieren Sie optional die VLAN-Filterung, um bis zu 4096 VLANs pro Instanz pro Schnittstelle zu konfigurieren. In diesem Beispiel müssen Sie kein NSVLAN konfigurieren, da sich die Instanzen keine physische Schnittstelle teilen und es keine getaggten VLANs gibt. Weitere Informationen zu NSVLANs finden Sie unter Hinzufügen einerNetScaler-Instanz

Die folgende Abbildung veranschaulicht den vorhergehenden Anwendungsfall.

Abbildung 1. Netzwerktopologie einer SDX-Appliance mit Management Service und NSIPs für Instanzen in verschiedenen Netzwerken



Als Appliance-Administrator können Sie den Datenverkehr zwischen dem Management Service und den NSIP-Adressen auf der SDX-Appliance aufrechterhalten. Oder Sie können den Datenverkehr vom Gerät erzwingen, wenn Sie beispielsweise möchten, dass der Datenverkehr über eine externe Firewall oder einen anderen Sicherheitsvermittler fließt und dann zur Appliance zurückkehrt.

In der folgenden Tabelle sind die Namen und Werte der Parameter aufgeführt, die in diesem Beispiel für die Bereitstellung von NetScaler-Instanz 1 verwendet wurden.

Parametername	Werte für Instanz 1
Name	vpx1
IP-Adresse	10.1.2.2
Netzmaske	255.255.255.0
Gateway	10.1.2.1
XVA-Datei	NS-VPX-XEN-10.0-51.308.a_nc.xva
Feature-Lizenz	Platinum
Admin-Profil	ns_nsroot_profile
Benutzername	vpx1
Kennwort	Sdx1
Confirm Password	Sdx1
Shell/Sftp/Scp Access	True
Gesamter Speicher (MB)	2048
#SSL -Chips	1
Durchsatz (Mbit/s)	1000
Pakete pro Sekunde	1000000

Parametername	Werte für Instanz 1
CPU	Freigegeben
Schnittstelle	0/2 und 1/1

Um NetScaler-Instanz 1 bereitzustellen, wie in diesem Beispiel gezeigt

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich den Bereich **NetScaler Configuration** und klicken Sie dann auf **Instanzen**.
2. Klicken Sie im Bereich NetScaler-Instanzen auf **Hinzufügen.**
3. Folgen Sie im **Provision NetScaler Wizard** den Anweisungen im Assistenten, um die Parameter auf die in der obigen Tabelle angegebenen Werte einzustellen.
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**. Die NetScaler-Instanz, die Sie bereitgestellt haben, wird im Bereich NetScaler-Instanzen angezeigt.

Konsolidierung über Sicherheitsbereiche hinweg

November 23, 2023

Eine SDX-Appliance wird häufig für die Konsolidierung über Sicherheitszonen hinweg verwendet. Die DMZ bietet eine zusätzliche Sicherheitsebene für das interne Netzwerk einer Organisation, da ein Angreifer nur Zugriff auf die DMZ hat. Es hat keinen Zugriff auf das interne Netzwerk der Organisation. In Umgebungen mit hohen Compliance-Anforderungen ist eine einzelne NetScaler-Instanz mit VIP-Adressen sowohl in der DMZ als auch in einem internen Netzwerk nicht akzeptabel. Mit SDX können Sie Instanzen bereitstellen, die VIP-Adressen in der DMZ hosten, und andere Instanzen, die VIP-Adressen in einem internen Netzwerk hosten.

Manchmal benötigen Sie möglicherweise separate Verwaltungsnetzwerke für jede Sicherheitszone. Die NSIP-Adressen der Instanzen in der DMZ können sich in einem Netzwerk befinden. Die NSIP-Adressen der Instanzen mit VIPs im internen Netzwerk können sich in einem anderen Verwaltungsnetzwerk befinden. Oft muss die Kommunikation zwischen dem Management Service und den Instanzen möglicherweise über ein externes Gerät wie einen Router geleitet werden. Sie können Firewall-Richtlinien konfigurieren, um den an die Firewall gesendeten Datenverkehr zu steuern und den Datenverkehr zu protokollieren.

Die SDX-Appliance verfügt über zwei Verwaltungsschnittstellen (0/1 und 0/2) und je nach Modell über bis zu acht 1G-Datenports und acht 10G-Datenports. Sie können die Datenports auch als Management-Ports verwenden (z. B. wenn Sie getaggte VLANs konfigurieren müssen, da das Tagging

auf den Verwaltungsschnittstellen nicht zulässig ist). In diesem Fall muss der Datenverkehr vom Management Service die Appliance verlassen und dann zur Appliance zurückkehren. Sie können diesen Datenverkehr weiterleiten oder optional ein NSVLAN auf einer der Instanz zugewiesenen Schnittstelle angeben. Wenn eine Verwaltungsschnittstelle zwischen einer Instanz und dem Management Service üblich ist, muss der Datenverkehr zwischen den beiden nicht geroutet werden. Wenn Ihr Setup dies jedoch ausdrücklich erfordert, kann der Verkehr weitergeleitet werden.

Hinweis: Tagging wird in Citrix Hypervisor Version 6.0 unterstützt.

Konsolidierung mit dedizierten Schnittstellen für jede Instanz

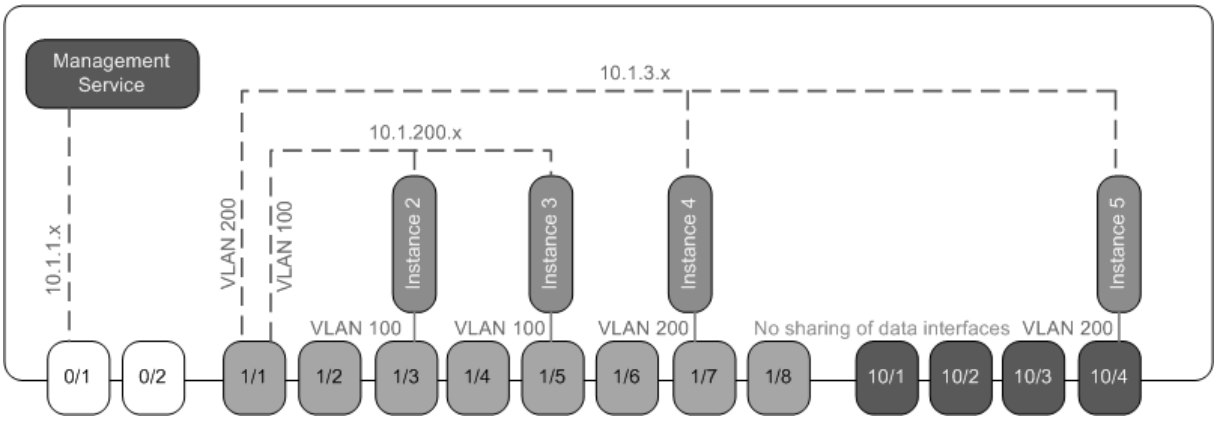
November 23, 2023

Im folgenden Beispiel sind die Instanzen Teil mehrerer Netzwerke. Die Schnittstelle 0/1 ist dem Management Service zugewiesen, der Teil des internen 10.1.1.x-Netzwerks ist. Die NetScaler-Instanzen 2 und 3 sind Teil des 10.1.200.x-Netzwerks (VLAN 100). Die NetScaler-Instanzen 4 und 5 sind Teil des 10.1.3.x-Netzwerks (VLAN 200).

