NetScaler Application Delivery Management 13.0

Machine translated content

Disclaimer

Contents

Versionshinweise

February 5, 2024

In den Versionshinweisen für NetScaler Application Delivery Management (ADM) 13.0 werden die neuen Features, Erweiterungen vorhandener Features und die bekannten Probleme in einem Build beschrieben. Das Release Notes Dokument für die Version 13.0 enthält die folgenden Abschnitte:

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

Um das vollständige Dokument mit den Versionshinweisen anzuzeigen, klicken Sie auf den folgenden Link:

Versionshinweise	Datum der Veröffentlichung	Version
Versionshinweise für Build 92.18 der Version Citrix ADM 13.0	Veröffentlicht: 06. September 2023	Version der Versionshinweise: 1.0
Versionshinweise für Build 91.12 der Citrix ADM 13.0-Version	Veröffentlicht: 18. Mai 2023	Version der Versionshinweise: 1.0
Versionshinweise für Build 90.7 der NetScaler ADM 13.0-Version	Veröffentlichung: 01. Februar 2023	Version der Versionshinweise: 1.0
Versionshinweise für Build 89.7 der NetScaler ADM 13.0-Version	Veröffentlichung: 19. Dezember 2022	Version der Versionshinweise: 1.0
Versionshinweise für Build 88.12 von NetScaler ADM 13.0	Veröffentlichung: 20. Oktober 2022	Version der Versionshinweise: 1.0
Versionshinweise für Build 87.9 von NetScaler ADM 13.0	Veröffentlichung: 06. Februar 2023	Version der Release: 2.0
Versionshinweise für Build 86.17 von NetScaler ADM 13.0	Veröffentlichung: 20. Juni 2022	Version der Versionshinweise: 1.0
Versionshinweise für Build 85.19 von NetScaler ADM 13.0	Veröffentlichung: 14. Juni 2022	Version der Versionshinweise: 1.0

Versionshinweise	Datum der Veröffentlichung	Version
Versionshinweise für Build 84.10 von NetScaler ADM 13.0	Veröffentlicht: 14. Dezember 2021	Version der Versionshinweise: 1.0
Versionshinweise für Build 83.27 von NetScaler ADM 13.0	Veröffentlichung: 28. September 2021	Version der Versionshinweise: 1.0
Versionshinweise für Build 82.41 von NetScaler ADM 13.0	Veröffentlichung: 09. Juni 2021	Version der Versionshinweise: 1.0
Versionshinweise für Build 79.64 von NetScaler ADM 13.0	Veröffentlicht: 06. April 2021	Version der Versionshinweise: 1.0
Versionshinweise für Build 76.29 von NetScaler ADM 13.0	Veröffentlicht: 19. Februar 2021	Version der Versionshinweise: 1.0
Versionshinweise für Build 71.40 von NetScaler ADM 13.0	Veröffentlicht: 20. Januar 2021	Version der Release: 2.0
Versionshinweise für Build 67.42 von NetScaler ADM 13.0	Veröffentlicht: 28. Oktober 2020	Version der Release-Notiz: 1.0 **Hinweis**: Build 67.42 ersetzt Build 67.39
Versionshinweise für Build 67.39 von NetScaler ADM 13.0	Veröffentlicht: 16. Oktober 2020	Version der Release: 2.0
Versionshinweise für Build 64.35 von NetScaler ADM 13.0	Veröffentlicht: 16. Oktober 2020	Version der Release: 2.0
Versionshinweise für Build 61.48 von NetScaler ADM 13.0	Veröffentlicht: 18. September 2020	Version der Release: 2.0
Versionshinweise für Build 58.30 der NetScaler ADM 13.0 Version	Veröffentlichung: 10. Juni 2020	Version der Versionshinweise: 1.0
Versionshinweise für Build 52.24 von NetScaler ADM 13.0	Veröffentlichung: 26. März 2020	Version der Versionshinweise: 1.0
Versionshinweise für Build 47.22 von NetScaler ADM 13.0	Veröffentlicht: 10. Dezember 2019	Version der Versionshinweise: 1.0
Versionshinweise für Build 41.28 von NetScaler ADM 13.0	Veröffentlicht: 27. September 2019 (Build 41.28 ersetzt Build 41.22)	Version der Versionshinweise: 1.0

> **Hinweis**
>
> Diese Versionshinweise dokumentieren keine sicherheitsrelevanten Korrekturen. Eine Liste der sicherheitsbezogenen Fixes und Advisorys finden Sie im Citrix Security Bulletin.

On-premises NetScaler ADM auf Citrix Cloud migrieren

February 5, 2024

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

ADM Service über Citrix Cloud ermöglicht Ihnen:

- Schnellere Releases, ungefähr alle zwei Wochen mit den neuesten Feature-Updates.
- Auf maschinellem Lernen basierende Analysen für Anwendungssicherheit und Bot, Performance und Nutzung.
- Verschiedene andere Funktionen, die derzeit nur im ADM-Service unterstützt werden, wie Peak- und Lean-Periodenanalyse, auf maschinellem Lernen basierende Analysen für Anwendungssicherheit und Bot, CPU-Analyse für Anwendungen und vieles mehr.

Für eine erfolgreiche Migration müssen Sie:

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

Wenn Sie nach der Migration vom on-premises ADM zu ADM Service wieder mit on-premises ADM fortfahren möchten, können Sie das Rollback-Skript verwenden. Weitere Informationen finden Sie unter Rollback zu lokalem ADM.

ADM Service Agent konfigurieren

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

- Wenn in Ihrem vorhandenen on-premises ADM (Standalone oder HA-Paar) keine On-Premises-Agents konfiguriert sind, müssen Sie mindestens einen Agent für ADM Service konfigurieren.
- Wenn Ihr vorhandenes lokales ADM (Standalone oder HA-Paar) mit On-Premises-Agents für Multisite-Bereitstellungen konfiguriert ist, müssen Sie die gleiche Anzahl von Agents für ADM Service konfigurieren.

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

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

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

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

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

Validierung der ADM Service-Lizenzen

Sie müssen Lizenzen für ADM Service erwerben.

- Die VIP-Lizenzen im ADM-Service müssen mehr als oder gleich den on-premises VIP-Lizenzen sein.

  > **Hinweis**
  >
  > Wenn VIP-Lizenzen geringer sind, werden virtuelle Server nach dem Zufallsprinzip ausgewählt und die VIP-Level-Konfiguration für ADM Service schlägt fehl.

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

Migrieren mit einem Skript

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

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

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

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

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

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

```
bash-3.2# cd /var
bash-3.2# pwd
/var
bash-3.2# ls -ltr secureclient.csv
-rw-r--r--  1 root  nobody  102 Dec 11 19:09 secureclient.csv
bash-3.2#
```


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

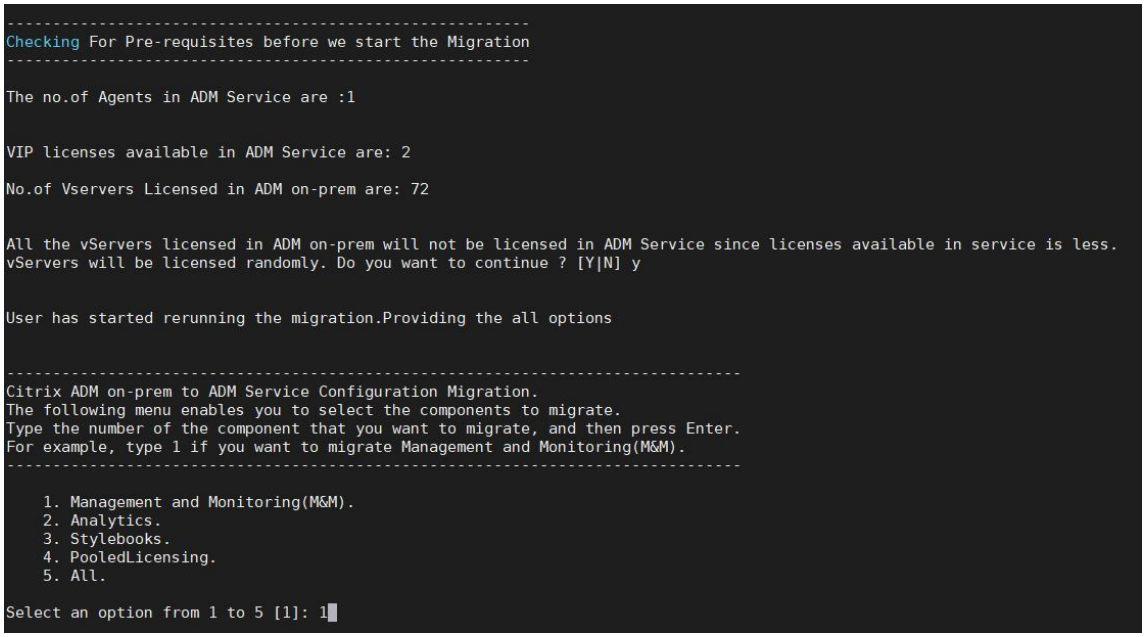
4. Führen Sie für die ADM **13.0 82.xx-Version**die folgenden Befehle aus, um die Migration abzuschließen:

   a) `cd /mps/scripts`

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

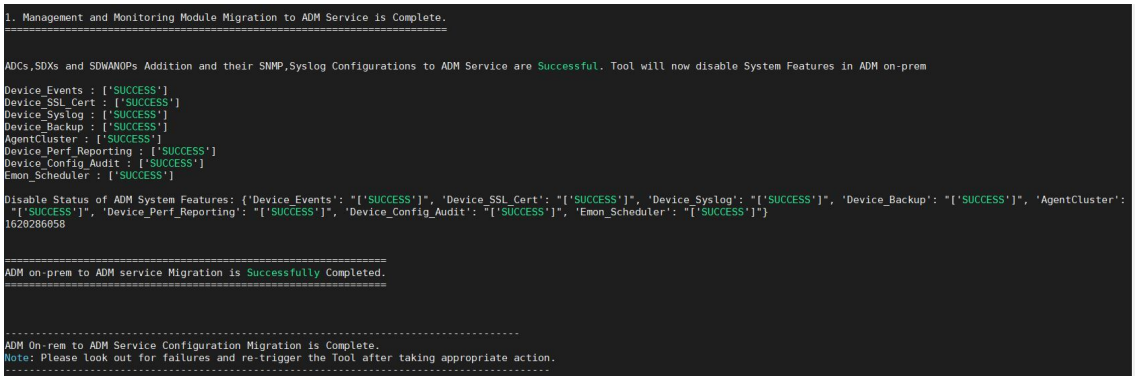
   Beispiel: `python servicemigrationtool.py /var/secureclient.csv`

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



   Abhängig von der von Ihnen bereitgestellten Auswahl wird nur diese Funktion zu ADM Service migriert.

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



Management and Monitoring (M&M) umfasst:

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

Die **Analytics-Funktion** umfasst:

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

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

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

   a) `cd /mps/scripts`

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

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

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

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

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

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

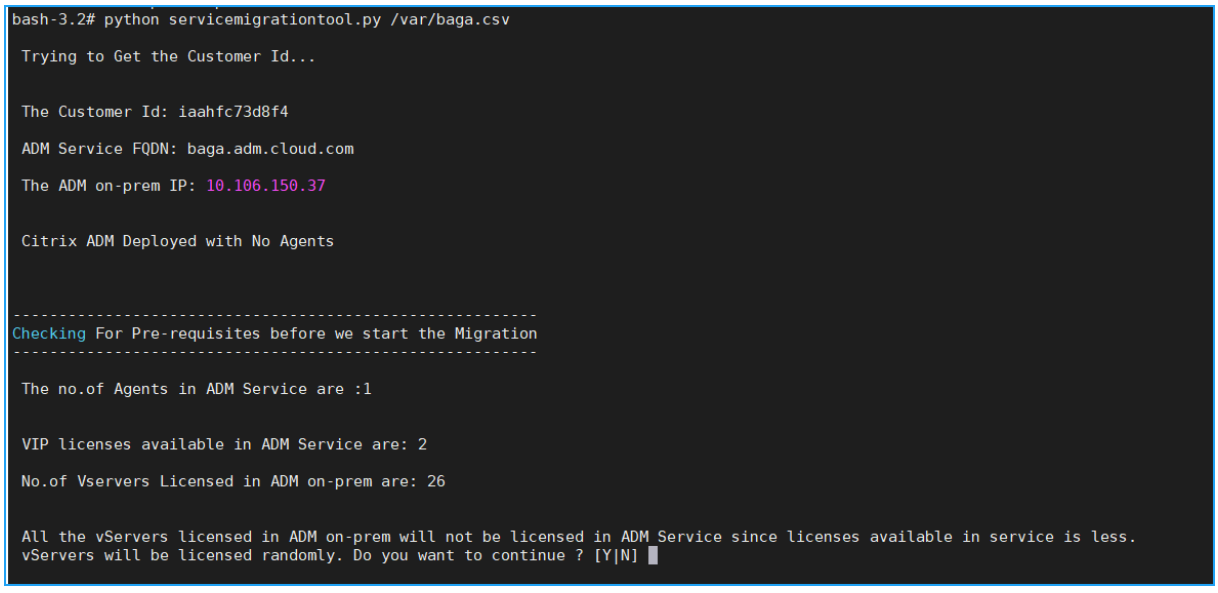
   c) Führen Sie die folgenden Befehle zur Migration aus:

      i. `cd /var`

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

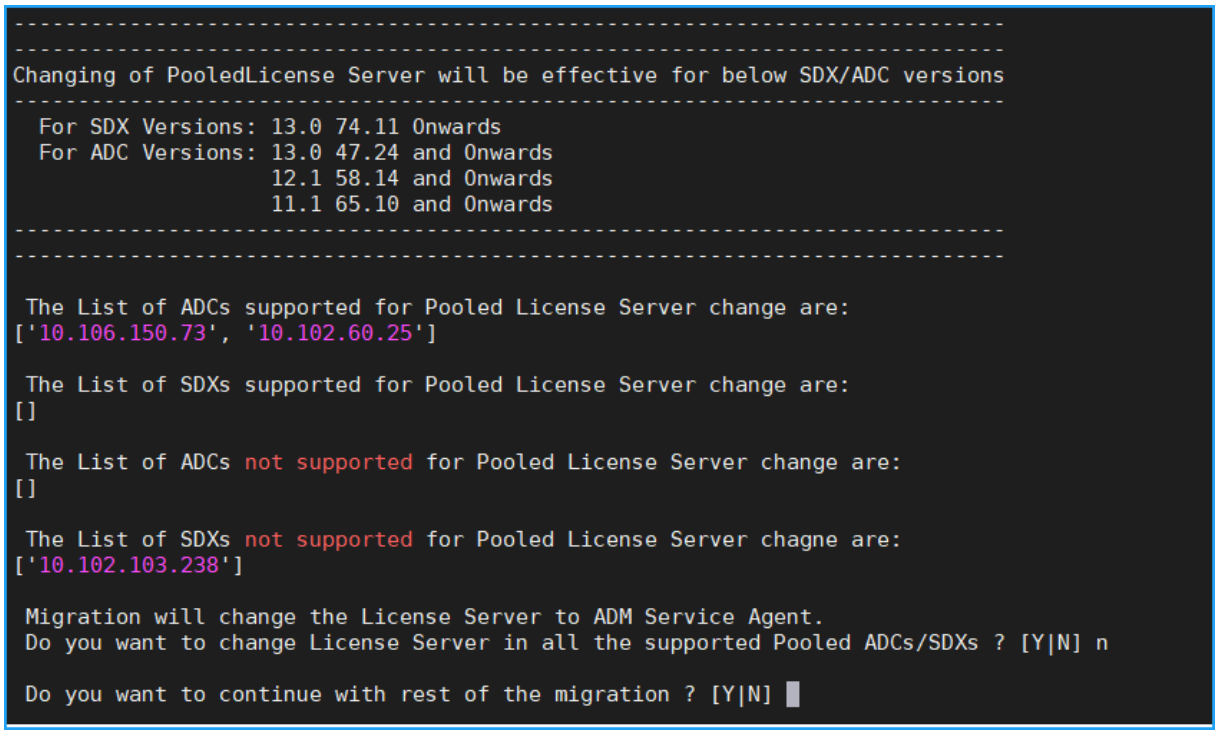
      Beispiel: `python servicemigrationtool_27.py /var/secureclient.csv`

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



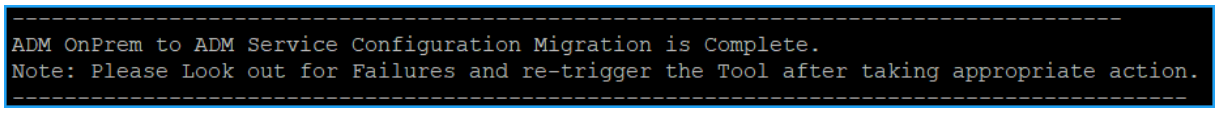
Wenn Sie **Y**auswählen, wird die Migration fortgesetzt, indem Sie den VIP nach dem Zufallsprinzip lizenzieren. Wenn Sie **N**wählen, stoppt das Skript die Migration.

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



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

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



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

- SSL-Zertifikate
- Syslog-Nachrichten
- Backup
- Agenten-Cluster
- Performance-Berichte

- Konfigurationsaudit
- Emon Planer

Rollback zu On-Premises ADM

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

Voraussetzungen

Für Ihr lokales ADM (vor der Migration zu ADM Service) gilt:

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

Verwenden Sie das Rollbackskript

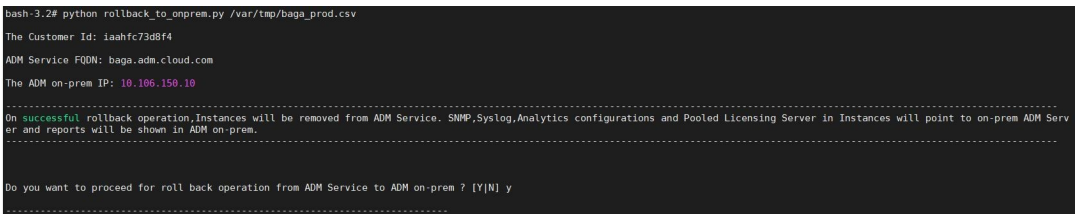
> Hinweis
>
> Nach dem Rollback sind dieselben Konfigurationen (vor der Migration) in Analytics, SNMP und gepoolte Lizenzierung wieder im on-premises ADM verfügbar. Wenn Sie nach der Migration Änderungen an diesen Konfigurationen vorgenommen haben, werden diese Änderungen nicht im on-premises ADM berücksichtigt.

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

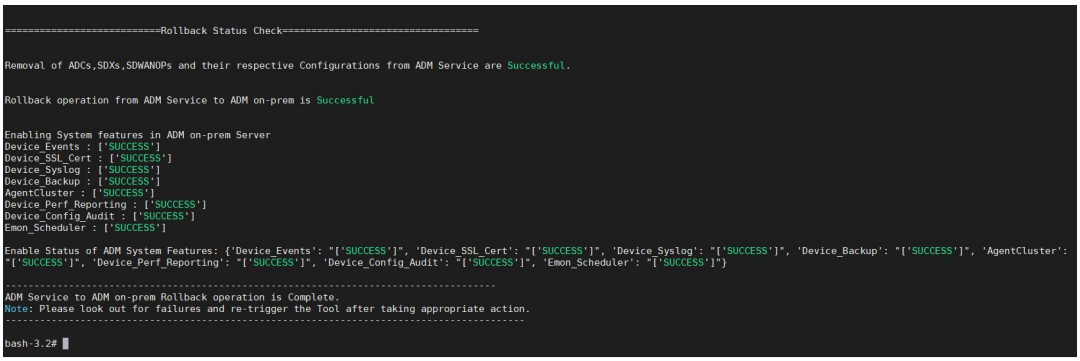
1. Melden Sie sich mit einem SSH-Client beim on-premises ADM an.
2. Geben Sie shell ein und drücken Sie die Eingabetaste, um in den Bash-Modus zu wechseln.
3. Führen Sie für ADM **13.0 82.xx** Build die folgenden Befehle aus, um das Rollback abzuschließen:
    a) cd /mps/scripts
    b) python rollback_to_onprem.py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

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

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



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



4. Für ADM vor 82.xx Build:

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

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

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

      i. `cd /mps/scripts`

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

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

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

      i. `cd /var`

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

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

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

Häufig gestellte Fragen

February 5, 2024

ADM Service

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

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

Warum ADM Service?

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

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

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

https://attendee.gotowebinar.com/register/4248811314610265355

Oder

https://attendee.gotowebinar.com/register/1601431406507289611

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

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

Was passiert, wenn der Agent aus irgendeinem Grund ausfällt?

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

Wird das Instanzbackup auch migriert?

Das Backup ist nicht in der Migration enthalten.

Sind historische Daten auch migriert?

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

Werden on-premises Lizenzen auch migriert?

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

Was wird nicht von on-premises NetScaler ADM migriert?

Die folgenden Funktionen können nicht auf ADM Service migriert werden:

- **RBAC** —In ADM Service basiert der Benutzerzugriff auf der Einladung des Administrators. Benutzer von ADM Service müssen ein Konto in Citrix Cloud haben. Infolgedessen werden die on-premises ADM-Benutzer nicht migriert.

- **Exportpläne** —Exportpläne enthalten Details wie Drilldown und Zeitpläne von verschiedenen Seiten. All diese detaillierten Exportpläne werden nicht migriert.
- **SSL-Zertifikate/Schlüssel/CSRs** —ADM Service kann nur die ADC SSL-Zertifikate/Schlüssel/CSRs anzeigen. Infolgedessen werden SSL-Zertifikate/Schlüssel, die auf ein on-premises NetScaler ADM hochgeladen wurden, nicht in ADM Service migriert.

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

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

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

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

Migrations-T

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

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

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

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

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

Was passiert, wenn das Migrationsskript die Konfiguration bezüglich ADC/SD-WANOP-Instanzen nicht möglich ist?

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

Was passiert, wenn einige der ADC- oder SD-WANOP-Instanzen nicht in ADM Service wechseln. Hilft die Wiederverbucht des Migrationsskripts?

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

Gibt es eine Protokolldatei, um den Migrationsstatus zu überprüfen?

Ja, eine Protokolldatei wird im `/var/mps/log/` Verzeichnis generiert. ADM mit python3.7 hat die Protokolldatei als `servicemigrationtool.py.log` und ADM mit Python 2.7 hat die Protokolldatei als `servicemigrationtool_27.py.log`.

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

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

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

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

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

Das ADM Service Express-Konto hat nur zwei virtuelle Serverlizenzen, zwei StyleBook-Konfigurationspakete und zwei Konfigurationsaufgaben. Wenn Ihr on-premises ADM mehr als diese Konfigurationen hat und Sie die Migration mit Express Account initiieren, kann das Skript nur die erwähnten Konfigurationen migrieren, die für Express Account gelten (zwei virtuelle Serverlizenzen, zwei StyleBook-Konfigurationspakete und zwei Konfigurationsaufträge)

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

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

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

Rollback-Skript

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

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

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

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

Problembehandlung

February 5, 2024

Wenn Sie das Migrationsskript zum ersten Mal ausführen, sucht es nach den Voraussetzungen und fährt mit der Migration fort. Wenn alle Voraussetzungen erfüllt sind, wird die Migration ohne Fehler

abgeschlossen. Wenn eine Voraussetzung fehlschlägt, zeigt das Skript Fehlermeldungen mit Gründen an. Nachdem Sie die Fehler behoben haben, müssen Sie das Skript erneut ausführen.

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

Beziehen Sie sich auf einige der folgenden Fehlermeldungen:

Manuelles Profil zu ADM Service hinzugefügt

```
==================Profiles Addition to ADM Service====================


60.26 : FAILURE : Profile 60.26 already exists

 The list of ADC profiles added to ADM Service are :

{'60.26': "['FAILURE']"}
```

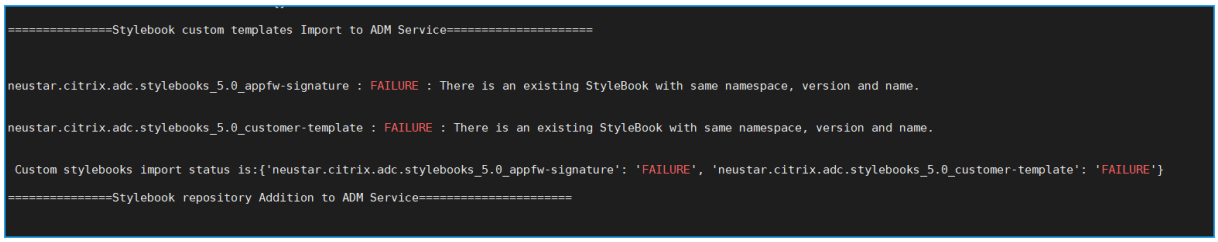
Workaround: Wenn Sie vor dem Ausführen des Migrationsskripts Administratorprofile in NetScaler ADM Service erstellt haben, müssen Sie diese Profile löschen und das Migrationsskript erneut ausführen.

NetScaler ADC-Gerät wurde zu ADM Service hinzugefügt

```
==============ADC Device Addition================

10.106.150.53 : FAILURE : Error in contacting Citrix ADC, invalid credentials.
10.102.60.26 : FAILURE :Device with this IP address already exists.


The list of ADCs added to ADM Service are:


['10.102.60.26']
```

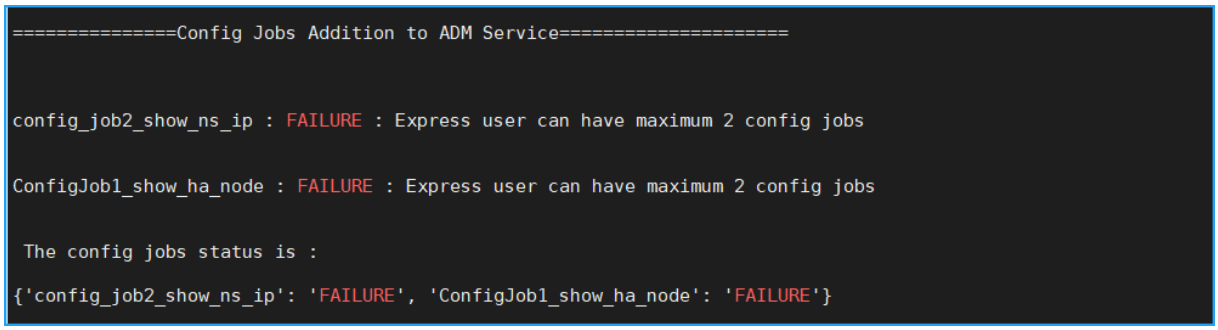

Workaround: Stellen Sie im on-premises ADM den Instanzstatus sicher und prüfen Sie, ob Sie ohne Probleme auf die Instanz zugreifen können. Wenn ein Problem weiterhin besteht, beheben Sie das Problem und führen Sie das Migrationsskript erneut aus.

Benutzerdefinierte Vorlagen von StyleBook werden in ADM Service importiert



Workaround: Diese Fehlermeldung ist ein Beispiel für das bereits migrierte StyleBook. Sie können diesen Fehler auch sehen, wenn Sie ein StyleBook mit demselben Namen, derselben Version und demselben Namespace in NetScaler ADM Service erstellt haben, bevor Sie das Migrationsskript ausführen.

Konfigurationsjobs zu ADM Service hinzugefügt



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

IP-Blöcke zu ADM Service hinzugefügt

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


ipblock1 : FAILURE : IP Block Name ipblock1 already exists

ipblock3 : FAILURE : IP Block Name ipblock3 already exists

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

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

Netzwerk-Dashboard Additionsstatus

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


new456 : FAILURE : Dashboard new456 already exists

new123 : FAILURE : Dashboard new123 already exists

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

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

Alle Wie-Macht-Man-Artikel

February 5, 2024

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

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

		Themen		
Instanzverwaltung	Ereignisverwaltung	StyleBooks	Zertifikatverwaltung	NetScaler ADI
Anwendungsverwaltung	Konfigurationsverwaltung	Authentifizierung	Analytics	Netzwerkfunk

Instanzverwaltung

So überwachen Sie global verteilte Websites

Verwalten von Adminpartitionen von NetScaler ADC-Instanzen

So fügen Sie Instanzen zu NetScaler ADM hinzu

So erstellen Sie Instanzgruppen auf NetScaler ADM

So konfigurieren Sie Sites für Geomaps in NetScaler ADM

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

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

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

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

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

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

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

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

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

So bearbeiten Sie die HAProxy-Konfigurationsdatei mit NetScaler ADM

So entdecken Sie mehrere NetScaler ADC VPX-Instanzen wieder

Abfragen von NetScaler ADC-Instanzen und Entitäten in NetScaler ADM

So heben Sie die Verwaltung einer Instanz auf NetScaler ADM auf

So verfolgen Sie die Route zu einer Instanz von NetScaler ADM

Konfigurationsverwaltung

So erstellen Sie einen Konfigurationsauftrag auf NetScaler ADM

Zertifikatverwaltung

So verwenden Sie das SSL-Dashboard auf NetScaler ADM

Abfragen von SSL-Zertifikaten von NetScaler ADC Instanzen

Anwendungsverwaltung

Erstellen einer Anwendungsdefinition in Citrix ADM

StyleBooks

So zeigen Sie verschiedene Gruppen von StyleBooks an

So erstellen Sie Ihre eigenen StyleBooks

So verwenden Sie benutzerdefinierte StyleBooks in NetScaler ADM

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

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

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

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

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

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

So verwenden Sie Microsoft Skype for Business StyleBook in Unternehmen

So verwenden Sie Microsoft Exchange StyleBook in Geschäftsunternehmen

So verwenden Sie Microsoft SharePoint StyleBook in Geschäftsunternehmen

Analytics

So aktivieren Sie Analysen für Instances

So konfigurieren Sie adaptive Schwellenwerte

So konfigurieren Sie das SLA-Management

So konfigurieren Sie die Datenbankzusammenfassung für Analysen

So erstellen Sie Schwellenwerte und Warnungen mit NetScaler ADM

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

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

So zeigen Sie die Spitzendatenrate für einen bestimmten Zeitrahmen an

So sehen Sie die Netzwerkeffizienz

Ereignisverwaltung

So legen Sie das Ereignisalter für Ereignisse in NetScaler ADM fest

So planen Sie einen Ereignisfilter mithilfe von NetScaler ADM

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

So unterdrücken Sie Ereignisse mithilfe von NetScaler ADM

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

So erstellen Sie Ereignisregeln auf NetScaler ADM

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

So zeigen Sie die Zusammenfassung der Ereignisse in NetScaler ADM an

So zeigen Sie Schweregrade und Verzerrungen von SNMP-Traps in NetScaler ADM an

So exportieren Sie Syslog-Nachrichten mit NetScaler ADM

So unterdrücken Sie Syslog-Meldungen in NetScaler ADM

So konfigurieren Sie die Prune-Einstellungen für Instanzereignisse

Authentifizierung

So aktivieren Sie externe Fallback- und Kaskadierungsserver

Hinzufügen von RADIUS-Authentifizierungsservern

Hinzufügen von LDAP-Authentifizierungsservern

Hinzufügen von TACACS-Authentifizierungsservern

So extrahieren Sie die Authentifizierungsservergruppe in NetScaler ADM

Aktivieren der lokalen Fallback-Authentifizierung

NetScaler ADM-System

So aktualisieren Sie NetScaler ADM

Kennwort für NetScaler ADM zurücksetzen

So generieren Sie eine Datei für den technischen Support für NetScaler ADM

So sichern und wiederherstellen Sie Ihren NetScaler ADM Server in einer Einzelserverbereitstellung

So sichern und stellen Sie eine NetScaler ADM-Konfiguration in einem HA-Paar wieder her

So aktivieren Sie den Shell-Zugriff für Nicht-Standardbenutzer in NetScaler ADM

So konfigurieren Sie den NTP-Server auf NetScaler ADM

So konfigurieren Sie SSL-Einstellungen für NetScaler ADM

So konfigurieren Sie das Syslog-Löschintervall für NetScaler ADM

So sehen Sie sich die Auditinformationen von NetScaler ADM an

So konfigurieren Sie die Systembenachrichtigungseinstellungen von NetScaler ADM

So überwachen Sie die CPU-, Speicher- und Festplattenauslastung von NetScaler ADM

So konfigurieren Sie eine Verschlüsselungsgruppe für NetScaler ADM

So erstellen Sie SNMP-Traps, Manager und Benutzer auf NetScaler ADM

So weisen Sie einem NetScaler ADM Server einen Hostnamen zu

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

So konfigurieren Sie die Systemsicherungseinstellungen mithilfe von NetScaler ADM

Konfigurieren und Anzeigen von Systemalarmen in NetScaler ADM

Netzwerkfunktionen

So generieren Sie Berichte für Load-Balancing-Entitäten

So exportieren oder planen Sie den Export von Netzwerkfunktionsberichten

Übersicht

February 5, 2024

NetScaler Application Delivery Management (ADM) ist eine zentralisierte Verwaltungslösung, die den Betrieb vereinfacht, indem sie Administratoren unternehmensweite Transparenz bietet und Verwaltungsaufträge automatisiert, die über mehrere Instanzen ausgeführt werden müssen. Sie können Citrix Anwendungsnetzwerkprodukte verwalten und überwachen, die NetScaler ADC MPX, NetScaler ADC VPX, NetScaler ADC SDX, NetScaler ADC CPX, NetScaler Gateway und Citrix SD-WAN umfassen. Sie können ADM verwenden, um die gesamte globale Infrastruktur für die Anwendungsbereitstellung von einer einzigen, einheitlichen Konsole aus zu verwalten, zu überwachen und Fehler zu beheben.

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

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

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

Features und Lösungen

February 5, 2024

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

Anwendungsanalyse und -verwaltung

Analyse der Anwendungsleistung

App Score ist das Produkt eines Bewertungssystems, das definiert, wie gut eine Anwendung funktioniert. Es zeigt, ob die Anwendung in Bezug auf die Reaktionsfähigkeit eine gute Leistung erbringt, nicht anfällig für Bedrohungen ist und alle Systeme in Betrieb hat.

Analysen zur Anwendungssicherheit

Das App Security Dashboard bietet einen ganzheitlichen Überblick über den Sicherheitsstatus Ihrer Anwendungen. Beispielsweise werden wichtige Sicherheitsmetriken wie Sicherheitsverletzungen, Signaturverletzungen, Bedrohungsindizes angezeigt. Das App Security-Dashboard zeigt auch angriffsbezogene Informationen wie SYN-Angriffe, Angriffe auf kleine Fenster und DNS-Hochwasserangriffe für die entdeckten ADC-Instanzen an.

Netzwerke

Instances

Ermöglicht die Verwaltung der Citrix ADC -, Citrix Gateway -, Citrix SD-WAN - und HAProxy-Instanzen.

Instanzgruppen

Ermöglicht es Ihnen, Ihre Instances wie folgt zu gruppieren:

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

Ereignisverwaltung

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

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

Zertifikatverwaltung

Citrix ADM optimiert jetzt alle Aspekte der Zertifikatverwaltung für Sie. Über eine einzige Konsole können Sie automatisierte Richtlinien einrichten, um den richtigen Aussteller, die richtige Schlüsselstärke und korrekte Algorithmen sicherzustellen, während Sie nicht verwendete oder bald ablaufende Zertifikate im Auge behalten. Um das SSL-Dashboard von ADM und seine Funktionen zu verwenden, müssen Sie verstehen, was ein SSL-Zertifikat ist und wie Sie ADM verwenden können, um Ihre SSL-Zertifikate zu verfolgen.

Konfigurationsverwaltung

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

Konfigurationsaudit

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

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

Netzwerkberichterstellung

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

Analytics

Web Insight

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

HDX Insight

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

Gateway Insight

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

Security Insight

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

SSL Insight

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

TCP Insight

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

Video Insight

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

WAN Insight

WAN Insight Analytics ermöglichen es Administratoren, den beschleunigten und nicht beschleunigten WAN-Datenverkehr, der zwischen dem Rechenzentrum und den WAN-Optimierungsgeräten des Zweigs fließt, einfach zu überwachen WAN Insight bietet auch Einblick in Clients, Anwendungen und Zweigstellen im Netzwerk, um Netzwerkprobleme effektiv zu beheben.

Orchestrierung

Cloud-Orchestrierung

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

Orchestration

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

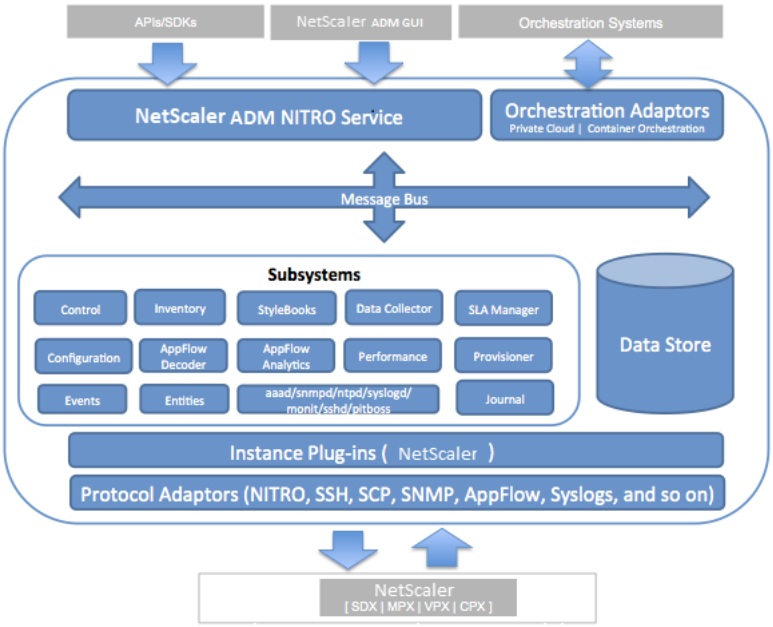
Architektur

February 5, 2024

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

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

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



Das Dienst-Subsystem in ADM fungiert als Webserver, der HTTP-Anfragen und -Antworten verarbeitet, die über die Ports 80 und 443 von der GUI oder der API aus an Subsysteme innerhalb von ADM gesendet werden. Diese Anfragen werden über den Message Bus (Message Processing System) an die Subsysteme über den IPC (Inter-Process Communication) -Mechanismus gesendet. Eine Anforderung wird an das Teilsystem "Control"gesendet, das die Informationen entweder verarbeitet oder an das entsprechende Teilsystem sendet. Jedes der anderen Subsysteme —Inventory, StyleBooks, Data Collector, Konfiguration, AppFlow Decoder, AppFlow Analytics, Performance, Events, Entities, SLA Manager, Provisioner und Journal —hat eine bestimmte Rolle.

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

Instanzdiscovery in NetScaler ADM

February 5, 2024

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

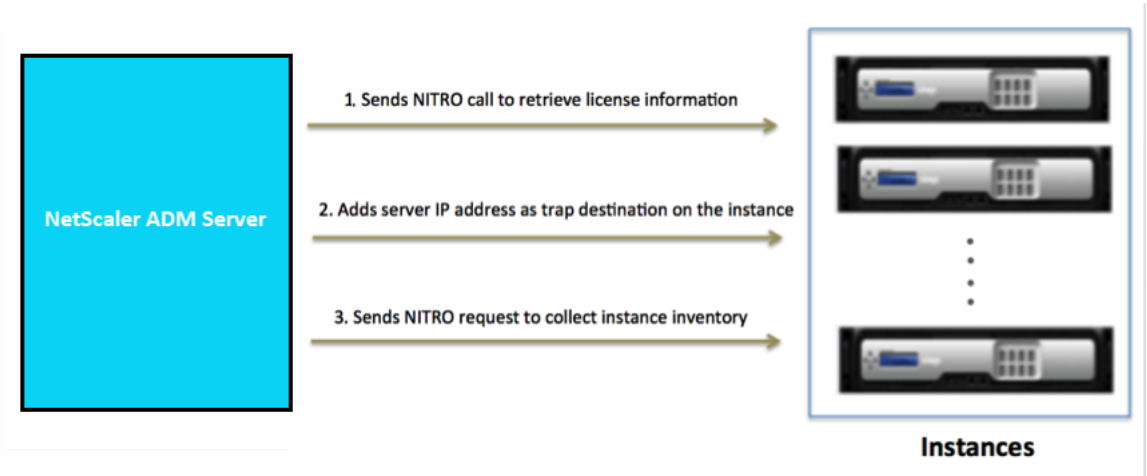
- NetScaler ADC-Instanzen
  - Citrix MPX
  - Citrix VPX
  - Citrix SDX
  - Citrix CPX
  - Citrix BLX
- NetScaler Gateway Instanzen
- Citrix SD-WAN Instanzen

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

> **Hinweis**
>
> NetScaler ADM verwendet die NetScaler ADC IP (NSIP) -Adresse der ADC-Instanzen für die Kommunikation. ADM kann auch ADC-Instanzen mit einer Subnetz-IP-Adresse (SNIP) erkennen, für die Verwaltungszugriff aktiviert ist. Informationen zu den Ports, die zwischen den ADC-Instanzen und ADM geöffnet sein müssen, finden Sie unter Ports.
>
> Wenn Sie ein ADC-HA-Paar mit SNIP hinzufügen möchten, stellen Sie sicher, dass der Independent Network Configuration (INC) -Modus für das ADC-HA-Paar aktiviert ist. Weitere Informationen zum Hinzufügen von Instanzen finden Sie unter Instanzen hinzufügen.
>
> Für Citrix SD-WAN WO verwendet ADM die Verwaltungs-IP-Adresse der Instanzen für die Kommunikation.
>
> Sie können keine Citrix SD-WAN SE/ PE-Instanzen in ADM hinzufügen. Sie können ADM als AppFlow-Collector auf den Citrix SD-WAN SE/PE-Appliances konfigurieren.

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

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



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

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

   Bei Citrix SD-WAN WO-Instanzen erkennt ADM die Instanz nicht mithilfe von Lizenzinformationen. Es sendet eine NITRO-Anforderung an die Instanz, um nach Instanztyp und -version zu überprüfen.

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

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

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

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

   Bei Citrix SD-WAN WO-Instanzen fügt ADM seine IP-Adresse als SNMP-Manager der Instanz hinzu.

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

Dieser Schritt kann aufgrund von Netzwerk- oder Firewallproblemen fehlschlagen.

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

Übersicht über die Abrufung

February 5, 2024

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

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

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

Wie NetScaler ADM verwaltete Instanzen und Entitäten abfragt

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

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

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

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

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

Abfrage-Typ	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufin
Entitätsabfrage	Alle 60 Minuten (standardmäßig)	Alle Entitäten, die auf den Instanzen konfiguriert sind. Eine Entität ist entweder eine Richtlinie, ein virtueller Server, ein Dienst oder eine Aktion, die mit einer ADC-Instanz verknüpft ist. Informationen zum Aktivieren der Entitätsabfrage finden Sie unter ADM-Funktionen aktivieren oder deaktivieren.	NITRO ruft an.	Ja, kann aber nicht auf weniger als 10 Minuten eingestellt werden. Navigieren Sie zur Konfiguration zu **Netzwerke** > **Netzwerkfunktionen**. Klicken Sie auf der Seite Netzwerkfunktion auf **Einstellungen**, um das Abrufintervall zu konfigurieren.

Abfrage-Typ	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufin
				Sie können Entitäten manuell abfragen und alle Entitäten der Instanzen sofort NetScaler ADM hinzufügen. Navigieren Sie dazu zu **Netzwerke** > **Netzwerkfunktionen** und klicken Sie auf **Jetzt abfragen**. Auf der Seite **Jetzt** abfragen können Sie alle oder ausgewählte Instanzen im Netzwerk abfragen

Hinweis

Zusätzlich zum Polling werden von verwalteten ADC-Instanzen generierte Ereignisse von NetScaler ADM über SNMP-Traps empfangen, die an die Instanzen gesendet werden. Beispielsweise wird ein Ereignis generiert, wenn ein Systemfehler oder eine Änderung der Konfiguration vorliegt.

Während des Instanzbackups werden SSL-Dateien, CA-Zertifikatdateien, ADC-Vorlagen, Datenbankinformationen usw. in NetScaler ADM heruntergeladen. Während einer Konfigurationsüberprüfung werden ns.conf-Dateien heruntergeladen und im Dateisystem gespeichert. Alle Informationen, die von verwalteten NetScaler ADC-Instanzen erfasst werden, werden intern in der Datenbank gespeichert.

Verschiedene Arten der Abfrage von Instanzen

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

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

Globale Abfrage von Instanzen

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

Manuelles Abrufen von Instanzen

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

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

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

So fragen Sie bestimmte Instanzen in NetScaler ADM ab:

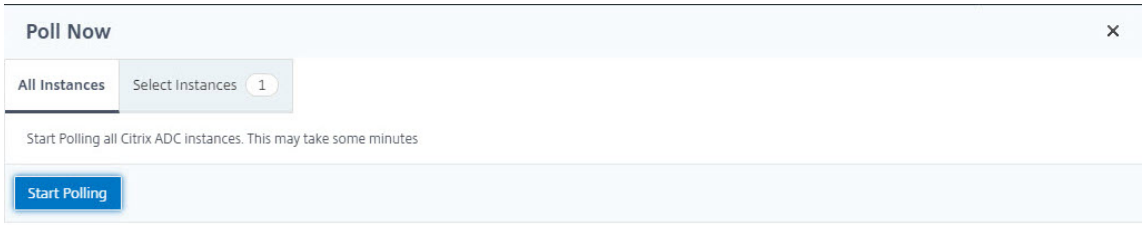
1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Netzwerkfunktionen**.
2. Klicken Sie auf der Seite **Netzwerkfunktionen** oben rechts auf **Jetzt abfragen**.

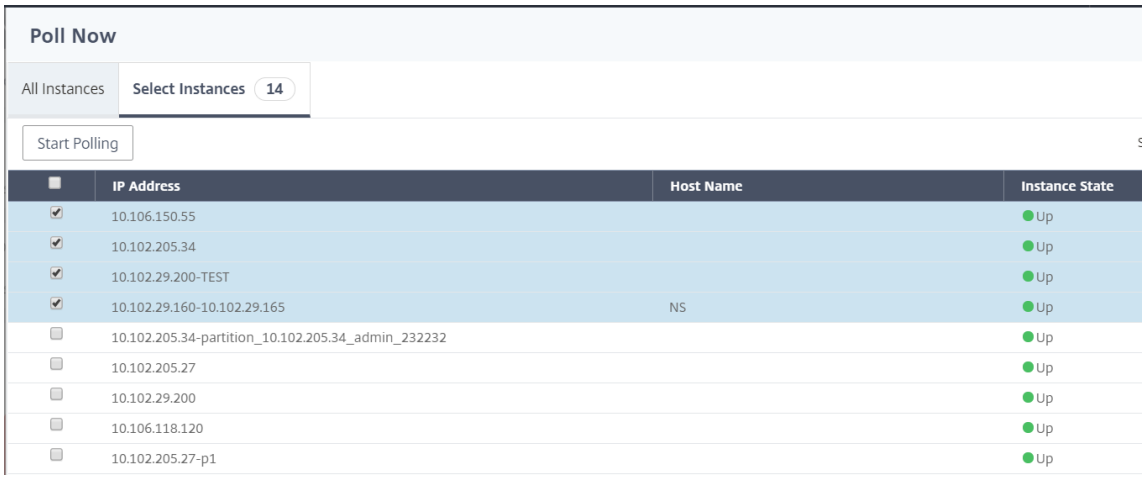
3. Auf der **Popupseite Jetzt** abfragen können Sie alle NetScaler ADC-Instanzen im Netzwerk abfragen oder die ausgewählten Instanzen abfragen.

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

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

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





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

Manuelles Abrufen von Entitäten

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

Stellen Sie sich ein Beispiel für einen virtuellen Server vor, der DOWN ist. Der Status dieses virtuellen Servers hat sich möglicherweise auf UP geändert, bevor die nächste automatische Abfrage stattfindet.

Um den geänderten Status des virtuellen Servers einzusehen, sollten Sie möglicherweise nur diesen virtuellen Server abfragen, sodass der richtige Status sofort auf der GUI angezeigt wird.

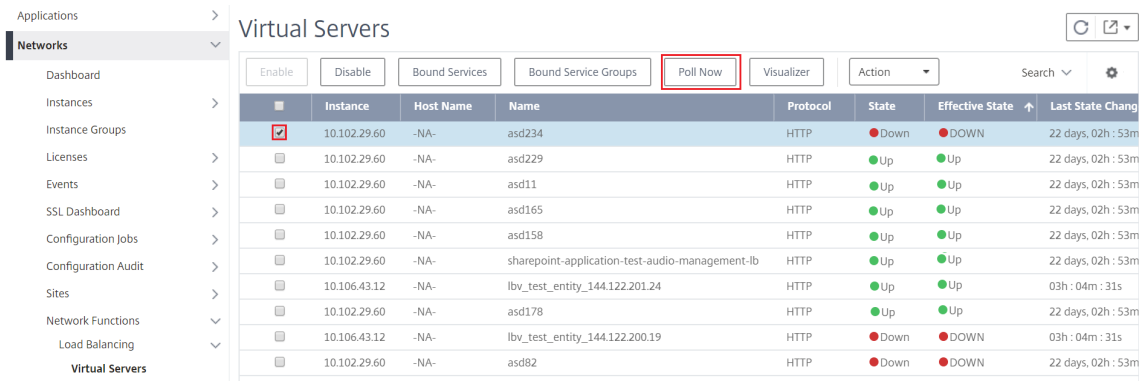
Sie können nun die folgenden Entitäten nach jedem Update in ihrem Status abfragen: Dienste, Dienstgruppen, virtuelle Server für den Lastausgleich, virtuelle Server zur Cachereduzierung, virtuelle Content Switching-Server, virtuelle Authentifizierungsserver, virtuelle VPN-Server, virtuelle GSLB-Server und Anwendungsserver.

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

So fragen Sie bestimmte Entitäten in NetScaler ADM ab:

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

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



Data Governance

February 5, 2024

Citrix sammelt Statistiken zu Ihren Citrix Application Delivery Management (ADM) -Bereitstellungen, um die Verwendung und Skalierung der Bereitstellung zu verstehen. Die Statistik umfasst den Zus-

tand, den Status und das Nutzungsmuster der ADM-Bereitstellung in Ihren Räumlichkeiten. Die Statistiken helfen Citrix dabei, Probleme in Ihrer ADM-Bereitstellung proaktiv zu beheben.

- **Erstellen Sie eine Kundenidentität in Citrix Cloud** —Um wichtige Statistiken über den Zustand, den Status und andere Kennzahlen von der on-premises ADM-Bereitstellung an das Citrix Cloud-Konto zu senden.

  Nachdem Sie eine Kundenidentität erstellt haben, stellt die "Cloud Connect"die Verbindung zwischen ADM on-prem und ADM Service her, indem Sie ein Citrix Cloud-Konto erstellen. Siehe Konfigurieren der Kundenidentität.

- **Wartungsskripte konfigurieren** - Um die Datenbank zu optimieren. Die Datenbankoptimierung kann Tabellen erstellen, Spalten ändern und mehr. Die gleiche "Cloud Connect" -Funktion wird verwendet, um Wartungsskripte zu konfigurieren. Siehe Datenbankoptimierung mit Wartungsskripten.

- **Customer User Experience Improvement Program (CUXIP)** - Dieses Programm ist standardmäßig aktiviert. Es sammelt die Nutzungsdaten von Citrix ADM. Diese Daten ermöglichen die Optimierung des ADM-Erlebnisses durch geführte Workflows, Suchartikel, Produktbenachrichtigungen, Feedback, Umfragen usw. Siehe Programm zur Verbesserung der Benutzerfreundlichkeit für Kunden.

Konfigurieren der Kundenidentität

Citrix Application Delivery Management (ADM) erfordert, dass Sie sich auf der ADM-GUI authentifizieren, bevor Sie auf die Informationen zugreifen. Es ist erforderlich, dass Sie sich bei Citrix Cloud Services registrieren, bevor Sie sich bei ADM authentifizieren. Geben Sie die Citrix Cloud-Benutzeranmeldeinformationen auf der ADM-GUI an. Weitere Informationen finden Sie unter Für Citrix Cloud anmelden.

Es gibt verschiedene Möglichkeiten, sich bei Citrix ADM zu authentifizieren. In den folgenden Abschnitten werden die Workflows beschrieben, wenn Sie ein neuer Benutzer oder ein vorhandener Benutzer in ADM sind.

Arbeitsablauf 1 —Wenn Sie ein neuer Benutzer sind

1. Schließen Sie die Installation von Citrix ADM auf dem ausgewählten Hypervisor ab.
2. Konfigurieren Sie die verschiedenen erforderlichen IP-Adressen.
3. Geben Sie in einem Webbrowser die IP-Adresse des Citrix ADM ein.
4. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.

Die Seite **Customer Identity konfigurieren** wird geöffnet, auf der Sie sich mit Ihren Citrix Cloud-Anmeldeinformationen identifizieren müssen.

Wenn Sie kein Konto in Citrix Cloud erstellt haben, klicken Sie zur Registrierung auf Citrix Cloud .

5. Klicken Sie auf **Authentifizieren**, und geben Sie Ihre E-Mail-Adresse an, mit der Sie sich bei Citrix Cloud registriert haben.
6. Markieren Sie das Kontrollkästchen neben **Ich stimme der Weitergabe von Daten für Telemetrie zu** und klicken Sie auf **Senden**.

Workflow 2 —wenn Sie ein vorhandener Benutzer sind, der auf die neueste ADM-Version aktualisiert

1. Geben Sie nach dem Upgrade von Citrix ADM auf die neueste Version in einem Webbrowser die IP-Adresse des Citrix ADM ein.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Die Seite **Customer Identity konfigurieren** wird geöffnet, auf der Sie sich mit Ihren Citrix Cloud-Anmeldeinformationen identifizieren müssen.

   Wenn Sie kein Konto in Citrix Cloud erstellt haben, klicken Sie zur Registrierung auf Citrix Cloud .
4. Klicken Sie auf **Authentifizieren**, und geben Sie Ihre E-Mail-Adresse an, mit der Sie sich bei Citrix Cloud registriert haben.
5. Aktivieren Sie das Kontrollkästchen neben “Ich stimme zu, Daten für Telemetrie freizugeben” und klicken Sie auf Absenden.

Als vorhandener Benutzer können Sie Ihre Identität auch später auf eine der folgenden zwei Arten in ADM konfigurieren:

- Navigieren Sie zu **System > Systemadministration**und klicken Sie auf **Authentifizierung**.
- Klicken Sie auf das Cloud-Symbol oben rechts in der ADM-GUI.
  Nach erfolgreicher Authentifizierung wird das X zu einem grünen Häkchen.

> **Hinweis:
>
> Stellen Sie**sicher, dass die folgenden Domänen auf die Positivliste gesetzt sind:
>
> - `*.citrixnetworkapi.net`
> - `*.blob.core.windows.net`

Durch das Hochladen Ihrer Daten in Citrix ADM und die Verwendung der Citrix ADM-Funktionen erklären Sie sich damit einverstanden, dass Citrix technische, Benutzer- oder verwandte Informationen zu Ihren Citrix Produkten und Diensten sammelt, speichert, übertragen, pflegen, verarbeiten und verwenden darf.

Von Citrix erhaltene Informationen werden immer in Übereinstimmung mit der Datenschutzrichtlinie von Citrix.combehandelt.

Diagnose und Datenerfassung

Citrix ADM sammelt die folgenden Telemetriedaten mithilfe der Kundenidentität:

- **In ADM ausgeführte Aktionen**:
  - Aktionen, die mit der Citrix ADM UI/API-Schnittstelle ausgeführt werden.
  - Aktionen, die mit der Citrix ADM SDK-Schnittstelle ausgeführt werden.
  - Anzahl der Operationen an einem einzigen Tag. Diese Anzahl beinhaltet alle Nicht-GET-Anfragen von API oder UI.
  - Anzahl der von ADM durchgeführten ADC-Upgrades.
- **Citrix ADM Lizenzinformationen**: Anzahl der berechtigten virtuellen Server.
- **Wichtige Statistiken**:
  - Gesamtzahl der Eventregeln.
  - Gesamtanzahl und benutzerdefinierte StyleBooks.
  - Anzahl der verwalteten und benutzerdefinierten Anwendungen.
  - Anzahl der registrierten Agents.
  - Gesamtdurchsatz im Citrix ADC (Rx+Tx).
  - Anzahl der verwalteten Instanzen. Diese Anzahl umfasst auch Admin-Partitionen.
  - Anzahl der Administratoren, die Citrix ADM SaaS verwenden.
- **Geolokalisierung von Citrix ADM**
- **Bereitstellungsinformationen**: Zu diesen Informationen gehören Bereitstellungstypen wie Hochverfügbarkeit, Notfallwiederherstellung und ADM-Agents.

Warum werden Daten gesammelt?

Die gesammelten Telemetriedaten helfen dabei:

- Empfehlen Sie die korrekte Dimensionierung und Bereitstellung von Citrix ADM.
- Beheben Sie proaktiv Probleme bei lokalen ADM-Bereitstellungen.

Wer kann diese Daten verwenden?

Citrix ist der alleinige Eigentümer der gesammelten Informationen. Citrix hat Zugriff auf Informationen, die Sie uns freiwillig zur Verfügung stellen, bzw. sammelt sie. Wir verkaufen oder vermieten diese Informationen an niemanden. Wir geben Ihre Daten nicht an Dritte außerhalb unserer Organisation weiter, es sei denn, dies ist zur Erfüllung Ihrer Anfrage erforderlich. Beispiel: Um eine Bestellung zu versenden oder um Probleme proaktiv zu lösen.

Wie lange speichern wir Ihre Daten?

In der Regel speichern wir Personen-/Nutzungsdaten, bis der Benutzer unsere Dienste nutzt. Oder wir haben einen anderen Zweck, dies zu tun. Danach werden die Daten nicht mehr gespeichert, als es gesetzlich vorgeschrieben oder zulässig ist oder für interne Berichts- und Abgleichszwecke erforderlich ist.

Alle Telemetriedaten werden für einen Zeitraum von nicht mehr als 13 Monaten oder 396 Tagen gespeichert.

Datenbankoptimierung mithilfe von Wartungsskripten

Wartungsskripts werden verwendet, um Datenbankprobleme in lokalen ADM-Bereitstellungen zu lösen. Die ADM-Software lädt die Datenbankwartungsskripte automatisch vom ADM-Service herunter und ermöglicht so eine schnellere Lösung für datenbankbezogene Probleme. Zuvor wurden diese Probleme durch manuelles Ausführen der Skripte behoben.

Mit dieser Funktion lädt ADM-Bereitstellung regelmäßig die Datenbankwartungsskripte von ADM Service herunter. Stellen Sie dazu sicher, dass Sie die Kundenidentität konfigurieren.

Wartungsskripte werden täglich und wöchentlich ausgeführt. Außerdem können die Skripts Tabellen erstellen oder Spalten hinzufügen oder entfernen, um die Datenbankleistung zu verbessern.

Programm zur Verbesserung der Benutzerfreundlichkeit

Unser Ziel bei Citrix Systems ist es, unseren Benutzern ein ansprechendes Produkterlebnis zu bieten. **Das Programm zur Verbesserung der Benutzerfreundlichkeit (CUXIP)** verwendet Pendo, um Benutzer durch einige häufig auftretende, aber detaillierte Aufgaben zu führen, indem es Suchartikel, In-App-Anleitungen usw. bereitstellt. Wir helfen unseren Benutzern auch, über alle aktuellen Ankündigungen auf dem Laufenden zu bleiben.

Welche Nutzungsdaten werden über CUXIP gesammelt?

Bei Nutzungsdaten dreht sich alles um Benutzeraktionen. Nutzungsdaten, auch als Daten auf Ereignisebene bezeichnet, umfassen alles von den Seiten, die unsere Benutzer auf einer Website besuchen, bis hin zur Anzahl der Klicks auf eine bestimmte Funktion. Nutzungsdaten sind wertvolle Informationen darüber, wie sich Benutzer in unseren Anwendungen bewegen. Diese Daten ermöglichen die Optimierung unserer Benutzererfahrung.

Im Folgenden sind einige der von uns gesammelten Nutzungsdaten aufgeführt:

- Details zu Seitenaufrufen, auf jeder Seite verbrachte Zeit.
- Die Besucher-ID ist eine eindeutige anonymisierte Kennung, mit der die Anzahl der eindeutigen Besucher auf einer Seite identifiziert werden kann.
- Umfragestatistiken —Ergebnis, Aufrufe, Anzahl der Einsendungen usw.

Wie hilft Ihnen CUXIP?

Wir verwenden Nutzungsdaten, um Ihre Erfahrung mit ADM zu verbessern. Im Folgenden sind einige der Möglichkeiten aufgeführt, mit denen wir die Benutzererfahrung unserer Kunden verbessern wollen:

- In-App-geführte Workflows und Möglichkeit, nach relevanten Artikeln zu suchen.
- Nehmen Sie von der App aus an einer Umfrage teil, um das Produkt zu verbessern.
- Bleiben Sie über aktuelle Ankündigungen und andere Benachrichtigungen auf dem Laufenden.
- Stellen Sie dem Produktteam eine Frage oder ein Feedback.

Wie funktioniert CUXIP?

Die Citrix ADM Appliance kann sich im internen Netzwerk befinden. Der Browser muss über eine Internetverbindung verfügen, um die Vorteile der geführten Unterstützung auf CUXIP nutzen zu können.

Wie kann ich CUXIP auf meinem ADM deaktivieren?

Um CUXIP zu deaktivieren, gehen Sie in der ADM-GUI wie folgt vor:

1. Navigieren Sie zu **System > Systemadministration**.
2. Deaktivieren Sie in **CUXIP-Einstellungen**CUXIP.

Änderungen unserer Datenschutzrichtlinie

Wir können unsere Datenschutzrichtlinie von Zeit zu Zeit aktualisieren. Wir werden Sie über die Änderungen informieren, indem wir die neue Datenschutzrichtlinie auf dieser Seite veröffentlichen. Wir werden Sie vor Inkrafttreten der Änderung per E-Mail und/oder durch einen gut sichtbaren Hinweis auf unserem Service informieren und das „Datum des Inkrafttretens“oben in dieser Datenschutzrichtlinie aktualisieren.

Es wird empfohlen, diese Datenschutzrichtlinie regelmäßig auf Änderungen zu überprüfen. Änderungen an dieser Datenschutzrichtlinie treten in Kraft, wenn sie auf der Citrix Datenschutzrichtlinienseite veröffentlicht werden.

Referenzen

Citrix Datenschutzrichtlinie: https://www.citrix.com/about/legal/privacy/

Lizenzierung

February 5, 2024

Citrix Application Delivery Management (ADM) erfordert eine verifizierte Citrix ADC Lizenz, um die Citrix ADC-Instanzen zu verwalten und zu überwachen, wenn die Instanzen über das `https`Protokoll erkannt werden.

Sie können beliebig viele Instanzen und Entitäten ohne Lizenz verwalten und überwachen. Sie können jedoch nur 30 erkannte Anwendungen im App-Dashboard verwalten und Analysedaten für 30 virtuelle Server einsehen, ohne eine Lizenz zu beantragen. Bei mehr als 30 erkannten Anwendungen oder 30 virtuellen Servern müssen Sie eine Lizenz erwerben und beantragen.

	Citrix ADM-Feature	[**KOSTENLOS**] Die Citrix ADM-Lizenz ist unabhängig von der Anzahl der virtuellen Server nicht erforderlich	Citrix ADM -Lizenz ist für > 30 virtuelle Server erforderlich	Citrix ADC Lizenzanforderung
Analytics	Web Insight	Nein	Ja	Nicht zutreffend

	Citrix ADM-Feature	[**KOSTENLOS**] Die Citrix ADM-Lizenz ist unabhängig von der Anzahl der virtuellen Server nicht erforderlich	Citrix ADM -Lizenz ist für > 30 virtuelle Server erforderlich	Citrix ADC Lizenzanforderung
	HDX Insight*	Nein	Ja	Advanced (Reporting < 1 Stunde) Premium (Reporting = Unbegrenzt)
	Security Insight	Nein	Ja	Premium (oder) Advanced mit App Firewall-Lizenz
	SSL Insight	Nein	Ja	Nicht zutreffend
	Gateway Insight	Nein	Ja	Advanced (Reporting < 1 Stunde) Premium (Reporting = Unbegrenzt)
	TCP Insight	Nein	Ja	Nicht zutreffend
	Video Insight	Nein	Ja	Premium (Citrix-T 1000-Serie, VPX-T)
	WAN-Einblick	Nein	Nicht zutreffend	Verwenden Sie die Citrix SD-WAN Instance Optimization Edition (WANOP)
Anwendungen				

	Citrix ADM-Feature	[**KOSTENLOS**] Die Citrix ADM-Lizenz ist unabhängig von der Anzahl der virtuellen Server nicht erforderlich	Citrix ADM -Lizenz ist für > 30 virtuelle Server erforderlich	Citrix ADC Lizenzanforderung
	Anwendungsstatistiken (App-Dashboard, App-Sicherheitsdashboard)	Nein	Ja	Für die Citrix ADC Web App Firewall in Bezug auf App-Dashboard und App-Sicherheits-Dashboard ist die Premium- (oder) Advanced with App Firewall-Lizenz erforderlich.
	StyleBooks	Ja	Nein	Nicht zutreffend
Netzwerke				
	Lizenzserver	Ja	Nein	Nicht zutreffend
	Inventarverwaltung—, Infrastruktur-Dashboard, Instanzgruppen, Instanz-Dashboard und Websites	Ja	Nein	Nicht zutreffend
	Eventmanagement & Syslog	Ja	Nein	Nicht zutreffend
	Konfigurationsaufträge, Konfigurationsaudit und Konfigurationsberatung	Ja	Nein	Nicht zutreffend

	Citrix ADM-Feature	[**KOSTENLOS**] Die Citrix ADM-Lizenz ist unabhängig von der Anzahl der virtuellen Server nicht erforderlich	Citrix ADM -Lizenz ist für > 30 virtuelle Server erforderlich	Citrix ADC Lizenzanforderung
	Network Reporting (Instanzebene)	Ja	Nein	Nicht zutreffend
	Netzwerkberichterstattung (virtuelle Serverebene)	Ja	Nein	Nicht zutreffend
	Netzwerkfunktionen (Sichtbarkeit und Verwaltung von virtuellen Servern, Diensten, Servicegruppen, Servern)	Ja	Nein	Nicht zutreffend
	Verwaltung, Überwachung und Dashboard von SSL-Zertifikaten (Instanzebene)	Ja	Nein	Nicht zutreffend
	SSL-Zertifikat-Dashboard (virtuelle Serverebene)	Ja	Nein	Nicht zutreffend
System				
	RBAC & externe Authentifizierung (Instanzebene)	Ja	Nein	Nicht zutreffend
	RBAC & externe Authentifizierung	Ja	Nein	Nicht zutreffend
Orchestrierung				

	Citrix ADM-Feature	[**KOSTENLOS**] Die Citrix ADM-Lizenz ist unabhängig von der Anzahl der virtuellen Server nicht erforderlich	Citrix ADM -Lizenz ist für > 30 virtuelle Server erforderlich	Citrix ADC Lizenzanforderung
	OpenStack-Integration	Ja	Nein	Nicht zutreffend
	Integration von VMware NSX	Ja	Nein	Nicht zutreffend
	Cisco APIC-Integration	Ja	Nein	Nicht zutreffend
	Integration von Containern	Ja	Nein	Nicht zutreffend
Load Balancer von Drittanbietern				
	HAProxy: Sichtbarkeit über Host/ Instanz/ Backend/ Server/ Frontend, Konfiguration herunterladen oder hochladen und Appliance neu starten.	Ja	Nein	Nicht zutreffend
	App-Dashboard	Nein	Ja (erfordert eine separate Lizenz)	Nicht zutreffend

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

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

Hohe Verfügbarkeit

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

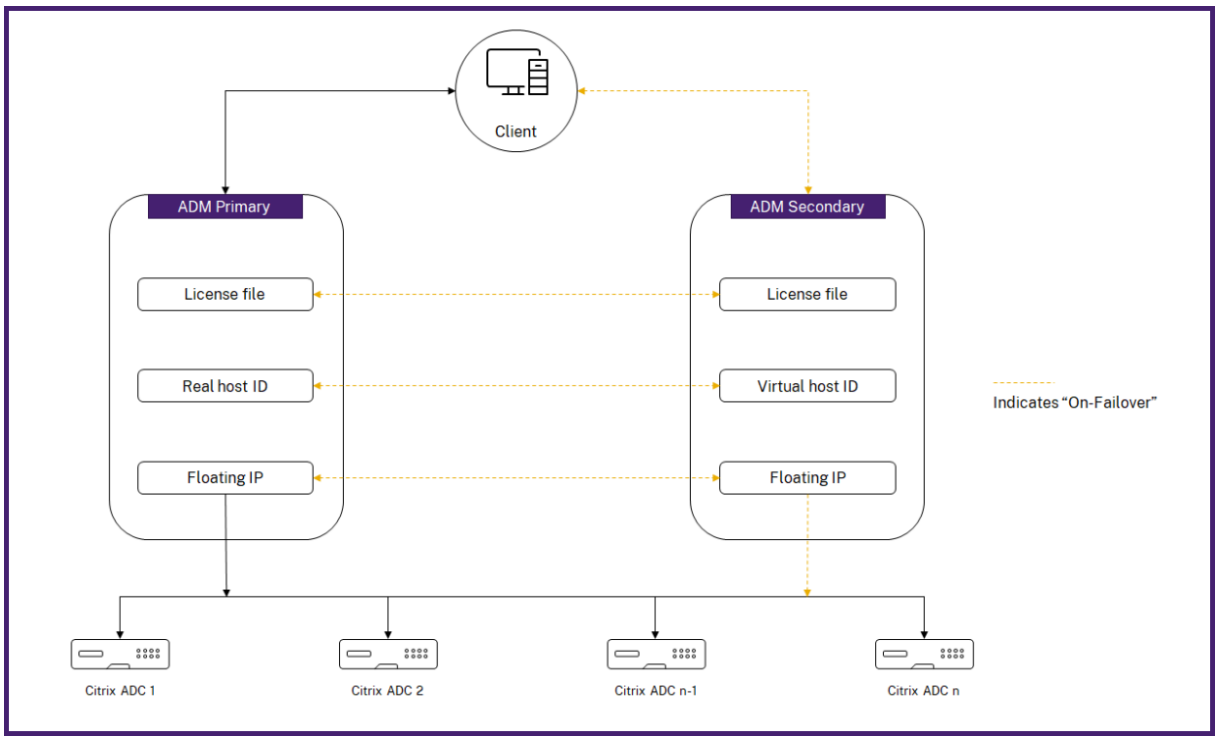
Wenn Sie ein ADM-Hochverfügbarkeitspaar als Lizenzserver konfigurieren, müssen die primären und sekundären Server dieselben Lizenzdateien haben. Daher unterstützt Citrix ADM in der Bereitstellung mit hoher Verfügbarkeit von ADM, dass Sie beiden Servern dieselben Lizenzdateien zuweisen.

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

Wie werden Lizenzen zwischen ADM-Hochverfügbarkeitsknoten synchronisiert?

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

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



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

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

Die Lizenzen sind an ADC-Instanzen gebunden. Um Lizenzen von einem Citrix ADM HA auszuchecken, benötigen Instanzen die IP-Adresse der jeweiligen Appliance. Wenn Sie Lizenzen auf einen primären Server anwenden, ist dies für die Lizenzierung zuständig und es werden alle zukünftigen Lizenzen auf diese Instanz angewendet. Sie können Lizenzen nur von dem Server löschen, auf dem Sie die Lizenzen installiert haben.

Orchestrierung

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

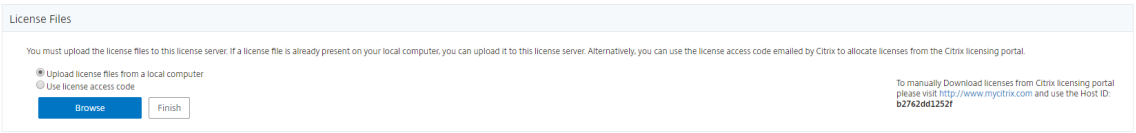
Aktualisieren Sie die virtuellen Serverlizenzen

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

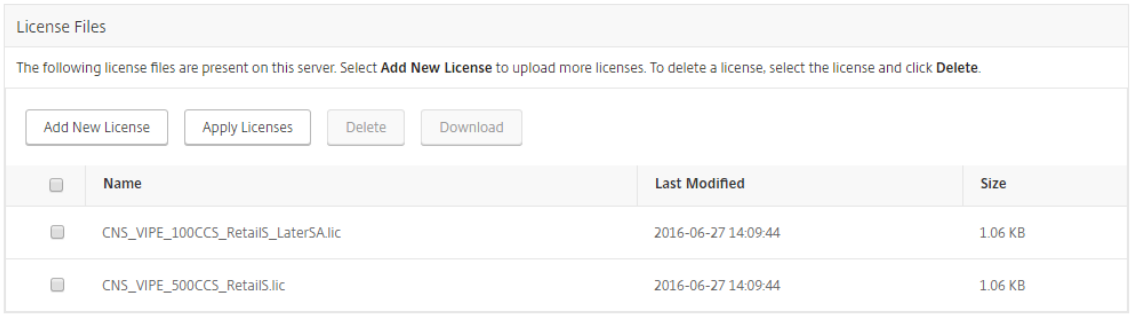
So aktualisieren Sie Ihre Appliance-Lizenzen:

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

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

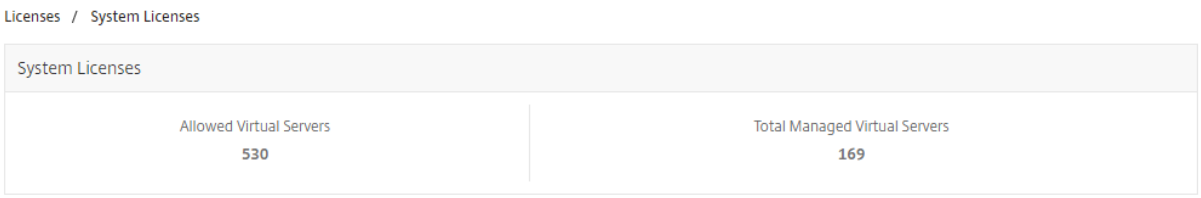


4. Auf der Seite Lizenzeinstellungen können Sie jederzeit weitere Lizenzen hinzufügen.



Verifizierung

Sie können die auf Ihrem Citrix ADM installierten Lizenzen überprüfen, indem Sie zu**System > Licensing &**Analytics navigieren.



Virtuelle Server verwalten

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

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

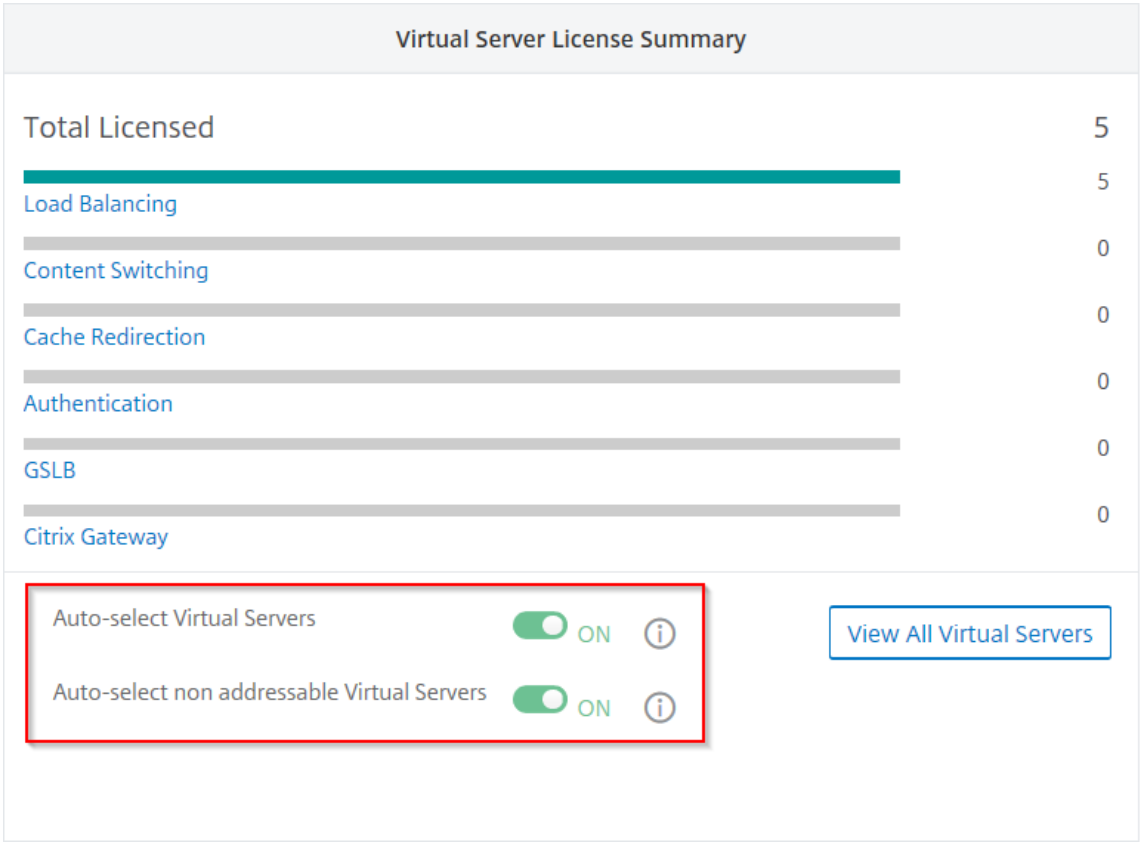
Um die virtuellen Server manuell auszuwählen oder die Lizenzierung auf eingeschränkte virtuelle Server zu beschränken, müssen Sie zuerst die automatische Lizenzierung der virtuellen Server deaktivieren und dann die virtuellen Server auswählen, die Sie verwalten möchten.

Deaktivieren der automatischen Lizenzierung virtueller Server

1. Navigieren Sie zu **System > Lizenzierung und Analyse**.

   Das Dashboard zeigt die verfügbaren virtuellen Serverlizenzen, die verwalteten virtuellen Server zusammen mit dem virtuellen Servertyp und Informationen zum Ablauf der Lizenz an.

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

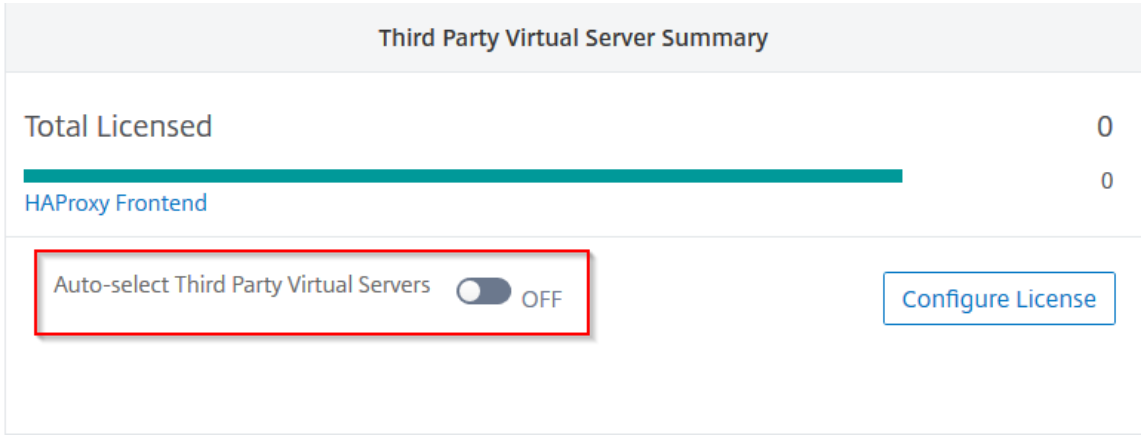


Virtuelle Server von Drittanbietern für die Lizenzierung auswählen

1. Navigieren Sie zu **System > Lizenzierung und Analyse**.

   Das Dashboard zeigt die verfügbaren virtuellen Serverlizenzen, die verwalteten virtuellen Server zusammen mit dem virtuellen Servertyp und Informationen zum Ablauf der Lizenz an.

2. Deaktivieren Sie in der **Übersicht über virtuelle Server**von **Drittanbietern die automatische Auswahl virtueller Server von Drittanbietern**.



Manuelles Anwenden virtueller Serverlizenzen

Sie können manuell Lizenzen auf einen einzelnen virtuellen Server anwenden.

1. Wählen Sie unter **Virtueller Server-Lizenzzuweisungdie Option Lizenzen konfigurieren**aus.

   Die Seite **Alle virtuellen Server** wird angezeigt.
2. Filtern Sie nicht lizenzierte virtuelle Server mithilfe der Eigenschaft: `Licensed: No`.
3. Wählen Sie den virtuellen Server aus, den Sie lizenzieren möchten.
4. Klicken Sie auf **Lizenz**.

Richtlinienbasierte Lizenzierung für virtuelle Server konfigurieren

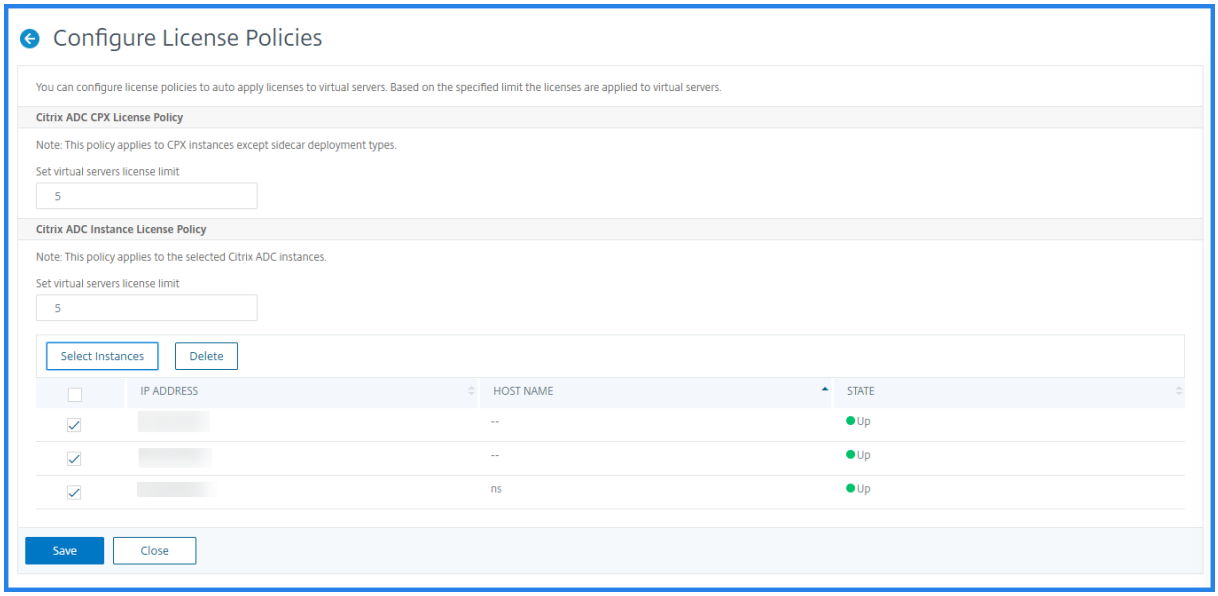
Sie können eine Richtlinie konfigurieren, um die Lizenz auf virtuelle Server anzuwenden. Diese Richtlinie steuert die Anzahl der virtuellen Server, die Sie automatisch lizenzieren möchten. Außerdem werden Lizenzen nur auf die virtuellen Server ausgewählter Instanzen angewendet.

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

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

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

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



Anzeigen der lizenzierten virtuellen Server

Nachdem die Lizenzen auf die virtuellen Server angewendet wurden, können Sie die lizenzierten virtuellen Server oder die virtuellen Server von Drittanbietern auf der Seite **Licensing & Analytics** einsehen. Gehen Sie wie folgt vor, um die lizenzierten virtuellen Server anzuzeigen:

1. Navigieren Sie zu **System > Lizenzierung und Analyse**.
2. Klicken Sie in der **Lizenzübersicht für virtuelle Server im Abschnitt**Gesamtlizenzierung**auf den virtuellen Servertyp**.

Konfigurieren der automatischen Lizenzunterstützung für nicht adressierbare virtuelle Server

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

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

Hinweis

- Citrix ADM wählt standardmäßig immer noch nicht automatisch nicht adressierbare virtuelle Server für die Lizenzierung aus.
- Anwendungsanalysen (App Dashboard) sind die einzige Analyse, die derzeit auf lizenzierten, nicht adressierbaren virtuellen Servern unterstützt wird.

Ablaufprüfungen für virtuelle Serverlizenzen

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

So zeigen Sie den Status der Lizenzen an:

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

So konfigurieren Sie die Benachrichtigungseinstellungen für Lizenzen:

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

- **Schwellenwert für den Lizenzablauf:** Anzahl der Tage, bevor die durch den Alert-Schwellenwert ermittelte Anzahl der Lizenzen abläuft.
- **Ablauf der Lizenzen:** Anzahl der verbleibenden Tage vor Ablauf.

Systemanforderungen

February 5, 2024

Bevor Sie NetScaler Application Delivery Management (ADM) installieren, müssen Sie die Softwareanforderungen, Browseranforderungen, Portinformationen, Lizenzinformationen und Einschränkungen kennen.

Anforderungen für NetScaler ADM

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

Komponente	Voraussetzung
	Wenn Ihre NetScaler ADM Speicheranforderung 120 GB überschreitet, müssen Sie einen zusätzlichen Datenträger bereitstellen. Sie können nur einen zusätzlichen Datenträger hinzufügen. Citrix empfiehlt, zum Zeitpunkt der Erstbereitstellung den Speicher zu schätzen und zusätzlichen Datenträger anzuhängen. Weitere Informationen finden Sie unter Bereitstellen eines zusätzlichen Datenträgers in NetScaler ADM.
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s oder 100 Mbit/s

> Hinweis
>
> NetScaler ADM wird im AMD-Chipsatz nicht unterstützt.

Anforderungen für NetScaler ADM On-Prem Agent

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

> Hinweis
>
> NetScaler ADM-Agent wird im AMD-Chipsatz nicht unterstützt.

Mindestens erforderliche NetScaler ADC Version für NetScaler ADM Funktionen

> **Wichtig!**
>
> Die NetScaler ADM-Version und der Build sollten **gleich oder höher** als Ihre NetScaler ADC-Version und Ihr Build sein. Wenn Sie beispielsweise NetScaler ADM 12.1 Build 50.39 installiert haben, stellen Sie sicher, dass Sie NetScaler ADC 12.1 Build 50.28/50.31 oder früher installiert haben.

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

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

Anforderungen für die Citrix SD-WAN-Instanzverwaltung

Interoperabilitätsmatrix von Citrix SD-WAN-Plattform-Editionen/-Versionen und NetScaler ADM-Funktionen

Plattform-Edition	Citrix SD-WANOP	Citrix SD-WAN SE	Citrix SD-WAN PE
Discovery	Ja	Ja	Ja
Konfiguration	Ja	Nein	Nein
Überwachen	Ja	Nein	Nein
Berichterstellung (Netzwerkberichte)	Ja	Nein	Nein
Event-Management	Ja	Nein	Nein
HDX Insight	Ja	Nein	Nein
WAN Insight	Ja	Nein	Nein
HDX Insight (Multi-Hop-Bereitstellung)	Ja	Ja	Nein

Thin Clients werden für Citrix SD-WAN-Instanzen unterstützt

NetScaler ADM unterstützt die folgenden Thin Clients zur Überwachung von Citrix SD-WAN-Bereitstellungen:

- Dell Wyse WTOS Modell R10L Rx0L Thin Client
- NComputing N400
- Dell Wyse WTOS Modell CX0 C00X Xenith
- Dell Wyse WTOS Modell TXO T00X Xenith2
- Dell Wyse WTOS Modell CX0 C10LE
- Dell Wyse WTOS Modell R00LX Rx0L HDX Thin Client
- Dell Wyse erweitert SUSE Linux Enterprise, Modell Dx0D, D50D
- Dell Wyse ZX0 Thin Client Z90D7 (WES7)

Anforderungen für NetScaler ADM Analytics

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

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

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

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

Für HDX Insight unterstützte Thin Clients

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

NetScaler ADC-Instanzlizenz für HDX Insight erforderlich

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

NetScaler ADC-Lizenz/Dauer	5 Minuten	1 Stunde	1 Tag	1 Woche	1 Monat
Standard	Nein	Nein	Nein	Nein	Nein

Erweitert	Ja	Ja	Nein	Nein	Nein
Premium	Ja	Ja	Ja	Ja	Ja

Unterstützte Hypervisoren

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

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

Unterstützte Betriebssysteme und Empfängerversionen

In der folgenden Tabelle sind die von NetScaler ADM unterstützten Betriebssysteme und die Citrix Receiver-Versionen aufgeführt, die derzeit von jedem System unterstützt werden:

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

* Anwendbar mit Citrix CloudBridge (Citrix SD-WANOP) Version 7.4 und höher.

Unterstützte Browser

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

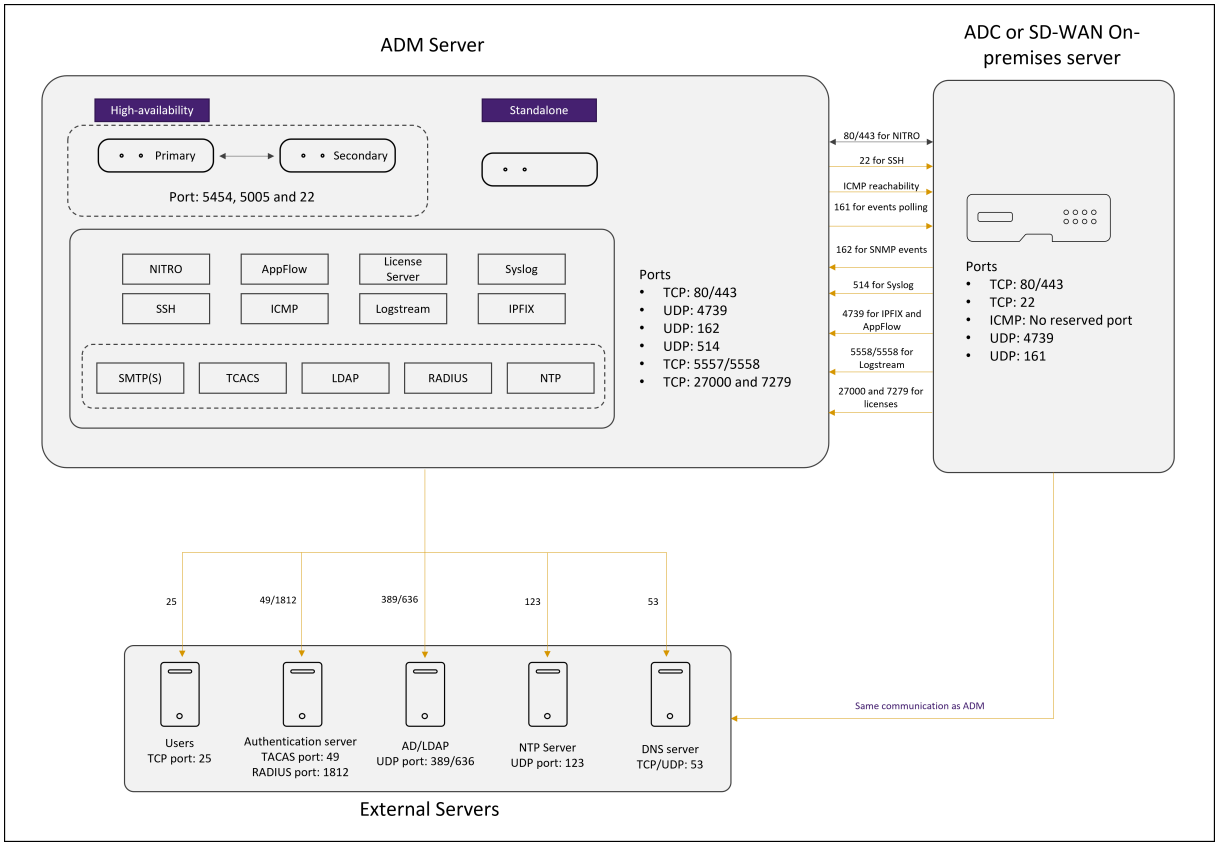
Webbrowser	Version
Microsoft Edge	79 und höher
Google Chrome	51 und höher
Safari	10 und höher
Mozilla Firefox	52 und höher

Unterstützte Ports

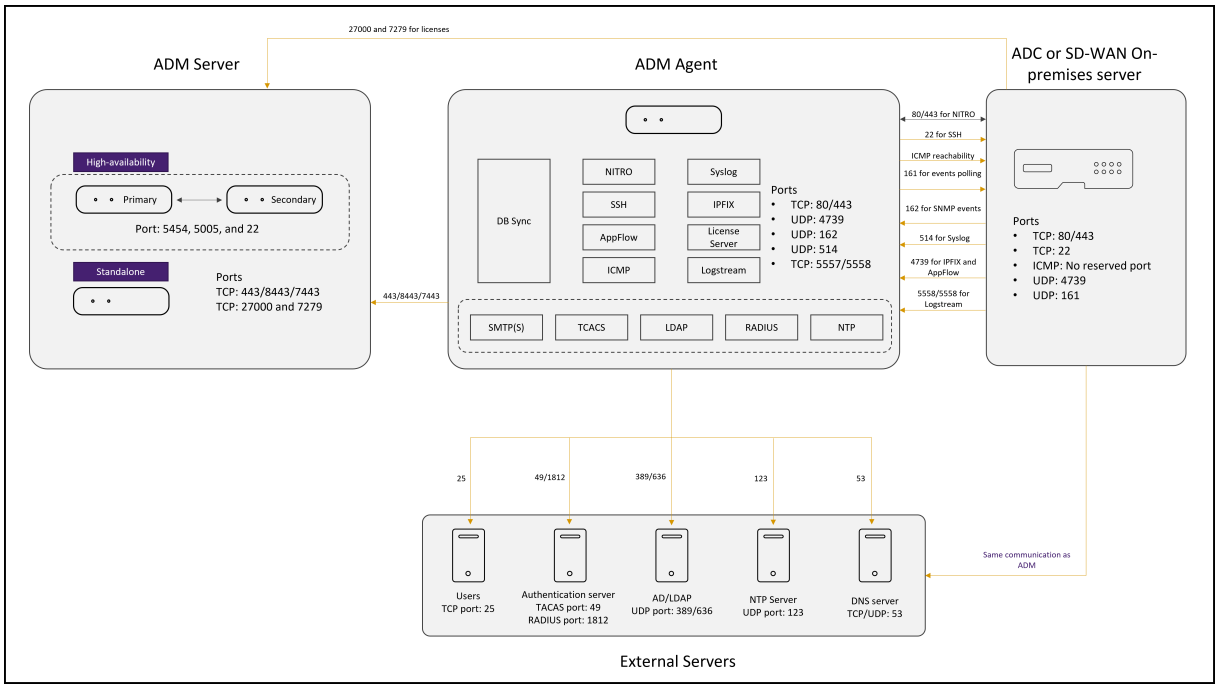
NetScaler ADM verwendet die NetScaler ADC-IP-Adresse (NSIP), um mit NetScaler ADC zu kommunizieren. Sie können ADM Agent als Vermittler zwischen der ADC-Instanz und ADM oder der SD-WAN-Instanz und ADM verwenden. Um eine Kommunikation mit diesen Servern herzustellen, öffnen Sie die erforderlichen Ports.

> **Hinweis**
>
> Wenn Sie Citrix ADCs im Modus “Hohe Verfügbarkeit”konfiguriert haben, verwendet NetScaler ADM die IP-Adresse des NetScaler ADC-Subnetzes (Management SNIP) für die Kommunikation mit NetScaler ADC. Für die Kommunikation mit SNIP mit NetScaler ADM bleiben die erforderlichen Ports unverändert.

Netzwerk-Port-Diagramm für agentlose Bereitstellung:



Netzwerkportdiagramm für die Bereitstellung mit ADM Agent:



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

- ADM-Server

- ADM-Agents
- ADC oder SD-WAN-Instanz
- Externe Server

Ports für den ADM-Server

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

Port	Typ	Details	Richtung der Kommunikation
5454 und 22	TCP	Standardport für die Kommunikation und Datenbanksynchronisierung zwischen NetScaler ADM Knoten im Hochverfügbarkeitsmodus.	Primärer NetScaler ADM-Knoten zum sekundären NetScaler ADM-Knoten
443/8443/7443	TCP	Port für die Kommunikation zwischen NetScaler ADM Agent und NetScaler ADM.	Der NetScaler ADM-Agent initiiert die Kommunikation mit NetScaler ADM. Dann interagieren Citrix ADM und Agent miteinander.

Wenn die ADM- und ADC-Instanzen keinen Agents für die Kommunikation verwenden, müssen Sie die folgenden Ports auf dem ADM-Server öffnen:

Port	Typ	Details	Richtung der Kommunikation
80/443	TCP	Für NITRO-Kommunikation von NetScaler ADM an NetScaler ADC oder Citrix SD-WAN Instanz.	NetScaler ADM Agent an NetScaler ADC und NetScaler ADC an NetScaler ADM Agent

Port	Typ	Details	Richtung der Kommunikation
4739	UDP	Für die AppFlow Kommunikation von der NetScaler ADC - oder Citrix SD-WAN Instanz zu NetScaler ADM.	NetScaler ADC oder Citrix SD-WAN an NetScaler ADM Agent
162	UDP	So empfangen Sie SNMP-Ereignisse von der NetScaler ADC-Instanz an NetScaler ADM.	NetScaler ADC an NetScaler ADM Agent
514	UDP	So empfangen Sie Syslog-Nachrichten von der NetScaler ADC - oder Citrix SD-WAN-Instanz an NetScaler ADM.	NetScaler ADC oder Citrix SD-WAN an NetScaler ADM Agent
5557/5558	TCP	Für die Logstream-Kommunikation (für Security Insight, Web Insight und HDX Insight) von NetScaler ADC zu NetScaler ADM.	NetScaler ADC zu NetScaler ADM
5005	TCP	Port zum Austausch von Heartbeats zwischen HA-Knoten.	NetScaler ADM primärer Knoten zum sekundären Knoten. Sekundärer NetScaler ADM-Knoten zum primären Knoten.

Ports für den ADM Agent

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

Port	Typ	Details	Richtung der Kommunikation
80/443	TCP	Für NITRO-Kommunikation von NetScaler ADM an NetScaler ADC oder Citrix SD-WAN Instanz.	NetScaler ADM Agent an NetScaler ADC und NetScaler ADC an NetScaler ADM Agent
4739	UDP	Für die AppFlow Kommunikation von der NetScaler ADC - oder Citrix SD-WAN Instanz zu NetScaler ADM.	NetScaler ADC oder Citrix SD-WAN an NetScaler ADM Agent
162	UDP	So empfangen Sie SNMP-Ereignisse von der NetScaler ADC-Instanz an NetScaler ADM.	NetScaler ADC an NetScaler ADM Agent
514	UDP	So empfangen Sie Syslog-Nachrichten von der NetScaler ADC - oder Citrix SD-WAN-Instanz an NetScaler ADM.	NetScaler ADC oder Citrix SD-WAN an NetScaler ADM Agent
5557/5558	TCP	Für die Logstream-Kommunikation (für Security Insight, Web Insight und HDX Insight) von NetScaler ADC zu NetScaler ADM.	NetScaler ADC zu NetScaler ADM

Ports für ADC- und SD-WAN-Instanzen

In dieser Tabelle werden die erforderlichen Ports erläutert, die auf NetScaler ADC- und SD-WAN-Instanzen geöffnet sein müssen.

Port	Typ	Details	Richtung der Kommunikation
80/443	TCP	Für die NITRO -Kommunikation von NetScaler ADM zu NetScaler ADC oder Citrix SD-WAN Instanz 443. Für die NITRO -Kommunikation zwischen NetScaler ADM-Servern im Hochverfüg- barkeitsmodus.	NetScaler ADM an NetScaler ADC und NetScaler ADC an NetScaler ADM
22	TCP	Für die SSH-Kommunikation von NetScaler ADM zur NetScaler ADC - oder Citrix SD-WAN Instanz. Für die Synchronisierung zwischen NetScaler ADM-Servern, die im Hochverfüg- barkeitsmodus bereitgestellt werden. Und dieser Port ist für die SSH-Kommunikation zwischen dem ADM-Agent und NetScaler ADC erforderlich.	NetScaler ADM an NetScaler ADC. Oder NetScaler ADM Agent an NetScaler ADC.

Port	Typ	Details	Richtung der Kommunikation
Kein reservierter Port	ICMP	Erkennen der Netzwerkerreichbarkeit zwischen NetScaler ADM- und NetScaler ADC-Instanzen, SD-WAN-Instanzen oder dem sekundären NetScaler ADM-Server, der im Hochverfügbarkeitsmodus bereitgestellt wird.	NetScaler ADM an NetScaler ADC
161	UDP	Ereignisse aus ADC-Instanzen abfragen.	NetScaler ADM an NetScaler ADC

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

Ports für externe Server

In dieser Tabelle werden die erforderlichen Ports erläutert, die auf externen Servern offen sein müssen:

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

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

Einschränkungen

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

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

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

Die folgenden Funktionen unterstützen IPv6 nicht:

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

Erste Schritte

February 5, 2024

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

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

Schritt 1 - Überprüfen der Systemanforderungen

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

- **Informationen zur Lizenz**. Sie können beliebig viele Instanzen und Entitäten ohne Lizenz verwalten und überwachen. Sie können jedoch nur 30 entdeckte Apps verwalten und Analyseinformationen für nur zwei virtuelle Server anzeigen, ohne eine Lizenz zu beantragen. Um mehr als 30 Apps zu verwalten oder Analysen für mehr als zwei virtuelle Server anzuzeigen, müssen Sie entsprechende Lizenzen erwerben. Erfahren Sie mehr.
- **Betriebssystem- und Empfängeranforderungen**. Überprüfen Sie diese Informationen, um sicherzustellen, dass Sie die richtige Empfängerversion für die unterstützten Betriebssysteme haben. Erfahren Sie mehr.
- **Anforderungen für den Browser**. Um auf NetScaler ADM GUI zugreifen zu können, müssen Sie sicherstellen, dass Sie über den erforderlichen Browser und die richtige Version verfügen. Erfahren Sie mehr.
- **Ports**.Stellen Sie sicher, dass die erforderlichen Ports für NetScaler ADM geöffnet sind, um mit NetScaler ADC- oder SD-WAN-Instanzen oder sowohl NetScaler ADC- als auch SD-WAN-Instanzen zu kommunizieren. Erfahren Sie mehr.
- **Anforderungen an die NetScaler ADC Instanz**. Verschiedene NetScaler ADM-Funktionen werden in verschiedenen NetScaler ADC-Softwareversionen unterstützt. Überprüfen Sie diese Informationen, um sicherzustellen, dass Sie die NetScaler ADC Instanzen auf die richtige Version aktualisiert haben. Erfahren Sie mehr.
- **Anforderungen an die Citrix SD-WAN Instanz**.Überprüfen Sie diese Informationen, um sicherzustellen, dass Sie die Citrix SD-WAN Instanzen auf die richtige Version aktualisiert haben und über die richtigen Plattformeditionen verfügen. Erfahren Sie mehr.

Schritt 2: Bereitstellen von NetScaler ADM

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

- **Bereitstellung auf einem Server**.In einer NetScaler ADM Einzelserverbereitstellung ist die Datenbank in den Server integriert, und ein einzelner Server verarbeitet den gesamten Daten-

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

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

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

Schritt 3: Hinzufügen von Instanzen zu NetScaler ADM

Instanzen sind Citrix-Appliances oder virtuelle Appliances oder Geräte von Drittanbietern, die Sie von NetScaler ADM aus erkennen, verwalten und überwachen möchten. Sie müssen dem NetScaler ADM -Server Instanzen hinzufügen, wenn Sie diese Instanzen verwalten und überwachen möchten. Sie können NetScaler ADM folgende Instanzen hinzufügen:

- Citrix ADC
  - NetScaler ADC MPX
  - NetScaler ADC VPX
  - NetScaler ADC SDX
  - NetScaler ADC CPX
  - Citrix Gateway
  - Citrix SD-WAN
- HAProxy

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

Weitere Infos

Schritt 4 —Analytik auf virtuellen Servern aktivieren

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

Weitere Infos

Schritt 5: Konfigurieren des NTP-Servers auf NetScaler ADM

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

Weitere Infos

Schritt 6 - Konfigurieren von Systemeinstellungen für optimale NetScaler ADM Leistung

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

- **Konfigurieren von Systemalarmen**. Konfigurieren Sie Systemalarme, um sicherzustellen, dass Sie kritische oder größere Systemprobleme kennen. Sie möchten z. B. benachrichtigt werden, wenn die CPU-Auslastung hoch ist oder wenn mehrere Anmeldefehler auf dem Server auftreten.
- **Konfigurieren Sie Systembenachrichtigungen**. Sie können Benachrichtigungen an ausgewählte Benutzergruppen für verschiedene systembezogene Funktionen senden. Sie können einen Benachrichtigungsserver in NetScaler ADM einrichten und E-Mail- und SMS-Gateway server (Short Message Service) so konfigurieren, dass E-Mail- und Textbenachrichtigungen an Benutzer gesendet werden. Dadurch wird sichergestellt, dass Sie über alle Aktivitäten auf Systemebene wie Benutzeranmeldung oder Systemneustart benachrichtigt werden.
- **Konfigurieren Sie die Einstellungen für den Systemausfall**.Um die Menge der Berichtsdaten zu begrenzen, die in der Datenbank Ihres NetScaler ADM-Servers gespeichert werden, können Sie das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle aufbewahren soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00.00 Uhr) bereinigt.

- **Konfigurieren Sie die Einstellungen für das Systembackup**. NetScaler ADM erstellt ein Backup des Systems automatisch jeden Tag um 00:30 Uhr. Standardmäßig werden drei Backupdateien gespeichert. Möglicherweise möchten Sie eine größere Anzahl von Backups des Systems beibehalten.
- **Konfigurieren Sie die Einstellungen für das Instanzbackup**.Wenn Sie den aktuellen Status einer NetScaler ADC-Instanz sichern, können Sie die Backupdateien verwenden, um die Stabilität wiederherzustellen, falls die Instanz instabil wird. Dies ist besonders wichtig, bevor Sie ein Upgrade durchführen. Standardmäßig wird alle 12 Stunden ein Backup erstellt und drei Sicherungsdateien werden im System aufbewahrt.
- **Konfigurieren Sie die Einstellungen für das Ausschneiden von Instanzereignissen**.Um die Anzahl der Ereignismeldungsdaten zu begrenzen, die in der Datenbank Ihres NetScaler ADM-Servers gespeichert werden, können Sie das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle aufbewahren soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00:00 Uhr) beschnitten.
- **Konfigurieren Sie die Syslog-Löscheinstellungen der Instanz**. Um die Menge der in der Datenbank gespeicherten Syslog-Daten zu begrenzen, können Sie das Intervall angeben, in dem Sie Syslog-Daten löschen möchten. Sie können die Anzahl der Tage angeben, nach denen die folgenden Syslog-Daten aus NetScaler ADM gelöscht werden:
  - Generische Syslog-Daten
  - AppFirewall-Daten
  - NetScaler Gateway-Daten.

    Weitere Infos

Nächste Schritte

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

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

Verwalten von Citrix ADC SD-WAN-Instanzen Nicht alle NetScaler ADM Funktionen werden auf SD-WAN-WO-Instanzen unterstützt, z. B. wird die Zertifikatverwaltung oder die Konfigurationsüberwachung nicht unterstützt. Informationen darüber, welche Funktionen unterstützt werden und wie sie verwendet werden, finden Sie unter Verwalten von Citrix SD-WAN WO mit NetScaler ADM.

Verwalten von HAProxy-Instanzen und -Anwendungen. Sie können die Frontends, Backends und Server überwachen, die in einer HAProxy-Bereitstellung konfiguriert sind. Sie können auch die Anwendungsverwaltungsfunktion verwenden, um Echtzeitstatistiken der von NetScaler ADM überwachten Frontends zu überwachen. Informationen darüber, welche Funktionen für HAProxy unterstützt werden und wie sie verwendet werden, finden Sie unter Verwalten und Überwachen von HAProxy-Instanzen mit NetScaler ADM.

Bereitstellen

February 5, 2024

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

- **Bereitstellung auf einem einzelnen Server**: Bei einem eigenständigen ADM, das auf einem Hypervisor bereitgestellt wird, ist die Datenbank in den Server integriert und ein einziger Server verarbeitet den gesamten Datenverkehr. Sie können NetScaler ADM mit Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V und Linux KVM bereitstellen. Siehe:
  - NetScaler ADM auf Citrix Hypervisor
  - NetScaler ADM unter Microsoft Hyper-V
  - NetScaler ADM auf VMware ESXi
  - NetScaler ADM auf Linux KVM-Server
  - NetScaler ADM im Kubernetes-Cluster
- **Bereitstellung mit hoher Verfügbarkeit (HA)**: Eine HA-Bereitstellung von zwei NetScaler ADM-Servern sorgt für einen unterbrechungsfreien Betrieb. In einem HA-Setup müssen beide NetScaler ADM-Knoten im aktiv-Passiven Modus im selben Subnetz mit derselben Softwareversion und demselben Build bereitgestellt werden und müssen dieselben Konfigurationen haben. Mit der HA-Bereitstellung entfällt die Möglichkeit, die schwebende IP-Adresse auf dem primären NetScaler ADM Knoten zu konfigurieren, dass kein separater NetScaler ADC Load Balancer erforderlich ist.Siehe:Konfiguration in Hochverfügbarkeitsbereitstellung.

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

- **Migrieren Sie von NetScaler Insight Center zu NetScaler ADM**: Sie können Ihre NetScaler Insight Center-Bereitstellung zu NetScaler ADM migrieren, ohne die vorhandene Konfiguration, Einstellungen oder Daten zu verlieren. Mit NetScaler ADM können Sie nicht nur die verschiedenen Analysen anzeigen, die von den NetScaler ADC - und Citrix SD-WAN Instanzen generiert werden, sondern auch die gesamte globale Anwendungsbereitstellungsinfrastruktur über eine einzige einheitliche Konsole verwalten, überwachen und beheben. Siehe:Migration von NetScaler Insight Center zu NetScaler ADM
- **Integration von NetScaler ADM mit Director**: Director integriert sich in NetScaler ADM für Netzwerkanalysen und Performance-Management. Siehe: Integrieren von NetScaler ADM mit Director

Voraussetzungen für die Installation von NetScaler ADM

February 5, 2024

Sie können Citrix Application Delivery Management (ADM) für Microsoft HyperV,
VMware ESXi, Linux KVM und Citrix Hypervisor Plattformen als virtuelle Appliance herunterladen und installieren. Bevor Sie
NetScaler ADM installieren, müssen Sie die Softwareanforderungen, Browseranforderungen, Portinformationen, Lizenzinformationen und Einschränkungen auf allen diesen Plattformen verstehen.

Spezielle Plattformanforderungen und detaillierte Schritte zur Installation von Citrix ADM finden Sie in den folgenden Themen:

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

Allgemeine Anforderungen für Citrix ADM

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8 CPUs
Speicherplatz	Citrix empfiehlt die Verwendung der SSD-Technologie (Solid State Drive) für Citrix ADM Bereitstellungen. Der Standardspeicherplatz beträgt 120 GB. Die tatsächliche Speicheranforderung hängt von der Schätzung der NetScaler ADM Größe ab. Verwenden Sie den Größenrechner, der im Abschnitt **Maximale Grenzwerte** (Seitenzahl 7) im NetScaler ADM HA Deployment Guide erwähnt wird. Dieses Handbuch ist auf unserer Download-Siteunter **NetScaler MAS Release 12.1 > Frühere Versionen verfügbar**. **Hinweis**: Sie benötigen ein Citrix Konto, um auf den Bereitstellungsleitfaden und den Größenrechner zuzugreifen Wenn Ihre NetScaler ADM-Speicheranforderungen 120 GB überschreiten, müssen Sie einen zusätzlichen Datenträger anschließen. Citrix empfiehlt, dass Sie den Speicher abschätzen und zum Zeitpunkt der ersten Bereitstellung einen zusätzlichen Datenträger anschließen. Sie können nur einen zusätzlichen Datenträger hinzufügen. Weitere Informationen finden Sie unter Bereitstellen eines zusätzlichen Datenträgers in NetScaler ADM.
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s

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

> erwartet. Daher wird die ADM-Bereitstellung auf SAN nicht unterstützt.

NetScaler ADM auf Citrix Hypervisor

February 5, 2024

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

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

Voraussetzungen

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

- Citrix Hypervisor Version 7.1 oder höher ist auf Hardware installiert, die die Mindestanforderungen erfüllt.
- XenCenter ist auf einer Management-Workstation installiert, die die Mindestanforderungen erfüllt. Sie müssen XenCenter verwenden, um Citrix ADM auf Citrix Hypervisor zu installieren.
- Sie haben die Citrix ADM .XVA-Imagedatei heruntergeladen.

XenCenter Systemanforderungen

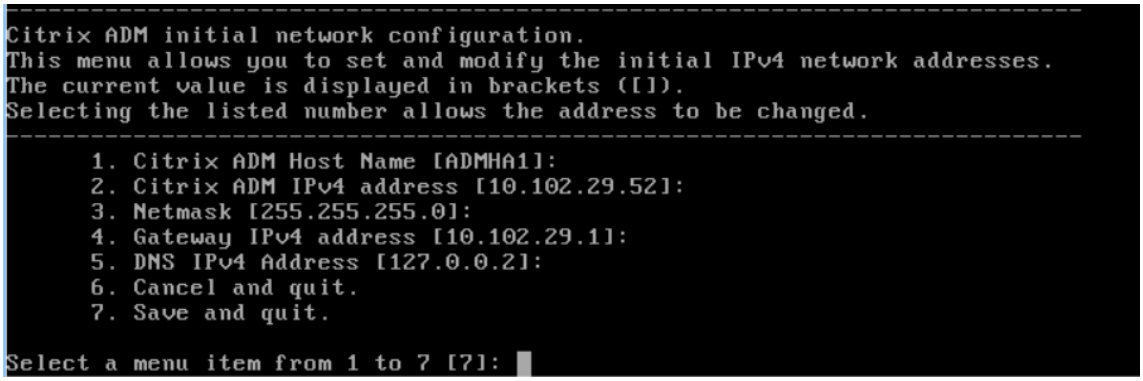
XenCenter ist eine Windows-Clientanwendung. Es kann nicht auf demselben Computer wie der Citrix Hypervisor-Host ausgeführt werden. In der folgenden Tabelle werden die Mindestsystemanforderungen beschrieben.

Komponente	Voraussetzung
Betriebssystem	Windows 7, Windows Server 2003 oder Windows 10
.NET-Framework	Version 2.0 oder höher
CPU	750 MHz (MHz), Empfohlen: 1 Gigahertz (GHz) oder schneller
RAM	1 GB, Empfohlen: 2 GB

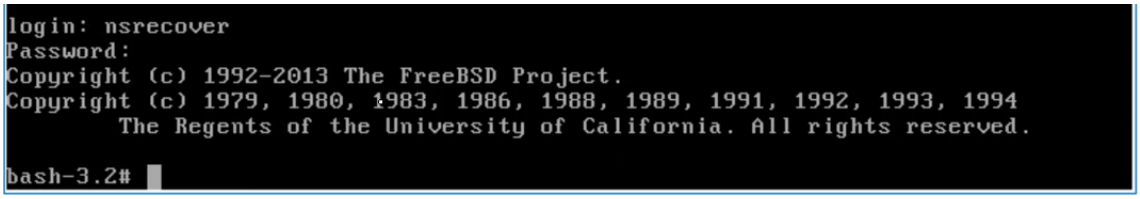
Komponente	Voraussetzung
Netzwerkkarte	100 Megabit pro Sekunde (Mbit/s) oder schnellere NIC

Installieren Sie Citrix Application Delivery Management

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



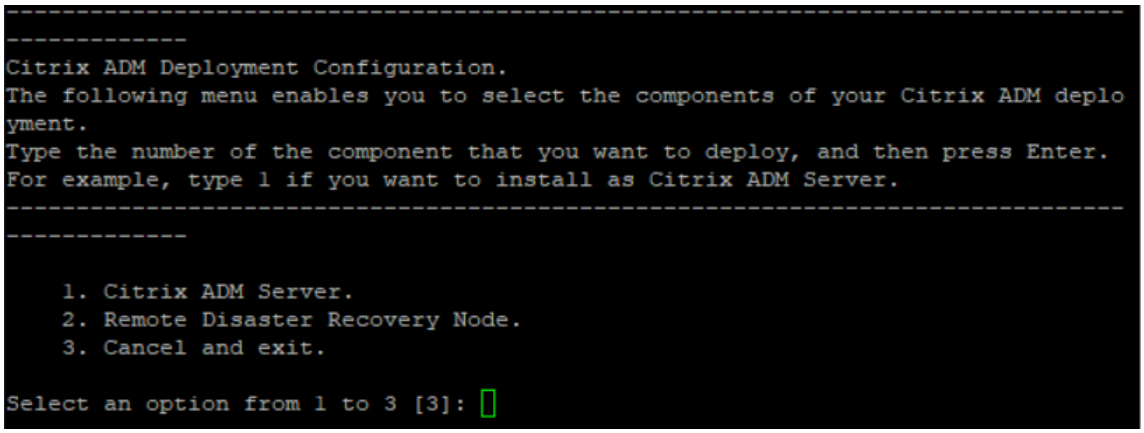
2. Speichern Sie die Konfigurationseinstellungen, nachdem Sie die erforderlichen IP-Adressen angegeben haben.
3. Melden Sie sich bei entsprechender Aufforderung mit den Anmeldeinformationen nsrecover/nsroot an.



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

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

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



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

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

Verifizierung

Nach der Installation des Servers können Sie auf die GUI zugreifen, indem Sie die IP-Adresse des NetScaler ADM-Servers im Webbrowser eingeben. Die standardmäßigen Administratoranmeldeinformationen für die Anmeldung am Server lauten nsroot/nsroot.

Der Browser zeigt das NetScaler ADM Konfigurationsprogramm an.

NetScaler ADM unter Microsoft Hyper-V

February 5, 2024

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

Voraussetzungen

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

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

Microsoft Hyper-V Systemanforderungen

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

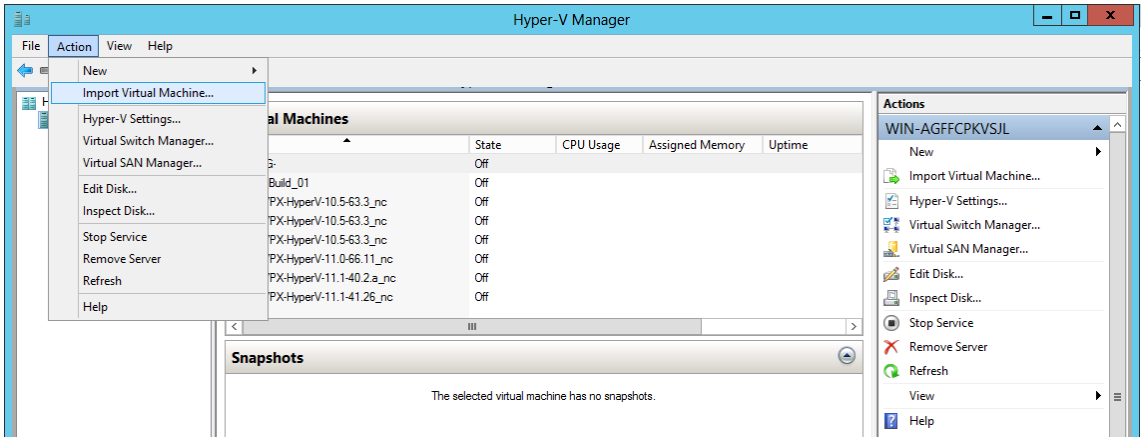
Komponente	Voraussetzung
Betriebssystem	Windows Server 2012 R2
.NET-Framework	Version 2.0 oder höher
CPU	750 MHz (MHz), Empfohlen: 1 Gigahertz (GHz) oder schneller
RAM	1 GB, Empfohlen: 2 GB
Netzwerkkarte	100 Megabit pro Sekunde (Mbit/s) oder schnellere NIC

Installieren der NetScaler Application Delivery Management

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

So installieren Sie NetScaler ADM:

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



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

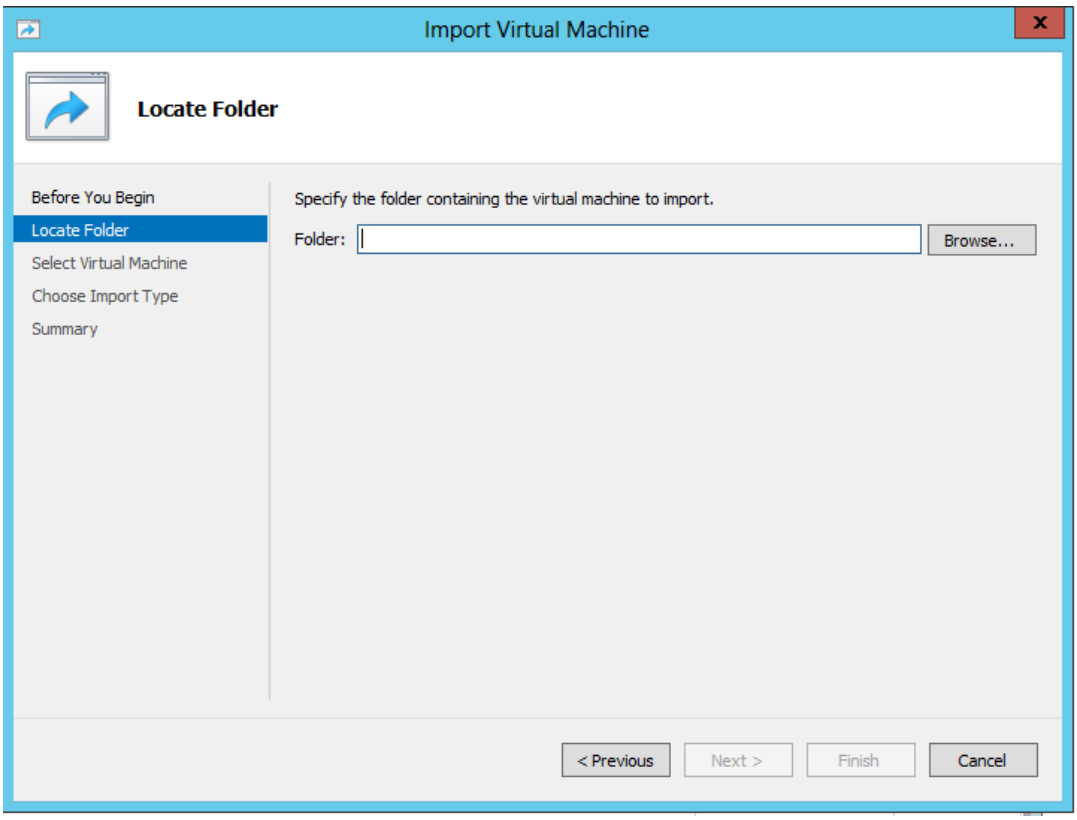
   a) Navigieren Sie im Dialogfeld Virtuelle Maschine importieren im Abschnitt **Ordner suchen** zu dem Ordner, in dem Sie das Citrix ADM Hyper-V-Image gespeichert haben, wählen Sie den Ordner aus, und klicken Sie auf **Weiter**.

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

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

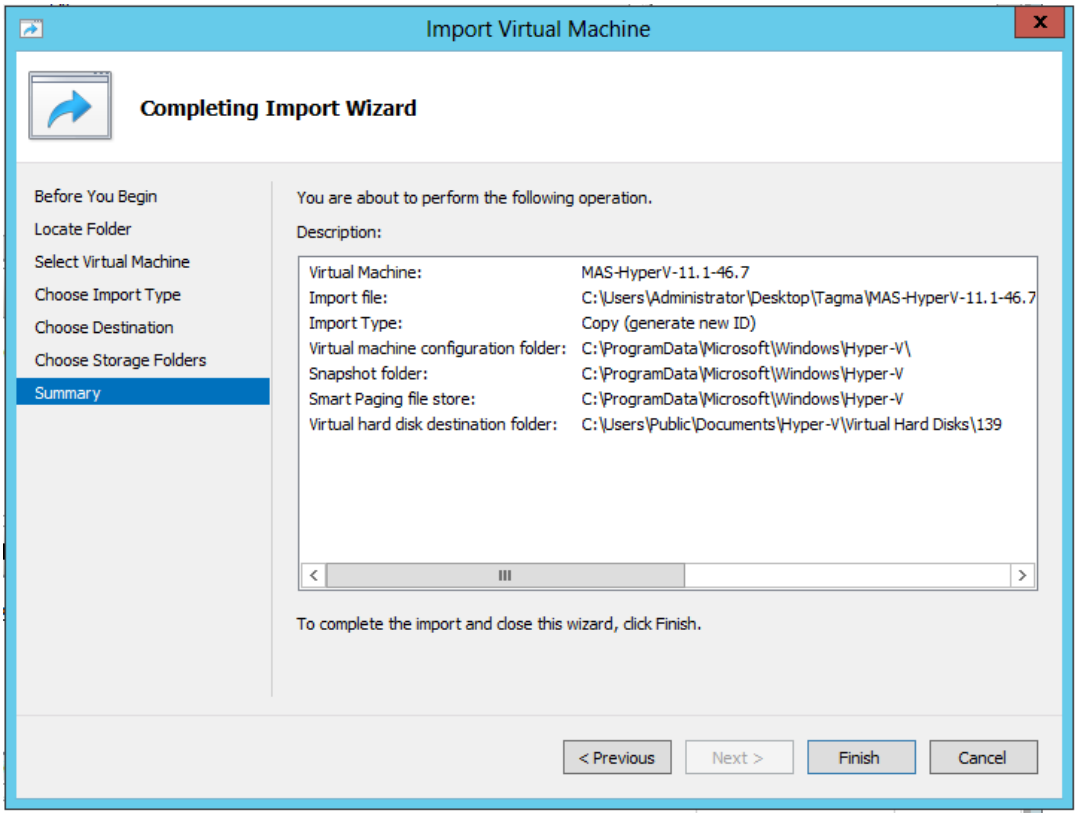
   d) Im Abschnitt **Ziel auswählen** können Sie die Ordner angeben, in denen die Dateien der virtuellen Maschine gespeichert werden sollen.

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



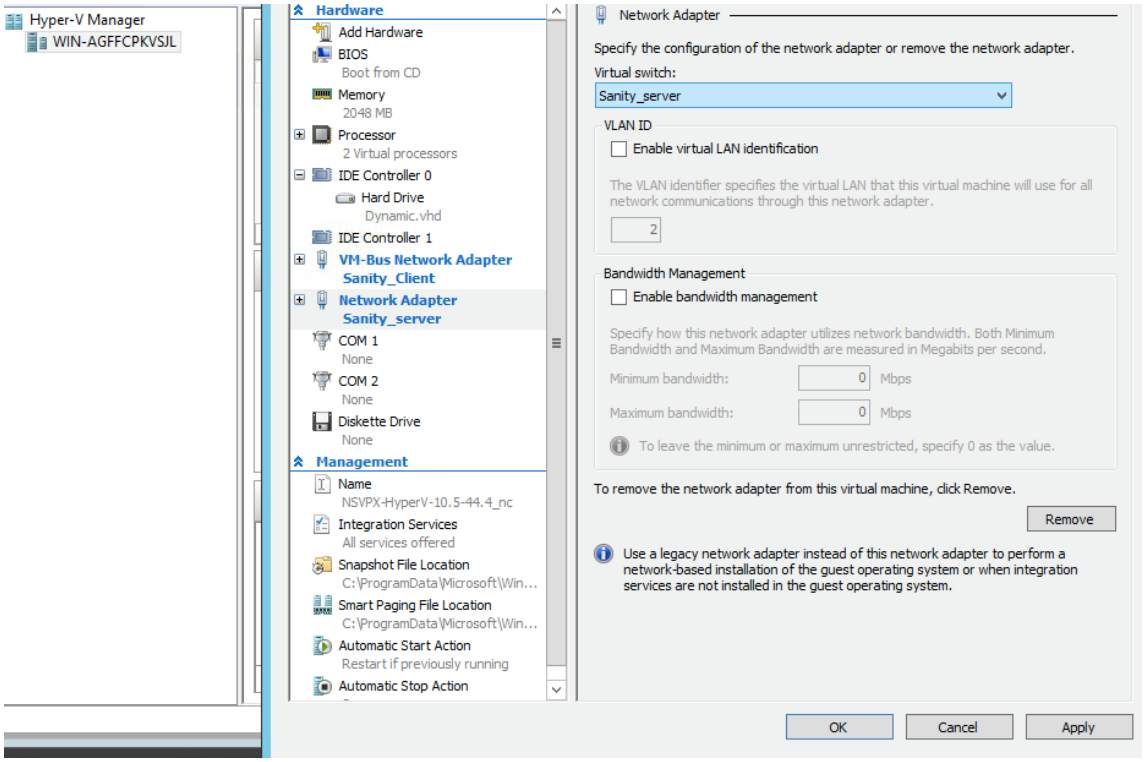
e) Im Abschnitt **Speicherordner auswählen** können Sie den Speicherort auswählen, an dem Sie die virtuellen Festplatten speichern möchten, und dann auf **Weiter**klicken.

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

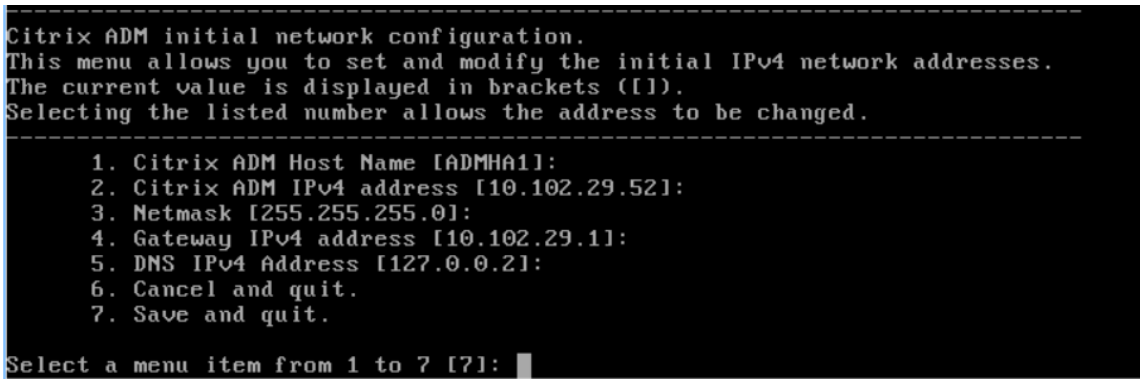


Das Citrix ADM Hyper-V-Image wird im rechten Fensterbereich angezeigt.

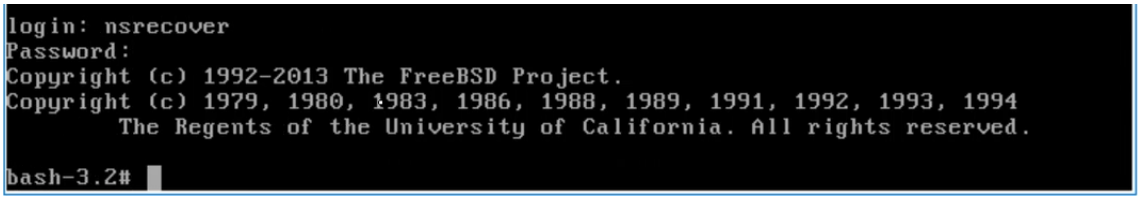
4. Klicken Sie mit der rechten Maustaste auf das NetScaler ADM Hyper-V-Image, und klicken Sie dann auf **Einstellungen**.
5. Navigieren Sie im linken Bereich des angezeigten Dialogfelds zu **Hardware** > **VM_Bus Network Adaptor**und wählen Sie im rechten Bereich aus der Netzwerkliste das entsprechende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



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



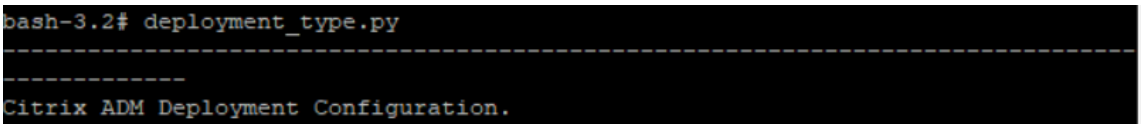
10. Speichern Sie die Konfigurationseinstellungen, nachdem Sie die erforderlichen IP-Adressen angegeben haben.
11. Melden Sie sich bei entsprechender Aufforderung mit den Anmeldeinformationen nsrecover/nsroot an.



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

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

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



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

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

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

Verifizierung

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

Der Browser zeigt das NetScaler ADM Konfigurationsprogramm an.

NetScaler ADM auf VMware ESXi

February 5, 2024

Um virtuelle NetScaler ADM Appliances auf VMware ESXi zu installieren, verwenden Sie den VMware vSphere-Client.

Voraussetzungen

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

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

> Hinweis
>
> VMotion wird nur von **NetScaler ADM 13.0 Build 47.22 oder höher** unterstützt. Sie können die Migration des auf einem ESXi-Hypervisor bereitgestellten ADM-Servers planen und automatisieren, einschließlich vSphere High Availability und vSphere DRS-Setups.

So installieren Sie NetScaler ADM

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

1. Starten Sie den VMware vSphere Client auf Ihrer Workstation.

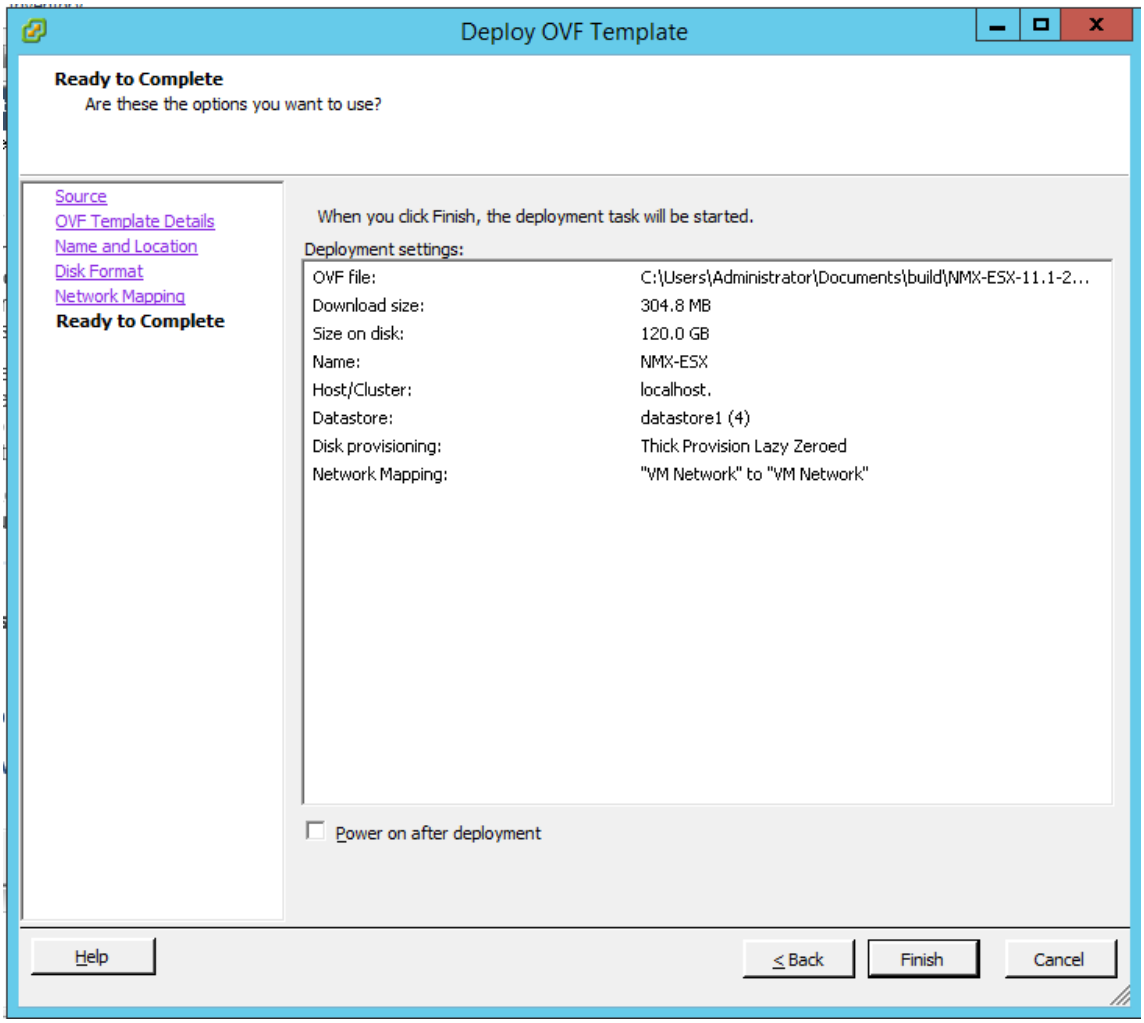
2. Geben Sie im Textfeld **IP-Adresse/Name** die IP-Adresse des VMware ESXi-Servers ein, mit dem Sie eine Verbindung herstellen möchten.
3. Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein, und klicken Sie dann auf **Anmelden**.
4. Klicken Sie im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

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

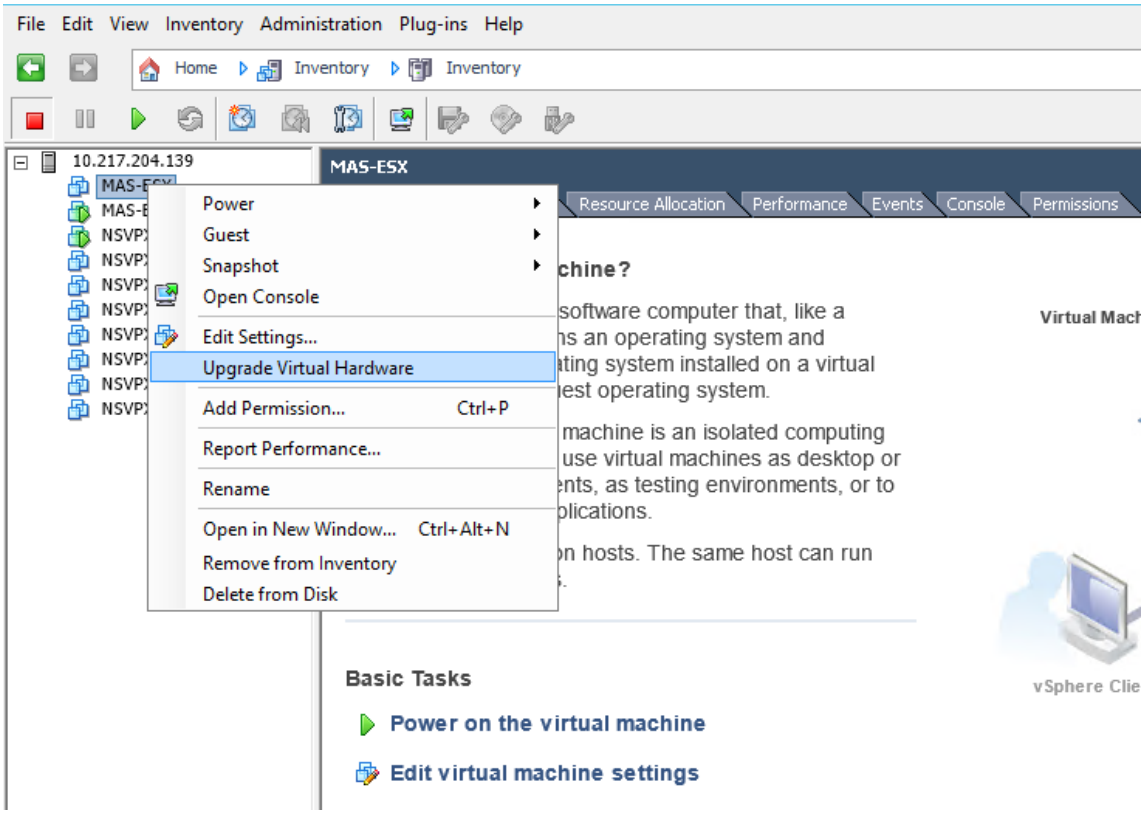
6. Klicken Sie auf der Seite **Details zur OVF-Vorlage** auf **Weiter**.
7. Geben Sie einen Namen für die virtuelle NetScaler ADM-Appliance ein, und klicken Sie dann auf **Weiter**.
8. Geben Sie das Datenträgerformat an, indem Sie entweder Thin Provisioned Format oder Thick Provisioned Format auswählen

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

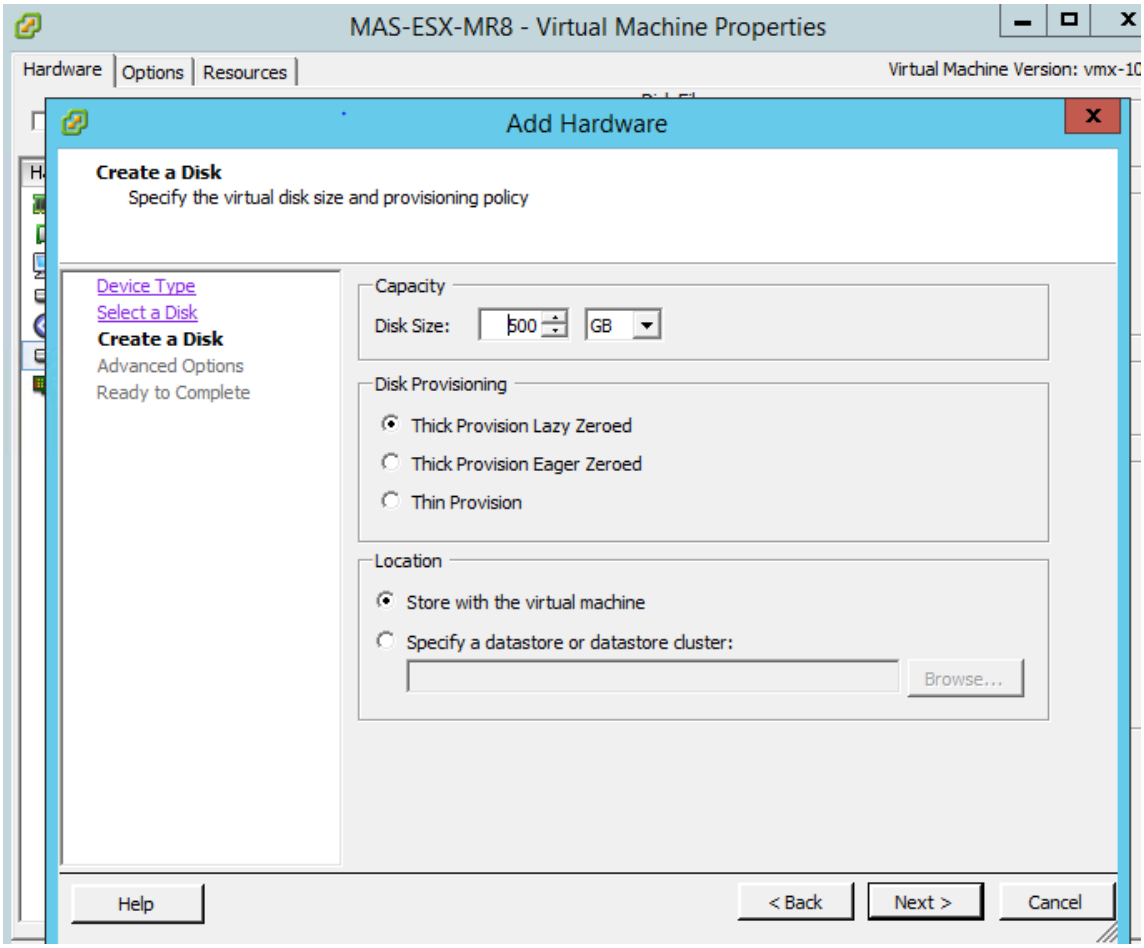
9. Klicken Sie auf **Fertig stellen**, um die Installation zu starten.



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

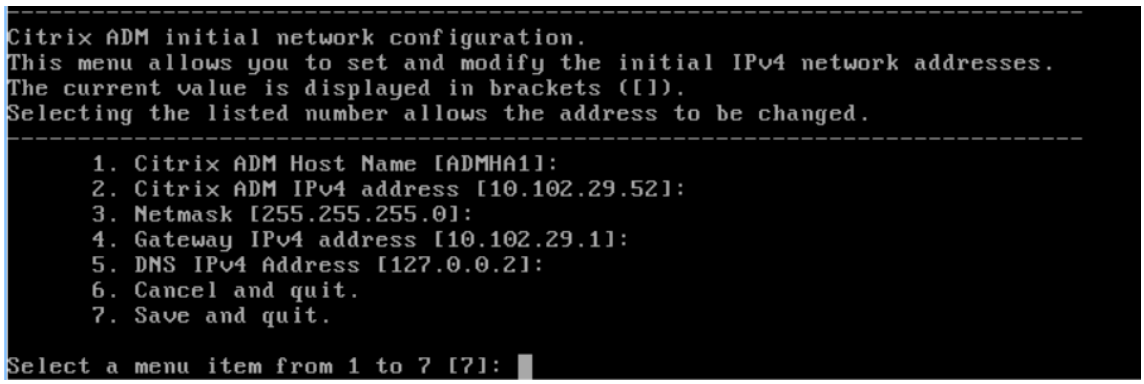


12. Klicken Sie im Menü **Inventar** auf **Virtuelle Maschine**und dann auf **Einstellungen bearbeiten**.
13. Klicken Sie im Dialogfeld **Eigenschaften der virtuellen Maschine** auf der Registerkarte **Hardware** auf **Speicher**, und geben Sie dann im rechten Bereich als **Speichergröße** 32 GB an.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



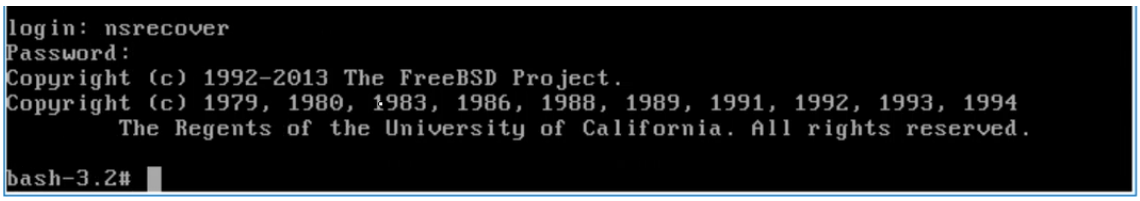
16. Wählen Sie im Navigationsbereich die virtuelle Appliance aus, die Sie installiert haben. Klicken Sie im Menü **Inventar** auf **Virtuelle Maschine**, klicken Sie auf **Einschalten**und dann **auf Einschalten**.

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



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

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

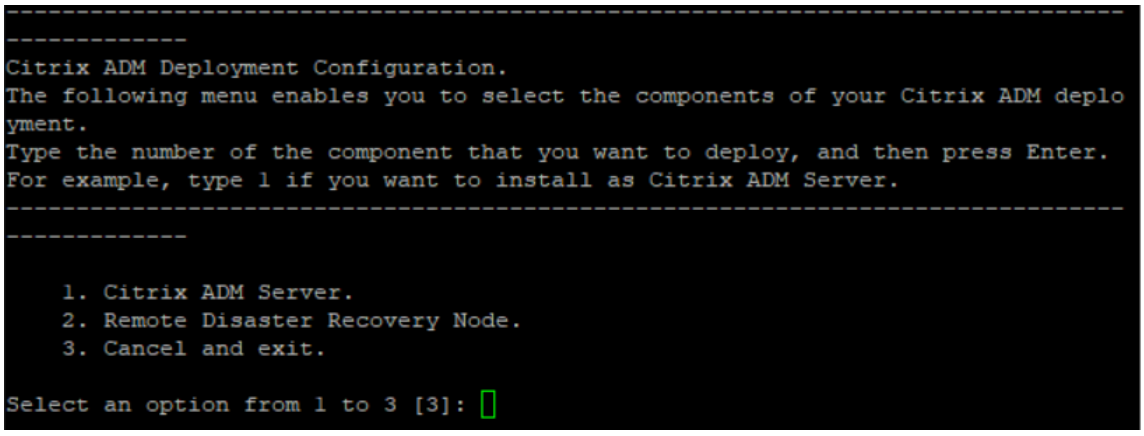


> **Hinweis**
>
> Wenn Sie sich nach der Anmeldung die anfängliche Netzwerkkonfiguration aktualisieren möchten, geben Sie die Konfiguration ein `networkconfig`, aktualisieren Sie sie und speichern Sie die Konfiguration.

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

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

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



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

> **Hinweis**

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

Verifizierung

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

Der Browser zeigt das NetScaler ADM Konfigurationsprogramm an.

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

NetScaler ADM im Kubernetes-Cluster

February 5, 2024

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

Voraussetzungen

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

Kubernetes-Cluster

- Der Kubernetes-Cluster muss die folgende Version oder höher haben:
  - Serverversion v1.13
  - Clientversion v1.13

  Geben Sie den Befehl ein `kubectl version`, um die Version zu überprüfen.
- Die auf dem Cluster installierte Helm-Anwendung muss die folgende Version oder höher haben.
  - Serverversion v2.12.1
  - Clientversion v2.12.0

Verwenden Sie den Befehl `helm version`, um die Version zu überprüfen.

- Der Kubernetes-Cluster CNI (Container Network Interface) muss Calico Version v3.1.3 oder höher sein.
- Auf allen untergeordneten Knoten im Cluster muss ein NFS-Client installiert sein. Dies liegt daran, dass die ADM-Anwendung die Daten und die Konfiguration auf Volumes, die auf einem Netzwerkdateiserver bereitgestellt werden, beibehalten. Um einen NFS-Client auf einem Ubuntu-basierten Untergebenen zu installieren, geben Sie die folgenden Befehle ein:

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

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

NFS-Freigabe

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

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

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

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

NetScaler ADC Appliance

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

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

Installieren von ADM auf Kubernetes Cluster

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

1. Gehen Sie zur Citrix Download-Site und laden Sie die Datei für das NetScaler ADM Helm Chart for Kubernetes herunter.
2. Extrahieren Sie den heruntergeladenen Helm Chart Tarball in das /var-Verzeichnis des Hauptknotens des Kubernetes-Clusters.
3. Öffnen Sie die `values.yaml`Datei unter dem `/var/citrixadm`Verzeichnis.
4. Geben Sie ein Kennwort für die Datenbank in das Feld `dbpasswd` in der Datei ein.
5. Ändern Sie die folgenden Werte. Die ADM-Anwendung verwendet diese Werte, um die NetScaler ADC Appliance so zu konfigurieren, dass die Dienste für die externe Welt verfügbar sind:
   - `ingressIP`: eine im NetScaler ADC für den Zugriff auf die Anwendung konfigurierte virtuelle IP.
   - `applicationID`: eine eindeutige ID, um die Ingress-Konfiguration vom Rest der Konfiguration auf der NetScaler ADC Appliance zu unterscheiden.
   - `ingressADCIP`: NetScaler ADC IP-Adresse (NSIP), die als Eintritt für die ADM-Anwendung verwendet wird.
   - `ingressADCUsername`: ein Benutzername für den Zugriff auf die NetScaler ADC Appliance. Dieser Benutzer muss über Schreibrechte verfügen.
   - `ingressADCPassword`: Kennwort für den Benutzernamen.

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

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

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

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

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

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


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

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

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

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

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

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

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

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

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

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

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

NetScaler ADM auf Linux KVM-Server

February 5, 2024

Virtualisierungsplattformen, auf denen NetScaler Application Delivery Management (ADM) bereitgestellt werden kann, umfassen Linux-KVM.

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

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

Voraussetzungen

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

Hardwareanforderungen

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

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

Softwareanforderungen

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

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

NetScaler ADM -Setupdateien herunterladen

So laden Sie die NetScaler ADM -Setupdateien von www.citrix.com herunter:

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

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

Installieren der NetScaler Application Delivery Management auf Linux-KVM

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

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

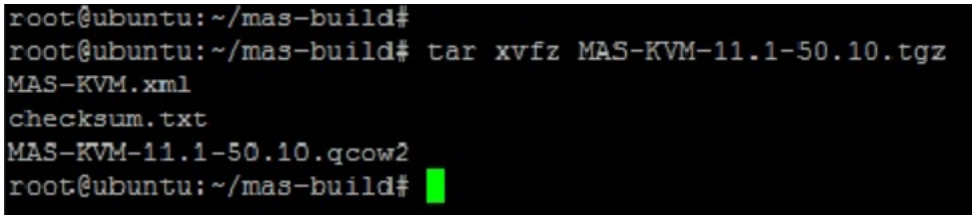
   b) Verwenden Sie den Befehl tar, um die Citrix Application Delivery Management Imagedatei zu dekomprimieren. Das entpackte Paket enthält die folgenden Komponenten:

      i. Eine Domänen-XML-Datei, die die Citrix ADM Attribute angibt

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

      iii. Ein Domänendatenträgerimage


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



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

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

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

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

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

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

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

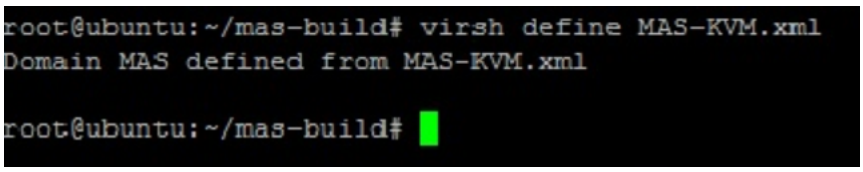
   E. `model type` - Stellen Sie auf VirtIO.

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

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

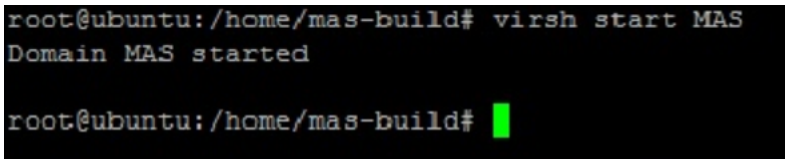
vi. Definieren Sie die VM-Attribute in der Datei MAS1-KVM.xml mit dem folgenden Befehl: `virsh define \<FileName\>.xml`

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

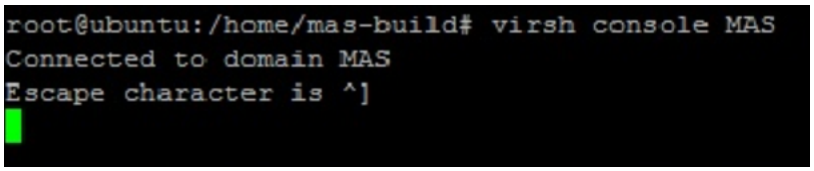
vii. Starten Sie den NetScaler ADM, indem Sie den folgenden Befehl eingeben: `virsh start \[\<DomainName\> | \<DomainUUID\>\]`

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



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

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



Konfigurieren der NetScaler Application Delivery Management

> **Hinweis**
>
> Auf einigen Linux-KVM-Hosts können FreeBSD-Gäste nicht ordnungsgemäß neu starten, wenn sie über mehr als eine CPU verfügen. Wenn die virtuelle Citrix ADM Appliance neu gestartet wird, reagieren die Citrix ADM CLI und die GUI nicht mehr. Einzelheiten finden Sie unter https://bugs.launchpad.net/qemu/+bug/1329956
>
> Um zu vermeiden, dass die NetScaler ADM CLI und die GUI beim Neustart der virtuellen NetScaler ADM-Appliance nicht mehr reagiert, fahren Sie alle virtuellen Maschinen auf dem KVM-Host herunter und führen Sie Folgendes auf dem KVM-Host aus:
>
> 1. Entfernen Sie das kvm_intel-Modul mit dem folgenden Befehl:
>
>   `rmmod kvm\\_intel`

2. Deaktivieren Sie **ApicV** und laden Sie das kvm_intel-Modul mit dem folgenden Befehl neu: `modprobe kvm\\_intel enable\\_apicv=N`
3. Starten Sie die virtuellen Maschinen auf dem KVM-Host.

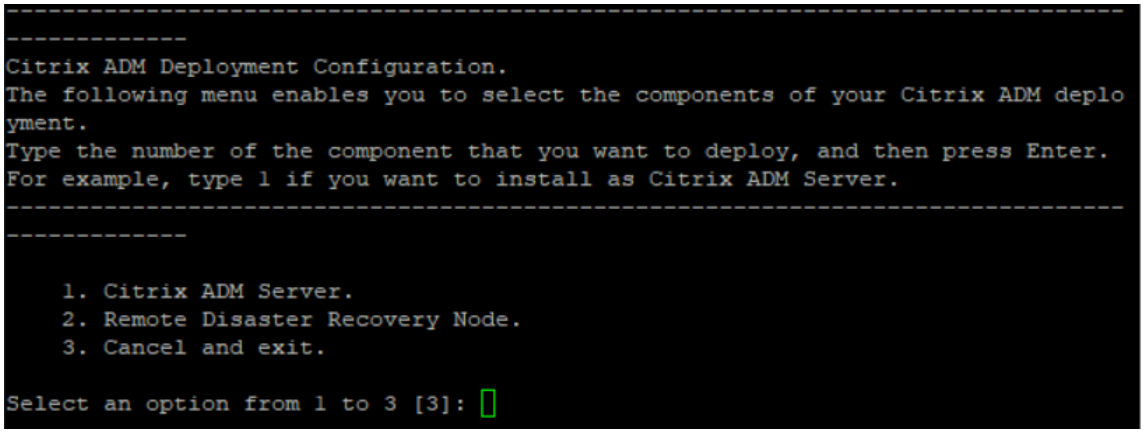
Nach der Installation des NetScaler ADM können Sie etwa 10 Minuten einplanen, bis die Dienste verfügbar werden, und melden Sie sich dann beim NetScaler ADM an.

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

   Hinweis

   Nachdem Sie sich zum ersten Mal angemeldet haben, ändern Sie das Administratorkennwort. Konfigurieren Sie dann den MAS so, dass er in Ihrem Netzwerk funktioniert. Sie können das Kennwort über die NetScaler ADM Benutzeroberfläche ändern. Navigieren Sie auf der Citrix ADM Homepage zu **System** > **Benutzerverwaltung** > **Benutzer**. Wählen Sie den Benutzer aus, klicken Sie auf **Bearbeiten**, und aktualisieren Sie das Kennwort im Feld Kennwort.
2. Geben Sie an der Eingabeaufforderung Folgendes ein: *shell*
3. Geben Sie **networkconfig** ein, um das Citrix ADM Menü für die anfängliche Netzwerkkonfiguration aufzurufen. Konfigurieren Sie die Management-IP-Adresse.
4. Befolgen Sie die Anweisungen, um die anfängliche Netzwerkkonfiguration von Citrix ADM abzuschließen. Die Konsole zeigt die anfänglichen Netzwerkkonfigurationsoptionen für Citrix ADM an, um die folgenden Parameter für Citrix ADM festzulegen. Der Hostname wird standardmäßig aufgefüllt.
   a) Geben Sie **2** ein, um die Citrix ADM IPv4-Adresse zu aktualisieren: Verwaltungs-IP-Adresse, unter der Sie auf ein Citrix ADM zugreifen
   b) Geben Sie **3** ein, um die Netzmaske zu aktualisieren —die der Management-IP-Adresse zugeordnete Subnetzmaske
   c) Geben Sie **4** ein, um die Gateway -IPv4-Adresse zu aktualisieren: Standard-Gateway-IP-Adresse für das Subnetz der Verwaltungs-IP-Adresse von Citrix ADM
   d) Geben Sie **7** ein, um zu speichern und zu beenden - speichert Ihre Konfigurationsänderungen und beendet das System.

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



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

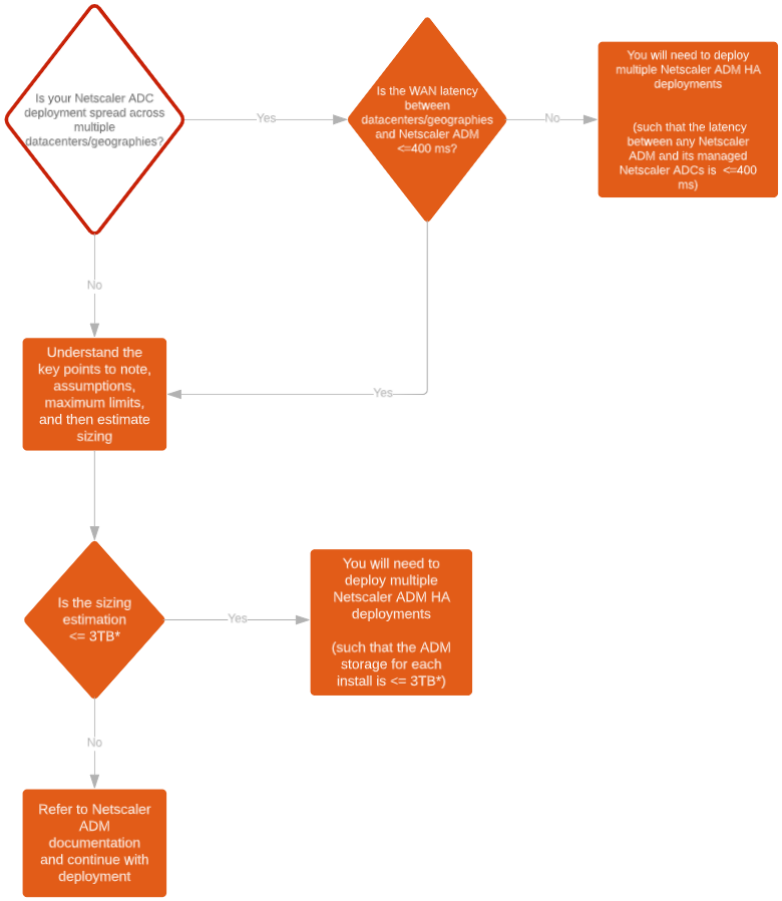
   Sie können später auf Citrix ADM zugreifen, indem Sie die IP-Adresse des Citrix ADM-Servers in die Adressleiste Ihres Browsers eingeben. Die standardmäßigen Administratoranmeldedaten für die Anmeldung am Server sind *nsroot/nsroot*.

Bereitstellung mit hoher Verfügbarkeit konfigurieren

February 5, 2024

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

Bereitstellungsszenario



> **Hinweis**
>
> Das validierte Maximalspeicherlimit für eine einzelne NetScaler ADM HA-Bereitstellung beträgt 3 TB. Weitere Informationen finden Sie im Bereitstellungshandbuch.
>
> **Wichtig!**
>
> **So greifen Sie mit HTTPS auf Citrix ADM 12.1 Build 48.18 oder spätere Versionen zu:**
>
> Wenn Sie eine Citrix ADC-Instanz für den Lastausgleich von Citrix ADM in einem Hochverfüg-

> barkeitsmodus konfiguriert haben, entfernen Sie zuerst die Citrix ADC-Instanz. Konfigurieren Sie anschließend eine Floating-IP für den Zugriff auf Citrix ADM im Hochverfügbarkeitsmodus.

Im Folgenden sind die Vorteile einer Hochverfügbarkeitsbereitstellung in Citrix ADM aufgeführt:

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

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

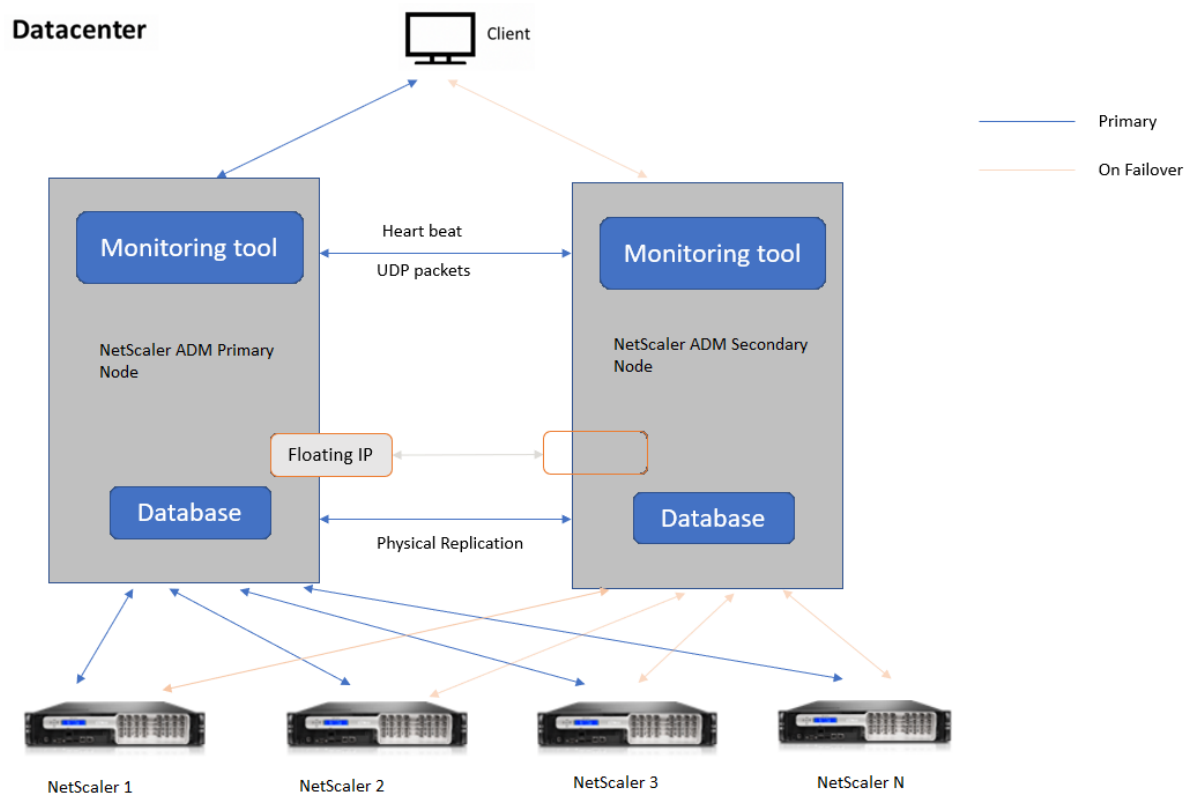
Begriff	Beschreibung
Primärer Knoten	Erster Knoten, der in der Hochverfügbarkeitsbereitstellung registriert wurde.
Sekundärer Knoten	Zweiter Knoten, der in der Hochverfügbarkeitsbereitstellung registriert wurde.
Herzschlag	Ein Mechanismus, der zum Austausch von Nachrichten zwischen primärem und sekundärem Knoten im Hochverfügbarkeits-Setup verwendet wird. Die Nachrichten bestimmen den Status und den Zustand der Anwendung auf jedem einzelnen Knoten.

Begriff	Beschreibung
Floating-IP-Adresse	Eine Floating-IP ist eine IP-Adresse, die sofort von einem Knoten auf einen anderen im selben Subnetz verschoben werden kann. Intern ist es als Alias auf der Netzwerkschnittstelle des primären Knotens eingerichtet. Bei einem Failover wird die Floating-IP nahtlos von der alten primären zur neuen verschoben. Sie ist bei der Einrichtung mit hoher Verfügbarkeit nützlich, da es Clients ermöglicht, mit den Hochverfügbarkeitsknoten über eine einzige IP-Adresse zu kommunizieren.

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

Komponenten der Hochverfügbarkeitsarchitektur

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



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

Tool zur Überwachung

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

Primärer Knoten

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

Sekundärer Knoten

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

Physische Streaming-Replikation

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

Heartbeat-Nachrichten

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

Floating-IP-Adresse

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

Wichtige Punkte, die es zu beachten gilt

- In einem Hochverfügbarkeits-Setup werden beide Citrix ADM Knoten im Aktiv-Passiv-Modus bereitgestellt. Sie müssen sich in denselben Subnetzen befinden und dieselbe Softwareversion und denselben Build verwenden und dieselbe Konfiguration haben.

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

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

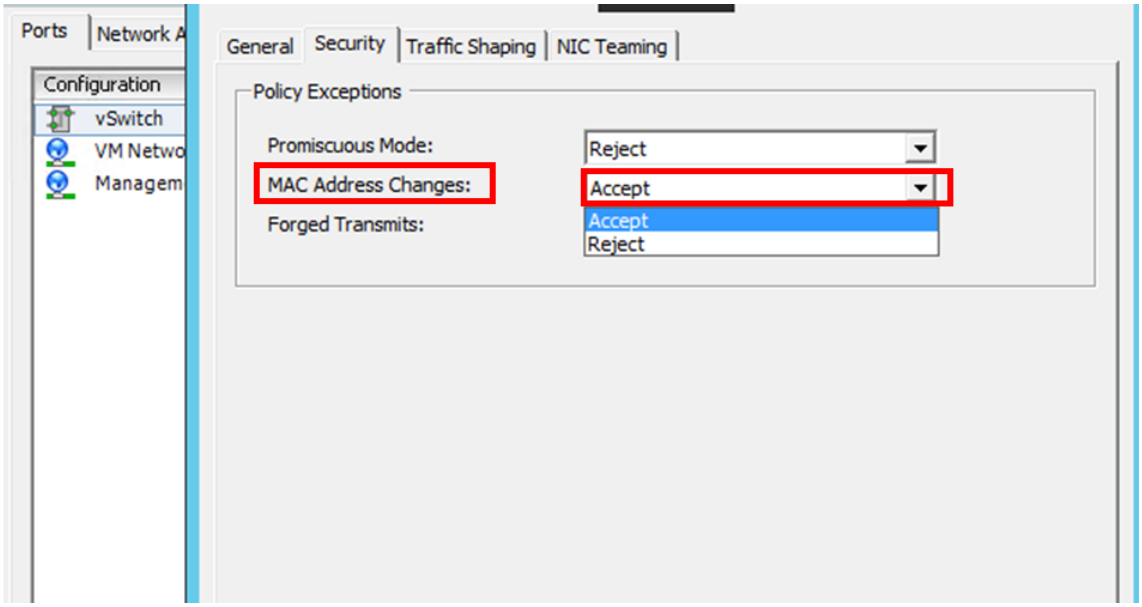
- Datenbank:
  - In einem Hochverfügbarkeits-Setup werden alle Konfigurationsdateien im Abstand von einer Minute automatisch vom primären Knoten zum sekundären Knoten synchronisiert.
  - Die Datenbanksynchronisierung erfolgt sofort durch physische Replikation der Datenbank.
  - Die Datenbank auf dem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

- NetScaler ADM Upgrade:
  - Interne Prozesse aktualisieren Citrix ADM implizit von früheren Versionen.

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

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

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



Voraussetzungen

Bevor Sie die Hochverfügbarkeit für Citrix ADM Nodes einrichten, beachten Sie die folgenden Voraussetzungen:

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

Citrix empfiehlt, dass Sie die CPU-Priorität (in den Eigenschaften der virtuellen Maschine) auf der höchsten Ebene festlegen, um das Planungsverhalten und die Netzwerklatenz zu verbessern.

In der folgenden Tabelle sind die Mindestanforderungen für die virtuellen Computerressourcen aufgeführt:

Komponente	Voraussetzung
RAM	**32 GB**
Virtuelle CPU	**8 CPUs**
Stauraum	Citrix empfiehlt die Verwendung der Solid-State-Drive-Technologie (SSD) für Citrix ADM Bereitstellungen. Der Standardwert ist 120 GB. Die tatsächliche Speicheranforderung hängt von der Schätzung der NetScaler ADM Größe ab. Wenn Ihre NetScaler ADM Speicheranforderung 120 GB überschreitet, müssen Sie einen zusätzlichen Datenträger bereitstellen. **Hinweis:** Sie können nur eine zusätzliche Festplatte hinzufügen. Citrix empfiehlt, zum Zeitpunkt der Erstbereitstellung den Speicher zu schätzen und zusätzlichen Datenträger anzuhängen. Weitere Informationen finden Sie unter So fügen Sie eine zusätzliche Festplatte an Citrix ADM an.
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s oder 100 Mbit/s
Hypervisor	**Versionen**
Citrix Hypervisor	6.2 und 6.5
VMware ESXi	5.5 und 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu und Fedora

So richten Sie Citrix ADM im Hochverfügbarkeitsmodus ein

1. Registrieren Sie den ersten Server (primärer Knoten) und stellen Sie ihn bereit.
2. Registrieren Sie den zweiten Server (sekundärer Knoten) und stellen Sie ihn bereit.
3. Stellen Sie den primären und sekundären Knoten für das Hochverfügbarkeits-Setup bereit.

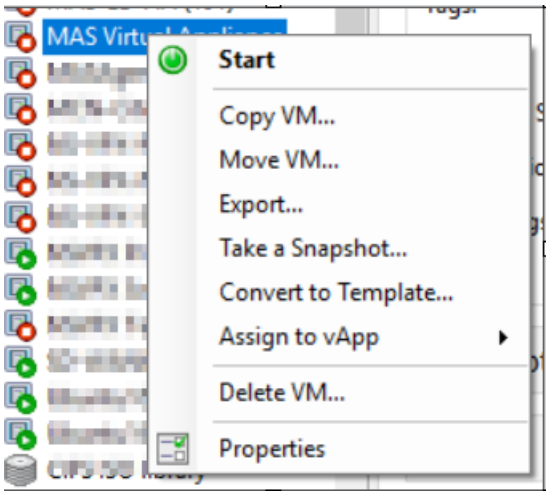
Registrieren und Bereitstellen des ersten Servers (primärer Knoten)

Um den ersten Knoten zu registrieren:

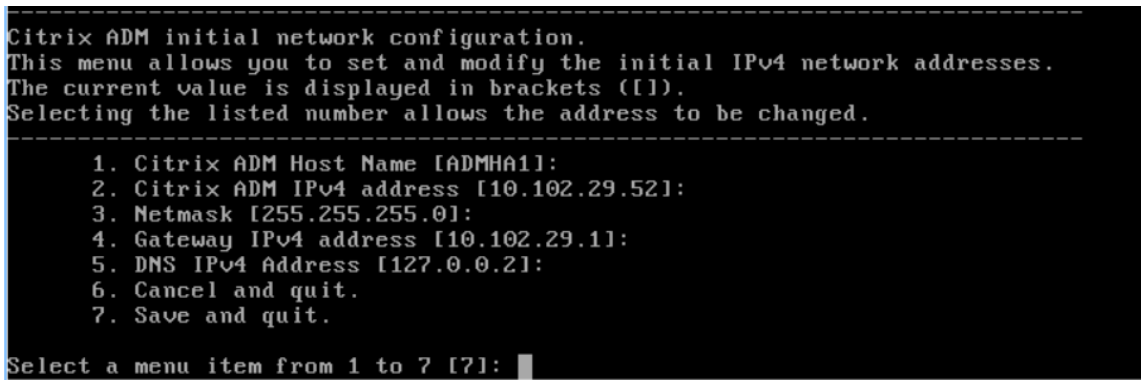
1. Verwenden Sie die XVA-Imagedatei, die von der Citrix Download-Site heruntergeladen wurde, und importieren Sie sie in Ihren Hypervisor.

   > **Hinweis:**
   >
   > Es kann einige Minuten dauern, bis die XVA-Imagedatei importiert und gestartet wird. Sie können den Status unten auf dem Bildschirm sehen.

2. Nachdem der Import erfolgreich ist, klicken Sie mit der rechten Maustaste, und klicken Sie auf **Start**.

3. Konfigurieren Sie Citrix ADM auf der Registerkarte **Konsole** mit den anfänglichen Netzwerkkonfigurationen.

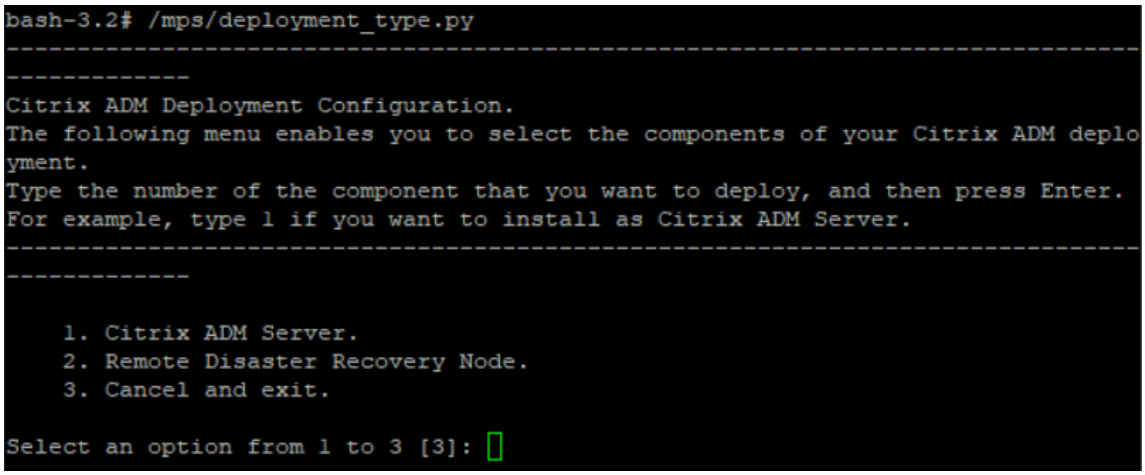
4. Nachdem die anfängliche Netzwerkkonfiguration abgeschlossen ist, fordert das System zur Anmeldung auf. Melden Sie sich mit den folgenden Anmeldeinformationen an: *nsrecover/nsroot*.

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

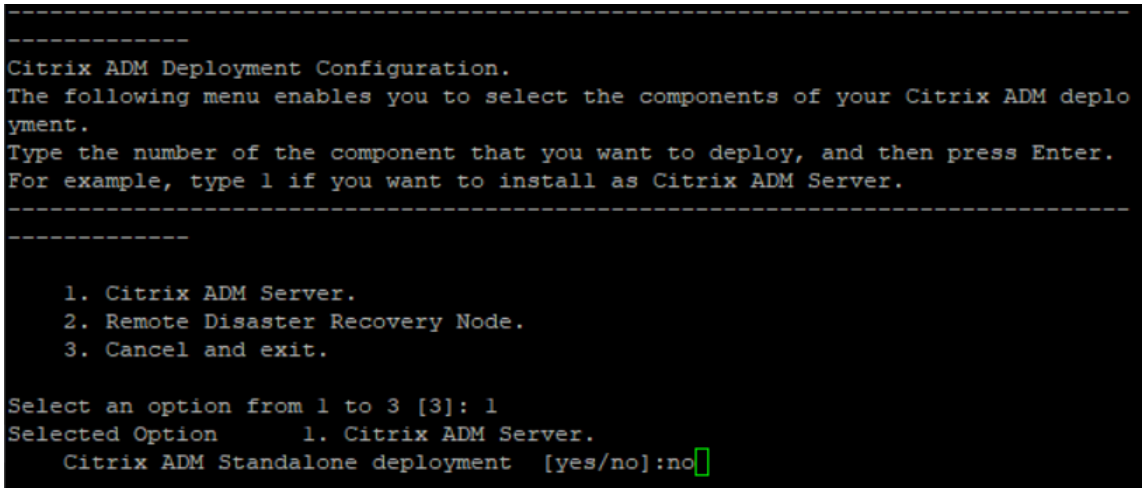
> ichern Sie die Konfiguration.

5. Geben Sie **/mps/deployment_type.py**ein, um den primären Knoten bereitzustellen. Das Konfigurationsmenü für die Citrix ADM-Bereitstellung wird angezeigt.

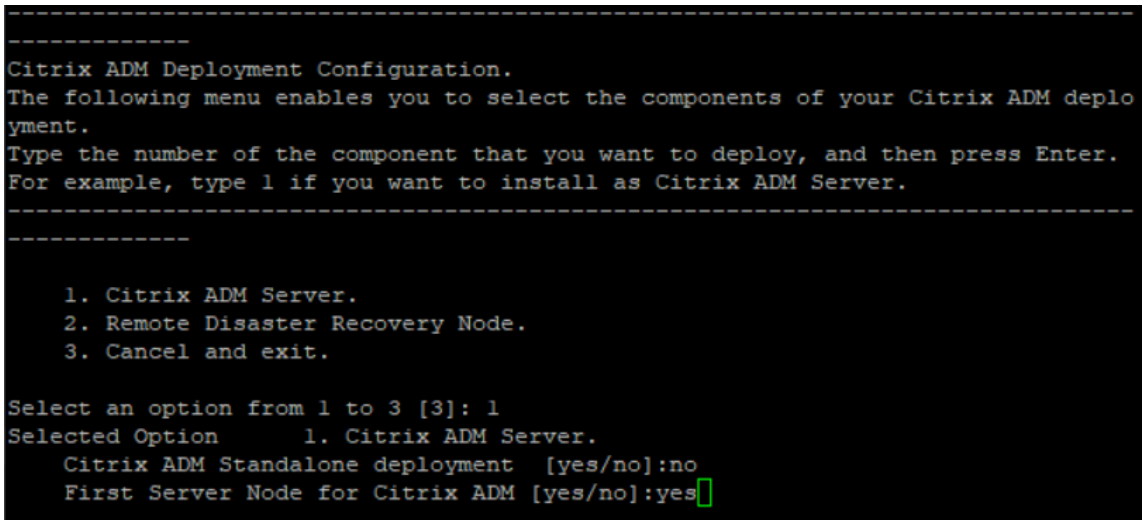
6. Wählen Sie **1** aus, um den NetScaler ADM -Server als primären Knoten zu registrieren.



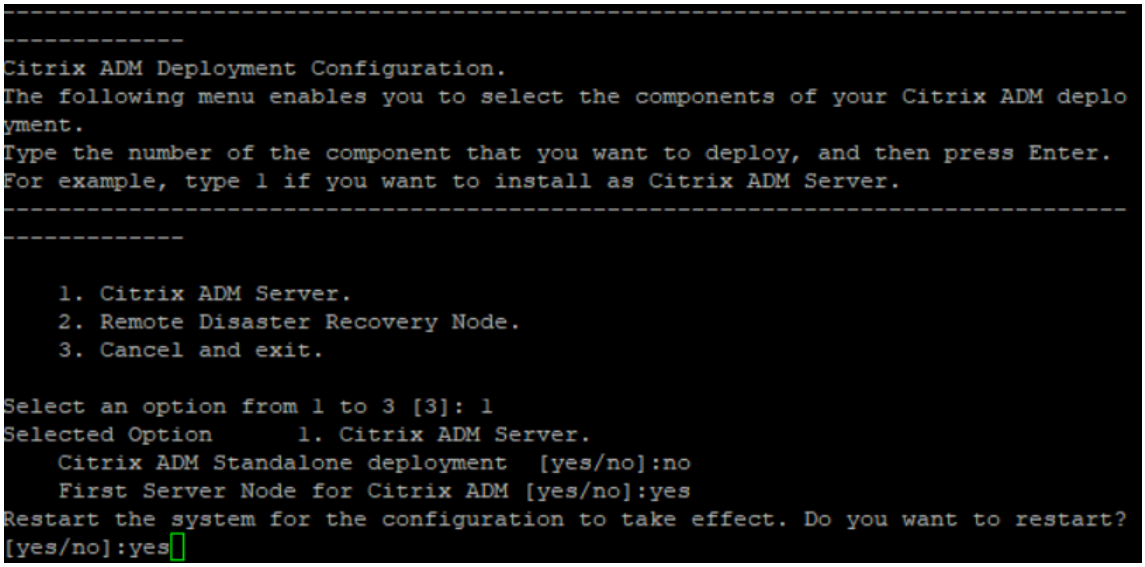
7. Die Konsole fordert Sie auf, die eigenständige NetScaler ADM Bereitstellung auszuwählen. Geben Sie**Nein** ein, um die Bereitstellung als Hochverfügbarkeit zu bestätigen.



8. Die Konsole fordert Sie auf, den ersten Serverknoten auszuwählen. Geben Sie**Ja** ein, um den Knoten als ersten Knoten zu bestätigen.



9. Die Konsole fordert Sie auf, das System neu zu starten. Geben Sie **Ja** ein, um neu zu starten.



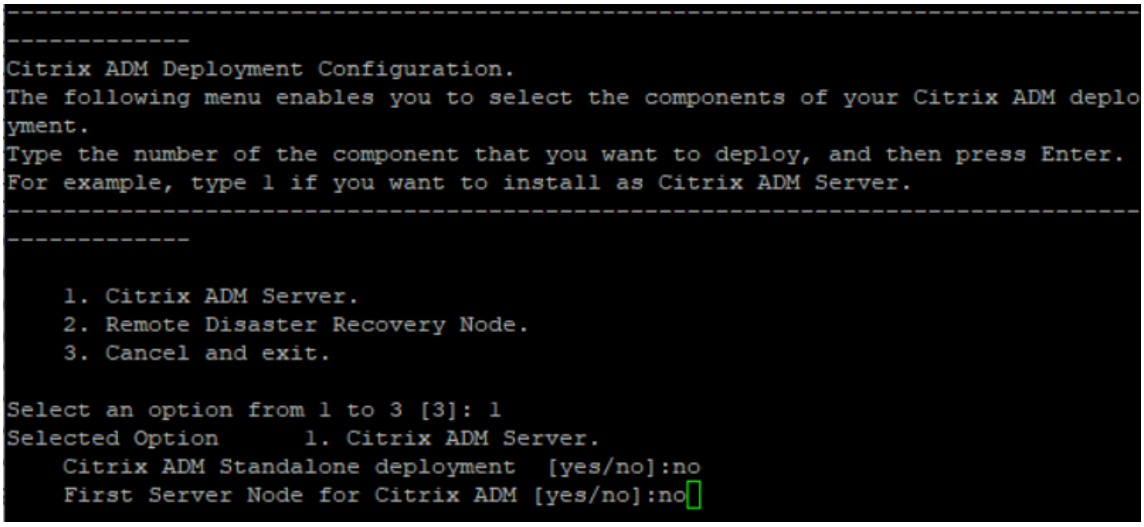
Das System wird neu gestartet und als primärer Knoten in der NetScaler ADM Benutzeroberfläche angezeigt.

Registrieren und Bereitstellen des zweiten Servers (sekundärer Knoten)

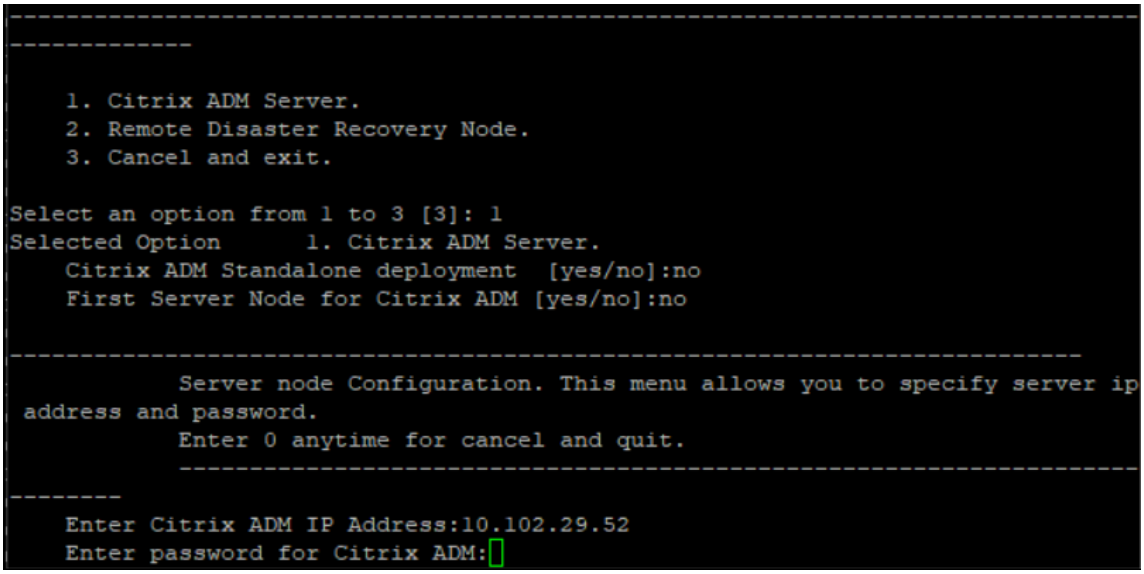
1. Verwenden Sie die **XVA-Imagedatei**, die von der Citrix Download-Site heruntergeladen wurde, und importieren Sie sie in Ihren Hypervisor.
2. Konfigurieren Sie Citrix ADM auf der Registerkarte **Konsole** mit den anfänglichen Netzwerkkonfigurationen, wie in der folgenden Abbildung dargestellt.
3. Nachdem die anfängliche Netzwerkkonfiguration abgeschlossen ist, fordert das System zur Anmeldung auf. Melden Sie sich mit den folgenden Anmeldeinformationen an: *nsrecover/nsroot*.

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

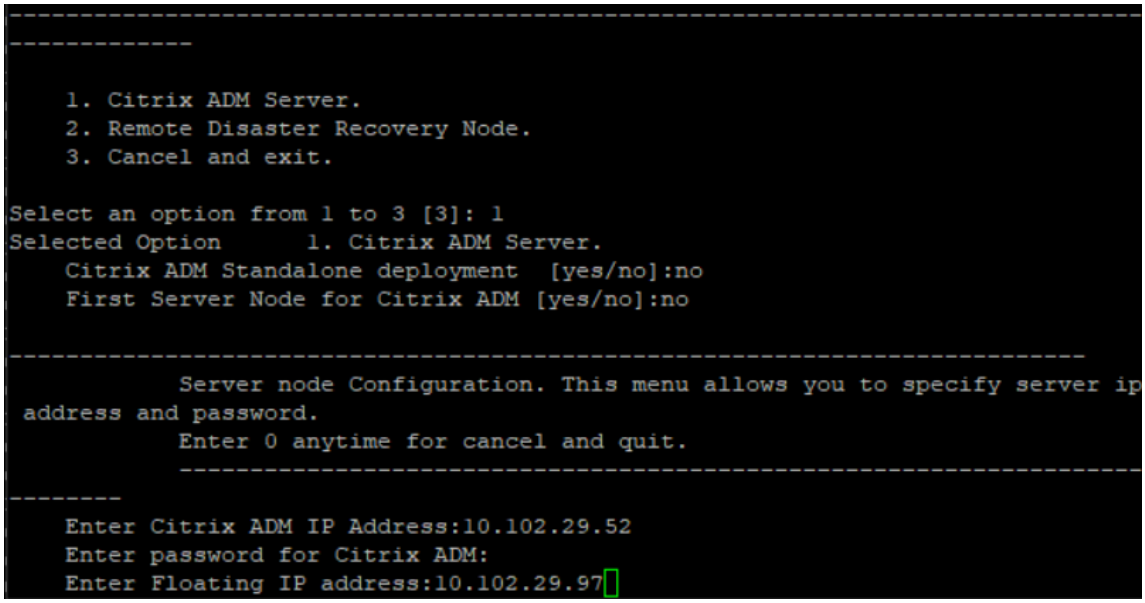
4. Geben Sie **/mps/deployment_type.py**ein, um den sekundären Knoten bereitzustellen. Das Konfigurationsmenü für die Citrix ADM-Bereitstellung wird angezeigt.
5. Wählen Sie **1**, um den Citrix ADM Server als sekundären Knoten zu registrieren.
6. Die Konsole fordert Sie auf, das Citrix ADM als eigenständige Bereitstellung auszuwählen. Geben Sie**Nein** ein, um die Bereitstellung als Hochverfügbarkeit zu bestätigen.
7. Die Konsole fordert Sie auf, den ersten Serverknoten auszuwählen. Geben Sie**Nein** ein, um den Knoten als zweiten Server zu bestätigen.



8. Die Konsole fordert Sie auf, die IP-Adresse und das Kennwort des primären Knotens einzugeben.



9. Die Konsole fordert Sie auf, die schwebende IP-Adresse einzugeben.



10. Die Konsole fordert Sie auf, das System neu zu starten. Geben Sie **Ja** ein, um neu zu starten.

> **Hinweis**
>
> - Eine Floating-IP-Adresse ist für die Bereitstellung von Knoten mit hoher Verfügbarkeit erforderlich.
> - Das System zeigt Fehlermeldungen an, wenn es Probleme mit der Konfiguration gibt.
> - Das System wird neu gestartet und es dauert einige Minuten, bis die Konfigurationen wirksam werden.

Bereitstellen des primären und sekundären Knotens als Hochverfügbarkeitspaar

Nach der Registrierung werden sowohl primäre als auch sekundäre Knoten auf der Citrix ADM Benutzeroberfläche angezeigt. Stellen Sie diese Knoten in einem Hochverfügbarkeitspaar bereit.

> **Hinweis**
>
> - Bevor Sie die Knoten in einem Hochverfügbarkeitspaar bereitstellen, stellen Sie sicher, dass der sekundäre Knoten nach der ersten Netzwerkkonfiguration mit einem Neustart abgeschlossen ist.
> - Verwenden Sie nach Abschluss der Hochverfügbarkeitsbereitstellung die Floating-IP, um auf die Citrix ADM-Benutzeroberfläche zuzugreifen.

Gehen Sie wie folgt vor, um Knoten als Hochverfügbarkeitspaar bereitzustellen:

1. Öffnen Sie einen Webbrowser und geben Sie die IP-Adresse des ersten Citrix ADM Serverknotens ein.

2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der Startseite auf **Get Started**.
4. Wählen Sie den Bereitstellungstyp als**Zwei Server im Hochverfügbarkeitsmodus**aus, und klicken Sie auf**Weiter**.
5. Klicken Sie auf der Seite Bereitstellung auf**Bereitstellen**.
6. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **Ja**.

   NetScaler ADM wird neu gestartet und dauert etwa 10 Minuten, bis die Konfiguration wirksam wird.

   > **Hinweis**
   >
   > Sie können jetzt die Floating-IP-Adresse verwenden.

7. Melden Sie sich mit Administratoranmeldeinformationen bei Citrix ADM an, klicken Sie auf der Homepage auf **Erste Schritte** und führen Sie optional die folgenden Schritte aus:

   a) Hinzufügen NetScaler ADC-Instanzen

   b) Kundenidentität konfigurieren

   > **Hinweis**
   >
   > Sie können auch auf **Überspringen klicken, um den** Vorgang später abzuschließen, und auf **Fertig stellen**klicken.

8. Navigieren Sie zu **System** > **Bereitstellung**, um die Bereitstellung zu überprüfen.

   Weitere Informationen finden Sie in den Häufig gestellten Fragen.

Hochverfügbarkeit deaktivieren

Sie können die Hochverfügbarkeit auf einem Citrix ADM Hochverfügbarkeitspaar deaktivieren und die Knoten in eigenständige Citrix ADM Server konvertieren.

> **Hinweis**
>
> Deaktivieren Sie die Hochverfügbarkeit vom primären Knoten aus.

Um die Hochverfügbarkeit zu deaktivieren:

1. Geben Sie in einem Webbrowser die IP-Adresse des primären Citrix ADM Serverknotens ein.
2. Geben Sie in die Felder **Benutzername**und**Kennwort** die Administratoranmeldeinformationen ein.

3. Navigieren Sie auf der Registerkarte**System** zu**Bereitstellung**, und klicken Sie auf**HA aufheben**.

   Es wird ein Dialog angezeigt. Klicken Sie auf **Ja**, um die Hochverfügbarkeitsbereitstellung zu unterbrechen.

Hochverfügbarkeit erneut bereitstellen

Nachdem Sie die Hochverfügbarkeit für eine eigenständige Bereitstellung deaktiviert haben, können Sie sie erneut in den Hochverfügbarkeitsmodus bereitstellen. Das erneute Bereitstellen von Hochverfügbarkeit ähnelt der Erstbereitstellung von Hochverfügbarkeit. Weitere Einzelheiten finden Sie unter Bereitstellen des primären und sekundären Knotens als Paar mit hoher Verfügbarkeit.

Hochverfügbarkeits-Failover-Szenarien

Ein Failover erfolgt, wenn eine der folgenden Bedingungen eintritt:

- **Knotenausfall**: Der primäre Knoten fällt aus, 180 Sekunden lang wird kein Herzschlag vom primären Knoten erkannt.
- **Anwendungsintegritätsfehler**: Der primäre Knoten ist gestartet und läuft, aber einer der NetScaler ADM Prozesse ist nicht mehr verfügbar.

Split-Hirn-Szenario

Wenn aufgrund einer Ausfallzeit der Netzwerkverbindung keine Kommunikation zwischen den beiden Knoten stattfindet, gilt Folgendes:

- Der primäre Knoten arbeitet weiterhin als primärer Knoten
- Der sekundäre Knoten übernimmt die Funktion des primären Knotens, da keine Herzschläge empfangen werden können
- Beide Knoten würden ihre einzelnen Datenbankinstanzen ausführen.

In einem Unternehmen wurden beispielsweise zwei Citrix ADM-Knoten als primär und sekundär bereitgestellt. Aufgrund einer möglichen Ausfallzeit der Netzwerkverbindung wird die Kommunikation zwischen den beiden Citrix ADM Knoten vollständig unterbrochen. Da über 180 Sekunden lang kein Herzschlagaustausch stattfindet, betrachten sich beide Knoten als primärer Knoten. Beide Knoten fungieren als aktive Knoten und führen ihre eigenen Instanzen der Datenbank aus.

Ab Citrix ADM 12.1 oder einer späteren Version wird diese Split-Brain-Situation ordnungsgemäß behandelt, nachdem die Netzwerkverbindung und der Heartbeat wiederhergestellt wurden. Hochverfügbarkeitssynchronisierung wird automatisch wiederhergestellt. Die Wiederherstellungszeit hängt von den Daten und der Geschwindigkeit der Verbindung zwischen den Knoten ab.

> **Hinweis**
>
> Während des Split-Brain-Zustands werden Änderungen, die am alten Primärknoten vorgenommen wurden, auf den neuen Primärknoten zurückgesetzt, wenn dieser wieder mit hoher Verfügbarkeit verbunden wird. Die Änderungen, die auf dem neuen Primärknoten während des Split-Gehirns aufgetreten sind, bleiben intakt.

Notfallwiederherstellung für hohe Verfügbarkeit konfigurieren

February 5, 2024

Katastrophe ist eine plötzliche Störung der Geschäftsfunktionen, die durch Naturkatastrophen oder durch Menschen verursachte Ereignisse verursacht werden. Katastrophen wirken sich auf den Betrieb des Rechenzentrums aus. Danach müssen die am Katastrophenort verlorenen Ressourcen und Daten vollständig neu aufgebaut und wiederhergestellt werden. Der Verlust von Daten oder Ausfallzeiten im Rechenzentrum ist entscheidend und reduziert die Business Continuity.

Die Citrix ADM Disaster Recovery (DR) -Funktion bietet vollständige Systemsicherungs- und Wiederherstellungsfunktionen für Citrix ADM, das im Hochverfügbarkeitsmodus bereitgestellt wird. Zum Zeitpunkt der Wiederherstellung stehen Zertifikate, Konfigurationsdateien und ein vollständiges Backup der Datenbank auf der Wiederherstellungs-Site zur Verfügung.

In der folgenden Tabelle werden die Begriffe beschrieben, die bei der Konfiguration der Notfallwiederherstellung in Citrix ADM verwendet werden.

Begriff	Beschreibung
Primärer Standort (Rechenzentrum A)	Am primären Standort sind Citrix ADM Knoten im Hochverfügbarkeitsmodus bereitgestellt.
Wiederherstellungsstandort (Rechenzentrum B)	Die Wiederherstellungs-Site verfügt über einen Disaster Recovery-Knoten, der im eigenständigen Modus bereitgestellt wird. Dieser Knoten befindet sich im schreibgeschützten Modus und ist erst betriebsbereit, wenn der primäre Standort ausgefallen ist.

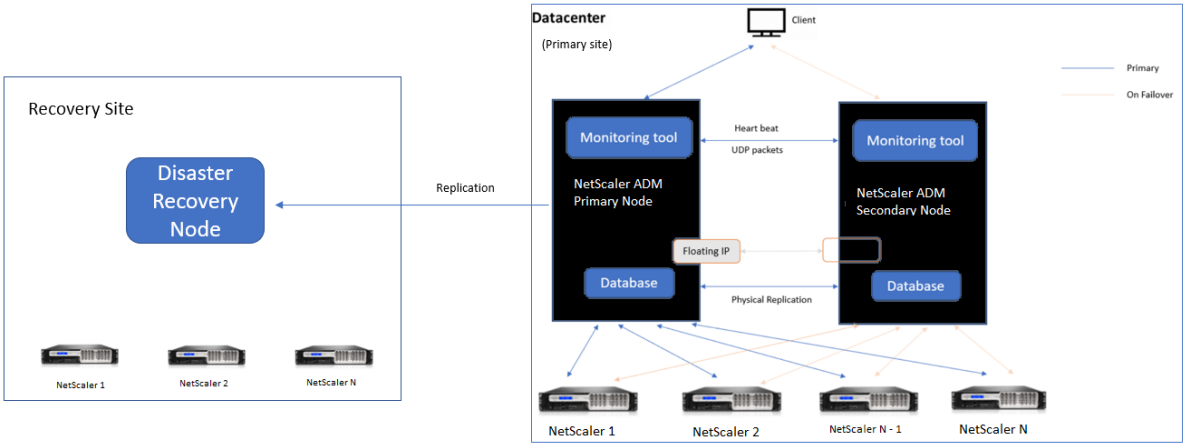
Begriff	Beschreibung
Knoten für die Notfallwiederherstellung	Der Wiederherstellungsknoten ist ein eigenständiger Knoten, der auf der Wiederherstellungs-Site bereitgestellt wird. Dieser Knoten wird betriebsbereit (zum neuen primären), falls eine Katastrophe am primären Standort auftritt und nicht funktionsfähig ist.

> Hinweis: Der primäre Standort und der DR-Standort kommunizieren über die Ports 5454 und 22 miteinander, und diese Ports sind standardmäßig aktiviert.
> Weitere Informationen zu Port- und Protokolldetails finden Sie unter Ports.

Disaster Recovery-Workflow

Die folgende Abbildung zeigt den Disaster Recovery-Workflow, die Ersteinrichtung vor der Katastrophe und den Arbeitsablauf nach der Katastrophe.

Ersteinrichtung vor dem Notfall



Das Bild zeigt das Setup für die Notfallwiederherstellung vor dem Notfall.

Der primäre Standort verfügt über NetScaler ADM Knoten, die im Hochverfügbarkeitsmodus bereitgestellt werden. Weitere Informationen finden Sie unter Hochverfügbarkeitsbereitstellung

Auf der Wiederherstellungs-Site ist ein eigenständiger NetScaler ADM Disaster Recovery-Knoten remote bereitgestellt. Der Disaster Recovery-Knoten befindet sich im schreibgeschützten Modus und empfängt Daten vom primären Knoten, um ein Datenbackup zu erstellen. Citrix ADC-Instanzen auf der Wiederherstellungs-Site werden ebenfalls erkannt, es fließt jedoch kein Datenverkehr durch

sie. Während des Backup-Vorgangs werden alle Daten, Dateien und Konfigurationen vom primären Knoten auf dem Disaster Recovery-Knoten repliziert.

Voraussetzungen

Bevor Sie den Disaster Recovery-Knoten einrichten, beachten Sie die folgenden Voraussetzungen:

- Um Disaster Recovery-Einstellungen zu aktivieren, müssen am primären Standort Citrix ADM Knoten im Hochverfügbarkeitsmodus konfiguriert sein.
- Die eigenständige Bereitstellung von Citrix ADM am primären Standort unterstützt die Disaster Recovery-Funktion nicht.
- Das Citrix ADM HA-Paar (am primären Standort) und der eigenständige Knoten (am DR-Standort) müssen dieselbe Softwareversion, denselben Build und dieselbe Konfiguration haben.

Citrix empfiehlt, dass Sie die CPU-Priorität (in den Eigenschaften der virtuellen Maschine) auf der höchsten Ebene festlegen, um das Planungsverhalten und die Netzwerklatenz zu verbessern.

In der folgenden Tabelle sind die Mindestanforderungen für die Konfiguration des Disaster Recovery-Knotens aufgeführt:

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8 CPUs
Stauraum	Citrix empfiehlt die Verwendung von Solid-State-Laufwerk-Technologie (SSD) für NetScaler ADM Bereitstellungen. Der Standardwert ist 120 GB. Die tatsächliche Speicheranforderung hängt von der Schätzung der NetScaler ADM Größe ab. Wenn Ihre NetScaler ADM Speicheranforderung 120 GB überschreitet, müssen Sie einen zusätzlichen Datenträger bereitstellen. **Hinweis:** Sie können nur eine weitere Festplatte hinzufügen. Citrix empfiehlt Ihnen, zum Zeitpunkt der Erstbereitstellung den Speicher zu schätzen und mehr Datenträger anzuhängen. Weitere Informationen finden Sie unter Bereitstellen eines zusätzlichen Datenträgers in NetScaler ADM.

Komponente	Voraussetzung
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s oder 100 Mbit/s
Hypervisor	**Versionen**
Citrix Hypervisor	6.2 und 6.5
VMware ESXi	5.5 und 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu und Fedora

Erstmaliger Disaster Recovery-Setup

- Bereitstellen von NetScaler ADM im Hochverfügbarkeitsmodus
- Bereitstellen und Registrieren des NetScaler ADM Notfallwiederherstellungsknotens
- Disaster Recovery-Einstellungen über die Benutzeroberfläche aktivieren und deaktivieren

Bereitstellen von NetScaler ADM im Hochverfügbarkeitsmodus

Um die Disaster Recovery-Einstellungen einzurichten, stellen Sie sicher, dass NetScaler ADM im Hochverfügbarkeitsmodus bereitgestellt wird. Informationen zur Bereitstellung von NetScaler ADM in Hochverfügbarkeit finden Sie unterHochverfügbarkeitsbereitstellung

> **Hinweis**
>
> - Citrix ADM, das im Hochverfügbarkeitsmodus bereitgestellt wird, muss auf Citrix ADM Release Version 13.0 aktualisiert werden.
> - Eine**schwebende IP-Adresse ist obligatorisch**, um Disaster Recovery-Knoten beim primären Knoten zu registrieren.

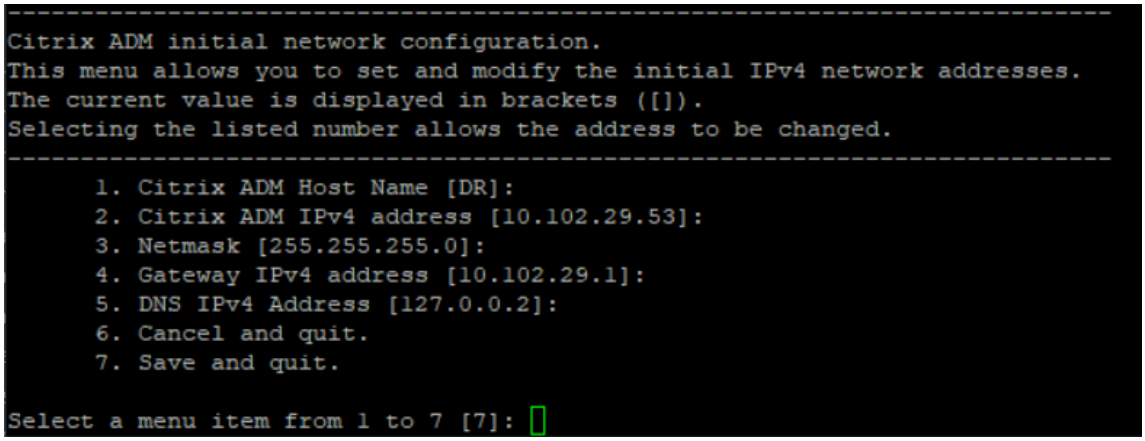
Bereitstellen und Registrieren des NetScaler ADM Notfallwiederherstellungsknotens über die DR-Konsole

So registrieren Sie den NetScaler ADM Notfallwiederherstellungsknoten:

1. Laden Sie die `.xva`-Imagedatei von der Citrix Download-Site herunter und importieren Sie sie in Ihren Hypervisor.

2. Konfigurieren Sie Citrix ADM auf der Registerkarte **Konsole** mit den anfänglichen Netzwerkkonfigurationen.

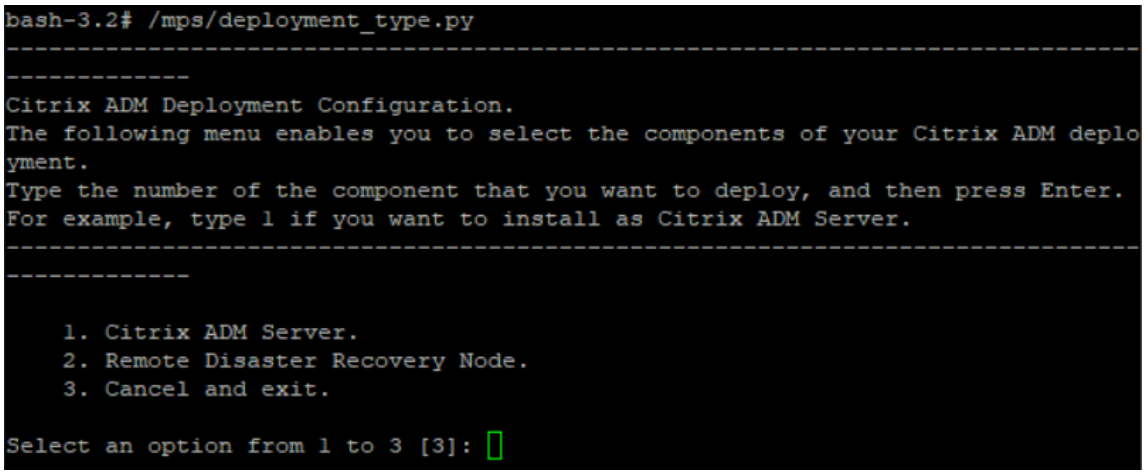
   > **Hinweis**
   >
   > Der Notfallwiederherstellungsknoten kann sich in einem anderen Subnetz befinden.



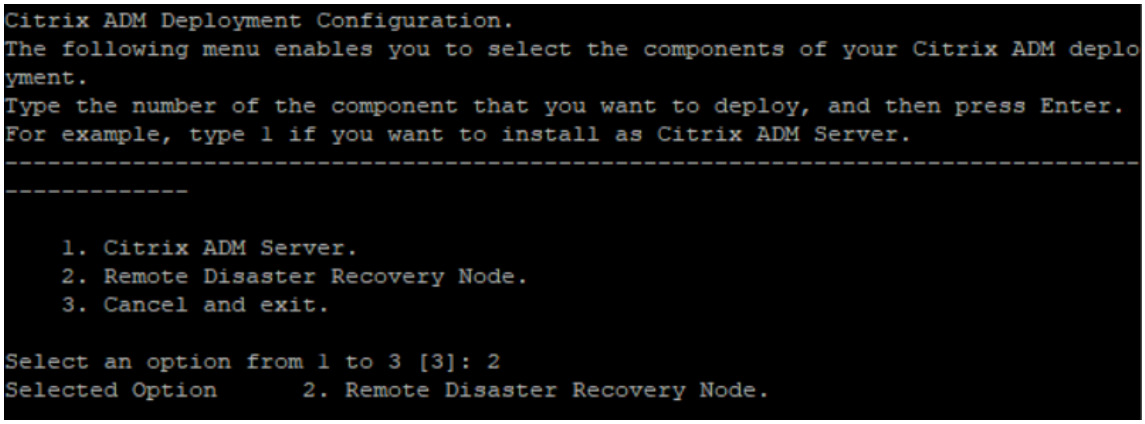
3. Nachdem die anfängliche Netzwerkkonfiguration abgeschlossen ist, fordert das System zur Anmeldung auf. Melden Sie sich mit den folgenden Anmeldeinformationen an —`nsrecover`/`nsroot`.

   > **Wichtig**
   >
   > Ändern Sie während der Registrierung nicht die Anmeldeinformationen des DR-Knotens (`nsrecover`/`nsroot`). Sie können die Anmeldeinformationen des DR-Knotens ändern, nachdem Sie den DR-Knoten erfolgreich registriert haben.

4. Um den Notfallwiederherstellungsknoten bereitzustellen, geben Sie **/mps/deployment_type.py** ein, und drücken Sie die Eingabetaste. Das Konfigurationsmenü für die Citrix ADM-Bereitstellung wird angezeigt.

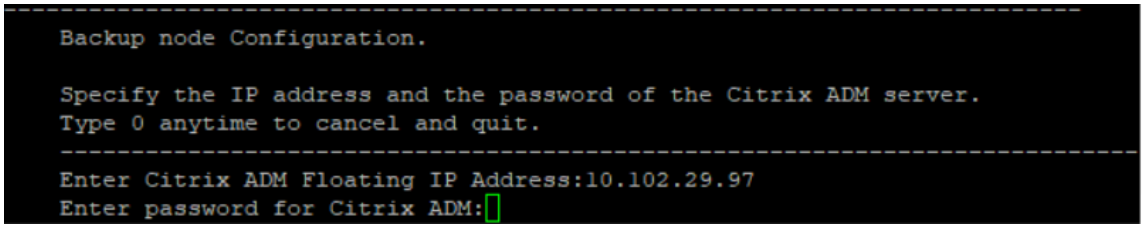


5. Wählen Sie **2** aus, um den Notfallwiederherstellungsknoten zu registrieren.

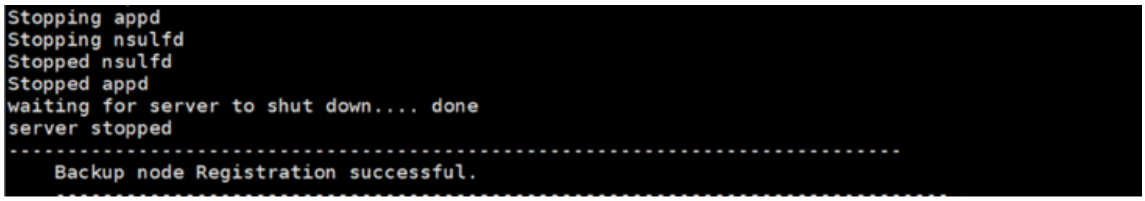


6. Die Konsole fordert zur Eingabe einer Floating-IP-Adresse des Hochverfügbarkeitsknotens und des Kennworts auf.

7. Geben Sie die schwebende IP-Adresse und das Kennwort ein, um den Disaster Recovery-Knoten beim primären Knoten zu registrieren.



Der Notfallwiederherstellungsknoten ist jetzt erfolgreich registriert.



> **Hinweis:**
>
> Der Disaster Recovery-Knoten verfügt über keine GUI.

8. Wenn Sie das Kennwort des DR-Knotens ändern möchten, führen Sie das folgende Skript aus:

```
/mps/change_freebsd_password.sh <username> <password>
<!--NeedCopy-->
```

Bereitstellen des Notfallwiederherstellungsknotens mit der NetScaler ADM GUI

Nachdem der Disaster Recovery-Knoten erfolgreich mit der DR-Konsole registriert wurde, stellen Sie den DR-Knoten über die Citrix ADM GUI bereit. Dieser Schritt aktiviert die Disaster Recovery-

Einstellungen vom primären Citrix ADM Standort.

1. Navigieren Sie zu **System > Systemverwaltung > Notfallwiederherstellungseinstellungen.**
2. Wählen Sie auf der Seite **Disaster Recovery** die Option **DR Node bereitstellen**aus.
3. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Ja**, um fortzufahren.

> **Hinweis**
>
> Die für das Systembackup benötigte Zeit hängt von der Datengröße und der Geschwindigkeit der WAN-Verbindung ab.

Nachdem Sie den DR-Knoten erfolgreich in der Citrix ADM GUI bereitgestellt haben, können Sie den Datenbankstatus, den Arbeitsspeicher, die CPU und die Festplattennutzung des DR-Knotens überwachen.

Um die Disaster Recovery-Einstellungen zu deaktivieren, wählen Sie**DR-Knoten entfernen**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf**Ja**, um fortzufahren.

Um den DR-Knoten erneut zu aktivieren, konfigurieren Sie den DR-Knoten für Ihr Hochverfügbarkeitspaar neu:

1. Melden Sie sich mit einem Hypervisor oder einer SSH-Konsole am DR-Knoten an.
2. Konfigurieren Sie den DR-Knoten, indem Sie das unter Deploy verfügbare Verfahren befolgen und den NetScaler ADM-Notfallwiederherstellungsknoten mithilfe der DR-Konsole registrieren.
3. Stellen Sie den Notfallwiederherstellungsknoten mit der NetScaler ADM GUIbereit.

Weitere Informationen finden Sie in den FAQs.

> **Wichtig!**
>
> - Es liegt in der Verantwortung des Administrators, festzustellen, dass eine Katastrophe am primären Standort aufgetreten ist.
> - Der Workflow zur Notfallwiederherstellung wird manuell vom Administrator initiiert, nachdem der primäre Standort ausfällt.
> - Ein Administrator muss den Prozess manuell initiieren, indem er ein Wiederherstellungsskript auf dem Disaster Recovery-Knoten am Recovery-Standort ausführt.
> - Wenn Sie das HA-Paar am primären Standort aktualisieren, müssen Sie auch manuell den eigenständigen Knoten am DR-Standort aktualisieren.

Workflow nach der Katastrophe

Wenn der primäre Standort nach einem Notfall ausfällt, muss der Disaster Recovery-Workflow wie folgt initiiert werden:

1. Der Administrator stellt fest, dass der primäre Standort von einer Katastrophe heimgesucht wurde und dieser nicht betriebsbereit ist.
2. Der Administrator leitet den Wiederherstellungsprozess ein.
3. Der Administrator muss basierend auf Ihren Anforderungen (an der Wiederherstellungs-Site) eines der folgenden Wiederherstellungsskripts manuell auf dem Disaster Recovery-Knoten ausführen:

   - Konfigurieren von SNMP, Syslog und Analytics auf dem DR-Knoten:

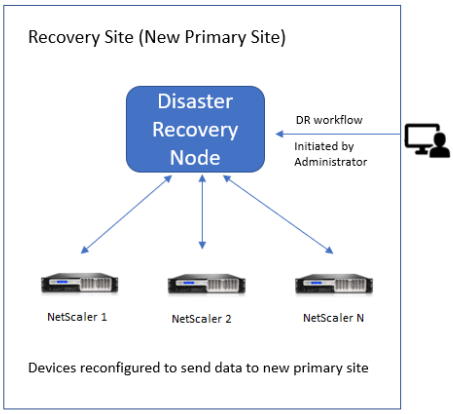
   ```
   /mps/scripts/pgsql/pgsql_restore_remote_backup.sh

   <!--NeedCopy-->
   ```

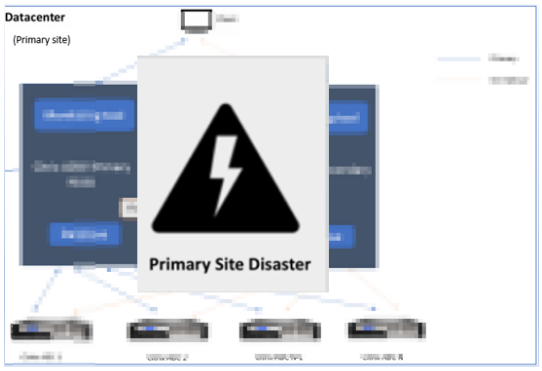
   - Konfigurieren Sie den DR-Knoten auch als Lizenzserver:

   ```
   /mps/scripts/pgsql/pgsql_restore_remote_backup.sh -reconfig-
       ls <IP-address-of-the-primary-site>

   <!--NeedCopy-->
   ```

4. Intern werden NetScaler ADC Instanzen automatisch neu konfiguriert, um die Daten an den Notfallwiederherstellungsknoten zu senden, der jetzt zum neuen primären Standort geworden ist.

   Die folgende Abbildung zeigt, dass der Disaster Recovery-Workflow nach dem primären Standort mit einem Notfall verbunden ist.





> Hinweis:
>
> Nachdem Sie das Skript auf der DR-Site initiiert haben, wird die DR-Site nun zur neuen primären Site. Sie können auch auf die DR-Benutzeroberfläche zugreifen.

Nachträgliche Notfallwiederherstellung

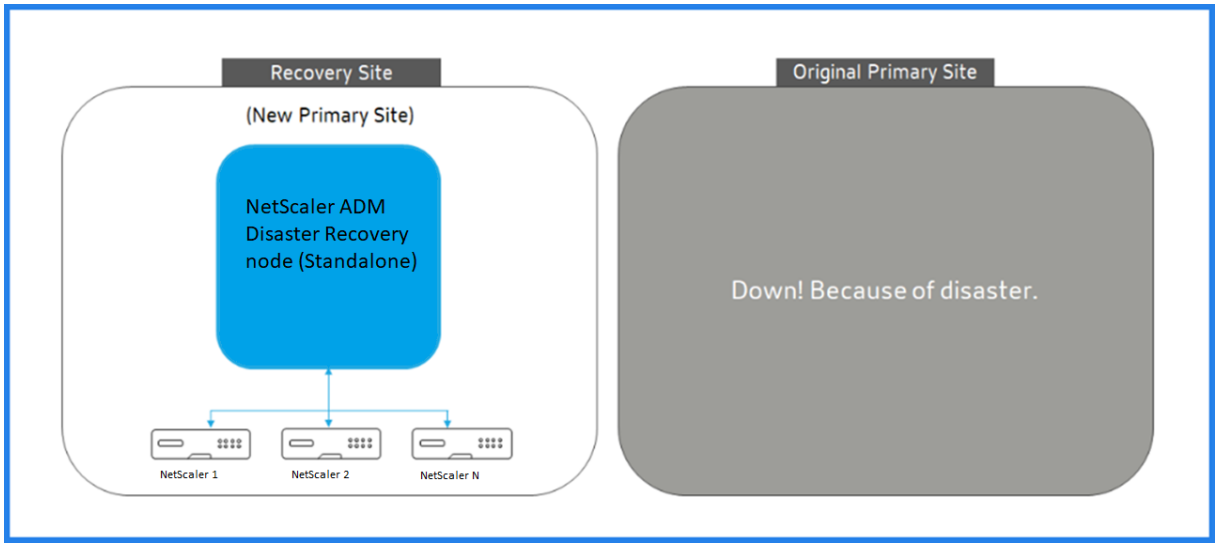
Nachdem der Notfall aufgetreten ist und der Administrator das Wiederherstellungsskript initiiert, wird der Notfallstandort nun zum neuen primären Standort.

Wenn Sie die Konfigurationen später auf den ursprünglichen Standort zurücksetzen möchten, lesen Sie Wiederherstellen von Konfigurationen auf den ursprünglichen primären Standort.

> **Wichtig!**
>
> - Wenn Sie Citrix ADM 12.1.49.x oder frühere Versionen installiert haben, erhalten Sie eine Übergangsfrist von 30 Tagen, um Citrix zu kontaktieren, um die ursprüngliche Lizenz auf dem Citrix ADM (am DR-Standort) erneut zu hosten.
> - Für Versionen 12.1.50.x oder höher wird die Citrix ADM-Lizenz automatisch mit der DR-Site synchronisiert (es ist nicht erforderlich, Citrix für die Lizenz zu kontaktieren).
> - Die gepoolte Lizenz für die DR-Site wird ab 12.1.50.x oder späteren Versionen unterstützt. Wenn Sie Poollizenzen für die Instanzen angewendet haben, konfigurieren Sie die Instanzen manuell am DR-Standort neu.

Wiederherstellen von Konfigurationen auf den ursprünglichen primären Standort

Nach einem Notfall wird der konfigurierte Disaster Recovery (DR) -Knoten zum neuen primären Standort, und der Client-Verkehr fließt über diesen Knoten.



Weitere Informationen finden Sie unter Workflow nach der Katastrophe.

Wenn der ursprüngliche primäre Standort frei von Notfällen ist und Sie sich entscheiden, alle Vorgänge auf den primären Standort zu verschieben, konfigurieren Sie den ursprünglichen primären Standort so, dass er mit den Konfigurationen des DR-Knotens übereinstimmt.

Bevor Sie beginnen, stellen Sie sicher, dass sowohl der primäre Standort als auch der DR-Standort aktiv sind.

Gehen Sie wie folgt vor, um die Änderungen vom DR-Standort auf den ursprünglichen primären Standort zurückzusetzen:

1. Melden Sie sich an der ursprünglichen primären Site an und führen Sie den folgenden Befehl aus:

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password> &
<!--NeedCopy-->
```

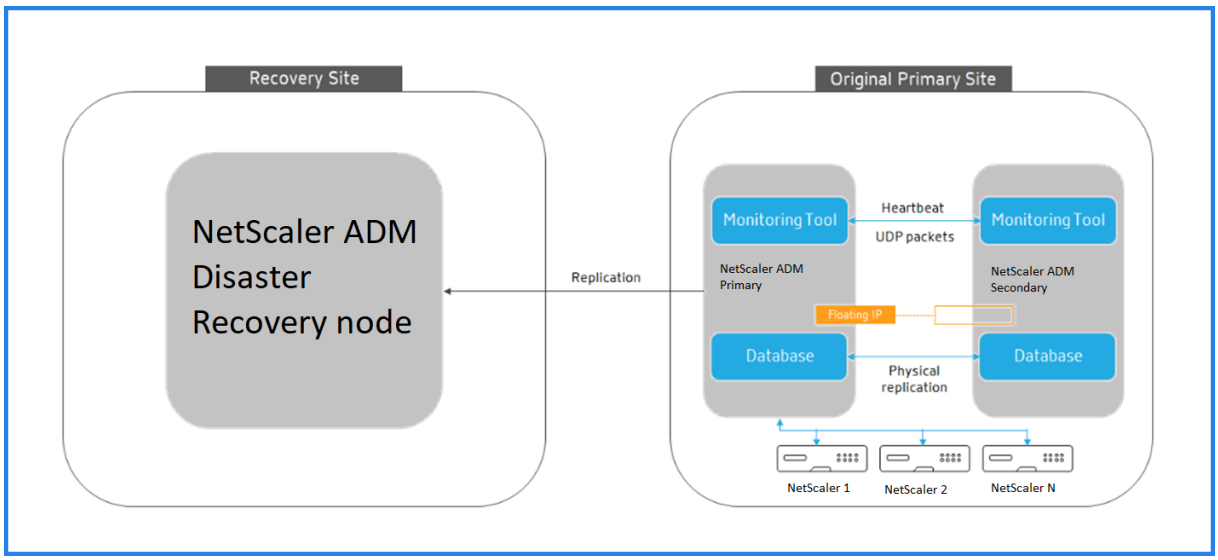
   Mit diesem Befehl werden nur Syslog, SNMP und Analytics für den primären Standort konfiguriert.

   Wenn Sie den primären Standort als gepoolten Lizenzserver für ADC-Instanzen konfigurieren möchten, führen Sie den folgenden Befehl aus:

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password>  -O yes &
<!--NeedCopy-->
```

   Der `-O` Befehl ruft die IP-Adresse der DR-Site ab und konfiguriert den primären Standort als gepoolten Lizenzserver neu.

2. Konfigurieren Sie den DR-Standort neu. Siehe Disaster Recovery-Setup bereitstellen.



Nachdem Sie die Konfigurationen vom DR-Standort auf den ursprünglichen primären Standort zurückgesetzt haben, fließt der Clientverkehr über den primären NetScaler ADM Knoten.

On-Prem-Agents für die Bereitstellung mehrerer Standorte konfigurieren

February 5, 2024

In früheren Versionen von NetScaler ADM können NetScaler ADC-Instanzen, die in Remote-Rechenzentren bereitgestellt werden, von NetScaler ADM verwaltet und überwacht werden, die in einem primären Rechenzentrum ausgeführt werden. NetScaler ADC-Instanzen sendeten Daten direkt an den primären NetScaler ADM, was zu einem Verbrauch der WAN-Bandbreite führte. Außerdem werden bei der Verarbeitung von Analysedaten CPU- und Speicherressourcen des primären NetScaler ADM verwendet.

Sie können Rechenzentren auf der ganzen Welt haben. Agenten spielen in den folgenden Szenarien eine wichtige Rolle:

- Installation von Agenten in Remote-Rechenzentren, sodass der WAN-Bandbreitenverbrauch reduziert wird.
- Um die Anzahl der Instanzen zu begrenzen, die Datenverkehr zur Datenverarbeitung direkt an das primäre NetScaler ADM senden.

> **Hinweis**
>
> - Die Installation von Agenten für Instanzen im Remote-Rechenzentrum wird empfohlen, aber nicht zwingend erforderlich. Bei Bedarf können Benutzer NetScaler ADC-Instanzen direkt zum primären NetScaler ADM hinzufügen.
> - Wenn Sie Agents für ein oder mehrere Remote-Rechenzentren installiert haben, erfolgt die Kommunikation zwischen den Agenten und dem primären Standort über eine schwebende IP-Adresse. Weitere Informationen finden Sie unter Port.
> - Sie können Agents installieren und gepoolte Lizenzen auf die Instanzen in einem oder mehreren Remote-Rechenzentren anwenden. In diesem Szenario erfolgt die Kommunikation zwischen dem primären Standort und einem oder mehreren Remote-Rechenzentren über die Floating-IP.

Ab NetScaler ADM 12.1 oder höher können Instanzen mit Agenten für die Kommunikation mit dem primären NetScaler ADM in einem anderen Rechenzentrum konfiguriert werden.

Agents arbeiten als Vermittler zwischen dem primären NetScaler ADM und den erkannten Instanzen in verschiedenen Rechenzentren. Die Installation von Agenten bietet folgende Vorteile:

- Die Instanzen sind für Agenten so konfiguriert, dass die unverarbeiteten Daten direkt an Agenten anstatt an das primäre NetScaler ADM gesendet werden. Agenten führen die erste Ebene

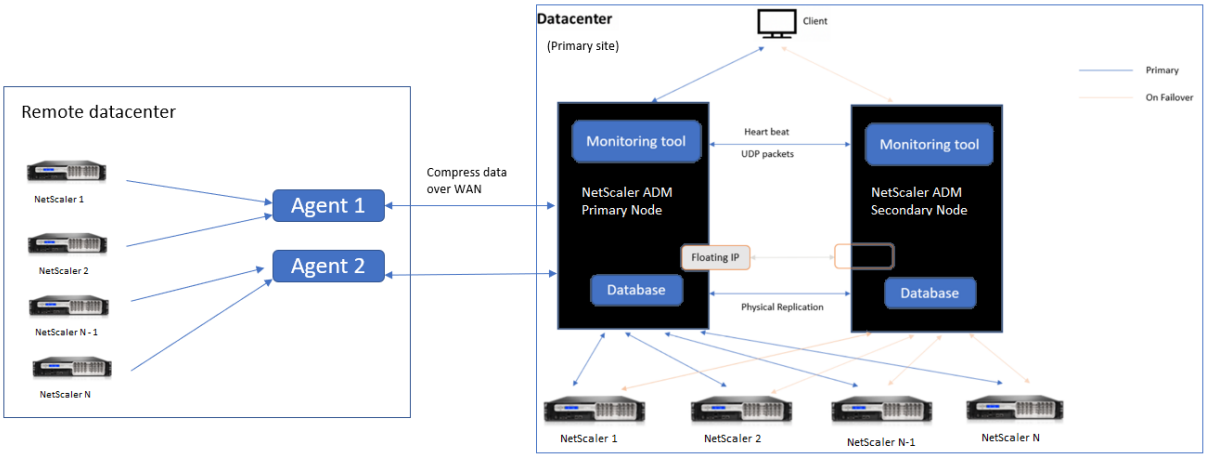
der Datenverarbeitung durch und senden die verarbeiteten Daten in komprimiertem Format zur Speicherung an das primäre NetScaler ADM.

- Agenten und Instanzen befinden sich im selben Rechenzentrum, sodass die Datenverarbeitung schneller erfolgt.
- Das Clustering der Agents ermöglicht die Neuverteilung von NetScaler ADC-Instanzen beim Agent-Failover. Wenn ein Agent in einer Site ausfällt, wird der Datenverkehr von NetScaler ADC-Instanzen auf einen anderen verfügbaren Agenten an derselben Site umgeschaltet.

> **Hinweis**
>
> Die Anzahl der Agenten, die pro Standort installiert werden sollen, hängt vom verarbeiteten Datenverkehr ab.

Architektur

Die folgende Abbildung zeigt NetScaler ADC-Instanzen in zwei Rechenzentren und NetScaler ADM Hochverfügbarkeitsbereitstellung mit Agent-basierter Architektur an mehreren Standorten.



Auf dem primären Standort sind die NetScaler ADM Knoten in einer Hochverfügbarkeitskonfiguration bereitgestellt. Die NetScaler ADC-Instanzen auf der primären Site sind direkt beim NetScaler ADM registriert.

Am sekundären Standort werden Agenten bereitgestellt und beim NetScaler ADM-Server am primären Standort registriert. Diese Agenten arbeiten in einem Cluster, um den kontinuierlichen Verkehrsfluss zu bewältigen, falls ein Agenten-Failover auftritt. Die NetScaler ADC-Instanzen am sekundären Standort werden über Agenten innerhalb dieser Site beim primären NetScaler ADM-Server registriert. Die Instanzen senden Daten direkt an Agenten statt an primäres NetScaler ADM. Die Agenten verarbeiten die von den Instanzen empfangenen Daten und senden sie in einem komprimierten Format an das primäre NetScaler ADM. Agenten kommunizieren mit dem NetScaler ADM-Server über einen sicheren

Kanal, und die über den Kanal gesendeten Daten werden aus Gründen der Bandbreiteneffizienz komprimiert.

Erste Schritte

- Installieren des Agenten in einem Rechenzentrum
  - Registrieren Sie den Agenten
  - Den Agenten an eine Site anhängen
- Hinzufügen NetScaler ADC-Instanzen
  - Neue Instanz hinzufügen
  - Eine bestehende Instanz aktualisieren

Installieren des Agenten in einem Rechenzentrum

Sie können den Agenten installieren und konfigurieren, um die Kommunikation zwischen dem primären NetScaler ADM und den verwalteten NetScaler ADC-Instanzen in einem anderen Rechenzentrum zu ermöglichen.

Sie können einen Agent auf den folgenden Hypervisoren in Ihrem Unternehmensrechenzentrum installieren:

- Citrix Hypervisor
- VMware ESXi
- Microsoft Hyper-V
- Linux KVM-Server

> **Hinweis**
>
> On-Prem-Agenten für die Multisite-Bereitstellung werden nur mit der NetScaler ADM-Hochverfügbarkeitsbereitstellung unterstützt.

Bevor Sie mit der Installation des Agenten beginnen, stellen Sie sicher, dass Sie über die erforderlichen virtuellen Computerressourcen verfügen, die der Hypervisor für jeden Agenten bereitstellen muss.

Komponente	Voraussetzung
RAM	32 GB

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

Ports

Für Kommunikationszwecke müssen die folgenden Ports zwischen dem Agenten und dem lokalen NetScaler ADM-Server geöffnet sein.

Typ	Port	Details	Richtung der Kommunikation
TCP	8443, 7443, 443	Für ausgehende und eingehende Kommunikation zwischen Agent und NetScaler ADM On-Prem-Server.	NetScaler ADM Agent an NetScaler ADM

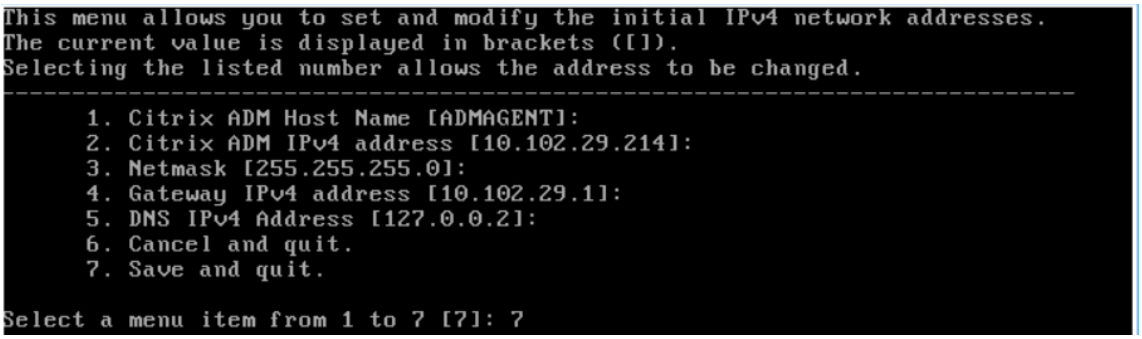
Die folgenden Ports müssen zwischen dem Agent und den NetScaler ADC-Instanzen geöffnet sein.

Typ	Port	Details	Richtung der Kommunikation
TCP	80	Für die NITRO -Kommunikation zwischen Agent und NetScaler ADC - oder Citrix SD-WAN Instanz.	NetScaler ADM an NetScaler ADC und NetScaler ADC an NetScaler ADM
TCP	22	Für die SSH-Kommunikation zwischen Agent und NetScaler ADC oder Citrix SD-WAN-Instanz. Für die Synchronisierung zwischen NetScaler ADM-Servern, die im Hochverfügbarkeitsmodus bereitgestellt werden.	NetScaler ADM an NetScaler ADC und NetScaler ADM Agent an NetScaler ADC
UDP	4739	Für die AppFlow Kommunikation zwischen Agent und NetScaler ADC - oder Citrix SD-WAN Instanz.	NetScaler ADC oder Citrix SD-WAN an NetScaler ADM
ICMP	No reserved port	To detect network reachability between NetScaler ADM and NetScaler ADC instances, SD WAN instances, or the secondary NetScaler ADM server deployed in high availability mode.
UDP	161, 162	To receive SNMP events from NetScaler ADC instance to agent.	Port 161 - NetScaler ADM to NetScaler ADC
			Port 162 - NetScaler ADC to NetScaler ADM

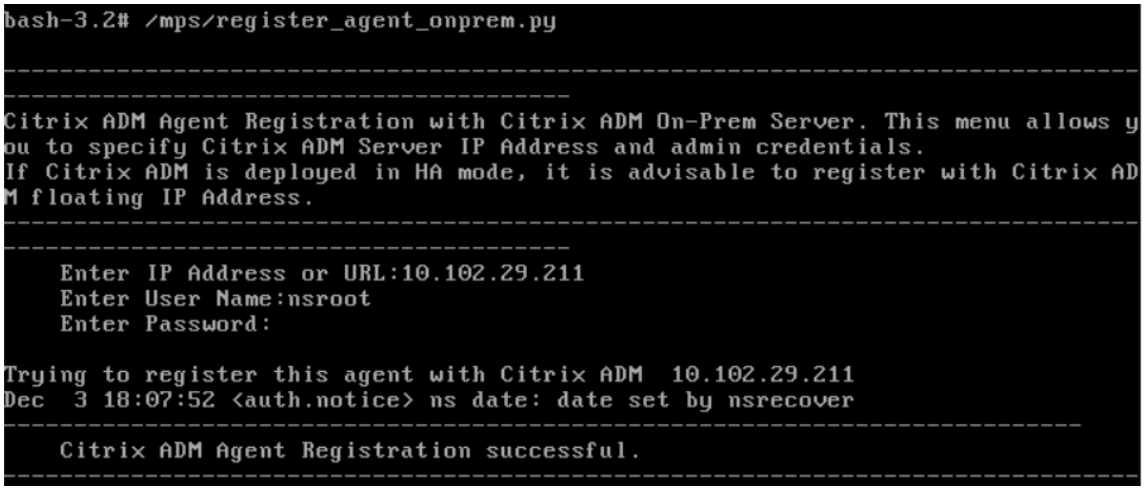
| UDP | 514 | To receive syslog messages from NetScaler ADC or Citrix SD-WAN instance to agent. |NetScaler ADC or Citrix SD-WAN to NetScaler ADM|
| TCP | 5557 | For Logstream communication between agent and NetScaler ADC instances. |NetScaler ADC to NetScaler ADM|

Registrieren Sie den Agenten

1. Verwenden Sie die Agentimagedatei, die von der Citrix-Downloadsite heruntergeladen wurde, und importieren Sie sie in Ihren Hypervisor. Das Benennungsmuster der Agent-Image-Datei lautet wie folgt: **MASAGENT-<HYPERVISOR>-<Version.no>.** Beispiel: **MASAGENT-XEN-13.0-xy.xva**
2. Konfigurieren Sie Citrix ADM auf der Registerkarte **Konsole** mit den anfänglichen Netzwerkkonfigurationen.
3. Geben Sie den NetScaler ADM-Hostnamen, die IPv4-Adresse und die Gateway-IPv4-Adresse ein. Wählen Sie Option 7, um die Konfiguration zu speichern und zu beenden.



4. Nach erfolgreicher Registrierung wird die Konsole aufgefordert, sich anzumelden. Verwenden Sie *nsrecover/nsroot* als Anmeldeinformationen.
5. Um den Agenten zu registrieren, geben Sie**/mps/register_agent_onprem.py** ein. Die Anmeldeinformationen für die NetScaler ADM Agentenregistrierung werden wie in der folgenden Abbildung gezeigt angezeigt.
6. Geben Sie die schwebende NetScaler ADM IP-Adresse und die Anmeldeinformationen des Benutzers ein.



Nachdem die Registrierung erfolgreich ist, wird der Agent neu gestartet, um den Installationsvorgang abzuschließen.

Greifen Sie nach dem Neustart des Agenten auf die NetScaler ADM-GUI zu. Gehen Sie im Hauptmenü auf die Seite **Netzwerke > Agenten**, um den Status des Agenten zu überprüfen.Der neu hinzugefügte Agent wird im Status **Up** angezeigt.

> **Hinweis**
>
> Das NetScaler ADM zeigt die Version des Agenten an und prüft außerdem, ob der Agent auf der neuesten Version ist. Das Download-Symbol bedeutet, dass der Agent nicht auf der neuesten Version ist und aktualisiert werden muss. Citrix empfiehlt, dass Sie die Agent-Version auf die NetScaler ADM Version aktualisieren.

Agent an eine Site anhängen

1. Wählen Sie den Agenten aus und klicken Sie auf **Site anhängen.**
2. Wählen Sie auf der Seite**Website anhängen** eine Website aus der Liste aus oder erstellen Sie eine Site mit der Plusschaltfläche (+).
3. Klicken Sie auf **Speichern**.

> **Hinweis**
>
> - Standardmäßig werden alle neu registrierten Agenten zum Standardrechenzentrum hinzugefügt.
> - Es ist wichtig, den Agent mit der richtigen Site zu verknüpfen. Im Falle eines Agentfehlers werden die ihm zugewiesenen NetScaler ADC-Instanzen automatisch auf andere funktionsfähige Agents am selben Standort umgestellt.

Agent-Aktionen

Sie können verschiedene Aktionen auf einen Agenten unter **Netzwerke > Agenten > Aktionen auswählen**anwenden.

Unter **Aktion auswählen**können Sie die folgenden Funktionen verwenden:

Installieren Sie ein neues Zertifikat: Wenn Sie ein anderes Agentzertifikat benötigen, um Ihre Sicherheitsanforderungen zu erfüllen, können Sie eines hinzufügen.

Ändern Sie das Standardkennwort: Um die Sicherheit Ihrer Infrastruktur zu gewährleisten, ändern Sie das Standardkennwort eines Agenten.

Generieren Sie eine Datei für den technischen Support: Generieren Sie eine Datei für den technischen Support für einen ausgewählten NetScaler ADM Agent. Sie können diese Datei herunterladen und an den technischen Support von Citrix zur Untersuchung und Fehlerbehebung senden.

Hinzufügen NetScaler ADC-Instanzen

Instanzen sind Citrix Appliances oder virtuelle Appliances, die Sie von NetScaler ADM aus über Agenten erkennen, verwalten und überwachen möchten. Sie können die folgenden Citrix Appliances und virtuellen Appliances zu NetScaler ADM oder Agents hinzufügen:

- NetScaler ADC MPX
- NetScaler ADC VPX
- NetScaler ADC SDX
- NetScaler ADC CPX
- Citrix Gateway
- Citrix SSL-Forward-Proxy
- Citrix SD-WAN WO

Weitere Informationen finden Sie unter Instanzen zu NetScaler ADM hinzufügen.

Eine vorhandene Instanz an den Agenten anhängen

Wenn eine Instanz bereits zum primären NetScaler ADM hinzugefügt wurde, können Sie sie an einen Agenten anhängen, indem Sie einen Agenten bearbeiten.

1. Navigieren Sie zu **Netzwerke > Instanzen**, und wählen Sie den Instanztyp aus. Beispiel: NetScaler ADC.
2. Klicken Sie auf **Bearbeiten**, um eine vorhandene Instanz zu bearbeiten.

3. Klicken Sie, um den Agent auszuwählen.
4. Wählen Sie auf der Seite **Agent** den Agenten aus, dem Sie die Instanz zuordnen möchten, und klicken Sie dann auf **OK**.

> **Hinweis**
>
> Stellen Sie sicher, dass Sie die **Site** auswählen, mit der Sie die Instanz verknüpfen möchten.

Greifen Sie auf die GUI einer Instanz zu, um Ereignisse zu validieren

Nachdem die Instanzen hinzugefügt und der Agent konfiguriert wurde, greifen Sie auf die GUI einer Instanz zu, um zu überprüfen, ob das Trapziel konfiguriert ist.

Navigieren Sie in NetScaler ADM zu**Netzwerke > Instanzen**. Wählen Sie unter**Instanzen**den Instanztyp aus, auf den Sie zugreifen möchten (z. B. NetScaler ADC VPX), und klicken Sie dann auf die IP-Adresse einer bestimmten Instanz.

Die GUI der ausgewählten Instanz wird in einem Popupfenster angezeigt.

Standardmäßig ist der Agent als Trapziel auf der Instanz konfiguriert. Melden Sie sich zur Bestätigung an der GUI der Instanz an und überprüfen Sie die Trapziele.

> **Wichtig!**
>
> Das Hinzufügen eines Agenten für NetScaler ADC-Instanzen in Remoterechenzentren wird empfohlen, ist aber nicht obligatorisch.
>
> Wenn Sie die Instanz direkt zum primären MAS hinzufügen möchten, wählen Sie beim Hinzufügen von Instanzen keinen **Agent** aus.

NetScaler ADM Agenten-Failover

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

> **Wichtig!**
>
> - Stellen Sie sicher, dass die **Agent-Failover-Funktion** für Ihr Konto aktiviert ist. Informationen zum Aktivieren dieser Funktion finden Sie unter ADM-Funktionen aktivieren oder deaktivieren.
> - Wenn ein Agent ein Skript ausführt, stellen Sie sicher, dass das Skript auf allen Agents in der Site vorhanden ist. Daher kann der geänderte Agent das Skript nach dem Agent-Failover ausführen.

Informationen zum Anhängen einer Site an einen Agenten in der ADM-GUI finden Sie unter Anhängen eines Agenten an eine Site.

Um ein Agent-Failover zu erzielen, wählen Sie NetScaler ADM -Agents nacheinander aus, und fügen Sie sie an dieselbe Site an.

Beispielsweise sind zwei Agenten 10.106.1xx.2x und 10.106.1xx.3x am Standort Bangalore angeschlossen und betriebsbereit. Wenn ein Agent inaktiv wird, erkennt NetScaler ADM ihn und zeigt den Status als heruntergefahren an.

Wenn ein NetScaler ADM Agent in einer Site inaktiv wird (Status Heruntergefahren), wartet NetScaler ADM fünf Minuten darauf, dass der Agent aktiv wird (Status Up). Wenn der Agent inaktiv bleibt, verteilt NetScaler ADM die Instanzen automatisch auf die verfügbaren Agents an derselben Site neu.

NetScaler ADM löst die Instanzumverteilung alle 30 Minuten aus, um die Last zwischen den aktiven Agent in der Site auszugleichen.

Installieren Sie einen ADM-Agenten als Microservice in einem Kubernetes-Cluster

February 5, 2024

Die Bereitstellung eines NetScaler ADM-Agenten als Microservice ist nützlich für die Verwaltung Ihres NetScaler ADC CPX. Die in diesem Dokument verfügbaren Verfahren sind nur anwendbar, wenn der NetScaler ADM und der Kubernetes-Cluster in einem anderen Netzwerk konfiguriert sind. In diesem Szenario können Sie einen ADM-Agenten als Microservice konfigurieren, in dem der Kubernetes-Cluster gehostet wird.

> Hinweis
>
> Sie können auch einen On-Premises-Agent konfigurieren und den Agenten im Netzwerk registrieren, in dem der Kubernetes-Cluster gehostet wird.

Erste Schritte

1. Navigieren Sie in NetScaler ADM zu **Netzwerke > Agenten**.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Download Agent Microservice** aus.
3. Geben Sie auf der Seite **Download Agent Microservice** die folgenden Parameter an:

    a) **Anwendungs-ID** —Eine String-ID, mit der der Dienst für den Agent im Kubernetes-Cluster definiert und dieser Agent von anderen Agents im selben Cluster unterschieden wird.

b) **Kennwort** —Geben Sie ein Kennwort an, mit dem CPX dieses Kennwort verwendet, um CPX über den Agenten in ADM einzubringen.

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

> Hinweis
>
> Sie dürfen das Standardkennwort (`nsroot`) nicht verwenden.

d) Klicken Sie auf **Yaml-Datei herunterladen**.

NetScaler ADM Agent im Kubernetes-Cluster installieren

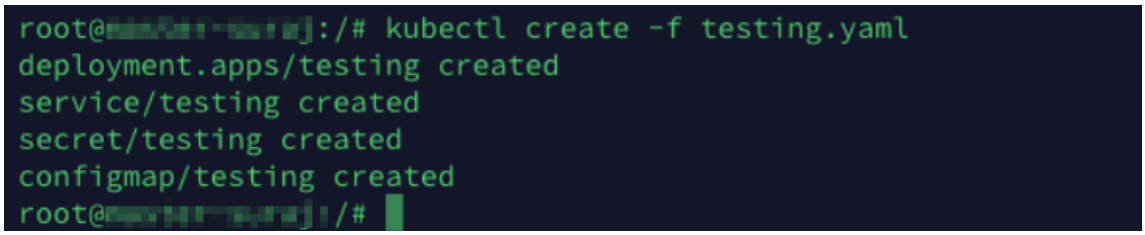
Im Hauptknoten von Kubernetes:

1. Speichern Sie die heruntergeladene YAML-Datei
2. Führen Sie den folgenden Befehl aus:

   `kubectl create -f <yaml file>`

   Beispiel: `kubectl create -f testing.yaml`

   Der Agent wurde erfolgreich erstellt.



Navigieren Sie in Citrix ADM zu **Netzwerke** > **Agents**, um den Agentenstatus anzuzeigen.

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

NetScaler ADM-Bereitstellung mit einem Server auf eine Bereitstellung mit hoher Verfügbarkeit migrieren

February 5, 2024

Sie können Ihren Citrix ADM Einzelserver auf eine Hochverfügbarkeitsbereitstellung von zwei Citrix ADM Servern aktualisieren. Ein Paar von Citrix ADM Servern mit hoher Verfügbarkeit befindet sich im Aktiv-Passiv-Modus, und beide Server haben dieselbe Konfiguration. Bei dieser Art der aktiv-passiven

Bereitstellung wird ein Citrix ADM Server als primärer Knoten und der andere als sekundärer Knoten konfiguriert. Wenn der primäre Knoten aus irgendeinem Grund ausfällt, übernimmt der sekundäre Knoten die Arbeit.

Um einen Citrix ADM Einzelserver zu einem Hochverfügbarkeitspaar zu migrieren, müssen Sie einen neuen Citrix ADM Serverknoten bereitstellen, ihn als zweiten Citrix ADM Einzelserver konfigurieren und beide Citrix ADM Server als Hochverfügbarkeitspaar bereitstellen.

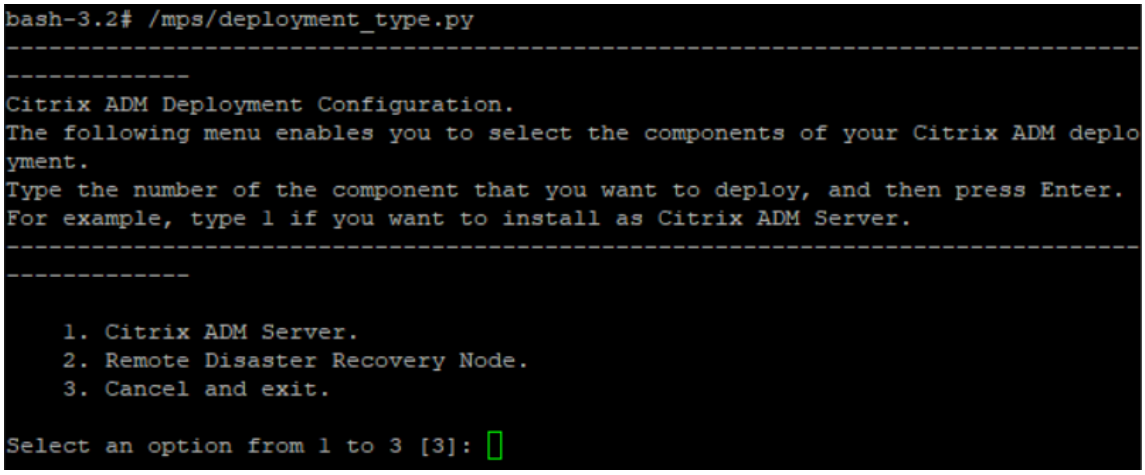
Die Migration eines Citrix ADM Einzelservers in einen Hochverfügbarkeitsmodus umfasst die folgenden Schritte:

1. Änderung des vorhandenen Serverknotens
2. Provisioning des zweiten Serverknotens
3. Bereitstellung der beiden Knoten im HA-Modus
4. Konfiguration des Hochverfügbarkeitspaars

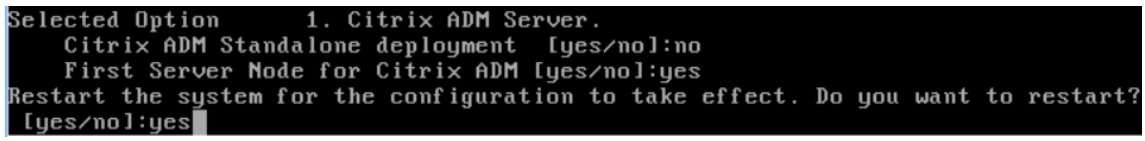
Ändern Sie den vorhandenen Citrix ADM Serverknoten

Um das Citrix ADM vom Einzelserver in den Hochverfügbarkeitsmodus zu migrieren, müssen Sie den anfänglichen Bereitstellungstyp des Serverknotens in den Hochverfügbarkeitsmodus ändern.

1. Öffnen Sie auf einer Workstation oder einem Laptop die Konsole des vorhandenen Citrix ADM Serverknotens. Stellen Sie sich beispielsweise vor, dass Sie ein Citrix ADM mit der IP-Adresse 10.106.171.17 als eigenständigen Server bereitgestellt haben.
2. Melden Sie sich bei Citrix ADM an. Die Standardanmeldeinformationen sind `nsroot` und `nsroot`.
3. Geben Sie in der Shell-Eingabeaufforderung ein `/mps/deployment_type.py`, und **drücken Sie die EIN**
4. Wählen Sie den Bereitstellungstyp als Citrix ADM Serveraus. Wenn Sie keine Option auswählen, wird diese standardmäßig als Server bereitgestellt.



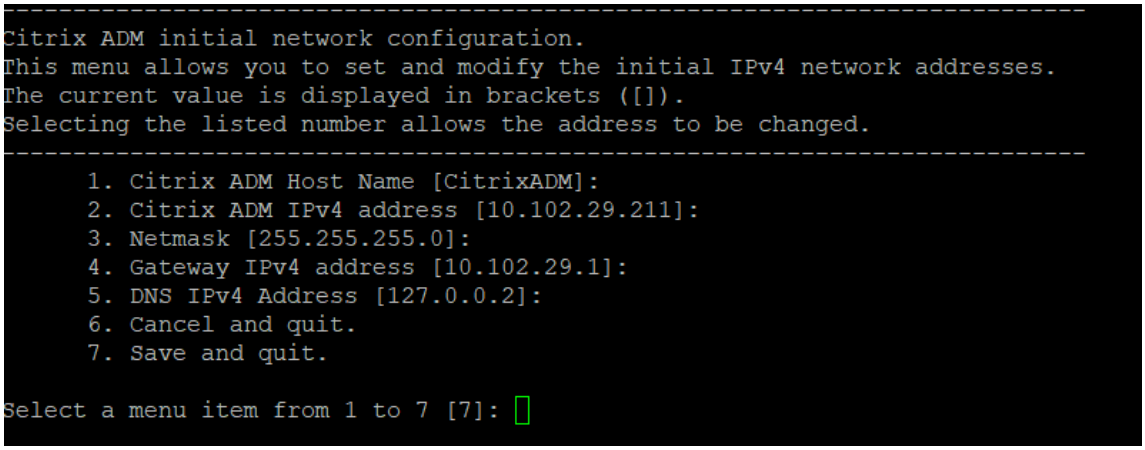
5. Die Bereitstellungskonsole fordert Sie auf, die Serverbereitstellung auszuwählen (als eigenständig). Geben Sie **Nein** ein, um die Bereitstellung als Hochverfügbarkeitspaar zu bestätigen.
6. Die Konsole fordert Sie auf, den (ersten Serverknoten) auszuwählen. Geben Sie **Ja** ein, um den Knoten als ersten Serverknoten zu bestätigen.
7. Die Konsole fordert Sie auf, den Server neu zu starten.
8. Geben Sie **Ja ein,** um den Neustart zu starten.



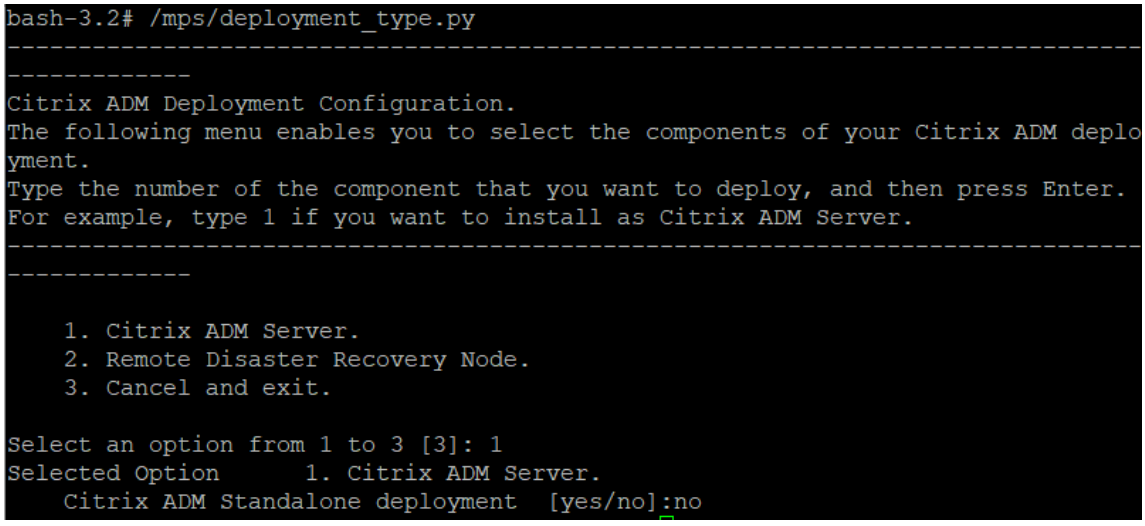
Bereitstellen des zweiten Serverknotens

Sie müssen den zweiten Server auf Ihrem Hypervisor bereitstellen. Verwenden Sie dieselbe Imagedatei, mit der Sie den ersten Server installiert haben, oder beziehen Sie eine Imagedatei derselben Version von der Citrix Download-Site.

1. Importieren Sie die Imagedatei in Ihren Hypervisor, und konfigurieren Sie dann über die Registerkarte Konsole die anfänglichen Netzwerkkonfigurationsoptionen, wie auf dem folgenden Bildschirm erläutert:



2. Nachdem Sie die erforderlichen IP-Adressen angegeben haben, geben Sie in der Shell-Eingabeaufforderung /mps/deployment_type.py ein, und drücken Sie die Eingabetaste.
3. Wählen Sie den Bereitstellungstyp als **Citrix ADM Server**aus.
4. Die Bereitstellungskonsole fordert Sie auf, die Serverbereitstellung auszuwählen (als eigenständig). Geben Sie **Nein** ein, um die Bereitstellung als Hochverfügbarkeitspaar zu bestätigen.



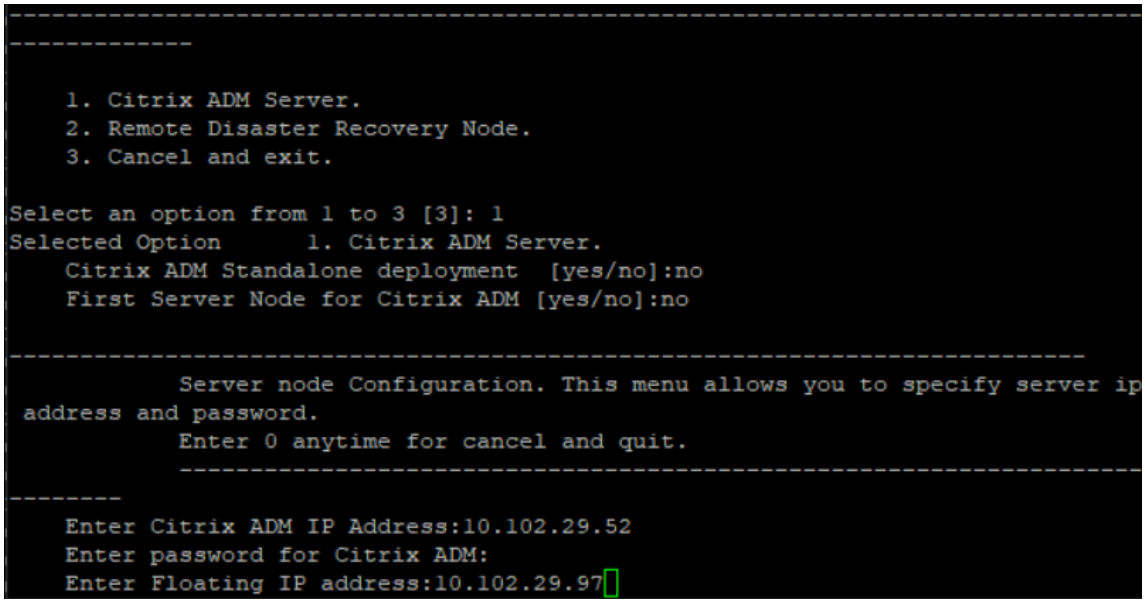
5. Die Konsole fordert Sie dann auf, den (ersten Serverknoten) auszuwählen. Geben Sie **Nein** ein, um den Knoten als zweiten Serverknoten zu bestätigen.


```
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:no
```

6. Geben Sie die IP-Adresse und das Kennwort des ersten Servers ein.

```
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:no

------------------------------------------------------------------------------
           Server node Configuration. This menu allows you to specify server ip
 address and password.
           Enter 0 anytime for cancel and quit.
           ------------------------------------------------------------------
--------
    Enter Citrix ADM IP Address:10.102.29.52
    Enter password for Citrix ADM:
```

7. Geben Sie die Floating-IP-Adresse des ersten Knotens ein.



8. Die Konsole fordert Sie auf, das System neu zu starten. Geben Sie **Ja** ein, um neu zu starten.

Stellen Sie die beiden Server in einem Hochverfügbarkeitsmodus bereit

Um den Installationsvorgang der beiden Serverknoten als Hochverfügbarkeitspaar abzuschließen, müssen Sie diese Knoten über die GUI des zuvor vorhandenen Citrix ADM Serverknotens bereitstellen. Die interne Kommunikation zwischen den beiden Servern wird gestartet, wenn Sie die beiden Serverknoten bereitstellen.

> **Wichtig**
>
> Bevor Sie Knoten mit hoher Verfügbarkeit bereitstellen, müssen Sie das Standardkennwort ändern.

1. Geben Sie in einem Webbrowser die IP-Adresse des zuvor vorhandenen NetScaler ADM -Serverknotens ein.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte **System** zu **Bereitstellung**, und klicken Sie auf **Bereitstellen**.
4. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **Ja**.

> **Hinweis**
>
> Nachdem Sie Citrix ADM in hoher Verfügbarkeit bereitgestellt haben, können Sie entweder

> auf den primären Knoten oder auf die Floating-IP zugreifen. Sie können nicht auf den sekundären Knoten ab Version 12.1 zugreifen.

5. Obwohl Sie die Floating-IP bei der Konfiguration des zweiten Serverknotens eingegeben haben, haben Sie die Möglichkeit, die FIP auf der **Systemseite** zu aktualisieren. Klicken Sie auf **HA-Einstellungen** > **Floating-IP-Adresse für den Hochverfügbarkeitsmodus konfigurieren**. Sie können die Floating-IP anzeigen, die Sie zuvor konfiguriert haben. Sie können eine neue IP-Adresse eingeben und auf **OK**klicken.

NetScaler Insight Center zu NetScaler ADM migrieren

February 5, 2024

Sie können jetzt Ihre NetScaler Insight Center er-Bereitstellung zu NetScaler ADM migrieren, ohne dass die vorhandene Konfiguration, Einstellungen oder Daten verloren gehen. Mit Citrix ADM können Sie nicht nur die verschiedenen Analysen anzeigen, die von den einer Anwendung zugeordneten Citrix ADC Instanzen generiert werden, sondern auch die gesamte globale Anwendungsbereitstellungsinfrastruktur über eine einzige einheitliche Konsole verwalten, überwachen und beheben.

> **Hinweis**
>
> Die Migration wird derzeit nur auf NetScaler Insight Center Standalone-Instances unterstützt.

Voraussetzungen

Stellen Sie vor der Migration der virtuellen NetScaler Insight Center er-Appliance zu Citrix ADM sicher, dass die folgenden Anforderungen erfüllt sind:

- NetScaler Insight Center 11.1 Build 47.14 oder höher ist installiert.
- Sie haben die NetScaler ADM 12.0 Build 57.24 .tgz-Imagedatei heruntergeladen.

  > **Hinweis:**
  >
  > Sie müssen NetScaler ADM 12.0 Build 57.24 installieren und dann auf den neuesten NetScaler ADM 13.0 Build aktualisieren. Weitere Informationen finden Sie unter Upgrade.

- Sie haben die neueste Version der NetScaler ADM 13.0 TGZ-Imagedatei heruntergeladen.

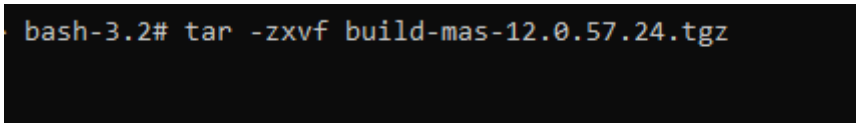
Hardwareanforderung

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8 CPUs
Speicherplatz	120 GB **Hinweis** Citrix empfiehlt,**500 GB**für eine bessere Leistung zu verwenden. Citrix empfiehlt außerdem, Solid-State-Laufwerk-Technologie (SSD) für Citrix ADM Bereitstellungen zu verwenden.
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s oder 100 Mbit/s
Hypervisor-Anforderungen	
Citrix Hypervisor	6.2, 6.5
VMware ESX	5.5, 6.0
Microsoft Hyper-V	2012 R2
Linux - KVM	Ubuntu, Fedora

Ablauf der Installation

So migrieren Sie NetScaler Insight Center zu NetScaler ADM:

1. Melden Sie sich bei der Shell-Eingabeaufforderung von NetScaler Insight Center an.
2. Laden Sie NetScaler ADM 12.0 Build 57.24 in den Ordner */var/mps/mps_images* herunter.
3. Entfernen Sie die TGZ-Datei mithilfe des Befehls **tar -zxvf build-mas-12.0-57.24.tgz**.



4. Installieren Sie NetScaler ADM mithilfe der **. /installmas** (Befehl).

5. Nach der Installation von NetScaler ADM 12.0 Build 57.24 müssen Sie ein Upgrade auf den neuesten NetScaler ADM 13.0-Build durchführen, indem Sie die oben genannten Schritte ausführen.

Nach der Migration werden alle Citrix ADC Instanzen, die in der NetScaler Insight Center er-Bestandsliste erkannt wurden, im Abschnitt **Netzwerke > Instanzen** von Citrix ADM angezeigt. Zum ersten Mal müssen Sie jedoch die virtuellen Server, die in den erkannten Appliances gehostet werden, manuell abfragen.

> **Hinweis**
>
> In Citrix ADM fallen standardmäßig keine Lizenzkosten für die Verwaltung und Überwachung von zwei virtuellen Servern an, die in den erkannten Citrix ADC Instanzen erstellt wurden. Installieren Sie die erforderlichen NetScaler ADM -Lizenzen, um mehr als zwei virtuelle Server zu überwachen und zu verwalten. Weitere Einzelheiten finden Sie unterNetScaler ADM-Lizenzierung.

Integration von NetScaler ADM und Citrix Director

February 5, 2024

Director lässt sich für Netzwerkanalysen und Leistungsmanagement in NetScaler ADM integrieren.

- Die Netzwerkanalyse ruft HDX Insight-Berichte von NetScaler ADM ab und bietet eine Anwendungs- und Desktopansicht des Netzwerks. Mit dieser Funktion bietet Director eine erweiterte Analyseansicht des ICA-Datenverkehrs in Ihrer Bereitstellung.
- Die Leistungsverwaltung bietet eine Verlaufsspeicherung und Trendberichte. Anhand der Beibehaltung historischer Daten können Sie im Gegensatz zur Echtzeitbewertung Trend-berichte über Kapazität und Integrität usw. erstellen.

Nachdem Sie NetScaler ADM in Director integriert haben, bieten Ihnen HDX Insight-Berichte die folgenden Informationen in Director:

- Auf der Registerkarte Netzwerk auf der Seite Trends werden Latenz- und Bandbreiteneffekte für Anwendungen, Desktops und Benutzer in Ihrer gesamten Bereitstellung angezeigt.
- Auf der Seite Benutzerdetails werden Latenz- und Bandbreiteninformationen zu spezifischen Benutzersitzungen angezeigt.

Voraussetzungen

Hardwareanforderungen für die Migration von HDX Insight zu NetScaler ADM

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8
Stauraum	500 GB. Citrix empfiehlt die Verwendung von Solid-State-Laufwerk-Technologie (SSD) für NetScaler ADM Bereitstellungen.
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s oder 100 Mbit/s

Softwareanforderungen

Stellen Sie vor der Migration auf die virtuelle NetScaler ADM-Appliance sicher, dass die folgenden Anforderungen erfüllt sind:

- Director Version 1811 ist installiert.
- NetScaler HDX Insight Version 10.1 oder höher ist installiert
- HDX Insight und NetScaler ADM unterstützen Citrix VDA Version 7.0 und höher
- Citrix Workspace wird von Citrix Virtual Apps and Desktops ab Version 7.0 unterstützt.
- Stellen Sie sicher, dass MAC, Citrix Receiver für Mac, Version 11.8 und höher, und Windows Citrix Receiver für Windows 14.0 und höher verfügbar sind, um genaue ICA-RTT-Metriken anzuzeigen.
- NetScaler ADM Version 11.0 und höher ist installiert. Weitere Informationen zur Installation von NetScaler ADM finden Sie unter Bereitstellen von NetScaler ADM.

Einschränkungen

- Die Verfügbarkeit dieser Funktion richtet sich nach der Lizenzierung der Organisation und den Administratorberechtigungen.
- Die Roundtrip-Zeit (RTT) der ICA-Sitzung zeigt die Daten für Citrix Receiver für Windows 3.4 oder höher und für Citrix Receiver für Mac 11.8 oder höher korrekt an. Bei früheren Versionen von Receiver werden die Daten nicht richtig angezeigt.

- In der Ansicht Trends werden HDX-Verbindungsanmeldedaten nicht für VDAs vor Version 7 erfasst. Für frühere VDAs werden die Diagrammdaten als 0 angezeigt.
- Bei Bereitstellungen, die bereits über eine externe Festplatte mit weniger als 500 GB Speicherplatz verfügen, können Sie keine weitere Festplatte hinzufügen.

> **Hinweis**
>
> - Weitere Informationen zu Director und Schritte zur Integration von NetScaler ADM mit Director finden Sie unterhttps://docs.citrix.com/en-us/xenapp-and-xendesktop/7-15-ltsr/director/hdx-insight.html.
> - Weitere Informationen zu HDX Insight finden Sie unterhttp://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html.

Stellen Sie einen zusätzlichen Datenträger für NetScaler ADM bereit

February 5, 2024

Die Speicheranforderungen für die NetScaler Application Delivery Management (ADM) werden auf der Grundlage Ihrer NetScaler ADM Größenberechnung festgelegt. NetScaler ADM bietet standardmäßig eine Speicherkapazität von 120 GB. Wenn Sie mehr als 120 GB zum Speichern Ihrer Daten benötigen, können Sie zusätzlichen Datenträger bereitstellen.

> **Hinweis**
>
> - Schätzen Sie die Speicheranforderungen und stellen Sie zum Zeitpunkt der Erstbereitstellung von NetScaler ADM einen zusätzlichen Datenträger für den Server bereit.
> - Bei einer NetScaler ADM Bereitstellung mit einem Server können Sie zusätzlich zum Standarddatenträger nur einen Datenträger an den Server anhängen.
> - Für eine NetScaler ADM Hochverfügbarkeitsbereitstellung müssen Sie für jeden Knoten einen zusätzlichen Datenträger bereitstellen. Die Größe beider Datenträger muss identisch sein.
> - Wenn Sie zuvor einen externen Datenträger mit geringerer Kapazität angeschlossen haben, müssen Sie den Datenträger entfernen, bevor Sie einen neuen Datenträger anfügen.
> - Sie können einen zusätzlichen Datenträger mit einer Kapazität von mehr als 2 Terabyte anschließen. Bei Bedarf kann die Größe des Datenträgers auch niedriger als 2 Terabyte sein.

> • Citrix empfiehlt die Verwendung von Solid-State-Laufwerk-Technologie (SSD) für NetScaler ADM Bereitstellungen.

In diesem Dokument werden die folgenden Szenarien zum Bereitstellen eines zusätzlichen, neuen Datenträgers, zum Erstellen von Partitionen und zum Ändern der Größe des zusätzlichen Datenträgers erläutert:

1. Stellen Sie einen neuen, zusätzlichen Datenträger bereit
2. Starten Sie das Datenträgerpartitionierungstool
3. Erstellen Sie Partitionen auf dem neuen, zusätzlichen Datenträger
4. Größe des vorhandenen zusätzlichen Datenträgers ändern
5. Entfernen von Partitionen auf dem zusätzlichen Datenträger

Bereitstellen eines zusätzlichen Datenträgers in einem eigenständigen NetScaler ADM

Führen Sie die folgenden Schritte aus, um einen Datenträger für die virtuelle Maschine bereitzustellen:

1. Fahren Sie die virtuelle NetScaler ADM Maschine herunter.
2. Stellen Sie im Hypervisor einen zusätzlichen Datenträger mit der erforderlichen Datenträgergröße für die virtuellen NetScaler ADM Maschine bereit.

   Auf dem neu zugeordneten größeren Datenträger werden die Datenbankdaten und die NetScaler ADM Protokolldateien gespeichert. Der vorhandene 120-Gigabyte-Standarddatenträger wird jetzt zum Speichern der Kerndateien, der Protokolldateien des Betriebssystems usw. verwendet.
3. Starten Sie die virtuelle NetScaler ADM Maschine.

NetScaler ADM Datenträgerpartitionstool

NetScaler ADM bietet jetzt das **NetScaler ADM Datenträgerpartitionstool**, ein neues Befehlszeilentool. Die Funktionalitäten dieses Tools werden wie folgt detailliert beschrieben:

1. Mit dem Tool können Sie Partitionen auf dem neu hinzugefügten zusätzlichen Datenträger erstellen.
2. Sie können die Größe vorhandener zusätzlicher Datenträger auch mit diesem Tool ändern. Der vorhandene externe Datenträger darf jedoch nicht größer als 2 Terabyte sein.

> **Hinweis**
>
> - Es ist nicht möglich, die Größe vorhandener Datenträger über 2 Terabyte hinaus zu ändern, ohne Daten zu verlieren. Dies ist auf eine bekannte Beschränkung der Plattform zurückzuführen.
> - Um eine Speicherkapazität von mehr als 2 Terabyte zu erstellen, müssen Sie die vorhandenen Partitionen entfernen und mit diesem neuen Tool Partitionen erstellen.

3. Mit diesem neuen Tool können Sie jede Partitionsaktion explizit auf dem Datenträger ausführen. Das Tool bietet Ihnen eine klare Sichtbarkeit und Kontrolle über den Datenträger und die zugehörigen Daten.

> **Hinweis**
>
> Sie können dieses Tool nur auf dem zusätzlichen Datenträger verwenden, den Sie an den NetScaler ADM-Server angeschlossen haben. Mit diesem Tool können Sie keine Partitionen auf dem primären (Standard-) 120-Gigabyte-Datenträger erstellen.

Starten Sie das Datenträgerpartitionstool

1. Öffnen Sie eine SSH-Verbindung zum NetScaler ADM, indem Sie einen SSH-Client wie PuTTY verwenden.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei Citrix ADM an.
3. Wechseln Sie zur Shell-Eingabeaufforderung und geben Sie Folgendes ein:

```
/mps/DiskPartitionTool.py
<!--NeedCopy-->
```

```
bash-3.2# /mps/DiskPartitionTool.py

------------------------------------
MAS/SVM Disk Partition Tool (DPT) 1.0
------------------------------------
Welcome to MAS/SVM DPT! Type 'help' or '?' to view a list of commands.

(dpt):
```

> **Hinweis**
>
> Für NetScaler ADM in der Hochverfügbarkeitsbereitstellung müssen Sie das Tool in beiden Knoten starten und Partitionen erstellen oder deren Größe ändern, nachdem Sie Datenträger an die jeweiligen virtuellen Maschinen angeschlossen haben.

Erstellen von Partitionen auf dem neuen zusätzlichen Datenträger

Der Befehl **create** wird verwendet, um Partitionen zu erstellen, wenn ein neuer sekundärer Datenträger hinzugefügt wird. Sie können diesen Befehl auch verwenden, um Partitionen auf einem vorhandenen sekundären Datenträger zu erstellen, nachdem die vorhandenen Partitionen mit dem Befehl “remove”gelöscht wurden.

```
(dpt): ?create
Creates a new partition on the attached disk. A swap partition of size 32GB is also created automatically.

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

> **Hinweis:**
>
> Beim Erstellen von Partitionen mit dem Datenträgerpartitionstool gibt es keine Beschränkung der Größe von 2 Terabyte. Das Tool kann Partitionen mit mehr als 2 Terabyte erstellen. Wenn Sie den Datenträger partitionieren, wird automatisch eine Swap-Partition der Größe 32 GB hinzugefügt. Die primäre Partition verwendet dann den gesamten verbleibenden Speicherplatz auf dem Datenträger.

Sobald der Befehl ausgeführt wurde, wird ein Partitionsschema der GUID-Partitionstabelle (GPT) erstellt. Außerdem werden eine 32 GB Swap-Partition und Datenpartition erstellt, um den Rest des Speicherplatzes zu nutzen. Ein neues Dateisystem wird dann auf der primären Partition erstellt.

> **Hinweis**
>
> Dieser Vorgang kann einige Sekunden dauern, und Sie dürfen den Prozess nicht unterbrechen.

```
(dpt): create

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

```
Creating GPT partition scheme...
da1 created

Creating partition 1 using (456287933) blocks. Leaving aside 32G for swap...
da1p1 added

Creating partition 2 for swap using remaining 32G...
da1p2 added

Formatting the new partition. This may take some time (~20 seconds). Please be patient and don't interrup the process...
```

Sobald der Befehl create abgeschlossen ist, wird die virtuelle Maschine automatisch neu gestartet, damit die neue Partition bereitgestellt wird.


```
Create Done.
VM has to be rebooted for the new partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

Nach dem Neustart wird die neue Partition unter /var/mps gemountet.

```
bash-3.2# df -k
Filesystem  1024-blocks     Used     Avail Capacity  Mounted on
/dev/md0         456046   374346     72580    84%    /
devfs                 1        1         0   100%    /dev
procfs                4        4         0   100%    /proc
fdescfs               1        1         0   100%    /dev/fd
/dev/da0s1a     1623950   284466   1209568    19%    /flash
/dev/da0s1e   116073918 2812298 103975708     3%    /var
/dev/da1p1    495168802   43854 455511444     0%    /var/mps
```

Die hinzugefügte Swap-Partition wird als Swap-Raum in der Ausgabe des Befehls “create” angezeigt.

```
CPU:  0.0% user,  0.0% nice,  0.0% system,  0.7% interrupt, 99.3% idle
Mem: 89M Active, 21M Inact, 123M Wired, 16M Cache, 74M Buf, 6965M Free
Swap: 37G Total, 37G Free
```

> **Hinweis**
>
> Das Tool startet die virtuelle Maschine neu, nachdem Sie die Partition erstellt haben.

Ändern Sie die Größe der Partitionen in dem vorhandenen zusätzlichen Datenträger

Sie können den Befehl **resize** verwenden, um die Größe des angeschlossenen (sekundären) Datenträgers zu ändern. Sie können die Größe eines Datenträgers ändern, die ein `master boot record` (`MBR`) oder GPT-Schema hat. Die Größe des Datenträgers muss weniger als 2 Terabyte bis maximal 2 Terabyte betragen.

> **Hinweis**
>
> - Der Befehl “Größe ändern”wurde entwickelt, um zu funktionieren, ohne dass vorhandene Daten verloren gehen. Citrix empfiehlt jedoch, dass Sie wichtige Daten auf dieser Datenträger auf einem externen Speicher sichern, bevor Sie die Größe ändern. Datenbackup ist

hilfreich in Fällen, in denen die Datenträgerdaten während des Größenänderungsvorgangs beschädigt werden können.

- Stellen Sie sicher, dass Sie den Speicherplatz in Schritten von 100 GB Speicherplatz vergrößern, während Sie die Größe der Partitionen ändern. Eine solche inkrementelle Erhöhung stellt sicher, dass Sie die Größe nicht öfter ändern müssten.

```
(dpt): ?resize
Resizes existing partition on attached disk to utilize all space available. Pre-conditions are:
1. Secondary disk exists and capcity of disk < 2TB
2. A single partition exists on secondary disk and there is atleast 100GB to gain by resizing

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Der Befehl "resize"prüft alle Voraussetzungen und geht weiter, ob alle Voraussetzungen erfüllt sind und nachdem Sie der Größenänderung zugestimmt haben. Es stoppt die Prozesse, die auf den Datenträger zugreifen. Dazu gehören die NetScaler ADM -Subsysteme, PostgreSQL DB-Prozesse und der NetScaler ADM-Monitorprozess. Sobald die Prozesse beendet wurden, wird die Bereitstellung des Datenträgers aufgehoben, um ihn für die Größenänderung vorzubereiten. Die Größenänderung erfolgt durch Erweitern der Partition, um den gesamten verfügbaren Speicherplatz zu belegen, und anschließendes Erweitern des Dateisystems. Wenn eine Swap-Partition auf dem Datenträger vorhanden ist, wird sie gelöscht und nach der Größenänderung am Ende des Datenträgers neu erstellt. Die Swap-Partition wird im Abschnitt Befehl **erstellen** des Dokuments erläutert.

Hinweis:

Der Prozess des "wachsenden Dateisystems"kann einige Zeit in Anspruch nehmen und es wird darauf geachtet, dass Sie den Vorgang nicht unterbrechen, während er ausgeführt wird. Das Tool startet die virtuelle Maschine neu, nachdem Sie die Größe der Partition geändert haben.

```
(dpt): resize

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to resize (Y/N): y
```

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1...
da1p1 resized

Adding a swap partition da1p2...
da1p2 added

Formatting the newly added portions of the partition. This may take some time (~10 seconds). Please be patient and don't
 interrup the process...
```


Alle Zwischenschritte im Größenänderungsprozess (Anhalten von Anwendungen, Ändern der Größe des Datenträgers, wachsendes Dateisystem) werden auf der Konsole angezeigt. Sobald der Prozess abgeschlossen ist, wird die folgende Meldung angezeigt.

```
Resize Done.
VM has to be rebooted for the resized partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

Nach dem Neustart kann die Zunahme der Größe mit dem Befehl "df"beobachtet werden. Hier sind die Vorher und Nachher Details, nachdem Sie die Größe vergrößert haben:

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0        456046  374864     72062    84%    /
devfs                1       1         0   100%    /dev
procfs               4       4         0   100%    /proc
fdescfs              1       1         0   100%    /dev/fd
/dev/da0s1a    1623950  284468   1209566    19%    /flash
/dev/da0s1e  116073918 1662048 105125958     2%    /var
/dev/da1s1a  152329216 3082226 137060654     2%    /var/mps
```

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0        456046  374838     72088    84%    /
devfs                1       1         0   100%    /dev
procfs               4       4         0   100%    /proc
fdescfs              1       1         0   100%    /dev/fd
/dev/da0s1a    1623950  284468   1209566    19%    /flash
/dev/da0s1e  116073918 1666800 105121206     2%    /var
/dev/da1s1a  304651668 3137954 277141582     1%    /var/mps
```

Entfernen der Partitionen des zusätzlichen Datenträgers

Eine vorhandene Partition auf dem sekundären Datenträger kann auf bis zu 2 Terabyte verkleinert werden. Dies ist auf eine bekannte Beschränkung der Partition zurückzuführen. Wenn Sie einen Datenträger mit mehr als 2 Terabyte wünschen, schließen Sie einen neuen Datenträger an und partitionieren Sie ihn mit dem Datenträgerpartitionstools. Sie können die vorhandene Partition auch mithilfe des Befehls **remove entfernen** und dann eine Partition erstellen.

> **Hinweis**
>
> Durch das Entfernen der vorhandenen Partition werden alle vorhandenen Daten gelöscht. Daher müssen alle kritischen Daten auf einem externen Speicher gesichert werden, bevor Sie diesen Befehl verwenden.

```
(dpt): ?remove
Removes existing partition from attached disk.

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Wenn Sie den Befehl "remove"ausführen, werden Sie zur Bestätigung aufgefordert. Nach der Bestätigung werden alle Prozesse (wie ADM-Subsysteme, PostgreSQL Prozesse und ADM-Monitor) mit dem

sekundären Datenträger gestoppt. Wenn eine Swap-Partition vorhanden ist und Swap auf der Partition aktiviert ist, wird der Swap deaktiviert.

```
(dpt): remove

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

Wenn Sie “y”eingeben, wird die Bereitstellung des Datenträgers aufgehoben und alle Partitionen auf dem Datenträger.

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to remove existing partitions.
Disabling swap on partition: /dev/da1p2
Removing all partitions from: da1
Remove Done.
Rebooting VM now...
```

> **Hinweis**
>
> Das Tool startet die virtuelle Maschine neu, nachdem Sie die Partition entfernt haben.

Starten Sie die virtuelle Maschine neu

Wenn eine Partition erstellt oder in der Größe geändert wird oder wenn eine Auslagerungsdatei erstellt wurde, starten Sie die virtuelle Maschine neu. Die Änderungen werden erst nach einem Neustart wirksam. Zu diesem Zweck wird ein **Reboot-Befehl** im Tool bereitgestellt.

```
(dpt): ?reboot
Reboot the VM. Note: VM has to be rebooted after new partition is created, existing one is resized or swap file is creat
ed.
The VM is rebooted automatically after these operations. If the automatic reboot does not happen, then this command can
be used to reboot the VM.
```

Sie werden zur Bestätigung aufgefordert und werden nach der Bestätigung alle Prozesse beendet (z. B. ADM-Subsysteme, PostgreSQL Prozesse und ADM-Monitor). Die virtuelle Maschine wird dann neu gestartet.

```
(dpt): reboot
Are you sure you want to reboot the VM (Y/N): y
```



```
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

Erstellen einer Backupdatei der Datenträgerdaten

Im Folgenden finden Sie die Schritte, um ein Backup der NetScaler ADM-Daten anzulegen, bevor Sie die Größe der Partitionen ändern oder entfernen.

> **Hinweis**
>
> Das Erstellen einer Backupdatei erfordert Speicherplatz. Citrix empfiehlt, dass Sie sicherstellen, dass genügend freier Speicherplatz (50% oder mehr) zur Verfügung steht, bevor Backupbefehle ausgeführt werden.

1. Beenden Sie ADM.

```
/mps/masd stop
<!--NeedCopy-->
```

2. Stoppen Sie PostgreSQL.

```
su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
<!--NeedCopy-->
```

3. Beenden Sie ADM-Monitor.

```
/mps/scripts/stop_mas_monit.sh
<!--NeedCopy-->
```

4. Erstellen Sie einen Tarball.

```
cd /var
tar cvfz /var/mps/mps_backup.tgz mps
<!--NeedCopy-->
```

> **Hinweis**
>
> Der Vorgang dauert Zeit, abhängig von der Größe der zu sichernden Daten.

5. Prüfsumme generieren.

```
md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
<!--NeedCopy-->
```

6. Kopieren Sie die Tarball- und Prüfsummendateien auf einen Remoteserver.

7. Überprüfen Sie die Richtigkeit des kopierten Tarballs. Generieren Sie eine Prüfsumme der übertragenen Datei und vergleichen Sie sie mit der Quellprüfsumme.
8. Entfernen Sie den Tarball von der virtuellen ADM-Maschine.

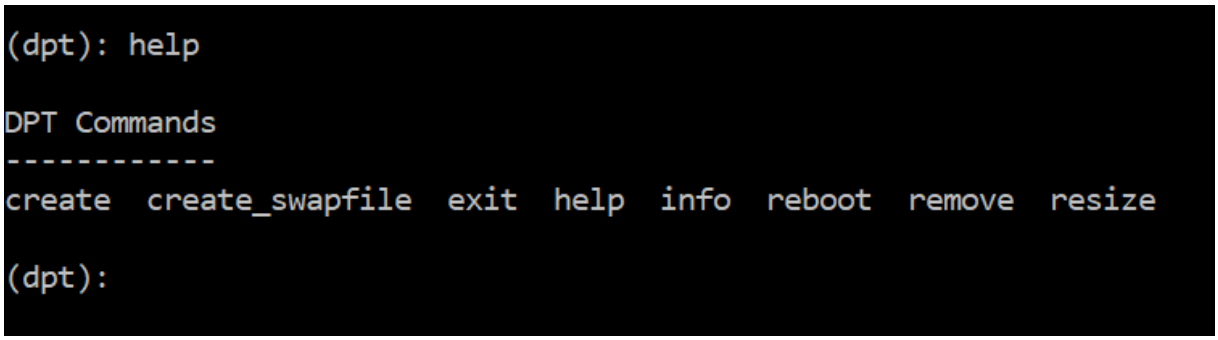
```
cd /var/mps/
rm mps_backup.tgz  mps_backup_checksum
<!--NeedCopy-->
```

Zusätzliche Befehle

Zusätzlich zu den zuvor aufgeführten Befehlen können Sie auch die folgenden Befehle im Tool verwenden:

Befehl "Hilfe":

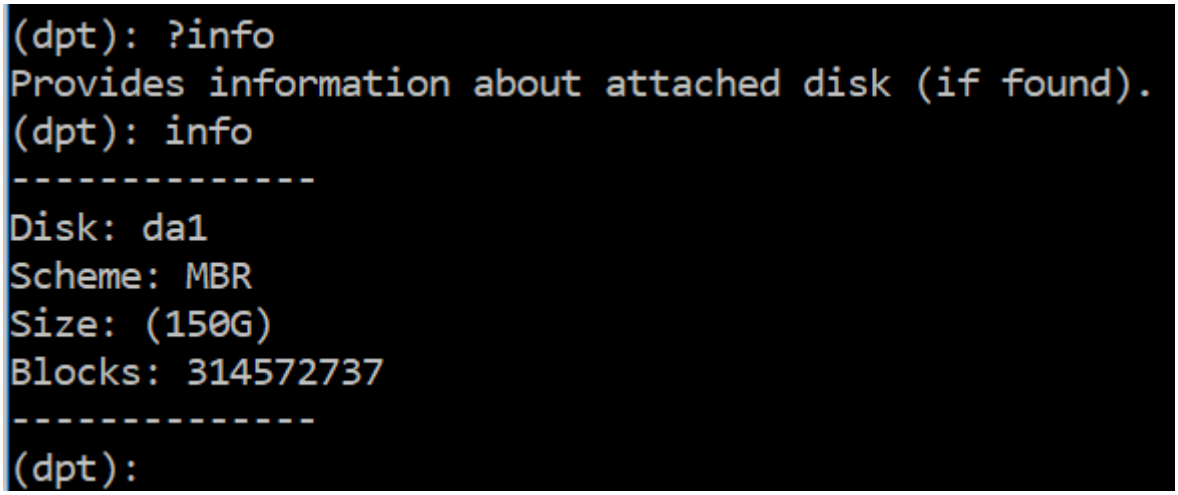
Um die unterstützten Befehle aufzulisten, geben Sie **help** oder **?** und drücken Sie Enter. Um weitere Hilfe zu jedem Befehl zu erhalten, drücken Sie bitte **help** oder **?** gefolgt von dem Befehlsnamen, und drücken Sie die **Eingabetaste**.



Info (Befehl):

Der Befehl **info** liefert Informationen über den angeschlossenen sekundären Datenträger, falls der Datenträger vorhanden ist. Der Befehl liefert den Gerätenamen, das Partitionsschema, die Größe in menschenlesbarer Form und die Anzahl der Datenträgerblöcke. Das Schema kann MBR oder GPT sein. Ein MBR-Schema bedeutet, dass der Datenträger mit einer früheren Version der NetScaler ADM-Version partitioniert wurde. Die MBR/GPT-basierte Partition kann in der Größe geändert werden, jedoch nicht über 2 Terabyte hinaus. GPT-Partitionsschema bedeutet, dass der Datenträger mit NetScaler ADM 12.1 oder höher partitioniert wurde.

> **Hinweis:**
>
> Eine GPT-Partition kann größer als 2 Terabyte sein, aber wenn sie erstellt wird. Sie können die Größe des Datenträgers jedoch nicht auf eine Größe von mehr als 2 Terabyte ändern, nachdem Sie einen Datenträger mit einer kleineren Größe erstellt haben. Dies ist eine bekannte Einschränkung der Plattform.



Create_swapfile (Befehl):

Die Standardauslagerungspartition auf dem primären Datenträger von NetScaler ADM beträgt 4 GB, daher beträgt der Standardauslagerungsspeicher 4 GB. Für die Standardspeicherkonfiguration von NetScaler ADM, die 2 GB beträgt, ist dieser Swap-Speicherplatz ausreichend. Wenn Sie NetScaler ADM jedoch mit einer höheren Speicherkonfiguration ausführen, benötigen Sie mehr Auslagerungsspeicher auf dem Datenträger.

> **Hinweis**
>
> Die Auslagerungspartition ist in der Regel eine dedizierte Partition, die während der Installation des Betriebssystems auf einer Festplatte (HDD) erstellt wird. Eine solche Partition wird auch als Swap Space bezeichnet. Die Auslagerungspartition wird für virtuellen Speicher verwendet, der den zusätzlichen Hauptspeicher simuliert.

Bei sekundären Datenträgern, die in früheren Versionen von NetScaler ADM hinzugefügt wurden, wird standardmäßig keine Auslagerungspartition erstellt. Der Befehl "create_swapfile"ist für sekundäre Datenträger gedacht, die mit älteren NetScaler ADM-Versionen ohne Auslagerungspartition erstellt wurden. Der Befehl prüft auf Folgendes:

- Vorhandensein eines sekundären Datenträgers
- Datenträger, der bereitgestellt wird
- Größe des Datenträgers (mindestens 500 GB)
- Die Existenz der Auslagerungsdatei

Der Befehl "create_swapfile"ist nur nützlich, wenn der Speicher größer oder gleich 16 GB ist und nicht, wenn der Speicher niedrig ist. Daher überprüft dieser Befehl auch nach Speicher, bevor Sie mit der Erstellung der Auslagerungsdatei fortfahren.


```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should n
ot be interrupted.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Wenn alle Bedingungen erfüllt sind und der Benutzer damit einverstanden ist, fortzufahren, wird eine 32 GB Auslagerungsdatei auf dem sekundären Datenträger erstellt. Die Erstellung der Auslagerungsdatei dauert einige Minuten und sorgt dafür, dass Sie den Vorgang während des Ablaufs nicht unterbrechen. Nach erfolgreichem Abschluss wird ein Neustart durchgeführt, damit die Auslagerungsdatei wirksam wird.

```
Creating swapfile. This may take some time (~5 mins). Please be patient and don't interrupt the process...
32768+0 records in
32768+0 records out
34359738368 bytes transferred in 724.061475 secs (47454173 bytes/sec)

Changing permissions for created swapfile...

Create (swapfile) Done.
VM has to be rebooted for the newly created swapfile to take effect.
```

Nach dem Neustart kann der Anstieg des Swap mit dem Befehl top beobachtet werden.

```
CPU:  1.7% user,  0.0% nice,  0.8% system,  0.2% interrupt, 97.4% idle
Mem: 1847M Active, 506M Inact, 382M Wired, 4684K Cache, 199M Buf, 4473M Free
Swap: 4198M Total, 4198M Free
```

```
CPU: 42.0% user,  0.0% nice,  7.6% system,  5.0% interrupt, 45.3% idle
Mem: 1805M Active, 423M Inact, 393M Wired, 4792K Cache, 199M Buf, 4587M Free
Swap: 36G Total, 36G Free
```

Befehl “Beenden”:

Um das Werkzeug zu verlassen, geben Sie exit ein, und drücken **Sie die Eingabetaste**.

```
(dpt): exit
bash-3.2#
```

Hinzufügen zusätzlicher Datenträger an NetScaler ADM, das in hoher Verfügbarkeit bereitgestellt wird

Betrachten wir ein Szenario, in dem Sie ein Paar von NetScaler ADM -Servern in einer Hochverfügbarkeit ohne sekundäre Datenträger konfiguriert haben. Bedenken Sie auch, dass Sie 2 oder mehr NetScaler ADC-Instanzen hinzugefügt, überprüft und sichergestellt haben, dass alle Prozesse ausgeführt werden. Möglicherweise möchten Sie den virtuellen Maschinen in diesem Setup sekundäre Laufwerke hinzufügen. In einer Hochverfügbarkeitseinrichtung müssen Sie zusätzliche Datenträger zu beiden Knoten hinzufügen, wie in dieser Aufgabe beschrieben:

1. Angenommen, die NetScaler ADM-Knotennamen lauten “ADM_Primary”und “ADM_Secondary” .
2. Führen Sie zunächst das Partitionstool auf ADM_Secondary aus und fügen Sie dann einen sekundären Datenträger hinzu. Die virtuelle Maschine wird neu gestartet, nachdem der Datenträger hinzugefügt wurde.
3. Fahren Sie ADM_Secondary nach dem Neustart herunter.
4. Führen Sie nun das Partitionstool auf ADM_Primary aus und fügen Sie einen sekundären Datenträger hinzu. Die virtuelle Maschine wird neu gestartet, nachdem der Datenträger hinzugefügt wurde.

   Stellen Sie sicher, dass Sie Datenträger mit ähnlicher Kapazität zu beiden Knoten hinzufügen. Wenn Sie beispielsweise einen Datenträger mit einer Kapazität von 500 GB zum primären Knoten hinzufügen, fügen Sie dem sekundären Knoten auch einen Datenträger mit 500 GB Kapazität hinzu.
5. Überprüfen Sie nach dem Neustart von ADM_Primary, ob es sich um den primären Knoten handelt.
6. Starten Sie nun den Knoten ADM_Secondary. Stellen Sie sicher, dass es als sekundärer Knoten hochgefahren ist und die Datenbanken synchronisiert wurden.
7. Bestätigen Sie, dass alle Daten noch vorhanden sind.

Um die RAM-Kapazität auf beiden Knoten zu erhöhen:

1. Fahren Sie ADM_Secondary herunter, und erhöhen Sie die RAM-Größe je nach Bedarf. Starten Sie den Knoten nicht neu.
2. Fahren Sie ADM_primary herunter, und erhöhen Sie die RAM-Größe je nach Bedarf.

   Stellen Sie sicher, dass Sie die RAM-Größe auf beiden Knoten gleichmäßig erhöhen. Wenn Sie beispielsweise die RAM-Größe auf dem primären Knoten auf 16 GB erhöhen, tun Sie dasselbe auch auf dem sekundären Knoten.
3. Starten Sie ADM_Primary neu.
4. Überprüfen Sie nach dem Neustart von ADM_Primary, ob es sich um den primären Knoten handelt.
5. Starten Sie nun den Knoten ADM_Secondary. Stellen Sie nach dem Neustart sicher, dass es als sekundär eingestuft wurde und die DB-Synchronisierung funktioniert.
6. Bestätigen Sie nun, dass alle Daten noch existieren.

> **Hinweis**
>
> Nachdem Sie den sekundären Datenträger hinzugefügt haben, dauert es einige Zeit, bis der primäre Knoten hochgefahren ist. Außerdem erfordert das gesamte Hinzufügen von sekundären Datenträger zu beiden Knoten und die Erhöhung der RAM-Kapazität, dass beide Knoten für einige Zeit heruntergefahren sind. Berücksichtigen Sie diese Ausfallzeiten bei der Planung dieser Wartungsaktivität.

Konfigurieren

February 5, 2024

Sie können nur mit der GUI auf einen NetScaler ADM-Server zugreifen. Sie müssen auf die GUI zugreifen, um Instanzen und Apps hinzuzufügen, Instanzen und Apps zu verwalten und zu überwachen, Analysen anzuzeigen und den NetScaler ADM -Server zu konfigurieren.

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

Die folgenden Browser werden unterstützt.

Webbrowser	Version
Internet Explorer	11.0 und höher
Google Chrome	Chrome 19 und höher
Safari	Safari 5.1.1 und höher
Mozilla Firefox	Firefox 3.6.25 und später

So greifen Sie auf die NetScaler ADM GUI zu:

Melden Sie sich mit den Administratoranmeldeinformationen bei Citrix ADM an.

Nachdem Sie sich bei NetScaler ADM angemeldet haben, müssen Sie folgende Schritte ausführen:

- Instanzen zu NetScaler ADM hinzufügen.Sie müssen dem Citrix ADM -Server Instanzen hinzufügen, wenn Sie diese Instanzen verwalten und überwachen möchten.
- Ermöglichen Sie Analysen auf virtuellen Servern.Um Analysedaten für den Anwendungsdatenfluss anzuzeigen, müssen Sie die Analytics-Funktion auf den virtuellen Servern aktivieren, die Datenverkehr für die spezifischen Anwendungen empfangen.

- Konfigurieren Sie den NTP-Server auf NetScaler ADM.Sie müssen einen NTP-Server (Network Time Protocol) in Citrix ADM konfigurieren, um seine Uhr mit dem NTP-Server zu synchronisieren.
- Konfigurieren Sie die Systemeinstellungen für eine optimale NetScaler ADM-Leistung.Bevor Sie mit NetScaler ADM Ihre Instanzen und Anwendungen verwalten und überwachen, wird empfohlen, einige Systemeinstellungen zu konfigurieren, die eine optimale Leistung des NetScaler ADM-Servers gewährleisten.

Instanzen zu NetScaler ADM hinzufügen

February 5, 2024

Instanzen sind Citrix-Appliances oder virtuelle Appliances, die Sie von NetScaler ADM aus erkennen, verwalten und überwachen möchten. Sie müssen dem NetScaler ADM -Server Instanzen hinzufügen, wenn Sie diese Instanzen verwalten und überwachen möchten. Sie können NetScaler ADM die folgenden Citrix Appliances und virtuellen Appliances hinzufügen:

- NetScaler ADC MPX
- NetScaler ADC VPX
- NetScaler ADC SDX
- NetScaler ADC CPX
- NetScaler ADC BLX
- Citrix Gateway
- Citrix SD-WAN

Sie können Instanzen hinzufügen, wenn Sie den NetScaler ADM-Server zum ersten Mal oder später einrichten. Anschließend müssen Sie ein Instanzprofil angeben, mit dem NetScaler ADM auf die Instanz zugreifen kann.

> **Hinweis**
>
> - NetScaler ADM verwendet die NetScaler IP (NSIP) -Adresse der NetScaler ADC Instanzen für die Kommunikation. Informationen zu den Ports, die zwischen den NetScaler ADC-Instanzen und NetScaler ADM geöffnet sein müssen, finden Sie unter Ports.
> - Für Citrix SD-WAN WO und Citrix SD-WAN EE-Instanzen verwendet NetScaler ADM die Verwaltungs-IP-Adresse der Instanzen für die Kommunikation.
> - Informationen darüber, wie NetScaler ADM Instanzen erkennt, finden Sie unter Instanzen

> entdecken.

Erstellen eines NetScaler ADC Profils

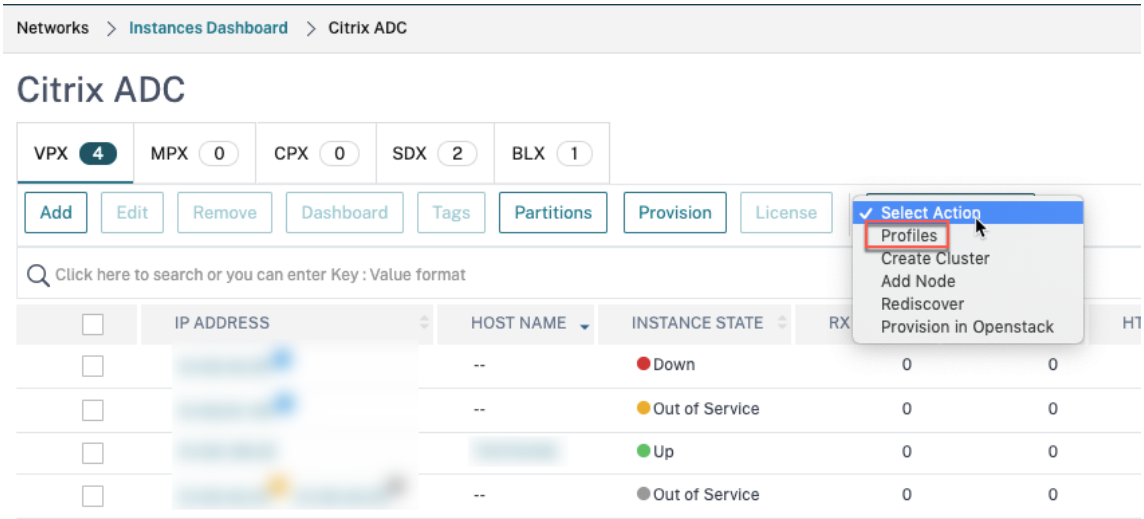
Das NetScaler ADC Profil enthält den Benutzernamen, das Kennwort, die Kommunikationsports und die Authentifizierungstypen der Instanzen, die Sie NetScaler ADM hinzufügen möchten. Für jeden Instanztyp ist ein Standardprofil verfügbar. Zum Beispiel `nsroot` ist das das Standardprofil für NetScaler ADC-Instanzen. Das Standardprofil wird mithilfe der standardmäßigen NetScaler ADC Administratoranmeldeinformationen definiert. Wenn Sie die standardmäßigen Administratoranmeldeinformationen Ihrer Instanzen geändert haben, können Sie benutzerdefinierte Instanzprofile für diese Instanzen definieren. Wenn Sie die Anmeldeinformationen einer Instanz ändern, nachdem die Instanz erkannt wurde, müssen Sie das Instanzprofil bearbeiten oder ein Profil erstellen und dann die Instanz neu ermitteln.

Sie können ein NetScaler ADC Profil auf der **Instanzseite** oder beim Hinzufügen oder Ändern einer Instanz erstellen.

> **Hinweis**
>
> Verwenden Sie unbedingt das Superadministrator-Konto, um ein Instanzprofil zu erstellen.

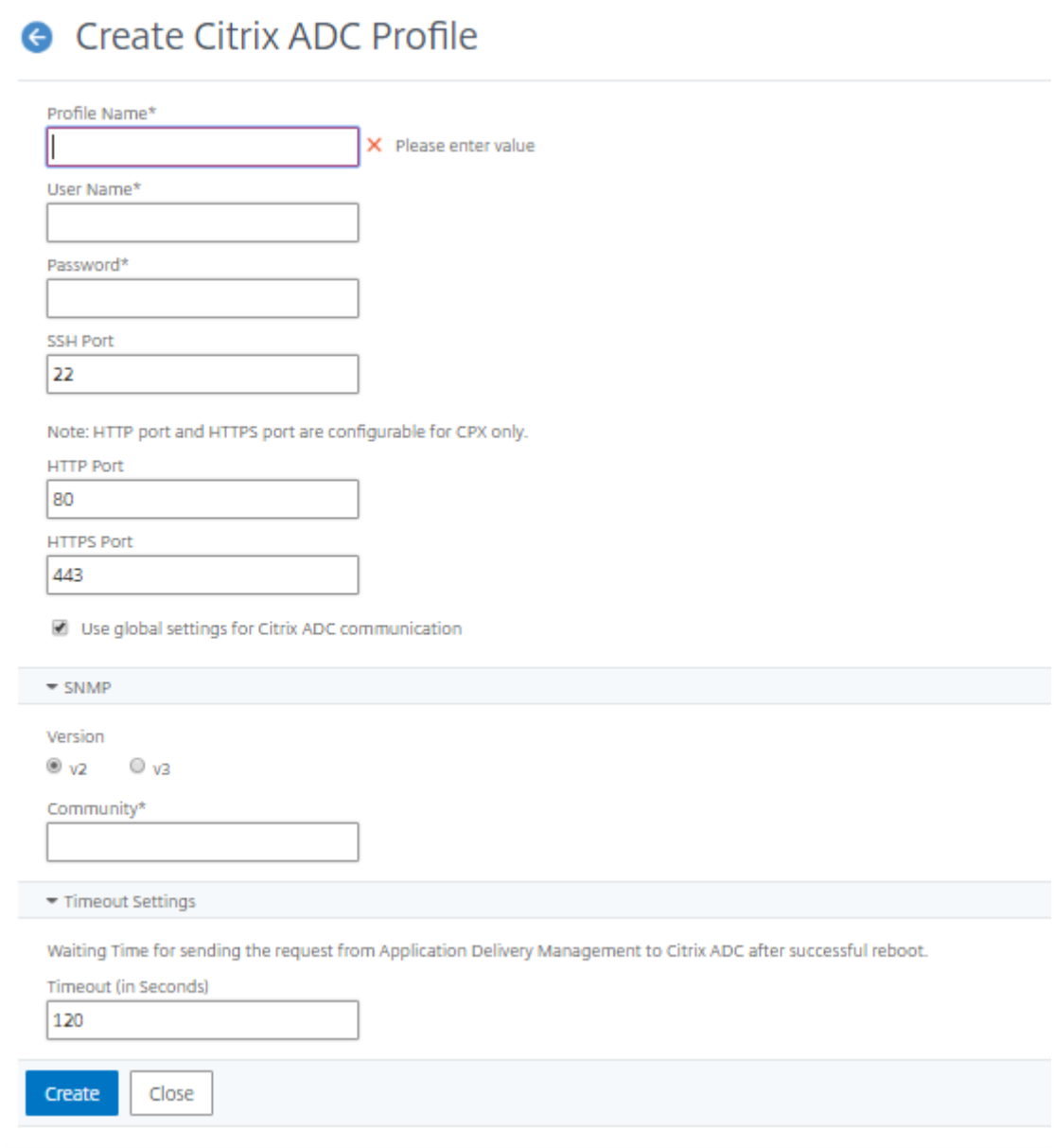
So erstellen Sie ein NetScaler ADC Profil auf der Instanzseite:

1. Navigieren Sie zu **Netzwerke > Instanzen**.
2. Wählen Sie eine Instanz aus. Beispiel: NetScaler ADC.
3. Wählen Sie auf der NetScaler ADC-Seite unter **Aktion auswählen** die Option **Profile**aus.



4. Wählen Sie auf der Seite **Admin-Profile** die Option **Hinzufügen**aus.

5. Gehen Sie auf der Seite **NetScaler ADC-Profil erstellen** wie folgt vor:



a) **Profilname**: Geben Sie einen Profilnamen für die NetScaler ADC-Instanz an.

b) **Benutzername**: Geben Sie einen Benutzernamen an, um sich bei der NetScaler ADC-Instanz anzumelden.

c) **Kennwort**: Geben Sie ein Kennwort an, um sich an der NetScaler ADC-Instanz

anzumelden.

d) **SSH-Port**: Geben Sie den Port für die SSH-Kommunikation zwischen NetScaler ADM und der NetScaler ADC-Instanz an.

e) **HTTP-Port**: Geben Sie den Port für die HTTP-Kommunikation zwischen NetScaler ADM und der NetScaler ADC-Instanz an.

> **Hinweis:**
>
> Der Standard-HTTP-Port ist 80. Sie können auch den nicht standardmäßigen oder benutzerdefinierten HTTP-Port angeben, den Sie möglicherweise in Ihrer NetScaler ADC CPX-Instanz konfiguriert haben. Der benutzerdefinierte HTTP-Port kann nur für die Kommunikation zwischen NetScaler ADM und NetScaler ADC CPX verwendet werden.

f) **HTTPS-Port**: Geben Sie den Port für die HTTPS-Kommunikation zwischen NetScaler ADM und der NetScaler ADC-Instanz an.

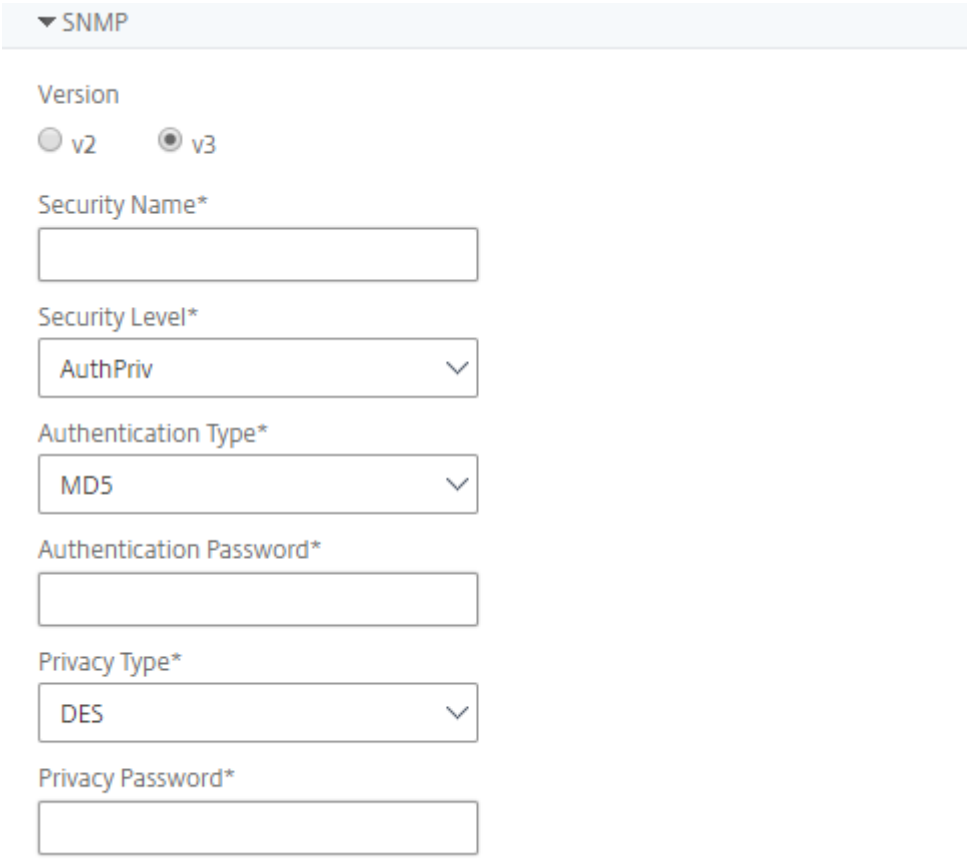
> **Hinweis:**
>
> Der Standard-HTTPS-Port ist 443. Sie können auch den nicht standardmäßigen oder benutzerdefinierten HTTPS-Port angeben, den Sie möglicherweise in Ihrer NetScaler ADC CPX-Instanz konfiguriert haben. Der angepasste HTTPS-Port kann nur für die Kommunikation zwischen NetScaler ADM und NetScaler ADC CPX verwendet werden.

g) **Globale Einstellungen für NetScaler ADC-Kommunikation**verwenden: Wählen Sie diese Option, wenn Sie die Systemeinstellungen für die Kommunikation zwischen NetScaler ADM und NetScaler ADC-Instanz verwenden möchten, andernfalls wählen Sie entweder HTTP oder https aus.

h) **SNMP-Version**: Wählen Sie entweder **SNMPv2** oder **SNMPv3** aus, und führen Sie die folgenden Schritte aus:

   i. Wenn Sie SNMPv2 auswählen, geben Sie den **Community-Namen** für die Authentifizierung an.

   ii. Wenn Sie SNMPv3 auswählen, geben Sie den **Sicherheitsnamen** und die **Sicherheitsstufe an**. Wählen Sie basierend auf der Sicherheitsstufe den **Authentifizierungstyp** und den **Datenschutztyp**aus.



> **Hinweis**
>
> Für NetScaler ADC SDX wird nur **SNMPv2** unterstützt.

i) **Timeout-Einstellungen**: Geben Sie die Zeit an, die NetScaler ADM warten muss, bevor es nach einem Neustart eine Verbindungsanfrage an die NetScaler ADC-Instanz sendet.

j) Wählen Sie **Create**.

Fügen Sie ADC-Instanzen zu NetScaler ADM hinzu

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

Um Instanzen hinzuzufügen, müssen Sie entweder den Hostnamen oder die IP-Adresse jeder NetScaler ADC-Instanz oder einen Bereich von IP-Adressen angeben.

Geben Sie für SD-WAN-Instanzen die IP-Adresse der einzelnen Instanzen oder einen Bereich von IP-Adressen an. Beachten Sie, dass NetScaler ADM nur Citrix SD-WAN WO und Citrix SD-WAN PE Editionen unterstützt.

Hinweis

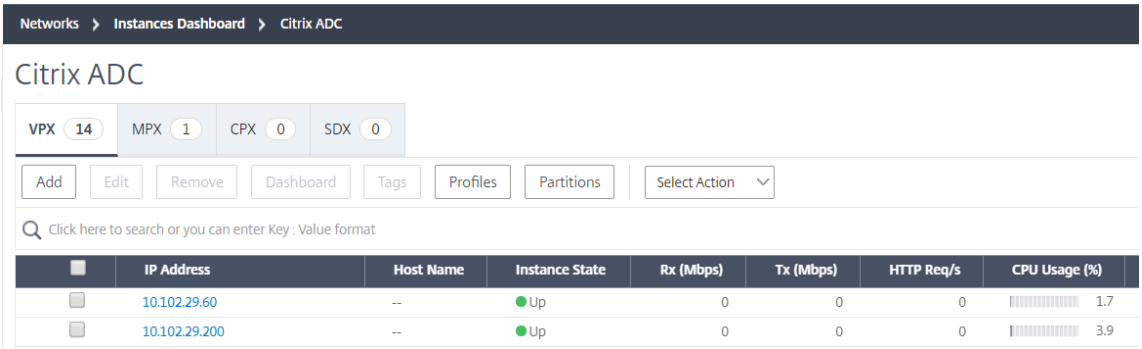
- Um NetScaler ADC-Instanzen hinzuzufügen, die in einem Cluster konfiguriert sind, müssen Sie entweder die Cluster-IP-Adresse oder einen der einzelnen Knoten im Cluster-Setup angeben. In NetScaler ADM wird der Cluster jedoch nur durch die Cluster-IP-Adresse dargestellt.
- Bei NetScaler ADC Instanzen, die als HA-Paar eingerichtet sind, wird beim Hinzufügen einer Instanz automatisch die andere Instanz im Paar hinzugefügt.

Wenn zwei NetScaler ADM-Server im Hochverfügbarkeitsmodus eingerichtet sind und eine Instanz hinzugefügt wird, erfolgt die Verkehrsquelle über die ADM-Floating-IP-Adresse.

Wenn Sie eine Instanz aus Remotedaten hinzufügen, die mit einem On-Prem-Agenten konfiguriert sind, erfolgt die Traffic-Quelle über den ADM-Agenten.

So fügen Sie NetScaler ADM eine Instanz hinzu:

1. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler ADM an.
2. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**. Wählen Sie den Instanztyp aus, den Sie hinzufügen möchten (z. B. NetScaler ADC VPX), und klicken Sie auf **Hinzufügen**.



3. Wählen Sie eine der folgenden Optionen:

   - **Geräte-IP-Adresse eingeben**: Geben Sie für NetScaler ADC Instanzen entweder den Hostnamen oder die IP-Adresse der einzelnen Instanzen oder einen Bereich von IP-Adressen an.

     Wenn Sie mithilfe von SNIP ein ADC-HA-Paar ermitteln möchten, stellen Sie sicher, dass der INC-Modus (Independent Network Configuration) aktiviert ist. Und geben Sie die SNIP-Adressen im folgenden Format an:

     ```
     <SNIP of primary instance>#<SNIP of secondary instance>
     <!--NeedCopy-->
     ```

     Beispiel: `10.10.10.11#10.10.10.12`

Geben Sie für SD-WAN-Instanzen die IP-Adresse jeder Instanz oder einen Bereich von IP-Adressen an.

- **Aus Datei importieren**—Laden Sie von Ihrem lokalen System eine Textdatei hoch, die die IP-Adressen aller Instanzen enthält, die Sie hinzufügen möchten.

4. Wählen Sie unter **Profilname** das entsprechende Instanzprofil aus, oder erstellen Sie ein neues Profil, indem Sie auf das Symbol + klicken.
5. Wählen Sie unter **Site** den Standort aus, an dem Sie die Instanz hinzufügen möchten, oder erstellen Sie einen neuen Standort, indem Sie auf das Symbol **+** klicken.
6. Klicken Sie auf**OK**, um das Hinzufügen von Instanzen zu NetScaler ADM zu starten.

> **Hinweis**
>
> Wenn Sie eine Instanz wiederfinden möchten, navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC**. Wählen Sie den Instanztyp aus (z. B. VPX), wählen Sie die Instanz aus, die Sie neu ermitteln möchten, und klicken Sie dann in der Liste **Aktion auswählen** auf **Wiedererkennen**.

Hinzufügen von ADC CPX-Instanzen zu NetScaler ADM

NetScaler ADM wurde verbessert, um die Verbesserungen der CPX-Funktionen zu unterstützen. Die NetScaler ADC CPX-Instanz wird jetzt in NetScaler ADM hinzugefügt, indem eine IP-Adresse für die CPX zusammen mit einem Geräteprofil bereitgestellt wird. Das Hinzufügen einer CPX-Instanz ähnelt jetzt dem Hinzufügen anderer ADC-Typen wie VPX oder MPX in ADM. Außerdem wurde die Registrierung von CPX in ADM verbessert. Wenn ein CPX gestartet wird, erkennt und registriert NetScaler ADM automatisch die CPX-Instanz. Eine CPX-Instanz wird nicht mehr über Docker Host erkannt.

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC** und klicken Sie auf die Registerkarte **CPX**.
2. Klicken Sie auf **Hinzufügen**, um neue CPX-Instanzen in NetScaler ADM hinzuzufügen.
3. Die Seite **NetScaler ADC CPX** hinzufügen wird geöffnet. Geben Sie die Werte für die folgenden Parameter ein:

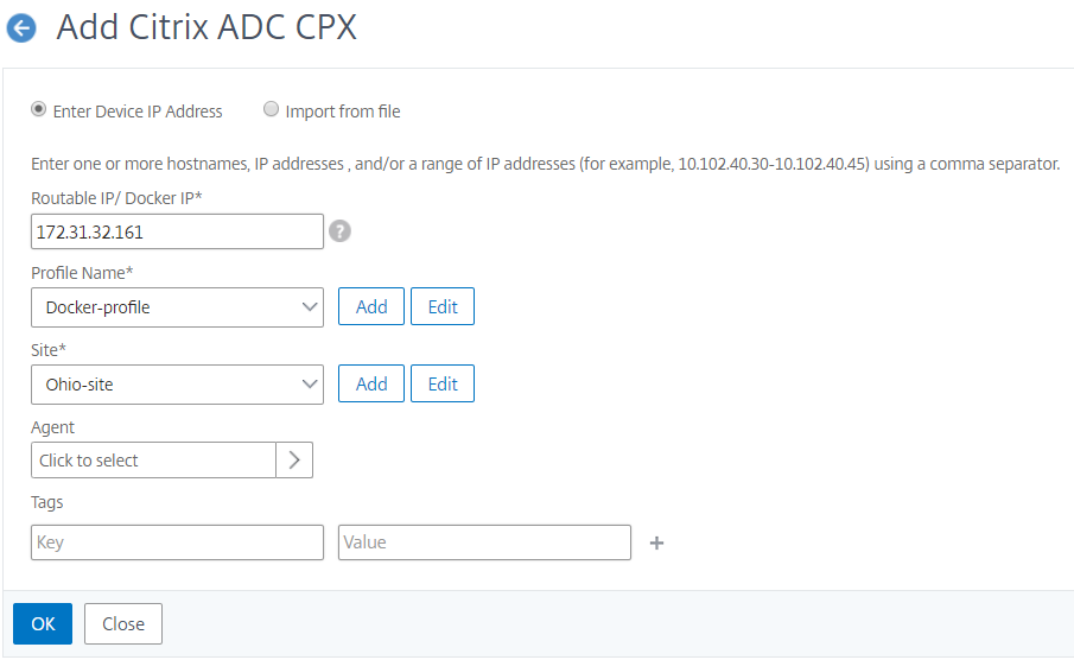
    a) Sie können CPX-Instanzen hinzufügen, indem Sie entweder die erreichbare IP-Adresse der CPX-Instanz oder die IP-Adresse des Docker-Containers angeben, in dem die CPX-Instanz gehostet wird.

    b) Wählen Sie das Profil der CPX-Instanz aus.

    c) Wählen Sie den Standort aus, an dem die Instanzen bereitgestellt werden sollen.

    d) Wählen Sie den Agenten aus.

e) Optional können Sie das Schlüssel-Wert-Paar für die Instanz eingeben. Durch das Hinzufügen von Schlüssel-Wert-Paar können Sie später nach der Instanz suchen.



> **Hinweis**
>
> Für NetScaler ADC CPX-Instanzen müssen Sie beim Erstellen des CPX-Instanzprofils die **HTTP-, HTTPS-, SSH**- und **SNMP-Portdetails** des Hosts angeben. Sie können auch den Portbereich, der vom Host veröffentlicht wurde, in den Feldern **Startport** und **Anzahl der Ports** angeben.

4. Klicken Sie auf **OK**.

Fügen Sie eine eigenständige NetScaler ADC BLX-Instanz in NetScaler ADM hinzu

Eine eigenständige NetScaler ADC BLX-Instanz ist eine einzelne Instanz, die auf dem dedizierten Host-Linux-Server ausgeführt wird.

1. ****Navigieren Sie zu Netzwerke > **Instanzen** > **Citrix ADC** .
2. Klicken Sie auf der Registerkarte **BLX** auf **Hinzufügen**.
3. Wählen Sie in der Liste **Instanztyp** die Option **Standalone** aus.
4. Geben Sie im Feld **IP-Adresse** die IP-Adresse der BLX-Instanz an.
5. Geben Sie im Feld **Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die BLX-Instanz gehostet wird.

6. Wählen Sie in der Liste **Profilname** das entsprechende Profil für eine BLX-Instanz aus, oder erstellen Sie ein Profil.

   Um ein Profil zu erstellen, klicken Sie auf **Hinzufügen**.

   > **Wichtig**
   >
   > Stellen Sie sicher, dass Sie den richtigen Host-Benutzernamen und das richtige Kennwort des Linux-Servers im Profil angegeben haben.

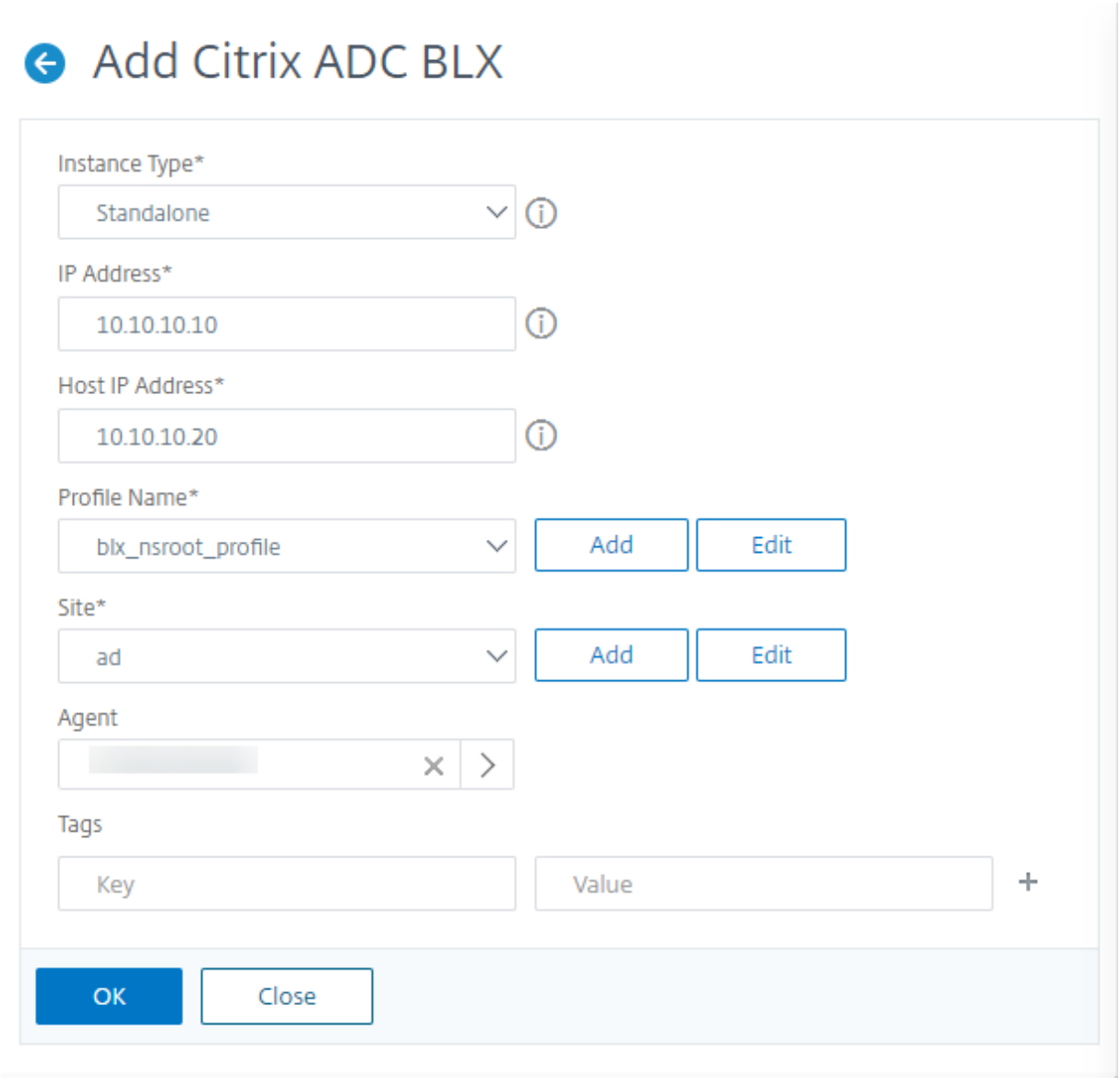
7. Wählen Sie in der Liste **Site** die Site aus, der Sie eine Instanz hinzufügen möchten.

   Wenn Sie eine Site hinzufügen möchten, klicken Sie auf **Hinzufügen**.

8. Wählen Sie in der Liste **Agent** den NetScaler ADM Agent aus, dem Sie die Instanz zuordnen möchten.

   Wenn auf Ihrem NetScaler ADM nur ein Agent konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.

9. Klicken Sie auf **OK**.



Fügen Sie hochverfügbare NetScaler ADC BLX-Instanzen in NetScaler ADM hinzu

Die hochverfügbaren NetScaler ADC BLX-Instanzen, die auf verschiedenen Host-Linux-Servern ausgeführt werden. Ein Linux-Server kann nicht mehr als eine BLX-Instanzen hosten.

1. Klicken Sie auf der Registerkarte **BLX** auf **Hinzufügen**.
2. Wählen Sie die Option **Hochverfügbarkeit** aus der Liste **Instanztyp** aus.
3. Geben Sie im Feld **IP-Adresse** die IP-Adresse der BLX-Instanz an.
4. Geben Sie im Feld **Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die BLX-Instanz gehostet wird.

5. Geben Sie im Feld **Peer-IP-Adresse** die IP-Adresse der Peer-BLX-Instanz an.
6. Geben Sie im Feld **Peer-Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die Peer-BLX-Instanz gehostet wird.
7. Wählen Sie in der Liste **Profilname** das entsprechende Profil für eine BLX-Instanz aus, oder erstellen Sie ein Profil.

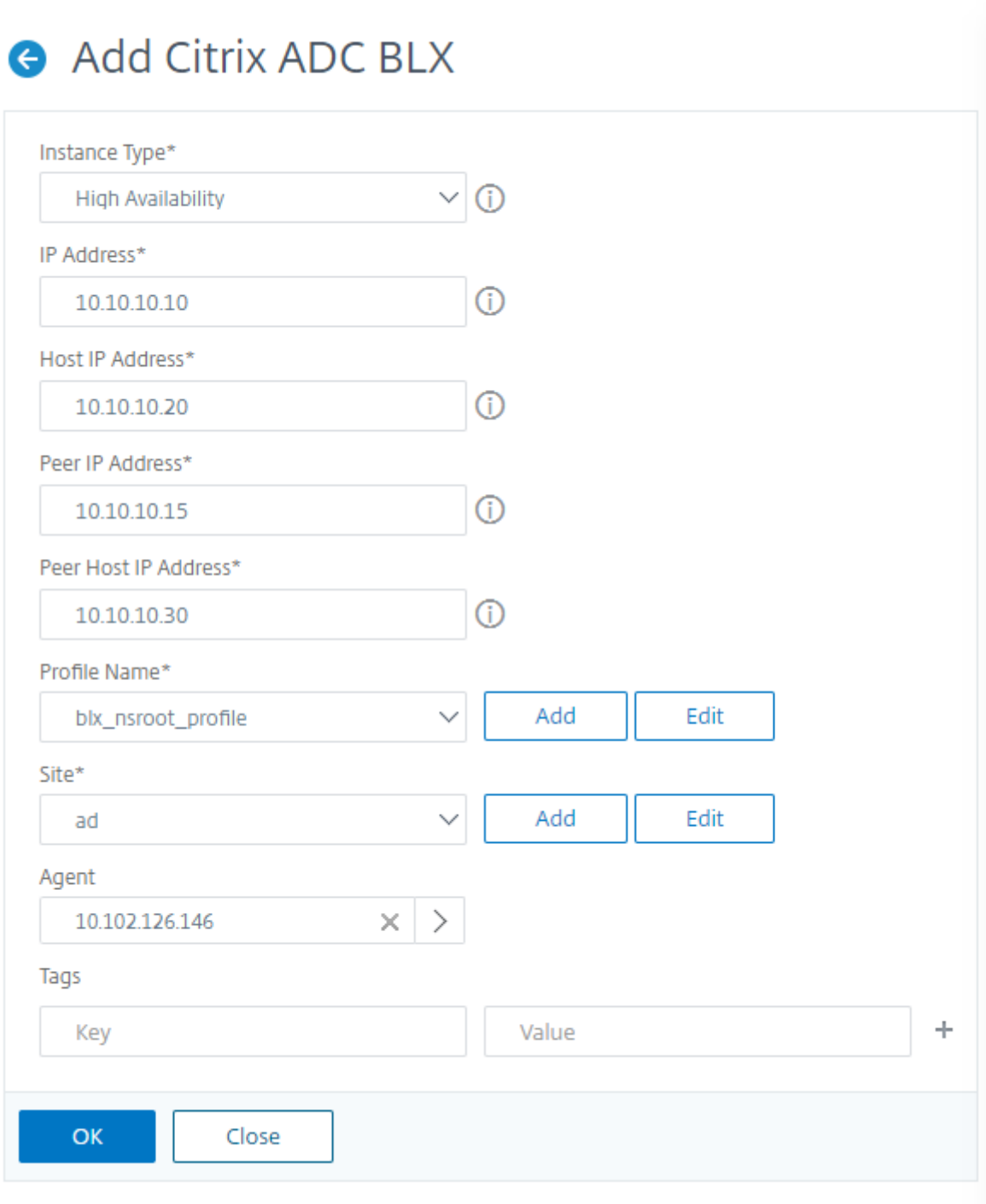
   Um ein Profil zu erstellen, klicken Sie auf **Hinzufügen**.

   > **Wichtig**
   >
   > Stellen Sie sicher, dass Sie den richtigen Host-Benutzernamen und das richtige Kennwort des Linux-Servers im Profil angegeben haben.

8. Wählen Sie in der Liste **Site** die Site aus, der Sie eine Instanz hinzufügen möchten.

   Wenn Sie eine Site hinzufügen möchten, klicken Sie auf **Hinzufügen**.
9. Wählen Sie in der Liste **Agent** den NetScaler ADM Agent aus, dem Sie die Instanz zuordnen möchten.

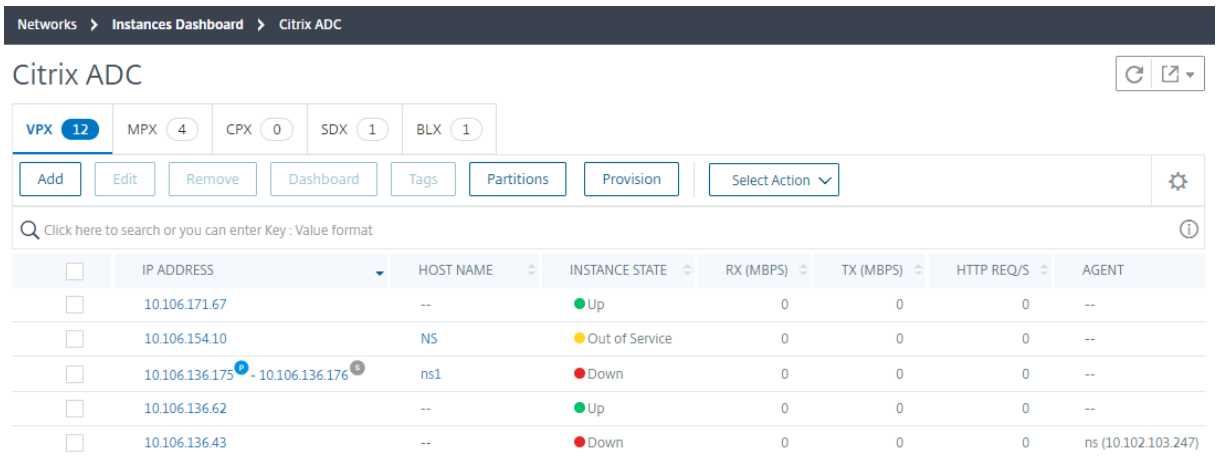
   Wenn auf Ihrem NetScaler ADM nur ein Agent konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.
10. Klicken Sie auf **OK**.



Zugriff auf eine Instanz-GUI über das NetScaler ADM

1. Navigieren Sie zu **Netzwerke > Instanzen** > **Citrix ADC**.
2. Wählen Sie den Instanztyp aus, auf den Sie zugreifen möchten (z. B. VPX, MPX, CPX, SDX oder BLX).

3. Klicken Sie auf die erforderliche NetScaler ADC IP-Adresse oder den Hostnamen.



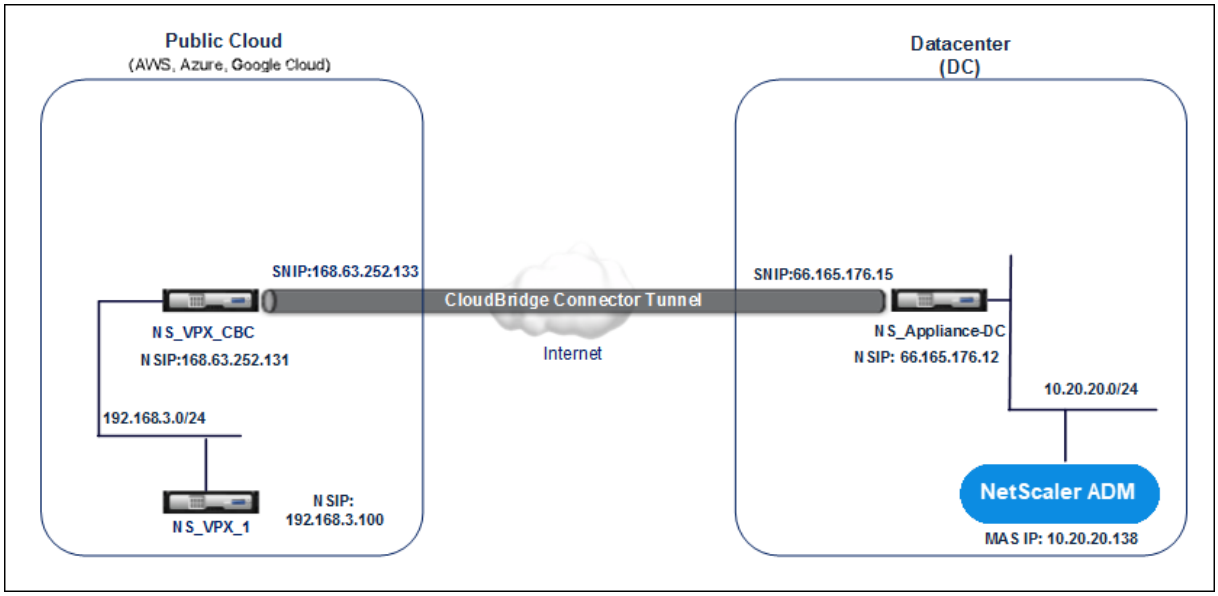
Die GUI der ausgewählten Instanz wird in einem Popup-Fenster angezeigt.

Hinzufügen von NetScaler ADC VPX Instanzen, die in der Cloud bereitgestellt werden, zu NetScaler ADM

February 5, 2024

Sie können Citrix ADM verwenden, um die Citrix ADC VPX Instanzen zu verwalten und zu überwachen, die in einer öffentlichen Cloud wie Amazon Web Services (AWS) oder Microsoft Azure bereitgestellt werden. Sie müssen Layer 3-Konnektivität zwischen NetScaler ADM und den in der Public Cloud bereitgestellten NetScaler ADC VPX-Instanzen herstellen. Um die Layer-3-Konnektivität herzustellen, können Sie Lösungen wie Citrix CloudBridge Connector, Citrix SD-WAN, Direct Connect to AWS, VPN in Azure oder Connectors von Drittanbietern wie Equinix usw. verwenden.

Die folgende Beispieltopologie verwendet Citrix CloudBridge Connector für Layer 3-Konnektivität zwischen NetScaler ADM und den in der Cloud bereitgestellten NetScaler ADC VPX-Instanzen.



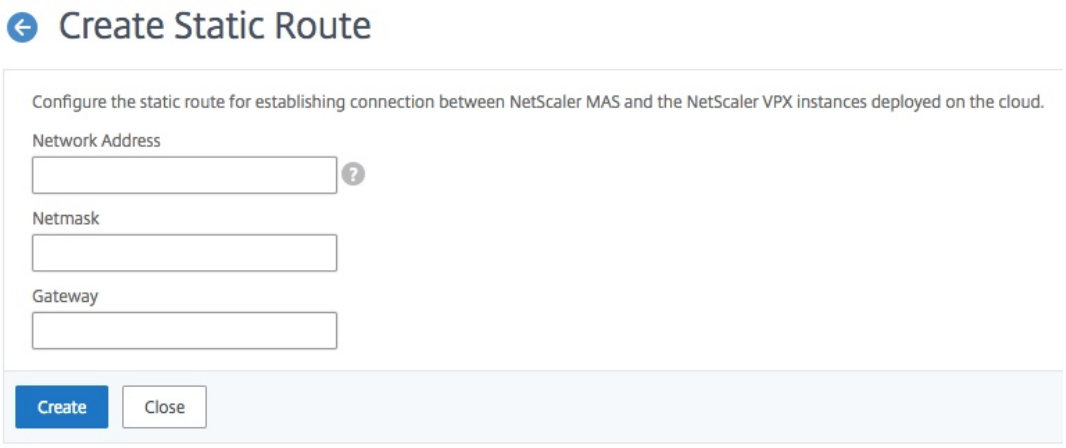
Ein Citrix CloudBridge Connector-Tunnel wird zwischen der NetScaler ADC Appliance ns_Appliance-DC, im Rechenzentrum DC und der virtuellen NetScaler ADC Appliance (VPX) NS_VPX_CBC in der Public Cloud eingerichtet. NS_Appliance-DC und NS_VPX_CBC ermöglichen die Kommunikation zwischen NetScaler ADM und der NetScaler ADC VPX Instanz, NS_VPX_1, die in der Public Cloud bereitgestellt wird. Nachdem die Kommunikation hergestellt wurde, können Sie NS_VPX_1 in NetScaler ADM entdecken.

Gehen Sie wie folgt vor, um diese Topologie zu konfigurieren:

1. Installieren, konfigurieren und starten Sie eine NetScaler ADC VPX Instanz in der Public Cloud.
   - Anweisungen findenSie unter Installieren von NetScaler ADC VPX auf AWS.
   - Anweisungen finden Sie unter Installieren von NetScaler ADC VPX auf Microsoft Azure.
2. Stellen Sie eine physische NetScaler ADC Appliance bereit und konfigurieren Sie sie oder stellen Sie eine virtuelle NetScaler ADC Appliance (VPX) auf einer Virtualisierungsplattform im Rechenzentrum bereit und konfigurieren Sie sie.
   - Anweisungen finden Sie unter Installieren einer NetScaler ADC VPX-Instanz auf Citrix Hypervisor.
   - Anweisungen finden Sie unter Installieren virtueller Citrix Appliances auf VMware ESXi.
   - Anweisungen finden Sie unter Installieren virtueller NetScaler ADC Appliances auf Microsoft Hyper-V.
3. Konfigurieren Sie den Citrix CloudBridge Connector zwischen dem Rechenzentrum und der Public Cloud. Anweisungen finden Sie unter Konfigurieren von Citrix CloudBridge Connector.
4. Konfigurieren Sie die statische Route zum Herstellen einer Verbindung zwischen NetScaler ADM und den in der Cloud bereitgestellten NetScaler ADC VPX Instanzen wie folgt:

a) Melden Sie sich bei Citrix ADM an.

b) Navigieren Sie zu **System > Statische Routen**, und klicken Sie auf **Hinzufügen**.



c) Geben Sie im Feld **Netzwerkadresse** die Adresse des Netzwerks ein, für das Sie eine statische Route von NetScaler ADM über den Connector einrichten möchten.

d) Geben Sie im Feld **Netzmaske** die Netzmaske für das Netzwerk ein.

e) Geben Sie im Feld **Gateway** die Adresse des Gateways ein.

5. Fügen Sie die NetScaler ADC VPX Cloudinstanzen zum NetScaler ADM hinzu, indem Sie den Bereich der IP-Adressen von NetScaler ADC VPX Instanzen in der Public Cloud angeben. Ausführliche Anweisungen finden Sie unter Instanzen zu NetScaler ADM hinzufügen.

Lizenzierung verwalten und Analysen auf virtuellen Servern aktivieren

February 5, 2024

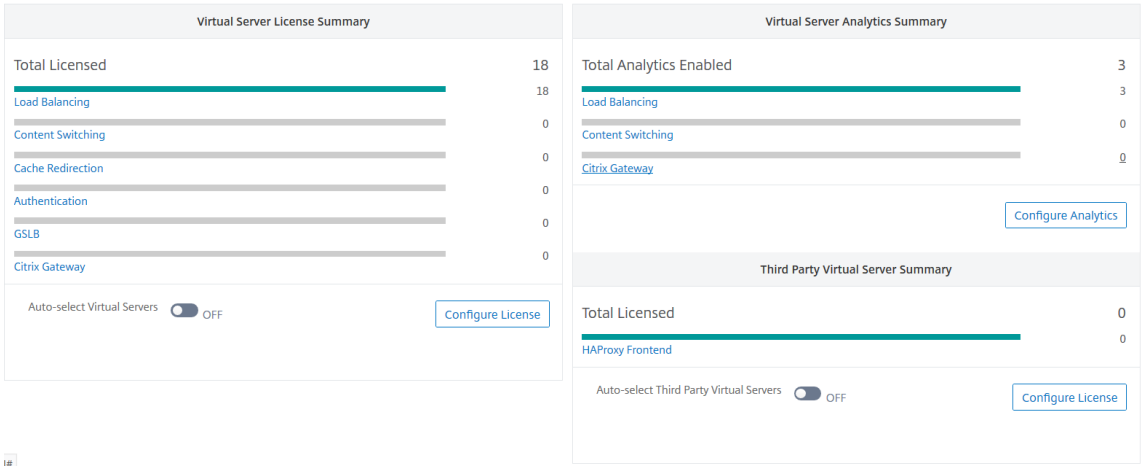
> **Hinweis**
>
> - Die folgenden Informationen und Vorgehensweisen zum Aktivieren von Analysen sind nur anwendbar, wenn Ihre NetScaler ADM-Version **13.0 Build 41.x** oder höher ist. Wenn Ihre NetScaler ADM-Version vor **13.0 Build 36.27**liegt, finden Sie weitere Informationen unter Analytics aktivieren.
> - Standardmäßig ist die Option **Automatisch lizenzierte virtuelle Server** aktiviert. Sie müssen sicherstellen, dass Sie über ausreichende Lizenzen verfügen, um die virtuellen Server zu lizenzieren. Wenn Sie über begrenzte Lizenzen verfügen und nur die ausgewählten virtuellen Server basierend auf Ihren Anforderungen lizenzieren möchten,

> deaktivieren Sie die Option **Automatisch lizenzierte virtuelle Server** . Navigieren Sie zu **Systeme > Lizenzierung und Analytics** und deaktivieren Sie die Option **Automatisch lizenzierte virtuelle Server** unter **Zuweisung virtueller Serverlizenzen**.

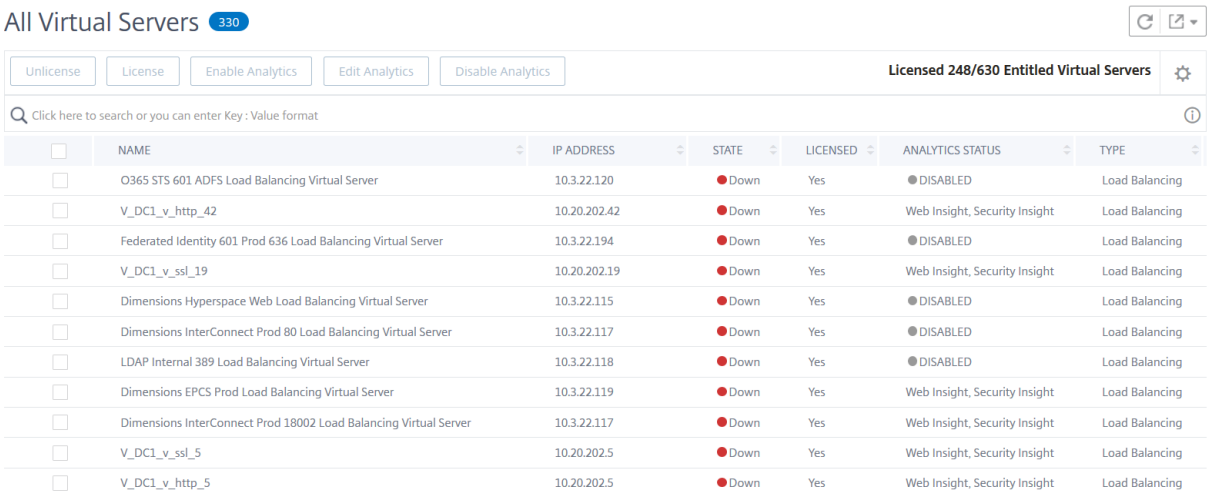
Der Prozess der Aktivierung von Analysen wird vereinfacht. Sie können jetzt den virtuellen Server lizenzieren und Analysen in einem einzigen Workflow aktivieren.

Navigieren Sie zu **System** > **Licensing & Analytics**, um:

- Übersicht über **virtuelle Server-Lizenzen** anzeigen
- Zusammenfassung der **Virtual Server Analytics** anzeigen



Wenn Sie auf **Lizenz konfigurieren** oder **Analytics konfigurieren**klicken, wird die Seite **Alle virtuellen Server** angezeigt.



Auf der Seite **Alle virtuellen Server** können Sie:

- Lizenz für nicht lizenzierte virtuelle Server beantragen
- Lizenz für lizenzierte virtuelle Server entfernen

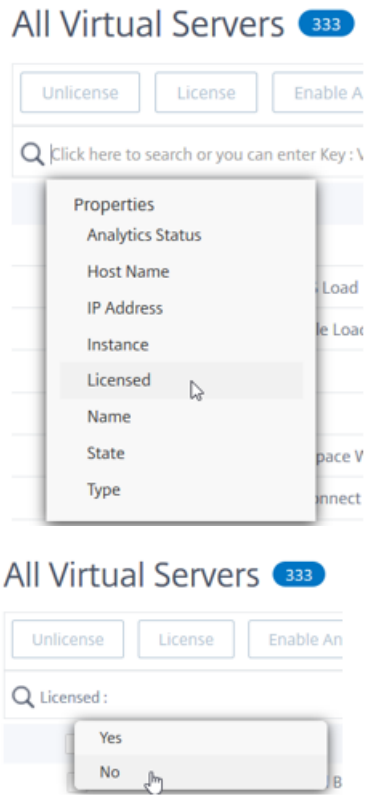
- Analytik auf lizenzierten virtuellen Servern aktivieren
- Analytics bearbeiten
- Analytics deaktivieren

> **Hinweis**
>
> Die unterstützten virtuellen Server zum Aktivieren von Analysen sind Load Balancing, Content Switching und NetScaler Gateway.

Verwalten der Lizenzierung auf virtuellen Servern

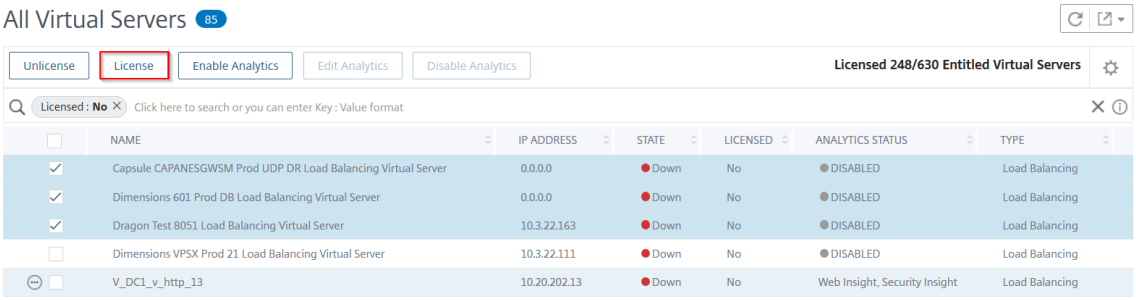
So lizenzieren Sie die virtuellen Server auf der Seite **Alle virtuellen Server** :

1. Klicken Sie auf die Suchleiste, wählen Sie **Lizenziert**und dann **Nein**aus.



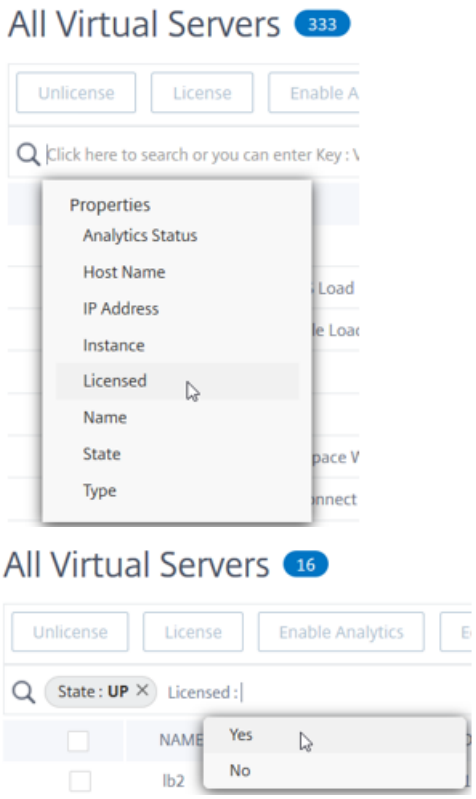
   Der Filter wird jetzt angewendet und nur die nicht lizenzierten virtuellen Server werden angezeigt.

2. Wählen Sie die virtuellen Server aus und klicken Sie dann auf **Lizenz**.

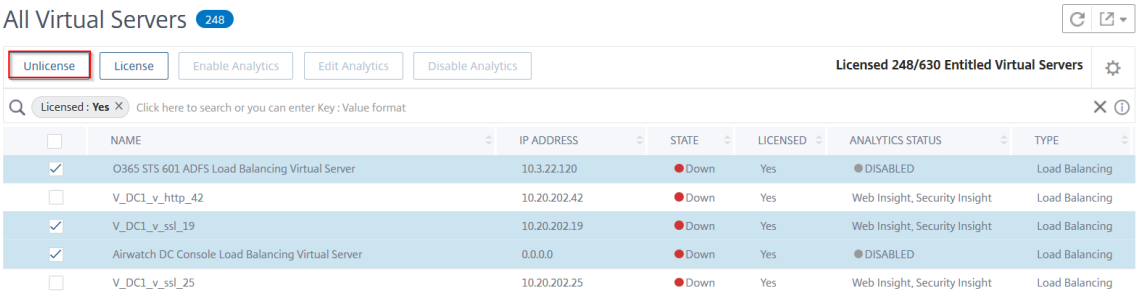


Um die Lizenz der virtuellen Server aufzuheben, gehen Sie auf der Seite **Alle virtuellen Server** wie folgt vor:

1. Klicken Sie auf die Suchleiste, wählen Sie **Lizenziert**und wählen Sie **Ja**aus.



2. Wählen Sie die virtuellen Server aus, und klicken Sie auf **Lizenz aufheben**.



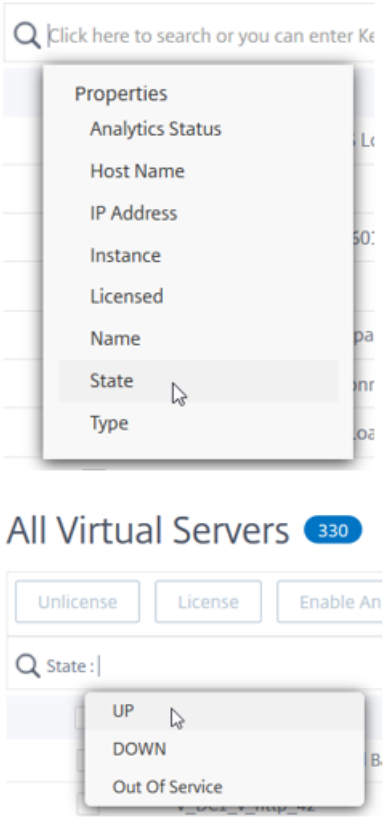
Analytics aktivieren

Im Folgenden sind die Voraussetzungen für die Aktivierung von Analysen für virtuelle Server aufgeführt:

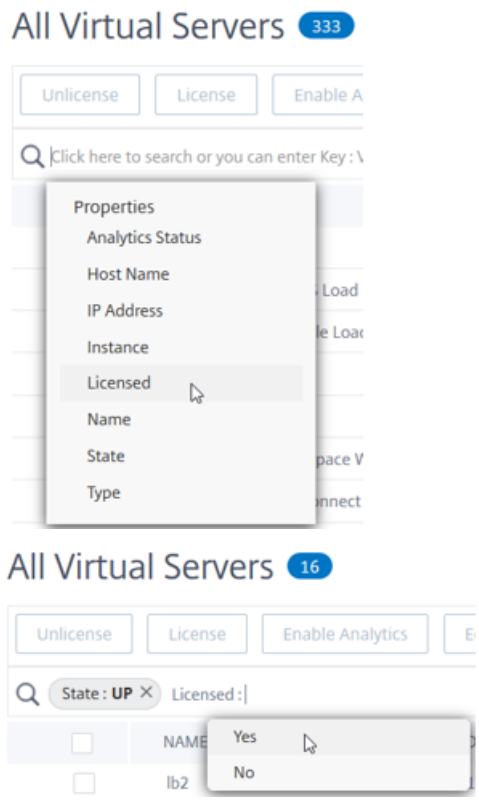
- Sicherstellen, dass virtuelle Server **lizenziert** sind
- Stellen Sie sicher, dass Analysestatus **Deaktiviert**
- Stellen Sie sicher, dass virtuelle Server im Status **UP** sind

Sie können die Ergebnisse filtern, um die virtuellen Server zu identifizieren, die in den Voraussetzungen erwähnt werden.

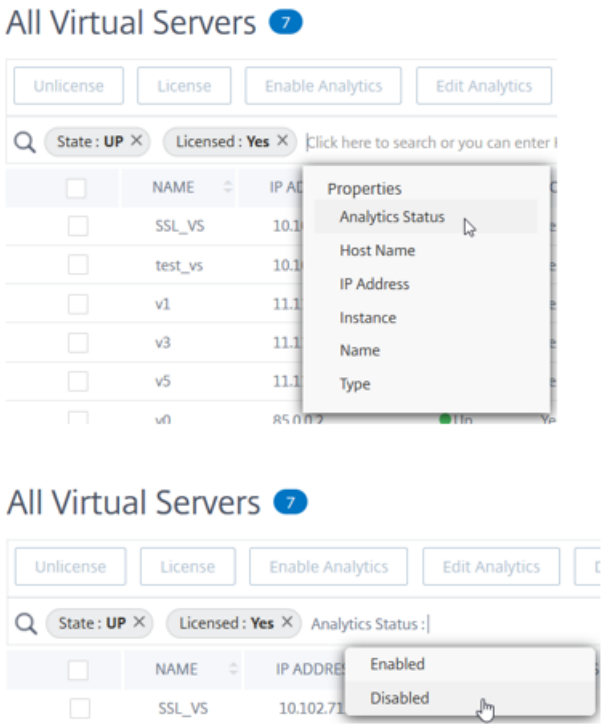
1. Klicken Sie auf die Suchleiste, wählen Sie **Status** und dann **UP**aus.



2. Klicken Sie auf die Suchleiste, wählen Sie **Lizenziert** aus, und wählen Sie dann **Ja** aus.

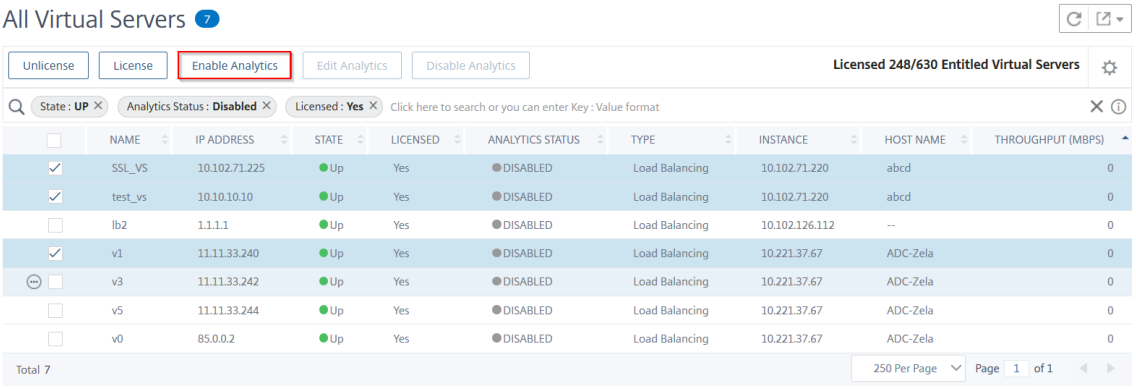


3. Klicken Sie auf die Suchleiste, wählen Sie **Analytics-Status** aus, und wählen Sie dann **Deaktiviert** aus.



4. Wählen Sie nach dem Anwenden der Filter die virtuellen Server aus und klicken Sie dann auf

Analytics aktivieren.



> **Hinweis**
>
> Alternativ können Sie Analysen für eine bestimmte Instanz aktivieren:
>
> ```
> 1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC** und wählen Sie dann den Instanz-Typ aus. Zum Beispiel VPX.
>
> 1. Wählen Sie die Instanz aus und wählen Sie in der Liste **„Aktion auswählen** “ die Option **Analytics konfigurieren** aus.
> 1. Wählen Sie auf der Seite „Analytics auf virtuellen Servern konfigurieren “ den virtuellen Server aus und klicken Sie auf **Analytics aktivieren**.
> ```

5. Gehen Sie im Fenster **Enable Analytics** wie folgt vor:

   a) Wählen Sie die Insight-Typen (Web Insight oder Security Insight)

   b) Wählen Sie **Logstream** als Transportmodus

   > **Hinweis**
   >
   > Für NetScaler ADC 12.0 oder früher ist **IPFIX** die Standardoption für den Transportmodus. Für NetScaler ADC 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.
   >
   > Weitere Informationen zu IPFIX und Logstream finden Sie unter Logstream-Übersicht .

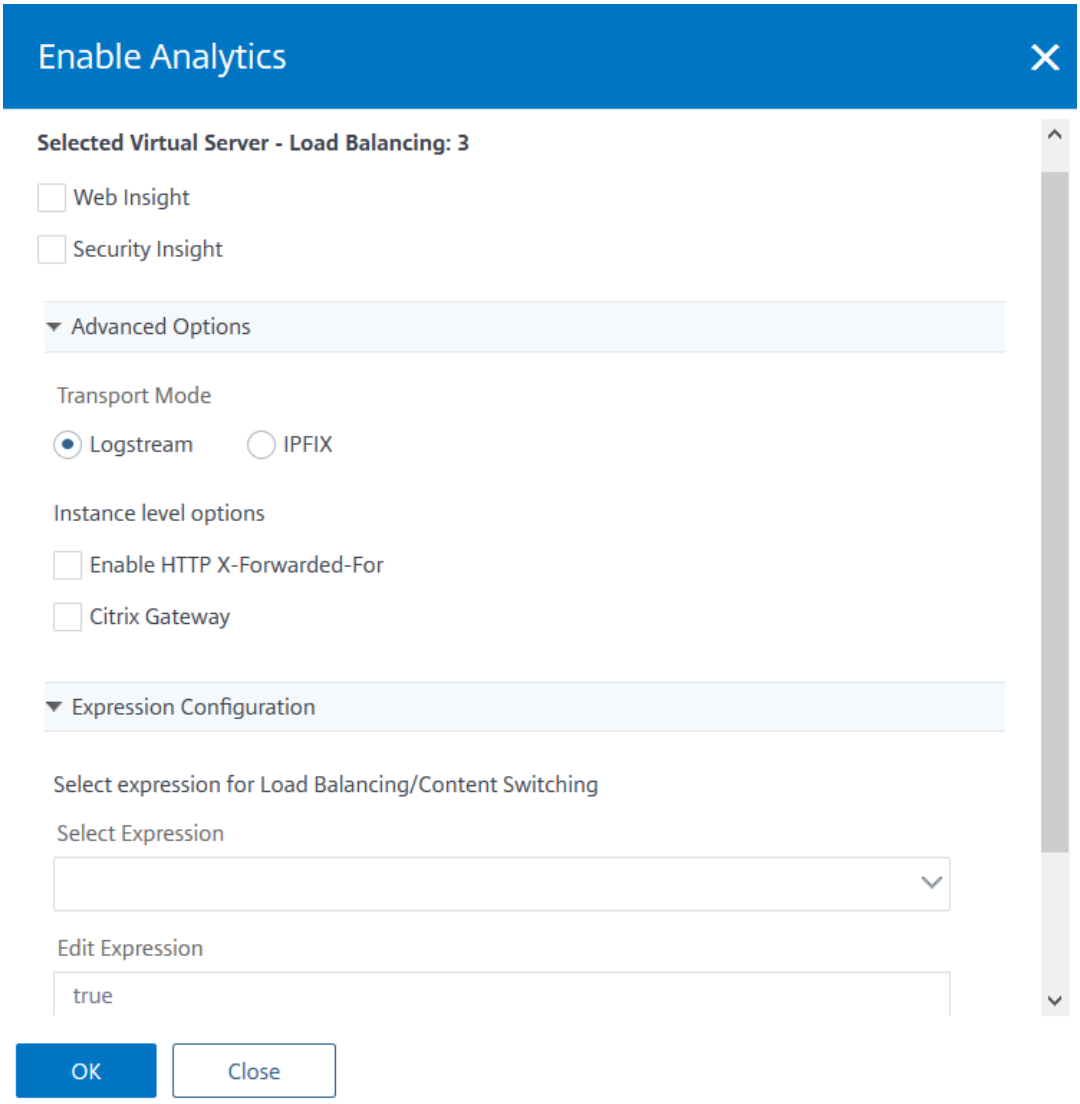
   c) Unter **Optionen auf Instanzebene**:

   - **HTTP X-Forwarded-For aktivieren** —Wählen Sie diese Option aus, um die IP-Adresse für die Verbindung zwischen Client und Anwendung über den HTTP-Proxy oder den Load Balancer zu ermitteln.

- **NetScaler Gateway** —Wählen Sie diese Option aus, um Analysen für NetScaler Gateway anzuzeigen.

d) Der Ausdruck ist standardmäßig wahr

e) Klicken Sie auf **OK**.

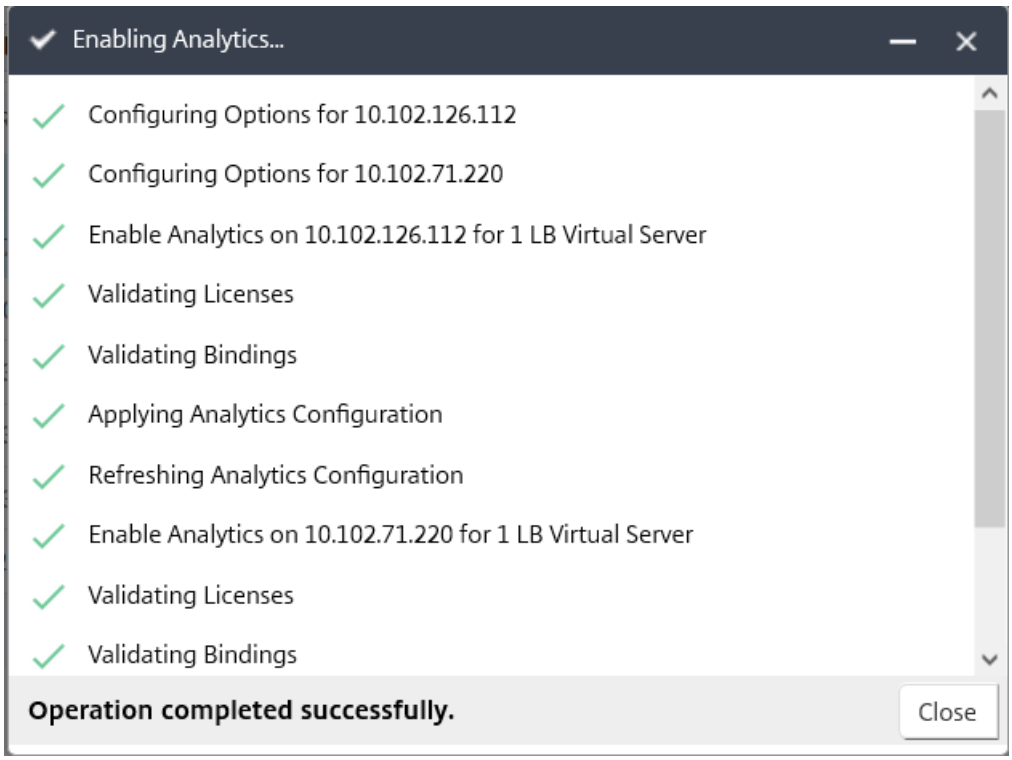


Hinweis

- Wenn Sie virtuelle Server auswählen, die nicht lizenziert sind, lizenziert NetScaler ADM zuerst diese virtuellen Server und aktiviert dann Analysen.
- Für Admin-Partitionen wird nur **Web Insight** unterstützt
- Für virtuelle Server wie Cache-Umleitung , Authentifizierung und GSLB können Sie Analysen nicht aktivieren. Eine Fehlermeldung wird angezeigt.

Nachdem Sie auf **OK** geklickt haben, verarbeitet NetScaler ADM Analysen auf den ausgewählten

virtuellen Servern zu aktivieren.



> **Hinweis**
>
> Citrix ADM verwendet Citrix ADC SNIP für Logstream und NSIP für IPFIX. Wenn zwischen dem Citrix ADM Agent und der Citrix ADC-Instanz eine Firewall aktiviert ist, stellen Sie sicher, dass Sie den folgenden Port öffnen, damit Citrix ADM AppFlow-Verkehr sammeln kann:

Transport-Modus	Quell-IP	Typ	Port
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

Analytics bearbeiten

So bearbeiten Sie Analysen auf den virtuellen Servern:

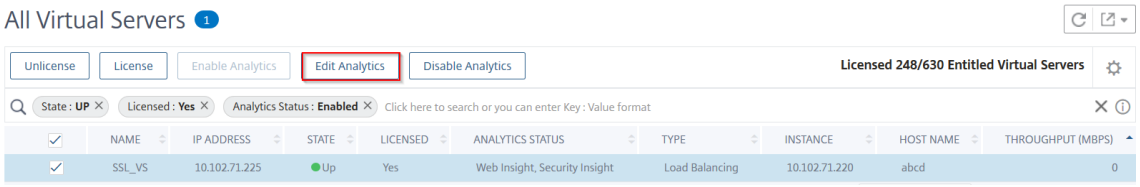
1. Wählen Sie die virtuellen Server aus

   > Hinweis
   >
   > Alternativ können Sie auch Analysen für eine bestimmte Instanz bearbeiten:
   >
   > ```
   > 1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC** und wählen Sie dann den Instanz-Typ aus.
   > ```



```
    Zum Beispiel VPX.
2
3 1.  Wählen Sie die Instanz aus und klicken Sie auf **Analytics
      bearbeiten**.
```

2. Klicken Sie auf **Analytics bearbeiten**

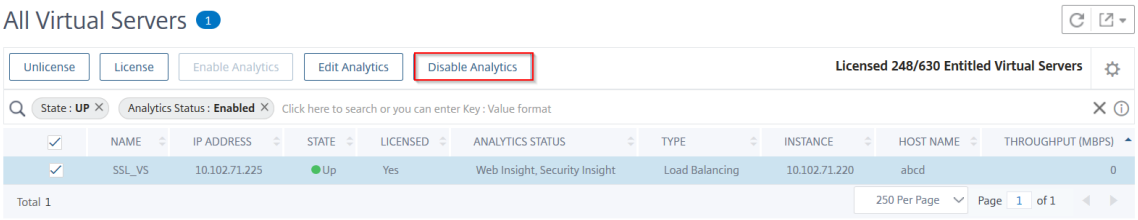


3. Bearbeiten Sie die Parameter, die Sie anwenden möchten, im Fenster **"Analytics-Konfiguration bearbeiten** "
4. Klicken Sie auf **OK**.

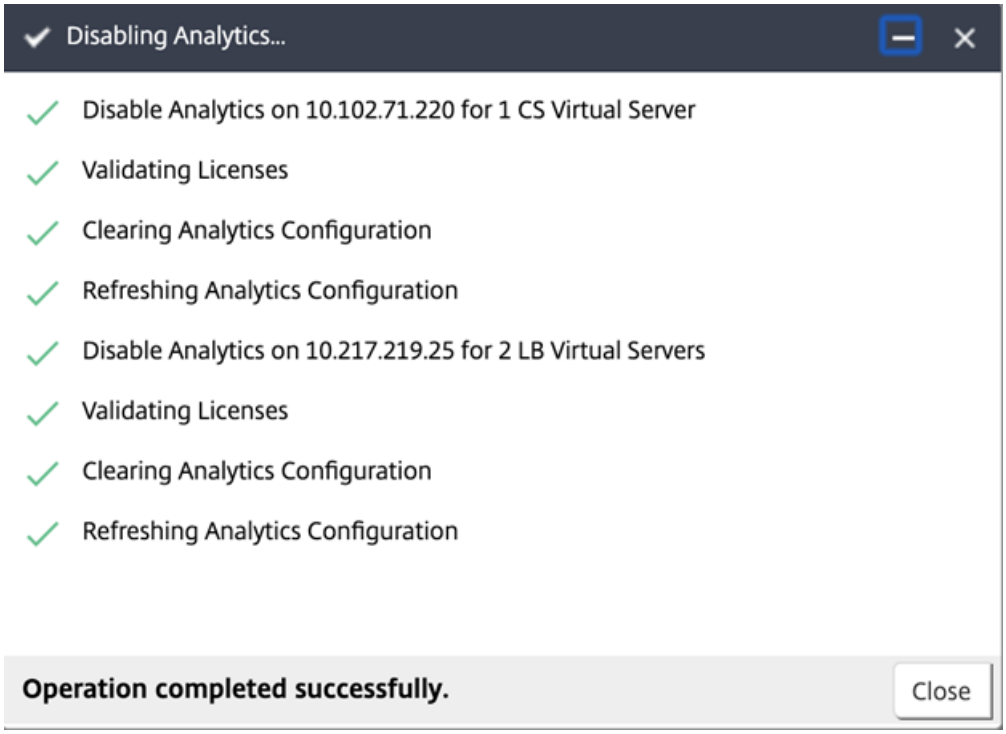
Analytics deaktivieren

So deaktivieren Sie Analysen auf den ausgewählten virtuellen Servern:

1. Wählen Sie die virtuellen Server aus
2. Klicken Sie auf **Analytics deaktivieren**



NetScaler ADM deaktiviert die Analyse auf den ausgewählten virtuellen Servern



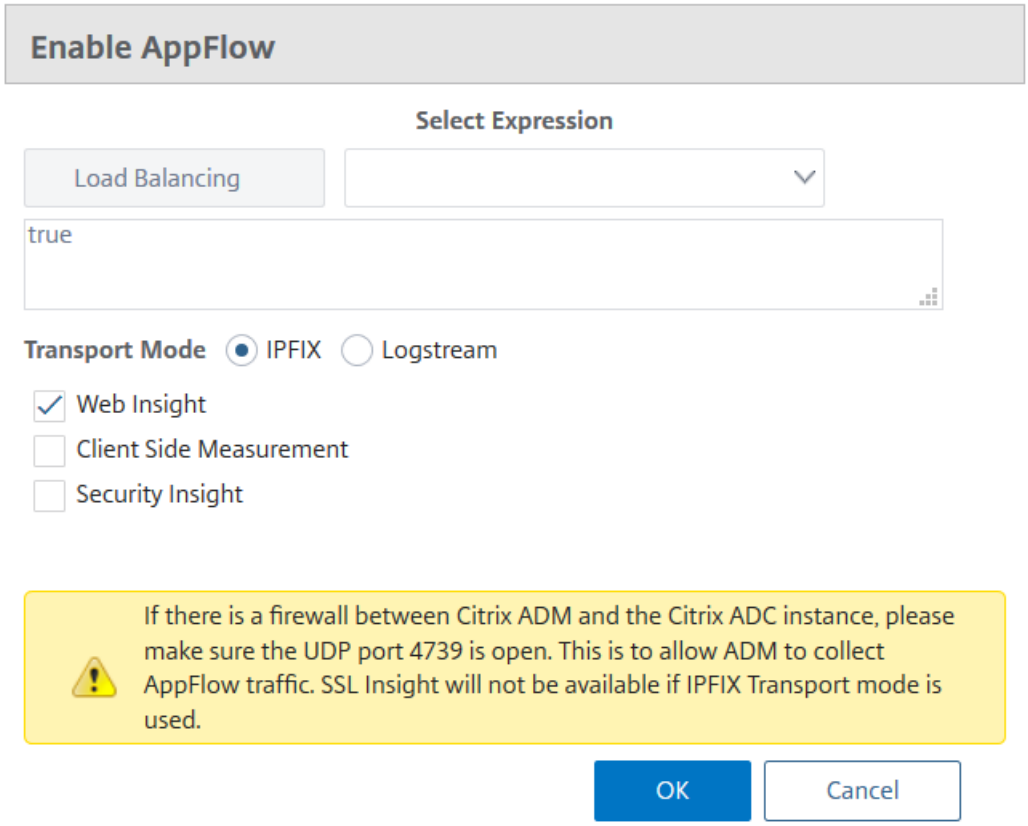
In der folgenden Tabelle werden die Features von NetScaler ADM beschrieben, die IPFIX und Logstream als Transportmodus unterstützen:

Feature	IPFIX	Logstream
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Nicht unterstützt	•
CR-Einblick	•	•
IP-Reputation	•	•
AppFirewall	•	•
Kundenseitige Messung	•	•
Syslog/Auditlog	•	•

Aktivieren Sie Analysen auf virtuellen Servern für frühere Builds

Um Analysen auf virtuellen Servern für **Citrix ADM 13.0 Build**36.27 zu aktivieren:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**und wählen Sie die Citrix ADC-Instanz aus, für die Sie Analysen aktivieren möchten.
2. Wählen Sie in der Liste der Instanzen eine Instanz aus.
3. **Wählen Sie in der Liste Aktion** auswählen die Option **Analytics konfigurieren**aus.
4. Wählen Sie in der Anwendungsliste die virtuellen Server aus und klicken Sie auf **AppFlow aktivieren**.
5. Geben Sie im Feld **AppFlow aktivieren** den Wert true ein und wählen Sie basierend auf den Analysen, die Sie aktivieren möchten, Security Insight oder Web Insight oder beides aus.

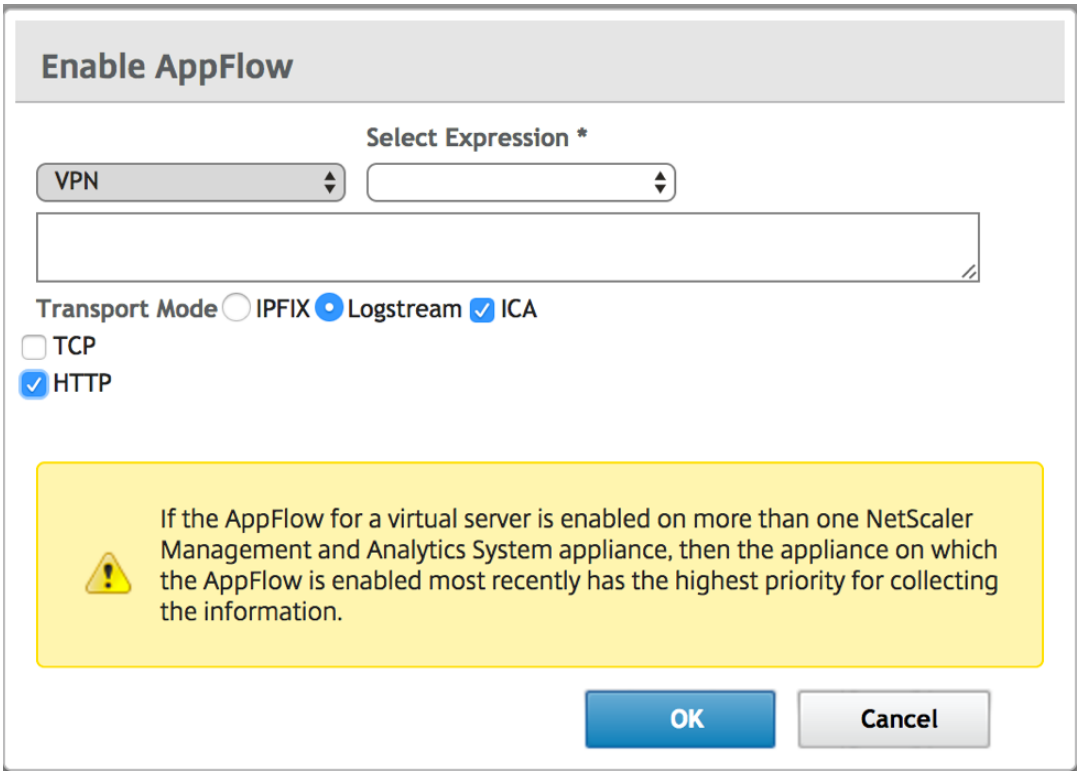


> **Hinweis**
>
> Citrix ADM verwendet Citrix ADC SNIP für Logstream und NSIP für IPFIX. Wenn zwischen der NetScaler ADM und der NetScaler ADC Instanz eine Firewall aktiviert ist, stellen Sie sicher, dass Sie den folgenden Port öffnen, damit NetScaler ADM AppFlow Datenverkehr erfassen kann:

Transport-Modus	Quell-IP	Typ	Port
IPFIX	NSIP	UDP	4739

Transport-Modus	Quell-IP	Typ	Port
Logstream	SNIP	TCP	5557

- Für HDX Insight und Gateway Insight müssen Sie beim Klicken auf AppFlow aktivieren den virtuellen VPN-Server auswählen, der auf Ihrer NetScaler ADC-Instanz konfiguriert ist, und die entsprechenden Kontrollkästchen für das Protokoll ICA oder HTTP aktivieren.



- Navigieren Sie für TCP Insight zu **System** > **Analytics-Einstellungen** > **Features konfigurieren**und wählen Sie **TCP Insight aktivieren**aus.
- Für Video Insight müssen Sie die Konfigurationsänderungen auf der NetScaler ADC Appliance vornehmen. Weitere Informationen zum Aktivieren von Analysen für Video Insight finden Sie unter Video Insight.
- Für WAN Insight:
  - Navigieren Sie zu **Infrastruktur > Instanzen > Citrix SD-WAN WO**, und wählen Sie die WAN-Optimierungs-Appliance für Rechenzentren aus.
  - Wählen Sie in der Liste **Aktion** die Option **Insight aktivieren**aus.
  - Wählen Sie die folgenden Parameter nach Bedarf aus:
    - Geodatenerfassung für HDX Insight: Teilt die Client-IP-Adresse mit der Google Geo API.

* AppFlow: Beginnt mit dem Sammeln von Daten aus WAN-Optimierungsinstanzen.
  - TCP und WANOpt: Stellt TCP- und WanOpt Insight-Berichte bereit.
  - HDX: Stellt HDX Insight-Berichte bereit.
  - TCP nur für HDX: Bietet TCP nur für HDX Insight Berichte.

Sie können den AppFlow-Transportmodus zu **IPFIX** oder **Logstream** auswählen, während Sie AppFlow auf den erkannten NetScaler ADC-Instanzen in NetScaler ADM aktivieren. Weitere Informationen zu IPFIX und Logstream finden Sie unter Logstream-Übersicht .

In der folgenden Tabelle werden die Features von NetScaler ADM beschrieben, die IPFIX und Logstream als Transportmodus unterstützen:

Feature	IPFIX	Logstream
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Nicht unterstützt	•
CR-Einblick	•	•
IP-Reputation	•	•
AppFirewall	•	•
Kundenseitige Messung	•	•
Syslog/Auditlog	•	•

Sie können die Verarbeitung des Web Insight-Datenverkehrs auch aktivieren oder deaktivieren, indem Sie die Option Enable Web Insight in Citrix ADM verwenden. Wenn Sie den Web Insight-Datenverkehr nicht überwachen möchten, können Sie die Option deaktivieren. NetScaler ADM verarbeitet den Web Insight-Datenverkehr von den virtuellen Servern auf den verwalteten Instanzen nicht.

NTP-Server konfigurieren

February 5, 2024

Sie können einen NTP-Server (Network Time Protocol) in Citrix ADM konfigurieren, um seine Uhr mit dem NTP-Server zu synchronisieren. Durch die Konfiguration eines NTP-Servers wird sichergestellt,

dass die NetScaler ADM Uhr dieselben Datums- und Uhrzeiteinstellungen wie die anderen Server im Netzwerk aufweist.

So konfigurieren Sie einen NTP-Server auf Citrix ADM:

1. Navigieren Sie in der ADM-GUI zu **System > Administration**. Klicken Sie auf der Seite **Systemadministration** unter **Netzwerkkonfigurationen**auf **NTP-Server**. Klicken Sie dann auf **Hinzufügen**.
2. Geben Sie auf der Seite **NTP-Server erstellen** die folgenden Details ein:
    - **Servername/IP-Adresse** —Geben Sie den Domainnamen oder die IP-Adresse des NTP-Servers ein. Der Name oder die IP-Adresse können nicht geändert werden, nachdem Sie den NTP-Server hinzugefügt haben.
    - **Minimales Abfrageintervall** —Geben Sie den Mindestwert für das Intervall zwischen übertragenen NTP-Nachrichten in Sekunden als Trennschärfe von 2. Wenn das Mindestabfrageintervall beispielsweise 64 Sekunden betragen soll, was als 2^6 ausgedrückt werden kann, geben Sie 6 ein
    - **Maximales Abfrageintervall** —Geben Sie den Maximalwert für das Intervall zwischen übertragenen NTP-Nachrichten in Sekunden als Trennschärfe von 2. Wenn Sie beispielsweise möchten, dass das maximale Abfrageintervall 256 Sekunden beträgt, was als 2^8 ausgedrückt werden kann, geben Sie 8 ein.
    - **Schlüssel-ID**—Geben Sie die Schlüssel-ID ein, die für die symmetrische Schlüsselauthentifizierung mit dem NTP-Server verwendet werden kann. Fügen Sie keine Schlüssel-ID hinzu, wenn Sie Autokey auswählen.
    - **Autokey** —Wählen Sie **Autokey** aus, wenn Sie die Authentifizierung mit öffentlichen Schlüsseln für den NTP-Server verwenden möchten. Wählen Sie nicht aus, ob Sie eine Schlüssel-ID hinzufügen möchten.
    - **Bevorzugt** —Wählen Sie diese Option, wenn Sie diesen NTP-Server als bevorzugten Server für die Uhrsynchronisierung angeben möchten. Dies gilt nur, wenn mehr als ein Server konfiguriert ist.
3. Klicken Sie auf **Erstellen**.

So aktivieren Sie die NTP-Synchronisierung auf NetScaler ADM:

1. Navigieren Sie zu **System** > **NTP-Server**.
2. Klicken Sie auf **NTP-Synchronisierung** und **aktivieren Sie das Kontrollkästchen NTP-Synchronisierung** aktivieren.
3. Klicken Sie auf **OK**.

Systemeinstellungen konfigurieren

February 5, 2024

Bevor Sie mit Citrix ADM Ihre Instanzen und Anwendungen verwalten und überwachen, wird empfohlen, einige Systemeinstellungen zu konfigurieren, um die optimale Leistung des Citrix ADM-Servers zu gewährleisten.

Konfigurieren von Systemalarmen

Konfigurieren Sie Systemalarme, um sicherzustellen, dass Sie kritische oder größere Systemprobleme kennen. Sie möchten z. B. benachrichtigt werden, wenn die CPU-Auslastung hoch ist oder wenn mehrere Anmeldefehler auf dem Server auftreten. Für einige Alarmkategorien, wie CPUUsageHigh oder MemoryUsageHigh, können Sie Schwellenwerte festlegen und den Schweregrad (z. B. Critical oder Major) für jede Alarmkategorie definieren. Für einige Kategorien, wie inventoryFailed oder loginFailure, können Sie nur den Schweregrad definieren. Wenn der Schwellenwert für eine Alarmkategorie (z. B. MemoryUsageHigh) überschritten wird oder wenn ein Ereignis auftritt, das der Alarmkategorie entspricht (z. B. loginFailure), wird eine Meldung im System aufgezeichnet, und Sie können die Meldung als Syslog-Nachricht anzeigen.

So konfigurieren Sie Systemalarme:

1. Navigieren Sie zu **System > SNMP**, und klicken Sie dann in der oberen rechten Ecke auf die Registerkarte **Alarme** .
2. Wählen Sie den Alarm aus, den Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie auf der Seite **Alarm konfigurieren** den Schweregrad des Alarms aus, und legen Sie den Schwellenwert fest.
4. Um die Alarme anzuzeigen, die den Schwellenwert überschritten haben oder für die ein Ereignis aufgetreten ist, navigieren Sie zu **System > Überwachung** und klicken Sie auf **Syslog-Nachrichten**.

Konfigurieren von Systembenachrichtigungen

Sie können Benachrichtigungen an ausgewählte Benutzergruppen für verschiedene systembezogene Funktionen senden. Sie können einen Benachrichtigungsserver in NetScaler ADM einrichten und E-Mail- und SMS-Gateway server (Short Message Service) so konfigurieren, dass E-Mail- und Textbenachrichtigungen an Benutzer gesendet werden. Durch das Festlegen von Benachrichtigungen wird sichergestellt, dass Sie über Aktivitäten auf Systemebene wie Benutzeranmeldung oder Systemneustart informiert werden.

So konfigurieren Sie Systembenachrichtigungen:

1. Navigieren Sie zu **System > Administration**. Klicken Sie auf der Seite **Systemadministration** unter **Ereignisbenachrichtigungen**auf **Ereignisbenachrichtigung konfigurieren und -digest > Ereignisbenachrichtigung**.
2. Wählen Sie auf der Seite **Einstellungen für Systembenachrichtigungen konfigurieren** die Kategorie oder Kategorie der Ereignisse aus, die von NetScaler ADM generiert wurden.
3. Konfigurieren Sie dann entweder den E-Mail-Server oder den SMS-Server, um Benachrichtigungen per E-Mail oder SMS oder beides zu erhalten.

Einstellungen für Systemausfall konfigurieren

Um die Menge der Berichtsdaten zu begrenzen, die in der Datenbank Ihres NetScaler ADM-Servers gespeichert werden, können Sie das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle aufbewahren soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00.00 Uhr) bereinigt.

So konfigurieren Sie die Einstellung für Systemausfall:

1. Navigieren Sie zu **System > Systemadministration**. Klicken Sie unter **Datenbereinigung** auf **System- und Instanzdatenbereinigung**.
2. Geben Sie auf der **Systemseite** die Anzahl der Tage an, für die Daten aufbewahrt werden sollen, und klicken Sie auf **Speichern**.

Konfigurieren der Einstellungen für die Instanz Syslog-Ausschneiden

Um die Menge der in der Datenbank gespeicherten Syslog-Daten zu begrenzen, können Sie das Intervall angeben, in dem Syslog-Daten gelöscht werden sollen. Sie können die Anzahl der Tage angeben, nach denen die generischen Syslog-Daten aus NetScaler ADM gelöscht werden.

So konfigurieren Sie die Einstellungen zum Löschen von Instanzsyslog-Einstellungen:

1. Navigieren Sie zu **System > Administration > Datenbereinigung**.
2. Klicken Sie auf **System- und Instanzdaten aufschneiden > Instanzsyslog**.
3. Geben **Sie auf der Seite „Syslog-Prune-Einstellungen für die Instanz konfigurieren**“im Feld Generische **Syslog-Daten speichern** die Anzahl der Tage zwischen 1 und 180 an.
4. Klicken Sie auf **Speichern**.

Einstellungen für das Ausschneiden von Instanzereignissen konfigurieren

Um die Anzahl der Ereignismeldungsdaten zu begrenzen, die in der Datenbank Ihres NetScaler ADM-Servers gespeichert werden, können Sie das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle aufbewahren soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00:00 Uhr) beschnitten.

So konfigurieren Sie die Einstellungen für das Ausschneiden von Instanzereignissen:

1. Navigieren Sie zu **System > Administration**.
2. Klicken Sie auf der Seite **Systemadministration** unter **Datenbereinigung** auf **System- und Instanzdatenbereinigung**.
3. Klicken Sie auf der Seite **Datenbereinigung** auf **Instanzereignisse**.
4. Geben Sie im Feld **Zu behaltende Daten (Tage)** das Zeitintervall in Tagen ein, für das Sie Daten auf dem Citrix ADM -Server beibehalten möchten, und klicken Sie auf **Speichern**.

Einstellungen für das Systembackup konfigurieren

NetScaler ADM erstellt ein Backup des Systems automatisch jeden Tag um 00:30 Uhr. Standardmäßig werden drei Backupdateien gespeichert. Möglicherweise möchten Sie eine größere Anzahl von Backups des Systems beibehalten. Sie können die Sicherungsdatei auch verschlüsseln. Sie können das Backup auch auf einem externen Server speichern.

So konfigurieren Sie die Einstellungen für das Systembackup:

1. Navigieren Sie zu **System > Administration**.
2. Klicken Sie unter **Backup**auf **System- und Instanz-Backup konfigurieren**.
3. Klicken Sie auf **System** und geben Sie auf der Seite **„System-Backup-Einstellungen konfigurieren** “die erforderlichen Werte an.

Konfigurieren der Einstellungen für das Instanzbackup

Wenn Sie den aktuellen Status einer Citrix ADC Instanz sichern, können Sie die Backupdateien verwenden, um die Stabilität wiederherzustellen, wenn die Instanz instabil wird. Dies ist besonders wichtig, bevor Sie ein Upgrade durchführen. Standardmäßig wird alle 12 Stunden ein Backup erstellt und drei Sicherungsdateien werden im System aufbewahrt.

So konfigurieren Sie Instanzbackupeinstellungen:

1. Navigieren Sie zu **System > Administration**.

2. Klicken Sie unter **Backup**auf **System- und Instanz-Backup konfigurieren**.
3. **Klicken Sie unter**Configure Instance Backup Settings**auf Instance und geben Sie die erforderlichen Werte an.**

ADM-Features aktivieren oder deaktivieren

Als Administrator können Sie die folgenden Funktionen auf der Seite **System > Administration > Konfigurierbare Funktionen** aktivieren oder deaktivieren:

- **Agentfailover** : Das Agent-Failover kann auf einem Standort mit zwei oder mehr aktiven Agents auftreten. Wenn ein Agent in der Site inaktiv wird (DOWN Status), verteilt der NetScaler ADM Dienst die ADC-Instanzen des inaktiven Agents mit anderen aktiven Agenten neu. Weitere Informationen finden Sie unter Konfigurieren von On-Prem-Agenten für die Multisite-Bereitstellung.
- **Entity-Polling-Netzwerkfunktion** : Eine Entität ist entweder eine Richtlinie, ein virtueller Server, ein Dienst oder eine Aktion, die an eine ADC-Instanz angehängt ist. Standardmäßig ruft NetScaler ADM konfigurierte Netzwerkfunktionsentitäten automatisch alle 60 Minuten ab. Weitere Informationen finden Sie unter Überblick über Statusabruf.
- **Instanzbackup**: Erstellen Sie ein Backup des aktuellen Status einer NetScaler ADC-Instanz und verwenden Sie später die Backupdateien, um die ADC-Instanz in demselben Zustand wiederherzustellen. Weitere Informationen finden Sie unter Backup und Wiederherstellen von NetScaler ADC-Instanzen.
- **Überwachung der Instanzkonfiguration** : Überwachen Sie Konfigurationsänderungen in verwalteten NetScaler ADC-Instanzen, beheben Sie Konfigurationsfehler und stellen Sie ungespeicherte Konfigurationen wieder her. Weitere Informationen finden Sie unter Erstellen von Überwachungsvorlagen.
- **Instanzereignisse** - Ereignisse stellen Vorkommen von Ereignissen oder Fehlern in einer verwalteten NetScaler ADC-Instanz dar. ******In Citrix ADM empfangene Ereignisse werden auf der Seite „Ereignisübersicht “(Netzwerke > Ereignisse**) angezeigt, und alle aktiven Ereignisse werden auf der Seite „Ereignisnachrichten“(Netzwerke > Ereignisse > Ereignisnachrichten) angezeigt. Weitere Informationen finden Sie unter Ereignisse.
- **Instanznetzwerk-Reporting** - Sie können Berichte für Instanzen auf globaler Ebene erstellen. Auch für Entitäten wie die virtuellen Server und Netzwerkschnittstellen. Weitere Informationen finden Sie unter Netzwerkberichte.
- **Instanz-SSL-Zertifikate** : NetScaler ADM bietet eine zentrale Ansicht der SSL-Zertifikate, die auf allen verwalteten NetScaler ADC-Instanzen installiert sind. Weitere Informationen finden Sie unter SSL-Dashboard.

- **Instanzsyslog** : Sie können die Syslog-Ereignisse überwachen, die auf Ihren NetScaler ADC-Instanzen generiert werden, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Nachrichten an NetScaler ADM umgeleitet werden.

Führen Sie die folgenden Schritte aus, um eine Funktion zu aktivieren:

1. Wählen Sie die Funktion aus der Liste aus, die Sie aktivieren möchten.
2. Klicken Sie auf **Aktivieren**.

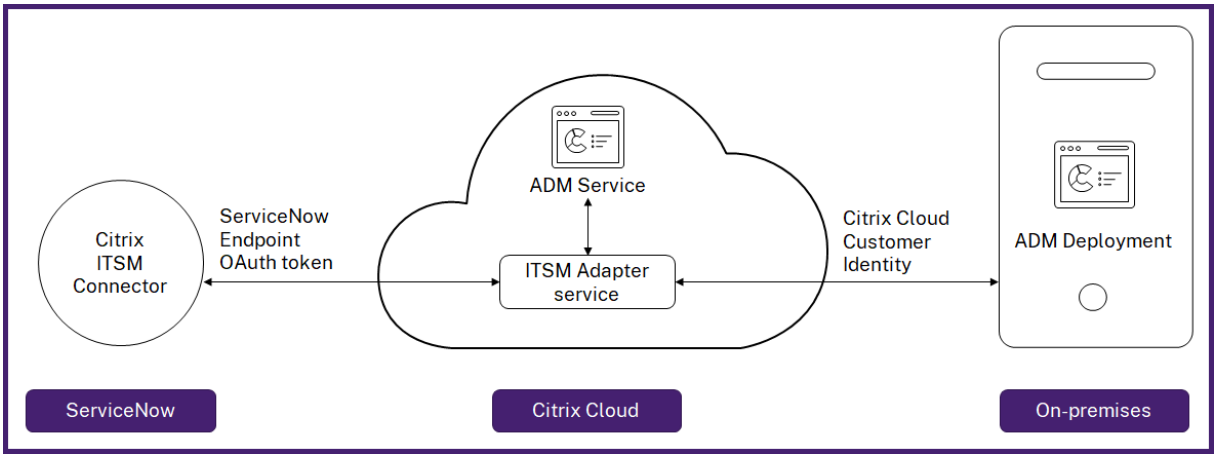
> **Wichtig**
>
> Wenn eine Funktion deaktiviert ist, kann der Benutzer die mit dieser Funktion verbundenen Vorgänge nicht ausführen.

Integration von NetScaler ADM in die ServiceNow-Instanz

February 5, 2024

Wenn Sie ServiceNow-Benachrichtigungen für NetScaler ADC- und ADM-Ereignisse aktivieren möchten, integrieren Sie NetScaler ADM in die ServiceNow-Instanz. Diese Integration verwendet den Citrix ITSM-Connector für die Kommunikation zwischen NetScaler ADM und der ServiceNow-Instanz.

Die ServiceNow-Integration mit ADM verwendet den ITSM-Adapter-Dienst für die tokenbasierte Authentifizierung. Zu diesem Zweck wird eine Endpunktinstanz in ServiceNow erstellt. Weitere Informationen finden Sie unter Funktionsweise des ITSM-Adapters.



Um Ihre ADM-Bereitstellung on-premises mit einem ITSM-Adapter zu verbinden, müssen Sie die Kundenidentität konfigurieren. Weitere Informationen finden Sie unter Konfigurieren der Kundenidentität.

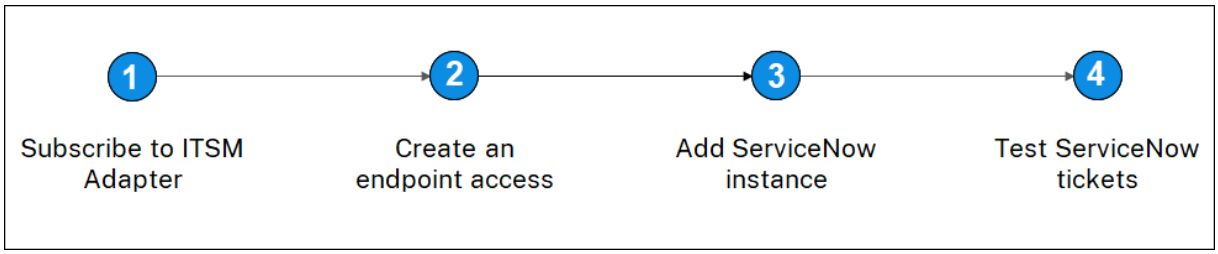
Voraussetzungen

Bevor Sie ADM mit ServiceNow integrieren, stellen Sie Folgendes sicher:

1. Melden Sie sich für Citrix Cloudan. Stellen Sie sicher, dass Sie Zugriff auf die Verwaltung von Citrix Cloud-Administratoren haben. Weitere Informationen finden Sie unter Verwalten von Citrix Cloud-Administratoren.

Wie integriert man ADM mit ServiceNow?

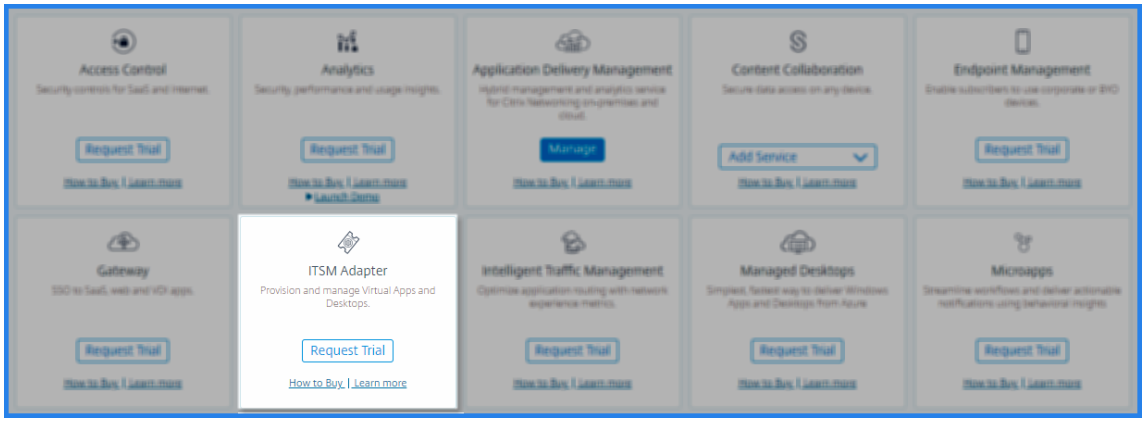
Führen Sie die folgenden Schritte aus, um NetScaler ADM mithilfe des ITSM-Connectors in ServiceNow zu integrieren:



1. Abonnieren Sie den ITSM-Adapterdienst in Citrix Cloud.
2. Erstellen Sie einen Endpunktzugriff in der ServiceNow-Instanz.
3. Fügen Sie eine ServiceNow-Instanzhinzu.
4. Testen Sie die automatische Generierung von ServiceNow-Tickets in ADM.

Schritt 1 —Abonnieren des ITSM-Adapterdienstes in Citrix Cloud

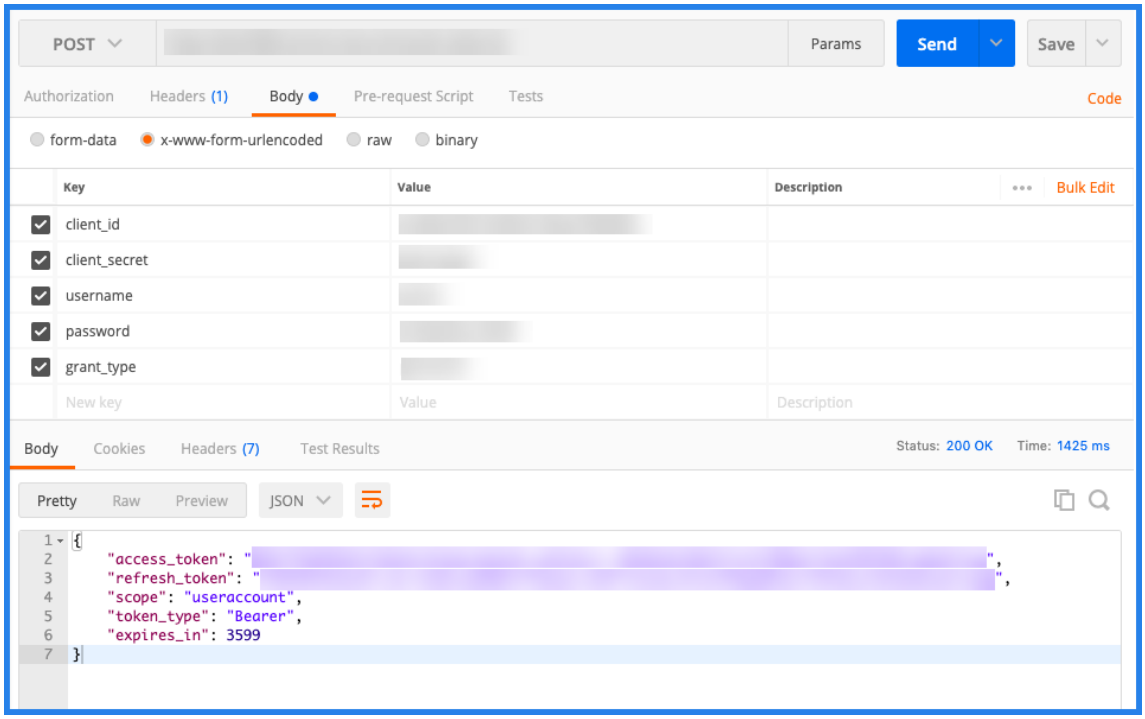
1. Klicken Sie auf der Kachel **ITSM-Adapter** auf **Testversion anfordern**.



2. Navigieren Sie zu **Identitätszugriff und Verwaltung** > **API-Zugriff**, und notieren Sie sich die **Client-ID** und **Client-Geheiminformationen**.

Schritt 2 —Erstellen eines Endpunktzugriffs in der ServiceNow-Instanz

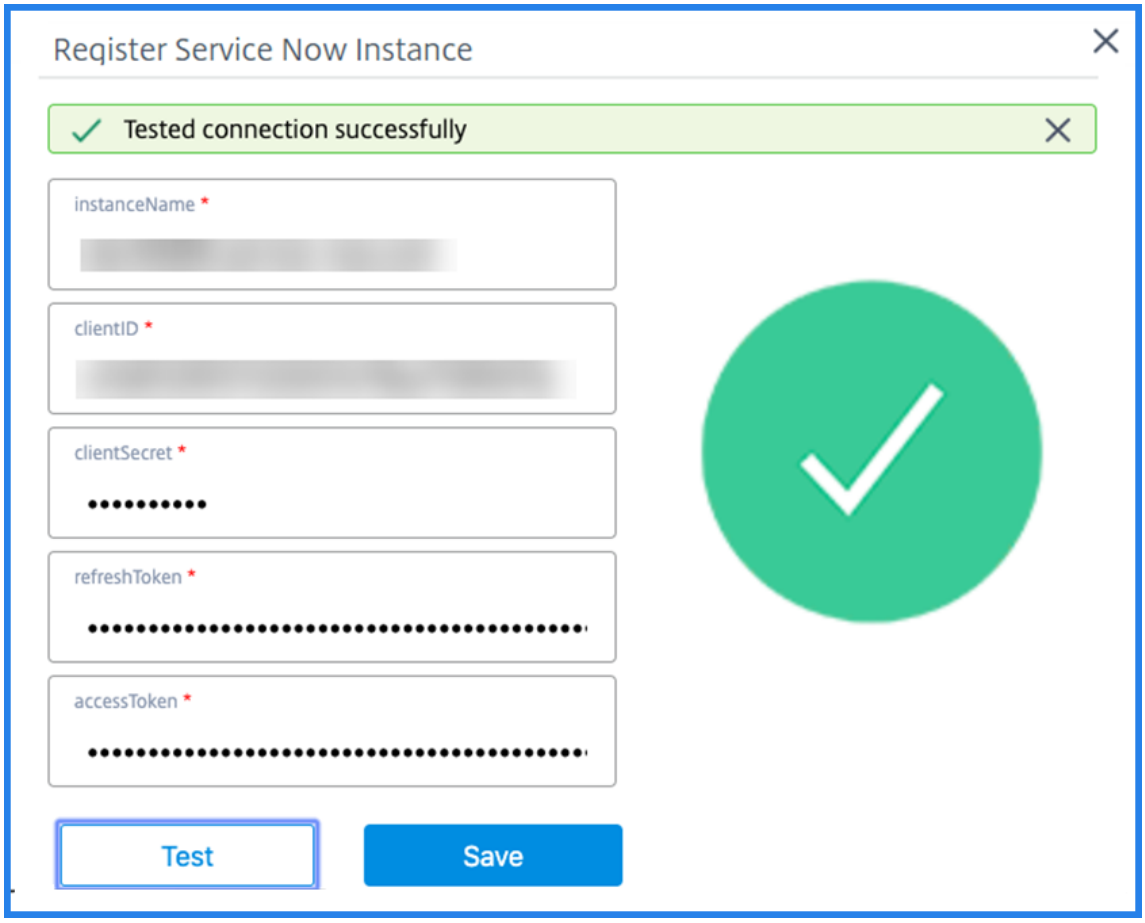
1. Melden Sie sich mit Administratoranmeldeinformationen bei Ihrer ServiceNow-Instanz an.
2. Gehen Sie zum ServiceNow Store. Laden Sie den **Citrix ITSM-Connector**herunter und installieren Sie ihn.
3. Wählen Sie im Bereich **Citrix ITSM Connector** die Option **Home** aus und klicken Sie dann auf **Authentifizieren**. Geben Sie die Client-ID und das Secret ein, die Sie von Citrix Cloud notiert haben.
4. Testen Sie die Verbindung.
5. Speichern Sie die Konfiguration. Eine Bestätigung von ServiceNow wird angezeigt, die darauf hinweist, dass die Verbindung aktiv ist.
6. Erstellen Sie einen Endpunkt für den Zugriff auf eine ServiceNow-Instanz. Weitere Informationen finden Sie unter Erstellen eines Endpunkts für Clients für den Zugriff auf die Instanz.
7. Rufen Sie die Zugriffs- und Aktualisierungstoken mit der Client-ID und dem Clientgeheimnis ab. Siehe OAuth-Token.



Schritt 3 —ServiceNow-Instanz hinzufügen

1. Wählen Sie auf der Registerkarte **Verwalten** die Option ServiceNow-Instanz hinzufügen aus.
2. Geben Sie den **Instanznamen**, die **Client-ID**, das **Client-Geheimnis, dasAktualisierungstoken**und das**Zugriffstoken**an.

3. Klicken Sie auf **Test**.



   Die ServiceNow-Instanz ist jetzt mit dem ITSM Adapter Service verbunden.

4. Nachdem Sie die Verbindung erfolgreich getestet haben, klicken **Sie auf Speichern**, um eine ServiceNow-Instanz hinzuzufügen.

Schritt 4 —Testen der automatischen Generierung von ServiceNow-Tickets in ADM

1. Melden Sie sich bei NetScaler ADM an.
2. Navigieren Sie zu **Konto > Benachrichtigungen** und wählen Sie **ServiceNow**aus.
3. Wählen Sie das ServiceNow-Profil aus der Liste aus.
4. Klicken Sie auf **Test**, um ein ServiceNow-Ticket automatisch zu generieren und die Konfiguration zu überprüfen.

   Wenn Sie ServiceNow-Tickets in der NetScaler ADM GUI anzeigen möchten, wählen Sie **ServiceNow Tickets**aus.

Stellen Sie ServiceNow-Benachrichtigungen in ADM ein

Nachdem die ServiceNow-Instanz auf dem ITSM-Adapter registriert wurde, können Sie ServiceNow-Benachrichtigungen für die folgenden Ereignisse in der NetScaler ADM-GUI einrichten:

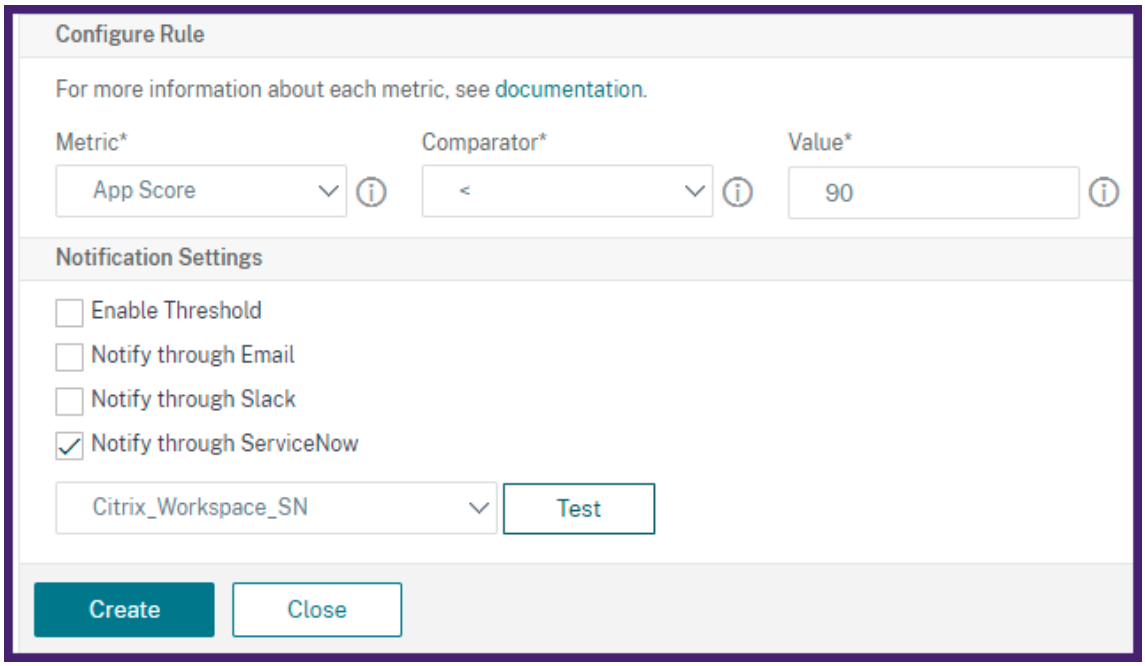
> **Wichtig**
>
> Diese Funktion wird von ServiceNow Cloud unterstützt.

- **NetScaler ADC-Ereignisse**: NetScaler ADM kann die ServiceNow-Incidents für den ausgewählten Satz von NetScaler ADC-Ereignissen aus ausgewählten verwalteten NetScaler ADC-Instanzen generieren.

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

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

- **Anwendungsanalyse**: NetScaler ADM kann ServiceNow-Vorfälle für die Anwendungen generieren, die den angegebenen Schwellenwert überschreiten.



  In diesem Beispiel wird ein ServiceNow-Vorfall generiert, wenn der App-Score von Anwendungen unter 90 fällt.

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

generieren.

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

Informationen zum Senden von ServiceNow-Benachrichtigungen für den Ablauf einer ADM-Lizenz finden Sie unter Ablauf der NetScaler ADM-Lizenz.

Exportberichte exportieren oder planen

February 5, 2024

In NetScaler ADM können Sie einen umfassenden Bericht für das ausgewählte NetScaler ADM Feature exportieren. Dieser Bericht bietet Ihnen einen Überblick über die Zuordnung zwischen den Instanzen, Partitionen und entsprechenden Details.

NetScaler ADM zeigt funktionsspezifische geplante Exportberichte unter einzelnen ADM-Features an, die Sie anzeigen, bearbeiten oder löschen können. Um beispielsweise die Exportberichte von NetScaler ADC-Instanzen anzuzeigen, navigieren Sie zu **Netzwerk > Instanzen > NetScaler ADC** und klicken Sie auf das Exportsymbol. Sie können diese Berichte im PDF-, JPEG-, PNG- und CSV-Dateiformat exportieren.

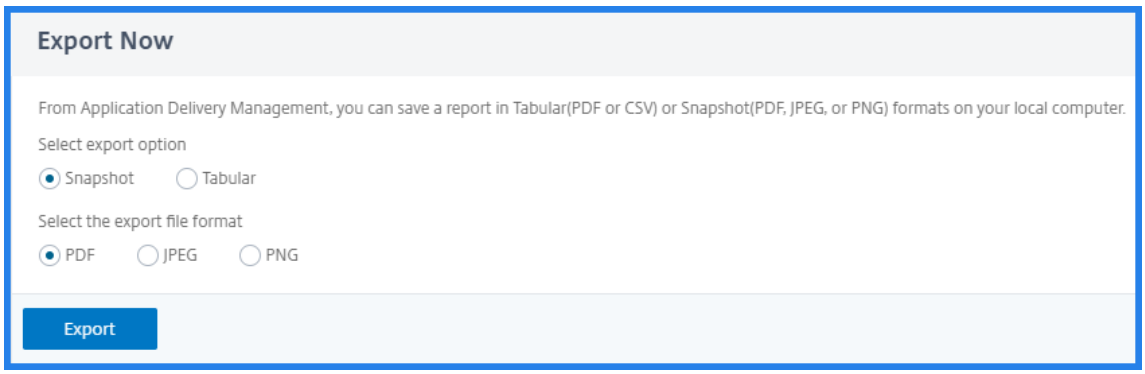
In **Berichte exportieren**können Sie die folgenden Aktionen ausführen:

- Exportieren eines Berichts auf einen lokalen Computer
- Exportberichte planen
- Anzeigen, Bearbeiten oder Löschen der geplanten Exportberichte

Exportieren eines Berichts

Um einen Bericht aus dem ADM auf den lokalen Computer zu exportieren, führen Sie die folgenden Schritte aus:

1. Klicken Sie oben rechts auf der Seite auf das Exportsymbol.
2. Wählen Sie **Jetzt exportieren**aus.
3. Wählen Sie eine der folgenden Exportoptionen aus:
    - **Snapshot** - Diese Option exportiert ADM-Berichte als Snapshot.
    - **Tabellarisch** - Diese Option exportiert ADM-Berichte in einem tabellarischen Format. Sie können auch auswählen, wie viele Datensätze in einem Tabellenformat exportiert werden sollen

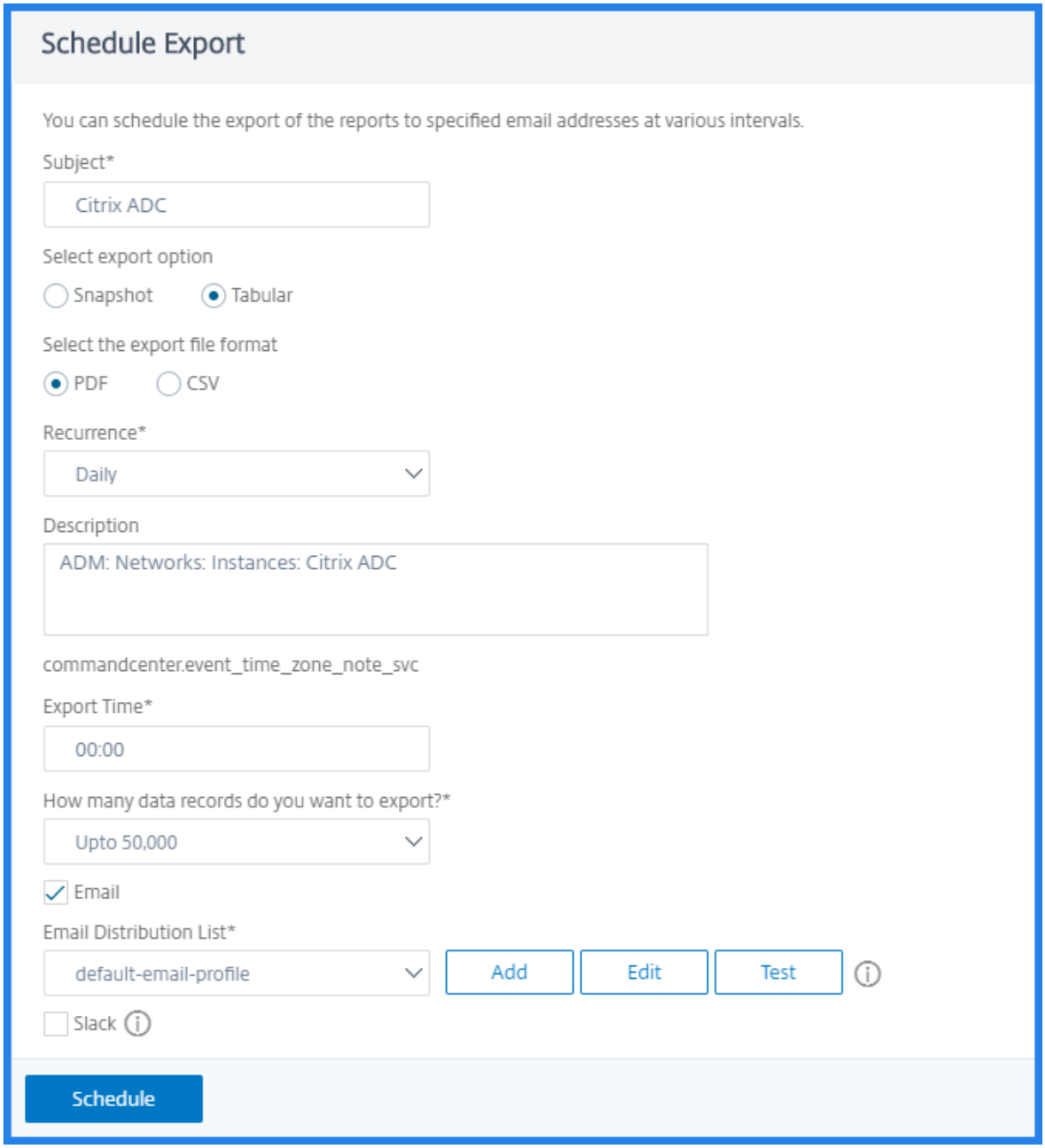


4. Wählen Sie das Dateiformat aus, das Sie den Bericht auf Ihrem lokalen Computer speichern möchten.
5. Klicken Sie auf **Exportieren**.

Exportbericht planen

Um den Exportbericht in regelmäßigen Intervallen zu planen, geben Sie das Wiederholungsintervall an. NetScaler ADM sendet den exportierten Bericht an das konfigurierte E-Mail- oder Slack-Profil.

1. Klicken Sie oben rechts auf der Seite auf das Exportsymbol.
2. Wählen Sie **Export planen** und geben Sie Folgendes an:
   - **Betreff** —Standardmäßig füllt dieses Feld den ausgewählten Feature-Namen automatisch aus. Sie können es jedoch mit einem aussagekräftigen Titel umschreiben.
   - **Exportoption** - Exportieren Sie ADM-Berichte in einem Snapshot oder einem Tabellenformat. Sie können auch auswählen, wie viele Datensätze in einem Tabellenformat exportiert werden sollen
   - **Format** - Wählen Sie das Dateiformat aus, das Sie den Bericht für das konfigurierte E-Mail- oder Pufferprofil erhalten möchten.
   - **Wiederholung** - Wählen Sie in der Liste **Täglich**, **Wöchentlich**oder **Monatlich** aus.
   - **Beschreibung** - Geben Sie die aussagekräftige Beschreibung für einen Bericht an.
   - **Exportzeit** —Geben Sie an, zu welcher Uhrzeit Sie den Bericht exportieren möchten.
   - **E-Mail** - Aktivieren Sie das Kontrollkästchen und wählen Sie das Profil aus dem Listenfeld aus. Wenn Sie ein Profil hinzufügen möchten, klicken Sie auf **Hinzufügen**.
   - **Slack** —Aktiviere das Kontrollkästchen und wähle das Profil aus dem Listenfeld aus. Wenn Sie ein Profil hinzufügen möchten, klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Zeitplan**.



Anzeigen und Bearbeiten der geplanten Exportberichte

Gehen Sie wie folgt vor, um die Exportberichte anzuzeigen:

1. Klicken Sie oben rechts auf der Seite auf das Exportsymbol.

   Auf der Seite **Bericht exportieren** werden alle funktionsspezifischen Exportberichte angezeigt.

2. Wählen Sie den Bericht aus, den Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.

Upgrade

February 5, 2024

Jede NetScaler ADM-Version bietet neue und aktualisierte Funktionen mit erweiterter Funktionalität. Citrix empfiehlt, NetScaler ADM auf die neueste Version zu aktualisieren, um die neuen Funktionen und Fehlerbehebungen in Anspruch zu nehmen. Eine umfassende Liste von Verbesserungen, bekannten Problemen und Bugfixes ist in den Versionshinweisen enthalten, die jeder Versionsankündigung beiliegen. Es ist auch wichtig, den Lizenzierungsrahmen und die Arten von Lizenzen zu verstehen, die verwendet werden können, bevor Sie mit dem Upgrade beginnen. Informationen zur NetScaler ADM-Lizenzierung finden Sie unterLizenzierung.

Die Informationen zum Upgrade-Pfad sind auch im Citrix Upgrade Guideverfügbar.

Upgradevorbereitung

Laden Sie das Upgrade-Paket von der Citrix ADM Download-Seite herunter und folgen Sie den Anweisungen in diesem Artikel, um Ihr System auf den neuesten 13.0-Build zu aktualisieren. Nach Beginn des Upgradevorgangs wird ADM neu gestartet, und die vorhandenen Verbindungen werden beendet und wieder verbunden, wenn das Upgrade abgeschlossen ist. Die vorhandene Konfiguration bleibt erhalten, aber NetScaler ADM verarbeitet keine Daten, bis das Upgrade erfolgreich abgeschlossen wurde.

> **Wichtig!**
>
> Die NetScaler ADM-Version und der Build sollten **gleich oder höher** als Ihre NetScaler ADC-Version und Ihr Build sein. Wenn Sie beispielsweise NetScaler ADM 12.1 Build 50.39 installiert haben, stellen Sie sicher, dass Sie NetScaler ADC 12.1 Build 50.28/50.31 oder früher installiert haben.

Punkte, die vor dem Upgrade auf 13.0 zu beachtensind:

- Wenn Sie ein Upgrade von Version 11.1 oder Version 12.0 56.x und früheren Builds durchführen, führen Sie die folgenden Schritte aus:
  1. Upgrade von der bestehenden Version auf 12.0 Build 57,24.
  2. Führen Sie ein Upgrade auf den neuesten Build der Version 12.1 durch.
  3. Aktualisieren Sie auf Version 13.0.
- Wenn Sie von 12.0 Build 57,24 und höher upgraden, führen Sie zuerst ein Upgrade auf 12.1 und dann auf 13.0 durch.

- Wenn Sie ein Upgrade von 12.1 durchführen, können Sie direkt auf 13.0 upgraden.
- Wenn Sie auf 13.0 67.xx und höher upgraden, führen Sie zuerst ein Upgrade auf 13.0 64.xx und dann auf 13.0 67.xx und höher ein, um eine bessere Benutzererfahrung zu erzielen.

Wichtige Punkte, die Sie vor dem Upgrade auf 13.0 67.xx und höher beachten sollten

Wenn Sie die ADM-Software auf Version 13.0 67.xx und höher aktualisieren, wird Ihre ADM-Datenbank ebenfalls migriert. Diese Datenmigration findet statt, weil ADM jetzt PostgreSQL Version 10.11 verwendet.

> **Hinweis**
>
> Das Herunterstufen der ADM-Software wird nicht unterstützt. Versuchen Sie nicht, ein Downgrade durchzuführen.

Empfohlene Vorsichtsmaßnahmen:

- Machen Sie einen Snapshot des NetScaler ADM-Servers, wenn Sie ein Upgrade auf 13.0 67.xx und höher durchführen.
- Sichern Sie den NetScaler ADM -Server, bevor Sie das Upgrade durchführen.
- Nach dem Upgrade müssen Sie möglicherweise Verbindungen zwischen dem NetScaler ADM-Server und den verwalteten Instanzen wiederherstellen. Eine Bestätigungsaufforderung warnt Sie, dass Verbindungen fehlschlagen können, wenn Sie fortfahren.
- Nehmen Sie bei NetScaler ADM-Servern im Hochverfügbarkeits-Setup beim Upgrade keine Konfigurationsänderungen auf einem der Knoten vor.

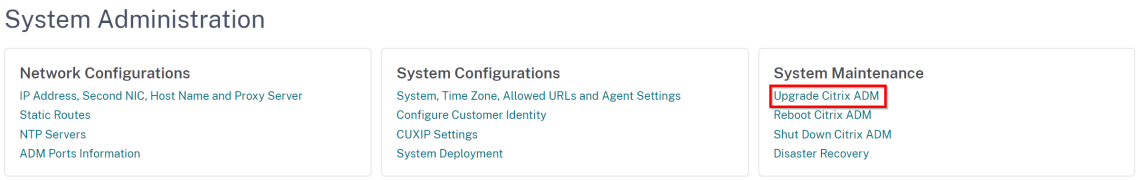
  > **Warnung**
  >
  > Aktualisieren Sie den Browser erst, wenn der Upgradevorgang erfolgreich abgeschlossen wurde. Überprüfen Sie die GUI auf die ungefähre Zeit für den Abschluss des Upgrades.

- Nach dem Upgrade kann sich der aktive Knoten in einem Hochverfügbarkeitspaar ändern.

Upgrade eines einzelnen NetScaler ADM-Servers

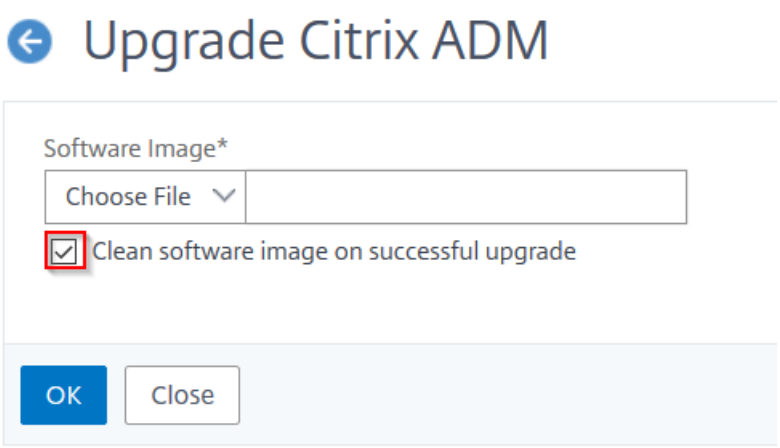
So aktualisieren Sie einen NetScaler ADM-Server:

1. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler ADM an.
2. Navigieren Sie zu **System** > **Systemadministration**. Klicken Sie unter der Unterüberschrift**Systemadministration**auf **NetScaler ADM aktualisieren**.

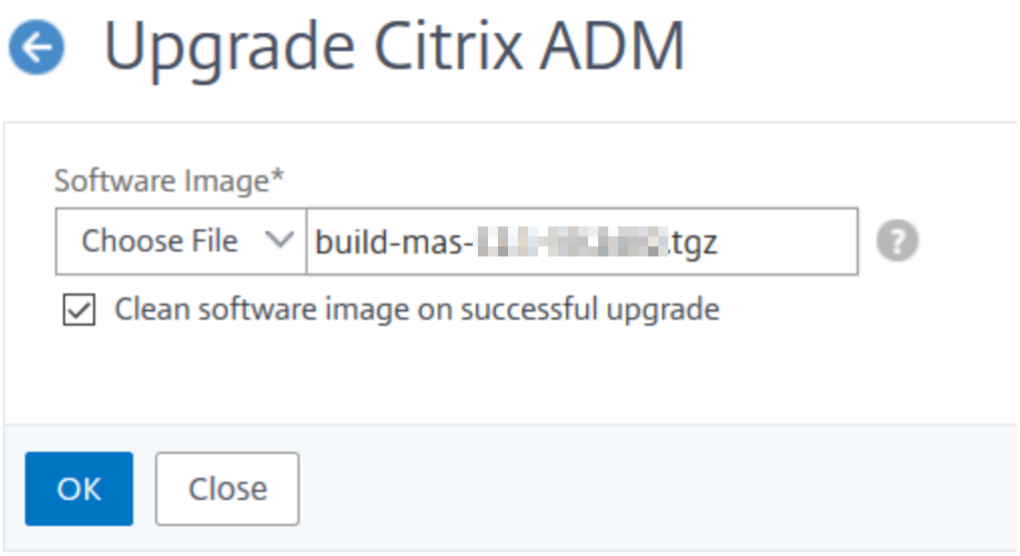


3. Aktivieren Sie auf der Seite**NetScaler ADM aktualisieren**das Kontrollkästchen**Software-Image bei erfolgreichem Upgrade säubern**, um Imagedateien nach dem Upgrade zu löschen. Wenn Sie diese Option auswählen, werden die NetScaler ADM Imagedateien beim Upgrade automatisch entfernt.

> **Hinweis**
>
> Diese Option ist standardmäßig ausgewählt. Wenn Sie dieses Kontrollkästchen vor dem Starten des Upgrade-Vorgangs nicht aktivieren, müssen Sie die Images manuell löschen.



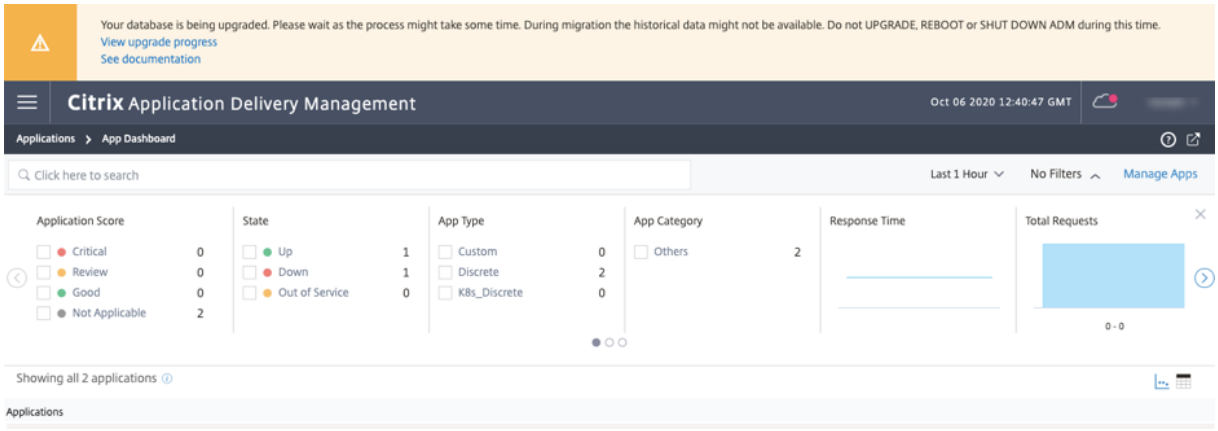
4. Sie können dann eine neue Imagedatei hochladen, indem Sie entweder **Lokal** (Ihr lokaler Computer) oder **Appliance**auswählen. Die Builddatei muss auf der virtuellen NetScaler ADM Appliance vorhanden sein.



5. Klicken Sie auf **OK**.
   Das Dialogfeld Bestätigen wird angezeigt. Klicken Sie auf **Ja**.

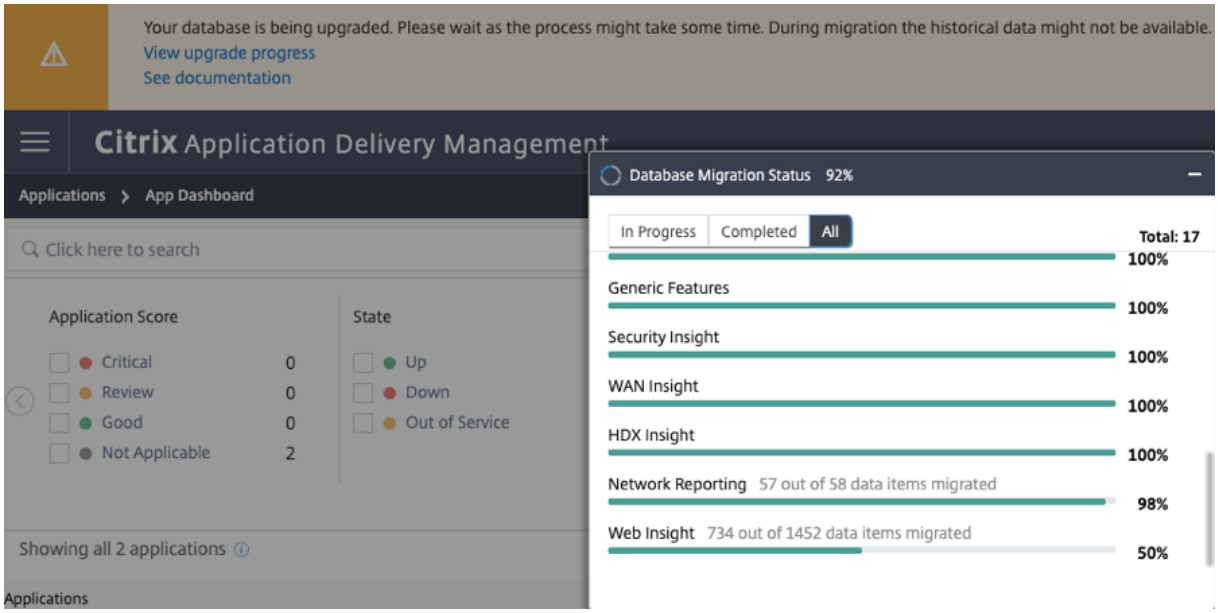
   Der Upgrade-Prozess wird gestartet.

Nachdem Ihre Konfiguration migriert wurde, können Sie sich bei der ADM-GUI anmelden. Bei der Anmeldung beginnen die historischen Daten im Hintergrund zu migrieren, während Sie weiterhin an ADM arbeiten können.



Während der Migration historischer Daten stehen einige der alten Daten möglicherweise nicht zur Verfügung. Die Zeit für die Migration Ihrer Datenbank hängt von der Größe der Daten und der Anzahl der Tabellen ab.

Sie können die Datenbankmigration mit der ADM-GUI überwachen. Klicken Sie auf **Upgrade-Fortschritt anzeigen** und der **Status der Datenbankmigration** wird angezeigt.



Problembehandlung bei Problemen bei der Datenbank

Während des Upgrade-Vorgangs auf 13.0 67.xx und höher scheint manchmal die Migration historischer Daten von Web Insight festzuhalten. Um in solchen Fällen Details der Datenmigration zu überprüfen, gehen Sie wie folgt vor.

Melden Sie sich bei der ADM-Shell-Eingabeaufforderung an und führen Sie den folgenden Befehl aus, um die detaillierten Details des Fortschritts anzuzeigen.