Optional können Sie ein NSVLAN für alle Instanzen konfigurieren.

Die folgende Abbildung veranschaulicht den vorhergehenden Anwendungsfall.

Abbildung 1. Netzwerktopologie einer SDX-Appliance mit NetScaler-Instanzen in mehreren Netzwerken



Die SDX-Appliance ist an einen Switch angeschlossen. Stellen Sie sicher, dass die VLAN-IDs 100 und 200 auf dem Switch-Port konfiguriert sind, an den Port 1/1 der Appliance angeschlossen ist.

In der folgenden Tabelle sind die Namen und Werte der Parameter aufgeführt, die in diesem Beispiel für die Bereitstellung der NetScaler-Instanzen 5 und 3 verwendet wurden.

Parametername	Werte für Instanz 5	Werte für Instanz 3
Name	vpx5	vpx3
IP-Adresse	10.1.3.2	10.1.200.2
Netzmaske	255.255.255.0	255.255.255.240
Gateway	10.1.3.1	10.1.200.1
XVA-Datei	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
Feature-Lizenz	Platinum	Platinum
Admin-Profil	ns_nsroot_profile	ns_nsroot_profile
Benutzername	vpx5	vpx3
Kennwort	Sdx1	Wurzel
Confirm Password	Sdx1	Wurzel
Shell/Sftp/Scp Access	True	True
Gesamter Speicher (MB)	2048	2048
#SSL -Chips	1	1
Durchsatz (Mbit/s)	1000	1000
Pakete pro Sekunde	1000000	1000000
CPU	Freigegeben	Freigegeben
Schnittstelle	1/1 und 10/4	1/1 und 1/5
NSVLAN	200	100
Hinzufügen (Schnittstelle)	1/1	1/1
Getagged Interface	Wählen Sie **Tagged**	Wählen Sie **Tagged**

Um die NetScaler-Instanzen 5 und 3 bereitzustellen, wie in diesem Beispiel gezeigt

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich den Bereich **NetScaler Configuration** und klicken Sie dann auf **Instanzen**.
2. Klicken Sie im Bereich NetScaler-Instanzen auf **Hinzufügen.**
3. Folgen Sie im **Provision NetScaler Wizard** den Anweisungen im Assistenten, um die Parameter auf die in der obigen Tabelle angegebenen Werte einzustellen.
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**. Die NetScaler-Instanz, die Sie bereitgestellt haben, wird im Bereich NetScaler-Instanzen angezeigt.

Konsolidierung mit Freigabe eines physischen Port durch mehr als eine Instanz

November 23, 2023

Sie können die VLAN-Filterung auf einer Schnittstelle nach Bedarf aktivieren und deaktivieren. Um beispielsweise mehr als 100 VLANs auf einer Instanz zu konfigurieren, weisen Sie dieser Instanz eine dedizierte physische Schnittstelle zu und deaktivieren Sie die VLAN-Filterung auf dieser Schnittstelle. Aktivieren Sie die VLAN-Filterung für Instanzen, die eine physische Schnittstelle gemeinsam nutzen, sodass eine Instanz den Datenverkehr für eine andere Instanz nicht sehen kann.

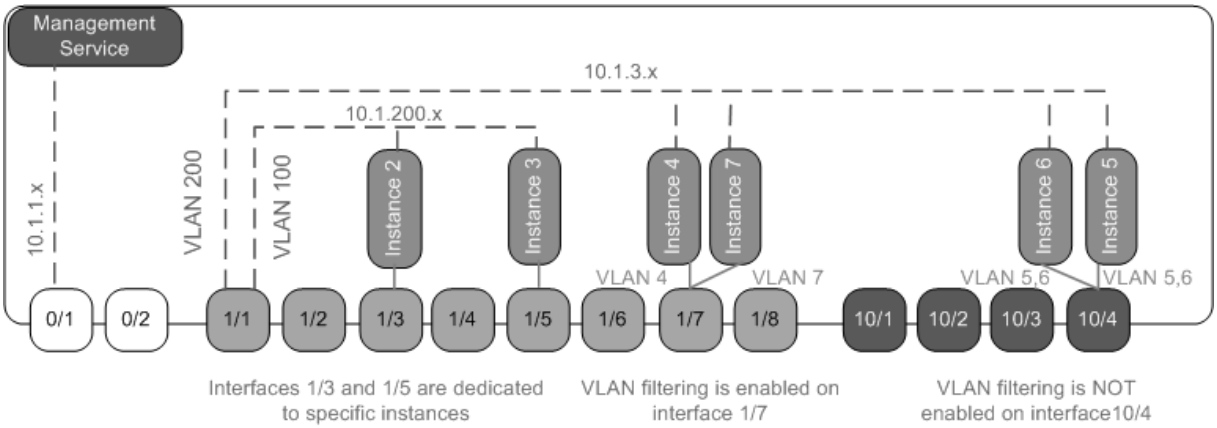
Hinweis: Die VLAN-Filterung ist keine globale Einstellung auf der Appliance. Sie aktivieren oder deaktivieren die VLAN-Filterung auf einer Schnittstelle, und die Einstellung gilt für alle Instanzen, die mit dieser Schnittstelle verknüpft sind. Wenn die VLAN-Filterung deaktiviert ist, können Sie bis zu 4096 VLANs konfigurieren. Wenn die VLAN-Filterung aktiviert ist, können Sie bis zu 63 getaggte VLANs auf einer 10G-Schnittstelle und bis zu 32 getaggte VLANs auf einer 1G-Schnittstelle konfigurieren.

Im folgenden Beispiel sind die Instanzen Teil mehrerer Netzwerke.

- Die Schnittstelle 1/1 ist allen Instanzen als Verwaltungsschnittstelle zugewiesen. Die Schnittstelle 0/1 ist dem Management Service zugewiesen, der Teil des internen 10.1.1.x-Netzwerks ist.
- Die NetScaler-Instanzen 2 und 3 befinden sich im 10.1.200.x-Netzwerk und die Instanzen 4, 5, 6 und 7 befinden sich im 10.1.3.x-Netzwerk. Die Instanzen 2 und 3 haben jeweils eine dedizierte physische Schnittstelle. Die Instanzen 4 und 7 teilen sich die physische Schnittstelle 1/7 und die Instanzen 5 und 6 teilen sich die physische Schnittstelle 10/4.
- Die VLAN-Filterung ist auf Schnittstelle 1/7 aktiviert. Der Datenverkehr für Instanz 4 ist für VLAN 4 gekennzeichnet, und der Datenverkehr für Instanz 7 ist für VLAN 7 gekennzeichnet. Daher ist der Datenverkehr für Instanz 4 für Instanz 7 nicht sichtbar. Umgekehrt ist der Datenverkehr für Instanz 7 für Instanz 4 nicht sichtbar. Auf der Schnittstelle 1/7 können maximal 32 VLANs konfiguriert werden.
- Die VLAN-Filterung ist auf Schnittstelle 10/4 deaktiviert, sodass Sie bis zu 4096 VLANs auf dieser Schnittstelle konfigurieren können. Konfigurieren Sie die VLANs 500—599 auf Instanz 5 und die VLANs 600—699 auf Instanz 6. Instanz 5 kann den Broadcast- und Multicast-Verkehr von VLAN 600—699 sehen, aber die Pakete werden auf Softwareebene verworfen. In ähnlicher Weise kann Instanz 6 den Broadcast- und Multicast-Verkehr von VLAN 500—599 sehen, aber die Pakete werden auf Softwareebene verworfen.