```
1     cat /var/mps/log/db_upgrade/web_insight_mapping_migration_status
2
3 <!--NeedCopy-->
```

Hier ist ein Beispiel für eine Ausgabe

```
1     bash-3.2# cat /var/mps/log/db_upgrade/
         web_insight_mapping_migration_status
2     Tue Oct  6 07:41:55 GMT 2020
3     157 out of 127346 done in 54 seconds
4     File
5      /var/mps/db_upgrade/hist_table_mig_data/Web_Insight/
          af_app_client_server_resp_second_l3p_d7_dump
6     bash-3.2#
7
8  <!--NeedCopy-->
```

In diesem Beispiel ist `af_app_client_server_resp_second_l3p_d7` der Eintrag, der aktualisiert wird. Und 157 Eintritte von 127.346 werden in 54 Sekunden migriert.

Aktualisieren eines Hochverfügbarkeitspaars von Version 12.1 auf Version 13.0

Für NetScaler ADM -Server in einem Hochverfügbarkeitsmodus können Sie ein Upgrade durchführen, indem Sie entweder auf den aktiven Knoten oder auf die schwebende IP-Adresse zugreifen. Beide NetScaler ADM -Server werden automatisch auf den neuesten Build aktualisiert, sobald Sie den Upgradevorgang auf einem der Server initiieren.

> **Hinweis**
>
> Wenn Sie ein Hochverfügbarkeitspaar von 12.0 oder früheren Versionen aktualisieren, lesen Sie NetScaler ADM 12.1 Upgrade

Upgrade der Bereitstellung von NetScaler ADM Disaster Recovery

Das Upgrade der NetScaler ADM Disaster Recovery-Bereitstellung erfolgt in zwei Schritten:

- Aktualisieren Sie die NetScaler ADM-Knoten, die im Hochverfügbarkeitsmodus am primären Standort konfiguriert sind. Später müssen Sie den Notfallwiederherstellungsknoten aktualisieren.
- Stellen Sie sicher, dass Sie die NetScaler ADM -Server aktualisiert haben, die in hoher Verfügbarkeit bereitgestellt werden, bevor Sie den Notfallwiederherstellungsknoten aktualisieren.

Aktualisieren des NetScaler ADM Notfallwiederherstellungsknotens

1. Laden Sie die NetScaler ADM Upgrade-Imagedatei von der Citrix Download-Site herunter.
2. Laden Sie diese Datei mit `nsrecover`-Anmeldeinformationen auf den Disaster Recovery-Knoten hoch.
3. Melden Sie sich mit den `nsrecover`-Anmeldeinformationen beim Disaster Recovery-Knoten an.
4. Navigieren Sie zu dem Ordner, in dem Sie die Imagedatei abgelegt haben, und entpacken Sie die Datei.

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Wed May 15 05:27:10 2019 from 10.252.241.103
bash-3.2# cd /var/mps/mps_images
bash-3.2# tar xvfz build-mas-13.0-36.25.tgz
```

5. Führen Sie das folgende Skript aus:

   ./installmas

```
bash-3.2# ./installmas
```


Upgrade von On-Premises-Agents für die Bereitstellung an mehreren Standorten

Das Upgrade der NetScaler ADM Agent-Bereitstellung erfolgt in drei Schritten.
Stellen Sie sicher, dass Sie die folgenden Aufgaben ausgeführt haben, bevor Sie die On-Premises-Agents aktualisieren:

1. Aktualisieren Sie die NetScaler ADM -Server, die in Hochverfügbarkeit bereitgestellt werden.
2. Aktualisieren Sie den NetScaler ADM Notfallwiederherstellungsknoten.

   Weitere Informationen finden Sie unter Aktualisieren der NetScaler ADM-Disaster Recovery-Bereitstellung.

Upgrade der On-Premises-Agents

1. Laden Sie die NetScaler ADM Agent-Upgrade-Imagedatei von der Citrix Download-Site herunter.
2. Laden Sie diese Datei mit den `nsrecover`-Anmeldeinformationen auf den Agentknoten hoch.
3. Stellen Sie sicher, dass Sie das richtige Agent-Upgradeimage herunterladen. Im Folgenden finden Sie ein Beispiel für ein Imagedateinamenformat:

   build-masagent-13.0-48.18.tgz
4. Melden Sie sich mit den `nsrecover`-Anmeldeinformationen beim On-Prem-Agent an.
5. Navigieren Sie zu dem Ordner, in dem Sie die Imagedatei abgelegt haben, und entpacken Sie die Datei.

   ```
   login as: nsrecover
   Using keyboard-interactive authentication.
   Password:
   Last login: Thu Aug 30 08:50:48 2018 from 10.252.241.37
   bash-3.2# cd /var/mps/mps_images/
   bash-3.2# tar zxvf build-masagent-12.1-502.109.tgz
   ```
6. Führen Sie das folgende Skript aus:

   `./installmasagent`

   ```
   bash-3.2# ./installmasagent
   ```

Zusätzlichen Datenträger für NetScaler ADM-Server bereitstellen

Wenn Ihre NetScaler ADM-Speicheranforderungen den Standardspeicherplatz (120 GB) überschreiten, können Sie einen zusätzlichen Datenträger anschließen. Sie können mehr Datenträger sowohl in Bereitstellungen mit einem Server als auch in Bereitstellungen mit hoher Verfügbarkeit anhängen.

Wenn Sie NetScaler ADM von Version 12.1—13.0 aktualisieren, bleiben die Partitionen unverändert, die Sie in der früheren Version auf dem zusätzlichen Datenträger erstellt haben. Die Partitionen werden weder entfernt noch in der Größe geändert.

Das Verfahren zum Bereitstellen weiterer Datenträger bleibt im aktualisierten Build unverändert. Sie können jetzt das neue Datenträgerpartitionierungstool in NetScaler ADM verwenden, um Partitionen auf dem neu hinzugefügten Datenträger zu erstellen. Sie können das Tool auch verwenden, um die Größe der Partitionen auf der vorhandenen More Disk zu ändern. Weitere Informationen zum Bereitstellen weiterer Datenträger und zur Verwendung des neuen Datenträgerpartitionierungstools finden Sie unter Bereitstellen eines zusätzlichen Datenträgers in NetScaler ADM.

NetScaler ADC-Instanzen in OpenStack mit StyleBooks bereitstellen

Ab NetScaler ADM 12.1 Build 49.23 wurde die Architektur eines OpenStack-Orchestrierungs-Workflows aktualisiert. Der Workflow verwendet jetzt NetScaler ADM StyleBooks, um NetScaler ADC Instanzen zu konfigurieren. Wenn Sie von Version 12.0 oder 12.1 Build 48.18 auf NetScaler ADM 13.0 aktualisieren, müssen Sie das folgende Migrationsskript ausführen:

```
/mps/scripts/migration_scripts/migrate_configurations.py
<!--NeedCopy-->
```

Weitere Informationen zum StyleBook `os-cs-lb-mon` und zum Migrationsskript finden Sie unter Provisioning der NetScaler ADC VPX-Instanz auf OpenStack mit StyleBook

Authentifizierung

February 5, 2024

Benutzer können entweder intern von Citrix ADM, extern von einem Authentifizierungsserver oder beides authentifiziert werden. Wenn die lokale Authentifizierung verwendet wird, muss sich der Benutzer in der NetScaler ADM -Sicherheitsdatenbank befinden. Wenn der Benutzer extern authentifiziert wird, muss der „externe Name“des Benutzers je nach ausgewähltem Authentifizierungsprotokoll mit der externen Benutzeridentität übereinstimmen, die auf dem Authentifizierungsserver registriert ist.

NetScaler ADM unterstützt externe Authentifizierung durch RADIUS-, LDAP- und TACACS-Server. Diese einheitliche Unterstützung bietet eine gemeinsame Schnittstelle zur Authentifizierung und Autorisierung aller lokalen und externen Benutzer von Authentifizierungs-, Autorisierungs- und Buchhaltungsservern, die auf das System zugreifen. NetScaler ADM kann Benutzer unabhängig von den tatsächlichen Protokollen authentifizieren, die sie für die Kommunikation mit dem System verwenden. Wenn ein Benutzer versucht, auf eine Citrix ADM-Implementierung zuzugreifen, die

für die externe Authentifizierung konfiguriert ist, sendet der angeforderte Anwendungsserver den Benutzernamen und das Kennwort zur Authentifizierung an den RADIUS-, LDAP- oder TACACS-Server. Wenn die Authentifizierung erfolgreich ist, erhält der Benutzer Zugriff auf Citrix ADM.

Externe Authentifizierungsserver

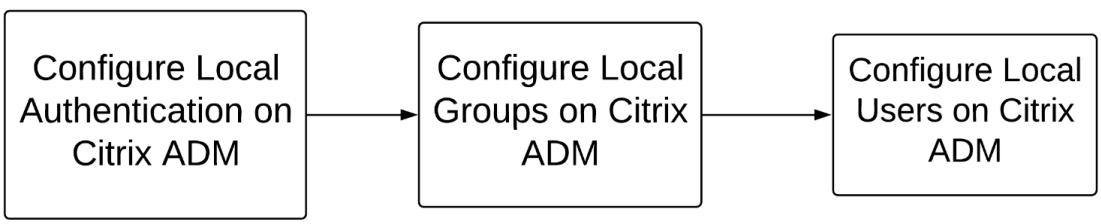
NetScaler ADM sendet alle Anforderungen an Authentifizierungs-, Autorisierungs- und Überwachungsdienste an den Remote-RADIUS-, LDAP- oder TACACS-Server. Der Remote-Authentifizierungs-, Autorisierungs- und Überwachungsserver erhält die Anfrage, validiert die Anfrage und sendet eine Antwort an NetScaler ADM. Bei der Konfiguration für die Verwendung eines RADIUS-, TACACS- oder LDAP-Servers für die Authentifizierung wird NetScaler ADM zu einem RADIUS-, TACACS- oder LDAP-Client. In jeder dieser Konfigurationen werden Authentifizierungsdatensätze in der Remotehostserver-Datenbank gespeichert. Der Kontoname, die zugewiesenen Berechtigungen und die Zeitbuchhaltungsdatensätze werden ebenfalls auf dem Authentifizierungs-, Autorisierungs- und Überwachungsserver für jeden Benutzer gespeichert.

Außerdem können Sie die interne Datenbank von NetScaler ADM verwenden, um Benutzer lokal zu authentifizieren. Sie erstellen Einträge in der Datenbank für Benutzer und deren Kennwörter und Standardrollen. Sie können auch die Authentifizierungsreihenfolge für bestimmte Authentifizierungstypen auswählen. Die Liste der Server in einer Servergruppe ist eine geordnete Liste. Der erste Server in der Liste wird immer verwendet, es sei denn, er ist nicht verfügbar. In diesem Fall wird der nächste Server in der Liste verwendet. Sie können Server so konfigurieren, dass sie die interne Datenbank als Fallback-Authentifizierungsbackup in die konfigurierte Liste der Authentifizierungs-, Autorisierungs- und Überwachungsserver aufnehmen.

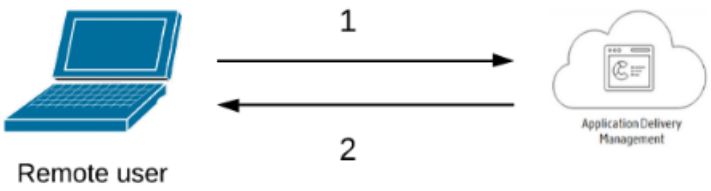
Authentifizieren von Benutzern in NetScaler ADM

Sie können Ihre Benutzer in NetScaler ADM auf zwei Arten authentifizieren:

- In Citrix ADM konfigurierte lokale Benutzer



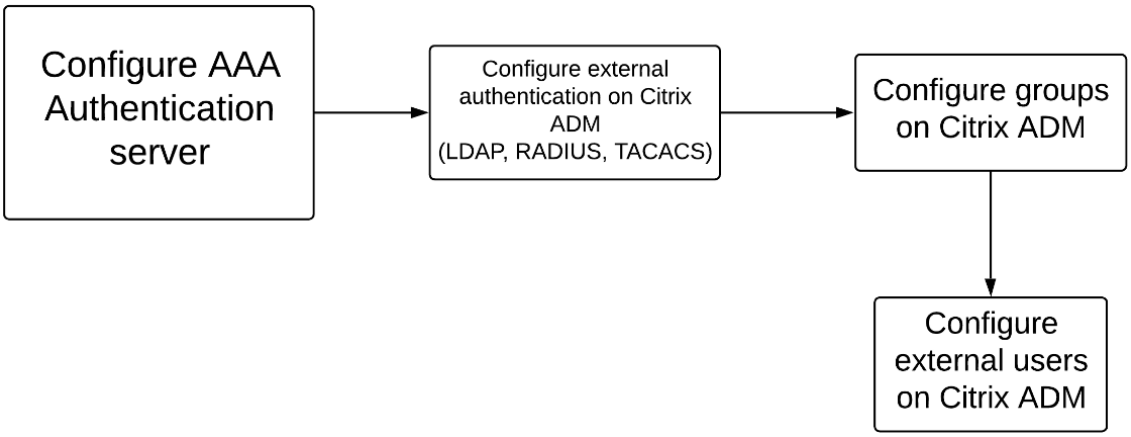
  Nach der Konfiguration ist der folgende Workflow für die Benutzerauthentifizierung auf dem lokalen Server beschrieben.



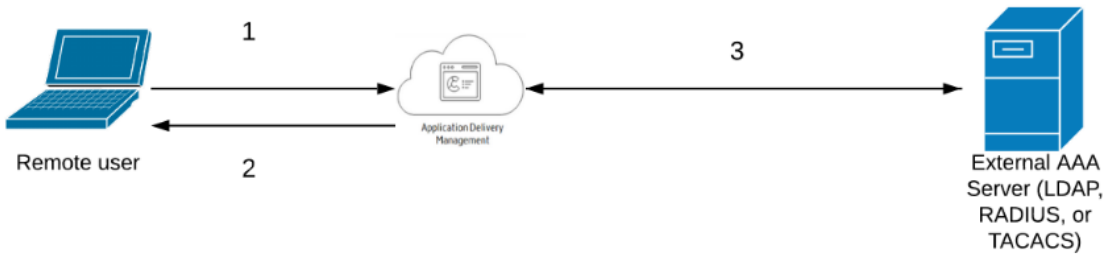
1 —Der Benutzer meldet sich bei Citrix ADM an

2 —Citrix ADM fordert die Benutzer zur Eingabe von Anmeldeinformationen für die Authentifizierung auf und prüft, ob die Anmeldeinformationen in der ADM-Datenbank übereinstimmen.

- Verwendung von externen Authentifizierungsservern



Nach der Konfiguration ist der folgende Workflow für die Benutzerauthentifizierung auf dem externen Authentifizierungs-, Autorisierungs- und Überwachungsserver beschrieben:



1 —Der Benutzer stellt eine Verbindung mit Citrix ADM her

2 —NetScaler ADM fordert den Benutzer zur Eingabe von Anmeldeinformationen auf

3 —NetScaler ADM validiert die Anmeldeinformationen des Benutzers mit dem externen Authentifizierungs-, Autorisierungs- und Überwachungsserver. Wenn die Validierung erfolgreich ist, kann sich der Benutzer weiterhin anmelden

Externe Authentifizierungsserver in NetScaler ADM konfigurieren

February 5, 2024

Nachdem Sie den LDAP-, RADIUS- oder TACACS-Server konfiguriert haben, können Sie diese Server in Citrix ADM hinzufügen.

LDAP-Authentifizierungsserver hinzufügen

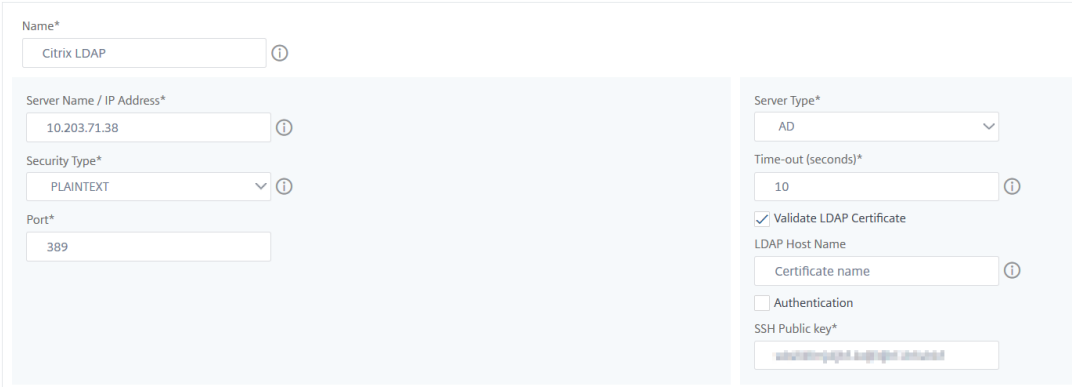
February 5, 2024

Wenn Sie das LDAP-Protokoll mit RADIUS- und TACAS-Authentifizierungsservern integrieren, können Sie ADM verwenden, um Benutzeranmeldeinformationen aus verteilten Verzeichnissen zu suchen und zu authentifizieren.

1. Navigieren Sie zu **System** > **Authentifizierung**.
2. Wählen Sie die Registerkarte **LDAP** aus, und klicken Sie dann auf **Hinzufügen**.
3. Geben Sie auf der Seite „ **LDAP-Server erstellen** “die folgenden Parameter an:
    a) **Name** —Geben Sie den LDAP-Servernamen an
    b) **Servername/IP-Adresse** —Geben Sie die LDAP-IP-Adresse oder den Servernamen an
    c) **Sicherheitstyp** —Art der Kommunikation, die zwischen dem System und dem LDAP-Server erforderlich ist. Wählen Sie aus der Liste aus. Wenn die Klartextkommunikation unzureichend ist, können Sie verschlüsselte Kommunikation wählen, indem Sie entweder Transport Layer Security (TLS) oder SSL auswählen.
    d) **Port** —Standardmäßig wird Port 389 für PLAINTEXT verwendet. Sie können auch Port 636 für SSL/TLS angeben
    e) **Servertyp** —Wählen Sie Active Directory (AD) oder Novell Directory Service (NDS) als Typ des LDAP-Servers aus.
    f) **Timeout (Sekunden)** —Zeit in Sekunden, auf die das NetScaler ADM -System auf eine Antwort vom LDAP-Server wartet
    g) **LDAP-Hostname** —Aktivieren Sie das Kontrollkästchen „LDAP-Zertifikat validieren“und geben Sie den Hostnamen an, der in das Zertifikat eingegeben werden soll

    Deaktivieren Sie die **Authentifizierungsoption**, und geben Sie den öffentlichen SSH-Schlüssel an. Mit der schlüsselbasierten Authentifizierung können Sie jetzt die Liste der

öffentlichen Schlüssel, die auf dem Benutzerobjekt auf dem LDAP-Server gespeichert sind, über SSH abrufen.



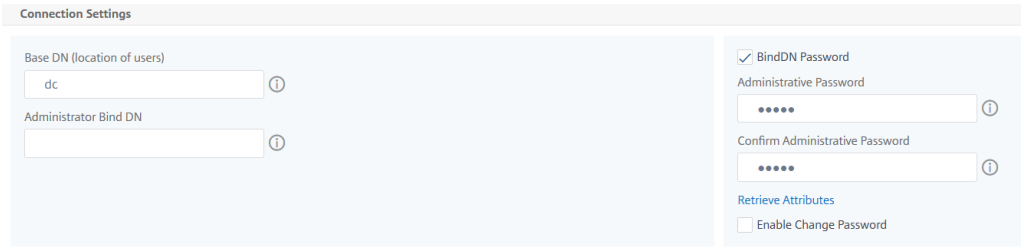
Geben Sie unter Verbindungseinstellungen die folgenden Parameter an:

i. **Basis-DN** —Der Basisknoten für den LDAP-Server, um die Suche zu starten

ii. **Administrator-Bind-DN** —Benutzername, der an den LDAP-Server gebunden ist. Zum Beispiel admin@aaa.local.

iii. **Bind-DN-Kennwort** —Wählen Sie diese Option, um ein Kennwort für die Authentifizierung bereitzustellen

iv. **Kennwort ändern aktivieren** —Wählen Sie diese Option, um die Kennwortänderung zu aktivieren



Geben Sie unter **Andere Einstellungen**die folgenden Parameter an

i. **Server-Anmeldenamensattribut** —Namensattribut, das vom System verwendet wird, um den externen LDAP-Server oder ein Active Directory abzufragen. Wählen Sie **samAccountname** aus der Liste aus.

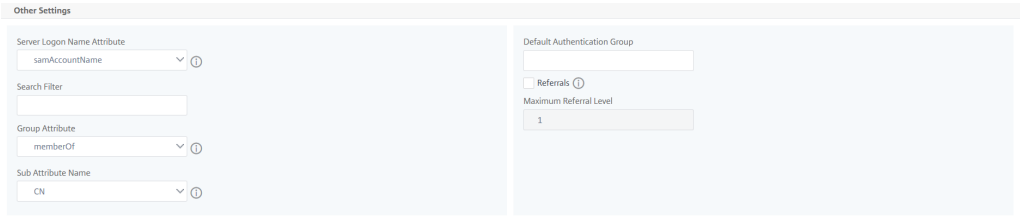
ii. **Suchfilter** —Konfigurieren Sie externe Benutzer für die Zwei-Faktor-Authentifizierung gemäß dem im LDAP-Server konfigurierten Suchfilter. Zum Beispiel würde vpnallowed=true mit ldaploginame `samaccount` und dem vom Benutzer bereitgestellten Benutzernamen bob eine LDAP-Suchzeichenfolge von: ergeben `&(vpnallowed=true)(samaccount=bob)`.

> Hinweis
>
> Standardmäßig sind die Werte im Suchfilter in Klammern eingeschlossen.

iii. **Gruppenattribut** —Wählen Sie MemberOf aus der Liste aus.

iv. **Name des Unterattributs** —Der Name des Unterattributs für die Gruppenextraktion vom LDAP-Server.

v. **Standardauthentifizierungsgruppe** —Standardgruppe, die zusätzlich zu den extrahierten Gruppen ausgewählt wird, wann die Authentifizierung erfolgreich ist.



4. Klicken Sie auf **Erstellen**.

   Der LDAP-Server ist jetzt konfiguriert.

> Hinweis
>
> Wenn die Benutzer Active Directory Gruppenmitglieder sind, müssen die Gruppe und die Namen der Benutzer in NetScaler ADM dieselben Namen von Active Directory Gruppenmitgliedern haben.

RADIUS-Authentifizierungsserver hinzufügen

February 5, 2024

1. Navigieren Sie zu **System** > **Authentifizierung**.
2. Wählen Sie die Registerkarte **RADIUS** aus, und klicken Sie dann auf **Hinzufügen**.

   Geben Sie auf der Seite **RADIUS-Server erstellen** die folgenden Parameter an:

   a) **Name** —Geben Sie einen RADIUS-Servernamen an

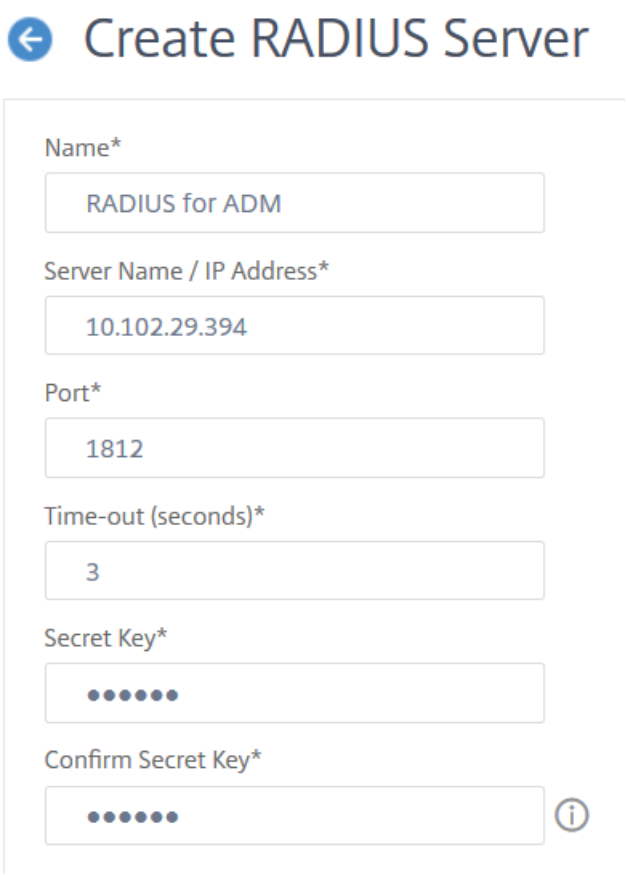
   b) **Servername/IP-Adresse** —Geben Sie die IP-Adresse des RADIUS-Servers an

   c) **Port** —Geben Sie die Portnummer an, auf der der RADIUS-Server gehostet wird. Der Standardport ist 1812

d) **Timeout (Sekunden)** —Zeit in Sekunden, für die das Citrix ADM System auf eine Antwort vom RADIUS-Server wartet

e) **Geheimer Schlüssel** —Geben Sie den geheimen RADIUS-Schlüssel für die Authentifizierung an

f) **Geheimen Schlüssel bestätigen** —Geben Sie den Schlüssel zur Bestätigung erneut an



Geben Sie unter **Details**die folgenden Parameter an:

i. **NAS-ID** —Geben Sie die ID an, um die Kennung an den RADIUS-Server zu senden

ii. **Group Vendor Identifier** —Geben Sie die Anbieter-ID für die Verwendung der RADIUS-Gruppenextraktion an.

iii. **Gruppenpräfix** —Eine Zeichenfolge, die Gruppennamen innerhalb eines RADIUS-Attributs für die RADIUS-Gruppenextraktion vorangeht

iv. **Gruppenattributtyp** —Geben Sie den Attributtyp für die RADIUS-Gruppenextraktion an

v. **Gruppentrennzeichen** —Eine Zeichenfolge, die Gruppennamen innerhalb eines RADIUS-Attributs für die RADIUS-Gruppenextraktion abgrenzt

vi. **IP Address Vendor Identifier** —Die Anbieter-ID in RADIUS bezeichnet die Intranet-IP. Ein Wert von 0 gibt an, dass das Attribut nicht herstellerkodiert ist.

vii. **Kennwort Vendor Identifier** —Anbieter-ID-Kennwort in der RADIUS-Antwort zum Extrahieren des Benutzerkennworts

viii. **IP-Adressattributtyp** —Remote-IP-Adressattribut, auf das der RADIUS antworten soll

ix. **Kennwortattributtyp** —Das Kennwortattribut, auf das RADIUS antworten soll

x. **Kennwortkodierung** —Wählen Sie pap, chap, mschapv1 oder mschapv2 aus der Liste aus. Dies gibt an, wie Kennwörter in den RADIUS-Paketen codiert werden sollten, die vom System zum RADIUS-Server übertragen werden.

xi. **Standardauthentifizierungsgruppe** —Standardgruppe, die zusätzlich zu den extrahierten Gruppen ausgewählt wird, wann die Authentifizierung erfolgreich ist

Wählen Sie Accounting aus, wenn die Appliance Auditinformationen auf dem RADIUS-Server protokollieren soll.

3. Klicken Sie auf **Erstellen**.

Der RADIUS-Server ist jetzt konfiguriert.

TACACS-Authentifizierungsserver hinzufügen

February 5, 2024

1. Navigieren Sie zu **System** > **Authentifizierung**.
2. Wählen Sie die Registerkarte **TACACS** aus, und klicken Sie dann auf **Hinzufügen**.
3. Geben Sie auf der Seite **TACACS erstellen** die folgenden Parameter an:

a) **Name** —Geben Sie einen TACACS-Servernamen an

b) **IP-Adresse** —Geben Sie die TACACS-IP-Adresse an

c) **Port** —Geben Sie die Portnummer an, auf der der TACACS-Server gehostet wird. Der Standardport ist 49

d) **Timeout (Sekunden)** —Zeit in Sekunden, auf die das NetScaler ADM -System auf eine Antwort vom LDAP-Server wartet

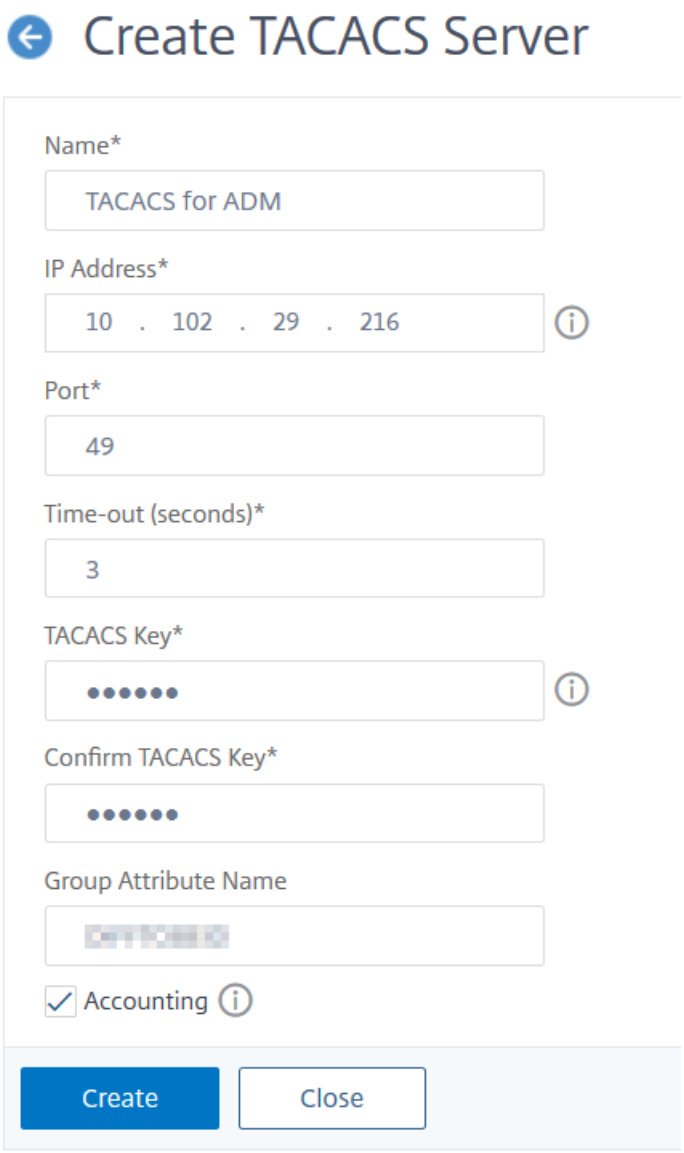
e) **TACACS-Schlüssel** —Geben Sie den TACACS-Schlüssel für die Authentifizierung an

f) **TACACS-Schlüssel bestätigen** —Geben Sie den TACACS-Schlüssel zur Bestätigung erneut an

g) **Name des Gruppenattributs** —Geben Sie den Gruppennamen an

Wählen Sie **Accounting** aus, wenn die Appliance Auditinformationen auf dem TACACS-Server protokollieren soll.

4. Klicken Sie auf **Erstellen**.



Benutzer in NetScaler ADM

February 5, 2024

Sie können Benutzerkonten lokal in NetScaler ADM erstellen, um die Benutzer auf Authentifizierungsservern zu ergänzen. Beispielsweise möchten Sie möglicherweise lokale Benutzerkonten für temporäre Benutzer wie Berater oder Besucher erstellen, ohne einen Eintrag für diese Benutzer auf dem Authentifizierungsserver zu erstellen.

Weitere Informationen zum Konfigurieren von Benutzern finden Sie unter Konfigurieren von Benutzern.

> Hinweis
>
> Wenn sich die Benutzer in Active Directory befinden, stellen Sie sicher, dass der Gruppenname in Citrix ADM mit dem Gruppennamen für die Active Directory-Gruppe auf dem externen Server übereinstimmt.

Benutzergruppen in Citrix ADM

Mit NetScaler ADM können Sie Ihre Benutzer authentifizieren und autorisieren, indem Sie Gruppen erstellen und die Benutzer zu den Gruppen hinzufügen. Eine Gruppe kann entweder über „Admin“- oder „Nur Lesen“-Berechtigungen verfügen, und alle Benutzer in dieser Gruppe erhalten die gleichen Berechtigungen.

In Citrix ADM:

- Eine Gruppe ist definiert als eine Sammlung von Benutzern mit ähnlichen Berechtigungen.
- Eine Gruppe kann eine oder mehrere Rollen haben
- Ein Benutzer ist als eine Entität definiert, die auf der Grundlage der zugewiesenen Berechtigungen Zugriff haben kann.
- Ein Benutzer kann einer oder mehreren Gruppen angehören.

Sie können lokale Gruppen in NetScaler ADM erstellen und die lokale Authentifizierung für die Benutzer in den Gruppen verwenden. Wenn Sie externe Server für die Authentifizierung verwenden, konfigurieren Sie die Gruppen in Citrix ADM so, dass sie den Gruppen entsprechen, die auf Authentifizierungsservern im internen Netzwerk konfiguriert sind. Wenn ein Benutzer sich anmeldet und authentifiziert wird und ein Gruppenname mit einer Gruppe auf einem Authentifizierungsserver übereinstimmt, erbt der Benutzer die Einstellungen für die Gruppe in NetScaler ADM.
Wenn Sie die lokale Authentifizierung verwenden, erstellen Sie Benutzer und fügen Sie sie Gruppen hinzu, die in Citrix ADM konfiguriert sind. Die Benutzer erben dann die Einstellungen für diese Gruppen.

Weitere Informationen zum Konfigurieren von Gruppen und zum Zuweisen von Gruppenberechtigungen finden Sie unter Konfigurieren von Gruppen.

Extrahieren einer Authentifizierungsservergruppe

February 5, 2024

> **Hinweis**
>
> Die TACACS-Serverextraktion wird von **Citrix ADM 13.0**unterstützt.

Mit Citrix ADM können Sie:

- Extrahieren Sie die Liste der Gruppen, denen ein Benutzer auf dem externen Authentifizierungsserver angehört.
- Weisen Sie sie den Gruppeneinstellungen zu, die mit den auf dem externen Server konfigurierten Gruppen übereinstimmen.

Vorteile:

- Sie müssen keine Benutzer in NetScaler ADM erstellen, da sie auf dem externen Server verwaltet werden.
- NetScaler ADM führt die Autorisierung von Benutzern durch Zuweisen von Gruppenberechtigungen für den Zugriff auf bestimmte virtuelle Load Balancer-Server und für bestimmte Anwendungen auf dem System durch.

Fallback und Kaskadierung externer Authentifizierungsserver aktivieren

February 5, 2024

Mit der Fallback-Option kann die lokale Authentifizierung übernommen werden, falls die externe Serverauthentifizierung fehlschlägt. Ein Benutzer, der sowohl auf Citrix ADM als auch auf einem externen Authentifizierungsserver konfiguriert ist, kann sich bei Citrix ADM anmelden, auch wenn die konfigurierten externen Authentifizierungsserver ausgefallen oder nicht erreichbar sind. Um sicherzustellen, dass die Fallback-Authentifizierung funktioniert:

- Nicht-NSRoot-Benutzer müssen auf Citrix ADM zugreifen können, wenn der externe Server ausgefallen oder nicht erreichbar ist
- Sie müssen mindestens einen externen Server hinzufügen

NetScaler ADM unterstützt außerdem ein einheitliches System von Authentifizierungs-, Autorisierungs- und Abrechnungsprotokollen (AAA) (LDAP, RADIUS und TACACS) sowie lokale Authentifizierung. Diese vereinheitlichte Unterstützung bietet eine gemeinsame Schnittstelle zur Authentifizierung und Autorisierung aller Benutzer und externen AAA-Clients, die auf das System zugreifen.

NetScaler ADM kann Benutzer unabhängig von den tatsächlichen Protokollen authentifizieren, die sie für die Kommunikation mit dem System verwenden.
Kaskadierende externe Authentifizierungsserver bieten einen kontinuierlichen, fehlerfreien Prozess zur Authentifizierung und Autorisierung externer Benutzer. Wenn die Authentifizierung auf dem ersten Authentifizierungsserver fehlschlägt, versucht NetScaler ADM, den Benutzer mithilfe des zweiten externen Authentifizierungsservers zu authentifizieren usw. Um die kaskadierte Authentifizierung zu aktivieren, müssen Sie die externen Authentifizierungsserver in Citrix ADM hinzufügen. Sie können jeden Typ der unterstützten externen Authentifizierungsserver (RADIUS, LDAP und TACACS) hinzufügen.

Stellen Sie sich beispielsweise vor, dass Sie vier externe Authentifizierungsserver hinzufügen und zwei RADIUS-Server, einen LDAP-Server und einen TACACS-Server konfigurieren möchten. Citrix ADM versucht, sich auf der Grundlage der Konfigurationen bei den externen Servern zu authentifizieren. In diesem Beispielszenario versucht Citrix ADM:

- Stellen Sie eine Verbindung zum ersten RADIUS-Server her
- Stellen Sie eine Verbindung zum zweiten RADIUS-Server her, wenn die Authentifizierung mit dem ersten RADIUS-Server fehlgeschlagen ist
- Stellen Sie eine Verbindung zum LDAP-Server her, wenn die Authentifizierung mit beiden RADIUS-Servern fehlgeschlagen ist
- Stellen Sie eine Verbindung zum TACACS-Server her, wenn die Authentifizierung sowohl bei RADIUS-Servern als auch beim LDAP-Server fehlgeschlagen ist.

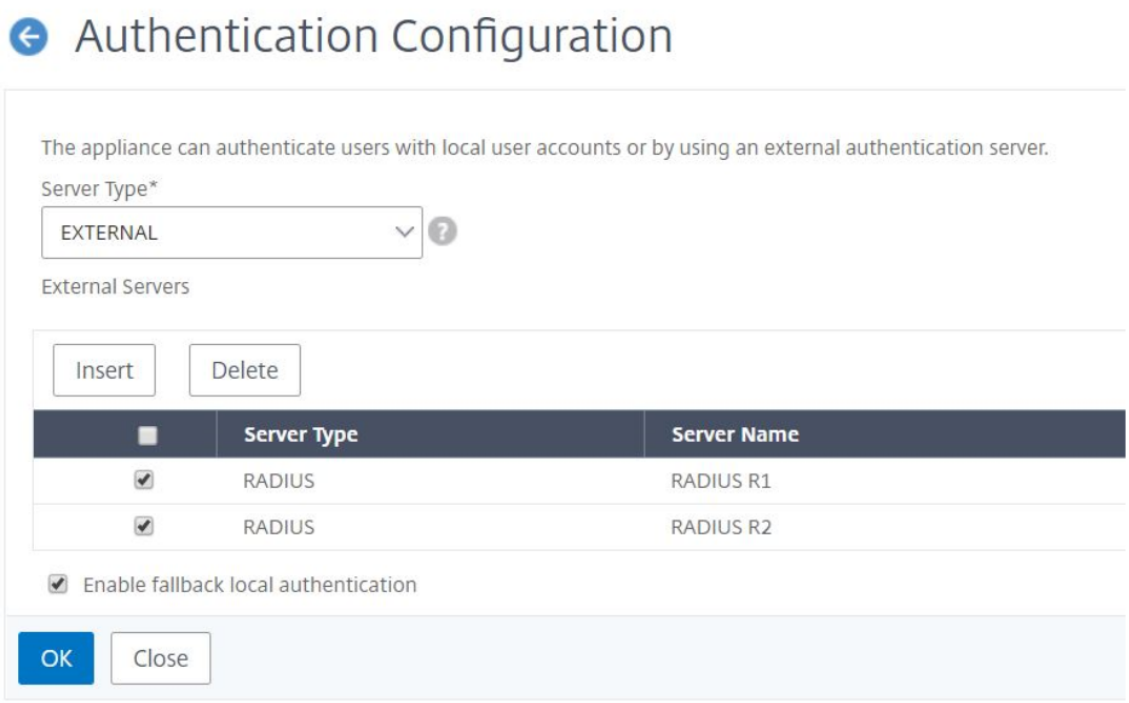
> Hinweis
>
> Sie können bis zu 32 externe Authentifizierungsserver in NetScaler ADM konfigurieren.

Konfigurieren von Fallback und Kaskadierung externer Server

1. Navigieren Sie zu **System** > **Authentifizierung**.
2. Klicken Sie auf der Seite **Authentifizierung** auf **Einstellungen**.
3. Wählen Sie auf der Seite **Authentifizierungskonfiguration** in der Liste **Servertyp** die Option **EXTERNAL** aus (nur externe Server können kaskadiert werden).
4. Klicken Sie auf **Einfügen**und wählen Sie auf der Seite **Externe Server** einen oder mehrere Authentifizierungsserver aus, die kaskadiert werden sollen.

5. Aktivieren Sie das Kontrollkästchen **Lokale Fallback-Authentifizierung aktivieren**, wenn die lokale Authentifizierung übernommen werden soll, wenn die externe Authentifizierung fehlschlägt.
6. Aktivieren Sie das Kontrollkästchen **Externe Gruppeninformationen protokollieren**, wenn Sie die externen Benutzergruppeninformationen im Systemüberwachungsprotokoll erfassen möchten.
7. Klicken Sie auf **OK**, um die Seite zu schließen.

   Die ausgewählten Server werden unter Externe Server angezeigt:



Sie können die Reihenfolge der Authentifizierung auch angeben, indem Sie das Symbol neben den Servernamen verwenden, um Server in der Liste nach oben oder unten zu verschieben.

Zugriffssteuerung

February 5, 2024

Authentifizierung ist ein Prozess, mit dem Sie überprüfen, ob jemand der ist, der sie behauptet, dass sie sind. Um eine Authentifizierung durchzuführen, muss ein Benutzer bereits über ein Konto in einem System verfügen, das durch den Authentifizierungsmechanismus abgefragt werden kann, oder ein Konto muss im Rahmen des Prozesses der ersten Authentifizierung erstellt werden. NetScaler Application Delivery Management (ADM) bietet eine Methode zur Authentifizierung sowohl lokaler als

auch externer Benutzer. Während lokale Benutzer intern authentifiziert werden, unterstützt Citrix ADM die externe Authentifizierung mit RADIUS-, LDAP- und TACACS-Protokollen. Wenn ein Benutzer versucht, auf NetScaler ADM zuzugreifen, das für die externe Authentifizierung konfiguriert ist, sendet der angeforderte Anwendungsserver den Benutzernamen und das Kennwort zur Authentifizierung an den RADIUS-, LDAP- oder TACACS-Server. Nach der Authentifizierung wird das erforderliche Protokoll verwendet, um den Benutzer in Citrix ADM zu identifizieren.

Zugriffskontrolle ist der Prozess, bei dem die erforderliche Sicherheit für eine bestimmte Ressource durchgesetzt wird. Es handelt sich um eine Sicherheitstechnik, mit der reguliert werden kann, wer Ressourcen in einer Computerumgebung einsehen oder verwenden kann. Der Zweck der Zugriffskontrolle besteht darin, die Aktionen oder Vorgänge einzuschränken, die ein rechtmäßiger Benutzer eines Computersystems ausführen kann. Die Zugriffskontrolle schränkt ein, was ein Benutzer direkt tun kann und welche Programme, die im Namen der Benutzer ausgeführt werden, ausführen dürfen. Auf diese Weise zielt die Zugriffssteuerung darauf ab, Aktivitäten zu verhindern, die zu einer Sicherheitsverletzung führen können. Bei der Zugriffssteuerung wird davon ausgegangen, dass die Authentifizierung des Benutzers vor der Erzwingung der Zugriffssteuerung über einen Referenzmonitor erfolgreich überprüft wurde. Citrix ADM ermöglicht eine feinkörnige, rollenbasierte Zugriffssteuerung (RBAC), mit der die Administratoren Benutzern Zugriffsberechtigungen basierend auf den Rollen einzelner Benutzer in einem Unternehmen bereitstellen können. RBAC in NetScaler ADM wird durch das Erstellen von Zugriffsrichtlinien, Rollen, Gruppen und Benutzern erreicht.

Rollenbasierte Zugriffssteuerung

February 5, 2024

Citrix ADM bietet eine abgestimmte, rollenbasierte Zugriffssteuerung (RBAC), mit der Sie Zugriffsberechtigungen basierend auf den Rollen einzelner Benutzer in Ihrem Unternehmen erteilen können. In diesem Zusammenhang ist der Zugriff die Möglichkeit, eine bestimmte Aufgabe auszuführen, z. B. eine Datei anzuzeigen, zu erstellen, zu ändern oder zu löschen. Rollen werden entsprechend der Autorität und Verantwortlichkeit der Benutzer innerhalb des Unternehmens definiert. Beispielsweise kann ein Benutzer alle Netzwerkvorgänge ausführen, während ein anderer Benutzer den Datenverkehrsfluss in Anwendungen beobachten und beim Erstellen von Konfigurationsvorlagen helfen kann.

Rollen werden durch in Richtlinien festgelegt. Nachdem Sie Richtlinien erstellt haben, erstellen Sie Rollen, binden jede Rolle an eine oder mehrere Richtlinien und weisen Benutzern Rollen zu. Sie können auch Benutzergruppen Rollen zuweisen.

Eine Gruppe ist eine Sammlung von Benutzern, die über gemeinsame Berechtigungen verfügen. Beispielsweise können Benutzer, die ein bestimmtes Rechenzentrum verwalten, einer Gruppe

zugewiesen werden. Eine Rolle ist eine Identität, die Benutzern oder Gruppen auf der Grundlage bestimmter Bedingungen gewährt wird. In NetScaler ADM ist das Erstellen von Rollen und Richtlinien spezifisch für die RBAC-Funktion in NetScaler ADC. Rollen und Richtlinien können einfach erstellt, geändert oder eingestellt werden, wenn sich die Anforderungen des Unternehmens entwickeln, ohne dass die Berechtigungen für jeden Benutzer individuell aktualisiert werden müssen.

Rollen können feature- oder ressourcenbasiert sein. Stellen Sie sich beispielsweise einen SSL-/Sicherheitsadministrator und einen Anwendungsadministrator vor. Ein SSL/Security-Administrator muss über vollständigen Zugriff auf die Verwaltungs- und Überwachungsfunktionen von SSL-Zertifikaten verfügen, muss jedoch über schreibgeschützten Zugriff für Systemadministrationsvorgänge verfügen. Ein Anwendungsadministrator muss nur auf die Ressourcen innerhalb des Bereichs zugreifen können.

Beispiel:

Chris, der Leiter der ADC-Gruppe, ist der Superadministrator von NetScaler ADM in seiner Organisation. Chris erstellt drei Administratorrollen: Sicherheitsadministrator, Anwendungsadministrator und Netzwerkadministrator.

David, der Sicherheitsadministrator, muss über vollständigen Zugriff auf die Verwaltung und Überwachung von SSL-Zertifikaten verfügen, aber auch über schreibgeschützten Zugriff für den Systemverwaltungsbetrieb verfügen.

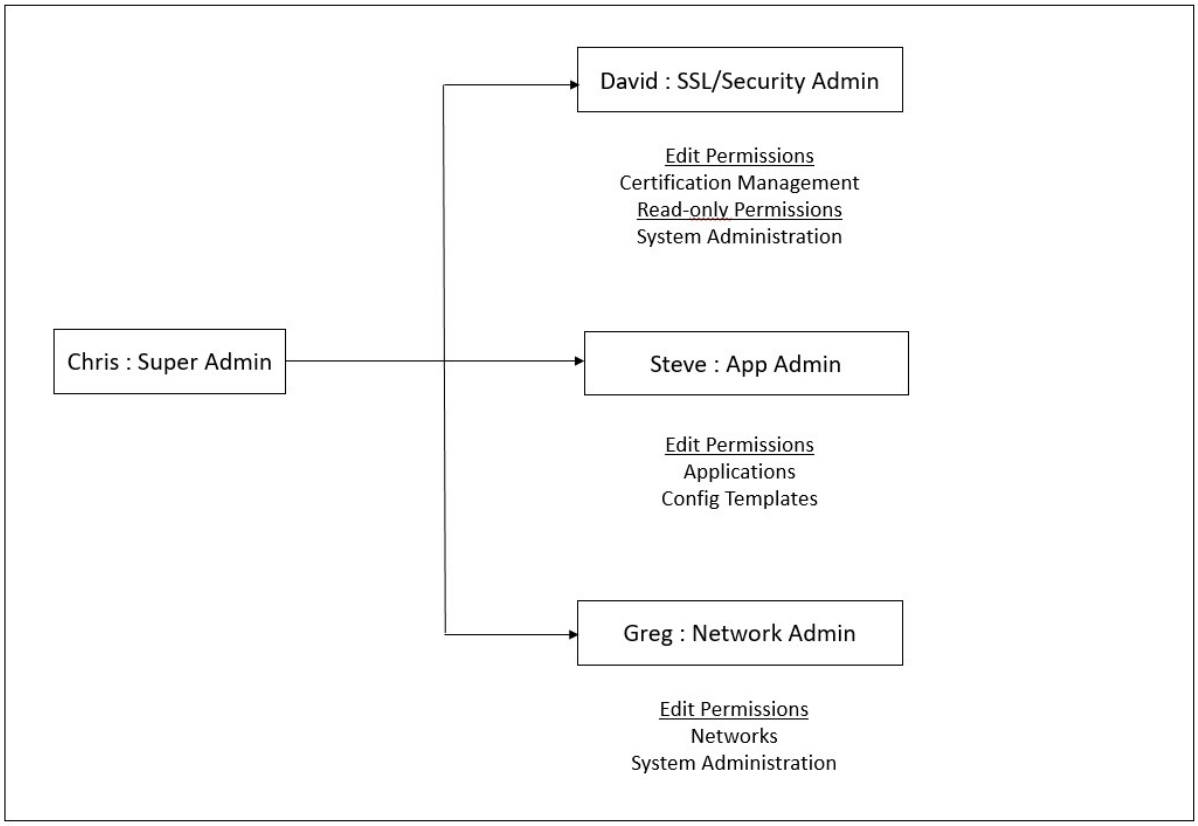
Steve, ein Anwendungsadministrator, benötigt nur Zugriff auf bestimmte Anwendungen und nur bestimmte Konfigurationsvorlagen.

Greg, ein Netzwerkadministrator, benötigt Zugriff auf System- und Netzwerkadministration.

Chris muss auch RBAC für alle Benutzer bereitstellen, unabhängig davon, dass sie lokal oder extern sind.

Benutzer von NetScaler ADM können lokal authentifiziert oder über einen externen Server (RADIUS/LDAP/TACACS) authentifiziert werden. RBAC-Einstellungen müssen unabhängig von der verwendeten Authentifizierungsmethode für alle Benutzer gelten.

Das folgende Bild zeigt die Berechtigungen, die Administratoren und andere Benutzer haben und ihre Rollen in der Organisation.



Einschränkungen

RBAC wird für die folgenden Citrix ADM Funktionen nicht vollständig unterstützt:

- **Analytics** - RBAC wird in den Analytics-Modulen nicht vollständig unterstützt. Die RBAC-Unterstützung ist auf Instanzebene beschränkt und gilt nicht auf Anwendungsebene in den Analyse-Modulen Web Insight, SSL Insight, Gateway Insight, HDX Insight und Security Insight. Beispiel:

Beispiel 1: Instanzbasierte RBAC (unterstützt)

Ein Administrator, dem einige Instanzen zugewiesen wurden, kann unter **Web Insight** > **Instances** nur diese Instanzen und unter **Web Insight** > **Applications** nur die entsprechenden virtuellen Server sehen, da RBAC auf Instanzebene unterstützt wird.

Beispiel 2: Anwendungsbasiertes RBAC (nicht unterstützt)

Ein Administrator, dem einige Anwendungen zugewiesen wurden, kann alle virtuellen Server unter **Web Insight** > **Anwendungen** sehen, kann aber nicht auf sie zugreifen, da RBAC auf Anwendungsebene nicht unterstützt wird.

- **StyleBooks** —RBAC wird für StyleBooks nicht vollständig unterstützt.

  - In NetScaler ADM werden StyleBooks und Konfigurationspakete als separate Ressourcen betrachtet. Zugriffsberechtigungen, entweder Anzeigen, Bearbeiten oder beides, können für StyleBook und Konfigurationspakete separat oder gleichzeitig bereitgestellt werden. Eine Anzeige- oder Bearbeitungsberechtigung für Konfigurationspakete ermöglicht es dem Benutzer implizit, die StyleBooks anzuzeigen, was für das Abrufen der Details des Konfigurationspakets und das Erstellen von Konfigurationspaketen
  - Die Zugriffsberechtigung für bestimmte StyleBook oder Konfigurationspakete wird nicht unterstützt
    Beispiel: Wenn es bereits ein Konfigurationspaket auf der Instanz gibt, können Benutzer die Konfiguration auf einer NetScaler ADC-Zielinstanz ändern, auch wenn sie keinen Zugriff auf diese Instanz haben.

- **Orchestrierung** - RBAC wird für Orchestration nicht unterstützt.

Zugriffsrichtlinien konfigurieren

February 5, 2024

Zugriffsrichtlinien definieren Berechtigungen. Eine Richtlinie kann auf einen einzelnen Benutzer oder eine Gruppe oder auf mehrere Benutzer und mehrere Gruppen angewendet werden. Citrix Application Delivery Management (ADM) bietet vier vordefinierte Zugriffsrichtlinien:

1. **Admin-Richtlinie.** Gewährt Zugriff auf alle Citrix ADM-Funktionen. Der Benutzer verfügt sowohl über Ansichts- als auch über Bearbeitungsberechtigungen, kann alle NetScaler ADM-Inhalte anzeigen und alle Bearbeitungsvorgänge ausführen. Das heißt, der Benutzer kann Operationen zum Hinzufügen, Ändern und Löschen an den Ressourcen ausführen.
2. **Richtlinie nur zum Lesen**. Gewährt schreibgeschützte Berechtigungen. Der Benutzer kann den gesamten Inhalt auf Citrix ADM anzeigen, ist jedoch nicht berechtigt, Vorgänge auszuführen.
3. **appAdminPolicy**. Gewährt Administratorberechtigungen für den Zugriff auf die Anwendungsfunktionen in NetScaler ADM. Ein Benutzer, der an diese Richtlinie gebunden ist, kann benutzerdefinierte Anwendungen hinzufügen, ändern und löschen und die Dienste, Dienstgruppen und die verschiedenen virtuellen Server für Content Switching, Cache-Umleitung und virtuelle HAProxy-Server aktivieren oder deaktivieren.
4. **appReadOnlyPolicy**. Gewährt schreibgeschützte Berechtigung für Anwendungsfunktionen. Ein an diese Richtlinie gebundener Benutzer kann die Anwendungen anzeigen, aber keine Vorgänge zum Hinzufügen, Ändern, Löschen, Aktivieren oder Deaktivieren ausführen.

> **Hinweis** Die vordefinierten Richtlinien können nicht bearbeitet werden.

Sie können auch Ihre eigenen (benutzerdefinierten) Richtlinien erstellen.

So erstellen Sie benutzerdefinierte Zugriffsrichtlinien:

1. Navigieren Sie in Citrix ADM zu **System** > **Benutzerverwaltung** > **Zugriffsrichtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Richtlinienname** den Namen der Richtlinie und die Beschreibung in das Feld **Richtlinienbeschreibung** ein.

   Im Abschnitt **Berechtigungen** werden alle NetScaler ADM-Funktionen mit Optionen zum Angeben von schreibgeschütztem Zugriff, Aktivieren/Deaktivieren oder Bearbeiten aufgeführt.
4. Klicken Sie auf das Symbol (+), um jede Feature-Gruppe in mehrere Features zu erweitern.

   a) Aktivieren Sie das Kontrollkästchen Berechtigung neben dem Feature-Namen, um den Benutzern Berechtigungen zu erteilen.

   - **Ansicht:** Mit dieser Option kann der Benutzer das Feature in NetScaler ADM anzeigen.
   - **Aktivieren-Deaktivieren:** Diese Option ist nur für die **Netzwerkfunktionsfunktionen** verfügbar, die das Aktivieren oder Deaktivieren von Aktionen in NetScaler ADM ermöglichen. Benutzer können die Funktion aktivieren oder deaktivieren. Und der Benutzer kann auch die Aktion **Jetzt abfragen** ausführen.

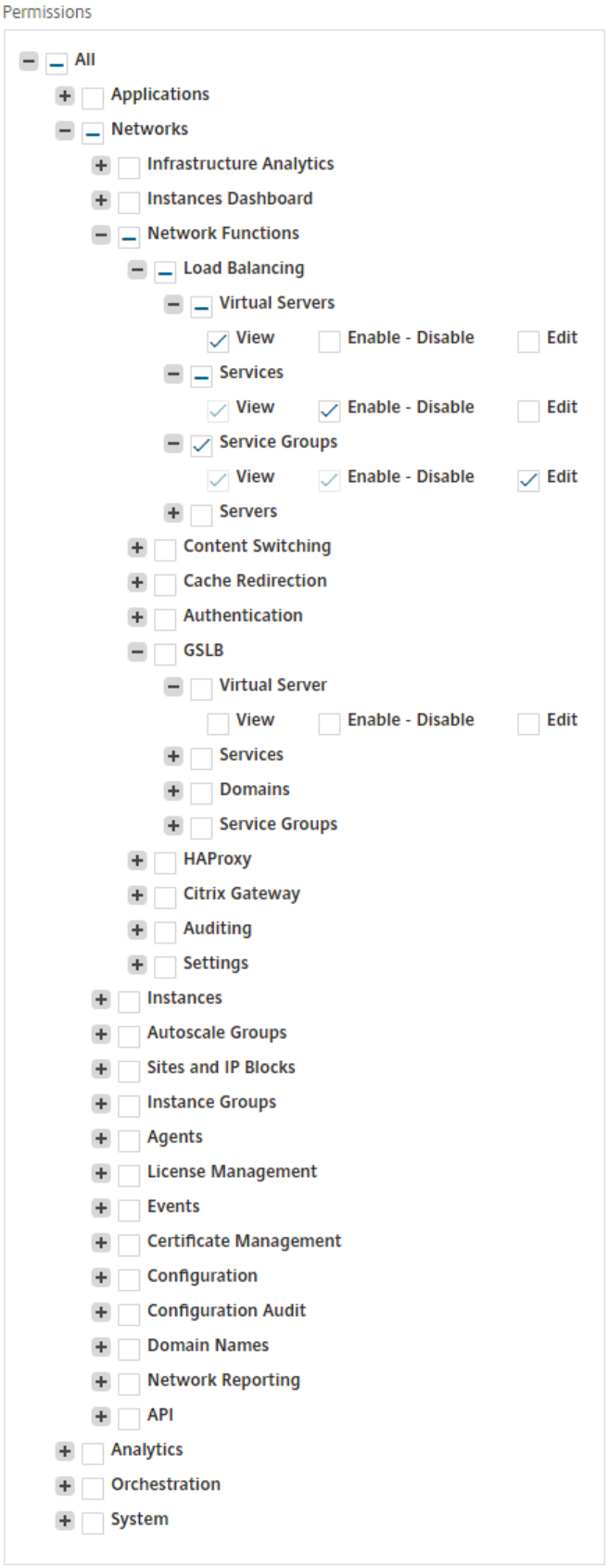
     Wenn Sie einem Benutzer die Berechtigung zum Aktivieren und **Deaktivieren** erteilen, wird auch die Berechtigung **Anzeigen** erteilt. Sie können diese Option nicht deaktivieren.
   - **Bearbeiten:** Diese Option gewährt dem Benutzer vollen Zugriff. Der Benutzer kann das Feature und seine Funktionen ändern.

     Wenn Sie die Berechtigung **Bearbeiten** erteilen, werden sowohl die Berechtigungen **Anzeigen** als auch **Aktivieren/Deaktivieren** gewährt. Sie können die Auswahl der automatisch ausgewählten Optionen nicht aufheben.

   Wenn Sie das Kontrollkästchen Feature aktivieren, werden alle Berechtigungen für das Feature ausgewählt.

   > **Hinweis: Erweitern Sie**
   >
   > Load Balancing und GSLB, um weitere Konfigurationsoptionen anzuzeigen.

   In der folgenden Abbildung haben die Konfigurationsoptionen der Load Balancing-Funktion unterschiedliche Berechtigungen:



Die **View-Berechtigung** wird einem Benutzer für die Funktion **Virtuelle Server** erteilt. Benutzer können die virtuellen Lastausgleichsserver in NetScaler ADM anzeigen. Um virtuelle Server anzuzeigen, navigieren Sie zu **Netzwerke** > **Netzwerkfunktionen** > **Load Balancing** und wählen Sie die Registerkarte **Virtuelle Server** aus.

Die Berechtigung **Aktivieren-Deaktivieren** wird einem Benutzer für die Funktion **Dienste** gewährt. Mit dieser Berechtigung wird auch die **View-Berechtigung** erteilt. Benutzer können die Dienste aktivieren oder deaktivieren, die an einen virtuellen Lastausgleichsserver gebunden sind. Außerdem kann Benutzer die Aktion **Jetzt abfragen** für Dienste ausführen. Um Dienste zu aktivieren oder zu deaktivieren, navigieren Sie zu **Netzwerke** > **Netzwerkfunktionen** > **Lastenausgleich** und wählen Sie die Registerkarte **Dienste**.

> **Hinweis**
>
> Wenn ein Benutzer über die Berechtigung **Enable-Disable**verfügt, ist die Aktion zum Aktivieren oder Deaktivieren für einen Dienst auf der folgenden Seite eingeschränkt:
>
> a) Navigieren Sie zu **Netzwerke** > **Netzwerkfunktionen**.
>
> b) Wählen Sie einen virtuellen Server aus, und klicken Sie auf **Konfigurieren**.
>
> c) Wählen Sie die Seite **Load Balancing Virtual Server Service Binding** .
> Auf dieser Seite wird eine Fehlermeldung angezeigt, wenn Sie **Aktivieren** oder **Deaktivieren**auswählen.

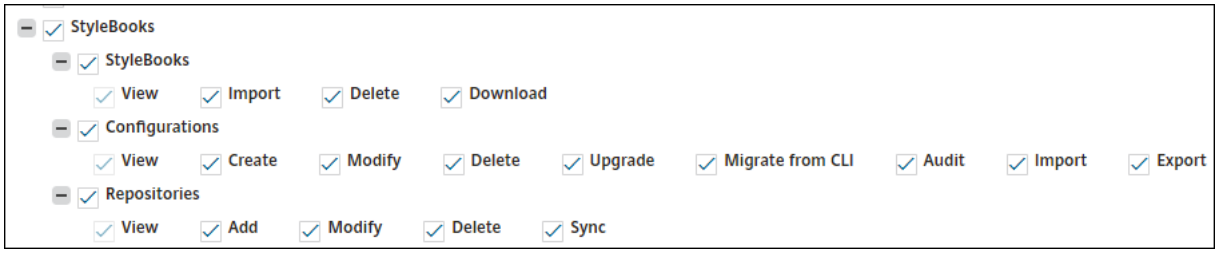
Die Berechtigung **Bearbeiten** wird einem Benutzer für die Funktion **Dienstgruppen** erteilt. Diese Berechtigung gewährt den vollen Zugriff, bei dem die Berechtigungen **Anzeigen** und **Enable-Disable** gewährt werden. Benutzer können die Dienstgruppen ändern, die an einen virtuellen Lastausgleichsserver gebunden sind. Um Dienstgruppen zu bearbeiten, navigieren Sie zu **Netzwerke** > **Netzwerkfunktionen** > **Load Balancing** und wählen Sie die Registerkarte **Dienstgruppen** aus.

5. Klicken Sie auf **Erstellen**.

Erteilen von StyleBook-Berechtigungen für Benutzer

Sie können eine Zugriffsrichtlinie erstellen, um StyleBook-Berechtigungen wie Importieren, Löschen, Herunterladen und mehr zu erteilen.

> **Hinweis**
>
> Die Anzeigeberechtigung wird automatisch aktiviert, wenn Sie andere StyleBook-Berechtigungen erteilen.



Gruppen konfigurieren

February 5, 2024

In NetScaler ADM kann eine Gruppe sowohl auf Feature- als auch auf Ressourcenebene zugreifen. Beispielsweise kann eine Benutzergruppe nur auf ausgewählte NetScaler ADC-Instanzen zugreifen, eine andere Gruppe mit nur wenigen ausgewählten Anwendungen usw.

Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, Zugriff auf Anwendungsebene für die Gruppe gewähren und der Gruppe Benutzer zuweisen. Allen Benutzern in dieser Gruppe werden in NetScaler ADM dieselben Zugriffsrechte zugewiesen.

Sie können einen Benutzerzugriff in NetScaler ADM auf der einzelnen Ebene von Netzwerkfunktionsentitäten verwalten. Sie können dem Benutzer oder der Gruppe auf Entitätsebene dynamisch bestimmte Berechtigungen zuweisen.

NetScaler ADM behandelt virtuelle Server, Dienste, Dienstgruppen und Server als Netzwerkfunktions-Entitäten.

- **Virtueller Server (Anwendungen)** —Load Balancing (lb), GSLB, Context Switching (CS), Cache-Umleitung (CR), Authentifizierung (`Auth`) und Citrix Gateway (VPN)
- **Services** - Lastenausgleich und GSLB-Dienste
- **Dienstgruppe** —Load Balancing und GSLB-Dienstgruppen
- **Server** —Load Balancing-Server

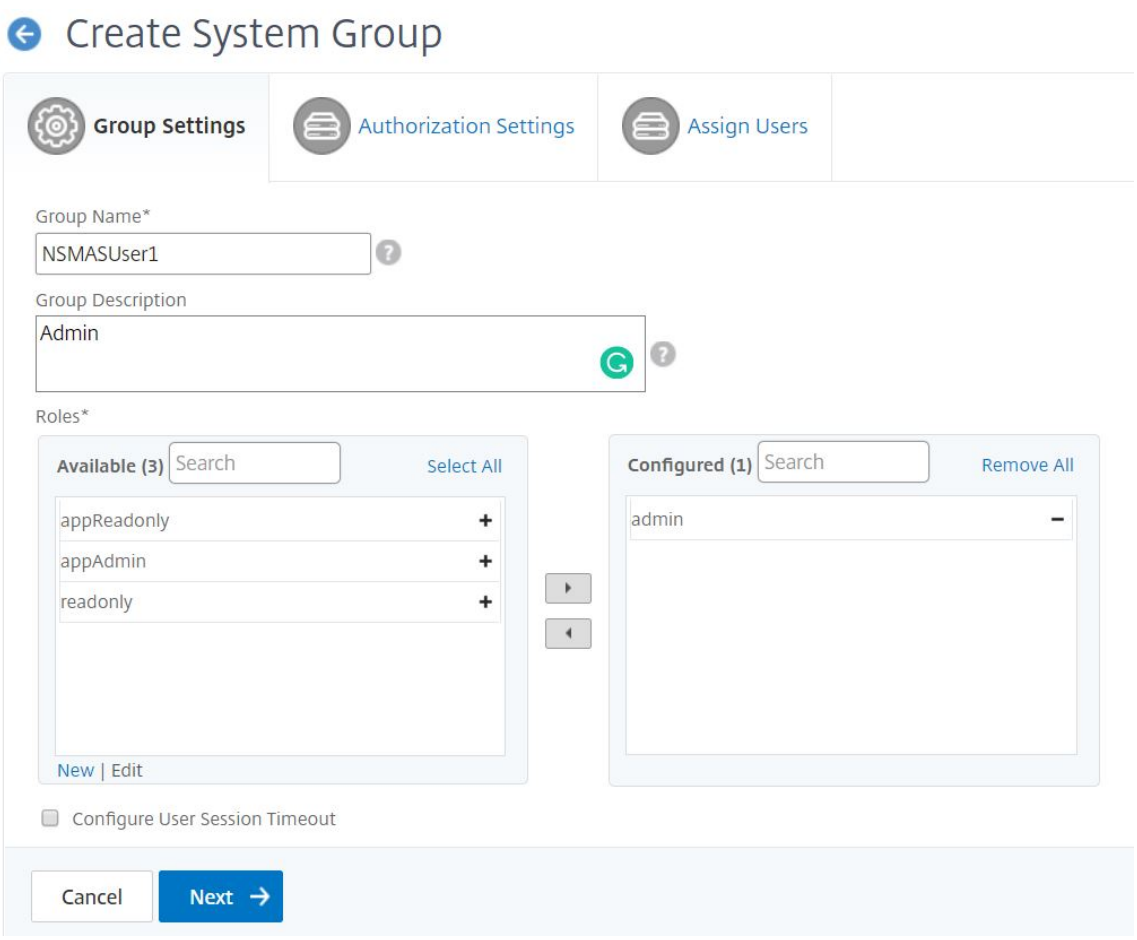
Erstellen einer Benutzergruppe

1. Navigieren Sie in NetScaler ADM zu **System** > **Benutzerverwaltung** > **Gruppen**.
2. Klicken Sie auf **Hinzufügen**.

   Die Seite **Systemgruppe erstellen** wird angezeigt.
3. Geben Sie im Feld **Gruppenname** den Namen der Gruppe ein.

4. Geben Sie im Feld**Gruppenbeschreibung** eine Beschreibung Ihrer Gruppe ein. Eine gute Beschreibung der Gruppe hilft Ihnen, die Rolle und Funktion der Gruppe zu einem späteren Zeitpunkt besser zu verstehen.
5. Fügen Sie im Abschnitt **Rollen** eine oder mehrere Rollen zur Liste **Konfiguriert** hinzu oder verschieben Sie sie.

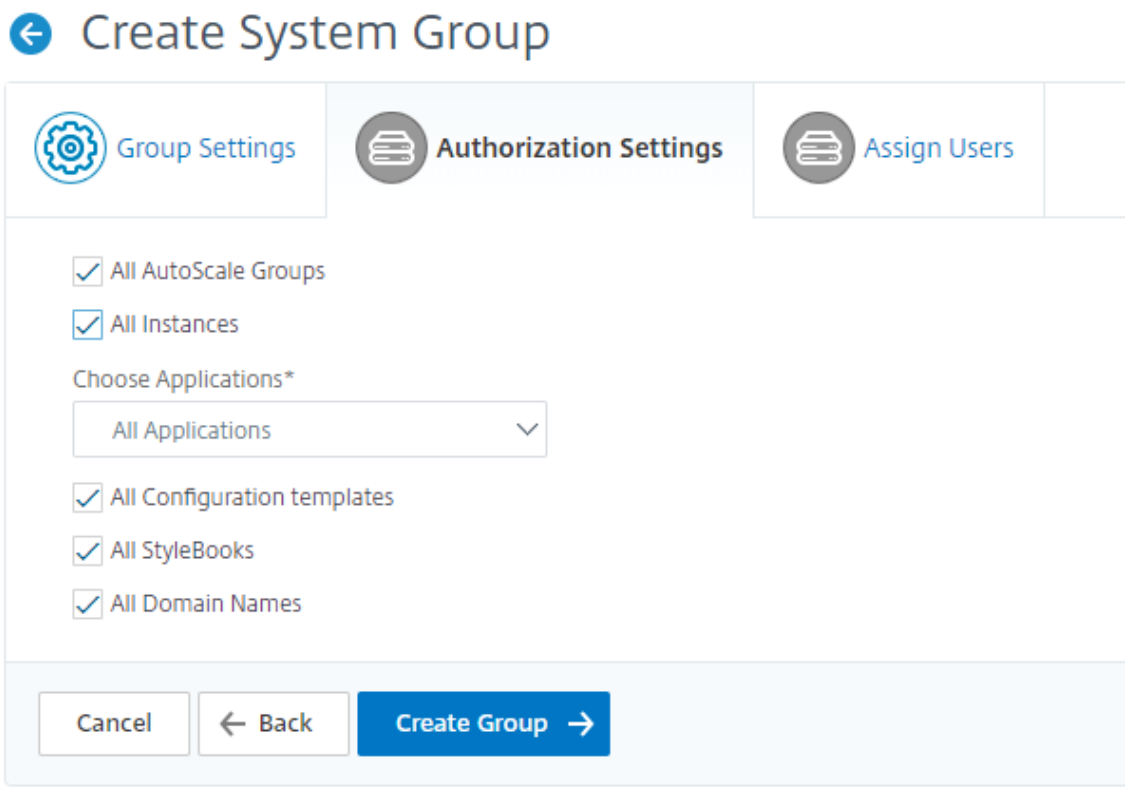
> **Hinweis**
> Unter der Liste **Verfügbar** können Sie auf **Neu** oder **Bearbeiten** klicken und Rollen erstellen oder ändern. Alternativ können Sie zu **System** > **Benutzerverwaltung** > **Benutzer navigieren und Benutzer** erstellen oder ändern.



6. Klicken Sie auf **Weiter**.Auf der Registerkarte **Autorisierungseinstellungen** können Sie Autorisierungseinstellungen für die folgenden Ressourcen angeben:

   - Autoscale-Gruppen
   - Instanzen
   - Anwendungen
   - Konfigurationsvorlagen

- StyleBooks
- Konfigurationspakete
- Domänennamen



Möglicherweise möchten Sie bestimmte Ressourcen aus den Kategorien auswählen, auf die Benutzer Zugriff haben können.

Autoscale-Gruppen:

Wenn Sie die spezifischen Autoscale-Gruppen auswählen möchten, die ein Benutzer anzeigen oder verwalten kann, gehen Sie wie folgt vor:

a) Deaktivieren Sie das Kontrollkästchen **Alle AutoScale-Gruppen**, und klicken Sie auf **AutoScale-Gruppen hinzufügen**.

b) Wählen Sie die erforderlichen Autoscale-Gruppen aus der Liste aus, und klicken Sie auf **OK**.

Instanzen:

Wenn Sie die spezifischen Instanzen auswählen möchten, die ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

a) Deaktivieren Sie das Kontrollkästchen **Alle Instanzen** und klicken Sie auf **Instanzen auswählen**.

b) Wählen Sie die erforderlichen Instanzen aus der Liste aus und klicken Sie auf **OK**.

Anwendungen:

In der Liste **Anwendungen auswählen** können Sie einem Benutzer Zugriff auf die erforderlichen Anwendungen gewähren.

Sie können Anwendungen Zugriff gewähren, ohne deren Instanzen auszuwählen. Weil Anwendungen unabhängig von ihren Instanzen sind, um Benutzerzugriff zu gewähren.

Wenn Sie einem Benutzer Zugriff auf eine Anwendung gewähren, ist der Benutzer berechtigt, unabhängig von der Instanzauswahl nur auf diese Anwendung zuzugreifen.

Diese Liste bietet Ihnen die folgenden Optionen:

- **Alle Anwendungen:** Diese Option ist standardmäßig ausgewählt. Es fügt alle Anwendungen hinzu, die im NetScaler ADM vorhanden sind.
- **Alle Anwendungen ausgewählter Instanzen:** Diese Option wird nur angezeigt, wenn Sie Instanzen aus der Kategorie **Alle Instanzen** auswählen. Es fügt alle Anwendungen hinzu, die auf der ausgewählten Instanz vorhanden sind.
- **Bestimmte Anwendungen:** Mit dieser Option können Sie die erforderlichen Anwendungen hinzufügen, auf die Benutzer zugreifen sollen. Klicken Sie auf **Anwendungen hinzufügen**, und wählen Sie die erforderlichen Anwendungen aus der Liste aus.
- **Individuellen Entitätstyp auswählen:** Mit dieser Option können Sie einen bestimmten Typ von Netzwerkfunktionsentität und entsprechende Entitäten auswählen.

  Sie können entweder einzelne Entitäten hinzufügen oder alle Entitäten unter dem erforderlichen Entitätstyp auswählen, um einem Benutzer den Zugriff zu gewähren.

  Die Option **Auch auf gebundene Entitäten anwenden** autorisiert die Entitäten, die an den ausgewählten Entitätstyp gebunden sind. Wenn Sie beispielsweise eine Anwendung auswählen und **auch auf gebundene Entitäten anwenden**auswählen, autorisiert Citrix ADM alle Entitäten, die an die ausgewählte Anwendung gebunden sind.

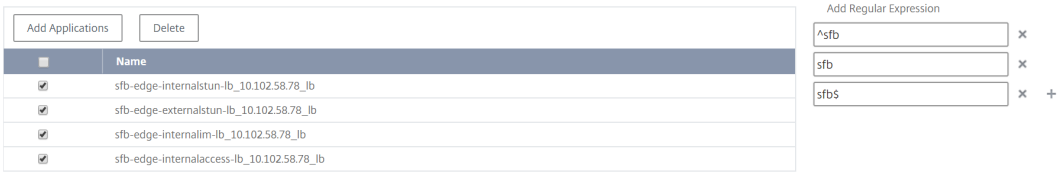
  > **Hinweis**
  >
  > Stellen Sie sicher, dass Sie nur einen Entitätstyp ausgewählt haben, wenn Sie gebundene Entitäten autorisieren möchten.

Sie können reguläre Ausdrücke verwenden, um die Netzwerkfunktionsentitäten zu suchen und hinzuzufügen, die die Regex-Kriterien für die Gruppen erfüllen. Der angegebene Regex-Ausdruck wird in NetScaler ADM beibehalten. Führen Sie die folgenden Schritte aus, um reguläre Ausdrücke hinzuzufügen:

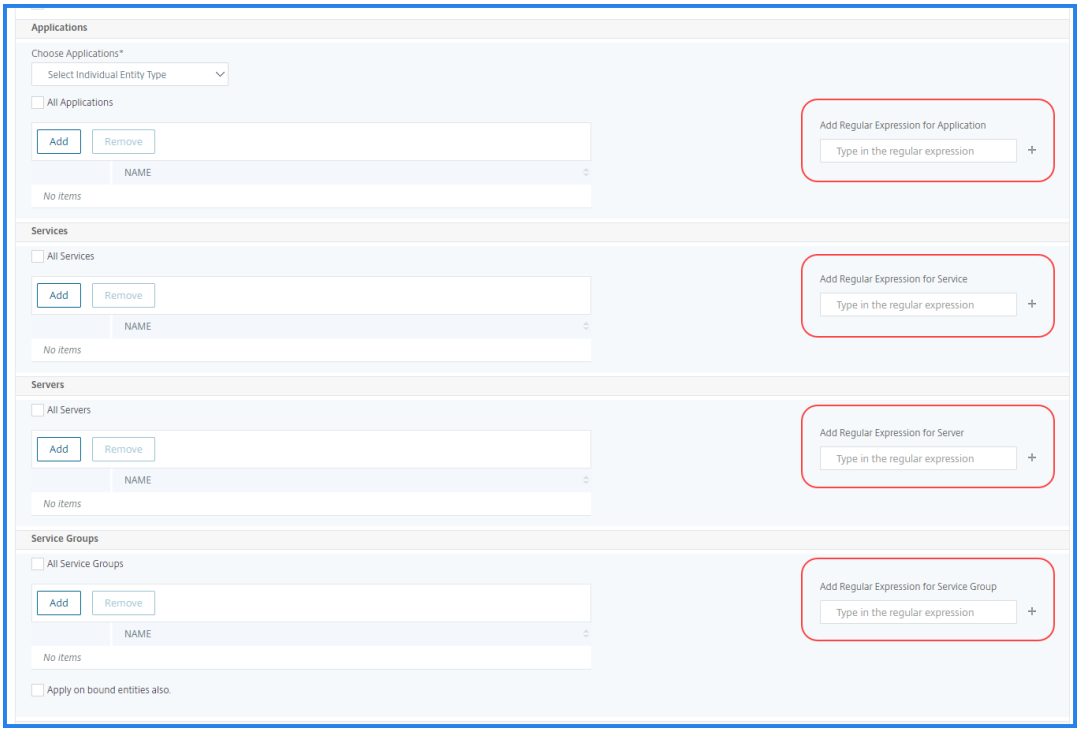
a) Klicken Sie auf **Regulären Ausdruck hinzufügen**.

b) Geben Sie den regulären Ausdruck im Textfeld an.

In der folgenden Abbildung wird erläutert, wie Sie einen regulären Ausdruck verwenden, um eine Anwendung hinzuzufügen, wenn Sie die Option **Spezifische Anwendungen** auswählen:



In der folgenden Abbildung wird erläutert, wie Sie regulären Ausdruck verwenden, um Netzwerkfunktionsobjekte hinzuzufügen, wenn Sie die Option **Individuelle Entitätstyp auswählen** auswählen:



Wenn Sie weitere reguläre Ausdrücke hinzufügen möchten, klicken Sie auf das Symbol **+** .

> **Hinweis:**
>
> Der reguläre Ausdruck stimmt nur mit dem Servernamen für den Entitätstyp **Server** überein und nicht mit der IP-Adresse des Servers.

Wenn Sie die Option **Auch auf gebundene Entitäten anwenden** für eine erkannte Entität auswählen, kann ein Benutzer automatisch auf die Entitäten zugreifen, die an die erkannte Entität gebunden sind.

Der reguläre Ausdruck wird im System gespeichert, um den Autorisierungsbereich zu aktualisieren. Wenn die neuen Entitäten mit dem regulären Ausdruck ihres Entitätstyps übereinstimmen, aktualisiert NetScaler ADM den Autorisierungsbereich auf die neuen Entitäten.

Vorlagen für die Konfiguration:

Wenn Sie die spezifische Konfigurationsvorlage auswählen möchten, die ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

a) Deaktivieren Sie das Kontrollkästchen **Alle Konfigurationsvorlagen** und klicken Sie auf **Konfigurationsvorlage hinzufügen**.

b) Wählen Sie die gewünschte Vorlage aus der Liste aus und klicken Sie auf **OK**.

StyleBooks:

Wenn Sie das spezifische StyleBook auswählen möchten, das ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

a) Deaktivieren Sie das Kontrollkästchen **Alle StyleBooks**, und klicken Sie auf **StyleBook zu Gruppe hinzufügen**. Sie können entweder einzelne StyleBooks auswählen oder eine Filterabfrage angeben, um StyleBooks zu autorisieren.

Wenn Sie die einzelnen StyleBooks auswählen möchten, wählen Sie die StyleBooks im Bereich **Einzelne StyleBooks** aus und klicken Sie auf **Auswahl speichern**.

Wenn Sie eine Abfrage zum Durchsuchen von StyleBooks verwenden möchten, wählen Sie den Bereich **Benutzerdefinierte Filter** aus. Eine Abfrage ist eine Zeichenfolge von Schlüssel-Wert-Paaren, wobei Schlüssel `name`, `namespace` und `version` sind.

Sie können reguläre Ausdrücke auch als Werte verwenden, um StyleBooks zu suchen und hinzuzufügen, die Regex-Kriterien für die Gruppen erfüllen. Eine benutzerdefinierte Filterabfrage zum Durchsuchen von StyleBooks unterstützt sowohl die Operation `And` als auch `Or`.

Beispiel:

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


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

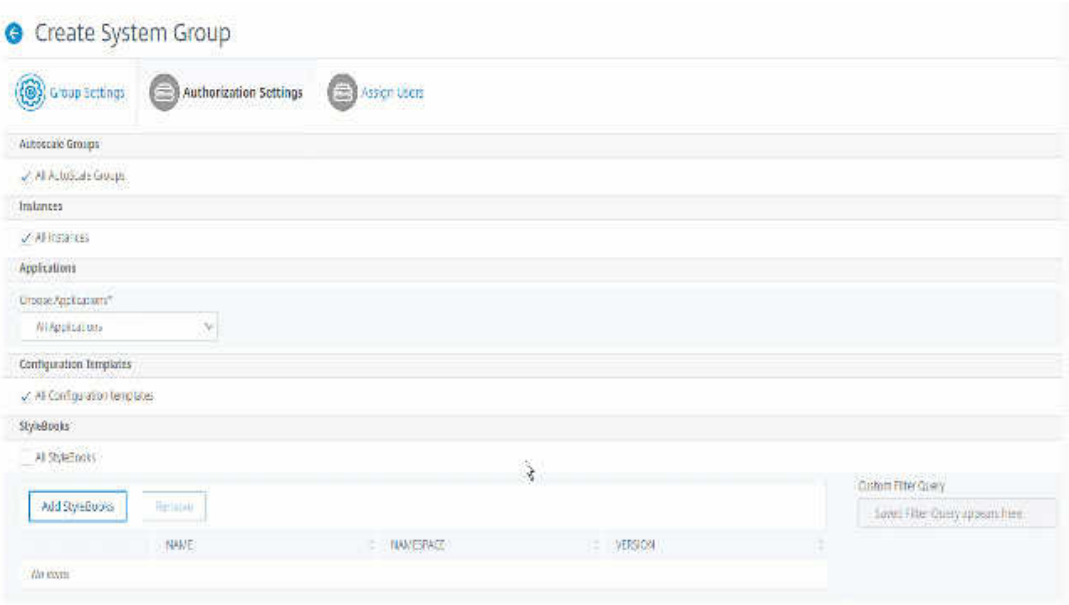
- StyleBook-Name ist entweder `lb-mon` oder `lb`.
- StyleBook Namespace ist `com.citrix.adc.stylebooks`.
- StyleBook-Version ist `1.0`.

Verwenden Sie eine `Or`-Operation zwischen Werteausdrücken, die für den Schlüsselausdruck definiert ist.

Beispiel:

- Die Abfrage `name=lb-mon|lb` ist gültig. Es gibt die StyleBooks zurück, die einen Namen `lb-mon` oder `lb` haben.
- Die Abfrage `name=lb-mon | version=1.0` ist ungültig.

Drücken Sie `Enter`, um die Suchergebnisse anzuzeigen, und klicken Sie auf **Abfrage speichern**.



Die gespeicherte Abfrage wird in der Abfrage "**Benutzerdefinierte Filter**"angezeigt. Basierend auf der gespeicherten Abfrage bietet das ADM dem Benutzer Zugriff auf diese StyleBooks.

b) Wählen Sie die gewünschten StyleBooks aus der Liste aus und klicken Sie auf **OK**.

Sie können die erforderlichen StyleBooks auswählen, wenn Sie Gruppen erstellen und Benutzer zu dieser Gruppe hinzufügen. Wenn Ihr Benutzer das erlaubte StyleBook auswählt, werden auch alle abhängigen StyleBooks ausgewählt.

Konfigurationspakete:

Wählen Sie in **Configpacks** eine der folgenden Optionen aus:

- **Alle Konfigurationen**: Diese Option ist standardmäßig ausgewählt. Es fügt alle Konfigurationspakete hinzu, die in ADM enthalten sind.
- **Alle Konfigurationen der ausgewählten StyleBooks**: Diese Option fügt alle Konfigurationspakete des ausgewählten StyleBook hinzu.
- **Spezifische Konfigurationen**: Mit dieser Option können Sie die erforderlichen Konfigurationspakete hinzufügen.

  Sie können die erforderlichen Konfigurationspakete auswählen, wenn Sie Gruppen erstellen und Benutzer zu dieser Gruppe hinzufügen.

Domänennamen:

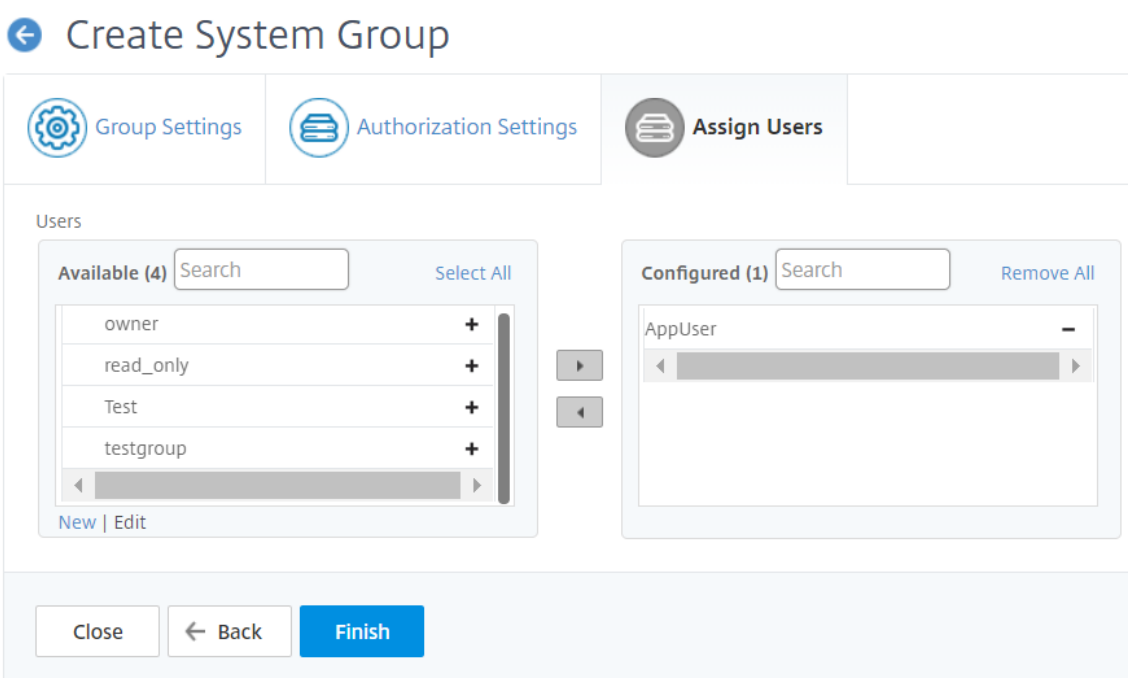
Wenn Sie den spezifischen Domänennamen auswählen möchten, den ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

a) Deaktivieren Sie das Kontrollkästchen **Alle Domainnamen** und klicken Sie auf **Domainnamen hinzufügen**.

b) Wählen Sie die erforderlichen Domänennamen aus der Liste aus und klicken Sie auf **OK**.

7. Klicken Sie auf **Gruppe erstellen**.
8. Wählen **Sie im Abschnitt Benutzer zuweisen** den Benutzer in der Liste **Verfügbar** aus, und fügen Sie den Benutzer zur Liste **Konfiguriert** hinzu.

> **Hinweis:**
>
> Sie können Benutzer auch hinzufügen, indem Sie auf **Neu**klicken.



9. Klicken Sie auf **Fertig stellen**.

Verwaltung des Benutzerzugriffs über mehrere Netzwerkfunktionsentitäten

Als Administrator können Sie den Benutzerzugriff auf der einzelnen Ebene der Netzwerkfunktionsentitäten in Citrix ADM verwalten. Und Sie können dem Benutzer oder einer Gruppe auf Entitätsebene dynamisch bestimmte Berechtigungen zuweisen, indem Sie den Filter für reguläre Ausdrücke verwenden.

In diesem Dokument wird beschrieben, wie die Benutzerautorisierung auf Entitätsebene definiert wird.

Bevor Sie beginnen, erstellen Sie eine Gruppe. Weitere Informationen finden Sie unter Konfigurieren von Gruppen in NetScaler ADM .

Verwendungsszenario:

Stellen Sie sich ein Szenario vor, in dem eine oder mehrere Anwendungen (virtuelle Server) auf demselben Server gehostet werden. Ein Superadministrator (George) möchte Steve (einem Anwendungsadministrator) nur Zugriff auf App1 und nicht auf den Hosting-Server gewähren.

Die folgende Tabelle zeigt diese Umgebung, in der Server-A die Anwendungen App-1 und App-2 hostet.

Host-Server	Anwendung (virtueller Server)	Service	Service-Gruppe
Server A	App 1	App-service-1	App-service-group-1
Server A	App 2	App-service-2	App-service-group-2

> **Hinweis**
>
> Citrix ADM behandelt virtuelle Server, Dienste, Dienstgruppen und Server als Netzwerkfunktionsentitäten. Der virtuelle Server vom Entitätstyp wird als Anwendung bezeichnet.

Um Netzwerkfunktionsentitäten Benutzerberechtigungen zuzuweisen, definiert George die Benutzerautorisierung wie folgt:

1. Navigieren Sie zu **Konto > Benutzerverwaltung > Gruppen** und fügen Sie eine Gruppe hinzu.
2. Wählen Sie auf der Registerkarte **Autorisierungseinstellungen** die Option Anwendungen auswählen aus.
3. Wählen Sie **Select Individual Entity Type**.

4. Wählen Sie den Entitätstyp **Alle Anwendungen** aus und fügen Sie die App-1-Entität aus der verfügbaren Liste hinzu.
5. Klicken Sie auf **Gruppe erstellen**.
6. Wählen Sie unter **Benutzer zuweisen** die Benutzer aus, die die Berechtigung benötigen. Für dieses Szenario wählt George Steves Benutzerprofil aus.
7. Klicken Sie auf **Fertig stellen**.

Mit dieser Autorisierungseinstellung kann Steve nur App-1 und keine anderen Netzwerkfunktionsentitäten verwalten.

> **Hinweis:**
>
> Stellen Sie sicher, dass die Option **Auch auf gebundene Entitäten anwenden** deaktiviert ist. Andernfalls gewährt Citrix ADM Zugriff auf alle Netzwerkfunktionsentitäten, die an App-1 gebunden sind. Dadurch wird auch Zugriff auf den Hosting-Server gewährt.

Ein Superadministrator kann die regulären Ausdrücke (Regex) für jeden Entitätstyp angeben. Der reguläre Ausdruck wird im System gespeichert, um den Umfang der Benutzerautorisierung zu aktualisieren. Wenn neue Entitäten dem regulären Ausdruck ihres Entitätstyps entsprechen, kann Citrix ADM Benutzern dynamisch Zugriff auf die spezifischen Netzwerkfunktionsentitäten gewähren.

Um Benutzerberechtigungen dynamisch zu gewähren, kann der Superadministrator reguläre Ausdrücke auf der Registerkarte **Autorisierungseinstellungen** hinzufügen.

In diesem Szenario fügt George App* als regulären Ausdruck für den Entitätstyp Applications hinzu und die Anwendungen, die den Regex-Kriterien entsprechen, werden in der Liste angezeigt. Mit dieser Autorisierungseinstellung kann Steve auf alle Anwendungen zugreifen, die dem Regex App* entsprechen. Sein Zugriff ist jedoch nur auf die Anwendungen beschränkt, nicht auf den gehosteten Server.

Wie sich der Benutzerzugriff basierend auf dem Berechtigungsumfang ändert

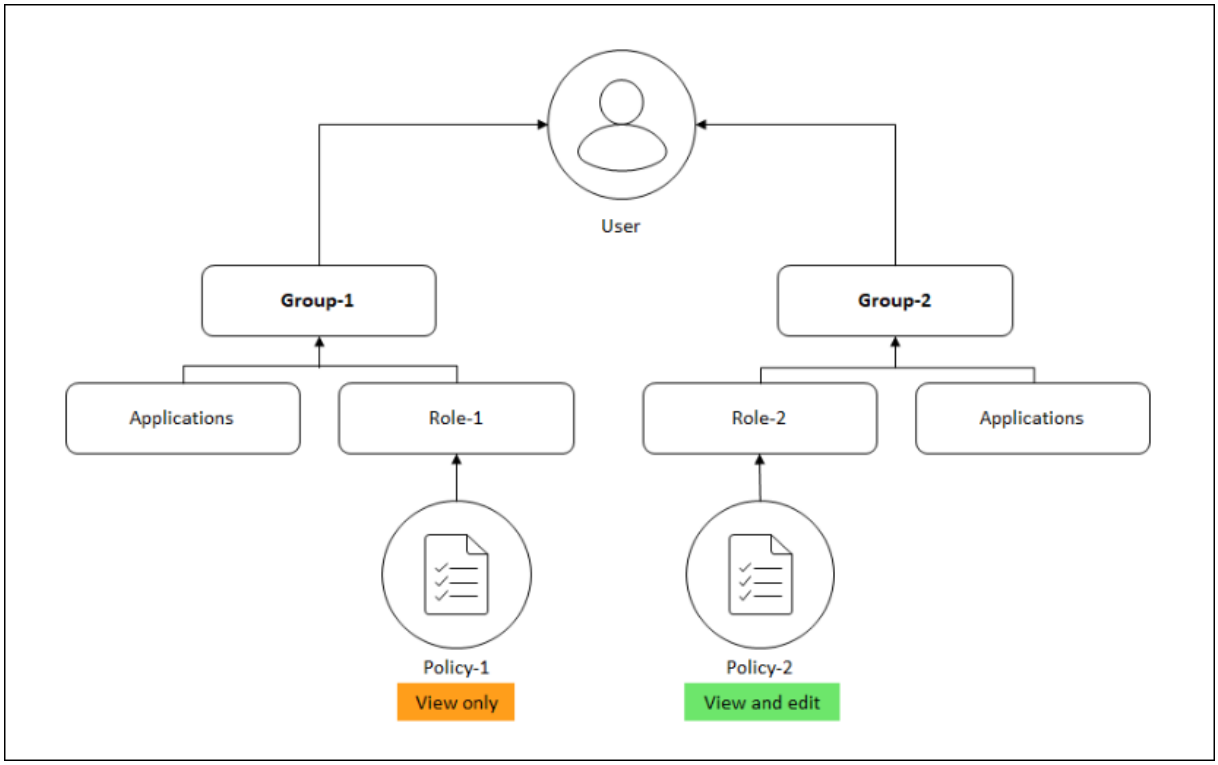
Wenn ein Administrator einen Benutzer zu einer Gruppe hinzufügt, die über unterschiedliche Zugriffsrichtlinieneinstellungen verfügt, wird der Benutzer mehreren Autorisierungsbereichen und Zugriffsrichtlinien zugeordnet.

In diesem Fall gewährt das ADM dem Benutzer je nach dem spezifischen Autorisierungsumfang Zugriff auf Anwendungen.

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

- **Policy-1** —Nur Berechtigungen für Anwendungen anzeigen.

- **Policy-2** —Anzeigen und Bearbeiten der Berechtigung für Anwendungen.



Der Benutzer kann die in Policy-1 angegebenen Anwendungen anzeigen. Außerdem kann dieser Benutzer die in Policy-2 angegebenen Anwendungen anzeigen und bearbeiten. Der Bearbeitungszugriff auf Gruppe-1-Anwendungen ist eingeschränkt, da er nicht unter den Autorisierungsbereich der Gruppe 1 fällt.

Zuordnung von RBAC beim Upgrade von NetScaler ADM von 12.0 auf spätere Releases

Wenn Sie Citrix ADM von 12.0 auf 13.0 aktualisieren, werden Ihnen beim Erstellen von Gruppen keine Optionen zur Bereitstellung von Lese-Schreib- oder Leserechten angezeigt. Diese Berechtigungen wurden durch “Rollen und Zugriffsrichtlinien”ersetzt, wodurch Sie den Benutzern mehr Flexibilität bieten können, rollenbasierte Berechtigungen bereitzustellen. Die folgende Tabelle zeigt, wie die Berechtigungen in Version 12.0 Version 13.0 zugeordnet sind:

12.0	Nur Anwendungen zulassen	13.0
Admin Lese-/Schreibzugriff	False	`admin`
Admin Lese-/Schreibzugriff	True	`appAdmin`
Admin schreibgeschützt	False	`readonly`
Admin schreibgeschützt	True	`appReadonly`

Rollen konfigurieren

February 5, 2024

In Citrix Application Delivery Management (ADM) ist jede Rolle an eine oder mehrere Zugriffsrichtlinien gebunden. Sie können Eins-zu-Eins-, Eins-zu-Viele- und Viele-zu-Viele-Beziehungen zwischen Richtlinien und Rollen definieren. Sie können eine Rolle an mehrere Richtlinien binden, und Sie können mehrere Rollen an eine Richtlinie binden.

Beispielsweise kann eine Rolle an zwei Richtlinien gebunden sein, wobei eine Richtlinie Zugriffsberechtigungen für ein Feature und die andere Richtlinie Zugriffsberechtigungen für ein anderes Feature definiert. Eine Richtlinie erteilt möglicherweise die Erlaubnis, Citrix ADC-Instanzen in Citrix ADM hinzuzufügen, und die andere Richtlinie erteilt möglicherweise die Erlaubnis, StyleBooks zu erstellen und bereitzustellen und Citrix ADC-Instanzen zu konfigurieren.

Wenn mehrere Richtlinien Bearbeitungs- und Leseberechtigungen für ein einzelnes Feature definieren, haben die Bearbeitungsberechtigungen Vorrang.

Citrix ADM bietet vier vordefinierte Rollen:

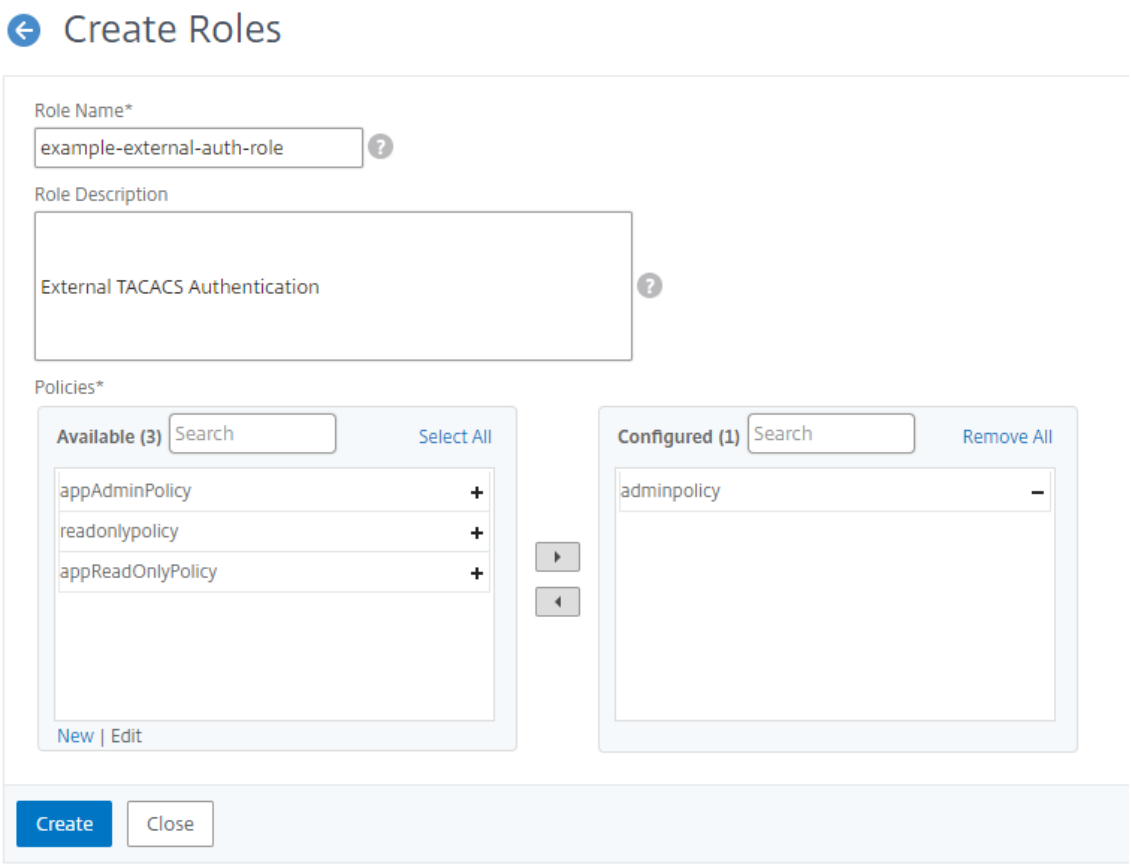
- **Administrator**. Hat Zugriff auf alle NetScaler ADM-Funktionen. (Diese Rolle ist an die Administratorrichtlinie gebunden.)
- **schreibgeschützt**. Schreibgeschützter Zugriff. (Diese Rolle ist an readonlypolicy gebunden.)
- **appAdmin**. Hat administrativen Zugriff nur auf die Anwendungsfunktionen in NetScaler ADM. (Diese Rolle ist an appAdminPolicy gebunden).
- **appReadonly**. Hat nur Lesezugriff auf die Anwendungsfunktionen. (Diese Rolle ist an appReadOnlyPolicy gebunden.)

> **Hinweis** Die vordefinierten Rollen können nicht bearbeitet werden.

Sie können auch Ihre eigenen (benutzerdefinierten) Rollen erstellen.

So erstellen Sie Rollen und weisen ihnen Richtlinien zu:

1. Navigieren Sie in Citrix ADM zu **System** > **Benutzerverwaltung** > **Rollen**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Rollenname** den Namen der Rolle ein und geben Sie die Beschreibung in das Feld **Rollenbeschreibung** ein (optional).
4. Fügen Sie im Abschnitt **Richtlinien** eine oder mehrere Richtlinien zur Liste „Konfiguriert“hinzu oder verschieben Sie sie in die Liste **Konfiguriert**.



5. Klicken Sie auf **Erstellen**.

Benutzer konfigurieren

February 5, 2024

Standardmäßig hat Citrix Application Delivery Management (ADM) einen Benutzer:

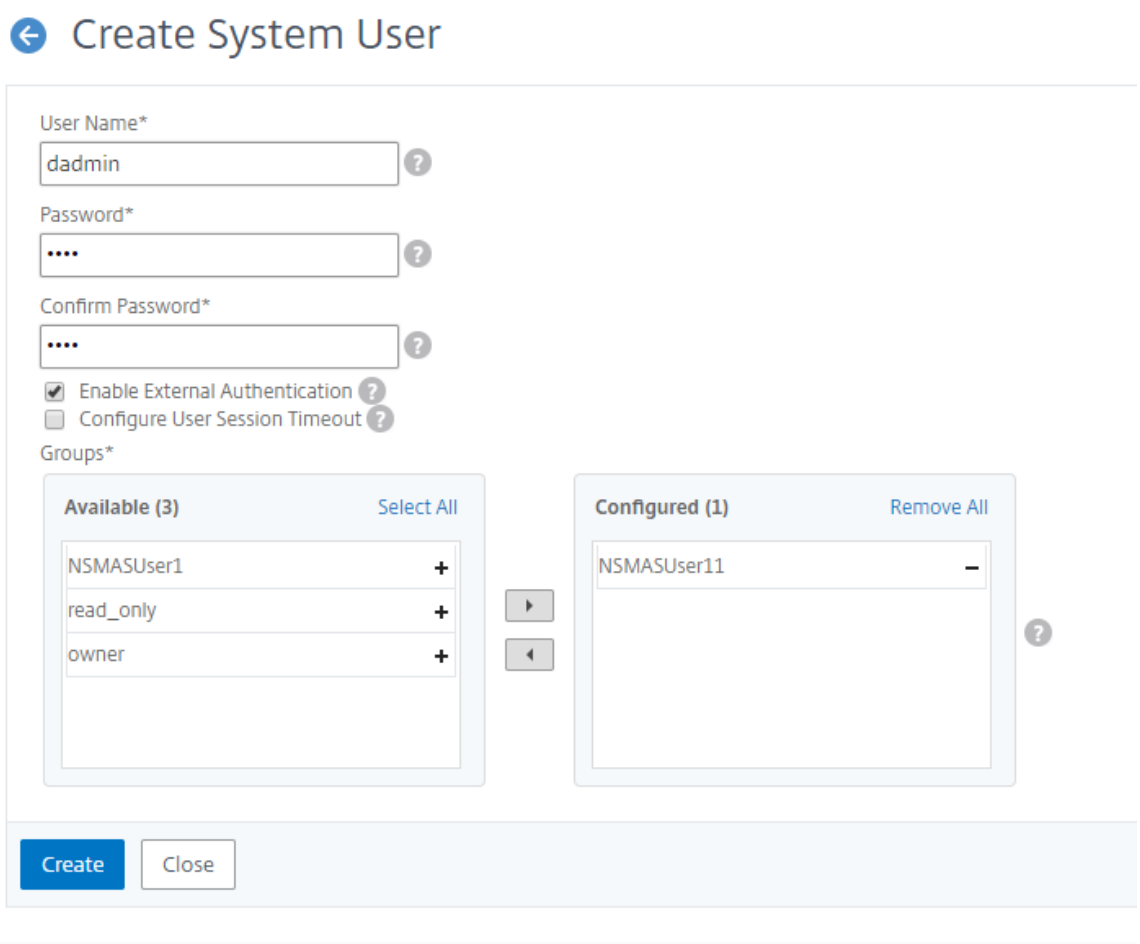
nsroot —Der Root-Benutzer (nsroot) hat volle Administratorrechte auf der Appliance. Der nsroot-Benutzer ist der Superadmin von Citrix ADM.

Sie können zusätzliche Benutzer erstellen, indem Sie Konten für sie konfigurieren. Wenn Sie neue Benutzer zu Citrix ADM hinzufügen, können Sie deren Berechtigungen definieren, indem Sie die entsprechenden Gruppen, Rollen und Richtlinien zuweisen.

Sie können einen Benutzer einer Gruppe zuweisen und die Gruppe an Rollen binden. Sie können die Beziehung eins zu eins, eins zu viele oder viele zu viele zwischen Benutzern, Gruppen, Rollen und Zugriffsrichtlinien definieren. Ein Benutzer kann mehreren Gruppen zugewiesen werden. Eine Gruppe kann mehrere Rollen haben, und mehrere Gruppen können identische Rollen haben.

So konfigurieren Sie Benutzer in NetScaler ADM:

1. Navigieren Sie in NetScaler ADM zu **System** > **Benutzerverwaltung** > **Benutzer**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie folgende Details ein:
   a) **Nutzername**. Name des Benutzers
   b) **Kennwort**. Kennwort, mit dem sich der Benutzer bei Citrix ADM anmeldet
4. Wählen Sie optional **Externe Authentifizierung aktivieren**aus, damit der Benutzer über einen externen Authentifizierungsserver authentifiziert werden kann.
5. Wenn Sie Gruppen erstellt haben und den Benutzer einer Gruppe zuweisen möchten, verschieben Sie im Abschnitt **Gruppen** eine oder mehrere Gruppen aus der Liste **Verfügbar** in die Liste **Konfiguriert** .



6. Klicken Sie auf **Erstellen**.

Anwendungen

February 5, 2024

Mit der Anwendungsanalyse- und Verwaltungsfunktion von NetScaler ADM können Sie die Anwendungen mithilfe eines anwendungszentrierten Ansatzes überwachen. Dieser Ansatz hilft Ihnen dabei:

- Überprüfen Sie den Score und analysieren Sie die Gesamtleistung der Anwendungen
- Überprüfen Sie auf Probleme, die mit dem Server oder Client bestehen
- Erkennen Sie Anomalien in den Datenverkehrsströmen der Anwendung und ergreifen Sie Korrekturmaßnahmen

> **Hinweis**
>
> Anwendungen beziehen sich auf einen oder mehrere virtuelle Server, die auf den Instanzen konfiguriert sind (NetScaler ADC).

Sie können die Anwendungen für die Dauer wie 1 Stunde, 1 Tag, 1 Woche und 1 Monat überwachen.

Voraussetzungen

- Stellen Sie sicher, dass Sie NetScaler ADC-Instanzen in NetScaler ADM hinzugefügt haben
- Stellen Sie sicher, dass Sie über eine gültige Lizenz für Ihre NetScaler ADC-Instanzen verfügen. Weitere Informationen finden Sie unter Lizenzierung
- Stellen Sie sicher, dass Sie die Lizenz für virtuelle Server angewendet haben. Weitere Informationen finden Sie unter Verwalten der Lizenzierung auf virtuellen Servern

Anwendungsüberblick

Anwendungen können sein:

- Diskrete Anwendungen
- Benutzerdefinierte Anwendungen
- Microservices-Anwendungen (k8s_discrete)

Diskrete Anwendungen

Alle virtuellen Server, die lizenziert sind, werden als diskrete Anwendungen bezeichnet.

Benutzerdefinierte Anwendungen

Die virtuellen Server einer Kategorie werden als benutzerdefinierte Anwendungen bezeichnet. Als Administrator müssen Sie benutzerdefinierte Anwendungen basierend auf einer Kategorie hinzufügen. Anschließend können Sie die Anwendungen über das Dashboard verwalten und überwachen. Sie können ganz einfach bestimmte Anwendungen überwachen, die in einer Kategorie zusammengefasst sind.

Sie können beispielsweise eine Kategorie für Ihr Datencenter1 erstellen und dessen ADC-Instanzen hinzufügen. Nachdem Sie eine Kategorie definiert und die Instanz für Ihr Datencenter1 hinzugefügt haben, wird das Anwendungs-Dashboard mit einer separaten Kategorie angezeigt, die alle Anwendungen umfasst, die sich auf Ihr Datencenter1 beziehen.

Wichtige Hinweise

- Die diskreten Anwendungen, die den benutzerdefinierten Anwendungen hinzugefügt werden, werden aus den diskreten Anwendungen entfernt.
- Alle Anwendungen, die keiner Kategorie hinzugefügt werden, stehen als **Andere** zur Verfügung.
- Standardmäßig können Sie mit NetScaler ADM Lizenzen für bis zu 2 Anwendungen hinzufügen. Abhängig von Ihrer Lizenz können Sie Lizenzen für die Anwendungen auswählen und anwenden, die Sie überwachen möchten.

Microservices-Anwendungen

In einem Kubernetes-Cluster stellt Citrix einen Ingress Controller für NetScaler ADC MPX (Hardware), NetScaler ADC VPX (virtualisiert) und NetScaler ADC CPX (containerisiert) bereit. Weitere Informationen finden Sie unter Citrix Ingress Controller.

Die diskreten Anwendungen, die mit den NetScaler ADC CPX-Instanzen konfiguriert werden, werden als Microservices-Anwendungen bezeichnet.

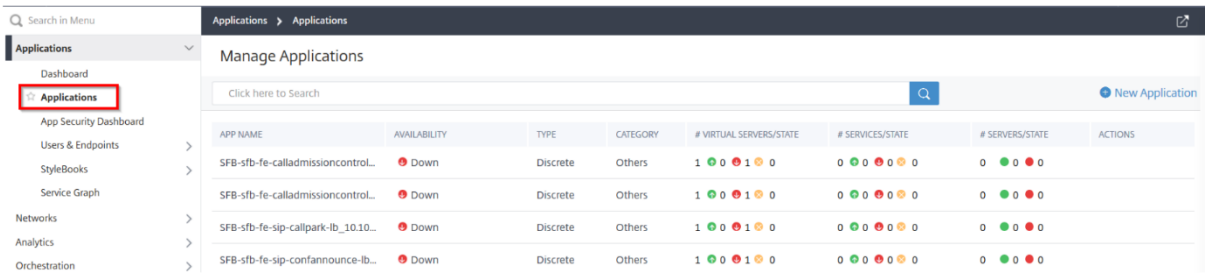
Anwendungsmanagement und Anwendungsdashboard

February 5, 2024

Mit Citrix ADM können Sie Anwendungen auf der Seite **Anwendungen** verwalten und Anwendungsdetails auf der Seite **Dashboard** anzeigen.

Anwendungen verwalten

Auf der Seite **Anwendungen** können Sie alle benutzerdefinierten und diskreten Anwendungen anzeigen.



Auf der Seite **Anwendungen** können Sie als Administrator folgende Aufgaben ausführen:

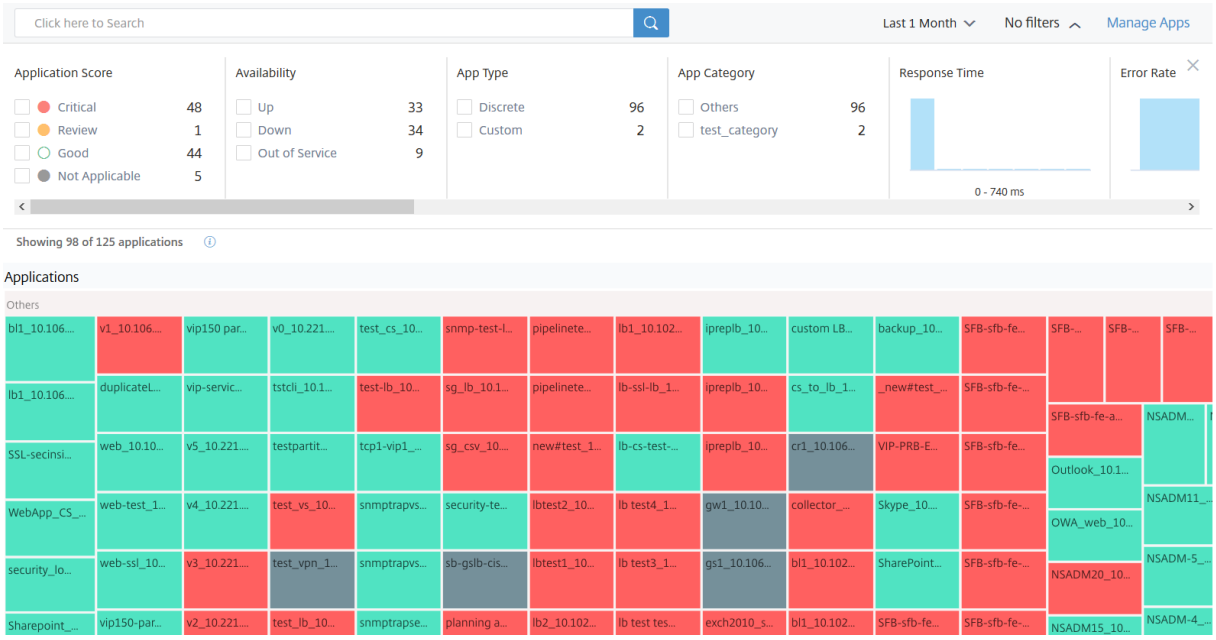
- Anwendungen hinzufügen
- Zeigen Sie Anwendungsdetails wie App-Name, App-Typ, App-Kategorie, zugehörige virtuelle Server, zugehörige Dienste usw. an.
- Bearbeiten oder Löschen von benutzerdefinierten Anwendungen

Nachdem Sie Anwendungen hinzugefügt, bearbeitet oder gelöscht haben, werden die Details sofort auf der Seite “Anwendungen”angezeigt.

Weitere Informationen finden Sie unter Anwendungen verwalten.

Anwendungsdashboard

Navigieren Sie zu **Anwendungen** > **Dashboard**, um die Liste der Anwendungen entweder in der tabellarischen Ansicht oder in der Diagrammansicht anzuzeigen.



Alle Anwendungen werden erst im Dashboard angezeigt, nachdem die Anwendungen mit dem Auffüllen von Daten beginnen. Klicken Sie im Dashboard auf eine Anwendung, um detaillierte Informationen zur Anwendungsleistung anzuzeigen. Weitere Informationen finden Sie unter Anwendungsdetails.

Wenn die Anwendungsanalyse auch nach einer Dauer von etwa 10—15 Minuten nicht angezeigt wird, führen Sie die Schritte zur Fehlerbehebung im App-Dashboard zur Fehlerbehebungdurch.

Aktualisierungen im neuen Dashboard-Verhalten im Vergleich zum früheren Dashboard

- Nachdem Sie eine benutzerdefinierte Anwendung hinzugefügt oder bearbeitet haben, kann es einige Minuten dauern, bis die Anwendung im Dashboard angezeigt wird.
- Wenn Sie eine benutzerdefinierte Anwendung löschen, zeigt das Dashboard die gelöschte Anwendung weiterhin an, bis ADM über die Analysedaten verfügt (maximale Dauer 1 Monat).

  Stellen Sie sich ein Szenario vor, in dem Sie am 2. Januar 2020 eine Anwendung erstellt und die Anwendung am 4. Januar 2020 gelöscht haben. Für dieses Szenario gilt:

  - Das Dashboard kann die gelöschte Anwendung weiterhin am 4. Januar 2020 anzeigen, wenn Sie die Zeitdauer für den letzten 1 Tag, 1 Woche und 1 Monat auswählen.
  - Das Dashboard kann die gelöschte Anwendung am 5. Januar 2020 weiterhin anzeigen, wenn Sie die Zeitdauer für die letzte Woche und den letzten Monat auswählen.
  - Wenn die Dauer das Löschdatum der App überschreitet, wird die Anwendung nicht im Dashboard angezeigt. Das heißt, das Dashboard wird am 6. Januar 2020 (für den letzten

Tag), 12. Januar 2020 (für die letzte Woche) und nach dem 5. Februar 2020 (für den letzten Monat) nicht mit der gelöschten Anwendung angezeigt.

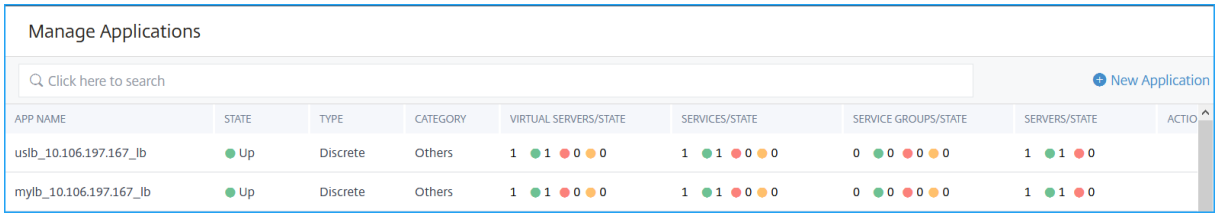
> **Hinweis**
>
> Wenn die zugeordnete NetScaler ADC-Instanz nach dem Hinzufügen einer Anwendung "Heruntergefahren", "außer Betrieb"ist oder aufgrund eines temporären Netzwerkfehlers nicht erreichbar ist:
>
> -Die der ADC-Instanz zugeordneten Anwendungen sind nur auf der Seite **Anwendungen**, jedoch nicht im Dashboard sichtbar.
>
> -Die Anwendungen werden im Dashboard angezeigt, nachdem die ADC-Instanz ausgeführt wurde.

Anwendungen verwalten

February 5, 2024

Klicken Sie im Dashboard auf **Apps verwalten**, um Anwendungsdetails anzuzeigen und benutzerdefinierte Anwendungen hinzuzufügen, zu bearbeiten oder zu löschen.

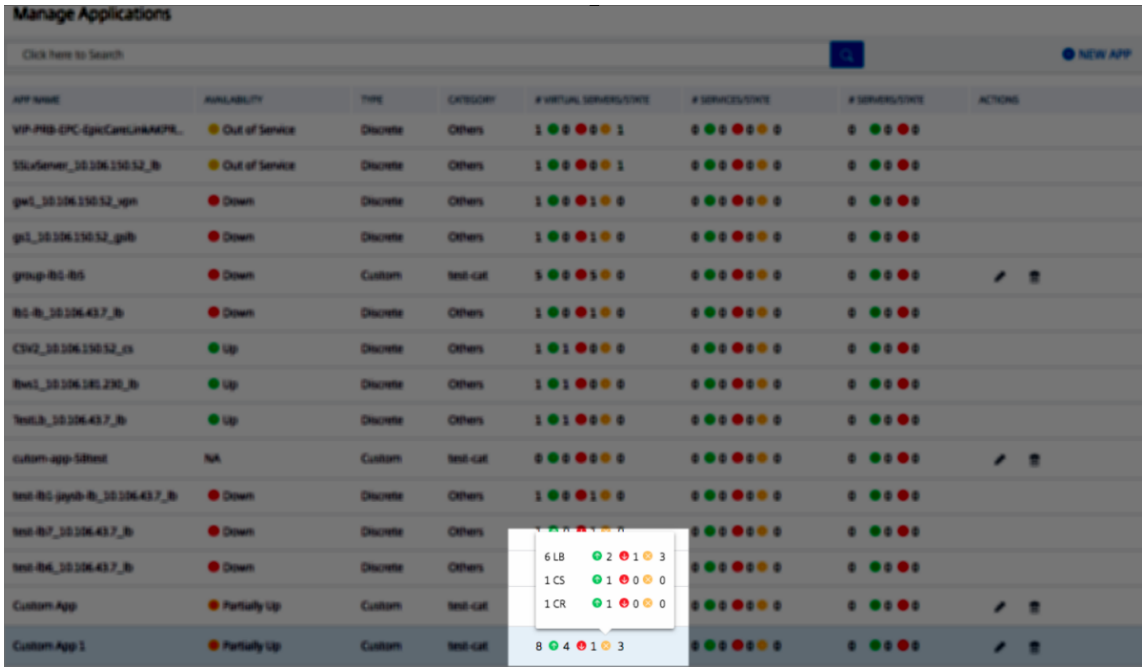
Anwendungsdetails anzeigen



- **App-Name** —Bezeichnet den Anwendungsnamen
- **Verfügbarkeit—Gibt die aktuelle Verfügbarkeit der Anwendung an, z. B. **Up**, **Down**, **Partially Up**, **Out of Service**und NA****
  - **Up** —Alle virtuellen Server, die der Anwendung zugeordnet sind, sind betriebsbereit.
  - **Ausgefallen** —Alle virtuellen Server, die der Anwendung zugeordnet sind, sind ausgefallen
  - **Teilweise** aktiv —Entweder ist eine der Anwendung zugeordnete virtuelle Maschine ausgefallen oder außer Betrieb

  - **Nicht in Betrieb** —Alle virtuellen Server, die mit den Anwendungen verknüpft sind, sind außer Betrieb
  - **NA** —Es sind keine virtuellen Server für die Anwendung konfiguriert

- **Typ** —Gibt an, ob die Anwendung zu Benutzerdefiniert oder diskret gehört
- **Kategorie** —Gibt die Anwendungskategorie an, die gruppiert ist
- **Virtueller Server/Status** —Gibt die Gesamtzahl der konfigurierten virtuellen Server und den aktuellen Status aller virtuellen Server an. Bewegen Sie den Mauszeiger, um Details wie die Gesamtzahl der virtuellen Server, den Typ des virtuellen Servers und den Status des virtuellen Servers anzuzeigen

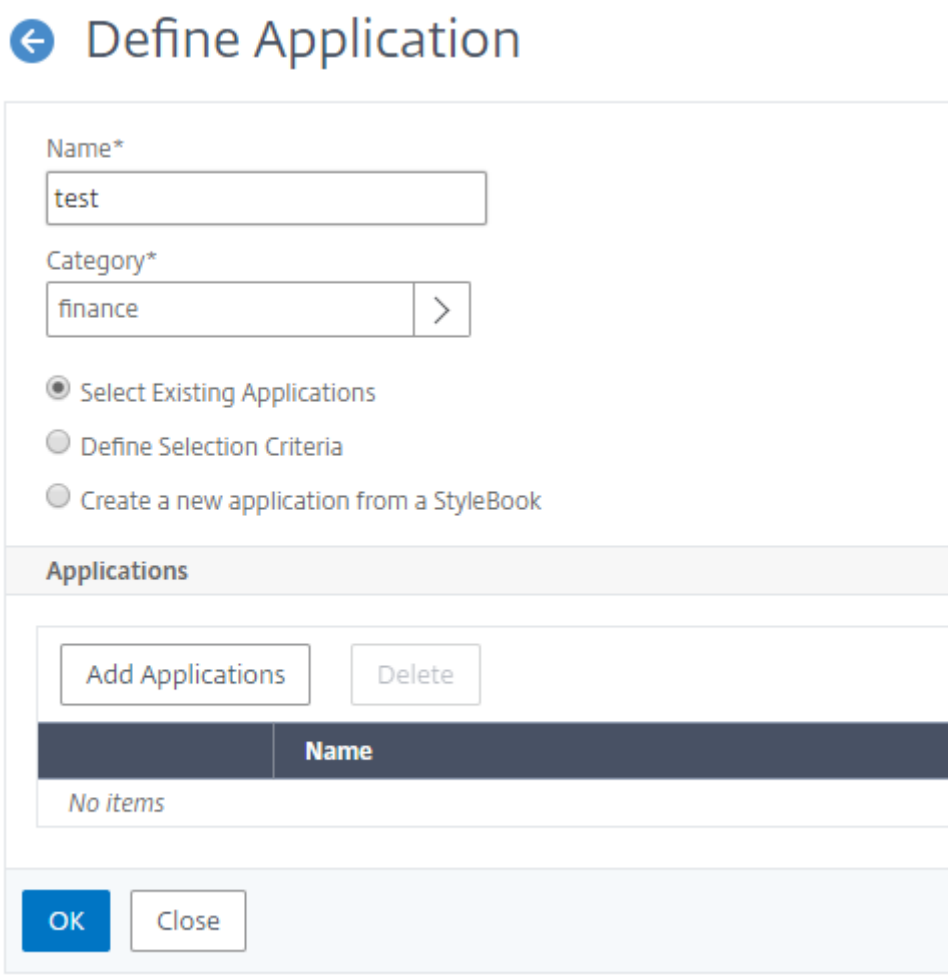


- **Dienstleistungen/Status** —Bezeichnet die Gesamtanzahl der konfigurierten Dienste und den aktuellen Status aller Dienste
- **Service Goups/State** —Bezeichnet die gesamten konfigurierten Servicegruppen und den Status aller Servicegruppen
- **Server/Status** —Bezeichnet die Gesamtanzahl der für die Anwendung konfigurierten Server und den aktuellen Status aller Server
- **Aktionen** —Ermöglicht das Bearbeiten oder Löschen der benutzerdefinierten Anwendungen

Eine Anwendung hinzufügen

1. Klicken Sie auf **Neue Anwendung**, um eine neue Anwendung zu erstellen

Die Seite **Anwendung definieren** wird angezeigt.



> **Hinweis:**
>
> Sie können auch auf **Anwendungen** klicken und dann **Neue Anwendung** auswählen, um eine neue Anwendung hinzuzufügen.

2. Legen Sie die folgenden Parameter fest:

Feld	Beschreibung
Name	Name der benutzerdefinierten Anwendung. Zum Beispiel LB_TEST.

Feld	Beschreibung
Kategorie	Die Kategorie, in der Sie die Anwendungen gruppieren können. Klicken Sie hier, um die Seite Anwendungskategorie aufzurufen. Wählen Sie die Kategorie und klicken Sie auf **Auswählen** So fügen Sie eine Kategorie hinzu a) Klicken Sie auf **Hinzufügen**. a) Geben Sie einen Namen Ihrer Wahl ein. a) Klicken Sie auf **Erstellen**.
Vorhandene Anwendungen auswählen	Ermöglicht die Auswahl der vorhandenen Anwendungen, die den NetScaler ADC-Instanzen hinzugefügt wurden.
Anwendung hinzufügen	Zeigt alle virtuellen Server an, die auf den Instanzen konfiguriert sind. Wählen Sie die Anwendungen aus der Liste aus und klicken Sie auf **OK**.
Auswahlkriterien definieren	Option zum Definieren der Anwendung nach virtuellem Serverbereich oder nach IP-Adressbereich des Ursprungsservers/-dienstes. • **Server.** Geben Sie die IP-Adresse des Servers oder Dienstes, den Servernamen oder den Port des Backend-Servers an, auf dem die Anwendungen ausgeführt werden. Sie können eine IP-Adresse, einen Bereich von IP-Adressen oder eine Kombination von beiden durch Kommas getrennt eingeben. Sie können beispielsweise 10.102.29.20, 10.102.43.10-60, 10.216.43.45 eingeben.

Feld	Beschreibung
	• **Virtuelle Server.** Sie können eine der folgenden Optionen angeben: die IP-Adresse des virtuellen Servers, den Namen des virtuellen Servers oder den Port des Backend-Servers, auf dem die Anwendungen ausgeführt werden. Sie können eine IP-Adresse oder einen Bereich von IP-Adressen oder eine Kombination von beiden durch Kommas getrennt eingeben. Sie können beispielsweise 10.102.29.20, 10.102.43.10-60, 10.216.43.45 eingeben.
Erstellen Sie eine neue Anwendung aus einem StyleBook	Ermöglicht das Erstellen einer Anwendung mit dem StyleBook. Weitere Informationen finden Sie unter Erstellen einer Anwendung mit dem StyleBook.

3. Klicken Sie auf **OK**.

   > **Hinweis:**
   >
   > Derzeit unterstützt Application Dashboard nur virtuelle Server für Lastausgleich und Content Switching.

   Das Anwendungs-Dashboard wird jetzt mit der Kategorie angezeigt und alle Anwendungen sind darunter gruppiert.

   Wenn Sie **eine neue Anwendung aus einer StyleBook-Option erstellen** für die benutzerdefinierte Anwendung auswählen, müssen Sie Citrix ADM erlauben, die virtuellen Server für die Lizenzierung automatisch auszuwählen. So aktivieren Sie die automatische Auswahl für die virtuellen Server:

   a) Navigieren Sie zu **System** > **Lizenzierung und Analytics**.

   b) Klicken Sie unter **Virtual Server License Summary**auf **Virtuelle Serverautomatisch auswählen und nicht adressierbare virtuelle Server**automatisch auswählen, die aktiviert werden sollen.

Erstellen Sie eine Anwendung mit dem StyleBook

So erstellen Sie eine Anwendung mit dem StyleBook:

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Dashboard**, und klicken Sie auf **Benutzerdefinierte App definieren**, um eine benutzerdefinierte Anwendung zu erstellen.
2. Geben Sie auf der Seite „ **Anwendung definieren** “den Namen der Anwendung in das Feld **Name** ein.
3. Wählen Sie im Abschnitt Kategorie die Anwendungskategorie aus. Mit NetScaler ADM können Sie Kategorien definieren, um die benutzerdefinierten Anwendungen zu gruppieren. Sie können bei Bedarf auch weitere Kategorien hinzufügen.
4. Wählen Sie **Create a new application from a StyleBook** aus und klicken Sie auf **OK**.

   Die Seite “StyleBook auswählen”wird angezeigt. Diese Seite enthält alle Standard-StyleBooks, die in NetScaler ADM verfügbar sind.
5. Wählen Sie das StyleBook aus.
   Die Seite **“Konfigurationsdetails** “wird angezeigt.
6. Geben Sie die Werte für alle Parameter im StyleBook ein. Sie können auch auf View Definition klicken, um das Konstrukt des StyleBook anzuzeigen, bevor Sie es verwenden.

   Weitere Informationen finden Sie unter Standard-StyleBooks verwenden.
7. Klicken Sie auf **Erstellen**.

   Sie können auch auf **Dry Run** klicken, um die Konfigurationen zu überprüfen, die NetScaler ADM auf der ausgewählten NetScaler ADC-Instanz zu erstellen versucht. Diese Option dient nur zu Testzwecken, um die endgültige Überprüfung der Konfigurationen zu sehen. Selbst wenn die Option Dry Run erfolgreich ist, kann die tatsächliche Konfiguration auf dem ausgewählten NetScaler ADC aus verschiedenen Gründen fehlschlagen (IP-Konflikt, Instanz nicht erreichbar usw.).

Bearbeiten oder Löschen einer Anwendung

Auf der Seite **Anwendungen** können Sie die benutzerdefinierten Anwendungen entweder bearbeiten oder löschen. Klicken Sie auf die Schaltfläche Bearbeiten, um eine Anwendung zu bearbeiten, und auf die Schaltfläche Löschen, um die Anwendung zu entfernen.

Exportieren von Berichten über App-Dashboard und Sicherheits-Dashboard

Mit NetScaler ADM können Sie einen Snapshot des aktuellen App Dashboards erstellen und als Berichte exportieren. In regelmäßigen Zeitabständen müssen die App-Administratoren diese Berichte möglicherweise verwenden, um über App-Nutzung und Leistungseinbußen auf dem Laufenden zu bleiben.

Mit dieser Funktion können die Administratoren diese Daten als .png-, .jpeg- oder .pdf-Berichte extrahieren.

> **Hinweis:**
>
> Im Gegensatz zu anderen Berichtsexportoptionen in NetScaler ADM können Sie die App Dashboard- und Security Dashboard-Berichte nur als PDF- oder PNG-Dateien exportieren. Das .csv-Format wird derzeit nicht unterstützt.

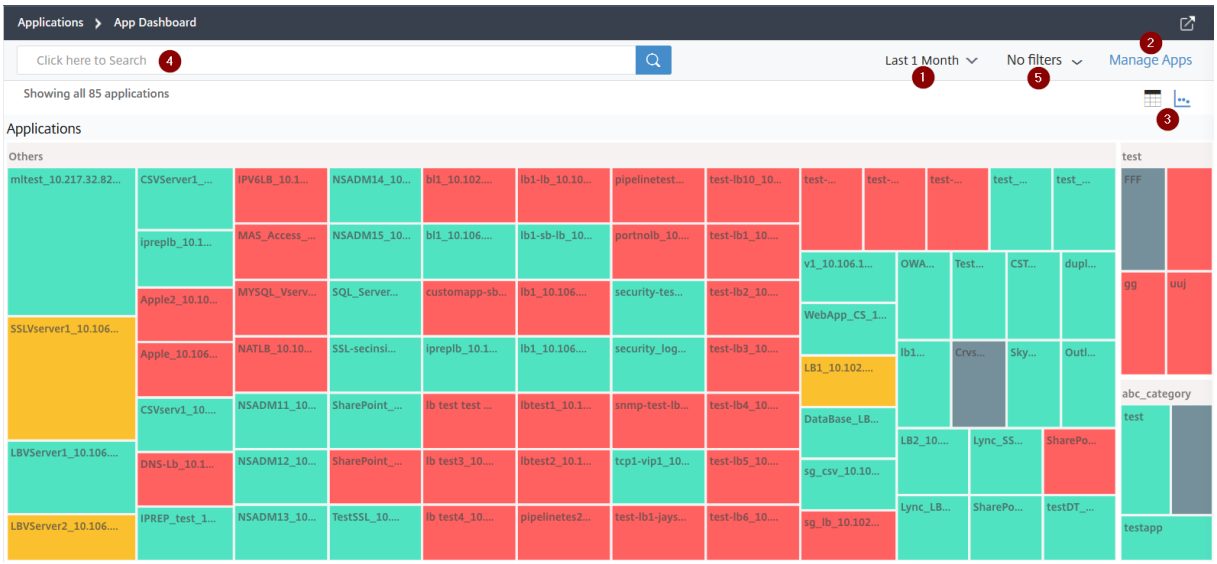
Der Bericht wird auf Ihr System heruntergeladen. Auf den Seiten App Dashboard und App Security Dashboard können Sie auch zu Seiten der zweiten Ebene navigieren und sie als Berichte exportieren. Derzeit können Sie Berichte von jeweils nur einer Anwendung herunterladen.

Übersicht über das Anwendungsdashboard

February 5, 2024

Das Anwendungsdashboard zeigt die einzelnen Anwendungen unter **Andere** und die benutzerdefinierten Anwendungen an, die unter ihren jeweiligen Kategorien gruppiert sind.

Navigieren Sie zu **Anwendung** > **Dashboard**, um das App-Dashboard anzuzeigen.



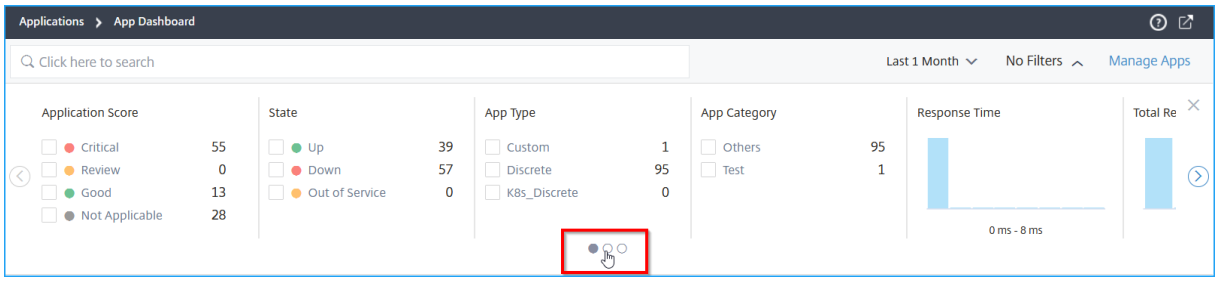
1 —Zeigt die Anwendungsdetails für den ausgewählten Zeitraum an, z. B. 1 Stunde, 1 Tag, 1 Woche und 1 Monat.

2 —Ermöglicht das Verwalten von Anwendungen und das Hinzufügen neuer Anwendungen

3 —Ermöglicht das Anzeigen von Anwendungen entweder in der Tabellen- oder in der Diagrammansicht

4 —Ermöglicht das Durchsuchen einer Anwendung über die Suchleiste

5 —Ermöglicht das Anwenden von Filtern zum Anzeigen von Anwendungen. Klicken Sie hier, um Details anzuzeigen.

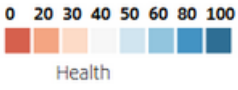


Sie können den Karussell-Schieberegler auswählen, der Ihnen den Zugriff auf alle Optionen erleichtert.

Sie haben folgende Möglichkeiten:

- Wählen Sie diese Option, um Anwendungen basierend auf den Ergebnissen anzuzeigen.
  - **Kritisch** —Anwendungspunktestand liegt zwischen 0 und < 40
  - **Fair**—Die Bewerbungspunktzahl liegt zwischen 40 und < 75
  - **Gut** —Anwendungspunktestand ist größer als 75
  - **Nicht zutreffend** —Es sind keine virtuellen Server für die Anwendung konfiguriert

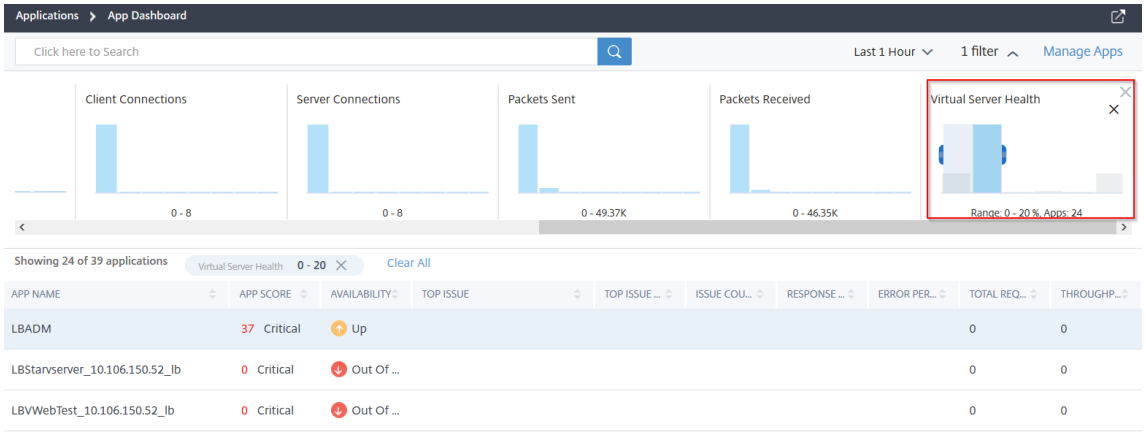
    In der folgenden Tabelle werden die Unterschiede zwischen dem früheren App-Score und dem aktuellen App-Score beschrieben.

Bewertungsergebnis (Kritisch, Überprüfung, Gut, Nicht zutreffend)	App-Score (frühere Ansicht mit Farblegenden)
Die Punktzahl wird berechnet als **100 minus Strafpunktzahl aller aktuellen Probleme der Anwendung** Anwendungen werden in den Farben **Rot (kritisch)**, **Orange (Überprüfung)**, **Grün (gut)**und **Grau (nicht anwendbar)**angezeigt.	Die Punktzahl wird als **100 berechnet — (App-Serverressource + NetScaler ADC-Systemressource)** Anwendungen werden in Farblegenden angezeigt. 

- Wählen Sie diese Option aus, um Anwendungen basierend auf dem Anwendungsstatus anzuzeigen, z. B. Up-, Down- und Out-of Service
- Wählen Sie diese Option, um Anwendungen basierend auf dem Anwendungstyp wie Diskret oder Benutzerdefiniert anzuzeigen

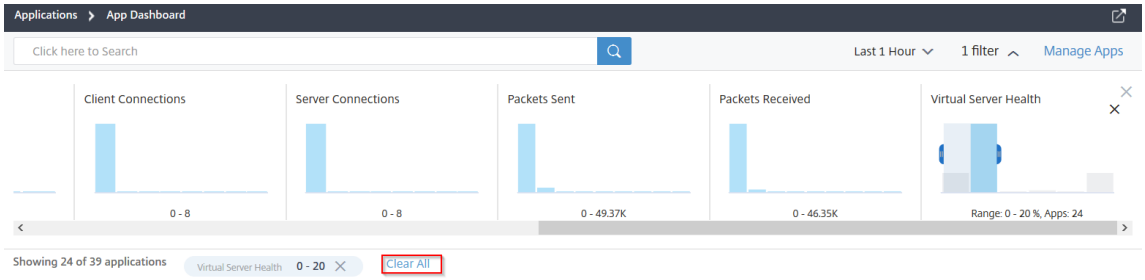
- Wählen Sie diese Option, um Anwendungen basierend auf den darunter gruppierten Kategorien anzuzeigen
- Ziehen Sie das Histogramm, um Filter anzuwenden und Anwendungen anzuzeigen.

  Wenn Sie beispielsweise Anwendungen anzeigen möchten, bei denen der Zustand des virtuellen Servers zwischen 0 und 20 liegt, ziehen Sie das Histogramm des virtuellen Serverzustands, um die Ergebnisse zu filtern.



> **Hinweis**
>
> Sie können auch auf das Histogramm klicken, um die entsprechenden Anwendungen anzuzeigen.

Klicken Sie auf **Alle löschen**, um den verwendeten Filter zu löschen.



Im Folgenden finden Sie die Anwendungsübersicht, für die Sie Filter anwenden können:

- **Reaktionszeit** —Ein Histogramm, das die durchschnittliche Antwortzeit anzeigt, die von den Anwendungen empfangen wurde
- **Fehlerrate** —Ein Histogramm, das den durchschnittlichen Fehlerprozentsatz von 5xx-Fehlern für die Anwendungen anzeigt
- **Anfragen insgesamt** —Ein Histogramm, das die Gesamtzahl der von den Anwendungen eingegangenen Anfragen anzeigt
- **Durchsatz** —Ein Histogramm, das den gesamten Netzwerkdurchsatz anzeigt, der von den Anwendungen verarbeitet wurde

- **Datenvolumen** —Ein Histogramm, das die von den Anwendungen verarbeiteten Gesamtdaten anzeigt. Das Datenvolumen wird anhand der gesamten Anforderungsbytes und Antwortbytes für die Anwendungen berechnet.
- **Client-Verbindungen** —Ein Histogramm, das die durchschnittlichen Client-Verbindungen anzeigt, die von den Anwendungen hergestellt wurden
- **Serververbindungen** —Ein Histogramm, das die durchschnittlichen Serververbindungen anzeigt, die von den Anwendungen hergestellt wurden
- **Gesendete Pakete** —Ein Histogramm, das die Gesamtzahl der von den Anwendungen gesendeten Pakete anzeigt
- **Empfangene Pakete** —Ein Histogramm, das die Gesamtzahl der von den Anwendungen empfangenen Pakete anzeigt
- **Virtueller Serverzustand** —Ein Histogramm, das die gesamten Anwendungen zwischen dem Bewertungsbereich 0% und 100% anzeigt. Der Zustand eines virtuellen Servers ist (%) der aktiven Dienste, die mit der Anwendung verknüpft sind. Wenn beispielsweise ein virtueller Server mit 2 Diensten konfiguriert ist und einer davon ausgefallen ist, beträgt die Punktzahl 50%.

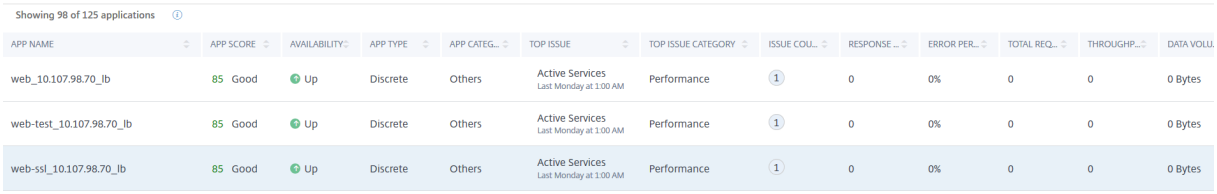
Suchen und filtern Sie Ergebnisse mit der Suchleiste

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

Anwendungen anzeigen

February 5, 2024

Standardmäßig zeigt das Anwendungs-Dashboard alle Anwendungen an. Je nach Anforderung können Sie die Filteroption verwenden, um Anwendungen anzuzeigen.



Das Dashboard zeigt die folgenden Anwendungsdetails an:

- **App-Name** —Bezeichnet den Anwendungsnamen

- **App Score** —Gibt den Anwendungswert und den Status wie **Kritisch**, **Gut**, **Fair**und **Nicht**zutreffend an
- **Verfügbarkeit—Gibt die aktuelle Verfügbarkeit der Anwendung an, z. B. **Up**, **Down**, **Partially Up**, **Out of Service**und NA**
  - **Up** —Alle virtuellen Server, die der Anwendung zugeordnet sind, sind betriebsbereit.
  - **Ausgefallen** —Alle virtuellen Server, die der Anwendung zugeordnet sind, sind ausgefallen.
  - **Teilweise** aktiv —Entweder ist eine der Anwendung zugeordnete virtuelle Maschine ausgefallen oder außer Betrieb.
  - **Nicht in Betrieb** —Alle virtuellen Server, die mit den Anwendungen verknüpft sind, sind außer Betrieb.
  - **NA** —Für die Anwendung sind keine virtuellen Server konfiguriert.
- **Häufigstes Problem** —Gibt das Problem an, bei dem die meisten Fehler in der Anwendung auftreten
- **Hauptkategorie des Problems** —Gibt die Kategorie der Ausgabe an
- **Anzahl der Probleme** —Gibt die Gesamtzahl der Probleme für die Anwendung an
- **Reaktionszeit** —Gibt die durchschnittliche Antwortzeit an, bis die Anwendung reagiert
- **Fehlerprozentsatz** —Gibt den Gesamtfehlerprozentsatz von 5xx-Fehlern für die Anwendung an

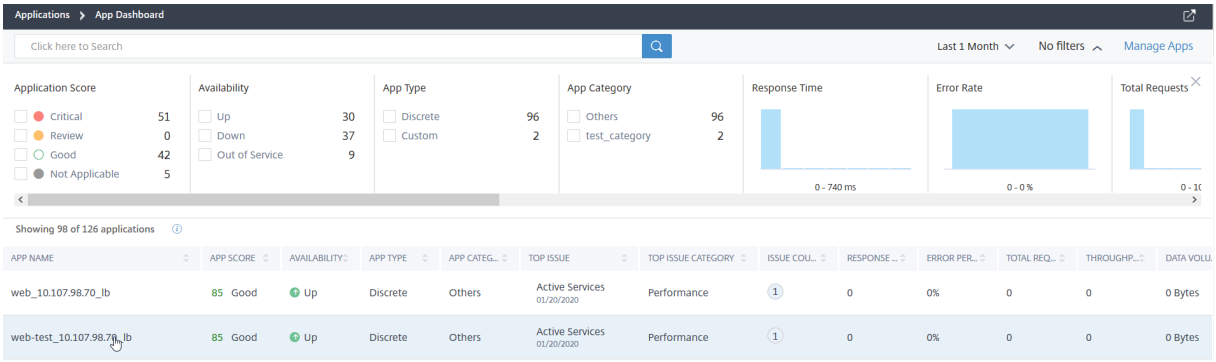
  > **Hinweis**
  >
  > Die Metrik 5xx Fehlerprozentsatz wird nur für **Citrix ADC 13.0 oder höher** angezeigt. In früheren Versionen wird der Wert als **0**angezeigt.

- **Anfragen insgesamt** —Gibt die Gesamtzahl der Anfragen an, die von der Anwendung eingegangen sind
- **Durchsatz** —Bezeichnet den gesamten Netzwerkdurchsatz für die Anwendung. Der Durchsatz wird anhand der Werte Req Bytes//Sek + Res Bytes//Sek für die virtuellen Server berechnet
- **Datenvolumen** —Bezeichnet die Gesamtdaten, die von der Anwendung verarbeitet werden
- **Client-Verbindungen** —Gibt die durchschnittlichen Client-Verbindungen an, die von der Anwendung hergestellt werden
- **Serververbindungen** —Bezeichnet die durchschnittlichen Serververbindungen, die von der Anwendung hergestellt werden.

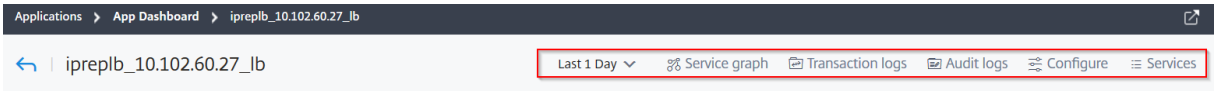
Details zur Anwendung

February 5, 2024

Klicken Sie im Dashboard auf eine Anwendung, um einen Drilldown für weitere detaillierte Informationen durchzuführen.



Die ausgewählte Anwendungsseite wird angezeigt.

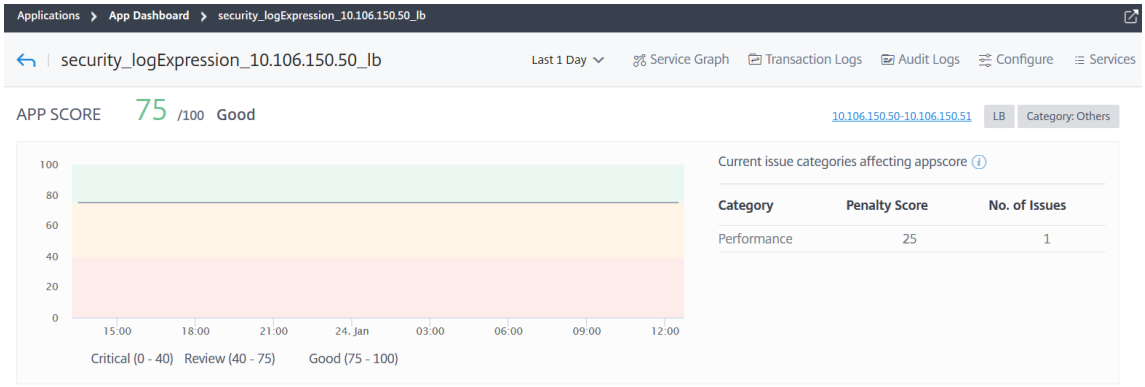


Auf der Seite mit den Anwendungsdetails:

- Wählen Sie die Zeitdauer aus der Liste aus, um Details für die bestimmte Zeitdauer anzuzeigen.
- Klicken Sie auf **Service-Diagramm**, um das Service-Diagramm für die ausgewählte Anwendung anzuzeigen. Weitere Informationen finden Sie unter Service Graph für Anwendungen
- Klicken Sie auf **Transaktionsprotokolle**, um die detaillierten Transaktionen für 5xx-Fehler anzuzeigen.
- Klicken Sie auf **Überwachungsprotokolle**, um die detaillierten Überwachungsprotokollinformationen anzuzeigen.
- Klicken Sie auf **Konfigurieren**, um den Dienst und die Dienstgruppenkonfiguration für die Anwendung anzuzeigen oder zu bearbeiten.
- Klicken Sie auf **Dienst**, um Dienste anzuzeigen, die an die Anwendung gebunden sind

Nachdem Sie die Zeitdauer ausgewählt haben, werden die folgenden Anwendungsdetails angezeigt:

- **App-Score** —Die Bewertungsbewertung für die ausgewählte Zeitdauer. Das Endergebnis wird als **100 minus Gesamtstrafe**berechnet.

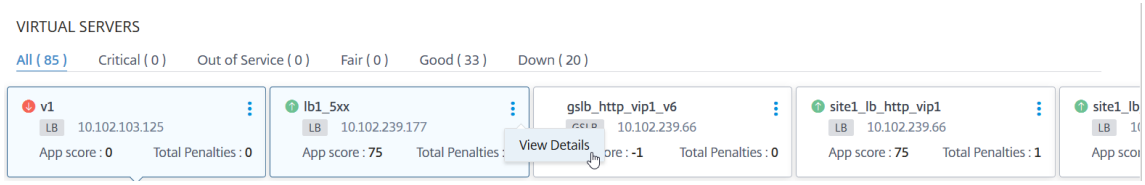


In diesem Dashboard können Sie auch die aktuellen Probleme anzeigen, die sich auf den App-Score auswirken. Sie können die Problemdetails unter Probleme einsehen.

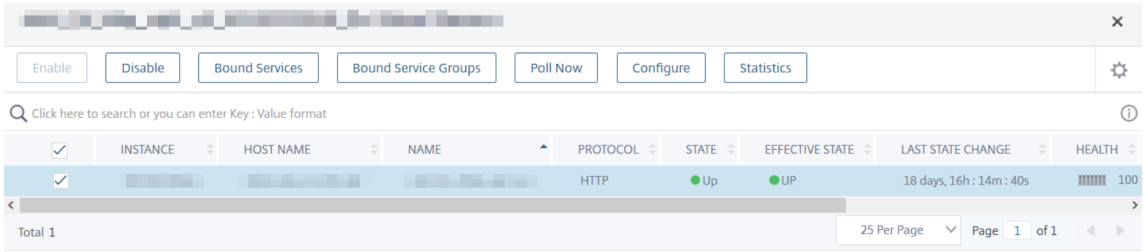
- **Virtuelle Server** —

  > **Hinweis**
  >
  > Der Abschnitt **Virtuelle Server** wird nur für die benutzerdefinierten Anwendungen angezeigt. Klicken Sie für separate Anwendungen auf die **IP-Adresse**, um die Details des virtuellen Servers anzuzeigen.

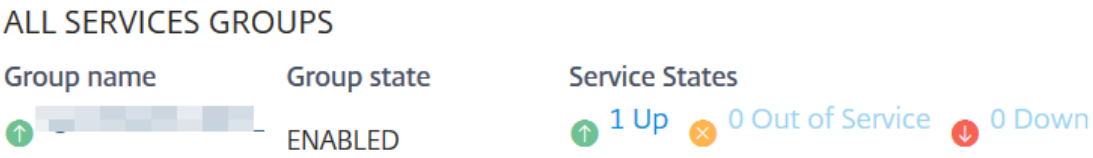
Zeigt alle virtuellen Server an, die der benutzerdefinierten Anwendung zugeordnet sind



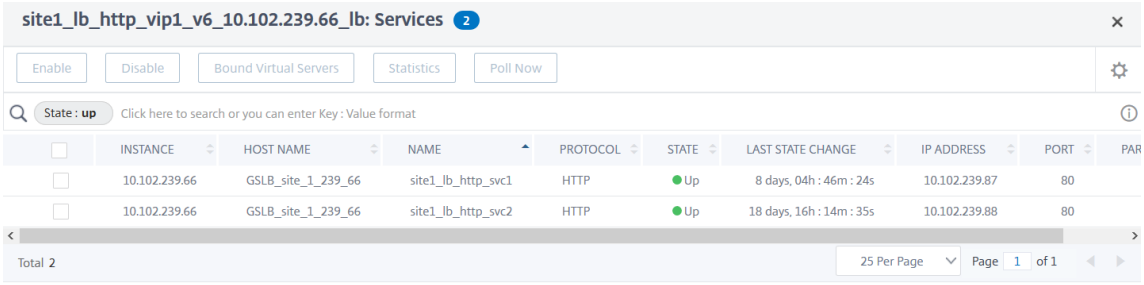
Klicken Sie auf **Details anzeigen**, um die Einstellungen des virtuellen Servers anzuzeigen und zu verwalten.



- **Alle Dienste** —Die Dienste, die an die Anwendung gebunden sind



Klicken Sie hier, um die Dienstdetails anzuzeigen und die Diensteinstellungen zu verwalten



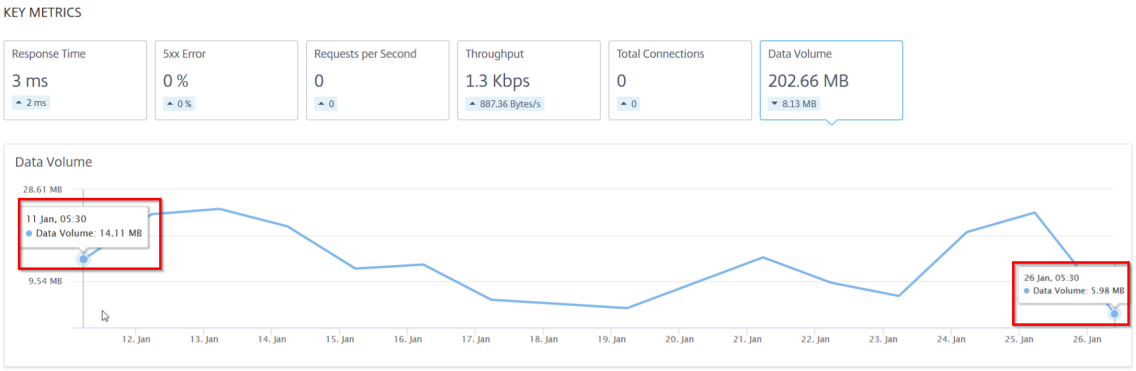
- **Schlüsselmetriken** —Details zu Anwendungsmetriken, wie **Anwendungs-Antwortzeit**, **Fehlerprozentsatz, **Anforderungen pro Sekunde**, Durchsatz**,**Gesamtverbindungen**und**Datenvolumen**. Für SSL-bezogene Anwendungen werden weitere Metrikdetails wie**Sitzungstreffer**,**Encrypted Bytes Rate**,**Decrypted Bytes Rate**und**New SSL Session Created** angezeigt.

  > **Hinweis**
  >
  > Die Metrik 5xx Fehlerprozentsatz wird nur für **Citrix ADC 13.0 oder höher** angezeigt. In früheren Versionen wird der Wert als **0**angezeigt.

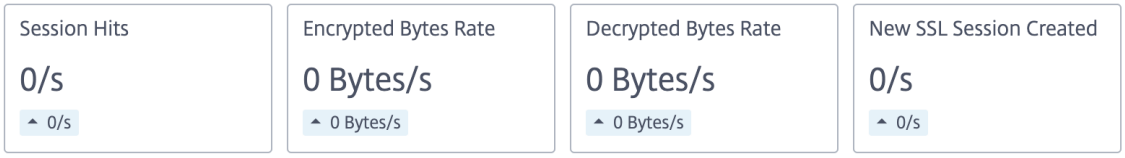
In jeder Metrik können Sie den Durchschnittswert und den Differenzwert für die ausgewählte Zeitdauer anzeigen. Der Differenzwert wird als **erster Wert minus dem letzten Wert** der ausgewählten Zeitdauer berechnet.

Sie können die folgenden Instanzmetriken für die ausgewählte Zeitdauer in einem Diagrammformat anzeigen:

Das folgende Bild ist ein Beispiel für das Datenvolumen und die gewählte Zeitdauer beträgt 1 Monat. Der Wert 202,66 MB ist das Gesamtdatenvolumen für die Dauer von 1 Monat und der Wert 8,13 MB ist der Differenzwert. In der Grafik ist der erste Wert 14,11 und der letzte Wert ist 5,98. Der Differenzwert beträgt 14,11 —5,98 = 8,13 MB.



Für SSL-bezogene Anwendungen können Sie die folgenden weiteren Metriken anzeigen:



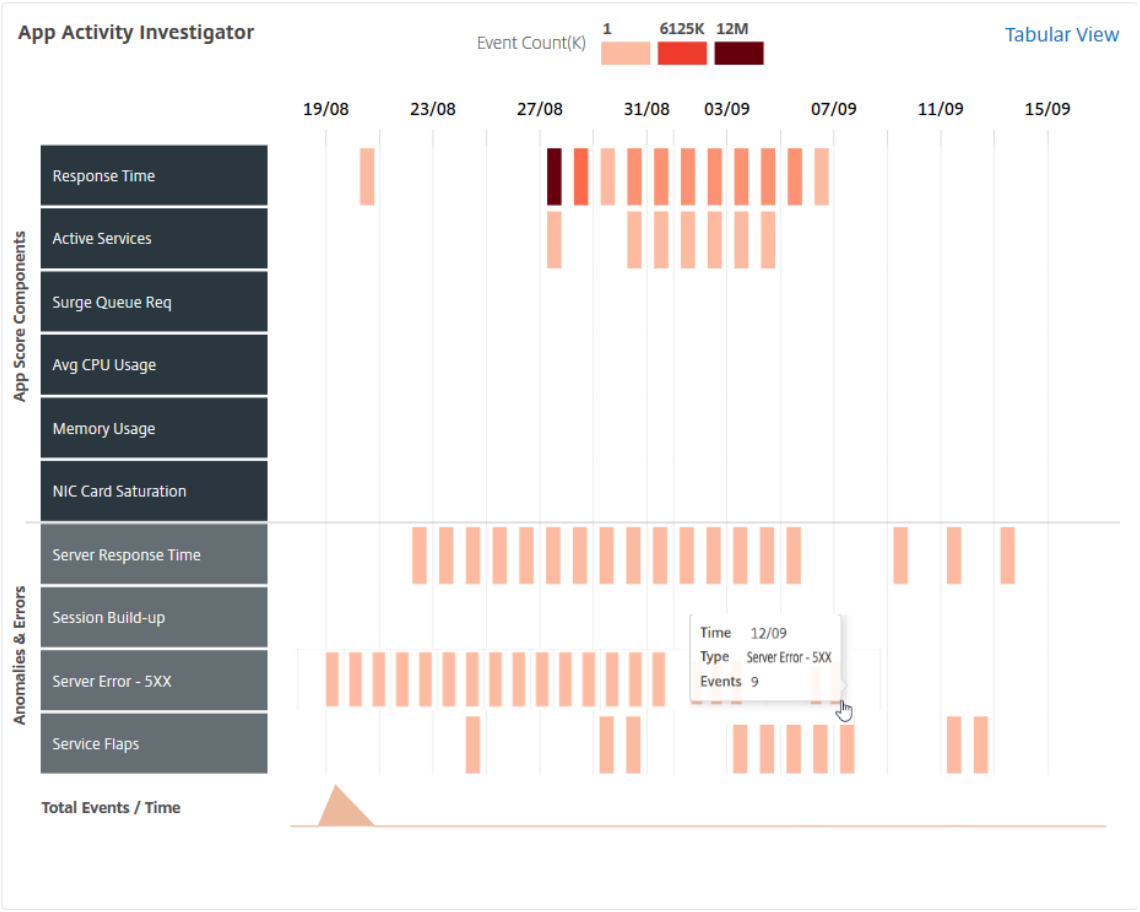
- **Probleme** —Die Probleme, die für die ausgewählte Anwendung gelten. Sie können die folgenden Probleme zusammen mit der Kategorie anzeigen:

Leistung	Instanz-Gesundheit	Config	Systemressourcen
Reaktionszeit	Durchschnittliche CPU-Auslastung	Instabiler Server	Unsachgemäßer Persistenz-Typ
Aktive Dienste	Speichernutzung	Ungewöhnlich große HTTP-Pakete	NIC-Karten-Sät
Wiederverwendung der niedrigen Sitzung		TCP-Reassemble-Queue-Limittreffer	
SurgeQueue-Aufbau			
SSL-Echtzeit-Traffic			
Aufbau einer Sitzung			
Service-Klappen			

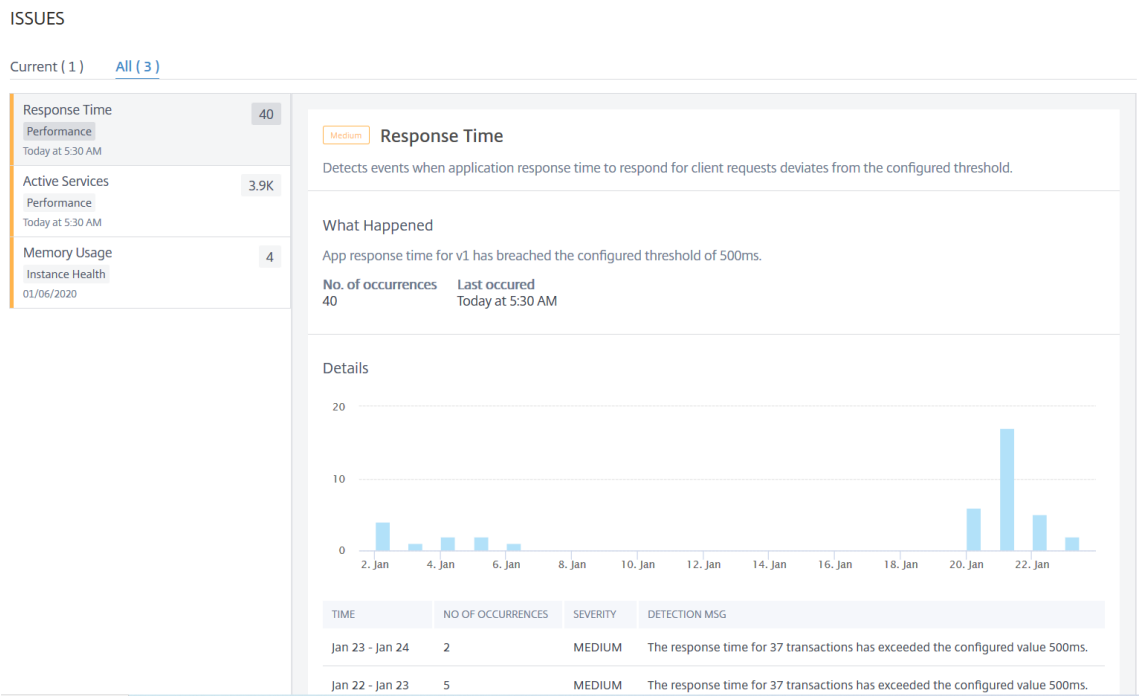
Klicken Sie auf jedes Problem, um Details wie Erkennungsmeldung, wann das Problem aufgetreten ist, Empfohlene Aktionen und Details zu überprüfen.

Weitere Informationen finden Sie unter Leistungsindikatoren für Anwendungsanalysen.

Das folgende Bild zeigt die frühere Ansicht der Seite “App Activity Investigator”:



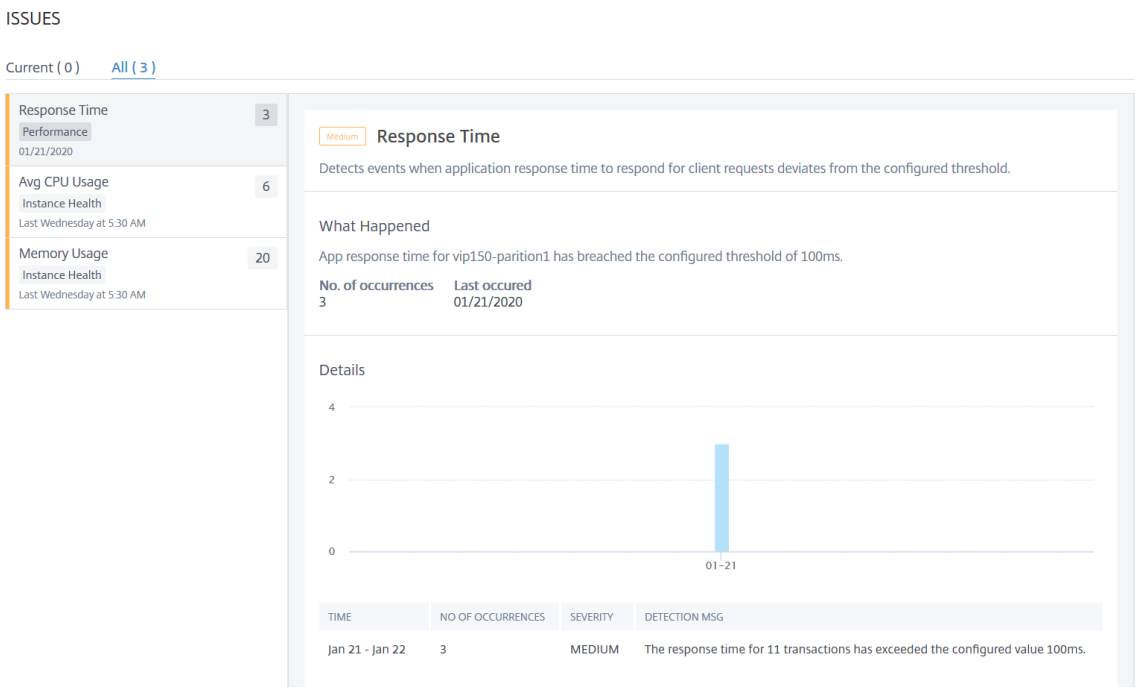
Sie können jetzt alle Probleme im Abschnitt **Probleme** zusammen mit der Kategorie anzeigen, die Sie auf der **App Activity Investigator-Seite** anzeigen konnten.



- Die Probleme, die auf der Registerkarte **Aktuell** angezeigt werden, beziehen sich auf die Anwendungsprobleme für die ausgewählte Zeitdauer.
- Die Probleme, die auf der Registerkarte **Alle** angezeigt werden, beziehen sich auf die gesamten Anwendungsprobleme.

Das folgende Beispiel zeigt die Anwendungsprobleme für eine Dauer von 1 Tag. Auf der Registerkarte **Aktuell** werden keine aktuellen Probleme angezeigt, die sich auf den App-Score auswirken.

Die Registerkarte **Alle** zeigt die Gesamtzahl der für den Zeitraum von 1 Tag erkannten Probleme an.



App-Score-Komponenten wählen und Schwellenwerte festlegen

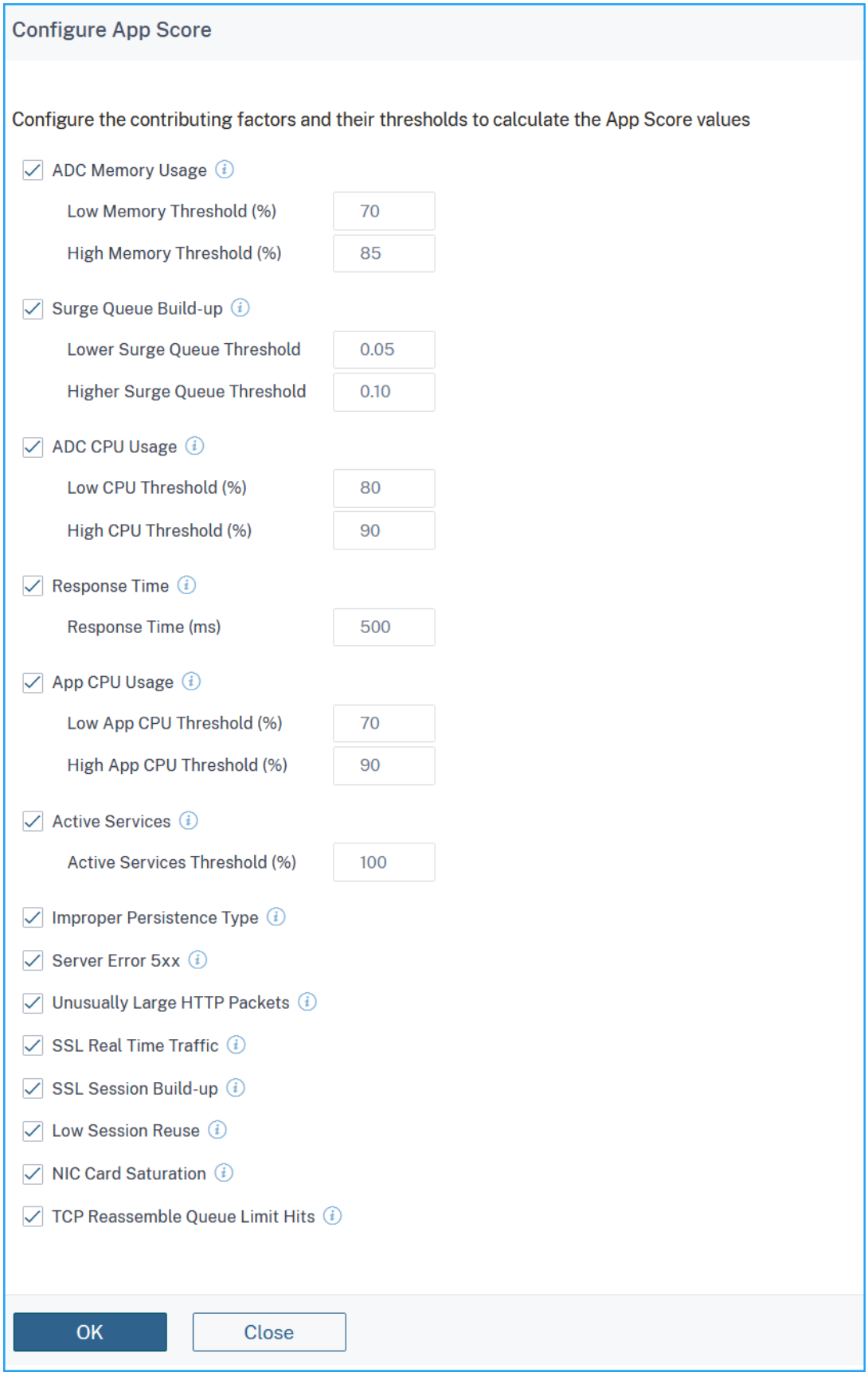
February 5, 2024

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

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

Navigieren Sie zu **Anwendungen > Dashboard** und wählen Sie dann das Einstellungssymbol aus.

Auf der Seite **App-Score konfigurieren** können Sie die Komponenten auswählen und Schwellenwerte konfigurieren, um den endgültigen App-Score zu bestimmen.



Die App-Score-Berechnung basiert auf den folgenden Komponenten:

App-Score-Komponenten	Vom Benutzer konfigurierte Schwellenwerte	Beschreibung
ADC-Speichernutzung	Ja	Der niedrige und hohe Schwellenwert für die Gesamtspeicherauslastung in der NetScaler ADC-Instanz
Aufbau von Überspannungswarteschlange	Ja	Der niedrige und hohe Schwellenwert für die gesamten Anstiegsanforderungen, die sich in der Warteschlange befinden und eine Antwort benötigen.
ADC-CPU-Auslastung	Ja	Der niedrige und hohe Schwellenwert für die gesamte CPU-Auslastung in der NetScaler ADC-Instanz.
Reaktionszeit	Ja	Das Zeitintervall zwischen dem Senden eines Anforderungspakets und dem Empfangen des ersten Antwortpakets vom Dienst, der auf dem virtuellen Server konfiguriert ist.
App-CPU-Nutzung	Ja	Der niedrige und hohe Schwellenwert für die gesamte CPU-Auslastung durch die Anwendung.
Aktive Dienste	Ja	Der Schwellenwert des Prozentsatzes der Dienste, die aktiv sein müssen, die an den virtuellen Server gebunden sind.
Unsachgemäßer Persistenz-Typ	Nein	Gibt an, ob die Persistenznutzung auf einem virtuellen Server gering ist.

App-Score-Komponenten	Vom Benutzer konfigurierte Schwellenwerte	Beschreibung
Serverfehler (5xx)	Nein	Gibt an, ob der Webserver mit 5xx-Fehlern antwortet.
Ungewöhnlich große HTTP-Pakete	Nein	Gibt das Vorkommen an, wenn die HTTP-Nachrichten mit HTTP-Header-Größe die konfigurierten Werte in der NetScaler ADC-Instanz überschreiten.
SSL Echtzeit-Verkehr	Nein	Analysiert den SSL-Verkehr, um den Echtzeitverkehr zu identifizieren, und schlägt optimale Konfigurationseinstellungen zur Verbesserung der Latenz vor.
Aufbau von SSL-Sitzungen	Nein	Gibt den Sitzungsaufbau über einen bestimmten Zeitraum an, der dazu führen kann, dass eine große Menge an Speicher von diesen Sitzungen in der NetScaler ADC-Instanz aufgehalten wird.
Geringe Wiederverwendung von Sitz	Nein	Gibt an, ob die tatsächliche Anzahl von Sitzungen, die von der NetScaler ADC-Instanz wiederverwendet werden, geringer ist.
Sättigung der NIC	Nein	Gibt die Gesamtzahl der Pakete an, die von den Schnittstellen verworfen werden.
TCP-Reassemble-Queue-Limittreffer	Nein	Gibt an, ob die Pakete einer TCP-Verbindung, die nicht in der richtigen Reihenfolge sind, die konfigurierte Größe der Paketwarteschlange für solche Pakete überschreiten.

Standardmäßig sind alle Komponenten aktiviert. Wenn Sie eine Komponente deaktivieren, führt NetScaler ADM die endgültige App-Score-Berechnung nur basierend auf den ausgewählten Komponenten durch.

> Hinweis
>
> Sie können auch weiterhin Schwellenwerte konfigurieren, indem Sie zu **Analytics > Einstellungen** navigieren und auf **App-Score konfigurieren**klicken.

Anwendungsdetails für Microservices-Anwendungen

February 5, 2024

Klicken Sie im Dashboard auf eine Microservices-Anwendung, um einen Drilldown für weitere detaillierte Informationen durchzuführen.

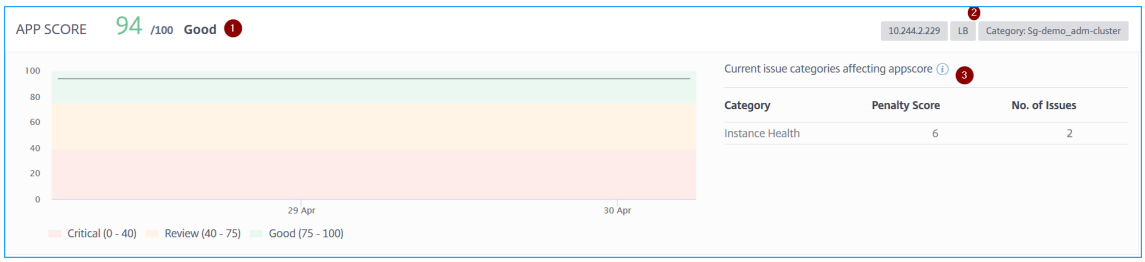
Die ausgewählte Anwendungsseite wird angezeigt.

Auf der Seite mit den Anwendungsdetails:

- Wählen Sie die Zeitdauer aus der Liste aus, um Details für die bestimmte Zeitdauer anzuzeigen.
- Klicken Sie auf **Service-Diagramm**, um das Service-Diagramm für die ausgewählte Anwendung anzuzeigen. Weitere Informationen finden Sie unter Service Graph für Anwendungen
- Klicken Sie auf **Transaktionslogs**, um die detaillierten Transaktionen für die ausgewählte Anwendung anzuzeigen.
- Klicken Sie auf **Überwachungsprotokolle**, um die detaillierten Überwachungsprotokollinformationen anzuzeigen.

Nachdem Sie die Zeitdauer ausgewählt haben, werden die folgenden Anwendungsdetails angezeigt:

- **App-Score** —Die Bewertungsbewertung für die ausgewählte Zeitdauer. Sie können sich auch die aktuellen Probleme mit der Anwendung ansehen. Dies wird als Strafpunktzahl bezeichnet, die je nach Problemkategorie gilt. Das Endergebnis wird als **100 minus Gesamtstrafe**berechnet.



1 —Bezeichnet den aktuellen App-Score

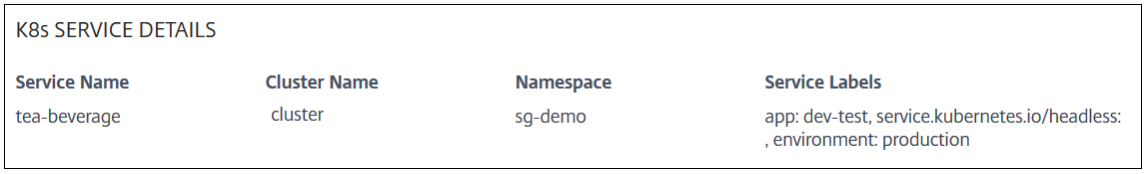
2 —Bezeichnet die CPX-IP-Adresse, den Anwendungstyp wie Lastenausgleich oder Content Switching sowie den Dienstnamespace und den Clusternamen, in dem der Dienst gehostet wird

3 —Bezeichnet die Probleme, die sich auf die aktuelle Anwendungsebene auswirken

In diesem Dashboard können Sie auch die aktuellen Probleme anzeigen, die sich auf den App-Score auswirken. Sie können die Problemdetails unter Probleme einsehen.

- **K8s Servicedetails**

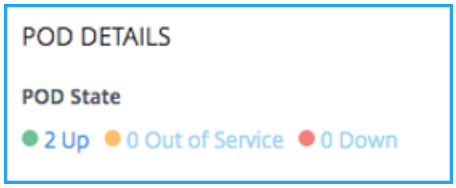
  Sie können die folgenden Details anzeigen:



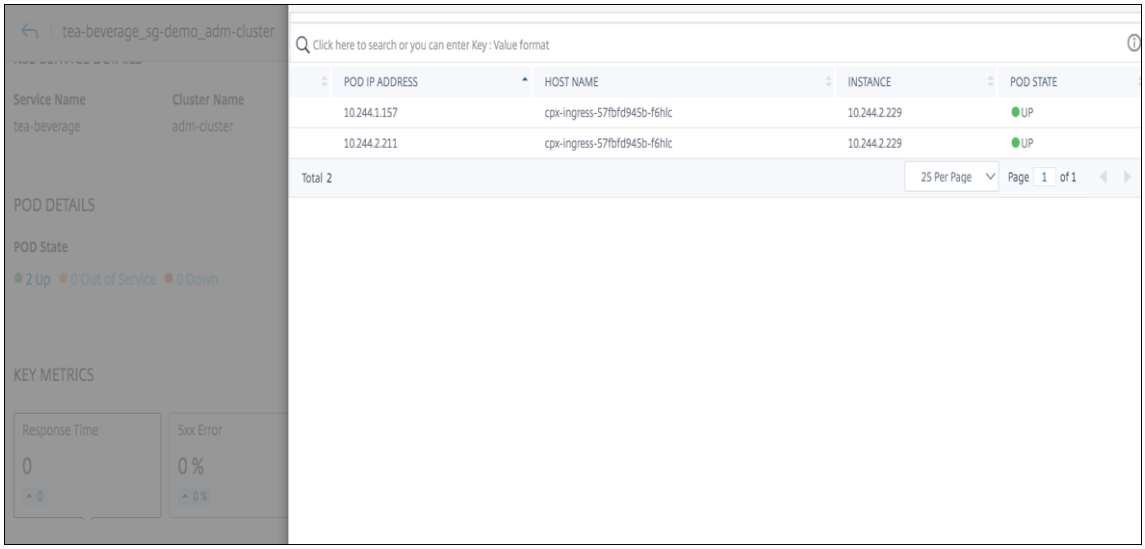
  - **Dienstname** —Der Dienstname
  - **Clustername** —Der Clustername, in dem der Dienst gehostet wird
  - **Namespace** —Der dem Service zugewiesene Namespace
  - **Service Labels** —Die Service-Labels, die dem Service zugewiesen sind

- **Pod Details**

  Ein Pod ist eine Gruppe von Containern, die im Kubernetes-Cluster gehostet werden. Innerhalb eines Pods können Sie mehrere containerisierte Anwendungen bereitstellen. Jeder Pod ist mit einer IP-Adresse verknüpft.



  Klicken Sie auf den Podstatus, um die Details anzuzeigen

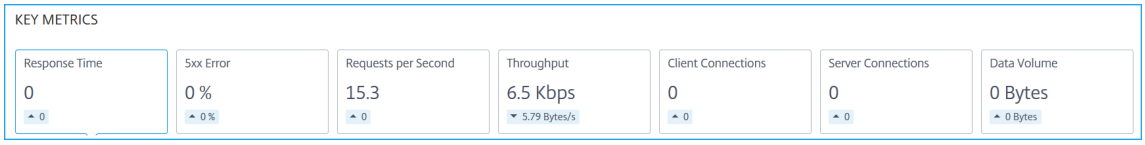


  - **Pod-IP-Adresse** —Bezeichnet die Pod-IP-Adresse
  - **Hostname** —Gibt den Hostnamen an, der dem Pod zugewiesen ist
  - **Instanz** —Bezeichnet die NetScaler ADC CPX-IP-Adresse
  - **POD-Status** —Bezeichnet den aktuellen Status des POD

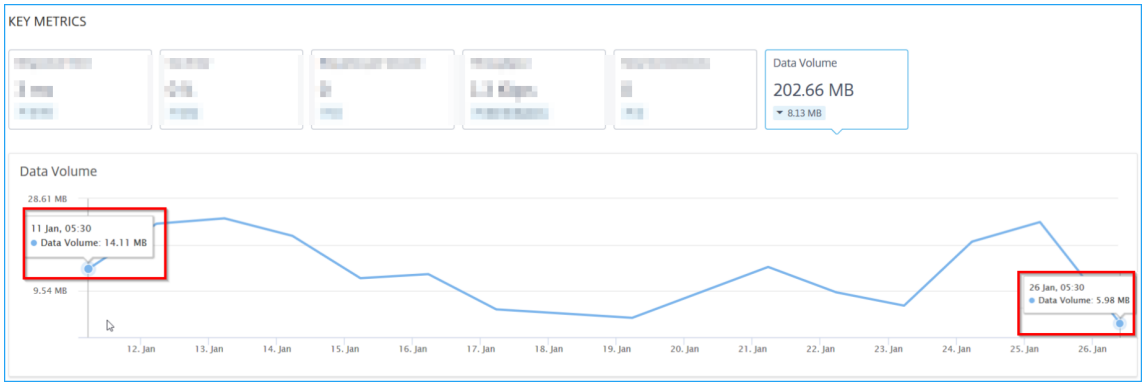
- **Wichtige Metriken** —Die wichtigsten Metrikdetails wie **Reaktionszeit**, **5xx Fehler**, **Anforderungen pro Sekunde**, **Durchsatz**, **Client-Verbindungen**, **Serververbindungen**und **Datenvolumen** werden angezeigt.

  In jeder Metrik können Sie den Durchschnittswert und den Differenzwert für die ausgewählte Zeitdauer anzeigen. Der Differenzwert wird als **erster Wert minus dem letzten Wert** der ausgewählten Zeitdauer berechnet.

  Sie können die folgenden Instanzmetriken für die ausgewählte Zeitdauer in einem Diagrammformat anzeigen:



  Die folgende Abbildung zeigt ein Beispiel für **Datenvolumen** und die ausgewählte Zeitdauer beträgt 1 Monat. Der Wert 202,66 MB ist das Gesamtdatenvolumen für die Dauer von 1 Monat und der Wert 8,13 MB ist der Differenzwert. In der Grafik ist der erste Wert 14,11 und der letzte Wert ist 5,98. Der Differenzwert beträgt 14,11 —5,98 = 8,13 MB.

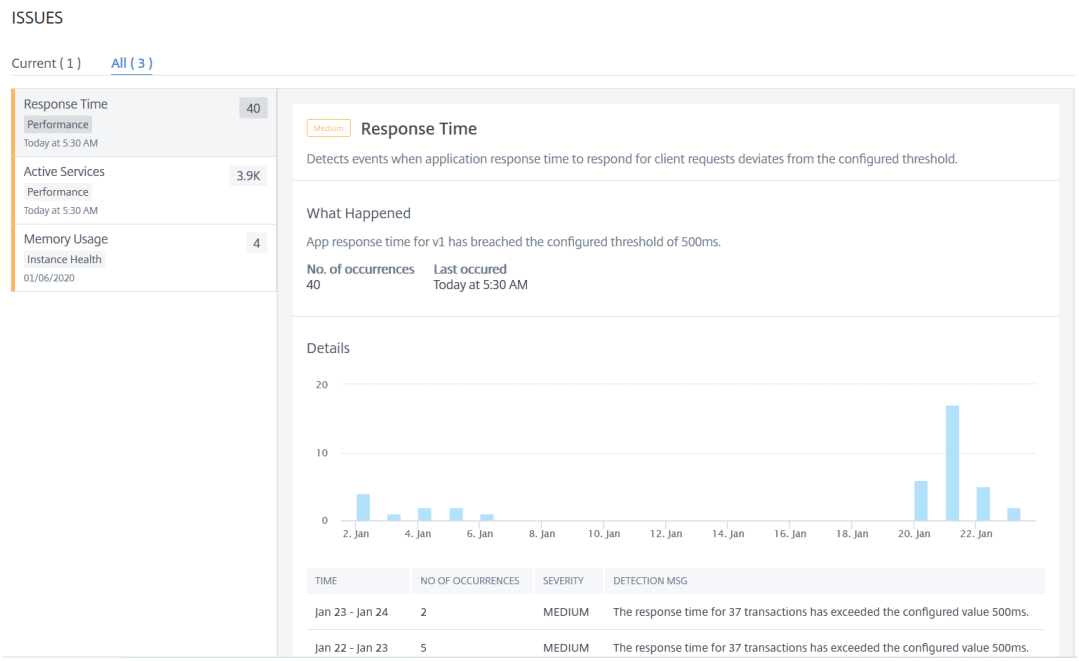


- **Probleme** —Die Probleme, die für die ausgewählte Anwendung gelten. Sie können die folgenden Probleme zusammen mit der Kategorie anzeigen:

Leistung	Instanz-Gesundheit	Config	Systemressourcen
Reaktionszeit	Durchschnittliche CPU-Auslastung	Hohe 5xx-Reaktion	Unsachgemäßer Persistenz-Typ
Wiederverwendung der niedrigen Sitzung	Speichernutzung	Ungewöhnlich große HTTP-Pakete	NIC-Karten-Sät
SurgeQueue-Aufbau		TCP-Reassemble-Queue-Limittreffer	
SSL-Echtzeit-Traffic			

Klicken Sie auf jedes Problem, um die folgenden Informationen anzuzeigen:

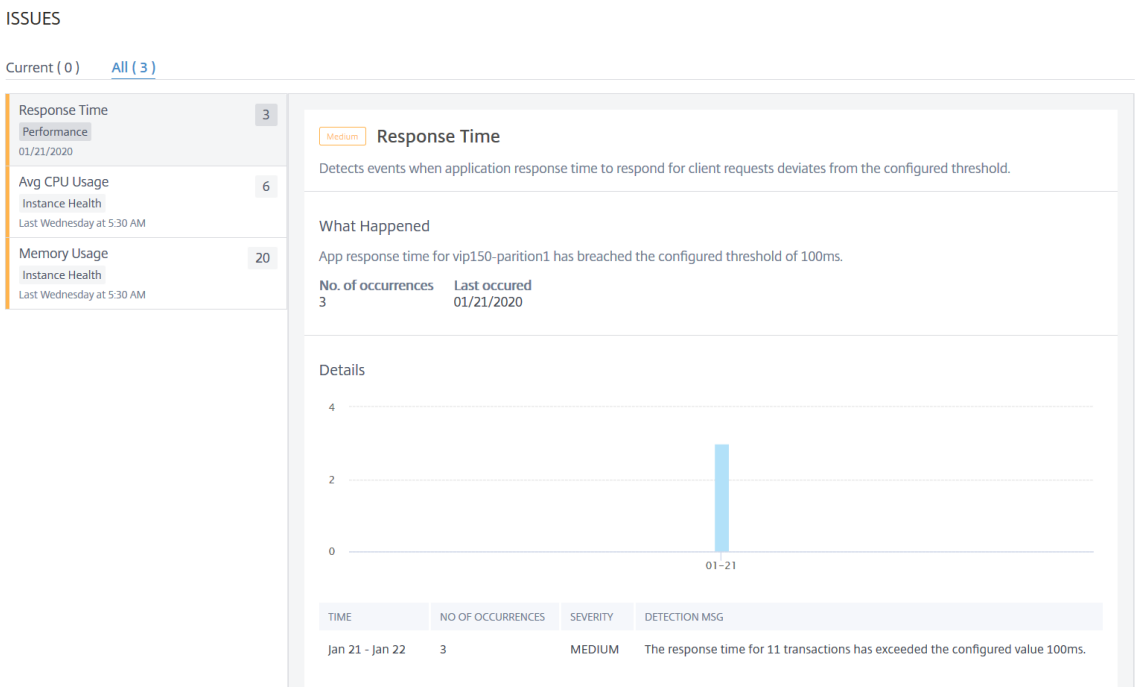
- Gesamtvorkommen
- Empfohlene Maßnahmen zur Behebung des Problems
- Die Problemdetails wie Uhrzeit, Dienstname, Gesamtzahl der Vorkommnisse, Schweregrad und Erkennungsmeldung



* Die Probleme, die auf der Registerkarte **Aktuell** angezeigt werden, beziehen sich auf die Anwendungsprobleme für die ausgewählte Zeitdauer.
* Die Probleme, die auf der Registerkarte **Alle** angezeigt werden, beziehen sich auf die gesamten Anwendungsprobleme.

Das folgende Beispiel zeigt die Anwendungsprobleme für eine Dauer von 1 Tag. Auf der Registerkarte **Aktuell** werden keine aktuellen Probleme angezeigt, die sich auf den App-Score auswirken.

Die Registerkarte **Alle** zeigt die Gesamtzahl der für den Zeitraum von 1 Tag erkannten Probleme an.



Web Insight-Dashboard

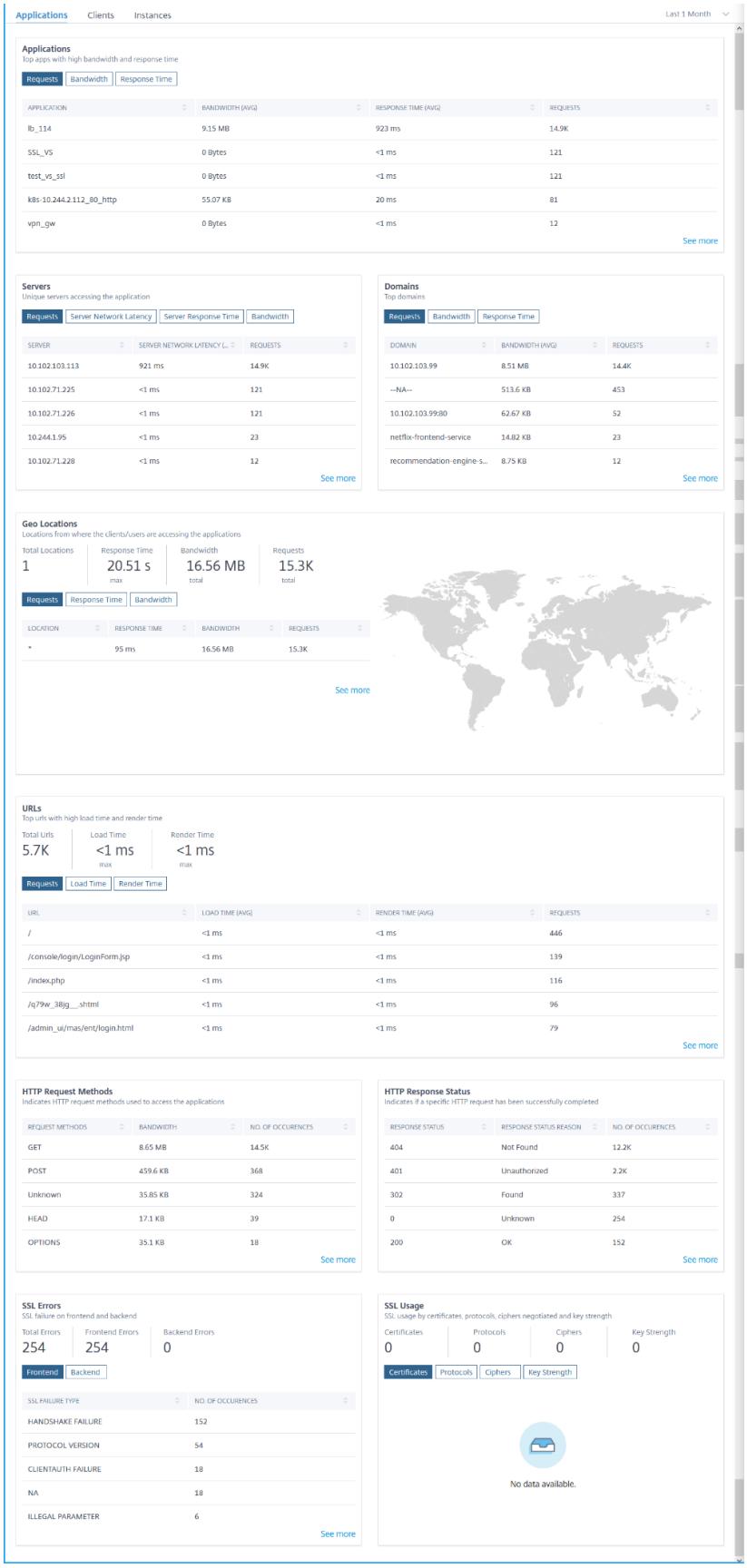
February 5, 2024

Die verbesserte Web Insight-Funktion wurde erweitert und bietet Einblicke in detaillierte Metriken für Webanwendungen, Clients und NetScaler ADC-Instanzen. Dieses verbesserte Web Insight ermöglicht es Ihnen, die gesamte Anwendung aus den Perspektiven von Performance und Nutzung gemeinsam zu bewerten und zu visualisieren. Als Administrator können Sie Web Insight anzeigen für:

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

Anwendungen	Kunden	Instanzen
Anwendungen	Kunden	Instanzmetriken
Server	Geo Standorte	Anwendungen
Domänen	HTTP-Anforderungsmethoden	Domänen

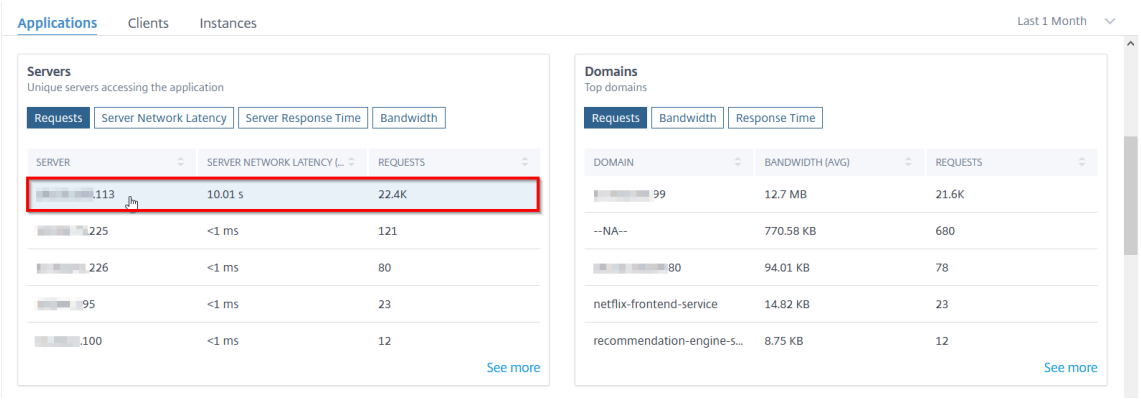
Anwendungen	Kunden	Instanzen
Geo Standorte	HTTP-Antwortstatus	URLs
URLs	URLs	HTTP-Anforderungsmethoden
HTTP-Anforderungsmethoden	Betriebssystem	HTTP-Antwortstatus
HTTP-Antwortstatus	Browser	Kunden
SSL-Fehler	SSL-Fehler	Server
SSL-Nutzung	SSL-Nutzung	Betriebssystem
		Browser



In jeder Metrik können Sie die Top-5-Ergebnisse anzeigen. Sie können klicken, um weitere Drill-downs durchzuführen, um das Problem zu analysieren und schneller Fehlerbehebungsmaßnahmen durchzuführen.

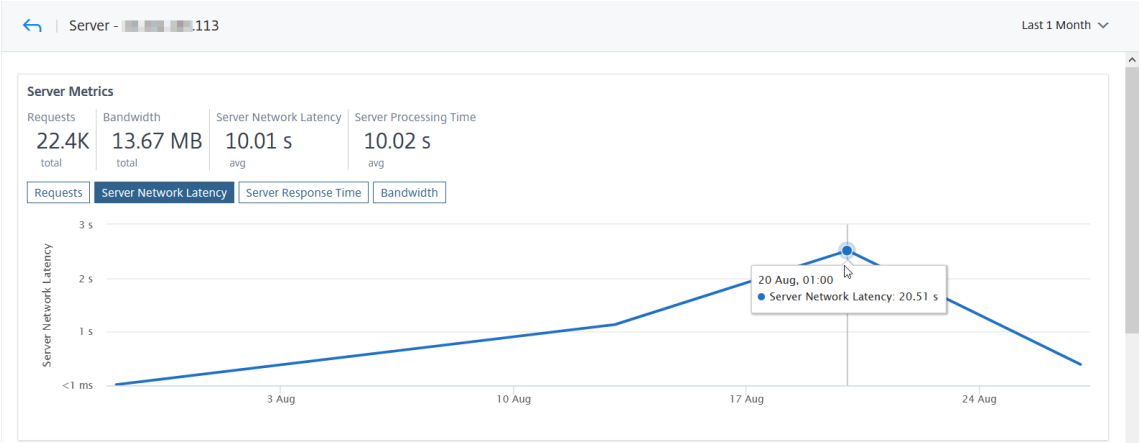
Bedenken Sie beispielsweise, dass Sie die Latenz des Servernetzwerks für eine Dauer von einem Monat analysieren und entscheiden möchten, ob Sie die Produktionsumgebung vergrößern oder verkleinern möchten. Um dies zu analysieren:

1. Wählen Sie Last 1 Month aus der Liste aus, scrollen Sie auf der Registerkarte **Anwendungen** nach unten zu **Servers**und klicken Sie auf einen Server.



   Die Metrikdetails für den ausgewählten Server werden angezeigt.

2. Wählen Sie die Registerkarte **Server Network Latency**, um die Latenz zu analysieren.



   Die durchschnittliche Latenz zeigt 10,01 s an, und aus dem Diagramm können Sie analysieren, dass die Latenz des Servernetzwerks für den letzten Monat hoch zu sein scheint. Als Administrator können Sie sich entscheiden, die Produktionsumgebung zu vergrößern.

   Weitere Informationen zum Anwendungsfall Web Insight finden Sie unter Web Insight.

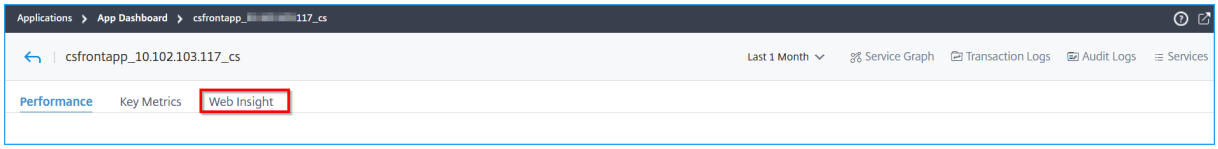
Analyse der Anwendungsverwendung

February 5, 2024

Anwendungseigentümer müssen in der Lage sein, die gesamte Anwendung unter Leistungs- und Nutzungsperspektiven zu bewerten und zu visualisieren.

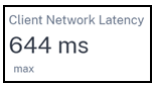
Das improvisierte **App Dashboard** ermöglicht es Ihnen, alle Anwendungsleistungen und Nutzungsmetriken zusammen anzuzeigen. Wenn Sie neben den vorhandenen Metriken zur Anwendungsleistung auf eine Anwendung klicken, werden auf der Registerkarte **Web Insight** die Metrikdetails angezeigt, die Ihnen helfen:

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



Hinweis

Für jede Metrik können Sie Optionen anzeigen, die den Höchstwert und den Gesamtwert angeben. Beispiel:

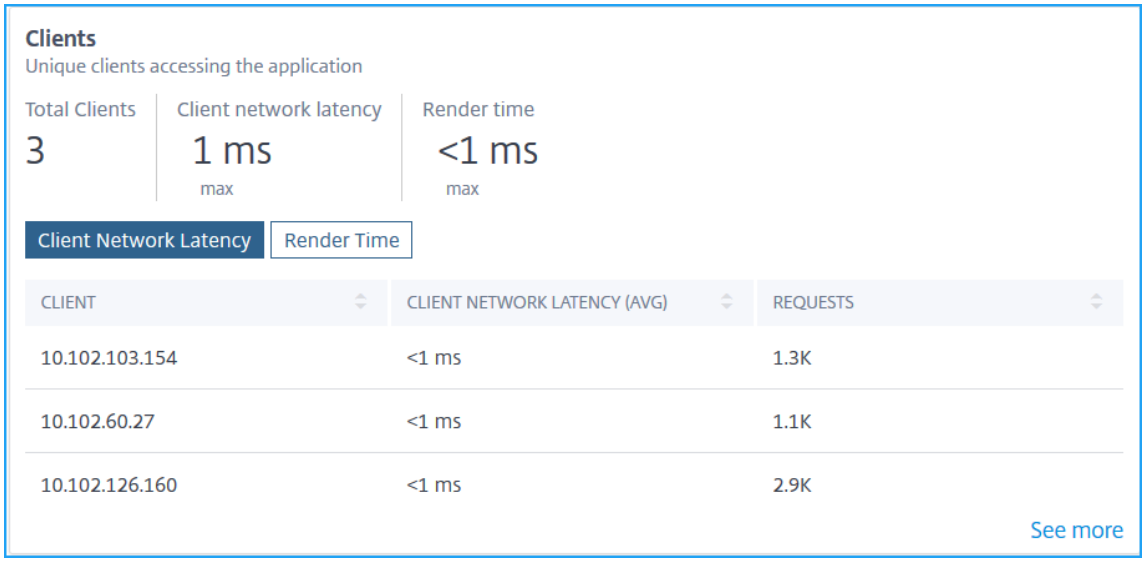
- 

Die maximale Client-Netzwerklatenz für die gewählte Dauer. Beachten Sie, dass Sie die Netzwerklatenz für Client 1 = 30 ms, Client 2 = 15 ms und Client 3 = 3 ms haben. In diesem Szenario zeigt die **Clientnetzwerklatenz** 30 ms an.
- 

Die gesamte Bandbreite, die von allen verfügbaren Clients/Servern für die gewählte Dauer verbraucht wurde. Beachten Sie, dass Sie den Bandbreitenverbrauch für Client 1 = 30 MB, Client 2 = 45 MB, Client 3 = 40 MB haben.
In diesem Szenario wird die Bandbreite angezeigt (30 MB + 45 MB + 40 MB) = 115 MB.

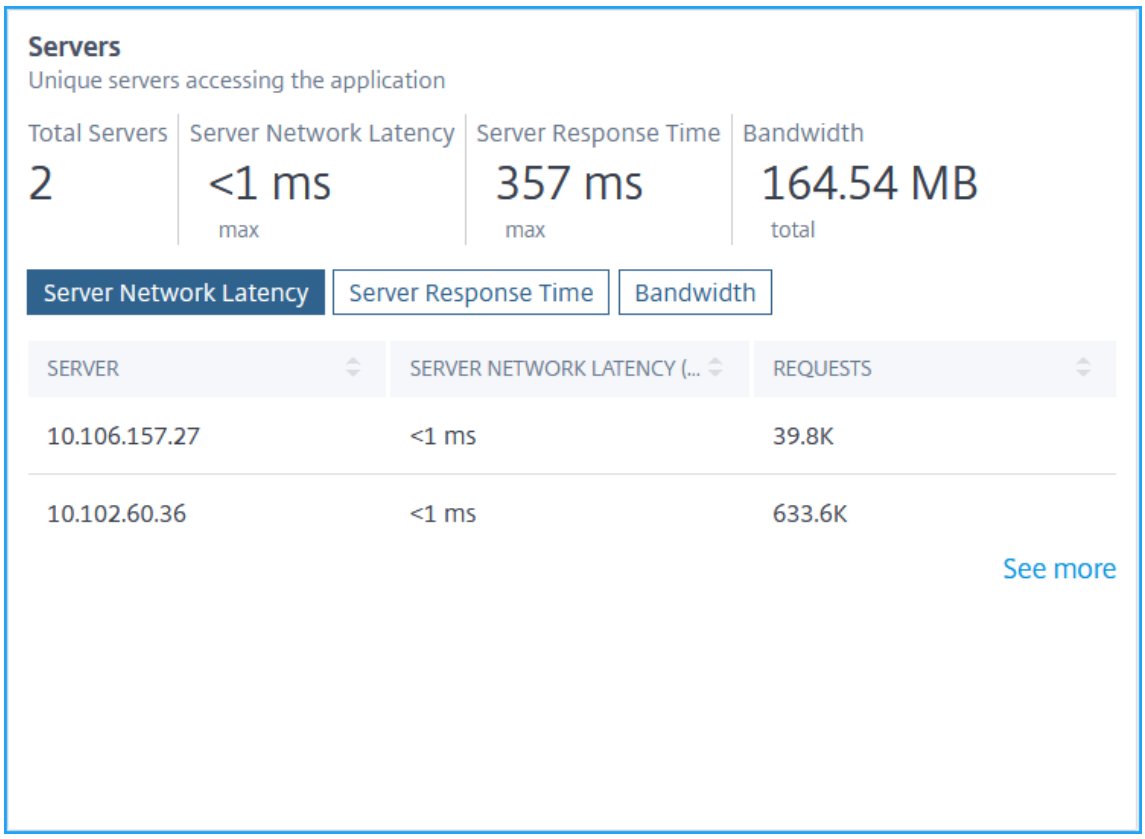
Im Folgenden finden Sie die Web Insight-Metriken, die Sie auf der Registerkarte **Verwendung** anzeigen können:

- **Clients** —Zeigt die Erkenntnisse für Clients an, die auf die Anwendung zugreifen:



- **Clients insgesamt** —Zeigt die Gesamtzahl der Clients an, die auf die Anwendung zugreifen.
- **Client-Netzwerklatenz** —Zeigt die Netzwerklatenz vom Client zum NetScaler ADC an. Klicken Sie auf die Registerkarte **Client Network Latency**, um Folgendes anzuzeigen:
  - **Client** —Die Client-IP-Adresse.
  - **Client-Netzwerklatenz (Durchschn.)** —Die durchschnittliche Netzwerklatenz des Clients.
  - **Anforderungen** —Die Gesamtanzahl der Anforderungen des Clients.
- **Renderzeit** —Zeigt die Zeit an, die zum Rendern der Serverantwort benötigt wurde Klicken Sie auf die Registerkarte **Renderzeit**, um Folgendes anzuzeigen:
  - **Client** —Die Client-IP-Adresse.
  - **Renderzeit (Durchschn.)** —Die durchschnittliche Renderzeit vom Client.
  - **Anforderungen** —Die Gesamtanzahl der Anforderungen des Clients.

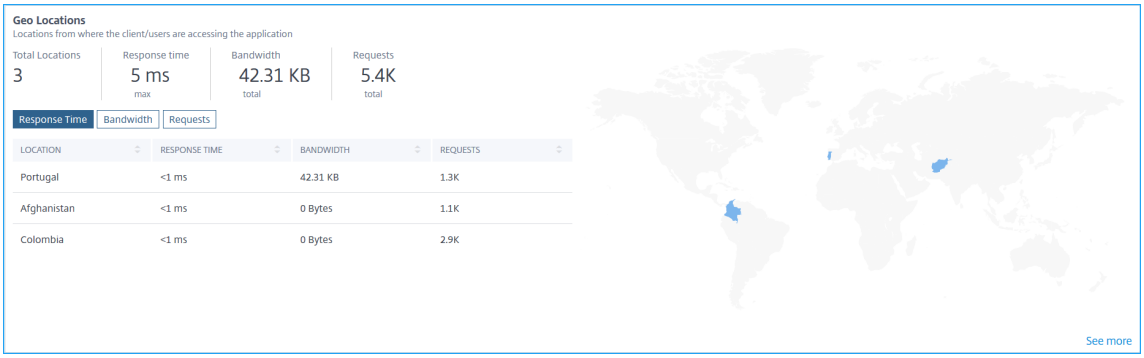
- **Server** —Zeigt die Erkenntnisse für Server an, die auf die Anwendung zugreifen:



- **Server insgesamt** —Zeigt die Gesamtzahl der Server an, die auf die Anwendung zugreifen.
- **Server-Netzwerklatenz** —Zeigt die Netzwerklatenz vom Server zu NetScaler ADC an. Klicken Sie auf die Registerkarte **Server-Netzwerklatenz**, um Folgendes anzuzeigen:
  - **Server** —Die IP-Adresse des Servers.
  - **Server-Netzwerklatenz (Durchschn.)** —Die durchschnittliche Netzwerklatenz des Servers.
  - **Anforderungen** —Die Gesamtanzahl der Anforderungen vom Server.
- **Serverantwortzeit** —Zeigt die Zeit an, die der Server benötigt, um auf Anforderungen zu antworten. Klicken Sie auf die Registerkarte **Serverantwortzeit**, um Folgendes anzuzeigen:
  - **Server** —Die IP-Adresse des Servers.
  - **Reaktionszeit (Durchschn.)** —Die durchschnittliche Antwortzeit des Servers.
  - **Anforderungen** —Die Gesamtanzahl der Anforderungen vom Server.
- **Bandbreite** —Zeigt die Gesamtbandbreite an, die von den Servern verbraucht wird. Klicken Sie auf die Registerkarte **Bandbreite**, um Folgendes anzuzeigen
  - **Server** —Die IP-Adresse des Servers.

        * **Bandbreite** —Die gesamte vom Server verbrauchte Bandbreite.
        * **Anforderungen** —Die Gesamtanzahl der Anforderungen vom Server.

- **Geo-Standorte** —Zeigt die Erkenntnisse für Clients an, die von einem bestimmten Standort aus auf die Anwendung zugreifen:

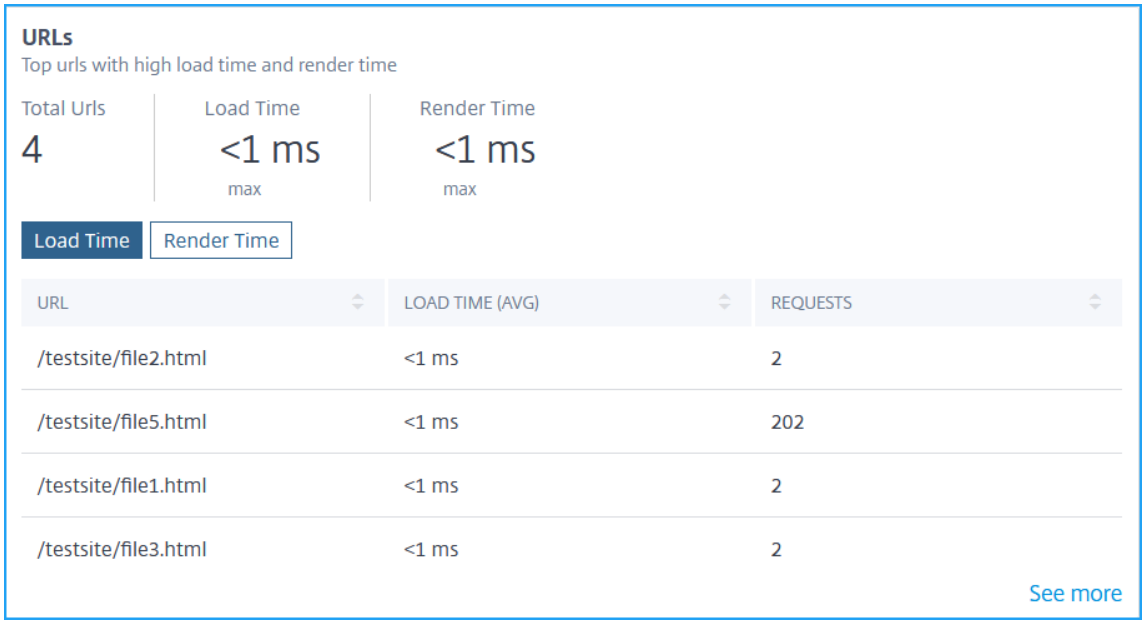


    - **Standorte insgesamt** —Zeigt die Gesamtzahl der Client-Standorte an, die auf die Anwendung zugreifen
    - **Reaktionszeit** —Zeigt die Reaktionszeit vom Standort des Clients an.
    - **Bandbreite** —Zeigt die Gesamtbandbreite an, die von Clients an allen Standorten verbraucht wird.
    - **Anfragen** —Zeigt die Gesamtzahl der Anfragen von allen Client-Standorten an.

      Klicken Sie auf jede Registerkarte, um sie anzuzeigen

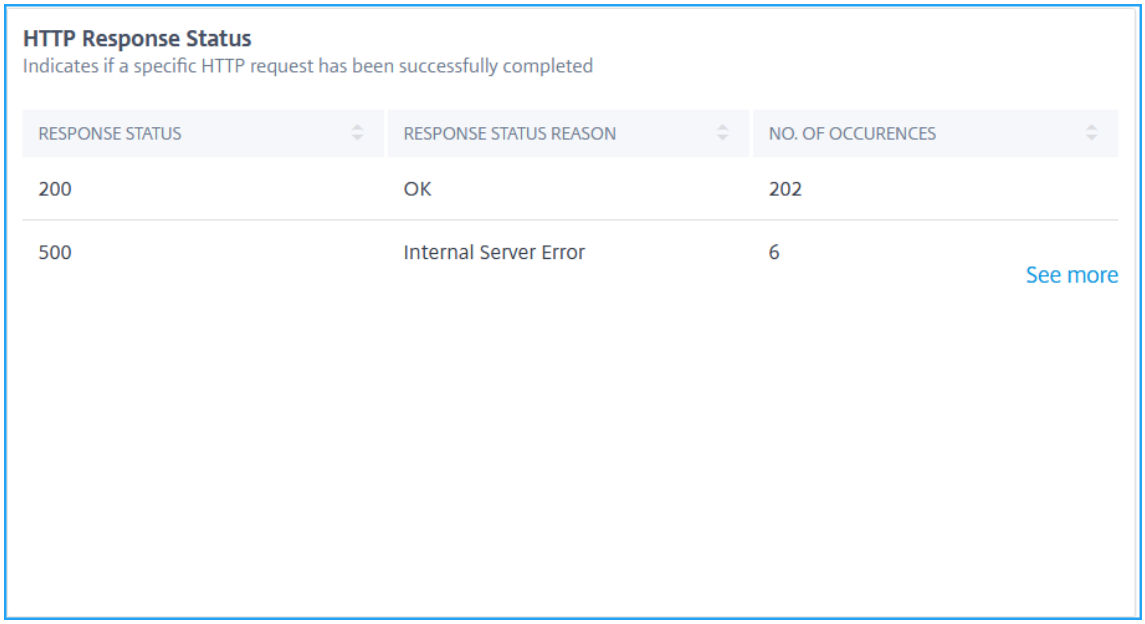
        * **Standort** —Der Name des Standorts.
        * **Reaktionszeit** —Die durchschnittliche Antwortzeit vom Standort des Clients.
        * **Bandbreite** —Die vom Client-Standort verbrauchte Bandbreite.
        * **Anfragen** —Die Gesamtzahl der Anfragen vom Clientstandort.

- **URLs** —Zeigt die Erkenntnisse für URLs mit hoher Last- und Renderzeit an:



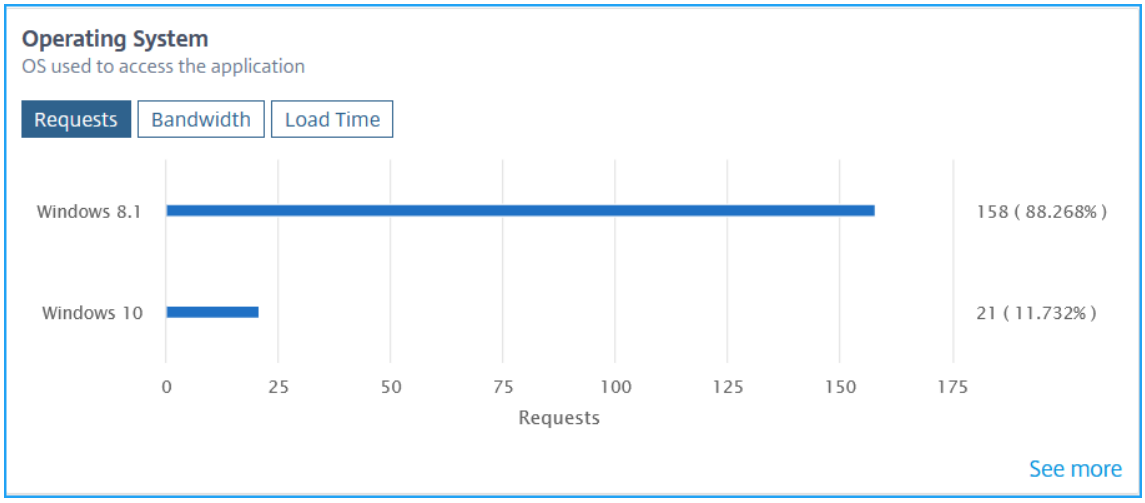
- **URLs gesamt** —Zeigt die Gesamtzahl der URLs an.
- Ladezeit —Zeigt die Zeit an, die für das Laden der URL gebraucht wurde. Klicken Sie auf die Registerkarte **Ladezeit**, um Folgendes anzuzeigen:
  - **URL** —Der URL-Name.
  - **Ladezeit (Durchschn.)** —Die durchschnittliche Zeit, die für das Laden der URL benötigt wird.
  - **Anforderungen** —Die Gesamtanzahl der Anforderungen von der URL.
- **Renderzeit** —Zeigt die Zeit an, die für das Rendern und Anzeigen der URL benötigt wird. Klicken Sie auf die Registerkarte **Renderzeit**, um Folgendes anzuzeigen:
  - **URL** —Der URL-Name.
  - **Renderzeit (Durchschn.)** —Die durchschnittliche Zeit, die die URL zum Rendern benötigt.
  - **Anforderungen** —Die Gesamtanzahl der Anforderungen von der URL.

- **HTTP-Antwortstatus** —Zeigt die Erkenntnisse für eine bestimmte abgeschlossene HTTP-Anforderung an.



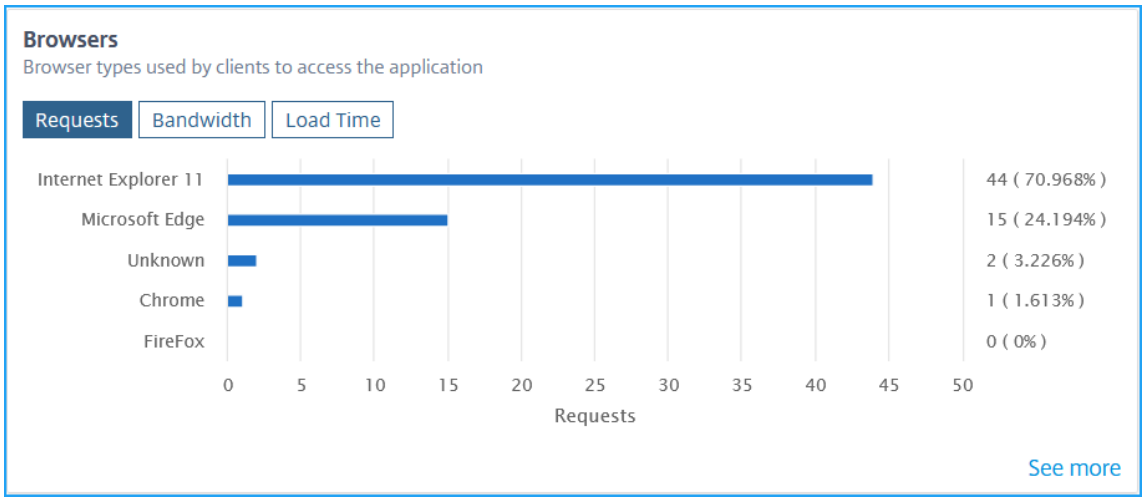
- **Antwortstatus** —Zeigt den Antwortcode an, z. B. 2xx, 4xx, 5xx usw.
- **Grund für den Antwortstatus** —Zeigt den Grund für die Antwort an, z. B. interner Serverfehler, Nicht gefunden usw.
- **Anzahl der Vorkommen** —Zeigt die Gesamtzahl der Vorkommen an.

- **Betriebssystem** —Zeigt die Erkenntnisse für das Betriebssystem an, das auf die Anwendung zugreift.



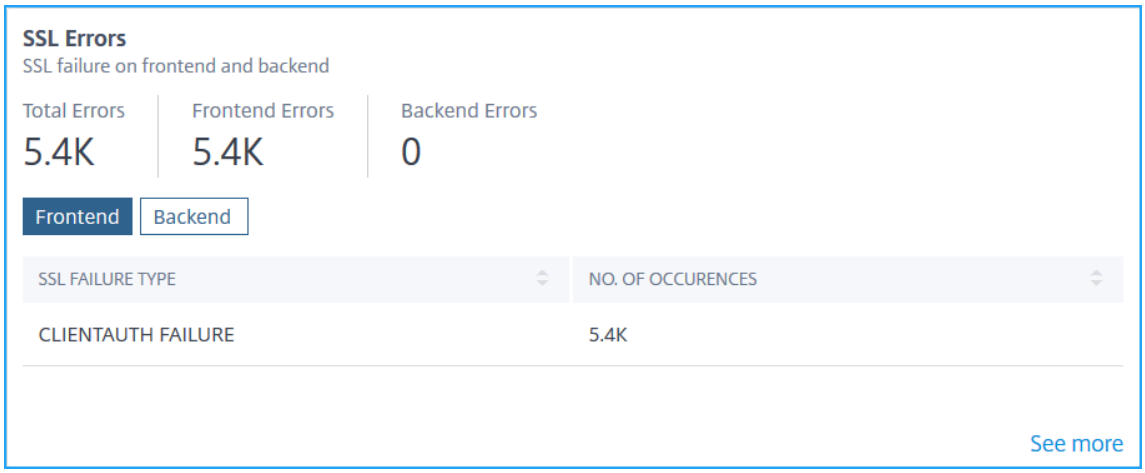
- **Anforderungen** —Zeigt die Gesamtzahl der Anforderungen von jedem Betriebssystem an.
- **Bandbreite** —Zeigt die Gesamtbandbreite an, die von jedem Betriebssystem verbraucht wird.
- **Ladezeit** —Zeigt die Gesamtzeit an, die jedes Betriebssystem zum Laden vom Server benötigt hat.

- **Browser** —Zeigt die Erkenntnisse für die Browsertypen an, die von den Clients für den Zugriff auf die Anwendung verwendet werden.



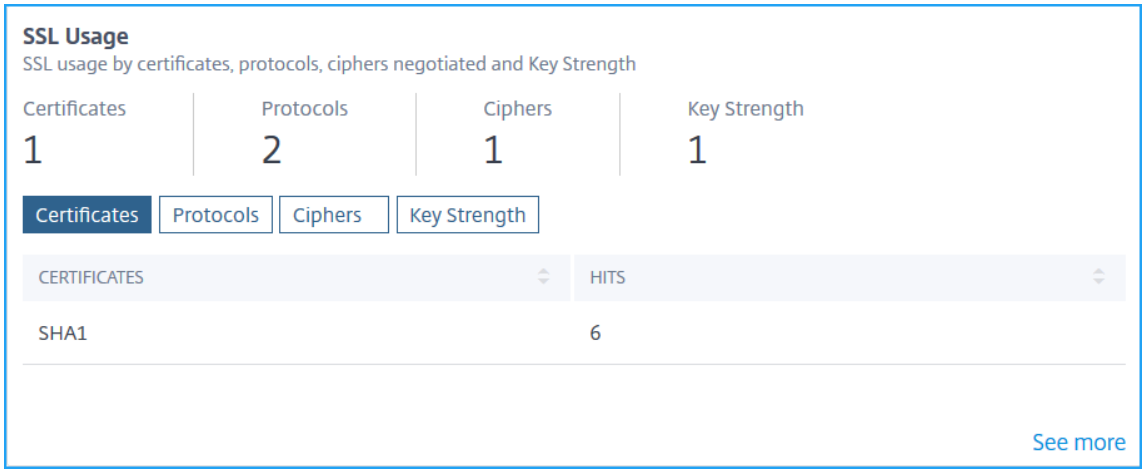
  - **Anfragen** —Zeigt die Gesamtzahl der Anfragen von jedem Browser an.
  - **Bandbreite** —Zeigt die Gesamtbandbreite an, die von jedem Browser verbraucht wird.
  - **Ladezeit** —Zeigt die Gesamtzeit an, die ein Browser vom Server geladen hat.

- **SSL-Fehler** —Zeigt die Erkenntnisse für die SSL-Fehler vom Front-End-Server und Back-End-Server an.



  - **Total Error** —Zeigt die gesamten SSL-Fehlervorkommen an.
  - **Frontend** —zeigt die gesamten SSL-Fehler vom Front-End-Server an. Klicken Sie auf die Registerkarte **Frontend**, um den SSL-Fehlertyp und die Gesamtereignisse anzuzeigen.
  - **Backend** —Zeigt die gesamten SSL-Fehler vom Back-End-Server an. Klicken Sie auf die Registerkarte **Backend**, um den SSL-Fehlertyp und die Gesamtereignisse anzuzeigen.

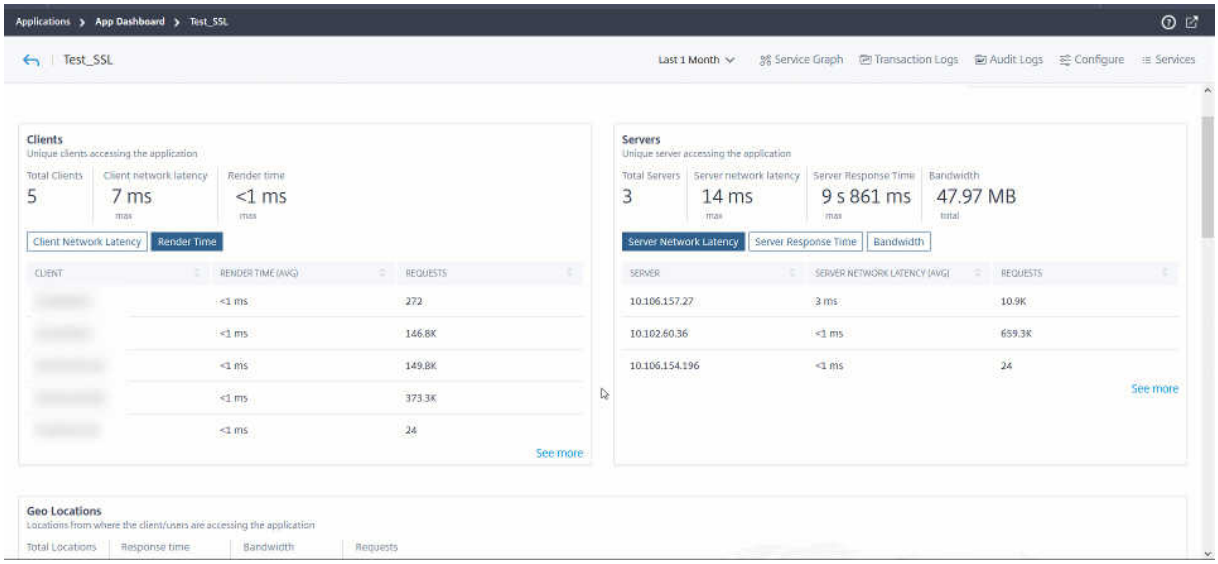
- **SSL-Nutzung** —Zeigt die Erkenntnisse für die SSL-Nutzung an, wie SSL-Zertifikate, Protokolle, Verschlüsselungen und Schlüsselstärke.



- **Zertifikate** —Zeigt die Gesamtzahl der SSL-Zertifikate an. Klicken Sie auf die Registerkarte **Zertifikate**, um den Zertifikatsnamen und die Gesamtzahl der Treffer anzuzeigen.
- **Protokolle** —Zeigt die Gesamtzahl der SSL-Protokolle an. Klicken Sie auf die Registerkarte **Protokolle**, um Details zum SSL/TSL-Protokoll und die Gesamtzahl der Treffer anzuzeigen.
- **Chiffren** —Zeigt die Gesamtzahl der Chiffren an. Klicken Sie auf die Registerkarte **Verschlüsselungen**, um Details für die einzelnen Chiffre-Suite-Namen und die Gesamtzahl der Treffer anzuzeigen.
- **Schlüsselstärke** —Zeigt die gesamte Schlüsselstärke an, die in SSL-Zertifikaten verwendet wird. Klicken Sie auf die Registerkarte **Schlüsselstärke**, um Details für jede Schlüsselstärke und die Gesamtzahl der Treffer anzuzeigen.

Anzeigen von Metriken im grafischen Format

Für jede Metrik können Sie weitere Details in einem grafischen Format anzeigen, indem Sie auf **Mehr anzeigen** klicken. Klicken Sie auf **, um Details in einem grafischen Format anzuzeigen.



Im Folgenden finden Sie die Details, die Sie für jede Metrik anzeigen können, nachdem Sie auf die Option **Mehr** anzeigen geklickt haben:

Insight-Name	Metriken	Beschreibung
—-	—-	—-
Clients	Kunden	Bezeichnet die Clientliste
	Renderzeit (AVG)	Gibt die durchschnittliche Zeit an, die der Client zum Rendern der Serverantwort benötigt.
	Netzwerklatenz des Clients (AVG)	Kennzeichnet die durchschnittliche Netzwerklatenz vom Client zur NetScaler ADC-Instanz
	Anfragen	Bezeichnet die Gesamtzahl der Anfragen des Clients
Server	Server	Bezeichnet die Serverliste
	Verarbeitungszeit des Servers (AVG)	Gibt die durchschnittliche Zeit an, die der Server benötigt, um die Anforderungen zu verarbeiten
	Netzwerklatenz des Servers (AVG)	Kennzeichnet die durchschnittliche Netzwerklatenz vom Server zur NetScaler ADC-Instanz
	Treffer	Gibt die Gesamtzahl der vom Server empfangenen Treffer an
Geo Standorte	Standorte	Bezeichnet die Clientstandorte
	Reaktionszeit	Gibt die gesamte Antwortzeit vom Clientstandort an
	Bandbreite	Gibt die gesamte Bandbreite an, die vom Standort verbraucht wird
	Anfragen	Bezeichnet die Gesamtzahl der Anfragen vom Standort
URL	Renderzeit (AVG)	Gibt die durchschnittliche Zeit an, die zum Laden der Seite vom Server benötigt wird
	Ladezeit (AVG)	Gibt die durchschnittliche Zeit an, die die URL zum Rendern und Anzeigen benötigt
	Treffer	Bezeichnet die Gesamtzahl der Treffer von der URL
HTTP-Antwortstatus	Name	Gibt den Namen des Antwortstatus an, z. B. OK, Nicht gefunden, In-

terner Serverfehler usw. |
	Antwortstatus	Gibt den vom Server empfangenen Antwortstatuscode an, z. B. 200, 400, 500 usw.
	Treffer	Gibt die Gesamtzahl der Treffer aus dem Antwortcode an
	Bandbreite	Gibt die insgesamt verbrauchte Bandbreite an
Betriebssystem	Betriebssystem	Bezeichnet den Betriebssystemnamen wie Windows, MAC
	Ladezeit	Gibt die Gesamtzeit an, die das Betriebssystem benötigt, um vom Server zu laden
	Bandbreite	Gibt die gesamte Bandbreite an, die vom Betriebssystem verbraucht wird
	Anforderungen	Bezeichnet die Gesamtzahl der Anfragen vom Betriebssystem
Browser	Browser	Bezeichnet den Browsernamen wie Mozilla Firefox, Chrome usw.
	Ladezeit	Gibt die Gesamtzeit an, die ein Browser benötigt, um vom Server zu laden
	Bandbreite	Gibt die Gesamtbandbreite an, die vom Browser verbraucht wird
	Anforderungen	Bezeichnet die Gesamtzahl der Anfragen vom Browser
SSL-Fehler	SSL-Fehltyp	Bezeichnet den Fehlernamen wie CLIENTAUTH FAILURE
	Vorkommen	Gibt die Gesamtzahl der Vorkommen für den SSL-Fehler an
SSL-Verwendung	Bezeichnet den Protokollnamen und die Versionen wie TLS, SSL
	Treffer	Bezeichnet die Gesamtzahl der Treffer aus dem Protokoll

Weitere Informationen zu Anwendungsfällen von Web Insight finden Sie unter Web Insight.

Problembehandlung bei App-Dashboard

February 5, 2024

Nachdem Sie eine Anwendung im App Dashboard hinzugefügt haben, zeigt das Dashboard sofort die grundlegenden Konfigurationsdetails der App an. Die Details der Anwendungsanalyse wie App-Score, wichtige Metriken und Probleme werden innerhalb weniger Minuten (etwa 10 bis 15 Minuten) ausgefüllt. Weitere Informationen finden Sie unter Anwendungen.

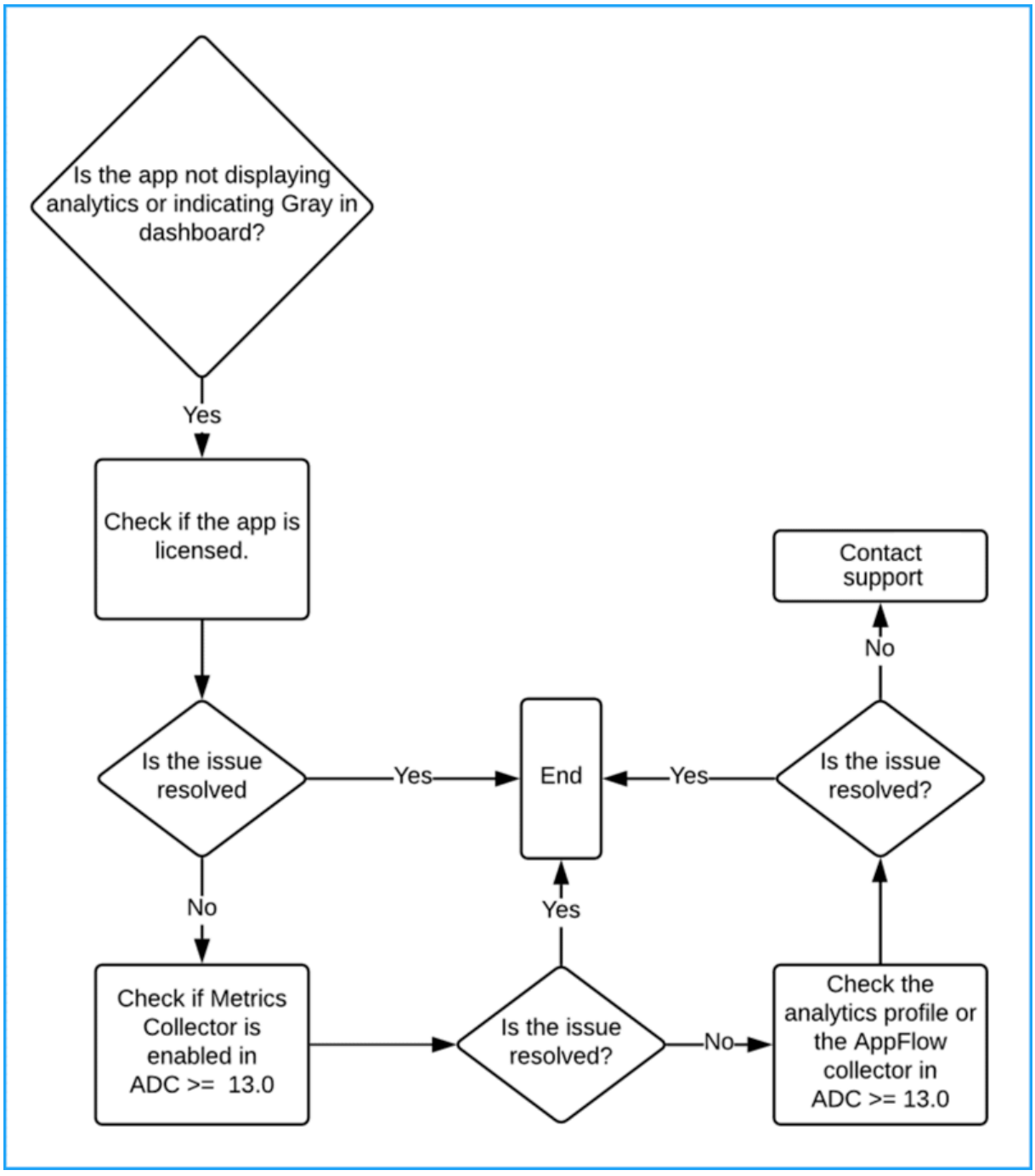
Sie müssen sicherstellen, dass es kein Problem mit dem Datenfluss von Metriken (AppFlow-Collector oder Analytics-Profil) aus der NetScaler ADC-Instanz gibt. In diesem Dokument erhalten Sie weitere Informationen zum AppFlow-Collector und zum Analytics-Profil.

In diesem Dokument werden die Schritte zur Fehlerbehebung beschrieben, die Sie ausführen müssen, wenn:

- Sie klicken auf eine Anwendung, die Analysen für die ausgewählte Anwendung zeigen die erforderlichen Daten auch nach der genannten Dauer (10-15 Minuten) nicht an.
- Die CS- oder LB-Anwendung zeigt im App Dashboard immer die graue Farbe (**nicht zutreffender** Status) an.

> **Hinweis**
>
> Die in diesem Dokument erwähnten Fehlerbehebungsverfahren gelten nur für virtuelle **Content Switching** und **Load Balancing**.

Szenario zur Problem



Die Anwendung ist lizenziert

Sie müssen sicherstellen, dass die Anwendung lizenziert ist.

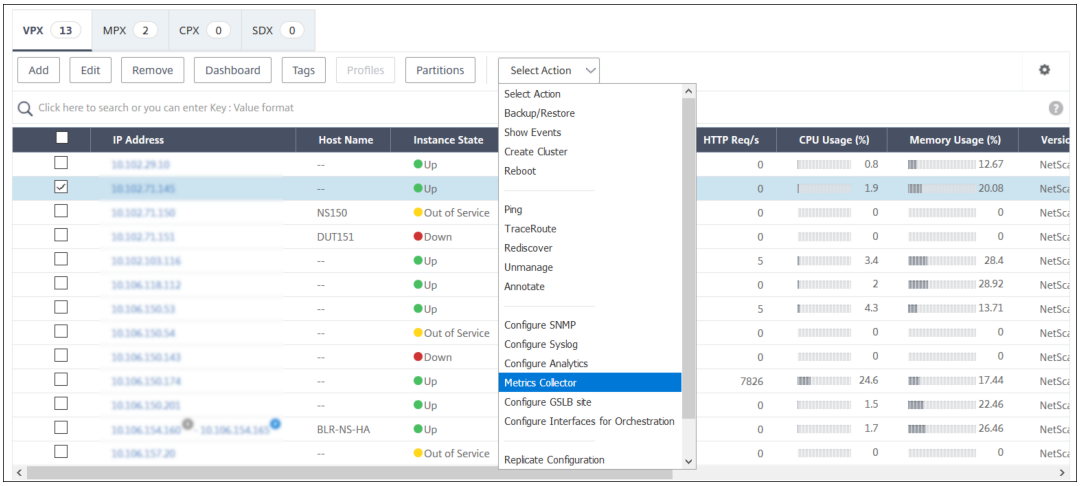
- **ADM Service** - Navigieren Sie zu **Konto > Abonnements** und überprüfen Sie, ob die Anwendung unter **Virtual Server License Summary**lizenziert ist. Wenn die Anwendung nicht lizenziert ist, lesen Sie Verwalten der Lizenzierung und Aktivieren von Analysen auf virtuellen Servern, um den virtuellen Server zu lizenzieren.
- **ADM on-prem** —Navigieren Sie zu **System > Licensing & Analytics** und überprüfen Sie, ob die Anwendung unter **Virtual Server License Summary**lizenziert ist. Wenn die Anwendung nicht lizenziert ist, lesen Sie Verwalten der Lizenzierung und Aktivieren von Analysen auf virtuellen Servern, um den virtuellen Server zu lizenzieren.

Metrikensammler ist aktiviert

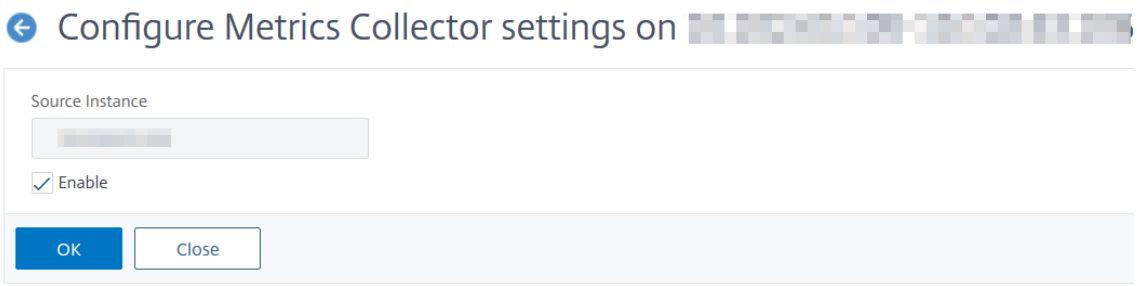
Sie müssen sicherstellen, dass **Metrics Collector** in der NetScaler ADC-Instanz aktiviert ist.

Für NetScaler ADC Version 13.0 oder höher ist Metrics Collector standardmäßig aktiviert, nachdem die ADC-Instanz erfolgreich in ADM hinzugefügt wurde. So stellen Sie sicher, ob der Metrikensammelpunkt

1. Navigieren Sie zu **Netzwerke > Instanzen**. Wählen Sie unter Instanzen den Instanz-Typ aus (z. B. NetScaler ADC VPX).
2. Wählen Sie die NetScaler ADC-Instanz aus.
   a) Wählen Sie in der Liste **Aktion auswählen** die Option **Metriksammlung** aus.



3. Stellen Sie auf der Seite **Einstellungen für Metriksammler konfigurieren** sicher, dass die Option **Aktivieren** ausgewählt ist Wenn nicht, wählen Sie die Option **Aktivieren** und klicken Sie auf **OK**.



Nachdem Sie den Metrikensammelpunkt aktiviert haben und die Daten immer noch nicht anzeigen können, überprüfen Sie Folgendes:

- Der AppFlow-Collector in der Citrix ADC-Instanzversion 13.0 **vor 47.x Build**.
- Das Analyseprofil in der Citrix ADC-Instanz Build **47.x oder** höher .

Ältere Builds von NetScaler ADC-Instanzen

Bei NetScaler ADC:

1. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass der Collector an Port 5563 **UP** ist:

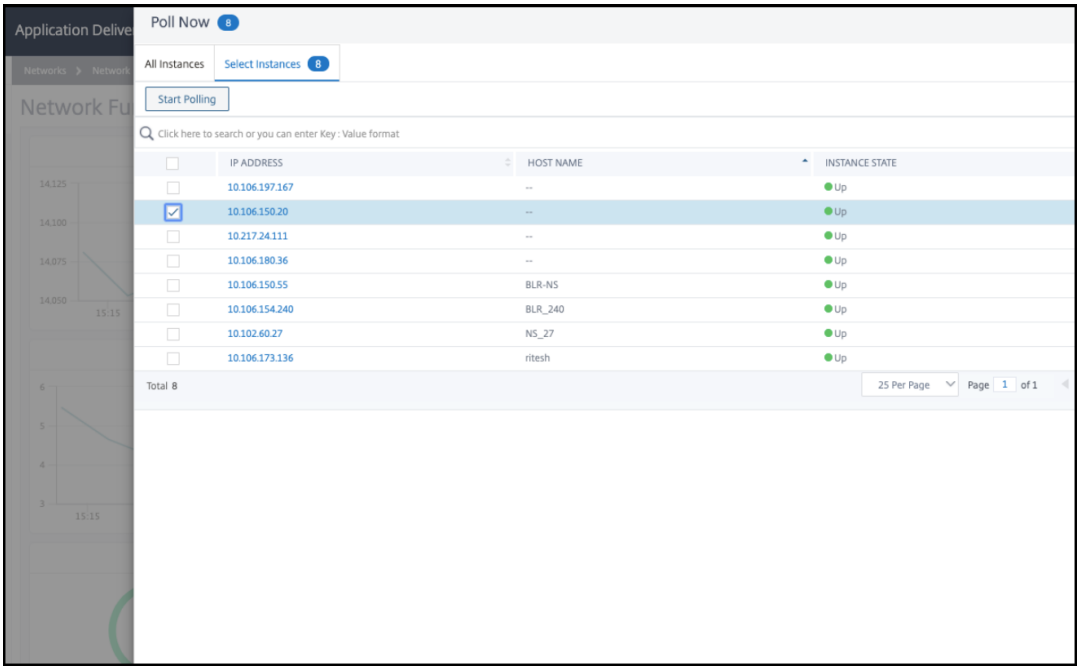
   ```
   sh appflow collector af_collector_rest_<adm_receiver_ip>
   ```

   ```
   > sh appflow collector af_collector_rest_10.102.103.114
   1) Name: af_collector_rest_10.102.103.114
   IPv4 address: 10.102.103.114
   Port: 5563
   Netprofile:
   Transport: rest
   State: UP
   Done
   ```

2. Wenn kein Collector verfügbar ist, führen Sie eine manuelle Instanzabfrage in NetScaler ADM durch.

   a) Navigiere zu **Netzwerke > Netzwerkfunktion > Jetzt abfragen**

   b) Wählen Sie die Instanz aus und klicken Sie auf **Polling starten**.



Wenn das Polling fehlschlägt, entfernen Sie die ADC-Instanz aus ADM und fügen Sie dann die ADC-Instanz erneut hinzu. Wenn Sie die ADC-Instanz hinzufügen, wird der Collector zu ADC hinzugefügt.

Wenn der Kollektor den Status **Down** anzeigt:

1. Stellen Sie sicher, dass die SNIP konfiguriert ist.

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP           Active   Enabled  Enabled  NA       Enabled
```

   Wenn SNIP nicht konfiguriert ist, müssen Sie SNIP konfigurieren. Weitere Informationen finden Sie unter SNIP konfigurieren.

2. Stellen Sie sicher, dass die ADC-Instanz für ADM erreichbar ist.

   Sie können validieren, indem Sie einen Ping-Test durchführen. Führen Sie `ping -S <SNIP> <adm_receiver_ip>` aus.

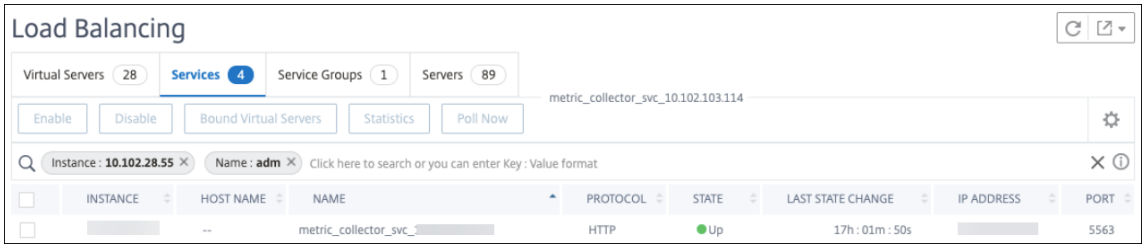
```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```


NetScaler ADC-Instanz wird später erstellt

Stellen Sie in NetScaler ADM sicher, dass der Metrik-Collector-Dienst verfügbar ist:

1. Navigieren Sie zu **Netzwerke > Netzwerkfunktion > Load Balancing > Services**.
2. Filtern Sie in der Suchleiste nach **Instanz: (IP-Adresse)** und **Name: ADM**.
3. Stellen Sie sicher, ob `adm_metric_collector_svc_<adm_receiver ip>` verfügbar ist. Die IP-Adresse kann entweder die ADM-Verwaltungs-IP oder die Agenten-IP sein.

   Stellen Sie sicher, dass sich dieser Dienst im **UP-Status** befindet und auf Port 5563 ausgeführt wird.



Wenn Sie die Daten immer noch nicht anzeigen können, stellen Sie sicher, dass der Collector-Dienst an das Zeitreihenanalyseprofil in NetScaler ADC gebunden ist.

1. Melden Sie sich bei NetScaler ADC an
2. Führen Sie den folgenden Befehl aus:

   `sh analytics profile ns_analytics_time_series_profile`

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Wenn der Kollektor den Status **Down** anzeigt:

1. Stellen Sie sicher, dass die SNIP konfiguriert ist.

```
> sh ip | grep SNIP
2)  10.106.150.34    0            SNIP           Active   Enabled  Enabled  NA      Enabled
```


Wenn SNIP nicht konfiguriert ist, müssen Sie SNIP konfigurieren. Weitere Informationen finden Sie unter SNIP konfigurieren.

2. Stellen Sie sicher, dass die ADC-Instanz für ADM erreichbar ist.

   Sie können validieren, indem Sie einen Ping-Test durchführen. Führen Sie `ping -S <SNIP> <adm_receiver_ip>` aus.

```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

3. Stellen Sie sicher, dass die Verkehrskonnektivität über Telnet den Dienst verbinden kann.

```
root@ns# telnet 10.102.103.114 5563
Trying 10.102.103.114...
Connected to 10.102.103.114.
Escape character is '^]'.
^]
telnet> q
Connection closed.
```

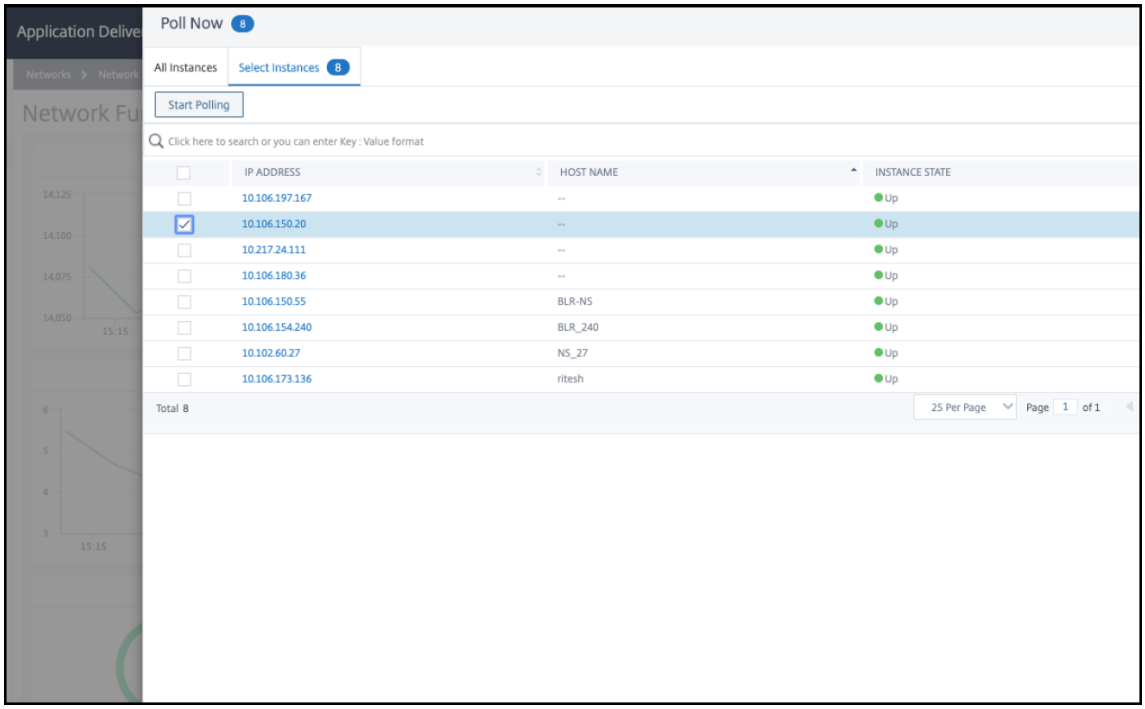
   Wenn Telnet in der Lage ist, den Dienst zu verbinden, existiert eine Firewall, die den Metrikdatenfluss blockiert. Sie müssen das Blockproblem der Firewall lösen.

Wenn kein Collector-Dienst an das Zeitreihenanalyseprofil in NetScaler ADC gebunden ist, wird Collector als leer angezeigt.

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector:
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Sie müssen eine manuelle Abfrage für die Instanz in NetScaler ADM durchführen.

1. Navigiere zu **Netzwerke > Netzwerkfunktion > Jetzt abfragen**
2. Wählen Sie die Instanz aus und klicken Sie auf **Polling starten**.



Wenn das Abfragen fehlschlägt, fügen Sie den Collector-Dienst direkt in der NetScaler ADC-Instanz mit den folgenden Befehlen hinzu:

```
add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip
> HTTP 5563
```

```
unset analyticsprofile ns_analytics_time_series_profile -collectors
```

```
set analytics profile ns_analytics_time_series_profile -collectors
 adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -
events enabled
```

Das Analytics-Zeitreihenprofil wird aktualisiert.

```
> add service adm_metric_collector_svc_10.102.103.114 10.102.103.114 HTTP 5563
 Done
> unset analyticsprofile ns_analytics_time_series_profile  -collectors
 Done
> set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_10.102.103.114 -metrics enab
 Done
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Wenn das Problem auch nach Durchführung aller genannten Schritte zur Fehlerbehebung weiterhin

besteht, wenden Sie sich an den **Citrix Support**.

Schwellenwert und Warnung für Anwendungsanalysen erstellen

February 5, 2024

Mit der Anwendungsanalyse in NetScaler ADM können Sie die verschiedenen Arten von Datenverkehr überwachen, der durch NetScaler ADC-Instanzen fließt. Mit Citrix ADM können Sie Schwellenwerte für die folgenden Leistungsindikatoren festlegen, um den Datenverkehr und die App-Bewertung zu überwachen.

Sie können Schwellenwerte konfigurieren und den App-Score für CPU, Arbeitsspeicher, NIC-Discards und Reaktionszeit überwachen.

So konfigurieren Sie die App-Score in NetScaler ADM:

1. Navigieren Sie in Citrix ADM zu **Analytics** > **Einstellungen**.
2. Klicken Sie auf der Seite **Einstellungen** auf **App-Score konfigurieren**.
3. Geben Sie auf der Seite **App-Score konfigurieren** die Werte für die folgenden Parameter ein:

    a) **Niedriger CPU-Schwellenwert**. Der niedrigere Schwellenwert der gesamten CPU-Auslastung in der NetScaler ADC-Instanz.

    b) **Hoher CPU-Schwellenwert**. Der höhere Schwellenwert der gesamten CPU-Auslastung in der NetScaler ADC-Instanz.

    c) **Niedriger Speicherschwellenwert**. Der niedrigere Schwellenwert der Gesamtspeicherauslastung in der NetScaler ADC-Instanz.

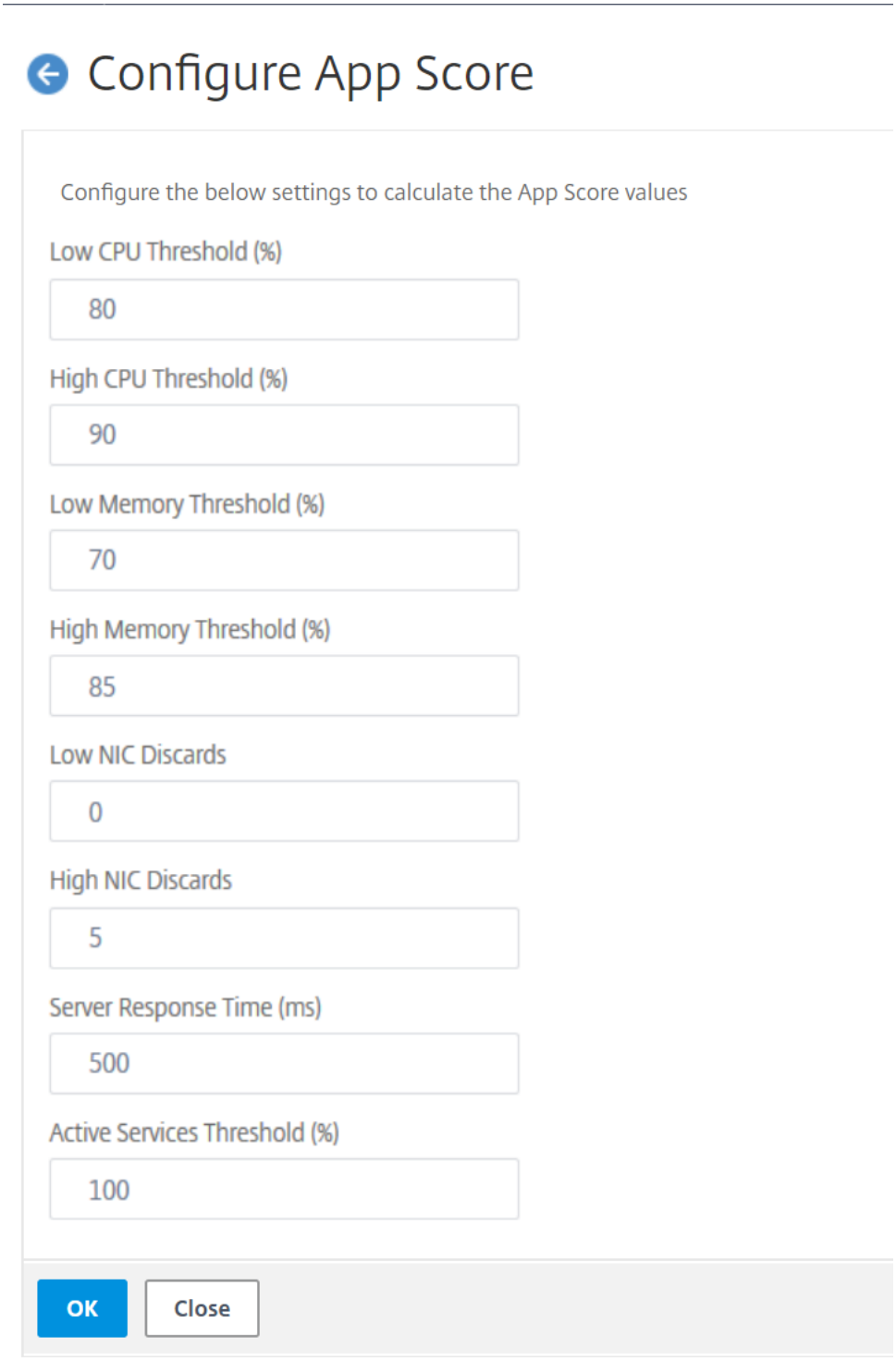
    d) **Hoher Speicherschwellenwert**. Der höhere Schwellenwert der Gesamtspeicherauslastung in der NetScaler ADC-Instanz.

    e) **Low NIC verwirft SLA**. Der untere Schwellenwert der Pakete, die von den Schnittstellen verworfen werden.

    f) **High NIC verwirft SLA**. Der höhere Schwellenwert der Pakete, die von den Schnittstellen verworfen werden.

    g) **Reaktionszeit**. Das Zeitintervall zwischen dem Senden eines Anforderungspakets und dem Empfangen des ersten Antwortpakets vom Dienst, der auf dem virtuellen Server konfiguriert ist. Der in Citrix ADM konfigurierte Standardwert beträgt 500 ms.

    h) **Schwellenwert für aktive Dienste**. Der Schwellenwert des Prozentsatzes der Dienste, die aktiv sein müssen, die an den virtuellen Server gebunden sind.



4. Klicken Sie auf **OK**.

Intelligente App Analytics

February 5, 2024

Intelligent App Analytics ermöglicht es Ihnen, Probleme mit der Anwendungsleistung mithilfe von maschinellem Lernen und regelbasierten Algorithmen zu identifizieren. Die Intelligent App Analytics-Funktion von NetScaler ADM:

- Bietet eine einfache und skalierbare Lösung für die Überwachung und Fehlerbehebung von Anwendungen, die über NetScaler ADC-Instanzen bereitgestellt werden.
- Überwacht alle Anwendungsebenen, um die Bearbeitungszeit für die Fehlerbehebung zu verkürzen und die Gesamtverfügbarkeit der Anwendung zu verbessern.

In einer typischen Bereitstellung erfüllen Tausende von Servern die Datenanforderungen der Benutzer. Der an diese Server gesendete Datenverkehr wird durch virtuelle Server ausgeglichen und von virtuellen Servern überwacht, die auf NetScaler ADC Appliances konfiguriert sind. Jeder virtuelle Server ist an mehrere Dienste gebunden, die die Backend-Server repräsentieren. In solchen Bereitstellungen hilft Ihnen die Intelligent App Analytics-Funktion:

- Überwachen, verwalten und treffen Sie Entscheidungen bei Ausfällen und anderen Ereignissen
- Überwachen der virtuellen Server und Dienste, die für eine Anwendung konfiguriert sind
- Zeigen Sie wichtige Informationen zu virtuellen Servern und Diensten an, sodass Sie die Konfigurationen nach Bedarf ändern können, um eine optimale Leistung der Anwendungen zu erzielen.

Wenn Sie die Serverfarm Ihrer Organisation skalieren, wird es schwierig, die Probleme zu verfolgen, die mit dem riesigen Datenverkehr auf den Servern verbunden sind, und sich auf die erforderlichen Problembehebungen zu beschränken.

Wenn eine Anwendung ausgeführt wird und eine große Menge an Datenverkehr empfängt, können verschiedene Probleme auftreten. **Sie können sich die Leistungsindikatoren für Anwendungsanalysen ansehen, indem Sie zu**Anwendungen**>**Dashboard**navigieren, eine Anwendung auswählen und nach unten scrollen, um die Probleme im Abschnitt Probleme zu sehen.**

Intelligente App-Analytics konfigurieren

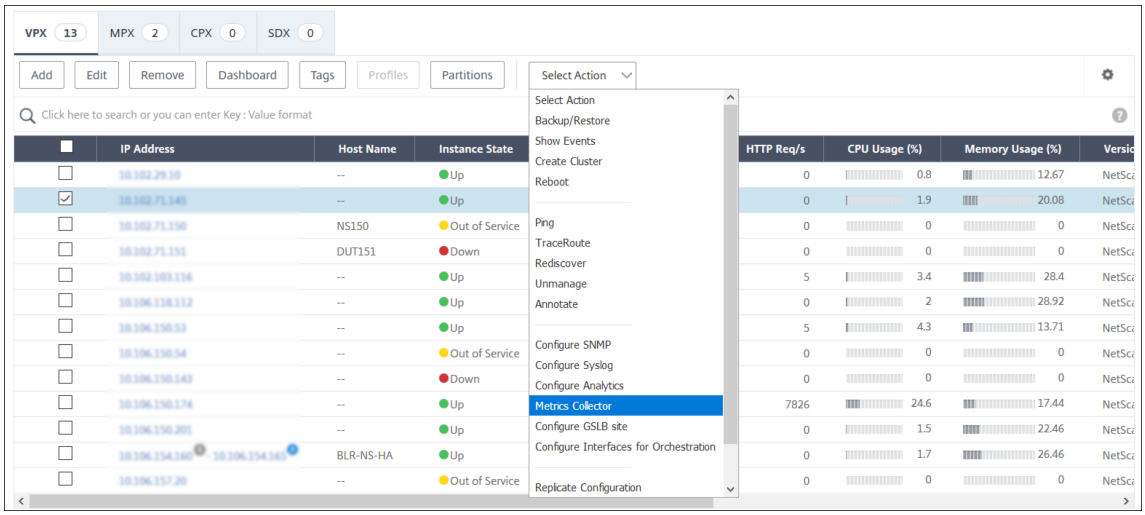
February 5, 2024

Die Funktion “Intelligent App Analytics”wird nur in **NetScaler ADC 12.1.50.x oder höher** unterstützt. **Metrics Collector** überträgt die NetScaler ADC-Leistungsindikatordaten an NetScaler ADM, das zur

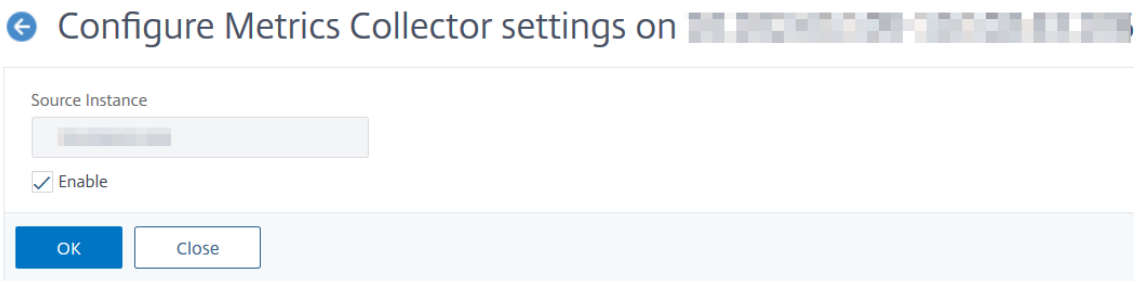
Erkennung von Anwendungsproblemen verwendet wird. Um die Funktion Intelligent App Analytics verwenden zu können, muss der **Metriksammler** für jede NetScaler ADC-Instanz konfiguriert werden. Standardmäßig ist **Metrics Collector** in Citrix ADC aktiviert, während Sie die Instanz zu Citrix ADM hinzufügen.

So stellen Sie sicher, dass **Metrics Collector** aktiviert ist:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**, und wählen Sie den Instanztyp aus, den Sie überwachen möchten (z. B. Citrix ADC VPX).
2. Wählen Sie die NetScaler ADC-Instanz aus.
3. Wählen Sie in der Liste **Aktion auswählen** die Option **Metriksammlung** aus.



4. Auf der **Einstellungsseite „Metrics Collector konfigurieren** “ist die Option **Aktivieren** standardmäßig ausgewählt. Wenn diese Option nicht ausgewählt ist, stellen Sie sicher, dass Sie die Option **Aktivieren** ausgewählt haben, und klicken Sie dann auf **OK**.



> **Hinweis**
>
> Um Anomalien für **Serverfehler** und deren **detaillierte Webtransaktion**anzuzeigen, müssen Sie die Analyse auf virtuellen Servern aktivieren.

Leistungsindikatoren für Anwendungsanalysen

February 5, 2024

Sie können die Leistungsindikatoren zusammen mit den Kategorien anzeigen, die in NetScaler ADC Webanwendungen vorkommen. Um diese Indikatoren anzuzeigen, müssen Sie sicherstellen, dass Sie Analytics und Metrik-Collector auf der ADC-Instanz aktivieren:

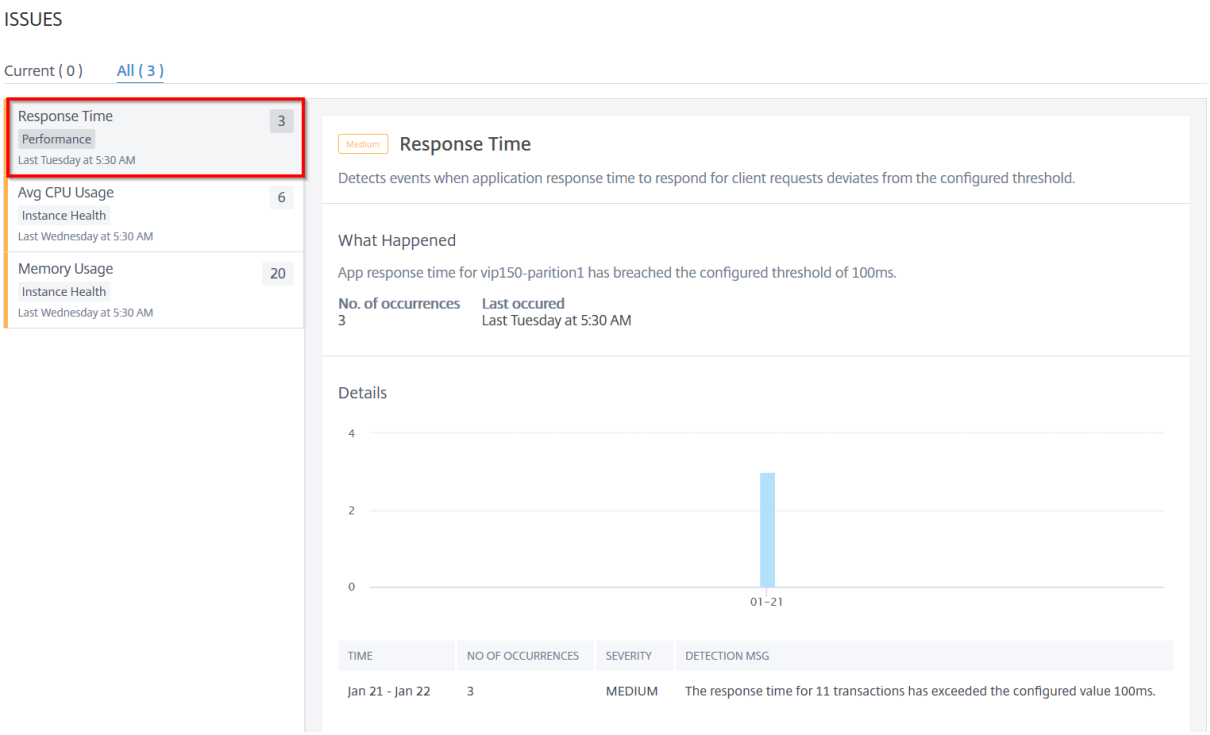
Nachdem Sie Analytics und Metriken Collector aktiviert haben, können Sie die folgenden Indikatoren anzeigen, indem Sie zu **Anwendungen** > **Dashboard**navigieren, eine Anwendung auswählen und zum Abschnitt **Probleme** nach unten scrollen:

- Reaktionszeit
- Aktive Dienste
- Durchschnittliche CPU-Auslastung
- Speichernutzung
- NIC-Karten-Sät
- Serviceklappen
- Geringe Wiederverwendung von Sitzungen
- Unsachgemäßer Persistenztyp
- Instabiler Server (5xx)
- SSL-Echtzeit-Traffic
- Ungewöhnlich große HTTP-Pakete
- Warteschlangenlimit für TCP-Wiederzusammenbau
- Aufbau von Überspannungswarteschlangen

Reaktionszeit

February 5, 2024

Dieses Problem erkennt, wenn die Antwortzeit der Anwendung zur Beantwortung von Clientanforderungen vom konfigurierten Schwellenwert abweicht. Klicken Sie auf die Registerkarte **Reaktionszeit**, um die Details zum Problem anzuzeigen.



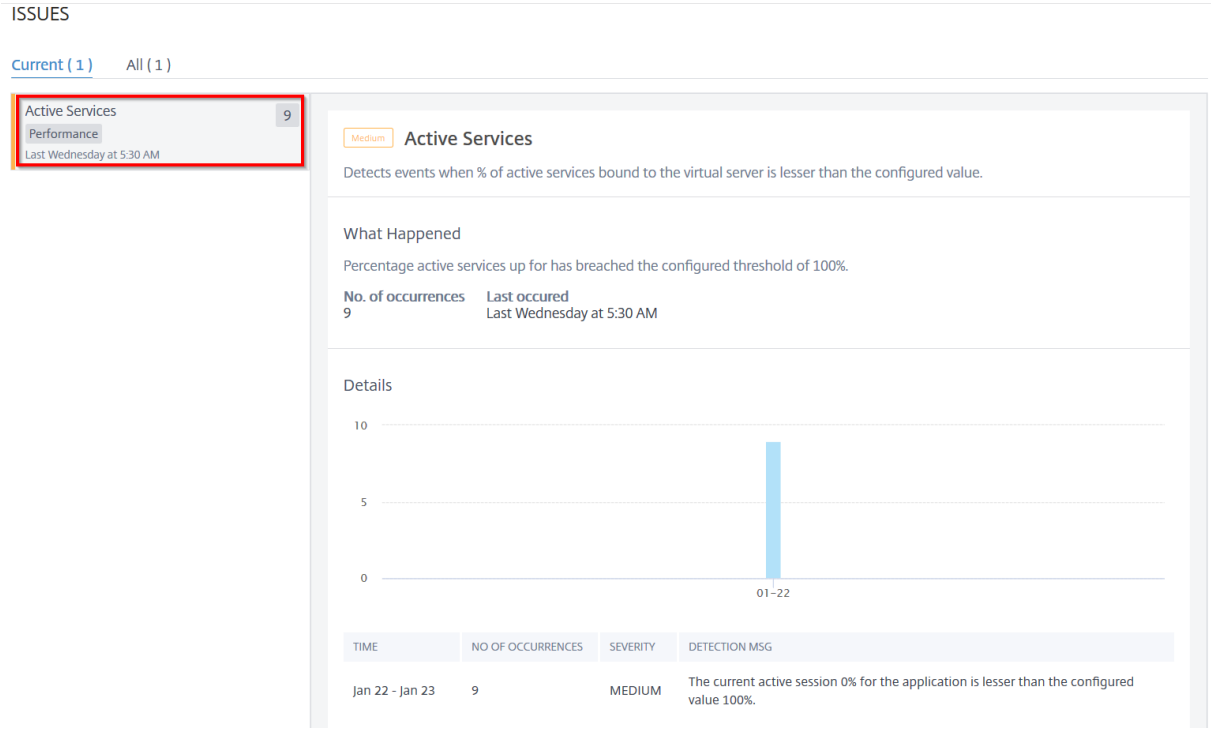
Unter **Details** können Sie Folgendes anzeigen:

- Das Diagramm, das die Gesamtzahl der Ereignisse für die ausgewählte Zeit anzeigt. Klicken Sie hier, um Filter anzuwenden und Details anzuzeigen
- Wenn das Problem aufgetreten ist
- Die Gesamtzahl der Vorkommen für die ausgewählte Zeit
- Der Schweregrad des Problems, z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die angibt, dass die gesamte Transaktionsantwortzeit den konfigurierten Schwellenwert überschreitet

Aktive Dienste

February 5, 2024

Dieses Problem erkennt, wenn der Prozentsatz der aktiven Dienste, die an den virtuellen Server gebunden sind, unter dem konfigurierten Schwellenwert liegt. Klicken Sie auf die Registerkarte **Aktive Dienste**, um die Details zum Problem anzuzeigen.



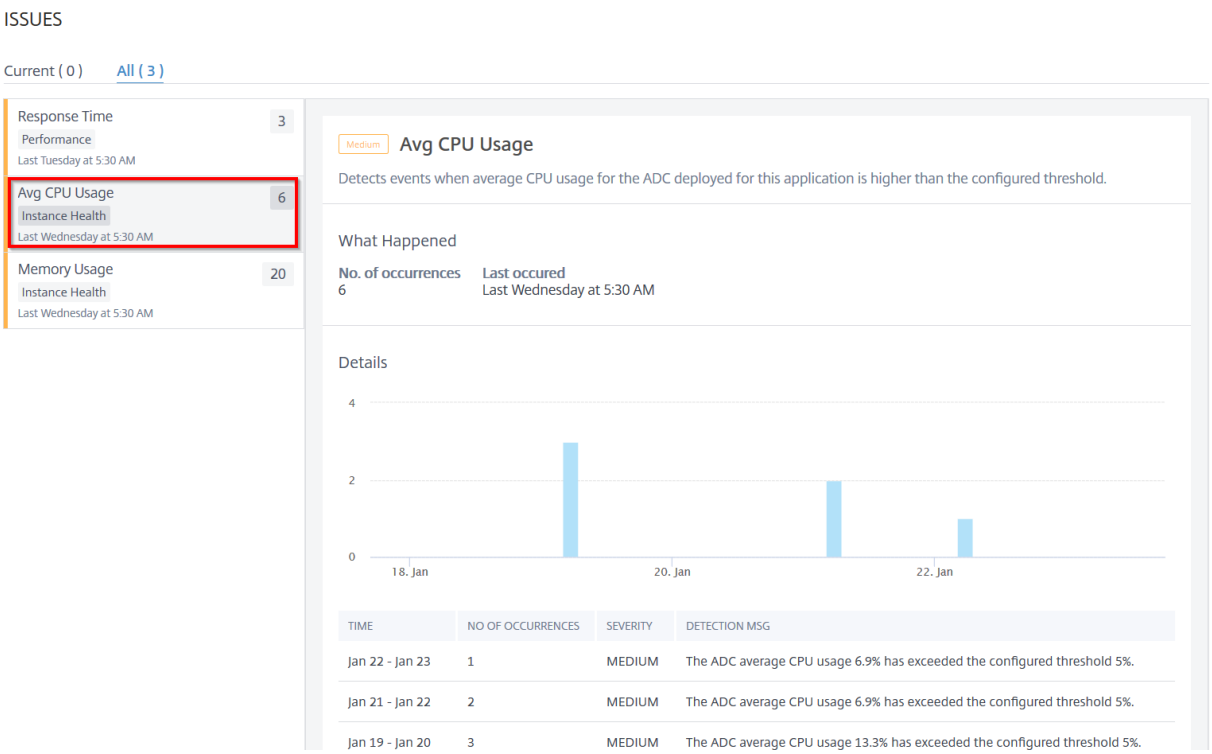
Unter **Details** können Sie Folgendes anzeigen:

- Das Diagramm, das die Gesamtzahl der Ereignisse für die ausgewählte Zeitdauer anzeigt. Klicken Sie hier, um Filter anzuwenden und Details anzuzeigen
- Wenn das Problem aufgetreten ist
- Die Gesamtzahl der Vorkommen für die ausgewählte Zeitdauer
- Der Schweregrad des Problems, z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die den Prozentsatz der aktiven Dienstsitzungen und den konfigurierten Schwellenwert angibt

Durchschnittliche CPU-Auslastung

February 5, 2024

Dieses Problem erkennt, wenn die ADC-CPU-Auslastung für diese Anwendung den konfigurierten Schwellenwert überschreitet. Klicken Sie auf die Registerkarte **Durchschnittliche CPU-Auslastung**, um die Problemdetails anzuzeigen.



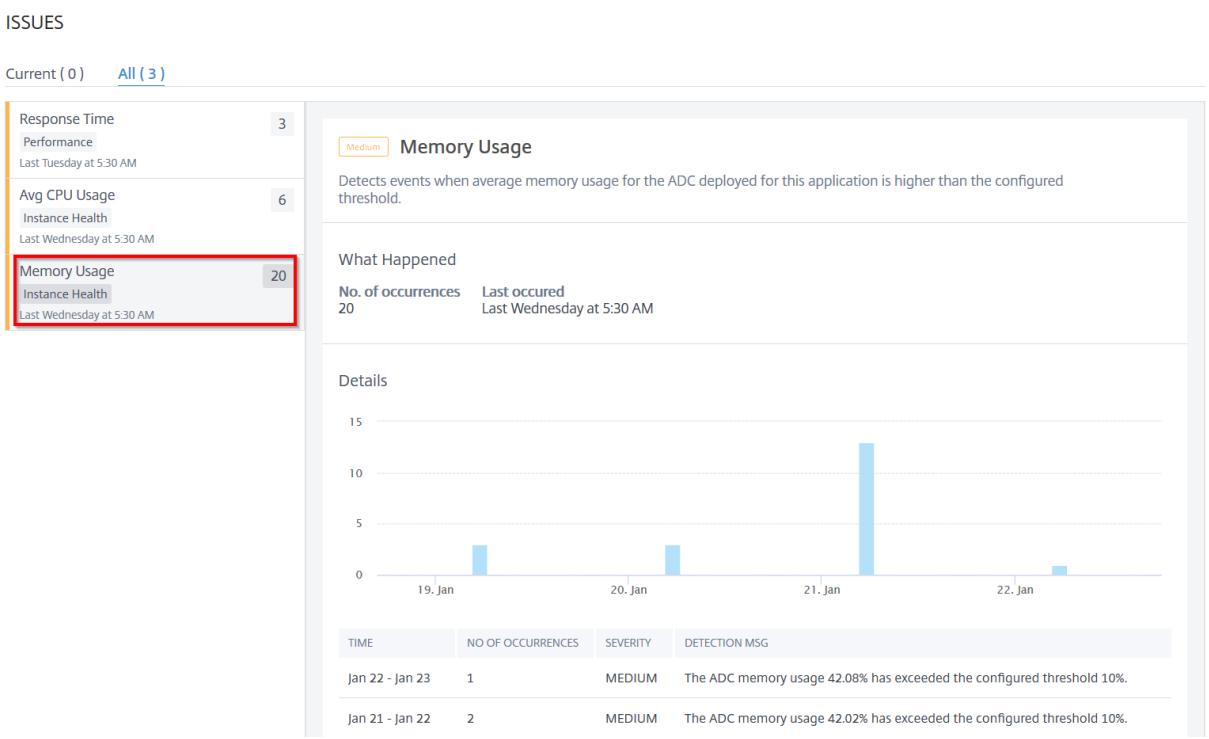
Unter **Details** können Sie Folgendes anzeigen:

- Das Diagramm, das die Gesamtzahl der Ereignisse für die ausgewählte Zeitdauer anzeigt. Klicken Sie hier, um Filter anzuwenden und Details anzuzeigen
- Wenn das Problem aufgetreten ist
- Die Gesamtzahl der Vorkommen für die ausgewählte Zeitdauer
- Der Schweregrad des Problems, z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die die durchschnittliche CPU-Auslastung% des ADC und den konfigurierten Schwellenwert angibt

Speichernutzung

February 5, 2024

Dieses Problem erkennt, wenn die ADC-Speicherauslastung für diese Anwendung den konfigurierten Schwellenwert überschreitet. Klicken Sie auf die Registerkarte **Speichernutzung**, um die Details zum Problem anzuzeigen.



Unter **Details** können Sie Folgendes anzeigen:

- Das Diagramm, das die Gesamtzahl der Ereignisse für die ausgewählte Zeitdauer anzeigt. Klicken Sie hier, um Filter anzuwenden und Details anzuzeigen
- Wenn das Problem aufgetreten ist
- Die Gesamtzahl der Vorkommen für die ausgewählte Zeitdauer
- Der Schweregrad des Problems, z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die die durchschnittliche ADC-Speicherauslastung in% und den konfigurierten Schwellenwert angibt

Serviceklappen

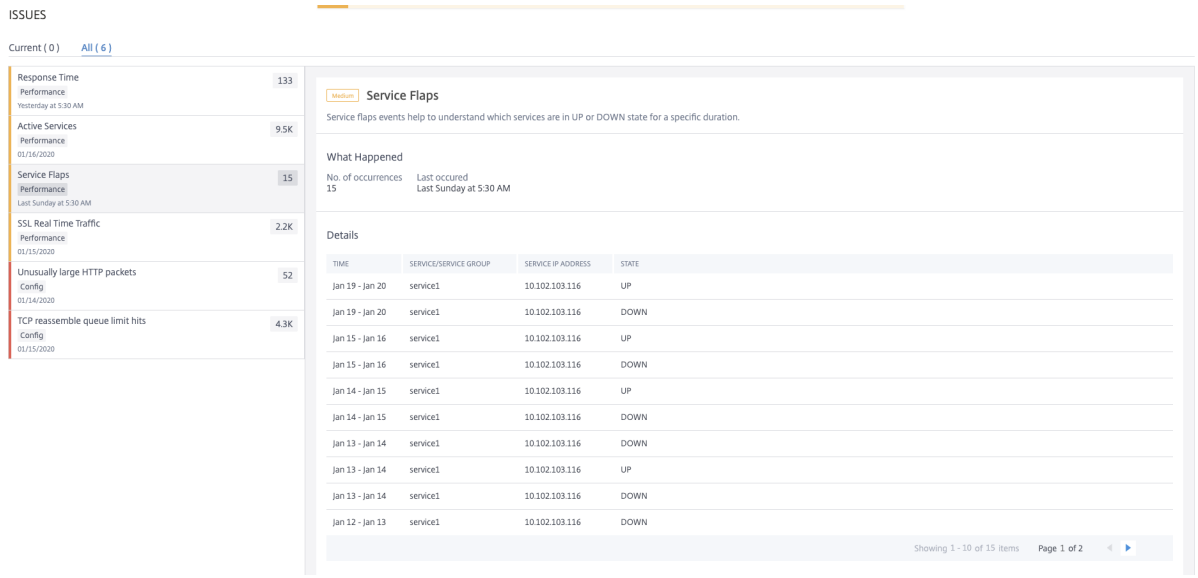
February 5, 2024

Als Netzwerkadministrator müssen Sie für eine optimale Verfügbarkeit der Anwendung sorgen. Bei Netzwerk- oder Konfigurationsproblemen können sich der Status und die Verfügbarkeit eines Anwendungsservers auf die Gesamtleistung auswirken.

Mithilfe der Service Flaps-Ereignisse können Sie die Anwendung identifizieren, bei der Probleme auftreten. Service Flaps Events helfen Ihnen auch dabei:

- Verstehen, welcher Dienst sich für eine bestimmte Dauer im DOWN-Status befindet
- Verstehen, wie viele Dienste sich für eine bestimmte Dauer im UP- oder DOWN-Status befinden

Klicken Sie auf die Registerkarte **Service Flaps**, um die Serviceklappen-Details anzuzeigen.



Sie können Details wie die Anzahl der Vorkommen und den Zeitpunkt des letzten Auftretens anzeigen.

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Serviceklappenanomalie auftrat
- Der Name der Dienst-/Dienstgruppe
- Die IP-Adresse des Dienstes
- Der aktuelle Dienststatus

Instabiler Server

February 5, 2024

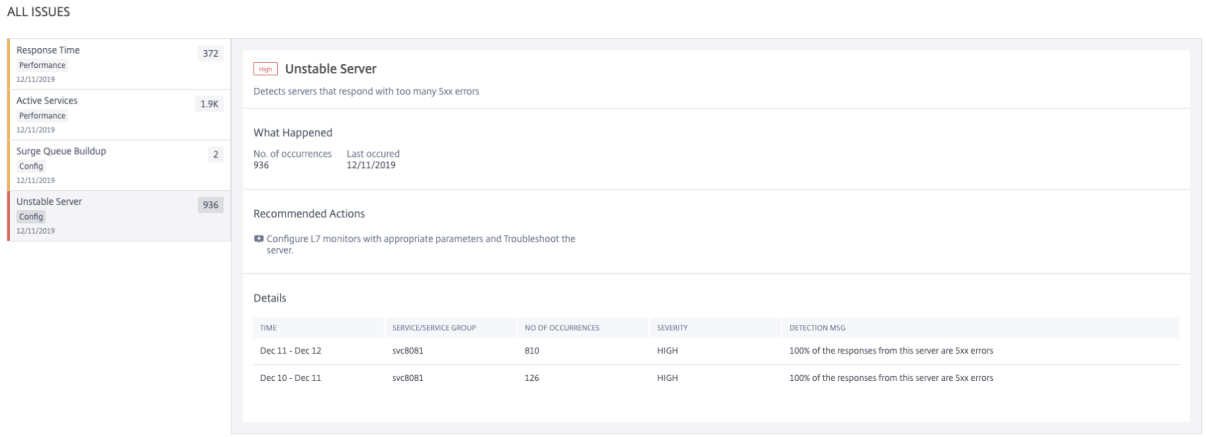
In einigen Szenarien antwortet der Webserver mit Statuscodes, wenn er die Anforderungen aus Gründen wie ungültigen Anforderungen, vorübergehender Überlastung oder Serverwartung nicht verarbeiten kann. Diese Fehler werden mit Fehlercodes angezeigt, die verschiedene Szenarien der Fehler definieren. Beispiel:

- **502 Schlechtes Gateway**
  Der Server agiert als Gateway oder Proxy und hat vom Upstream-Server eine ungültige Antwort erhalten.
- **503 Dienst nicht verfügbar**
  Der Server ist derzeit nicht verfügbar. Die Server sind möglicherweise wegen Wartungsarbeiten überlastet oder ausgefallen.
- **504 Gateway-Timeout**
  Der Server fungiert als Gateway oder Proxy und hat keine zeitnahe Antwort vom Upstream-Server erhalten.

Dies können vorübergehende Bedingungen sein, aber manchmal müssen Sie eine Korrekturmaßnahme auf den Webservern implementieren, um die Webseiten verfügbar zu machen.

Mithilfe des Indikators **Unstable Server** können Sie diese Fehler anzeigen und Entscheidungen über Korrekturmaßnahmen treffen, um die Probleme zu beheben und sicherzustellen, dass die Clientanforderungen erfüllt werden und die Webseiten immer verfügbar sind.

Wählen Sie die Registerkarte **Instabiler Server**, um die Details zum Problem anzuzeigen.



Die **empfohlenen Aktionen** zur Behebung des Problems sind:

- Konfigurieren Sie L7-Monitore mit entsprechenden Parametern für den Server, der mit 5xx-Fehlern reagiert. Ein Monitor ist eine Entität, die den Dienstzustand verfolgt. Die Appliance überprüft regelmäßig die Server mithilfe des Monitors, der an jeden Dienst gebunden ist. Wenn ein Server nicht innerhalb eines angegebenen Antwort-Timeouts antwortet und die angegebenen Tests fehlschlagen, wird der Dienst als DOWN markiert. Anschließend führt die Appliance den Lastausgleich unter den verbleibenden Diensten durch. Weitere Informationen zum Konfigurieren eines Monitors finden Sie unter Benutzerdefinierte Monitore
- Problembehandlung beim Server

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die instabile Serveranomalie auftrat
- Der Name der Dienst-/Dienstgruppe
- Gesamtvorkommen
- Schweregrad der Anomalie, z. B. hoch, niedrig und mittel
- Die Erkennungsnachricht, die% der Antworten dieses Dienstes angibt, die 5xx-Fehler meldet

Ausführliche Informationen zur Webtransaktion mit Serverfehlern finden Sie unter Webtransaktionsanalyse für Serverfehler

Aufbau der Sitzung

February 5, 2024

Für alle gesicherten Transaktionen führt Citrix ADC den SSL-Abladungsprozess für die erste Transaktion durch und speichert dann die SSL-Sitzung basierend auf der Konfiguration der **Sitzungswiederverwendung**.

Basierend auf der Datenverkehrsrate kann der Sitzungsaufbau über einen bestimmten Zeitraum erfolgen, was dazu führen kann, dass in diesen Sitzungen in Citrix ADC eine große Menge an Speicher gehalten wird.

Sitzungsaufbauereignisse warnen die Administratoren und stellen empfohlene Aktionen zur Behebung dieses Ereignisses bereit. Klicken Sie auf den Tab **Session Buildup**, um die Problemdetails einzusehen.

Unter **Details** können Sie Folgendes anzeigen:

- Der Zeitpunkt, zu dem die Anomalie beim Sitzungsaufbau aufgetreten ist
- Der Name des virtuellen Servers
- Schweregrad der Anomalie, z. B. hoch, niedrig und mittel
- Die Meldung, die angibt, dass **X** SSL-Sitzungen auf dem virtuellen Server verfügbar sind und dass derzeit innerhalb der konfigurierten Timeout-Sitzung **Y** von SSL-Handshakes pro Sekunde vorhanden sind.

Die **empfohlene Aktion** zur Behebung dieser Anomalie besteht darin, entweder das Sitzungszeitlimit zu reduzieren oder die Wiederverwendung der Sitzung zu deaktivieren. Weitere Informationen finden Sie unter Sitzungs-Timeout.

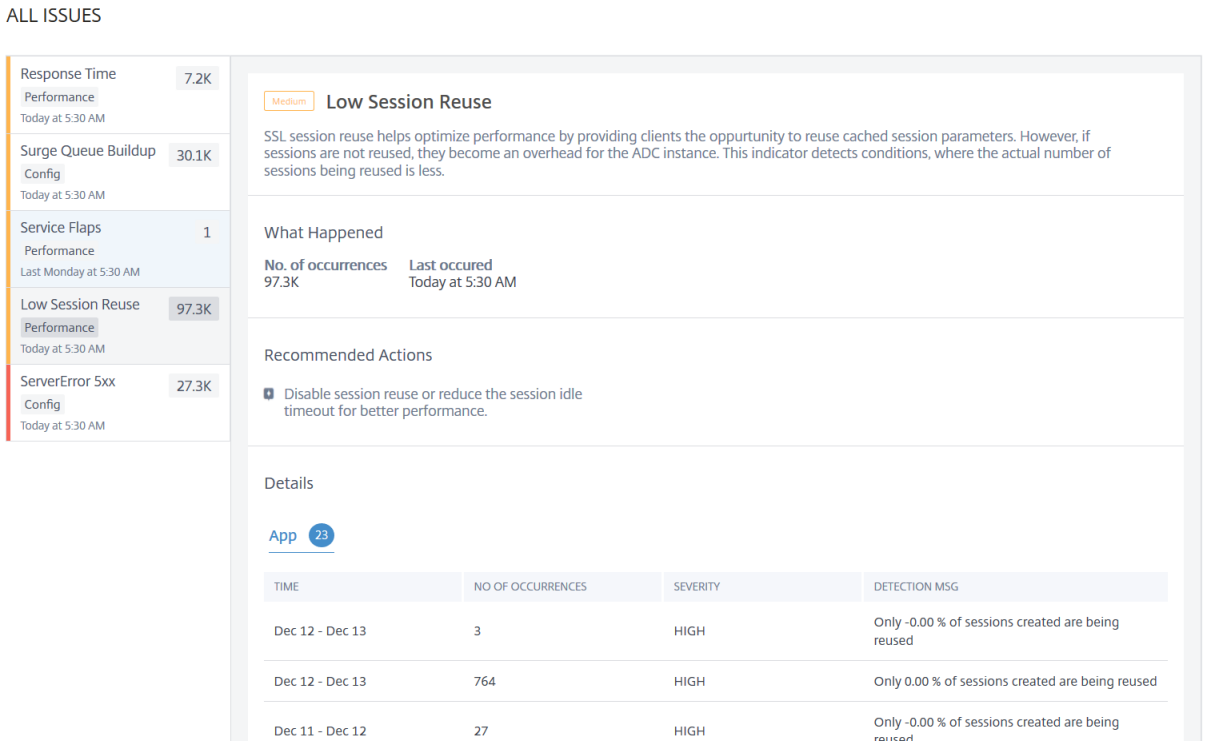
Wiederverwendung der niedrigen Sitzung

February 5, 2024

NetScaler ADC-Instanzen verarbeiten SSL-Transaktionen, indem sie den SSL-Handshake-Prozess vom Server auslagern. Nach Erhalt der Antwort vom Server schließt die NetScaler ADC-Instanz die sichere Transaktion mit dem Client ab. Unter Verwendung der zwischengespeicherten Sitzungsparameter schließt die NetScaler ADC-Instanz den SSL-Handshake-Prozess für die aufeinanderfolgenden Anforderungen ab.

Wenn diese Sitzungen nicht wiederverwendet werden, werden sie zu einem Overhead für die NetScaler ADC-Instanzen. Anhand des Indikators **Niedrige Sitzungswiederverwendung** können Sie feststellen, ob die tatsächliche Anzahl der wiederverwendeten Sitzungen geringer ist.

Klicken Sie auf die Registerkarte **Wiederverwendung bei geringer Sitzungsdauer**, um Details zum Problem anzuzeigen



Die **empfohlene Aktion** zur Behebung des Problems besteht darin, entweder die Wiederverwendung der Sitzung zu deaktivieren oder das Sitzungstimeout zu reduzieren. Weitere Informationen finden Sie unter Wiederverwendung von Sitzungen.

Unter **Details** können Sie Folgendes anzeigen:

- Gesamtzahl der Anwendungen mit geringer Wiederverwendung von Sitzungen

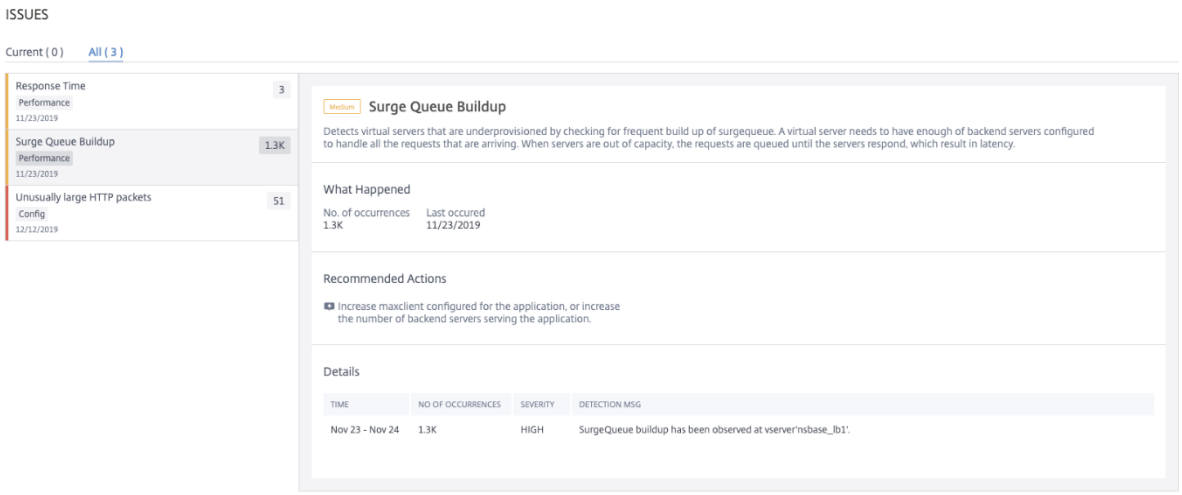
- Die Zeit, in der die geringe Anomalie der Sitzungswiederverwendung aufgetreten
- Gesamtvorkommen
- Schweregrad der Anomalie, z. B. hoch, niedrig und mittel
- Die Erkennungsmeldung zeigt an, dass nur% der konfigurierten Sitzungen wiederverwendet werden

Aufbau von Überspannungswarteschlangen

February 5, 2024

Wenn ein Server eine Flut von Anfragen empfängt, reagiert der Server langsam auf die Clients. Oft führt die Überlastung auch dazu, dass Clients Fehlerseiten erhalten. Für einen virtuellen Server müssen genügend Back-End-Server konfiguriert sein, um die eingehenden Anforderungen zu bearbeiten.

Mit dem Indikator **Surge Queue Buildup** können Sie die virtuellen Server anzeigen, die Surge Queue Buildup haben. Klicken Sie auf die Registerkarte **Surge Queue Buildup**, um die Problemdetails anzuzeigen.



Die **empfohlenen Aktionen** zur Behebung des Problems sind:

- Erhöhen Sie die Anzahl der Clientverbindungen. Weitere Informationen finden Sie unter Festlegen eines Limits für die Anzahl der Clientverbindungen.
- Erhöhen Sie die Back-End-Server, um die Anwendungsanforderungen zu bedienen

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Anomalie beim Aufbau der Surge-Warteschlange

- Gesamtvorkommen
- Schweregrad der Anomalie, z. B. hoch, niedrig und mittel
- Die Erkennungsmeldung, die den Aufbau der Überspannungswarteschlange auf dem virtuellen Server

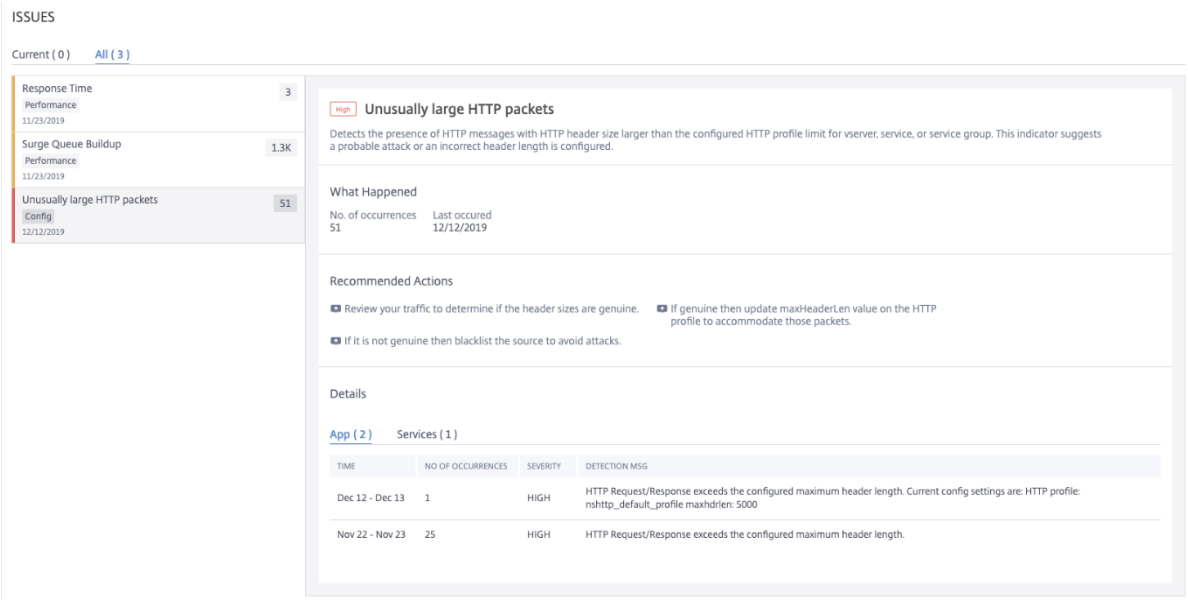
Ungewöhnlich große HTTP-Pakete

February 5, 2024

Eine HTTP-Transaktion verwendet Anforderungs-Antwort-Nachrichten zwischen dem Client und dem Server. In den Anforderungs- und Antwortmeldungen sind HTTP-Header die Werte, die im HTTP-Protokoll angezeigt werden. Sie können die Länge des HTTP-Headers in einem virtuellen Server, Dienst oder einer Dienstgruppe konfigurieren, um 4xx-Fehler zu vermeiden

Wenn eine HTTP-Anforderung/Antwort die maximale Header-Länge überschreitet, kann dies ein möglicher Angriff sein. Mit dem Indikator **Ungewöhnlich große HTTP-Pakete** können Sie die Vorkommen anzeigen, bei denen die HTTP-Nachrichten mit HTTP-Headergröße die konfigurierten Werte überschreiten.

Klicken Sie auf die Registerkarte **Ungewöhnlich große HTTP-Pakete**, um die Problemdetails anzuzeigen.



Die **empfohlenen Aktionen** zur Behebung des Problems sind:

- Überprüfen Sie den Datenverkehr, um festzustellen, ob die Headergröße echt ist Wenn die

Header-Größe echt ist, aktualisieren Sie den Header-Wert im HTTP-Profil. Weitere Informationen finden Sie unter Prüfung des Pufferüberlaufs.

- Wenn die Header-Größe nicht echt ist, listet Block die Quelle auf, um Angriffe zu vermeiden.

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Anomalie auftrat
- Gesamtvorkommen
- Schweregrad der Anomalie, z. B. hoch, niedrig und mittel
- Die Erkennungsmeldung, die die aktuelle HTTP-Headerlänge angibt, die auf dem virtuellen Server, Server oder der Dienstgruppe konfiguriert ist

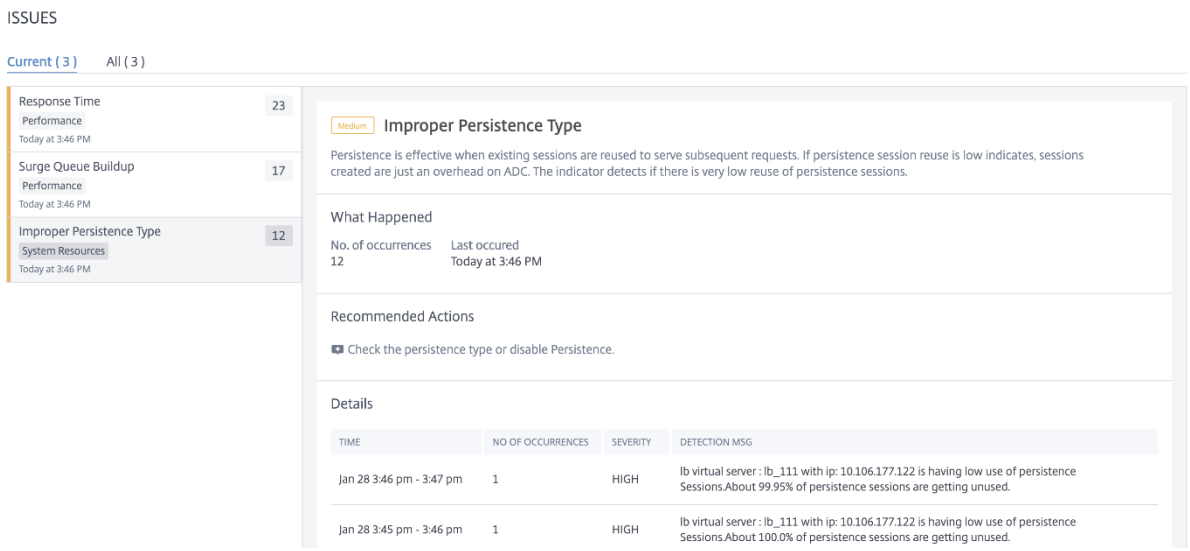
Unsachgemäßer Persistenztyp

February 5, 2024

Sie müssen die Persistenz auf einem virtuellen Server konfigurieren, wenn Sie den Status der Verbindungen auf den Servern beibehalten möchten, die durch diesen virtuellen Server dargestellt werden (z. B. Verbindungen, die im E-Commerce verwendet werden). Die Appliance verwendet dann die konfigurierte Lastausgleichsmethode für die erste Serverauswahl, leitet jedoch alle nachfolgenden Anfragen von demselben Client an denselben Server weiter.

Persistenz ist wirksam, wenn bestehende Sitzungen wiederverwendet werden, um nachfolgende Anforderungen zu bearbeiten. Wenn die Wiederverwendung von Persistenzsitzungen gering ist, sind Sitzungen, die auf ADC erstellt wurden, nur ein Overhead.

Mit dem Indikator **Unsachgemäßer Persistenztyp** können Sie feststellen, ob die Persistenzauslastung auf einem virtuellen Server gering ist. Klicken Sie auf die Registerkarte **Unsachgemäßer Persistenztyp**, um die Problemdetails anzuzeigen.



Die **empfohlene Aktion** zur Behebung des Problems besteht darin, den Persistenztyp zu überprüfen oder die Persistenz zu deaktivieren. Weitere Informationen finden Sie unter Persistenzeinstellungen.

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Anomalie auftrat
- Gesamtvorkommen
- Schweregrad der Anomalie, z. B. hoch, niedrig und mittel
- Die Erkennungsmeldung, die den Prozentsatz der nicht verwendeten Sitzungen angibt

TCP-Reassemble-Queue-Limittreffer

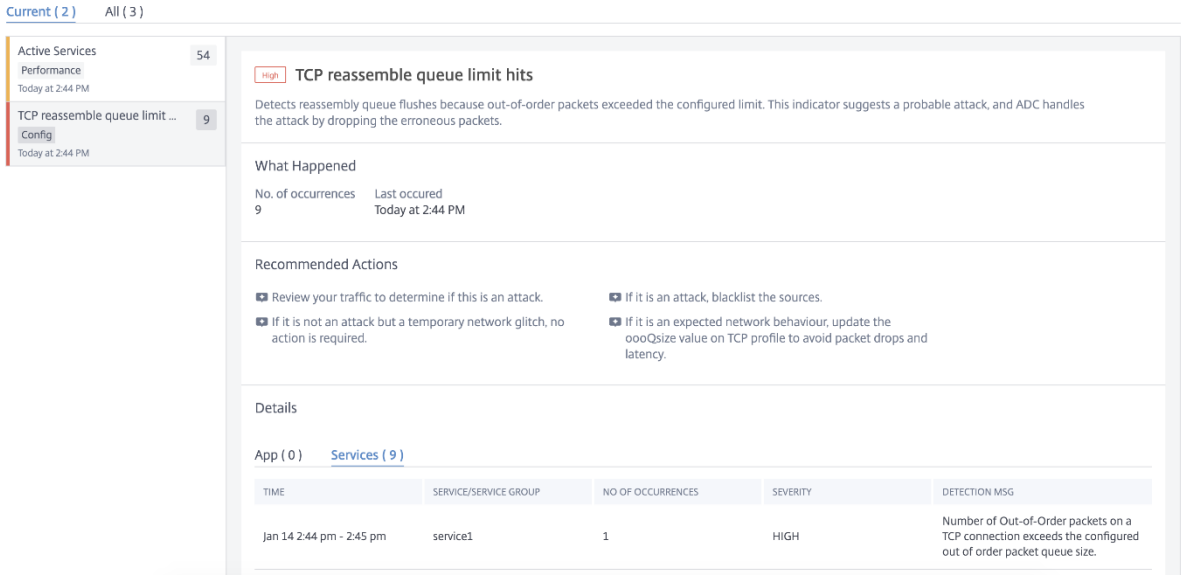
February 5, 2024

TCP unterhält eine Warteschlange außerhalb der Bestellung, um die OOO-Pakete in der TCP-Kommunikation zu halten. Diese Einstellung wirkt sich auf den NetScaler ADC Speicher aus, wenn die Warteschlangengröße lang ist, wie die Pakete im Laufzeitspeicher aufbewahrt werden müssen.

Diese Warteschlangengröße muss basierend auf den Netzwerk- und Anwendungsmerkmalen auf einem optimierten Niveau sein.

Mit dem Indikator **TCP reassemble queue limit hits** können Sie anzeigen, ob die Out-of-Order-Pakete auf einer TCP-Verbindung die konfigurierte Paketwarteschlangengröße außerhalb der Reihenfolge überschreiten.

Klicken Sie auf die Registerkarte **TCP-Warteschlangenlimit wieder zusammensetzen**, um die Problemdetails anzuzeigen.



Die **empfohlenen Aktionen** zur Behebung des Problems sind:

- Überprüfen Sie den Datenverkehr und blockieren Sie die Quelle, wenn es sich um einen Angriff handelt
- Wenn es sich bei diesem Verhalten um ein erwartetes Netzwerkverhalten handelt, aktualisieren Sie den Wert der Paketgröße außerhalb der Reihenfolge im TCP-Profil. Weitere Informationen finden Sie unter TCP-Optimierung
- Wenn es sich nur um einen temporären Netzwerk-Fehler handelt, ist keine weitere Aktion erforderlich

Unter **Details** können Sie Folgendes anzeigen:

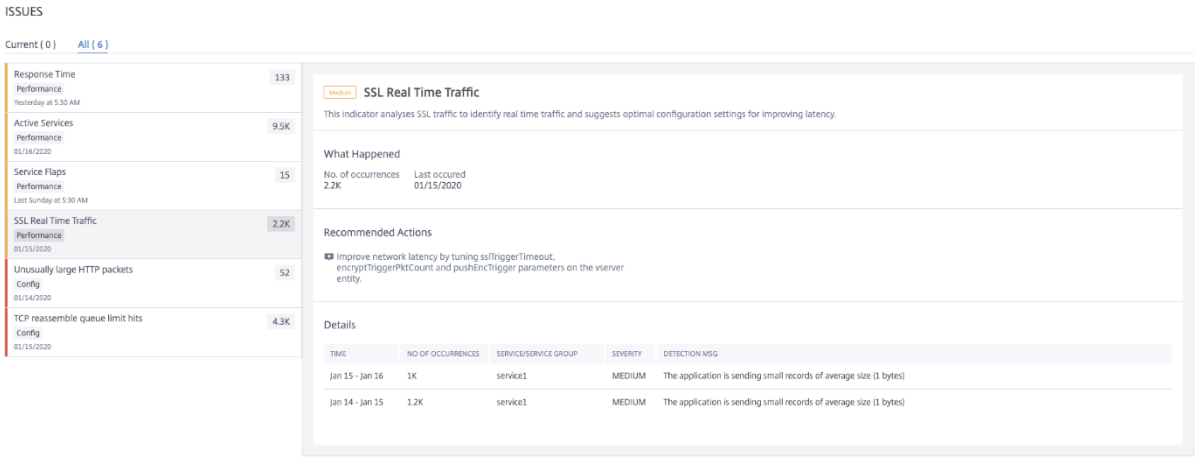
- Die Zeit, zu der die Anomalie auftrat
- Gesamtvorkommen
- Schweregrad der Anomalie, z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die das aktuelle TCP-Profil und die oooQSize-Einstellungen

SSL-Echtzeit-Traffic

February 5, 2024

In der NetScaler ADC-Instanz können Sie ein SSL-Profil für die Verarbeitung von SSL-Datenverkehr verwenden. Das SSL-Profil umfasst bestimmte SSL-Parameter für virtuelle Server, Dienste und Dienstgruppen. Der Indikator **SSL Real Time Traffic** analysiert den SSL-Datenverkehr, um Echtzeitverkehr zu identifizieren, und schlägt optimale Konfigurationseinstellungen zur Verbesserung der Latenz vor.

Klicken Sie auf die Registerkarte **SSL-Echtzeitverkehr**, um die Details zum Problem anzuzeigen.



Die **empfohlene Aktion** zur Behebung des Problems besteht darin, die Netzwerklatenz durch Aktualisieren von SSL-Parametern zu verbessern. Weitere Informationen finden Sie unter Globale SSL-Parameter.

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Anomalie auftrat
- Der Name der Dienst-/Dienstgruppe
- Schweregrad der Anomalie, z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung mit der aktuellen Einstellung in der Anwendung

AnwendungsSicherheitsdashboard

February 5, 2024

Das **App Security-Dashboard** bietet Ihnen einen Überblick über die Sicherheitsmetriken für die entdeckten/lizenzierten Anwendungen. In diesem Dashboard werden die Sicherheitsangriffsinformationen für die erkannten/lizenzierten Anwendungen angezeigt, z. B. Sync-Angriffe, Small-Flod-Angriffe, DNS-Flood-Angriffe usw.

So zeigen Sie die Sicherheitsmetriken im App-Sicherheitsdashboard an:

1. Navigieren Sie zu **Anwendungen** > **App-Sicherheits-Dashboard**.
2. Wählen Sie die Instanz-IP-Adresse aus der Instanzliste aus.

   Die Berichte enthalten für jede Anwendung die folgenden Informationen:

   - **Bedrohungsindex**. Ein einstelliges Bewertungssystem, das die Kritikalität von Angriffen auf die Anwendung angibt. Je kritischer die Angriffe auf eine Anwendung sind, desto höher ist der Bedrohungsindex für diese Anwendung. Die Werte reichen von 1 bis 7.

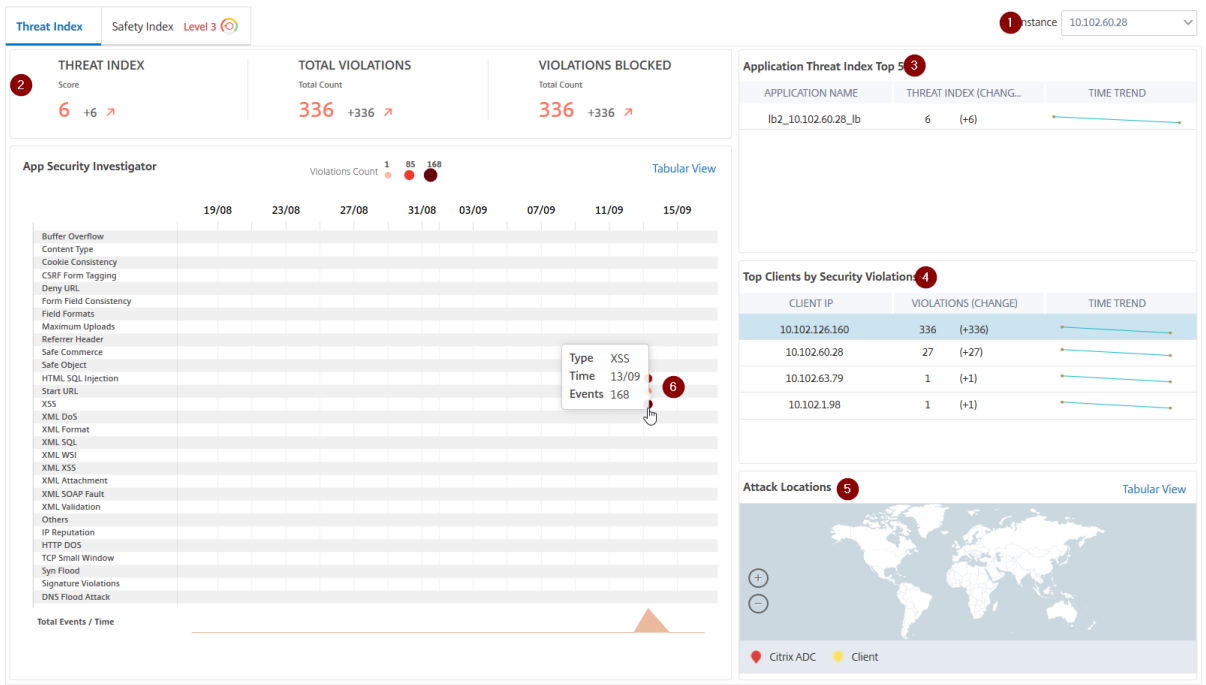
     Der Bedrohungsindex basiert auf Angriffsinformationen. Die angriffsbezogenen Informationen wie Verstoßtyp, Angriffskategorie, Standort und Client-Details geben einen Einblick in die Angriffe auf die Anwendung. Verstöße werden nur dann an NetScaler ADM gesendet, wenn eine Verletzung oder ein Angriff auftritt. Eine große Anzahl von Sicherheitslücken und Sicherheitslücken führt zu einem hohen Bedrohungsindexwert.

   - **Sicherheitsindex**. Ein einstelliges Bewertungssystem, das angibt, wie sicher Sie die NetScaler ADC-Instanzen zum Schutz von Anwendungen vor externen Bedrohungen und Sicherheitslücken konfiguriert haben. Je niedriger die Sicherheitsrisiken für eine Anwendung, desto höher der Sicherheitsindex. Die Werte reichen von 1 bis 7.

     Der Sicherheitsindex berücksichtigt sowohl die Konfiguration der Anwendungsfirewall als auch die Sicherheitskonfiguration des NetScaler ADC -Systems. Für einen hohen Sicherheitsindex müssen beide Konfigurationen stark sein. Wenn beispielsweise strenge Prüfungen der Anwendungsfirewall vorhanden sind, aber Sicherheitsmaßnahmen für NetScaler ADC-Systeme, z. B. ein sicheres Kennwort für den `nsroot` Benutzer, nicht bereitgestellt werden, wird Anwendungen ein niedriger Sicherheitsindexwert zugewiesen.

Sie können die im **App Security Investigator**gemeldeten Diskrepanzen einsehen.

Bedrohungsindizes



1 - Zeigt die IP-Adresse der NetScaler ADC-Instanz an, für die Sie Details anzeigen können.

2 —Zeigt Details wie den Bedrohungsindex, die Gesamtzahl der aufgetretenen Verstöße und die Gesamtzahl der blockierten Verstöße an.

3 - Zeigt den virtuellen Server der ausgewählten Instanz an.

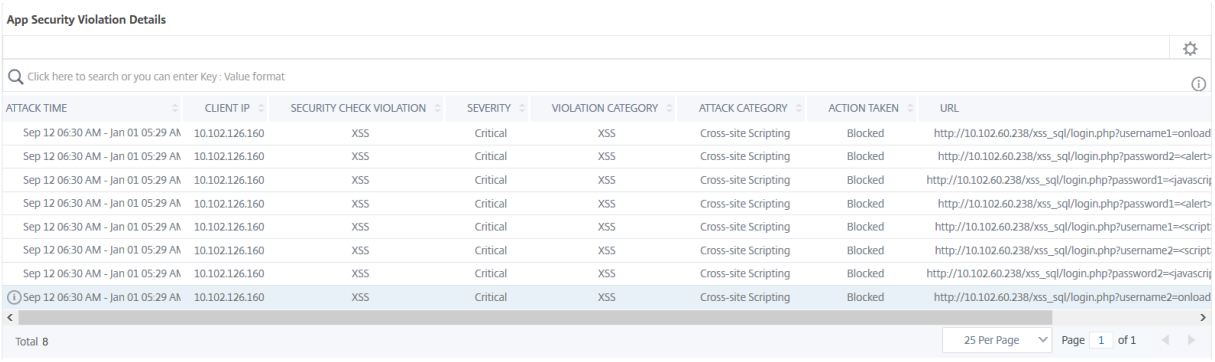
4 - Zeigt die Sicherheitsverletzungen basierend auf Clients an. Das Diagramm App Security Investigator wird für jeden Client angezeigt. Sie können auf jede Client-IP klicken, um die Ergebnisse anzuzeigen.

5 - Zeigt die Verstöße in Kartenansicht und Tabellenansicht an.

6 - Zeigt die Details des Verstoßes an. Wenn Sie den Mauszeiger auf das Diagramm bewegen, werden die Details wie Verletzungstyp, Zeitpunkt des Angriffs und Gesamtereignisse angezeigt.

Wenn Sie auf ein Blasendiagramm klicken, werden die Details auf der Seite **Details zu App-Sicherheitsverletzungen** angezeigt. Wenn Sie beispielsweise weitere Details für Cross-Site-Scripting (Cross-Site-Skript) anzeigen möchten, klicken Sie auf das Diagramm, das für **XSS** in **App Security Investigator**ausgefüllt ist.

Die **Details zu App-Sicherheitsverletzungen** werden mit Verstoßdetails wie Angriffszeit, Angriffskategorie, Schweregrad, URL usw. angezeigt.



Sie können auch auf die Option **Einstellungen** klicken, um die Optionen auszuwählen, die angezeigt werden sollen.

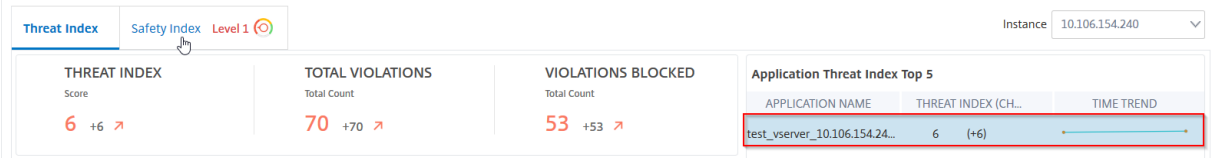
Sicherheitsindex Details

Nachdem Sie die Bedrohungsgefahr einer Anwendung überprüft haben, möchten Sie ermitteln, welche Anwendungssicherheitskonfigurationen vorhanden sind und welche Konfigurationen für diese Anwendung fehlen. Sie können diese Informationen erhalten, indem Sie einen Drilldown in die Zusammenfassung des Anwendungssicherheitsindex durchführen.

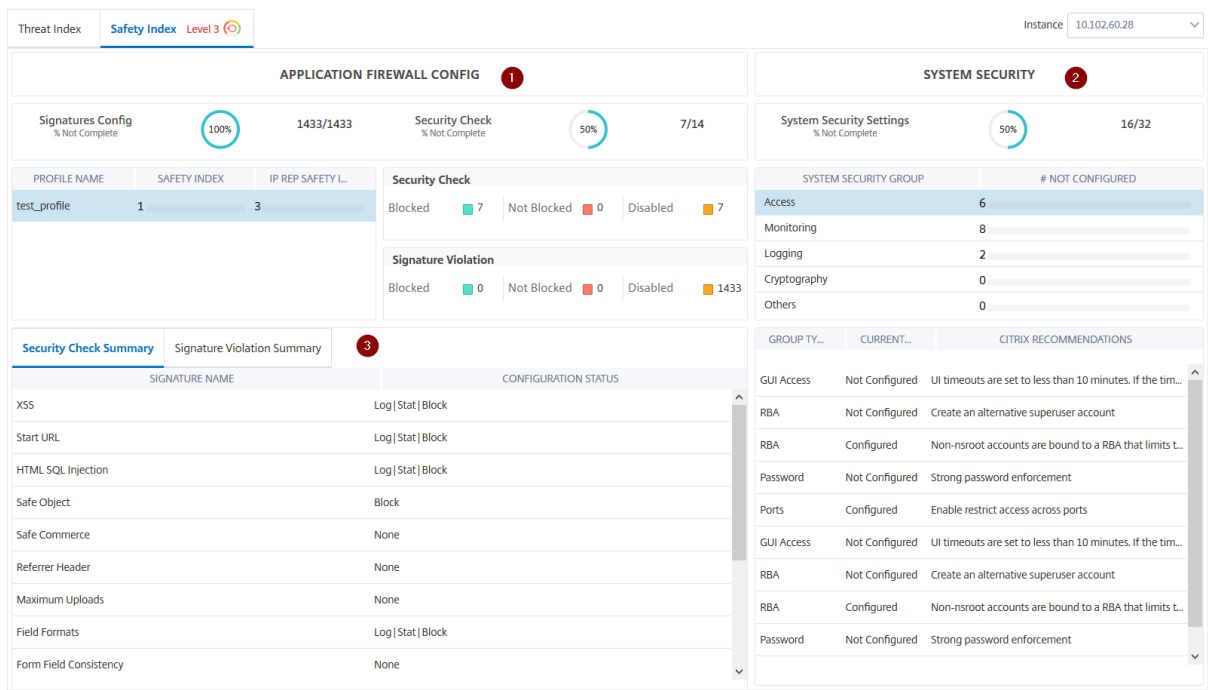
Die Zusammenfassung des Sicherheitsindex gibt Ihnen Informationen über die Wirksamkeit der folgenden Sicherheitskonfigurationen:

- **Konfiguration der Anwendungsfirewall**. Zeigt an, wie viele Signatur- und Sicherheitseinheiten nicht konfiguriert sind.
- **NetScaler ADM Systemsicherheit**. Zeigt an, wie viele Systemsicherheitseinstellungen nicht konfiguriert sind.

Um die Details des **Sicherheitsindex** anzuzeigen, wählen Sie einen virtuellen Server/eine Anwendung aus, und klicken Sie auf die Registerkarte **Sicherheitsindex**.



Die Details werden angezeigt.



1 - Zeigt die detaillierten Informationen für Anwendungs-Firewall-Konfigurationen an.

2 - Zeigt die detaillierten Informationen für Systemsicherheit an. Klicken Sie auf jede Sicherheitsgruppe, um Details zum aktuellen Status und zu den Empfehlungen von Citrix zu erhalten.

3 - Zeigt die Zusammenfassung für Sicherheitsprüfung und Signaturverletzung an.

Sie können auch eine Zusammenfassung der Bedrohungsumgebung anzeigen, indem Sie die Sicherheitsinformationen für virtuelle Server aktivieren und dann zu **Analytics** > **Security Insight**navigieren. Weitere Informationen zum Anwendungsfall des Sicherheitsindex finden Sie unter Sicherheitsinformationen

Service-Diagramm

February 5, 2024

Mit der Service Graph-Funktion in NetScaler ADM können Sie alle Dienste in einer grafischen Darstellung überwachen. Mit dieser Funktion können Sie auch eine detaillierte Analyse und umsetzbare Metriken der Services anzeigen. Sie können sich das Service-Diagramm ansehen für:

- Für alle NetScaler ADC-Instanzen konfigurierte Anwendungen
- Kubernetes-Anwendungen
- 3-stufige Webanwendungen

Dienstdiagramm für Anwendungen über alle NetScaler ADC-Instanzen hinweg

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

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

Navigieren Sie zu **Anwendungen > Service Graph** und klicken Sie auf die Registerkarte **Global**, um Folgendes anzuzeigen:

- End-to-End-Details aller Anwendungen, die vom Client zu Back-End-Servern verbunden sind
- Alle NetScaler ADC-Instanzen, die mit den jeweiligen Rechenzentren verbunden sind

  > **Hinweis**
  >
  > Sie können Rechenzentren nur anzeigen, wenn Sie über GSLB-Apps verfügen.

- Informationen zu den Kundenmetri
- Informationen zu den NetScaler ADC-Metriken
- Alle NetScaler ADC-Instanzen mit diskreten Anwendungen, benutzerdefinierten Anwendungen und diskreten Microservice-Anwendungen
- Die 4 Anwendungen mit niedriger Punktzahl, die zu benutzerdefinierten Apps, diskreten Apps und Microservices-Apps gehören
- Die Metrikinformationen für die vier besten virtuellen Server mit niedriger Bewertung
- Der Status von Anwendungen (separate Apps, benutzerdefinierte Apps und Microservices-Apps), z. B. **Kritisch**, **Überprüfen**, **Gut** und **Nicht anwendbar**.

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

Service-Diagramm für Kubernetes-Anwendungen

Navigieren Sie zu **Anwendungen > Service Graph** und klicken Sie auf die Registerkarte **Microservices**, um Folgendes anzuzeigen:

- Sicherstellung der Gesamtleistung der Anwendung durch End-to-End-Anwendung

- Identifizieren Sie Engpässe, die durch die wechselseitige Abhängigkeit verschiedener Komponenten Ihrer Anwendungen entstehen
- Sammeln Sie Einblicke in die Abhängigkeiten der verschiedenen Komponenten Ihrer Anwendungen
- Überwachen Sie Dienste innerhalb des Kubernetes-Clusters
- Überwachen Sie, welcher Dienst Probleme hat
- Prüfen Sie die Faktoren, die zu Leistungsproblemen beitragen
- Detaillierte Sichtbarkeit der HTTP-Transaktionen des Dienstes anzeigen
- Analysieren der HTTP-, TCP- und SSL-Metriken

Durch die Visualisierung dieser Metriken in NetScaler ADM können Sie die Ursache von Problemen analysieren und die erforderlichen Fehlerbehebungsaktionen schneller durchführen. Das Service-Diagramm zeigt Ihre Anwendungen in verschiedenen Komponentendiensten an. Diese Dienste, die innerhalb des Kubernetes-Clusters ausgeführt werden, können mit verschiedenen Komponenten innerhalb und außerhalb der Anwendung kommunizieren. Informationen zu den ersten Schritten finden Sie unter Service Graph einrichten.

Service-Diagramm für 3-Tier-Webanwendungen

Navigieren Sie zu **Anwendungen > Service Graph** und klicken Sie auf die Registerkarte **Web-Apps**, um Folgendes anzuzeigen:

- Details zur Konfiguration der Anwendung (mit dem virtueller Content Switching-Server und dem virtuellen Load Balancing-Server)

  Für GSLB-Anwendungen können Sie virtuelle Rechenzentrums-, ADC-Instanz-, CS- und LB-Server anzeigen.
- Ende-zu-Ende-Transaktionen vom Kunden zum Service
- Der Ort, von dem aus der Client auf die Anwendung zugreift
- Der Name des Rechenzentrums, in dem die Clientanforderungen verarbeitet werden, und die zugehörigen NetScaler ADC-Metriken des Rechenzentrums (nur für GSLB-Anwendungen)
- Metrikdetails für Client, Service und virtuelle Server
- Wenn die Fehler vom Kunden oder vom Dienst stammen
- Der Dienststatus wie "**Kritisch**", "**Überprüfung**"und "**Gut**". NetScaler ADM zeigt den Dienststatus basierend auf der Reaktionszeit des Dienstes und der Fehleranzahl an.
  - **Kritisch (rot)** —Zeigt an, wenn die durchschnittliche Reaktionszeit des Service > 200 ms UND Fehlerzähler > 0

  - **Überprüfung (orange)** —Zeigt an, wenn die durchschnittliche Reaktionszeit des Service > 200 ms ODER Fehlerzähler > 0
  - **Gut (grün)** —Zeigt keinen Fehler an und durchschnittliche Reaktionszeit < 200 ms

- Der Kundenstatus wie "**Kritisch**", "**Überprüfung**"und "**Gut**". NetScaler ADM zeigt den Clientstatus basierend auf der Latenz des Clientnetzwerks und der Fehleranzahl an.
  - **Kritisch (rot)**—Zeigt an, wenn die durchschnittliche Netzwerklatenz des Clients > 200 ms UND Fehleranzahl > 0
  - **Überprüfung (orange)** —Zeigt an, wenn die durchschnittliche Clientnetzwerklatenz > 200 ms ODER Fehlerzähler > 0
  - **Gut (grün)** —Zeigt keinen Fehler an und durchschnittliche Latenz des Client-Netzwerks < 200 ms

- Der Status des virtuellen Servers wie "**Kritisch**", "**Überprüfung**"und "**Gut**". NetScaler ADM zeigt den Status des virtuellen Servers basierend auf dem App-Score an.
  - **Kritisch (rot)** —Zeigt an, wenn der App-Wert < 40 ist
  - **Überprüfung (orange)** —Zeigt an, wenn der App-Score zwischen 40 und 75 liegt
  - **Gut (grün)** —Zeigt an, wenn der App-Score > 75 ist

Zu beachtenswerte Punkte:

- Nur virtuelle Server für Load Balancing, Content Switching und GSLB werden im Service-Diagramm angezeigt.
- Wenn kein virtueller Server an eine benutzerdefinierte Anwendung gebunden ist, sind die Details im Service-Diagramm für die Anwendung nicht sichtbar.
- Sie können Metriken für Clients und Services in Service Graph nur anzeigen, wenn aktive Transaktionen zwischen virtuellen Servern und Webanwendungen stattfinden.
- Wenn keine aktiven Transaktionen zwischen virtuellen Servern und Webanwendung verfügbar sind, können Sie nur Details im Dienstdiagramm anzeigen, die auf den Konfigurationsdaten wie virtuelle Server für Lastausgleich, Content Switching und GSLB sowie Dienste basieren.
- Wenn Änderungen in der Anwendungskonfiguration vorgenommen werden, kann es 10 Minuten dauern, bis sie im Service-Diagramm angezeigt werden.

Weitere Informationen finden Sie unter Service-Diagramm für Anwendungen.

Servicediagramm einrichten

February 5, 2024

Softwareanforderungen

Kubernetes-Distribution	Kubernetes-Version	Container-Netzwerkschnittstellen (CNI)	CBX Version	CIC-Version	NetScaler ADM-Version	NetScaler ADM Agent-Version
Open Source	v1.16.3	Flanell, Kattun oder Kanal	13.0—41.28 oder später	1.5.25 oder höher	13.0—47.22 oder höher	13.0—47.22 oder höher

Sie können den Kubernetes-Cluster mit verschiedenen Bereitstellungstopologien konfigurieren, und die folgende Tabelle enthält die Topologien, die in Service Graph unterstützt werden:

Topologie	In Service Graph unterstützt
Single-Tier or Unified ingress	Ja
Zweistufig	Ja
Cloud	Ja, aber der Cloud-Load-Balancer wird im Diagramm nicht angezeigt
Service Mesh lite	Ja
Service-Mesh	Ja
Dienstleistungen des Typs LoadBalancer	Nein
Dienste des Typs NodePort	Nein

Um das Setup-Dienstdiagramm in NetScaler ADM abzuschließen, klicken Sie auf den Topologie-Typ, den Sie für Ihren Kubernetes-Cluster konfiguriert haben, und führen Sie die genannten Verfahren aus:

- Einstufige oder einheitliche Ingress-Topologie
- Dual-Tier- oder Service Mesh Lite Topologie
- Service-Mesh-Topologie

> **Hinweis**
>
> Das Verfahren zum Einrichten des Servicegraphen für Dual-Tier- und Service-Mesh-Topologien bleibt gleich.

Voraussetzungen

Sie können Service-Graph in den folgenden Szenarien anzeigen:

- NetScaler ADM und Kubernetes clustern sich im selben Netzwerk (z. B. NetScaler ADM und Kubernetes-Cluster, die auf demselben Citrix Hypervisor gehostet werden).
- NetScaler ADM und Kubernetes Cluster in einem anderen Netzwerk. In diesem Szenario müssen Sie einen lokalen Agenten konfigurieren und den Agenten im Netzwerk registrieren, in dem der Kubernetes-Cluster gehostet wird.

Einstufige oder einheitliche Ingress-Topologie

Folgende Voraussetzungen müssen erfüllt sein:

- Kubernetes-Cluster mit Single-Tier- oder einheitlicher Ingress-Topologie konfiguriert.
- VPX-, MPX-, SDX-, BLX-Instanz in NetScaler ADM hinzugefügt und **Web Insight** aktiviert.
- Kubernetes-Cluster in NetScaler ADM hinzugefügt.

Dual-Tier- oder Service Mesh Lite Topologie

Folgende Voraussetzungen müssen erfüllt sein:

- Der Kubernetes-Cluster wurde mit einem der unterstützten Topologien konfiguriert.
- Konfigurierte statische Routen auf NetScaler ADM, um die Kommunikation zwischen NetScaler ADM und NetScaler ADC CPX zu ermöglichen.

  > **Hinweis**
  >
  > Sie können dieses Verfahren ignorieren, wenn Sie NetScaler ADM als Microservice im selben Cluster bereitgestellt haben.

- Die Beispielbereitstellungsdateien wurden aus dem GitHub-Repository heruntergeladen.
- Erforderliche Parameter in der CPX-YAML-Datei hinzugefügt, um eine erfolgreiche CPX-Registrierung bei Citrix ADM sicherzustellen.
- In NetScaler ADM wurde eine VPX-, MPX-, SDX- oder BLX-Instanz hinzugefügt.

- Der Kubernetes-Cluster wurde in NetScaler ADM hinzugefügt.
- Eine Microservice-Beispielanwendungwurde bereitgestellt.
- NetScaler ADC CPX bereitgestellt und CPX für ADM registriert (gilt nur für zweistufige Architektur)
- Automatische Auswahl virtueller Server aktiviert, um die virtuellen Server zu lizenzieren.
- Webtransaktions- und TCP-Transaktionseinstellungen für **Alle** aktiviert, damit der NetScaler ADM-Agent HTTP- und TCP-Transaktionen abrufen kann.
- Traffic an Microservices gesendet.

Service-Mesh-Topologie

Folgende Voraussetzungen müssen erfüllt sein:

- Die Kubernetes-Clusterversion `1.14.0` wurde mit einer der folgenden Service-Mesh-Topologien konfiguriert:
  - NetScaler ADC CPX als Sidecar-Proxy für Istio
  - NetScaler ADC als Ingress-Gateway für Istio

  Weitere Informationen finden Sie unter NetScaler ADC Istio Adapter-Bereitstellungsarchitektur.
- `admissionregistration.k8s.io/v1beta1` API aktiviert. Sie können die API überprüfen, indem Sie Folgendes verwenden:

  ```
  kubectl api-versions | grep admissionregistration.k8s.io/v1beta1
  ```

  Die folgende Ausgabe zeigt an, dass die API aktiviert ist:

  ```
  admissionregistration.k8s.io/v1beta1
  ```
- Istio installiert `istio v.1.3.0`.
- Helm Version 3.x installiert.
- Konfigurierte statische Routen auf NetScaler ADM, um die Kommunikation zwischen NetScaler ADM und NetScaler ADC CPX zu ermöglichen.

  > **Hinweis**
  >
  > Sie können dieses Verfahren ignorieren, wenn Sie NetScaler ADM Agent als Microservice im selben Cluster bereitgestellt haben.

- Die erforderlichen Parameter zum Füllen der Service-Mesh-Topologiedaten wurden konfiguriert.
- Eine Beispielanwendungwurde bereitgestellt.

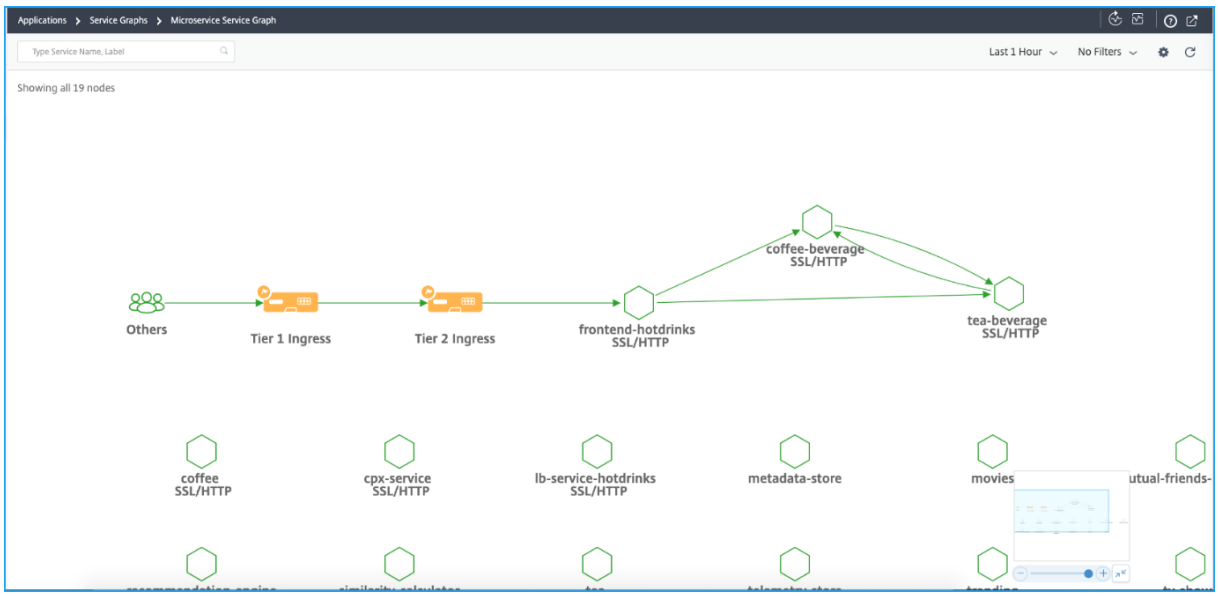
- Der Kubernetes-Cluster wurde in NetScaler ADM hinzugefügt.
- Automatische Auswahl virtueller Server aktiviert, um die virtuellen Server zu lizenzieren.
- Webtransaktions- und TCP-Transaktionseinstellungen für **Alle** aktiviert, damit der NetScaler ADM-Agent HTTP- und TCP-Transaktionen abrufen kann.
- Traffic an Microservices gesendet.

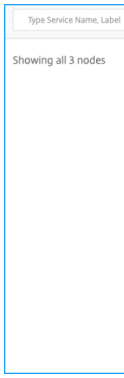
Details im Servicediagramm anzeigen

February 5, 2024

Navigieren Sie in NetScaler ADM zu **Application > Service Graphs > Kubernetes Service-Diagramm** und wählen Sie die Zeitdauer aus der Liste aus, um die Details des Servicegraphen anzuzeigen.

Mesh Lite Topologie mit zwei Tieren/Service | Single-Tie





- **Tier 1-Eintritt** —Citrix Ingress Controller innerhalb des Kubernetes-Clusters konfiguriert eine NetScaler ADC-Instanz (VPX/MPX/SDX/BLX) außerhalb des Kubernetes-Clusters.
- **Tier 2 Ingress** —Citrix Ingress Controller läuft zusammen mit der NetScaler ADC CPX-Instanz im Kubernetes-Cluster als Sidecar.
- **Ingress** —Wird für alle anderen Bereitstellungstopologien angezeigt.

Service-Diagramm-Dashboard

1 —End-to-End-Netzwerkzuordnung Ihrer Anwendung, die zeigt, wie Ihre Komponentendienste kommunizieren

2 —Grafik, die Treffer und Fehler für eine bestimmte Zeitdauer anzeigt

3 —Suchleiste für die Suche nach Diensten

4 —Zeitliste zur Auswahl der Zeitdauer

5 - Filter auf Anzeigedienste anwenden

6 —Einstellungssymbol

7 —Ansicht vergrößern und verkleinern

8 —Diagrammansicht oder tabellarische Ansicht

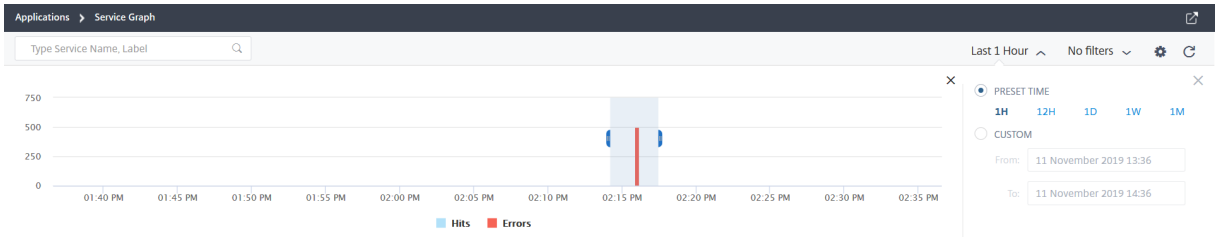
Basierend auf der gewählten Zeitdauer können Sie das Service-Diagramm anzeigen.

Service-Symbol	Beschreibung
	Die Kantenbreite gibt die Anzahl der Treffer an. Je größer oder mehr die Kantenbreite ist, gibt an, dass die Anzahl der Treffer höher ist.

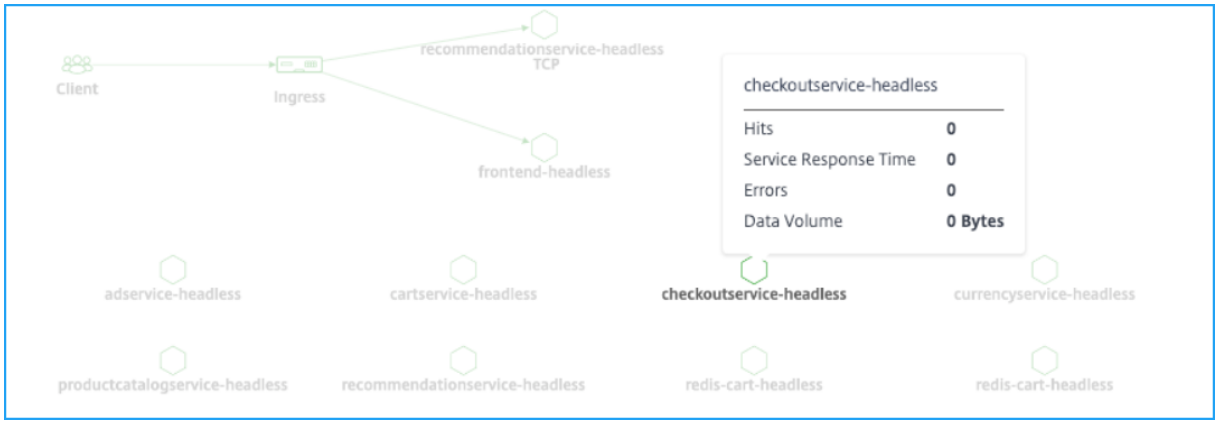
Service-Symbol	Beschreibung
	Der Dienst mit einem Warnsymbol zeigt an, dass der Dienst Fehler enthält.
	Der Dienst mit einem Stoppuhrsymbol zeigt an, dass der Dienst Latenz- oder Reaktionszeitprobleme aufweist.
	Der Dienst mit Stoppuhr- und Warnsymbolen weist darauf hin, dass der Dienst sowohl Fehler als auch Probleme mit Latenz-/Reaktionszeiten hat.

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

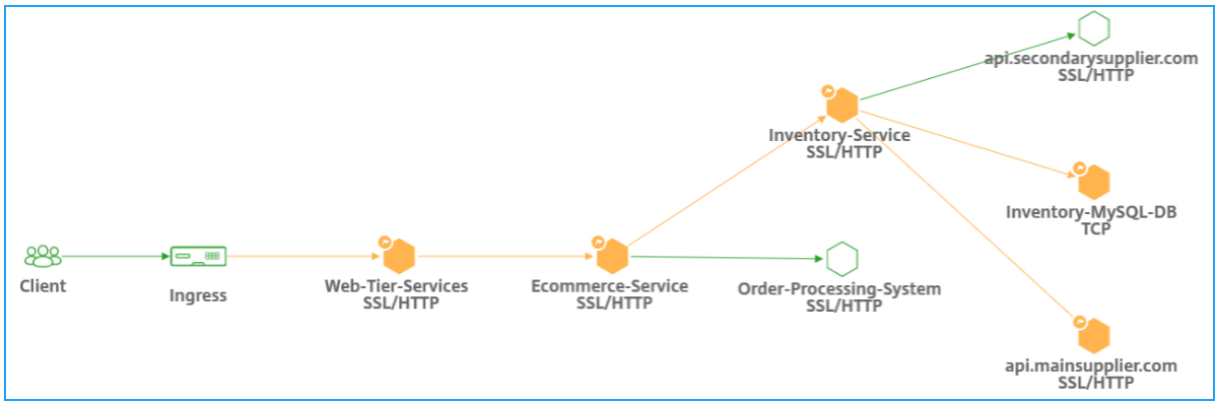
Basierend auf der gewählten Zeitdauer können Sie das Service-Diagramm anzeigen. Wählen Sie den Zeitraum aus dem Diagramm aus, der Treffer anzeigt, um weitere Informationen zu erhalten.



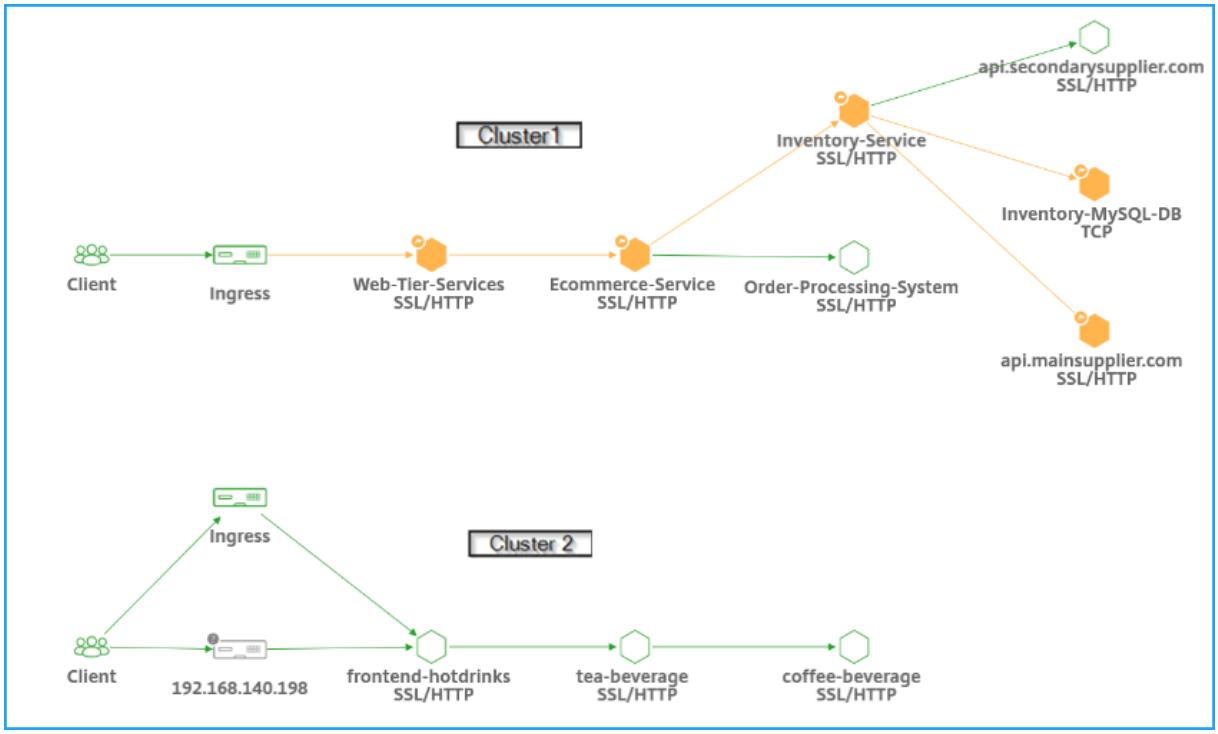
> **Hinweis**
>
> Wenn keine aktiven Transaktionen von NetScaler ADM empfangen werden, können Sie nur die Services anzeigen, die von der NetScaler ADC-Instanz mit Lastenausgleich ausgeglichen werden. Wenn Sie den Mauszeiger auf einen Dienst bewegen, werden alle Metriken als 0 angezeigt.



Das Servicediagramm wird mit dem von den Diensten verwendeten Protokoll angezeigt. Beachten Sie, dass in Ihrem Kubernetes-Cluster die folgenden Dienste ausgeführt werden, wie im Bild gezeigt:



> Hinweis
>
> Wenn Sie unter **Orchestration** > **Kubernetes** > Clusters mehrere Cluster hinzugefügt haben, können Sie die mit jedem **Cluster**verknüpften Dienste anzeigen.



Sie können den folgenden Status für Ihre Dienste anzeigen:

- **Kritisch (rot)** —Zeigt an, wenn die durchschnittliche Reaktionszeit des Service > 200 ms UND Fehlerzähler > 0
- **Überprüfung (orange)** —Zeigt an, wenn die durchschnittliche Reaktionszeit des Service > 200 ms ODER Fehlerzähler > 0
- **Gut (grün)** —Zeigt keinen Fehler an und durchschnittliche Reaktionszeit < 200 ms

Im Folgenden finden Sie Protokolle, mit denen Sie das Protokoll identifizieren können, das von einem Dienst verwendet wird:

- **TCP** —Zeigt an, dass der Dienst das TCP-Protokoll verwendet.
- **SSL, HTTP** —Zeigt an, dass der Dienst das SSL-über-HTTP-Protokoll verwendet.
- **SSL, TCP** —Zeigt an, dass der Dienst das SSL-über-TCP-Protokoll verwendet.

> **Hinweis**
>
> Der Dienst ohne Protokoll gibt an, dass der Dienst das HTTP-Protokoll verwendet.

Anzeigen wichtiger Metrikentrends mithilfe der tabellarischen Ansicht

Anhand der tabellarischen Ansicht können Sie Folgendes sehen:

- Die wichtigsten Kennzahlen für den Dienst

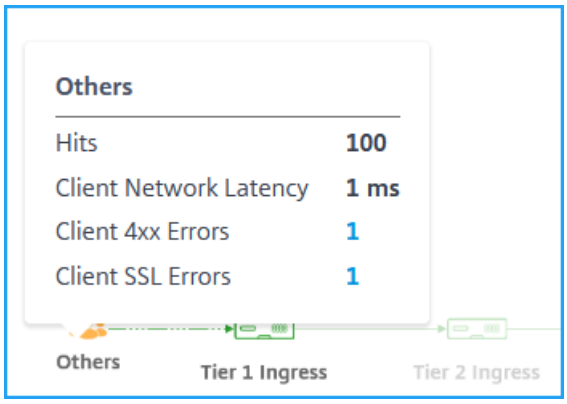
- Wichtige Metriken zwischen einem Quelldienst und einem Zieldienst

Als Administrator können Sie mithilfe dieser wichtigen Metriken die Trends der goldenen Signale für die ausgewählte Zeitdauer analysieren.

Client-Metriken anzeigen

Sie können sehen, von welchem Standort der Client auf den Dienst zugreift. Als Administrator können Sie die Client-Metriken visualisieren und die Probleme analysieren, die vom Kunden auftreten.

Bewegen Sie den Mauszeiger auf eine Client-Region, um die Metriken anzuzeigen.



- **Treffer** - Gibt die Gesamtzahl der Treffer an, die der Kunde erhalten hat.
- **Client-Netzwerklatenz** : Gibt die durchschnittliche Clientnetzwerklatenz an.
- **Client 4xx-Fehler** - Zeigt die Gesamtzahl der 4xx-Fehler des Clients an.
- **Client-SSL-Fehler** - Gibt die gesamte Client-SSL-Fehler an.

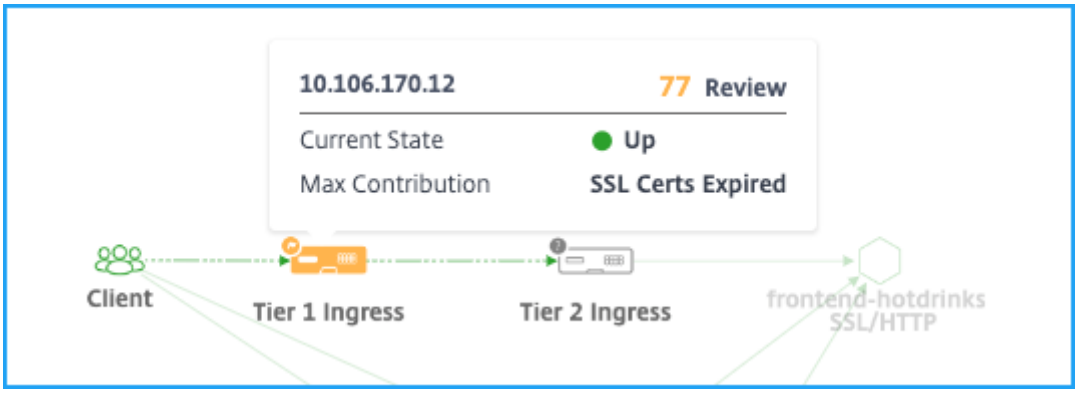
IP-Blöcke in NetScaler ADM - NetScaler ADM kann den Standort des Clients erkennen, wenn der Client eine öffentliche IP-Adresse verwendet. NetScaler ADM verfügt über eine integrierte CSV-Datei, die dem Speicherort basierend auf dem Client-IP-Adressbereich entspricht.

NetScaler ADM kann den Clientstandort mit privater IP-Adresse nur erkennen, wenn die IP-Adresse zum NetScaler ADM-Server hinzugefügt wird. Wenn die Client-IP-Adresse beispielsweise in einen privaten IP-Adressbereich fällt, der mit Stadt A verknüpft ist, erkennt NetScaler ADM, dass der Datenverkehr für diesen Client aus Stadt A stammt.

Weitere Informationen finden Sie unter Erstellen eines privaten IP-Blocks.

Anzeigen von Ingress-Metriken

Sie können die Art von Ingress anzeigen, die im Kubernetes-Cluster verwendet wird.



- NetScaler ADC IP-Adresse und seine Punktzahl
- **Aktueller Status** —Gibt an, ob die NetScaler ADC-Instanz Up, Down oder Out of Status ist
- **Maximaler Beitrag** —Zeigt das Problem an, das den Instanz-Score beeinflusst

Für die einstufige Topologie können Sie nur einen einzelnen **Ingress**anzeigen.

Klicken Sie auf den **Ingress**, um weitere Informationen zu erhalten. Weitere Informationen finden Sie unter Details zu eingehenden Daten zur Fehlerbehebunganzeigen.

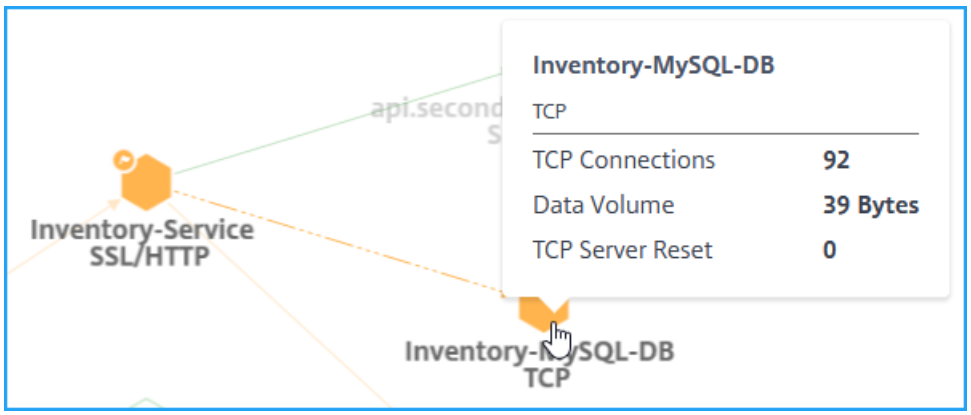
Anzeigen von TCP- und SSL-Metriken

Mit den TCP- und SSL-Metriken können Sie:

- TCP-Verbindungsdetails zwischen Diensten anzeigen
- Ermitteln, ob TCP-bezogene Probleme vom Quell- oder Zieldienst stammen
- Prüfen Sie, ob der SSL-Fehler vom Quell- oder Zieldienst stammt
- Zeigen Sie die von SSL-Diensten verwendete SSL-Protokollversion an

TCP-Messwerte

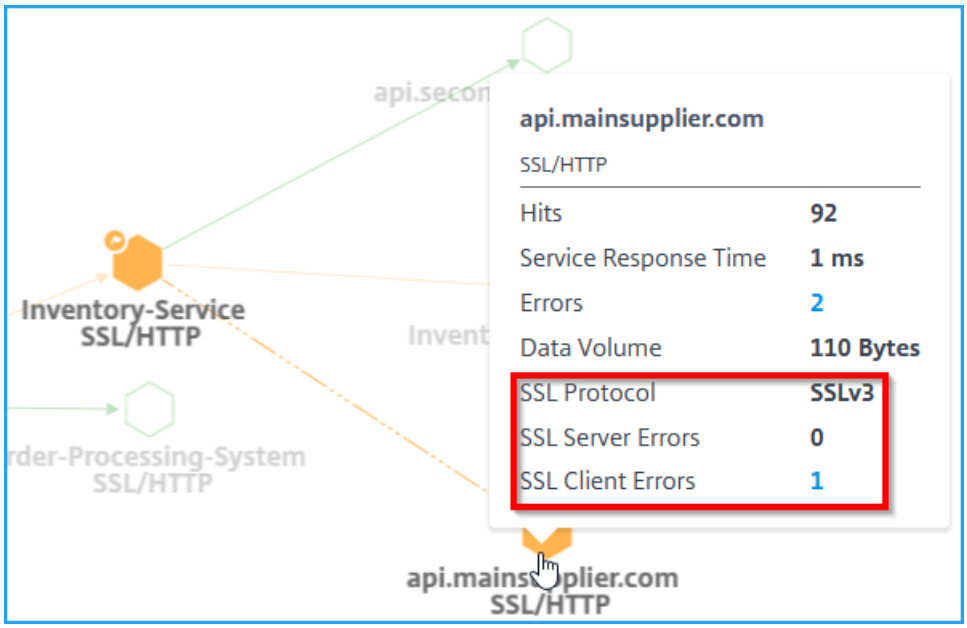
Bewegen Sie den Mauszeiger über einen TCP-Dienst oder den zugehörigen eingehenden Dienst, um die TCP-Metriken anzuzeigen.



- **TCP-Verbindungen** —Gesamtzahl der zwischen den Diensten hergestellten Verbindungen
- **Datenvolumen** —Gesamtmenge der vom Dienst verarbeiteten Daten
- **TCP-Serverrücksetzung** —Gesamtzahl der vom Server initiierten TCP-Resets

SSL-Metriken

Bewegen Sie den Mauszeiger auf einen Dienst, der das SSL-Protokoll verwendet, um die SSL-Metriken anzuzeigen.



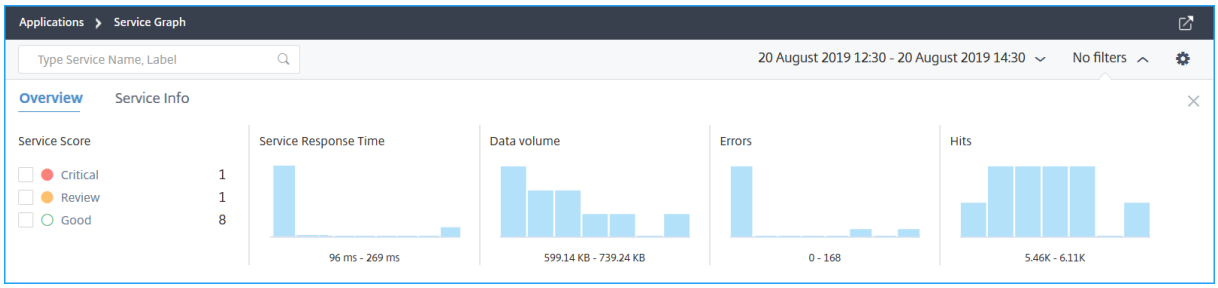
- **SSL-Serverfehler** —Zeigt die Gesamtzahl der SSL-Fehler vom Server an. (Beispiel: SSL-Zertifikat unbekannt)
- **SSL-Protokoll** —Gibt die vom Dienst verwendete SSL-Protokollversion an
- **SSL-Clientfehler** —Geben Sie die Gesamtzahl der SSL-Fehler des Clients an. (Beispiel: SSL-Clientauthentifizierungsfehler)

Servicedetails anzeigen

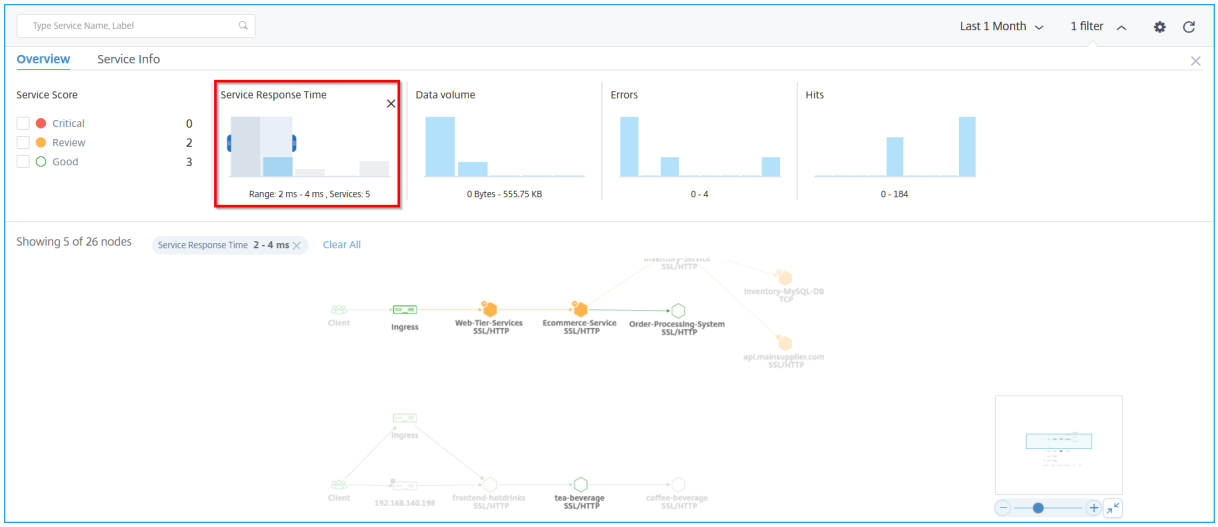
Klicken Sie auf einen Dienst und wählen Sie **Details anzeigen** aus, um die Servicedetails anzuzeigen. Weitere Informationen finden Sie unter Servicedetails anzeigen.

Filter anwenden

Sie können Filter anwenden, um bestimmte Serviceinformationen anzuzeigen. Klicken Sie auf Liste **Keine Filter**, um die Filteroptionen aufzurufen.

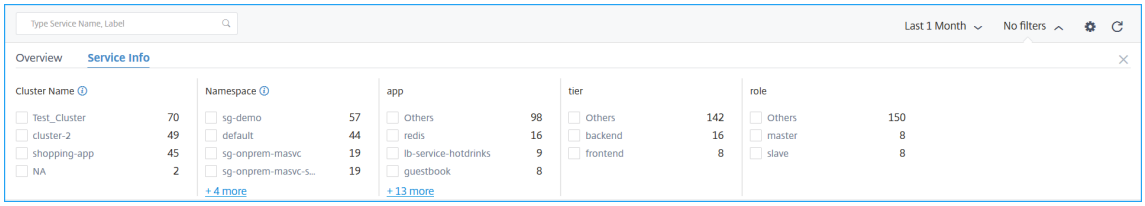


Wenn Sie beispielsweise Dienste mit einer Latenz von weniger als 150 ms anzeigen möchten, klicken Sie auf das Balkendiagramm unter **Service-Reaktionszeit**, um die Ergebnisse anzuzeigen.



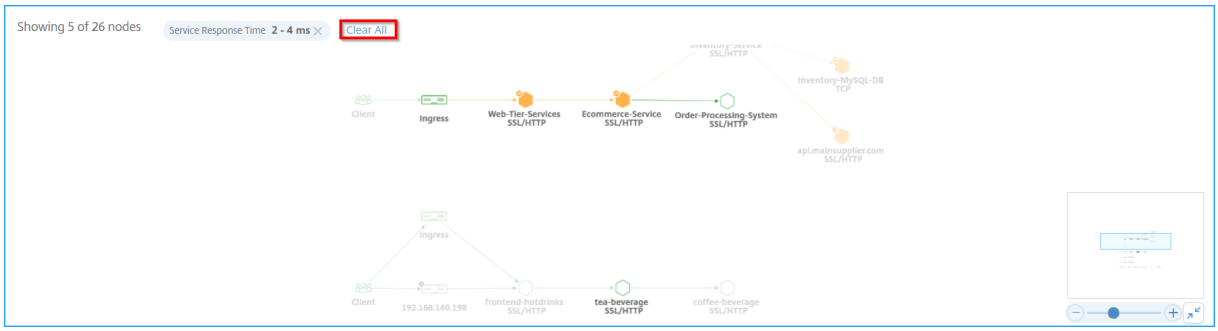
Klicken Sie auf **Service-Info**, um Filter auszuwählen und anzuwenden für:

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

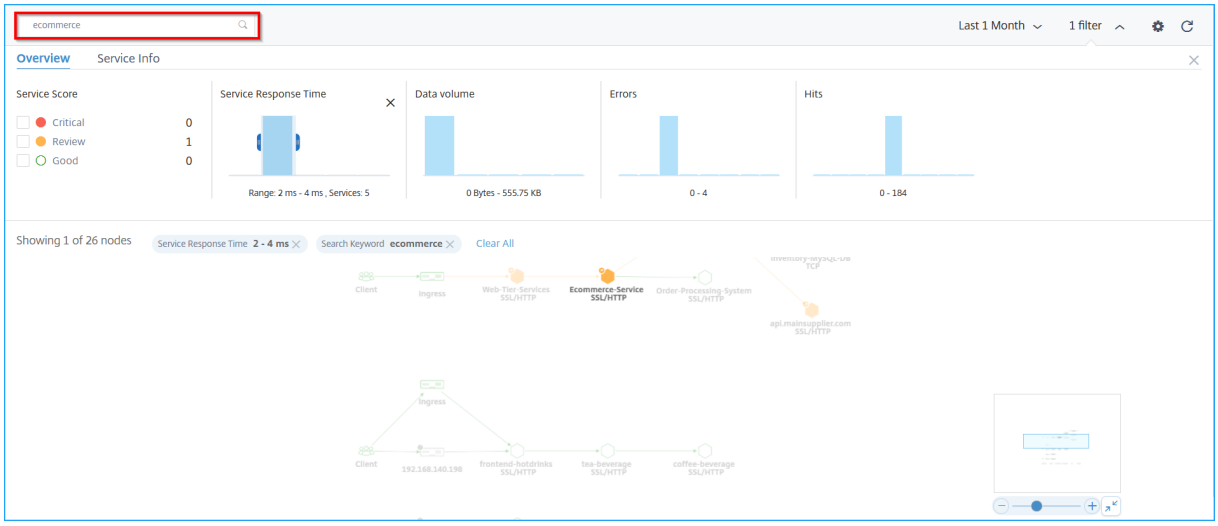


> Hinweis
>
> Abhängig von den in der Kubernetes Service-Definition YAML für den Dienst konfigurierten Labels können Sie auch weitere Filteroptionen anzeigen.

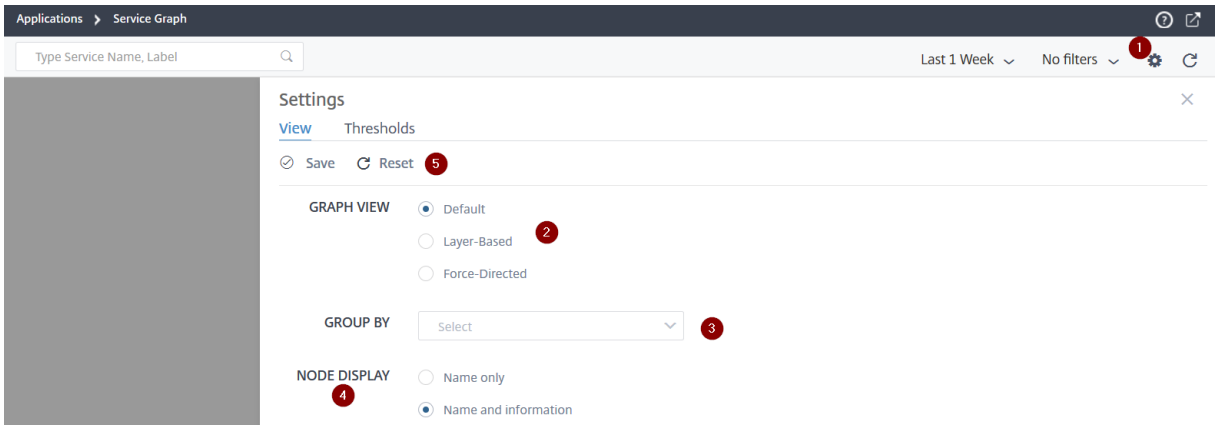
Klicken Sie auf **Alle löschen**, um alle Filter zu löschen.



Alternativ können Sie auch das Suchtextfeld verwenden und einen Servicenamen eingeben, um die Ergebnisse im Service-Graph anzuzeigen.



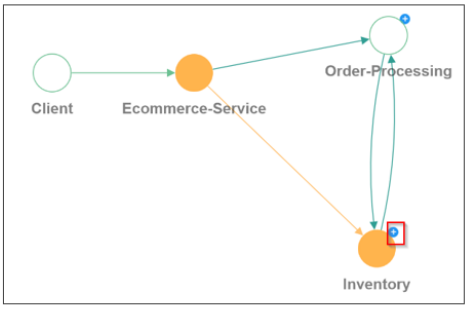
Verwenden der Einstellungsoption



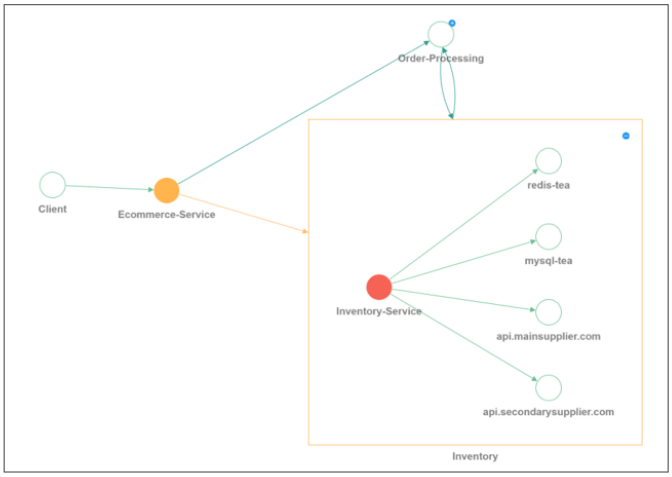
1 —Symbol “Einstellungen”

2 —Optionen zum Anzeigen des Service-Graphen als Standardansicht, ebenenbasierte oder erzwungene Ansichten

3 —Wählen Sie die Optionen aus der Liste aus, um die Dienste basierend auf Kategorien anzuzeigen. Nachdem Sie eine Kategorie aus der Liste ausgewählt haben, klicken Sie im Diagramm auf **+**, um alle Dienste anzuzeigen



Collapsed view



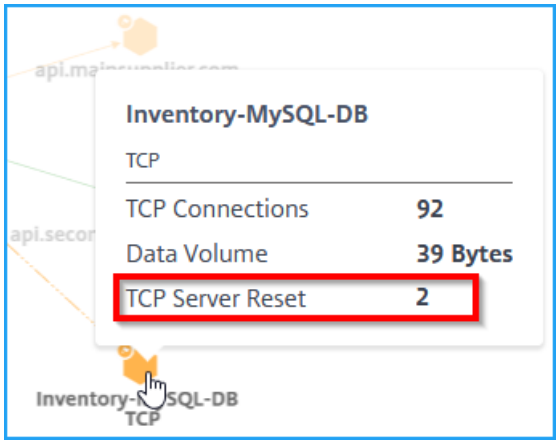
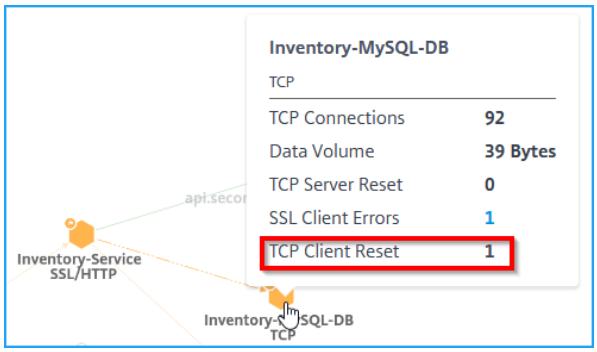
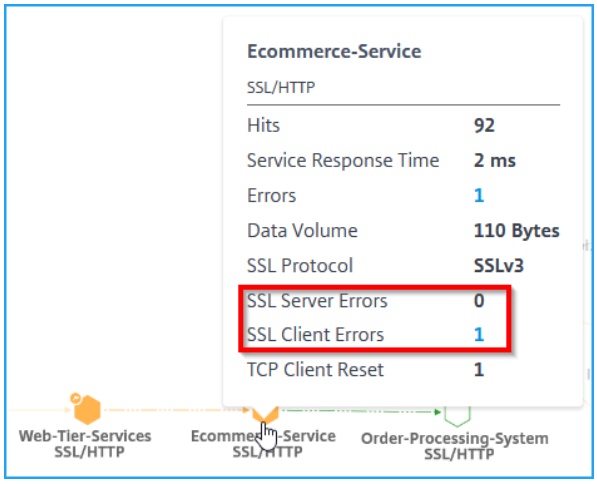
Expanded view

4 —Ermöglicht die Auswahl der Option, wie Sie die Dienste anzeigen möchten.

5 - Optionen zum Speichern der Einstellungen oder zum Zurücksetzen auf die Standardeinstellungen.

Analysieren Sie die Fehler

Bewegen Sie den Mauszeiger auf einen Dienst, der auf Fehler hinweist.

Fehler	Beschreibung
	Das **TCP-Server-Reset** zeigt die Gesamtzahl der vom Server initiierten TCP-Resets an.
	Der **TCP-Client-Reset** zeigt die Gesamtzahl der vom Client initiierten TCP-Resets an.
	Die SSL-Client-Fehler geben die Gesamtzahl der SSL-Fehler des Clients an. (Beispiel: Fehler bei der SSL-Client-Authentifizierung). Die SSL-Serverfehler Geben die Gesamtzahl der SSL-Fehler vom Server an. (Beispiel: SSL-Zertifikat unbekannt)

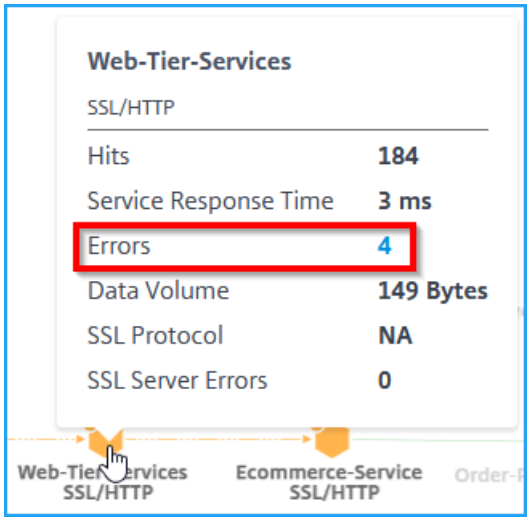
Hinweis

- Die Anzahl der Clientfehler (unabhängig vom Protokolltyp) wird in jedem Dienst angezeigt, wenn die Anzahl der Clientfehler **1 oder höher**ist.
- Die für einen Dienst angezeigte Anzahl von Client-Fehlern zeigt an, dass die Fehler vom Client stammen.

HTTP-Transaktionsdetails anzeigen

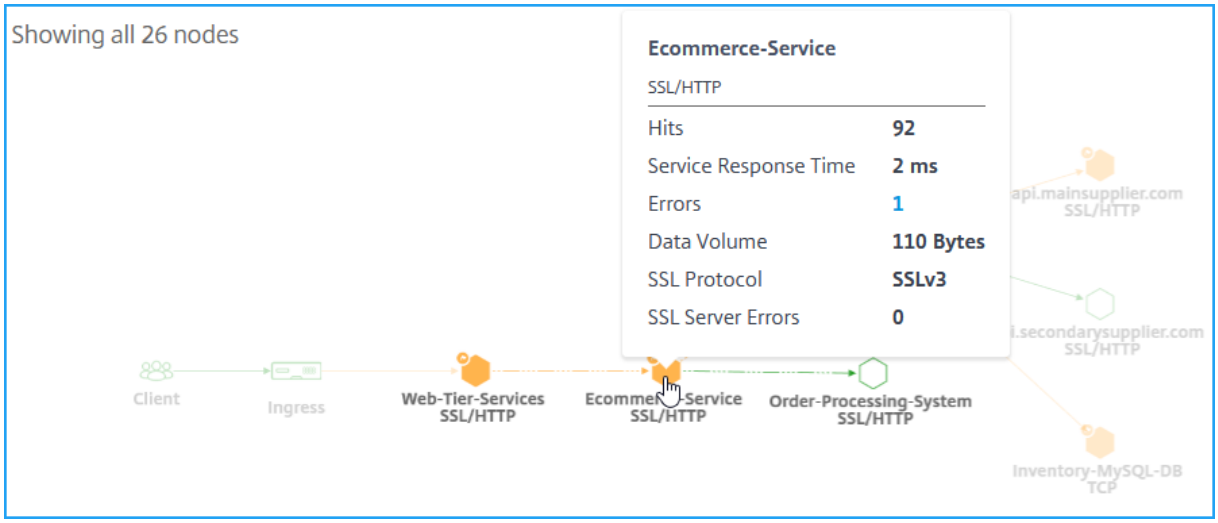
Hinweis

Sie können die Fehler anzeigen, indem Sie den Mauszeiger auf einen fehlerhaften Dienst bewegen und auf die Anzahl der Probleme klicken.

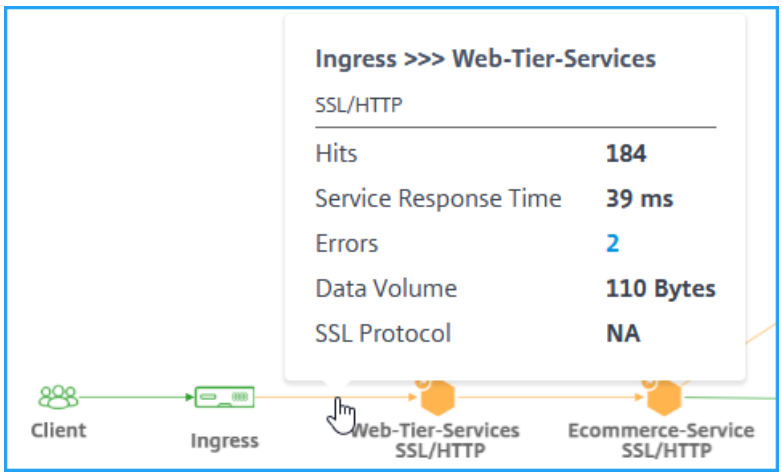


Gemäß dem in der Abbildung gezeigten Beispiel können Sie eine End-to-End-Netzwerkkarte Ihrer Anwendung anzeigen, die zeigt, wie Ihre Komponentendienste kommunizieren.

Wenn Sie den Mauszeiger auf den **E-Commerce-Dienst**bewegen, können Sie Metrik-Details für **Ecommerce-Service**anzeigen.



Mit NetScaler ADM können Sie auch Transaktionsdetails zwischen Ingress und Diensten anzeigen. Bewegen Sie den Mauszeiger, um Details wie Gesamtfehler, durchschnittliche Service-Antwortzeit usw. zwischen Eingang und Service anzuzeigen.



Treffer —Gibt die Gesamtzahl der vom Service erhaltenen Treffer an.

Service-Antwortzeit —Gibt die durchschnittliche Antwortzeit an, die der Service benötigt, um auf Time To First Byte (TTFB) zu antworten.

Fehler —Zeigt die Gesamtzahl der Fehler an, z. B. 4xx, 5xx usw.

Datenvolumen —Gibt das Gesamtvolumen der vom Dienst verarbeiteten Daten an.

SSL-Protokoll —Gibt die Version des SSL-Protokolls an.

Klicken Sie auf den Pfeil zwischen **Ingress** und **Service**, um die detaillierten Transaktionen anzuzeigen.

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

Schwellenwerte im Servicediagramm konfigurieren

February 5, 2024

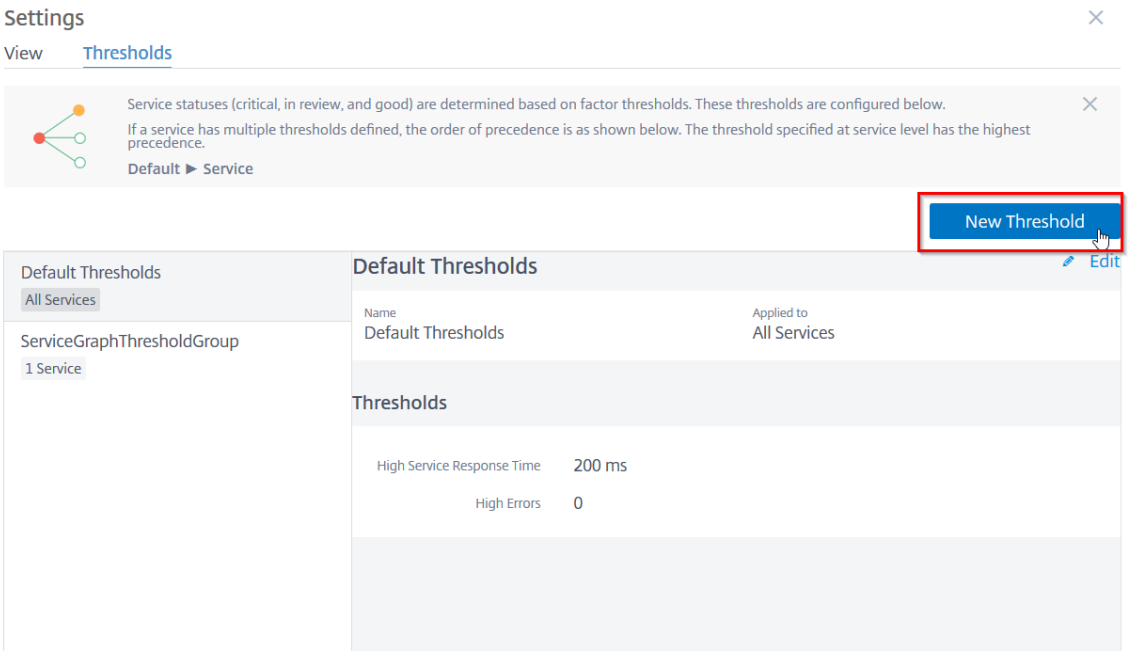
Als Administrator können Sie Schwellenwerte für Kubernetes-Dienste konfigurieren. NetScaler ADM zeigt den Dienststatus (Kritisch, Überprüfung und Gut) basierend auf der Service-Antwortzeit und der Fehleranzahl an. Standardmäßig können Sie den **Standardschwellwert** (Service-Reaktionszeit = 200 ms und Fehleranzahl = 0) anzeigen, der auf alle Dienste angewendet wird.

> **Hinweis**
>
> Sie können den Standardschwellenwert nicht löschen.

So konfigurieren Sie einen neuen Schwellenwert:

Im Servicediagramm:

1. Klicken Sie auf das Symbol “Einstellungen”und wählen Sie die Registerkarte “**Schwellenwerte** “.
2. Klicken Sie auf **Neuer Schwellenwert**, um einen neuen Schwellenwert zu



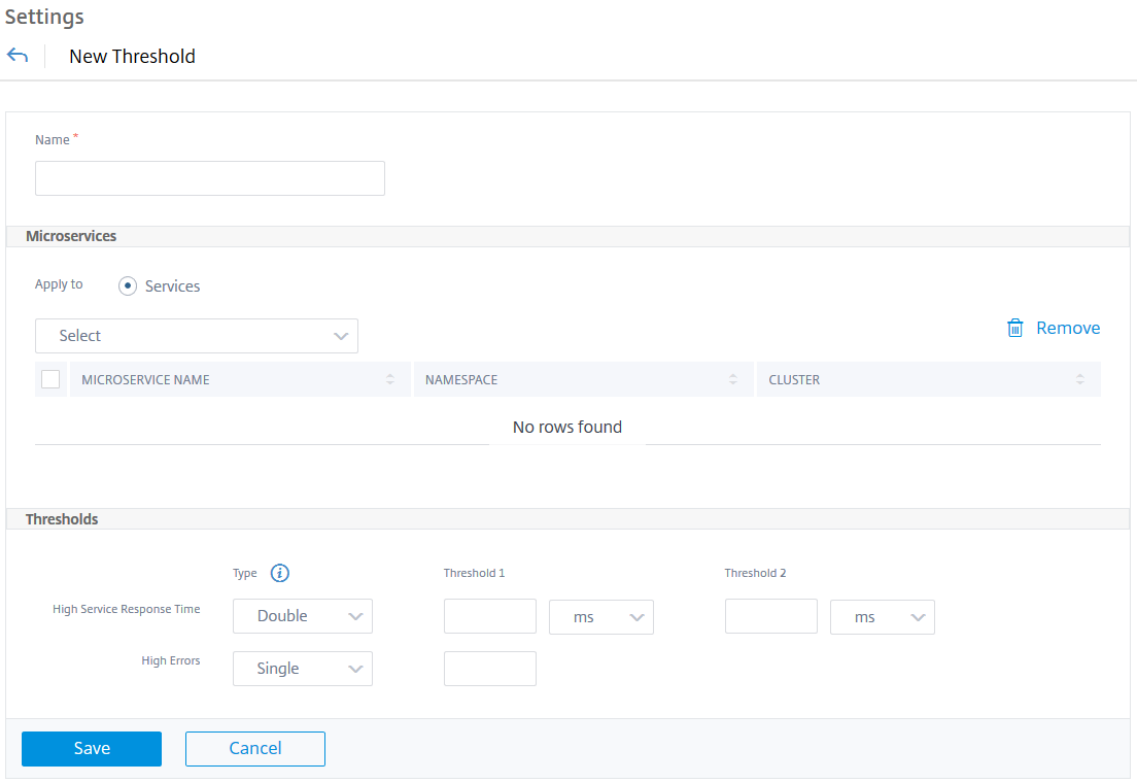
   Die Seite **Neuer Schwellenwert** wird angezeigt.
3. Konfigurieren Sie die folgenden Parameter:
   a) **Name** —Geben Sie einen Namen für den Schwellenwert an.
   b) Wählen Sie unter **Microservices**die Dienste aus, für die Sie den Schwellenwert anwenden möchten

c) Wählen Sie unter **Schwellenwerte**die Option **Einfach** oder **Zweifach** für Hohe Reaktionszeit und Hohe Fehler aus.

d) Geben Sie die Schwellenwerte an.

> **Hinweis**
>
> Wenn Sie den doppelten Schwellenwert auswählen, stellen Sie sicher:
>
> - Der Wert für Schwellenwert 1 ist kleiner als der Wert für Schwellenwert 2. Wenn Sie beispielsweise Schwellenwert 1 als 250 ms konfigurieren, muss der Schwellenwert 2 251 ms oder höher sein.
> - Der Wert für Schwellenwert 1 darf nicht mit dem Wert für Schwellenwert 2 übereinstimmen.

4. Klicken Sie auf **Speichern**.



Der Schwellenwert wurde erfolgreich erstellt. Sie können die Schwellenwertdetails auf der Seite **Schwellenwerte** anzeigen.

Einzelner Schwellenwert

Wenn Sie einen einzelnen Schwellenwert konfigurieren, ist NetScaler ADM:

- Vergleicht die aktuellen Werte mit den konfigurierten Schwellenwerten
- Berechnet die Gesamtstrafe basierend auf den überschrittenen Schwellenwerten
- Zeigt die Service-Bewertung und den Service-Status basierend auf der Penalty Berechnung an

Doppelter Schwellenwert

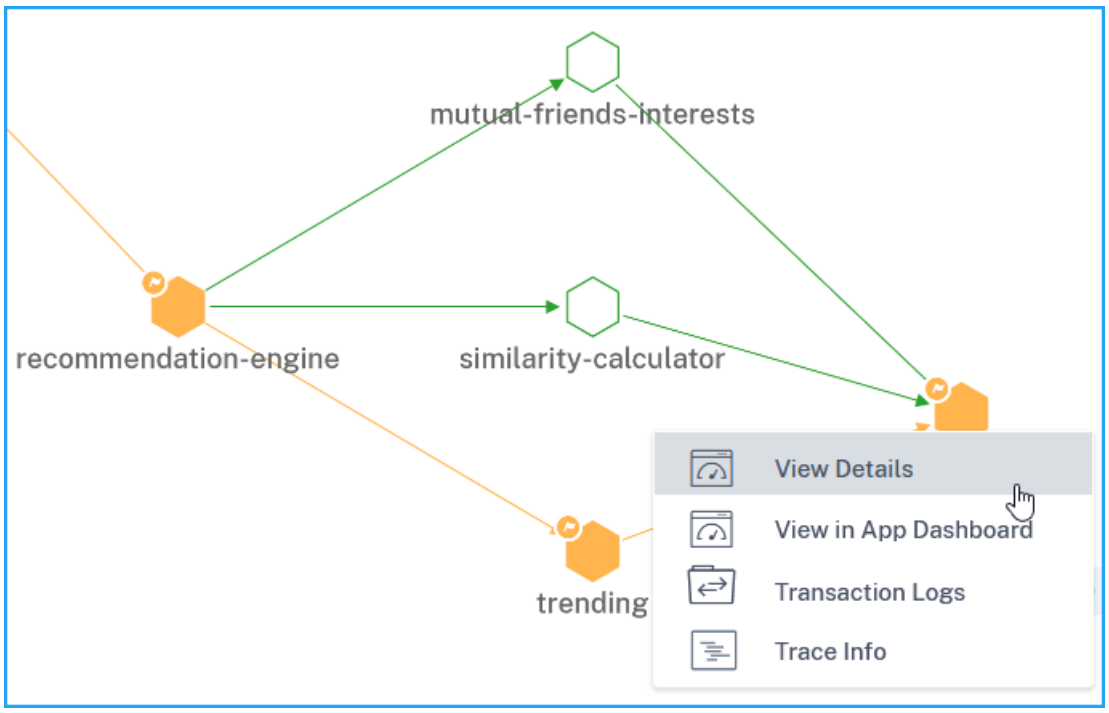
Wenn Sie den doppelten Schwellenwert konfigurieren, ist NetScaler ADM:

- Vergleicht die aktuellen Werte mit den konfigurierten Schwellenwerten
- Überprüft, ob die aktuellen Werte sind:
  - Weniger als Schwellenwert 1
  - Zwischen Schwelle 1 und Schwellenwert 2
  - Größer als Schwellenwert 2
- Berechnet die Gesamtstrafe basierend auf den überschrittenen Schwellenwerten
- Zeigt die Service-Bewertung und den Service-Status basierend auf der Penalty Berechnung an

Servicedetails anzeigen

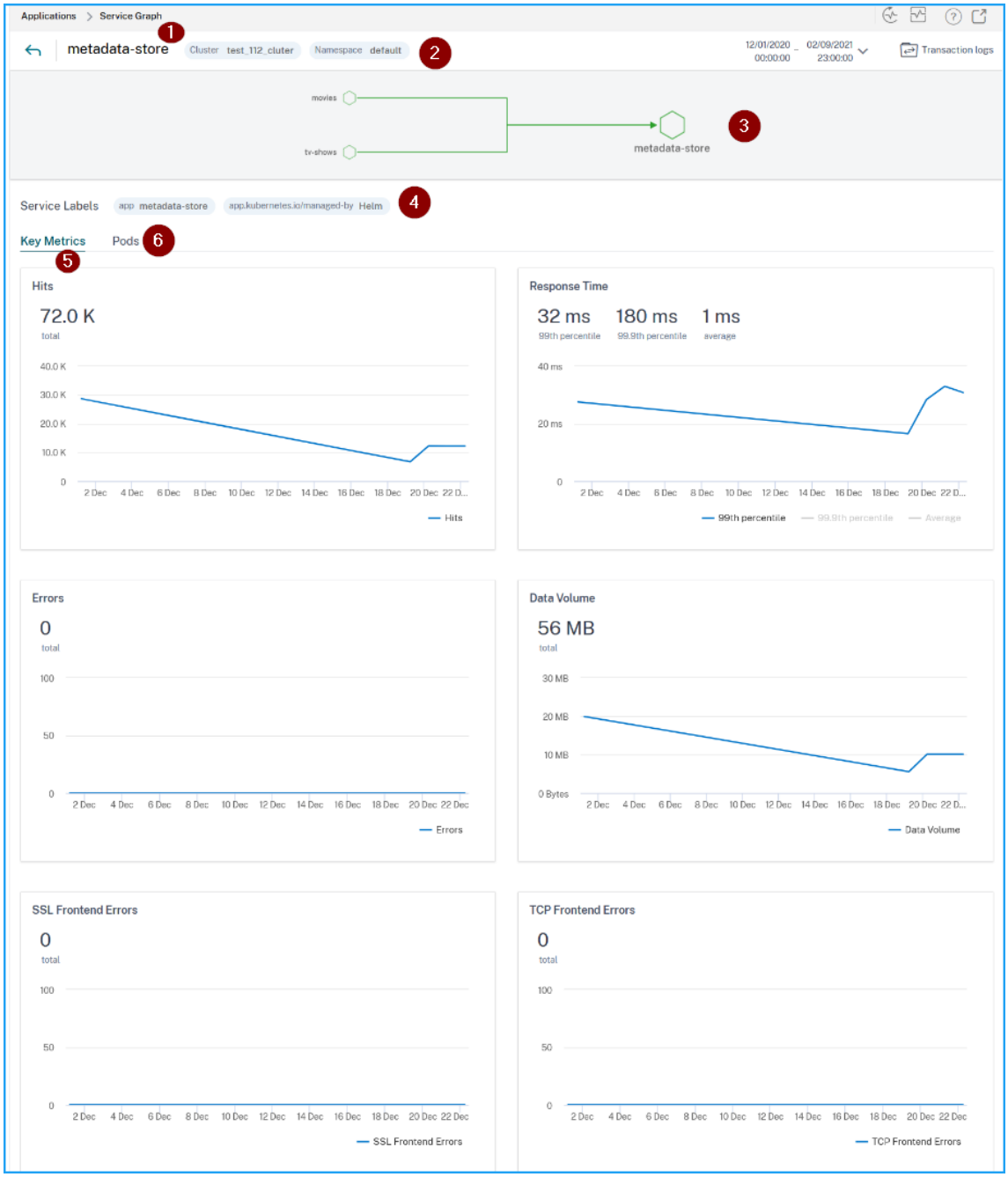
February 5, 2024

Klicken Sie auf einen Dienst und wählen Sie **Details anzeigen**aus.



Auf der Seite mit den Servicedetails können Sie Folgendes anzeigen:

- Der Clustername, in dem der Dienst gehostet wird (1)
- Der Namespace und die Dienstbezeichnungen des Dienstes (2) (4)
- Alle zugeordneten eingehenden und ausgehenden Dienste, die mit dem ausgewählten Dienst verbunden sind (3)
- Service-Schlüssel-Metriken in einem Diagrammformat wie Hits, Reaktionszeit, Fehler, Datenvolumen, SSL-Frontend-Fehler und TCP-Frontend-Fehler (5).
- Die mit dem Dienst verbundenen Backend-Pods (6).



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

Mit der **Reaktionszeit-Metrik** können Sie Folgendes anzeigen:

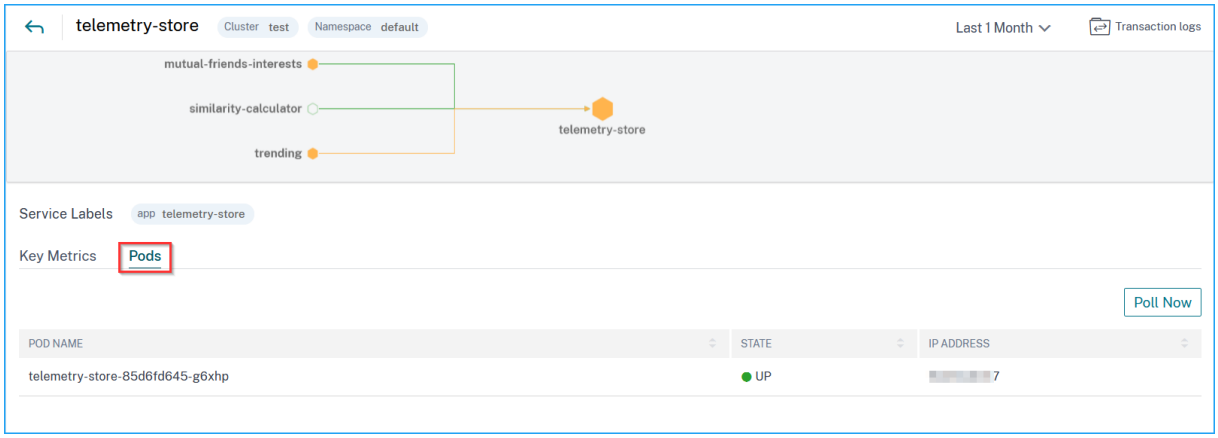
- **99tes Perzentil** —Gibt an, dass die 99% der Anforderungen für die ausgewählte Dauer weniger als 32 ms beträgt (laut Beispielbild).
- **Durchschnitt** —Gibt die durchschnittliche Reaktionszeit des Dienstes an
- **99,9. Perzentil** —zeigt die höchste Reaktionszeit des Dienstes

Details zu Metriken

Metriken	Beschreibung
Treffer	Die Gesamtzahl der vom Dienst empfangenen Anfragen
Errors	Die gesamten HTTP-Fehler des Dienstes
Service-Reaktionszeit	Die durchschnittliche Antwortzeit, die der Dienst für die Reaktion auf Time To First Byte (TTFB) verwendet hat.
Datenvolume	Das gesamte Datenvolumen, das vom Dienst verarbeitet wird
SSL Front-End-Fehler	Die gesamten SSL-Front-End-Fehler des Dienstes. Beispiel: SSL CLIENTAUTH FAILURE
SSL-Back-End-Fehler	Die gesamten SSL-Back-End-Fehler des Dienstes. Beispiel: SSL-Client-Fehler
TCP-Backend-Fehler	Die gesamten TCP-Back-End-Fehler vom Dienst. Beispiel: TCP-Server-Reset
TCP-Front-End-Fehler	Die gesamten TCP-Front-End-Fehler vom Dienst. Beispiel: Zurücksetzen des TCP-Clients

Details Back-End Backend-Pod anzeigen

Klicken Sie auf die Registerkarte **Pods**, um die Backend-Pods anzuzeigen, die mit dem Dienst verknüpft sind.

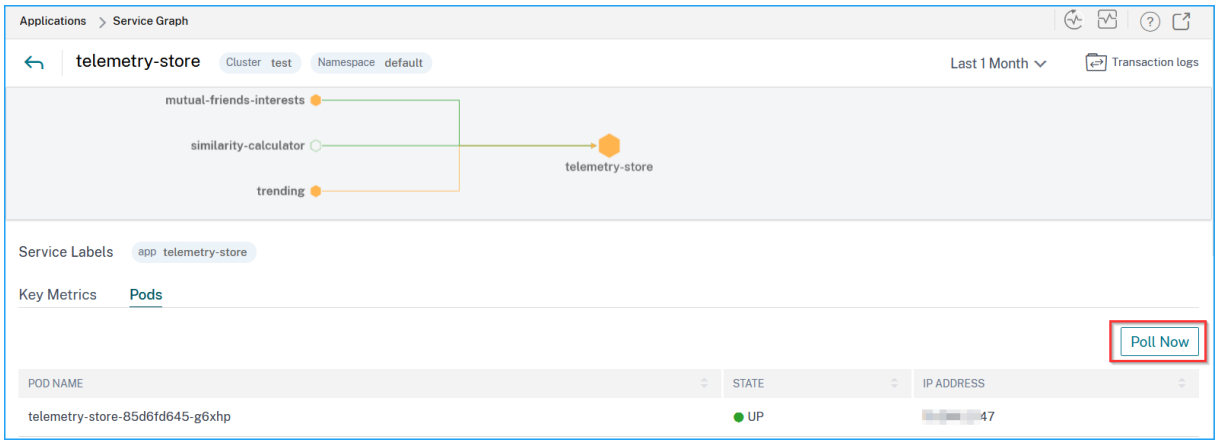


- **Pod-Name** —Bezeichnet den Pod-Namen
- **Status** —Gibt an, ob der Pod läuft (UP) oder nicht (DOWN).

- **IP-Adresse** —Bezeichnet die Pod-IP-Adresse

Verwenden Sie die Option "Jetzt abfragen", um den Podstatus zu ermitteln

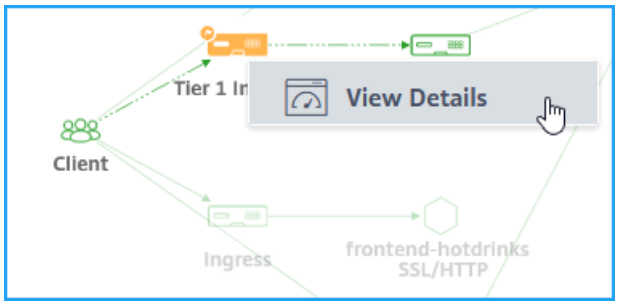
Mit **der Option Jetzt** abfragen wird der neueste Pod-Status aus dem Cluster abgerufen.



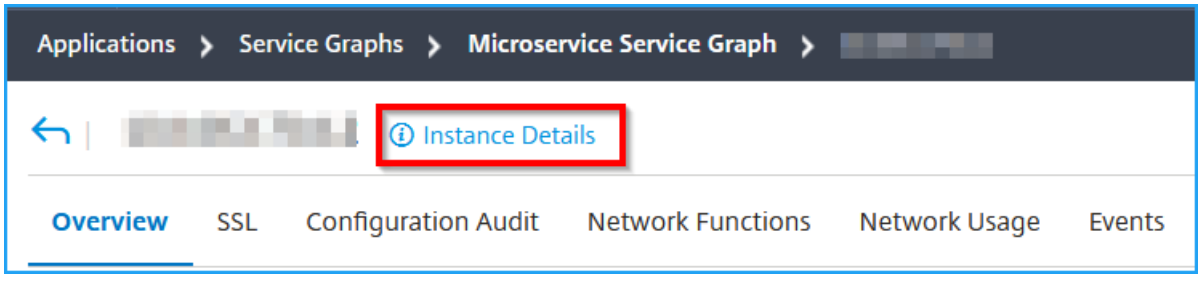
Anzeigen von Ingress-Details zur Problembehandlung

February 5, 2024

Klicken Sie im Service-Diagramm auf den Ingress und wählen Sie **Details anzeigen** aus, um die Details der NetScaler ADC-Instanz zu visualisieren, die für den Kubernetes-Cluster konfiguriert ist.

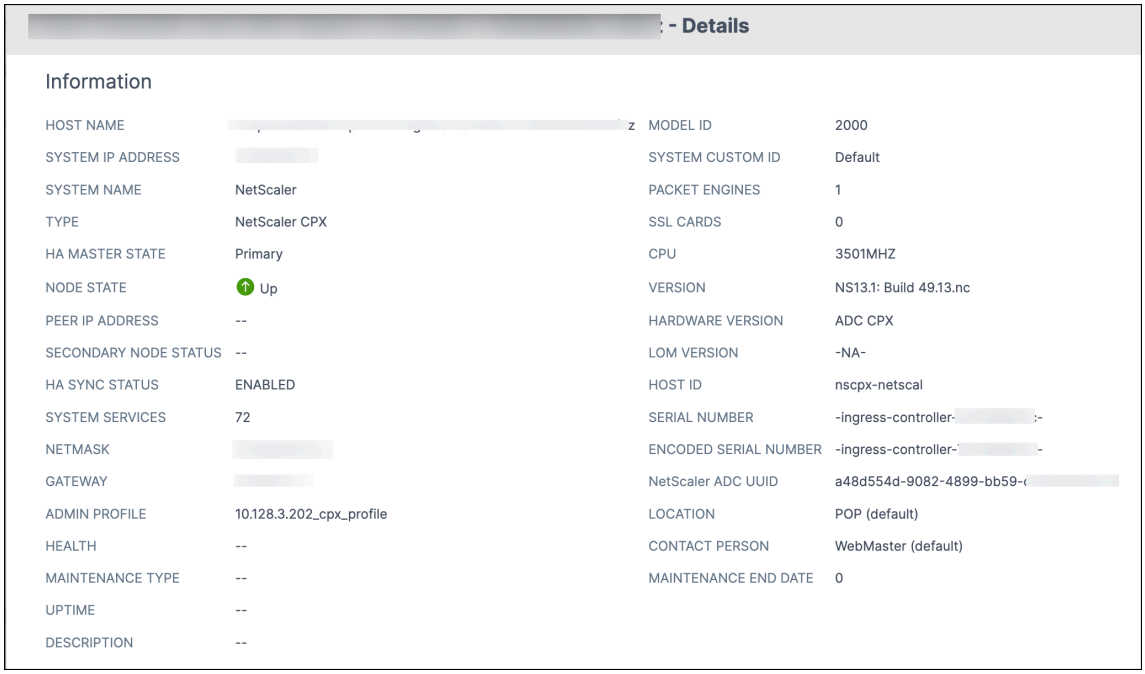


Klicken Sie auf **Instanzdetails**, um die Details anzuzeigen.

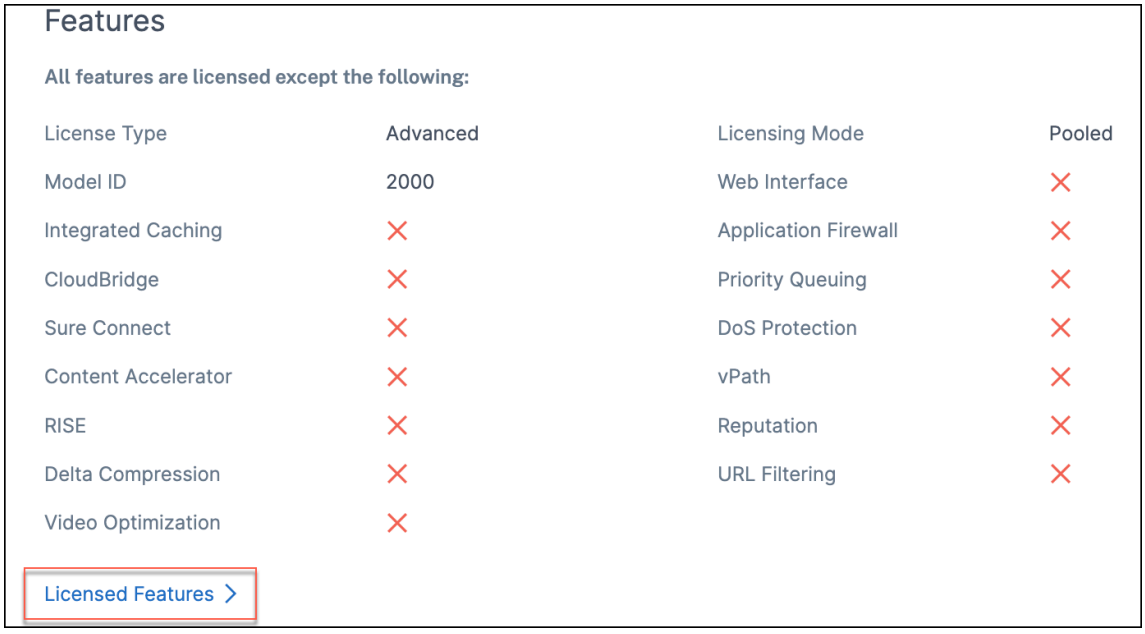


Die folgenden Details werden angezeigt:

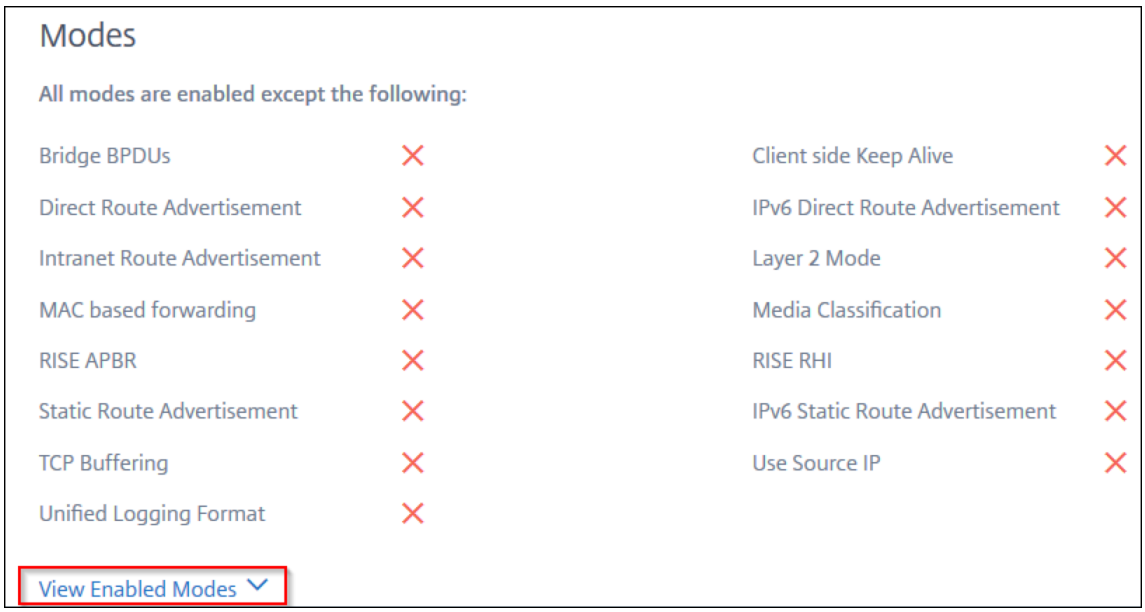
- **Informationen** —Instanzdetails wie Instanztyp, Bereitstellungstyp, Version, Modell usw.



- **Funktionen** —Standardmäßig werden die Funktionen angezeigt, die nicht lizenziert sind. Klicken Sie auf **Lizenzierte Funktionen**, um die lizenzierten Funktionen anzuzeigen.

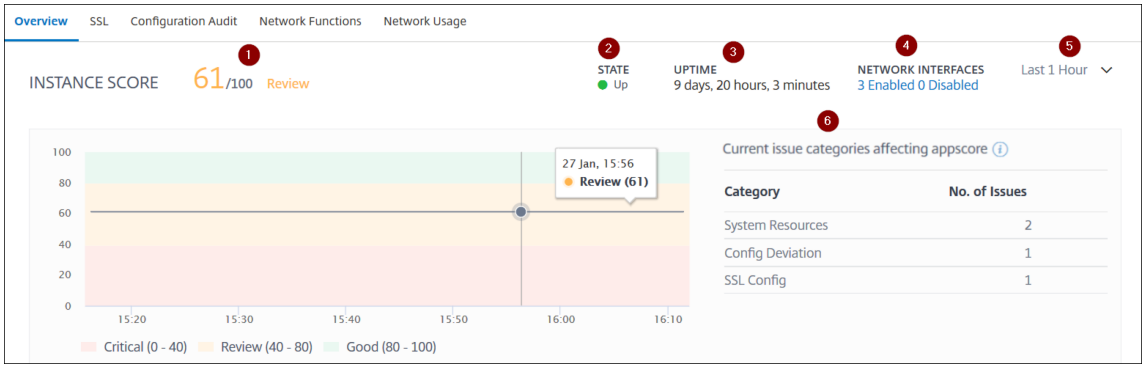


- **Modi** —Standardmäßig werden alle Modi angezeigt, die auf der Instanz deaktiviert sind. Klicken Sie auf **Aktivierte Modi** anzeigen, um die aktivierten Modi auf der Instanz anzuzeigen.



Das Instanz-Dashboard bietet eine Instanzübersicht, in der Sie die folgenden Details sehen können:

- **Instanz-Score**



1 —Gibt die aktuelle NetScaler ADC-Instanzbewertung für die ausgewählte Zeitdauer an. Das Endergebnis wird als **100 minus Gesamtstrafen**berechnet. Das Diagramm zeigt die Score-Bereiche für die ausgewählte Zeitdauer an.

2 —Gibt den aktuellen Status der NetScaler ADC-Instanz an, z. B. **Up-**, **Down-**und **Out-Out of Service**.

3 —Gibt die Dauer an, die die NetScaler ADC-Instanz ausgeführt wird.

4 —Zeigt die Gesamtzahl der für die Instanz aktivierten und deaktivierten Netzwerkschnittstellen an. Klicken Sie hier, um Details wie den Namen der Netzwerkschnittstelle und den Status (aktiviert oder deaktiviert) anzuzeigen.

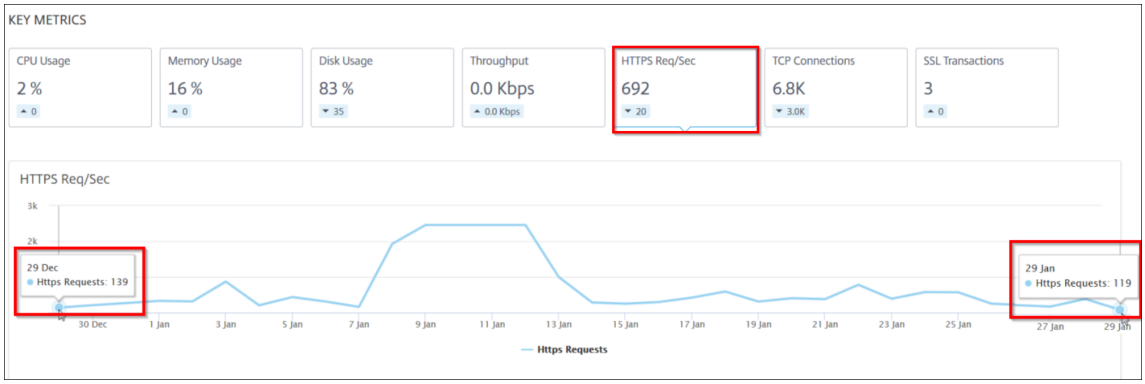
5 —Wählen Sie die Zeitdauer aus der Liste aus, um die Instanzdetails anzuzeigen.

6 —Zeigt die Gesamtzahl der Probleme und die Problemkategorie der ADC-Instanz an.

- **Wichtige Metriken**

  Klicken Sie auf jede Registerkarte, um die Details anzuzeigen. In jeder Metrik können Sie den Durchschnittswert und den Differenzwert für die ausgewählte Zeit anzeigen.

  Das folgende Bild ist ein Beispiel für HTTPS Req/Sec und die ausgewählte Zeitdauer gilt für den letzten Monat. Der Wert **692** ist der durchschnittliche HTTPS Req/Sek für die letzte Dauer von einem Monat und der Wert **20** ist der Differenzwert. In der Grafik ist der erste Wert **139** und der letzte Wert **119**. Der Differenzwert beträgt **139 —119 = 20.**



  Sie können die folgenden Instanzmetriken für die ausgewählte Zeitdauer in einem Diagrammformat anzeigen:

  - **CPU-Auslastung** —Der durchschnittliche CPU-Prozentsatz der Instanz für die ausgewählte Dauer (wird sowohl für die Paket-CPU als auch für die Verwaltungs-CPU angezeigt).
  - **Speichernutzung** —Die durchschnittliche Speichernutzung in% der Instanz für die ausgewählte Dauer.
  - **Datenträgernutzung** —Der durchschnittliche Speicherplatz in % der Instanz für die ausgewählte Dauer.
  - **Durchsatz** —Der durchschnittliche Netzwerkdurchsatz, der von der Instanz für die ausgewählte Dauer verarbeitet wird.
  - **HTTPS-Anforderung/Sekunde** —Die durchschnittlichen HTTPS-Anforderungen, die von der Instanz für die ausgewählte Dauer empfangen wurden.
  - **TCP-Verbindungen** —Die durchschnittlichen TCP-Verbindungen, die vom Client und Server für die ausgewählte Dauer eingerichtet wurden.
  - **SSL-Transaktionen** —Die durchschnittlichen SSL-Transaktionen, die von der Instanz für die ausgewählte Dauer verarbeitet wurden.

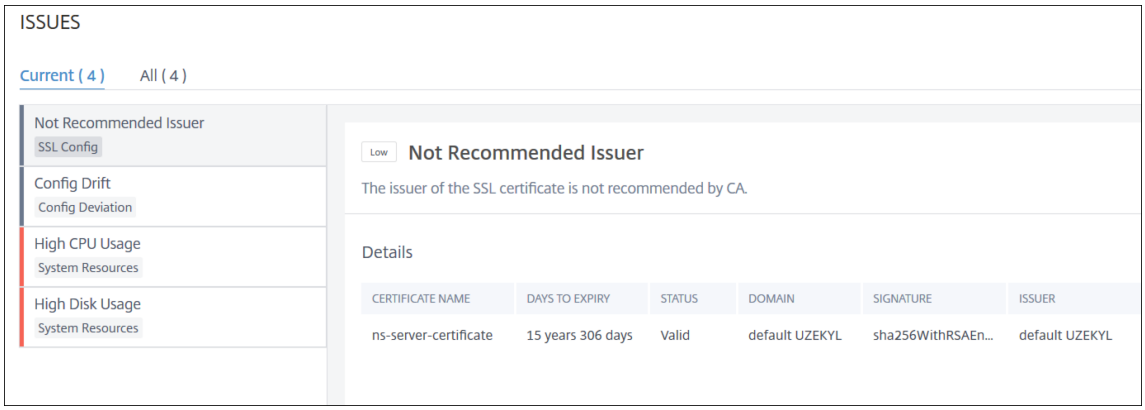
- **Probleme**

  Sie können die folgenden Probleme anzeigen, die in der NetScaler ADC-Instanz auftreten:

Kategorie der Ausgabe	Beschreibung	Probleme
Systemressourcen	Zeigt alle Probleme im Zusammenhang mit der NetScaler ADC-Systemressource an, wie CPU, Arbeitsspeicher, Datenträgernutzung usw.	– Hohe CPU-Auslastung – Hoher Speicherverbrauch – Hohe Datenträgernutzung – SSL-Kartenfehler – Stromausfall – Datenträgerfehler – Flashfehler – NIC Discards
SSL-Konfiguration	Zeigt alle Probleme im Zusammenhang mit der SSL-Konfiguration auf der NetScaler ADC-Instanz an.	– SSL-Zertifikate sind abgelaufen – Nicht empfohlener Herausgeber – Nicht empfohlener Algorithmus – Nicht empfohlene Schlüsselstärke
Abweichung der Konfiguration	Zeigt alle Probleme im Zusammenhang mit den Konfigurationsaufträgen an, die in der NetScaler ADC-Instanz angewendet werden.	– Konfigurationsdrift – Running vs Template

Kategorie der Ausgabe	Beschreibung	Probleme
Kapazitätsprobleme	Zeigt ADC-Kapazitätsprobleme an. Der ADM ruft diese Ereignisse alle fünf Minuten von der ADC-Instanz ab und zeigt die verworfenen Pakete oder Rate-Limit-Zähler-Inkremente an, falls vorhanden. Die Probleme sind nach den folgenden Kapazitätsparametern kategorisiert.	– Durchsatzlimit erreicht
Netzwerke	Zeigt die Betriebsprobleme an, die in den Instanzen auftreten.	Weitere Informationen finden Sie unter Verbesserte Infrastrukturanalyse mit neuen Indikatoren.

Klicken Sie auf die einzelnen Registerkarten, um das Problem zu analysieren und zu beheben. Stellen Sie sich beispielsweise vor, dass eine Instanz für die ausgewählte Zeitdauer die folgenden Fehler aufweist:



– Die Registerkarte **Aktuell** zeigt die aktuellen ADC-Betriebsprobleme an, die sich auf den Instanzscore auswirken.

- Auf der Registerkarte **Alle** werden alle Infrarotprobleme angezeigt, die für die ausgewählte Dauer erkannt wurden.

Verteilte Ablaufverfolgung

February 5, 2024

In Service Graph können Sie die Ansicht "Verteilte Ablaufverfolgung"verwenden, um:

- Analysieren Sie die gesamte Leistung des Dienstes.
- Visualisieren Sie den Kommunikationsfluss zwischen dem ausgewählten Dienst und seinen voneinander abhängigen Diensten.
- Identifizieren Sie, welcher Dienst auf Fehler hinweist, und beheben Sie den fehlerhaften Dienst
- Zeigen Sie Transaktionsdetails zwischen dem ausgewählten Service und dem jeweils voneinander abhängigen Service an.

Voraussetzungen

Um die Trace-Informationen für den Dienst anzuzeigen, müssen Sie:

- Stellen Sie sicher, dass eine Anwendung die folgenden Trace-Header verwaltet, während sie Ost-West-Verkehr sendet:
  - `x-request-id`
  - `x-b3-traceid`
  - `x-b3-spanid`
  - `x-b3-parentspanid`
  - `x-b3-sampled`
  - `x-b3-flags`
  - `x-ot-span-context`
- Aktualisieren Sie für **CIC-Builds vor 1.7.23** die CPX YAML-Datei mit `NS_DISTRIBUTED_TRACING` und Wert `yes`

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: cpx-ingress
spec:
  selector:
    matchLabels:
      app: cpx-ingress
  replicas: 1
  template:
    metadata:
      name: cpx-ingress
      labels:
        app: cpx-ingress
      annotations:
    spec:
      serviceAccountName: cpx-ingress-k8s-role
      containers:
        - name: cpx-ingress
          image: "quay.io/citrix/citrix-k8s-cpx-ingress:13.0-47.103"
          securityContext:
             privileged: true
          env:
          - name: "EULA"
            value: "yes"
          - name: "KUBERNETES_TASK_ID"
            value: ""
          - name: "NS_MGMT_SERVER"
            value: "192.168.0.1"
          - name: "NS_MGMT_FINGER_PRINT"
            value: "12:12:AB:CD:EA:72:E3:10:47:CD:AF:AG:C3:B7:82:6O:97:3O:E2:5D"
          - name: "NS_HTTP_PORT"
            value: "9080"
          - name: "NS_HTTPS_PORT"
            value: 9443"
          - name: "LOGSTREAM_COLLECTOR_IP"
            value: "192.168.0.1"
          imagePullPolicy: Always
```

- Für **CIC-Builds, die später als 1.7.23**sind, müssen Sie eine ConfigMap verwenden.

  ConfigMaps ermöglicht es Ihnen, Ihre Konfigurationen von Ihren Pods zu trennen und Ihre Workloads portabel zu machen. Mit ConfigMaps können Sie Ihre Workload-Konfigurationen einfach ändern und verwalten und den Bedarf an Hardcode-Konfigurationsdaten auf Pod-Spezifikationen reduzieren.

  Mit der ConfigMap-Unterstützung können Sie die Konfiguration automatisch aktualisieren, während der NetScaler Ingress Controller Pod am Laufen gehalten wird. Sie müssen den Pod nach dem Update nicht neu starten. Weitere Informationen finden Sie unter ConfigMap-Unterstützung für den Ingress-Controller.

  Mit ConfigMap können Sie verteilte Ablaufverfolgung, Ereignisse, Überwachungsprotokolle usw. aktivieren oder deaktivieren. So verwenden Sie ConfigMap:

  1. Erstellen Sie eine YAML-Datei mit den erforderlichen Parametern.

     In der folgenden Beispiel-YAML-Datei ist die verteilte Ablaufverfolgung aktiviert und andere Variablen wie Audit-Logs, Ereignisse und Transaktionen deaktiviert:

     ```
     apiVersion: v1
     kind: ConfigMap
     metadata:
       name: cic-configmap
       namespace: default
     data:
     ```



```
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'false'
      events:
        enable: 'false'
    transactions:
      enable: 'false'
      port: 5557
<!--NeedCopy-->
```

> Hinweis
>
> Sie können die Werte für `Samplingrate` zwischen 0 und 100 angeben. NetScaler ADM zeigt die erwähnte Anzahl von Trace-Transaktionen an.

2. Stellen Sie die ConfigMap bereit, indem Sie Folgendes verwenden:

   ```
   kubectl create -f <configmap-yaml>.yaml
   ```

3. Bearbeiten Sie die CPX YAML-Datei und verwenden Sie entweder `envFrom` oder `args`, um die folgenden Argumente anzugeben:

   ```
   envFrom:
    - configMapRef:
        name: cic-configmap
   <!--NeedCopy-->
   ```

   ODER

   ```
   args:
     - --configmap
       default/cic-configmap
   ```

4. Wenn Sie den Wert für eine Variable ändern möchten, bearbeiten Sie die Werte in der ConfigMap. In diesem Beispiel werden alle anderen Variablen von **`false`** in geändert **`true`**.

   ```
   apiVersion: v1
   ```



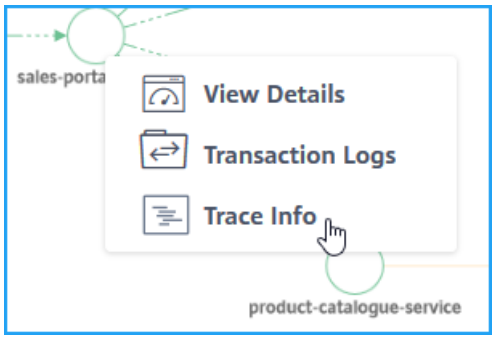
```
kind: ConfigMap
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'true'
      events:
        enable: 'true'
    transactions:
      enable: 'true'
      port: 5557
  <!--NeedCopy-->
```

5. Wenden Sie ConfigMap erneut mit dem folgenden Befehl an:

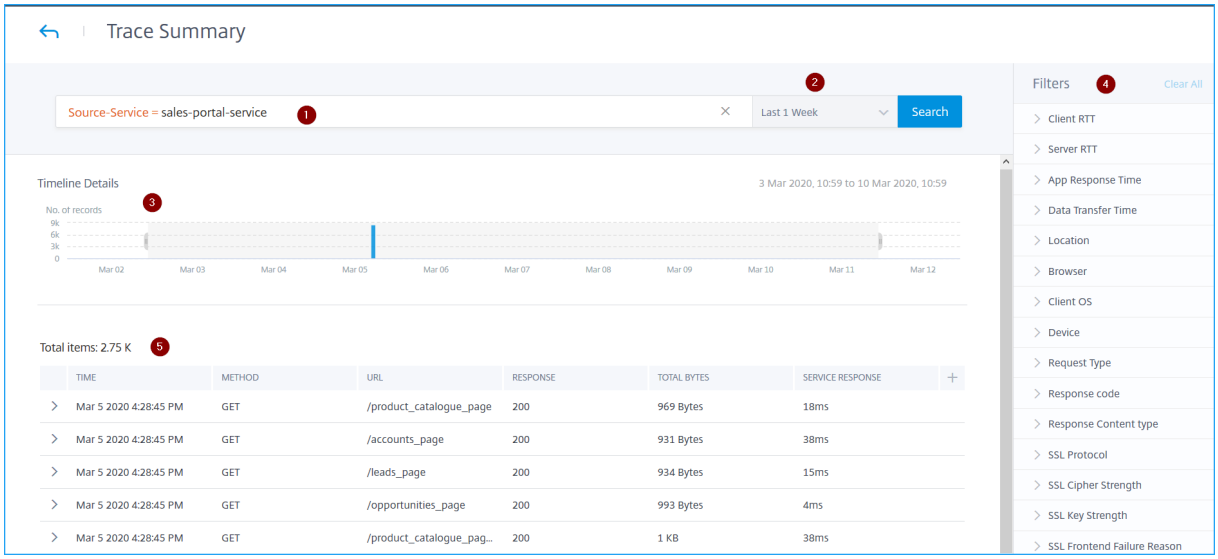
   ```
   kubectl apply -f <yaml-file>.yaml
   ```

Details zur Service-Ablaufverfolgung anzeigen

Klicken Sie im Service-Graph auf einen Service, und wählen Sie **Informationen zur Ablaufverfolgung**aus.



Die Seite “Ablaufverfolgungszusammenfassung”wird für den ausgewählten Service angezeigt.



Die **Zusammenfassung der Ablaufverfolgung** zeigt an:

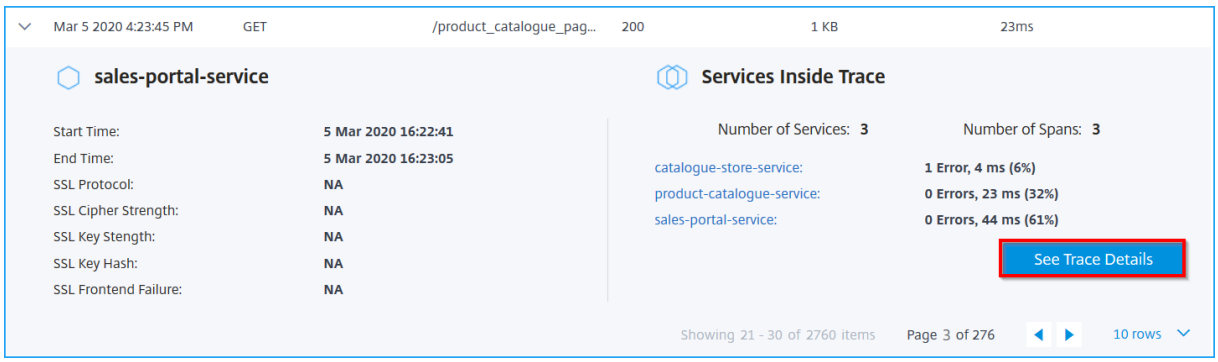
- Eine erweiterte Suche, mit der Sie nach Transaktionen mit Vorschlägen und Operatoren suchen können (1). Weitere Informationen finden Sie unter Erweiterte Suche.
- Die Liste der Zeitdauer, mit der Sie die Zeitdauer auswählen können, z. B. 1 Stunde, 12 Stunden, 1 Tag, 1 Woche, 1 Monat und benutzerdefinierte Zeit (2).
- Das Diagramm “Zeitleistendetails”, mit dem Sie die Ergebnisse für eine bestimmte Zeitdauer durch Ziehen und Auswählen anzeigen können (3).
- Das Bedienfeld “Filter”, in dem Sie Optionen aus jeder Metrik auswählen können (4).
- Die Transaktionsdetails für den ausgewählten Dienst (5).

Zeigen Sie die Transaktionsdetails an

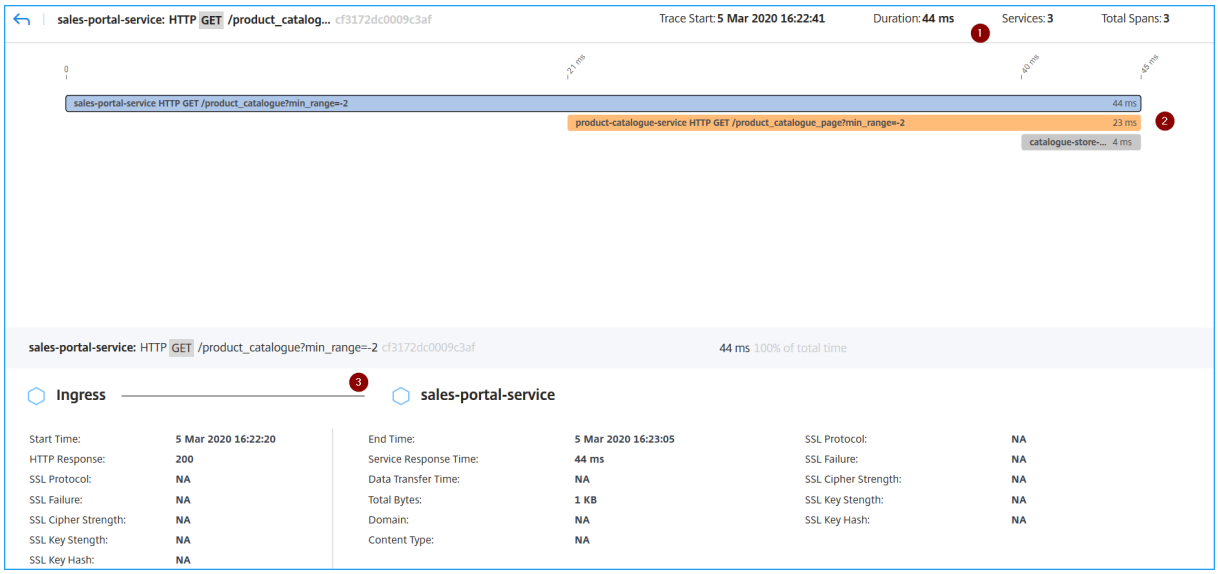
Klicken Sie auf eine Transaktion, um detaillierte Informationen zu erhalten. Sie können Transaktionsdetails für den ausgewählten Service anzeigen, z. B.:

- Startzeit
- Endzeit
- SSL-Metriken
- Kommunikation mit voneinander abhängigen Diensten (zusammen mit Fehlern und Reaktionszeit bei jedem Dienst).

Das folgende Beispiel weist auf einen Fehler von hin `catalogue-store-service`. Klicken **Sie auf Verfolgungsdetails anzeigen**, um weitere Informationen zu



Die Seite “Verfolgungsdetails”wird angezeigt.

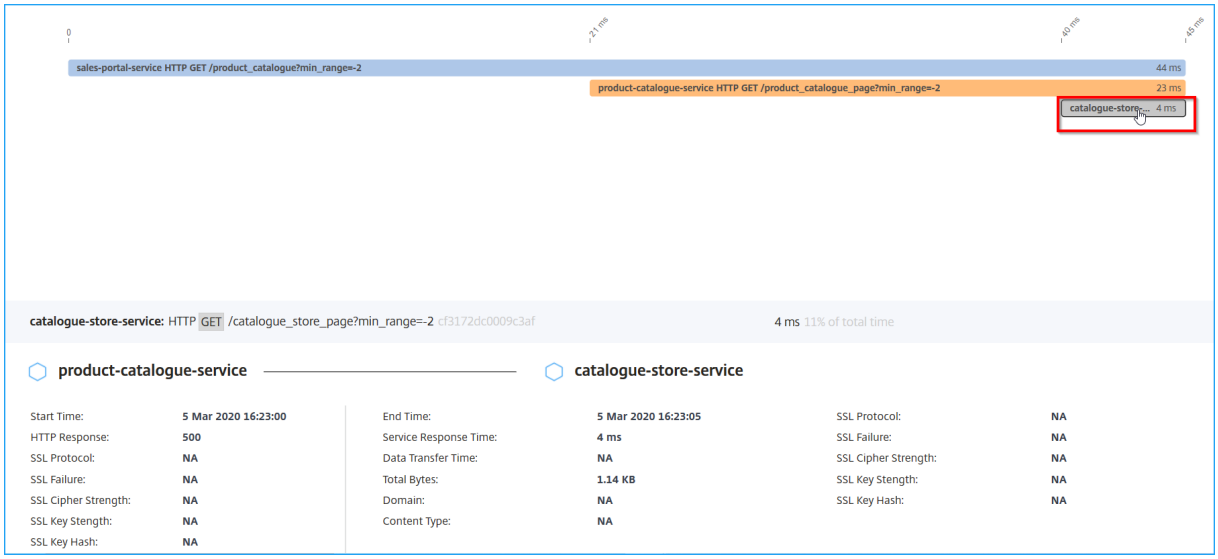


1 —Zeigt die Startzeit, die Antwortzeit, die Gesamtzahl der Services und die gesamten Spannweiten für die Transaktion an.

2 —Zeigt die Details für den ausgewählten Dienst an, der mit seinen Interdependency-Diensten kommuniziert hat. Sie können auf jede Transaktion klicken, um Details anzuzeigen.

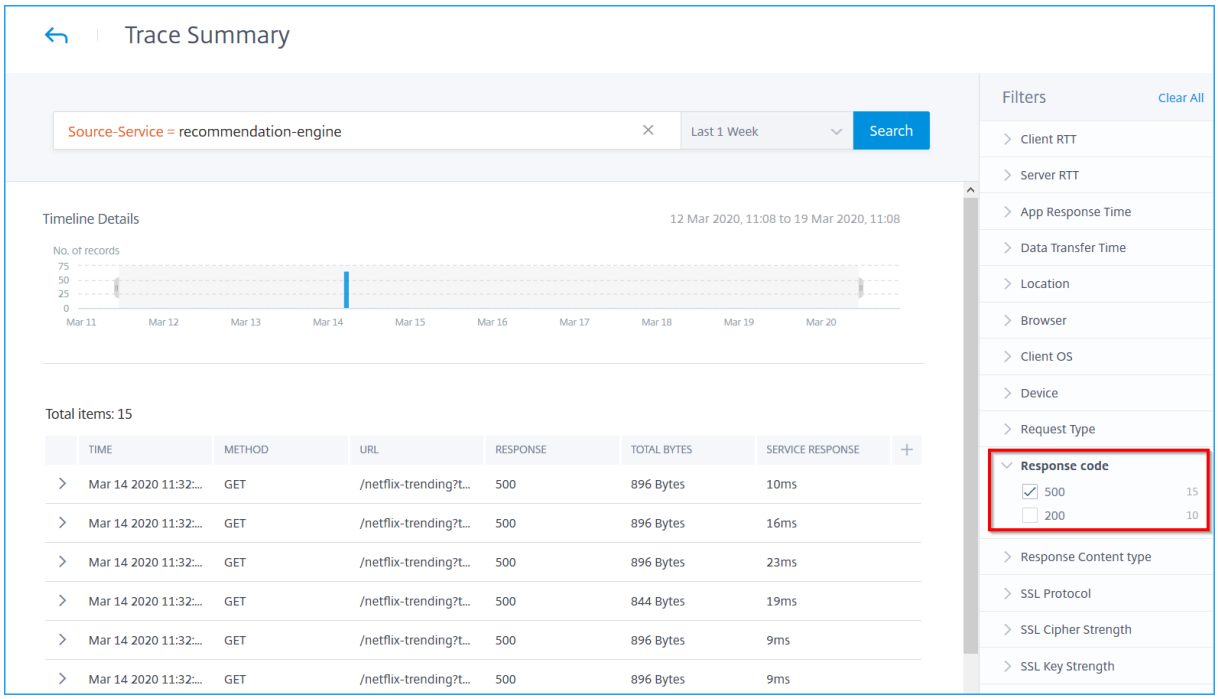
3 —Zeigt die Transaktionsdetails für jeden Service an.

Laut Beispielbild, zeigt `catalogue-store-service` einen Fehler an. Klicken Sie auf die verfügbare Transaktion `catalogue-store-service`.



Die Transaktionsdetails zwischen `product-catalogue-service` und `catalogue-store-service` geben die HTTP-Antwort als 500 an. Mit diesen Details können Sie als Administrator den fehlerhaften Dienst analysieren und Fehler in `product-catalogue-service` beheben.

Sie können Ergebnisse auch filtern, indem Sie Optionen aus jeder Metrik im Bereich **Filter** auswählen. Wenn Sie beispielsweise alle 5xx-Transaktionen anzeigen möchten, klicken Sie auf **Antwortcode** und wählen Sie **500**aus.



- **Client RTT**: Die Zeitdauer für die Übertragung eines Pakets vom Client.
- **Server-RTT**: Die Zeitdauer, während der ein Paket vom Server übertragen wird.

- **Reaktionszeit der App**: Die durchschnittliche Antwortzeit der Anwendung
- **Datenübertragungszeit**: Die Datenübertragungsgröße und die Geschwindigkeit, mit der die Übertragung von/zu einem Dienst erfolgen kann.
- **Standort**: Der Kundenstandort
- **Browser**: Die von den Clients verwendeten Browsertypen. Zum Beispiel: Chrome, Firefox.
- **Client-Betriebssystem**: Das Clientbetriebssystem, das auf den Benutzeragentdetails aus dem Browser basiert.
- **Gerät**: Die Geräte, die auf den Benutzeragentdetails aus dem Browser basieren. Zum Beispiel: Tablet, Handy.
- **Anforderungstyp**: Der Transaktionsanforderungstyp Zum Beispiel: GET.
- **Antwortcode**: Der vom Server empfangene Antwortcode. Zum Beispiel: 501, 404, 200.
- **Inhaltstyp der Antwort**: Der Inhaltstyp der Transaktion. Wenn die Clientanforderung für text/html ist, muss die Antwort vom Server text/html lauten.
- **SSL-Protokoll**: Die von den Clients verwendete SSL-Protokollversion. Zum Beispiel: SSLv3.
- **SSL-Verschlüsselungsstärke**: Die Verschlüsselungsstärke basierend auf der Schlüsselgröße des SSL-Zertifikats, z. B. hoch, mittel und niedrig.
- **SSL-Schlüsselstärke**: Die SSL-Verschlüsselungsstärke wird anhand der Schlüsselgröße des SSL-Zertifikats berechnet. Die Schlüssellänge definiert die Sicherheit des SSL-Algorithmus. Zum Beispiel: 2048
- **SSL Front-End-Grund**: Die Fehlermeldung Front-End-SSL-Handshake. Beispiel: SSL CLIENTAUTH FAILURE

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

February 5, 2024

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

- Statische Route ist nicht konfiguriert

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

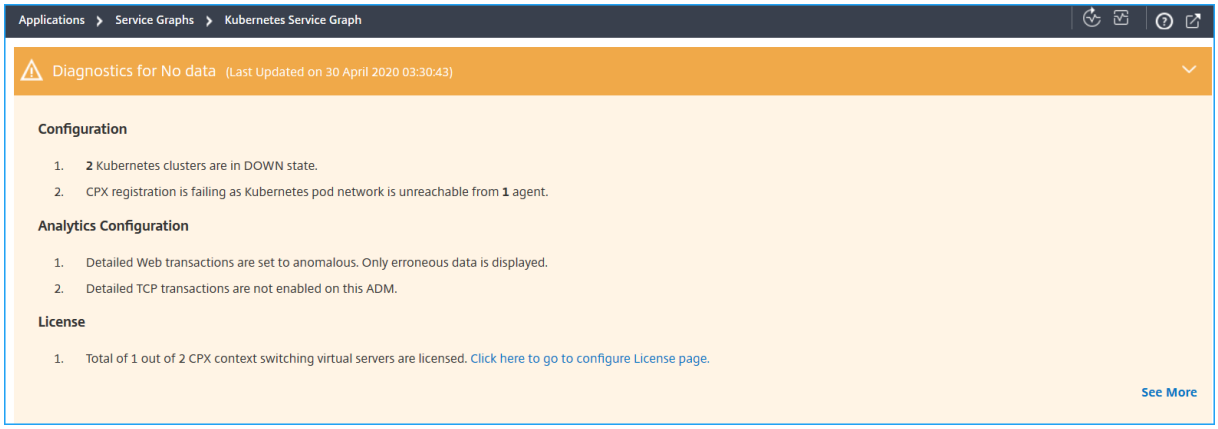
Als Administrator fällt es Ihnen möglicherweise schwer, die Gründe zu analysieren, aus denen ein Servicegramm Teildaten oder keine Daten anzeigt. Auf der Seite “Diagnoseinformationen”im Service-Diagramm können Sie die möglichen Gründe und erforderlichen Maßnahmen zur Behebung der Teildaten oder des Datenproblems anzeigen.

Navigieren Sie in NetScaler ADM zu **Applications** > **Service Graph** und klicken Sie auf die Registerkarte **Microservices**.

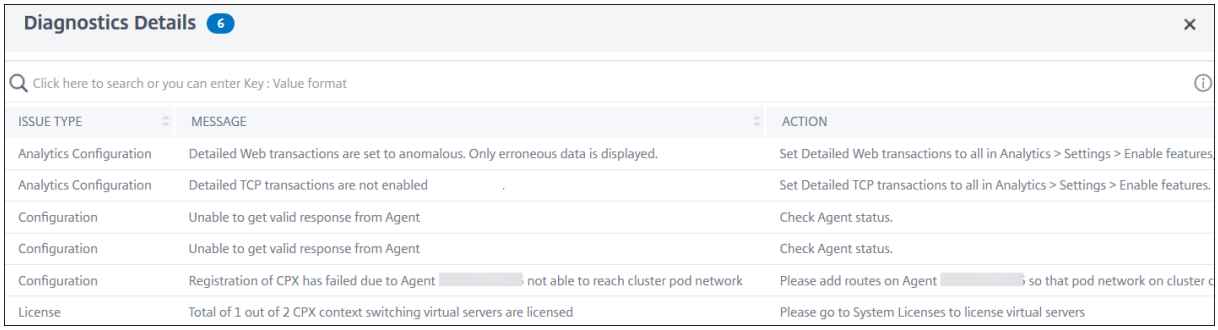
Diagnose für keine Daten

Wenn in der Servicekurve keine Daten angezeigt werden, wird die folgende Diagnosemeldung angezeigt.

Klicken Sie auf **, um Details anzuzeigen. Sie können die möglichen Gründe dafür anzeigen, dass Service Graph keine Daten anzeigt. Die folgende Abbildung ist ein Beispiel dafür, dass keine Daten im Servicegraphen enthalten sind.



Klicken Sie auf **Mehr** anzeigen, um Details zu den Problemen anzuzeigen.

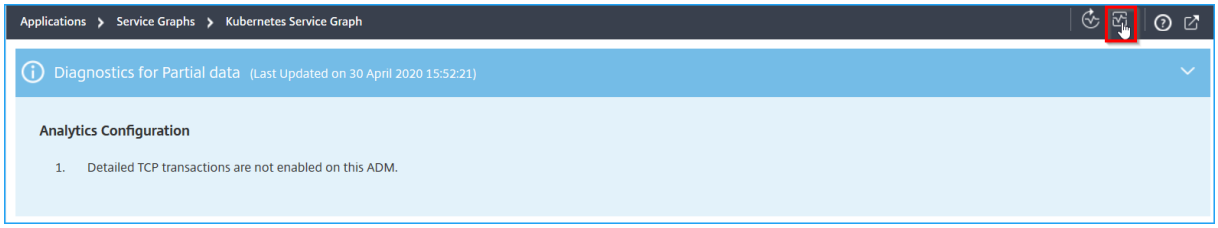


- **Problemtyp** —Gibt an, ob die Probleme bei der Konfiguration, Analysekonfiguration oder Lizenzierung auftreten.
- **Meldung** —Zeigt an, was das Problem verursacht hat.
- **Aktion** —Gibt an, welche Aktion ausgeführt werden muss, um das Problem zu beheben.

Diagnose für Teildaten

Wenn das Servicegriph nur mit Teildaten angezeigt wird, klicken Sie auf die Schaltfläche **Diagnose anzeigen**, um die Diagnoseinformationen anzuzeigen.

Das folgende Beispiel zeigt an, dass die TCP-Transaktionen deaktiviert sind.

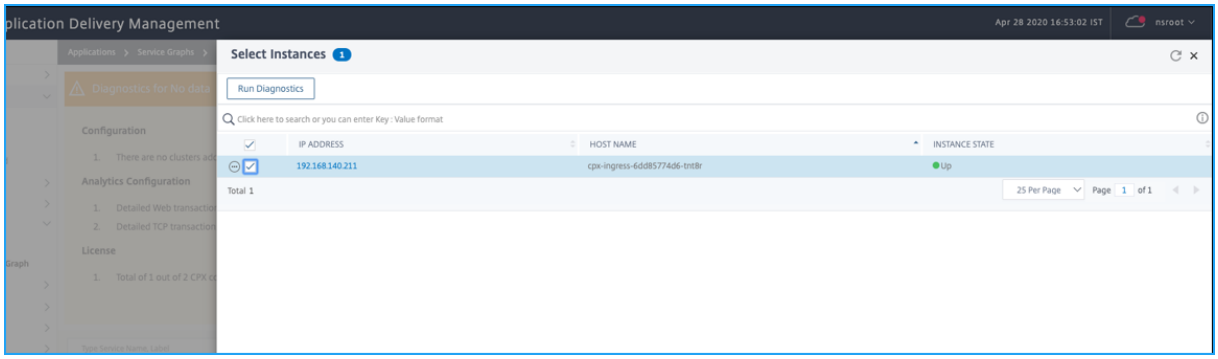


In diesem Beispiel müssen Sie die **TCP-Transaktionseinstellungen** auf **Alle** aktivieren, indem Sie zu **Analytics** > **Einstellungen**navigieren.

Problembehandlung

Als Administrator können Sie mithilfe dieser Diagnosemeldungen diese Probleme überprüfen und versuchen, diese Probleme zu beheben. Nach der Fehlerbehebung führt NetScaler ADM in regelmäßigen Abständen automatisch eine regelmäßige Diagnoseprüfung durch. Nachdem die Diagnoseprüfung abgeschlossen ist, wird das Problem mit Teildaten oder “Keine Daten im Servicegraphen”behoben.

Sie können auch auf **Diagnose ausführen**klicken, die **CPX-Instanzen**auswählen und auf **Diagnose ausführen**klicken.



Weitere Szenarien zur Fehlerbehebung finden Sie in den FAQs.

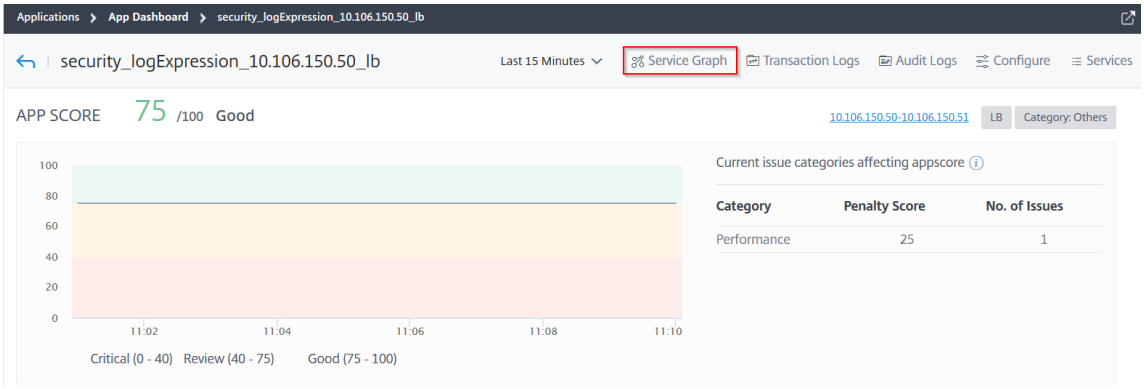
Servicediagramm für Anwendungen

February 5, 2024

So zeigen Sie Service-Graph für eine Anwendung an:

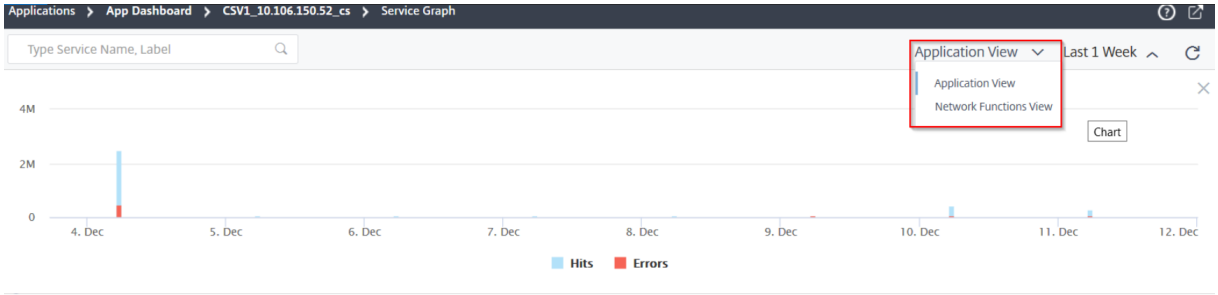
1. Navigieren Sie zu **Anwendungen** > **Dashboard**.
2. Wählen Sie eine Anwendung aus.

   Die Seite mit den Anwendungsdetails wird angezeigt.
3. Wählen Sie die Zeitdauer und klicken Sie auf **Service-Graph**.

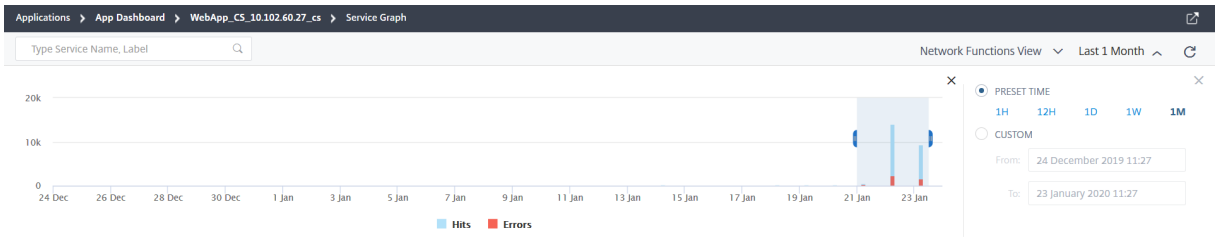


   Die Service-Graph-Seite wird für die ausgewählte Anwendung angezeigt.

Sie können das Service-Diagramm in der **Anwendungsansicht** oder in der Ansicht "**Netzwerkfunktionen**"**anzeigen**.

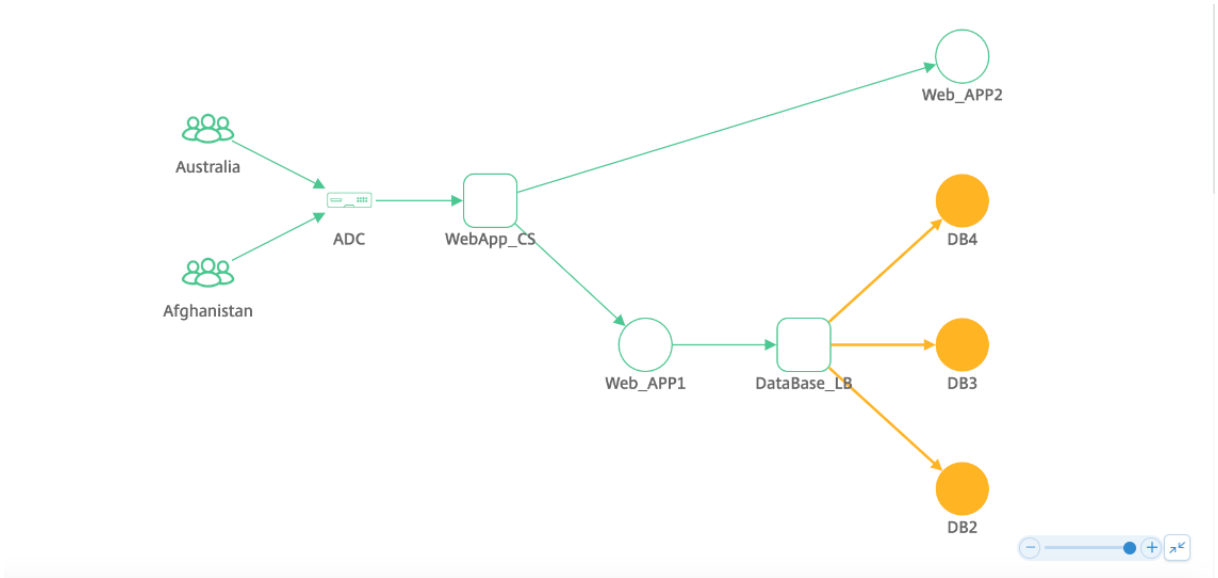


Sie können die Treffer und Fehler auch ziehen und auswählen, um die Ergebnisse zu ändern.



Ansicht der Anwendung

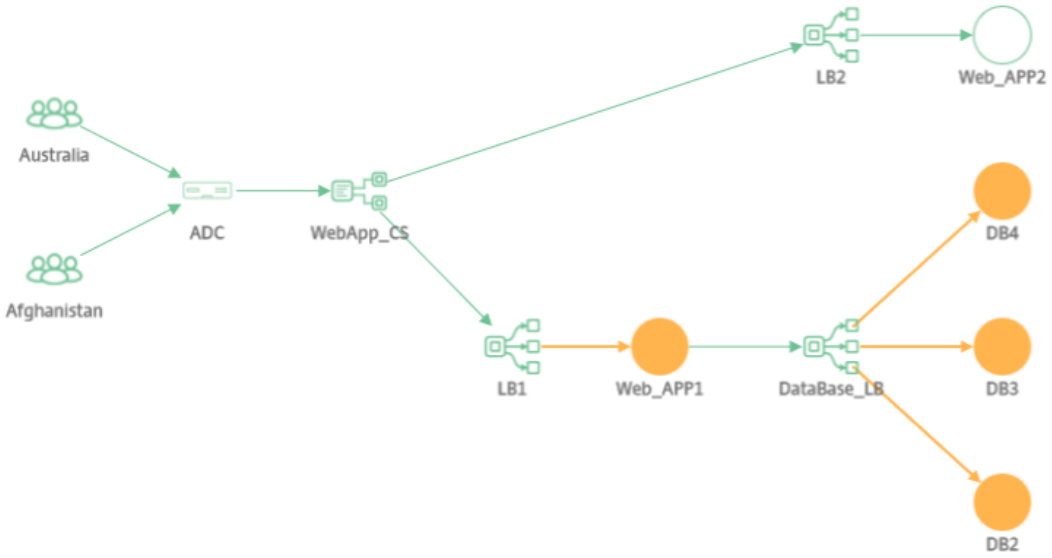
Zeigt die Übersicht der Anwendungskonfiguration an. In dieser Ansicht können Sie die Kommunikation zwischen Client-, ADC- und Webanwendungen visualisieren.



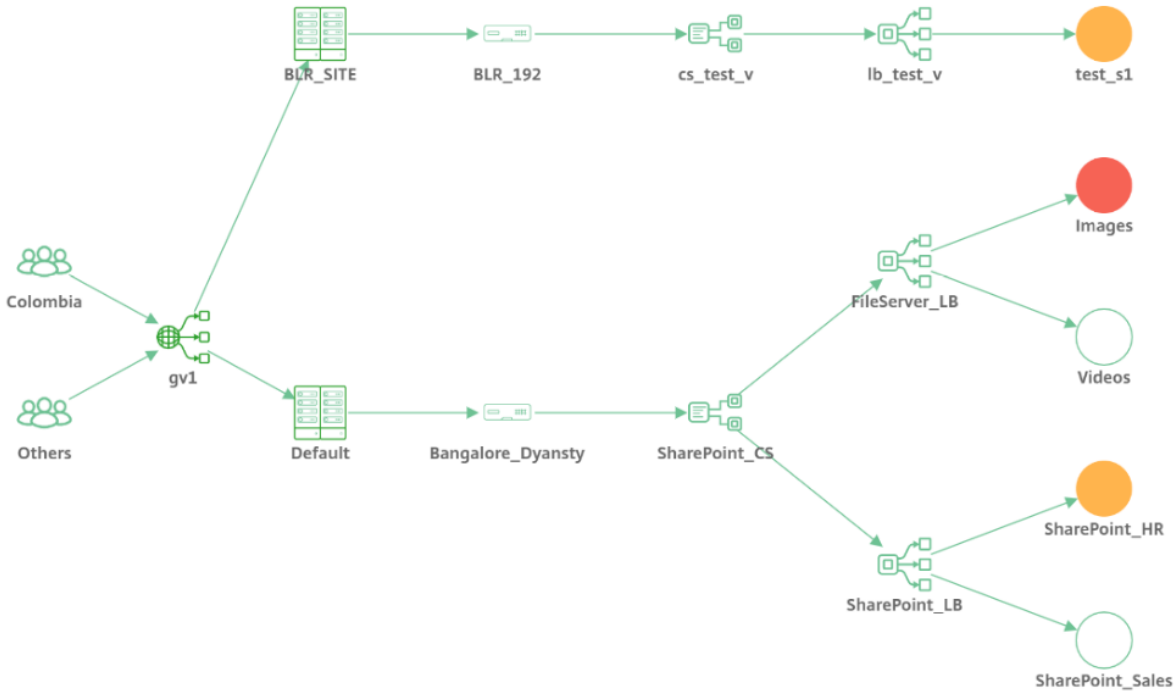
Ansicht der Netzwerkfunktionen

Zeigt die virtuellen Server an, die der Anwendung zugeordnet sind. In dieser Ansicht können Sie visualisieren, ob der ADC kommuniziert mit:

- Virtueller Content Switching-Server für den Zugriff auf die Anwendung
- Virtueller Load Balancing-Server für den Zugriff auf
- Virtuelle Server für Content Switching und Load Balancing für den Zugriff auf die Anwendung



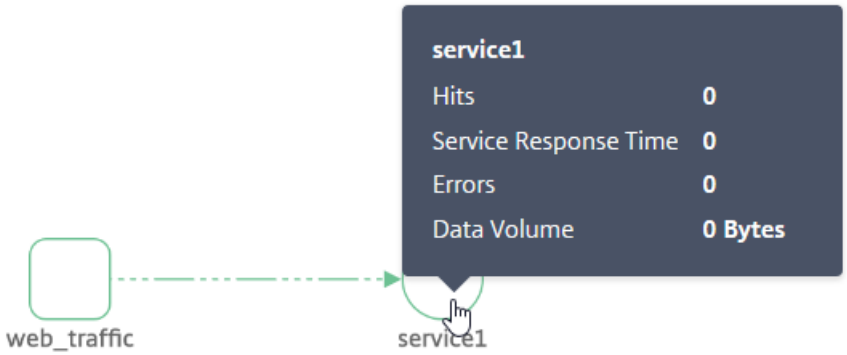
Für die GSLB-Anwendung werden die Details zusammen mit dem Rechenzentrum und NetScaler ADC angezeigt.



Service-Graph-Ansicht für keine aktiven Transaktionen

Wenn keine aktiven Transaktionen zwischen ADC und Webanwendung stattfinden, zeigt das Service-diagramm nur die Grundkonfiguration der Anwendung an (ohne Client und ADC).

Wenn Sie den Mauszeiger auf einen Dienst oder virtuellen Server bewegen, werden die Details für alle Metriken als 0 angezeigt, da keine Transaktionen vorhanden sind.

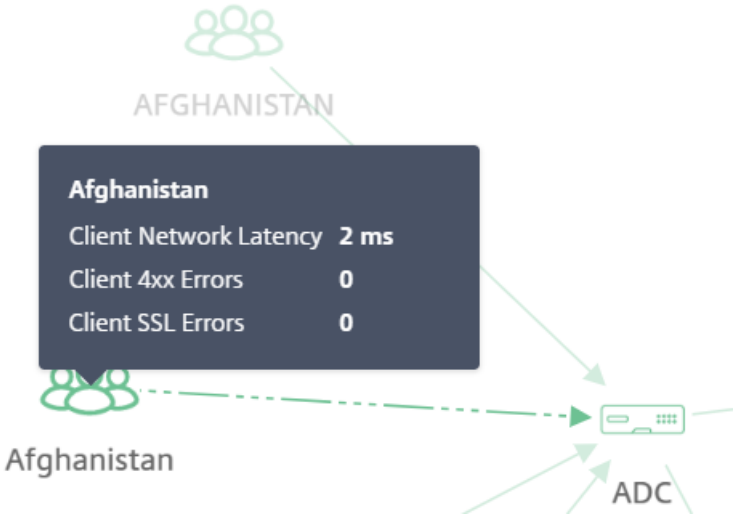


Analysieren Sie Kennzahlen

Bewegen Sie den Mauszeiger auf jeden Dienst, um Metrikdetails entweder in der Anwendungsansicht oder in der Netzwerkfunktionsansicht anzuzeigen.

Client-Metriken

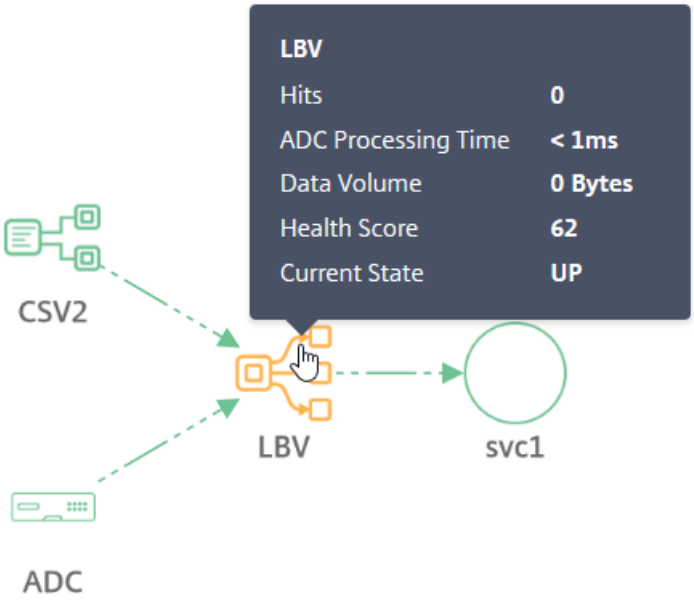
Bewegen Sie den Mauszeiger auf den Client, um die Client-Metriken anzuzeigen.



- **Client-Netzwerklatenz** —Gibt die Netzwerklatenz des Clients an.
- **Client-4xx-Fehler** —Gibt die Gesamtzahl der 4xx-Fehler an, die vom Client aufgetreten sind.
- **Client-SSL-Fehler** —Gibt die Gesamtzahl der SSL-Fehler des Clients an.

Metriken der Netzwerkfunktion

Bewegen Sie den Mauszeiger auf einen Lastausgleichs- oder Content Switching-Dienst, um die Metrikdetails anzuzeigen.

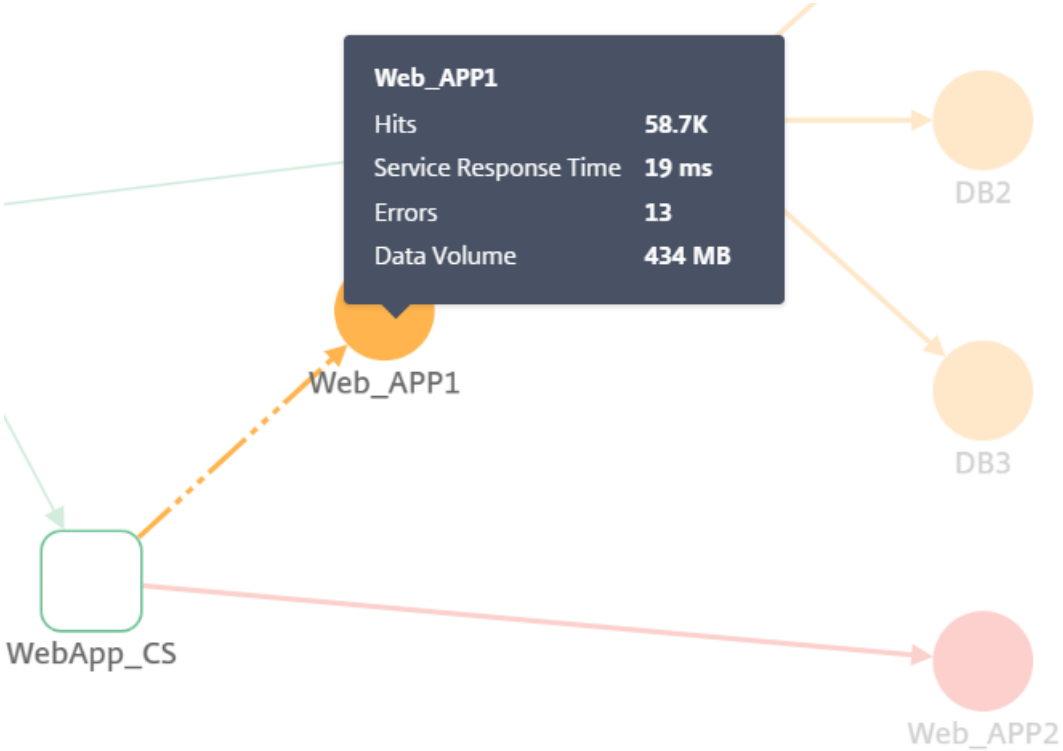


- **Treffer** —Gibt die Gesamtzahl der vom virtuellen Server empfangenen Treffer an

- **ADC-Verarbeitungszeit** —Gibt die durchschnittliche Verarbeitungszeit durch die ADC-Instanz an
- **Datenvolumen** —Gibt das gesamte vom virtuellen Server verarbeitete Datenvolumen an.
- **Gesundheitswert** —Gibt den App-Score an
- **Aktueller Status** —Gibt den aktuellen Status des virtuellen Servers an

Service-Metriken

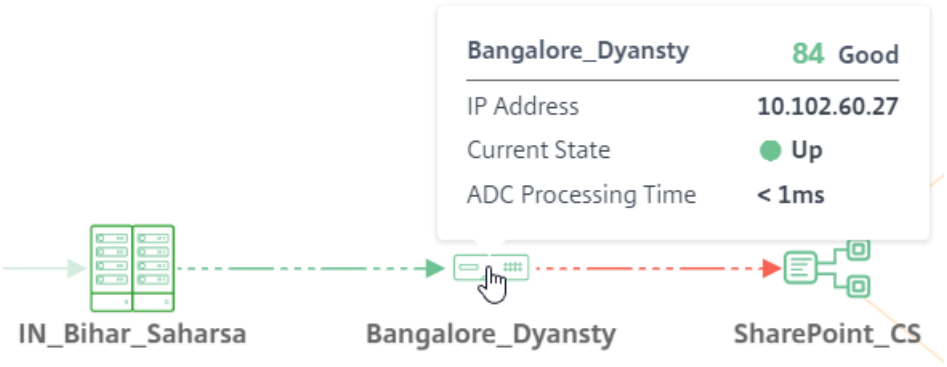
Bewegen Sie den Mauszeiger auf einen Dienst (Webanwendung), um die Metriken anzuzeigen



- **Treffer** —Gibt die Gesamtzahl der vom Dienst empfangenen Treffer an
- **Service-Antwortzeit** —Gibt die durchschnittliche Antwortzeit des Service an
- **Fehler** —Zeigt die Gesamtzahl der vom Service aufgetretenen Fehler an
- **Datenvolumen** —Gibt die Gesamtmenge der vom Service verarbeiteten Daten an

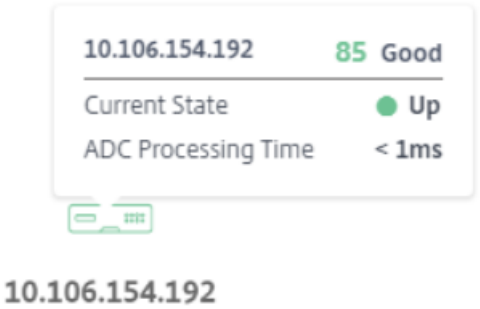
NetScaler ADC-Metriken (nur für GSLB-Anwendungen)

Bewegen Sie den Mauszeiger auf den ADC, um die Metriken anzuzeigen.



- Zeigt den Hostnamen und den aktuellen ADC-Score an. Die Bewertung wird basierend auf den verschiedenen potenziellen Problemen von NetScaler ADC berechnet. Weitere Informationen finden Sie unter Instanz-Score.
- **IP-Adresse** —Bezeichnet die NetScaler ADC IP-Adresse
- **Aktueller Status** —Gibt den NetScaler ADC-Status an, z. B. Up, Down oder Out of Service
- **ADC-Verarbeitungszeit** —Gibt die durchschnittliche Verarbeitungszeit durch die ADC-Instanz an

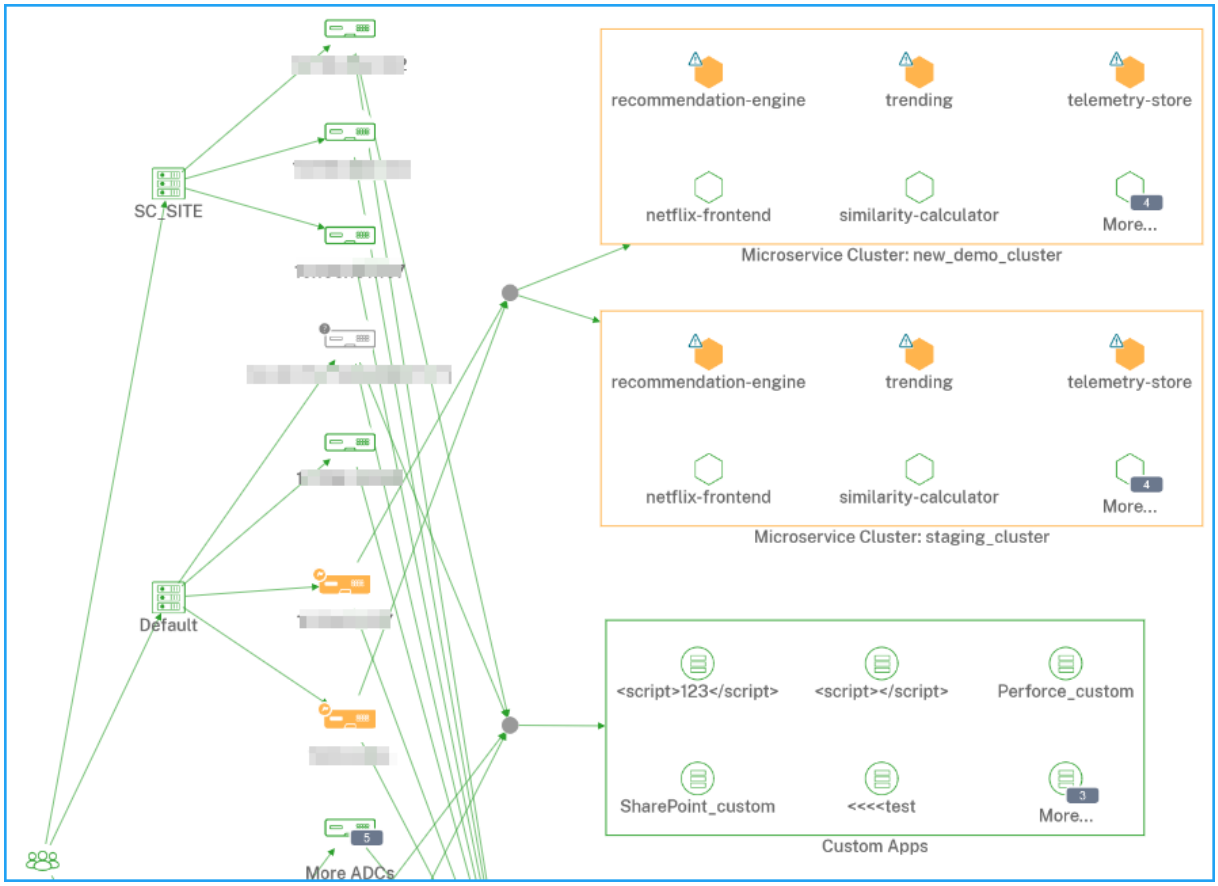
> **Hinweis**
>
> Wenn NetScaler ADC kein Hostname zugewiesen ist:
>
> -NetScaler ADC IP-Adresse wird anstelle des Hostnamens angezeigt.
>
> -In den Metriken werden die NetScaler ADC IP-Adressinformationen nicht angezeigt.



Ganzheitliche Ansicht aller Anwendungen im Service-Graph

February 5, 2024

Navigieren Sie zu **Anwendungen** > **Service Graph** und klicken Sie dann auf **Global**.



Das Servicegriph zeigt für die ausgewählte Zeitdauer Folgendes an:

- Die Region, von der aus die Benutzer auf die spezifische Anwendung zugreifen

Rechenzentren, in denen die NetScaler ADC-Instanzen gehostet werden

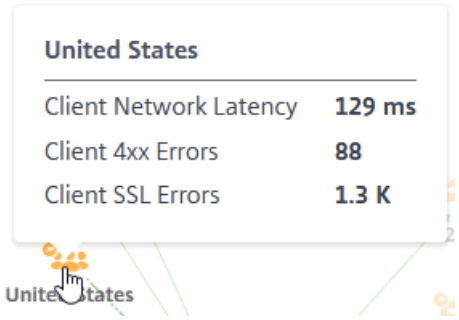
- Gesamt diskrete Anwendungen von allen NetScaler ADC-Instanzen

> **Hinweis**
>
> Wenn eine NetScaler ADC-Instanz keine diskreten Anwendungen hat, ist der Pfeilrand von der NetScaler ADC-Instanz in Richtung des diskreten virtuellen Servers nicht sichtbar

- Gesamtanzahl der benutzerdefinierten Anwendungen aus allen NetScaler ADC-Instanzen
- Die gesamten Microservice-Anwendungen aus der NetScaler ADC CPX-Instanz

Client-Metriken anzeigen

Bewegen Sie den Mauszeiger auf eine Client-Region, um die Metriken anzuzeigen.

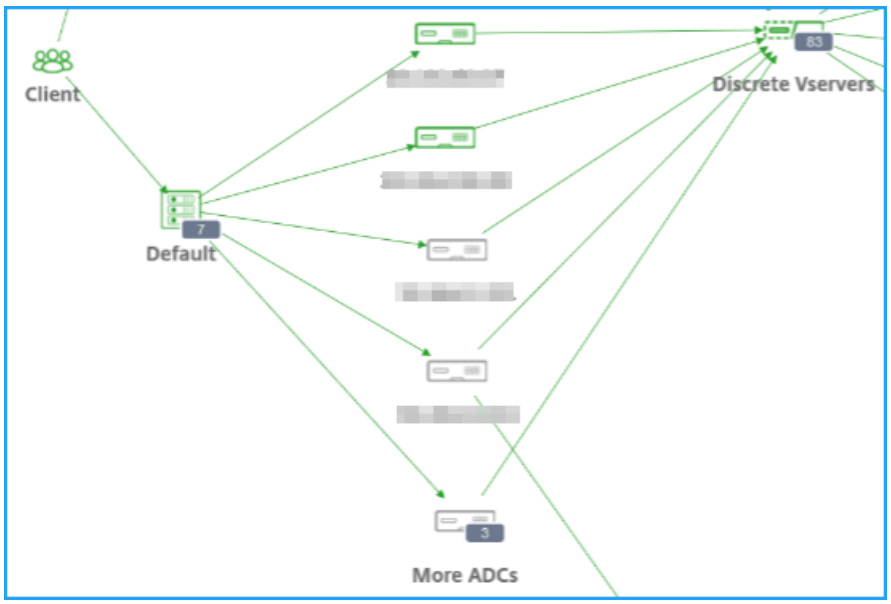


- **Client-Netzwerklatenz** : Gibt die durchschnittliche Clientnetzwerklatenz an.
- **Client 4xx-Fehler** - Zeigt die Gesamtzahl der 4xx-Fehler des Clients an.
- **Client-SSL-Fehler** - Gibt die gesamte Client-SSL-Fehler an.

NetScaler ADC-Details anzeigen

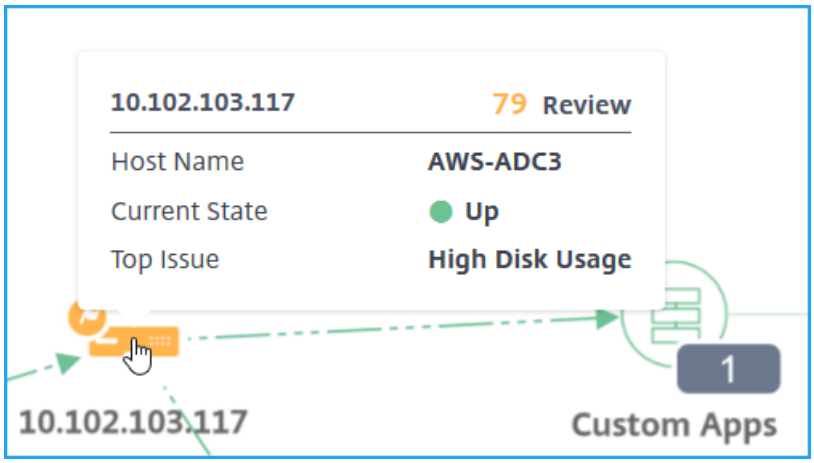
Mit dem Service-Graph können Sie Folgendes anzeigen:

- Das Rechenzentrum gruppiert mit den gesamten NetScaler ADC-Instanzen
- Nur die 4 besten NetScaler ADC-Instanzen mit niedriger Punktzahl aus jedem Rechenzentrum



Klicken Sie auf **Weitere ADCs**, um alle NetScaler ADC-Instanzen anzuzeigen, indem Sie die entsprechenden Registerkarten “Kritisch”, “Prüfen”, “Gut”und “Nicht anwendbar”auswählen.

Bewegen Sie den Mauszeiger auf eine NetScaler ADC-Instanz, um die Metriken anzuzeigen.



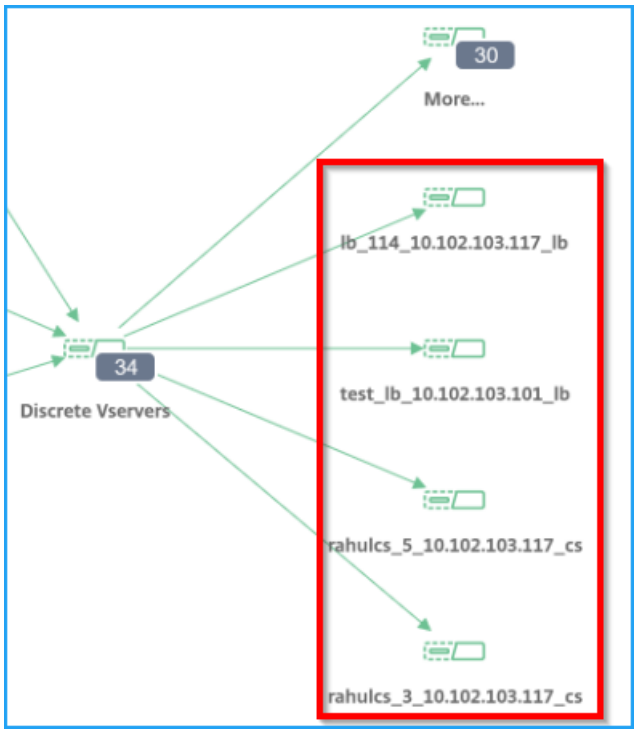
Sie können Folgendes anzeigen:

- IP-Adresse und Punktzahl der NetScaler ADC-Instanz
- **Hostname** —Gibt den Hostnamen an, der der NetScaler ADC-Instanz zugewiesen ist
- **Aktueller Status** —Gibt den aktuellen Status der NetScaler ADC-Instanz an, z. B. “Aufwärts”, “Heruntergefahren”, “Out-of-Service”.
- **Top Problem** —Gibt das höchste Problem an, das sich auf die aktuelle Citrix ADC Bewertung auswirkt.

Klicken Sie auf die **NetScaler ADC-Instanz**, um Instanzdetails wie Instanzbewertung, Schlüsselmetriken und Probleme im Zusammenhang mit der ADC-Instanz anzuzeigen. Weitere Informationen finden Sie unter Anzeigen von Instanzdetails in Infrastructure Analytics.

Diskrete Anwendungen anzeigen

Das Servicegriph zeigt die 4 am häufigsten bewerteten diskreten Anwendungen an.



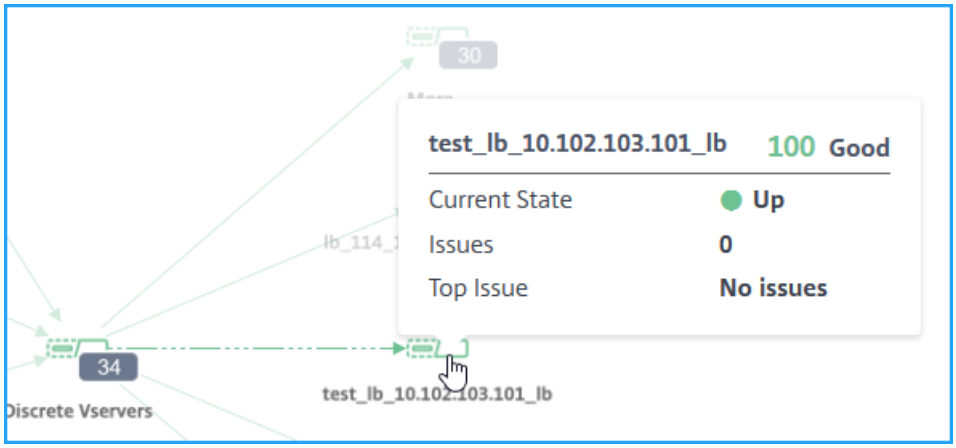
Bedenken Sie, dass Sie die folgenden diskreten Anwendungen haben:

App-Name	Citrix ADC	AppScore	App-Status
App 1	10.102.29.50	35 (Kritisch)	Hoch
App 2	10.102.29.90	100 (Gut)	Runter
App 3	10.102.32.40	49 (Bewertung)	Hoch
App 4	10.102.113.208	92 (Gut)	Runter
App 5	10.102.25.25	86 (Gut)	Hoch
App 6	10.102.29.41	77 (Gut)	Hoch
App 7	10.102.29.102	41 (Bewertung)	Hoch

In diesem Szenario können Sie App1, App3, App6 und App 7 als die vier am besten bewerteten Anwendungen im Service-Diagramm anzeigen.

In ähnlicher Weise können Sie auch die 4 am besten bewerteten Anwendungen für **Custom** - und **Microservices-Anwendungen** anzeigen.

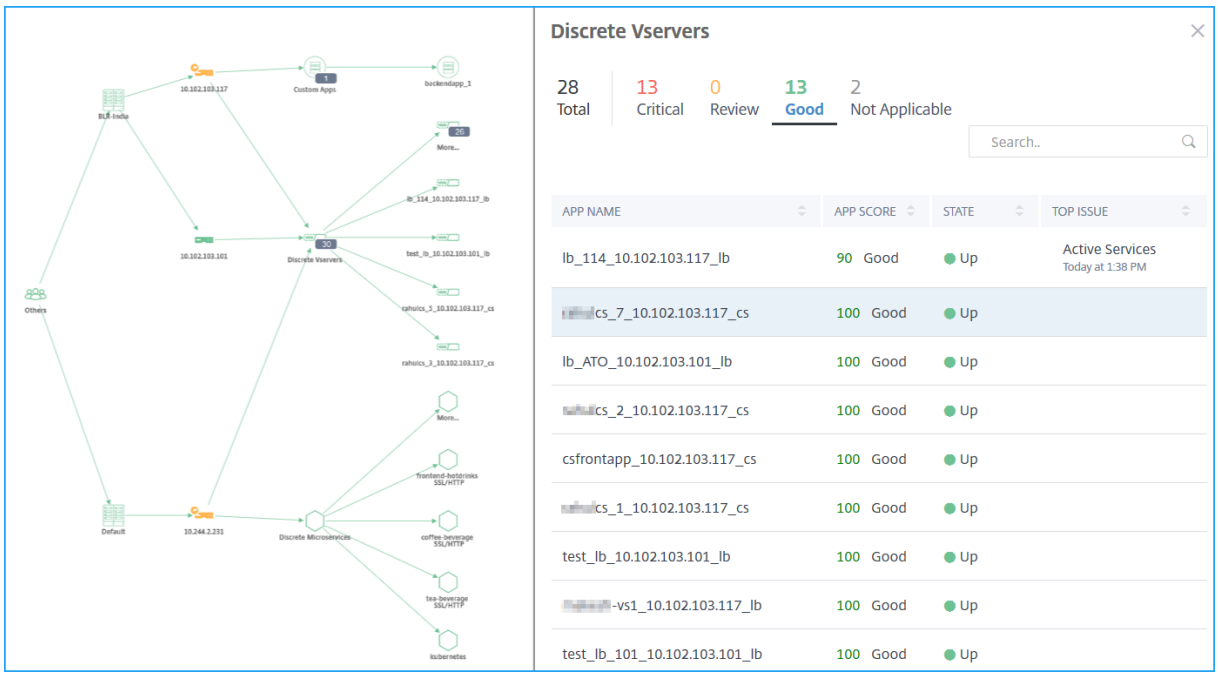
Bewegen Sie den Mauszeiger auf einen Service, um die Metrikinformationen anzuzeigen.



Sie können Folgendes anzeigen:

- Der Name und die Bewertung der Anwendung
- **Aktueller Status** —Zeigt den aktuellen Status der Anwendung an, z. B. Auf oder Ab.
- **Probleme** —Zeigt die Gesamtzahl der Probleme an, die für die Anwendung zutreffen
- **Häufigstes Problem** —Gibt das Hauptproblem an, das sich auf die Gesamtbewertung der Anwendung auswirkt

Klicken Sie auf **Mehr**, um alle diskreten Anwendungen anzuzeigen. Die Seite Diskreter virtueller Server wird wie in der folgenden Abbildung dargestellt angezeigt:

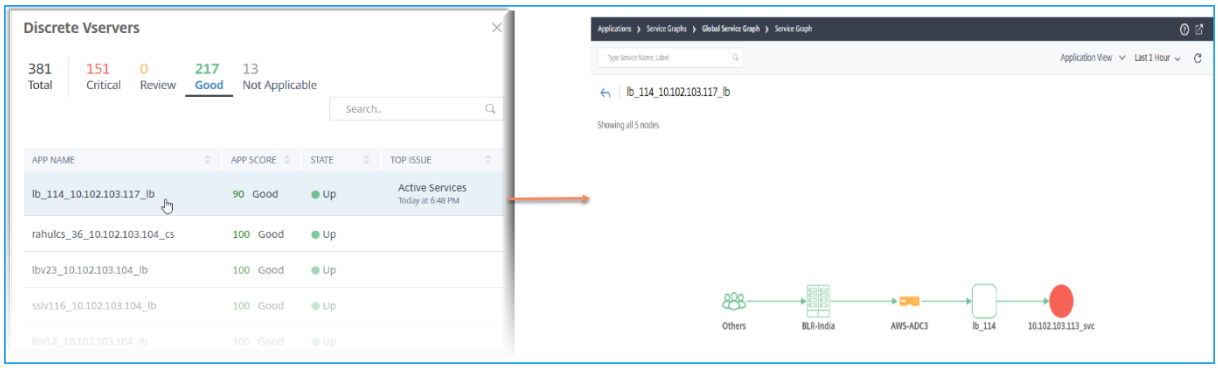


Die virtuellen Server werden dem Status entsprechend angezeigt.

- **Insgesamt** —Gesamtzahl diskreter Anwendungen

- **Kritisch** —App-Punktzahl liegt zwischen 0 und < 40
- **Bewertung** —App-Punktzahl liegt zwischen 40 und < 75
- **Gut** —App-Score ist > 75
- **Nicht zutreffend** —App ist an keinen virtuellen Server gebunden

Sie können auf jede Registerkarte klicken, um die virtuellen Server anzuzeigen. Wenn Sie auf eine Anwendung klicken, wird das Service-Diagramm für die ausgewählte Anwendung angezeigt.



Weitere Informationen finden Sie unter Service Graph für Anwendungen.

Anzeigen von Microservice-Anwendungen

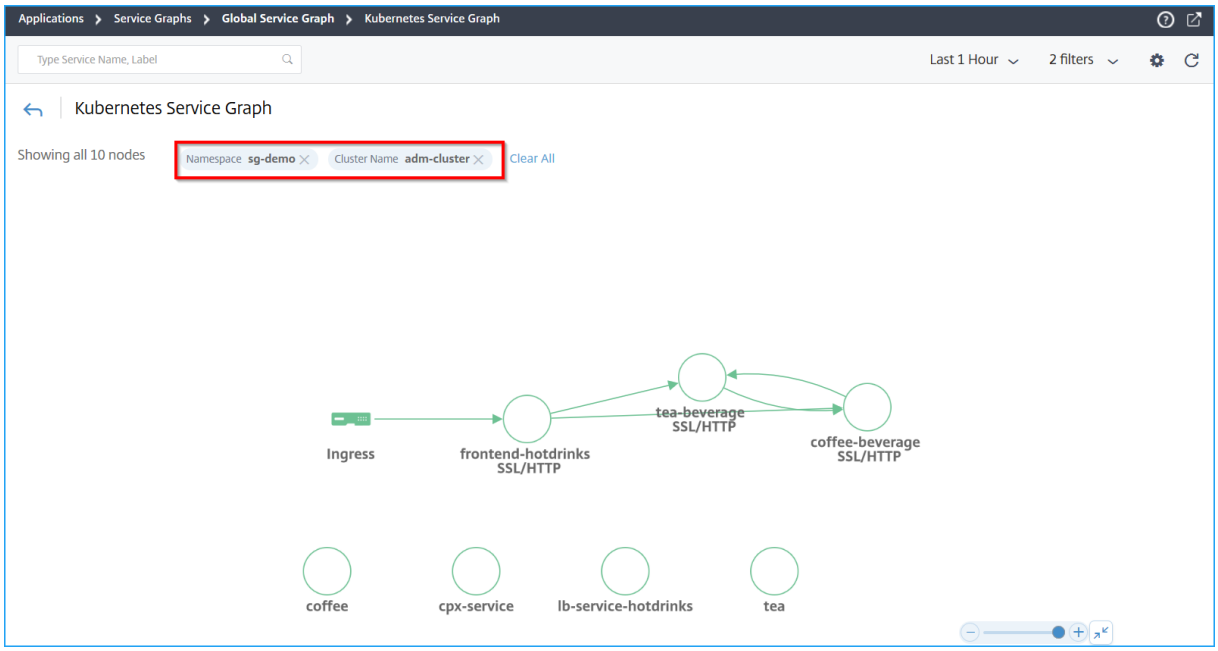
Das Service-Diagramm zeigt auch alle Microservice-Anwendungen an, die zu den Kubernetes-Clustern gehören. Bewegen Sie den Mauszeiger auf einen Service, um die Metrik-Details anzuzeigen.

Sie können Folgendes anzeigen:

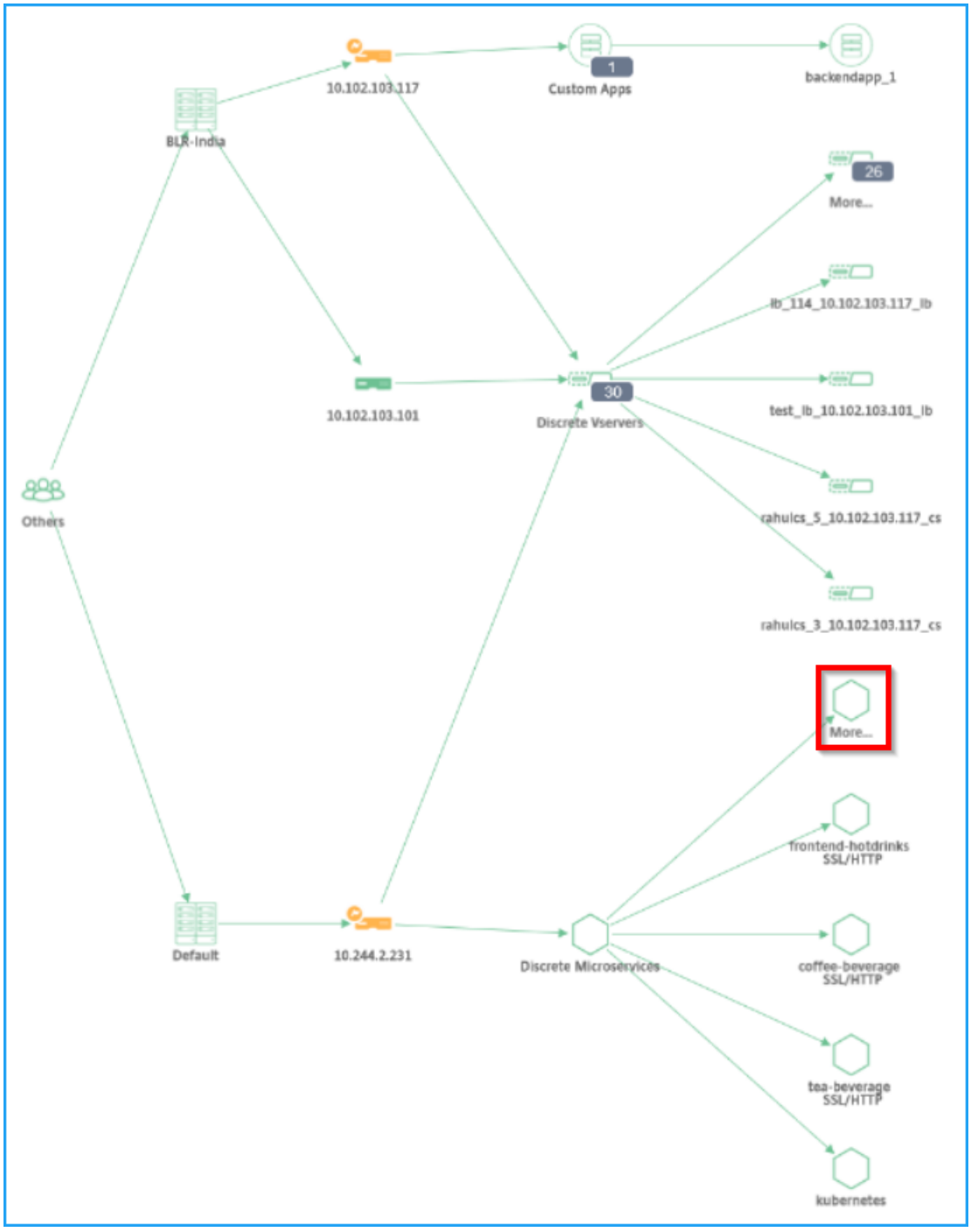
- Der Dienstname
- Das vom Dienst verwendete Protokoll wie SSL, HTTP, TCP, SSL über HTTP
- **Treffer** —Die Gesamtzahl der vom Dienst erhaltenen Treffer
- **Reaktionszeit des Service** —Die durchschnittliche Reaktionszeit, die vom Service in Anspruch genommen wurde.

  (Antwortzeit = Client RTT + Anfrage letztes Byte —erstes Byte anfordern)
- **Errors** —Die Gesamtzahl der Fehler wie 4xx, 5xx usw.
- **Datenvolumen** —Das Gesamtvolumen der vom Dienst verarbeiteten Daten
- **Namespace** —Der Namensraum des Service
- **Clustername** —Der Clustername, in dem der Dienst gehostet wird
- **SSL-Serverfehler** —Die gesamten SSL-Fehler vom Dienst

Wenn Sie auf einen Dienst klicken, wird das Kubernetes-Dienstdiagramm für den ausgewählten Dienst zusammen mit den angewendeten Dienstnamespace- und Clusternamenfiltern angezeigt.



Klicken Sie auf **Mehr**, um das Kubernetes-Dienstdiagramm anzuzeigen, das alle Dienste enthält. Weitere Informationen zum Kubernetes-Servicediagramm finden Sie unter Service-Diagramm für Cloud-native Anwendungen.

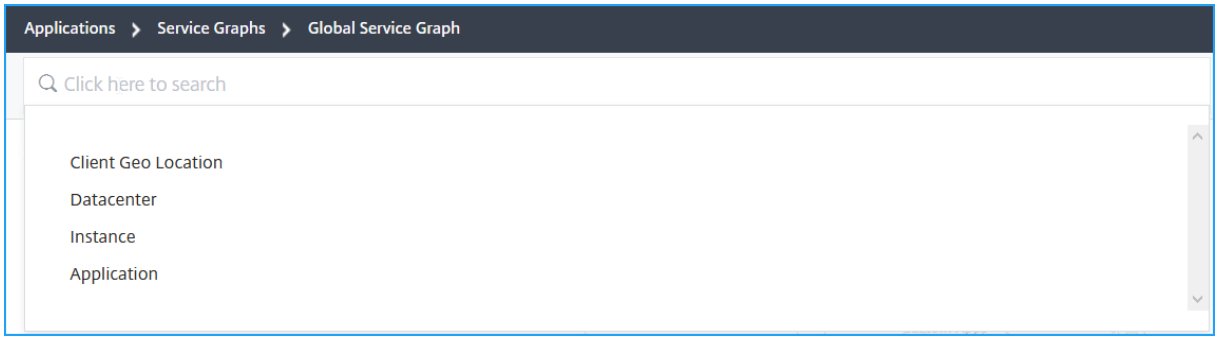


Suchleiste um Ergebnisse zu filtern

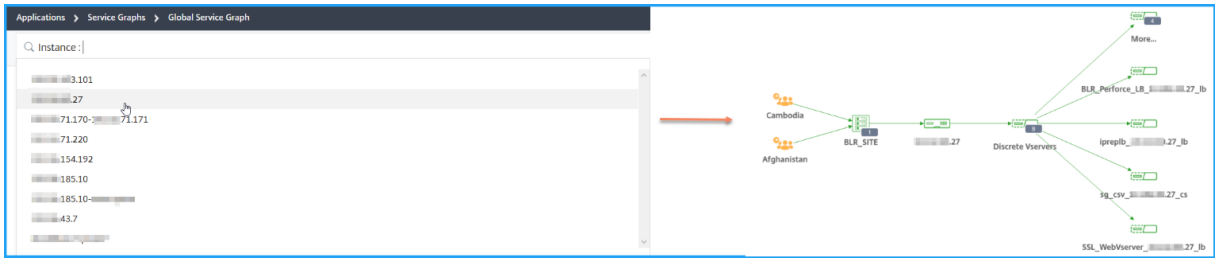
Sie können die Suchleiste verwenden, um Ergebnisse zu filtern. Als Administrator können Sie mit dieser Suchleiste schnell auf eine bestimmte Instanz/einen bestimmten Client/eine bestimmte Anwendung/Rechenzentrum eingrenzen, wenn Sie:

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

Platzieren Sie den Mauszeiger auf die Suchleiste und wählen Sie die Kategorie aus, in der Sie den Filter erstellen möchten.



Wenn Sie beispielsweise eine bestimmte ADC-Instanz anzeigen möchten, wählen Sie Instanz in der Suchleiste aus und wählen Sie die IP-Adresse der Instanz aus. Das globale Servicediagramm zeigt die ausgewählte Instanz und die zugehörigen Anwendungen, Rechenzentren und Kundenstandorte an.



StyleBooks

February 5, 2024

StyleBooks vereinfachen die Verwaltung komplexer NetScaler ADC Konfigurationen für Ihre Anwendungen. Ein StyleBook ist eine Vorlage, mit der Sie NetScaler ADC-Konfigurationen erstellen und verwalten können. Sie können ein StyleBook zum Konfigurieren einer bestimmten Funktion von NetScaler ADC erstellen, oder Sie können ein StyleBook entwerfen, um Konfigurationen für eine Bereitstellung von Unternehmensanwendungen wie Microsoft Exchange oder Lync zu erstellen.

StyleBooks passen gut zu den Prinzipien von Infrastructure-as-Code, die von DevOps-Teams praktiziert werden, wo Konfigurationen deklarativ und versionsgesteuert sind. Die Konfigurationen werden ebenfalls wiederholt und als Ganzes bereitgestellt. StyleBooks bieten folgende Vorteile:

- **Deklarativ**: StyleBooks werden in einer deklarativen statt zwingenden Syntax geschrieben. Mit StyleBooks können Sie sich auf die Beschreibung des Ergebnisses oder des "gewünschten Status"der Konfiguration konzentrieren und nicht auf die Schritt-für-Schritt-Anweisungen, wie Sie diese auf einer bestimmten NetScaler ADC Instanz erreichen können. Citrix Application Delivery Management (ADM) berechnet den Unterschied zwischen dem vorhandenen Status in einem Citrix ADC und dem von Ihnen angegebenen Status und nimmt die erforderlichen Änderungen an der Infrastruktur vor. Da StyleBooks eine deklarative Syntax verwenden, die in YAML geschrieben wird, können Komponenten eines StyleBook in beliebiger Reihenfolge angegeben werden, und NetScaler ADM bestimmt die richtige Reihenfolge basierend auf den berechneten Abhängigkeiten.
- **Atomic**: Wenn Sie StyleBooks zum Bereitstellen von Konfigurationen verwenden, wird die vollständige Konfiguration bereitgestellt oder keine davon bereitgestellt. Dadurch wird sichergestellt, dass die Infrastruktur immer in einem konsistenten Zustand bleibt.
- **Versioniert**: Ein StyleBook hat einen Namen, einen Namespace und eine Versionsnummer, die es eindeutig von jedem anderen StyleBook im System unterscheidet. Jede Änderung an einem StyleBook erfordert eine Aktualisierung seiner Versionsnummer (oder seines Namens oder Namespace), um dieses eindeutige Zeichen zu erhalten. Mit dem Versionsupdate können Sie auch mehrere Versionen desselben StyleBook verwalten.
- **Composable**: Nachdem ein StyleBook definiert wurde, kann das StyleBook als Einheit zum Erstellen anderer StyleBooks verwendet werden. Sie können vermeiden, gängige Konfigurationsmuster zu wiederholen. Es ermöglicht Ihnen auch, Standardbausteine in Ihrer Organisation festzulegen. Da StyleBooks versioniert sind, führen Änderungen an vorhandenen StyleBooks zu neuen StyleBooks, wodurch sichergestellt wird, dass abhängige StyleBooks niemals unbeabsichtigt beschädigt werden.
- **App-Centric**: StyleBooks können verwendet werden, um die NetScaler ADC-Konfiguration einer vollständigen Anwendung zu definieren. Die Konfiguration der Anwendung kann mithilfe von Parametern abstrahiert werden. Daher können Benutzer, die Konfigurationen aus einem StyleBook erstellen, mit einer einfachen Schnittstelle interagieren, die darin besteht, einige Parameter zu füllen, um eine komplexe Citrix ADC Konfiguration zu erstellen. Konfigurationen, die aus StyleBooks erstellt werden, sind nicht an die Infrastruktur gebunden. Eine einzelne Konfiguration kann somit auf einem oder mehreren Citrix ADCs bereitgestellt werden und kann auch zwischen Instanzen verschoben werden.
- **Automatisch generierte Benutzeroberfläche**: NetScaler ADM generiert automatisch UI-Formulare, die zum Ausfüllen der Parameter des StyleBook verwendet werden, wenn die

Konfiguration über die NetScaler ADM GUI erfolgt. StyleBook-Autoren müssen keine neue GUI-Sprache erlernen oder Benutzeroberflächenseiten und -formulare separat erstellen.

- **API-gesteuert**: Alle Konfigurationsvorgänge werden mithilfe der NetScaler ADM-GUI oder über REST-APIs unterstützt. Die APIs können im synchronen oder asynchronen Modus verwendet werden. Zusätzlich zu den Konfigurationsaufgaben können Sie mit den StyleBooks-APIs auch das Schema (Parameterbeschreibung) eines beliebigen StyleBooks zur Laufzeit ermitteln.

Sie können ein StyleBook verwenden, um mehrere Konfigurationen zu erstellen. Jede Konfiguration wird als Config Pack gespeichert. Angenommen, Sie haben ein StyleBook, das eine typische HTTP-Load Balancing-Anwendungskonfiguration definiert. Sie können eine Konfiguration mit Werten für die Lastausgleichseinheiten erstellen und sie auf einer Citrix ADC Instanz ausführen. Diese Konfiguration wird als Konfigurationspaket gespeichert. Sie können dasselbe StyleBook verwenden, um eine andere Konfiguration mit unterschiedlichen Werten zu erstellen und diese auf derselben oder einer anderen Citrix ADC Instanz auszuführen. Für diese Konfiguration wird ein neues Konfigurationspaket erstellt. Ein Konfigurationspaket wird sowohl auf Citrix ADM als auch auf der Citrix ADC Instanz gespeichert, auf der die Konfiguration ausgeführt wird.

Sie können entweder Standard-StyleBooks verwenden, die im Lieferumfang von NetScaler ADM enthalten sind, um Konfigurationen für Ihre Bereitstellung zu erstellen, oder eigene StyleBooks entwerfen und in NetScaler ADM importieren. Sie können die StyleBooks verwenden, um Konfigurationen entweder mithilfe der NetScaler ADM GUI oder mithilfe von APIs zu erstellen.

Dieses Dokument enthält die folgenden Informationen:

- So zeigen Sie StyleBooks an
- Standard-StyleBooks
- Für Geschäftsanwendungen entwickelte Stylebooks
- Benutzerdefinierte StyleBooks
- APIs in StyleBooks
- StyleBooks Grammatik

StyleBook-Kategorien

February 5, 2024

In Citrix Application Delivery Management (ADM) gibt es zwei StyleBook-Kategorien. Sie sind die Standard-StyleBooks und die benutzerdefinierten StyleBooks. Unabhängig davon, ob es sich um ein Standard- oder ein benutzerdefiniertes StyleBook handelt, ist ein StyleBook entweder ein öffentliches oder ein privates In NetScaler ADM können Sie alle StyleBooks anzeigen, die im System

vorhanden sind, unabhängig von ihrem Typ oder Sichtbarkeitsstatus. Sie können auch eine grafische Darstellung anzeigen, wie StyleBooks miteinander verbunden sind.

Dieses Dokument erklärt die verschiedenen Arten von StyleBooks. Außerdem werden die folgenden Aktionen erläutert, die Sie in den StyleBooks von NetScaler ADM ausführen können:

- Laden Sie ein benutzerdefiniertes StyleBook herunter und nehmen Sie Änderungen vor, oder erstellen Sie ein StyleBook basierend auf einem vorhandenen.
- Blenden Sie die ADM-Standard-StyleBooks aus.
- Löschen Sie ein benutzerdefiniertes StyleBook aus NetScaler ADM.
- Fügen Sie den StyleBooks Tags hinzu.

Standard- und benutzerdefinierte StyleBooks

- **StandardstyleBooks** sind die StyleBooks, die mit NetScaler ADM ausgeliefert werden, und sie ermöglichen es Ihnen, Konfigurationen zu erstellen, die Sie auf Ihren NetScaler ADC-Instanzen bereitstellen können. Sie können Standard-StyleBooks nicht löschen, aber Sie können sie in der ADM-GUI ausblenden.
- **Benutzerdefinierte StyleBooks** sind Ihre eigenen StyleBooks, die Sie in NetScaler ADM importiert haben.

Sowohl Standard- als auch benutzerdefinierte StyleBooks können entweder öffentlich oder privat sein.

Öffentliche und private StyleBooks

StyleBooks, aus denen Sie Konfigurationspakete erstellen können, können als **öffentliche** StyleBooks kategorisiert werden. Das heißt, sie stehen alle für Ihre direkte Verwendung zur Verfügung, um Konfigurationen über die NetScaler ADM GUI und APIs zu erstellen.

Einige StyleBooks werden jedoch als Bausteine für andere StyleBooks verwendet. Solche StyleBooks sind als **privat**gekennzeichnet. Die privaten StyleBooks können nicht direkt verwendet werden, um Konfigurationspakete aus der NetScaler ADM-Benutzeroberfläche zu erstellen. Sie können diese StyleBooks jedoch weiterhin auf NetScaler ADM anzeigen und anzeigen. Um Ihre benutzerdefinierten StyleBooks als **privat**zu markieren, setzen Sie das private Attribut im StyleBook auf **true**. Sie können weiterhin private StyleBooks verwenden, um Konfigurationspakete mit den NetScaler ADM APIs zu erstellen.

Beispiel für ein StyleBook, das als privat markiert ist

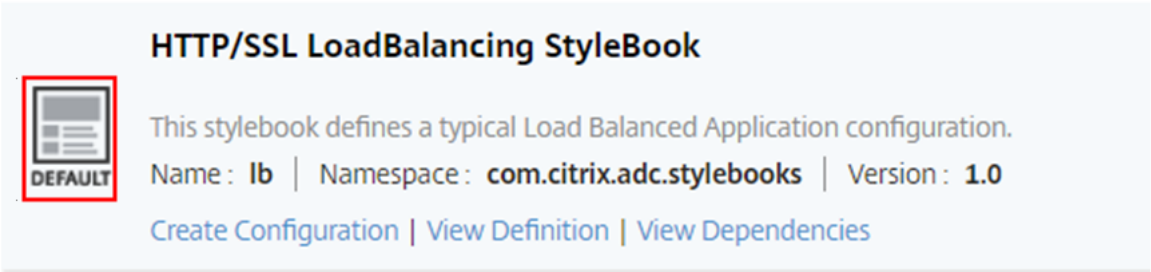

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: |
    This StyleBook defines a simple load balancing configuration and is
        a building block to build other load balancing configurations.
schema-version: "1.0"
private: true
<!--NeedCopy-->
```

StyleBooks ansehen

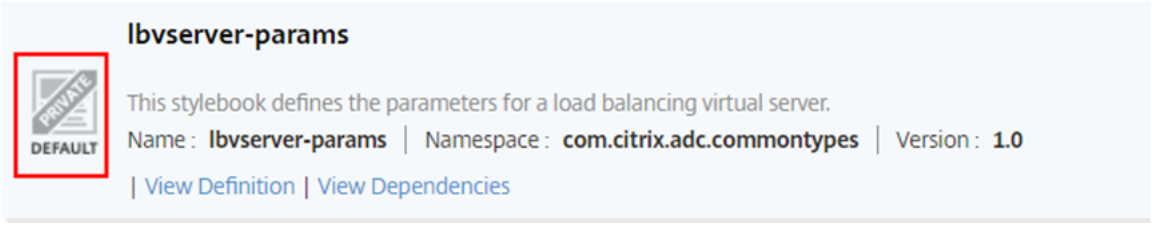
Die Anzahl der StyleBooks - sowohl Standard als auch Private - nimmt in NetScaler ADM zu. Möglicherweise möchten Sie nach dem bestimmten StyleBook suchen, auf das Sie zugreifen möchten. Möglicherweise möchten Sie auch beide StyleBook-Typen separat anzeigen.

Wenn Sie in Citrix ADM zu **Applications** > **StyleBooks**navigieren, können Sie eine Liste der StyleBooks anzeigen, die im System vorhanden sind.

Ein öffentliches Standard-StyleBook hat das folgende Symbol im Bedienfeld:

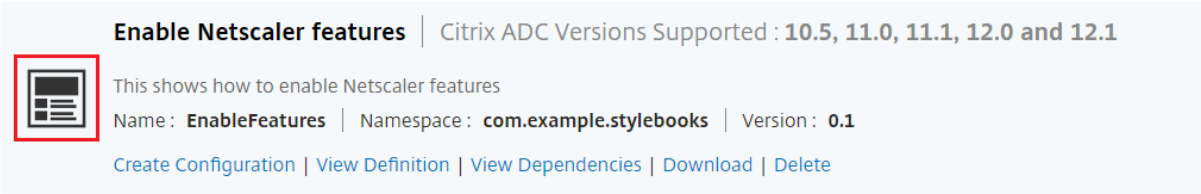


Während ein privates Standard-StyleBook ein Symbol hat, das es als privates StyleBook deklariert:

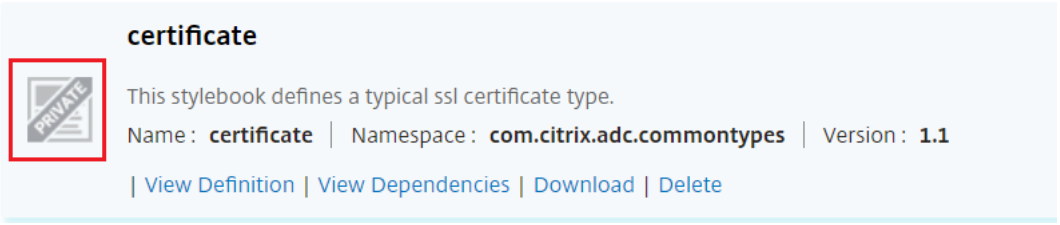


Während Sie die Definition und Abhängigkeiten eines privaten StyleBook anzeigen können, können Sie mit der GUI keine Konfigurationspakete aus einem privaten StyleBook erstellen. Der Hauptzweck eines privaten StyleBook besteht darin, es als Baustein für ein anderes StyleBook zu verwenden. Die Verwendung der building-blocks-stylebooks fördert die Wiederverwendung gängiger Konfigurationsmuster.

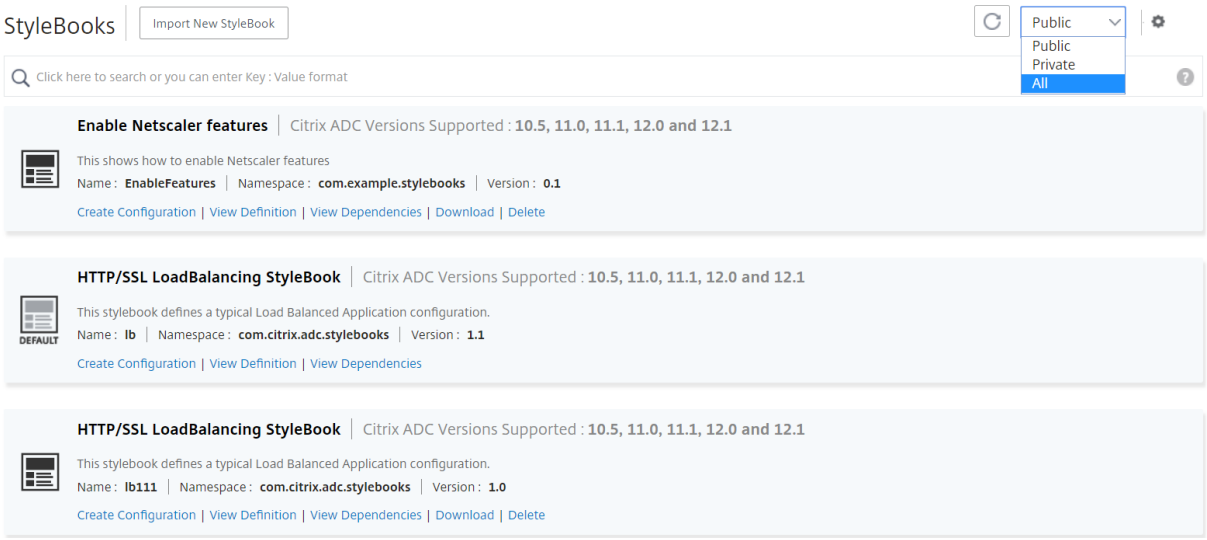
Ein benutzerdefiniertes öffentliches StyleBook hat ein anderes Symbol, wie in der folgenden Abbildung gezeigt:



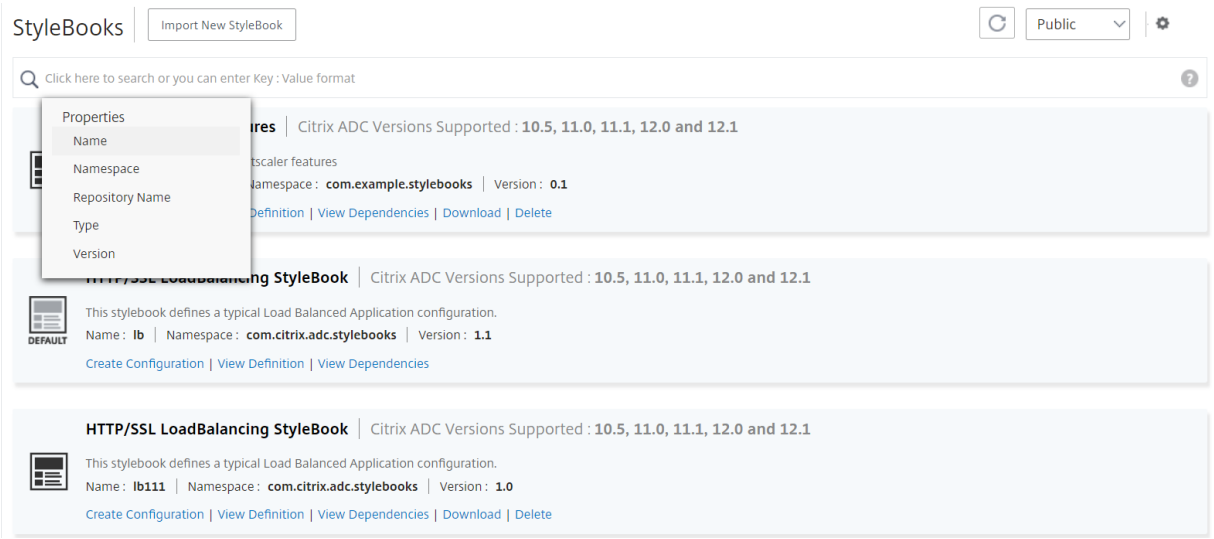
Während ein benutzerdefiniertes privates StyleBook mit diesem Symbol angezeigt wird:



Rechts oben auf der Seite sehen Sie eine Option, um den Typ der anzuzeigenden StyleBooks auszuwählen. Es gibt drei Optionen - alle, öffentliche oder private StyleBooks. Klicken Sie auf eine der Optionen.



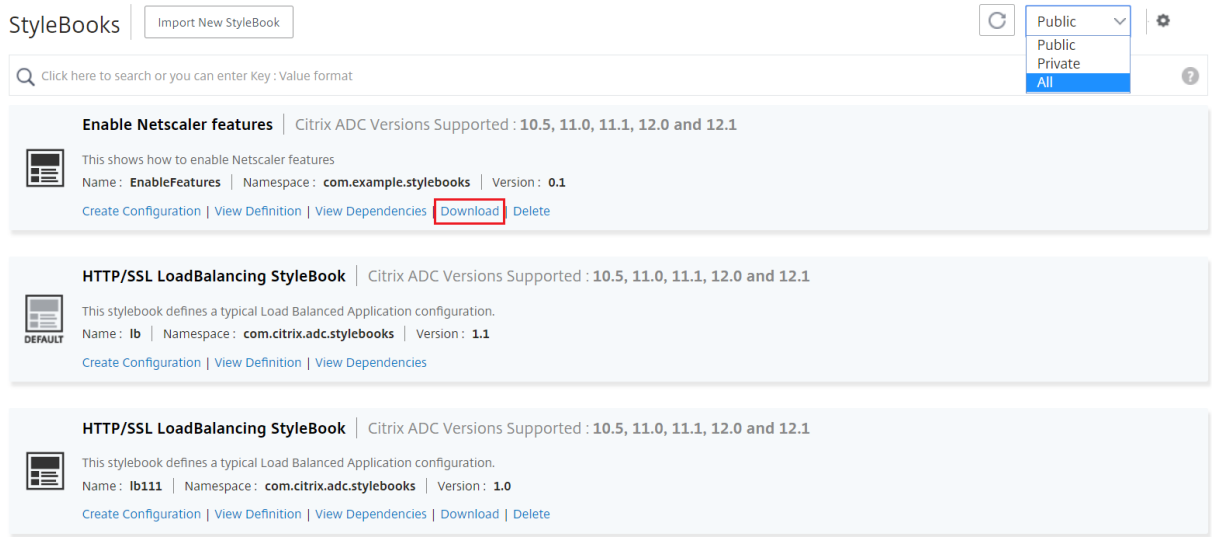
Sie können auch nach einem bestimmten StyleBook suchen, indem Sie auf das Suchsymbol klicken. Sie können nach Namen, Namespace und Versionsattributen oder einer Kombination dieser Optionen suchen. Bei der Suche wird die Groß- und Kleinschreibung nicht berücksichtigt.



Benutzerdefinierte StyleBooks herunterladen

Um die benutzerdefinierten StyleBooks von NetScaler ADM herunterzuladen, navigieren Sie zu **Anwendungen** > **StyleBooks** > **Configurations**. Aktivieren Sie in der Liste der StyleBooks, die auf der rechten Seite angezeigt werden, die Option zum Herunterladen der benutzerdefinierten StyleBooks. Klicken Sie auf **Download**. Wenn das StyleBook abhängige benutzerdefinierte StyleBooks hat, können Sie die abhängigen StyleBooks in das heruntergeladene Bundle aufnehmen.

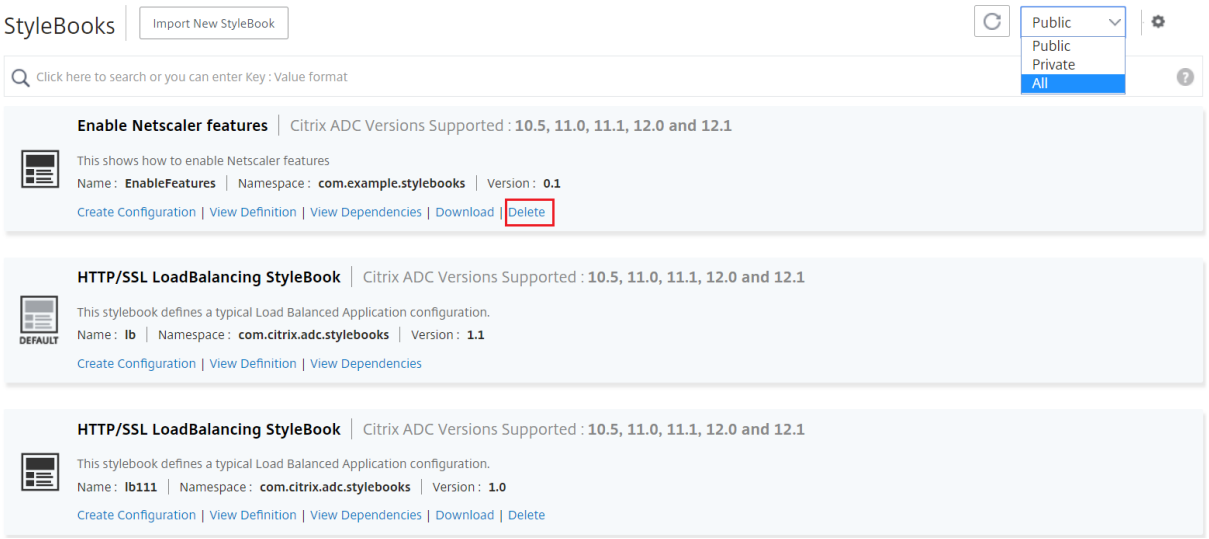
> **Hinweis:**
>
> Sie können benutzerdefinierte StyleBooks herunterladen, die entweder als öffentlich oder privat gekennzeichnet sind.



> **Hinweis:**
>
> NetScaler ADM Standard-StyleBooks können nicht heruntergeladen werden. Sie können ihre Definitionen und Abhängigkeiten einsehen. Klicken Sie dazu im StyleBook-Bedienfeld auf "**Definition anzeigen**"**und "Abhängigkeiten** anzeigen".

Benutzerdefinierte StyleBooks löschen

Sie können ein benutzerdefiniertes StyleBook auch löschen, indem Sie auf die Schaltfläche **Löschen** klicken. In einem Popup-Fenster werden Sie aufgefordert, zu bestätigen, ob Sie das StyleBook aus NetScaler ADM entfernen möchten. Wenn das StyleBook andere benutzerdefinierte StyleBooks verwendet, können Sie diese StyleBooks entfernen, indem Sie das Kontrollkästchen aktivieren.



> **Hinweis:**
>
> Löschen Sie kein benutzerdefiniertes StyleBook, wenn es abhängige StyleBooks in NetScaler ADM hat. Andernfalls würde es die vorhandenen StyleBooks beschädigen.

Anzeigen von StyleBook-Abhängigkeiten

Eine wichtige und leistungsstarke Funktion von StyleBooks ist, dass sie als Bausteine für andere StyleBooks verwendet werden können. Sie können ein StyleBook in ein anderes StyleBook importieren. Ein importiertes StyleBook ist als Typ deklariert und wird von Komponenten oder Parametern des zweiten StyleBook verwendet. Sie können die vorhandenen Standard-StyleBooks in NetScaler ADM untersuchen, um zu erfahren, wie ein StyleBook auf einem anderen StyleBook aufgebaut werden kann.

Mit NetScaler ADM können Sie eine grafische Darstellung der Verbindung von StyleBooks anzeigen. Diese Darstellung ist besonders nützlich für komplexe StyleBooks, die mit anderen StyleBooks als Bausteine erstellt werden. Wenn Sie das Abhängigkeitsdiagramm betrachten, ist es möglich, die Beziehungen und Abhängigkeiten zwischen mehreren StyleBooks zu sehen.

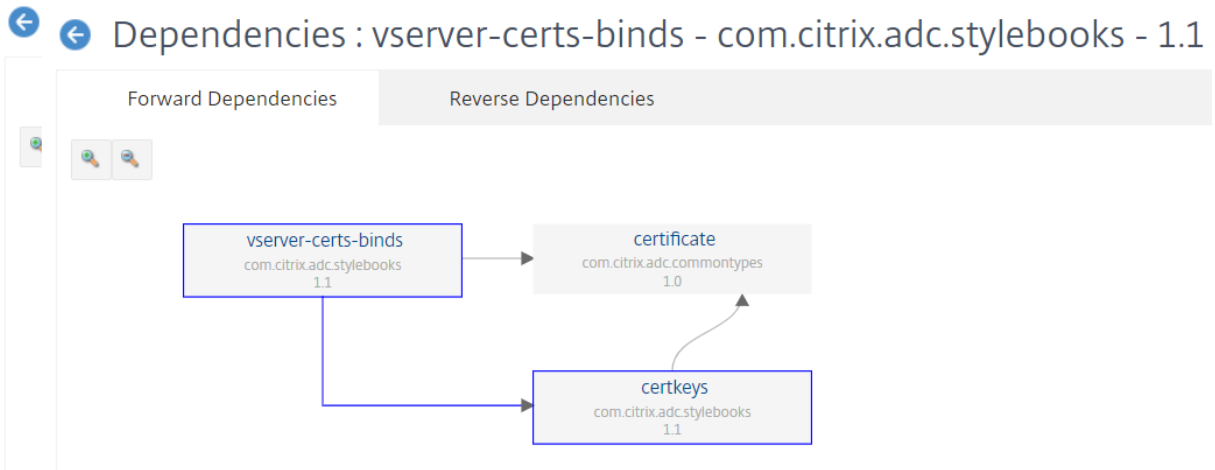
Ein von anderen StyleBooks verwendetes StyleBook kann nicht aus dem System entfernt werden, da es die vorhandenen StyleBooks beschädigen würde. Mithilfe der Abhängigkeitsdiagrammanzeige können Sie ermitteln, welche StyleBooks das Entfernen eines StyleBook verhindern.

StyleBook-Abhängigkeiten anzeigen

Navigieren Sie in Citrix ADM zu **Anwendungen** > **StyleBooks**. Auf der Seite StyleBooks werden alle StyleBooks angezeigt, die für die Verwendung in Citrix ADM verfügbar sind. Scrollen Sie nach unten und finden Sie Ihr StyleBook. Die **StyleBook-Kachel** zeigt Links zum Erstellen einer Konfiguration, zum Anzeigen der StyleBook-Definition und zum Anzeigen der StyleBook-Abhängigkeiten an. Klicken Sie **auf Abhängigkeiten anzeigen**.

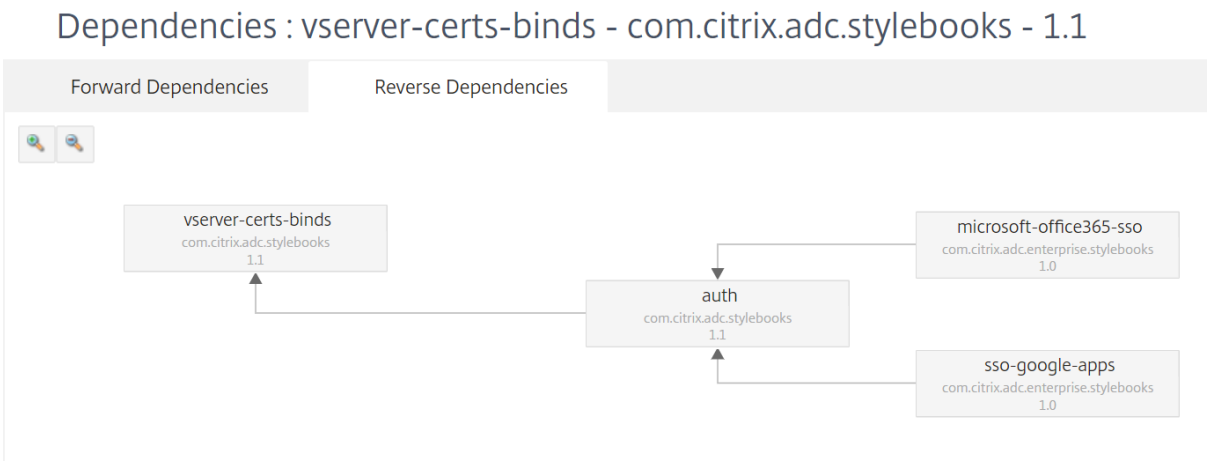
Vorwärtsabhängigkeiten

Auf der Registerkarte **Abhängigkeiten weiterleiten** können Sie die verschiedenen Standard-StyleBooks anzeigen, die Ihr StyleBook verwendet. Folgen Sie den Pfeilen, um das StyleBook zu finden, das ein StyleBook verwendet. Wenn Sie mit der Maus auf einen der Pfeile zeigen, werden der Pfeil und die StyleBooks, die miteinander verbunden sind, hervorgehoben. Sie können auch auf die StyleBook-Namen klicken, um die Definition dieses StyleBooks anzuzeigen.



Umgekehrte Abhängigkeiten

Auf der Registerkarte **Abhängigkeiten umkehren** können Sie die StyleBooks, die Ihr StyleBook verwenden, grafisch anzeigen. Wenn Sie den Pfeilen folgen, können Sie sehen, dass alle StyleBooks in der Anzeige auf Ihr StyleBook zeigen. Einige StyleBooks verwenden möglicherweise direkt das StyleBook und einige StyleBooks verwenden das StyleBook möglicherweise über ein anderes StyleBook.



ADC-Konfiguration anhand des Konfigurationspakets überwachen

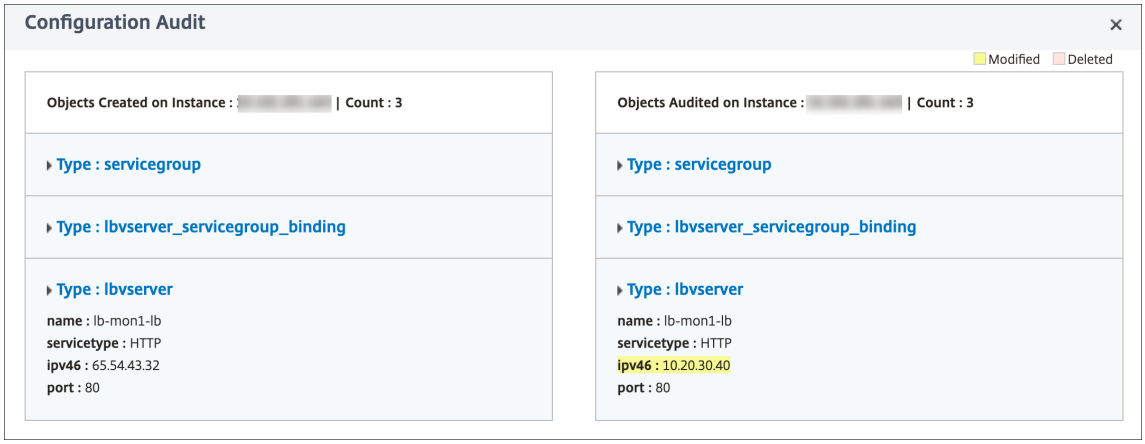
Sie können die von einem StyleBook-Konfigurationspaket vorgenommenen Änderungen mit der aktuellen ADC-Konfiguration vergleichen. Mit diesem Vergleich können Sie Folgendes tun:

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

Um die Änderungen des Konfigurationspakets mit der ADCs-Konfiguration zu vergleichen, führen Sie die folgenden Schritte aus.

1. Navigieren Sie zu **Anwendungen** > **StyleBooks** > **Konfigurationen**.
2. Klicken Sie auf **Konfigurationsüberprüfung**.

   Auf der Seite “Konfigurationsüberwachung”werden die erstellten und überwachten Objekte angezeigt.

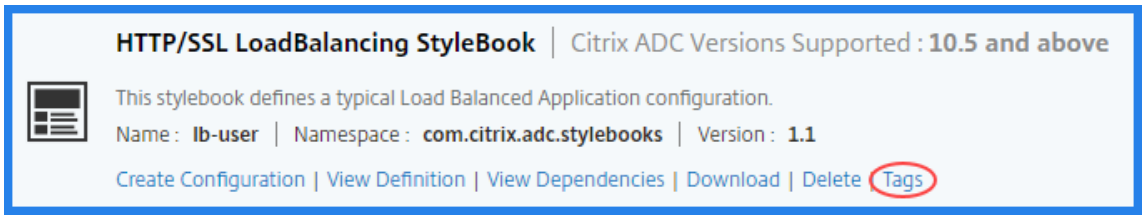


Erstellen Sie ein Tag für das StyleBook

Sie können jedem StyleBook in NetScaler ADM Tags hinzufügen. Tags sind Schlüssel-Wert-Paare, mit denen Sie StyleBooks nach verschiedenen Kriterien gruppieren können. Sie können diese Tags verwenden, während Sie in NetScaler ADM nach StyleBooks suchen oder filtern.

So fügen Sie dem StyleBook ein Tag hinzu:

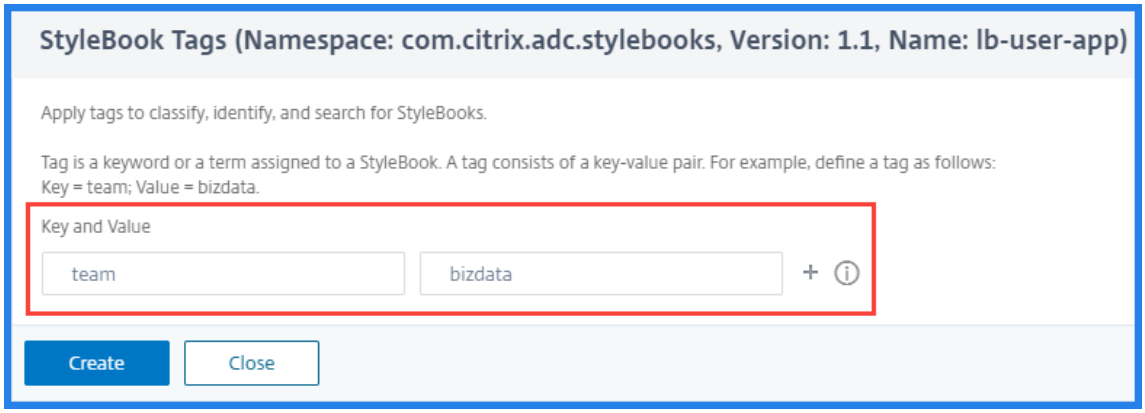
1. Navigieren Sie zu **Applications** > **StyleBooks**.
2. Wählen Sie im StyleBook **Tags** aus, für das Sie Tags hinzufügen möchten.



   Sie können allen Arten von StyleBooks Tags hinzufügen.

3. Geben Sie die erforderlichen **Schlüssel-** und **Wert-Informationen** an, mit denen Sie das StyleBook filtern können.

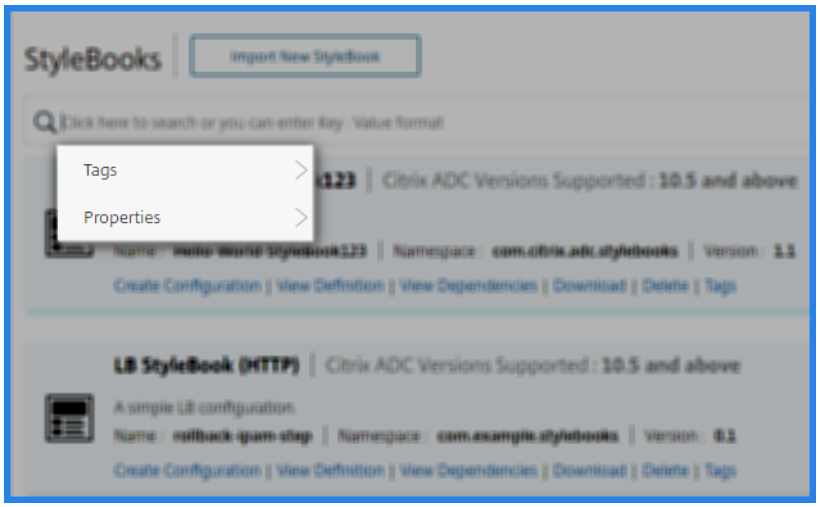
   Beispiel: Schlüssel=Team und Wert=BizData



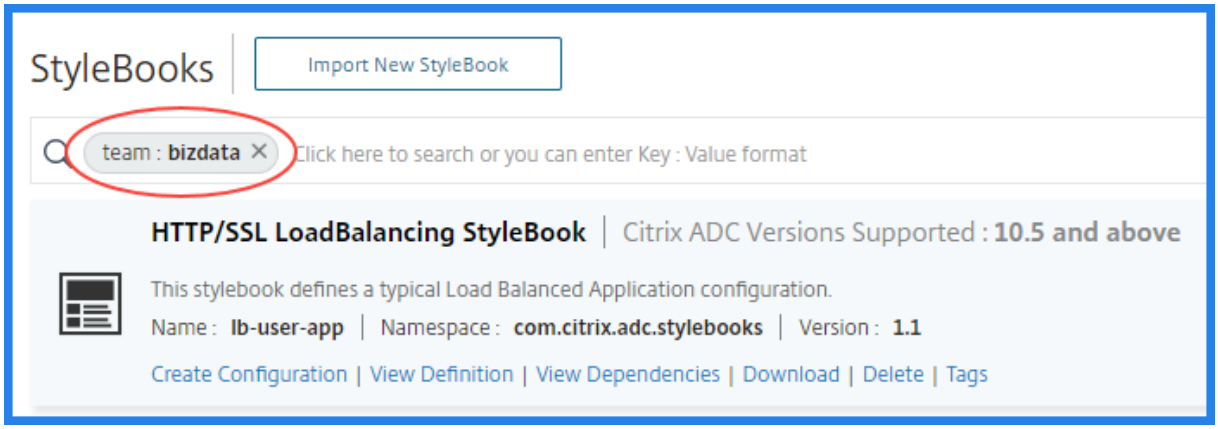
Um weitere Tags hinzuzufügen, klicken Sie auf **+**.

4. Klicken Sie auf **Erstellen**.

Um StyleBooks mithilfe von Tags zu filtern, klicken Sie in der Suchleiste auf **Tags** und wählen Sie Schlüssel und Wert aus der Liste aus. Die StyleBooks, die mit dem angegebenen Tag übereinstimmen, werden angezeigt.



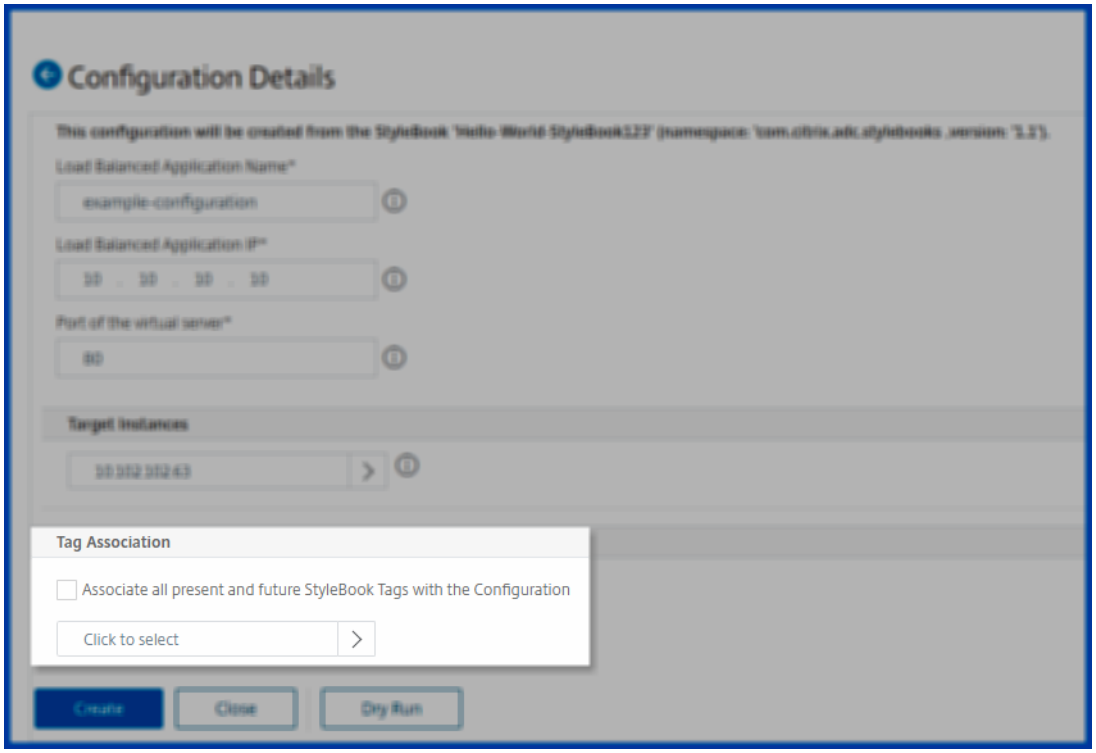
Im Folgenden finden Sie ein Beispiel für die StyleBooks, die ein Tag wo `key=team` und haben `value =bizdata`:



Sie können die StyleBook-Tags seinem Konfigurationspaket zuordnen. Sie können also die Konfigurationspakete mithilfe der StyleBook-Tags selbst durchsuchen.

Wenn Sie ein Konfigurationspaket erstellen, verwenden Sie eine der folgenden Optionen im Abschnitt "**Tag-Zuordnung** ":

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



Importieren und Synchronisieren von StyleBooks aus GitHub-Repository

February 5, 2024

Stellen Sie sich ein Szenario vor, in dem Sie CI/CD-Prozesse für Ihre Entwicklung verwenden. Oder ein Szenario, in dem Sie den gesamten Anwendungsquellcode und die Bereitstellungsobjekte in GitHub verwalten.

Im GitHub-Repository haben Sie möglicherweise mehrere StyleBooks für die Bereitstellung der Citrix ADC Konfigurationen und die Verwaltung dieser StyleBooks erstellt. Diese StyleBooks sind auch in Citrix Applications and Delivery Management (ADM) erforderlich. Jetzt können Sie diese StyleBooks direkt in Citrix ADM importieren. Sie müssen sie nicht manuell von GitHub kopieren und dann in Citrix ADM hochladen oder die Dateien in ADM und GitHub manuell synchronisieren.

Sie können nun ein Repository in NetScaler ADM definieren, das ein GitHub-Repository darstellt. Geben Sie die GitHub-Repository-URL sowie Ihren in GitHub erstellten Benutzernamen und Ihr Kennwort (oder API-Token) an. Das bedeutet, dass nur autorisierte Benutzer, die ein gültiges Konto in GitHub haben, StyleBooks importieren und synchronisieren können.

Nachdem Sie das Repository erstellt haben, können Sie NetScaler ADM mit Ihrem GitHub-Repository synchronisieren. Citrix ADM stellt eine Verbindung mit GitHub her und importiert StyleBooks, die in diesem Repository gefunden wurden. ADM validiert dann die StyleBooks und fügt sie der Liste der StyleBooks in Citrix ADM hinzu. StyleBooks werden NetScaler ADM nicht hinzugefügt, wenn die Validierung fehlschlägt. Korrigieren Sie die Fehler und übertragen Sie aktualisierte Versionen in Ihr GitHub-Repository. Später können Sie versuchen, sie zu importieren oder erneut mit NetScaler ADM zu synchronisieren.

> **Hinweis**
>
> - StyleBooks-Dateien können aus jedem Zweig eines GitHub-Repositorys importiert und synchronisiert werden.
> - Sie können StyleBooks importieren und synchronisieren, denen auch abhängige StyleBooks zugeordnet sind.
> - Die Synchronisation von StyleBooks aus einem GitHub-Repository muss manuell über die NetScaler ADM GUI oder API initiiert werden. Das heißt, derzeit geschieht das Importieren und Synchronisieren von StyleBooks nicht automatisch basierend auf GitHub Commit-Aktivität.

Fügen Sie ein Repository hinzu und importieren Sie StyleBooks aus dem GitHub-Repository

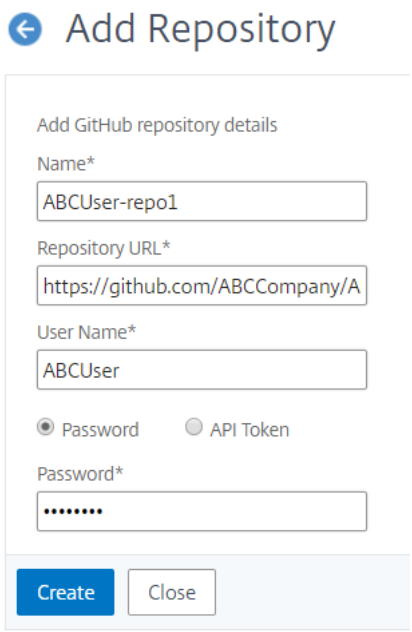
Bevor Sie beginnen, stellen Sie sicher, dass Sie über ein gültiges Konto in GitHub verfügen.

Sie können StyleBook-Dateien aus jedem Ordner im GitHub-Repository in ADM importieren.

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **StyleBooks** > **Repositories**.
2. Klicken Sie auf **Hinzufügen**. Geben **Sie im Fenster Repository hinzufügen** die folgenden Parameter ein:
   - **Name**. Geben Sie den Namen des Repositorys ein. Dieser Name kann mit dem Repository-Namen in GitHub oder einem anderen Namen identisch sein.
   - **Repository-URL**. Geben Sie die GitHub-Repository-URL ein.
   - **Benutzername und Kennwort**. Geben Sie den Benutzernamen und das Kennwort ein, mit dem Sie auf das GitHub-Konto zugreifen.

   > **Hinweis:**
   >
   > Sie können das API-Token auch anstelle eines Kennworts angeben. API-Token können anstelle eines Kennworts für GitHub über HTTPS verwendet werden. Informationen zum Erstellen von API-Token für Ihr GitHub-Repository finden Sie in der GitHub-Dokumentation zum Erstellen persönlicher Zugriffstoken.

3. Klicken Sie auf **Erstellen**.



Das Repository wird in NetScaler ADM erstellt.

4. **Um StyleBooks zu importieren oder zu synchronisieren, wählen Sie das Repository auf der Seite**Repositories**aus und klicken Sie auf Synchronisieren.**

Die anderen Aktionen, die Sie hier verwenden können, sind:

- **Bearbeiten:** Sie können die Repository-URL, den Benutzernamen und das Kennwort (oder das API-Token) bearbeiten.
- **Löschen**. Sie können das Repository zusammen mit allen in Citrix ADM vorhandenen StyleBooks löschen, die zuvor aus diesem GitHub-Repository importiert wurden.

  > **Hinweis:**
  >
  > Sie können ein Repository nicht aus NetScaler ADM löschen, wenn StyleBooks mit Config-Packs verknüpft sind. Löschen Sie zunächst alle Konfigurationspakete dieser StyleBooks. Sie können das Repository später aus NetScaler ADM entfernen, um die StyleBooks aus diesem Repository zu bereinigen.

- **Zurücksetzen**. Sie können alle StyleBooks in Citrix ADM synchronisiert aus diesem Repository entfernen, ohne den Repository-Eintrag tatsächlich aus Citrix ADM zu löschen.
- **Dateien auflisten**. Sie können eine Liste aller in NetScaler ADM vorhandenen StyleBooks anzeigen, die aus dem GitHub-Repository stammen.

Standard-StyleBooks verwenden

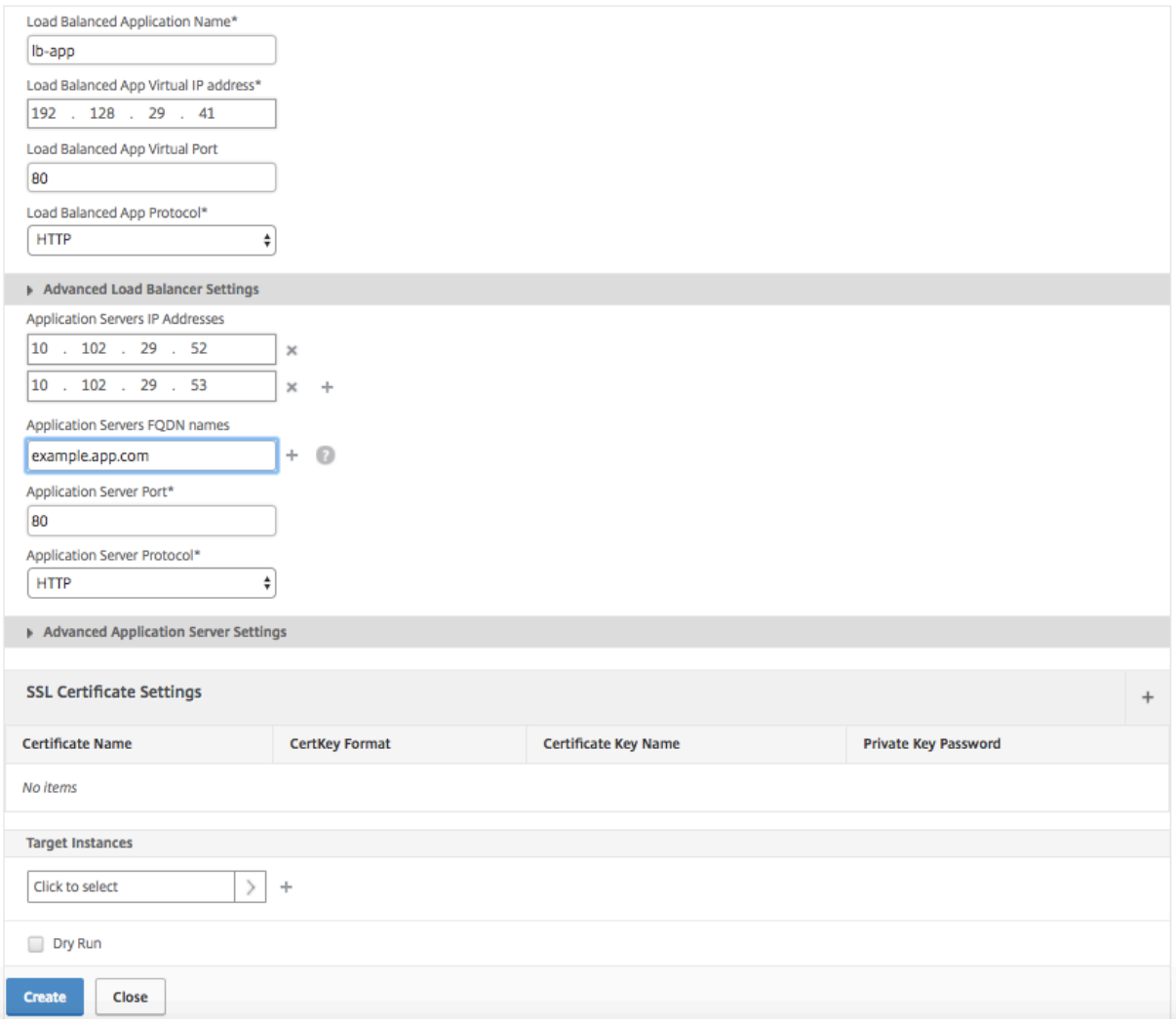
February 5, 2024

Eine Reihe von Standard-StyleBooks wird mit NetScaler Application Delivery Management (ADM) bereitgestellt. Wenn Sie ein Standard-StyleBook verwenden, müssen Sie Werte für die Parameter im StyleBook angeben und die IP-Adressen der NetScaler ADC-Instanzen auswählen, in denen Sie die Konfiguration ausführen möchten. Nachdem Sie die Konfiguration gesendet haben, überprüft NetScaler ADM die angegebenen Parameterwerte, erstellt ein Diagramm der Konfiguration, stellt eine Verbindung zu den NetScaler ADC-Instanzen her und führt die Konfiguration auf den Instanzen aus.

So erstellen Sie eine Konfiguration aus einem Standard-StyleBook

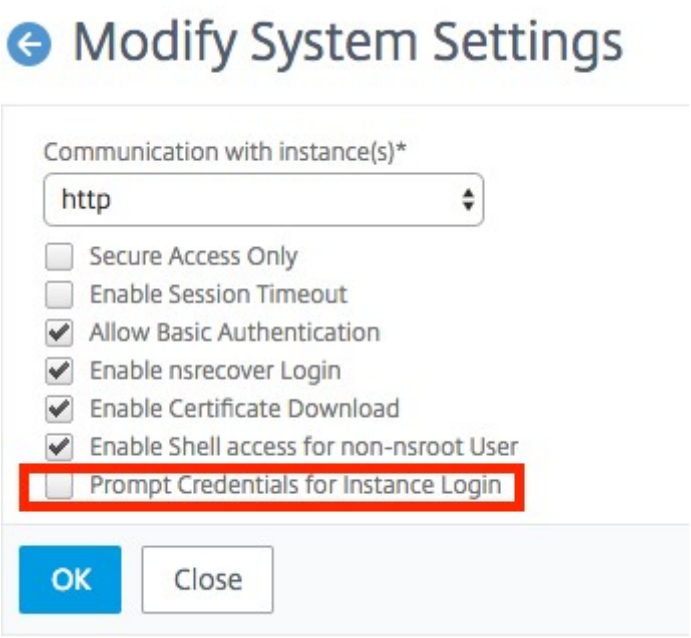
1.Navigieren Sie zu **Anwendungen** > **Konfigurationen > StyleBooks**. Auf der Seite StyleBooks werden alle StyleBooks in NetScaler ADM angezeigt. Diese Liste enthält sowohl Standard- als auch benutzerdefinierte StyleBooks. Sie können den Namen des StyleBooks in das Suchfeld eingeben und die **Eingabetaste** drücken. Andernfalls können Sie in der Liste nach unten scrollen, um das StyleBook zu finden.

2.Klicken Sie auf **Konfiguration erstellen**. Geben Sie die erforderlichen Werte für die Parameter an.

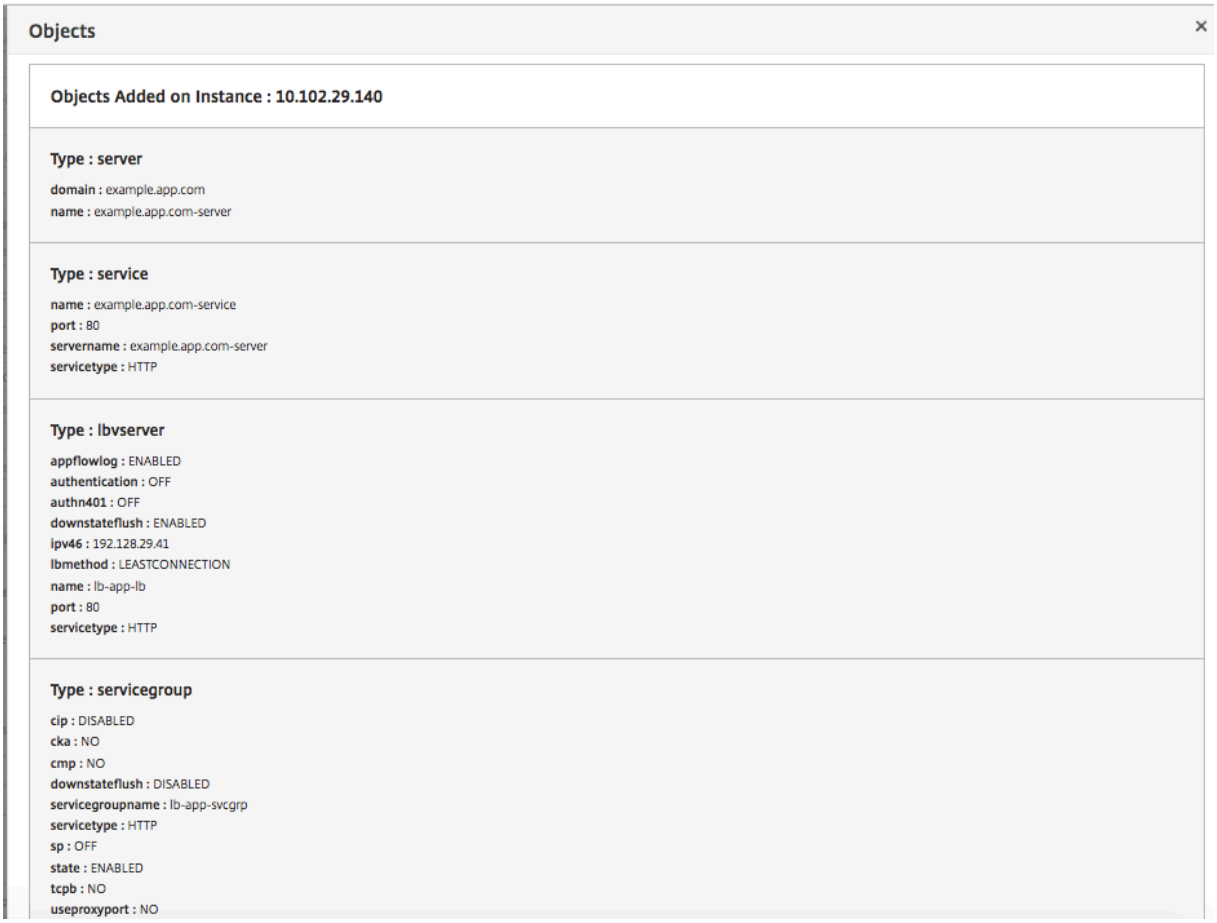


3.Wählen Sie unter **Target Instances** die IP-Adresse der NetScaler ADC-Instanz aus, in der Sie die Konfiguration ausführen möchten. Wenn Sie diese Konfiguration auf mehreren Instanzen ausführen möchten, klicken Sie auf "+", um weitere Instanzen hinzuzufügen.

Wenn die Option**Anmeldeinformationen für Instanzanmeldung auffordernunter Citrix ADM**>**System > Systemeinstellungenändern > Systemeinstellungenänderna**ktiviert ist, werden Sie aufgefordert, die Anmeldeinformationen der Citrix ADC Instanz einzugeben, wenn Sie den Befehl -Konfigurationen auf den ausgewählten Citrix ADC Instanzen. Andernfalls verwendet NetScaler ADM die im Instanzprofil gespeicherten Instanzanmeldeinformationen für die Anmeldung bei der Instanz.



Wenn Sie Ihre Konfiguration testen oder validieren möchten, bevor Sie sie auf der NetScaler ADC-Instanz ausführen, wählen Sie **Dry Run** und klicken Sie dann auf **Erstellen**. Wenn Ihre Konfiguration gültig ist, werden die Objekte angezeigt, die anhand der von Ihnen angegebenen Werte erstellt werden.



4. Deaktivieren Sie das Kontrollkästchen **Dry Run**, und klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und die Konfiguration auf der NetScaler ADC-Instanz auszuführen. Die von Ihnen erstellte StyleBook-Konfiguration wird in der Liste der Konfigurationen angezeigt, wie unten gezeigt.

> **Hinweis**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte NetScaler ADC-Instanzen in NetScaler ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

Sie können dieses Konfigurationspaket jetzt mithilfe von NetScaler ADM überprüfen, aktualisieren oder entfernen.

Webanwendungs-Firewall-StyleBook

February 5, 2024

Die Citrix Web App Firewall ist eine Web Application Firewall (WAF), die Webanwendungen und Websites vor bekannten und unbekannten Angriffen schützt, einschließlich aller Bedrohungen auf Anwen-

dungsebene und Zero-Day-Bedrohungen.

NetScaler ADM bietet jetzt ein Standard-StyleBook, mit dem Sie eine Anwendungs-Firewall-Konfiguration auf NetScaler ADC-Instanzen bequemer erstellen können.

Bereitstellen von Firewall-

Die folgende Aufgabe unterstützt Sie bei der Bereitstellung einer Lastausgleichskonfiguration zusammen mit der Anwendungsfirewall und der IP-Reputationsrichtlinie auf NetScaler ADC-Instanzen in Ihrem Unternehmensnetzwerk.

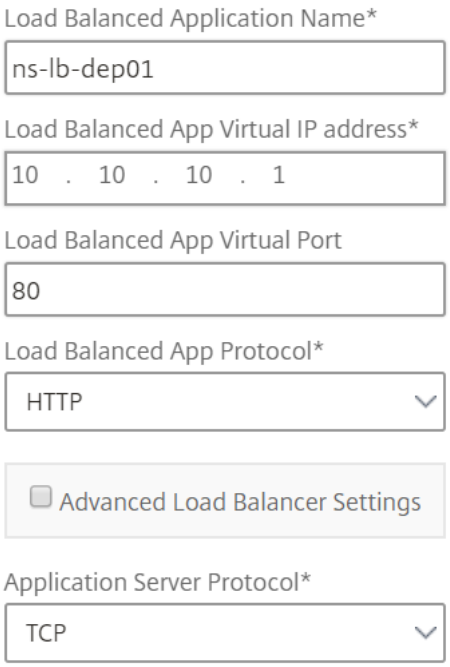
So erstellen Sie eine LB-Konfiguration mit Firewalleinstellungen der Anwendung:

1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Konfigurationen** > **StyleBooks**. Auf der Seite StyleBooks werden alle StyleBooks angezeigt, die für die Verwendung in Citrix ADM verfügbar sind. Scrollen Sie nach unten und suchen Sie das HTTP/SSL Load Balancing StyleBook mit der Firewall-Richtlinie und der IP-Reputationsrichtlinie. Sie können auch nach dem StyleBook suchen, indem Sie den Namen als eingeben `lb-appfw`. Klicken Sie auf **Konfiguration erstellen**.

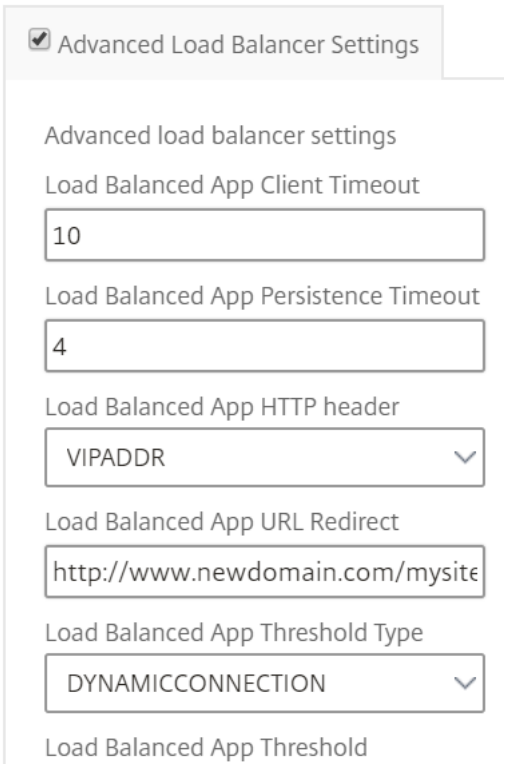
   Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

2. Geben Sie Werte für die folgenden Parameter ein:

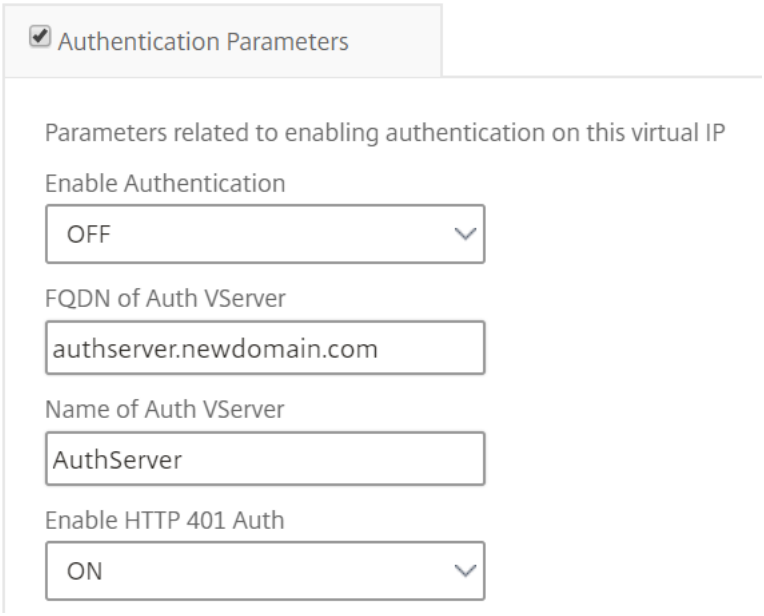
   - **Anwendungsname für Lastausgleich**. Name der Konfiguration mit Lastausgleich und Anwendungs-Firewall, die in Ihrem Netzwerk bereitgestellt werden soll.
   - **Laden Sie ausbalancierte virtuelle IP-Adresse der App**. Virtuelle IP-Adresse, unter der die NetScaler ADC-Instanz Clientanforderungen empfängt.
   - **Virtueller App-Port mit Lastausgleich** Der TCP-Port, der von den Benutzern beim Zugriff auf die Anwendung mit Lastausgleich verwendet werden soll.
   - **Load Balanced App-Protokoll**. Wählen Sie das Frontend-Protokoll aus der Liste aus.
   - **Anwendungsserver-Protokoll**. Wählen Sie das Protokoll des Anwendungsservers aus.



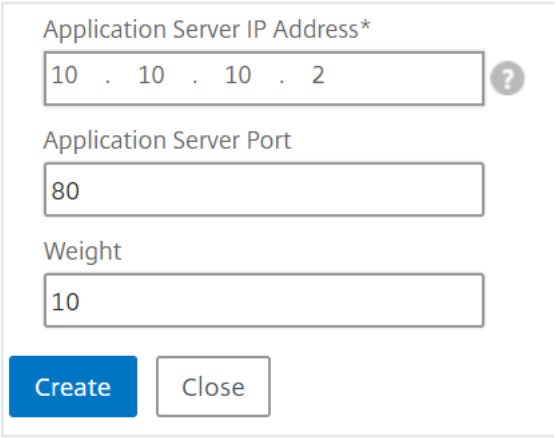
3. Optional können Sie die **erweiterten Lastenausgleichseinstellungen**aktivieren und konfigurieren.



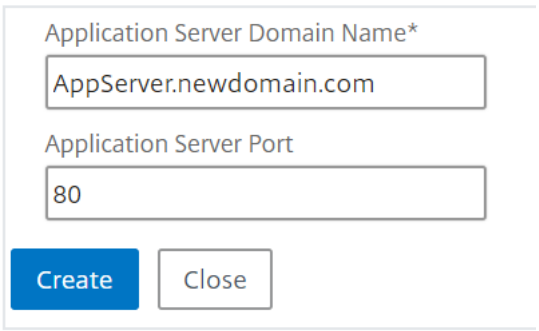
4. Optional können Sie auch einen Authentifizierungsserver für die Authentifizierung des Datenverkehrs für den virtuellen Lastausgleichsserver einrichten.



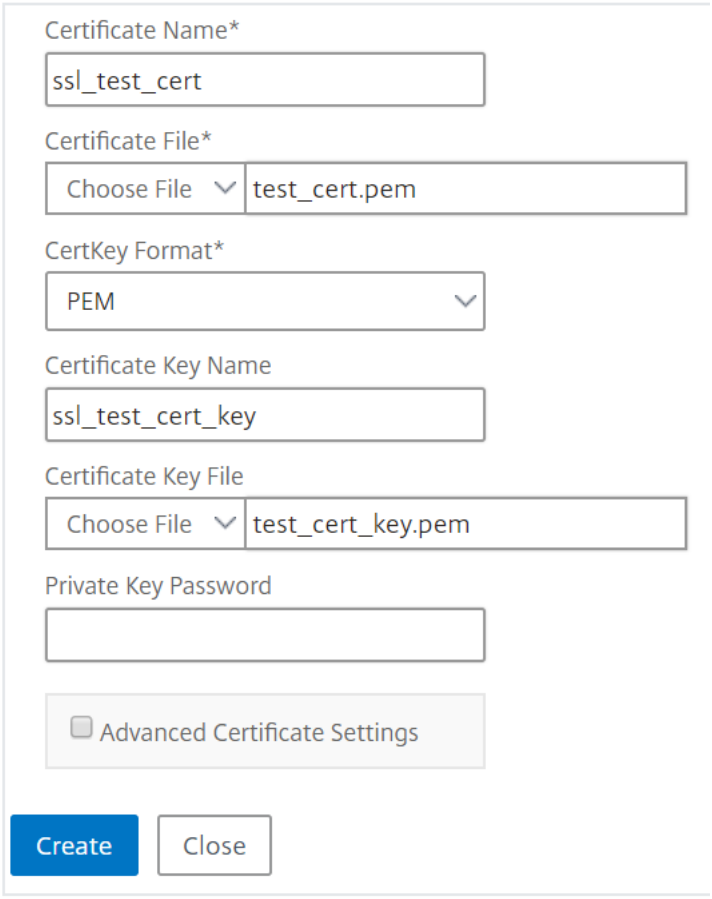
5. Klicken Sie im Abschnitt Server-IPs und -Ports auf +, um Anwendungsserver und die Ports zu erstellen, auf die sie zugegriffen werden können.



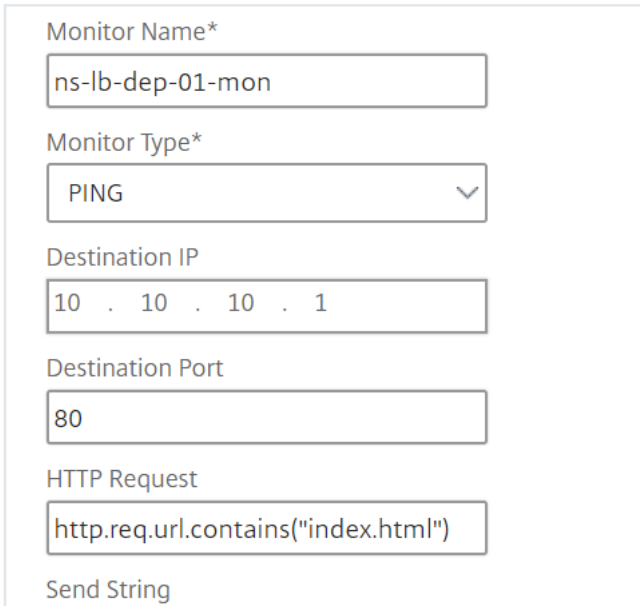
6. Sie können auch FQDN-Namen für Anwendungsserver erstellen.



7. Sie können auch die Details des SSL-Zertifikats angeben.

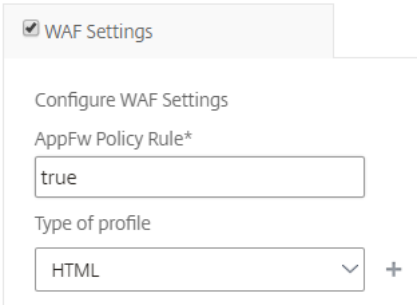


8. Sie können auch Monitore in der NetScaler ADC Zielinstanz erstellen.



9. Um eine Anwendungsfirewall auf dem virtuellen Server zu konfigurieren, aktivieren Sie WAF-Einstellungen.

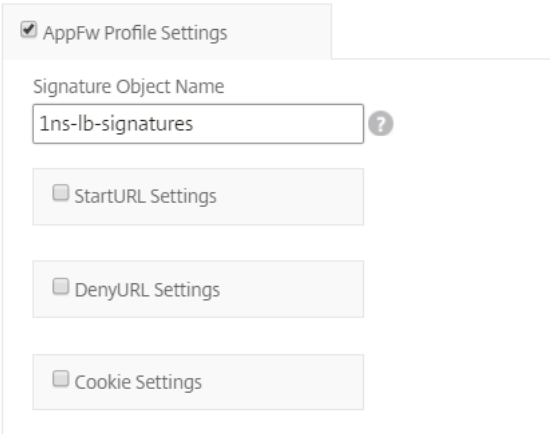
Stellen Sie sicher, dass die Richtlinienregel für die Anwendungsfirewall wahr ist, wenn Sie die Einstellungen für die Anwendungsfirewall auf den gesamten Datenverkehr in diesem VIP anwenden möchten. Andernfalls geben Sie die NetScaler ADC Richtlinienregel an, um eine Teilmenge von Anforderungen auszuwählen, auf die die Firewalleinstellungen der Anwendung angewendet werden sollen. Wählen Sie als Nächstes den Profiltyp aus, der angewendet werden soll - HTML oder XML.



10. Optional können Sie detaillierte Profileinstellungen der Anwendungsfirewall konfigurieren, indem Sie das Kontrollkästchen Profileinstellungen der Anwendungsfirewall aktivieren.
11. Wenn Sie die Anwendungsfirewall Signaturen konfigurieren möchten, geben Sie optional den Namen des Signaturobjekts ein, das auf der NetScaler ADC-Instanz erstellt wird, in der der virtuelle Server bereitgestellt werden soll.

> **Hinweis**
>
> Sie können mit diesem StyleBook kein Signature-Objekt erstellen.

12. Als Nächstes können Sie auch andere Anwendungs-Firewall-Profileinstellungen wie StartURL-Einstellungen, DenyURL-Einstellungen und andere konfigurieren.



Weitere Informationen zur Anwendungsfirewall und Konfigurationseinstellungen finden Sie unter Anwendungsfirewall.

13. Wählen Sie im Abschnitt "**Target Instanzen** "die NetScaler ADC-Instanz aus, auf der der virtuelle Lastausgleichsserver mit der Anwendungsfirewall bereitgestellt werden soll.

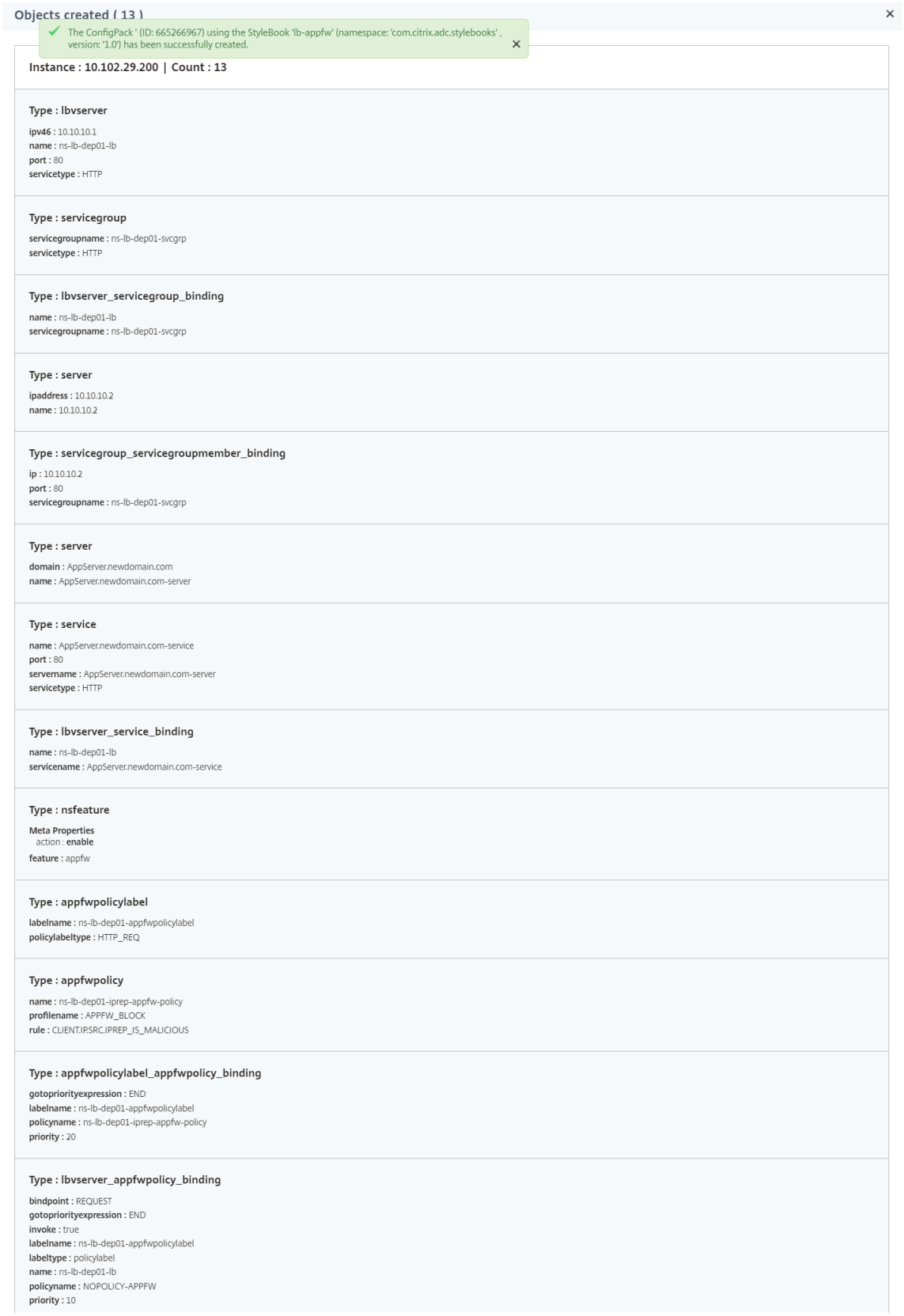
    > **Hinweis**
    >
    > Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte NetScaler ADC-Instanzen in NetScaler ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

14. Sie können auch die **IP-Reputationsprüfung** aktivieren, um die IP-Adresse zu identifizieren, die unerwünschte Anfragen sendet. Sie können die IP-Reputationsliste verwenden, um Anforderungen vorbeugend abzulehnen, die von der IP mit der schlechten Reputation stammen.
15. Klicken Sie auf **Erstellen**, um die Konfiguration für die ausgewählten NetScaler ADC-Instanzen zu erstellen.

    > **Tipp**
    >
    > Citrix empfiehlt, dass Sie die Option Trockenlauf auswählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt werden müssen, bevor Sie die eigentliche Konfiguration auf der Instanz ausführen.

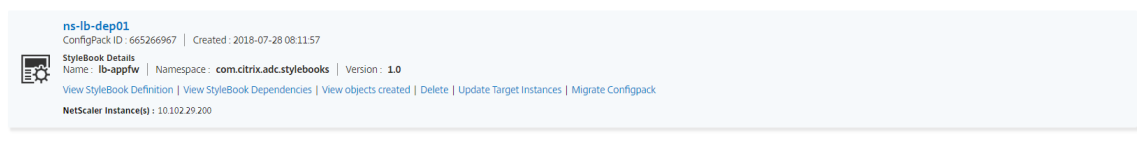
    Wenn die Konfiguration erfolgreich erstellt wurde, erstellt das StyleBook den erforderlichen virtuellen Lastenausgleichsserver, Anwendungsserver, Dienste, Dienstgruppen, Anwendungsfirewall Labels, Anwendungsfirewall Richtlinien und bindet sie an den virtuellen Lastausgleichsserver.

    Die folgende Abbildung zeigt die in jedem Server erstellten Objekte:



16. Um das ConfigPack anzuzeigen, das auf NetScaler ADM erstellt wurde, navigieren Sie zu **Anwen-**

dungen > **Konfigurationen**.



WAF- und BOT-Profile mit StyleBook erstellen

February 5, 2024

Wenn Sie eine Richtlinie für eine API-Ressource in **API Gateway**auswählen können, können Sie die Kriterien zur Verkehrsauswahl definieren, um eine API-Anfrage zu authentifizieren. Außerdem können Sie API-Sicherheitsrichtlinien für den API-Datenverkehr konfigurieren. Weitere Informationen finden Sie unter API-Gateway verwalten.

Sie können WAF- und BOT-Richtlinien für eine API-Ressource konfigurieren. Bevor Sie eine Richtlinie konfigurieren, müssen Sie sicherstellen, dass Sie ihr Profil in NetScaler Application Delivery Management (ADM) erstellen. Verwenden Sie die folgenden Standard-StyleBooks, um ein Profil zu erstellen:

- API WAF Erkennung StyleBook
- API BOT Erkennung StyleBook

Erstellen Sie ein WAF-Profil mit dem StyleBook

Führen Sie Folgendes aus, um ein WAF-Profil zu erstellen:

1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Konfigurationen** > **StyleBooks**. Suchen Sie nach dem StyleBook, indem Sie den Namen als eingeben `api-waf-profile`. Klicken Sie auf **Konfiguration erstellen**.

   Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

2. Geben Sie Werte für die folgenden Parameter an:

   - **API WAF-Profilname** - Ein Name zur Identifizierung eines WAF-Profils.
   - **Anwendungstyp** - Fügen Sie dem Profil Anwendungstypen hinzu. Das WAF-Profil unterstützt JSON- und XML-Anwendungstypen.

3. Optional: Aktivieren Sie **Sicherheitseinstellungen**, um HTTP-, JSON- oder XML-Schutzprüfungen anzugeben. Sie können auch eine Fehler-URL für die Citrix Web App Firewall angeben. Weitere Informationen finden Sie unter Erstellen eines Web App Firewall-Profils.

4. Wählen Sie die NetScaler ADC-Zielinstanz oder Instanzgruppe aus, auf der Sie diese Konfiguration bereitstellen möchten.
5. Klicken Sie auf **Erstellen**.

Informationen zum Konfigurieren einer WAF-Richtlinie finden Sie unter Hinzufügen von Richtlinien zu einer API-Bereitstellung.

Erstellen Sie ein BOT-Profil mit dem StyleBook

Führen Sie Folgendes aus, um ein BOT-Profil zu erstellen:

1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Konfigurationen** > **StyleBooks**. Suchen Sie nach dem StyleBook, indem Sie den Namen als eingeben `api-bot-profile`. Klicken Sie auf **Konfiguration erstellen**.

   Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
2. Geben Sie in **BOT Profile Name**einen Namen zur Identifizierung eines BOT-Profils an.
3. Optional können Sie die folgenden Optionen basierend auf Ihren Anforderungen aktivieren:

   - **Überprüfung der IP-Reputation aktivieren** - Diese Option identifiziert die IP-Adresse, die unerwünschte Anfragen sendet. Sie können die IP-Reputationsliste verwenden, um Anforderungen vorbeugend abzulehnen, die von der IP mit der schlechten Reputation stammen.
   - **Aktivieren von BOT-Signaturen** - Geben Sie den Namen der BOT-Sig Es blockiert die Anfragen von der angegebenen Signatur.
   - **Liste zulassen** - Geben Sie die IPv4- oder Subnetzadresse (CIDR) an. Diese Option ermöglicht es dem BOT-Profil, Anfragen von der angegebenen IPv4- oder Subnetzadresse zu Bypass.
   - **Liste ablehnen** - Geben Sie die IPv4- oder Subnetzadresse (CIDR) an. Diese Option ermöglicht es dem BOT-Profil, Anfragen von der angegebenen IPv4- oder Subnetzadresse zu blockieren.
4. Wählen Sie die NetScaler ADC-Zielinstanz oder Instanzgruppe aus, auf der Sie diese Konfiguration bereitstellen möchten.
5. Klicken Sie auf **Erstellen**.

Informationen zum Konfigurieren einer BOT-Richtlinie finden Sie unter Hinzufügen von Richtlinien zu einer API-Bereitstellung.

Alle Standard-StyleBooks ausblenden

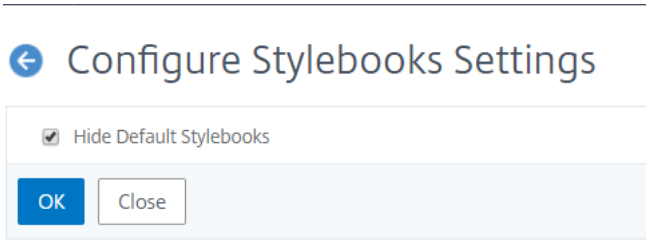
February 5, 2024

Citrix ADM listet alle StyleBooks auf, die im Citrix ADM Ordnersystem vorhanden sind. Die Liste der StyleBooks enthält Standard- und benutzerdefinierte StyleBooks, die sowohl privat als auch öffentlich sein können. Als Administrator möchten Sie möglicherweise alle Standard-StyleBooks ausblenden. Sie können Ihren Benutzern erlauben, nur benutzerdefinierte StyleBooks anzuzeigen und darauf zuzugreifen, die von Ihnen oder den Benutzern erstellt wurden.

Mit NetScaler ADM können Sie Ihre benutzerdefinierten StyleBooks anzeigen und alle Standard-StyleBooks ausblenden, die mit NetScaler ADM geliefert werden. Es wird eine neue GUI-Option bereitgestellt, mit der Sie alle Standard-StyleBooks ausblenden können.

So blenden Sie alle Standard-StyleBooksaus:

1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Konfigurationen > Einstellungen**.
2. Auf der Seite **Einstellungen** werden Informationen angezeigt, ob die Standard-StyleBooks für Benutzer sichtbar sind oder nicht.
3. Um die Standard-StyleBooks auszublenden, klicken Sie auf das Bearbeitungssymbol oben rechts.
4. Wählen Sie auf der Seite **StyleBook-Einstellungen konfigurieren** die Option **Standard-StyleBooks ausblenden** aus.
5. Klicken Sie auf **OK**.



Die Seite **„StyleBook-Einstellungen konfigurieren** “ist für Benutzer weiterhin sichtbar, wenn Sie sich nicht dafür entschieden haben, die Seite mithilfe der RBAC-Funktion auszublenden. Möglicherweise haben die Benutzer weiterhin die Option, die Standard-StyleBooks einblenden.

Um die Seite **„StyleBook-Einstellungen konfigurieren** “auszublenden, müssen Sie eine Richtlinie erstellen und diese Richtlinie den Benutzern zuweisen, denen die Standard-StyleBooks nicht angezeigt werden sollen.

So erstellen Sie eine RBAC-Richtlinie:

1. Navigieren Sie in NetScaler ADM zu **Konto** > **Benutzerverwaltung** > **Zugriffsrichtlinien**.
2. Klicken Sie auf **Hinzufügen**, um eine Richtlinie zu erstellen.
3. Geben Sie den Namen der Richtlinie ein.
4. Vergewissern Sie sich, dass im Abschnitt **Berechtigungen** unter **Alle** > **Anwendungen** > **Konfiguration** >**Einstellungen** nicht ausgewählt ist, und klicken Sie auf **OK**.

Nach dem Erstellen von Richtlinien müssen Sie Rollen erstellen, jede Rolle an eine oder mehrere Richtlinien binden und Benutzergruppen Rollen zuweisen. Weitere Informationen zum Verknüpfen von Richtlinien mit Benutzern finden Sie unter Konfiguration der rollenbasierten Zugriffskontrolle.

Migrieren der NetScaler ADC Anwendungskonfiguration mit dem StyleBooks Configuration Builder

February 5, 2024

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

Der StyleBooks Configuration Builder wird verwendet, um eine Anwendungskonfiguration StyleBook aus einer vorhandenen Citrix ADC-Konfiguration zu erstellen. Diese Funktion automatisiert auch die Migration der Anwendungskonfiguration von einer NetScaler ADC-Instanz zu einer anderen Instanz.

Mit Configuration Builder können Sie die Erstellung eines benutzerdefinierten StyleBook vereinfachen. Mit dieser Funktion können Sie ein StyleBook ohne gründliche Kenntnisse der StyleBooks-Grammatik und -Konstrukte erstellen. Andernfalls ist das Wissen über StyleBooks Grammatik und Konstrukte notwendig, um ein StyleBook zu erstellen.

Der Configuration Builder erstellt außerdem ein ConfigPack, das dieselbe ADC-Konfiguration auf einer neuen ADC-Instanz widerspiegelt. Mit diesem ConfigPack kann die anfängliche ADC-Konfiguration von einer ADC-Instanz auf eine andere ADC-Instanz dupliziert werden. Die ursprüngliche Konfigurationsquelle kann eine der folgenden sein:

- **Eine NetScaler ADC-Instanz:** Geben Sie die Instanz an, in der die zu duplizierende Anwendungskonfiguration gehostet wird.

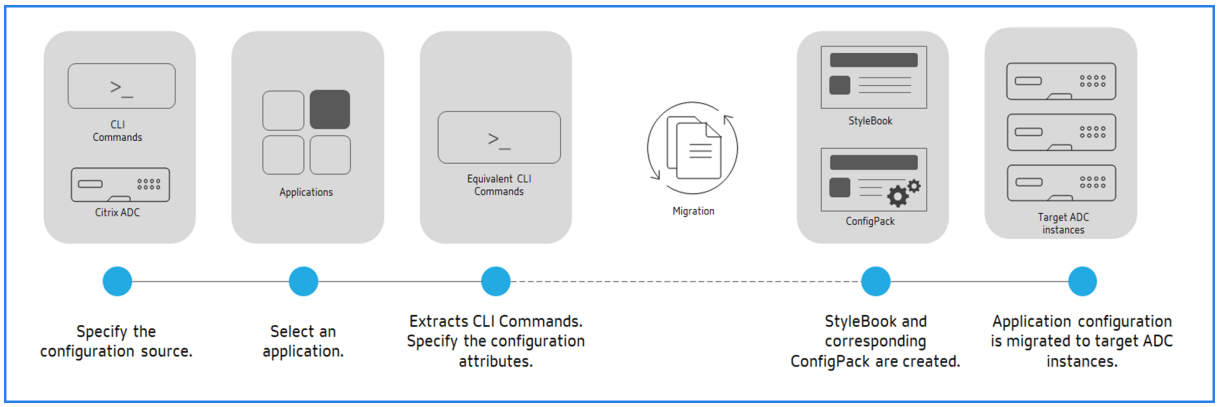
  Der Configuration Builder konvertiert die ADC-Konfiguration in ein StyleBook und ein ConfigPack, auch wenn Sie die Zielinstanz nicht angeben. Sie können dieses Configpack später verwenden, um die ADC-Konfiguration auf andere ADC-Instanzen zu migrieren.

- **Eine Reihe von CLI-Befehlen:** Fügen Sie die Konfiguration von`ns.conf` oder ein`Application config`.

Der Configuration Builder identifiziert die Liste der unterschiedlichen Anwendungen, die in die Quellkonfiguration eingebettet sind. Wenn Sie die gewünschte Anwendungskonfiguration auswählen, extrahiert der Configuration Builder die CLI-Befehle für die ausgewählte Anwendung. Diese CLI-Befehle werden aus der Quellkonfiguration extrahiert. Außerdem werden die Bereitstellungs- und Konfigurationsattribute identifiziert, die möglicherweise Ihre Eingabe erfordern.

- **Bereitstellungsattribute** —Sie können die IP-Adresse und den Port der virtuellen Server, Dienste und Dienstgruppenmitglieder anhand der ursprünglichen Konfiguration anzeigen und bearbeiten.
- **Konfigurationsattribute** —Bei diesen Attributen kann es sich um Kennwörter oder Zertifikate handeln, die in der Quellkonfiguration angegeben sind.

Nachdem Sie die erforderlichen Informationen angegeben haben, starten Sie mit der Migration oder Duplizierung der Anwendungskonfiguration auf einer ADC-Zielinstanz.



Nachdem Sie die Anwendungserstellung und Migration abgeschlossen haben, wird in Citrix ADM ein ConfigPack zusammen mit dem entsprechenden StyleBook erstellt. Dieses ConfigPack stellt die Anwendungskonfiguration auf der ADC-Zielinstanz dar. Um das erstellte ConfigPack anzuzeigen, navigieren Sie zu **Anwendungen** > **StyleBooks** > **Configurations**.

Unterstützte NetScaler ADC Funktionen

Der StyleBook Configuration Builder erkennt und unterstützt die folgenden NetScaler ADC-Funktionen in der Quellkonfiguration:

- Content Switching
- Lastausgleich
- Überwachen
- SSL Offloading
- Ratenlimit
- Rewrite

- Responder
- Firewall für Webanwendungen (WAF)

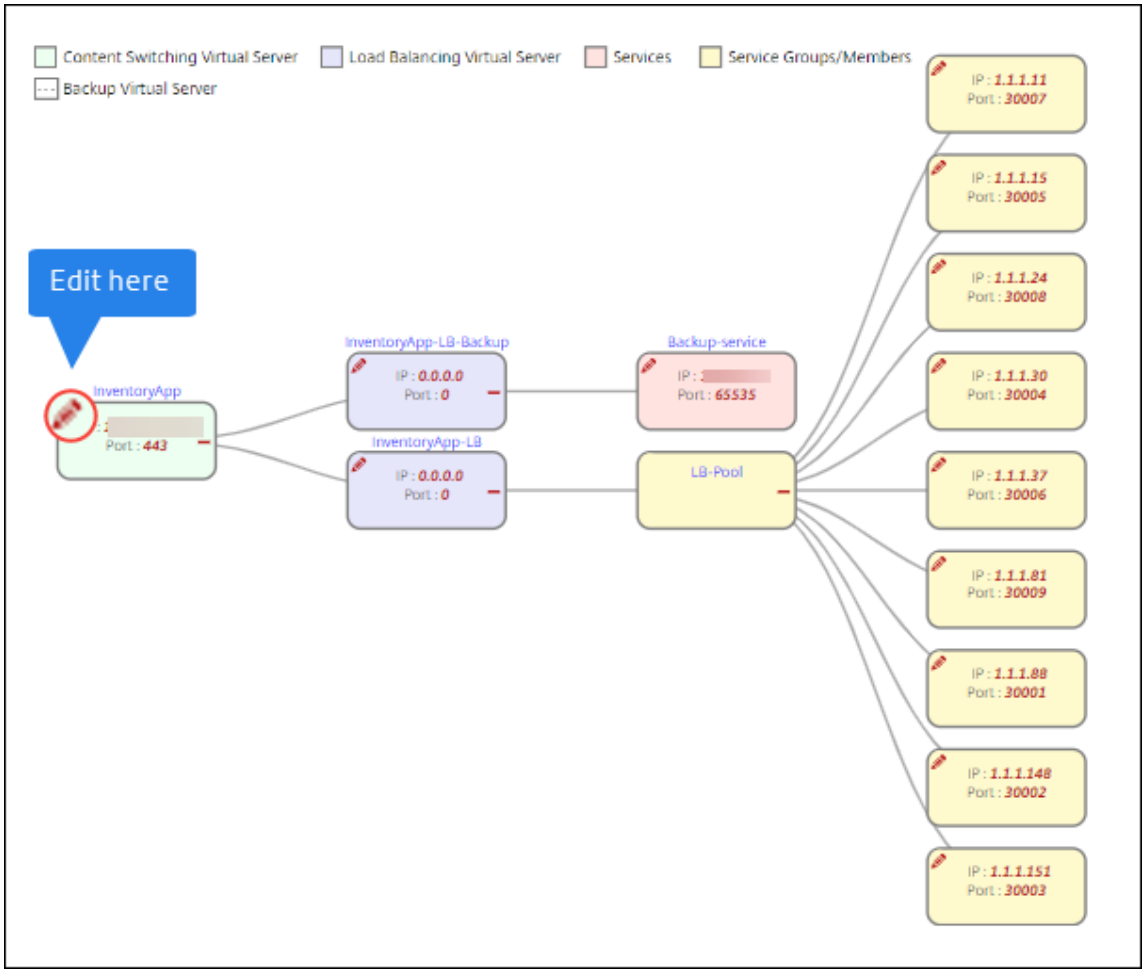
Erstellen Sie ein StyleBook, um die NetScaler ADC-Anwendungskonfiguration zu migrieren

Das folgende Verfahren besteht darin, ein StyleBook zu erstellen, das die NetScaler ADC-Anwendungsmigration in NetScaler ADM migriert:

1. Navigieren Sie zu **Anwendungen** > **StyleBooks** > **Konfigurationen**.
2. Klicken Sie auf **ADC-Konfiguration migrieren**.
3. Klicken Sie auf **Erste Schritte**.
4. Wählen **Sie unter Konfiguration angeben**die Konfigurationsquelle aus:
    - **Von einem ADC importieren**: Diese Option erkennt die aktiven Anwendungen auf der ausgewählten ADC-Instanz.
    - **Import mit CLI-Befehlen**: Diese Option analysiert die CLI-Befehle und extrahiert die Anwendungen aus den CLI-Befehlen.
5. Geben Sie die **Quell-ADC-Instanz** an, von der Sie die Anwendungskonfiguration migrieren oder duplizieren möchten.
6. Geben Sie die **Ziel-ADC-Instanz** an, zu der Sie die Anwendungskonfiguration migrieren oder duplizieren möchten.
7. In **Anwendung definieren,**
    a) Geben Sie **unter Anwendungsname**den Namen der Anwendung an.
    b) Wählen Sie die virtuellen Server aus, die Sie migrieren möchten.
    c) Klicken Sie auf **Weiter**.
8. Überprüfen Sie **unter Äquivalente CLI-Befehle**die Befehle und klicken Sie auf **Weiter**.

    Diese Befehle sind spezifisch für die ausgewählte Anwendungskonfiguration.
9. In **Bereitstellungsattribute**können Sie die IP-Adresse und den Port der virtuellen Server, Dienste und Dienstgruppenmitglieder anzeigen und bearbeiten.

    Um die IP-Adresse und den Port zu bearbeiten, klicken Sie im Flussdiagramm auf dem virtuellen Server, Dienst oder Dienstgruppenmitglied auf das Bearbeitungssymbol.



Diese Registerkarte wird nur in den folgenden Fällen angezeigt:

- Die Quell- und Zielinstanzen sind unterschiedlich.
- Importieren Sie Konfigurationen mit CLI-Befehlen.

10. Geben Sie **unter Konfigurationsattribute**die erforderlichen Details an und klicken Sie auf **Weiter**.

    Auf dieser Registerkarte werden die Geheimnisse wie Schlüssel zum Entschlüsseln von Kennwörtern und Zertifikaten aufgeführt.

    > **Hinweis** Bevor Sie mit der Migration beginnen, werden die fehlenden oder nicht unterstützten Konfigurationen auf einer der folgenden Registerkarten angezeigt:
    >
    > **Nicht unterstützte Konfigurationen Nicht unterstützte globale Konfigurationen**
    >
    > **Um diese Konfigurationen**
    >
    > erfolgreich zu migrieren, müssen Sie die fehlenden oder nicht unterstützten Konfigurationen separat auf die Ziel-Instance anwenden. Klicken Sie auf **Weiter**.

11. Geben Sie in **Migrate**die erforderlichen StyleBook-Details an. Klicken Sie auf **Migrate**.

Einschränkungen

- Die benannten Ausdrücke, die in der Quellinstanz `responderhtmlpages` erwähnt werden, werden nicht identifiziert. Stellen Sie sicher, dass Sie die benannten Ausdrücke und `responderhtmlpages` auf der Zielinstanz vor der Migration konfigurieren.
- Wenn die Quelle eine Konfiguration für `servicegroup` und eine Monitorbindung wie folgt hat:

  ```
  bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>
  ```

  Der folgende Fehler wird angezeigt:

  ```
  1  CLI Command conversion failed: 100 - No such command [{
  2   "errorcode": 1090, "message": "No such argument [XXX]", "
         severity": "ERROR"  }
  3  ]
  4  <!--NeedCopy-->
  ```

  Dieser Fehler tritt auf, weil NetScaler ADC die Bindung zwischen Dienstgruppe und Monitor in einem ungültigen Format speichert. Dieses Problem wurde von NetScaler ADC 12.1.52.15 Build behoben.

Geschäftsanwendungs-StyleBooks

February 5, 2024

NetScaler ADM bietet die StyleBooks, mit denen Sie eine ADC-Konfiguration für bestimmte Geschäftsanwendungen bereitstellen können. Weitere Informationen zu solchen StyleBooks finden Sie in den folgenden Themen:

- SSO Google Apps-StyleBook
- SSO Office 365-StyleBook
- Microsoft Skype for Business StyleBook
- Microsoft Exchange-StyleBook
- Microsoft SharePoint-StyleBook
- Microsoft ADFS-Proxy-StyleBook
- Oracle e-business StyleBook

- Webanwendungs-Firewall-StyleBook
- WAF- und BOT-Profile mit StyleBook erstellen

SSO Google Apps-StyleBook

February 5, 2024

Google Apps ist eine Sammlung von Tools, Software und Produkten für Cloud Computing, Produktivität und Zusammenarbeit, die von Google entwickelt wurden. Single Sign-On (SSO) ermöglicht Benutzern den Zugriff auf alle Cloud-Unternehmensanwendungen —einschließlich Administratoren, die sich bei der Admin-Konsole anmelden —, indem sie sich mit ihren Unternehmensanmeldeinformationen für alle Dienste einmalig anmelden.

Mit dem NetScaler ADM SSO Google Apps StyleBook können Sie SSO für Google Apps über NetScaler ADC-Instanzen aktivieren. Das StyleBook konfiguriert die NetScaler ADC-Instanz als SAML-Identitätsanbieter für die Authentifizierung von Benutzern für den Zugriff auf Google Apps.

Das Aktivieren von SSO für Google-Apps in einer NetScaler ADC-Instanz mit diesem StyleBook führt zu den folgenden Schritten:

1. Konfigurieren des virtuellen Authentifizierungsservers
2. Konfigurieren einer SAML-IdP-Richtlinie und eines Profils
3. Binden der Richtlinie und des Profils an den virtuellen Authentifizierungsserver
4. Konfigurieren eines LDAP-Authentifizierungsservers und einer Richtlinie für die Instanz
5. Binden des LDAP-Authentifizierungsservers und der Richtlinie an Ihren virtuellen Authentifizierungsserver, der auf der Instanz konfiguriert ist

Konfigurationsdetails:

In der folgenden Tabelle sind die erforderlichen Mindestsoftwareversionen aufgeführt, damit diese Integration erfolgreich funktioniert. Der Integrationsprozess wird auch die höheren Versionen desselben unterstützen.

Produkt	Erforderliche Mindestversion
Citrix ADC	Version 11.0, Advanced/Premium Lizenz

Bei den folgenden Anweisungen wird davon ausgegangen, dass Sie bereits die entsprechenden externen oder internen DNS-Einträge erstellt haben, um Authentifizierungsanforderungen an eine von NetScaler ADC überwachte IP-Adresse weiterzuleiten.

Bereitstellen von SSO Google Apps StyleBook-Konfigurationen:

Die folgende Aufgabe unterstützt Sie bei der Bereitstellung des Microsoft SSO Google Apps StyleBook in Ihrem Unternehmensnetzwerk.

So stellen Sie SSO Google Apps bereit | StyleBook

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfigurationen** >**StyleBooks**. Auf der Seite StyleBooks werden alle StyleBooks angezeigt, die für die Verwendung in Citrix ADM verfügbar sind. Scrollen Sie nach unten und suchen Sie **SSO Google Apps StyleBook**. Klicken Sie auf **Konfiguration erstellen**.
2. Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
3. Geben Sie Werte für die folgenden Parameter ein:

    a) **Name der Anwendung**. Name der SSO Google Apps-Konfiguration, die in Ihrem Netzwerk bereitgestellt werden soll.

    b) **Authentifizierung Virtuelle IP-Adresse**. Virtuelle IP-Adresse, die vom virtuellen Server für Authentifizierung, Autorisierung und Überwachung verwendet wird, an den die SAML-IdP-Richtlinie für Google Apps gebunden ist.

    c) **SAML-Regelausdruck**. Standardmäßig wird der folgende NetScaler ADC Richtlinienausdruck (PI) verwendet: HTTP.REQ.HEADER (“Referrer”) .CONTAINS (“Google”). Aktualisieren Sie dieses Feld mit einem anderen Ausdruck, wenn Ihre Anforderung anders ist. Dieser Richtlinienausdruck entspricht dem Datenverkehr, auf den diese SAML-SSO-Einstellungen angewendet werden, und stellt sicher, dass der Referrer-Header von einer Google-Domain stammt.

4. Im Abschnitt SAML-IdP-Einstellungen können Sie Ihre NetScaler ADC-Instanz als SAML-Identitätsanbieter konfigurieren, indem Sie das SAML-IdP-Profil und die Richtlinie erstellen, die von dem in Schritt 3 erstellten virtuellen Server für Authentifizierung, Autorisierung und Überwachung verwendet werden.

    a) **Name des SAML-Ausstellers**. Geben Sie in diesem Feld den öffentlichen FQDN Ihres virtuellen Authentifizierungsservers ein. Beispiel:`https://<Citrix ADC Auth VIP>/saml/login`

    b) **ID des SAML-Dienstanbieters (SP)**. (optional) Der NetScaler ADC Identity Provider akzeptiert SAML-Authentifizierungsanforderungen von einem Ausstellernamen, der mit dieser ID übereinstimmt.

c) **Assertion-Verbraucherdienst-URL**. Geben Sie die URL des Dienstanbieters ein, an die der NetScaler ADC Identity Provider die SAML-Assertionen nach erfolgreicher Benutzerauthentifizierung senden muss. Die Assertion-Consumer-Service-URL kann an der Server-Site des Identitätsanbieters oder der Service-Provider-Site initiiert werden

d) Es gibt weitere optionale Felder, die Sie in diesem Abschnitt eingeben können. Sie können beispielsweise die folgenden Optionen festlegen:

i. SAML-Bindungsprofil (das Standardprofil ist das "POST"-Profil).

ii. Signaturalgorithmus zum Überprüfen/Signieren von SAML-Anforderungen/Antworten (Standard ist "RSA-SHA1").

iii. Methode zum Digest von Hash für SAML-Anfragen/Antworten (Standard ist "SHA-1").

iv. Verschlüsselungsalgorithmus (Standard ist AES256) und andere Einstellungen.

> **Hinweis**
>
> Citrix empfiehlt, dass Sie die Standardeinstellungen beibehalten, da diese Einstellungen auf Kompatibilität mit Google Apps getestet wurden.

e) Sie können auch das Kontrollkästchen Benutzerattribute aktivieren, um die Benutzerdetails einzugeben, z. B.:

i. Name des Benutzerattributs

ii. NetScaler ADC PI-Ausdruck, der ausgewertet wird, um den Wert des Attributs zu extrahieren

iii. Benutzerfreundlicher Name des Attributs

iv. Wählen Sie das Format des Benutzerattributs aus.

Diese Werte sind in der ausgegebenen SAML-Assertion enthalten. Sie können bis zu fünf Sätze von Benutzerattributen in eine Assertion aufnehmen, die von NetScaler ADC mit diesem StyleBook ausgestellt wurde.

5. Geben Sie im Abschnitt LDAP-Einstellungen die folgenden Details ein, um Google Apps-Benutzer zu authentifizieren. Damit Domänenbenutzer mithilfe ihrer Unternehmens-E-Mail-Adressen bei der NetScaler ADC-Instanz anmelden können, müssen Sie Folgendes konfigurieren:

a) **LDAP-Basis (Active Directory)**. Geben Sie den Basisdomänennamen für die Domäne ein, in der sich die Benutzerkonten im Active Directory (AD) befinden, für die Sie die Authentifizierung zulassen möchten. Zum Beispiel `dc=netscaler:dc=com`

b) **LDAP (Active Directory) Bindet DN**. Fügen Sie ein Domänenkonto hinzu (unter Verwendung einer E-Mail-Adresse zur Vereinfachung der Konfiguration), das über die Rechte zum

Durchsuchen der AD-Struktur verfügt. Beispiel:`cn=Manager,dc=netscaler,dc=com`

c) **LDAP (Active Directory) Bindet DN Kennwort**. Geben Sie das Kennwort des Domänenkontos für die Authentifizierung ein.

d) Einige andere Felder, die Sie in diesem Abschnitt eingeben müssen, sind wie folgt:

i. LDAP-Server-IP-Adresse, mit der NetScaler ADC eine Verbindung zur Authentifizierung von Benutzern herstellt

ii. FQDN-Name des LDAP-Servers

> **Hinweis:**
>
> Sie müssen mindestens eine der beiden oben genannten angeben - die IP-Adresse des LDAP-Servers oder den FQDN-Namen.

iii. LDAP-Serverport, mit dem NetScaler ADC eine Verbindung zur Authentifizierung von Benutzern herstellt (Standard ist 389).

iv. LDAP-Hostname. Dies wird verwendet, um das LDAP-Zertifikat zu validieren, wenn die Validierung aktiviert ist (standardmäßig deaktiviert).

v. LDAP-Anmeldenamen-Attribut. Das Standardattribut zum Extrahieren von Anmeldenamen ist "sAMAccountName".

vi. Weitere optionale verschiedene LDAP-Einstellungen

6. Im Abschnitt SAML-IdP-SSL-Zertifikat können Sie die Details des SSL-Zertifikats angeben:

a) **Name des Zertifikats**. Geben Sie den Namen des SSL-Zertifikats ein.

b) **Zertifikatdatei**. Wählen Sie die SSL-Zertifikatsdatei aus dem Verzeichnis auf Ihrem lokalen System oder auf NetScaler ADM.

c) **CertKey-Format**. Wählen Sie das Format des Zertifikats und der Dateien mit privatem Schlüssel aus dem Dropdownlistenfeld aus. Die unterstützten Formate sind Erweiterungen PEM und .der.

d) **Name des Zertifikatsschlüssels**. Geben Sie den Namen des privaten Zertifikatsschlüssels ein.

e) **Zertifikatsschlüsseldatei**. Wählen Sie die Datei mit dem privaten Schlüssel des Zertifikats von Ihrem lokalen System oder von NetScaler ADM aus.

f) **Kennwort für privaten Schlüssel**. Wenn Ihre private Schlüsseldatei durch eine Passphrase geschützt ist, geben Sie sie in dieses Feld ein.

g) Sie können auch das Kontrollkästchen Erweiterte Zertifikatseinstellungen aktivieren, um Details wie den Benachrichtigungszeitraum für den Ablauf des Zertifikats einzugeben und die Ablaufüberwachung des Zertifikats zu aktivieren oder zu deaktivieren.

7. Optional können Sie das IdP-SSL-CA-Zertifikat auswählen, wenn für das oben angegebene SAML-IdP-Zertifikat ein öffentliches CA-Zertifikat auf NetScaler ADC installiert sein muss. Stellen Sie sicher, dass Sie in den erweiterten Einstellungen "Ist ein CA-Zertifikat"ausgewählt haben.
8. Optional können Sie SAML SP SSL-Zertifikat auswählen, um das Google-SSL-Zertifikat (öffentlicher Schlüssel) anzugeben, das zum Validieren von Authentifizierungsanforderungen von Google Apps (SAML SP) verwendet wird.
9. Klicken Sie auf **Zielinstanzen**, und wählen Sie die NetScaler ADC-Instanz (en) aus, für die diese Google Apps SSO-Konfiguration bereitgestellt werden soll. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und die Konfiguration auf den ausgewählten NetScaler ADC-Instanzen bereitzustellen.

   > **Hinweis**
   >
   > Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte NetScaler ADC-Instanzen in NetScaler ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

   auch,

   > **Tipp**
   >
   > Citrix empfiehlt, dass Sie vor dem Ausführen der eigentlichen Konfiguration**Dry Run**auswählen, um die Konfigurationsobjekte, die auf den NetScaler ADC-Zielinstanzen (n) vom StyleBook erstellt wurden, visuell zu bestätigen.

SSO Office 365 StyleBook

February 5, 2024

Microsoft™ Office 365 ist eine Suite von Cloud-basierten Produktivitäts- und Kollaborationsanwendungen, die von Microsoft auf Abonnementbasis bereitgestellt werden. Es umfasst die beliebten serverbasierten Anwendungen von Microsoft wie Exchange, SharePoint, Office und Skype for Business. Single Sign-On (SSO) ermöglicht Benutzern den Zugriff auf alle Cloud-Unternehmensanwendungen:

- Einschließlich Administratoren, die sich bei der Verwaltungskonsole anmelden

- Einmalige Anmeldung für alle Microsoft Office 365-Dienste mit ihren Unternehmensanmeldeinformationen.

Mit dem SSO Office 365 StyleBook können Sie SSO für Microsoft Office 365 über NetScaler ADC-Instanzen aktivieren. Sie können jetzt die SAML-Authentifizierung mit NetScaler ADC als SAML-Identitätsanbieter (IdP) und Microsoft Office 365 als SAML-Dienstanbieter konfigurieren.

Das Aktivieren von SSO für Microsoft Office 365 in einer NetScaler ADC-Instanz mit diesem StyleBook umfasst die folgenden Schritte:

1. Konfigurieren des virtuellen Authentifizierungsservers
2. Konfiguration einer SAML-IDP-Richtlinie und eines Profils
3. Binden der Richtlinie und des Profils an den virtuellen Authentifizierungsserver
4. Konfigurieren eines LDAP-Authentifizierungsservers und einer Richtlinie für die Instanz
5. Binden des LDAP-Authentifizierungsservers und der Richtlinie an Ihren virtuellen Authentifizierungsserver, der auf der Instanz konfiguriert ist.

In der Tabelle sind die erforderlichen Mindestsoftwareversionen aufgeführt, damit diese Integration erfolgreich funktioniert. Der Integrationsprozess sollte auch mit höheren Versionen derselben funktionieren.
Product	Erforderliche Mindestversion
———	———————
Citrix ADC	11.0, Advanced/Premium-Lizenz

In den folgenden Anweisungen wird davon ausgegangen, dass Sie bereits die entsprechenden externen und internen DNS-Einträge erstellt haben. Diese Einträge sind wichtig, um Authentifizierungsanforderungen an eine von NetScaler ADC überwachte IP-Adresse weiterzuleiten.

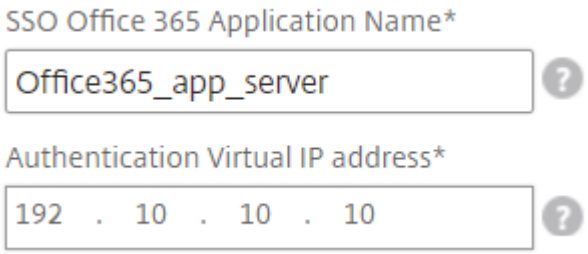
Die folgenden Anweisungen helfen Ihnen bei der Implementierung des SSO Office 365 StyleBook in Ihrem Unternehmensnetzwerk.

So stellen Sie SSO Microsoft Office 365 StyleBook bereit

1. Navigieren Sie in Citrix Application Delivery Management (ADM) zu **Anwendungen** > **StyleBooks**. Auf der Seite **StyleBooks** werden alle StyleBooks angezeigt, die für Ihre Verwendung in NetScaler ADM verfügbar sind. Scrollen Sie nach unten und suchen Sie **SSO Office 365 StyleBook**. Klicken Sie auf **Konfiguration erstellen**.
2. Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
3. Geben Sie Werte für die folgenden Parameter ein:

    a) **Name der Anwendung**. Name der SSO Microsoft Office 365-Konfiguration, die in Ihrem Netzwerk bereitgestellt werden soll.

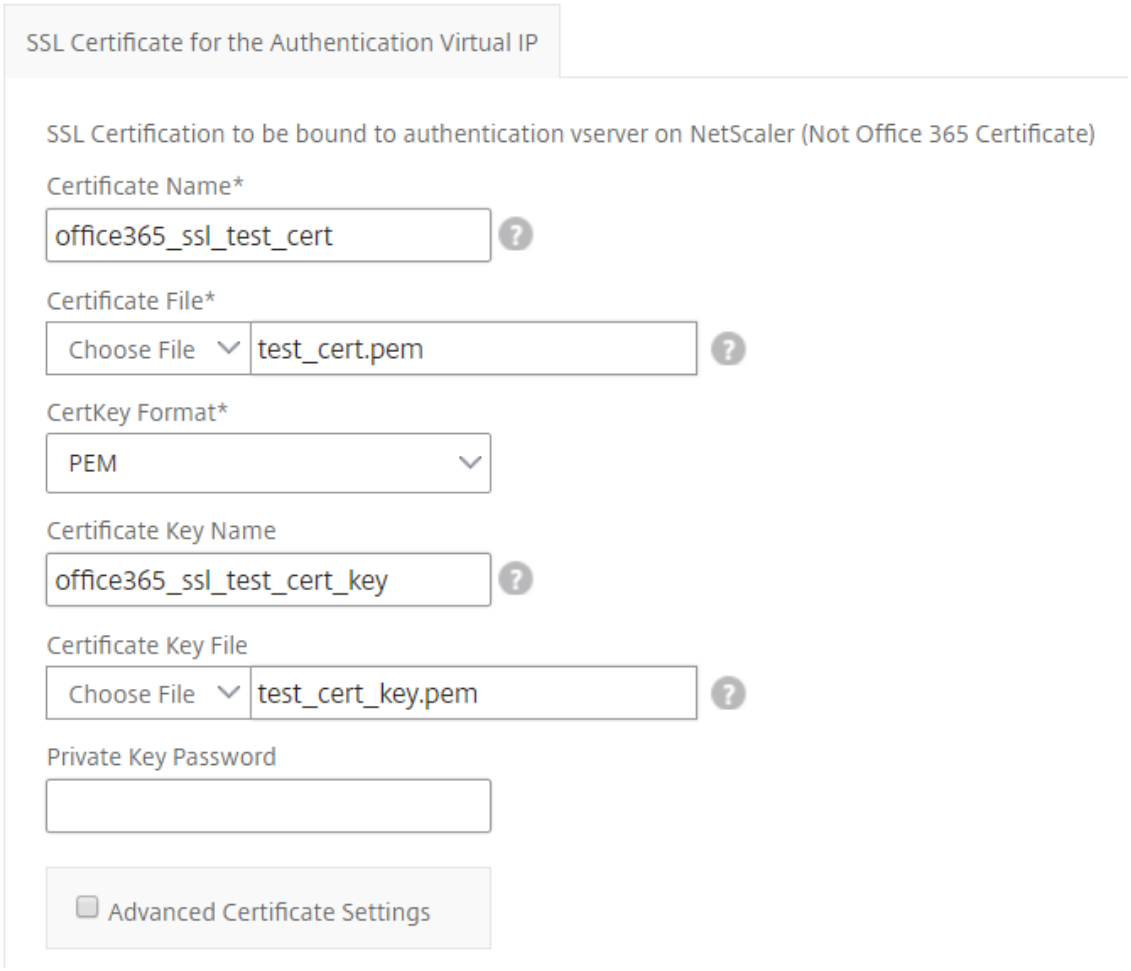
b) **Authentifizierung Virtuelle IP-Adresse**. Virtuelle IP-Adresse, die von dem virtuellen AAA-Server verwendet wird, an den die Microsoft Office 365-SAML-IdP-Richtlinie gebunden ist.



4. Geben Sie im Abschnitt**SSL-Zertifikatseinstellungen**die Namen des SSL-Zertifikats und den Zertifikatsschlüssel ein.

   > **Hinweis**
   >
   > Dies ist nicht das Office 365-Dienstanbieterzertifikat. Dieses SSL-Zertifikat ist an den virtuellen Authentifizierungsserver der NetScaler ADC-Instanz gebunden.

5. Wählen Sie die entsprechenden Dateien aus Ihrem lokalen Speicherordner aus. Sie können auch das Kennwort für den privaten Schlüssel eingeben, um verschlüsselte private Schlüssel im PEM-Format zu laden.



6. Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Ablauf der Benachrichtigung des Zertifikats eingeben, den Ablaufmonitor des Zertifikats aktivieren oder deaktivieren.
7. Optional können Sie das Kontrollkästchen **SSL-CA-Zertifikat für die virtuelle IP-Authentifizierung** aktivieren, wenn für das SSL-Zertifikat ein öffentliches Zertifizierungsstellenzertifikat auf NetScaler ADC installiert sein muss. Stellen Sie sicher, dass Sie im obigen Abschnitt "**Erweiterte Zertifikatseinstellungen"die Option "Ist ein CA-Zertifikat** "auswählen.
8. Geben Sie im Abschnitt **LDAP-Einstellungen für SSO Office 365** die folgenden Details ein, um Office 365-Benutzer zu authentifizieren. Um Domänenbenutzern die Anmeldung bei der NetScaler ADC-Instanz mithilfe ihrer Unternehmens-E-Mail-Adressen zu ermöglichen, konfigurieren Sie Folgendes:

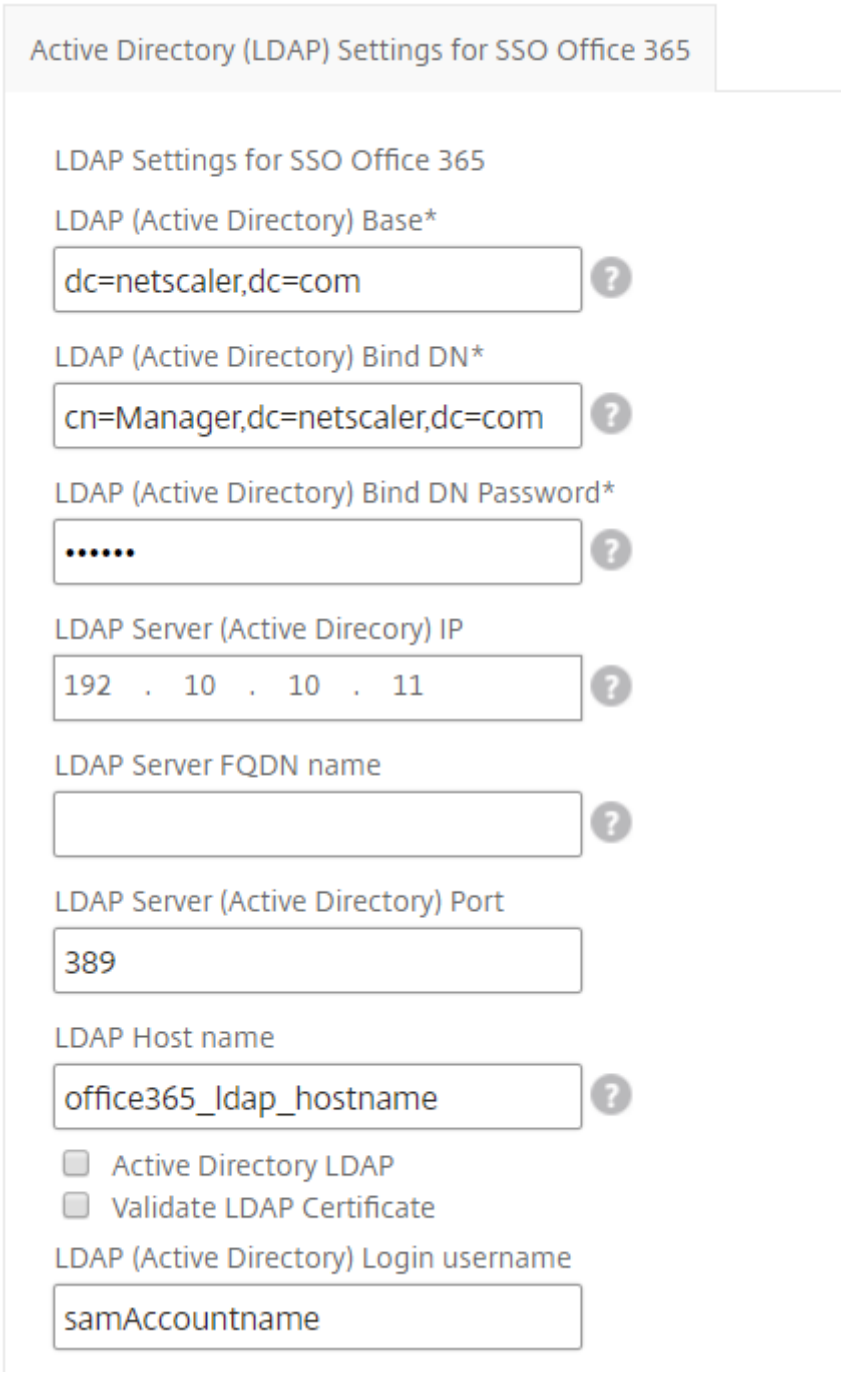
   - **LDAP-Basis (Active Directory)**. Geben Sie den Basisdomänennamen für die Domäne ein, in der sich die Benutzerkonten im Active Directory (AD) befinden, um die Authentifizierung zu ermöglichen. Zum Beispiel dc=netscaler, dc=com
   - **LDAP (Active Directory) Bindet DN**. Fügen Sie ein Domänenkonto hinzu (unter Verwen-

dung einer E-Mail-Adresse zur Vereinfachung der Konfiguration), das über die Rechte zum Durchsuchen der AD-Struktur verfügt. Zum Beispiel cn=Manager, dc=netscaler, dc=com

- **LDAP (Active Directory) Bindet DN Kennwort**. Geben Sie das Kennwort des Domänenkontos für die Authentifizierung ein.
- Einige andere Felder, die Sie in diesem Abschnitt eingeben müssen, sind wie folgt:
  - LDAP-Server-IP-Adresse, mit der NetScaler ADC eine Verbindung zur Authentifizierung von Benutzern herstellt.
  - Der FQDN-Name des LDAP-Servers.

    > **Hinweis:**
    >
    > Sie müssen mindestens eine der beiden oben genannten angeben - die IP-Adresse des LDAP-Servers oder den FQDN-Namen.

  - LDAP-Serverport, mit dem NetScaler ADC eine Verbindung zur Authentifizierung von Benutzern herstellt (Standard ist 389). LDAPS verwendet 636.
  - LDAP-Hostname. Der Hostname wird verwendet, um das LDAP-Zertifikat zu validieren, wenn die Validierung aktiviert ist (standardmäßig ist sie deaktiviert).
  - LDAP-Anmeldenamen-Attribut. Das Standardattribut, das zum Extrahieren von Anmeldenamen verwendet wird, ist samAccountname.
  - Andere optionale verschiedene LDAP-Einstellungen.



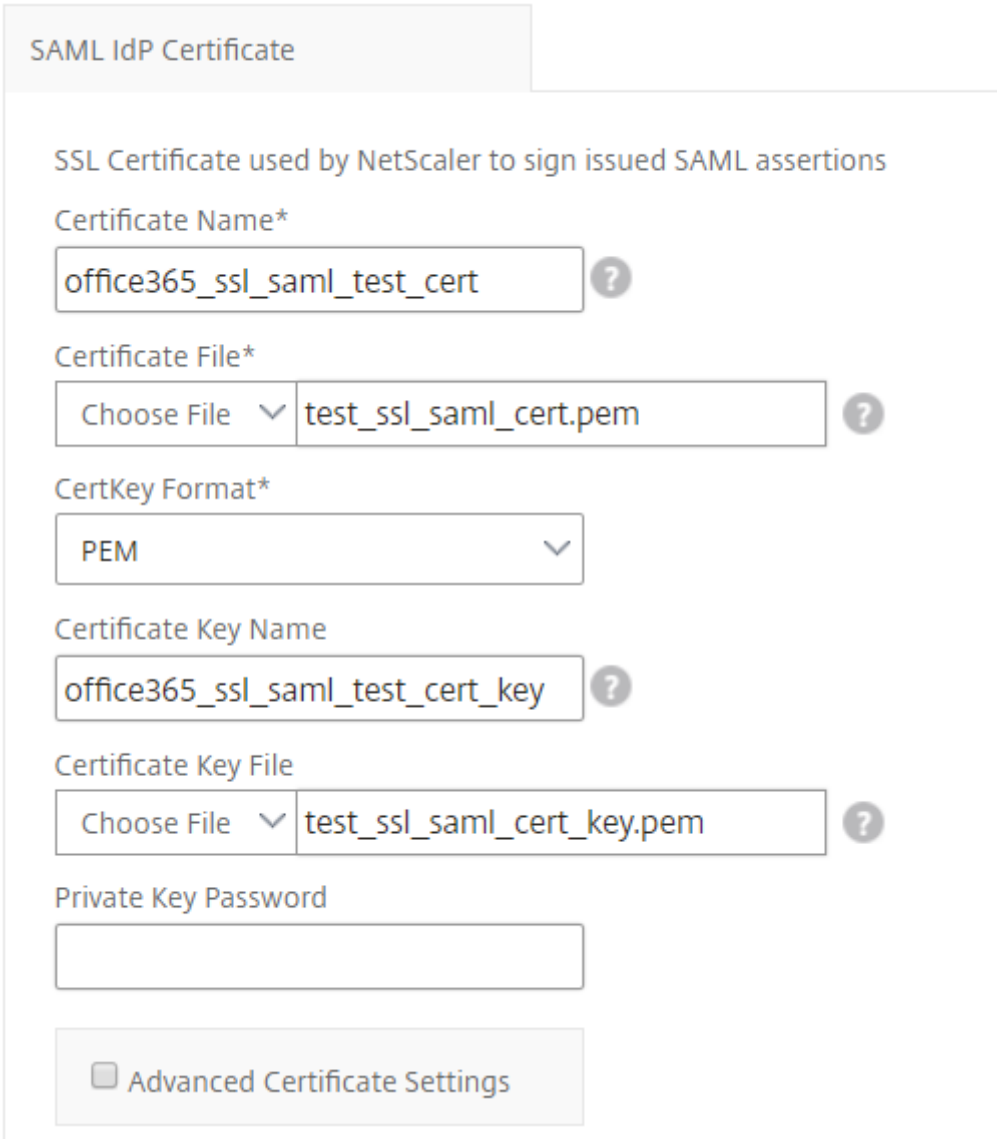
9. Im Abschnitt **SAML-IdP-Zertifikat** können Sie die Details der SSL-Zertifikate angeben, die für die SAML-Assertion verwendet werden.

   - **Name des Zertifikats**. Geben Sie den Namen des SSL-Zertifikats ein.
   - **Zertifikatdatei**. Wählen Sie die SSL-Zertifikatsdatei aus dem Verzeichnis auf Ihrem lokalen System.
   - **CertKey-Format**. Wählen Sie das Format des Zertifikats und der Dateien mit privatem

Schlüssel aus dem Dropdownlistenfeld aus. Die unterstützten Formate sind die Dateierweiterungen.pem und .der.

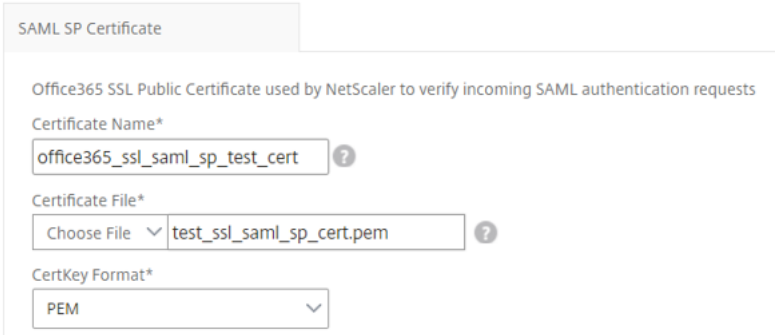
- **Name des Zertifikatsschlüssels**. Geben Sie den Namen des privaten Zertifikatsschlüssels ein.
- **Zertifikatsschlüsseldatei**. Wählen Sie die Datei mit dem privaten Schlüssel des Zertifikats aus Ihrem lokalen System aus.
- **Kennwort für privaten Schlüssel**. Geben Sie die Passphrase ein, die Ihre private Schlüsseldatei schützt.

Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Ablauf der Benachrichtigung des Zertifikats eingeben, den Ablaufmonitor des Zertifikats aktivieren oder deaktivieren.



10. Optional können Sie **SAML-IdP-Zertifizierungsstellenzertifikat** auswählen, wenn für das oben eingegebene SAML-IdP-Zertifikat ein öffentliches Zertifizierungsstellenzertifikat auf NetScaler ADC installiert werden muss. Stellen Sie sicher, dass Sie im obigen Abschnitt „ **Erweiterte**Zertifikatseinstellungen“die Option Ist ein CA-Zertifikat** auswählen.
11. Geben Sie im Abschnitt **SAML-SP-Zertifikat** die folgenden Details für das öffentliche Office 365-SSL-Zertifikat ein. Dieses Zertifikat wird von der NetScaler ADC-Instanz verwendet, um eingehende SAML-Authentifizierungsanforderungen zu überprüfen.

    - **Name des Zertifikats**. Geben Sie den Namen des SSL-Zertifikats ein.
    - **Zertifikatdatei**. Wählen Sie die SSL-Zertifikatsdatei aus dem Verzeichnis auf Ihrem lokalen System.
    - **CertKey-Format**. Wählen Sie das Format des Zertifikats und der Dateien mit privatem Schlüssel aus dem Dropdownlistenfeld aus. Die unterstützten Formate sind die Dateierweiterungen.pem und .der.
    - Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Ablauf der Benachrichtigung des Zertifikats eingeben, den Ablaufmonitor des Zertifikats aktivieren oder deaktivieren.



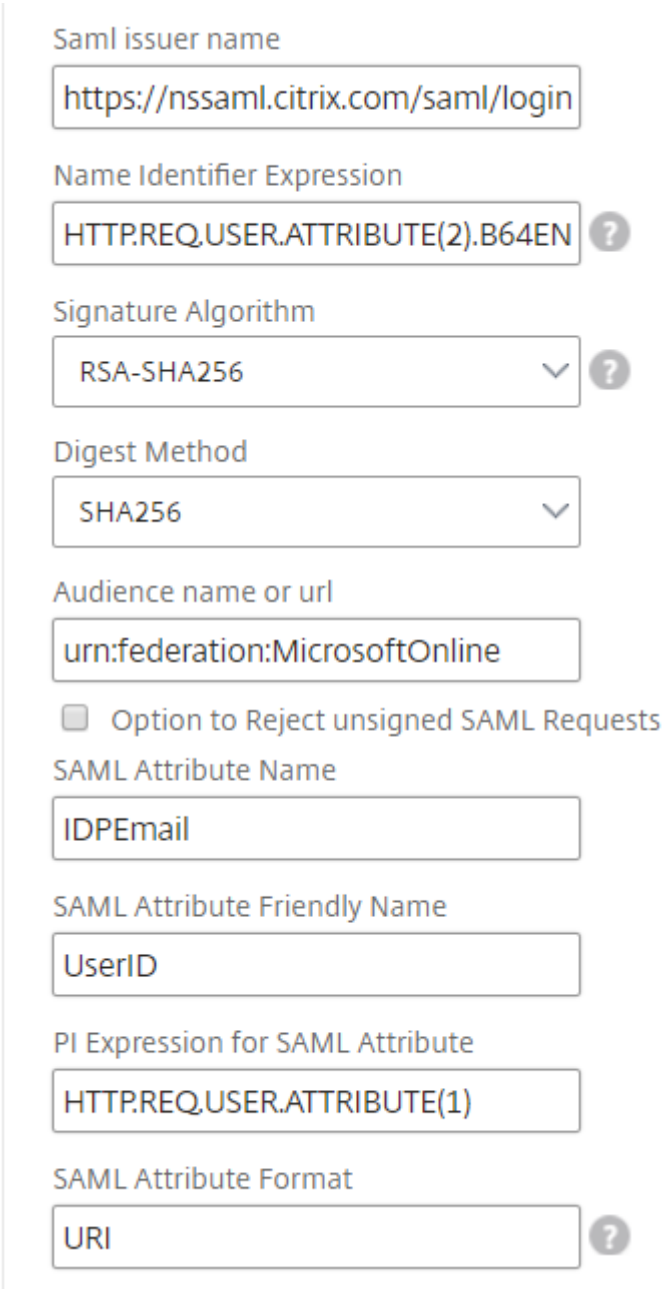
12. Im Abschnitt **SAML-Idp-Einstellungen** können Sie Ihre Citrix ADC-Instanz als SAML-Identitätsanbieter konfigurieren, indem Sie das SAML-IDP-Profil und die Richtlinie erstellen, die vom in Schritt 3 erstellten virtuellen AAA-Server verwendet werden.

    - **Name des SAML-Ausstellers**. Geben Sie in diesem Feld den öffentlichen FQDN Ihres virtuellen Authentifizierungsservers ein. Beispiel:`https://<Citrix ADC Auth VIP>/saml/login`
    - **Namensbezeichner-Ausdruck**. Geben Sie den NetScaler ADC-Ausdruck ein, der ausgewertet wird, um den in der SAML-Assertion gesendeten SAML-NameIdentifier zu extrahieren. Beispiel:`"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`
    - **Signaturalgorithmus**: Wählen Sie den Algorithmus zum Überprüfen/Signieren von SAML-Anfragen/Antworten aus (Standard ist „RSA-SHA256“).

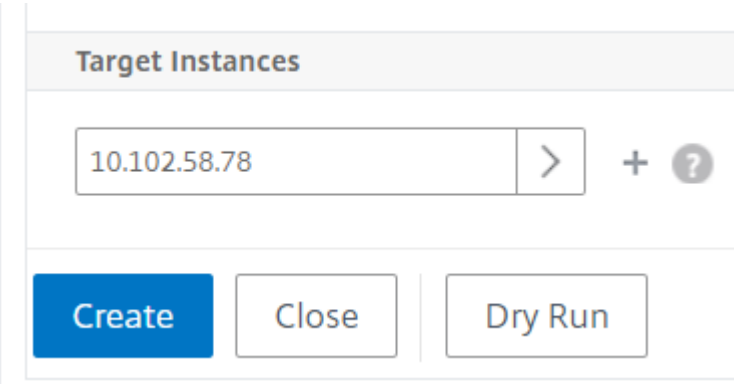
- **Digest-Methode**. Wählen Sie die Methode aus, um den Hash für SAML-Anforderungen/Antworten zu verdauen (Standard ist „SHA256“).
- **Name des Publikums**. Geben Sie den Namen oder die URL der Entität ein, die den Dienstanbieter darstellt (Microsoft Office 365).
- **ID des SAML-Dienstanbieters (SP)**. (optional) Der NetScaler ADC Identity Provider akzeptiert SAML-Authentifizierungsanforderungen von einem Ausstellernamen, der mit dieser ID übereinstimmt.
- **Assertion-Verbraucherdienst-URL**. Geben Sie die URL des Dienstanbieters ein, an die der NetScaler ADC Identity Provider die SAML-Assertionen nach erfolgreicher Benutzerauthentifizierung senden muss. Die Assertion-Consumer-Service-URL kann an der Server-Site des Identitätsanbieters oder der Service-Provider-Site initiiert werden
- Es gibt weitere optionale Felder, die Sie in diesem Abschnitt eingeben können. Sie können beispielsweise die folgenden Optionen festlegen:
  - **SAML-Attributname**. Name des Benutzerattributs, das in SAML Assertion gesendet wurde.
  - **SAML-Attribut-freundlicher Name**. Anzeigename des in SAML Assertion gesendeten Benutzerattributs.
  - **PI-Ausdruck für SAML-Attribut**. Standardmäßig wird der folgende NetScaler ADC Policy (PI) -Ausdruck verwendet: HTTP.REQ.USER.ATTRIBUTE (1). Dieses Feld gibt das erste vom LDAP-Server (E-Mail) gesendete Benutzerattribut als SAML-Authentifizierungsattribut an.
  - Wählen Sie das Format des Benutzerattributs aus.

  Diese Werte sind in der ausgegebenen SAML-Assertion enthalten.

  > **Tipp**
  >
  > Citrix empfiehlt, die Standardeinstellungen beizubehalten, da diese Einstellungen für die Verwendung mit Microsoft Office 365-Apps getestet wurden.



13. Klicken Sie auf **Zielinstanzen**, und wählen Sie die NetScaler ADC-Instanz (en) aus, für die diese Microsoft Office 365-SSO-Konfiguration bereitgestellt werden soll. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und die Konfiguration auf den ausgewählten NetScaler ADC-Instanzen bereitzustellen.



Tipp

Citrix empfiehlt, dass Sie vor der Ausführung der eigentlichen Konfiguration die Option**Dry Run**auswählen, um die Konfigurationsobjekte anzuzeigen, die vom StyleBook auf den Citrix ADC Zielinstanzen erstellt werden.

Microsoft Skype for Business StyleBook

February 5, 2024

Die Skype for Business 2015-Anwendung ist auf mehrere externe Komponenten angewiesen, um zu funktionieren. Das Skype for Business-Netzwerk besteht aus verschiedenen Systemen wie Servern und deren Betriebssystemen, Datenbanken, Authentifizierungs- und Autorisierungssystemen, Netzwerksystemen und -infrastrukturen sowie Telefon-PBX-Systemen. Skype for Business Server 2015 ist in zwei Versionen verfügbar: Standard Edition und Enterprise Edition. Der Hauptunterschied besteht in der Unterstützung von Hochverfügbarkeitsfunktionen, die nur in der Enterprise Edition enthalten sind. Um Hochverfügbarkeit zu implementieren, müssen mehrere Front-End-Server in einem Pool bereitgestellt und SQL-Server gespiegelt werden.

Eine Enterprise Edition-Bereitstellung ermöglicht die Erstellung mehrerer Server mit unterschiedlichen Rollen.

Primäre Komponenten

Die Hauptkomponenten der Skype for Business 2015-Anwendung sind:

- Front-End-Server
- Edge-Server
- Director-Server
- Datenbankserver (SQL)

Front-End-Server

In der Skype for Business-Anwendung ist der Front-End-Server der Kernserver in Ihrem Netzwerk. Es stellt die Links und Dienste für Benutzerauthentifizierung, Registrierung, Präsenz, Adressbuch, A/V-Konferenzen, Anwendungsfreigabe, Instant Messaging und Webkonferenzen bereit. Wenn Sie Skype for Business 2015 Enterprise Edition bereitstellen, besteht die Topologie in der Regel aus mindestens zwei Front-End-Servern mit Lastausgleich in einem Front-End-Pool mit einem Datenbankserver, der die SQL Server-Instanz hostet, auf der sich die Skype for Business-Datenbank befindet.

Edge-Server

Die Bereitstellung von Edge-Servern für Skype for Business ist erforderlich, wenn externe Benutzer, die nicht im internen Netzwerk Ihrer Organisation angemeldet sind, in der Lage sein müssen, mit internen Benutzern zu interagieren. Bei diesen externen Benutzern kann es sich um authentifizierte und anonyme Remotebenutzer, Verbundpartner oder andere mobile Clients handeln.

Auf dem Skype for Business Edge-Server gibt es vier Arten von Rollen:

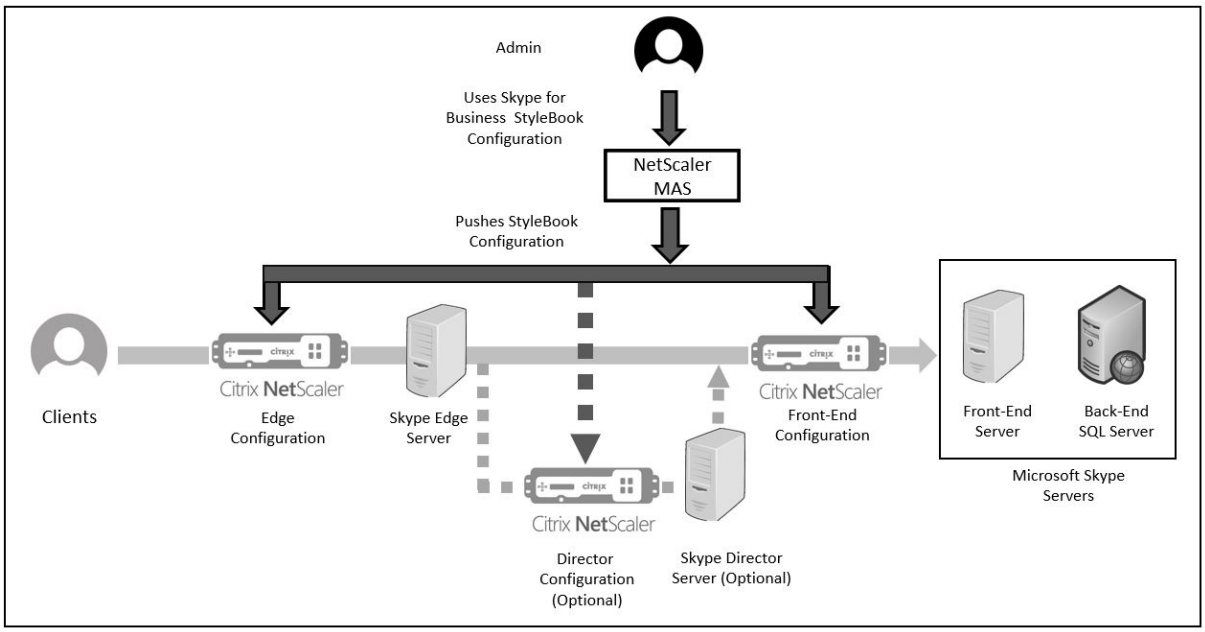
- Access Edge, der SIP-Datenverkehr verarbeitet und externe Verbindungen authentifiziert, Remoteverbindung ermöglicht und Verbundverbindung ermöglicht
- Webkonferenzen, die Datenkonferenzpakete verarbeiten und externen Benutzern den Zugriff auf Skype for Business ermöglichen
- A/V-Konferenzen, die A/V-Konferenzpakete verarbeiten und Audio und Video, App-Sharing und Dateiübertragung auf externe Benutzer ausweiten
- XMPP Proxy, der XMPP-Pakete verarbeitet und XMPP-basierten Servern oder Clients die Verbindung zu Skype for Business ermöglicht.

Director-Server

Die Hauptfunktion des Director-Servers in Skype for Business 2015 besteht darin, Endpunkte zu authentifizieren und die Benutzer an den Pool weiterzuleiten, der ihr Konto enthält. In Skype for Business 2015 ist der Director zwar eine vollständig dedizierte und spezifische Rolle auf einem eigenständigen Server, aber ein optionaler Server. Dies erleichtert die Sicherheit, da es einfacher ist, die Konfigurationen bereitzustellen oder zu entfernen.

Directors sind am nützlichsten, wenn mehrere Pools vorhanden sind, da sie einen einzigen Ansprechpartner für die Authentifizierung von Endpunkten bieten. Darüber hinaus dient ein Director für Remote-Benutzer als zusätzlicher Hop zwischen dem Edge-Pool und dem Front-End-Pool und bietet eine zusätzliche Schutzschicht vor Angriffen.

Die folgende Abbildung zeigt die Bereitstellung von Skype-Servern im Netzwerk:



Konfigurieren von NetScaler ADC-Instanzen in einem Unternehmen

In der folgenden Tabelle sind die IP-Adressen aufgeführt, die in der Beispielkonfiguration verwendet werden, die in den folgenden Anweisungen enthalten ist:

Skype for Business-Server	Virtuelle IP-Adresse	Server-IP-Adressen	NetScaler ADC-Instanz
Edge-Server	Externer VIP - 192.20.20.20 Interne VIP - 10.10.10.20	192.20.20.21; 192.20.20.22 10.10.10.21; 10.10.10.22	10.102.29.141
Front-End-Server	10.10.10.10	10.10.10.11; 10.10.10.12	10.102.29.60
Director-Server	10.10.10.30	10.10.10.31; 10.10.10.32	10.102.29.93

So konfigurieren Sie Front-End-Server

1. Navigieren Sie in Citrix Application Delivery Management (ADM) zu **Anwendungen** > **Konfiguration**und klicken Sie auf **Neu erstellen**. Auf der Seite **StyleBook auswählen** werden alle StyleBooks angezeigt, die für Ihre Verwendung in NetScaler ADM verfügbar sind. Scrollen Sie nach unten und wählen Sie **Microsoft Skype for Business 2015 StyleBook**. Das StyleBook öffnet

sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

2. Geben Sie im Abschnitt **Edge-Server** die folgenden virtuellen IP-Adressen (VIP) und IP-Adressen aller Edge-Server im Netzwerk ein.

   a) Externe VIP-Adresse und IP-Adressen für die Edge-Server, die für Access Edge, Webkonferenz-Edge und A/V Edge verwendet werden.
   b) Interne VIP-Adresse und IP-Adressen für die Edge-Server, die mit dem internen Netzwerk verbunden werden.
   c) Zwei externe und zwei interne Edge-Server in Ihrem Netzwerk.

3. Geben Sie im Abschnitt **Front-End-Server** die IP-Adresse des virtuellen Front-End-Servers (VIP) ein, der für die Skype for Business Front-End-Server erstellt werden soll. Geben Sie außerdem die IP-Adressen aller Skype for Business-Front-End-Server im Netzwerk ein.
4. Geben Sie im Abschnitt **Director Server** die virtuelle IP-Adresse (VIP) für die Director-Server ein, die für die Skype for Business-Anwendung erstellt werden sollen. Geben Sie außerdem die IP-Adressen für alle Skype for Business Director-Server im Netzwerk ein. Erstellen Sie mindestens zwei Director-Server für hohe Verfügbarkeit.
5. Im Abschnitt **Erweiterte Einstellungen** werden alle Standardports aufgeführt, die auf den NetScaler ADC-Instanzen für die drei Skype-Server konfiguriert sind.

Die folgende Tabelle enthält eine Liste aller Standardports und -protokolle:

Beschriftung	Port	Protokoll	Beschreibung
HTTP-Anschluss	80	HTTP	Wird für die Kommunikation von Front-End-Servern zu den FQDNs der Webfarm verwendet, wenn HTTPS nicht verwendet wird.
HTTPS-Port	443	HTTPS	Wird für die Kommunikation von Front-End-Servern zu den FQDNs der Webfarm verwendet.

Beschriftung	Port	Protokoll	Beschreibung
Interner AutoDiscover-Port	4443	HTTPS	HTTPS (von Reverse Proxy) und HTTPS-Front-End-Kommunikation zwischen Pools für die AutoDiscover-Anmeldung.
RPC Port	135	DCOM und Remote-Prozeduraufruf (RPC)	Wird für DCOM-basierte Vorgänge wie das Verschieben von Benutzern, die Synchronisation des Benutzerreplikators und die Adressbuch-synchronisierung verwendet.
SIP-Anschluss	5061	TCP (TLS)	Wird von Front-End-Servern für die gesamte interne SIP-Kommunikation verwendet.
SIP Focus-Anschluss	444	HTTPS, TCP	Wird für die HTTPS-Kommunikation zwischen Focus (der Komponente, die den Skype-Konferenzstatus verwaltet) und den einzelnen Servern verwendet.
SIP-Gruppenanschluss	5071	TCP	Wird für eingehende SIP-Anfragen für die Antwortgruppenan-wendung verwendet.

Beschriftung	Port	Protokoll	Beschreibung
SIP AppSharing-Anschluss	5065	TCP	Wird für eingehende SIP-Abhöranforderungen für die Anwendungsfreigabe verwendet.
SIP-Attendant-Anschluss	5072	TCP	Wird für eingehende SIP-Anfragen für die Telefonzentrale (d. h. für Einwahlkonferenzen) verwendet.
Port für SIP-Conf-Ankündigung	5073	TCP	Wird für eingehende SIP-Anfragen für den Skype for Business-Serverkonferenzankündigungsdiens (d. h. für Einwahlkonferenzen) verwendet.
SIP CallPark-Anschluss	5075	TCP	Wird für eingehende SIP-Anfragen für die CallPark-Anwendung verwendet.
SIP-Anruf-Zugangsport	448	TCP	Wird vom Skype for Business-Serverbandbreitenrichtliniendienst zur Anrufzugangss-teuerung verwendet.
TURN-Anschluss für SIP-Anruf	5080	TCP	Wird vom Bandbreiten-richtliniendienst für Audio/Video Edge TURN-Verkehr zur An-rufzugangssteuerung verwendet.
SIP-Audiotestanschluss	5076	TCP	Wird für eingehende SIP-Anfragen für den Audiotestdienst verwendet.

Beschriftung	Port	Protokoll	Beschreibung
Externer HTTPS-Anschluss	443	HTTPS	Wird für externe Ports für die SIP/TLS-Kommunikation für den Remote-Benutzerzugriff, den Zugriff auf interne Webkonferenzen und STUN/TCP-eingehende und ausgehende Medienkommunikation für den Zugriff auf interne Medien und A/V-Sitzungen verwendet.
Interner HTTPS-Port	443	HTTPS	Wird für interne Ports für die SIP/TLS-Kommunikation für den Remote-Benutzerzugriff, den Zugriff auf interne Webkonferenzen und STUN/TCP-eingehende und ausgehende Medienkommunikation für den Zugriff auf interne Medien und A/V-Sitzungen verwendet.
Externer SIP-Remotezugriffsan	5061	TCP	Wird für externe Ports für die SIP/MTLS-Kommunikation für den Remote-Benutzerzugriff oder den Verbund verwendet.

Beschriftung	Port	Protokoll	Beschreibung
Interner SIP-Fernzugriffsanschluss	5061	TCP	Wird für interne Ports für die SIP/MTLS-Kommunikation für den Remote-Benutzerzugriff oder den Verbund verwendet.
Externer SIP-STUN-UDP-Anschluss	3478	UDP	Wird für externe Ports für eingehende und ausgehende STUN/UDP-Medienkommunikation verwendet.
Interner SIP-STUN-UDP-Port	3478	UDP	Wird für interne Ports für eingehende und ausgehende STUN/UDP-Medienkommunikation verwendet.
Interner SIP-IM-Port	5062		Wird für interne Ports für die SIP/MTLS-Authentifizierung der ausgehenden IM-Kommunikation durch die interne Firewall verwendet.
HTTP-Anschluss	80	TCP	Wird für die erste Kommunikation von Directors mit den FQDNs der Webfarm verwendet.
HTTPS-Port	443	HTTPS	Wird für die Kommunikation von Directors zu den FQDNs der Webfarm verwendet.

Beschriftung	Port	Protokoll	Beschreibung
Interner AutoDiscover-Port	4443	HTTPS	Wird für die Kommunikation zwischen Pools über HTTPS (von Reverse Proxy) und HTTPS Director für die AutoDiscover-Anmeldung verwendet.
SIP Internal Port	5061	TCP	Wird für die interne Kommunikation zwischen Servern und für Client-Verbindungen verwendet.

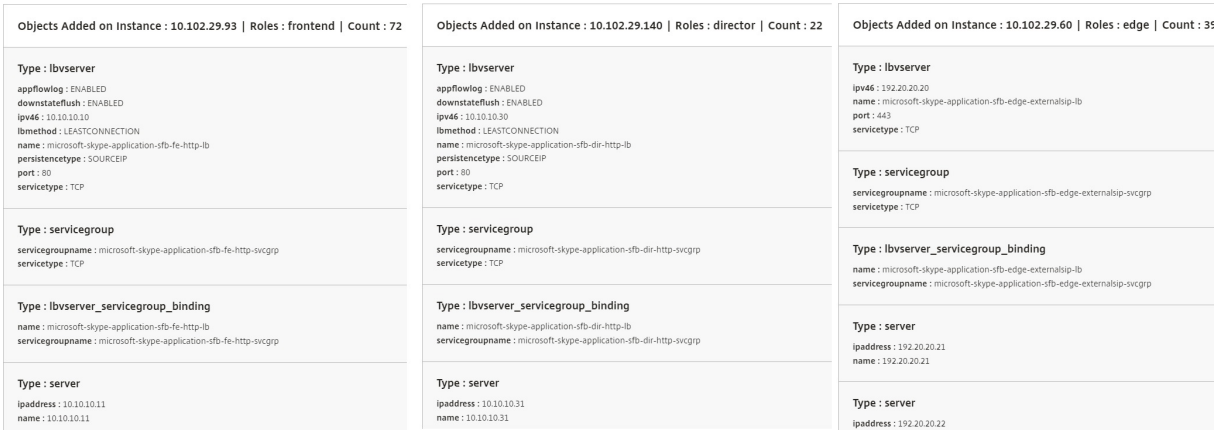
6. Wählen Sie im Abschnitt **Zielinstanzen die drei verschiedenen Citrix ADC-Instanzen** aus, auf denen die drei Skype for Business-Server bereitgestellt werden sollen.

> **Hinweis**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

7.Klicken Sie auf**Erstellen**, um die Konfiguration für die ausgewählten Citrix ADC Instanzen zu erstellen.

> **Tipp**
>
> Citrix empfiehlt, dass Sie**Dry Run**auswählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt werden müssen, bevor Sie die tatsächliche Konfiguration für die Instanz ausführen.
>
> Wenn die Konfiguration erfolgreich erstellt wurde, erstellt das StyleBook 25 virtuelle Server mit Lastenausgleich. Das heißt, für jeden Port wird ein virtueller Lastausgleichsserver zusammen mit einer Dienstgruppe definiert, und die Dienstgruppe ist an den virtuellen Lastausgleichsserver gebunden. Die Konfiguration fügt auch die Front-End-Server als Servicegruppenmitglieder hinzu und bindet sie an die Servicegruppe. Die Anzahl der erstellten Servicegruppenmitglieder entspricht der Anzahl der erstellten Front-End-Server.

Die folgende Abbildung zeigt die in jedem Server erstellten Objekte:



Microsoft Exchange-StyleBook

February 5, 2024

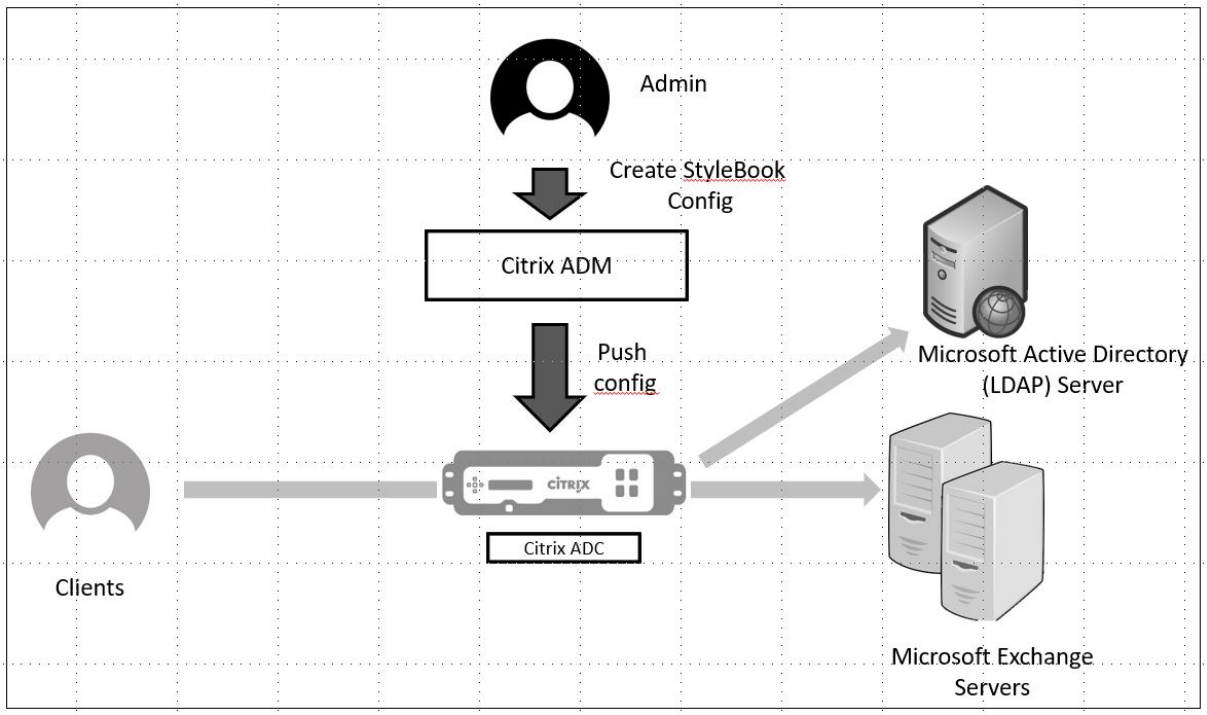
Sie können das Microsoft Exchange 2016 StyleBook verwenden, um eine NetScaler ADC-Konfiguration bereitzustellen, die eine Microsoft Exchange 2016-Unternehmensanwendung in Ihrem Netzwerk optimiert und schützt. Microsoft Exchange 2016 ist eine wichtige Unternehmensanwendung für die Bereitstellung von E-Mail-, Personal Information Management- und Messaging-Diensten für Ihre Mitarbeiter und andere Stakeholder.

NetScaler ADC-Funktionen, die mithilfe von Microsoft Exchange StyleBook konfiguriert wurden

Das Microsoft Exchange 2016 StyleBook aktiviert und konfiguriert die folgenden Citrix ADC-Funktionen für Microsoft Exchange 2016-Server:

- Load Balancing —Grundlegender Lastenausgleich, der den Lastenausgleich mehrerer
- Content Switching - Content Switching, dass Einzel-IP-Zugriff und Umleitung von Abfragen an die richtigen virtuellen Server mit Lastenausgleich ermöglicht
- Rewrite —Leitet Benutzer auf sichere Seiten um
- SSL-Offload - Verlagert die SSL-Verarbeitung an den NetScaler ADC, wodurch die Belastung des Exchange-Servers verringert wird

Die folgende Abbildung zeigt die Bereitstellung von Exchange-Servern im Netzwerk:



Voraussetzungen

- Für die zertifikatbasierte Authentifizierung müssen alle adressierbaren Hosts, die Teil des Netzwerk-Setups sind, auflösbare Domänennamen und nicht nur IP-Adressen haben.
- Stellen Sie sicher, dass die SIP-Ports im Microsoft Exchange 2016-Server zugänglich sind.

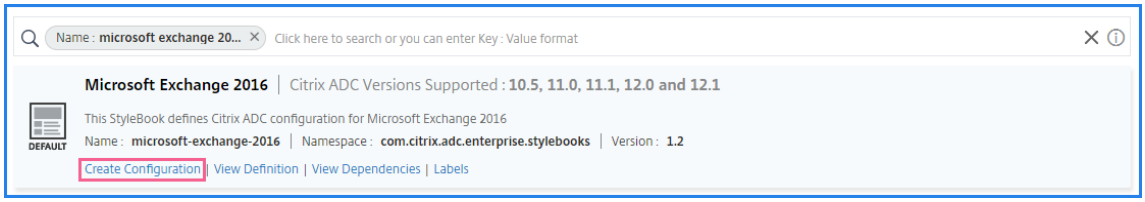
Microsoft Exchange StyleBook konfigurieren

Konfigurieren Sie das Microsoft Exchange StyleBook in Ihrem Unternehmen für die Bereitstellung der NetScaler ADC-Konfiguration.

So konfigurieren Sie Microsoft Exchange-Anwendung

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **StyleBooks**.
2. Suchen Sie nach **Microsoft Exchange 2016 StyleBook**, und klicken Sie auf **Konfiguration erstellen**.

   Das StyleBook wird als Benutzeroberflächenformular angezeigt, auf dem Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.



3. Geben Sie die Details für die folgenden Parameter ein:

   - **Exchange-Anwendungsname** —Name der Microsoft Exchange-Anwendung in Ihrem Netzwerk
   - **Exchange VIP** — Virtuelle IP-Adresse auf Citrix ADC, die Clientanfragen für die Microsoft Exchange-Anwendung empfängt
   - **Exchange Server-IPs** —IP-Adressen aller Exchange Server im Netzwerk.

     Wenn Sie weitere IP-Adressen hinzufügen möchten, klicken Sie auf das Pluszeichen (**+**). Normalerweise sind zwei Exchange-Server im Netzwerk konfiguriert.

4. Laden Sie im Abschnitt **Exchange-Zertifikate** Exchange-Zertifikate auf NetScaler ADM hoch. Geben Sie die Namen des Zertifikats und der Schlüsseldateien ein und laden Sie sie vom lokalen Speicher hoch. Sie können auch ein Kennwort für den privaten Schlüssel angeben, um die Schlüsseldatei zu verschlüsseln.

   > **Hinweis Stellen Sie**
   >
   > sicher, dass die Zertifikatsdateien das Format “.pem”oder “.der”aufweisen. NetScaler ADM lehnt die Dateien anderer Formate ab.

   Wenn Sie Details zum Ablauf des Zertifikats oder erweiterte Einstellungen angeben möchten, wählen Sie **Erweiterte Zertifikatseinstellungen**.

5. Konfigurieren Sie im Abschnitt **Konfiguration der Exchange Active Directory-Authentifizierung** die AD-Einstellungen, indem Sie die Daten eingeben.

   - **Active Directory-Authentifizierung VIP** —Die virtuelle IP-Adresse, die zum Erstellen und Konfigurieren des virtuellen AD (LDAP) -Servers auf einer Citrix ADC Appliance verwendet wird.
   - **Active Directory-Server-IP**—Die IP-Adresse Ihres Active Directory-Domänencontrollers.
   - **Active Directory-Basiszeichenfolge**—Die LDAP-Basiszeichenfolge in Active Directory. Beispiel: CN=Users, DC=CTXNSSFB, DC=COM.
   - **Active Directory LDAP Bind Distinguished Name (DN)** —LDAP Bind Distinguished Name (DN) wird verwendet, um dieses Objekt an den LDAP-Server (AD) zu binden. Beispiel: “cn=Administrator, cn=Users, dc=acme, dc=com”

- **Kennwort für Active Directory LDAP Bind Distinguished Name (DN)** —LDAP Bind Distinguished Name (DN) ist das Kennwort für die AD-Authentifizierung
- **Active Directory-Benutzernamenattribut** —AD-Attribut für den Benutzernamen. Der Citrix ADC verwendet das LDAP-Attribut, um externe Active Directory-Server abzufragen. Beispiel: "sAMAccountName"
- **Active Directory-Gruppenattributname**—Die auf dem LDAP-Server konfigurierten Namen der LDAP-Gruppenattribute. Zum Beispiel „memberOf"für das Gruppenattribut in LDAP.
- **Name des Active Directory-Unterattributs** —die Namen der LDAP-Unterattribute, die auf dem LDAP-Server konfiguriert sind. Zum Beispiel „cn"für das Unterattribut in LDAP.
- **Active Directory-Authentifizierungsdomäne** —Der für die Authentifizierung verwendete AD/LDAP-Domänenname. Zum Beispiel ctxnssfb.com.

6. Wählen Sie im Abschnitt**Zielinstanzen** die Citrix ADC-Instanz aus, auf der diese Exchange-Konfiguration bereitgestellt werden soll.

   > **Hinweis**
   >
   > Wenn Sie die kürzlich erkannten NetScaler ADC-Instanzen anzeigen möchten, klicken Sie auf das Aktualisierungssymbol.

7. Klicken Sie auf **Erstellen**, um die Konfigurationsdatei zu erstellen und die Konfiguration auf der ausgewählten Citrix ADC-Instanz auszuführen.

   Citrix empfiehlt, dass Sie zunächst**Dry Run**auswählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt wurden, bevor Sie die eigentliche Konfiguration auf der Instanz ausführen.

Wenn die Konfiguration erfolgreich erstellt wurde, hat das StyleBook einen virtuellen Content Switching-Server, fünf virtuelle Lastenausgleichsserver und eine LDAP-Richtlinie erstellt, die an einen virtuellen LDAP-Authentifizierungsserver gebunden ist. Außerdem wurden die entsprechenden Dienstgruppen erstellt und an die virtuellen Server mit Lastenausgleich gebunden.

Microsoft SharePoint-StyleBook

February 5, 2024

Microsoft SharePoint 2016 ist eine wichtige Unternehmensanwendung, die in erster Linie ein Dokumentenverwaltungs- und Speichersystem bietet, das hochgradig konfigurierbar ist und von allen gängigen Browsern unterstützt wird.

Sie können das Microsoft SharePoint 2016 StyleBook verwenden, um eine NetScaler ADC-Konfiguration bereitzustellen, die die Microsoft SharePoint 2016-Unternehmensanwendung in Ihrem Netzwerk optimiert und schützt.

Voraussetzungen

- Microsoft SharePoint 2016
- NetScaler ADM, Version 12.0 und höher
- NetScaler ADC, Version 10.5 und höher

Vom Microsoft SharePoint 2016 StyleBook konfigurierte NetScaler ADC-Funktionen

Sie können das Microsoft SharePoint 2016 StyleBook verwenden, um die folgenden NetScaler ADC-Funktionen für Microsoft SharePoint 2016 zu aktivieren und zu konfigurieren:

- Lastausgleich
- Content Switching
- Responder
- Rewrite
- Komprimierung
- Integriertes Caching

Lastausgleich

Der Citrix ADC Load Balancing verteilt Anfragen gleichmäßig an Backend-SharePoint-Server. Eine intelligente Überwachung der Backend-Server verhindert, dass Anfragen an fehlerhafte Server gesendet werden.

Das SharePoint-StyleBook konfiguriert 12 virtuelle Server mit Lastenausgleich, die jeweils für Lastenausgleichsanforderungen für einen bestimmten Inhaltstyp wie Dokumente, Bilder, Audio-, Video- und andere Dateitypen bestimmt sind.

Das SharePoint StyleBook unterstützt jetzt den SSL-Modus der SharePoint-Anwendung, indem SSL-basierte virtuelle LB-Server konfiguriert werden. Stellen Sie sicher, dass SSL als Frontend-Protokoll ausgewählt ist. Beachten Sie, dass der virtuelle Port standardmäßig auf 443 festgelegt ist. Sie können SSL auch auswählen, um Dienstgruppen (SharePoint-Anwendungsserver) an die virtuellen Zielserver für den Lastausgleich zu binden. Beachten Sie, dass das Backend-Protokoll standardmäßig auf HTTP gesetzt ist.

Content Switching

Content Switching wird verwendet, um Clientanforderungen auf mehrere virtuelle Server mit Lastenausgleich auf der Grundlage bestimmter Arten von angeforderten SharePoint-Inhalten (z. B. Dokumente, Bilder sowie Audio- oder Videodateien) zu verteilen. Das Content Switching-Modul leitet eingehenden Datenverkehr an einen optimal passenden virtuellen Lastausgleichsserver weiter, der diesen Inhaltstyp verarbeiten kann. Sie können daher unterschiedliche Optimierungsrichtlinien auf verschiedene Arten von Datenverkehr anwenden. Beispielsweise möchten Sie möglicherweise andere Komprimierungs- oder Caching-Richtlinien für Videos als für Textdokumente verwenden.

Responder

Die Responder-Funktionalität einer NetScaler ADC-Instanz kann verwendet werden, um Benutzer nahtlos von HTTP zu HTTPS umzuleiten. Der Responder kann auch so konfiguriert werden, dass er angepasste Fehlerseiten bereitstellt. Die Responderrichtlinie bestimmt die Anforderungen (Datenverkehr), für die eine Aktion ausgeführt werden muss, und bindet jede Richtlinie an einen virtuellen Lastausgleichsserver. Das SharePoint StyleBook enthält eine Konfiguration, die Benutzer von HTTP- zu HTTPS-URLs umleitet.

Neuschreiben

Das Rewrite-Modul wird verwendet, um Anforderungs-/Antwort-Header, URLs oder Inhalte im laufenden Betrieb zu ändern. Dieses Modul arbeitet im Einklang mit der Verkehrsverarbeitung und kann daher den Verkehrsfluss entsprechend für bestimmte Anwendungsfälle ändern. Beispielsweise kann das Umschreiben den Zugriff auf den angeforderten Inhalt ermöglichen, ohne unnötige Details über den Server der Website preiszugeben.

Im SharePoint StyleBook wird die Rewrite-Funktion verwendet, um unnötige Header aus Benutzeranforderungen zu entfernen.

Komprimierung

Das NetScaler ADC-Komprimierungsmodul identifiziert und komprimiert komprimierbaren Inhalt. Dieser Prozess verbessert die Datenübertragungszeit und reduziert die Anforderungen an die Netzwerkbandbreite für die Clients, während CPU-Zyklen auf SharePoint-Inhaltsservern eingespart werden. Eine NetScaler ADC-Instanz kann sowohl statische als auch dynamisch generierte Daten komprimieren. Es wendet den GZIP- oder den DEFLATE-Komprimierungsalgorithmus an, um fremde und sich wiederholende Informationen aus den Serverantworten zu entfernen und die ursprünglichen Informationen in einem kompakteren und effizienteren Format darzustellen. Die Fähigkeit des

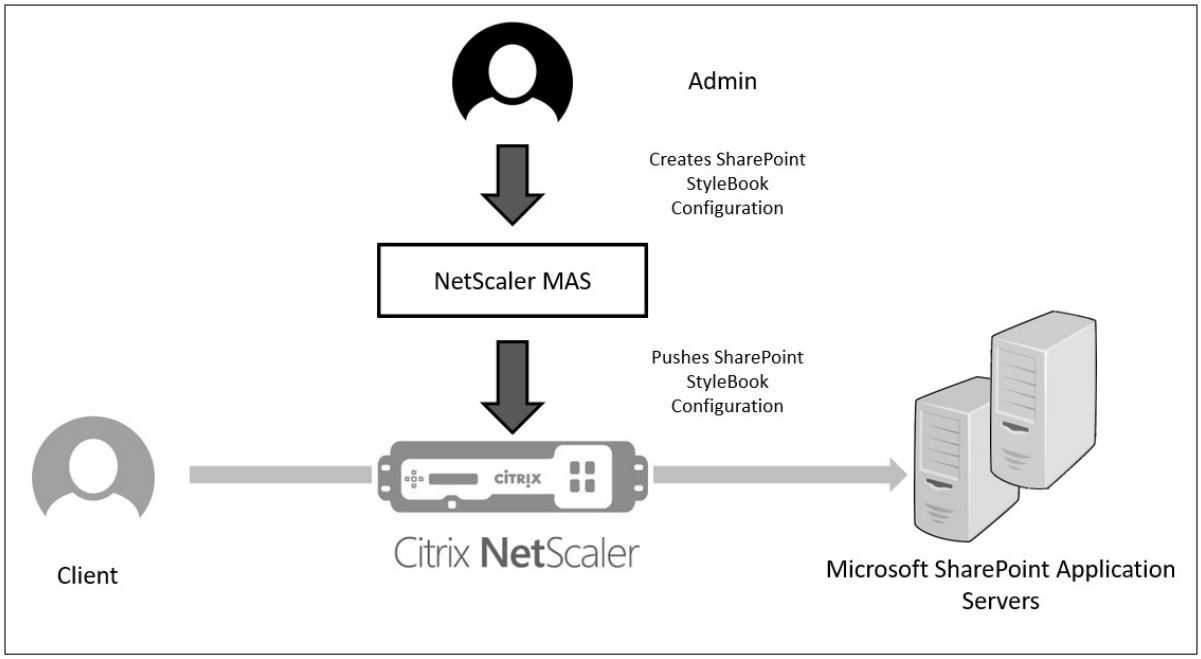
Client-Browsers, die Daten zu dekomprimieren, hängt davon ab, welchen Algorithmus oder welche Algorithmen er unterstützt: GZIP, DEFLATE oder beides.

Eine NetScaler ADC-Instanz ist so konfiguriert, dass der Text in HTML-, XML-, Nur-Text-, Cascading Stylesheet (CSS) und Microsoft Office-Dokumenten komprimiert wird, aber keine Bilder im GIF- oder JPG-Format komprimiert werden. Zu den Hauptvorteilen des komprimierten Datenverkehrs gehören geringere Bandbreitenkosten, eine Reduzierung der WAN-Latenz und eine bessere Serverleistung.

Integriertes Caching

Der NetScaler ADC In-Memory-Cache kann SharePoint-Objekte speichern, um Benutzern häufig angeforderte Inhalte schnell bereitzustellen. Zu den zwischengespeicherten Inhalten gehören heruntergeladene Dokumente sowie Audio-, Video- und Bilddateien.

In der folgenden Abbildung wird die Bereitstellung von SharePoint-Servern in einem Netzwerk dargestellt, das von einer NetScaler ADC-Instanz auf der NetScaler ADM zum Bereitstellen einer SharePoint StyleBook-Konfiguration verwendet wird.



Bereitstellen von SharePoint StyleBook-Konfigurationen

Die folgende Aufgabe unterstützt Sie bei der Bereitstellung des Microsoft SharePoint 2016 StyleBook in Ihrem Unternehmensnetzwerk.

So stellen Sie Microsoft SharePoint 2016 StyleBookbereit:

1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Administration** > **Konfiguration**, und klicken Sie auf **Neu erstellen**.

   Auf der Seite **StyleBook auswählen** werden alle StyleBooks angezeigt, die für Ihre Verwendung in NetScaler ADM verfügbar sind.

2. Blättern Sie nach unten und wählen Sie **Microsoft SharePoint 2016 StyleBook**.

   > **Hinweis:**
   >
   > Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Konfigurationen** > **StyleBooks**. Scrollen Sie nach unten, um das **Microsoft SharePoint 2016 StyleBook**zu finden, und klicken Sie auf **Konfiguration erstellen**.

   Das StyleBook öffnet sich als Benutzeroberflächenformular, auf dem Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

   Geben Sie Werte für die folgenden Parameter ein:

   a) **Name der SharePoint-Anwendung**. Name der SharePoint-Konfiguration, die in Ihrem Netzwerk bereitgestellt werden soll.

   b) **Virtuelle SharePoint-IP**. Virtuelle IP-Adresse, unter der die NetScaler ADC-Instanz Clientanforderungen für die Microsoft SharePoint-Anwendung empfängt.

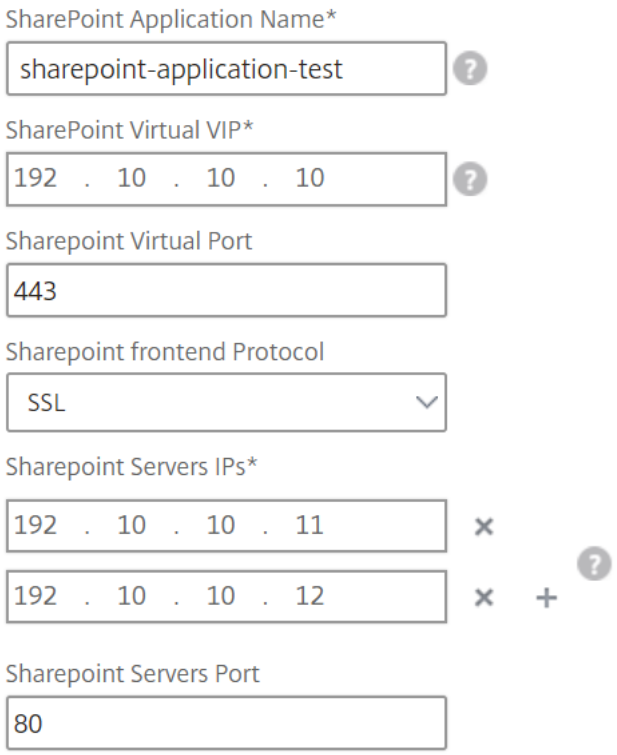
   c) **Virtueller SharePoint-Anschluss**. Der TCP-Port, der von den Benutzern beim Zugriff auf die SharePoint-Anwendung verwendet werden soll

   d) **SharePoint-Frontend-Protokoll**. Wählen Sie das SharePoint-Frontend-Protokoll aus der Dropdownliste aus. Die verfügbaren Optionen sind HTTP oder SSL.

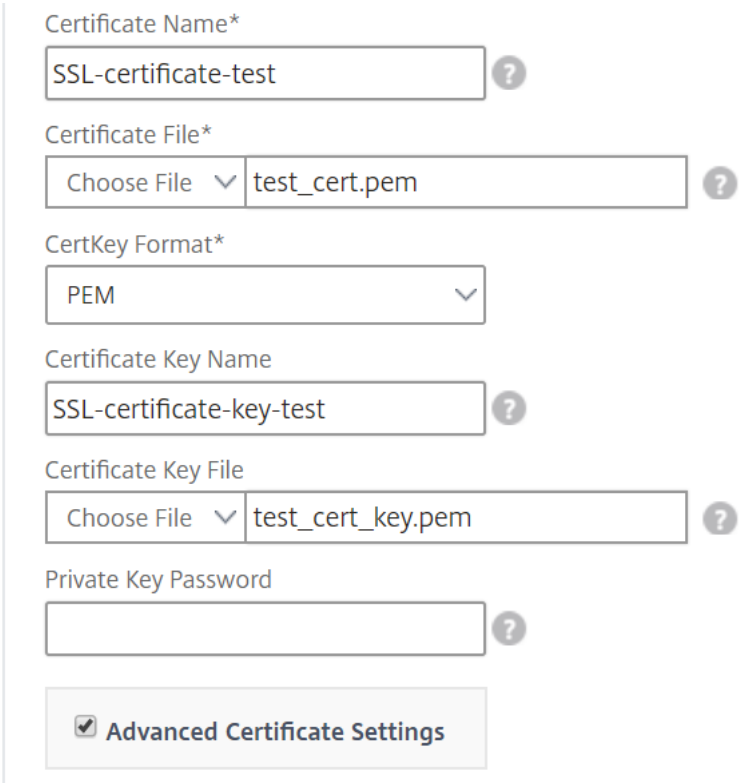
      > **Hinweis**
      >
      > Wenn Sie SSL auswählen, stellen Sie sicher, dass der Rewrite-Configuration-Parameter im Abschnitt Erweiterte SharePoint-Einstellungen in diesem StyleBook aktiviert ist.

   e) **SharePoint Server-IPs**. IP-Adressen aller SharePoint-Server im Netzwerk.

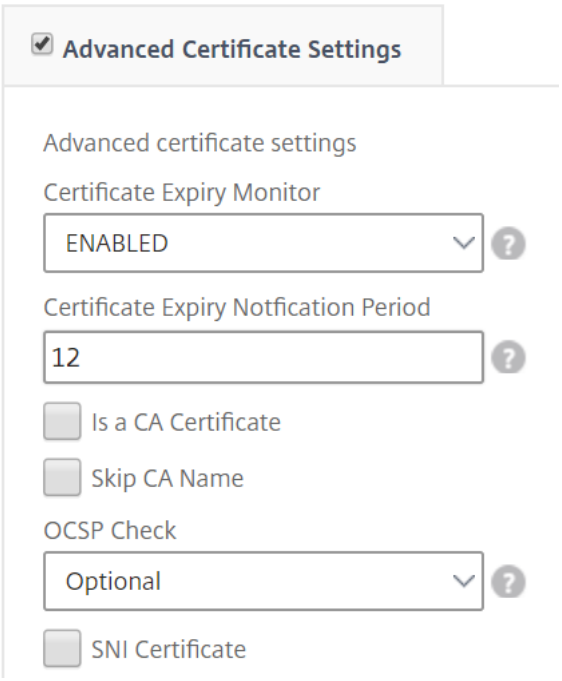
   f) **Anschluss für SharePoint-Server** Von den SharePoint-Servern verwendete TCP-Portnummer In der Standardeinstellung ist dies 80. Sie können diesen Wert bei Bedarf bearbeiten, stellen Sie jedoch sicher, dass auf diesen Port auf Microsoft SharePoint 2016-Servern zugegriffen werden kann.



3. Klicken Sie im Abschnitt **Einstellungen für SSL-Zertifikate** auf +, um den Namen des SSL-Zertifikats und den Zertifikatschlüssel einzugeben und die entsprechenden Dateien aus Ihrem lokalen Speicherordner auszuwählen.

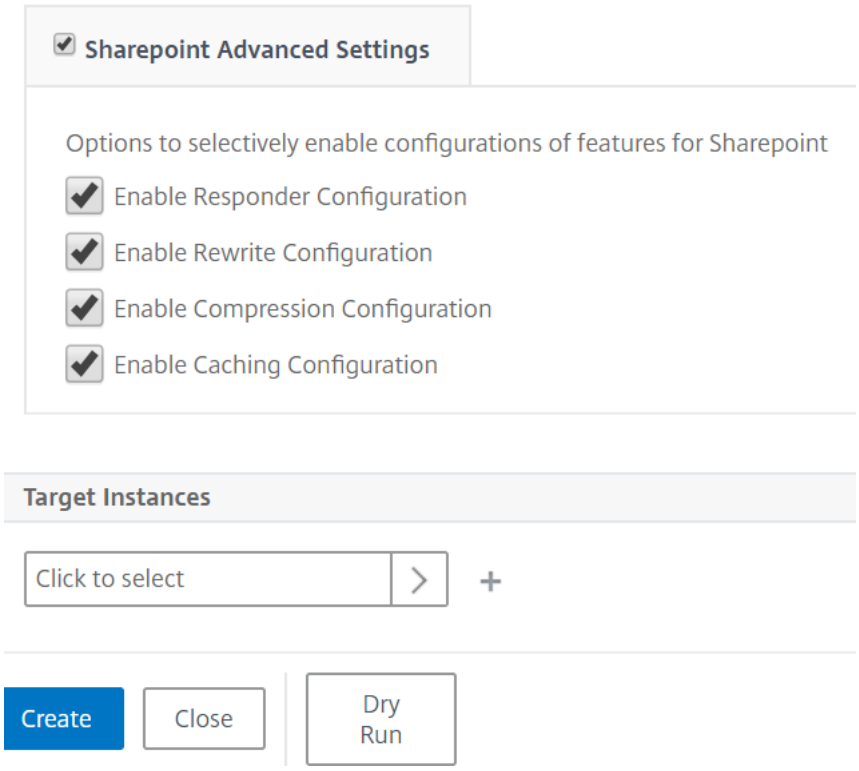


4. Klicken Sie optional auf **Erweiterte Zertifikateinstellungen**, um die Ablaufüberwachung von SSL-Zertifikaten zu aktivieren oder zu deaktivieren. Wenn Sie die Überwachung des Zertifikatablaufs aktivieren, legen Sie die Anzahl der Tage fest, damit NetScaler ADM nach diesen vielen Tagen, wenn das Zertifikat abläuft, einen Alarm ausgibt. Sie haben auch die Möglichkeit, die OCSP-Prüfung als optionales Feature oder als obligatorisches Feature durchzuführen.



5. Im Abschnitt **Erweiterte SharePoint-Einstellungen** können Sie die NetScaler ADC Features aktivieren, die auf den NetScaler ADC-Instanzen konfiguriert werden. Während die Load Balancing- und Content Switching-Funktionen standardmäßig auf den Instanzen konfiguriert sind, können Sie die anderen Funktionen auswählen, d. h. die Responderkonfiguration, die Rewrite-Konfiguration, die Komprimierungskonfiguration und die integrierte Caching-Konfiguration, die Sie für die Instanz konfigurieren möchten.
6. Klicken Sie auf **Zielinstanzen**, und wählen Sie die NetScaler ADC-Instanz aus, auf der diese SharePoint-Konfiguration bereitgestellt werden soll. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und die Konfiguration auf der ausgewählten NetScaler ADC-Instanz bereitzustellen.

> **Hinweis**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.



> **Hinweis**
>
> Citrix empfiehlt, dass Sie vor der Ausführung der eigentlichen Konfiguration „ **Dry Run** “auswählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt werden.

Wenn die Konfiguration erstellt und erfolgreich bereitgestellt wird, erstellt das SharePoint-StyleBook einen virtuellen Content Switching-Server und 12 virtuelle Lastenausgleichsserver. Es erstellt auch Richtlinien und Dienstgruppen und bindet sie an die virtuellen Lastausgleichsserver. Welche Richtlinien erstellt werden, hängt von den Funktionen ab, die während der Erstellung des Konfigurationspakets im StyleBook ausgewählt wurden.

Anzeigen der in der NetScaler ADC-Instanz definierten Objekte

Nachdem das Konfigurationspaket auf NetScaler ADM erstellt wurde, können Sie alle Objekte anzeigen, die in der NetScaler ADC-Instanz für das SharePoint StyleBook erstellt wurden. Navigieren Sie zu **Anwendungen** > **Administration** > **Konfiguration**, und klicken Sie auf **Erstellte Objekte anzeigen**. Die folgende Abbildung zeigt einige der erstellten Objekte mit den IP-Adressen, die im Beispiel unter ‘‘Deploying SharePoint StyleBook Configurations from NetScaler ADM’’angegeben sind.

Type : lbvserver

appflowlog : DISABLED
backuppersistencetimeout : 20
downstateflush : DISABLED
ipv46 : 0.0.0.0
lbmethod : LEASTCONNECTION
name : sharepoint application test frontpage services lb
persistencebackup : SOURCEIP
persistencetype : COOKIEINSERT
port : 0
servicetype : HTTP
timeout : 20

Type : servicegroup

cip : DISABLED
cka : YES
cmp : NO
downstateflush : DISABLED
healthmonitor : NO
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp
servicetype : HTTP
sp : ON
state : ENABLED
tcpb : NO
useproxyport : NO
usip : NO

Type : lbvserver_servicegroup_binding

name : sharepoint-application-test-frontpage-services-lb
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.11
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.12
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : csaction

name : sharepoint-application-test-cs-frontpage-services-csaction
targetlbvserver : sharepoint-application-test-frontpage-services-lb

Type : cspolicy

action : sharepoint-application-test-cs-frontpage-services-csaction
policyname : sharepoint-application-test-cs-frontpage-services-cspol
rule : HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS

Type : csvserver_cspolicy_binding

name : sharepoint-application-test-cs
policyname : sharepoint-application-test-cs-frontpage-services-cspol
priority : 10

Microsoft ADFS-Proxy-StyleBook

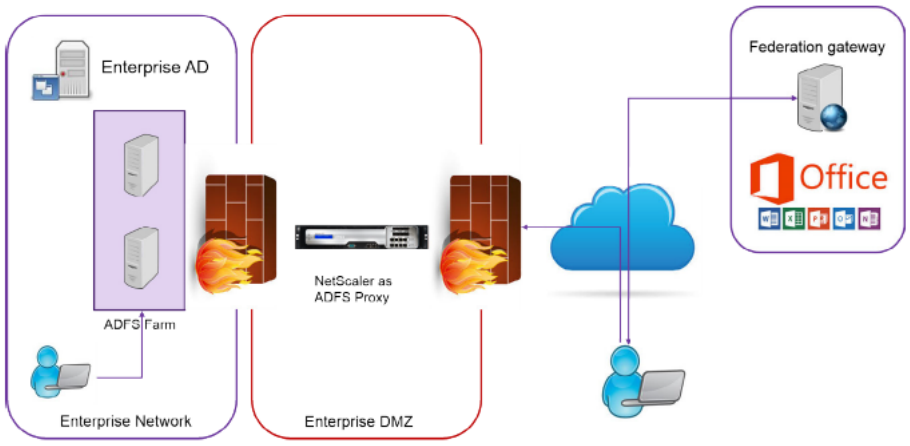
February 5, 2024

Der Microsoft™ ADFS-Proxy spielt eine wichtige Rolle, da er Single Sign-On-Zugriff sowohl für interne verbundfähige Ressourcen als auch für Cloud-Ressourcen gewährt. Ein solches Beispiel für Cloud-Ressourcen ist Office 365. Der Zweck des ADFS-Proxyservers besteht darin, Anfragen zu empfangen und an ADFS-Server weiterzuleiten, auf die nicht über das Internet zugegriffen werden kann. Der ADFS-Proxy ist ein Reverse-Proxy und befindet sich in der Regel im Perimeter-Netzwerk (DMZ) Ihres Unternehmens. Der ADFS-Proxy spielt eine entscheidende Rolle bei der Remote-Benutzerkonnektivität und dem Anwendungszugriff.

NetScaler ADC verfügt über die genaue Technologie, um sichere Konnektivität, Authentifizierung und Verarbeitung der föderierten Identität zu ermöglichen. Durch die Verwendung von NetScaler ADC als ADFS-Proxy entfällt die Notwendigkeit, eine zusätzliche Komponente in der DMZ bereitzustellen.

Mit dem Microsoft ADFS Proxy StyleBook in NetScaler Application Delivery Management (ADM) können Sie einen ADFS-Proxyserver auf einer NetScaler ADC-Instanz konfigurieren.

Das folgende Bild zeigt die Bereitstellung einer Citrix ADC Instanz als ADFS-Proxyserver in der Enterprise DMZ.



Vorteile der Verwendung von NetScaler ADC als ADFS-Proxy

1. Erfüllt sowohl Load Balancing als auch ADFS-Proxy-Anforderungen
2. Unterstützt sowohl interne als auch externe Benutzerzugriffsszenarien
3. Unterstützt umfangreiche Methoden für die Vorauthentifizierung
4. Bietet ein einmaliges Anmelden für Benutzer
5. Unterstützt sowohl aktive als auch passive Protokolle

   a) Beispiele für aktive Protokoll-Apps sind —Microsoft Outlook, Microsoft Skype for Business
   b) Beispiele für passive Protokoll-Apps sind: Microsoft Outlook-Webanwendung, Webbrowser

6. Gehärtetes Gerät für DMZ-basierte Bereitstellung
7. Mehrwert durch die Verwendung zusätzlicher Citrix ADC Kernfunktionen

   a) Content Switching
   b) SSL-Offload
   c) Rewrite
   d) Sicherheit (NetScaler ADC AAA)

Für aktive protokollbasierte Szenarien können Sie eine Verbindung zu Office 365 herstellen und Ihre Anmeldeinformationen angeben. Microsoft Federation Gateway kontaktiert den ADFS-Dienst (über ADFS-Proxy) im Namen des aktiven Protokollclients. Das Gateway übermittelt dann die Anmeldeinformationen unter Verwendung der Standardauthentifizierung (401). NetScaler ADC verarbeitet die Clientauthentifizierung vor dem Zugriff auf den ADFS-Dienst. Nach der Authentifizierung stellt der ADFS-Dienst dem Federation Gateway ein SAML-Token zur Verfügung. Das Federation Gateway wiederum sendet das Token an Office 365, um den Clientzugriff zu ermöglichen.

Für passive Clients erstellt das ADFS Proxy StyleBook ein Kerberos Constrained Delegation (KCD) -Benutzerkonto. Das KCD-Konto ist für die Kerberos-SSO-Authentifizierung erforderlich, um eine Verbindung zu den ADFS-Servern herzustellen. Das StyleBook generiert auch eine LDAP-Richtlinie und eine Sitzungsrichtlinie. Diese Richtlinien werden später an den virtuellen NetScaler ADC AAA-Server gebunden, der die Authentifizierung für passive Clients abwickelt.

Das StyleBook kann auch sicherstellen, dass die DNS-Server auf dem NetScaler ADC für ADFS konfiguriert sind.

Im folgenden Konfigurationsabschnitt wird beschrieben, wie Sie NetScaler ADC für die Verarbeitung der aktiven und passiven protokollbasierten Clientauthentifizierung einrichten.

Konfigurationsdetails

In der folgenden Tabelle sind die mindestens erforderlichen Softwareversionen aufgeführt, damit diese Integration erfolgreich bereitgestellt werden kann.

Product	Erforderliche Mindestversion
Citrix ADC	11.0, Advanced/Premium-Lizenz

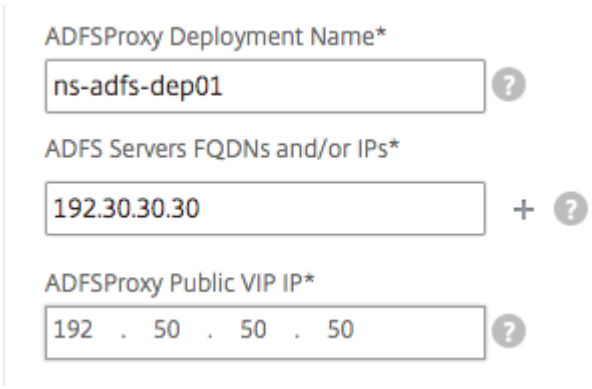
In den folgenden Anweisungen wird davon ausgegangen, dass Sie bereits die entsprechenden externen und internen DNS-Einträge erstellt haben.

Bereitstellen von Microsoft ADFS-Proxy-StyleBook-Konfigurationen von NetScaler ADM

Die folgenden Anweisungen helfen Ihnen bei der Implementierung des Microsoft ADFS-Proxys StyleBook in Ihrem Unternehmensnetzwerk.

So stellen Sie Microsoft ADFS Proxy StyleBook bereit

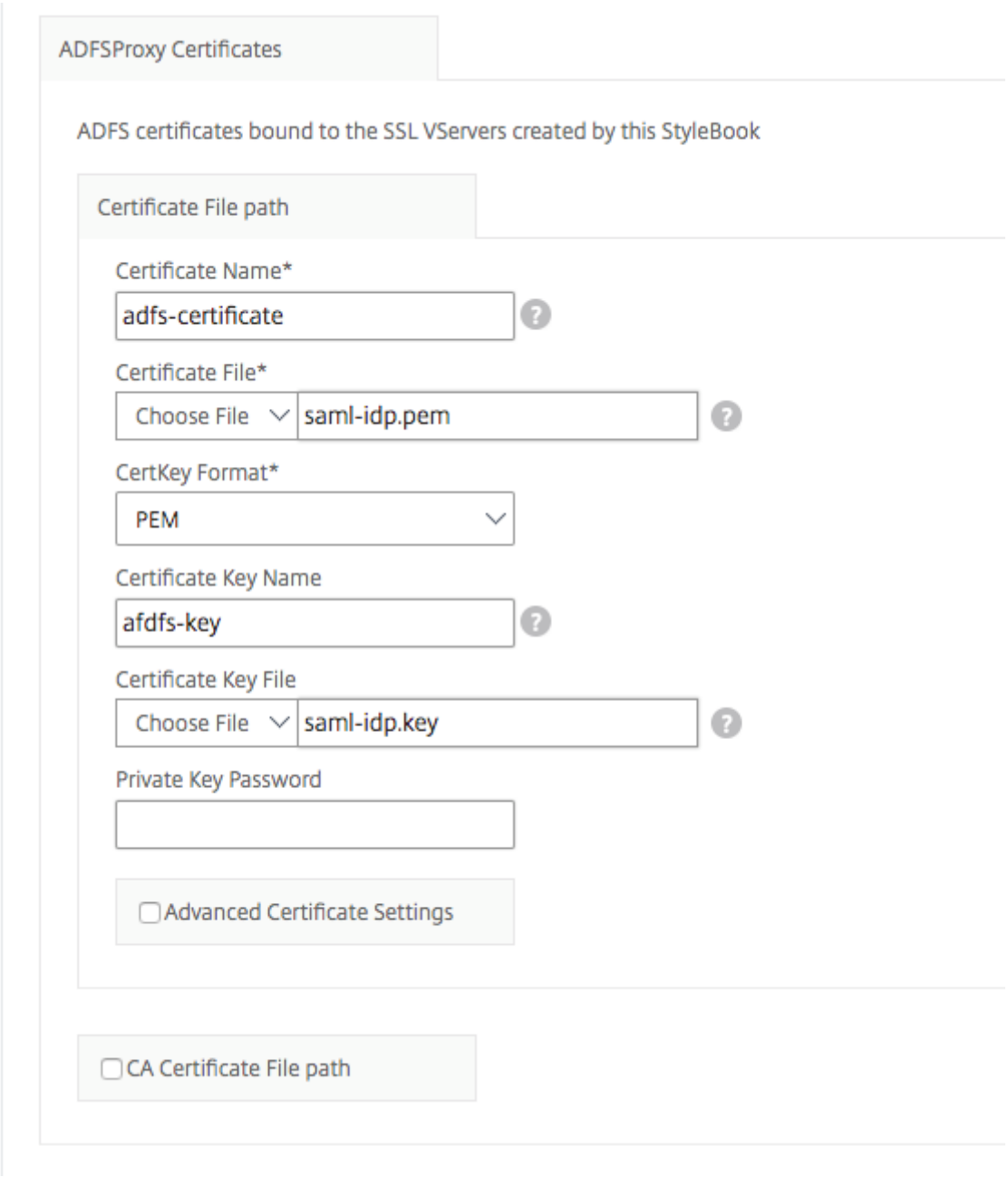
1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **StyleBooks**. Auf der Seite **StyleBooks** werden alle StyleBooks angezeigt, die für Ihre Verwendung in NetScaler ADM verfügbar sind.
2. Scrollen Sie nach unten und suchen Sie das **Microsoft ADFS proxy StyleBook**. Klicken Sie auf **Konfiguration erstellen**.
   Das StyleBook wird als Benutzeroberflächenseite geöffnet, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
3. Geben Sie Werte für die folgenden Parameter ein:
   a) **Name der ADFS-Proxybereitstellung** Wählen Sie einen Namen für die in Ihrem Netzwerk bereitgestellte ADFS-Proxykonfiguration aus.
   b) **ADFS-Server-FQDNs oder IPs**. Geben Sie die IP-Adressen oder FQDNs (Domänennamen) aller ADFS-Server im Netzwerk ein.
   c) **Öffentliche VIP-IP des ADFS-Proxy**. Geben Sie die öffentliche virtuelle IP-Adresse auf dem NetScaler ADC ein, der als ADFS-Proxyserver ausgeführt wird.



4. Geben Sie im Abschnitt **ADFS-Proxyzertifikate** die Details des SSL-Zertifikats und des Zertifikatsschlüssels ein.

   Dieses SSL-Zertifikat ist an alle virtuellen Server gebunden, die auf der NetScaler ADC-Instanz erstellt wurden.

   Wählen Sie die entsprechenden Dateien aus Ihrem lokalen Speicherordner aus. Sie können auch das Kennwort für den privaten Schlüssel eingeben, um verschlüsselte private Schlüssel im PEM-Format zu laden.



Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Benachrichtigungszeitraum für den Ablauf des Zertifikats eingeben, die Überwachung des Zertifikatsablaufes aktivieren oder deaktivieren.

5. Optional können Sie das Kontrollkästchen **SSL-CA-Zertifikat** aktivieren, wenn für das SSL-Zertifikat ein öffentliches CA-Zertifikat auf NetScaler ADC installiert sein muss. Stellen Sie sicher, dass Sie im Abschnitt **Erweiterte**Zertifikatseinstellungen die Option Ist ein CA-Zertifikat** auswählen.
6. Aktivieren Sie die Authentifizierung für aktive und passive Clients. Geben Sie den in Active Di-

rectory für die Benutzerauthentifizierung verwendeten DNS-Domänennamen ein. Sie können dann die Authentifizierung entweder für aktive oder passive Clients oder für beide konfigurieren.

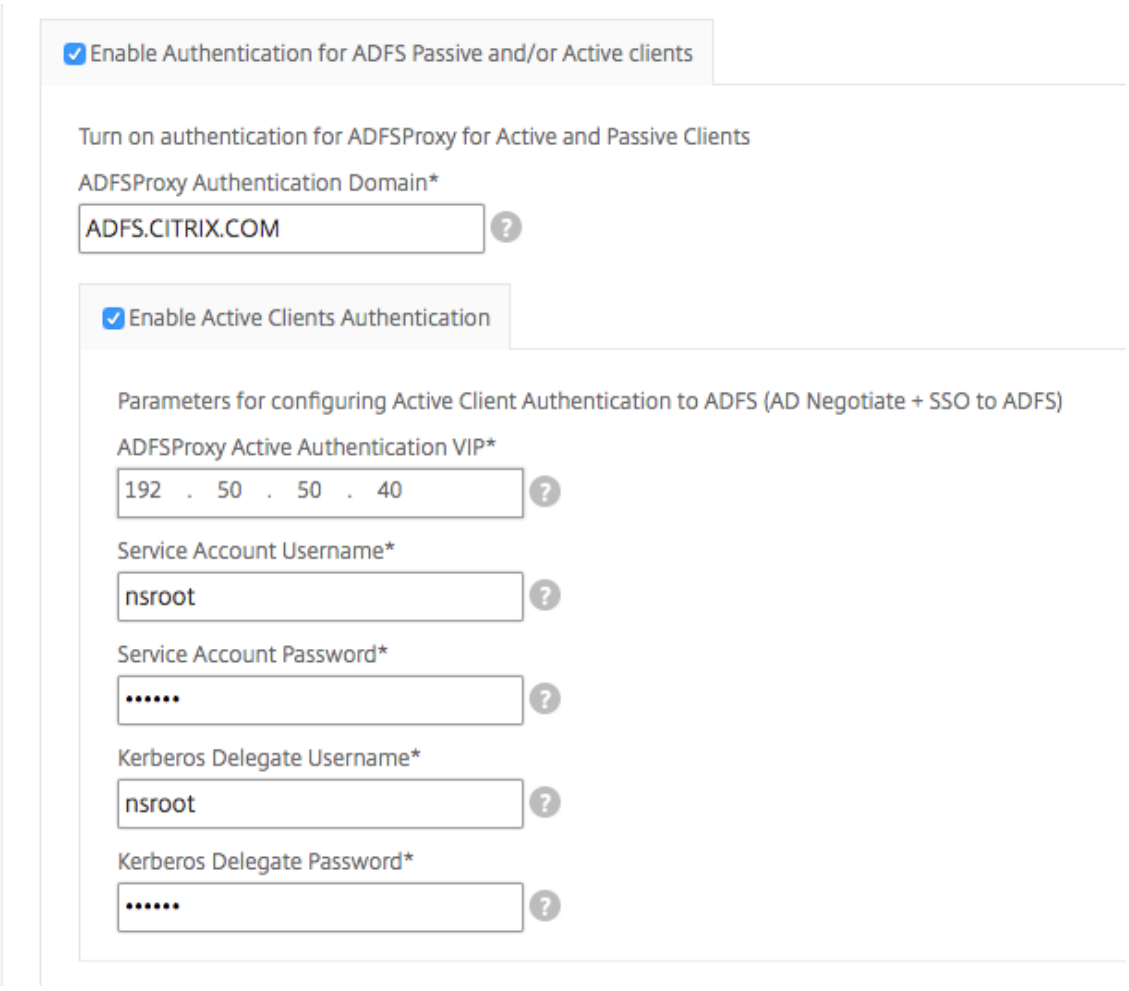
7. Geben Sie die folgenden Details ein, um die Authentifizierung für aktive Clients zu aktivieren:

> **Hinweis**
>
> Es ist optional, die Unterstützung für aktive Clients zu konfigurieren.

a) **Aktive Authentifizierung des ADFS-Proxys** Geben Sie die virtuelle IP-Adresse des virtuellen Authentifizierungsservers auf der NetScaler ADC-Instanz ein, in der die aktiven Clients zur Authentifizierung umgeleitet werden.

b) **Benutzername des Dienstkontos** Geben Sie den Benutzernamen des Dienstkontos ein, der von NetScaler ADC zur Authentifizierung Ihrer Benutzer beim Active Directory verwendet wird.

c) **Kennwort für das Dienstkonto**. Geben Sie das Kennwort ein, das von NetScaler ADC verwendet wird, um Ihre Benutzer beim Active Directory zu authentifizieren.



8. Konfigurieren Sie die Authentifizierung für passive Clients, indem Sie die entsprechende Option aktivieren und die LDAP-Einstellungen konfigurieren.

   > **Hinweis**
   >
   > Es ist optional, die Unterstützung für passive Clients zu konfigurieren.

   Geben Sie die folgenden Details ein, um die Authentifizierung für passive Clients zu aktivieren:

   a) **LDAP-Basis (Active Directory)**. Geben Sie den Basisdomänennamen für die Domäne ein, in der sich die Benutzerkonten im Active Directory (AD) befinden, um die Authentifizierung zu ermöglichen. Zum Beispiel dc=netscaler, dc=com

   b) **LDAP (Active Directory) Bindet DN**. Fügen Sie ein Domänenkonto hinzu (unter Verwendung einer E-Mail-Adresse zur Vereinfachung der Konfiguration), das über Berechtigungen zum Durchsuchen der AD-Struktur verfügt. Zum Beispiel cn=Manager, dc=netscaler, dc=com

   c) **LDAP (Active Directory) Bindet DN Kennwort**. Geben Sie das Kennwort des Domänenkontos für die Authentifizierung ein.

      Einige andere Felder, die Sie in die Werte in diesem Abschnitt eingeben müssen, lauten wie folgt:

   d) **LDAP-Server-IP (Active Directory)**. Geben Sie die IP-Adresse des Active Directory-Servers ein, damit die AD-Authentifizierung ordnungsgemäß funktioniert.

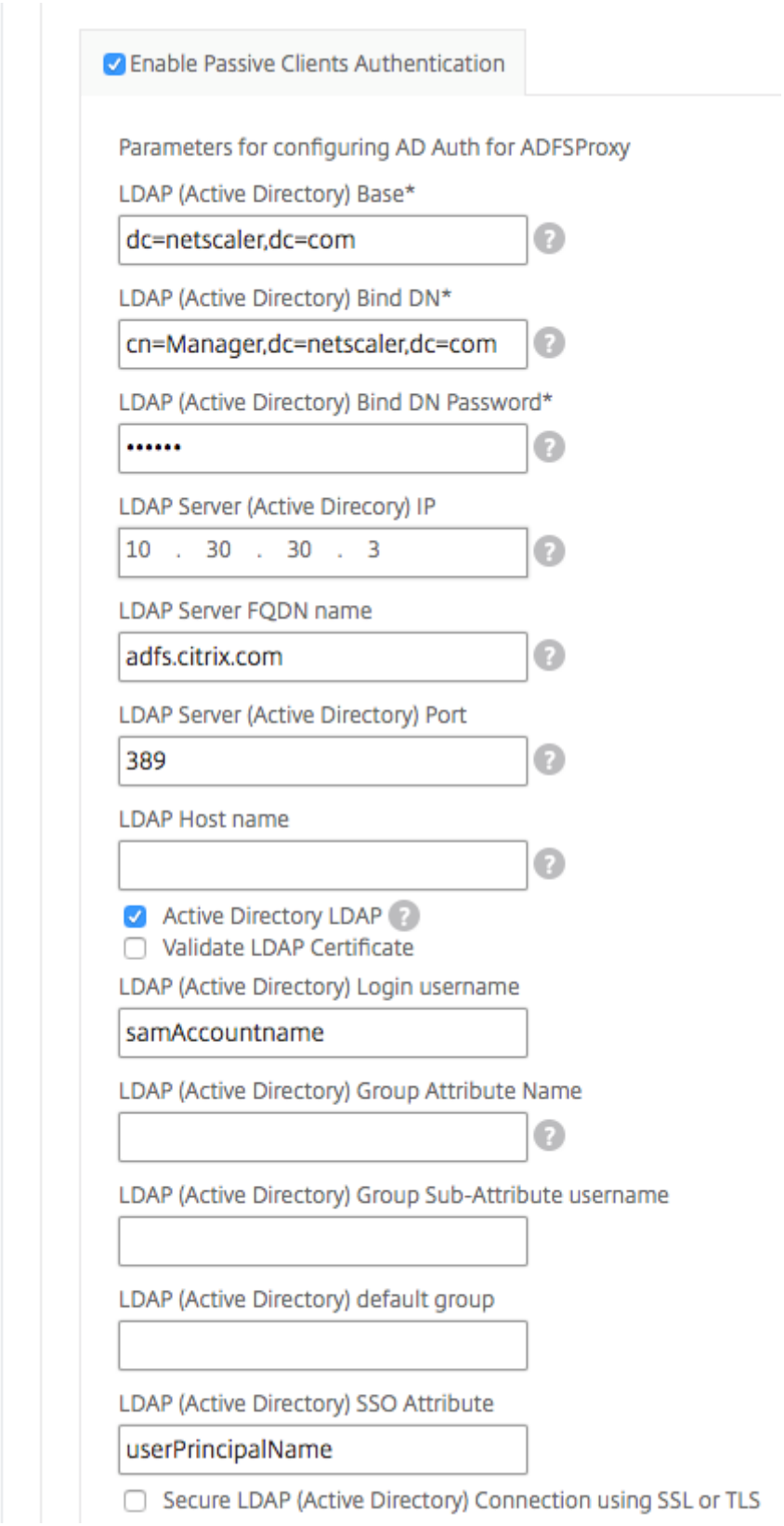
   e) **FQDN**-**Name** des LDAP-Servers . Geben Sie den FQDN-Namen des Active Directory-Servers ein. Der FQDN-Name ist optional. Geben Sie die IP-Adresse wie in Schritt 1 oder den FQDN-Namen an.

   f) **Active Directory-Port für LDAP-Server**. Standardmäßig sind die TCP- und UDP-Ports für das LDAP-Protokoll 389, wohingegen der TCP-Port für Secure LDAP 636 ist.

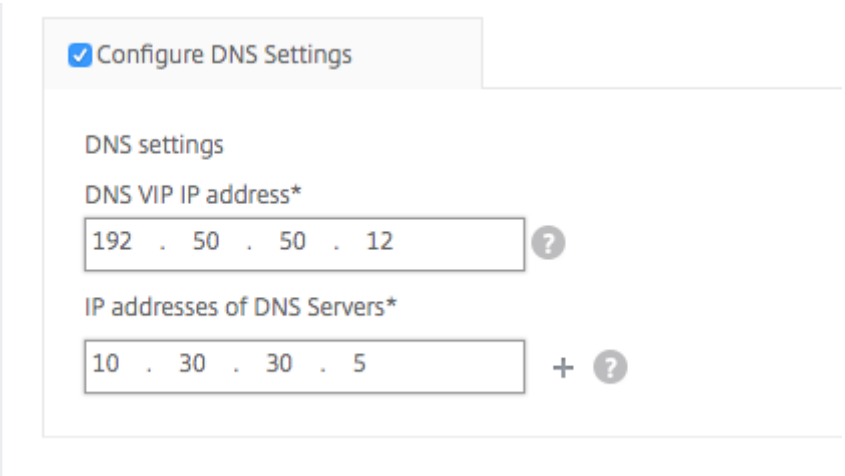
   g) **LDAP-Anmeldebenutzername (Active Directory)**. Geben Sie den Benutzernamen als samAccountname ein.

   h) **ADFS Proxy Passive Authentifizierung VIP**. Geben Sie die IP-Adresse des virtuellen ADFS-Proxyservers für passive Clients ein.