Die folgende Abbildung veranschaulicht den vorhergehenden Anwendungsfall.

Abbildung 1. Netzwerktopologie einer SDX-Appliance mit Management Service- und NetScaler-Instanzen, die über Netzwerke verteilt sind



In der folgenden Tabelle sind die Namen und Werte der Parameter aufgeführt, die in diesem Beispiel für die Bereitstellung der NetScaler-Instanzen 7 und 4 verwendet wurden.

Parametername	Werte für Instanz 7	Werte für Instanz 4
Name	vpx7	vpx4
IP-Adresse	10.1.3.7	10.1.3.4
Netzmaske	255.255.255.0	255.255.255.240
Gateway	10.1.3.1	10.1.3.1
XVA-Datei	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
Feature-Lizenz	Platinum	Platinum
Admin-Profil	ns_nsroot_profile	ns_nsroot_profile
Benutzername	vpx4	vpx4
Kennwort	Sdx1	Sdx1
Confirm Password	Sdx1	Sdx1
Shell/Sftp/Scp Access	True	True
Gesamter Speicher (MB)	2048	2048
#SSL -Chips	1	1
Durchsatz (Mbit/s)	1000	1000
Pakete pro Sekunde	1000000	1000000
CPU	Freigegeben	Freigegeben
Schnittstelle	1/1 und 1/7	1/1 und 1/7
NSVLAN	200	200

Um die NetScaler-Instanzen 7 und 4 in diesem Beispiel bereitzustellen

1. Erweitern Sie auf der Registerkarte **Konfiguration** im Navigationsbereich die NetScaler-Konfiguration und klicken Sie dann auf **Instances**.
2. Klicken Sie im Bereich NetScaler-Instanzen auf **Hinzufügen.**
3. Folgen Sie im Bereitstellung NetScaler Wizard den Anweisungen des Assistenten, um die Parameter auf die in der vorherigen Tabelle angegebenen Werte einzustellen.
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**. Die NetScaler-Instanz, die Sie bereitgestellt haben, wird im Bereich NetScaler-Instanzen angezeigt.

NITRO API

November 23, 2023

Mit dem NetScaler SDX NITRO-Protokoll können Sie die SDX-Appliance programmgesteuert konfigurieren und überwachen.

NITRO stellt seine Funktionalität durch Representational State Transfer (REST) -Schnittstellen zur Verfügung. Daher können NITRO-Anwendungen in jeder Programmiersprache entwickelt werden. Für Anwendungen, die in Java oder .NET oder Python entwickelt werden müssen, wird das NITRO-Protokoll als relevante Bibliotheken bereitgestellt, die als separate Software Development Kits verpackt sind.

Hinweis: Sie müssen über grundlegende Kenntnisse der SDX-Appliance verfügen, bevor Sie NITRO verwenden können.

Um das NITRO-Protokoll zu verwenden, benötigt die Clientanwendung Folgendes:

- Zugriff auf eine SDX-Appliance.
- Um REST-Schnittstellen verwenden zu können, benötigen Sie ein System zum Generieren von HTTP- oder HTTPS-Anforderungen (Nutzlast im JSON-Format) an die SDX-Appliance. Sie können jede Programmiersprache oder jedes Tool verwenden.
- Für Java-Clients benötigen Sie ein System, in dem Java Development Kit (JDK) 1.5 oder höher verfügbar ist. Das JDK kann von heruntergeladen werden http://www.oracle.com/technetwork/java/javase/downloads/index.html.
- Für .NET-Clients benötigen Sie ein System, in dem .NET-Framework 3.5 oder höher verfügbar ist. Das .NET-Framework kann unter http://www.microsoft.com/downloads/en/default.aspxheruntergeladen werden.
- Für Python-Clients benötigen Sie ein System, auf dem Python 2.7 oder höher und die Requests-Bibliothek (verfügbar in <NITRO_SDK_HOME>/lib) installiert ist.

NITRO-Paket erhalten

November 23, 2023

Das NITRO-Paket ist als TAR-Datei auf der Downloads-Seite des Konfigurationsprogramms der SDX-Appliance verfügbar. Sie müssen die Datei in einen Ordner auf Ihrem lokalen System herunterladen und enttarnen. Dieser Ordner wird <NITRO_SDK_HOME>in dieser Dokumentation genannt.

Der Ordner enthält die NITRO-Bibliotheken im
lib-Unterordner. Die Bibliotheken müssen dem Classpath der Clientanwendung hinzugefügt werden, um auf die NITRO-Funktionalität zugreifen zu können. Der
<NITRO_SDK_HOME>Ordner enthält auch Beispiele und Dokumentationen, die Ihnen helfen können, das NITRO SDK zu verstehen.

Hinweis:

- Das REST-Paket enthält nur Dokumentation zur Verwendung der REST-Schnittstellen.
- Für das Python-SDK muss die Bibliothek auf dem Clientpfad installiert sein. Für Installationsanweisungen lesen Sie die \Datei /README.txt.

.NET-SDK

November 23, 2023

SDX NITRO-APIs werden je nach Umfang und Zweck der APIs in System-APIs und Konfigurations-APIs unterteilt. Sie können auch NITRO-Vorgänge beheben.

System-APIs

Der erste Schritt zur Verwendung von NITRO besteht darin, eine Sitzung mit der SDX-Appliance einzurichten und die Sitzung anschließend mithilfe der Anmeldeinformationen des Administrators zu authentifizieren.

Erstellen Sie ein Objekt der Klasse nitro_service, indem Sie die IP-Adresse der Appliance und das Protokoll für die Verbindung mit der Appliance (HTTP oder HTTPS) angeben. Anschließend verwenden Sie dieses Objekt und melden sich bei der Appliance an, indem Sie den Benutzernamen und das Kennwort des Administrators angeben.

Hinweis: Sie müssen über ein Benutzerkonto auf dieser Appliance verfügen. Die Konfigurationsvorgänge, die Sie ausführen können, sind durch die Ihrem Konto zugewiesene Administratorrolle begrenzt.

Der folgende Beispielcode stellt mithilfe des HTTPS-Protokolls eine Verbindung zu einer SDX-Appliance mit der IP-Adresse 10.102.31.16 her:

```
1 //Specify the IP address of the appliance and service type
2 nitro_service nitroservice = new nitro_service ("10.102.31.16", "https"
      );
3
4 //Specify the login credentials
5 nitroservice.login("nsroot", "verysecret");
6 <!--NeedCopy-->
```

Hinweis: Verwenden Sie das
nitro_service-Objekt in allen weiteren NITRO-Vorgängen auf der Appliance.

Um die Verbindung zur Appliance zu trennen, rufen Sie die logout () -Methode wie folgt auf:

```
1 nitroservice.logout();
2 <!--NeedCopy-->
```

Konfigurations-APIs

Das NITRO-Protokoll kann verwendet werden, um die Ressourcen der SDX-Appliance zu konfigurieren.

Die APIs zum Konfigurieren einer Ressource sind in Pakete oder Namensräume gruppiert, die das Format com.citrix.sdx.nitro.resource.config haben.. Jedes dieser Pakete oder Namensräume enthält eine Klasse mit dem Namen das stellt die APIs zur Konfiguration der Ressource bereit.

Die NetScaler-Ressource hat beispielsweise das Paket oder den Namespace com.citrix.sdx.nitro.resource.config.ns

Eine Ressourcenklasse stellt APIs bereit, um andere Vorgänge durchzuführen. Diese Vorgänge können das Erstellen einer Ressource, das Abrufen von Ressourcen und Ressourceneigenschaften, das Aktualisieren einer Ressource, das Löschen von Ressourcen und das Durchführen von Massenvorgängen mit Ressourcen sein.

Erstellen einer Ressource

Um eine Ressource (z. B. eine NetScaler-Instanz) auf der SDX-Appliance zu erstellen:

1. Legen Sie den Wert für die erforderlichen Eigenschaften der Ressource fest, indem Sie den entsprechenden Eigenschaftsnamen verwenden. Das Ergebnis ist ein Ressourcenobjekt, das die für die Ressource erforderlichen Details enthält.

Hinweis: Diese Werte werden lokal auf dem Client festgelegt. Die Werte werden erst in der Appliance wiedergegeben, wenn das Objekt hochgeladen wurde.

2. Laden Sie das Ressourcenobjekt mithilfe der statischen add () -Methode auf die Appliance hoch.

Der folgende Beispielcode erstellt eine NetScaler-Instanz mit dem Namen „ns_instance“auf der SDX-Appliance:

```
ns newns = new ns();

//Set the properties of the NetScaler locally
newns.name = "ns_instance";
newns.ip_address = "10.70.136.5";
newns.netmask = "255.255.255.0";
newns.gateway = "10.70.136.1";
newns.image_name = "nsvpx-9.3.45_nc.xva";
newns.profile_name = "ns_nsroot_profile";
newns.vm_memory_total = 2048;
newns.throughput = 1000;
newns.pps = 1000000;
newns.license = "Standard";
newns.username = "admin";
newns.password = "admin";

int number_of_interfaces = 2;
network_interface[] interface_array = new network_interface[
   number_of_interfaces];

//Adding 10/1
interface_array[0] = new network_interface();
interface_array[0].port_name = "10/1";

//Adding 10/2
interface_array[1] = new network_interface();
interface_array[1].port_name = "10/2";

newns.network_interfaces = interface_array;

//Upload the NetScaler instance
ns result = ns.add(nitroservice, newns);
<!--NeedCopy-->
```

Ressourcendetails abrufen

Gehen Sie wie folgt vor, um die Eigenschaften einer Ressource auf der SDX-Appliance abzurufen:

1. Rufen Sie die Konfigurationen mithilfe der get () -Methode von der Appliance ab. Das Ergebnis ist ein Ressourcenobjekt.
2. Extrahieren Sie die erforderliche Eigenschaft aus dem Objekt, indem Sie den entsprechenden Eigenschaftsnamen verwenden.

Der folgende Beispielcode ruft die Details aller NetScaler-Ressourcen ab:

```
//Retrieve the resource object from the SDX appliance
ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object
Console.WriteLine(returned_ns[i].ip_address);
Console.WriteLine(returned_ns[i].netmask);
<!--NeedCopy-->
```

Ressourcen-Statistiken abrufen

Eine SDX-Appliance sammelt Statistiken über die Nutzung ihrer Funktionen. Sie können diese Statistiken mit NITRO abrufen.

Der folgende Beispielcode ruft die Statistiken einer NetScaler-Instanz mit der ID 123456a ab:

```
ns obj = new ns();
obj.id = "123456a";
ns stats = ns.get(nitroservice, obj);
Console.WriteLine("CPU Usage:" + stats.ns_cpu_usage);
Console.WriteLine("Memory Usage:" + stats.ns_memory_usage);
Console.WriteLine("Request rate/sec:" +stats.http_req);
<!--NeedCopy-->
```

Aktualisieren einer Ressource

Gehen Sie wie folgt vor, um die Eigenschaften einer vorhandenen Ressource auf der Appliance zu aktualisieren:

1. Setzt die id -Eigenschaft auf die ID der zu aktualisierenden Ressource.
2. Legen Sie den Wert für die erforderlichen Eigenschaften der Ressource fest, indem Sie den entsprechenden Eigenschaftsnamen verwenden. Das Ergebnis ist ein Ressourcenobjekt.
   Hinweis: Diese Werte werden lokal auf dem Client festgelegt. Die Werte werden erst in der Appliance wiedergegeben, wenn das Objekt hochgeladen wurde.
3. Laden Sie das Ressourcenobjekt mithilfe der update () -Methode auf die Appliance hoch.

Der folgende Beispielcode aktualisiert den Namen der NetScaler-Instanz mit der ID 123456a auf ‘ns_instance_new’:

```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated
update_obj.id = "123456a";

//Get existing NetScaler details
update_obj = ns.get(nitroservice, update_obj);
```



```
8
9  //Update the name of the NetScaler to "ns_instance_new" locally
10 update_obj.name = "ns_instance_new";
11
12 //Upload the updated NetScaler details
13 ns result = ns.update(nitroservice, update_obj);
14 <!--NeedCopy-->
```

Löschen einer Ressource

Um eine vorhandene Ressource zu löschen, rufen Sie die statische Methode delete () für die Ressourcenklasse auf, indem Sie die ID der zu entfernenden Ressource als Argument übergeben.

Der folgende Beispielcode löscht eine NetScaler-Instanz mit ID 1:

```
1 ns obj = new ns();
2 obj.id = "123456a";
3 ns.delete(nitroservice, obj);
4 <!--NeedCopy-->
```

Bulk-Operationen

Sie können mehrere Ressourcen gleichzeitig abfragen oder ändern und so den Netzwerkverkehr minimieren. Sie können beispielsweise mehrere NetScaler SDX-Appliances in derselben Operation hinzufügen.

Jede Ressourcenklasse verfügt über Methoden, die ein Array von Ressourcen zum Hinzufügen, Aktualisieren und Entfernen von Ressourcen benötigen. Um einen Massenvorgang durchzuführen, geben Sie die Details jedes Vorgangs lokal an und senden Sie die Details dann gleichzeitig an den Server.

Um den Ausfall einiger Vorgänge innerhalb des Bulk-Vorgangs zu berücksichtigen, können Sie mit NITRO eines der folgenden Verhaltensweisen konfigurieren:

- **Beenden.** Wenn der erste Fehler auftritt, stoppt die Ausführung. Die Befehle, die vor dem Fehler ausgeführt wurden, werden festgeschrieben.
- **Fahren Sie fort.** Alle Befehle in der Liste werden ausgeführt, auch wenn einige Befehle fehlschlagen.

Hinweis: Konfigurieren Sie das erforderliche Verhalten beim Herstellen einer Verbindung mit der Appliance, indem Sie den
`onerror` Parameter in der
nitro_service () -Methode festlegen.