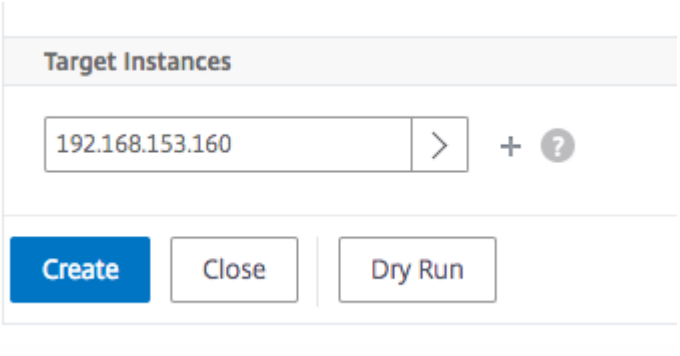
      > **Hinweis:**
      >
      > Die mit * gekennzeichneten Felder sind Pflichtfelder.



9. Optional können Sie auch eine DNS-VIP für Ihre DNS-Server konfigurieren.



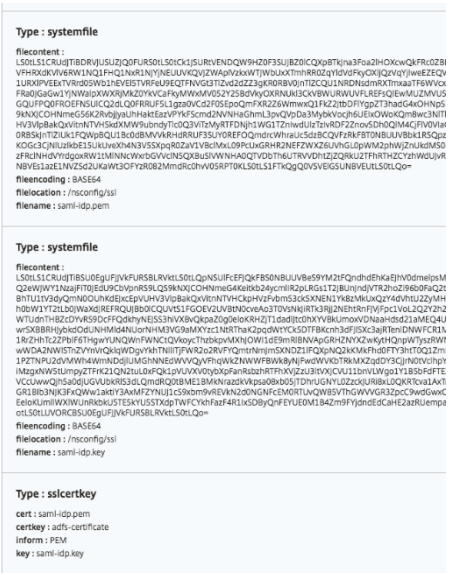
10. Klicken Sie auf **Zielinstanzen**, und wählen Sie die NetScaler ADC-Instanzen aus, um diese Microsoft ADFS-Proxykonfiguration bereitzustellen. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und die Konfiguration auf den ausgewählten NetScaler ADC-Instanzen bereitzustellen.



> **Hinweis**
>
> Citrix empfiehlt, dass Sie vor der Ausführung der eigentlichen Konfiguration die Option **Testlauf auswählen.** Sie können zunächst die Konfigurationsobjekte anzeigen, die vom StyleBook auf den NetScaler ADC Zielinstanzen erstellt werden. Sie können dann auf **Erstellen** klicken, um die Konfiguration auf den ausgewählten Instanzen bereitzustellen.

Erstellte Objekte

Mehrere Konfigurationsobjekte werden erstellt, wenn die ADFS-Proxykonfiguration auf der NetScaler ADC-Instanz bereitgestellt wird. In der folgenden Abbildung wird die Liste der erstellten Objekte angezeigt.



Objects Added on Instance : 192.168.153.160 | Count : 57

Type : nsfeature

Meta Properties
action : **enable**

feature : cs lb ssl rewrite aaa

Type : lbvserver

ipv46 : 192.50.50.12
name : ns-adfs-dep01-adfs-dns
port : 53
servicetype : DNS

Type : service

ip : 10.30.30.5
name : ns-adfs-dep01-dns-svc-1
port : 53
servicetype : DNS

Type : lbvserver_service_binding

name : ns-adfs-dep01-adfs-dns
servicename : ns-adfs-dep01-dns-svc-1

Type : authenticationnegotiateaction

domain : ADFS.CITRIX.COM
domainuser : nsroot
domainuserpasswd : nsroot
name : ns-adfs-dep01-negotiate-action

Type : authenticationpolicy

action : ns-adfs-dep01-negotiate-action
name : ns-adfs-dep01-negotiate-policy
rule : true

Type : aaakcdaccount

delegateduser : nsroot
kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
kcdpassword : nsroot
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
name : ns-adfs-dep01-adfs-auth401-tmsession-action
persistentcookie : ON
persistentcookievalidity : 3
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-auth401-tmsession-action
name : ns-adfs-dep01-adfs-auth401-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.40
maxloginattempts : 255
name : ns-adfs-dep01-adfs-auth401-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-auth401-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-negotiate-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-adfs-auth401-tmsession-policy
priority : 10

Type : authenticationldapaction

authentication : ENABLED
authtimeout : 30
followreferrals : OFF
ldapbase : dc=netscaler,dc=com
ldapbinddn : cn=Manager,dc=netscaler,dc=com
ldapbinddnpassword : nsroot
ldaploginname : samAccountname
name : ns-adfs-dep01-ldap-action
passwdchange : DISABLED
sectype : PLAINTEXT
serverip : 10.30.30.3
serverport : 389
ssonameattribute : userPrincipalName
svrtype : AD
validateservercert : NO

Type : authenticationpolicy

action : ns-adfs-dep01-ldap-action
name : ns-adfs-dep01-ldap-policy
rule : true

Type : aaakcdaccount

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
name : ns-adfs-dep01-adfs-ldap-tmsession-action
persistentcookie : OFF
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-ldap-tmsession-action
name : ns-adfs-dep01-adfs-ldap-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.30
maxloginattempts : 255
name : ns-adfs-dep01-adfs-ldap-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-ldap-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-ldap-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-adfs-ldap-tmsession-policy
priority : 10

Type : csvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-cs
port : 443
servicetype : SSL

Type : lbvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
port : 445
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : server

ipaddress : 192.30.30.30
name : 192.30.30.30

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
priority : 9800

Type : lbvserver

appflowlog : ENABLED
authentication : ON
authenticationhost : ADFS.CITRIX.COM
authn401 : OFF
authnvsname : ns-adfs-dep01-adfs-ldap-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
port : 446
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
priority : 9900

Type : lbvserver

appflowlog : ENABLED
authentication : OFF
authn401 : ON
authnvsname : ns-adfs-dep01-adfs-auth401-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
port : 444
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
rule : true

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
priority : 10000

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-cs

Type : rewritepolicylabel

labelname : ns-adfs-dep01-request-rewritepolicylabel
transform : HTTP_REQ

Type : rewritepolicylabel

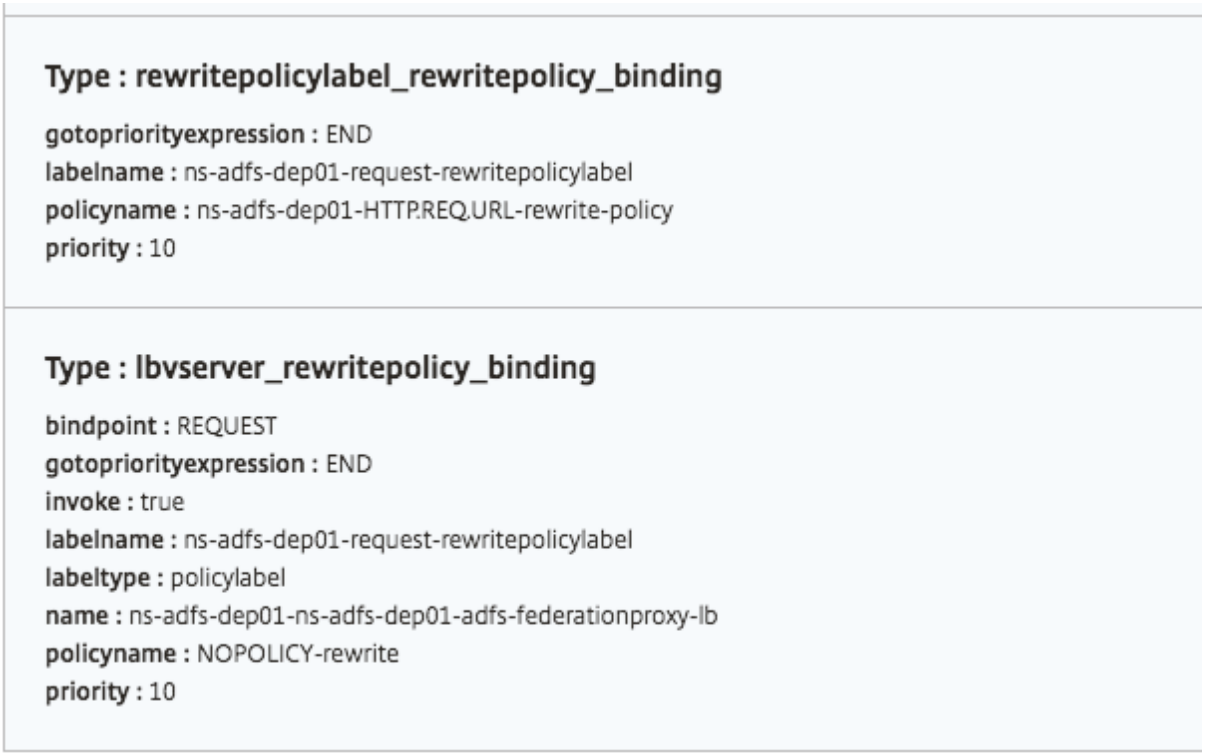
labelname : ns-adfs-dep01-response-rewritepolicylabel
transform : HTTP_RES

Type : rewriteaction

name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
stringbuilderexpr : "/adfs/services/trust/proxymex"
target : HTTP.REQ.URL
type : REPLACE

Type : rewritepolicy

action : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") && (!HTTP.REQ.URL.CONTAINS("/trust/proxymex"))



Oracle e-business StyleBook

February 5, 2024

Oracle E-Business Suite ist die umfassendste Suite integrierter, globaler Geschäftsanwendungen. Diese Suite ermöglicht es Unternehmen, bessere Entscheidungen zu treffen, Kosten zu senken und die Leistung zu steigern. Sie besteht aus den folgenden Anwendungen.

- Ressourcenplanung für Unternehmen (ERP)
- Kundenbeziehungsmanagement (CRM)
- Lieferkettenmanagement (SCM)

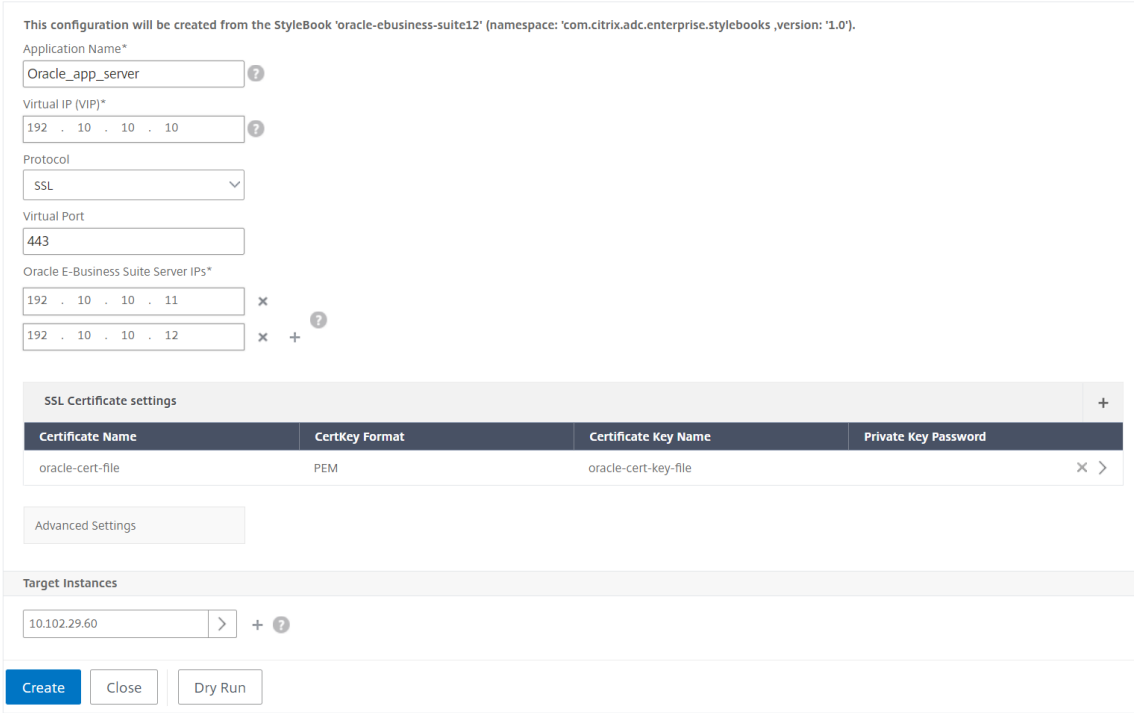
Diese Computeranwendungen werden entweder von Oracle entwickelt oder erworben. Mit dem Oracle E-Business Suite 12.2 StyleBook können Sie die Konfiguration auf den ausgewählten NetScaler ADC-Instanzen bereitstellen.

Dieses StyleBook erstellt eine Lastausgleichskonfiguration, die einen virtuellen Lastausgleichsserver, eine Dienstgruppe und eine Liste von Diensten umfasst. Es bindet die Dienste auch an die Dienstgruppe und bindet die Dienstgruppe an den virtuellen Server. Sie können die verschlüsselte Kommunikation auswählen, indem Sie SSL auswählen und die SSL-Dateien und Schlüsseldateien Ihres lokalen Systems bereitstellen.

So erstellen Sie eine Konfiguration für Oracle E-Business Suite 12.2

1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zu **Anwendungen** > **Konfiguration > StyleBooks**. Auf der Seite **StyleBooks** werden alle StyleBooks angezeigt, die in Ihrem NetScaler ADM verfügbar sind. Scrollen Sie nach unten und wählen Sie **Oracle E-Business Suite 12.2**. Sie können auch die Suchoption verwenden, um das StyleBook zu durchsuchen.
2. Klicken Sie im StyleBook-Bedienfeld auf **Konfiguration erstellen** .
3. Geben Sie den Namen der Load Balancer-Anwendung und die virtuelle IP-Adresse im Abschnitt Load Balancer-Einstellungen ein.
4. Wählen Sie das erforderliche Protokoll aus. Sie haben hier zwei Möglichkeiten - HTTP und HTTP-S/SSL. Sie können die Portnummer auch eingeben.
5. Geben Sie die IP-Adressen aller Oracle E-Business Suite-Anwendungsserver im Netzwerk ein, für die ein Lastenausgleich erfolgen soll. Klicken Sie auf **+**, um weitere Server-IP-Adressen hinzuzufügen.
6. Wählen Sie im Abschnitt **SSL-Zertifikatseinstellungen** die entsprechenden Dateien aus Ihrem lokalen Speicher aus. Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie weitere Details wie den Benachrichtigungszeitraum für den Ablauf des Zertifikats konfigurieren. Sie können auch die Ablaufüberwachung für Zertifikate aktivieren oder deaktivieren.

   Wählen Sie die NetScaler ADC Zielinstanz aus, für die die Konfiguration erstellt werden muss, und klicken Sie auf **Erstellen**.



> **Tipp**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen. Das Aktualisierungssymbol ist derzeit nur auf NetScaler ADM verfügbar.

Citrix StoreFront StyleBooks

February 5, 2024

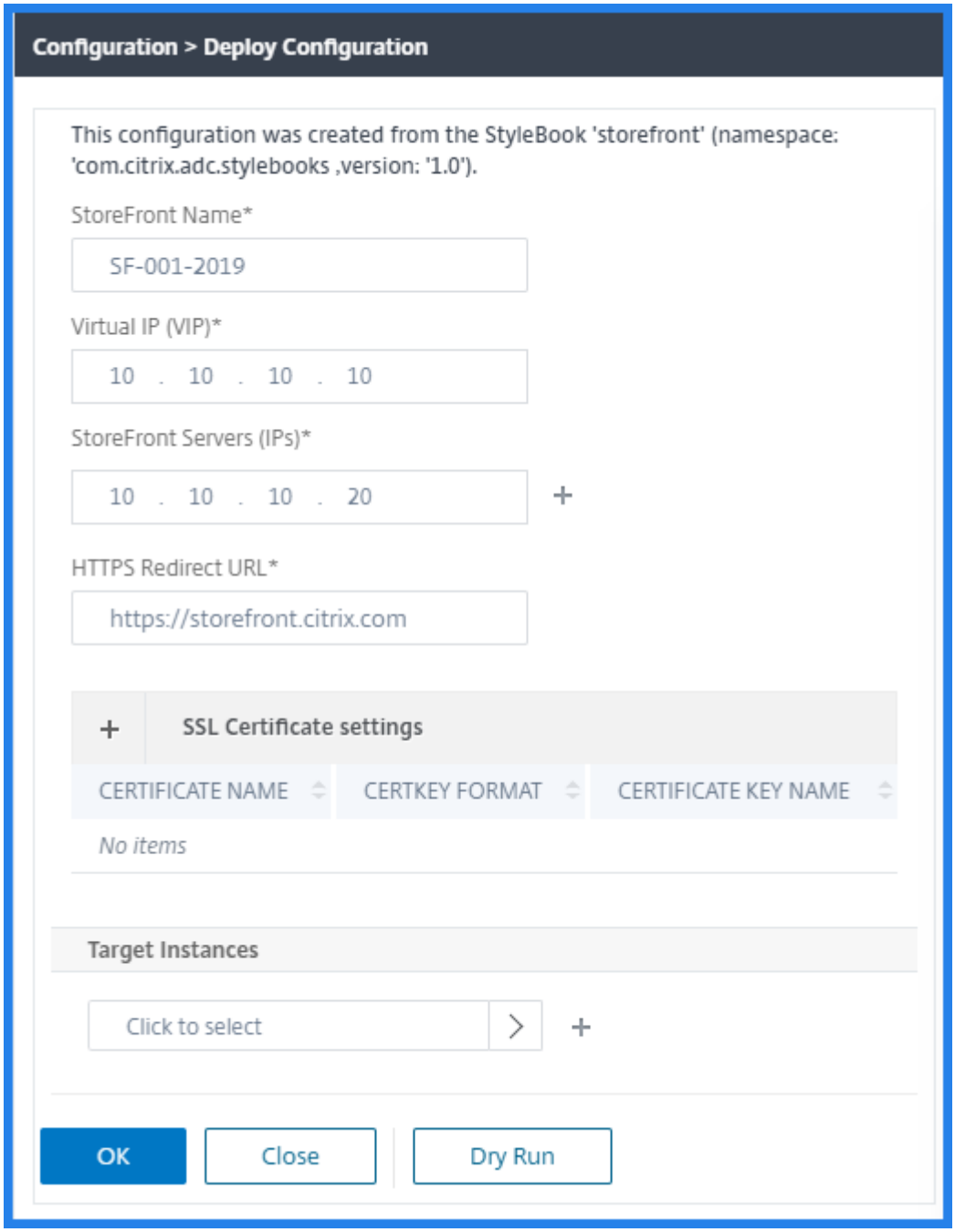
StoreFront ist ein Unternehmens-App-Store, der Anwendungen und Desktops von Citrix Virtual Apps and Desktops-Websites in einem einzigen Store für Benutzer zusammenfasst. StoreFront authentifiziert Benutzer bei Websites, auf denen Ressourcen gehostet werden, und verwaltet Anwendungsspeicher und Desktops, auf die Benutzer zugreifen. Es hostet Ihren Unternehmensanwendungsspeicher, sodass Sie Benutzern Self-Service-Zugriff auf Apps und Desktops gewähren können, die Sie ihnen zur Verfügung stellen.

Dieses StyleBook definiert die NetScaler ADC Konfigurationen für StoreFront -Server. Mit diesem StyleBook können Sie StoreFront-Server für die gewünschten NetScaler ADC-Instanzen konfigurieren. Sie können die verschlüsselte Kommunikation auswählen, indem Sie SSL auswählen und die SSL-Dateien und Schlüsseldateien Ihres lokalen Systems bereitstellen.

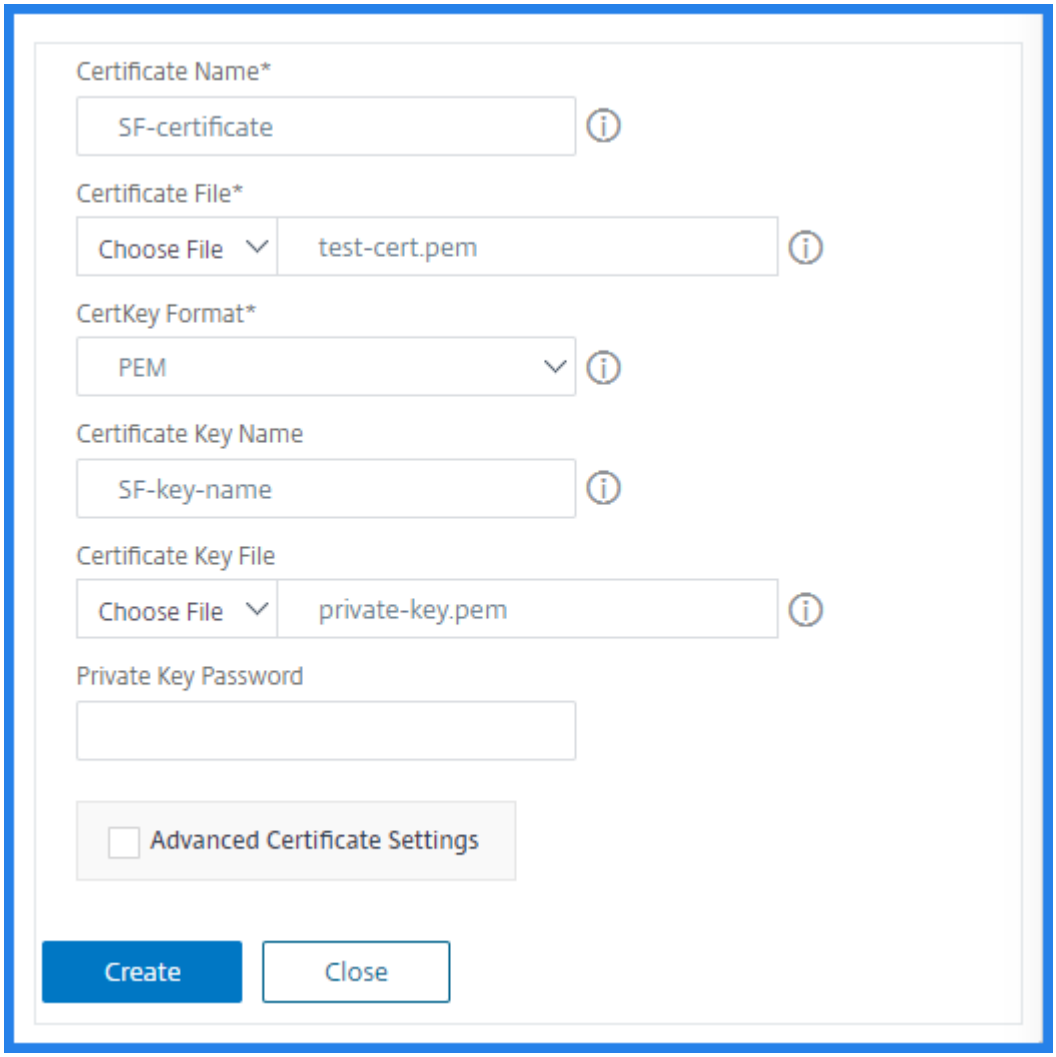
Konfiguration für Citrix StoreFront-Anwendungen erstellen

1. Navigieren Sie in der Citrix ADM GUI zu **Anwendungen > StyleBooks**.
2. Verwenden Sie in der Suchleiste die **Namenseigenschaften** und suchen Sie `Citrix StoreFront`.
3. Klicken Sie im Citrix StoreFront StyleBook auf Konfiguration erstellen.
4. Geben Sie die folgenden Details an:

    - **StoreFront-Name**: Geben Sie den StoreFront-Namen an. Das StoreFront ConfigPack wird mit demselben StoreFront-Namen erstellt.
    - **Virtuelle IP (VIP)**: Geben Sie die virtuelle IP-Adresse an, an der die Citrix ADC Instanz die Clientanforderungen empfängt.
    - **StoreFront -Server**: Geben Sie die IP-Adressen der StoreFront -Server an, die Sie mit einer Citrix ADC Instanz konfigurieren möchten.
    - **HTTPS-Umleitungs-URL**: Geben Sie die HTTPS-URL an, an die die HTTPS-Anfragen umgeleitet werden.



5. Geben Sie im Abschnitt **SSL-Zertifikatseinstellungen** die Namen des SSL-Zertifikats und den Zertifikatsschlüssel ein.
6. Wählen Sie die entsprechenden Dateien aus Ihrem lokalen Speicherordner aus. Sie können auch das Kennwort für den privaten Schlüssel eingeben, um die verschlüsselten privaten Schlüssel im PEM-Format anzugeben.



7. Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Zeitraum für die Benachrichtigung über den Ablauf des Zertifikats eingeben und die Überwachung des Zertifikatsablaufs aktivieren oder deaktivieren.
8. Optional können Sie das Kontrollkästchen **SSL-Zertifizierungsstellenzertifikat für das virtuelle Authentifizierungs-IP** aktivieren, wenn für das SSL-Zertifikat ein öffentliches Zertifizierungsstellenzertifikat auf Citrix ADC installiert werden muss. Stellen Sie sicher, dass Sie im Abschnitt **Erweiterte**Zertifikatseinstellungen die Option Ist ein CA-Zertifikat** auswählen.
9. Klicken Sie auf **Erstellen**.
10. Klicken Sie auf **Zielinstanzen**, und wählen Sie die Citrix ADC Instanzen aus, auf denen Sie die StoreFront -Server konfigurieren möchten.
11. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und die Konfiguration auf den ausgewählten NetScaler ADC-Instanzen bereitzustellen.

Benutzerdefinierten StyleBooks erstellen und verwenden

February 5, 2024

Sie können ein eigenes StyleBook für Ihre Bereitstellung schreiben, es in Citrix Application Delivery Management (ADM) importieren und Konfigurationsobjekte erstellen. Sie können die API auch verwenden, um Konfigurationen aus Ihren StyleBooks zu erstellen.

Dieses Dokument enthält die folgenden Informationen:

Voraussetzungen

Bevor Sie mit der Erstellung von StyleBooks beginnen, stellen Sie sicher, dass Sie über folgende Kenntnisse verfügen:

- NITRO API. Weitere Informationen finden Sie in der Nitro API-Dokumentation
- YAML

StyleBook-Dateien verwenden das YAML-Format. Hinweise zum YAML-Format finden Sie unter YAML-Syntax.

Im Folgenden finden Sie eine Liste der YAML-Richtlinien, die Sie beim Erstellen von StyleBooks beachten müssen:

- YAML unterscheidet zwischen Groß- und Klein
- YAML erfordert eine korrekte Einrückung
- Verwenden Sie die Taste <spacebar>, um eine korrekte Einrückung zu erstellen Verwenden Sie nicht die Taste <tab>. Die Verwendung der Taste <tab> führt zu einem Kompilierungsfehler beim Importieren Ihres StyleBook in MA
- Verwenden Sie keine Zeichenfolgen in Anführungszeichen. Schließen Sie die Zeichenfolge nur dann in Anführungszeichen ein, wenn eine Zeichenfolge Satzzeichen (Bindestriche, Doppelpunkte usw.) enthält. Wenn Sie eine Zahl als String interpretieren möchten, fügen Sie die Zahl entweder in Anführungszeichen ein oder verwenden Sie die integrierte Funktion str () von StyleBooks.
- Literale wie YES/Yes/yes/Y/y/NO/no/No/n/N, ON/On/on/OFF/Off/off und TRUE/true/truthy/-FALSE/False/false/falsely werden als boolesch betrachtet und sind äquivalent zu true und false. Um sie als Zeichenfolgen zu interpretieren, setzen Sie sie in Anführungszeichen. Zum Beispiel:
  - “JA”
  - “Nein”
  - “Stimmt”

- "Falsch"und so weiter.

> **Hinweis**
>
> Bevor Sie Ihre StyleBook-Datei in NetScaler ADM importieren, sollten Sie überprüfen, ob Ihre Datei mit dem YAML-Format kompatibel ist. Citrix empfiehlt, den integrierten YAML-Validator in StyleBooks zu verwenden, um den YAML-Inhalt zu validieren und zu importieren.
>
> Während der Konfiguration von StyleBooks können Sie nur Nitro-Konfigurationsressourcen verwenden, die die Vorgänge zum **Erstellen** und **Löschen (POST- und DELETE-HTTP-Methoden**) unterstützen. Weitere Informationen finden Sie in der Dokumentation zu Nitro-APIs.

Anatomie eines StyleBook

Das Schreiben von StyleBooks setzt voraus, dass Sie die Grammatik, Syntax und Struktur von StyleBooks verstehen. Ein typisches StyleBook hat die folgenden Abschnitte:

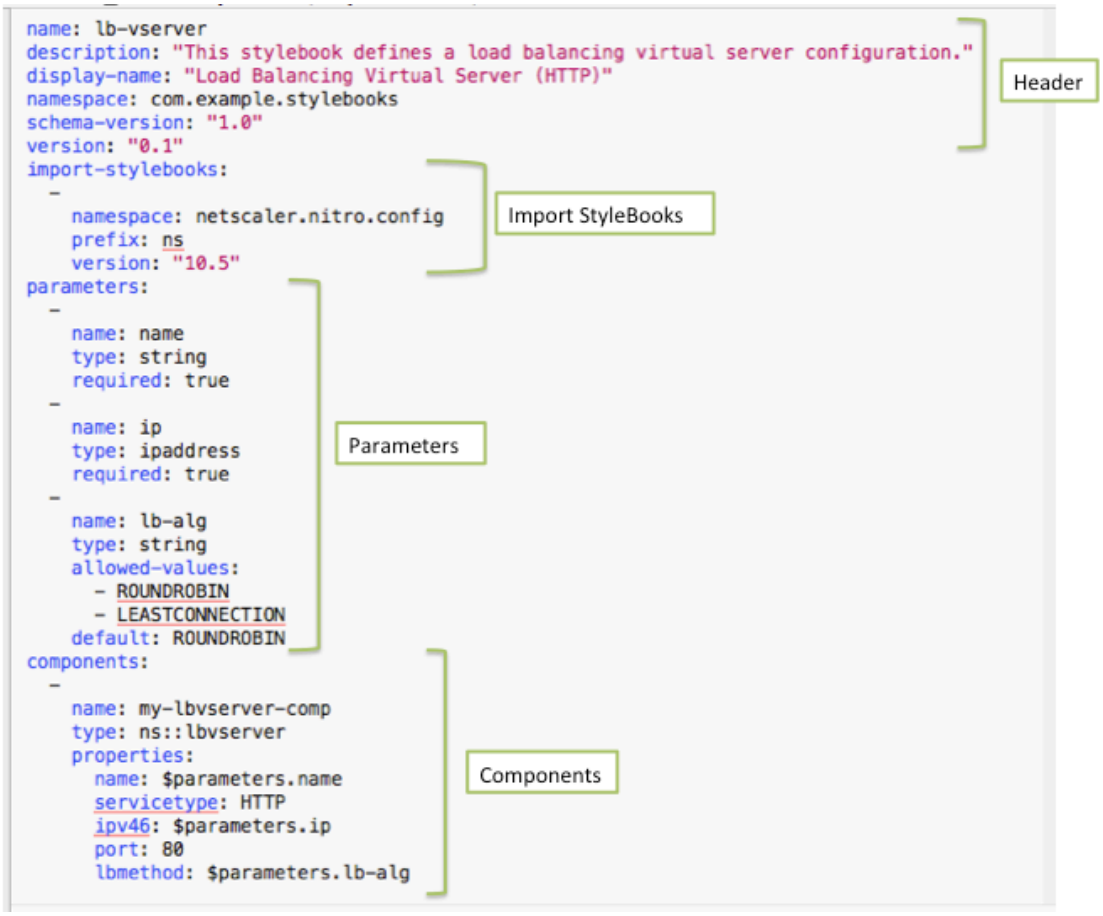
- **Kopfzeile**: In diesem Abschnitt können Sie die Identität eines StyleBooks definieren und beschreiben, was es tut. Dies ist ein obligatorischer Abschnitt.
- **StyleBooks importieren**: In diesem Abschnitt können Sie festlegen, auf welches andere StyleBook Sie aus Ihrem aktuellen StyleBook verweisen möchten. Das Importieren der NetScaler ADC NITRO-Konfiguration StyleBooks oder anderer StyleBooks ist erforderlich, um ein StyleBook zu schreiben. Dies ist ein obligatorischer Abschnitt.
- **Parameter**: In diesem Abschnitt können Sie die Parameter definieren, die Sie in Ihrem StyleBook benötigen, um eine Konfiguration zu erstellen. Es beschreibt die Eingabe, die Ihr StyleBook nimmt. Dies ist ein optionaler Abschnitt.
- **Komponenten**: In diesem Abschnitt können Sie die Entitäten (Konfigurationsobjekte) definieren, die vom StyleBook für eine bestimmte Konfiguration erstellt werden. Dieser Abschnitt wird als Kern eines StyleBook betrachtet. Komponenten verwenden in der Regel die im Parameterbereich bereitgestellten Eingaben, um die vom StyleBook generierte Konfiguration anzupassen. Dies ist ein optionaler Abschnitt.

  Ein StyleBook kann einen Parameterabschnitt oder einen Komponentenbereich oder beides haben. Ein StyleBook, das nur den Parameterbereich enthält, ist nützlich, um eine Liste von Parametern zu definieren, die von anderen StyleBooks verwendet werden können. Dies fördert die Wiederverwendbarkeit von Parametergruppen über eine Reihe von StyleBooks hinweg. Ein StyleBook mit nur einem Komponentenabschnitt kann verwendet werden, wenn Sie die Werte für Attribute im StyleBook angeben möchten, anstatt Parameter für Benutzereingaben zu definieren.
- **Ausgaben**: Während der Parameterbereich die Eingänge des StyleBook definiert, definiert dieser optionale Abschnitt seine Ausgaben. In diesem optionalen Ausgabeabschnitt können

Sie die Komponenten angeben, die Sie Benutzern, die eine Konfiguration aus diesem StyleBook erstellen, und anderen StyleBooks, die dieses StyleBook importieren, zur Verfügung stellen möchten. Benutzer und importierende StyleBooks können dann auf die Eigenschaften der bereitgestellten Komponenten verweisen.

- **Operationen**: Ein StyleBook kann einen optionalen Abschnitt enthalten, um Analytics in NetScaler ADM auf jedem virtuellen Server zu aktivieren, der Teil des StyleBook ist.

Die folgende Abbildung zeigt einen einfachen Überblick über ein StyleBook.



Die folgenden Beispiele helfen Ihnen, die Grammatik und Struktur eines StyleBook zu kennenlernen und StyleBooks mit zunehmender Komplexität zu schreiben.

- StyleBook zum Erstellen eines virtuellen Lastausgleichsservers
- StyleBook, um eine grundlegende Lastausgleichskonfiguration zu erstellen
- Zusammengesetztes StyleBook erstellen
- Passen Sie Ihr StyleBook mithilfe von GUI-Attributen an

StyleBook zum Erstellen eines virtuellen Lastausgleichsservers

February 5, 2024

In diesem Beispiel entwerfen Sie ein einfaches StyleBook, das einen virtuellen Lastausgleichsserver vom Typ HTTP-Protokoll erstellt und auf Port 80 überwacht. Die Parameter für den virtuellen Servernamen, die IP-Adresse und die Load-Balancing-Methode akzeptieren benutzerdefinierte Werte, d. h. sie sind die Parameter des StyleBook.

Header

Die ersten sechs Zeilen eines StyleBook bilden den Header-Bereich. In diesem Beispiel ist der Header-Abschnitt wie folgt geschrieben:

```
1 name: lb-vserver
2 description: This StyleBook defines a load balancing virtual server
     configuration.
3 display-name: Load Balancing Virtual Server (HTTP)
4 namespace: com.example.stylebooks
5 schema-version: "1.0"
6 version: "0.1"
7 <!--NeedCopy-->
```

Der Header-Abschnitt enthält die folgenden Details:

- **name**: Ein Name für dieses StyleBook.
- **description**: Eine Beschreibung, die definiert, was dieses StyleBook tut. Diese Beschreibung wird auf NetScaler ADM angezeigt.
- **displayname**: Ein beschreibender Name für das StyleBook, das auf NetScaler ADM angezeigt wird.
- **Namespace**: Ein Namespace ist Teil einer eindeutigen Kennung für ein StyleBook, um Namenskollisionen zu vermeiden.
- **schema-version**: Nimmt in dieser Version immer den Wert „1.0“an.
- **version**: Die Versionsnummer des StyleBook. Sie können die Versionsnummer ändern, wenn Sie das StyleBook aktualisieren.

Die Kombination aus **Name**, **Namespace** und **Version** identifiziert ein StyleBook im System eindeutig. Sie können nicht zwei StyleBooks mit derselben Kombination aus Name, Namespace und Version in NetScaler ADM haben. Sie können jedoch zwei StyleBooks mit demselben Namen und derselben Version, aber unterschiedlichen Namespaces oder mit demselben Namespace und derselben Version, aber unterschiedlichen Namen haben.

> **Hinweis**
>
> Bedenken Sie, dass Sie Ihr StyleBook aktualisiert haben und eine aktualisierte Versionsnummer haben. Wenn Sie nun in anderen StyleBooks auf dieses StyleBook verweisen (das heißt, wenn Sie es importieren), stellen Sie sicher, dass Sie die Versionsnummer auch in anderen StyleBooks aktualisieren, damit diese die richtige Version des importierten StyleBooks verwenden.

StyleBooks importieren

Der Abschnitt hinter dem Header heißt „Import-Stylebooks“. In diesem Abschnitt müssen Sie den Namespace und die Versionsnummer jedes anderen StyleBooks deklarieren, auf das Sie in Ihrem aktuellen StyleBook verweisen möchten. Auf diese Weise können Sie andere StyleBooks importieren und wiederverwenden, anstatt dieselbe Konfiguration in Ihrem eigenen StyleBook neu zu erstellen.

In diesem Beispiel ist der Abschnitt import-stylebooks wie folgt geschrieben:

```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
<!--NeedCopy-->
```

Jedes StyleBook muss auf den Namespace netscaler.nitro.config verweisen, wenn es eines der NITRO-Konfigurationsobjekte direkt verwendet. Dieser Namespace enthält alle NetScaler ADC NITRO-Typen, z. B. LBVServer.Da Softwareversionen 10.5 und höher unterstützt werden, können Sie Ihr StyleBook verwenden, um Konfigurationen auf jeder NetScaler ADC-Instanz zu erstellen und auszuführen, auf der Version 10.5 und höher ausgeführt wird.

Das im Abschnitt import-stylebooks verwendete Präfix ist eine Abkürzung für die Kombination von Namespace und Version. In diesem Fall bezieht sich ns auf netscaler.nitro.config der Version 10.5. In den späteren Abschnitten Ihres StyleBooks können Sie, anstatt den Namespace und die Version zu verwenden, um auf das importierte StyleBook zu verweisen, die im obigen Beispiel ausgewählt wurde, z. B. ns, verwenden.

Die in den StyleBooks verwendete Version ist die NetScaler ADC NITRO Version. Ein StyleBook, das auf Nitro Version X basiert, kann verwendet werden, um Citrix ADC mit Version X oder höher zu konfigurieren.

> **Hinweis**
>
> Um sicherzustellen, dass Ihre StyleBooks verwendet werden können, um jede Citrix ADC Instanz der Version 10.5 oder höher zu konfigurieren, empfiehlt Citrix, den Nitro 10.5-Namespace aus Gründen der maximalen Kompatibilität in Ihre StyleBooks zu importieren, die direkt Nitro inte-

> grierte StyleBooks verwenden (Namespace: netscaler.nitro.config, Version: 10.5).

Es ist wichtig, dass ein StyleBook, das andere StyleBooks importiert, auf einer Nitro-Version basieren muss, die dieselbe oder eine höhere Version als die importierten StyleBooks hat. Beispielsweise kann ein StyleBook, das auf Nitro Version 10.5 basiert, nicht von einem StyleBook abhängig sein oder ein StyleBook verwenden oder importieren, das auf 11.1 basiert. Ein StyleBook basierend auf Version 11.1 kann jedoch ein StyleBook importieren, das auf einer beliebigen Version von weniger als 11.1 basiert.

Es ist auch möglich, dass ein StyleBook, das den Nitro-Namespace überhaupt nicht importiert. Das bedeutet, dass ein StyleBook Nitro-Komponenten nicht direkt definieren muss, sondern StyleBooks importieren kann (abhängig von), die Nitro-Komponenten definieren. Das StyleBook, das andere StyleBooks importiert, erhält immer die höchste Nitro-Version in der Hierarchie seiner Abhängigkeiten und kann daher zur Konfiguration von Citrix ADCs verwendet werden, die dieser Version oder höher sind.

Parameter

Im Parameterbereich können Sie alle Parameter deklarieren, die Sie in Ihrem StyleBook benötigen. Sie als StyleBook-Entwickler müssen entscheiden, welche Eingaben die Benutzer Ihres StyleBooks angeben sollen. In diesem Beispiel haben Sie Ihr StyleBook so aufgebaut, dass die Benutzer den Namen des virtuellen Servers, seine IP-Adresse und die Lastausgleichsmethode angeben müssen.

Der Abschnitt “Parameter”würde wie folgt aussehen:

```
1  parameters:
2   -
3    name: name
4    type: string
5    label: Application Name
6    description: Name of the application configuration.
7    required: true
8
9   -
10   name: ip
11   type: ipaddress
12   label: Application Virtual IP (VIP)
13   description: Application VIP that the clients access.
14   required: true
15
16 -
17   name: lb-alg
18   type: string
19   label: LoadBalancing Algorithm
20   description: Choose the load balancing algorithm (method) used for
        load balancing client request between the application servers.
21   allowed-values:
```



```
    - ROUNDROBIN
    - LEASTCONNECTION
    default: ROUNDROBIN
<!--NeedCopy-->
```

> **Hinweis**
>
> Wenn Sie die Bezeichnung eines Parameters nicht angeben, verwendet NetScaler ADM bei der Anzeige dieses Parameters das name-Attribut. Sie müssen immer eine Bezeichnung für Ihre Parameter definieren, damit Sie steuern können, wie sie in NetScaler ADM angezeigt werden.
>
> Bei Verwendung der APIs wird der Parameter jedoch durch seinen Namen gekennzeichnet.

In diesem Abschnitt haben Sie drei Parameter deklariert, die durch ihre **Namensattributwerte** gekennzeichnet sind: **Name** für den virtuellen Servernamen, **IP** für die IP-Adresse des virtuellen Servers und **lb-alg** für die Lastausgleichsmethode.

- **Typ**. Art des Werts, den diese Parameter annehmen können. Beispielsweise können name und lb-alg einen Zeichenfolgenwert annehmen und der IP-Wert muss vom Typ IP-Adresse sein. Parameter in einem StyleBook können von einem der folgenden integrierten Typen sein:
- **string**. Eine Reihe von Charakteren. Wenn keine Länge angegeben wird, kann der Zeichenfolgenwert beliebig viele Zeichen annehmen. Sie können jedoch die Länge eines String-Typs einschränken, indem Sie die Attribute min-length und max-length verwenden.
- **Nummer**. Eine Ganzzahl. Sie können die minimale und maximale Anzahl angeben, die dieser Typ annehmen kann, indem Sie die Attribute min-value und max-value verwenden.
- **boolesch**. Kann entweder wahr oder falsch sein. Beachten Sie auch, dass alle Literale von YAML als boolesche Werte betrachtet werden (z. B. Ja oder Nein).
- **ipadresse**. Eine Zeichenfolge, die eine gültige IPv4- oder IPv6-Adresse darstellt.
- **TCP-Anschluss**. Eine Zahl zwischen 0 und 65535, die einen TCP- oder UDP-Port darstellt.
- **password**. Ein undurchsichtiger/geheimer Zeichenfolgenwert. Wenn NetScaler ADM einen Wert für diesen Parameter anzeigt, wird er als Sternchen (*****) angezeigt.
- **certfile**. Zertifikatsdatei.
- **Schlüsseldatei**. Private Schlüsseldatei des Zertifikats.
- **-Datei**. Ein Parameter dieses Typs erfordert, dass der Benutzer eine Datei hochlädt, z. B. ein Zertifikat oder eine Schlüsseldatei.
- **Objekt**. Besteht aus mehreren Elementen und jedes dieser Elemente ist ein Parameter. Dieser Typ kann verwendet werden, um mehrere verwandte Parameter unter einem übergeordneten Parameter zu gruppieren.
- **erforderlich**. Gibt an, ob ein Parameter obligatorisch oder optional ist. Wenn er auf true gesetzt ist, ist der Parameter obligatorisch und der Benutzer muss beim Erstellen von Konfigurationen mit diesem StyleBook einen Wert für diesen Parameter angeben. Standardmäßig sind alle Parameter optional. In diesem Beispiel sind **name** und **ip** obligatorische Parameter, während **lb-alg** ein optionaler Parameter ist, dessen Standardwert “ROUNDROBIN”ist.

Verwenden Sie das **Standardattribut**, um einem optionalen Parameter einen Standardwert zuzuweisen. Wenn ein Benutzer beim Erstellen einer Konfiguration keinen Wert angibt, wird der Standardwert verwendet. Für den Parameter **lb-alg** ist der Standardwert beispielsweise ROUNDROBIN.

Verwenden Sie das Attribut **allowed-values**, um bestimmte Werte zu definieren, aus denen ein Benutzer beim Erstellen einer Konfiguration auswählen kann. In diesem Beispiel haben Sie zwei Werte für den Parameter **lb-alg** angegeben - ROUNDROBIN und LEASTCONNECTION.

Wenn Sie Ihr StyleBook importieren und es verwenden, zeigt NetScaler ADM ein Formular mit diesen drei Parametern an. Die für Name und IP angezeigten Felder ermöglichen die Eingabe von Werten vom Typ Zeichenfolge und IP-Adresse. Das Feld lb-alg wird als Dropdownliste angezeigt, wobei ROUNDROBIN als Standardwert ausgewählt ist.

> **Hinweis**
>
> Zusätzlich zu den integrierten Typen kann ein Parameter ein anderes StyleBook als Typ haben. Dies ist eine Möglichkeit, in anderen StyleBooks definierte Parameter wiederzuverwenden.

Komponenten

Der letzte Abschnitt in diesem StyleBook wird als Komponentenbereich bezeichnet und gilt als der wichtigste Abschnitt im StyleBook. In diesem Abschnitt definieren Sie die Konfigurationsobjekte, die vom SyleBook erstellt werden müssen.

Für dieses Beispiel müssen Sie den Komponentenabschnitt wie folgt schreiben:

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Dieses Beispiel enthält nur eine Komponente. Die Hauptattribute einer Komponente sind Name, Typ und Eigenschaften. Der Typ einer Komponente bestimmt, welche Eigenschaften diese Komponente bietet. Komponenten sind von zwei Arten:

- **Eingebauter Typ**. Dieser Typ wird vom System bereitgestellt und Sie müssen ihn nicht definieren, z. B. die NITRO-Entitätstypen „lbvserver“oder „servicegroup“. In diesem Beispiel verwenden Sie einen integrierten Komponententyp.

- **Verbundtyp**. Bei diesem Typ handelt es sich um das StyleBook, das Sie erstellt und in NetScaler ADM importiert haben, oder um das StandardstyleBook, das mit NetScaler ADM ausgeliefert wird. Weitere Informationen zu Composite StyleBooks finden Sie unter Erstellen eines Composite StyleBook.

In diesem Beispiel haben Sie eine Komponente namens **lbvserver-comp**definiert. Diese Komponente ist vom Typ **ns: :lbvserver**(ein integrierter Nitro-Typ), wobei „ns“das Präfix ist, das sich auf den Namespace netscaler.nitro.config und Version 10.5 bezieht, die Sie im Abschnitt Import-Stylebooks angegeben haben, und „lbvserver“eine Nitro-Ressource in diesem Namespace ist.

Die hier definierten **Eigenschaften** sind die Attribute der Ressource lbvserver. Weitere Informationen über alle verfügbaren NetScaler ADC Nitro-Ressourcen und deren Attribute finden Sie in der NetScaler ADC NITRO REST API-Dokumentation.

Die Eigenschaften in diesem Abschnitt enthalten die obligatorischen Attribute der Ressource lbvserver und können Sie Werte für diese Attribute angeben. In diesem Beispiel geben Sie statische Werte für servicetype und port an, während die Eigenschaften name, ipv46 und lbmethod ire Werte aus den Eingabeparametern abrufen. Im Rest des StyleBook können Sie auf die Parameternamen verweisen, die im Parameterabschnitt definiert sind, indem Sie den Ausdruck **$parameters.<parameter-name>** verwenden, zum Beispiel **$parameters.ip**.

> **Hinweis**
>
> Per Konvention wird das Präfix “ns”immer verwendet, um einen Citrix ADC Nitro Namespace im Abschnitt “import-stylebooks”zu bestimmen. Obwohl dies nicht obligatorisch ist, empfiehlt Citrix, die gleiche Konvention in Ihren eigenen StyleBooks zur Konsistenz zu verwenden.

Erstellen Sie Ihr StyleBook

Nachdem Sie alle erforderlichen Abschnitte dieses StyleBooks definiert haben, fügen Sie sie alle zusammen, um Ihr erstes StyleBook zu erstellen. Kopieren Sie den StyleBook-Inhalt, fügen Sie ihn in einen Texteditor ein, und speichern Sie die Datei dann unter dem **Namen lb-vserver.yaml**. Citrix empfiehlt, den integrierten YAML-Validator in StyleBooks zu verwenden, um den YAML-Inhalt zu validieren und zu importieren.

Der vollständige Inhalt der Datei lb-vserver.yaml ist unten wiedergegeben:

```
name: lb-vserver
namespace: com.example.stylebook
version: "1.0"
display-name: Load Balancing Virtual Server (HTTP)
description: "This stylebook defines a very simple load balancing HTTP
   virtual server configuration"
schema-version: "1.0"

```



```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
 -
  namespace: com.citrix.adc.stylebooks
  version: "1.0"
  prefix: stlb

parameters:
 -
  name: name
  label: "Application Name"
  description: "Give a name to the application configuration."
  type: string
  required: true
 -
  name: vip-ipaddress
  label: "Load Balancer IP Address"
  description: "The Application VIP that clients access"
  type: ipaddress
  required: true
 -
  name: lb-alg
  label: LB Algorithm
  description: Load Balancing Algorithm
  type: string
  default: ROUNDROBIN
  allowed-values:
   - ROUNDROBIN
   - LEAST-CONNECTION

components:
 -
  name: lbvserver-comp
  description: This StyleBook component (a Builtin Nitro StyleBook)
     builds a Citrix ADC load balancing virtual server configuration
     object.
  type: ns::lbvserver
  properties:
   name: $parameters.name
   ipv46: $parameters.vip-ipaddress
   lbmethod: $parameters.lb-alg
   servicetype: HTTP
   port: 80
<!--NeedCopy-->
```

Um mit dem StyleBook Konfigurationen zu erstellen, müssen Sie es in NetScaler ADM importieren und es dann verwenden. Weitere Informationen finden Sie unter Verwenden von benutzerdefinierten StyleBooks.

Sie können dieses StyleBook auch in andere StyleBooks importieren (mit dem Import-StyleBooks-

Konstrukt). Oder Sie können dieses StyleBook so ändern, dass es weitere Parameter und Komponenten enthält, wie im nächsten Abschnitt beschrieben.

StyleBook, um eine grundlegende Lastausgleichskonfiguration zu erstellen

February 5, 2024

Im vorherigen Beispiel haben Sie ein einfaches StyleBook erstellt, um einen virtuellen Lastausgleichsserver zu erstellen. Sie können dieses StyleBook unter einem anderen Namen speichern und es dann aktualisieren, um zusätzliche Parameter und Komponenten für eine grundlegende Load-Balancing-Konfiguration aufzunehmen. Speichern Sie diese StyleBook-Datei unter dem **Namen basic-lb-config.yaml**.

In diesem Abschnitt entwerfen Sie ein neues StyleBook, das eine Lastausgleichskonfiguration erstellt, die aus einem virtuellen Lastausgleichsserver, einer Dienstgruppe und einer Liste von Diensten besteht. Es bindet die Dienste auch an die Dienstgruppe und bindet die Dienstgruppe an den virtuellen Server.

Header

Um dieses StyleBook zu erstellen, müssen Sie zunächst den Header-Abschnitt aktualisieren. Dieser Abschnitt ähnelt dem Abschnitt, den Sie für den Lastausgleich des virtuellen Servers StyleBook erstellt haben. Ändern Sie im Header-Abschnitt den Wert von **name** in basic-lb-config. Aktualisieren Sie außerdem die **Beschreibung** und den **Anzeigenamen**, um dieses StyleBook entsprechend zu beschreiben. Sie müssen den **Namespace** und die **Versionswerte** nicht ändern. Da Sie den Namen geändert haben, erstellt die Kombination aus Name, Namespace und Version eine eindeutige Kennung für dieses StyleBook im System.

```
1 name: basic-lb-config
2 description: This StyleBook defines a simple load balancing
     configuration.
3 display-name: Load Balancing Configuration
4 namespace: com.example.stylebooks
5 schema-version: "1.0"
6 version: "0.1"
7 <!--NeedCopy-->
```


StyleBooks importieren

Der Abschnitt Import-StyleBooks bleibt unverändert. Es bezieht sich auf den netscaler.nitro.config-Namespace, um die Nitro-Konfigurationsobjekte zu verwenden.

```
import-stylebooks:
 -
 namespace: netscaler.nitro.config
 prefix: ns
 version: "10.5"
<!--NeedCopy-->
```

Parameter

Sie müssen den Parameterbereich aktualisieren, um zwei zusätzliche Parameter hinzuzufügen, um die Liste der Dienste oder Server und den Port zu definieren, auf dem die Dienste hören. Die ersten drei Parameter, name, ip und lb-alg, bleiben unverändert.

```
parameters:
 -
 name: name
 type: string
 label: Application Name
 description: Name of the application configuration
 required: true
  -
   name: ip
   type: ipaddress
   label: Application Virtual IP (VIP)
   description: Application VIP that the clients access
   required: true
  -
   name: lb-alg
   type: string
   label: LoadBalancing Algorithm
   description: Choose the load balancing algorithm used for load
      balancing client requests between the application servers.
     allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
      default: ROUNDROBIN
  -
   name: svc-servers
   type: ipaddress[]
   label: Application Server IPs
   description: The IP addresses of all the servers of this application
   required: true
  -
   name: svc-port
   type: tcp-port
```



```
    label: Server Port
    description: The TCP port open on the application servers to receive
        requests.
    default: 80
<!--NeedCopy-->
```

In diesem Beispiel wird der Parameter **svc-servers** hinzugefügt, um eine Liste von IP-Adressen der Dienste zu akzeptieren, die die Backend-Server der Anwendung repräsentieren. Dies ist ein obligatorischer Parameter, wie angegeben durch **required: true**. Der zweite Parameter, **svc-port**, gibt die Portnummer an, auf die die Server lauschen. Die Standard-Portnummer ist 80 für den svc-Port-Parameter, falls sie nicht vom Benutzer angegeben wurde.

Komponenten

Sie müssen auch den Komponentenabschnitt aktualisieren, um zusätzliche Komponenten so zu definieren, dass sie die beiden neuen Parameter verwenden und die vollständige Lastausgleichskonfiguration erstellen.

Für dieses Beispiel müssen Sie den Komponentenabschnitt wie folgt schreiben:

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg

components:
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
   name: $parameters.name + "-svcgrp"
   servicetype: HTTP

components:
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $parent.parent.properties.name
   servicegroupname: $parent.properties.name
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
```



```
31    repeat-item: srv
32    properties:
33     ip: $srv
34     port: str($parameters.svc-port)
35     servicegroupname: $parent.properties.name
36  <!--NeedCopy-->
```

In diesem Beispiel hat die ursprüngliche Komponente **lbvserver-comp** (aus dem vorherigen Beispiel) jetzt eine untergeordnete Komponente namens **svcg-comp**. Und die **svcg-comp-Komponente** enthält zwei untergeordnete Komponenten. Durch das Verschachteln einer Komponente innerhalb einer anderen Komponente kann die verschachtelte Komponente Konfigurationsobjekte erstellen, indem sie auf Attribute in der übergeordneten Komponente verweist. Die verschachtelte Komponente kann für jedes Objekt, das in der übergeordneten Komponente erstellt wurde, ein oder mehrere Objekte erstellen.

Die **svcg-comp-Komponente** wird verwendet, um eine Dienstgruppe auf der NetScaler ADC-Instanz zu erstellen, indem die Werte verwendet werden, die für die Attribute der Ressource "Servicegroup" bereitgestellt werden. In diesem Beispiel geben Sie einen statischen Wert für servicetype an, während name seinen Wert aus dem Eingabeparameter bezieht. Sie verweisen auf den im Parameter-Abschnitt definierten **Parameternamen**, indem Sie die Notation **$parameters.name + „-svcgrp"verwenden, wobei**-svcgrp** an den benutzerdefinierten Namen angehängt (verkettet) wird.

Die Komponente **svcg-comp** hat zwei untergeordnete Komponenten, **lbvserver-svg-binding-comp** und **members-svcg-comp**.

Die erste untergeordnete Komponente, **lbvserver-svg-binding-comp**, wird verwendet, um ein Konfigurationsobjekt zwischen der von der übergeordneten Komponente erstellten Dienstgruppe und dem virtuellen Lastausgleichsserver (lbvserver) zu binden, der von der übergeordneten Komponente des übergeordneten Elements erstellt wurde. Die $parent Notation, auch übergeordnete Referenz genannt, wird verwendet, um auf Entitäten in den übergeordneten Komponenten zu verweisen. **Beispielsweise bezieht sich**servicegroupname: $parent.properties.name auf die Dienstgruppe, die von der übergeordneten Komponente svcg-comp erstellt wurde, und Name: $parent.parent.properties.name****bezieht sich auf den virtuellen Server, der von der übergeordneten Komponente lbvserver-compdes** Elternteils erstellt wurde.**

Die **members-svcg-Komponente** wird verwendet, um Konfigurationsobjekte zwischen der Liste der Dienste an die von der übergeordneten Komponente erstellte Dienstgruppe zu binden. Die Erstellung mehrerer Bindungskonfigurationsobjekte wird erreicht, indem das **repeat**-Konstrukt von StyleBook verwendet wird, um über die Liste der Server zu iterieren, die im Parameter **svc-Server** angegeben ist. Während der Iteration erstellt diese StyleBook-Komponente ein Nitro-Konfigurationsobjekt vom Typ **servicegroup_servicegroupmember_binding** für jeden Dienst (im **Repeat-Item-Konstrukt** als srv bezeichnet) in der Dienstgruppe und setzt das ip-Attribut in jedem Nitro-Konfigurationsobjekt auf die **IP-Adresse** des entsprechenden Servers.

Im Allgemeinen können Sie die Konstrukte **Repeat** und **Repeat Item** in einer Komponente verwen-

den, damit diese Komponente mehrere Konfigurationsobjekte desselben Typs erstellt. Sie können dem **Repeat-Item-Konstrukt** einen Variablennamen zuweisen, z. B. srv, um den aktuellen Wert in der Iteration festzulegen. Dieser Variablenname wird in den Eigenschaften derselben Komponente oder in untergeordneten Komponenten als **$<varname>** bezeichnet , zum Beispiel $srv.

Im obigen Beispiel haben Sie Verschachtelung von Komponenten ineinander verwendet, um diese Konfiguration einfach zu konstruieren. In diesem speziellen Fall war das Verschachteln von Komponenten nicht die einzige Möglichkeit, die Konfiguration zu erstellen. Das gleiche Ergebnis hätten Sie auch ohne Verschachtelung erzielen können, wie unten gezeigt:

```
components:
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   servicegroupname: $components.svcg-comp.properties.name
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $components.lbvserver-comp.properties.name
   servicegroupname: $components.svcg-comp.properties.name
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
  name: $parameters.name + "-svcgrp"
  servicetype: HTTP
<!--NeedCopy-->
```

Hier befinden sich alle Komponenten auf der gleichen Ebene (d. h. sie sind nicht verschachtelt), aber das erzielte Ergebnis (die generierte Citrix ADC Konfiguration) ist mit dem der zuvor verwendeten verschachtelten Komponenten identisch. Auch die Reihenfolge, in der die Komponenten im StyleBook deklariert werden, wirkt sich nicht auf die Reihenfolge der Erstellung der Konfigurationsobjekte aus. In diesem Beispiel müssen die Komponenten **svcg-comp und lbvserver-comp, obwohl sie zuletzt deklariert wurden, erstellt werden, bevor die zweite Komponente lbvserver-svg-**

binding-comperstellt wird, da es in der zweiten Komponente Vorwärtsverweise auf diese Komponenten gibt.

> **Hinweis**
>
> Konventionell werden die Namen von StyleBooks, Parametern, Ersetzungen, Komponenten und Ausgaben in Kleinbuchstaben geschrieben. Wenn sie mehrere Wörter enthalten, werden sie durch ein "-"-Zeichen getrennt. Zum Beispiel „lb-bindings", „app-name", „rewrite-config"und so weiter. Eine andere Konvention besteht darin, Komponentennamen mit der Zeichenfolge „-comp"zu versehen.

Ausgaben

Der letzte Abschnitt, den Sie dem neuen StyleBook hinzufügen können, ist der Ausgabebereich, in dem Sie angeben, was dieses StyleBook seinen Benutzern (oder in anderen StyleBooks) zur Verfügung stellt, nachdem es zum Erstellen einer Konfiguration verwendet wird. Sie können beispielsweise im Abschnitt Ausgaben angeben, dass die Konfigurationsobjekte lbvserver und servicegroup verfügbar gemacht werden sollen, die von diesem StyleBook erstellt würden.

```
outputs:
 -
  name: lbvserver-comp
  value: $components.lbvserver-comp
  description: The component that builds the Nitro lbvserver
     configuration object
 -
  name: servicegroup-comp
  value: $components.svcg-comp
  description: The component that builds the Nitro servicegroup
     configuration object
<!--NeedCopy-->
```

Der Ausgabebereich eines StyleBook ist optional. Ein StyleBook muss keine Ausgaben zurückgeben. Durch die Rückgabe einiger interner Komponenten als Ausgabe erhalten StyleBooks, die dieses StyleBook importieren, jedoch mehr Flexibilität, wie Sie beim Erstellen eines zusammengesetzten StyleBooks sehen können.

> **Hinweis**
>
> Es empfiehlt sich, eine gesamte Komponente des StyleBook im Ausgabe-Abschnitt verfügbar zu machen und nicht nur eine einzelne Eigenschaft einer Komponente (z. B. die gesamte $components.lbvserver-comp und nicht nur den Namen $components.lbvserver-comp.properties.name verfügbar zu machen). Fügen Sie der Ausgabe auch eine Beschreibung hinzu, die erklärt, was die spezifische Ausgabe darstellt.

Erstellen Sie Ihr StyleBook

Nachdem Sie alle erforderlichen Abschnitte dieses StyleBooks definiert haben, fügen Sie sie alle zusammen, um Ihr zweites StyleBook zu erstellen. Sie haben diese StyleBook-Datei bereits als **basic-lb-config.yaml**gespeichert. Citrix empfiehlt, dass Sie den integrierten YAML-Validator auf der StyleBooks-Seite verwenden, um den YAML-Inhalt zu validieren und zu importieren.

Der vollständige Inhalt der Datei **basic-lb-config.yaml** ist unten wiedergegeben:

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the loadbalancing algorithm (method) used for
     loadbalancing client requests between the application servers.
  allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: svc-servers
  type: ipaddress[]
  label: Application Server IPs
  description: The IP addresses of all the servers of this application
  required: true

```



```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
    servicegroupname: $parameters.name + "-svcgrp"
    servicetype: HTTP

 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $components.lbvserver-comp.properties.name
   servicegroupname: $components.svcg-comp.properties.servicegroupname
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: 80
   servicegroupname: $components.svcg-comp.properties.servicegroupname
outputs:
-
  name: lbvserver-comp
  value: $components.lbvserver-comp
  description: The component that builds the Nitro lbvserver
     configuration object
-
  name: servicegroup-comp
  value: $components.svcg-comp
  description: The component that builds the Nitro servicegroup
     configuration object
<!--NeedCopy-->
```

Um mit dem StyleBook Konfigurationen zu erstellen, müssen Sie es in NetScaler ADM importieren und es dann verwenden. Weitere Informationen finden Sie unter Verwenden von benutzerdefinierten StyleBooks.

Sie können dieses StyleBook auch in andere StyleBooks importieren und seine Eigenschaften wie im nächsten Abschnitt beschrieben verwenden.

Zusammengesetztes StyleBook erstellen

February 5, 2024

Eine wichtige und leistungsstarke Funktion von StyleBooks ist, dass sie als Bausteine für andere StyleBooks verwendet werden können. Ein StyleBook kann in ein anderes StyleBook importiert werden und es kann als ein **Typ** bezeichnet werden, der von Komponenten des zweiten StyleBook verwendet wird, ähnlich wie ein in Nitro integriertes StyleBook.

Sie können beispielsweise das StyleBookbasic-lb-config**verwenden, das Sie im vorherigen Abschnitt erstellt haben, um ein weiteres StyleBook namens composite-example zu erstellen.** Um das StyleBook "basic-lb-config"verwenden zu können, müssen Sie es in das neue StyleBook im Bereich import-stylebooks importieren.

Erstellen Sie Ihr StyleBook

Das neue StyleBook würde wie folgt aussehen:

```
name: composite-example
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
description: This StyleBook defines a RoundRobin load balancing
   configuration with a monitor.
schema-version: "1.0"
import-stylebooks:
  -
   namespace: netscaler.nitro.config
   version: "10.5"
   prefix: ns
  -
   namespace: com.example.stylebooks
   version: "0.1"
   prefix: stlb
parameters:
  -
    name: name
    type: string
    label: Application Name
    description: Give a name to the application configuration.
    required: true
  -
    name: ip
    type: ipaddress
    label: Application Virtual IP (VIP)
    description: The Application VIP that clients access
    required: true
  -
```



```
30      name: svc-servers
31      type: ipaddress[]
32      label: Application Server IPs
33      description: The IP addresses of all the servers of this
           application
34      required: true
35
36    -
37      name: response-code
38      type: string[]
39      label: List of Response Codes
40      description: List of Response Codes - Provide a list of response
           codes in integer.
41
42  components:
43    -
44      name: basic-lb-comp
45      type: stlb::basic-lb-config
46      description: This component's type is another StyleBook that builds
            the NetScaler lbvserver, servicegroups and services
           configuration objects.
47      properties:
48       name: $parameters.name
49       ip: $parameters.ip
50       svc-servers: $parameters.svc-servers
51    -
52       name: monit-comp
53       type: ns::lbmonitor
54       description: This component is a basic Nitro type (a Builtin
            StyleBook) that builds the NetScaler monitor configuration
            object.
55       properties:
56         monitorname: $parameters.name + "-mon"
57         type: HTTP
58         respcode: $parameters.response-code
59         httprequest: "'GET /'"
60         lrtm: ENABLED
61         secure: "YES"
62
63       components:
64          -
65            name: monit-svcgrp-bind-comp
66            type: ns::servicegroup_lbmonitor_binding
67            properties:
68              servicegroupname: $components.basic-lb-comp.outputs.
                   servicegroup-comp.properties.servicegroupname
69              monitor_name: $parent.properties.monitorname
70  <!--NeedCopy-->
```

Im Abschnitt import-stylebooks importieren Sie das StyleBook basic-lb-config, indem Sie seinen Namespace und seine Version verwenden, auf die mit dem Präfix „stlb“verwiesen wird.

Im Komponentenabschnitt werden zwei Komponenten definiert. Die erste Komponente ist vom Typ

stlb: :basic-lb-config, wobei “basic-lb-config”der Name des StyleBooks ist, das Sie in StyleBook erstellt haben, um eine grundlegende Lastausgleichskonfiguration zu erstellen. Die für diese Komponente definierten Eigenschaften entsprechen den obligatorischen Parametern, die im Basic-lb-config StyleBook deklariert sind. Sie können jedoch jeden Parameter des StyleBook verwenden (sowohl erforderlich als auch optional). Anstatt einen lbvserver, eine Dienstgruppe sowie Dienst- und Dienstgruppenbindungen neu zu erstellen, importieren Sie das StyleBook, das all dies tut, als Komponente und verwenden es, um diese Konfigurationsobjekte im neuen StyleBook zu erstellen.

StyleBook fügt eine zweite Komponente „monit-comp“hinzu, die die Attribute der Nitro-Ressource „lbmonitor“(ein integriertes StyleBook) verwendet, um ein Monitor-Konfigurationsobjekt zu erstellen. Es hat auch eine Unterkomponente „monit-svcgrp-bind-comp“, um das Bindungskonfigurationsobjekt zu erstellen, das den Monitor an die in der ersten Komponente erstellte Servicegruppe bindet. **Da die im StyleBook „basic-lb-config“erstellte Servicegroup-Komponente als Ausgabe verfügbar gemacht wird, kann dieses StyleBook mit dem Ausdruck $components.basic-lb-comp.outputs.servicegroup-comp darauf zugreifen.** Dies ist ein Beispiel dafür, wie der Ausgabeabschnitt vom importierenden StyleBooks verwendet werden kann, um Zugriff auf Komponenten in den importierten StyleBooks zu haben, auf die sie sonst nicht zugreifen können.

Kopieren Sie anschließend den StyleBook-Inhalt, fügen Sie ihn in einen Texteditor ein und speichern Sie die Datei dann unter dem **Namen composite-example.yaml**. Überprüfen Sie den YAML-Inhalt, bevor Sie die Datei in NetScaler ADM importieren. Importieren Sie es dann in NetScaler ADM und erstellen Sie mit diesem StyleBook eine oder mehrere Konfigurationen.

Citrix empfiehlt, den integrierten YAML-Validator in StyleBooks zu verwenden, um den YAML-Inhalt zu validieren und zu importieren.

GUI-Attribute in einem benutzerdefinierten StyleBook verwenden

February 5, 2024

Sie können GUI-Attribute im Parameterabschnitt Ihres StyleBook hinzufügen, um die Felder intuitiv zu gestalten, wenn sie in NetScaler Application Delivery Management (ADM) angezeigt werden.

Beispiel. Sie können einen beschreibenden Namen für den Parameter hinzufügen, indem Sie das Label-Attribut verwenden, und mithilfe des Beschreibungsattributs einen Tooltip für diesen Parameter hinzufügen.

```
name: ip
label: Virtual Server IP Address
description: IP address of the virtual server that represents the load
   balanced application.
type: ipaddress
required: true
```



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

Beispiel. Wenn Sie einen Parameter vom Typ "object"haben, können Sie das Layout mit dem Attribut **gui** definieren. In diesem Beispiel ist das Layout ein reduzierbares Objekt, in dem Felder in zwei Spalten angezeigt werden.

```
name: svcg-advanced
label: Advanced Application Server Settings
type: object
required: false
gui:
 collapse_pane: true
 columns: 2
<!--NeedCopy-->
```

Beispiel. Einige StyleBooks in Citrix ADM werden nur als Bausteine für andere StyleBooks verwendet. Und Sie möchten möglicherweise nicht, dass Benutzer Konfigurationen direkt aus diesen StyleBooks erstellen. Weil diese StyleBooks als Teil anderer StyleBooks verwendet werden sollen. Markieren Sie das StyleBook als privat, um sicherzustellen, dass das StyleBook nicht direkt zum Erstellen von Konfigurationen in der NetScaler ADM GUI verwendet wird.

```
name: basic-lb-config
description: This stylebook defines a simple load balancing
   configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
private: true
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

Benutzerdefinierte StyleBooks importieren

February 5, 2024

Nachdem Sie Ihr StyleBook erstellt haben, müssen Sie es in Citrix Application Delivery Management (ADM) importieren, um es zu verwenden. Mit NetScaler ADM können Sie ein einzelnes StyleBook in YAML-Form oder mehrere StyleBook-YAML-Dateien als Bundle in einem Zip-, TGZ- oder GZ-Formular importieren. Das NetScaler ADM-System validiert Ihre StyleBooks beim Import. Das StyleBook kann jetzt für die Erstellung von Konfigurationen verwendet werden.

NetScaler ADM verfügt auch über einen integrierten YAML-Editor, mit dem Sie die StyleBook YAML-Inhalte erstellen können. Der YAML-Editor ermöglicht es Ihnen, Ihre YAML-Konstrukte über die NetScaler ADM GUI selbst zu validieren. Sie müssen kein separates Tool für diese Validierungsprüfungen verwenden. Der Inhalt wird anhand der YAML-Standards validiert und jede Abweichung wird

hervorgehoben. Sie können dann den Inhalt korrigieren und versuchen, das StyleBook in NetScaler ADM zu importieren. Der integrierte YAML-Editor bietet zwei Vorteile beim Schreiben Ihres eigenen StyleBooks.

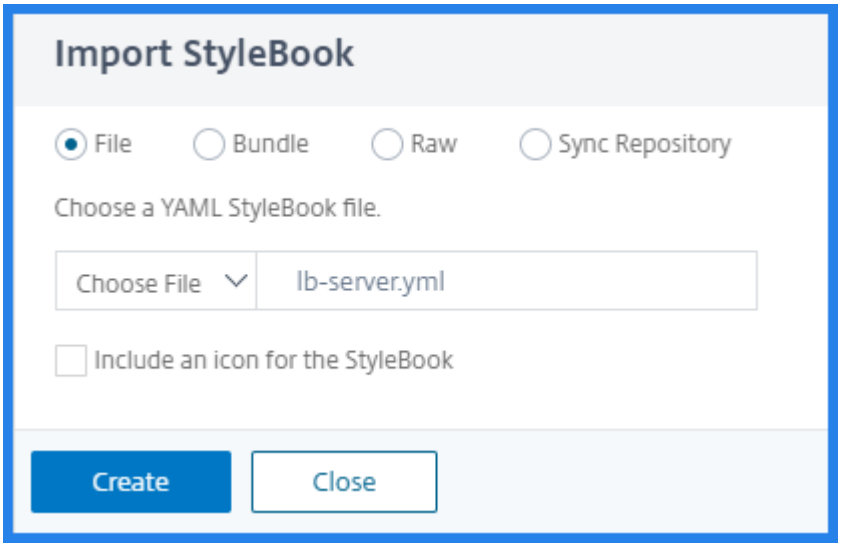
- **Farbcodiert**. Der Editor zeigt den nach YAML-Richtlinien analysierten StyleBook-Inhalt an, und die Farbcodierung hilft Ihnen, einfach zwischen den Schlüsseln und den im YAML-Inhalt definierten Werten zu unterscheiden.
- **YAML-Validierung**. Der Inhalt wird bei der Eingabe auf YAML-Fehler überprüft und jede Abweichung wird sofort hervorgehoben. Mit dieser Validierung können Sie Text schreiben, der den YAML-Richtlinien entspricht, noch bevor Sie das StyleBook in das ADM importieren.

> **Hinweis**
>
> Aktuell überprüft der Editor den Inhalt gemäß den YAML-Richtlinien. Es validiert nicht auf Code Korrektheit und typografische Fehler.

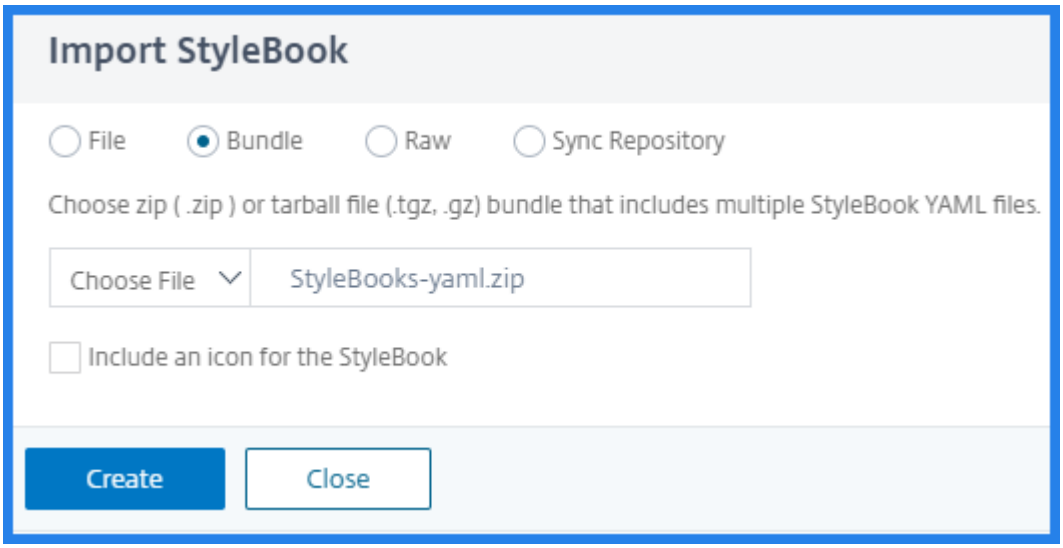
So importieren Sie Ihr StyleBook

1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Konfiguration** > **StyleBooks**, und klicken Sie dann auf **Neues StyleBook importieren**.
2. Klicken Sie auf eine der folgenden Optionen, um ein StyleBook zu importieren.
   - **Datei** - Wählen Sie die gewünschte Datei oder das Bündel von Dateien aus Ihrem lokalen Speicher aus.

     > **Hinweis**
     >
     > Importieren Sie in diesem Beispiel das StyleBook `lb-vserver.yml`, das Sie in StyleBook zum Erstellen eines virtuellen Load Balancing-Servers erstellt haben.



- **Bundle** - Mit NetScaler ADM können Sie mehrere StyleBooks im YAML-Format importieren. Sie können mehrere YAML StyleBook-Dateien importieren, die im ZIP-Format (.zip) oder Tarball-Format (.tgz, .gz) komprimiert sind.



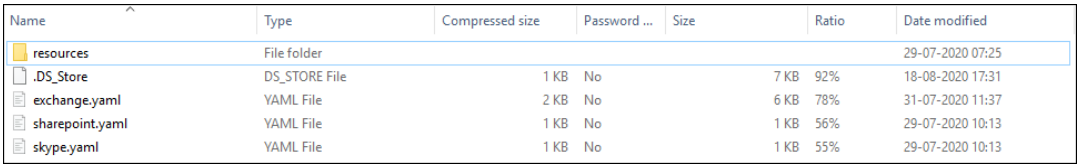
Sie können jetzt jedem StyleBook im Bundle Symbole hinzufügen. Stellen Sie sicher, dass Sie den Ressourcenordner haben, der Symbole in den Formaten PNG, GIF oder JPEG enthält. Wenn der Name der Symboldatei mit dem StyleBook-Namen übereinstimmt, werden die Symbole automatisch den StyleBooks zugeordnet. Ansonsten machen Sie folgendes:

a) Fügen Sie die `icon_mapping.json` Datei im Ressourcen-Ordner hinzu.

b) Ordnen Sie StyleBooks und Symbole in der `icon_mapping.json` Datei wie folgt zu:

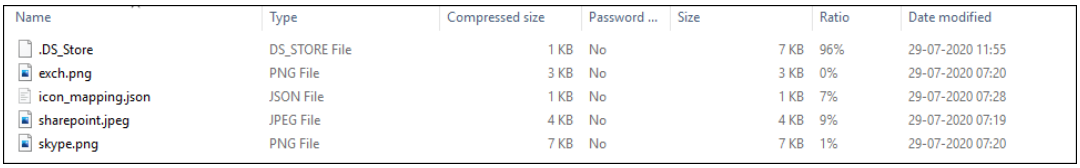
```
<StyleBook file name> : <icon file name>
<!--NeedCopy-->
```

Es folgt ein Beispiel für ein StyleBook-Bundle:



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
resources	File folder					29-07-2020 07:25
.DS_Store	DS_STORE File	1 KB	No	7 KB	92%	18-08-2020 17:31
exchange.yaml	YAML File	2 KB	No	6 KB	78%	31-07-2020 11:37
sharepoint.yaml	YAML File	1 KB	No	1 KB	56%	29-07-2020 10:13
skype.yaml	YAML File	1 KB	No	1 KB	55%	29-07-2020 10:13

Der Ordner `resources` enthält die erforderlichen Symbole.



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
.DS_Store	DS_STORE File	1 KB	No	7 KB	96%	29-07-2020 11:55
exch.png	PNG File	3 KB	No	3 KB	0%	29-07-2020 07:20
icon_mapping.json	JSON File	1 KB	No	1 KB	7%	29-07-2020 07:28
sharepoint.jpeg	JPEG File	4 KB	No	4 KB	9%	29-07-2020 07:19
skype.png	PNG File	7 KB	No	7 KB	1%	29-07-2020 07:20

In diesem Beispiel werden die Dateien `sharepoint.yaml` und `skype.yaml` automatisch `sharepoint.jpeg` und `skype.png` zugeordnet.

Um `exchange.yaml exch.png` zuzuordnen, geben Sie Folgendes in der Datei `icon_mapping.json` an:

```
{

"exchange.yaml":"exch.png"
 }

<!--NeedCopy-->
```

Wenn Sie den `defaulticon` Eintrag angeben, werden die StyleBooks dem Standardsymbol zugeordnet, es sei denn, sie werden einem anderen Symbol zugeordnet.

```
defaulticon: <icon file name>
<!--NeedCopy-->
```

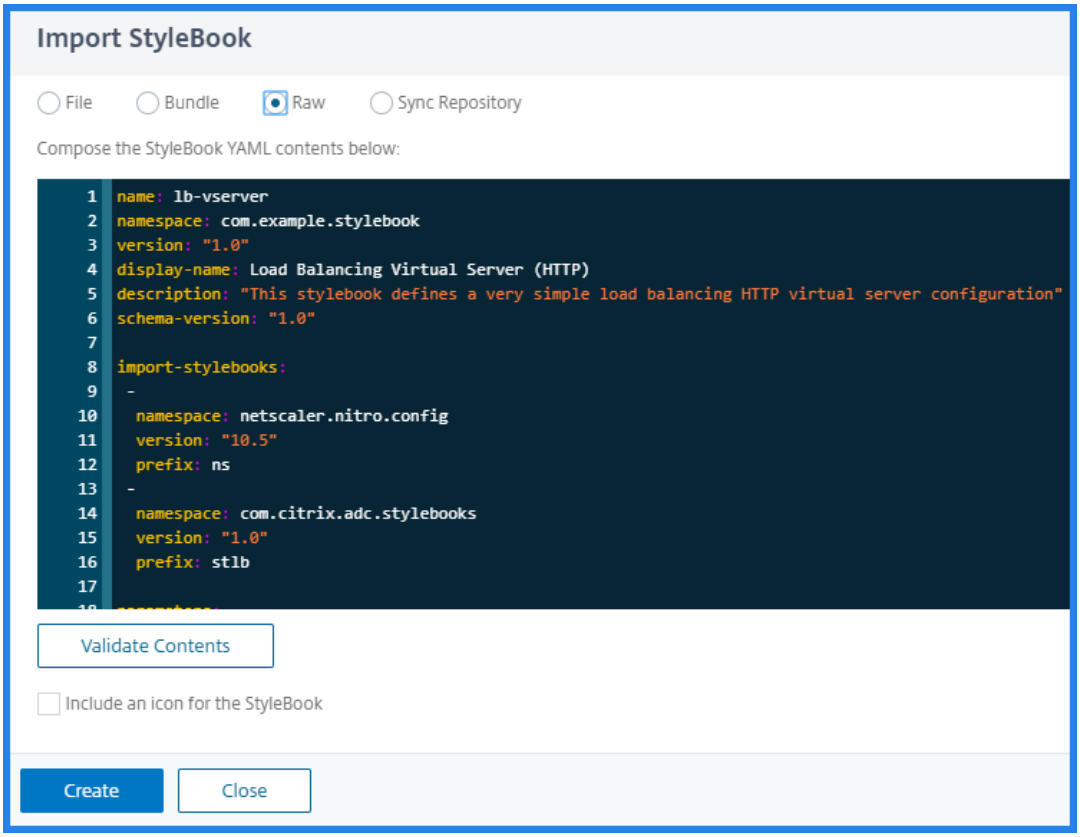
In **Application > StyleBooks**werden die importierten StyleBooks mit den zugeordneten Symbolen angezeigt.

- **Raw** - Verfassen Sie den Inhalt Ihres StyleBook im YAML-Editor.

  Sie können den StyleBook-Inhalt überprüfen, um die StyleBook-Grammatikfehler zu überprüfen Um StyleBook-Inhalte zu überprüfen, klicken Sie auf **Inhalt überprüfen**.

  > **Hinweis: Achten Sie**
  >
  > beim Erstellen von StyleBook darauf, die folgenden Konzepte zu kennen:
  >
  > - NITRO API
  > - YAML

  Weitere Informationen zum Schreiben eigener StyleBooks finden Sie unter How To Create Your Own StyleBooks.



- **Repository synchronisieren** —Diese Option listet die zu ADM hinzugefügten Repositorys auf. Wählen Sie das Repository aus, das Sie mit ADM synchronisieren möchten.

> **Hinweis**
>
> Sie können den Inhalt auch aus einer StyleBook YAML-Datei kopieren und in den YAML-Editor einfügen.

3. Optional können Sie ein Symbol für ein StyleBook auswählen.

   Unter **Applications > StyleBook**wird das importierte StyleBook mit diesem Symbol angezeigt.

4. Klicken Sie auf **Erstellen**.

   NetScaler ADM überprüft jetzt Ihr StyleBook auf alle syntaktischen und semantischen Fehler gemäß der StyleBook-Grammatik. Ihr StyleBook wird nicht in NetScaler ADM importiert, wenn Fehler auftreten.

   Wenn keine Fehler vorliegen, wurde das StyleBook erfolgreich importiert und auf der **StyleBooks-Seite** aufgeführt. Sie können das StyleBook anhand des Anzeigenamens identifizieren, den Sie im Header-Bereich des StyleBook definiert haben.

> **Hinweis:**
>
> Wenn Sie ein Dateipaket importieren, dekomprimiert NetScaler ADM den gezippten Ordner und validiert alle StyleBooks.
> Das Bundle wird nicht importiert, auch wenn eine StyleBook-Datei den Validierungstest fehlschlägt.

Weitere Informationen zur StyleBook-Grammatik und Syntax der verschiedenen Konstrukte und Attribute finden Sie unter StyleBook Grammar.

5. Klicken Sie auf den Link **Konfiguration erstellen**, um Konfigurationen aus diesem StyleBook zu erstellen.

   Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

6. Geben Sie die erforderlichen Werte für die Parameter an.

   Im folgenden Beispiel wird

   a) Geben Sie den **Anwendungsnamen** und die erforderliche **Load Balancer-IP-Adresse** an.

   b) Wählen Sie den **LoadBalancing-Algorithmus** aus der Liste. Standardmäßig ist **ROUNDROBIN** ausgewählt.

7. Wählen Sie unter **Zielinstanzen**die IP-Adresse der NetScaler ADC-Instanz aus, in der Sie die Konfiguration bereitstellen möchten.

   Sie können die Konfiguration auch auf mehreren NetScaler ADC bereitstellen, indem Sie beliebig viele Zielinstanzen angeben.

8. Wenn Sie vor der Bereitstellung der Konfiguration an den NetScaler ADC (NITRO) -Konfigurationsobjekten testen möchten, klicken Sie auf **Trockenlauf**.

   Wenn die Konfiguration gültig ist, werden die Konfigurationsobjekte basierend auf den angegebenen Werten erstellt.

   In diesem Beispiel erstellt das StyleBook nur ein Objekt vom Typ `lbvserver`. Dieser Load-Balancing-Server war die einzige Komponente, die in diesem einfachen Beispiel StyleBook definiert wurde.

   Klicken Sie später auf **Erstellen**, um die Konfiguration auf den ausgewählten NetScaler ADC-Instanzen bereitzustellen.

Nachdem Sie die Konfiguration erfolgreich bereitgestellt haben, wird auf der Seite “**Konfigurationen** “ein neues Konfigurationspaket angezeigt.

> **Hinweis**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte NetScaler ADC-Instanzen in NetScaler ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

Benutzerdefinierte StyleBooks suchen

Mit Citrix ADM können Sie jetzt basierend auf ihrem Typ nach StyleBooks suchen. Das heißt, Sie können jetzt entweder nach Standard-StyleBooks oder nach benutzerdefinierten StyleBooks suchen. Diese Option ist besonders hilfreich, wenn Sie in vielen Standard-StyleBooks nach Ihren benutzerdefinierten StyleBooks suchen müssen.

Um nach benutzerdefinierten StyleBooks zu suchen

1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Konfigurationen** > **StyleBooks**.
2. Klicken Sie oben rechts auf das Suchsymbol.
3. Wählen Sie in der Suchleiste **Typ** und dann **Benutzerdefiniert** aus der Unterliste aus.
4. Citrix ADM zeigt nur die benutzerdefinierten StyleBooks an.

Konfigurationspaket erstellen und bearbeiten

January 23, 2024

In NetScaler Application Delivery Management (ADM) können Sie ein Konfigurationspaket aus einem StyleBook erstellen. Und das Konfigurationspaket ist an das StyleBook gebunden, aus dem es erstellt wurde. Die Aktualisierungen des Konfigurationspakets werden über das StyleBook vorgenommen, an das es gebunden ist.

Erstellen Sie ein Konfigurationspaket

Führen Sie Folgendes aus, um ein Konfigurationspaket aus einem StyleBook zu erstellen:

1. Navigieren Sie zu **Anwendungen > StyleBooks > Konfigurationen**.
2. Klicken Sie auf **Hinzufügen**.
3. **Wählen Sie in Choose StyleBooks**die erforderlichen StyleBooks aus, aus denen Sie ein Konfigurationspaket erstellen möchten.

Diese Seite kategorisiert StyleBooks in Standard- und benutzerdefinierte StyleBooks. Wählen Sie die entsprechenden Reiter aus, um die erforderlichen StyleBooks zu finden

4. Geben Sie die erforderlichen Details wie Anwendungsname, IP-Adresse, Port oder Protokolltyp an.

   Die GUI-Felder unterscheiden sich von StyleBook zu StyleBook.

5. Wählen Sie in **Target Instanzen** Instanzen oder Instanzgruppen aus, in denen Sie die Konfiguration ausführen möchten.

   > **Hinweis:**
   >
   > Sie können die Konfiguration auf mehr als einem NetScaler ADC bereitstellen, indem Sie beliebig viele Zielinstanzen angeben.

6. Klicken Sie auf **Dry Run**.

   Auf der Seite **Objekte** werden die Objekte angezeigt, die erstellt, geändert oder aus den NetScaler ADC-Instanzen entfernt werden.

7. Klicken Sie auf **Erstellen**.

   Das Konfigurationspaket wird auf der Seite **StyleBook > Konfigurationen** angezeigt.

Wenn Sie die vorhandenen Konfigurationspakete bearbeiten möchten, wählen Sie das Konfigurationspaket aus und klicken Sie auf **Bearbeiten**.

Ändern des StyleBook eines Konfigurationspakets

Manchmal müssen Sie das StyleBook aktualisieren, um Funktionen hinzuzufügen oder ein Problem zu beheben. Wenn Sie bereits Konfigurationspakete mit dem alten StyleBook erstellt haben, möchten Sie diese möglicherweise aktualisieren, um das neue aktualisierte StyleBook zu verwenden. Um ein neues StyleBook zu verwenden, ändern Sie das vorhandene StyleBook des Konfigurationspakets.

Betrachten Sie ein Beispiel für ein **StyleBook-Beispiel-lb**, das eine grundlegende Load Balancer-Konfiguration auf einer ADC-Instanz bereitstellt. Und Sie erstellen ein Konfigurationspaket CP1 aus diesem StyleBook.

Wenn Sie Monitore mit der grundlegenden Load Balancer-Konfiguration konfigurieren möchten, benötigen Sie ein neues StyleBook. Erstellen Sie daher **beispiel-lb-mon** StyleBook, das die Möglichkeit bietet, Monitore zusammen mit der grundlegenden Load Balancer-Konfiguration zu konfigurieren.

Nachdem Sie ein StyleBook erstellt haben, aktualisieren Sie das vorhandene Konfigurationspaket CP1, um einige Monitore hinzuzufügen. Führen Sie dazu folgende Schritte aus:

1. Navigieren Sie zu **Anwendungen > StyleBooks > Konfigurationen**.

2. Wählen Sie das Konfigurationspaket aus, für das Sie das StyleBook ändern möchten.

   In diesem Beispiel wählen Sie CP1 aus der Liste aus.

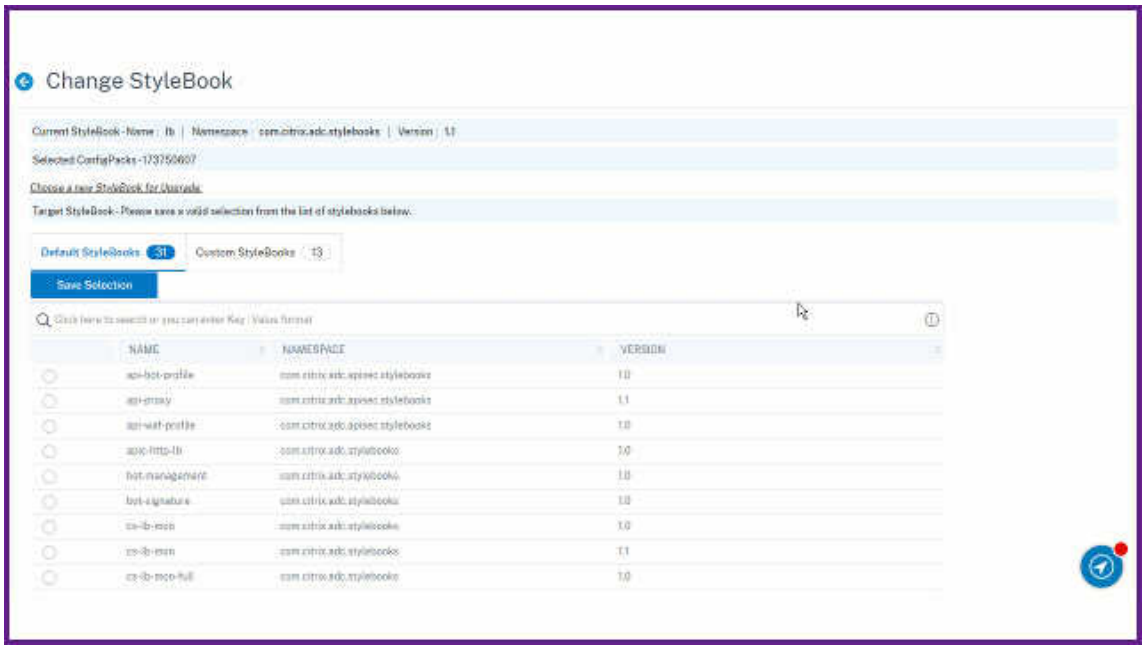
3. Klicken Sie auf **StyleBook ändern**.

4. Wählen Sie das gewünschte StyleBook aus der Liste aus. Klicken Sie dann auf "**Auswahl speichern**".

5. Klicken Sie auf **Ändern**.

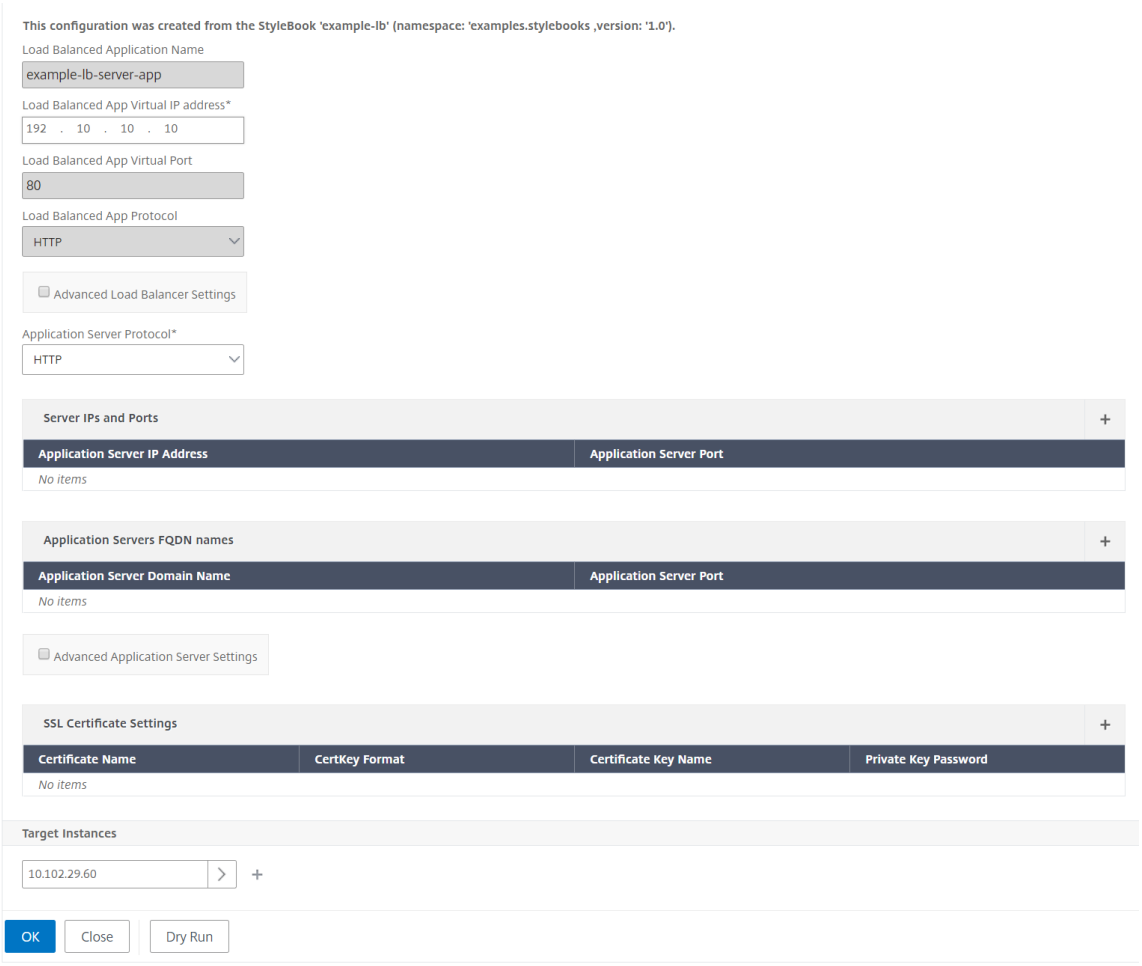
   In diesem Beispiel wählen Sie **example-lb-mon** aus der Liste aus.

   Wenn Sie das StyleBook eines Konfigurationspakets ändern, haben die Parameter im neuen StyleBook möglicherweise eine andere Struktur als das vorhandene StyleBook. Wenn die Parameterstruktur dem vorherigen StyleBook ähnelt, werden die Werte der Parameter automatisch in den jeweiligen Feldern beibehalten. Andernfalls werden nur Parameter übertragen, die die gleiche Struktur zwischen den beiden StyleBooks haben. Zum Beispiel derselbe Parametername, Typ, übergeordnetes Parameterelement und vieles mehr.

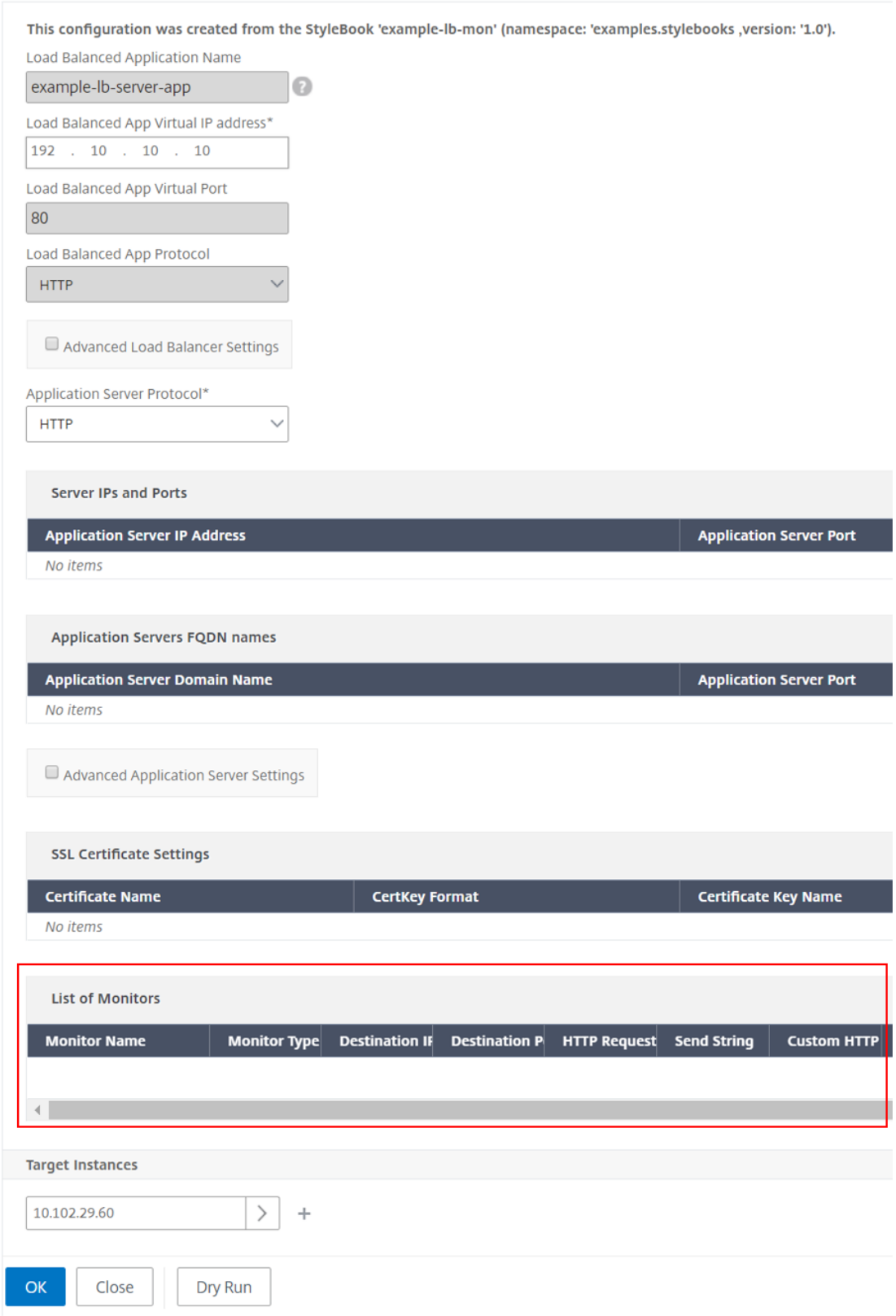
   

   Wenn neue erforderliche Parameter im neuen StyleBook hinzugefügt werden, müssen Sie nach dem Ändern des StyleBook die Werte für solche Parameter manuell angeben.

   In diesem Beispiel lauten die Parameter, die auf der Konfigurationsseite für das StyleBook **example-lb** angezeigt werden:



Die Parameter, die auf der Konfigurationsseite für das neue StyleBook **example-lb-mon** angezeigt werden, lauten wie folgt:



In diesem Fall behalten die StyleBooks die älteren Werte für die grundlegende Load Balancer-

Konfiguration bei, da das neue StyleBook vorhandene Parameter nicht geändert hat. Und es fügt nur die neuen Parameter hinzu. Geben Sie für Monitorparameter manuell die erforderlichen Werte an.

6. Überprüfen Sie in **Target Instanzen** die ausgewählten Instanzen und aktualisieren Sie die Liste bei Bedarf.
7. Klicken Sie auf **Dry Run**.

   Auf der Seite **Objekte** werden die Objekte angezeigt, die erstellt, geändert oder aus den NetScaler ADC-Instanzen entfernt werden.
8. Klicken Sie auf **OK**.

   Auf der Seite **StyleBook > Configurations** wird in der Spalte **StyleBook Name** der neue StyleBook-Name für das ausgewählte Konfigurationspaket angezeigt. In diesem Fall wird **Beispiel-lb-mon**angezeigt.

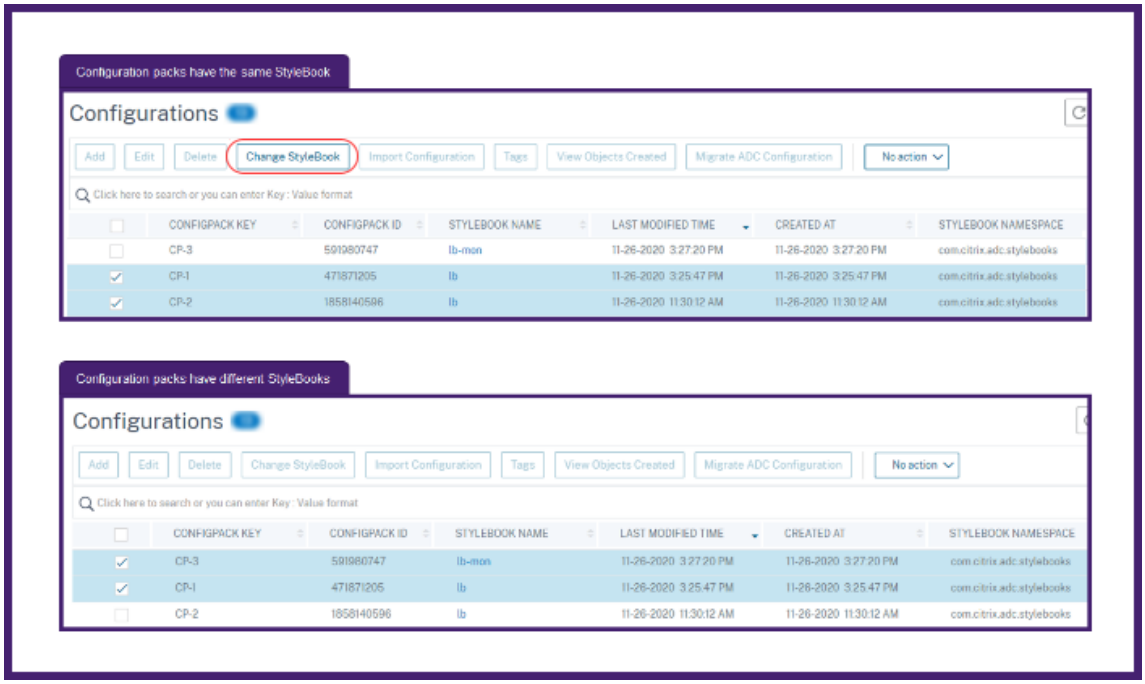
Ändern des StyleBook mit mehreren Konfigurationspaketen

Wenn Sie ein vorhandenes StyleBook mit mehreren Konfigurationspaketen ändern, führen Sie die folgenden Schritte aus:

1. Importieren Sie ein neues StyleBook in ADM.

   In der Regel hat das neue StyleBook den gleichen Namen und den gleichen Namespace mit einer höheren Version als das vorhandene StyleBook. Sie können diesen Schritt jedoch überspringen, wenn der Name, der Namensraum oder die Version unterschiedlich sind.
2. Ändern Sie das StyleBook für die Konfigurationspakete, die mit dem vorhandenen StyleBook verknüpft sind.

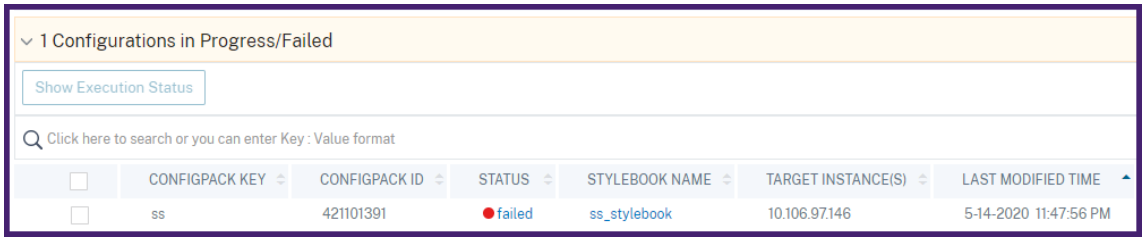
   Sie können **StyleBook ändern** nur auswählen, wenn die ausgewählten Konfigurationspakete mit demselben StyleBook verknüpft sind.



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

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

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



3. Entfernen Sie das alte StyleBook aus ADM, sobald alle Konfigurationspakete an das neue StyleBook gebunden sind.

Exportieren oder Importieren von Konfigurations

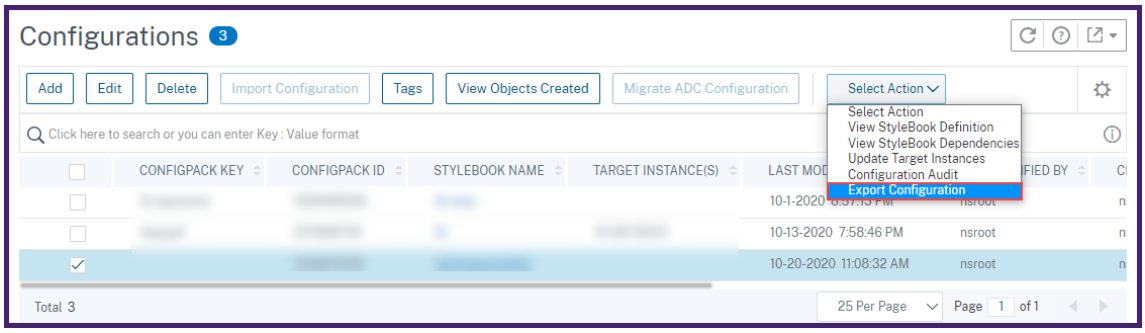
Sie können ein Konfigurationspaket wie StyleBooks exportieren oder importieren. Mit dieser Funktion können Sie die StyleBook-Konfiguration problemlos mit einem anderen ADM-Server teilen. Wenn Sie ein Konfigurationspaket exportieren, wird ein `tgz` oder `zip` Paket auf Ihren lokalen Computer

heruntergeladen. Dieses Bundle enthält eine JSON-Datei mit allen in einem Konfigurationspaket definierten Parameter.

Export-Konfiguration

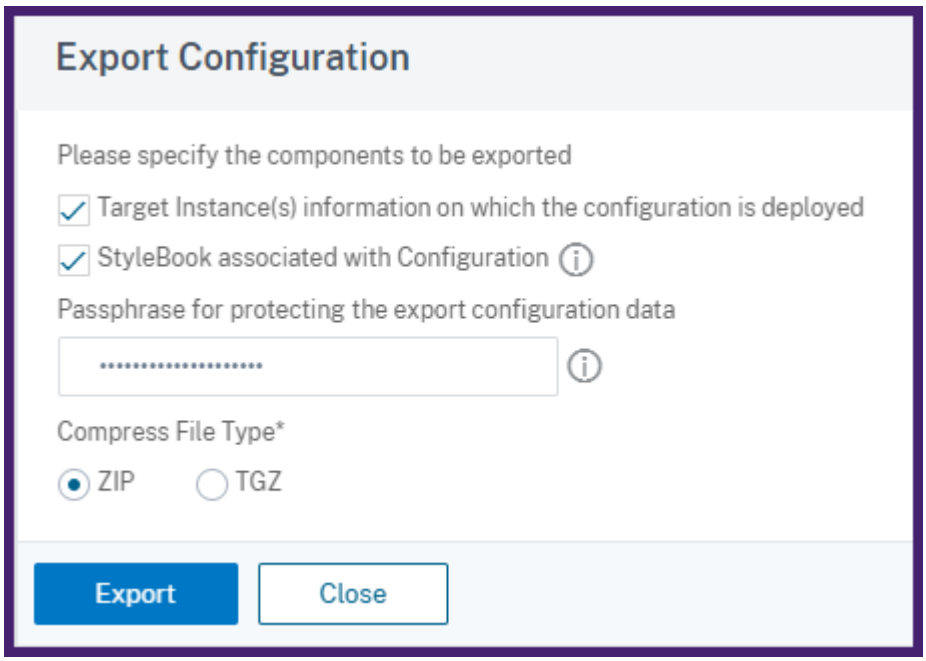
Führen Sie Folgendes aus, um ein Konfigurationspaket zu exportieren:

1. Navigieren Sie zu **Anwendungen > StyleBooks > Konfigurationen**.
2. Wählen Sie ein Konfigurationspaket aus, das Sie exportieren möchten.
3. **Wählen Sie unter Aktion**auswählen die Option **Konfiguration exportieren**aus.



4. Geben Sie im Bereich **Exportkonfiguration** Folgendes an:

   - **Informationen zu Zielinstanzen, für die die Konfiguration bereitgestellt wird**: Wählen Sie diese Option aus, um die Informationen der Zielinstanzen in das Exportpaket aufzunehmen.
   - **Mit Konfiguration verknüpftes StyleBook**: Wählen Sie diese Option aus, um das StyleBook in das Export-Bundle aufzunehmen.
   - **Passphrase zum Schutz der Exportkonfigurationsdaten**: Geben Sie eine Passphrase an, um das Export-Bundle zu verschlüsseln. Diese Passphrase sichert die sensiblen Daten eines Konfigurationspakets.
   - **Dateityp komprimieren**: Wählen Sie entweder **ZIP-** oder **TGZ-Dateityp** aus.



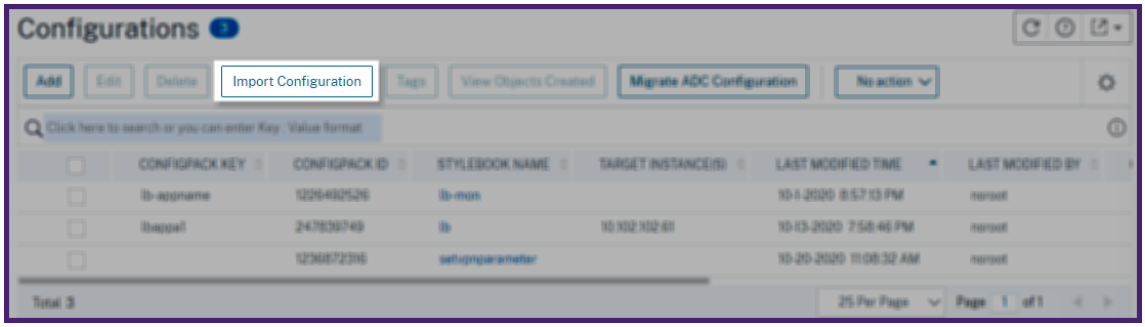
5. Klicken Sie auf **Exportieren**.

   Speichern Sie das Export-Bundle auf Ihrem lokalen Computer.

Konfiguration importieren

Sie können ein Konfigurationspaket von Ihrem lokalen Computer auf einen anderen ADM-Server importieren. Um ein Konfigurationspaket zu importieren, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Anwendungen > StyleBooks > Konfigurationen**.
2. Wählen Sie **Konfiguration importieren**aus.



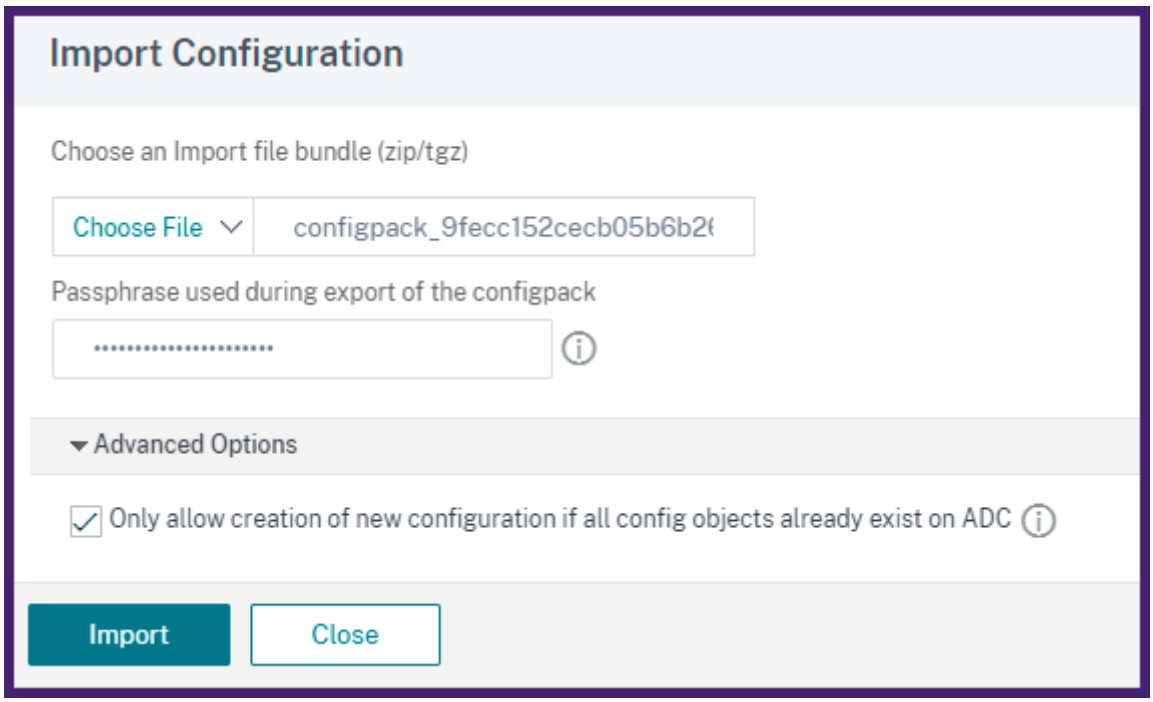
3. Wählen Sie das Importdatei-Paket von Ihrem Computer aus.
4. Verwenden Sie die Passphrase, die Sie beim Export angegeben haben.
5. Optional können Sie in Erweiterte Optionen die Option **Erstellen einer neuen Konfiguration nur zulassen, wenn alle Konfigurationsobjekte bereits auf ADC vorhanden sind**.

Diese Option ändert nicht die Objekte, die bereits auf der ADC-Instanz erstellt wurden.

Bedenken Sie, dass Sie dieselbe ADC-Instanz auf zwei ADM-Servern hinzugefügt haben. Und Sie möchten ein Konfigurationspaket von einem ADM-Server auf einen anderen Server migrieren. Verwenden Sie diese Option, um ein Konfigurationspaket zu importieren, ohne seine Konfigurationsobjekte auf einer ADC-Instanz zu ändern.

> **Wichtig**
>
> Um diese Option zu verwenden, stellen Sie sicher, dass das angegebene Konfigurationspaket die Informationen zu Zielinstanzen enthält. Siehe Konfiguration exportieren.
>
> Diese Option migriert die Konfiguration nur, wenn alle Objekte auf der Zielinstanz vorhanden sind.

6. Klicken Sie auf **Importieren**.



Wenn Sie ein Konfigurationspaket importieren, überprüft der ADM Folgendes:

- **Assoziiertes StyleBook**: Wenn das zugehörige StyleBook nicht im ADM enthalten ist, importiert es das StyleBook zusammen mit dem Konfigurationspaket.
- **Zielinstanzen**: Suchen Sie nach Zielinstanzen und stellt die Konfiguration auf den angegebenen Zielinstanzen bereit. Wenn die genannten ADC-Instanzen im ADM nicht vorhanden sind, wird das Konfigurationspaket ohne Zielinstanzen importiert.
- **Quell-ADM**: Wenn Sie ein Konfigurationspaket auf demselben ADM-Server importieren, aktualisiert das ausgewählte Bundle das vorhandene Konfigurationspaket.

Erstellen Sie Ihre StyleBooks

Der vollständige Inhalt von **Beispiel-lb** StyleBook wird wie folgt als Referenz bereitgestellt:

```
name: example-lb
namespace: examples.stylebooks
version: "1.0"
display-name: Basic Load Balancer App
description: This is an example StyleBook that creates a load balancer application
schema-version: "1.0"
import-stylebooks:
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
parameters-default-sources:
  - stlb::lb
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb configuration objects
    properties-default-sources:
      - $parameters
<!--NeedCopy-->
```

Der vollständige Inhalt von **beispiel-lb-mon** StyleBook wird wie folgt als Referenz bereitgestellt:

```
name: example-lb-mon
namespace: examples.stylebooks
version: "1.0"
description: This is an example StyleBook that creates a load balancer application with monitors
display-name: Basic Load Balancer App with Monitors
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
  - stlb::lb
parameters:
```



```
23    -
24      name: monitors
25      label: "List of Monitors"
26      description: "List of Monitors to monitor Application Servers"
27      type: cmtypes::monitor[]
28  substitutions:
29    mon-name(appname, monname): $appname + "-mon-" + $monname
30  components:
31    -
32      name: lb-comp
33      type: stlb::lb
34      description: Uses the default lb StyleBook to build the typical lb
           configuration objects
35      properties-default-sources:
36        - $parameters
37    -
38      name: monitors-comp
39      type: cmtypes::monitor
40      condition: $parameters.monitors
41      repeat: $parameters.monitors
42      repeat-item: mon
43      repeat-index: ndx
44      description: Builds a list of Citrix ADC monitor objects and binds
           them to the servicegroup of this LB config
45      properties-default-sources:
46        - $mon
47      properties:
48          monitorname: $substitutions.mon-name($parameters.lb-appname,
              $mon.monitorname)
49      components:
50        -
51          name: monitor-svcg-binding-comp
52          condition:  $parameters.svc-servers
53          type: ns::servicegroup_lbmonitor_binding
54          properties:
55            servicegroupname: $components.lb-comp.outputs.servicegroup.
                properties.servicegroupname
56            monitor_name: $parent.properties.monitorname
57  <!--NeedCopy-->
```

Erstellen eines StyleBook zum Hochladen von Dateien in NetScaler ADM

February 5, 2024

Mit Citrix Application Delivery Management (Citrix ADM) -StyleBooks können Sie Citrix ADC Konfigurationen erstellen, die unter anderem beim Hochladen von Dateien beliebiger Art von Ihrem lokalen Dateisystem auf die Citrix ADC-Instanz unter Verwendung der Citrix ADM GUI oder der APIs umfassen können. Bei diesen Dateien kann es sich um Beispielzertifikatsdateien oder Geolocation-Dateien han-

deln. Sie können auch das Verzeichnis angeben, in das diese Dateien hochgeladen werden sollen.

StyleBook-Konfiguration

Im Folgenden finden Sie ein Beispiel-StyleBook, das beschreibt, wie eine Geo-Location-Datei auf die NetScaler ADC-Instanz hochgeladen wird. Die Geodateien werden normalerweise in GSLB-Konfigurationen verwendet, um statische Nähe basierend auf dem geografischen Standort zu definieren:

Erstellen des StyleBooks -1

```
name: upload-geolocations
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
-
 namespace: netscaler.nitro.config
 version: "11.1"
 prefix: ns

parameters:
-
 name: locationfile
 label: Location File
 description: The system file path of the geolocation file on Citrix
    ADM
 type: file
 required: true

components:
-
 name: upload-file-comp
 type: ns::systemfile
 properties:
    filename: $parameters.locationfile.filename
    filelocation: "/var/netscaler/inbuilt_db/"
    filecontent: base64.encode($parameters.locationfile.contents)
<!--NeedCopy-->
```

> **Hinweis**
>
> Der in diesem Beispiel verwendete Parameter ist vom Typ Datei. Sie können dieses StyleBook in

> NetScaler ADM importieren und es zum Hochladen von Geolocationsdateien verwenden.

Dieses StyleBook erfordert, dass die Datei bereits in Citrix ADM vorhanden ist (Sie hätten sie beispielsweise bereits mit einem Dienstprogramm wie scp in Citrix ADM kopiert).
Wenn Sie eine Datei über NetScaler ADM auf Citrix ADCs hochladen möchten, ohne sie zuerst in das NetScaler ADM-Dateisystem zu kopieren, können Sie ein StyleBook erstellen, das über zwei string-Parameter verfügt. Einer ist für die Angabe des Dateinamens, der auf dem NetScaler ADC verwendet werden soll, und der andere, um den Inhalt des -Datei und verwenden Sie diese beiden Parameter in den Upload-file-comp-Komponenten. Im Folgenden finden Sie ein alternatives StyleBook zum Hochladen einer Geolokalisierungsdatei:

Erstellen Sie Ihr StyleBook - 2

```
name: upload-geolocations-alt
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "11.1"
  prefix: ns

parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the Citrix ADC
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true

components:
 -
  name: upload-file-comp
  type: ns::systemfile
  properties:
   filename: $parameters.filename
   filelocation: "/var/Citrix ADC/inbuilt_db/"
   filecontent: base64.encode($parameters.filecontents)
```



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

Erstellen von Konfigurationen zum Hochladen von Dateien

Im folgenden Verfahren wird eine Konfiguration für eine ausgewählte NetScaler ADC-Instanz erstellt, die eine Geolocationsdatei mithilfe des ersten oben beschriebenen StyleBook hochladen würde.

So erstellen Sie eine Konfiguration für das Hochladen von Dateien:

1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Konfiguration**, und klicken Sie auf **Neu erstellen**. Auf der Seite StyleBook auswählen werden alle StyleBooks angezeigt, die in Ihrem NetScaler ADM verfügbar sind. Scrolle nach unten und wähle das StyleBook aus, das du importiert hast

   Die StyleBook-Parameter werden als Benutzeroberflächenseite angezeigt, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

2. Geben Sie den Namen des Load Balancers und die virtuelle IP-Adresse im Abschnitt Grundeinstellungen des Load Balancers ein.

3. Geben Sie im Abschnitt **Standortdatei** den Namen oder Speicherort der Datei ein.

   > **Hinweis:
   >
   > Stellen Sie**sicher, dass sich die Datei in Citrix ADM nur im Ordner des aktuellen Mandanten befindet. Verwenden Sie ein beliebiges Dateiübertragungsprotokoll, um die Datei in das Citrix ADM Dateisystem zu kopieren.

4. Möglicherweise werden Sie aufgefordert, Ihre Benutzeranmeldeinformationen anzugeben, bevor Sie auf die Zielinstanzen zugreifen.

5. Wählen Sie die NetScaler ADC Zielinstanz aus, für die die Konfiguration erstellt werden muss, und klicken Sie auf **Erstellen**.

> **Hinweis**
>
> Citrix empfiehlt, dass Sie**Dry Run**auswählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt werden, bevor Sie die tatsächliche Konfiguration für die Instanz ausführen.

Wenn die Erstellung des Konfigurationspakets erfolgreich ist, wird die Datei im NetScaler ADC-Instanzdateisystem unter dem Speicherort gespeichert: /var/netscaler/inbuilt_db/

> **Hinweis**

> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte NetScaler ADC-Instanzen in NetScaler ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

Verwenden der NetScaler ADM -API zum Erstellen eines Konfigurationspakets

Sie können die NetScaler ADM API auch verwenden, um ein Konfigurationspaket zu erstellen, das Dateien in die ausgewählte NetScaler ADC-Instanz hochlädt. Weitere Informationen zur Verwendung von APIs finden Sie unter So erstellen Sie mithilfe der API Konfigurationen zum Hochladen beliebiger Dateitypen .

Erstellen eines StyleBook zum Hochladen von SSL-Zertifikats- und Zertifikatsschlüsseldateien in NetScaler ADM

February 5, 2024

Wenn Sie eine StyleBook-Konfiguration erstellen, die das SSL-Protokoll verwendet, müssen Sie die SSL-Zertifikatsdateien und Zertifikatsschlüsseldateien entsprechend den Anforderungen der StyleBook-Parameter hochladen. Mit StyleBook können Sie die SSL-Dateien und Schlüsseldateien direkt von Ihrem lokalen System hochladen, indem Sie die NetScaler ADM GUI verwenden. Sie können NetScaler ADM-APIs auch verwenden, um Zertifikatdateien und Schlüsseldateien hochzuladen, die bereits von NetScaler ADM verwaltet werden.

StyleBook-Konfiguration

Dieses Dokument unterstützt Sie bei der Erstellung Ihres eigenen StyleBook - **Load Balancing Virtual Server (SSL)**
mit Komponenten zum Hochladen von SSL-Zertifikaten und Schlüsseldateien. Das hier bereitgestellte StyleBook als Beispiel erstellt eine grundlegende Konfiguration des Lastenausgleichs für die virtuelle Serverkonfiguration auf der ausgewählten NetScaler ADC-Instanz. Die Konfiguration verwendet das SSL-Protokoll. Um eine Konfiguration mit diesem StyleBook zu erstellen, müssen Sie den Namen und die IP-Adresse des virtuellen Servers angeben, die Parameter der Lastausgleichsmethode auswählen und die Zertifikatsdatei und die Zertifikatsschlüsseldatei für den virtuellen Server hochladen oder eine Zertifikatsdatei und eine Zertifikatschlüsseldatei verwenden, die bereits vorhanden sind im NetScaler ADM vorhanden. Diese werden im Abschnitt “Parameter”spezifiziert, wie unten gezeigt:

```
parameters:
 -
  name: name
```



```
    type: string
    required: true
  -
    name: ip
    type: ipaddress
    required: true
  -
    name: lb-alg
    type: string
    allowed-values:
      - ROUNDROBIN
      - LEASTCONNECTION
    default: ROUNDROBIN
  -
    name: certificate
    label: "SSL Certificate File"
    description: "The file name of the SSL certificate file"
    type: certfile
  -
    name: key
    label: "SSL Certificate Key File"
    description: "The file name of the server certificate's private key
       file"
    type: keyfile
<!--NeedCopy-->
```

Im Komponentenbereich des StyleBook werden dann zwei Komponenten erstellt, wie unten gezeigt. Die Komponente „my-lbvserver-comp“ist vom Typ ns: :lbvserver, wobei:

- „ns“ist das Präfix, das sich auf den eingebauten Namespace netscaler.nitro.config und Version 10.5 bezieht, die Sie im Abschnitt import-stylebooks angegeben haben.
- „lbvserver“ist ein integriertes StyleBook in diesem Namespace. Sie entspricht der gleichnamigen virtuellen Serverressource des Citrix ADC NITRO -Lastenausgleichs.

Die zweite Komponente „lbvserver-certificate-comp“ist vom Typ stlb: :vserver-certs-binds. Das Präfix „stlb“bezieht sich auf den Namespace „com.citrix.adc.stylebooks“und Version 1.0, die im Abschnitt import-stylebooks des StyleBook angegeben ist. Wenn der Namespace „com.citrix.adc.stylebooks “als Ordner betrachtet werden kann, ist „vserver-certs-binds“ein weiteres StyleBook (oder eine Datei) in diesem Ordner. StyleBooks, die sich im Namespace com.citrix.adc.stylebooks befinden, werden als Teil von NetScaler ADM ausgeliefert.

Mit dem StyleBook vserver-certs-binds, das von benutzerdefinierten StyleBooks verwendet wird, können Sie die Zertifikate einfach konfigurieren, indem Sie das Zertifikat und die Schlüsseldateien auf die NetScaler ADC Zielinstanz hochladen und die Bindung des Zertifikats und der Schlüsseldateien an die entsprechenden virtuellen Server konfigurieren. Die Eigenschaften für diese Komponente lauten - der Name des virtuellen lb Servers und die Namen der SSL-Zertifikate, die Sie beim Erstellen des Konfigurationspakets angeben.


```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: SSL
   ipv46: $parameters.ip
   port: 443
   lbmethod: $parameters.lb-alg
 -
  name: lbvserver-certificate-comp
  type: stlb::vserver-certs-binds
  description: Binds lbvserver with server certificate
  properties:
   vserver-name: $components.my-lbvserver-comp.properties.name
   certificates:
    -
     cert-name: $parameters.name + "-lb-cert"
     cert-file: $parameters.certificate
     ssl-inform: PEM
     key-name: $parameters.name + "-key"
     key-file: $parameters.key
<!--NeedCopy-->
```

Wenn Sie die API verwenden, um eine Konfiguration aus einem solchen StyleBook zu erstellen, verwenden Sie nur die Dateinamen (nicht den vollständigen Dateipfad). Es wird erwartet, dass diese Dateien bereits in den Zertifikats- und Schlüsseldateiordnern auf NetScaler ADM verfügbar sind. Die hochgeladene SSL-Zertifikatsdatei wird auf NetScaler ADM im Verzeichnis /var/mps/tenants/…gespeichert. /ns_ssl_certs Verzeichnis, und die Schlüsseldatei des SSL-Zertifikats wird in /var/mps/tenants/…gespeichert /ns_ssl_keys Verzeichnis in NetScaler ADM.

Erstellen von Konfigurationen zum Hochladen von SSL-Dateien

Das folgende Verfahren erstellt eine grundlegende Konfiguration des virtuellen Lastenausgleichs auf einer ausgewählten NetScaler ADC-Instanz unter Verwendung des SSL-Protokolls aus dem oben angegebenen StyleBook. Mit diesem Verfahren können Sie die SSL-Zertifikatsdateien und die Zertifikatschlüsseldateien in NetScaler ADM hochladen.

Um eine Konfiguration für das Hochladen von Dateien zu erstellen

1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Konfiguration > StyleBooks**.Auf der Seite "**StyleBooks** "werden alle StyleBooks angezeigt, die in Ihrem Citrix ADM verfügbar sind.
2. Scrollen Sie nach unten, wählen Sie **Load Balancing Virtual Server (SSL)** oder geben Sie**Load Balancing Virtual Server (SSL)** in das Suchfeld ein, und drücken **Sie die Eingabetaste**.

3. Klicken Sie im StyleBook-Bedienfeld auf den Link **Konfiguration erstellen** .

   Die StyleBook-Parameter werden als Benutzeroberflächenseite angezeigt, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

4. Geben Sie den Namen des Load Balancers und die virtuelle IP-Adresse im Abschnitt Grundeinstellungen des Load Balancers ein.

5. Wählen Sie im Abschnitt **SSL-Zertifikatseinstellungen** die entsprechenden Dateien aus Ihrem lokalen Speicherordner aus. Alternativ können Sie die Dateien auswählen, die auf dem NetScaler ADM selbst vorhanden sind.

6. Wählen Sie die NetScaler ADC Zielinstanz aus, für die die Konfiguration erstellt werden muss, und klicken Sie auf **Erstellen**.

> **Hinweise:**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte NetScaler ADC-Instanzen in NetScaler ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.
>
> In Citrix ADM können Sie mit den folgenden Standard-StyleBooks, die als Teil von Citrix ADM ausgeliefert werden, SSL-Unterstützung erstellen, indem Sie die SSL-Zertifikate und Schlüssel hochladen.
>
> - HTTP/SSL LoadBalancing StyleBook (lb)
> - HTTP/SSL-LoadBalancing (mit Monitoren) StyleBook (lb-mon)
> - HTTP/SSL Content-Switching-Anwendung mit Monitoren (cs-lb-mon)
> - Beispielanwendung StyleBook mit CS-, LB- und SSL-Funktionen (sample-cs-app)
>
> Sie können auch Ihre eigenen StyleBooks erstellen, die SSL-Zertifikate verwenden, wie im obigen StyleBook beschrieben

Erstellen Sie Ihr StyleBook

Der vollständige Inhalt der Datei lb-vserver-ssl.yaml ist unten dargestellt:

```
name: lb-vserver-ssl
description: "This stylebook defines a load balancing virtual server
   configuration."
display-name: "Load Balancing Virtual Server (SSL)"
namespace: com.example.ssl.stylebooks
schema-version: "1.0"
version: "0.1"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
```



```
12    version: "10.5"
13   -
14    namespace: com.citrix.adc.stylebooks
15    prefix: stlb
16    version: "1.0"
17
18  parameters:
19   -
20    name: name
21    type: string
22    required: true
23   -
24    name: ip
25    type: ipaddress
26    required: true
27   -
28    name: lb-alg
29    type: string
30    allowed-values:
31      - ROUNDROBIN
32      - LEASTCONNECTION
33    default: ROUNDROBIN
34   -
35    name: certificate
36    label: "SSL Certificate File"
37    description: "The file name of the SSL certificate file"
38    type: certfile
39   -
40    name: key
41    label: "SSL Certificate Key File"
42    description: "The file name of the server certificate's private key
         file"
43    type: keyfile
44
45  components:
46   -
47    name: my-lbvserver-comp
48    type: ns::lbvserver
49    properties:
50      name: $parameters.name
51      servicetype: SSL
52      ipv46: $parameters.ip
53      port: 443
54      lbmethod: $parameters.lb-alg
55   -
56    name: lbvserver-certificate-comp
57    type: stlb::vserver-certs-binds
58    description: Binds lbvserver with server certificate
59    properties:
60     vserver-name: $ components.my-lbvserver-comp.properties.name
61     certificates:
62      -
63       cert-name: $parameters.name + "-lb-cert"
```



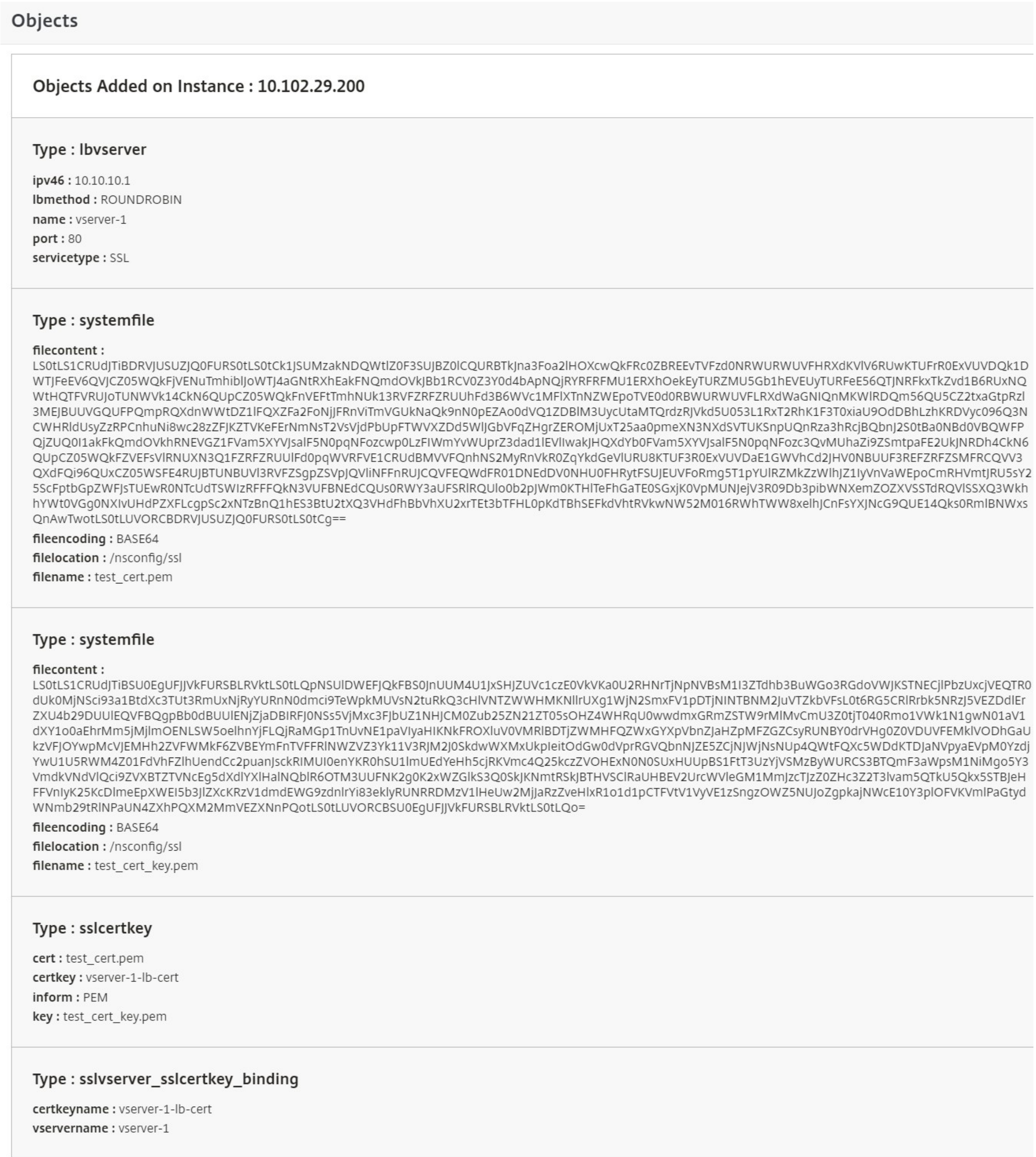
```
64       cert-file: $parameters.certificate
65       ssl-inform: PEM
66       key-name: $parameters.name + "-key"
67       key-file: $parameters.key
68  <!--NeedCopy-->
```

Verwenden der NetScaler ADM -API zum Erstellen eines Konfigurationspakets

Sie können die NetScaler ADM-API auch verwenden, um ein Konfigurationspaket zu erstellen, das Cert- und Key-Dateien auf die ausgewählte NetScaler ADC-Instanz hochlädt. Weitere Informationen zur Verwendung von APIs finden Sie unter So erstellen Sie mithilfe der API Konfigurationen zum Hochladen von Zertifikats- und Schlüsseldateien .

Anzeigen der in der NetScaler ADC-Instanz definierten Objekte

Nachdem das StyleBook-Konfigurationspaket auf NetScaler ADM erstellt wurde, klicken Sie auf **View objects**, um alle NetScaler ADC-Objekte anzuzeigen, die auf der NetScaler ADC-Zielinstanz erstellt wurden



Analytics aktivieren und Alarme auf einem virtuellen Server konfigurieren, der in einem StyleBook definiert ist

February 5, 2024

Sie können das Betriebskonstrukt verwenden, um Citrix ADM Analytics so zu konfigurieren, dass Appflow-Datensätze für alle oder einige der Datenverkehrstransaktionen gesammelt werden, die von einer virtuellen Serverkomponente, die Teil eines StyleBook ist, verarbeitet werden. Sie können dieses Konstrukt auch verwenden, um Alarme zu konfigurieren, um Einblicke in den vom virtuellen Server verwalteten Datenverkehr zu erhalten.

Das folgende Beispiel zeigt einen Operationsabschnitt eines StyleBook:

```
operations:
  analytics:
   -
    name: lbvserver-ops
    properties:
    target: $components.basic-lb-comp.outputs.lbvserver
    filter: HTTP.REQ.URL.CONTAINS("catalog")
   -
    alarms:
     -
      name: lbvserver-alarm
      properties:
      target: $outputs.lbvserver
      email-profile: $parameters.emailprofile
      sms-profile: "NetScalerSMS"

    rules:
     -
      metric: "total_requests"
      operator: "greaterthan"
      value: 25
      period-unit: $parameters.period
     -
       metric: "total_bytes"
       operator: "lessthan"
       value: 60
       period-unit: "day"
<!--NeedCopy-->
```

Die Attribute im Analyseabschnitt werden verwendet, um die Citrix ADM Analysefunktion anzuweisen, Appflow-Datensätze auf einer virtuellen Serverkomponente zu sammeln, die von der Zieleigenschaft identifiziert wird. Optional können Sie auch eine Filtereigenschaft angeben, die einen NetScaler ADC Richtlinienausdruck akzeptiert, um Anforderungen zu filtern, für die Appflow-Datensätze auf dem virtuellen Server gesammelt werden.

Wenn ein Konfigurationspaket aus diesem StyleBook erstellt wird, ist die NetScaler ADM Analytics-Funktion so konfiguriert, dass es Appflow-Datensätze auf den virtuellen Servern sammelt, die beim Erstellen eines Konfigurationspakets angegeben wurden.

Die Attribute im Abschnitt “Alarme”werden verwendet, um Schwellenwerte für die Generierung von Alarmen und das Senden von Benachrichtigungen auf dem virtuellen Server festzulegen, der von der Zieleigenschaft identifiziert wird. Im obigen Beispiel werden die Eigenschaften E-Mail-Profil und SMS-

Profil verwendet, um anzugeben, wohin die Benachrichtigungen gesendet werden sollen. Der Abschnitt Regeln definiert die Schwellenwerte. Wenn beispielsweise die Gesamtzahl der vom virtuellen Server verarbeiteten Anforderungen größer als 25 ist und für einen vom Benutzer definierten Zeitraum ein Alarm gesetzt und eine Benachrichtigung gesendet wird. Die „Periodeneinheit“gibt an, wie oft ein Alarm ausgelöst wird. Es kann den Wert des Tages, der Stunde oder der Woche annehmen.

Sie können die folgenden Operatoren verwenden, wenn Sie den Metrikwert mit dem Schwellenwert vergleichen:

- „größer als“für „>“
- „kleiner als“für „<“
- „greaterthanequal“für „>=“
- „weniger als gleich“für „<=“

Beachten Sie, dass StyleBooks API-Namen für die Metriken verwenden und nicht die Namen, die auf der NetScaler ADM Analytics-GUI angezeigt werden.

Informationen zum Anzeigen und Analysieren von Daten, die auf virtuellen Servern gesammelt wurden, die als Teil eines Konfigurationspakets erstellt wurden, finden Sie in der NetScaler ADM Analytics-Dokumentation.

Instanzrollen

February 5, 2024

In NetScaler Application Delivery Management (ADM) kann es ein Szenario geben, in dem Sie mehrere NetScaler ADC-Instanzen für eine einzelne Anwendung konfigurieren müssen, aber auch, wenn für jede ADC-Instanz eine andere Konfiguration erforderlich ist. Ein Beispiel für einen solchen Fall ist das standardmäßige Microsoft Skype for Business StyleBook.

StyleBooks unterstützt derzeit die Möglichkeit, ein Konfigurationspaket zu erstellen und dieselbe Konfiguration auf mehrere NetScaler ADC-Instanzen anzuwenden. Ein solches Szenario, in dem die Konfiguration auf allen ADC-Instanzen identisch ist, kann als symmetrische Konfiguration bezeichnet werden.

Mit der Funktion “Instanzrollen”von StyleBooks können Sie jetzt eine asymmetrische Konfiguration erstellen, dh ein Konfigurationspaket, das auf mehrere ADC-Instanzen angewendet werden kann, jedoch mit unterschiedlichen Konfigurationen auf verschiedenen ADC-Instanzen.

Wenn ein StyleBook mit Instanzrollen zum Erstellen eines Konfigurationspakets verwendet wird, kann jeder ADC-Instanz in einem Konfigurationspaket eine andere Rolle zugewiesen werden. Diese Rolle bestimmt die Konfigurationsobjekte des Konfigurationspakets, das die ADC-Instanz erhalten wird.

Zu beachtenswerte Punkte:

- Die Gruppe der Instanzrollen in einem StyleBook werden beim Erstellen des StyleBook definiert.
- Die Rollen werden einer bestimmten ADC-Instanz beim Erstellen oder Aktualisieren des Konfigurationspakets zugewiesen.

Abschnitt Zielrollen

In einem StyleBook wird ein neuer Abschnitt namens „target-roles“eingeführt, in dem alle vom StyleBook unterstützten Rollen deklariert werden.

Dieser Abschnitt wird normalerweise nach dem Abschnitt „Import-StyleBooks“eines StyleBooks und vor dem Abschnitt mit den Parametern platziert.

Im folgenden StyleBook-Beispiel sind im Abschnitt „Zielrollen“zwei Rollen definiert: A und B.

```
target-roles:

  -
   name: A
   name: B
     min-targets: 2
     max-targets: 5
<!--NeedCopy-->
```

Sie können sehen, dass Rolle B auch zwei optionale Untereigenschaften definiert, min-targets und max-targets.

Obwohl diese beiden Untereigenschaften optional sind, geben Min-Ziele die minimale obligatorische Anzahl von ADC-Instanzen an, denen diese Rolle zugewiesen werden soll, wenn ein Konfigurationspaket aus diesem StyleBook erstellt wird, und max-targets geben die maximale Anzahl von ADC-Instanzen an, denen diese Rolle beim Erstellen eines Konfigurationspaket aus diesem StyleBook.

Wenn diese Untereigenschaften nicht angegeben sind, gibt es keine Begrenzung für die Anzahl der ADC-Instanzen, die für diese Rolle konfiguriert werden können. Wenn min-targets = 0 ist, ist die mit dieser Rolle verknüpfte Konfiguration optional und wenn min-targets = 1 ist, dann ist diese Konfiguration obligatorisch und mindestens eine ADC-Instanz muss für diese Rolle konfiguriert werden.

Rolle „Standard“

Zusätzlich zu den explizit definierten Rollen gibt es eine implizite Rolle, die alle StyleBooks haben, und diese Rolle wird als Standardrolle bezeichnet. Diese Rolle kann wie jede andere Rolle in einem StyleBook verwendet werden. Wenn beim Erstellen eines Konfigurationspakets eine ADC-Instanz nicht mit einer bestimmten Rolle zugewiesen wird, wird die Instanz implizit der Rolle “Standard”zugewiesen. Die Instanz erhält nun alle Konfigurationsobjekte, die von Komponenten mit der Rolle “Standard” generiert werden.

Komponenten mit Rollen

Nachdem die Rollen definiert wurden, die ein StyleBook unterstützen kann (einschließlich der Rolle „Standard“), können die Rollen im Komponentenbereich eines StyleBooks verwendet werden. Wenn eine Komponente nur auf ADC-Instanzen bereitgestellt werden soll, die eine bestimmte Rolle spielen, können Sie das Attribut roles als Teil der Komponente angeben, wie im folgenden Beispiel einer Komponente dargestellt:

```
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
<!--NeedCopy-->
```

Im obigen Beispiel generiert die Komponente einen „lbvserver“, der auf Instanzen bereitgestellt wird, die die Rolle A spielen. Beachten Sie, dass das roles-Attribut einer Komponente eine Liste ist und einer Komponente mehrere Rollen zugewiesen werden können. Diese Rollen wären im Abschnitt „Zielrollen“des StyleBook deklariert worden.

Hinweis: Wenn eine Komponente in einem StyleBook kein Rollenattribut angibt, werden Konfigurationsobjekte, die von der Komponente generiert werden, auf allen NetScaler ADC Instanzen unabhängig von ihrer Rolle erstellt. Sie können diese Funktion effektiv verwenden, um Konfigurationsobjekte zu erstellen, die auf alle Instanzen eines Konfigurationspakets angewendet werden können.

Nehmen wir an, dass es ein StyleBook mit zwei definierten Rollen gibt - A und B, und das vier Komponenten enthält.

- Komponente C1 hat die Rollen A und B.
- Komponente C2 hat die Rolle B
- Für Komponente C3 sind keine Rollen definiert
- Komponente C4 hat die Rolle „Standard“

Der Komponentenabschnitt dieses StyleBooks ist unten wiedergegeben:

```
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
```



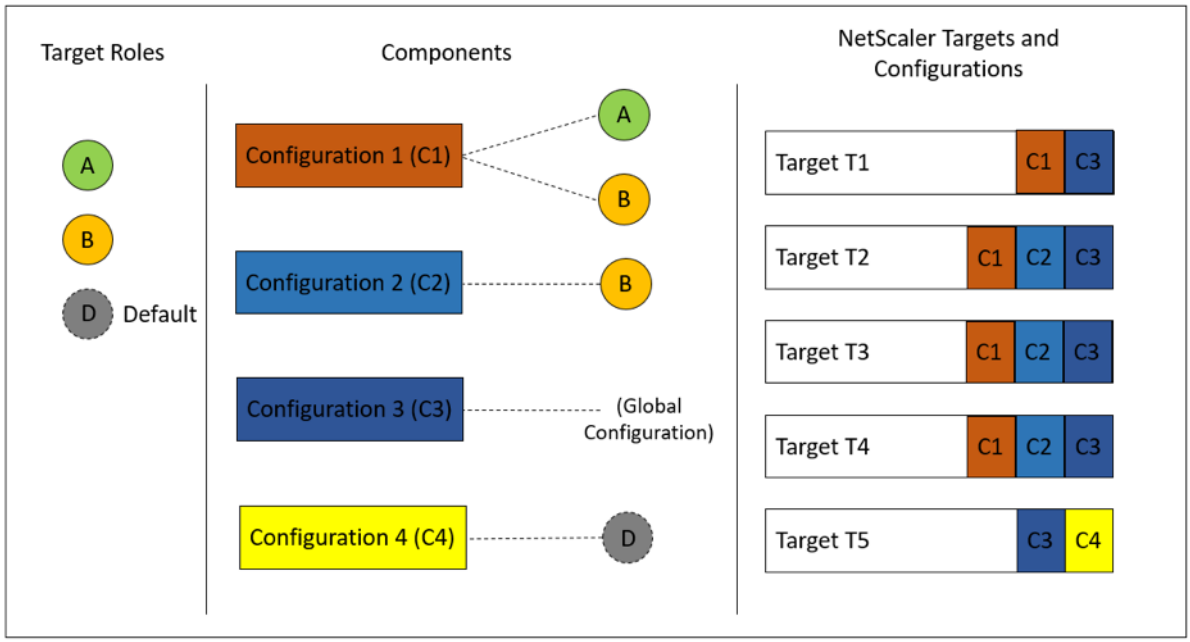
```
9         name: lb1
10        servicetype: HTTP
11        ipv46: 1.1.1.1
12        port: 80
13    -
14      name: C2
15      type: ns::lbvserver
16      roles:
17        - B
18      properties:
19        name: lb2
20        servicetype: HTTP
21        ipv46: 12.12.12.12
22        port: 80
23    -
24      name: C3
25      type: ns::lbvserver
26      properties:
27        name: lb3
28        servicetype: HTTP
29        ipv46: 13.13.13.13
30        port: 80
31    -
32      name: C4
33      type: ns::lbvserver
34      roles:
35        - default
36      properties:
37        name: lb4
38        servicetype: HTTP
39        ipv46: 14.14.14.14
40        port: 80
41  <!--NeedCopy-->
```

Beachten Sie, dass für die Komponente C3 keine Rolle definiert ist, was bedeutet, dass die Komponente unabhängig von ihrer Rolle auf allen Instanzen bereitgestellt wird. Auf der anderen Seite hat die Komponente C4 die Rolle “default”, was bedeutet, dass sie auf jede Instanz angewendet wird, der keine explizite Rolle zugewiesen ist.

Bedenken Sie nun, dass Sie ein Konfigurationspaket mit diesem StyleBook erstellen und es auf fünf ADC-Instanzen bereitstellen möchten. In diesem Stadium können Sie den Instanzen die Rollen folgendermaßen zuweisen:

- Rolle A wird den Instanzen T1, T2, T3 und T4 zugewiesen
- Rolle B ist den Instanzen T2, T3 und T4 zugewiesen
- Instanz T5 ist keine Rolle zugewiesen

Das folgende Bild fasst die Rollenzuweisungen zusammen und zeigt die resultierende Konfiguration, die jede ADC-Instanz erhält:



Beachten Sie, dass die Komponente C3 unabhängig von der Rolle auf allen Instanzen bereitgestellt wird, da diese Komponente kein Rollenattribut hatte.

Sie können auch die Funktion “Dry Run”verwenden, wenn Sie ein Konfigurationspaket erstellen, um die korrekte Zuweisung von Rollen und die Konfigurationsobjekte anzuzeigen und zu überprüfen, die für jede ADC-Instanz erstellt werden.

Erstellen Sie Ihr StyleBook

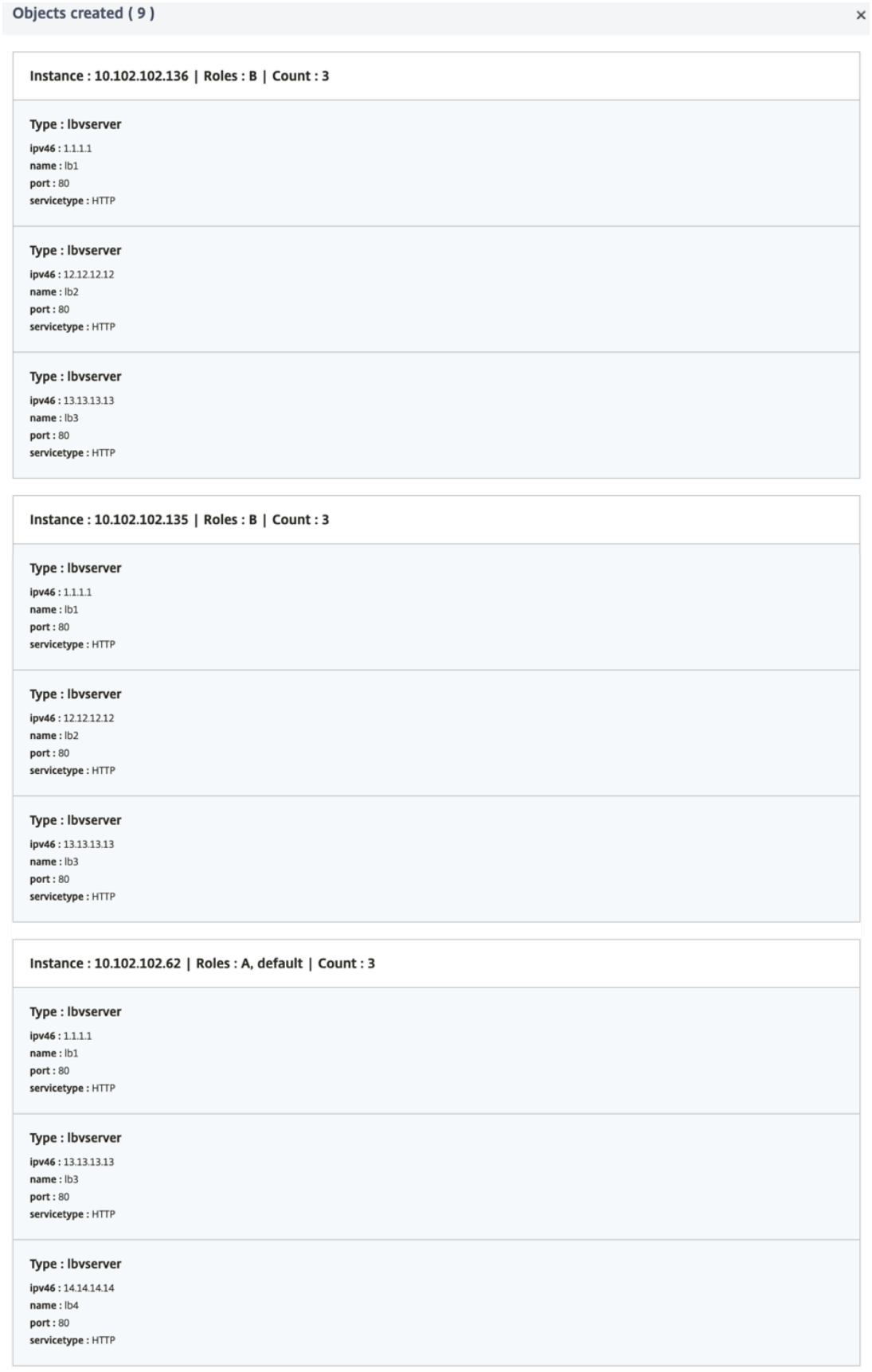
Der vollständige Inhalt des StyleBooks “demo-target-roles”finden Sie unten:

```
---
name: demo-target-roles
namespace: com.example.stylebooks
version: "1.2"
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
  -
    name: A
```



```
20    -
21      name: B
22      min-targets: 2
23      max-targets: 5
24  components:
25    -
26      name: C1
27      type: ns::lbvserver
28      roles:
29        - A
30        - B
31      properties:
32        name: lb1
33        servicetype: HTTP
34        ipv46: 1.1.1.1
35        port: 80
36    -
37      name: C2
38      type: ns::lbvserver
39      roles:
40        - B
41      properties:
42        name: lb2
43        servicetype: HTTP
44        ipv46: 12.12.12.12
45        port: 80
46    -
47      name: C3
48      type: ns::lbvserver
49      properties:
50        name: lb3
51        servicetype: HTTP
52        ipv46: 13.13.13.13
53        port: 80
54    -
55      name: C4
56      type: ns::lbvserver
57      roles:
58        - default
59      properties:
60        name: lb4
61        servicetype: HTTP
62        ipv46: 14.14.14.14
63        port: 80
64  <!--NeedCopy-->
```

Die folgende Abbildung zeigt die für ein Beispiel-Konfigurationspaket erstellten Objekte:



Verwenden von APIs

Wenn Sie die REST-API verwenden, können Sie beim Erstellen oder Aktualisieren des Konfigurationspakets Rollen für jede ADC-Instanz wie folgt angeben. Geben Sie im Block “Ziele”die UUID der jeweiligen NetScaler ADC Instanz an, auf der Sie die einzelnen Komponenten bereitstellen möchten.

```
"targets": [
            {

             "id": "<ADC-UUID>",
             "roles": ["A"]
             }
 ,
           ]
<!--NeedCopy-->
```

Eine vollständige REST-API wird als Referenz bereitgestellt.

POST/<ADM-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"
     }
 ,
     "targets": [
        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",
        "roles": ["A"]
         }
 ,
        {

          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
          "roles": ["A", "B"]
         }
 ,
        {

          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
         }
 ,
        {

```



```
            "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
            "roles": ["A", "B"]
           }
 ,
         {

            "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
            "roles": ["default"]
           }

        ]
       }

 }

<!--NeedCopy-->
```

StyleBooks zum Durchführen von Nicht-CRUD-Operationen erstellen

February 5, 2024

StyleBooks verwalten NetScaler ADC Konfigurationen, indem die erforderlichen Konfigurationsobjekte auf den NetScaler ADC-Instanzen berechnet werden. Diese Objekte werden der Instanz jedes Mal hinzugefügt, aktualisiert oder aus ihr entfernt, wenn Sie ein ConfigPack erstellen oder aktualisieren. Das ist, wenn Sie den gewünschten Zustand angeben.

Einige Citrix ADC Konfigurationsobjekte unterstützen jedoch einige andere Vorgänge als das Erstellen, Aktualisieren oder Löschen (CRUD-Vorgänge). Beispielsweise kann ein Load Balancer-Objekt (lbvserver) oder ein Citrix ADC Featureobjekt (nsfeature) den Vorgang enable oder disable unterstützen. Ähnlich unterstützen Citrix ADC Certkeys den Vorgang Verknüpfung und Verknüpfung aufheben, um ein Zertifikat mit einem anderen Zertifikat zu verknüpfen oder aufzuheben. Diese Vorgänge für NetScaler ADC Objekte werden als Nicht-CRUD-Vorgänge bezeichnet. In diesem Abschnitt wird beschrieben, wie nicht-CRUD-Vorgänge für Konfigurationsobjekte ausgeführt werden, die sie mithilfe von StyleBooks unterstützen.

> **Hinweis:**
>
> Die Bindung zwischen Konfigurationsobjekten (z. B. das Binden eines Certkeys an einen lbvserver) wird nicht als eine Nicht-CRUD-Operation betrachtet. Dies liegt daran, dass Nitro-Bindungen als eigenständige Konfigurationsobjekte dargestellt werden. Diese Objekte werden wie jedes andere NetScaler ADC Konfigurationsobjekt erstellt und gelöscht.

Unterstützung der Nicht-CRUD-Operationen

Ein neues Konstrukt namens „Meta-Eigenschaften“wird der Komponente auf derselben Ebene wie das Konstrukt „Eigenschaften“hinzugefügt. Das einzige Attribut, das in diesem Konstrukt derzeit unterstützt wird, heißt action Dieses Attribut kann Werte wie enable oder disable annehmen, die von diesem Konfigurationsobjekt unterstützt werden.

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  meta-properties
   action: enable
  properties:
    name: $parameters.name
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Im obigen Beispiel ist die Komponente “my-lbvserver-comp”vom Typ “ns: :lbvserver”. Das „ns“ist das Präfix, das sich auf den Namespace netscaler.nitro.config und Version 10.5 bezieht, die Sie im Abschnitt import-stylebooks angegeben haben. Der „lbvserver“ist eine NITRO-Ressource in diesem Namespace. Als implizite Aktion wird der lbvserver zuerst vom StyleBook erstellt; dann wird die Operation „enable“darauf ausgeführt.

Die in den Meta-Eigenschaften angegebene Aktion wird für das Konfigurationsobjekt nur während der Erstellung des ConfigPack ausgeführt. Updates für das ConfigPack führen keine Nicht-CRUD-Aktionen aus.

> **Hinweis:**
>
> Der Wert des action -Attributs kann kein StyleBook-Ausdruck sein, der dynamisch ausgewertet wird.

Konfigurationspaket eines StyleBook auf ein anderes StyleBook migrieren

January 23, 2024

In NetScaler Application Delivery Management (ADM) sind Konfigurationspakete immer an das StyleBook gebunden, aus dem sie erstellt wurden. Jede Aktualisierung des Konfigurationspakets kann nur über das StyleBook durchgeführt werden, an das das Konfigurationspaket gebunden ist. NetScaler

ADM ermöglicht es Ihnen jetzt, ein bestehendes Konfigurationspaket auf ein neues StyleBook zu migrieren. Das neue StyleBook kann eine originellere Version des aktuellen StyleBook sein, das an das Konfigurationspaket gebunden ist. Oder Sie können das Konfigurationspaket auch auf ein völlig anderes StyleBook migrieren.

Sie haben beispielsweise ein StyleBook namens **example-lb**erstellt. Dieses StyleBook wird verwendet, um eine grundlegende Load Balancer-Konfiguration auf einer NetScaler ADC Instanz bereitzustellen. Sie haben ein Konfigurationspaket CP1 aus diesem StyleBook auf einer NetScaler ADC-Instanz erstellt. Später haben Sie erkannt, dass Ihr StyleBook keine Überwachungskonfiguration enthält. Sie haben jetzt ein StyleBook namens **example-lb-mon**erstellt. Dieses StyleBook hat die gleiche Load Balancer-Konfiguration wie example-lb StyleBook, fügt jedoch die Möglichkeit hinzu, Monitore zu konfigurieren.

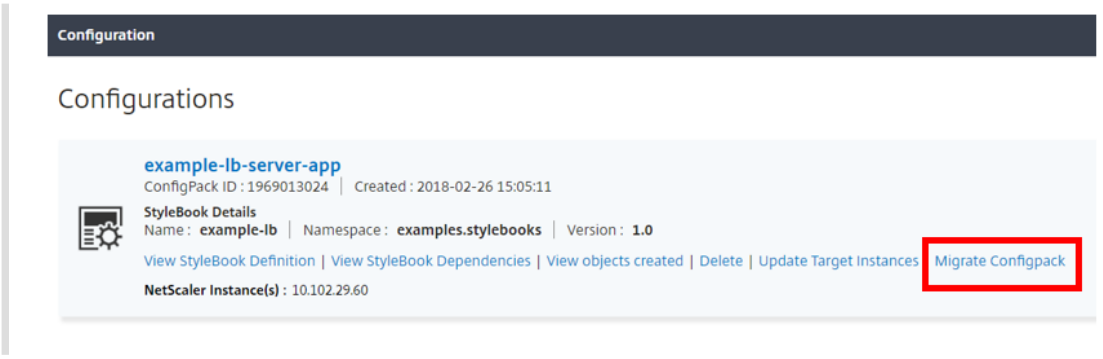
Jetzt möchten Sie Ihre vorhandene Konfiguration, die im Konfigurationspaket CP1 erstellt wurde, aktualisieren, um einige Monitore hinzuzufügen. Zuvor mussten Sie das Konfigurationspaket CP1 löschen und ein Konfigurationspaket CP2 aus dem neuen StyleBook erstellen, um Ihrer Konfiguration Monitore hinzuzufügen. Das Löschen von CP1 führt dazu, dass alle im Konfigurationspaket CP1 erstellten Konfiguration auf einer oder mehreren NetScaler ADC-Instanzen entfernt wird. Zuvor mussten Sie ein neues Konfigurationspaket über das neue StyleBook neu erstellen, indem Sie Werte für alle Parameter eingeben.

Stattdessen können Sie jetzt das vorhandene Konfigurationspaket CP1 auf das neue Beispiel-lb-mon StyleBook migrieren. Ihr neues StyleBook kann Monitor-Details konfigurieren. Nur diese monitorbezogenen Konfigurationsobjekte werden den NetScaler ADC-Instanzen hinzugefügt, in denen das Konfigurationspaket bereitgestellt wurde. Sie müssen jetzt nur die Monitordetails angeben. Die vorhandene Konfiguration, die auf den nicht geänderten NetScaler ADC Instanzen bereitgestellt wird, bleibt davon unberührt.

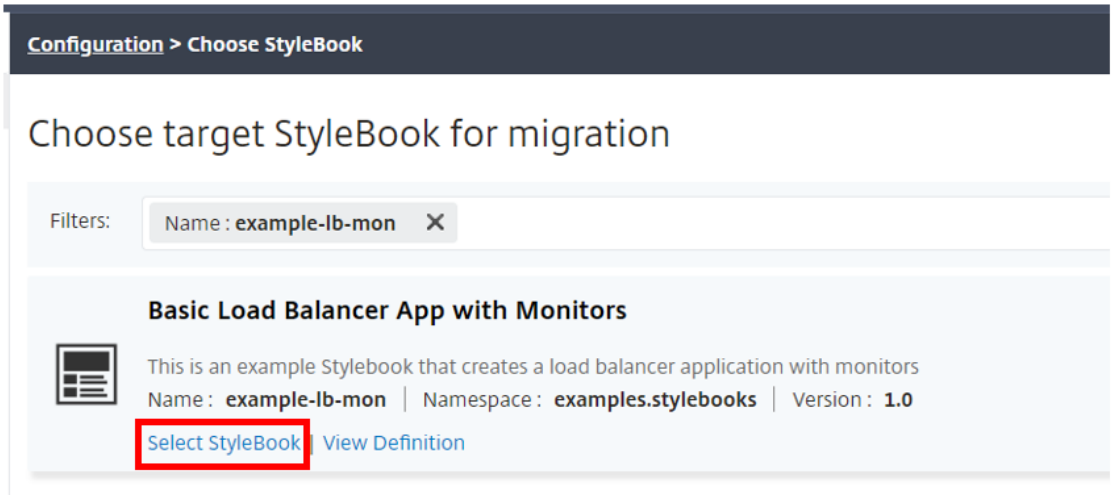
Konfigurationspaket migrieren

So migrieren Sie ein mit example-lb StyleBook erstelltes Konfigurationspaket zum Beispiel lb-mon StyleBook

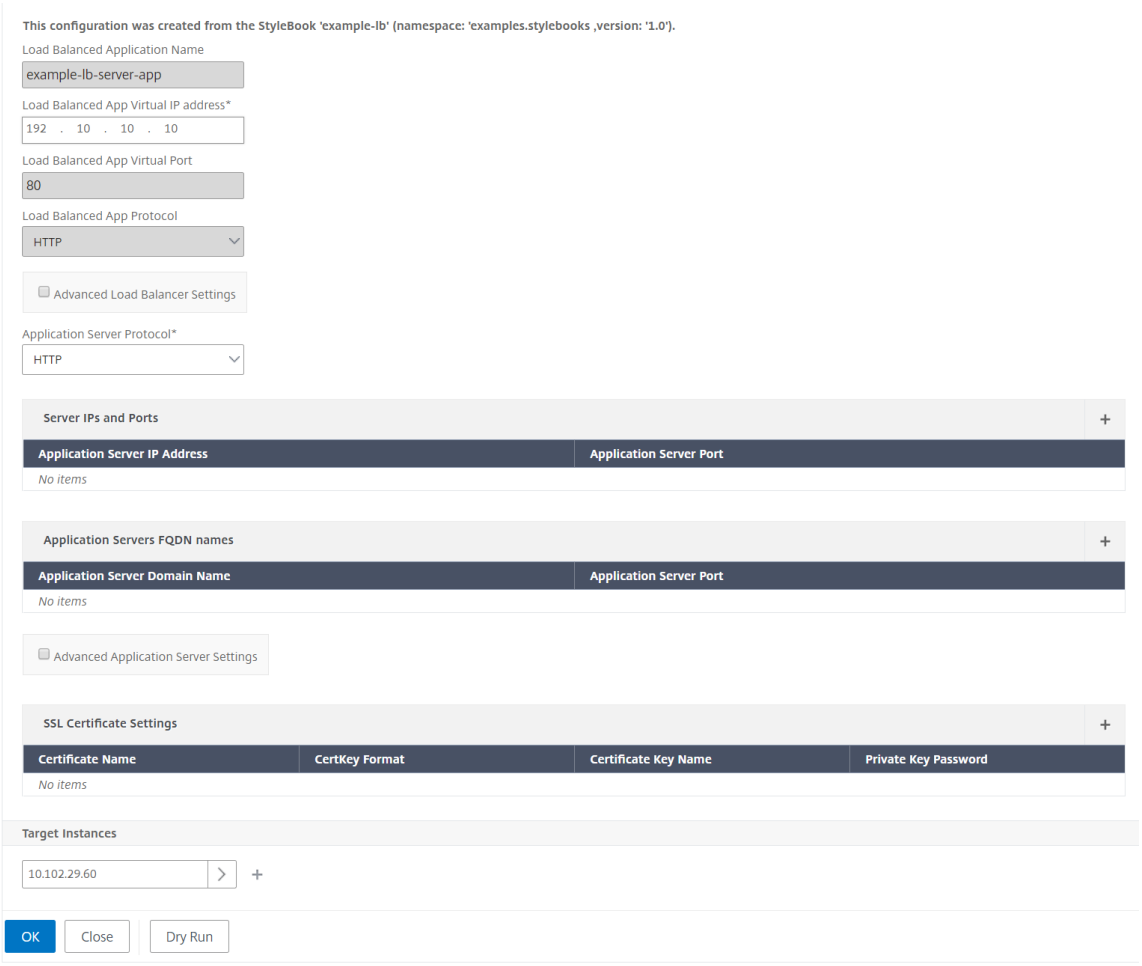
1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Konfigurationen**. Auf der Seite “**Konfigurationen** “werden alle im System vorhandenen Konfigurationspakete angezeigt.
2. Scrollen Sie nach unten, um das **Example-lb-Konfigurationspaket** zu finden, das Sie zuvor erstellt hätten, und klicken Sie auf **Migrate Configpack**.



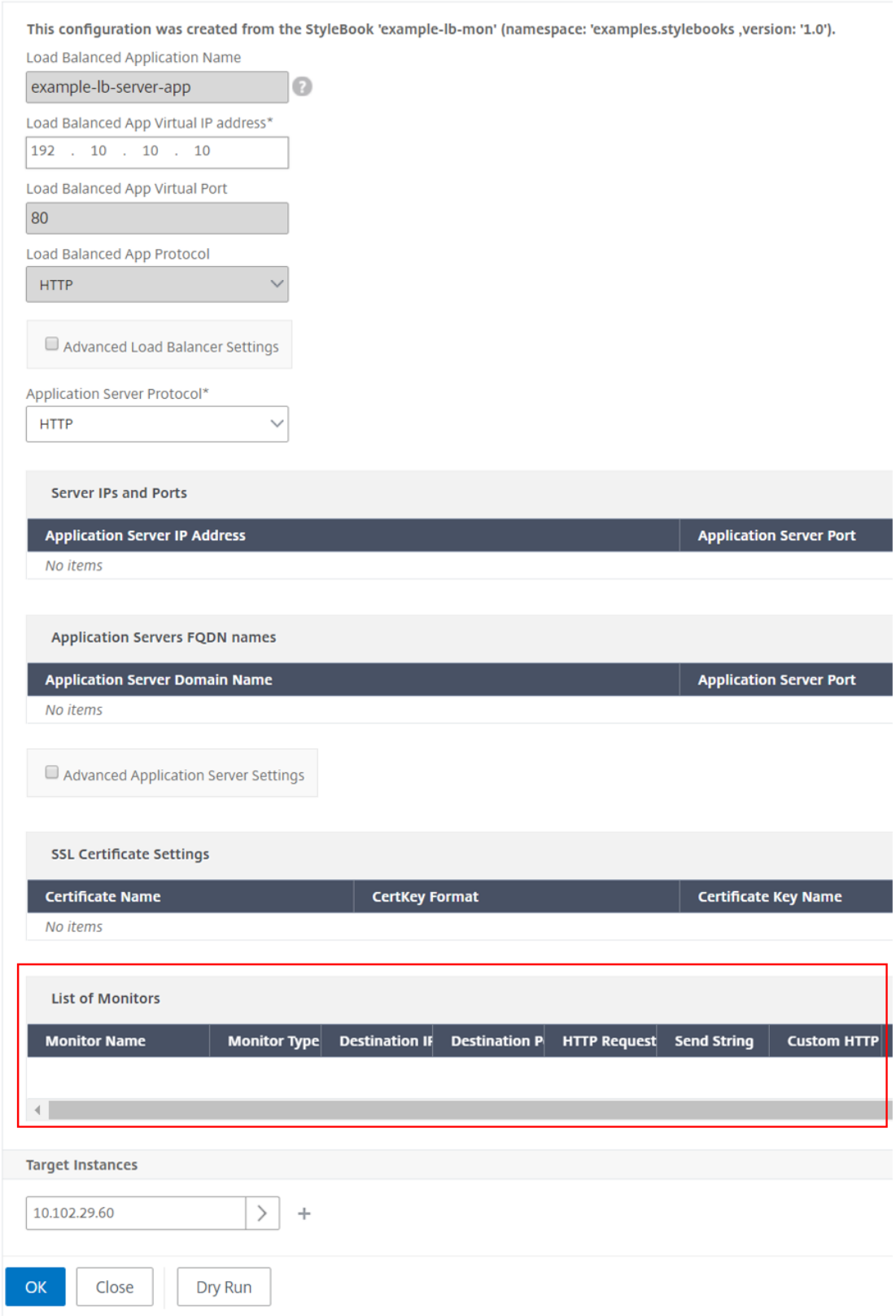
3. Die Seite **Ziel-StyleBook für Migration auswählen** wird geöffnet, auf der alle StyleBooks aufgeführt sind, die in Citrix ADM verfügbar sind. Scrollen Sie nach unten, um das StyleBook **example-lb-mon** zu finden, und klicken Sie auf **StyleBook auswählen**. Sie können auch nach dem StyleBook suchen, indem Sie example-lb-mon eingeben.



Wenn Sie von einem StyleBook zu einem anderen migrieren, haben möglicherweise nicht alle Parameter in den beiden StyleBooks dieselbe Struktur. Wenn die Parameterstruktur ähnlich ist, werden die vorherigen Werte automatisch in den Parameterfeldern beibehalten. Einige der Parameter im neuen StyleBook sind möglicherweise neu, oder ihre Struktur wurde geändert. In einem solchen Fall müssen Sie die Werte für die StyleBook-Parameter manuell eingeben. Die folgende Abbildung zeigt beispielsweise die Parameter des example-lb StyleBook.



Die folgende Abbildung zeigt die Parameter nach der Migration des Konfigurationspakets auf example-lb-mon StyleBook.



In diesem Fall können Sie sehen, dass die StyleBooks die älteren Werte für die grundlegende

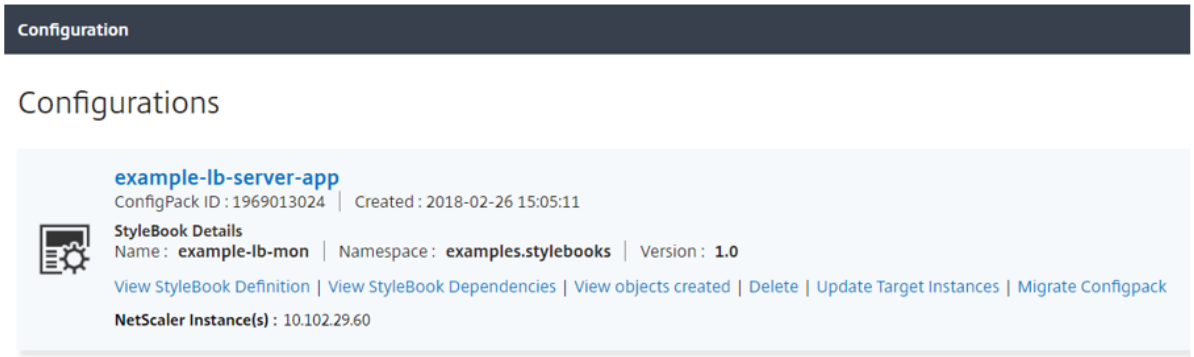
Load Balancer-Konfiguration beibehalten. Sie müssen die Werte für die Monitorparameter jedoch manuell eingeben.

4. Geben Sie Werte für die neuen Parameter ein, die für die Erstellung von Monitoren auf der Instanz verwendet werden.
5. Klicken Sie unter **Zielinstanzen** auf die IP-Adresse der Citrix ADC-Instanz, auf der Sie die Konfiguration ausführen möchten, und wählen Sie sie aus. Beachten Sie, dass Sie die Konfiguration auf mehr als einem Citrix ADC bereitstellen können, indem Sie so viele Zielinstanzen wie nötig angeben.
6. Klicken Sie auf **Dry Run**. Auf der Seite **Objekte** werden die Objekte angezeigt, die neu erstellt, geändert oder aus den Citrix ADC-Instanzen entfernt wurden.
7. Klicken Sie auf **Erstellen**, um die Konfiguration der ausgewählten Instanzen zu erstellen oder zu aktualisieren. Das Konfigurationspaket wird erstellt, wenn die Zielinstanzen neu sind. Andernfalls werden die vorhandenen Konfigurationen, die auf den Instanzen bereitgestellt werden, aktualisiert.

   > **Hinweis:**
   >
   > Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC-Instanzen hinzuzufügen. Diese Instanzen sind also sofort in der Liste der Instanzen in diesem Fenster verfügbar. Das Aktualisierungssymbol ist derzeit nur auf NetScaler ADM verfügbar.

Sie können auch ein Konfigurationspaket von einer Version eines StyleBook auf die nächste Version migrieren. Hier können Sie auch die Werte aller neuen erforderlichen Parameter eingeben, die in der neuen Version vorhanden sind. Sie können das Konfigurationspaket auch auf eine ältere Version des StyleBook migrieren. In diesem Fall werden die zusätzlichen Parameter, die im älteren StyleBook nicht vorhanden sind, entfernt. Auf der **Objektseite** werden alle Objekte angezeigt, die aus der Konfiguration entfernt wurden.

Nach einer erfolgreichen Migration ist das ConfigPack an das neue StyleBook gebunden.



Sie können sehen, dass der Name des Konfigurationspakets und die ID des Konfigurationspakets identisch sind wie zuvor. NetScaler ADM aktualisiert jedoch den StyleBook-Namen in example-lb-mon von example-lb.

Erstellen Sie Ihre StyleBooks

Der vollständige Inhalt des StyleBooks **example-lb** ist unten als Referenz zur Verfügung gestellt:

```
name: example-lb
namespace: examples.stylebooks
version: "1.0"
display-name: Basic Load Balancer App
description: This is an example StyleBook that creates a load balancer
   application
schema-version: "1.0"
import-stylebooks:
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
parameters-default-sources:
  - stlb::lb
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb
       configuration objects
    properties-default-sources:
      - $parameters
<!--NeedCopy-->
```

Der vollständige Inhalt des StyleBooks **example-lb-mon** ist unten für Ihre Referenz zur Verfügung gestellt:

```
name: example-lb-mon
namespace: examples.stylebooks
version: "1.0"
description: This is an example StyleBook that creates a load balancer
   application with monitors
display-name: Basic Load Balancer App with Monitors
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
```



```
16    -
17      namespace: com.citrix.adc.commontypes
18      prefix: cmtypes
19      version: "1.0"
20  parameters-default-sources:
21    - stlb::lb
22  parameters:
23    -
24      name: monitors
25      label: "List of Monitors"
26      description: "List of Monitors to monitor Application Servers"
27      type: cmtypes::monitor[]
28  substitutions:
29    mon-name(appname, monname): $appname + "-mon-" + $monname
30  components:
31    -
32      name: lb-comp
33      type: stlb::lb
34      description: Uses the default lb StyleBook to build the typical lb
           configuration objects
35      properties-default-sources:
36        - $parameters
37    -
38      name: monitors-comp
39      type: cmtypes::monitor
40      condition: $parameters.monitors
41      repeat: $parameters.monitors
42      repeat-item: mon
43      repeat-index: ndx
44      description: Builds a list of Citrix ADC monitor objects and binds
           them to the servicegroup of this LB config
45      properties-default-sources:
46        - $mon
47      properties:
48          monitorname: $substitutions.mon-name($parameters.lb-appname,
              $mon.monitorname)
49      components:
50        -
51          name: monitor-svcg-binding-comp
52          condition:  $parameters.svc-servers
53          type: ns::servicegroup_lbmonitor_binding
54          properties:
55            servicegroupname: $components.lb-comp.outputs.servicegroup.
                properties.servicegroupname
56            monitor_name: $parent.properties.monitorname
57  <!--NeedCopy-->
```


API zum Erstellen von Konfigurationen aus StyleBooks verwenden

February 5, 2024

Nachdem Sie Ihr StyleBook erstellt haben, müssen Sie es in Citrix Application Delivery Management (ADM) importieren, um es entweder mithilfe des Citrix ADM oder mithilfe von Citrix ADM-APIs zu verwenden. NetScaler ADM validiert Ihr StyleBook, wenn Sie es importieren. Wenn die Validierung erfolgreich ist, wird Ihr StyleBook im NetScaler ADM-Katalog von StyleBooks angezeigt und kann zum Erstellen von Konfigurationen verwendet werden.

Sie können jetzt die StyleBook-APIs verwenden, um Konfigurationen basierend auf diesem StyleBook zu erstellen. Sie können beliebige Tools wie das Befehlszeilentool curl oder die Postman Chrome-Browsererweiterung verwenden, um HTTP-Anforderungen an Citrix ADM zu senden.

Beispiel 1

Betrachten Sie das "lb-vserver"-StyleBook, das Sie in StyleBook erstellt haben, um einen virtuellen Lastausgleichsserver zu erstellen. Verwenden Sie die REST-API, um ein Konfigurationspaket aus diesem StyleBook wie folgt zu erstellen:

```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks

<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters": {

      "name": "lb1",
      "ip": "10.102.117.31"
     }
 ,
    "target_devices":
    [
      {

        "id": "deecee30-f478-4446-9741-a85041903410"
       }

```



```
    ]
 }

 }

<!--NeedCopy-->
```

In dieser HTTP-Anforderung ist die ID (z. B. “deecee30-f478-4446-9741-a85041903410”) die Instanz-ID der NetScaler ADC-Instanz, auf der der virtuelle Lastausgleichsserver lb1 mit der IP-Adresse 10.102.117.31 erstellt wird. Die Instanz-ID der NetScaler ADC-Instanz wird von NetScaler ADM abgerufen.

Um die ID einer Instanz zu erhalten, die von NetScaler ADM verwaltet wird, können Sie NetScaler ADM-APIs verwenden. Um beispielsweise die Instanz-ID einer Citrix ADC Instanz abzurufen, deren IP-Adresse 192.168.153.160 lautet, können Sie die folgende API verwenden:

```
GET https://<MAS-IP>/nitro/v1/config/ns?filter=ip_address
   :192.168.153.160
<!--NeedCopy-->
```

```
Accept: application/json
<!--NeedCopy-->
```

Die Antwort enthält die ID in der Nutzlast:

```
200
OK
Content-Type: application/json
{

  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "ns",
  "username": "nsroot",
  "tenant_name": "Owner",
  "resourceName": "",
  "ns":
  [
    {

    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    …"id": "deecee30-f478-4446-9741-a85041903410",
    ...
    }

 ]
 }
```



```
27
28 <!--NeedCopy-->
```

Wenn das Konfigurationspaket erfolgreich erstellt wurde, erhalten Sie die folgende HTTP-Antwort:

```
1  200 OK
2  Content-Type: application/json
3  {
4
5    "configpack":
6    {
7
8      "config_id": "1460806080"
9     }
10
11   }
12
13 <!--NeedCopy-->
```

Sie haben Ihr erstes Konfigurationspaket erstellt, das durch die ID 1460806080 eindeutig identifiziert wird. Mit dieser ID können Sie die Konfiguration abfragen, aktualisieren oder löschen.

Beispiel 2

Sie können dasselbe StyleBook verwenden, um ein anderes Konfigurationspaket zu erstellen und es auf denselben oder verschiedenen NetScaler ADC-Instanzen auszuführen. Erstellen Sie in diesem Beispiel eine weitere Konfiguration, geben Sie einen anderen Namen und eine andere IP-Adresse für den virtuellen Server an und geben Sie LEASTCONNECTION als Lastausgleichsmethode an. Stellen Sie diese Konfiguration auf zwei NetScaler ADC-Instanzen bereit.

Die HTTP-Anfrage lautet wie folgt:

```
1  POST
2
3  https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
       example.stylebooks/0.1/lb-vserver/configpacks
4  <!--NeedCopy-->
```

```
1  Content-Type: application/json
2  Accept: application/json
3  {
4
5    "configpack":
6    {
7
8      "parameters":
9      {
10
11       "name": "lb2",
12       "ip": "10.102.117.32",
```



```
13         "lb-alg": "LEASTCONNECTION"
14       }
15   ,
16      "target_devices"
17      [
18       {
19   "id": "deecee30-f478-4446-9741-a85041903410" }
20   ,
21       {
22   "id": "debecc60-d589-4557-8632-a74032802412" }
23
24      ]
25     }
26
27   }
28
29   <!--NeedCopy-->
```

In dieser HTTP-Anforderung wird der virtuelle Server lb2 mit der IP-Adresse 10.102.117.32 auf den beiden NetScaler ADC-Instanzen erstellt, die durch die IDs deecee30-f478-4446-9741-a85041903410" und debecc60-d589-4557-8632-a74032802412"dargestellt werden.

Bei erfolgreicher Erstellung des Konfigurationspakets wird die folgende HTTP-Antwort empfangen:

```
1   200 OK
2   Content-Type: application/json
3   {
4
5      "configpack":
6     {
7
8        "config_id": "1657696292"
9      }
10
11   }
12
13   <!--NeedCopy-->
```

Dieses neue Konfigurationspaket hat eine andere ID 165769629. Sie können diese Konfiguration mithilfe dieser ID aktualisieren oder entfernen.

Beispiel 3

Betrachten Sie das "basic-lb-config"-StyleBook, das Sie in StyleBook erstellt haben, um eine grundlegende Lastausgleichskonfiguration zu erstellen. Verwenden Sie die REST-API, um ein Konfigurationspaket aus diesem StyleBook wie folgt zu erstellen:

```
1   POST
2
```



```
http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example
    .stylebooks/0.1/basic-lb-config/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters":
    {

      "name": "myapp",
      "ip": "10.70.122.25",
      "svc-servers":
      ["192.168.100.11","192.168.100.12"],
       "svc-port": 8080
     }
 ,
    "target_devices":
    [
     {

      "id": "deecee30-f478-4446-9741-a85041903410"
      }
 ,
     {

      "id": "debecc60-d589-4557-8632-a74032802412"
      }

    ]
   }

 }

<!--NeedCopy-->
```

In dieser HTTP-Anforderung wird die Lastausgleichskonfiguration auf zwei NetScaler ADC Instanzen ausgeführt. Sie können sich bei diesen NetScaler ADC-Instanzen anmelden, um zu überprüfen, ob ein virtueller Server und eine Dienstgruppe mit zwei Diensten erstellt werden.

Beispiel 4

Betrachten Sie das zusammengesetzte **StyleBook-Composite-Beispiel**, das Sie in Composite StyleBook erstellenerstellt haben. Verwenden Sie die REST-API, um ein Konfigurationspaket aus diesem StyleBook wie folgt zu erstellen:


```
POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters": {

      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53"]
     }
 ,
    "target_devices":
    [
    {

      "id": "deecee30-f478-4446-9741-a85041903410"
     }
 ,
    {

      "id": "debecc60-d589-4557-8632-a74032802412"
     }

    ]
   }

 }

<!--NeedCopy-->
```

In dieser HTTP-Anforderung wird die Konfiguration auf zwei NetScaler ADC Instanzen erstellt, die durch ihre IDs dargestellt werden. Wenn Sie sich bei NetScaler ADC-Instanzen anmelden, können Sie die Konfigurationsobjekte anzeigen, die mit dem StyleBook “basic-lb-config”erstellt wurden, das in das StyleBook “composite-example”importiert wurde. Sie können auch einen neuen HTTP-Monitor namens “myapp-mon”sehen, der Teil des “composite-example”StyleBook war.

Bei erfolgreicher Erstellung des Konfigurationspakets wird die folgende HTTP-Antwort empfangen:

```
200 OK
Content-Type: application/json{

  "configpack": {

    "config_id": "4917276817"
```



```
    }

 }

<!--NeedCopy-->
```

Aktualisieren einer Konfiguration

Um diese Konfiguration beispielsweise durch Hinzufügen eines neuen Backend-Servers mit IP-Adresse 10.102.29.54 zum virtuellen Lastausgleichsserver myapp zu aktualisieren, verwenden Sie die API zum Aktualisieren eines Konfigurationspakets wie folgt:

```
PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack": {

    "parameters": {

      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
    }
 ,
  "target_devices":
  [
    {

    "id": "deecee30-f478-4446-9741-a85041903410"
     }
 ,
  {

    "id": "debecc60-d589-4557-8632-a74032802412"
    }

]
 }

 }

<!--NeedCopy-->
```

Bei erfolgreichem Update des Konfigurationspakets wird die folgende HTTP-Antwort empfangen:


```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config-id": "4917276817"
   }

 }

<!--NeedCopy-->
```

Löschen einer Konfiguration

Um diese Konfiguration (aus allen NetScaler ADC-Instanzen) zu löschen, können Sie die API wie folgt zum Löschen eines Konfigurationspakets verwenden:

```
DELETE http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
<!--NeedCopy-->
```

```
Accept: application/json
<!--NeedCopy-->
```

Bei erfolgreichem Löschen des Konfigurationspakets wird die folgende HTTP-Antwort empfangen:

```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config_id": "4917276817"
   }

 }

<!--NeedCopy-->
```

Sie können sich bei der NetScaler ADC-Instanz anmelden und sicherstellen, dass alle Konfigurationsobjekte, die Teil dieses Konfigurationspakets sind, entfernt wurden.

Wenn Sie die Konfiguration von bestimmten NetScaler ADC-Instanzen anstelle von allen entfernen möchten, verwenden Sie den oben beschriebenen Update-Konfigurationspack-Vorgang und ändern Sie das Attribut “target_devices”in der JSON-Nutzlast, um die spezifischen NetScaler ADC-Instanz-IDs zu entfernen.

API zum Erstellen von Konfigurationen zum Hochladen von Zertifikaten und Schlüsseldateien verwenden

February 5, 2024

Verwenden Sie die StyleBook-APIs, um Konfigurationen basierend auf diesem StyleBook zu erstellen. Sie können ein beliebiges Tool wie das Befehlszeilentool curl oder die Browsererweiterung Postman Chrome verwenden, um HTTP-Anforderungen an NetScaler Application Delivery Management (ADM) zu senden.

Betrachten Sie das StyleBook-Beispiel, das Sie zum Hochladen des Zertifikats und der Schlüsseldateien in How to Create a StyleBook to Upload SSL-Zertifikat und Zertifikatsschlüsseldateien zu NetScaler ADMerstellt haben. Verwenden Sie die REST-API, um ein Konfigurationspaket aus diesem StyleBook wie folgt zu erstellen:

```
POST

https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.
   citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async
<!--NeedCopy-->
```

```
Content-Type: application/jsonAccept: application/json {

   "configpack": {

       "parameters": {

           "lb-appname": "lbmon",
           "lb-virtual-ip": "13.1.11.10",
           "lb-virtual-port": "80",
           "lb-service-type": "HTTP",
           "svc-service-type": "HTTP",
           "svc-servers": [
               {

                   "ip": "14.1.1.15",
                   "port": "80"         }

      ],
           "certificates": [
               {

                   "cert-name": "server_cert",
                   "cert-file": "server_cert.pem",
                   "ssl-inform": "PEM",
                   "key-name": "server_key",
                   "key-file": "server_key.pem",
                   "cert-password": "secret",
                   "cert-advanced": {
```



```
                        "is-ca-cert": false,
                        "skip-ca-name": false
            }

          }

       ],
            "lb-advanced": {

                "flush-on-state-down": "ENABLED",
                "auth-params": {

                    "authentication": "OFF",
                    "authentication-http-401": "OFF"
          }
  ,
                "appflow-log": "ENABLED",
                "algorithm": "LEASTCONNECTION"
        }
  ,
            "svcg-advanced": {

                "svc-client-ip": "DISABLED",
                "svc-use-source-ip": "NO",
                "svc-use-proxy-port": "NO",
                "svc-surge-protection": "OFF",
                "svc-client-keepalive": "NO",
                "svc-tcp-buffering": "NO",
                "svc-compression": "NO",
                "svc-state": "ENABLED",
                "svc-downstate-flush": "DISABLED",
                "svc-enable-health-monitor": "NO"
        }

      }
  ,
        "targets": [
            {

                "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"
        }

     ]
    }

  }

<!--NeedCopy-->
```

Dieses Konfigurationspaket wird unter Verwendung der ID 8c158e7a-0087-423f-91b0-0ccf16de552a eindeutig identifiziert. Mit dieser ID können Sie die Konfiguration abfragen, aktualisieren oder löschen. Bei erfolgreicher Aktualisierung des Konfigurationspakets werden das Zertifikat und die

Schlüsseldateien in das NetScaler ADM-Dateisystem hochgeladen.

API zum Erstellen von Konfigurationen zum Hochladen beliebiger Dateitypen verwenden

February 5, 2024

Sie können auch die NetScaler Application Delivery Management (ADM) -API verwenden, um ein Konfigurationspaket zu erstellen, das Dateien in die ausgewählte NetScaler ADC-Instanz hochlädt.

Betrachten Sie das StyleBook-Beispiel, das Sie zum Hochladen von Dateien eines beliebigen Typs inHow to Create a StyleBook to Upload Files to NetScaler ADC MA Serviceerstellt haben. Erstellen Sie wie im Beispiel im obigen Thema ein Konfigurationspaket und geben Sie den Wert des Parameters "locationfile"als Dateipfad der Standortdatei auf NetScaler ADM an.
Verwenden Sie REST API, um ein Konfigurationspaket aus diesem StyleBook wie folgt zu erstellen:

```
POST

https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.stylebooks.samples/1.0/upload-geolocations/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

   "configpack":
   {

      "parameters": {

         "locationfile": "/var/mps/tenants/root/files/ / custom_geolocations.csv"
      }
 ,
      "targets": [
         {

            "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"
         }

    ]
   }

 }

<!--NeedCopy-->
```


API zum Importieren benutzerdefinierter StyleBooks verwenden

February 5, 2024

Mit den StyleBook-APIs können Sie nun benutzerdefinierte StyleBooks in NetScaler Application Delivery Management (ADM) importieren. Verwenden Sie die REST-API, um ein Konfigurationspaket aus diesem StyleBook wie in einem Tool wie dem curl-Befehlszeilentool oder der Chrome-Browsererweiterung von Postman zu erstellen Sie können beispielsweise ein StyleBook mit dem Namen example-lb importieren, das zum Erstellen einer Load Balancer-Konfiguration auf einer NetScaler ADC-Instanz verwendet werden kann.

```
HTTP Method: POST
URL: http://<mas-ip>/stylebook/nitro/v1/config/stylebooks
Headers:
Content-Type: application/json
Accept: application/json
RequestBody:
{

       "stylebook":
  {

     "file_name": "example-lb.yaml",
     "source": "<base64-contents>",
     "encoding": "base64"
   }

 }

<!--NeedCopy-->
```

wobei der Wert des Attributs „source“die Base64-Codierung des Inhalts Ihrer StyleBook-Datei ist. Sie können den YAML-Inhalt Ihrer StyleBook-Datei in ein Online-Tool einfügen,https://www.browserling.com/tools/file-to-base64 um beispielsweise die Base64-Zeichenfolge zu erhalten, die Sie dann als Wert für das obige Attribut „source“verwenden können.

Mit diesem API-Aufruf können Sie auch eine komprimierte Tarball-Datei (TGZ-Datei) hochladen, die mehrere StyleBook-Dateien in einem API-Vorgang enthält. Ändern Sie dazu einfach das Attribut file_name auf den Dateinamen .tgz und den Wert für das Quellattribut auf die Base64-Kodierung des Inhalts Ihrer .tgz-Datei.

Nachdem die API erfolgreich im Tool ausgeführt wurde, erhalten Sie die folgende Antwort, die angibt, dass das StyleBook in NetScaler ADM importiert wurde.

```
200 OK
<!--NeedCopy-->
```

Antworttext:


```
{


  "stylebook":
{


    "name": "example-lb",

    "namespace": "com.example.stylebook",

    "version": "1.0"

   }


 }

<!--NeedCopy-->
```

API zum Herunterladen benutzerdefinierter StyleBooks verwenden

February 5, 2024

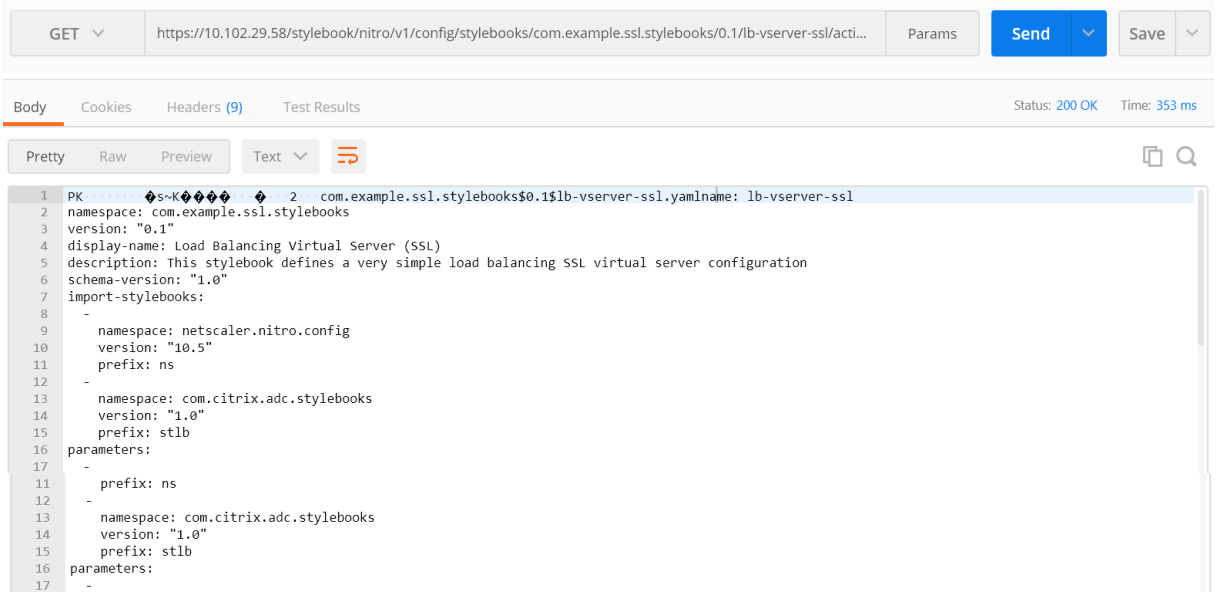
Sie können ein benutzerdefiniertes StyleBook herunterladen, indem Sie die folgende StyleBooks-REST-API bereitstellen:

```
GET

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
   VERSION>/<NAME>/actions/download
<!--NeedCopy-->
```

Sie können die API in jedem Tool wie dem curl-Befehlszeilentool oder der Postman Chrome-Browsererweiterung ausführen, nachdem Sie Änderungen an den Feldern IP-Adresse, Name, Version und Namespace vorgenommen haben.

```
GET

https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.
   ssl.stylebooks/0.1/lb-vserver-ssl/actions/download`
<!--NeedCopy-->
```

Das StyleBook im Format.yaml wird heruntergeladen.



API zum Löschen benutzerdefinierter StyleBooks verwenden

February 5, 2024

Sie können das benutzerdefinierte StyleBook löschen, indem Sie die folgende StyleBooks-REST-API bereitstellen:

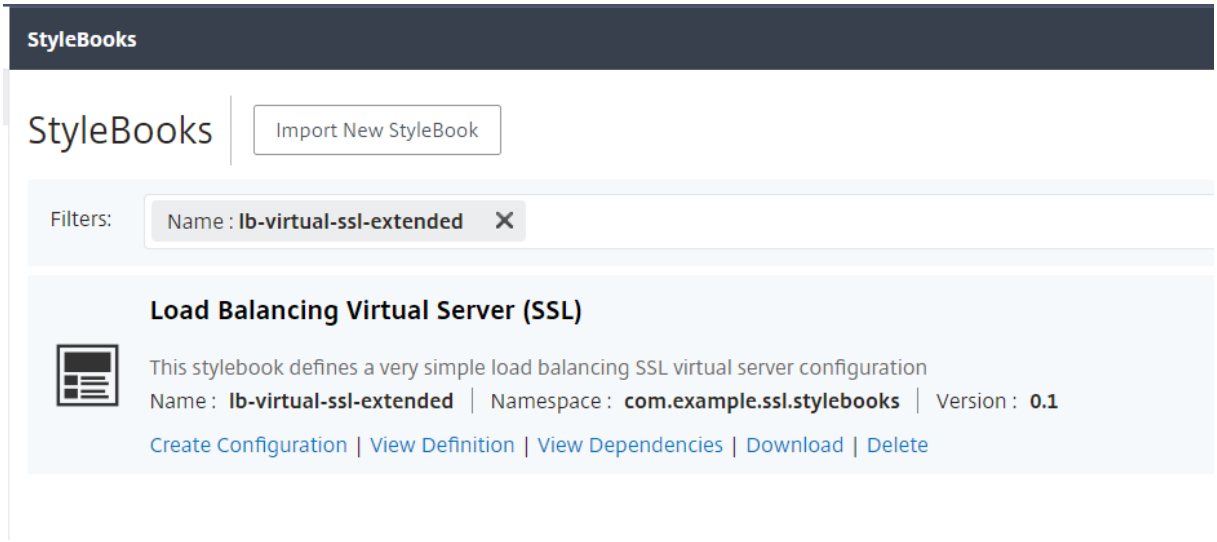
```
DELETE

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
    VERSION>/<NAME>?dependencies=true
<!--NeedCopy-->
```

Wenn der Abfrageparameter für Abhängigkeiten in der URL nicht bereitgestellt wird oder sein Wert auf false gesetzt ist, werden die StyleBook-Abhängigkeiten nicht gelöscht (nur das StyleBook selbst wird gelöscht).

Wenn Sie einen HTTP-Antwortstatuscode von 200 erhalten, bedeutet dies, dass das benutzerdefinierte StyleBook (und seine Abhängigkeiten) erfolgreich aus Citrix ADM entfernt wurde.

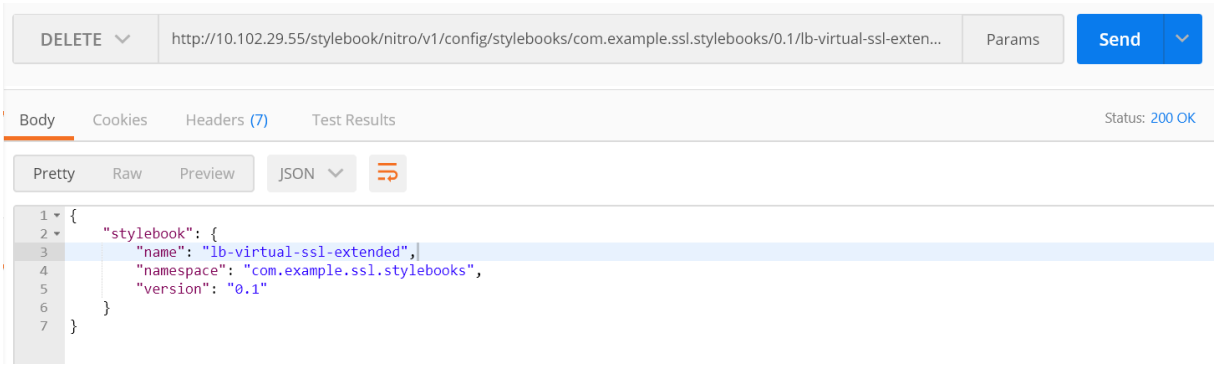
> **Hinweis:**
>
> Sie können kein benutzerdefiniertes StyleBook löschen, das andere StyleBooks in MA Service enthält, die davon abhängen.

Angenommen, Sie haben ein StyleBook mit dem Namen lb-virtual-ssl-extended in Citrix ADM erstellt. Sie haben sich später entschieden, dieses StyleBook zu löschen.

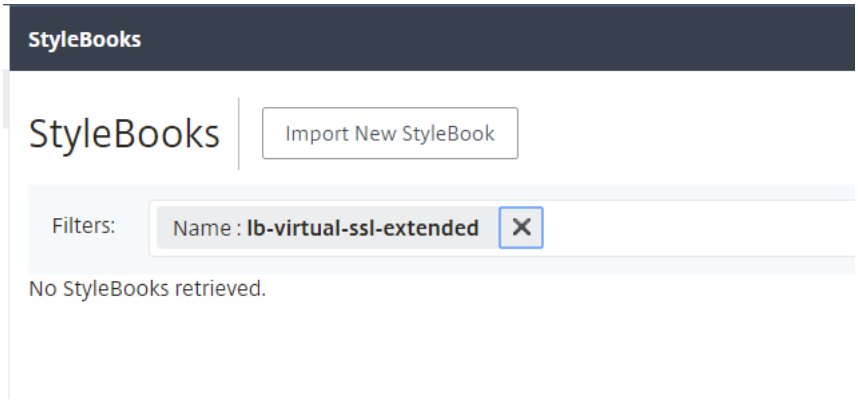


Sie können die API in jedem Tool wie dem curl-Befehlszeilentool oder der Postman Chrome-Browsererweiterung ausführen, nachdem Sie Änderungen an den Feldern IP-Adresse, Name, Version und Namespace vorgenommen haben.

LÖSCHEN https://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=false



Das StyleBook wird aus NetScaler ADM gelöscht.



StyleBooks Grammatik

February 5, 2024

Sie können Ihre eigenen StyleBooks entwerfen, sie in Citrix Application Delivery Management (ADM) importieren und anschließend Konfigurationen mithilfe von Citrix ADM GUI oder mithilfe von APIs erstellen. Um eigene StyleBooks erstellen zu können, müssen Sie zunächst die Grammatik und Syntax der verschiedenen Konstrukte und Attribute verstehen, die Sie verwenden können.

Dieses Dokument beschreibt die verschiedenen Konstrukte und Referenzen, die Sie beim Erstellen von StyleBooks verwenden können.

Klicken Sie in der Tabelle unten auf einen Abschnitt, eine Konstruktion oder einen Referenznamen, um die Details anzuzeigen.

[Header](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/header-section.html)	[StyleBooks importieren](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/import-stylebooks-section.html)
[Parameters](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parameters-section.html)	[Parameters-Default-Sources-Konstrukt](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parameters-default-sources-construct.html)
[Substitutions](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/substitutions.html)	[Components](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/components.html)
[Optionale Eigenschaften](/de-de/netscaler-application-delivery-management-software/13/stylebooks/styleboo grammar/optional-properties.html)	[Hilfskomponenten](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/helper-components.html)
[Eigenschaften, Standardquellen](/de-de/netscaler-application-delivery-management-software/13/stylebooks/s grammar/properties-default-sources.html)	[Verschachtelte Komponenten](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/nested-components.html)
[Konditionskonstrukt](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/condition-construct.html)	[Konstrukt wiederholen](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/repeat-construct.html)
[Konstrukt für Wiederholungsbedingung](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/repeat-condition-construct.html)	[Outputs](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/outputs.html)

[Verschachtelte Wiederholungen](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/nested-repeats.html)	[Übergeordnete Referenz](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parent-reference.html)
[Parameterreferenz](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parameter-reference.html)	[Substitutionsreferenz](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/substitutions-reference.html)
[Komponentenreferenz](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/components-reference.html)	[Operations](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/operations.html)
[Variablenreferenz](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/variable-reference.html)	[Alarms](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/alarms.html)
[Analytics](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/analytics.html)	[Integrierte Funktionen](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/built-in-functions.html)
[Expressions](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/expressions.html)	[Abhängigkeitserkennung](/de-de/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/dependency-detection.html)
Interpolationen vor Ort

> **Hinweis**
>
> Verwenden Sie bei der Definition von Wiederholungselementen, Wiederholungsindizes oder Argumenten für Substitutionsfunktionen nicht die folgenden reservierten Wörter, um eine benutzerdefinierte Variable zu benennen, `$<var-name>`
>
> - Stylebook, Parameter, Substitutionen, Komponenten, Eigenschaften, Ausgaben, Parent, Selbst, Operationen, Analytik, Alarme
> - repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
> - repeat-index, repeat-index-0, repeat-index-1, repeat-index-2
> - Standard
> - Rollen, Rolle, Ziele, Ziel
> - context, parent-context, parent_context

Informationen und Beispiele zum Entwerfen eigener StyleBooks finden Sie unter How to Create Your Own StyleBooks.

Header

February 5, 2024

Die ersten sechs Zeilen eines StyleBook bilden den Header-Bereich. In diesem Abschnitt können Sie die Identität eines StyleBooks definieren und beschreiben, was es tut. Dies ist ein obligatorischer Abschnitt.

In der folgenden Tabelle werden die Attribute des Header-Abschnitts beschrieben:

|Attribut| Beschreibung|
—	—
name	Ein Name zur Identifizierung des StyleBook. Dieses Attribut ist obligatorisch.
Anzeigename	Ein beschreibender Name für das StyleBook. Dieser Name wird auf der NetScaler ADM GUI angezeigt. Dies ist ein optionales Attribut.
Beschreibung	Ein Beschreibungstext definiert, was dieses StyleBook tut. Diese Beschreibung wird auf der ADM-GUI angezeigt. Dies ist ein optionales Attribut. **Hinweis:** Dies ist ein HTML-Fragment und Sie können HTML-Tags verwenden, um Überschriften anzupassen oder Bilder mithilfe des Tags <img> mit URLs oder eingebetteten Bildern einzufügen.
Autor	Der Autor, die Person oder Organisation, die das StyleBook erstellt. Dies ist ein optionales Attribut.
Namespace	Ein Namespace ist Teil einer eindeutigen Kennung für ein StyleBook, um Namenskollisionen zu vermeiden. Ein Namespace kann eine beliebige Zeichenfolge sein. Es empfiehlt sich jedoch, ihn für die Benennung des Unternehmens, der Abteilung oder der Einheit zu verwenden, die eine Reihe von StyleBooks erstellt hat oder besitzt. Beispielsweise, Sie können das folgende Format verwenden: <company>.<department>.<unit>.stylebooks. Dies ist ein obligatorisches Attribut.
version	Die Versionsnummer des StyleBook. Sie können die Versionsnummer ändern, wenn Sie ein StyleBook aktualisieren. StyleBooks verschiedener Versionen können zusammen existieren. Dies ist ein obligatorisches Attribut.
Schemaversion	Die Version des StyleBooks-Schemas. Es nimmt den Wert ”1.0” in der aktuellen Version von NetScaler ADM an. Dies ist ein obligatorisches Attribut.
Privat	Wenn dieses Attribut auf true gesetzt ist, wird das StyleBook nicht auf der NetScaler ADM GUI angezeigt. Dies ist eine nützliche Einstellung für StyleBooks, die Bausteine für andere StyleBooks sind und nicht für die direkte Verwendung durch Benutzer gedacht sind. Dies ist ein optionales Attribut. Der Standardwert ist false.

Beispiel:

```
1      name: lb
2      description: "This stylebook defines a sample load balancing
      configuration."
3      display-name: "Load Balancing StyleBook (HTTP)"
4      author: Mike Smith (ACME Infra team)
5      namespace: com.example.stylebooks
6      schema-version: "1.0"
7      version: "0.1"
```



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

Die Kombination aus Name, Namespace und Version identifiziert ein StyleBook im System eindeutig. Sie können nicht zwei StyleBooks mit derselben Kombination aus Name, Namespace und Version in NetScaler ADM haben. Sie können jedoch zwei StyleBooks mit demselben Namen und derselben Version, aber unterschiedlichen Namespaces oder mit demselben Namespace und derselben Version, aber unterschiedlichen Namen haben.

StyleBooks importieren

February 5, 2024

Dies ist der zweite Abschnitt Ihres StyleBook und ermöglicht es Ihnen, von Ihrem aktuellen StyleBook aus zu deklarieren, auf welches andere StyleBook Sie verweisen möchten. Auf diese Weise können Sie andere StyleBooks importieren und wiederverwenden, anstatt dieselbe Konfiguration in Ihrem eigenen StyleBook neu zu erstellen. Dies ist ein obligatorischer Abschnitt.

Sie müssen den **Namespace** und die **Versionsnummer** der StyleBooks deklarieren, auf die Sie in Ihrem aktuellen StyleBook verweisen möchten. Jedes StyleBook muss auf den Namespace netscaler.nitro.config verweisen, wenn es eines der NITRO-Konfigurationsobjekte direkt verwendet. Dieser Namespace enthält alle Citrix ADC NITRO -Typen, wie lbvserver Dienst oder Monitor. StyleBooks für NetScaler ADC Versionen 10.5 und höher werden unterstützt. Das bedeutet, dass Sie mit Ihrem StyleBook Konfigurationen auf jeder NetScaler ADC-Instanz erstellen und ausführen können, auf der Version 10.5 oder höher ausgeführt wird.

Das **Präfix-Attribut**, das im Abschnitt import-stylebooks verwendet wird, ist eine Abkürzung für die Kombination aus Namespace und Version. Das Präfix „ns“kann beispielsweise verwendet werden, um auf den Namespace netscaler.nitro.config mit Version 10.5 zu verweisen. In den späteren Abschnitten Ihres StyleBook können Sie einfach die Präfixzeichenfolge verwenden, die zusammen mit dem Namen des StyleBooks ausgewählt wurde, um es eindeutig zu identifizieren, anstatt jedes Mal, wenn Sie auf ein StyleBook mit diesem Namespace und dieser Version verweisen möchten, den Namespace und die Version zu verwenden.

Beispiel:

```
      import-stylebooks:
       -
         namespace: netscaler.nitro.config
         version: "10.5"
         prefix: ns
      -
       namespace: com.acme.stylebooks
        version: "0.1"
```



```
        prefix: stlb
<!--NeedCopy-->
```

Im obigen Beispiel heißt das erste definierte Präfix ns und bezieht sich auf den Namespace netscaler.nitro.config und Version 10.5. Das zweite definierte Präfix heißt stlb und bezieht sich auf den Namespace com.acme.stylebooks und Version 0.1.

Nachdem Sie ein Präfix definiert haben, können Sie jedes Mal, wenn Sie auf einen Typ oder ein StyleBook verweisen möchten, das zu einem bestimmten Namespace und einer bestimmten Version gehört, die Notation verwenden::.<namespace-shorthand><type-name> Beispielsweise bezieht sich **ns: :lbvserver auf den Typ lbvserver**, der im Namespace netscaler.nitro.config, Version 10.5, definiert ist.

Wenn Sie im Namespace com.acme.stylebooks auf ein StyleBook mit der Version "0.1"verweisen möchten, können Sie die Notation **stlb::<stylebook-name>** verwenden.

> **Hinweis**
>
> Konventionsgemäß wird das Präfix ns verwendet, um auf den NITRO-Namespace von Citrix ADC zu verweisen.

Parameter

February 5, 2024

In diesem Abschnitt können Sie alle Parameter definieren, die Sie in Ihrem StyleBook benötigen, um eine Konfiguration zu erstellen. Es beschreibt die Eingabe, die Ihr StyleBook nimmt. Obwohl dieser Abschnitt optional ist, benötigen die meisten StyleBook möglicherweise einen. Sie können den Abschnitt Parameter in Betracht ziehen, um die Felder für die Benutzer zu definieren, die das StyleBook zum Erstellen einer Konfiguration auf einer NetScaler ADC-Instanz verwenden.

Wenn Sie Ihr StyleBook in NetScaler ADM importieren und zum Erstellen einer Konfiguration verwenden, verwendet die GUI diesen Abschnitt des StyleBook, um ein Formular anzuzeigen. Dieses Formular nimmt eine Eingabe für die definierten Parameterwerte an.

Im folgenden Abschnitt werden die Attribute beschrieben, die Sie für jeden Parameter in diesem Abschnitt angeben müssen:

'**name**'

Der Name des Parameters, den Sie definieren möchten. Sie können einen alphanumerischen Namen angeben.

Der Name muss mit einem Alphabet beginnen und kann mehr Alphabete, Zahlen, Bindestriche (-) oder Unterstriche (_) enthalten.

Wenn Sie ein StyleBook schreiben, können Sie dieses Attribut “name”verwenden, um mithilfe der Notation $parameters auf den Parameter in anderen Abschnitten zu verweisen. <name>.

Obligatorisch? Ja

‘label’

Eine Zeichenfolge, die in der ADM-GUI als Name dieses Parameters angezeigt wird.

Obligatorisch? Nein

‘description’

Eine Hilfe-Zeichenfolge, die beschreibt, wofür der Parameter verwendet wird. Die ADM-GUI zeigt diesen Text an, wenn der Benutzer auf das Hilfesymbol für diesen Parameter klickt.

Obligatorisch? Nein

‘type’

Die Art des Wertes, den diese Parameter annehmen können. Parameter können von einem der folgenden integrierten Typen sein:

- string: Eine Reihe von Zeichen. Wenn keine Länge angegeben wird, kann der Zeichenfolgenwert beliebig viele Zeichen annehmen. Sie können jedoch die Länge eines String-Typs einschränken, indem Sie die Attribute min-length und max-length verwenden.
- `number`: Eine ganze Zahl. Sie können die minimale und maximale Anzahl angeben, die dieser Typ annehmen kann, indem Sie die Attribute min-value und max-value verwenden.
- **`boolean`**: Kann entweder wahr oder falsch sein. YAML betrachtet alle Literale als Boolesche (zum Beispiel Ja oder Nein).
- `ipaddress`: Eine Zeichenfolge, die eine gültige IPv4- oder IPv6-Adresse darstellt.
- `tcp-port`: Eine Zahl zwischen 0 und 65535, die einen TCP- oder UDP-Port repräsentiert.
- `password`: Repräsentiert einen undurchsichtigen/geheimen String-Wert. Wenn die ADM-GUI einen Wert für diesen Parameter anzeigt, wird sie als Sternchen (*****) angezeigt.
- `certfile`: Repräsentiert eine Zertifikatdatei. Mit diesem Wert können Sie die Dateien direkt von Ihrem lokalen System hochladen, wenn Sie eine StyleBook-Konfiguration mit der ADM-GUI

erstellen. Die hochgeladene Zertifikatsdatei wird im Verzeichnis `/var/mps/tenants/\<tenant_path>/ns_ssl_certs` in ADM gespeichert.

Die Zertifikatsdatei wird der Liste der von ADM verwalteten Zertifikate hinzugefügt.

- `keyfile`: Repräsentiert eine Zertifikatschlüsseldatei. Mit diesem Wert können Sie die Datei direkt von Ihrem lokalen System hochladen, wenn Sie eine StyleBook-Konfiguration mit der ADM-GUI erstellen. Die hochgeladene Zertifikatsdatei wird im Verzeichnis `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` in ADM gespeichert.

  Die Zertifikatschlüsseldatei wird zur Liste der von ADM verwalteten Zertifikatschlüssel hinzugefügt.

- `file`: Repräsentiert eine Datei.
- `object`: Dieser Typ wird verwendet, wenn Sie mehrere verwandte Parameter unter einem übergeordneten Element gruppieren möchten. Geben Sie den übergeordneten Parameter den Typ als “Objekt”an. Ein Parameter vom Typ “object”kann einen verschachtelten Abschnitt “parameter”haben, um die darin enthaltenen Parameter zu beschreiben.
- `another StyleBook`: Wenn Sie diesen Parametertyp verwenden, erwartet dieser Parameter, dass sein Wert in Form der Parameter vorliegt, die im StyleBook definiert sind und seinen Typ angibt.

Ein Parameter kann auch eine `type` die Liste der Typen haben. Fügen Sie dazu `[]` am Ende des Typs hinzu. Wenn das `type` Attribut beispielsweise lautet `string[]`, verwendet dieser Parameter eine Liste von Strings als Eingabe. Sie können eine, zwei oder mehrere Strings für diesen Parameter angeben, wenn Sie eine Konfiguration aus diesem StyleBook erstellen.

Obligatorisch? Ja

‘network’

Für können Sie das `network` Attribut angeben `type: ipaddress`, um eine IP-Adresse automatisch aus einem ADM IPAM-Netzwerk zuzuweisen.

ADM weist automatisch eine IP-Adresse aus dem `network`Attribut zu, wenn Sie eine StyleBook-Konfiguration erstellen.

Beispiel:

```
        name: virtual-ip
        label: "Load Balancer IP Address"
        type: ipaddress
        network: "network-1"
        required: true
<!--NeedCopy-->
```


In diesem Beispiel weist das `virtual-ip`Feld automatisch eine IP-Adresse aus. `network-1`Die IP-Adresse wird wieder an das Netzwerk freigegeben, wenn die Konfiguration gelöscht wird.

‘dynamic-allocation’

Das `dynamic-allocation` Attribut wird in der Parameterdefinition von hinzugefügt `type: ipaddress`. Verwenden Sie dieses Attribut, um die ADM IPAM-Netzwerke dynamisch aufzulisten. Dieses Attribut kann entweder **`true`** oder **`false`** als Eingabe verwendet werden. Geben Sie für das `dynamic-allocation: true` Attribut an `type: ipaddress`, um die ADM IPAM-Netzwerke, die sich in ADM befinden, dynamisch aufzulisten. Im Formular zur Erstellung von Konfigurationspakets können Sie Folgendes tun:

1. Wählen Sie das erforderliche IPAM-Netzwerk aus der Liste aus.
2. Geben Sie eine IP-Adresse an, die Sie aus dem ausgewählten IPAM-Netzwerk zuweisen möchten.

   Wenn keine IP-Adresse angegeben ist, weist der ADM automatisch eine IP-Adresse aus dem ausgewählten IPAM-Netzwerk zu.

Beispiel:

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

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

‘key’

Geben Sie true oder false an, um anzugeben, ob dieser Parameter ein Schlüsselparameter für das StyleBook ist.

In einem StyleBook kann nur ein Parameter als “key”-Parameter definiert sein.

Wenn Sie verschiedene Konfigurationen aus demselben StyleBook erstellen (auf denselben oder verschiedenen ADC-Instanzen), hat jede Konfiguration einen anderen/eindeutigen Wert für diesen Parameter.

Der Standardwert ist falsch.

Obligatorisch? Nein

‘required’

Geben Sie true oder false an, um anzugeben, ob ein Parameter obligatorisch oder optional ist. Wenn es auf true
gesetzt ist, ist der Parameter obligatorisch und der Benutzer muss beim Erstellen von Konfigurationen einen Wert für diesen
Parameter angeben.

Die ADM-GUI zwingt den Benutzer, einen gültigen Wert für diesen Parameter anzugeben.

Der Standardwert ist false.

Obligatorisch? Nein

‘allowed-values’

Verwenden Sie dieses Attribut, um eine Liste gültiger Werte für einen Parameter zu definieren, wenn der Typ auf string gesetzt ist.

Beim Erstellen einer Konfiguration über die ADM-GUI wird der Benutzer aufgefordert, einen Parameterwert aus dieser Liste auszuwählen.

> **Hinweis**
>
> Wenn Sie die Listenwerte als Radiooptionen anzeigen möchten, legen Sie das Attribut `layout` fest.

Beispiel 1:

```
-
      name: ipaddress
      type: string
      allowed-values:
            -  SOURCEIP
            -  DEST IP
            -  NONE
<!--NeedCopy-->
```

Beispiel 2:

```
-
      name: TCP Port
      type: tcp-port
      allowed-values:
            -  80
            -  81
```



```
7                 -  8080
8  <!--NeedCopy-->
```

Beispiel 3:

Liste von `tcp-ports`, in der jedes Element der Liste nur Werte in angegeben haben kann `allowed-values`.

```
1  -
2        name: tcpports
3        type: tcp-port[]
4        allowed-values:
5              -  80
6              -  81
7              -  8080
8              -  8081
9  <!--NeedCopy-->
```

Obligatorisch? Nein

‘default’

Verwenden Sie dieses Attribut, um einem optionalen Parameter einen Standardwert zuzuweisen. Wenn ein Benutzer eine Konfiguration erstellt, ohne einen Wert anzugeben, wird der Standardwert verwendet.

Der Parameter nimmt keinen Wert an, wenn die folgenden Bedingungen erfüllt sind:

- Der Parameter hat keinen Standardwert.
- Ein Benutzer gibt keinen Wert für den Parameter an.

Beispiel 1:

```
1  -
2        name: timeout
3        type: number
4        default: 20
5  <!--NeedCopy-->
```

Beispiel 2:

So listen Sie die Standardwerte des Parameters auf:

```
1  -
2        name: protocols
3        type: string[]
4        default:
5              -  TCP
6              -  UDP
7              -  IP
```



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

Beispiel 3:

```
-
      name: timeout
      type: number
      default: 20
<!--NeedCopy-->
```

Beispiel 4:

```
-
      name: tcpport
      type: tcp-port
      default: 20
<!--NeedCopy-->
```

Obligatorisch? Nein

‘pattern’

Verwenden Sie dieses Attribut, um ein Muster (regulärer Ausdruck) für die gültigen Werte dieses Parameters zu definieren, wenn der Typ des Parameters string ist.

Beispiel:

```
-
      name: appname
      type: string
      pattern: "[a-z]+"
<!--NeedCopy-->
```

Obligatorisch? Nein

‘min-value’

Verwenden Sie dieses Attribut, um den Mindestwert für Parameter vom Typ `number` oder `tcp-port` zu definieren.

Beispiel:

```
-
      name: audio-port
      type: tcp-port
      min-value: 5000
<!--NeedCopy-->
```


`min-value` für Zahlen kann negativ sein. `min-value` für `tcp-port` muss jedoch positiv sein.

Obligatorisch? Nein

‘max-value’

Verwenden Sie dieses Attribut, um den Höchstwert für Parameter vom Typ `number` oder zu definieren `tcp-port`.

Stellen Sie sicher, dass der Maximalwert größer als der Mindestwert ist, falls definiert.

Beispiel:

```
-
      name: audio-port
      type: tcp-port
      min-value: 5000
      max-value: 15000
<!--NeedCopy-->
```

Obligatorisch? Nein

‘min-length’

Verwenden Sie dieses Attribut, um die Mindestlänge der Werte zu definieren, die für einen Parameter vom
Typ “string”akzeptiert werden.

Stellen Sie sicher, dass die Mindestlänge der Zeichen definiert ist, die größer oder gleich Null sind.

Beispiel:

```
-
      name: appname
      type: string
      min-length: 3
<!--NeedCopy-->
```

Obligatorisch? Nein

‘max-length’

Verwenden Sie dieses Attribut, um die maximale Länge der Werte zu definieren, die für einen Parameter vom
Typ “string”akzeptiert werden.

Stellen Sie sicher, dass die maximale Länge der Werte größer oder gleich der Länge der in definierten Zeichen ist `min-length`.

Beispiel:

```
-
      name: appname
      type: string
      max-length: 64
<!--NeedCopy-->
```

Obligatorisch? Nein

‘min-items’

Verwenden Sie dieses Attribut, um die Mindestanzahl von Elementen in einem Parameter zu definieren, der eine Liste ist.

Stellen Sie sicher, dass die Mindestanzahl von Elementen größer oder gleich Null ist.

Beispiel:

```
-
      name: server-ips
      type: ipaddress[]
      min-items: 2
<!--NeedCopy-->
```

Obligatorisch? Nein

‘max-items’

Verwenden Sie dieses Attribut, um die maximale Anzahl von Elementen in einem Parameter zu definieren,
der eine Liste ist.

Stellen Sie sicher, dass die maximale Anzahl von Artikeln größer ist als die Mindestanzahl von Elementen, falls definiert.

Beispiel:

```
-
      name: server-ips
      type: ipaddress[]
      min-items: 2
      max-items: 250
<!--NeedCopy-->
```

Obligatorisch? Nein

‘gui’

Verwenden Sie dieses Attribut, um das Layout des Parameters in der ADM-GUI anzupassen.

Obligatorisch? Nein

‘columns’

Dieses Attribut ist ein Unterattribut des Attributs `gui`. Verwenden Sie dieses Attribut, um die Anzahl der Spalten zu definieren, die die `type: object[]` Parameter in der ADM-GUI anzeigen.

Obligatorisch? Nein

‘updatable’

Dieses Attribut ist ein Unterattribut des Attributs `gui`. Verwenden Sie dieses Attribut, um anzugeben, ob der Parameter nach dem Erstellen der Konfiguration aktualisiert werden kann. Legen Sie dieses Attribut nur für einfache Parametertypen wie String, Boolesch oder Zahl fest.

Wenn der Wert auf festgelegt ist **`false`**, ist das Parameterfeld beim Aktualisieren der Konfiguration abgeblendet.

Obligatorisch? Nein

‘collapse_pane’

Dieses Attribut ist ein Unterattribut des `gui` Attributs. Verwenden Sie dieses Attribut, um anzugeben, ob der Bereich, der das Layout dieses Objektparameters definiert, zusammenlegbar ist.

Wenn der Wert auf true gesetzt ist, kann der Benutzer die untergeordneten Parameter unter diesem übergeordneten Parameter erweitern oder reduzieren.

Beispiel:

```
gui:

 collapse_pane: true

 columns: 2
<!--NeedCopy-->
```

Beispiel für einen vollständigen Parameterabschnitt:

```
parameters:

   -
```



```
4
5        name: name
6
7        label: Name
8
9        description: Name of the application
10
11       type: string
12
13       required: true
14
15    -
16
17       name: ip
18
19       label: IP Address
20
21       description: The virtual IP address used for this application
22
23       type: ipaddress
24
25       required: true
26
27    -
28
29       name: svc-servers
30
31       label: Servers
32
33       type: object[]
34
35       required: true
36
37       parameters:
38
39         -
40
41               name: svc-ip
42
43               label: Server IP
44
45               description: The IP address of the server
46
47               type: ipaddress
48
49               required: true
50
51         -
52
53               name: svc-port
54
55               label: Server Port
56
```



```
                description: The TCP port of the server

                type: tcp-port

                default: 80

        -

                name: lb-alg

                label: LoadBalancing Algorithm

                type: string

                allowed-values:

                   - ROUNDROBIN

                   - LEASTCONNECTION

                default: ROUNDROBIN

        -

                name: enable-healthcheck

                label: Enable HealthCheck?

                type: boolean

                default: true
<!--NeedCopy-->
```

Im Folgenden finden Sie ein Beispiel, das alle Attribute einer Liste und die in früheren Abschnitten erläuterten Werte definiert:

```
        -
                name: features-list

                type: string[]

                min-length: 1

                max-length: 3

                min-items: 1

                max-items: 3

                pattern: "[A-Z]+"

                allowed-values:

```



```
                  - SP

                  - LB

                  - CS

               default:

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

‘layout’

Dieses Attribut ist ein Unterattribut des Attributs `gui`. Verwenden Sie dieses Attribut, um die Listenwerte als Optionsfelder anzuzeigen. Legen Sie das `layout` Attribut `radio` im Parameterabschnitt einer StyleBook-Definition fest. Sie gilt für den Parameter, der das Attribut `allowed-values` hat. Wenn Sie ein Konfigurationspaket erstellen, zeigt die ADM-GUI die Werte in der `allowed-values` Liste als Optionsfelder an.

Beispiel:

```
-
    gui:
        layout: radio
    allowed-values:
        - One
        - Two
        - Three
<!--NeedCopy-->
```

Die Werte Eins, Zwei und Drei werden als Optionsfelder in der ADM-GUI angezeigt.

‘dependent-parameter’

Dieses Attribut ist ein Unterattribut des Attributs `gui`. Es steuert dynamisch das Aussehen des Parameters oder seinen Anfangswert im StyleBook-Konfigurationsformular basierend auf dem in einem anderen Parameter angegebenen Wert.

Geben Sie dieses Attribut für einen Quellparameter an, der das Verhalten des Parameters im Formular steuert. Sie können mehrere Bedingungen einbeziehen, die andere Parameter steuern. Beispielsweise `protocol` kann ein Quellparameter einen dependent-Parameter haben, der nur angezeigt wird `certificate`, wenn der `protocol` Parameterwert lautet `SSL`.

Jede Bedingung kann die folgenden Attribute haben:

- **target-parameter**: Geben Sie den Zielparameter an, für den diese Bedingung gilt.

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

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

Beispiel:

```
-
   name: lb-virtual-port
   label: "Load Balanced App Virtual Port"
   description: "TCP port representing the Load Balanced application"
   type: tcp-port
   gui:
     updatable: false
     dependent-parameters:
           -
             matching-values:
               - 80
             target-parameter: $parameters.lb-service-type
             action: set-value
             allowed-values:
             - HTTP
             - TCP
             - UDP

   default: 80

<!--NeedCopy-->
```

In diesem Beispiel wird der abhängige Parameter unter dem `lb-virtual-port` Parameter (Quellparameter) angegeben.

Wenn der Quellparameterwert auf festgelegt ist `80`, löst der `lb-service-type` Parameter die `set-value` Aktion aus. Infolgedessen kann ein Benutzer eine der folgenden Optionen auswählen:

- HTTP
- TCP
- UDP

Parameters-Default-Sources-Konstrukt

February 5, 2024

Mit diesem Konstrukt können Sie Parameterdefinitionen aus anderen StyleBooks wiederverwenden.

Stellen Sie sich ein Szenario vor, in dem ein Parameter oder eine Gruppe von Parametern wiederholt in mehreren StyleBooks verwendet wird. Um eine Neudefinition dieser Parameter zu vermeiden, können Sie sie jedes Mal, wenn Sie ein neues StyleBook erstellen möchten, sie einmal definieren und dann ihre Definitionen mithilfe des Konstrukts **parameters-default-sources** in die StyleBooks importieren, die diese Parameter benötigen.

Wenn beispielsweise viele Ihrer StyleBooks eine virtuelle IP konfigurieren müssen, müssen Sie möglicherweise dieselben Parameter für virtuelle IPs in jedem neuen StyleBook definieren, das Sie erstellen. Stattdessen können Sie ein separates StyleBook mit dem Namen „vip-params“erstellen, in dem Sie alle zugehörigen Parameter definieren, wie im folgenden Beispiel gezeigt:

```
1       -
2       name: vip-params
3       namespace: com.acme.commontypes
4       version: "1.0"
5       description: This StyleBook defines a typical virtual IP config.
6       private: true
7       schema-version: "1.0"
8       parameters:
9         -
10            name: lb-appname
11            label: Load Balanced Application Name
12           description: Name of the Load Balanced application
13            type: string
14            required: true
15        -
16            name: lb-virtual-ip
17            label: Load Balanced App Virtual IP address
18            description: Virtual IP address representing the Load
      Balanced application
19            type: ipaddress
20            required: true
21        -
22            name: lb-virtual-port
23            label: Load Balanced App Virtual Port
24            description: TCP port representing the Load Balanced
      application
25            type: tcp-port
26            default: 80
27        -
28            name: lb-service-type
29            label: Load Balanced App Protocol
```



```
30            description: Protocol used for the Load Balanced application
    .
31            type: string
32            default: HTTP
33            required: true
34            allowed-values:
35                 - HTTP
36                 - SSL
37                 - TCP
38 <!--NeedCopy-->
```

Anschließend können Sie andere StyleBooks erstellen, die diese Parameter verwenden. Es folgt ein Beispiel für ein solches StyleBook.

```
1      -
2      name: acme-biz-app
3      namespace: com.acme.stylebooks
4      version: "1.0"
5      description: This stylebook defines the Citrix ADC configuration
      for Biz App
6      schema-version: "1.0"
7      import-stylebooks:
8        -
9          namespace: com.acme.commontypes
10         prefix: cmtypes
11         version: "1.0"
12     parameters-default-sources:
13           - cmtypes::vip-params
14     parameters:
15         -
16           name: monitorname
17           label: Monitor Name
18           description: Name of the monitor
19           type: string
20           required: true
21         -
22           name: type
23           label: Monitor Type
24           description: Type of the monitor
25           type: string
26           required: true
27           allowed-values:
28             - PING
29             - TCP
30             - HTTP
31             - HTTP-ECV
32             - TCP-ECV
33             - HTTP-INLINE
34 <!--NeedCopy-->
```

Im StyleBook, acme-biz-app, werden zunächst der Namespace und die Version des vip-params StyleBook mithilfe des Abschnitts „import-stylebooks“importiert. Dann wird das Konstrukt **parameters-**

default-sources hinzugefügt und der StyleBook-Name, also vip-params, angegeben. Dies hat den gleichen Effekt wie die Definition der Parameter des vip-params StyleBook direkt in diesem StyleBook.

Sie können Parameter aus mehreren StyleBooks einbeziehen, da es sich bei den parameters-default-sources um eine Liste handelt und bei jedem Element in der Liste erwartet wird, dass es sich um ein StyleBook handelt.

Sie können nicht nur Parameter aus anderen StyleBooks einbeziehen, sondern auch Ihre eigenen Parameter definieren, indem Sie den Parameterbereich verwenden. Die vollständige Liste der Parameter des StyleBook ist die Kombination von Parametern aus anderen StyleBooks und Parametern, die in diesem StyleBook definiert sind. Daher bezieht sich der Ausdruck **$parameters** auf diese Kombination von Parametern.

Beachten Sie, dass, wenn ein Parameter sowohl in einem importierten StyleBook als auch im aktuellen StyleBook definiert ist, die Definition im aktuellen StyleBook die aus einem anderen StyleBook importierte Definition überschreibt. Sie können dies effektiv nutzen, indem Sie bei Bedarf einige der importierten Parameter anpassen und die übrigen importierten Parameter unverändert verwenden.

Das Konstrukt parameters-default-sources kann auch in verschachtelten Parametern verwendet werden, wie gezeigt:

```
parameters:
    -
      name: vip-details
      label: Virtual IP details
      description: Details of the Virtual IP
      type: object
      required: true
      parameters-default-sources:
              - cmtypes::vip-params
<!--NeedCopy-->
```

Dies ähnelt dem, dass die Parameter der StyleBook vip-Parameter direkt als untergeordnete Parameter des vip-details-Parameters in diesem StyleBook hinzugefügt werden.

Ersetzungen

February 5, 2024

Der Abschnitt “Ersetzungen”wird verwendet, um Kurznamen für komplexe Ausdrücke zu definieren, die im Rest des StyleBook verwendet werden können, um das Lesen des StyleBooks zu erleichtern. Sie sind auch nützlich, wenn der gleiche Ausdruck oder Wert mehrmals im StyleBook wiederholt wird, z. B. ein konstanter Wert. Wenn Sie einen Substitutionsnamen für diesen Wert verwenden, können

Sie nur den Substitutionswert aktualisieren, wenn dieser Wert geändert werden muss, anstatt ihn an jedem Speicherort im StyleBook zu aktualisieren, der möglicherweise fehleranfällig ist.

Ersetzungen werden auch zum Definieren von Zuordnungen zwischen Werten verwendet, wie in Beispielen weiter unten in diesem Dokument beschrieben.

Jede Ersetzung in der Liste besteht aus einem Schlüssel und einem Wert.Der Wert kann ein einfacher Wert, ein Ausdruck, eine Funktion oder ein Map sein.

Im folgenden Beispiel werden zwei Substitutionen definiert. Der erste ist http-port, der als Kurzschrift für 8181 verwendet werden kann. Wenn Sie eine Substitution verwenden, können Sie dies im Rest des StyleBook als **$substitutions.http-port** anstelle von 8181 verweisen.

Substitutionen:

http-Port: 8181

Auf diese Weise können Sie einen mnemonischen Namen für eine Portnummer angeben und diese Portnummer an einer Stelle im StyleBook definieren, unabhängig davon, wie oft es verwendet wird. Wenn Sie die Portnummer auf 8080 ändern möchten, können Sie sie im Substitutionsbereich ändern, und die Änderung wird überall dort wirksam, wo der mnemonische Name http-port verwendet wird. Das folgende Beispiel zeigt, wie eine Substitution in einer Komponente verwendet wird.

```
components:
 -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
          name: $parameters.name + "-lb"
          servicetype: HTTP
          ipv46: $parameters.ip
          port: \*\*$substitutions.http-port\*\*
          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Eine Substitution kann auch ein komplexer Ausdruck sein. Das folgende Beispiel zeigt, wie zwei Ersetzungen Ausdrücke verwenden.

```
substitutions:
  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS
  app-name: str("acme-") + $parameters.name + str("-app")
<!--NeedCopy-->
```

Ein Substitutionsausdruck kann auch vorhandene Substitutionsausdrücke verwenden, wie im folgenden Beispiel gezeigt.

```
substitutions:
  http-port: 8181
  app-name: str("acme-") + $parameters.name + str($substitutions.http-
    port) + str("-app")
<!--NeedCopy-->
```


Eine weitere nützliche Funktion von Substitutionen sind Karten, mit denen Sie Schlüssel zu Werten zuordnen können. Das Folgende ist ein Beispiel für eine Kartenersetzung.

```
substitutions:
    secure-port:
        true: int("443")
        false: int("80")
    secure-protocol:
        true: SSL
        false: HTTP
<!--NeedCopy-->
```

Das folgende Beispiel zeigt, wie Sie die Karten Secure-Port und Secure-Protokoll verwenden.

```
components:
 -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
          name: $parameters.name + "-lb"
          servicetype: $substitutions.secure-protocol[$parameters.is-
   secure]
          ipv46: $parameters.ip
          port: $substitutions.secure-port[$parameters.is-secure]
          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Dies bedeutet, dass, wenn der Benutzer des StyleBook den booleschen Wert true für den Parameter is-secure angibt oder das Kontrollkästchen dieses Parameters in der Citrix ADM GUI aktiviert, der servicetype-Eigenschaft dieser Komponente wird der Wert **SSL** zugewiesen und der Port Eigenschaft hat den Wert **443**zugewiesen. Wenn der Benutzer jedoch für diesen Parameter false angibt oder das entsprechende Kontrollkästchen in der Citrix ADM GUI deaktiviert, wird der servicetype-Eigenschaft der Wert **HTTP** zugewiesen und dem Port wird der Wert **80.**

Das folgende Beispiel zeigt, wie Substitutionen als Funktion verwendet werden. Eine Substitutionsfunktion kann ein oder mehrere Argumente annehmen.Argumente sollten vom einfachen Typ sein, z. B. string, number, ipaddress, boolean und andere Typen.

Substitutionen:

form-lb-name (Name): $name + „-lb“

In diesem Beispiel definieren wir eine Substitutionsfunktion form-lb-name, die ein String-Argument namens “name”nimmt **und es verwendet, um eine neue Zeichenfolge zu erstellen, die -lb an die Zeichenfolge im Namen Argument. Ein Ausdruck, der diese Substitutionsfunktion verwendet, kann wie folgt geschrieben werden:

$substitutions.form-lb-name(“my”)

die “my-lb”zurückgibt

Betrachten Sie ein anderes Beispiel:

Substitutionen:

cspol-priority (Priorität): 10100 - 100 * $priority

Die Substitution cspol-priority ist eine Funktion, die ein Argument namens Priorität nimmt und es verwendet, um einen Wert zu berechnen. Im Rest des StyleBook kann diese Substitution verwendet werden, wie im folgenden Beispiel gezeigt:

```
components:
  -
    name: cspolicy-binding-comp
    type: ns::csvserver_cspolicy_binding
    condition: not $parameters.is-default
    properties:
         name: $parameters.csvserver-name
         policyname: $components.cspolicy-comp.properties.policyname
         priority: $substitutions.cspol-priority($parameters.pool.
   priority)
<!--NeedCopy-->
```

Die Substitution kann auch aus einem Schlüssel und einem Wert bestehen. Der Wert kann ein einfacher Wert, ein Ausdruck, eine Funktion, eine Karte, eine Liste oder ein Wörterbuch sein.

Im Folgenden finden Sie ein Beispiel für eine Substitution namens slist, deren Wert eine Liste ist:

```
substitutions:
  slist:
    - a
    - b
    - c
<!--NeedCopy-->
```

Der Wert einer Substitution kann auch ein Wörterbuch von Schlüssel-Wert-Paaren sein, wie im folgenden Beispiel einer Substitution namens ‘sdict’unten zu sehen ist:

```
substitutions:
  sdict:
    a: 1
    b: 2
    c: 3
<!--NeedCopy-->
```

Sie können komplexere Attribute erstellen, indem Sie Listen und Wörterbücher kombinieren. Zum Beispiel gibt eine Substitution namens slistofdict eine Liste von Schlüssel-Wert-Paaren zurück.

```
  slistofdict:
    -
      a: $parameters.cs1.lb1.port
```



```
        b: $parameters.cs1.lb2.port
      -
        a: $parameters.cs2.lb1.port
        b: $parameters.cs2.lb2.port
<!--NeedCopy-->
```

Im folgenden Beispiel gibt eine Substitution sdictoflist jedoch ein Schlüssel-Wert-Paar zurück, wobei der Wert selbst eine andere Liste ist.

```
  sdictoflist:
    a:
      - 1
      - 2
    b:
      - 3
      - 4
<!--NeedCopy-->
```

In Komponenten können diese Substitutionen in Condition, Properties, repeat-condition Konstrukten verwendet werden.

Das folgende Beispiel einer Komponente zeigt, wie eine Substitution verwendet werden kann, wenn die Eigenschaften angegeben werden:

```
    properties:
      a: $substitutions.slist
      b: $substitutions.sdict
      c: $substitutions.slistofdict
      d: $substitutions.sdictoflist
<!--NeedCopy-->
```

Ein Anwendungsfall zum Definieren einer Substitution, deren Wert eine Liste oder ein Wörterbuch ist, ist, wenn Sie einen virtuellen Content Switching-Server und mehrere virtuelle Server für den Lastenausgleich konfigurieren. Da alle virtuellen lb-Server, die an denselben virtuellen cs Server gebunden sind, möglicherweise eine identische Konfiguration aufweisen, können Sie die Substitutionsliste und das Wörterbuch verwenden, um diese Konfiguration zu erstellen, um zu vermeiden, dass diese Konfiguration für jeden virtuellen lb-Server wiederholt wird.

Das folgende Beispiel zeigt die Ersetzung und die Komponente in den cs-lb-mon StyleBooks, um eine Konfiguration für einen virtuellen Content Switching-Server zu erstellen. Beim Konstruieren der Eigenschaften von cs-lb-mon StyleBooks legt die komplexe Substitution lb-properties die Eigenschaften der virtuellen lb Server fest, die dem virtuellen CS Server zugeordnet sind. Die Substitution lb-properties ist eine Funktion, die den Namen, den Diensttyp, die virtuelle IP-Adresse, den Port und die Server als Parameter annimmt und ein Schlüssel-Wert-Paar als Wert generiert. In der Komponente cs-pools weisen wir den Wert dieser Substitution lb-pool Parameter für jeden Pool zu.

```
substitutions:
```



```
  cs-port[]:
    true: int("80")
    false: int("443")
  lb-properties(name, servicetype, vip, port, servers):
    lb-appname: $name
    lb-service-type: $servicetype
    lb-virtual-ip: $vip
    lb-virtual-port: $port
    svc-servers: $servers
    svc-service-type: $servicetype
    monitors:
      -
        monitorname: $name
        type: PING
        interval: $parameters.monitor-interval
        interval_units: SEC
        retries: 3
components:
  -
    name: cs-pools
    type: stlb::cs-lb-mon
    description: | Updates the cs-lb-mon configuration with the
   different pools provided. Each pool with rule result in a dummy LB
   vserver, cs action, cs policy, and csvserver_cspolicy_binding
   configuration.
    condition: $parameters.server-pools
    repeat: $parameters.server-pools
    repeat-item: pool
    repeat-condition: $pool.rule
    repeat-index: ndx
    properties:
      appname: $parameters.appname + "-cs"
      cs-virtual-ip: $parameters.vip
      cs-virtual-port: $substitutions.cs-port($parameters.protocol == "
   HTTP")
      cs-service-type: $parameters.protocol
      pools:
        -
          lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP"
   , "0.0.0.0", 0, $pool.servers)
          rule: $pool.rule
          priority: $ndx + 1
<!--NeedCopy-->
```

Substitutionszuordnung:

Sie können Substitutionen erstellen, die Schlüssel Werten zuordnen. Stellen Sie sich beispielsweise ein Szenario vor, in dem Sie den Standardport (Wert) definieren möchten, der für jedes Protokoll (Schlüssel) verwendet werden soll. Schreiben Sie für diese Aufgabe wie folgt eine Substitutionszuordnung.

```
substitutions:
     port:
```



```
3           HTTP: 80
4           DNS: 53
5           SSL: 443
6  <!--NeedCopy-->
```

In diesem Beispiel wird HTTP auf 80, DNS auf 53 und SSL auf 443 abgebildet. Um den Port eines bestimmten Protokolls abzurufen, der als Parameter angegeben ist, verwenden Sie den Ausdruck

$substitutions.port [$parameters.protocol]

Der Ausdruck gibt einen Wert zurück, der auf dem vom Benutzer angegebenen Protokoll basiert.

- Wenn der Schlüssel HTTP ist, gibt der Ausdruck 80 zurück.
- Wenn der Schlüssel DNS ist, gibt der Ausdruck 53 zurück
- Wenn der Schlüssel SSL ist, gibt der Ausdruck 443 zurück
- Wenn der Schlüssel nicht in der Karte vorhanden ist, gibt der Ausdruck keinen Wert zurück

Komponenten

February 5, 2024

Das Komponenten-Konstrukt in einem StyleBook wird als der wichtigste Abschnitt im StyleBook angesehen. In diesem Abschnitt definieren Sie die Konfigurationsobjekte, die erstellt werden müssen. Mit diesem Konstrukt können Sie ein oder mehrere Konfigurationsobjekte desselben Typs erstellen.

Das Komponentenkonstrukt kann die im Parameterbereich bereitgestellten Eingaben verwenden, um die vom StyleBook generierte Konfiguration anzupassen. Dies ist ein optionaler Abschnitt, obwohl die meisten StyleBooks einen Komponentenabschnitt haben.

In der folgenden Tabelle werden die Hauptattribute einer Komponente beschrieben.

|Attribut| Beschreibung|
—	—
name	Der Name der Komponente. Sie können einen alphanumerischen Namen angeben. Der Name muss mit einem Alphabet beginnen und kann zusätzliche Alphabete, Zahlen, Bindestriche (-) oder Unterstriche (_) enthalten.
Beschreibung	Eine Beschreibung der Rolle dieser Komponente im StyleBook.
typ	Der Typ bestimmt, welche Eigenschaften diese Komponente bietet. Komponenten haben zwei Arten von Typen: **Eingebauter Typ**: Dieser Typ wird vom System bereitgestellt und Sie müssen ihn nicht definieren, z. B. die NITRO-Entitätstypen „lbvserver“oder „servicegroup“. Wenn eine Komponente über ein integriertes Typattribut verfügt, erstellt sie ein Konfigurationsobjekt dieses Typs auf dem NetScaler ADC. Wenn sich eine Komponente beispielsweise auf den integrierten Typ ”lbvserver” bezieht, erstellt diese Komponente einen virtuellen Lastausgleichsserver auf der Citrix ADC Instanz,

der das Ziel der Konfiguration ist. **Composite-Typ**: Dieser Typ bezieht sich auf ein vorhandenes StyleBook, das Sie erstellt und in NetScaler ADM importiert haben. Wenn eine Komponente über ein zusammengesetztes Typattribut verfügt, erstellt sie alle Konfigurationsobjekte, die im referenzierten StyleBook angegeben sind, auf der NetScaler ADC-Instanz, die das Ziel der Konfiguration ist. Auf diese Weise können Sie mehrere StyleBooks kombinieren, in denen jedes StyleBook einen Teil der endgültigen Konfiguration erstellt. Weitere Informationen zu zusammengesetzten StyleBooks finden Sie unter [Erstellen eines zusammengesetzten StyleBook](/de-de/netscaler-application-delivery-management-software/13/stylebooks/how-to-create-custom-stylebooks).|
| properties|Die Unterattribute, die für ein Komponententypattribut verwendet werden können. Die Eigenschaften, die für eine Komponente gültig sind, werden durch ihren Typ bestimmt. Für einen eingebauten Typ sind dies die Eigenschaften oder Attribute des entsprechenden Nitro-Objekts. Für eine Komponente, deren Typ ein anderes StyleBook ist, d. h. ein zusammengesetzter Typ, entsprechen die Eigenschaften den in diesem StyleBook definierten Parametern.|
|

Beispiel:

```
components:
   -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
         name: $parameters.name
         servicetype: HTTP
         ipv46: $parameters.ip
         port: 80
         lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

In diesem Beispiel haben Sie eine Komponente namens my-lbvserver-comp definiert. Diese Komponente ist vom Typ ns: :lbvserver (ein integrierter Typ), wobei „ns“das Präfix ist, das sich auf den Namespace netscaler.nitro.config und Version 10.5 bezieht, die Sie im Abschnitt Import-Stylebooks angegeben haben, und „lbvserver“eine NITRO-Ressource in diesem Namespace ist.

Die Eigenschaften in diesem Abschnitt beinhalten vier obligatorische und ein optionales Attribut (lbmethod) der Ressource „lbvserver“und ermöglichen es Ihnen, Werte für diese Attribute anzugeben. In diesem Beispiel geben Sie statische Werte für servicetype und port an, während die Eigenschaften name, ipv46 und lbmethod ire Werte aus den Eingabeparametern abrufen. Sie beziehen sich auf die im Abschnitt “Parameter”definierten Parameternamen, indem Sie die $parameters.<name> verwenden, zum Beispiel $parameters.ip.

> **Hinweis**
>
> Sie müssen Kleinbuchstaben für die Attributnamen von NITRO-Ressourcentypen (deren Komponenteneigenschaften) verwenden. Andernfalls schlägt der Import eines StyleBook fehl.

Hilfskomponenten

February 5, 2024

Der Abschnitt „Komponenten“in einem StyleBook wird hauptsächlich zum Generieren von Konfigurationsobjekten mithilfe der integrierten Nitro-Typen oder eines anderen StyleBook verwendet, das die eigentlichen Konfigurationsobjekte erstellt. Die Hilfskomponenten erstellen Konfigurationsobjekte nicht selbst. Hilfskomponenten übernehmen die Eingaben aus anderen Abschnitten wie Parameterobjekten, Eigenschaften anderer Komponenten oder Ausgaben anderer Komponenten und wandeln sie in andere Formen um. Dies kann später von anderen Komponenten verwendet werden, um die eigentlichen Konfigurationsobjekte zu generieren. Eine Hilfskomponente kann von zwei Typen sein: Objekttyp oder ein anderes StyleBook, das keinen Komponentenabschnitt enthält.

Das folgende Beispiel zeigt einen Ausschnitt eines StyleBook, mit dem ein Lastausgleichsserver mit Monitor (lb-mon-comp) auf einer Citrix ADC Instanz erstellt wird.

```
parameters:
  -
    name: appname
    type: string
  -
    name: ips
    type: ipaddress[]
  -
    name: vip
    type: ipaddress

components:
  -
    name: help-comp
    type: cmtypes::server-ip-port-params
    repeat:
      repeat-list: $parameters.ips
      repeat-item: server-ip
    properties:
      ip: $server-ip
      port: 80
 -
    name: lb-mon-comp
    type: stlb::lb-mon
    properties:
      lb-appname: $parameters.appname
      lb-virtual-ip: $parameters.vip
      lb-virtual-port: 80
      lb-service-type: HTTP
      svc-service-type: HTTP
      svc-servers: $components.help-comp.properties
<!--NeedCopy-->
```


Im Parameterbereich können Sie den Namen der Anwendung und die IP-Adressen der Load Balancing Server eingeben. Im Komponentenabschnitt lb-mon-comp erwartet der svc-servers-Parameter von lb-mon StyleBook eine Liste von Objekten, wobei jedes Element zwei Unterparameter hat: ip und port.

Der Parameterabschnitt dieses StyleBook akzeptiert jedoch nur die Server-IPs über $parameters.ips. Das StyleBook geht davon aus, dass alle Server auf Port 80 ausgeführt werden. Um die Load-Balancing-Konfiguration mit lb-mon StyleBook zu erstellen, müssen Sie $parameters.ips in eine Liste von Objekten umwandeln. Dies wird mit der Hilfskomponente help-comp im obigen Beispiel erreicht. Die Komponente help-comp ist vom Typ server-ip-port-params StyleBook. Dieses StyleBook hat keine Komponenten. Daher werden keine Konfigurationsobjekte erstellt. Der Help-Comp erstellt eine Wiederholungsliste über $parameters.ips und konstruiert ein Objekt, das aus IP und Port (der auf statische 80 gesetzt ist) für jedes Element von $parameters.ips besteht. Daher wandelt help-comp eine Liste von IP-Adressen in eine Liste von Objekten um, die später in lb-mon-comp verwendet werden können, um die Eigenschaft svc-servers zuzuweisen. Das Ergebnis von help-comp wird der Eigenschaft svc-servers von lb-mon-comp zugewiesen.

Optionale Eigenschaften

February 5, 2024

In einigen Fällen bezieht eine Eigenschaft einer Komponente ihren Wert aus einem Ausdruck, bei dem es sich um einen einfachen Ausdruck wie eine Parameterreferenz oder um einen komplexeren Ausdruck handeln kann. Das Festlegen dieses Eigenschaftswerts ist in der Komponente optional. Sie können den Eigenschaftswert nur festlegen, wenn der Ausdruck einen tatsächlichen Wert zurückgibt, andernfalls können Sie diese Eigenschaft nicht festlegen.

Stellen Sie sich zum Beispiel vor, dass eine der Eigenschaften, die Sie festlegen möchten, die lbmethod (Loadbalancing-Algorithmus) einer Komponente vom Typ ns: :lbvserver ist. Der Wert der Eigenschaft lbmethod wird einem vom Benutzer bereitgestellten Parameterwert entnommen, wie unten dargestellt:

```
components
  -
      name: lbvserver_comp
      type: ns::lbvserver
      properties:
        name: $parameters.lb-appname + "-lb"
        servicetype: $parameters.lb-service-type
        ipv46: $parameters.lb-virtual-ip
        port: 80
        lbmethod: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```


Betrachten Sie nun, dass der Parameter **lb-advanced.algorithm** ein optionaler Parameter ist. Wenn der Benutzer keinen Wert für diesen Parameter bereitstellt, weil er optional ist, wird der Ausdruck **$parameters.lb-advanced.algorithm** als leerer Wert ausgewertet. Daher wird ein ungültiger Wert für die Eigenschaft lbmethod übergeben. Um eine solche Situation zu vermeiden, können Sie die Eigenschaft als optional kommentieren, indem Sie ihren Namen mit ? wie folgt:

```
components
   -
     name: lbvserver_comp
     type: ns::lbvserver
     properties:
       name: $parameters.lb-appname + "-lb"
       servicetype: $parameters.lb-service-type
       ipv46: $parameters.lb-virtual-ip
       port: 80
       lbmethod?: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```

Die Verwendung von ? wird die Eigenschaft weggelassen, wenn der Ausdruck rechts zu nichts ausgewertet wird, was in diesem Fall einer Komponente gleichwertig wäre, die wie folgt definiert ist:

```
components
  -
    name: lbvserver_comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb-appname + "-lb"
      servicetype: $parameters.lb-service-type
      ipv46: $parameters.lb-virtual-ip
      port: 80
<!--NeedCopy-->
```

Da **lbmethod** optional ist, ist es dennoch eine gültige Komponente, wenn es weggelassen wird. Beachten Sie, dass lbmethod möglicherweise seinen Standardwert annimmt, wenn einer in seinem Typ “ns::lbvserver”definiert ist.

Eigenschaften-Default-Source-Konstrukt

February 5, 2024

Das Konstrukt properties-default-sources entspricht dem Konstrukt parameters-default-sources. Während das Parameter-Default-Sources-Konstrukt die Wiederverwendung vorhandener Parameter (aus anderen StyleBooks) in einem StyleBook ermöglicht, ermöglicht das Properties-Default-Sources-Konstrukt dem Benutzer, Eigenschaften einer Komponente basierend auf vorhandenen Quellen anzugeben.

Die Eigenschaften einer Komponente können auf verschiedene Abschnitte des StyleBook verteilt werden. Die Eigenschaften können beispielsweise aus Objektparametern, Substitutionen, die ein Objekt zurückgeben, Eigenschaften anderer Komponenten oder Ausgaben anderer Komponenten stammen. In solchen Fällen müssen Sie die Eigenschaften, die in anderen Abschnitten des StyleBook vorkommen, in der Definition der Komponente neu definieren. Dies ist eindeutig überflüssig und kann zu Fehlern führen. Um dieses Problem zu lösen, kann das Konstrukt properties-default-sources verwendet werden. Das Eigenschaften-default-sources-Konstrukt ist eine Liste, in der jedes Element eine Quelle für einige Eigenschaften der Komponente identifiziert.

Stellen Sie sich zum Beispiel eine Komponente vor, die eine lbvserver-Konfiguration erstellt. Diese Komponente sollte die Eigenschaften des lbvservers wie folgt definieren.

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb.name
      ipv46: $parameters.lb.ipv46
      port: $parameters.lb.port
      servicetype: $parameters.lb.servicetype
      lbmethod: $parameters.lb.lbmethod
<!--NeedCopy-->
```

Beachten Sie im obigen Beispiel, dass die Werte für alle Eigenschaften, die im Komponentenabschnitt definiert sind, aus $parameters.lb Objekt genommen werden. Obwohl sie aus einer einzigen Quelle stammen, werden die Eigenschaften im StyleBook erneut definiert. Wenn dem $parameters.lb-Objekt ein neuer Unterparameter hinzugefügt wird, der für die Konfiguration des lbvservers relevant ist, müssen Sie außerdem die lb-comp-Komponente aktualisieren, um die neue Eigenschaft hinzuzufügen, die dem neuen Unterparameter entspricht.

Um eine Neudefinition von Eigenschaften zu vermeiden und alle relevanten Eigenschaften einer Komponente abzurufen, ohne sie explizit im Eigenschaftenabschnitt aufzulisten, kann Eigenschaftendefault-sources-Konstrukt verwendet werden. Das obige Beispiel kann wie folgt geschrieben werden.

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
```



```
    properties-default-sources:
      - $parameters.lb
<!--NeedCopy-->
```

Im obigen Beispiel führt die Verwendung des Konstrukt properties-default-sources zu einer Verringerung der Größe der Komponentendefinition, sodass Sie eine Komponente präzise definieren können. Darüber hinaus werden jedes Mal, wenn sich die Quelle der Eigenschaften der Komponente ändert, die Änderungen automatisch reflektiert. Wenn zum Beispiel eine neue Eigenschaft, sagen wir „persistencetype“, zum $parameters.lb-Objekt hinzugefügt wird, wird diese Eigenschaft standardmäßig zur Konfiguration von lb-comp hinzugefügt, da persistencetype eine Eigenschaft von lbvserver ist. Somit bietet Eigenschaften-default-sources-Konstrukt eine dynamische Schnittstelle, um die Komponenten zu definieren, ohne sich Gedanken über Änderungen an den Quellen der Eigenschaften der Komponente zu machen.

Berechnung der Eigenschaften der Komponente

In diesem Abschnitt wird erläutert, wie die Eigenschaften abgerufen werden, wenn Eigenschaften-default-sources-Konstrukt in einer Komponente verwendet wird. Zunächst identifiziert der StyleBooks-Compiler die Liste der Eigenschaften für eine Komponente anhand ihres Typs (im obigen Beispiel lbvserver). Als Nächstes ruft der Compiler diese Eigenschaften aus den verschiedenen Quellen in der Reihenfolge ab, in der sie definiert sind (im Abschnitt properties-default-sources der Komponente). Wenn eine Eigenschaft in mehreren Quellen vorhanden ist, hat die Eigenschaft, die in der letzten Quelle angezeigt wird, Vorrang vor anderen. Schließlich kann eine Eigenschaft, die mit Eigenschaften-default-sources-Konstrukt abgerufen wird, im Eigenschaftenabschnitt der Komponente außer Kraft gesetzt werden. Es ist wichtig zu beachten, dass die Definition eines Komponentenabschnitts mindestens einen Abschnitt properties-default-sources oder einen Eigenschaftenabschnitt haben sollte. Es kann beides haben.

Verschachtelte Komponenten

February 5, 2024

Durch das Verschachteln einer Komponente innerhalb einer anderen Komponente kann die verschachtelte Komponente ihre Konfigurationsobjekte erstellen, indem sie auf Konfigurationsobjekte oder den von der übergeordneten Komponente erstellten Kontext verweist. Die verschachtelte Komponente kann für jedes Objekt, das in der übergeordneten Komponente erstellt wurde, ein oder mehrere Objekte erstellen. Das Verschachteln einer Komponente innerhalb einer anderen Komponente zeigt keine Beziehung zwischen den erstellten Konfigurationsobjekten an. Verschachtelung

ist eine Möglichkeit, die Aufgabe von Komponenten zu erleichtern, Konfigurationsobjekte in einem vorhandenen Kontext der übergeordneten Komponenten zu konstruieren.

Beispiel:

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
   properties:
      name: $parameters.name + "-lb"
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
      components:
        -
         name: my-svcg-comp
         type: ns::servicegroup
         properties:
            name: $parameters.name + "-svcgrp"
            servicetype: HTTP
         components:
            -
              name: lbvserver-svg-binding-comp
              type: ns::lbvserver_servicegroup_binding
              properties:
                name: $parent.parent.properties.name
                servicegroupname: $parent.properties.name
                  -
                    name: members-svcg-comp
                    type: ns::servicegroup_servicegroupmember_binding
                    repeat:
                      repeat-list: $parameters.svc-servers
                      repeat-item: srv
                    properties:
                      ip: $srv
                      port: str($parameters.svc-port)
                      servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

In diesem Beispiel wird eine mehrstufige Verschachtelung verwendet. Die Komponente my-lbvserver-comp hat eine untergeordnete Komponente namens my-svcg-comp. Und die Komponente my-svcg-comp enthält zwei untergeordnete Komponenten. Die my-svcg-comp-Komponente wird verwendet, um ein Service-Gruppen-Konfigurationsobjekt auf der Citrix ADC Instanz zu erstellen, indem Werte für die Attribute des integrierten NITRO -Ressourcentyps servicegroup bereitgestellt werden. Die erste untergeordnete Komponente der my-svcg-Komponente, lbvserver-svg-binding-comp, wird verwendet, um die von der übergeordneten Komponente erstellte Dienstgruppe an den virtuellen Lastausgleichsserver (lbvserver) zu binden, der von der übergeordneten Komponente des übergeordneten Elements erstellt wurde. Die $parent Notation, auch übergeordnete Referenz genannt, wird verwen-

det, um auf Entitäten in den übergeordneten Komponenten zu verweisen. Die zweite untergeordnete Komponente, members-svcg-comp, wird verwendet, um die Liste der Dienste an die Dienstgruppe zu binden, die von der übergeordneten Komponente erstellt wurde. Die Bindung wird erreicht, indem das Wiederholungskonstrukt von StyleBook verwendet wird, um über die Liste der Dienste zu iterieren, die für den Parameter svc-Server angegeben sind. Informationen zu Wiederholungskonstrukten finden Sie unter Repeat Construct.

Sie können auch dieselben Konfigurationsobjekte erstellen, ohne die Verschachtelung von Komponenten zu verwenden. Weitere Informationen und Beispiele finden Sie unter StyleBook to Create a Basic Load Balancing Configuration.

Konditionskonstrukt

February 5, 2024

Sie können eine Komponente bedingt machen, indem Sie ein Bedingungskonstrukt verwenden. Der Wert eines bedingten Konstrukts ist ein boolescher Ausdruck, der als wahr oder falsch ausgewertet wird. Wenn die Bedingung erfüllt ist, wird die Komponente verwendet, um ihre Konfigurationsobjekte zu erstellen. Wenn die Bedingung falsch ist, wird die Komponente übersprungen und durch sie werden keine Konfigurationsobjekte erstellt. Der boolesche Ausdruck basiert oft auf Parameterwerten.

Beispiel:

```
components:
      -
        name: servicegroup-comp
        type: ns::servicegroup
        condition: $parameters.svc-server-ips
        properties:
              name: $parameters.name + "-svcgrp"
              servicetype: HTTP
<!--NeedCopy-->
```

Wenn der Benutzer in diesem Beispiel einen Wert für den optionalen Parameter svc-server-ips angibt, wird die Komponente servicegroup-comp von der StyleBook-Engine verarbeitet. Wenn die Bedingung falsch ist, d. h. wenn der Benutzer diesem Parameter keinen Wert zuweist, wird diesem Parameter ein Nullwert zugewiesen und als falsch ausgewertet, ignoriert die StyleBook-Engine das Vorhandensein dieser Komponente und es wird keine Servicegruppe erstellt.

Beachten Sie, dass der boolesche Ausdruck auf einem beliebigen gültigen Ausdruck basieren kann, der in StyleBooks unterstützt wird (z. B. ob eine andere Komponente vorhanden ist oder ob ein Parameter einen bestimmten Wert hat).

Das folgende Beispiel erstellt das Konfigurationsobjekt des NITRO-Typs ns: :systemfile, wenn die Bedingung als wahr ausgewertet wird.

Beispiel:

```
      components
           -
             name: pem_key_files
             type: ns::systemfile
             condition: "$components.der-certificate-files-comp or
    $components.pem-certificate-files-comp"
             properties:
                    filecontent: $certificate.keyfile.contents
                    fileencoding: "BASE64"
                    filelocation: "/nsconfig/ssl"
                    filename: $certificate.keyfile.filename
<!--NeedCopy-->
```

In diesem Beispiel ist die Bedingung ein komplexer „OR“-Ausdruck, bei dem dieses Konfigurationsobjekt nur dann vom StyleBook erstellt werden soll, wenn zwei andere Komponenten im StyleBook verarbeitet (nicht übersprungen) wurden, wodurch eine Abhängigkeit zwischen den Komponenten entsteht.

Konstrukt wiederholen

February 5, 2024

Sie können das **Wiederholungskonstrukt** einer Komponente verwenden, um mehrere Konfigurationsobjekte desselben Typs zu erstellen.

Im folgenden Beispiel wird die **members-svcg-comp-Komponente** verwendet, um die Liste der Dienste an die von der übergeordneten Komponente erstellte Dienstgruppe zu binden. Um ein Konfigurationsobjekt zu erstellen, das jeden Server an die Dienstgruppe bindet, verwenden Sie das **Wiederholungskonstrukt**, um über die Liste der Dienste zu iterieren, die für den Parameter **svc-servers** angegeben ist. Während der Iteration erstellt die Komponente ein NITRO-Objekt vom Typ **servicegroup_servicegroupmember_binding** für jeden Dienst (im **Repeat-Item-Konstrukt** als **srv** bezeichnet) in der Dienstgruppe und setzt das IP-Attribut in jedem NITRO-Objekt auf die **IP-Adresse** des entsprechenden Dienstes.

Beispiel:

```
components:
  -
      name: my-lbvserver-comp
      type: ns::lbvserver
      properties:
```



```
6             name: $parameters.name + "-lb"
7             servicetype: HTTP
8             ipv46: $parameters.ip
9             port: 80
10            lbmethod: $parameters.lb-alg
11          components:
12                -
13                   name: my-svcg-comp
14                   type: ns::servicegroup
15                   properties:
16                        name: $parameters.name + "-svcgrp"
17                        servicetype: HTTP
18                  components:
19                         -
20                         name: lbvserver-svg-binding-comp
21                         type: ns::lbvserver\servicegroup\binding
22                         properties:
23                               name: $parent.parent.properties.name
24                               servicegroupname: $parent.properties.
      name
25                         -
26                         name: members-svcg-comp
27                         type: ns::servicegroup\servicegroupmember\
      binding
28                         repeat:
29                           repeat-list: $parameters.svc-servers
30                           repeat-item: srv
31                         properties:
32                                ip: $srv
33                                port: $parameters.svc-port
34                                servicegroupname: $parent.properties.
      name
35  <!--NeedCopy-->
```

Die **Wiederholung** ist ein eigenständiges Objekt, und **Wiederholungsliste und Wiederholungselementsind Attribute für das Wiederholungsobjekt** .

- repeat-list ist ein obligatorisches Attribut, das die Liste identifiziert, auf der die Komponente iteriert.
- repeat-item ist optional und wird verwendet, um dem aktuellen Element in der Iteration einen benutzerfreundlichen Namen zu geben.

Wenn nicht angegeben, kann mit dem Ausdruck **$repeat-item** auf das aktuelle Element zugegriffen werden. Die letzte Komponente im obigen Beispiel kann auch wie folgt geschrieben werden:

```
1           -
2           name: members-svcg-comp
3           type: ns::servicegroup_servicegroupmember_binding
4           repeat:
5             repeat-list: $parameters.svc-servers
6           properties:
7                  ip: $repeat-item
```



```
                port: $parameters.svc-port
                servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

Neben der Möglichkeit, auf das aktuelle Element während der Iteration über eine Liste zu verweisen, ist es auch möglich, auf den aktuellen Index des Elements in der Liste mit **repeat-index**zu verweisen. Im folgenden Beispiel wird der **Wiederholungsindex** verwendet, um eine Portnummer auf der Grundlage des aktuellen Index zu berechnen:

```
            name: services
            type: ns::service
            repeat:
               repeat-list: $parameters.app-services
               repeat-item: srv
            properties:
                ip: $parameters.app-ip
                port: $parameters.base-port + repeat-index
                servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

Ähnlich wie beim Konstrukt **repeat-item** können Sie einen anderen Variablennamen zuweisen, um auf den aktuellen Index der Iteration zu verweisen. Das vorherige Beispiel entspricht dem folgenden Beispiel:

```
    -
            name: services
            type: ns::service
            repeat:
               repeat-list: $parameters.app-services
               repeat-item: srv
               repeat-index: idx
            properties:
                ip: $parameters.app-ip
                port: $parameters.base-port + $idx
                servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

Konstrukt für Wiederholungsbedingung

February 5, 2024

Das Konstrukt mit wiederholten Bedingungen wird in jeder Iteration eines Wiederholungskonstrukts ausgewertet, und das Ergebnis bestimmt, ob das Konfigurationsobjekt in dieser Iteration erstellt oder zur nächsten Iteration übergegangen werden soll. Das folgende Beispiel zeigt die Verwendung des Wiederholungsbedingungskonstrukts:

Beispiel:


```
components
   -
      name: der-key-files-comp
      type: ns::systemfile
      repeat:
      repeat-list: $parameters.certificates
      repeat-item: certificate
        repeat-condition: $certificate.ssl-inform == DER
        properties:
         filecontent: base64($certificate.keyfile.contents)
         fileencoding: BASE64
         filelocation: /nsconfig/ssl
         filename: $certificate.keyfile.file
<!--NeedCopy-->
```

In diesem Beispiel iteriert die Komponente der-key-files-comp über alle vom Benutzer angegebenen Zertifikate, erstellt jedoch nur Konfigurationsobjekte, die Zertifikaten mit DER-Codierung entsprechen. In jeder Iteration wird der Wiederholungsbedingung Ausdruck ausgewertet, um zu testen, ob die Zertifikatkodierung vom Typ DER ist. Wenn es nicht vom Typ DER ist, wird in der aktuellen Iteration kein Konfigurationsobjekt erstellt, und die Iteration wird zum nächsten Zertifikat in der Liste verschoben.

Verschachtelte Wiederholungen

February 5, 2024

Mit dem verschachtelten Wiederholungskonstrukt können Sie je nach Definition der Komponente mehr als ein Wiederholungskonstrukt in jeder Komponente haben. Stellen Sie sich eine verschachtelte Wiederholung von zwei Ebenen vor. Für jedes Element in der äußeren Liste (erste Wiederholungsliste) können Sie eine Wiederholungsliste für alle Elemente der inneren Liste (zweite Wiederholungsliste) erstellen. Der StyleBook-Compiler unterstützt bis zu drei verschachtelte Wiederholungen. Jeder Wiederholungsebene sind die Attribute Wiederholungselement und Wiederholungsindex zugeordnet. Sowohl die Attribute repeat-item als auch repeat-index sind optional. Zusätzlich kann für jede Wiederholung auch eine Wiederholungsbedingung angegeben werden.

Beispiel:

```
parameters:
  -
      name: vips
      type: ipaddress[]
  -
      name: vip-ports
      type: tcp-port[]
components:
```



```
9    -
10       name: lbvservers-comp
11       type: ns::lbvserver
12       repeat:
13          repeat-list: $parameters.vips
14          repeat-item: ip
15          repeat:
16               repeat-list: $parameters.vip-ports
17               repeat-item: port
18       properties:
19          name: str("lb-") + str($ip) + '-' + str($port)
20          servicetype: HTTP
21          ipv46: $ip
22          port: $port
23 <!--NeedCopy-->
```

Im obigen Beispiel iterieren wir für jedes Element in $parameters.vips über alle Elemente von $parameters.vip-ports. Daher erstellen wir für jede in $parameters.vips angegebene IP-Adresse lbvserver-Konfigurationsobjekte für alle in $parameters.vip-ports angegebenen Ports. Der Eigenschaftenbereich definiert den Namen des Objekts mit „lb“als Präfix für die Kombination aus IP-Adresse und Port. Daher definiert $ip + $port für jede Iteration eine eindeutige Kombination aus der IP-Adresse und der Portnummer.

Wenn das Attribut repeat-item nicht bereitgestellt wird, generiert der Compiler einen Standardwert dafür. Die Standardwerte für repeat-item sind: $repeat-item, $repeat-item-1, $repeat-item-2 jeweils für jede Wiederholungsebene. Ebenso generiert der Compiler einen Standardwert dafür, wenn das Attribut repeat-index nicht bereitgestellt wird. Die Standardwerte für repeat-index sind: $repeat-index, $repeat-index-1 und $repeat-index-2 jeweils für jede Wiederholungsebene.

Das folgende Beispiel beschreibt die Benennungskonvention, wenn die Attribute repeat-item und repeat-index in einem verschachtelten Wiederholungsobjekt fehlen.

Beispiel:

```
1  components:
2  -
3       name: lbvservers-comp
4       type: ns::lbvserver
5       repeat:
6           repeat-list: $parameters.vips
7           repeat:
8              repeat-list: $parameters.vip-ports
9       properties:
10         name: str("lb-") + str($repeat-item) + '-' + str($repeat-item
       -1)
11          servicetype: HTTP
12          ipv46: $repeat-item
13          port: $repeat-item-1
14 <!--NeedCopy-->
```


Ausgaben

February 5, 2024

Im Abschnitt Ausgaben geben Sie an, was ein StyleBook seinen Benutzern zur Verfügung stellt, nachdem es alle Konfigurationsobjekte erfolgreich erstellt hat. Der Ausgabebereich eines StyleBook ist optional. Ein StyleBook muss keine Ausgaben zurückgeben. Durch die Rückgabe einiger interner Komponenten als Ausgaben erhalten StyleBooks, die sie importieren, jedoch mehr Flexibilität, wie Sie bei der Erstellung eines zusammengesetzten StyleBooks sehen können.

In der folgenden Tabelle werden die Attribute beschrieben, die im Abschnitt Ausgaben verwendet werden.

Attribut	Beschreibung	Erforderlich
name	Der Name der Ausgabe, die dem Konfigurationsobjekt entspricht, das Sie verfügbar machen möchten.	Ja
Beschreibung	Eine Textzeichenfolge, die die Ausgabe beschreibt.	Nein
Wert	Dieses Attribut gibt an, wie der Wert extrahiert wird, der von einem StyleBook zurückgegeben wird.	Ja

Beispiel:

```
outputs:
 -
   name: lbvserver
   description: LBVServer component
   value: $components.my-lbvserver-comp
 -
   name: svc-grp
     description: ServiceGroup name
     value: $components.my-svcg.properties.name
<!--NeedCopy-->
```

In diesem Beispiel machen Sie die **lbvserver-Komponente** und den **Servicegroup-Namen** verfügbar, die vom StyleBook erstellt würden. Der Wert der Ausgabe namens **lbvserver** ist die Komponente **my-lbvserver-comp**. Ebenso ist der Wert der Ausgabe **svc-grp** der Name der Dienstgruppe, die von der Komponente **my-svcg** erstellt wurde.

Parameterreferenz

February 5, 2024

Im Komponentenkonstrukt verweisen Sie mithilfe der Notation `$parameters.<parametername>` auf die im Parameterabschnitt definierten Parameter. Wenn `<parametername>` selbst Parameter enthält (wenn type = object ist), müssen Sie die Notation `$parameters.<parametername>.<sub-parametername>` usw. verwenden.

Beispiel:

```
parameters:
  -
    name: name
    label: Name
    type: string
    required: true
     -
      name: vip
      label: Virtual IP and Port
      type: object
      required: true
      parameters:
        -
          name: ip
          label: Virtual IP
          description: The Virtual IP Address
          type: ipaddress
          required: true
            -
              name: port
              label: The Virtual Port
              description: The TCP port for the Virtual IP
              type: tcp-port
              default: 80
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
       name: $parameters.name
       servicetype: HTTP
       ipv46: $parameters.vip.ip
       port: $parameters.vip.port
<!--NeedCopy-->
```


Übergeordnete Referenz

February 5, 2024

Wenn Sie verschachtelte Komponentenverwenden, können Sie mit der $parent Notation auf die übergeordnete Komponente verweisen. Wenn die übergeordnete Komponente mehrere Konfigurationsobjekte mit dem Wiederholungskonstrukt erstellt und untergeordnete Komponenten innerhalb jeder Iteration andere Konfigurationsobjekte erstellen, bezieht sich die $parent Notation immer auf die aktuelle Iteration der übergeordneten Komponente. Beispielsweise bezieht sich $parent.properties.name auf die Eigenschaft name des Konfigurationsobjekts, das in der aktuellen Iteration vom übergeordneten Objekt erstellt wurde.

Beispiel:

```
components:
 -
   name: my-lbvserver-comp
   type: ns::lbvserver
   properties:
     name: $parameters.name + "-lb"
     servicetype: HTTP
     ipv46: $parameters.ip
     port: 80
     lbmethod: $parameters.lb-alg
     components:
       -
         name: my-svcg-comp
         type: ns::servicegroup
         properties:
           name: $parameters.name + "-svcgrp"
           servicetype: HTTP
           components:
            -
              name: lbvserver-svg-binding-comp
              type: ns::lbvserver_servicegroup_binding
              properties:
                 name: $parent.parent.properties.name
                 servicegroupname: $parent.properties.name
                   -
                     name: members-svcg-comp
                     type: ns::servicegroup_servicegroupmember_binding
                     repeat: $parameters.svc-servers
                     repeat-item: srv
                     properties:
                       ip: $srv
                       port: str($parameters.svc-port)
                       servicegroupname: $parent.properties.name
<!--NeedCopy-->
```


Sie können auch in der Hierarchie der Komponenten nach oben navigieren, indem Sie auf die Eigenschaften der übergeordneten Elemente bis hin zu den Komponenten der obersten Ebene zugreifen. Beispielsweise bezieht der Eigenschaftsname der Komponente **lbvserver-svg-binding-comp** seinen Wert aus dem Eigenschaftsnamen der übergeordneten Komponente seiner übergeordneten Komponente, der Komponente **my-lbvserver-comp**, indem die Notation **$parent.parent** verwendet wird.

Komponentenreferenz

February 5, 2024

Im Komponentenkonstrukt verweisen Sie auf die Komponente der obersten Ebene im StyleBook, indem Sie die Notation **$components .<componentname>** verwenden. Wenn innerhalb einer Komponente der obersten Ebene verschachtelte Komponenten vorhanden sind, ist die verwendete Notation **$components.<componentname>.components.<component-name>** und so weiter.

Beispiel:

```
components:
 -
    name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
           name: $parameters.name + "-lb"
           servicetype: HTTP
           ipv46: $parameters.ip
           port: 80
           lbmethod: $parameters.lb-alg
  -
     name: my-svcg-comp
     type: ns::servicegroup
     properties:
          name: $parameters.name + "-svcgrp"
          servicetype: HTTP
 -
     name: members-svcg-comp
     type: ns::servicegroup_servicegroupmember_binding
     repeat: $parameters.svc-servers
     repeat-item: srv
     properties:
        ip: $srv
          port: str($parameters.svc-port)
          servicegroupname: $components.my-svcg-comp.properties.name
 -
     name: lbvserver-svg-binding-comp
     type: ns::lbvserver_servicegroup_binding
     properties:
```



```
            name: $components.my-lbvserver-comp.properties.name
            servicegroupname: $components.my-svcg-comp.properties.name
<!--NeedCopy-->
```

In diesem Beispiel müssen die Komponenten **my-svcg-comp** und **my-lbvserver-comp** erstellt werden, bevor die letzte Komponente **lbvserver-svg-binding-comp** erstellt wird, da in dieser letzten Komponente Verweise auf diese Komponenten vorhanden sind. Diese Referenzen werden über Komponentenreferenzen bereitgestellt, die durch **$components.<componentname>** gekennzeichnet sind.

Substitutionsreferenz

February 5, 2024

Im Abschnitt Komponenten oder Operationen verweisen Sie mithilfe der Notation **$substitutions.<substitution-name>** auf Substitutionen, die im Abschnitt Substitutionen definiert sind. Beispiel: **$substitutions.http-port**.

Wenn es sich bei einer Substitution um eine Map handelt, können Sie auf ein Element in der Map als **$substitutions.<substitutions-name>[<map-key>]** verweisen. Beispiel: **$substitutions.protocol-map[$parameters.port]**.

Variablenreferenz

February 5, 2024

Wenn Sie die Konstrukte repeat und repeat-item in Komponenten verwenden, um mehrere Konfigurationsobjekte zu erstellen, können Sie dem Repeat-Item-Konstrukt einen Variablennamen zuweisen. Diese Variable kann dann in den Eigenschaften dieser Komponente oder in untergeordneten Komponenten mithilfe der Notation **$\<varname\>** referenziert werden. Beachten Sie, dass, wenn das Wiederholungskonstrukt ohne das Repeat-Item-Konstrukt in einer Komponente verwendet wird, eine Standardvariable namens $repeat-item für den Zugriff auf die Iterationselemente verwendet werden kann.

Beispiel:

```
components:
  -
    name: server-members-comp
    type: ns::server
    condition: $parameters.svc-server-domain-names
```



```
6       repeat: $parameters.svc-server-domain-names
7       repeat-item: server-name
8       properties:
9         name: $server-name + "-server"
10        domain: $server-name
11      components:
12        -
13           name: service-members-comp
14           type: ns::service
15           properties:
16             name: $server-name + "-service"
17             servername: $parent.properties.name
18             servicetype: $parameters.svc-service-type
19             port: $parameters.svc-server-port
20  <!--NeedCopy-->
```

Im obigen Beispiel wird dem Repeat-Item-Konstrukt ein Variablenname, Servername, zugewiesen. Auf diesen Variablennamen wird sowohl in den Eigenschaften derselben Komponente als auch in den untergeordneten Komponenten **$\<varname\>** verwiesen.

Operationen

February 5, 2024

Operationen sind ein optionaler Abschnitt in einem StyleBook. In diesem Abschnitt können Sie Citrix Application Delivery Management (ADM) Analytics so konfigurieren, dass AppFlow Datensätze für alle oder einige der Traffic-Transaktionen erfasst werden. Der virtuelle Server, der auf einer NetScaler ADC-Instanz mithilfe des StyleBook erstellt wurde, verarbeitet diese Verkehrstransaktionen. In diesem Abschnitt können Sie NetScaler ADM auch so konfigurieren, dass Alarme ausgelöst werden, wenn bestimmte Verkehrsbedingungen auf einem virtuellen Server erfüllt sind.

Sie können NetScaler ADM über StyleBooks so konfigurieren, dass Verkehrsstatistiken aus verschiedenen NetScaler ADM Insights gesammelt werden, die wie folgt aufgeführt sind:

- Web Insight
- Sicherheitshinweise
- HDX Insight
- Citrix Gateway Insight:

Zu den unterstützten virtuellen Servern zählen Lastenausgleich, Content Switching und virtuelle VPN-Server.

Aktivieren Sie Web Insight oder Security Insight oder beide für Analysen auf einem Lastausgleich oder einem virtuellen Content Switching-Server. Bei virtuellen VPN-Servern müssen Sie jedoch HDX Insight und NetScaler Gateway Insight oder einen davon aktivieren.

Jedes NetScaler ADM Insight, das auf NetScaler ADC-Instanzen über StyleBooks aktiviert ist, verwendet das IPFIX-Protokoll (AppFlow), um die Daten von den Instanzen an NetScaler ADC zu senden.

Wenn Sie Web Insight aktivieren, ist clientseitige Messungen auch auf dem Lastenausgleich und den virtuellen Content Switching-Server aktiviert. Bei aktivierten clientseitigen Messungen erfasst ADM über HTML-Injection Ladezeit und Rendering-Zeit-Metriken für HTML-Seiten. Mit diesen Metriken können Administratoren Probleme mit der L7-Latenz identifizieren.

Beispiel 1:

Das folgende Beispiel zeigt, wie Sie den Abschnitt "Vorgänge"in ein StyleBook schreiben, um sowohl HDX Insight als auch Citrix Gateway Insight auf einem virtuellen VPN-Server zu aktivieren:

```
name: simple-vpn-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable hdxinsight and gatewayinsight on
   a VPN vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
components:
    -
        name: vpnvserver-comp
        type: ns::vpnvserver
        properties:
            name: str("vpn-") + str($current-target.ip)
            servicetype: SSL
            ipv46: 1.1.21.37
            port: 443
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.vpnvserver-comp
                filter: "true"
                insights:
                  -
                 type: hdxinsight**
                  -
                    type: gatewayinsight
outputs:
  -
    name: myvpns
    value: $components.vpnvserver-comp
<!--NeedCopy-->
```

Beispiel 2:

Das folgende Beispiel zeigt, wie der Abschnitt Vorgänge in einem StyleBook geschrieben wird, um Web Insight und Security Insight auf einem virtuellen Lastausgleichsserver zu aktivieren:

```
name: simple-lb-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable webinsight and securityinsight on
    LB vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
components:
    -
        name: lbvserver-comp
        type: ns::lbvserver
        properties:
            name: str("lb-") + str($current-target.ip)
            servicetype: HTTP
            ipv46: 1.1.21.37
            port: 80
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.lbvserver-comp
                filter: "true"
                 insights:
                 -
                  type: webinsight
                   -
                  type: securityinsight
outputs:
  -
    name: mylbs
    value: $components.lbvserver-comp
<!--NeedCopy-->
```

Analytics

February 5, 2024

Der Analytics-Unterabschnitt des Operations-Abschnitts weist eine Struktur auf, die dem Komponentenabschnitt ähnelt. Jedes Element im Analyseabschnitt wird verwendet, um die NetScaler ADM Analytics-Funktion für einen oder mehrere virtuelle Server zu konfigurieren, die vom StyleBook

erstellt wurden.

Ein Element im Analytics-Bereich hat die folgenden Attribute:

Attribut	Beschreibung	Erforderlich
name	Name des Analyseelements.	Ja
Beschreibung	Eine Textzeichenfolge, die beschreibt, was dieses Element ist.	Nein
Bedingung	Ein boolescher Ausdruck. Wenn diese Bedingung als falsch ausgewertet wird, wird das gesamte Analyseelement übersprungen.	Nein
Wiederholen	Iteriert über eine Liste.	Nein
Wiederholungsbedingung	Ein boolescher Ausdruck. Wenn der Ausdruck falsch ausgewertet wird, wird die aktuelle Iteration übersprungen.	Nein
wiederholender Artikel	Name des Elements in der aktuellen Iteration.	Nein
Wiederholungsindex	Name des Indexwerts der aktuellen Iteration.	Nein
properties	Die Liste der Eigenschaften von Analytics.	Ja
target	Eine der Eigenschaften in der Liste. Der Zielausdruck ist der Name eines virtuellen Servers, der auf dem NetScaler ADC konfiguriert ist und für den Analysen gesammelt werden.	Ja

Attribut	Beschreibung	Erforderlich
Filter	Eine der Eigenschaften in der Liste. Der Wert dieses Attributs ist ein erweiterter NetScaler ADC-Richtlinienausdruck, der zum Filtern der Anforderungen auf dem virtuellen Server verwendet wird, für den Analysen gesammelt werden. Standardmäßig werden die Analysedaten für den gesamten Datenverkehr gesammelt, der durch den virtuellen Server fließt.	Nein

Beispiel:

```
operations:

  analytics:

    -

    name: lbvserver-ops-comp

    properties:

    target: $components-basic-lb-comp.outputs.lbvserver-name

    filter: HTTP.REQ.URL.CONTAINS("catalog")
<!--NeedCopy-->
```

Jedes Attribut im Analyseabschnitt wird verwendet, um die NetScaler ADM Analytics-Funktion anzuweisen, die NetScaler ADC Instanzen so zu konfigurieren, dass Appflow-Datensätze auf dem virtuellen Server erfasst werden, der von der Zieleigenschaft identifiziert wird.

Alarme

February 5, 2024

Der Unterabschnitt „Alarme“des Abschnitts „Operationen“hat eine ähnliche Struktur und dieselben

Attribute wie der Unterabschnitt „Analytik“. Der einzige Unterschied besteht im Attribut properties. Eine Liste aller Attribute (mit Ausnahme des Attributs properties) finden Sie unter Analytics.

Die folgenden Eigenschaften sind in einem Alarm-Unterabschnitt verfügbar:

Attribut	Beschreibung	Erforderlich
target	Ein Ausdruck, der den Namen eines virtuellen Servers auswertet, der auf dem NetScaler ADC konfiguriert ist, für den Alarme konfiguriert sind.	Ja
E-Mail-Profil	Name eines E-Mail-Profils, das in der NetScaler ADM Analytics-Funktion definiert ist und eine Liste von E-Mail-Adressen enthält, die Sie benachrichtigen möchten, wenn der Alarm ausgelöst wird.	Nein (entweder ein E-Mail-Profil oder ein SMS-Profil muss definiert sein)
SMS-Profil	Name eines SMS-Profils, das in der NetScaler ADM Analytics-Funktion definiert ist und eine Liste der Telefonnummern enthält, die Sie benachrichtigen möchten, wenn der Alarm ausgelöst wird.	Nein (entweder ein E-Mail-Profil oder ein SMS-Profil muss definiert sein)
rules	Eine Liste von Regeln, die die Bedingungen definieren, die einen Alarm für den durch die Zieleigenschaft definierten virtuellen Server auslösen würden.	Ja
metrisch	Ein Attribut der Regel. Der Name einer Metrik, die Sie für den virtuellen NetScaler ADC-Server verfolgen möchten.	Ja

Attribut	Beschreibung	Erforderlich
Operator	Ein Attribut der Regel. Der Operator, mit dem die Metrik mit dem Wert verglichen werden soll. Gültige Operatoren sind „größer als “und „kleiner als“.	Ja
Wert	Ein Attribut der Regel. Der Schwellenwert, mit dem die Metrik mithilfe des Operators verglichen wird. Wenn der Metrikwert diesen Schwellenwert überschreitet, werden die zugehörigen Alarme ausgelöst.	Ja
Periodeneinheit	Ein Attribut einer Regel. Die Häufigkeit, mit der Benutzer benachrichtigt werden sollen, wenn die Alarmregel erfüllt ist. Dies kann den Wert Tag, Stunde oder Woche enthalten. Das bedeutet, dass bei Einhaltung der Regel einmal pro Periodeneinheit (z. B. einmal täglich) ein Alarm gesendet wird.	Ja

Die folgende Tabelle enthält eine Liste der Metriken, die für den virtuellen NetScaler ADC-Server verfolgt werden.

Zähler|Beschreibung|Ausführliche Beschreibung|NetScaler ADM Berechnung
|—|—|—|—|
|Für einen virtuellen VPN-Server:|
total_requests|Gesamtzahl der Starts von VPN-Sitzungen|Gesamtzahl der aktiven Sitzungen auf diesem virtuellen VPN-Server, die während eines vom Benutzer angegebenen Zeitintervalls gestartet wurden.|Monoton ansteigender Zähler, erhöht bei jedem Start einer neuen Sitzung|
|app_count|Anzahl der Starts der VPN-App|Gesamtzahl der eindeutigen VPN-Anwendungen auf diesem virtuellen VPN-Server, die während eines vom Benutzer angegebenen Zeitintervalls gestartet wurden.|Monoton ansteigender Zähler bei jedem Start einer neuen Anwendung|

app_launch_dauer	Dauer des Starts der VPN-App	Durchschnittliche Zeit zum Starten einer Anwendung (in Millisekunden)	Durchschnittlicher Wert, der über die Dauer der Startzeit aller auf diesem virtuellen VPN-Server gestarteten VPN-Anwendungen hinweg berechnet wird
Andere virtuelle Server (CS, LB, Auth, GSLB)		
Total_Requests	Anzahl der Anforderungen	Anzahl der Clientanforderungen auf diesem virtuellen Server seit dem letzten Neustart der Appliance oder seit der Erstellung des virtuellen Servers, je nachdem, welcher Wert aktueller ist.	Monoton zunehmender Zähler, erhöht bei jeder neuen Anforderung an diesen virtuellen Server.
Total_Bytes	Bytes	Gesamtzahl der Bytes, die im angegebenen Zeitintervall vom virtuellen Server an Citrix ADM übertragen wurden.	Monoton zunehmender Zähler, um die Gesamtzahl der Bytes zu berücksichtigen, die von diesem virtuellen Server bereitgestellt werden.
Application_Response_time	Antwortzeit	Durchschnittliche Antwortzeit des virtuellen Servers.	Der durchschnittliche Wert der Antwortzeiten aller Anfragen, die dieser virtuelle Server seit dem letzten Neustart der Appliance (oder seit der Erstellung des virtuellen Servers) empfangen hat, je nachdem, welcher Wert zuletzt ist.

Beispiel für einen Alarmabschnitt in einem StyleBook:

```
operations:
alarms:
 -
  name:lbvserver_alarm
  properties:
  target: $outputs.lbvserver
  email-profile: $parameters.emailprofile
  sms-profile: "NetScalerSMS"
     rules:
      -
        metric: "total_requests"
        operator: "greaterthan"
        value: 25
        period-unit: weekly
        -
          metric: "total_bytes"
          operator: "lessthan"
          value: 1024
          period-unit: day

<!--NeedCopy-->
```

Ausdrücke

February 5, 2024

Eine der mächtigsten Funktionen eines StyleBook ist die Verwendung von Ausdrücken. Sie können

StyleBooks-Ausdrücke in verschiedenen Szenarien verwenden, um dynamische Werte zu berechnen. Das folgende Beispiel ist ein Ausdruck zum Verketten eines Parameterwerts mit einer Literalzeichenfolge.

Beispiel:

```
$parameters.appname + "-mon"
<!--NeedCopy-->
```

Dieser Ausdruck ruft den Parameter mit dem Namen `appname` ab und verkettet ihn mit der Zeichenfolge `-mon`.

Die folgenden Ausdruckstypen werden unterstützt:

Arithmetische Ausdrücke

- Zusatz (+)
- Subtraktion (-)
- Multiplikation (*)
- Abteilung (/)
- Modul (%)

Beispiele:

- Zwei Zahlen hinzufügen: $parameters.a + $parameters.b
- Zwei Zahlen multiplizieren: $parameters.a * 10
- Finden des Restes nach Division einer Zahl durch eine andere:

`15%10` Ergebnisse in 5

String-Ausdrücke

- Verketten Sie zwei Strings (+)

Beispiel:

Verketten Sie zwei Strings: str (“app-“) + $parameters.appname

Ausdrücke auflisten

Führt zwei Listen zusammen (+)

Beispiel:

- Verketten Sie zwei Listen: $parameters.external-servers + $parameters.internal-servers

- Wenn `$parameters.ports-1` [80, 81] und `$parameters.port-2` [81, 82] ist, wird `$parameters.ports-1 + $parameters.ports-2` als Liste [80, 81, 81, 82] angezeigt.

Relationale Ausdrücke

- **==** : Prüft, ob zwei Operanden gleich sind und gibt true zurück, wenn sie gleich sind, sonst gibt false zurück.
- **!** =: Testet, ob zwei Operanden unterschiedlich sind und gibt true zurück, wenn sie unterschiedlich sind, andernfalls wird false zurückgegeben.
- **: Gibt true zurück, wenn der erste Operand größer als der zweite Operand ist, andernfalls wird false zurückgegeben.
- **>=** : Gibt true zurück, wenn der erste Operand größer oder gleich dem zweiten Operanden ist, andernfalls wird false zurückgegeben.
- **<** : Gibt true zurück, wenn der erste Operand kleiner als der zweite Operand ist, andernfalls wird false zurückgegeben.
- **<=** : Gibt true zurück, wenn der erste Operand kleiner oder gleich dem zweiten Operanden ist, andernfalls wird false zurückgegeben.

Beispiel:

- Verwendung des Gleichstellungs-Operators: `$parameters.name = = "abcd"`
- Verwendung des Inequality Operators: `$parameters.name != "default"`
- Beispiele für andere relationale Operatoren
  - 10 > 9
  - 10 >= 10
  - 0 < 9
  - 10 <= 9
  - 10 == 10
  - 10 != 1

Logische Ausdrücke - boolescher Wert

- **und**: Der logische ‘und’Operator. Wenn beide Operanden wahr sind, ist das Ergebnis wahr, andernfalls ist es falsch.
- **oder**: Der logische “oder”-Operator. Wenn einer der Operanden wahr ist, ist das Ergebnis wahr, andernfalls ist es falsch.
- **nicht**: Der unäre Operator. Wenn der Operand wahr ist, ist das Ergebnis falsch und umgekehrt.

- **in**: Prüft, ob das erste Argument eine Teilzeichenfolge des zweiten Arguments ist
- **in**: Prüft, ob ein Element Teil einer Liste ist

> **Hinweis**
>
> Sie können Ausdrücke eingeben, bei denen Zeichenketten in Zahlen und Zahlen in Zeichenketten umgewandelt werden. In ähnlicher Weise können Sie `tcp-port` in eine Zahl umwandeln, und eine IP-Adresse kann in eine Zeichenfolge umgewandelt werden.
>
> Verwenden Sie ein Trennzeichen vor und nach einem Operator. Sie können die folgenden Trennzeichen verwenden:
>
> - Vor einem Operator: `spacetab`, `comma`, `(`, `)`, `[`, `]`
> - Nach einem Operator: `space`, `tab`, `(`, `[`
>
> Beispiel:
>
> - `abc + def`
> - `100 % 10`
> - `10 > 9`

Wörtliche Zeichenfolgenausdrücke

Sie können wörtliche Zeichenfolgen verwenden, wenn Sonderzeichen in einer Zeichenfolge ihre literale Form annehmen müssen. Diese Zeichenfolgen können Escape-Zeichen, umgekehrte Schrägstriche, Anführungszeichen, Klammern, Leerzeichen, Klammern usw. enthalten. In wörtlichen Zeichenketten wird die übliche Interpretation der Sonderzeichen übersprungen. Alle Zeichen in der Zeichenfolge bleiben in ihrer wörtlichen Form erhalten.

In StyleBooks können Sie NetScaler ADC Richtlinienausdrücke in ihre literale Form mithilfe von wörtlichen Zeichenfolgen einschließen. Die Richtlinienausdrücke enthalten in der Regel Sonderzeichen. Ohne wörtliche Zeichenfolgen müssen Sie Sonderzeichen umgehen, indem Sie Strings in Teilstrings zerlegen.

Um eine wörtliche Zeichenfolge zu erstellen, kapseln Sie eine Zeichenfolge wie folgt zwischen Sonderzeichen:

```
~{
 string }
 ~
<!--NeedCopy-->
```

Sie können wörtliche Zeichenketten überall im StyleBook verwenden.

> **Hinweis**
>
> Verwenden Sie nicht die Zeichenfolge `}~` in einer Eingabezeichenfolge, da diese Sequenz das Ende einer wörtlichen Zeichenfolge angibt.

Beispiel:

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

Target-Ausdrücke

In einer StyleBook-Definition können Sie den `$current-target` Ausdruck verwenden, um auf die aktuelle ADC-Zielinstanz zu verweisen. Um sich ausdrücklich auf die IP-Adresse der ADC-Zielinstanz zu beziehen, verwenden Sie diesen Ausdruck wie folgt:

```
$current-target.ip
<!--NeedCopy-->
```

Beispiel:

```
components:
 -
  name: lb-comp
  type: ns::lbvserver
  properties:
    name: $current-target.ip + "-lbvserver"
<!--NeedCopy-->
```

In diesem Beispiel `lbvserver` wird der Name des mit der IP-Adresse der ADC-Zielinstanz erstellt.

Ausdruckstypvalidierung

Die StyleBook-Engine ermöglicht eine stärkere Typprüfung während der Kompilierungszeit, dh die beim Schreiben des StyleBook verwendeten Ausdrücke werden beim Import von StyleBook selbst und nicht beim Erstellen des Konfigurationspakets validiert.

Alle Verweise auf Parameter, Substitutionen, Komponenten, Eigenschaften von Komponenten, Ausgaben von Komponenten, benutzerdefinierte Variablen (Repeat-Item, Repeat-Index, Argumente auf Substitutionsfunktionen) usw. werden auf ihre Existenz und Typen validiert.

Beispiel für Typprüfungen:

Im folgenden Beispiel lautet der erwartete Typ der Port-Eigenschaft von `lbvserver` StyleBook `tcp-port`. In Citrix Application Delivery Management (ADM) werden die Typvalidierungen zur Kompilierungszeit (Importzeit) durchgeführt. Der Compiler findet diese Zeichenfolge und `tcp-port` es handelt sich nicht um kompatible Typen. Daher zeigt der StyleBook-Compiler einen Fehler an und kann ein StyleBook nicht importieren oder migrieren.

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
      servicetype: HTTP
<!--NeedCopy-->
```

Um dieses StyleBook erfolgreich zu kompilieren, deklarieren Sie Folgendes als Zahl im Compiler:

`port: 80`

Beispiel für das Markieren ungültiger Ausdrücke:

In früheren Versionen hat der Compiler, wenn einem Eigenschaftsnamen ein ungültiger Ausdruck zugewiesen wurde, keine ungültigen Ausdrücke erkannt und die StyleBooks in Citrix ADM importiert werden können. Wenn dieses StyleBook nun in Citrix ADM importiert wird, identifiziert der Compiler solche ungültigen Ausdrücke und kennzeichnet es. Daher kann das StyleBook nicht in NetScaler ADM importiert werden.

In diesem Beispiel lautet der Ausdruck, der der Namenseigenschaft in der Komponente `lb-sg-binding-comp` zugewiesen ist: `$components.lbvserver-comp.properties.lbvservername`. Es gibt jedoch keine Eigenschaft, die `lbvservername`in der Komponente aufgerufen wird `lbvserver-comp`. In früheren Citrix ADM Versionen hätte der Compiler diesen Ausdruck zugelassen und erfolgreich importiert. Der eigentliche Fehler würde auftreten, wenn ein Benutzer mit diesem StyleBook ein Konfigurationspaket erstellen möchte. Diese Art von Fehler wird jedoch beim Import erkannt und das StyleBook wird nicht in Citrix ADM importiert. Korrigieren Sie solche Fehler manuell und importieren Sie die StyleBooks.

```
Components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: sg-comp
```



```
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.lbvservername
      servicegroupname: $components.sg-comp.properties.servicegroupname
<!--NeedCopy-->
```

Indizierung von Listen

Auf Elemente einer Liste kann jetzt zugegriffen werden, indem Sie sie direkt indizieren:

Ausdruck	Beschreibung
`$components.test-lbs[0]`	Bezieht sich auf das erste Element in der Komponente test-lbs
`$components.test-lbs[0].properties.p1`	Bezieht sich auf die Eigenschaft p1 des ersten Elements in der test-lbs-Komponente
`$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname`	Bezieht sich auf die Eigenschaft `servicegroupname` des zweiten Elements in der `servicegroups` Komponente, die eine Ausgabe des ersten Elements der `lbcomps` Komponente ist

In-Place-Interpolationen

February 6, 2024

Es ist jetzt möglich, Teile einer Zeichenfolge mithilfe eines oder mehrerer StyleBook-Ausdrücke zu ersetzen. Wenn diese Zeichenfolgenausdrücke vom StyleBook-Compiler ausgewertet werden, wird der Teil der Zeichenfolge, der einen StyleBook-Ausdruck verwendet, durch den Wert des Ausdrucks ersetzt. Um StyleBook-Ausdrücke in eine Zeichenfolge einzuschließen, verwenden wir die folgende Notation:

“…%{…}%…”

wobei die zwischen “%{ “und “}%”eingeschlossenen Zeichen einen StyleBook-Ausdruck bilden. Diese Ausdrücke werden als In-Place-Interpolationen bezeichnet.

Beispielsweise ist die Zeichenfolge “lb-%{$parameters.appname}%-svc”ein Zeichenfolgenausdruck mit In-Place-Interpolation eines StyleBook-Ausdrucks. Der Wert des Zeichenfolgenausdrucks hängt vom Wert des Interpolationsausdrucks ab. Beachten Sie, dass **$parameters.appname** mit “app1” zugewiesen ist. Dann wird der Zeichenfolgenausdruck zu **lb-app1-svc** ausgewertet. Dadurch können die Werte nicht in Zeichenfolgenausdrücken hartcodiert, sondern anhand der benutzerdefinierten Werte ausgewertet werden.

Ein praktischer Anwendungsfall von In-Place-Interpolationen ist die Parametrisierung von Richtlinienausdrücken in StyleBooks. Stellen Sie sich ein Szenario vor, in dem Sie einen Richtlinienausdruck schreiben möchten, der überprüft, ob die HTTP-URL ein bestimmtes Wort enthält, z. B. „jpeg“.

Dazu schreiben Sie einen Richtlinienausdruck wie folgt: “HTTP.REQ.URL.CONTAINS(\“jpeg\”)”.

Wenn Sie nun das Objekt in der HTTP-URL parametrisieren möchten, können Sie dem StyleBook einen String-Parameter hinzufügen, z. B. $parameters.url-object. Der Richtlinienausdruck sollte auf der Grundlage dieses Parameters geschrieben werden. Dazu verwenden Sie String-Verkettung, um das Ergebnis zu erzielen. Der Ausdruck würde wie folgt aussehen:

str(“HTTP.REQ.URL.CONTAINS(\’”+ $parameters.url-object + “\”)”)

Wenn $parameter.url-object „csv“zugewiesen ist, wird der obige Ausdruck als “HTTP.REQ.URL.CONTAINS(\ “csv\”)”ausgewertet. Dieser Ausdruck ist jedoch nicht leicht zu lesen. Um diese Parametrisierung leicht lesbar und verständlich zu machen, können Sie In-Place-Interpolationen verwenden.

Der Ausdruck mit In-Place-Interpolation lautet nun:

str(“HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)”)

Im obigen Ausdruck haben Sie einen Interpolationsausdruck verwendet, der die inneren Anführungszeichen um den Wert des $parameters.url-Objekts hinzufügt. Das Ergebnis dieses Ausdrucks ist dasselbe wie oben, sieht jedoch intuitiver aus und kommt dem tatsächlichen Ergebnis näher.

Zulässige Typen innerhalb von Interpolationen

Sie können innerhalb von Interpolationen Ausdrücke verwenden, die Werte der folgenden Typen generieren: boolean, number, tcp-port, ipaddress und string. Der generierte Wert wird automatisch in eine Zeichenfolge umgewandelt, wenn die Interpolationen durch das Ergebnis ersetzt werden.

Zeichenfolgenausdrücke können 0, 1 oder mehr Interpolationen haben. Bei einer sequentiellen Interpolation können verschiedene Teile des Zeichenfolgenausdrucks durch verschiedene StyleBook-Ausdrücke ersetzt werden. Die Zeichenfolge g lb-%{$parameters.appname}%-%{$parameters.vip}%

gibt “lb-app1-1.1.1.1”zurück, wenn $parameters.appname “app1”und $parameters.vip “1.1.1.1” ist.

Zeichenfolgenausdrücke unterstützen auch verschachtelte Interpolationen. Das heißt, ein Interpolationsausdruck kann in einem anderen Interpolationsausdruck verschachtelt werden, so dass der Wert eines Ausdrucks eine Eingabe für den zweiten Ausdruck werden kann.

Betrachten Sie zum Beispiel eine Zeichenfolge “%{lb-%{$parameters.port + 1}%}%”

Die interne Zeichenfolge “**%{$parameters.port + 1}%**”gibt “lb-81”zurück, wenn $parameters.port 80 ist. Hier ist dieser Ausdruck in einem anderen Interpolationsausdruck verschachtelt.

In der folgenden Tabelle werden die verschiedenen Interpolationstypen mit Beispielen und entsprechenden Ergebnissen beschrieben. Die Werte der in den Beispielen verwendeten Parameter sind:

- $parameters.appname: “lb1”
- $parameters.vip: “1.1.1.1”
- $parameters.n1: 1
- $parameters.n2: 3

Einfache Interpolationen

Ausdruck	Ergebnis
lb-%{$parameters.appname}%-def	lb-lb1-def

Automatische Typkonvertierungen

Ausdruck	Ergebnis
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

Sequentielle Interpolationen

Ausdruck	Ergebnis
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

Verschachtelte Interpolationen

Ausdruck	Ergebnis
%{abc-%{$parameters.n1 + 1}%}%	abc-2
str(“%{abc-%{$parameters.n1}%}%-%{$parameters.n2}%”)	bc-1-3

Interpolationen mit Quotewrap

Ausdruck	Ergebnis
str(“%{quotewrap(abcd)}%”)	“abcd
str(“%{quotewrap(https://)} %+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")	“«code class=”language-plaintext highlighter-rouge”>https://”+HTTP.REQ.HOSTNAME+HTTP.REQ.URL</code>

Escape-Zeichen in Interpolationen

Wenn die Zeichen “%{“oder “}%”Teil der Zeichenfolge sind, müssen Sie “\”als Escape-Zeichen angeben, damit der StyleBook-Compiler diese nicht als Interpolations-Tags auswertet.

Beispiel:

str(“%{\%{ + str($parameters.vip) + }\%}%”) returns “%{1.1.1.1}%”if $parameters.vip is 1.1.1.1

In der folgenden Tabelle werden einige weitere Ausdrücke und deren Ergebnisse beschrieben:

Kategorie	Ausdruck	Ergebnis
Escape-Interpolationen	str(“%{str($parameters.n1) + }%}%”)	1}%
	lb-%{str($parameters.n1) + }%}%	lb-1}%
	”%{str($parameters.n1) + \” }\%\”}%”	1}%

Integrierte Funktionen

February 6, 2024

Ausdrücke in StyleBooks können integrierte Funktionen nutzen.

Beispielsweise können Sie die integrierte Funktion `str()` verwenden, um eine Zahl in eine Zeichenfolge umzuwandeln.

```
str($parameters.order)
```

Oder Sie können die integrierte Funktion verwenden, **`int()`** um eine Zeichenfolge in eine Ganzzahl umzuwandeln.

```
int($parameters.priority)
```

Im Folgenden finden Sie die Liste der integrierten Funktionen, die in StyleBook-Ausdrücken unterstützt werden, mit Beispielen, wie sie verwendet werden können:

str()

Die `str()` Funktion transformiert das Eingabeargument in einen String-Wert.

Zulässige Argumenttypen:

- `string`
- `number`
- `TCP-port`
- **`boolean`**
- `IP address`

Beispiele:

- Die Funktion `"set-"+ str(10)` gibt `"set-10"` zurück.
- Die Funktion `str(10)` gibt `10` zurück.
- Die Funktion `str(1.1.1.1)` gibt `1.1.1.1` zurück.
- Die Funktion `str(T rue)` gibt `"T rue"` zurück.
- Die Funktion `str(ADM)` gibt `"mas"` zurück.

int()

Die **`int`**`()` Funktion verwendet eine Zeichenfolge, eine Zahl, eine IP-Adresse oder `tcpport` als Argument und gibt eine Ganzzahl zurück.

Beispiele:

- Die Funktion **`int`**`("10")` gibt `10` zurück.
- Die Funktion **`int`**`(10)` gibt `10` zurück.
- Die Funktion **`int`**`(ip('0.0.4.1'))` gibt `1025` zurück.

bool()

Die `bool()` Funktion verwendet einen beliebigen Typ als Argument. Wenn der Argumentwert leer oder nicht vorhanden ist **`false`**, wird diese Funktion zurückgegeben **`false`**.

Ansonsten kehrt es zurück **`true`**.

Beispiele:

- Die Funktion `bool(`**`true`**`)` gibt **`true`** zurück.
- Die Funktion `bool(`**`false`**`)` gibt **`false`** zurück.
- Die Funktion `bool($parameters.a)` gibt **`false`** zurück, wenn `$parameters.a` den Wert **`false`** hat, leer oder nicht vorhanden ist.

len()

Die `len()` Funktion verwendet eine Zeichenfolge oder eine Liste als Argument und gibt die Anzahl der Zeichen in einer Zeichenfolge oder die Anzahl der Elemente in einer Liste zurück.

Beispiel 1:

Wenn Sie eine Substitution wie folgt definieren:

```
items: ["123", "abc", "xyz"]
```

Die Funktion `len($substitutions.items)` gibt 3 zurück.

Beispiel 2:

Die Funktion `len("Citrix ADM")` gibt `10` zurück.

Beispiel 3:

Wenn `$parameters.vips` die Werte `['1.1.1.1', '1.1.1.2', '1.1.1.3']` hat, gibt die Funktion `len($parameters.vips)` das Ergebnis 3 zurück.

min()

Die `min()` Funktion verwendet entweder eine Liste oder eine Reihe von Zahlen oder `tcp-ports` als Argumente und gibt das kleinste Element zurück.

Beispiele mit einer Reihe von Zahlen/TCP-Ports:

- Die Funktion `min(80, 100, 1000)` gibt `80` zurück.
- Die Funktion `min(-20, 100, 400)` gibt `-20` zurück.
- Die Funktion `min(-80, -20, -10)` gibt `-80` zurück.
- Die Funktion `min(0, 100, -400)` gibt `-400` zurück.

Beispiele mit einer Liste von Zahlen/TCP-Ports:

- Support `$parameters.ports` ist eine Liste von `tcp-ports` und hat Werte: `[80, 81, 8080]`.

  Die Funktion `min($parameters.ports)` gibt `80` zurück.

max()

Die Funktion `max()` verwendet entweder eine Liste oder eine Reihe von Zahlen oder `tcp-ports` als Argumente und gibt das größte Element zurück.

Beispiele mit einer Reihe von Zahlen/TCP-Ports:

- Die Funktion `max(80, 100, 1000)` gibt `1000` zurück.
- Die Funktion `max(-20, 100, 400)` gibt `400` zurück.
- Die Funktion `max(-80, -20, -10)` gibt `-10` zurück.
- Die Funktion `max(0, 100, -400)` gibt `100` zurück.

Beispiele mit einer Liste von Zahlen/TCP-Ports:

- Unterstützung `$parameters.ports` ist Liste von `tcp-ports` und hat Werte: `[80, 81, 8080]`.

  Die Funktion `max($parameters.ports)` gibt `8080` zurück.

bin()

Die Funktion `bin()` verwendet eine Zahl als Argument und gibt eine Zeichenfolge zurück, die die Zahl im Binärformat darstellt.

Beispiele für Ausdrücke:

Die Funktion `bin(100)` gibt `0b1100100` zurück.

oct()

Die Funktion `oct()` verwendet eine Zahl als Argument und gibt eine Zeichenfolge zurück, die die Zahl im Oktalformat darstellt.

Beispiele für Ausdrücke:

Die Funktion `oct(100)` gibt `0144` zurück.

hex()

Die `hex()` Funktion verwendet eine Zahl als Argument und gibt eine Kleinbuchstabenzeichenfolge zurück, die die Zahl im Hexadezimalformat darstellt.

Beispiele für Ausdrücke:

Die Funktion `hex(100)` gibt `0x64` zurück.

lower()

Die Funktion `lower()` verwendet eine Zeichenfolge als Argument und gibt die gleiche Zeichenfolge in Kleinbuchstaben zurück.

Beispiel:

Die Funktion `lower("ADM")` gibt `adm` zurück.

upper()

Die `upper()` Funktion verwendet eine Zeichenfolge als Argument und gibt dieselbe Zeichenfolge in Großbuchstaben zurück.

Beispiel:

Die Funktion `upper("Citrix ADM")` gibt `CITRIX ADM` zurück.

sum()

Die `sum()` Funktion nimmt eine Liste von Zahlen oder `tcpports` als Argumente und gibt die Summe der Zahlen in der Liste zurück.

Beispiel 1:

Wenn Sie eine Substitution wie folgt definieren:
Substitutionen:

```
list-of-numbers = [11, 22, 55]
```

Die Funktion `sum($substitutions.list-of-numbers)` gibt 88 zurück.

Beispiel 2:

Wenn ja `$parameters.ports[80, 81, 82]`, kehrt die `sum($parameters.ports)` Funktion zurück 243.

pow()

Die `pow()` Funktion nimmt zwei Zahlen als Argumente und gibt eine Zahl zurück, die das erste Argument darstellt, das die Potenz des zweiten darstellt.

Beispiel:

Die Funktion `pow(3,2)` gibt 9 zurück.

ip()

Die Funktion `ip()` verwendet eine Ganzzahl, einen String oder eine IP-Adresse als Argument und gibt die IP-Adresse basierend auf dem Eingabewert zurück.

Beispiele:

- Geben Sie eine IP-Adresse in der `ip` Funktion an:

  Die Funktion `ip(3.1.1.1)` gibt `3.1.1.1` zurück.

- Geben Sie eine Zeichenfolge in der `ip` Funktion an:

  Die Funktion `ip('2.1.1.1')` gibt `2.1.1.1` zurück.

- Geben Sie eine Ganzzahl in der Funktion `ip` an:

  - Die Funktion `ip(12)` gibt `0.0.0.12` zurück.
  - Wenn Sie eine Ganzzahl als String in der `ip` Funktion angeben, wird eine entsprechende IP-Adresse der Eingabe zurückgegeben.

    Die Funktion `ip('1025')` gibt `0.0.4.1` zurück.

Diese Funktion unterstützt auch die Integer-Additions- und Subtraktionsoperationen und gibt eine resultierende IP-Adresse zurück.

- Addition: Die Funktion `ip(1025)+ ip(12)` gibt `0.0.4.13` zurück.
- Subtraktion: Die Funktion `ip('1025')- ip(12)` gibt `0.0.3.245` zurück.
- Kombinieren Sie Addition und Subtraktion: Die `ip('1.1.1.1')+ ip('1.1.1.1')- ip(2)` Renditen `2.2.2.0`.

base64.encode()

Die `base64.encode()` Funktion verwendet ein String-Argument und gibt die Base64-codierte Zeichenfolge zurück.

Beispiel:

Die Funktion `base64.encode("abcd")` gibt `YWJjZA==` zurück.

base64.decode()

Die `base64.decode` Funktion verwendet eine Base64-codierte Zeichenfolge als Argument und gibt die dekodierte Zeichenfolge zurück.

Beispiel:

Die Funktion `base64.decode("YWJjZA==")` gibt `abcd` zurück.

exists()

Die Funktion `exists()` verwendet ein Argument eines beliebigen Typs und gibt einen booleschen Wert zurück. Der Rückgabewert ist `True`, wenn die Eingabe einen Wert hat. Der Rückgabewert ist `False` Wenn das Eingabeargument keinen Wert hat (also keinen Wert).

Bedenken Sie, dass der ein optionaler Parameter `$parameters.monitor` ist. Wenn Sie beim Erstellen eines Konfigurationspakets einen Wert für diesen Parameter angeben, gibt die `($parameters.monitor)` Funktion zurück `True`.

Ansonsten kehrt es zurück `False`.

filter()

Die `filter()` Funktion benötigt zwei Argumente.

Argument 1: eine Substitutionsfunktion, die ein Argument annimmt und einen booleschen Wert zurückgibt.

Argument 2: eine Liste.

Die Funktion gibt eine Teilmenge der ursprünglichen Liste zurück, zu der jedes Element `True` bei der Übergabe an die Substitutionsfunktion im ersten
Argument ausgewertet wird.

Beispiel:

Angenommen, wir haben eine Substitutionsfunktion wie folgt definiert.

Substitutionen:

```
x(a): $a != 81
```

Diese Funktion gibt True zurück, wenn der Eingabewert nicht gleich ist `81`. Ansonsten kehrt es zurück `False`.

Nehmen wir an,`$parameters.ports` ist es `[81, 80, 81, 89]`.

Die `filter($substitutions.x, $parameters.ports)` Rückgabe, `[80, 89]` indem alle Vorkommen von `81` aus der Liste entfernt werden.

if-then-else()

Die Funktion **`if`**`-then-`**`else`**`()` benötigt drei Argumente.

Argument 1: Boolescher Ausdruck

Argument 2: Beliebiger Ausdruck

Argument 3: Beliebiger Ausdruck (optional)

Wenn der Ausdruck in Argument 1 zu ausgewertet wird `True`, gibt die Funktion den Wert des als Argument 2 bereitgestellten Ausdrucks zurück.

Andernfalls, wenn Argument 3 angegeben wird, gibt die Funktion den Wert des Ausdrucks in Argument 3 zurück.

Wenn Argument 3 nicht angegeben wird, kehrt die Funktion zurück `no`.

Beispiel 1:

Die **`if`**`-then-`**`else`**`($parameters.servicetype == HTTP, 80, 443)` Funktion gibt zurück `80`, wenn Wert `$parameters.servicetype` hat `HTTP`. Andernfalls wird die Funktion zurückgegeben `443`.

Beispiel 2:

Die Funktion `if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` gibt den Wert `$parameters.hport` zurück, wenn `$parameters.servicetype` den Wert `HTTP` hat.

Andernfalls gibt die Funktion den Wert von zurück `$parameters.sport`.

Beispiel 3:

Die `if-then-else($parameters.servicetype == HTTP, 80)` gibt zurück `80`, wenn Wert `$parameters.servicetype` hat `HTTP`.

Andernfalls gibt die Funktion keinen Wert zurück.

join()

Die Funktion `join()` hat zwei Argumente:

Argument 1: Liste von Zahlen `tcp-ports`, Strings oder IP-Adressen

Argument 2: Trennzeichenfolge (optional)

Diese Funktion verbindet die Elemente der Liste, die als Argument eins bereitgestellt werden, in einer Zeichenfolge, wobei jedes Element durch die als Argument zweite angegebene Begrenzungszeichenfolge getrennt ist. Wenn Argument zwei nicht angegeben wird, werden die Elemente in der Liste als eine Zeichenfolge verbunden.

Beispiel:

- `$parameters.ports` ist `[81, 82, 83]`.
  - Mit Trennzeichen Argument:

    Die Funktion `join($parameters.ports, '-')` gibt `81-82-83` zurück.
  - Ohne Trennzeichen Argument:

    Die Funktion `join($parameters.ports)` gibt `818283` zurück.

split()

Die Funktion `split()` teilt eine Eingabezeichenfolge in mehrere Listen auf, abhängig von den angegebenen Trennzeichen. Wenn kein oder leeres (`''`) Trennzeichen angegeben wird, betrachtet diese Funktion das Leerzeichen als Trennzeichen und teilt die Zeichenfolge in Listen auf.

Beispiele:

- Die Funktion `split('Example_string_split', 's')` gibt `['Example_','tring_','plit']` zurück.

- Die Funktion `split('Example string split')` gibt `['Example','string','split']` zurück.
- Die Funktion `split('Example string split', '')` gibt `['Example','string','split']` zurück.
- Die Funktion `split('Example string')` gibt `['Example','string']` zurück.

  Diese Funktion betrachtet kontinuierliche Räume als ein Leerzeichen.

map()

Die Funktion `map()` benötigt zwei Argumente;

Argument 1: Jede Funktion

Argument 2: Eine Liste von Elementen.

Die Funktion gibt eine Liste zurück, in der jedes Element in der Liste das Ergebnis der Anwendung der `map()` Funktion (Argument eins) auf das entsprechende Element in Argument zwei ist.

Zulässige Funktionen in Argument 1:

- Integrierte Funktionen, die ein Argument annehmen:

  `base64.encode, base64.decode, bin, bool, exists, hex, int, ip, len, lower, upper, oct, quotewrap, str, trim, upper, url.encode, url.decode`

- Substitutionsfunktionen, die mindestens ein Argument verwenden.

Beispiel:

Angenommen, $parameters.nums ist `[81, 82, 83]`.

- Map using a built-in function, str

  Die Funktion `map(str, $parameters.nums)` gibt `["81", "82", "83"]` zurück.

  Das Ergebnis der Map-Funktion ist die Liste der Strings, in denen jedes Element String ist, wird durch Anwenden der str Funktion auf das entsprechende Element in der Eingabeliste berechnet ($parameters.nums).

- Map mit einer Substitutionsfunktion

  - Substitutionen:

    ```
    add-10(port): $port + 10
    ```


- Ausdruck:

  Die `map($substitutions.add-10, $parameters.nums)` Funktion gibt eine Liste von Zahlen zurück: `[ 91, 92, 93 ]`

Das Ergebnis dieser Map-Funktion ist eine Liste von Zahlen, wobei jedes Element durch Anwendung der Substitutionsfunktion `$substitutions.add-10` auf das entsprechende Element in der Eingabeliste (`$parameters.nums`) berechnet wird.

quotewrap()

Die Funktion `quotewrap()` verwendet eine Zeichenfolge als Argument und gibt eine Zeichenfolge zurück, nachdem vor und nach dem Eingabewert ein doppeltes Anführungszeichen hinzugefügt wurde.

Beispiel:

Die Funktion `quotewrap("ADM")` gibt `"mas"` zurück.

replace()

Die Funktion `replace()` hat drei Argumente:

Argument 1: Zeichenfolge

Argument 2: String oder Liste

Argument 3: Zeichenfolge (optional)

Die Funktion ersetzt alle Vorkommen von Argument zwei durch Argument drei in Argument eins.

Wenn Argument drei nicht angegeben wird, werden alle Vorkommen von Argument zwei aus dem ersten Argument entfernt (mit anderen Worten, durch eine leere Zeichenfolge ersetzt).

Ersetzen Sie eine Teilzeichenfolge durch eine andere Teilzeichenfolge:

- Die Funktion `replace('abcdef', 'def', 'xyz')` gibt `abcxyz` zurück.

  Alle Vorkommnisse von `def` werden durch ersetzt `xyz`.

- `replace('abcdefabc', 'def')` kehrt zurück `abcabc`.

  Da es kein drittes Argument gibt, `def` wird aus der resultierenden Zeichenfolge entfernt.

Geben Sie die Liste der Zeichen an, die Sie in einer Zeichenfolge ersetzen möchten.

```
$parameters.spl_chars = ['@', '#', '!', '%']
```

Diese Liste enthält die Werte, die in einer Eingabezeichenfolge ersetzt werden müssen.

Die Funktion `replace('An#example@to%replace!characters', $parameters.spl_chars, '_')` gibt `An_example_to_replace_characters` zurück.

Die Ausgabezeichenfolge hat einen unterstreichen (_) anstelle der in der `$parameters.spl_chars` Liste angegebenen Zeichen.

trim()

Die Funktion `trim()` gibt eine Zeichenfolge zurück, in der die führenden und nachfolgenden Leerzeichen aus der Eingabezeichenfolge entfernt werden.

Beispiel:

Die Funktion `trim('abc ')` gibt `abc` zurück.

truncate()

Die Funktion `truncate()` hat zwei Argumente:

Argument 1: Zeichenfolge

Argument 2: Zahl

Die Funktion gibt einen String zurück, bei dem die Eingabezeichenfolge in Argument eins auf die durch Argument zwei angegebene Länge gekürzt wird.

Beispiel:

Die `truncate('Citrix ADM', 6)` Renditen `Citrix`.

distinct()

Die `distinct()` Funktion extrahiert eindeutige Elemente aus einer Listeneingabe.

Beispiele:
Wenn `$parameters.input_list` den Wert `['ADM', 'ADC', 'VPX', 'ADC', 'ADM', 'CPX']` hat, gibt die Funktion `distinct($parameters.input_list)` das Ergebnis `['ADM', 'ADC', 'VPX', 'CPX']` zurück.

url.encode()

Die `url.encode()` Funktion gibt eine Zeichenfolge zurück, in die Zeichen mithilfe des ASCII-Zeichensatzes gemäß RFC 3986 transformiert werden.

Beispiel:

Die Funktion `url.encode("a/b/c")` gibt `a%2Fb%2Fc` zurück.

url.decode()

Die Funktion `url.decode()` gibt eine Zeichenfolge zurück, in der das URL-codierte Argument gemäß RFC 3986 in eine reguläre Zeichenfolge decodiert wird.

Beispiel:

Die Funktion `url.decode("a%2Fb%2Fc")` gibt `a/b/c` zurück.

ist-ipv4 ()

Die Funktion `is-ipv4()` verwendet eine IP-Adresse als Argument und gibt den booleschen Wert `True` zurück, wenn die IP-Adresse im IPv4-Format vorliegt.

Die Funktion `is-ipv4(10.10.10.10)` gibt `True` zurück.

ist-ipv6 ()

Die Funktion `is-ipv6()` nimmt eine IP-Adresse als Argument und gibt den booleschen Wert `True` zurück, wenn die IP-Adresse im IPv6-Format vorliegt.

Die Funktion `is-ipv6(2001:DB8::)` gibt `True` zurück.

startswith()

Die Funktion `startswith()` bestimmt, ob ein String mit einem bestimmten Präfix beginnt. Diese Funktion erfordert zwei obligatorische Zeichenfolgenargumente.

```
startswith(str, sub_str)
```

Diese Funktion gibt zurück `True`, wenn die Zeichenfolge (`str`) mit der Teilzeichenfolge (`sub_str`) beginnt.

Beispiele:

- Die Funktion `startswith('Citrix', 'Ci')` gibt `True` zurück.
- Die Funktion `startswith('Citrix', 'iC')` gibt `False` zurück.
- Die Funktion `startswith('Citrix', 'Ab')` gibt `False` zurück.

endswith()

Die Funktion `endswith()` bestimmt, ob ein String mit einem bestimmten Suffix endet. Diese Funktion erfordert zwei obligatorische Zeichenfolgenargumente.

`endswith(str, sub_str)`

Diese Funktion gibt zurück `True`, wenn die Zeichenfolge (`str`) mit der Teilzeichenfolge (`sub_str`) endet.

Beispiele:

- Die Funktion `endswith('Citrix', 'ix')` gibt `True` zurück.
- Die Funktion `endswith('Citrix', 'Ix')` gibt `False` zurück.
- Die Funktion `endswith('Citrix', 'ab')` gibt `False` zurück.

contains()

Die Funktion `contains()` ermittelt, ob ein String einen bestimmten Teilstring enthält. Diese Funktion erfordert zwei obligatorische Zeichenfolgenargumente.

`contains(str, sub_str)`

Diese Funktion gibt zurück `True`, wenn der Teilstring (`sub_str`) irgendwo in der Zeichenkette (`str`) enthalten ist.

Beispiel:

- Die Funktion `contains('Citrix', 'tri')` gibt `True` zurück.
- Die Funktion `contains('Citrix', 'Ci')` gibt `True` zurück.
- Die Funktion `contains('Citrix', 'ti')` gibt `False` zurück.

substring()

Verwenden Sie die Funktion `substring()`, um einen Teilstring aus einem String zu extrahieren.

`substring(str, start_index, end_index)`

Diese Funktion erfordert die beiden obligatorischen Argumente und ein optionales Integer-Argument.

- `str` (Obligatorisch)
- `start_index` (Obligatorisch)
- `end_index` (Fakultativ)

Diese Funktion gibt den Teilstring aus dem string (`str`) zurück, der sich zwischen den angegebenen Indexpositionen befindet. Wenn Sie die Endindexposition nicht angeben, extrahiert die Funktion den Teilstring vom Startindex bis zum Ende des Strings.

> **Hinweis**
>
> Wenn Sie `end_index` angeben, schließt die Teilzeichenfolge das Zeichen an der Position `end_index` aus.

Beispiel:

- Die Funktion `substring('Citrix', 2)` gibt `trix` zurück.
- Die Funktion `substring('Citrix', 10)` gibt (") zurück.

  In diesem Beispiel gibt die Funktion eine leere Zeichenfolge zurück, da sie eine ungültige Position `start_index` hat.
- Die Funktion `substring('Citrix', 2, 4)` gibt `tr` zurück.

  In diesem Beispiel extrahiert die Funktion die Zeichen zwischen 2 und 4 Indexpositionen.
- Die Funktion `substring('Citrix', -3)` gibt `rix` zurück.

  Wenn Sie Zeichen extrahieren möchten, die sich am Ende der Zeichenfolge befinden, geben Sie einen negativen Wert für das `start_index`Argument an.

  In diesem Beispiel extrahiert die Funktion den Teilstring, der die letzten drei Zeichen in der Zeichenfolge enthält.

Abhängigkeitserkennung

February 5, 2024

Komponenten in einem StyleBook können auf Eigenschaften oder Abschnitte anderer Komponenten im selben StyleBook verweisen. Komponenten sind für sich genommen komplette Blöcke und sie werden möglicherweise nicht in der gleichen Reihenfolge geschrieben, in der sie ausgeführt werden müssen. Der StyleBook-Compiler überprüft die Reihenfolge, in der die Komponenten geschrieben werden, und führt sie dann in einer logischen Reihenfolge aus.