Der folgende Beispielcode fügt zwei ADC-Appliances in einem Arbeitsgang hinzu:


```
ns[] newns = new ns[2];

//Specify details of first NetScaler
newns[0] = new ns();
newns[0].name = "ns_instance1";
newns[0].ip_address = "10.70.136.5";
newns[0].netmask = "255.255.255.0";
newns[0].gateway = "10.70.136.1";
...
...

//Specify details of second NetScaler
newns[1] = new ns();
newns[1].name = "ns_instance2";
newns[1].ip_address = "10.70.136.8";
newns[1].netmask = "255.255.255.0";
newns[1].gateway = "10.70.136.1";
...
...

//upload the details of the ADC appliances to the NITRO server
ns[] result = ns.add(nitroservice, newns);
<!--NeedCopy-->
```

Behandlung von Ausnahmen

Das Feld errorcode zeigt den Status des Vorgangs an.

- Ein Fehlercode von 0 zeigt an, dass der Vorgang erfolgreich war.
- Ein Fehlercode ungleich Null weist auf einen Fehler bei der Verarbeitung der NITRO-Anforderung hin.

Das Feld für die Fehlermeldung enthält eine kurze Erklärung und die Art des Fehlers.

Die com.citrix.sdx.nitro.exception.nitro_exception Klasse fängt alle Ausnahmen bei der Ausführung von NITRO-APIs ab. Um Informationen über die Ausnahme zu erhalten, können Sie die Methode `getErrorCode()` verwenden.

Eine detailliertere Beschreibung der Fehlercodes finden Sie in der API-Referenz, die im Ordner `<NITRO_SDK_HOME>/doc` verfügbar ist.

REST-Webdienste

November 23, 2023

REST (Representational State Transfer) ist ein Architekturstil, der auf einfachen HTTP-Anfragen und -Antworten zwischen dem Client und dem Server basiert. REST wird verwendet, um den Status von Objekten auf der Serverseite abzufragen oder zu ändern. In REST wird die Serverseite als eine Reihe von Entitäten modelliert, wobei jede Entität durch eine eindeutige URL identifiziert wird.

Jede Ressource hat auch einen Status, in dem die folgenden Vorgänge ausgeführt werden können:

- **Erstellen.** Clients können neue serverseitige Ressourcen auf einer "Container"-Ressource erstellen. Sie können sich Containerressourcen als Ordner und untergeordnete Ressourcen als Dateien oder Unterordner vorstellen. Der aufrufende Client liefert den Status für die zu erstellende Ressource. Der Status kann in der Anforderung mithilfe des XML- oder JSON-Formats angegeben werden. Der Client kann auch die eindeutige URL angeben, die das neue Objekt identifiziert. Alternativ kann der Server eine eindeutige URL auswählen und zurückgeben, die das erstellte Objekt identifiziert. Die zum Erstellen von Anforderungen verwendete HTTP-Methode ist POST.
- **Lesen.** Clients können den Status einer Ressource abrufen, indem sie ihre URL mit der Methode HTTP GET angeben. Die Antwortnachricht enthält den Ressourcenstatus, ausgedrückt im JSON-Format.
- **Aktualisieren.** Sie können den Status einer vorhandenen Ressource aktualisieren, indem Sie mithilfe der PUT-HTTP-Methode die URL angeben, die dieses Objekt und seinen neuen Status identifiziert, in JSON oder XML.
- **Löschen.** Sie können eine auf der Serverseite vorhandene Ressource löschen, indem Sie die DELETE HTTP-Methode und die URL verwenden, die die zu entfernende Ressource identifiziert.

Zusätzlich zu diesen vier CRUD-Vorgängen (Erstellen, Lesen, Aktualisieren und Löschen) können Ressourcen andere Vorgänge oder Aktionen unterstützen. Bei diesen Vorgängen wird die HTTP-POST-Methode verwendet, wobei der Request-Body in JSON den auszuführenden Vorgang und die Parameter für diesen Vorgang angibt.

SDX NITRO-APIs werden je nach Umfang und Zweck der APIs in System-APIs und Konfigurations-APIs unterteilt.

System-APIs

Der erste Schritt zur Verwendung von NITRO besteht darin, eine Sitzung mit der SDX-Appliance einzurichten und die Sitzung anschließend mithilfe der Anmeldeinformationen des Administrators zu authentifizieren.

Geben Sie den Benutzernamen und das Kennwort im Anmeldeobjekt an. Die erstellte Sitzungskennung muss im Anforderungsheader aller weiteren Vorgänge in der Sitzung angegeben werden.

Hinweis: Sie müssen über ein Benutzerkonto auf dieser Appliance verfügen. Die Konfigurationen, die Sie durchführen können, sind durch die Ihrem Konto zugewiesene Administratorrolle begrenzt.

So stellen Sie mithilfe des HTTPS-Protokolls eine Verbindung zu einer SDX-Appliance mit der IP-Adresse 10.102.31.16 her:

- **URL** `https://10.102.31.16/nitro/v2/config/login/`
- **HTTP-Methode** POST
- **Anfrage**
  - **Header**

```
Content-Type:application/vnd.com.citrix.sdx.login+json
<!--NeedCopy-->
```

Hinweis: Inhaltstypen wie "application/x-www-form-urlencoded", die in früheren Versionen von NITRO unterstützt wurden, können ebenfalls verwendet werden. Stellen Sie sicher, dass die Nutzlast mit der in früheren Versionen verwendeten identisch ist. Die in dieser Dokumentation bereitgestellten Nutzdaten sind nur anwendbar, wenn der Inhaltstyp die Form "application/vnd.com.citrix.sdx.login+json"hat.

  - **Payload**

```
{

    "login":
    {

        "username":"nsroot",
        "password":"verysecret"
     }

 }

<!--NeedCopy-->
```

- **Nutzlast der Antwort**
  - **Header**

```
HTTP/1.0 201 Created
Set-Cookie:
NITRO_AUTH_TOKEN=##87305E9C51B06C848F0942; path=/nitro/v2
<!--NeedCopy-->
```

Hinweis: Verwenden Sie die Sitzungs-ID bei allen weiteren NITRO-Vorgängen auf der Appliance.

Hinweis: Standardmäßig läuft die Verbindung zur Appliance nach 30 Minuten Inaktivität ab. Sie können den Timeout-Zeitraum ändern, indem Sie im
Anmeldeobjekt einen neuen Timeout-Zeitraum (in Sekunden) angeben. Um beispielsweise den Timeout-Zeitraum auf 60 Minuten zu ändern, lautet die Anforderungsnutzlast:

```
{
```



```
2
3     "login":
4     {
5
6         "username":"nsroot",
7         "password":"verysecret",
8         "timeout":3600
9      }
10
11  }
12
13 <!--NeedCopy-->
```

Sie können auch eine Verbindung zur Appliance herstellen, um einen einzelnen Vorgang durchzuführen, indem Sie den Benutzernamen und das Kennwort im Anforderungsheader des Vorgangs angeben. So stellen Sie beispielsweise eine Verbindung zu einer Appliance her, während Sie eine NetScaler-Instanz erstellen:

- **URL**
- **HTTP-Methode**
- **Anfrage**
  - **Header**

```
1  X-NITRO-USER:nsroot
2  X-NITRO-PASS:verysecret
3  Content-Type:application/vnd.com.citrix.sdx.ns+json
4  <!--NeedCopy-->
```

  - **Payload**

```
1  {
2
3      "ns":
4      {
5
6          ...
7       }
8
9   }
10
11 <!--NeedCopy-->
```

- **Antwort.**
  - **Header**

```
1  HTTP/1.0 201 Created
2  <!--NeedCopy-->
```