Beispiel:

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
```



```
10  -
11     name: lb-sg-binding-comp
12     type: ns::lbvserver_servicegroup_binding
13     condition: $parameters.create-binding
14     properties:
15       name: $components.lbvserver-comp.properties.name
16       servicegroupname: $components.sg-comp.properties.servicegroupname
17  -
18     name: sg-comp
19     type: ns::servicegroup
20     properties:
21       servicegroupname: mysg
22       servicetype: HTTP
23  <!--NeedCopy-->
```

Im obigen Beispiel gibt es drei Komponenten definiert - **lbvserver-comp**, **lb-sg-binding-comp**und **sg-comp**. Wenn dieses StyleBook ausgeführt wird, wird zuerst der lbvserver-comp erstellt. Der lb-sg-binding-comp bezieht sich auf die Eigenschaften von lbvserver-comp, kann aber nicht als Nächstes erstellt werden, obwohl er die zweite im StyleBook definierte Komponente ist. Das liegt daran, dass der lb-sg-binding-comp auch vom sg-comp abhängig ist, der noch erstellt werden muss. Infolgedessen ordnet der Compiler die Komponenten neu an, sodass die Abhängigkeiten einer Komponente zum Zeitpunkt der Erstellung einer Komponente aufgelöst sind, und führt diese neu geordnete Liste von Komponenten aus. Die Ausführungsreihenfolge des obigen StyleBooks ist: lbvserver-comp, sg-comp und lb-sg-binding-comp.

Daher muss sich der Autor eines StyleBook nicht um die korrekte Reihenfolge der Komponenten kümmern. Die Komponenten können in beliebiger Reihenfolge erscheinen. Der Compiler berechnet die korrekte Reihenfolge der Ausführung der Komponenten basierend darauf, wie die Komponenten einander verweisen. Beachten Sie, dass diese Abhängigkeitserkennung und Neuordnung auch für Substitutions- und Ausgabebereiche funktioniert.

Zyklische Abhängigkeiten

Da eine Komponente auf eine andere Komponente verweisen kann, ist es möglich, dass ein Abhängigkeitszyklus in die Definition des StyleBook eingeführt wird. Beispiel: Wenn Komponente A auf eine Eigenschaft verweist, die in Komponente B definiert ist, die wiederum auf eine Eigenschaft verweist, die in Komponente A definiert ist. Diese Art von Abhängigkeit wird als zyklische Abhängigkeiten bezeichnet. Zyklische Abhängigkeiten können nicht automatisch aufgelöst werden. Der Autor des StyleBook sollte die StyleBook-Definition manuell korrigieren, um solche zyklischen Abhängigkeiten zu beseitigen. Der Compiler kann zyklische Abhängigkeiten identifizieren - wenn sie existieren, und melden.

Das folgende Beispiel zeigt eine zyklische Abhängigkeit von Komponenten:

```
1  components:
```



```
2    -
3      name: lbvserver-comp
4      type: ns::lbvserver
5      properties:
6        name: $components.lb-sg-binding-comp.properties.name
7        ipv46: 10.102.190.15
8        port: 80
9        servicetype: HTTP
10   -
11     name: lb-sg-binding-comp
12     type: ns::lbvserver_servicegroup_binding
13     condition: $parameters.create-binding
14     properties:
15      name: mylb
16       servicegroupname: $components.sg-comp.properties.servicegroupname
17   -
18     name: sg-comp
19     type: ns::servicegroup
20     properties:
21       servicegroupname: mysg
22       servicetype: $components.lbvserver-comp.properties.servicetype
23 <!--NeedCopy-->
```

Im obigen Beispiel gibt es drei Komponenten: **lbvserver-comp, lb-sg-binding-comp und sg-comp. lbvserver-comp hängt**von **lb-sg-binding-comp ab, lb-sg-binding comp hängt von sg-comp**ab und **sg-comp hängt von lbvserver-comp**ab. Hier wird ein Zyklus von Abhängigkeiten zwischen diesen Komponenten gebildet, der nicht automatisch aufgelöst werden kann. Daher kann dieses StyleBook nicht ausgeführt werden. Der StyleBook-Compiler erkennt dies und verhindert, dass das StyleBook in NetScaler ADM importiert wird.

Instanzverwaltung

February 5, 2024

Instanzen sind Citrix Application Delivery Controller (ADC) -Appliances, die Sie mit NetScaler Application Delivery Management (ADM) verwalten, überwachen und beheben können. Sie müssen Instanzen zu Citrix ADM hinzufügen, um sie zu überwachen. Instanzen können hinzugefügt werden, wenn Sie Citrix ADM oder höher einrichten. Nachdem Sie NetScaler ADM Instanzen hinzugefügt haben, werden diese kontinuierlich abgefragt, um Informationen zu sammeln, die später zur Behebung von Problemen oder als Berichtsdaten verwendet werden können.

Instanzen können als statische Gruppe oder als privater IP-Block gruppiert werden. Eine statische Gruppe von Instanzen kann nützlich sein, wenn Sie bestimmte Aufgaben wie Konfigurationsaufträge usw. ausführen möchten. Ein privater IP-Block gruppiert Ihre Instanzen basierend auf ihren geografischen Standorten.

Eine Instanz hinzufügen

Sie können Instanzen hinzufügen, wenn Sie den NetScaler ADM-Server zum ersten Mal oder später einrichten. Um Instanzen hinzuzufügen, müssen Sie entweder den Hostnamen oder die IP-Adresse jeder NetScaler ADC-Instanz oder einen Bereich von IP-Adressen angeben.

Informationen zum Hinzufügen einer Instanz zu NetScaler ADM finden Sie unter Hinzufügen von Instanzen zu NetScaler ADM.

Wenn Sie dem NetScaler ADM -Server eine Instanz hinzufügen, fügt sich der Server implizit als Trap-Ziel für die Instanz hinzu und sammelt die Bestandsaufnahme der Instanz. Weitere Informationen finden Sie unter Wie NetScaler ADM Instanzen erkennt.

Nachdem Sie eine Instanz hinzugefügt haben, können Sie sie löschen, indem Sie zu "**Netzwerke**"> "**Dashboard** "navigieren und auf "**Alle Instanzen**"klicken. Wählen Sie auf der Seite Instanzen die Instanz aus, die Sie löschen möchten, und klicken Sie auf **Entfernen**.

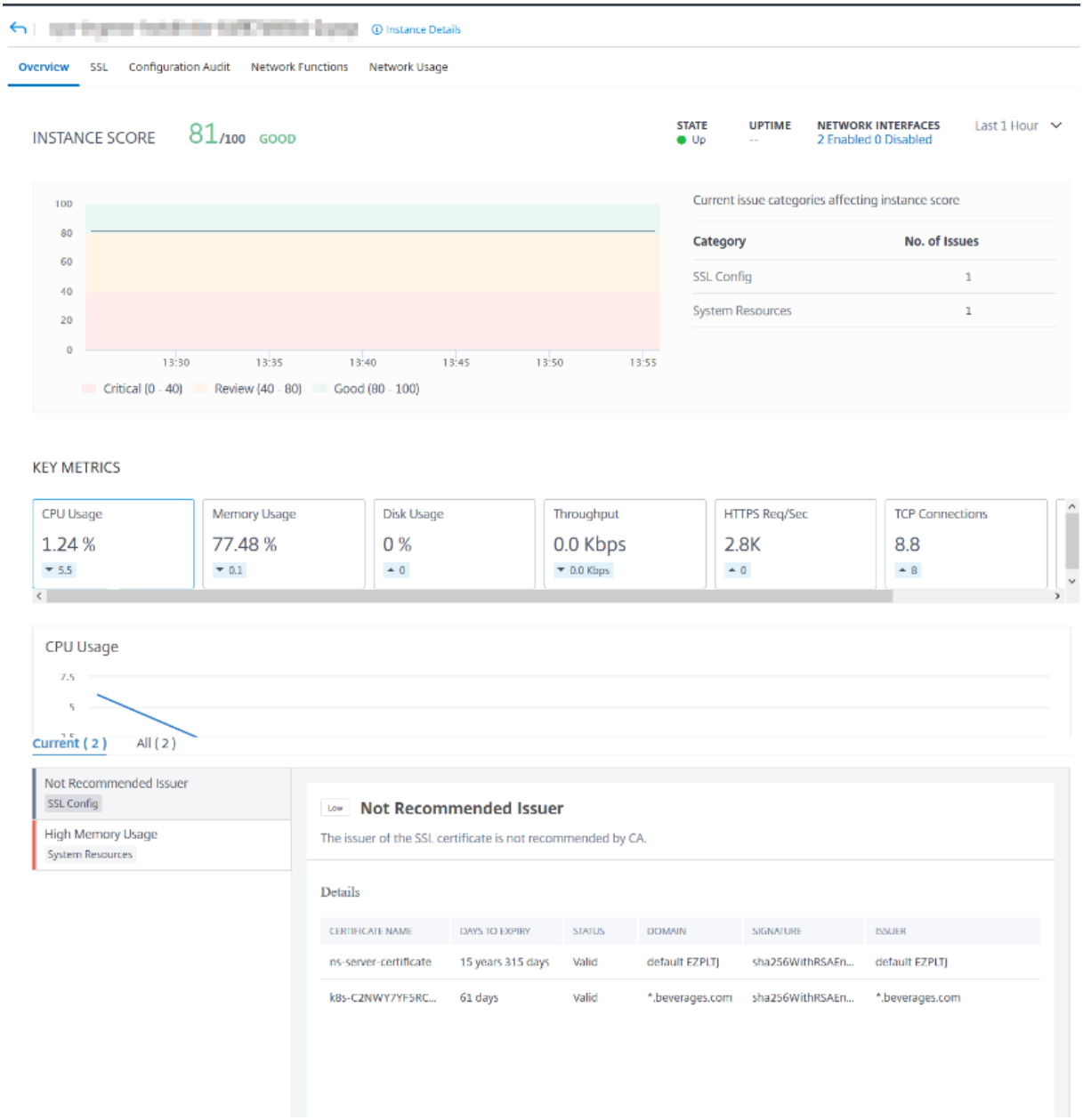
So verwenden Sie das Instanz-Dashboard

Das Instanzen-Dashboard in NetScaler ADM zeigt Daten in einem tabellarischen und grafischen Format für die ausgewählte Instanz an. Daten, die während des Abfragevorgangs von Ihrer Instanz gesammelt wurden, werden im Dashboard angezeigt.

Standardmäßig werden verwaltete Instanzen jede Minute zur Datenerfassung abgefragt. Statistische Informationen wie Status, HTTP-Anforderungen pro Sekunde, CPU-Auslastung, Speicherauslastung und Durchsatz werden kontinuierlich mithilfe von NITRO-Aufrufen erfasst. Als Administrator können Sie all diese gesammelten Daten auf einer einzigen Seite anzeigen, Probleme in der Instanz identifizieren und sofortige Maßnahmen ergreifen, um sie zu beheben.

Um das Dashboard einer bestimmten Instanz anzuzeigen, navigieren Sie zu **Netzwerke** > **Instanzen**. Wählen Sie in der Zusammenfassung den Instanztyp aus, wählen Sie dann die Instanz aus, die Sie anzeigen möchten, und klicken Sie auf **Dashboard**.

Die folgende Abbildung bietet einen Überblick über die verschiedenen Daten, die auf dem Instanz-Dashboard angezeigt werden:



- **Übersicht**. Die Registerkarte "Übersicht"zeigt die CPU- und Speicherauslastung der ausgewählten Instanz an. Sie können auch Ereignisse anzeigen, die von der Instanz generiert werden und die Durchsatzdaten. Instanzspezifische Informationen wie die IP-Adresse, die Hardware- und LOM-Versionen, die Profildetails, die Seriennummer, die Kontaktperson usw. werden hier ebenfalls angezeigt. Wenn Sie weiter nach unten scrollen, werden die lizenzierten Funktionen, die für die ausgewählte Instanz verfügbar sind, zusammen mit den darauf konfigurierten Modi.

  Weitere Informationen finden Sie unter Instanzdetails.

- **SSL-Dashboard**. Sie können die Registerkarte SSL im Dashboard für jede Instanz verwenden,

um die Details der SSL-Zertifikate, virtuellen SSL-Server und SSL-Protokolle Ihrer ausgewählten Instanz einzusehen oder zu überwachen. Sie können auf die „Zahlen“in den Grafiken klicken, um weitere Details anzuzeigen.

- **Prüfung der Konfiguration**. Sie können die Registerkarte Konfigurationsüberprüfung verwenden, um alle Konfigurationsänderungen anzuzeigen, die an der ausgewählten Instanz vorgenommen wurden. Die Diagramme für den**gespeicherten Status der NetScaler-Konfiguration** und die **Driftdiagramme der NetScaler-Konfiguration**auf dem Dashboard zeigen allgemeine Details zu Konfigurationsänderungen, die im Vergleich zu nicht gespeicherten Konfigurationen gespeichert wurden.
- **Netzwerk-Funktionen**. Mithilfe des Dashboards für Netzwerkfunktionen können Sie den Status der Entitäten überwachen, die auf der ausgewählten NetScaler ADC-Instanz konfiguriert sind. Sie können Diagramme für Ihre virtuellen Server anzeigen, in denen Daten wie Clientverbindungen, Durchsatz und Serververbindungen angezeigt werden.
- **Netzwerk-Nutzung**. Sie können die Netzwerkleistungsdaten für Ihre ausgewählte Instanz auf der Registerkarte Netzwerknutzung anzeigen. Sie können Berichte für eine Stunde, einen Tag, eine Woche oder einen Monat anzeigen. Die Zeitleisten-Schiebereglerfunktion kann verwendet werden, um die Dauer der zu generierenden Netzwerkberichte anzupassen. Standardmäßig werden nur acht Berichte angezeigt. Sie können jedoch auf das Plussymbol in der unteren rechten Ecke des Bildschirms klicken, um einen weiteren Leistungsbericht hinzuzufügen.

Global verteilte Standorte überwachen

February 5, 2024

Als Netzwerkadministrator müssen Sie möglicherweise Netzwerkinstanzen überwachen und verwalten, die über geografische Standorte verteilt sind. Es ist jedoch nicht einfach, die Anforderungen des Netzwerks bei der Verwaltung von Netzwerkinstanzen in geografisch verteilten Rechenzentren zu beurteilen.

Geomaps in NetScaler Application Delivery Management (ADM) bietet Ihnen eine grafische Darstellung Ihrer Sites und teilt die Netzwerküberwachung nach geografischer Herkunft auf. Mit Geomaps können Sie Ihre Netzwerkinstanzverteilung nach Standort visualisieren und Netzwerkprobleme überwachen.

Im folgenden Abschnitt wird erläutert, wie Sie Rechenzentren in NetScaler ADM überwachen können.

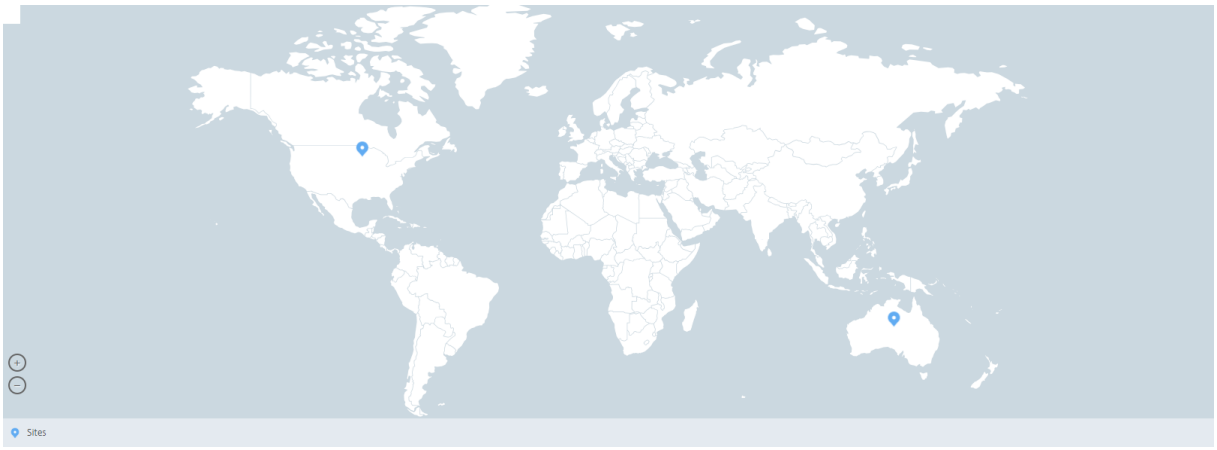
Die NetScaler ADM -Site ist eine logische Gruppierung von ADC-Instanzen (Citrix Application Delivery Controller) an einem bestimmten geografischen Standort. Zum Beispiel, während ein Standort

Amazon Web Services (AWS) zugewiesen ist und ein anderer Standort Azure™ zugewiesen sein kann. Noch eine andere Website wird auf dem Gelände des Mandanten gehostet. NetScaler ADM verwaltet und überwacht alle NetScaler ADC-Instanzen, die mit allen Standorten verbunden sind. Sie können NetScaler ADM verwenden, um Syslog, AppFlow, SNMP und alle derartigen Daten, die von den verwalteten Instanzen stammen, zu überwachen und zu sammeln.

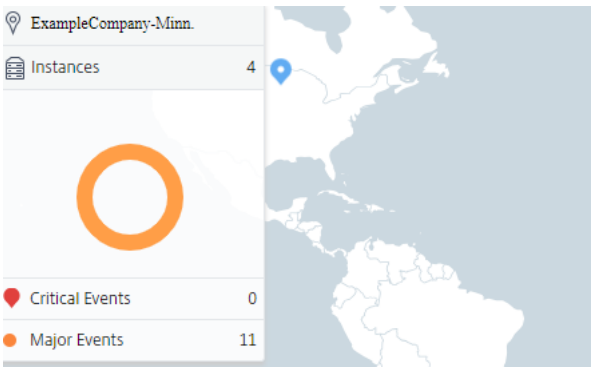
Geomaps in NetScaler ADM bieten Ihnen eine grafische Darstellung Ihrer Websites. Geomaps schlüsselt auch Ihre Netzwerküberwachungserfahrung nach Geografie auf. Mit Geomaps können Sie Ihre Netzwerkinstanzverteilung nach Standort visualisieren und alle Netzwerkprobleme überwachen. Sie können zur Seite "**Netzwerke** "> "**Dashboard** "navigieren, um eine visuelle Darstellung der auf der Weltkarte erstellten Websites zu erhalten.

Anwendungsfall

Ein führendes Mobilfunkanbieterunternehmen, ExampleCompany, verließ sich beim Hosten seiner Ressourcen und Anwendungen auf private Dienstleister. Das Unternehmen hatte bereits zwei Standorte - einen in Minneapolis in den USA und einen weiteren in Alice Springs in Australien. In diesem Bild sehen Sie, dass zwei Marker die beiden vorhandenen Standorte darstellen.

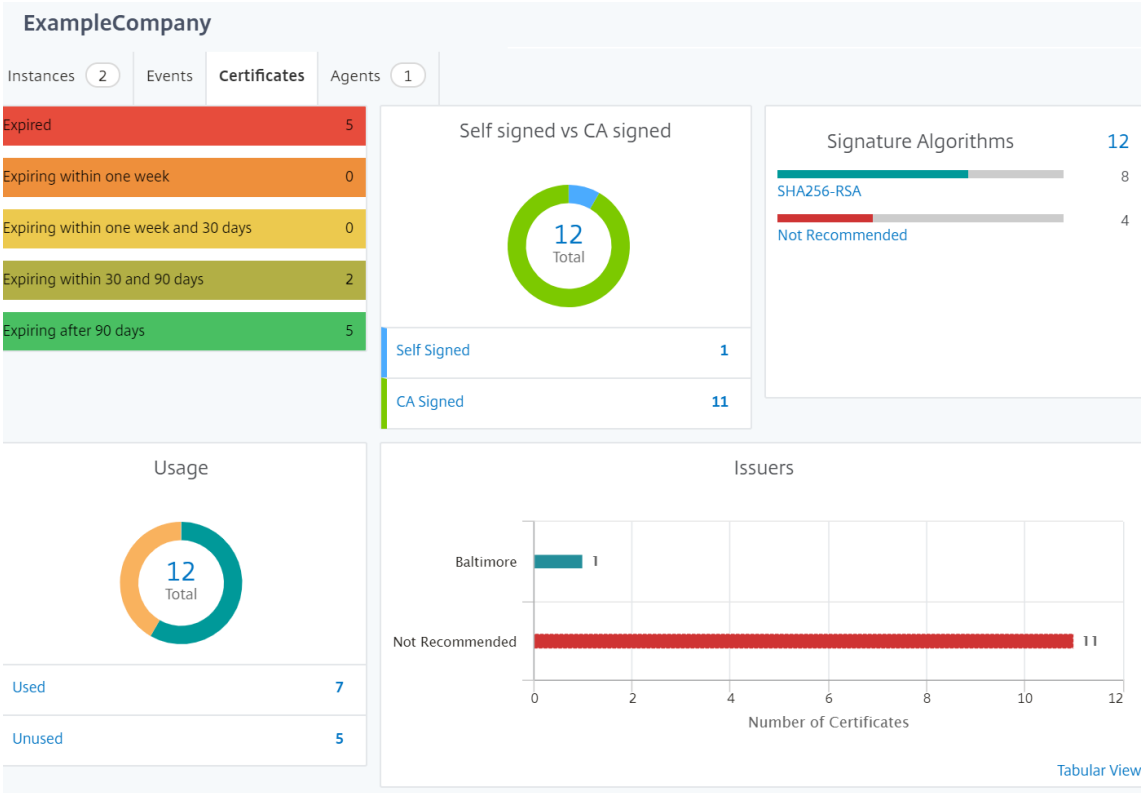


Die Marker zeigen auch eine Zahl an, die die Anzahl der Anwendungen an jedem Standort anzeigt. Sie können auf diese Marker klicken, um weitere Informationen zu den einzelnen Websites zu erhalten.



Klicken Sie auf die Registerkarten, um weitere Informationen anzuzeigen:

- Registerkarte “**Instanzen** “: Sehen Sie sich auf dieser Registerkarte Folgendes an:
  - IP-Adresse jeder Netzwerkinstanz
  - Typ der Instanz
  - Anzahl der kritischen Ereignisse auf ihnen
  - Bedeutende Ereignisse und alle Ereignisse, die auf einer NetScaler ADC-Instanz ausgelöst werden.
- Registerkarte**Ereignisse** : Zeigen Sie eine Liste kritischer und bedeutender Ereignisse an, die in den Instanzen ausgelöst wurden.
- Registerkarte**Zertifikate** : Sehen Sie sich auf dieser Registerkarte Folgendes an:
  - Liste der Zertifikate aller Instanzen
  - Ablauf-Status
  - Wichtige Informationen und die 10 wichtigsten Instanzen durch viele verwendete Zertifikate.
- Registerkarte **Agents**: Zeigt eine Liste der Agents an, an die die Instanzen gebunden sind.



Geomaps konfigurieren

ExampleCompany hat beschlossen, einen dritten Standort in Bangalore, Indien, einzurichten. Das Unternehmen wollte die Cloud testen, indem es einige seiner weniger kritischen, internen IT-Anwendungen an das Büro in Bangalore verlagerte. Das Unternehmen entschied sich für die Nutzung der AWS-Cloud-Computing-Services.

Als Administrator müssen Sie zuerst eine Site erstellen und anschließend die NetScaler ADC-Instanzen in NetScaler ADM hinzufügen. Sie müssen außerdem die Instanz zur Site hinzufügen, einen Agent hinzufügen und den Agent an die Site binden. NetScaler ADM erkennt dann den Standort, zu dem die NetScaler ADC-Instanz und der Agent gehören.

Weitere Informationen zum Hinzufügen von Citrix ADC-Instanzen finden Sie unter Hinzufügen von Instanzen .

So erstellen Sie Websites:

Erstellen Sie Sites, bevor Sie Instanzen in NetScaler ADM hinzufügen. Die Bereitstellung von Standortinformationen ermöglicht es Ihnen, den Standort genau zu lokalisieren.

Navigieren Sie zu **Netzwerke** > **Sites**, und klicken Sie dann auf **Hinzufügen**.

1. Geben Sie auf der Seite **Site erstellen** die folgenden Informationen an:

   a) **Standorttyp**: Wählen Sie **Rechenzentrum**aus.

   > **Hinweis**
   >
   > Der Standort kann als primäres Rechenzentrum oder als Zweigstelle fungieren. Wählen Sie entsprechend.

   b) **Typ**: Wählen Sie AWS als Cloud-Anbieter aus der Liste aus.

   > **Hinweis**
   >
   > Aktivieren Sie das Kontrollkästchen **Vorhandene VPC als Site verwenden** entsprechend.

   c) **Site-Name**: Geben Sie den Namen der Site ein.

   d) **Stadt**: Geben Sie die Stadt ein.

   e) **Postleitzahl**: Geben Sie die Postleitzahl ein.

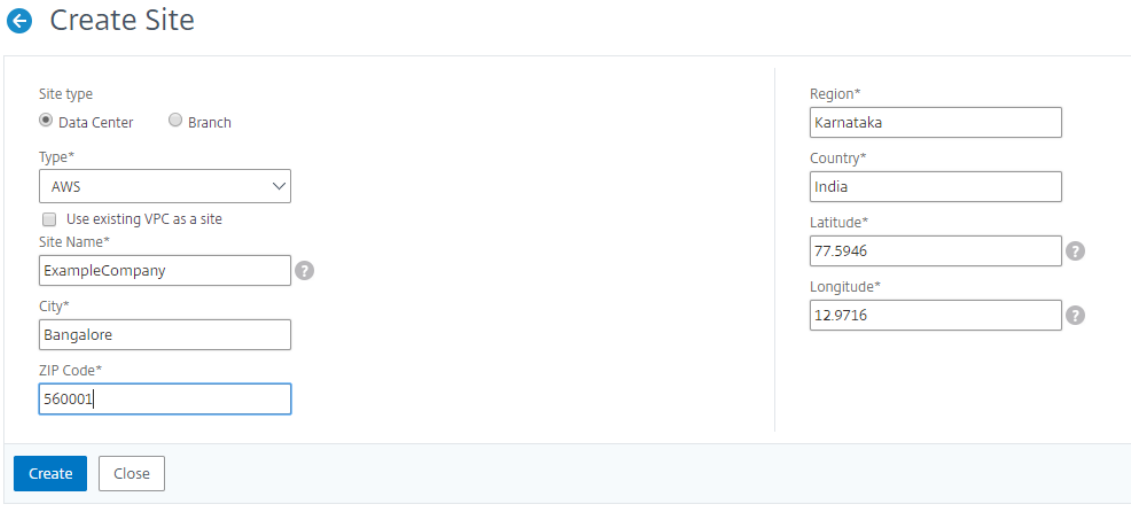
   f) **Region**: Geben Sie die Region ein.

   g) **Land**: Geben Sie das Land ein

   h) **Breitengrad**: Geben Sie den Breitengrad des Standorts ein.

i) **Längengrad**: Geben Sie den Längengrad der Position ein.

2. Klicken Sie auf **Erstellen**.

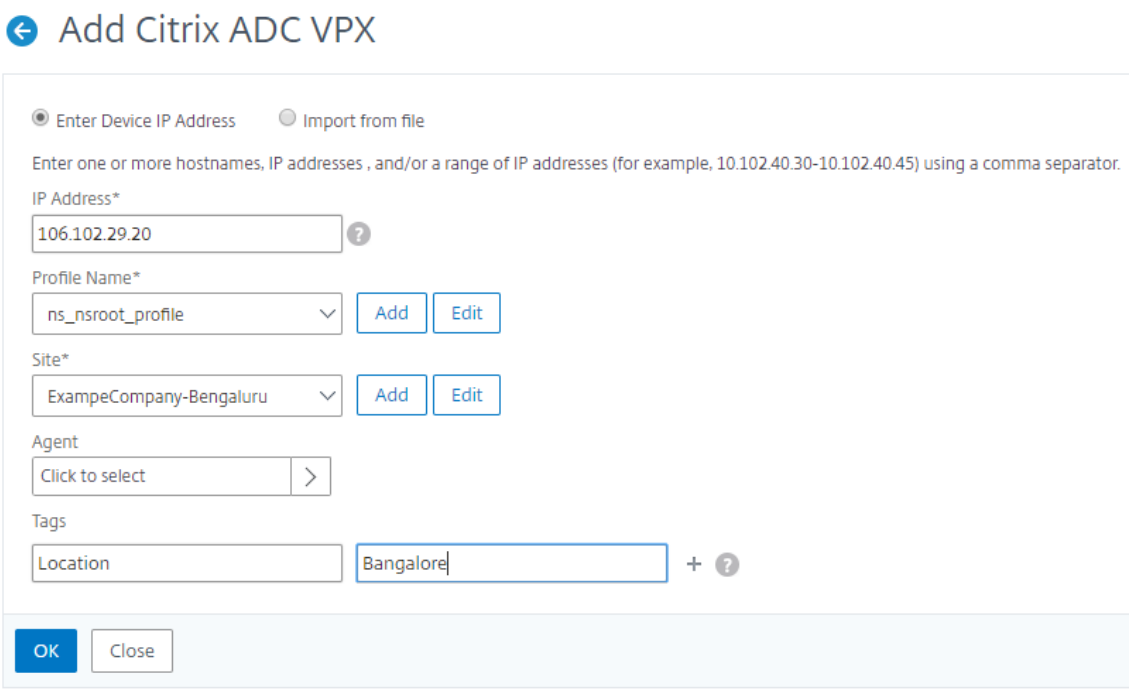


So fügen Sie Instanzen hinzu und wählen Sie Sites aus:

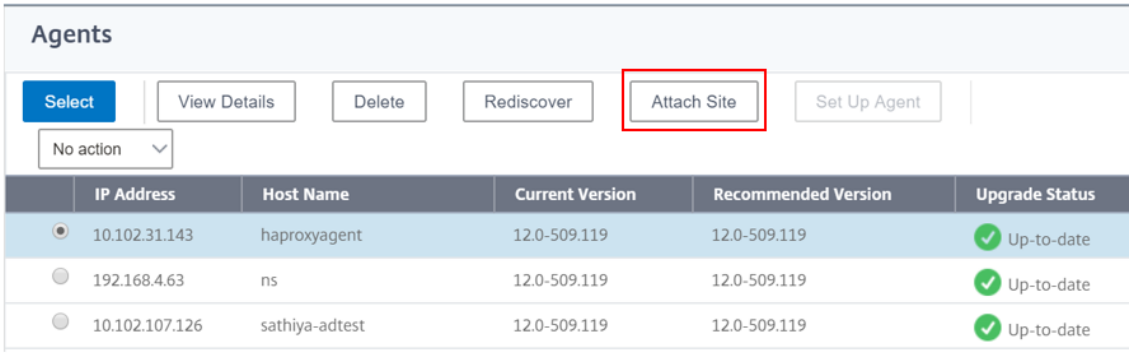
Nach dem Erstellen von Sites müssen Sie Instanzen in NetScaler ADM hinzufügen. Sie können die zuvor erstellte Site auswählen, oder Sie können auch eine Site erstellen und die Instanz zuordnen.

Nach dem Erstellen von Sites müssen Sie Instanzen in NetScaler ADM hinzufügen. Sie können die zuvor erstellte Site auswählen, oder Sie können auch eine Site erstellen und die Instanz zuordnen.

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen**.
2. Wählen Sie den Typ der Instanz aus, die Sie erstellen möchten, und klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **NetScaler ADC VPX hinzufügen** die IP-Adresse ein und wählen Sie das Profil aus der Liste aus.
4. Wählen Sie die Site aus der Liste aus. Sie können auf das Pluszeichen neben dem Feld **Site** klicken, um eine Site zu erstellen, oder auf das Bearbeitungssymbol klicken, um die Details der Standardwebsite zu ändern.
5. Klicken Sie auf den Pfeil nach rechts, und wählen Sie den Agent aus der angezeigten Liste aus.



6. Nachdem Sie den Agent ausgewählt haben, müssen Sie den Agent der Site zuordnen. In diesem Schritt kann der Agent an die Site gebunden werden. Wählen Sie den Agenten aus und klicken Sie auf **Site anhängen**.



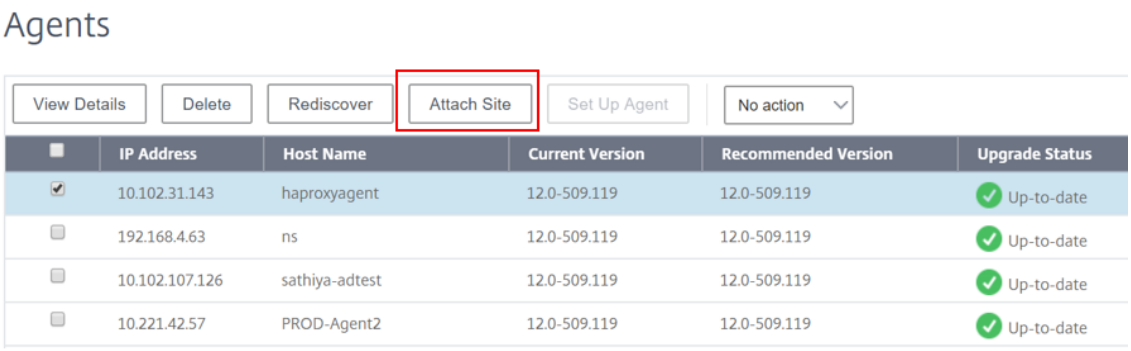
1. Wählen Sie die Website aus der Liste aus, und klicken Sie auf **Speichern**.

1. Klicken Sie auf **OK**.

Sie können einen Agenten auch an eine Site anhängen, indem Sie zu **Netzwerke** > **Agents** navigieren.

So verknüpfen Sie einen NetScaler ADM Agent mit der Site:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Agents**.
2. Wählen Sie den Agent aus, und klicken Sie auf **Site anhängen**.



1. Sie können die Website zuordnen und auf **Speichern**klicken.

NetScaler ADM beginnt mit der Überwachung der NetScaler ADC Instanzen, die in Bangalore-Standort hinzugefügt werden, zusammen mit den Instanzen an den beiden anderen Standorten.

Tags erstellen und Instanzen zuweisen

February 5, 2024

Mit Citrix Application Delivery Management (ADM) können Sie nun Ihre Citrix Application Delivery Controller (ADC) -Instanzen Tags zuordnen. Ein Tag ist ein Schlüsselwort oder ein aus einem Wort bestehendes Wort, das Sie einer Instanz zuweisen können. Die Tags fügen einige zusätzliche Informationen über die Instanz hinzu. Die Tags können als Metadaten betrachtet werden, die helfen, eine Instanz zu beschreiben. Mit Tags können Sie Instanzen anhand dieser spezifischen Schlüsselwörter klassifizieren und suchen. Sie können einer einzelnen Instanz auch mehrere Tags zuweisen.

Die folgenden Anwendungsfälle helfen Ihnen zu verstehen, wie das Tagging von Instanzen Ihnen hilft, diese besser zu überwachen.

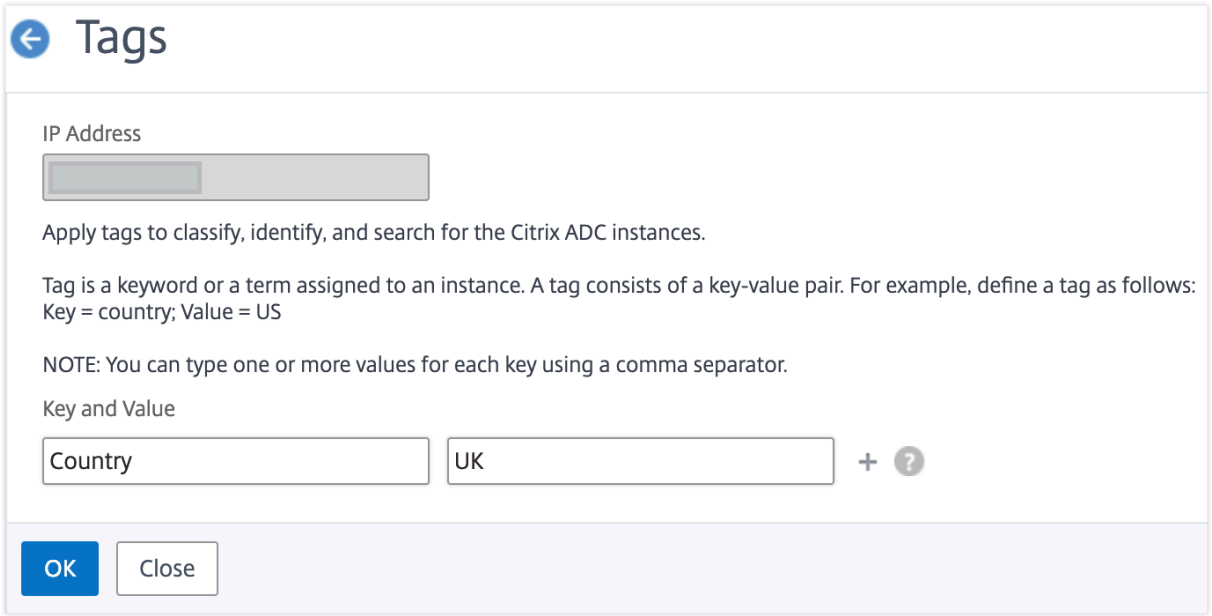
- **Anwendungsfall 1**: Sie können ein Tag erstellen, um alle Instanzen in Großbritannien zu identifizieren. Hier können Sie ein Tag mit dem Schlüssel “Country”und dem Wert als “UK”erstellen. Dieses Tag hilft Ihnen bei der Suche und Überwachung all dieser Instanzen in Großbritannien.
- **Anwendungsfall 2**: Sie möchten nach Instanzen suchen, die sich in der Stagingumgebung befinden. Hier können Sie ein Tag mit dem Schlüssel “Purpose”und dem Wert als “Staging_NS” erstellen. Mit diesem Tag können Sie alle Instanzen, die in der Stagingumgebung verwendet werden, von den Instanzen trennen, die Clientanforderungen durchlaufen.
- **Anwendungsfall 3**: Betrachten Sie eine Situation, in der Sie die Liste der NetScaler ADC-Instanzen herausfinden möchten, die sich im Bereich “Swindon”in Großbritannien befinden und Ihnen gehören. David T. Sie können Tags für all diese Anforderungen erstellen und diese allen Instanzen zuweisen, die diese Bedingungen erfüllen.

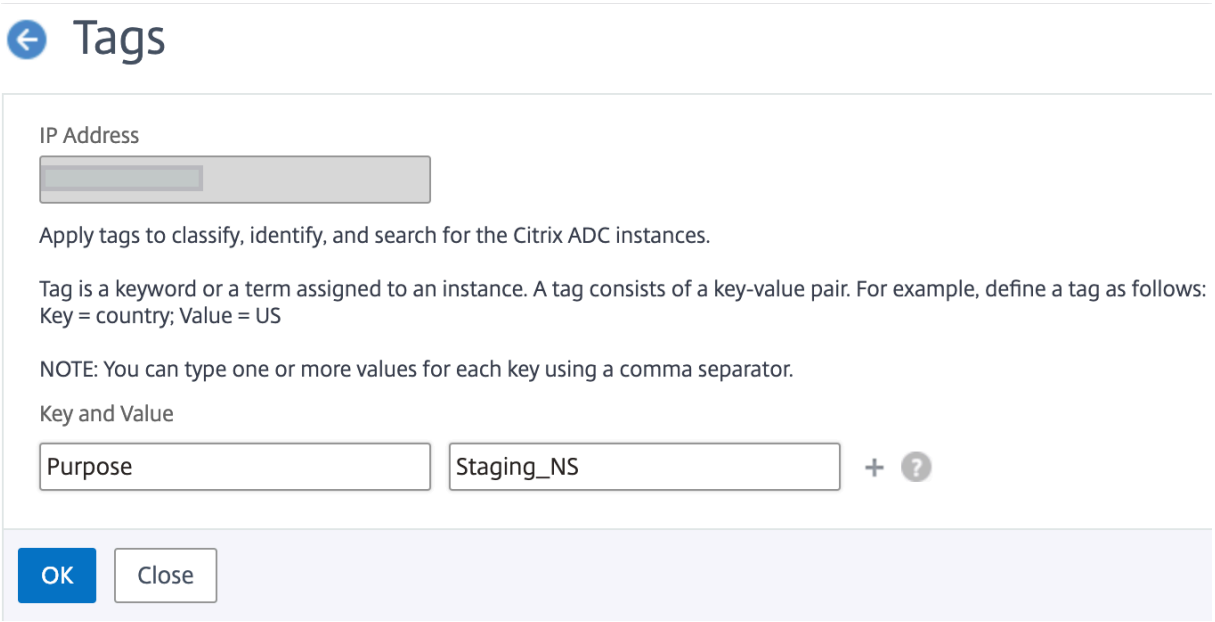
So weisen Sie der NetScaler ADC VPX Instanz Tags zu:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Wählen Sie die Registerkarte **NetScaler ADC VPX** aus.
3. Wählen Sie das erforderliche Citrix VPX aus.
4. Klicken Sie **auf Tags**.
5. Erstellen Sie Tags und klicken Sie auf **OK**.

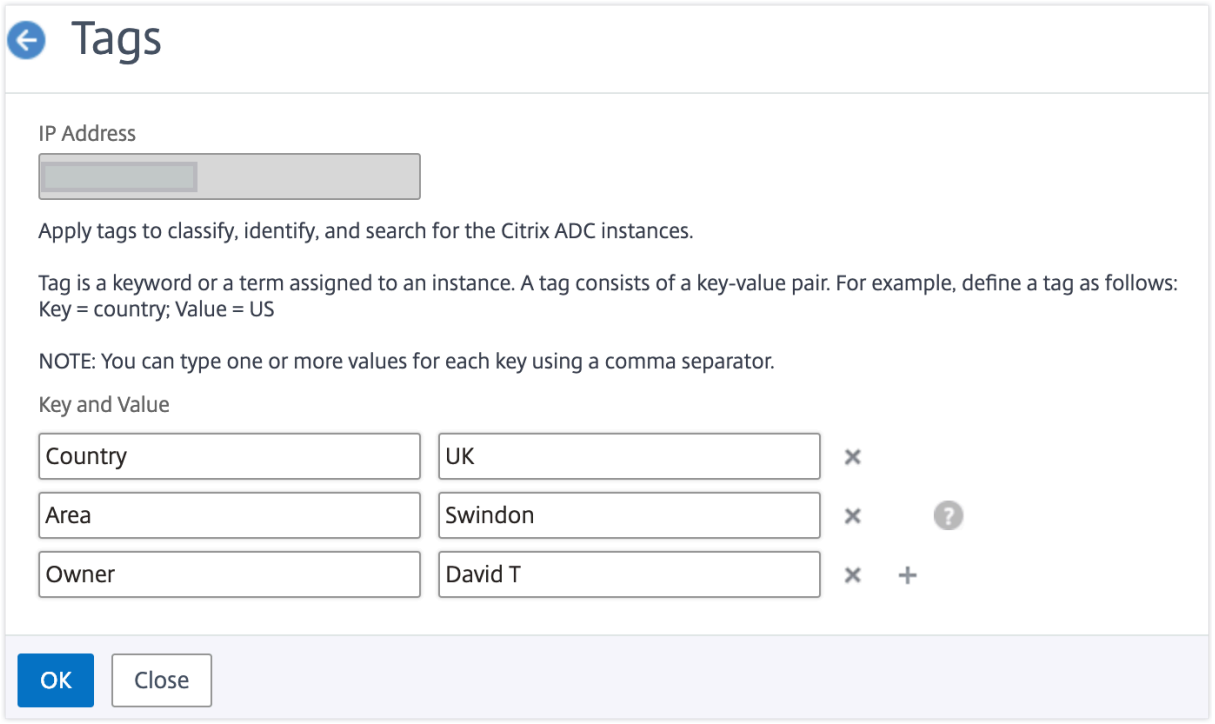
Im angezeigten **Tags-Fenster** können Sie Ihre eigenen "Schlüssel-Wert"-Paare erstellen, indem Sie jedem von Ihnen erstellten Schlüsselwort Werte zuweisen.

Die folgenden Bilder zeigen beispielsweise einige erstellte Keywords und deren Werte. Sie können eigene Schlüsselwörter hinzufügen und für jedes Schlüsselwort einen Wert eingeben.



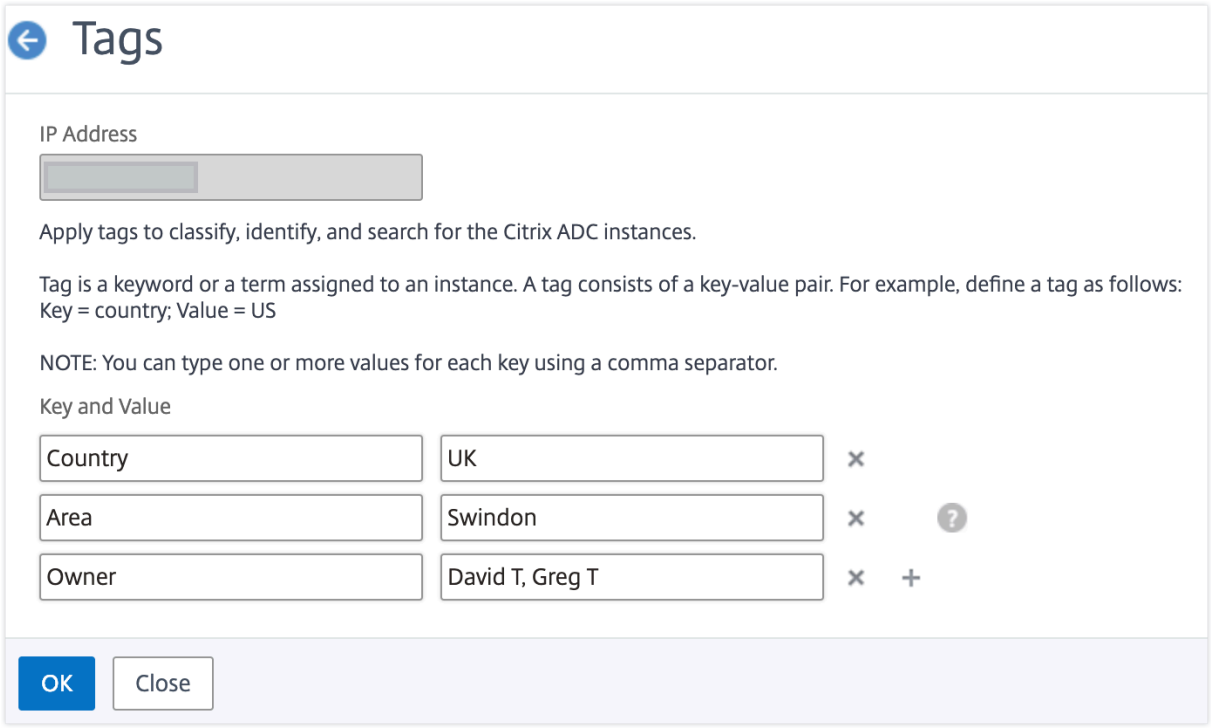


Sie können auch mehrere Tags hinzufügen, indem Sie auf “+”klicken. Durch das Hinzufügen mehrerer und aussagekräftiger Tags können Sie effizient nach den Instanzen suchen.



Sie können einem Schlüsselwort mehrere Werte hinzufügen, indem Sie sie durch Kommas trennen.

Sie weisen beispielsweise einem anderen Kollegen, Greg T., die Administratorrolle zu. Sie können seinen Namen durch ein Komma getrennt hinzufügen. Durch das Hinzufügen mehrerer Namen können Sie entweder nach den Namen oder nach beiden Namen suchen. NetScaler ADM erkennt die durch Kommas getrennten Werte in zwei verschiedene Werte.



Weitere Informationen zum Suchen nach Instanzen basierend auf Tags finden Sie unter Suchen von Instanzen mithilfe von Werten von Tags und Eigenschaften.

> **Hinweis**
>
> Sie können später neue Tags hinzufügen oder vorhandene Tags löschen. Es gibt keine Einschränkung für die Anzahl der Tags, die Sie erstellen.

Instanzen über Werte von Tags und Eigenschaften suchen

February 5, 2024

Es könnte eine Situation geben, in der NetScaler Application Delivery Management (ADM) viele NetScaler ADC-Instanzen verwaltet. Als Administrator möchten Sie möglicherweise die Flexibilität, die Instanzinventar anhand bestimmter Parameter zu durchsuchen. NetScaler ADM bietet jetzt eine verbesserte Suchfunktion, um eine Teilmenge von NetScaler ADC-Instanzen basierend auf den Parametern zu durchsuchen, die Sie im Suchfeld definieren. Sie können anhand von zwei Kriterien —Tags und Eigenschaften —nach den Instanzen suchen.

- **Tags**. Tags sind Begriffe oder Schlüsselwörter, die Sie einer NetScaler ADC-Instanz zuweisen können, um eine zusätzliche Beschreibung der NetScaler ADC-Instanz hinzuzufügen. Sie können Ihre NetScaler ADC-Instanzen nun Tags zuordnen. Diese Tags können verwendet werden,

um die NetScaler ADC-Instanzen besser zu identifizieren und zu suchen.

- **Eigenschaften**. Jede NetScaler ADC-Instanz, die in NetScaler ADM hinzugefügt wird, verfügt über einige Standardparameter oder Eigenschaften, die dieser Instanz zugeordnet sind. Zum Beispiel hat jede Instanz ihren eigenen Hostnamen, ihre IP-Adresse, ihre Version, ihre Host-ID, ihre Hardwaremodell-ID und so weiter. Sie können nach Instanzen suchen, indem Sie Werte für jede dieser Eigenschaften angeben.

Betrachten Sie beispielsweise eine Situation, in der Sie die Liste der NetScaler ADC-Instanzen ermitteln möchten, die sich auf Version 12.0 befinden und sich im UP Status befinden. Hier werden die Version und der Status der Instanz durch die Standardeigenschaften definiert.

Neben der Version 12.0 und dem UP-Status der Instanzen können Sie auch die Instanzen durchsuchen, die Ihnen gehören. Sie können ein Owner -Tag erstellen und diesem Tag einen Wert David T zuweisen. Weitere Informationen zum Erstellen und Zuweisen von Tags finden Sie unter Erstellen von Tags und Zuweisen zu Instanzen.

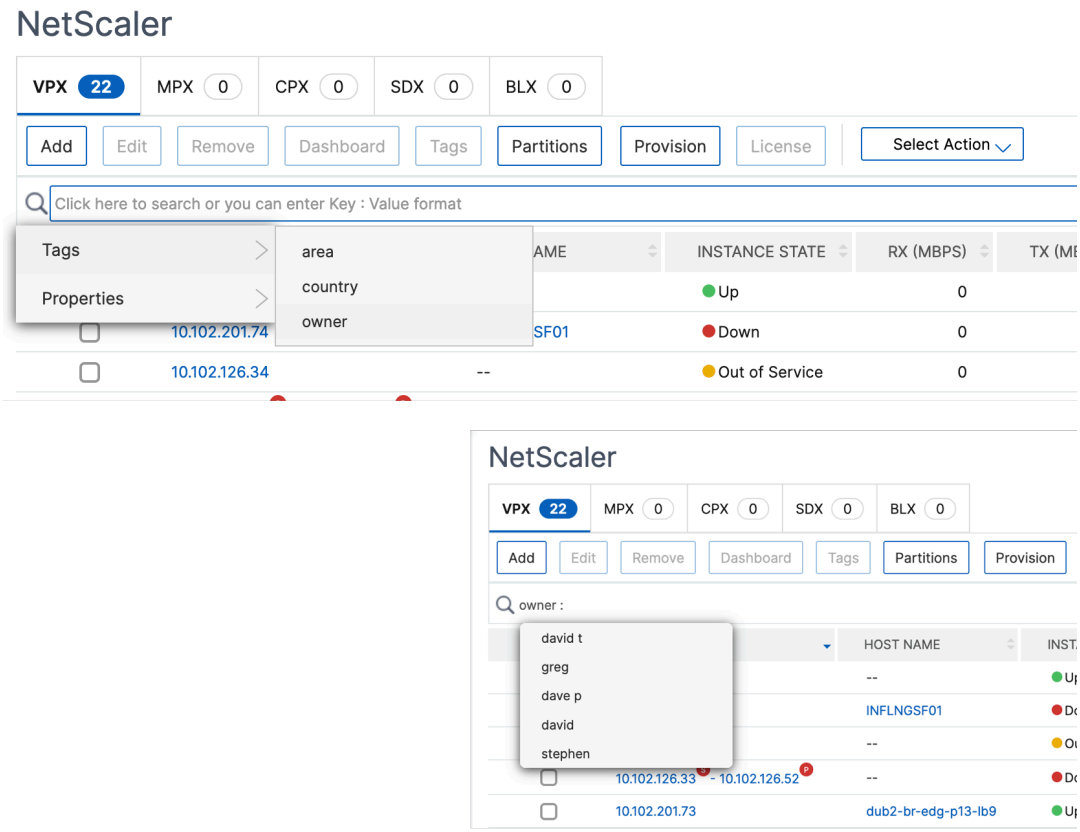
Sie können eine Kombination aus Tags und Eigenschaften verwenden, um eigene Suchkriterien zu erstellen.

So suchen Sie nach NetScaler ADC VPX Instanzen

1. Navigieren Sie in NetScaler ADM zur Registerkarte **Netzwerke** > **Instanzen** > **NetScaler ADC** > **VPX**.
2. Klicken Sie auf das Suchfeld. Sie können einen Suchausdruck erstellen, indem Sie Tags oder Eigenschaften verwenden oder beide kombinieren.

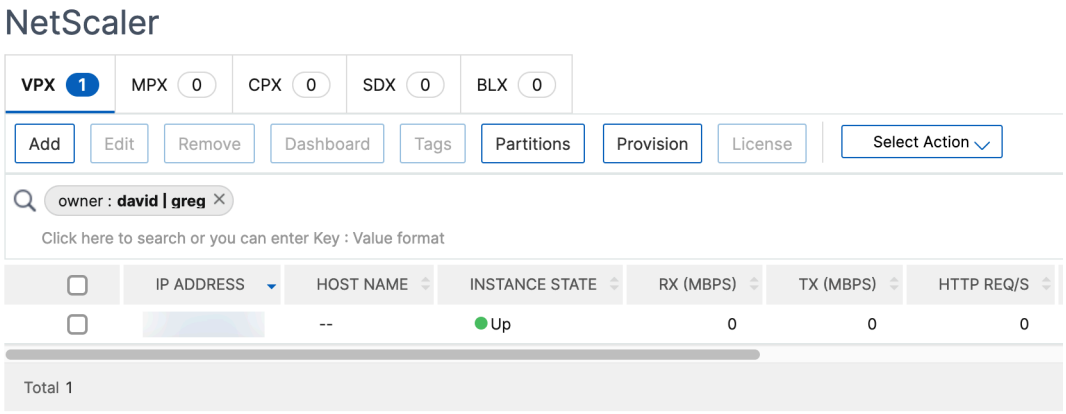
   Die folgenden Beispiele zeigen, wie Sie den Suchausdruck effizient verwenden können, um nach der Instanz zu suchen.

   a) Wählen Sie die Option **Tags** und dann **Besitzer**aus. Wählen Sie “David T.”

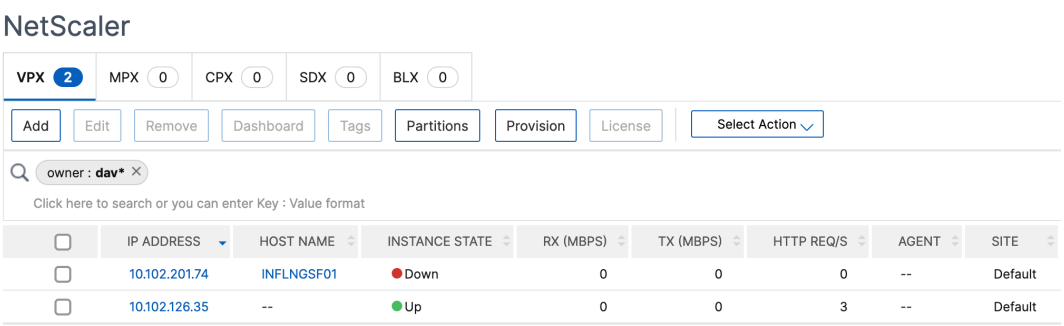


NetScaler ADM unterstützt reguläre Ausdrücke und Platzhalterzeichen in den Suchausdrücken.

b) Sie können reguläre Ausdrücke verwenden, um die Suchkriterien weiter zu erweitern. Sie möchten beispielsweise Instanzen suchen, die entweder David oder Stephen gehören. In einem solchen Fall können Sie die Werte eingeben, indem Sie die Werte durch einen |-Ausdruck trennen.



c) Sie können auch Platzhalterzeichen verwenden, um ein oder mehrere Zeichen zu ersetzen oder darzustellen. Sie können beispielsweise Dav* nach allen Instanzen suchen, die David T und Dave P gehören.



> **Hinweis**
>
> Weitere Informationen zu regulären Ausdrücken und Platzhalterzeichen sowie deren Verwendung finden Sie in der Suchleiste auf das Symbol Informationen.

Adminpartitionen von NetScaler ADC-Instanzen verwalten

February 5, 2024

Sie können Admin-Partitionen auf Ihren Citrix Application Delivery Controller Instanzen (ADC) so konfigurieren, dass verschiedenen Gruppen in Ihrer Organisation unterschiedliche Partitionen auf derselben Citrix ADC Instanz zugewiesen werden. Ein Netzwerkadministrator kann zugewiesen werden, um mehrere Partitionen auf mehreren Citrix ADC Instanzen zu verwalten.

Citrix Application Delivery Management (ADM) bietet eine nahtlose Möglichkeit, alle Partitionen eines Administrators von einer einzigen Konsole aus zu verwalten. Sie können diese Partitionen verwalten, ohne andere Partitionskonfigurationen zu stören.

Damit mehrere Benutzer verschiedene Admin-Partitionen verwalten können, müssen Sie Gruppen erstellen und dann Benutzer und Partitionen diesen Gruppen zuweisen. Jeder Benutzer kann nur die Partitionen in der Gruppe anzeigen und verwalten, zu der der Benutzer gehört. Jede Admin-Partition wird in NetScaler ADM als Instanz betrachtet. Wenn Sie eine NetScaler ADC-Instanz entdecken, werden die für diese NetScaler ADC-Instanz konfigurierten Adminpartitionen automatisch dem System hinzugefügt.

Beachten Sie, dass Sie zwei Citrix VPX-Instanzen mit zwei Partitionen für jede Instanz konfiguriert haben. Beispielsweise hat die NetScaler ADC Instanz 10.102.216.49 Partition_1, Partition_2 und Partition_3, und die NetScaler ADC-Instanz 10.102.29.120 hat p1 und p2, wie in der folgenden Abbildung gezeigt.

Um die Partitionen anzuzeigen, navigieren Sie zu**Netzwerke > Instanzen > NetScaler ADC > VPX**, und klicken Sie dann auf **Partitionen**.

Sie können user-p1 die folgenden Partitionen zuweisen: 10.102.29.120-p1 und 10.102.216.49-Partition_1. Und Sie können user-p2 der Verwaltung der Partitionen 10.102.29.80-p2, 10.102.216.49-Partition_2 und 10.102.216.49-Partition_3 zuweisen.

Dann müssen Sie die beiden Benutzer user-p1 und user-p2 erstellen und die Benutzer den Gruppen zuweisen, die Sie für sie erstellt haben.

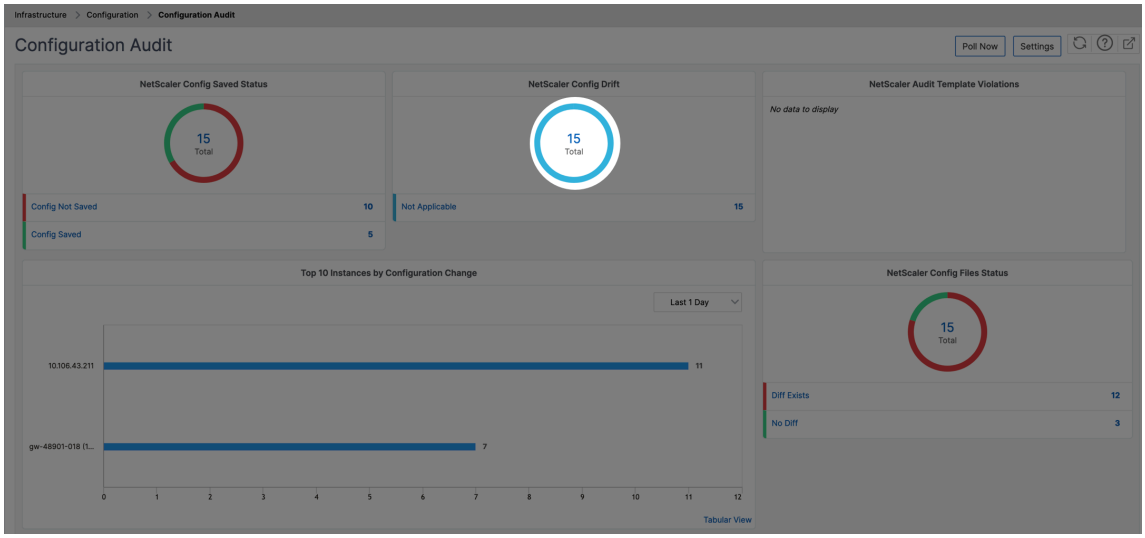
Zunächst müssen Sie zwei Gruppen mit entsprechenden Berechtigungen erstellen (Beispiel: Administratorberechtigungen) und die erforderlichen Admin-Partitionsinstanzen in jede Gruppe aufnehmen. Erstellen Sie beispielsweise Systemgruppenpartition1-admin und fügen Sie der Gruppe Citrix ADC Administratorpartitionen 10.102.29.120-p1 und 10.102.216.49-Partition_1 hinzu. Erstellen Sie außerdem Systemgruppenpartition2-admin und fügen Sie Citrix ADC Administratorpartitionen 10.102.29.120-p2, 10.102.216.49-Partition_2 und 10.102.216.49-Partition_3 und dieser Gruppe hinzu.

Nachdem Sie die Admin-Partition erstellt haben, können Sie zu Prüfungszwecken auch die Funktion zum Unterschied des Versionsverlaufs und die Funktion Auditvorlage für die Admin-Partition verwenden.

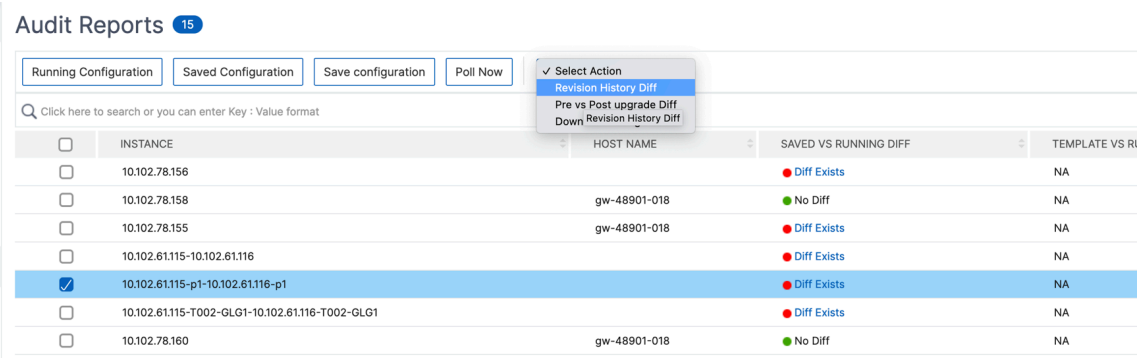
Der Unterschied zwischen den fünf neuesten Konfigurationsdateien für eine partitionierte Citrix ADC Instanz ermöglicht es Ihnen, den Unterschied zwischen den fünf neuesten Konfigurationsdateien anzuzeigen. Sie können die Konfigurationsdateien miteinander vergleichen (Beispiel Configuration Revision —1 mit Configuration Revision -2) oder mit der aktuell laufenden/gespeicherten Konfiguration mit Configuration Revision. Neben den Unterschieden in der Konfiguration werden auch die Korrekturkonfigurationen angezeigt. Sie können alle Korrekturbefehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.

So zeigen Sie die Differenz der Versionshistorie an:

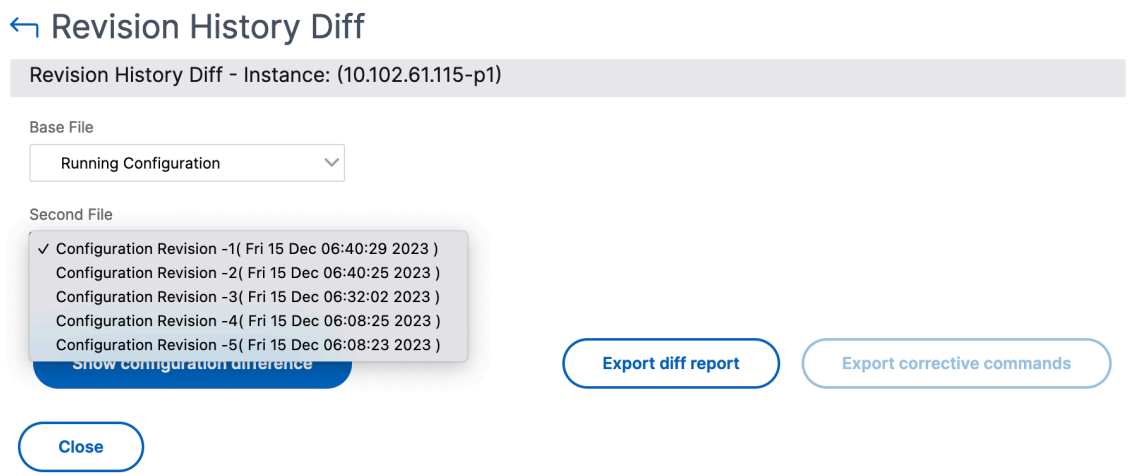
1. **Navigieren Sie zu Netzwerke > Configuration Audit.** Klicken Sie in das Donutdiagramm, das den Status der Instanzkonfiguration darstellt. Klicken Sie auf der Seite **Überwachungsberichte**, die geöffnet wird, auf die partitionierte NetScaler ADC Instanz.



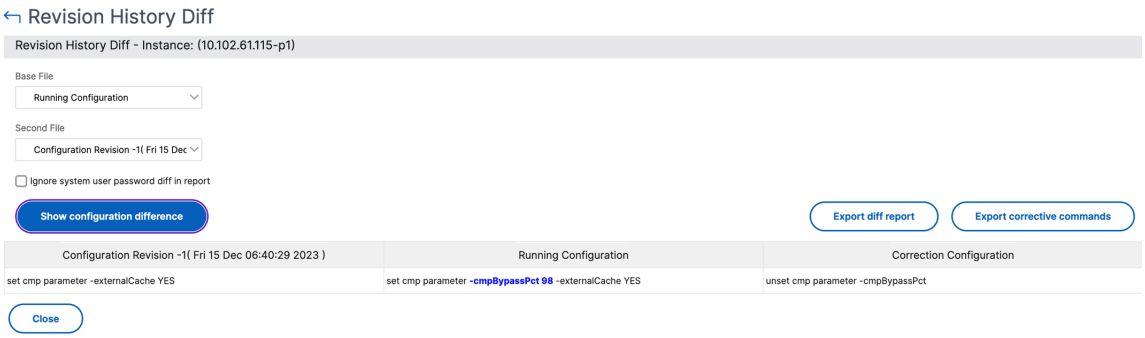
2. Klicken Sie im Menü **Aktion** auf **Versionsverlauf Diff.**



3. Wählen Sie auf der Seite **Versionsverlauf-Diff** die Dateien aus, die Sie vergleichen möchten. Vergleichen Sie beispielsweise die gespeicherte Konfiguration mit der Konfigurationsversion -1, und klicken Sie dann auf **Konfigurationsdifferenz anzeigen**.



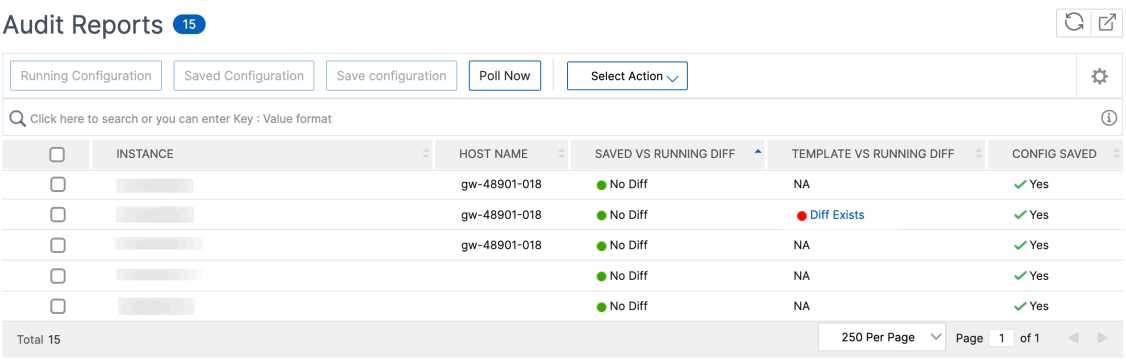
4. Sie können dann den Unterschied zwischen den fünf neuesten Konfigurationsdateien für die ausgewählte partitionierte NetScaler ADC Instanz anzeigen, wie unten gezeigt. Sie können auch die Korrekturkonfigurationsbefehle anzeigen und diese Korrekturbefehle in Ihren lokalen Ordner exportieren. Diese Korrekturbefehle sind die Befehle, die für die Basisdatei ausgeführt werden müssen, um die Konfiguration in den gewünschten Zustand zu bringen (Konfigurationsdatei, die zum Vergleich verwendet wird).



Überwachungsvorlagen für die Partition ermöglichen es Ihnen, eine benutzerdefinierte Konfigurationsvorlage zu erstellen und sie einer Partitionsinstanz zuzuordnen. Jede Variation in der laufenden Konfiguration der Instanz mit der Audit-Vorlage wird in der Spalte „ **Template vs. Running Diff** “auf der Seite „ **Auditberichte** “angezeigt. Neben den Unterschieden in der Konfiguration werden auch die Korrekturkonfigurationen angezeigt. Sie können auch alle Korrekturbefehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.

So zeigen Sie die Vorlage im Vergleich zu den laufenden Differenzen an:

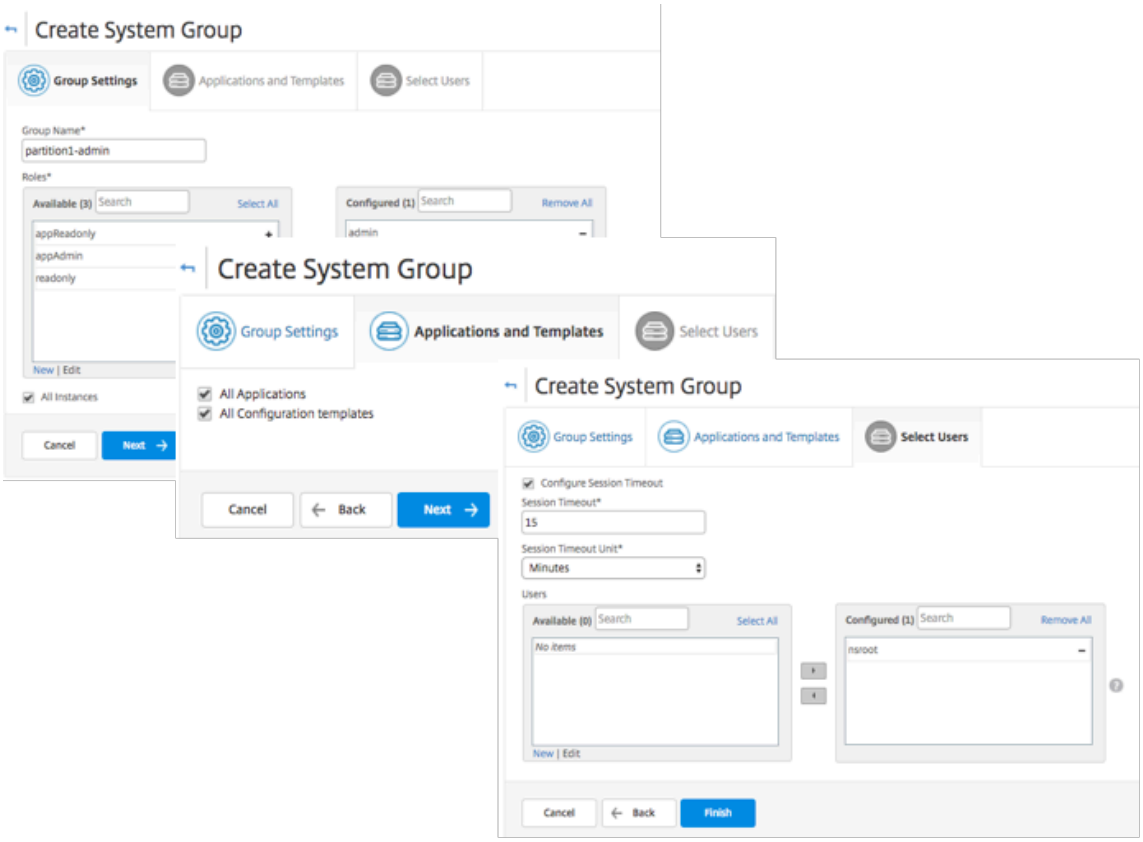
1. Klicken Sie auf der Seite “**Audit-Berichte** “auf die partitionierte NetScaler ADC-Instanz.



2. Wenn zwischen der Audit-Vorlage und der laufenden Differenz ein Unterschied besteht, wird die Differenz als Hyperlink angezeigt. Klicken Sie auf den Hyperlink, um die Unterschiede anzuzeigen, falls vorhanden. Neben den Unterschieden in der Konfiguration werden auch die Korrekturkonfigurationen angezeigt. Sie können auch alle Korrekturbefehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.

So erstellen Sie Gruppen:

1. Navigieren Sie zu **System > User Administration > Groups**, und klicken Sie dann auf **Hinzufügen**.
2. Geben **Sie auf der Seite "Systembenutzer erstellen** "Folgendes an:
   - Registerkarte „**Gruppeneinstellungen** ": Geben Sie den Gruppennamen und die Rollenberechtigungen ein. Um den Zugriff auf bestimmte Instances zu ermöglichen, deaktivieren Sie das Kontrollkästchen**All Instances**und wählen Sie dann Ihre Instances auf der Seite **Select Instances aus** .
   - Registerkarte „**Anwendungen und Vorlagen** ": Sie können wählen, ob Sie diese Gruppe für alle Anwendungen und Konfigurationsvorlagen verwenden möchten.
   - Registerkarte**Benutzer auswählen** : Wählen Sie Benutzer aus, die Sie dieser Gruppe hinzufügen möchten. Sie können auf den Link **Neu** in der Tabelle **Verfügbar** klicken, um neue Benutzer zu erstellen. Konfigurieren Sie optional das Sitzungstimeout, in dem Sie den Zeitraum konfigurieren können, wie lange ein Benutzer aktiv bleiben kann.
3. Klicken Sie auf **Fertig stellen**.



So erstellen Sie Benutzer:

1. Navigieren Sie zu**System > User Administration > Users**und klicken Sie dann auf **Add**.

2. Geben Sie auf der Seite "**Systembenutzer erstellen**"den Benutzernamen und das Kennwort an. Optional können Sie die externe Authentifizierung aktivieren und das Sitzungs-Timeout konfigurieren.
3. Weisen Sie den Benutzer einer Gruppe zu, indem Sie den Gruppennamen aus der Liste**Verfügbar zur**Liste**Konfiguriert**hinzufügen.
4. Klicken Sie auf **Erstellen**.

Melden Sie sich jetzt ab und melden Sie sich mit Benutzer-p1-Anmeldeinformationen an. Sie können nur die Admin-Partitionen anzeigen und verwalten, die Ihnen zur Verwaltung und Überwachung zugewiesen sind.

NetScaler ADC Hochverfügbarkeitspaar erstellen

January 23, 2024

Ein Citrix ADC Hochverfügbarkeitspaar (HA) kann bei Ausfallzeiten oder Netzwerkausfällen einen unterbrechungsfreien Betrieb gewährleisten. Sie können ein HA-Paar von ADC-Instanzen mit NetScaler ADM erstellen. Weitere Informationen finden Sie unter NetScaler ADC Hochverfügbarkeit.

Führen Sie die folgenden Schritte aus, um ein HA-Paar von ADC-Instanzen in NetScaler ADM zu erstellen:

1. Navigieren Sie zu **Netzwerke > Instanzen > NetScaler ADC**.
2. Wählen Sie eine ADC-Instanz aus der Liste aus, mit der Sie ein HA-Paar erstellen möchten.

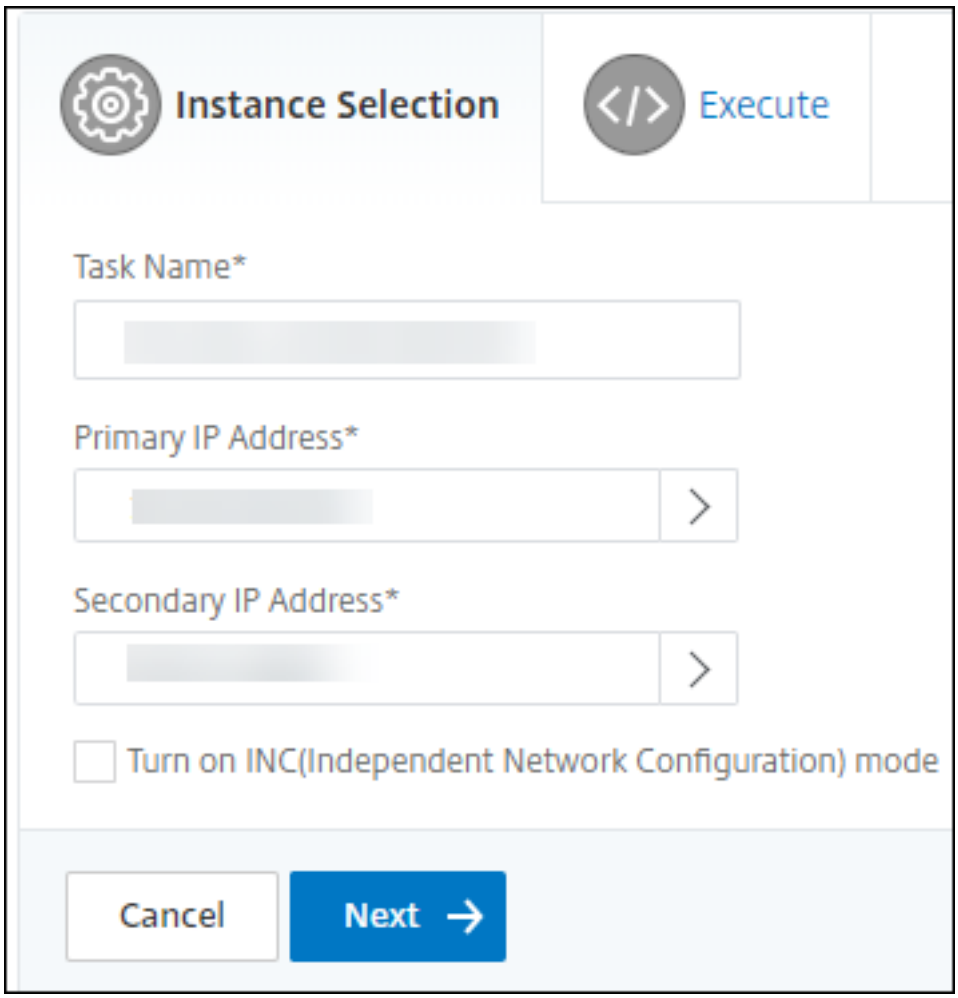
   Die ausgewählte Instanz wird zu einer primären Instanz im HA-Paar.
3. Klicken Sie auf **Aktion auswählen > HA-Paar erstellen**.
4. Führen Sie unter **Instanzauswahl**die folgenden Schritte aus:

   a) Klicken Sie unter **Sekundäre IP-Adresse**, um eine sekundäre Instanz auszuwählen.

   b) Wählen Sie eine ADC-Instanz aus, die Sie als sekundäre Instanz im HA-Paar konfigurieren möchten.

   c) Wählen Sie optional **den INC-Modus (Independent Network Configuration) aktivieren**, wenn die Instanzen des HA-Paars in zwei Subnetzen sind.

   d) Klicken Sie auf **Weiter**.



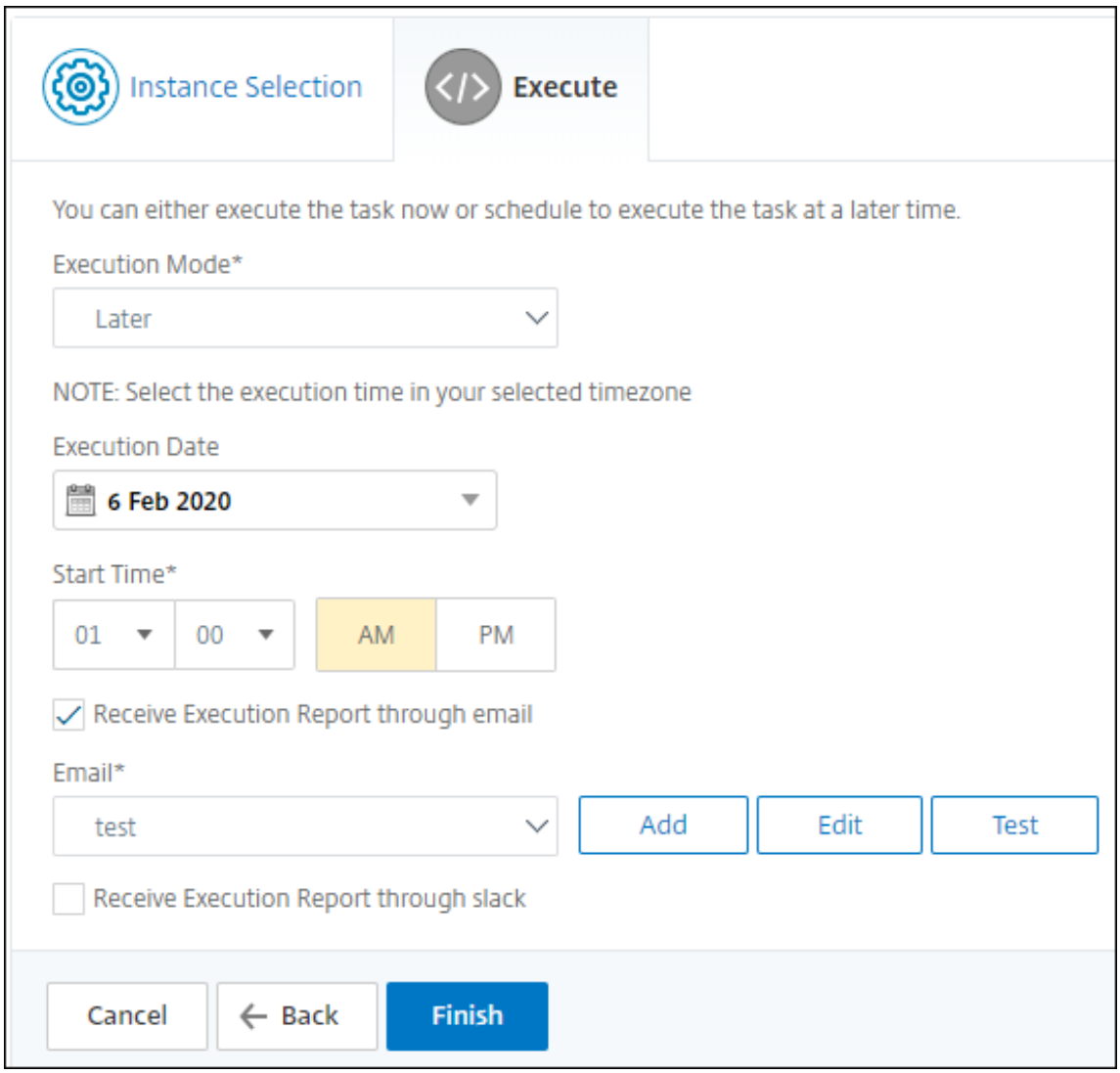
5. In **Execute**können Sie entscheiden, ob Sie jetzt oder zu einem späteren Zeitpunkt ein HA-Paar erstellen möchten.

   a) Wählen Sie im **Ausführungsmodus**einen der folgenden Ausführungsmodi aus:

   - **Jetzt** —Wählen Sie diese Option, um jetzt ein HA-Paar zu erstellen.
   - **Später** - Wählen Sie diese Option, um ein HA-Paar zu einem bestimmten Datum und einer bestimmten Uhrzeit zu erstellen.

   b) Wenn Sie **Später** in der Liste **Ausführungsmodus** ausgewählt haben, wählen Sie **Ausführungsdatum** und **Startzeit** aus, wenn Sie diesen Task ausführen möchten.

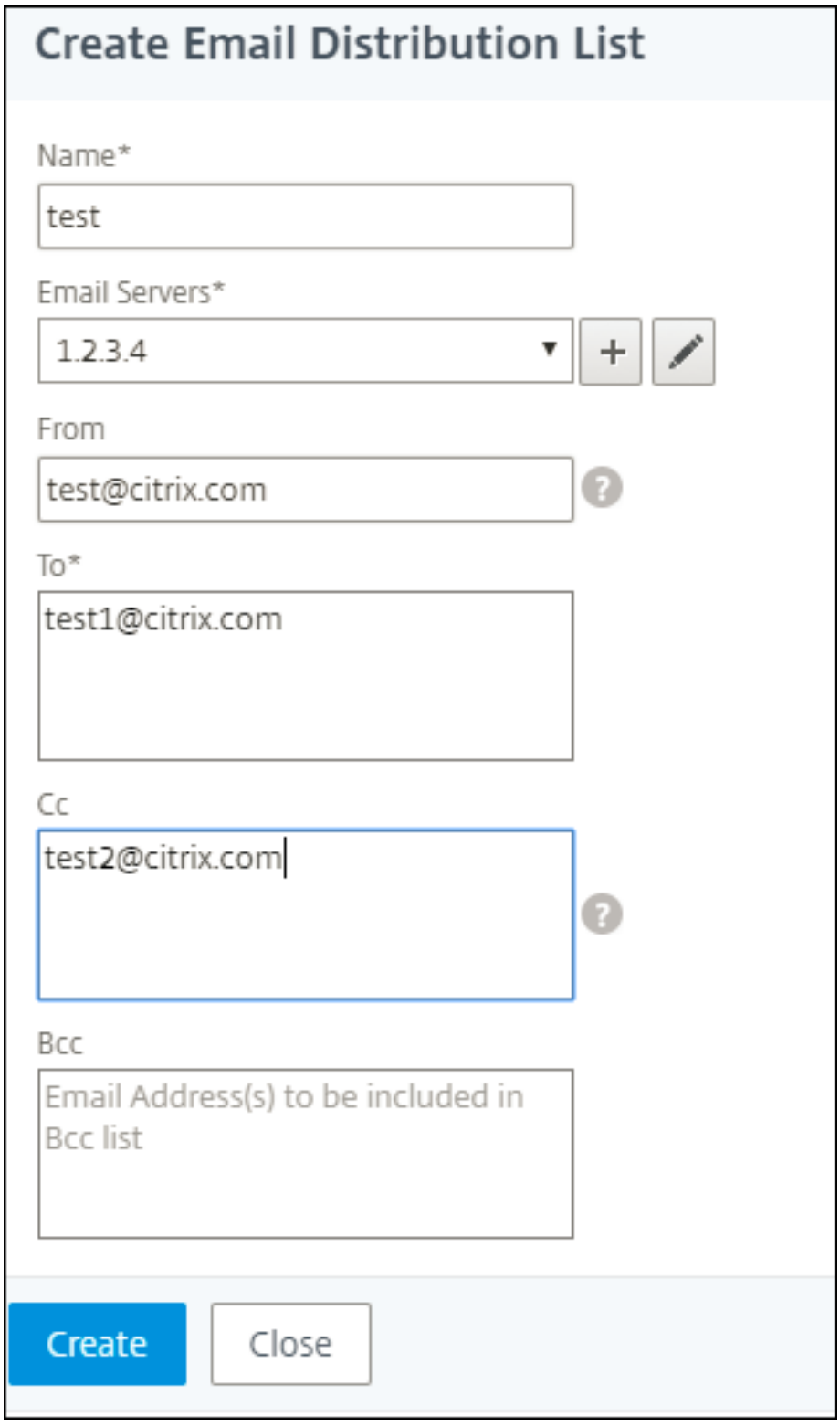
   > **Hinweis**
   >
   > Die Ausführungszeit wird in der Zeitzone angezeigt, die in NetScaler ADM festgelegt ist.



Sie können einen Ausführungsbericht dieser Aufgabe über Folgendes erhalten:

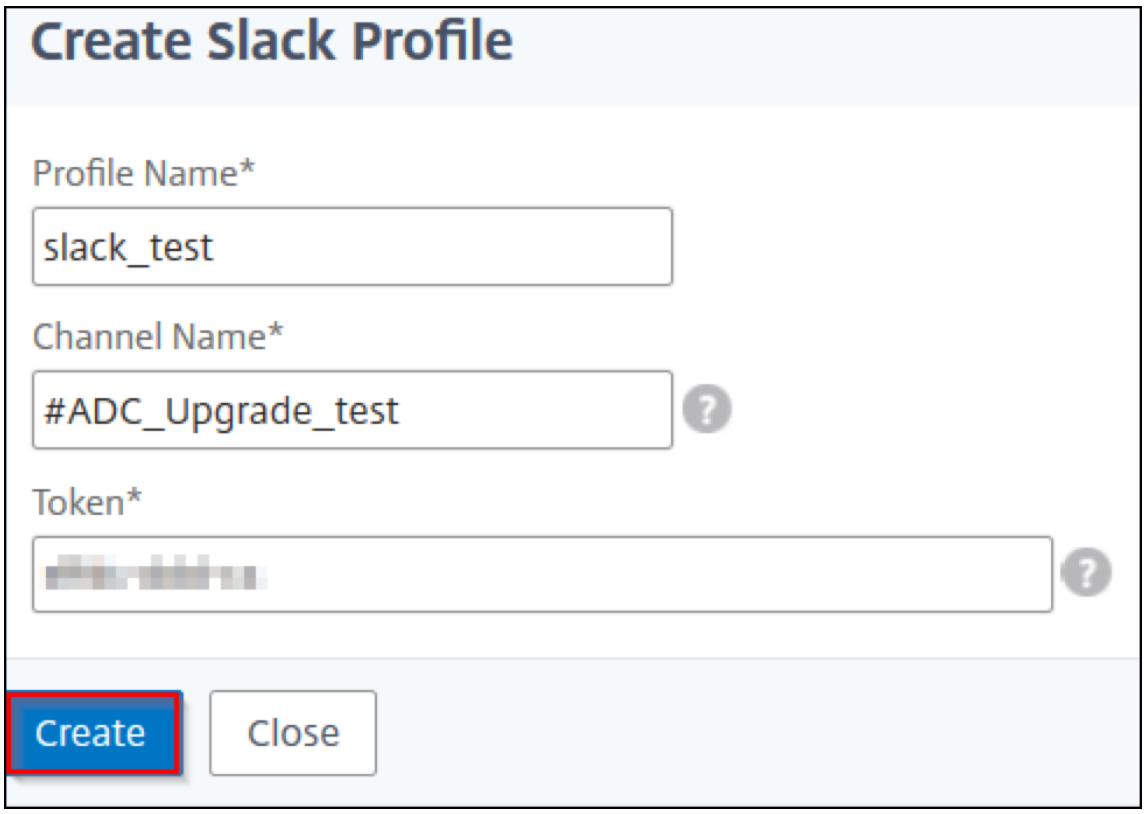
- **E-Mail** —Wählen Sie den E-Mail-Versand aus der Liste aus.

  Um eine Verteilerliste hinzuzufügen, klicken Sie auf **Hinzufügen**. Geben Sie die erforderlichen Parameter an, um die Verteilerliste hinzuzufügen, und klicken Sie auf **Erstellen**.



- **Slack** —Wähle das Slack-Profil aus der Liste aus.

  Um ein Slack-Profil hinzuzufügen, klicken Sie auf **Hinzufügen**. Geben Sie den **Profilnamen**, den **Kanalnamen**und das **Token** an und klicken Sie auf **Erstellen**.



Backup und Wiederherstellen von NetScaler ADC-Instanzen

February 5, 2024

Sie können den aktuellen Status einer NetScaler ADC Instanz sichern und später die gesicherten Dateien verwenden, um sie in demselben Zustand wiederherzustellen. Erstellen Sie immer ein Backup einer Instance, bevor Sie sie aktualisieren oder aus Vorsichtsgründen. Backup eines stabilen Systems ermöglicht es Ihnen, es wieder zu einem stabilen Punkt wiederherzustellen, wenn es instabil wird.

Es gibt mehrere Möglichkeiten, Backups und Wiederherstellungen auf einer NetScaler ADC-Instanz durchzuführen. Sie können manuell ein Backup der NetScaler ADC Konfigurationen mit der GUI und der CLI anlegen und es wiederherstellen. Sie können Citrix ADM auch verwenden, um automatische Backups und manuelle Wiederherstellungen durchzuführen.

NetScaler ADM sichert den aktuellen Status der verwalteten NetScaler ADC-Instanzen mithilfe von NITRO -Aufrufen und der Secure Shell (SSH) und Secure Copy (SCP) Protokolle.

NetScaler ADM erstellt ein vollständiges Backup und stellt die folgenden NetScaler ADC-Instanztypen wieder her:

- Citrix SDX
- Citrix VPX
- Citrix MPX
- Citrix BLX

Weitere Informationen finden Sie unter Sichern und Wiederherstellen einer ADC-Instanz .

> **Hinweis**
>
> - Stellen Sie sicher, dass das NetScaler ADM-Profil Administratorzugriff auf das Backup und Wiederherstellen von ADC-Instanzen hat.
> - Von NetScaler ADM aus können Sie den Backup- und Wiederherstellungsvorgang auf einem NetScaler ADC Cluster nicht ausführen.
> - Sie können die Backupdatei aus einer Instanz nicht verwenden, um eine andere Instanz wiederherzustellen.

Die gesicherten Dateien werden als komprimierte TAR-Datei im folgenden Verzeichnis gespeichert:

```
/var/mps/tenants/root/device_backup/
<!--NeedCopy-->
```

Um Probleme aufgrund der Nichtverfügbarkeit von Speicherplatz zu vermeiden, können Sie in diesem Verzeichnis maximal 50 Backupdateien pro ADC-Instanz speichern.

Um NetScaler ADC-Instanzen zu sichern und wiederherzustellen, müssen Sie zunächst die Backupeinstellungen auf NetScaler ADM konfigurieren. Nach dem Konfigurieren der Einstellungen können Sie eine einzelne NetScaler ADC Instanz oder mehrere Instanzen auswählen und ein Backup der Konfigurationsdateien in diesen Instanzen erstellen. Bei Bedarf können Sie die Citrix ADC Instanzen auch mithilfe dieser gesicherten Dateien wiederherstellen.

Konfigurieren der Einstellungen für das Instanzbackup

Auf der Seite **Instanz Backup Settings** können Sie Einstellungen in NetScaler ADM konfigurieren, um eine ausgewählte NetScaler ADC Instanz oder mehrere Instanzen zu sichern:

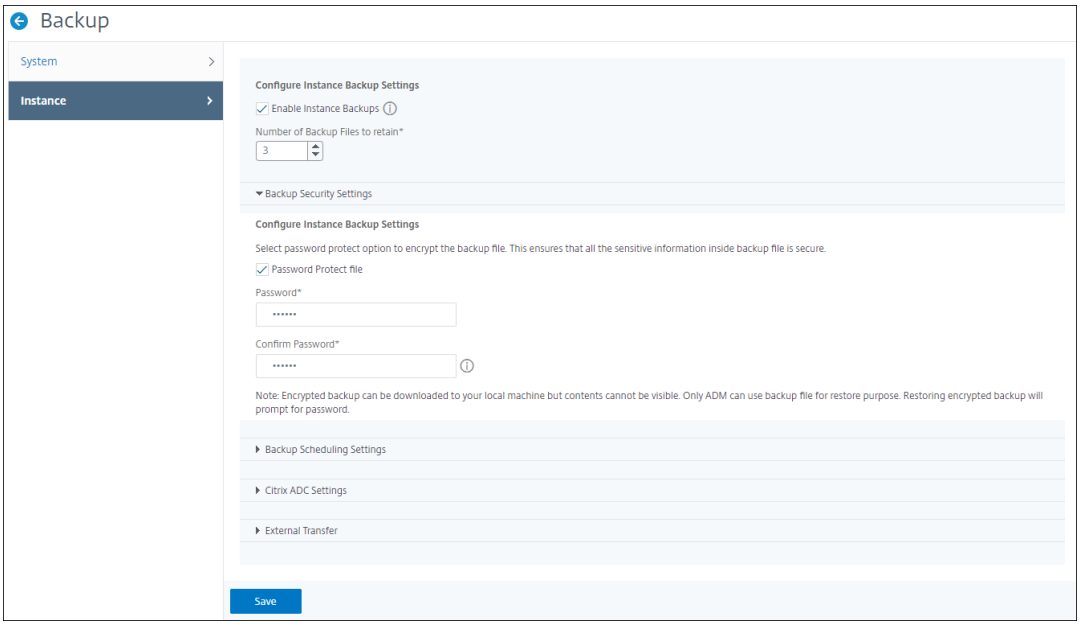
1. Navigieren Sie in Citrix ADM zu **System** > **Administration**.
2. Wählen Sie unter **Backup** die Option **System- und Instanz-Backup konfigurieren** aus.
3. Wählen Sie **Instance** aus und geben Sie Folgendes an:
    - **Instanzbackup aktivieren**: NetScaler ADM ist standardmäßig für das Erstellen von Backups von NetScaler ADC Instanzen aktiviert. Deaktivieren Sie diese Option, wenn Sie keine Sicherungsdateien für die Instanzen erstellen möchten.

- **Kennwortschutzdatei**: (optional) Wählen Sie die Kennwortschutzoption aus, um die Backupdatei zu verschlüsseln. Durch die Verschlüsselung der Sicherungsdatei wird sichergestellt, dass alle vertraulichen Informationen in der Sicherungsdatei sicher sind.

  > **Hinweis**
  >
  > Sie können die verschlüsselte Backupdatei auf Ihren lokalen Computer herunterladen, Sie können die Datei jedoch weder mit NetScaler ADM GUI noch mit einem Texteditor öffnen. Beim Wiederherstellen der verschlüsselten Backupdatei werden Sie aufgefordert, das Kennwort anzugeben. Sie können jedoch eine unverschlüsselte Sicherungsdatei auf Ihrem System öffnen.

- **Anzahl der beizubehaltenden Backupdateien**: Geben Sie die Anzahl der Backupdateien an, die in NetScaler ADM aufbewahrt werden sollen. Sie können bis zu 50 Backup-Dateien pro ADC-Instance aufbewahren. Der Standardwert ist drei Backupdateien.

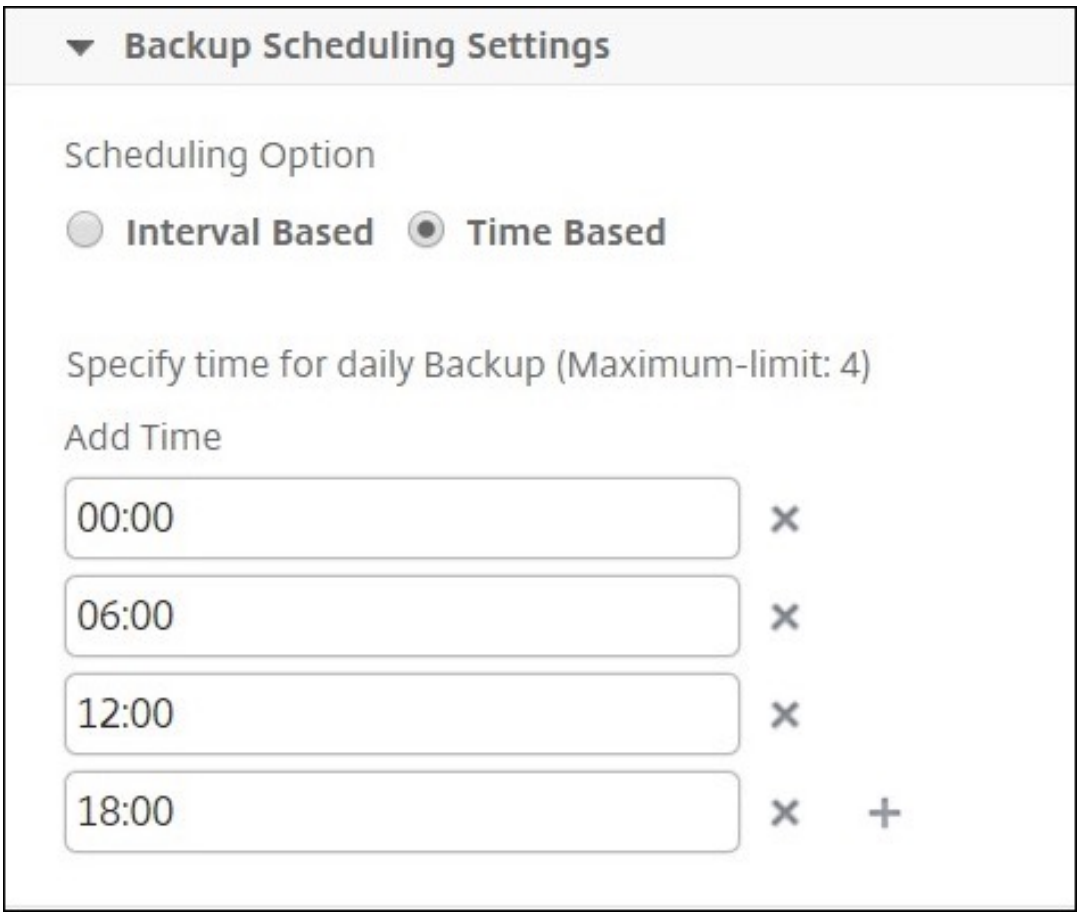
  > **Hinweis**
  >
  > Jede Sicherungsdatei entspricht einem gewissen Speicherbedarf. Citrix empfiehlt, dass Sie gemäß Ihren Anforderungen eine optimale Anzahl von NetScaler ADC -Backupdateien auf NetScaler ADM speichern.



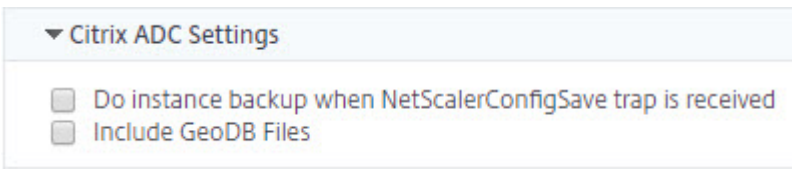
- **Einstellungen für die Backupplanung**: (optional) Zum Erstellen von Backupdateien stehen zwei Optionen zur Verfügung, obwohl Sie jeweils nur eine Option verwenden können:

  a) Die Standardoption für die Backupplanung ist “intervalbasiert”. Nach Ablauf des angegebenen Intervalls wird in Citrix ADM eine Backupdatei erstellt. Das Standardintervall für Backups ist 12 Stunden.

b) Sie können auch den Typ der geplanten Backups in “zeitbasiert”ändern. Geben Sie in dieser Option die Uhrzeit im `hours:minutes` Format an, um Instanzen zur angegebenen Zeit zu sichern. Mit NetScaler ADM können maximal vier tägliche Backups auf den Instanzen durchgeführt werden.



- **NetScaler ADC Einstellungen**: (optional) Standardmäßig erstellt NetScaler ADM keine Backupdatei, wenn das Trap “NetScalerConfigSave”empfängt. Sie können jedoch die Option zum Erstellen einer Backupdatei aktivieren, wenn eine Citrix ADC Instanz eine “NetScalerConfigSave”-Trap an Citrix ADM sendet. Eine Citrix ADC Instanz sendet “NetScalerConfigSave”jedes Mal, wenn die Konfiguration auf der Instanz gespeichert wird.
- **Geodatabase-Dateien**: (optional) Standardmäßig werden die GeoDatabase-Dateien von Citrix ADM nicht gespeichert. Sie können die Option aktivieren, um ein Backup dieser Dateien auch zu erstellen.



- **Externe Übertragung:**(optional) Mit NetScaler ADM können Sie die Backupdateien der NetScaler ADC Instanz an einen externen Speicherort übertragen:

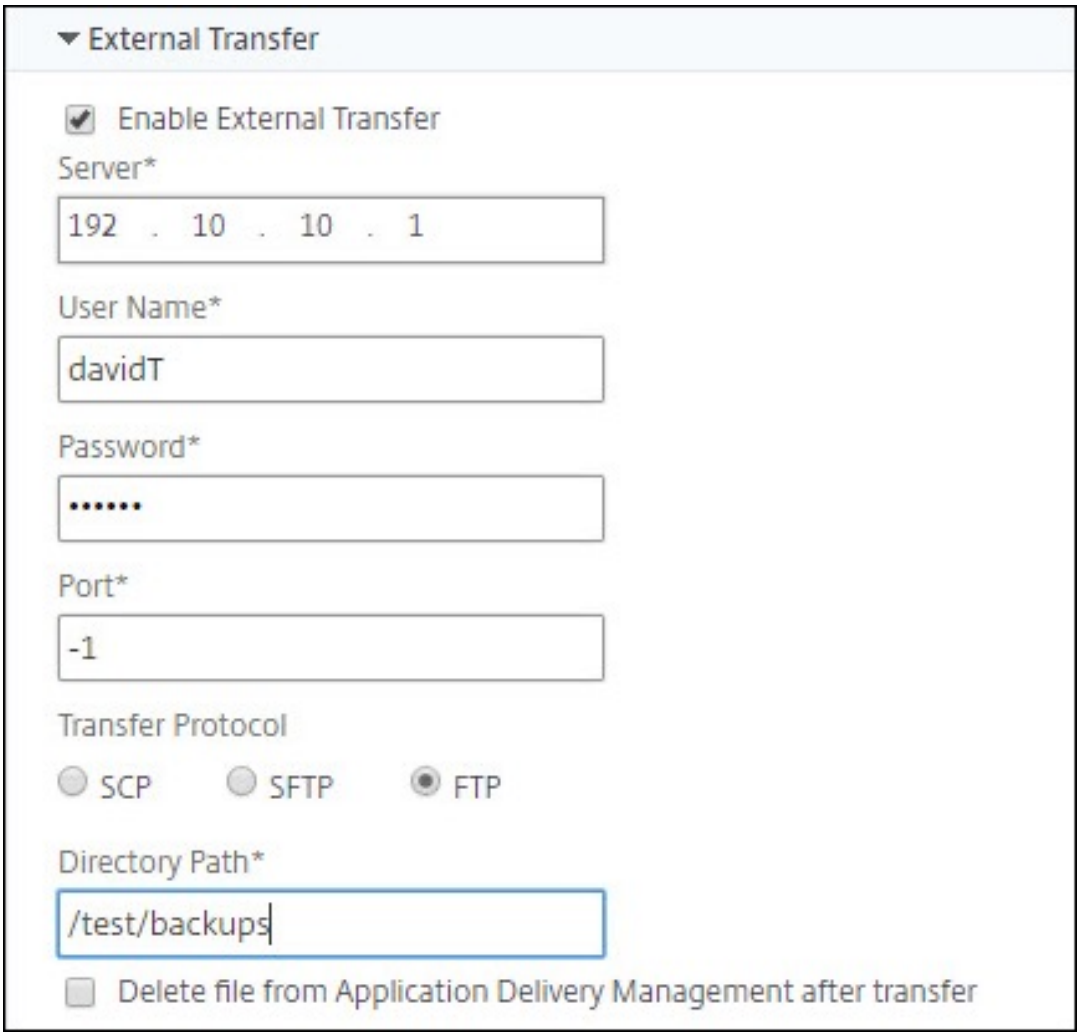
  a) Geben Sie die IP-Adresse des Standorts an.

  b) Geben Sie den Benutzernamen und das Kennwort des externen Servers an, auf den Sie die Backupdateien übertragen möchten.

  c) Geben Sie das Übertragungsprotokoll und die Portnummer an.

  d) Sie können den Verzeichnispfad angeben, in dem die Datei gespeichert werden muss.

  e) Optional können Sie die Backupdatei auch aus Citrix ADM löschen, nachdem Sie sie auf den externen Server übertragen haben.



> **Hinweis**
>
> Citrix ADM sendet eine SNMP-Trap oder eine Syslog-Benachrichtigung an sich selbst, wenn ein Backupfehler für eine der ausgewählten Citrix ADC Instanzen vorliegt.

Erstellen eines Backups für eine ausgewählte NetScaler ADC-Instanz über NetScaler ADM

Führen Sie diese Aufgabe aus, wenn Sie eine ausgewählte NetScaler ADC-Instanz oder mehrere Instanzen sichern möchten:

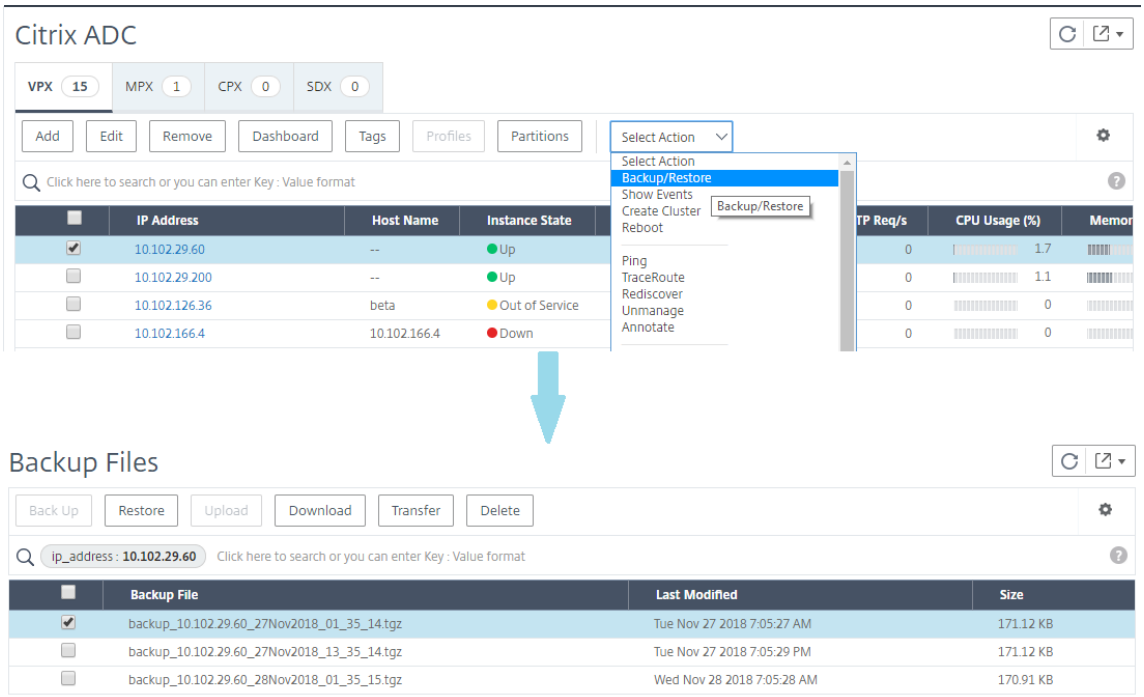
1. Navigieren Sie in Citrix ADM zu**Netzwerke** >**Instanzen**. Wählen Sie unter**Instanzen**den Typ der Instanzen (z. B. Citrix VPX) aus, die auf dem Bildschirm angezeigt werden sollen.
2. Wählen Sie die Instanz aus, die Sie sichern möchten.
    - Wählen Sie für MPX-, VPX- und BLX-Instanzen in der Liste **Aktion auswählen** die Option**Backup/Wiederherstellen** aus.
    - Klicken Sie für eine SDX-Instanz auf **Backup/Restore**.
3. Klicken Sie auf der Seite **Backupdateien** auf **Backup**.
4. Sie können angeben, ob die Backupdatei verschlüsselt werden soll, um mehr Sicherheit zu gewährleisten. Sie können entweder Ihr Kennwort eingeben oder das globale Kennwort verwenden, das Sie zuvor auf der Seite Instanz-Backup-Einstellungenangegeben haben.
5. Klicken Sie auf **Weiter**.

Wiederherstellen einer NetScaler ADC-Instanz über NetScaler ADM

> Hinweis:
>
> Wenn Sie NetScaler ADC-Instanzen in einem HA-Paar haben, müssen Sie Folgendes beachten:
>
> - Stellen Sie dieselbe Instanz wieder her, aus der die Backupdatei erstellt wurde. Betrachten wir beispielsweise ein Szenario, dass ein Backup von der primären Instanz des HA-Paares genommen wurde. Stellen Sie während des Wiederherstellungsvorgangs sicher, dass Sie dieselbe Instanz wiederherstellen, auch wenn es sich nicht mehr um die primäre Instanz handelt.
> - Wenn Sie den Wiederherstellungsprozess auf der primären ADC-Instanz initiieren, können Sie nicht auf die primäre Instanz zugreifen und die sekundäre Instanz wird in **STAYSECONDARY**geändert. Sobald der Wiederherstellungsprozess auf der primären Instanz abgeschlossen ist, wechselt die sekundäre ADC-Instanz vom Modus **STAYSECONDARY** in den **ENABLED-Modus** und wird wieder Teil des HA-Paars. Sie können mit einer möglichen Ausfallzeit auf der primären Instanz rechnen, bis der Wiederherstellungsprozess abgeschlossen ist.

Führen Sie diese Aufgabe aus, um eine NetScaler ADC-Instanz mit der zuvor erstellten Backupdatei wiederherzustellen:

1. Navigieren Sie zu**Netzwerke** >**Instanzen**, wählen Sie die Instanz aus, die Sie wiederherstellen möchten, und klicken Sie dann auf**Backup anzeigen**.
2. Wählen Sie auf der Seite**Backupdateien**die Backupdatei aus, die die wiederherzustellenden Einstellungen enthält, und klicken Sie dann auf**Wiederherstellen**.



Wiederherstellen einer NetScaler ADC SDX-Appliance mit NetScaler ADM

In NetScaler ADM umfasst ein Backup der NetScaler ADC SDX-Appliance Folgendes:

- NetScaler ADC-Instanzen, die auf der Appliance gehostet werden
- SVM-SSL-Zertifikate und -Schlüssel
- Einstellungen für die Instanzbereinigung (im XML-Format)
- Instanzbackupeinstellungen (im XML-Format)
- Abfrageeinstellungen für SSL-Zertifikate (im XML-Format)
- SVM-Datenbankdatei
- NetScaler ADC Konfigurationsdateien von Geräten, die auf SDX vorhanden sind
- NetScaler ADC Build-Images
- NetScaler ADC XVA-Images, diese Images werden am folgenden Speicherort gespeichert: `/var/mps/sdx_images/`
- SDX-Einzelpaket-Image (SVM+XS)
- Instanz-Images von Drittanbietern (sofern bereitgestellt)

Stellen Sie die Citrix ADC SDX-Appliance auf die in der Backupdatei verfügbare Konfiguration

wieder her. Während der Wiederherstellung der Appliance wird die gesamte aktuelle Konfiguration gelöscht.

Wenn Sie die Citrix ADC SDX-Appliance mit einem Backup einer anderen Citrix ADC SDX-Appliance wiederherstellen, müssen Sie die Lizenzen hinzufügen und die Verwaltungsdienst-Netzwerkeinstellungen der Appliance so konfigurieren, dass sie den Einstellungen in der Backupdatei entsprechen, bevor Sie den Wiederherstellungsvorgang starten.

Stellen Sie vor dem Wiederherstellen der SDX-Appliance sicher, dass die gesicherte SDX-Appliance-Plattformvariante mit der Appliance identisch ist. Sie können nicht von einer anderen Plattformvariante wiederherstellen.

> **Hinweis**
>
> Bevor Sie eine SDX RMA-Appliance wiederherstellen, stellen Sie sicher, dass die gesicherte Version entweder gleich oder höher ist als die RMA-Version.

So stellen Sie die SDX-Appliance aus der gesicherten Datei wieder her:

1. Navigieren Sie in der Citrix ADM GUI zu **Netzwerke > Instanzen > Citrix ADC**.
2. Klicken Sie auf **Backup/Restore**.
3. Wählen Sie die Backupdatei derselben Instanz aus, die Sie wiederherstellen möchten.
4. Klicken Sie auf **Backup neu verpacken**.

   Wenn die SDX-Appliance gesichert wird, werden die XVA-Dateien und -Images separat gespeichert, um die Netzwerkbandbreite und den Speicherplatz zu sparen. Daher müssen Sie die gesicherte Datei neu verpacken, bevor Sie die SDX-Appliance wiederherstellen.

   Wenn Sie die Backupdatei neu verpacken, enthält sie alle gesicherten Dateien zusammen, um die SDX-Appliance wiederherzustellen. Die neu verpackte Backupdatei stellt die erfolgreiche Wiederherstellung der SDX-Appliance sicher.
5. Wählen Sie die neu verpackte Backupdatei aus und klicken Sie auf **Wiederherstellen**.

Failovers auf die sekundäre NetScaler ADC-Instanz erzwingen

February 5, 2024

Möglicherweise möchten Sie einen Failover erzwingen, wenn Sie beispielsweise die primäre Citrix Application Delivery Controller (ADC) -Instanz ersetzen oder aktualisieren müssen. Sie können ein Failover entweder von der primären Instanz oder der sekundären Instanz erzwingen. Wenn Sie ein Failover für die primäre Instanz erzwingen, wird die primäre Instanz zur sekundären und die

sekundäre zur primären Instanz. Ein erzwungenes Failover ist nur möglich, wenn die primäre Instanz feststellen kann, dass die sekundäre Instanz aktiv ist.

Ein erzwungenes Failover wird nicht weitergegeben oder synchronisiert. Um den Synchronisierungsstatus nach einem erzwungenen Failover anzuzeigen, können Sie den Status der Instanz anzeigen.

Ein erzwungenes Failover schlägt unter den folgenden Umständen fehl:

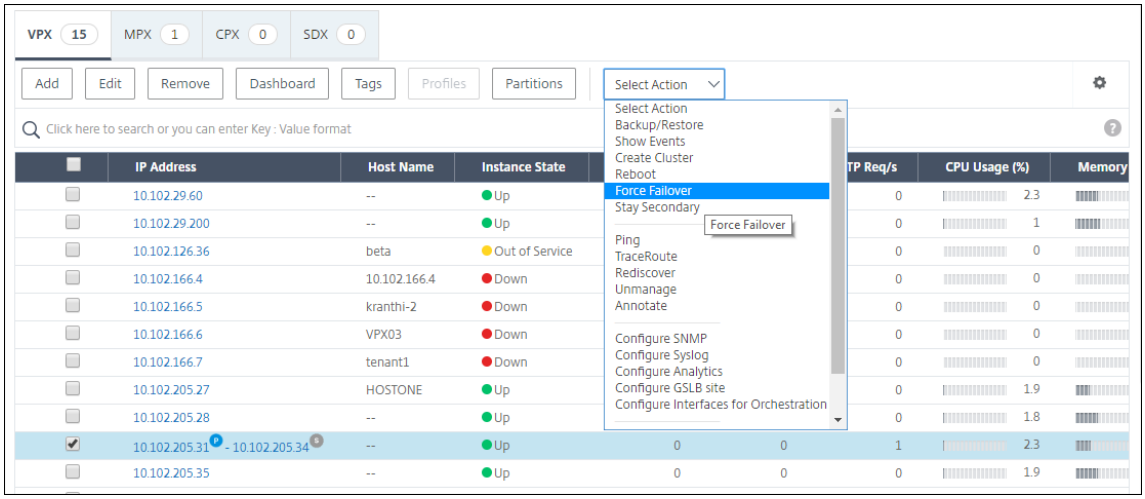
- Sie erzwingen ein Failover auf einem eigenständigen System.
- Die sekundäre Instanz ist deaktiviert oder inaktiv. Wenn sich die sekundäre Instanz in einem inaktiven Zustand befindet, müssen Sie warten, bis ihr Status AKTIV ist, um ein Failover zu erzwingen.
- Die sekundäre Instanz ist konfiguriert, um sekundär zu bleiben.

Die NetScaler ADC-Instanz zeigt eine Warnmeldung an, wenn ein potenzielles Problem beim Ausführen des Force-Failoverbefehls erkannt wird. Die Nachricht enthält die Informationen, die die Warnung ausgelöst haben, und fordert eine Bestätigung an, bevor Sie fortfahren.

Sie können ein Failover auf einer primären Instanz oder einer sekundären Instanz erzwingen.

So erzwingen Sie ein Failover auf die sekundäre NetScaler ADC-Instanz mithilfe von NetScaler ADM:

1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zur Registerkarte **Netzwerke > Instanzen > NetScaler ADC > VPX**, und wählen Sie dann eine Instanz aus.
2. Wählen Sie Instanzen in einem HA-Setup aus den Instanzen aus, die unter dem ausgewählten Instanztyp aufgeführt sind.
3. Wählen Sie im Menü **Aktion** die Option **Force Failover**aus.
4. Klicken Sie auf **Ja**, um die Aktion “Failover erzwingen”zu bestätigen.



Erzwingen, dass eine sekundäre NetScaler ADC-Instanz sekundär bleibt

February 5, 2024

In einem HA-Setup kann der sekundäre Knoten unabhängig vom Status des primären Knotens gezwungen werden, sekundär zu bleiben.

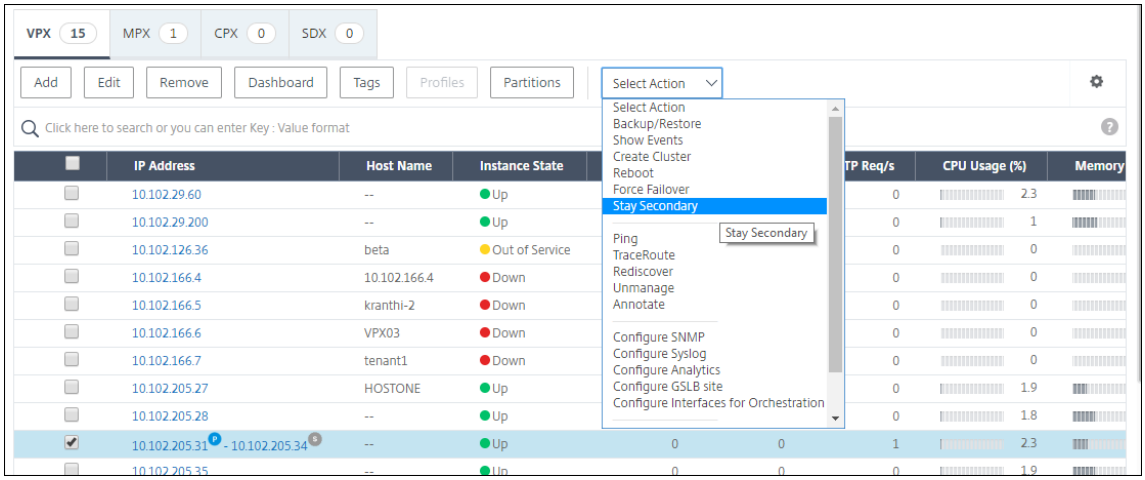
Angenommen, der primäre Knoten muss aktualisiert werden und der Prozess dauert einige Sekunden. Während des Upgrades kann der primäre Knoten für einige Sekunden ausfallen, aber Sie möchten nicht, dass der sekundäre Knoten die Kontrolle übernimmt. Sie möchten, dass er der sekundäre Knoten bleibt, selbst wenn er einen Fehler im primären Knoten erkennt.

Wenn Sie den sekundären Knoten zwingen, sekundär zu bleiben, bleibt er sekundär, selbst wenn der primäre Knoten ausfällt. Wenn Sie erzwingen, dass der Status eines Knotens in einem HA-Paar sekundär bleibt, nimmt er nicht an Übergängen des HA-Zustands der Maschine teil. Der Status des Knotens wird als STAYSECONDARY angezeigt.

> **Hinweis**
>
> Wenn Sie ein System zwingen, sekundär zu bleiben, wird der erzwungene Prozess weder propagiert noch synchronisiert. Sie wirkt sich nur auf den Knoten aus, auf dem Sie den Befehl ausführen.

So konfigurieren Sie mithilfe von NetScaler ADM eine sekundäre NetScaler ADC-Instanz, um mithilfe von NetScaler ADM sekundär zu bleiben:

1. Navigieren Sie in Citrix Application Delivery Management (ADM) zur Registerkarte **Netzwerke** > **Instanzen** > **Citrix ADC** > **VPX**, und wählen Sie dann eine Instanz aus.
2. Wählen Sie Instanzen in einem HA-Setup aus den Instanzen aus, die unter dem ausgewählten Instanztyp aufgeführt sind.
3. Wählen Sie im Menü **Aktion** die Option **Sekundär bleiben**aus.
4. Klicken Sie auf **Ja**, um die Ausführung der Aktion “Sekundär bleiben”zu bestätigen.



Instanzgruppen erstellen

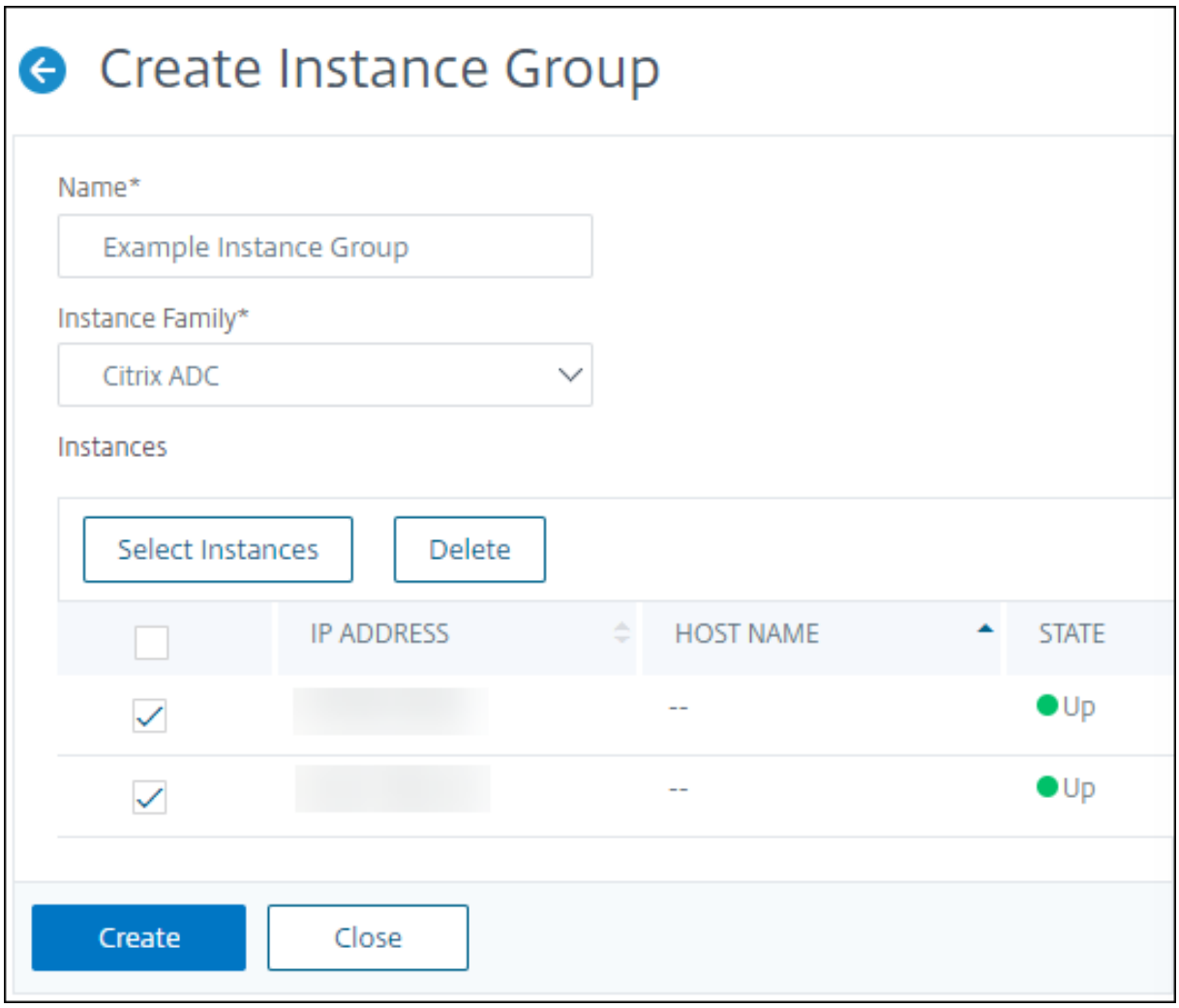
February 5, 2024

Um eine Instanzgruppe zu erstellen, müssen Sie zuerst alle NetScaler ADC-Instanzen zu NetScaler ADM hinzufügen. Nachdem Sie die Varianten erfolgreich hinzugefügt haben, erstellen Sie Instanzgruppen basierend auf ihrer Instanzfamilie. Das Erstellen einer Gruppe von Instanzen hilft Ihnen dabei, für die gruppierten Instanzen gleichzeitig Upgrades und Backups zu erstellen oder sie wiederherzustellen.

So erstellen Sie eine Instanzgruppe mit NetScaler ADM

1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Instanzgruppen**, und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie einen Namen für Ihre Instanzgruppe an, und wählen Sie **NetScaler ADC** aus der Liste **Instanzfamilie** aus.
3. Klicken Sie auf **Instanz auswählen**. Wählen Sie auf der Seite **Instanzen auswählen** die Instanzen aus, die Sie gruppieren möchten, und klicken Sie auf **Auswählen**.

   In der Tabelle sind die ausgewählten Instanzen und ihre Details aufgeführt. Wenn Sie eine Instanz aus der Gruppe entfernen möchten, wählen Sie die Instanz aus der Tabelle aus und klicken Sie auf **Löschen** .
4. Klicken Sie auf **Erstellen**.



Provisioning von ADC VPX-Instanzen auf SDX über ADM

February 5, 2024

Sie können eine oder mehrere ADC VPX-Instanzen auf der SDX-Appliance mithilfe von NetScaler ADM bereitstellen. Die Anzahl der Instanzen, die Sie bereitstellen können, hängt von der erworbenen Lizenz ab. Wenn die Anzahl der hinzugefügten Instanzen der in der Lizenz angegebenen Anzahl entspricht, schränkt der ADM Sie davon Provisioning, weitere NetScaler ADC-Instanzen bereitzustellen.

Bevor Sie beginnen, stellen Sie sicher, dass Sie eine SDX-Instanz in ADM hinzufügen, in der Sie VPX-Instanzen bereitstellen möchten.

Führen Sie die folgenden Schritte aus, um eine VPX-Instanz bereitzustellen:

1. Navigieren Sie zu **Netzwerke > Instanzen > NetScaler ADC**.

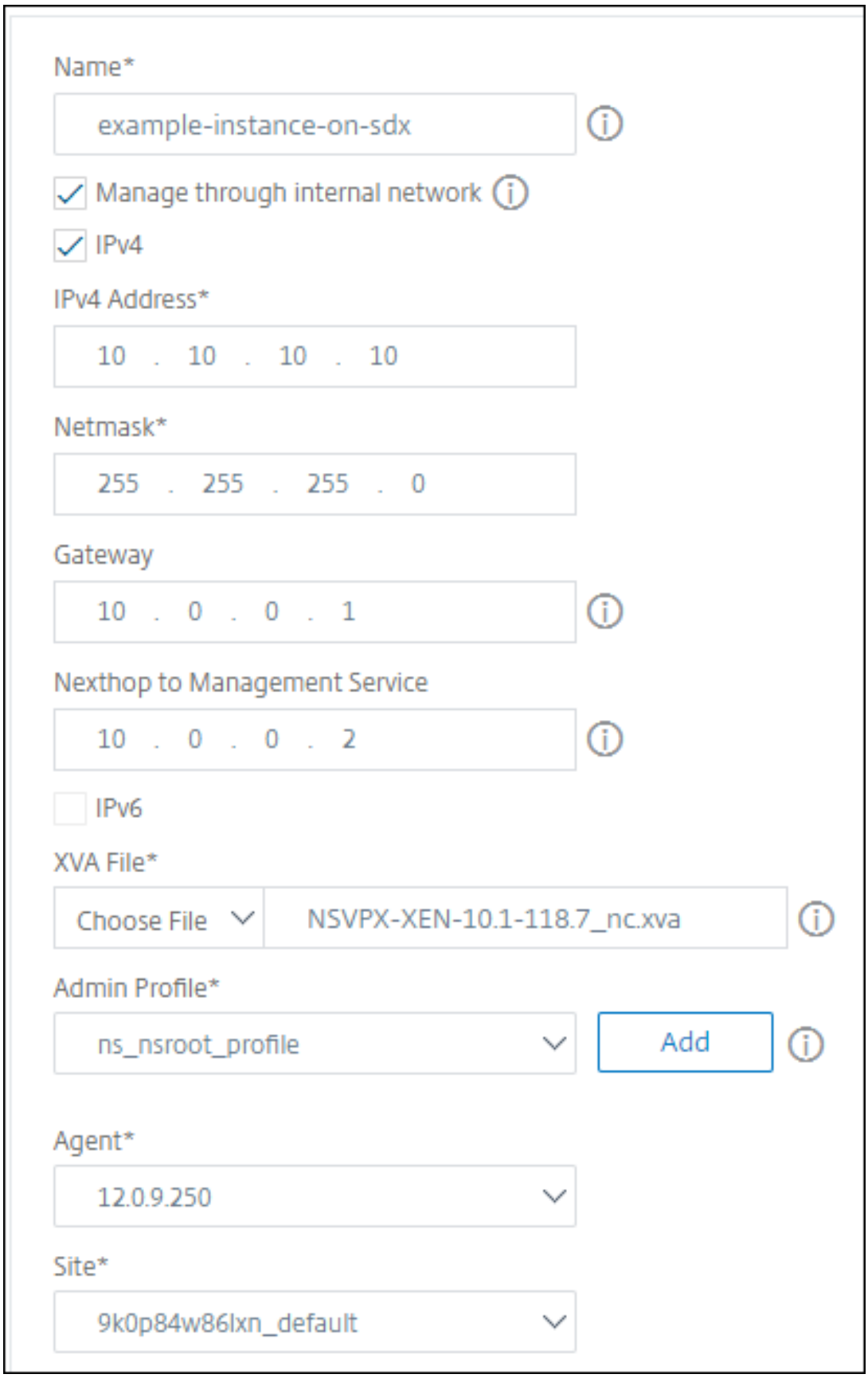
2. Wählen Sie auf der Registerkarte **SDX** eine SDX-Instanz aus, in der Sie eine VPX-Instanz bereitstellen möchten.
3. Wählen Sie unter **Aktion auswählen** die Option **VPX bereitstellen** aus.

Schritt 1 - Hinzufügen einer VPX-Instanz

Der ADM verwendet die folgenden Informationen, um VPX-Instanzen in einer SDX-Appliance zu konfigurieren:

- **Name** - Geben Sie einen Namen für eine ADC-Instanz an.
- Richten Sie ein Kommunikationsnetzwerk zwischen SDX und VPX ein. Wählen Sie dazu die gewünschten Optionen aus der Liste aus:
  - **Über internes Netzwerk verwalten** —Diese Option richtet ein internes Netzwerk für die Kommunikation zwischen dem ADM und einer VPX-Instanz ein.
  - **IP-Adresse** - Sie können eine **IPv4- oder**IPv6-Adresse** oder beide auswählen, um die Citrix VPX-Instanz zu verwalten. Eine VPX-Instanz kann nur eine Verwaltungs-IP haben (auch NetScaler ADC IP genannt). Sie können die NetScaler ADC IP-Adresse nicht entfernen.

    Weisen Sie für die ausgewählte Option dem ADM-Server eine Netzmaske, ein Standard-Gateway und einen nächsten Hop für die IP-Adresse zu.
- **XVA-Datei** - Wählen Sie die XVA-Datei aus, aus der Sie eine VPX-Instanz bereitstellen möchten. Verwenden Sie eine der folgenden Optionen, um die XVA-Datei auszuwählen.
  - **Lokal** - Wählen Sie die XVA-Datei von Ihrem lokalen Computer aus.
  - **Appliance** —Wählen Sie die XVA-Datei in einem ADM-Dateibrowser aus.
- **Admin-Profil** —Dieses Profil bietet Zugriff auf die Bereitstellung von VPX-Instanzen. Mit diesem Profil ruft ADM die Konfigurationsdaten von einer Instanz ab. Wenn Sie ein Profil hinzufügen müssen, klicken Sie auf **Hinzufügen**.
- **Agent** —Wählen Sie den Agent aus, dem Sie die Instanzen zuordnen möchten
- **Site** —Wählen Sie die Site aus, zu der die Instanz hinzugefügt werden soll.



Schritt 2 —Zuteilung von Lizenzen

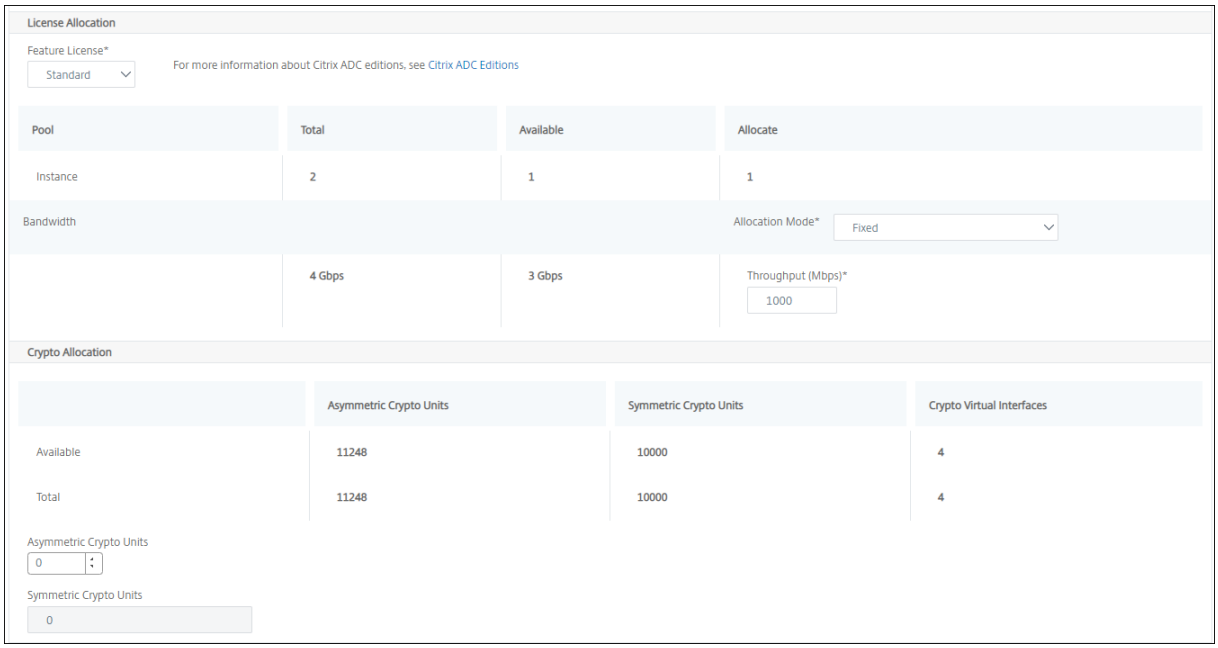
Geben Sie im Abschnitt **Lizenzzuweisung** die VPX-Lizenz an. Sie können Standard-, Advanced- und Premium-Lizenzen verwenden.

- **Zuweisungsmodus** - Sie können den **festen** oder den **Burstable-Modus** für den Bandbreitenpool wählen.

  Wenn Sie den **Burstable-Modus** wählen, können Sie zusätzliche Bandbreite verwenden, wenn die feste Bandbreite erreicht ist.

- **Durchsatz** —Weisen Sie einer Instanz den Gesamtdurchsatz (in Mbit/s) zu.

> **Hinweis:**
>
> Kaufen Sie eine separate Lizenz (SDX 2-Instanz Add-On Pack for Secure Web Gateway) für Citrix Secure Web Gateway (SWG) -Instanzen auf SDX-Appliances. Dieses Instanz-Paket unterscheidet sich von der SDX-Plattformlizenz oder dem SDX-Instanzpaket.
>
> Weitere Informationen finden Sie unter Bereitstellen einer Citrix Secure Web Gateway-Instanz auf einer SDX-Appliance.



Ab der SDX 12.0 57.19 Version hat sich die Schnittstelle zur Verwaltung der Krypto-Kapazität geändert. Weitere Informationen finden Sie unter Verwalten der Krypto-Kapazität.

Schritt 3 - Zuweisen von Ressourcen

Weisen Sie im Abschnitt **Ressourcenzuweisung** Ressourcen einer VPX-Instanz zu, um den Datenverkehr aufrechtzuerhalten.

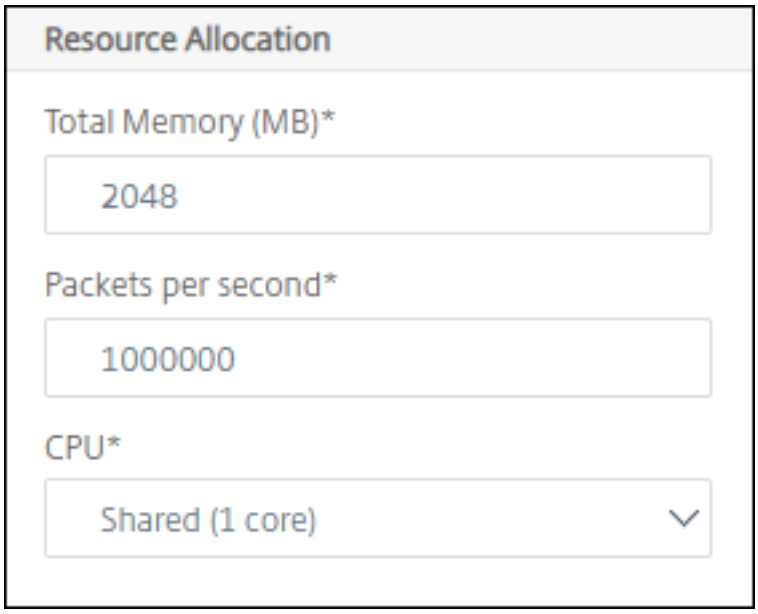
- **Gesamtspeicher (MB)** - Weisen Sie einer Instanz den gesamten Arbeitsspeicher zu. Der Mindestwert ist 2048 MB.
- **Pakete pro Sekunde** - Geben Sie die Anzahl der Pakete an, die pro Sekunde übertragen werden sollen.
- **CPU** —Geben Sie die Anzahl der CPU-Kerne für eine Instanz an. Sie können gemeinsam genutzte oder dedizierte CPU-Kerne verwenden.

  Wenn Sie einen gemeinsam genutzten Kern für eine Instanz auswählen, können die anderen Instanzen den gemeinsam genutzten Kern zum Zeitpunkt der Ressourcenknappheit verwenden.

  Starten Sie Instanzen neu, auf denen CPU-Kerne neu zugewiesen wurden, um Leistungseinbußen

  Wenn Sie die SDX 25000xx-Plattform verwenden, können Sie einer Instanz maximal 16 Kerne zuweisen. Wenn Sie die SDX 2500xxx-Plattform verwenden, können Sie einer Instanz außerdem maximal 11 Kerne zuweisen.

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



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

Plattformname	Kerne insgesamt	Gesamtzahl der für VPX-Provisioning verfügbaren Kerne	Maximale Kerne, die einer einzelnen Instanz zugewiesen werden können
SDX 8015, SDX 8400 und SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500 und SDX 20500	12	10	5
SDX 11515, SDX 11520, SDX 11530, SDX 11540 und SDX 11542	12	10	5
SDX 17500, SDX 19500 und SDX 21500	12	10	5
SDX 17550, SDX 19550, SDX 20550 und SDX 21550	12	10	5
SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 und SDX 14100	12	10	5
SDX 22040, SDX 22060, SDX 22080, SDX 22100 und SDX 22120	16	14	7
SDX 24100 und SDX 24150	16	14	7
SDX 14020 40G, SDX 14030 40G, SDX 14040 40G, SDX 14060 40G, SDX 14080 40G und SDX 14100 40G	12	10	10
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS und SDX 14100. FIPS	12	10	5

Plattformname	Kerne insgesamt	Gesamtzahl der für VPX-Provisioning verfügbaren Kerne	Maximale Kerne, die einer einzelnen Instanz zugewiesen werden können
SDX 14040 40S, SDX 14060 40S, SDX 14080 40S und SDX 14100 40S	12	10	5
SDX 25100A, 25160A, 25200A	20	18	9
SDX 25100-40 G, 25160-40 G, 25200-40 G	20	18	16 (wenn Version 11.1-51.x oder höher ist); 9 (wenn Version 11.1-50.x oder niedriger ist; alle Versionen von 11.0 und 10.5)
SDX 26100, 26160, 26200, 26250	28	26	13
15000-50G	16	14	7

> **Hinweis:**
>
> Auf der SDX 26xxx-Plattform können einer VPX-Instanz maximal 26 CPU-Kerne zugewiesen werden. Wenn der Instanz Kryptoeinheiten zugewiesen sind, hängt die maximale Anzahl von Kernen von der Anzahl der Kryptoeinheiten und Datenschnittstellen ab.
>
> Wenn Sie beispielsweise einer Instanz 24000 Kryptoeinheiten zuweisen, können Sie der Instanz 24 CPU-Kerne und maximal zwei Datenschnittstellen zuweisen. Die SDX-Appliance betrachtet Datenschnittstellen und Kryptoeinheiten als PCI-Geräte. Bei 26000 Kryptoeinheiten schlägt die Bereitstellung von VPX-Instanzen fehl, da kein Platz zum Hinzufügen von Datenschnittstellen vorhanden ist.

Schritt 4 —Instanzverwaltung hinzufügen

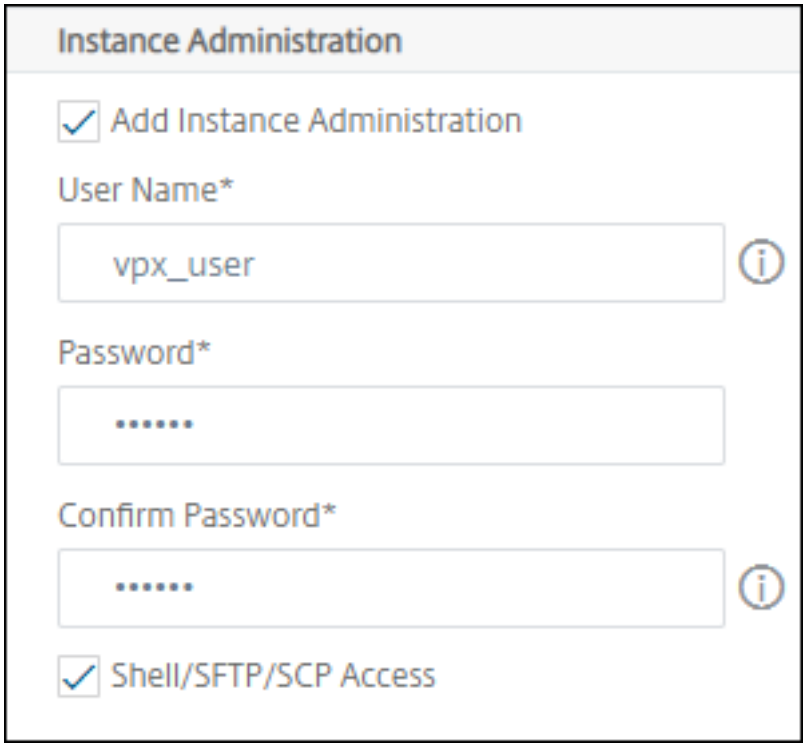
Sie können einen Admin-Benutzer für die VPX-Instanz erstellen. Wählen Sie dazu im Abschnitt **Instanzverwaltung die Option**Instanzverwaltung**hinzufügen** aus.

Geben Sie die folgenden Details an:

- **Benutzername**: Der Benutzername für den Citrix ADC Instanzadministrator. Dieser Benutzer hat Superuser-Zugriff, hat aber keinen Zugriff auf Netzwerkbefehle zum Konfigurieren von

VLANs und Schnittstellen.

- **Kennwort**: Geben Sie das Kennwort für den Benutzernamen an.
- **Shell/Sftp/Scp Access**: Der Zugriff, der dem Citrix ADC Instanzadministrator gewährt wird. Diese Option ist standardmäßig ausgewählt.



Schritt 5 —Netzwerkeinstellungen festlegen

Wählen Sie die erforderlichen Netzwerkeinstellungen für eine Instanz aus:

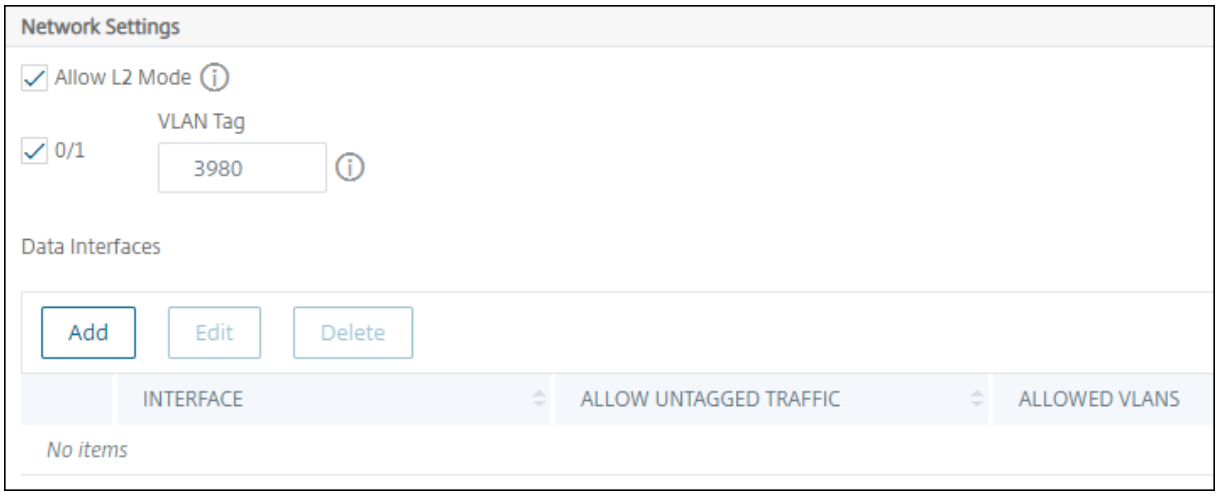
- **L2-Modus unter Netzwerkeinstellungen** zulassen: Sie können den L2-Modus auf der NetScaler ADC-Instanz zulassen. Wählen Sie unter Netzwerkeinstellungen die Option L2-Modus zulassen aus. Bevor Sie sich bei der Instanz anmelden und den L2-Modus aktivieren. Weitere Informationen finden Sie unter Zulassen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

  > **Hinweis**
  >
  > Wenn Sie den L2-Modus für eine Instanz deaktivieren, müssen Sie sich bei der Instanz anmelden und den L2-Modus von dieser Instanz aus deaktivieren. Andernfalls werden möglicherweise alle anderen NetScaler ADC-Modi deaktiviert, nachdem Sie die Instanz neu gestartet haben.

- **0/1** - Geben Sie im **VLAN-Tag**eine VLAN-ID für die Verwaltungsschnittstelle an.

- **0/2** - Geben Sie im **VLAN-Tag**eine VLAN-ID für die Verwaltungsschnittstelle an.

Standardmäßig sind die Schnittstellen **0/1** und **0/2** ausgewählt.



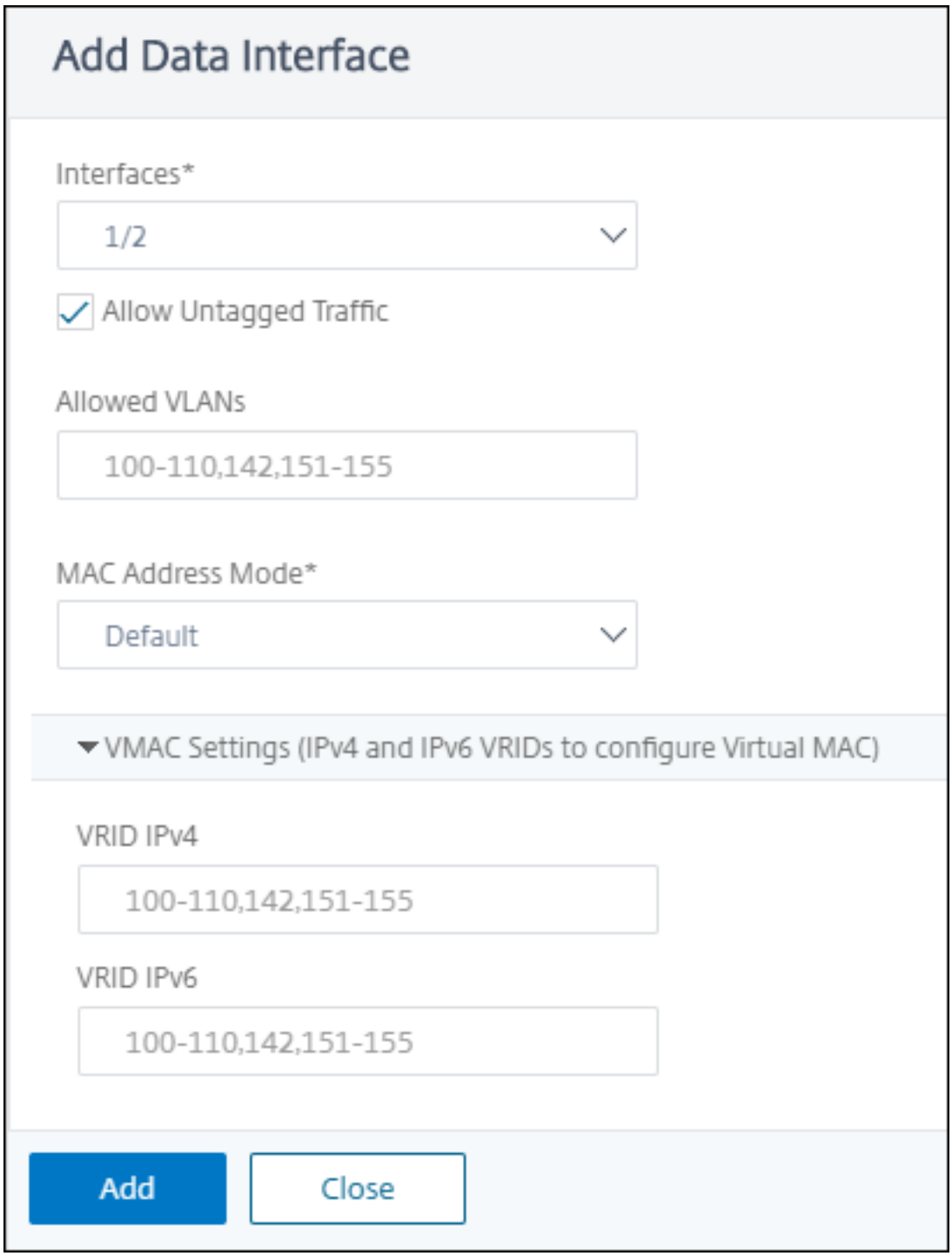
Klicken Sie unter **Datenschnittstellen**auf **Hinzufügen**, um Datenschnittstellen hinzuzufügen, und geben Sie Folgendes an:

- **Schnittstellen** - Wählen Sie die Schnittstelle aus der Liste aus.

  > **Hinweis:**
  >
  > Die Schnittstellen-IDs von Schnittstellen, die Sie einer Instanz hinzufügen, entsprechen nicht unbedingt der physischen Schnittstellennummerierung auf der SDX-Appliance.
  >
  > Beispielsweise ist die erste Schnittstelle, die Sie mit Instanz-1 verknüpfen, die SDX-Schnittstelle 1/4. Sie wird als Schnittstelle 1/1 angezeigt, wenn Sie die Schnittstelleneinstellungen in dieser Instanz anzeigen. Diese Schnittstelle zeigt an, dass es sich um die erste Schnittstelle handelt, die Sie mit Instanz-1 verknüpft haben.

- **Zulässige VLANs** : Geben Sie eine Liste von VLAN-IDs an, die einer NetScaler ADC-Instanz zugeordnet werden können.
- **MAC-Adressmodus** - Weisen Sie einer Instanz eine MAC-Adresse zu. Wählen Sie eine der folgenden Optionen:
  - **Standard** —Citrix Workspace weist eine MAC-Adresse zu.
  - **Benutzerdefiniert** —Wählen Sie diesen Modus, um eine MAC-Adresse anzugeben, die die generierte MAC-Adresse außer Kraft setzt.
  - **Generiert** - Generiert eine MAC-Adresse mithilfe der zuvor festgelegten Basis-MAC-Adresse. Informationen zum Festlegen einer MAC-Basisadresse finden Sie unter Zuweisen einer MAC-Adresse zu einer Schnittstelle.
- **VMAC-Einstellungen (IPv4- und IPv6-VRIDs zur Konfiguration des virtuellen MAC)**

- **VRID IPV4** —Die IPv4-VRID, die den VMAC identifiziert. Mögliche Werte: 1—255. Weitere Informationen finden Sie unter Konfigurieren von VMACs auf einer Schnittstelle.
- VRID IPV6 - Die IPv6-VRID, die die VMAC identifiziert. Mögliche Werte: 1—255. Weitere Informationen finden Sie unter Konfigurieren von VMACs auf einer Schnittstelle.



Klicken Sie auf **Hinzufügen**.

Schritt 6 —Festlegen der Management-VLAN-Einstellungen

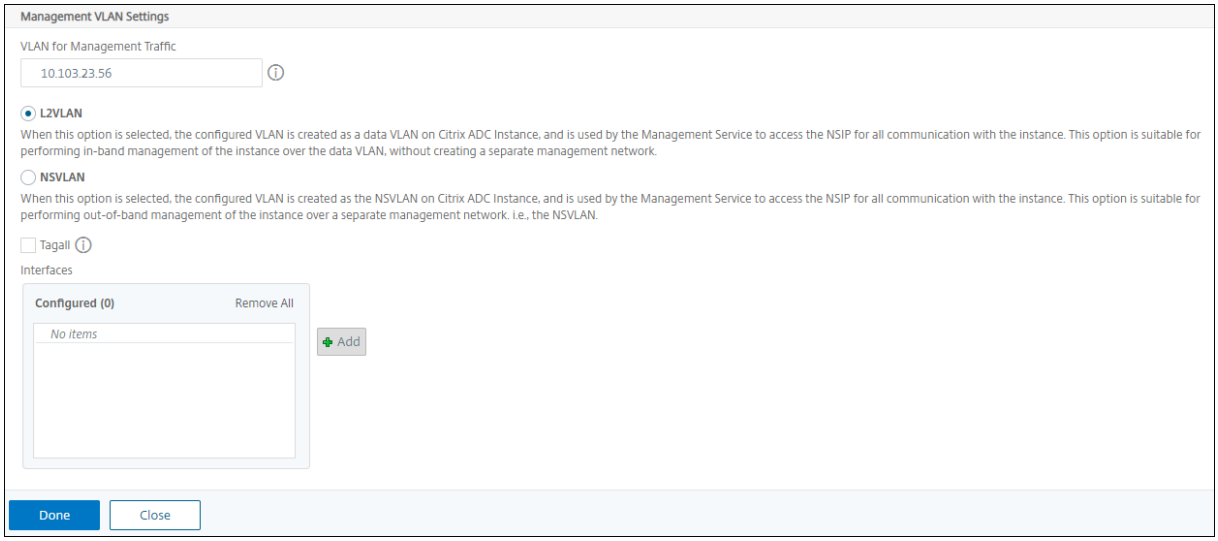
Der Verwaltungsdienst und die Verwaltungsadresse (NSIP) der VPX-Instanz befinden sich im selben Subnetz, und die Kommunikation erfolgt über eine Verwaltungsschnittstelle.

Wenn sich der Verwaltungsdienst und die Instanz in unterschiedlichen Subnetzen befinden, geben Sie eine VLAN-ID an, während Sie eine VPX-Instanz bereitstellen. Daher ist die Instanz über das Netzwerk erreichbar, wenn sie aktiv ist.

Wenn Ihre Bereitstellung erfordert, dass NSIP während der Bereitstellung der VPX-Instanz nur über die ausgewählte Schnittstelle zugänglich ist, wählen Sie **NSVLAN**aus. Und das NSIP wird über andere Schnittstellen nicht mehr zugänglich.

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

> **Wichtig!**
>
> - Sie können diese Einstellung nicht ändern, nachdem Sie die VPX-Instanz bereitgestellt haben.
> - Der Befehl `clear config full` auf der VPX-Instanz löscht die VLAN-Konfiguration, wenn **NSVLAN** nicht ausgewählt ist.

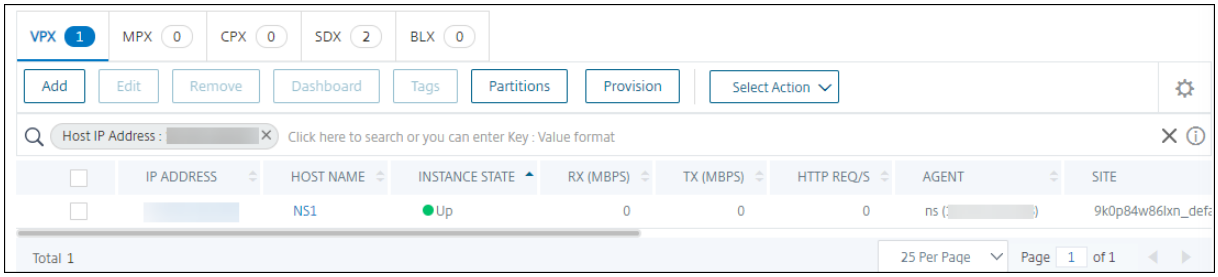


Klicken Sie auf **Fertig**, um eine VPX-Instanz bereitzustellen.

Zeigen Sie die bereitgestellte VPX-Instanz an

Führen Sie die folgenden Schritte aus, um die neu bereitgestellte Instanz anzuzeigen:

1. Navigieren Sie zu **Netzwerke > Instanzen > NetScaler ADC**.
2. Suchen Sie auf der Registerkarte **VPX** eine Instanz nach der Eigenschaft **Host-IP-Adresse**, und geben Sie die IP-Adresse der SDX-Instanz an.



Wiedererkennen mehrerer Citrix VPX-Instanzen

February 5, 2024

Sie können mehrere Citrix VPX-Instanzen in Ihrem NetScaler Application Delivery Management (ADM) -Setup wiederfinden. Außerdem können Sie mehrere Citrix VPX-Instanzen wiederfinden, wenn Sie die neuesten Zustände und Konfigurationen dieser Instanzen anzeigen möchten. Der NetScaler ADM -Server erkennt alle Citrix VPX-Instanzen erneut und prüft, ob die Citrix Application Delivery Controller (ADC) -Instanzen erreichbar sind.

So ermitteln Sie mehrere Citrix VPX-Instanzen neu:

1. Geben Sie in einem Webbrowser die IP-Adresse des Citrix ADM -Servers ein (z. B. http://192.168.100.1).
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein. Die Standardanmeldeinformationen des Administrators sind `nsrootnsroot`
3. Navigieren Sie zur Registerkarte **Netzwerke** > **Instanzen** > **NetScaler ADC** > **VPX**, und wählen Sie die Instanzen aus, die Sie neu ermitteln möchten.
4. Klicken **Sie im Menü Aktion auswählen** auf **Neu entdecken**.
5. Wenn die Bestätigungsmeldung für die Ausführung des Dienstprogramms Wiederermittlung angezeigt wird, klicken Sie auf **Ja**.

   Auf dem Bildschirm wird der Fortschritt der erneuten Erkennung der einzelnen Citrix VPX-Instanzen angezeigt.

Verwalten einer Instanz aufheben

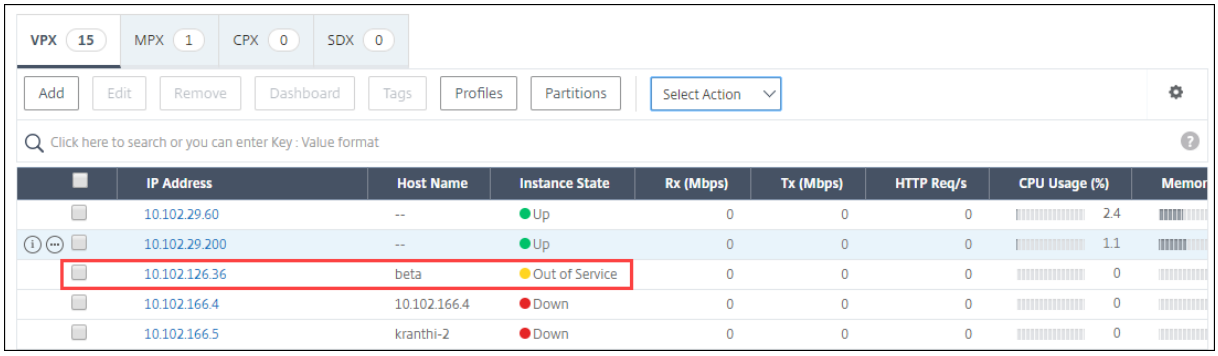
February 5, 2024

Wenn Sie den Informationsaustausch zwischen Citrix Application Delivery Management (ADM) und den Instanzen im Netzwerk beenden möchten, können Sie die Verwaltung der Instanzen aufheben.

So heben Sie die Verwaltung einer Instanz auf:

Navigieren Sie zur Registerkarte **Netzwerke** > **Instanzen** > **Citrix ADC** > **VPX**. Klicken Sie in der Liste der Instanzen mit der rechten Maustaste auf eine Instanz, und wählen Sie dann **Verwalten aufheben**aus, oder wählen Sie die Instanz aus, und wählen Sie in der Liste **Aktion auswählen**die Option **Verwalten aufheben**aus.

Der Status der ausgewählten Instanz ändert sich in "**Abgemeldet**", wie in der folgenden Abbildung dargestellt.



Die Instanz wird nicht mehr von NetScaler ADM verwaltet und tauscht keine Daten mehr mit NetScaler ADM aus.

Tracing einer Route zu einer Instanz

February 5, 2024

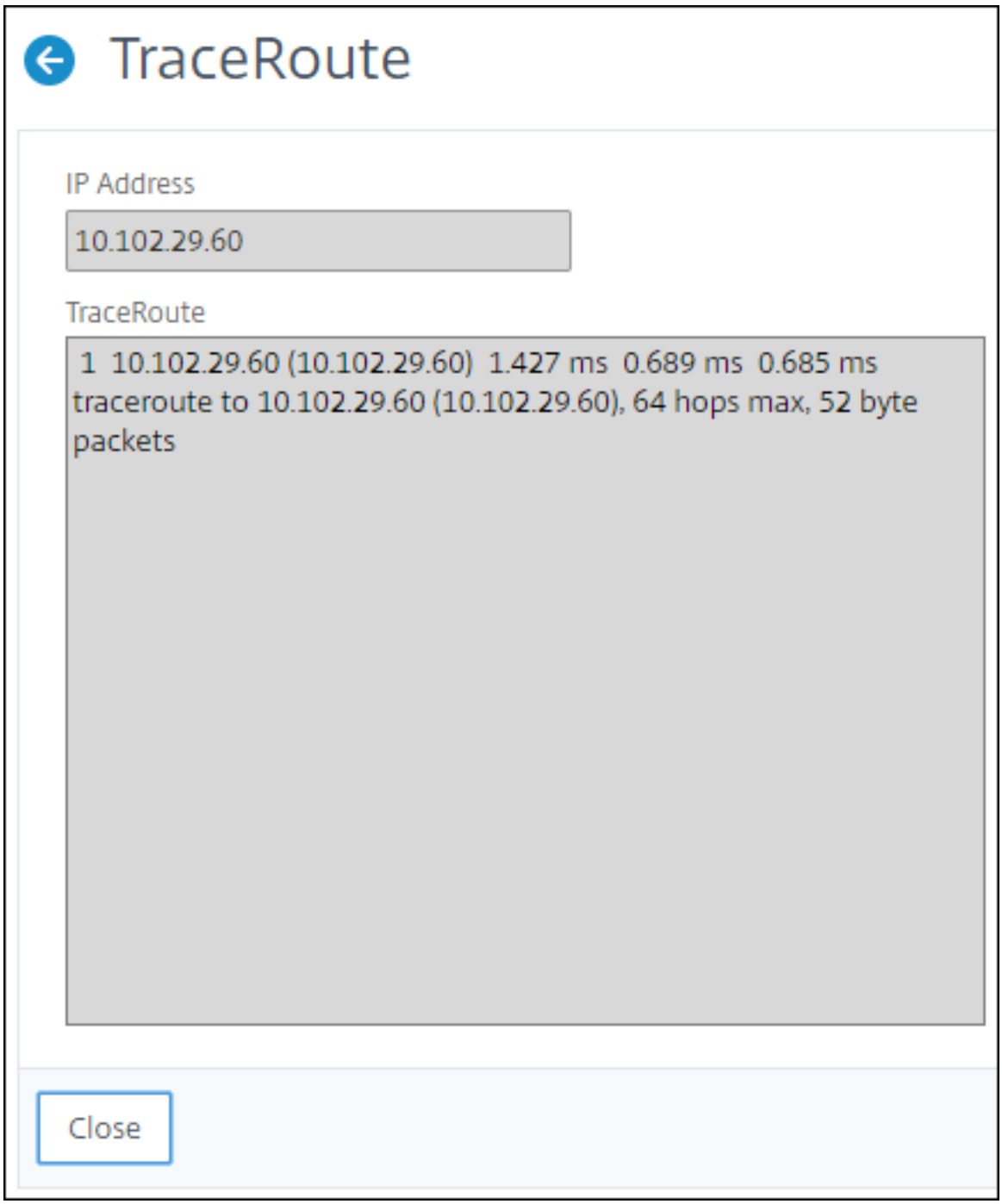
Indem Sie die Route eines Pakets von NetScaler Application Delivery Management (ADM) zu einer Instanz verfolgen, finden Sie Informationen wie die Anzahl der Hops, die zum Erreichen der Instanz erforderlich sind. Traceroute verfolgt den Pfad des Pakets von Quelle zu Ziel. Es zeigt die Liste der Netzwerk-Hops zusammen mit dem Hostnamen und der IP-Adresse der einzelnen Entitäten in der Route an.

Traceroute erfasst auch die Zeit, die ein Paket für die Reise von einem Hop zum anderen nimmt. Wenn die Übertragung von Paketen unterbrochen wird, zeigt Traceroute, wo das Problem besteht.

So verfolgen Sie die Route einer Instanz:

1. Navigieren Sie in NetScaler ADM zur Registerkarte **Netzwerke** > **Instanzen** > **NetScaler ADC** > **VPX**.
2. Klicken Sie in der Liste der Instanzen mit der rechten Maustaste auf eine Instanz, und wählen Sie dann **TraceRoute** aus, oder wählen Sie die Instanz aus, und klicken Sie im Menü **Aktion auswählen** auf **TraceRoute**.

Das **TraceRoute**-Meldungsfeld zeigt die Route zur Instance und die von jedem Hop verbrauchte Zeit in Millisekunden an.



Upgrade-Empfehlungen

February 5, 2024

Als Netzwerkadministrator können Sie viele ADC-Instanzen verwalten, die auf verschiedenen

ADC-Versionen in NetScaler ADM ausgeführt werden. Die Überwachung des Lebenszyklus jeder ADC-Instanz kann eine umständliche Aufgabe sein. Sie müssen die Citrix Product Matrixbesuchen und die ADC-Instanzen identifizieren, die End of Life (EOL) oder End of Maintenance (EOM) erreichen oder erreicht haben. Planen Sie dann ihr Upgrade.

Mit der Upgrade-Empfehlung können Sie den Lebenszyklus Ihrer ADC-Instanzen überwachen. Es identifiziert Instanzen, die EOL/EOM erreichen, und Sie können ADC-Upgrades vor dem EOL- oder EOM-Datum planen.

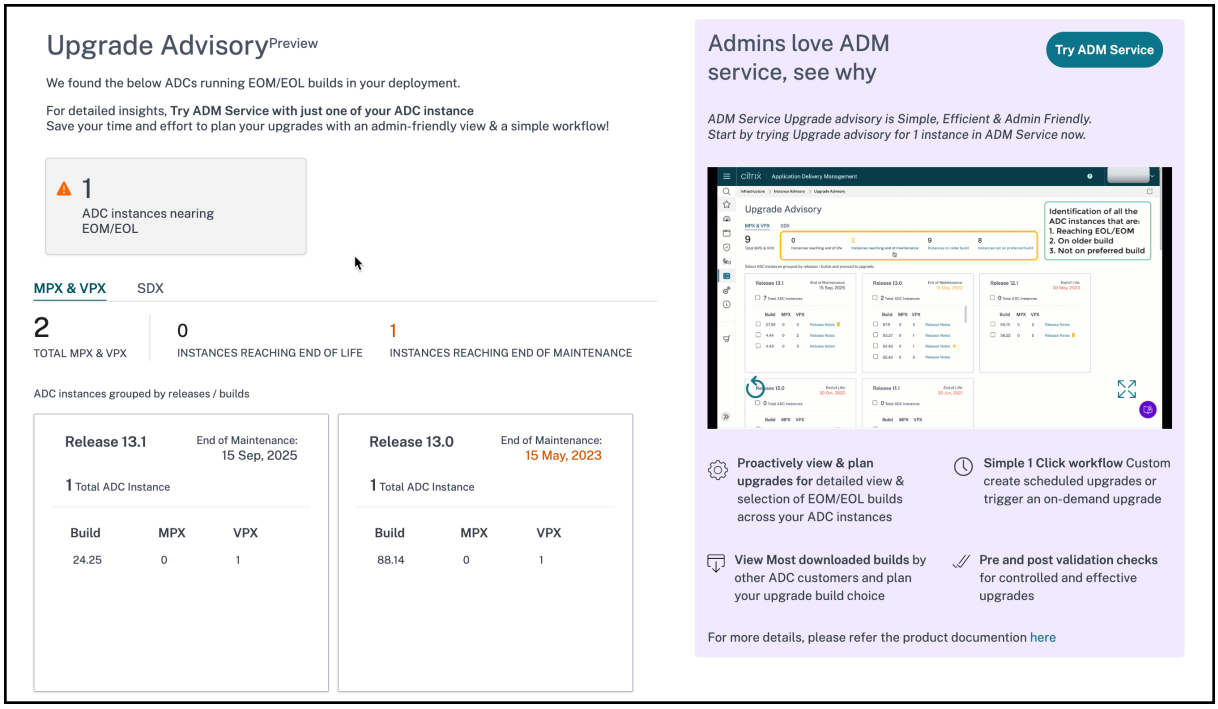
Die Upgrade-Empfehlung führt einen Versionsscan der ADCs durch und bietet einen Überblick über die EOM/EOL-Builds in Ihren ADC-Instanzen.

Sie können eine der ADC-Instanzen auswählen und in den ADM Service integrieren. Klicken Sie auf **ADM Service testen**und integrieren Sie eine ADC-Instanz, um detaillierte Einblicke zu erhalten. Weitere Informationen zur ADM Service Upgrade-Beratungsfunktion finden Sie in einer Vorschau der GIF-Animation auf der Seite mit den **Upgrade-Hinweisen** .

Upgrade-Advisory anzeigen

Navigieren Sie in **Netzwerken > Instanz Advisory > Upgrade Advisory** und zeigen Sie die folgenden Informationen an:

- Gesamtzahl der ADC-Instanzen.
- Instanzen, die das Lebensende erreichen.
- Instanzen, die das Ende der Wartung erreichen.



Auf der Seite **Upgrade Advisory** werden die ADC-Instanzen nach ihren Releases gruppiert.

Sicherheitsempfehlungen

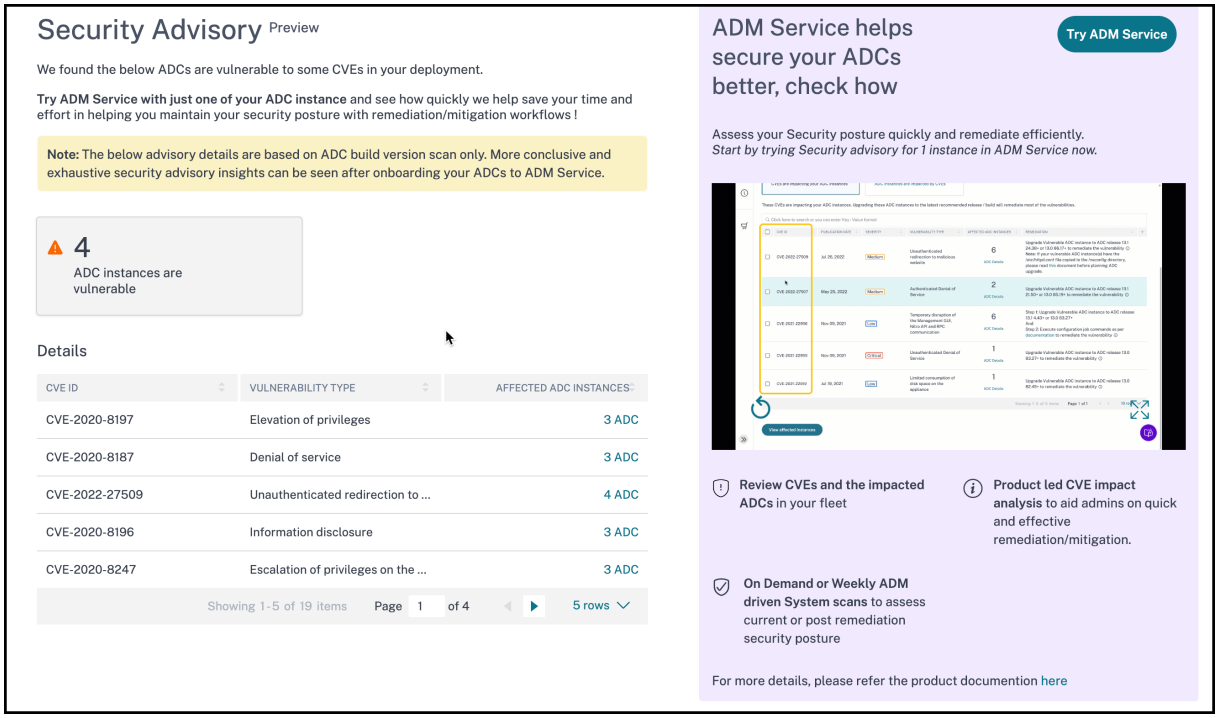
February 5, 2024

Eine sichere und belastbare Infrastruktur ist die Lebensader jeder Organisation. Unternehmen müssen neue Common Vulnerabilities and Exposures (CVEs) verfolgen und die Auswirkungen von CVEs auf ihre Infrastruktur bewerten. Sie müssen auch die Abschwächung und Behebung der Sicherheitsrisiken verstehen und planen, um die Sicherheitslücken zu beheben.

Die NetScaler ADM-Sicherheitsempfehlung hebt Citrix CVEs hervor, die Ihre ADC-Instanzen gefährden.

Sicherheitsempfehlung anzeigen

Um auf den **Security Advisory** zuzugreifen, navigieren Sie zu **Networks > Instance Advisory > Security Advisory**. Sie können den Sicherheitsstatus aller ADC-Instanzen sehen, die Sie über NetScaler ADM verwalten.



Security Advisory führt nur einen ADC-Versionsscan durch, um nach CVEs zu suchen, und eine Tabelle mit der Anzahl der CVEs, die sich auf die ADC-Instanzen auswirken, wird angezeigt.

- **CVE-ID**: Die ID des CVE, der sich auf die Instanzen auswirkt.
- **Schwachstellentyp**: Die Art der Sicherheitsanfälligkeit für dieses CVE.
- **Betroffene ADC-Instanzen**: Die Anzahl der Instanzen, auf die sich die CVE-ID auswirkt.

Um den Schwachstellentyp eines bestimmten CVE und Informationen zur Risikominderung und Behebung der Sicherheitsanfälligkeit zu überprüfen, wählen Sie eine der ADC-Instanzen aus und klicken Sie auf **ADM Service testen** und integrieren Sie die ADC-Instance in den ADM Service. Weitere Informationen zur ADM Service Security-Beratungsfunktion finden Sie in einer Vorschau der GIF-Animation auf der Seite mit den **Sicherheitshinweisen** .

Ereignisse

February 5, 2024

Wenn die IP-Adresse einer Citrix Application Delivery Controller Instanz (ADC) zu NetScaler Application Delivery Management (ADM) hinzugefügt wird, sendet NetScaler ADM einen NITRO -Aufruf und fügt sich implizit als Trap-Ziel für die Instanz hinzu, um die Traps oder Ereignisse zu empfangen.

Ereignisse stellen Ereignisse oder Fehler in einer verwalteten NetScaler ADC-Instanz dar. Wenn beispielsweise ein Systemausfall oder eine Änderung in der Konfiguration vorliegt, wird ein Ereignis generiert und auf dem NetScaler ADM -Server aufgezeichnet. In NetScaler ADM empfangene Ereignisse werden auf der Seite “Ereignisübersicht”(**Netzwerke** > **Ereignisse**) angezeigt, und alle aktiven Ereignisse werden auf der Seite “Ereignismeldungen”(**Netzwerke** > **Ereignisse** > **Ereignismeldungen**) angezeigt.

NetScaler ADM überprüft auch die auf Instanzen generierten Ereignisse, um Alarme mit unterschiedlichen Schweregraden zu bilden. Diese Alarme werden dann als Nachrichten angezeigt, von denen einige möglicherweise sofortige Aufmerksamkeit erfordern. Beispielsweise kann ein Systemausfall als “kritischer”Ereignisschweregrad eingestuft werden und müsste sofort behoben werden.

Sie können Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Regeln erleichtern die Überwachung der Ereignisse, die viele sein können, die in Ihrer NetScaler ADC-Infrastruktur generiert werden.

Sie können eine Reihe von Ereignissen filtern, indem Sie Regeln mit bestimmten Bedingungen konfigurieren und den Regeln Aktionen zuweisen. Wenn die generierten Ereignisse die Filterkriterien in der Regel erfüllen, wird die mit der Regel verknüpfte Aktion ausgeführt. Die Bedingungen für die Erstellung von Filtern sind: Schweregrad, NetScaler ADC-Instanzen, Kategorie, Fehlerobjekte, Konfigurationsbefehle und Meldungen.

Sie können auch sicherstellen, dass mehrere Benachrichtigungen für ein Ereignis für ein bestimmtes Zeitintervall ausgelöst werden, bis das Ereignis gelöscht wird. Als zusätzliche Maßnahme können Sie Ihre E-Mail mit einer bestimmten Betreffzeile und einer Benutzernachricht anpassen und einen Anhang hochladen.

Ereignisdashboard verwenden

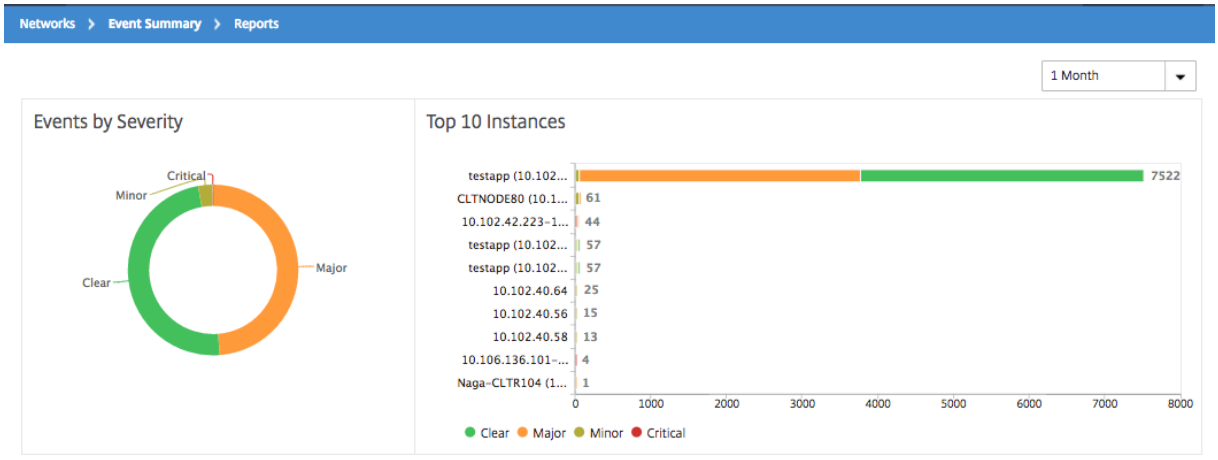
February 5, 2024

Als Netzwerkadministrator können Sie Details wie Konfigurationsänderungen, Anmeldebedingungen, Hardwarefehler, Schwellenwertverletzungen und Änderungen des Entitätsstatus auf Ihren Citrix Application Delivery Controller (ADC) -Instanzen sowie Ereignisse und deren Schweregrad für bestimmte Instanzen einsehen. Sie können das Ereignis-Dashboard von NetScaler Application Delivery Management (ADM) verwenden, um Berichte anzuzeigen, die für Details zum Schweregrad kritischer Ereignisse für all Ihre NetScaler ADC-Instanzen generiert wurden.

So zeigen Sie die Details im Ereignis-Dashboard an:

Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Berichte**.

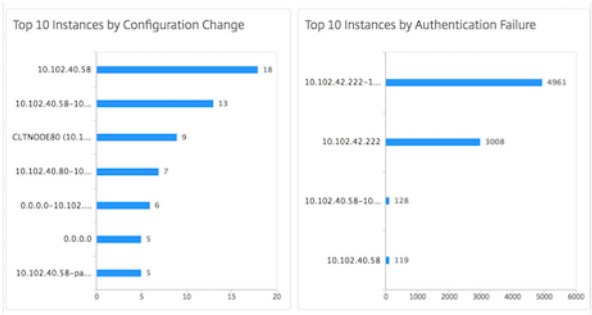
Das Diagramm Top 10 Geräte auf dem Dashboard zeigt einen Bericht der Top 10 Instanzen anhand der Anzahl der auf ihnen erzeugten Ereignisse an. Sie können auf eine Instanz im Diagramm klicken, um weitere Details zum Schweregrad des Ereignisses anzuzeigen.



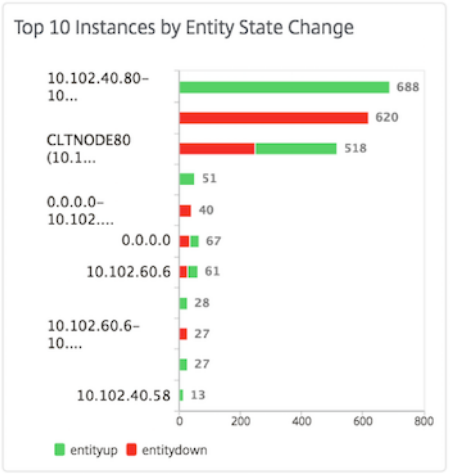
Sie können weitere Details anzeigen, indem Sie zum NetScaler ADC-Instanztyp navigieren (**Netzwerke** > **Ereignisse** > **Berichte** > **NetScaler ADC/NetScaler ADC SDX/NetScaler ADC SD-WAN WO**), um Folgendes anzuzeigen:

- Top 10 Geräte nach Hardwarefehler
- Top 10 Geräte nach Konfigurationsänderung

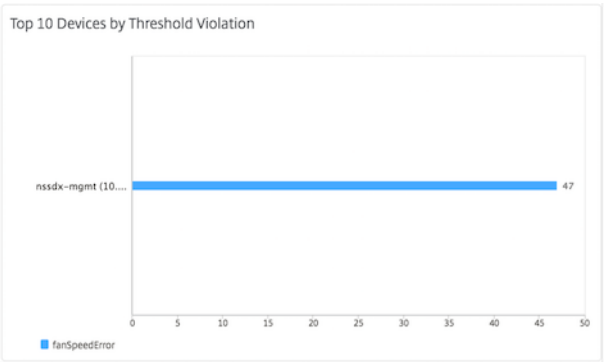
- Top 10 Geräte durch Authentifizierungsfehler



- Top 10 Geräte nach Entitätsstatusänderungen



- Top 10 Geräte nach Schwellenverletzung



Ereignisalter für Ereignisse festlegen

February 5, 2024

Sie können die Option Ereignisalter festlegen, um das Zeitintervall (in Sekunden) anzugeben.

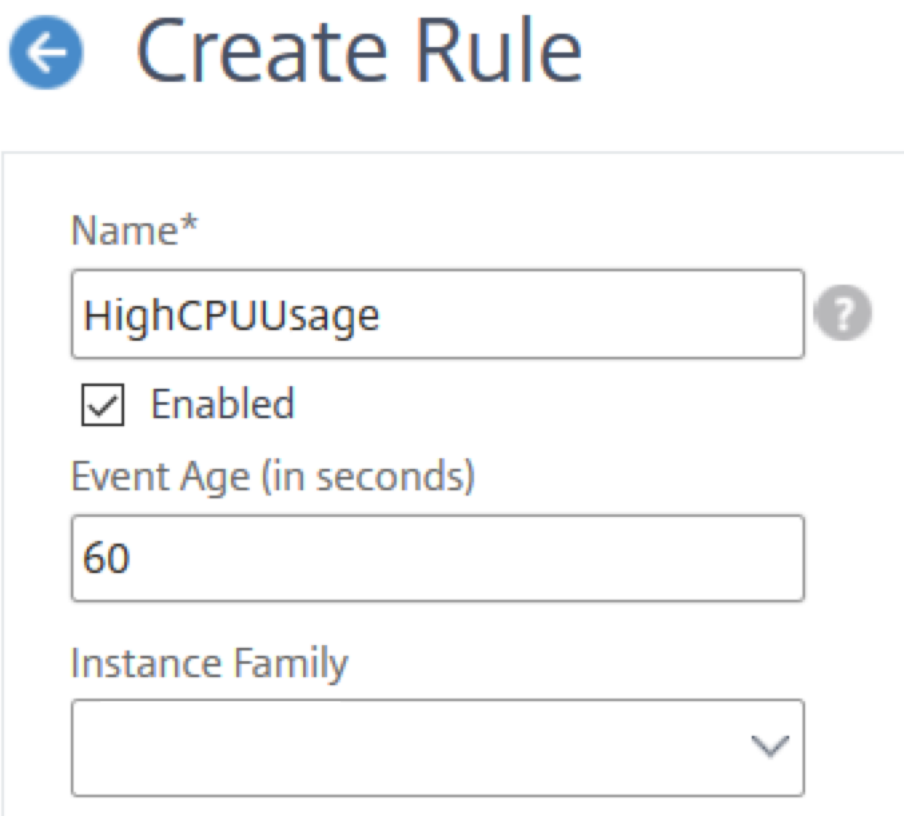
NetScaler ADM überwacht die Appliances bis zur festgelegten Dauer und generiert nur dann ein Ereignis, wenn das Ereignisalter die festgelegte Dauer überschreitet.

> Hinweis:
>
> Der Mindestwert für das Ereignisalter ist 60 Sekunden. Wenn Sie das Feld **Ereignisalter** leer lassen, wird die Ereignisregel unmittelbar nach dem Auftreten des Ereignisses angewendet.

Stellen Sie sich beispielsweise vor, dass Sie verschiedene ADC-Appliances verwalten und per E-Mail benachrichtigt werden möchten, wenn einer Ihrer virtuellen Server für 60 Sekunden oder länger ausfällt. Sie können eine Ereignisregel mit den erforderlichen Filtern erstellen und das Ereignisalter der Regel auf 60 Sekunden festlegen. Wenn ein virtueller Server dann 60 oder mehr Sekunden lang ausfällt, erhalten Sie eine E-Mail-Benachrichtigung mit Details wie Entitätsname, Statusänderung und Uhrzeit.

So legen Sie das Ereignisalter in NetScaler ADM fest:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Ereignisse** > **Regeln**, und klicken Sie auf **Hinzufügen**.
2. Legen Sie auf der Seite **Regel erstellen** die Regelparameter fest.
3. Geben Sie das Ereignisalter in Sekunden an.



Stellen Sie sicher, dass alle ko-bezogenen Traps im Abschnitt **Kategorie** festgelegt sind, und legen Sie auch den entsprechenden Schweregrad im Abschnitt **Schweregrad** fest, wenn Sie das Ereignisalter festlegen. Wählen Sie im vorherigen Beispiel die `entityofs` Traps `entityup` `entitydown`, und aus.

Ereignisfilter planen

February 5, 2024

Wenn Sie nach dem Erstellen eines Filters für Ihre Regel nicht möchten, dass der Citrix Application Delivery Management (ADM) -Server jedes Mal eine Benachrichtigung sendet, wenn das generierte Ereignis die Filterkriterien erfüllt, können Sie den Filter so planen, dass er nur in bestimmten Zeitintervallen ausgelöst wird, z. B. täglich, wöchentlich oder monatlich.

Wenn Sie beispielsweise eine Systemwartungsaktivität für verschiedene Anwendungen auf Ihren Instanzen zu unterschiedlichen Zeiten geplant haben, können die Instanzen mehrere Alarme generieren.

Wenn Sie einen Filter für diese Alarme konfiguriert und E-Mail-Benachrichtigungen für diese Filter aktiviert haben, sendet der Server eine große Anzahl von E-Mail-Benachrichtigungen, wenn Citrix ADM diese Traps empfängt. Wenn Sie möchten, dass der Server diese E-Mail-Benachrichtigungen nur während eines bestimmten Zeitraums sendet, können Sie dies tun, indem Sie einen Filter planen.

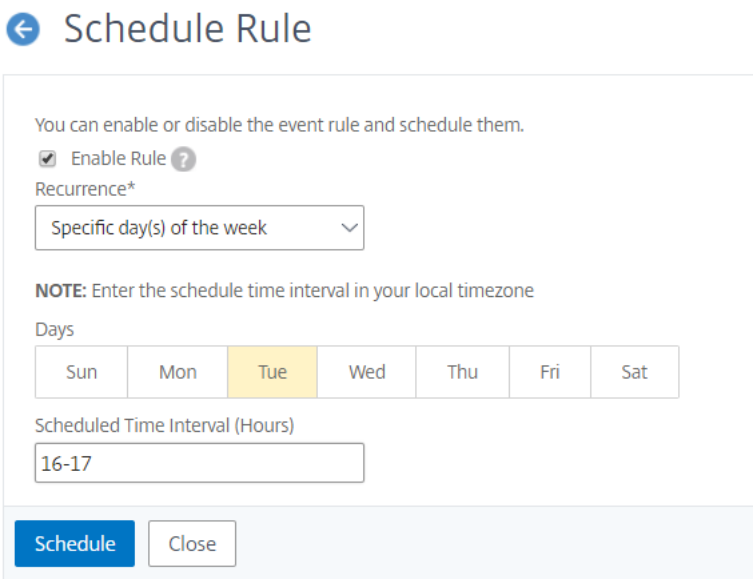
So planen Sie einen Filter mit NetScaler ADM:

1. Navigieren Sie im Citrix ADM zu **Netzwerke** > **Ereignisse** > **Regeln**.
2. Wählen Sie die Regel aus, für die Sie einen Filter planen möchten, und klicken Sie auf **Zeitplan anzeigen**.
3. Klicken Sie auf der Seite **Geplante Regel** auf **Zeitplan**, und geben Sie die folgenden Parameter an:

    - **Regel aktivieren** —Aktivieren Sie dieses Kontrollkästchen, um die Regel für geplante Ereignisse zu aktivieren.
    - **Wiederholung** - Intervall, in dem die Regel geplant werden soll. Wählen Sie entweder einen bestimmten Wochentag oder ein bestimmtes Datum in einem Monat aus.
    - **Tage**: Wählen Sie den Wochentag aus, an dem die Regel ausgeführt werden soll. Sie können mehrere Tage auswählen.
    - **Termine**: Geben Sie die Daten ein. Sie können mehrere Datumsangaben als kommagetrennte Werte eingeben.

- **Geplantes Zeitintervall (Stunden)** —Stunden, in denen die Regel geplant werden soll (verwenden Sie das 24-Stunden-Format).

4. Klicken Sie auf **Zeitplan**.



Wiederholte E-Mail-Benachrichtigungen für Ereignisse festlegen

February 5, 2024

Um sicherzustellen, dass alle kritischen Ereignisse behandelt werden und keine wichtigen E-Mail-Benachrichtigungen übersehen werden, können Sie sich dafür entscheiden, wiederholte E-Mail-Benachrichtigungen zu senden, wenn die Eventregeln die von Ihnen ausgewählten Kriterien erfüllen. Wenn Sie beispielsweise eine Ereignisregel für Instanzen mit Datenträgerausfällen erstellt haben und Sie benachrichtigt werden möchten, bis das Problem behoben ist, können Sie sich entscheiden, wiederholte E-Mail-Benachrichtigungen zu diesen Ereignissen zu erhalten.

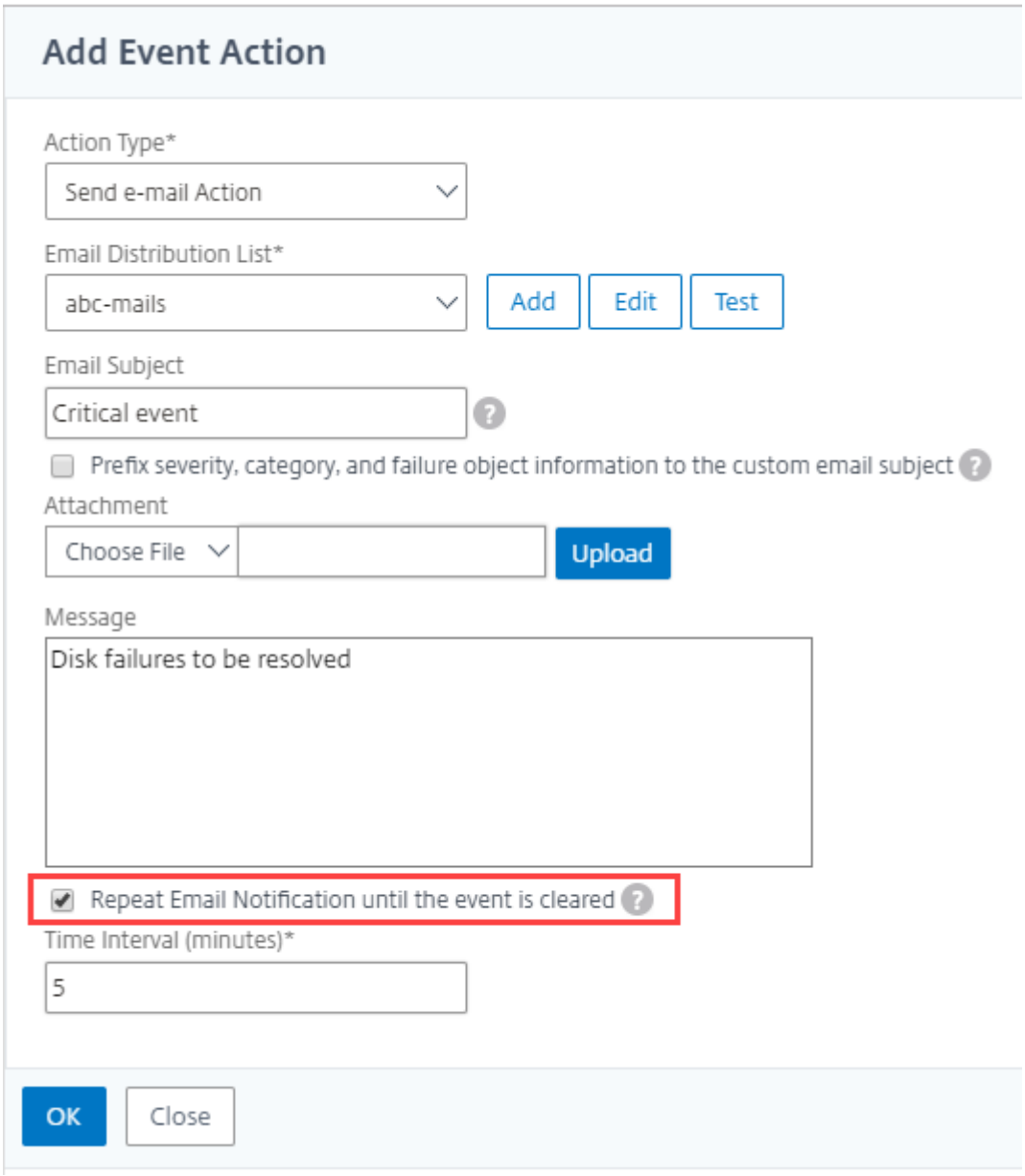
Diese E-Mail-Benachrichtigungen werden wiederholt in vordefinierten Intervallen gesendet, bis der Empfänger bestätigt, dass er die Benachrichtigung gesehen hat oder die Ereignisregel gelöscht wurde.

> **Hinweis**
>
> Ereignisse können nur automatisch gelöscht werden, wenn ein entsprechender “Clear”-Trap eingerichtet und von Ihrer Citrix Application Delivery Controller (ADC)-Instanz gesendet wird.
>
> Um ein Ereignis manuell zu löschen, können Sie Folgendes tun:

> - Navigieren Sie zu **Netzwerke > Ereignisse > Ereignisübersicht**, wählen Sie eine **Kategorie**, wählen Sie ein Ereignis in der Kategorie aus und klicken Sie auf **Löschen**.
> - Oder navigieren Sie zu **Netzwerke > Ereignisse > Ereignismeldungen**. Wählen Sie einen Instanztyp aus, wählen Sie ein Ereignis aus dem unten stehenden Raster aus, und klicken Sie auf **Löschen**.

So legen Sie wiederholte E-Mail-Benachrichtigungen von NetScaler ADM fest:

1. Navigieren Sie in Citrix Application Delivery Management (ADM) zu **Netzwerke** > **Ereignisse** > **Regeln**, und klicken Sie auf **Hinzufügen**, um eine Regel zu erstellen.
2. Legen Sie auf der Seite **Regel erstellen** die Regelparameter fest.
3. ****Klicken Sie unter Aktionen für Veranstaltungsregeln auf **Aktion hinzufügen** . Wählen Sie dann in der Dropdownliste****Aktionstyp die Option E-Mail-Aktion** senden** und wählen Sie eine **E-Mail-Verteilerliste**aus.
4. Sie können auch eine benutzerdefinierte Betreffzeile und eine Benutzernachricht hinzufügen und eine Anlage in Ihre E-Mail hochladen, wenn ein eingehendes Ereignis mit der konfigurierten Regel übereinstimmt.
5. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigung wiederholen, bis das Ereignis deaktiviert ist**.



Ereignisse unterdrücken

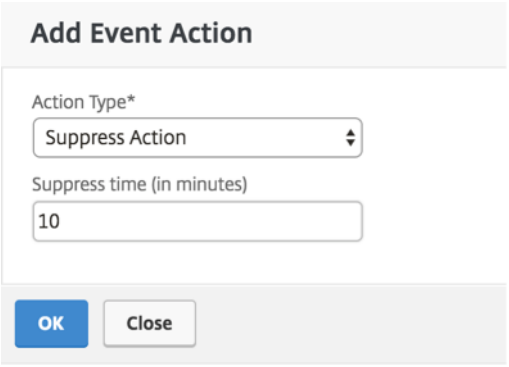
February 5, 2024

Wenn Sie die Ereignisaktion **Aktion unterdrücken** wählen, können Sie einen Zeitraum in Minuten konfigurieren, für den ein Ereignis unterdrückt oder gelöscht wird. Sie können das Ereignis mindestens 1 Minute unterdrücken.

> Hinweis:
>
> Sie können die Unterdrückungszeit auch als 0 Minuten konfigurieren und das bedeutet unendlich viel Zeit. Wenn Sie keine Zeitdauer angeben, betrachtet NetScaler ADM die Unterdrückungszeit als Null und läuft nie ab.

So unterdrücken Sie Ereignisse mithilfe von NetScaler ADM:

1. Navigieren Sie in Citrix Application Delivery Management (ADM) zu **Netzwerke** > **Ereignisse** > **Regeln**. Klicken Sie auf **Hinzufügen**.
2. Geben Sie alle Parameter an, die zum Erstellen einer Regel erforderlich sind.
3. Klicken Sie unter **Ereignisregelaktionen**auf **Aktion hinzufügen**, um Benachrichtigungsaktionen für das Ereignis zuzuweisen.
4. Wählen Sie auf der Seite "**Ereignisaktion hinzufügen** "in der Dropdownliste **Aktionstyp die Option Aktionunterdrücken** aus, und geben Sie den Zeitraum in Minuten an, für den ein Ereignis unterdrückt werden muss.
5. Klicken Sie auf **OK**.



Ereignisregeln erstellen

February 5, 2024

Sie können Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Regeln erleichtern die Überwachung einer großen Anzahl von Ereignissen, die in Ihrer Infrastruktur generiert werden.

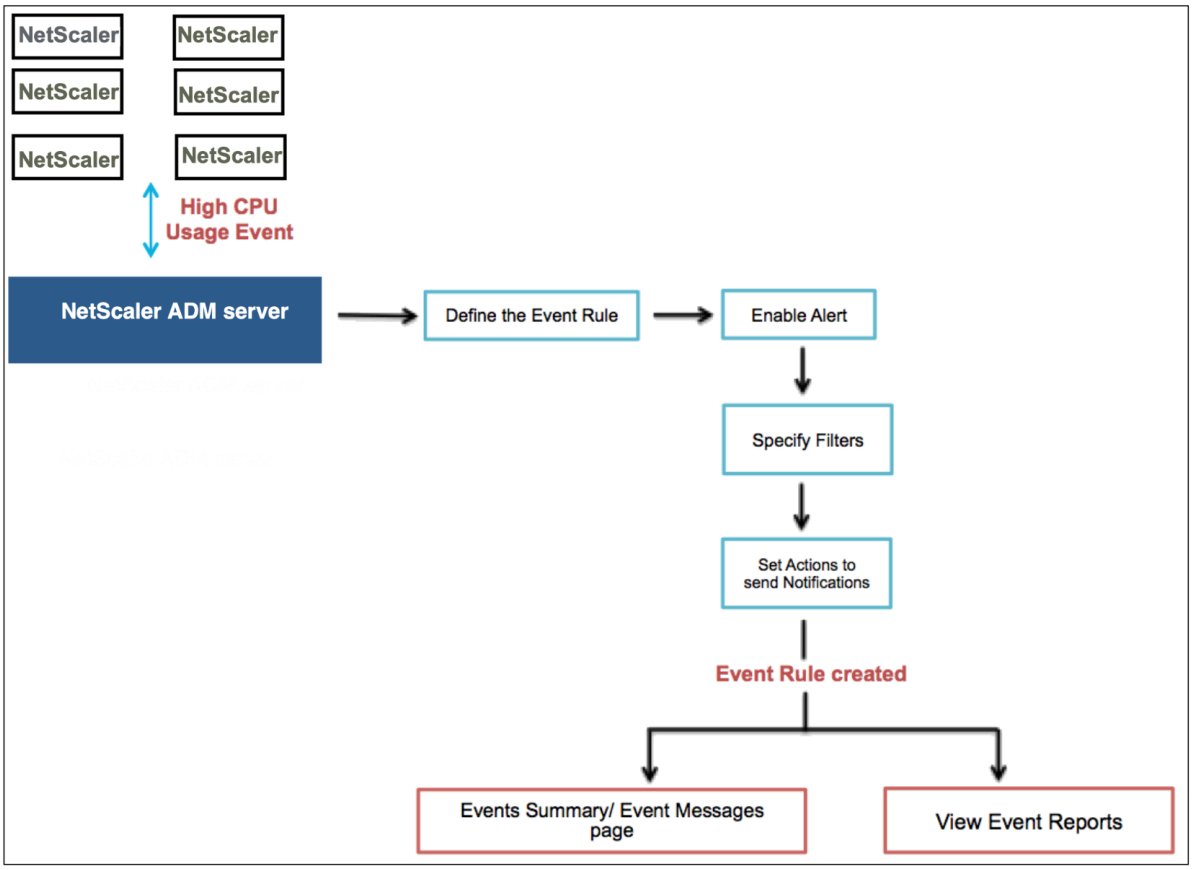
Sie können eine Reihe von Ereignissen filtern, indem Sie Regeln mit bestimmten Bedingungen konfigurieren und den Regeln Aktionen zuweisen. Wenn die generierten Ereignisse die Filterkriterien in der Regel erfüllen, wird die mit der Regel verknüpfte Aktion ausgeführt. Die Bedingungen für die Erstellung von Filtern sind: Schweregrad, Citrix Application Delivery Controller Instanzen (NetScaler ADC), Kategorie, Fehlerobjekte, Konfigurationsbefehle und Meldungen.

Sie können den Ereignissen die folgenden Aktionen zuweisen:

- **E-Mail-Aktion senden**: Senden Sie eine E-Mail für die Ereignisse, die den Filterkriterien entsprechen.
- **Trap-Aktion senden**: SNMP-Traps an ein externes Trap-Ziel senden oder weiterleiten
- **Befehlsaktion ausführen**: Führen Sie einen Befehl aus, wenn ein eingehendes Ereignis die konfigurierte Regel erfüllt.
- **Job-Aktion ausführen**: Die Ausführung eines Jobs ist für Ereignisse vorgesehen, die den von Ihnen angegebenen Filterkriterien entsprechen.
- **Aktion unterdrücken**: Unterdrückt das Löschen eines Ereignisses für einen bestimmten Zeitraum.
- **Slack-Benachrichtigungen**senden: Sende Benachrichtigungen auf dem konfigurierten Slack-Kanal für die Ereignisse, die den Filterkriterien entsprechen.
- **PagerDuty-Benachrichtigungen**senden: Senden Sie Ereignisbenachrichtigungen basierend auf den PagerDuty-Konfigurationen für die Ereignisse, die den Filterkriterien entsprechen.
- **ServiceNow-Benachrichtigungen senden**: Generieren Sie automatisch ServiceNow-Vorfälle für ein Ereignis, das den Filterkriterien entspricht.

Weitere Informationen finden Sie unter Aktionen für Ereignisregeln hinzufügen

Sie können Benachrichtigungen auch in einem bestimmten Intervall erneut senden lassen, bis ein Ereignis gelöscht wird. Außerdem können Sie die E-Mail mit einer bestimmten Betreffzeile, einer Benutzernachricht und einem Anhang anpassen.



Als Administrator möchten Sie beispielsweise Ereignisse mit hoher CPU-Auslastung für bestimmte NetScaler ADC-Instanzen überwachen, wenn diese Ereignisse zu einem Ausfall Ihrer NetScaler ADC-Instanzen führen können. Sie haben folgende Möglichkeiten:

- Erstellen Sie eine Regel zur Überwachung der Instanzen und geben Sie eine Aktion an, mit der Sie eine E-Mail-Benachrichtigung erhalten, wenn ein Ereignis in der Kategorie “Hohe CPU-Auslastung”eintritt.
- Planen Sie die Regel so, dass sie zu einer bestimmten Zeit ausgeführt wird, z. B. zwischen 11 und 23 Uhr, damit Sie nicht jedes Mal benachrichtigt werden, wenn ein Ereignis generiert wird.

Das Konfigurieren einer Ereignisregel umfasst die folgenden Aufgaben:

1. Definieren Sie die Regel
2. Wählen Sie den Schweregrad des Ereignisses aus, das die Regel erkennt
3. Ereigniskategorie angeben
4. NetScaler ADC-Instanzen angeben, für die die Regel gilt
5. Fehlerobjekte auswählen
6. Erweiterte Filter angeben

7. Aktionen angeben, die ausgeführt werden sollen, wenn die Regel ein Ereignis erkennt

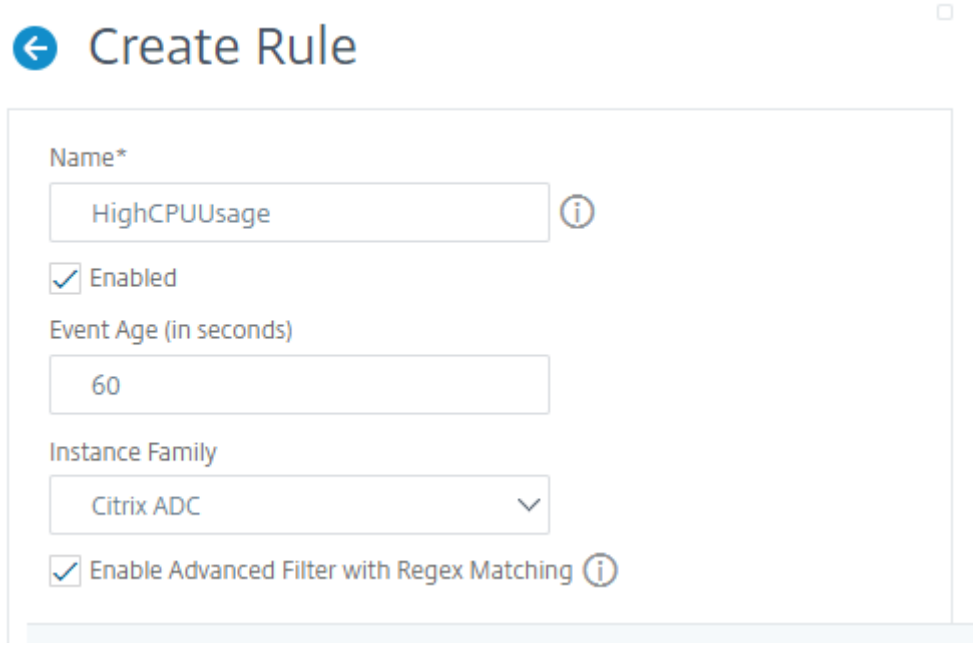
Schritt 1 - Definieren einer Ereignisregel

Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Regeln**, und klicken Sie auf **Hinzufügen**. Wenn Sie die Regel aktivieren möchten, **aktivieren Sie das Kontrollkästchen Regel aktivieren**.

Sie können die Option **Ereignisalter** festlegen, um das Zeitintervall (in Sekunden) anzugeben, nach dem NetScaler ADM eine Ereignisregel aktualisiert.

> Hinweis:
>
> Der Mindestwert für das Ereignisalter ist 60 Sekunden. Wenn Sie das Feld **Ereignisalter** leer lassen, wird die Ereignisregel unmittelbar nach dem Auftreten des Ereignisses angewendet.

Basierend auf dem obigen Beispiel möchten Sie möglicherweise jedes Mal per E-Mail benachrichtigt werden, wenn Ihre NetScaler ADC-Instanz 60 Sekunden oder länger ein Ereignis mit “hoher CPU-Auslastung”aufweist. Sie können das Ereignisalter auf 60 Sekunden festlegen, sodass Sie jedes Mal, wenn Ihre NetScaler ADC-Instanz 60 Sekunden oder länger ein Ereignis mit “hoher CPU-Auslastung” aufweist, eine E-Mail-Benachrichtigung mit Details zum Ereignis erhalten.



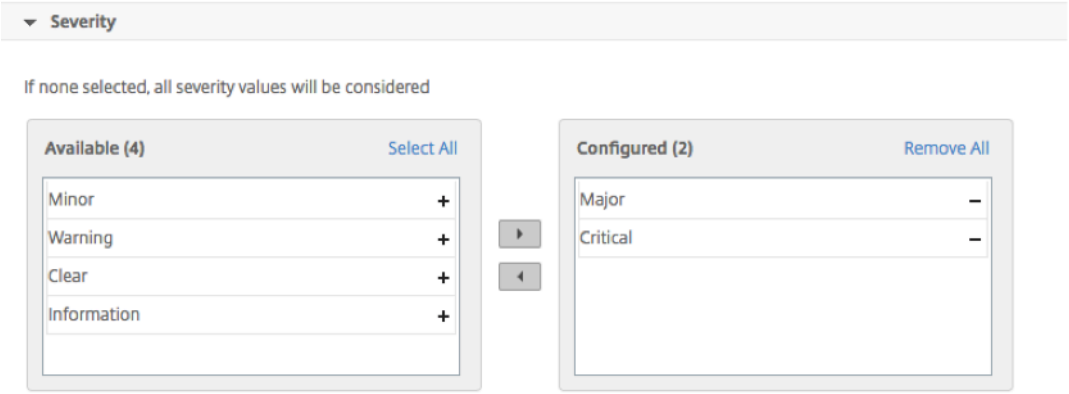
Sie können Ereignisregeln auch nach **Instanzfamilie** filtern, um die NetScaler ADC-Instanz zu verfolgen, von der NetScaler ADM ein Ereignis empfängt.

Wenn Sie einen anderen regulären Ausdruck als den Mustervergleich mit Sternchen (*) einschließen möchten, wählen Sie **Erweiterte Filter mit Regex-Abgleich aktivieren**aus.

Schritt 2 —Wählen Sie den Schweregrad des Ereignisses

Sie können Ereignisregeln erstellen, die die Standardeinstellungen für den Schweregrad verwenden. Schweregrad gibt den aktuellen Schweregrad der Ereignisse an, denen Sie die Ereignisregel hinzufügen möchten.

Sie können die folgenden Schweregrade definieren: Kritisch, Major, Minor, Warnung, Löschen und Information.

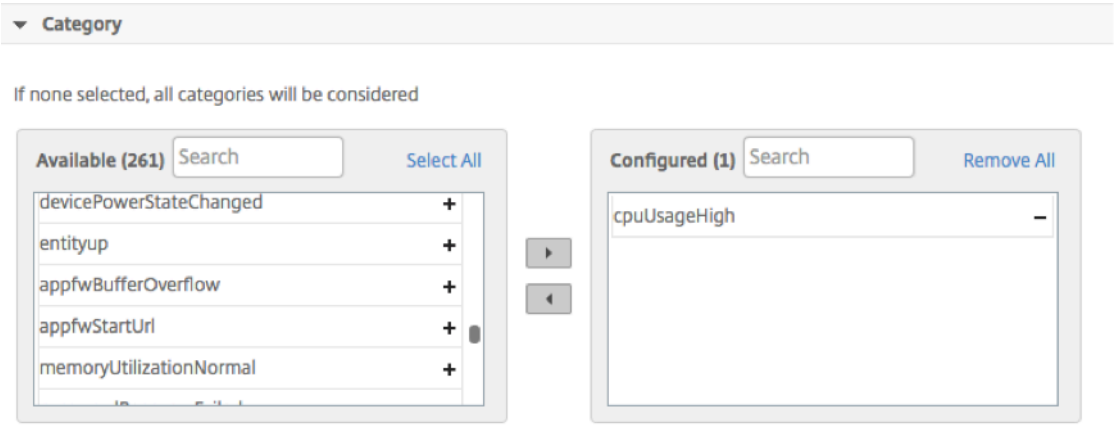


> **Hinweis**
>
> Sie können den Schweregrad sowohl für generische als auch für fortgeschrittene Ereignisse konfigurieren. Um den Schweregrad für NetScaler ADC-Instanzen zu ändern, die auf NetScaler ADM verwaltet werden, navigieren Sie zu **Netzwerke** > **Ereignisse** > **Ereigniseinstellungen**. Wählen Sie die **Kategorie** aus, für die Sie den Schweregrad des Ereignisses konfigurieren möchten, und klicken Sie auf **Schweregrad konfigurieren**. Weisen Sie einen neuen Schweregrad zu, und klicken Sie auf **OK**.

Schritt 3 —Event-Kategorie angeben

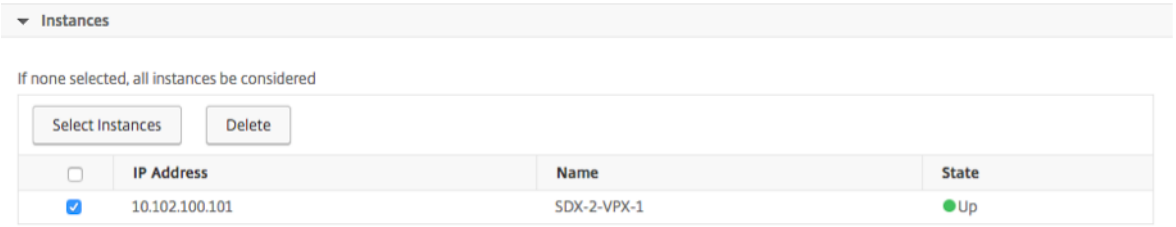
Sie können die Kategorie oder Kategorien der Ereignisse angeben, die von Ihren NetScaler ADC-Instanzen generiert werden. Alle Kategorien werden auf NetScaler ADC-Instanzen erstellt. Diese Kategorien werden dann mit NetScaler ADM zugeordnet, das zur Definition von Ereignisregeln verwendet werden kann. Wählen Sie die Kategorie aus, die Sie berücksichtigen möchten, und verschieben Sie sie aus der Tabelle **Verfügbar** in die Tabelle **Konfiguriert**.

Im obigen Beispiel müssen Sie “cpuUsageHigh”als Ereigniskategorie aus der angezeigten Tabelle auswählen.



Schritt 4 - Angeben von NetScaler ADC-Instanzen

Wählen Sie die IP-Adressen der NetScaler ADC-Instanzen aus, für die Sie die Ereignisregel definieren möchten. Klicken Sie im Abschnitt **Instanzen** auf **Instanzen auswählen**. Wählen Sie auf der Seite **Instanzen auswählen** Ihre Instanzen aus und klicken Sie auf **Auswählen**.



Schritt 5 - Auswählen von Fehlerobjekten

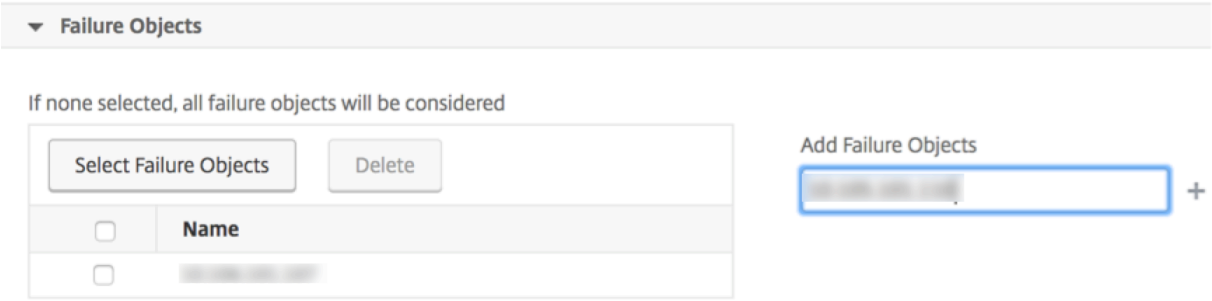
Sie können entweder ein Versagensobjekt aus der bereitgestellten Liste auswählen oder ein Fehlerobjekt hinzufügen, für das ein Ereignis generiert wurde. Sie können auch einen regulären Ausdruck angeben, um Fehlerobjekte hinzuzufügen. Abhängig vom angegebenen regulären Ausdruck werden die Fehlerobjekte automatisch zur Liste hinzugefügt. Fehlerobjekte sind Entitätsinstanzen oder Leistungsindikatoren, für die ein Ereignis generiert wurde.

> **Wichtig**
>
> Um Fehlerobjekte mit regulärem Ausdruck aufzulisten, wählen Sie in Schritt 1**Erweiterten Filter mit Regex-Abgleich aktivieren**.

Das Fehlerobjekt wirkt sich auf die Art und Weise aus, in der ein Ereignis verarbeitet wird, und stellt sicher, dass es genau das Problem wie benachrichtigt widerspiegelt. Mit diesem Filter können Sie Probleme auf den Fehlerobjekten schnell verfolgen und die Ursache für ein Problem identifizieren.

Wenn ein Benutzer beispielsweise Anmeldeprobleme hat, ist das Fehlerobjekt hier der Benutzername oder das Kennwort, z. `nsroot`B.

Diese Liste kann Leistungsindikatornamen für alle mit Schwellenwert verbundenen Ereignisse, Entitätsnamen für alle Entity-bezogenen Ereignisse, Zertifikatnamen für zertifikatbezogene Ereignisse usw. enthalten.

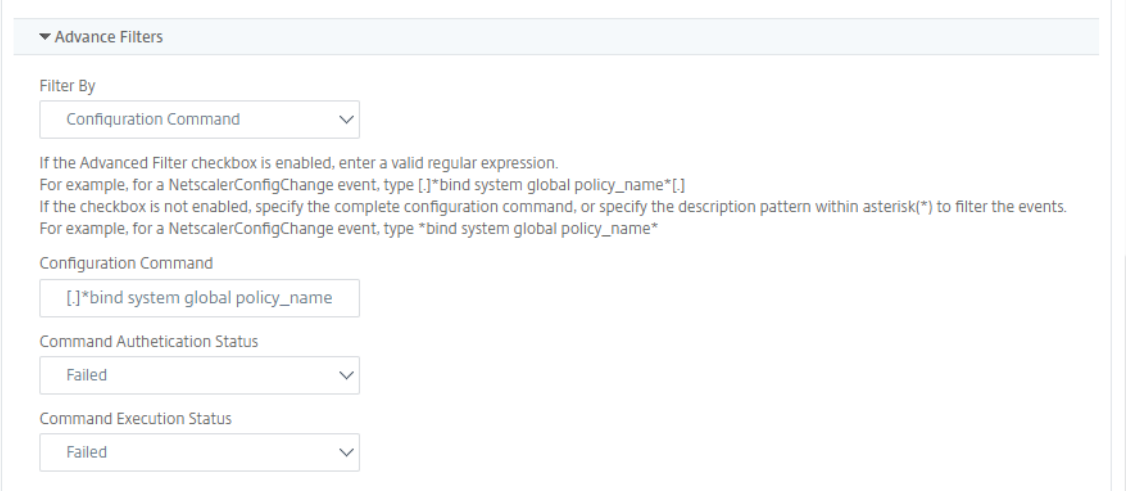


Schritt 6 - Angeben von erweiterten Filtern

Sie können eine Ereignisregel weiter filtern nach:

- **Konfigurationsbefehle** - Sie können den vollständigen Konfigurationsbefehl angeben oder einen regulären Ausdruck angeben, um Ereignisse zu filtern.

  Sie können die Ereignisregel weiter nach dem Authentifizierungsstatus des Befehls und/oder seinem Ausführungsstatus filtern. Geben Sie beispielsweise für a `NetscalerConfigChange event`, ein `[.]*bind system global policy_name[.]*`.

- **Meldungen** - Sie können die vollständige Nachrichtenbeschreibung angeben oder einen regulären Ausdruck angeben, um die Ereignisse zu filtern.
  Geben Sie beispielsweise für ein Ereignis `NetscalerConfigChange` die Option `[.]*`

`ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)` ein.

Schritt 7 —Aktionen für Ereignisregeln hinzufügen

Sie können Ereignisregelaktionen hinzufügen, um Benachrichtigungsaktionen für ein Ereignis zuzuweisen. Diese Benachrichtigungen werden gesendet oder ausgeführt, wenn ein Ereignis die oben festgelegten Filterkriterien erfüllt. Sie können die folgenden Ereignisaktionen hinzufügen:

- E-Mail senden Action
- Trap-Aktion senden
- Befehls-Aktion ausführen
- Job-Aktion ausführen
- Aktion unterdrücken
- Slack Benachrichtigungen senden
- PagerDuty-Benachrichtigungen senden
- ServiceNow-Benachrichtigungen senden

So richten Sie eine E-Mail-Ereignisregelaktion ein

Wenn Sie den Aktionstyp Aktion E-Mail senden auswählen, wird eine E-Mail ausgelöst, wenn die Ereignisse die definierten Filterkriterien erfüllen. Sie müssen entweder eine E-Mail-Verteilerliste erstellen, indem Sie E-Mail-Server- oder E-Mail-Profildetails angeben, oder Sie können eine E-Mail-Verteilerliste auswählen, die Sie zuvor erstellt haben.

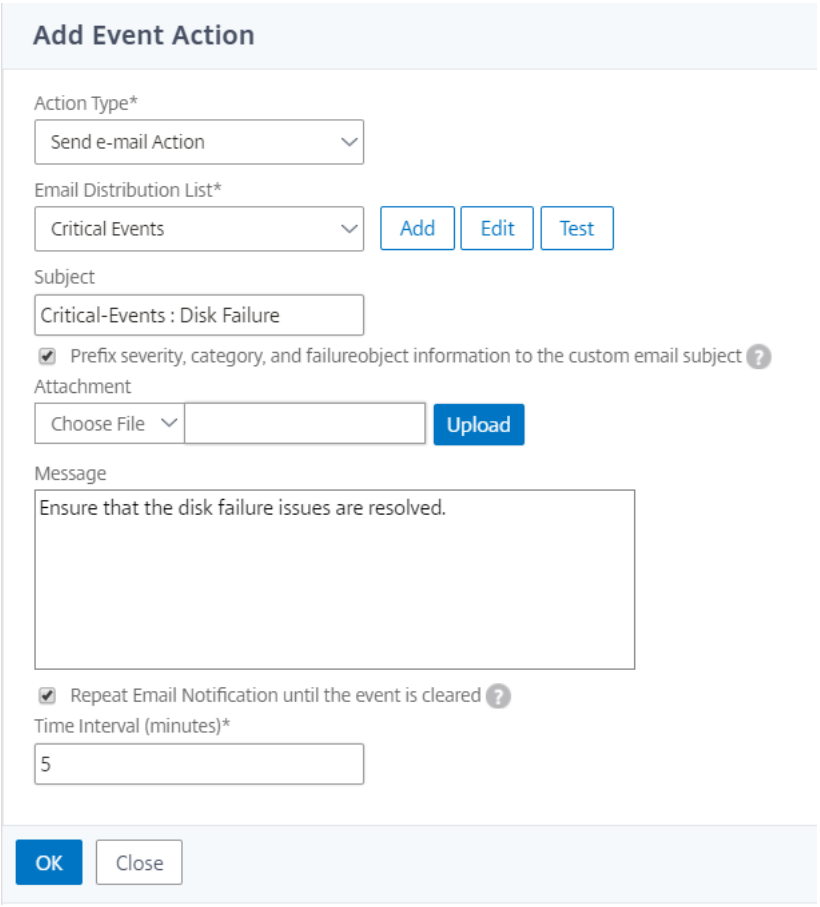
Aufgrund einer hohen Anzahl virtueller Server, die in NetScaler ADM konfiguriert werden, erhalten Sie möglicherweise täglich eine hohe Anzahl von E-Mails. Die E-Mails haben eine standardmäßige Betreffzeile, die Informationen über den Schweregrad des Ereignisses, die Kategorie des Ereignisses und das Fehlerobjekt enthält. Die Betreffzeile enthält jedoch keine Informationen über den Namen

des virtuellen Servers, von dem diese Ereignisse stammen. Sie haben jetzt die Möglichkeit, einige zusätzliche Informationen wie den Namen der betroffenen Entität, also den Namen des Fehlerobjekts, einzufügen.

Sie können auch eine benutzerdefinierte Betreffzeile und eine Benutzernachricht hinzufügen und einen Anhang in Ihre E-Mail hochladen, wenn ein eingehendes Ereignis mit der konfigurierten Regel übereinstimmt.

Beim Senden von E-Mails für Ereignisbenachrichtigungen möchten Sie möglicherweise eine Test-E-Mail senden, um die konfigurierten Einstellungen zu testen. Mit der Schaltfläche "Test"können Sie jetzt eine Test-E-Mail senden, nachdem Sie einen E-Mail-Server, zugehörige verteilte Listen und andere Einstellungen konfiguriert haben. Diese Funktion stellt sicher, dass die Einstellungen einwandfrei funktionieren.

Sie können auch sicherstellen, dass alle kritischen Ereignisse behandelt werden und keine wichtigen E-Mail-Benachrichtigungen verpasst werden, indem **Sie das Kontrollkästchen E-Mail-Benachrichtigung wiederholen, bis das Ereignis deaktiviert ist**, um wiederholte E-Mail-Benachrichtigungen für Ereignisregeln zu senden, die die von Ihnen ausgewählten Kriterien erfüllen. Wenn Sie beispielsweise eine Ereignisregel für Instanzen mit Datenträgerausfällen erstellt haben und Sie benachrichtigt werden möchten, bis das Problem behoben ist, können Sie sich entscheiden, wiederholte E-Mail-Benachrichtigungen zu diesen Ereignissen zu erhalten.



So legen Sie die Aktion Trap-Ereignisregel fest

Wenn Sie den Ereignistyp **Trap-Aktion senden** auswählen, werden SNMP-Traps an ein externes Trap-Ziel gesendet oder weitergeleitet. Durch die Definition einer Trap-Verteilerliste (oder eines Trap-Ziels und Trap-Profildetails) werden Trap-Nachrichten an bestimmte Trap-Listener gesendet, wenn die Ereignisse die definierten Filterkriterien erfüllen.

So legen Sie die Aktion Befehl ausführen fest

Wenn Sie die **Ereignisaktion Befehlsaktion ausführen** auswählen, können Sie einen Befehl oder ein Skript erstellen, das in NetScaler ADM für Ereignisse ausgeführt werden kann, die einem bestimmten Filterkriterium entsprechen.

Sie können auch die folgenden Parameter für das Skript **Befehlsaktion ausführen** festlegen:

Parameter	Beschreibung
$source	Dieser Parameter entspricht der Quell-IP-Adresse des empfangenen Ereignisses.
$category	Dieser Parameter entspricht dem Typ der Fallen, die in der Kategorie des Filters definiert sind.
$entity	Dieser Parameter entspricht den Entitätsinstanzen oder Leistungsindikatoren, für die ein Ereignis generiert wurde. Sie kann die Leistungsindikatornamen für alle Ereignisse im Zusammenhang mit dem Schwellenwert, Entitätsnamen für alle entitätsbezogenen Ereignisse und Zertifikatsnamen für alle zertifikatbezogenen Ereignisse enthalten.
$severity	Dieser Parameter entspricht dem Schweregrad des Ereignisses.
$ failure.obj	Das Fehlerobjekt beeinflusst die Art und Weise, wie ein Ereignis verarbeitet wird, und stellt sicher, dass das Fehlerobjekt genau das gemeldete Problem widerspiegelt. Dies kann verwendet werden, um Probleme schnell aufzuspüren und den Grund für den Fehler zu identifizieren, anstatt einfach rohe Ereignisse zu melden.

> **Hinweis**
>
> Während der Befehlsausführung werden diese Parameter durch tatsächliche Werte ersetzt.

Stellen Sie sich beispielsweise vor, dass Sie eine Aktion zum Ausführen von Befehlen festlegen möchten, wenn der Status eines virtuellen Lastausgleichsservers **auf Nicht verfügbar**ist Als Administrator sollten Sie eine schnelle Problemumgehung in Betracht ziehen, indem Sie einen weiteren virtuellen Server hinzufügen. In NetScaler ADM können Sie:

- Schreiben Sie eine Skriptdatei (.sh).

  Im Folgenden finden Sie eine Beispielskriptdatei (.sh):

```
1  #!/bin/sh
2  source=$1
3  failureobj=$2
```



```
payload='{
"params":{
"warning":"YES" }
,"lbvserver":{
"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","
   port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"
   PASSIVE","appflowlog":"ENABLED","
bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
 }
'
url="http://$source/nitro/v1/config/lbvserver"
curl --insecure -basic -u nsroot:nsroot -H "Content-type:
   application/json" -X POST -d $payload $url

<!--NeedCopy-->
```

- Speichern Sie die .sh-Datei an einem beliebigen persistenten Ort auf dem NetScaler ADM Agent. Beispiel: `/var`.
- Geben Sie den Speicherort der SH-Datei in NetScaler ADM an, der ausgeführt werden soll, wenn die Regelkriterien erfüllt sind.

So legen Sie die Aktion **Befehl ausführen** zum Erstellen eines neuen virtuellen Servers fest:

1. Definieren Sie die Regel
2. Wählen Sie den Schweregrad des Ereignisses
3. Wählen Sie die Event-Kategorie **entitydown**
4. Wählen Sie die Instanz aus, für die der virtuelle Server konfiguriert ist
5. Wählen oder erstellen Sie ein Fehlerobjekt für den virtuellen Server
6. Klicken Sie unter **Ereignisregelaktionen**auf **Aktion hinzufügen**, und wählen Sie in der Liste ****Aktionstyp die Option Befehlsaktion** ausführen** aus.
7. Klicken **Sie unter Liste der Befehlsausführung**auf **Hinzufügen**.

   Die Seite “Befehlsverteilerliste erstellen”wird angezeigt.

   a) Geben Sie unter **Profilname**einen Namen Ihrer Wahl an

   b) Geben Sie **unter Run Command**den NetScaler ADM Agent-Speicherort an, in dem das Skript ausgeführt werden muss. Beispiel: `/sh/var/demo.sh $source $failureobj`.

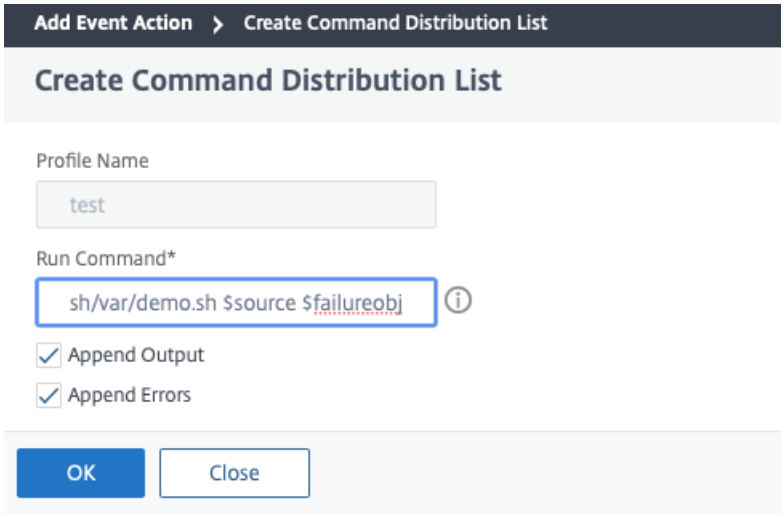
   c) Wählen Sie **Ausgabe anhängen** und **Fehler anhängen**.

   > **Hinweis**
   >
   > Sie können die Optionen **Ausgabe anfügen** und **Fehler anhängen** aktivieren, wenn Sie die Ausgabe und die Fehler speichern möchten, die bei der Ausführung eines

> Befehlsskripts in den NetScaler ADM -Serverprotokolldateien generiert wurden (falls vorhanden). Wenn Sie diese Optionen nicht aktivieren, verwirft NetScaler ADM alle Ausgaben und Fehler, die während der Ausführung des Befehlsskripts generiert wurden.

d) Klicken Sie auf **Erstellen**.

8. Klicken Sie auf der Seite **Ereignisaktion hinzufügen** auf **OK**.



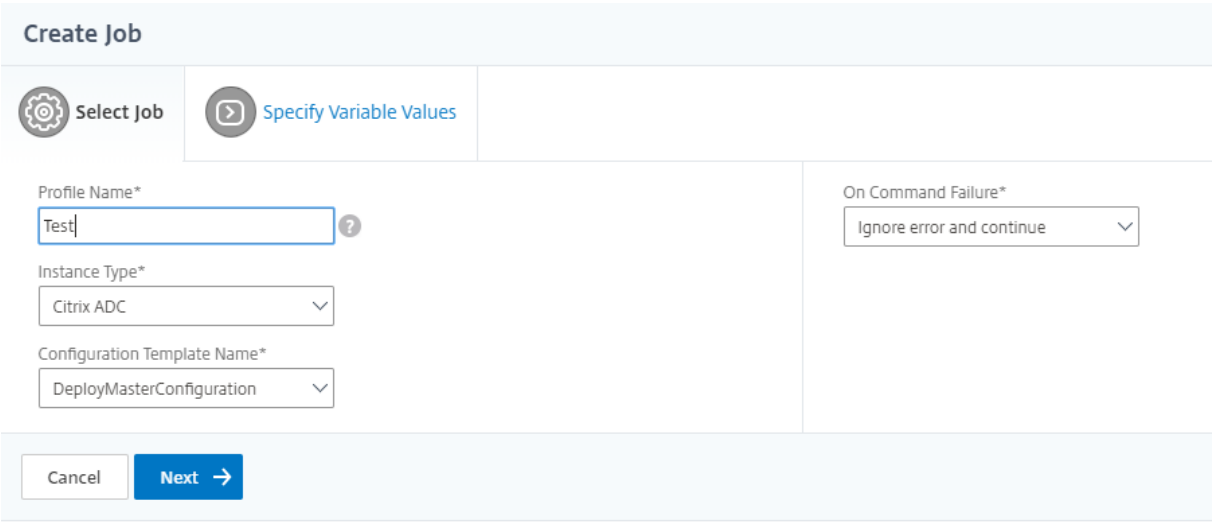
> **Hinweis**
>
> Sie können die Optionen **Ausgabe anfügen** und **Fehler anhängen** aktivieren, wenn Sie die Ausgabe und die Fehler speichern möchten, die bei der Ausführung eines Befehlsskripts in den NetScaler ADM -Serverprotokolldateien generiert wurden (falls vorhanden). Wenn Sie diese Optionen nicht aktivieren, verwirft NetScaler ADM alle Ausgaben und Fehler, die während der Ausführung des Befehlsskripts generiert wurden.

So legen Sie die `Execute` Job-Aktion fest

Durch das Erstellen eines Profils mit Konfigurationsaufträgen wird ein Job als integrierter Job oder benutzerdefinierter Job für Instanzen NetScaler ADC, NetScaler ADC SDX und Citrix SD-WAN WO für Ereignisse und Alarme ausgeführt, die den von Ihnen angegebenen Filterkriterien entsprechen.

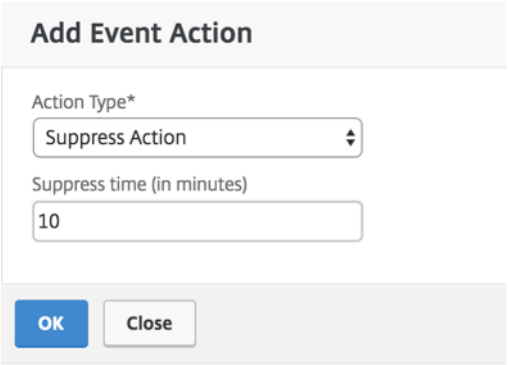
1. Klicken Sie unter **Ereignisregelaktionen**auf **Aktion hinzufügen** und wählen Sie aus der Dropdownliste ****Aktionstyp die Option Job-Aktion** ausführen** aus.
2. Erstellen Sie ein Profil mit einem Job, den Sie ausführen möchten, wenn die Ereignisse die definierten Filterkriterien erfüllen.
3. Geben Sie beim Erstellen eines Auftrags einen Profilnamen, den Instanztyp, die Konfigurationsvorlage und die Aktion an, die Sie ausführen möchten, wenn die Befehle für den Auftrag fehlschlagen.

4. Geben Sie anhand des ausgewählten Instanztyps und der gewählten Konfigurationsvorlage die Variablenwerte an, und klicken Sie auf **Fertig stellen**, um den Job zu erstellen.



So legen Sie die Aktion Unterdrücken fest

Wenn Sie die Ereignisaktion **Aktion unterdrücken** auswählen, können Sie einen Zeitraum in Minuten konfigurieren, für den ein Ereignis unterdrückt oder gelöscht wird. Sie können das Ereignis mindestens 1 Minute unterdrücken.



So legen Sie Slack -Benachrichtigungen von NetScaler ADM fest

Konfigurieren Sie den erforderlichen Slack-Channel, indem Sie den Profilnamen und die Webhook-URL in der NetScaler ADM GUI angeben. Die Ereignisbenachrichtigungen werden dann an diesen Kanal gesendet. Sie können mehrere Slack Kanäle konfigurieren, um diese Benachrichtigungen zu erhalten

1. Navigieren Sie in Citrix ADM zu**Netzwerke**>**Ereignisse**>**Regeln**, und klicken Sie auf**Hinzufügen**, um eine Regel zu erstellen.

2. Legen Sie auf der Seite **Regel erstellen**die Regelparameter wie Schweregrad und Kategorie fest. Wählen Sie Instanzen und auch Fehlerobjekte aus, die überwacht werden müssen.
3. Klicken Sie unter**Ereignisregelaktionen**auf**Aktion hinzufügen**. Wähle dann in der Liste**Aktionstyp**die Option**Slack-Benachrichtigungen senden** aus und wähle **Slack-Profilliste aus.**
4. Sie können auch eine Slack-Profilliste hinzufügen, indem Sie neben dem Feld **Slack-Profilliste** auf **Hinzufügen** klicken.
5. Geben Sie die folgenden Parameter ein, um eine Profilliste zu erstellen:
    a) **Profilname**. Geben Sie einen Namen für die Profilliste ein, die auf NetScaler ADM konfiguriert werden soll.
    b) **Name des Kanals**. Geben Sie den Namen des Slack-Kanals ein, an den die Ereignisbenachrichtigungen gesendet werden sollen.
    c) **Webhook-URL**. Geben Sie die Webhook-URL des Kanals ein, den Sie zuvor eingegeben haben. Eingehende Webhooks sind eine einfache Möglichkeit, Nachrichten aus externen Quellen in Slack zu posten. Die URL ist intern mit dem Kanalnamen verknüpft und alle Ereignisbenachrichtigungen werden an diese URL gesendet, um auf dem angegebenen Slack -Kanal gepostet zu werden. Ein Beispiel für Webhook lautet wie folgt: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK
6. Klicken Sie auf **Erstellen**, und klicken Sie im Fenster **Ereignisaktion hinzufügen** auf **OK**.

> **Hinweis:**
>
> Du kannst die Slack-Profile auch hinzufügen, indem du zu **System** > **Benachrichtigungen** > **Slack-Profile navigierst**. Klicken Sie auf **Hinzufügen** und erstellen Sie das Profil wie im vorherigen Abschnitt beschrieben.

Du kannst den Status der von dir erstellten Slack-Profile anzeigen.

Ihre Ereignisregel wird jetzt mit geeigneten Filtern und gut definierten Ereignisregelaktionen erstellt.

So richten Sie PagerDuty-Benachrichtigungen von NetScaler ADM ein

Sie können in NetScaler ADM ein PagerDuty-Profil als Option hinzufügen, um die Vorfallbenachrichtigungen basierend auf Ihren PagerDuty-Konfigurationen zu überwachen. Mit PagerDuty können Sie Benachrichtigungen per E-Mail, SMS, Push-Benachrichtigung und Telefonanruf auf einer registrierten Nummer konfigurieren.

Bevor Sie ein PagerDuty-Profil in NetScaler ADM hinzufügen, stellen Sie sicher, dass Sie die erforderlichen Konfigurationen in PagerDuty abgeschlossen haben. Weitere Informationen finden Sie in der PagerDuty-Dokumentation.

Sie können Ihr PagerDuty-Profil als eine der Optionen auswählen, um Benachrichtigungen für die folgenden Funktionen zu erhalten:

- **Ereignisse** —Liste der Ereignisse, die für NetScaler ADC-Instanzen generiert werden.
- **Lizenzen** —Liste der Lizenzen, die derzeit aktiv sind, bald ablaufen usw.
- **SSL-Zertifikate** —Liste der SSL-Zertifikate, die NetScaler ADC-Instanzen hinzugefügt werden.

Um ein PagerDuty-Profil in ADM hinzuzufügen:

1. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler ADM an.
2. Navigieren Sie zu **System** > **Benachrichtigungen** > **PagerDuty Profile**.
3. Klicken Sie auf **Hinzufügen**, um ein neues Profil zu erstellen.
4. Auf der Seite PagerDuty-Profil erstellen:
   a) Geben Sie einen Profilnamen Ihrer Wahl an.
   b) Geben Sie den **Integrationsschlüssel ein**.

      Sie können den Integrationsschlüssel von Ihrem PagerDuty-Portal erhalten.
   c) Klicken Sie auf **Erstellen**.

   Anwendungsfall:

   Stellen Sie sich ein Szenario vor, das Sie

   - möchten Benachrichtigungen an Ihr PagerDuty-Profil senden.
   - habe Telefonanruf als Option in PagerDuty konfiguriert, um Benachrichtigungen zu erhalten.
   - möchte Telefonanrufwarnungen für NetScaler ADC-Ereignisse erhalten.

   Schrittfolge zum Konfigurieren:

   a) Navigiere zu **Ereignisse** > **Regeln**
   b) Konfigurieren Sie auf der Seite **Regel erstellen** alle anderen Parameter, um eine Regel zu erstellen.
   c) Klicken **Sie unter Regelaktionen erstellen**auf **Aktion hinzufügen**.

      Die Seite **“Ereignisaktion hinzufügen** “wird angezeigt.

i. Wählen Sie unter **Aktionstyp**die Option **PagerDuty-Benachrichtigungen senden**aus.

ii. Wählen Sie Ihr PagerDuty-Profil aus und klicken Sie auf **OK**.

Sobald die Konfiguration abgeschlossen ist, erhalten Sie einen Anruf, wenn ein neues Ereignis für die NetScaler ADC Instanz generiert wird. Aus dem Telefonanruf können Sie entscheiden:

- Bestätigen Sie das Ereignis
- Markiere es als gelöst
- Eskalieren Sie zu einem anderen Teammitglied

So generieren Sie ServiceNow-Vorfälle automatisch aus NetScaler ADM

Sie können ServiceNow-Vorfälle für NetScaler ADM-Ereignisse automatisch generieren, indem Sie das ServiceNow-Profil auf der NetScaler ADM-GUI auswählen. Sie müssen das ServiceNow-Profil in Citrix ADM auswählen, um eine Ereignisregel zu konfigurieren.

Bevor Sie eine Ereignisregel zum automatischen Generieren von ServiceNow-Vorfällen konfigurieren, integrieren Sie NetScaler ADM in eine ServiceNow-Instanz. Weitere Informationen finden Sie unter Konfigurieren des ITSM-Adapters für ServiceNow.

Um eine Ereignisregel zu konfigurieren, navigieren Sie zu **Ereignisse** > **Regeln**.

1. Konfigurieren Sie auf der Seite **Regel erstellen** alle anderen Parameter, um eine Regel zu erstellen.
2. Klicken **Sie unter Regelaktionen erstellen**auf **Aktion hinzufügen**.

   Die Seite **“Ereignisaktion hinzufügen** ‘‘wird angezeigt.

   a) Wählen Sie **unter Aktionstyp**die Option **ServicNow-Benachrichtigungen senden**aus.

   b) Wählen Sie **ServiceNow ServiceNow-Profil**das Profil **Citrix_Workspace_SN** aus der Liste aus.

   c) Klicken Sie auf **OK**.

Gemeldeten Schweregrad von Ereignissen auf NetScaler ADC-Instanzen ändern

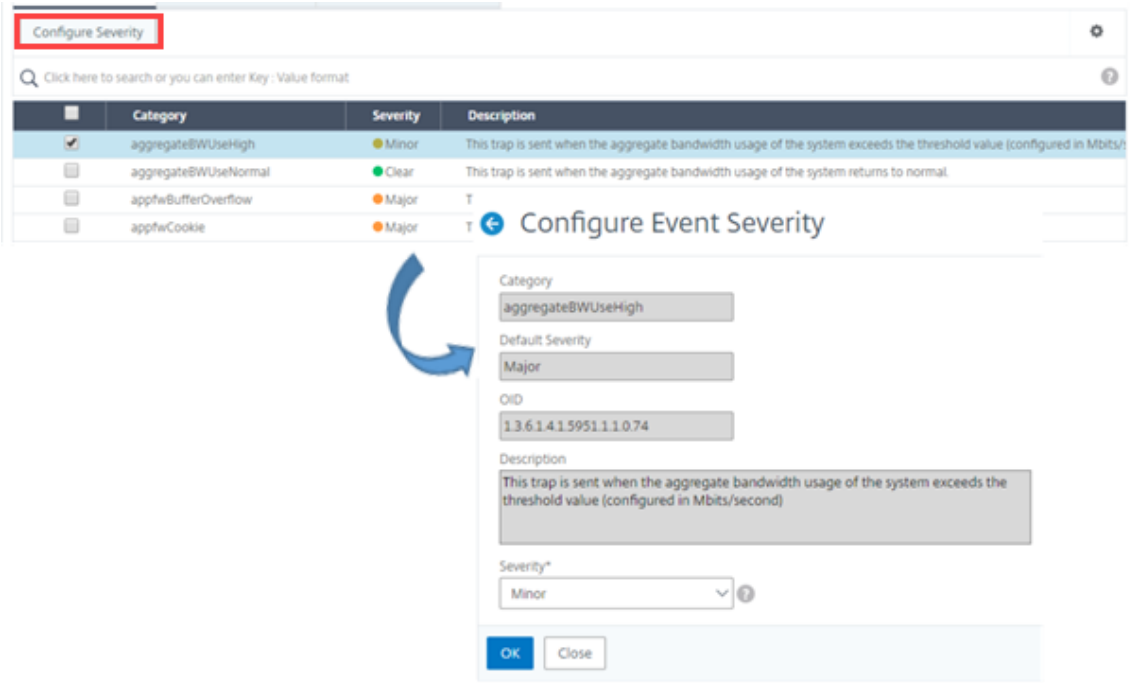
February 5, 2024

Sie können die Berichterstattung über Ereignisse verwalten, die auf all Ihren Geräten generiert wurden, sodass Sie Ereignisdetails zu einem bestimmten Ereignis in einer bestimmten Instanz einsehen und Berichte auf der Grundlage des Schweregrads des Ereignisses einsehen können. Sie können Ereignisregeln erstellen, die die Standardeinstellungen für den Schweregrad verwenden, und Sie können die Schweregradeinstellungen ändern. Sie können den Schweregrad für allgemeine und unternehmensspezifische Ereignisse konfigurieren.

Sie können die folgenden Schweregrade definieren: Kritisch, Groß, Minor, Warnung und Klar.

So ändern Sie den Schweregrad des Ereignisses:

1. Navigieren Sie zu **Netzwerke > Ereignisse > Event-Einstellungen**.
2. Klicken Sie auf die Registerkarte für den Instanztyp von Citrix Application Delivery Controller (ADC), den Sie ändern möchten. Wählen Sie dann die Kategorie aus der Liste aus und klicken Sie auf **Schweregrad konfigurieren**.
3. Wählen **Sie unter Konfigurieren des Ereignisschweregrads**den Schweregrad aus der Drop-downliste aus.
4. Klicken Sie auf **OK**.

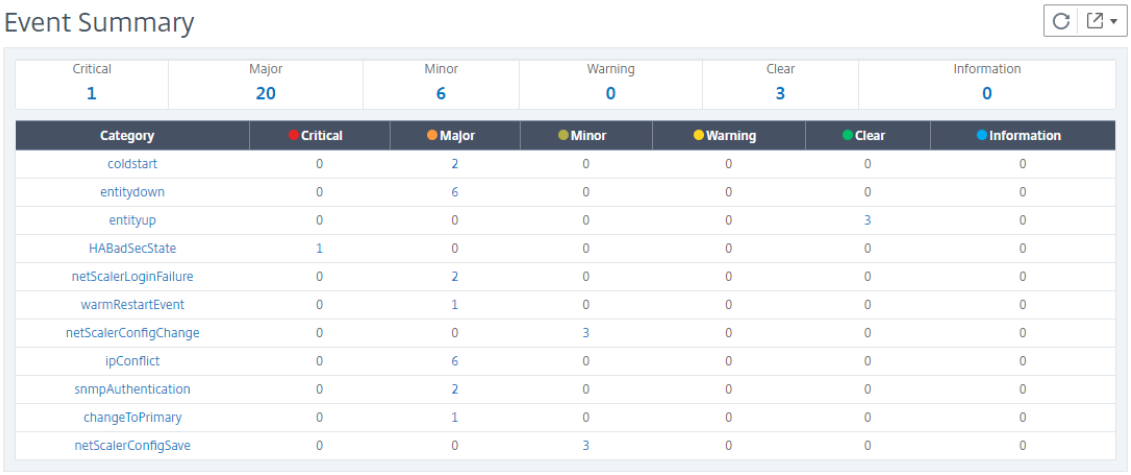


Zusammenfassung der Ereignisse anzeigen

February 5, 2024

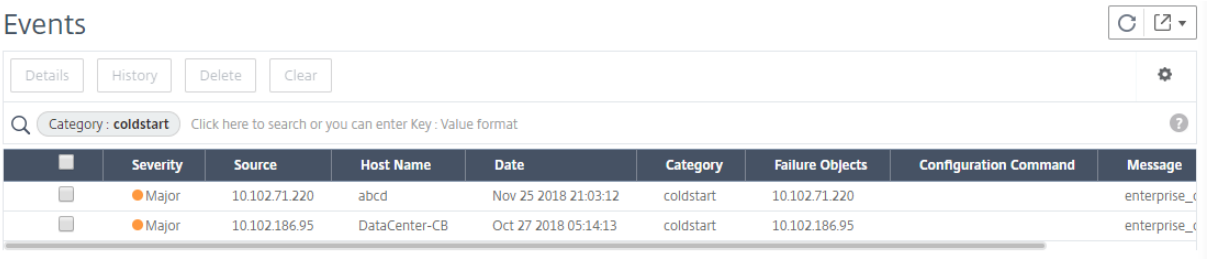
Sie können nun eine Seite “Ereignisübersicht”anzeigen, um die Ereignisse und Traps zu überwachen, die auf dem NetScaler Application Delivery Management (ADM) -Server empfangen wurden. Navigieren Sie zu **Netzwerke** > **Ereignisse**. Auf der Seite Ereignisübersicht werden die folgenden Informationen in einem tabellarischen Format angezeigt:

- **Zusammenfassung aller Ereignisse, die NetScaler ADM erhalten hat**. Die Ereignisse sind nach Kategorien sortiert, und die verschiedenen Schweregrade werden in verschiedenen Spalten angezeigt: Kritisch, schwerwiegend, geringfügig, Warnung, Klar und Information. Ein kritisches Ereignis tritt beispielsweise auf, wenn eine Citrix Application Delivery Controller Instanz (ADC) ausfällt und keine Informationen an den NetScaler ADM -Server sendet. Während des Ereignisses wird eine Benachrichtigung an einen Administrator gesendet, in der der Grund erläutert wird, warum die Instanz ausgefallen ist, die Zeit, in der sie nicht verfügbar war, und so weiter. Das Ereignis wird dann auf der Seite “Ereignisübersicht”aufgezeichnet, auf der Sie eine Zusammenfassung anzeigen und auf die Details des Ereignisses zugreifen können.



- **Anzahl der empfangenen Traps für jede Kategorie**. Die Anzahl der empfangenen Traps, kategorisiert nach Schweregrad. Standardmäßig hat jeder Trap, der von NetScaler ADC-Instanzen an NetScaler ADM gesendet wird, einen zugewiesenen Schweregrad, aber als Netzwerkadministrator können Sie den Schweregrad in der NetScaler ADM GUI angeben.

Wenn Sie auf einen Kategorietyp oder einen Trap klicken, gelangen Sie zur Seite **Ereignisse**, auf der Filter wie Kategorie und Schweregrad vorausgewählt sind. Auf dieser Seite werden weitere Informationen zum Ereignis angezeigt, z. B. die IP-Adresse und der Hostname der NetScaler ADC Instanz, das Datum, an dem das Trap empfangen wurde, die Kategorie, Fehlerobjekte, die Ausführung des Konfigurationsbefehls und die Meldung.



Ereignisschweregrade und SNMP-Trap-Details anzeigen

February 5, 2024

Wenn Sie ein Ereignis und seine Einstellungen in Citrix Application Delivery Management (ADM) erstellen, können Sie das Ereignis sofort auf der Seite “Ereignisübersicht”anzeigen. In ähnlicher Weise können Sie den Status, die Betriebszeit, die Modelle und die Versionen aller ADC-Instanzen (Citrix Application Delivery Controller) anzeigen und überwachen, die dem Citrix ADM -Server im Infrastructure Dashboard hinzugefügt wurden.

Auf dem Infrastruktur-Dashboard können Sie jetzt irrelevante Werte maskieren, sodass Sie Informationen wie Ereignisse nach Schweregrad, Status, Uptime, Modelle und Version von NetScaler ADC-Instanzen einfacher anzeigen und überwachen können.

Beispielsweise können Ereignisse mit einem **kritischen** Schweregrad selten auftreten. Wenn diese kritischen Ereignisse jedoch in Ihrem Netzwerk auftreten, sollten Sie möglicherweise weiter untersuchen, Fehler beheben und überwachen, wo und wann das Ereignis aufgetreten ist. Wenn Sie alle Schweregrade außer Kritisch auswählen, zeigt das Diagramm nur das Vorkommen kritischer Ereignisse an. Wenn Sie auf das Diagramm klicken, gelangen Sie zur Seite **Schweregrade basierende Ereignisse**, auf der Sie alle Details darüber sehen können, wann ein kritisches Ereignis für die von Ihnen ausgewählte Dauer aufgetreten ist: die Instanzquelle, das Datum, die Kategorie und die Benachrichtigung über die Nachricht, die beim Auftreten des kritischen Ereignisses gesendet wurde.

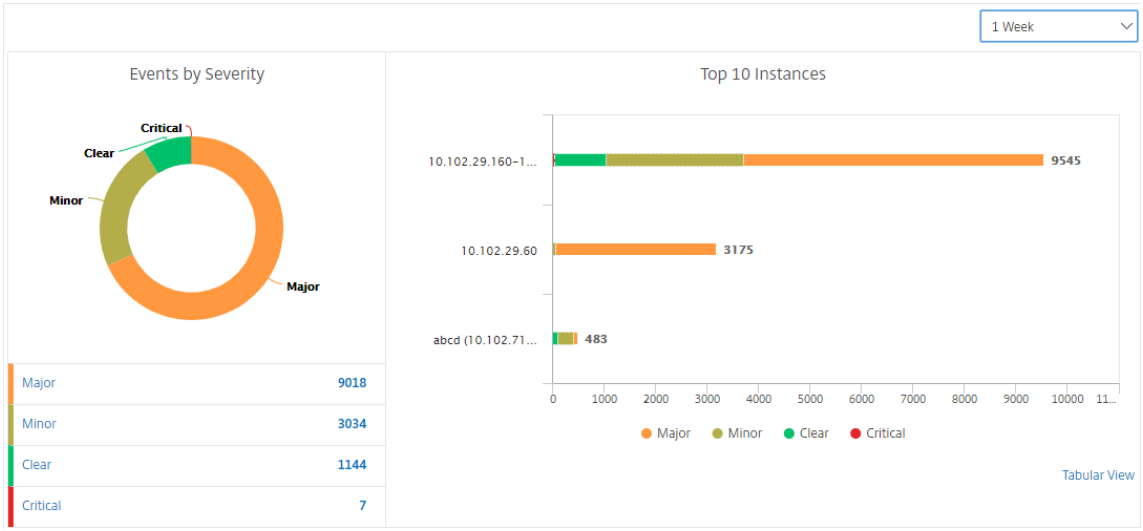
Ebenso können Sie die Integrität einer Citrix VPX-Instanz auf dem Dashboard anzeigen. Sie können die Zeit maskieren, in der die Instanz gestartet und ausgeführt wurde, und nur die Zeiten anzeigen, in denen die Instanz außer Betrieb war. Wenn Sie auf das Diagramm klicken, gelangen Sie zur Seite dieser Instanz, auf der *der Out-Of-Service-Filter* bereits angewendet wurde, und sehen Sie Details wie Hostname, die Anzahl der HTTP-Anforderungen, die pro Sekunde empfangen wurden, die CPU-Auslastung usw. Sie können auch die Instanz auswählen und das Dashboard der jeweiligen Citrix Instanz für weitere Details einsehen.

So wählen Sie bestimmte Ereignisse nach Schweregrad in NetScaler ADM aus:

1. Melden Sie sich mit Ihren Administratoranmeldeinformationen bei NetScaler ADM an.
2. Navigieren Sie zu **Netzwerke > Dashboard**.

   Oder

   Navigieren Sie zu **Netzwerke > Ereignisse > Berichte**.
3. Wählen Sie im Menü in der oberen rechten Ecke der Seite die Dauer aus, für die Ereignisse nach Schweregrad angezeigt werden sollen.

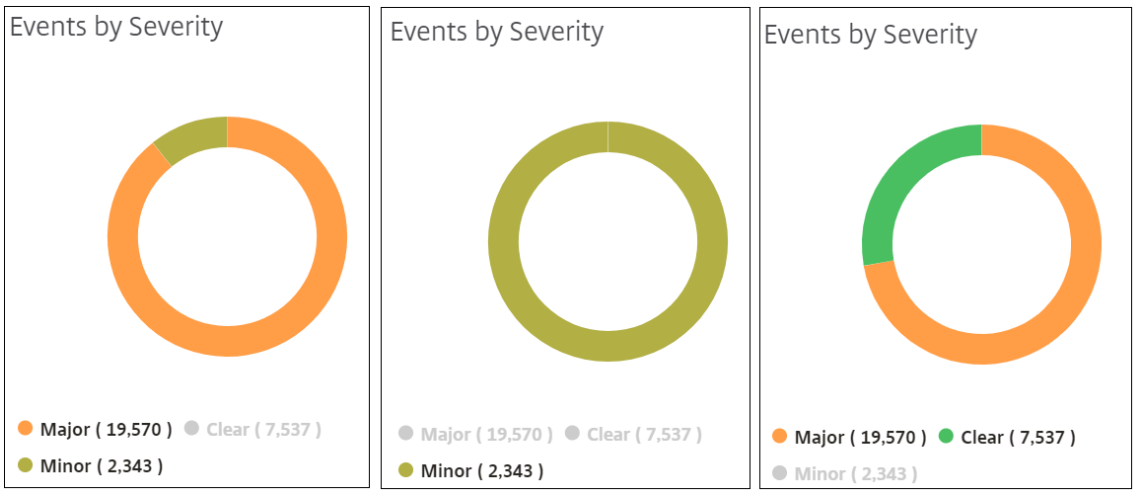


4. Das Donutdiagramm **Ereignisse nach Schweregrad**zeigt eine visuelle Darstellung aller Ereignisse nach ihrem Schweregrad an. Verschiedene Arten von Ereignissen werden als unterschiedliche farbige Abschnitte dargestellt, und die Länge jedes Abschnitts entspricht der Gesamtzahl der Ereignisse dieser Art von Schweregrad.
5. Sie können auf jeden Abschnitt des Donut-Diagramms klicken, um die entsprechende Seite mit dem **Schweregrad basierenden Ereignissen** anzuzeigen, auf der die folgenden Details für den ausgewählten Schweregrad für die ausgewählte Dauer angezeigt werden:

   - Instanz-Quelle
   - Daten des Ereignisses
   - Kategorie der Ereignisse, die von der NetScaler ADC-Instanz generiert werden
   - Nachrichtenbenachrichtigung gesendet

   > **Hinweis**
   >
   > Unterhalb des Donut-Diagramms sehen Sie eine Liste der Schweren, die im Diagramm dargestellt sind. Standardmäßig werden in einem Donutdiagramm alle Ereignisse aller Schweregradtypen angezeigt. Daher werden alle Schweregradtypen in der Liste hervorgehoben. Sie können die Schweregrade umschalten, um den gewählten Schweregrad ein-

> facher anzuzeigen und zu überwachen.



So zeigen Sie NetScaler ADC SNMP-Trapdetails auf NetScaler ADM an:

Sie können nun die Details der einzelnen SNMP-Traps anzeigen, die von den verwalteten NetScaler ADC Instanzen auf dem NetScaler ADM-Server auf der Seite **Ereigniseinstellungen** empfangen wurden. Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Ereigniseinstellungen**. Für ein bestimmtes Trap, das von Ihrer Instanz empfangen wird, können Sie die folgenden Details im tabellarischen Format anzeigen:

- **Kategorie** - Gibt die Kategorie der Instanz an, zu der das Ereignis gehört.
- **Schweregrad** - Der Schweregrad des Ereignisses wird durch Farben und seinen Schweregrad angezeigt.
- **Beschreibung** - Gibt die mit dem Ereignis verbundenen Nachrichten an.

Beispielsweise wird bei einem Ereignis mit der Trap-Kategorie **monRespTimeoutBelowThresh** die Beschreibung des Traps wie folgt angezeigt: “Dieser Trap wird gesendet, wenn das Antwort-Timeout für eine Monitorprobe wieder normal ist und unter dem eingestellten Schwellenwert liegt.”

Anzeigen und Exportieren von NetScaler ADC Syslog-Nachrichten

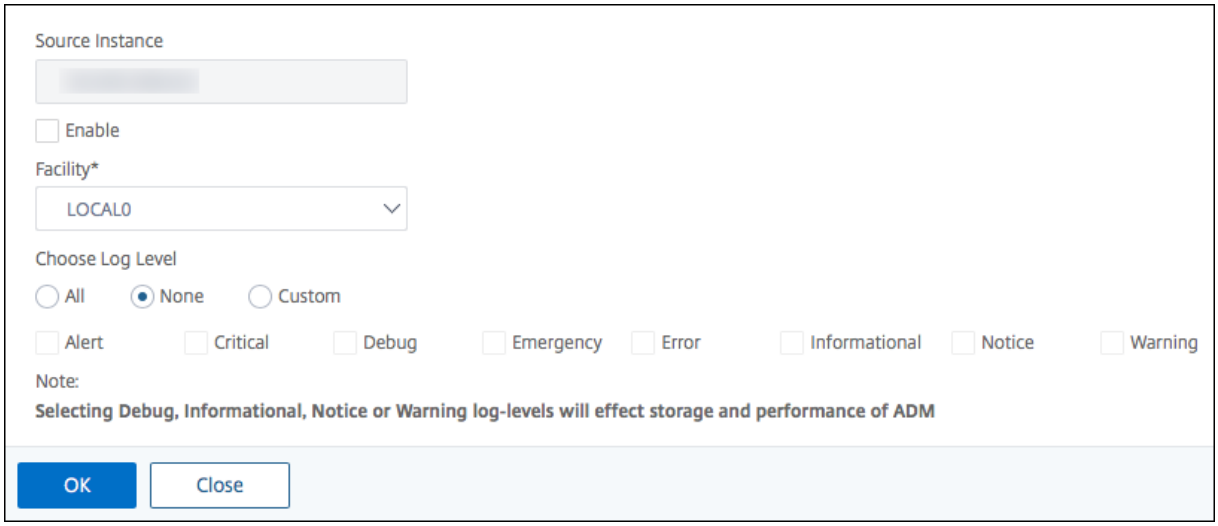
February 5, 2024

Über Ihre ADM-Software können Sie die Syslog-Ereignisse überwachen, die auf Ihren Citrix Application Delivery Controller (ADC) -Instanzen generiert werden. Dazu müssen Sie ADM als Syslog-Server für Ihre NetScaler ADC-Instanzen konfigurieren. Nachdem Sie ADM konfiguriert haben, werden alle Syslog-Nachrichten von den ADC-Instanzen zu ADM umgeleitet.

Konfigurieren von ADM als Syslog-Server

Gehen Sie folgendermaßen vor, um ADM als Syslog-Server zu konfigurieren:

1. Navigieren Sie in der ADM-GUI zu **Networks > Instances**.
2. Wählen Sie die NetScaler ADC-Instanz aus, aus der die Syslog-Nachrichten gesammelt und in NetScaler ADM angezeigt werden sollen.
3. Wählen Sie in der Liste **Aktion auswählen** die Option **Syslog konfigurieren** aus.
4. Klicken Sie auf **Aktivieren**.
5. Wählen Sie in der Dropdownliste **Einrichtung** eine Einrichtung auf lokaler Ebene oder auf Benutzerebene aus.
6. Wählen Sie die erforderliche Protokollebene für die Syslog-Meldungen aus.
7. Klicken Sie auf **OK**.

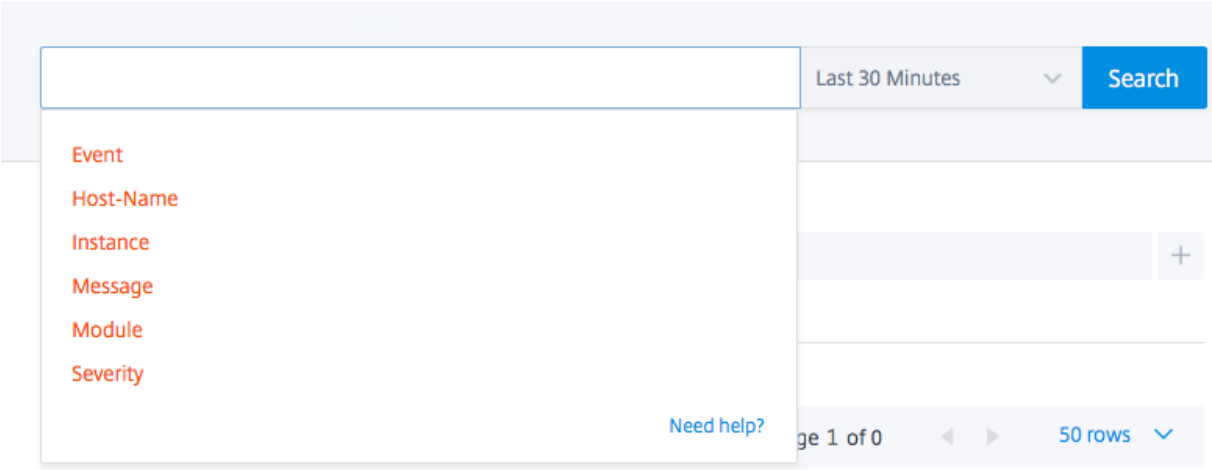


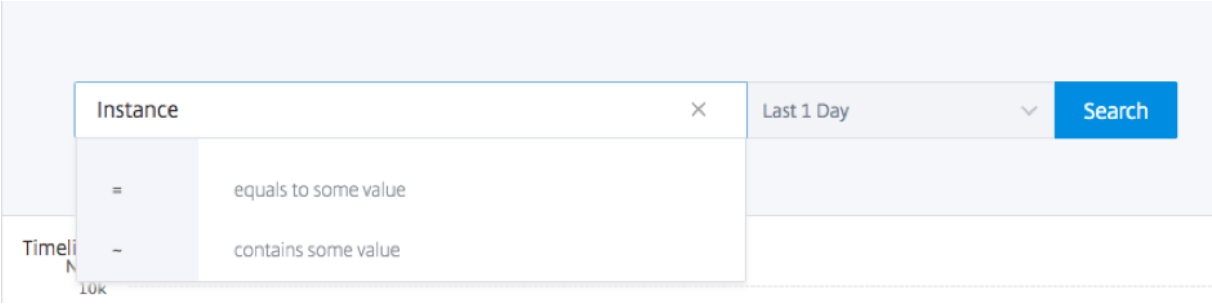
Mit diesen Schritten werden alle Syslog-Befehle in der NetScaler ADC-Instanz konfiguriert, und NetScaler ADM beginnt mit dem Empfang der Syslog-Nachrichten.

Anzeigen und Durchsuchen von Syslog-Nachrichten

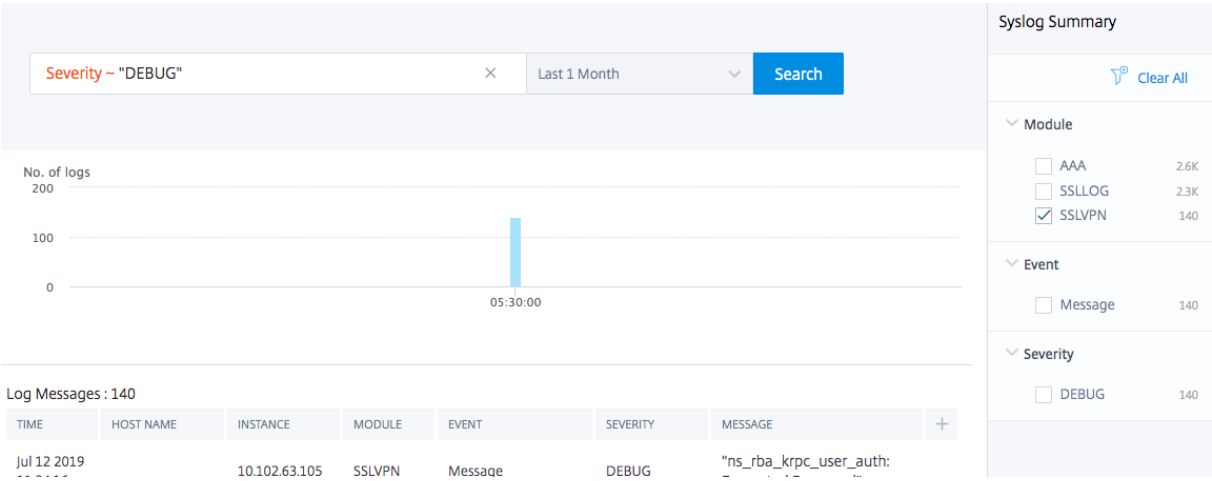
Sie können alle Syslog-Nachrichten anzeigen, die auf Ihren verwalteten NetScaler ADC-Instanzen generiert wurden. Die Syslog-Nachrichten werden zentral in der Datenbank gespeichert und stehen unter **Netzwerke > Ereignisse > Syslog Messages** zu Überwachungszwecken zur Verfügung. Sie können diese Protokollierungsinformationen kombinieren und Berichte für Analysen aus den gesammelten Daten ableiten.

Darüber hinaus können Sie mithilfe von Filtern die Suchergebnisse von Syslog-Nachrichten eingrenzen und genau das finden, wonach Sie suchen, und zwar in Echtzeit. Klicken Sie auf **Hilfe?**, um die integrierte Suchhilfe zu öffnen.





Fügen Sie als Nächstes den Suchbegriff hinzu. Für einige Kategorien wird eine vorausgefüllte Liste mit Suchbegriffen angezeigt. Standardmäßig beträgt die Suchzeit 1 Tag. Sie können den Zeit- und Datumsbereich ändern, indem Sie auf den Pfeil nach unten klicken. Sie können Ihre Suche weiter eingrenzen, indem Sie Optionen im Bereich **Syslog Summary** auswählen.

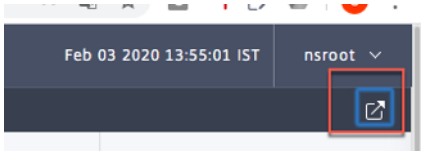


Exportieren und planen Sie Syslog-Nachrichten

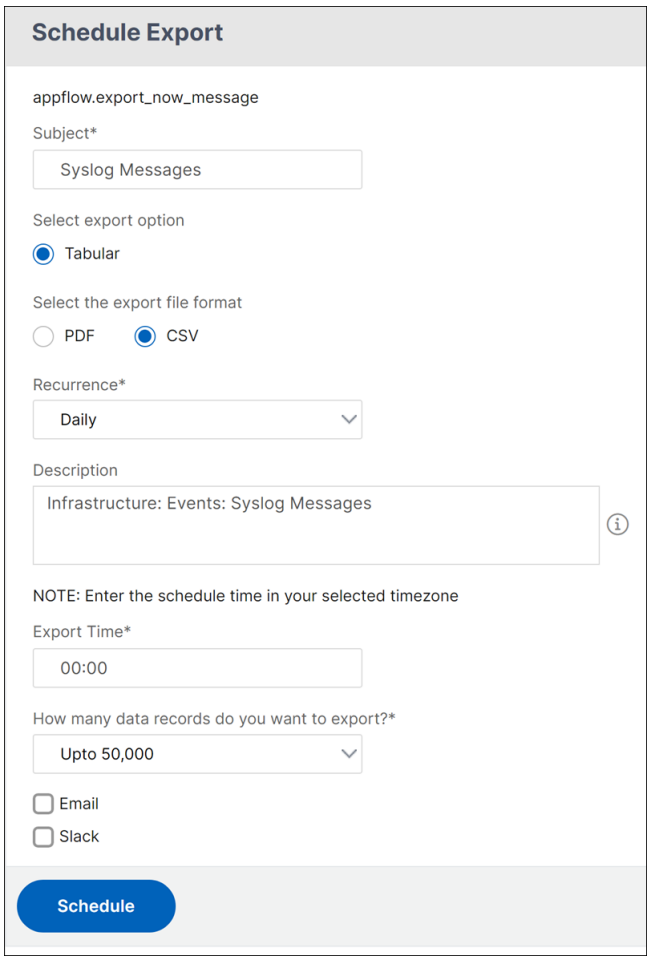
Sie können Syslog-Nachrichten anzeigen, ohne sich bei ADM anzumelden, indem Sie einen Export aller auf dem Server empfangenen Syslog-Nachrichten planen. Sie können Syslog-Nachrichten ex-

portieren, die auf Ihren ADC-Instanzen in PDF-, CSV-, PNG- und JPEG-Formaten generiert werden. Du kannst den Export dieser Berichte in bestimmte E-Mail-Adressen oder Slack-Konten in verschiedenen Intervallen planen.

Um die Protokollmeldungen zu exportieren und zu planen, klicken Sie auf das Pfeilsymbol in der oberen rechten Ecke.



- Um die Protokollmeldungen zu exportieren, klicken Sie auf **Exportieren > Jetzt exportieren**, wählen Sie das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.
- Um den Export von Syslog-Nachrichten zu planen, klicken Sie auf **Exportieren Berichte > Bericht planen**und legen Sie die erforderlichen Parameter fest. Du kannst den Bericht per E-Mail oder Slack erhalten.



Syslog-Nachrichten unterdrücken

February 5, 2024

Bei der Konfiguration als Syslog-Server empfängt Citrix Application Delivery Management (ADM) alle Syslog-Nachrichten, die von den konfigurierten ADC-Instanzen (Citrix Application Delivery Controller) an diesen Server gesendet werden. Möglicherweise gibt es eine große Anzahl von Nachrichten, die Sie möglicherweise nicht sehen möchten. Beispielsweise sind Sie möglicherweise nicht daran interessiert, alle Meldungen auf Informationsebene zu sehen. Sie können nun einige Syslog-Nachrichten verwerfen, die Sie nicht interessieren. Sie können einige der Syslog-Meldungen, die in NetScaler ADM eingehen, unterdrücken, indem Sie einige Filter einrichten. Citrix ADM löscht alle Nachrichten, die mit den Kriterien übereinstimmen. Diese gelöschten Nachrichten werden nicht auf der NetScaler ADM GUI angezeigt, und diese Nachrichten werden auch nicht in der NetScaler ADM-Datenbank des Kunden gespeichert.

Sie können einige der protokollierten Syslog-Meldungen, die in NetScaler ADM eingehen, unterdrücken, indem Sie einige Filter einrichten. Die beiden Filter, die zum Unterdrücken von Syslog-Nachrichten verwendet werden können, sind Schweregrad und Einrichtung. Sie können auch Nachrichten unterdrücken, die von einer bestimmten NetScaler ADC-Instanz oder mehreren Instanzen stammen. Sie können auch ein Textmuster für NetScaler ADM bereitstellen, um Nachrichten zu suchen und zu unterdrücken. Citrix ADM löscht alle Nachrichten, die mit den Kriterien übereinstimmen. Diese gelöschten Nachrichten werden nicht auf der NetScaler ADM GUI angezeigt, und diese Nachrichten werden auch nicht in der Kundendatenbank gespeichert. Daher wird eine gute Menge an Speicherplatz auf dem Speicherserver gespart.

Einige Anwendungsfälle für die Unterdrückung von Syslog-Meldungen lauten wie folgt:

- Wenn Sie alle Meldungen auf Informationsebene ignorieren möchten, unterdrücken Sie Level 6 (informativ)
- Wenn Sie nur Firewall-Fehlerbedingungen aufzeichnen möchten, unterdrücken Sie alle Ebenen außer Stufe 3 (Fehler)

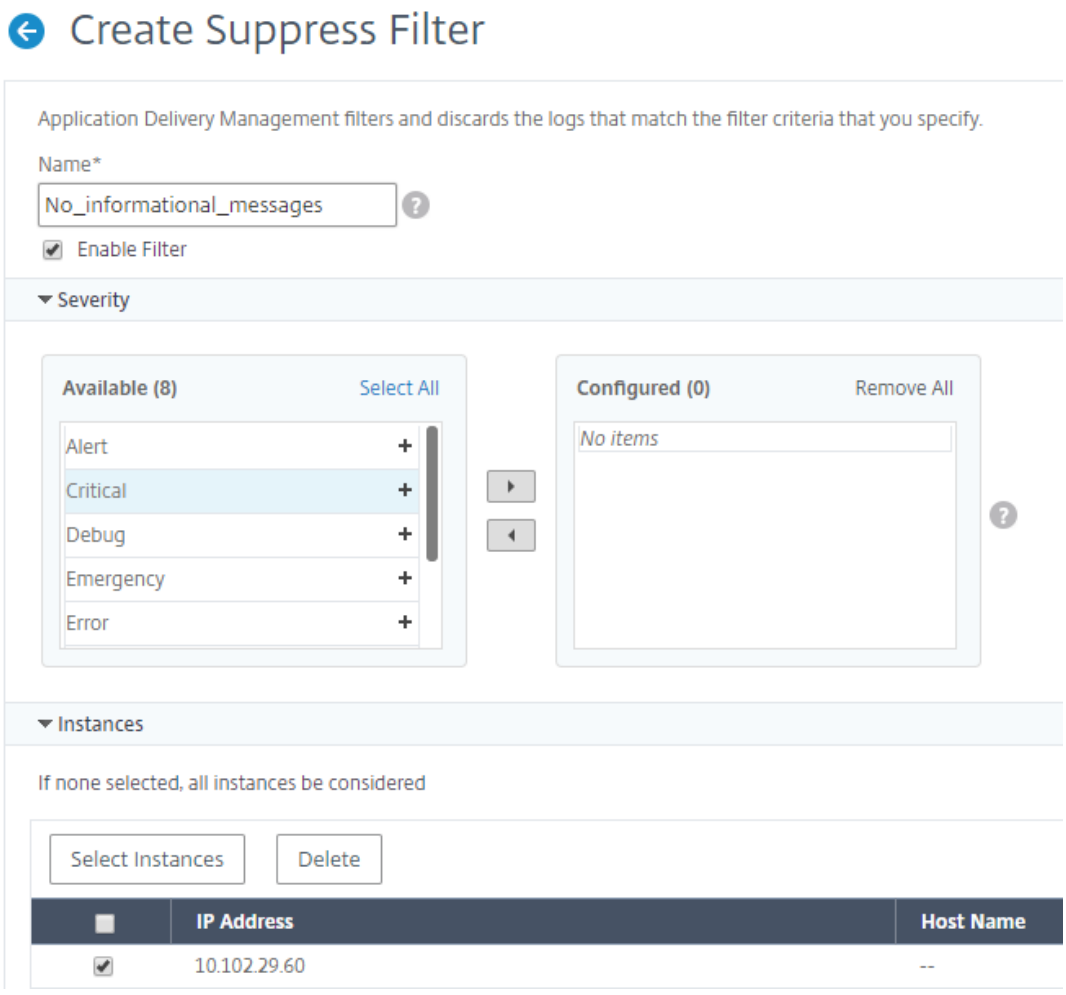
Unterdrücken von Syslog-Nachrichten durch Erstellen von Filtern

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Ereignisse** > **Syslog-Nachrichten** > **Filter unterdrücken**.
2. Aktualisieren **Sie auf der Seite Unterdrückungsfilter erstellen** die folgenden Informationen:
    a) **Name** - geben Sie einen Namen für den Filter ein.

> **Hinweis:**
>
> Wenn verschiedene Benutzer unterschiedliche Zugriffsrechte auf mehrere NetScaler ADC-Instanzen haben, müssen unterschiedliche Filter für verschiedene Instanzen erstellt werden, da Benutzer nur die Filter sehen können, in denen sie Zugriff auf alle Instanzen haben.

b) **Schweregrad** —Wählen Sie die Protokollebenen aus, für die Sie die Meldungen unterdrücken müssen, und fügen Sie Wenn Sie beispielsweise keine eingehenden Informationsmeldungen anzeigen möchten, können Sie Informativ auswählen, um diese Meldungen zu unterdrücken.

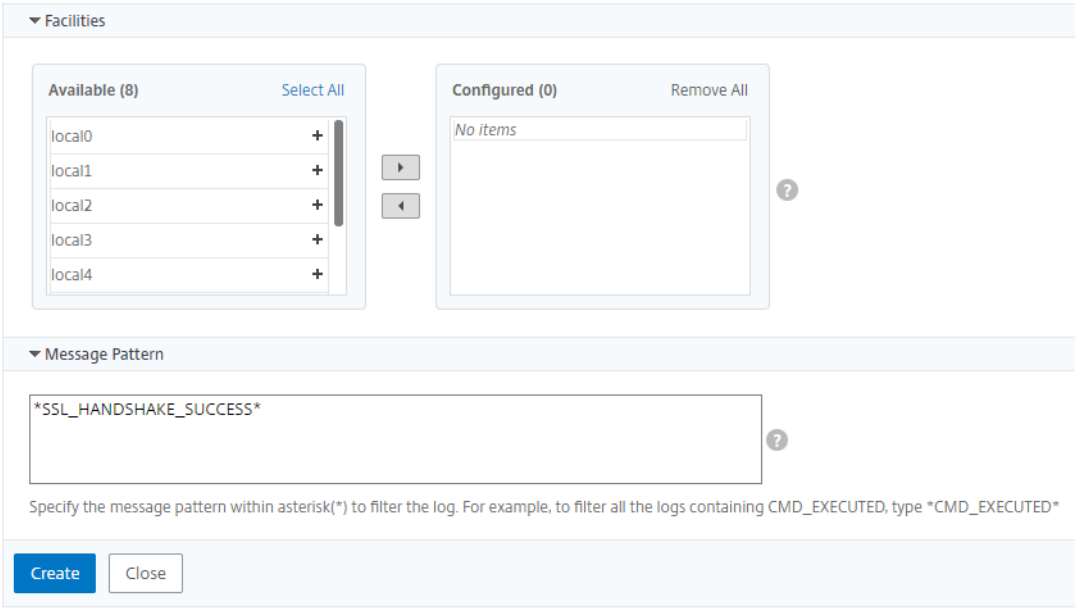
c) **Instanzen** - Wählen Sie die NetScaler ADC-Instanzen aus, für die die Syslog-Meldungen konfiguriert wurden.



d) **Einrichtungen** - Wählen Sie die Einrichtung aus, um Nachrichten auf der Grundlage der Quelle zu unterdrücken, die sie generiert.

e) **Nachrichtenmuster** —Sie können auch ein Textmuster eingeben, das von einem

Sternchen (*) umgeben ist, um die Nachrichten zu unterdrücken. Die Nachrichten werden nach der Textmusterzeichenfolge gesucht und die Meldungen, die dieses Muster enthalten, werden unterdrückt.



Deaktivieren des Filters

Damit die Nachrichten in NetScaler ADM angezeigt werden können, müssen Sie den Filter deaktivieren.

1. Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Syslog-Nachrichten** > **Filter unterdrücken**, wählen Sie auf der Seite **Filter unterdrücken** den Filter aus, und klicken Sie auf **Bearbeiten**.
2. **Deaktivieren Sie auf der Seite Filter unterdrücken** das Kontrollkästchen **Filter aktivieren**, um den Filter zu deaktivieren.

Löscheinstellungen für Instanzereignisse konfigurieren

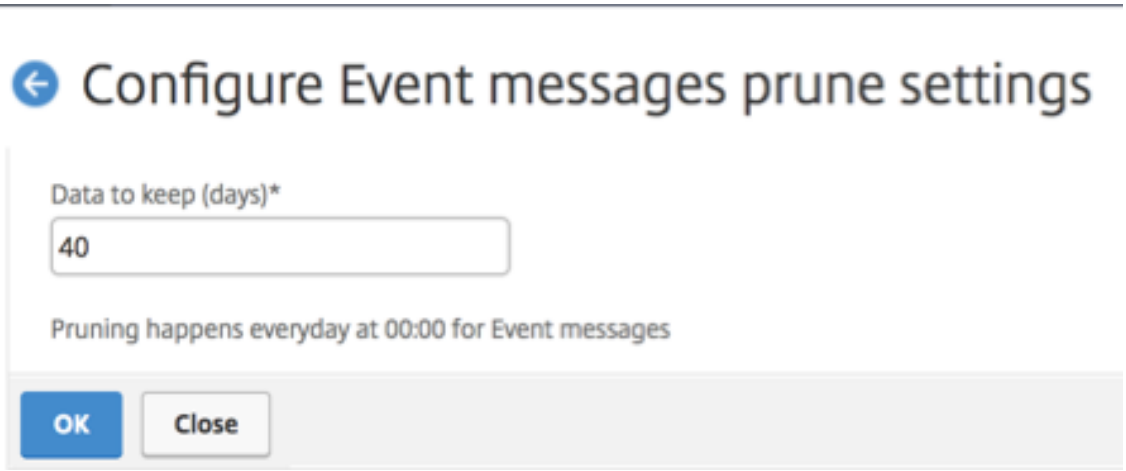
February 5, 2024

Citrix Application Delivery Controller (ADC) -Instanzen, die vom Citrix Application Delivery Management (ADM) -Server verwaltet werden, senden Ereignisnachrichten kontinuierlich Daten, die in Citrix ADM gespeichert werden. Sie können das Intervall angeben, für das Citrix ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle beibehalten soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00.00 Uhr) bereinigt.

> **Hinweis**
>
> Der Wert, den Sie angeben können, darf 40 Tage nicht überschreiten oder weniger als 1 Tag betragen.

So konfigurieren Sie Prune-Einstellungen für Instanzereignisse:

1. Navigieren Sie zu **System** > **Systemadministration**.
2. Klicken Sie unter**Prune-Einstellungen**auf**Instanzereignisse Prune-Einstellungen**.
3. Geben Sie das Zeitintervall in Tagen ein, für das Sie Daten auf dem NetScaler ADM -Server beibehalten möchten, und klicken Sie auf**OK**.



SSL Zertifikatsverwaltung

February 5, 2024

Jede Organisation oder einzelne Website, die den Umgang mit vertraulichen oder sensiblen Informationen erfordert, muss über ein SSL-Zertifikat verfügen. Das SSL-Zertifikat auf einem Webserver garantiert die Authentizität des Webservers gegenüber dem verbindenden Client. Es authentifiziert nicht nur die Identität einer Website, sondern hilft auch bei der Generierung des Sitzungsschlüssels, der später für die Verschlüsselung der gesamten Sitzung verwendet wird.

Ein SSL-Zertifikat (Secure Socket Layer), das Teil einer SSL-Transaktion ist, ist ein digitales Eingabeformular (X509), das ein Unternehmen (Domain) oder eine Person identifiziert. Das Zertifikat verfügt über eine Public-Key-Komponente, die für jeden Client sichtbar ist, der eine sichere Transaktion mit dem Server initiieren möchte. Der entsprechende private Schlüssel, der sich sicher auf der Citrix Application Delivery Controller (ADC) -Appliance befindet, wird verwendet, um die Verschlüsselung und Entschlüsselung des asymmetrischen Schlüssels (oder des öffentlichen Schlüssels) abzuschließen.

Citrix Application Delivery Management (ADM) bietet Ihnen eine einheitliche Konsole zur Automatisierung der Installation, Aktualisierung, Löschung, Verknüpfung und zum Herunterladen von SSL-Zertifikaten. Es hilft dabei, den Ruf der Website und das Vertrauen der Kunden zu erhalten. Citrix ADM optimiert jetzt alle Aspekte der Zertifikatverwaltung für Sie. Über eine einheitliche Konsole können Sie automatisierte Richtlinien konfigurieren, um den empfohlenen Aussteller, die Schlüsselstärke, das Protokoll und die Algorithmen gemäß den IT-Richtlinien der Organisation sicherzustellen. Auf diese Weise können Sie Zertifikate, die unbenutzt sind oder kurz vor dem Ablauf stehen, genau im Auge behalten.

Sie können ein SSL-Zertifikat und einen Schlüssel auf eine der folgenden Arten beziehen:

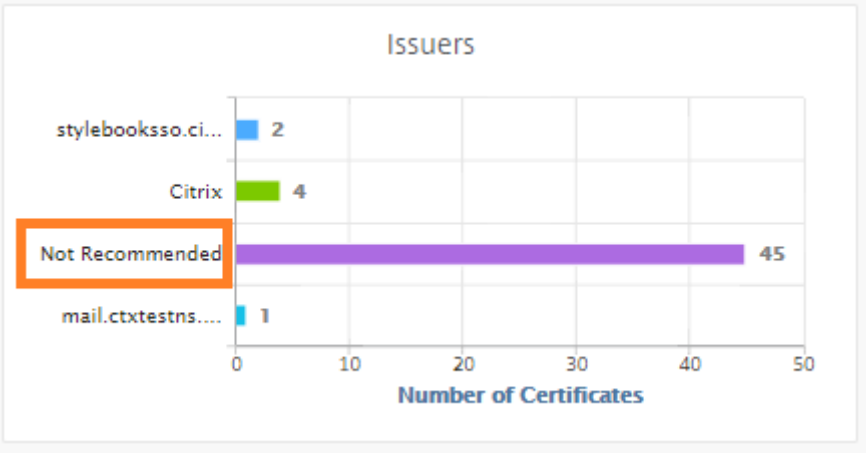
- Von einer autorisierten Zertifizierungsstelle (CA) wie Verisign
- Durch Generieren eines neuen SSL-Zertifikats und eines neuen Schlüssels auf der Citrix ADC-Appliance

SSL-Richtlinieneinstellungen für Unternehmen

Jedes Unternehmen hat seine eigene SSL-Richtlinie und definiert die Anforderungen, die alle SSL-Zertifikate einhalten müssen. Sicherheit war bei allen Unternehmensbenutzern immer zu den obersten Prioritäten und daher spielen SSL-Einstellungen eine wichtige Rolle.

Zum Beispiel schreibt eine ABC-Gesellschaft vor, dass alle Zertifikate mindestens wichtige Stärken von 2.048 Bit und mehr haben müssen. Die Zertifikate müssen von vertrauenswürdigen Zertifizierungsstellen oder Emittenten autorisiert werden. Administratoren müssen alle diese SSL-Parameter überprüfen, um sicherzustellen, dass die Zertifikate die Unternehmensrichtlinien einhalten. Es ist eine mühsame Aufgabe, jedes Zertifikat manuell zu überprüfen. Um dieses Szenario zu überwinden, hilft Ihnen das Citrix ADM bei der Konfiguration von SSL-Richtlinieneinstellungen für Unternehmen und zeigt jedes Nicht-Compliance-Zertifikat mit dem Tag “Nicht empfohlen”an.

Sie können die Zusammenfassung der Non-Compliance-Zertifikate (nicht empfohlen) im SSL-Dashboard anzeigen.

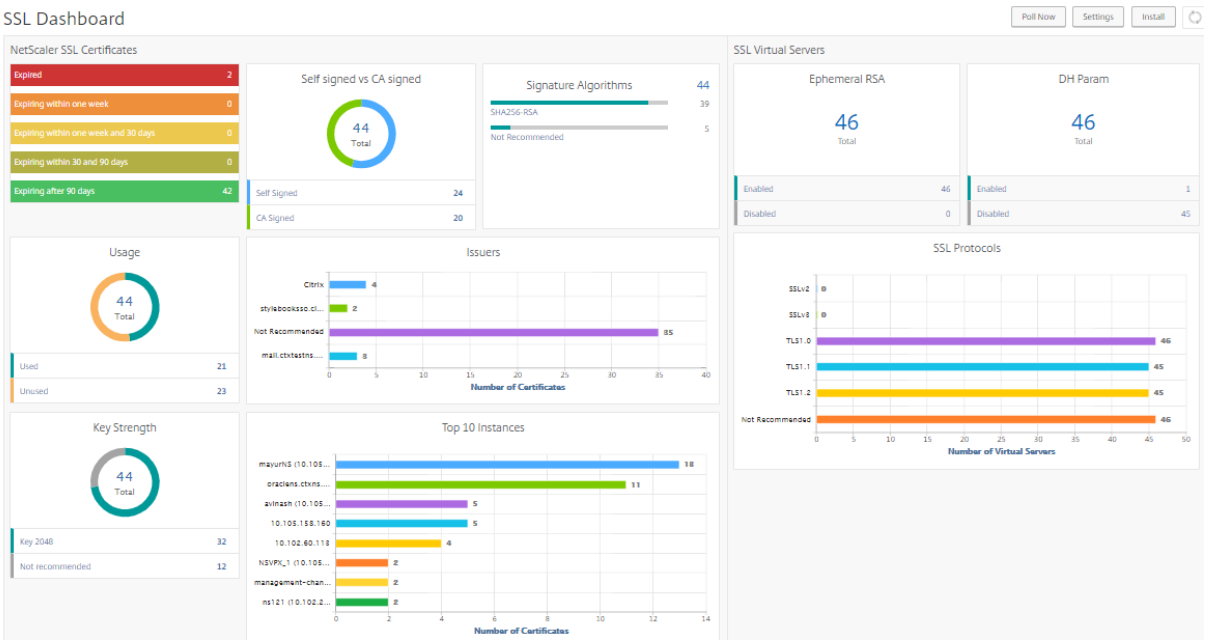


> **Hinweis**
>
> Die ‘‘Nicht empfohlenen’’Zertifikate werden basierend auf verschiedenen Parametern kategorisiert und Sie können sie in relevanten Komponenten anzeigen.

So funktioniert das Citrix ADM-Zertifikat

SSL Dashboard bietet Ihnen eine visuelle Darstellung aller SSL-Zertifikate, die auf verschiedenen Citrix ADC-Instanzen installiert sind. Das SSL-Dashboard enthält die folgenden Informationen für jedes Zertifikat, das auf Citrix ADC-Instanzen installiert ist. Es ist auf der Grundlage der folgenden kategorisiert:

- **Selbstsigniert gegen CA signiert.** Der selbstsignierte und CA-signierte Bereich hilft Ihnen, die Zertifikate in selbstsignierte Zertifikate und CA-signierte Zertifikate zu unterteilen.
- **Signature-Algorithmen.** In diesem Abschnitt werden die SSL-Zertifikate basierend auf Signaturalgorithmen getrennt, die für die Verschlüsselung verwendet werden.
- **Verwendung.** In diesem Abschnitt werden Ihre SSL-Zertifikate basierend auf verwendeten und ungenutzten Zertifikaten getrennt. Unbenutzte Zertifikate erfordern besondere Aufmerksamkeit, da sie möglicherweise verpasst wurden, um an die virtuellen Server gebunden zu sein.
- **Emittenten.** In diesem Abschnitt trennt sich die SSL-Zertifikate basierend auf dem Aussteller der Zertifikate.
- **Wichtigste Stärke.** In diesem Abschnitt werden die SSL-Zertifikate basierend auf der Schlüsselstärke eines privaten Schlüssels getrennt.
- **Top-10-Instanz.** Dieser Abschnitt enthält die Details der 10 wichtigsten Citrix ADC-Instanzen basierend auf der Anzahl der installierten SSL-Zertifikate.



Anwendungsfälle für die Verwaltung von SSL-Zertifikaten

In den folgenden Anwendungsfällen wird beschrieben, wie Sie das SSL-Zertifikat verwenden können, um die Zertifikate über mehrere Citrix ADC-Instanzen hinweg zu verwalten und zu überwachen.

Installieren von SSL-Zertifikaten

Stellen Sie sich vor, Sie haben eine Flotte von Citrix ADC-Instanz, auf denen Sie die erforderlichen SSL-Zertifikate bereitstellen müssen. Citrix ADM bietet Ihnen eine einheitliche Konsole, mit der Sie die SSL-Zertifikate in einem Versuch für mehrere Citrix ADC-Instanzen bereitstellen können.

Beispielsweise möchten Sie möglicherweise einige SSL-Zertifikate auf einer oder mehreren Citrix ADC-Instanzen installieren. Mit diesem Ansatz können Sie den manuellen Eingriff bei der Installation des SSL-Zertifikats auf jeder Citrix ADC-Instanz minimieren. Sie können eine Masseninstallation von SSL-Zertifikaten über eine oder mehrere Citrix ADC-Instanzen durchführen.

Um eine Zusammenfassung der SSL-Zertifikate zu erhalten, melden Sie sich bei **Citrix ADM**an und navigieren Sie dann zu **Networks > SSL Dashboard**.

Benachrichtigungseinstellungen für Ablauf des Zertifikats

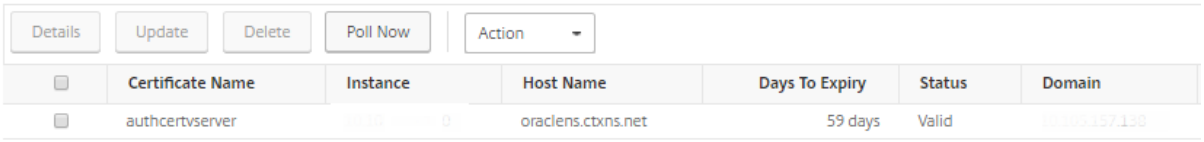
In diesem Anwendungsfall haben Sie möglicherweise viele Zertifikate für mehrere Citrix ADC-Instanzen, und es wird zu einem Overhead, um den Ablauf jedes Zertifikats zu verfolgen. Es ist eine mühsame Aufgabe, jedes Zertifikat manuell zu verfolgen und zu aktualisieren, bevor es abläuft. Um

solche Szenarien zu vermeiden, können Sie Citrix ADM so konfigurieren, dass die Benachrichtigungen oder Warnungen an die konfigurierten E-Mail-, Pager-, Slack- oder ServiceNow-Profile gesendet werden. Auf diese Weise können Sie sich über die Ablaufdaten der Zertifikate auf dem Laufenden halten und die Zertifikate lange vor den Ablaufdaten erneuern.

Beispielsweise vergessen Sie möglicherweise, das Zertifikat zu verfolgen, das kurz vor dem Ablauf steht. Und das Zertifikat läuft ab, was zu einem Dienstausfall führt, der sich auf zahlreiche Anwendungen für die Benutzer auswirken kann. Mit den Einstellungen für Benachrichtigungen über den Ablauf von ADM-Zertifikaten können Sie solche unvorhergesehenen Szenarien vermeiden.

Sie können die Zusammenfassung anzeigen und die Zertifikate, die kurz vor dem Ablauf stehen, auf dem **SSL-Dashboard**verfolgen.

Um den Bericht über abzulaufende Zertifikate in beliebiger Dauer anzuzeigen, können Sie auf die Kachel klicken, um die Details aller derartigen Zertifikate zu erhalten, die in diesem Fenster ablaufen.



Erneuerung von Zertifikaten

Sie können die Zertifikate jetzt von Citrix ADM erneuern. Sie können entweder die vorhandenen Zertifikate erneuern oder die Zertifikate basierend auf den folgenden Kriterien erstellen:

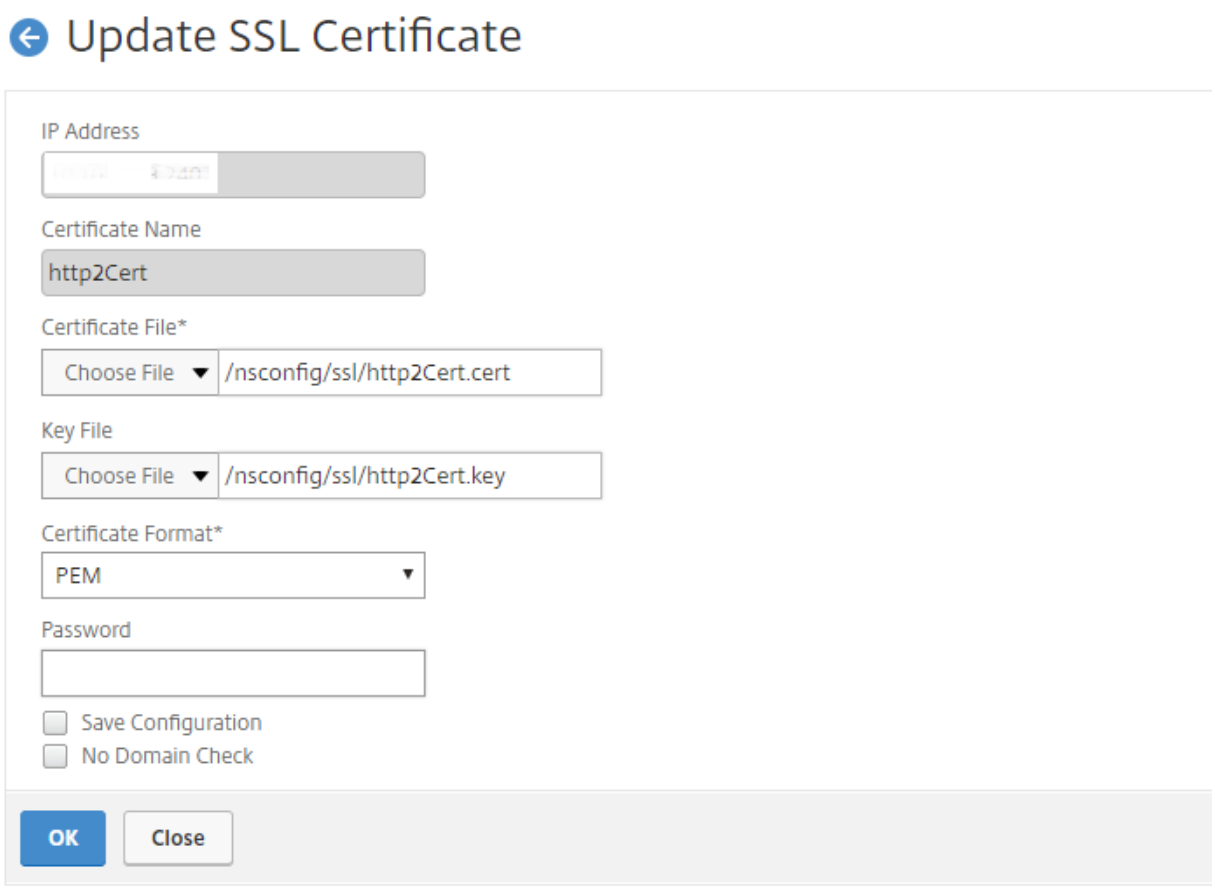
Aktualisieren Sie das vorhandene Zertifikat In diesem Anwendungsfall müssen Sie ein vorhandenes Zertifikat aktualisieren, sobald Sie ein erneuertes Zertifikat von der Zertifizierungsstelle (CA) erhalten haben. Sie können jetzt die vorhandenen Zertifikate von Citrix ADM aktualisieren, ohne sich bei Citrix ADC-Instanzen anzumelden.

Beispielsweise kann es einige Änderungen oder Änderungen an den vorhandenen Zertifikaten geben. Die CA stellt erneuerte Zertifikate aus. Anstatt zur Citrix ADC Appliance zu gehen, können Sie jetzt das SSL-Zertifikat von Citrix ADM aktualisieren.

Um ein Zertifikat zu aktualisieren, melden Sie sich bei Citrix ADM an und navigieren Sie dann zu **Networks > SSL Dashboard**.

Wählen Sie das Zertifikat aus, das Sie aktualisieren möchten, und klicken Sie auf **Aktualisieren**.

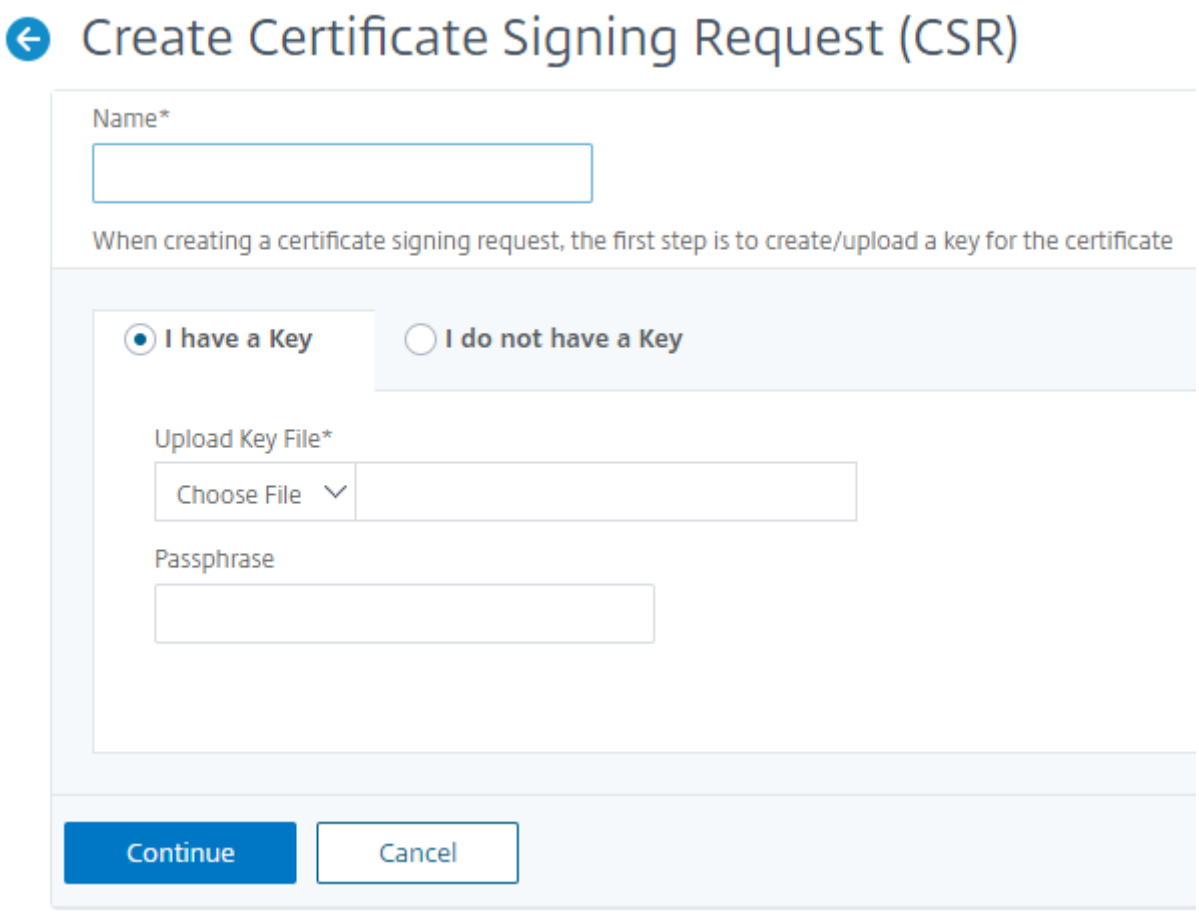
Sie haben die Möglichkeit, die relevanten Felder des ausgewählten Zertifikats von Citrix ADM zu aktualisieren.



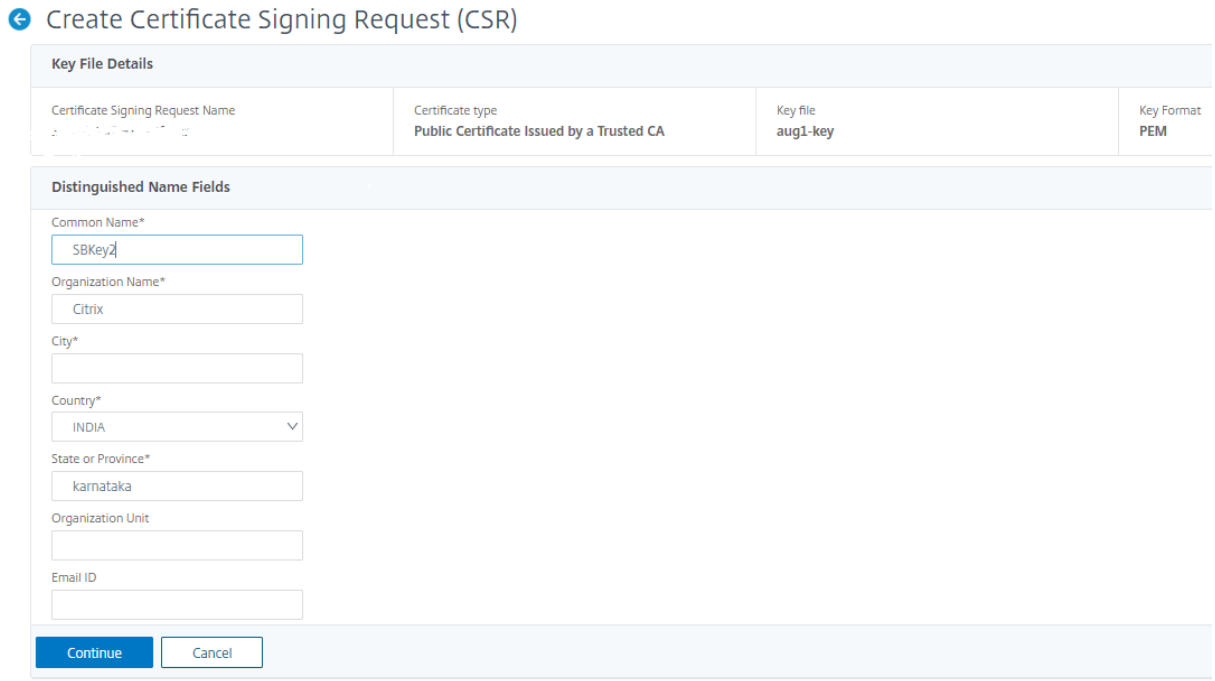
Erstellen einer Zertifikatsignieranforderung Stellen Sie sich einen Anwendungsfall vor, in dem eines der SSL-Zertifikate nicht den Richtlinien der Organisation entspricht. Sie möchten ein neues Zertifikat von der Zertifizierungsstelle erhalten. Sie können jetzt eine Zertifikatsignieranforderung (CSR) von Citrix ADM generieren. Ein CSR und ein öffentlicher Schlüssel können an eine CA gesendet werden, um das SSL-Zertifikat zu erhalten.

Um CSR zu bestimmen und zu erstellen, wählen Sie das gewünschte Zertifikat aus und klicken Sie auf **CSR erstellen**.

Sie müssen ein öffentliches oder privates Schlüsselwertpaar haben. Um einen Schlüssel hochzuladen, klicken Sie auf **Datei auswählen** und wählen Sie aus der Liste aus. Um einen Schlüssel zu erstellen, wählen Sie **Ich habe keine Schlüsseloption** und geben Sie die relevanten Parameter an.

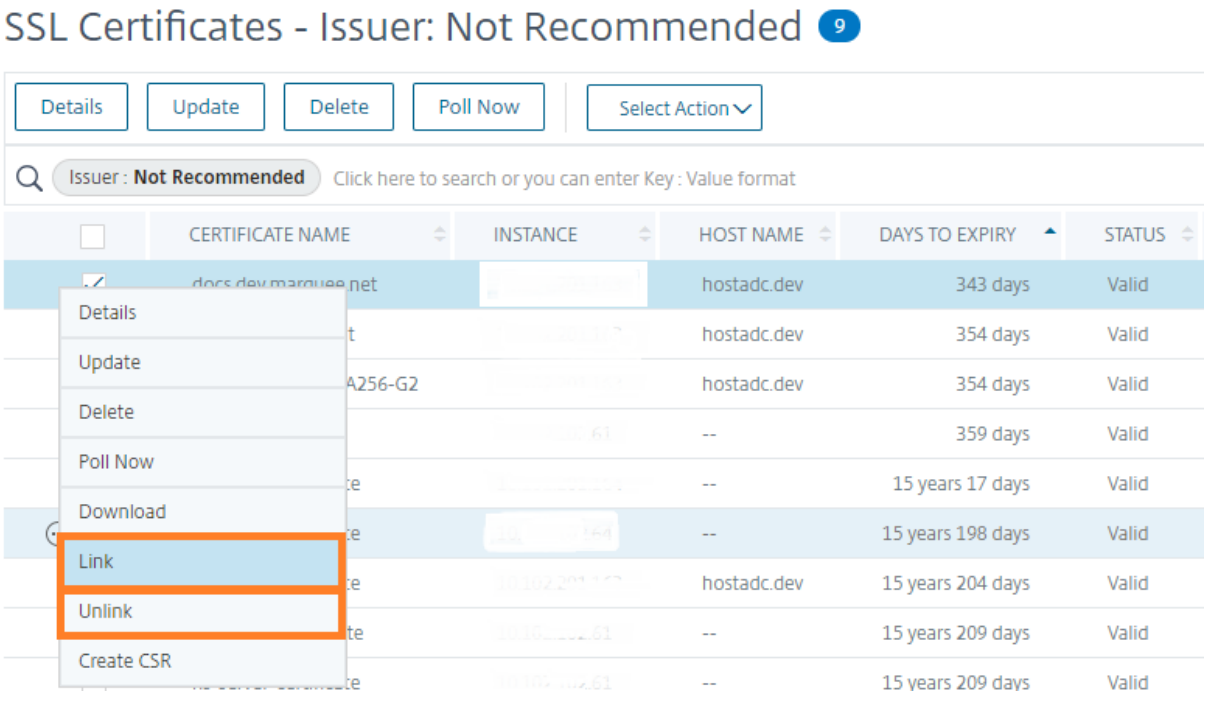


Um weitere Details zum ausgewählten Schlüssel wie Common Name, Org Name, Stadt, Land, Bundesland, Org Unit und E-Mail-ID anzugeben, um die CSR zu erstellen.



SSL-Zertifikate verknüpfen und aufheben

Sie können mehrere SSL-Zertifikate aneinander binden, um ein Zertifikatspaket zu erstellen. Um ein Zertifikat mit einem anderen Zertifikat zu verknüpfen, muss der Aussteller des ersten Zertifikats mit der Domäne des zweiten Zertifikats übereinstimmen.

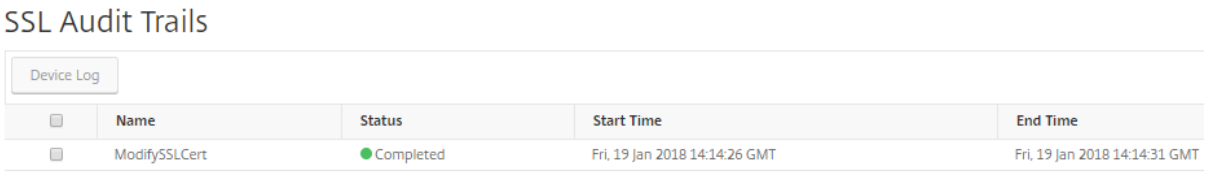


Auditprotokolle

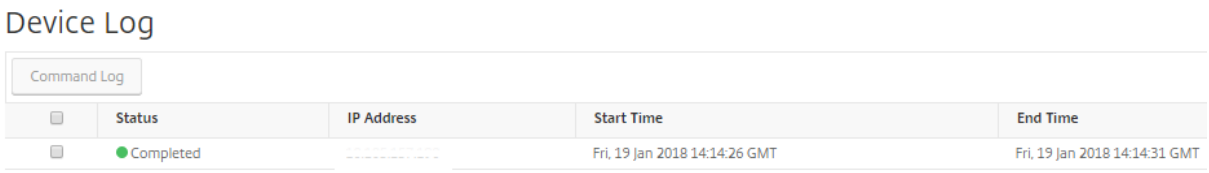
Audit Logs ist eine Sammlung von Textprotokolldateien, die vom Citrix ADM generiert werden. Es zeigt eine Historie von SSL-Zertifikaten, die mithilfe von Citrix ADM für die spezifische Citrix ADC Appliance hinzugefügt, geändert und geändert werden. Die Überwachungsprotokolle zeigen auch die IP-Adresse der Citrix ADC Appliance, den Status, die Startzeit und die Endzeit des jeweiligen Vorgangs an.

In diesem Beispiel möchten Sie möglicherweise die Änderung überprüfen, die über einen Zeitraum für das jeweilige Zertifikat stattgefunden hat. Und Sie haben die Möglichkeit, den Verlauf der Änderungen am Zertifikat über das Geräteprotokoll und das Befehlsprotokoll anzuzeigen.

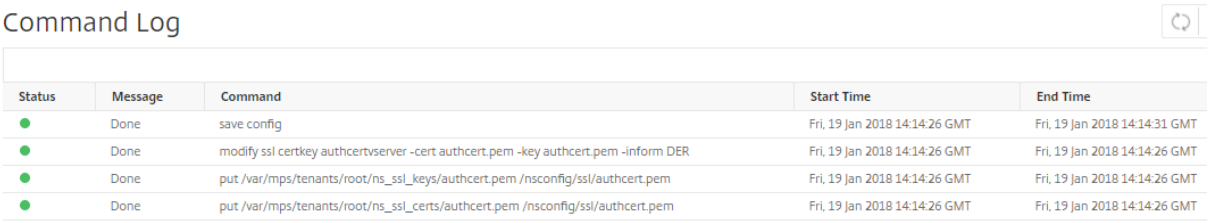
Um die Informationen von SSL-Zertifikaten zu ermitteln, klicken Sie im **SSL-Dashboard**auf **Audit Log**. Die Anwendungsübersicht enthält den Status der SSL-Zertifikate mit Startzeit und Endzeit.



Um die Informationen der Citrix ADC Appliance eines bestimmten SSL-Zertifikats zu ermitteln, aktivieren Sie das entsprechende Kontrollkästchen Ihres Wunschzertifikats. Klicken Sie auf **Geräte-Log**



Um die Informationen des Befehlstyps und der Meldung anzuzeigen, klicken Sie auf **Befehlsprotokoll**.



Verwenden des SSL-Dashboards

February 5, 2024

Sie können das SSL-Zertifikat-Dashboard in Citrix Application Delivery Management (ADM) verwenden, um Diagramme anzuzeigen, mit denen Sie Zertifikatsaussteller, wichtige Stärken und Signaturalgorithmen verfolgen können. Das SSL-Zertifikat-Dashboard zeigt außerdem Diagramme an, die Folgendes angeben:

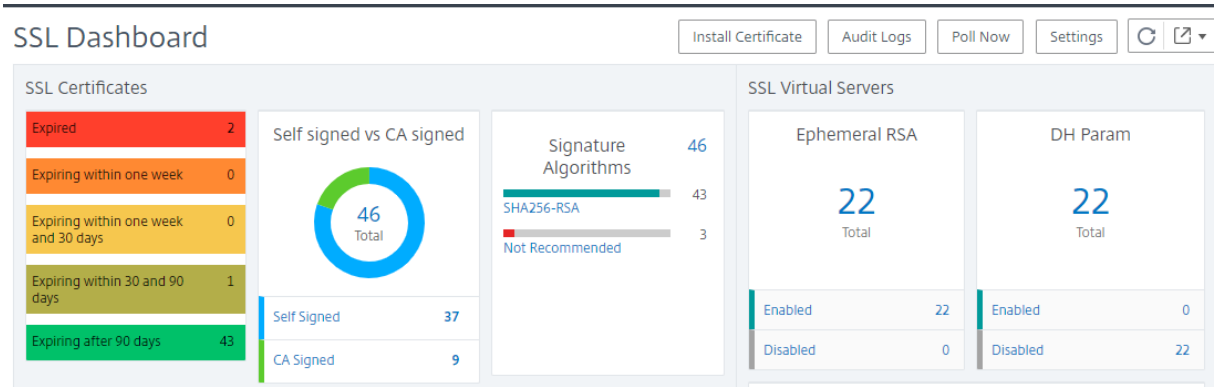
- Anzahl der Tage, nach denen Zertifikate ablaufen
- Anzahl verwendeter und nicht verwendeter Zertifikate
- Anzahl selbstsignierter und von einer Zertifizierungsstelle signierter Zertifikate
- Anzahl der Emittenten
- Signatur-Algorithmen
- SSL-Protokolle
- Top 10 Instanzen nach Anzahl der verwendeten Zertifikate

So überwachen Sie SSL-Zertifikate

Sie können das SSL-Dashboard in Citrix ADM verwenden, um Ihre Zertifikate zu überwachen, wenn Ihr Unternehmen über eine SSL-Richtlinie verfügt, in der Sie bestimmte SSL-Zertifikatsanforderungen definiert haben, z. B. müssen alle Zertifikate eine Mindestschlüsselstärke von 2048 Bit haben und eine vertrauenswürdige Zertifizierungsstelle muss sie autorisieren.

In einem anderen Beispiel haben Sie möglicherweise ein neues Zertifikat hochgeladen, aber vergessen, es an einen virtuellen Server zu binden. Das SSL-Dashboard hebt die verwendeten oder nicht verwendeten SSL-Zertifikate hervor. Im Abschnitt **Verwendung** sehen Sie die Anzahl der installierten Zertifikate und die Anzahl der verwendeten Zertifikate. Sie können weiter auf das Diagramm klicken, um den Zertifikatnamen, die Instanz, auf der es verwendet wird, seine Gültigkeit, seinen Signaturalgorithmus usw. anzuzeigen.

Um SSL-Zertifikate in Citrix ADM zu überwachen, navigieren Sie zu**Netzwerke**> **SSL-Dashboard**.



Mit Citrix ADM können Sie SSL-Zertifikate abfragen und alle SSL-Zertifikate der Instanzen sofort Citrix ADM hinzufügen. Um dies zu tun,

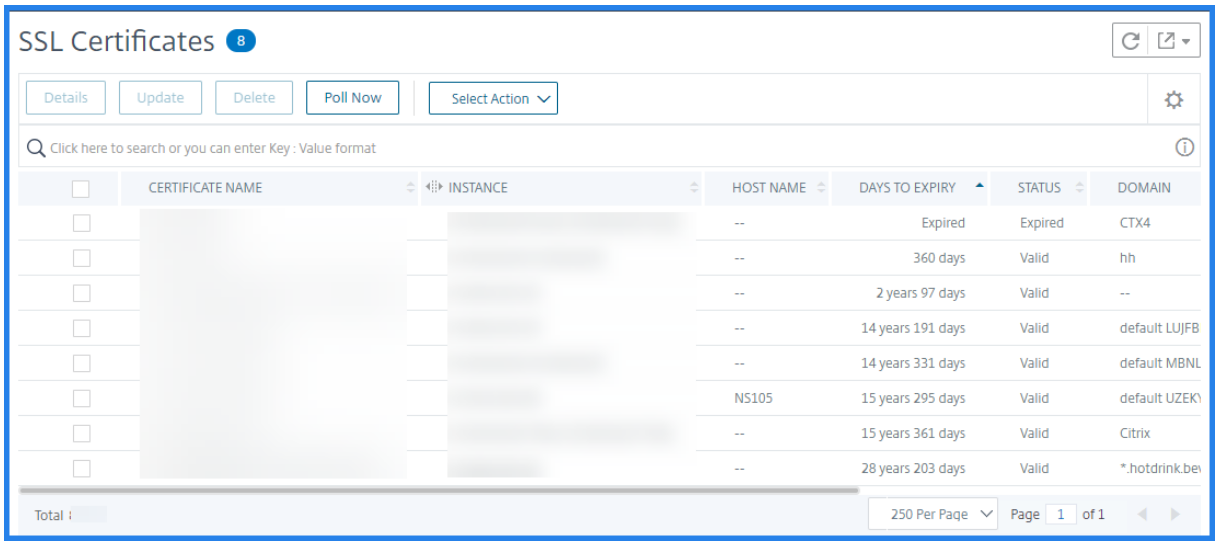
1. Navigieren Sie zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf **Jetzt abfragen**.

   Auf der Seite **Jetzt abfragen** können Sie entweder alle verwalteten ADC-Instances abfragen oder bestimmte Instances auswählen.
3. Klicken Sie auf **Abruf starten**.

Im **SSL-Dashboard**können Sie die ADC-SSL-Zertifikate, virtuellen SSL-Server und SSL-Protokolle überwachen.

Sie können auf die Metriken im Dashboard klicken, um Details zu SSL-Zertifikaten, virtuellen SSL-Servern oder SSL-Protokollen anzuzeigen.

Wenn Sie beispielsweise auf die Nummer unter **Self signed vs CA signed** auf dem Dashboard klicken, zeigt die ADM-GUI alle SSL-Zertifikate auf den Citrix ADC Instanzen an.



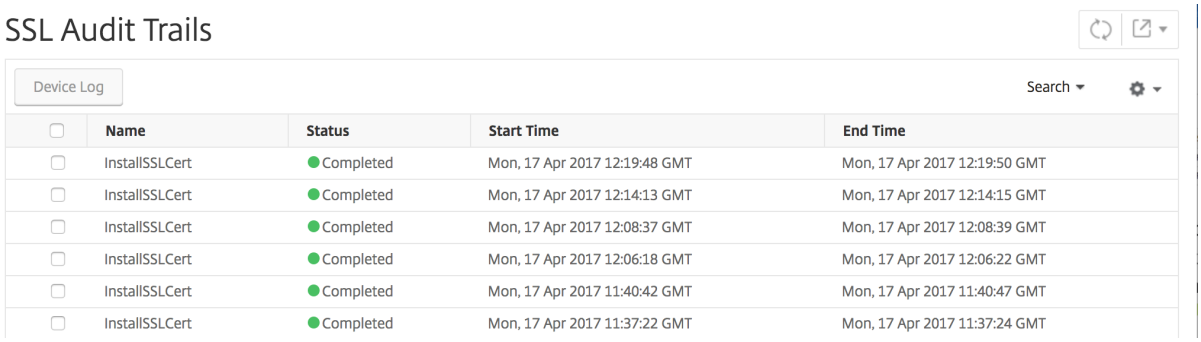
Das Citrix ADM SSL-Dashboard zeigt auch die Verteilung der SSL-Protokolle an, die auf Ihren virtuellen Servern ausgeführt werden. Als Administrator können Sie die Protokolle, die Sie überwachen möchten, über die SSL-Richtlinie angeben. Weitere Informationen finden Sie unter Konfigurieren von SSL-Richtlinien. Die unterstützten Protokolle sind SSLv2, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 und TLS 1.3. Die auf virtuellen Servern verwendeten SSL-Protokolle werden in einem Balkendiagrammformat angezeigt. Durch Klicken auf ein bestimmtes Protokoll wird eine Liste der virtuellen Server angezeigt, die dieses Protokoll verwenden.

Ein Ringdiagramm wird angezeigt, nachdem Diffie-Hellman (DH) - oder Ephemeral RSA-Schlüssel im SSL-Dashboard aktiviert oder deaktiviert wurden. Diese Schlüssel ermöglichen eine sichere Kommunikation mit Exportclients, auch wenn das Serverzertifikat keine Exportclients unterstützt, wie im Fall eines 1024-Bit-Zertifikats. Wenn Sie auf das entsprechende Diagramm klicken, wird eine Liste der virtuellen Server angezeigt, auf denen DH- oder Ephemere RSA-Schlüssel aktiviert sind.

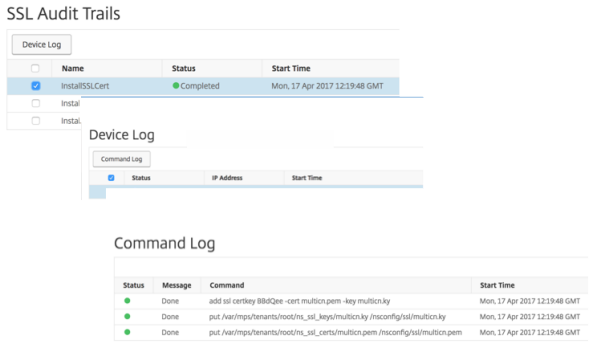
So zeigen Sie Audit-Trails für SSL-Zertifikate an

Sie können jetzt Protokolldetails von SSL-Zertifikaten auf Citrix ADM anzeigen. In den Protokolldetails werden Vorgänge angezeigt, die mit SSL-Zertifikaten auf Citrix ADM ausgeführt wurden, z. B.: Installieren von SSL-Zertifikaten, Verknüpfen und Aufheben der Verknüpfung von SSL-Zertifikaten, Aktualisieren von SSL-Zertifikaten und Löschen von SSL- Audit-Pfadinformationen sind nützlich, während SSL-Zertifikatänderungen in einer Anwendung mit mehreren Eigentümern überwacht werden.

Um ein Überwachungsprotokoll für einen bestimmten Vorgang anzuzeigen, der in Citrix ADM mit SSL-Zertifikaten ausgeführt wird, navigieren Sie zu **Netzwerke** > **SSL-Dashboard** > und klicken Sie auf **Überwachungsprotokolle**.



Für einen bestimmten Vorgang, der mit SSL-Zertifikat ausgeführt wird, können Sie den Status, die Startzeit und die Endzeit anzeigen. Darüber hinaus können Sie die Instanz anzeigen, für die der Vorgang ausgeführt wurde, und die Befehle, die für diese Instanz ausgeführt werden.



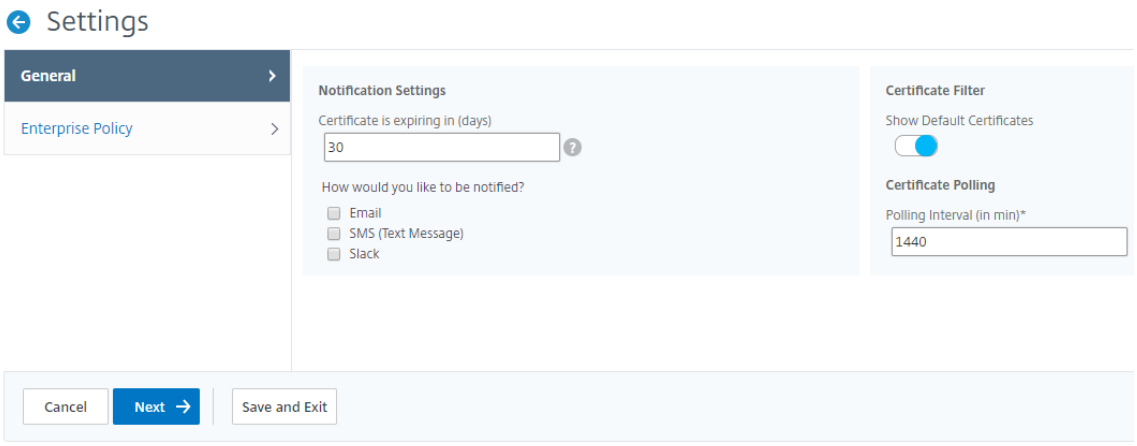
So schließen Sie standardmäßige Citrix ADC Zertifikate im SSL-Dashboard aus

Mit Citrix ADM können Sie Citrix ADC-Standardzertifikate, die in den SSL-Dashboard-Diagrammen angezeigt werden, je nach Ihren Einstellungen ein- oder ausblenden. Standardmäßig werden alle Zertifikate im SSL-Dashboard angezeigt, einschließlich Standardzertifikaten.

So blenden Sie Standardzertifikate auf dem SSL-Dashboard ein oder aus:

1. Navigieren Sie zu **Netzwerke** > **SSL-Dashboard** in der Citrix ADM GUI.

2. Klicken Sie auf der Seite **SSL-Dashboard** auf **Einstellungen**.
3. Wählen Sie auf der Seite **Einstellungen** die Option **Allgemein** aus.
4. Geben Sie die Anzahl der Tage ein, an denen das Zertifikat abläuft, um eine Benachrichtigung über den Ablauf des Zertifikats zu erhalten.
5. Wählen Sie die Benachrichtigungsmethode und erstellen Sie die entsprechenden Profile.
6. Deaktivieren Sie im Abschnitt **Zertifikatfilter**das Kontrollkästchen **Standardzertifikate anzeigen**, und klicken Sie auf **Speichern und Beenden**.



Anzeigen, Hochladen und Herunterladen von SSL-Dateien

Um SSL-Dateien auf Citrix ADM anzuzeigen, navigieren Sie zu **Netzwerke > SSL-Dashboard > SSL-Dateien auf Citrix ADM**.

Auf dieser Seite können Sie die folgenden Dateien in Citrix ADM anzeigen, hochladen und herunterladen:

- SSL-Zertifikate
- SSL-Schlüssel
- SSL-CSRs

Um SSL-Dateien auf einer Citrix ADC-Instanz anzuzeigen und herunterzuladen, navigieren Sie zu **Netzwerke > SSL-Dashboard > SSL-Dateien auf Citrix ADC**.

> **Wichtig!**
>
> Um den Download von SSL-Dateien von ADC-Instanzen zu aktivieren, aktivieren Sie die **Instanz-SSL-Zertifikatfunktion**. Weitere Informationen finden Sie unter ADM-Funktionen aktivieren oder deaktivieren.

Benachrichtigungen für das Ablaufdatum des SSL-Zertifikats einrichten

February 5, 2024

Als Sicherheitsadministrator können Sie Benachrichtigungen einrichten, die Sie informieren, wenn Zertifikate bald ablaufen, und Informationen darüber enthalten, welche Citrix Application Delivery Controller (ADC) -Instanzen diese Zertifikate verwenden. Durch die Aktivierung von Benachrichtigungen können Sie Ihre SSL-Zertifikate rechtzeitig erneuern.

Sie können beispielsweise festlegen, dass eine E-Mail-Benachrichtigung 30 Tage vor Ablauf Ihres Zertifikats an eine E-Mail-Verteilerliste gesendet wird.

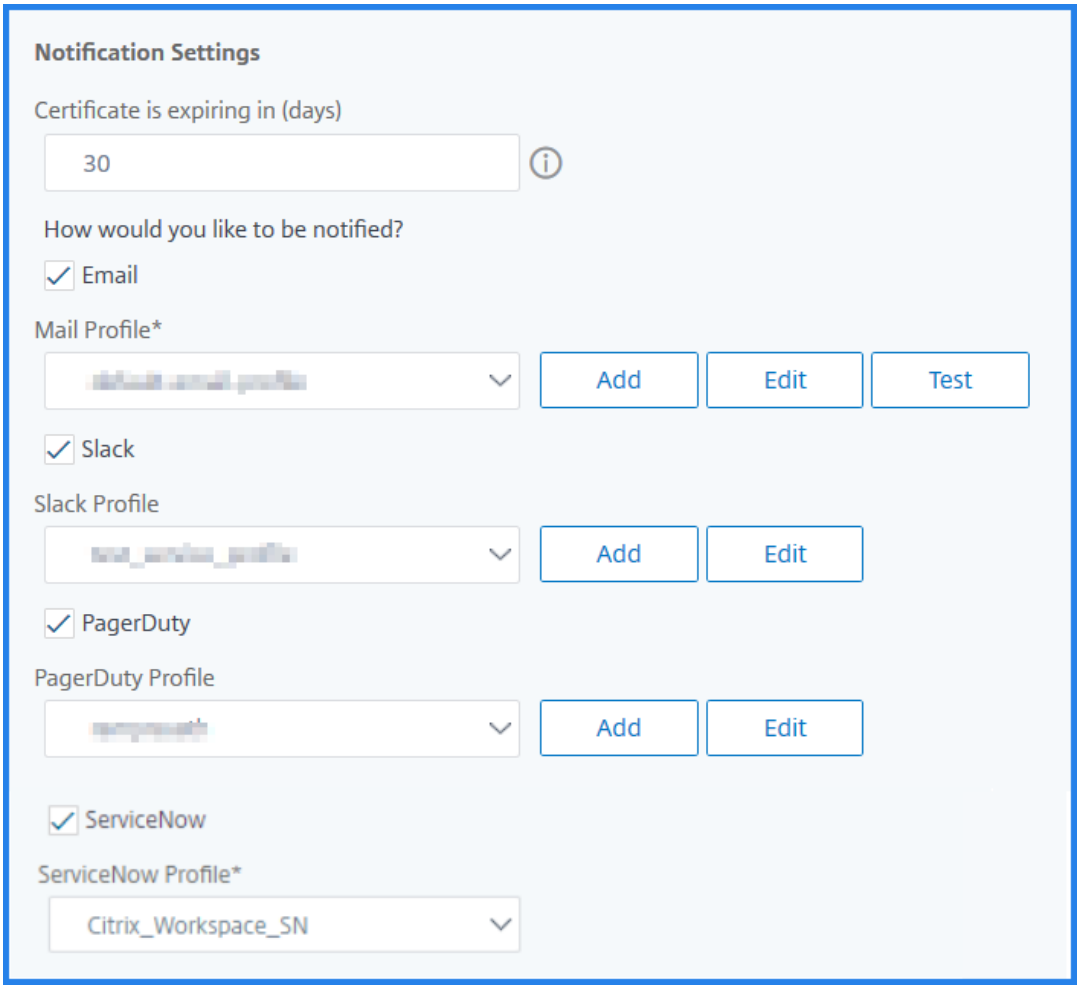
So richten Sie Benachrichtigungen von NetScaler ADM ein:

1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zu **Netzwerke > SSL Dashboard**.
2. Klicken Sie auf der Seite **SSL-Dashboard** auf **Einstellungen**.
3. Klicken Sie auf der Seite **SSL-Einstellungen** auf das Symbol **Bearbeiten**.
4. Geben Sie im Abschnitt **Benachrichtigungseinstellungen** an, wann Sie die Benachrichtigung versenden möchten, und geben Sie die Anzahl der Tage vor dem Ablaufdatum an.
5. Wählen Sie die Art der Benachrichtigung, die Sie senden möchten. Wählen Sie den Benachrichtigungstyp und die Verteilerliste aus dem Drop-down-Menü aus. Die Benachrichtigungstypen sind wie folgt:

    - **E-Mail**—Geben Sie einen Mailserver und Profildetails an. Eine E-Mail wird ausgelöst, wenn Ihre Zertifikate bald ablaufen.
    - **SMS** —Geben Sie einen SMS-Server (Short Message Service) und Profildetails an. Eine SMS-Nachricht wird ausgelöst, wenn Ihre Zertifikate bald ablaufen.
    - **Slack** - Geben Sie die Details des Slack Profils an.
    - **PagerDuty-Warnungen** - Geben Sie ein PagerDuty-Profil an Basierend auf den in Ihrem PagerDuty-Portal konfigurierten Benachrichtigungseinstellungen wird eine Benachrichtigung gesendet, wenn Ihre Zertifikate bald ablaufen.
    - **ServiceNow** - Eine Benachrichtigung wird an das standardmäßige ServiceNow-Profil gesendet, wenn Ihre Zertifikate bald ablaufen.

        > **Wichtig**
        >
        > Stellen Sie sicher, dass der Citrix Cloud ITSM-Adapter für ServiceNow konfiguriert und

> in NetScaler ADM integriert ist. Weitere Informationen finden Sie unter Integrieren von NetScaler ADM mit ServiceNow-Instanz.



6. Klicken Sie auf **Speichern und Beenden**.

NetScaler ADM sendet nun SSL-Zertifikatablauftrap an den externen Trap-Zielserver, wenn Ihre SSL-Zertifikate abgelaufen sind. Citrix ADM sendet eine Trap, wenn die folgenden beiden Bedingungen erfüllt sind:

- Sie haben die Anzahl der Tage, an denen das Zertifikat abläuft, auf der Seite mit den SSL-Dashboard-Einstellungen konfiguriert.
- Sie haben das Trap-Ziel hinzugefügt.

Sie können Trap-Ziele festlegen, indem Sie zu **System > SNMP > Trap-Ziele**navigieren. Geben Sie die IP-Adresse des Ziel-SNMP-Servers ein, an den die Traps gesendet werden. Geben Sie die Portnummer ein und geben Sie „public“(ohne Anführungszeichen) als Community-Zeichenfolge ein.

Installiertes Zertifikat aktualisieren

February 5, 2024

Nachdem Sie ein erneuertes Zertifikat von der Zertifizierungsstelle erhalten haben, können Sie vorhandene Zertifikate von Citrix Application Delivery Management (ADM) aktualisieren, ohne sich bei einzelnen ADC-Instanzen (Citrix Application Delivery Controller) anmelden zu müssen.

So aktualisieren Sie ein SSL-Zertifikat, einen Schlüssel oder beides von NetScaler ADM:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf eine der Diagramme, um die Liste der SSL-Zertifikate anzuzeigen.
3. Wählen Sie auf der Seite **SSL-Zertifikate** ein Zertifikat aus und klicken Sie auf **Update**. Alternativ klicken Sie auf das SSL-Zertifikat, um die Details anzuzeigen, und klicken Sie dann oben rechts auf der Seite **SSL-Zertifikat** auf **Aktualisieren**.
4. Nehmen Sie auf der Seite **SSL-Zertifikat aktualisieren** die erforderlichen Änderungen am Zertifikat, Schlüssel oder beides vor, und klicken Sie auf **OK**.

SSL-Zertifikate auf einer NetScaler ADC-Instanz installieren

February 5, 2024

Stellen Sie vor der Installation von SSL-Zertifikaten auf Citrix Application Delivery Controller (ADC) -Instanzen sicher, dass die Zertifikate von vertrauenswürdigen Zertifizierungsstellen ausgestellt wurden. Stellen Sie außerdem sicher, dass die Schlüsselstärke der Zertifikatschlüssel 2048 Bit oder höher beträgt und dass die Schlüssel mit sicheren Signaturalgorithmen signiert sind.

So installieren Sie ein SSL-Zertifikat von einer anderen NetScaler ADC-Instanz:

Sie können auch ein Zertifikat aus einer ausgewählten NetScaler ADC Instanz importieren und es auf andere zielgerichtete NetScaler ADC-Instanzen von der NetScaler Application Delivery Management (ADM) GUI anwenden.

1. Navigieren Sie zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie in der rechten oberen Ecke des SSL-Dashboards auf **Installieren**.
3. Geben Sie auf der Seite **SSL-Zertifikat auf Citrix ADC Instanzen installieren**die folgenden Parameter an:

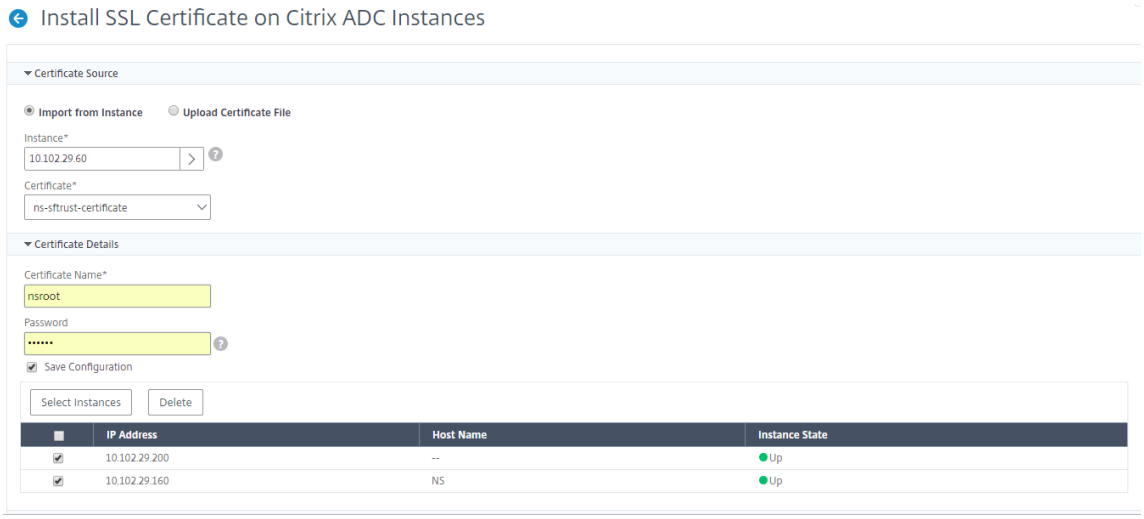
    a) Zertifikatquelle
    Wählen Sie die Option aus der **Instanz importieren aus**.

- Wählen Sie die **Instanz** aus, aus der Sie das Zertifikat importieren möchten.
- Wählen Sie das **Zertifikat** aus der Liste aller SSL-Zertifikatsdateien auf der Instanz aus.

b) Zertifikatdetails

- **Name des Zertifikats**. Geben Sie einen Namen für den Zertifikatsschlüssel an.
- **Kennwort**. Kennwort zum Verschlüsseln des privaten Schlüssels. Sie können diese Option verwenden, um verschlüsselte private Schlüssel hochzuladen.

4. Klicken Sie auf **Instanzen auswählen**, um die NetScaler ADC-Instanzen auszuwählen, auf denen Sie Ihre Zertifikate installieren möchten.
5. Klicken Sie auf **OK**.



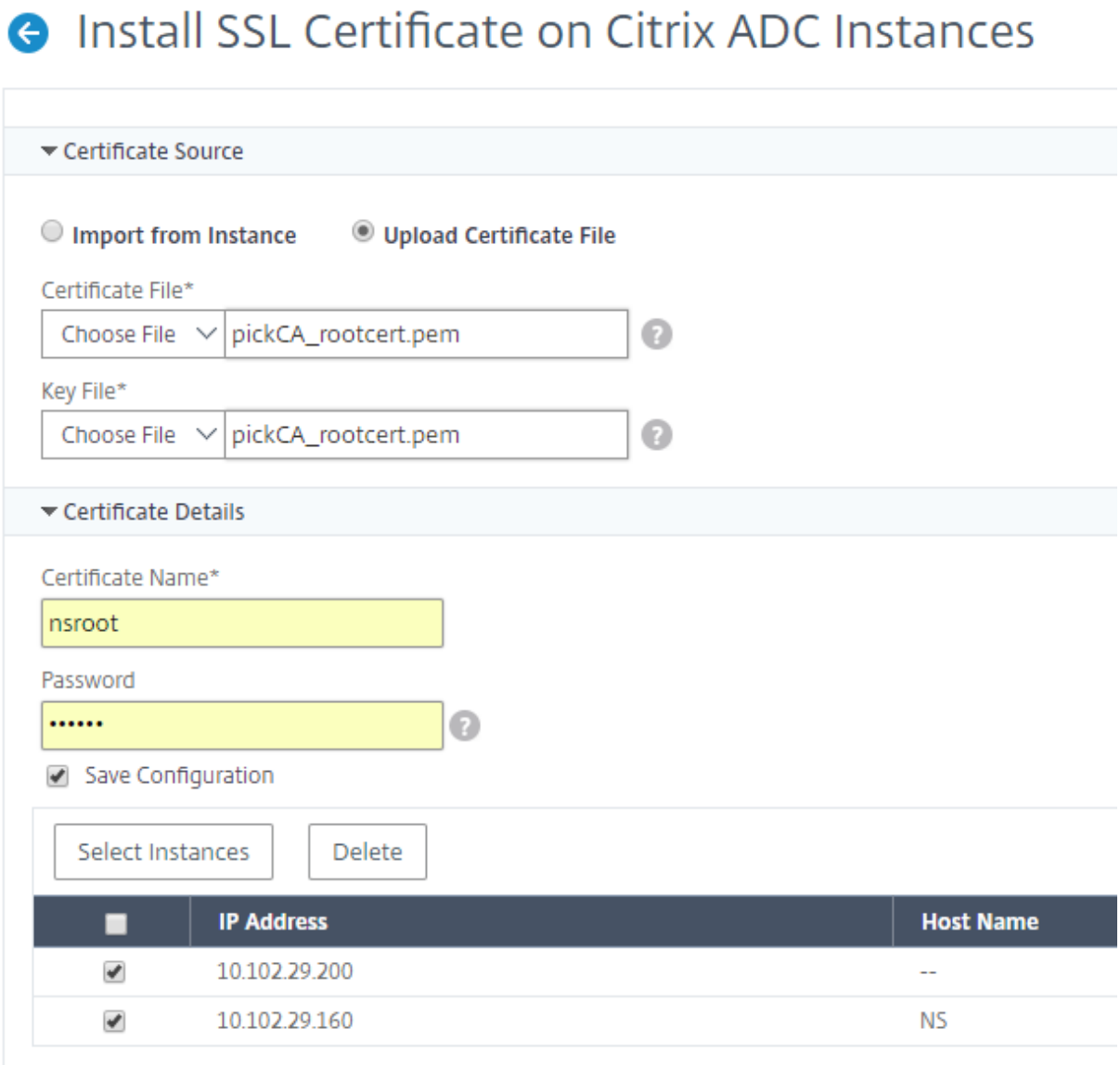
So installieren Sie ein SSL-Zertifikat von NetScaler ADM:

1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie in der rechten oberen Ecke des Dashboards auf **Installieren**.
3. Wählen Sie auf der Seite **SSL-Zertifikat auf NetScaler ADC Instanz installieren** die Option **Zertifikatdatei hochladen** aus, und geben Sie die folgenden Parameter an:

- **Zertifikatsdatei** - Laden Sie eine SSL-Zertifikatsdatei hoch, indem Sie entweder **Local** (Ihr lokaler Computer) oder **Appliance** auswählen (die Zertifikatsdatei muss in der virtuellen NetScaler ADM-Instanz vorhanden sein).
- **Schlüsseldatei** - Laden Sie die Schlüsseldatei hoch.
- **Zertifikatsname** —Geben Sie einen Namen für den Zertifikatsschlüssel an.
- **Kennwort** —Kennwort zum Verschlüsseln des privaten Schlüssels. Sie können diese Option verwenden, um verschlüsselte private Schlüssel hochzuladen.

- **Instanzen auswählen** - Wählen Sie die Citrix ADM Instanzen aus, auf denen Sie die Zertifikate installieren möchten.

4. Um die Konfiguration für die spätere Verwendung zu **speichern, aktivieren Sie das Kontrollkästchen Konfiguration speichern** .
5. Klicken Sie auf **OK**.



Zertifikatsignieranforderung (CSR) erstellen

February 5, 2024

Eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) ist ein Block mit verschlüsseltem Text, der auf dem Server generiert wird, auf dem das Zertifikat verwendet wird. Es enthält Informationen, die in das Zertifikat aufgenommen werden, wie z. B. den Namen Ihrer Organisation, den allgemeinen Namen (Domainname), den Ort und das Land.

So erstellen Sie eine CSR mit NetScaler ADM:

1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf eines der Diagramme, um die Liste der installierten SSL-Zertifikate anzuzeigen. Wählen Sie dann das Zertifikat aus, für das Sie eine CSR erstellen möchten, und wählen Sie in der Liste **Aktion auswählen die OptionCSR erstellen** aus.
3. Geben Sie auf der Seite **Certificate Signing Request (CSR)** einen Namen für die CSR an.
4. Führen Sie einen der folgenden Schritte aus:
    - **Schlüssel hochladen** —Wählen Sie die Option **Ich habe einen Schlüssel** aus. Um Ihre Schlüsseldatei hochzuladen, wählen Sie entweder **Lokal** (Ihr lokaler Computer) oder **Appliance** (die Schlüsseldatei muss in der virtuellen NetScaler ADM-Instanz vorhanden sein).
    - **Schlüssel erstellen** —Wählen Sie die Option Ich habe keinen Schlüssel aus, und geben Sie dann die folgenden Parameter an:

Verschlüsselungsalgorithmus	Art des Schlüssels. Zum Beispiel RSA.
Name der Schlüsseldatei	Name für Ihre Datei, in der der RSA-Schlüssel gespeichert ist.
Größe des Schlüssels	Schlüsselgröße in Bit.
Öffentlicher Exponentenwert	Wählen Sie entweder **3** oder **F4** aus der bereitgestellten Dropdown-Liste aus. Dieser Wert ist Teil des Verschlüsselungsalgorithmus, der zum Erstellen Ihres RSA-Schlüssels erforderlich ist.
Schlüssel-Format	Standardmäßig ist PEM ausgewählt. PEM ist das empfohlene Schlüsselformat für Ihr SSL-Zertifikat.

PEM-Kodierungsalgorithmus	Wählen Sie in der Dropdownliste den Algorithmus (**DES** oder **DES3**) aus, den Sie zum Verschlüsseln des generierten RSA-Schlüssels verwenden möchten. Wenn Sie diesen Algorithmus auswählen, müssen Sie eine PEM-Passphrase angeben.
PEM-Passphrase	Wenn Sie den PEM-Kodierungsalgorithmus ausgewählt haben, geben Sie eine Passphrase ein.
PEM-Passphrase bestätigen	Bestätigen Sie Ihre PEM-Passphrase.

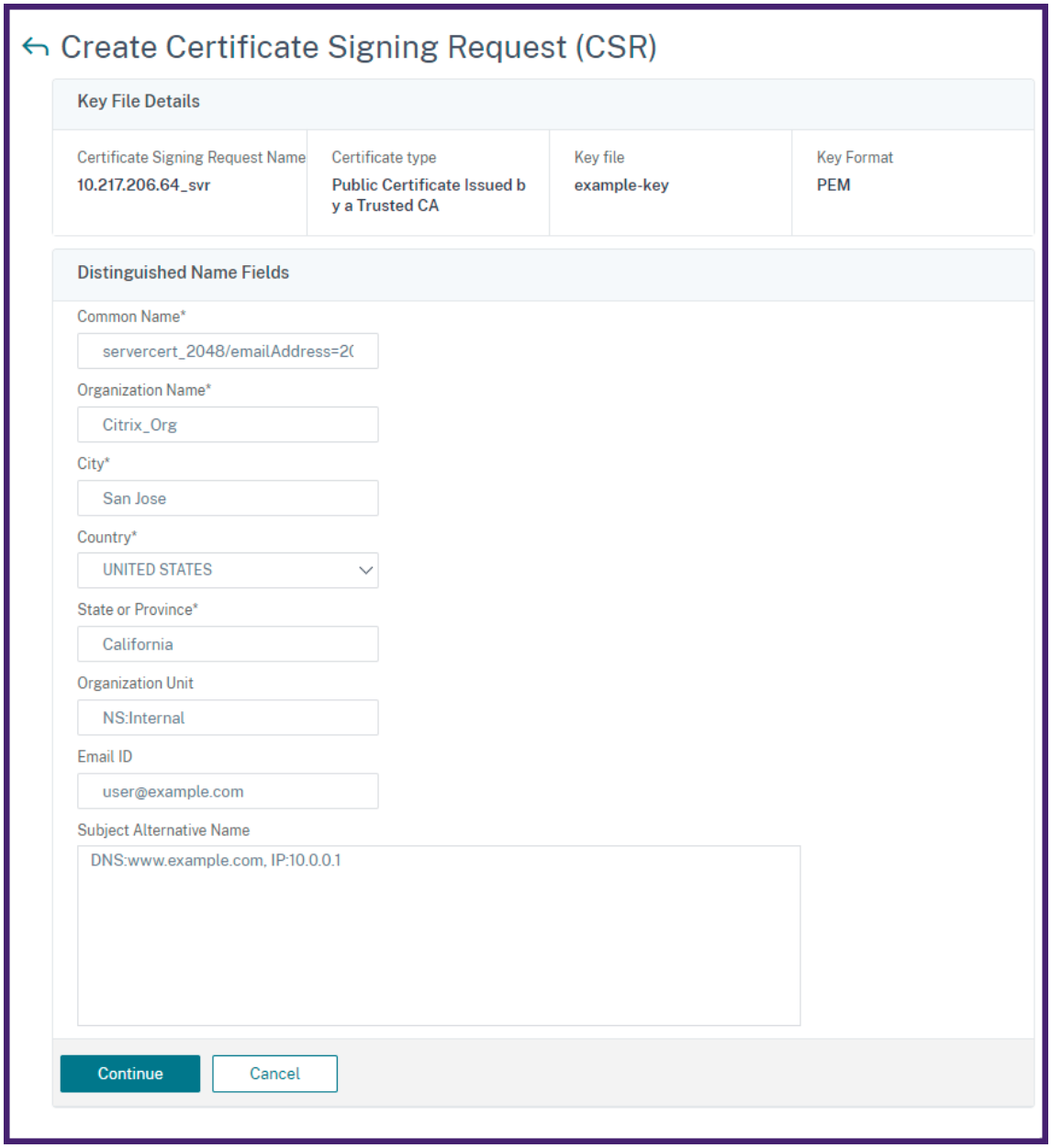
5. Klicken Sie auf **Weiter**.
6. Geben Sie auf der folgenden Seite weitere Details an.

   Die meisten Felder haben Standardwerte, die aus dem Betreff des ausgewählten Zertifikats extrahiert wurden. Der Betreff enthält Details wie den allgemeinen Namen, den Namen der Organisation, den Bundesstaat und das Land.

   Im Feld **Subject Alternative Name** können Sie mehrere Werte wie Domänennamen und IP-Adressen mit einem einzigen Zertifikat angeben. Die alternativen Namen des Subjekts helfen Ihnen, mehrere Domänen mit einem einzigen Zertifikat zu sichern.

   Geben Sie die Domänennamen und IP-Adressen im folgenden Format an:

```
DNS:<Domain name>, IP:<IP address>
<!--NeedCopy-->
```

In diesem Beispiel sichert es `10.0.0.1` und `www.example.com`.

Überprüfen Sie die Felder und klicken Sie auf **Weiter**.

> **Hinweis**
>
> Die meisten Zertifizierungsstellen akzeptieren Zertifikatsübermittlungen per E-Mail. Die Zertifizierungsstelle gibt ein gültiges Zertifikat an die E-Mail-Adresse zurück, von der Sie die CSR übermitteln.

SSL-Zertifikate verknüpfen und aufheben

February 5, 2024

Sie erstellen ein Zertifikatspaket, indem Sie mehrere Zertifikate miteinander verknüpfen. Um ein Zertifikat mit einem anderen Zertifikat zu verknüpfen, muss der Aussteller des ersten Zertifikats mit der Domäne des zweiten Zertifikats übereinstimmen. Wenn Sie beispielsweise Zertifikat A mit Zertifikat B verknüpfen möchten, muss der „Aussteller“von Zertifikat A der „Domäne“von Zertifikat B entsprechen.

So verknüpfen Sie mithilfe von NetScaler ADM ein SSL-Zertifikat mit einem anderen Zertifikat:

1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf eine der Diagramme, um die Liste der SSL-Zertifikate anzuzeigen.
3. Wählen Sie das Zertifikat aus, das Sie verknüpfen möchten, und wählen Sie dann in der Dropdownliste **Aktion** die Option **Verknüpfung** aus.
4. Wählen Sie in der Liste der übereinstimmenden Zertifikate das Zertifikat aus, mit dem Sie eine Verknüpfung herstellen möchten, und klicken Sie dann auf **OK**.

> **Hinweis**
>
> Wenn kein übereinstimmendes Zertifikat gefunden wird, wird die folgende Meldung angezeigt: Kein Zertifikat zum Verknüpfen gefunden.

So heben Sie die Verknüpfung eines SSL-Zertifikats mithilfe von NetScaler ADM auf:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf eine der Diagramme, um die Liste der SSL-Zertifikate anzuzeigen.
3. Wählen Sie eines der verknüpften Zertifikate aus, die verknüpft sind, und wählen Sie dann **Verknüpfung aufheben** aus der Dropdownliste **Aktion** aus.
4. Klicken Sie auf **OK**.

> **Hinweis**
>
> Wenn das ausgewählte Zertifikat nicht mit einem anderen Zertifikat verknüpft ist, wird die folgende Meldung angezeigt: Zertifikat verfügt über keine Zertifizierungsstellen-Verknüpfung.

Unternehmensrichtlinie konfigurieren

February 5, 2024

Sie können eine Unternehmensrichtlinie konfigurieren und alle vertrauenswürdigen Zertifizierungsstellen und sicheren Signaturalgorithmen hinzufügen und die empfohlene Schlüsselstärke für Ihre Zertifikatsschlüssel in NetScaler Application Delivery Management (ADM) auswählen. Wenn eines der auf Ihrer Citrix Application Delivery Controller (ADC) -Instanz installierten Zertifikate nicht zur Unternehmensrichtlinie hinzugefügt wurde, zeigt das SSL-Zertifikats-Dashboard den Aussteller dieser Zertifikate als **nicht empfohlen**an.

Wenn die Schlüsselstärke des Zertifikats nicht mit der in der Unternehmensrichtlinie empfohlenen Schlüsselstärke übereinstimmt, zeigt das SSL-Zertifikats-Dashboard die Stärken dieser Schlüssel außerdem als **Nicht empfohlen** an.

So konfigurieren Sie eine Unternehmensrichtlinie auf NetScaler ADM:

1. Navigieren Sie in Citrix ADM zu **Infrastruktur** > **SSL Dashboard**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf der Seite SSL-Einstellungen auf das Symbol **Bearbeiten**, um alle vertrauenswürdigen Zertifizierungsstellen und sicheren Signaturalgorithmen hinzuzufügen und die empfohlene Schlüsselstärke für Ihre Zertifikate und Schlüssel auszuwählen.
3. Klicken Sie auf **Speichern**, um Ihre Unternehmensrichtlinie zu speichern.

SSL-Zertifikate von Citrix ADC-Instanzen abfragen

February 5, 2024

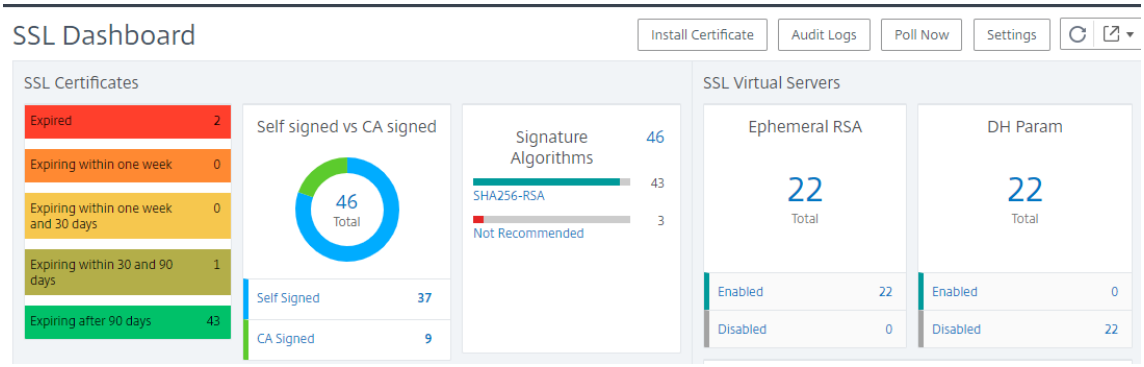
Citrix Application Delivery Management (ADM) fragt SSL-Zertifikate automatisch alle 24 Stunden mithilfe von NITRO-Aufrufen und dem Secure Copy (SCP) -Protokoll ab. Sie können die SSL-Zertifikate auch manuell abfragen, um neu hinzugefügte SSL-Zertifikate auf den Citrix Application Delivery Controller (ADC) -Instanzen zu ermitteln. Durch das Abrufen aller Citrix ADC-Instanzen SSL-Zertifikate wird das Netzwerk stark belastet.

Anstatt alle SSL-Zertifikate der Citrix ADC-Instanzen abzufragen, können Sie manuell nur die SSL-Zertifikate einer ausgewählten Instanz oder Instanzen abfragen.

So fragen Sie SSL-Zertifikate auf Citrix ADC-Instanzen ab:

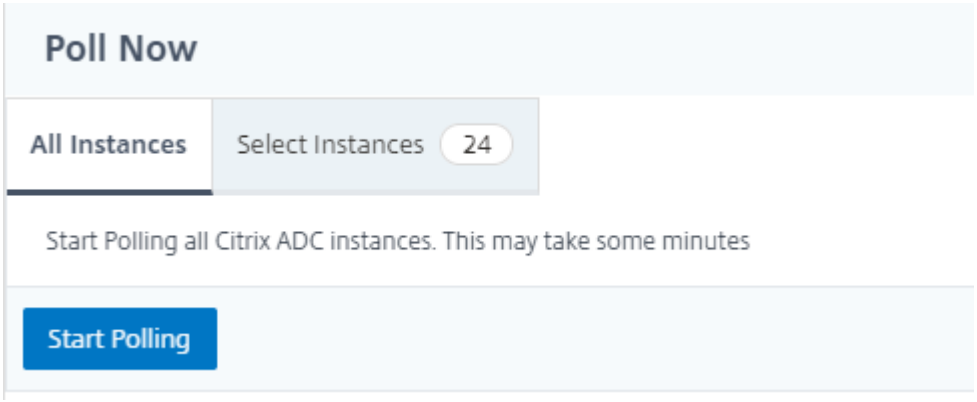
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**.

2. Klicken Sie auf der Seite **SSL-Dashboard** oben rechts auf **Jetzt abfragen**.

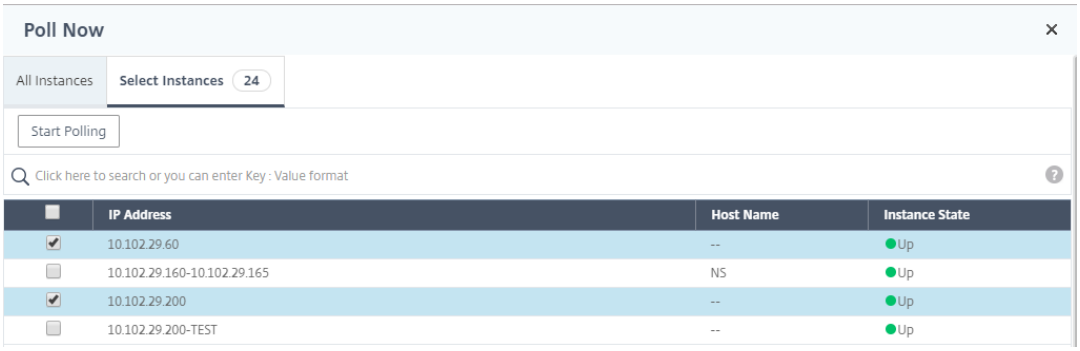


3. Die **Seite „Jetzt abfragen** "wird geöffnet und bietet Ihnen die Möglichkeit, alle Citrix ADC-Instanzen im Netzwerk oder ausgewählte Instanzen abzufragen.

   a) Um die SSL-Zertifikate aller Citrix ADC-Instanzen abzufragen, wählen Sie die Registerkarte **Alle Instanzen** und klicken Sie auf **Abfrage starten**.



   b) Um bestimmte Instanzen abzufragen, wählen Sie die Registerkarte**Instanzenauswählen**aus, wählen Sie die Instanzen aus der Liste aus und klicken Sie auf**Jetzt abfragen**.



Konfigurieren der IP-Adressverwaltung (IPAM)

February 5, 2024

ADM IPAM bietet Ihnen die Möglichkeit, IP-Adressen in von ADM verwalteten Konfigurationen automatisch zuzuweisen und freizugeben. Sie können IPs aus Netzwerken oder IP-Bereichen zuweisen, die mit den folgenden IP-Anbietern definiert wurden:

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

Derzeit können Sie ADM IPAM in folgenden Bereichen verwenden:

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

Sie können auch die zugewiesenen und verfügbaren IP-Adressen in jedem Netzwerk oder IP-Bereich verfolgen, der von ADM verwaltet wird.

Einen externen IP-Adressanbieter hinzufügen

ADM verfügt über einen integrierten IPAM-Anbieter zur Verwaltung von IPs und IP-Bereichen. Wenn Sie eine externe IP-Anbieterlösung in ADM hinzufügen möchten, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Netzwerke > IPAM**.
2. Klicken Sie unter **Anbieter**auf **Hinzufügen**.
3. Geben Sie die folgenden Details an, um einen IP-Anbieter hinzuzufügen:
    - **Name** —Geben Sie den Namen des IP-Anbieters an, der in ADM verwendet werden soll.
    - **Anbieter** —Wählen Sie einen IP-Adressenanbieter aus der Liste aus.
    - **URL** —Geben Sie die URL der IPAM-Lösung an, die IP-Adressen in der ADM-Umgebung zuweist.
    - **Benutzername** —Geben Sie den Benutzernamen an, um sich bei der IPAM-Lösung anzumelden.
    - **Kennwort** —Geben Sie das Kennwort an, um sich bei der IPAM-Lösung anzumelden.
4. Klicken Sie auf **Hinzufügen**.

Ein Netzwerk hinzufügen

Fügen Sie ein Netzwerk hinzu, um IPAM mit ADM-verwalteten Konfigurationen zu verwenden.

1. Navigieren Sie zu **Netzwerke > IPAM**.
2. Klicken Sie unter **Netzwerke**auf **Hinzufügen**.
3. Geben Sie die folgenden Details an:
   - **Netzwerkname** —Geben Sie den Netzwerknamen an, um das Netzwerk in ADM zu identifizieren.
   - **Anbieter** —Wählen Sie den Anbieter aus der Liste aus.

     In dieser Liste werden die in ADM hinzugefügten Anbieter angezeigt.
   - **Netzwerktyp** - Wählen Sie **IP-Bereich** oder **CIDR** aus der Liste basierend auf Ihren Anforderungen aus.
   - **Netzwerkwert** —Geben Sie den Netzwerkwert an.

     > **Hinweis**
     >
     > ADM IPAM unterstützt nur IPv4-Adressen.

     Geben Sie für **IP-Bereich**den Netzwerkwert im folgenden Format an:

     ```
     <first-IP-address>-<last-IP-address>
     <!--NeedCopy-->
     ```

     Beispiel:

     ```
     10.0.0.20-10.0.0.100
     <!--NeedCopy-->
     ```

     Geben Sie für **CIDR**den Netzwerkwert im folgenden Format an:

     ```
     <IP-address>/<subnet-mask>
     <!--NeedCopy-->
     ```

     Beispiel:

     ```
     10.70.124.0/24
     <!--NeedCopy-->
     ```
4. Klicken Sie auf **Erstellen**.

Anzeigen zugewiesenen IP-Adressen

Um weitere Details zu zugewiesenen IP-Adressen aus dem IPAM-Netzwerk anzuzeigen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Netzwerke > IPAM**.
2. Klicken Sie auf der Registerkarte **Netzwerke** auf **Alle zugewiesenen IPs**anzeigen.

   In diesem Bereich werden IP-Adresse, Anbietername, Anbieter des Anbieters und Beschreibung angezeigt. Außerdem werden die Ressourcendetails angezeigt, die diese IP-Adresse reserviert haben:

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

> **Hinweis**
>
> Wenn Sie die IP-Adresse freigeben möchten, wählen Sie die IP-Adresse aus, die Sie freigeben möchten, und klicken Sie auf **Zugeteilte IPs freigeben**.

Konfigurationsaufträge

February 5, 2024

NetScaler Application Delivery Management (NetScaler ADM) -Konfigurationsverwaltungsprozess stellt die ordnungsgemäße Replikation von Konfigurationsänderungen, Systemaktualisierungen und anderen Wartungsaktivitäten über mehrere ADC-Instanzen (Citrix Application Delivery Controller) im Netzwerk sicher.

NetScaler ADM ermöglicht es Ihnen, Konfigurationsaufträge zu erstellen, die Ihnen helfen, all diese Aktivitäten problemlos auf mehreren Geräten als eine einzige Aufgabe auszuführen. Konfigurationsaufträge und Vorlagen vereinfachen die sich wiederholenden Verwaltungsaufgaben zu einer einzigen Aufgabe auf NetScaler ADM. Ein Konfigurationsauftrag enthält eine Reihe von Konfigurationsbefehlen, die Sie auf einem oder mehreren verwalteten Geräten ausführen können.

Konfigurationsjobs können entweder SSH-Befehle verwenden, um Konfigurationsbefehle auszuführen, oder SCP verwenden, um Dateien entweder lokal oder auf eine andere Appliance zu kopieren. Beispielsweise können wir ein HA-Failover oder HA-Upgrade planen.

Sie können einen Konfigurationsauftrag erstellen, indem Sie eine der folgenden vier Optionen in NetScaler ADM verwenden. Verwenden Sie eine davon, um eine wiederverwendbare Quelle

von Befehlen und Anweisungen für das System zur Ausführung eines Konfigurationsauftrags zu erstellen.

1. Konfigurationsvorlage
2. Instanz
3. Datei
4. Aufnehmen und Abspielen

Konfigurationsvorlage

Sie können Konfigurationsvorlagen erstellen, während Sie einen Auftrag erstellen und eine Reihe von Konfigurationsbefehlen als Vorlage speichern. Wenn Sie diese Vorlagen auf der Seite Jobs erstellen speichern, werden sie automatisch auf der Seite Vorlage erstellen angezeigt.

> **Hinweis**
> Die Option **Umbenennen** ist für die Standardkonfigurationsvorlagen deaktiviert. Sie können jedoch benutzerdefinierte Konfigurationsvorlagen umbenennen.

Sie können eine der folgenden Vorlagen verwenden:

Konfigurationseditor: Sie können den Konfigurationseditor verwenden, um CLI-Befehle einzugeben, die Konfiguration als Vorlage zu speichern und sie zum Konfigurieren von Aufträgen zu verwenden.

Integrierte Vorlage: Sie können aus einer Liste von Konfigurationsvorlagen wählen. Diese Vorlagen stellen die Syntaxen der CLI-Befehle bereit und ermöglichen es Ihnen, Werte für die Variablen anzugeben. Die integrierten Vorlagen sind mit ihren Beschreibungen in der folgenden Tabelle aufgeführt. Sie können einen Job planen, indem Sie die integrierte Vorlagenoption verwenden. Ein Job ist ein Satz von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Sie können beispielsweise die integrierte Vorlagenoption verwenden, um einen Auftrag zum Konfigurieren von Syslog-Servern zu planen. Sie können den Job auch sofort ausführen oder den Job planen, der zu einem späteren Zeitpunkt ausgeführt werden soll.

Instanz

Sie können eine Aktualisierung der Citrix SDX-Instanzen mit Citrix ADC Version 11.0 und höher durchführen. Um ein Einzelbündel-Upgrade durchzuführen, verwenden Sie einen integrierten Task in NetScaler ADM. Sie können eine NetScaler ADC-Instanz auch aktualisieren, indem Sie die ausgeführte Konfiguration oder eine gespeicherte Konfiguration extrahieren und die Befehle auf einer anderen NetScaler ADC-Instanz desselben Typs ausführen. Auf diese Weise können Sie die Konfiguration einer Instanz auf der anderen replizieren.

Datei

Sie können eine Konfigurationsdatei von Ihrem lokalen Computer hochladen und Jobs erstellen.

Vorteile der Verwendung einer Datei

- Sie können eine beliebige Textdatei verwenden, um eine wiederverwendbare Quelle für Konfigurationsbefehle zu erstellen.
- Jegliche Formatierung ist nicht erforderlich.
- Die Datei kann auf Ihrem lokalen Computer gespeichert werden.

Sie können entweder eine neue Datei erstellen und speichern oder eine vorhandene Datei importieren und die Befehle ausführen.

Aufnehmen und Abspielen

Mit Job erstellen können Sie entweder Ihre eigenen CLI-Befehle eingeben oder die Schaltfläche "Aufnehmen und Abspielen"verwenden, um Befehle aus einer NetScaler ADC-Sitzung zu erhalten. Wenn Sie den Auftrag ausführen, werden Änderungen in der ns.conf auf der ausgewählten Instanz aufgezeichnet und in NetScaler ADM kopiert.

Verwandte Artikel

- Verwendung des SCP (put) -Befehls in Konfigurationsjobs
- So verwenden Sie Variablen in Konfigurationsjobs
- So erstellen Sie Konfigurationsaufträge aus Korrekturbefehlen
- So verwenden Sie Konfigurationsvorlagen, um Auditvorlagen zu erstellen
- So verwenden Sie Record-and-Play zum Erstellen von Konfigurationsaufträgen
- Verwenden der Masterkonfigurationsvorlage unter Citrix ADM

Erstellen eines Konfigurationsauftrags

February 5, 2024

Ein Auftrag ist eine Reihe von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen erstellen und ausführen können. Sie können Jobs erstellen, um Konfigurationsänderungen über Instanzen hinweg vorzunehmen, Konfigurationen auf mehreren Instanzen in Ihrem Netzwerk zu replizieren und Konfigurationsaufgaben mit der NetScaler Application Delivery Management (ADM) -GUI aufzeichnen und in CLI-Befehle konvertieren.

Mit der Funktion Konfigurationsaufträge von NetScaler ADM können Sie einen Konfigurationsauftrag erstellen, E-Mail-Benachrichtigungen senden und Ausführungsprotokolle der erstellten Aufträge überprüfen.

So erstellen Sie einen Konfigurationsauftrag auf NetScaler ADM:

1. Navigieren Sie zu **Netzwerke > Konfigurationsaufträge**.
2. Klicken Sie auf **Job erstellen**.
3. Geben Sie auf der Seite **Job erstellen** auf der Registerkarte **Konfiguration auswählen** den Job-Namen an und wählen Sie den **Instanztyp** aus der Liste aus.
4. Wählen Sie in der Liste **Konfigurationsquelle** die Konfigurationsauftragsvorlage aus, die Sie erstellen möchten. Fügen Sie die Befehle für die ausgewählte Vorlage hinzu.

    - Sie können entweder die Befehle eingeben oder die vorhandenen Befehle aus den gespeicherten Konfigurationsvorlagen importieren.
    - Sie können auch mehrere Vorlagen verschiedener Typen im Konfigurationseditor hinzufügen, während Sie einen Job in den Konfigurationsaufträgen erstellen.
    - Wählen Sie in der Liste **Konfigurationsquelle** die verschiedenen Vorlagen aus und ziehen Sie die Vorlagen dann in den Konfigurationseditor. Die Vorlagentypen können **Konfigurationsvorlage**, **In-Built-Vorlage**, **Master-Konfiguration**, **Aufnahme und Wiedergabe**, **Instanz** und **Datei**sein.

    > **Hinweis**
    >
    > Wenn Sie die `Deploy Master Configuration Job` Vorlage zum ersten Mal hinzufügen, fügen Sie eine Vorlage eines anderen Typs hinzu, dann wird die gesamte Auftragsvorlage zu einem `Master Configuration` Typ.

    Sie können die Befehle auch im Konfigurationseditor neu anordnen und neu anordnen. Sie können den Befehl von einer Zeile in eine andere verschieben, indem Sie die Befehlszeile ziehen und dort ablegen. Sie können die Befehlszeile auch von einer Zeile zu einer beliebigen Zielzeile verschieben oder neu anordnen, indem Sie einfach die Befehlszeilennummer im Textfeld ändern. Sie können die Befehlszeile auch beim Bearbeiten des Konfigurationsauftrags neu anordnen und neu anordnen.

    Sie können Variablen definieren, mit denen Sie verschiedene Werte für diese Parameter zuweisen oder einen Auftrag über mehrere Instanzen ausführen können. Sie können alle Variablen überprüfen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags in einer einzigen konsolidierten Ansicht definiert haben. Klicken Sie auf die Registerkarte „**Variablenvorschau**“, um eine Vorschau der Variablen in einer einzigen konsolidierten Ansicht anzuzeigen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben.

Sie können Rollback-Befehle für jeden Befehl im Konfigurationseditor anpassen. Um Ihre benutzerdefinierten Befehle anzugeben, aktivieren Sie die benutzerdefinierte Rollback-Option.

> **Wichtig**
>
> Damit das benutzerdefinierte Rollback wirksam wird, schließen Sie den Assistenten zum **Erstellen eines Auftrags** ab. Wählen Sie auf der Registerkarte **Ausführen** die Option **Rollback Erfolgreicher Befehle** aus der Liste **Bei Befehlsfehler** aus.

5. **Wählen Sie auf der Registerkarte Instanzen** auswählen die Instanzen aus, für die Sie die Konfigurationsüberwachung ausführen möchten.

   a) In einem NetScaler ADC Hochverfügbarkeitspaar können Sie einen Konfigurationsauftrag lokal auf einem primären oder sekundären Knoten ausführen. Wählen Sie aus, auf welchem Knoten Sie den Job ausführen möchten.

      - **Auf primären Knoten ausführen** - Wählen Sie diese Option, um den Job nur auf primären Knoten auszuführen.
      - **Auf sekundären Knoten ausführen** - Wählen Sie diese Option, um den Job nur auf sekundären Knoten auszuführen.

   Sie können auch sowohl den primären als auch den sekundären Knoten auswählen, um denselben Konfigurationsauftrag auszuführen. Wenn Sie keinen primären oder sekundären Knoten auswählen, wird der Konfigurationsauftrag automatisch auf dem primären Knoten ausgeführt.

6. Auf der Registerkarte**Variablenwerte angeben** stehen Ihnen zwei Optionen zur Verfügung:

   a) Laden Sie die Eingabedatei herunter, um die Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den NetScaler ADM Server hoch.

   b) Geben Sie gemeinsame Werte für die Variablen ein, die Sie für alle Instanzen definiert haben

   c) Klicken Sie auf **Weiter**.

So senden Sie eine E-Mail und eine Slack Benachrichtigung für einen Job:

Eine E-Mail- und Slack-Benachrichtigung wird jetzt jedes Mal gesendet, wenn ein Job ausgeführt oder geplant wird. Die Benachrichtigung enthält Details wie den Erfolg oder Misserfolg des Auftrags sowie die relevanten Details.

1. Navigieren Sie zu **Netzwerke**>**Konfigurationsaufträge**.
2. Wählen Sie den Job aus, den Sie E-Mail- und Slack -Benachrichtigung aktivieren möchten, und klicken Sie auf **Bearbeiten**.

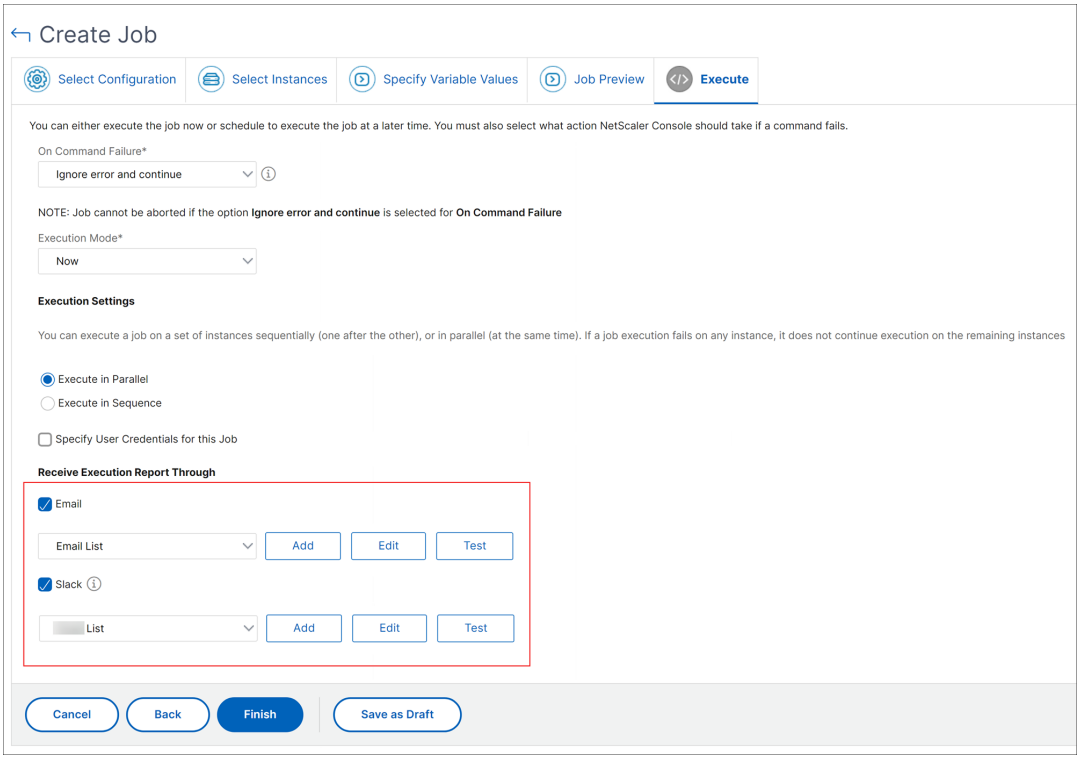
3. Wechseln Sie auf der Registerkarte **Ausführen** zum Bereich **Ausführungsbericht empfangen über** :

   - Aktivieren Sie das Kontrollkästchen **E-Mail** und wählen Sie die E-Mail-Verteilerliste aus, an die Sie den Ausführungsbericht senden möchten.

     Wenn Sie eine E-Mail-Verteilerliste hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie die E-Mail-Serverdetails an.

   - Aktivieren Sie das Kontrollkästchen **Slack** und wählen Sie den Slack-Kanal aus, an den Sie den Ausführungsbericht senden möchten.

     Wenn Sie ein Slack -Profil hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie den **Profilnamen**, den **Kanalnamen** und das **Token** des erforderlichen Slack-Kanals an.



4. Klicken Sie auf **Fertig stellen**.

So senden Sie eine E-Mail und eine Slack Benachrichtigung für einen Job:

Eine E-Mail- und Slack-Benachrichtigung wird jetzt jedes Mal gesendet, wenn ein Job ausgeführt oder geplant wird. Die Benachrichtigung enthält Details wie den Erfolg oder Misserfolg des Auftrags sowie die relevanten Details.

1. Navigieren Sie zu **Netzwerke**>**Konfigurationsaufträge**.
2. Wählen Sie den Job aus, den Sie E-Mail- und Slack -Benachrichtigung aktivieren möchten, und klicken Sie auf **Bearbeiten**.

3. Wechseln Sie auf der Registerkarte **Ausführen** zum Bereich **Ausführungsbericht empfangen über** :

    - Aktivieren Sie das Kontrollkästchen **E-Mail** und wählen Sie die E-Mail-Verteilerliste aus, an die Sie den Ausführungsbericht senden möchten.

      Wenn Sie eine E-Mail-Verteilerliste hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie die E-Mail-Serverdetails an.

    - Aktivieren Sie das Kontrollkästchen **Slack** und wählen Sie den Slack-Kanal aus, an den Sie den Ausführungsbericht senden möchten.

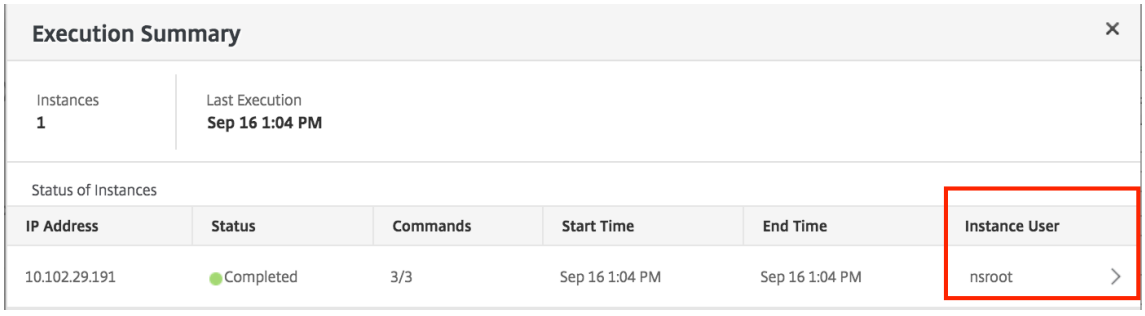
      Wenn Sie ein Slack -Profil hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie den **Profilnamen**, den **Kanalnamen** und das **Token** des erforderlichen Slack-Kanals an.

4. Klicken Sie auf **Fertig stellen**.

So zeigen Sie Details zur Ausführungszusammenfassung an:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**.
2. Wählen Sie den Job aus, den Sie die Ausführungszusammenfassung anzeigen möchten, und klicken Sie auf **Details**.
3. Klicken Sie auf **Ausführungsübersicht**, um Folgendes anzuzeigen:

    - Der Status der Instanz, bei der der Auftrag ausgeführt wird
    - Die Befehle werden für den Auftrag ausgeführt
    - Die Start- und Endzeit des Auftrags und
    - Der Name des Instanzbenutzers



Aufzeichnung und Wiedergabe zum Erstellen von Konfigurationsaufträgen verwenden

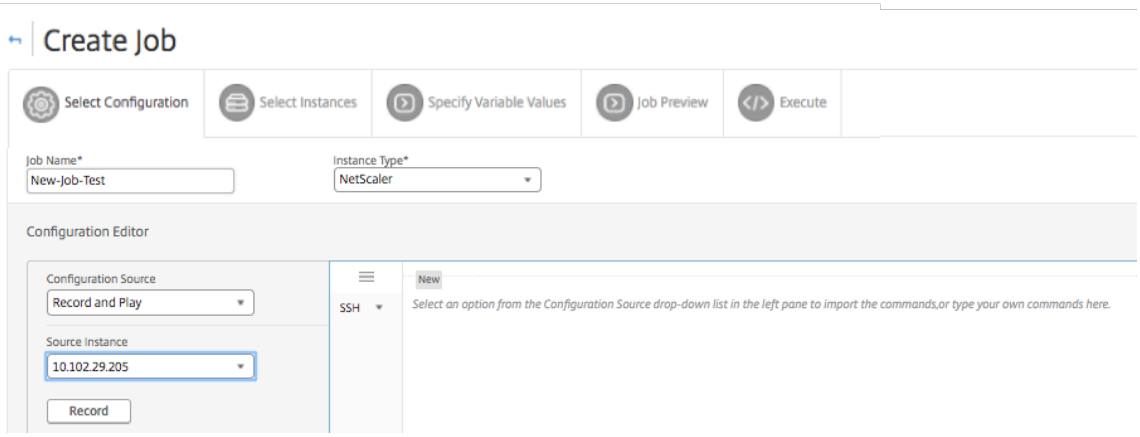
February 5, 2024

Wenn Sie es gewohnt sind, die NetScaler ADC GUI zum Konfigurieren einer NetScaler ADC-Instanz zu verwenden, kann es manchmal schwierig sein, die genauen CLI-Befehle abzurufen, um eine Konfigurationsaufgabe zu erstellen und sie auf mehreren NetScaler ADC-Instanzen auszuführen.

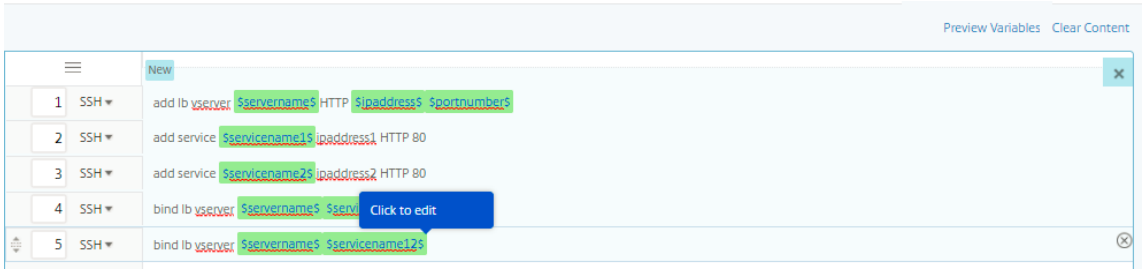
Mit NetScaler ADM können Sie die Konfigurationsaufgaben aufzeichnen, die mit der GUI einer NetScaler ADC-Instanz ausgeführt wurden, und sie in CLI-Befehle konvertieren. Sie können dann aus diesen CLI-Befehlen eine Konfigurationsaufgabe erstellen und diesen Task auf mehreren Instanzen ausführen.

So zeichnen Sie die GUI-Konfiguration auf und konvertieren sie in eine Konfigurationsaufgabe

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**, und klicken Sie dann auf **Job erstellen**.
2. Geben Sie den Jobnamen und den Instanztyp an.
3. Wählen Sie in der Liste **Konfigurationsquelle** die Option **Aufzeichnen und wiedergeben**aus, und wählen Sie dann die Quellinstanz aus, von der Sie die Konfiguration aufzeichnen möchten. Klicken Sie auf **Aufzeichnen**.

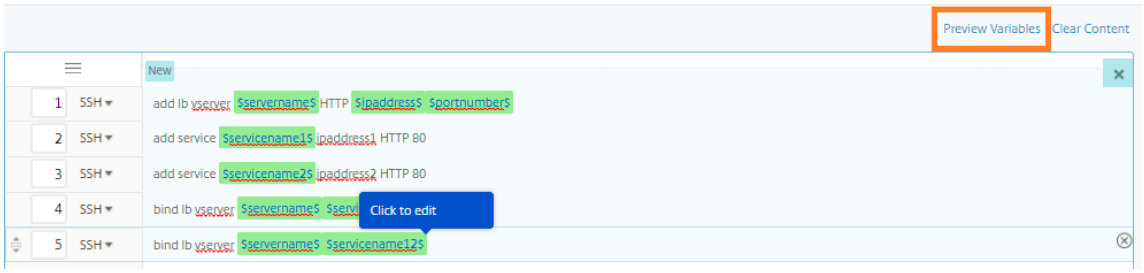


4. Die **NetScaler ADC GUI** wird geöffnet. Konfigurieren Sie die Features und Einstellungen, die die Konfigurationsaufgabe enthalten soll. Schließen Sie dann das NetScaler ADC GUI-Fenster und klicken Sie im **Konfigurationseditor** auf **Stopp**. Die Befehle werden im linken Fensterbereich als Link angezeigt. Ziehen Sie die Befehle in den rechten Bereich und klicken Sie dann auf **Weiter**.

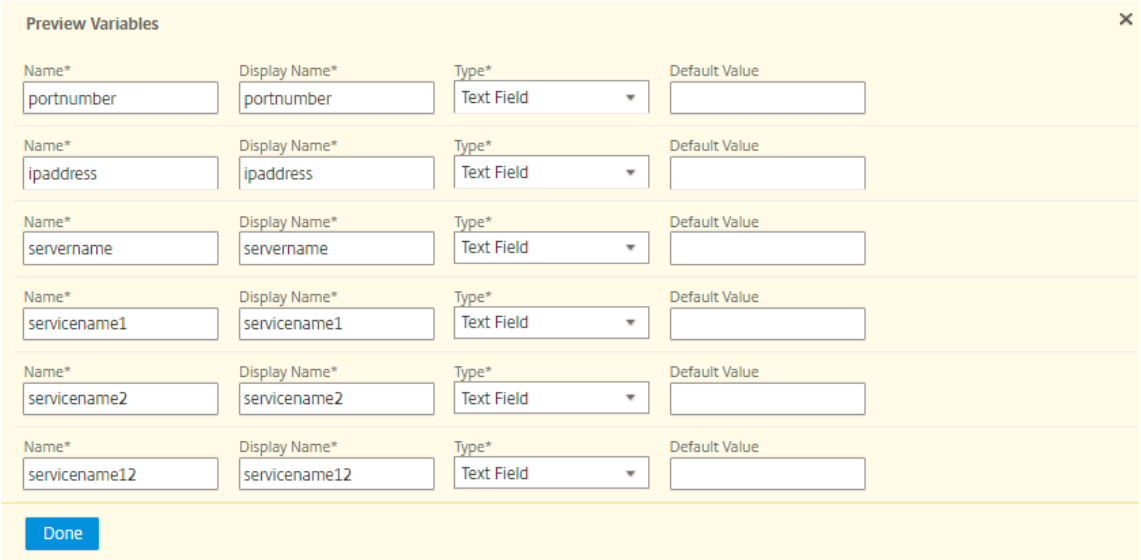


Anschließend können Sie die Befehle im Konfigurationseditor neu anordnen und neu anordnen. Sie können den Befehl von einer Zeile in eine andere verschieben, indem Sie die Befehlszeile ziehen und dort ablegen. Sie können die Befehlszeile auch von einer Zeile zu einer beliebigen Zielzeile verschieben oder neu anordnen, indem Sie einfach die Befehlszeilennummer im Textfeld ändern.

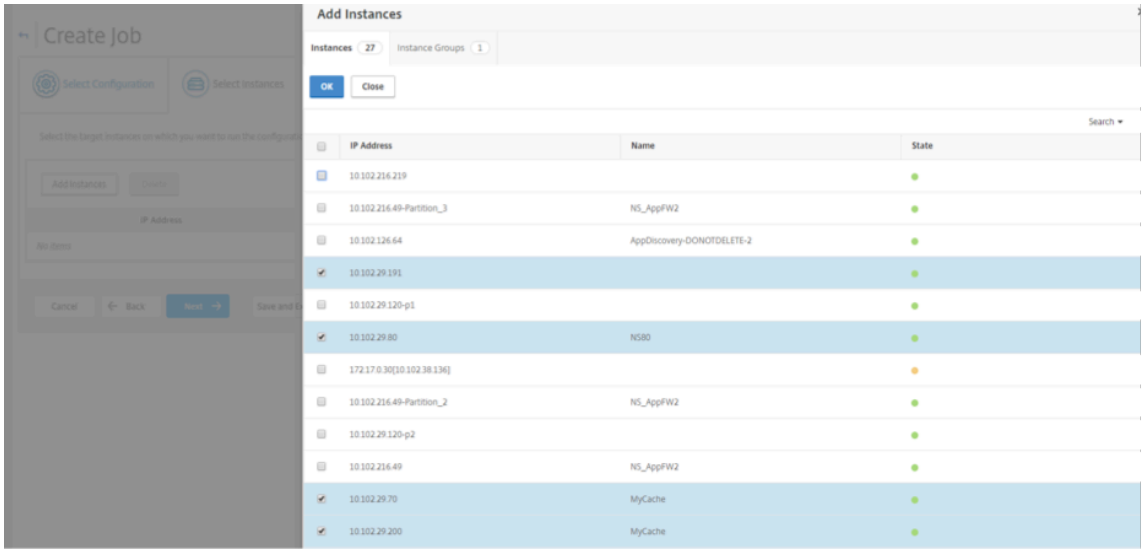
5. Sie können alle Variablen überprüfen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags in einer einzigen konsolidierten Ansicht definiert haben.
6. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:
   - Navigieren Sie beim Erstellen eines Konfigurationsauftrags zu **Netzwerke > Konfigurationsaufträge** und wählen Sie **Job erstellen** aus. Auf der Seite **Job erstellen** können Sie alle Variablen überprüfen, die Sie beim Erstellen des Konfigurationsauftrags hinzugefügt haben.
   - Während Sie einen Konfigurationsauftrag bearbeiten, navigieren Sie zu **Netzwerk > Konfigurationsjobs**, wählen Sie den Job-Namen aus und klicken Sie auf **Bearbeiten**. Auf der Seite **Job konfigurieren** können Sie alle Variablen überprüfen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.
7. Sie können dann auf die Registerkarte **Vorschauvariablen** klicken, um eine Vorschau der Variablen in einer einzelnen konsolidierten Ansicht anzuzeigen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben.



8. Ein neues Popup-Fenster wird angezeigt, in dem alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem tabellarischen Format angezeigt werden. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Fertig**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.



9. Klicken Sie auf**Instanzen hinzufügen**, und wählen Sie die Instanzen aus, auf denen Sie den Konfigurationsauftrag ausführen möchten. Klicken Sie auf**OK**, und klicken Sie dann auf**Weiter**.



10. Wenn Sie Variablen in den Befehlen angegeben haben, wählen Sie auf der Registerkarte**Variablenwerte angeben**eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:

    - **** Eingabedatei für Variablenwerte hochladen: ** Klicken Sie auf Eingabeschlüsseldatei herunterladen, um eine Eingabedatei herunterzuladen. Geben Sie in der Eingabedatei Werte für die Variablen ein, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den NetScaler ADM Server hoch.
    - **Gemeinsame Variablenwerte für alle Instanzen**: Geben Sie Werte für die Variablen ein. Die Variablen variieren je nach ausgewählter Vorlage.

    Die Eingabedateien, die die Variablenwerte enthalten, werden in den Konfigurationsaufträ-

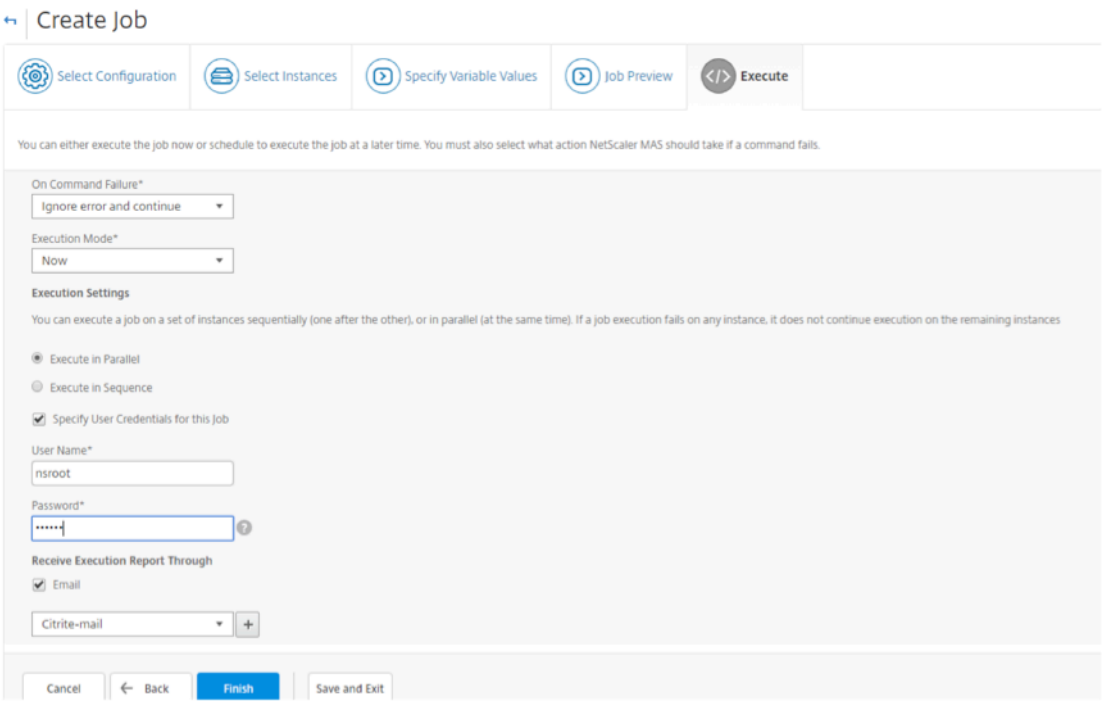
gen beibehalten (mit demselben Dateinamen). Sie können diese Eingabedateien anzeigen und bearbeiten, die Sie früher beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben.

Um die Ausführungskonfigurationsaufträge beim Erstellen eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk > Konfigurationsaufträge**, und klicken Sie auf **Job erstellen**. Auf der Seite **Job erstellen**. Wählen Sie auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

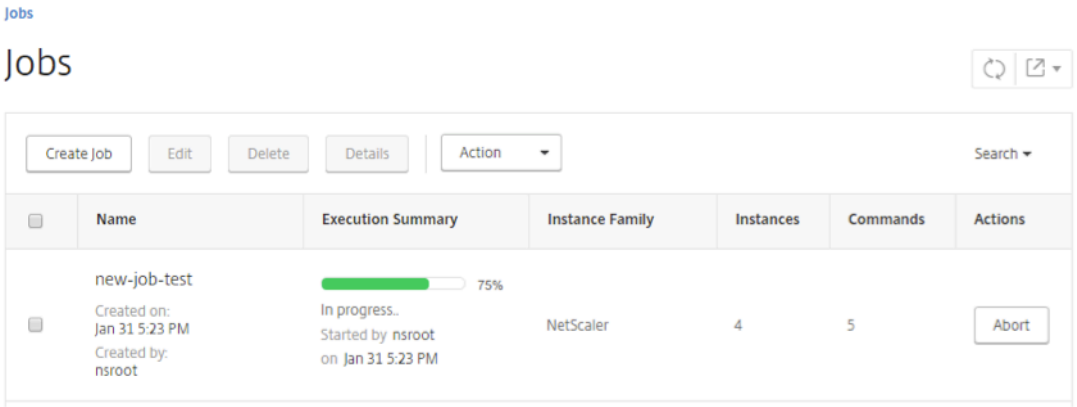
Um die bereits ausgeführten Konfigurationsaufträge beim Bearbeiten eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk > Konfigurationsaufträge**, wählen Sie den Auftragsnamen aus und klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite **Job konfigurieren** auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten Sie die Dateien und laden sie hoch (unter Beibehaltung des gleichen Dateinamens) .10.Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.

11. Auf der Registerkarte**Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.
12. Auf der Registerkarte**Ausführen**können Sie wählen, ob Sie Ihren Job jetzt ausführen oder planen, dass er später ausgeführt wird. Sie können auch auswählen, welche Aktion NetScaler ADM ausführen muss, wenn der Befehl fehlschlägt.

    Sie können auch autorisierten Benutzern erlauben, Aufträge auf Ihren verwalteten Instanzen auszuführen, und Sie können wählen, ob Sie eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Auftrags zusammen mit anderen Details senden möchten.



13. Auf der Seite **Jobs** können Sie dann den Fortschritt der Ausführung der Konfigurationsaufgabe für alle Instanzen anzeigen.



Konfigurationsaufträge zum Replizieren der Konfiguration von einer Instanz auf mehrere Instanzen verwenden

February 5, 2024

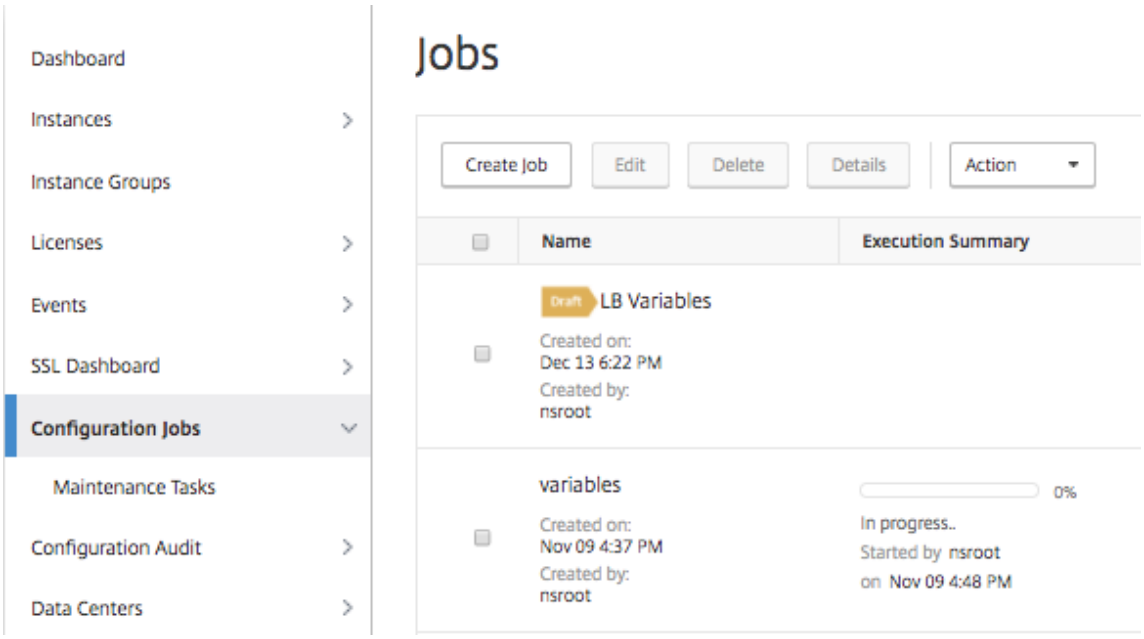
Sie können die Funktion Configuration Jobs von Citrix ADM verwenden, um eine bestimmte Konfiguration aus einer Citrix ADC-Instanz zu extrahieren und auf mehreren Instanzen zu replizieren.

Beispielsweise haben Sie möglicherweise sowohl Load Balancing als auch Front-End-Optimierung

(FEO) auf einer Citrix ADC-Instanz für Ihre Bereitstellung konfiguriert. Jetzt möchten Sie jedoch nur die FEO-Konfiguration auf andere Citrix ADC-Instanzen replizieren.

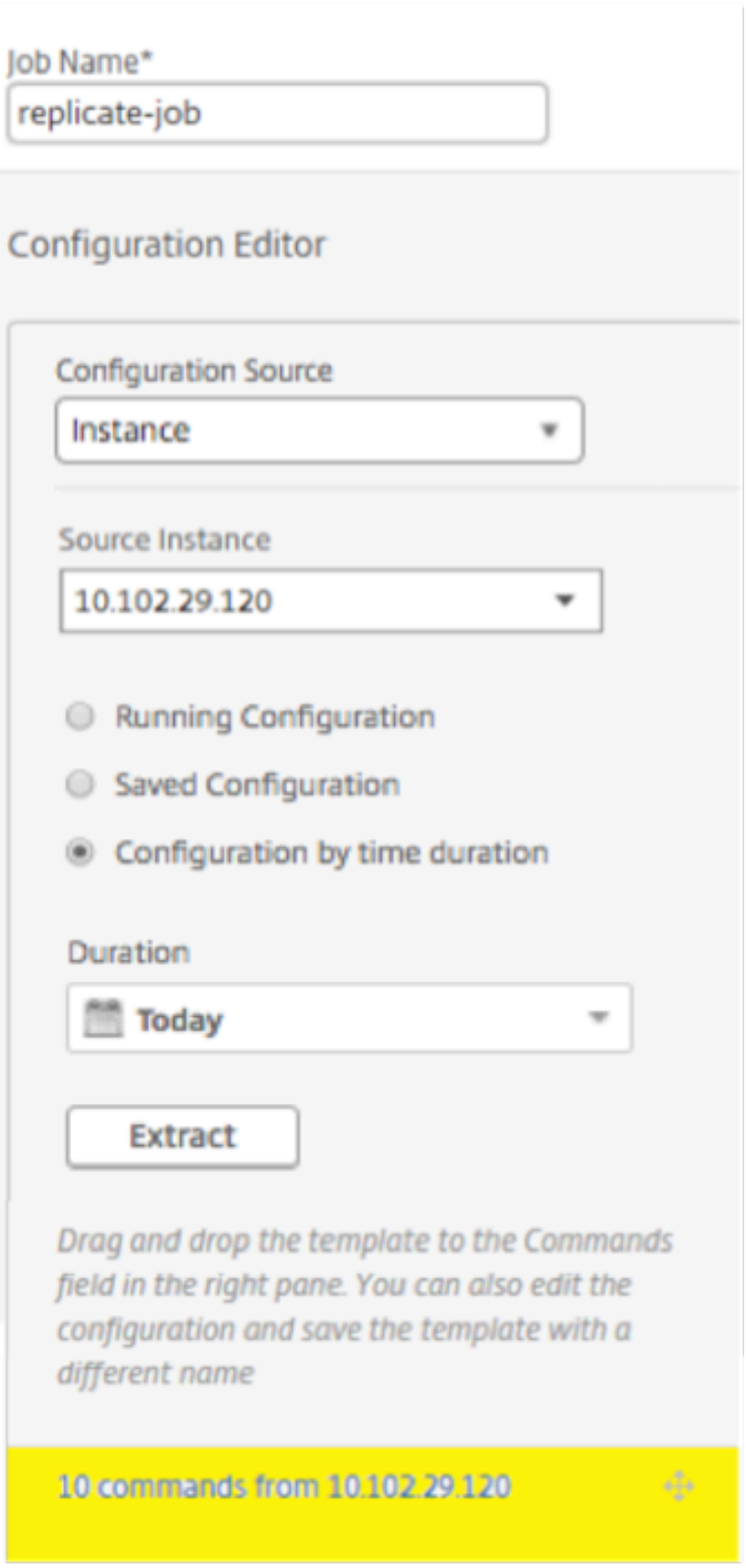
So rufen Sie die Konfiguration von einer Instanz auf andere NetScaler ADC-Instanzen ab und replizieren sie:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**, und klicken Sie dann auf **Job erstellen**.



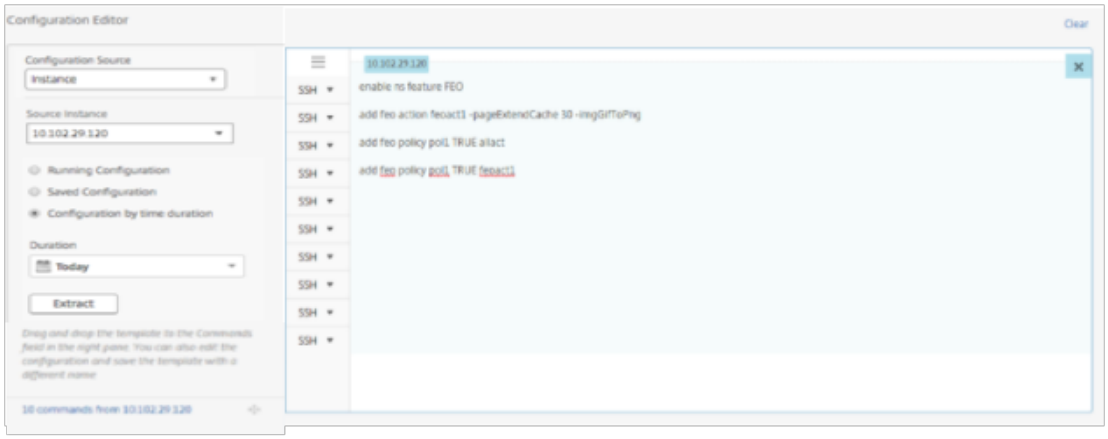
2. Geben Sie den Jobnamen und den Instanztyp an.
3. Wählen Sie **Instanz** als **Konfigurationsquelle** und wählen Sie die Quellinstanz aus, deren Konfiguration Sie replizieren möchten. Wählen Sie die Art der Konfiguration aus, die Sie extrahieren möchten. Wenn Sie die Option "Konfiguration nach Zeitdauer"auswählen, legen Sie den Zeitraum fest, in dem Sie diese Konfiguration ausgeführt haben, und klicken Sie dann auf **Extrahieren**.

   Die Anzahl der Befehle, die auf dieser Instanz in der von Ihnen ausgewählten Zeitdauer ausgeführt werden, wird auf dem Bildschirm angezeigt, wie in der folgenden Abbildung hervorgehoben.



4. Ziehen Sie die Befehle in das Feld **Befehle** im rechten Fensterbereich.

Behalten Sie nur die Befehle im Zusammenhang mit FEO bei und löschen Sie manuell die Befehle für den Lastenausgleich oder Befehle, die sich auf eine andere Konfiguration beziehen, und klicken Sie dann auf **Weiter**.



5. Klicken Sie auf **Instanzen hinzufügen**, und fügen Sie die Instanzen hinzu, auf die Sie die FEO-Konfiguration anwenden möchten. Klicken Sie auf **OK**und dann auf **Weiter**.
6. **Wenn Sie in den Befehlen Variablen angegeben haben, klicken Sie auf der Registerkarte Variablenwerte angeben auf Eingabeschlüsseldatei herunterladen** . Geben Sie in der heruntergeladenen Datei Werte für die Variablen an und laden Sie die Datei dann in NetScaler ADM hoch.
7. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.
8. Klicken Sie auf der Registerkarte **Execute** auf **Finish**, um den Job auf den ausgewählten NetScaler ADC-Instanzen auszuführen.

Variablen in Konfigurationsaufträgen verwenden

February 5, 2024

Ein Konfigurationsauftrag besteht aus einer Reihe von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Wenn Sie dieselbe Konfiguration auf mehreren Instanzen ausführen, möchten Sie möglicherweise andere Werte für die in Ihrer Konfiguration verwendeten Parameter verwenden. Sie können Variablen definieren, mit denen Sie verschiedene Werte für diese Parameter zuweisen oder einen Auftrag über mehrere Instanzen ausführen können.

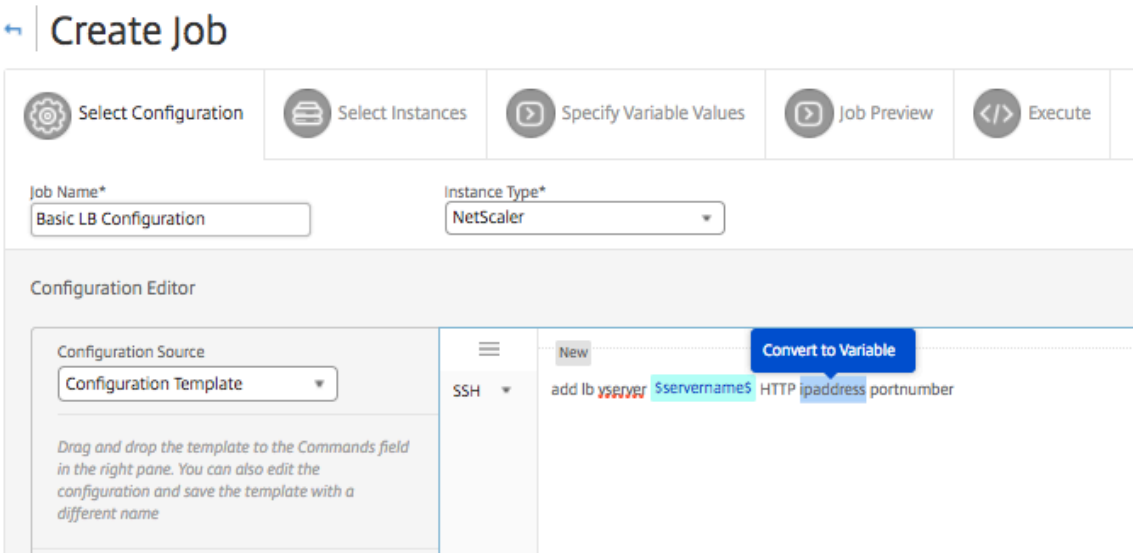
Betrachten Sie beispielsweise eine grundlegende Lastausgleichskonfiguration, bei der Sie einen virtuellen Lastausgleichsserver hinzufügen, zwei Dienste hinzufügen und die Dienste an den virtuellen Server binden. Jetzt möchten Sie möglicherweise dieselbe Konfiguration auf zwei Instanzen haben, jedoch mit unterschiedlichen Werten für die Namen und IP-Adressen des virtuellen Servers und der Dienste. Sie können die Konfigurationsaufträge verwenden, um dies zu erreichen, indem Sie Variablen verwenden, um die Namen und IP-Adressen des virtuellen Servers und der Dienste zu definieren.

In diesem Beispiel werden die folgenden Befehle und Variablen verwendet:

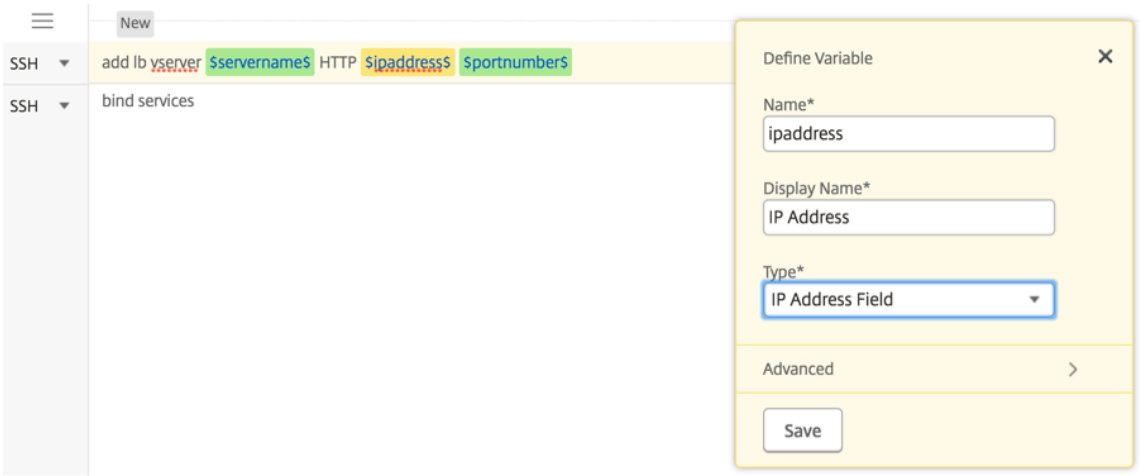
```
add lb vserver <servername> HTTP <ipaddress> <portnumber>