Verwenden Sie die DELETE-Methode, um die Verbindung zur Appliance zu trennen

- **URL**
- **HTTP Methode** DELETE
- **Anfrage**
  - **Header**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.login+json
<!--NeedCopy-->
```

Konfigurations-APIs

Das NITRO-Protokoll kann verwendet werden, um die Ressourcen der SDX-Appliance zu konfigurieren.

Jeder SDX-Ressource ist je nach Art des auszuführenden Vorgangs eine eindeutige URL zugeordnet. URLs für Konfigurationsvorgänge haben das Format: `http://<IP>/nitro/v2/config/<resource_type>`

Erstellen einer Ressource

Um eine Ressource (z. B. eine NetScaler-Instanz) auf der SDX-Appliance zu erstellen, geben Sie den Ressourcennamen und andere verwandte Argumente in dem spezifischen Ressourcenobjekt an. Um beispielsweise eine NetScaler-Instanz mit dem Namen vpx1 zu erstellen:

- **URL**
- **HTTP-Methode**
- **Anfrage**
  - **Header**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
<!--NeedCopy-->
```

  - **Payload**

```
{

    "ns":
    {

        "name":"vpx1",
        "ip_address":"192.168.100.2",
        "netmask":"255.255.255.0",
        "gateway":"192.168.100.1",
        "image_name":"nsvpx-9.3-45_nc.xva",
```



```
            "vm_memory_total":2048,
            "throughput":1000,
            "pps":1000000,
            "license":"Standard",
            "profile_name":"ns_nsroot_profile",
            "username":"admin",
            "password":"admin",
            "network_interfaces":
            [
                {

                    "port_name":"10/1"
                 }
,
                {

                    "port_name":"10/2"
                 }

            ]
        }

 }

<!--NeedCopy-->
```

Abrufen von Ressourcendetails und Statistiken

SDX-Ressourcendetails können wie folgt abgerufen werden:

- Um Details einer bestimmten Ressource auf der SDX-Appliance abzurufen, geben Sie die ID der Ressource in der URL an.
- Um die Eigenschaften von Ressourcen basierend auf einem Filter abzurufen, geben Sie die Filterbedingungen in der URL an.

  Die URL hat das Formular: `http://<IP>/nitro/v2/config/<resource_type>?filter=<property1>:<value>,<property2>:<value>`
- Wenn Ihre Anfrage wahrscheinlich zu vielen Ressourcen führt, die von der Appliance zurückgegeben werden, können Sie diese Ergebnisse in Chunks abrufen, indem Sie sie in "Seiten" aufteilen und sie Seite für Seite abrufen.

  Nehmen wir beispielsweise an, dass Sie alle NetScaler-Instanzen auf einem SDX abrufen möchten, das 53 davon hat. Anstatt alle 53 in einer großen Antwort abzurufen, konfigurieren Sie die Ergebnisse so, dass sie in Seiten mit jeweils 10 NetScaler-Instanzen aufgeteilt werden (insgesamt 6 Seiten). Rufen Sie sie dann Seite für Seite vom Server ab.

  Sie geben die Seitenzahl mit dem Abfragezeichenfolgenparameter für das Seitenformat an

und verwenden den Abfragezeichenfolgenparameter für die Seitenzahl, um die Seitenzahl anzugeben, die Sie abrufen möchten.
Die URL hat das Formular: `http://<IP>/nitro/v2/config/<resource_type>?pageno=<value>&pagesize=<value>`

Sie müssen nicht alle Seiten abrufen oder die Seiten der Reihe nach abrufen. Jede Anfrage ist unabhängig, und Sie können sogar die Seitengrößeneinstellung zwischen Anforderungen ändern.

Hinweis: Um eine Vorstellung von der Anzahl der Ressourcen zu erhalten, die wahrscheinlich von einer Anforderung zurückgegeben werden, können Sie den Abfragezeichenfolgenparameter "count"verwenden, um eine Anzahl der zurückzugebenden Ressourcen anstelle der Ressourcen selbst anzufordern. Um die Anzahl der verfügbaren NetScaler-Instances zu ermitteln, wäre die URL
`http://<IP>/nitro/v2/config/<resource_type>?count=yes`

So rufen Sie die Konfigurationsinformationen für die NetScaler-Instanz mit der ID 123456a ab:

- **URL**
- **HTTP-Methode** GET

Aktualisieren einer Ressource

Um eine vorhandene SDX-Ressource zu aktualisieren, verwenden Sie die PUT-HTTP-Methode. Geben Sie in der Nutzlast der HTTP-Anforderung den Namen und die anderen Argumente an, die geändert werden müssen. Um beispielsweise den Namen der NetScaler-Instanz mit der ID 123456a in vpx2 zu ändern:

- **URL**
- **HTTP-Methode**
- **Nutzlast anfragen**
  - **Header**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
<!--NeedCopy-->
```

  - **Payload**

```
{

    "ns":
    {

        "name":"vpx2",
```



```
            "id":"123456a"
        }

    }

<!--NeedCopy-->
```

Löschen einer Ressource

Um eine vorhandene Ressource zu löschen, geben Sie in der URL den Namen der zu löschenden Ressource an. Um beispielsweise eine NetScaler-Instanz mit der ID 123456a zu löschen:

- **URL**
- **HTTP-Methode**
- **Anfrage**
  - **Header**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
<!--NeedCopy-->
```

Bulk-Operationen

Sie können mehrere Ressourcen gleichzeitig abfragen oder ändern und so den Netzwerkverkehr minimieren. Sie können beispielsweise mehrere NetScaler SDX-Appliances in derselben Operation hinzufügen. Sie können auch Ressourcen verschiedener Typen in einer Anforderung hinzufügen.

Um den Ausfall einiger Vorgänge innerhalb des Bulk-Vorgangs zu berücksichtigen, können Sie mit NITRO eines der folgenden Verhaltensweisen konfigurieren:

- **Beenden.** Wenn der erste Fehler auftritt, stoppt die Ausführung. Die Befehle, die vor dem Fehler ausgeführt wurden, werden festgeschrieben.
- **Fahren Sie fort.** Alle Befehle in der Liste werden ausgeführt, auch wenn einige Befehle fehlschlagen.

Hinweis: Konfigurieren Sie das erforderliche Verhalten im Request-Header mithilfe des Parameters `X-NITRO-ONERROR`.