add service <servicename1> <ipaddress1> HTTP 80

add service <servicename2> <ipaddress2> HTTP 80

bind lb vserver <servername> <servicename1>

bind lb vserver <servername> <servicename2>
```

So erstellen Sie einen Konfigurationsauftrag durch Definieren von Variablen in NetScaler ADM:

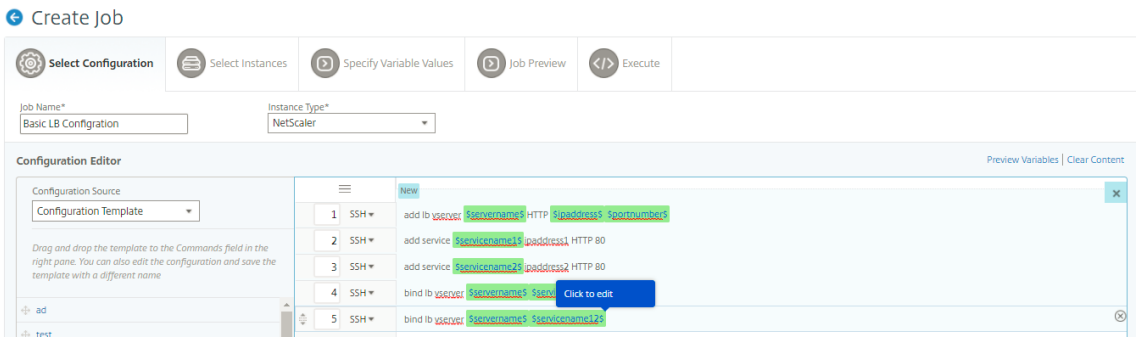
1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**.
2. Klicken Sie auf **Job erstellen**.
3. Wählen Sie auf der Seite **Job erstellen** die benutzerdefinierten Job-Parameter wie den Namen des Jobs, den Instanztyp und den Konfigurationstyp aus.
4. Geben Sie im Konfigurationseditor die Befehle ein, um einen virtuellen Lastausgleichsserver, zwei Dienste hinzuzufügen und die Dienste an den virtuellen Server zu binden. Doppelklicken Sie, um die Werte auszuwählen, die Sie in eine Variable konvertieren möchten, und klicken Sie dann **auf In Variable umwandeln**. Wählen Sie beispielsweise die IP-Adresse des Load Balancing-Servers aus und klicken Sie auf In **Variable umwandeln** *`ipaddress`*, wie in der folgenden Abbildung gezeigt.



5. Wenn Sie sehen, dass Dollarzeichen den Wert der Variablen einschließen, klicken Sie auf die Variable, um die Details der Variablen wie Name, Anzeigename und Typ anzugeben. Sie können auch auf die Option **Erweitert** klicken, wenn Sie einen Standardwert für Ihre Variable weiter angeben möchten. Klicken Sie auf **Speichern**, und klicken Sie dann auf **Weiter**.



Geben Sie die restlichen Befehle ein und definieren Sie alle Variablen.



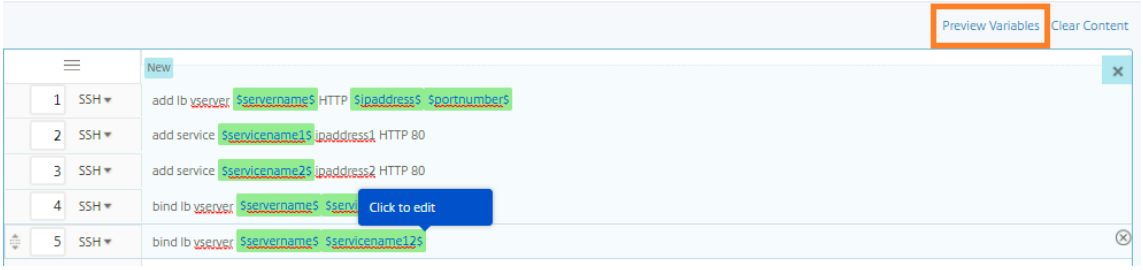
6. Sie können alle Variablen überprüfen, die Sie beim Erstellen oder Bearbeiten eines Konfigura-

tionsauftrags in einer einzigen konsolidierten Ansicht definiert haben.

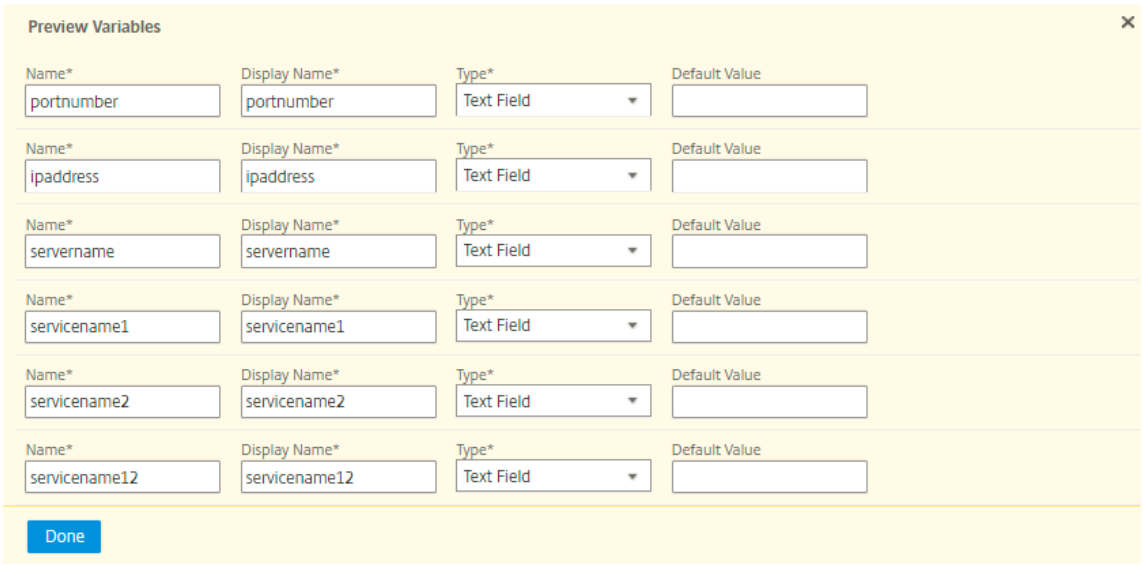
7. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:

   - Navigieren Sie beim Erstellen eines Konfigurationsauftrags zu **Netzwerke > Konfigurationsaufträge** und wählen Sie **Job erstellen** aus. Auf der Seite **Job erstellen** können Sie alle Variablen überprüfen, die Sie beim Erstellen des Konfigurationsauftrags hinzugefügt haben.
   - Während Sie einen Konfigurationsauftrag bearbeiten, navigieren Sie zu **Netzwerk > Konfigurationsjobs**, wählen Sie den Job-Namen aus und klicken Sie auf **Bearbeiten**. Auf der Seite **Job konfigurieren** können Sie alle Variablen überprüfen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.

8. Sie können dann auf die Registerkarte **Vorschauvariablen** klicken, um eine Vorschau der Variablen in einer einzelnen konsolidierten Ansicht anzuzeigen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben.



9. Ein neues Popup-Fenster wird angezeigt, in dem alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem tabellarischen Format angezeigt werden. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Fertig**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.

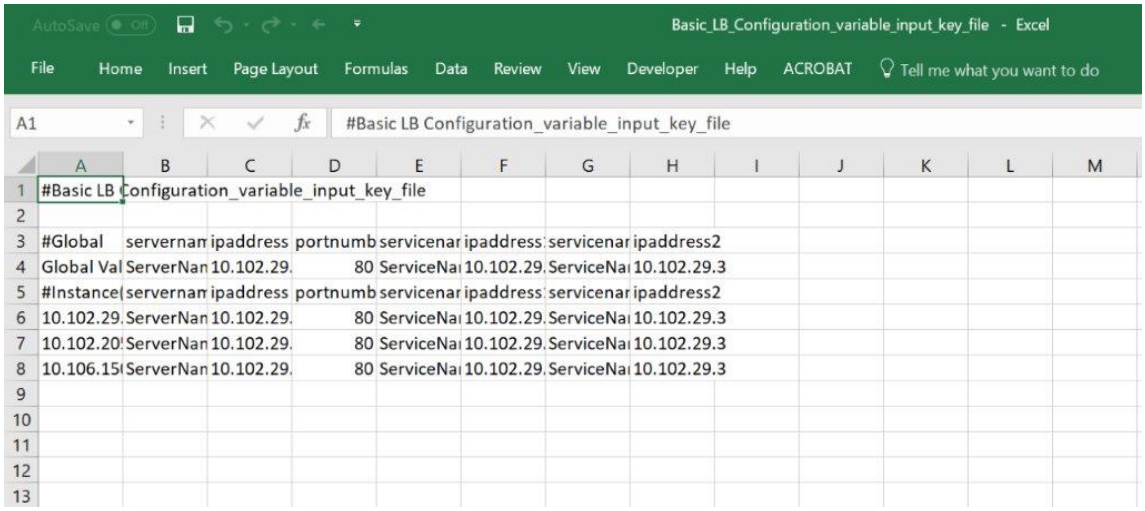


10. Anschließend können Sie die Befehle im Konfigurationseditor neu anordnen und neu anordnen. Sie können den Befehl von einer Zeile in eine andere verschieben, indem Sie die Befehlszeile ziehen und dort ablegen. Sie können die Befehlszeile auch von einer Zeile zu einer beliebigen Zielzeile verschieben oder neu anordnen, indem Sie einfach die Befehlszeilennummer im Textfeld ändern.
11. Wählen Sie die Instanzen aus, auf denen Sie den Konfigurationsauftrag ausführen möchten.
12. Wählen Sie auf der Registerkarte **Variablenwerte angeben** die Option **Eingabedatei für Variablenwerte hochladen** aus und klicken Sie dann auf **Eingabeschlüsseldatei herunterladen**. In unserem Beispiel müssen Sie den Servernamen auf jeder Instanz, die IP-Adressen des Servers und der Dienste, Portnummern und Dienstnamen angeben. Speichern Sie die Datei und laden Sie sie hoch. Wenn Ihre Werte nicht genau definiert sind, kann das System einen Fehler auslösen.
13. Die Eingabeschlüsseldatei wird auf Ihr lokales System heruntergeladen und Sie können sie bearbeiten, indem Sie die Variablenwerte für jede zuvor ausgewählte Citrix ADC-Instanz angeben und auf **Hochladen** klicken, um die Eingabeschlüsseldatei auf Citrix ADM hochzuladen. Klicken Sie auf **Weiter**. Die Eingabeschlüsseldatei wird in Ihr lokales System heruntergeladen und Sie können sie bearbeiten, indem Sie die Variablenwerte für jede zuvor ausgewählte NetScaler ADC-Instanz angeben.

    > **Hinweis** In der Eingabeschlüsseldatei werden die Variablen auf drei Ebenen definiert:
    >
    > - Globales Niveau
    > - Instanzgruppen-Ebene
    > - Instanz-Ebene

    Globale Variablen sind Variablenwerte, die auf alle Instanzen angewendet werden. Variablenwerte auf Instanzgruppenebene werden auf alle Instanzen angewendet, die in einer Gruppe definiert sind. Variablenwerte auf Instanzebene werden nur auf eine bestimmte Instanz angewendet.

    NetScaler ADM räumt Werten auf Instanzebene erste Priorität ein. Wenn für die Variablen für einzelne Instanzen keine Werte bereitgestellt werden, verwendet NetScaler ADM den auf Gruppenebene bereitgestellten Wert. Wenn auf Gruppenebene keine Werte bereitgestellt werden, verwendet NetScaler ADM den auf globaler Ebene bereitgestellten Variablenwert. Wenn Sie eine Eingabe für eine Variable über alle drei Ebenen hinweg bereitstellen, verwendet NetScaler ADM den Wert der Instanzebene als Standardwert.
14. Klicken Sie auf **Hochladen**, um die Eingabeschlüsseldatei auf Citrix ADM hochzuladen. Klicken Sie auf **Weiter**.



> **Wichtig!**
>
> Wenn Sie eine CSV-Datei von einem Mac hochladen, speichert der Mac die CSV-Datei mit Semikolons anstelle von Kommas. Dies führt dazu, dass die Konfiguration fehlschlägt, wenn Sie die Eingabedatei hochladen und den Auftrag ausführen. Wenn Sie einen Mac verwenden, verwenden Sie einen Texteditor, um die erforderlichen Änderungen vorzunehmen und dann die Datei hochzuladen.

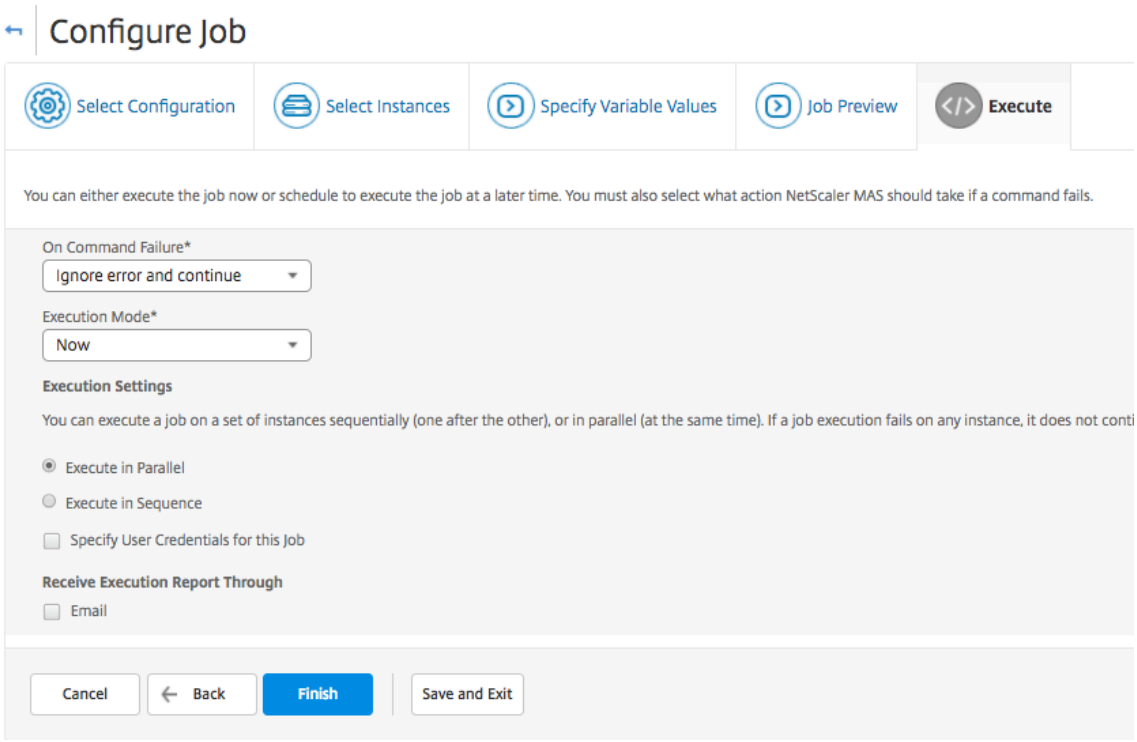
15. Sie können auch gemeinsame Variablenwerte für alle Instanzen angeben und auf **Hochladen** klicken, um die Eingabeschlüsseldatei auf Citrix ADM hochzuladen.

    Die wichtigsten Eingabedateien, die die Variablenwerte enthalten, werden in den Konfigurationsjobs beibehalten (mit demselben Dateinamen). Sie können diese Eingabedateien anzeigen und bearbeiten, die Sie früher beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben.

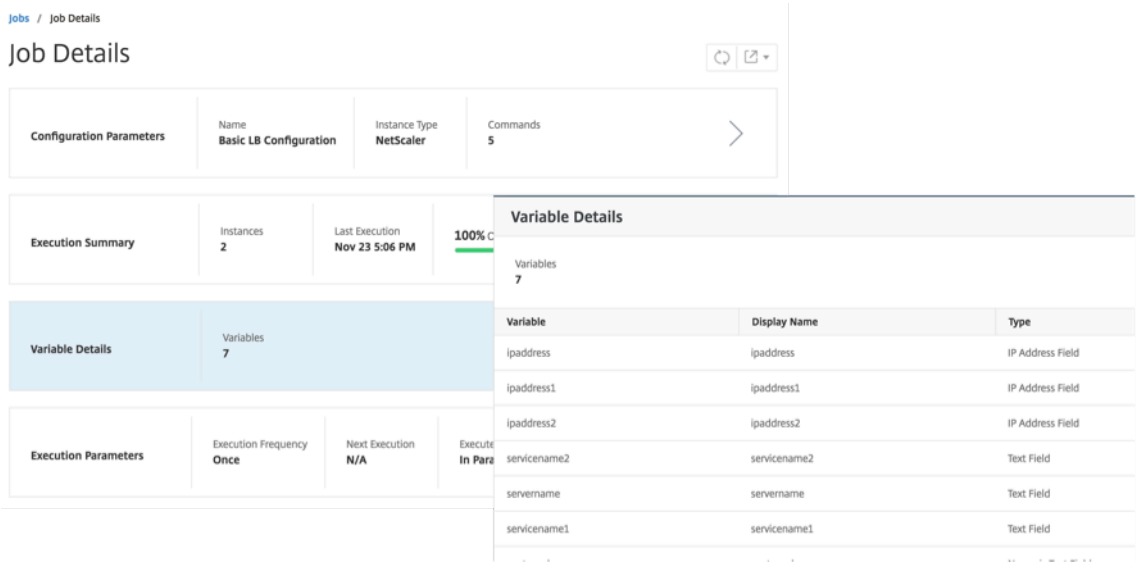
    Um die Ausführungskonfigurationsaufträge beim Erstellen eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk > Konfigurationsaufträge**, und klicken Sie auf **Job erstellen**. Auf der Seite **Job erstellen**. Wählen Sie auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

    Um die bereits ausgeführten Konfigurationsaufträge beim Bearbeiten eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk > Konfigurationsaufträge**, wählen Sie den Auftragsnamen aus und klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite **Job konfigurieren** auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

16. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.
17. Auf der Registerkarte "**Ausführen** "können Sie Ihren Job jetzt ausführen oder planen, dass er zu einem späteren Zeitpunkt ausgeführt wird. Sie können auch auswählen, welche Aktion NetScaler ADM ausführen muss, wenn der Befehl fehlschlägt und Sie eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Jobs zusammen mit anderen Details senden möchten.



Nachdem Sie Ihre Jobs konfiguriert und ausgeführt haben, können Sie die Auftragsdetails anzeigen, indem Sie zu **Netzwerke** > **Konfigurationsaufträge** navigieren und den gerade konfigurierten Job auswählen. Klicken Sie auf **Details** und dann auf **Variablendetails**, um die Liste der Variablen anzuzeigen, die Ihrem Job hinzugefügt wurden.



> **Hinweis**
>
> Die Werte, die Sie in **SCHRITT 5** für die Variablen angegeben haben, werden von Citrix ADM beibehalten, wenn Sie den Job speichern und beenden oder wenn Sie einen Job für die Ausführung zu einem späteren Zeitpunkt planen.

Konfigurationsaufträgen aus Korrekturbefehlen erstellen

February 5, 2024

Sie können die Überwachungsvorlagenfunktion in NetScaler Application Delivery Management (ADM) verwenden, um Konfigurationsänderungen über verwaltete NetScaler ADC-Instanzen hinweg zu überwachen und Konfigurationsfehler zu beheben.

Der typische Arbeitsablauf für die Prüfung von Konfigurationsänderungen mithilfe von Prüfvorlagen besteht aus den folgenden Schritten:

1. Erstellen Sie eine Prüfungsvorlage mit einer Reihe gültiger/erwarteter Citrix ADC-Befehle für die Prüfung von Instanzkonfigurationen.
2. Wählen Sie die NetScaler ADC-Instanzen aus, für die Sie die Überwachungsvorlage ausführen möchten, um auf Unterschiede zwischen der laufenden Konfiguration und den erwarteten Konfigurationen zu überprüfen.
3. Machen Sie sich mit den Differential-/Korrekturbefehlen vertraut und nutzen Sie die Funktion „Job erstellen“, um die Konfigurationen der Instanz in den gewünschten Zustand zu bringen

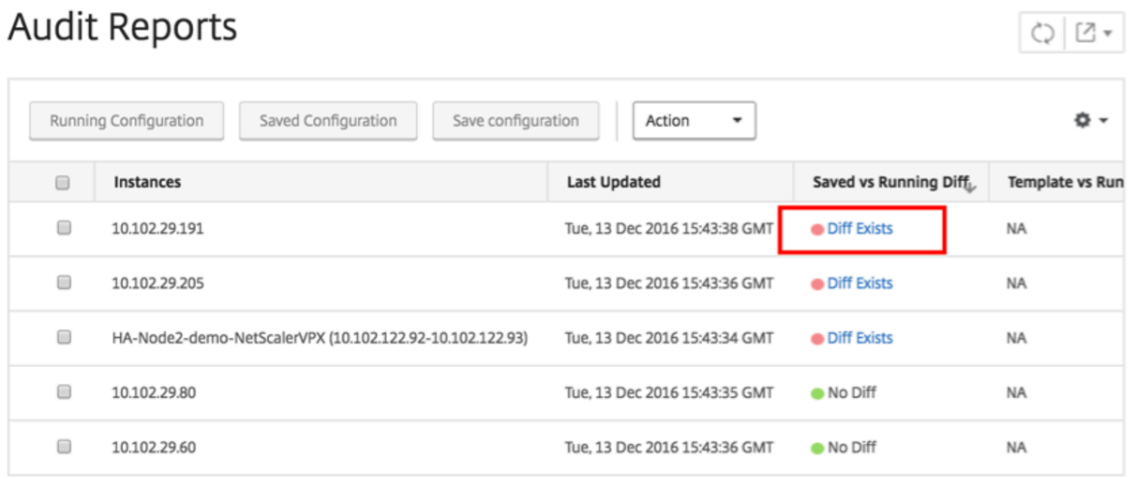
Betrachten Sie ein Szenario, in dem mehrere Administratoren fünf NetScaler ADC-Instanzen verwalten. Alle diese Administratoren nehmen Aktualisierungen an der vorhandenen Instanzkonfiguration vor, wenn Änderungen erforderlich sind. Der Superadministrator möchte sicherstellen, dass ein bestimmter Satz wichtiger Konfigurationen unabhängig von den Änderungen, die von anderen Administratoren vorgenommen werden, unberührt bleibt. Für diesen Anwendungsfall erstellt der Superadministrator eine Vorlage der Konfiguration, die voraussichtlich auf den Citrix ADC-Instanzen vorhanden sein wird, und führt sie für die Instanzen aus. NetScaler ADM vergleicht die Überwachungsvorlagenkonfiguration mit der ausgeführten Konfiguration und meldet eventuelle Abweichungen im Dashboard **Configuration Audit**.

Wenn Sie feststellen, dass sich die Konfiguration einiger Instanzen ändert, können Sie die NetScaler ADM-Korrekturbefehle verwenden, um einen Konfigurationsauftrag mit den geänderten und korrigierten Konfigurationsbefehlen für bestimmte NetScaler ADC-Instanzen zu erstellen.

Wenn zwischen der Konfiguration der Überwachungsvorlage und der ausgeführten Konfiguration ein Unterschied besteht, wird auf der Seite “**Audit-Bericht** “eine Statusmeldung “**Diff Exists** “angezeigt. Wenn Sie auf den Link “**Diff beendet** “klicken, gelangen Sie zur Seite “**Konfigurationsdiff** “, auf der Sie den Korrekturbefehl anzeigen können. Sie können diese fehlerbehebenden Befehle auch verwenden, um einen Konfigurationsauftrag zu erstellen und diesen auf den spezifischen NetScaler ADC-Instanzen auszuführen, um sie wieder in die gewünschte Konfiguration zu bringen.

So erstellen Sie einen Konfigurationsauftrag über Korrekturbefehle in NetScaler ADM

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaudit**.
2. Klicken Sie auf der Seite **Konfigurationsüberwachung** in eines der beiden Donutdiagramme, um die Seite **Überwachungsberichte** aufzurufen.
3. Klicken Sie auf den Link **Diff Exists** (in der Tabelle unter der Spalte **Gespeicherter vs. laufender Unterschied**) für die Instanz, für die Sie die Konfigurationsbefehle korrigieren möchten. Die Seite **Konfigurationsabweichung** wird angezeigt, auf der die Unterschiede zwischen der gespeicherten Konfiguration, der laufenden Konfiguration und der Korrekturkonfiguration für diese Instanz aufgeführt sind.



4. Klicken Sie auf **Job erstellen**, um zur Seite **Job erstellen** zu gehen, auf der die Korrekturbefehle bereits ausgefüllt wurden. Anweisungen zum Erstellen eines Konfigurationsauftrags finden Sie unter Erstellen eines Konfigurationsauftrags auf NetScaler ADM.

Laufende und gespeicherte Konfiguration von einer NetScaler ADC-Instanz auf eine andere replizieren

February 5, 2024

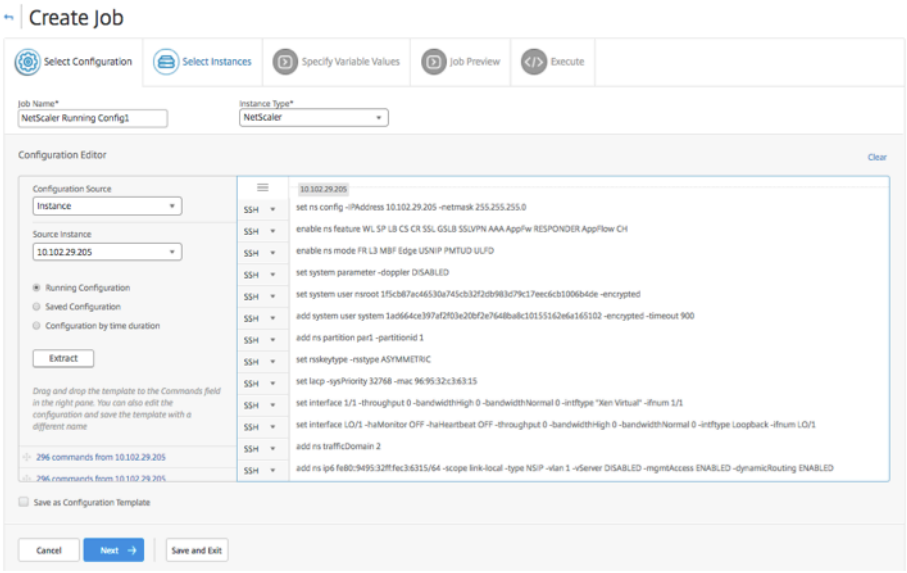
24. Mai 2018

Sie können jetzt die Konfiguration einer Citrix ADC-Instanz auf anderen Instanzen replizieren. Wenn Sie einen Auftrag in NetScaler ADM konfigurieren, wählen Sie eine Instanz als Konfigurationsquelle aus, und wählen Sie die ausgeführte oder gespeicherte Konfiguration der ausgewählten Instanz aus.

Wenn Sie beispielsweise **Laufende Konfiguration** auswählen und auf **Extrahieren** klicken, sendet NetScaler ADM eine Anforderung an die ausgewählte NetScaler ADC-Instanz, um die ausgeführte Konfiguration zu finden, und zeigt sie als Vorlage an. Sie können die Vorlage in das Feld **Befehle** im rechten Bereich ziehen. Sie können die Befehle, Parameter und Instanzen ändern.

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

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge** und klicken Sie auf **Job erstellen**.
2. Geben Sie den Jobnamen und den Instanztyp an. Geben Sie beispielsweise*Citrix ADC Running Config1* als Namen Ihres Jobs und den Instanztyp als *Citrix ADC*an.
3. Wählen Sie **Instanz** als **Konfigurationsquelle**, und wählen Sie die Quellinstanz aus, deren Konfiguration Sie auf anderen Instanzen replizieren möchten.
4. Sie sehen die folgenden drei Optionen:
   - Laufende Konfiguration
   - Konfiguration gespeichert
   - Konfiguration nach Zeitdauer
5. Wählen Sie **Konfiguration ausführen**und klicken Sie auf **Extrahieren**. Die Anzahl der ausgeführten Konfigurationsbefehle, die auf dieser Instanz ausgeführt werden, wird angezeigt.



6. Ziehen Sie die Befehle in das Feld **Befehle** im rechten Fensterbereich.
7. Sie können die Befehle im Feld Befehle bearbeiten. Wenn die extrahierten Befehle beispielsweise eine NetScaler ADC-Instanz einrichten sollen. Dies kann das Hinzufügen von Partitionen, das Einrichten des Lastenausgleichs, das Binden des Lastausgleichsservers an Dienste usw. umfassen. Vielleicht möchten Sie Ihre Befehle bearbeiten, um Ihre neuen NetScaler ADC-Instanzen

ohne Partitionen einzurichten. Um Partitionen zu entfernen, löschen Sie manuell Befehle im Zusammenhang mit der Erstellung von Partitionen und klicken Sie auf **Weiter**.

8. Klicken Sie auf **Instanzen hinzufügen** und fügen Sie die Instanzen hinzu, auf die Sie die ausgeführten Konfigurationsbefehle anwenden möchten. Klicken Sie auf **OK** und dann auf **Weiter**.
9. Wenn Sie in den Befehlen Variablen angegeben haben, klicken Sie auf der Registerkarte **Variablenwerte angeben** auf **Eingabeschlüsseldatei herunterladen**. Geben Sie in der heruntergeladenen Datei Werte für die Variablen an und laden Sie die Datei dann in NetScaler ADM hoch.
10. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.

11. Auf der Registerkarte "**Ausführen** "können Sie Ihren Job jetzt ausführen oder planen, dass er später ausgeführt wird. Sie können auch auswählen, welche Aktion NetScaler ADM ausführen muss, der Befehl schlägt fehl und wenn Sie eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Auftrags zusammen mit anderen Details senden möchten.

Wiederverwendung von Ausführungsaufträgen

February 5, 2024

Mit Konfigurationsaufträgen können Sie eine Reihe von Konfigurationsbefehlen erstellen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Sie können denselben Satz gespeicherter Konfigurationsaufträge auch ausführen, nachdem Sie die Befehle, Parameter, Konfigurationsquelle und Instanzen im Auftrag geändert haben. Dies ist nützlich, wenn dieselben Befehlssätze auf einer anderen Instanz ausgeführt werden müssen oder wenn der Job auf einen Fehler trifft und die weitere Ausführung stoppt.

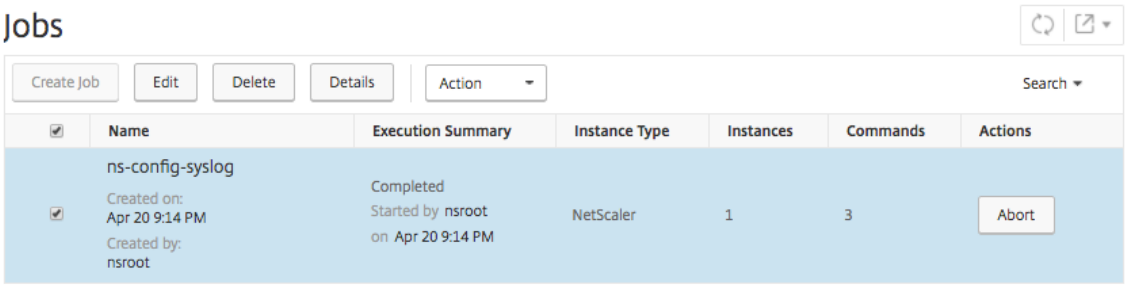
NetScaler Application Delivery Management (ADM) bietet eine Funktion zum erneuten Ausführen der abgeschlossenen Aufträge. Mit dieser Funktion können Jobs, die vollständig ausgeführt werden, erneut ausgeführt werden, ohne den Jobnamen zu ändern.

> **Hinweis:** Sie können nur die Jobs erneut ausführen, die ausgeführt werden, wenn der Ausführungsmodus "Jetzt"ist.

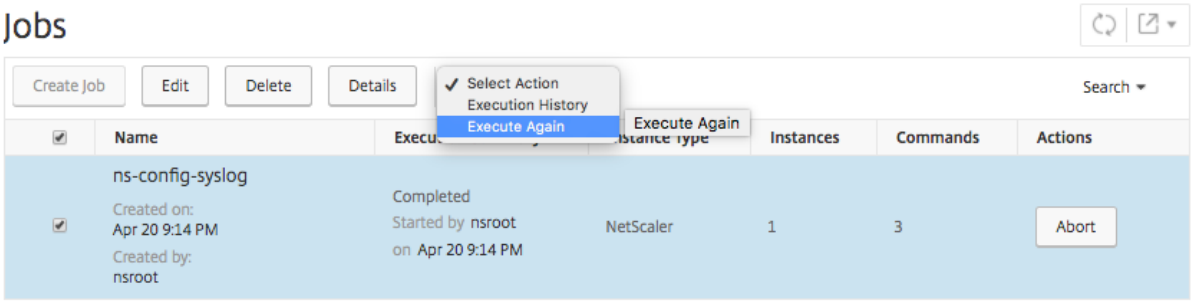
So bearbeiten Sie abgeschlossene Aufträge:

1. Navigieren Sie von der NetScaler ADM-Homepage zu **Netzwerke > Konfigurationsjobs**.
2. Wählen Sie auf der Seite **Jobs** einen Job aus, der die Ausführungsübersicht als abgeschlossen anzeigt, und klicken Sie auf **Bearbeiten**. Sie können einen geplanten Konfigurationsauftrag auch bearbeiten.

3. Auf der Seite **Job konfigurieren** können Sie sehen, dass der Job-Name und der Instanztyp nicht bearbeitet werden können. Sie können andere Felder wie Konfigurationsquelle ändern, Instanzen hinzufügen, Variablenwerte bearbeiten und Ausführungseinstellungen festlegen.
4. Klicken Sie auf **Fertig stellen**, um den Konfigurationsauftrag erneut auszuführen.



> **Hinweis**
>
> Sie können den Job auch auswählen und erneut auf **Ausführen** klicken, um den Job auszuführen, ohne Quelle, Instanz und Befehle zu ändern. Dies ist nützlich, wenn Sie dieselben Befehle für dieselben Instanzen ausführen müssen. Manchmal tritt der Auftrag möglicherweise auf einen vorübergehenden Fehler von der Serverseite auf, und Sie müssen den Auftrag möglicherweise erneut ausführen.



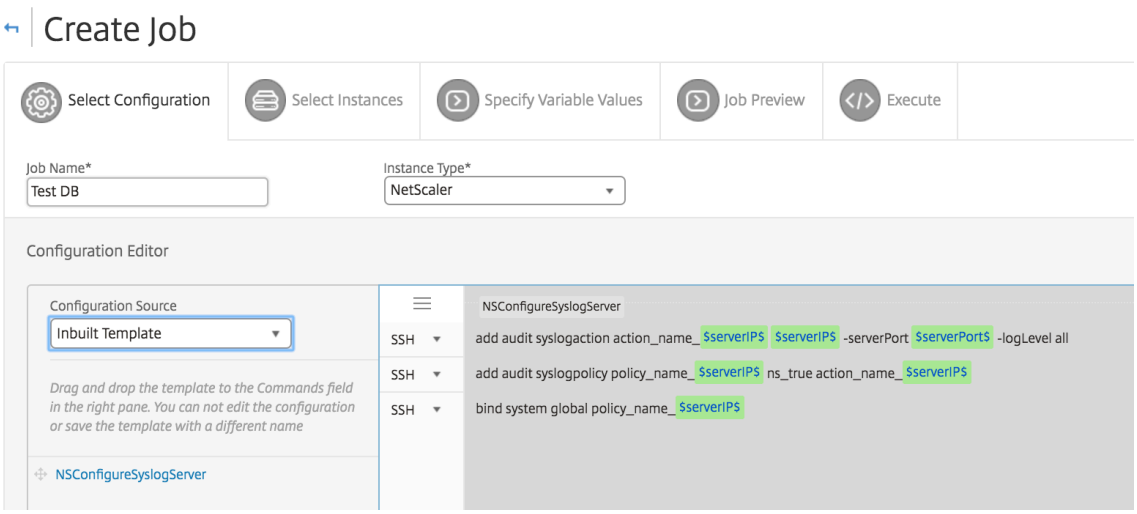
Jobs planen, die mit integrierten Vorlagen erstellt wurden

February 5, 2024

Sie können einen Job planen, indem Sie die integrierte Vorlagenoption verwenden. Ein Job ist ein Satz von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Verwenden Sie beispielsweise die integrierte Vorlagenoption, um einen Auftrag zur Konfiguration von Syslog-Servern zu planen. Sie können den Job auch sofort ausführen oder den Job so planen, dass er zu einem späteren Zeitpunkt ausgeführt wird.

So planen Sie einen Auftrag mithilfe integrierter Vorlagen in NetScaler Application Delivery Management (ADM)

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge**und klicken Sie dann auf **Job erstellen**.
2. Geben Sie auf der Seite **Job erstellen** auf der Registerkarte **Konfiguration auswählen** den **Auftragsnamen** an, und wählen Sie in der Dropdownliste den **Instanztyp** aus.
3. Wählen Sie in der Dropdownliste **Konfigurationsquelle** die Option **Inbuilt Template** aus. Ziehen Sie den Befehl ***NSConfigureSyslogServer** in den rechten Bereich, und klicken Sie dann auf **Weiter**.



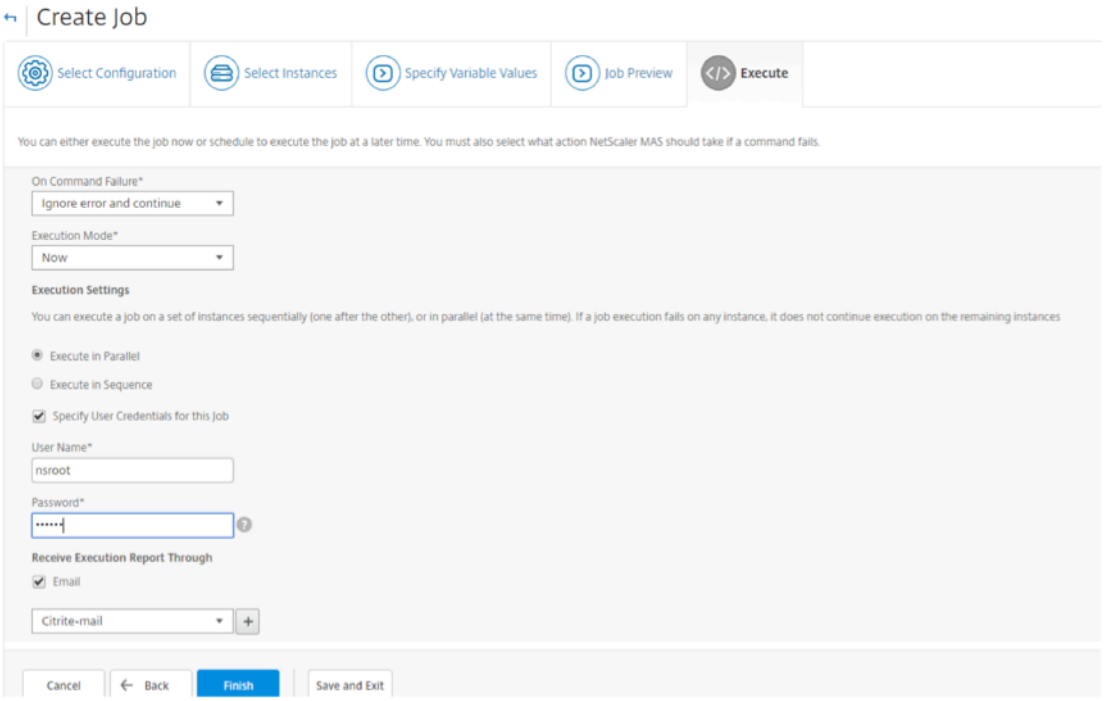
4. Klicken Sie auf der Registerkarte **Instanzen auswählen** auf **Instanzen hinzufügen**, wählen Sie die Instanzen aus, für die Sie den Auftrag ausführen möchten, und klicken Sie dann auf **OK**.
5. Klicken Sie auf **Weiter**. Wählen Sie auf der Registerkarte **Variablenwerte angeben** eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:
   - **Variablenwerte aus einer Eingabedatei** —Laden Sie eine Eingabedatei herunter, um Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben. Laden Sie dann die Datei auf den Citrix ADM Server hoch.
   - **Gemeinsame Variablenwerte für alle Instanzen**—Geben Sie die IP-Adresse und den Port des Syslog-Servers an.
6. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.
7. Klicken Sie auf **Weiter**.
8. Legen Sie auf der Registerkarte **Ausführen** die folgenden Bedingungen fest:

- **Bei Befehlsfehler** - Wenn ein Befehl fehlschlägt, können Sie entweder die Fehler ignorieren und den Job weiterhin ausführen oder die weitere Ausführung des Jobs stoppen. Wählen Sie in der Dropdownliste die Aktion aus, die Sie ausführen möchten.
- **Ausführungsmodus** - Sie können den Job entweder jetzt ausführen oder die spätere Ausführung des Auftrags planen. Wenn Sie den Job später planen möchten, müssen Sie die Ausführungsfrequenzeinstellungen für diesen Job angeben. Wählen Sie aus der Dropdownliste den Zeitplan aus, dem der Auftrag folgen soll.

9. Sie können einen Auftrag auch für eine Reihe von Instanzen sequenziell oder parallel ausführen, indem Sie die erforderliche Methode unter **Ausführungseinstellungen**auswählen. Wenn eine Auftragsausführung auf einer Instanz fehlschlägt, wird sie auf den verbleibenden Instanzen nicht fortgesetzt.

   Sie können autorisierten Benutzern die Ausführung von Aufträgen auf Ihren verwalteten Instanzen erlauben. Darüber hinaus kann eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Auftrags gesendet werden, zusammen mit anderen Details.

10. Klicken Sie auf **Fertig stellen**.



Verwenden von Wartungsaufträgen zum Aktualisieren von NetScaler ADC SDX-Instanzen

February 5, 2024

Sie können ein Einzelbündel-Upgrade Ihrer NetScaler ADC SDX-Instanzen mit NetScaler ADC Version 11.0 und höher durchführen. Um ein Einzelbündel-Upgrade durchzuführen, verwenden Sie einen integrierten Task in NetScaler ADM.Mit dieser integrierten Aufgabe können Sie den Citrix ADC SDX-Verwaltungsdienst, Citrix Hypervisor und die zusätzlichen Packs und Hotfixes für Citrix Hypervisor aktualisieren.

So aktualisieren Sie NetScaler ADC SDX-Instanzen mithilfe von NetScaler ADM:

1. Navigieren Sie zu **Netzwerke > Konfigurationsjobs > Wartungsaufträge**.
2. Klicken Sie auf **Job erstellen**. Wählen Sie auf der Seite "**Job erstellen** "die integrierte Task "**NetScaler ADC SDX** aktualisieren"aus, um Ihre NetScaler ADC SDX-Instanzen zu aktualisieren. Klicken Sie auf **Weiter**.
3. Geben Sie auf der Seite **NetScaler ADC Appliances aktualisieren** auf der Registerkarte **Instanzauswahl** den **Job-Namen** an und klicken Sie auf**Add Instanzen.**
4. Wählen Sie die Zielinstanzen oder Instanzgruppen aus, die Sie aktualisieren möchten.
5. Nachdem Sie die NetScaler ADC-Instanzen oder Instanzgruppen hinzugefügt haben, klicken Sie auf**Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten. Auf dem Bildschirm wird der Fortschritt der Vorvalidierung der einzelnen NetScaler ADC-Instanzen angezeigt.
6. Wählen Sie auf der Seite**Upgrade ändern NetScaler ADC Appliance (s)** die Registerkarte**Upgrade**aus. Wählen Sie im Dropdown-Menü "**Software-Image**"entweder "**Lokal**"(Ihr lokaler Computer) oder "**Appliance**"(die Builddatei muss in NetScaler ADM vorhanden sein).
7. Sie können auch sehen, ob Instanzen Fehler beim Upgrade vor der Validierung aufweisen. Diese Fehler werden in Form einer Nachricht angezeigt. Die Meldungen zeigen die Fehler im Zusammenhang mit Speicherplatz, Festplattenlaufwerk und Benutzeranpassungen an. Wenn Sie nicht mit Instanzen fortfahren möchten, die die Überprüfung vor der Validierung fehlgeschlagen haben, können Sie die Instanzen entfernen. Um die Instanzen zu entfernen, wählen Sie die Instanzen aus, und klicken Sie auf**Löschen.**
8. Auf der Registerkarte**Task planen**können Sie auch Ausführungsdetails festlegen, in denen Sie den Upgradevorgang jetzt durchführen oder für einen späteren Zeitpunkt planen können. Sie können auch Ihre NetScaler ADC SDX-Instanz sichern, einen Ausführungsbericht per E-Mail erhalten oder ein zweistufiges Upgrade für Knoten in HA durchführen.

Das zweistufige Upgrade für Knoten in HA bietet Ihnen die Möglichkeit, das Upgrade sofort durchzuführen oder einen Zeitpunkt für die Aktualisierung der Knoten nacheinander zu planen.Synchronisierung und Weitergabe der Knoten sind deaktiviert, bis beide Knoten erfolgreich aktualisiert wurden.

Erstellen von Konfigurationsaufträgen für Citrix SD-WANOP-Instanzen

February 5, 2024

Ein Auftrag ist ein Satz von Konfigurationsbefehlen, die Sie für eine oder mehrere verwaltete Instanzen erstellen und planen können. Für Citrix SD-WANOP-Instanzen können Sie die folgenden Optionen verwenden, um Jobs zu erstellen:

- **Konfigurationsvorlage**: Sie können den Konfigurationseditor verwenden, um CLI-Befehle einzugeben, die Konfiguration als Vorlage zu speichern und sie zum Konfigurieren von Aufträgen zu verwenden.
- **Integrierte Vorlage**: Sie können aus einer Liste von Konfigurationsvorlagen wählen. Diese Vorlagen stellen die Syntaxen der CLI-Befehle bereit und ermöglichen es Ihnen, Werte für die Variablen anzugeben. Die integrierten Vorlagen sind mit ihren Beschreibungen in der folgenden Tabelle aufgeführt.
- **Datei**: Sie können eine Konfigurationsdatei von Ihrem lokalen Computer hochladen und Aufträge erstellen.

Sobald ein Job erstellt wurde, können Sie den Job sofort ausführen oder den Job so planen, dass er später ausgeführt wird. Sie können auch die Ausführungsfrequenz

Eingebaute Vorlage	Beschreibung
EnableCloudBridgeWANOpt	Aktiviert den Datenverkehr über die Citrix SD-WANOP-Appliance.
DisableCloudBridgeWANOpt	Deaktiviert den Datenverkehr über die Citrix SD-WANOP-Appliance.
RestartCloudBridgeWANOpt	Startet die Citrix SD-WANOP-Appliance neu.
RestoreConfig	Stellt die Konfiguration der Citrix SD-WANOP-Appliance wieder her.
AddLink	Durch das Erstellen oder Definieren von Links kann die SD-WANOP-Appliance Staus und Verluste auf den Verbindungen verhindern und Traffic Shaping durchführen. Sie können die maximale Bandbreite definieren, die über den Link gesendet oder empfangen wird, und auch angeben, dass es sich um einen LAN-seitigen oder WAN-seitigen Datenverkehr handelt.

Eingebaute Vorlage	Beschreibung
ConfigureBandwidth	Legt die Bandbreitenlimits und andere Bandbreitenverwaltungseinstellungen fest
AddUser	Fügt einen neuen Benutzer hinzu, für den Sie Berechtigungen zuweisen können.
AddUserAdvancedPlatform	Fügt einen neuen Benutzer hinzu, mit dem Sie Berechtigungen zuweisen können, die in der `AddUser` Vorlage nicht verfügbar sind.
AddService-class	Erstellt eine Serviceklasse für Citrix SD-WANOP-Appliance mit einem oder mehreren Serviceklassenfiltern und aktiviert diese.
SetApplication	Setzt die Definition des Anwendungsklassifizierers
AddorRemoveVideoCachingPorts	Fügt die Portnummer hinzu oder entfernt sie, an der die Videoquelle Daten senden oder empfangen kann. Der Standardport ist 80.
RemoveVideoCachingSource	Entfernt eine oder mehrere Video-Caching-Quellen. Geben Sie die IP-Adresse oder den Domänennamen der Videoquelle an.
RemoveAllVideoCaching	Entfernt alle verfügbaren Video-Caching-Quellen.
VideoCachingState	Aktiviert oder deaktiviert die Video-Caching-Funktion auf Citrix SD-WANOP-Appliances.
ClearVideoCaching	Löscht entweder den Video-Cache oder die Video-Caching-Statistik.
SetVideoCaching	Legt die maximale Größe für zwischengespeicherte Objekte fest. Ein Objekt, das diesen Grenzwert überschreitet, wird nicht zwischengespeichert. Standardmäßig beträgt die maximale Größe des Cache-Objekts 100 MB.
AddVideoCachingSource	Fügt die IP-Adresse oder den Domainnamen der Videoquelle hinzu. Enthält Optionen zum Aktivieren oder Deaktivieren des Video-Caching für diese Quelle.

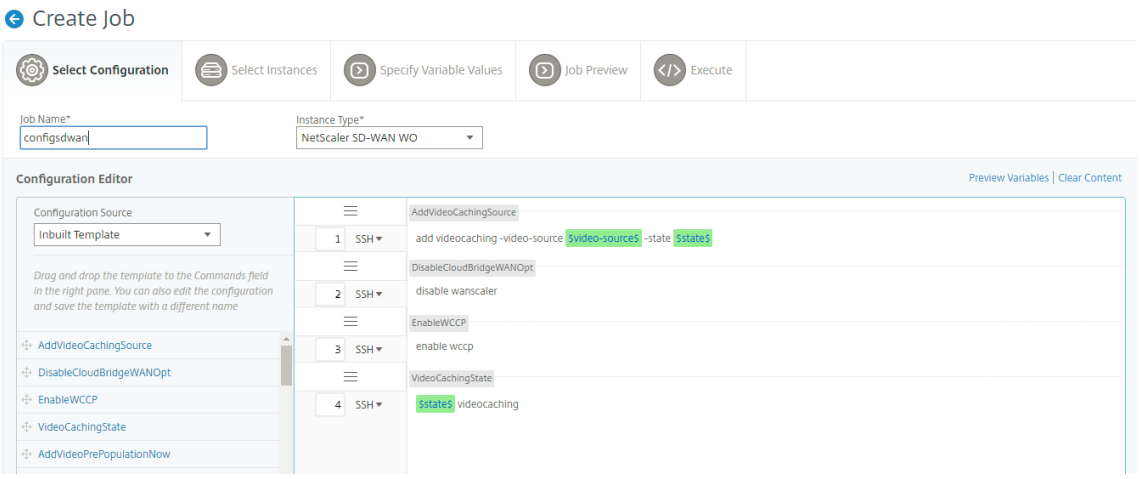
Eingebaute Vorlage	Beschreibung
ConfigureRemoteLicenseServer	Konfiguriert den zentralen Lizenzserver. Geben Sie das Lizenzservermodell, die IP-Adresse und die Portnummer an.
ConfigureLocalLicenseServer	Legt den Speicherort des Lizenzservers als lokal fest.
InstallCACert	Installiert CA-Zertifikate auf der Citrix SD-WANOP-Appliance. Geben Sie den Zertifikatsnamen, den Dateinamen und das Schlüsselspeicherkennwort an.
InstallCombinedCerKey	Installiert eine kombinierte SSL-Zertifikatsschlüsselpaardatei.
InstallSeperateCertKey	Installiert das SSL-Zertifikat und den Schlüssel als separate Dateien.
EnableWCCP	Aktiviert den WCCP-Bereitstellungsmodus.
AddWCCPServiceGroup	Fügt eine neue WCCP-Dienstgruppendefinition für die Citrix SD-WANOP-Appliance hinzu.
DisableWCCP	Deaktiviert den WCCP-Bereitstellungsmodus.
AddTrafficShapingPolicy	Erstellt eine Traffic-Shaping-Richtlinie für die Citrix SD-WAN-Appliance. Die Richtlinie steuert die Netzwerkbandbreite.
SetTrafficShapingPolicy	Ändert die Traffic Shaping-Richtlinie für die Citrix SD-WANOP-Appliance. Die Richtlinie steuert die Netzwerkbandbreite.
AddVideoPrePopulation	Erstellt einen Videovorfüllungseintrag, mit dem Sie ein Video im Voraus herunterladen und zwischenspeichern können. Sie können auch angeben, wann ein Video zwischengespeichert werden soll.
UpdateVideoPrePopulation	Ändert einen Videovorbelegungseintrag, der angibt, wann ein Video zwischengespeichert werden soll.
AddVideoPrePopulationNow	Konfiguriert die Videovorbestückung, sodass Sie ein Video sofort herunterladen und zwischenspeichern können. Sie können steuern, wie Sie Videos von den URLs herunterladen und zwischenspeichern möchten.

Eingebaute Vorlage	Beschreibung
VideoPrePopulationState	Ändert, startet, aktualisiert oder entfernt die Vorbelegung von Videos.
ConfigureSyslogServer	Legt die IP-Adresse und die Portnummer des Syslog-Servers fest.
ConfigureAlert	Konfiguriert die Warnstufe.

So erstellen Sie einen Konfigurationsauftrag für Citrix SD-WANOP-Instanzen:

1. Navigieren Sie in Citrix ADM zu **Netzwerke**> **Konfigurationsaufträge**, und klicken Sie dann auf **Job erstellen**.
2. Geben Sie auf der Seite **Auftrag erstellen** auf der Registerkarte **Konfiguration auswählen** den **Auftragsnamen** an.
3. Wählen Sie im Feld **Instanztyp** die Option **Citrix SD-WAN WO**aus.
4. Wählen Sie in der Dropdownliste **Konfigurationsquelle** eine Option zum Erstellen eines Auftrags aus.

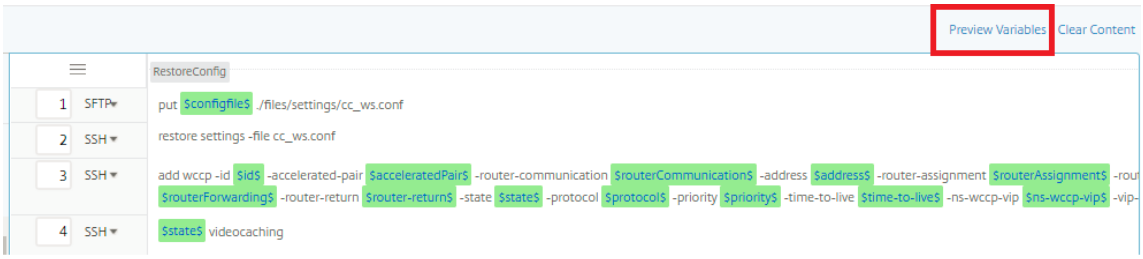
> **Hinweis**
>
> Wählen Sie **Als Konfigurationsvorlage speichern** aus, und geben Sie einen Namen an, um die Konfiguration als Vorlage zu speichern und wiederzuverwenden.



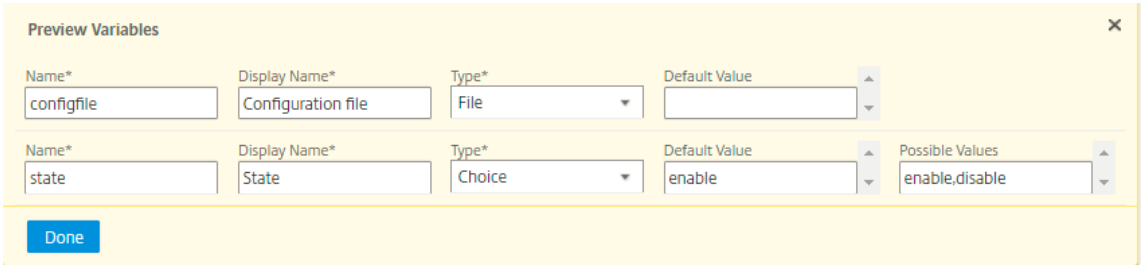
5. Sie können alle Variablen überprüfen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags in einer einzigen konsolidierten Ansicht definiert haben.
6. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:

- Navigieren Sie beim Erstellen eines Konfigurationsauftrags zu **Netzwerke > Konfigurationsaufträge** und wählen Sie **Job erstellen** aus. Auf der Seite **Job erstellen** können Sie alle Variablen überprüfen, die Sie beim Erstellen des Konfigurationsauftrags hinzugefügt haben.
- Während Sie einen Konfigurationsauftrag bearbeiten, navigieren Sie zu **Netzwerk > Konfigurationsjobs**, wählen Sie den Job-Namen aus und klicken Sie auf **Bearbeiten**. Auf der Seite **Job konfigurieren** können Sie alle Variablen überprüfen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.

7. Sie können dann auf die Registerkarte **Vorschauvariablen** klicken, um eine Vorschau der Variablen in einer einzelnen konsolidierten Ansicht anzuzeigen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben.



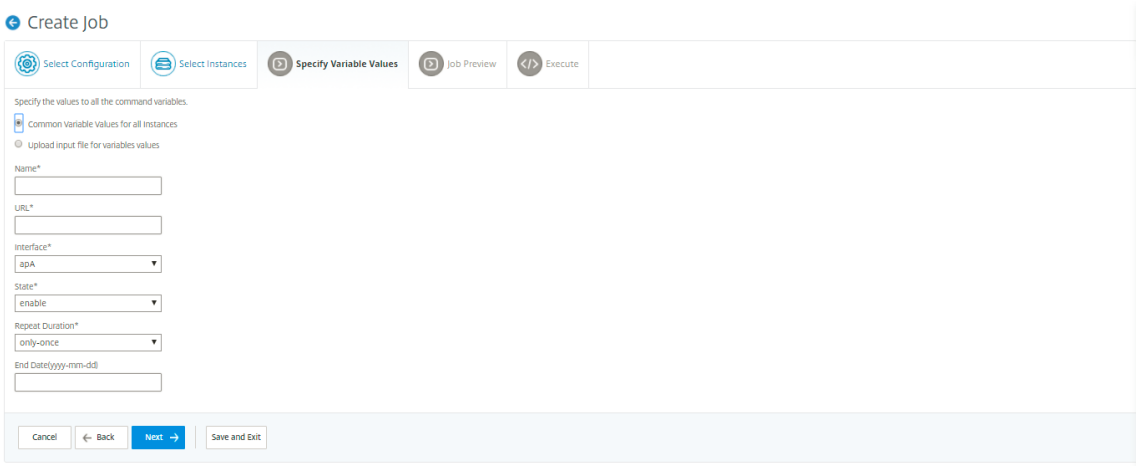
8. Ein neues Popup-Fenster wird angezeigt, in dem alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem tabellarischen Format angezeigt werden. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Fertig**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.



9. Klicken **Sie**auf Weiter und dann auf der Registerkarte **Instanzen** auswählen auf **Instanzen hinzufügen.** Wählen Sie die Instanzen aus, auf denen Sie den Job ausführen möchten, und klicken Sie dann auf **OK** .
10. Klicken Sie auf**Weiter**, und wählen Sie dann auf der Registerkarte**Variablenwerte angeben**eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:

- ** Eingabedatei für Variablenwerte hochladen: ** Klicken Sie auf Eingabeschlüsseldatei herunterladen, um eine Eingabedatei herunterzuladen. Geben Sie in der Eingabedatei Werte für die Variablen ein, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den NetScaler ADM Server hoch.

- **Gemeinsame Variablenwerte für alle Instanzen**: Geben Sie Werte für die Variablen ein. Die Variablen variieren je nach ausgewählter Vorlage.



Die Eingabedateien, die die Variablenwerte enthalten, werden in den Konfigurationsaufträgen beibehalten (mit demselben Dateinamen). Sie können diese Eingabedateien anzeigen und bearbeiten, die Sie früher beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben.

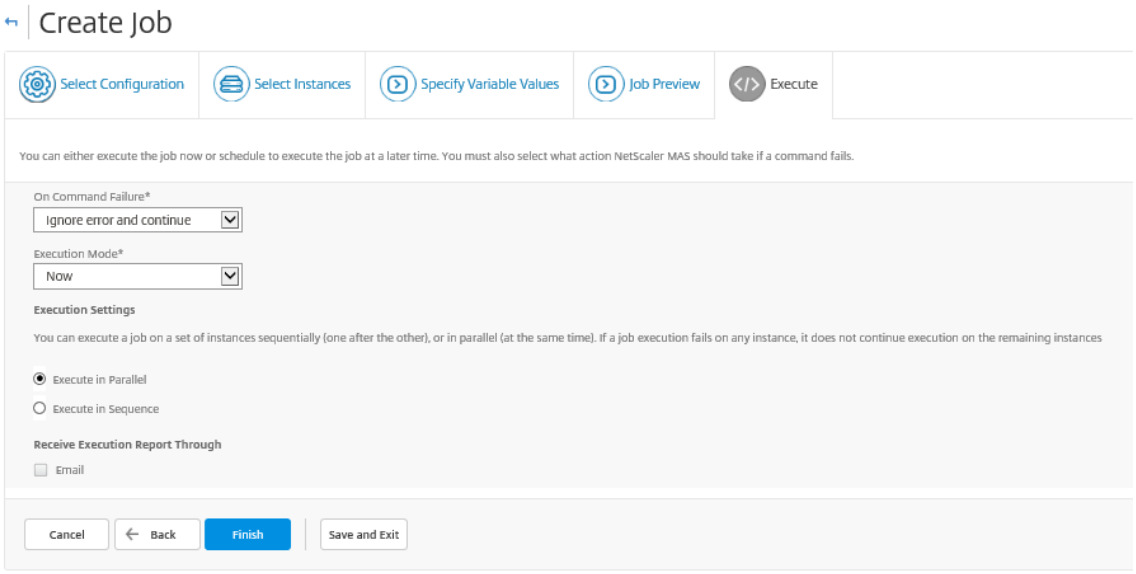
Um die Run Configuration Jobs beim Erstellen eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk > Konfigurationsjobs**und klicken Sie auf **Job erstellen**. Auf der Seite**"Job erstellen"**. Wählen Sie auf der Registerkarte**Variablenwerte angeben**die Option**Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

Um die bereits ausgeführten Konfigurationsaufträge anzuzeigen, während Sie einen Konfigurationsauftrag bearbeiten, navigieren Sie zu **Netzwerk > Konfigurationsjobs**, wählen Sie den Job-Namen aus und klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite "**Job konfigurieren**" auf der Registerkarte**Variablenwerte angeben**die Option**Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

11. Klicken Sie auf **Weiter**, auf der Registerkarte **Job-Vorschau** können Sie die als Job auszuführenden Befehle bewerten und überprüfen.
12. Klicken Sie auf **Weiter**, legen Sie auf der Registerkarte **Ausführen**die folgenden Bedingungen fest:

    - **Bei Befehlsfehler**: Was tun, wenn ein Befehl fehlschlägt: Ignorieren Sie die Fehler und setzen Sie den Job fort, oder stoppen Sie die weitere Ausführung des Auftrags. Wählen Sie eine Aktion aus der Dropdownliste aus.

- **Ausführungsmodus**: Führen Sie den Auftrag sofort aus oder planen Sie die Ausführung für einen späteren Zeitpunkt ein. Wenn Sie die Ausführung für einen späteren Zeitpunkt planen, müssen Sie die Einstellungen für die Ausführungsfrequenz für den Job angeben. Wählen Sie in der Dropdownliste **Ausführungsfrequenz** den Zeitplan aus, dem der Auftrag folgen soll.



13. Wählen Sie unter **Ausführungseinstellungen**aus, um den Job sequenziell (nacheinander) oder parallel (gleichzeitig) auszuführen.
14. Damit ein Bericht zur Auftragsausführung an eine Liste von Empfängern per E-Mail gesendet wird, aktivieren Sie das Kontrollkästchen **E-Mail** im Abschnitt **Ausführungsbericht erhalten durch**. Wählen Sie in der angezeigten Dropdownliste eine E-Mail-Verteilerliste aus. Um eine E-Mail-Verteilerliste zu erstellen, klicken Sie auf das Symbol **+** und geben Sie die E-Mail-Adressen der Empfänger sowie die E-Mail-Serverdetails ein.
15. Klicken Sie auf **Fertig stellen**.

Masterkonfigurationsvorlage verwenden

February 5, 2024

Die Verwendung einer Hauptkonfigurationsvorlage ist eine flexible Option zum Erstellen und Bereitstellen einer Master-Konfiguration auf mehreren NetScaler ADC-Instanzen.

Als Administrator möchten Sie möglicherweise Konfigurationsänderungen vornehmen und Lizenzen, Zertifikate und andere Dateien auf der ADC-Instanz speichern. Sie können die neue Konfiguration als

Masterkonfigurationsvorlage (.conf-Datei) speichern.

Um Ihre Master-Konfigurationsvorlage von einer ADC-Instanz zu speichern, können Sie einen der folgenden Schritte ausführen:

- Geben Sie an der Eingabeaufforderung **save ns config**ein. Die Konfiguration wird im FLASH-Speicher der Instanz in der Datei /nsconfig/ns.conf gespeichert.
- Navigieren Sie in der GUI der Instanz zu **Diagnostics** > **View Configuration**. Wählen Sie die Art der Konfiguration, die Sie speichern möchten. Wenn Sie beispielsweise die gespeicherte Konfiguration Ihrer Instance speichern möchten, wählen Sie **Gespeicherte Konfiguration** aus.Klicken Sie auf den Link **Text in eine Datei** speichern, um die Datei 'ns.conf'auf Ihrem lokalen Rechner zu speichern.

Wenn Sie die Master-Konfigurationsvorlage bereitstellen, indem Sie beim Erstellen eines Auftrags die Konfigurationsvorlage "DeployMasterConfiguration"verwenden, können Sie sie für jede spezifische ADC-Instanz weiter anpassen, indem Sie weitere Befehle hinzufügen, vorhandene Befehle ändern und unterschiedliche Variablenwerte in der Eingabedatei angeben.

Als Administrator können Sie beispielsweise Zertifikatschlüssel in Ihre ADC-Instanzen zusätzlich ns.conf-Datei hochladen und die Master-Konfiguration auf ihnen bereitstellen.

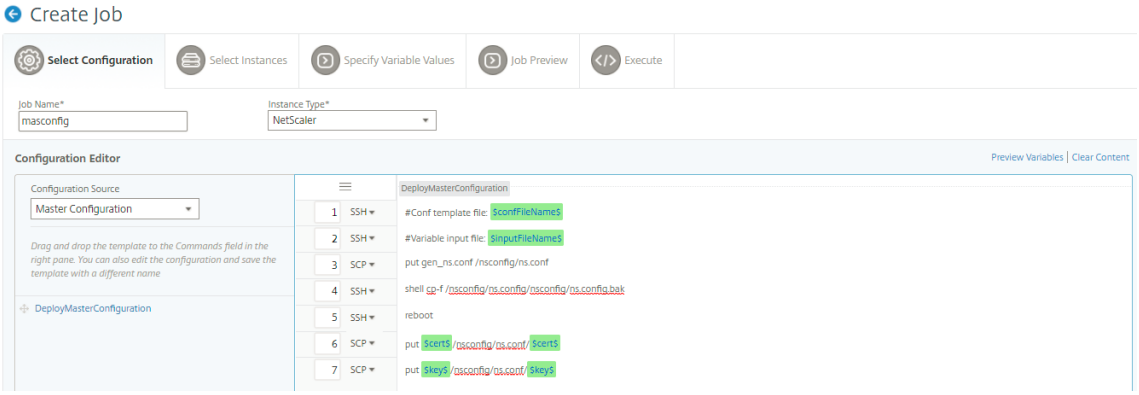
> **Wichtig!**
>
> Sie können einen Konfigurationsauftrag nicht mit der DeployMasterConfiguration-Vorlage auf NetScaler ADC CPX-Instanzen, in einem Cluster konfigurierten Instanzen oder auf partitionierten ADC-Instanzen ausführen.

So erstellen Sie einen Konfigurationsauftrag mit der Konfigurationsvorlage Master Config unter NetScaler ADM:

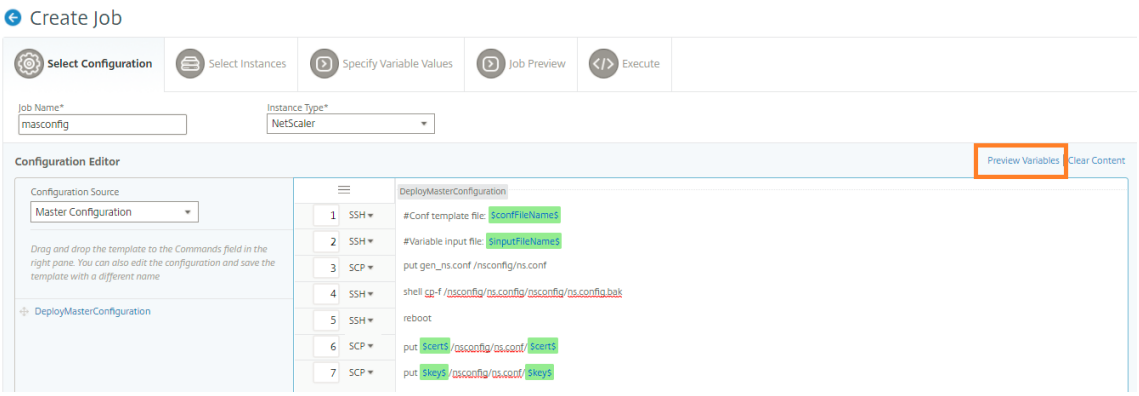
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge**und klicken Sie dann auf **Job erstellen**.
2. Geben Sie auf der Seite **Job erstellen** auf der Registerkarte **Konfiguration auswählen** den **Auftragsnamen** an, und wählen Sie in der Dropdownliste den **Instanztyp** aus.
3. Wählen Sie in der Dropdownliste **Konfigurationsquelle** die Option **Hauptkonfiguration** aus. Ziehen Sie die Befehle der DeployMasterConfiguration-Vorlage in den rechten Bereich. Sie können Befehle auch im rechten Fensterbereich hinzufügen, ändern oder löschen. Klicken Sie auf **Weiter**.

   > **Hinweis**
   >
   > Sie können ***Put-Befehle*** hinzufügen, um Ihrer Vorlage Eingabedateien hinzuzufügen. In

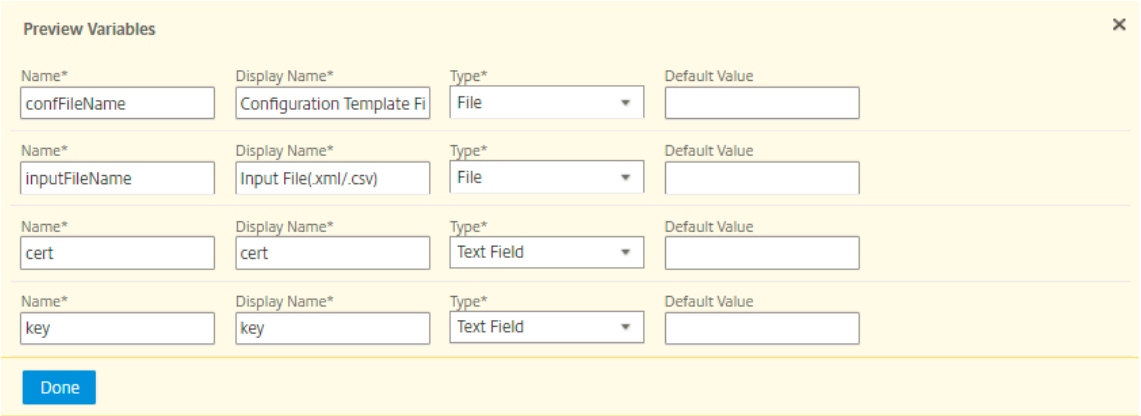
> unserem Beispiel müssen wir neben der Konfigurationsvorlagendatei und den variablen Eingabedateien auch Zertifikat- und Schlüsseldateien hochladen.



4. Sie können alle Variablen überprüfen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags in einer einzigen konsolidierten Ansicht definiert haben.
5. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:
   - Navigieren Sie beim Erstellen eines Konfigurationsauftrags zu **Netzwerke > Konfigurationsaufträge** und wählen Sie **Job erstellen** aus. Auf der Seite **Job erstellen** können Sie alle Variablen überprüfen, die Sie beim Erstellen des Konfigurationsauftrags hinzugefügt haben.
   - Während Sie einen Konfigurationsauftrag bearbeiten, navigieren Sie zu **Netzwerk > Konfigurationsjobs**, wählen Sie den Job-Namen aus und klicken Sie auf **Bearbeiten**. Auf der Seite **Job konfigurieren** können Sie alle Variablen überprüfen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.
6. Sie können dann auf die Registerkarte **Vorschauvariablen** klicken, um eine Vorschau der Variablen in einer einzelnen konsolidierten Ansicht anzuzeigen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben.



7. Ein neues Popup-Fenster wird angezeigt, in dem alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem tabellarischen Format angezeigt werden. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Fertig**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.



8. Wählen Sie die Instanzen aus, auf denen Sie den Konfigurationsauftrag ausführen möchten, und klicken Sie dann auf **Weiter**.
9. Laden Sie auf der Registerkarte "**Variablenwerte angeben** "Folgendes hoch:

   - **Konfigurationsvorlagendatei (.conf)** —Laden Sie die .conf-Datei hoch, die Sie aus einer ADC-Instance extrahiert haben.
   - **Eingabedatei hochladen (.xml/csv)** - Laden Sie die Eingabedatei mit Werten für die Variablen hoch, die Sie in Ihren Befehlen definiert haben.

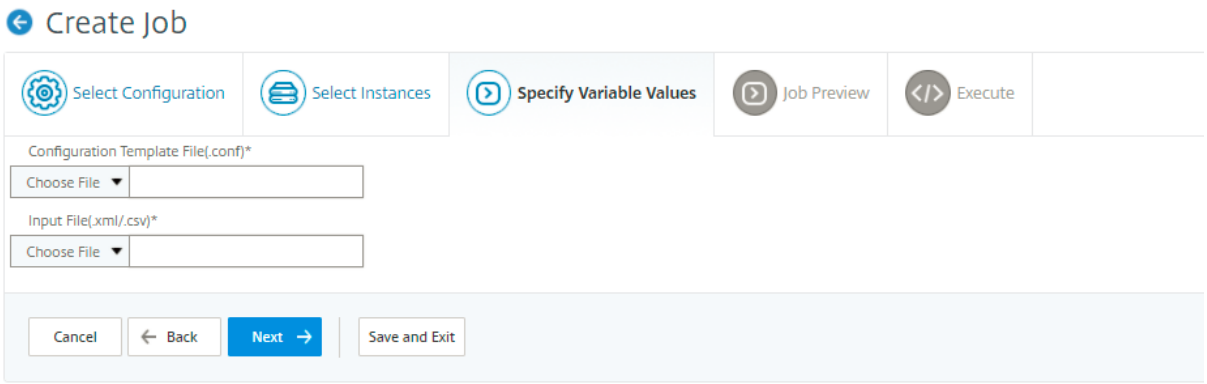
   Eine Beispiel-XML-Datei wird hier für Ihre Verwendung bereitgestellt. Stellen Sie sicher, dass die xml-Dateien die Details enthalten, die den von Ihnen verwendeten ADC-Instanzen entsprechen.

```
<?xml version="1.0" encoding="UTF-8" ?>

<properties>

<!--

Provide inputs for all the parameters defined in the master config
    file.

-  global. This tag contains all the common parameters and value.

-  devicegroup. This tag contains all the instance group specific
   parameters and values.

If the same parameters are defined in global and instance tags,
   the instance specific parameters value will take precedence
   over the instance group. The instance group specific parameters
    value will take precedence over global parameters in the
   execution.
```



```
14
15  -  name. This attribute represents the name of the instance group.
16
17  -  device. This tag contains all the instance specific parameters
       and value.
18
19  If the same parameters are defined in global and instance tags,
       the instance specific parameters value will take precedence in
       the execution.
20
21  -  name. This attribute represents the IP Address of the instance.
        Host name is not supported for the attibute.
22
23  HA pair should be represented as <primaryip>-<secondaryip>.
       Example 10.102.2.1-10.102.2.2
24
25  In the template file, the parameter name must be specified within
       the dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters
       names are case sensitive.
26  -->
27
28  <global>
29
30  </global>
31  <devicegroup name="BLR_DEVS">
32  </devicegroup>
33  <device name="10.106.101.209">
34  <param name="IP" value="10.106.101.209"/>
35  </device>
36
37  <!-- HA PAIR-->
38  <!--<device name="10.102.43.154-10.102.43.155">
39  <param name="NSIP" value="10.102.43.154"/>
40  <param name="HostName" value="NS43HA"/>
41  <param name="LBSERVER" value="haserver43http"/>
42  <param name="SNMPTrapDest" value="10.102.43.130"/>
43  </device>-->
44  </properties>
45
46  <!--NeedCopy-->
```

10. Klicken Sie auf **Weiter**.

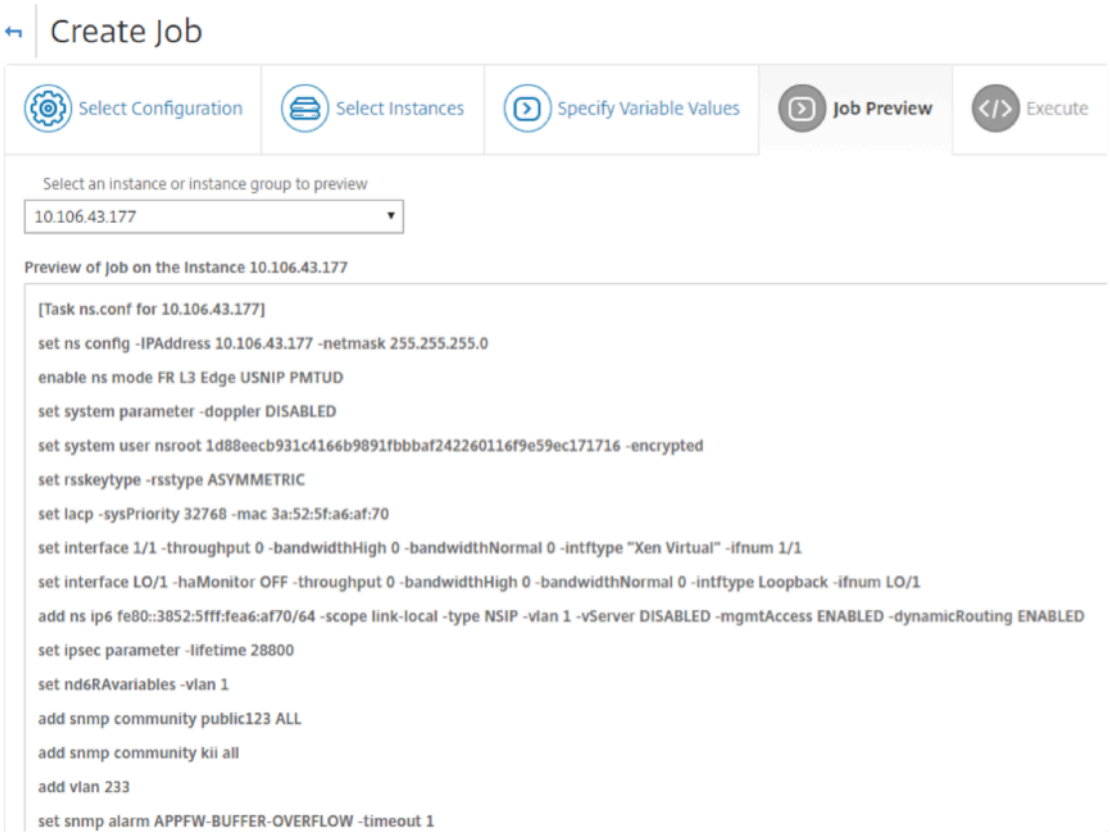


Die Eingabedateien, die die Variablenwerte enthalten, werden in den Konfigurationsaufträgen beibehalten (mit demselben Dateinamen). Sie können diese Eingabedateien anzeigen und bearbeiten, die Sie früher beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben.

Um die Ausführungskonfigurationsaufträge beim Erstellen eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk > Konfigurationsaufträge**, und klicken Sie auf **Job erstellen**. Auf der Seite **Job erstellen**. Wählen Sie auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

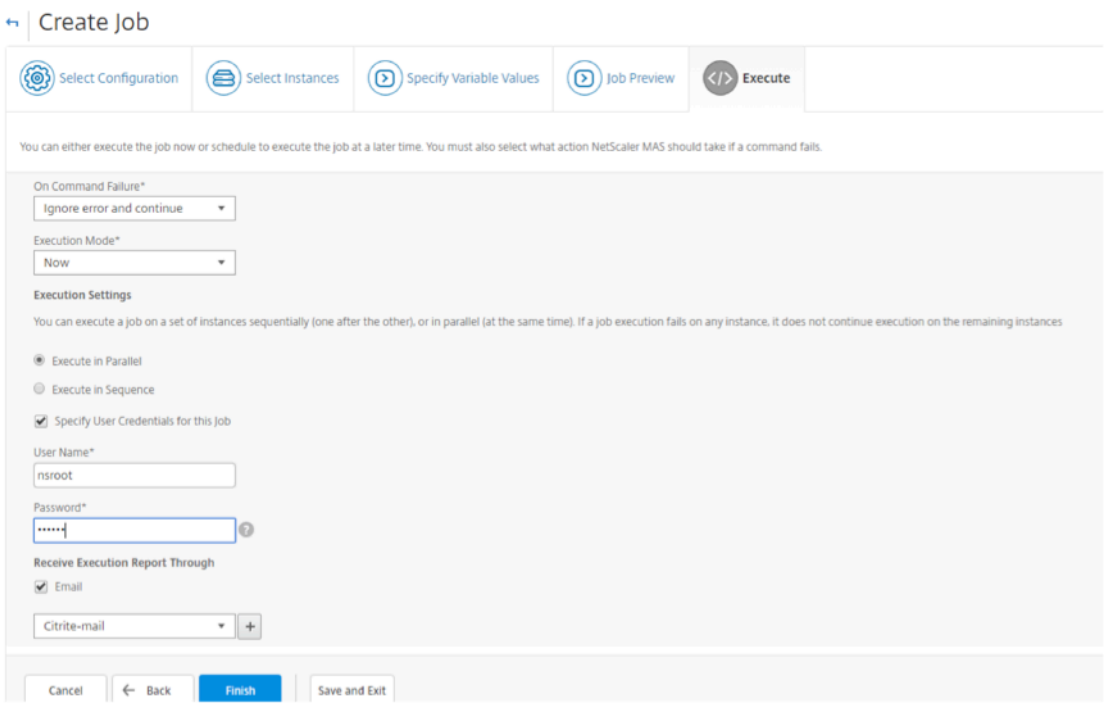
Um die bereits ausgeführten Konfigurationsaufträge beim Bearbeiten eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk > Konfigurationsaufträge**, wählen Sie den Auftragsnamen aus und klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite **Job konfigurieren** auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien hoch (unter gleichem Dateinamen).

1. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen, und klicken Sie dann auf **Weiter**.

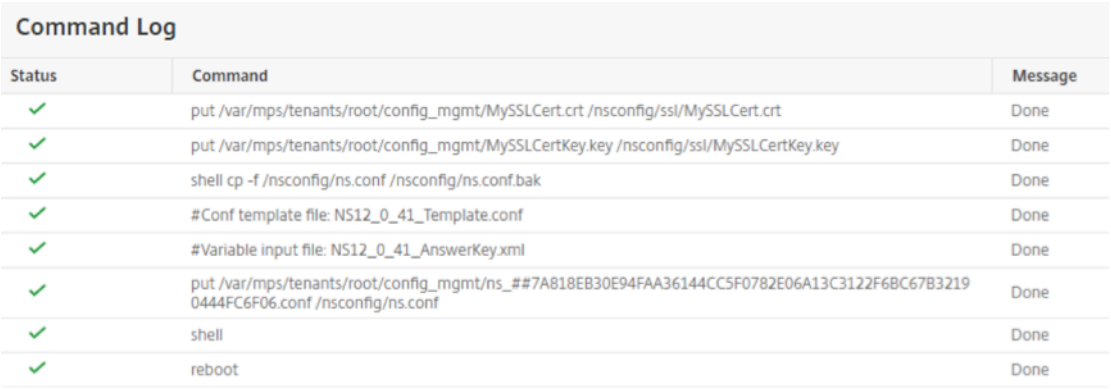


2. Auf der Registerkarte**Ausführen**können Sie wählen, ob Sie Ihren Job jetzt ausführen oder planen, dass er später ausgeführt wird. Sie können auch auswählen, welche Aktion NetScaler ADM ausführen muss, wenn der Befehl fehlschlägt.

   Sie können auch autorisierten Benutzern erlauben, Aufträge auf Ihren verwalteten Instanzen auszuführen, und Sie können wählen, ob Sie eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Auftrags zusammen mit anderen Details senden möchten.



Nachdem Sie Ihren Job ausgeführt haben, können Sie die Jobdetails anzeigen, indem Sie zu**Netzwerke** >**Konfigurationsjobs**navigieren und den von Ihnen konfigurierten Job auswählen. Klicken Sie auf**Details**und dann auf**Ausführungszusammenfassung**, um die Details Ihres Jobs anzuzeigen. Klicken Sie auf die Instanz, um die **Befehlsprotokolle** anzuzeigen, damit die Befehle für den Auftrag ausgeführt werden.



Command Log

Status	Command	Message
✓	put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt	Done
✓	put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key	Done
✓	shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak	Done
✓	#Conf template file: NS12_0_41_Template.conf	Done
✓	#Variable input file: NS12_0_41_AnswerKey.xml	Done
✓	put /var/mps/tenants/root/config_mgmt/ns_##7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B3219 0444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

Verwenden von Aufträgen zum Upgrade von NetScaler ADC-Instanzen

February 5, 2024

Sie können Citrix Application Delivery Management (ADM) verwenden, um eine oder mehrere Citrix ADC-Instanzen zu aktualisieren. Sie müssen das Lizenzierungsframework und die Lizenztypen kennen,

bevor Sie eine Instanz aktualisieren.

Wenn Sie Ihre NetScaler ADC-Instanz durch Erstellen eines Wartungsauftrags aktualisieren, führen Sie die Vorvalidierungsprüfung für die Instanzen durch, die Sie aktualisieren möchten.

1. Auf**Anpassungen prüfen** - Sichern Sie Ihre Anpassungen, und löschen Sie sie aus den Instanzen. Sie können die gesicherten Anpassungen nach dem Instanz-Upgrade erneut anwenden.
2. **Überprüfen Sie die Festplattenauslastung** —Wenn der `/var` Ordner weniger als 6 GB Speicherplatz hat und der `/flash` Ordner weniger als 200 MB Speicherplatz hat, bereinigen Sie den Speicherplatz. Überprüfen Sie die folgenden Ordnerpfade, um den Speicherplatz zu leeren:
   - `/var/nstrace`
   - `/var/log`
   - `/var/nslog`
   - `/var/tmp/support`
   - `/var/core`
   - `/var/crash`
   - `/var/nsinstall`
   - `/var/netscaler/nsbackup`
3. **Überprüfen Sie auf Datenträger-Hardwareprobleme** - Beheben Sie ggf. die Hardwareprobleme.

Sie können ein ADC-HA-Paar in zwei Stufen aktualisieren:

1. Erstellen Sie einen Upgrade-Auftrag und führen Sie sofort auf einem der Knoten aus oder planen Sie später ein.
2. Planen Sie den Upgrade-Auftrag später auf dem verbleibenden Knoten. Stellen Sie sicher, dass Sie diesen Auftrag nach dem ersten Upgrade des Knotens planen.

Beachten Sie beim Upgrade eines ADC-HA-Paars Folgendes:

- Der sekundäre Knoten wird zuerst aktualisiert.
- Synchronisation und Weitergabe der Knoten werden deaktiviert, bis beide Knoten erfolgreich aktualisiert wurden.
- Nach dem erfolgreichen HA-Paar-Upgrade erscheint eine Fehlermeldung in der Ausführungshistorie. Diese Meldung wird angezeigt, wenn sich Ihre Knoten im HA-Paar auf unterschiedlichen Builds oder Versionen befinden. Diese Meldung zeigt an, dass die Synchronisierung zwischen primären und sekundären Knoten deaktiviert ist.

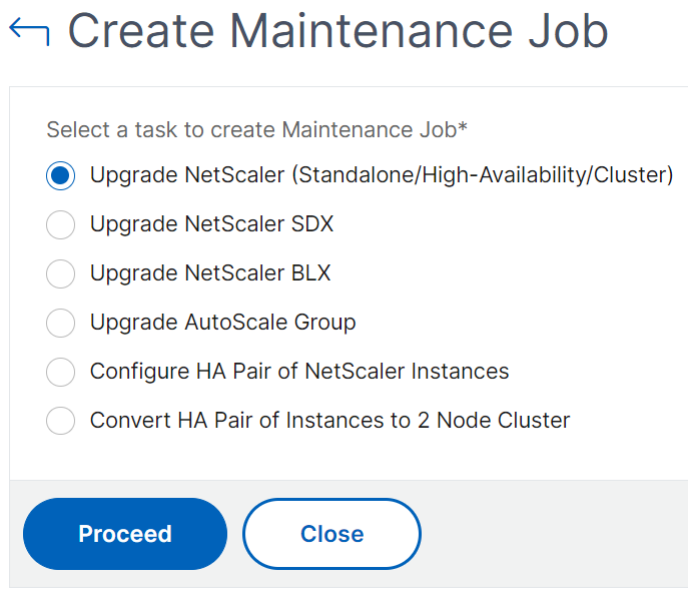
Wenn Sie einen ADC-Cluster aktualisieren, führt das ADM die Validierung vor dem Upgrade nur für die angegebene Instanz durch. Überprüfen und beheben Sie vor dem Upgrade die Probleme mit Anpassungen, Festplattenauslastung und Hardwareproblemen auf den Clusterknoten.

Erstellen eines Upgrade-Wartungsauftrags zum Aktualisieren von ADC-Instanzen

> **Hinweis**
>
> Ein ADC-Upgrade von einer höheren Version auf eine niedrigere Version wird nicht unterstützt. Wenn Ihre NetScaler ADC-Instanz beispielsweise 13.0 82.x ist, können Sie die ADC-Instanz nicht auf 13.0 79.x oder andere frühere Versionen herunterstufen.

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Job erstellen**.

2. Wählen Sie unter **Wartungsaufträge erstellen** die Option **NetScaler ADC (Standalone/Hochverfügbarkeit/Cluster) aktualisieren** aus und klicken Sie auf **Fortfahren**.



3. Geben Sie unter **Instanz auswählen** einen Namen Ihrer Wahl für **Auftragsname ein**.
4. Klicken Sie auf **Instanzen hinzufügen**, um ADC-Instanzen hinzuzufügen, die Sie aktualisieren möchten.

- Um ein HA-Paar zu aktualisieren, geben Sie die IP-Adresse eines primären oder sekundären Knotens an.
- Um einen Cluster zu aktualisieren, geben Sie die Cluster-IP-Adresse an.

5. Klicken Sie auf **Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten.

   Auf der Registerkarte **Validierung vor dem Upgrade** werden die fehlgeschlagenen Instanzen angezeigt. Sie können die fehlgeschlagenen Instanzen entfernen und auf **Weiter**klicken.

   Wenn Sie auf einer Instanz nicht genügend Speicherplatz haben, können Sie den Speicherplatz überprüfen und bereinigen. Siehe ADC-Speicherplatz aufräumen.

   > **Wichtig**
   >
   > Wenn Sie die Cluster-IP-Adresse angeben, führt ADM die Validierung vor dem Upgrade nur für die angegebene Instanz und nicht auf den anderen Clusterknoten durch.

6. Optional geben Sie in **Custom scripts**die Scripts an, die vor und nach einem Instanzupgrade ausgeführt werden sollen. Verwenden Sie eine der folgenden Möglichkeiten, um die Befehle auszuführen:

   Die benutzerdefinierten Skripte werden verwendet, um die Änderungen vor und nach einem ADC-Instanz-Upgrade zu überprüfen. Beispiel:

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

   Ein Instanz-Upgrade hat mehrere Phasen. Sie können jetzt festlegen, dass diese Skripte in den folgenden Phasen ausgeführt werden:

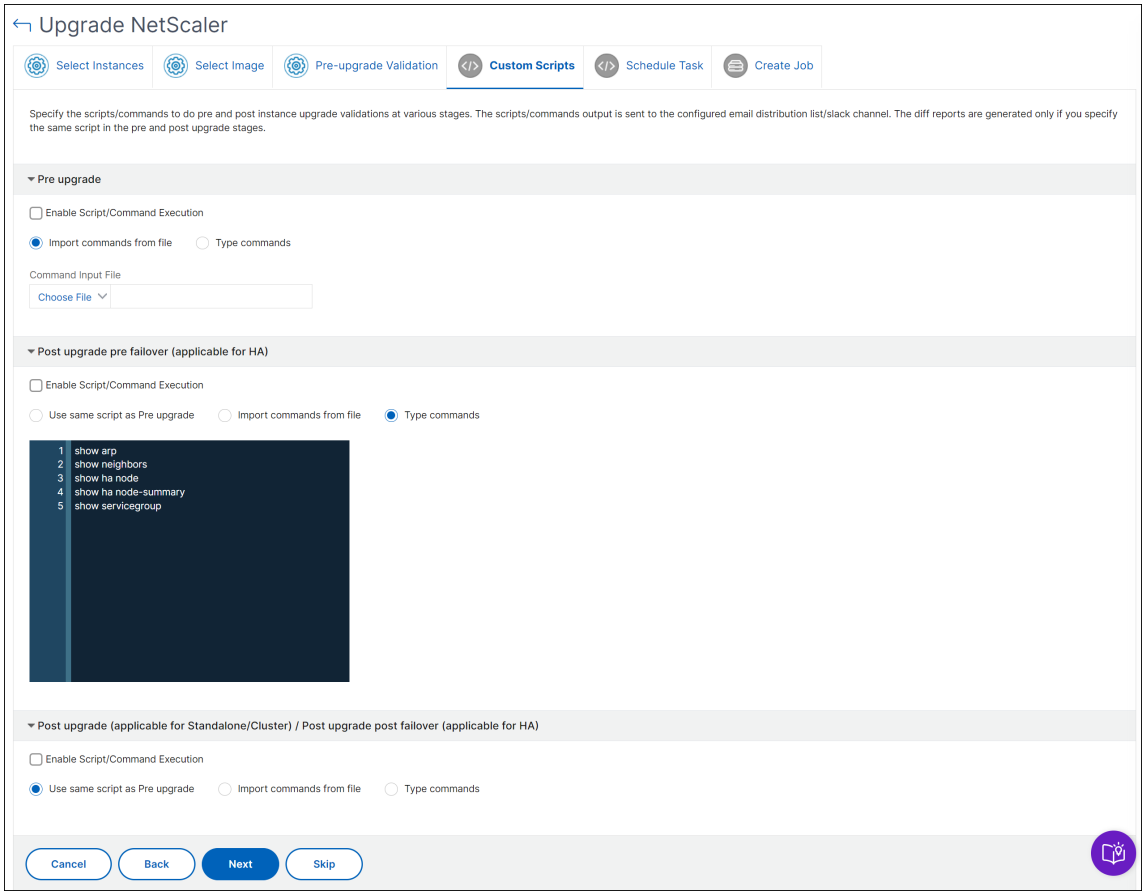
   - **Vor dem Upgrade**: Das angegebene Script wird vor dem Upgrade einer Instanz ausgeführt.
   - **Vorab-Failover nach dem Upgrade (gilt für HA)**: Diese Phase gilt nur für die Bereitstellung mit hoher Verfügbarkeit. Das angegebene Skript wird nach dem Upgrade der Knoten, jedoch vor ihrem Failover ausgeführt.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

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

Sie können eine Skriptdatei importieren oder Befehle direkt in die ADM-GUI eingeben.

- **Befehle aus Datei importieren**: Wählen Sie die Befehlseingabedatei von Ihrem lokalen Computer aus.
- **Type-Befehle**: Geben Sie Befehle direkt auf der GUI ein.

In den Phasen nach dem Upgrade können Sie das gleiche Skript verwenden, das in der Pre-Upgrade-Phase angegeben ist.



7. Wählen Sie unter **Task planen** eine der folgenden Optionen aus:

   - **Jetzt upgraden** - Der Upgrade-Auftrag wird sofort ausgeführt.
   - **Später planen** - Wählen Sie diese Option, um diesen Upgrade-Auftrag später auszuführen. Geben Sie das **Ausführungsdatum** und die **Startzeit** an, wenn Sie die Instanzen aktualisieren möchten.

Wenn Sie ein ADC-HA-Paar in zwei Stufen aktualisieren möchten, wählen Sie **Zweistufiges Upgrade für Knoten in HA durchführen**aus.

Geben Sie das **Ausführungsdatum** und die **Startzeit an**, zu der Sie eine andere Instanz im HA-Paar aktualisieren möchten.

8. Geben Sie unter **Job erstellen** die folgenden Details an:

   a) Wählen Sie eine der folgenden Optionen aus der Liste **Software-Image** aus:

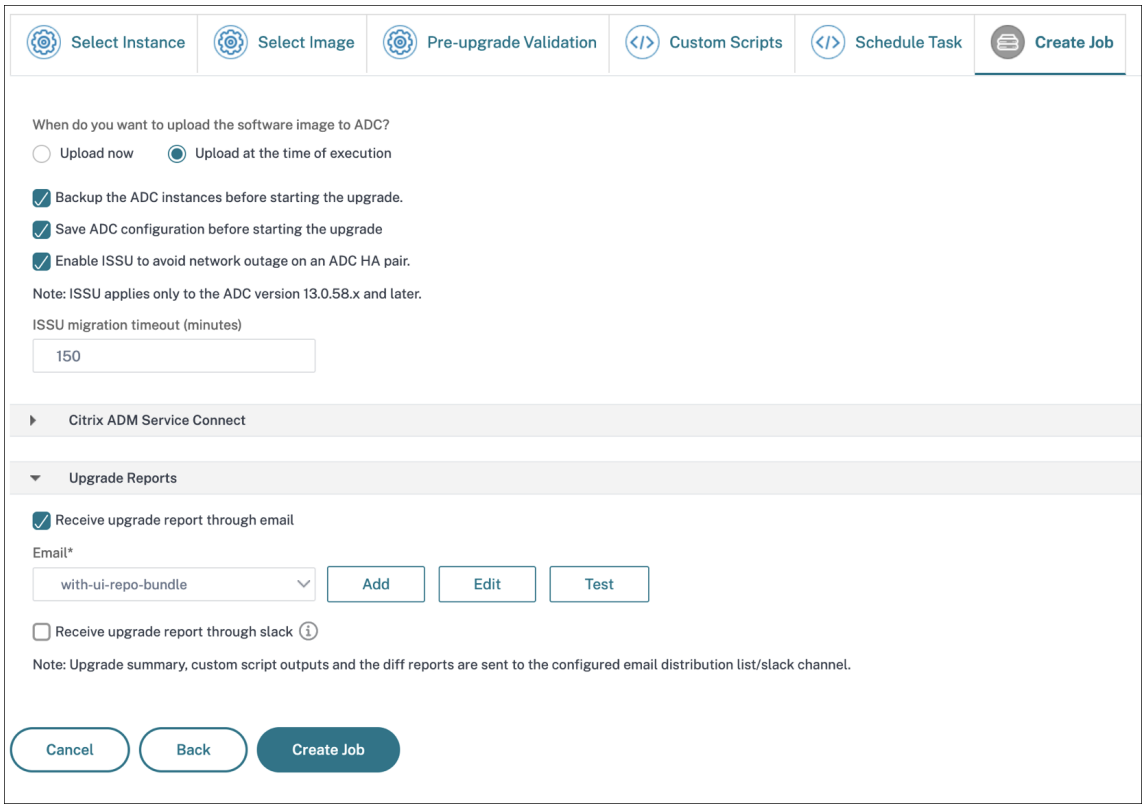
      - **Lokal** —Wählen Sie die Instanzupgradedatei von Ihrem lokalen Computer
      - **Appliance** —Wählen Sie die Instance-Upgrade-Datei in einem ADM-Dateibrowser aus. Die ADM-GUI zeigt die Instanzdateien an `/var/mps/ns_images`, die vorhanden sind.

   b) Geben Sie an, wann Sie das Image auf eine Instanz hochladen möchten:

      - **Jetzt hochladen** - Wählen Sie diese Option, um das Image sofort hochzuladen. Der Upgrade-Auftrag wird jedoch zum geplanten Zeitpunkt ausgeführt.
      - **Upload zum Zeitpunkt des Ausführens** - Wählen Sie diese Option, um das Image hochzuladen, wenn der Upgradeauftrag ausgeführt wird.

   - **Software-Image von NetScaler ADC bei erfolgreichem Upgrade bereinigen**: Wählen Sie diese Option, um das hochgeladene Image in der ADC-Instanz nach dem Instanz-Upgrade zu löschen.
   - **Erstellen Sie ein Backup der ADC-Instanzen, bevor Sie das Upgrade starten.** - Erstellt ein Backup der ausgewählten ADC-Instanzen.
   - **Behalten Sie den primären und sekundären Status von HA-Knoten nach dem Upgrade**bei: Wählen Sie diese Option, wenn der Upgrade-Auftrag nach dem Upgrade jedes Knotens ein Failover auslösen soll. Auf diese Weise behält der Upgrade-Job den primären und sekundären Status der Knoten bei.
   - **Speichern Sie die ADC-Konfiguration vor dem Start des Upgrades** - Speichert die laufende ADC-Konfiguration vor dem Upgrade der ADC-Instanzen.
   - **Aktivieren Sie ISSU, um Netzwerkausfälle beim ADC HA-Paar zu vermeiden** - ISSU stellt das Upgrade ohne Ausfallzeiten bei einem ADC-Hochverfügbarkeitspaar sicher. Diese Option bietet eine Migrationsfunktionalität, die die vorhandenen Verbindungen während des Upgrades berücksichtigt. Sie können also ein ADC HA-Paar ohne Ausfallzeiten aktualisieren. Geben Sie das Timeout der ISSU Migration in Minuten an.
   - **Ausführungsbericht per E-Mail empfangen** - Sendet den Ausführungsbericht per E-Mail. Informationen zum Hinzufügen einer E-Mail-Verteilerliste finden Sie unter Erstellen einer E-Mail-Verteilerliste.

- **Ausführungsbericht über Pufferzeit empfangen** - Sendet den Ausführungsbericht in Pufferzeit. Informationen zum Hinzufügen eines Slack-Profils findest du unter Erstellen eines Slack-Profils.



9. Klicken Sie auf **Job erstellen**.

Der Upgrade-Auftrag wird unter **Netzwerke > Konfiguration > Wartungsaufträge** angezeigt. Wenn Sie einen vorhandenen Job bearbeiten, können Sie zu allen Registerkarten wechseln, wenn die erforderlichen Felder bereits ausgefüllt sind. Wenn Sie sich beispielsweise auf der Registerkarte **Konfiguration auswählen** befinden, können Sie auf die Registerkarte **Job-Vorschau** wechseln.

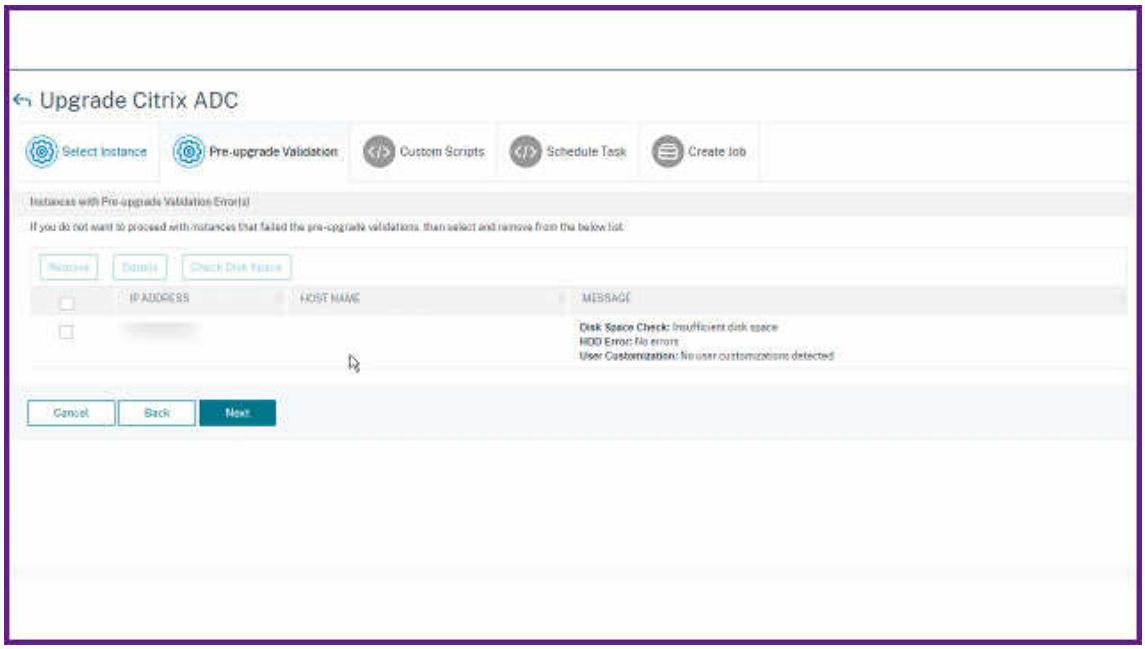
Bereinigen Sie den ADC-Speicherplatz

Wenn Sie beim Upgrade einer ADC-Instanz auf das Problem mit unzureichendem Speicherplatz stoßen, bereinigen Sie den Speicherplatz von der ADM-GUI selbst.

1. Wählen Sie auf der Registerkarte **Validierung vor dem Upgrade** die Instanz aus, die das Problem mit dem Speicherplatz hat.
2. Wählen Sie **Speicherplatz prüfen**aus.

   In diesem Bereich wird der Datenträger der Instanz mit geringem Speicherplatz angezeigt. Es zeigt auch an, wie viel Speicher auf dem Datenträger verwendet und verfügbar ist.

3. Wählen Sie im Bereich **Speicherplatz überprüfen** die Instanz aus, die eine Bereinigung erfordert.
4. Klicken Sie auf **Datenträgerbereinigung**.



5. Wählen Sie die Dateien aus, die Sie löschen möchten.
6. Klicken Sie auf **Löschen**

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

Sie können einen Diff-Bericht über einen ADC-Upgrade-Auftrag herunterladen, wenn benutzerdefinierte Skripts angegeben werden. Ein Diff-Bericht enthält die Unterschiede zwischen den Ausgaben des Pre-Upgrade- und Post-Upgrade-Skripts. Mit diesem Bericht können Sie bestimmen, welche Änderungen bei der ADC-Instanz nach dem Upgrade aufgetreten sind.

> **Hinweis**
>
> Der Diff-Bericht wird nur generiert, wenn Sie dasselbe Skript in den Phasen vor dem Upgrade und nach dem Upgrade angeben.

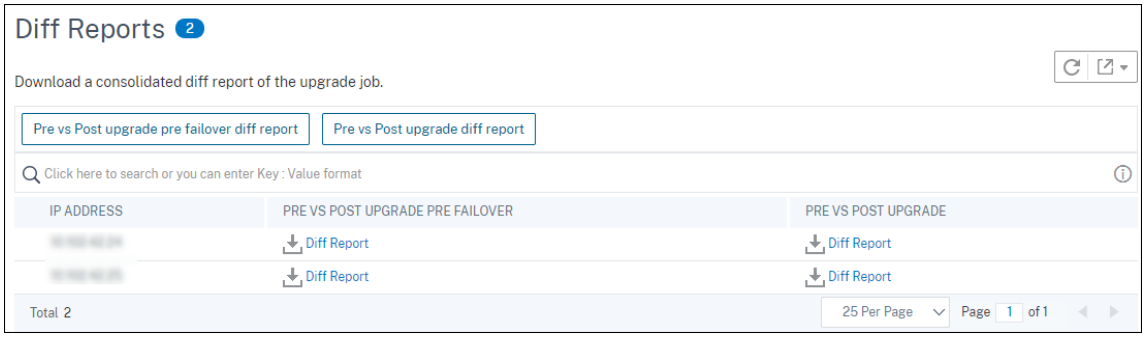
Um einen Diff-Bericht über einen Upgrade-Job herunterzuladen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Netzwerke > Konfigurationsjobs > Wartungsaufträge**.
2. Wählen Sie den Upgrade-Job aus, für den Sie einen Diff-Bericht herunterladen möchten.
3. Klicken Sie auf **Diff-Berichte**.

4. Laden Sie in **Diff Reports**einen konsolidierten Diff-Bericht des ausgewählten Upgrade-Jobs herunter.

   Auf dieser Seite können Sie einen der folgenden Arten von Diff-Berichten herunterladen:

   - **Vor und nach dem Upgrade vor dem Failover-Diff-Bericht**
   - **Diff-Bericht vor und nach dem Upgrade**



Konfigurationsvorlagen zum Erstellen von Überwachungsvorlagen verwenden

February 5, 2024

Sie können jetzt Konfigurationsbefehle verwenden, die zuvor als Konfigurationsvorlagen gespeichert wurden, um Überwachungsvorlagen zu erstellen, die auf bestimmte NetScaler ADC-Instanzen angewendet werden können. Beim Erstellen einer Prüfungsvorlage können Sie zuvor gespeicherte Konfigurationsvorlagen in das Feld Befehle ziehen und die Vorlage entsprechend Ihren Anforderungen bearbeiten. Anschließend können Sie die Überwachungsvorlage auf bestimmte NetScaler ADC-Instanzen anwenden. NetScaler ADM vergleicht diese Instanzen mit der Überwachungsvorlage und meldet etwaige Abweichung. Dieser Prozess hilft Ihnen, Fehler zu erkennen und rechtzeitig zu beheben.

Sie können Konfigurationsvorlagen erstellen, während Sie einen Auftrag erstellen und eine Reihe von Konfigurationsbefehlen als Vorlage speichern. Wenn Sie diese Vorlagen auf der Seite „ **Jobs erstellen** “speichern, werden sie automatisch auf der Seite „ Vorlage **erstellen** “angezeigt.

Betrachten Sie beispielsweise eine grundlegende Lastausgleichskonfiguration, für die Sie einen virtuellen Lastausgleichsserver hinzufügen, zwei Dienste hinzufügen und die Dienste an den virtuellen Server binden.

In diesem Beispiel werden die folgenden Befehle verwendet:

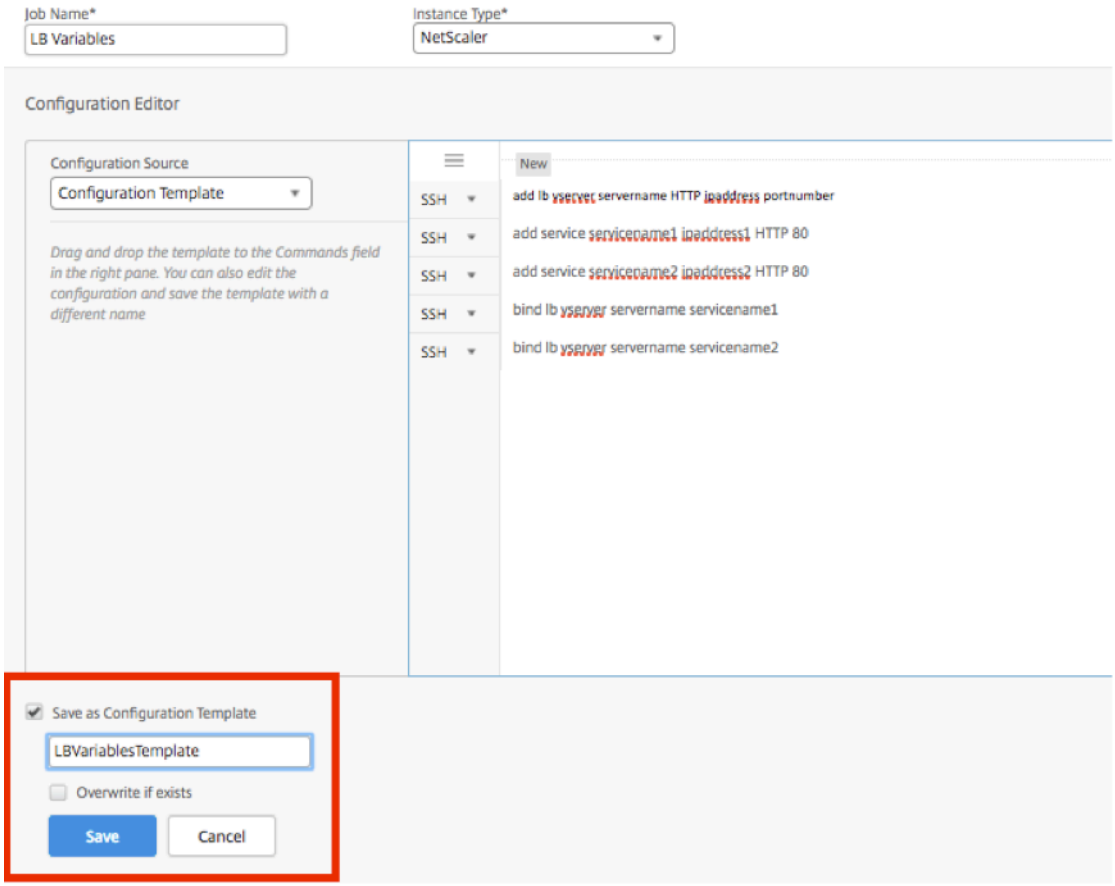
```
add lb vserver >servername> HTTP <ipaddress portnumber>
```



```
add service <servicename1 ipaddress1> HTTP 80
add service <servicename2 ipaddress2> HTTP 80
bind lb vserver <servername servicename1>
bind lb vserver <servername servicename2>
```

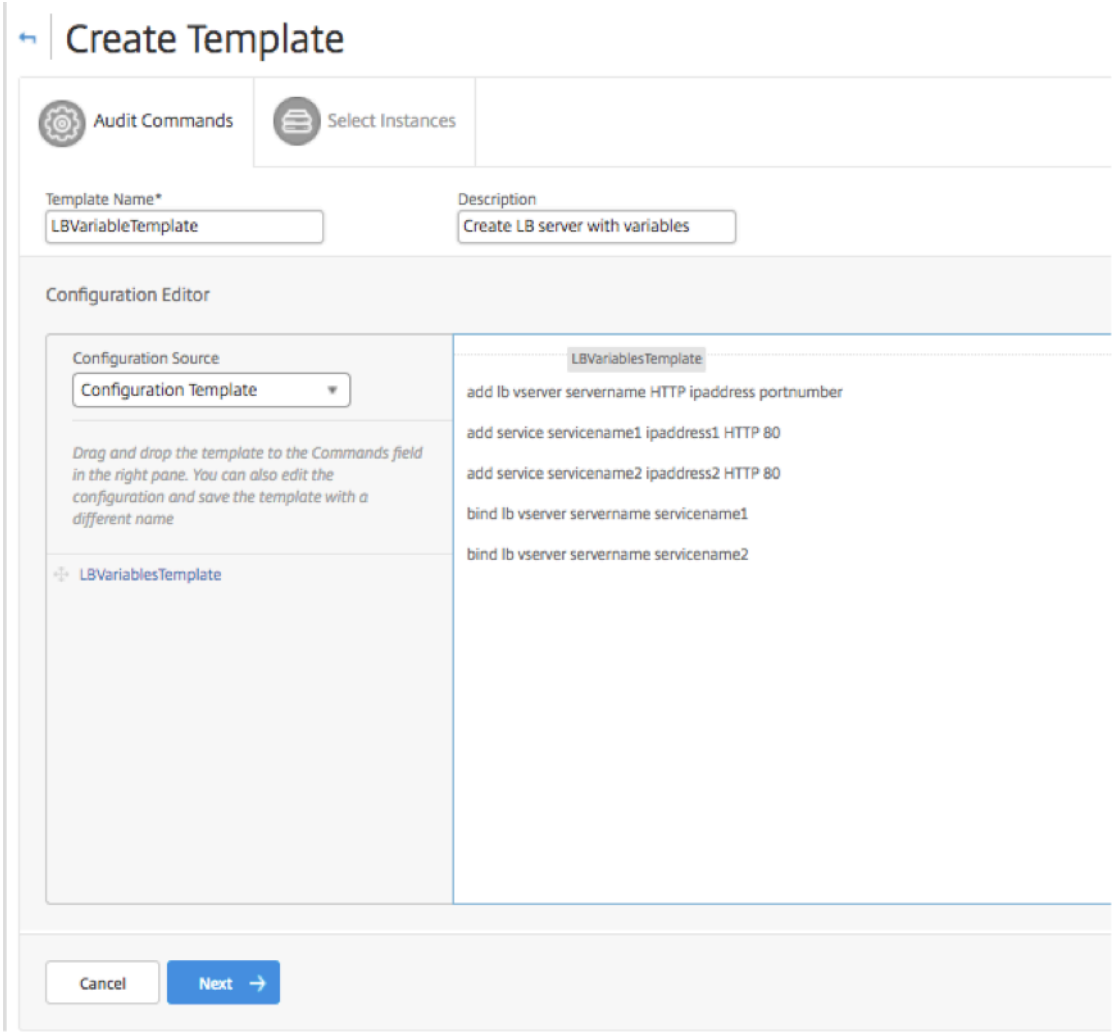
So speichern Sie eine Konfigurationsvorlage in NetScaler ADM:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge** und klicken Sie auf **Job erstellen**.
2. Geben Sie auf der Seite **Job erstellen** den Jobnamen und den Instanztyp an.
3. Wählen Sie als **Konfigurationsquelle die Option Konfigurationsvorlage** aus, und geben Sie im Feld **Befehle** Befehle wie die im obigen Beispiel angegebenen Befehle ein.
4. Aktivieren Sie das Kontrollkästchen **Als Konfigurationsvorlage speichern** und geben Sie einen Namen für Ihre Vorlage an. Sie können andere Vorlagen mit demselben Namen überschreiben.
5. Klicken Sie auf **Speichern**.



So erstellen Sie eine Überwachungsvorlage in NetScaler ADM mithilfe einer Konfigurationsvorlage:

1. Navigieren Sie zu **Netzwerke** > **Configuration Audit** > **Audit-Vorlagen**und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Vorlage erstellen** einen Namen für den Vorlagennamen an, und geben Sie eine Beschreibung ein.
3. Wählen Sie in der Liste **Konfigurationsquelle** die Option **Konfigurationsvorlage**aus, und ziehen Sie die Vorlage dann in das Feld Befehle im rechten Fensterbereich. Sie können die Konfiguration auch bearbeiten und die Vorlage unter einem anderen Namen speichern. Klicken Sie auf **Weiter**.
4. Klicken Sie auf der Registerkarte **Instanzen auswählen** auf **Instanzen hinzufügen** und fügen Sie die Instanzen hinzu, auf denen Sie die Konfiguration ausführen möchten. Klicken Sie auf **OK**.
5. Klicken Sie auf **Fertig stellen**.



Die Überwachungsvorlage wird in der Liste Überwachungsvorlagen angezeigt und wird alle 12 Stunden für die Konfigurationen der angegebenen Instanzen ausgeführt.

SCP-Befehl (put) in Konfigurationsaufträgen verwenden

February 5, 2024

Sie können die Konfigurationsaufträge von Citrix ADM verwenden, um Konfigurationsaufträge zu erstellen, E-Mail-Benachrichtigungen zu senden und Ausführungsprotokolle der erstellten Aufträge zu überprüfen. Ein Auftrag ist ein Satz von Konfigurationsbefehlen, die Sie auf einer einzelnen verwalteten Instanz oder auf mehreren verwalteten Instanzen erstellen und ausführen können. Sie können beispielsweise Konfigurationsaufträge für Geräte-Upgrades verwenden.

Konfigurationsaufträge in NetScaler ADM verwenden Secure Shell (SSH) -Befehle, um Instanzen zu konfigurieren, und Sie können einen Konfigurationsauftrag so konfigurieren, dass Secure Copy (SCP) zum sicheren Übertragen von Dateien verwendet wird. SCP basiert auf dem SSH-Protokoll. Einer der **SCP**-Befehle , die Sie in einen Konfigurationsjob aufnehmen können, ist der Befehl „put“. Sie können den Befehl put in Konfigurationsaufträgen verwenden, um eine oder mehrere Dateien, die in einem lokalen Verzeichnis auf Ihrem System gespeichert sind, in NetScaler ADM und dann in ein Verzeichnis auf der NetScaler ADC-Instanz oder -Instanzen hochzuladen oder zu übertragen.

> **Hinweis:** Die Datei wird auf Citrix ADM hochgeladen und später in die ausgewählten Citrix ADC-Instanzen kopiert (abgelegt). Die hochgeladene Datei wird in NetScaler ADM gespeichert und nur gelöscht, wenn der Auftrag gelöscht wird. Dies ist notwendig für Jobs, die später laufen sollen.

Der Befehl hat die folgende Syntax:

```
put <local_filename> <remote_path/remote_filename>
```

Hierbei gilt:

<local_filename> ist der Name der lokalen Datei, die hochgeladen werden soll.

<remote_path / remote_filename> ist der Pfad zu einem Remote-Verzeichnis und der Name, der der Datei zugewiesen werden soll, wenn sie in dieses Verzeichnis kopiert wird.

Beim Erstellen des Konfigurationsauftrags können Sie die Parameter für lokale und remote Dateinamen in Variablen konvertieren. Auf diese Weise können Sie diesen Parametern bei jeder Ausführung des Auftrags verschiedene Dateien für denselben Satz von NetScaler ADC-Instanzen zuweisen. Wenn Sie eine Datei an mehreren Stellen in einem Auftrag verwenden und die Datei umbenennen möchten, können Sie die Variable umdefinieren, anstatt den Dateinamen an allen Stellen zu ändern.

So verwenden Sie den Befehl put zum Hochladen von Dateien in einem Konfigurationsauftrag:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**.
2. Klicken Sie auf der Seite **Jobs** auf **Job erstellen**.

3. Geben Sie auf der Seite **Job erstellen** den Namen des Jobs in das Feld Jobname ein, und geben Sie im **Konfigurationseditor** den Befehl put ein.

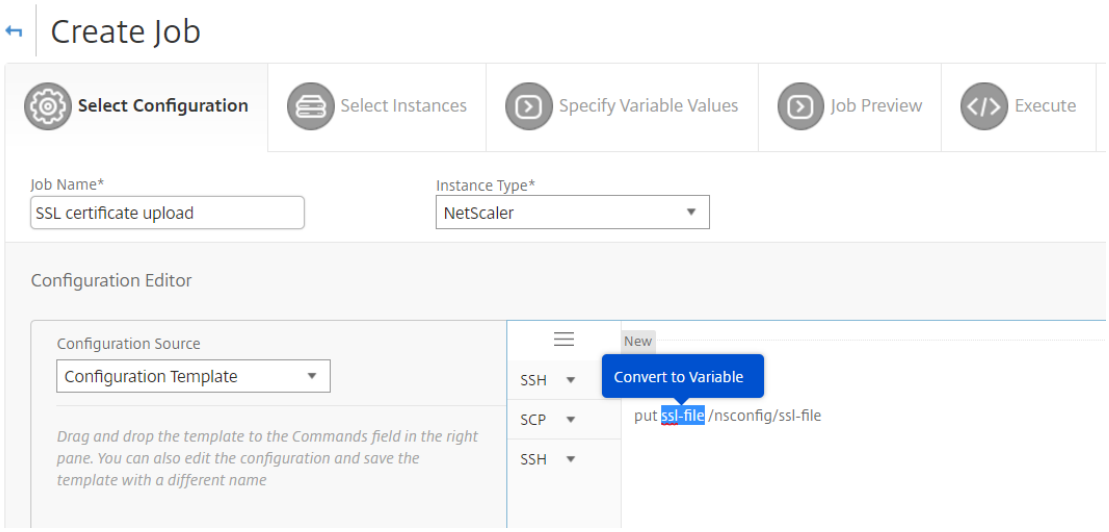
   Wenn Sie beispielsweise einen Konfigurationsauftrag erstellen möchten, der eine auf Ihrem lokalen System gespeicherte SSL-Zertifikatsdatei auf mehrere NetScaler ADC-Instanzen kopiert, können Sie einen "put"-Befehl hinzufügen, der eine Variable anstelle des Namens einer bestimmten Datei verwendet, und den Variablentyp als "Datei"definieren.

   ```
   put ssl-file /nsconfig/ssl-file
   ```

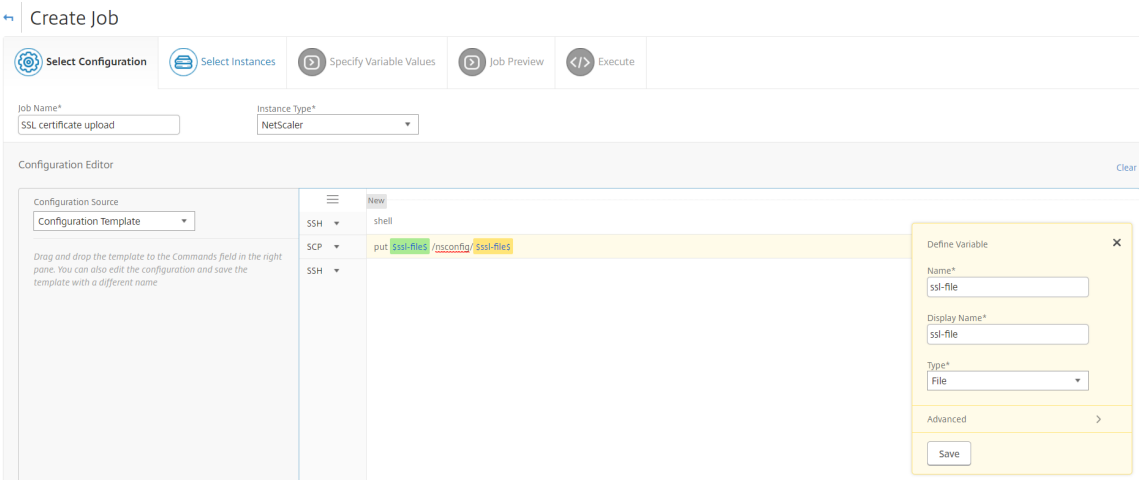
   In diesem Beispiel wird

   - `ssl-file` - Dies ist der Name der Datei, die in die NetScaler ADC-Instanz hochgeladen werden muss.
   - `/nsconfig/ssl-file` - Dies ist der Zielordner in der Instanz, in den der nach der Ausführung der Aufgabe abgelegt `ssl-file` wird.

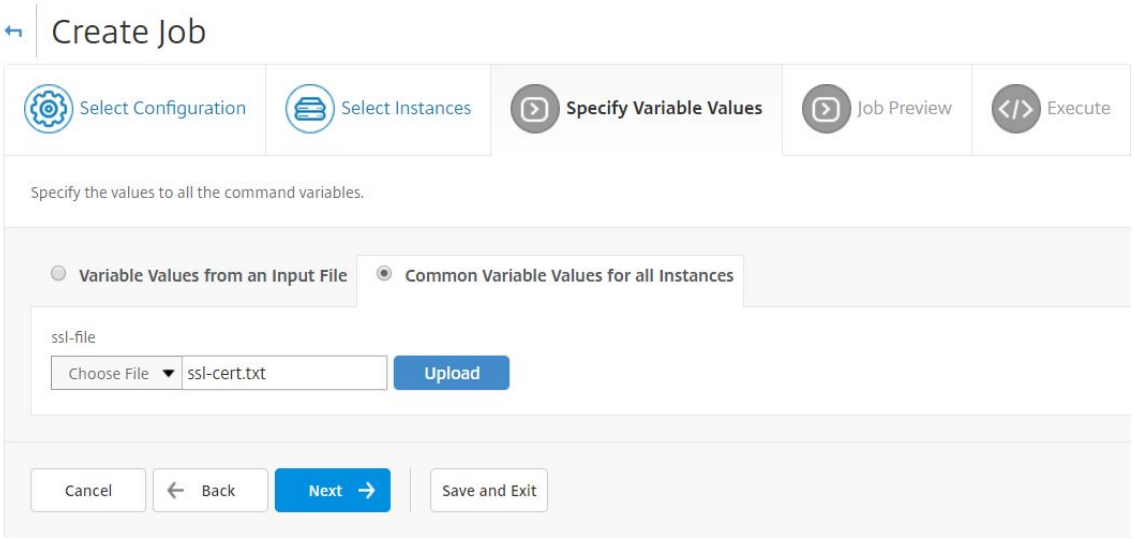
4. Wählen Sie in dem eingegebenen Befehl den Dateinamen aus, den Sie in eine Variable konvertieren möchten, und klicken Sie dann auf In**Variable umwandeln**, wie in der folgenden Abbildung dargestellt.



5. Stellen Sie sicher, dass der Dateiname von Dollarzeichen enthalten ist (die darauf hinweisen, dass es sich jetzt um eine Variable handelt), und klicken Sie dann auf die Variable.
6. Geben Sie die Details der Variablen an, wie Name, Anzeigename und Typ.
7. Wählen **Sie in der Dropdownliste Typ** die Option **Datei**aus. Klicken Sie auf **Speichern**. Wenn Sie die Variable als Dateityp deklarieren, können Sie Dateien in NetScaler ADM hochladen.

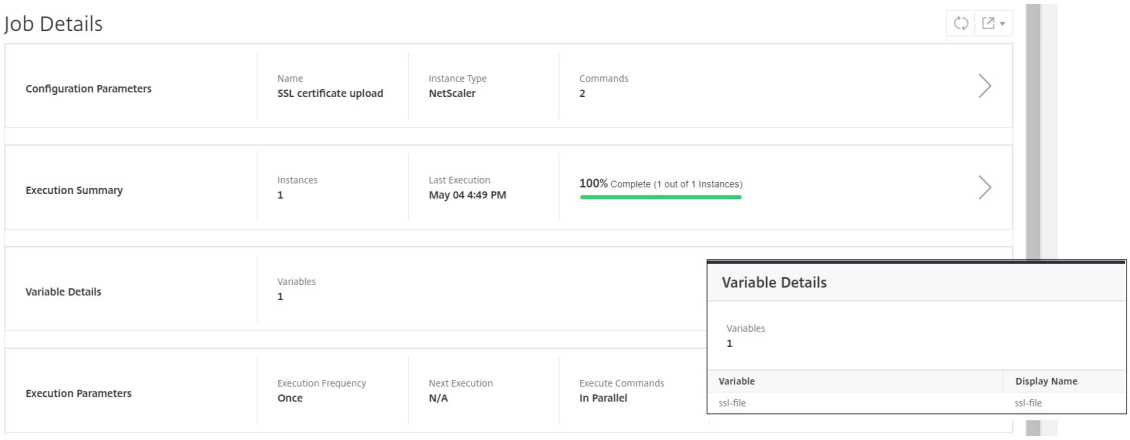


8. Klicken Sie auf**Weiter**, und wählen Sie die NetScaler ADC Instanzen aus, in die die Dateien kopiert werden sollen.
9. Wählen Sie auf der Registerkarte **Variablenwerte angeben** den Abschnitt **Allgemeine Variablenwerte für alle Instanzen**, wählen Sie die Datei aus dem lokalen Speicher auf Ihrem System aus, klicken Sie auf**Hochladen**, um die Datei in NetScaler ADM hochzuladen, und klicken Sie auf**Weiter**.



10. Auf der Registerkarte**Auftragsvorschau**können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.
11. Auf der Registerkarte**Ausführen**können Sie den Job jetzt ausführen oder planen, dass er später ausgeführt wird. Sie können auch auswählen, welche Aktion NetScaler ADM ausführen muss, wenn der Befehl fehlschlägt. Sie können auch eine E-Mail-Benachrichtigung erstellen, um Benachrichtigungen über den Erfolg oder Misserfolg des Auftrags und andere Details zu erhalten. Klicken Sie auf **Fertig stellen**.

12. Sie können die Auftragsdetails anzeigen, indem Sie zu**Netzwerke** >**Konfigurationsaufträge**navigieren und den von Ihnen konfigurierten Job auswählen. Klicken Sie auf **Details**, und klicken Sie dann auf **Variablendetails**, um die Variablen aufzulisten, die Ihrem Auftrag hinzugefügt wurden.



Neuplanen von Jobs, die mit integrierten Vorlagen konfiguriert wurden

February 5, 2024

Sie können einen geplanten Auftrag mithilfe integrierter Vorlagen in Citrix Application Delivery Management (ADM) neu planen. Sie können beispielsweise die Aktion ändern, die NetScaler ADM ausführen muss, wenn ein Befehl fehlschlägt. Wenn Sie zuvor entschieden hatten, einen Fehler zu ignorieren und fortzufahren, können Sie ihn so ändern, dass alle erfolgreichen Befehle zurückgesetzt werden, wenn ein Befehl fehlschlägt.

So planen Sie einen Auftrag neu, der mithilfe integrierter Vorlagen in NetScaler ADM konfiguriert wurde

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge**.
2. Wählen Sie den Job aus, den Sie bearbeiten möchten, fügen Sie Instanzen hinzu oder entfernen Sie sie, geben Sie Variablenwerte an und ändern Sie dann Ausführungsaktionen und -einstellungen.
3. Klicken Sie auf **Fertigstellen**, um den Auftrag neu zu planen

> **Hinweis**
>
> Sie können den Job auch auswählen und auf **Erneut ausführen** klicken, um den Job auszuführen, ohne Quelle, Instanz und Befehle zu ändern. Diese Funktion ist nützlich,

> wenn Sie dieselben Befehle für dieselben Instanzen ausführen müssen. Manchmal tritt der Auftrag möglicherweise auf einen vorübergehenden Fehler von der Serverseite auf, und Sie müssen den Auftrag möglicherweise erneut ausführen.

Konfigurationsüberwachungsvorlagen in Konfigurationsaufträgen wiederverwenden

February 5, 2024

Als Administrator können Sie Konfigurationsbefehle jetzt als Satz wiederverwendbarer Konfigurationsvorlagen speichern, wenn Sie einen Job erstellen und ein Konfigurationsaudit ausführen. Die in Configuration Jobs erstellte und gespeicherte Konfigurationsvorlage ist in Configuration Audit verfügbar, um eine Prüfungsvorlage zu erstellen, die auf bestimmte Citrix ADC-Instanzen angewendet werden kann. Ebenso ist die im Konfigurationsüberwachungsmodul erstellte Überwachungsvorlage in Konfigurationsaufträgen verfügbar, sodass Sie die Vorlage als Konfigurationsauftrag ausführen können. Jede in der Vorlage vorgenommene Änderung ist nun sowohl in den Konfigurationsaufträgen als auch in den Konfigurationsüberwachungsmodulen sichtbar.

Zuvor mussten die Konfigurationsjob- und Konfigurationsüberprüfungsvorlagen für dieselbe Konfiguration separat erstellt und als unterschiedliche Dateien gespeichert werden. Dies führte zu einem doppelten Aufwand bei der Erstellung und Pflege der Vorlagen.

Mit Citrix Application Delivery Management (ADM) können Sie diese Vorlage im System speichern, sodass die Überwachungsvorlage auch in Konfigurationsaufträgen verfügbar ist. Jetzt können die Überwachungsvorlagen zum Erstellen von Konfigurationsaufträgen verwendet werden. Auf diese Weise können die Vorlagen synonym zwischen Konfigurationsaufträgen und Konfigurationsaudits verwendet werden.

Betrachten Sie beispielsweise eine grundlegende Lastausgleichskonfiguration, für die Sie einen virtuellen Lastausgleichsserver hinzufügen, zwei Dienste hinzufügen und die Dienste an den virtuellen Server binden.

In diesem Beispiel werden die folgenden Befehle verwendet:

```
add lb vserver servername HTTP ipaddress portnumber

add service servicename1 ipaddress1 HTTP 80

add service servicename2 ipaddress2 HTTP 80

bind lb vserver servername servicename1

bind lb vserver servername servicename2
```



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

Erstellen einer Vorlage in Konfigurationsprüfungen und Wiederverwenden in Konfigurationsaufträgen

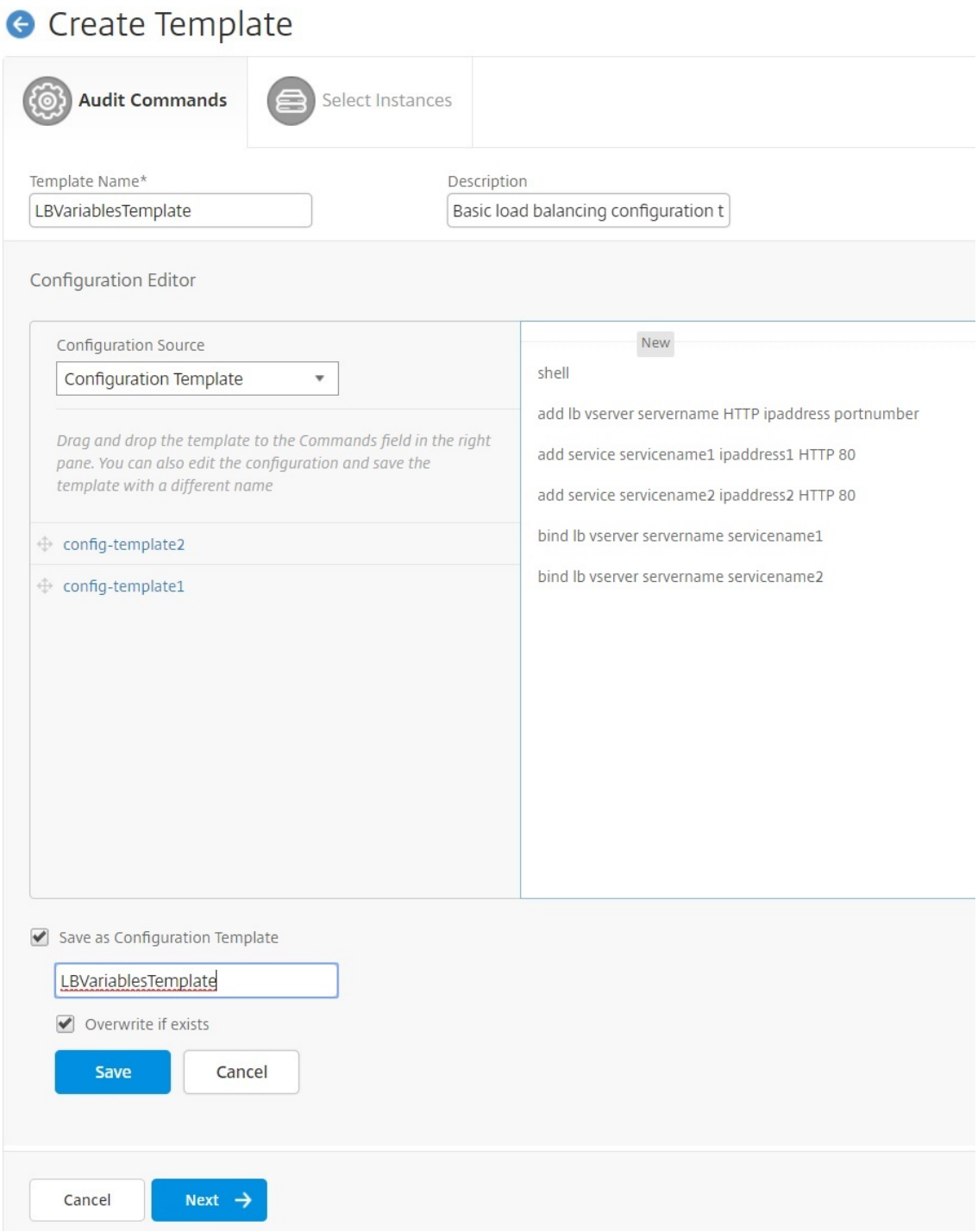
Führen Sie die folgende Aufgabe aus, um eine Vorlage für das Konfigurationsüberwachungsmodul zu erstellen und diese im Modul für Konfigurationsaufträge wiederzuverwenden.

So erstellen Sie eine Überwachungsvorlage:

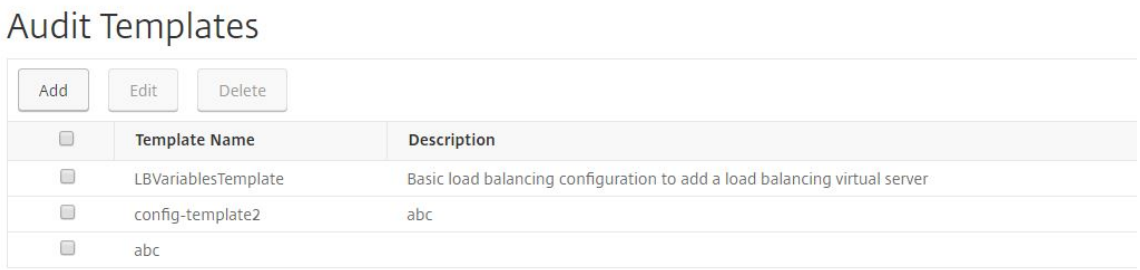
1. Navigieren Sie in NetScaler ADM zu**Netzwerke > Konfigurationsprüfung > Auditvorlage**, und klicken Sie auf**Hinzufügen**.
2. Geben Sie auf der Seite **Vorlage erstellen** den Namen der Vorlage an. Sie können auch weitere Informationen zur Vorlage im Feld **Beschreibung** hinzufügen.
3. Geben Sie im Bereich **Befehle** Befehle aus dem Beispiel ein.
4. Aktivieren Sie das Kontrollkästchen **Als Konfigurationsvorlage speichern** und geben Sie einen Namen für Ihre Vorlage an, z. B. können Sie diese Vorlage als “LBVariablesTemplate”bezeichnen. Sie können andere Vorlagen mit demselben Namen überschreiben.

   > **Hinweis:** Der Name der Prüfvorlage kann mit dem Namen der Konfigurationsvorlage identisch sein.

5. Klicken Sie auf **Speichern** und dann auf **Weiter**.



6. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Registerkarte **Instanzen auswählen** die **Citrix ADC-Instanzen** aus, auf denen Sie diese Konfigurationsbefehle ausführen möchten, und klicken Sie auf **Fertig stellen**. Die neue Vorlage ist nun in der Liste der Überwachungsvorlagen sichtbar.



8. ****Wenn Sie diese Konfigurationsbefehle ausführen möchten, navigieren Sie zu Netzwerke > Konfigurationsaufträge und klicken Sie auf **Job erstellen** . Die zuvor erstellte Überwachungsvorlage wird als Konfigurationsvorlage aufgeführt.

So verwenden Sie die Überwachungsvorlage in Konfigurationsaufträgen erneut:

1. Geben Sie einen Namen für den Auftrag ein, wählen Sie den Instanztyp aus und ziehen Sie die Vorlage in den Bereich "Befehle".

   Beim Erstellen des Konfigurationsauftrags können Sie die Parameter für lokale und remote Dateinamen in Variablen konvertieren. Auf diese Weise können Sie diesen Parametern bei jeder Ausführung des Auftrags verschiedene Dateien für denselben Satz von NetScaler ADC-Instanzen zuweisen.

2. Wählen Sie in dem eingegebenen Befehl den Dateinamen aus, den Sie in eine Variable konvertieren möchten, und klicken Sie dann auf **In Variable konvertieren**.
3. Wählen Sie auf der Registerkarte **Instanzen auswählen** die Instanzen aus, auf denen Sie diese Befehle ausführen möchten.
4. Wenn Sie in den Befehlen Variablen angegeben haben, wählen Sie auf der Registerkarte **Variablenwerte angeben** eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:

   - Variablenwerte aus einer Eingabedatei —Laden Sie eine Eingabedatei herunter, um Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den Citrix ADM Server hoch.
   - Allgemeine Variablenwerte für alle Instanzen —Geben Sie die IP-Adresse und den Port des Syslog-Servers an.

5. Auf der Registerkarte**Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen, und klicken Sie auf **Weiter**.
6. Klicken Sie auf der Registerkarte**Ausführen** auf **Fertig stellen**, um den Konfigurationsauftrag auszuführen. Wenn Sie nun einen anderen Dienst zu diesem Lastausgleichsserver hinzufügen

und den Dienst an den Server binden möchten, können Sie die Befehle auf der Befehlsseite bearbeiten und speichern.

7. Navigieren Sie zu **Überwachungsvorlagen**, und klicken Sie auf **Hinzufügen**.
8. Ziehen Sie die Vorlage "LBVariablesTemplate"in den Bereich "Befehle". Sie können sehen, dass die Vorlage mit den neuen Befehlen aktualisiert wurde.

Die Überwachungsvorlage wird in der Liste Überwachungsvorlagen angezeigt und wird alle 12 Stunden für die Konfigurationen der angegebenen Instanzen ausgeführt. Sie können jetzt Vorlagen erstellen und sie zwischen Konfigurationsaufträgen und Konfigurationsüberwachungsmodulen wiederverwenden.

Konfigurationsvorlagen importieren und exportieren

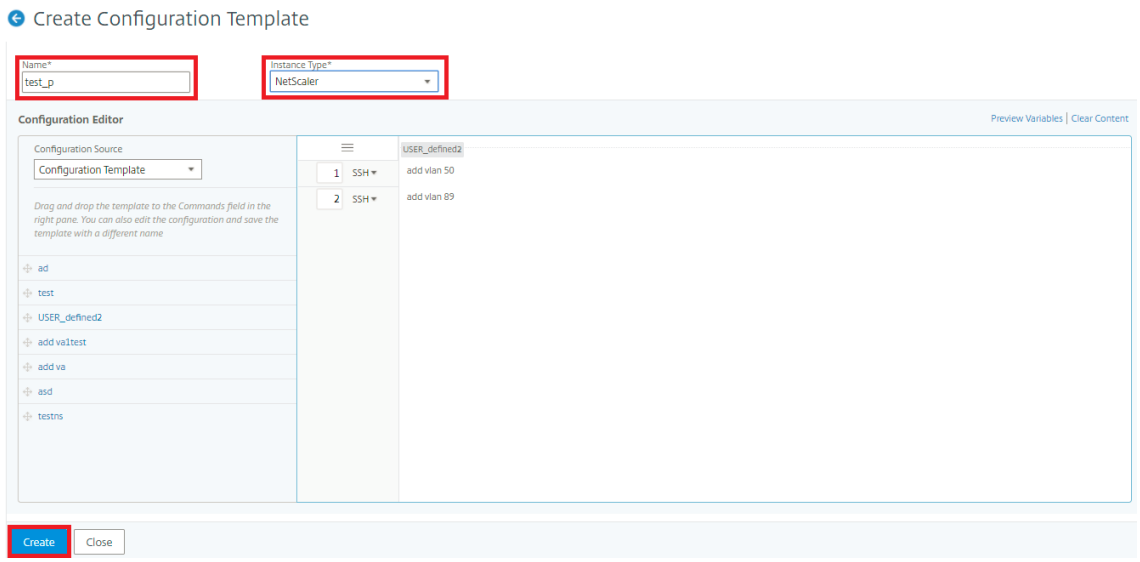
February 5, 2024

Sie können die Konfigurationsvorlagen aus jedem Citrix Application Delivery Management (ADM) exportieren. Sie können die Datei auch jederzeit in dasselbe oder ein anderes Citrix ADM importieren. Die Daten der Konfigurationsvorlagen (wie Konfigurationsbefehle, Variablendefinitionen und Parameter) gehen nicht verloren.

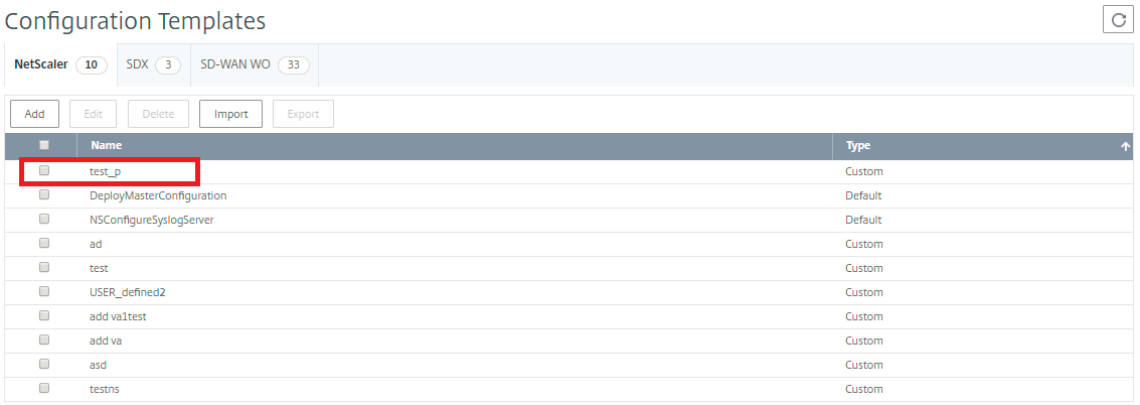
Sie können die Konfigurationsvorlagen in ein **JSON-Dateiformat** exportieren und im lokalen Ordner speichern. Sie können eine Konfigurationsvorlage importieren.**JSON-Dateien** in Citrix ADM. Diese Datei ist möglicherweise neu oder die, die Sie aus demselben oder einem anderen Citrix ADM exportiert haben.

So exportieren Sie die Konfigurationsvorlagen:

1. Navigieren Sie zu **Netzwerke > Konfigurationsjobs > Konfigurationsvorlagen**.
2. Klicken Sie auf die Schaltfläche "**Hinzufügen** ", um die Konfigurationsvorlage zu erstellen.
3. Geben Sie auf der Seite **Konfigurationsvorlage erstellen** den Namen der Konfigurationsvorlage an, und wählen Sie den Instanztyp aus. Wählen Sie unter **Konfigurationseditor**Konfigurationsquelle als Konfigurationsvorlage aus dem Dropdownmenü aus. Sie können die vorhandenen Konfigurationsvorlagen in den Konfigurationseditor ziehen. Klicken Sie auf **Erstellen**.



4. Navigieren Sie zu **Netzwerke > Konfigurationsjobs > Konfigurationsvorlagen**, um die in der Liste der Konfigurationsvorlagen erstellten Vorlagen anzuzeigen.



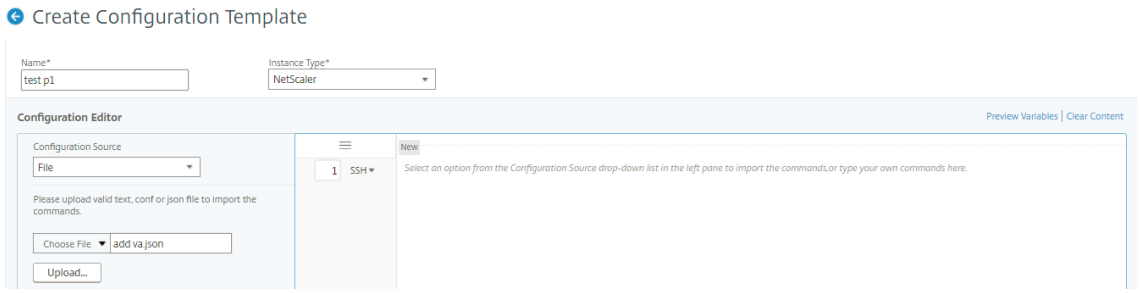
5. Wählen Sie die neu erstellte Konfigurationsvorlage aus, und klicken Sie auf die Schaltfläche **Exportieren**.

Die entsprechende Konfigurationsvorlage wird im **JSON-Format** auf Ihrem lokalen System heruntergeladen.

So importieren Sie die Konfigurationsvorlagen:

1. Navigieren Sie zu **Netzwerke > Konfigurationsjobs > Konfigurationsvorlagen** und klicken Sie auf die Schaltfläche **Importieren**. Wählen Sie den Pfad aus, in dem die **JSON-Dateien** der Konfigurationsvorlage sind und laden Sie die **JSON-Dateien** hoch. Es wird empfohlen, die **JSON-Dateien** hochzuladen, die Sie bereits exportiert haben.
2. Sie können die Konfigurationsvorlage auch mit der Option **Datei** im Konfigurationseditor importieren.
3. Wählen Sie im **Konfigurationseditor** im Drop-down-Menü die Option **Datei**aus.

4. **Wählen Sie Datei auswählen** (.**JSON-Dateien**) von Ihrem lokalen System aus und laden Sie die Konfigurationsvorlage hoch.**JSON-Dateien**.



> **Hinweis**
>
> - Jede neue importierte Vorlage wird mit einer neuen ID-Zeichenfolge gespeichert.
> - Sie können die Konfigurationsvorlagen nur importieren, wenn die Datei in der gespeichert ist. **JSON**-Format . Wenn Sie andere Konfigurationsvorlagen als **JSON-Dateien** aus Ihrem lokalen System importieren, wird ein Fehler angezeigt und der Import der Dateien schlägt fehl.

Wartungsaufträge

February 5, 2024

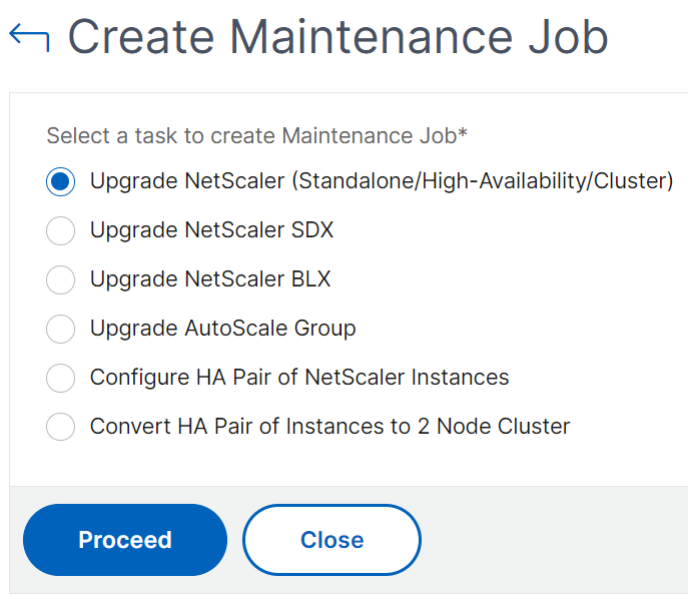
Sie können die folgenden Wartungsjobs mit Citrix ADM erstellen. Anschließend können Sie die Wartungsarbeiten an einem bestimmten Datum und zu einer bestimmten Uhrzeit planen.

- Upgrade von NetScaler ADC-Instanzen
- Aktualisieren von Citrix ADC SD WAN-WO-Instanzen
- Upgrade von NetScaler ADC SDX-Instanzen
- Aktualisieren von NetScaler ADC-Instanzen in der Autoscale-Gruppe
- HA-Paar der NetScaler ADC-Instanzen konfigurieren
- HA-Instanzen in Cluster mit 2 Knoten konvertieren

Upgrades der NetScaler ADC-Instanzen planen

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Job erstellen**.

2. Wählen Sie unter **Wartungsaufträge erstellen**die Option **NetScaler ADC (Standalone/Hochverfügbarkeit/Cluster) aktualisieren** aus und klicken Sie auf **Fortfahren**.



3. Geben Sie unter **Instanz auswählen**einen Namen Ihrer Wahl für **Auftragsname ein**.
4. Klicken Sie auf **Instanzen hinzufügen**, um ADC-Instanzen hinzuzufügen, die Sie aktualisieren möchten.

   - Um ein HA-Paar zu aktualisieren, geben Sie die IP-Adresse des primären oder sekundären Knotens an. Es wird jedoch empfohlen, die primäre Instanz zum Upgrade des HA-Paars zu verwenden.
   - Um einen Cluster zu aktualisieren, geben Sie die Cluster-IP-Adresse an.

5. Klicken Sie auf **Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten.

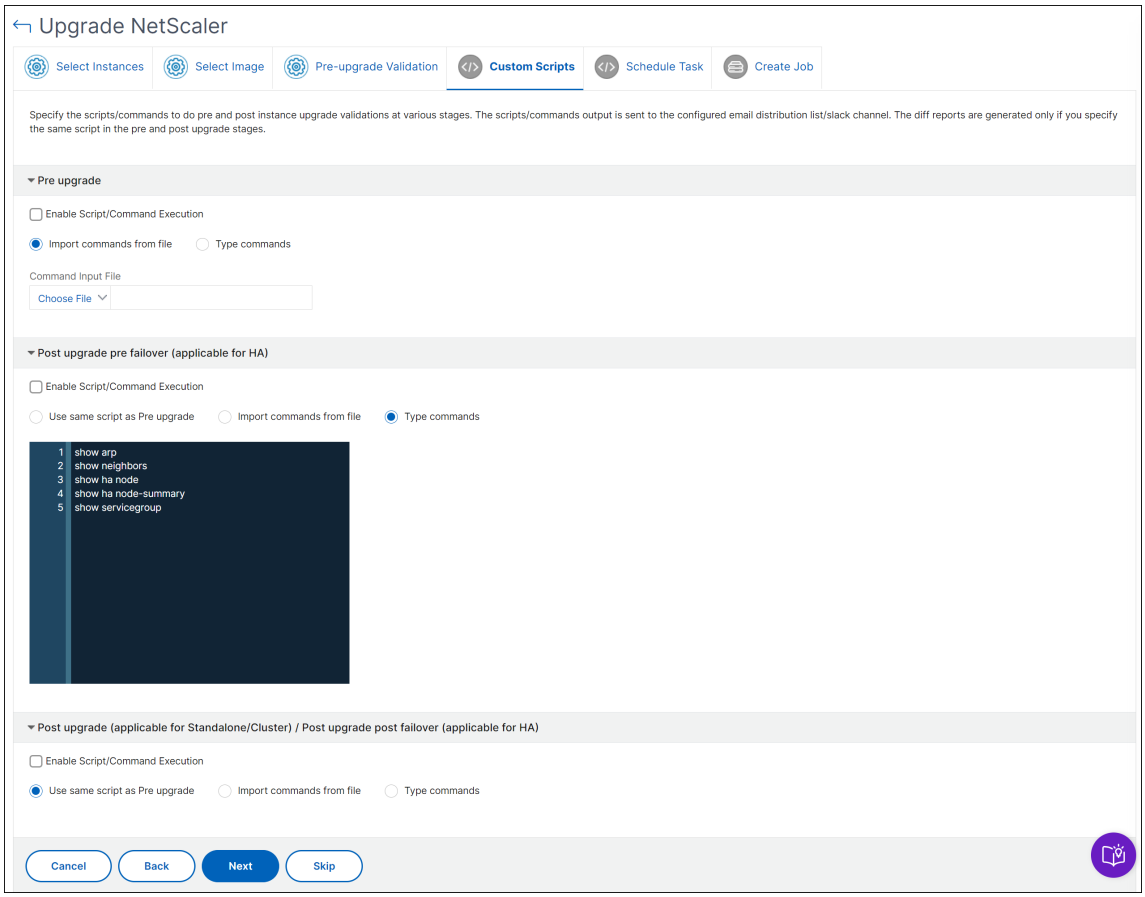
   Auf der Registerkarte **Überprüfung vor dem Upgrade** werden die ausgefallenen Instanzen

angezeigt Entfernen Sie die fehlerhaften Instanzen und klicken Sie auf **Weiter**

> **Wichtig**
>
> Wenn Sie die Cluster-IP-Adresse angeben, führt ADM die Validierung vor dem Upgrade nur für die angegebene Instanz und nicht auf den anderen Clusterknoten durch.

6. Optional geben Sie in **Custom scripts**die Scripts an, die vor und nach einem Instanzupgrade ausgeführt werden sollen. Verwenden Sie eine der folgenden Möglichkeiten, um die Befehle auszuführen:

   - **Befehle aus Datei importieren** - Wählen Sie die Befehlseingabedatei von Ihrem lokalen Computer aus.
   - **Befehle eingeben** - Geben Sie Befehle direkt auf der GUI ein.



Sie können benutzerdefinierte Skripts verwenden, um die Änderungen vor und nach einem Instanz-Upgrade zu überprüfen. Beispiel:

- Die Instanzversion vor und nach dem Upgrade.
- Der Status von Schnittstellen, Hochverfügbarkeitsknoten, virtuellen Servern und Diensten vor und nach dem Upgrade.

- Die Statistik der virtuellen Server und Dienste.
- Die dynamischen Routen.

7. Wählen Sie unter **Task planen** eine der folgenden Optionen aus:

   - **Jetzt upgraden** - Der Upgrade-Auftrag wird sofort ausgeführt.
   - **Später planen** - Wählen Sie diese Option, um diesen Upgrade-Auftrag später auszuführen. Geben Sie das **Ausführungsdatum** und die **Startzeit** an, wenn Sie die Instanzen aktualisieren möchten.

     Wenn Sie ein ADC-HA-Paar in zwei Stufen aktualisieren möchten, wählen Sie **Zweistufiges Upgrade für Knoten in HA durchführen**aus.

     Geben Sie das **Ausführungsdatum** und die **Startzeit an**, zu der Sie eine andere Instanz im HA-Paar aktualisieren möchten.

8. Geben Sie unter **Job erstellen** die folgenden Details an:

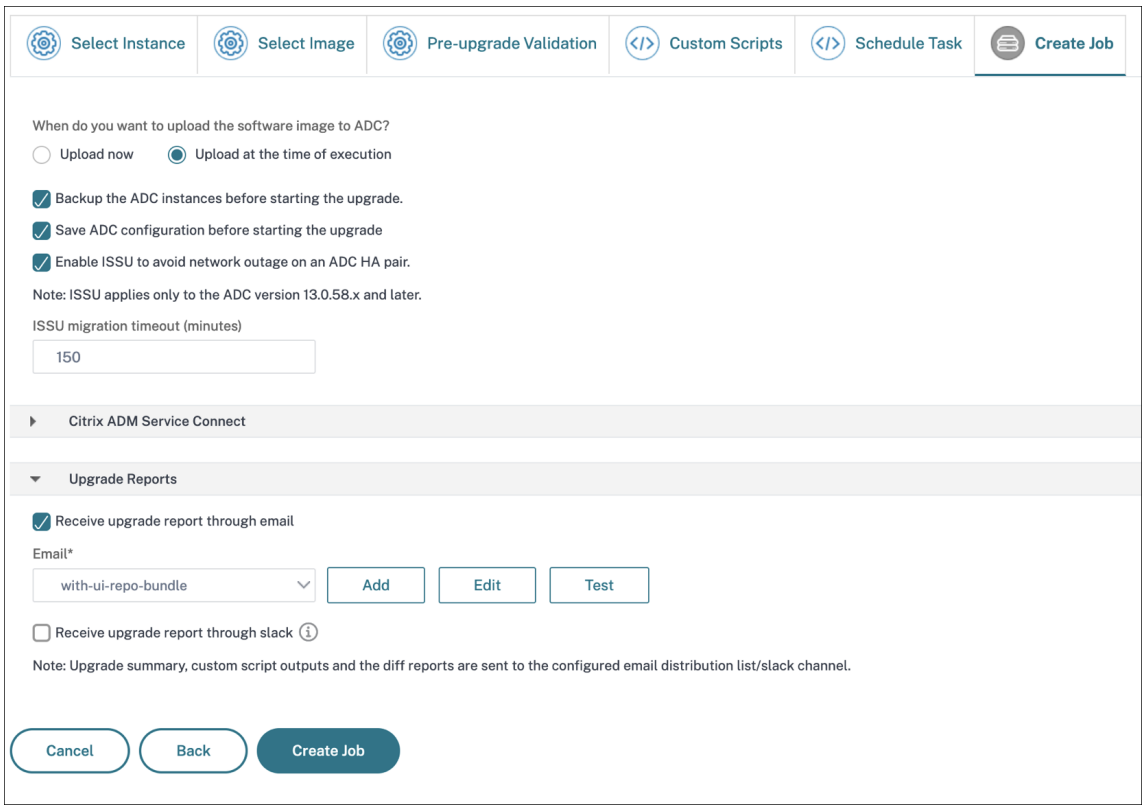
   a) Wählen Sie eine der folgenden Optionen aus der Liste **Software-Image** aus:

      - **Lokal** —Wählen Sie die Instanzupgradedatei von Ihrem lokalen Computer
      - **Appliance** —Wählen Sie die Instance-Upgrade-Datei in einem ADM-Dateibrowser aus. Die ADM-GUI zeigt die Instanzdateien an `/var/mps/mps_images`, die vorhanden sind.

   b) Geben Sie an, wann Sie das Image auf eine Instanz hochladen möchten:

      - **Jetzt hochladen** - Wählen Sie diese Option, um das Image sofort hochzuladen. Der Upgrade-Auftrag wird jedoch zum geplanten Zeitpunkt ausgeführt.
      - **Upload zum Zeitpunkt des Ausführens** - Wählen Sie diese Option, um das Image hochzuladen, wenn der Upgradeauftrag ausgeführt wird.

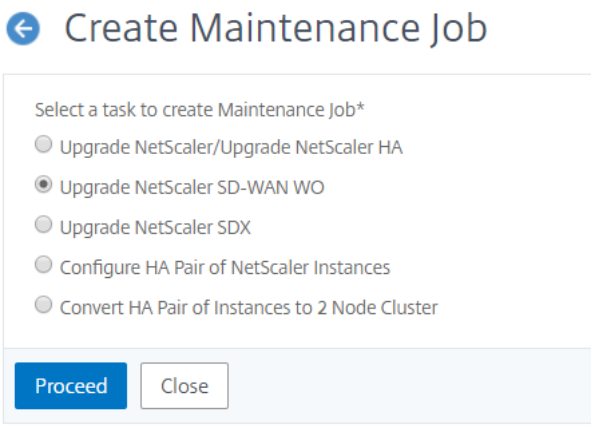
   - **Software-Image von NetScaler ADC bei erfolgreichem Upgrade bereinigen**: Wählen Sie diese Option, um das hochgeladene Image in der ADC-Instanz nach dem Instanz-Upgrade zu löschen.
   - **Erstellen Sie ein Backup der ADC-Instanzen, bevor Sie das Upgrade starten.** - Erstellt ein Backup der ausgewählten ADC-Instanzen.
   - **Ausführungsbericht per E-Mail empfangen** - Sendet den Ausführungsbericht per E-Mail. Informationen zum Hinzufügen einer E-Mail-Verteilerliste finden Sie unter Erstellen einer E-Mail-Verteilerliste.
   - **Ausführungsbericht über Pufferzeit empfangen** - Sendet den Ausführungsbericht in Pufferzeit. Informationen zum Hinzufügen eines Slack-Profils findest du unter Erstellen eines Slack-Profils.



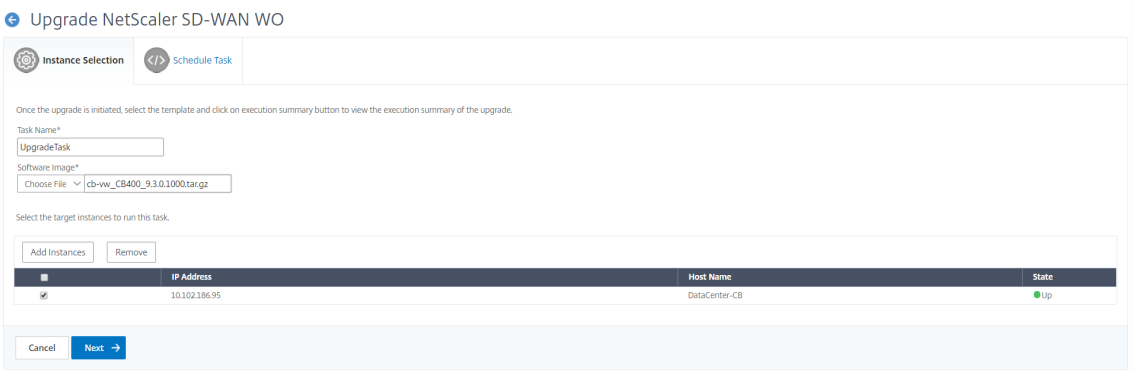
9. Klicken Sie auf **Job erstellen**.

Planen des Upgrades von NetScaler ADC SD-WAN WO-Instanzen

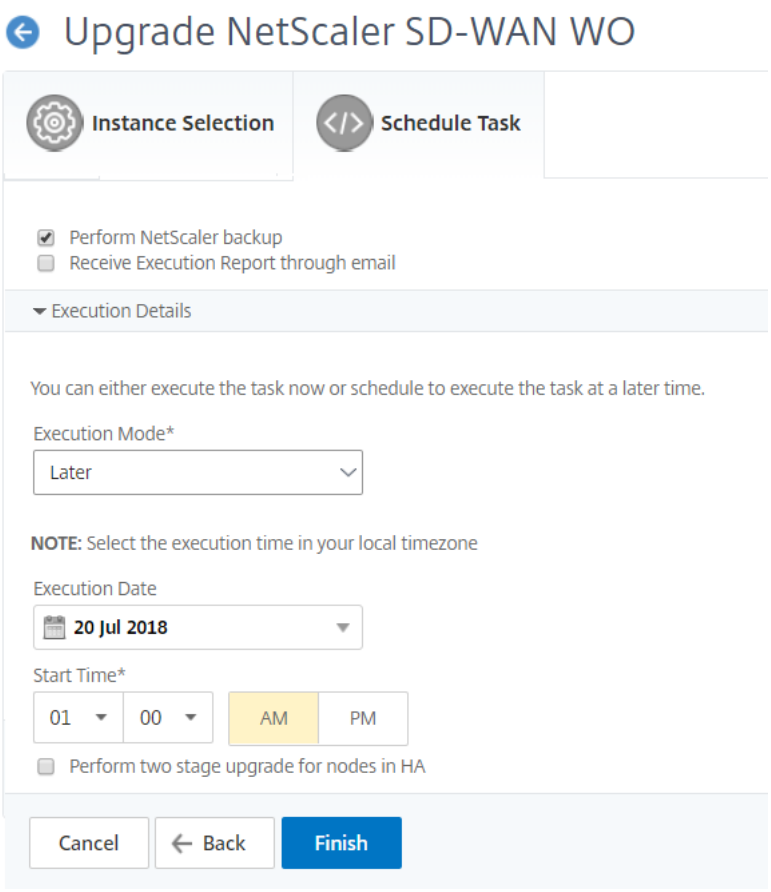
1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Auftrag erstellen**.
2. Wählen Sie auf der Seite **Wartungsauftrag erstellen** die Option **Upgrade NetScaler ADC SD-WAN WO** aus, und klicken Sie auf **Fortfahren**.



3. Fügen Sie auf der Seite **NetScaler ADC SD-WAN WO aktualisieren** auf der Registerkarte **Instanzauswahl** einen **Task-Namen** hinzu. Wählen Sie in der Liste Software-Image entweder Lokal (Ihre lokale Maschine) oder Appliance (die Builddatei muss auf der virtuellen Citrix ADM Appliance vorhanden sein). Fügen Sie die Citrix ADC SD-WAN WO-Instanzen hinzu, auf denen Sie den Upgradevorgang ausführen möchten. Klicken Sie auf **Weiter**.



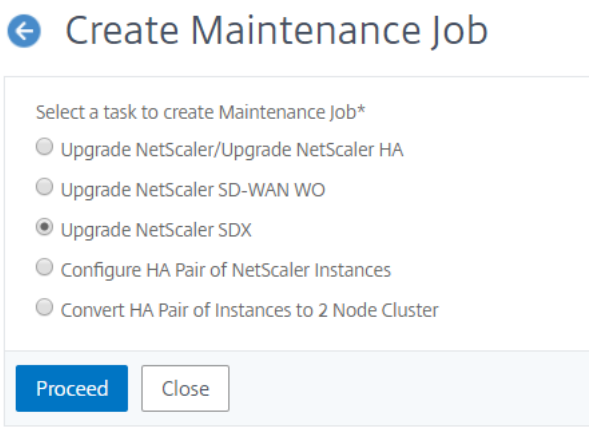
4. Um die NetScaler ADC SD-WAN WO-Instanz jetzt zu aktualisieren, wählen Sie in der Liste **Ausführungsmodus** die Option **Jetzt** aus. Klicken Sie auf **Fertig stellen**.
5. Um die Citrix ADC SD-WAN WO-Instanz später zu aktualisieren, wählen Sie **Später** aus der Liste**Ausführungsmodus** aus. Anschließend können Sie das Ausführungsdatum und die Startzeit für das Upgrade der Citrix ADC SD-WAN WO-Instanz auswählen.
6. Sie können die E-Mail-Benachrichtigung aktivieren, um den Ausführungsbericht für das Upgrade der Citrix ADC SD-WAN WO-Instanz zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail empfangen**, um die E-Mail-Benachrichtigung zu aktivieren.
7. Wählen Sie das **Plus-Symbol** aus, um die E-Mail-Verteilerliste zu erstellen.



8. Geben Sie auf der Seite **E-Mail-Verteilerliste erstellen** einen Namen für die E-Mail-Verteilerliste an. Fügen Sie den SMTP-Mailserver hinzu, der zum Senden von E-Mail-Benachrichtigungen an den E-Mail-Server verwendet wird. Fügen Sie im Feld **Von** die E-Mail-Adresse hinzu, von der Nachrichten gesendet werden sollen. Fügen Sie im Feld **An** eine E-Mail-Adresse oder Adressen hinzu, an die Nachrichten gesendet werden sollen. Sie können auch eine E-Mail-Adresse oder Adressen hinzufügen, an die Kopien und Kopien von Nachrichten gesendet werden sollen, ohne diese Adressen in den Nachrichten oder Kopien anzuzeigen. Klicken Sie auf **Erstellen**. Nachdem Sie die E-Mail-Verteilerliste erstellt haben, klicken Sie auf **Fertig stellen**, um die Konfiguration abzuschließen.

Planen des Upgrades von NetScaler ADC SDX-Instanzen

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Auftrag erstellen**.
2. Wählen Sie auf der Seite **Wartungsauftrag erstellen** die Option **Upgrade NetScaler ADC SDX** aus, und klicken Sie auf **Weiter**.



3. Fügen Sie auf der Seite **NetScaler ADC SDX-Appliance (s) aktualisieren** auf der Registerkarte **Instanzauswahl** einen **Task-Namen**hinzu. Wählen Sie in der Liste Software-Image entweder Lokal (Ihre lokale Maschine) oder Appliance (die Builddatei muss auf der virtuellen Citrix ADM Appliance vorhanden sein). Fügen Sie die NetScaler ADC SDX-Instanzen hinzu, auf denen Sie den Upgradevorgang ausführen möchten. Klicken Sie auf **Weiter**.
4. Sie können die E-Mail-Benachrichtigung aktivieren, um den Ausführungsbericht für das Upgrade der NetScaler ADC SDX-Instanz zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail empfangen**, um die E-Mail-Benachrichtigung zu aktivieren.
5. Wählen Sie das **Plus-Symbol** aus, um die E-Mail-Verteilerliste zu erstellen.
6. Um die Citrix ADC SDX-Instanz jetzt zu aktualisieren, wählen Sie **Jetzt** aus der Liste **Ausführungsmodus** aus. Klicken Sie auf **Fertig stellen**.
7. Um die Citrix ADC SDX-Instanz zu einem späteren Zeitpunkt zu aktualisieren, wählen Sie **Später** aus der Liste **Ausführungsmodus**. Anschließend können Sie das Ausführungsdatum und die Startzeit für das Upgrade der NetScaler ADC SDX-Instanz auswählen.
8. Geben Sie auf der Seite **E-Mail-Verteilerliste erstellen** einen Namen für die E-Mail-Verteilerliste an. Fügen Sie den SMTP-Mailserver hinzu, der zum Senden von E-Mail-Benachrichtigungen an den E-Mail-Server verwendet wird. Fügen Sie im Feld **Von** die E-Mail-Adresse hinzu, von der Nachrichten gesendet werden sollen. Fügen Sie im Feld **An** eine E-Mail-Adresse oder Adressen hinzu, an die Nachrichten gesendet werden sollen. Sie können auch eine E-Mail-Adresse oder Adressen hinzufügen, an die Kopien und Kopien von Nachrichten gesendet werden sollen, ohne diese Adressen in den Nachrichten oder Kopien anzuzeigen. Klicken Sie auf **Erstellen**. Nachdem Sie die E-Mail-Verteilerliste erstellt haben, klicken Sie auf **Fertig stellen**, um die Konfiguration abzuschließen.

Ein Upgrade der Autoscale-Gruppe planen

Führen Sie die folgenden Schritte aus, um alle Instanzen in den Clouddiensten zu aktualisieren, die Teil der Autoscale-Gruppe sind:

1. Navigieren Sie in Citrix ADM zu **Netzwerke > Konfigurationsaufträge > Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Job erstellen**.
2. Wählen Sie auf der Seite **Wartungsaufträge erstellen** die Option **Autoskalierungsgruppe aktualisieren** aus, und klicken Sie auf **Weiter**.
3. Auf der Registerkarte **Upgradeeinstellungen**:
   a) Wählen Sie die **Autoscale-Gruppe** aus, die Sie aktualisieren möchten.
   b) Wählen Sie unter **Image** die NetScaler ADC-Version aus. Dieses Image ist die vorhandene Version von NetScaler ADC-Instanzen in der Autoscale-Gruppe.
   c) Durchsuchen Sie in **NetScaler ADC Image**die NetScaler ADC Versionsdatei, auf die Sie ein Upgrade durchführen möchten.

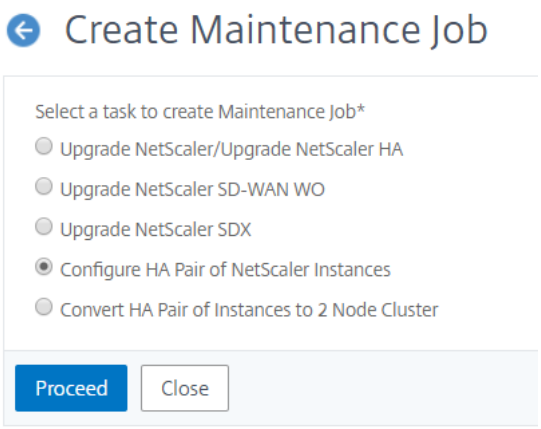
      Wenn Sie **Graceful Upgrade**aktivieren, wartet die Upgrade-Aufgabe, bis der angegebene Zeitraum für die Drain-Verbindung abgelaufen ist.
   d) Klicken Sie auf **Weiter**.
4. Auf der Registerkarte **Task planen**:
   a) Wählen Sie in der Liste "Ausführungsmodus"eine der folgenden Optionen aus:
      - **Jetzt:**Um das Upgrade der NetScaler ADC-Instanzen sofort zu starten.
      - **Später:** Um das Upgrade der NetScaler ADC-Instanzen zu einem späteren Zeitpunkt zu starten.
   b) Wenn Sie die Option **Später** auswählen, wählen Sie das Ausführungsdatum und die Startzeit, wenn Sie den Upgrade-Task starten möchten.

   Sie können auch E-Mail- und Pufferbenachrichtigungen aktivieren, um den Ausführungsbericht der Aktualisierung der Autoscale-Gruppe zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail** empfangen und **Ausführungsbericht über Pufferzeit** empfangen, um die Benachrichtigungen zu aktivieren.
5. Klicken Sie auf **Fertig stellen**.

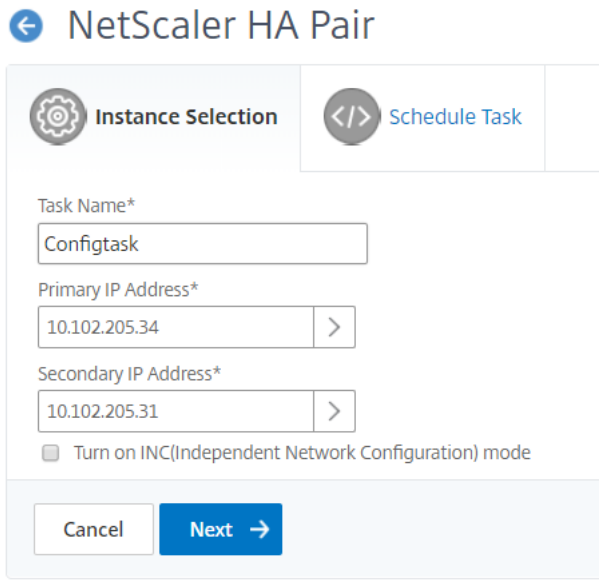
Planen der Konfiguration von HA-Paar von NetScaler ADC Instanzen

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Auftrag erstellen**.

2. Wählen Sie auf der Seite **Wartungsauftrag erstellen** die Option **HA-Paar von NetScaler ADC Instanzen konfigurieren** aus, und klicken Sie auf **Fortfahren**.



3. Fügen Sie auf der Seite **NetScaler ADC HA-Paar** auf der Registerkarte **Instanzauswahl** einen **Task-Namen**hinzu. Geben Sie die primäre IP-Adresse und die sekundäre Adresse ein, und klicken Sie auf **Weiter**.



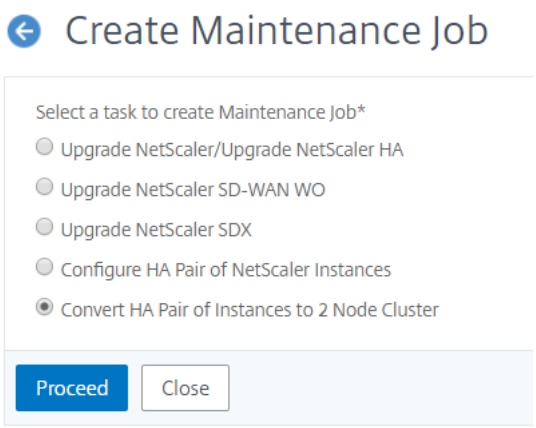
4. Auf der Registerkarte **Task planen** können Sie entweder das NetScaler ADC HA-Paar jetzt oder höher konfigurieren.
5. Um das Citrix ADC HA-Paar jetzt zu konfigurieren, wählen Sie **Jetzt** aus der Liste **Ausführungsmodus** aus. Sie können die E-Mail-Benachrichtigung aktivieren, um den Ausführungsbericht des NetScaler ADC HA-Paares zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail empfangen**, um die E-Mail-Benachrichtigung zu aktivieren.
6. Um das NetScaler ADC HA-Paar zu einem späteren Zeitpunkt zu konfigurieren, wählen Sie **Später** aus der Liste **Ausführungsmodus**. Sie können dann das eExecution-Datum und

die Startzeit auswählen. Sie können die E-Mail-Benachrichtigung aktivieren, um den Ausführungsbericht des NetScaler ADC HA-Paares zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail empfangen**, um die E-Mail-Benachrichtigung zu aktivieren.

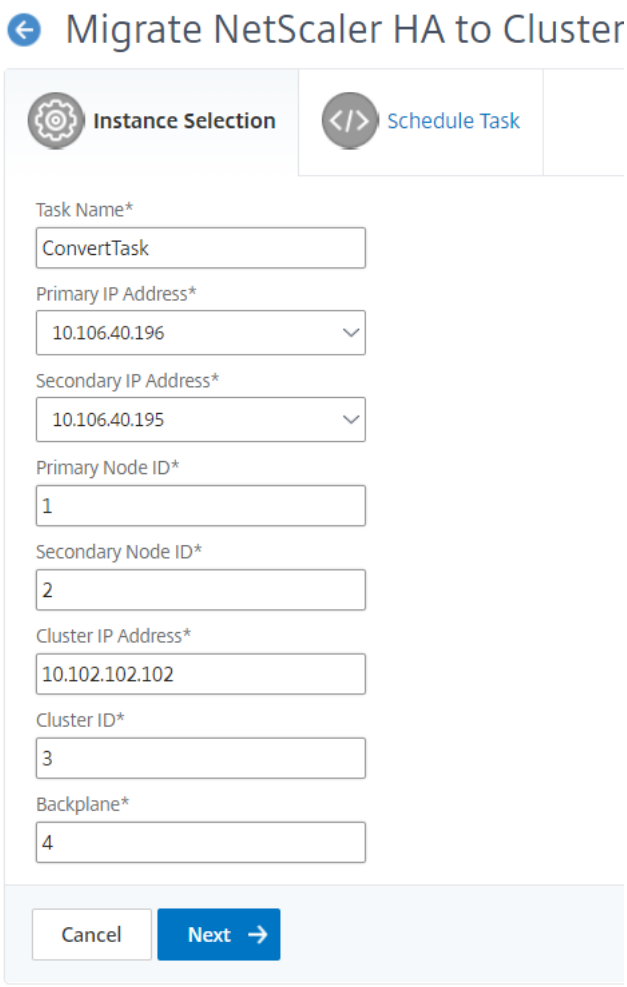
7. Wählen Sie das **Plus-Symbol** aus, um die E-Mail-Verteilerliste zu erstellen.
8. Geben Sie auf der Seite **E-Mail-Verteilerliste erstellen** einen **Namen** für die E-Mail-Verteilerliste an. Fügen Sie den SMTP-Mailserver hinzu, der zum Senden von E-Mail-Benachrichtigungen an den E-Mail-Server verwendet wird. Geben Sie im Feld **Von** die E-Mail-Adresse ein, von der aus Nachrichten gesendet werden sollen. Fügen Sie im Feld **An** eine E-Mail-Adresse oder Adressen hinzu, an die Nachrichten gesendet werden sollen. Sie können auch eine E-Mail-Adresse oder Adressen hinzufügen, an die Kopien und Kopien von Nachrichten gesendet werden sollen, ohne diese Adressen in den Nachrichten oder Kopien anzuzeigen. Klicken Sie auf **Erstellen**. Nachdem Sie die E-Mail-Verteilerliste erstellt haben, klicken Sie auf **Fertig stellen**, um die Konfiguration abzuschließen.

Planen Sie die Konvertierung von HA-Instanzen in Cluster

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Auftrag erstellen**.
2. Wählen Sie auf der Seite **Wartungsauftrag erstellen** die Option **HA-Instanzen in Cluster mit 2 Knoten konvertieren** aus, und klicken Sie auf **Weiter**.



3. Fügen Sie auf der Seite **NetScaler ADC HA zu Cluster migrieren** auf der Registerkarte **Instanzauswahl** einen **Task-Namen**hinzu. Geben Sie die primäre IP-Adresse, die sekundäre Adresse, die primäre Knoten-ID, die sekundäre Knoten-ID, die Cluster-IP-Adresse, die Cluster-ID und die Backplane an. Klicken Sie auf **Weiter**.



4. Auf der Registerkarte **Task planen** können Sie entweder festlegen, ob Sie NetScaler ADC HA jetzt oder höher auf Cluster migrieren möchten.
5. Um das NetScaler ADC HA-Paar zu einem späteren Zeitpunkt zu konfigurieren, wählen Sie **Später** aus der Liste **Ausführungsmodus**. Sie können dann das Ausführungsdatum und die Startzeit auswählen. Sie können die E-Mail-Benachrichtigung aktivieren, um den Ausführungsbericht des NetScaler ADC HA-Paares zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht über E-Mail empfangen**, um die E-Mail-Benachrichtigung zu aktivieren.
6. Wählen Sie das **Plus-Symbol** aus, um die E-Mail-Verteilerliste zu erstellen.
7. Geben Sie auf der Seite **E-Mail-Verteilerliste erstellen** einen Namen für die E-Mail-Verteilerliste an. Fügen Sie den SMTP-Mailserver hinzu, der zum Senden von E-Mail-Benachrichtigungen an den E-Mail-Server verwendet wird. Geben Sie im Feld **Von** die E-Mail-Adresse ein, von der aus Nachrichten gesendet werden sollen. Fügen Sie im Feld **An** eine E-Mail-Adresse oder Adressen hinzu, an die Nachrichten gesendet werden sollen. Sie können auch eine E-Mail-Adresse oder Adressen hinzufügen, an die Kopien und Kopien von Nachrichten gesendet werden sollen, ohne

diese Adressen in den Nachrichten oder Kopien anzuzeigen. Klicken Sie auf **Erstellen**. Nachdem Sie die E-Mail-Verteilerliste erstellt haben, klicken Sie auf **Fertig stellen**, um die Konfiguration abzuschließen.

Konfigurationsaudit

February 5, 2024

Dieses Dokument beinhaltet:

- Audit-Vorlagen erstellen
- Auditberichte anzeigen
- Änderungen der Konfiguration auf allen Instanzen überprüfen
- Informationen zur Konfiguration der Netzwerkkonfiguration erhalten
- Abfragen der Konfigurationsüberwachung von Citrix ADC Instanzen

Überwachungsvorlagen erstellen

February 5, 2024

Sie möchten sicherstellen, dass bestimmte Konfigurationen auf bestimmten Instanzen ausgeführt werden, um die optimale Leistung Ihres Netzwerks zu gewährleisten. Außerdem möchten Sie Konfigurationsänderungen über verwaltete Citrix Application Delivery Controller (ADC) -Instanzen überwachen, Konfigurationsfehler beheben und ungespeicherte Konfigurationen nach einem plötzlichen Herunterfahren des Systems wiederherstellen. Sie können Überwachungsvorlagen mit bestimmten Konfigurationen erstellen, die Sie für bestimmte Instanzen überwachen möchten. Citrix Application Delivery Management (Citrix ADM) vergleicht diese Instanzen mit der Überwachungsvorlage und meldet, wenn eine Nichtübereinstimmung in der Konfiguration vorliegt.Wenn eine Konfigurationsabweichung vorliegt, generiert Citrix ADM einen Konfigurationsabweichbericht, mit dem Sie unerwünschte Konfigurationsänderungen beheben und beheben können.

Sie können die Ausführung der Prüfvorlage automatisieren, indem Sie

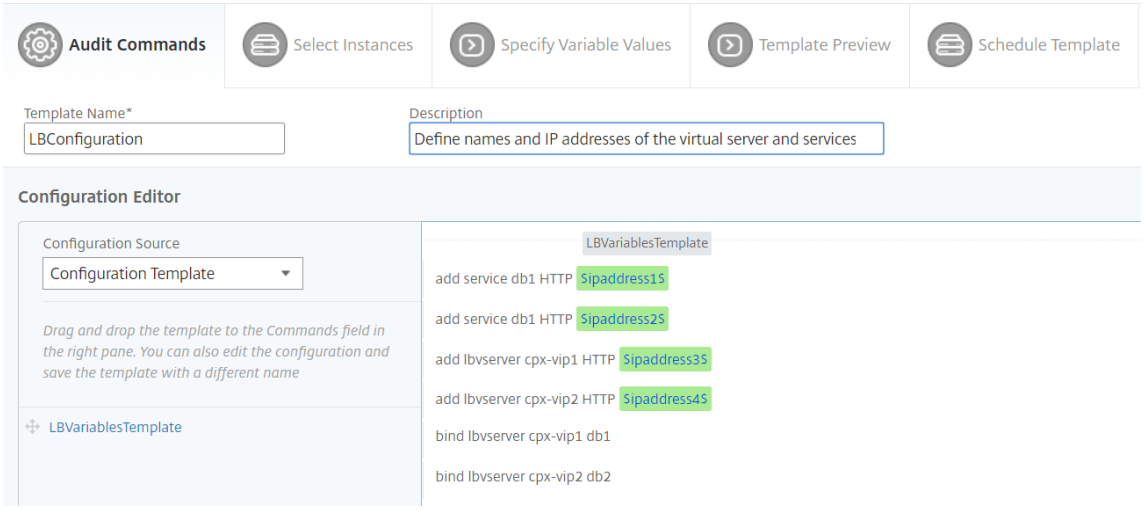
- Planen der Zeit, zu der die Vorlage ausgeführt werden muss
- Festlegen der Häufigkeit, mit der NetScaler ADM die Vorlage ausführen muss. Sie können die Vorlage täglich, an einem bestimmten Tag in einer Woche oder an einem bestimmten Datum in einem Monat ausführen.

Sie haben auch die Möglichkeit, den von NetScaler ADM generierten Vergleichsbericht an angegebene E-Mail-Adressen zu senden, die Sie konfigurieren können. Mit dieser Option kann der Benutzer den Bericht als E-Mail-Anhang empfangen, und der Benutzer muss sich nicht bei NetScaler ADM anmelden, um die Berichte manuell zu exportieren.

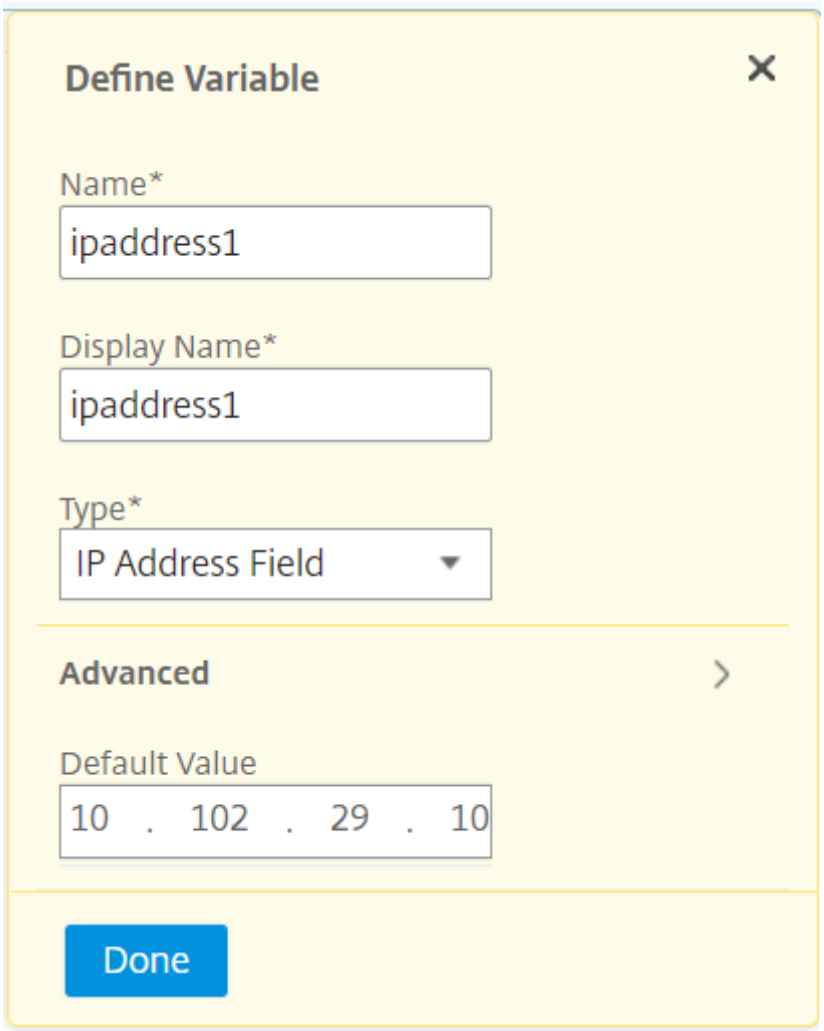
> **Hinweis**
> Die Option **Umbenennen** ist für die Standardkonfigurationsvorlagen deaktiviert. Sie können jedoch benutzerdefinierte Konfigurationsvorlagen umbenennen.

So erstellen Sie Überwachungsvorlagen:

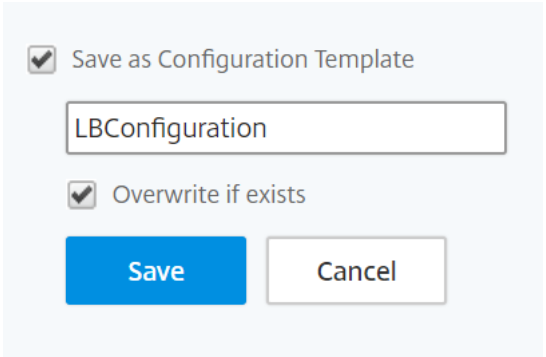
1. Navigieren Sie zu**Netzwerke** >**Konfigurationsüberwachung**>**Überwachungsvorlagen**, und klicken Sie auf**Hinzufügen**.
2. Geben Sie auf der Seite**Vorlage erstellen** und auf der Registerkarte**Überwachungsbefehle** den Vorlagennamen und die Beschreibung an.
3. Geben Sie auf der Seite **Konfigurations-Editor** Ihre Befehle ein und speichern Sie die Befehle als Konfigurationsvorlage. Sie können auch eine vorhandene Vorlage aus dem linken Bereich in den Editor ziehen.
4. Wählen Sie die Werte aus, die Sie in eine Variable konvertieren möchten, und klicken Sie dann auf **In Variable konvertieren**. Wählen Sie beispielsweise die IP-Adresse des Load Balancing-Servers „ipaddress1“aus und klicken Sie auf In Variable**konvertieren**. Die Variable ist nun mit “$”eingeschlossen, wie in der Abbildung unten gezeigt.



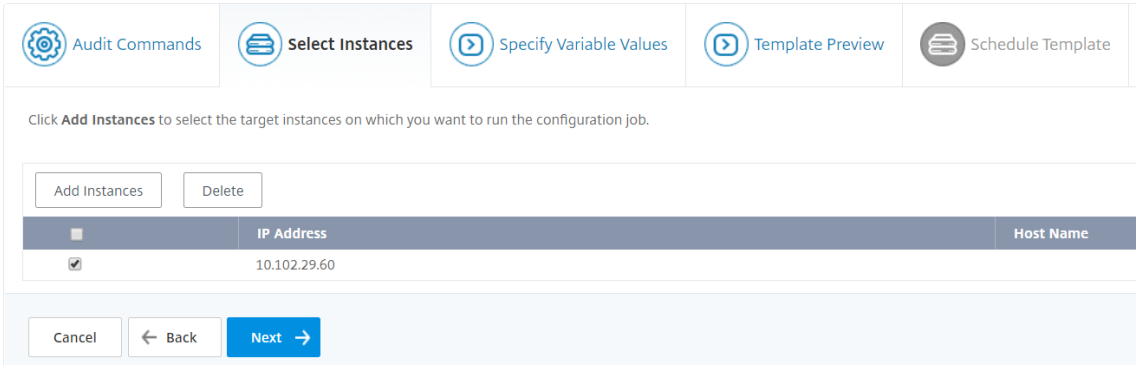
Legen Sie im Fenster **Variable definieren** die Eigenschaften für diese Variable fest: Name, Anzeigename und Typ der Variablen. Klicken Sie auf die Option**Erweitert**, wenn Sie einen Standardwert für die Variable angeben möchten.



Sie können die Befehle auch als Konfigurationsvorlage speichern.



5. Klicken Sie auf**Speichern** und dann auf **Weiter**.
6. Wählen Sie auf der Registerkarte **Instanzen auswählen** die Instanzen aus, auf denen die Konfigurationsüberwachung ausgeführt werden soll, und klicken Sie auf **Weiter**.

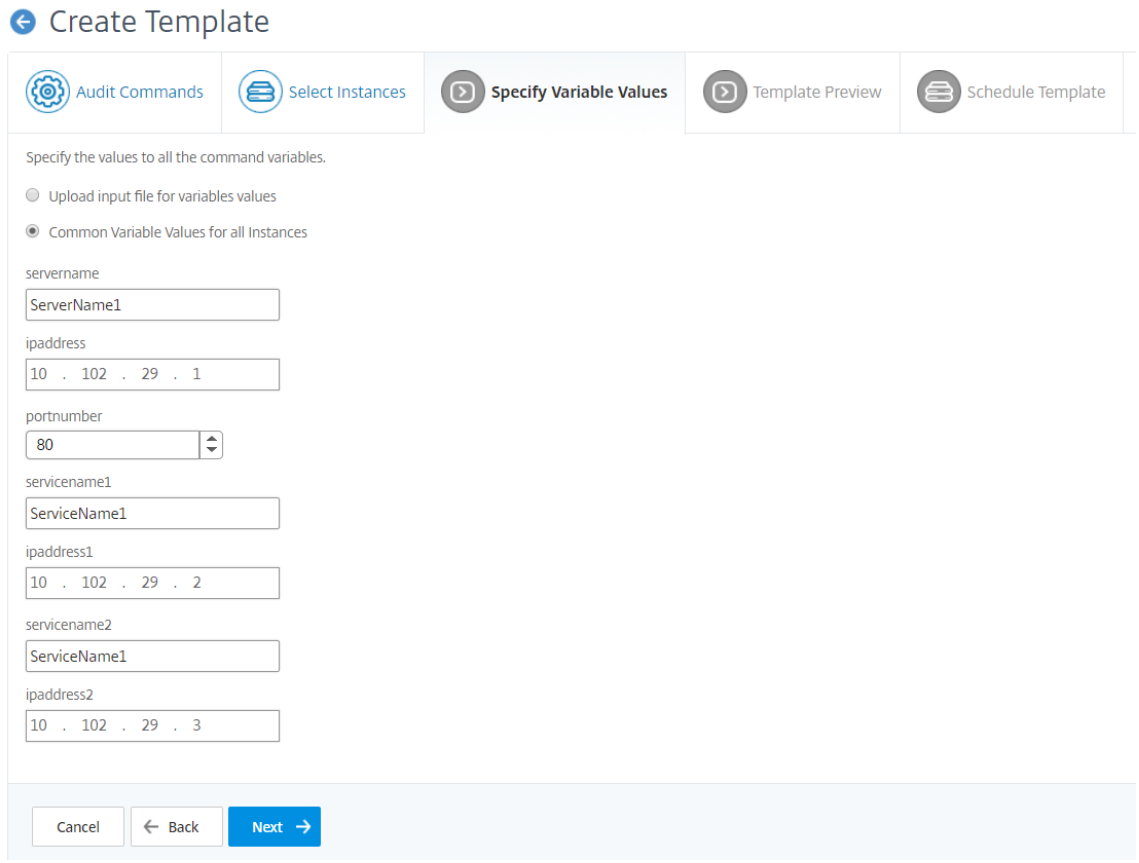


7. Auf der Registerkarte**Variablenwerte angeben** stehen Ihnen zwei Optionen zur Verfügung:

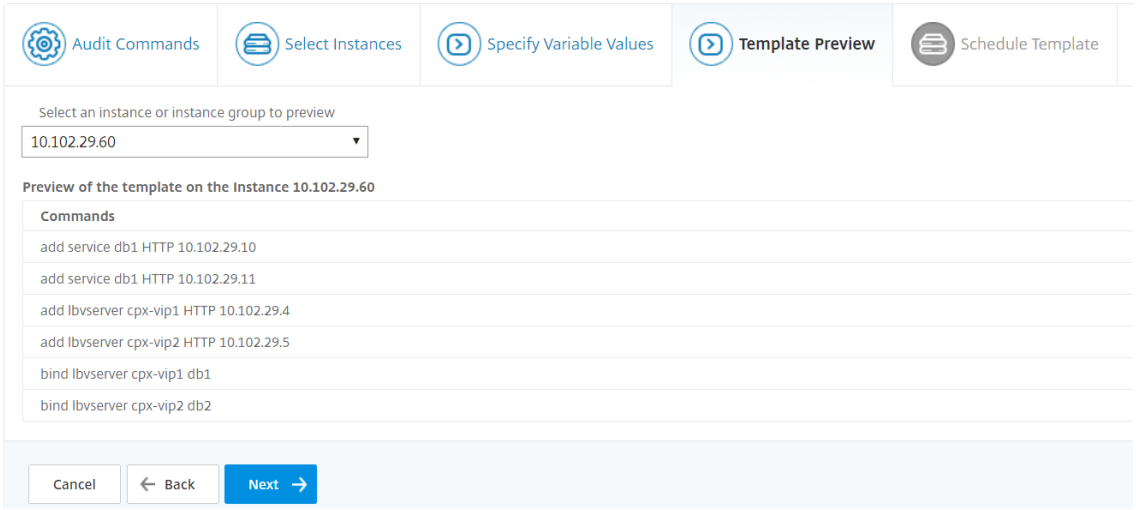
   a) Laden Sie die Eingabedatei herunter, um die Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den NetScaler ADM Server hoch.

   b) Geben Sie gemeinsame Werte für die Variablen ein, die Sie für alle Instanzen definiert haben

8. Klicken Sie auf **Weiter**.



9. Auf der Registerkarte **Vorlagenvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen. Klicken Sie auf **Weiter**.



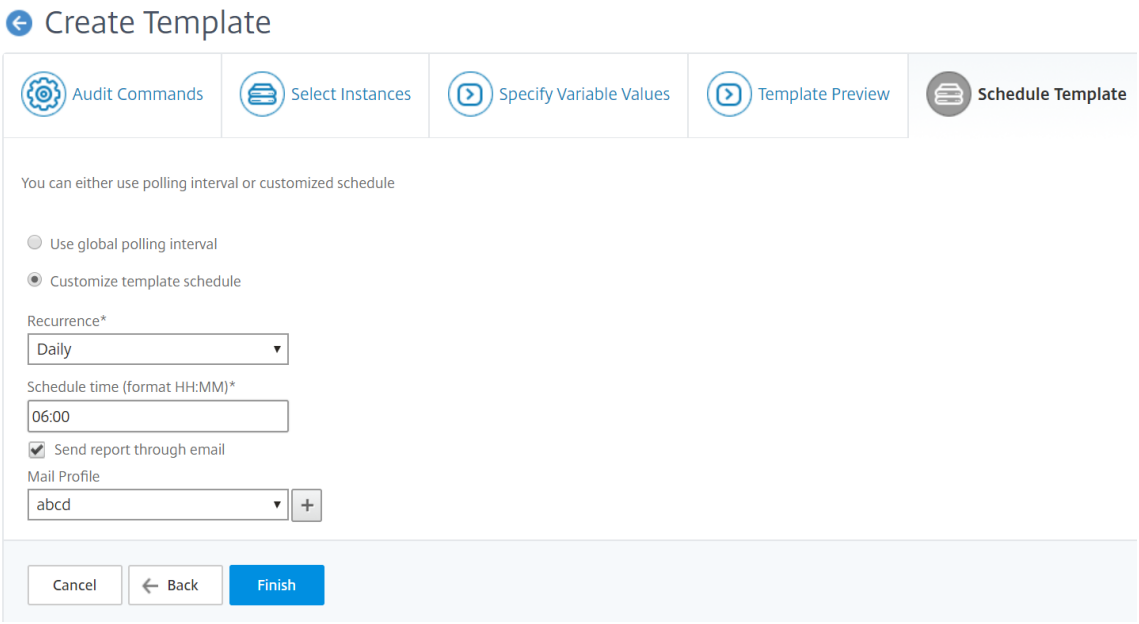
10. Auf der Registerkarte **Vorlage planen** haben Sie die folgenden Optionen, um die Ausführung der Vorlage zu planen und die E-Mail-Adresse so zu konfigurieren, dass der Diff-Bericht gesendet wird.

    - **Verwenden Sie das globale Polling-Intervall** Wählen Sie diese Option aus, um die Vorlage auf den Instanzen zu einem Zeitpunkt auszuführen, der global auf NetScaler ADM konfiguriert ist.

      > **Hinweis:**
      >
      > Um das globale Abrufintervall in NetScaler ADM zu konfigurieren, navigieren Sie zu **Netzwerke**> **Konfigurationsüberwachung** > **Überwachungsvorlagen** und klicken Sie auf **Globales Abrufintervall**. Geben Sie im Feld **Abfrageintervall** die Minuten ein, in denen NetScaler ADM die Instanzen global abfragen muss.

    - **Anpassen des Vorlagenzeitplans**. Verwenden Sie diese Option, um die Zeit und die Häufigkeit zu konfigurieren, mit der die Vorlagen ausgeführt werden müssen
    - **Bericht per E-Mail senden**. Verwenden Sie diese Option, um das E-Mail-Profil zu konfigurieren, an das der Diff-Bericht als E-Mail-Anhang gesendet werden muss.

11. Klicken Sie auf **Fertig stellen**.



Die Überwachungsvorlage wird in der Liste **Überwachungsvorlagen** angezeigt und zum geplanten Zeitpunkt für die Konfigurationen in den angegebenen Instanzen ausgeführt.

Auditberichte anzeigen

February 5, 2024

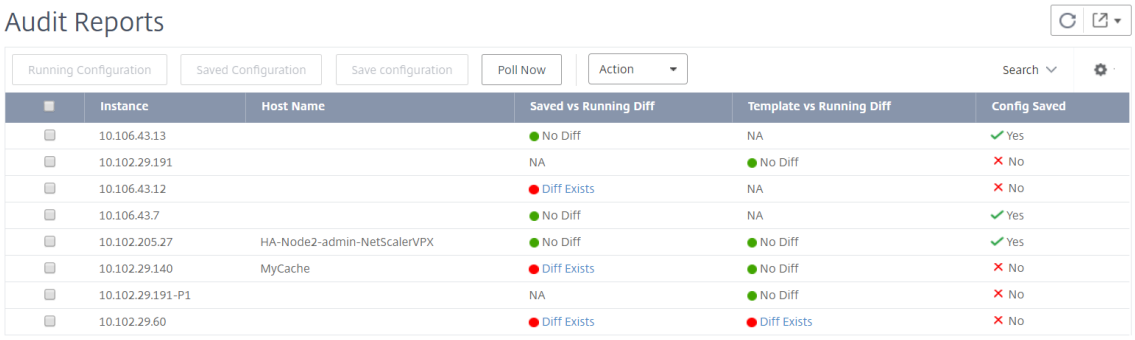
Citrix Application Delivery Management (Citrix ADM) ermöglicht Ihnen das Anzeigen und Herunterladen des Berichts zur Konfigurationsüberwachung im Abschnitt “Configuration Audit Diff”. Im Abschnitt zur Konfigurationsprüfung können Sie den zusammenfassenden Bericht für alle Instanzen und pro Instanz exportieren. Außerdem können Sie einen detaillierten Vergleichsbericht für jedes Instanz-Vorlagenpaar exportieren.

Die Überwachungsvorlagen, die in der Liste Überwachungsvorlagen angezeigt werden, werden zum geplanten Zeitpunkt für die Konfigurationen in den angegebenen Instanzen ausgeführt. Das Diagramm **NetScaler Config Drift** im **Konfigurationsüberprüfungs-Dashboard** zeigt allgemeine Details zu Konfigurationsänderungen an, die für nicht gespeicherte Konfigurationen gespeichert wurden. Wenn Sie auf**NetScaler Config Drift** chart klicken, wird auf der folgenden Seite “**Audit-Berichte** “eine Liste von Instanzen angezeigt, in denen sowohl “Diff Exists”als auch “No Diff”angezeigt werden. “Sie können die von Citrix ADM angezeigten Diff-Berichte herunterladen.

NetScaler ADM bietet auch die Option, den automatischen Export von Diff-Bericht als E-Mail-Anlage zu planen. Weitere Informationen zum Planen des Exports von Berichten finden Sie unter Erstellen von Überwachungsvorlagen.

So exportieren Sie Konfigurationsüberwachungsberichte:

1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Konfigurationsüberwachung**.
2. Klicken Sie auf der Seite **Configuration Audit** in das Diagramm **NetScaler Config Drift** .
3. Auf der Seite **Auditberichte** werden Instanzen aufgeführt, die einen Unterschied aufweisen. Auf der Seite wird auch eine Liste der Instanzen angezeigt, die in ihren ausgeführten Konfigurationen keinen Unterschied aufweisen.

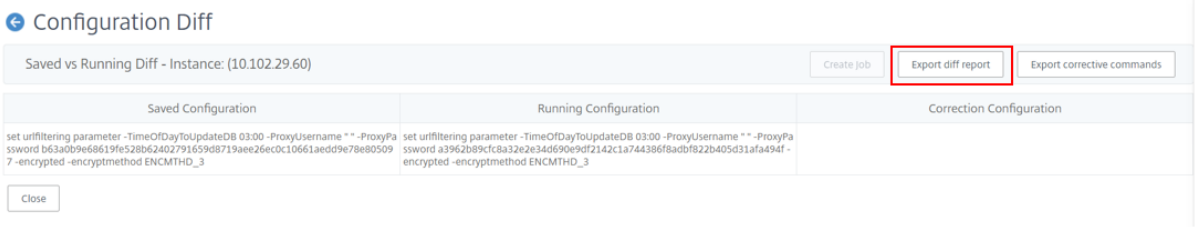


Im Bild sehen Sie, dass für einige Instanzen ein Diff nur in **Saved Vs Running Diff** vorhanden ist und für einige Instanzen ein Diff nur in **Template vs Running Diff** vorhanden ist. In einigen Fällen gibt es Unterschiede sowohl zwischen **Saved Vs Running Diff** als auch **Template vs Running Diff.**

Gespeichert Vs Laufdiff

Sie können einen Bericht über den Unterschied zwischen der auf der Instanz gespeicherten Konfiguration und der aktuell auf dieser Instanz ausgeführten Konfiguration anzeigen. Klicken Sie beispielsweise für eine Instanz unter **Gespeicherte Vs Laufdiff auf Diff**vorhanden**.**

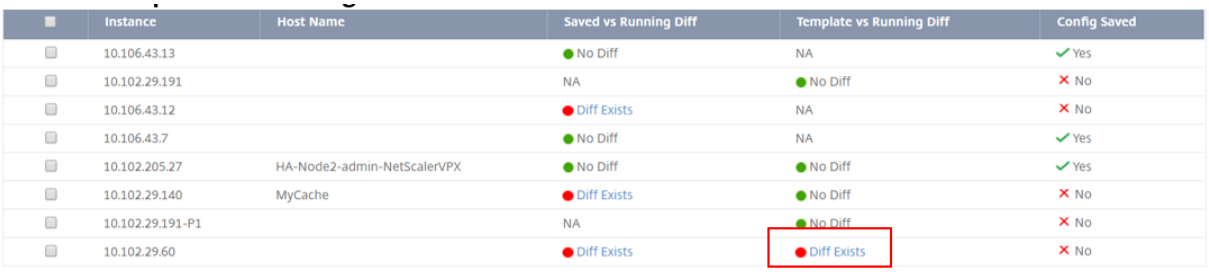
Hier sehen Sie einen Bericht für die gespeicherte Konfiguration gegen den laufenden Konfigurationsdiff für diese Instanz.



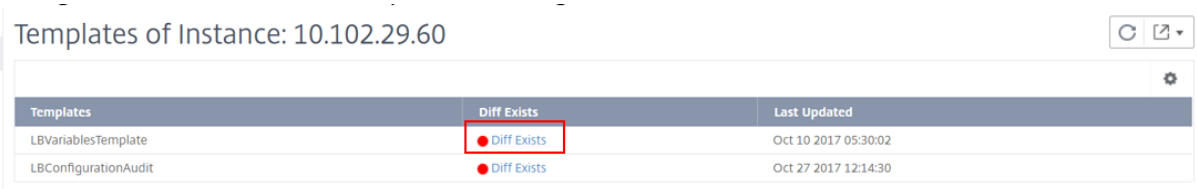
Klicken Sie auf **Diff-Bericht exportieren**, um eine CSV-Datei des Diff-Berichts herunterzuladen. Sie können auch auf Korrekturbefehle exportieren klicken, um die Befehle in eine TXT-Datei zu exportieren. Anschließend können Sie die Befehle für die zugeordnete Citrix ADM Instanz über Konfigurationsaufträge ausführen, um die Konfiguration in dieser Instanz zu korrigieren.

Template gegen Running Diff

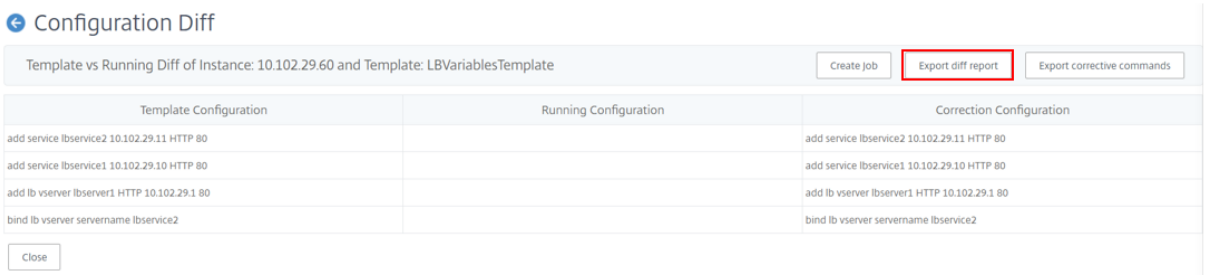
Das **Template vs Running Diff** enthält alle Vorlagen außer **Saved Vs Running Diff**, der Standardvorlage. Sie können den Unterschied anzeigen, der zwischen der Vorlage und der laufenden Konfiguration besteht.Klicken Sie beispielsweise für eine der Instanzen unter **Vorlage vs Laufende**Diff auf Diff Existiert**.**



Jetzt können Sie sehen, dass zwei Vorlagen Diff anzeigen und die NetScaler ADM Instanz eine andere Konfiguration als die gewünschte Vorlage hat.



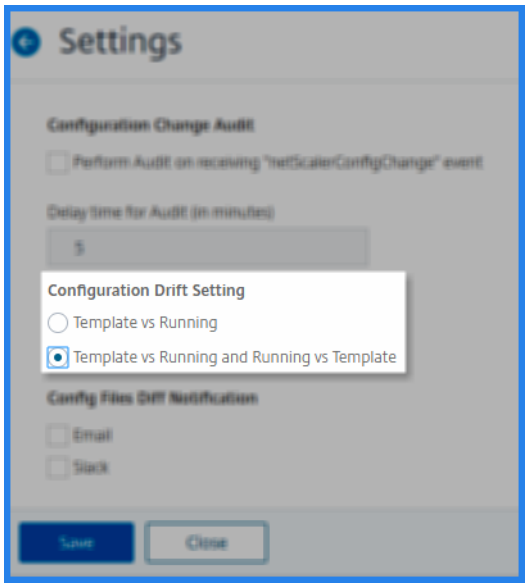
Klicken Sie erneut auf**Diff Existent**. Die folgende Abbildung zeigt die Konfiguration, nach der die Vorlage sucht, und die laufende Konfiguration, die leer ist, da keine derartigen Befehle konfiguriert oder entfernt wurden. Sie können auch die Korrekturkonfigurationen oder die Befehle sehen, die ausgeführt werden sollen, um die Konfiguration zu korrigieren.



Sie können auch die Einstellung Template vs Running und Running vs Template Drift verwenden, um die Konfiguration auf beiden Arten zu vergleichen:

- Vergleicht die Audit-Vorlagenkonfiguration mit der laufenden Konfiguration auf der Instanz.
- Vergleicht die laufende Konfiguration auf der Instanz mit der Audit-Vorlage.

Standardmäßig ist die Einstellung Template vs. Running Drift ausgewählt. Um die Drift-Einstellung zu ändern, wählen Sie in der ADM-GUI auf der Seite **Configuration Audit** die Option **Einstellungen** aus.



Klicken Sie auf **Diff-Bericht exportieren**, um eine CSV-Datei des Diff-Berichts herunterzuladen. Sie können auch auf **Korrekturbefehle exportieren** klicken, um die Befehle in eine TXT-Datei zu exportieren. Anschließend können Sie die Befehle in CLI ausführen, um die Konfiguration in dieser Instanz zu korrigieren.

Das folgende Bild zeigt eine CSV-Beispieldatei, die auf Ihr System heruntergeladen wird:

#Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate		
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lbserver1 HTTP 10.102.29.1 80		add lb vserver lbserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

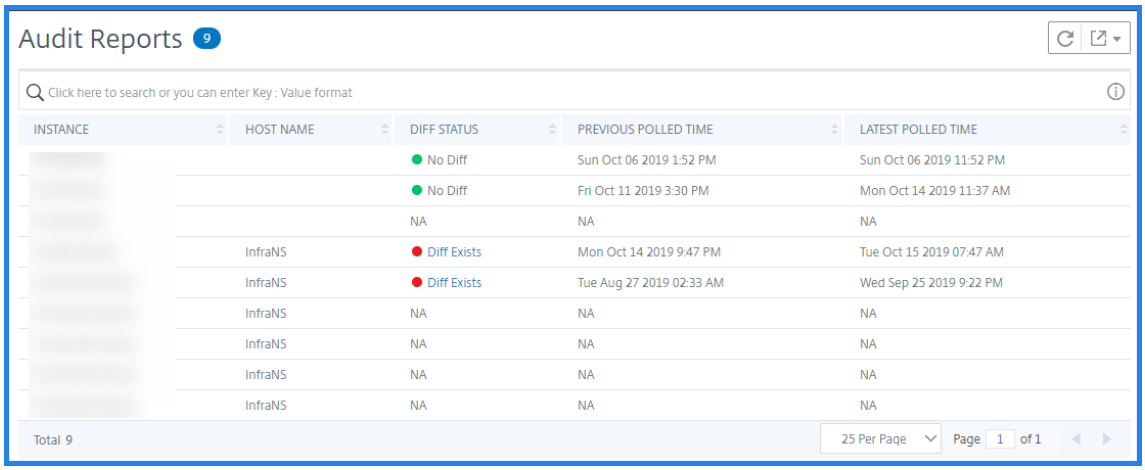
Anzeigen der Dateistatus-Überwachungsberichte

Mit dem **NetScaler ADC File Statusdiagramm** können Sie überwachen, ob Dateien im `nsconfig` Ordner hinzugefügt, geändert oder entfernt werden. Beispiel: Wenn die Lizenzdatei auf einer ADC-Instanz aktualisiert wird, können Sie überprüfen, wann diese Datei zuletzt aktualisiert wurde, und entsprechende Maßnahmen ergreifen.

So exportieren Sie die Dateistatus-Überwachungsberichte für die NetScaler ADC-Instanzen:

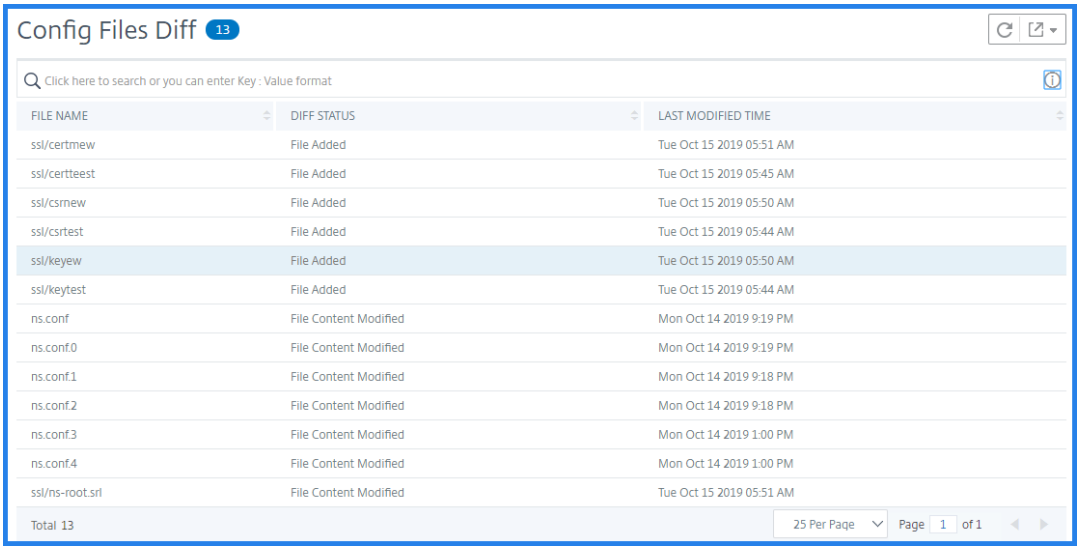
1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Konfigurationsüberwachung**.
2. Klicken Sie auf der Seite **Konfigurationsüberwachung** auf das Diagramm **NetScaler ADC Dateistatus**.

   Auf der Seite **Auditberichte** werden Instanzen mit dem Status “Vergleich”aufgeführt.



   Der **Diff-Status** wird für das Intervall zwischen der **vorherigen Abfragezeit** und der **letzten Abfragezeit**berechnet. Der **Diff-Status** kann einer der folgenden sein:

   - **Diff existiert** - Dieser Status zeigt an, dass sich die Dateien im Ordner `nsconfig` einer Instanz seit dem **vorherigen Abfragezeitpunkt**geändert haben. Um die Änderungen an der Datei anzuzeigen, klicken Sie auf **Diff Existiert**.



   - **Kein Diff** - Dieser Status zeigt an, dass sich die Dateien im`nsconfig` Ordner seit der vorherigen Abfragezeit nicht geändert haben.
   - **NA** - Dieser Status zeigt an, dass die Überwachung des Dateistatus nicht anwendbar ist. Dieser Status wird angezeigt, wenn der NetScaler ADM die Instanz nicht abfragt. Wenn

beispielsweise eine Instanz neu hinzugefügt wird oder der Instanzstatus inaktiv ist, findet die Abfrage der Instanz nicht statt.

Konfigurationsänderungen über alle Instanzen hinweg überwachen

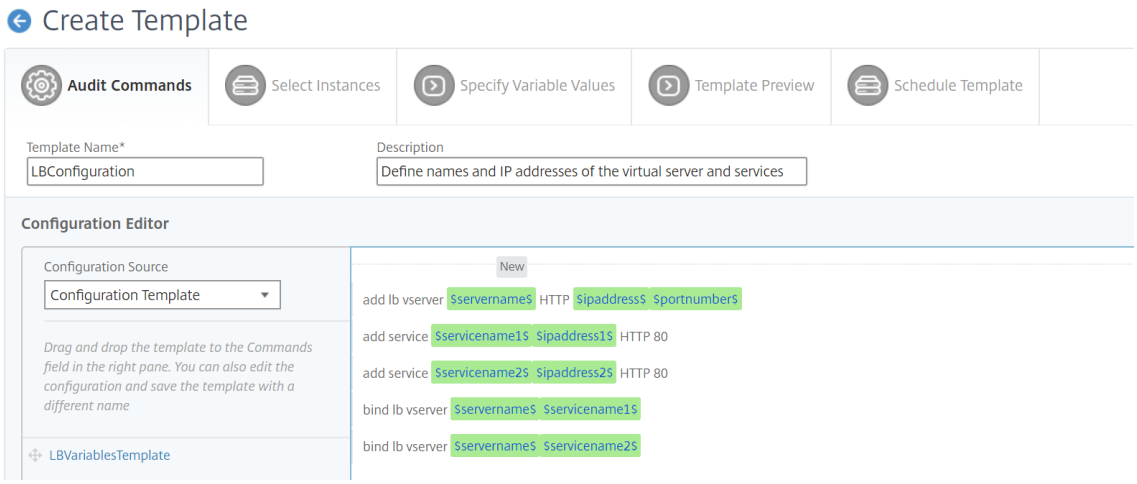
February 5, 2024

Sie möchten sicherstellen, dass bestimmte Konfigurationen auf bestimmten Instanzen ausgeführt werden, um die optimale Leistung Ihres Netzwerks zu gewährleisten. Außerdem möchten Sie Konfigurationsänderungen über verwaltete Citrix Application Delivery Controller (ADC) -Instanzen überwachen, Konfigurationsfehler beheben und ungespeicherte Konfigurationen nach einem plötzlichen Herunterfahren des Systems wiederherstellen. Sie können Überwachungsvorlagen mit bestimmten Konfigurationen erstellen, die Sie auf bestimmten Instanzen ausführen möchten. NetScaler Application Delivery Management (NetScaler ADM) vergleicht diese Instanzen mit der Überwachungsvorlage und meldet, wenn eine nicht übereinstimmende Konfiguration vorliegt. Auf diese Weise können Sie die Fehler beheben und beheben.

Sie können die Ausführung der Prüfungsvorlage automatisieren, indem Sie den Zeitpunkt planen, zu dem die Vorlage ausgeführt werden muss. Sie können auch festlegen, mit welcher Häufigkeit NetScaler ADM die Vorlage ausführen muss. Sie können die Vorlage täglich, an einem bestimmten Tag in einer Woche oder an einem bestimmten Datum in einem Monat ausführen. Sie haben auch die Möglichkeit, den von Citrix ADM generierten Diff-Bericht an bestimmte E-Mail-Adressen zu senden, die Sie konfigurieren können. Mit dieser Option erhält der Benutzer den Bericht als E-Mail-Anlage, und der Benutzer muss sich nicht bei NetScaler ADM anmelden, um die Berichte manuell zu überprüfen.

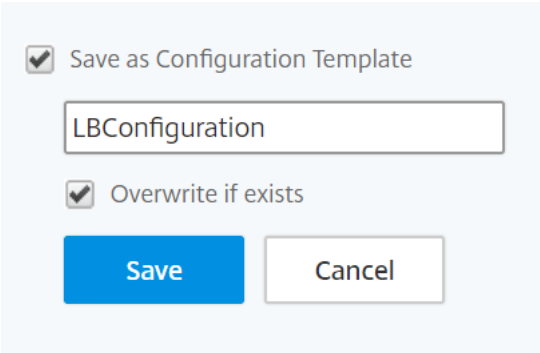
So erstellen Sie Überwachungsvorlagen:

1. Navigieren Sie zu**Netzwerke > Konfigurationsprüfung > Audit-Vorlagen**, und klicken Sie auf**Hinzufügen**.
2. Geben Sie auf der Seite**Vorlage erstellen** und auf der Registerkarte**Überwachungsbefehle** den Vorlagennamen und die Beschreibung an.
3. Geben Sie im **Konfigurationseditor**Ihre Befehle ein, und speichern Sie die Befehle als Konfigurationsvorlage. Sie können auch eine vorhandene Vorlage aus dem linken Bereich des Editors ziehen.
4. Wählen Sie die Werte aus, die Sie in eine Variable konvertieren möchten, und klicken Sie dann auf **In Variable konvertieren**. Wählen Sie beispielsweise die IP-Adresse des Load Balancing-Servers aus und klicken Sie auf In**Variable konvertieren**`ipaddress`, wie in der Abbildung unten gezeigt.

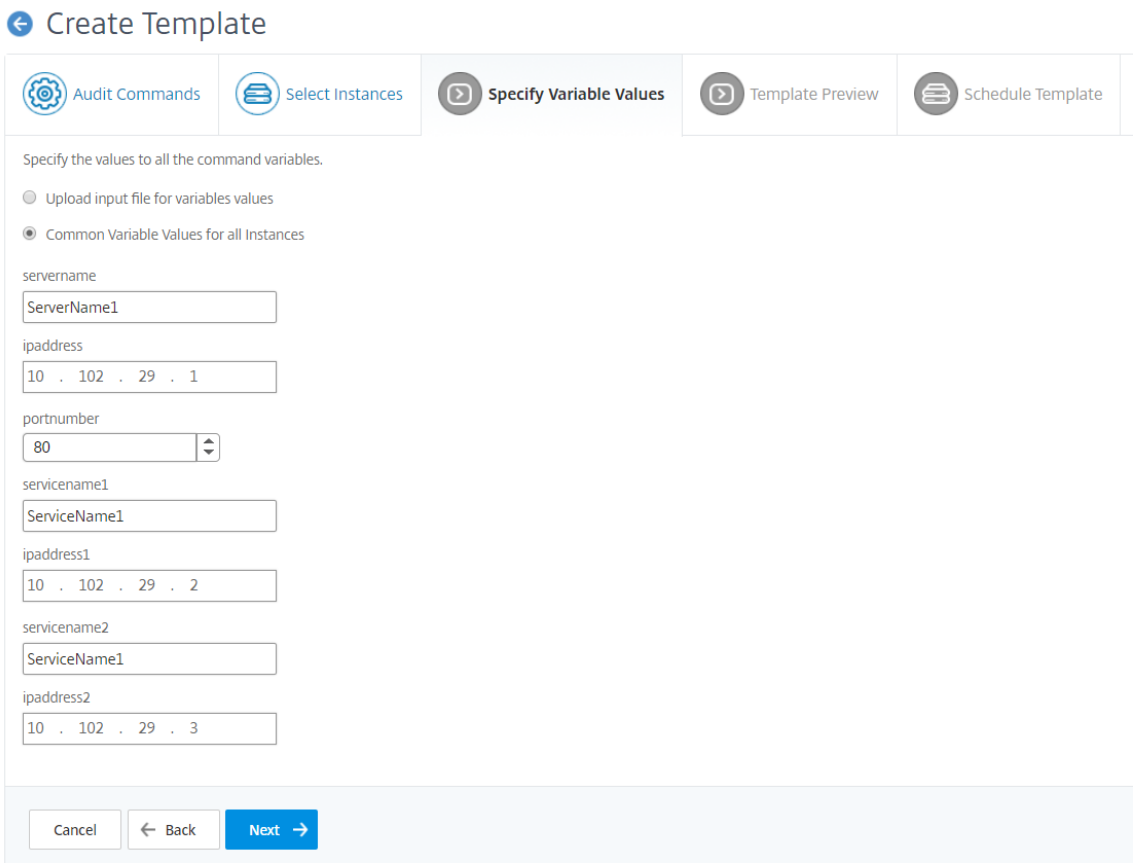


Klicken Sie auf die Option**Erweitert**, wenn Sie einen Standardwert für die Variable angeben möchten.

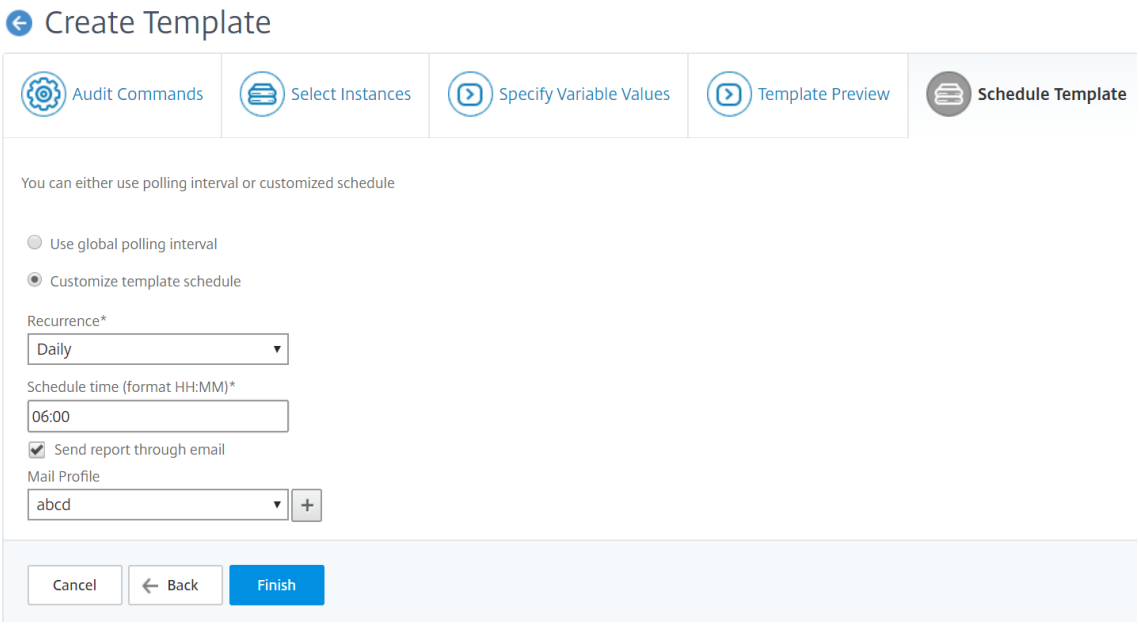
Sie können die Befehle auch als Konfigurationsvorlage speichern.



5. Klicken Sie auf**Speichern** und dann auf **Weiter**.
6. Wählen Sie auf der Registerkarte **Instanzen auswählen** die Instanzen aus, auf denen Sie die Konfigurationsüberprüfung ausführen möchten.
7. Auf der Registerkarte**Variablenwerte angeben** stehen Ihnen zwei Optionen zur Verfügung:
   a) Laden Sie die Eingabedatei herunter, um die Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den NetScaler ADM Server hoch.
   b) Geben Sie gemeinsame Werte für die Variablen ein, die Sie für alle Instanzen definiert haben
8. Klicken Sie auf **Weiter**.



9. Auf der Registerkarte **Vorlagenvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen. Klicken Sie auf **Weiter**.
10. Auf der Registerkarte **Zeitplanvorlage** haben Sie drei Optionen, um die Ausführung der Vorlage zu automatisieren, und die E-Mail-Adresse, an die der Vergleichsbericht gesendet werden soll.
    - **Verwenden Sie das globale Polling-Intervall** Wählen Sie diese Option, um die Vorlage auf den Instanzen zu einem global konfigurierten Zeitpunkt in NetScaler ADM auszuführen.
    - **Anpassen des Vorlagenzeitplans**. Verwenden Sie diese Option, um die Zeit und die Häufigkeit zu konfigurieren, mit der die Vorlagen ausgeführt werden müssen
    - **Bericht per E-Mail senden**. Verwenden Sie diese Option, um das E-Mail-Profil zu konfigurieren, an das der Diff-Bericht als E-Mail-Anhang gesendet werden muss.
11. Klicken Sie auf **Fertig stellen**.

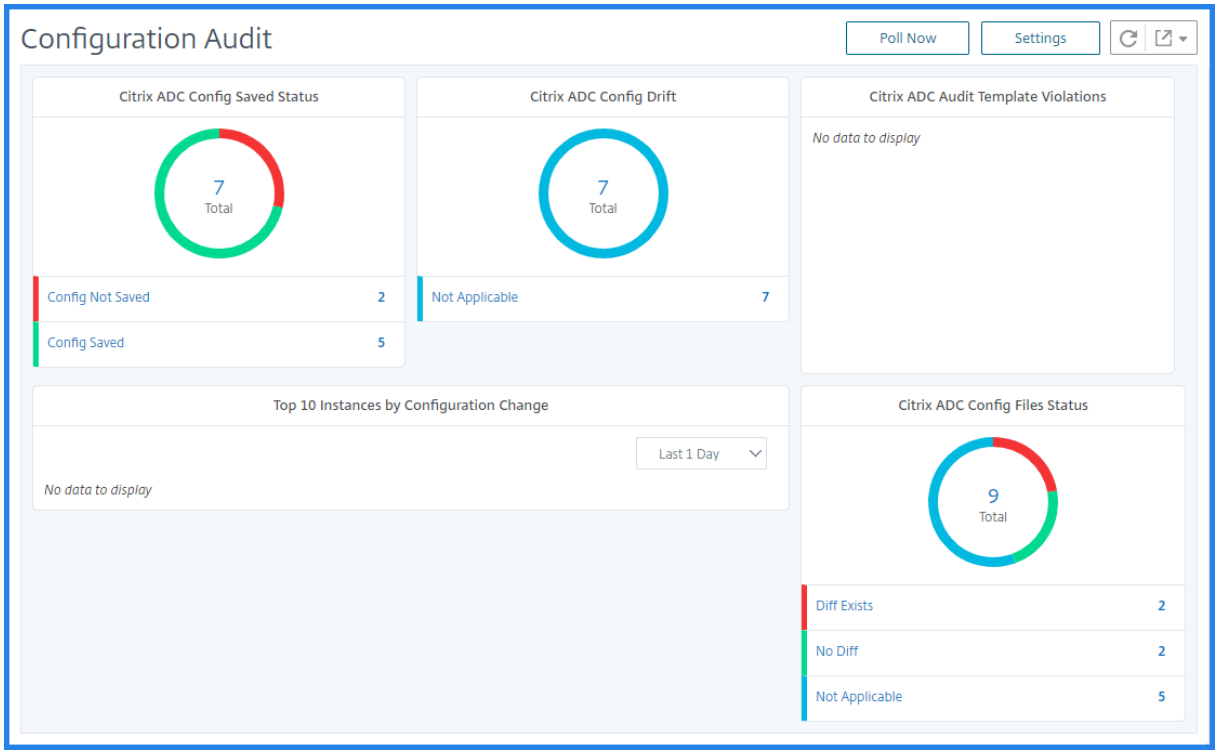


Die Überwachungsvorlage wird in der Liste Überwachungsvorlagen angezeigt und zum geplanten Zeitpunkt für die Konfigurationen in den angegebenen Instanzen ausgeführt.

Details von Konfigurationsänderungen anzeigen

Sie können das Dashboard Configuration Audit auch verwenden, um Details zu Konfigurationsänderungen auf hoher Ebene anzuzeigen, z. B.:

- Die zehn häufigsten Instanzen nach Konfigurationsänderungen
- Die Anzahl der gespeicherten und nicht gespeicherten Konfigurationen
- Die im`nsconfig` Ordner hinzugefügte, entfernte oder geänderte Datei

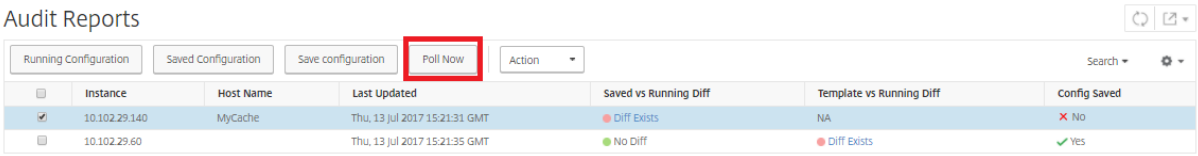


Mit NetScaler ADM können Sie Konfigurationsaudits manuell abfragen und alle Konfigurationsaudits der Instanzen sofort dem NetScaler ADM hinzufügen. Navigieren Sie dazu zu "**Netzwerke**>**Konfigurationsüberwachung",** klicken Sie auf "**Jetzt abfragen** ". Auf der Popupseite "**Jetzt** abfragen"können Sie alle Citrix ADC Instanzen im Netzwerk abfragen oder die ausgewählten Instanzen abfragen.

Sie können auch eine Prüfung für eine Instanz erzwingen. Klicken Sie dazu auf eines der folgenden Diagramme:

- **Status der gespeicherten NetScaler ADC Konfiguration**
- **NetScaler ADC Konfigurationsdrift**

Wählen Sie auf der Seite **Überwachungsberichte** die Instanz aus, und wählen Sie in der Liste **Aktion** die Option **Jetzt abfragen** aus.



Das Diagramm **Status der NetScaler ADC Konfigurationsdatei** enthält den Status der NetScaler ADC Dateien, die im`nsconfig` Ordner vorhanden sind. NetScaler ADM zeichnet Änderungen in Dateien innerhalb des Ordners `nsconfig`auf und vergleicht diese und zeigt die Unterschiede an. Weitere Informationen finden Sie unter Anzeigen der Berichte zur Dateistatusprüfung

Konfigurationsüberwachungsbenachrichtigungen festlegen

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaudit**.
2. Klicken Sie auf der Seite **Konfigurationsüberwachung** auf **Einstellungen**.
3. Klicken Sie auf der Seite mit den **Benachrichtigungseinstellungen** auf das Symbol **Bearbeiten**, um die Benachrichtigungseinstellungen zu aktivieren.
4. Aktivieren Sie das Kontrollkästchen **Aktiviert**, und wählen Sie dann eine E-Mail-Verteilerliste aus der Dropdownliste aus. Sie können auch eine E-Mail-Verteilerliste erstellen, indem Sie auf das Symbol **+** klicken und Details des E-Mail-Servers angeben.

Konfigurationshinweise zur Netzwerkkonfiguration erhalten

February 5, 2024

Sie richten Ihre Citrix Application Delivery Controller (ADC) -Instanzen mit optimalen Konfigurationen ein, damit Sie eine optimale Leistung für Ihre Anwendungen erzielen können. Einige Konfigurationen sind jedoch möglicherweise keine Standardkonfigurationen, die sich auf die Leistung Ihrer Anwendungen auswirken können.

Um die Anwendungsleistung zu optimieren, analysiert NetScaler Application Delivery Management (NetScaler ADM) die Konfiguration der NetScaler ADC Instanz und gibt Empfehlungen. Sie können die empfohlenen Konfigurationen von NetScaler ADM anwenden.

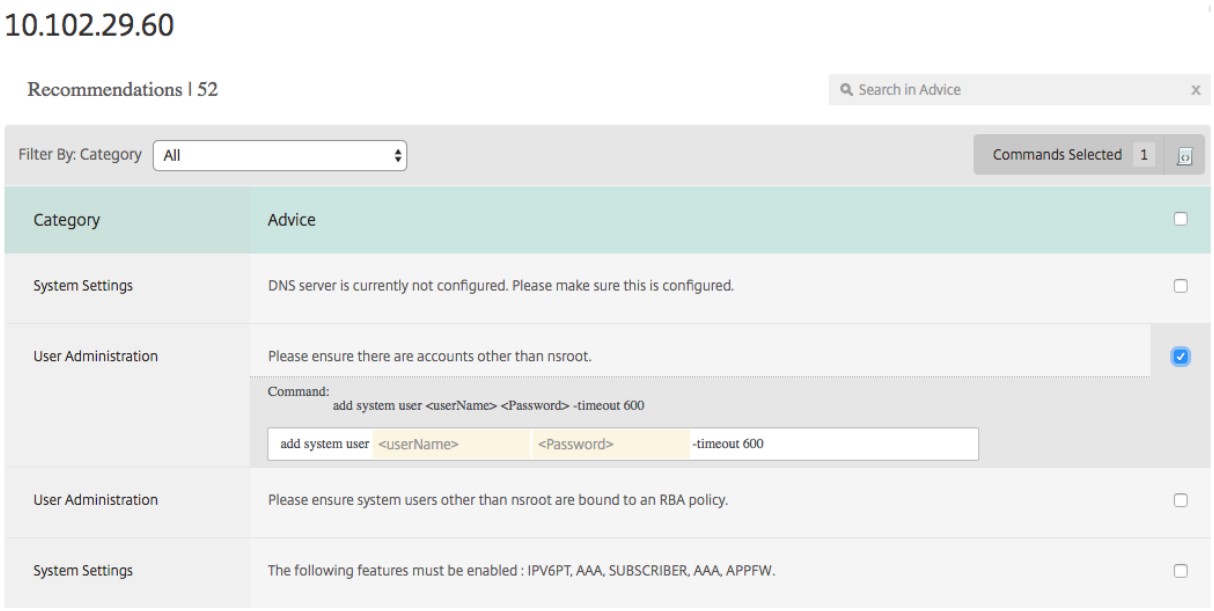
So analysieren Sie die NetScaler ADC-Instanz:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsüberwachung** > **Konfigurationshinweise**.
2. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf **Konfigurationsdatei** hochladen und laden Sie die Konfigurationsdatei Ihrer Netzwerkinstanz hoch.

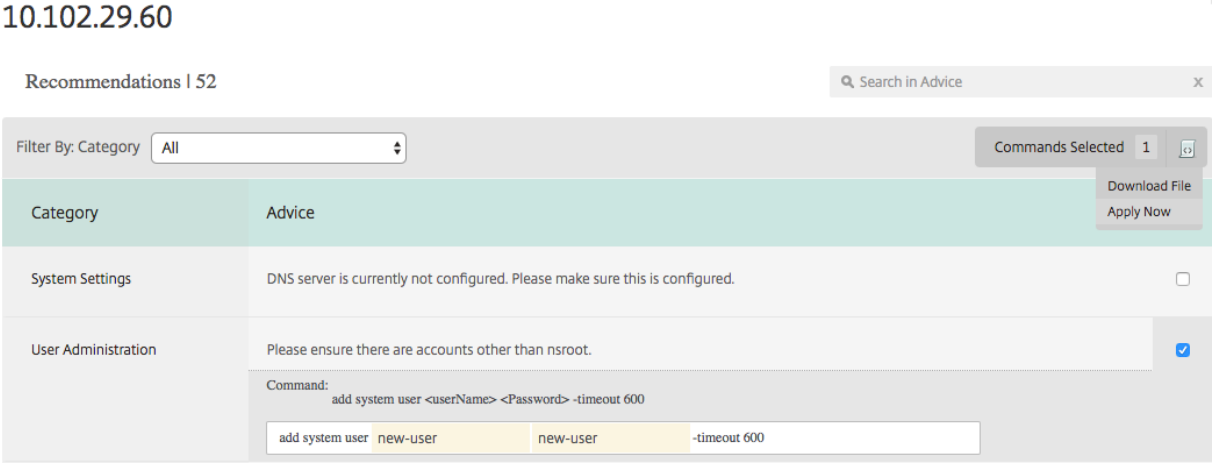
   - Klicken **Sie auf Gerät** auswählen und wählen Sie die NetScaler ADC Instanz aus, die Sie analysieren möchten.

NetScaler ADM analysiert die Konfiguration auf Ihrer Instanz und stellt eine Liste von Konfigurationsempfehlungen bereit, wie in der folgenden Abbildung gezeigt. Aktivieren Sie das Kontrollkästchen neben einer Konfigurationsempfehlung, um die Korrekturbefehle anzuzeigen.

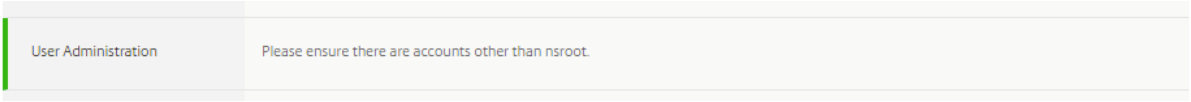


Wenn Sie Ihre Konfiguration aktualisieren möchten, geben Sie die Werte für die Variablen in den Korrekturbefehlen an und klicken Sie auf **Jetzt anwenden**, wie in der folgenden Abbildung gezeigt.

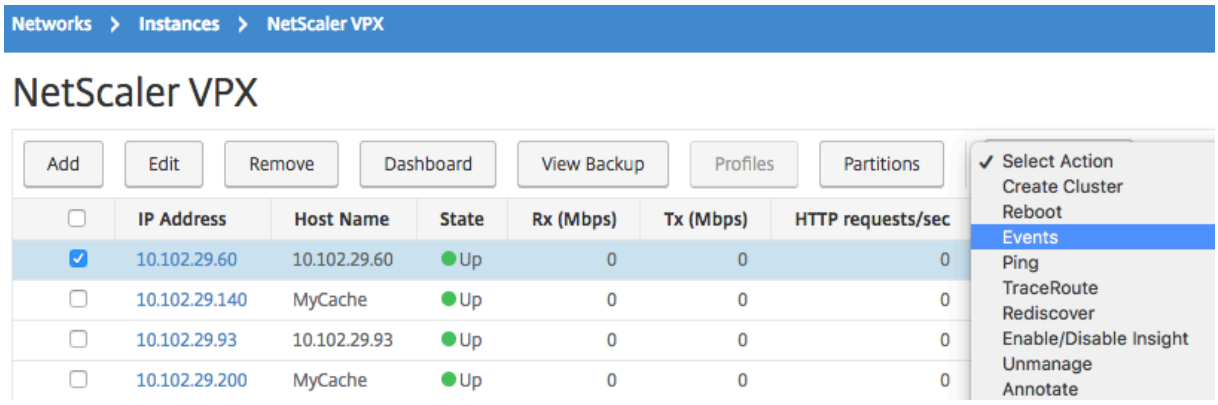
> **Hinweis:**
>
> Die hier aufgeführten Befehle sind nur Empfehlungen. Ein Benutzer mit Lese- und Schreibzugriff kann unter Umständen beliebige Befehle mit dieser Funktion bearbeiten. Stellen Sie sicher, dass Sie Benutzern einen eingeschränkten privilegierten Zugriff gewähren, von denen Sie glauben, dass sie die Befehle nicht bearbeiten dürfen.



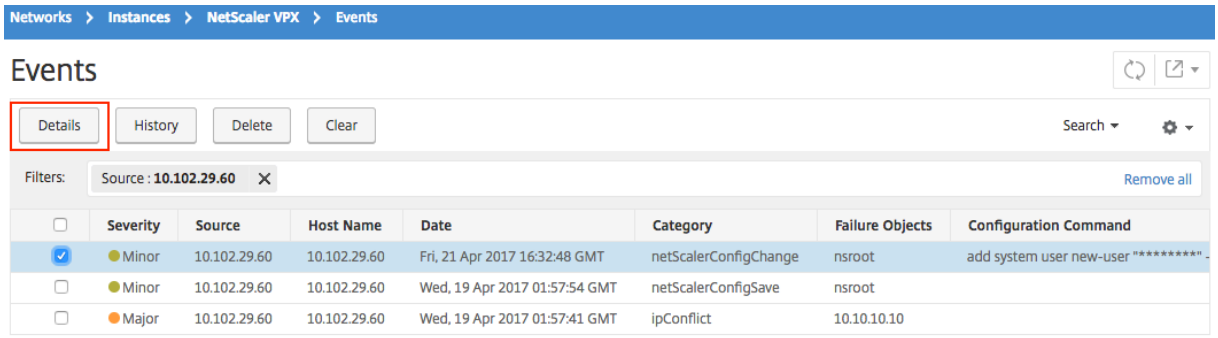
Wenn der Befehl auf der Netzwerkinstanz erfolgreich ausgeführt wird, wird das Kontrollkästchen neben dem Hinweis ausgeblendet.



Wenn Sie die Details der Befehle anzeigen möchten, die auf Ihrer Netzwerkinstanz ausgeführt werden, navigieren Sie zu **Netzwerke > Instanzen > <Instance_Type\>**, wählen Sie die IP-Adresse der Instanz aus und klicken Sie dann in der Dropdownliste **Aktionen** auf **Ereignisse**.



Auf der Seite **Ereignisse** können Sie die Details der Konfigurationsänderung anzeigen.



Konfigurationsprüfung von NetScaler ADC-Instanzen abfragen

February 5, 2024

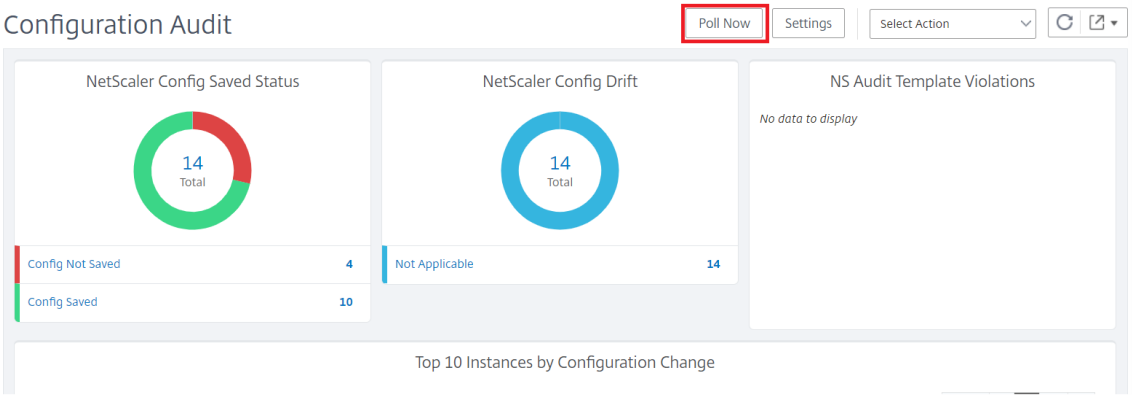
Citrix Application Delivery Management (Citrix ADM) ruft die Konfigurationsaudits automatisch alle 10 Stunden ab, um nach Konfigurationsänderungen zu suchen, die auf ADC-Instanzen (Citrix Application Delivery Controller) auftreten. Sie können die Konfigurationsprüfungen auch manuell abfragen, um die letzten Änderungen zu erkennen. Das Abrufen aller NetScaler ADC-Instanzen führt jedoch zu einer hohen Belastung des Netzwerks.

Anstatt die gesamte Konfigurationsüberwachung der NetScaler ADC-Instanzen abzufragen, können Sie nur die Konfigurationsaudits einer ausgewählten Instanz oder Instanzen manuell abfragen.

So fragen Sie Konfigurationsaudits von NetScaler ADC-Instanzen ab:

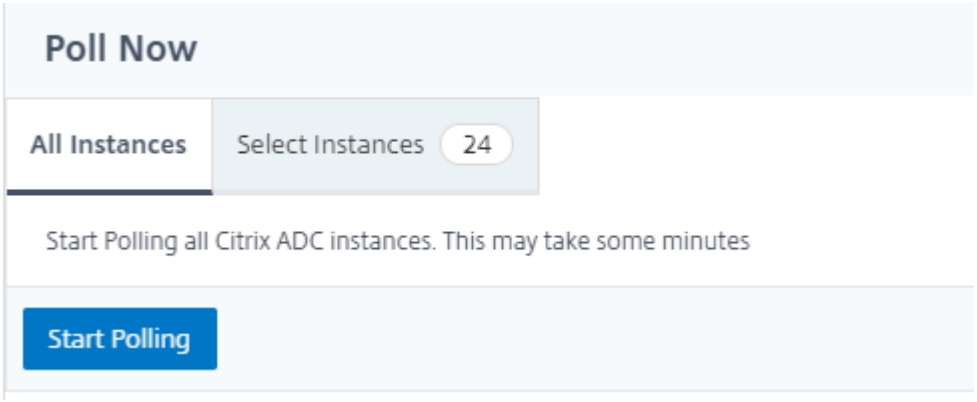
1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Konfigurationsüberwachung**.

2. Klicken Sie auf der Seite **Konfigurationsüberwachung** oben rechts auf **Jetzt abfragen**.

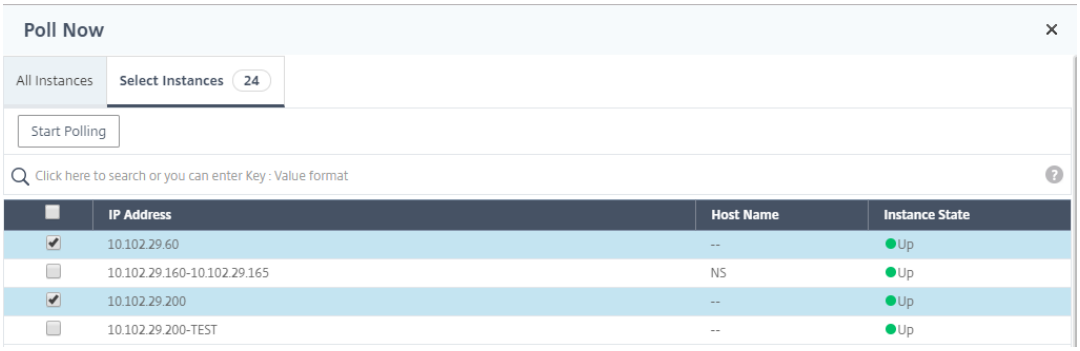


3. Die Seite **Jetzt abfragen** wird geöffnet und bietet Ihnen die Möglichkeit, alle NetScaler ADC-Instanzen im Netzwerk abzufragen oder ausgewählte Instanzen abzufragen.

   a) Um alle NetScaler ADC-Instanzen abzufragen, wählen Sie die Registerkarte **Alle Instanzen**, und klicken Sie auf **Polling starten**.



   b) Um bestimmte Instanzen abzufragen, wählen Sie die Registerkarte**Instanzenauswählen**aus, wählen Sie die Instanzen aus der Liste aus und klicken Sie auf**Jetzt abfragen**.



Konfigurations-Audit-Diff für ConfigChange SNMP-Traps generieren

February 5, 2024

Bei jeder Konfigurationsänderung in einer Citrix Application Delivery Controller (ADC) -Instanz im Netzwerk wird die Konfigurationsdatei aktualisiert. Die Instanz sendet einen ConfigChange SNMP-Trap an Citrix Application Delivery Management (Citrix ADM). Sie können NetScaler ADM aktivieren, um eine Konfigurationsüberprüfung für diese Instanz durchzuführen, wenn die Instanz einen ConfigChange SNMP-Trap sendet.

Wenn ein Unterschied zwischen der Konfiguration der Überwachungsvorlage und der laufenden Konfiguration besteht, wird auf der Seite Überwachungsbericht eine Statusmeldung "Diff Existiert "angezeigt. Wenn Sie auf den Link Diff Exits klicken, gelangen Sie zur Seite Configuration Diff, auf der Sie den Korrekturbefehl anzeigen können. Sie können diese fehlerbehebenden Befehle verwenden, um einen Konfigurationsauftrag zu erstellen und diesen auf den spezifischen NetScaler ADC-Instanzen auszuführen. Wenn Sie den Konfigurationsauftrag ausführen, werden die Instanzen zur gewünschten Konfiguration zurückgesetzt. Weitere Informationen zum Erstellen eines Konfigurationsauftrags aus fehlerbehebenden Befehlen finden Sie unter Erstellen von Konfigurationsaufträgen aus fehlerbehebenden Befehlen auf NetScaler ADM.

So führen Sie Konfigurationsüberwachungsvorlagen beim Empfang von ConfigChange SNMP-Trap aus:

Mit NetScaler ADM können Sie die Option zum Ausführen der Konfigurationsüberwachungsvorlage in NetScaler ADM aktivieren.

1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Konfigurationsüberwachung**.
2. Klicken Sie auf der Seite **Konfigurationsüberwachung** auf**Einstellungen**.
3. Klicken Sie im Abschnitt **Überwachungseinstellungen für Konfigurationsänderungen** auf das Symbol Bearbeiten.
4. Aktivieren Sie das Kontrollkästchen **Konfigurationsprüfung durchführen, wenn das NetScalerConfigChange-Ereignis empfangen wird** .

> **Hinweis**
>
> Dies ist eine globale Einstellung für alle Instanzen. NetScaler ADM führt eine Konfigurationsüberprüfung für jede Instanz durch, in der es in Zukunft die NetScalerConfigChange SNMP-Traps erhält.

1. **Geben Sie im Feld Zeitverzögerung für die Ausführung der Prüfungsvorlage (in Minuten) die Minuten ein. NetScaler ADM führt die Konfigurationsüberwachungsvorlage auf der NetScaler ADC-Instanz nach dieser Zeitverzögerung aus, wenn sie das ConfigChange-SNMP-Trap von dieser Instanz empfängt.

Netzwerkfunktionen

February 5, 2024

Mit der Funktion Netzwerkfunktionen können Sie den Status der Entitäten überwachen, die auf Ihren verwalteten Citrix Application Delivery Controller (ADC) -Instanzen konfiguriert sind. Sie können Statistiken wie Transaktionsdetails, Verbindungsdetails und Durchsatz eines virtuellen Lastausgleichsservers anzeigen. Sie können die Entitäten auch aktivieren oder deaktivieren, wenn Sie eine Wartung planen.

Das Dashboard "Netzwerkfunktionen"bietet Ihnen die folgenden Grafiken:

- Top 5 virtuelle Server mit den höchsten Client-Verbindungen
- Top 5 virtuelle Server mit den höchsten Serververbindungen
- Top 5 virtuelle Server mit maximalem Durchsatz (MB/s)
- Unterste 5 virtuelle Server mit niedrigstem Durchsatz (MB/s)
- Top 5 Instanzen mit den meisten virtuellen Servern
- Status der virtuellen Server
- Integrität der virtuellen Lastausgleichsserver
- Protokolle

Berichte für Lastausgleichseinheiten generieren

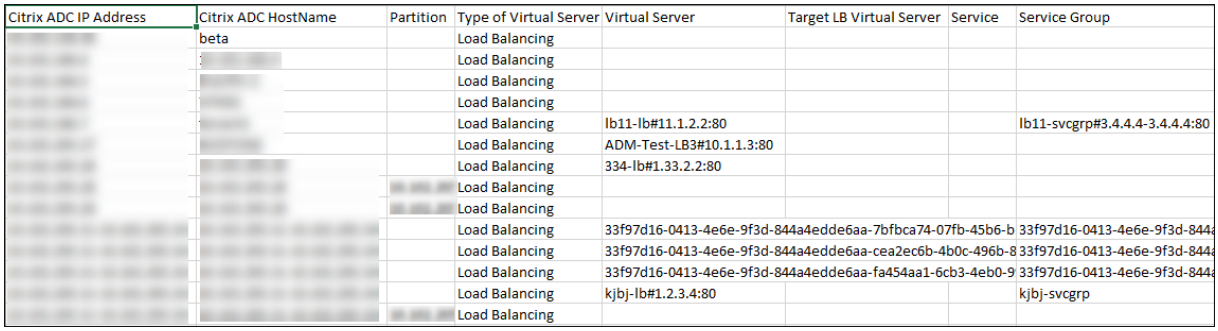
February 5, 2024

Mit Citrix Application Delivery Management (ADM) können Sie die Berichte der Citrix Application Delivery Controller (ADC) -Instanzentitäten auf allen Ebenen anzeigen. Es gibt zwei Arten von Berichten, die Sie in NetScaler ADM > Netzwerkfunktionen herunterladen können: konsolidierte Berichte und einzelne Berichte.

Konsolidierte Berichte: Sie können einen konsolidierten oder zusammenfassenden Bericht für alle Entitäten herunterladen und anzeigen, die auf NetScaler ADC-Instanzen verwaltet werden.

Mit diesem Bericht erhalten Sie einen Überblick über die Zuordnung zwischen den NetScaler ADC-Instanzen, Partitionen und den entsprechenden Lastausgleichseinheiten (virtuelle Server, Dienstgruppen und Dienste), die im Netzwerk vorhanden sind.

Die folgende Abbildung zeigt ein Beispiel für einen zusammengefassten Bericht.



Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
	beta		Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:80
			Load Balancing	ADM-Test-LB3#10.1.1.3:80			
			Load Balancing	334-lb#1.33.2.2:80			
			Load Balancing				
			Load Balancing				
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-9			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
			Load Balancing				

Der konsolidierte Bericht hat ein CSV-Format. Die Einträge in jeder Spalte werden wie folgt beschrieben:

- **NetScaler-IP-Adresse: Die**IP-Adresse der Citrix ADC-Instanz wird im Bericht angezeigt
- **NetScaler HostName**: Der Hostname wird im Bericht angezeigt.
- **Partition**: Die IP-Adresse der administrativen Partition wird angezeigt
- **Virtueller Server**: <name_of_the_virtual_server>#virtual_IP_address :port_number
- **Dienste**: <name_of_the_service>#service -IP_Adresse:Port_Number
- **Dienstgruppen**: <name_of_service_group>#Server_Member1_IP_Adresse:Port, Server_Member2_IP_Adre Server_Member3_IP_Adresse:Port,…, Server_Membern_IP_Address:Port

> **Hinweis**
>
> - Wenn kein Hostname verfügbar ist, wird die entsprechende IP-Adresse angezeigt.
> - Leere Spalten geben an, dass die entsprechenden Entitäten für diese NetScaler ADC-Instanz nicht konfiguriert sind.

Einzelberichte: Sie können auch unabhängige Berichte aller Instanzen und Entitäten herunterladen und anzeigen. Sie können beispielsweise einen Bericht nur für virtuelle Lastausgleichsserver oder Lastausgleichsdienste oder Lastausgleichsdienstgruppen herunterladen.

Mit NetScaler ADM können Sie den Bericht sofort herunterladen. Sie können den Bericht auch so planen, dass er einmal täglich, einmal pro Woche oder einmal pro Monat zu einem festen Zeitpunkt erstellt wird.

Erstellen eines kombinierten Lastausgleichsberichts

1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Netzwerkfunktionen** > **Lastenausgleich**.
2. Klicken Sie auf der Seite **Load Balancing** .
3. Auf der sich öffnenden Seite **Exportieren** haben Sie zwei Optionen, um den Bericht anzuzeigen:

a) Wählen Sie die Registerkarte **Jetzt exportieren** und klicken Sie auf **OK**.

   Der konsolidierte Bericht wird auf Ihr System heruntergeladen.

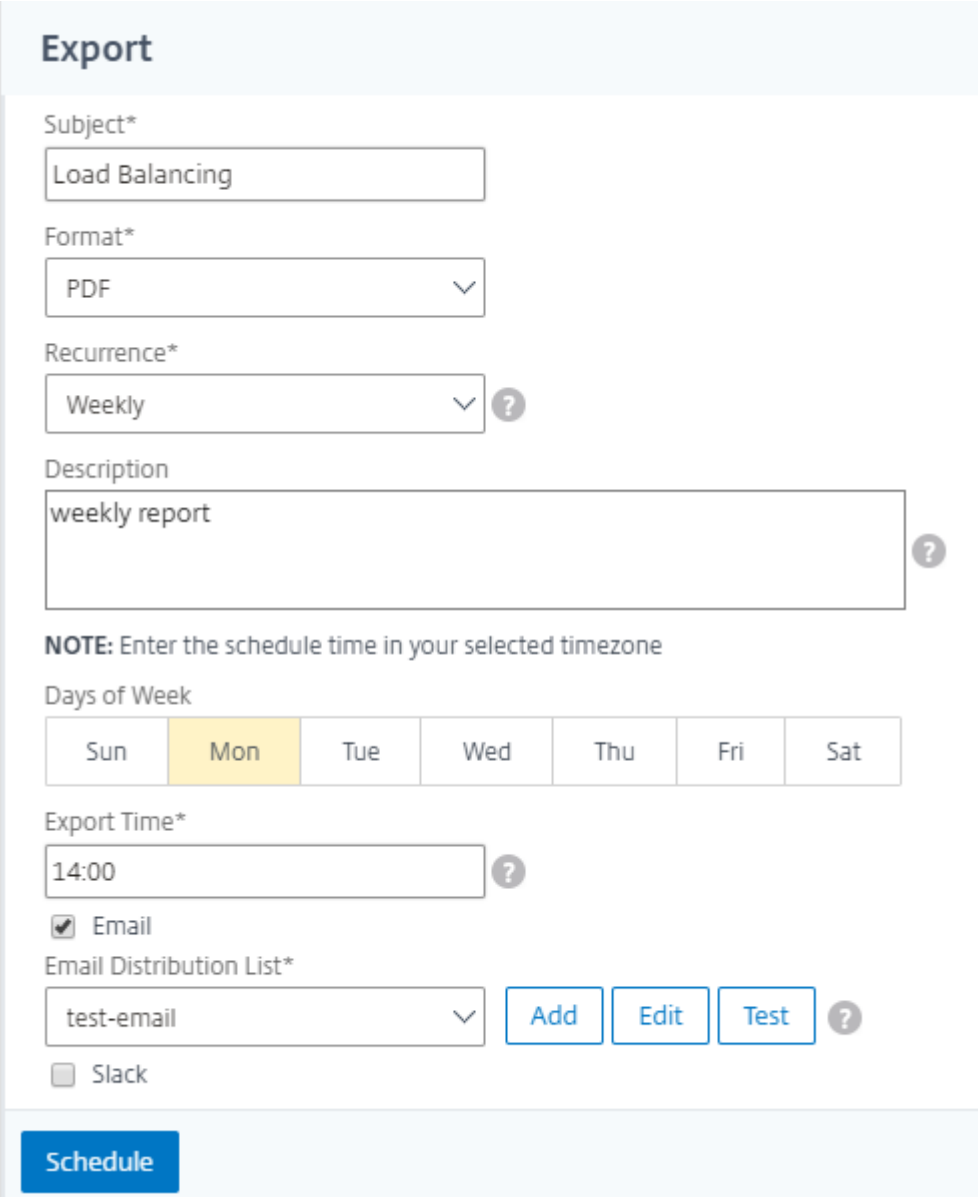
b) Wählen Sie die Registerkarte **Bericht planen**, um das Generieren und Exportieren des Berichts in regelmäßigen Abständen zu planen. Geben Sie die Einstellungen für die Berichtsgenerierung an, und erstellen Sie ein E-Mail-Profil, in das der Bericht exportiert wird.

   i. **Wiederholung** —wählen Sie im Drop-down-Listenfeld die Option **Täglich**, **Wöchentlich**oder **Monatlich** aus.

   ii. **Wiederholungszeit** —Geben Sie die Zeit als Stunde:Minute im 24-Stunden-Format ein.

   iii. **E-Mail-Profil** - Wählen Sie ein Profil aus dem Dropdownlistenfeld aus, oder klicken Sie auf **+**, um ein E-Mail-Profil zu erstellen.

> **Hinweis**
>
> Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.



Hinweis

Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

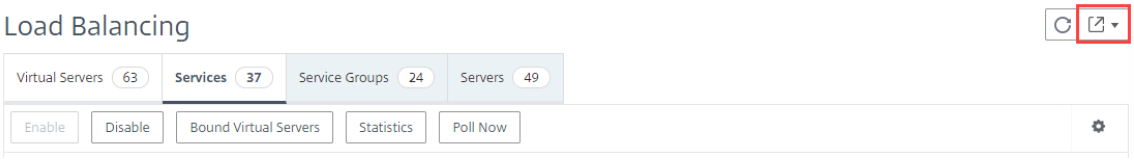
Erstellen eines individuellen Lastausgleichsentitätsberichts

Sie können einen individuellen Bericht für einen bestimmten Entitätstyp generieren und exportieren, der den Instanzen zugeordnet ist. Betrachten Sie beispielsweise ein Szenario, in dem Sie eine Liste aller Lastausgleichsdienste im Netzwerk anzeigen möchten.

1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Netzwerkfunktionen** > **Load Balancing >**

Services.

2. Klicken Sie auf der Seite **Dienste** oben rechts auf die Schaltfläche **Exportieren**.



   a) Wählen Sie die Registerkarte **Jetzt exportieren**, wenn Sie den Bericht in diesem Moment generieren und anzeigen möchten.

   b) Wählen Sie **Export planen**, um die Generierung und den Export des Berichts in regelmäßigen Abständen zu planen.

> **Hinweis**
>
> Sie können die Berichte nur herunterladen oder als E-Mail-Anhänge exportieren. Sie können die Berichte auf der NetScaler ADM GUI nicht anzeigen.

Netzwerkfunktionenberichte exportieren oder planen

February 5, 2024

Sie können einen umfassenden Bericht für ausgewählte Netzwerkfunktionen wie Load Balancing, Content Switching, Cache-Umleitung, Global Server Load Balancing (GSLB), Authentifizierung und NetScaler Gateway in NetScaler Application Delivery Management (ADM) generieren. Dieser Bericht ermöglicht Ihnen einen allgemeinen Überblick über die Zuordnung zwischen den NetScaler ADC-Instanzen, Partitionen und den entsprechenden gebundenen Entitäten (virtuelle Server, Dienstgruppen und Dienste), die im Netzwerk vorhanden sind. Sie können diese Berichte im CSV-Dateiformat exportieren.

Der Bericht zeigt die folgenden virtuellen Serverdaten an:

- NetScaler IP-Adresse
- Hostname
- Daten partitionieren
- Name des virtuellen Servers
- Typ des virtuellen Servers
- Virtueller Server
- Virtueller LB-Zielserver

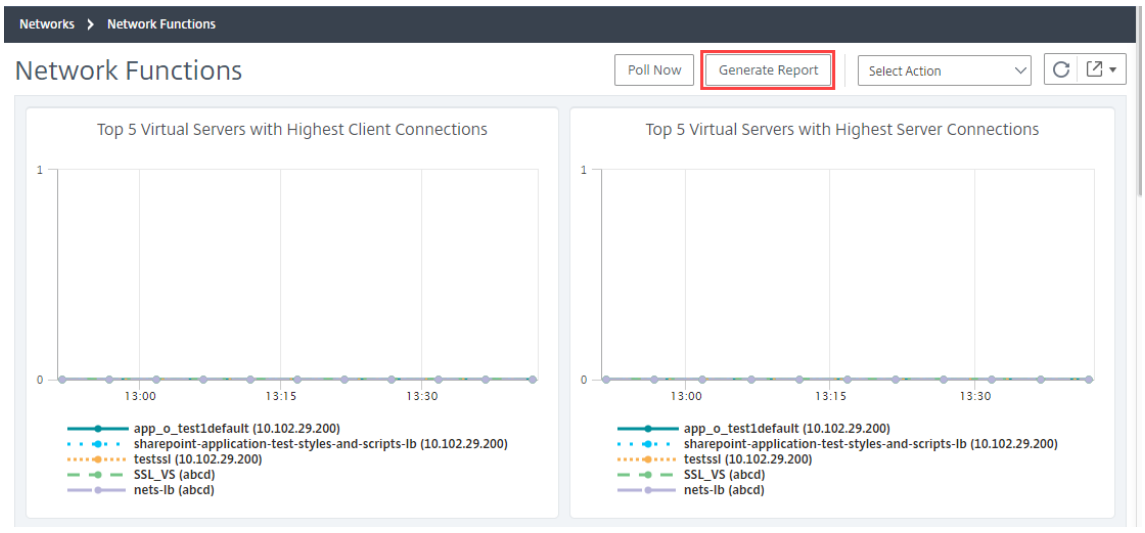
> **Hinweis**
>
> Für virtuelle Server mit Content Switching und Cache-Umleitung werden in der Spalte Virtueller Ziel-LB-Server alle LB-Server aufgeführt, d. h. sowohl Standardserver als auch richtlinienbasierte Server.
>
> - Name des Dienstes
> - Name der Dienstgruppe

Sie können planen, diese Berichte in unterschiedlichen Intervallen an bestimmte E-Mail-Adressen zu exportieren.

> **Hinweis**
>
> - Bei virtuellen GSLB-Servern werden im Netzwerkfunktionsbericht nur virtuelle GSLB-Server und zugehörige Dienste angezeigt.
> - Für virtuelle Server für Content Switching und Cache-Umleitung zeigt der Bericht nur die Bindungen an die zugeordneten LB-Server an.
> - Virtuelle SSL-Server werden in diesem Bericht nicht aufgeführt, da in NetScaler ADM keine separate Liste virtueller SSL-Server verwaltet wird.
> - Wenn ein neuer Bericht generiert wird, werden die älteren Berichte automatisch aus Ihrem Konto gelöscht.
> - Sie können keinen Netzwerkfunktionsbericht für HAProxy generieren.

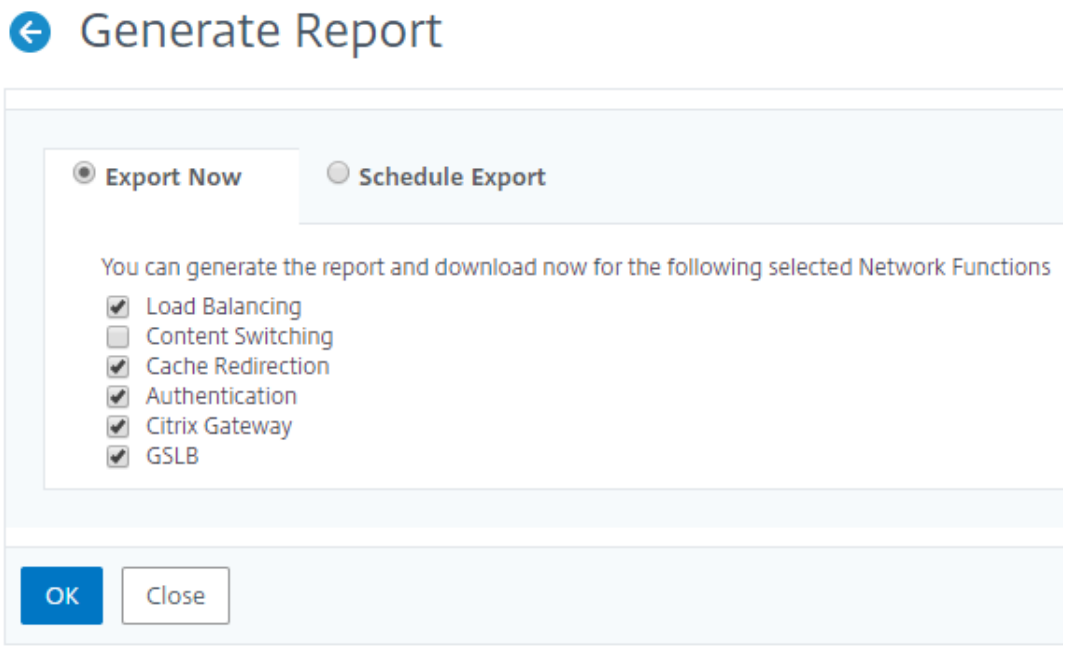
So exportieren und planen Sie Berichte über Netzwerkfunktionen:

1. Navigieren Sie zu**Netzwerke > Netzwerkfunktionen**.
2. Klicken Sie auf der Seite**Netzwerkfunktionen** im rechten Bereich oben rechts auf der Seite auf**Bericht generieren**.



3. Auf der Seite **Bericht generieren** haben Sie die folgenden 2 Optionen:

   a) Wählen Sie die Registerkarte **Jetzt exportieren** und klicken Sie auf **OK**. Der Bericht wird auf Ihr System heruntergeladen.



   Die folgende Abbildung zeigt ein Beispiel für einen Bericht über Netzwerkfunktionen.

NetScaler ADC IP Address	NetScaler ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
10.	10.		Load Balancing	lb_test_1#10.10.10.10:80		adm_metric_collector_svc_10.106.171.41#10.10	
10.	10.		Load Balancing	lbvs_511#51.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	lbvs_521#52.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	SG_HS_DNS_MON#1.2.22.2:80			sc1
10.	10.		Load Balancing	SG_HS_DNS_MONgdvfffs#1.3.4.5:80			
10.	10.		Load Balancing	atest94#1.1.1.11:80			
10.	10.		Load Balancing	lbvs1_101#1.10.1.1:80			
10.	10.		Load Balancing	lbvs1_1010#1.10.1.10:80			
10.	10.		Load Balancing	lbvs1_10100#1.10.1.100:80			
10.	10.		Load Balancing	lbvs1_10101#1.10.1.101:80			
10.	10.		Load Balancing	lbvs1_10102#1.10.1.102:80			
10.	10.		Load Balancing	lbvs1_10103#1.10.1.103:80			

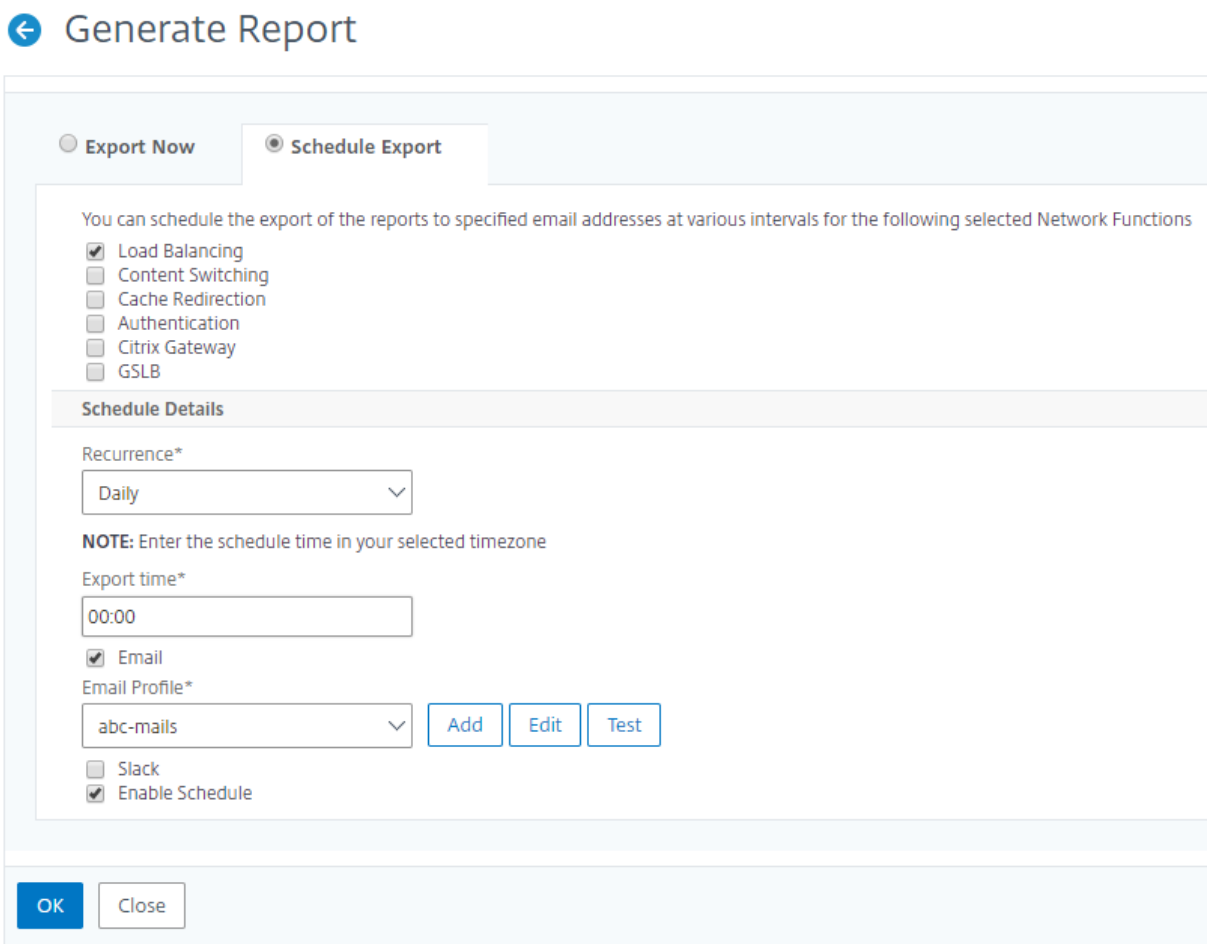
   b) Wählen Sie die Registerkarte**Bericht planen**, um den Bericht in regelmäßigen Abständen zu generieren und zu exportieren. Geben Sie die Einstellungen für die Berichtsgenerierung an, und erstellen Sie ein E-Mail-Profil, in das der Bericht exportiert wird.

      i. **Wiederholung**- Wählen Sie im Dropdownlistenfeld**Täglich**,**Wöchentlich**oder**Monatlich**aus.

      ii. **Wiederholzeit**- Geben Sie die Zeit als Stunde: Minute im 24-Stunden-Format ein.

      iii. **E-Mail-Profil**—Wählen Sie ein Profil aus dem Drop-down-Listenfeld aus, oder klicken Sie auf**+**, um ein E-Mail-Profil zu erstellen.

Klicken Sie auf **Zeitplan aktivieren**, um den Bericht zu planen, und klicken Sie dann auf **OK**. Wenn Sie auf das Kontrollkästchen **Zeitplan aktivieren** klicken, können Sie die ausgewählten Berichte erstellen.



Netzwerkberichterstellung

February 5, 2024

Sie können die Ressourcennutzung optimieren, indem Sie Ihre Netzwerkberichte auf NetScaler Application Delivery Management (NetScaler ADM) überwachen. Möglicherweise verfügen Sie über eine verteilte Bereitstellung mit vielen Anwendungen, die an mehreren Standorten bereitgestellt werden. Um eine optimale Leistung Ihrer Anwendungen zu gewährleisten, haben Sie auch mehrere Citrix Application Delivery Controller (NetScaler ADC) -Instanzen bereitgestellt, um den Datenverkehr auszugleichen, Inhalte zu wechseln oder zu komprimieren. Die Netzwerkleistung kann sich auf die Anwendungsleistung auswirken. Um die Leistung Ihrer Anwendungen weiterhin aufrechtzuerhalten, müssen Sie Ihre Netzwerkleistung regelmäßig überwachen und sicherstellen, dass alle Ressourcen optimal genutzt werden.

Mit NetScaler ADM können Sie jetzt Berichte nicht nur für Instanzen auf globaler Ebene erstellen, sondern auch für Entitäten wie virtuelle Server und Netzwerkschnittstellen. Die Instanzfamilie umfasst

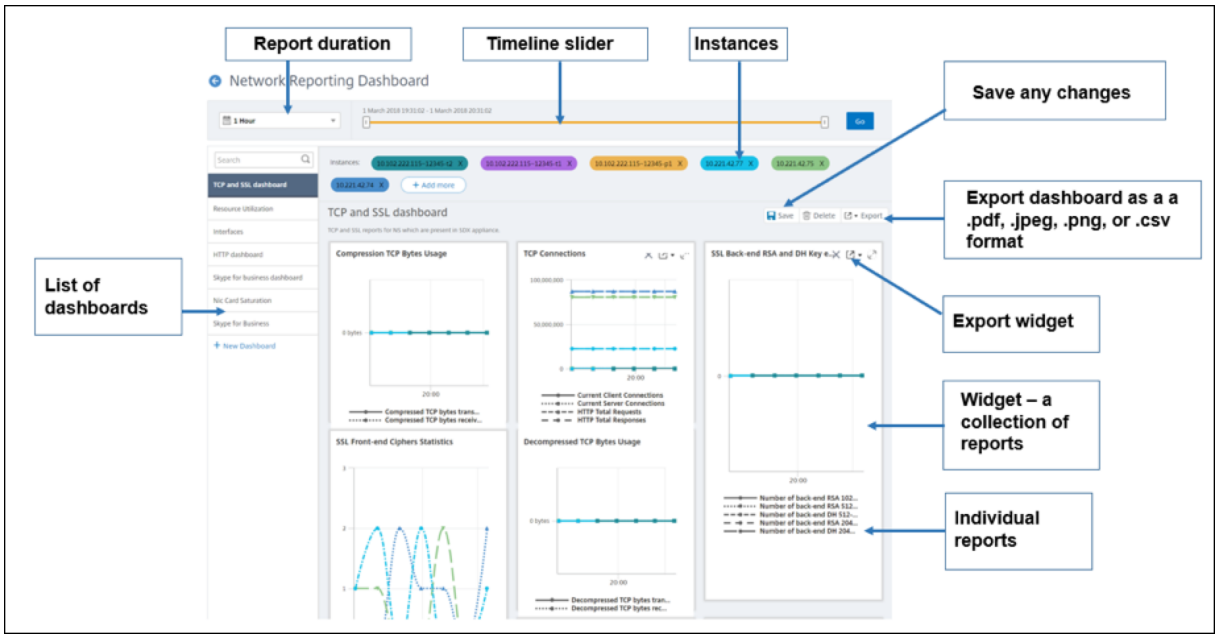
sowohl NetScaler ADC - als auch SD-WAN-Instanzen. Die virtuellen Server, für die Sie Berichte erstellen können, sind wie folgt:

- Load Balancing-Server, Dienste und Dienstgruppen
- Content Switching-Server
- Cache-Umleitungsserver
- Globaler Service Load Balancing (GSLB)
- Authentifizierung
- Citrix Gateway

Das Netzwerkberichts-Dashboard in NetScaler ADM ist hochgradig anpassbar. Sie können jetzt mehrere Dashboards für verschiedene Instanzen, virtuelle Server und andere Entitäten erstellen.

Netzwerkberichterstattungs-Dashboard

Das folgende Bild ruft die verschiedenen Funktionen im Dashboard auf:



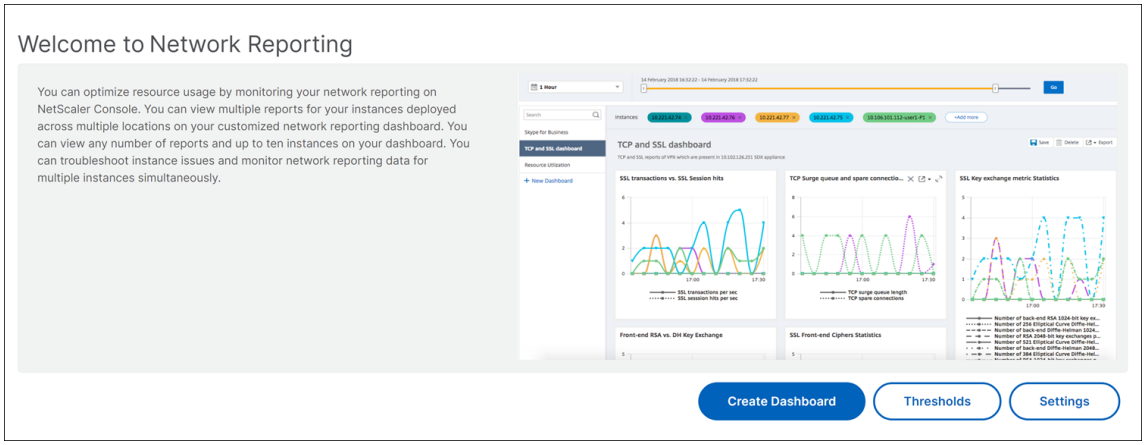
- Im linken Bereich werden alle benutzerdefinierten Dashboards aufgelistet, die in NetScaler ADM erstellt werden. Sie können auf einen von ihnen klicken, um die verschiedenen Berichte anzuzeigen, aus denen das Dashboard besteht. Beispielsweise enthält ein TCP- und SSL-Dashboard verschiedene Berichte, die sich auf TCP und SSL-Protokolle beziehen.
- Sie können jedes Dashboard mit mehreren Widgets anpassen, um verschiedene Berichte anzuzeigen. Ein Widget stellt einen Bericht auf dem Dashboard dar, d. h. eine Sammlung von verwandten Berichten. Beispielsweise enthält ein komprimierter TCP-Byte-Nutzungsbericht Berichte für komprimierte TCP-Bytes, die pro Sekunde übertragen und empfangen wurden.

- Sie können Berichte für eine Stunde, einen Tag, eine Woche oder für einen Monat anzeigen. Darüber hinaus können Sie jetzt den Timeline-Schieberegler verwenden, um die Dauer der Berichte anzupassen, die auf dem NetScaler ADM generiert werden.
- Sie können einen Bericht entfernen, indem Sie auf "X"klicken. Sie können den Bericht auch als PDF-, JPEG-, PNG- oder CSV-Format in Ihr System exportieren. Sie können auch einen Zeitpunkt und eine Wiederholung der Erstellung des Berichts planen. Sie können auch eine E-Mail-Verteilerliste konfigurieren, an die die Berichte gesendet werden müssen.
- Im Abschnitt Instanzen oben im Dashboard werden die IP-Adressen aller Instanzen aufgeführt, für die der Bericht generiert wird.
- Sie können Instanzen entweder entfernen, indem Sie auf X klicken oder weitere Instanzen zu den Berichten hinzufügen. Derzeit ermöglicht Ihnen NetScaler ADM jedoch, Berichte für 10 Instanzen anzuzeigen.
- Sie können das gesamte Dashboard auch als PDF-, JPEG-, PNG- oder CSV-Format in Ihr System exportieren. Alle am Dashboard vorgenommenen Änderungen müssen gespeichert werden. Klicken Sie auf Speichern, um die Änderungen zu speichern.

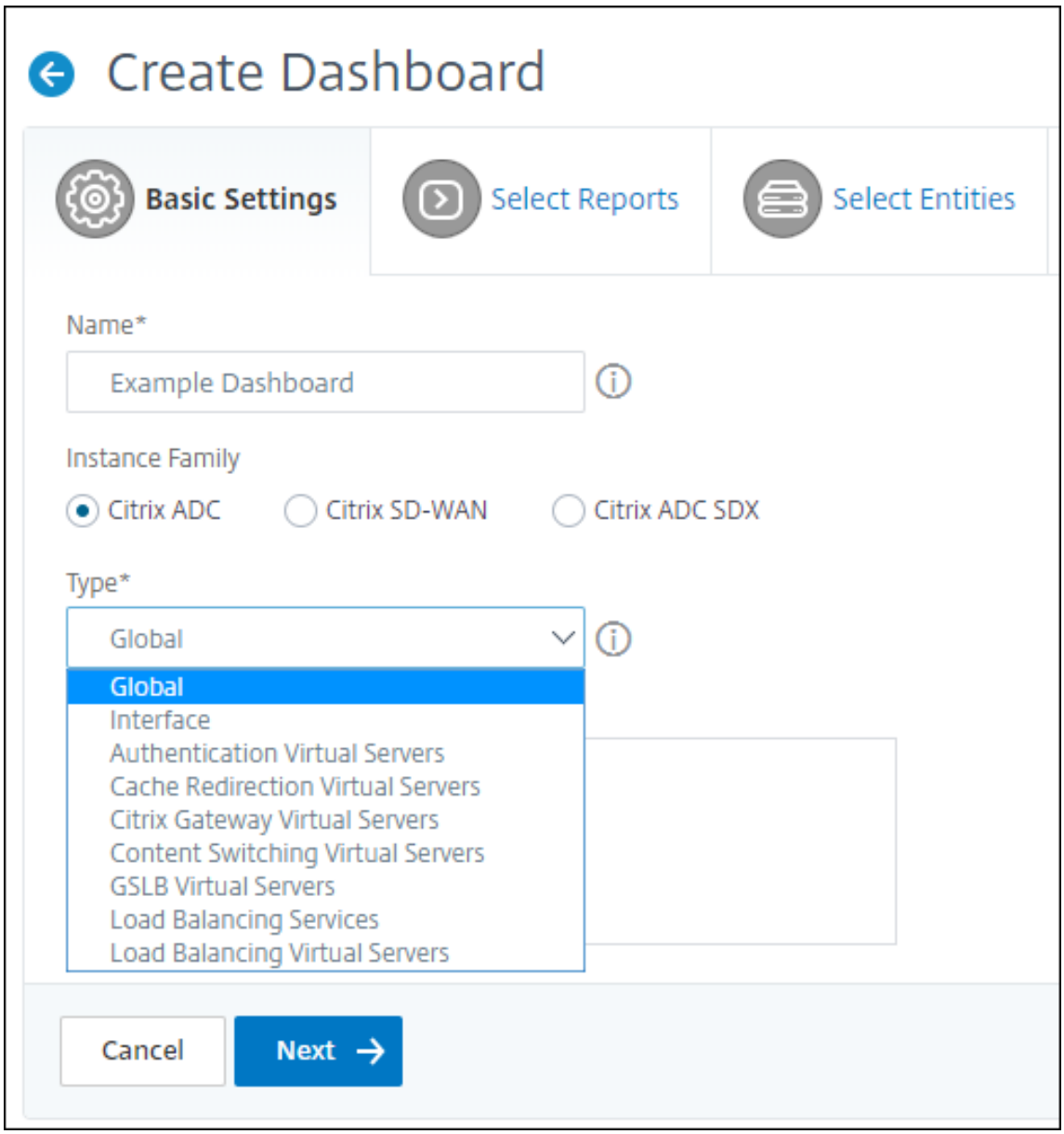
Im folgenden Abschnitt werden ausführlich die Aufgaben zum Erstellen eines Dashboards, zum Generieren von Berichten und zum Exportieren von Berichten erläutert.

So zeigen Sie ein Dashboard an oder erstellen Sie es:

1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Netzwerkberichterstattung**.



2. Klicken Sie auf Dashboard anzeigen, um die vorhandenen **Dashboards anzuzeigen**. Die Seite **Network Reporting Dashboard** wird geöffnet, auf der Sie alle Dashboards und Berichtwidgets anzeigen können.
3. Um ein Dashboard zu erstellen, klicken Sie auf **Neues Dashboard**. Die Seite Dashboard erstellen wird geöffnet.



4. Geben Sie auf der Registerkarte Grundeinstellungen die folgenden Details ein:

   a) **Name**. Geben Sie den Namen des Dashboards ein.

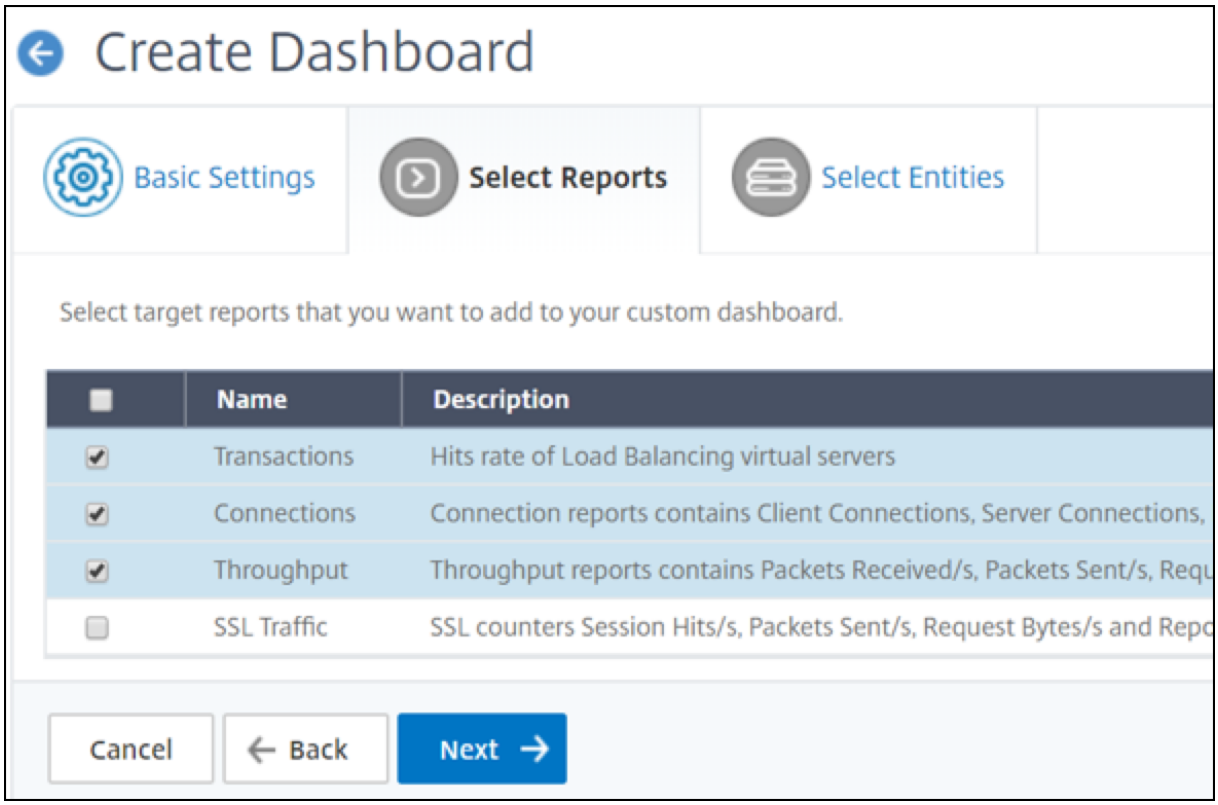
   b) **Instanzfamilie**. Wählen Sie den Instanz-Typ aus - Citrix ADC, Citrix SD-WAN oder Citrix ADC SDX.

   c) **Typ**. Wählen Sie den Entitätstyp aus, für den Sie Berichte erstellen möchten. Wählen Sie in diesem Beispiel virtuelle Server für den Lastenausgleich aus.

   d) **Beschreibung**. Geben Sie eine aussagekräftige Beschreibung für das Dashboard ein.

5. Klicken Sie auf **Weiter**. Alle unterstützten Berichte für die Instanz und die spezifische Entität werden angezeigt.

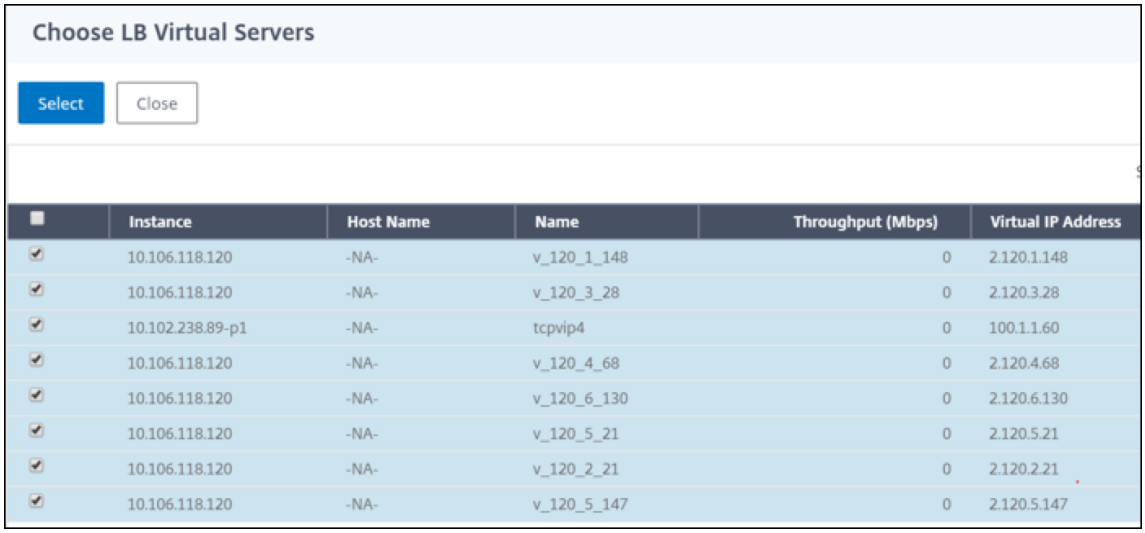
6. **Wählen Sie auf der Registerkarte Berichte** auswählen die erforderlichen Berichte aus. In diesem Beispiel können Sie Transaktionen, Verbindungen und Durchsatz auswählen. Klicken Sie auf **Weiter**.



1. Klicken **Sie auf der Registerkarte Entitäten auswählen** auf **Hinzufügen**.

   Je nach ausgewähltem Entitätstyp auf der Registerkarte **Grundeinstellungen** wird ein Fenster mit der Entitätsliste angezeigt. In diesem Beispiel wird das Fenster **Choose LB Virtual Servers** angezeigt.

2. Wählen Sie die Entitäten aus, die Sie überwachen möchten.



3. Klicken Sie auf **Erstellen**.

Das Dashboard wird erstellt und zeigt alle von Ihnen ausgewählten Berichte an.

> **Hinweis**
>
> Derzeit können Änderungen, die Sie an Legenden oder Filtern vornehmen, nicht gespeichert werden.

Exportieren von Netzwerkberichten

Sie können Widget-Berichte zwar in den Formaten .pdf, .png, .jpeg oder .csv exportieren, aber Sie können die gesamten Dashboards nur in den Formaten .pdf, .jpeg oder .png exportieren.

> **Hinweis**
>
> Sie können keine Berichte in NetScaler ADM exportieren, wenn Sie über schreibgeschützte Berechtigungen verfügen. Sie benötigen eine Bearbeitungsberechtigung, um eine Datei in NetScaler ADM erstellen und die Datei exportieren zu können.

So exportieren Sie Dashboard-Berichte:

1. Navigieren Sie zu **Netzwerke** > **Netzwerkberichterstattung**
2. Klicken Sie auf **Dashboards** anzeigen, um alle von Ihnen erstellten Dashboards anzuzeigen.
3. Klicken Sie im linken Bereich auf ein Dashboard. Klicken Sie in diesem Beispiel auf **Dashboard 1.**
4. Klicken Sie oben rechts auf der Seite auf die Schaltfläche Exportieren.
5. Wählen Sie auf der Registerkarte **Jetzt exportieren** das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.

Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

6. Wählen Sie die Registerkarte **Jetzt exportieren** . Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
7. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht über eine E-Mail oder Slack-Nachricht zu senden.

   Sie können einen Export der Dashboardseite "**Network Reporting-Dashboard** "auf wiederkehrender Basis planen. Sie können beispielsweise eine Option festlegen, um wöchentlich einen Dashboard-Bericht für die vorherige Stunde zu einem bestimmten Zeitpunkt zu generieren. Der Bericht wird dann jede Woche generiert und zeigt den Status des Dashboards an. Der Bericht überschreibt den Zeit- und Datumsstempel, sofern vom Benutzer festgelegt.

> **Hinweis**
>
> - Wenn Sie Wöchentliche Wiederholung auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie Monatliche Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Bei der Planung von Netzwerkberichten können Sie die Überschrift des Berichts anpassen, indem Sie eine Textzeichenfolge in das **Feld**Betreff eingeben. Der zum geplanten Zeitpunkt erstellte Bericht hat diese Zeichenfolge als Namen.

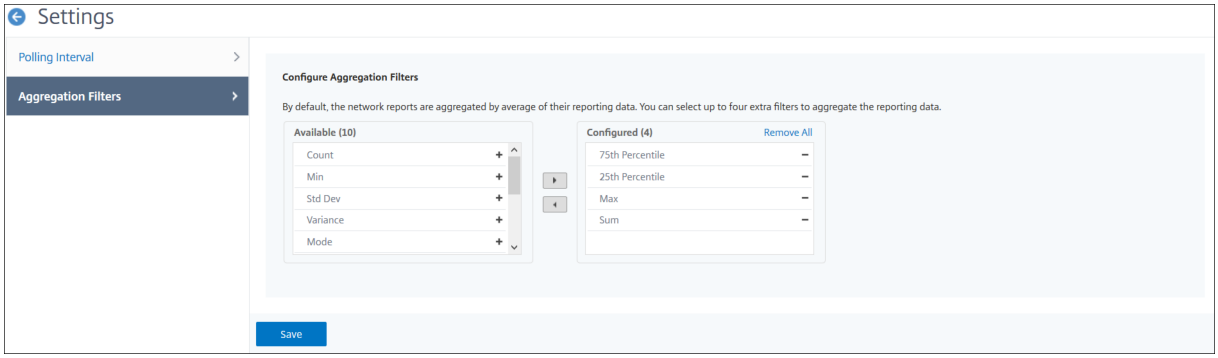
Beispielsweise können Sie für Netzwerkberichte, die von einem bestimmten virtuellen Server stammen, den Betreff als "authentication-reports-10.106.118.120"eingeben, wobei 10.106.118.120 die IP-Adresse des überwachten virtuellen Servers ist.

> **Hinweis**
>
> Derzeit ist diese Option nur verfügbar, wenn Sie den Export von Berichten planen. Sie können dem Bericht keine Überschrift hinzufügen, wenn Sie sie sofort exportieren.

Anzeigen von Netzwerkberichtsdaten durch Anwendung von Aggregationen

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

In den vorhandenen Durchschnittsdaten können Sie Aggregationen anwenden, indem Sie die Option aus der Liste **Anzeigen nach** auswählen. Wenn Sie Aggregation anwenden, werden die Daten für jede Metrik im Dashboard aktualisiert. Klicken Sie auf **Einstellungen** und wählen Sie **Aggregationsfilter**aus.



Im Folgenden finden Sie die Aggregationen, die Sie hinzufügen können:

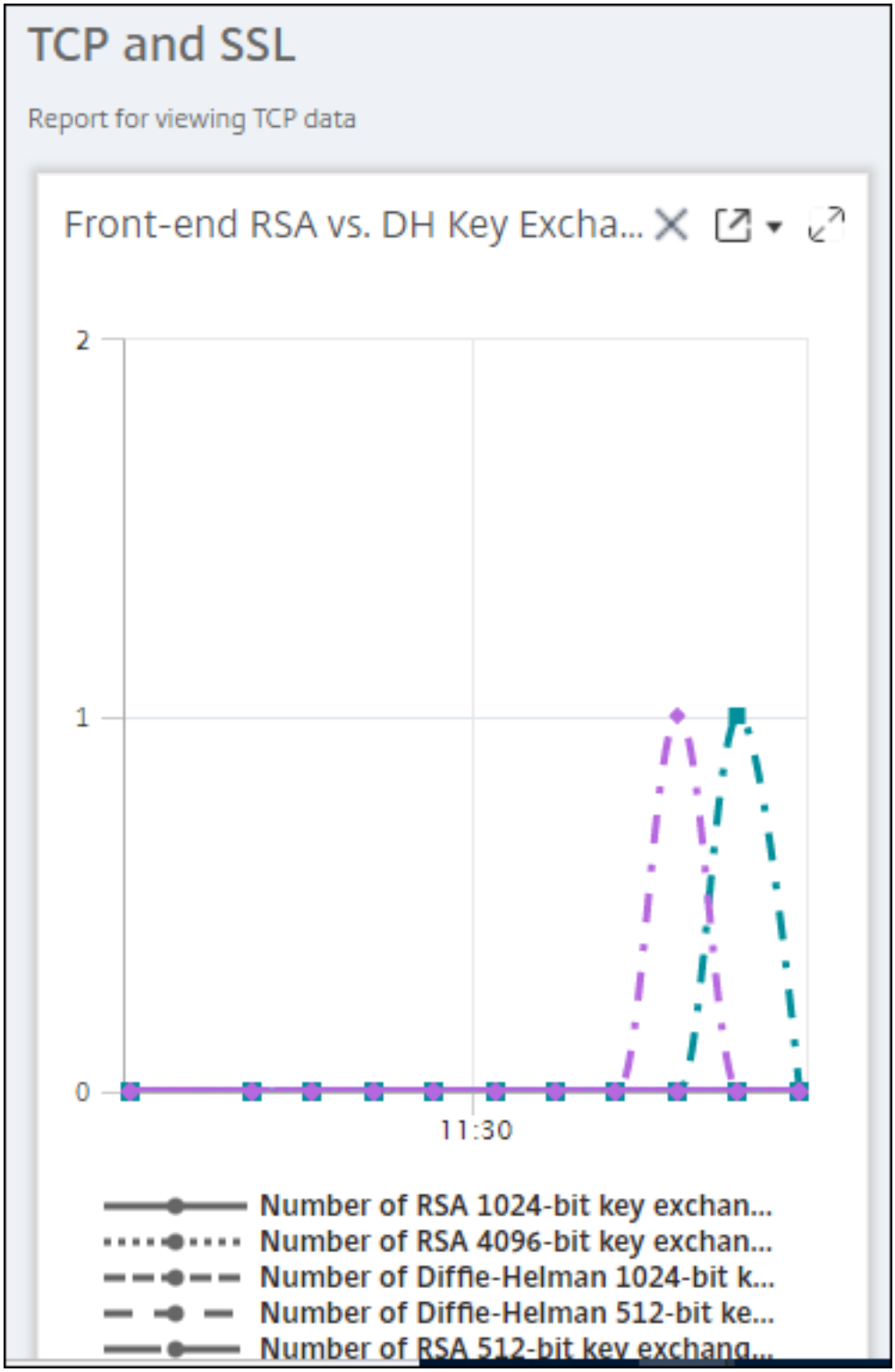
- Anzahl
- Max.
- Min
- Summe
- Std Dev
- Varianz
- Modus
- Median
- 25. Perzentil
- 75. Perzentil
- 95. Perzentil
- 99. Perzentil
- Vorname
- Nachname

Sie können dem Dashboard bis zu 4 Aggregationsoptionen hinzufügen. Nachdem Sie die Aggregationsoptionen hinzugefügt haben, benötigt NetScaler ADM ungefähr eine Stunde, um Berichte für die ausgewählten Aggregationsoptionen zu erstellen.

So exportieren Sie Widget-Berichte:

1. Navigieren Sie zu **Netzwerke** > **Network Reporting.**

2. Klicken Sie auf **Dashboards** anzeigen, um alle von Ihnen erstellten Dashboards anzuzeigen.
3. Klicken Sie im linken Bereich auf ein Dashboard. Klicken Sie in diesem Beispiel auch auf **Skype for Business**.
4. Wählen Sie ein Widget aus. Wählen Sie beispielsweise **Load Balancing Virtual Server Transactions**aus.
5. Klicken Sie auf die Schaltfläche Exportieren in der oberen rechten Ecke der Seite
6. Wählen Sie auf der Registerkarte **Jetzt exportieren** das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.



Verwalten von Schwellenwerten für Netzwerkberichte in NetScaler ADM

Um den Status einer NetScaler ADC-Instanz zu überwachen, können Sie Schwellenwerte für Leistungsindikatoren festlegen und Benachrichtigungen erhalten, wenn ein Schwellenwert überschritten wird. In NetScaler ADM können Sie Schwellenwerte konfigurieren und sie anzeigen, bearbeiten und löschen.

Sie können beispielsweise eine E-Mail-Benachrichtigung erhalten, wenn der Leistungsindikator Verbindungen für einen virtuellen Content Switching-Server einen angegebenen Wert erreicht. Sie können einen Schwellenwert für einen bestimmten Instanztyp definieren. Sie können auch die Berichte auswählen, die Sie für bestimmte Zählermetriken aus der gewählten Instanz generieren möchten.

Wenn der Wert eines Zählers den Schwellenwert (wie in der Regel festgelegt) überschreitet oder unterschreitet, wird ein Ereignis mit dem angegebenen Schweregrad generiert, um auf ein leistungsbezogenes Problem hinzuweisen. Wenn der Zählerwert zu einem Wert zurückkehrt, den Sie als normal betrachten, wird das Ereignis gelöscht. Diese Ereignisse können angezeigt werden, indem Sie zu **Netzwerke** > **Ereignisse** > **Berichte** navigieren. Auf der Seite Berichte können Sie auf den Donut **Ereignisse nach Schweregrad** klicken, um Ereignisse nach Schweregrad anzuzeigen.

Sie können eine Aktion auch einem Schwellenwert zuordnen, z. B. beim Versenden einer E-Mail- oder SMS-Nachricht, wenn der Schwellenwert überschritten wird.

So erstellen Sie einen Schwellenwert:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Netzwerkberichterstattung** > **Schwellenwerte**. Klicken Sie unter **Schwellenwerte**auf **Hinzufügen**.
2. Geben Sie auf der Seite **Schwellenwert erstellen** die folgenden Details an:
    - **Name**. Name des Schwellenwerts.
    - **Instanztyp**. Wählen Sie Citrix ADC oder Citrix SD-WAN WO.
    - **Name des Berichts**. Name des Leistungsberichts, der Informationen zu diesem Schwellenwert enthält.
3. Sie können auch Regeln festlegen, um festzulegen, wann ein Ereignis generiert oder gelöscht werden soll. Im Abschnitt **Regel konfigurieren** können Sie die folgenden Details angeben:
    - **metrisch**. Wählen Sie die Metrik aus, für die Sie einen Schwellenwert festlegen möchten.
    - **Komparator**. Wählen Sie einen Komparator, um zu überprüfen, ob der überwachte Wert größer oder gleich oder kleiner oder gleich dem Schwellenwert ist.
    - **Schwellenwert**. Geben Sie den Wert ein, für den die Schwere des Ereignisses berechnet wird. Beispielsweise können Sie ein Ereignis mit dem Schweregrad eines kritischen Ereignisses generieren, wenn der überwachte Wert für Aktuelle Clientverbindungen 80 Prozent erreicht. Geben Sie in diesem Fall 80 als Schwellenwert ein. Sie können

Ereignisse “kritischer Schweregrad”anzeigen, indem Sie zu “**Netzwerke** “> “**Ereignisse** “> “**Berichte**”navigieren. Auf der Seite Berichte können Sie auf den Donut **Ereignisse nach Schweregrad** klicken, um Ereignisse nach Schweregrad anzuzeigen.

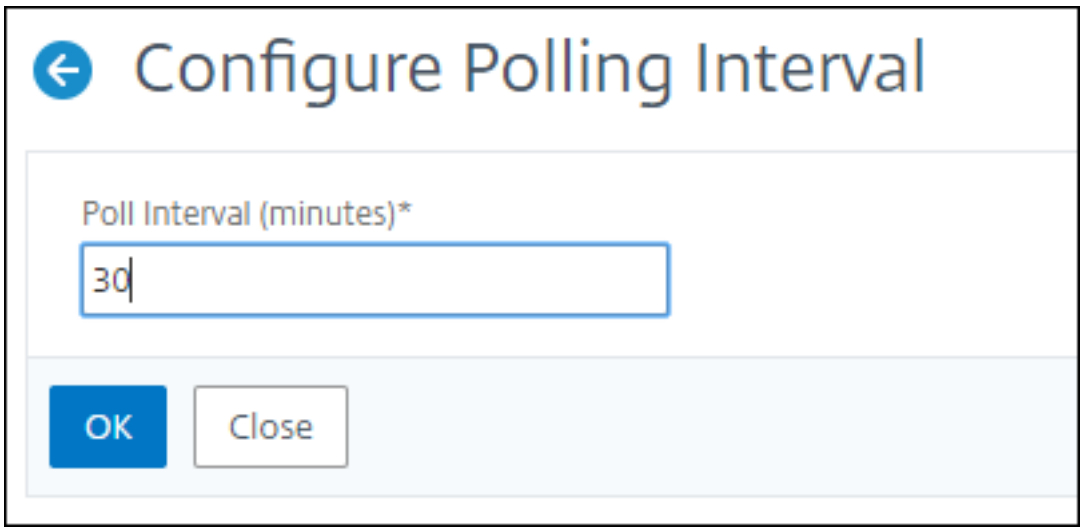
- **Wert löschen**. Geben Sie den Wert ein, der angibt, wann der Wert gelöscht werden soll. Beispielsweise können Sie den Schwellenwert Aktuelle Clientverbindungen löschen, wenn der überwachte Wert 50 Prozent erreicht. Geben Sie in diesem Fall 50 als Löschwert ein.
- **Schwere des Ereignisses**. Wählen Sie die Sicherheitsstufe aus, die Sie für den Schwellenwert festlegen möchten.

4. Wählen Sie die IP-Adresse der Instanz oder der Instanzen, für die Sie den Schwellenwert festlegen möchten.
5. Sie können auch eine **Ereignisnachricht**hinzufügen. Geben Sie eine Nachricht ein, die angezeigt werden soll, wenn der Schwellenwert erreicht ist. NetScaler ADM hängt den überwachten Wert und den Schwellenwert an diese Nachricht an.
6. Wählen Sie**Aktivieren**, um den Schwellenwert für die Generierung von Alarmen zu aktivieren.
7. Optional kannst du **Aktionen** wie E-Mail- oder Slack-Benachrichtigungen oder sowohl E-Mail- als auch Slack-Benachrichtigungen konfigurieren.
8. Klicken Sie auf **Erstellen**.

Festlegen des Intervalls für Leistungsabfragen

Standardmäßig erfassen NITRO -Aufrufe alle 5 Minuten Leistungsdaten für das Netzwerk-Reporting. ADM ruft Instanzstatistiken wie Zählerinformationen ab und aggregiert sie basierend auf pro Minute, pro Stunde, pro Tag oder pro Woche. Sie können diese aggregierten Daten in vordefinierten Berichten anzeigen.

Um das Leistungsabrufintervall festzulegen, navigieren Sie zu **Netzwerke** > **Netzwerkberichterstattung**, und klicken Sie auf**Abrufintervall konfigurieren**. Das Abrufintervall darf nicht weniger als 5 Minuten oder mehr als 60 Minuten betragen.



Konfigurieren von Netzwerkberichterstattungseinstellungen

Sie können das Löschintervall von Netzwerkberichtsdaten in NetScaler ADM konfigurieren. Diese Einstellung begrenzt die Menge der Netzwerkberichtsdaten, die in der Datenbank des NetScaler ADM-Servers gespeichert werden. Standardmäßig erfolgt die Beschneidung alle 24 Stunden (um 01.00 Uhr) für das Netzwerk, das historische Daten meldet.

> **Hinweis**
>
> Der Wert, den Sie angeben können, darf 90 Tage oder weniger als 1 Tag betragen.

Verwenden von ADM-Audit-Protokollen zur Verwaltung und Überwachung Ihrer Infrastruktur

February 5, 2024

Sie können den Citrix ADM Service verwenden, um alle Ereignisse auf ADM- und Syslog-Ereignissen zu verfolgen, die auf ADM-verwalteten ADC-Instanzen generiert wurden. Diese Meldungen können Ihnen bei der Verwaltung und Überwachung Ihrer Infrastruktur helfen. Protokollnachrichten sind jedoch nur dann eine hervorragende Informationsquelle, wenn Sie sie überprüfen, und ADM vereinfacht die Überprüfung von Protokollnachrichten.

Sie können Filter verwenden, um nach ADM-Syslog- und Audit-Logmeldungen zu suchen. Die Filter helfen dabei, Ihre Ergebnisse einzugrenzen und in Echtzeit genau das zu finden, wonach Sie suchen. Die integrierte Suchhilfe hilft Ihnen beim Filtern der Protokolle. Eine andere Möglichkeit, Protokollmeldungen anzuzeigen, besteht darin, sie in die Formate PDF, CSV, PNG und JPEG zu

exportieren. Sie können den Export dieser Berichte an bestimmte E-Mail-Adressen in verschiedenen Intervallen planen.

Sie können die folgenden Arten von Protokollmeldungen in der ADM-GUI überprüfen:

- Auditprotokolle im Zusammenhang mit ADC-Instanz
- ADM-bezogene Überwachungsprotokolle
- Audit-Protokolle für Anwendungen

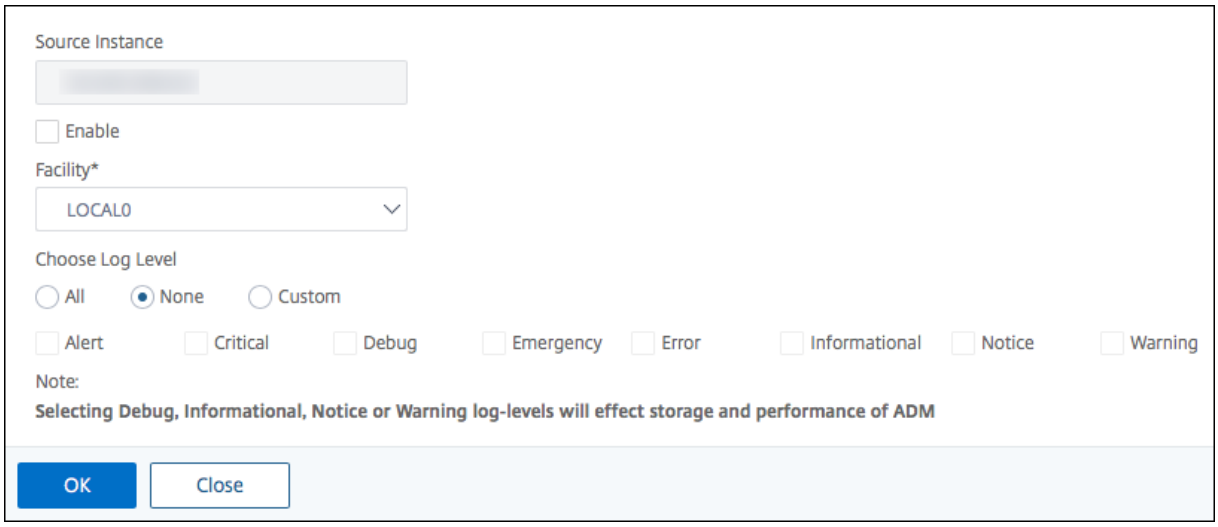
Auditprotokolle im Zusammenhang mit ADC-Instanz

Bevor Sie ADC-Instanz-bezogene Syslog-Nachrichten von ADM anzeigen können, konfigurieren Sie den NetScaler ADM Dienst als Syslog-Server für die NetScaler ADC-Instanz. Nachdem die Konfiguration abgeschlossen ist, werden alle Syslog-Meldungen von der Instanz an ADM umgeleitet.

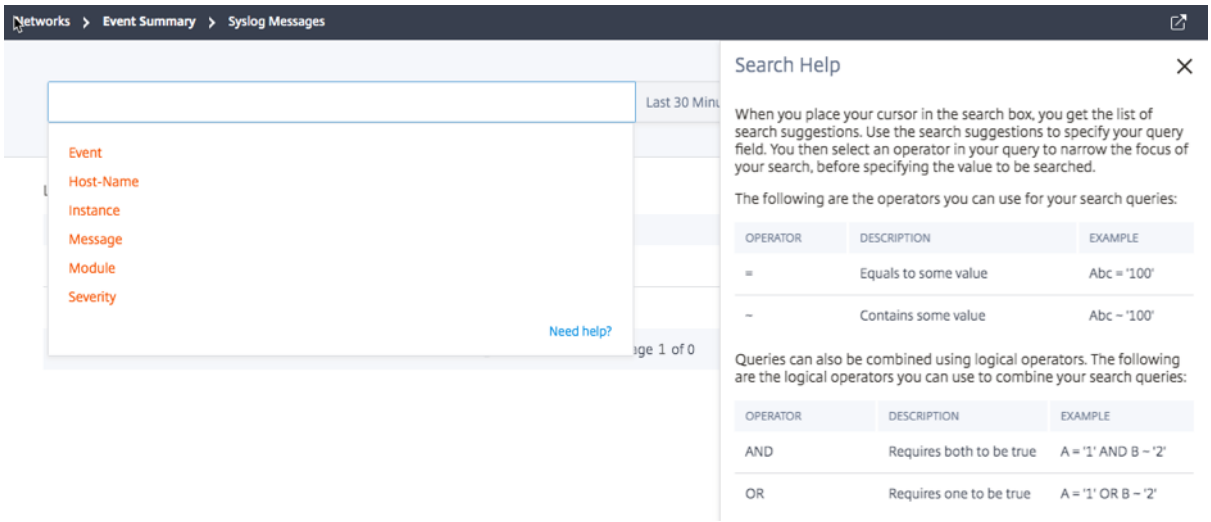
Konfigurieren von ADM Service als Syslog-Server

Gehen Sie folgendermaßen vor, um ADM als Syslog-Server zu konfigurieren:

1. Navigieren Sie in der ADM-GUI zu **Networks > Instances**.
2. Wählen Sie die NetScaler ADC-Instanz aus, aus der die Syslog-Nachrichten gesammelt und in NetScaler ADM angezeigt werden sollen.
3. Wählen Sie in der Liste **Aktion auswählen** die Option **Syslog konfigurieren** aus.
4. Klicken Sie auf **Aktivieren**.
5. Wählen Sie in der Dropdownliste **Einrichtung** eine Einrichtung auf lokaler Ebene oder auf Benutzerebene aus.
6. Wählen Sie die erforderliche Protokollebene für die Syslog-Meldungen aus.
7. Klicken Sie auf **OK**.



Mit diesen Schritten werden alle Syslog-Befehle in der NetScaler ADC-Instanz konfiguriert, und NetScaler ADM beginnt mit dem Empfang der Syslog-Nachrichten. Sie können die Nachrichten anzeigen, indem Sie zu **Netzwerke > Ereignisse > Syslog-Nachrichten** navigieren. Klicken Sie auf **Hilfe?**, um die integrierte Suchhilfe zu öffnen. Weitere Informationen finden Sie unter Anzeigen und Exportieren von Syslog-Nachrichten.

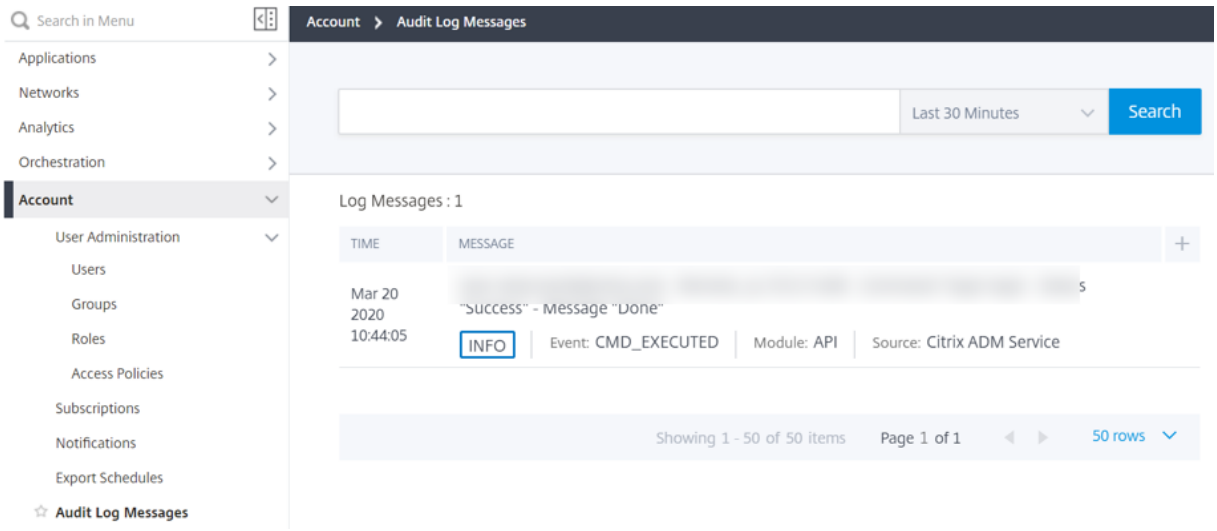


Um die Protokollmeldungen zu exportieren, klicken Sie auf das Pfeilsymbol in der oberen rechten Ecke.

Klicken Sie als Nächstes auf **Jetzt exportieren** oder **Export planen**. Weitere Informationen finden Sie unter Anzeigen und Exportieren von Syslog-Nachrichten.

ADM-bezogene Überwachungsprotokolle

Basierend auf vorkonfigurierten Regeln generiert ADM Überwachungsprotokollmeldungen für alle Ereignisse auf und hilft Ihnen dabei, den Zustand Ihrer Infrastruktur zu überwachen. Um alle im ADM vorhandenen Audit-Log-Meldungen anzuzeigen, navigieren Sie zu **System > Audit Log Messages**.



Um die Protokollmeldungen zu exportieren, klicken Sie auf das Pfeilsymbol in der oberen rechten Ecke.

Anwendungsbezogene Audit-Logs

Sie können die Überwachungsprotokollmeldungen für alle ADM-Anwendungen oder für eine bestimmte Anwendung anzeigen.

- Um alle Überwachungsprotokollmeldungen für alle im ADM vorhandenen Anwendungen anzuzeigen, navigieren Sie zu **Networks->Network Functions >Auditing**.
- Um Überwachungsprotokollmeldungen für eine bestimmte Anwendung im ADM anzuzeigen, navigieren Sie zu **Anwendung > Dashboard > doppelklicken Sie auf den virtuellen Server > Überwachungsprotokoll**.

Analytics

February 5, 2024

Die Citrix ADM Analytics-Funktion bietet eine einfache und skalierbare Möglichkeit, verschiedene Citrix ADC Erkenntnisse zu untersuchen, um die Anwendungsleistung zu analysieren und zu verbessern. Sie können eine oder mehrere Analysefunktionen gleichzeitig in NetScaler ADM verwenden.

In der folgenden Tabelle werden verschiedene Analysefunktionen beschrieben, die von Citrix ADM unterstützt werden:

Analytics-Funktion	Beschreibung
Web Insight	Web Insight ermöglicht Transparenz in Enterprise-Webanwendungen und ermöglicht Ihnen, alle Webanwendungen in Citrix ADC zu überwachen. Als Administrator können Sie sich die integrierte Überwachung von Anwendungen in Echtzeit ansehen.
HDX Insight	HDX Insight bietet End-to-End-Sichtbarkeit für ICA-Datenverkehr, der durch NetScaler ADC fließt. HDX Insight ermöglicht Ihnen die Anzeige von Client- und Netzwerklatenzmetriken in Echtzeit, historische Berichte und umfassende Leistungsdaten sowie die Behebung von Leistungsproblemen.
Gateway Insight	Gateway Insight bietet Einblick in die Fehler, die bei der Anmeldung bei Citrix Gateway auftreten, unabhängig vom Zugriffsmodus.
Security Insight	Security Insight bietet eine Lösung aus einem Bereich, mit der Sie Ihren Anwendungssicherheitsstatus beurteilen und Korrekturmaßnahmen ergreifen können, um Ihre Anwendungen zu schützen.
SSL Insight	SSL Insight bietet Einblick in sichere Webtransaktionen (HTTPS) und ermöglicht die Überwachung aller sicheren Webanwendungen in Citrix ADC. Als Administrator können Sie die integrierte Überwachung sicherer Webtransaktionen in Echtzeit und im Verlaufe verfolgen.
TCP Insight	TCP Insight bietet eine einfache und skalierbare Lösung zur Überwachung der Metriken der Optimierungstechniken und Engpasssteuerungsstrategien (oder Algorithmen), die in Citrix ADC Instanzen verwendet werden, um Netzwerküberlastung bei der Datenübertragung zu vermeiden.

Analytics-Funktion	Beschreibung
Video Insight	Die Video Insight-Funktion bietet eine einfache und skalierbare Lösung zur Überwachung der Metriken der Videooptimierungstechniken, die von Citrix ADC Appliances verwendet werden, um das Kundenerlebnis und die betriebliche Effizienz zu verbessern.
WAN Insight	WAN-Insight-Analysen ermöglichen Administratoren die einfache Überwachung des beschleunigten und nicht beschleunigten WAN-Datenverkehrs, der zwischen dem Rechenzentrum und den Zweigstellen WAN-Optimierungs-Appliances fließt. WAN Insight bietet auch Einblick in Clients, Anwendungen und Zweigstellen im Netzwerk, um Netzwerkprobleme effektiv zu beheben.

Lizenzanforderungen

February 5, 2024

In der folgenden Tabelle werden die Lizenzanforderungen für die NetScaler ADC-Instanzen beschrieben, um die verschiedenen Analyseberichte auf NetScaler ADM anzuzeigen:

Funktionen von NetScaler ADM Analytics	NetScaler ADC-Lizenzanforderung
Web Insight	Der Web Insight-Bericht über NetScaler ADM wird in allen NetScaler ADC-Lizenzeditionen (Standard/Advanced/Premium) unterstützt.
HDX Insight	Der HDX Insight-Bericht auf NetScaler ADM wird auf jeder der folgenden NetScaler ADC-Lizenzen unterstützt: Advanced Edition (für Berichte unter 1 Stunde) oder Premium Edition (für unbegrenzte Berichterstattung). **Hinweis:** Die Standard-Lizenzausgabe wird nicht unterstützt.

Funktionen von NetScaler ADM Analytics	NetScaler ADC-Lizenzanforderung
Security Insight	Der Security Insight-Bericht auf NetScaler ADM wird in der Premium Edition oder Advanced Edition mit App Firewall-Lizenz unterstützt. **Hinweis:** Die Standard-Lizenzversion und die eigenständige App Firewall-Lizenz werden nicht unterstützt.
SSL Insight	Der SSL Insight-Bericht über NetScaler ADM wird in allen NetScaler ADC-Lizenzeditionen (Standard/Advanced/Premium) unterstützt.
Gateway Insight	Der Gateway Insight-Bericht auf NetScaler ADM wird auf jeder der folgenden NetScaler ADC-Lizenzen unterstützt: Advanced Edition (für Berichte unter 1 Stunde) oder Premium Edition (für unbegrenzte Berichterstattung). **Hinweis:** Die Standard-Lizenzausgabe wird nicht unterstützt.
TCP Insight	TCP Insight-Bericht wird in allen NetScaler ADC-Lizenzeditionen (Standard/Advanced/Premium) unterstützt.
Video Insight	Der Video Insight-Bericht über NetScaler ADM wird in der NetScaler ADC Premium Edition (VPX-T 1000-Serie, VPX-T) unterstützt.
WAN-Einblick	Der WAN Insight-Bericht für Citrix ADM wird in der Citrix SD-WAN WO Edition (WAN Optimization Edition) unterstützt.

Übersicht über den Logstream

February 5, 2024

NetScaler ADC-Instanzen generieren AppFlow Datensätze und stellen einen zentralen Kontrollpunkt für den gesamten Anwendungsdatenverkehr im Rechenzentrum dar. IPFIX und Logstream sind die Protokolle, die diese AppFlow Datensätze von Citrix ADC Instanzen zu Citrix ADM transportieren. Weitere Informationen finden Sie unter AppFlow.

- IPFIX ist ein offener IETF-Standard (Internet Engineering Task Force), der in RFC 5101 definiert

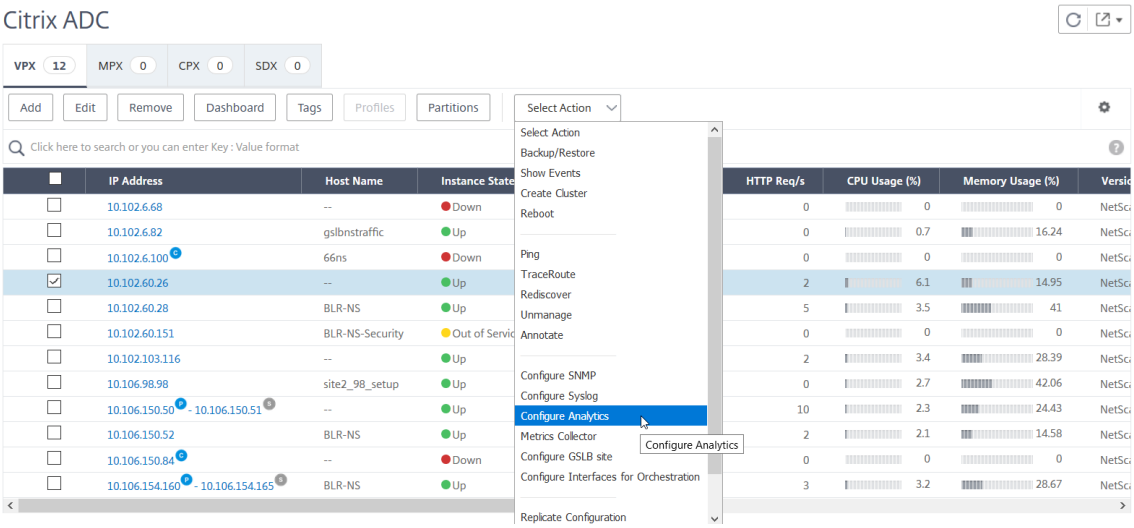
ist. IPFIX verwendet UDP-Protokoll, das ein unzuverlässiges Transportprotokoll für den Datenfluss in eine Richtung ist. Da IPFIX das UDP-Protokoll verwendet, führt die Einhaltung des IPFIX-Standards dazu, dass mehr Ressourcen in NetScaler ADM verarbeitet werden.

- Logstream ist ein Citrix-eigenes Protokoll, das als einer der Transportmodi verwendet wird, um die Analytics-Protokolldaten von Citrix ADC-Instanzen effizient an Citrix ADM zu übertragen. Logstream verwendet ein zuverlässiges TCP-Protokoll und benötigt weniger Ressourcen bei der Verarbeitung der Daten.

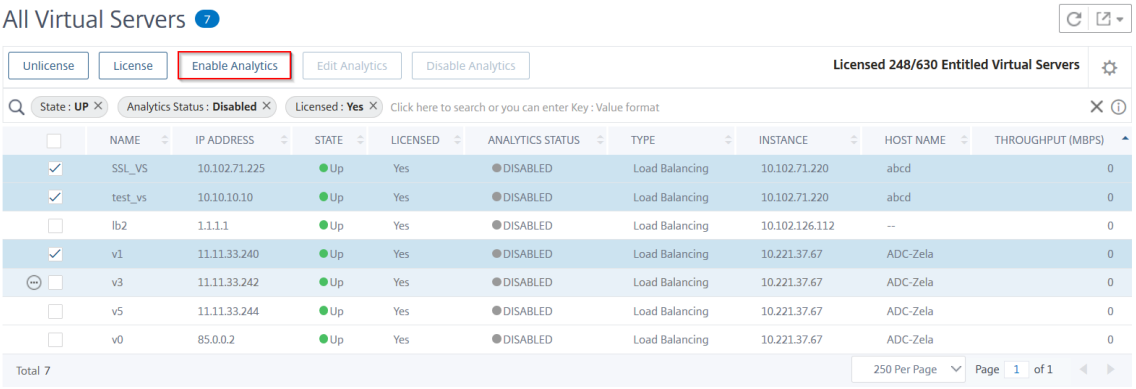
Für Citrix ADC zwischen **11.1 Build 47.14 und 11.1 Build 62.8**ist Logstream der Standardtransportmodus für die Aktivierung von Web Insight (HTTP) und IPFIX ist der einzige Transportmodus für die Aktivierung anderer Insights. Für NetScaler ADC Version ab **12.0 bis zur neuesten Version** können Sie entweder **Logstream**oder **IPFIX** als Transportmodus auswählen.

Logstream als Transportmodus aktivieren

1. Navigieren Sie zu **Netzwerke > Instanzen**und wählen Sie die ADC-Instanz aus, die Sie Analytics aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.



3. Wählen Sie die virtuellen Server aus, und klicken Sie dann auf **Analytics aktivieren**.



4. Gehen Sie im Fenster **Enable Analytics** wie folgt vor:

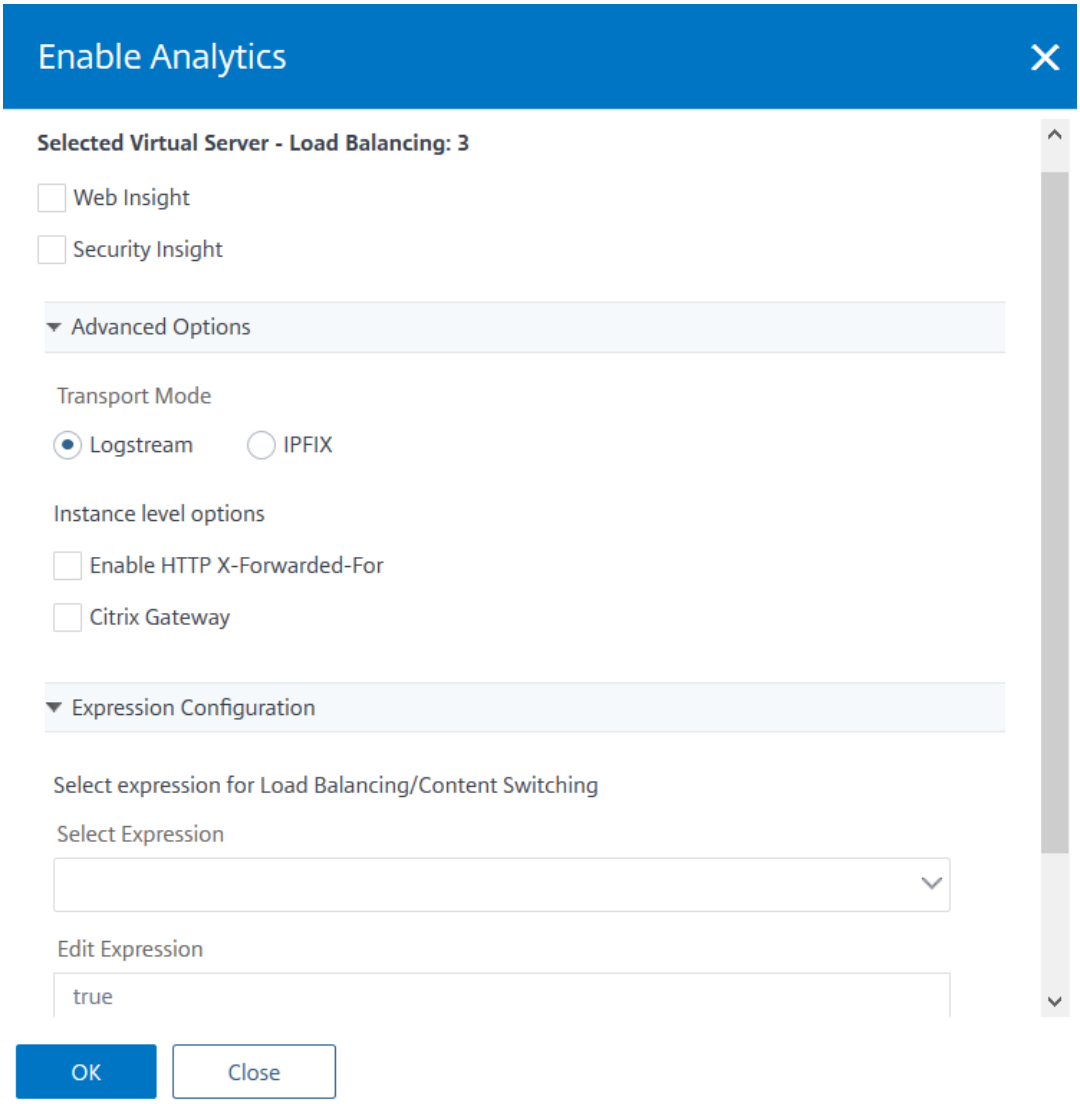
   a) Wählen Sie die Insight-Typen (Web Insight oder Security Insight)

   b) Wählen Sie **Logstream** als Transportmodus

   > **Hinweis**
   >
   > Für Citrix ADC zwischen **11.1 Build 47.14 und 11.1 Build 62.8**ist Logstream der Standardtransportmodus für die Aktivierung von Web Insight (HTTP) und IPFIX ist der einzige Transportmodus für die Aktivierung anderer Insights. Für NetScaler ADC Version ab **12.0 bis zur neuesten Version** können Sie entweder **Logstream**oder **IPFIX** als Transportmodus auswählen.

   c) Der Ausdruck ist standardmäßig wahr

   d) Klicken Sie auf **OK**.



Hinweis

- Wenn Sie virtuelle Server auswählen, die nicht lizenziert sind, lizenziert NetScaler ADM zuerst diese virtuellen Server und aktiviert dann Analysen.
- Für Admin-Partitionen wird nur **Web Insight** unterstützt
- Für virtuelle Server wie Cache-Umleitung , Authentifizierung und GSLB können Sie Analysen nicht aktivieren. Eine Fehlermeldung wird angezeigt

In der folgenden Tabelle werden die Features von Citrix ADM beschrieben, die Logstream als Transportmodus unterstützt:

Feature	IPFIX	Logstream
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Nicht unterstützt	•
CR-Einblick	•	•
IP-Reputation	•	•
AppFirewall	•	•
Kundenseitige Messung	•	•
Syslog/Auditlog	•	•

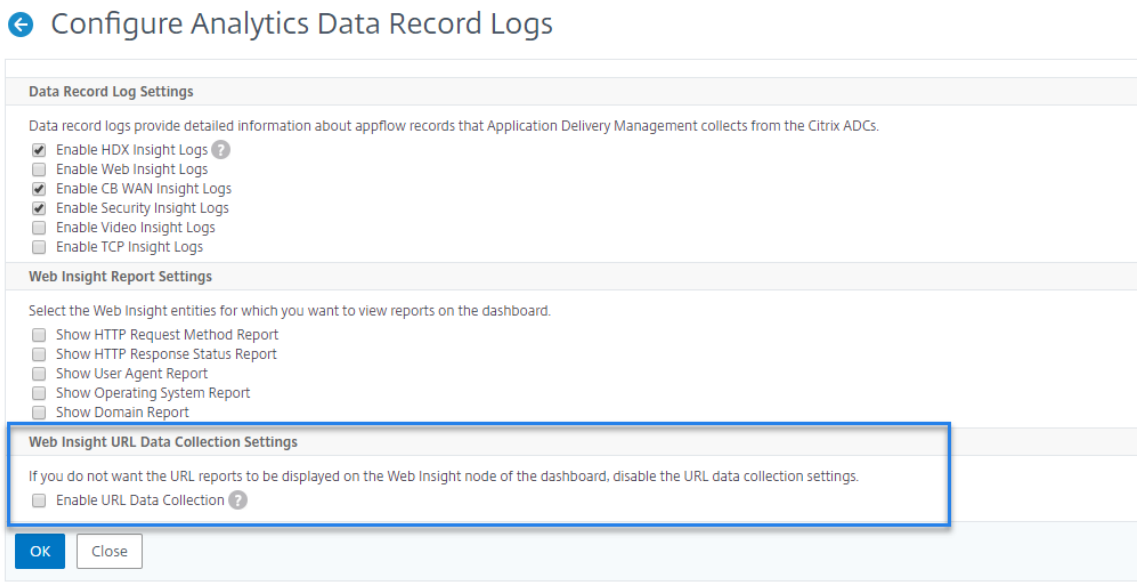
URL-Datenerfassung deaktivieren

February 5, 2024

Sie können die URL-Datenerfassung deaktivieren, wenn Sie nicht möchten, dass URL-Berichte auf dem Web Insight-Knoten des Dashboards in Citrix Application Delivery Management (ADM) angezeigt werden.

So deaktivieren Sie die URL-Datenerfassung von NetScaler ADM

1. Navigieren Sie in Citrix ADM zu **Analytics** > **Einstellungen**, und klicken Sie dann auf **Analytics-Datensatzprotokolle konfigurieren**.
2. Deaktivieren Sie im Abschnitt **Web Insight-URL-Datenerfassungseinstellungen** das Kontrollkästchen, wenn die Option **URL-Datenerfassung aktivieren** aktiviert ist.
3. Klicken Sie auf **OK**.



Erstellen von Schwellenwerten und Warnungen

February 5, 2024

Sie können Schwellenwerte und Warnungen festlegen, um den Status einer Citrix ADC Instanz zu überwachen. Sie können Schwellenwerte für Leistungsindikatoren festlegen und Instanzen und Entitäten auf verwalteten Instanzen überwachen.

Wenn der Wert eines Leistungsindikators den Schwellenwert überschreitet, generiert Citrix Application Delivery Management (ADM) ein Ereignis, das ein leistungsbezogenes Problem darstellt. Wenn der Zählerwert mit dem im Schwellenwert angegebenen Klarwert übereinstimmt, wird das Ereignis gelöscht, was bedeutet, dass der bestimmte Schwellenwert in seinen normalen Zustand zurückkehrt.

Sie können dem Schwellenwert auch eine Aktion zuordnen. Zu den Aktionen gehört das Senden einer Warnung, E-Mail oder SMS-Benachrichtigung. Wenn der Schwellenwert überschritten wird, führt NetScaler ADM automatisch die von Ihnen definierte Aktion aus, z. B. das Aktivieren einer Warnung und das Senden einer E-Mail- oder SMS-Benachrichtigung.

So erstellen Sie einen Schwellenwert und eine Warnung mit NetScaler ADM:

1. Navigieren Sie in NetScaler ADM zu **Analytics** > **Einstellungen** > **Schwellenwerte**. Klicken Sie unter **Schwellenwerte**auf **Hinzufügen**.
2. Geben Sie auf der Seite **Schwellenwerte erstellen** die folgenden Details an:

- **Name** —Name für die Konfiguration des Schwellenwerts.
- **Verkehrstyp** —Art des Datenverkehrs, für den Sie den Schwellenwert konfigurieren möchten.
- **Entität** —Kategorie oder Ressourcentyp, für die Sie den Schwellenwert konfigurieren möchten.
- **Referenzschlüssel** —Automatisch generierter Wert basierend auf dem ausgewählten Traffic-Typ und der ausgewählten Entität.
- **Dauer** —Intervall, für das Sie den Schwellenwert konfigurieren möchten.
- **Regel konfigurieren** —Regel für die Metrik, für die Sie den Schwellenwert konfigurieren möchten.
- **Benachrichtigungseinstellungen** - Aktivieren Sie den Schwellenwert und erhalten Sie Benachrichtigungen über verschiedene Kanäle wie E-Mail, Slack oder SMS, wenn der Schwellenwert höher ist.

3. Klicken Sie auf **Erstellen**.

Für HDX-Einblicke können Sie auch mehrere Schwellenwerte festlegen, für die eine Warnung nur dann generiert wird, wenn alle Entitäten im konfigurierten Schwellenwert überschritten werden.

Konfigurieren adaptiver Schwellenwerte

February 5, 2024

Die adaptive Schwellenwertfunktion legt den Schwellenwert für die maximale Anzahl von Treffern auf jeder URL fest. Wenn die maximale Anzahl von Treffern auf einer URL den für die URL festgelegten Schwellenwert überschreitet, wird eine Syslog-Meldung an einen externen Syslog-Server gesendet. Das Schwellenwertintervall kann entweder in Tagen oder Wochen liegen.

Der Schwellenwert wird wie folgt berechnet:

Schwellenwert = **Max. Treffer * Schwellenwertmultiplikator**

Ort:

- Max. Treffer ist die maximale Anzahl von Treffern auf einer URL.
- Der Schwellenwert-Multiplikator ist ein ganzzahliger Wert, den Sie definieren (Standard: 2).

So erstellen Sie einen adaptiven Schwellenwert mit NetScaler ADM

1. Navigieren Sie in Citrix ADM zu **Analytics** > **Einstellungen** > **Adaptive Schwellenwerte**, und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie auf der Seite **Adaptive Schwellenwerte** die folgenden Parameter an:
    - **Name** - Name des Schwellenwerts
    - **Entität** —URL
    - **Dauer** —Dauer des Schwellenwerts (Tag oder Woche)
    - **Schwellenwert-Multiplikator** - Eine benutzerdefinierte Ganzzahl, die mit der maximalen Trefferanzahl der angegebenen URL multipliziert wird, um den adaptiven Schwellenwert für die URL zu erhalten.

Datenbankpersistenz konfigurieren

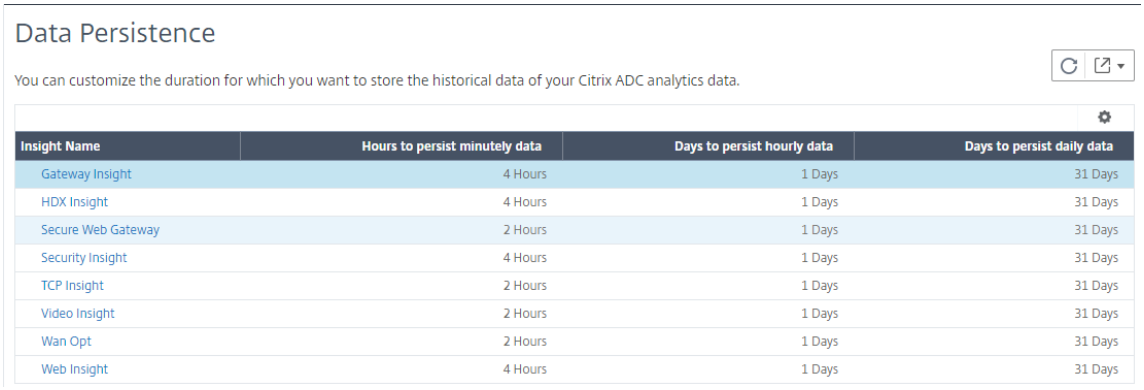
February 5, 2024

Wenn Sie Datenbankpersistenz in Citrix Application Delivery Management (ADM) konfigurieren, können Sie die Dauer anpassen, in der Sie die historischen Daten der Citrix ADC Analysedaten speichern möchten. Sie können die folgenden Datenbankpersistenztypen für die historischen Daten Ihrer Analysen wählen:

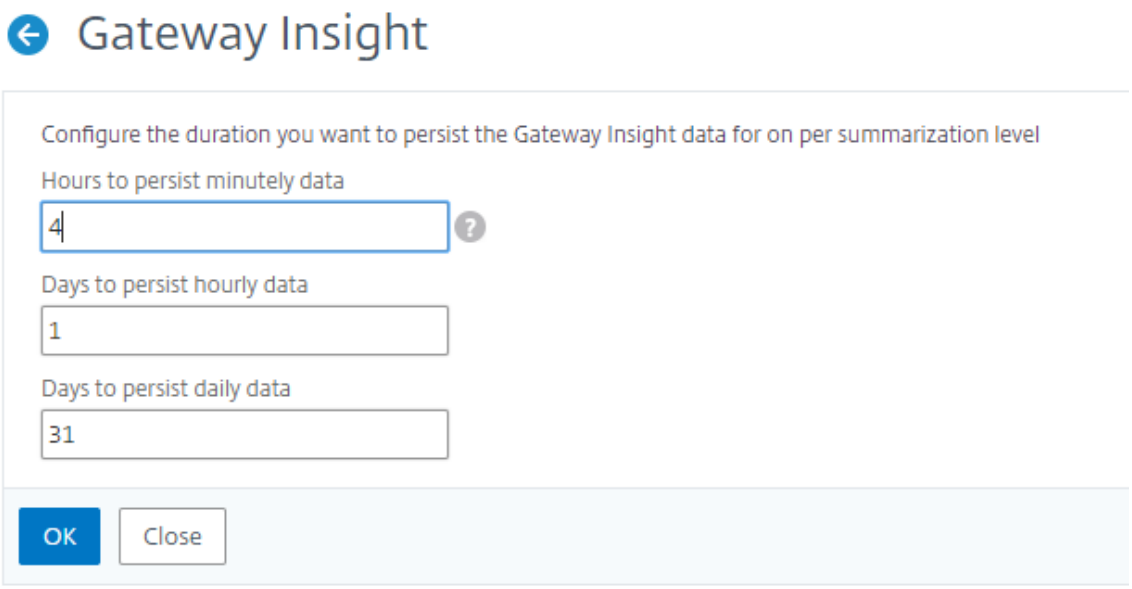
- Stunden, um kleinste Daten zu speichern
- Tage, um die Stundendaten beizubehalten
- Tage, die täglich erfasste Daten erhalten bleiben

So konfigurieren Sie Datenbankpersistenz

1. Navigieren Sie zu > **Analytics** > **Einstellungen** > **Datenbankpersistenz**.
2. Klicken Sie auf den Einsichtstyp, den Sie die Datenbankpersistenz konfigurieren möchten.



3. Geben Sie die Dauer an, für die Sie Insight-Daten in NetScaler ADM beibehalten möchten. Beispielsweise können Sie bei Gateway Insight die verfallenen Daten Ihrer Analysen für 2 Stunden oder stündliche Daten für 1 Tag speichern.



Self-Service-Diagnose für Analytics

February 5, 2024

Citrix Application Delivery Management (ADM) führt eine Self-Service-Diagnose durch, um die Lizenz- und Konfigurationsprobleme auf den verwalteten Instanzen für die folgenden Analysefeatures zu identifizieren:

- Web Insight

- HDX Insight
- Gateway Insight
- Security Insight
- SSL-Forward-Proxyanalyse

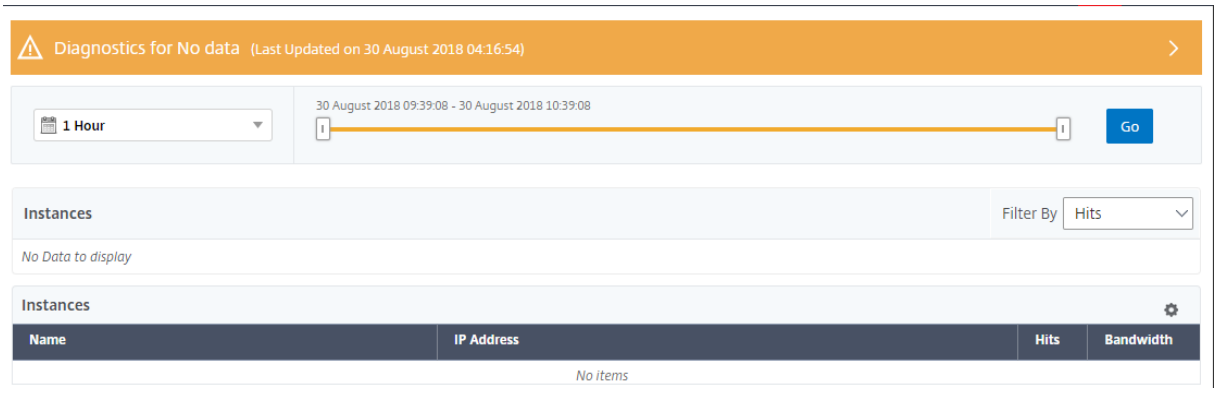
Die Self-Service-Diagnose wird alle 12 Stunden ausgeführt und generiert einen Diagnosebericht, wenn Probleme für jedes der angegebenen Analysefunktionen gefunden werden. Der Diagnosebericht enthält die Ursachen der Probleme, die Art der Probleme und die Korrekturmaßnahmen zur Behebung der Probleme. Die Self-Service-Diagnose hilft Ihnen, die Probleme schneller zu erkennen und zu beheben.

Wenn beispielsweise die AppFlow-Richtlinie nicht an einen virtuellen Server gebunden ist oder ein virtueller Server nicht lizenziert ist, erhält NetScaler ADM nicht die gewünschten Daten für die Web Insight-Überwachung. Die Self-Service-Diagnose identifiziert die Probleme und generiert einen Diagnosebericht. Sie können den Diagnosebericht anzeigen, um die Probleme zu überprüfen und Korrekturmaßnahmen durchzuführen.

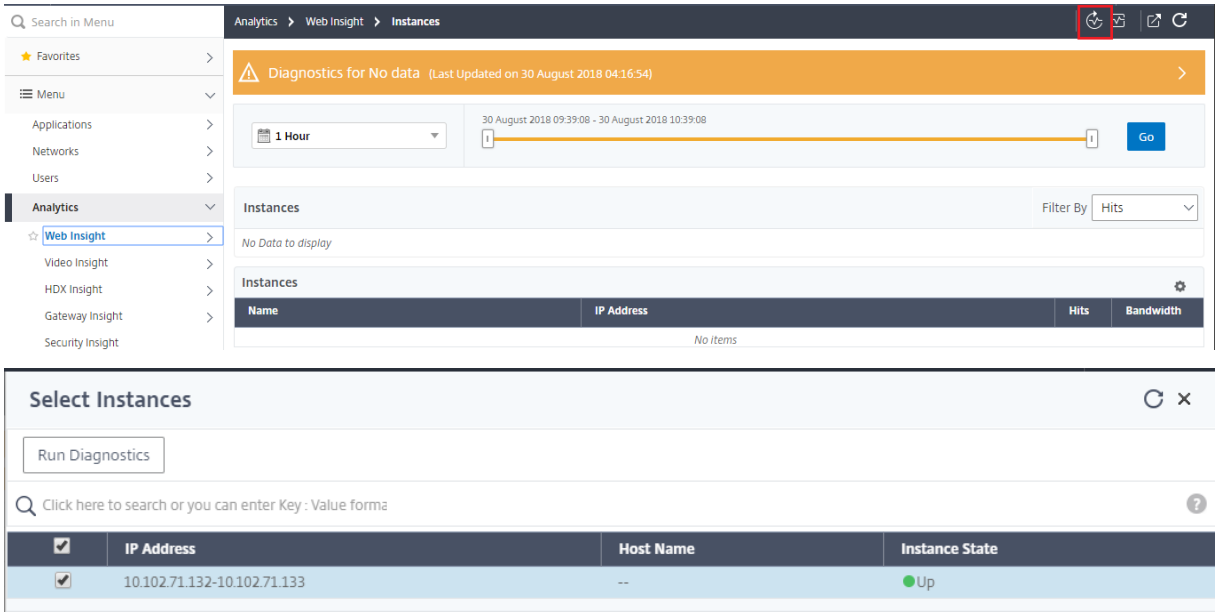
Diagnosebericht anzeigen

Um die Diagnoseberichte für die angegebenen Analytics-Features anzuzeigen, müssen Sie im Dashboard von NetScaler ADM zum entsprechenden Analytics-Knoten wechseln.

Um beispielsweise den Diagnosebericht für Web Insight anzuzeigen, navigieren Sie zu **Analytics > Web Insight**. Wählen Sie auf der Seite Web Insight das Symbol **Diagnose anzeigen** aus.



Sie können auch eine Sofortdiagnose durchführen, wenn Sie nach Problemen suchen möchten. Klicken Sie auf **Diagnose ausführen**. Wählen Sie die Instanzen aus und wählen Sie **Diagnose ausführen**.



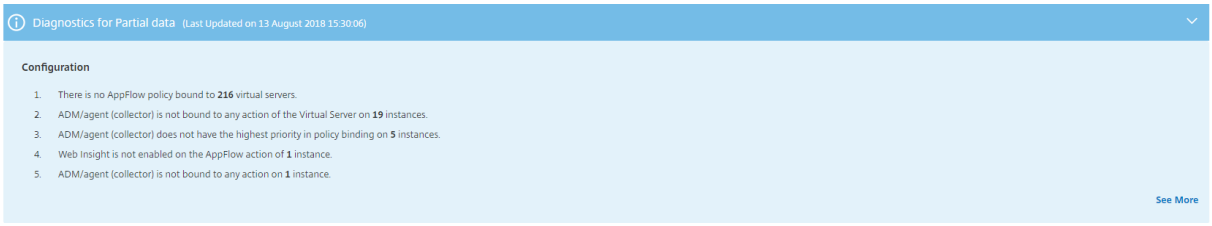
Analyse des Diagnoseberichts

Die Self-Service-Diagnose zeigt den Diagnosebericht je nach Kritikalität der Probleme entweder in orangefarbenem oder blauem Hintergrund an.

Diagnosebericht auf orangefarbenem Hintergrund bedeutet eine höhere Kritikalität als der blaue Hintergrund.

Beispielsweise sind auf der NetScaler ADC-Instanz fünf virtuelle Server konfiguriert. Wenn Sie die AppFlow-Parameter auf keinen virtuellen Servern aktiviert haben, empfängt NetScaler ADM den Web Insight- und Security Insight-Datenverkehr nicht zur Analyse. Die Self-Service-Diagnose identifiziert die Konfigurationsprobleme als kritisch. Sie sehen die Diagnoseberichte in orangefarbenem Hintergrund in Web Insight und Security Insight Funktion.

Wenn Sie AppFlow auf einem der virtuellen Server aktiviert haben, empfängt NetScaler ADM Daten für Analysen. Der Diagnosebericht wird in blauem Hintergrund angezeigt, da mindestens ein virtueller Server Datenverkehr zur Analyse sendet.

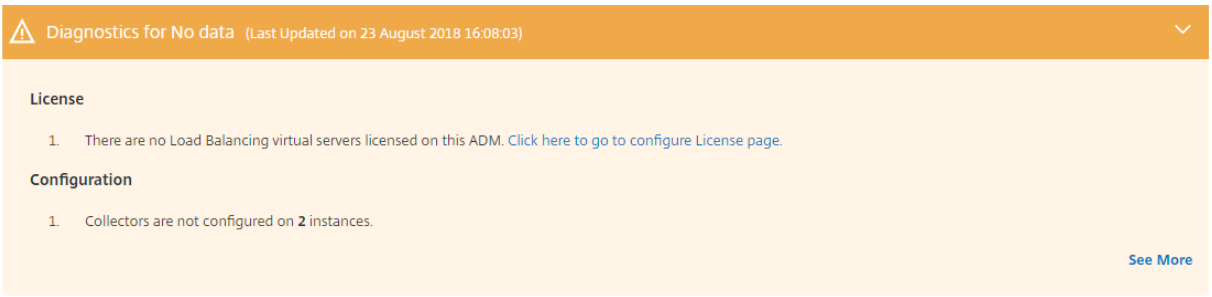


> **WICHTIG**: Die Self-Service-Diagnose überprüft nicht den Verkehrsfluss. Es prüft nur auf Lizenz- oder Konfigurationsprobleme, die mit den angegebenen Analysefunktionen auf den verwalteten Instanzen verbunden sind. Manchmal werden keine Analysedaten angezeigt, da kein aktiver Datenverkehr durch virtuelle Server fließt.

Der Diagnosebericht hat eine Übersichtsseite und eine detaillierte Informationsseite.

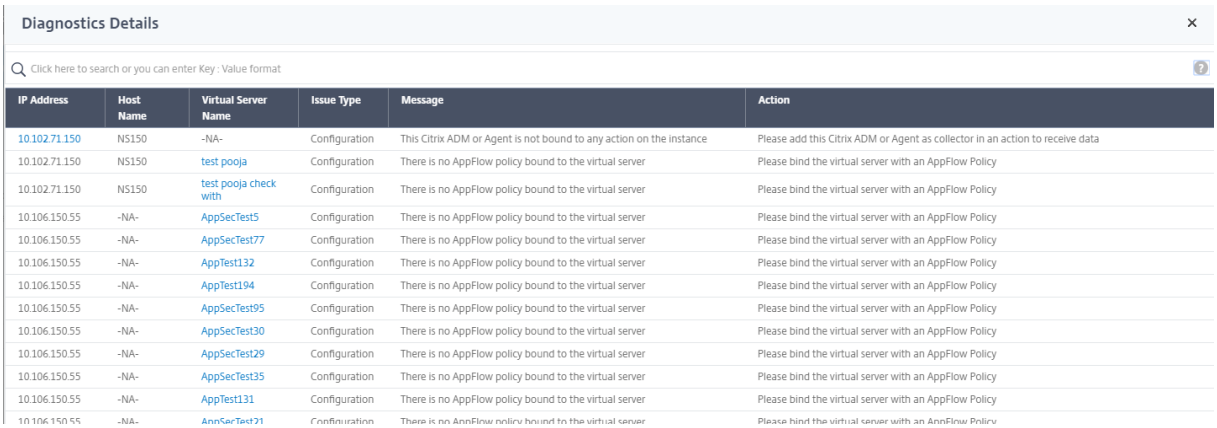
Die Übersichtsseite bietet einen Überblick über die Arten von Problemen —Lizenz oder Konfiguration. Die Seite kann Hyperlinks enthalten, die Sie zu den entsprechenden Konfigurationsseiten führen.

Wenn beispielsweise keine virtuellen Lastenausgleichsserver auf Ihrem NetScaler ADM lizenziert sind, enthält die Übersichtsseite einen Hyperlink, der Sie zur Seite "**Systemlizenzen** "weiterleitet.

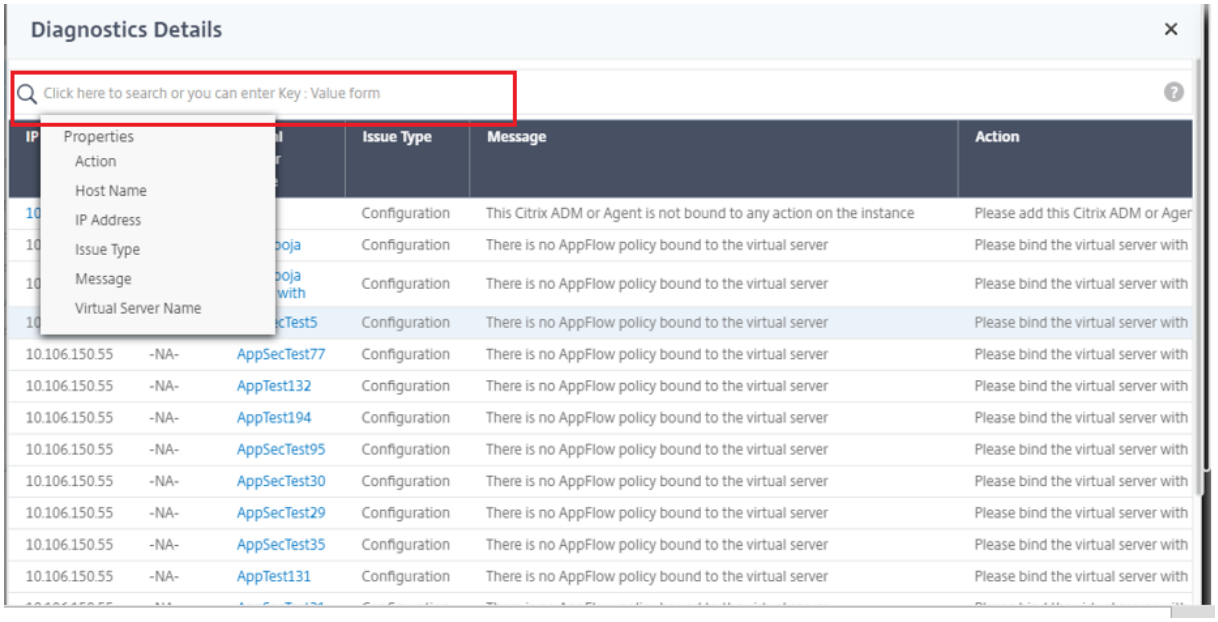


Um detaillierte Informationen zu den Problemen anzuzeigen, klicken Sie auf der Übersichtsseite auf **Mehr** anzeigen.

Die detaillierte Informationsseite enthält vollständige Informationen zu den Problemen und empfiehlt Maßnahmen, die Sie durchführen müssen. Sie können auf den Hyperlink für jedes Problem klicken, um die verwaltete Instanz oder den virtuellen Server zu konfigurieren.



Sie können die Probleme auch basierend auf der Aktion, dem Hostnamen, der IP-Adresse und dem Problemtyp usw. durchsuchen.



Nachdem Sie die Probleme behoben haben, müssen Sie eine sofortige Diagnose ausführen, um den neuesten Diagnosebericht zu generieren.

Web Insight

February 5, 2024

Mit Web Insight können Administratoren alle Webanwendungen überwachen, die von NetScaler ADC-Instanzen bedient werden. Als Administrator erhalten Sie eine integrierte Echtzeitüberwachung der Anwendungen von NetScaler ADC-Instanzen. Web Insight stellt wichtige Informationen wie Client-netzwerklatenz und Server-Reaktionszeit bereit, um die Anwendungsleistung zu überwachen und zu verbessern. Die für die Analyse verwendeten Daten werden aus jeder HTTP-, HTTPS-Transaktion erfasst, die von der NetScaler ADC-Instanz verarbeitet werden. Mit den Analysedaten können Sie die Leistung von NetScaler ADC-Instanzen, Anwendungen, URL, Client und Server in Ihrer Umgebung analysieren.

Im Folgenden finden Sie einige der Anwendungsfälle, die Sie mit Web Insight anzeigen können:

- Die Liste der Clients mit hoher Latenz beim Zugriff auf eine Anwendung wie SharePoint
- Die Top-Anwendung, die die meisten Treffer innerhalb einer Stunde hatte
- Die Liste der Anwendungen und URLs, auf die von Clients zugegriffen wird

- Betriebssystem und Browser, die von einem bestimmten Client verwendet werden
- Die Anwendungen oder Server, die die meisten fehlerbezogenen Antworten senden
- Barrierefreiheitsprobleme mit einem bestimmten Client
- Probleme mit der Barrierefreiheit über wenige oder alle Anwendungen eines bestimmten Clients hinweg
- Einige Seiten einer Anwendung sind von einem bestimmten Client und vom Back-End-Server langsam
- Die Anwendung ist langsam, wenn Sie von einem bestimmten Client und von einem Back-End-Server aus aufgerufen werden

Sie können Web Insight für einen bestimmten virtuellen Server auf einer ausgewählten Instanz aktivieren, um den Datenverkehr in Ihrer Webanwendung zu überwachen. Das Web Insight-Feature stellt dann Statistiken für den virtuellen Server in NetScaler ADM bereit.

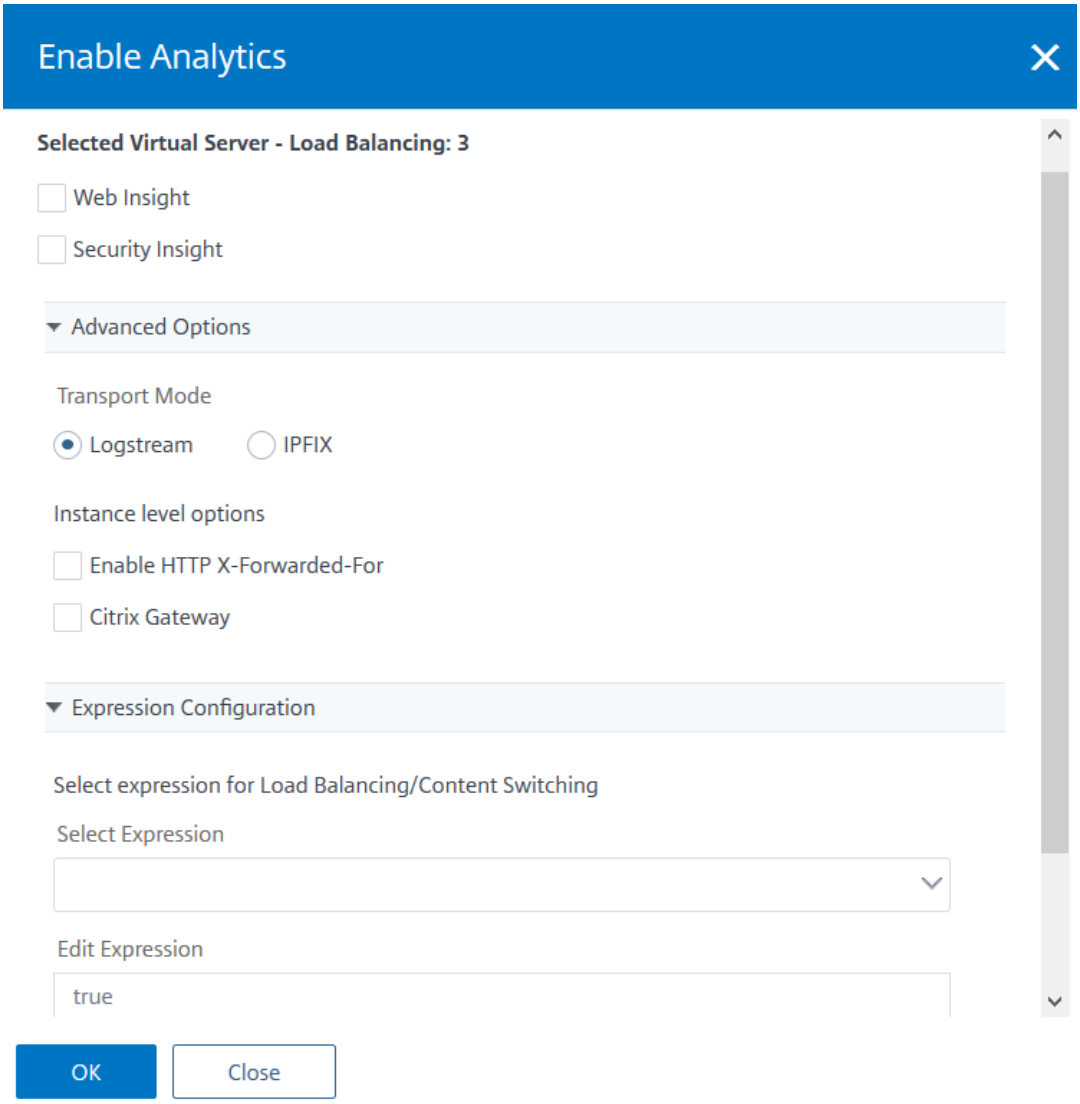
So aktivieren Sie Web Insight:

Wenn Ihr NetScaler ADM **13.0 Build 41.x oder höher**ist:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC**, und wählen Sie den Instanztyp aus. Zum Beispiel VPX.
2. Wählen Sie die Instanz aus, und klicken Sie in der Liste **Aktion auswählen** auf **Analytics konfigurieren**.
3. Wählen Sie auf der Seite **Configure Analytics on Virtual Server** den virtuellen Server aus und klicken Sie auf **Analytics aktivieren**.
4. Gehen Sie im Fenster **Enable Analytics** wie folgt vor:
   a) Wählen Sie **Web Insight**
   b) Wählen Sie **Logstream** als Transportmodus

      > **Hinweis**
      >
      > Für NetScaler ADC 12.0 oder früher ist **IPFIX** die Standardoption für den Transportmodus. Für NetScaler ADC 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.
      >
      > Weitere Informationen zu IPFIX und Logstream finden Sie unter Logstream-Übersicht .

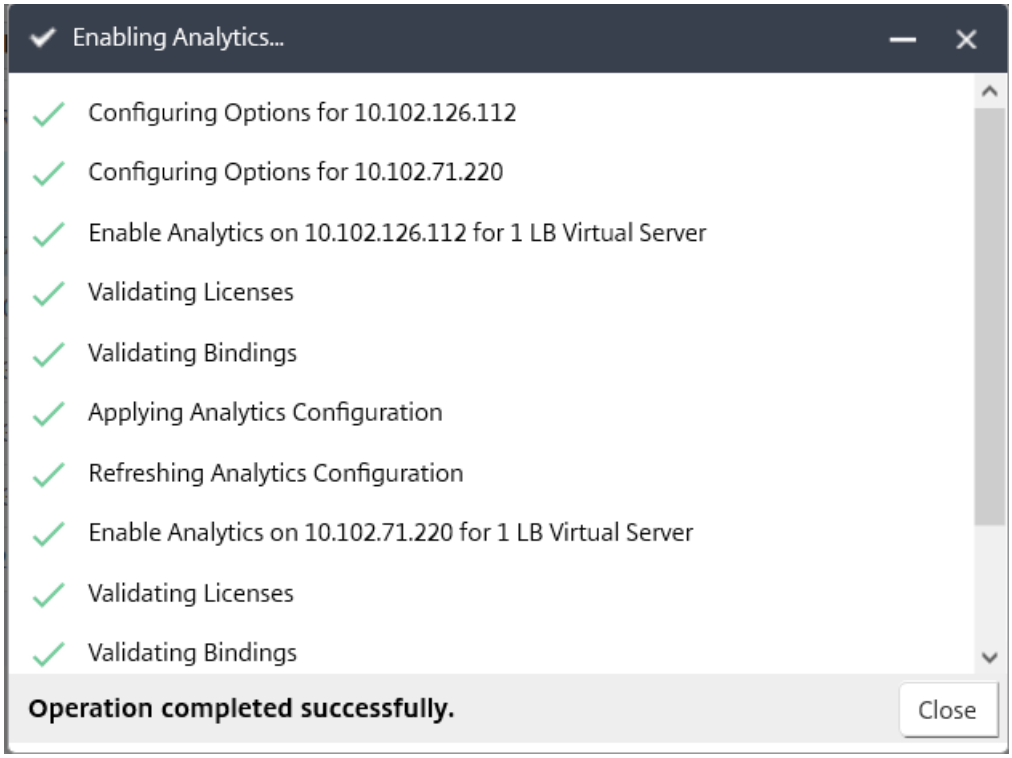
   c) Der Ausdruck ist standardmäßig wahr
   d) Klicken Sie auf **OK**.



Hinweis

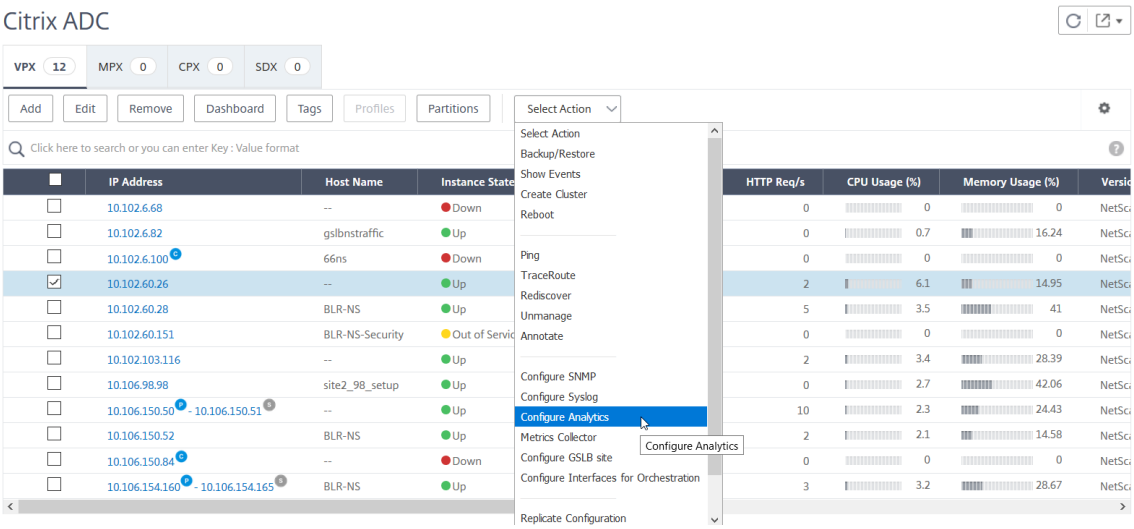
- Wenn Sie virtuelle Server auswählen, die nicht lizenziert sind, lizenziert NetScaler ADM zuerst diese virtuellen Server und aktiviert dann Analysen.
- Für Admin-Partitionen wird nur **Web Insight** unterstützt
- Für virtuelle Server wie Cache-Umleitung , Authentifizierung und GSLB können Sie Analysen nicht aktivieren. Eine Fehlermeldung wird angezeigt.

Nachdem Sie auf **OK** geklickt haben, verarbeitet NetScaler ADM Analysen auf den ausgewählten virtuellen Servern zu aktivieren.



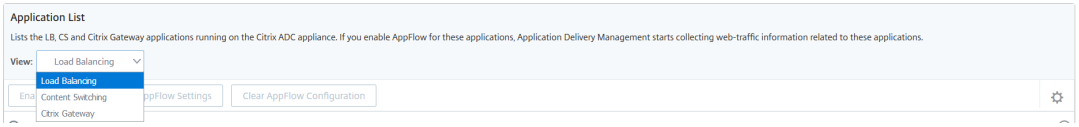
Wenn Ihr NetScaler ADM **13.0 ist Build 36.27 oder früher**:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC**, und wählen Sie die NetScaler ADC-Instanz aus, für die Sie die Analyse aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.

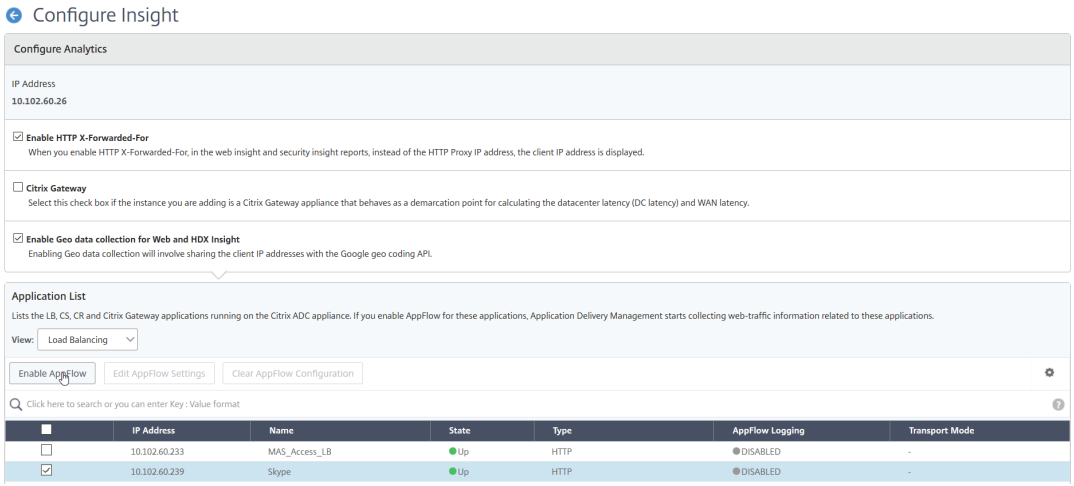


3. Gehen Sie auf der Seite **"Insight konfigurieren** "wie folgt vor:

   a) Wählen Sie die **Anwendungsliste** für Load Balancing oder Content Switching aus.



b) Wählen Sie den virtuellen Server aus, und klicken Sie auf **AppFlow aktivieren**.

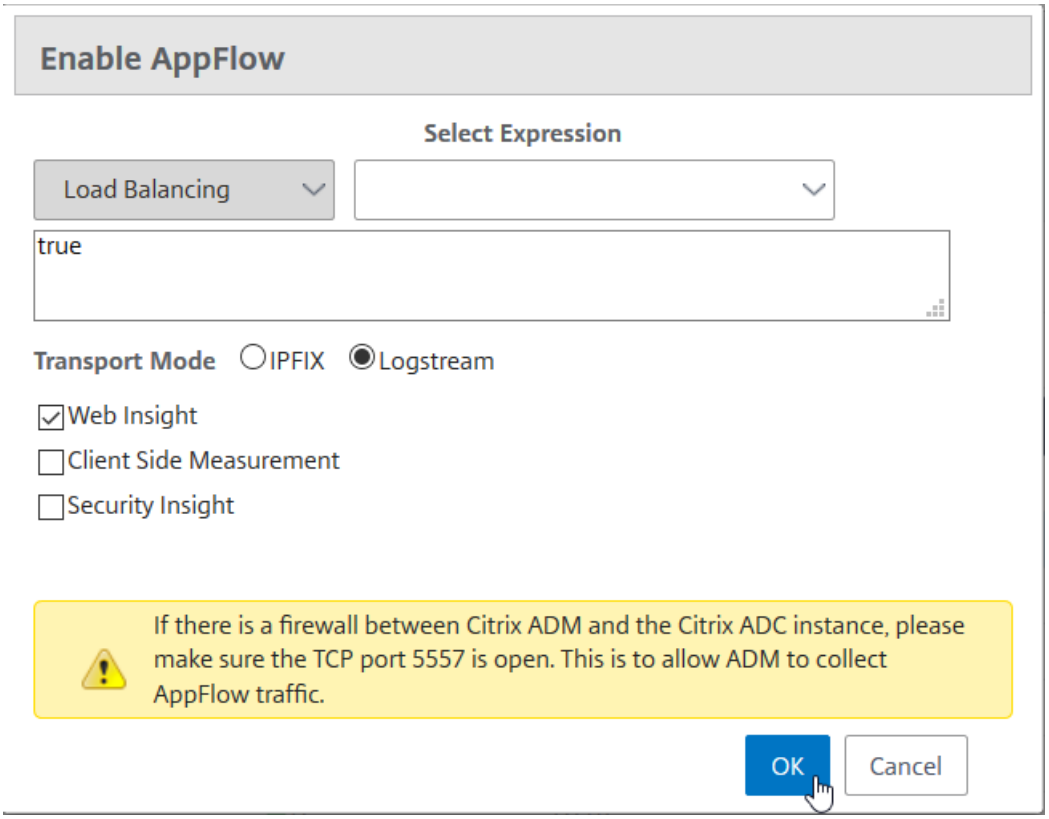


4. Gehen Sie im Dialogfeld “AppFlow aktivieren”wie folgt vor:

   - Geben Sie **true** in das Textfeld ein
   - Wählen Sie **Logstream** als Transportmodus

     > Hinweis: Citrix empfiehlt Ihnen, Logstream als Transportmodus auszuwählen.

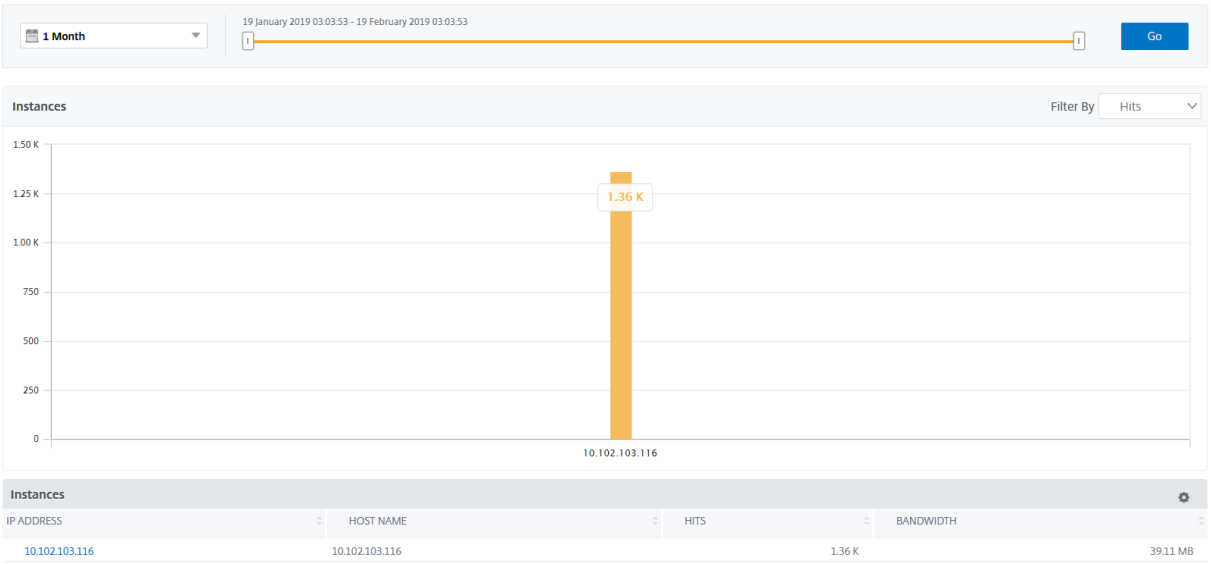
   - Wählen Sie **Web Insight** aus, und klicken Sie auf **OK**.



Analysieren von Problemen mit Webanwendungen

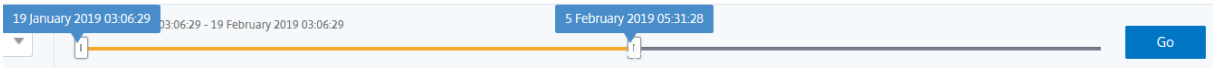
Eines der häufigsten Probleme, die ein Administrator identifizieren muss, sind die Latenzprobleme. Als Administrator müssen Sie herausfinden, ob das Latenzproblem vom Servernetzwerk, dem Clientnetzwerk oder dem Server-Antwortzeit stammt. Mithilfe von Citrix ADM können Sie diese Informationen identifizieren, indem Sie zu **Analytics** > **Web Insight** navigieren.

Wenn Sie zu **Analytics** > **Web Insight** navigieren, werden die NetScaler ADC-Instanzen angezeigt, die mit Web Insight aktiviert sind. Sie können die detaillierten Informationen für die Instanzen wie IP-Adresse, Hostname, Gesamtzahl der Treffer und Bandbreite anzeigen.



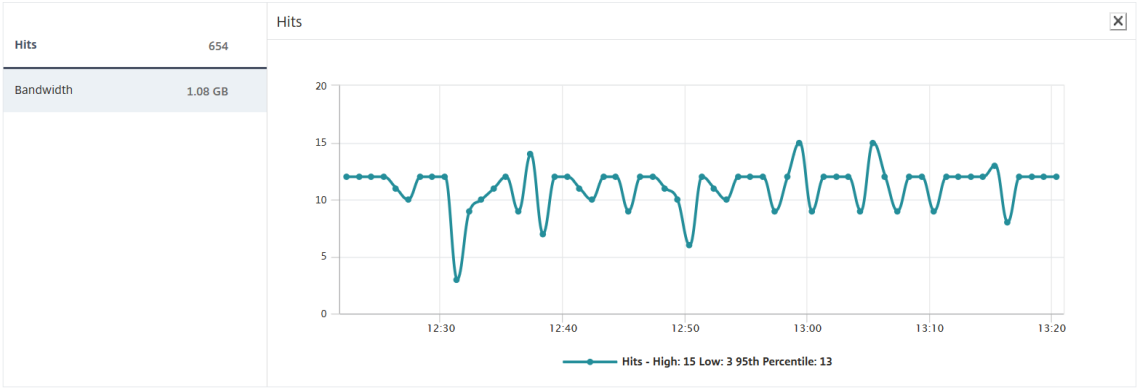
In der Liste können Sie die Zeitdauer auswählen, um die Einblicke für die Instanzen anzuzeigen.

Sie können den Schieberegler auch verwenden, um die Zeitdauer anzupassen, und klicken Sie auf **Los**, um die Ergebnisse anzuzeigen.

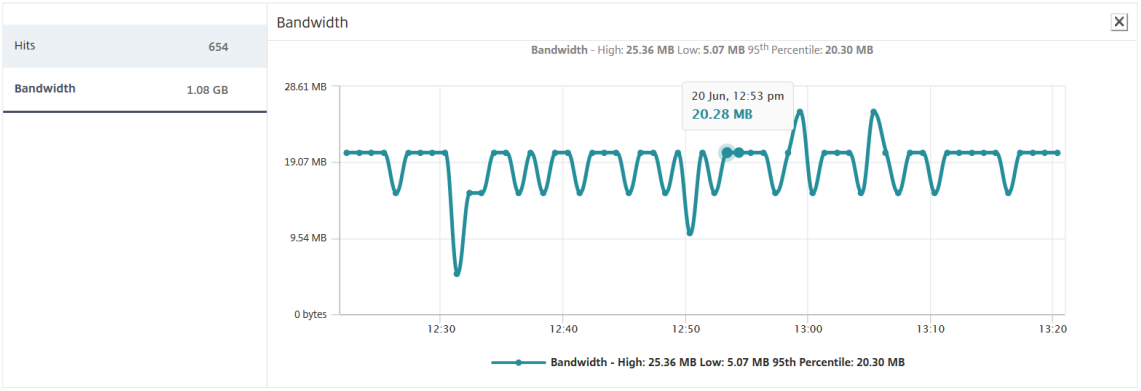


Wenn Sie auf das Diagramm oder die IP-Adresse der Instanz klicken, werden die detaillierten Informationen über die Instanz angezeigt. Sie können Einblicke für Folgendes anzeigen:

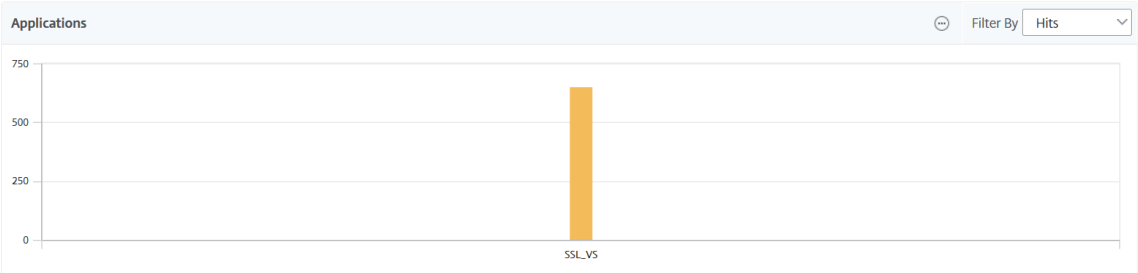
- **Gesamtzahl der Treffer**



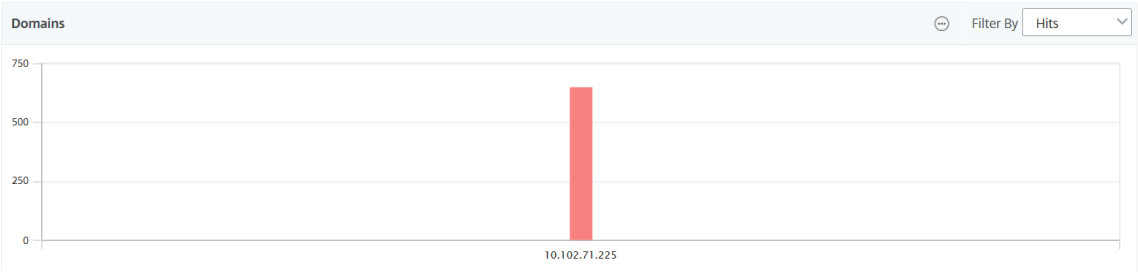
- **Bandbreite**



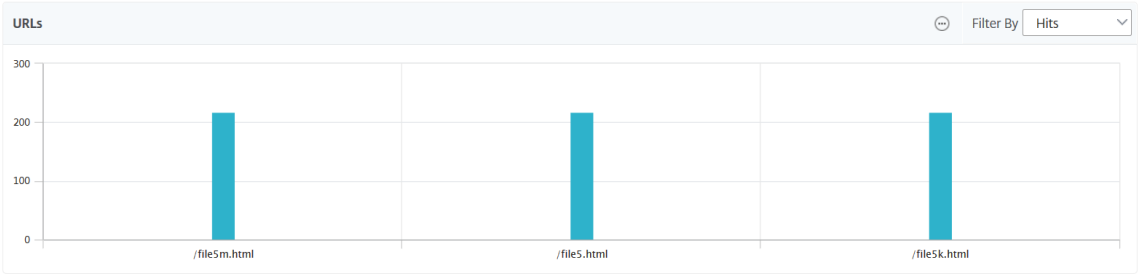
- **Anwendungen**



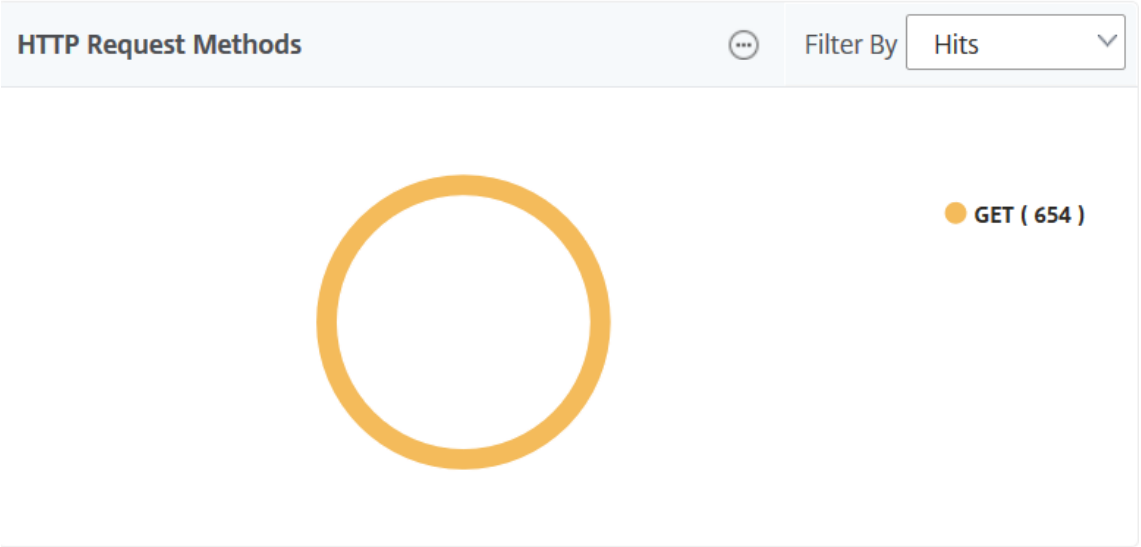
- **Domänen**



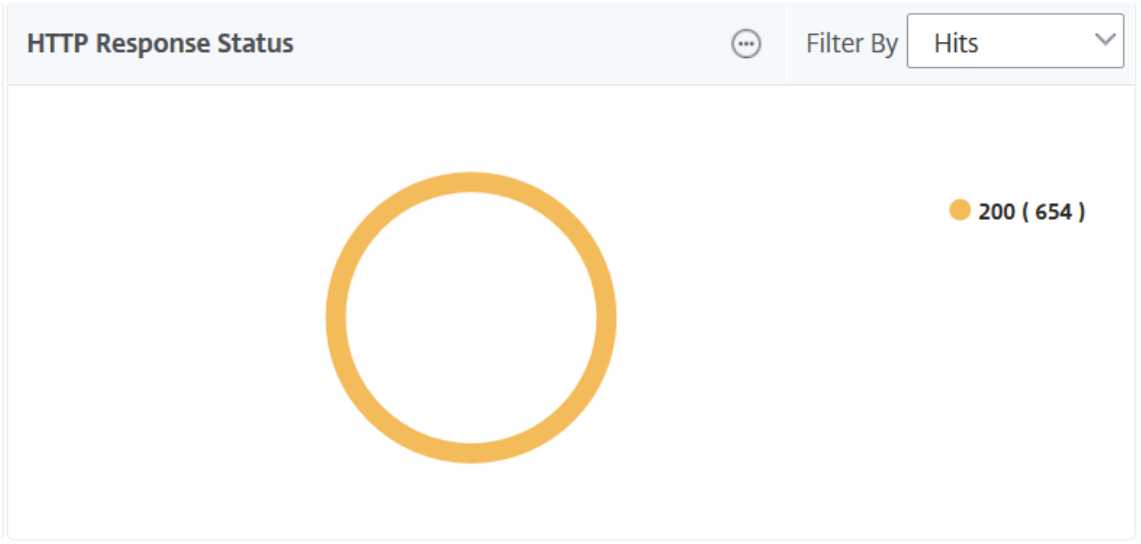
- **URLs**



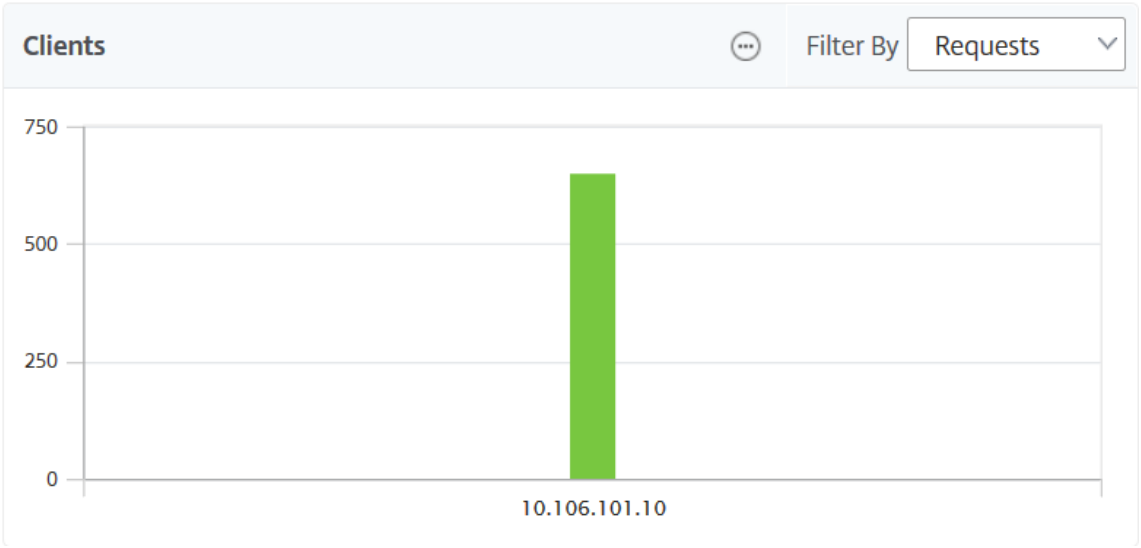
- **HTTP-Anforderungsmethoden**



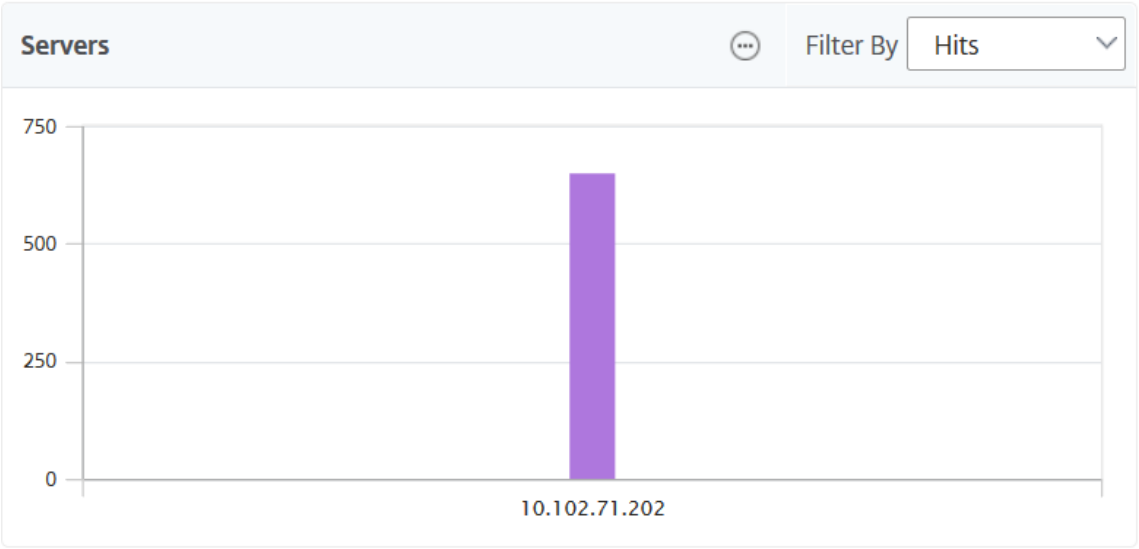
- **HTTP-Antwortstatus**



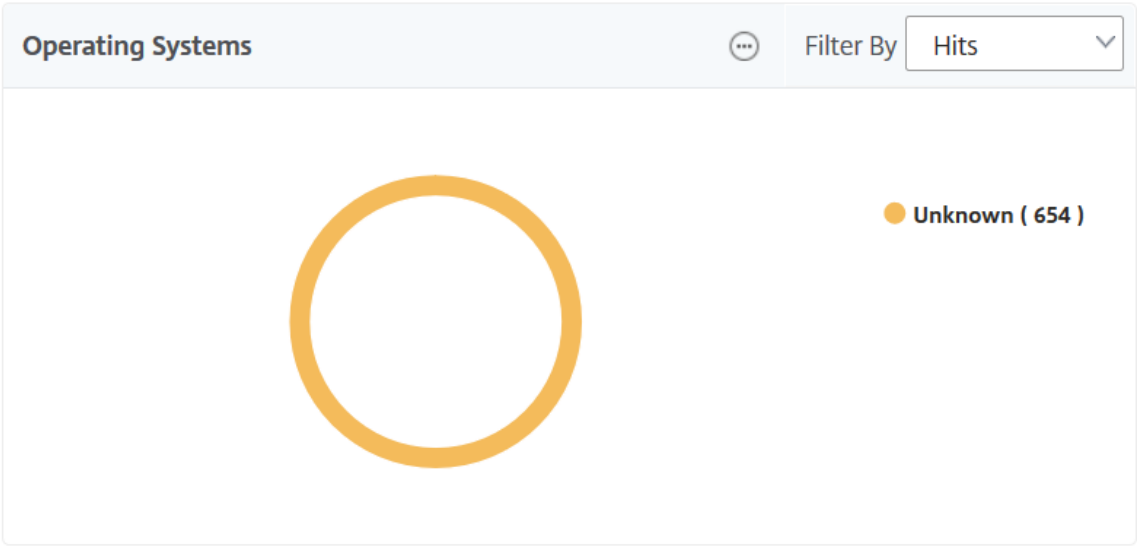
- **Clients**



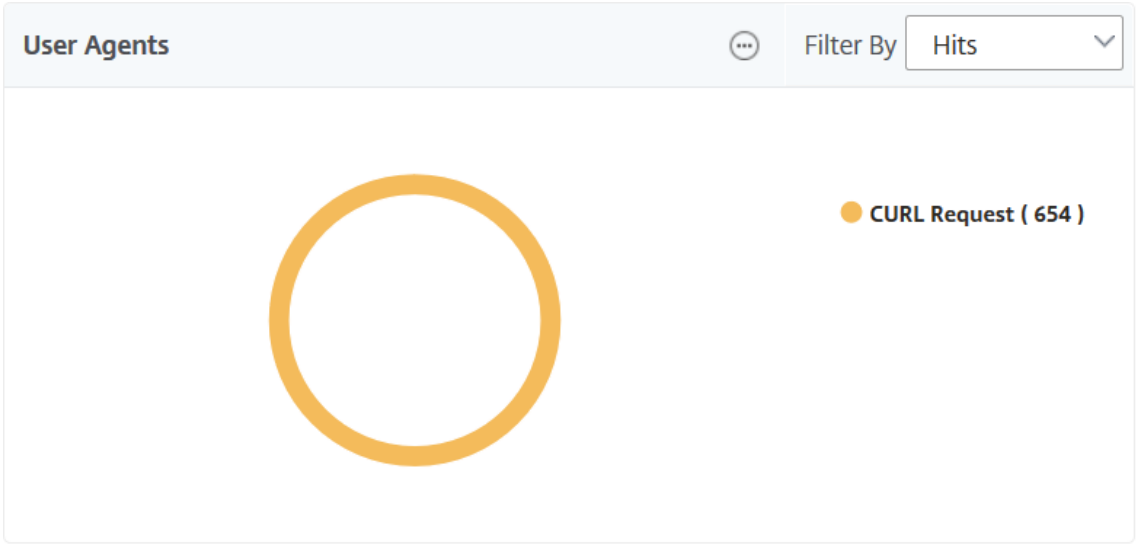
- **Server**



- **Betriebssysteme**

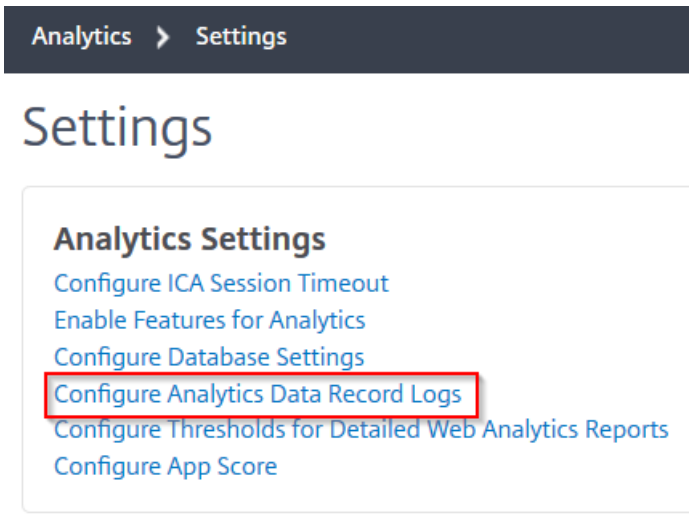


- **Benutzeragents**

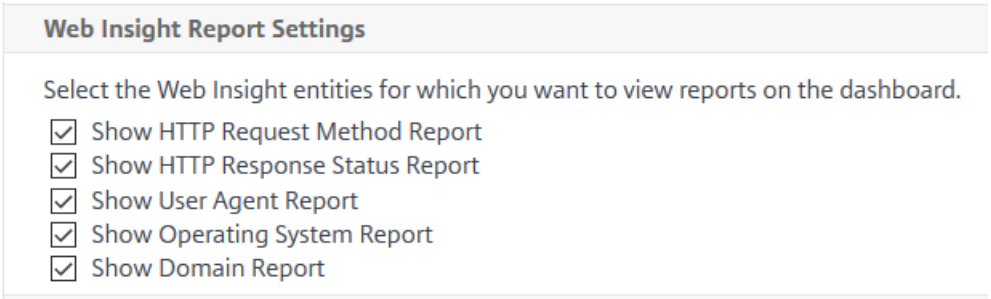


Sie können auch **Web Insight-Entitäten** auswählen, für die Sie Berichte auf der GUI anzeigen möchten.

1. Navigieren Sie zu **Analytics** > **Web Insight** > **Einstellungen**.
2. Klicken Sie auf **Analytics-Datensatzprotokolle konfigurieren**.



3. Wählen Sie unter **Web Insight-Berichtseinstellungen**die Entitäten aus, die Sie Berichte auf der GUI anzeigen möchten.



4. Klicken Sie auf **OK**.

Um eine Aufgliederung für weitere Analysen durchzuführen, können Sie auf jede Insight-Kategorie unter Web Insight in der GUI klicken. Wenn Sie beispielsweise Probleme für die konfigurierten Server überprüfen möchten:

1. Navigieren Sie zu **Analytics** > **Web Insight** > **Server**.
2. Die Seite Server wird mit allen konfigurierten Servern angezeigt.
3. Klicken Sie im Diagramm auf die IP-Adresse. Sie können auch in der Tabelle auf die IP-Adresse klicken.

Die Detailansicht für den ausgewählten Server wird angezeigt. In dieser Ansicht können Sie nach mehreren Erkenntnissen suchen, z. B.:

- Gesamtzahl der vom Server empfangenen Treffer
- Bandbreite
- Verarbeitungszeit des Servers
- Servernetzwerklatenz
- Virtuelle Server, die für den Server konfiguriert sind
- Gesamtzahl der Clients, die auf den Server zugreifen
- Gesamtzahl der vom Server bereitgestellten Antwortcodes

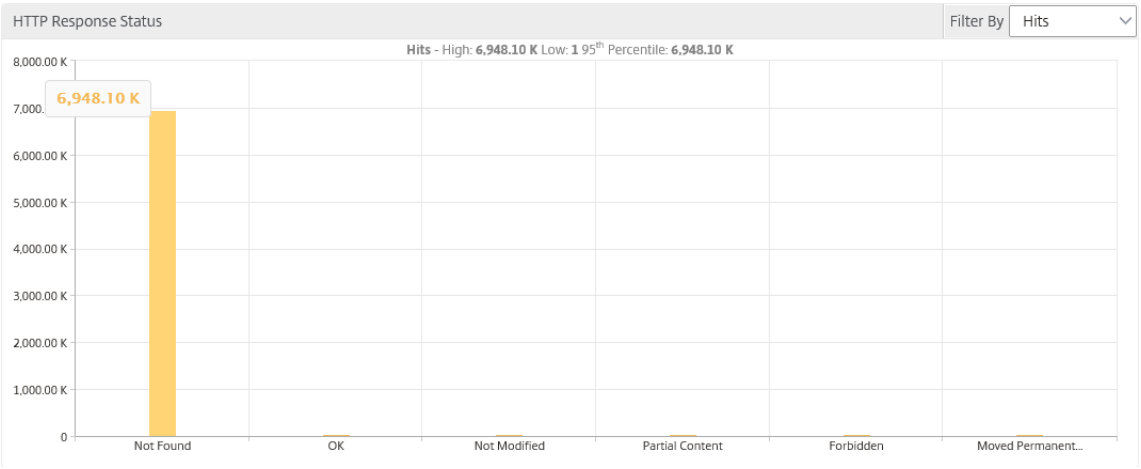
Anwendungsfall 1 - Interner Serverfehler

Betrachten Sie ein Szenario, dass Ihre Benutzer Unzugänglichkeit Fehler 500 für Ihre Webanwendung haben. Der Fehler 500 (Not Found) ist HTTP-Antwortstatusfehler, der auf ein Problem auf dem Webserver hinweist, aber der Server gibt das Problem nicht explizit an. Um das eigentliche Problem zu identifizieren und einen Drilldown durchzuführen:

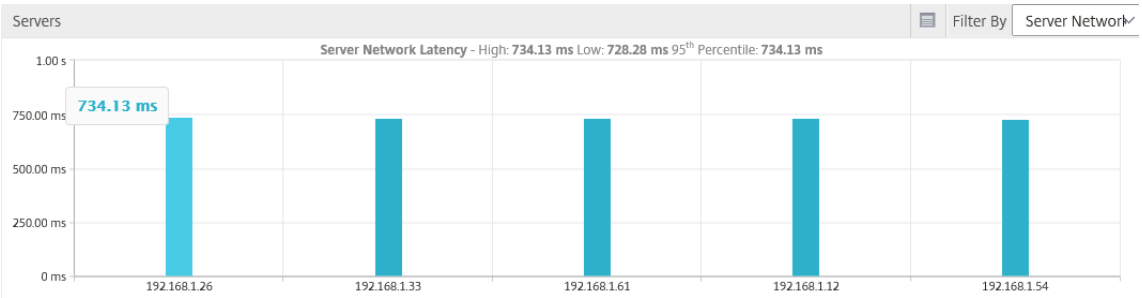
1. Navigieren Sie zu **Analytics** > **Web Insight** > **Antwortstatus**.

   Die Dashboard-Seite wird angezeigt. Das Dashboard stellt Ihnen die Metriken zur Verfügung, mit denen Sie den Erfolg und Fehler der verarbeiteten HTTP-Transaktionen analysieren können.

2. Klicken Sie im Diagramm auf **Nicht gefunden**.



3. Führen Sie einen Bildlauf nach unten aus, um das **Serverdiagramm**anzuzeigen, und wählen Sie in der Liste **Filtern nach**die Option **Servernetzwerklatenz**aus.



Das Diagramm zeigt an, dass jeder Anwendungsserver ein Problem beim Abrufen der Webanwendung hatte und daher die Antwortzeit für Webserver erhöht wird. Das Problem kann auftreten, dass der Webserver nicht auf Anfragen von einem Server reagiert.

Anwendungsfall 2 - Benutzer mit langsamem Zugriff auf die Webanwendung

Betrachten Sie ein Szenario, dass Ihre Webanwendung über 10 verschiedene Webserver gehostet wird. Wenn mehrere Benutzer gleichzeitig auf die Anwendung zugreifen, kann es bei einem oder mehreren Benutzern zu einer langsamen Anwendung kommen. Als Administrator müssen Sie die folgenden Szenarien analysieren, um die Ursache des Problems zu verstehen:

Szenario 1 - Serververarbeitungszeit:

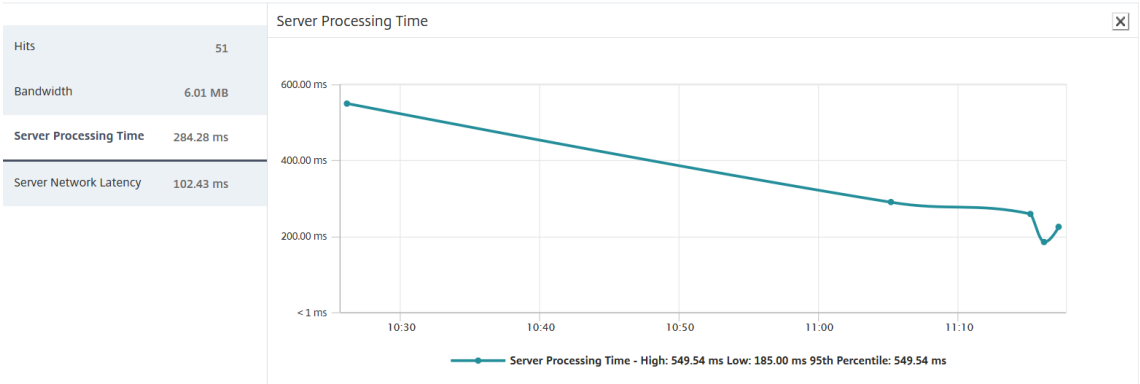
Wenn mehrere Anforderungen gleichzeitig die 10 Webserver treffen, unterscheidet sich die Zeit, die zum Laden der Anforderung erforderlich ist:

- Anzahl der Anforderungen in der Warteschlange.
- Die Bandbreite, die von jeder Anforderung zur Verarbeitung der HTTP-Transaktion belegt wird.

  Das Serverdiagramm kann Ihnen helfen, die Verarbeitungszeit jedes Servers für die von den

Servern verarbeitete Anforderung zu verstehen. Ebenso zeigt das Anwendungsdiagramm die Treffer, die Antwortzeit und die Bandbreite an, die von jeder HTTP-Transaktion belegt wird.

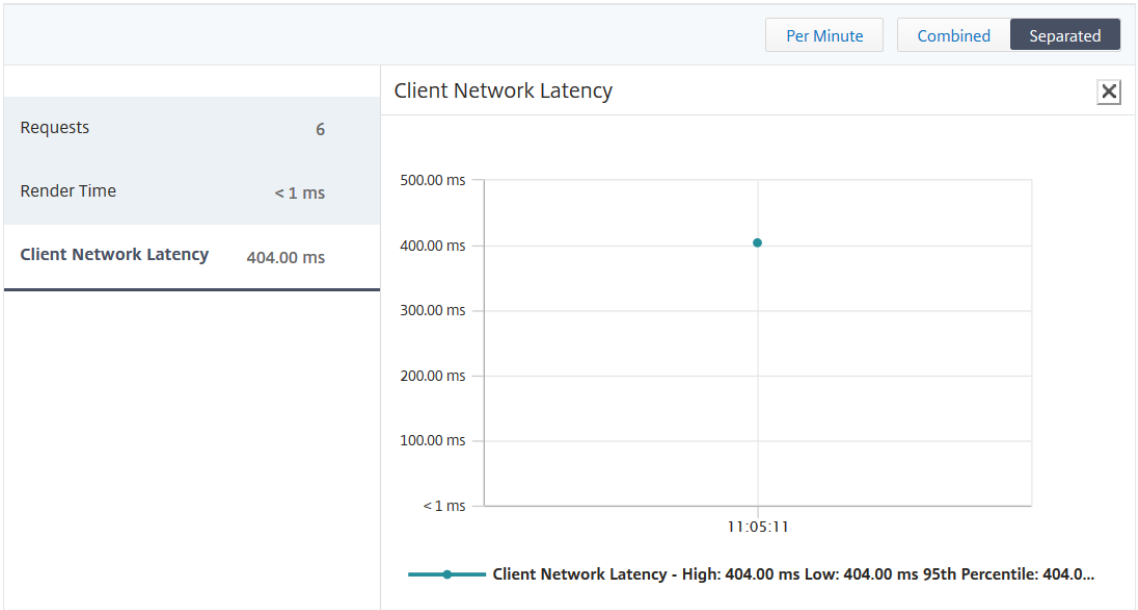
1. Navigieren Sie zu **Analytics** > **Web Insight** > **Server**.
2. Wählen Sie den Server aus dem Diagramm aus.
3. Klicken Sie auf **Serververarbeitungszeit**, um die Verarbeitungszeit des Servers zu analysieren.



Szenario 2 - Client-Latenz:

Die Antwortzeit und die Gesamtzahl der Treffer für die Anwendung können der Grund für die Langsamkeit des Anwendungszugriffs sein. Sie können die Latenz des Client-Netzwerks überprüfen und die Metriken für die Latenz des Client-Netzwerks analysieren. So analysieren Sie die Ursache:

1. Navigieren Sie zu **Analytics** > **Web Insight** > **Clients**.
2. Wählen Sie den Client aus dem Diagramm aus.
3. Klicken Sie auf **Clientnetzwerklatenz**, um die hohe Latenz zu analysieren.



In diesem Beispiel können Sie als Administrator sehen, dass die Ursache des Problems aus dem Clientnetzwerk stammt, da die Clientnetzwerklatenz eine hohe Latenz anzeigt.

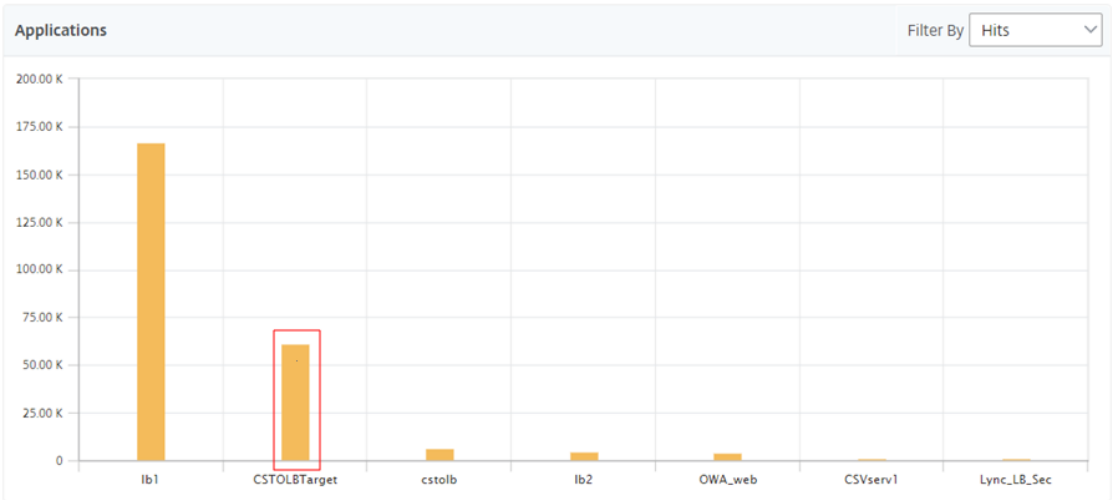
Anwendungsfall 3 - Langsamkeit beim Zugriff auf die Webanwendung

Betrachten Sie ein Szenario, dass Sie Webserver für Windows-Benutzer und Webserver für Mac-Benutzer haben, und Ihre Benutzer melden Langsamkeit beim Zugriff auf die Webanwendung. Als Administrator wissen Sie, dass Sie Folgendes haben:

- Konfiguriert einen virtuellen Content Switching-Server für Windows-Benutzer.
- Konfiguriert einen virtuellen Content Switching-Server für Mac-Benutzer.
- Konfigurierte zugeordnete Dienste, die an die virtuellen Server gebunden sind, um Anforderungen basierend auf Windows- und Mac-Benutzern umzuleiten.

So analysieren Sie die Ursache des Problems mit der Langsamkeit der Webanwendung:

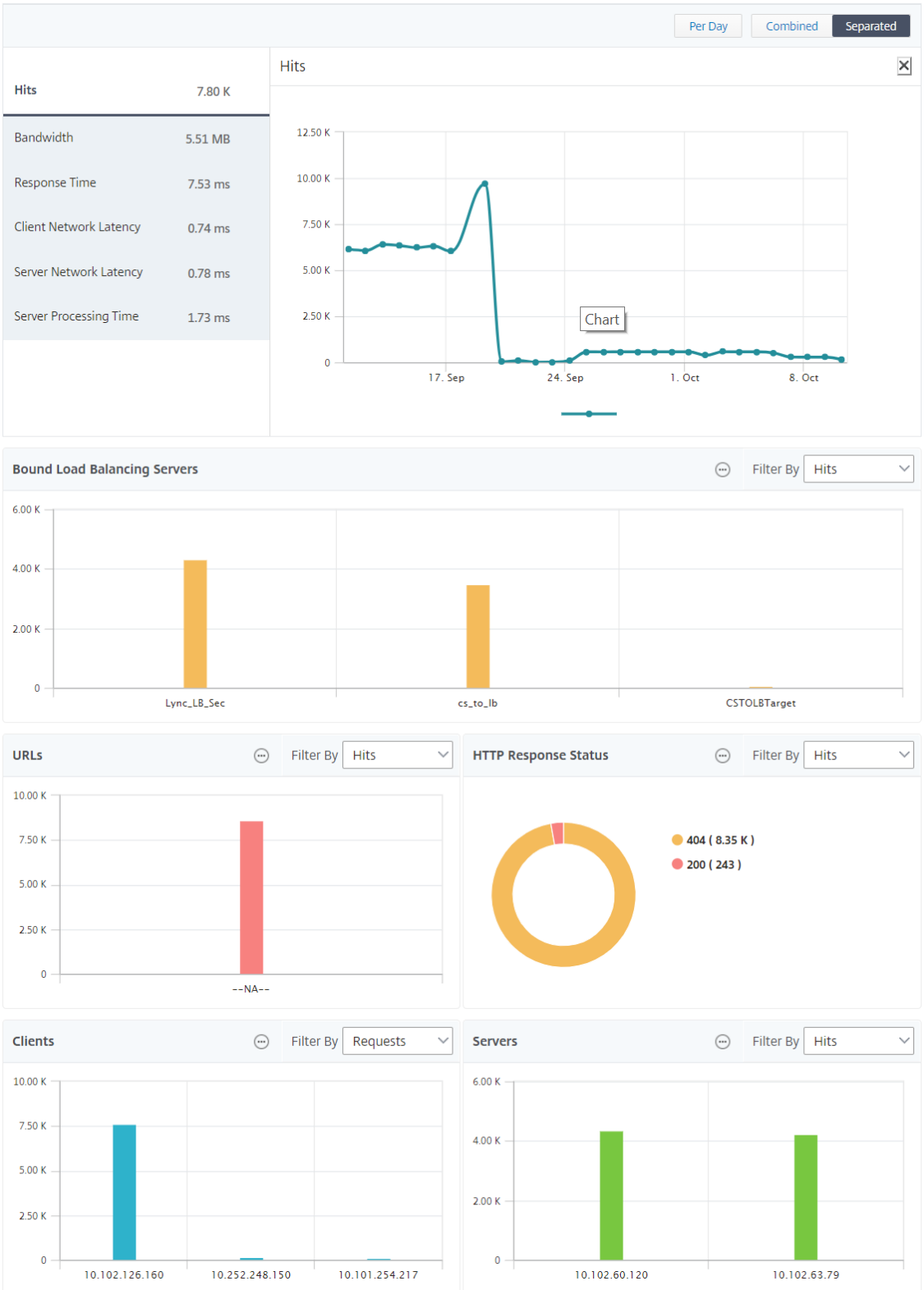
1. Navigieren Sie zu **Analytics** > **Web Insight** > **Anwendungen**
2. Wählen Sie den virtuellen Content Switching-Server aus.
   Beispielsweise ist die Anwendung CSTOLBTarget im Image ein virtueller Content Switching-Server, der an andere virtuelle Server mit Lastenausgleich gebunden ist



Applications

Name	Hits	Bandwidth	Response Time
lb1	167.05 K	136.74 MB	0.74 ms
CSTOLBTarget	61.06 K	60.14 MB	8.66 ms
cstolb	6.61 K	4.80 MB	374.97 ms
lb2	4.83 K	3.61 MB	0.67 ms
OWA_web	4.31 K	3.27 MB	3.21 ms
CSVserv1	291	184.82 KB	157.12 ms
Lync_LB_Sec	10	12.63 KB	86.43 ms

3. Klicken Sie auf den virtuellen Content Switching-Server, um den anderen virtuellen Lastausgleichsserver anzuzeigen. Sie können auch auf den Anwendungsnamen in der Tabelle klicken.



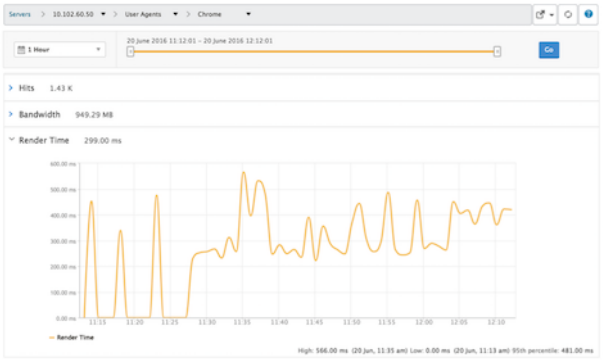
Sie können weiter auf die gebundenen Lastausgleichsserver klicken, um die Web Insight-Details dieser Anwendungen anzuzeigen.

Analysieren von Erkenntnissen für Browser und Betriebssysteme

Mithilfe von Web Insight können Sie L7-Latenzprobleme trennen und die Nutzung mobiler Geräte verstehen. Als Administrator können Sie die Erkenntnisse dazu beitragen, unterschiedliche Betriebssystemzugaben in Ihrer Benutzerbasis zu verstehen.

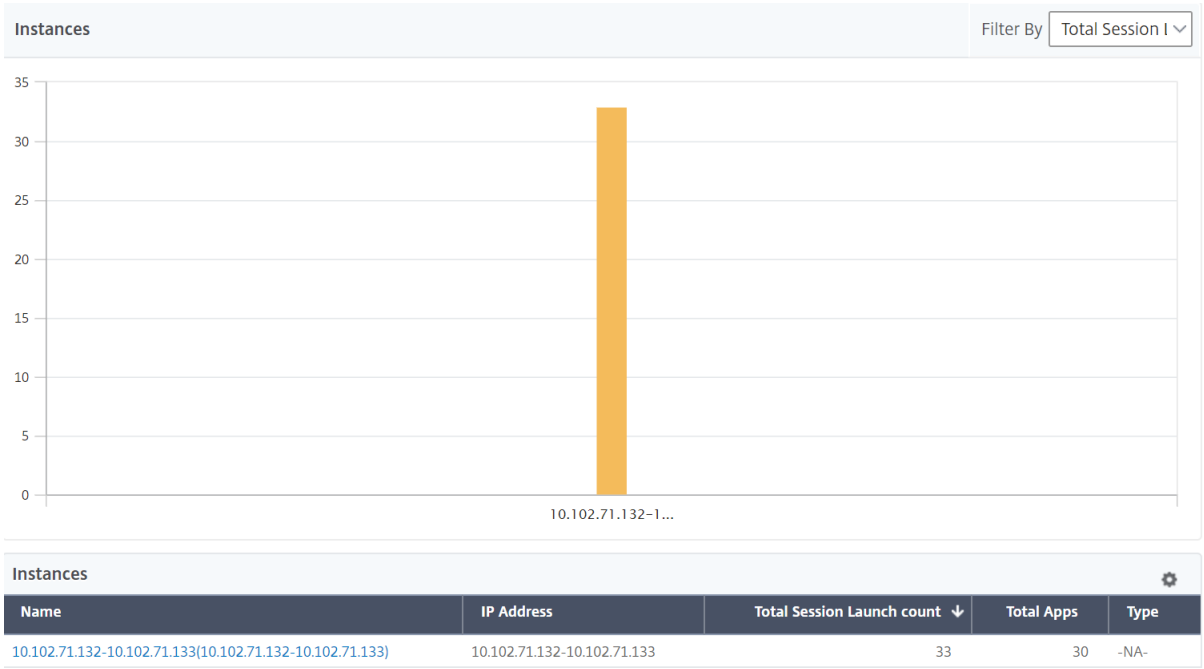
Navigieren Sie zu **Analytics** > **Web Insight** > **Betriebssystem**, um zu sehen, warum der Benutzerzugriff langsam ist und ob dies auf Inkompatibilität in bestimmten Browsern zurückzuführen ist. Sie können auch sehen, welche Betriebssysteme auf bestimmten Clients verwendet werden und welche Browser aufgerufen werden. Sie können die gerenderte Zeit in den verschiedenen Browsern vergleichen und einen weiteren Drilldown zu einem bestimmten Browser erstellen, um zu ermitteln, welche Anwendungsseiten mit der höchsten Rendering-Zeit für diesen Browser verknüpft sind.

Sie können beispielsweise **Google Chrome** auswählen und sich die entsprechenden Renderzeiten für die verschiedenen URL-Seiten für eine bestimmte Anwendung anzeigen lassen.

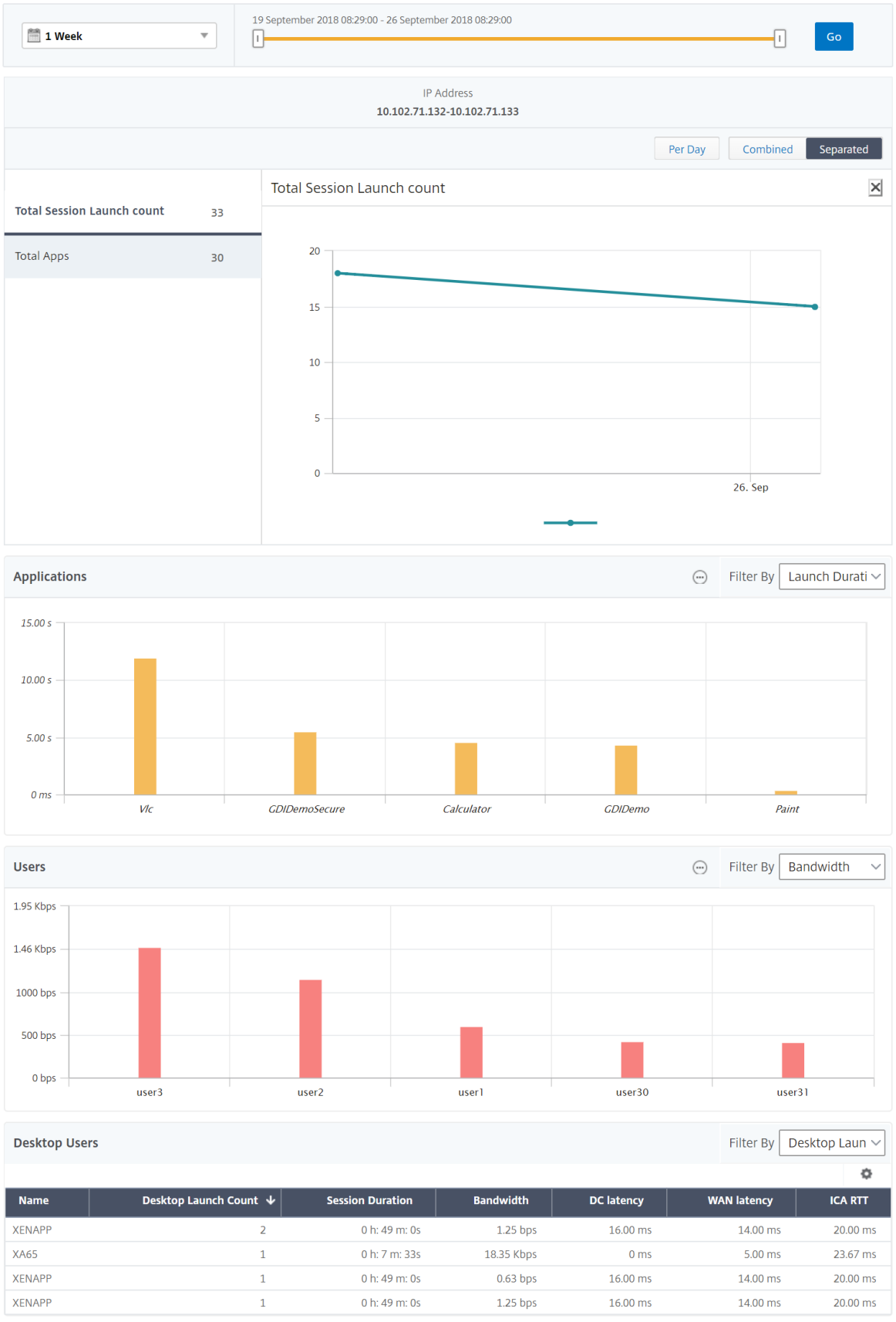


NetScaler ADC-Instanzen, die im Hochverfügbarkeitsmodus bereitgestellt werden

Citrix ADM stellt Berichte für ADC-Instanzen bereit, die im Hochverfügbarkeitsmodus bereitgestellt werden. Aggregierte Berichte für Instanzen im Hochverfügbarkeitsmodus werden in allen Analysen unterstützt.



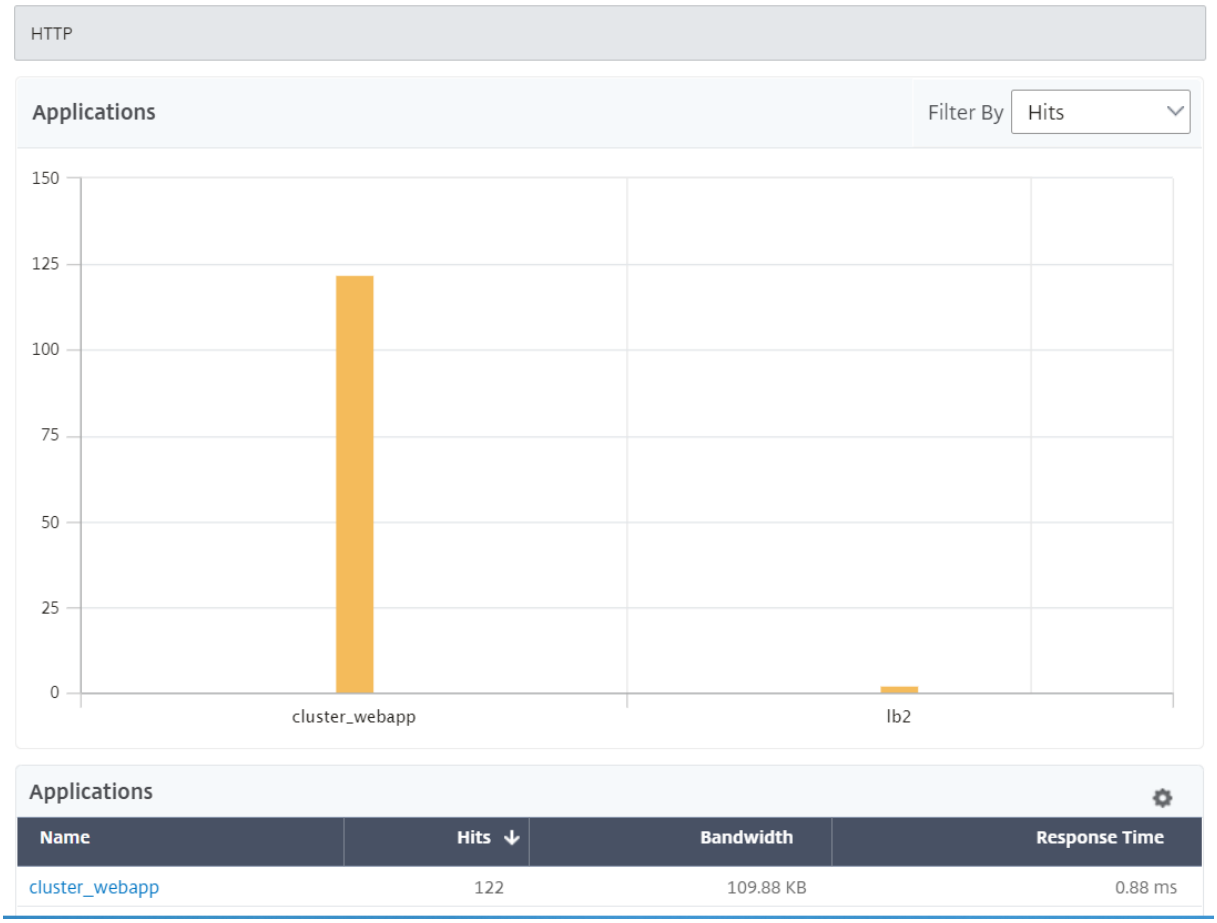
Sie können auf den Namen der Instanzen klicken, die hochverfügbar sind, um weitere Details anzuzeigen.



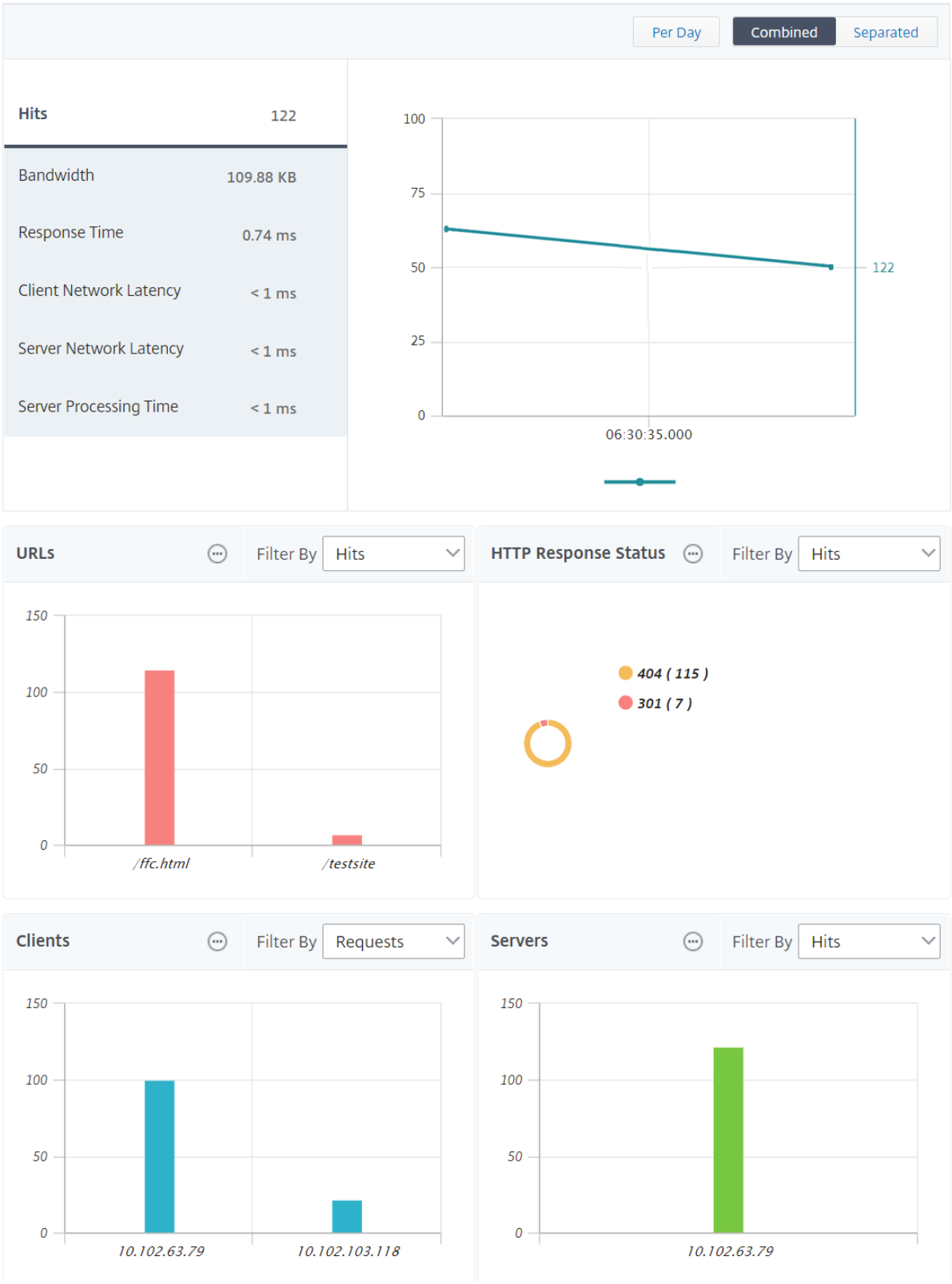
Name	Desktop Launch Count	Session Duration	Bandwidth	DC latency	WAN latency	ICA RTT
XENAPP	2	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms
XA65	1	0 h: 7 m: 33s	18.35 Kbps	0 ms	5.00 ms	23.67 ms
XENAPP	1	0 h: 49 m: 0s	0.63 bps	16.00 ms	14.00 ms	20.00 ms
XENAPP	1	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms

NetScaler ADC-Instanzen, die im Clustermodus bereitgestellt werden

Citrix ADM stellt Berichte für ADC-Instanzen bereit, die im Clustermodus bereitgestellt werden. Aggregierte Berichte für Instanzen im Clustermodus werden in allen Analysen unterstützt.



Sie können auch auf den **CLIP**-Hostnamen klicken, um alle Details zu den ADC-Instanzen anzuzeigen, die in einem Clustermodus bereitgestellt werden.



> **Hinweis**
>
> - Alle Daten, die zuvor vor dem Upgrade auf NetScaler ADM 12.1 Build 503.x erhoben wurden, bleiben für den Zeitraum bis zur Dauer der Daten als unabhängige Berichte angezeigt.
> - Bei ADC-Instanzen, die im Clustermodus bereitgestellt werden, werden Observation Domain ID/Observation Domain Names durch CLIP Hostname und CLIP ersetzt. Alle zuvor gesammelten Daten melden weiterhin Observation Domain ID/Observation Domain Name.

Web Insight-Geokarten-Konfiguration

Die Geomaps-Funktion in NetScaler ADM zeigt die Verwendung von Webanwendungen an verschiedenen geografischen Standorten auf einer Karte an. Administratoren können diese Informationen verwenden, um die Trends bei der Anwendungsnutzung und bei der Kapazitätsplanung zu verstehen.

Die Geo-Map bietet Informationen zu den folgenden Kennzahlen, die für ein Land, einen Bundesstaat und eine Stadt spezifisch sind:

- Treffer insgesamt: Gesamtzahl der Zugriffe auf eine Anwendung.
- Bandbreite: Gesamtbandbreite, die bei der Bearbeitung von Clientanfragen
- Antwortzeit: Durchschnittliche Zeit für das Senden von Antworten auf Clientanforderungen.

Geomaps liefern Informationen, die verwendet werden können, um verschiedene Anwendungsfälle wie die folgenden:

- Region mit der maximalen Anzahl von Clients, die auf eine Anwendung zugreifen
- Region mit der höchsten Reaktionszeit
- Region, die die größte Bandbreite verbraucht

Citrix ADM bietet Ihnen die Möglichkeit, Geomaps für private IP-Adressen oder öffentliche IP-Adressen zu konfigurieren.

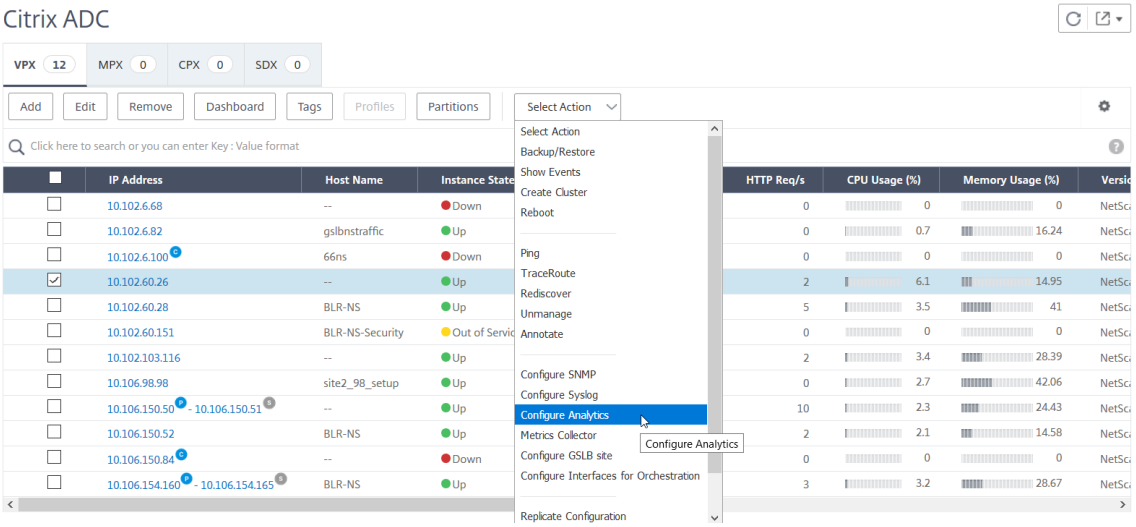
Konfigurieren von Geomaps für private IP-Adressen

> **Hinweis**
>
> Das folgende Verfahren ist nur anwendbar, wenn Citrix ADM **13.0 Build 36.27 oder früher**ist. Für NetScaler ADM **13.0 Build 41.x oder höher**wird die Geodatenerfassung automatisch aktiviert, wenn Sie Web Insight aktivieren.

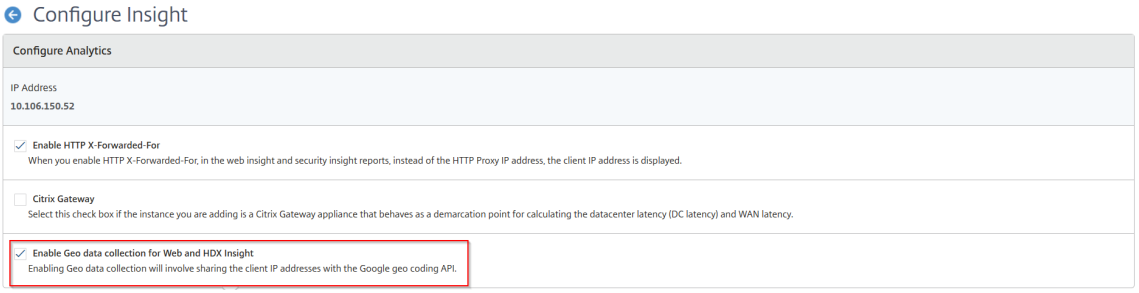
Um den Webanwendungsverkehr anzuzeigen, der von privaten IP-Adressen auf der Geomap ausgeht, müssen Sie zuerst private IP-Adressblöcke erstellen und dann die Erfassung von Geo-Daten aktivieren.

So aktivieren Sie die Geo-Datenerfassung:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC**, und wählen Sie die Citrix ADC-Instanz aus.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.



3. Wählen Sie auf der Seite **Insight konfigurieren** die Option **Geo-Datenerfassung für Web und HDX Insight aktivieren** aus.



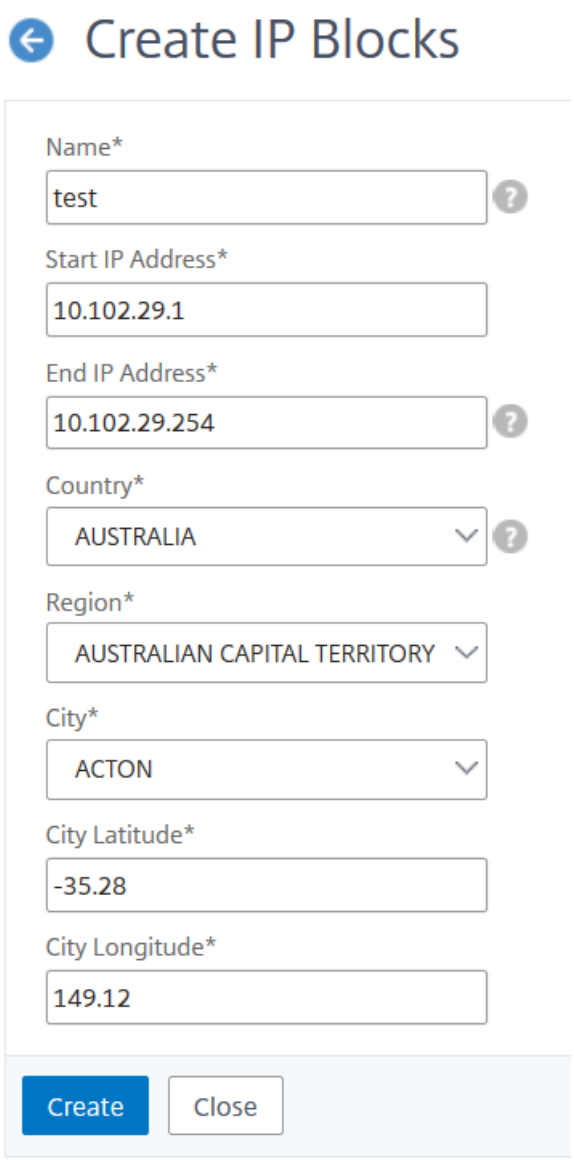
Erstellen eines privaten IP-Blocks NetScaler ADM kann den Standort eines Clients erkennen, wenn die private IP-Adresse des Clients zum NetScaler ADM Server hinzugefügt wird. Wenn beispielsweise die IP-Adresse eines Clients in den Bereich eines privaten IP-Adressblocks fällt, der mit Stadt A verknüpft ist, erkennt NetScaler ADM, dass der Datenverkehr von Stadt A für diesen Client stammt.

So erstellen Sie einen IP-Block:

1. Navigieren Sie in Citrix ADM zu **Analytics** > **Einstellungen** > **IP-Blöcke**, und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie auf der Seite **IP-Blöcke erstellen** die folgenden Parameter an:
   - **Name**. Geben Sie einen Namen für den privaten IP-Block an

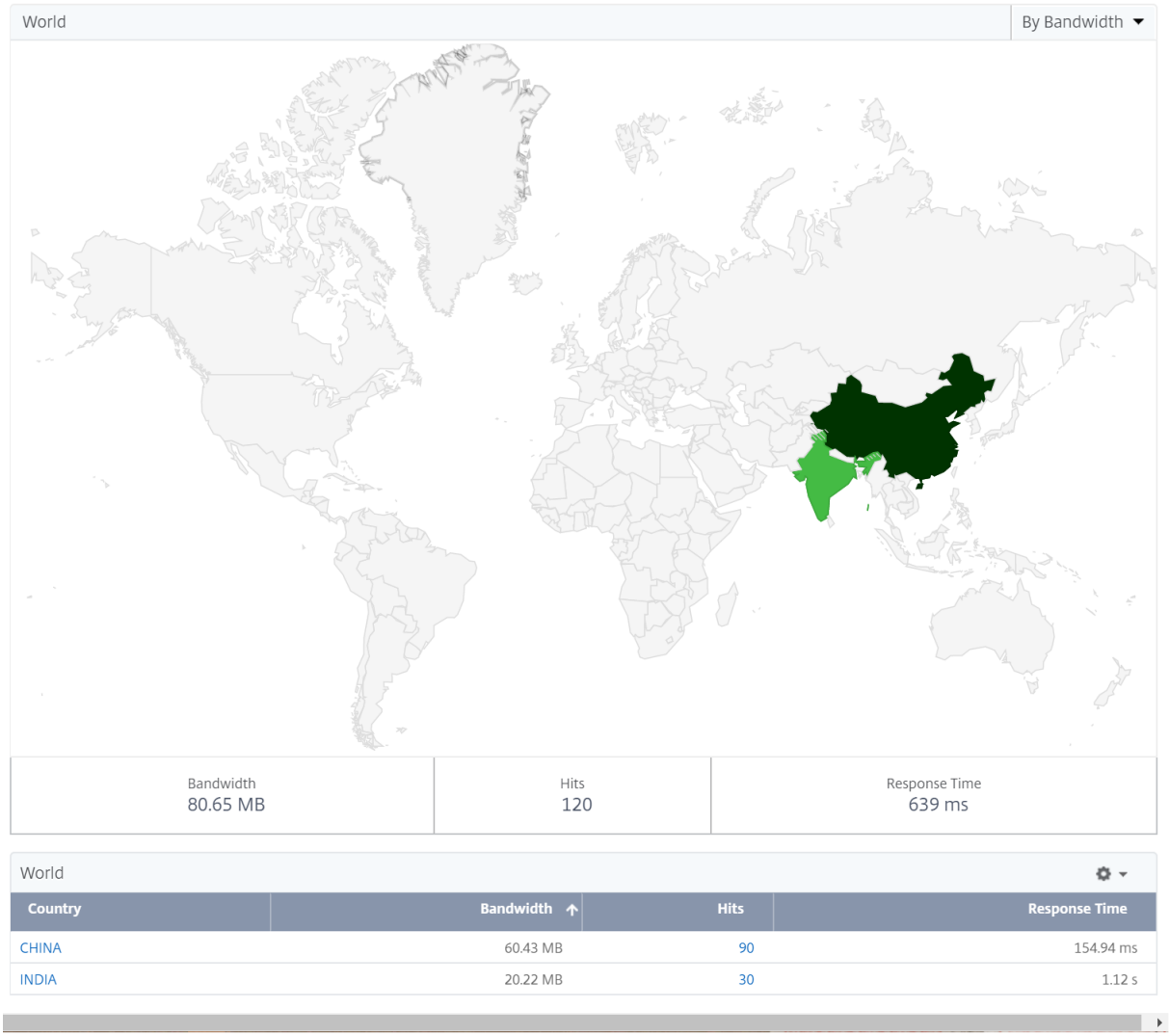
- **Starten Sie die IP-Adresse**. Geben Sie den niedrigsten IP-Adressbereich für den IP-Block an.
- **IP-Adresse beenden**. Geben Sie den höchsten IP-Adressbereich für den IP-Block an.
- **Land**. Wählen Sie das Land aus der Liste aus.
- **Region**. Je nach Land wird die Region automatisch ausgefüllt, Sie können jedoch Ihre Region auswählen.
- **Stadt**. Je nach Region wird die Stadt automatisch ausgefüllt, Sie können jedoch Ihre Stadt auswählen.
- **Breitengrad** der **Stadt und Längengrad**der Stadt. Basierend auf der ausgewählten Stadt werden Breiten- und Längengrade automatisch ausgefüllt.

3. Klicken Sie zum Abschluss auf **Erstellen**.



Öffentliche IP-Blöcke Citrix ADM kann auch den Standort eines Clients erkennen, wenn der Client öffentliche IP-Adresse verwendet. NetScaler ADM verfügt über eine integrierte CSV-Datei, die dem Speicherort basierend auf dem Client-IP-Adressbereich entspricht. **Um den öffentlichen IP-Block verwenden zu können, müssen Sie lediglich die Option Geodatenerfassung aktivieren** auf der Seite **Configure Insight** aktivieren.

> Hinweis
>
> NetScaler ADM erfordert eine Internetverbindung, um die Geomaps für einen bestimmten geografischen Standort anzuzeigen. Eine Internetverbindung ist auch erforderlich, um die GeoMap in den Formaten PDF-, PNG- oder JPG-Format zu exportieren.



So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu **exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren** . Zum Anzeigen und Speichern des Berichts im PDF-, JPEG-, PNG- oder CSV-Format.
2. Wählen Sie die Registerkarte **Export planen** aus. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu senden.

> **Hinweis**
>
> - Wenn Sie **Wöchentliche** Wiederholung wählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
> - Wenn Sie **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage

> eingeben, an denen der Bericht geplant werden soll, getrennt durch Kommas.

Schwellenwerte konfigurieren

Sie können Schwellenwerte erstellen und diese benachrichtigen lassen, wenn der Schwellenwert überschritten wird. In einer typischen Bereitstellung können Sie Schwellenwerte wie folgt festlegen:

- Verschiedene Anwendungsmetriken verfolgen
- Erleichtert die Planung
- Lassen Sie sich benachrichtigen, wenn der Metrikwert der Anwendung den festgelegten

So konfigurieren Sie Schwellenwerte:

1. Navigieren Sie zu **Analytics** > **Einstellungen** > **Schwellenwerte**.
2. Klicken Sie auf der Seite **Schwellenwerte** auf **Hinzufügen**.

   Die Seite **Schwellenwert erstellen** wird angezeigt.
3. Geben Sie die folgenden Details an:

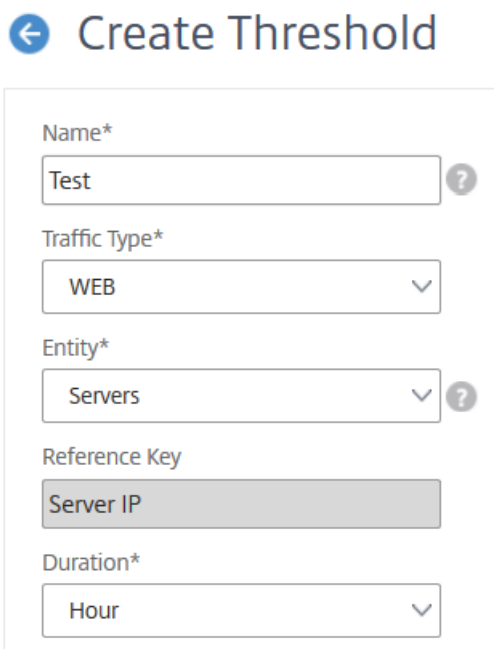
   a) **Name** - Geben Sie einen Namen zum Erstellen eines Ereignisses an.

   b) **Traffic Type** - Wählen Sie in der Liste WEB aus.

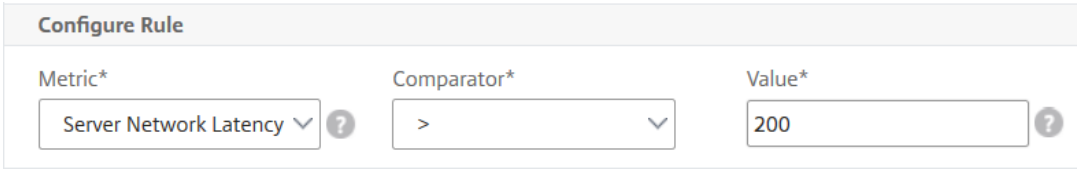
   c) **Entity** - Wählen Sie in der Liste die Kategorie oder den Ressourcentyp aus. Standardmäßig wird “Anwendungen”als Entität ausgewählt.

   d) **Referenzschlüssel** - Ein Referenzschlüssel wird automatisch basierend auf dem ausgewählten Datenverkehrstyp und der ausgewählten Entität generiert.

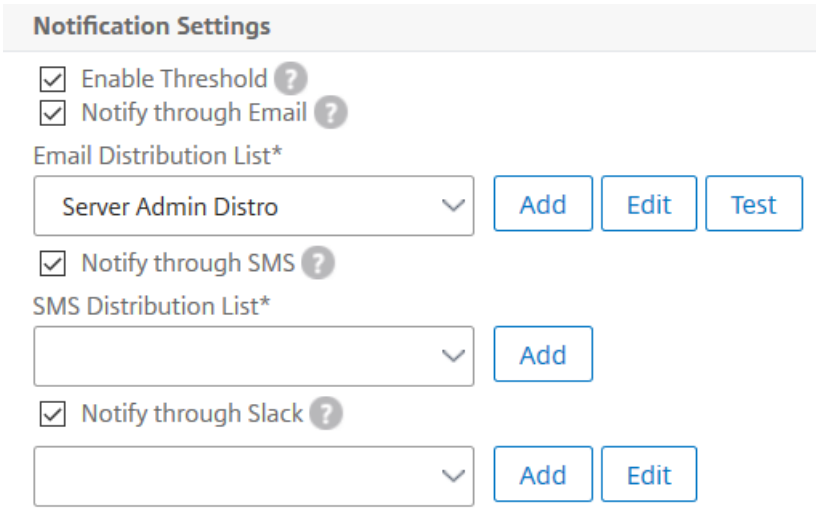
   e) **Dauer** - Wählen Sie in der Liste das Zeitintervall aus, für das Sie die Entität überwachen möchten. Sie können die Entitäten für eine Stunde, für einen Tag oder für eine Woche überwachen.



f) Erstellen **Sie im Abschnitt Regel konfigurieren** eine Regel, indem Sie die Metrik, einen erforderlichen Komparator auswählen und einen Schwellenwert angeben.



g) Wählen Sie im Abschnitt **Benachrichtigungseinstellungen** die Option **Schwellenwert aktivieren** und den Warnmodus, für den Sie die Warnungen abrufen möchten.



4. Klicken Sie auf **Erstellen**.

Beheben von Web Insight-Problemen

Einzelheiten finden Sie im Dokument zur Fehlerbehebung bei Problemen mit Web Insight.

Beheben von Web Insight-Problemen

February 5, 2024

Mit dem NetScaler ADM Web Insight Dashboard können Sie Ihre Anwendungsnutzung visualisieren und alle Webanwendungen überwachen, die die NetScaler ADC-Instanzen bedienen. Mit Web Insight senden die ADC-Instanzen HTTP- und SSL-Transaktionsdaten an den als AppFlow-Collector konfigurierten ADM. AppFlow ist der Flow-Exportstandard, mit dem Anwendungs- und Transaktionsdaten in der Netzwerkinfrastruktur identifiziert und gesammelt werden.

Dieses Dokument hilft Ihnen bei der Behebung häufiger Probleme bei der Web Insight-Bereitstellung.

Probleme im Zusammenhang mit NetScaler ADM Web Insight Dashboard-Berichten

Wenn das ADM Web Insight-Dashboard (**ADM GUI > Analytics > Web Insight**) Berichte nicht anzeigen kann, kann das Problem eines der folgenden Probleme auftreten:

- Web Insight-Konfigurationsproblem
- Verbindungsproblem zwischen NetScaler ADC und NetScaler ADM
- Zählerproblem
- Problem mit der Lizenz
- Problem mit der ID des Beobach
- Fehlende AppFlow-Parameter-Problem

Konfigurationsproblem: NetScaler ADM Web Insight zeigt keine Berichte an

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Stellen Sie sicher, dass das AppFlow Feature in der NetScaler ADC Instanz aktiviert ist. Einzelheiten finden Sie unter AppFlow aktivieren.
2. Überprüfen Sie die Web Insight-Konfiguration in der ADC-Instanz:
    a) Führen Sie den `show running | grep -i <appflow_policy>` Befehl aus, um die Web Insight-Konfiguration der Richtlinie zu überprüfen. Stellen Sie sicher, dass der Bindungstyp `REQUEST`ist. Beispiel: `bind lb vserver afsanity -policy afp -priority 100 -type REQUEST`

b) Führen Sie den `show appflow action` Befehl aus, um die Web Insight-Konfiguration bei Aktion zu überprüfen. Stellen Sie sicher, dass die Option `-webinsight`aktiviert ist
c) Überprüfen Sie den Parameter `appflowlog` im virtuellen LB/CS/CR-Server entsprechend. Stelle sicher, dass dieser Parameter aktiviert ist.

Konnektivitätsproblem zwischen NetScaler ADC und NetScaler ADM: NetScaler ADM Web Insight zeigt keine Berichte an

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Überprüfen Sie den AppFlow Collector-Status in NetScaler ADC. Einzelheiten finden Sie unter So überprüfen Sie den Status der Konnektivität zwischen NetScaler ADC und AppFlow Collector.
2. Überprüfen Sie auf der ADC-GUI, ob die AppFlow Richtlinien Treffer erhalten. Führen Sie den Befehl `show appflow policy <policy_name>` aus, um die Treffer der AppFlow-Richtlinie zu überprüfen. Sie können auch in der GUI zu **System > AppFlow > Richtlinien** navigieren, um die AppFlow-Richtlinientreffer zu überprüfen.
3. Überprüfen Sie jede Firewall, die AppFlow Ports 4739 oder 5557 blockiert.

Gegenproblem: NetScaler ADM Web Insight zeigt keine Berichte an

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

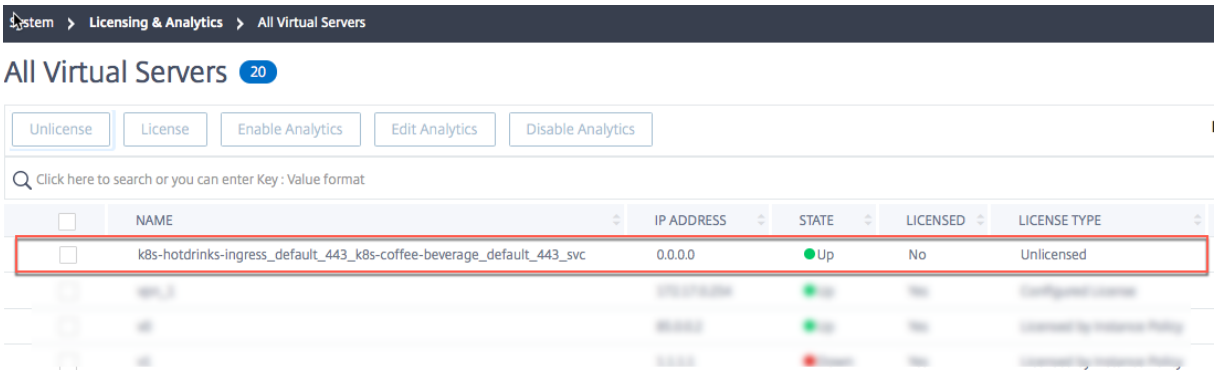
1. Stellen Sie sicher, dass keine AppFlow-Konfigurations- und Verbindungsprobleme vorliegen Weitere Informationen finden Sie in den Lösungsabschnitten in diesem Thema für Konfigurationsprobleme und Konnektivitätsprobleme zwischen NetScaler ADC und NetScaler ADM.
2. Führen Sie auf der ADC-Instanz an der Shell-Eingabeaufforderung den Befehl `nsconmsg -g appflow_tmpl -d current` aus und überprüfen Sie die folgenden Zähler:

   - `appflow_tmpl_v4_l7_clt2ns_complete`
   - `appflow_tmpl_v4_l7_srvr2ns_complete`
   - `appflow_tmpl_v46_ulfd_client_eot`
   - `appflow_tmpl_v46_ulfd_server_eot`

   Wenn einer der Zähler fehlt, führen Sie eine Ablaufverfolgung auf der ADC-Instanz durch. Bestätigen Sie anschließend, dass die Transaktion abgeschlossen ist und die Antwort vom Original-Server gesendet wird. Wenn die Transaktion korrekt ist und einige Zähler fehlen, melden Sie einen Fehler.

Lizenzproblem: NetScaler ADM Web Insight zeigt keine Berichte an

Bei diesem Problem wird die Lizenz für den bestimmten virtuellen Server, für den Sie den Web Insight-Bericht anzeigen möchten, unter **System > Lizenzierung und Analyse > Lizenz konfigurieren** "Nein" angezeigt.



Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Stellen Sie in der ADC-Instanz sicher, dass die AppFlow-Richtlinien-Treffer zunehmen und die Instanz AppFlow-Datensätze an ADM sendet
2. Prüfen Sie, ob der entsprechende virtuelle Server lizenziert ist. Wenn der virtuelle Server nicht lizenziert ist, löscht ADM AppFlow-Datensätze. Daher werden Web Insight-Berichte nicht angezeigt.

Problem mit der Beobachtungspunkt-ID: NetScaler ADM Web Insight zeigt keine Berichte an

Dieses Problem tritt auf, weil die Beobachtungspunkt-ID nicht eindeutig ist.

> Hinweis:
> Eine Beobachtungspunkt-ID ist die Kennung für den NetScaler ADC, aus dem AppFlow-Datensätze exportiert werden. Standardmäßig ist die NetScaler ADC IP die Beobachtungspunkt-ID.

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Stellen Sie in der ADC-Instanz sicher, dass die AppFlow-Richtlinien-Treffer zunehmen und die Instanz AppFlow-Datensätze an ADM beendet.
2. Überprüfen Sie, ob der entsprechende virtuelle Server lizenziert ist.
3. Stellen Sie sicher, dass die Konfiguration nicht von einer ADC-Instanz auf eine andere kopiert wird. Wenn sie kopiert wird, kann die Konfiguration ein Problem mit der Exporter-ID erstellen, wodurch der ADM AppFlow Datensätze gelöscht hat.
4. Melden Sie sich bei der ADC-Instanz an und führen Sie den Befehl `unset appflow param -observationpointId` aus.

Fehlende AppFlow-Parameter-Problem: NetScaler ADM Web Insight zeigt keine Berichte an

Dieses Problem tritt auf, weil ADM AppFlow-Datensätze aufgrund fehlender Daten löscht.

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Stellen Sie sicher, dass in der ADC-Instanz die AppFlow-Richtlinien-Treffer zunehmen und die Instanz AppFlow-Datensätze an ADM beendet.
2. Überprüfen Sie, ob der entsprechende virtuelle Server lizenziert ist.
3. Stellen Sie sicher, dass die Konfiguration nicht von einer ADC-Instanz auf eine andere kopiert wird. Wenn sie kopiert wird, kann die Konfiguration ein Problem mit der Exporter-ID erstellen, wodurch der ADM AppFlow Datensätze gelöscht hat.
4. Stellen Sie sicher, dass die folgenden AppFlow-Parameter auf der ADC-Instanz aktiviert sind:

   a) `HTTP method logging`
   b) `HTTP domain name logging`
   c) `HTTP URL logging`
   d) `HTTP host logging`
   e) `HTTP Content-Type header logging`

Citrix ADM Web Insight Verschiedene Probleme

- **Problem**: Auf dem HTTP-Client wird die Seite nicht geladen, wenn AppFlow aktiviert ist.
- **Lösung**: Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

  1. Deaktivieren Sie im AppFlow Aktionsbefehl die Funktion "PageTracking": `set appflow action <name> -pageTracing disable`. Diese Aktion hat keinen Einfluss auf die Funktionalität.

  Wenn das Problem nicht behoben ist, führen Sie diesen Schritt aus:

  1. Heben Sie in derselben Aktion die Einstellung des Features `clientsidemeasurement` auf `set appflow action <name> -clientsidemeasurements disable`. Wenn dieser Schritt das Problem behebt, erfassen Sie Traces in der ADC-Instanz und melden Sie einen Fehler.

- **Problem**: Die ADC-Appliance stürzt ab, wenn AppFlow aktiviert ist.
- **Lösung**: Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

Wenn Backtrace (BT) über AppFlow Funktionen verfügt, liegt das Problem möglicherweise in der AppFlow-Funktion vor. Wenn sich der BT im Feature-spezifischen Code befindet, liegt das Problem möglicherweise in den Features, die AppFlow verwenden, um Daten an die Collectors zu senden. Deaktivieren Sie im letzteren Fall jede funktionsspezifische AppFlow Konfiguration, und überprüfen

Sie sie. Deaktivieren Sie die AppFlow Funktion nicht global, da dieser Schritt nicht viel Einblick in das Problem gibt.

Problembehandlung bei der Verwendung von Zählern

Überprüfen Sie die folgenden AppFlow-Zähler auf Probleme im Zusammenhang mit AppFlow oder Web Insight.

Zähler	Beschreibung
appflow_tot_record_drop	AppFlow-Datensätze wurden aufgrund eines ungültigen Collectors gelöscht. Dies geschieht normalerweise, wenn sich die Collector-Konfiguration ändert und die vorhandenen Verbindungen die alte Collector-Konfiguration verwenden.
lstream_tot_trans_written	Dieser Zähler muss für jede Transaktion, die protokolliert werden soll, erhöht werden.
lstream_sent	Dieser Zähler erhöht sich für jedes gesendete Transaktionslog.

HDX Insight

February 5, 2024

HDX Insight bietet eine durchgängige Sichtbarkeit des HDX-Datenverkehrs zu Citrix Virtual Apps and Desktop, der über Citrix ADC übertragen wird. Außerdem können Administratoren Client- und Netzwerklatenzmetriken, historische Berichte und End-to-End-Leistungsdaten in Echtzeit anzeigen und Leistungsprobleme beheben. Die Verfügbarkeit von Echtzeit- und historischen Sichtbarkeitsdaten ermöglicht es NetScaler Application Delivery Management (ADM), eine Vielzahl von Anwendungsfällen zu unterstützen.

Damit Daten angezeigt werden, müssen Sie AppFlow auf Ihren virtuellen Citrix Gateway-Servern aktivieren. AppFlow kann über das IPFIX-Protokoll oder die LogStream-Methode bereitgestellt werden.

> **Hinweis**
>
> Aktivieren Sie die folgenden Richtlinieneinstellungen, damit ICA-Rundtrip-Zeitberechnungen

protokolliert werden können:

- ICA Roundtrip Berechnung
- ICA-Roundtrip-Berechnungs
- ICA Roundtrip Berechnung für Leerlaufverbindungen

Wenn Sie auf einen einzelnen Benutzer klicken, können Sie jede aktive oder beendete HDX-Sitzung sehen, die der Benutzer innerhalb des ausgewählten Zeitraums erstellt hat. Weitere Informationen umfassen mehrere Latenzstatistiken und während der Sitzung verbrauchte Bandbreite. Sie können Bandbreiteninformationen auch von einzelnen virtuellen Kanälen wie Audio, Druckerzuordnung und Clientlaufwerkszuordnung abrufen.

Hinweis

Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, Zugriff auf Anwendungsebene für die Gruppe gewähren und Benutzer der Gruppe zuweisen. Citrix ADM Analytics unterstützt jetzt die auf virtuellen IP-Adressen basierende Autorisierung. Ihre Benutzer können jetzt Berichte für alle Insights nur für die Anwendungen (virtuelle Server) anzeigen, für die sie autorisiert sind. Weitere Informationen zu Gruppen und zum Zuweisen von Benutzern zur Gruppe finden Sie unter Konfigurieren von Gruppen.

Sie können auch zu **HDX Insight** > **Anwendungen** navigieren und auf **Startdauer**klicken, um die Zeit für den Start der Anwendung anzuzeigen. Sie können auch den Benutzeragent aller verbundenen Benutzer anzeigen, indem Sie zu **HDX Insight -> Benutzer** navigieren.

Hinweis:HDX Insight unterstützt Admin Partitions, die in NetScaler ADC Instanzen konfiguriert sind, die auf der Softwareversion 12.0 ausgeführt werden.

Die folgenden Thin Clients unterstützen HDX Insight:

- WYSE Windows-basierte Thin Clients
- WYSE Linux-basierte Thin Clients
- WYSE ThinOS-basierte Thin Clients
- 10ZiG Ubuntu-basierte Thin Clients

Identifizierung der Hauptursache für Probleme mit langsamer Leistung

Szenario 1

Der Benutzer hat Verzögerungen beim Zugriff auf Citrix Virtual Apps and Desktops.

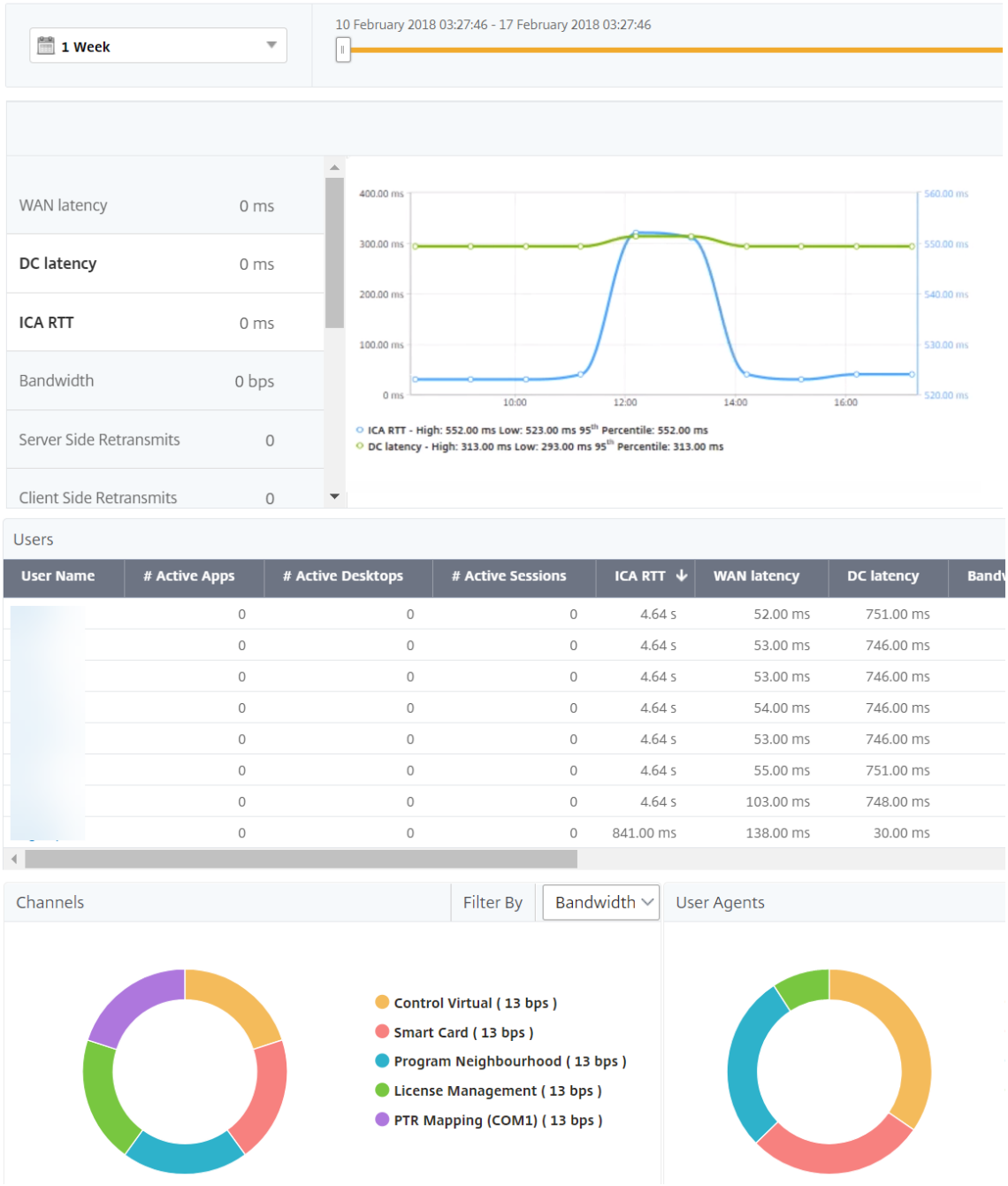
Die Verzögerungen können auf Latenz im Servernetzwerk, durch das Servernetzwerk verursachte ICA-Verkehrsverzögerungen oder Latenz im Client-Netzwerk zurückzuführen sein.

Analysieren Sie die folgenden Metriken, um die Grundursache des Problems zu ermitteln:

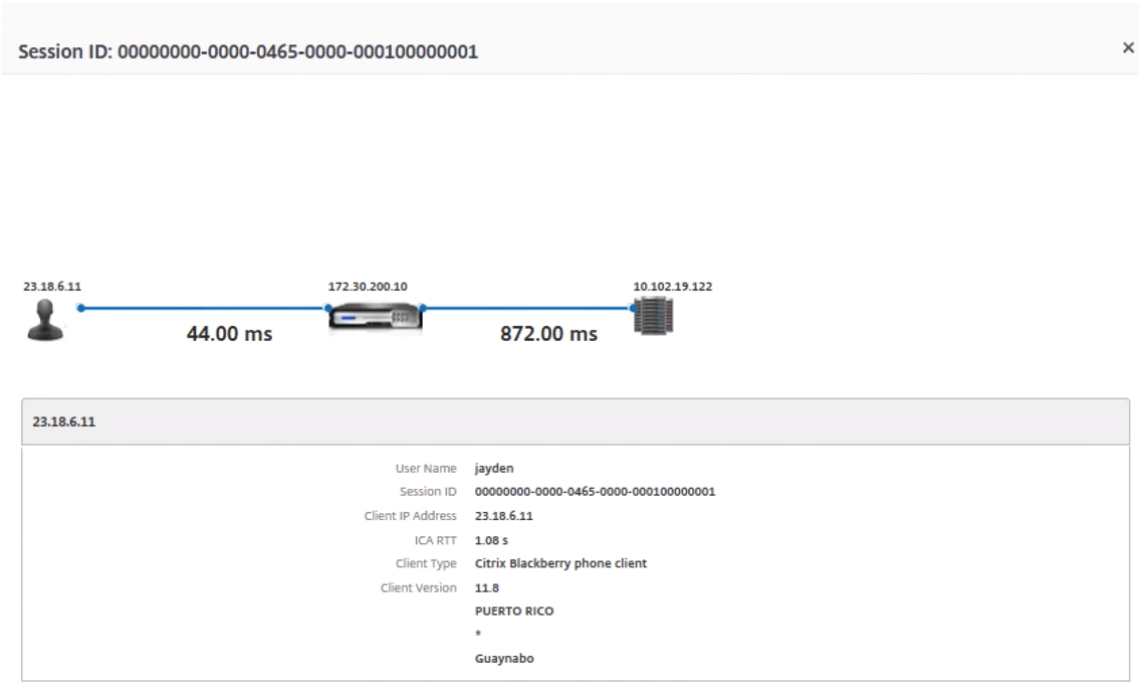
- WAN-Latenz
- DC-Latenz
- Hostverzögerung

So zeigen Sie die Client-Metriken an:

1. Navigieren Sie auf der Registerkarte “**Analytics**”zu “**HDX Insight** “> “**Benutzer**”.
2. Scrollen Sie nach unten, wählen Sie den Benutzernamen aus, und wählen Sie den Zeitraum aus der Liste aus. Der Zeitraum kann ein Tag, eine Woche, ein Monat sein, oder Sie können sogar den Zeitraum anpassen, für den Sie die Daten anzeigen möchten.
3. Das Diagramm zeigt die ICA-RTT- und DC-Latenzwerte des Benutzers für den angegebenen Zeitraum als Diagramm an.



4. Bewegen Sie in der Tabelle**Aktuelle Sitzungen**den Mauszeiger über den**RTT-Wert**, und notieren Sie die Hostverzögerung, DC-Latenz und WAN-Latenz.
5. Klicken Sie in der Tabelle**Aktuelle Sitzungen** auf das Hopdiagrammsymbol, um Informationen über die Verbindung zwischen dem Client und dem Server anzuzeigen, einschließlich Latenzwerte.



Zusammenfassung In diesem Beispiel beträgt die **DC-Latenz** 751 Millisekunden, die **WAN-Latenz** 52 Millisekunden und die **Hostverzögerungen** 6 Sekunden. Dies weist darauf hin, dass es beim Benutzer aufgrund der vom Servernetzwerk verursachten durchschnittlichen Latenz zu Verzögerungen kommt.

Szenario 2

Beim Starten einer Anwendung auf Citrix Virtual App oder Desktop kommt es beim Benutzer zu Verzögerungen

Die Verzögerung kann auf Latenz im Servernetzwerk, durch das Servernetzwerk verursachte ICA-Verkehrsverzögerungen, Latenz im Client-Netzwerk oder auf die zum Starten einer Anwendung benötigte Zeit zurückzuführen sein.

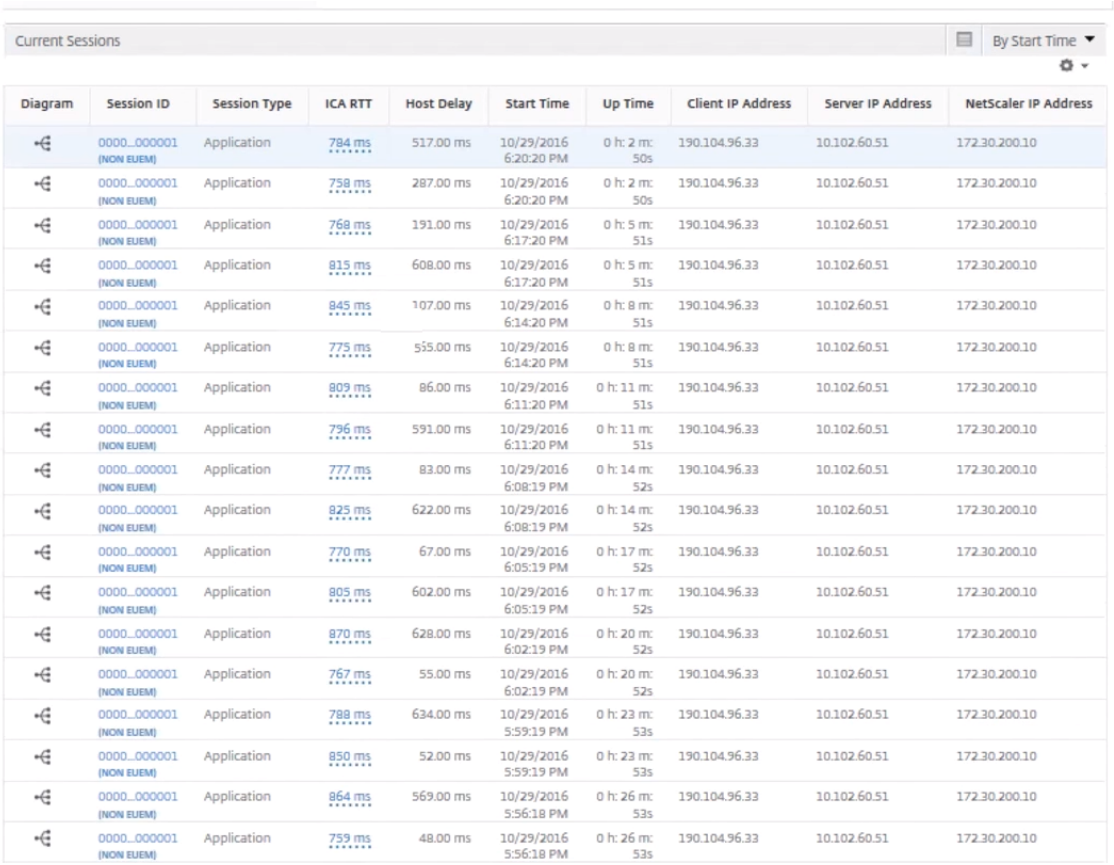
Analysieren Sie die folgenden Metriken, um die Grundursache des Problems zu ermitteln:

- WAN-Latenz
- DC-Latenz
- Host-Verzögerung

So zeigen Sie die Benutzermetriken an:

1. Navigieren Sie auf der Registerkarte **Analytics** zu **HDX Insight** > **Benutzer .**
2. Scrollen Sie nach unten und klicken Sie auf den Benutzernamen

3. Beachten Sie in der grafischen Darstellung die WAN-Latenz-, DC-Latenz- und RTT-Werte für die jeweilige Sitzung.
4. Beachten Sie, dass die Hostverzögerung in der Tabelle **Aktuelle Sitzungen**hoch ist.



Current Sessions — By Start Time

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001 (NON EUEM)	Application	784 ms	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	758 ms	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	768 ms	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	815 ms	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	845 ms	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	775 ms	515.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	809 ms	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	796 ms	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	777 ms	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	825 ms	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	770 ms	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	805 ms	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	870 ms	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	767 ms	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	788 ms	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	850 ms	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	864 ms	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	759 ms	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

Zusammenfassung In diesem Beispiel beträgt die **DC-Latenz** 1 Millisekunde, die **WAN-Latenz** 12 Millisekunden, aber die **Host-Delay** beträgt 517 Millisekunden. Ein hoher RTT mit niedrigen DC- und WAN-Latenzen weist auf einen Anwendungsfehler auf dem Hostserver hin.

> **Hinweis:**HDX Insight zeigt auch mehr Benutzermetriken wie WAN-Jitter und serverseitige Retransmits an, wenn Sie NetScaler ADM verwenden, auf dem Software 11.1 Build 51.21 oder höher ausgeführt wird. Um diese Metriken anzuzeigen, navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**, und wählen Sie einen Benutzernamen aus. Die Benutzermetriken werden in der Tabelle neben dem Diagramm angezeigt.

Geomaps für HDX Insight

Die Citrix ADM Geomaps-Funktion zeigt die Nutzung von Anwendungen an verschiedenen geografischen Standorten auf einer Karte an. Administratoren können diese Informationen verwenden, um die Trends bei der Anwendungsnutzung an verschiedenen geografischen Standorten zu verstehen.

Sie können Citrix ADM so konfigurieren, dass die Geomaps für einen bestimmten geografischen Standort oder ein bestimmtes LAN angezeigt werden, indem Sie den privaten IP-Bereich (Start- und End-IP-Adresse) für den Standort angeben.

Sie können auch die Details der historischen und aktiven Benutzer in den Geostandskarten in HDX Insight anzeigen. Navigieren Sie zu **Analytics** > **HDX Insight**, und klicken Sie im Abschnitt **Welt** der Karte auf das Land oder die Region, für das Sie die Details anzeigen möchten. Sie können weiter aufgliedern, um Informationen nach Stadt und Bundesland anzuzeigen.

So konfigurieren Sie eine Geomap für Rechenzentren:

Navigieren Sie auf der Registerkarte “**Analytics** “zu “**Einstellungen** “> “**IP-Blöcke** “, um Geomaps für einen bestimmten Standort zu konfigurieren.

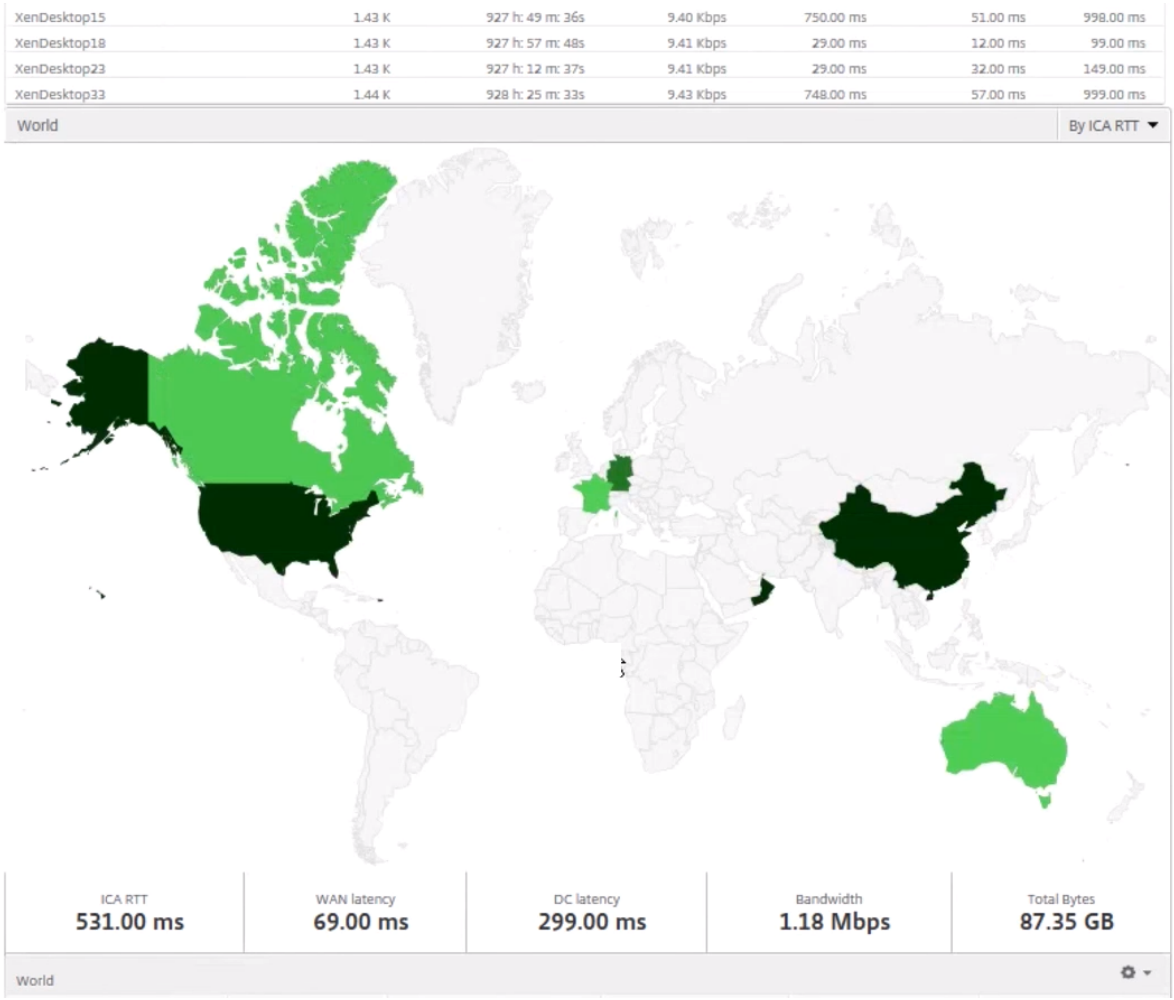
Anwendungsfall

Betrachten Sie ein Szenario, in dem Organisation ABC 2 Niederlassungen hat, eine in Santa Clara und die andere in Indien.

Die Benutzer von Santa Clara verwenden die Citrix Gateway-Appliance unter SCLARA.X.com, um auf den VPN-Verkehr zuzugreifen. Die indischen Benutzer verwenden das Citrix Gateway-Gerät unter India.X.com, um auf den VPN-Verkehr zuzugreifen.

Während eines bestimmten Zeitintervalls, beispielsweise von 10 bis 17 Uhr, stellen die Benutzer in Santa Clara eine Verbindung zu Sclara.x.com her, um auf den VPN-Verkehr zuzugreifen. Die meisten Benutzer greifen auf dasselbe NetScaler Gateway zu, was zu einer Verzögerung bei der Verbindung mit dem VPN führt, sodass einige Benutzer eine Verbindung zu India.x.com anstelle von SClara.x.com herstellen.

Ein NetScaler ADC-Administrator, der den Datenverkehr analysiert, kann die Geokarten-Funktionalität verwenden, um den Datenverkehr im Büro von Santa Clara anzuzeigen. Die Karte zeigt, dass die Reaktionszeit im Büro von Santa Clara hoch ist, da das Büro in Santa Clara nur über ein NetScaler Gateway Gerät verfügt, über das Benutzer auf VPN-Datenverkehr zugreifen können. Der Administrator kann daher entscheiden, ein anderes NetScaler Gateway zu installieren, sodass Benutzer über zwei lokale NetScaler Gateway-Geräte verfügen, über die auf das VPN zugreifen können.



Einschränkungen

Wenn Citrix ADC-Instanzen über eine Advanced-Lizenz verfügen, werden in Citrix ADM für HDX Insight festgelegte Schwellenwerte nicht ausgelöst, da analytische Daten nur 1 Stunde lang erfasst werden.

Aktivieren der HDX Insight Datenerfassung

February 5, 2024

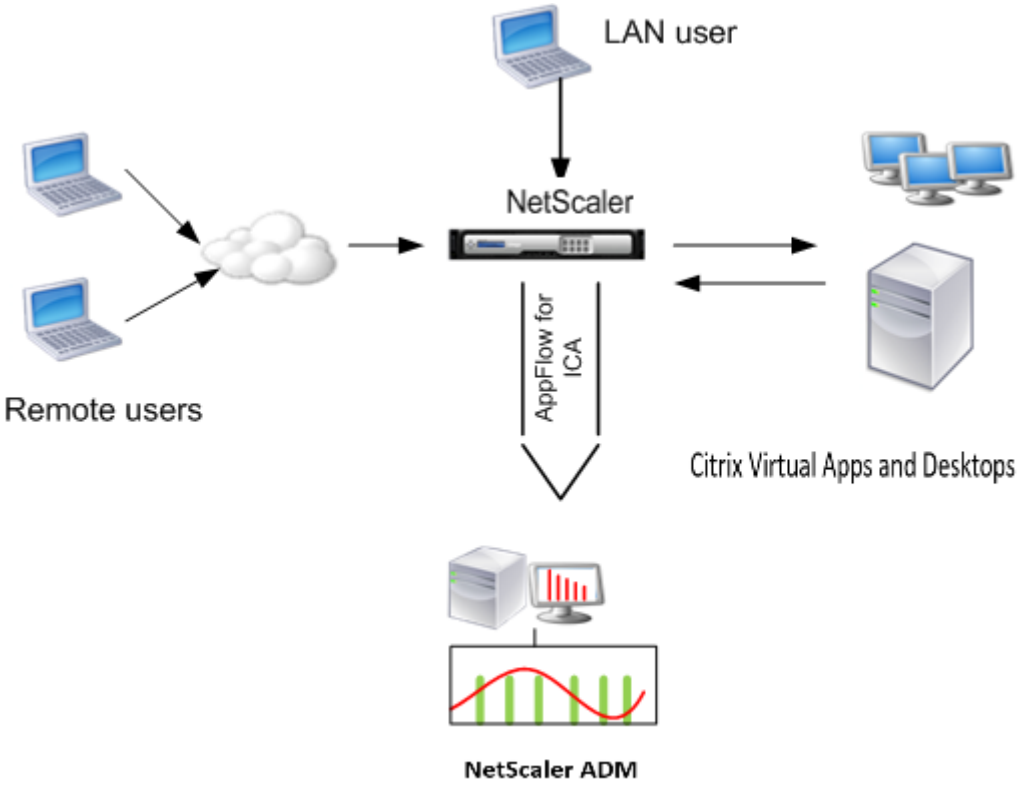
HDX Insight ermöglicht der IT eine außergewöhnliche Benutzererfahrung, indem sie beispiellose End-to-End-Transparenz des ICA-Datenverkehrs bietet, der durch die NetScaler ADC Instanzen oder Citrix SD-WAN Appliances fließt und Teil von NetScaler Application Delivery Management (ADM) Analytics ist. HDX Insight bietet überzeugende und leistungsstarke Business Intelligence- und Fehleranalysefunktionen für Netzwerk, virtuelle Desktops, Anwendungen und Anwendungs-Fabric. HDX Insight kann Benutzerprobleme sofort erfassen, Daten über virtuelle Desktopverbindungen sammeln, AppFlow Datensätze generieren und als visuelle Berichte präsentieren.

Die Konfiguration zur Aktivierung der Datenerfassung im NetScaler ADC unterscheidet sich von der Position der Appliance in der Bereitstellungstopologie.

Aktivieren der Datenerfassung für die Überwachung der im LAN-Benutzermodus bereitgestellten Citrix ADCs

Externe Benutzer, die auf Citrix Virtual App- und Desktop-Anwendungen zugreifen, müssen sich am NetScaler Gateway authentifizieren. Interne Benutzer müssen jedoch möglicherweise nicht an NetScaler Gateway weitergeleitet werden. Außerdem muss der Administrator in einer Bereitstellung im transparenten Modus die Routingrichtlinien manuell anwenden, damit die Anforderungen an die NetScaler ADC Appliance umgeleitet werden.

Um diese Herausforderungen zu meistern und LAN-Benutzer direkt mit Citrix Virtual App- und Desktop-Anwendungen zu verbinden, können Sie das NetScaler ADC Gerät im LAN-Benutzermodus bereitstellen, indem Sie einen virtuellen Cacheumleitungsserver konfigurieren, der als SOCKS-Proxy auf dem NetScaler Gateway Gerät fungiert.



> **Hinweis:** NetScaler ADM und NetScaler Gateway Gerät befinden sich im selben Subnetz.

Um die in diesem Modus bereitgestellten NetScaler ADC-Appliances zu überwachen, fügen Sie zuerst die NetScaler ADC Appliance zum NetScaler Insight-Inventar hinzu, aktivieren Sie AppFlow und sehen Sie sich dann die Berichte im Dashboard an.

Nachdem Sie die NetScaler ADC Appliance zur NetScaler ADM Bestandsliste hinzugefügt haben, müssen Sie AppFlow für die Datenerfassung aktivieren.

> **Hinweis**
>
> - In einer ADC-Instanz können Sie zu **System > AppFlow > Collectors** navigieren, um zu überprüfen, ob der Collector (also NetScaler ADM) aktiviert ist oder nicht. Die NetScaler ADC Instanz sendet AppFlow Datensätze mithilfe von NSIP an NetScaler ADM. Die Instanz verwendet jedoch ihren SNIP, um die Konnektivität mit NetScaler ADM zu überprüfen. Stellen Sie also sicher, dass das SNIP auf der Instanz konfiguriert ist.
> - Sie können die Datenerfassung auf einem NetScaler ADC, der im LAN-Benutzermodus bereitgestellt wird, nicht mithilfe des NetScaler ADM Konfigurationsdienstprogramms aktivieren.
> - Detaillierte Informationen zu den Befehlen und ihrer Verwendung finden Sie in der Befehlsreferenz .

- Informationen zu Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke .

So konfigurieren Sie die Datenerfassung auf einer NetScaler ADC Appliance mithilfe der Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Melden Sie sich bei einer Appliance an.
2. Fügen Sie einen virtuellen Forward-Proxy-Cache-Umleitungsserver mit Proxy-IP und Port hinzu, und geben Sie den Diensttyp als HDX an.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

Beispiel