So fügen Sie 2 NetScaler-Ressourcen in einem Vorgang hinzu und fahren fort, wenn ein Befehl fehlschlägt:

- **URL.**
- **HTTP-Methode.**
- **Nutzlast anfordern.**

- **Header**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
X-NITRO-ONERROR:continue
<!--NeedCopy-->
```

- **Payload**

```
{

    "ns":
    [
        {

            "name":"ns_instance1",
            "ip_address":"10.70.136.5",
            "netmask":"255.255.255.0",
            "gateway":"10.70.136.1"
         }
,
        {

            "name":"ns_instance2",
            "ip_address":"10.70.136.8",
            "netmask":"255.255.255.0",
            "gateway":"10.70.136.1"
         }

    ]
 }

<!--NeedCopy-->
```

Um mehrere Ressourcen (NetScaler und zwei MPS-Benutzer) in einem Vorgang hinzuzufügen und fortzufahren, falls ein Befehl fehlschlägt:

- **URL.**
- **HTTP-Methode.** POST
- **Nutzlast anfordern.**

- **Header**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
X-NITRO-ONERROR:continue
<!--NeedCopy-->
```

- **Payload**

```
{

    "ns":
```



```
4       [
5           {
6
7               "name":"ns_instance1",
8               "ip_address":"10.70.136.5",
9               "netmask":"255.255.255.0",
10              "gateway":"10.70.136.1"
11           }
12  ,
13          {
14
15              "name":"ns_instance2",
16              "ip_address":"10.70.136.8",
17              "netmask":"255.255.255.0",
18              "gateway":"10.70.136.1"
19           }
20
21      ],
22       "mpsuser":
23      [
24          {
25
26              "name":"admin",
27              "password":"admin",
28              "permission":"superuser"
29           }
30  ,
31          {
32
33              "name":"admin",
34              "password":"admin",
35              "permission":"superuser"
36           }
37
38      ]
39   }
40
41  <!--NeedCopy-->
```

Behandlung von Ausnahmen

Das Feld errorcode zeigt den Status des Vorgangs an.

- Ein Fehlercode von 0 zeigt an, dass der Vorgang erfolgreich war.
- Ein Fehlercode ungleich Null weist auf einen Fehler bei der Verarbeitung der NITRO-Anforderung hin.

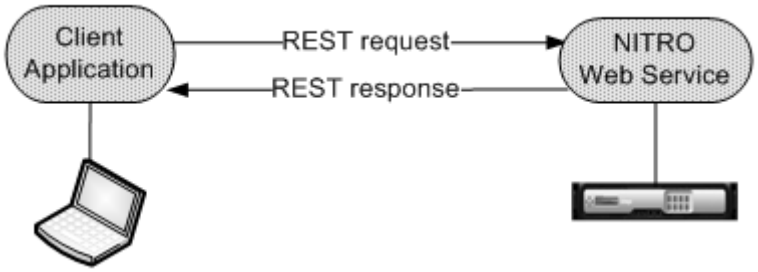
Das Feld für die Fehlermeldung enthält eine kurze Erklärung und die Art des Fehlers.

So funktioniert NITRO

November 23, 2023

Die NITRO-Infrastruktur besteht aus einer Client-Anwendung und dem NITRO-Webservice, der auf einer NetScaler SDX-Appliance ausgeführt wird. Die Kommunikation zwischen der Clientanwendung und dem NITRO-Webservice basiert auf der REST-Architektur unter Verwendung von HTTP oder HTTPS.

Abbildung 1. NITRO-Workflow



Schritte zur Beschreibung des Arbeitsablaufs:

1. Die Clientanwendung sendet eine REST-Anforderungsnachricht an den NITRO-Webdienst. Bei Verwendung der SDKs wird ein API-Aufruf in die entsprechende REST-Anforderungsnachricht übersetzt.
2. Der Webdienst verarbeitet die REST-Anforderungsnachricht.
3. Der NITRO-Webdienst gibt die entsprechende REST-Antwortnachricht an die Clientanwendung zurück. Bei Verwendung der SDKs wird die REST-Antwortnachricht in die entsprechende Antwort für den API-Aufruf übersetzt.

Um den Datenverkehr im Netzwerk zu minimieren, rufen Sie den gesamten Status einer Ressource vom Server ab. Nehmen Sie lokal Änderungen am Zustand der Ressource vor. Laden Sie es dann in einer Netzwerktransaktion wieder auf den Server hoch.

Hinweis: Lokale Operationen an einer Ressource (Änderung ihrer Eigenschaften) wirken sich erst auf ihren Status auf dem Server aus, wenn der Status des Objekts explizit hochgeladen wird.

NITRO-APIs sind synchron. Das heißt, die Clientanwendung wartet auf eine Antwort des NITRO-Webdienstes, bevor sie eine weitere NITRO-API ausführt.

SDK

November 23, 2023

SDX NITRO-APIs werden je nach Umfang und Zweck der APIs in System-APIs und Konfigurations-APIs unterteilt. Sie können auch NITRO-Vorgänge beheben.

System-APIs

Der erste Schritt zur Verwendung von NITRO besteht darin, eine Sitzung mit der SDX-Appliance einzurichten und die Sitzung anschließend mithilfe der Anmeldeinformationen des Administrators zu authentifizieren.

Erstellen Sie ein Objekt der Klasse nitro_service, indem Sie die IP-Adresse der Appliance und das Protokoll für die Verbindung mit der Appliance (HTTP oder HTTPS) angeben. Anschließend verwenden Sie dieses Objekt und melden sich bei der Appliance an, indem Sie den Benutzernamen und das Kennwort des Administrators angeben.

Hinweis: Sie müssen über ein Benutzerkonto auf dieser Appliance verfügen. Die Konfigurationsvorgänge, die Sie ausführen können, sind durch die Ihrem Konto zugewiesene Administratorrolle begrenzt.

Der folgende Beispielcode stellt mithilfe des HTTPS-Protokolls eine Verbindung zu einer SDX-Appliance mit der IP-Adresse 10.102.31.16 her:

```
1 //Specify the IP address of the appliance and service type
2 nitro_service nitroservice = new nitro_service ("10.102.31.16", "https"
      );
3
4 //Specify the login credentials
5 nitroservice.login("nsroot", "verysecret");
6 <!--NeedCopy-->
```

Hinweis: Verwenden Sie das
nitro_service-Objekt in allen weiteren NITRO-Vorgängen auf der Appliance.

Um die Verbindung zur Appliance zu trennen, rufen Sie die Methode `logout()` wie folgt auf:

```
1 nitroservice.logout();
2 <!--NeedCopy-->
```

Konfigurations-APIs

Das NITRO-Protokoll kann verwendet werden, um die Ressourcen der SDX-Appliance zu konfigurieren.

Die APIs zum Konfigurieren einer Ressource sind in Pakete oder Namensräume gruppiert, die das Format com.citrix.sdx.nitro.resource.config haben.. Jedes dieser Pakete oder Namensräume enthält eine Klasse mit dem Namen das stellt die APIs zur Konfiguration der Ressource bereit.

Die NetScaler-Ressource hat beispielsweise das Paket oder den Namespace com.citrix.sdx.nitro.resource.config.ns

Eine Ressourcenklasse stellt APIs bereit, um viele andere Vorgänge durchzuführen. Diese Vorgänge können das Erstellen einer Ressource, das Abrufen von Ressourcendetails und Statistiken, das Aktualisieren einer Ressource, das Löschen von Ressourcen und das Ausführen von Massenvorgängen für Ressourcen sein.

Erstellen einer Ressource

Gehen Sie wie folgt vor, um eine Ressource (z. B. eine NetScaler-Instanz) auf der SDX-Appliance zu erstellen:

1. Legen Sie den Wert für die erforderlichen Eigenschaften der Ressource fest, indem Sie den entsprechenden Eigenschaftsnamen verwenden. Das Ergebnis ist ein Ressourcenobjekt, das die für die Ressource erforderlichen Details enthält.
   Hinweis: Diese Werte werden lokal auf dem Client festgelegt. Die Werte werden erst in der Appliance wiedergegeben, wenn das Objekt hochgeladen wurde.
2. Laden Sie das Ressourcenobjekt mithilfe der statischen add () -Methode auf die Appliance hoch.

Der folgende Beispielcode erstellt eine NetScaler-Instanz mit dem Namen „ns_instance“auf der SDX-Appliance:

```
ns newns = new ns();

//Set the properties of the NetScaler locally
newns.set_name("ns_instance");
newns.set_ip_address("10.70.136.5");
newns.set_netmask("255.255.255.0");
newns.set_gateway("10.70.136.1");
newns.set_image_name("nsvpx-9.3.45_nc.xva");
newns.set_profile_name("ns_nsroot_profile");
newns.set_vm_memory_total(new Double(2048));
newns.set_throughput(new Double(1000));
newns.set_pps(new Double(1000000));
newns.set_license("Standard");
newns.set_username("admin");
newns.set_password("admin");

int number_of_interfaces = 2;
network_interface[] interface_array = new network_interface[
    number_of_interfaces];

//Adding 10/1
interface_array[0] = new network_interface();
```



```
interface_array[0].set_port_name("10/1");

//Adding 10/2
interface_array[1] = new network_interface();
interface_array[1].set_port_name("10/2");

newns.set_network_interfaces(interface_array);

//Upload the NetScaler instance
ns result = ns.add(nitroservice, newns);
<!--NeedCopy-->
```

Ressourcendetails werden abgerufen

Gehen Sie wie folgt vor, um die Eigenschaften einer Ressource auf der SDX-Appliance abzurufen:

1. Rufen Sie die Konfigurationen mithilfe der get () -Methode von der Appliance ab. Das Ergebnis ist ein Ressourcenobjekt.
2. Extrahieren Sie die erforderliche Eigenschaft aus dem Objekt, indem Sie den entsprechenden Eigenschaftsnamen verwenden.

Der folgende Beispielcode ruft die Details aller NetScaler-Ressourcen ab:

```
//Retrieve the resource object from the SDX appliance
ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object
System.out.println(returned_ns[i].get_ip_address());
System.out.println(returned_ns[i].get_netmask());
<!--NeedCopy-->
```

Ressourcenstatistiken abrufen

Eine SDX-Appliance sammelt Statistiken über die Nutzung ihrer Funktionen. Sie können diese Statistiken mit NITRO abrufen.

Der folgende Beispielcode ruft die Statistiken einer NetScaler-Instanz mit der ID 123456a ab:

```
ns obj = new ns();
obj.set_id("123456a");
ns stats = ns.get(nitroservice, obj);
System.out.println("CPU Usage:" + stats.get_ns_cpu_usage());
System.out.println("Memory Usage:" + stats.get_ns_memory_usage());
System.out.println("Request rate/sec:" +stats.get_http_req());
<!--NeedCopy-->
```


Aktualisieren einer Ressource

Gehen Sie wie folgt vor, um die Eigenschaften einer vorhandenen Ressource auf der Appliance zu aktualisieren:

1. Setzt die id -Eigenschaft auf die ID der zu aktualisierenden Ressource.
2. Legen Sie den Wert für die erforderlichen Eigenschaften der Ressource fest, indem Sie den entsprechenden Eigenschaftsnamen verwenden. Das Ergebnis ist ein Ressourcenobjekt.
   Hinweis: Diese Werte werden lokal auf dem Client festgelegt. Die Werte werden erst in der Appliance wiedergegeben, wenn das Objekt hochgeladen wurde.
3. Laden Sie das Ressourcenobjekt mithilfe der update () -Methode auf die Appliance hoch.

Der folgende Beispielcode aktualisiert den Namen der NetScaler-Instanz mit der ID 123456a auf 'ns_instance_new':

```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated
update_obj.set_id("123456a");

//Get existing NetScaler details
update_obj = ns.get(nitroservice, update_obj);

//Update the name of the NetScaler to "ns_instance_new" locally
update_obj.set_name("ns_instance_new");

//Upload the updated NetScaler details
ns result = ns.update(nitroservice, update_obj);
<!--NeedCopy-->
```

Eine Ressource löschen

Um eine vorhandene Ressource zu löschen, rufen Sie die statische Methode delete () für die Ressourcenklasse auf, indem Sie die ID der zu entfernenden Ressource als Argument übergeben.

Der folgende Beispielcode löscht eine NetScaler-Instanz mit ID 1:

```
ns obj = new ns();
obj.set_id("123456a");
ns.delete(nitroservice, obj);
<!--NeedCopy-->
```

Bulk-Vorgänge

Sie können mehrere Ressourcen gleichzeitig abfragen oder ändern und so den Netzwerkverkehr minimieren. Sie können beispielsweise mehrere NetScaler SDX-Appliances in derselben Operation

hinzufügen.

Jede Ressourcenklasse verfügt über Methoden, die ein Array von Ressourcen zum Hinzufügen, Aktualisieren und Entfernen von Ressourcen benötigen. Um einen Massenvorgang durchzuführen, geben Sie die Details jedes Vorgangs lokal an und senden Sie die Details dann gleichzeitig an den Server.

Um den Ausfall einiger Vorgänge innerhalb des Bulk-Vorgangs zu berücksichtigen, können Sie mit NITRO eines der folgenden Verhaltensweisen konfigurieren:

- **Beenden.** Wenn der erste Fehler auftritt, stoppt die Ausführung. Die Befehle, die vor dem Fehler ausgeführt wurden, werden festgeschrieben.
- **Fahren Sie fort.** Alle Befehle in der Liste werden ausgeführt, auch wenn einige Befehle fehlschlagen.

Hinweis: Konfigurieren Sie das erforderliche Verhalten beim Herstellen einer Verbindung mit der Appliance, indem Sie den
`onerror` Parameter in der
nitro_service () -Methode festlegen.

Der folgende Beispielcode fügt zwei ADC-Appliances in einem Arbeitsgang hinzu:

```
ns[] newns = new ns[2];

//Specify details of first NetScaler
newns[0] = new ns();
newns[0].set_name("ns_instance1");
newns[0].set_ip_address("10.70.136.5");
newns[0].set_netmask("255.255.255.0");
newns[0].set_gateway("10.70.136.1");
...
...
...

//Specify details of second NetScaler
newns[1] = new ns();
newns[1].set_name("ns_instance2");
newns[1].set_ip_address("10.70.136.8");
newns[1].set_netmask("255.255.255.0");
newns[1].set_gateway("10.70.136.1");
...
...

//upload the details of the NetScalers to the NITRO server
ns[] result = ns.add(nitroservice, newns);
<!--NeedCopy-->
```

Behandlung von Ausnahmen

Das Feld errorcode zeigt den Status des Vorgangs an.

- Ein Fehlercode von 0 zeigt an, dass der Vorgang erfolgreich war.
- Ein Fehlercode ungleich Null weist auf einen Fehler bei der Verarbeitung der NITRO-Anforderung hin.

Das Feld für die Fehlermeldung enthält eine kurze Erklärung und die Art des Fehlers.

Die com.citrix.sdx.nitro.exception.nitro_exception Klasse fängt alle Ausnahmen bei der Ausführung von NITRO-APIs ab. Um Informationen über die Ausnahme zu erhalten, können Sie die Methode `getErrorCode()` verwenden.

Eine detailliertere Beschreibung der Fehlercodes finden Sie in der API-Referenz, die im Ordner `<NITRO_SDK_HOME>/doc` verfügbar ist.