```
add cr vserver cr1 HDX 10.12.2.2 443 – cacheType FORWARD –
   cltTimeout 180
<!--NeedCopy-->
```

> **Hinweis:** Wenn Sie mit einem NetScaler Gateway-Gerät auf das LAN-Netzwerk zugreifen, fügen Sie eine Aktion hinzu, die durch eine Richtlinie angewendet wird, die dem VPN-Verkehr entspricht.

```
add vpn trafficAction <name> <qual> [-HDX ( ON or OFF )]

add vpn trafficPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Beispiel

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. Fügen Sie NetScaler ADM als AppFlow Collector auf der NetScaler ADC Appliance hinzu.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Example:

‘‘‘

add appflow collector MyInsight -IPAddress 192.168.1.101

‘‘‘

4. Erstellen Sie eine AppFlow Aktion, und ordnen Sie den Kollektor der Aktion zu.


```
add appflow action <name> -collectors <string>
```

Beispiel:

```
add appflow action act -collectors MyInsight
```

5. Erstellen Sie eine AppFlow Richtlinie, um die Regel zum Generieren des Datenverkehrs anzugeben.

```
add appflow policy <policyname> <rule> <action>
```

Beispiel:

```
add appflow policy pol true act
```

6. Binden Sie die AppFlow-Richtlinie an einen globalen Bindepunkt.

```
bind appflow global <policyname> <priority> -type <type>
```

Beispiel:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> **Hinweis**
>
> Der Wert vom Typ muss ICA_REQ_OVERRIDE oder ICA_REQ_DEFAULT sein, um auf ICA-Datenverkehr anzuwenden.

7. Legen Sie den Wert des Parameters FlowRecordInterval für AppFlow auf 60 Sekunden fest.

```
set appflow param -flowRecordInterval 60
```

Beispiel:

```
set appflow param -flowRecordInterval 60
```

8. Speichern Sie die Konfiguration. Typ: `save ns config`

Aktivierung der Datenerfassung für NetScaler Gateway-Appliances, die im Single-Hop-Modus bereitgestellt werden

Wenn Sie NetScaler Gateway im Single-Hop-Modus bereitstellen, befindet es sich am Netzwerkrand. Die Gateway-Instanz stellt ICA-Proxy-Verbindungen zur Desktop-Bereitstellungsinfrastruktur bereit. Single-Hop ist das einfachste und gebräuchlichste Deployment. Der Single-Hop-Modus bietet Sicherheit, wenn ein externer Benutzer versucht, auf das interne Netzwerk in einer Organisation zuzugreifen. Im Single-Hop-Modus greifen Benutzer über ein virtuelles privates Netzwerk (VPN) auf die NetScaler ADC-Appliances zu.

Um mit dem Sammeln der Berichte zu beginnen, müssen Sie das NetScaler Gateway Gerät der NetScaler Application Delivery Management (ADM) -Bestandsliste hinzufügen und AppFlow auf ADM aktivieren.

So aktivieren Sie die AppFlow Funktion von NetScaler ADM:

1. Geben Sie in einem Webbrowser die IP-Adresse des NetScaler ADM ein (z. B. http://192.168.100.1).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **Netzwerke** > **Instanzen**, und wählen Sie die NetScaler ADC Instanz aus, die Sie die Analyse aktivieren möchten.
4. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
5. Wählen Sie die virtuellen VPN-Server aus, und klicken Sie auf **Analytics aktivieren**.
6. Wählen Sie **HDX Insight** und dann **ICA** aus.
7. Klicken Sie auf **OK**.

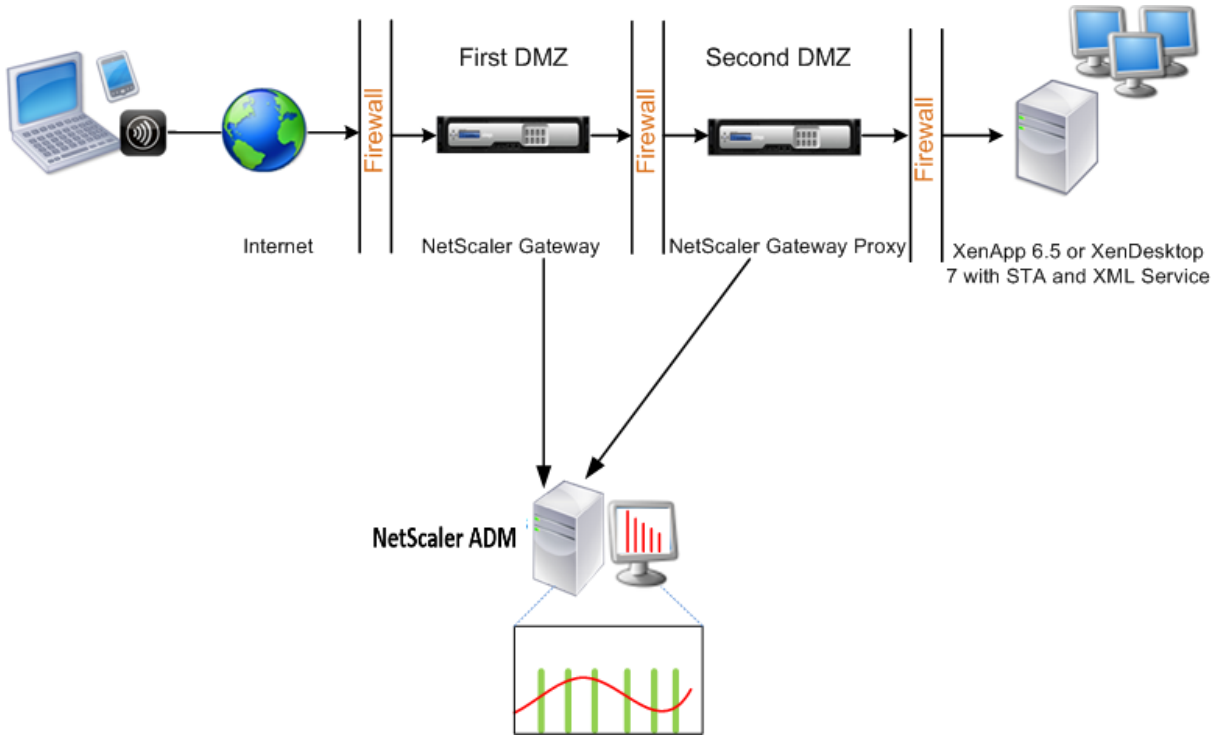
> **Hinweis**
>
> Wenn Sie AppFlow im Single-Hop-Modus aktivieren, werden die folgenden Befehle im Hintergrund ausgeführt. Diese Befehle werden hier explizit zur Fehlerbehebung angegeben.

```
- add appflow collector <name> -IPAddress <ip_addr>

- add appflow action <name> -collectors <string>

- set appflow param -flowRecordInterval <secs>

- disable ns feature AppFlow

- enable ns feature AppFlow

- add appflow policy <name> <rule> <expression>

- set appflow policy <name> -rule <expression>

- bind vpn vserver <vsname> -policy <string> -type <type> -priority <
  positive_integer>

- set vpn vserver <name> -appflowLog ENABLED

- save ns config
```

Virtuelle EUEM-Kanaldaten sind Teil von HDX Insight Daten, die NetScaler ADM von Gateway-Instanzen erhält. Der virtuelle EUEM-Kanal stellt die Daten über ICA-RTT bereit. Wenn der virtuelle EUEM-Kanal nicht aktiviert ist, werden die verbleibenden HDX Insight Daten weiterhin in NetScaler ADM angezeigt.

Aktivierung der Datenerfassung für NetScaler Gateway-Appliances, die im Double-Hop-Modus bereitgestellt werden

Der NetScaler Gateway -Doppelhop-Modus bietet zusätzlichen Schutz für das interne Netzwerk einer Organisation, da ein Angreifer mehrere Sicherheitszonen oder demilitarisierte Zonen (DMZ) durchdringen muss, um die Server im sicheren Netzwerk zu erreichen. Wenn Sie die Anzahl der Hops (NetScaler Gateway Geräte) analysieren möchten, über die die ICA-Verbindungen weitergeleitet werden, sowie die Details zur Latenz für jede TCP-Verbindung und wie sie mit der gesamten ICA-Latenz verglichen wird, die vom Client wahrgenommen wird, müssen Sie NetScaler ADM installieren, damit die NetScaler Gateway-Geräte diese wichtigen Statistiken zu berichten.



NetScaler Gateway in der ersten DMZ verarbeitet Benutzerverbindungen und führt die Sicherheitsfunktionen eines SSL-VPN aus. Dieses NetScaler Gateway verschlüsselt Benutzerverbindungen, bestimmt, wie die Benutzer authentifiziert werden, und steuert den Zugriff auf die Server im internen Netzwerk.

Das NetScaler Gateway in der zweiten DMZ dient als NetScaler Gateway-Proxygerät. Dieses NetScaler Gateway ermöglicht es dem ICA-Datenverkehr, die zweite DMZ zu durchqueren, um Benutzerverbindungen zur Serverfarm herzustellen.

Das NetScaler ADM kann entweder im Subnetz der NetScaler Gateway-Appliance in der ersten DMZ oder im Subnetz des zweiten DMZ der NetScaler Gateway-Appliance bereitgestellt werden. Im obigen Bild werden NetScaler ADM und NetScaler Gateway in der ersten DMZ im selben Subnetz bereitgestellt.

Im Double-Hop-Modus sammelt NetScaler ADM TCP-Datensätze von einer Appliance und ICA-Einträge von der anderen Appliance. Nachdem Sie die NetScaler Gateway-Appliances zum NetScaler ADM-Inventar hinzugefügt und die Datenerfassung aktiviert haben, exportiert jede der Appliances die Berichte, indem sie die Hop-Anzahl und die Verbindungsketten-ID verfolgt.

Damit NetScaler ADM identifiziert, welche Appliance Datensätze exportiert, wird jede Appliance mit einer Hop-Anzahl angegeben, und jede Verbindung wird mit einer Verbindungsketten-ID angegeben. Die Hop-Anzahl gibt die Anzahl der NetScaler Gateway-Appliances an, durch die der Datenverkehr von einem Client zu den Servern fließt. Die Verbindungsketten-ID stellt die End-to-End-Verbindungen zwischen dem Client und dem Server dar.

NetScaler ADM verwendet die Hop-Anzahl und die Verbindungsketten-ID, um die Daten der beiden NetScaler Gateway Geräte miteinander zu verknüpfen und die Berichte zu generieren.

Um NetScaler Gateway Geräte zu überwachen, die in diesem Modus bereitgestellt werden, müssen Sie zuerst NetScaler Gateway zur NetScaler ADM Bestandsliste hinzufügen, AppFlow auf NetScaler ADM aktivieren und dann die Berichte auf dem NetScaler ADM-Dashboard anzeigen.

Konfigurieren Sie HDX Insight auf virtuellen Servern, die für Optimal Gateway verwendet werden

Schritte zum Konfigurieren von HDX Insight auf virtuellen Servern, die für Optimal Gateway verwendet werden:

1. Navigieren Sie zu **Netzwerke** > **Instanzen**, und wählen Sie die NetScaler ADC Instanz aus, die Sie die Analyse aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
3. Wählen Sie den für die Authentifizierung konfigurierten virtuellen VPN-Server aus und klicken Sie auf **Enable Analytics**.
4. Wählen Sie **HDX Insight** und dann **ICA** aus.
5. Wählen Sie je nach Bedarf weitere erweiterte Optionen aus.
6. Klicken Sie auf **OK**.
7. Wiederholen Sie die Schritte 3 bis 6 auf dem anderen virtuellen VPN-Server.

Aktivieren der Datenerfassung auf NetScaler ADM

Wenn Sie NetScaler ADM aktivieren, um die ICA-Details von beiden Appliances zu erfassen, sind die erfassten Details redundant. Das ist, dass beide Appliances die gleichen Metriken melden. Um diese Situation zu umgehen, müssen Sie AppFlow für ICA auf einer der ersten NetScaler Gateway-Appliances

und dann AppFlow für TCP auf der zweiten Appliance aktivieren. Auf diese Weise exportiert eine der Appliances ICA-AppFlow Datensätze, und die andere Appliance exportiert TCP-AppFlow-Datensätze. Dies spart auch die Verarbeitungszeit beim Analysieren des ICA-Datenverkehrs.

So aktivieren Sie die AppFlow Funktion von NetScaler ADM:

1. Geben Sie in einem Webbrowser die IP-Adresse des NetScaler ADM ein (z. B. http://192.168.100.1).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **Netzwerke** > **Instanzen**, und wählen Sie die NetScaler ADC Instanz aus, die Sie die Analyse aktivieren möchten.
4. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
5. Wählen Sie die virtuellen VPN-Server aus, und klicken Sie auf **Analytics aktivieren**.
6. Wählen Sie **HDX Insight** und dann **ICA** oder **TCP** für ICA-Verkehr bzw. TCP-Verkehr aus.

   > **Hinweis**
   >
   > Wenn die AppFlow-Protokollierung für die jeweiligen Dienste oder Dienstgruppen auf der NetScaler ADC Appliance nicht aktiviert ist, zeigt das NetScaler ADM-Dashboard die Datensätze nicht an, auch wenn in der Insight-Spalte Aktiviert angezeigt wird.

7. Klicken Sie auf **OK**.

Konfigurieren von NetScaler Gateway Geräten zum Exportieren von Daten

Nach der Installation der NetScaler Gateway Geräte müssen Sie die folgenden Einstellungen auf den NetScaler Gateway-Geräten konfigurieren, um die Berichte in NetScaler ADM zu exportieren:

- Konfigurieren Sie virtuelle Server der NetScaler Gateway-Appliances in der ersten und zweiten DMZ, um miteinander zu kommunizieren.
- Binden Sie den virtuellen NetScaler Gateway -Server in der zweiten DMZ an den virtuellen NetScaler Gateway-Server in der ersten DMZ.
- Aktivieren Sie den Double-Hop auf dem NetScaler Gateway in der zweiten DMZ.
- Deaktivieren Sie die Authentifizierung auf dem virtuellen NetScaler Gateway -Server in der zweiten DMZ.
- Aktivieren Sie eine der NetScaler Gateway-Appliances, um ICA-Datensätze zu exportieren
- Aktivieren Sie die andere NetScaler Gateway-Appliance, um TCP-Datensätze zu exportieren:
- Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway Geräten.

NetScaler Gateway über die Befehlszeilenschnittstelle konfigurieren:

1. Konfigurieren Sie den virtuellen NetScaler Gateway -Server in der ersten DMZ für die Kommunikation mit dem virtuellen NetScaler Gateway-Server in der zweiten DMZ.

```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (
    ON or OFF)] [-imgGifToPng]

add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
```

2. Binden Sie den virtuellen NetScaler Gateway -Server in der zweiten DMZ an den virtuellen NetScaler Gateway-Server in der ersten DMZ. Führen Sie den folgenden Befehl auf dem NetScaler Gateway in der ersten DMZ aus:

```
bind vpn vserver <name> -nextHopServer <name>

bind vpn vserver vs1 -nextHopServer nh1
```

3. Aktivieren Sie Double-Hop und AppFlow auf dem NetScaler Gateway in der zweiten DMZ.

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [-
     appflowLog ( ENABLED or DISABLED )]

set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
```

4. Deaktivieren Sie die Authentifizierung auf dem virtuellen NetScaler Gateway -Server in der zweiten DMZ.

```
set vpn vserver <name> [-authentication (ON or OFF)]

set vpn vserver vs -authentication OFF
```

5. Aktivieren Sie eines der NetScaler Gateway Geräte zum Exportieren von TCP-Datensätzen.

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
    OTHERTCP_REQUEST
```

6. Aktivieren Sie das andere NetScaler Gateway Gerät zum Exportieren von ICA-Datensätzen:

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
    ICA_REQUEST
```

7. Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway Geräten:

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]

```



```
3 set appflow param -connectionChaining ENABLED
```

NetScaler Gateway über das Konfigurationsdienstprogramm konfigurieren:

1. Konfigurieren Sie das NetScaler Gateway in der ersten DMZ für die Kommunikation mit dem NetScaler Gateway in der zweiten DMZ, und binden Sie das NetScaler Gateway in der zweiten DMZ an das NetScaler Gateway in der ersten DMZ.
   a) Erweitern Sie auf der Registerkarte**KonfigurationCitrix Gateway**, und klicken Sie auf**Virtuelle Server**.
   b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe “Erweitert”die Option **Published Applications**.
   c) Klicken Sie auf**Next Hop Server**, und binden Sie einen nächsten Hop-Server an das zweite NetScaler Gateway Gerät.
2. Aktivieren Sie den Double-Hop auf dem NetScaler Gateway in der zweiten DMZ.
   a) Erweitern Sie auf der Registerkarte**KonfigurationCitrix Gateway**, und klicken Sie auf**Virtuelle Server**.
   b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und klicken Sie in der Gruppe**Grundeinstellungen** auf das Symbol Bearbeiten.
   c) Erweitern Sie More, wählen Sie **Double Hop** und klicken Sie auf **OK**.
3. Deaktivieren Sie die Authentifizierung auf dem virtuellen Server auf dem NetScaler Gateway in der zweiten DMZ.
   a) Erweitern Sie auf der Registerkarte **Konfiguration Citrix Gateway** und klicken Sie auf **Virtuelle Server** .
   b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und klicken Sie in der Gruppe**Grundeinstellungen** auf das Symbol Bearbeiten.
   c) Erweitern Sie**Mehr**, und deaktivieren Sie **Authentifizierung aktivieren**.
4. Aktivieren Sie eines der NetScaler Gateway Geräte zum Exportieren von TCP-Datensätzen.
   a) Erweitern Sie auf der Registerkarte **Konfiguration Citrix Gateway** und klicken Sie auf **Virtuelle Server** .
   b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe Erweitert die Option Richtlinien.
   c) Klicken Sie auf das Symbol + und**wählen Sie in der Liste Choose Policy** die Option**AppFlow**aus und **wählen Sie in der Liste Choose Type** die Option**Other TCP-Request**aus.

d) Klicken Sie auf **Weiter**.

e) Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Schließen**.

5. Aktivieren Sie das andere NetScaler Gateway Gerät zum Exportieren von ICA-Datensätzen:

a) Erweitern Sie auf der Registerkarte **Konfiguration Citrix Gateway** und klicken Sie auf **Virtuelle Server** .

b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server und erweitern Sie in der Gruppe **Erweitert**
die Option **Richtlinien**.

c) Klicken Sie auf das Symbol + und wählen Sie in der Liste **Richtlinie auswählen** die Option AppFlow aus, und wählen Sie in der Liste "Typ auswählen"die Option **Andere TCP-Anforderung**aus.

d) Klicken Sie auf **Weiter**.

e) Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Schließen**.

6. Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway Geräten.

a) Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **Appflow**.

b) Doppelklicken Sie im rechten Bereich in der Gruppe **Einstellungen** auf **Change Appflow Settings**.

c) Wählen Sie **Verbindungsverkettung** aus, und klicken Sie auf **OK**.

7. Konfigurieren Sie das NetScaler Gateway in der ersten DMZ für die Kommunikation mit dem NetScaler Gateway in der zweiten DMZ, und binden Sie das NetScaler Gateway in der zweiten DMZ an das NetScaler Gateway in der ersten DMZ.

a) Erweitern Sie auf der Registerkarte "Konfiguration"die Option **NetScaler Gateway** und klicken Sie auf **Virtual Servers**.

b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der**Gruppe Erweitert**die Option**Veröffentlichte Anwendungen**.

c) Klicken Sie auf**Next Hop Server** und binden Sie einen nächsten Hop-Server an das zweite NetScaler Gateway-Gerät.

8. Aktivieren Sie den Double-Hop auf dem NetScaler Gateway in der zweiten DMZ.

a) Erweitern Sie auf der Registerkarte "Konfiguration"die Option **NetScaler Gateway** und klicken Sie auf **Virtual Servers**.

b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und klicken Sie in der Gruppe **Grundeinstellungen**auf das Symbol "Bearbeiten".

c) Erweitern Sie More, wählen Sie **Double Hop** aus und klicken Sie auf **OK**.

9. Deaktivieren Sie die Authentifizierung auf dem virtuellen Server auf dem NetScaler Gateway in der zweiten DMZ.

   a) Erweitern Sie auf der Registerkarte Konfiguration Citrix Gateway, und klicken Sie auf**Virtuelle Server**.

   b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und klicken Sie in der Gruppe **Grundeinstellungen**auf das Symbol "Bearbeiten".

   c) Erweitern Sie**Mehr**, und deaktivieren Sie **Authentifizierung aktivieren**.

10. Aktivieren Sie eines der NetScaler Gateway Geräte zum Exportieren von TCP-Datensätzen.

    a) Erweitern Sie auf der Registerkarte "Konfiguration"die Option **NetScaler Gateway** und klicken Sie auf **Virtual Servers**.

    b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe Erweitert die Option**Richtlinien**.

    c) Klicken Sie auf das Symbol**+**und wählen Sie in der Liste Choose Policy die Option AppFlow aus und **wählen Sie in der Liste Choose Type** die Option**Other TCP-Request**aus.

    d) Klicken Sie auf **Weiter**.

    e) Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Schließen**.

11. Aktivieren Sie die andere NetScaler Gateway-Appliance, um ICA-Datensätze zu exportieren.

    a) Erweitern Sie auf der Registerkarte "Konfiguration"die Option **NetScaler Gateway** und klicken Sie auf **Virtual Servers**.

    b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe Erweitert die Option**Richtlinien**.

    c) Klicken Sie auf das Symbol**+**und**wählen Sie in der Liste Choose Policy**die Option AppFlow aus und **wählen Sie in der Liste Choose Type**die Option**Other TCP-Request**aus.

    d) Klicken Sie auf **Weiter**.

    e) Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Schließen**.

12. Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway Geräten.

Aktivieren der Datensammlung zur Überwachung von Citrix ADCs, die im transparenten Modus bereitgestellt werden

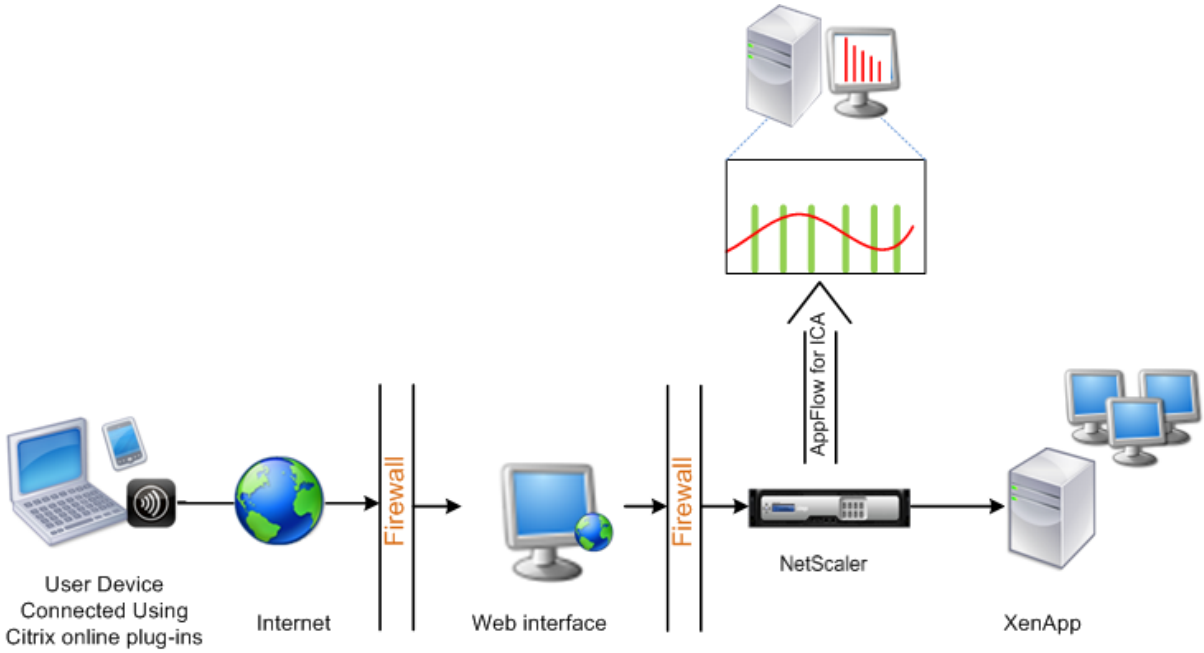
Wenn ein NetScaler ADC im transparenten Modus bereitgestellt wird, können die Clients direkt auf die Server zugreifen, ohne dass ein virtueller Server vorhanden ist. Wenn eine NetScaler ADC Appliance

im transparenten Modus in einer Citrix Virtual Apps and Desktop-Umgebung bereitgestellt wird, wird der ICA-Verkehr nicht über ein VPN übertragen.

Nachdem Sie NetScaler ADC zur NetScaler ADM Bestandsliste hinzugefügt haben, müssen Sie AppFlow für die Datensammlung aktivieren. Die Aktivierung der Datenerfassung hängt vom Gerät und vom Modus ab. In diesem Fall müssen Sie NetScaler ADM als AppFlow-Collector auf jeder NetScaler ADC Appliance hinzufügen, und Sie müssen eine AppFlow-Richtlinie konfigurieren, um den gesamten oder spezifischen ICA-Datenverkehr zu erfassen, der durch die Appliance fließt.

> **Hinweis**
>
> - Sie können die Datenerfassung auf einem NetScaler ADC, der im transparenten Modus bereitgestellt wird, nicht mithilfe des NetScaler ADM Konfigurationsdienstprogramms aktivieren.
> - Detaillierte Informationen zu den Befehlen und ihrer Verwendung finden Sie in der Befehlsreferenz .
> - Informationen zu Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke .

Die folgende Abbildung zeigt die Netzwerkbereitstellung eines NetScaler ADM, wenn ein NetScaler ADC im transparenten Modus bereitgestellt wird:



So konfigurieren Sie die Datenerfassung auf einer NetScaler ADC Appliance mithilfe der Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Melden Sie sich bei einer Appliance an.
2. Geben Sie die ICA-Ports an, an denen die NetScaler ADC Appliance auf Datenverkehr wartet.

```
set ns param --icaPorts <port>...
```

Beispiel:

```
set ns param -icaPorts 2598 1494
```

> **Hinweis**
>
> - Mit diesem Befehl können Sie bis zu 10 Ports angeben.
> - Die Standardportnummer ist 2598. Sie können die Portnummer nach Bedarf ändern.

3. Fügen Sie NetScaler Insight Center als AppFlow-Collector auf der NetScaler ADC Appliance hinzu.

```
add appflow collector <name> -IPAddress <ip_addr>
```

Beispiel:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

> **Hinweis** Um die auf der NetScaler ADC Appliance konfigurierten AppFlow-Collector anzuzeigen, verwenden Sie den Befehl **show appflow collector**.

4. Erstellen Sie eine AppFlow Aktion, und ordnen Sie den Kollektor der Aktion zu.

```
add appflow action <name> -collectors <string> ...
```

Beispiel:

add AppFlow action act-collectors MyInsight

5. Erstellen Sie eine AppFlow Richtlinie, um die Regel zum Generieren des Datenverkehrs anzugeben.

```
add appflow policy <policyname> <rule> <action>
```

Beispiel:

```
add appflow policy pol true act
```

6. Binden Sie die AppFlow-Richtlinie an einen globalen Bindepunkt.

```
bind appflow global <policyname> <priority> -type <type>
```

Beispiel:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```


> **Hinweis**
>
> Der Wert des **Typs** muss ICA_REQ_OVERRIDE oder ICA_REQ_DEFAULT sein, damit er auf ICA-Verkehr angewendet wird.

7. Legen Sie den Wert des Parameters FlowRecordInterval für AppFlow auf 60 Sekunden fest.

```
set appflow param -flowRecordInterval 60
```

Beispiel:

```
set appflow param -flowRecordInterval 60
```

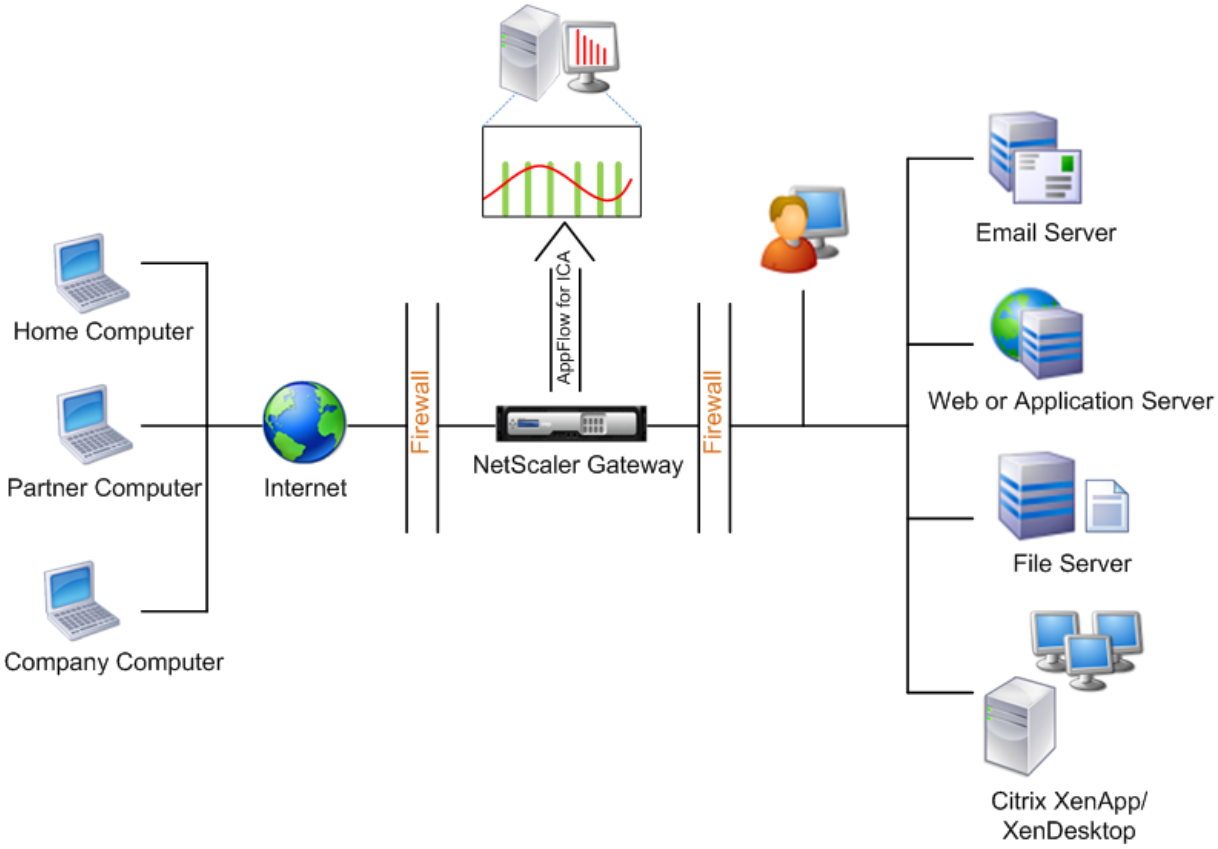
8. Speichern Sie die Konfiguration. Typ: `save ns config`
“‘

Datensammlung für NetScaler Gateway-Geräte im Single-Hop-Modus aktivieren

February 5, 2024

Wenn Sie NetScaler Gateway im Single-Hop-Modus bereitstellen, befindet es sich am Netzwerkrand. Die Gateway-Instanz stellt ICA-Proxy-Verbindungen zur Desktop-Bereitstellungsinfrastruktur bereit. Single-Hop ist das einfachste und gebräuchlichste Deployment. Der Single-Hop-Modus bietet Sicherheit, wenn ein externer Benutzer versucht, auf das interne Netzwerk in einer Organisation zuzugreifen. Im Single-Hop-Modus greifen Benutzer über ein virtuelles privates Netzwerk (VPN) auf die NetScaler ADC-Appliances zu.

Um mit dem Sammeln der Berichte zu beginnen, müssen Sie das NetScaler Gateway Gerät der NetScaler Application Delivery Management (ADM) -Bestandsliste hinzufügen und AppFlow auf ADM aktivieren.



So aktivieren Sie die AppFlow Funktion von ADM:

1. Navigieren Sie zu **Infrastruktur** > **Instanzen**, und wählen Sie die NetScaler ADC-Instanz aus, die Sie die Analyse aktivieren möchten.
2. Wählen Sie in der Liste **Aktion** die Option **Insight aktivieren/deaktivieren**aus.
3. Wählen Sie die **virtuellen VPN-Server** aus und klicken Sie auf **AppFlow aktivieren** .
4. Geben Sie in das Feld **Enable AppFlow** den Wert **true**ein und wählen Sie **ICA**aus.
5. Klicken Sie auf **OK**.

> **Hinweis**
>
> Wenn Sie AppFlow im Single-Hop-Modus aktivieren, werden die folgenden Befehle im Hintergrund ausgeführt. Diese Befehle werden hier explizit zur Fehlerbehebung angegeben.
>
> - `add appflow collector \<name\> -IPAddress \<ip\\_addr\>`
> - `add appflow action \<name\> -collectors \<string\>`
> - `set appflow param -flowRecordInterval \<secs\>`
> - `disable ns feature AppFlow`
> - `enable ns feature AppFlow`
> - `add appflow policy \<name\> \<rule\> \<expression\>`

- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

Virtuelle EUEM-Kanaldaten sind Teil von HDX Insight Daten, die NetScaler ADM von Gateway-Instanzen erhält. Der virtuelle EUEM-Kanal stellt die Daten über ICA-RTT bereit. Wenn der virtuelle EUEM-Kanal nicht aktiviert ist, werden die verbleibenden HDX Insight Daten weiterhin in NetScaler ADM angezeigt.

Datenerfassung zur Überwachung der im transparenten Modus bereitgestellten Citrix ADCs aktivieren

February 5, 2024

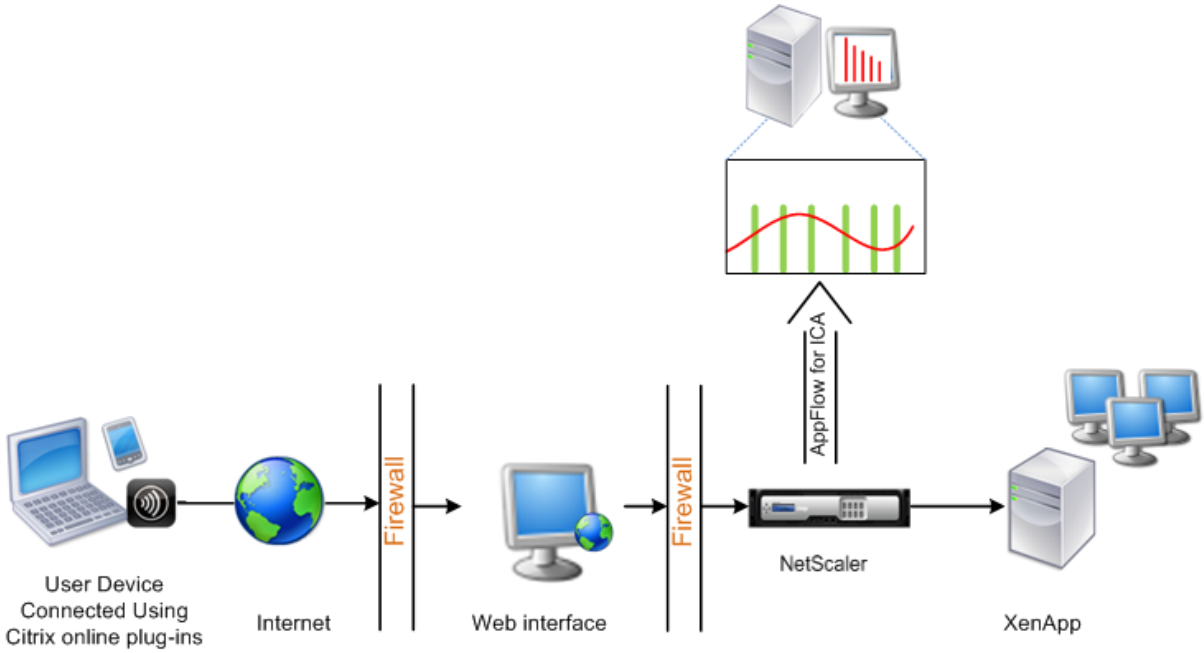
Wenn ein NetScaler ADC im transparenten Modus bereitgestellt wird, können die Clients direkt auf die Server zugreifen, ohne dass ein virtueller Server vorhanden ist. Wenn ein Citrix ADC im transparenten Modus in einer Citrix Virtual Apps and Desktops-Umgebung bereitgestellt wird, wird der ICA-Verkehr nicht über ein VPN übertragen.

Nachdem Sie NetScaler ADC zur NetScaler ADM Bestandsliste hinzugefügt haben, müssen Sie AppFlow für die Datensammlung aktivieren. Die Aktivierung der Datenerfassung hängt vom Gerät und vom Modus ab. In diesem Fall müssen Sie Citrix ADM als AppFlow-Collector auf jeder Citrix ADC-Instanz hinzufügen, und Sie müssen eine AppFlow-Richtlinie konfigurieren, um den gesamten oder einen bestimmten ICA-Verkehr zu sammeln, der durch die Appliance fließt.

Hinweis

- Sie können die Datenerfassung auf einem NetScaler ADC, der im transparenten Modus bereitgestellt wird, nicht mithilfe des NetScaler ADM Konfigurationsdienstprogramms aktivieren.
- Detaillierte Informationen zu den Befehlen und ihrer Verwendung finden Sie in der Befehlsreferenz .
- Informationen zu Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke .

Die folgende Abbildung zeigt die Netzwerkbereitstellung eines NetScaler ADM, wenn ein NetScaler ADC im transparenten Modus bereitgestellt wird:



So konfigurieren Sie die Datenerfassung auf einer NetScaler ADC Appliance mithilfe der Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Melden Sie sich bei einer Appliance an.
2. Geben Sie die ICA-Ports an, an denen die NetScaler ADC Appliance auf Datenverkehr wartet.

```
set ns param --icaPorts \<port\>...
<!--NeedCopy-->
```

Beispiel:

```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```

> **Hinweis**
>
> - Mit diesem Befehl können Sie bis zu 10 Ports angeben.
> - Die Standardportnummer ist 2598. Sie können die Portnummer nach Bedarf ändern.

3. Fügen Sie NetScaler Insight Center als AppFlow-Collector auf der NetScaler ADC-Instanz hinzu.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Beispiel:


```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> **Hinweis** Um die AppFlow-Collector anzuzeigen, die für die NetScaler ADC-Instanz konfiguriert sind, verwenden Sie den Befehl**show appflow collector**.

4. Erstellen Sie eine AppFlow Aktion, und ordnen Sie den Kollektor der Aktion zu.

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

Beispiel:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Erstellen Sie eine AppFlow Richtlinie, um die Regel zum Generieren des Datenverkehrs anzugeben.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Beispiel:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Binden Sie die AppFlow-Richtlinie an einen globalen Bindepunkt.

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

Beispiel:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Hinweis**
>
> Der Wert des **Typs** muss ICA_REQ_OVERRIDE oder ICA_REQ_DEFAULT sein, damit er auf ICA-Verkehr angewendet wird.

7. Legen Sie den Wert des Parameters FlowRecordInterval für AppFlow auf 60 Sekunden fest.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. Speichern Sie die Konfiguration.

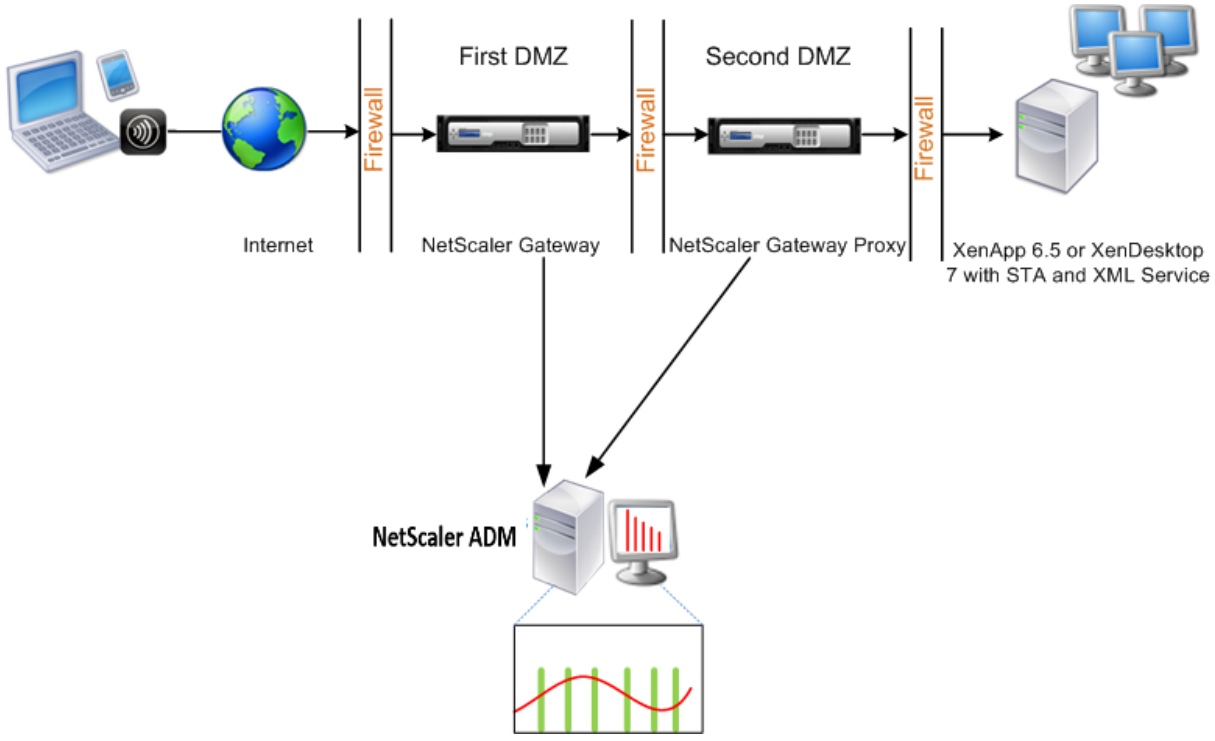

```
save ns config
<!--NeedCopy-->
```

Datensammlung für NetScaler Gateway-Geräte im Double-Hop-Modus aktivieren

February 5, 2024

Der Doppel-Hop-Modus von NetScaler Gateway bietet zusätzlichen Schutz für das interne Netzwerk einer Organisation, da ein Angreifer mehrere Sicherheitszonen oder entmilitarisierte Zonen (DMZ) durchdringen muss, um die Server im sicheren Netzwerk zu erreichen. Wenn Sie die Anzahl der Hops (NetScaler Gateway Geräte) analysieren möchten, über die die ICA-Verbindungen weitergeleitet werden, sowie die Details zur Latenz für jede TCP-Verbindung und wie sie mit der gesamten ICA-Latenz verglichen wird, die vom Client wahrgenommen wird, müssen Sie NetScaler ADM installieren, damit die NetScaler Gateway-Geräte diese wichtigen Statistiken zu berichten.

Abbildung 3. NetScaler ADM im Double-Hop-Modus bereitgestellt



NetScaler Gateway in der ersten DMZ verarbeitet Benutzerverbindungen und führt die Sicherheitsfunktionen eines SSL-VPN aus. Dieses NetScaler Gateway verschlüsselt Benutzerverbindungen, bestimmt, wie die Benutzer authentifiziert werden, und steuert den Zugriff auf die Server im internen

Netzwerk.

Das NetScaler Gateway in der zweiten DMZ dient als NetScaler Gateway-Proxygerät. Dieses NetScaler Gateway ermöglicht es dem ICA-Datenverkehr, die zweite DMZ zu durchqueren, um Benutzerverbindungen zur Serverfarm herzustellen.

Das NetScaler ADM kann entweder im Subnetz der NetScaler Gateway-Appliance in der ersten DMZ oder im Subnetz des zweiten DMZ der NetScaler Gateway-Appliance bereitgestellt werden. Im obigen Bild werden NetScaler ADM und NetScaler Gateway in der ersten DMZ im selben Subnetz bereitgestellt.

Im Double-Hop-Modus sammelt NetScaler ADM TCP-Datensätze von einer Appliance und ICA-Einträge von der anderen Appliance. Nachdem Sie die NetScaler Gateway-Appliances zum NetScaler ADM-Bestand hinzugefügt und die Datenerfassung aktiviert haben, exportiert jede Appliance die Berichte, indem sie die Hop-Anzahl und die Verbindungsketten-ID verfolgt.

Damit NetScaler ADM identifiziert, welche Appliance Datensätze exportiert, wird jede Appliance mit einer Hop-Anzahl angegeben, und jede Verbindung wird mit einer Verbindungsketten-ID angegeben. Die Hop-Anzahl gibt die Anzahl der NetScaler Gateway-Appliances an, durch die der Datenverkehr von einem Client zu den Servern fließt. Die Verbindungsketten-ID stellt die End-to-End-Verbindungen zwischen dem Client und dem Server dar.

NetScaler ADM verwendet die Hop-Anzahl und die Verbindungsketten-ID, um die Daten der beiden NetScaler Gateway Geräte miteinander zu verknüpfen und die Berichte zu generieren.

Um NetScaler Gateway Geräte zu überwachen, die in diesem Modus bereitgestellt werden, müssen Sie zuerst NetScaler Gateway zur NetScaler ADM Bestandsliste hinzufügen, AppFlow auf NetScaler ADM aktivieren und dann die Berichte auf dem NetScaler ADM-Dashboard anzeigen.

Aktivieren der Datenerfassung auf NetScaler ADM

Wenn Sie NetScaler ADM aktivieren, um die ICA-Details von beiden Appliances zu erfassen, sind die erfassten Details redundant. Das ist, dass beide Appliances die gleichen Metriken melden. Um diese Situation zu umgehen, müssen Sie AppFlow für TCP auf einem der ersten NetScaler Gateway-Appliances und dann AppFlow für ICA auf dem zweiten Gerät aktivieren. Auf diese Weise exportiert eine der Appliances ICA-AppFlow Datensätze, und die andere Appliance exportiert TCP-AppFlow-Datensätze. Dies spart auch die Verarbeitungszeit beim Analysieren des ICA-Datenverkehrs.

So aktivieren Sie die AppFlow Funktion von NetScaler ADM:

1. Navigieren Sie zu **Infrastruktur > Instanzen** und wählen Sie die NetScaler ADC-Instanz aus, für die Sie Analysen aktivieren möchten.
2. Wählen Sie in der Liste **Aktion** die Option **Insight aktivieren/deaktivieren**aus.
3. Wählen Sie die virtuellen VPN-Server aus und klicken Sie auf **AppFlow aktivieren**.

4. Geben **Sie im Feld Enable AppFlow** den **Wert true** ein, und wählen Sie **ICA/TCP** für ICA-Verkehr einen TCP-Verkehr aus.

   > **Hinweis**
   >
   > Wenn die AppFlow-Protokollierung für die Dienste oder Dienstgruppen auf der NetScaler ADC Appliance nicht aktiviert ist, zeigt das NetScaler ADM Dashboard die Datensätze nicht an, selbst wenn in der Spalte Insight Aktiviert angezeigt wird.

5. Klicken Sie auf **OK**.

Konfigurieren von NetScaler Gateway-Appliances zum Expor

Nach der Installation der NetScaler Gateway Geräte müssen Sie die folgenden Einstellungen auf den NetScaler Gateway-Geräten konfigurieren, um die Berichte in NetScaler ADM zu exportieren:

- Konfigurieren Sie virtuelle Server der NetScaler Gateway-Appliances in der ersten und zweiten DMZ, um miteinander zu kommunizieren.
- Binden Sie den virtuellen NetScaler Gateway -Server in der zweiten DMZ an den virtuellen NetScaler Gateway-Server in der ersten DMZ.
- Aktivieren Sie den Double-Hop auf dem NetScaler Gateway in der zweiten DMZ.
- Deaktivieren Sie die Authentifizierung auf dem virtuellen NetScaler Gateway -Server in der zweiten DMZ.
- Aktivieren Sie eine der NetScaler Gateway-Appliances, um ICA-Datensätze zu exportieren
- Aktivieren Sie die andere NetScaler Gateway-Appliance, um TCP-Datensätze zu exportieren:
- Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway Geräten.

Konfigurieren Sie NetScaler Gateway mit der Befehlszeilenschnittstelle:

1. Konfigurieren Sie den virtuellen NetScaler Gateway -Server in der ersten DMZ für die Kommunikation mit dem virtuellen NetScaler Gateway-Server in der zweiten DMZ.

---

add vpn nextHopServer [**-secure**(ON OFF)] [**-imgGifToPng**] …

```
1 add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
2 <!--NeedCopy-->
```

2. Binden Sie den virtuellen NetScaler Gateway -Server in der zweiten DMZ an den virtuellen NetScaler Gateway-Server in der ersten DMZ. Führen Sie den folgenden Befehl auf dem NetScaler Gateway in der ersten DMZ aus:

   bind vpn vserver <name> **-nextHopServer** <name>


```
bind vpn vserver vs1 -nextHopServer nh1
<!--NeedCopy-->
```

3. Aktivieren Sie Double-Hop und AppFlow auf dem NetScaler Gateway in der zweiten DMZ.

set vpn vserver [**- doubleHop** (ENABLED DISABLED)] [**- appflowLog** (ENABLED DISABLED)]

```
set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
<!--NeedCopy-->
```

4. Deaktivieren Sie die Authentifizierung auf dem virtuellen NetScaler Gateway -Server in der zweiten DMZ.

set vpn vserver [**-authentication** (ON OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. Aktivieren Sie eines der NetScaler Gateway Geräte zum Exportieren von TCP-Datensätzen.

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```

6. Aktivieren Sie das andere NetScaler Gateway Gerät zum Exportieren von ICA-Datensätzen:

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA_REQUEST
<!--NeedCopy-->
```

7. Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway Geräten:

set appFlow param [**-connectionChaining** (ENABLED DISABLED)]

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```


Konfiguration von Citrix Gateway mit dem Konfigurationsdienstprogramm:

1. Konfigurieren Sie das NetScaler Gateway in der ersten DMZ für die Kommunikation mit dem NetScaler Gateway in der zweiten DMZ, und binden Sie das NetScaler Gateway in der zweiten DMZ an das NetScaler Gateway in der ersten DMZ.

    a) Erweitern Sie auf der Registerkarte**KonfigurationCitrix Gateway**, und klicken Sie auf**Virtuelle Server**.

    b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe "Erweitert"die Option **Published Applications**.

    c) Klicken Sie auf**Next Hop Server**, und binden Sie einen nächsten Hop-Server an das zweite NetScaler Gateway Gerät.

2. Aktivieren Sie den Double-Hop auf dem NetScaler Gateway in der zweiten DMZ.

    a) Erweitern Sie auf der Registerkarte**KonfigurationCitrix Gateway**, und klicken Sie auf**Virtuelle Server**.

    b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und klicken Sie in der Gruppe**Grundeinstellungen** auf das Symbol Bearbeiten.

    c) Erweitern Sie **More**, wählen Sie **Double Hop**, und klicken Sie auf**OK**.

3. Deaktivieren Sie die Authentifizierung auf dem virtuellen Server auf dem NetScaler Gateway in der zweiten DMZ.

    a) Erweitern Sie auf der Registerkarte **Konfiguration Citrix Gateway** und klicken Sie auf **Virtuelle Server** .

    b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und klicken Sie in der Gruppe**Grundeinstellungen** auf das Symbol Bearbeiten.

    c) Erweitern Sie**Mehr**, und deaktivieren Sie **Authentifizierung aktivieren**.

4. Aktivieren Sie eines der NetScaler Gateway Geräte zum Exportieren von TCP-Datensätzen.

    a) Erweitern Sie auf der Registerkarte **Konfiguration Citrix Gateway** und klicken Sie auf **Virtuelle Server** .

    b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe Erweitert die Option Richtlinien.

    c) Klicken Sie auf das Symbol +, und**wählen Sie in der Liste Choose policy** die Option**AppFlow**aus, und**wählen Sie in der Dropdownliste Typ**auswählen die Option**Andere TCP-Anforderung**aus.

    d) Klicken Sie auf **Weiter**.

e) Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Schließen**.

5. Aktivieren Sie das andere NetScaler Gateway Gerät zum Exportieren von ICA-Datensätzen:

   a) Erweitern Sie auf der Registerkarte **Konfiguration Citrix Gateway** und klicken Sie auf **Virtuelle Server** .

   b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe**Erweitert** die Option**Richtlinien**.

   c) Klicken Sie auf das Symbol + und wählen Sie in der Dropdownliste **Richtlinie auswählen** die Option **AppFlow** aus, und wählen Sie in der Dropdownliste "Typ wählen"die Option **Andere TCP-Anforderung** aus.

   d) Klicken Sie auf **Weiter**.

   e) Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Schließen**.

6. Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway Geräten.

   a) Navigieren Sie auf der Registerkarte**Konfiguration** zu **System > Appflow**.

   b) Klicken Sie im rechten Bereich in der Gruppe**Einstellungen** auf **Appflow-Einstellungen ändern**.

   c) Wählen Sie **Verbindungsverkettung** aus, und klicken Sie auf **OK**.

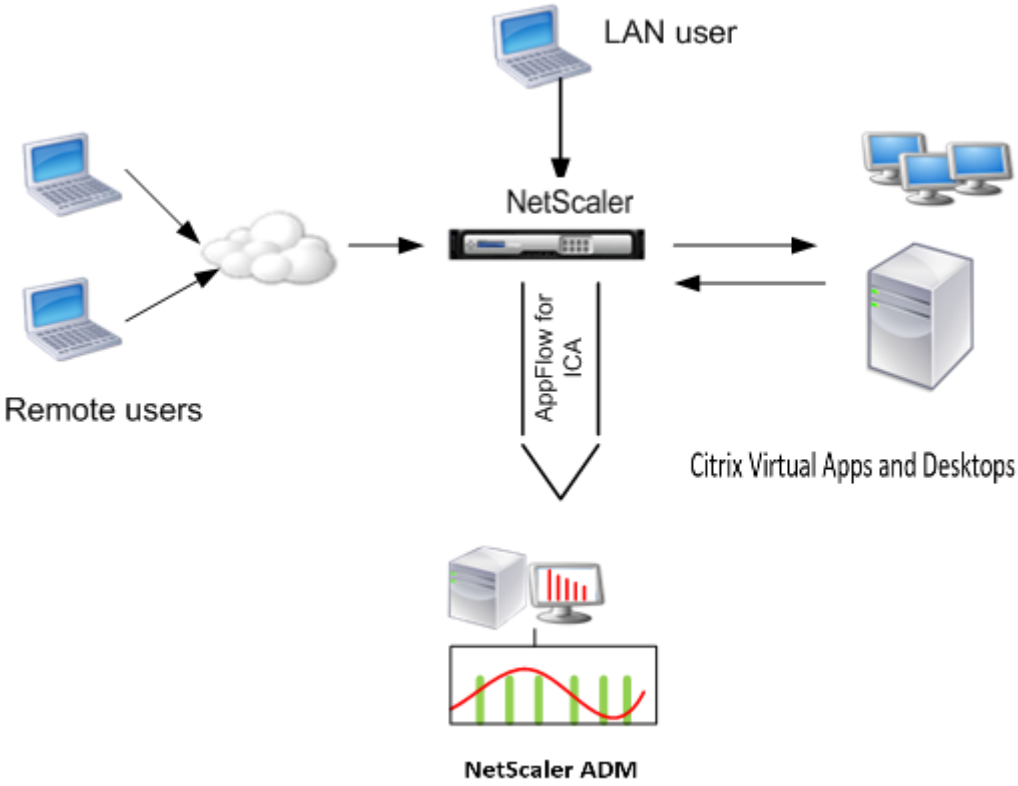
Datenerfassung zur Überwachung der im LAN-Benutzermodus bereitgestellten Citrix ADCs aktivieren

February 5, 2024

Externe Benutzer, die auf Citrix Virtual App- oder Desktop-Anwendungen zugreifen, müssen sich am Citrix Gateway authentifizieren. Interne Benutzer müssen jedoch möglicherweise nicht an NetScaler Gateway weitergeleitet werden. Außerdem muss der Administrator in einer Bereitstellung im transparenten Modus die Routingrichtlinien manuell anwenden, damit die Anforderungen an die NetScaler ADC Appliance umgeleitet werden.

Um diese Herausforderungen zu meistern und LAN-Benutzer direkt mit Citrix Virtual Apps and Desktops s-Anwendungen zu verbinden, können Sie das NetScaler ADC Gerät im LAN-Benutzermodus bereitstellen, indem Sie einen virtuellen Cacheumleitungsserver konfigurieren, der als SOCKS-Proxy auf dem NetScaler Gateway Gerät fungiert.

Figure 4. NetScaler ADM im LAN-Benutzermodus bereitgestellt



Hinweis: NetScaler ADM und NetScaler Gateway Gerät befinden sich im selben Subnetz.

Um die in diesem Modus bereitgestellten NetScaler ADC-Appliances zu überwachen, fügen Sie zuerst die NetScaler ADC Appliance zum NetScaler Insight-Inventar hinzu, aktivieren Sie AppFlow und sehen Sie sich dann die Berichte im Dashboard an.

Nachdem Sie die NetScaler ADC Appliance zur NetScaler ADM Bestandsliste hinzugefügt haben, müssen Sie AppFlow für die Datenerfassung aktivieren.

> **Hinweis**
>
> - Sie können die Datenerfassung auf einem NetScaler ADC, der im LAN-Benutzermodus bereitgestellt wird, nicht mithilfe des NetScaler ADM Konfigurationsdienstprogramms aktivieren.
> - Detaillierte Informationen zu den Befehlen und ihrer Verwendung finden Sie in der Befehlsreferenz .
> - Informationen zu Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke .

So konfigurieren Sie die Datenerfassung auf einer NetScaler ADC Appliance mithilfe der Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Melden Sie sich bei einer Appliance an.

2. Fügen Sie einen virtuellen Forward-Proxy-Cache-Umleitungsserver mit Proxy-IP und Port hinzu, und geben Sie den Diensttyp als HDX an.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

Beispiel:

```
add cr vserver cr1 HDX 10.12.2.2 443 – cacheType FORWARD –
   cltTimeout 180
<!--NeedCopy-->
```

> **Hinweis:** Wenn Sie mit einem NetScaler Gateway -Gerät auf das LAN-Netzwerk zugreifen, fügen Sie eine Aktion hinzu, die von einer Richtlinie angewendet wird, die dem VPN-Datenverkehr entspricht.

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]

add vpn trafficPolicy** \<name\> \<rule\> \<action\>
<!--NeedCopy-->
```

Beispiel:

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. Fügen Sie NetScaler ADM als AppFlow Collector auf der NetScaler ADC Appliance hinzu.

```
add appflow collector** \<name\> \*\*-IPAddress\*\* \\<ip\\_addr
   \\>
<!--NeedCopy-->
```

Beispiel:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. Erstellen Sie eine AppFlow Aktion, und ordnen Sie den Kollektor der Aktion zu.

```
add appflow action** \<name\> \*\*-collectors\*\* \<string\> ...
<!--NeedCopy-->
```

Beispiel:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```


5. Erstellen Sie eine AppFlow Richtlinie, um die Regel zum Generieren des Datenverkehrs anzugeben.

```
add appflow policy** \<policyname\> \<rule\> \<action\>
<!--NeedCopy-->
```

Beispiel:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Binden Sie die AppFlow-Richtlinie an einen globalen Bindepunkt.

```
bind appflow global** \<policyname\> \<priority\> \*\*-type\*\* \<
   type\>
<!--NeedCopy-->
```

Beispiel:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Hinweis**
>
> Der Wert vom Typ muss ICA_REQ_OVERRIDE oder ICA_REQ_DEFAULT sein, um auf ICA-Datenverkehr anzuwenden.

7. Legen Sie den Wert des Parameters FlowRecordInterval für AppFlow auf 60 Sekunden fest.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

Beispiel:

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. Speichern Sie die Konfiguration.

```
save ns config
<!--NeedCopy-->
```

Schwellenwerte erstellen und Warnungen für HDX Insight konfigurieren

February 5, 2024

Mit HDX Insight on Citrix Application Delivery Management (ADM) können Sie den HDX-Verkehr überwachen, der durch Citrix ADC-Instanzen fließt. Mit Citrix ADM können Sie Schwellenwerte

für verschiedene Leistungsindikatoren festlegen, die zur Überwachung des Insight-Datenverkehrs verwendet werden. Sie können auch Regeln konfigurieren und Warnungen in Citrix ADM erstellen.

Der HDX-Datenverkehrstyp ist mit verschiedenen Entitäten wie Anwendungen, Desktops, Gateways, Lizenzen und Benutzern verknüpft. Jede Entität kann verschiedene Metriken enthalten, die ihnen zugeordnet sind. Beispielsweise ist die Anwendungseinheit mit verschiedenen Treffern, der von der Anwendung verbrauchten Bandbreite und der Reaktionszeit des Servers verknüpft. Eine Benutzerentität kann WAN-Latenz, DC-Latenz, ICA RTT und Bandbreite zugeordnet werden, die von einem Benutzer belegt wird.

Die Schwellenwertverwaltung für HDX Insight in Citrix ADM ermöglichte es Ihnen, proaktiv Regeln zu erstellen und Warnungen zu konfigurieren, wenn die festgelegten Schwellenwerte überschritten werden. Diese Schwellenwertverwaltung wurde nun erweitert, um eine Gruppe von Schwellenwertregeln zu konfigurieren. Sie können jetzt die Gruppe anstelle einzelner Regeln überwachen. Eine Schwellenwertregelgruppe umfasst eine oder mehrere benutzerdefinierte Schwellenwertregeln für Metriken, die aus Entitäten wie Benutzern, Anwendungen und Desktops ausgewählt wurden. Jede Regel wird mit einem erwarteten Wert überwacht, den Sie beim Erstellen der Regel eingeben. Im Falle einer Benutzerentität kann die Schwellengruppe auch mit einer Geolocation verknüpft werden.

Eine Warnung wird nur dann auf Citrix ADM generiert, wenn alle Regeln in der konfigurierten Schwellenwertgruppe verletzt werden. Beispielsweise können Sie eine Anwendung anhand der Gesamtzahl der Sitzungsstarts und auch der Anzahl der Anwendungsstarts als eine Schwellenwertgruppe überwachen. Eine Warnung wird nur generiert, wenn beide Regeln verletzt werden. Auf diese Weise können Sie realistischere Schwellenwerte für eine Entität festlegen.

Einige Beispiele sind wie folgt aufgeführt:

- Schwellenwertregel1: ICA RTT (Metrik) für Benutzer (Entität) muss <= 100 ms sein
- Schwellenwertregel2: WAN-Latenz (Metrik) für Benutzer (Entität) muss <= 100 ms sein

Ein Beispiel für eine Schwellenwertgruppe kann sein: {Schwellenwertregel 1 + Schwellenwertregel 2}

Um eine Regel zu erstellen, müssen Sie zuerst die Entität auswählen, die Sie überwachen möchten. Wählen Sie dann beim Erstellen einer Regel eine Metrik aus. Sie können z. B. Anwendungsentität auswählen und dann Gesamte Sitzungsstartanzahl oder App-Startanzahl auswählen. Sie können für jede Kombination aus einer Entität und einer Metrik eine Regel erstellen. Verwenden Sie die bereitgestellten Komparatoren (>, <, >= und <=) und geben Sie einen Schwellenwert für jede Metrik ein.

> **Hinweis**
>
> Wenn Sie nicht mehrere Entitäten in einer einzelnen Gruppe überwachen möchten, müssen Sie für jede Entität eine separate Schwellenwertregelgruppe erstellen.

Wenn der Wert eines Zählers den Wert eines Schwellenwerts überschreitet, generiert Citrix ADM ein

Ereignis, das auf eine Schwellenwertverletzung hinweist, und für jedes Ereignis wird eine Warnung erstellt.

Sie müssen konfigurieren, wie Sie die Warnung erhalten. Sie können die Anzeige der Warnung auf Citrix ADM aktivieren und/oder die Warnung als E-Mail oder SMS auf Ihrem Mobilgerät erhalten. Für die letzten beiden Aktionen müssen Sie den E-Mail-Server oder den SMS-Server auf Citrix ADM konfigurieren.

Schwellenwertgruppen können auch an Geolocations gebunden werden, um die geospezifische Überwachung der Benutzerentität zu ermöglichen.

Beispiele für Anwendungsfälle

ABC Inc. ist ein globales Unternehmen und hat Niederlassungen in über 50 Ländern. Das Unternehmen verfügt über zwei Rechenzentren, eines in Singapur und eines in Kalifornien, in denen Citrix Virtual Apps and Desktops gehostet werden. Mitarbeiter des Unternehmens greifen über Citrix Gateway und Citrix GSLB-basierte Umleitung auf Citrix Virtual Apps and Desktops auf der ganzen Welt zu. Eric, der Citrix Virtual Apps and Desktops Admin für ABC Inc. möchte die Benutzererfahrung für alle ihre Büros verfolgen, um die Apps und die Desktop-Bereitstellung für den Zugriff von überall und jederzeit zu optimieren. Eric möchte auch die User-Experience-Metriken wie ICA-RTTs und Latenzen überprüfen und etwaige Abweichungen proaktiv erhöhen.

Die Anwender von ABC Inc. haben eine verteilte Präsenz. Einige Benutzer befinden sich in der Nähe des Rechenzentrums, während sich einige wenige weiter vom Rechenzentrum entfernt befinden. Da die Benutzerbasis breit verteilt ist, variieren auch die Metriken und die entsprechenden Schwellenwerte zwischen diesen Standorten. Beispielsweise kann der ICA-RTT für einen Standort in der Nähe des Rechenzentrums 5 - 10 ms betragen, während der ICA-RTT für einen Remote-Standort etwa 100 ms betragen kann.

Mit der Verwaltung von Schwellenwertregelgruppen für HDX Insight kann Eric geospezifische Schwellenwertregelgruppen für jeden Standort festlegen und per E-Mail oder SMS bei Verstößen pro Gebiet gewarnt werden. Eric ist auch in der Lage, die Verfolgung mehrerer Metriken innerhalb einer Schwellenwertregelgruppe zu kombinieren und die Grundursache auf Kapazitätsprobleme einzugrenzen, falls vorhanden. Eric ist jetzt in der Lage, jede Abweichung proaktiv zu verfolgen, ohne sich Gedanken über die Komplexität machen zu müssen, die mit der manuellen Überprüfung aller Portfoliokennzahlen von Citrix Virtual Apps and Desktops verbunden ist.

So erstellen Sie eine Schwellenwertregelgruppe und konfigurieren Warnungen für HDX Insight mit Citrix ADM:

1. Navigieren Sie in Citrix ADM zu**Analytics** > **Einstellungen** > **Schwellenwerte**. Klicken Sie auf der Seite **Schwellenwerte**, die geöffnet wird, auf **Hinzufügen**.
2. Geben Sie auf der Seite **Schwellenwerte und Warnungen erstellen** die folgenden Details an:

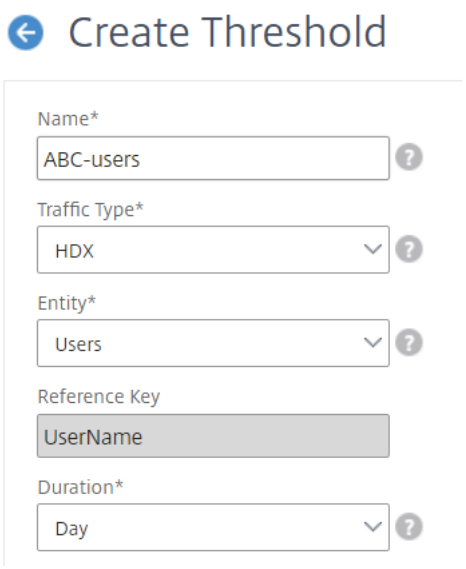
a) **Name**. Geben Sie einen Namen zum Erstellen eines Ereignisses ein, für das Citrix ADM eine Warnung generiert.

b) **Art des Datenverkehrs**. Wählen Sie im Listenfeld HDX aus.

c) **Entität**. Wählen Sie im Listenfeld die Kategorie oder den Ressourcentyp aus. Die Entitäten unterscheiden sich für jeden Datenverkehrstyp, den Sie zuvor ausgewählt haben.

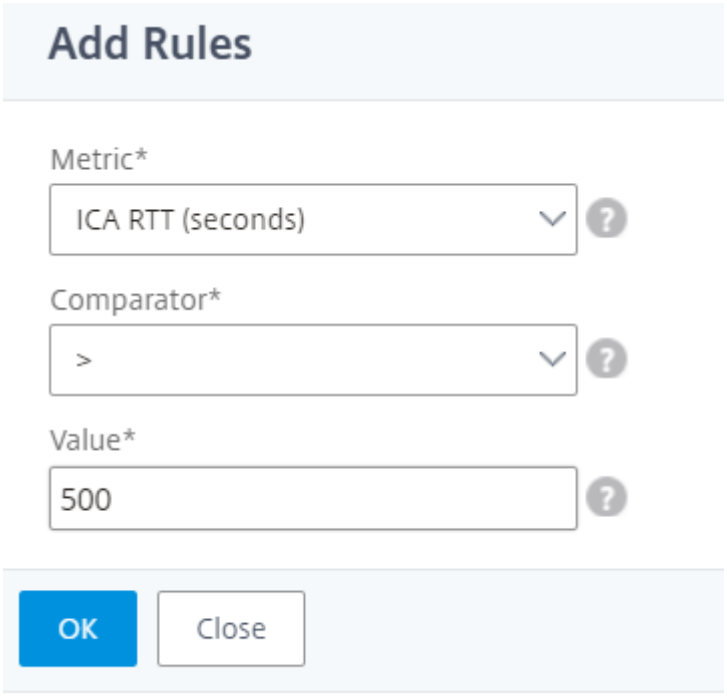
d) **Referenz-Schlüssel**. Basierend auf dem Traffic-Typ und der Entität, die Sie ausgewählt haben, wird automatisch ein Referenzschlüssel generiert.

e) **Dauer**. Wählen Sie im Listenfeld das Zeitintervall aus, für das Sie die Entität überwachen möchten. Sie können die Entitäten für eine Stunde, für einen Tag oder für eine Woche überwachen.

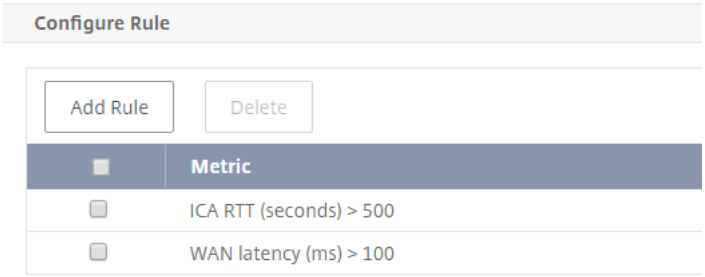


3. Erstellen von Schwellenwertregelgruppen für alle Entitäten:

   Für HDX-Verkehr müssen Sie eine Regel erstellen, indem Sie auf **Regel hinzufügen klicken.**Geben Sie die Werte in das Popup-Fenster **Regeln hinzufügen** ein, das geöffnet wird.

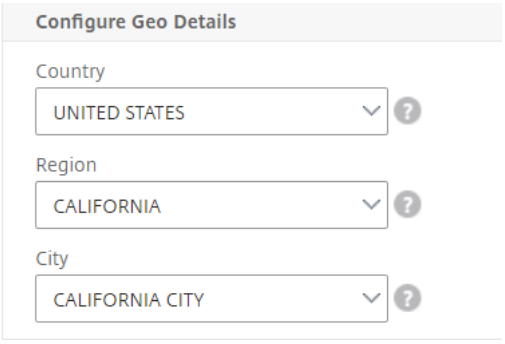


Sie können mehrere Regeln erstellen, um jede Entität zu überwachen. Wenn Sie mehrere Regeln in einer einzigen Gruppe erstellen, können Sie die Entitäten als Gruppe von Schwellenwertregeln anstelle einzelner Regeln überwachen. Klicken Sie auf **OK**, um das Fenster zu schließen.



4. Konfigurieren von Geolocation-Tagging für Benutzerentität

   Optional können Sie im Abschnitt **Geo-Details konfigurieren** eine standortbasierte Warnung für die Benutzerentität erstellen. Die folgende Abbildung zeigt ein Beispiel für die Erstellung eines Geolocation-basierten Tagging zur Überwachung der WAN-Latenzleistung für Benutzer an der Westküste der Vereinigten Staaten.



5. Klicken Sie auf **Schwellenwerte aktivieren**, damit Citrix ADM mit der Überwachung der Entitäten beginnen kann.
6. Konfigurieren Sie optional Aktionen wie E-Mail-Benachrichtigungen und SMS-Benachrichtigungen.
7. Klicken Sie auf **Erstellen**, um eine Schwellenregelgruppe zu erstellen.

Anzeigen von HDX Insight-Berichten und -Metriken

February 5, 2024

HDX Insight bietet vollständige Transparenz der Berichte und Metriken im Zusammenhang mit HDX-Datenverkehr auf Ihren NetScaler ADC-Instanzen.

Sie können die HDX-Metriken für jede ausgewählte Entität anzeigen. Die Ansichten umfassen die folgenden Kategorien von Entitäten:

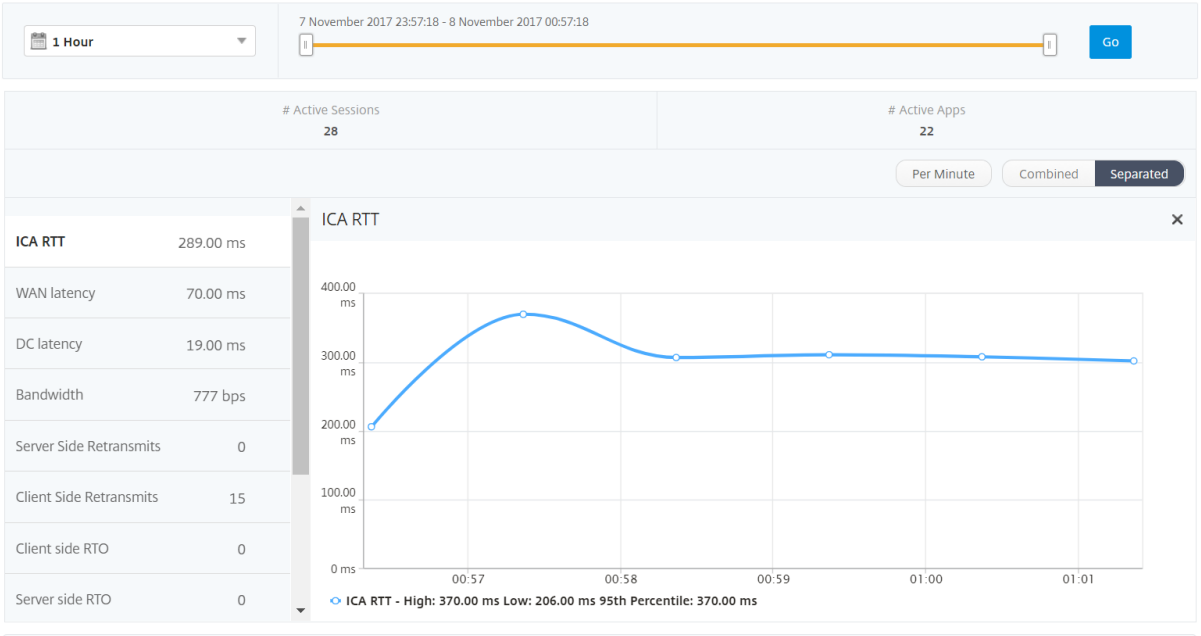
- **Benutzer**: Zeigt die Berichte für alle Benutzer an, die innerhalb des ausgewählten Zeitintervalls auf die Citrix Virtual App oder den Desktop zugreifen.
- **Anwendungen**: Zeigt die Berichte für die Gesamtzahl der Anwendungen und alle zugehörigen relevanten Informationen an, z. B. die Gesamtzahl der Starts der Anwendungen innerhalb des angegebenen Zeitintervalls.
- **Instanzen**: Zeigt die Berichte auf den NetScaler ADC Instanzen an, die als Gateways für eingehenden Datenverkehr fungieren.
- **Desktops**: Zeigt die Berichte für die im ausgewählten Zeitraum verwendeten Desktops an.
- **Lizenzen**: Zeigt die Berichte für die Gesamtzahl der innerhalb des angegebenen Zeitfensters verwendeten SSL-VPN-Lizenzen an.

> **Hinweis**
>
> Der Wert “Lizenzen”gilt nicht für Citrix SD-WAN Appliances.

Berichte und Metriken der Benutzeransicht

Die Berichte und Metriken in dieser Ansicht werden pro Citrix Virtual Apps und Desktop-Benutzer angezeigt.

Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**.



Berichte und Metriken der Benutzeransicht bestehen aus den folgenden Abschnitten:

- Zusammenfassende Ansicht
- Ansicht pro Benutzer
- Session-Ansicht pro Benutzer

Übersichtsansicht

In der Zusammenfassungsansicht werden die Berichte für alle Benutzer angezeigt, die sich während der ausgewählten Zeitleiste angemeldet haben. Alle Metriken/Berichte in dieser Ansicht zeigen die ihnen entsprechenden Werte für den ausgewählten Zeitraum an, sofern nicht anders angegeben.

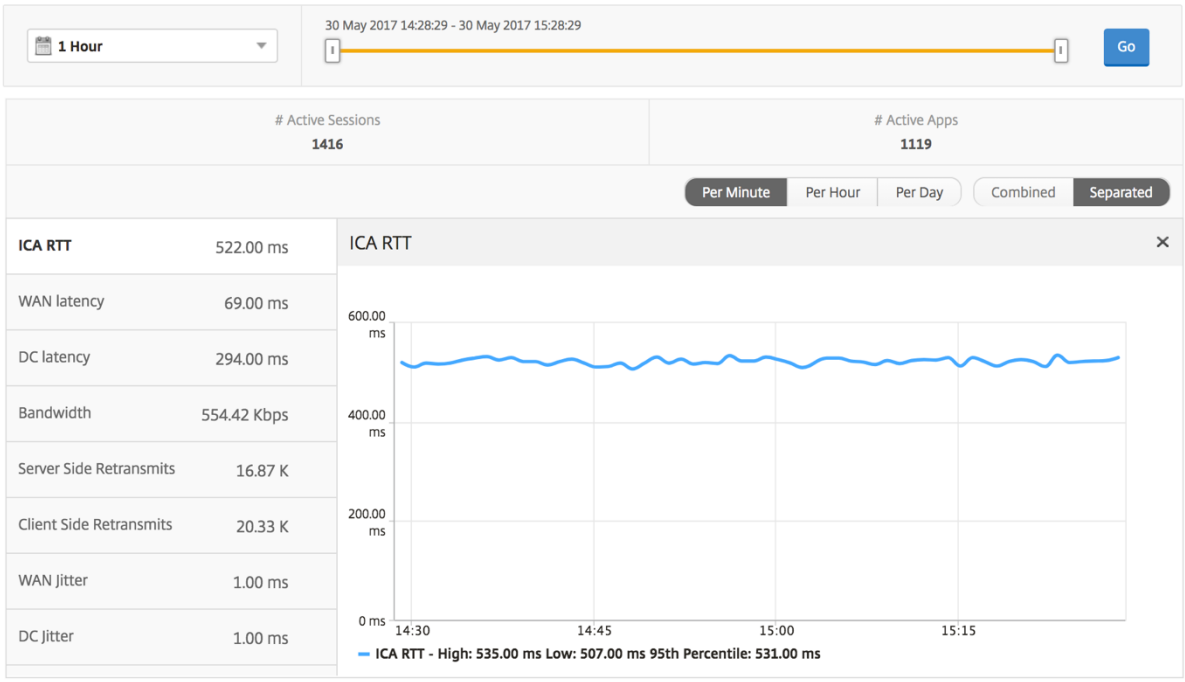
So ändern Sie den ausgewählten Zeitraum:

1. Verwenden Sie die Zeitraumeliste oder den Zeitschieberegler, um das gewünschte Zeitintervall einzustellen.
2. Klicken Sie auf **Go**.

Liniendiagramm

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.

Metriken	Beschreibung
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.

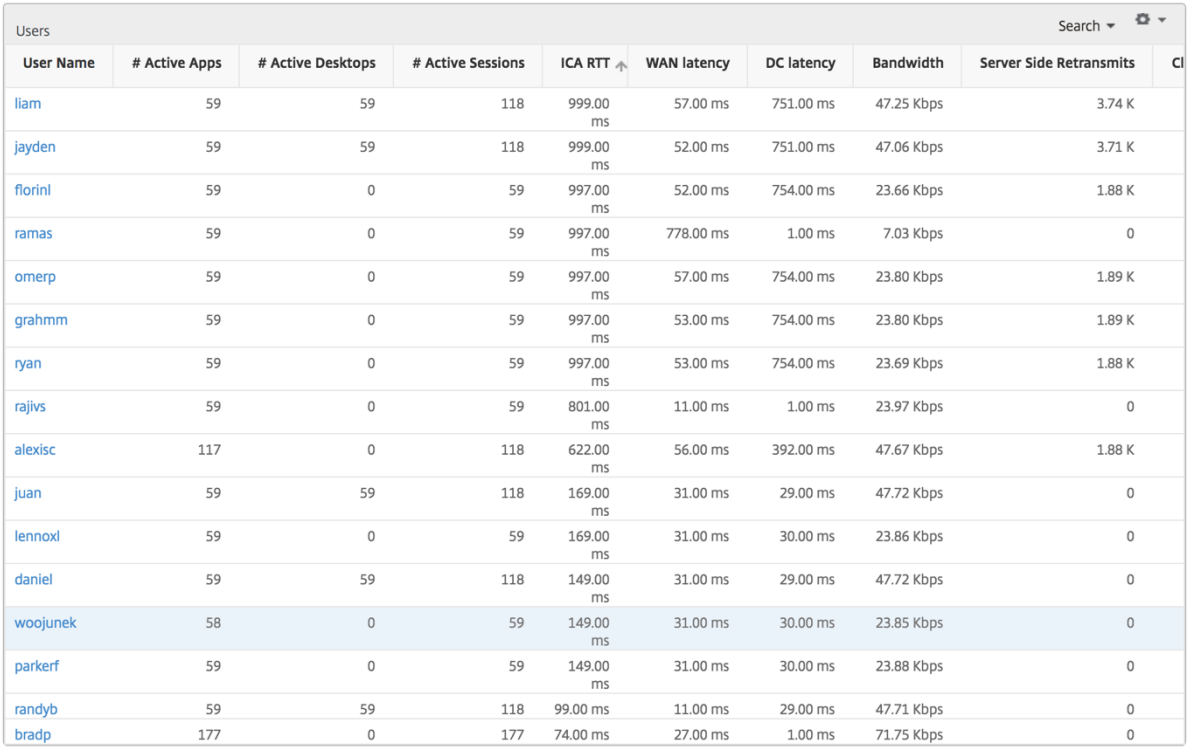


Bericht "Benutzerzusammenfassung" Im Folgenden finden Sie die Metriken, die für diesen Bericht spezifisch sind.

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App and Desktop-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.

Metriken	Beschreibung
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
App-Starts insgesamt	Gesamtzahl der Apps, die vom Benutzer während des ausgewählten Zeitraums gestartet wurden.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.

Metriken	Beschreibung
Aktive Desktops	Gesamtzahl der aktiven Citrix Virtual Desktops in einem bestimmten Zeitintervall.

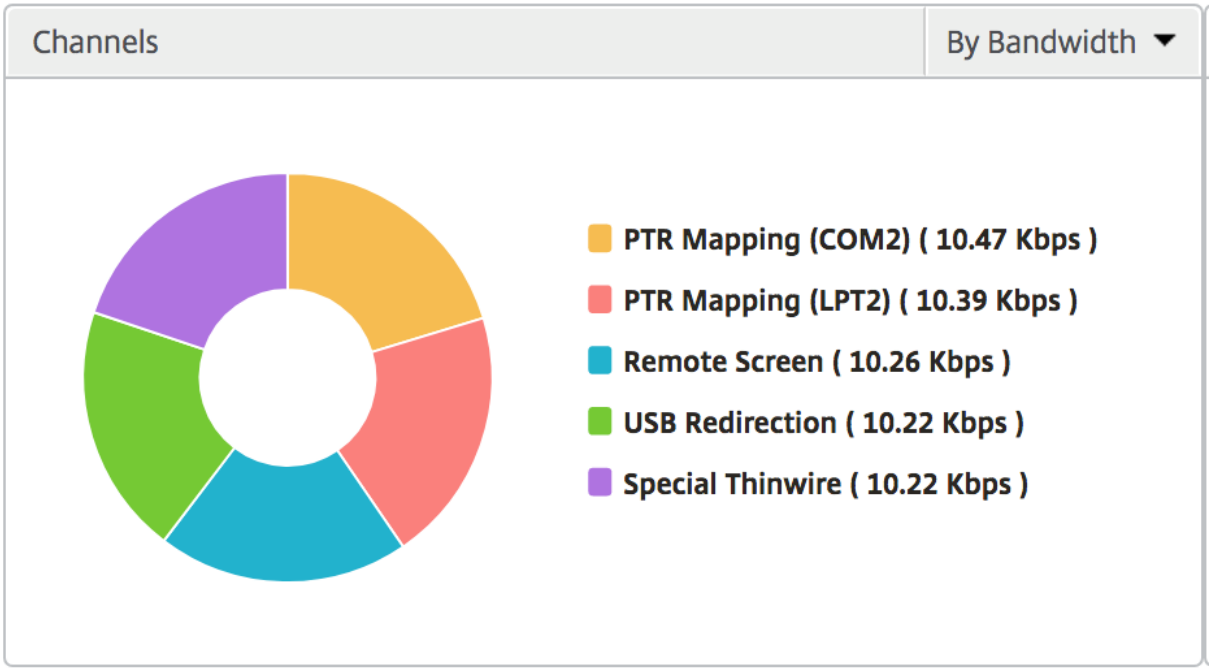


Users

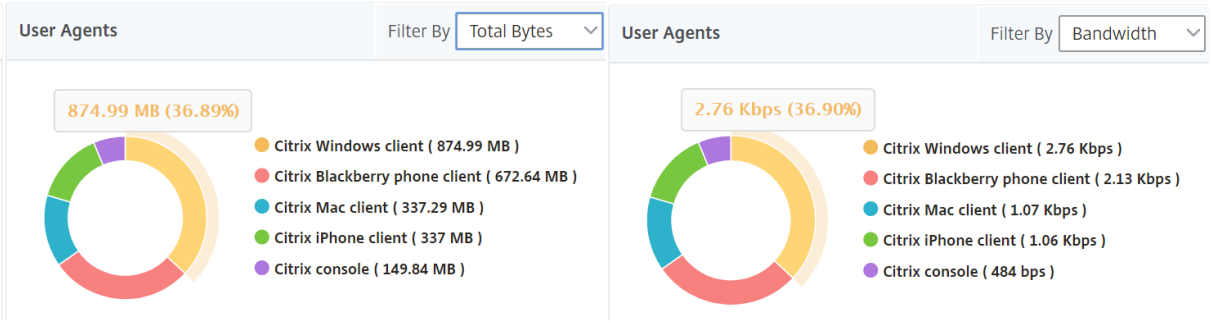
Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

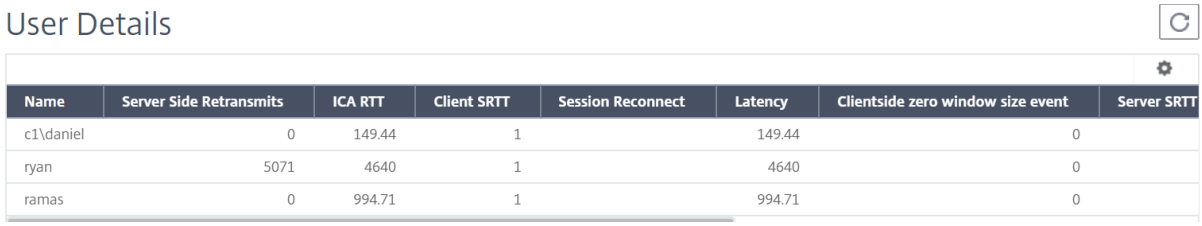
Kanäle Kanäle stellen die Gesamtbandbreite oder die Gesamtzahl der von jedem virtuellen ICA-Kanal verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Benutzer-Agenten Benutzeragenten stellen die gesamte Bandbreite/Gesamt-Bytes dar, die von jedem Empfängerclient in Form eines Ringdiagramms verbraucht werden. Jedes farbige Segment im Diagramm repräsentiert einen Empfängerclient. Die Länge des Segments hängt von der Anzahl der Benutzer ab, die ihre Anwendungen auf diesem Empfängerclient starten. Sie können die Metriken auch nach Bandbreite oder Gesamtzahl der Bytes sortieren.



Klicken Sie auf jedes Segment, um die Details der Benutzer anzuzeigen, die diesen Receiver-Client verwenden.



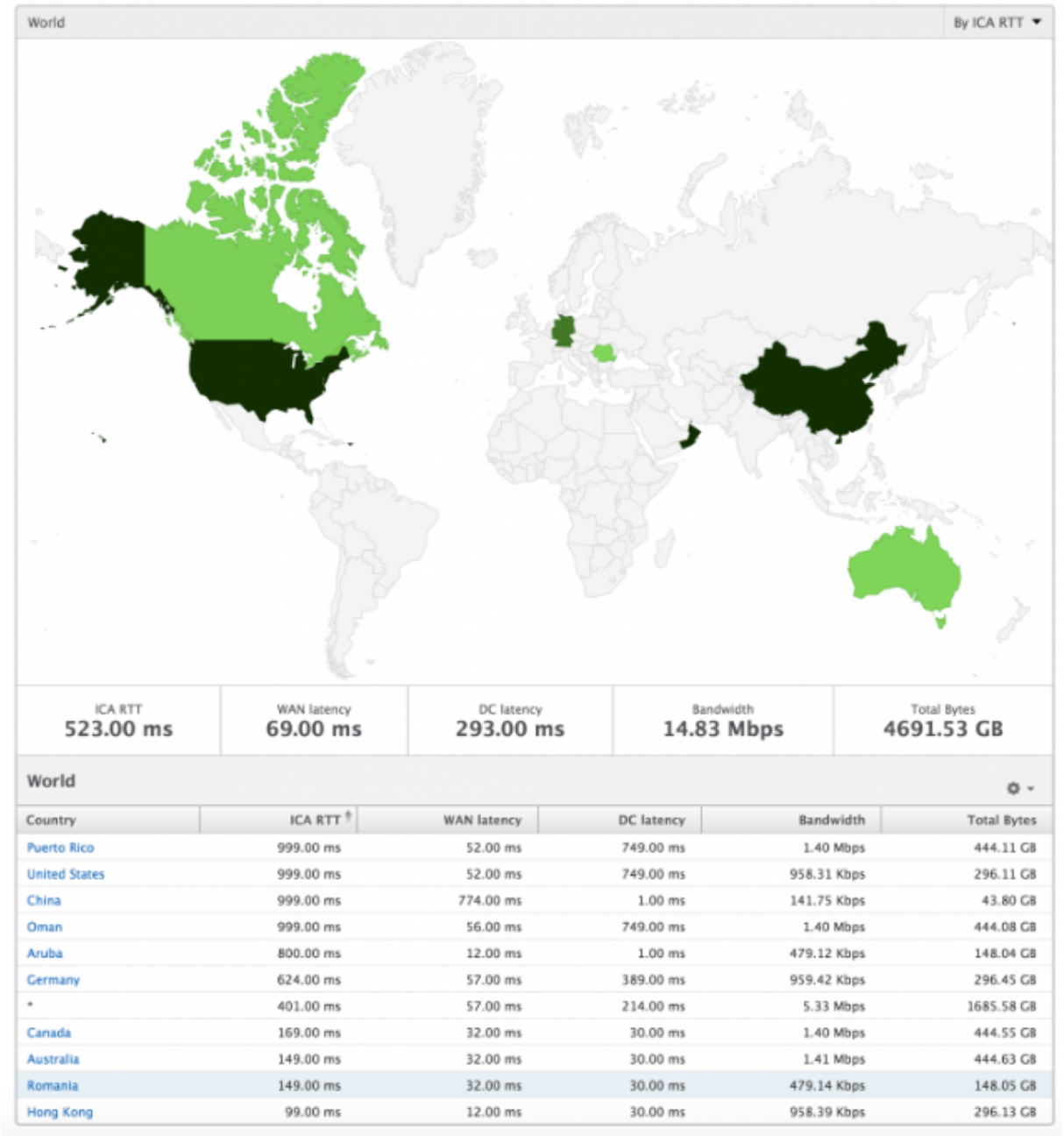
Name	Server Side Retransmits	ICA RTT	Client SRTT	Session Reconnect	Latency	Clientside zero window size event	Server SRTT
c1\daniel	0	149.44	1		149.44	0	
ryan	5071	4640	1		4640	0	
ramas	0	994.71	1		994.71	0	

Anzahl der Schwellenwertverstöße Die Metriken für die Anzahl der Schwellenwertverstöße stellen die Anzahl der Schwellenwerte dar, die im ausgewählten Zeitraum überschritten wurden.

Weltkarte Mit der Weltkartenansicht in HDX Insight können Administratoren die historischen und aktiven Benutzerdetails aus geografischer Sicht anzeigen. Die Administratoren können eine Weltsicht auf das System haben, einen Drilldown zu einem bestimmten Land und auch weiter in Städte hineinfahren, indem sie einfach auf die Region klicken. Die Administratoren können weitere Informationen nach Stadt und Bundesstaat anzeigen. Ab NetScaler ADM Version 12.0 und höher können Sie einen Drilldown zu Benutzern durchführen, die von einem Geostandort aus verbunden sind.

Die folgenden Details können auf der Weltkarte in HDX Insight angezeigt werden, und die Dichte jeder Metrik wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Bytes insgesamt



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Ansicht pro Benutzer

Die Ansicht pro Benutzer bietet detaillierte Berichte über die Endbenutzererfahrung für einen bestimmten ausgewählten Benutzer.

So navigieren Sie zu den Metriken eines bestimmten Benutzers:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**.

3. Wählen Sie im Übersichtsbericht Benutzer einen bestimmten Benutzer aus.

Liniendiagramm Das Liniendiagramm zeigt eine Zusammenfassung aller Metriken für den ausgewählten Benutzer während des ausgewählten Zeitraums an.

Bericht über aktuelle/abgeschlossene Sitzungen Dieser Bericht bezieht sich auf alle aktuellen/beendeten Benutzersitzungen für den ausgewählten Benutzer. Diese Metriken können nach Startzeit, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der durch die Citrix ADCs fließt, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Receiver-Typ: Citrix Windows Client und so weiter
Clientversion	Receiver-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.

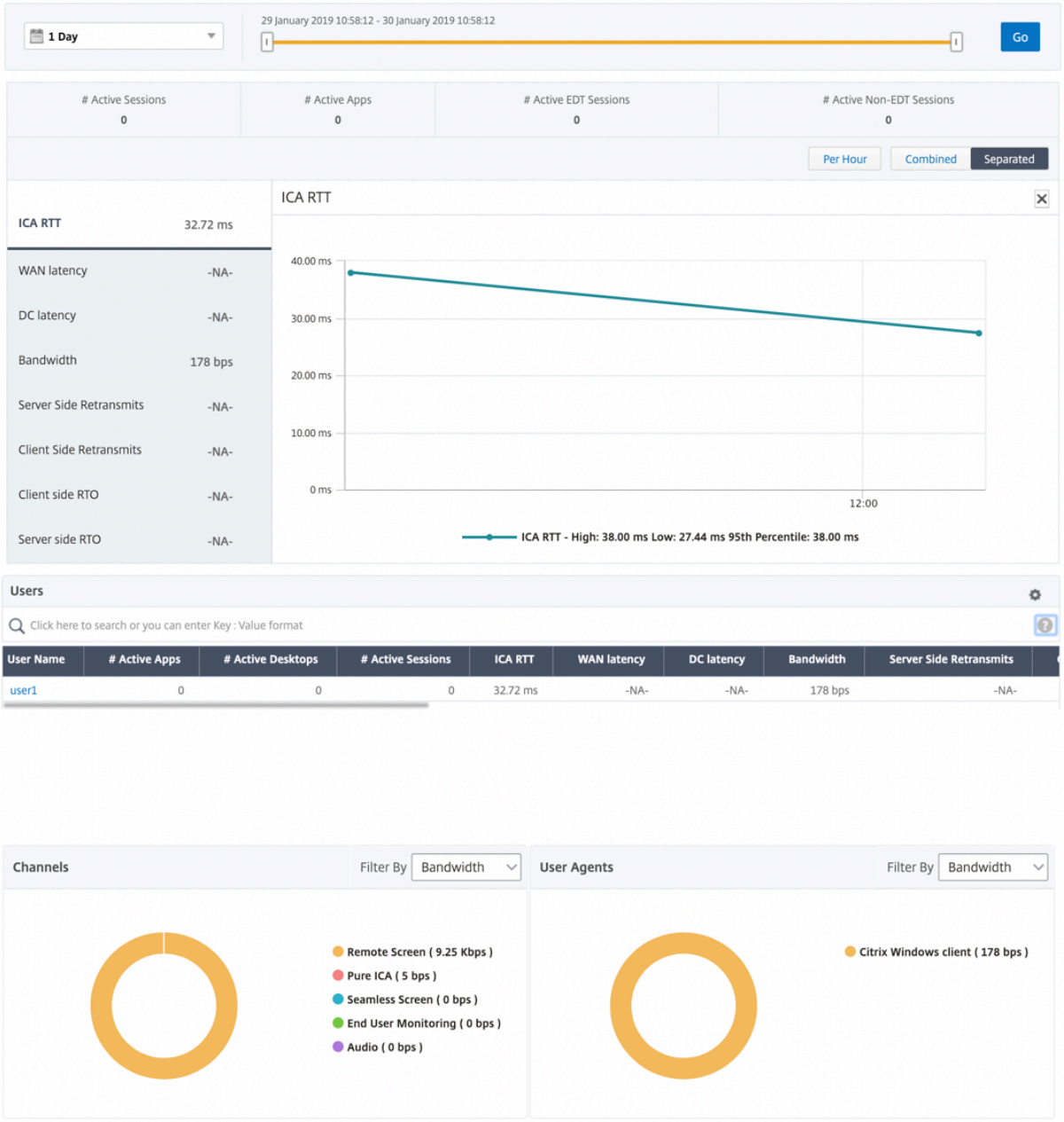
Metriken	Beschreibung
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway-Benutzer/Transparentmodus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet wurde.
USB-Status	Aktiv/Inaktiv - Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.

Metriken	Beschreibung
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.

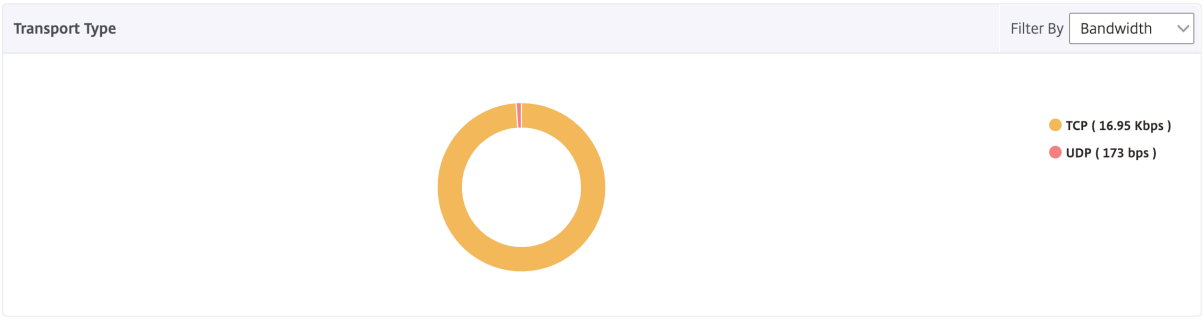
Unterstützung für EDT in HDX Insight

NetScaler Application Delivery Management (ADM) unterstützt jetzt Enlightened Data Transport (EDT) zur Anzeige von Analysen für HDX Insight. Das heißt, ADM unterstützt jetzt sowohl das UDP- als auch das TCP-Protokoll. Die EDT-Unterstützung für NetScaler Gateway gewährleistet eine hochauflösende Benutzererfahrung virtueller Desktops während der Sitzung für Benutzer, die Citrix Receiver ausführen.

HDX Insight zeigt jetzt die Anzahl der EDT-Sitzungen und Nicht-EDT-Sitzungen als Teil des Berichts über aktive Sitzungen an. In der Tabelle Benutzer wird ein detaillierter Bericht aller Benutzer im System angezeigt. Die Tabelle zeigt Metriken wie WAN-Latenz, DC-Latenz, erneute Übertragungen, RTOs. Einige dieser Metriken sind für Benutzer mit EDT-Sitzungen nicht verfügbar, da sie derzeit aus dem TCP-Stack berechnet werden. Daher erscheinen sie als “NA”.



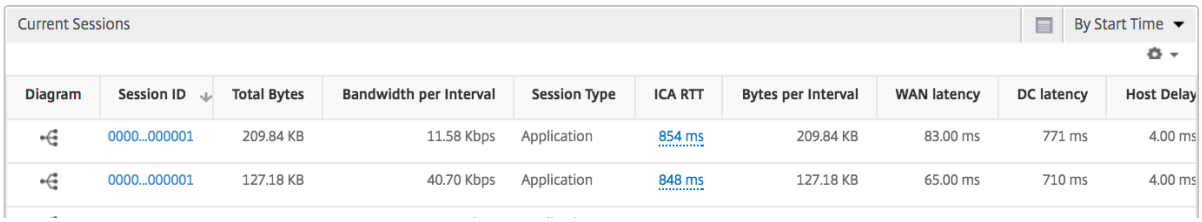
Es wurde ein neues Donutdiagramm eingeführt, mit dem Sie die vom Benutzer verbrauchte Bandbreite und die Gesamtzahl der Bytes basierend auf dem von den Benutzern verwendeten Protokolltyp sehen können.

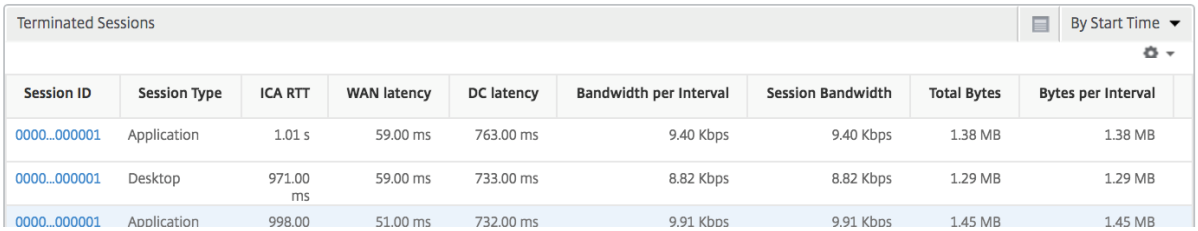


> **Hinweis:**
>
> EDT in HDX Insight wird von NetScaler ADM ab Version 12.1 Build 50.28 unterstützt und ist für ADC-Instanzen ab Version 12.1 Build 49.23 verfügbar.

HDX Insight Metriken, die ab NetScaler ADM 12.0 und höher verfügbar sind:

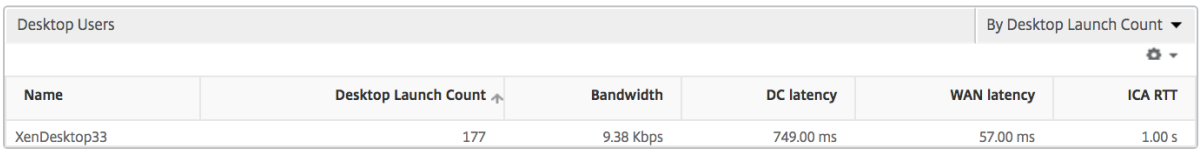
L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der NetScaler ADC-Instanz beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.
L7 Serverseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem NetScaler ADC Gerät und der Citrix Virtual App beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.
Maximale Verletzungslatenz	Der höchste Wert der L7-Latenz, wenn ein definierter Schwellenwert für ein festgelegtes Zeitintervall überschritten wird.
Durchschnittliche Latenz bei Sicherheitsverletzungen	Der Durchschnittswert der L7-Latenz, wenn sich das System in einem Zustand “L7-Latenz verletzt”befindet.
Anzahl von L7-Schwellenwertverletzungen	Gibt an, wie oft eine L7-Schwellenverletzung aufgetreten ist.



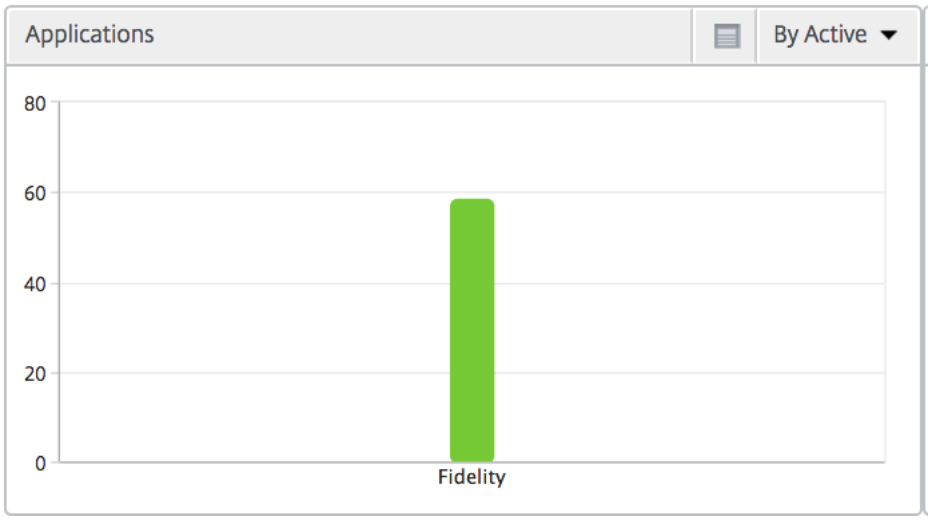


Desktop-Benutzer Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

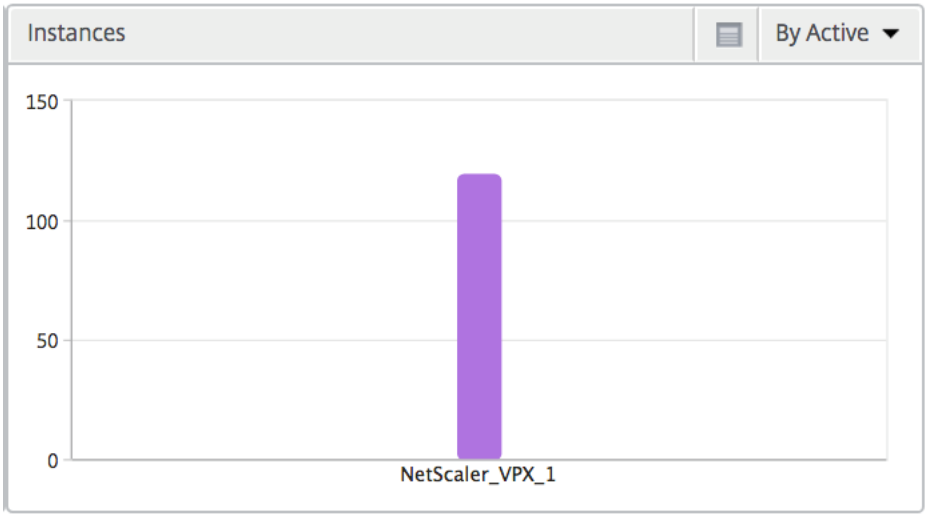
Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.



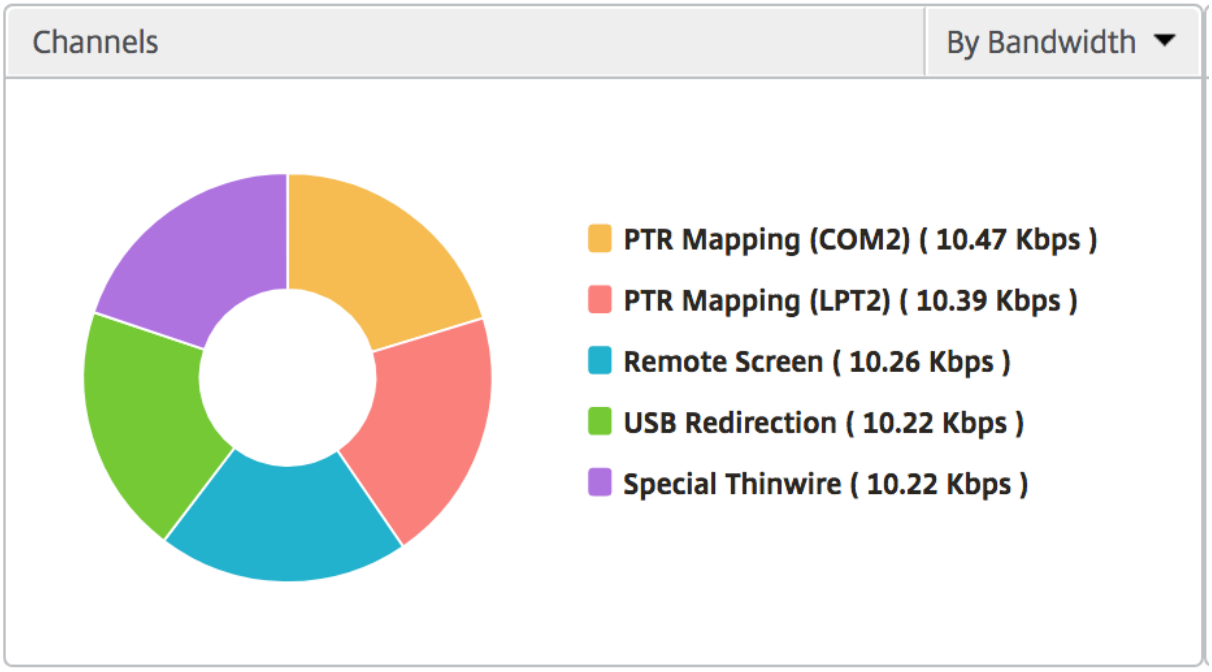
Anwendungen Ein Balkendiagramm, das Apps sortiert nach Aktiv, Gesamtzahl der Sitzungsstarts, Gesamtanzahl des App-Starts und Startdauer darstellt.



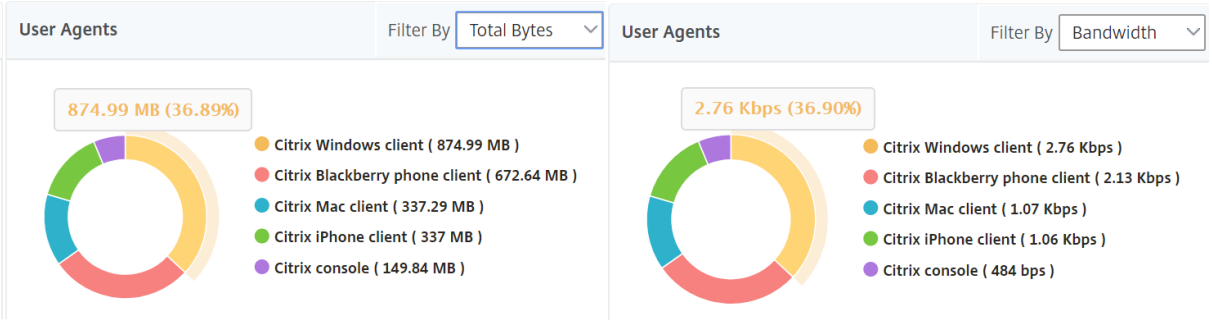
Instanzen Ein Balkendiagramm, das NetScaler ADC Instanzen darstellt, sortiert nach Active und Apps insgesamt



Kanäle Kanäle stellen die Gesamtbandbreite oder die Gesamtzahl der von jedem virtuellen ICA-Kanal verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Benutzer-Agenten Benutzeragenten stellen die gesamte Bandbreite/Gesamtanzahl der von jedem Endpunkt verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Sitzungsansicht pro Benutzer Die Sitzungsansicht pro Benutzer bietet Berichte für die Sitzung eines bestimmten ausgewählten Benutzers.

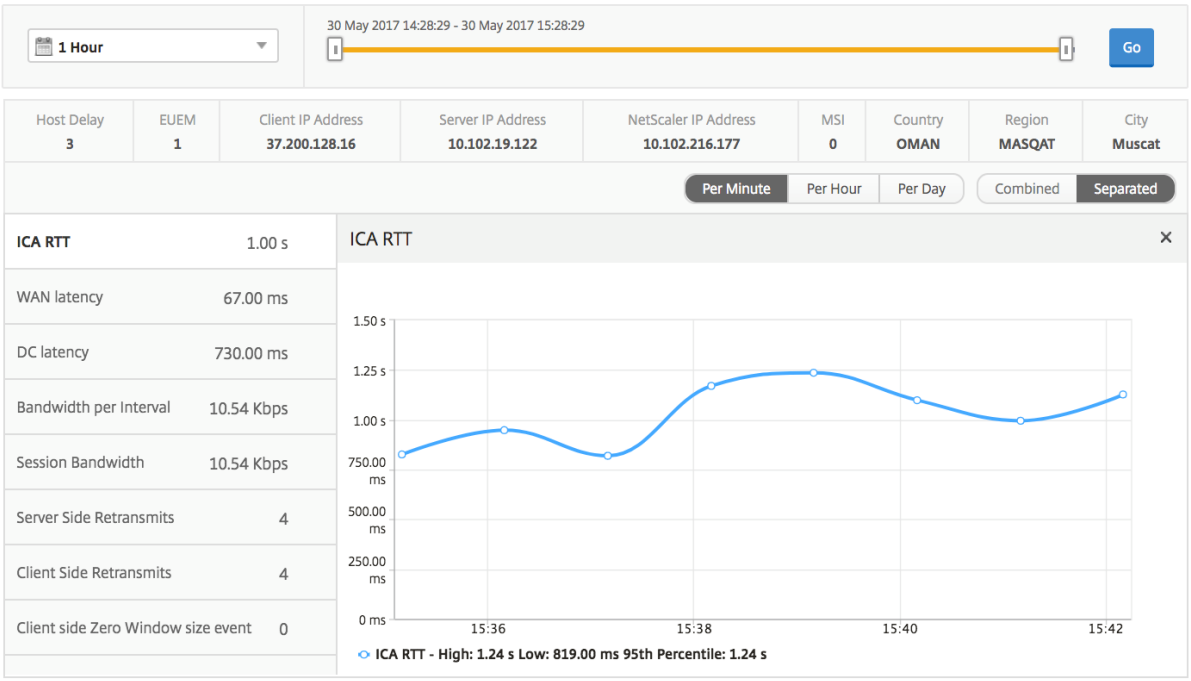
So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**.
2. Wählen Sie im Abschnitt **Benutzerübersichtsbericht** einen bestimmten Benutzer aus.
3. Wählen Sie in der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** eine Sitzung aus.

Zeitleistendiagramm

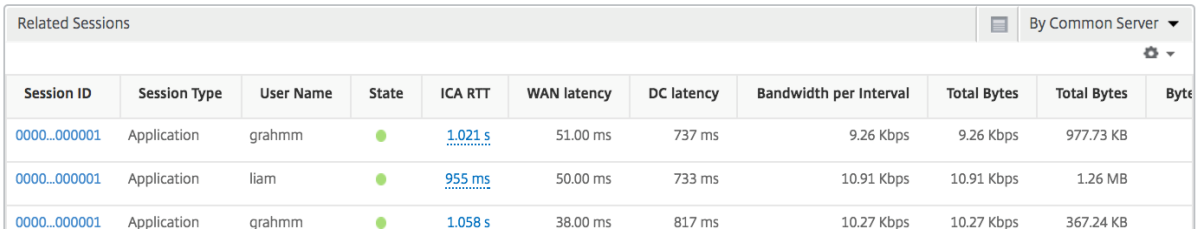
Metriken	Beschreibung
Wiederverbindung der Sitzung	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
ACR-Anzahl	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die auf Citrix Virtual Apps bzw. Desktops gehostet werden.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.

Metriken	Beschreibung
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.



Aktive Anwendung Im Abschnitt **Aktive Anwendungen** werden die aktiven Anwendungen des ausgewählten Benutzers angezeigt. Diese Anwendungen können auch nach Anzahl der aktiven Sitzungen und Startdauer sortiert werden.

Verwandte Sitzungen Im Abschnitt "Sessions"werden die zugehörigen Sitzungen der Sitzungen des ausgewählten Benutzers angezeigt. Die Beziehung kann als gemeinsame Server oder gemeinsames NetScaler ADC ausgewählt werden.



Berichte und Metriken der Anwendungsansicht

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf Citrix Virtual Apps.

So navigieren Sie zur Anwendungsansicht:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Anwendungen**.

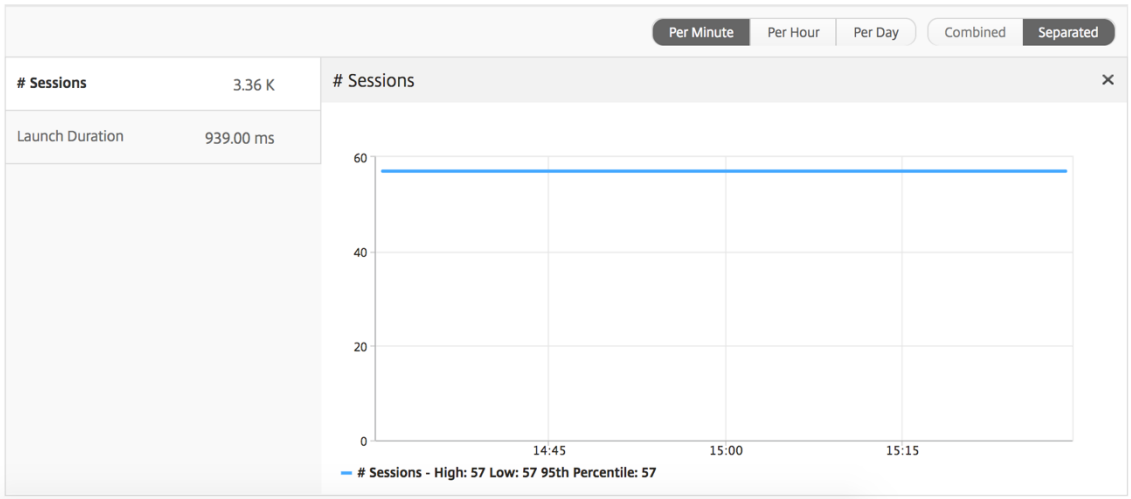
Übersichtsansicht

In der Zusammenfassungsansicht werden die Berichte für alle Anwendungen angezeigt, die während der ausgewählten Zeitachse angemeldet sind.

Alle Metriken/Berichte, sofern nicht ausdrücklich erwähnt, haben die Werte, die ihnen für den ausgewählten Zeitraum entsprechen.

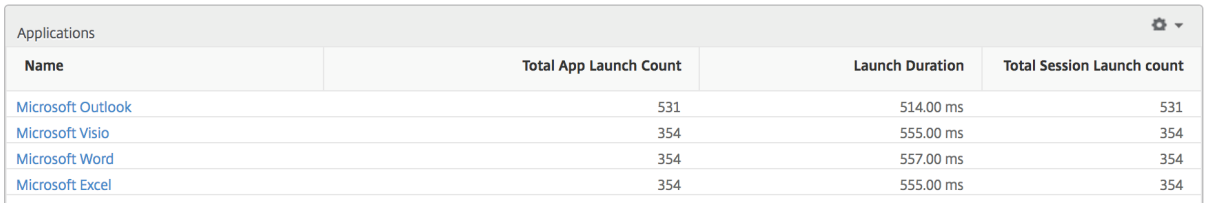
Liniendiagramm

Metriken	Beschreibung
Anzahl Sitzungen	Gesamtzahl der Sitzungen während eines bestimmten Zeitintervalls.
Dauer des Starts	Durchschnittliche Zeit zum Starten einer Anwendung.



Zusammenfassender Bericht für Anwendungen

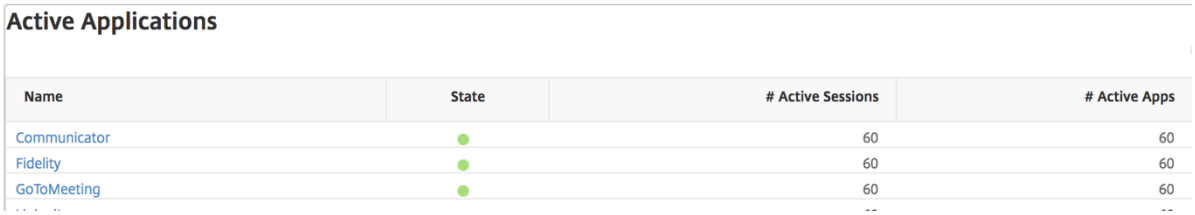
Metriken	Beschreibung
Name	Name der Citrix Virtual App.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual App-Sitzungen während des angegebenen Zeitintervalls.
App-Starts insgesamt	Gesamtzahl der Citrix Virtual App-Anwendungen, die während des angegebenen Zeitintervalls gestartet wurden.
Startdauer	Durchschnittliche Zeit für den Start der Citrix Virtual App.



Bericht über aktive Anwendungen

Metriken	Beschreibung
Name	Name der Citrix Virtual App.

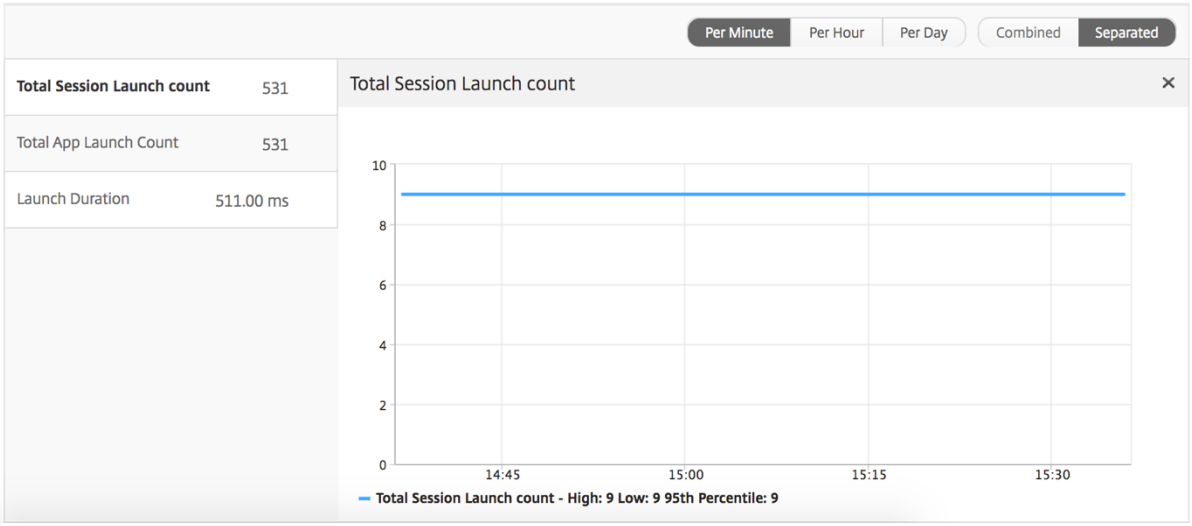
Metriken	Beschreibung
Status	Zeigt den Status der Anwendung an: Grün-Aktiv, Rot-Inaktiv
Anzahl aktiver Sitzungen	Anzahl der aktiven Benutzersitzungen, die diese App während eines bestimmten Zeitintervalls verwenden.
Anzahlt aktiver Apps	Anzahl der aktiven Sitzungen für diese Anwendung.



Bericht "Schwellenwert" Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* im ausgewählten Zeitraum als Anwendung ausgewählt wurde. Weitere Informationen finden Sie unter Erstellen von Schwellenwerten.

Liniendiagramm

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Dauer des Starts	Durchschnittliche Zeit zum Starten einer Anwendung.



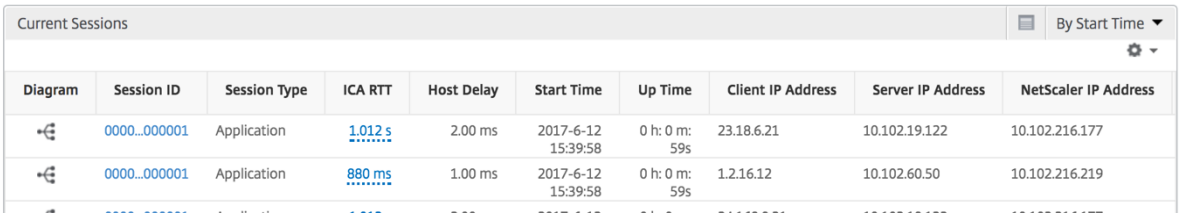
Bericht zu aktuellen Sitzungen

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der durch die Citrix ADCs fließt, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).

Metriken	Beschreibung
Clienttyp	Receiver-Typ: Citrix Windows Client und so weiter
Clientversion	Receiver-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway-Benutzer/Transparentmodus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet wurde.
USB-Status	Aktiv/Inaktiv - Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die auf Citrix Virtual Apps bzw. Desktops gehostet werden.

Metriken	Beschreibung
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
Benutzername	Der Benutzername des Benutzers, der auf diese bestimmte Citrix Virtual App zugreift.
Sitzungs-ID	Eindeutige Kennung für die Citrix Virtual App-Sitzung.
Sitzungstyp	Wird “Anwendung”sein.
Status	Sitzungsstatus: Grün für aktiv, Rot für Inaktiv.

Metriken	Beschreibung
Maximale Verletzungslatenz	Der höchste Wert der L7-Latenz, wenn ein definierter Schwellenwert für ein festgelegtes Zeitintervall überschritten wird.
Durchschnittliche Latenz bei Sicherheitsverletzungen	Der Durchschnittswert der L7-Latenz, wenn sich das System in einem Zustand “L7-Latenz verletzt”befindet.
Anzahl von L7-Schwellenwertverletzungen	Gibt an, wie oft eine L7-Schwellenverletzung aufgetreten ist.
L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der NetScaler ADC-Instanz beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.
L7 Serverseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem NetScaler ADC Gerät und der Citrix Virtual App beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.



Sitzungsansicht pro Anwendung

Die Session-Ansicht pro Anwendung zeigt Berichte für eine bestimmte ausgewählte Anwendungssitzung an.

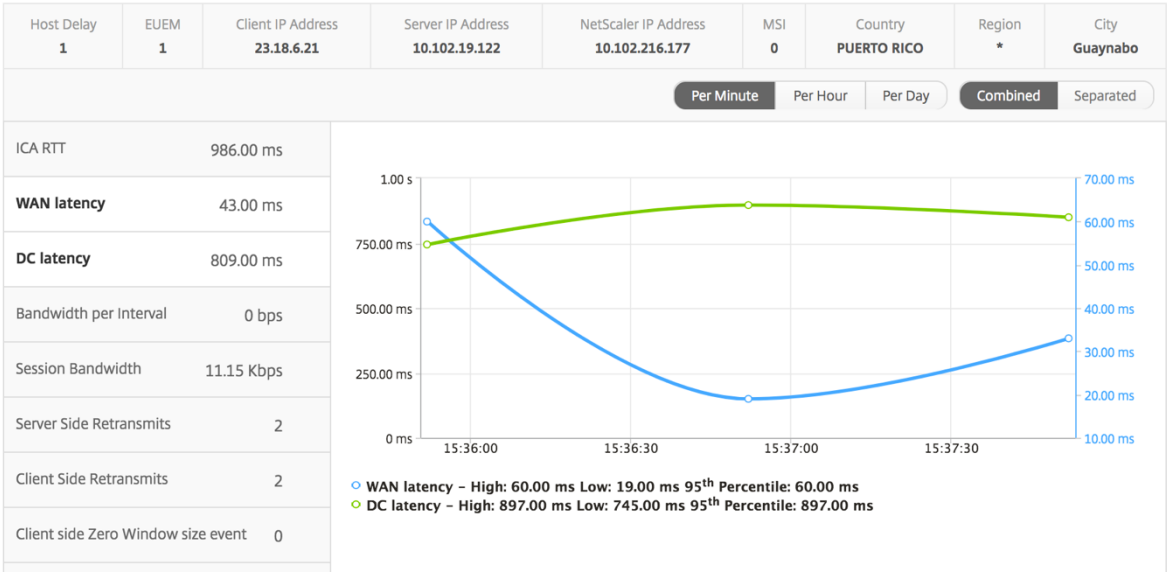
So zeigen Sie die Sitzungsberichte an:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics** > **HDX Insight** > **Anwendungen**.
3. Wählen Sie im Anwendungsübersichtsbericht einen bestimmten Benutzer aus.
4. Eine Sitzung aus dem Bericht über aktuelle Sitzungen ausgewählt.

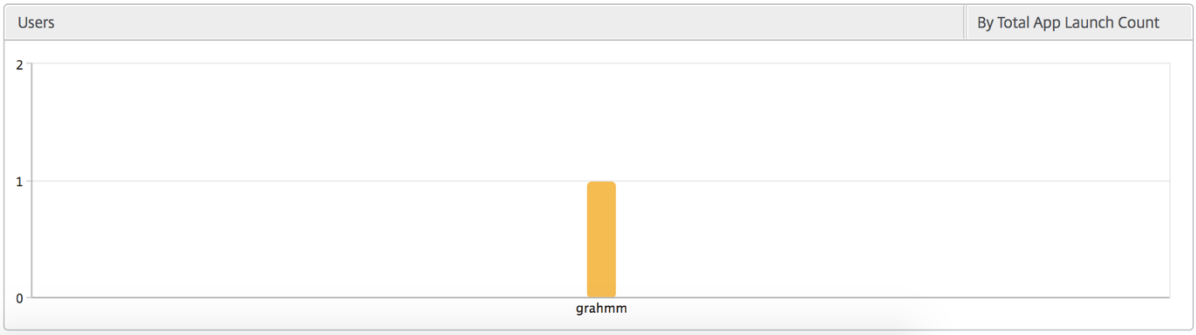
Liniendiagramm

Metriken	Beschreibung
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
Serverseitiges Ereignis mit Zero Window-Größe	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zu Backend-Servern.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.

Metriken	Beschreibung
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.



Benutzerbalkendiagramm Das Balkendiagramm des Benutzers stellt die Benutzer dar, die in dieser speziellen App angemeldet sind.



Berichte und Metriken für Desktopansichten

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf Citrix Virtual Desktops.

So navigieren Sie zur Desktopansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics** > **HDX Insight** > **Desktop**.

Übersichtsansicht

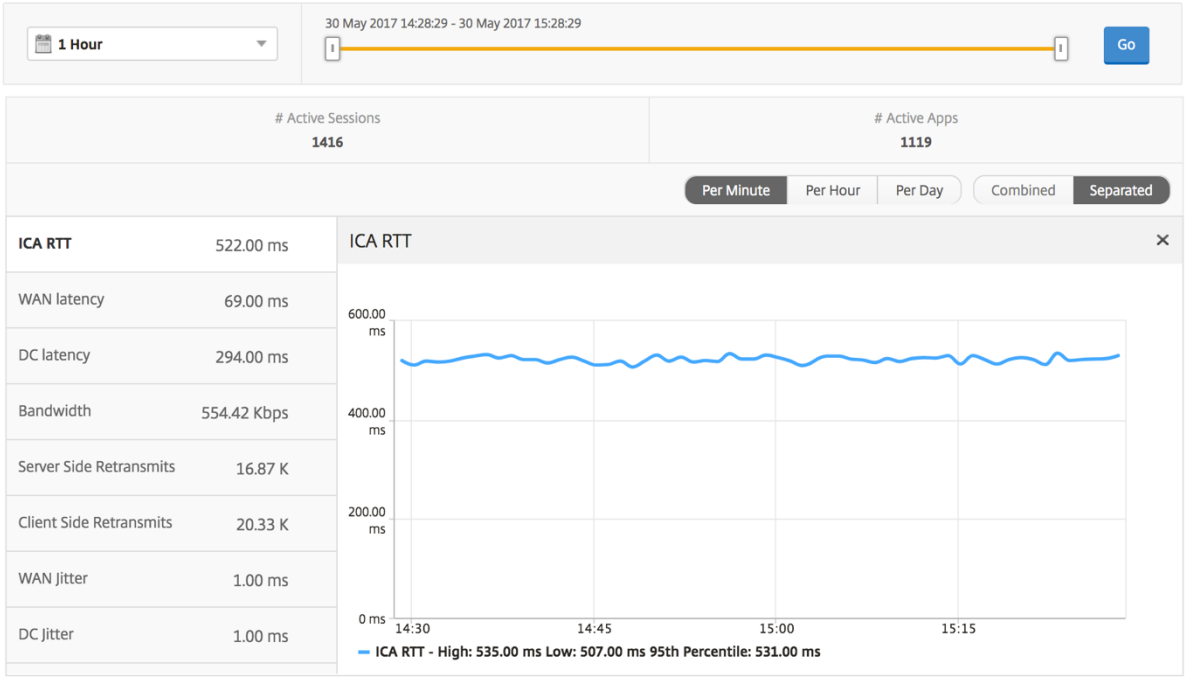
In der Zusammenfassungsansicht werden die Berichte für alle Citrix Virtual Desktops angezeigt, die während der ausgewählten Zeitleiste angemeldet sind.

Alle Metriken/Berichte, sofern nicht ausdrücklich erwähnt, haben die Werte, die ihnen für den ausgewählten Zeitraum entsprechen.

Liniendiagramm

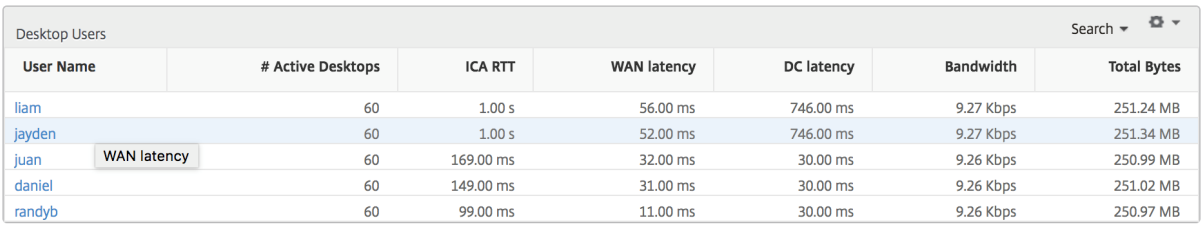
Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.

Metriken	Beschreibung
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.



Desktop-Sammelbericht

Metriken	Beschreibung
Aktive Sitzungen	Gesamtzahl der aktiven Citrix Virtual Desktop-Sitzungen während eines bestimmten Zeitintervalls.
Aktive Desktops	Gesamtzahl der aktiven Citrix Virtual Desktops in einem bestimmten Zeitintervall.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.



Bericht "Schwellenwert" Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* in der ausgewählten Periode als Desktop ausgewählt wurde. Weitere Informationen finden Sie unter Erstellen von Schwellenwerten.

Pro Desktop-Ansicht

Die Ansicht pro Desktop bietet detaillierte Berichte zur Endbenutzererfahrung für einen ausgewählten Citrix Virtual Desktop.

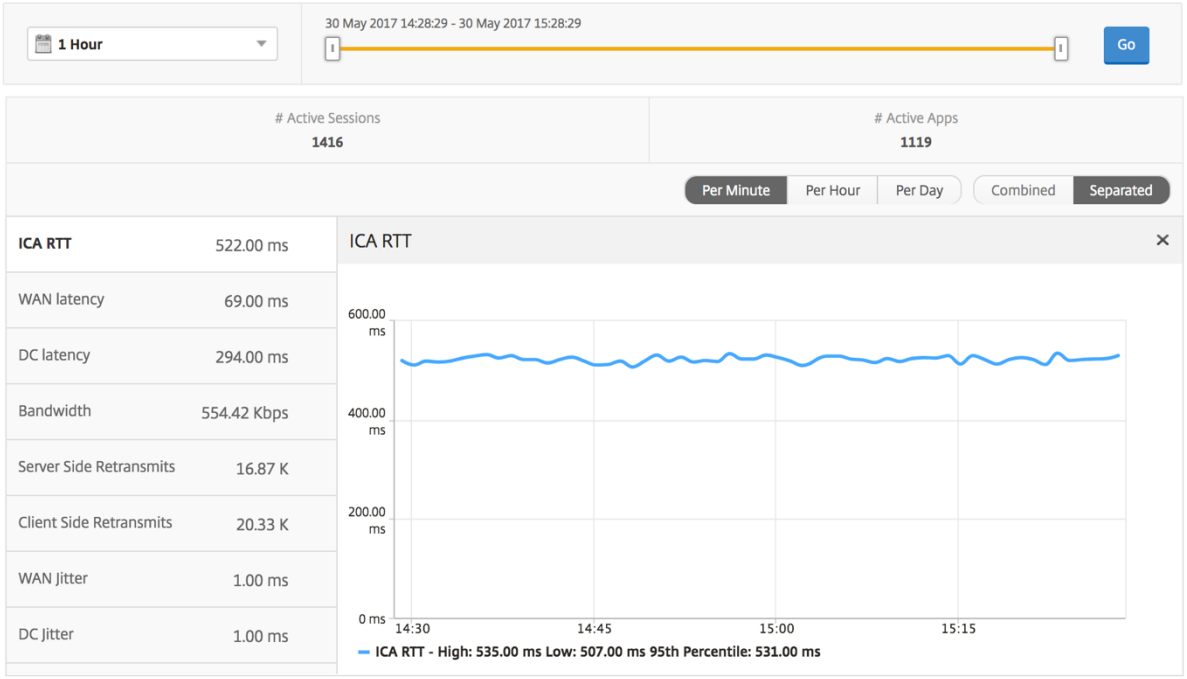
So navigieren Sie zur jeweiligen Desktop-Ansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem Citrix ADM an.
2. Navigieren Sie zu **Analytics > HDX Insight > Desktop**.
3. Wählen Sie im **Desktop-Zusammenfassungsberichteinen bestimmten Desktop**aus.

Liniendiagramm

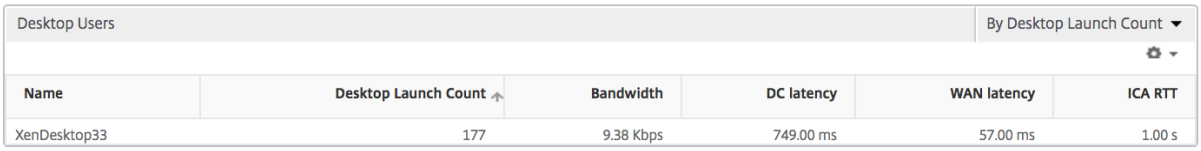
Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.

Metriken	Beschreibung
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.



Bericht "Desktop-Benutzer" Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.



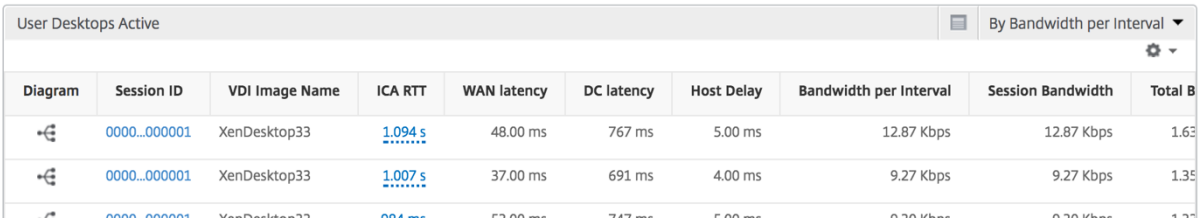
Benutzerdesktops Aktiv/Inaktiv Bericht Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.

Metriken	Beschreibung
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der durch die Citrix ADCs fließt, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Receiver-Typ: Citrix Windows Client und so weiter
Clientversion	Receiver-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway-Benutzer/Transparentmodus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet wurde.
USB-Status	Aktiv/Inaktiv - Grün/Rot.

Metriken	Beschreibung
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.

Metriken	Beschreibung
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
VDI-Imagename	Name des Citrix Virtual Desktop, mit dem der Benutzer verbunden ist
Diagramm	



Sitzungsansicht pro Desktop-Sitzung

Pro Desktop-Sitzungsansicht stellt Berichte für eine bestimmte ausgewählte Citrix Virtual Desktop-Sitzung bereit.

So navigieren Sie zur Desktop-Sitzungsansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem Citrix ADM an.
2. Navigieren Sie zu **Analytics > HDX Insight > Desktop**.
3. Wählen Sie im **Desktopübersichtsbericht einen bestimmten Desktop**aus.
4. Wählen Sie eine Sitzung aus dem Bericht über aktuelle Sitzungen aus.

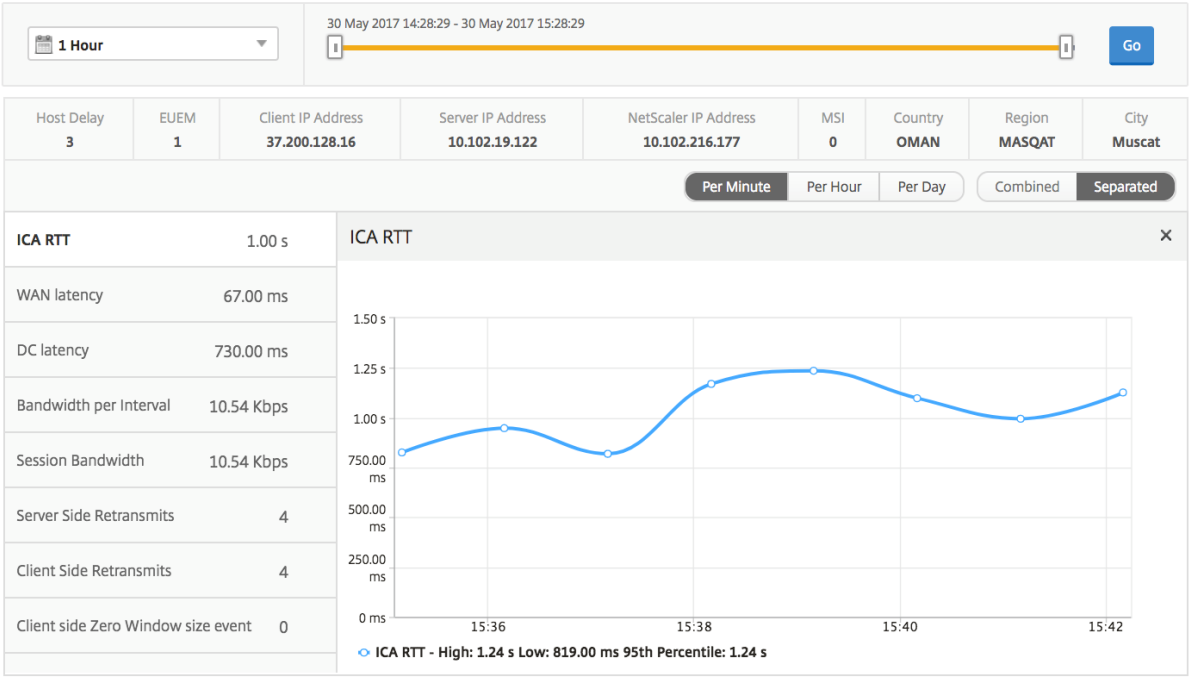
Zeitleistendiagramm Die Sitzungsansicht pro Benutzer bietet Berichte für die Sitzung eines bestimmten ausgewählten Benutzers.

So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**.
3. Wählen Sie im Abschnitt **Benutzerübersichtsbericht** einen bestimmten Benutzer aus.
4. Wählen Sie in der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** eine Sitzung aus.

Metriken	Beschreibung
Wiederverbindung der Sitzung	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
ACR-Anzahl	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.

Metriken	Beschreibung
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.



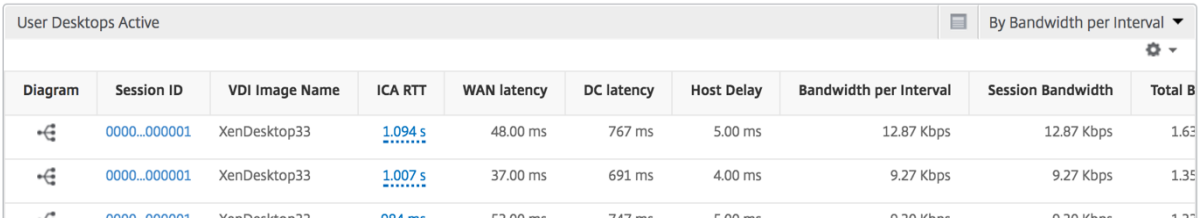
Bericht zu verwandten Desktop-Sitzungen Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.

Metriken	Beschreibung
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der durch die Citrix ADCs fließt, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Receiver-Typ: Citrix Windows Client und so weiter
Clientversion	Receiver-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway-Benutzer/Transparentmodus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet wurde.

Metriken	Beschreibung
USB-Status	Aktiv/Inaktiv - Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.

Metriken	Beschreibung
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.



Instanzansicht von Berichten und Metriken

Die Berichte und Metriken in der Instanzansicht konzentrieren sich auf die NetScaler ADC Instanzen.

So navigieren Sie zur Instanzansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics > HDX Insight > Instances**.

Berichte und Metriken zur Instanzansicht bestehen aus den folgenden Abschnitten:

- Instanzzusammenfassungsansicht
- Ansicht pro Instanz

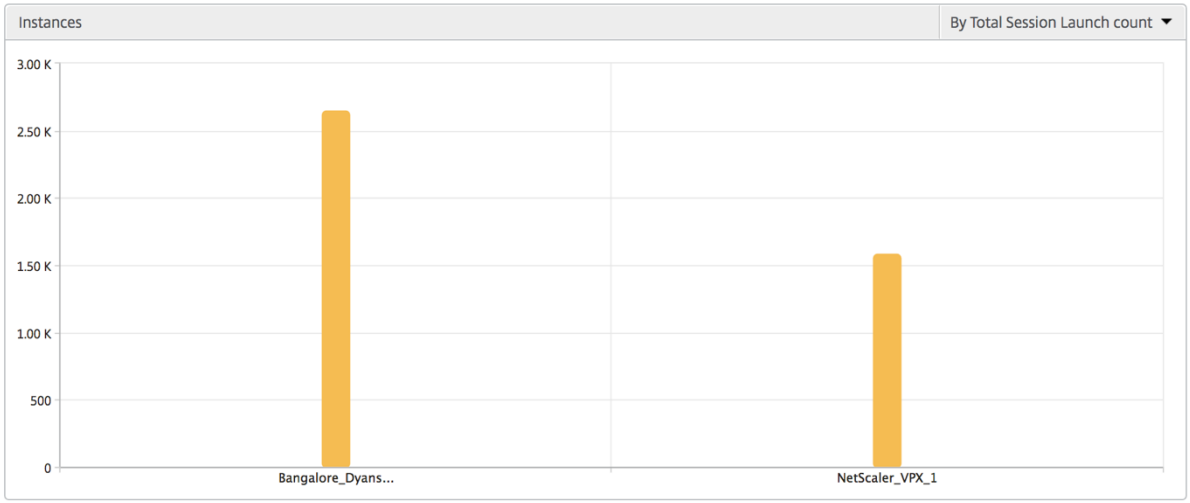
Instanz-Zusammenfassungsansicht

Diese Ansicht wird als Zusammenfassungsansicht bezeichnet, da sie die Berichte für alle NetScaler ADC Instanzen anzeigt, die NetScaler ADM hinzugefügt werden.

Alle unten aufgeführten Metriken/Berichte, sofern nicht explizit erwähnt, haben die Werte, die ihnen für den ausgewählten Zeitraum entsprechen.

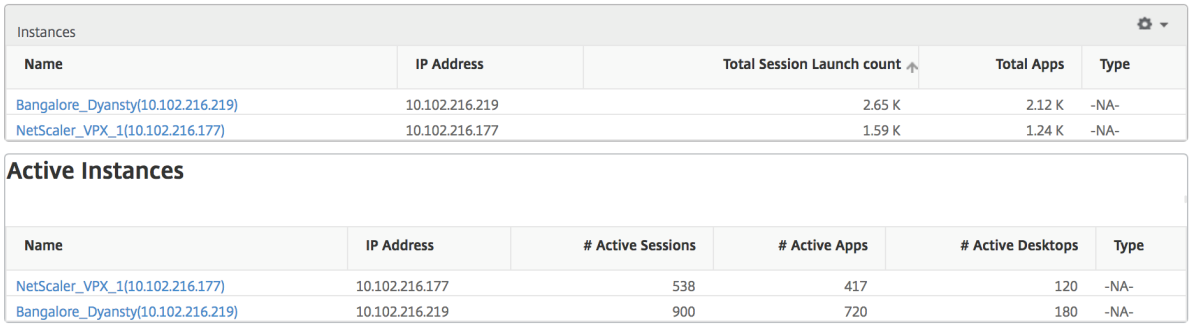
Instanz-Balkendiagramm

In diesem Diagramm wird die Instanz im Vergleich zur Gesamtzahl der Sitzungsstarts angezeigt.	Gesamtzahl der Apps, die aus der Liste oben rechts auf der Diagrammfläche ausgewählt werden können.



Übersichtsbericht “Instanz/Aktive Instanzen”

Metriken	Beschreibung
Name	Hostname der NetScaler ADC-Instanz.
IP-Adresse	NetScaler-IP-Adresse.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der eindeutigen Benutzersitzungen, die während eines bestimmten Zeitintervalls erstellt wurden.
Apps insgesamt	Gesamtzahl der eindeutigen Anwendungen, die während eines bestimmten Zeitintervalls gestartet wurden.
Typ	–



Instances

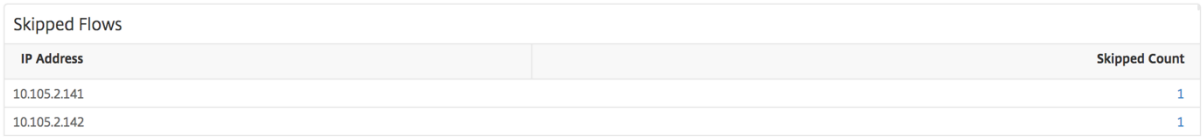
Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

Bericht "Schwellenwert" Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* in der ausgewählten Periode als Instanz ausgewählt wurde. Weitere Informationen finden Sie unter Erstellen von Schwellenwerten.

Übersprungene Flows Ein übersprungener Flow ist ein Datensatz, der die Parsing ICA-Verbindung übersprungen hat. Dies kann aus mehreren Gründen auftreten, z. B. bei nicht unterstützten Citrix Virtual Apps- und Desktop-Versionen, nicht unterstützten Versionen des Receiver- oder Empfängertyps usw. In dieser Tabelle werden die IP-Adresse und die Anzahl der übersprungenen Datenflüsse angezeigt. Diese Empfänger dürfen nicht Teil von Receivern auf der Positivliste sein. Daher werden diese Sitzungen von der Überwachung übersprungen.



Skipped Flows

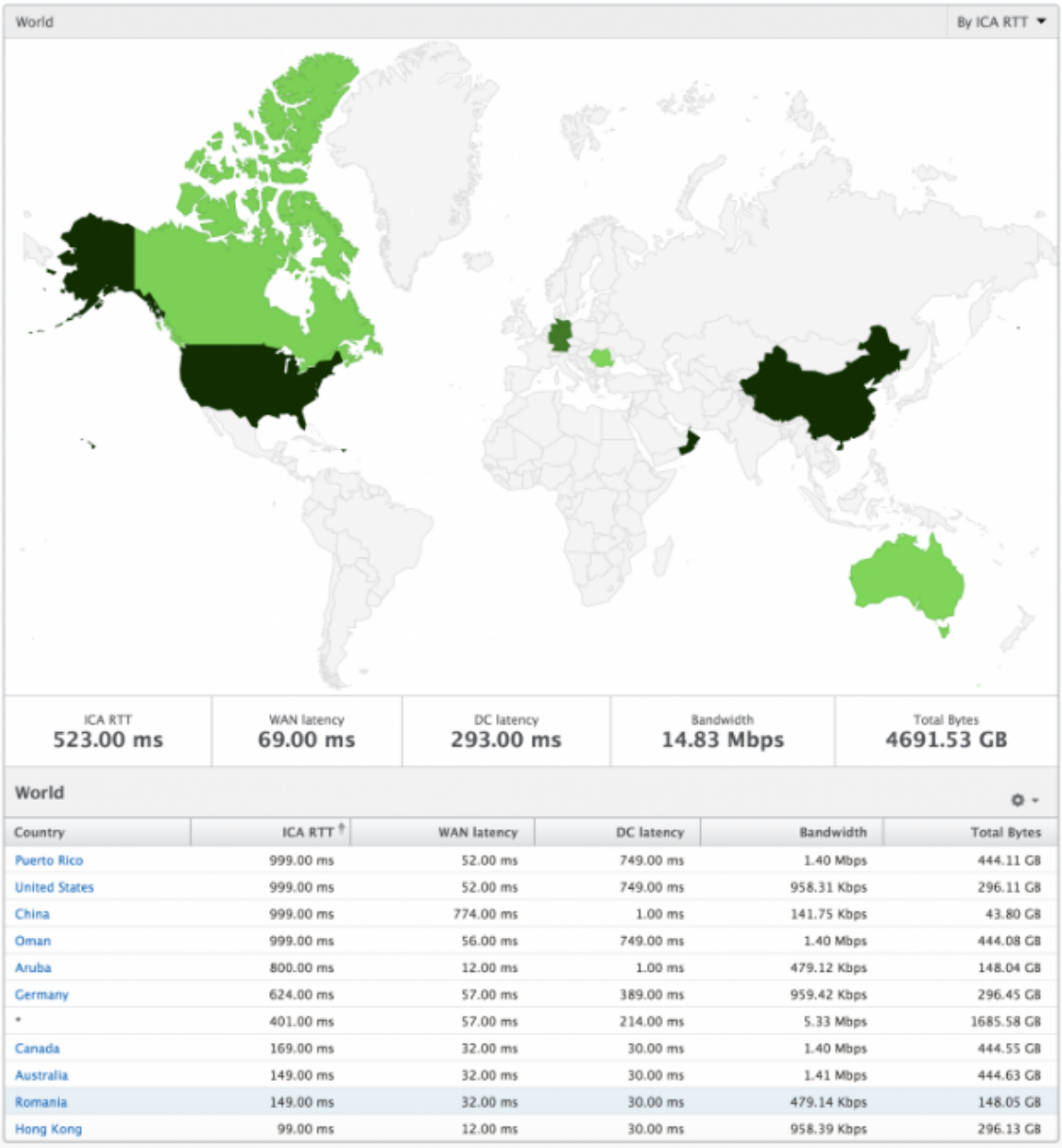
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

Weltansicht Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die historischen und aktiven Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können durch einfaches Klicken auf die Region einen Überblick über das System haben, einen Drilldown zu einem bestimmten Land und weiter in die Städte einsehen. Die Administratoren können weitere Informationen nach Stadt und Bundesstaat anzeigen. Ab NetScaler ADM Version 12.0 und höher können Sie einen Drilldown zu Benutzern durchführen, die von einem Geostandort aus verbunden sind.

Die folgenden Details können auf der Weltkarte in HDX Insight angezeigt werden, und die Dichte jeder Metrik wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite

- Bytes insgesamt



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Ansicht pro Instanz

Die Ansicht pro Instanz bietet detaillierte Berichte über die Benutzererfahrung für eine bestimmte ausgewählte NetScaler ADC Instanz.

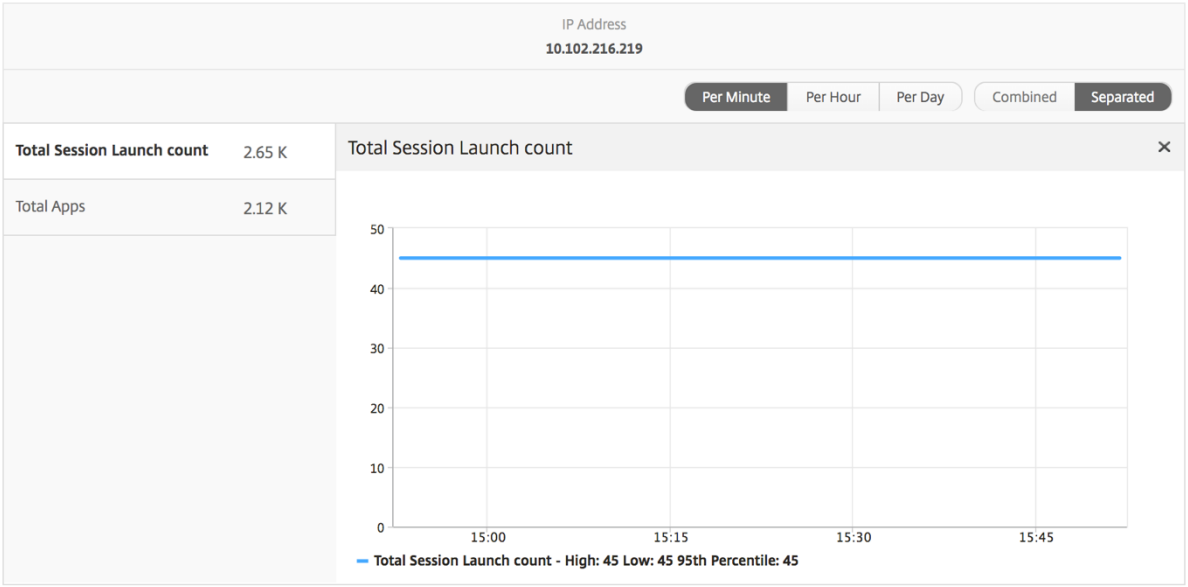
So navigieren Sie zur Instanzansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.

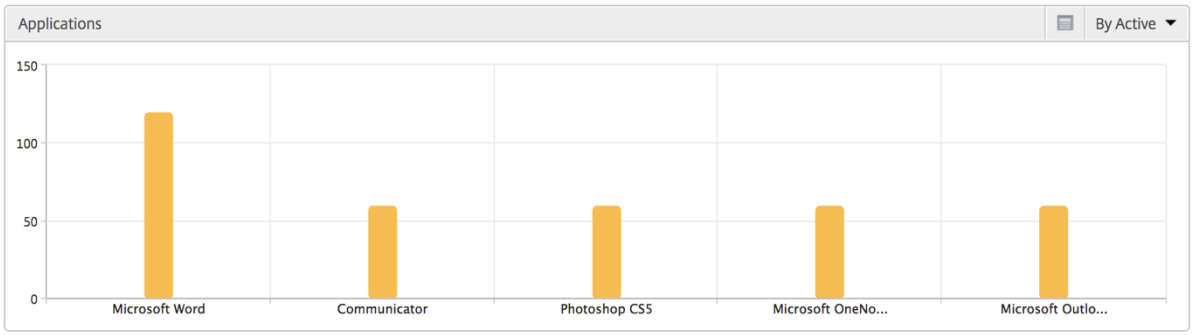
2. Navigieren Sie zu **Analytics > HDX Insight > Instances**.
3. Wählen Sie in der **Auswertung "Instanzübersicht"** eine bestimmte Instanz aus.

Liniendiagramm

Metriken	Beschreibung
IP-Adresse	Dies stellt die NetScaler-IP-Adresse der ausgewählten Instanz dar.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual App-Sitzungen während des angegebenen Zeitintervalls.
Apps insgesamt	Gesamtzahl der eindeutigen Anwendungen, die während eines bestimmten Zeitintervalls gestartet wurden.

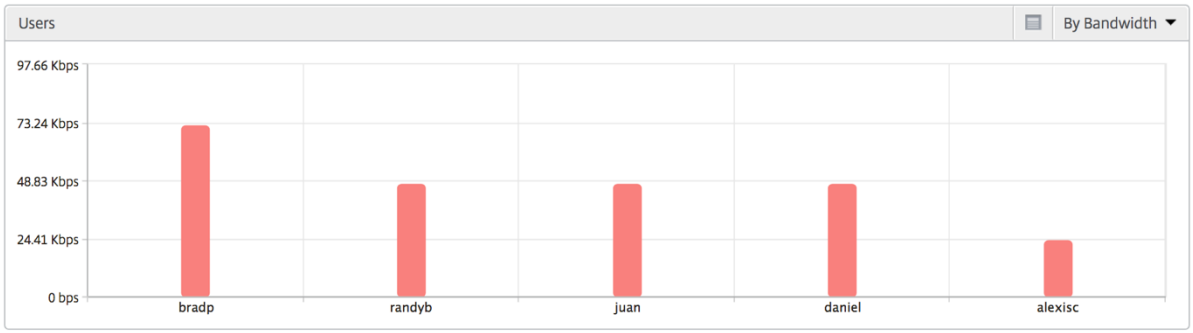


Balkendiagramm für Anwendungen Zeigt die 5 wichtigsten Anwendungen basierend auf den folgenden Kriterien an: nach aktiven Apps, Gesamtzahl der Sitzungsstarts, Gesamtzahl der App-Startstarts oder Startdauer.



Balkendiagramm "Benutzer" Das Balkendiagramm "Benutzer"zeigt die fünf wichtigsten Benutzer anhand der folgenden Kriterien an:

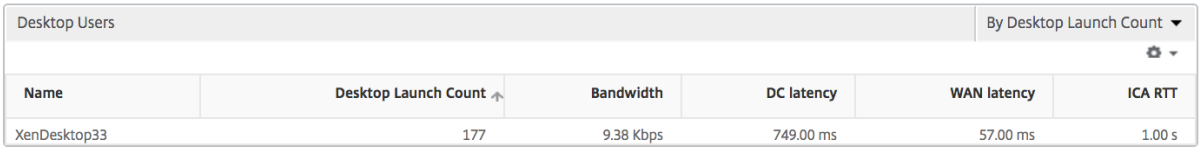
- Bandbreite
- WAN-Latenz
- DC-Latenz
- ICA RTT



Bericht "Desktop-Benutzer" Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.

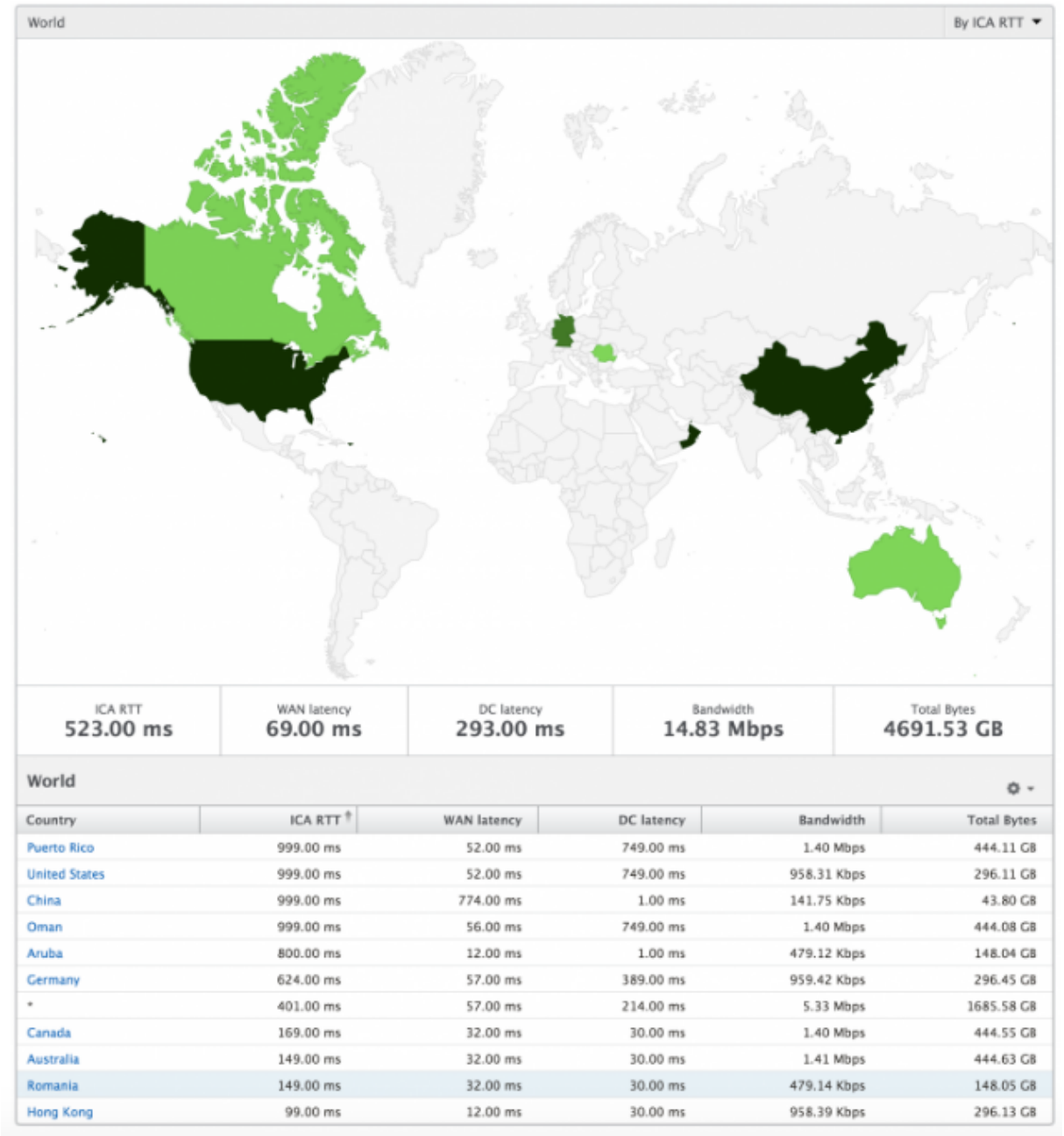
Metriken	Beschreibung
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.



Weltansicht Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die historischen und aktiven Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltanschauung des Systems, Drilldown zu einem bestimmten Land und weiter in die Städte als auch durch Klicken auf die Region. Die Administratoren können einen weiteren Drilldown durchführen, um Informationen nach Stadt und Bundesland anzuzeigen. Ab NetScaler ADM Version 12.0 und höher können Sie einen Drilldown zu Benutzern durchführen, die von einem Geostandort aus verbunden sind.

Die folgenden Details können auf der Weltkarte in HDX Insight angezeigt werden, und die Dichte jeder Metrik wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Bytes insgesamt



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Lizenzansicht Berichte und Metriken

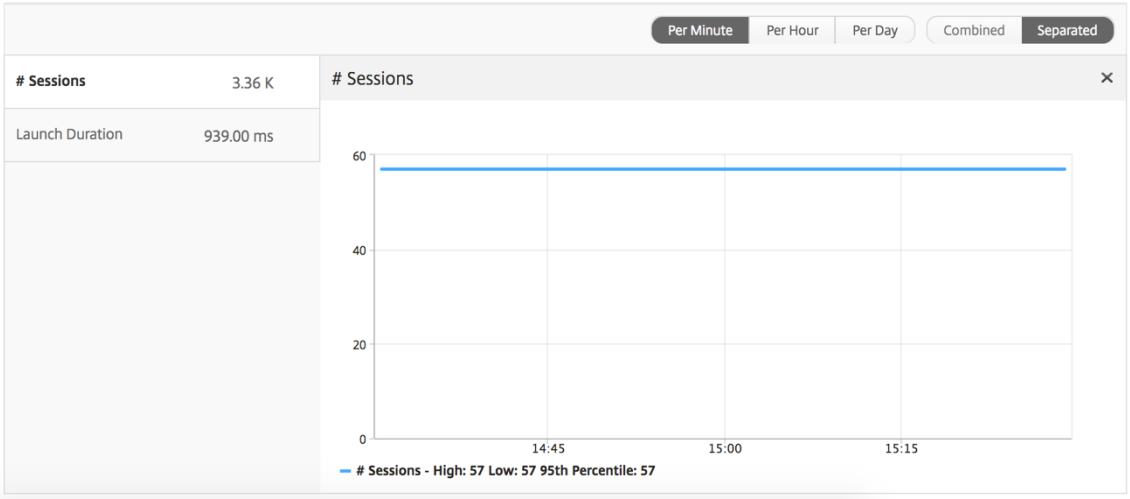
Die Lizenzansicht enthält Details zu den NetScaler Gateway -Lizenzinformationen.

So navigieren Sie zur Lizenzansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics > HDX Insight > Lizenzen**.

Liniendiagramm

Metriken	Beschreibung
Verwendete Lizenzen	Die NetScaler Gateway CCU-Lizenzen, die während der ausgewählten Zeitleiste verwendet werden. Jede Zählung steht für die Anzahl der Benutzersitzungen. Dies ist unabhängig von den Anwendungs- und Desktopsitzungen, die von diesem Benutzer gestartet wurden.
Gesamtzahl der Lizenzen	Gesamtanzahl der NetScaler Gateway CCU-Lizenzen, die für den Kunden verfügbar sind.



Bericht "Schwellenwert" Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* im ausgewählten Zeitraum als Lizenz ausgewählt wurde. Weitere Informationen finden Sie unter Erstellen von Schwellenwerten.

Berichte und Metriken der Anwendungsansicht

February 5, 2024

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf Citrix Virtual Apps.

So navigieren Sie zur Anwendungsansicht:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Anwendungen**.

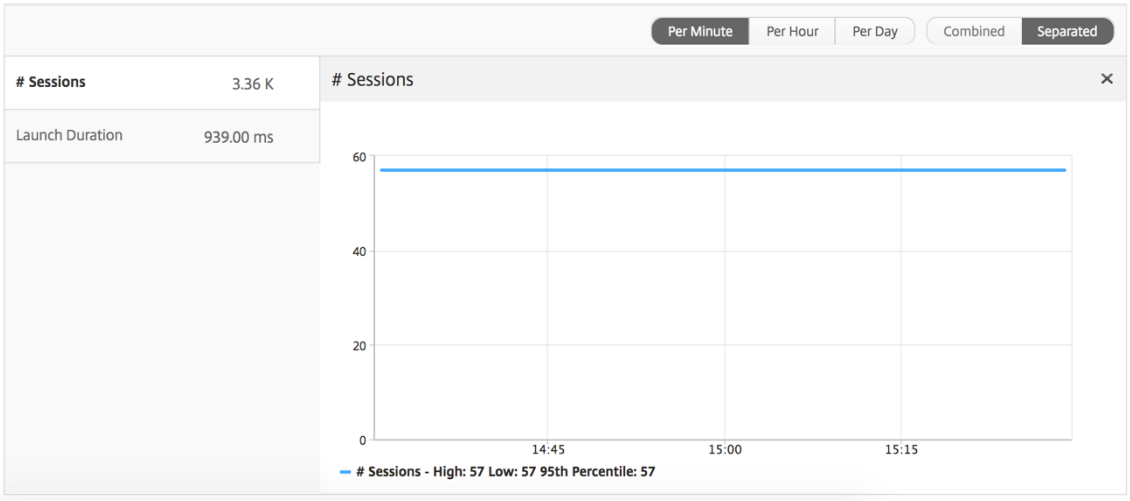
Übersichtsansicht

In der Zusammenfassungsansicht werden die Berichte für alle Anwendungen angezeigt, die während der ausgewählten Zeitachse angemeldet sind.

Alle unten aufgeführten Metriken/Berichte haben, sofern nicht ausdrücklich erwähnt, die entsprechenden Werte für den ausgewählten Zeitraum.

Liniendiagramm

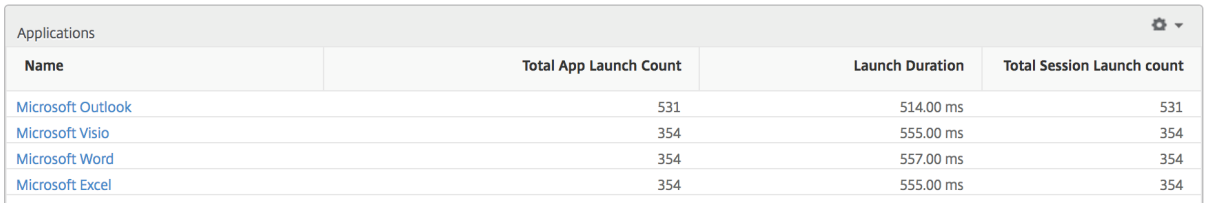
Metriken	Beschreibung
Anzahl Sitzungen	Gesamtzahl der Sitzungen während eines bestimmten Zeitintervalls.
Dauer des Starts	Durchschnittliche Zeit zum Starten einer Anwendung.



Zusammenfassender Bericht für Anwendungen

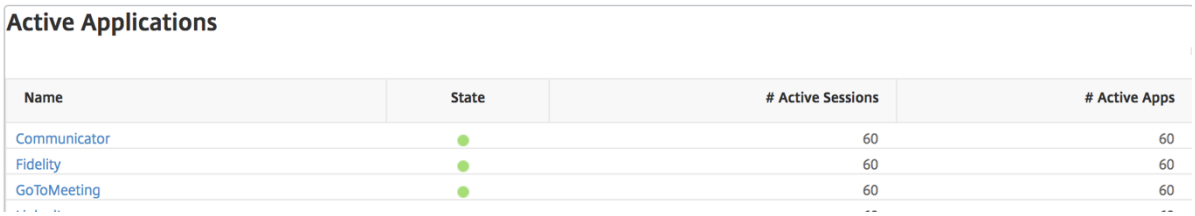
Metriken	Beschreibung
Name	Name der Citrix Virtual App.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual App-Sitzungen während des angegebenen Zeitintervalls.

Metriken	Beschreibung
App-Starts insgesamt	Gesamtzahl der Citrix Virtual App-Anwendungen, die während des angegebenen Zeitintervalls gestartet wurden.
Startdauer	Durchschnittliche Zeit für den Start der Citrix Virtual App.



Bericht über aktive Anwendungen

Metriken	Beschreibung
Name	Name der Citrix Virtual App.
Status	Zeigt den Status der Anwendung an: Grün-Aktiv, Rot-Inaktiv
Anzahl aktiver Sitzungen	Anzahl der aktiven Benutzersitzungen, die diese App während eines bestimmten Zeitintervalls verwenden.
Anzahlt aktiver Apps	Anzahl der aktiven Sitzungen für diese Anwendung.

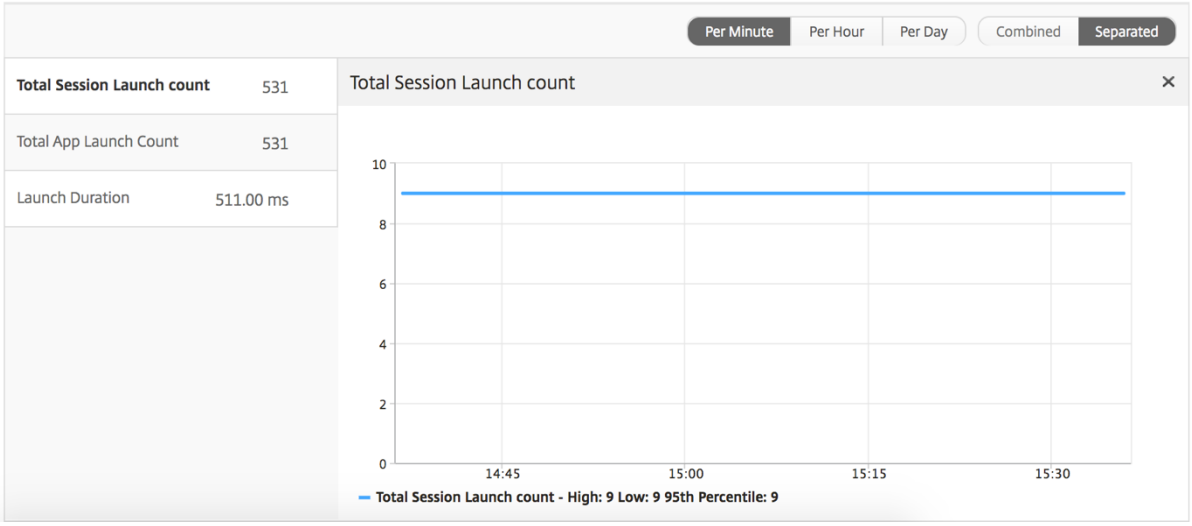


Bericht “Schwellenwert”

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* im ausgewählten Zeitraum als Anwendung ausgewählt wurde. Weitere Informationen finden Sie unter So erstellen Sie Schwellenwerte und Warnungen .

Liniendiagramm

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Dauer des Starts	Durchschnittliche Zeit zum Starten einer Anwendung.



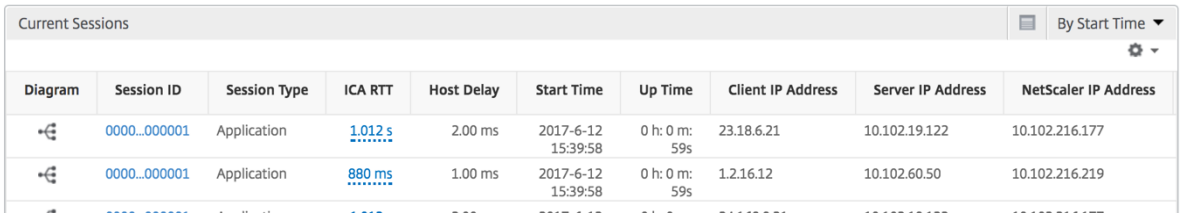
Bericht zu aktuellen Sitzungen

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der durch die Citrix ADCs fließt, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.

Metriken	Beschreibung
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Receiver-Typ: Citrix Windows Client und so weiter
Clientversion	Receiver-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway-Benutzer/Transparentmodus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet wurde.
USB-Status	Aktiv/Inaktiv - Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.

Metriken	Beschreibung
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zu Backend-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.

Metriken	Beschreibung
Benutzername	Der Benutzername des Benutzers, der auf diese bestimmte Citrix Virtual App zugreift.
Sitzungs-ID	Eindeutige Kennung für die Citrix Virtual App-Sitzung.
Sitzungstyp	Wird “Anwendung”sein.
Status	Sitzungsstatus: Grün für aktiv, Rot für Inaktiv.
Maximale Verletzungslatenz	Der höchste Wert der L7-Latenz, wenn ein definierter Schwellenwert für ein festgelegtes Zeitintervall überschritten wird.
Durchschnittliche Latenz bei Sicherheitsverletzungen	Der Durchschnittswert der L7-Latenz, wenn sich das System in einem Zustand “L7-Latenz verletzt”befindet.
Anzahl von L7-Schwellenwertverletzungen	Gibt an, wie oft eine L7-Schwellenverletzung aufgetreten ist.
L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der NetScaler ADC-Instanz beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.
L7 Serverseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem NetScaler ADC Gerät und der Citrix Virtual App beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.



Sitzungsansicht pro Anwendung

Die Session-Ansicht pro Anwendung zeigt Berichte für eine bestimmte ausgewählte Anwendungssitzung an.

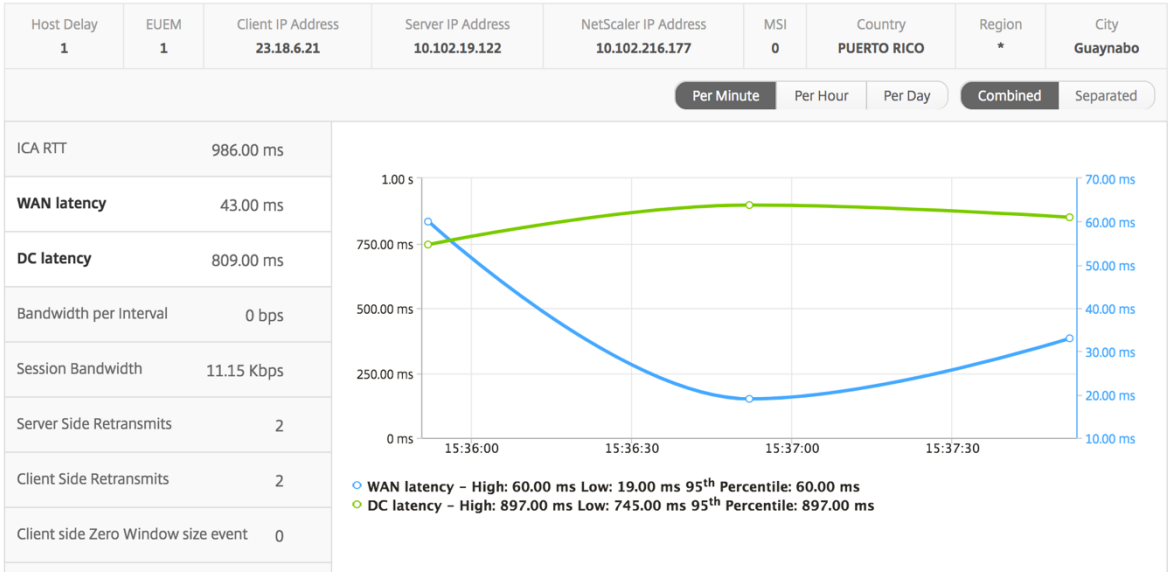
So zeigen Sie die Sitzungsberichte an:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Anwendungen**.
2. Wählen Sie im Anwendungsübersichtsbericht einen bestimmten Benutzer aus.
3. Eine Sitzung aus dem Bericht über aktuelle Sitzungen ausgewählt.

Liniendiagramm

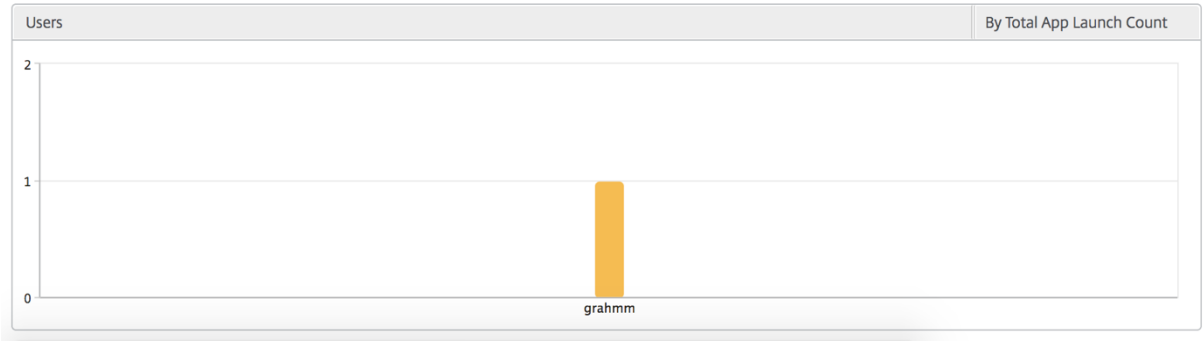
Metriken	Beschreibung
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
Serverseitiges Ereignis mit Zero Window-Größe	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zu Backend-Servern.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.

Metriken	Beschreibung
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.



Benutzerbalkendiagramm

Das Balkendiagramm des Benutzers stellt die Benutzer dar, die in dieser speziellen App angemeldet sind.



Desktop-View-Berichte und Metriken

February 5, 2024

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf Citrix Virtual Desktops.

So navigieren Sie zur Desktopansicht:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Desktop**.

Übersichtsansicht

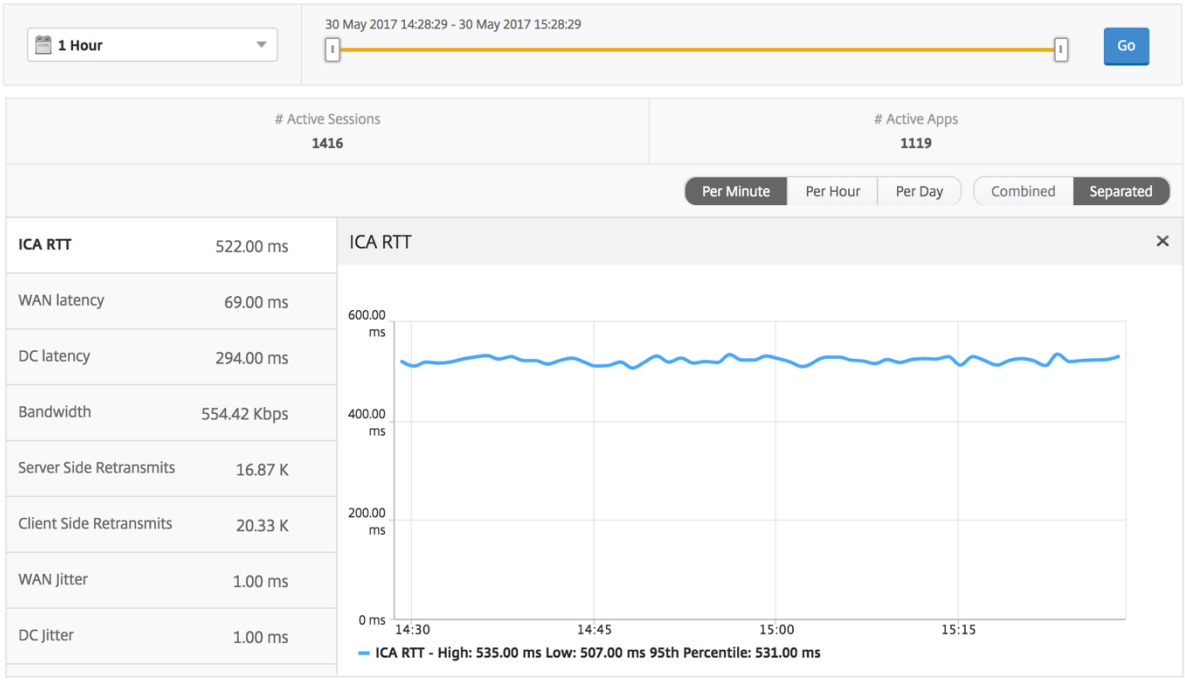
In der Zusammenfassungsansicht werden die Berichte für alle Citrix Virtual Desktops angezeigt, die während der ausgewählten Zeitleiste angemeldet sind.

Alle Metriken/Berichte, sofern nicht ausdrücklich erwähnt, haben die Werte, die ihnen für den ausgewählten Zeitraum entsprechen.

Liniendiagramm

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.

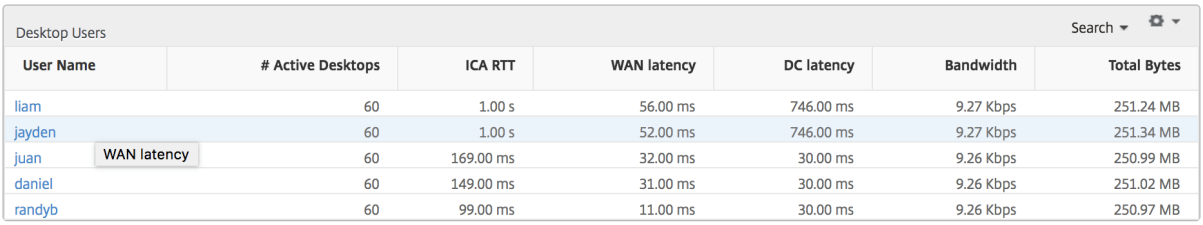
Metriken	Beschreibung
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.



Desktop-Sammelbericht

Metriken	Beschreibung
Aktive Sitzungen	Gesamtzahl der aktiven Citrix Virtual Desktop-Sitzungen während eines bestimmten Zeitintervalls.
Aktive Desktops	Gesamtzahl der aktiven Citrix Virtual Desktops in einem bestimmten Zeitintervall.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.

Metriken	Beschreibung
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.



Bericht “Schwellenwert”

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* in der ausgewählten Periode als Desktop ausgewählt wurde. Weitere Informationen finden Sie unter So erstellen Sie Schwellenwerte und Warnungen .

Pro Desktop-Ansicht

Die Ansicht pro Desktop bietet detaillierte Berichte zur Endbenutzererfahrung für einen ausgewählten Citrix Virtual Desktop.

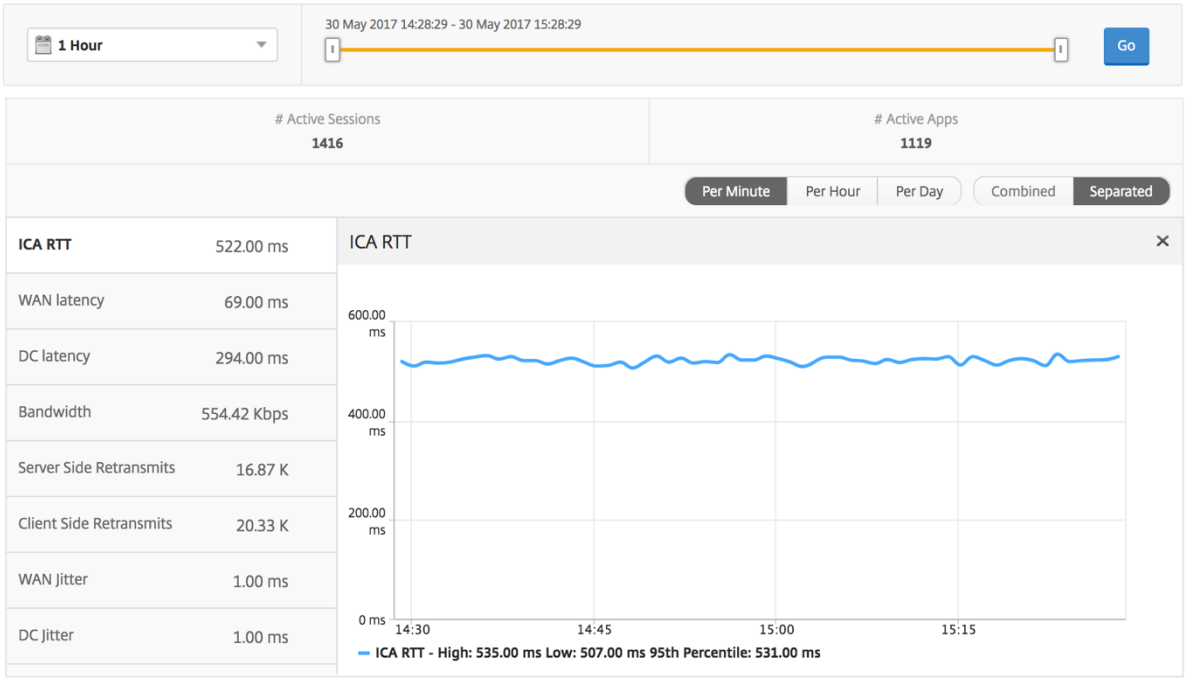
So navigieren Sie zur jeweiligen Desktop-Ansicht:

1. Navigieren Sie zu **Analytics > HDX Insight > Desktop**.
2. Wählen Sie im **Desktop-Zusammenfassungsberichteinen bestimmten Desktop**aus.

Liniendiagramm

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.

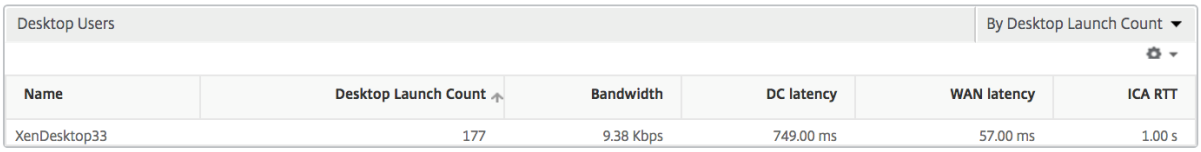
Metriken	Beschreibung
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.



Bericht für Desktopbenutzer

Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zu Backend-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.



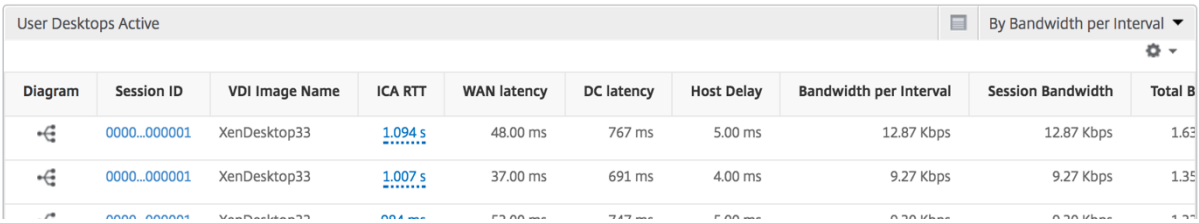
Benutzerdesktops Aktiv/Inaktiv Bericht

Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der durch die NetScaler ADCs geleitet wird, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Receiver-Typ: Citrix Windows Client und so weiter
Clientversion	Receiver-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.

Metriken	Beschreibung
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway-Benutzer/Transparentmodus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet wurde.
USB-Status	Aktiv/Inaktiv - Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die auf Citrix Virtual Apps bzw. Desktops gehostet werden.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zu Backend-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.

Metriken	Beschreibung
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
VDI-Imagename	Name des Citrix Virtual Desktop, mit dem der Benutzer verbunden ist
Diagramm	



Ansicht pro Desktop-Sitzung

Pro Desktop-Sitzungsansicht stellt Berichte für eine bestimmte ausgewählte Citrix Virtual Desktop-Sitzung bereit.

So navigieren Sie zur Desktop-Sitzungsansicht:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Desktop**.
2. Wählen Sie im **Desktopübersichtsbericht einen bestimmten Desktop**aus.
3. Wählen Sie eine Sitzung aus dem Bericht über aktuelle Sitzungen aus.

Zeitleistendiagramm

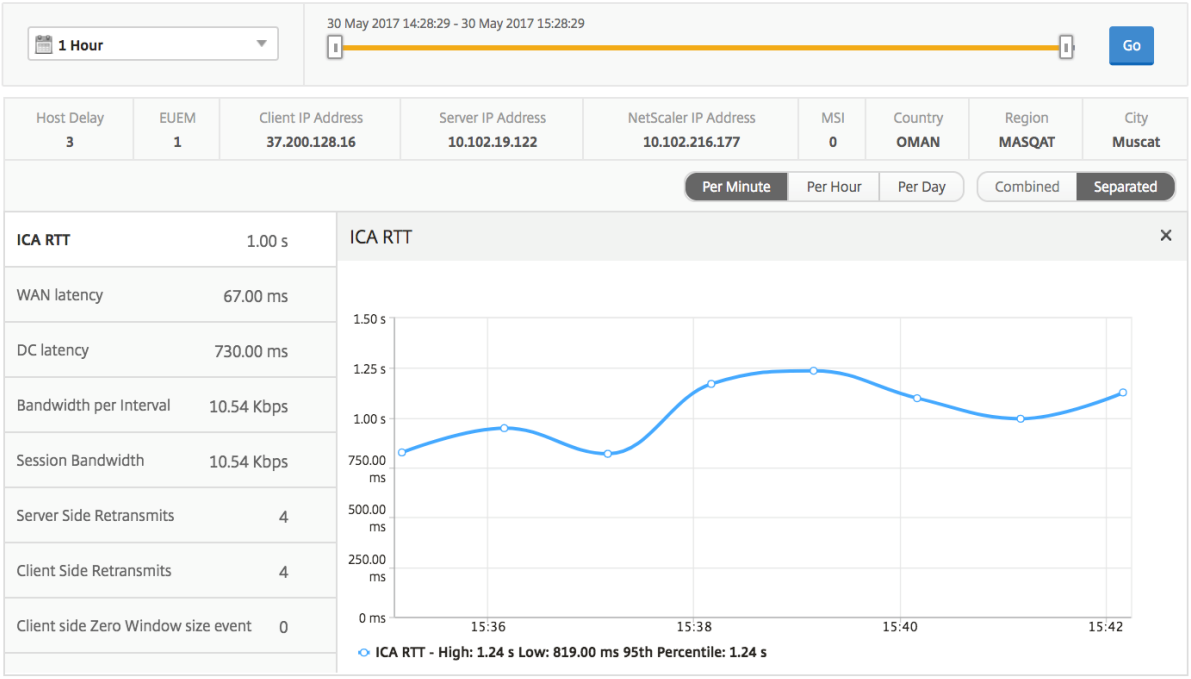
Die Sitzungsansicht pro Benutzer bietet Berichte für die Sitzung eines bestimmten ausgewählten Benutzers.

So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**.
2. Wählen Sie im Abschnitt **Benutzerübersichtsbericht** einen bestimmten Benutzer aus.
3. Wählen Sie in der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** eine Sitzung aus.

Metriken	Beschreibung
Wiederverbindung der Sitzung	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App and Desktop-Sitzungen an.
ACR-Anzahl	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die auf Citrix Virtual App bzw. Desktop gehostet werden.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zu Backend-Servern.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.

Metriken	Beschreibung
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.



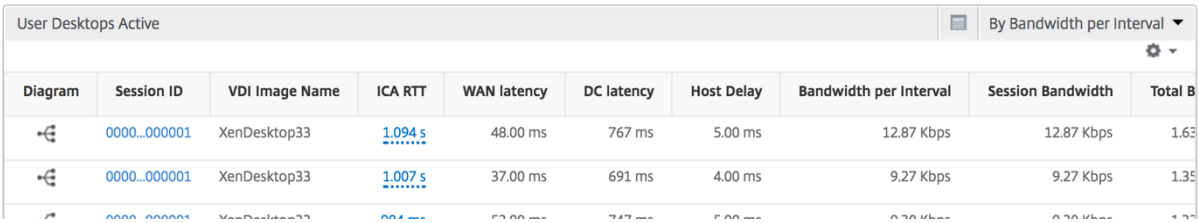
Bericht zu verwandten Desktopsitzungen

Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der durch die Citrix ADCs fließt, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.

Metriken	Beschreibung
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Receiver-Typ: Citrix Windows Client und so weiter
Clientversion	Receiver-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler ADC Gateway Benutzer/transparenter Modus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet wurde.
USB-Status	Aktiv/Inaktiv - Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde vom Benutzer beendet.

Metriken	Beschreibung
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zu Backend-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Serverseitige Neuübertragungen	Die Anzahl der erneut auf der Verbindung zwischen NetScaler ADC und Backend-Server übertragenen Pakete.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Häufigkeit, mit denen das Timeout für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Backend-Server aufgetreten ist.
VDI-Imagename	Name des Citrix Virtual Desktop, mit dem der Benutzer verbunden ist

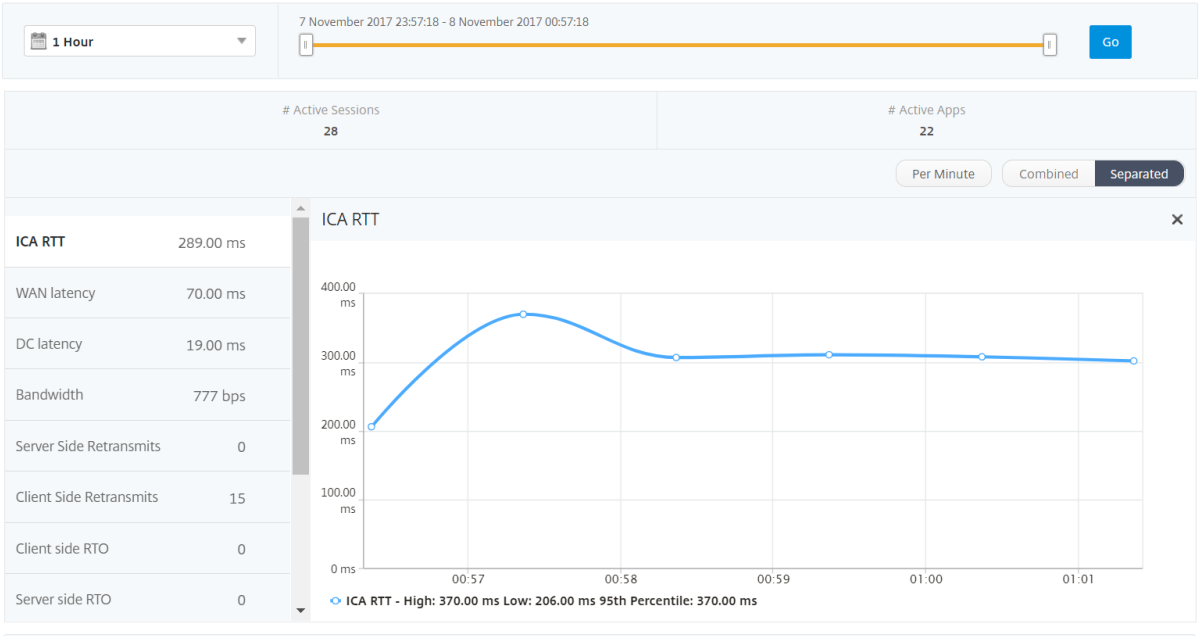


Berichte und Metriken der Benutzeransicht

February 5, 2024

Die Berichte und Metriken in dieser Ansicht werden pro Citrix Virtual Apps und Desktop-Benutzer angezeigt.

Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**.



Übersichtsansicht

In der Zusammenfassungsansicht werden die Berichte für alle Benutzer angezeigt, die sich während der ausgewählten Zeitleiste angemeldet haben. Alle Metriken/Berichte in dieser Ansicht zeigen die ihnen entsprechenden Werte für den ausgewählten Zeitraum an, sofern nicht anders angegeben.

So ändern Sie den ausgewählten Zeitraum:

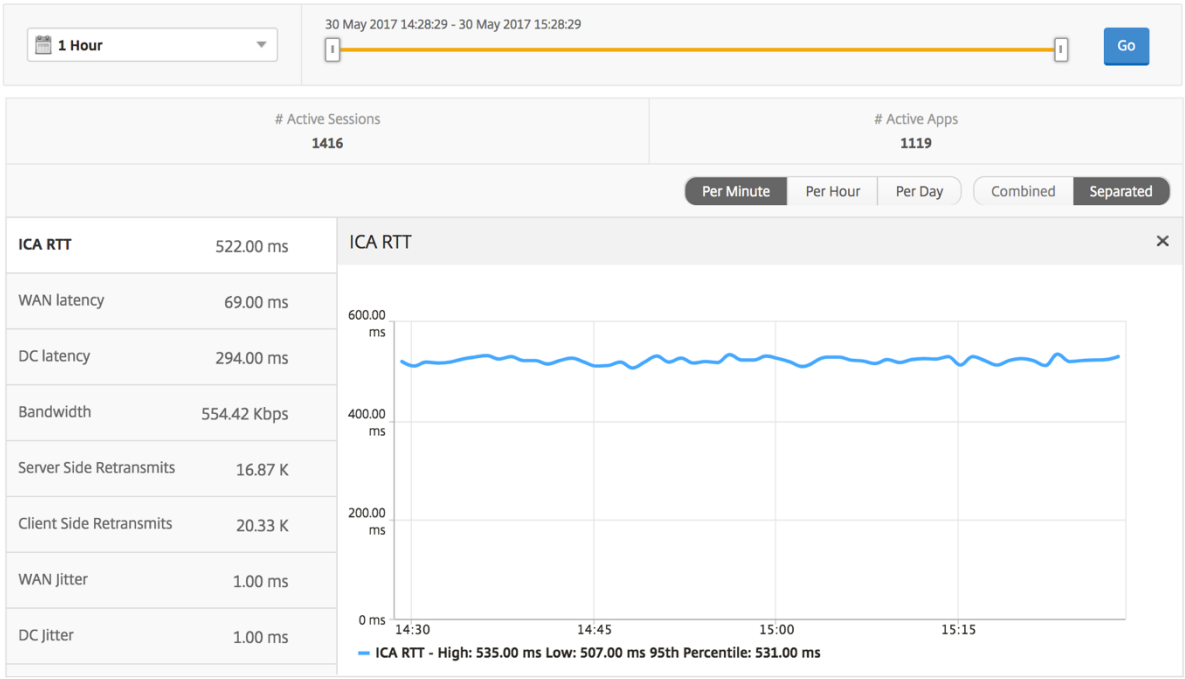
1. Verwenden Sie die Zeitraumeliste oder den Zeitschieberegler, um das gewünschte Zeitintervall einzustellen.

2. Klicken Sie auf **Go**.

Liniendiagramm

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App and Desktop-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis hin zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.

Metriken	Beschreibung
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und Backend-Server.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.



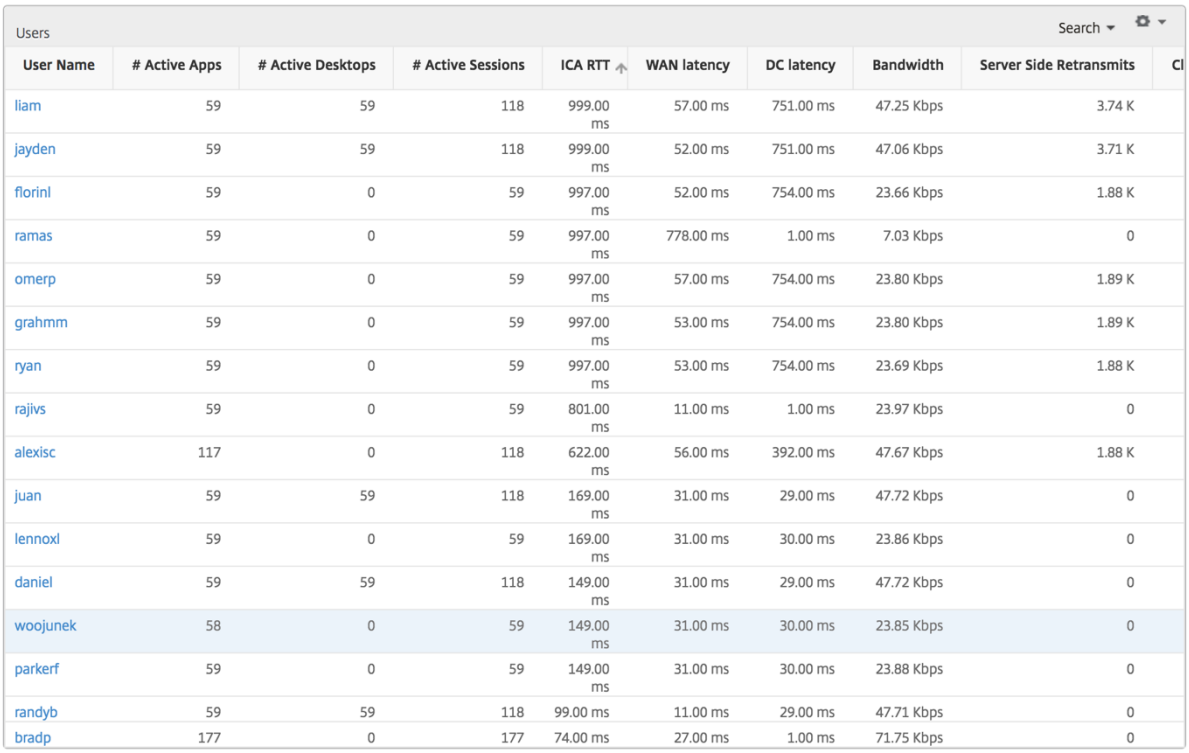
Bericht “Benutzerzusammenfassung”

Im Folgenden finden Sie die Metriken, die für diesen Bericht spezifisch sind.

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App and Desktop-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.

Metriken	Beschreibung
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis hin zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und Backend-Server.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
App-Starts insgesamt	Gesamtzahl der Apps, die vom Benutzer während des ausgewählten Zeitraums gestartet wurden.

Metriken	Beschreibung
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Aktive Desktops	Gesamtzahl der aktiven Citrix Virtual Desktops in einem bestimmten Zeitintervall.



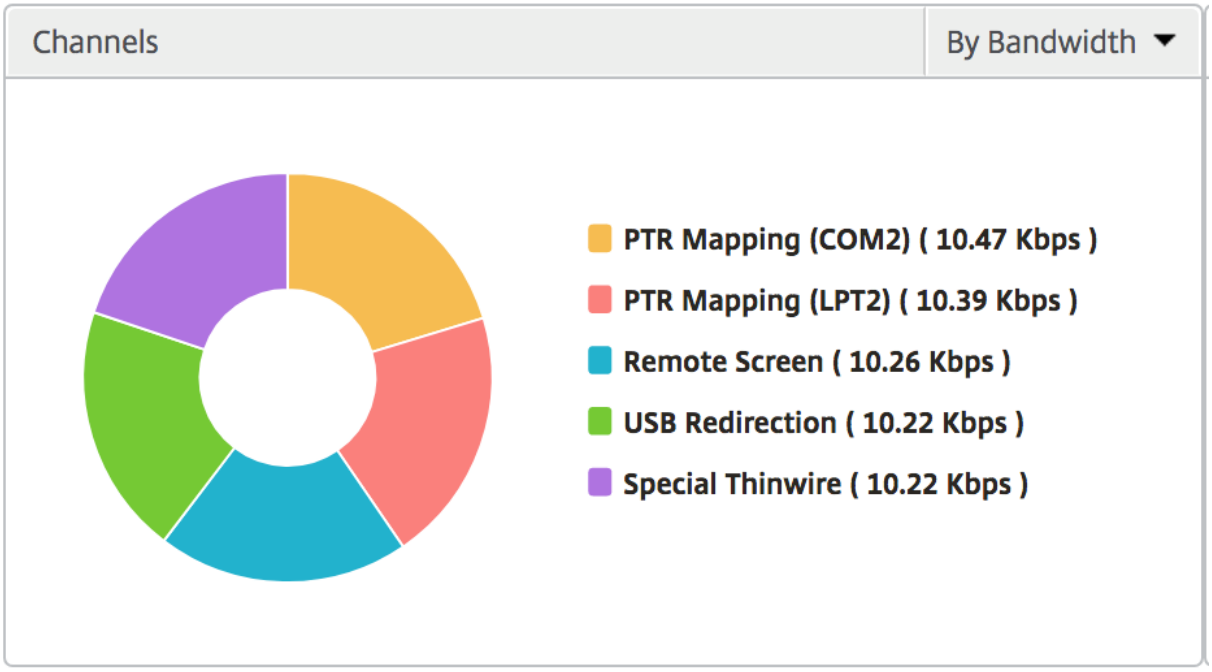
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

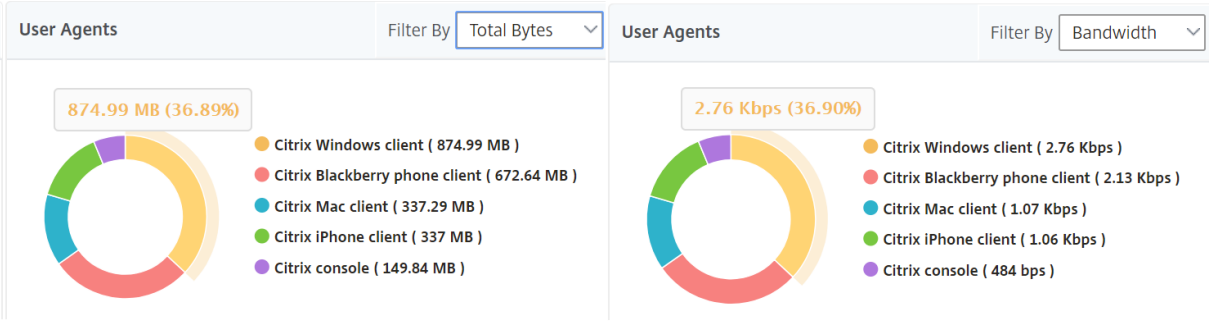
Kanäle

Kanäle stellen die Gesamtbandbreite oder die Gesamtzahl der von jedem virtuellen ICA-Kanal verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Benutzer-Agenten

Benutzeragenten stellen die gesamte Bandbreite/Gesamtanzahl der von jedem Endpunkt verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Anzahl der Schwellenwertverstöße

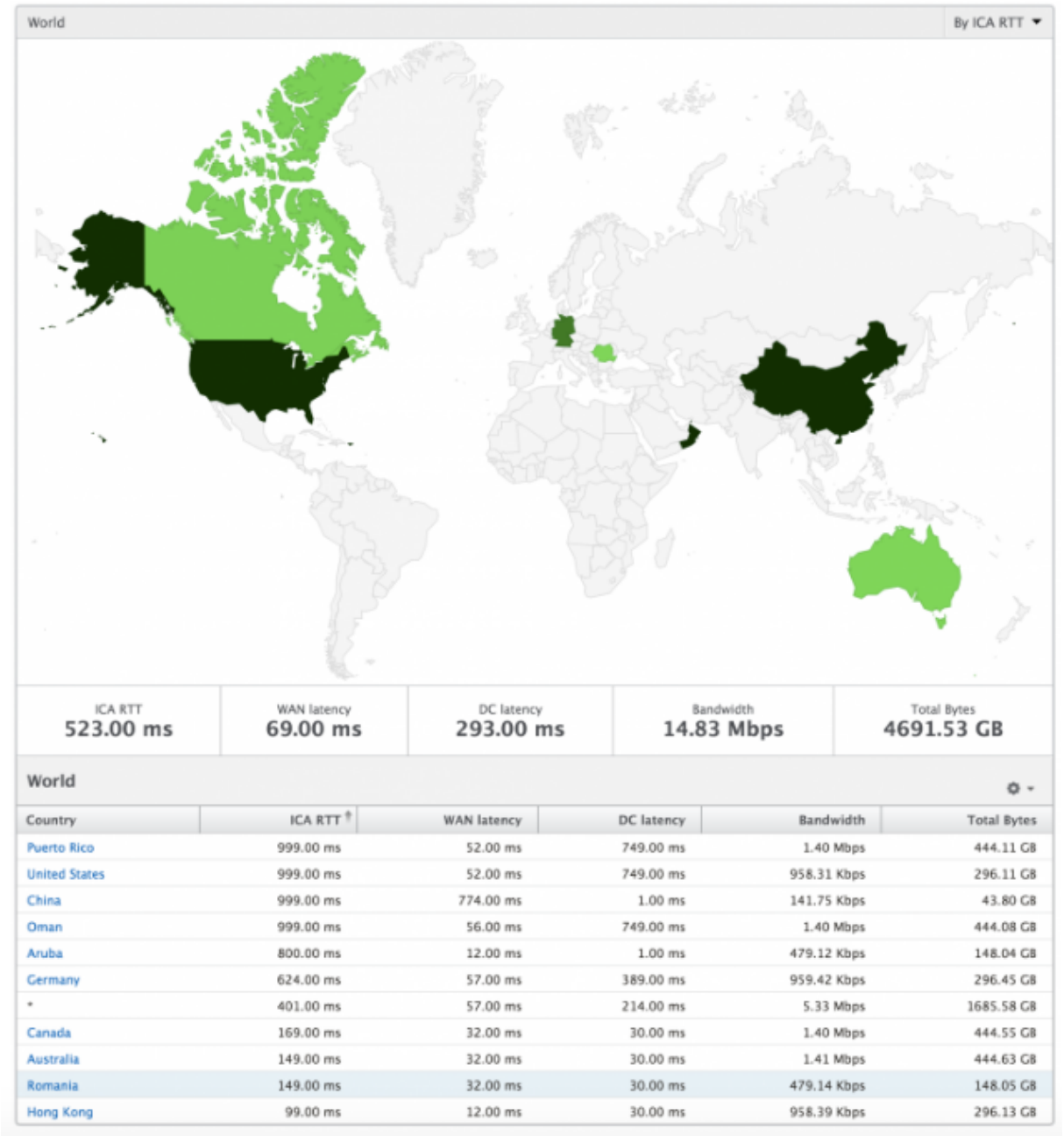
Die Metriken für die Anzahl der Schwellenwertverstöße stellen die Anzahl der Schwellenwerte dar, die im ausgewählten Zeitraum überschritten wurden. Weitere Informationen finden Sie unter So erstellen Sie Schwellenwerte und Warnmeldungen.

Weltkarte

Mit der Weltkartenansicht in HDX Insight können Administratoren die historischen und aktiven Benutzerdetails aus geografischer Sicht anzeigen. Die Administratoren können eine Weltanschauung des Systems, Drilldown zu einem bestimmten Land und weiter in die Städte als auch durch Klicken auf die Region. Die Administratoren können einen weiteren Drilldown durchführen, um Informationen nach Stadt und Bundesland anzuzeigen. Ab NetScaler ADM Version 12.0 und höher können Sie einen Drilldown zu Benutzern durchführen, die von einem Geostandort aus verbunden sind.

Die folgenden Details können auf der Weltkarte in HDX Insight angezeigt werden, und die Dichte jeder Metrik wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Bytes insgesamt



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Ansicht pro Benutzer

Die Ansicht pro Benutzer bietet detaillierte Berichte über die Endbenutzererfahrung für einen bestimmten ausgewählten Benutzer.

So navigieren Sie zu den Metriken eines bestimmten Benutzers:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**.
2. Wählen Sie im Übersichtsbericht Benutzer einen bestimmten Benutzer aus.

Liniendiagramm

Das Liniendiagramm zeigt eine Zusammenfassung aller Metriken für den ausgewählten Benutzer während des ausgewählten Zeitraums an.

Bericht über aktuelle/abgeschlossene Sitzungen

Dieser Bericht bezieht sich auf alle aktuellen/beendeten Benutzersitzungen für den ausgewählten Benutzer. Diese Metriken können nach Startzeit, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der durch die NetScaler ADCs geleitet wird, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual App-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Receiver-Typ: Citrix Windows Client und so weiter
Clientversion	Receiver-Version.

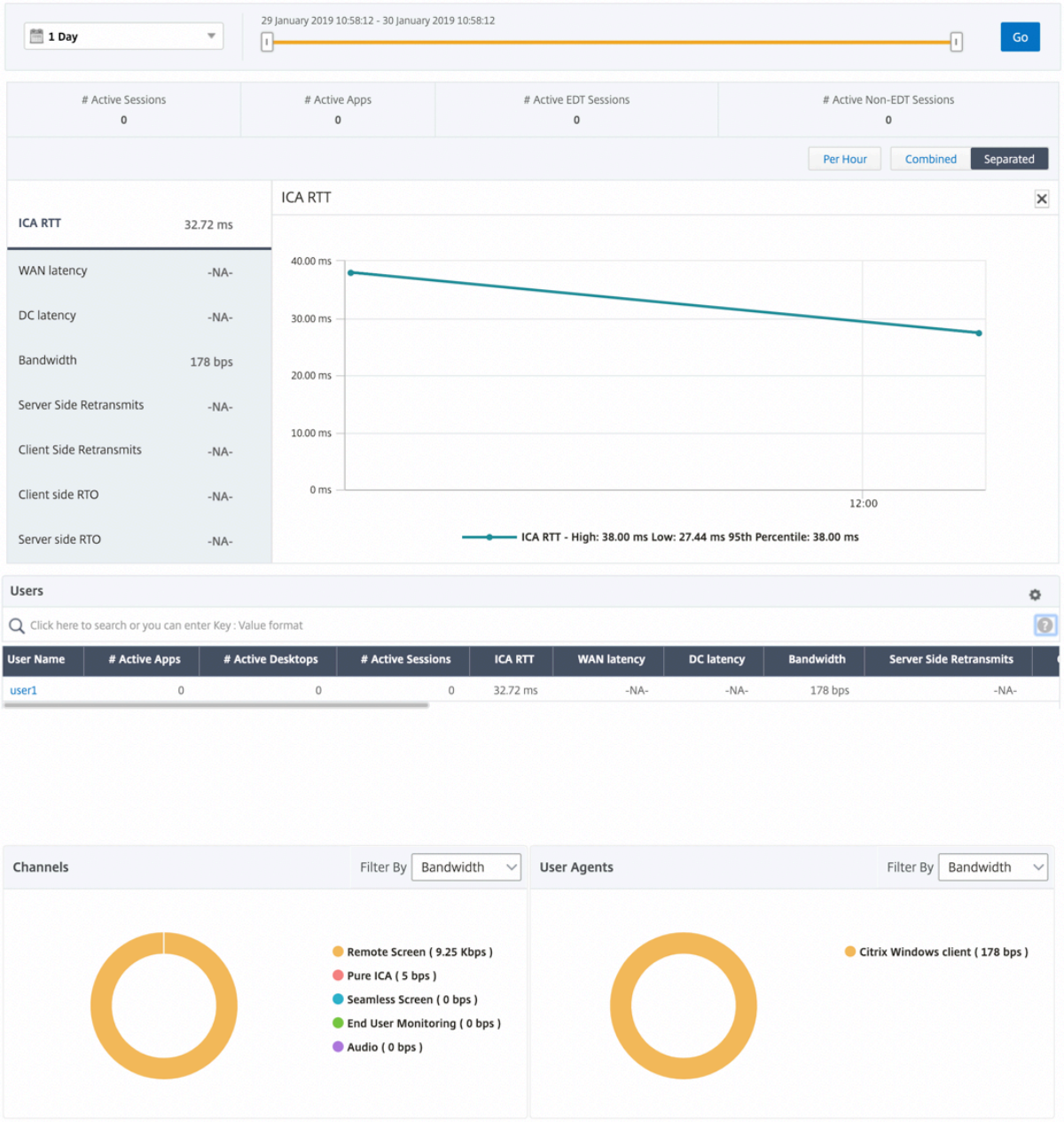
Metriken	Beschreibung
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
Typ des Benutzerzugriffs	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway-Benutzer/Transparentmodus.
Land	Land, von dem aus die Sitzung eingerichtet wurde.
Region	Region, von der aus die Sitzung eingerichtet wurde.
Ort	Stadt, von der aus die Sitzung eingerichtet wurde.
USB-Status	Aktiv/Inaktiv - Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der gestoppten USB-Instanzen	Die Anzahl der USB-Instanzen wurde gestoppt.
Hostname des Kunden	Der Hostname des Kunden.
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis hin zu Backend-Servern.

Metriken	Beschreibung
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und Backend-Server.

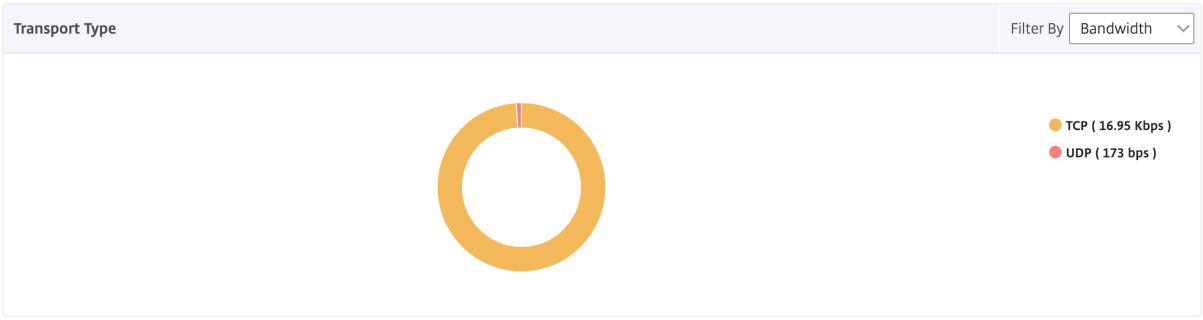
Unterstützung für EDT in HDX Insight

NetScaler Application Delivery Management (ADM) unterstützt jetzt Enlightened Data Transport (EDT) zur Anzeige von Analysen für HDX Insight. Das heißt, ADM unterstützt jetzt sowohl das UDP- als auch das TCP-Protokoll. Die EDT-Unterstützung für NetScaler Gateway gewährleistet eine hochauflösende Benutzererfahrung virtueller Desktops während der Sitzung für Benutzer, die Citrix Receiver ausführen.

HDX Insight zeigt jetzt die Anzahl der EDT-Sitzungen und Nicht-EDT-Sitzungen als Teil des Berichts über aktive Sitzungen an. In der Tabelle Benutzer wird ein detaillierter Bericht aller Benutzer im System angezeigt. Die Tabelle zeigt Metriken wie WAN-Latenz, DC-Latenz, Rückübertragungen und RTOs. Einige dieser Metriken sind für Benutzer mit EDT-Sitzungen nicht verfügbar, da sie derzeit anhand des TCP-Stacks berechnet werden. Daher erscheinen sie als “NA”.

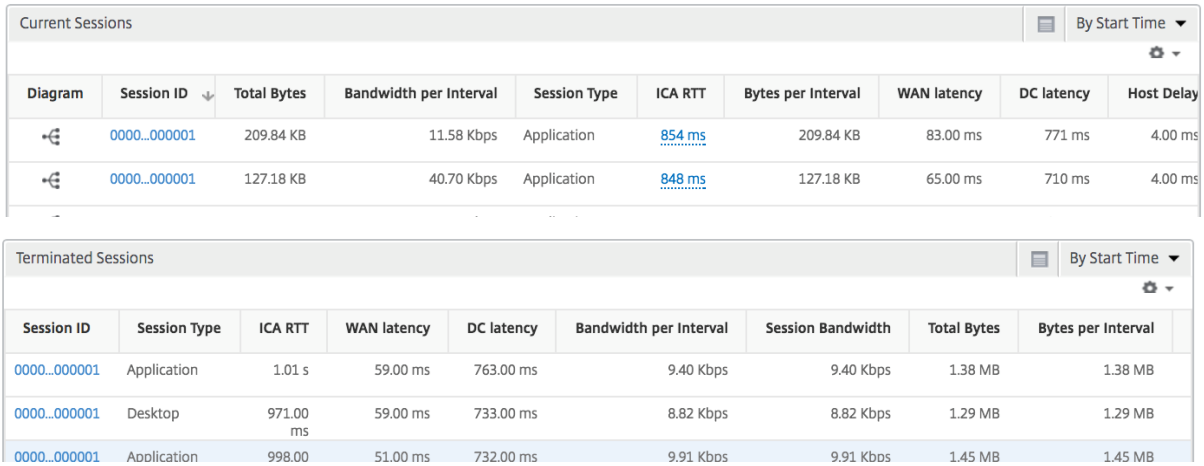


Es wurde ein neues Donutdiagramm eingeführt, mit dem Sie die vom Benutzer verbrauchte Bandbreite und die Gesamtzahl der Bytes basierend auf dem von den Benutzern verwendeten Protokolltyp sehen können.



HDX Insight Metriken, die ab NetScaler ADM 12.0 und höher verfügbar sind:

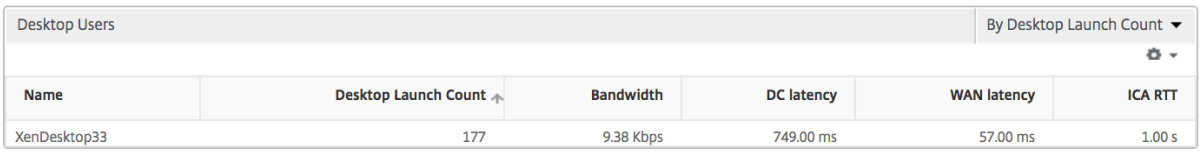
L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der NetScaler ADC-Instanz beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.
L7 Serverseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem NetScaler ADC Gerät und der Citrix Virtual App beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.
Maximale Verletzungslatenz	Der höchste Wert der L7-Latenz, wenn ein definierter Schwellenwert für ein festgelegtes Zeitintervall überschritten wird.
Durchschnittliche Latenz bei Sicherheitsverletzungen	Der Durchschnittswert der L7-Latenz, wenn sich das System in einem Zustand “L7-Latenz verletzt”befindet.
Anzahl von L7-Schwellenwertverletzungen	Gibt an, wie oft eine L7-Schwellenverletzung aufgetreten ist.



Desktopbenutzer

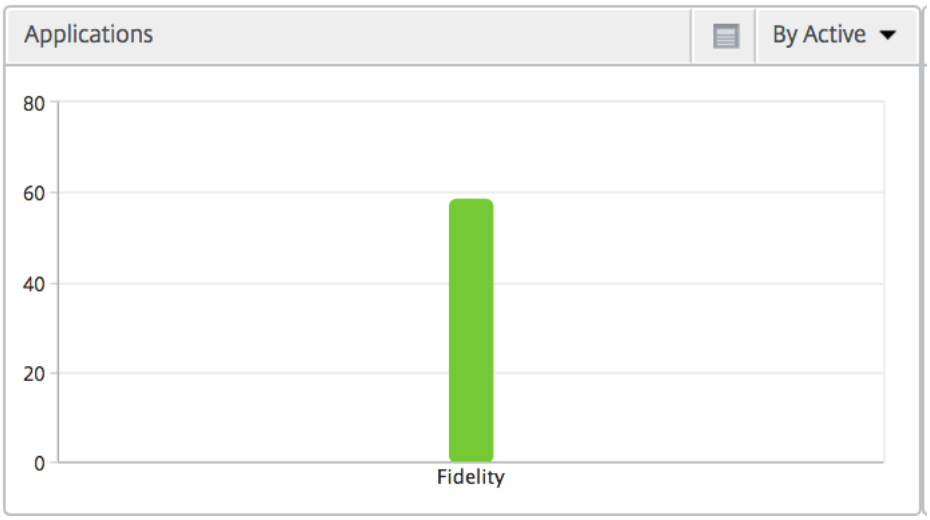
Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis hin zu Backend-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.



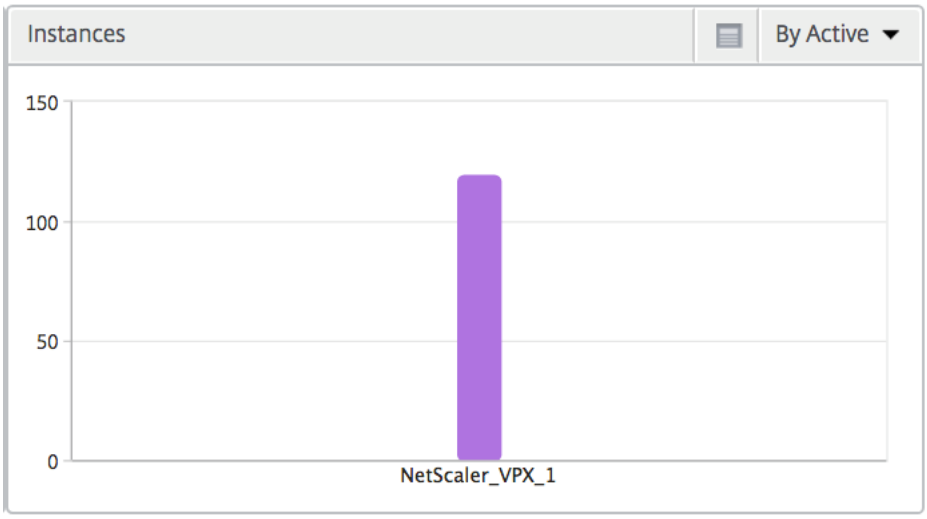
Anwendungen

Ein Balkendiagramm, das Apps sortiert nach Aktiv, Gesamtzahl der Sitzungsstarts, Gesamtanzahl des App-Starts und Startdauer darstellt.



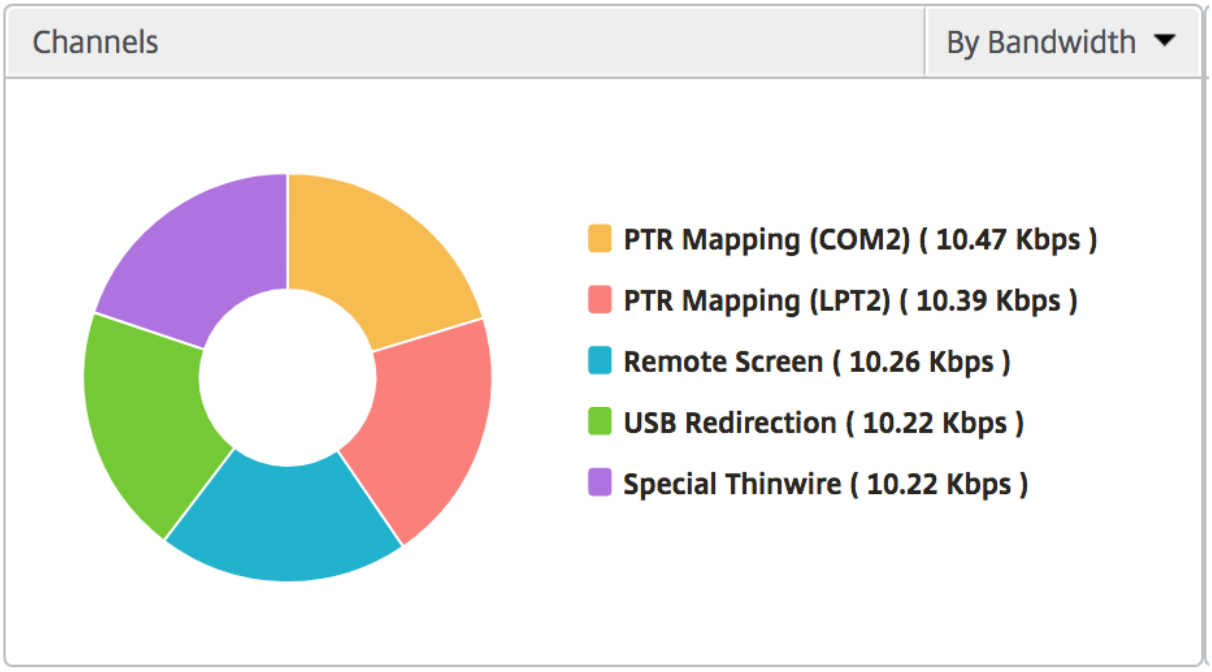
Instanzen

Ein Balkendiagramm, das NetScaler ADC Instanzen darstellt, sortiert nach Active und insgesamt Apps



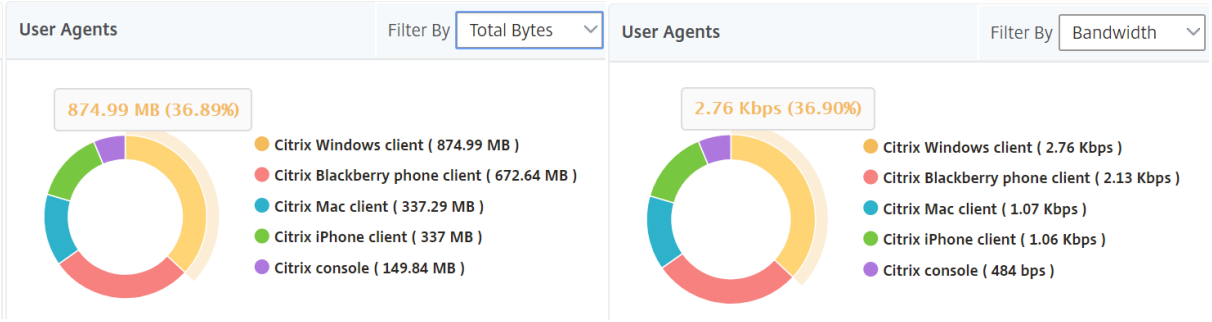
Kanäle

Kanäle stellen die Gesamtbandbreite oder die Gesamtzahl der von jedem virtuellen ICA-Kanal verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Benutzer-Agenten

Benutzeragenten stellen die gesamte Bandbreite/Gesamtanzahl der von jedem Endpunkt verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.



Sitzungsansicht pro Benutzer

Die Sitzungsansicht pro Benutzer bietet Berichte für die Sitzung eines bestimmten ausgewählten Benutzers.

So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

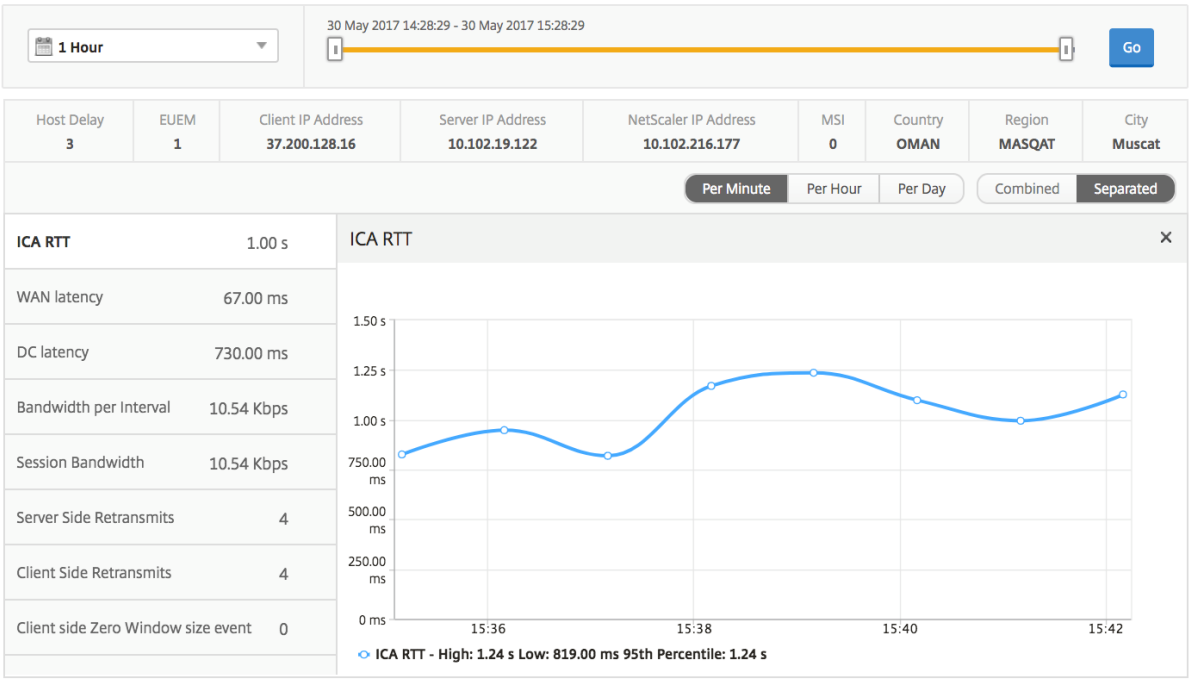
1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**.
2. Wählen Sie im Abschnitt **Benutzerübersichtsbericht** einen bestimmten Benutzer aus.

3. Wählen Sie in der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** eine Sitzung aus.

Zeitleistendiagramm

Metriken	Beschreibung
Wiederverbindung der Sitzung	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App and Desktop-Sitzungen an.
ACR-Anzahl	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis hin zu Backend-Servern.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und Backend-Server.

Metriken	Beschreibung
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.

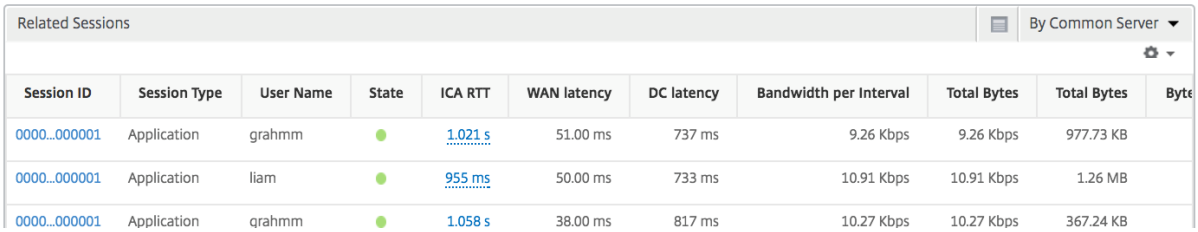


Aktive Anwendung

Im Abschnitt **Aktive Anwendungen** werden die aktiven Anwendungen des ausgewählten Benutzers angezeigt. Diese Anwendungen können auch nach Anzahl der aktiven Sitzungen und Startdauer sortiert werden.

Verwandte Sitzungen

Im Abschnitt “Sessions”werden die zugehörigen Sitzungen der Sitzungen des ausgewählten Benutzers angezeigt. Die Beziehung kann als gemeinsame Server oder gemeinsames NetScaler ADC ausgewählt werden.



Session ID	Session Type	User Name	State	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Total Bytes	Total Bytes	Byte
0000...000001	Application	grahmm		1.021 s	51.00 ms	737 ms	9.26 Kbps	9.26 Kbps	977.73 KB	
0000...000001	Application	liam		955 ms	50.00 ms	733 ms	10.91 Kbps	10.91 Kbps	1.26 MB	
0000...000001	Application	grahmm		1.058 s	38.00 ms	817 ms	10.27 Kbps	10.27 Kbps	367.24 KB	

Instanzansichtsberichte und -metriken

February 5, 2024

Die Berichte und Metriken in der Instanzansicht konzentrieren sich auf die NetScaler ADC Instanzen.

So navigieren Sie zur Instanzansicht:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Instanzen**.

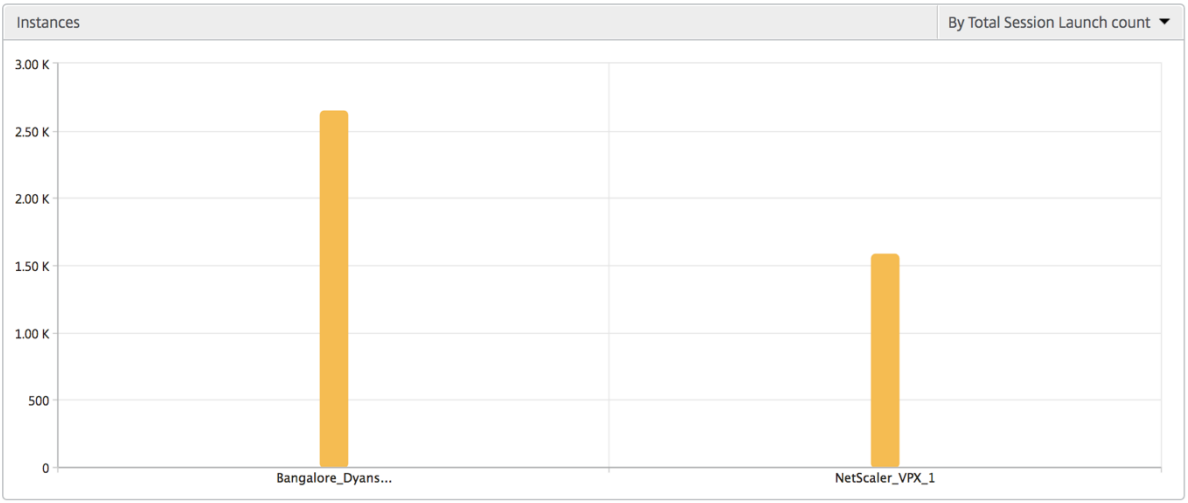
Instanz-Zusammenfassungsansicht

Diese Ansicht wird als Zusammenfassungsansicht bezeichnet, da sie die Berichte für alle NetScaler ADC Instanzen anzeigt, die NetScaler ADM hinzugefügt werden.

Alle Metriken/Berichte haben, sofern nicht ausdrücklich erwähnt, die ihnen entsprechenden Werte für den ausgewählten Zeitraum.

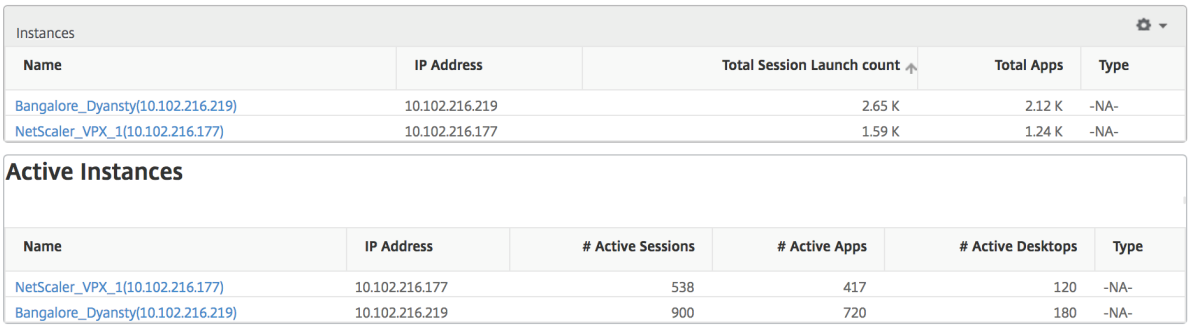
Instanz-Balkendiagramm

Dieses Diagramm zeigt die Instanz im Vergleich zur Gesamtzahl der Sitzungsstarts und der Gesamtzahl der Apps an, die in der Liste oben rechts auf der Diagrammfläche ausgewählt werden können.



Übersichtsbericht “Instanz/Aktive Instanzen”

Metriken	Beschreibung
Name	Hostname der NetScaler ADC-Instanz.
IP-Adresse	NetScaler-IP-Adresse.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der eindeutigen Benutzersitzungen, die während eines bestimmten Zeitintervalls erstellt wurden.
Apps insgesamt	Gesamtzahl der eindeutigen Anwendungen, die während eines bestimmten Zeitintervalls gestartet wurden.
Typ	–


Instances

Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

Bericht “Schwellenwert”

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* in der ausgewählten Periode als Instanz ausgewählt wurde. Weitere Informationen finden Sie unter So erstellen Sie Schwellenwerte und Warnungen .

Übersprungene Flows

Ein übersprungener Flow ist ein Datensatz, der die Parsing ICA-Verbindung übersprungen hat. Dies kann aus mehreren Gründen auftreten, z. B. bei der Verwendung nicht unterstützter Versionen von Citrix Virtual Apps and Desktops, einer nicht unterstützten Version des Receivers oder Receiver-Typs usw. Diese Tabelle zeigt die IP-Adresse und die Anzahl der übersprungenen Flows. Diese Empfänger dürfen nicht Teil von Receivern auf der Positivliste sein. Daher werden diese Sitzungen von der Überwachung übersprungen.

See **Error! Hyperlinkverweis ist nicht gültig** für weitere Details zu Problemen im Zusammenhang mit der ICA-Analyse.

Skipped Flows

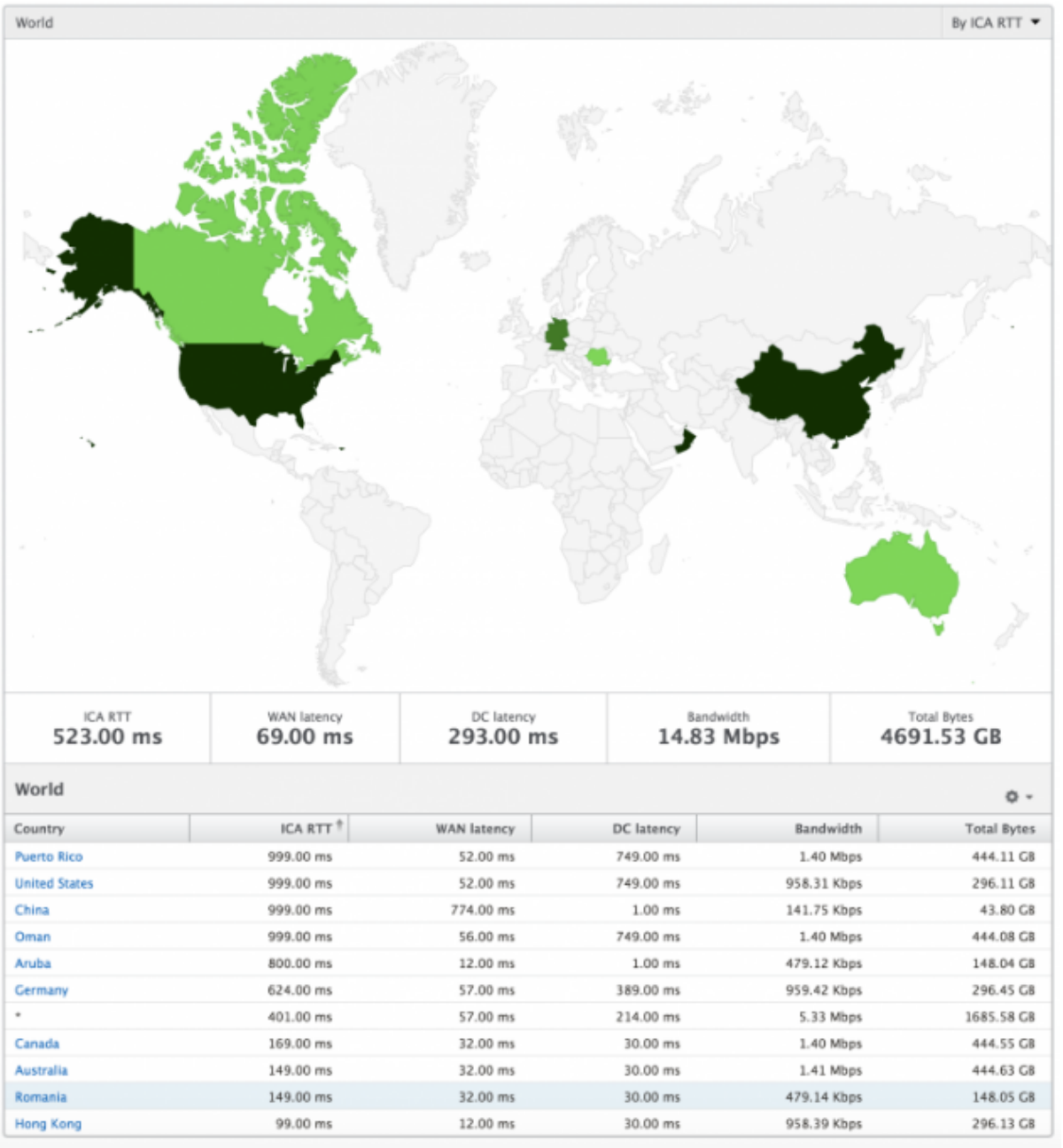
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

Weltansicht

Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die historischen und aktiven Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltanschauung des Systems, Drilldown zu einem bestimmten Land und weiter in die Städte als auch durch Klicken auf die Region. Die Administratoren können weitere Informationen nach Stadt und Bundesstaat anzeigen. Ab NetScaler ADC Version 12.0 und höher können Sie Benutzer aufschlüsseln, die von einem Geostandort aus verbunden sind.

Die folgenden Details können auf der Weltkarte in HDX Insight angezeigt werden, und die Dichte jeder Metrik wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Bytes insgesamt



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Ansicht pro Instanz

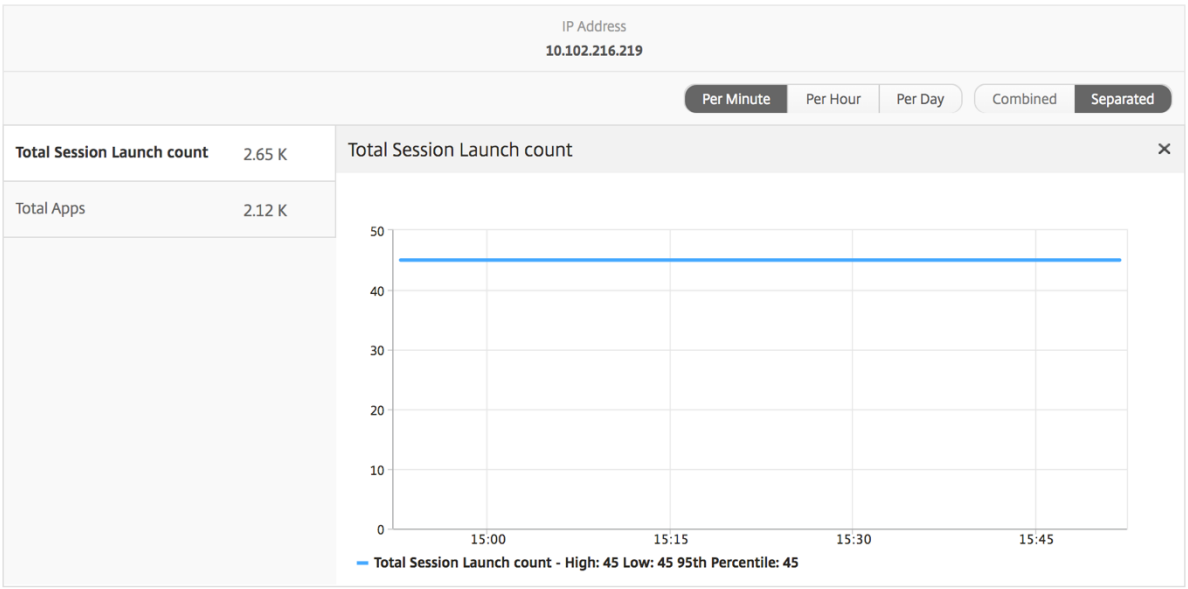
Die Ansicht pro Instanz bietet detaillierte Berichte über die Benutzererfahrung für eine bestimmte ausgewählte NetScaler ADC Instanz.

So navigieren Sie zur Instanzansicht:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Instanzen**.
2. Wählen Sie in der **Auswertung "Instanzübersicht"** eine bestimmte Instanz aus.

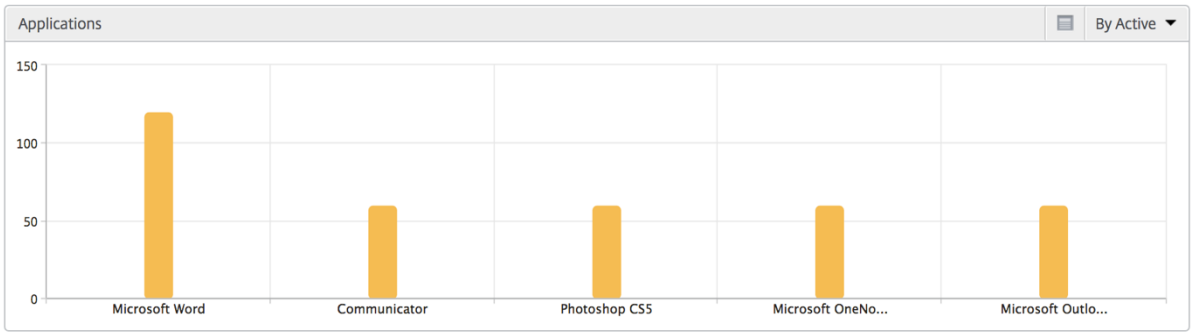
Liniendiagramm

Metriken	Beschreibung
IP-Adresse	Dies stellt die NetScaler-IP-Adresse der ausgewählten Instanz dar.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual App-Sitzungen während des angegebenen Zeitintervalls.
Apps insgesamt	Gesamtzahl der eindeutigen Anwendungen, die während eines bestimmten Zeitintervalls gestartet wurden.



Balkendiagramm für Anwendungen

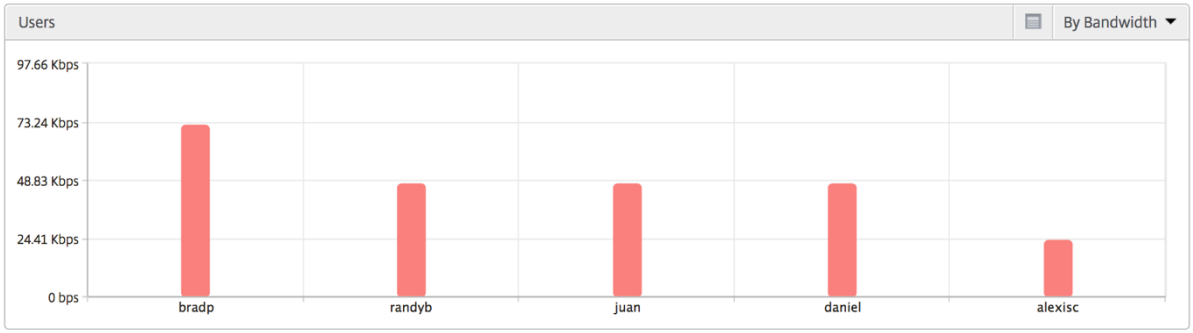
Zeigt die 5 wichtigsten Anwendungen basierend auf den folgenden Kriterien an: nach aktiven Apps, Gesamtzahl der Sitzungsstarts, Gesamtzahl der App-Startstarts oder Startdauer.



Balkendiagramm “Benutzer”

Das Balkendiagramm “Benutzer”zeigt die fünf wichtigsten Benutzer anhand der folgenden Kriterien an:

- Bandbreite
- WAN-Latenz
- DC-Latenz
- ICA RTT

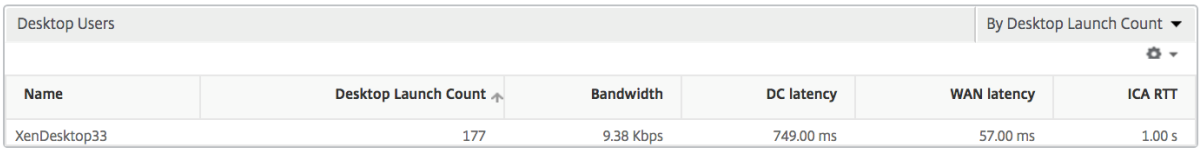


Bericht für Desktopbenutzer

Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.

Metriken	Beschreibung
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zu Backend-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler ADC bis zum Endbenutzer.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual App bzw. Desktop gehostet wird.

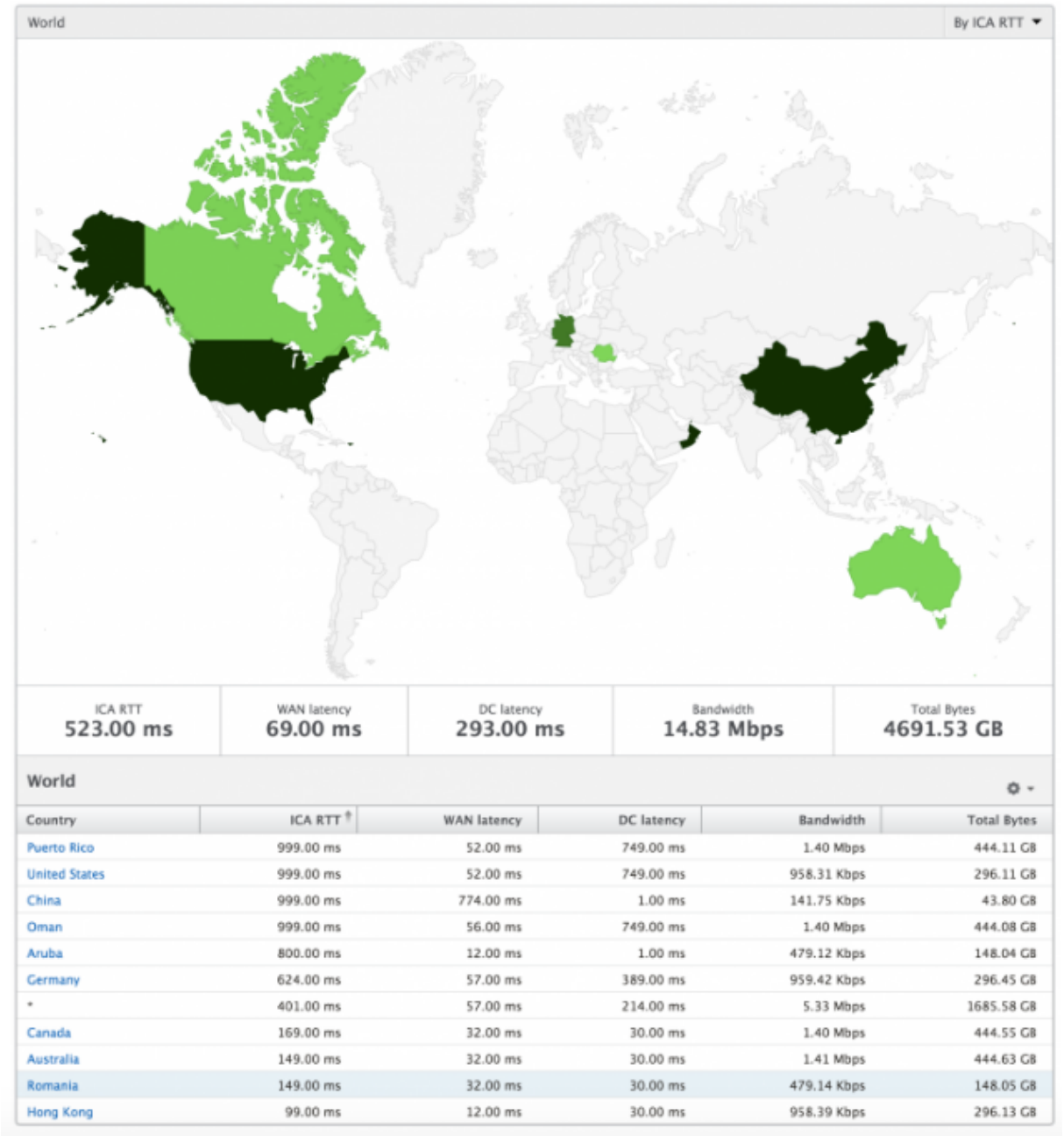


Weltansicht

Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die historischen und aktiven Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltsicht auf das System haben, einen Drilldown zu einem bestimmten Land und auch weiter in Städte hineinfahren, indem sie auf die Region klicken. Die Administratoren können weitere Informationen nach Stadt und Bundesstaat anzeigen. Ab NetScaler ADM Version 12.0 und höher können Sie einen Drilldown zu Benutzern durchführen, die von einem Geostandort aus verbunden sind.

Die folgenden Details können auf der Weltkarte in HDX Insight angezeigt werden, und die Dichte jeder Metrik wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Bytes insgesamt



Lizenzansichtsberichte und -metriken

February 5, 2024

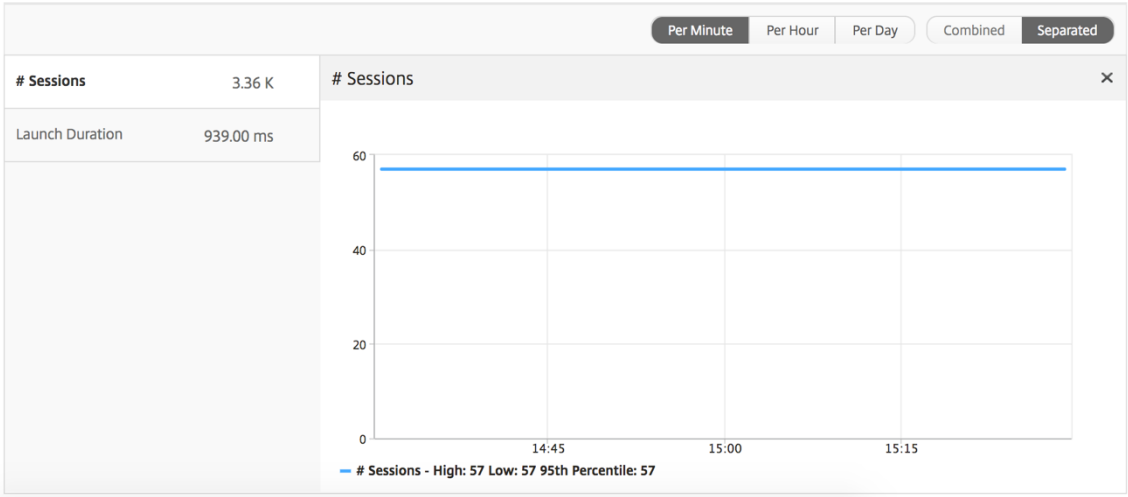
Die Lizenzansicht enthält Details zu den NetScaler Gateway -Lizenzinformationen.

So navigieren Sie zur Lizenzansicht:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Lizenzen**.

Liniendiagramm

Metriken	Beschreibung
Verwendete Lizenzen	Die NetScaler Gateway CCU-Lizenzen, die während der ausgewählten Zeitleiste verwendet werden. Jede Zählung steht für die Anzahl der Benutzersitzungen. Dies ist unabhängig von den Anwendungs- und Desktopsitzungen, die von diesem Benutzer gestartet wurden.
Gesamtzahl der Lizenzen	Gesamtanzahl der NetScaler Gateway CCU-Lizenzen, die für den Kunden verfügbar sind.



Bericht “Schwellenwert”

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* im ausgewählten Zeitraum als Lizenz ausgewählt wurde. Weitere Informationen finden Sie unter So erstellen Sie Schwellenwerte und Warnungen .

Problemen mit HDX Insight beheben

February 5, 2024

Wenn die HDX Insight-Lösung nicht wie erwartet funktioniert, liegt das Problem möglicherweise an einem der folgenden Probleme. Informationen zur Fehlerbehebung finden Sie in den Checklisten in den entsprechenden Abschnitten.

- HDX Insight-Konfiguration.
- Konnektivität zwischen NetScaler ADC und NetScaler ADM.
- Datensatzgenerierung für HDX/ICA-Verkehr in NetScaler ADC.
- Population von Datensätzen in NetScaler ADM.

Checkliste zur Konfiguration von HDX Insight

- Stellen Sie sicher, dass die AppFlow Funktion in NetScaler ADC aktiviert ist. Einzelheiten finden Sie unter AppFlow aktivieren.
- Überprüfen Sie die HDX Insight Konfiguration in der NetScaler ADC Konfiguration.

  Führen Sie den Befehl `show running | grep -i <appflow_policy>` aus, um die HDX Insight-Konfiguration zu überprüfen. Stellen Sie sicher, dass der Bindungstyp ICA REQUEST ist. Zum Beispiel;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  Für den transparenten Modus muss der Bindungstyp ICA_REQ_DEFAULT sein. Zum Beispiel;

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- Stellen Sie bei Single-Hop-/Access-Gateway- oder Double-Hop-Bereitstellungen sicher, dass die HDX Insight AppFlow-Richtlinie an den virtuellen VPN-Server gebunden ist, auf dem HDX/ICA-Verkehr fließt.
- Stellen Sie für den transparenten Modus oder den LAN-Benutzermodus sicher, dass die ICA-Ports 1494 und 2598 eingestellt sind.
- Prüfen Sie, dass der Parameter `appflowlog` in NetScaler Gateway oder dem virtuellem VPN-Server für die Access Gateway- oder Double-Hop-Bereitstellung aktiviert ist. Einzelheiten finden Sie unter AppFlow für virtuelle Server aktivieren.
- Aktivieren Sie “Connection Chaining”in Double-Hop-NetScaler ADC. Einzelheiten finden Sie unter Konfigurieren von NetScaler Gateway-Geräten zum Exportieren von Daten.
- Wenn die HDX Insight Details nach HA-Failover analysiert werden, überprüfen Sie den ICA-Parameter “enableSRonHAFailover”aktiviert ist. Einzelheiten finden Sie unter Sitzungszuverlässigkeit auf dem NetScaler ADC-Hochverfügbarkeitspaar.

Konnektivität zwischen NetScaler ADC und NetScaler ADM Checkliste

- Überprüfen Sie den AppFlow Collector-Status in NetScaler ADC. Einzelheiten finden Sie unter So überprüfen Sie den Status der Konnektivität zwischen NetScaler ADC und AppFlow Collector.
- Überprüfen Sie die HDX Insight AppFlow Richtlinientreffer.

  Führen Sie den Befehl `show appflow policy <policy_name>` aus, um die Treffer der AppFlow-Richtlinie zu überprüfen.

  Sie können auch in der GUI zu **System > AppFlow > Richtlinien** navigieren, um die AppFlow-Richtlinientreffer zu überprüfen.
- Überprüfen Sie jede Firewall, die AppFlow Ports 4739 oder 5557 blockiert.

Datensatzgenerierung für HDX/ICA-Datenverkehr in der NetScaler ADC Checkliste

Führen Sie den Befehl `tail -f /var/log/ns.log | grep -i "default ICA Message "` zur Log-Validierung aus. Basierend auf den generierten Protokollen können Sie diese Informationen für die Fehlerbehebung verwenden.

- Protokoll: **Analyse der ICA-Verbindung wurde übersprungen —HDX Insight wird für diesen Host nicht unterstützt**

  Ursache: Nicht unterstützte Citrix Virtual Apps and Desktops-Versionen

  Workaround: Aktualisieren Sie die Citrix Virtual Apps and Desktops s-Server auf eine unterstützte Version.
- Protokoll: **Client type received 0x53, NOT SUPPORTED**

  Ursache: Nicht unterstützte Version von Citrix Workspace

  Lösung: Aktualisieren Sie Citrix Workspace auf eine unterstützte Version. Einzelheiten finden Sie unter Citrix Workspace-App.
- Log: **Fehler von Expand Packet - Überspringen der gesamten hdx-Verarbeitung für diesen Flow**

  Ursache: Problem beim Dekomprimieren von ICA-Verkehr

  Lösung: Für diese ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wurde.
- Log: **Ungültiger Übergang: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT**

  Ursache: Problem beim Analysieren des ICA-Handshakes

  Lösung: Für diese spezielle ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wurde.

- Protokoll: **EUEM ICA RTT fehlt**

  Ursache: Kanaldaten der Endbenutzer-Erlebnisüberwachung können nicht analysiert werden

  Lösung: Stellen Sie sicher, dass der Dienst zur Überwachung der Benutzererfahrung auf den Citrix Virtual Apps and Desktops-Servern gestartet wurde. Stellen Sie sicher, dass Sie die unterstützten Versionen der Citrix Workspace App verwenden.

- Protokoll: **Ungültiger Channel-Header**

  Ursache: Channel-Header konnte nicht identifiziert werden

  Lösung: Für diese spezielle ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wurde.

- Protokoll: **Code überspringen**

  Wenn Sie einen der folgenden Werte für den Überspringen-Code sehen, werden die Insight-Details übersprungen.

  > Skip-Code 0 zeigt an, dass der Datensatz erfolgreich aus NetScaler ADC exportiert wurde.

Code überspringen	Fehlermeldung	Ursache des Fehlers
100	NS_ICA_ERR_NULL_FRAG	Fehler bei der Behandlung von ICA-Fragmenten, wahrscheinlich aufgrund von Speicherbedingungen
101	NS_ICA_ERR_INVALID_HS_CMD	Ungültiger Handshake-Befehl erhalten
102	NS_ICA_ERR_REDUC_PARAM_CNT	Ungültiger Parameter für V3-Expander-Initialisierung angegeben
103	NS_ICA_ERR_REDUC_INIT	Der V3-Expander konnte nicht korrekt initialisiert werden
104	NS_ICA_ERR_REDUC_PARAM_BYTES	Unzureichende Byte, um einem Kanal einen Coder zuzuweisen
105	NS_ICA_ERR_INVALID_CHANNEL	Ungültige ICA-Kanal Nummer
106	NS_ICA_ERR_INVALID_DECODER	Ungültiger Decoder für einen Kanal angegeben
107	NS_ICA_ERR_INVALID_TW_PARAM	Ungültige Parameteranzahl für Thinwire-Kanal angegeben
108	NS_ICA_ERR_INVALID_TW_DECODER	Ungültiger Decoder für Thinwire-Kanal

Code überspringen	Fehlermeldung	Ursache des Fehlers
109	NS_ICA_ERR_REDUC_NO_DECODER	Kein Decoder für Kanal definiert
110	NS_ICA_ERR_REDUC_V3_EXPANDER	Kanaldaten konnten nicht erweitert werden
111	NS_ICA_ERR_REDUC_BYTES_V3_OOB	Expander-Fehler: Byte verbrauchten mehr als verfügbare Byte
112	NS_ICA_ERR_REDUC_BYTES_OOR	Fehler: Unkomprimierter Datenüberlauf
113	NS_ICA_ERR_REDUC_INVALID_CMD	Undefinierter Expander-Befehl
114	NS_ICA_ERR_CGP_FILL_HOLE	Fehler beim Umgang mit geteilten CGP-Frames
115	NS_ICA_ERR_MEM_NSB_ALLOC	NSB-Zuweisungsfehler — aufgrund unzureichender Speicherbedingungen
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	Speicherzuweisungsfehler für Expander-Kontext
117	NS_ICA_ERR_ICA_OLD_SERVER	Alter Server, Capability-Blöcke werden nicht unterstützt
118	NS_ICA_ERR_PIR_MANY_FRAG	Die Paket-Init-Anforderung ist fragmentiert und kann nicht verarbeitet werden
119	NS_ICA_ERR_INIT_ICA_CAPS	Initialisierungsfehler der ICA-Fähigkeit
120	NS_ICA_ERR_NO_MSI_SUPPORT	Der Host unterstützt keine MSI-Funktion. Zeigt eine niedrigere XenApp-Version als 6.5 oder eine niedrigere XenDesktop-Version als 5.0 an
121	NS_ICA_ERR_CGP_INVALID_CMD	Ungültiger CGP-Befehl gefunden
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	Unzureichende Byte über Kanal
123	NS_ICA_ERR_CHANNEL_DATA	Falsche Daten auf dem Kanal EUEM, CONTROL oder SEAMLESS

Code überspringen	Fehlermeldung	Ursache des Fehlers
124	NS_ICA_ERR_INVALID_PURE_CMD	Ungültiger Befehl bei der Verarbeitung reiner ICA-Kanaldaten
125	NS_ICA_ERR_INVALID_PURE_LEN	Ungültige Länge bei der Verarbeitung reiner ICA-Kanaldaten festgestellt
126	NS_ICA_ERR_INVALID_PURE_LEN	Bei der Verarbeitung von PURE ICA-Kanaldaten wurde eine ungültige Länge gefunden
127	NS_ICA_ERR_INVALID_CLNT_DATA	Ungültige Datenlänge vom Client erhalten
128	NS_ICA_ERR_MSI_GUID_SZ	Fehler in der MSI-GUID-Größe
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	Ungültiger Kanalheader erkannt
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_ID	Abruf der wiederverbundenen Sitzung ist fehlgeschlagen
131	NS_ICA_ERR_DISABLE_SR_NON_RECONNECT	Deaktivieren von SR
132	NS_ICA_ERR_REDUC_NOT_V3	Nicht unterstützte ICA-Reducer-Version
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Komprimierung deaktiviert, wird vom Host nicht berücksichtigt
134	NS_ICA_ERR_IDENT_PROTO	Das ICA- oder CGP-Protokoll kann nicht identifiziert werden, bei falschen Empfängern beobachtet
135	NS_ICA_ERR_INVALID_SIGNATURE	Falsche ICA-Signatur oder magische Zeichenfolge
136	NS_ICA_ERR_PARSE_RAW	Fehler beim Analysieren des ICA-Handshake-Pakets
137	NS_ICA_ERR_INCOMPLETE_PKT	Unvollständiges Paket im Handshake empfangen
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	ICA-Frame ist zu groß und überschreitet 1460 Bytes

Code überspringen	Fehlermeldung	Ursache des Fehlers
139	NS_ICA_ERR_FORWARD	Fehler beim Weiterleiten der ICA-Daten
140	NS_ICA_ERR_MAX_HOLES	Der CGP-Befehl kann nicht verarbeitet werden, da er über das unterstützte Limit hinaus aufgeteilt ist
141	NS_ICA_ERR_ASSEMBLE_FRAME	ICA-Rahmen kann nicht korrekt wieder zusammengebaut werden
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	ICA-Parsing für diesen Receiver (Client) übersprungen, da es nicht in der Zulassungsliste enthalten ist
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	Der Analysestatus für das Wiederverbindungscookie des Clients kann nicht erkannt werden
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	Ungültige Länge des Wiederverbindungs-Cookies wurde nach der Wiederverbindung erkannt
145	NS_ICA_ERR_INVALID_RECONNECT_ID	Client reconnects Cookie hat die erforderliche Einschränkung verpasst
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	Ungültige Zeichenfolge für Empfängerversion vom Client erhalten
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	Ungültige Produkt-ID vom Kunden erhalten
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	Ungültige Kanallänge nach der Erweiterung
149	NS_ICA_ERR_SPECIAL_THINWIRE	Dekomprimierungsfehler
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	Nicht genügend Byte für Seamless-Befehl
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Unzureichende Byte für den EUEM-Befehl festgestellt

Code überspringen	Fehlermeldung	Ursache des Fehlers
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	Ungültiges Ereignis für Seamless Channel Parsing
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Ungültiges Ereignis für CTRL-Kanalanalyse
154	NS_ICA_ERR_EUEM_INVALID_EVENT	Ungültiges Ereignis für EUEM-Kanal-Parsing
155	NS_ICA_ERR_USB_INVALID_EVENT	Ungültiges Ereignis für USB-Kanal-Parsing
156	NS_ICA_ERR_PURE_INVALID_EVENT	Ungültiges Ereignis für reines Kanalparsing
157	NS_ICA_ERR_VCP_INVALID_EVENT	Ungültiges Ereignis für das Parsen virtueller Kanäle
158	NS_ICA_ERR_ICAP_INVALID_EVENT	Ungültiges Ereignis für ICA-Datenanalyse
159	NS_ICA_ERR_CGPP_INVALID_EVENT	Ungültiges Ereignis für CGP-Datenanalyse
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	Ungültiger Status für einen crypt-Befehl in der Basisverschlüsselung
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	Ungültiger crypt-Befehl in der Basisverschlüsselung
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	Ungültiger Status für einen crypt-Befehl in der RC5-Verschlüsselung
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	Ungültiger crypt-Befehl in der RC5-Verschlüsselung
164	NS_ICA_ERR_ADVCRYPT_ENC	Fehler bei der RC5-Verschlüsselung/Entschlüsselung
165	NS_ICA_ERR_ADVCRYPT_DEC	Fehler bei der RC5-Verschlüsselung/Entschlüsselung
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	Der unterstützt Reducer Version 3 nicht
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Der unterstützt Reducer Version 3 nicht
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Unerwartete Anzahl von Byte im ICA-Handshake

Code überspringen	Fehlermeldung	Ursache des Fehlers
169	NS_ICA_ERR_HIGHER_RECONSEQ	Höhere CGP-Wiederaufnahme-Sequenznummer aus Peer-Post-Wiederverbindungen
170	NS_ICA_ERR_DESCSRINFO_ABSENT	Der ICA-Parsing-Status kann nach der Wiederverbindung nicht wiederhergestellt werden
171	NS_ICA_ERR_NSAP_PARSING	Fehler beim Analysieren von Insight-Kanaldaten
172	NS_ICA_ERR_NSAP_APP	Fehler beim Analysieren von App-Details aus Insight-Kanaldaten
173	NS_ICA_ERR_NSAP_ACR	Fehler beim Analysieren von ACR-Details aus Insight-Kanaldaten
174	NS_ICA_ERR_NSAP_SESSION_END	Fehler beim Analysieren der Details zum Sitzungsende aus den Insight-Kanaldaten
175	NS_ICA_ERR_NON_NSAP_SN	ICA-Parsing auf Dienstknoten wurde übersprungen, da keine Insight-Channel-Unterstützung vorhanden ist
176	NS_ICA_ERR_NON_NSAP_CLIENT	NSAP wird vom Client nicht unterstützt
177	NS_ICA_ERR_NON_NSAP_SERVER	NSAP wird vom VDA nicht unterstützt
178	NS_ICA_ERR_NSAP_NEG_FAIL	Fehler bei der NSAP-Datenaushandlung
179	NS_ICA_ERR_SN_RECONNECT_TKT_FETCH	Fehler beim Abrufen des Dienstes verbindet das Ticket im Serviceknoten
180	NS_ICA_ERR_SN_HIGHER_RECONSEQ	Fehler beim Empfangen einer höheren Sequenznummer für die Wiederverbindung im Dienstknoten
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP	Fehler beim Deaktivieren von HDX Insight für Nicht-NSAP-Verbindungen

Beispielprotokolle:

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT
 ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data
 send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/
Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI
 Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0
x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"
```

```
Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41
GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow
: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port
 [10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI
Client Cookie [Non-MSI], Session setup time [01/09/2020:22:55:39
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0
x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

Zähler für Fehler

Verschiedene Zähler werden beim ICA-Parsen erfasst. In der folgenden Tabelle sind die verschiedenen Leistungsindikatoren für die ICA-Analyse aufgeführt.
Führen Sie den Befehl `nsconmsg –g hdx –d statswt0`zum Anzeigen der Leistungsindikatordetails aus.

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_tot_ica_conn	Gibt die Gesamtzahl der von NS erkannten reinen ICA-Verbindungen an. Wird immer dann erhöht, wenn eine ICA-Verbindung erkannt wird, die auf der ICA-Signatur auf einer Client-Leiterplatte basiert.	Statistiken

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_tot_cgp_conn	Zeigt die Gesamtzahl der von NS erkannten CGP-Verbindungen an (Sitzungszuverlässigkeit EIN). Wird immer dann erhöht, wenn eine CGP-Verbindung basierend auf der CGP-Signatur auf einer Client-PCB erkannt wird.	Statistiken
hdx_dbg_tot_udt_conn	Zeigt die Gesamtzahl der von NS erkannten UDP-ICA-Verbindungen an	Statistiken
hdx_dbg_tot_nsap_conn	Gibt die Gesamtzahl der von NS erkannten NSAP-unterstützten Verbindungen an	Statistiken
hdx_tot_skip_conn	Gibt an, wie viele ICA-Verbindungen vom Parser aufgrund einer ungültigen ICA- oder CGP-Signatur übersprungen	Statistiken
hdx_dbg_active_conn	Gesamtzahl der aktiven EDT/CGP/ICA-Verbindungen zu diesem Zeitpunkt.	Statistiken
hdx_dbg_active_nsap_conn	Gesamtzahl der aktiven EDT/CGP/ICA-NSAP-Verbindungen zu diesem Zeitpunkt.	Statistiken
hdx_dbg_skip_appflow_disabled	Gesamtzahl der Instanzen, in denen AppFlow aufgrund der Deaktivierung von AppFlow von einer Sitzung getrennt wurde	Stats/Diagnostik
hdx_dbg_transparent_user	Gesamtzahl der transparenten Benutzerzugriffe	Stats/Diagnostik
hdx_dbg_ag_user	Gesamtzahl der Access Gateway-Benutzerzugriffe	Stats/Diagnostik
hdx_dbg_lan_user	Gesamtzahl der Zugriffe auf den LAN-Benutzermodus	Stats/Diagnostik

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_basic_enc	Gibt die Anzahl der ICA-Verbindungen an, die die Standardverschlüsselung verwenden	Stats/Diagnostik
hdx_advanced_enc	Gibt die Anzahl der ICA-Verbindungen an, die erweiterte RC5-basierte Verschlüsselung verwenden	Stats/Diagnostik
dx_dbg_wanscaler_on_clientside	Gesamtzahl der CGP/ICA-Verbindungen mit Citrix SD-WAN auf der Clientseite	Stats/Diagnostik
hdx_dbg_wanscaler_on_serverside	Gesamtzahl der CGP/ICA-Verbindungen mit Citrix SD-WAN -Serverseite	Stats/Diagnostik
hdx_dbg_reconnected_session	Gesamtzahl der Wiederverbindungsanforderungen vom Client ohne NetScaler ADC-Fehler	Stats/Diagnostik
hdx_dbg_host_rejected_ns_reconnect	Gesamtzahl der von Hosts abgelehnten Wiederverbindungsanfragen nach Client	Stats/Diagnostik
hdx_euem_available	Gibt die Anzahl der Verbindungen an, für die der Kanal “Überwachung der Benutzererfahrung”verfügbar ist. Der End User Experience Monitoring-Kanal ist erforderlich, um Statistiken wie ICA RTT zu sammeln.	Stats/Diagnostik
hdx_err_disabled_sr	Die Sitzungszuverlässigkeit ist mit dem `nsapimgr`Drehknopf deaktiviertDie Sitzung funktioniert für diese Sitzung nicht.	Fehler

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_err_skip_no_msi	Auf dem XA/XD-Server fehlt die MSI-Fähigkeit. Dies weist auf eine ältere Serverversion hin. HDX Insight überspringt diese Verbindung.	Fehler
hdx_err_skip_old_server	Alte, nicht unterstützte Serverversion	Fehler
hdx_err_clnt_not_whitelist	Clientempfänger nicht in der Zulassungsliste, HDX Insight überspringt diese Verbindung	Fehler
hdx_sm_ica_cam_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CAM_CHANNEL	Diagnose
hdx_sm_ica_usb_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_USB_CHANNEL	Diagnose
hdx_sm_ica_clip_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CLIP_CHANNEL	Diagnose
hdx_sm_ica_ccm_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CCM_CHANNEL	Diagnose
hdx_sm_ica_cdm_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CDM_CHANNEL	Diagnose
hdx_sm_ica_com1_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_COM1_CHANNEL	Diagnose

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_sm_ica_com2_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_COM2_CHANNEL	Diagnose
hdx_sm_ica_cpm_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CPM_CHANNEL	Diagnose
hdx_sm_ica_lpt1_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_LPT1_CHANNEL	Diagnose
hdx_sm_ica_lpt2_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_LPT2_CHANNEL	Diagnose
dx_dbg_sm_ica_msi_disabled	Gesamtzahl der Fälle, in denen MSI über die SmartAccess-Richtlinie deaktiviert ist	Diagnose
hdx_sm_ica_file_channel_disabled	Die Gesamtzahl von NS_ICA_FILE_CHANNEL ist über die SmartAccess-Richtlinie deaktiviert	Diagnose
hdx_dbg_usb_accept_device	Gesamtzahl der akzeptierten USB-Geräte	Diagnose
hdx_dbg_usb_reject_device	Gesamtzahl der abgelehnten USB-Geräte	Diagnose
hdx_dbg_usb_reset_endpoint	Gesamtzahl der zurückgesetzten USB-Endpunkte	Diagnose
hdx_dbg_usb_reset_device	Gesamtzahl der zurückgesetzten USB-Geräte	Diagnose
hdx_dbg_usb_stop_device	Gesamtzahl der gestoppten USB-Geräte	Diagnose

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_dbg_usb_stop_device_response	Gesamtzahl der Antworten von gestoppten USB-Geräten	Diagnose
hdx_dbg_usb_device_gone	Gesamtzahl der ausgelaufenen USB-Geräte	Diagnose
hdx_dbg_usb_device_stopped	Gesamtzahl der gestoppten USB-Geräte	Diagnose

nstrace-Validierung

Suchen Sie nach dem CFLOW-Protokoll, um zu sehen, dass alle AppFlow-Datensätze aus NetScaler ADC ausgehen.

Grundgesamtheit der Datensätze in der NetScaler ADM Checkliste

- Führen Sie den Befehl aus `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"`und überprüfen Sie die Protokolle, um zu bestätigen, dass NetScaler ADM AppFlow-Einträge erhält.
- Bestätigen Sie, dass NetScaler ADC-Instanz zu NetScaler ADM hinzugefügt wird.
- Überprüfen Sie, ob der virtuelle NetScaler Gateway/VPN-Server in NetScaler ADM lizenziert ist.
- Stellen Sie sicher, dass Multi-Hop-Parametereinstellung für Double-Hop aktiviert ist
- Stellen Sie sicher, dass NetScaler Gateway für den zweiten Hop in der Double-Hop-Bereitstellung freigegeben

Bevor Sie den technischen Support von Citrix kontaktieren

Stellen Sie für eine schnelle Lösung sicher, dass Sie über die folgenden Informationen verfügen, bevor Sie sich an den technischen Support von Citrix wenden:

- Einzelheiten zur Bereitstellung und Netzwerktopologie.
- NetScaler ADC- und NetScaler ADM-Versionen.
- Serverversionen von Citrix Virtual Apps and Desktops.
- Versionen von Client Receiver.
- Anzahl der aktiven ICA-Sitzungen, bei denen das Problem aufgetreten ist.

- Das technische Supportpaket wird durch Ausführen des `show techsupport` Befehls an der NetScaler ADC-Eingabeaufforderung erfasst.
- Technischer Support Paket für NetScaler ADM erfasst.
- Paketspuren wurden auf allen NetScaler ADC erfasst.
  Um eine Paketablaufverfolgung zu starten, geben Sie Folgendes ein: `start nstrace -size 0'`
  Um eine Paketablaufverfolgung zu stoppen: `stop nstrace`
- Sammeln Sie Einträge in der ARP-Tabelle des Systems, indem Sie den Befehl `show arp` ausführen.

Bekannte Probleme

Bekannte Probleme in HDX Insight finden Sie in den NetScaler ADC Versionshinweisen.

Gateway Insight

February 5, 2024

In einer Citrix Gateway-Bereitstellung ist der Einblick in die Zugriffsdetails eines Benutzers für die Behebung von Zugriffsfehlern unerlässlich. Als Netzwerkadministrator möchten Sie wissen, wann sich ein Benutzer nicht bei Citrix Gateway anmelden kann, und Sie möchten die Benutzeraktivität und die Gründe für den Anmeldefehler kennen. Diese Informationen sind normalerweise nicht verfügbar, es sei denn, der Benutzer sendet eine Lösungsanfrage.

Gateway Insight bietet Einblick in die Fehler, die bei der Anmeldung bei Citrix Gateway auftreten, unabhängig vom Zugriffsmodus. Sie können eine Liste aller verfügbaren Benutzer, die Anzahl der aktiven Benutzer, die Anzahl der aktiven Sitzungen sowie die Bytes und Lizenzen anzeigen, die von allen Benutzern zu einem bestimmten Zeitpunkt verwendet werden. Sie können die Endpunktanalyse (EPA), Authentifizierung, Single Sign-On (SSO) und Fehler beim Starten von Anwendungen für einen Benutzer anzeigen. Sie können auch die Details zu aktiven und beendeten Sitzungen für einen Benutzer anzeigen.

Gateway Insight bietet auch Einblick in die Gründe für das Fehlschlagen des Anwendungsstarts für virtuelle Anwendungen. Dadurch können Sie Probleme bei der Anmeldung oder beim Starten von Anwendungen beheben. Sie können die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen, die Anzahl der gesamten Byte und die von den Anwendungen verbrauchte Bandbreite anzeigen. Sie können Details der Benutzer, Sitzungen, Bandbreite und Startfehler für eine Anwendung anzeigen.

Sie können die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die Gesamtanzahl der Bytes und die Bandbreite aller Gateways, die mit einem Citrix Gateway Gerät verknüpft sind, jederzeit anzeigen. Sie können EPA, Authentifizierung, Single Sign-On und Anwendungsstartfehler für ein Gateway anzeigen. Sie können auch die Details aller Benutzer, die einem Gateway zugeordnet sind, und deren Anmeldeaktivitäten anzeigen.

Alle Protokollmeldungen werden in der Citrix ADM-Datenbank gespeichert, sodass Sie Fehlerdetails für einen beliebigen Zeitraum anzeigen können. Sie können auch eine Zusammenfassung der Anmeldefehler anzeigen und feststellen, in welcher Phase des Anmeldevorgangs ein Fehler aufgetreten ist.

Punkte zu beachten

- Gateway Insight wird in den folgenden Bereitstellungen unterstützt:
  - Access Gateway
  - Unified Gateway
- Die Citrix ADM-Version und der Build müssen mit denen des Citrix Gateway-Geräts identisch oder höher sein.
- Eine Stunde Gateway Insight-Berichte können für Citrix ADC Instanzen mit Advanced-Lizenz angezeigt werden. Eine Premium-Lizenz ist ein Muss, um Gateway Insight-Berichte länger als eine Stunde anzusehen.

Einschränkungen

- Citrix Gateway unterstützt Gateway Insight nicht, wenn die Authentifizierungsmethode als zertifikatbasierte Authentifizierung konfiguriert ist.
- Für Gateway Insight-Berichte werden Geostandortinformationen nicht von der Citrix ADC Appliance bereitgestellt.
- Erfolgreiche Benutzeranmeldungen, Latenz und Details auf Anwendungsebene für virtuelle ICA-Anwendungen und -Desktops sind nur auf dem HDX Insight User-Dashboard sichtbar.
- In einem Double-Hop-Modus ist kein Einblick in Fehler auf der Citrix Gateway-Appliance in der zweiten DMZ verfügbar.
- Probleme mit dem Remotedesktopprotokoll (RDP) -Desktop-Zugriff werden nicht gemeldet.
- Gateway Insight wird für die folgenden Authentifizierungstypen unterstützt. Wenn ein anderer Authentifizierungstyp als diese verwendet wird, können Abweichungen in Gateway Insight auftreten.

- Lokal
- LDAP
- RADIUS
- TACACS
- SAML
- Natives OTP

Gateway Insight aktivieren

Um Gateway Insight für Ihr Citrix Gateway Gerät zu aktivieren, müssen Sie das Citrix Gateway-Gerät zunächst Citrix ADM hinzufügen. Anschließend müssen Sie AppFlow für den virtuellen Server aktivieren, der die VPN-Anwendung darstellt. Informationen zum Hinzufügen von Geräten zu Citrix ADM finden Sie unter Geräte hinzufügen.

> **Hinweis**
>
> Um Fehler bei der Endpunktanalyse (EPA) in Citrix ADM anzuzeigen, müssen Sie die AppFlow-Authentifizierung, -Autorisierung und die Protokollierung von Benutzernamen auf dem Citrix Gateway-Gerät aktivieren.

Das folgende Verfahren zum Aktivieren von Gateway Insight ist anwendbar, wenn Citrix ADM **13.0 Build 36.27** lautet:

1. Navigieren Sie zu **Netzwerke** > **Instanzen**, und wählen Sie die Instanz aus, für die Sie AppFlow aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
3. Wählen **Sie auf der Seite Configure Insight** unter **Configure Analytics** die Option **Citrix Gateway** aus.
4. Wählen Sie den virtuellen Server aus und klicken Sie dann auf **AppFlow aktivieren**.
5. Klicken Sie auf dem Bildschirm **AppFlow aktivieren** in der Liste **Ausdruck auswählen** auf true.
6. Aktivieren Sie neben **Transportmodus** das Kontrollkästchen **Logstream**.

   > **Hinweis**
   >
   > Sie können entweder **IPFIX** oder **Logstream** als Transportmodus wählen.
   >
   > Weitere Informationen zu **IPFIX** und **Logstream** finden Sie unter **Logstream-Übersicht**.

7. Klicken Sie auf **OK**.

Für Citrix ADM Version 13.0 Build 41.x oder höher

1. Navigieren Sie zu **Netzwerke** >**Instanzen**und wählen Sie die Instanz aus.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
3. Wählen Sie den virtuellen Server aus und klicken Sie auf **Analytics aktivieren**.
4. Unter **Erweiterte Optionen**:
    a) Wählen Sie **Logstream** aus
    b) Wählen Sie **Citrix Gateway**
5. Klicken Sie auf **OK**.

Aktivieren der AppFlow-Authentifizierung, Autorisierung und Auditing-Benutzernamenprotokollierung auf einer Citrix Gateway-Appliance mithilfe der GUI

1. Navigieren Sie zu **Konfiguration > System > AppFlow > Einstellungen**, und klicken Sie dann auf **AppFlow Einstellungen ändern**.
2. Wählen **Sie im Bildschirm AppFlow-Einstellungen konfigurieren** die Option **AAA-Benutzername**aus, und klicken Sie dann auf **OK**.

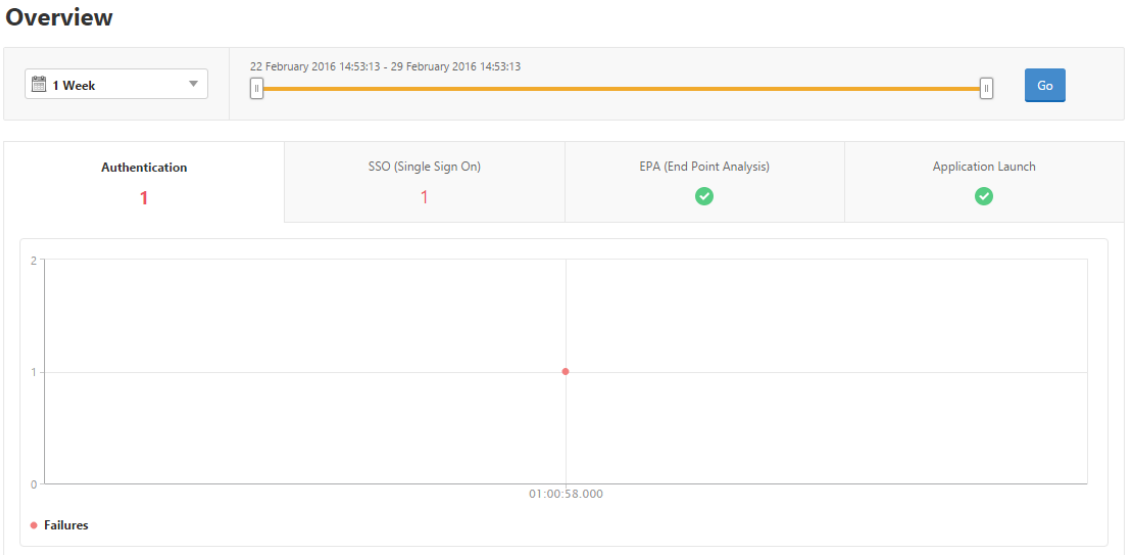
Gateway Insight-Berichte anzeigen

In Citrix ADM können Sie Berichte für alle Benutzer, Anwendungen und Gateways anzeigen, die den Citrix Gateway-Appliances zugeordnet sind, und Sie können Details für einen bestimmten Benutzer, eine bestimmte Anwendung oder ein bestimmtes Gateway anzeigen. Im Abschnitt **Überblick** können Sie die Fehler EPA, SSO, Authentifizierung und Application Launch anzeigen. Sie können auch eine Zusammenfassung der verschiedenen Sitzungsmodi anzeigen, die von Benutzern für die Anmeldung verwendet werden, die Clienttypen und die Anzahl der stündlich angemeldeten Benutzer.

> **Hinweis**
>
> Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, Zugriff auf Anwendungsebene für die Gruppe gewähren und der Gruppe Benutzer zuweisen. Citrix ADM Analytics unterstützt jetzt die auf virtuellen IP-Adressen basierende Autorisierung. Ihre Benutzer können jetzt Berichte für alle Insights nur für die Anwendungen (virtuelle Server) anzeigen, für die sie autorisiert sind. Weitere Informationen zu Gruppen und zum Zuweisen von Benutzern zur Gruppe finden Sie unter Konfigurieren von Gruppen.

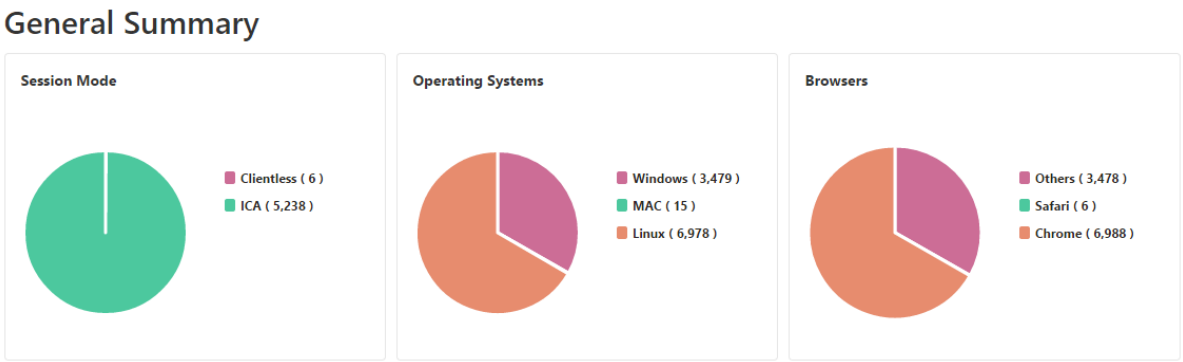
So zeigen Sie EPA-, SSO-, Authentifizierungs-, Autorisierungs- und Anwendungsstartfehler an

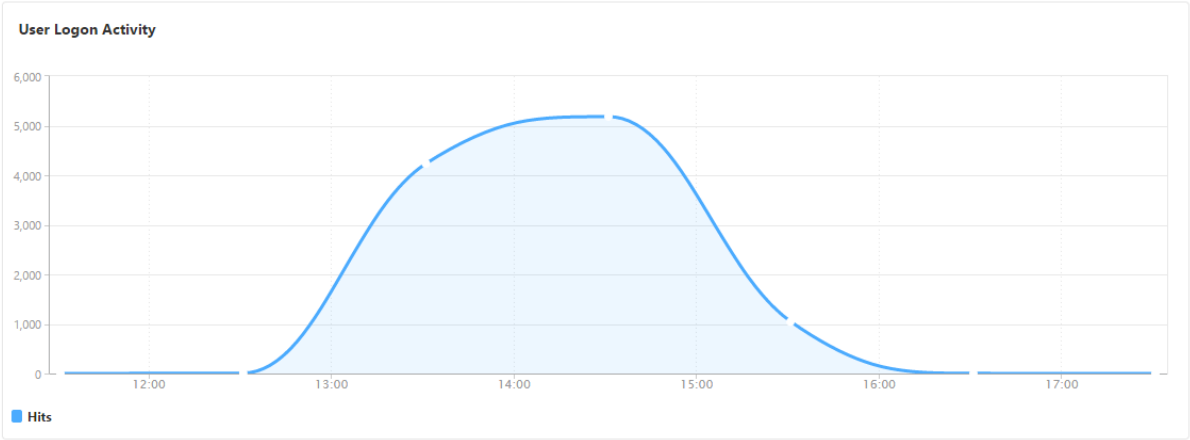
1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Wählen Sie den Zeitraum aus, für den Sie die Benutzerdetails anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.
3. Klicken Sie auf die Registerkarten EPA (Endpunktanalyse), Authentifizierung, Autorisierung, SSO (Single Sign On) oder Anwendungsstart, um die Fehlerdetails anzuzeigen.



So zeigen Sie eine Zusammenfassung der Sitzungsmodi, Clients und der Anzahl der Benutzer an

Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**, scrollen Sie nach unten, um die Berichte anzuzeigen.





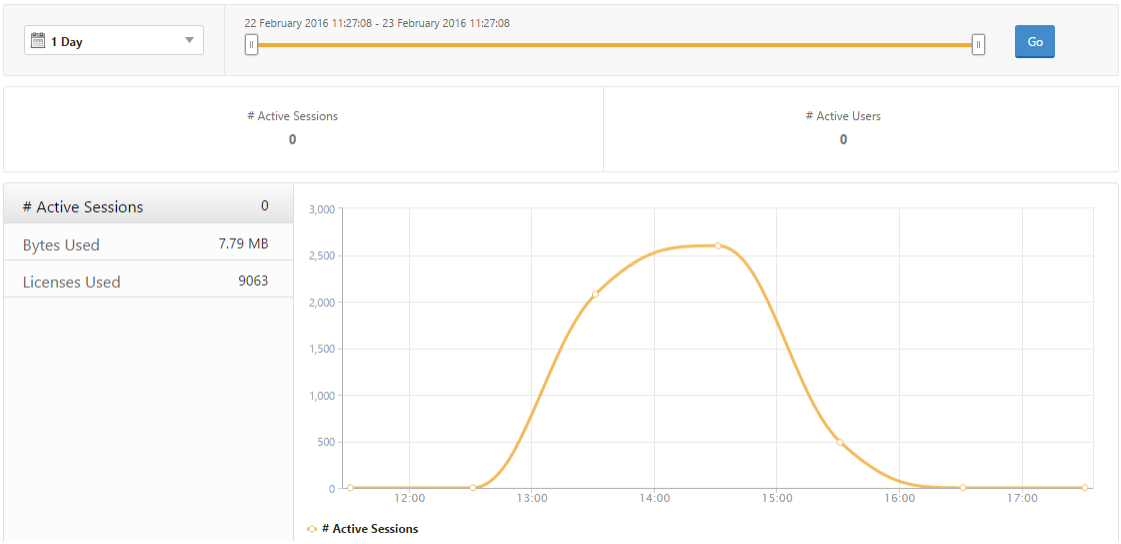
Anzeigen von Gateway Insight-Berichten für Benutzer

Sie können die Berichte anzeigen für:

- Alle mit den Citrix Gateway-Appliances verknüpften Benutzer
- Fehler bei EPA, Authentifizierung, SSO und Anwendungsstart für einen Benutzer.
- Die Details von aktiven und beendeten Sitzungen für einen Benutzer.
- Die Arten von Sitzungsmodi wie Full Tunnel, Clientless VPN und ICA-Proxy.

So zeigen Sie Benutzerdetails an

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight > Benutzer**.
2. Wählen Sie den Zeitraum aus, für den Sie die Benutzerdetails anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.
3. Sie können die Anzahl der aktiven Benutzer, die Anzahl der aktiven Sitzungen, Bytes und Lizenzen anzeigen, die von allen Benutzern während des Zeitraums verwendet werden.

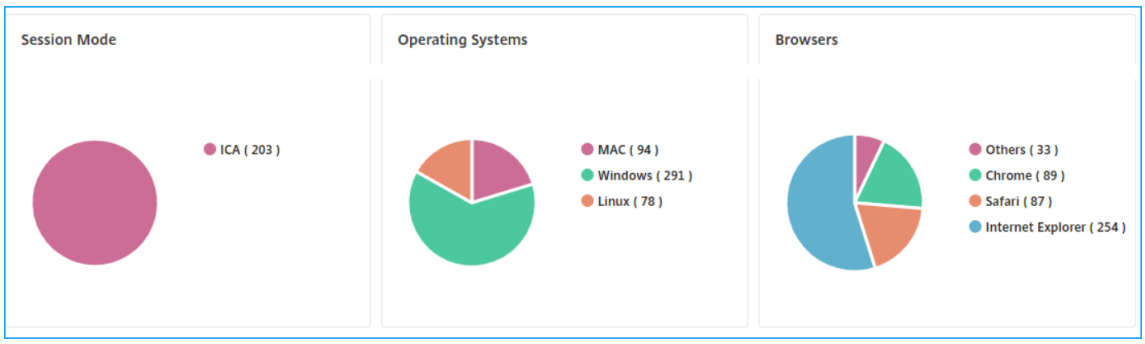


Scrollen Sie nach unten, um eine Liste der verfügbaren Benutzer und aktiven Benutzer anzuzeigen.

User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

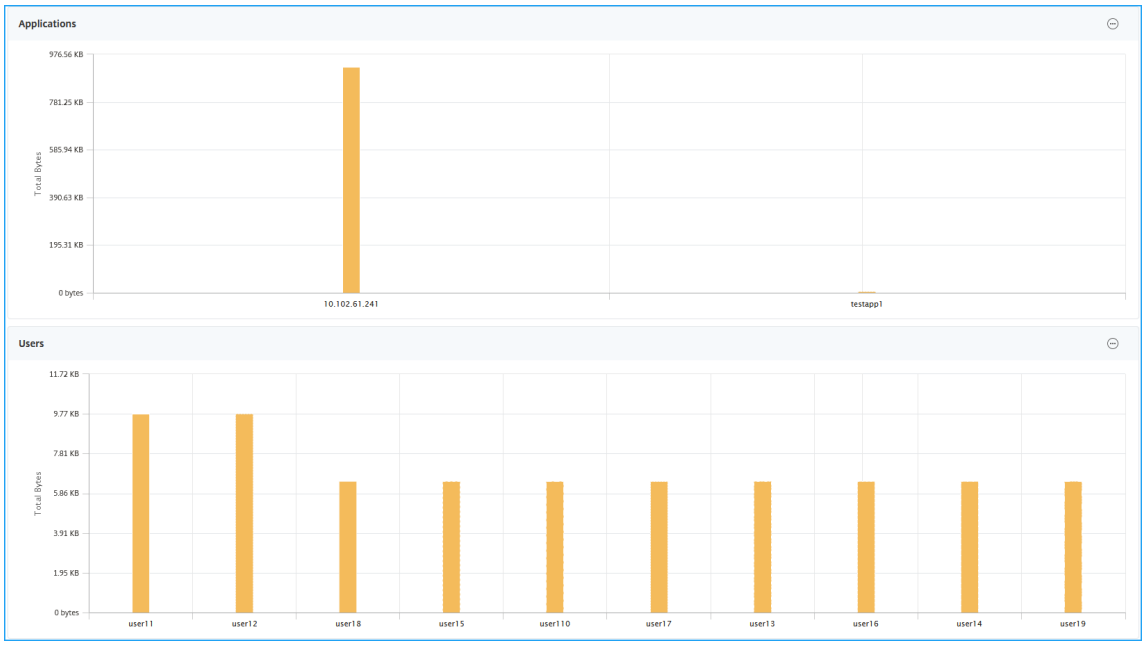
Klicken Sie auf der Registerkarte **Benutzer** oder **Aktive Benutzer** auf einen Benutzer, um die folgenden Benutzerdetails anzuzeigen:

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

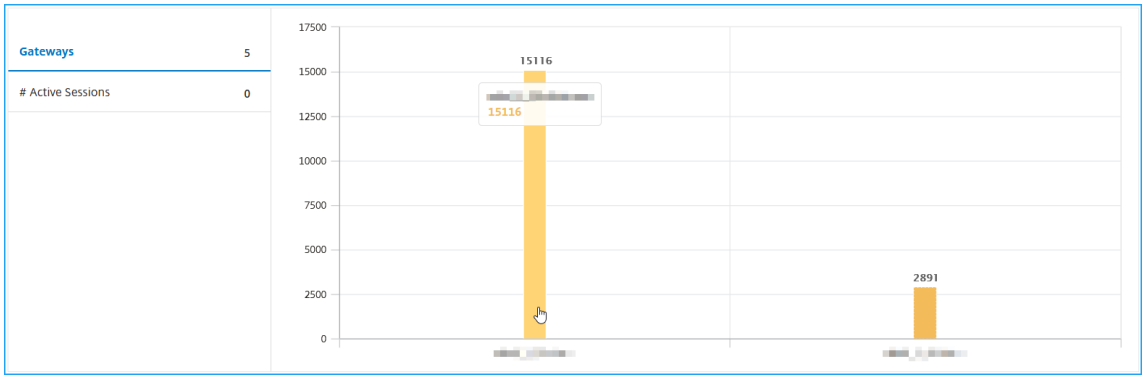


- **Benutzer und Anwendungen für das ausgewählte Gateway** - Navigieren Sie zu **Analytics** >

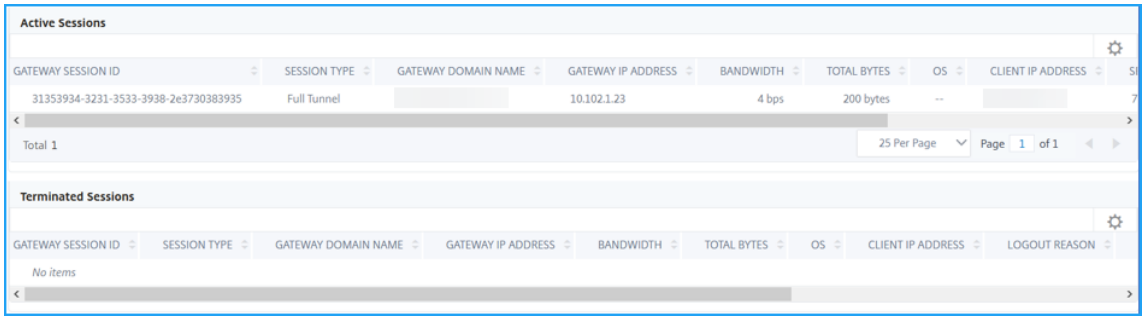
Gateway Insight > **Gateway** und klicken Sie auf einen Gateway-Domänennamen, um die 10 wichtigsten Anwendungen und Top-10-Benutzer anzuzeigen, die mit dem ausgewählten Gateway verknüpft sind.



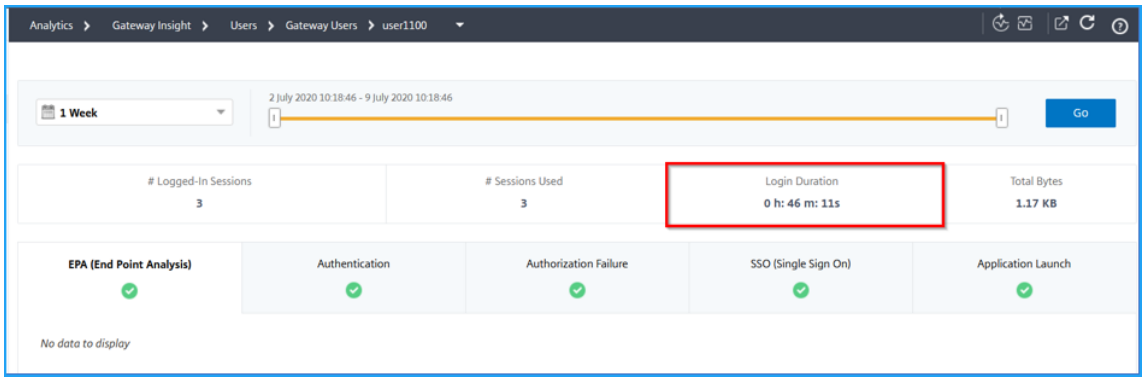
- **Weitere Optionen für Anwendungen und Benutzer anzeigen** —Für mehr als 10 Anwendungen und Benutzer können Sie auf das Mehr-Symbol in Anwendungen und Benutzer klicken, um alle Benutzer- und Anwendungsdetails anzuzeigen, die mit dem ausgewählten Gateway verknüpft sind.
- **Zeigen Sie Details an, indem Sie auf das Balkendiagramm klicken** —Wenn Sie auf ein Balkendiagramm klicken, können Sie die relevanten Details anzeigen. Navigieren Sie beispielsweise zu **Analytics > Gateway Insight > Gateway** und klicken Sie auf das Gateway-Bar-Diagramm, um die Gateway-Details anzuzeigen.



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



- Der Gateway-Domänenname und die Gateway-IP-Adresse in **Active Sessions**
- Die Dauer der Benutzeranmeldung.



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

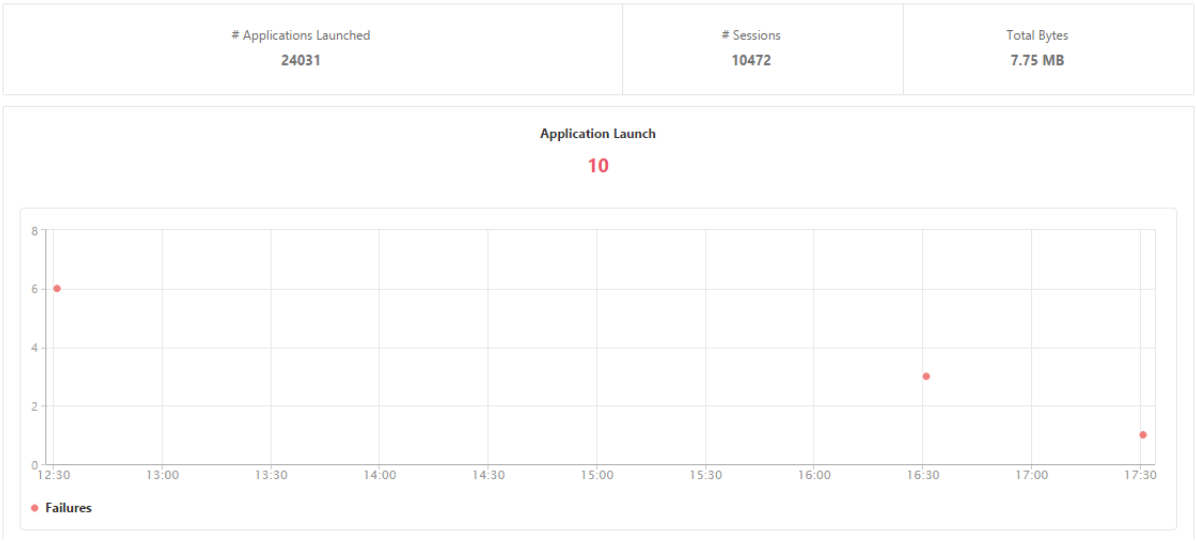
Anzeigen von Gateway Insight-Berichten für Anwendungen

Sie können die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen, die Anzahl der gesamten Byte und die von den Anwendungen verbrauchte Bandbreite anzeigen. Sie können Details der Benutzer, Sitzungen, Bandbreite und Startfehler für eine Anwendung anzeigen.

So zeigen Sie Anwendungsdetails an

1. Navigieren Sie in NetScaler ADM zu **Analytics > Gateway Insight > Anwendungen**.
2. Wählen Sie den Zeitraum aus, für den Sie die Anwendungsdetails anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.

Sie können jetzt die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen, die Anzahl der gesamten Byte und die von den Anwendungen verbrauchte Bandbreite anzeigen.



Führen Sie einen Bildlauf nach unten durch, um die Anzahl der Sitzungen, Bandbreite und Gesamtbytes anzuzeigen, die von ICA und anderen Anwendungen belegt werden.

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

Auf der Registerkarte **Andere Anwendungen** können Sie in der Spalte **Name** auf eine Anwendung klicken, um Details zu dieser Anwendung anzuzeigen.

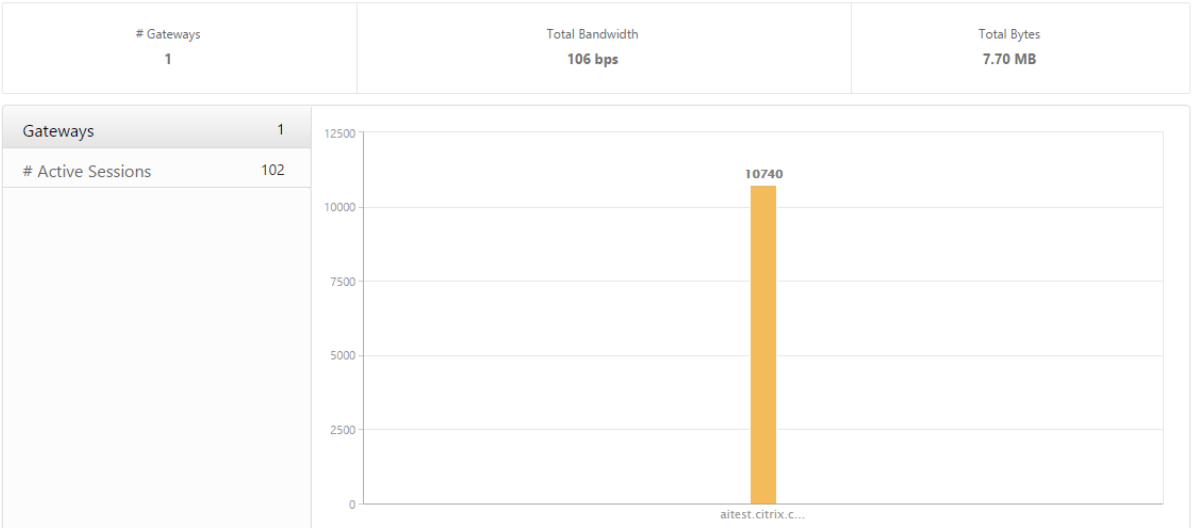
Anzeigen von Gateway Insight-Berichten für Gateways

Sie können die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die Gesamtanzahl der Bytes und die Bandbreite aller Gateways, die mit einem Citrix Gateway Gerät verknüpft sind, jederzeit anzeigen. Sie können EPA, Authentifizierung, Single Sign-On und Anwendungsstartfehler für ein Gateway anzeigen. Sie können auch die Details aller Benutzer, die einem Gateway zugeordnet sind, und deren Anmeldeaktivitäten anzeigen.

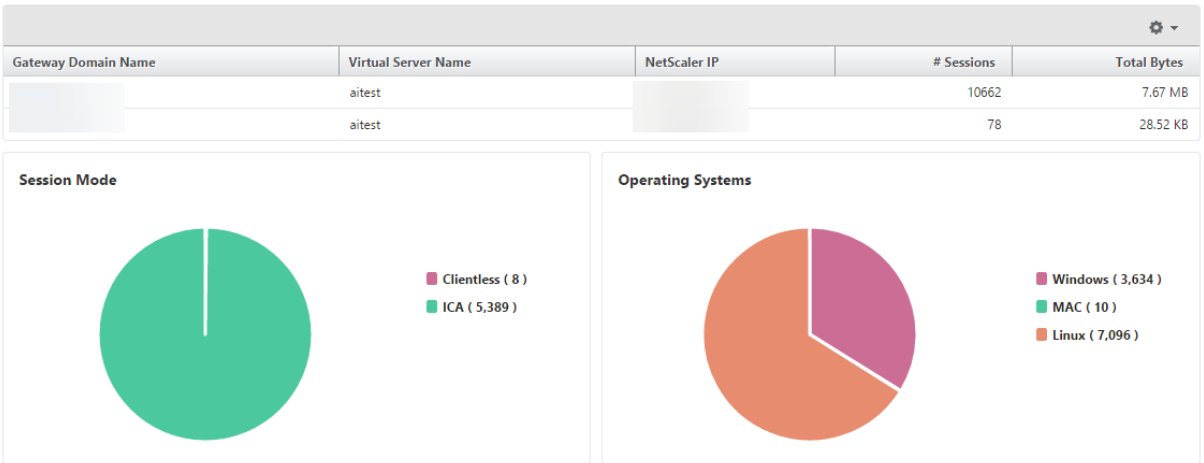
So zeigen Sie Gateway Details an

1. Navigieren Sie in **Citrix ADM** zu **Analytics > Gateway Insight > Gateways**.
2. Wählen Sie den Zeitraum aus, für den Sie die Gateway Details anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.

Sie können jetzt die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die Gesamtanzahl der Bytes und die Bandbreite anzeigen, die von allen Gateways verwendet wird, die mit einem Citrix Gateway Gerät verknüpft sind.



Führen Sie einen Bildlauf nach unten durch, um die Gatewaydetails wie Gatewaydomänenname, Name des virtuellen Servers, NetScaler IP-Adresse, Sitzungsmodi und Total Bytes anzuzeigen.



Sie können in der Spalte **Gateway-Domänenname** auf ein Gateway klicken, um EPA, Authentifizierung, Single Sign-On und Anwendungsstart sowie andere Details für ein Gateway anzuzeigen.

Exportieren von Berichten

Sie können die Gateway Insight-Berichte mit allen in der GUI angezeigten Details im PDF-, JPEG-, PNG- oder CSV-Format auf Ihrem lokalen Computer speichern. Sie können auch den Export der Berichte an bestimmte E-Mail-Adressen in verschiedenen Intervallen planen.

> **Hinweis**
>
> - Benutzer mit schreibgeschütztem Zugriff können keine Berichte exportieren.
> - Geokartenberichte werden nur exportiert, wenn der Citrix ADM über eine Internetverbindung verfügt.

Um einen Bericht zu exportieren

1. Klicken Sie auf der Registerkarte **Dashboard** im rechten Fensterbereich auf die Schaltfläche **Exportieren** .
2. Wählen Sie unter **Jetzt exportieren**das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.

So planen Sie den Export:

1. Klicken Sie auf der Registerkarte **Dashboard** im rechten Fensterbereich auf die Schaltfläche **Exportieren** .
2. Geben Sie unter **Export planen**die Details an und klicken Sie auf **Zeitplan**.

So fügen Sie einen E-Mail-Server oder eine E-Mail-Verteilerliste hinzu:

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **Benachrichtigungen** > **E-Mail**.
2. Wählen Sie im rechten Bereich **E-Mail-Server**aus, um einen E-Mail-Server hinzuzufügen, oder wählen Sie **E-Mail-Verteilerliste** aus, um eine E-Mail-Verteilerliste zu erstellen.
3. Geben Sie die Details an und klicken Sie auf **Erstellen**

So exportieren Sie das gesamte Gateway Insight Dashboard:

1. Klicken Sie auf der Registerkarte **Dashboard** im rechten Fensterbereich auf die Schaltfläche **Exportieren** .
2. Wählen Sie unter **Jetzt exportieren**die Option **PDF-Format** aus, und klicken Sie dann auf **Exportieren**.

Gateway Insight Anwendungsfälle

Die folgenden Anwendungsfälle zeigen, wie Sie Gateway Insight verwenden können, um Einblick in die Zugriffsdetails, Anwendungen und Gateways der Benutzer auf Citrix Gateway-Geräten zu erhalten.

Ein Benutzer kann sich nicht beim Citrix Gateway Gerät oder bei den internen Webservern anmelden

Sie sind ein Citrix Gateway-Administrator, der Citrix Gateway-Appliances über Citrix ADM überwacht, und Sie möchten sehen, warum sich ein Benutzer nicht anmelden kann oder in welcher Phase des Anmeldevorgangs der Fehler aufgetreten ist.

Mit Citrix ADM können Sie die Fehlerdetails der Benutzeranmeldung in den folgenden Phasen des Anmeldevorgangs anzeigen:

- Authentifizierung
- Endpunktanalyse (EPA)
- Single Sign-On

In Citrix ADM können Sie nach einem bestimmten Benutzer suchen und dann alle Details für diesen Benutzer anzeigen.

So suchen Sie nach einem Benutzer:

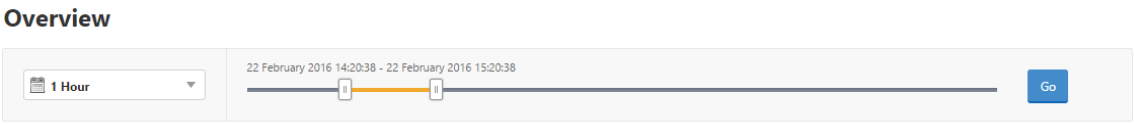
Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight** und geben Sie im Textfeld Nach **Benutzern suchen** den Benutzer an, den Sie suchen möchten.

Authentifizierungsfehler

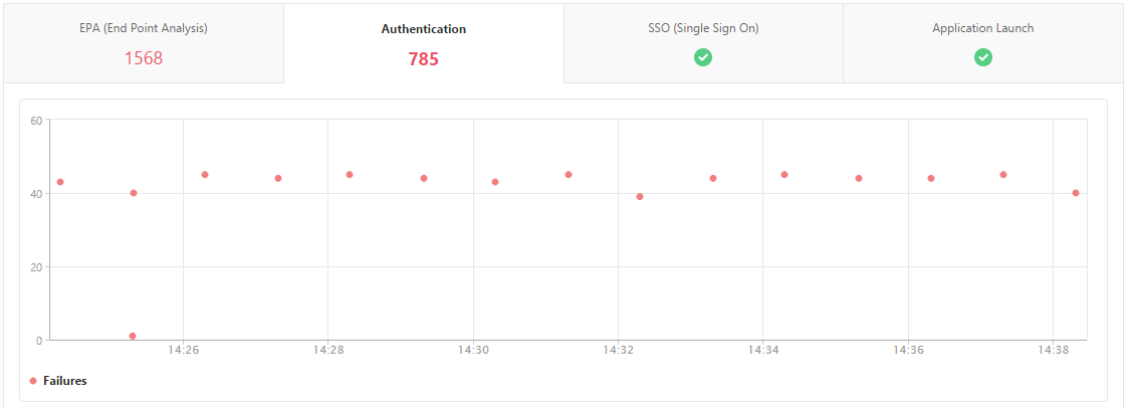
Sie können Authentifizierungsfehler wie falsche Anmeldeinformationen oder keine Antwort vom Authentifizierungsserver anzeigen. Sie können auch den Faktor sehen, bei dem die Authentifizierung fehlgeschlagen ist.

So zeigen Sie die Details zum Authentifizierungsfehler an:

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Wählen Sie im Abschnitt **Übersicht** den Zeitraum aus, für den Sie die Authentifizierungsfehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.



3. Klicken Sie auf die Registerkarte **Authentifizierung**. Sie können die Anzahl der Authentifizierungsfehler zu einem bestimmten Zeitpunkt im Diagramm "**Fehler** "anzeigen.



Führen Sie einen Bildlauf nach unten durch, um Details zu jedem Authentifizierungsfehler wie **Benutzername, Client-IP-Adresse, Fehlerzeit, Authentifizierungstyp, IP-Adresse des Authentifizierungsservers**und mehr aus der Tabelle auf derselben Registerkarte anzuzeigen. In der Spalte **Fehlerbeschreibung** in der Tabelle wird der Grund für den Anmeldefehler angezeigt, und in der Spalte **Status** wird der n-te Faktor angezeigt, bei dem der Fehler aufgetreten ist.

IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR TIME	ERROR DESCRIPTION	ERROR COUNT	STATE	AUTHEN
183	vpnvserver		15/03/2019, 06:30:04	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	3	2nd Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	1	2nd Factor	RADIUS
111	vpnvip		19/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	3	1st Factor	LDAP
183	vpnvserver		13/04/2019, 06:30:28	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Account is disabled	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	Local
183	vpnvserver		12/04/2019, 06:30:13	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Bad(format) password passed to nsaaad	5	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	4	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	22	1st Factor	RADIUS
.88	_XD_10.217.205.88_443		15/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die Authentifizierungsfehler und andere Details für diesen Benutzer anzuzeigen. Sie können die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen, indem Sie das Einstellungssymbol verwenden.

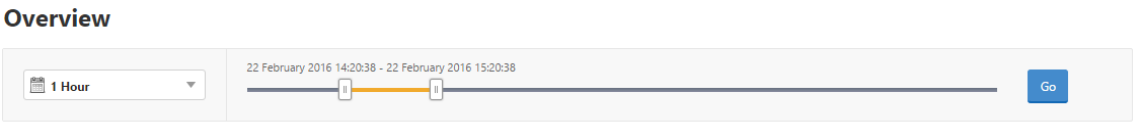
EPA-Fehler

Sie können EPA-Fehler in der Vor- oder Nachauthentifizierungsphase anzeigen.

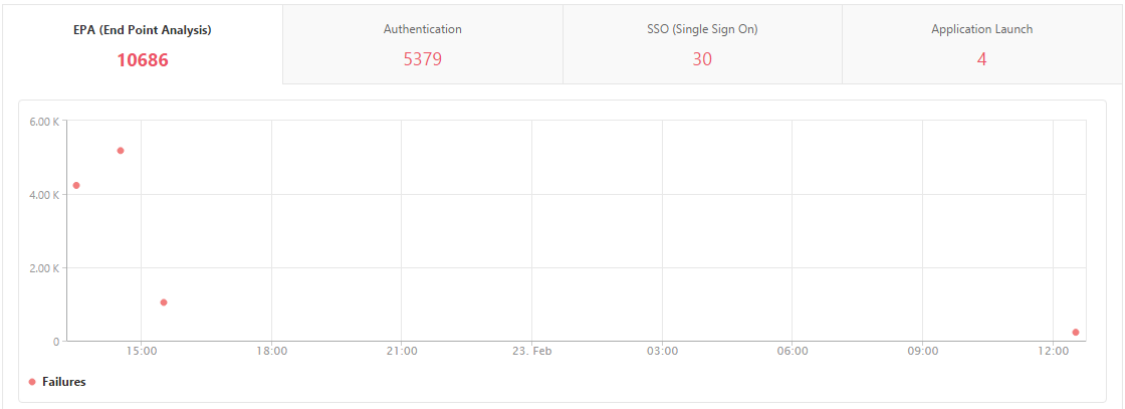
> **Wichtig:**
>
> - EPA-Ausfälle werden nur gemeldet, wenn klassische Ausdrücke konfiguriert sind.
> - EPA-Fehler werden nicht gemeldet, wenn erweiterter Ausdruck in der Vorauthentifizierungs- oder Nachauthentifizierungsrichtlinie konfiguriert ist.
> - EPA-Ausfälle werden nicht gemeldet, wenn EPA als einer der Faktoren in einem nFactor-Authentifizierungsablauf konfiguriert ist.

So zeigen Sie EPA-Fehlerdetails an:

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Wählen Sie im Abschnitt Übersicht den Zeitraum aus, für den Sie die EPA-Fehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.



3. Klicken Sie auf die Registerkarte **EPA (Endpunktanalyse)**. Sie können die Anzahl der EPA-Fehler jederzeit im Diagramm **Fehler** anzeigen.



Scrollen Sie nach unten, um Details zu jedem EPA-Fehler wie **Benutzername, NetScaler-IP-Adresse, Gateway-IP-Adresse, VPN, Fehlerzeit, Richtlinienname, Gateway-Domainname** und mehr aus der Tabelle auf derselben Registerkarte anzuzeigen. In der Spalte **Fehlerbeschreibung** in der Tabelle wird der Grund für den EPA-Fehler angezeigt, und in der Spalte **Richtlinienname** wird die Richtlinie angezeigt, die zum Fehler geführt hat.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die EPA-Fehler und andere Details für diesen Benutzer anzuzeigen. Sie können die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen, indem Sie den Abwärtspfeil verwenden.

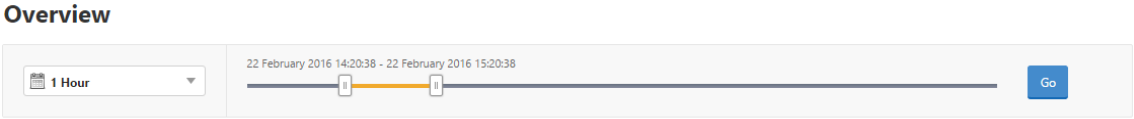
> **Hinweis**
>
> Citrix Gateway meldet die EPA-Fehler nicht, wenn der Ausdruck “ClientSecurity”als Richtlinienregel für VPN-Sitzungen konfiguriert ist.

SSO-Fehler

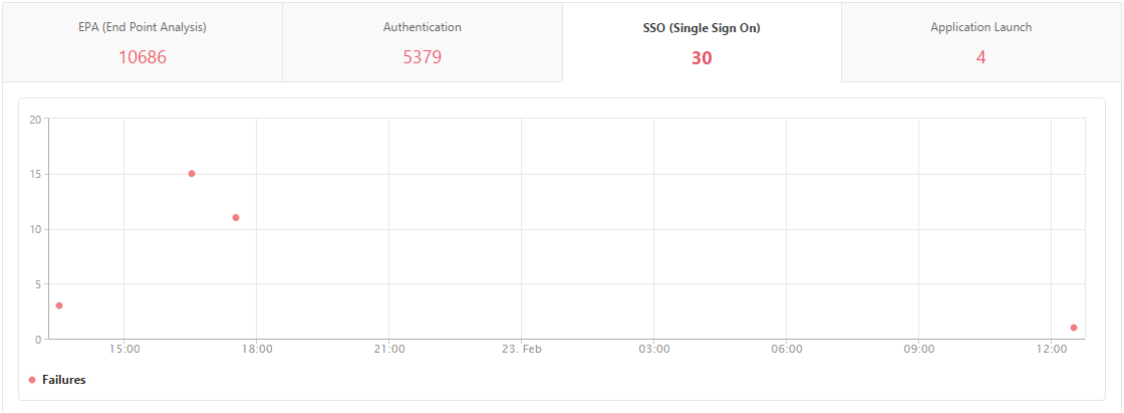
Sie können zu jedem Zeitpunkt alle SSO-Fehler eines Benutzers anzeigen, der über das Citrix Gateway-Gerät auf Anwendungen zugreift.

So zeigen Sie die Details zum SSO-Fehler an:

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Wählen Sie im Abschnitt Übersicht den Zeitraum aus, für den Sie die SSO-Fehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.



3. Klicken Sie auf die Registerkarte **SSO (Single Sign On)**. Sie können die Anzahl der SSO-Fehler jederzeit im Diagramm Fehler anzeigen.



Scrollen Sie nach unten, um Details zu jedem SSO-Fehler wie **Benutzername, NetScaler IP-Adresse, Fehlerzeit, Fehlerbeschreibung, Ressourcenname** und mehr aus der Tabelle auf derselben Registerkarte anzuzeigen.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

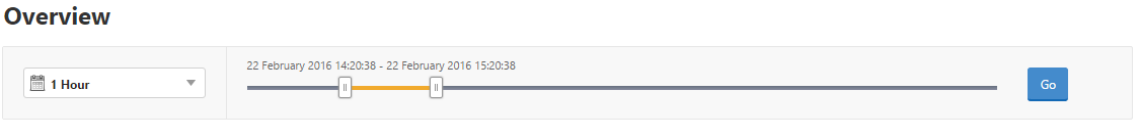
Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die SSO-Fehler und andere Details für diesen Benutzer anzuzeigen. Sie können die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen, indem Sie den Abwärtspfeil verwenden.

Nach erfolgreicher Anmeldung bei Citrix Gateway kann ein Benutzer keine virtuelle Anwendung starten

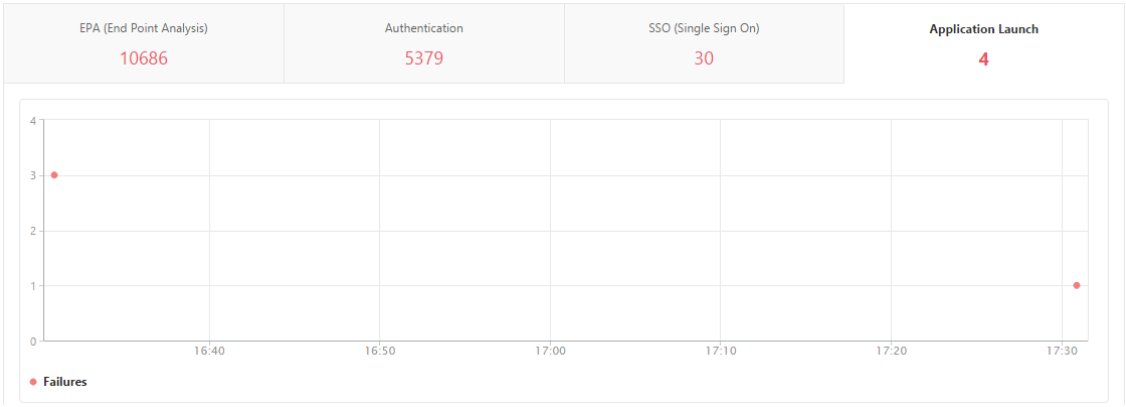
Bei einem Fehler beim Starten der Anwendung erhalten Sie Einblick in die Gründe, z. B. unzugängliche Secure Ticket Authority (STA) - oder Citrix Virtual App-Server oder ein ungültiges STA-Ticket. Sie können den Zeitpunkt des Auftretens des Fehlers, Details des Fehlers und die Ressource anzeigen, für die die STA-Validierung fehlgeschlagen ist.

So zeigen Sie Details zum Anwendungsstart an:

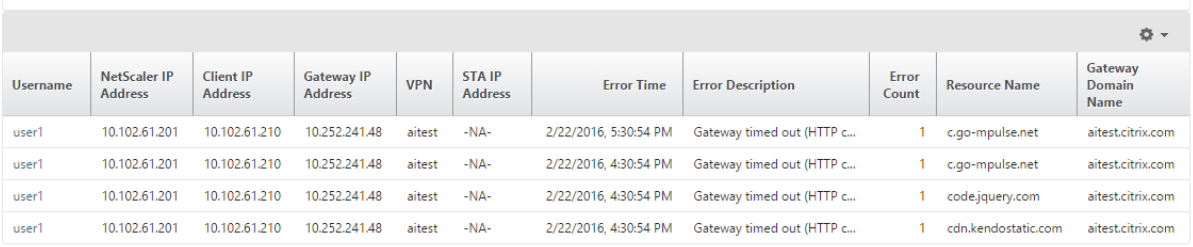
1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Wählen Sie im Abschnitt **Übersicht** den Zeitraum aus, für den Sie die SSO-Fehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.



3. Klicken Sie auf die Registerkarte **Anwendungsstart**. Sie können die Anzahl der Anwendungsstartfehler zu einem bestimmten Zeitpunkt im Diagramm **Fehler** anzeigen.



Führen Sie einen Bildlauf nach unten durch, um Details zu jedem Anwendungsstartfehler wie **NetScaler IP-Adresse, Fehlerzeit, Fehlerbeschreibung, Ressourcenname, Gateway-Domänenname**usw. aus der Tabelle auf derselben Registerkarte anzuzeigen. In der Spalte **Fehlerbeschreibung** in der Tabelle wird die IP-Adresse des STA-Servers angezeigt, und in der Spalte **Ressourcenname** werden die Details der Ressource angezeigt, für die die STA-Validierung fehlgeschlagen ist.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die Programmstartfehler und andere Details für diesen Benutzer anzuzeigen. Sie können die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen, indem Sie den Abwärtspfeil verwenden.

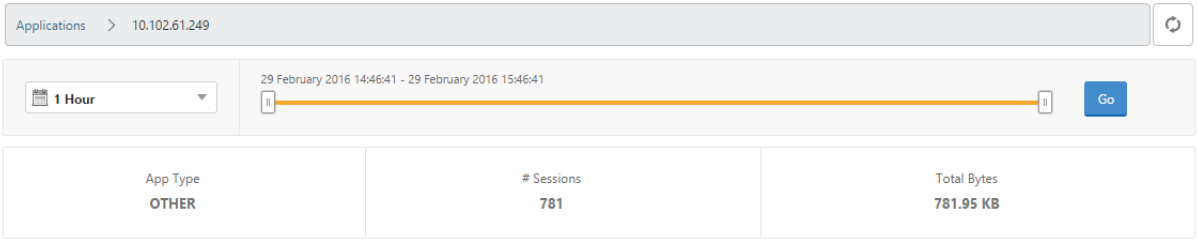
Nachdem eine neue Anwendung erfolgreich gestartet wurde, möchte ein Benutzer die Gesamtbytes und Bandbreite anzeigen, die von dieser Anwendung belegt wurden

Nachdem Sie eine neue Anwendung erfolgreich gestartet haben, können Sie in Citrix ADM die Gesamtbytes und die Bandbreite anzeigen, die von dieser Anwendung verbraucht werden.

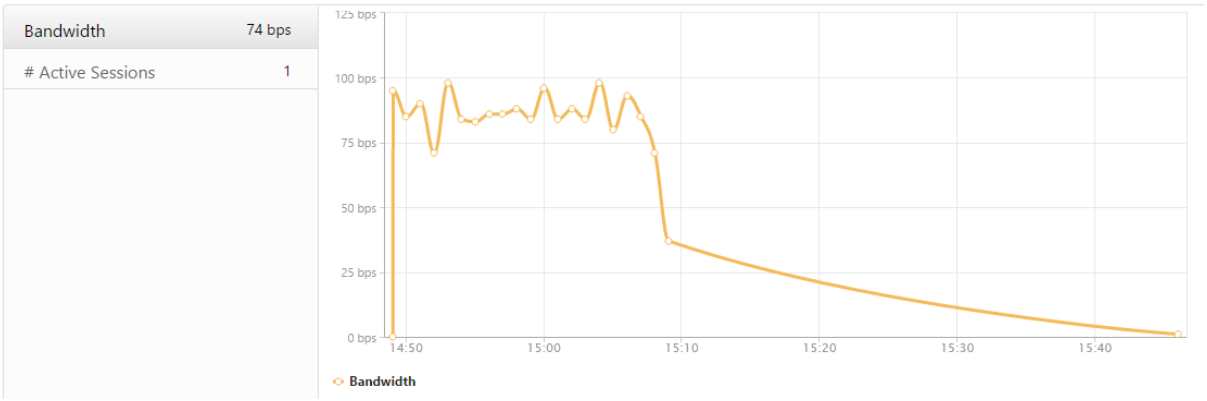
So zeigen Sie die Gesamtanzahl von Bytes und Bandbreite an, die von einer Anwendung verbraucht wird:

Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight > Anwendungen**, scrollen Sie nach unten, und klicken Sie auf der Registerkarte **Andere Anwendungen**auf die Anwendung, für die Sie die Details anzeigen möchten.

Sie können die Anzahl der Sitzungen und die Gesamtanzahl der Bytes anzeigen, die von dieser Anwendung belegt werden.



Sie können auch die von dieser Anwendung verbrauchte Bandbreite anzeigen.

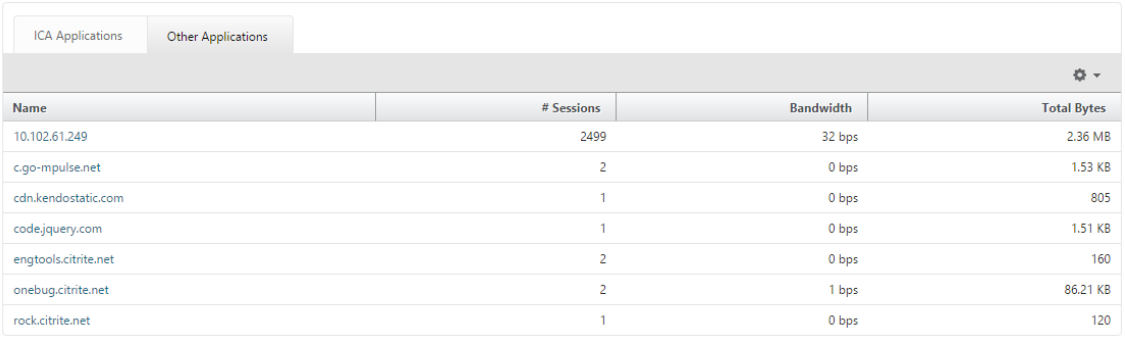


Ein Benutzer hat sich erfolgreich bei Citrix Gateway angemeldet, kann jedoch nicht auf bestimmte Netzwerkressourcen im internen Netzwerk zugreifen

Mit Gateway Insight können Sie feststellen, ob der Benutzer Zugriff auf die Netzwerkressourcen hat oder nicht. Sie können auch den Namen der Richtlinie anzeigen, die zu dem Fehler geführt hat.

So zeigen Sie den Benutzerzugriff auf Ressourcen an:

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight > Applications**.
2. Scrollen Sie auf dem angezeigten Bildschirm nach unten, und wählen Sie auf der Registerkarte **Andere Anwendungen** die Anwendung aus, bei der sich der Benutzer nicht anmelden konnte.



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

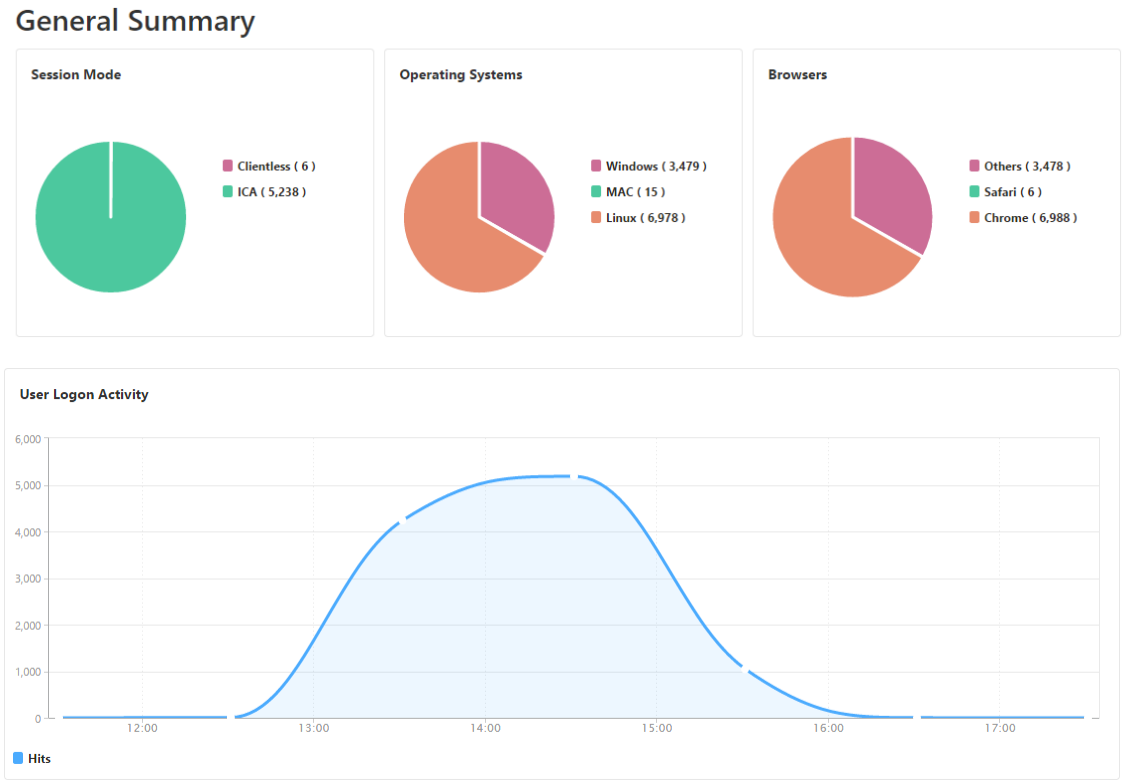
3. Scrollen Sie nach unten, und in der Tabelle **Benutzer** werden alle Benutzer angezeigt, die Zugriff auf diese Anwendung haben.

Verschiedene Benutzer verwenden möglicherweise unterschiedliche Citrix Gateway Bereitstellungen oder melden sich über unterschiedliche Zugriffsmodi bei Citrix Gateway an. Der Administrator muss in der Lage sein, Details zu den Bereitstellungstypen und Zugriffsmodi anzuzeigen

Mit Gateway Insight können Sie eine Zusammenfassung der verschiedenen Sitzungsmodi anzeigen, die von Benutzern für die Anmeldung verwendet werden, die Clienttypen und die Anzahl der stündlich angemeldeten Benutzer. Sie können auch festlegen, ob die Bereitstellung eines Benutzers ein einheitliches Gateway oder eine klassische Citrix Gateway-Bereitstellung ist. Bei Unified Gateway Bereitstellungen können Sie den Namen und die IP-Adresse des virtuellen Content Switching-Servers sowie den Namen des virtuellen VPN-Servers anzeigen.

Um die Zusammenfassung der Sitzungsmodi, der Art der Clients und der Anzahl der angemeldeten Benutzer anzuzeigen, gehen Sie wie folgt vor:

1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Führen Sie im Abschnitt **Übersicht einen** Bildlauf nach unten durch, um die Diagramme **Sitzungsmodus, Betriebssysteme, Browser** und **Benutzeranmeldeaktivitätsdiagramme** anzuzeigen, die von Benutzern zur Anmeldung verwendeten Sitzungsmodi, die Clienttypen und die Anzahl der stündlich angemeldeten Benutzer.



Gateway Insight-Probleme beheben

February 5, 2024

Wenn die Gateway Insight-Lösung nicht wie erwartet funktioniert, liegt das Problem möglicherweise an einer der folgenden Ursachen. Informationen zur Fehlerbehebung finden Sie in den Checklisten in den entsprechenden Abschnitten.

- Gateway Insight-Konfiguration.
- Verbindungsproblem zwischen NetScaler ADC und NetScaler ADM.
- Datensatzgenerierung in NetScaler ADC.
- Validierungen in NetScaler ADM.

Checkliste für die Konfiguration von Gateway Insight

- Stellen Sie sicher, dass die AppFlow-Funktion in der NetScaler ADC Appliance aktiviert ist. Einzelheiten finden Sie unter AppFlow aktivieren.
- Überprüfen Sie die Gateway Insight-Konfiguration in der laufenden Konfiguration von NetScaler ADC.

Führen Sie den Befehl `show running | grep -i <appflow_policy>` aus, um die Gateway Insight-Konfiguration zu überprüfen. Stellen Sie sicher, dass der Bindungstyp REQUEST ist. Zum Beispiel;

```
bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
<!--NeedCopy-->
```

Der Bind-Typ OTHERTCP_REQUEST ist auch für Gateway Insight erforderlich.

```
bind vpn vserver afsanity -policy afp -priority 100 -type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```

- Stellen Sie bei der Bereitstellung von Single-Hop-, Access Gateway- oder Unified Gateway-Bereitstellung sicher, dass die Gateway Insight AppFlow Richtlinie an den virtuellen VPN-Server gebunden ist, auf dem der VPN-Datenverkehr fließt. Einzelheiten finden Sie unter HDX Insight-Datenerfassung aktivieren.
- Für Double-Hop muss Gateway Insight auf beiden Hops konfiguriert sein.
- Überprüfen Sie die Parameter `appflowlog` auf dem virtuellen NetScaler Gateway/VPN-Server. Einzelheiten finden Sie unter AppFlow für virtuelle Server aktivieren.

Konnektivität zwischen NetScaler ADC und NetScaler ADM Checkliste

- Überprüfen Sie den AppFlow Collector-Status in NetScaler ADC. Einzelheiten finden Sie unter So überprüfen Sie den Status der Konnektivität zwischen NetScaler ADC und AppFlow Collector.
- Überprüfen Sie Gateway Insight AppFlow Richtlinientreffer.

  Führen Sie den Befehl `show appflow policy <policy_name>` aus, um die Treffer der AppFlow-Richtlinie zu überprüfen.

  Sie können auch in der GUI zu **System > AppFlow > Richtlinien** navigieren, um die AppFlow-Richtlinientreffer zu überprüfen.
- Überprüfen Sie jede Firewall, die AppFlow Ports 4739 oder 5557 blockiert.

Datensatzgenerierung in NetScaler ADC Checkliste

- Führen Sie den Befehl `nsconmsg -d stats -g ai_tot` aus und suchen Sie nach den Statistik-Inkrementen in NetScaler ADC.
- Zeichnen Sie `nstrace logs` auf und prüfen Sie CFLOW-Pakete, um zu bestätigen, dass NetScaler ADC AppFlow-Datensätze exportiert.

> **Hinweis:**
>
> Die `nstrace logs` sind nur für IPFIX erforderlich. Bei Logstream bestätigen nstrace-Protokolle nicht, ob die ADC-Appliance die AppFlow-Datensätze exportiert hat.

Validierung von Datensätzen in NetScaler ADM

- Führen Sie den Befehl `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` aus, um die Protokolle zu überprüfen, um zu bestätigen, dass NetScaler ADM AppFlow-Einträge erhält.
- Stellen Sie sicher, dass die NetScaler ADC-Instanz zum NetScaler ADM hinzugefügt wird.
- Stellen Sie sicher, dass der virtuelle NetScaler Gateway/VPN-Server in NetScaler ADM lizenziert ist.

Validierung von Logstream-Protokollen in NetScaler ADM

Die Validierung der von NetScaler ADM empfangenen Logstream-Daten kann mit den folgenden Methoden erfolgen:

- **Aktivieren der Datendatensatzprotokollierung in NetScaler ADM**

  Nach der Aktivierung können die Protokolle in /var/mps/log/mps_afdecoder.log angezeigt werden

- **Aktivieren der Protokollierung von ULFD-Bibliothek**

  Führe den Befehl aus `/mps/decoder_enable_debug`

  Die Protokolle werden in `/var/ulflog/libulfd.log` aufgezeichnet

  Sie können die Protokollierung mit dem Befehl `/mps/decoder_disable_debug` deaktivieren

Gateway Insight-Zähler

Die folgenden Gateway Insight-Leistungsindikatoren sind verfügbar.

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export

- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled
- ai_tot_appflow_pol_eval_in_gwinsight
- ai_tot_app_launch_success

AppFlow-Einträge im NetScaler ADC-Protokoll

Ab Release 13.0 Build 71.x können Sie die NetScaler ADC-Protokolle überprüfen, um zu bestätigen, ob die AppFlow-Datensätze exportiert werden. Die Standardprotokollstufe von `syslogparams` erfasst alle Fehler- und Informationsprotokolle. Falls Sie keine Ahnung über die Fehler finden, aktivieren Sie alle Protokollebenen einschließlich DEBUG in `syslogparams`, um sogar die DEBUG-Protokolle zu erfassen.

Beispielprotokolle

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 147 0 : "
    GwInsight: Sent auth record Func=ns_sslvpn_export_auth_data Username
    =<name> Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid>
    Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<
    vpnfqdn> Authtype=3 EPAid=(null) AuthStage=1 AuthDuration=309
    AuthAgent=<auth_server_ip> Groupname= Policyname=<name>
    CurfactorPolname=<name> NextfactorPolname= CSecExpr= Devicetype
    =16777219 Deviceid=0 email="
<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight
    : Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is
    zero"
<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight
    : Func=update_session_appflow_collector pcb or session is NULL"
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 165 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<> Clientip=<ip>:<port> Destip
    =<ip>:80 SessSeq=1 Sessid=<sessid> Gwip=<ip>:443 StatusCode=0
    CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=0 SessState
    =2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/Citrix/Store
Web BackendServername= SSOurl= email="
SSO logs:
<!--NeedCopy-->
```



```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 463 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=1
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 582 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=3
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 513 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=2
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:443 SessSeq=c Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =155 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=6
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

Wenden Sie sich an den technischen Support von Citrix

Stellen Sie für eine schnelle Lösung sicher, dass Sie über die folgenden Informationen verfügen, bevor Sie sich an den technischen Support von Citrix wenden:

- Einzelheiten zur Bereitstellung und Netzwerktopologie.
- NetScaler ADC- und NetScaler ADM-Versionen.
- Technisches Support-Paket für NetScaler ADC und NetScaler ADM.
- `nstrace` während der Ausgabe erfassen.

Bekannte Probleme

Informationen zu bekannten Problemen in Gateway Insight finden Sie in den NetScaler ADC Versionshinweisen

Security Insight

February 5, 2024

> Hinweis
>
> Wenn Ihr NetScaler ADM-Build früher als **13.0-79.x**ist, können Sie Sicherheitseinblicke einsehen, indem Sie zu **Analytics > Sicherheit > Security Insight**navigieren. Für Build **13.0-79.x oder höher**können Sie die Details zur WAF-Verletzung anzeigen, indem Sie zu **Analytics > Sicherheit > Sicherheitsverstöße > Anwendungsübersicht** navigieren und unter **Aufschlüsselung der Anwendungen nach** auf **WAF**klicken.

Web- und Webdienstanwendungen, die dem Internet ausgesetzt sind, sind zunehmend anfällig für Angriffe geworden. Um Anwendungen vor Angriffen zu schützen, benötigen Sie Einblick in Art und Ausmaß vergangener, aktueller und drohender Bedrohungen, in Echtzeit verwertbare Daten zu Angriffen und Empfehlungen zu Gegenmaßnahmen. Security Insight bietet eine Lösung aus einem Bereich, mit der Sie Ihren Anwendungssicherheitsstatus beurteilen und Korrekturmaßnahmen ergreifen können, um Ihre Anwendungen zu schützen.

> **Hinweis**
>
> Security Insight wird von Citrix Application Delivery Management (ADM) mit Citrix ADC Appliances unterstützt, die auf Version 11.0 Build 65.31 und höher ausgeführt werden.

Funktionsweise von Security Insight

Security Insight ist eine intuitive Dashboard-basierte Sicherheitsanalyselösung, die Ihnen umfassenden Einblick in die Bedrohungsumgebung bietet, die mit Ihren Anwendungen verbunden ist. Sicherheitsinformationen sind in Citrix ADM enthalten und werden regelmäßig Berichte basierend auf den Sicherheitskonfigurationen der Application Firewall und des Citrix ADC -Systems generiert. Die Berichte enthalten für jede Anwendung die folgenden Informationen:

- **Bedrohungsindex.** Ein einstelliges Bewertungssystem, das die Wichtigkeit von Angriffen auf die Anwendung angibt, unabhängig davon, ob die Anwendung durch eine Citrix ADC Appliance geschützt ist oder nicht. Je kritischer die Angriffe auf eine Anwendung sind, desto höher ist der Bedrohungsindex für diese Anwendung. Die Werte reichen von 1 bis 7.

Der Bedrohungsindex basiert auf Angriffsinformationen. Die angriffsbezogenen Informationen wie Verstoßtyp, Angriffskategorie, Standort und Client-Details geben Ihnen Einblick in die Angriffe auf die Anwendung. Verstöße werden nur dann an NetScaler ADM gesendet, wenn eine Verletzung oder ein Angriff auftritt. Viele Verstöße und Schwachstellen führen zu einem hohen Bedrohungsindexwert.

- **Sicherheitsindex.** Ein einstelliges Bewertungssystem, das angibt, wie sicher Sie die NetScaler ADC-Instanzen zum Schutz von Anwendungen vor externen Bedrohungen und Sicherheitslücken konfiguriert haben. Je niedriger die Sicherheitsrisiken für eine Anwendung, desto höher der Sicherheitsindex. Die Werte reichen von 1 bis 7.

  Der Sicherheitsindex berücksichtigt sowohl die Konfiguration der Anwendungsfirewall als auch die Sicherheitskonfiguration des NetScaler ADC -Systems. Für einen hohen Sicherheitsindex müssen beide Konfigurationen stark sein. Wenn beispielsweise strenge Prüfungen der Anwendungsfirewall vorhanden sind, aber Sicherheitsmaßnahmen für NetScaler ADC-Systeme, z. B. ein sicheres Kennwort für den `nsroot` Benutzer, nicht übernommen wurden, wird Anwendungen ein niedriger Sicherheitsindexwert zugewiesen.

- **Umsetzbare Informationen.** Die Informationen, die Sie benötigen, um den Bedrohungsindex zu senken und den Sicherheitsindex zu erhöhen, was die Anwendungssicherheit erheblich verbessert. Beispielsweise können Sie Informationen zu Verstößen, vorhandenen und fehlenden Sicherheitskonfigurationen für die Anwendungsfirewall und andere Sicherheitsfunktionen, die Rate, mit der die Anwendungen angegriffen werden, usw. überprüfen.

Konfigurieren von Security Insight

Citrix ADM unterstützt Security Insight von allen Citrix ADC Instanzen, auf denen eine Anwendungsfirewall konfiguriert ist.

Um Sicherheitsinformationen für eine ADC-Instanz zu konfigurieren, konfigurieren Sie zunächst ein Anwendungs-Firewall-Profil und eine Anwendungs-Firewall-Richtlinie. Obwohl Sie die Firewall-Richtlinie für die Anwendung global binden können, empfiehlt Citrix, dass die Richtlinie an den virtuellen Server gebunden ist.

Um die Analysen in Citrix ADM anzuzeigen, aktivieren Sie das AppFlow Feature in der Instanz, konfigurieren Sie einen AppFlow-Collector, eine Aktion und eine Richtlinie und binden die Richtlinie global. Auch wenn Sie die Firewall-Richtlinie der Anwendung global binden können, empfiehlt Citrix, dass die Richtlinie an den virtuellen Server gebunden ist. Citrix empfiehlt außerdem, dass Sie AppFlow Konfigurationen auf den ADC-Instanzen mit Citrix ADM bereitstellen. Wenn Sie den Collector konfigurieren, müssen Sie die IP-Adresse des NetScaler ADM-Servers angeben, auf dem Sie die Berichte überwachen möchten.

So konfigurieren Sie Sicherheitsinformationen für eine Citrix ADC Instanz:

1. Führen Sie die folgenden Befehle aus, um ein Anwendungsfirewallprofil und eine Richtlinie zu konfigurieren und die Anwendungsfirewall global oder an den virtuellen Lastausgleichsserver zu binden.

---

add appfw profile [**-defaults** (basic advanced)]

---

set appfw profile <name> [**-startURLAction** <startURLAction> …]

add appfw policy <name> <rule> <profileName>

bind appfw global <policyName> <priority>

Oder

bind lb vserver <lb vserver> **-policyName** <policy> **-priority** <priority>

```
add appfw profile pr_appfw -defaults advanced
set  appfw profile pr_appfw -startURLaction log stats learn
add appfw policy pr_appfw_pol "HTTP.REQ.HEADER("Host").EXISTS"
   pr_appfw
bind appfw global pr_appfw_pol 1
or,
bind lb vserver outlook – policyName pr_appfw_pol – priority “20
   ”
<!--NeedCopy-->
```

2. Führen Sie die folgenden Befehle aus, um das AppFlow Feature zu aktivieren, einen AppFlow-Kollektor, eine Aktion und eine Richtlinie zu konfigurieren und die Richtlinie global oder an den virtuellen Lastausgleichsserver zu binden:

add appflow collector <name> **-IPAddress** <ipaddress>

---

set appflow param DISABLED)]
[**-SecurityInsightRecordInterval**]
[**-SecurityInsightTraffic** (ENABLED

---

add appflow action <name> **-collectors** <string>

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

oder,

bind lb vserver <vserver> **-policyName** <policy> **-priority** <priority>

```
add appflow collector col -IPAddress 10.102.63.85
set appflow param  -SecurityInsightRecordInterval 600 -
   SecurityInsightTraffic ENABLED
```



```
add appflow action act1 -collectors col
add appflow action af_action_Sap_10.102.63.85 -collectors col
add appflow policy pol1 true act1
add appflow policy af_policy_Sap_10.102.63.85 true
   af_action_Sap_10.102.63.85
bind appflow global pol1 1 END -type REQ_DEFAULT
or,
bind lb vserver Sap  – policyName af_action_Sap_10.102.63.85  –
   priority  “ 20 ”
<!--NeedCopy-->
```

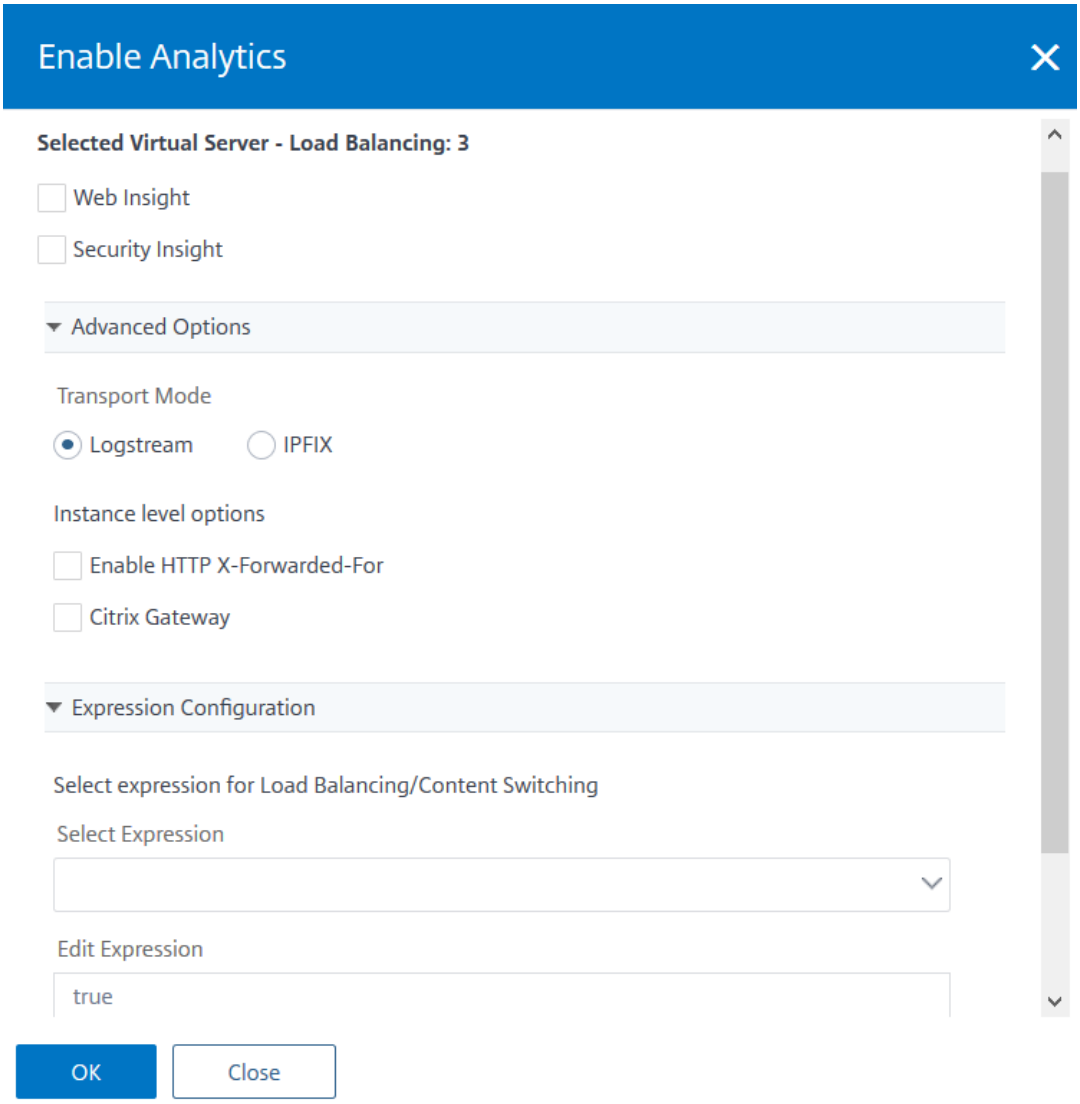
So aktivieren Sie Security Insight von NetScaler ADM:

Wenn Sie NetScaler ADM **13.0 Build 41.x** verwenden:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC**, und wählen Sie den Instanztyp aus. Zum Beispiel VPX.
2. Wählen Sie die Instanz aus, und klicken Sie in der Liste **Aktion auswählen** auf **Analytics konfigurieren**.
3. Wählen Sie auf der Seite **Analytics auf virtuellen Servern konfigurieren** den virtuellen Server aus und klicken Sie auf **Analytics aktivieren**.
4. Gehen Sie im Fenster **Enable Analytics** wie folgt vor:
   a) **Sicherheitsinformationen**auswählen
   b) Wählen Sie **Logstream** als Transportmodus

      > **Hinweis**
      >
      > Für NetScaler ADC 12.0 oder früher ist **IPFIX** die Standardoption für den Transportmodus. Für NetScaler ADC 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.
      >
      > Weitere Informationen zu IPFIX und Logstream finden Sie unter Logstream-Übersicht .

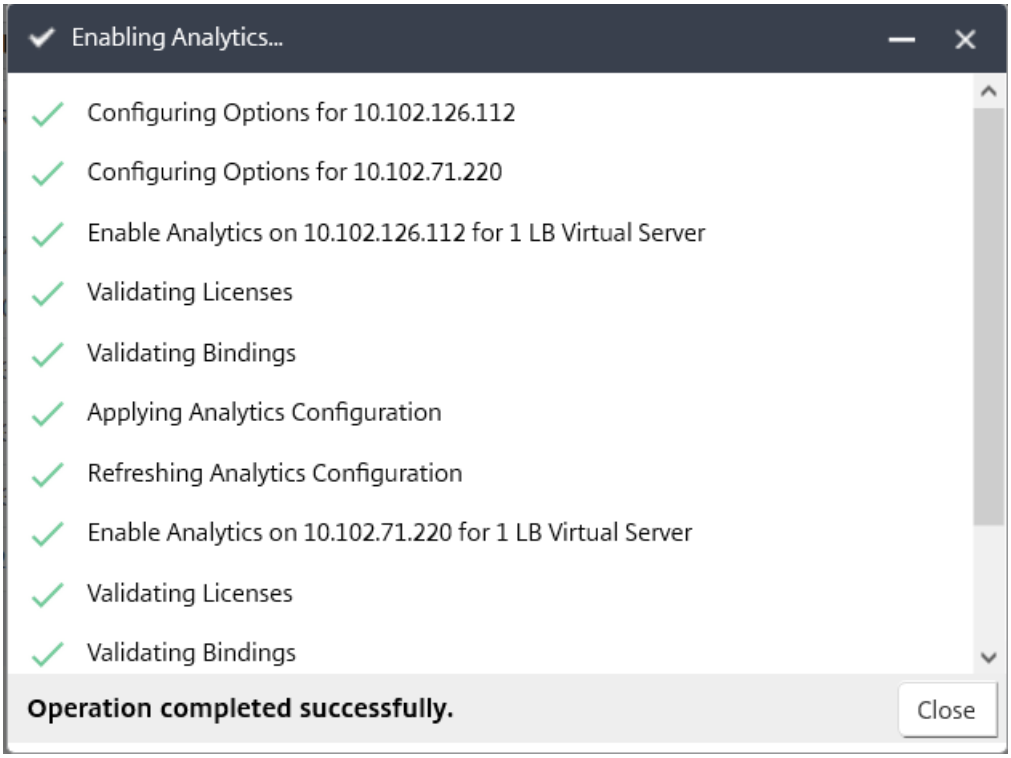
   c) Der Ausdruck ist standardmäßig wahr
   d) Klicken Sie auf **OK**.



Hinweis

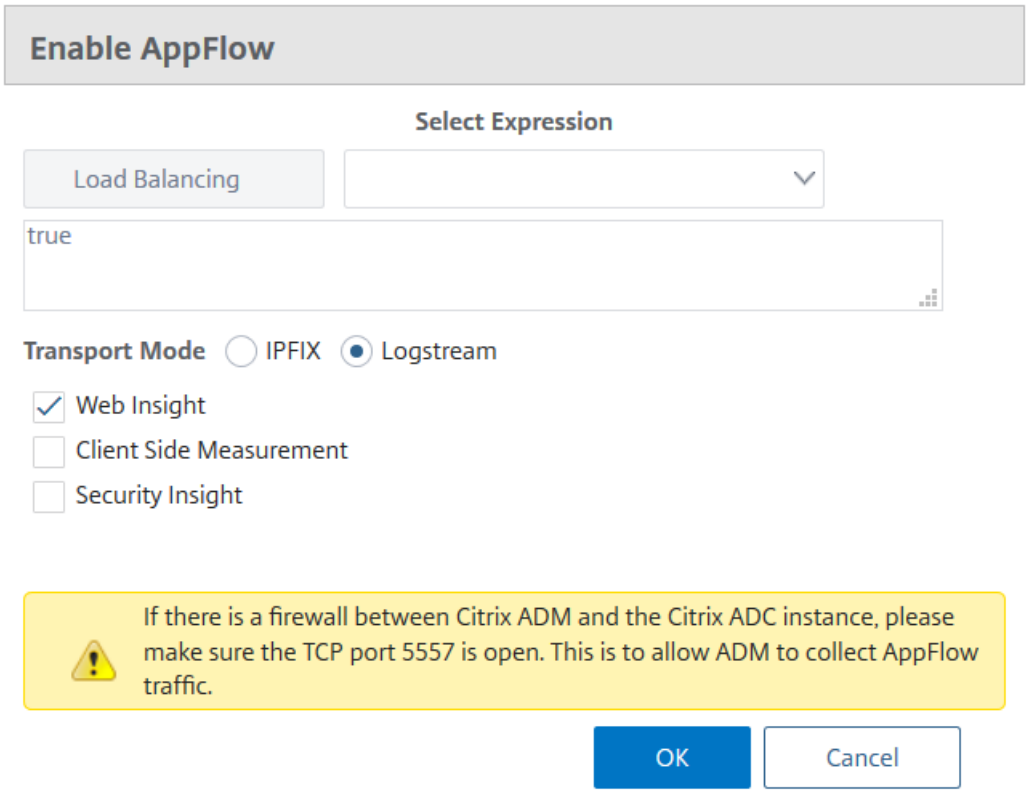
- Wenn Sie virtuelle Server auswählen, die nicht lizenziert sind, lizenziert NetScaler ADM zuerst diese virtuellen Server und aktiviert dann Analysen.
- Für Admin-Partitionen wird nur **Web Insight** unterstützt
- Für virtuelle Server wie Cache-Umleitung , Authentifizierung und GSLB können Sie Analysen nicht aktivieren. Eine Fehlermeldung wird angezeigt.

Nachdem Sie auf **OK** geklickt haben, verarbeitet NetScaler ADM Analysen auf den ausgewählten virtuellen Servern zu aktivieren.



Wenn Sie NetScaler ADM **13.0 Build 36.27** verwenden:

1. Navigieren Sie zu **Netzwerke** > **Instanzen**, und wählen Sie die NetScaler ADC Instanz aus, die AppFlow aktiviert werden soll.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
3. Wählen Sie die virtuellen Server aus, und klicken Sie auf **AppFlow aktivieren**.
4. Geben Sie im Feld **AppFlow aktivieren** den **Wert true**ein, und wählen Sie **Security Insight**aus.
5. Klicken Sie auf **OK**.



> **Hinweis**
>
> Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, Zugriff auf Anwendungsebene für die Gruppe gewähren und Benutzer der Gruppe zuweisen. Citrix ADM Analytics unterstützt jetzt die auf virtuellen IP-Adressen basierende Autorisierung. Ihre Benutzer können jetzt Berichte für alle Insights nur für die Anwendungen (virtuelle Server) anzeigen, für die sie autorisiert sind. Weitere Informationen zu Gruppen und zum Zuweisen von Benutzern zur Gruppe finden Sie unter Konfigurieren von Gruppen.

Geo-Standorte für Security Insight-Berichte anzeigen

Security Insight-Berichte enthalten die genauen geografischen Standorte, von denen Clientanforderungen stammen. Sie können die geografischen Standorte in Citrix ADM anzeigen. Die Geodatenbankdatei, die in Citrix ADC integriert ist, enthält die meisten öffentlichen IP-Adressen. Die Datei ist unter **/var/netscaler/inbuilt_db** in Citrix ADC verfügbar.

So aktivieren Sie Geostandorte:

Führen Sie die folgenden Befehle aus, um die Geo-Location-Protokollierung und -Protokollierung im CEF-Format zu aktivieren:

- **add locationFile** <Complete path with the DB filename>

- **set appfw settings -geoLocationLogging ON**
- **set appfw settings -CEFLogging ON**

Wenn keine IP-Adresse in der Geodatenbankdatei verfügbar ist, können Sie die IP-Adresse für den geografischen Standort hinzufügen. Zusammen mit der IP-Adresse können Sie auch Stadt/Bundesland/-Land Namen und die Breiten- und Längengradkoordinaten jedes Standorts hinzufügen.

Öffnen Sie die Geodatenbankdatei mit einem Texteditor, z. B. vi-Editor, und fügen Sie für jeden Speicherort einen Eintrag hinzu.

Der Eintrag muss das folgende Format haben:

```
\<start IP\>,\<end IP\>,,\<country\>,\<state\>,,\<city\>,,longitude,
latitude
```

Beispiel:

```
4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568
<!--NeedCopy-->
```

IP-Reputation

Sie können NetScaler Insight Center verwenden, um die IP-Reputation Ihres eingehenden Datenverkehrs zu überwachen und zu verwalten. Sie können Richtlinien so konfigurieren, dass weitere IPs bösartig hinzugefügt werden, und eine benutzerdefinierte Blockliste erstellen.

Informationen zur Konfiguration und Verwendung von IP-Reputation finden Sie unter IP-Reputation.

Überwachen der IP-Reputation

Die IP-Reputation-Funktion bietet angriffsbezogene Informationen über bösartige IP-Adressen. Beispielsweise werden IP-Reputationsbewertung, IP-Reputationskategorie, IP-Reputation-Angriffszeit, Geräte-IP und Details zur Client-IP-Adresse gemeldet.

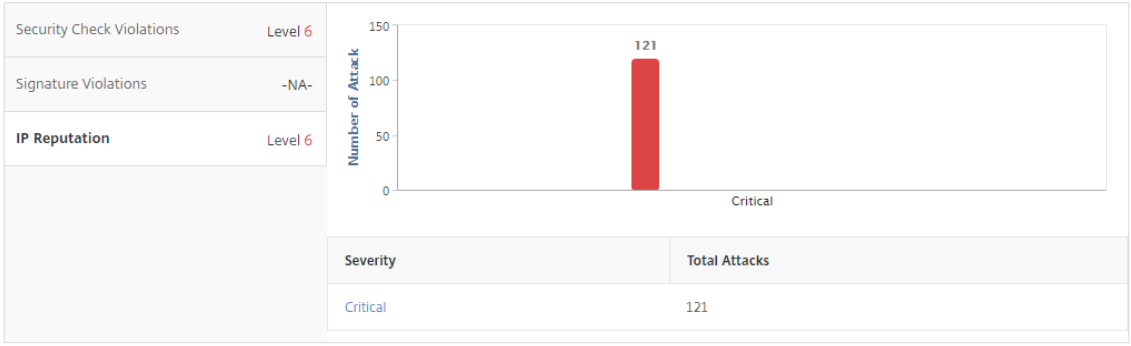
IP-Reputationsbewertung gibt das Risiko an, das mit einer IP-Adresse verbunden ist. Die Punktzahl hat die folgenden sind die Bereiche:

Bewertung der IP-Reputation	Grad des Risikos
1–20	Hohes Risiko
21–40	Verdächtig
41–60	Mäßiges Risiko
61–80	Niedriges Risiko

Bewertung der IP-Reputation	Grad des Risikos
81–100	Vertrauensvoll

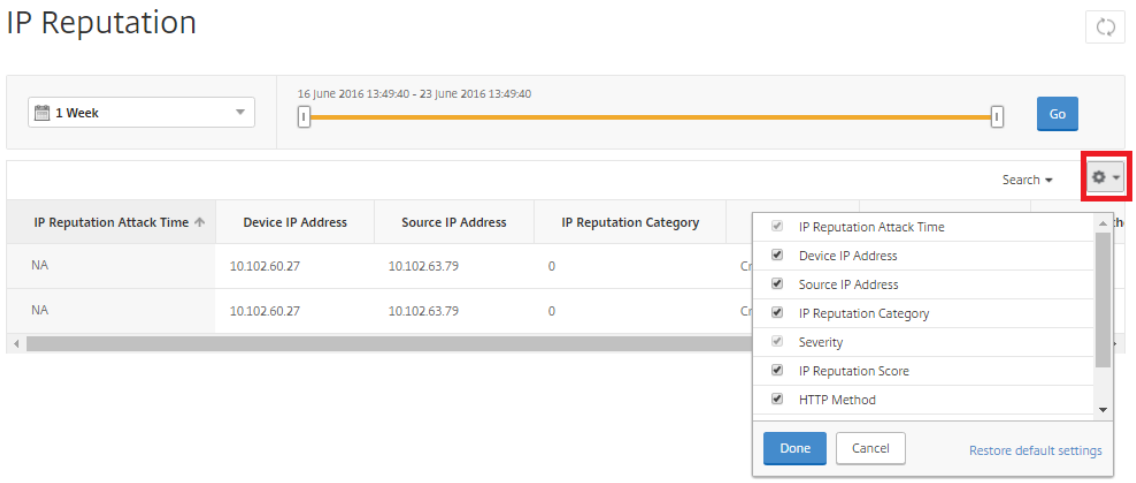
So überwachen Sie die IP-Reputation:

1. Navigieren Sie zu **Analytics**> **Security Insight**, und wählen Sie die Anwendung aus, die Sie überwachen möchten.
2. Wählen Sie auf der Registerkarte **Bedrohungsindex** die Option **IP-Reputation** aus.



3. Wählen Sie einen Schweregrad aus, um weitere Details zu den Angriffen anzuzeigen, die sich auf dieser Ebene befanden. Sie können auf das Balkendiagramm oder in der Tabelle unter dem Diagramm klicken.
4. Wählen Sie den Zeitraum aus, für den Sie die Details anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie dann auf **Los**.

5. Um die Anzeige anzupassen, klicken Sie auf die Schaltfläche Einstellungen.



Schwellenwerte

In Security Insight können Sie Schwellenwerte für den Sicherheitsindex und den Bedrohungsindex von Anwendungen festlegen und anzeigen.

So legen Sie einen Schwellenwert fest:

1. Navigieren Sie zu **Analytics** > **Einstellungen** > **Schwellenwerte**, und wählen Sie **Hinzufügen**aus.
2. Wählen Sie im Feld **Verkehrstyp** den Verkehrstyp als **Sicherheit** aus und geben Sie die erforderlichen Informationen in die anderen entsprechenden Felder wie Name, Dauer und Entität ein.
3. Verwenden **Sie im Abschnitt Regel konfigurieren** die Felder Metrik, Komparator und Wert, um einen Schwellenwert festzulegen.

   Zum Beispiel “Bedrohungsindex”“>”“5”
4. Wählen Sie in den **Benachrichtigungseinstellungen**den Benachrichtigungstyp aus.
5. Klicken Sie auf **Erstellen**.

So zeigen Sie die Schwellenwertverletzungen an:

1. Navigieren Sie zu **Analytics** > **Security Insight** > **Devices**, und wählen Sie die Citrix ADC Instanz aus.
2. Im Abschnitt “**Anwendung** “können Sie in der Spalte “Schwellenwertüberschreitung”die Anzahl der **Schwellenwertverletzungen** für jeden virtuellen Server anzeigen.

Anwendungsfälle für Security Insight

In den folgenden Anwendungsfällen wird beschrieben, wie Sie Sicherheitsinformationen verwenden können, um die Bedrohungsgefahr von Anwendungen zu bewerten und Sicherheitsmaßnahmen zu verbessern.

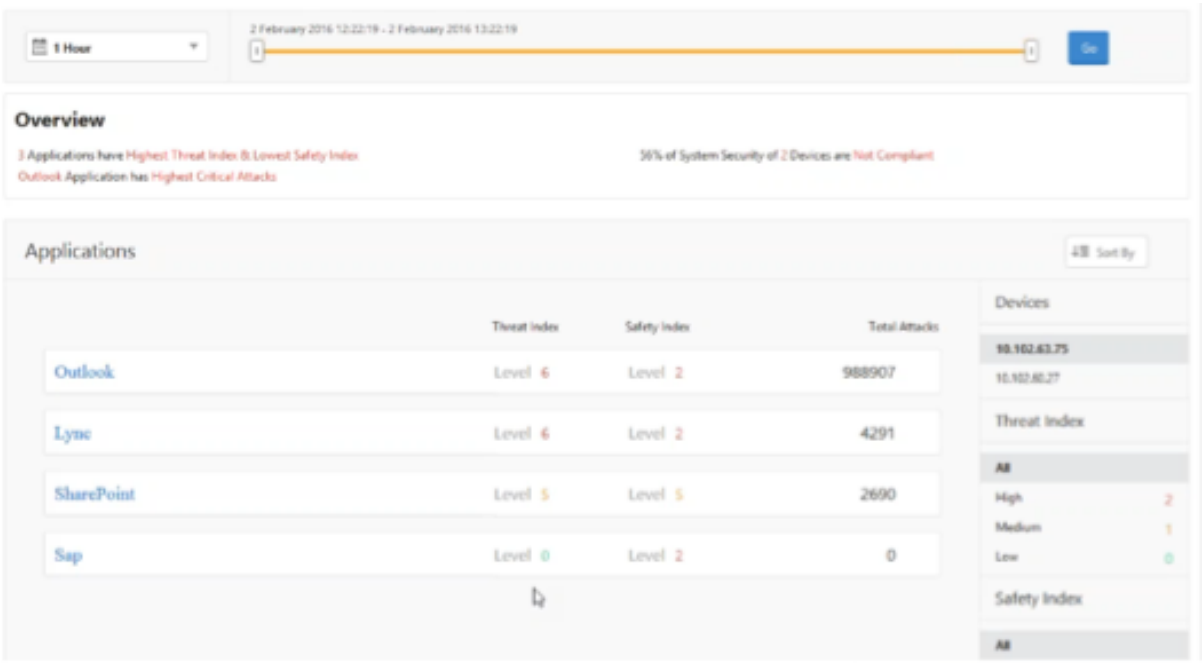
Verschaffen Sie sich einen Überblick über die Bedrohungs

In diesem Anwendungsfall verfügen Sie über eine Reihe von Anwendungen, die Angriffen ausgesetzt sind, und Sie haben NetScaler ADM für die Überwachung der Bedrohungsumgebung konfiguriert. Sie müssen häufig den Bedrohungsindex, den Sicherheitsindex sowie die Art und den Schweregrad aller Angriffe, die in den Anwendungen aufgetreten sind, überprüfen, damit Sie sich zuerst auf die Anwendungen konzentrieren können, die die größte Aufmerksamkeit benötigen. Das Security Insight-Dashboard bietet eine Zusammenfassung der Bedrohungen, die Ihre Anwendungen über einen bestimmten Zeitraum Ihrer Wahl und für ein ausgewähltes NetScaler ADC Gerät ausgesetzt haben. Es zeigt die Liste der Anwendungen, deren Bedrohungs- und Sicherheitsindizes sowie die Gesamtzahl der Angriffe für den gewählten Zeitraum an.

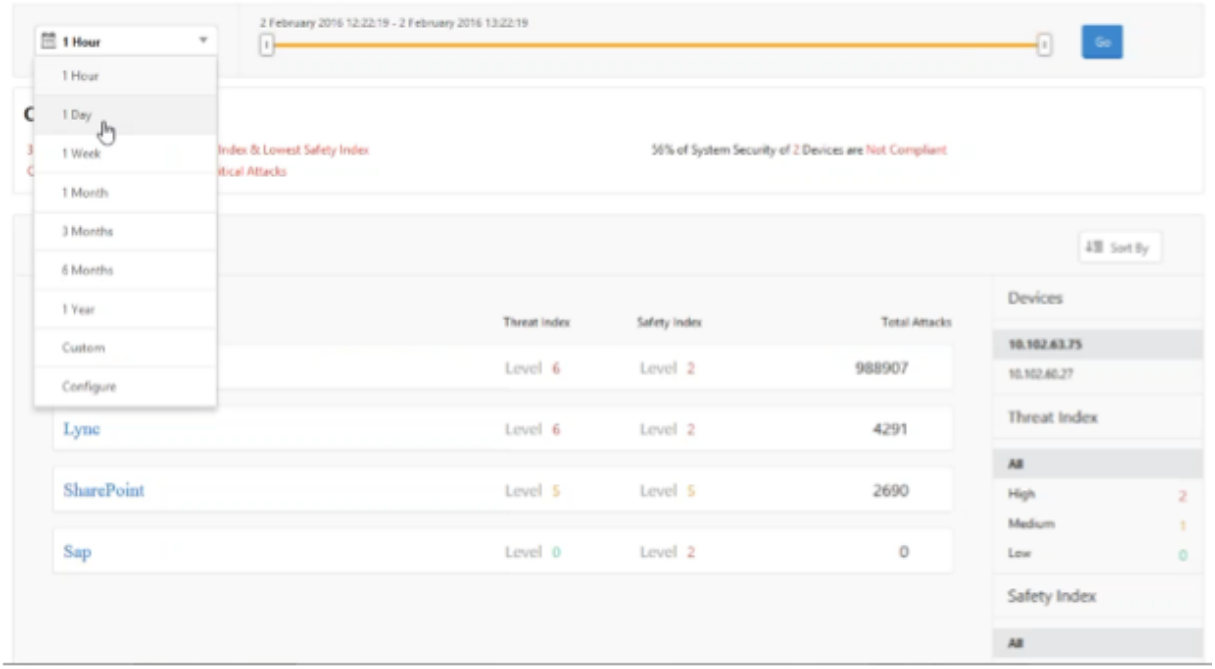
Sie könnten beispielsweise Microsoft Outlook, Microsoft Lync, SharePoint und eine SAP-Anwendung überwachen und eine Zusammenfassung der Bedrohungsumgebung für diese Anwendungen überprüfen.

Um eine Zusammenfassung der Bedrohungsumgebung zu erhalten, melden Sie sich bei **NetScaler ADM**an und navigieren Sie dann zu **Analytics > Security Insight**.

Für jede Anwendung werden Schlüsselinformationen angezeigt. Der Standardzeitraum ist 1 Stunde.



Um Informationen für einen anderen Zeitraum anzuzeigen, wählen Sie in der Liste oben links einen Zeitraum aus.



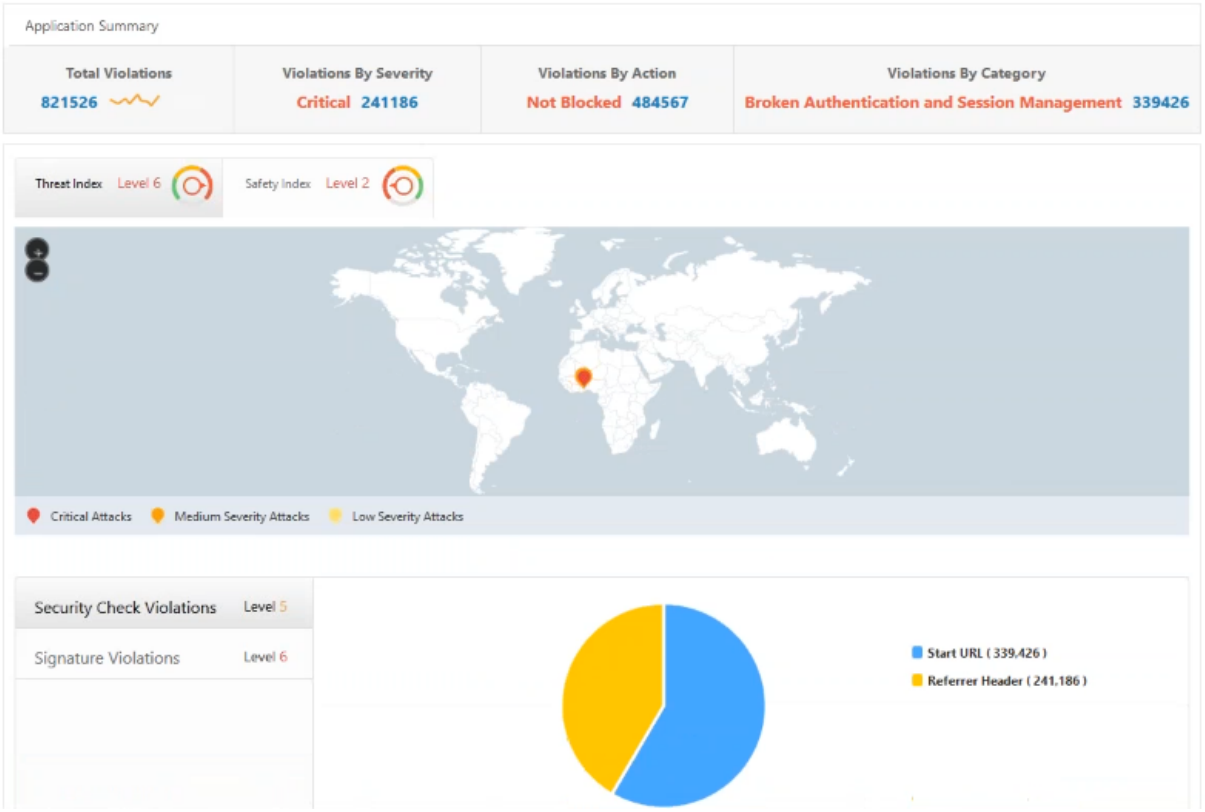
Um eine Zusammenfassung für eine andere NetScaler ADC Instanz anzuzeigen, klicken Sie unter **Geräte**auf die IP-Adresse der NetScaler ADC-Instanz. Um die Anwendungsliste nach einer bestimmten Spalte zu sortieren, klicken Sie auf die Spaltenüberschrift.

Bestimmen der Gefährdung einer Anwendung

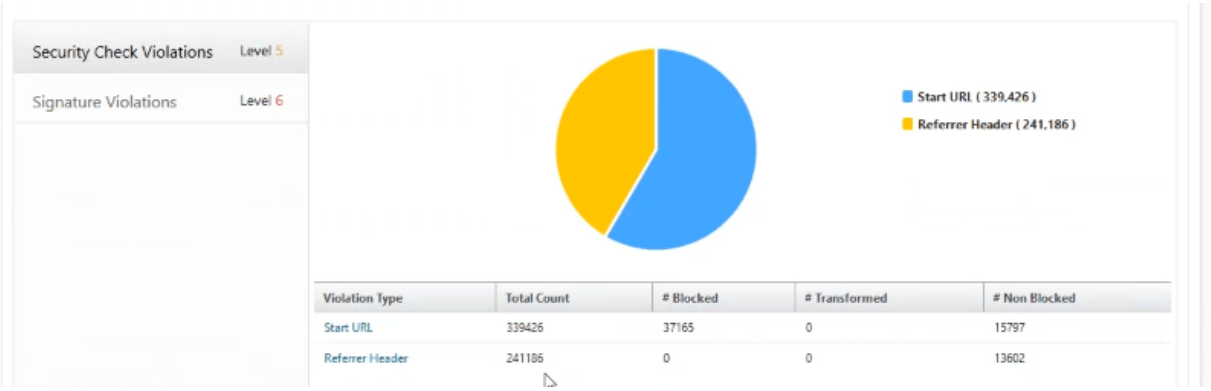
Um die Anwendungen zu identifizieren, die über einen hohen Bedrohungsindex und einen niedrigen Sicherheitsindex im Security Insight-Dashboard verfügen, sollten Sie die Bedrohung ermitteln, bevor Sie sich entscheiden, sie zu schützen. Das heißt, Sie möchten den Typ und den Schweregrad der Angriffe bestimmen, die ihre Indexwerte verschlechtern. Sie können die Bedrohungsgefahr einer Anwendung ermitteln, indem Sie die Anwendungsübersicht überprüfen.

In diesem Beispiel hat Microsoft Outlook den Bedrohungsindexwert 6, und Sie möchten wissen, welche Faktoren zu diesem hohen Bedrohungsindex beitragen.

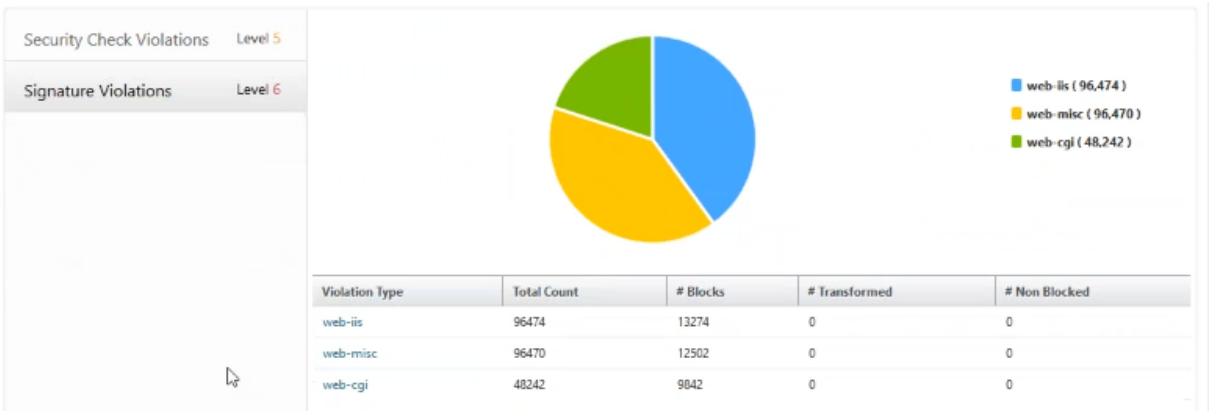
Klicken Sie im **Security Insight-Dashboard** auf Outlook, um die Bedrohungsgefahr von Microsoft **Outlook** zu ermitteln. Die Anwendungsübersicht enthält eine Karte, die den geografischen Standort des Servers identifiziert.



Klicken Sie auf **Bedrohungsindex > Sicherheitsüberprüfungsverstöße**, und überprüfen Sie die angezeigten Informationen zur Verletzung.



Klicken Sie auf **Signaturverletzungen**, und überprüfen Sie die angezeigten Verstoßinformationen.

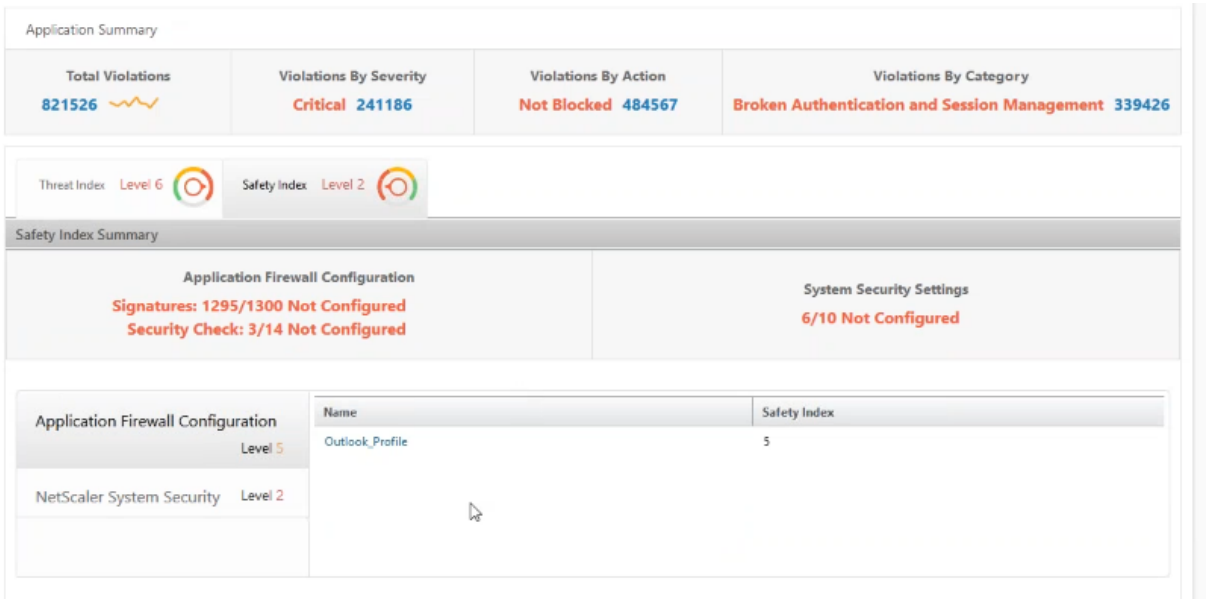


Bestimmen der vorhandenen und fehlenden Sicherheitskonfiguration für eine Anwendung

Nachdem Sie die Bedrohungsgefahr einer Anwendung überprüft haben, möchten Sie ermitteln, welche Anwendungssicherheitskonfigurationen vorhanden sind und welche Konfigurationen für diese Anwendung fehlen. Sie können diese Informationen erhalten, indem Sie in die Zusammenfassung des Sicherheitsindex der Anwendung eingehen.

Die Zusammenfassung des Sicherheitsindex gibt Ihnen Informationen über die Wirksamkeit der folgenden Sicherheitskonfigurationen:

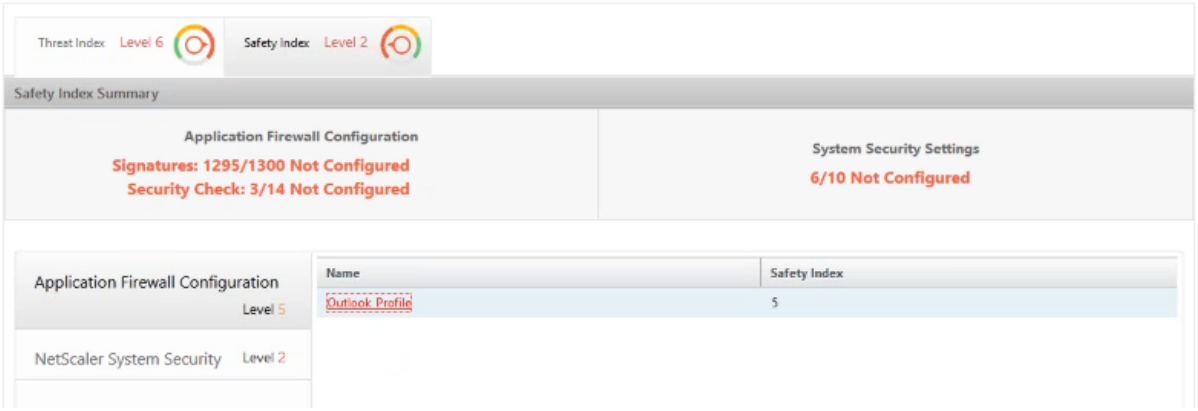
- **Konfiguration der Anwendungsfirewall.** Zeigt an, wie viele Signatur- und Sicherheitseinheiten nicht konfiguriert sind.
- **NetScaler Systemsicherheit.** Zeigt an, wie viele Systemsicherheitseinstellungen nicht konfiguriert sind.



Im vorherigen Anwendungsfall haben Sie das Bedrohungsrisiko von Microsoft Outlook überprüft, das den Bedrohungsindexwert 6 aufweist. Jetzt möchten Sie wissen, welche Sicherheitskonfigurationen für Outlook vorhanden sind und welche Konfigurationen hinzugefügt werden können, um den Bedrohungsindex zu verbessern.

Klicken Sie im **Security Insight-Dashboard** auf **Outlook**, und klicken Sie dann auf die Registerkarte **Sicherheitsindex**. Überprüfen Sie die Informationen im Bereich **Safety Index Summary**.

Klicken Sie auf dem Knoten **Application Firewall-Konfiguration** auf **Outlook_Profile**, und überprüfen Sie die Informationen zur Sicherheitsprüfung und zur Signaturverletzung in den Kreisdiagrammen.



Überprüfen Sie den Konfigurationsstatus der einzelnen Schutztypen in der Übersichtstabelle der Anwendungsfirewall. Um die Tabelle in einer Spalte zu sortieren, klicken Sie auf die Spaltenüberschrift.

Application Firewall Summary

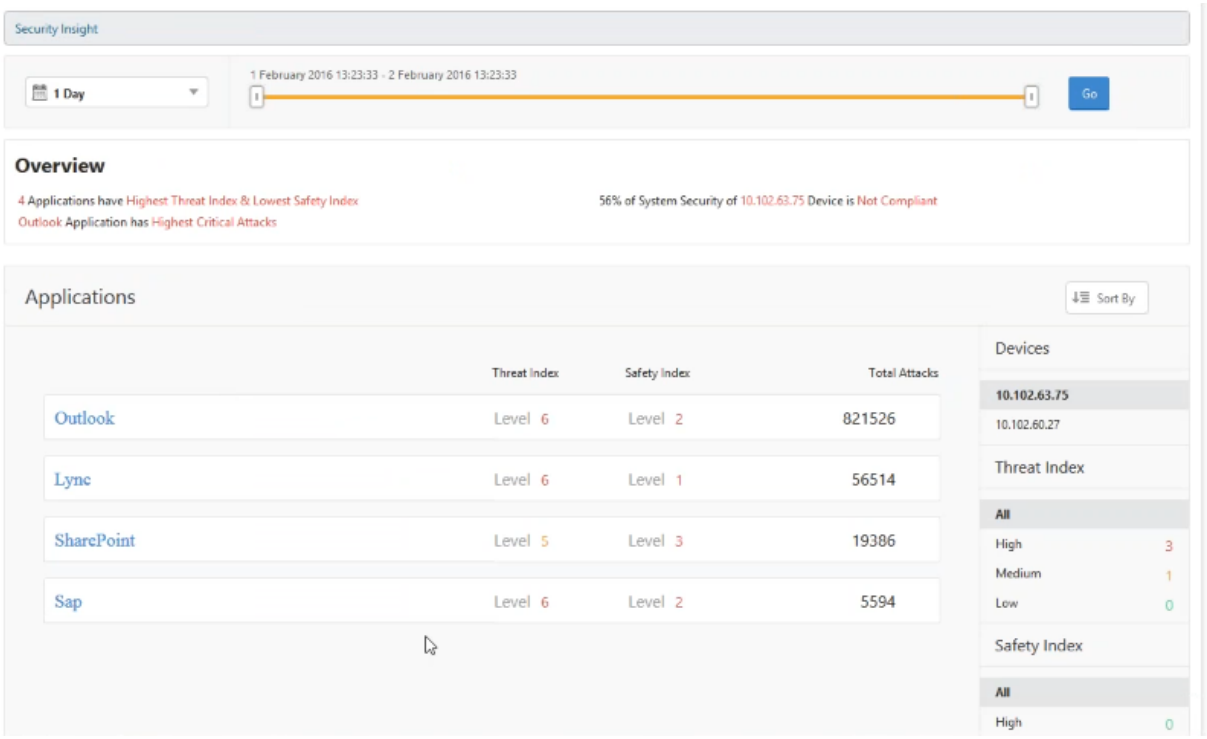
Protections	Configuration Status
XML Attachment	Not Configured
XML DoS	Not Configured
XML Format	Not Configured
XML SOAP Fault	Not Configured
XML SQL	Not Configured
XML Validation	Not Configured
XML WSI	Not Configured
XML XSS	Not Configured
Buffer Overflow	Log|Stat|Block
Buffer Overflow	Log|Block
Content Type	Log

Klicken Sie auf den Knoten **NetScaler System Security**, und überprüfen Sie die Systemsicherheitseinstellungen und Empfehlungen von Citrix, um den Anwendungssicherheitsindex zu verbessern.

Identifizieren von Anwendungen, die sofortige Aufmerksamkeit erfordern

Die Anwendungen, die sofortige Aufmerksamkeit erfordern, sind diejenigen mit einem hohen Bedrohungsindex und einem niedrigen Sicherheitsindex.

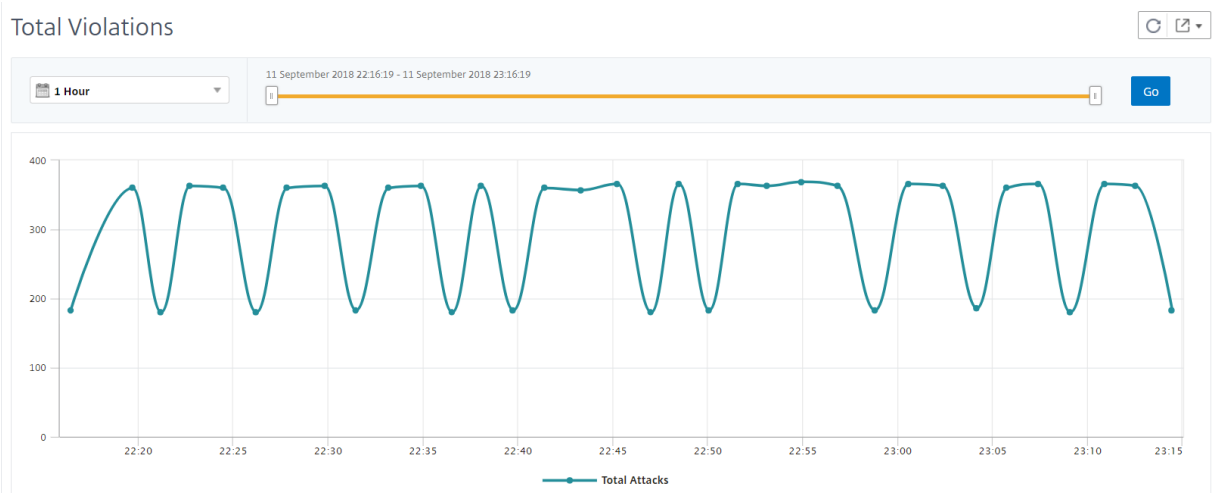
In diesem Beispiel weisen sowohl Microsoft Outlook als auch Microsoft Lync einen hohen Bedrohungsindexwert von 6 auf, Lync weist jedoch den unteren der beiden Sicherheitsindizes auf. Daher müssen Sie möglicherweise Ihre Aufmerksamkeit auf Lync konzentrieren, bevor Sie die Bedrohungsumgebung für Outlook verbessern.



Bestimmen Sie die Anzahl der Angriffe in einer bestimmten Zeit

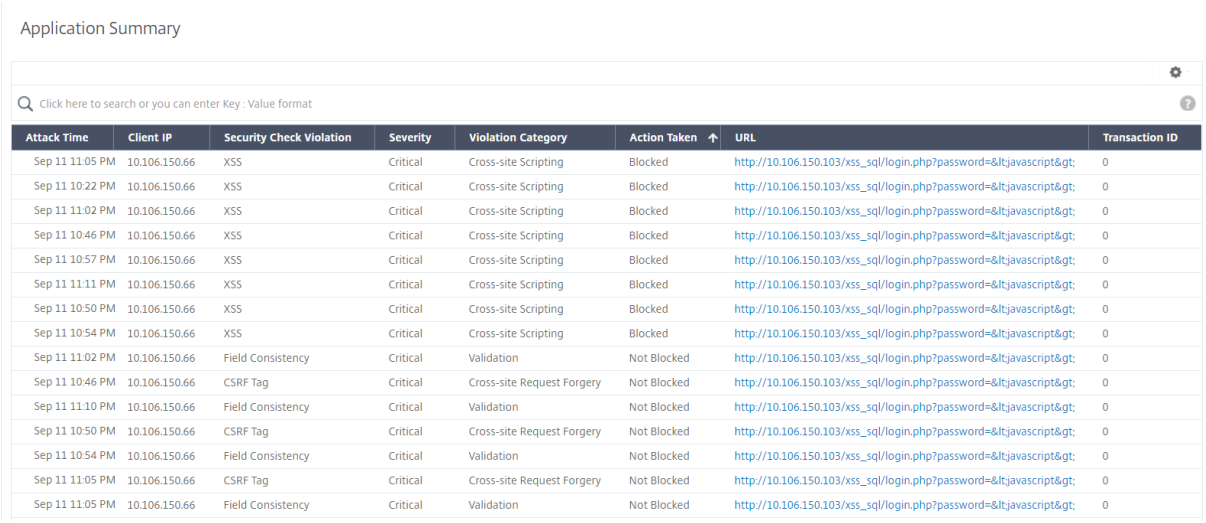
Sie können bestimmen, wie viele Angriffe auf eine bestimmte Anwendung zu einem bestimmten Zeitpunkt aufgetreten sind, oder Sie möchten die Angriffsquote für einen bestimmten Zeitraum untersuchen.

Klicken Sie auf der Seite **Security Insight** auf eine Anwendung und klicken Sie in der **Anwendungsübersicht**auf die Anzahl der Verstöße. Auf der Seite Total Violations werden die Angriffe grafisch für eine Stunde, einen Tag, eine Woche und einen Monat angezeigt.



Die Tabelle Anwendungsübersicht enthält die Details zu den Angriffen. Einige von ihnen sind wie folgt:

- Angriffszeit
- IP-Adresse des Clients, von dem aus der Angriff erfolgte
- Schweregrad
- Kategorie des Verstoßes
- URL, von der der Angriff stammt, und weitere Details.

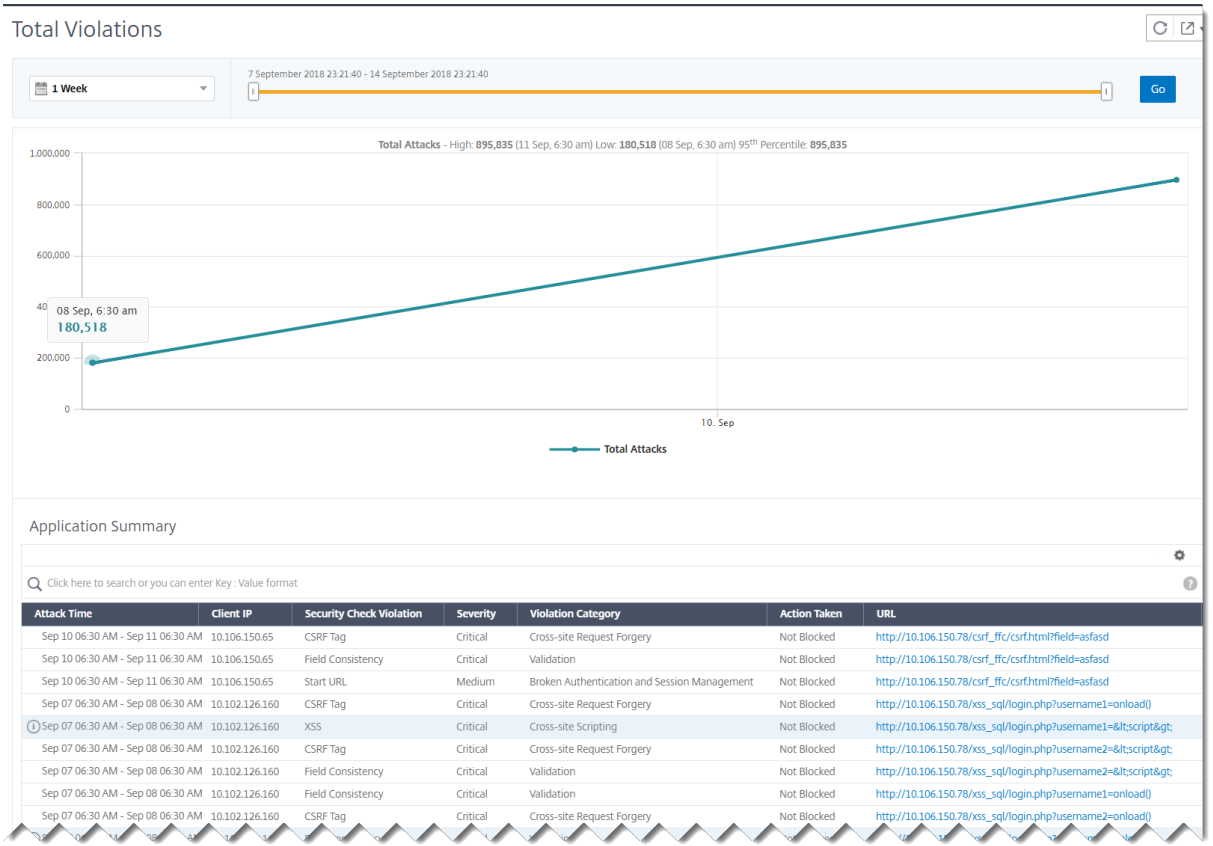


Application Summary

Click here to search or you can enter Key : Value format

Attack Time	Client IP	Security Check Violation	Severity	Violation Category	Action Taken	URL	Transaction ID
Sep 11 11:05 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:22 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:02 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:46 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:57 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:11 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:50 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:54 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:02 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:46 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:10 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:50 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:54 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:05 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:05 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0

Während Sie die Angriffszeit immer in einem stündlichen Bericht anzeigen können, wie im Bild zu sehen ist, können Sie jetzt den Angriffszeitbereich für aggregierte Berichte auch für tägliche oder wöchentliche Berichte anzeigen. Wenn Sie in der Zeitperiodenliste 1 Tag auswählen, zeigt der Security Insight-Bericht alle aggregierten Angriffe an und die Angriffszeit wird in einer Stunde angezeigt. Wenn Sie 1 Woche oder 1 Monat wählen, werden alle Angriffe aggregiert und die Angriffszeit wird in einem Tagesbereich angezeigt.

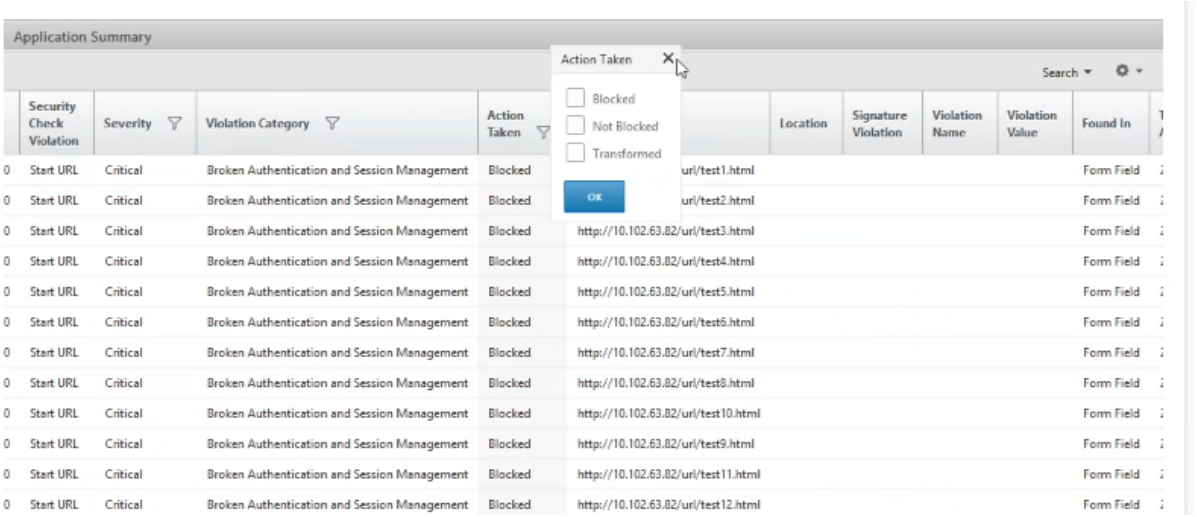


Erhalten Sie detaillierte Informationen über Sicherheitsverletzungen

Möglicherweise möchten Sie eine Liste der Angriffe auf eine Anwendung anzeigen und Einblicke in die Art und den Schweregrad der Angriffe, die von der Citrix ADC Instanz durchgeführten Aktionen, die angeforderten Ressourcen und die Quelle der Angriffe erhalten.

Sie können beispielsweise bestimmen, wie viele Angriffe auf Microsoft Lync blockiert wurden, welche Ressourcen angefordert wurden und welche IP-Adressen der Quellen.

Klicken Sie im **Security Insight-Dashboard**auf **Lync > Total Violations**. Klicken Sie in der Tabelle in der Spaltenüberschrift **Aktion** auf das Filtersymbol, und wählen Sie dann **Blockiert** aus.



Informationen zu den angeforderten Ressourcen finden Sie in der **URL-Spalte**. Informationen zu den Quellen der Angriffe finden Sie in der Spalte **Client-IP**.

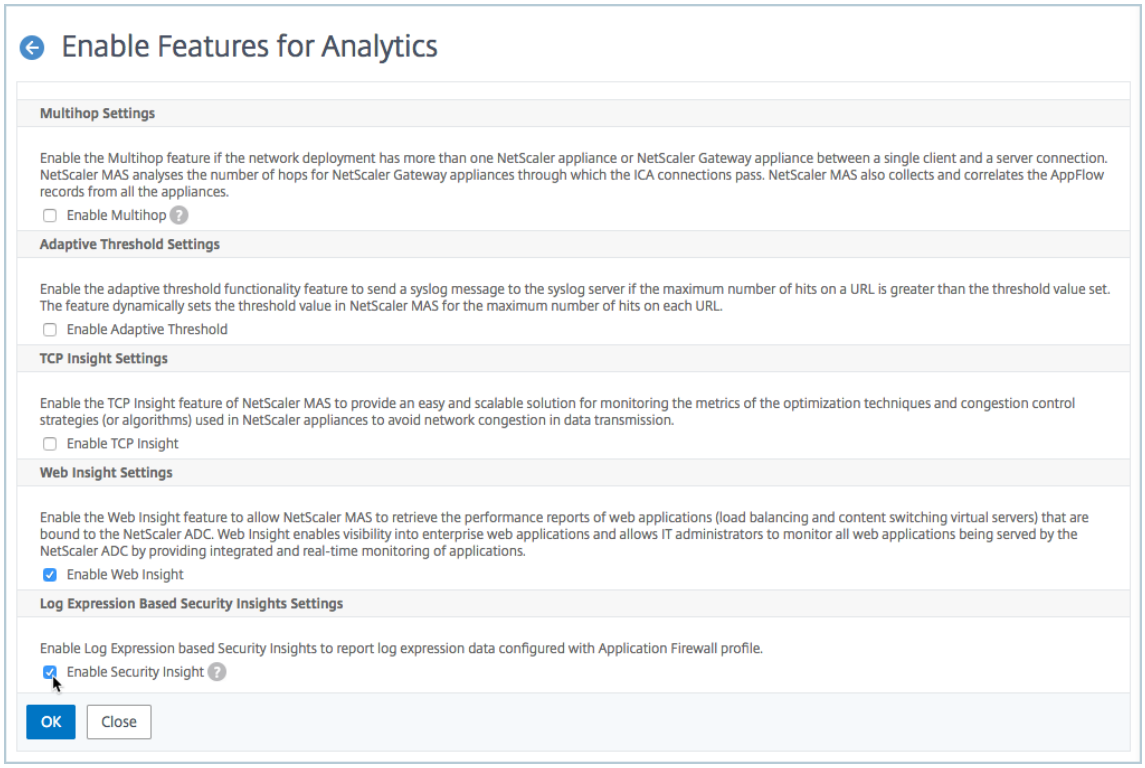
Details zum Protokollausdruck anzeigen

Citrix ADC Instanzen verwenden Protokollausdrücke, die mit dem Application Firewall-Profil konfiguriert sind, um Maßnahmen für Angriffe auf eine Anwendung in Ihrem Unternehmen zu ergreifen. In Security Insight können Sie die Werte anzeigen, die für die Protokollausdrücke zurückgegeben werden, die von der Citrix ADC Instanz verwendet werden. Diese Werte umfassen den Anforderungsheader, den Anforderungstext usw. Neben den Protokollausdruckswerten können Sie auch den Namen des Protokollausdrucks und den Kommentar für den Protokollausdruck anzeigen, der im Application Firewall-Profil definiert ist, mit dem die Citrix ADC Instanz Maßnahmen für den Angriff ergriffen hat.

Voraussetzungen Stellen Sie sicher, dass Sie:

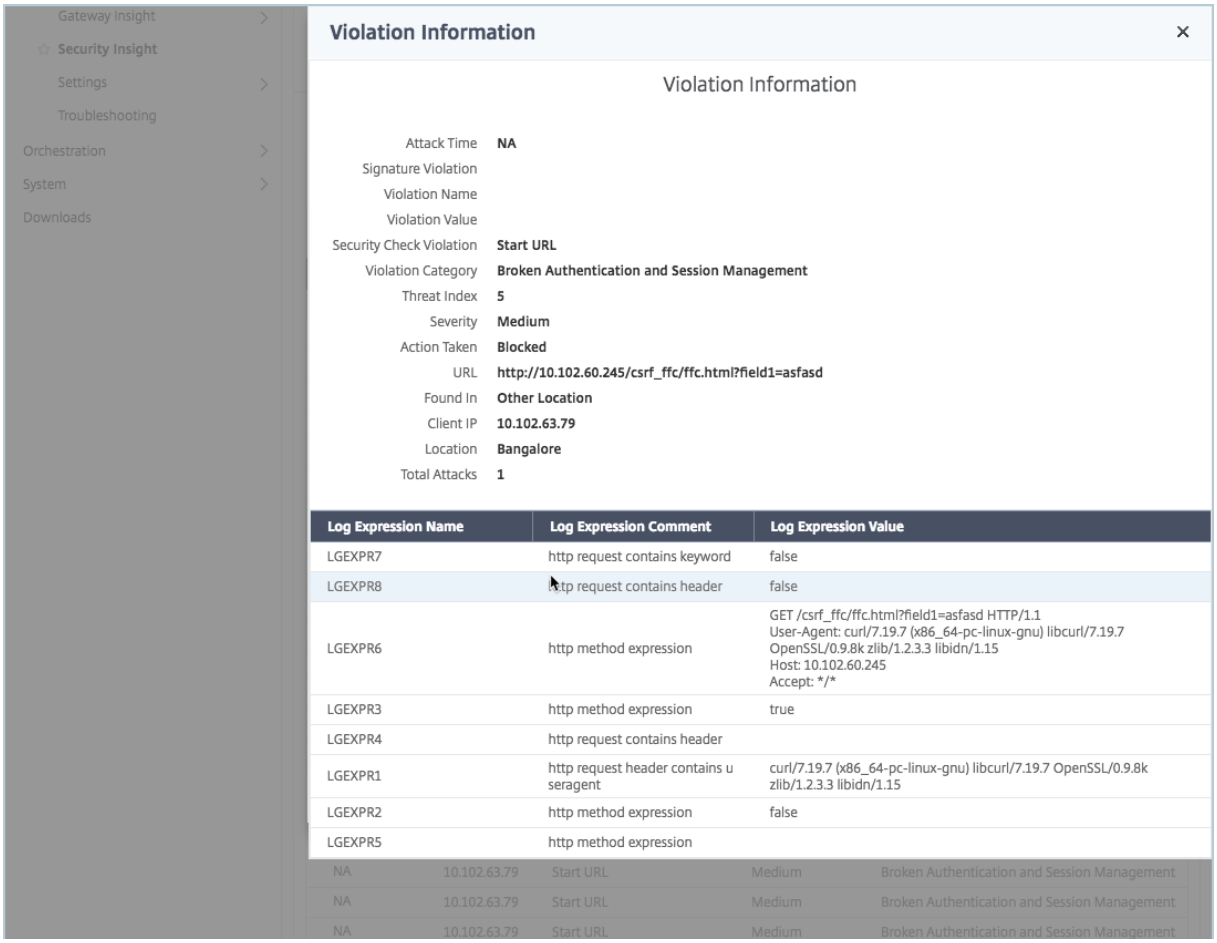
- Konfigurieren Sie Protokollausdrücke im Application Firewall-Profil. Weitere Informationen finden Sie unter Application Firewall.
- Aktivieren Sie die Einstellung Security Insights auf Protokollausdruck in Citrix ADM. Führen Sie folgende Schritte aus:

  1. Navigieren Sie zu **Analytics > Einstellungen** und klicken Sie auf **Funktionen für Analytics aktivieren** .
  2. Wählen Sie auf der Seite Funktion für Analytics **aktivieren** im Abschnitt **Log Expression Based Security Insight Enable Security Insight** aus und klicken Sie auf **OK**.



Sie können beispielsweise die Werte des Protokollausdrucks anzeigen, der von der NetScaler ADC Instanz für die Aktion zurückgegeben wird, die sie für einen Angriff auf Microsoft Lync in Ihrem Unternehmen ergriffen hat.

Navigieren Sie im Security Insight-Dashboard zu **Lync > Total Verletzungen**. Klicken Sie in der **Tabelle Anwendungszusammenfassung**auf die URL, um die vollständigen Details der Verletzung auf der Seite **Verstoßinformationen** anzuzeigen, einschließlich des Protokollausdrucks, des Kommentars und der Werte, die von der NetScaler ADC Instanz für die Aktion zurückgegeben werden.



Verstöße für Web Application Firewall (WAF) hervorheben

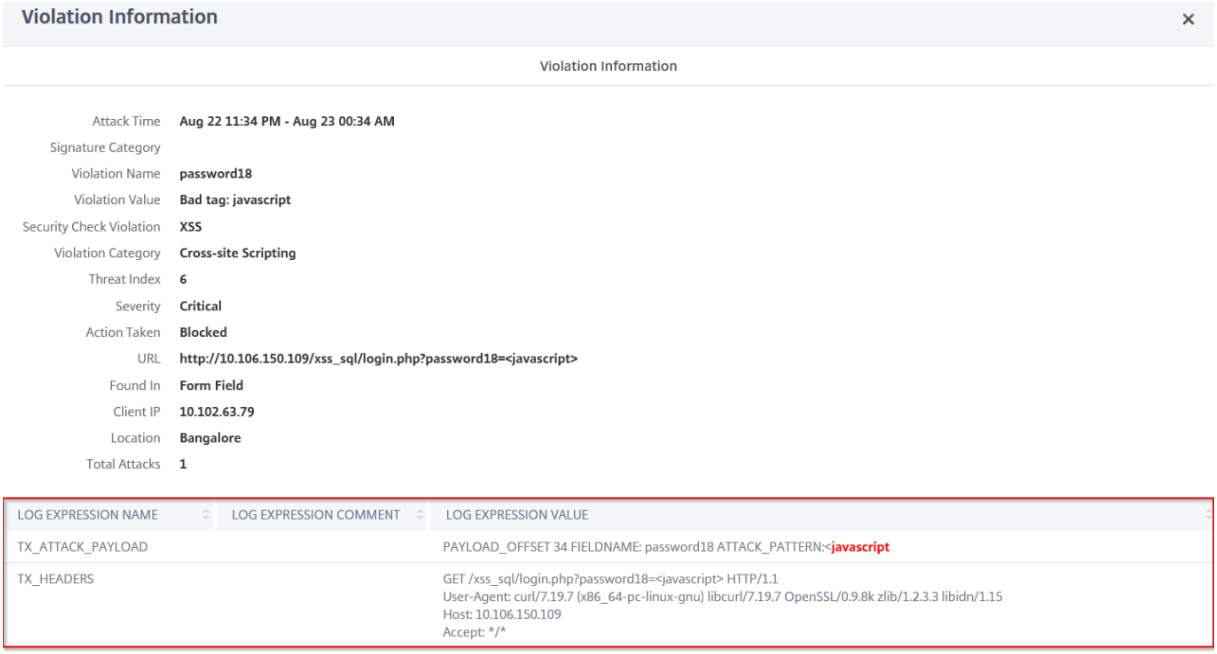
Sie können jetzt Details zu Angriffen wie HTTP-Header und HTTP-Nutzlast abrufen, um die Angriffe zu beheben oder zu analysieren. Um Details zu Angriffen zu erhalten, müssen Sie die "VerboseLogLevel" im Application Firewall-Profil mit dem folgenden Befehl aktualisieren:

```
Set appfw profile <profile_name> -VerboseLogLevel (pattern|patternPayload
|patternPayloadHdr)
```

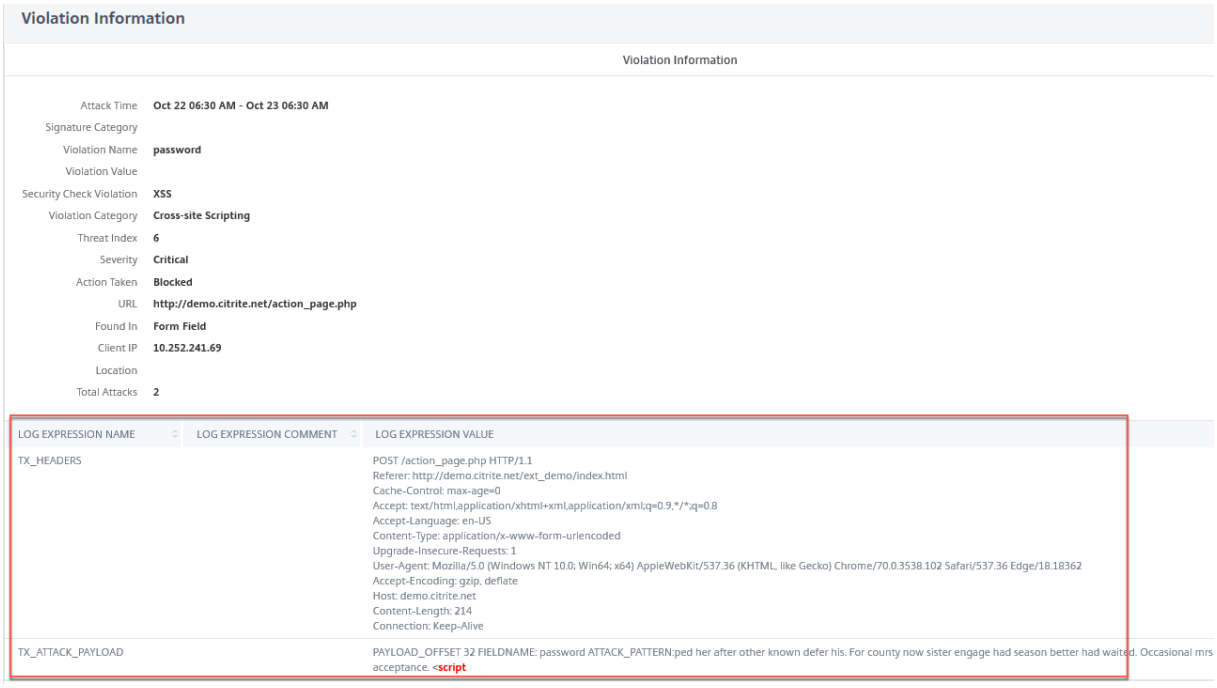
- `pattern` - Es wird nur Verstöße protokolliert
- `patternPayload` - Verletzungsmuster + 150 Bytes Feldelementwert vor dem Angriffsmuster werden protokolliert
- `patternPayloadHdr` - Verstoßmuster + 150 Byte Wert des Feldelements vor dem Angriffsmuster + HTTP-Anforderungsheader werden protokolliert

Basierend auf der Konfiguration "VerboseLogLevel"zeigt NetScaler ADM die detaillierten Protokollausdrucksdatensätze an.

Die folgende Abbildung ist ein Beispiel, das das Angriffsmuster für die GET-Anforderung hervorhebt:



Die folgende Abbildung ist ein Beispiel, das das Angriffsmuster für die POST-Anforderung hervorhebt:



In diesen beiden Beispielen:

- **FIELDNAME** bezieht sich auf den entsprechenden Feldnamen für das Angriffsmuster.
- **PAYLOAD_OFFSET** bezieht sich auf den Angriff Offset in der tatsächlichen Nutzlast.

- **ATTACK_PATTERN** hebt das Angriffsmuster hervor und enthält 150 Bytes Präfix-Nutzlast im Wert.

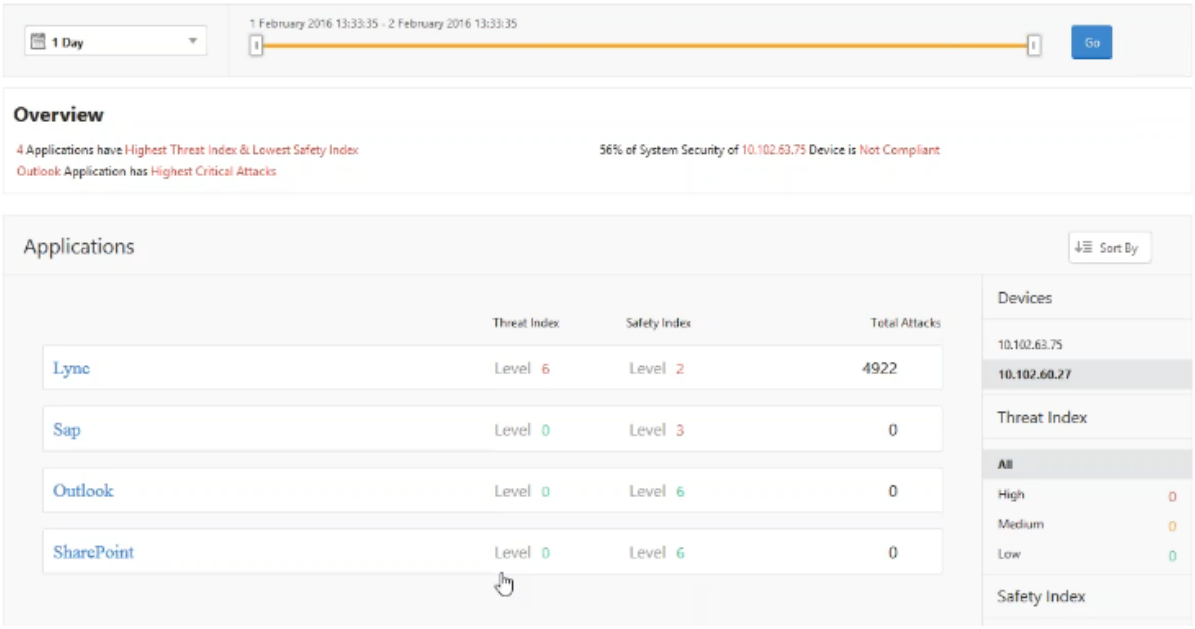
Weitere Informationen zum Konfigurieren der ausführlichen Protokollebene in NetScaler ADC finden Sie unter Einfache Fehlerbehebung mit Web Application Firewall-Protokollen.

Bestimmen Sie den Sicherheitsindex, bevor Sie die Konfiguration bereitstellen

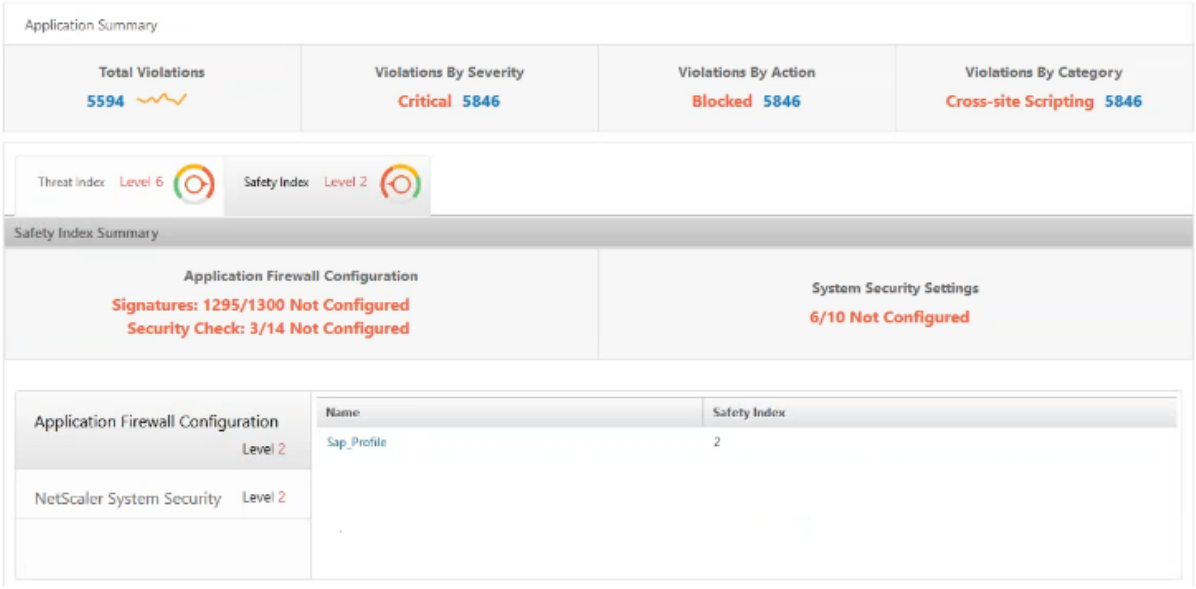
Sicherheitsverletzungen treten auf, nachdem Sie die Sicherheitskonfiguration auf einer NetScaler ADC Instanz bereitgestellt haben. Sie sollten jedoch vor der Bereitstellung die Effektivität der Sicherheitskonfiguration beurteilen.

Sie können beispielsweise den Sicherheitsindex der Konfiguration für die SAP-Anwendung auf der Citrix ADC Instanz mit der IP-Adresse 10.102.60.27 bewerten.

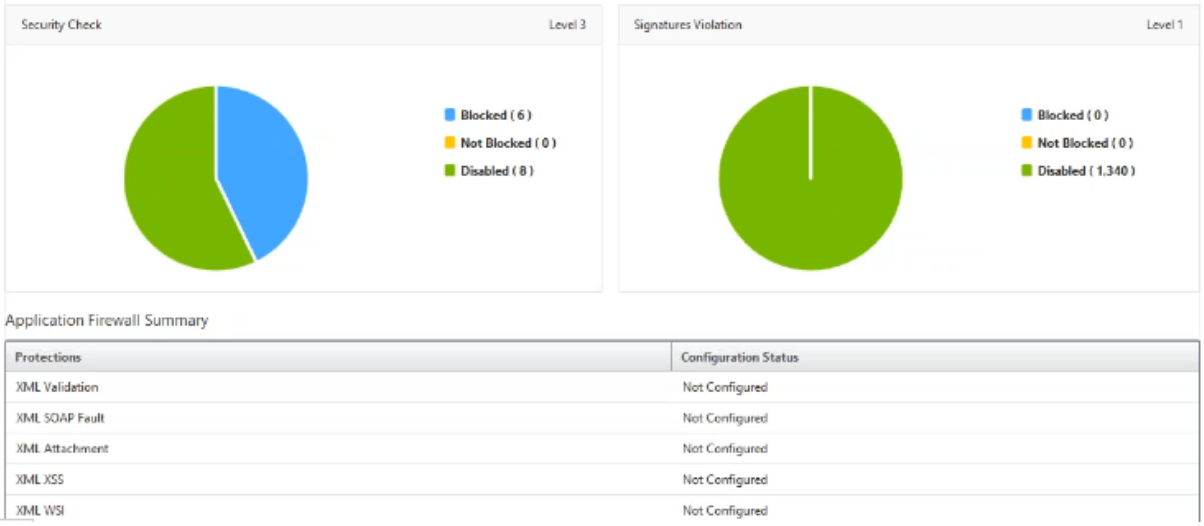
Klicken Sie im **Security Insight-Dashboard** unter **Geräte**auf die IP-Adresse der Citrix ADC Instanz, die Sie konfiguriert haben. Sie können sehen, dass sowohl der Bedrohungsindex als auch die Gesamtzahl der Angriffe 0 sind. Bedrohungsindex ist eine direkte Reflexion der Anzahl und Art der Angriffe auf die Anwendung. Keine Angriffe bedeuten, dass die Anwendung keiner Bedrohung ausgesetzt ist.



Klicken Sie auf **SAP > Sicherheitsindex > SAP_profile** und bewerten Sie die angezeigten Sicherheitsindexinformationen.



In der Zusammenfassung der Anwendungsfirewall können Sie den Konfigurationsstatus der verschiedenen Schutzeinstellungen anzeigen. Wenn eine Einstellung auf Protokollierung gesetzt ist oder wenn eine Einstellung nicht konfiguriert ist, wird der Anwendung ein niedrigerer Sicherheitsindex zugewiesen.



Bot

February 5, 2024

> Hinweis

> Wenn Ihr NetScaler ADM-Build früher als **13.0-79.x** ist, können Sie Bot Insight anzeigen, indem Sie zu **Analytics > Sicherheit > Bot Insight** navigieren. Für Build **13.0-79.x oder höher** können Sie Botdetails anzeigen, indem Sie zu **Analytics > Sicherheit > Sicherheitsverletzungen > Anwendungsübersicht** navigieren und unter **Aufschlüsselung der Anwendungen nach** auf **Bot** klicken.

Ein Bot ist ein Software-Programm, das automatisch bestimmte Aktionen immer und immer mit einer viel schnelleren Geschwindigkeit ausführt als ein Mensch. Über 35 Prozent Ihres Web-Traffics bestehen aus Bots und 80 Prozent der Unternehmen leiden unter Bot-Angriffen. Sie können mit einer Webseite interagieren, Formulare senden, Links klicken, Text scannen oder Inhalte herunterladen. Bots können auf Videos zugreifen, Kommentare posten und auf Social-Media-Plattformen twittern. Einige Bots können sogar grundlegende Gespräche mit menschlichen Benutzern führen. Diese werden als Chatbots bezeichnet.

Ein Bot, der einen brauchbaren oder hilfreichen Service wie Kundenservice, Chatbots, Suchmaschinen-Crawler durchführt, werden als gute Bots bekannt. Einige böswillige Bots können Inhalte von einer Website durchsuchen oder herunterladen, Benutzeranmeldeinformationen stehlen, Spam-Inhalte verbreiten und verschiedene andere Arten von Cyberangriffen durchführen. Diese bösartigen Bots werden als schlechte Bots bekannt. Es ist wichtig, bösartige Bots zu identifizieren und Ihre Appliance vor fortschrittlichen Sicherheitsangriffen zu schützen. Sie können dies mit einem Bot-Management-System erreichen.
Weitere Informationen zu Bot finden Sie unter Bot-Management .

Konfigurieren von Bot-Erkennungstechniken in NetScaler ADC

In NetScaler ADC können Sie Bot-Erkennungstechniken konfigurieren, um den eingehenden Bot-Datenverkehr zu erkennen. Im Folgenden finden Sie die Bot-Techniken, die Sie in der NetScaler ADC-Instanz konfigurieren:

- **Positivliste**. Diese Regel enthält eine Liste von URLs und Richtlinienausdrücken, um zu bewerten, ob eine bestimmte Gruppe von guten Bots, die auf Ihre Webressource zugreifen können.
- **Sperrliste**. Diese Regel enthält eine Liste von URLs und Richtlinienausdrücken, um zu prüfen, ob ein bestimmter Satz von fehlerhaften Bots auf Ihre Website zugreifen kann.
- **IP reputation**. Diese Regel erkennt, ob der eingehende Bot-Verkehr eine bösartige IP-Adresse ist.
- **Gerätefingerabdruck**. Diese Regel erkennt, ob der eingehende Bot-Verkehr die Geräte-Fingerabdruck-ID im Header der eingehenden Anfrage und die Browserattribute eines eingehenden Client-Bot-Datenverkehrs aufweist.
- **Ratenbegrenzung**. Diese Regelrate begrenzt mehrere Anfragen desselben Kunden.

- **Unterschriften**. Diese Regel erkennt und blockiert Bots basierend auf der Signaturerkennung. Es verhindert auch nicht autorisierte URLs, die Websites kratzen, brutale Anmeldungen erzwingen und Bots, die auf Schwachstellen untersuchen.
- **Bot-Traps**. Diese Regel erkennt Bots, die auf das Skript zugreifen, das auf der Webseite aktiviert ist.
- **TPS**. Diese Regel erkennt den eingehenden Datenverkehr als Bots, wenn die maximalen Anforderungen und der prozentuale Anstieg der Anforderungen das konfigurierte Zeitintervall überschreiten.

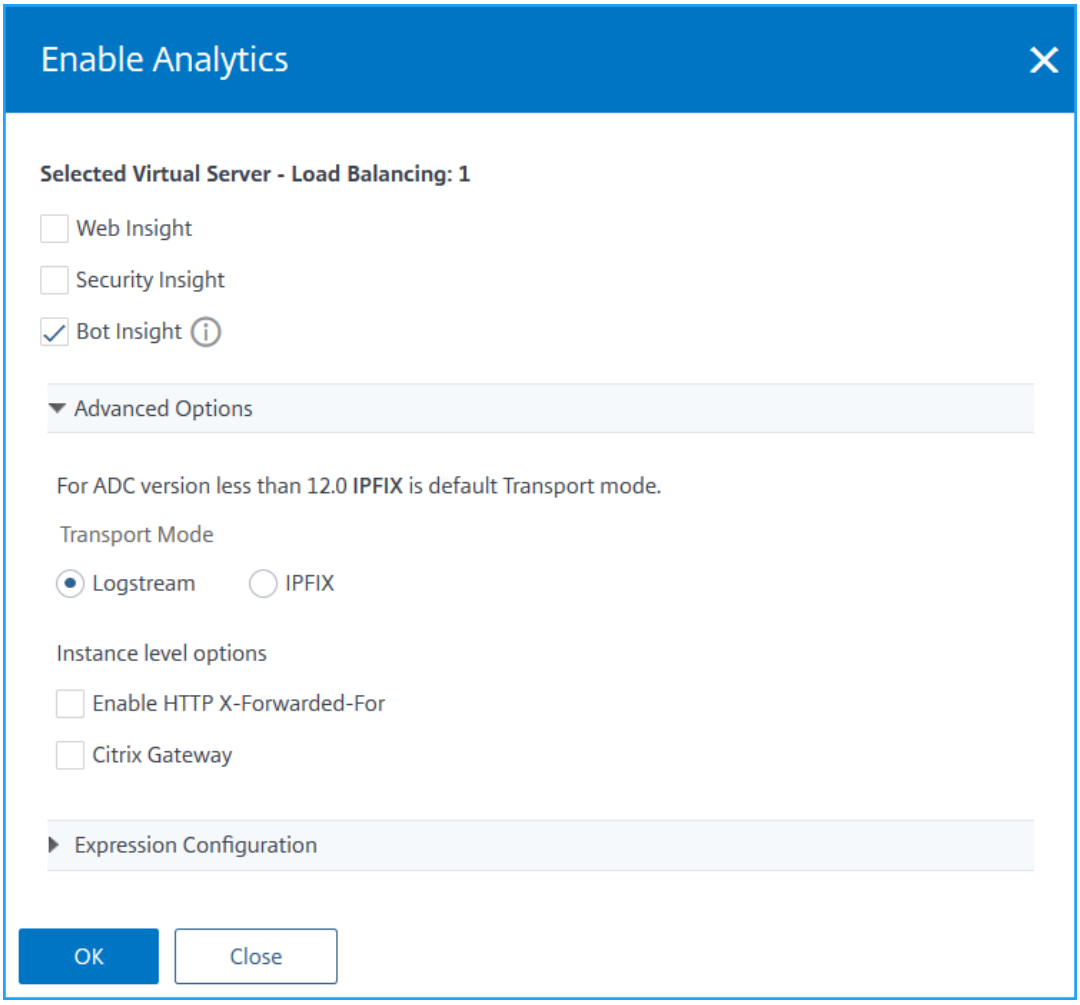
Weitere Informationen zum Konfigurieren der Bot-Verwaltung finden Sie unter Konfigurieren der Bot-Verwaltung.

Verwenden von Bot Insight in NetScaler ADM

Nachdem Sie die Bot-Verwaltung in NetScaler ADC konfiguriert haben, müssen Sie **Bot Insight** auf virtuellen Servern aktivieren, um Einblicke in NetScaler ADM anzuzeigen.

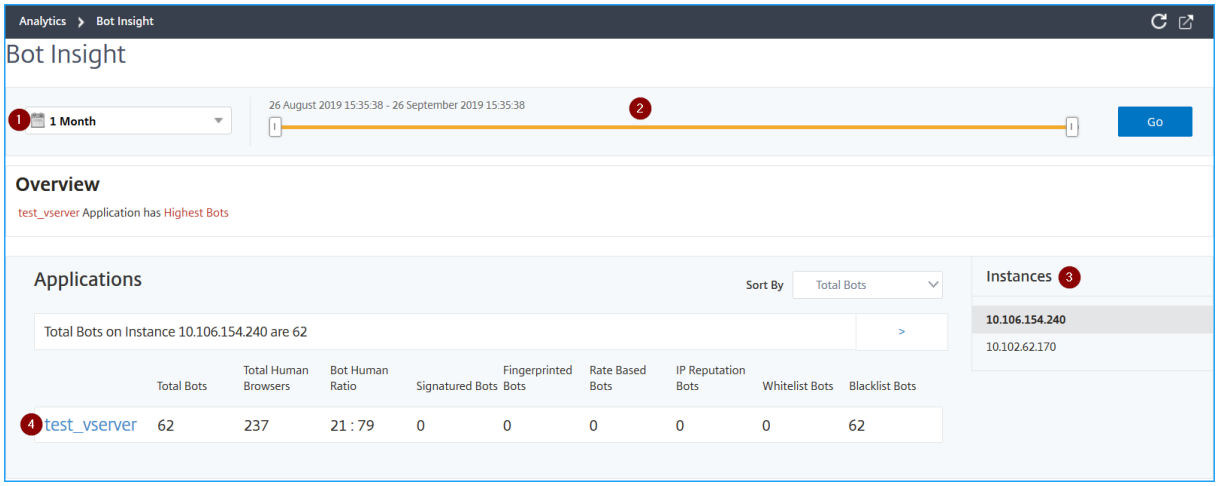
Um **Bot Insight**zu aktivieren:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC**, und wählen Sie den Instanztyp aus. Zum Beispiel VPX.
2. Wählen Sie die Instanz aus und **wählen Sie in der Liste Aktion** auswählen die Option **Analytics konfigurieren**aus.
3. Wählen Sie den virtuellen Server aus und klicken Sie auf **Analytics aktivieren**.
4. Gehen Sie im Fenster **Enable Analytics** wie folgt vor:
    a) Wählen Sie **Bot Insight**
    b) Wählen Sie unter **Erweiterte Option die OptionLogstream**aus.



c) Klicken Sie auf **OK**.

Nachdem Sie **Bot Insight**aktiviert haben, navigieren Sie zu **Analytics** > **Bot Insight**.



1 —Zeitliste zum Anzeigen von Bot-Details

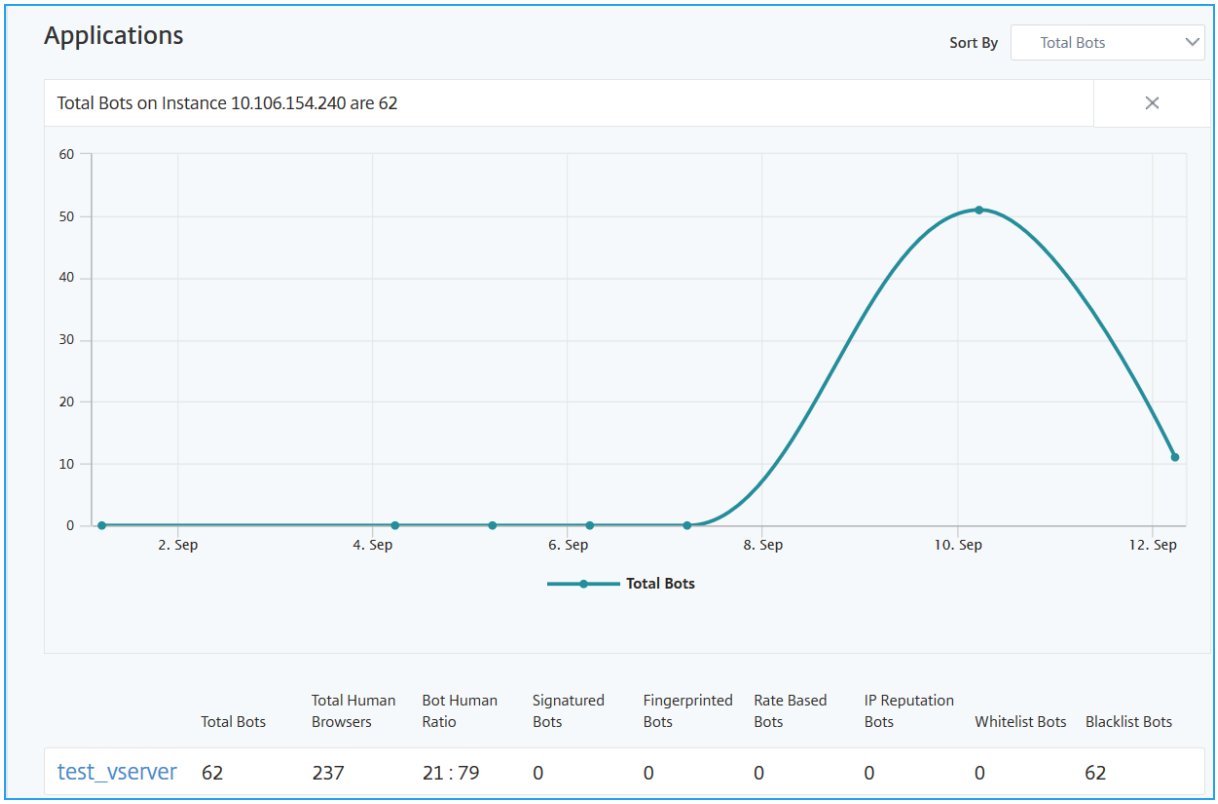
2 —Ziehen Sie den Schieberegler, um einen bestimmten Zeitraum auszuwählen, und klicken Sie auf **Go**, um die benutzerdefinierten Ergebnisse anzuzeigen

3 —Gesamtzahl der von Bots betroffenen Instanzen

4 —Virtueller Server für die ausgewählte Instanz mit allen Bot-Angriffen

- **Gesamtzahl der Bots** —Gibt die Gesamtzahl der Bot-Angriffe (einschließlich aller Bot-Kategorien) an, die für den virtuellen Server gefunden wurden.
- **Gesamtzahl menschlicher Browser** —Gibt die Gesamtzahl menschlicher Benutzer an, die auf den virtuellen Server zugreifen.
- **Bot Human Ratio** —Gibt das Verhältnis zwischen menschlichen Benutzern und Bots an, die auf den virtuellen Server zugreifen.
- **Signatur-Bots**, **Fingerabdruck-Bot**, **Ratenbasierte Bots**, **IP-Reputation-Bots**, **Positivlisten-bots**und **Sperrlistenbots** —Gibt die gesamten Bot-Angriffe basierend auf der konfigurierten Bot-Kategorie an. Weitere Informationen zur Bot-Kategorie finden Sie unter Konfigurieren von Bot-Erkennungstechniken in NetScaler ADC.

5 - Klicken Sie auf **>**, um Bot-Details in einem Diagrammformat anzuzeigen.

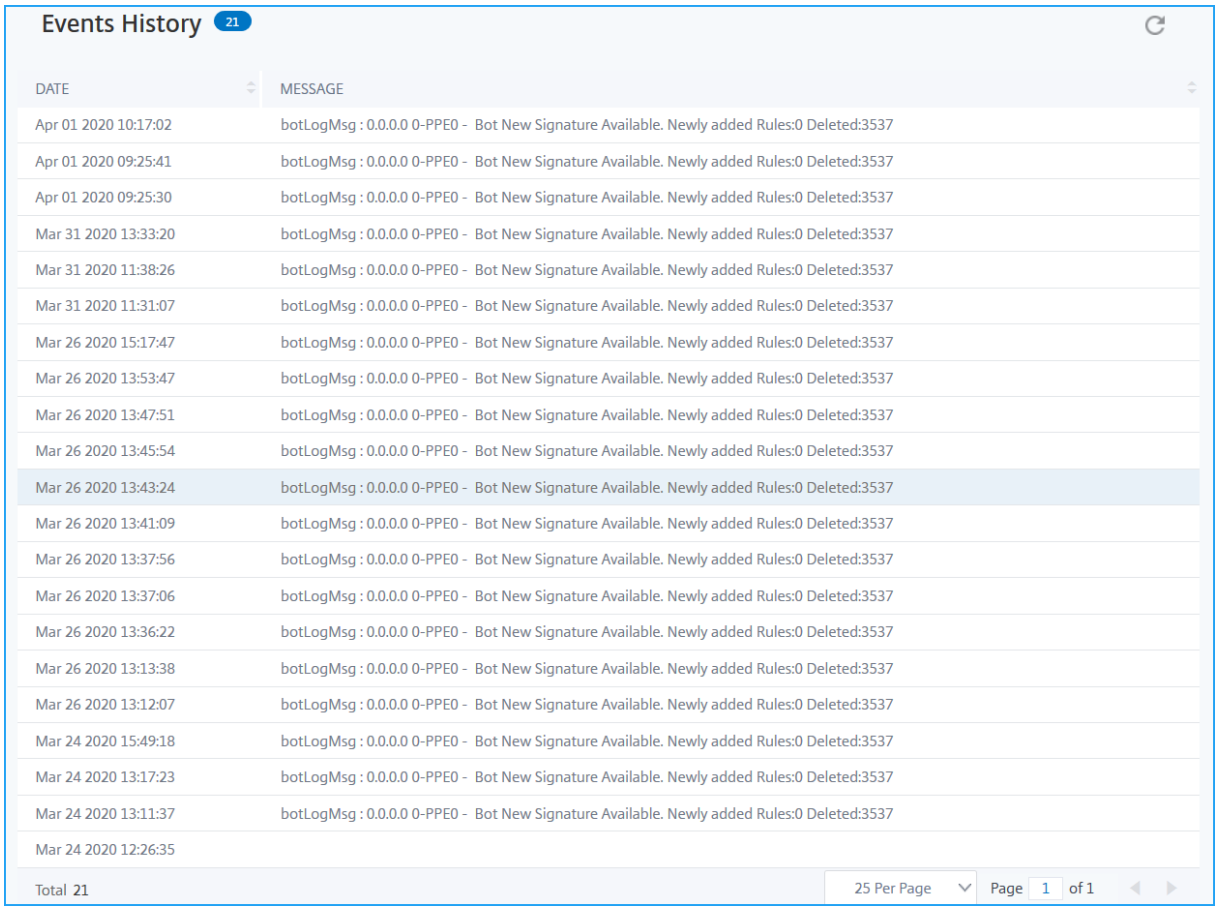


Ereignisverlauf anzeigen

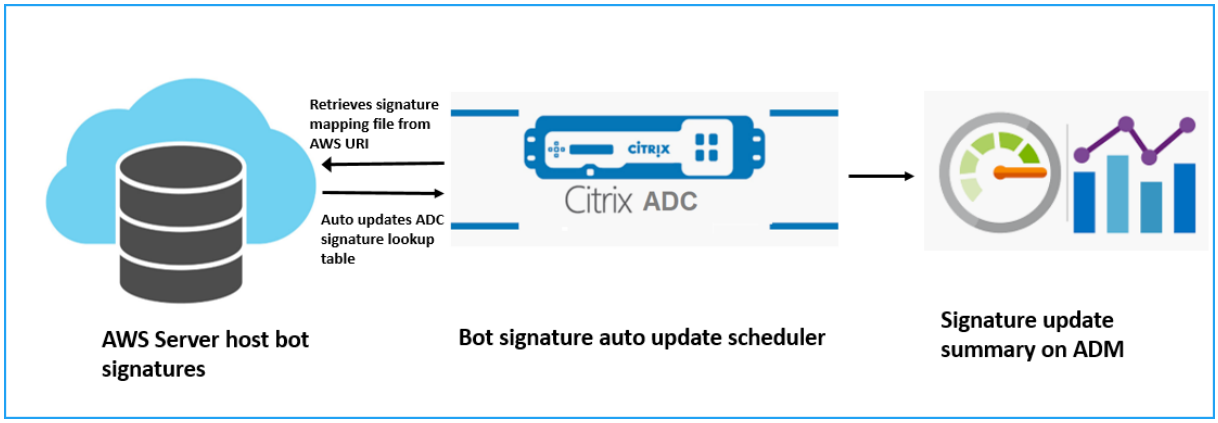
Sie können die Bot-Signaturaktualisierungen in der **Ereignishistorie**anzeigen, wenn:

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

Sie können die Zeitdauer auf der Bot-Insight-Seite auswählen, um den Ereignisverlauf anzuzeigen.



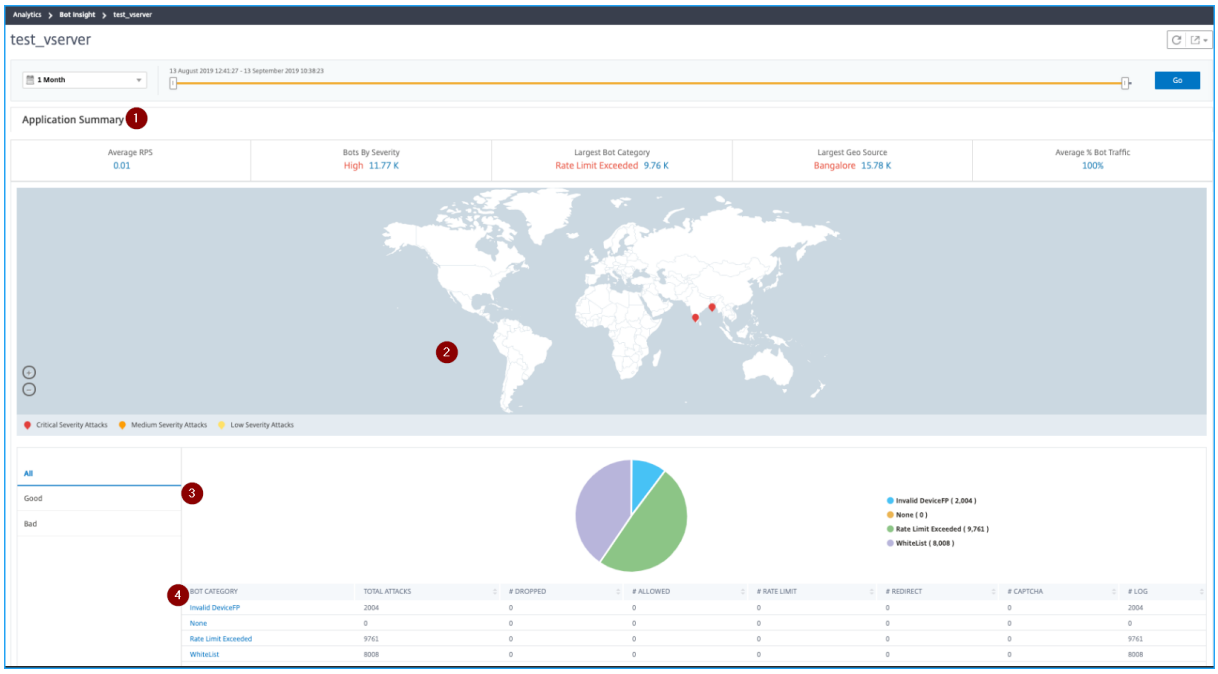
Das folgende Diagramm zeigt, wie die Bot-Signaturen aus der AWS-Cloud abgerufen, auf NetScaler ADC aktualisiert werden und wie die Signaturaktualisierungszusammenfassung in NetScaler ADM angezeigt wird.



1. Der Planer für automatische Aktualisierung der Bot-Signatur ruft die Zuordnungsdatei vom AWS-URI ab.
2. Überprüft die neuesten Signaturen in der Zuordnungsdatei mit den vorhandenen Signaturen in der ADC-Appliance.
3. Lädt die neuen Signaturen von AWS herunter und überprüft die Signaturintegrität.
4. Aktualisiert die vorhandenen Bot-Signaturen mit den neuen Signaturen in der Bot-Signaturdatei.
5. Generiert eine SNMP-Warnung und sendet die Signaturaktualisierungszusammenfassung an NetScaler ADM.

Bots ansehen

Klicken Sie auf den virtuellen Server, um die **Anwendungsübersicht**anzuzeigen.



1 —Stellt Details zur Anwendungsübersicht bereit, z. B.:

- **Durchschnittliche RPS** —Gibt die durchschnittlichen Bot-Transaktionsanfragen pro Sekunde (RPS) an, die auf virtuellen Servern empfangen wurden.
- **Bots nach Schweregrad** —Gibt die höchsten Bot-Transaktionen basierend auf dem Schweregrad an. Der Schweregrad wird nach **Kritisch**, **Hoch**, **Mittel**und **Niedrig**kategorisiert.

  Wenn die virtuellen Server beispielsweise 11770 Bots mit hohem Schweregrad und 1550 Bots mit kritischem Schweregrad haben, zeigt Citrix ADM unter Bots nach Schweregrad Kritisch 1,55 K**an.**
- **Größter Bot-Kategorie** —Gibt die höchsten Bot-Angriffe basierend auf der Bot-Kategorie an.

  Wenn die virtuellen Server beispielsweise über 8000 blockgelistete Bots, 5000 gelistete Bots zulassen und 10000 Rate Limit Exceeded Bots verfügen, zeigt NetScaler ADM unter **Largest Bot Category** die Option **Rate Limit Exceeded 10 K** an.
- **Größte Geoquelle** —Gibt die höchsten Bot-Angriffe basierend auf einer Region an.

  Wenn die virtuellen Server beispielsweise 5000 Bot-Angriffe in Santa Clara, 7000 Bot-Angriffe in London und 9000 Bot-Angriffe in Bangalore haben, zeigt Citrix ADM Bangalore 9 K unter Largest Geo**Source an.**
- **Durchschnittlicher Bot-Traffic in%** —Gibt den Anteil menschlicher Bots an.

2 —Zeigt den Schweregrad der Bot-Angriffe anhand von Standorten in der Kartenansicht an

3 —Zeigt die Arten von Bot-Angriffen an (Gut, Schlecht und Alle)

4 —Zeigt die Gesamtzahl der Bot-Angriffe zusammen mit den entsprechenden konfigurierten Aktionen an. Wenn Sie beispielsweise Folgendes konfiguriert haben:

- IP-Adressbereich (192.140.14.9 bis 192.140.14.254) als Blocklisten-Bots und Auswahl von Löschen als Aktion für diese IP-Adressbereiche
- IP-Bereich (192.140.15.4 bis 192.140.15.254) als Sperrlistenbots und ausgewählt, um Log-Message als Aktion für diese IP-Bereiche zu erstellen

  In diesem Szenario zeigt NetScaler ADM Folgendes an:

  - Gesamtzahl der blockierten Bots
  - Anzahl Bots unter **Dropped**
  - Gesamtzahl der Bots im **Log**

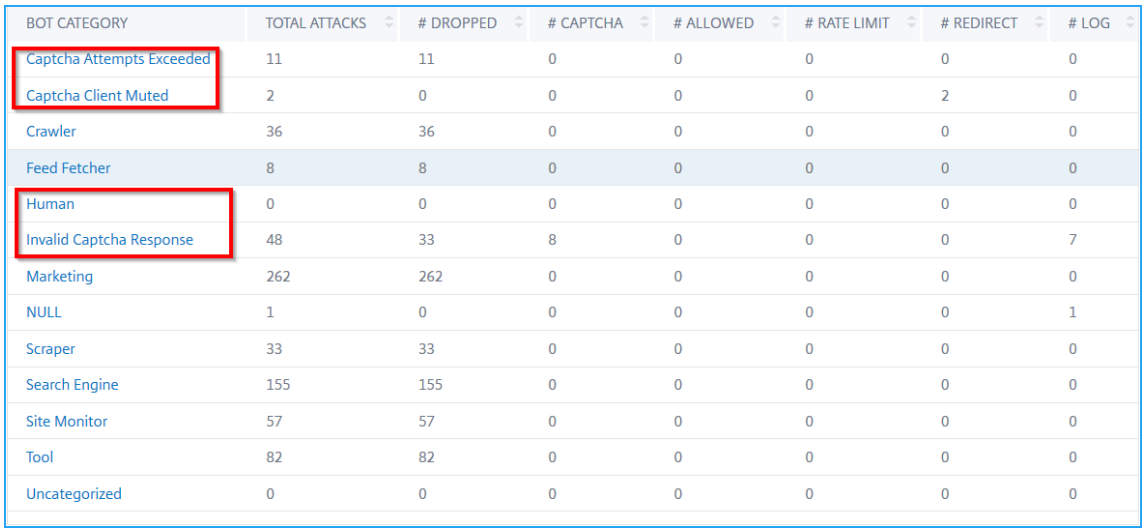
CAPTCHA-Bots ansehen

Auf Webseiten sollen CAPTCHAs erkennen, ob der eingehende Traffic von einem Menschen oder einem automatisierten Bot stammt. Um die CAPTCHA-Aktivitäten in NetScaler ADM anzuzeigen, müssen

Sie CAPTCHA als Bot-Aktion für IP-Reputation und Gerätefingerabdruckerkennungstechniken in einer NetScaler ADC Instanz konfigurieren. Weitere Informationen finden Sie unter Bot-Verwaltung.

Im Folgenden werden die CAPTCHA Aktivitäten aufgeführt, die NetScaler ADM in Bot Insight anzeigen:

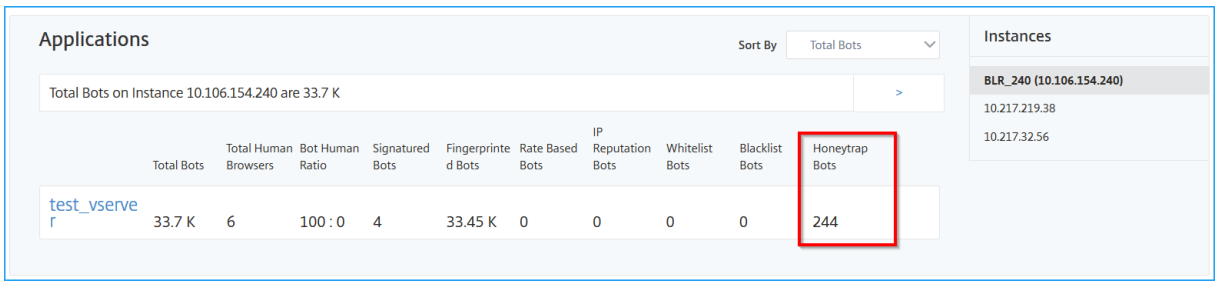
- **Captcha-Versuche überschritten** —Gibt die maximale Anzahl von CAPTCHA-Versuchen an, die nach fehlgeschlagenen Anmeldeversuchen unternommen wurden
- **Captcha-Client stummgeschaltet** —Gibt die Anzahl der Client-Anfragen an, die verworfen oder umgeleitet wurden, weil diese Anfragen zuvor mit der CAPTCHA-Herausforderung als bösartige Bots erkannt wurden
- **Mensch** —Bezeichnet die Captcha-Einträge, die von menschlichen Benutzern ausgeführt wurden
- **Ungültige Captcha-Antwort** —Gibt die Anzahl der falschen CAPTCHA-Antworten an, die vom Bot oder Menschen erhalten wurden, wenn NetScaler ADC eine CAPTCHA-Herausforderung sendet



BOT CATEGORY	TOTAL ATTACKS	# DROPPED	# CAPTCHA	# ALLOWED	# RATE LIMIT	# REDIRECT	# LOG
Captcha Attempts Exceeded	11	11	0	0	0	0	0
Captcha Client Muted	2	0	0	0	0	2	0
Crawler	36	36	0	0	0	0	0
Feed Fetcher	8	8	0	0	0	0	0
Human	0	0	0	0	0	0	0
Invalid Captcha Response	48	33	8	0	0	0	7
Marketing	262	262	0	0	0	0	0
NULL	1	0	0	0	0	0	1
Scraper	33	33	0	0	0	0	0
Search Engine	155	155	0	0	0	0	0
Site Monitor	57	57	0	0	0	0	0
Tool	82	82	0	0	0	0	0
Uncategorized	0	0	0	0	0	0	0

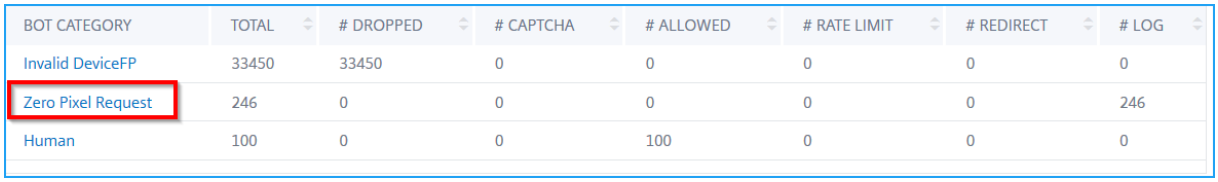
Bot-Trap-Bots anzeigen

Um Bot-Traps in NetScaler ADM anzuzeigen, müssen Sie den Bot-Trap in der NetScaler ADC-Instanz konfigurieren. Weitere Informationen finden Sie unter Bot-Verwaltung.



Um die Bot-Traps zu identifizieren, wird ein Skript auf der Webseite aktiviert und dieses Skript ist vor Menschen, aber nicht für Bots verborgen. NetScaler ADM identifiziert und meldet die Bot-Traps, wenn Bots auf dieses Skript zugreifen.

Klicken Sie auf den virtuellen Server und wählen Sie **Zero Pixel Request**

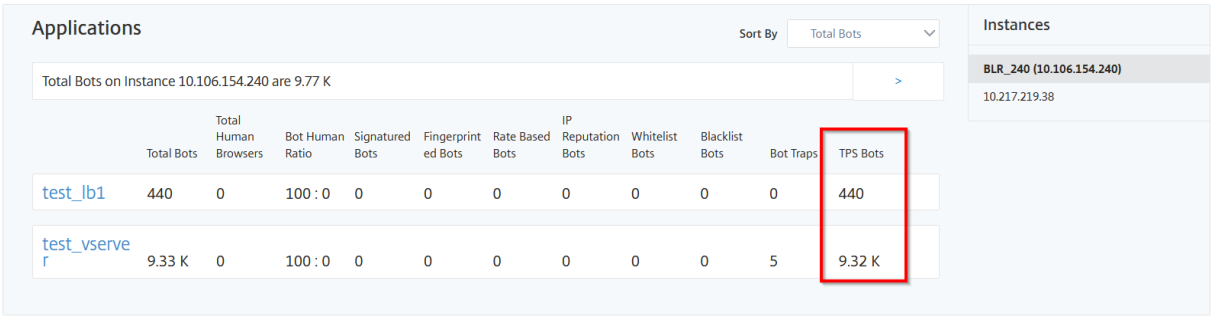


Anzeigen von TPS-Bots

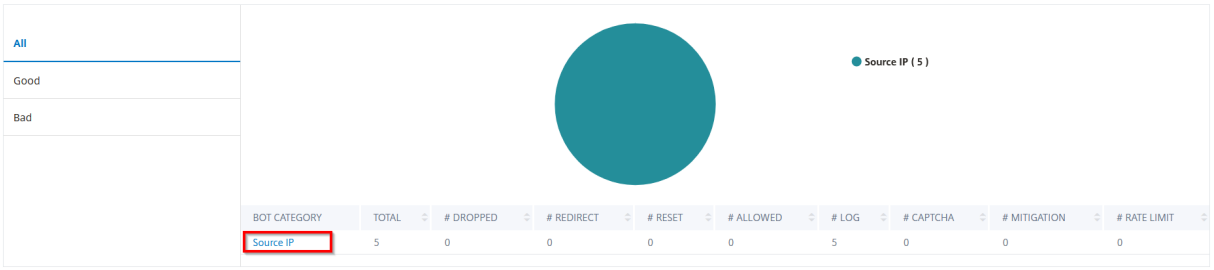
Im Folgenden sind die TPS-Bot-Kategorien aufgeführt, die Sie in NetScaler ADM anzeigen können:

- Quell-IP
- Geolocation
- Host
- URL

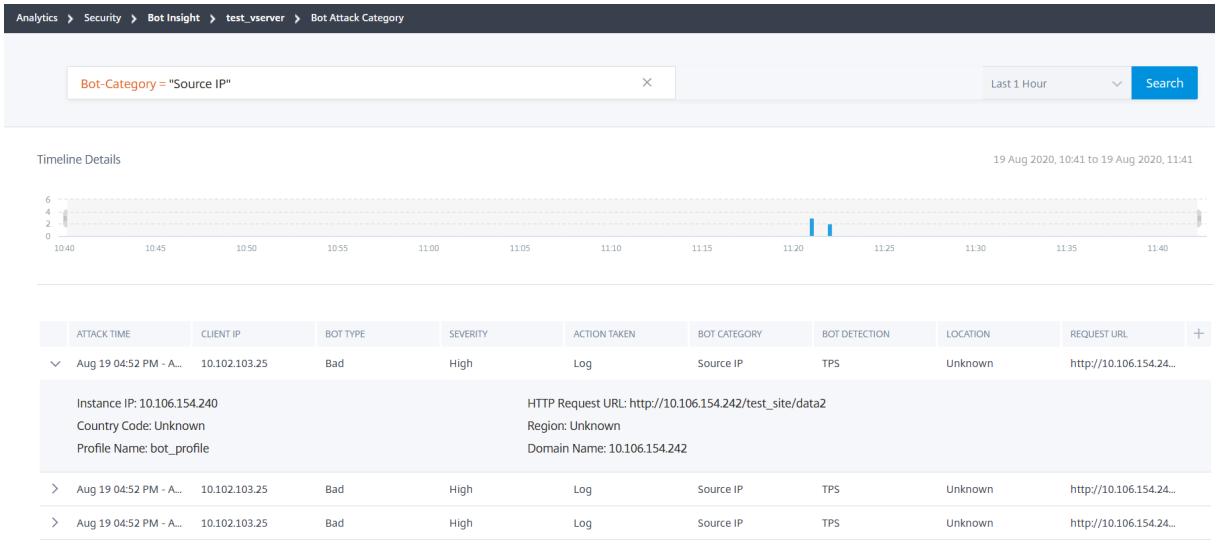
Klicken Sie auf den virtuellen Server, um die TPS-Bots anzuzeigen.



Klicken Sie auf die **TPS-Bot-Kategorie**, um die Bot-Details anzuzeigen.



Die Detailseite wird angezeigt.



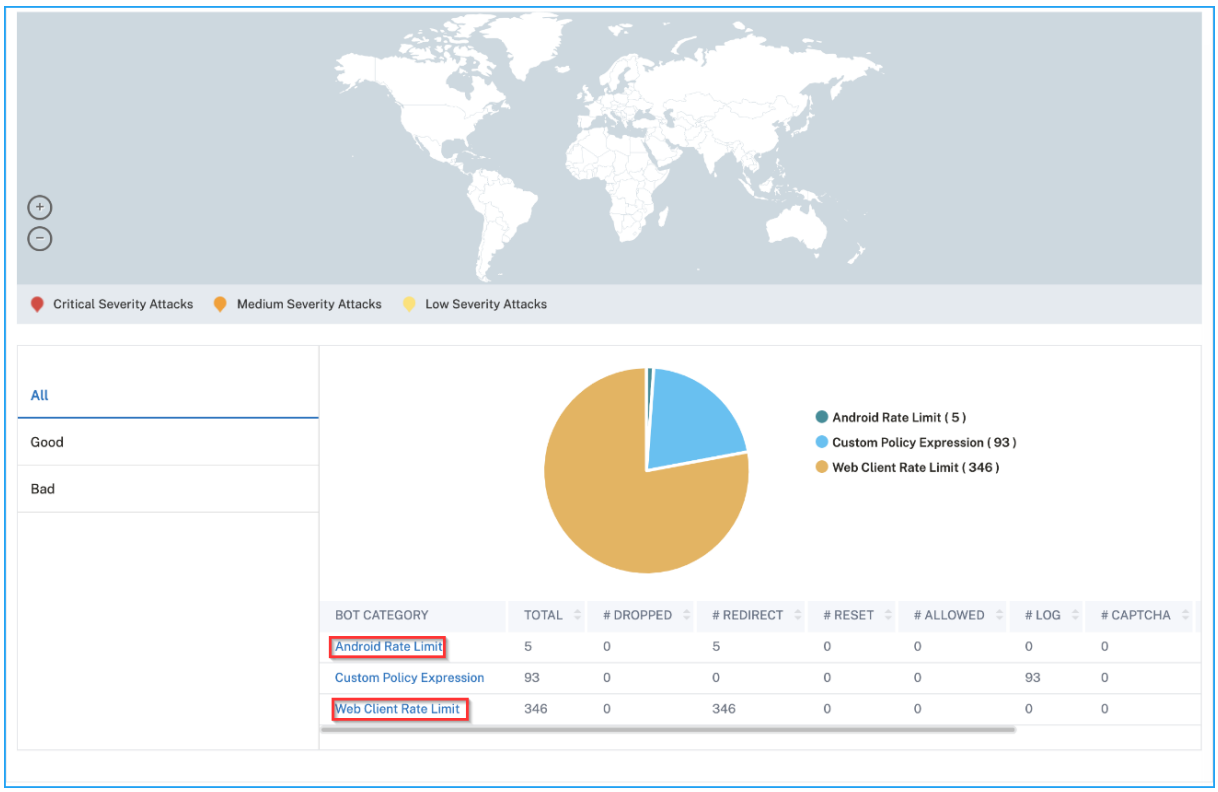
Anzeigen von Bot-Kategorien für mobile (Android) -Anwendungen

Um die Bots für mobile (Android) Anwendungen anzuzeigen, müssen Sie die Technik zur Erkennung von Fingerabdrücken in NetScaler ADC konfigurieren. Weitere Informationen finden Sie unter Konfigurieren der Fingerabdrucktechnik für Geräte für mobile Anwendungen.

Nachdem Sie die Einstellungen in NetScaler ADC konfiguriert haben, können Sie die folgenden Bot-Kategorien in NetScaler ADM anzeigen:

- Preislimit für Web-Clients
- Android Rate Limit
- Webclient-Gerät
- Android-Gerät

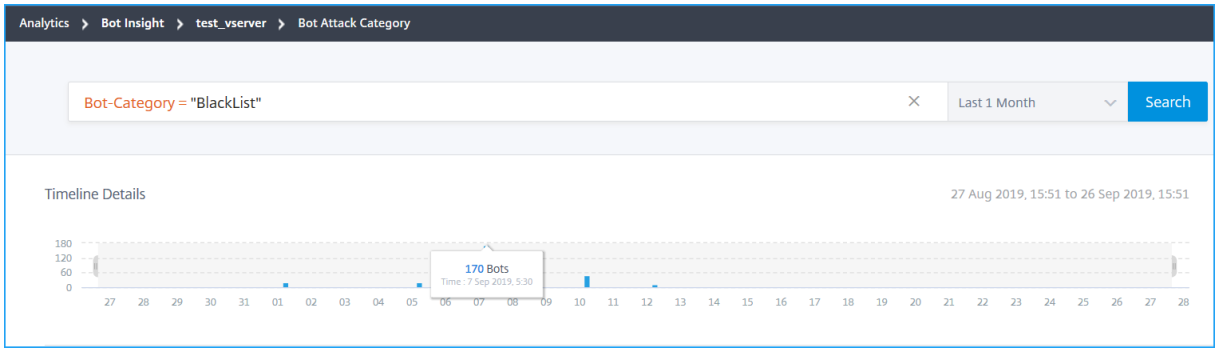
Klicken Sie auf den virtuellen Server, um die für mobile Anwendungen geltenden Bot-Kategorien anzuzeigen.



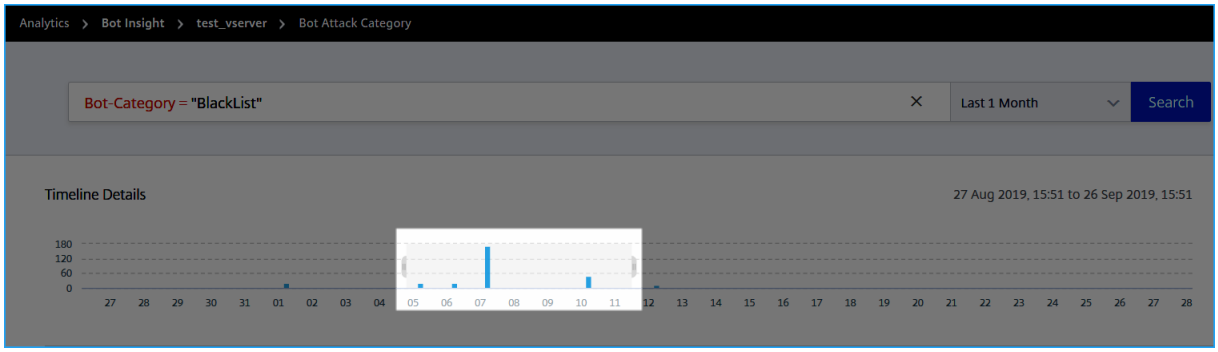
Bot-Details anzeigen

Um weitere Details zu erhalten, klicken Sie unter **Bot-Kategorie auf den Bot-Angriffstyp**. Wenn Sie beispielsweise Details für blockgelistete Bot-Angriffe anzeigen möchten, klicken Sie unter **Bot-Kategorie** auf **Liste blockieren**.

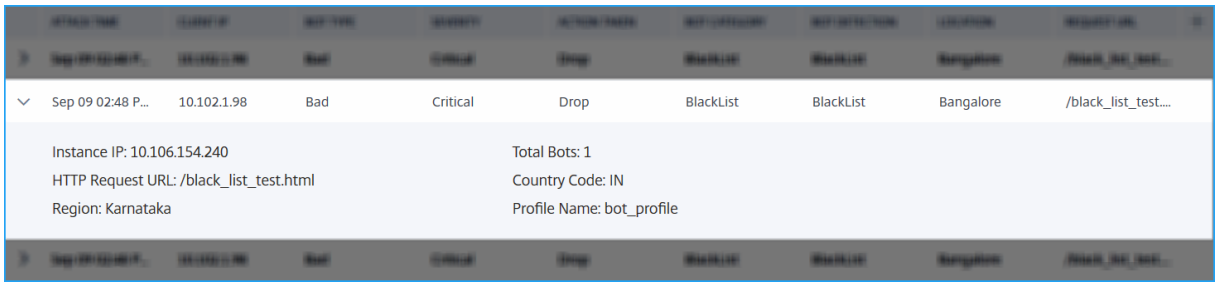
Die Details wie Angriffszeit und die Gesamtzahl der Bot-Angriffe werden angezeigt.



Sie können das Balkendiagramm auch ziehen, um den spezifischen Zeitraum auszuwählen, der bei Bot-Angriffen angezeigt werden soll.



Um weitere Informationen zum Bot-Angriff zu erhalten, klicken Sie zum Erweitern.



- **Instanz-IP** —Gibt die IP-Adresse der Citrix ADC-Instanz an
- **Total Bots** —Zeigt die Gesamtanzahl der Bot-Angriffe an, die für diese bestimmte Zeit aufgetreten sind.
- **HTTP-Request-URL** —Gibt die URL an, die für die Blockierung konfiguriert ist
- **Ländercode** —Gibt das Land an, in dem der Bot-Angriff stattgefunden hat
- **Region** —Gibt die Region an, in der der Bot-Angriff stattgefunden hat
- **Profilname** —Gibt den Profilnamen an, den Sie bei der Konfiguration angegeben haben

Erweiterte Suche

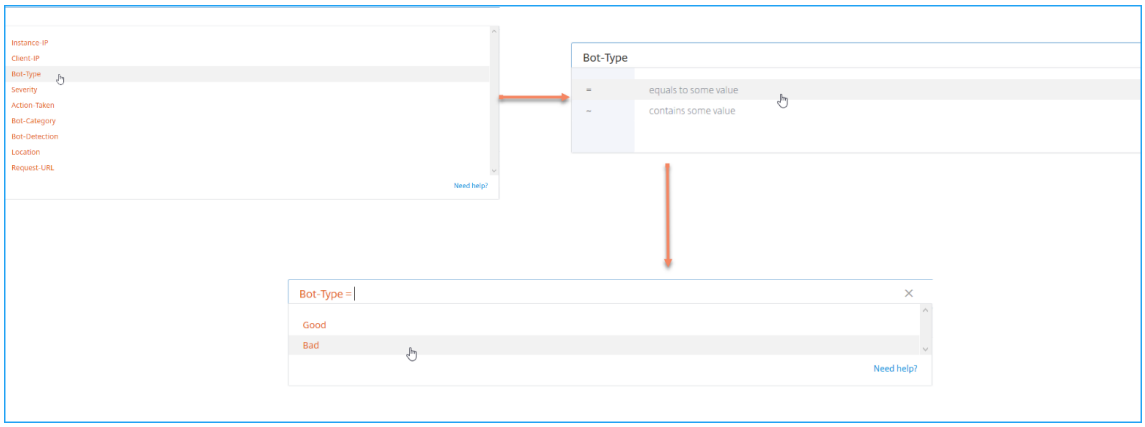
Sie können auch das Suchtextfeld und die Zeitdauerliste verwenden, in der Sie Bot-Details gemäß Ihren Anforderungen anzeigen können. Wenn Sie auf das Suchfeld klicken, wird im Suchfeld die folgende Liste mit Suchvorschlägen angezeigt.

- **Instanz-IP** —**IP-Adresse** der NetScaler ADC-Instanz
- **Client-IP** —Client-IP-Adresse
- **Bot-Type** —Bot-Typ wie Gut oder Schlecht
- **Schweregrad** —Schwere des Bot-Angriffs
- **Aktionsgetätigt** —Nach dem Bot-Angriff durchgeführte Aktion wie Drop, Keine Aktion, Umleiten

- **Bot-Category** —Kategorie des Bot-Angriffs wie Blockliste, Zulassungsliste, Fingerabdruck usw. Basierend auf einer Kategorie können Sie ihr eine Bot-Aktion zuordnen
- **Bot-Erkennung** —Bot-Erkennungstypen (Blockierungsliste, Zulassungsliste usw.), die Sie auf der NetScaler ADC-Instanz konfiguriert haben
- **Standort** —Region/Land, in dem der Bot-Angriff stattgefunden hat
- **Request-URL** —URL, die die möglichen Bot-Angriffe enthält

Sie können auch Operatoren in Ihren Suchanfragen verwenden, um den Fokus Ihrer Suche einzuschränken. Zum Beispiel, wenn Sie alle schlechten Bots anzeigen möchten:

1. Klicken Sie auf das Suchfeld und wählen Sie **Bot-Type**
2. Klicken Sie erneut auf das Suchfeld und wählen Sie den Operator **=**
3. Klicken Sie erneut auf das Suchfeld und wählen Sie **Schlecht**
4. Klicken Sie auf **Suchen**, um die Ergebnisse anzuzeigen



Details zu Sicherheitsverletzungen bei Anwendungen anzeigen

February 5, 2024

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

- Visualisieren Sie Anwendungen mit umfassendem Einblick in die Bedrohungsdetails, die sowohl mit Sicherheits-Einblicken als auch mit Bot-Erkennt

- Greifen Sie auf die Anwendungssicherheitsverletzungen basierend auf den Kategorien **Netzwerk**, **Bot**und **WAF**zu.
- Ergreifen Sie Korrekturmaßnahmen, um die Anwendungen zu sichern

Die Seite "**Sicherheitsverletzungen** "enthält die folgenden Optionen:

- **Anwendungsübersicht** —Zeigt eine Übersicht mit Anwendungen an, die totale Verstöße, totale WAF- und Bot-Verstöße, Verstöße nach Ländern usw. aufweisen. Weitere Informationen finden Sie unter Anwendungsübersicht.
- **Alle Verstöße** —Zeigt die Details zur Verletzung der Anwendungssicherheit an. Weitere Informationen finden Sie unter Alle Verstöße.

Voraussetzung

Stellen Sie sicher, dass **Metrics Collector** aktiviert ist Standardmäßig ist **Metrics Collector** auf der NetScaler ADC-Instanz aktiviert. Weitere Informationen finden Sie unter Konfigurieren von Intelligent App Analytics.

SSL Insight

February 5, 2024

SSL Insight bietet Einblick in sichere Webtransaktionen (HTTPS) und ermöglicht IT-Administratoren, alle vom NetScaler ADC bereitgestellten sicheren Webanwendungen zu überwachen, indem sie eine integrierte Echtzeit- und historische Überwachung sicherer Webtransaktionen bereitstellen. Mit dieser Sichtbarkeit kann der Administrator Folgendes beurteilen:

- **Ermitteln Sie die Auswirkungen von Konfigurationsänderungen auf die Kundennutzung**: Der Administrator kann nachvollziehen, welche Auswirkungen eine Konfigurationsänderung wie das Deaktivieren von SSLv3 oder das Entfernen einer Chiffre wie RC4-MD5 auf die Clients hat. Dies kann durch Bewertung der historischen Transaktionsdaten auf diesem Protokoll und Chiffre erfolgen.
- **Quantifizierung der Clientleistung**: Der Administrator kann die Auswirkungen auf die Reaktionszeit der Anwendung anhand der verwendeten SSL-Verschlüsselungen/-Protokoll oder der ausgehandelten Zertifikate verstehen.
- **Anwendungssicherheit**: Prüfen Sie, ob bei einer der Anwendungen Transaktionen mit niedrigen Sicherheitsprotokollen, Verschlüsselungen oder einer schwachen Schlüsselstärke ausgeführt werden.

Wenn SSL Analytics auf einer NetScaler ADC Instanz aktiviert ist, werden SSL-Statistiken für jede SSL-Transaktion aufgezeichnet und protokolliert. Die Statistik zeigt die Details des SSL-Flusses. Außerdem wird jede erfolgreiche Verbindung von Citrix Application Delivery Management (ADM) Analytics protokolliert und angezeigt.

SSL Insight bietet die folgenden wichtigen Informationen, die von NetScaler ADM Analytics angezeigt werden:

- Version des SSL-Protokolls ausgehandelt
- Verschlüsselung ausgehandelt und die Verschlüsselungsstärke
- Signatur-Hash-Algorithmus des verwendeten Zertifikats
- Typ und Größe des Zertifikats
- SSL-Frontend- und Backend-Fehler

> **Hinweis**
>
> Bei erfolgreichen SSL-Verbindungen erfolgt die SSL-AppFlow-Protokollierung am Ende jeder Transaktion.

Voraussetzungen

- Auf der NetScaler ADC-Instanz, auf der Sie SSL Insight konfigurieren möchten, muss die NetScaler ADC -Softwareversion 11.1 51.21 und höher ausgeführt werden. Führen Sie die folgenden Befehle auf der ADC-Instanz aus, auf der 11.1 51.21 ausgeführt wird, um Logstream als Transporttyp für SSL Insight zu aktivieren.

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the ADM>`

   Wählen Sie für ADC-Instanzen mit Version 12.0 und höher als Transportart Logstream aus, während Sie AppFlow von ADM aktivieren.

- Die NetScaler ADM-Version und der Build müssen gleich oder höher als die NetScaler ADC-Version und der Build sein. Wenn Sie beispielsweise NetScaler ADM 11.1 Build 61.7 installiert haben, stellen Sie sicher, dass Sie NetScaler ADC 11.1 Build 60.14 oder früher installiert haben.

SSL Insight konfigurieren

SSL Insight Metriken sind in Web Insight-Berichten enthalten, wenn Sie die folgenden Elemente aktivieren:

- Aktivieren Sie AppFlow für Web Insight auf jeder Citrix ADC Instanz.

- Aktivieren Sie den ULFD-Modus auf jeder Citrix ADC Instanz.
- Aktivieren Sie die erforderlichen AppFlow Parameter auf jeder NetScaler ADC Instanz.

Aktivieren der AppFlow-Funktion

> **Hinweis**
>
> Sie können die AppFlow Funktion entweder von Citrix ADM oder von jeder Citrix ADC Instanz aus aktivieren.

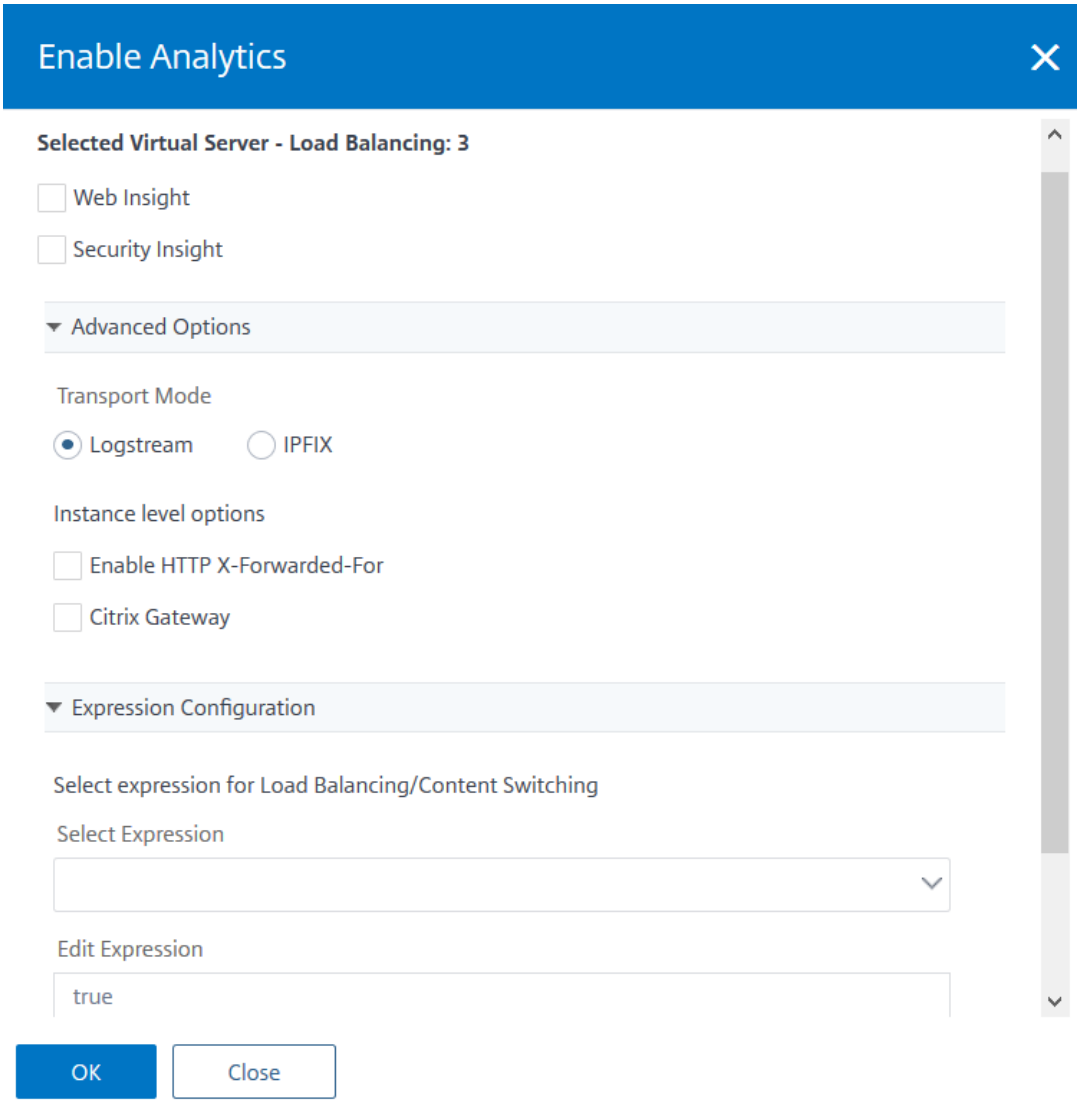
So aktivieren Sie die AppFlow Funktion von NetScaler ADM:

Wenn Ihr NetScaler ADM **13.0 Build 41.x oder höher**ist:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC**, und wählen Sie den Instanztyp aus. Zum Beispiel VPX.
2. Wählen Sie die Instanz aus, und klicken Sie in der Liste **Aktion auswählen** auf **Analytics konfigurieren**.
3. Wählen Sie auf der Seite **Configure Analytics on Virtual Server** den virtuellen Server aus und klicken Sie auf **Analytics aktivieren**.
4. Gehen Sie im Fenster **Enable Analytics** wie folgt vor:
   a) Wählen Sie **Web Insight**
   b) Wählen Sie **Logstream** als Transportmodus

      > **Hinweis**
      >
      > Für NetScaler ADC 12.0 oder früher ist **IPFIX** die Standardoption für den Transportmodus. Für NetScaler ADC 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.
      >
      > Weitere Informationen zu IPFIX und Logstream finden Sie unter Logstream-Übersicht .

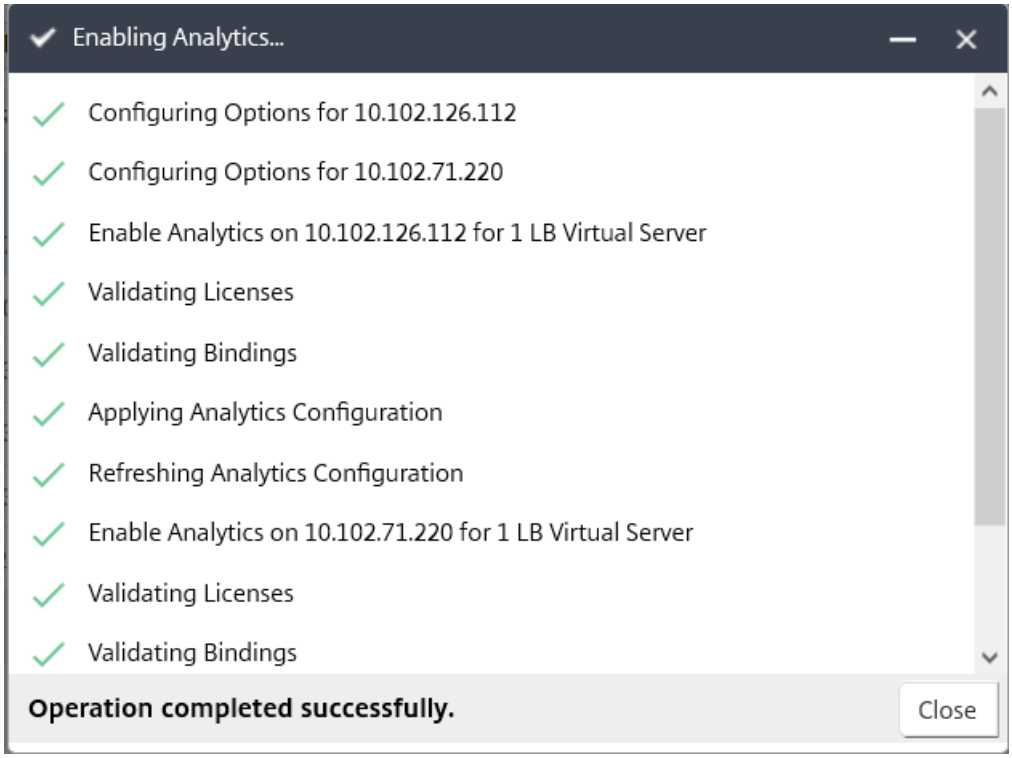
   c) Der Ausdruck ist standardmäßig wahr
   d) Klicken Sie auf **OK**.



Hinweis

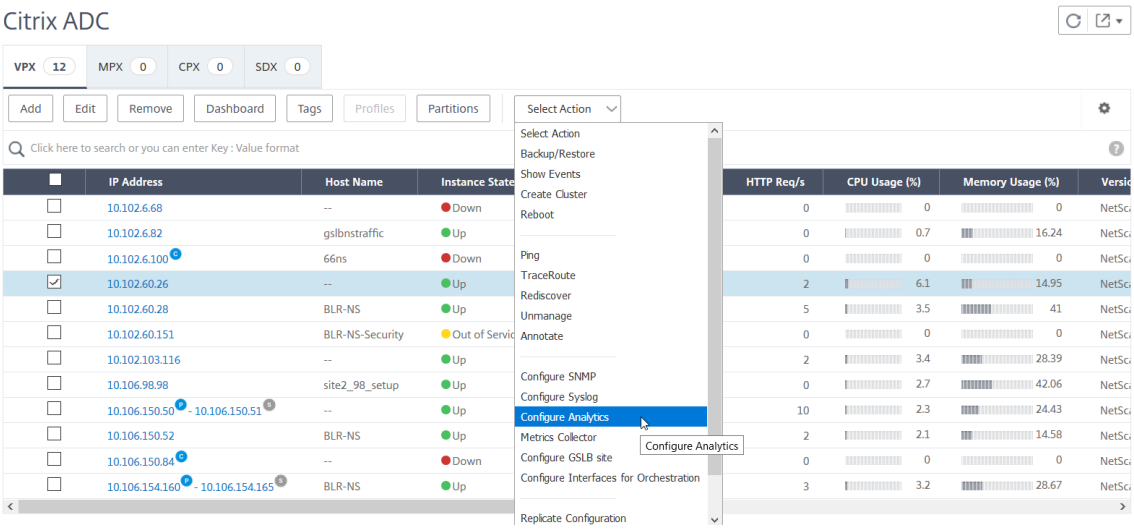
- Wenn Sie virtuelle Server auswählen, die nicht lizenziert sind, lizenziert NetScaler ADM zuerst diese virtuellen Server und aktiviert dann Analysen.
- Für Admin-Partitionen wird nur **Web Insight** unterstützt
- Für virtuelle Server wie Cache-Umleitung , Authentifizierung und GSLB können Sie Analysen nicht aktivieren. Eine Fehlermeldung wird angezeigt.

Nachdem Sie auf **OK** geklickt haben, verarbeitet NetScaler ADM Analysen auf den ausgewählten virtuellen Servern zu aktivieren.



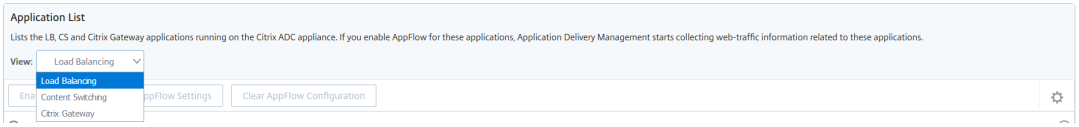
Wenn Ihr NetScaler ADM **13.0 ist Build 36.27 oder früher**:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC**, und wählen Sie die NetScaler ADC-Instanz aus, für die Sie die Analyse aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.

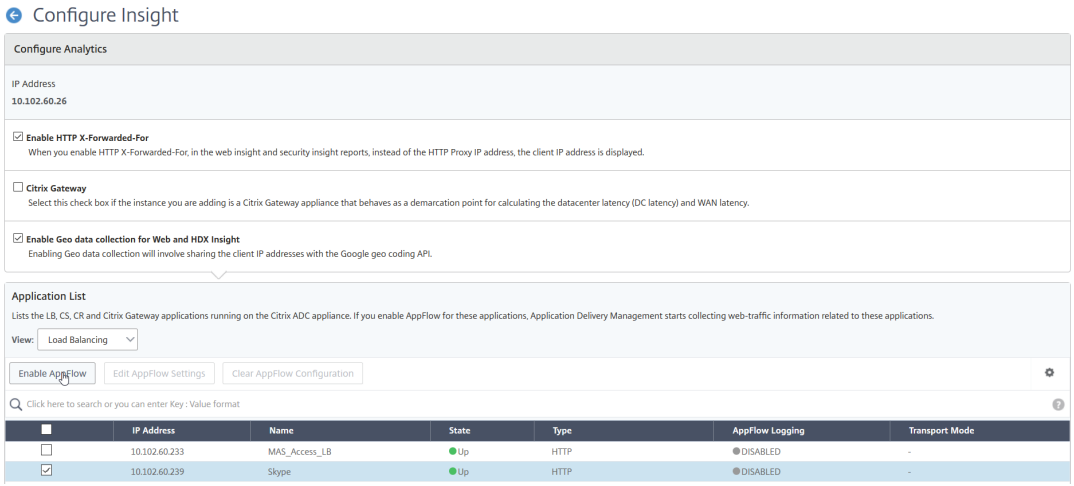


3. Gehen Sie auf der Seite **"Insight konfigurieren** "wie folgt vor:

   a) Wählen Sie die **Anwendungsliste** für Load Balancing oder Content Switching aus.



b) Wählen Sie den virtuellen Server aus, und klicken Sie auf **AppFlow aktivieren**.

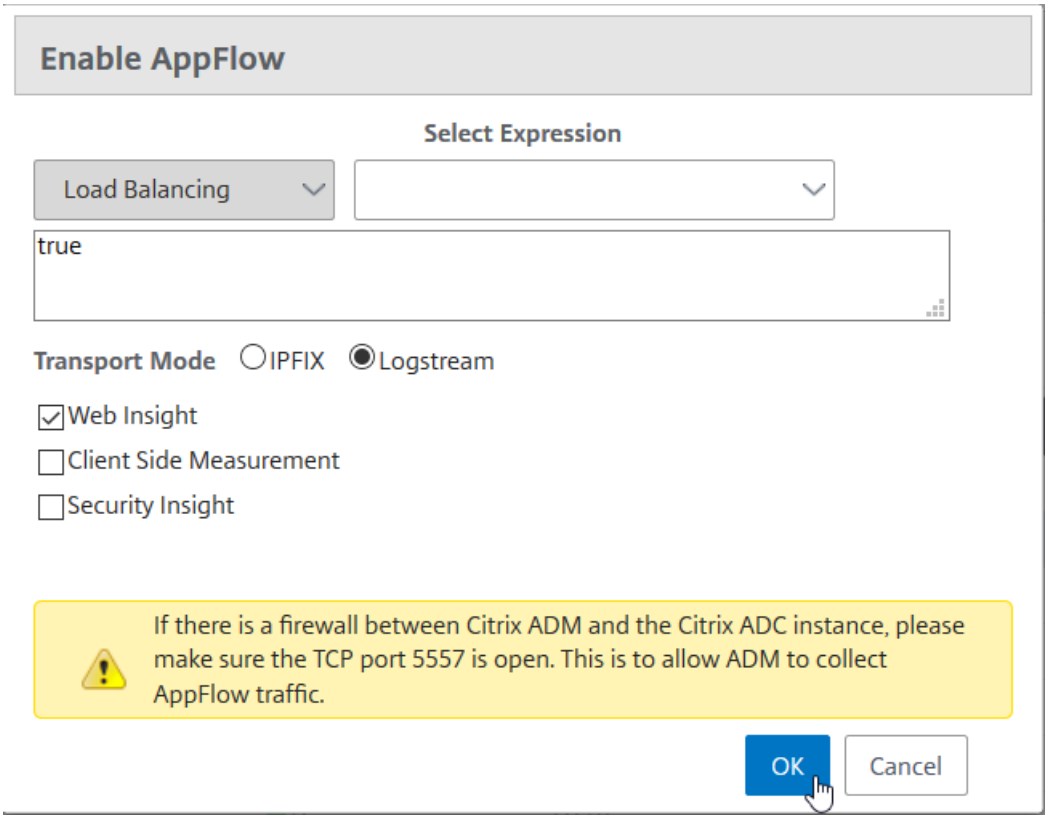


4. Gehen Sie im Dialogfeld “AppFlow aktivieren”wie folgt vor:

   - Geben Sie **true** in das Textfeld ein
   - Wählen Sie **Logstream** als Transportmodus

     > Hinweis: Citrix empfiehlt Ihnen, Logstream als Transportmodus auszuwählen.

   - Wählen Sie **Web Insight** aus, und klicken Sie auf **OK**.



So aktivieren Sie das AppFlow Feature mithilfe der NetScaler ADC GUI:

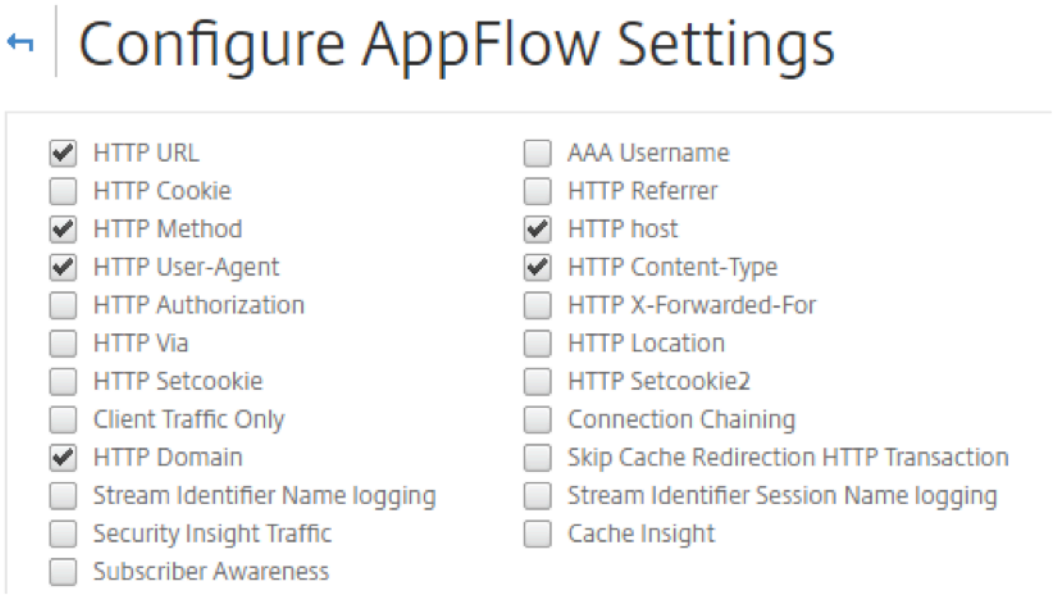
Navigieren Sie in der Benutzeroberfläche einer NetScaler ADC Instanz zu **Konfiguration** > **System** > **Einstellungen**, klicken Sie auf **Erweiterte Funktionen konfigurieren**und wählen Sie **AppFlow**aus.

SSL Insight-Parameter aktivieren

Auf jeder NetScaler ADC Instanz müssen Sie einige HTTP-Parameter aktivieren, um SSL-Insight-Datensätze in NetScaler ADM anzuzeigen.

So aktivieren Sie SSL-Insight-Parameter über das Citrix ADC Konfigurationsprogramm:

1. Navigieren Sie zu **Konfiguration** > **System** > **AppFlow**und klicken Sie auf **AppFlowSettings ändern**.
2. Aktivieren Sie die folgenden Kontrollkästchen: **HTTP-Domäne**, **HTTP-Host**, **HTTP-Methode**, **HTTP-URL**, **HTTP-Benutzeragent**, **HTTP-Inhaltstyp**.
3. Klicken Sie auf **OK**.



Anzeigen der SSL Insight-Metriken

SSL Insight-Metriken in NetScaler ADM bieten einen detaillierten Überblick über die Leistung der SSL-Transaktionen, die von den NetScaler ADC Instanzen bereitgestellt werden. Sie können die SSL Insight-Metriken auf Client-, Server- oder Anwendungsebene sowie die Metriken für SSL-Erfolgs- und Fehlschlagstransaktionen einsehen. Mithilfe dieser Metriken können Sie Ihre **NetScaler ADC HTTPS-Einstellungen** und SSL-Zertifikatseinstellungen analysieren und optimieren und Leistungsprobleme verfolgen.

> **Hinweis**
>
> Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, Zugriff auf Anwendungsebene für die Gruppe gewähren und Benutzer der Gruppe zuweisen. Citrix ADM Analytics unterstützt jetzt die auf virtuellen IP-Adressen basierende Autorisierung. Ihre Benutzer können jetzt Berichte für alle Insights nur für die Anwendungen (virtuelle Server) anzeigen, für die sie autorisiert sind. Weitere Informationen zu Gruppen und zum Zuweisen von Benutzern zur Gruppe finden Sie unter Konfigurieren von Gruppen.

So überwachen Sie SSL-Insight-Metriken in NetScaler ADM:

Sie können SSL-Metriken anzeigen für:

- Eine Anwendung. Navigieren Sie zu **Anwendungen > Dashboard**, klicken Sie auf eine Anwendung und wählen Sie die Registerkarte **Web Insight** aus, um die detaillierten Metriken anzuzeigen. Weitere Informationen finden Sie unter Analyse der Anwendungsnutzung.

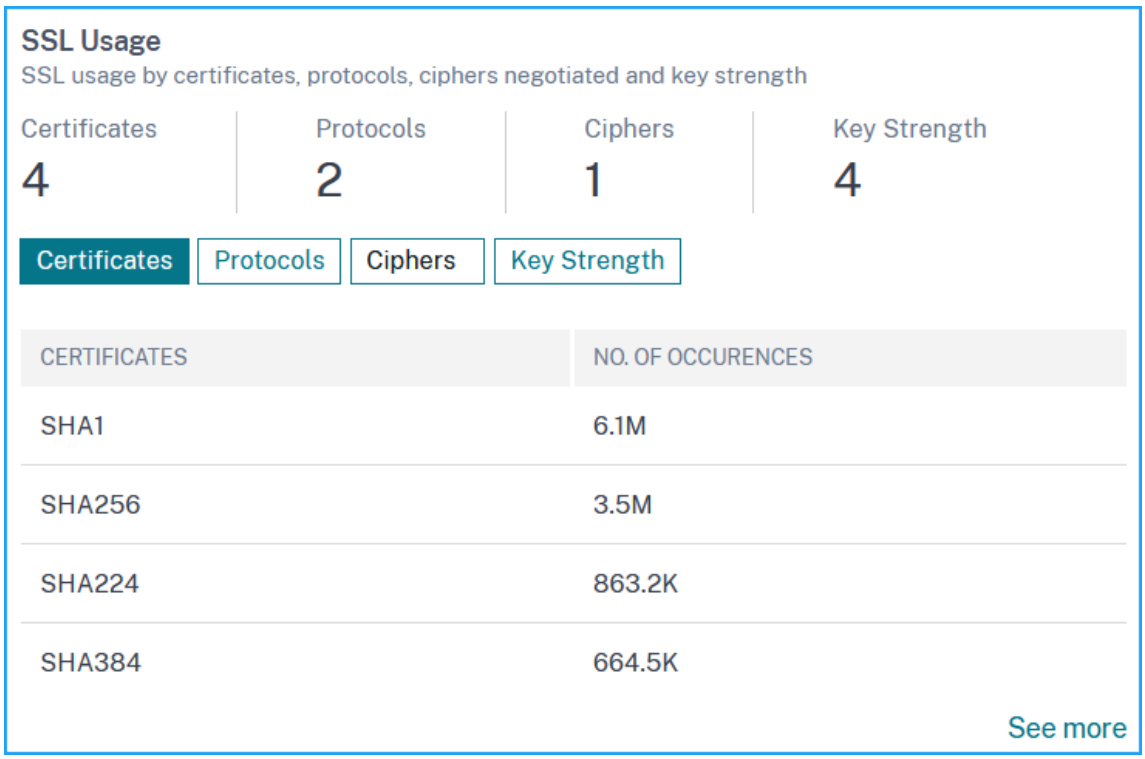
- Alle Anwendungen. Navigieren Sie zu **Applications > Web Insight** und klicken Sie auf **Anwendungen** und **Clients**, um die SSL-Metriken anzuzeigen

Anwendungsfall: Verschaffen Sie sich einen Überblick über die SSL-Transaktionen

Der folgende Anwendungsfall beschreibt, wie Sie SSL Insight verwenden können, um die Verwendung verschiedener SSL-Parameter zu bewerten und die Sicherheitsmaßnahmen zu verbessern.

Beachten Sie, dass Sie über eine Reihe von Anwendungen verfügen, die SSL-Transaktionen (HTTPS) für die Kommunikation verwenden, und Sie NetScaler ADM konfiguriert haben, um die SSL-Komponenten zu überwachen. Möglicherweise müssen Sie die Anwendungen häufig überprüfen, damit Sie sich zuerst auf die Anwendungen konzentrieren können, die die größte Aufmerksamkeit benötigen. Das **Web Insight** Dashboard für eine Anwendung oder alle Anwendungen bietet eine Zusammenfassung der folgenden SSL-Parameter unter **SSL-Fehler** und **SSL-Nutzung**:

- SSL-Zertifikate
- SSL-Protokolle
- SSL-Verschlüsselung
- SSL-Schlüsselstärke
- SSL-Fehler —Frontend
- SSL-Fehler —Back-End

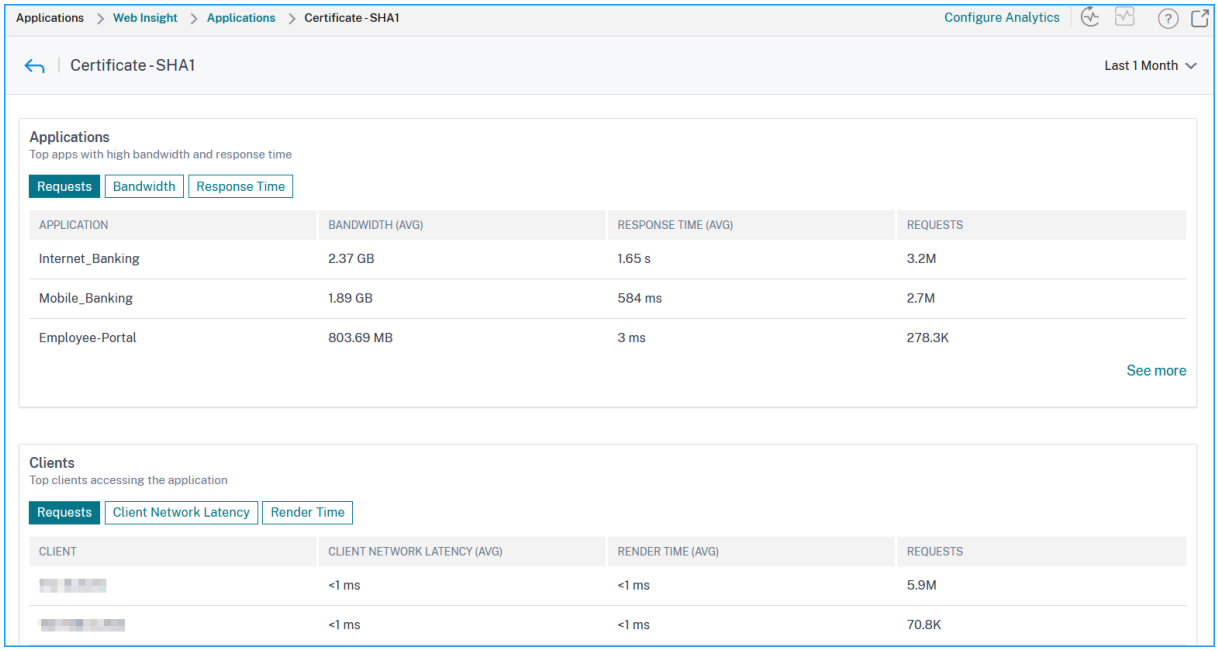


Sie können auf jede Registerkarte klicken, um Details anzuzeigen.

Anwendungsfall: SSL-Metriken für Kunden

Sie können eine Liste der Clients (identifiziert durch ihre IP-Adressen) und die Gesamtzahl der Vorkommen pro Client sehen. Navigieren Sie zu **Applications > Web Insight** und wählen Sie die Registerkarte **Clients** aus, um die Details unter **SSL-Nutzung**anzuzeigen.

Klicken Sie auf eine Metrik, um Details anzuzeigen, und klicken Sie unter **Clients**auf eine beliebige Client-IP-Adresse, um die SSL-Metriken für den ausgewählten Client anzuzeigen



TCP Insight

February 5, 2024

Die TCP Insight-Funktion von Citrix Application Delivery Management (ADM) bietet eine einfache und skalierbare Lösung zur Überwachung der Metriken der Optimierungstechniken und der Engpasskontrollstrategien (oder Algorithmen), die in Citrix ADC Appliances verwendet werden, um Netzwerküberlastung bei der Datenübertragung zu vermeiden. Diese Funktion verwendet die Funktion “TCP Speed Report”, die die Leistung beim Herunterladen oder Hochladen von TCP-Dateien mit und ohne TCP-Optimierung misst.

Sie können die wichtigsten **Transport Layer-Metriken**wie Datenvolumen, Durchsatz und Geschwindigkeit anzeigen und diese Informationen verwenden, um das von den NetScaler ADC-

Instanzen bereitgestellte Verkehrsvolumen zu messen und die Vorteile der TCP-Optimierung zu überprüfen. Aufschlüsselungen nach Streamrichtung (vom Client zum NetScaler ADC und NetScaler ADC zum Ursprungsserver), TCP-Port und virtuellem LAN werden für die oben genannten Metriken bereitgestellt.

Voraussetzungen

Bevor Sie mit der Konfiguration der TCP Insight-Funktion beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Die NetScaler ADC-Instanzen werden auf Softwareversion 11.1 Build 51.21 oder höher ausgeführt.
- Sie haben NetScaler ADM installiert, das auf der Softwareversion 11.1 Build 51.21 oder höher ausgeführt wird.
- Alle für eine Anwendung konfigurierten virtuellen Server sind für die Verwaltung und Überwachung auf NetScaler ADM lizenziert.
  Informationen zur Citrix ADM Lizenzierung finden Sie unter Lizenzierung.

TCP Insight aktivieren

Bevor Sie die TCP Insight-Metriken anzeigen können, müssen Sie die Funktion in NetScaler ADM aktivieren.

So aktivieren Sie TCP Insight:

1. Geben Sie in einem Webbrowser die IP-Adresse der virtuellen Citrix ADM Appliance ein (z. B.http://192.168.100.1).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **Analytics** > **Einstellungen**, und klicken Sie auf **Features für Analytics aktivieren**.
4. Wählen Sie auf der Seite **Features für Analysen aktivieren** die Option **TCP Insight aktivieren** aus.
5. Klicken Sie im Bestätigungsfenster auf **OK**.

Anzeigen der TCP Insight-Metriken in NetScaler ADM

Nachdem Sie TCP Insight in NetScaler ADM aktiviert haben, können Sie wichtige Transportschichtinformationen wie Verkehrsmodus (Internet- oder Mobildaten), Datenvolumen, Durchsatz,

Schnittstellen, Ports, durchschnittliche Upload-Geschwindigkeit und durchschnittliche Download-Geschwindigkeit anzeigen.

So zeigen Sie TCP Insight-Metriken in NetScaler ADM an:

Navigieren Sie zu **Analytics** > **TCP Insight**.

Sie können den Mauszeiger auf die Balkendiagramme bewegen, um das Datenvolumen der entsprechenden Transporttechniken anzuzeigen. Sie können auch das Datenvolumen und andere Metriken in der Tabelle unterhalb des Diagramms anzeigen.

> **Hinweis** Sie können die im Diagramm angezeigten Metriken anpassen, indem Sie das Einstellungssymbol in der Tabelle verwenden. Sie können auch den Zeitraum auswählen, auf den sich die Metriken beziehen, und den Zeitschieberegler verwenden, um den Zeitraum anzupassen.

Sie können auch Metriken für beispielsweise Schnittstellen, Ports und Bitraten anzeigen, indem Sie aus der **TCP Insight-Liste** auswählen.

Anwendungsfälle

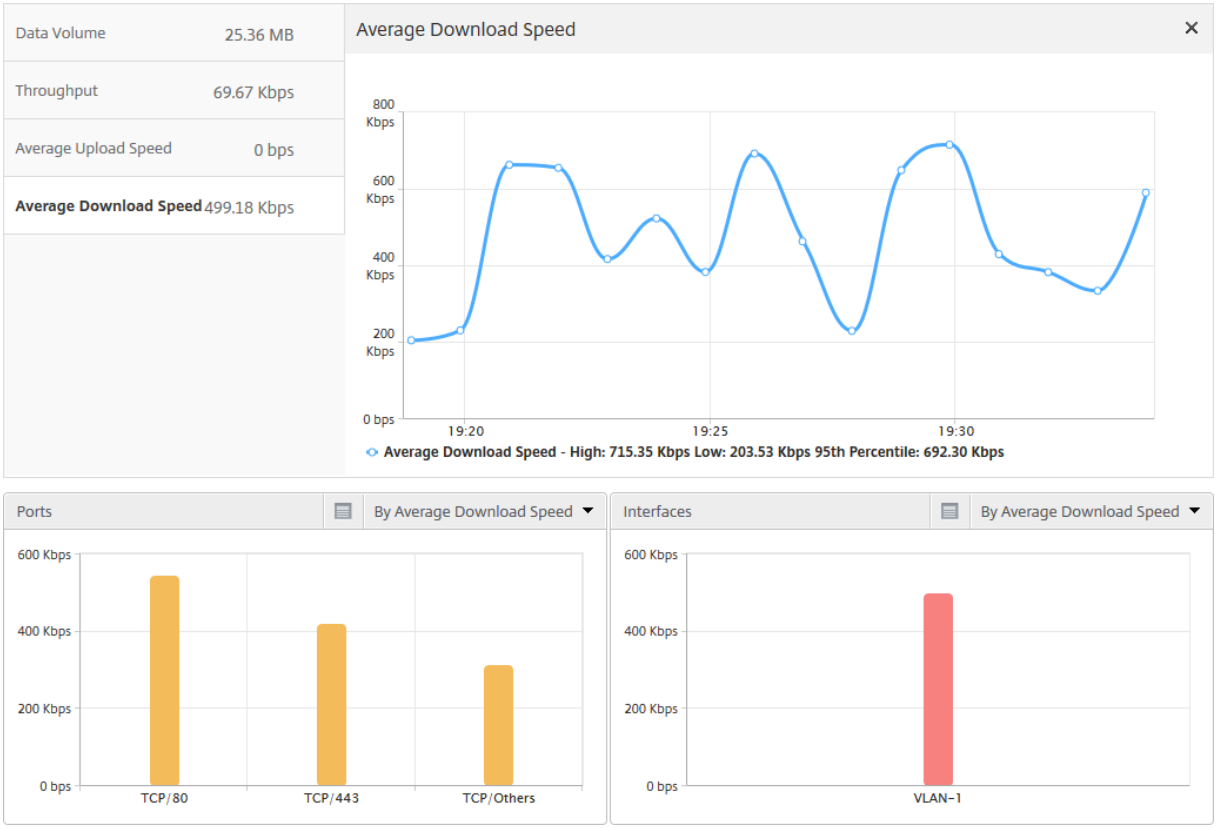
Die folgenden Anwendungsfälle veranschaulichen einige Möglichkeiten zur Verwendung von TCP Insight auf NetScaler ADC Appliances:

- Bewertung der Vorteile der TCP-Optimierung
- TCP-Parameter optimieren
- Messung der Auswirkungen der TCP-Optimierung auf das Verkehrsaufkommen

Bewertung der Vorteile der TCP-Optimierung

Inwieweit kommt die NetScaler ADC TCP-Optimierung tatsächlich einem Mobil- (Radio) oder Unternehmensnetzwerk (Internet) zugute? Sie können die Geschwindigkeit von Datenübertragungen anzeigen, die über TCP stattfinden, und nicht optimierte und optimierte Leistung vergleichen. Diese Messungen werden separat für die Download- und Upload-Richtungen (immer auf der Radio/Client-Seite) und für verschiedene Zielports HTTP (80) und HTTPS (443) angezeigt.
Durch die Untersuchung der TCP Insight-Metriken können Sie die durch die Optimierung der TCP-Flows erzielte Geschwindigkeitsverbesserung quantifizieren.

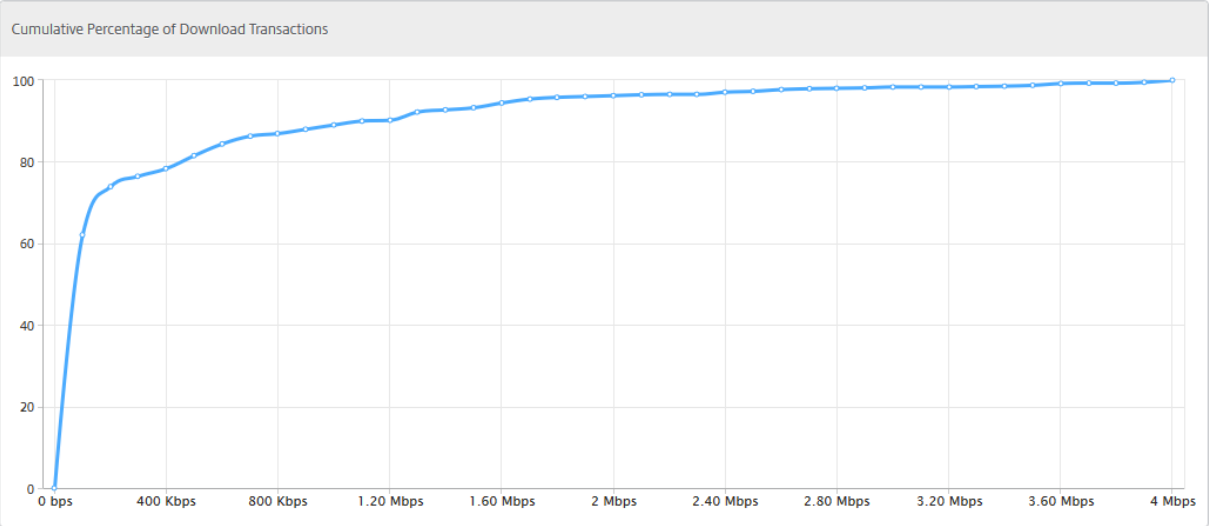
Um eine Zusammenfassung dieser Parameter anzuzeigen, melden Sie sich bei NetScaler ADM an, und klicken Sie auf die Registerkarte **TCP Insight**. Klicken Sie dann auf **Seiten**, und wählen Sie **Internet** oder **Radio** aus dem Balkendiagramm oder der Tabelle unterhalb des Diagramms aus.



TCP-Parameter optimieren

Die Verwendung verschiedener TCP-Profile kann zu unterschiedlichen Ausgaben für denselben Datenverkehr führen. In solchen Situationen möchten Sie möglicherweise die Geschwindigkeitsmessungen von Zeiträumen anzeigen und vergleichen, in denen NetScaler ADC verschiedene TCP-Optimierungsprofile ausführt. Sie können die Ergebnisse verwenden, um TCP-Parameter für eine schnellere Übertragung zu optimieren und ein TCP-Profil zu entwickeln, das die vom Benutzer wahrgenommene Erfahrung in einem bestimmten Kundennetzwerk maximiert.

Melden Sie sich bei NetScaler ADM an, um die Berichte anzuzeigen. Klicken Sie dann auf der Registerkarte **TCP Insight** auf **Bitraten**und wählen Sie die gewünschte Bitrate aus dem Balkendiagramm oder der Tabelle unter dem Diagramm aus.

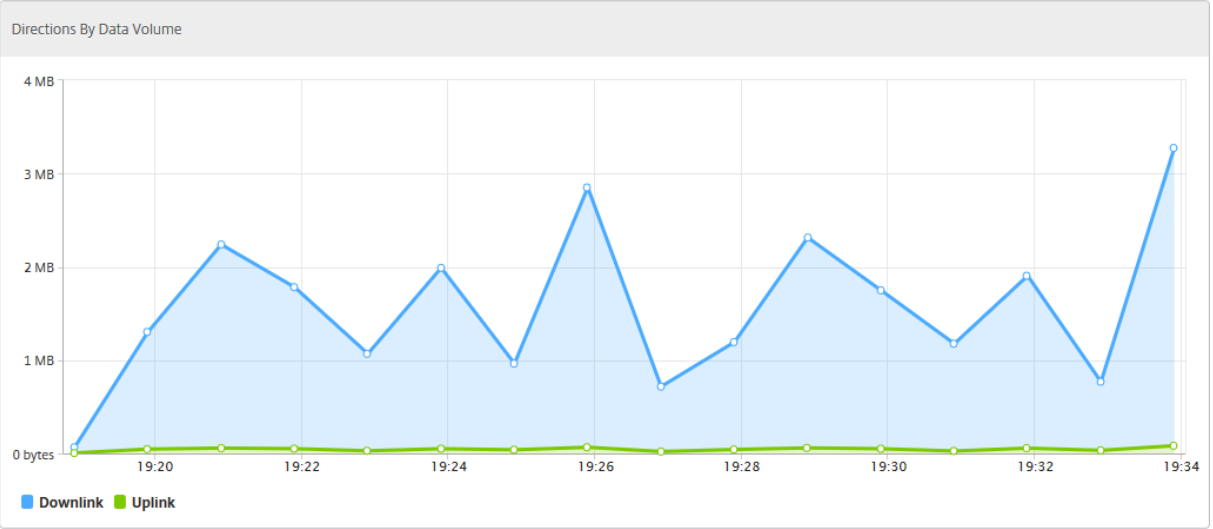


Messung der Auswirkungen der TCP-Optimierung auf das Verkehrsaufkommen

Messungen von IP-Layer Data Volume/Durchsatz, die von einer NetScaler ADC-Instanz verarbeitet werden, können zwischen verschiedenen Zeiträumen verglichen werden, um die Auswirkungen der TCP-Optimierung auf den Verbrauch von Teilnehmerdaten zu bewerten. Die Messungen können separat für jede Seite des Netzwerks (funkseitig vs. internetseitig), für verschiedene Verkehrssegmente (abgegrenzt durch verschiedene Schnittstellen oder VLANs), für jede Richtung (Downlink vs. Uplink) und für verschiedene Zielports (HTTP und HTTPS) angewendet werden. Der Vergleich kann verwendet werden, um zu bestätigen, dass die TCP-Optimierung Abonnenten dazu ermutigt, mehr Daten zu konsumieren.

Um eine Zusammenfassung der Messungen zu erhalten, melden Sie sich bei NetScaler ADM an, klicken Sie auf der Registerkarte **TCP Insight** auf **Sides**, und wählen Sie dann **Internet** oder **Radio** aus dem Balkendiagramm oder der Tabelle unter dem Diagramm aus.

Sie können auch einen anderen Zeitrahmen aus der Zeitliste auswählen. Sie können den Zeitrahmen mithilfe des Zeitrahmen-Schiebereglers anpassen.



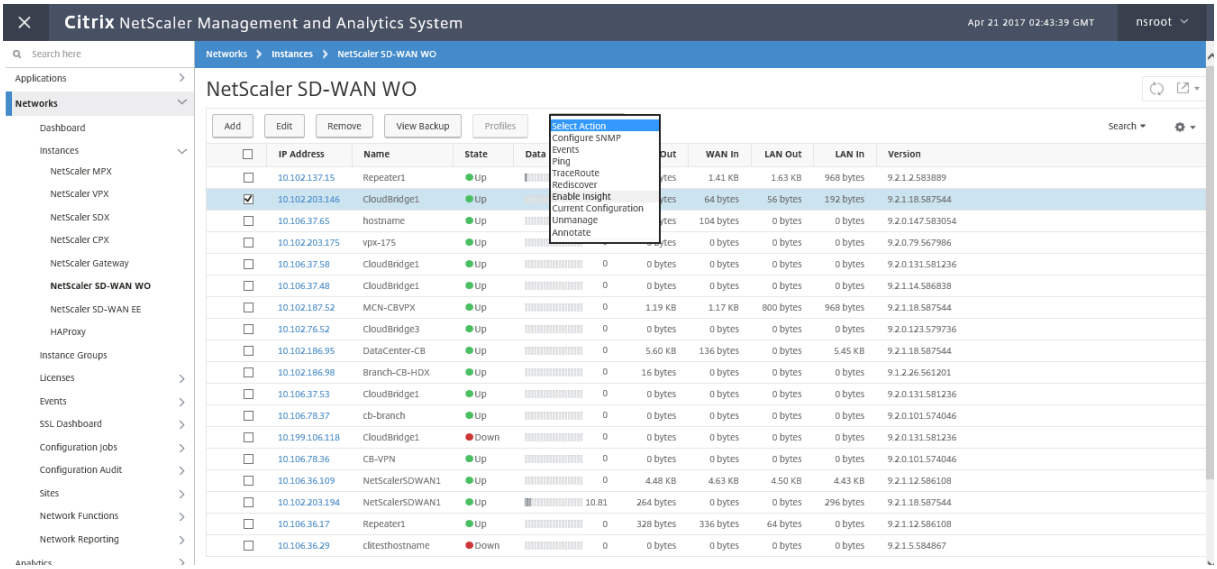
WAN-Einblick

February 5, 2024

Die Citrix SD-WAN Optimization (WO) -Appliances optimieren die Bereitstellung vieler Anwendungen über das WAN, indem sie die Effizienz des Datenflusses über das Netzwerk zwischen dem Rechenzentrum und den Zweigstellen verbessern.

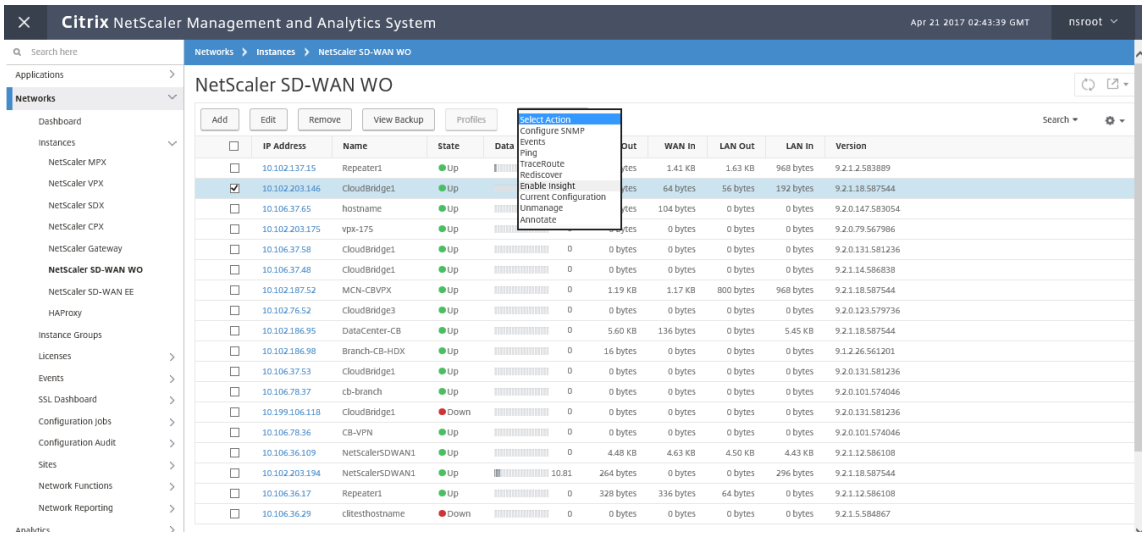
WAN Insight Analytics ermöglichen es Administratoren, den beschleunigten und nicht beschleunigten WAN-Datenverkehr, der zwischen dem Rechenzentrum und den WAN-Optimierungsgeräten des Zweigs fließt, einfach zu überwachen WAN Insight bietet Einblick in Clients, Anwendungen und Zweigstellen im Netzwerk, um Netzwerkprobleme effektiv zu beheben. Live- und Verlaufsberichte ermöglichen es Ihnen, Probleme, falls vorhanden, proaktiv anzugehen.

Die Aktivierung von Analysen auf der WAN-Optimierungs-Appliance für Rechenzentren ermöglicht es dem NetScaler ADM, Daten zu sammeln und Berichte und Statistiken für das Rechenzentrum und die Zweigstellen-WAN-Optimierungsgeräte bereitzustellen.



So aktivieren Sie Analysen auf der WAN-Optimierungs-Appliance:

1. Navigieren Sie zu **Netzwerke**> **Instanzen** > **Citrix SD-WAN**, und wählen Sie die SD-WAN WO-Instanz aus.

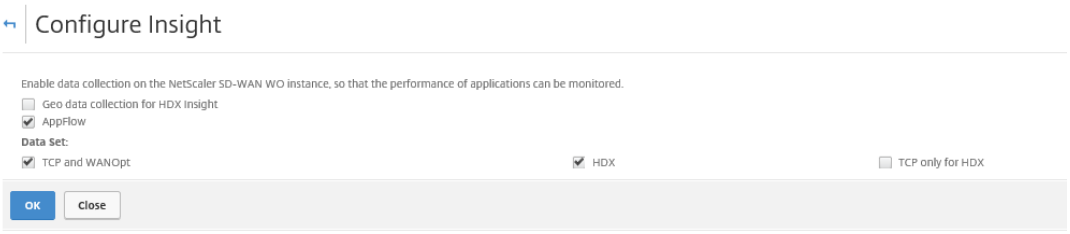


2. **Wählen Sie in der Liste Aktion**auswählen die Option**Analytics konfigurieren**aus.
3. Wählen Sie die folgenden Parameter nach Bedarf aus:

   - **Geodatenerfassung für HDX Insight**: Freigabe der Client-IP-Adresse mit der Google Geo API.

   - **AppFlow**: Beginnt das Sammeln von Daten aus WAN-Optimierungsinstanzen.

     - **TCP und WANOpt**: Stellt **TCP- und WANOpt** Insight-Berichte bereit.
     - **HDX**: Stellt HDX Insight-Berichte bereit.
     - **TCP nur für HDX**: Bietet TCP nur für HDX Insight Berichte.



4. Klicken Sie auf **OK**.

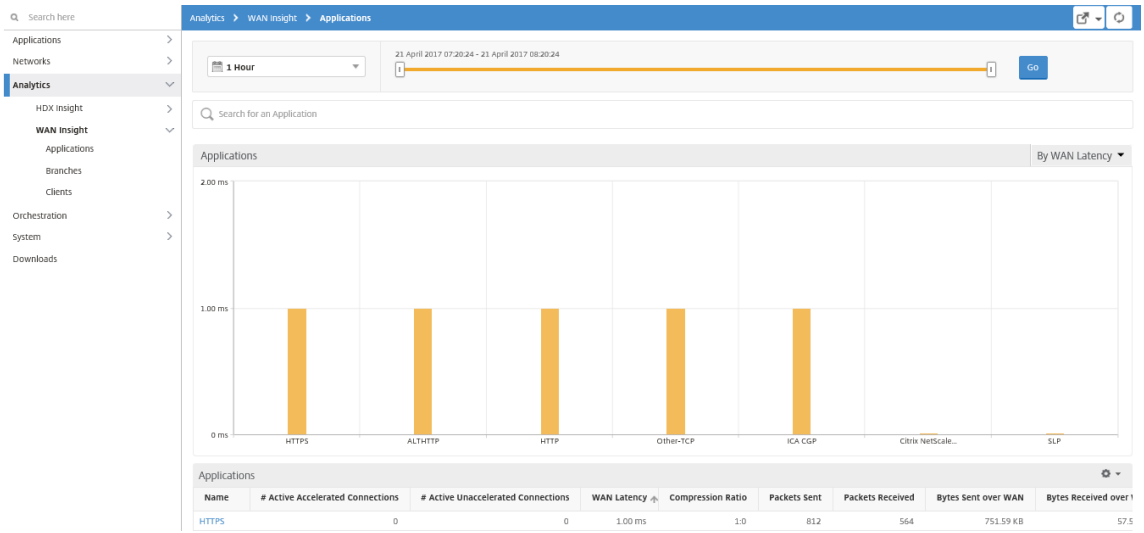
So zeigen Sie WAN Insight-Berichtean:

1. Navigieren Sie zu **Analytics** > **WAN Insight**.

> **Hinweis**
>
> Die Option WAN Insight ist erst sichtbar, nachdem Sie eine SD-WAN WO-Instanz zu NetScaler ADM hinzugefügt haben.

Sie können die folgenden Berichte anzeigen:

- **Anwendungen** - Zeigt die Nutzungs- und Leistungsstatistiken aller Anwendungen für die ausgewählte Dauer an.
- **Zweige** - Zeigt die Nutzungs- und Leistungsstatistiken aller Geräte für WAN-Optimierungszweige an.
- **Clients** - Zeigt die Nutzungs- und Leistungsstatistiken aller Clients an, die auf die WAN-Optimierungs-Appliances in jedem Zweig zugreifen.



Die folgenden Metriken werden angezeigt:

Metrik	Beschreibung
Aktive beschleunigte Verbindungen	Anzahl der aktiven WAN-Verbindungen, die beschleunigt werden.
Aktive nicht beschleunigte Verbindungen	Anzahl der aktiven WAN-Verbindungen, die nicht beschleunigt werden.
WAN-Latenz	Verzögerung in Millisekunden, die der Benutzer bei der Interaktion mit einer Anwendung erlebt.
Komprimierungsverhältnis	Verhältnis der Datenkomprimierung zwischen der Zweigstelle und den Appliances des Rechenzentrums für die ausgewählte Dauer.
Gesendete Pakete	Anzahl der Pakete, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer über das Netzwerk gesendet hat.
Empfangene Pakete	Anzahl der Pakete, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer vom Netzwerk empfangen hat.
Über WAN gesendete Bytes	Anzahl der Bytes, die die Citrix WAN-Optimierungs-Appliance für die ausgewählte Dauer über das WAN gesendet hat.
Über WAN empfangene Bytes	Anzahl der Bytes, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer vom WAN empfangen hat.
LAN RTO	Anzahl der Male, mit denen die WAN-Optimierungs-Appliance die erneute Übertragung an das LAN für die ausgewählte Dauer überschritten hat.
WAN RTO	Anzahl der Male, mit denen die WAN-Optimierungs-Appliance die erneute Übertragung an das WAN für die ausgewählte Dauer überschritten hat.
Pakete erneut übertragen (LAN)	Anzahl der Pakete, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer erneut an das LAN-Netzwerk übertragen hat.

Metrik	Beschreibung
Pakete erneut übertragen (WAN)	Anzahl der Pakete, die die WAN-Optimierungs-Appliance für die ausgewählte Dauer erneut an das WAN-Netzwerk übertragen hat.

Video Insight

February 5, 2024

Die Video Insight-Funktion bietet eine einfache und skalierbare Lösung für die Überwachung der Metriken der Videooptimierungstechniken, die von NetScaler ADC Appliances zur Verbesserung der Kundenerfahrung und betrieblichen Effizienz verwendet werden. Sie bietet folgende Vorteile:

- Verwalten Sie das Netzwerk bei Überlastung in Spitzenzeiten.
- Verbessern Sie die Konsistenz der Videowiedergabe und reduzieren Sie Videoverzögerungen
- Aktivieren Sie neue Videodienstangebote (z. B. Binge-on-Videodienste).
- Ermöglichen Sie Kunden die Auswahl der besten nachhaltigen Videoqualität.
- Bieten Sie dem Abonnenten eine konsistente Benutzererfahrung.

Bei der Optimierung des Videoverkehrs verwendet die NetScaler ADC Appliance einen speziellen Mechanismus, um die Videobitrate dynamisch zu beschleunigen, und eine Zufallsabtastung, um die Einsparungen durch die Optimierungstechnik abzuschätzen. Weitere Informationen zur NetScaler ADC-Videooptimierungsfunktion finden Sie unter Videooptimierung.Wenn Sie die NetScaler ADC Appliance in NetScaler Application Delivery Management (ADM) integrieren, werden wichtige Informationen aus den Videodaten gesammelt, die über die NetScaler ADC Appliance fließen. Sie können diese Informationen verwenden, um die optimierte und nicht optimierte Leistung des ABR-Videoverkehrs zu vergleichen, die Einsparungen aufgrund der Optimierung zu ermitteln und so weiter.

> **Hinweis**
>
> Die Statistiken der nicht optimierten Sitzungen in NetScaler ADM entsprechen den Sitzungen, die Sie in der NetScaler ADC Appliance ausgewählt haben. Weitere Informationen zur Zufallsstichprobe finden Sie unterVideooptimierung.

Video Insight in NetScaler ADM stellt Metriken für die folgenden Arten von Videoverkehr bereit:

- Progressiver Download (PD) von Videos über HTTP
- ABR-Videos über HTTP
- ABR-Videos über HTTPS
- YouTube ABR-Videos über QUIC

Video Insight konfigurieren

> **Hinweis**
>
> Video Insight wird auf NetScaler ADC-Instanzen mit NetScaler ADC Premium-Lizenz unterstützt. Die NetScaler ADC Premium-Lizenz wird für NetScaler ADC Telco-Plattformen (VPX T1000 und VPX-T) unterstützt.

Um Video Insight in einer Citrix ADC Instanz zu konfigurieren, aktivieren Sie zunächst die AppFlow Funktion, konfigurieren Sie einen AppFlow-Collector, eine Aktion und eine Richtlinie und binden die Richtlinie global. Wenn Sie den Collector konfigurieren, müssen Sie die IP-Adresse des Citrix ADM -Servers angeben, auf dem die Berichte überwacht werden sollen.

Um Videoinformationen für eine NetScaler ADC-Instanz zu konfigurieren, führen Sie die folgenden Befehle aus, um ein AppFlow Profil und eine Richtlinie zu konfigurieren und die AppFlow-Richtlinie global zu binden.

add appflow collector <name> **-IPAddress** <ipaddress> **-port** <port_number> **-Transport** logstream

set appflow param -**videoInsight** ENABLED

add appflow action <name> **-collectors** <string> **-videoAnalytics** ENABLED

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

enable ns mode `ulfd`

enable feature AppFlow

Beispiel

```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
    Transport logstream
set appflow param -videoInsight ENABLED
add appflow action act1 -collectors col1 -videoAnalytics ENABLED
add appflow policy appol true act1
bind appflow global appol 1
enable ns mode ulfd
```



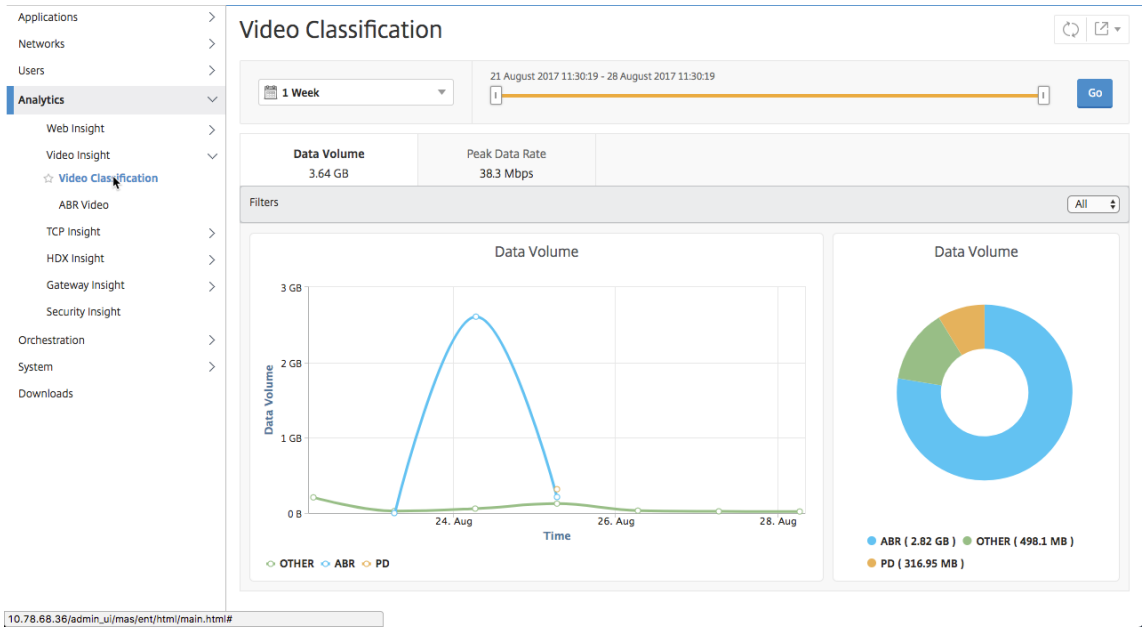
```
enable feature appflow
<!--NeedCopy-->
```

Anzeigen der Video Insight-Metriken in NetScaler ADM

Nachdem Sie Video Insight in NetScaler ADM aktiviert haben, können Sie Video-Optimierungsmetriken wie Videoklassifizierung, Datenvolumen, Spitzendatenrate und ABR-Videowiedergabe anzeigen. Diese Metriken helfen Ihnen dabei, Ihr Netzwerk zu analysieren und die Videos zu optimieren, um die Nutzererfahrung, die betriebliche Effizienz und andere Leistungskriterien zu verbessern.

So zeigen Sie die Video Insight-Metriken in Citrix ADM an:

1. Geben Sie in einem Webbrowser die IP-Adresse der virtuellen Citrix ADM Appliance ein (z. B.http://192.168.100.1).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **Analytics > Video Insight**.



> **Hinweis**
>
> Die von der Legende **OTHER** in den Diagrammen bereitgestellten Werte stellen die Nicht-ABR- und Nicht-PD-Daten im Videoverkehr dar, abhängig vom ausgewählten Filter:
>
> - **Alle** —Summe der Nicht-ABR-Daten (HTTP, HTTPS und QUIC) und Nicht-PD (HTTP) im Videoverkehr.
> - **HTTP** —Summe der Nicht-ABR- und Nicht-PD-Daten im Videoverkehr.
> - **HTTPS** —Summe der Nicht-ABR-Videodaten im Videoverkehr.

- **QUIC** —Summe der Nicht-ABR-Videodaten im Videoverkehr.

Netzwerkeffizienz anzeigen

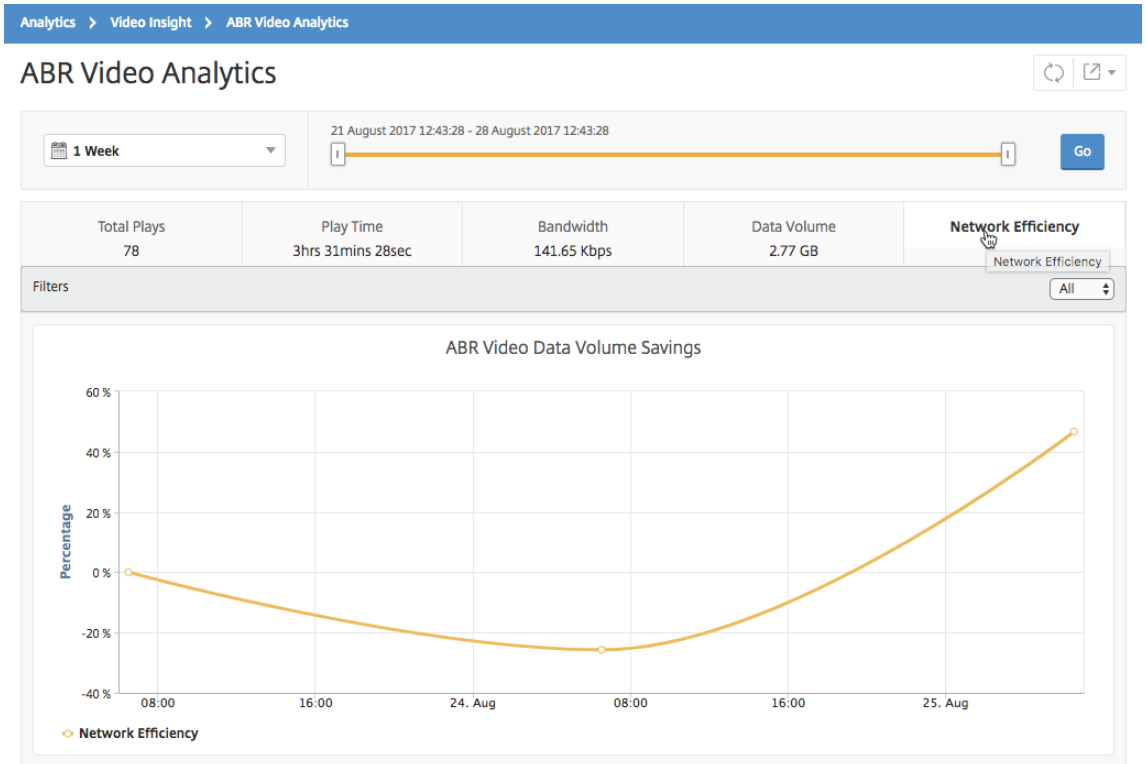
February 5, 2024

Für einen bestimmten Zeitraum stellt Citrix Application Delivery Management (ADM) ein Diagramm bereit, das das Verhältnis von optimierten zu nicht optimierten Videositzungen im Zeitrahmen anzeigt. Es zeigt auch den Prozentsatz der durch die Optimierung eingesparten Bandbreite an. Der Prozentsatz der eingesparten Bandbreite wird mit der folgenden Formel berechnet:

Prozentsatz der gesparten Bandbreite = **Durchschnittliches optimiertes ABR-Videodatenvolumen/Durchschn des nicht optimierten ABR-Videodatenvolumens**.

So sehen Sie den Prozentsatz der durch die Optimierung eingesparten Bandbreite:

1. Navigieren Sie zu **Analytics > Video Insight**und klicken Sie auf **ABR Video.**
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.
3. Klicken Sie auf **Los**, und wählen Sie die Registerkarte **Netzwerkeffizienz**.



Datenvolumen von optimierten und nicht optimierten ABR-Videos vergleichen

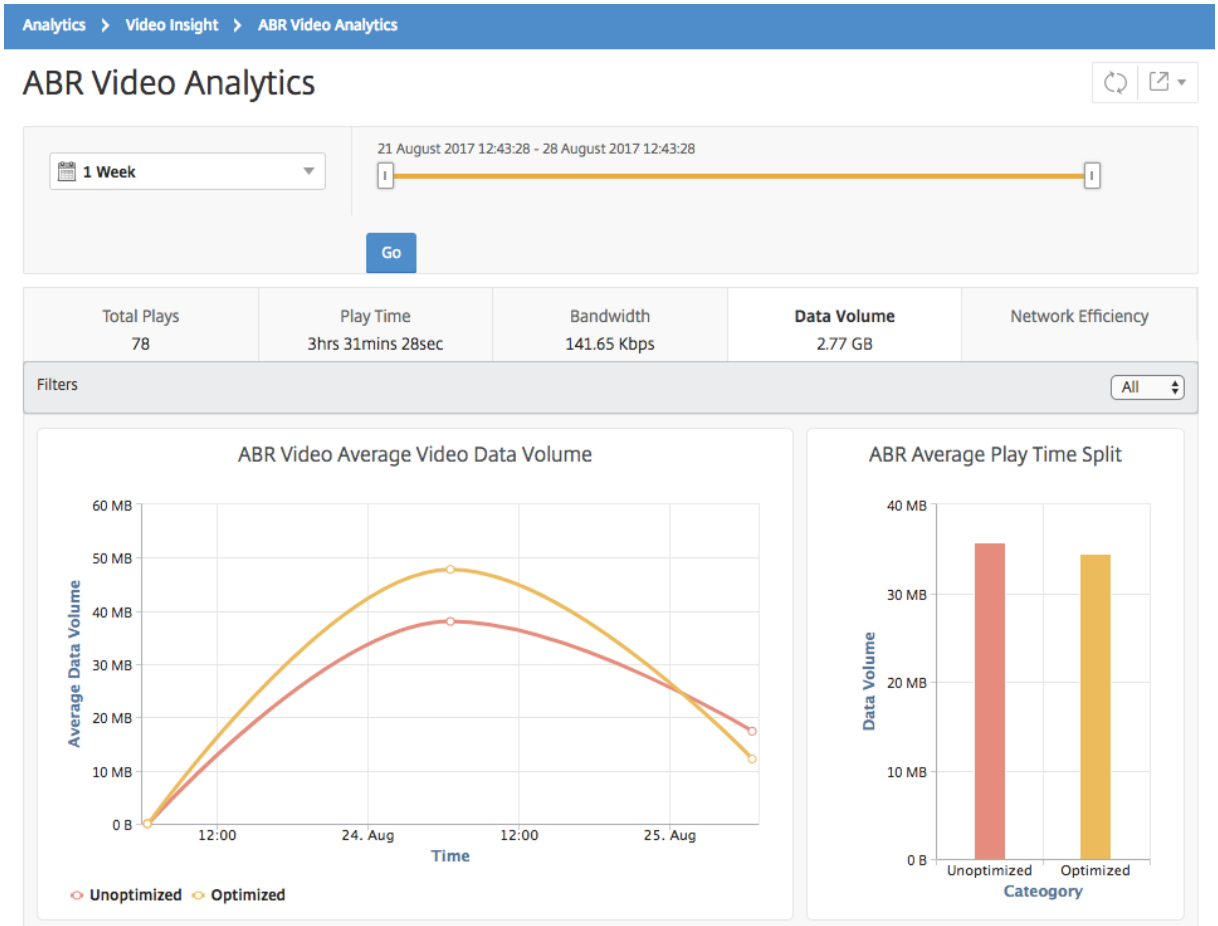
February 5, 2024

Für einen bestimmten Zeitraum zeigt Citrix Application Delivery Management (ADM) das Datenvolumen an, das von optimierten und nicht optimierten ABR-Videos verwendet wird, sodass Sie die beiden Volumes vergleichen können.

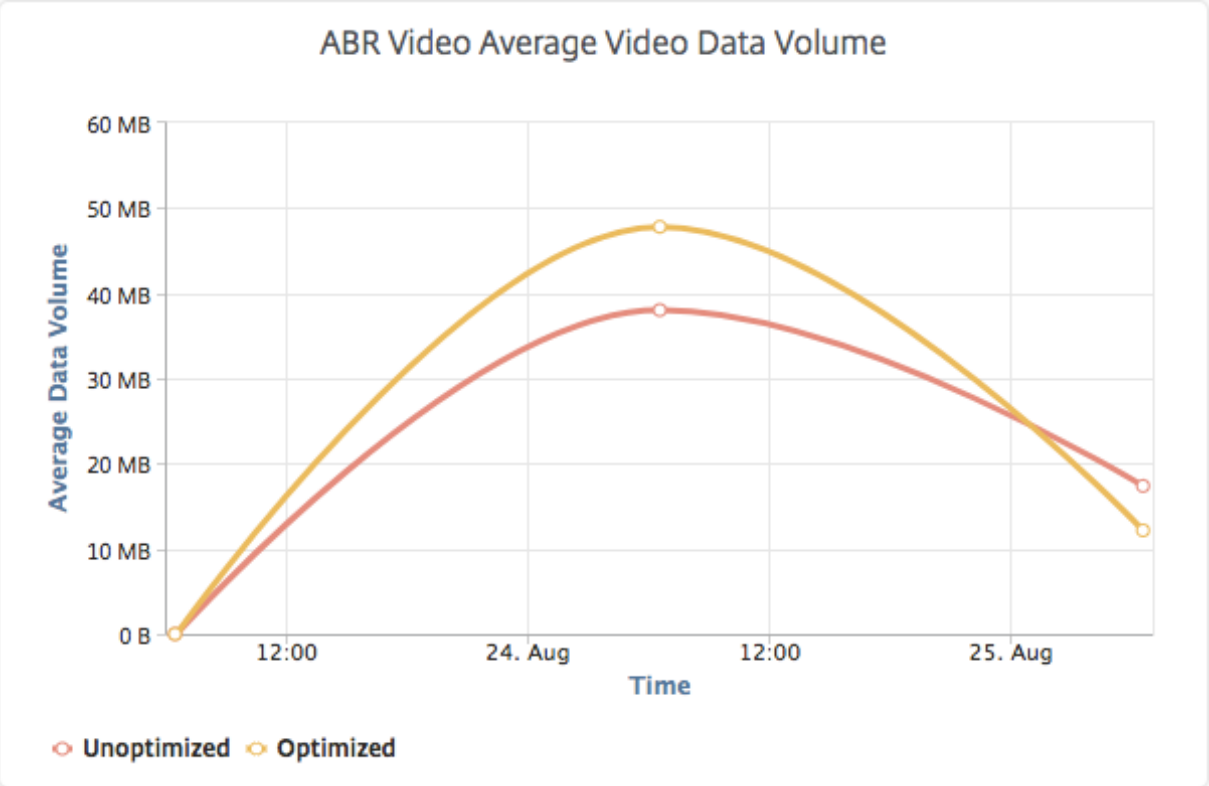
Um das von ABR-Videos verwendete Datenvolumen zu sehen:

1. Navigieren Sie zu **Analytics > Video Insight**und klicken Sie auf **ABR Video.**
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.
3. Klicken Sie auf **Los**, und wählen Sie die Registerkarte **Datenvolumen** aus.

Sie können die Liste **Filter** verwenden, um die HTTP-, HTTPS- oder QUIC-ABR-Videos auszuwählen.



Die Registerkarte **Datenvolumen** enthält ein Liniendiagramm und ein Kreisdiagramm, das das durchschnittliche Datenvolumen, das von ABR-Videos verwendet wird, sowie das Datenvolumen, das von optimierten und nicht optimierten ABR-Videos aus Ihrem Netzwerk für den ausgewählten Zeitraum verbraucht wird. Sie können den Mauszeiger auf das Liniendiagramm bewegen, um das durchschnittliche Datenvolumen anzuzeigen, das während eines bestimmten Zeitrahmens verwendet wird:



Typs der gestreamten Videos und des vom Netzwerk verbrauchten Datenvolumens anzeigen

February 5, 2024

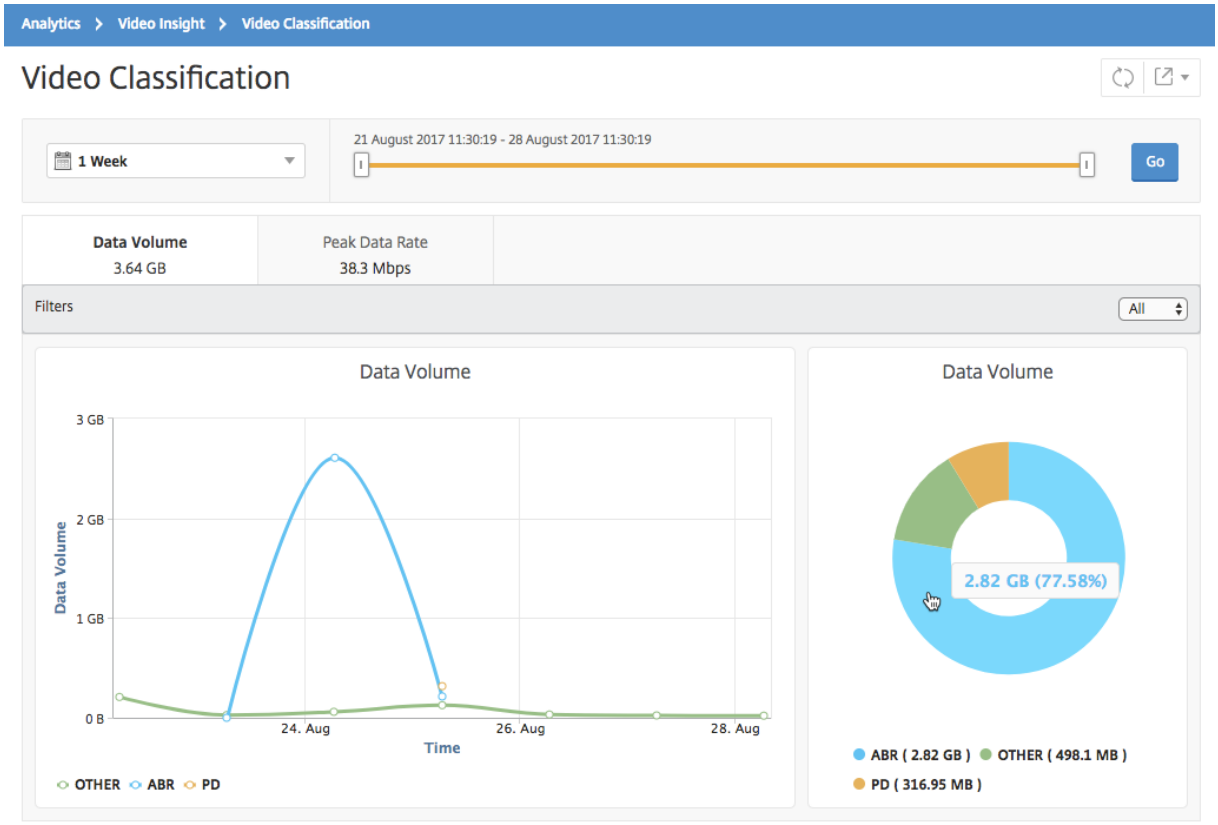
Die NetScaler ADC Appliance erkennt den verschlüsselten oder unverschlüsselten Videoverkehr in Ihrem Netzwerk und die Art des Videostreamings (PD oder ABR). NetScaler Application Delivery Management (ADM) zeigt diese Metriken und das Datenvolumen an, das vom Videoverkehr für einen definierten Zeitraum belegt wird.

So sehen Sie die Arten von Videos und das verbrauchte Datenvolumen:

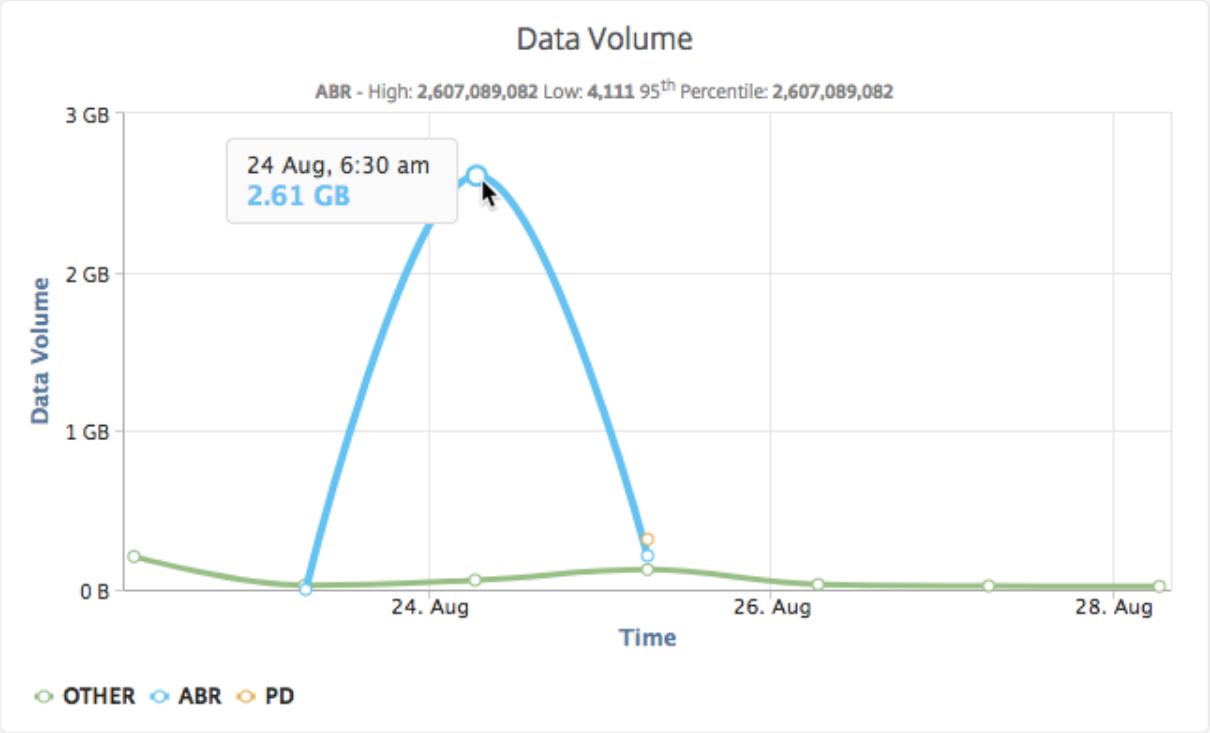
1. Navigieren Sie zu **Analytics > Video Insight** und klicken Sie auf **Videoklassifizierung**.

2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.
3. Klicken Sie auf **Go**.

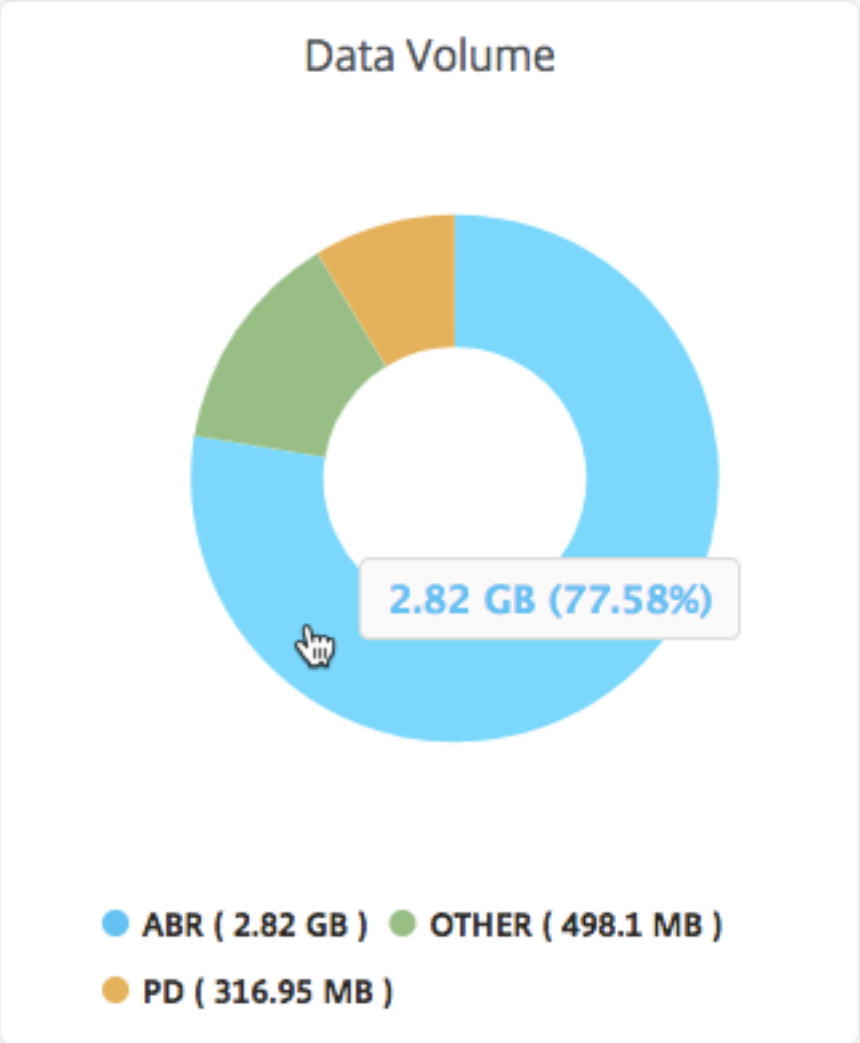
Sie können die Liste **Filter** verwenden, um den HTTP-, HTTPS- oder QUIC-Datenverkehr auszuwählen.



Die Registerkarte **Datenvolumen** enthält ein Liniendiagramm und ein Kreisdiagramm, in dem die Arten des Streamings von Videoverkehr aus Ihrem Netzwerk und das Datenvolumen angezeigt werden, das von Ihrem Netzwerk verbraucht wird. Sie können den Mauszeiger auf das Liniendiagramm bewegen, um die während eines bestimmten Zeitrahmens verbrauchten Daten anzuzeigen:



Außerdem können Sie den Mauszeiger auf das Kreisdiagramm bewegen, um den Prozentsatz des Datenvolumens anzuzeigen, der von einem bestimmten Typ von Videoverkehr verbraucht wird.



Optimierte und nicht optimierte Wiedergabezeit von ABR-Videos vergleichen

February 5, 2024

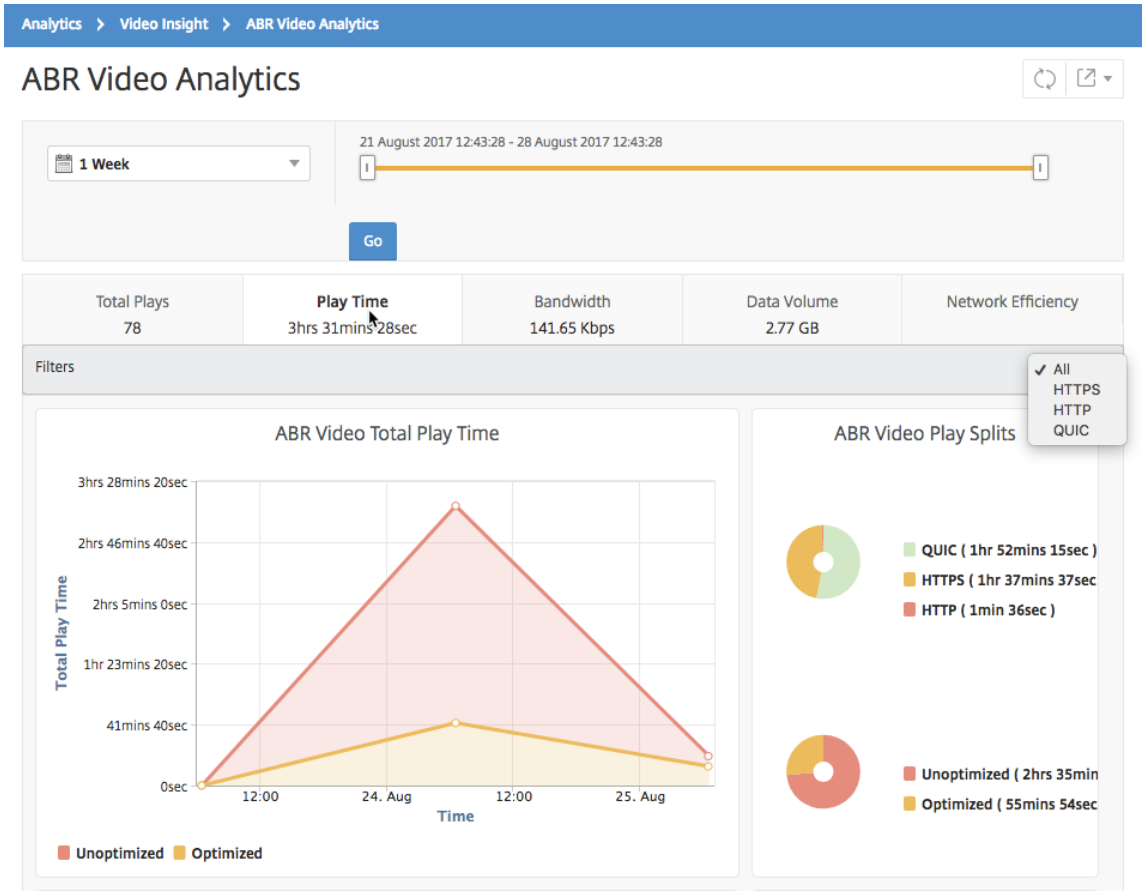
Für einen bestimmten Zeitraum bietet Citrix Application Delivery Management (ADM) die Wiedergabezeit von ABR-Videos und ermöglicht Ihnen außerdem, die Wiedergabezeit optimierter und nicht optimierter ABR-Videos in Ihrem Netzwerk zu vergleichen.

So zeigen Sie die Spielzeit an:

1. Navigieren Sie zu **Analytics > Video Insight** und klicken Sie auf **ABR Video.**
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.

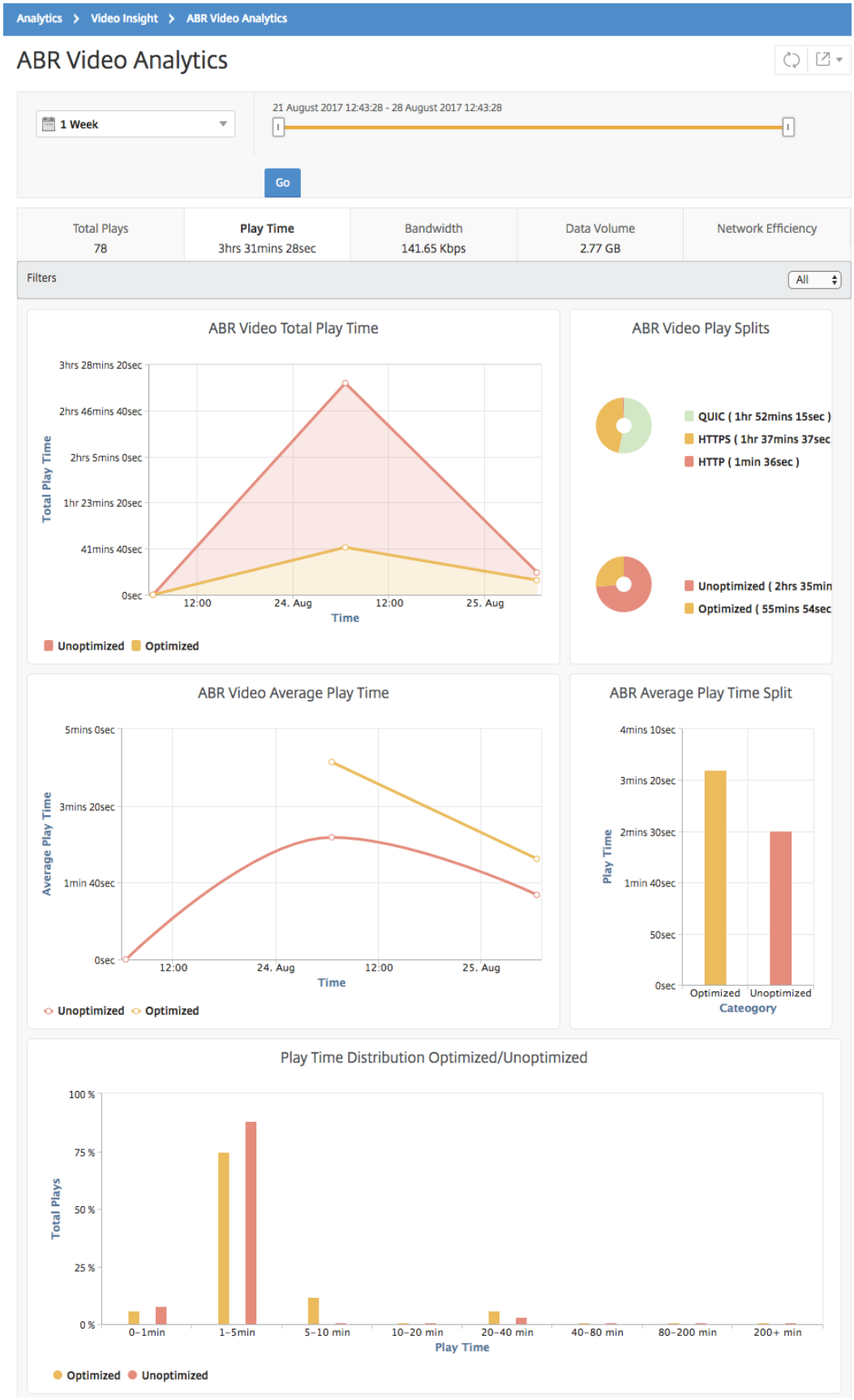
3. Klicken Sie auf **Los** und wählen Sie die Registerkarte **Wiedergabezeit** aus.

   Sie können die Liste **Filter** verwenden, um die HTTP-, HTTPS- oder QUIC-ABR-Videos auszuwählen.



Für den ausgewählten Zeitraum enthält die Registerkarte **Wiedergabezeit** ein Liniendiagramm und ein Kreisdiagramm, in dem Folgendes beschrieben wird:

- Gesamte Wiedergabezeit von ABR-Videos aus Ihrem Netzwerk
- Gesamtwiedergabezeit optimierter und nicht optimierter Wiedergaben von ABR-Videos aus Ihrem Netzwerk für den ausgewählten Zeitraum
- Gesamtspielzeit von verschlüsselten und unverschlüsselten ABR-Videos
- Durchschnittliche Wiedergabezeit von ABR-Videos
- Durchschnittliche Wiedergabezeit optimierter und nicht optimierter Wiedergaben von ABR-Videos
- Durchschnittliche Wiedergabezeit von verschlüsselten und unverschlüsselten ABR-Videos
- Wiedergabe der Zeitverteilung zwischen optimierten und nicht optimierten ABR-Videos



Bandbreitenverbrauch optimierter und nicht optimierter ABR-Videos vergleichen

February 5, 2024

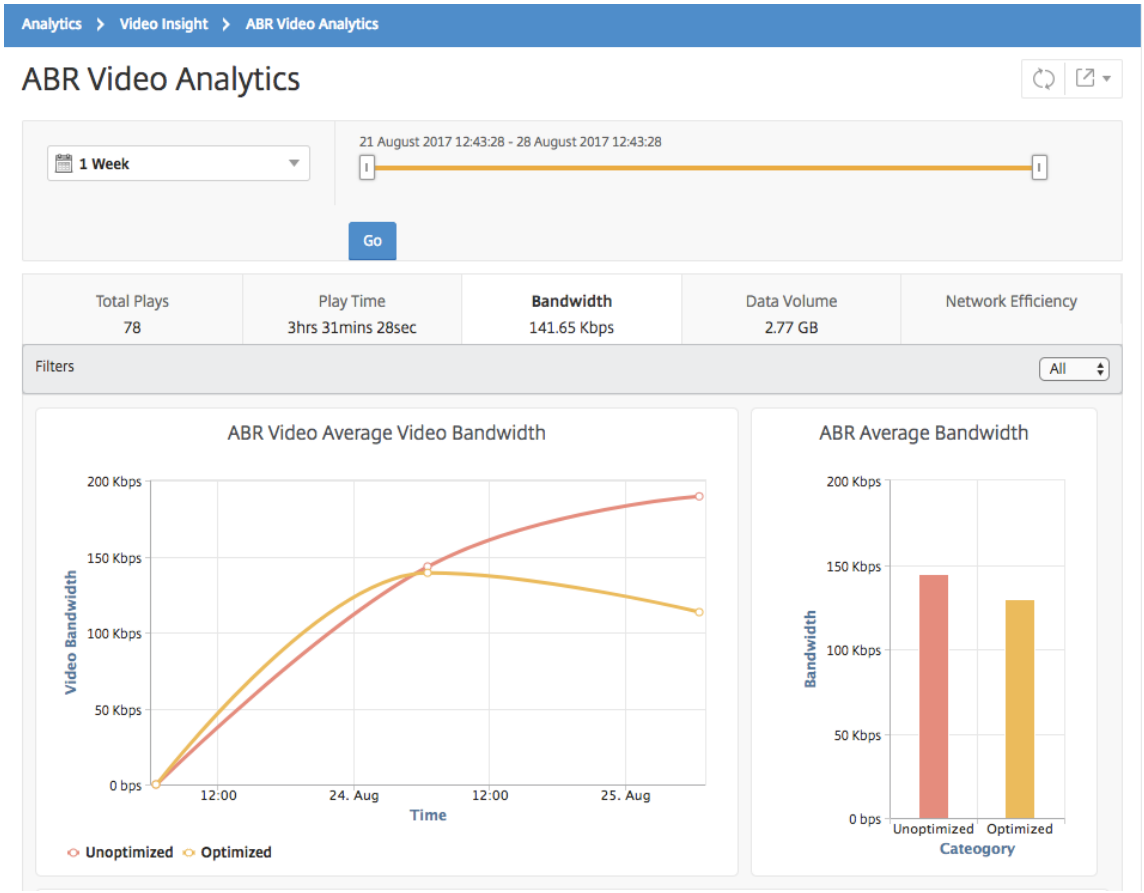
Für einen bestimmten Zeitraum bietet NetScaler Application Delivery Management (ADM) die Bandbreite, die von optimierten und nicht optimierten ABR-Videos verbraucht wird, und ermöglicht es Ihnen auch, die Bandbreite zu vergleichen, die von optimierten und nicht optimierten ABR-Videos in Ihrem Netzwerk verbraucht wird, basierend auf:

- Spielzeit
- Datenvolume

Um den Bandbreitenverbrauch anzuzeigen:

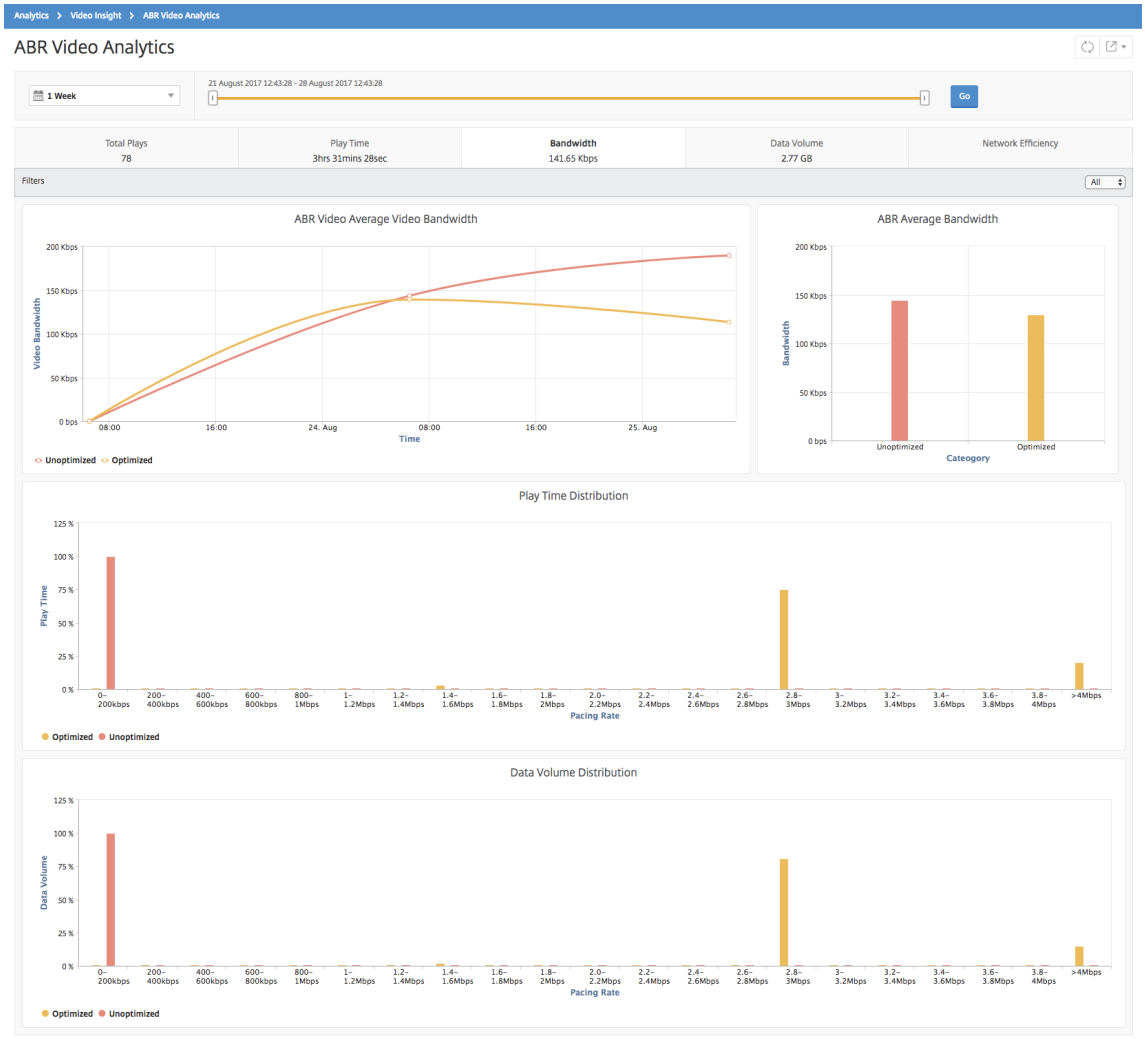
1. Navigieren Sie zu **Analytics > Video Insight** und klicken Sie auf **ABR Video Analytics**.
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.
3. Klicken Sie auf **Los** und wählen Sie die Registerkarte **Bandbreite** aus.

   Sie können die HTTP-, HTTPS- oder QUIC-ABR-Videos in der Liste **Filter** auswählen.



Für den ausgewählten Zeitraum enthält die Registerkarte **Bandbreite** ein Liniendiagramm und ein Kreisdiagramm, in dem Folgendes beschrieben wird:

- Durchschnittliche Bandbreite, die von optimierten und nicht optimierten ABR-Videos verbraucht wird.
- Die verbrauchte Bandbreite basiert auf der Verteilung der Wiedergabezeit zwischen optimierten und nicht optimierten ABR-Videos.
- Bandbreitenverbrauch basierend auf dem Datenvolumen, das zwischen optimierten und nicht optimierten ABR-Videos verteilt wird.



Optimierte und nicht optimierte Wiedergabezahlen von ABR-Videos vergleichen

February 5, 2024

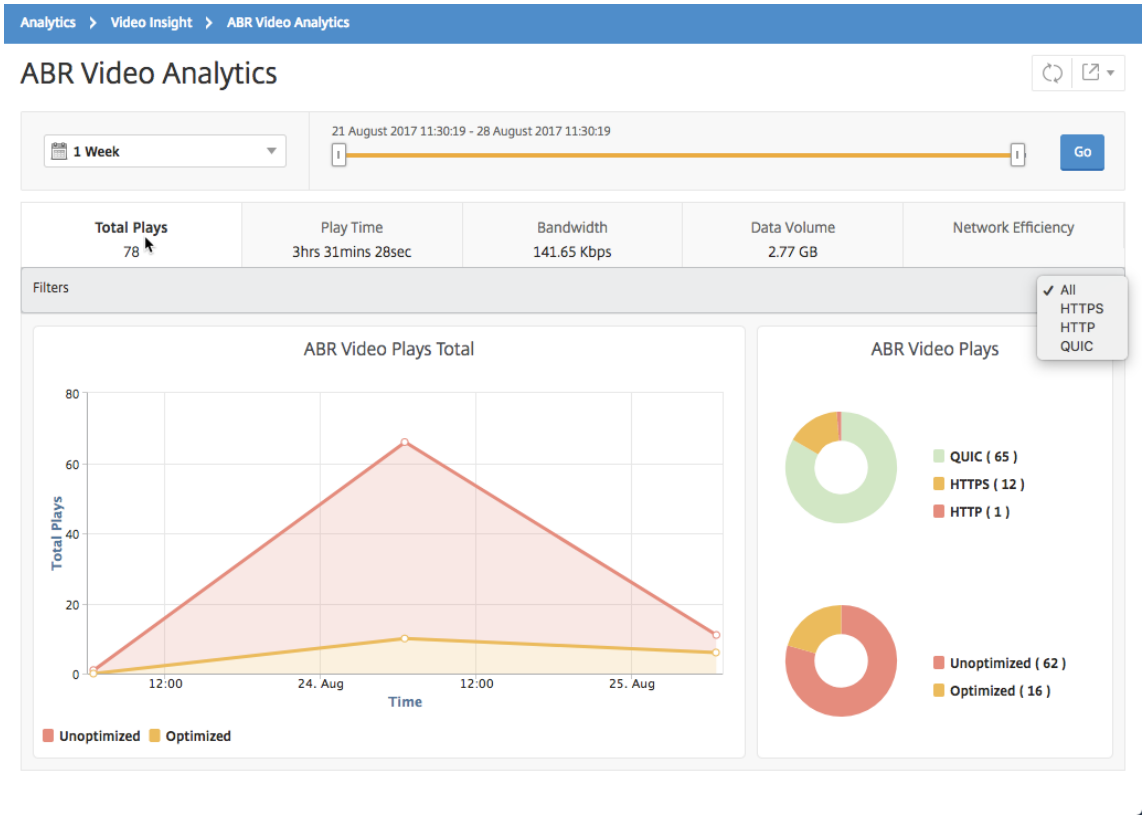
Für einen bestimmten Zeitraum zeigt NetScaler Application Delivery Management (ADM) die Anzahl der Abspielungen von ABR-Videos an und ermöglicht es Ihnen, die Anzahl der optimierten und nicht optimierten Wiedergaben in Ihrem Netzwerk zu vergleichen.

Um die Anzahl der Spiele zu sehen:

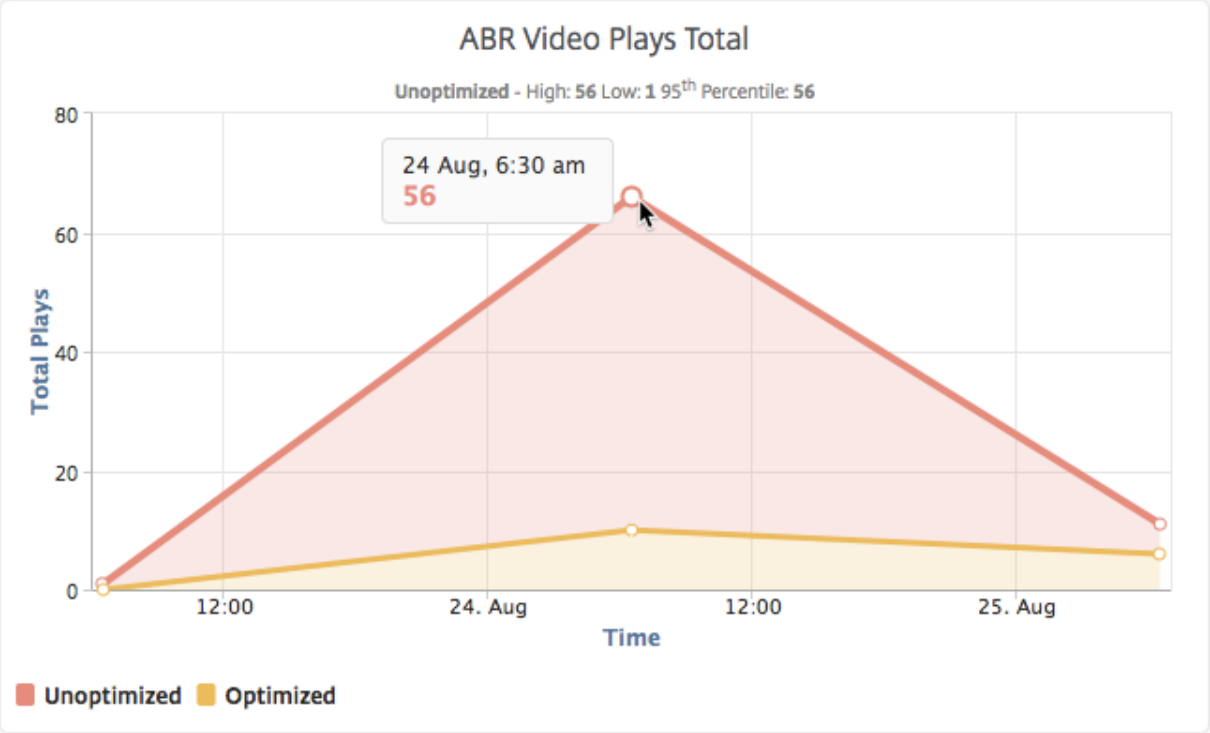
1. Navigieren Sie zu **Analytics > Video Insight**und klicken Sie auf **ABR Video Analytics**.
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.

3. Klicken Sie auf **Los** und wählen Sie die Registerkarte **Anzahl der Wiedergaben**.

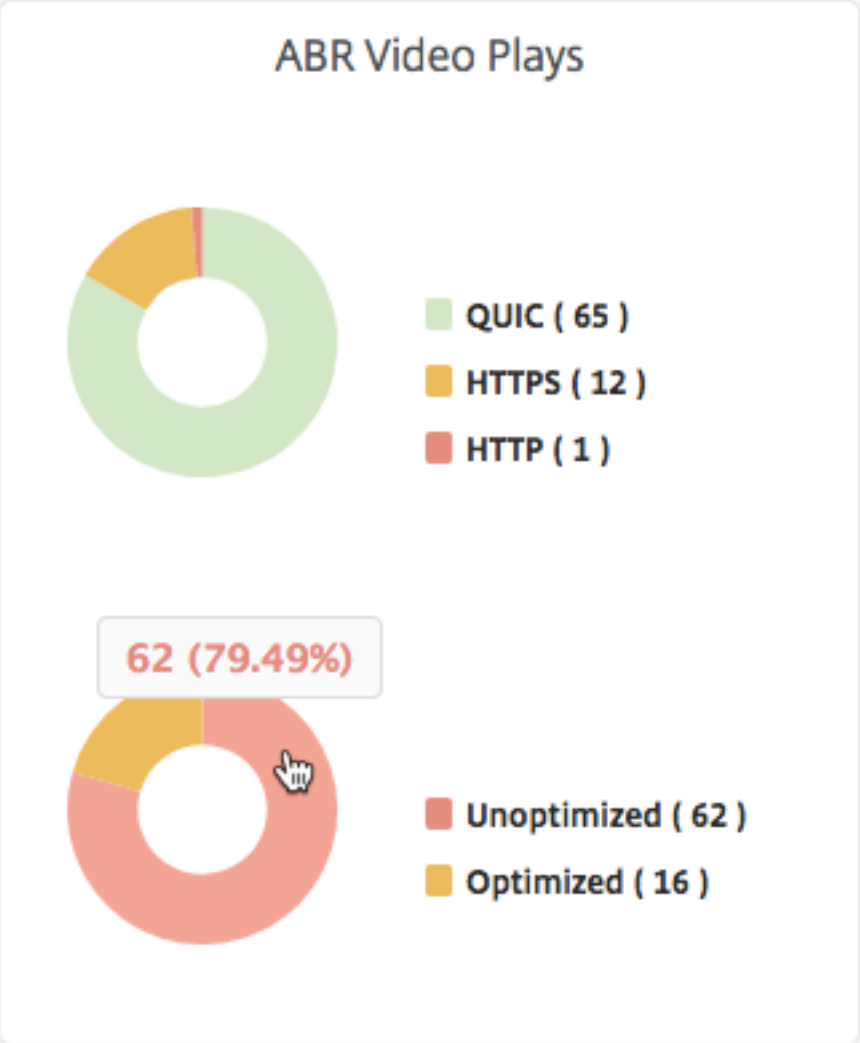
   Sie können die Liste **Filter** verwenden, um die HTTP-, HTTPS- oder QUIC-ABR-Videos auszuwählen.



Die Registerkarte **Anzahl der Wiedergaben** enthält ein Liniendiagramm und ein Kreisdiagramm, das die Anzahl der Wiedergaben von ABR-Videos aus Ihrem Netzwerk sowie die Anzahl der optimierten und nicht optimierten Wiedergaben von ABR-Videos aus Ihrem Netzwerk für den ausgewählten Zeitraum beschreibt. Sie können den Mauszeiger auf das Liniendiagramm bewegen, um die Anzahl der Wiedergaben während eines bestimmten Zeitrahmens anzuzeigen:



Außerdem können Sie den Mauszeiger auf das Kreisdiagramm bewegen, um den Prozentsatz der optimierten und nicht optimierten Wiedergaben und den Prozentsatz der verschlüsselten und unverschlüsselten ABR-Videos für den ausgewählten Zeitraum anzuzeigen.



Spitzendatenrate für einen bestimmten Zeitraum anzeigen

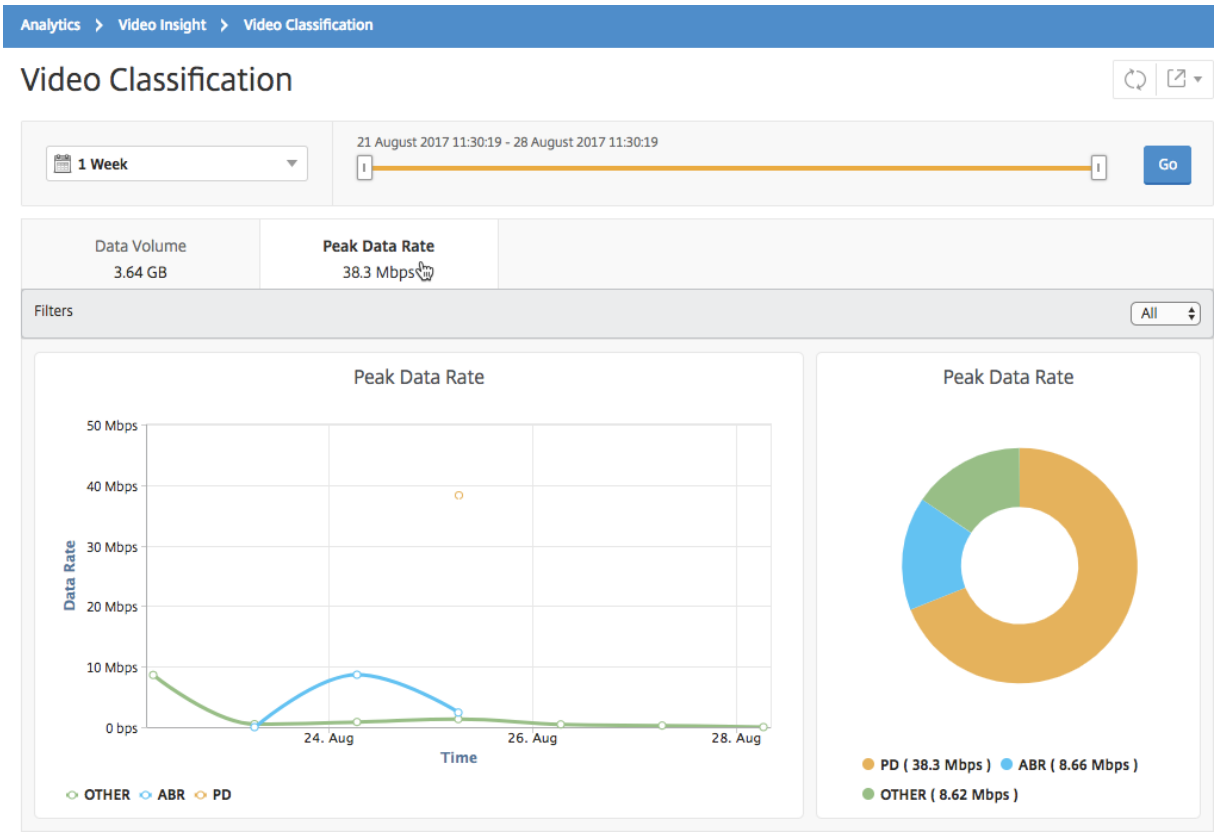
February 5, 2024

NetScaler Application Delivery Management (ADM) zeigt den Spitzendurchsatz oder die Datenrate des Videodatenverkehrs in Ihrem Netzwerk an.

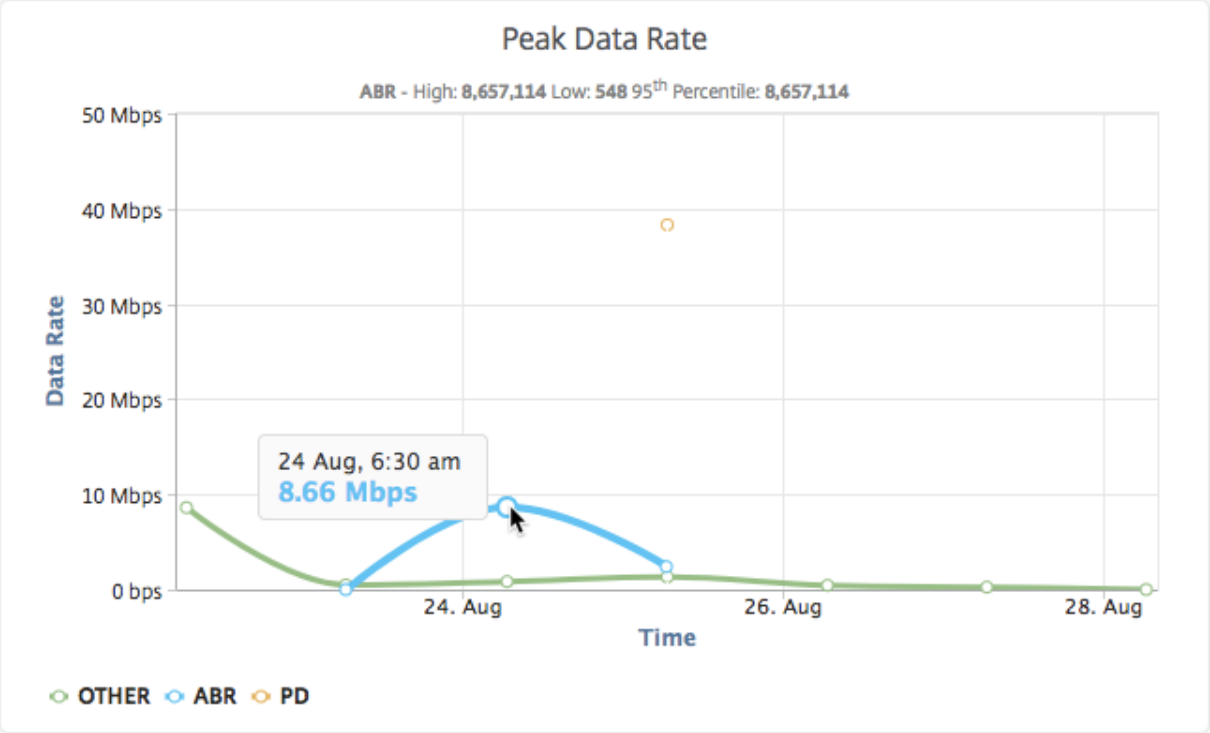
So sehen Sie die Spitzendatenrate des Videoverkehrs:

1. Navigieren Sie zu **Analytics > Video Insight**und klicken Sie auf **Videoklassifizierung**.
2. Wählen Sie im rechten Fensterbereich einen Zeitrahmen aus der Liste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden.
3. Klicken Sie auf **Los**, und wählen Sie die Registerkarte **Spitzendatenrate** aus.

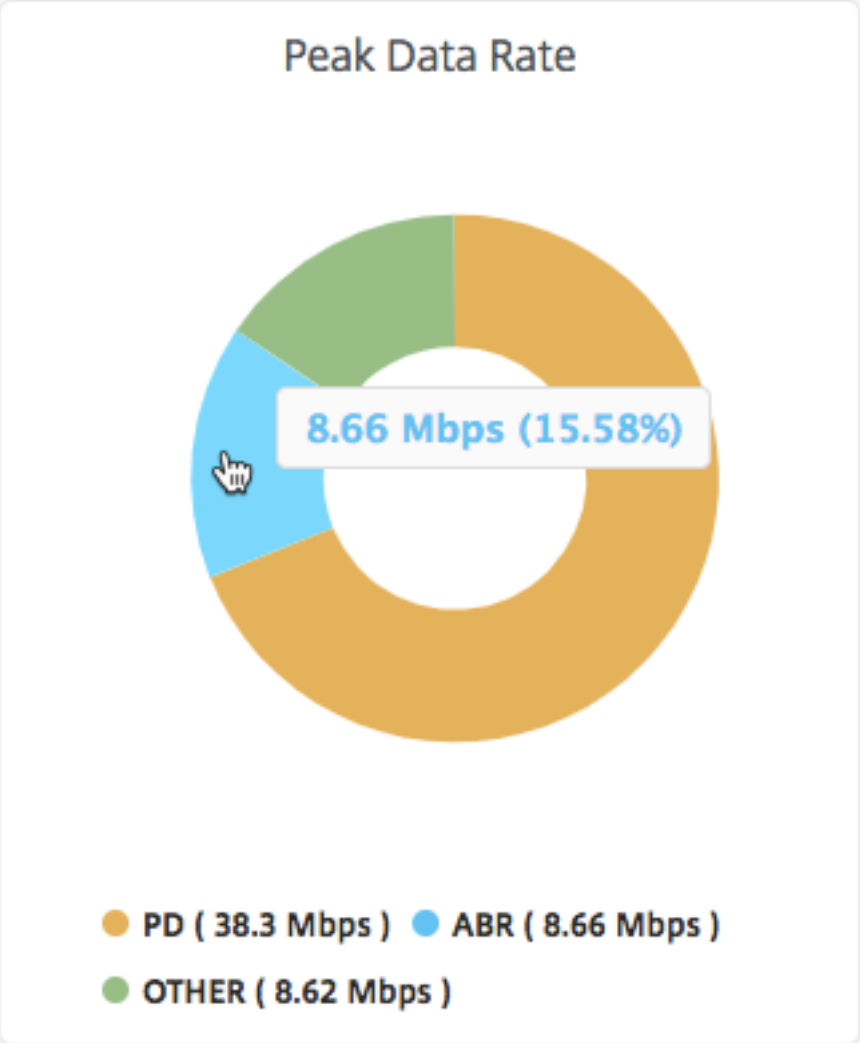
Sie können die Liste **Filter** verwenden, um den HTTP-, HTTPS- oder QUIC-Datenverkehr auszuwählen.



Die Registerkarte **Spitzendatenrate** enthält ein Liniendiagramm und ein Kreisdiagramm, das die Spitzendatenrate des vom Netzwerk ausgehenden Videodatenverkehrs und die Spitzendatenrate des Videodatenverkehrs im Netzwerk während des ausgewählten Zeitrahmens beschreibt. Sie können den Mauszeiger auf das Liniendiagramm bewegen, um die Spitzendatenrate während eines bestimmten Zeitrahmens anzuzeigen.



Außerdem können Sie den Mauszeiger auf das Kreisdiagramm bewegen, um den Prozentsatz der Spitzendatenrate anzuzeigen, die vom Typ des während des ausgewählten Zeitrahmens gestreamten Videoverkehrs verbraucht wird.



SSL-Forward-Proxyanalyse

February 5, 2024

Eine NetScaler ADC Appliance am Rand des Unternehmensnetzwerks fungiert als Internet-Proxy. Die Appliance kann im transparenten Proxy-Modus oder im expliziten Proxymodus betrieben werden und bietet Steuerelemente zum Abfangen des Internetverkehrs, einschließlich HTTPS. Die Entscheidung, Anfragen abzufangen, zu Bypass oder zu blockieren, wird auf der Grundlage der auf der Appliance konfigurierten Richtlinien getroffen. Ein Benutzer wird authentifiziert, bevor er sich am Unternehmensnetzwerk anmeldet. Alle Anfragen und Antworten werden mit dem Benutzer gekennzeichnet, und die Benutzeraktivitäten werden in der Appliance protokolliert. Weitere Informationen finden Sie unter Citrix SSL Forward Proxy .

Wenn Sie NetScaler Application Delivery Management (ADM) in eine NetScaler ADC Appliance inte-

grieren, werden die protokollierten Benutzeraktivitäten und die nachfolgenden Datensätze auf der Appliance mithilfe von Logstream in NetScaler ADM exportiert. NetScaler ADM stellt Informationen über die Aktivitäten der Nutzer zusammen, z. B. besuchte Websites und die verbrauchte Bandbreite. Es meldet auch die Bandbreitennutzung und erkannte Bedrohungen wie Malware und Phishing-Sites. Sie können diese Schlüsselmetriken verwenden, um Ihr Netzwerk zu überwachen und Korrekturmaßnahmen mit der NetScaler ADC Appliance durchzuführen.

So integrieren Sie eine NetScaler ADC Appliance mit NetScaler ADM:

1. Aktivieren Sie auf der NetScaler ADC Appliance beim Konfigurieren des SSL Forward Proxy **Analytics** und geben Sie die Details der NetScaler ADM-Instanz an, die Sie für Analysen verwenden möchten.
2. Fügen Sie in NetScaler ADM die NetScaler ADC-Appliance als Instanz zu NetScaler ADM hinzu. Weitere Informationen finden Sie unter Instanzen zu NetScaler ADM hinzufügen.

Dashboards

February 5, 2024

NetScaler Application Delivery Management (ADM) bietet zwei Dashboards, das **Dashboard für ausgehenden Datenverkehr** und das **Benutzerdashboard**. Diese Dashboards zeigen mehrere Diagramme an, in denen die Websites oder Anwendungen zusammengefasst werden, auf die aus dem Unternehmensnetzwerk zugegriffen wird, sowie die Aktivitäten, die von den Benutzern im Netzwerk ausgeführt werden.

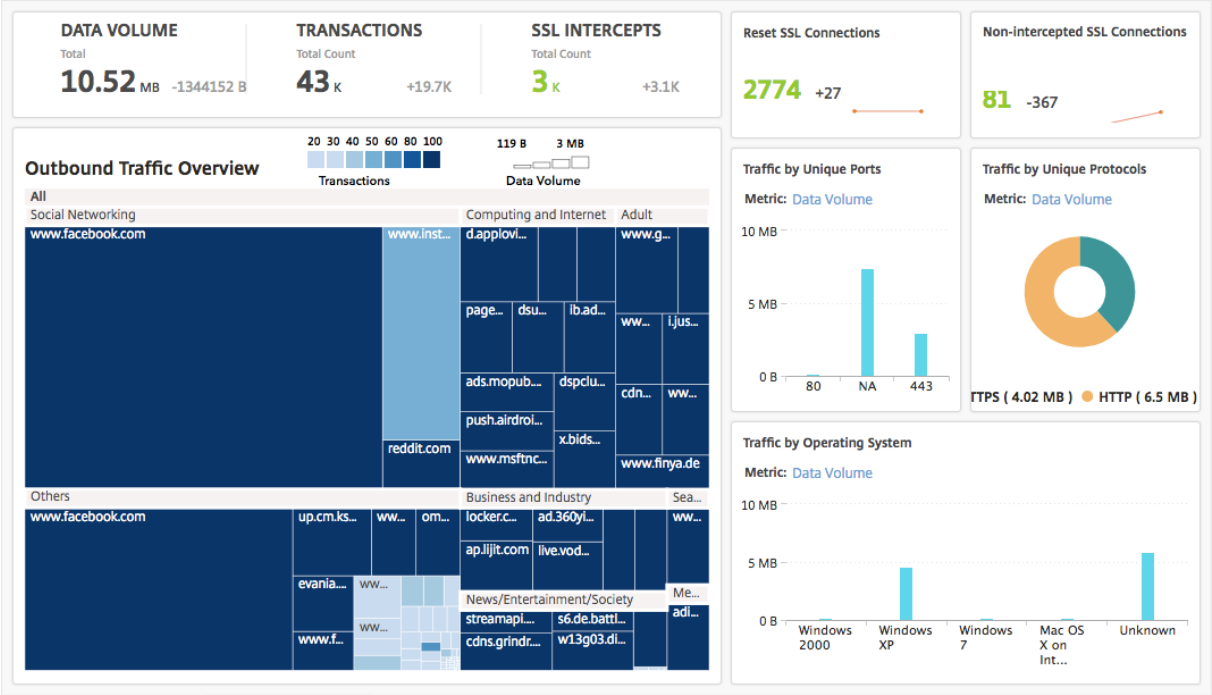
Dashboard für ausgehenden Datenverkehr

Das **Dashboard für ausgehenden Datenverkehr** enthält eine Zusammenfassung der URLs oder Domänen, auf die von Ihrem Netzwerk zugegriffen wird. Es bietet eine ganzheitliche Ansicht aller URLs oder Domänen nach Anzahl der Transaktionen oder Datenvolumen, die von den URLs oder Domains verbraucht werden.
Es enthält auch Details wie die folgenden:

1. Menge an Bandbreite, die von den URLs oder Domänen verbraucht wird, auf die über Ihr Netzwerk zugegriffen wird
2. Anzahl der Transaktionen, die beim Zugriff auf die URLs und Domänen aus Ihrem Netzwerk aufgetreten sind.
3. Anzahl der SSL-Verbindungen, die von der NetScaler ADC Appliance während der Transaktionen abgefangen wurden.

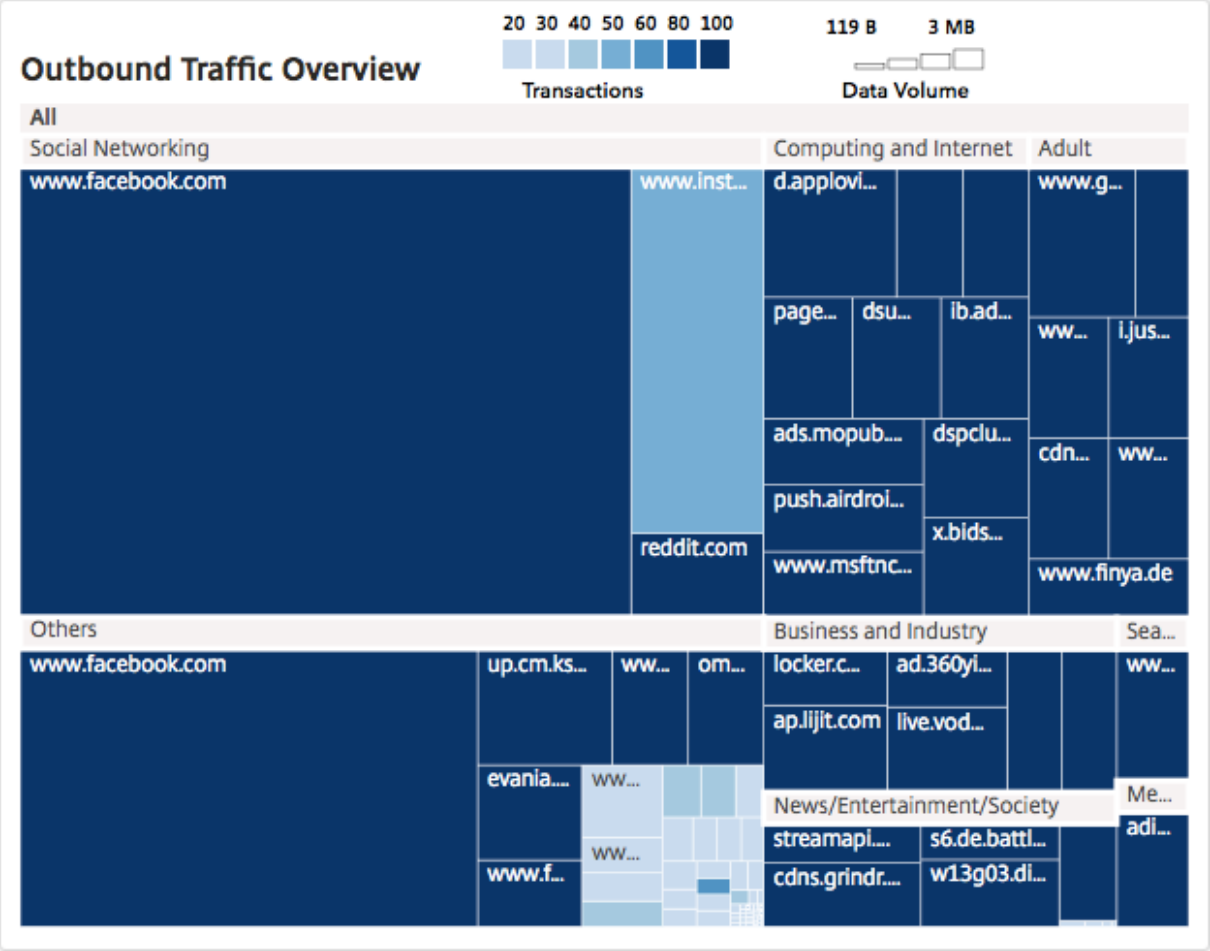
4. Anzahl der SSL-Verbindungen, die während der Transaktionen nicht von der NetScaler ADC Appliance abgefangen wurden.
5. Anzahl der SSL-Verbindungen, die von der NetScaler ADC Appliance während der Transaktionen zurückgesetzt wurden.
6. Umfang des übertragenen Webverkehrs, basierend auf dem für die Übertragung des Datenverkehrs verwendeten Port, dem Protokoll, das vom Webdatenverkehr verwendet wird, und den Client-Betriebssystemen, die für die Übertragung des Datenverkehrs verwendet werden.

Um auf das Dashboard für ausgehenden Datenverkehr zuzugreifen, navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**.



Anzeigen des ausgehenden Datenverkehrs aus dem Netzwerk

Das **Dashboard für ausgehenden Datenverkehr** enthält einen Bereich **Übersicht über den ausgehenden Datenverkehr**. Im Bereich **Übersicht über ausgehenden Datenverkehr** gruppiert NetScaler ADM die URLs oder Domänen, auf die zugegriffen wurde, in Kategorien wie Einkaufen, Nachrichten, Soziale Netzwerke usw. Im Bereich **Übersicht über ausgehenden Datenverkehr** werden die URLs oder Domänen, auf die über Ihr Netzwerk zugegriffen wird, als Knoten in den URL-Kategorien angezeigt Die Größe der Knoten richtet sich nach dem Datenvolumen, das durch den Zugriff auf die URL oder Domäne verbraucht wird. Die Farbe des Knotens gibt die Anzahl der Transaktionen an, die beim Zugriff auf die URL oder Domäne aufgetreten sind.



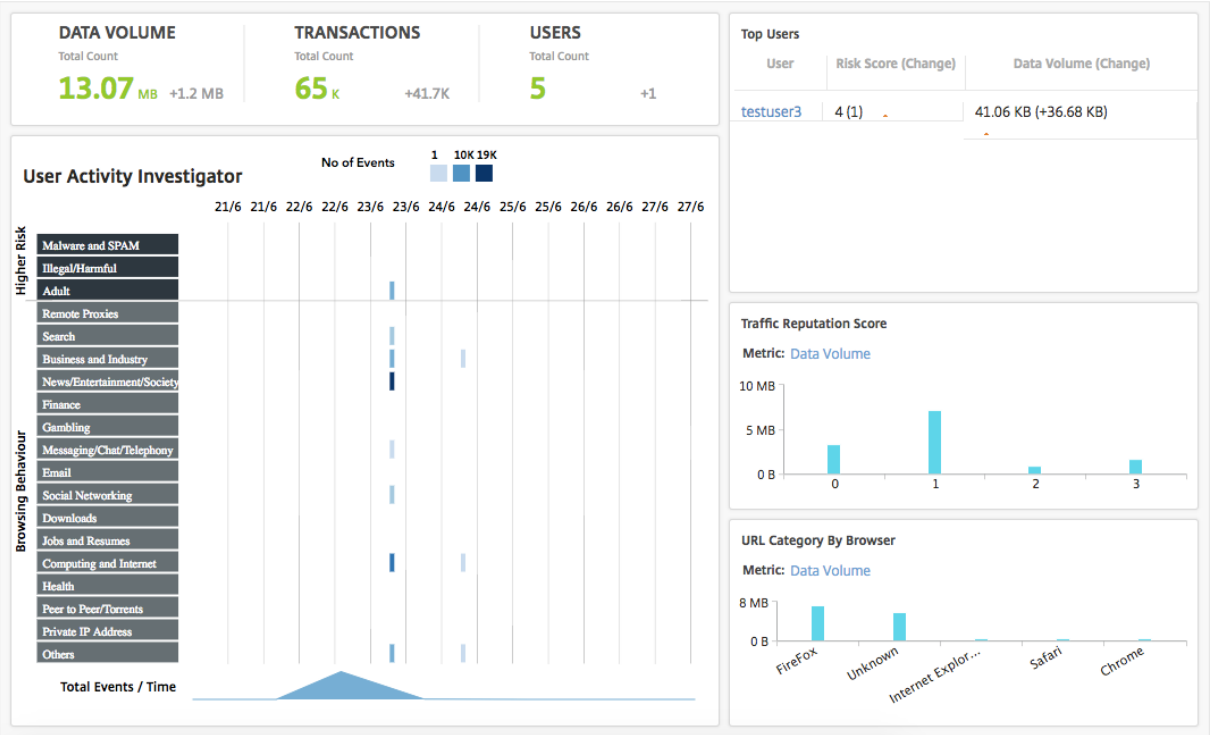
Sie können auf eine Kategorie klicken, um die Diagramme zu filtern, um Details zu der Kategorie für den angegebenen Zeitraum anzuzeigen.

Benutzerdashboard

Das **Benutzerdashboard** zeigt eine Zusammenfassung der Aktivitäten an, die von den Benutzern in Ihrem Unternehmen ausgeführt werden. Es enthält wichtige Metriken, anhand derer Sie Folgendes ermitteln können:

1. Das Surfverhalten der Benutzer in Ihrem Unternehmen.
2. URL-Kategorien, auf die die Benutzer in Ihrem Unternehmen zugreifen.
3. Die fünf besten Benutzer, basierend auf ihren Risikobewertungen und der Bandbreite, die sie verbrauchen. Weitere Informationen zur Risikobewertung finden Sie unter Risikobewertung.
4. Browser, mit denen auf die URLs oder Domains zugegriffen wurde.
5. Menge des von den Benutzern erzeugten Web-Traffic basierend auf dem Traffic-Reputation Score.

Um auf das **Benutzer-Dashboard**zuzugreifen, navigieren Sie zu **Benutzer > Dashboard**.

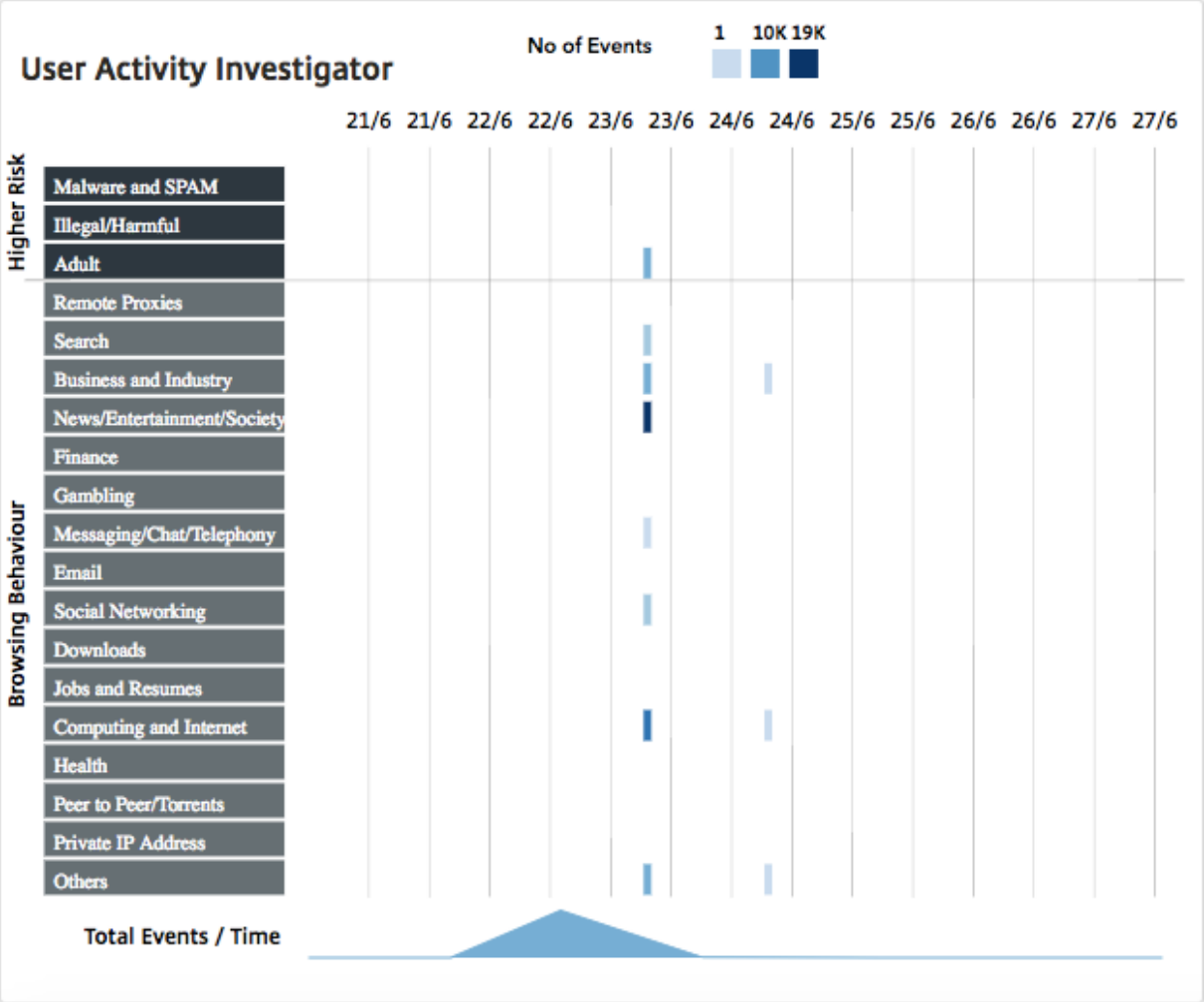


Sie können im Bereich **Top Benutzer auf einen Benutzer** klicken, um die Diagramme zu filtern, um Details der Webaktivität anzuzeigen, die der Benutzer im angegebenen Zeitraum ausgeführt hat.

Ermittler der Benutzeraktivität

Das **Benutzer-Dashboard** enthält einen Bereich **Ermittlungsprogramm**, in dem verschiedene Webaktivitäten angezeigt werden, die von den Benutzern ausgeführt werden. Es zeigt die URL-Kategorien, auf die die Benutzer während des ausgewählten Zeitrahmens zugreifen, und verschiedene Ereignisse, die pro URL-Kategorie ausgelöst werden. Sie können auf die Ereignisse klicken, um Details zur Transaktionsebene abzurufen.

Der **User Activity Investigator** zeigt wichtige Informationen wie das Browserverhalten des Benutzers, die Aktivität mit hohem Risiko des Benutzers und die ausgelösten Ereignisse pro URL-Kategorie an. Die Ereignisse werden in der Tabelle als rechteckige Legenden dargestellt. Jede der Legenden wird in Intervallen von einer Minute aggregiert, wenn die gewählte Dauer eine Stunde beträgt, und in 1-Stunden-Intervallen, wenn die ausgewählte Dauer einen Tag beträgt.



Diese Legenden werden aggregiert und werden entsprechend der Anzahl der aufgetretenen Ereignisse farbcodiert. Sie können den Mauszeiger auf eine Legende bewegen, um Details wie die Zeit und die Anzahl der Ereignisse anzuzeigen, die für die ausgewählte Legende aggregiert wurden. Sie können den Zeitraum des Diagramms anpassen, indem Sie eine Zeit aus der Zeitperiodenliste auswählen.

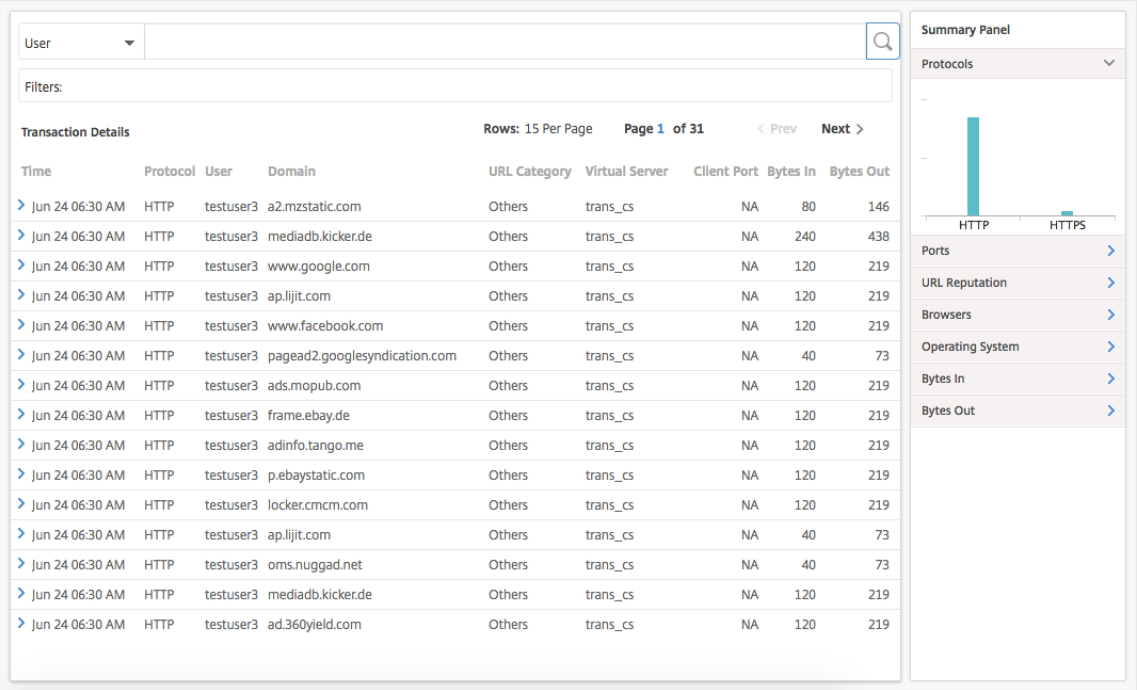
Sie können auf die Ereignisse klicken, um einen weiteren Drilldown für die Details der Transaktionen durchzuführen.

Benutzer-Transaktionen

Auf der Seite Benutzertransaktionen werden die Details der Benutzertransaktionen in Ihrem Netzwerk angezeigt. Es bietet Details auf Transaktionsebene wie:

1. Zeitpunkt, zu dem die Transaktion stattgefunden hat
2. Für die Transaktion verwendetes Protokoll
3. Benutzername

4. Domain, auf die der Benutzer zugreift
5. URL-Kategorie
6. Proxyserver, der zum Abfangen der Transaktion verwendet wurde
7. Details zum Client-Port
8. Bytes In
9. Bytes aus



Übersichtsfenster Im **Zusammenfassungsbereich** werden alle Metriken der Transaktionen angezeigt, die im Bereich **Transaktionsdetails** sichtbar sind. In diesem Bereich können Sie die Transaktionen im Bereich **Transaktionsdetails** sortieren und anzeigen, indem Sie die Metriken auswählen oder deren Auswahl aufheben. Im **Zusammenfassungsbereich** werden die folgenden Metriken angezeigt:

Metriken	Beschreibung
Protokolle	In den Transaktionen verwendete Protokolle
Ports	Für die Transaktionen verwendete Ports
URL-Ruf	URL-Reputationsbewertung
Browser	Für die Transaktionen verwendete Browser

Metriken	Beschreibung
Betriebssystem	Für die Transaktionen verwendetes Betriebssystem
Bytes In	Menge der über die Citrix ADC Appliance empfangenen Daten.
Bytes aus	Datenmenge, die über die Citrix ADC Appliance gesendet wird.

Risiko-Score

Risk Score ist ein Bewertungssystem, das in NetScaler ADM verwendet wird, um die Risiken zu ermitteln, die mit Benutzern in Ihrem Unternehmen verbunden sind. NetScaler ADM weist eine Risikobewertung auf der Grundlage der URL-Reputationsbewertung zu, die von der NetScaler ADC Appliance für die URLs zugewiesen wurde, auf die die Benutzer im Netzwerk zugreifen. Informationen zum URL-Reputationswert finden Sie unter URL-Reputationsbewertung In der folgenden Tabelle werden die von NetScaler ADM zugewiesenen Risikobewertungen beschrieben.

Risikobewertung	Beschreibung
1	Die Webaktivität des Benutzers hat keine wahrgenommene Bedrohung oder ist nicht ungewöhnlich.
2	Die Webaktivität des Benutzers wird nicht als Bedrohung wahrgenommen oder ist nicht ungewöhnlich, aber der Benutzer greift auf “Unbekannte Websites”zu, für die keine URL-Reputationswerte vorliegen.
3	In der Webaktivität des Benutzers wird keine Bedrohung erkannt, aber der Benutzer hat versucht, auf Websites zuzugreifen, die potenziell anfällig sind oder mit Websites verbunden sind, die potenziell anfällig sind.
4	Potenziell gefährdeter Benutzer.
5	Die Web-Aktivität des Benutzers ist abnormal und der Benutzer hat auf bekannte bösartige Websites zugegriffen.

Anwendungsfälle

February 5, 2024

Überwachung des SSL-Abfanges

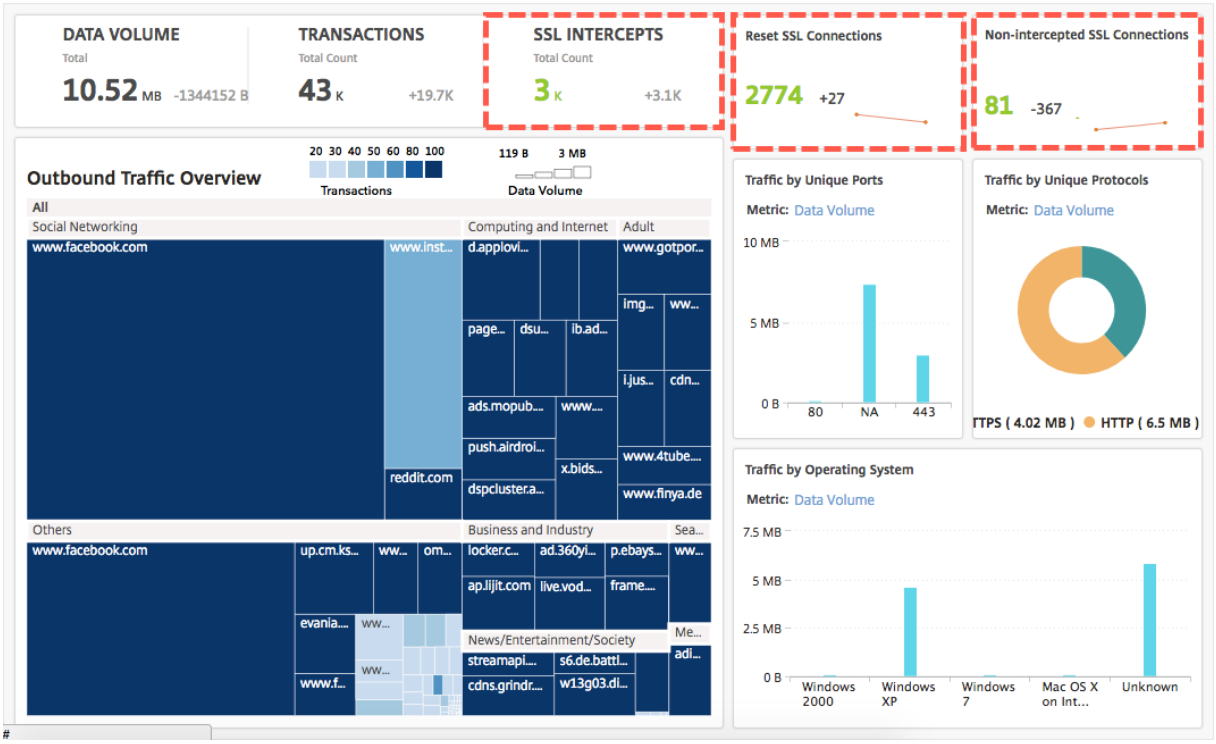
Mit einer NetScaler ADC Appliance können Sie Ihren verschlüsselten ausgehenden Datenverkehr überprüfen. Sie können alle HTTPS-Anforderungen basierend auf den auf der Appliance konfigurierten Richtlinien abfangen, Bypass oder blockieren. NetScaler Application Delivery Management (ADM) enthält die folgenden Details zu den SSL-Verbindungen im **Dashboard für ausgehenden Datenverkehr** für einen ausgewählten Zeitraum:

- Anzahl der SSL-Verbindungen, die von der NetScaler ADC Appliance abgefangen, nicht abgefangen und zurückgesetzt werden
- Transaktionsdetails der SSL-Verbindungen

Anhand dieser Details können Sie die Richtlinien auf Ihrer NetScaler ADC Appliance weiter optimieren, um den verschlüsselten ausgehenden Datenverkehr effizient zu überprüfen. Weitere Informationen finden Sie unter Citrix SSL Forward Proxy.

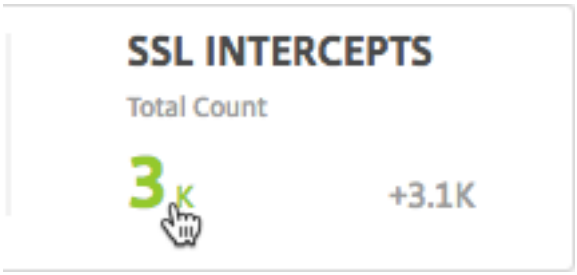
So zeigen Sie die Anzahl der SSL-Verbindungen an, die abgefangen, nicht abgefangen und zurückgesetzt wurden:

Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**.Das Outboard Traffic Dashboard zeigt die Anzahl der SSL-Verbindungen an, die abgefangen, nicht abgefangen und zurückgesetzt werden.

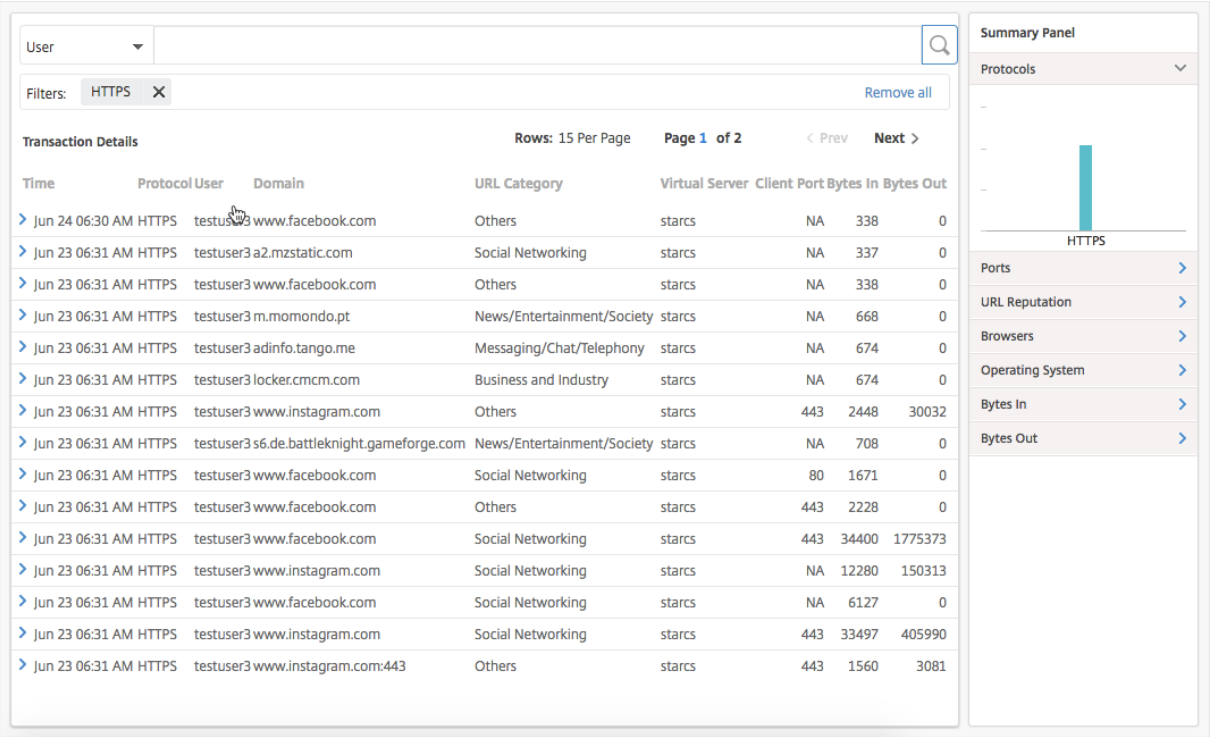


So zeigen Sie die Transaktionsdetails der abgefangenen SSL-Verbindungen an:

1. Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**.
2. Klicken Sie im **Dashboard des Außenbordverkehrs**auf die Gesamtanzahl im Abschnitt **SSL-INTERCEPTS**.



Die Transaktionsdetails der SSL-Verbindungen, die während des ausgewählten Zeitrahmens abgefangen wurden, werden auf der Seite **Transaktionsdetails** angezeigt.

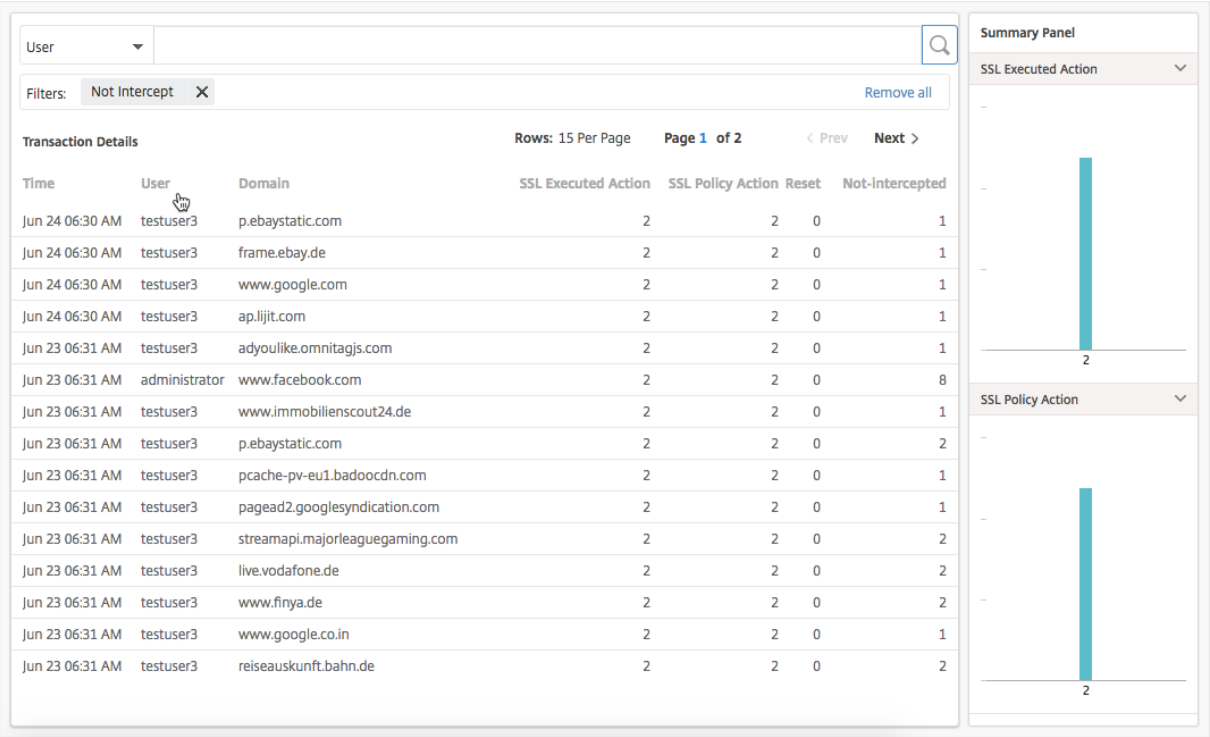


Sie können die Transaktionsdetails weiter nach Benutzer und URL-Kategorie filtern.

So zeigen Sie die Transaktionsdetails der SSL-Verbindungen an, bei denen der Datenverkehr nicht abgefangen wurde:

1. Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**.
2. Klicken Sie im **Dashboard für Außenbordverkehr**im Abschnitt **Nicht-abgefangene SSL-Verbindungen** auf die Gesamtanzahl.

Die Transaktionsdetails der SSL-Verbindungen, für die der Datenverkehr während des ausgewählten Zeitraums nicht abgefangen wurde, werden auf der Seite **Transaktionsdetails** angezeigt.

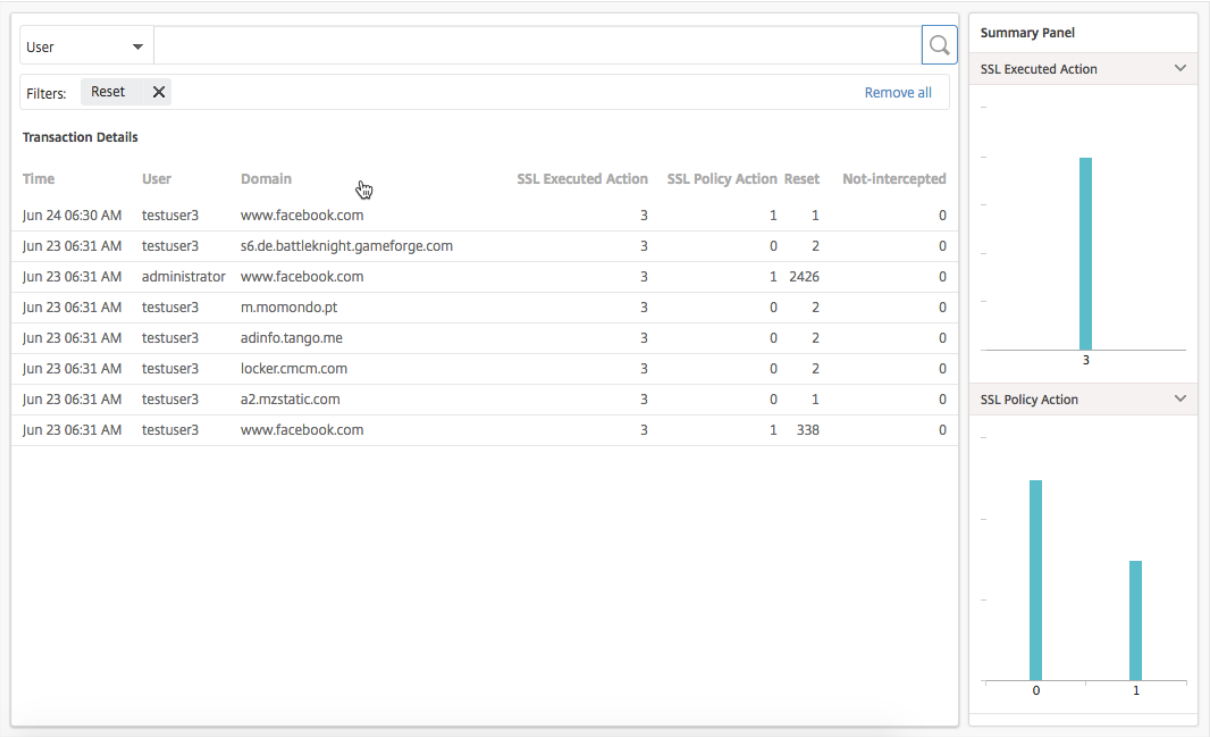


Sie können die Transaktionsdetails weiter nach Benutzer und URL-Kategorie filtern.

So zeigen Sie die Transaktionsdetails der zurückgesetzten SSL-Verbindungen an:

1. Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**.
2. Klicken Sie im **Dashboard für Außenbordverkehr**im Abschnitt **SSL-Verbindungen zurücksetzen**auf die Gesamtanzahl.

Die Transaktionsdetails der SSL-Verbindungen, für die der Datenverkehr während des ausgewählten Zeitraums nicht abgefangen wurde, werden auf der Seite **Transaktionsdetails** angezeigt.



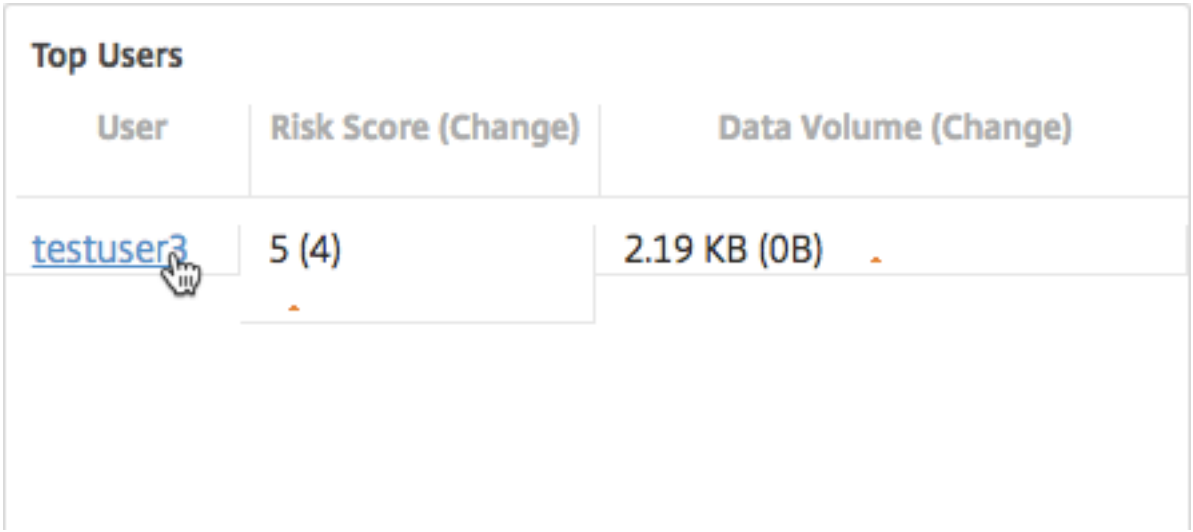
Sie können die Transaktionsdetails weiter nach Benutzer und URL-Kategorie filtern.

Inspektion von Endpunkten

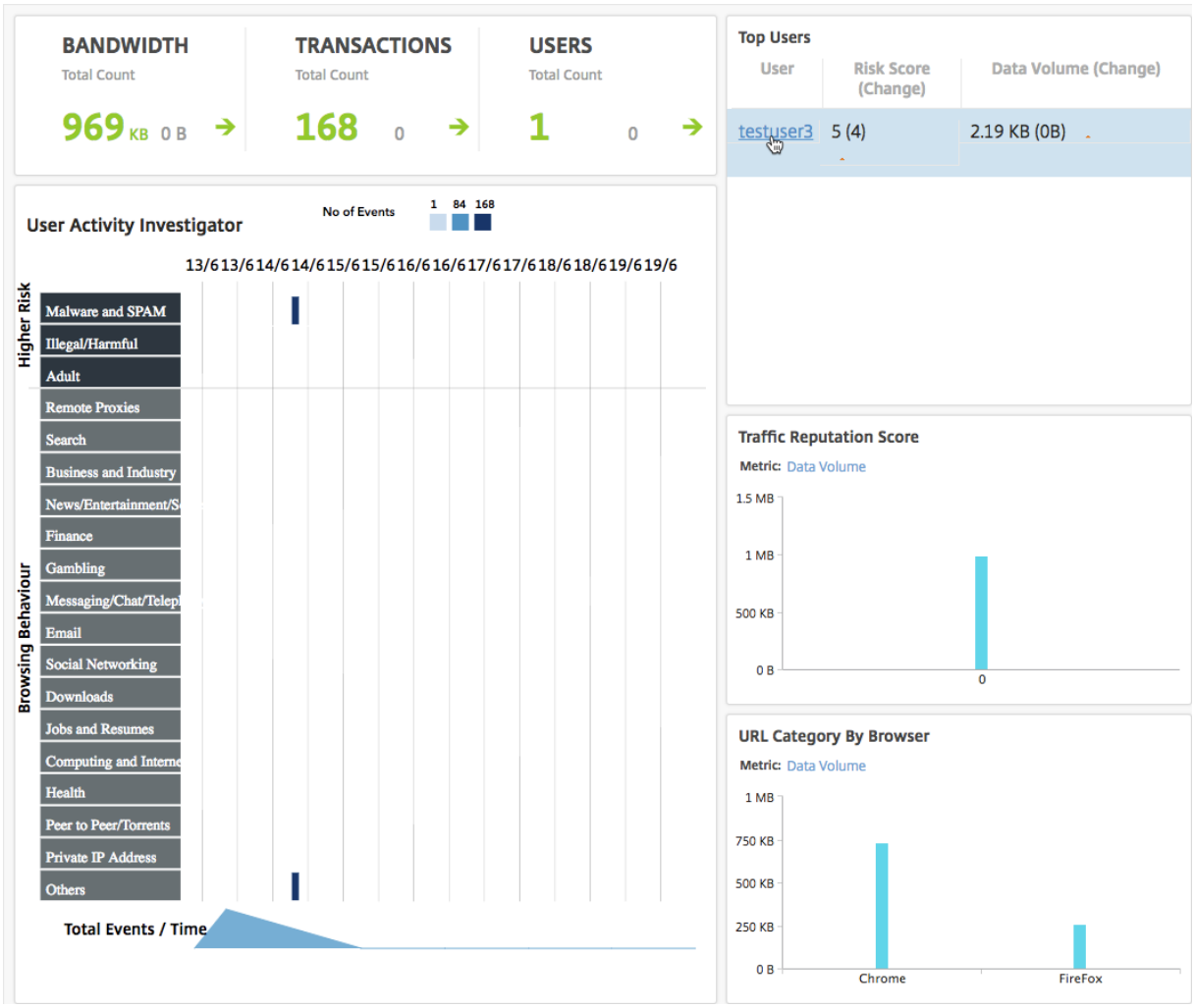
Die Richtlinien, die Sie auf einer NetScaler ADC Appliance konfiguriert haben, geben an, wie die Appliance alle in Ihrem Unternehmen ausgeführten Benutzeraktivitäten protokolliert. NetScaler ADM stellt wichtige Metriken zur Verfügung, mit denen Sie Folgendes ermitteln können:

1. Das Surfverhalten der Benutzer in Ihrem Unternehmen.
2. URL-Kategorien, auf die die Benutzer in Ihrem Unternehmen zugreifen.
3. Die fünf besten Benutzer, basierend auf ihren Risikobewertungen und der Bandbreite, die sie verbrauchen. Weitere Informationen zu Risikobewertungen finden Sie unter Risikobewertung.
4. Browser, mit denen auf die URLs oder Domains zugegriffen wurde.
5. Menge des von den Benutzern erzeugten Web-Traffic basierend auf dem Traffic-Reputation Score.

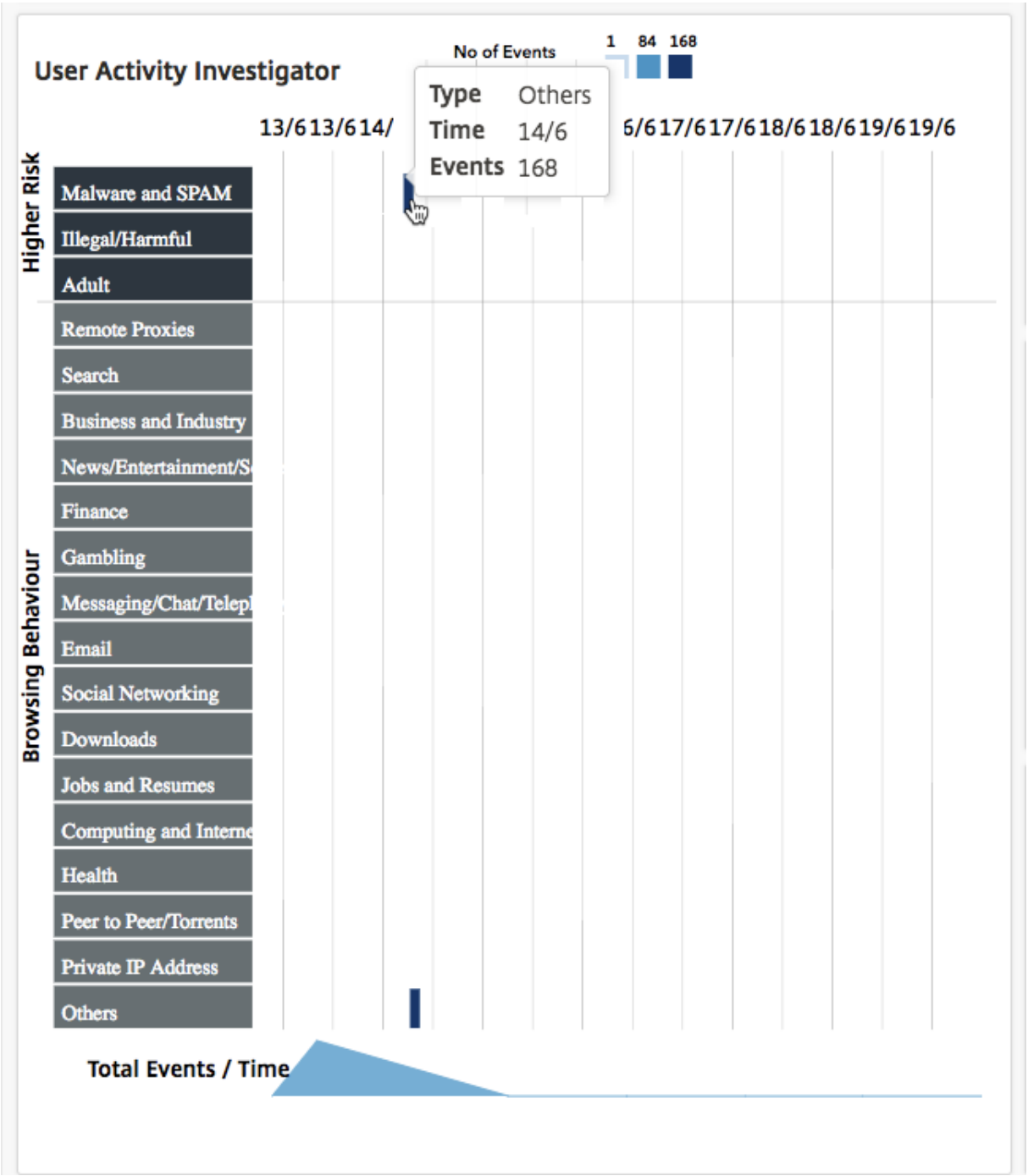
Wenn beispielsweise ein Benutzer mit Benutzer-ID testuser3 ständig auf Malware-bezogene Websites in Ihrem Unternehmen zugreift, identifiziert NetScaler ADM den Benutzer als Benutzer mit hoher Risikoaktivität und weist eine höhere Risikobewertung zu. Die Informationen testuser3 werden im Abschnitt **Top Users** des **User Dashboards** angezeigt.



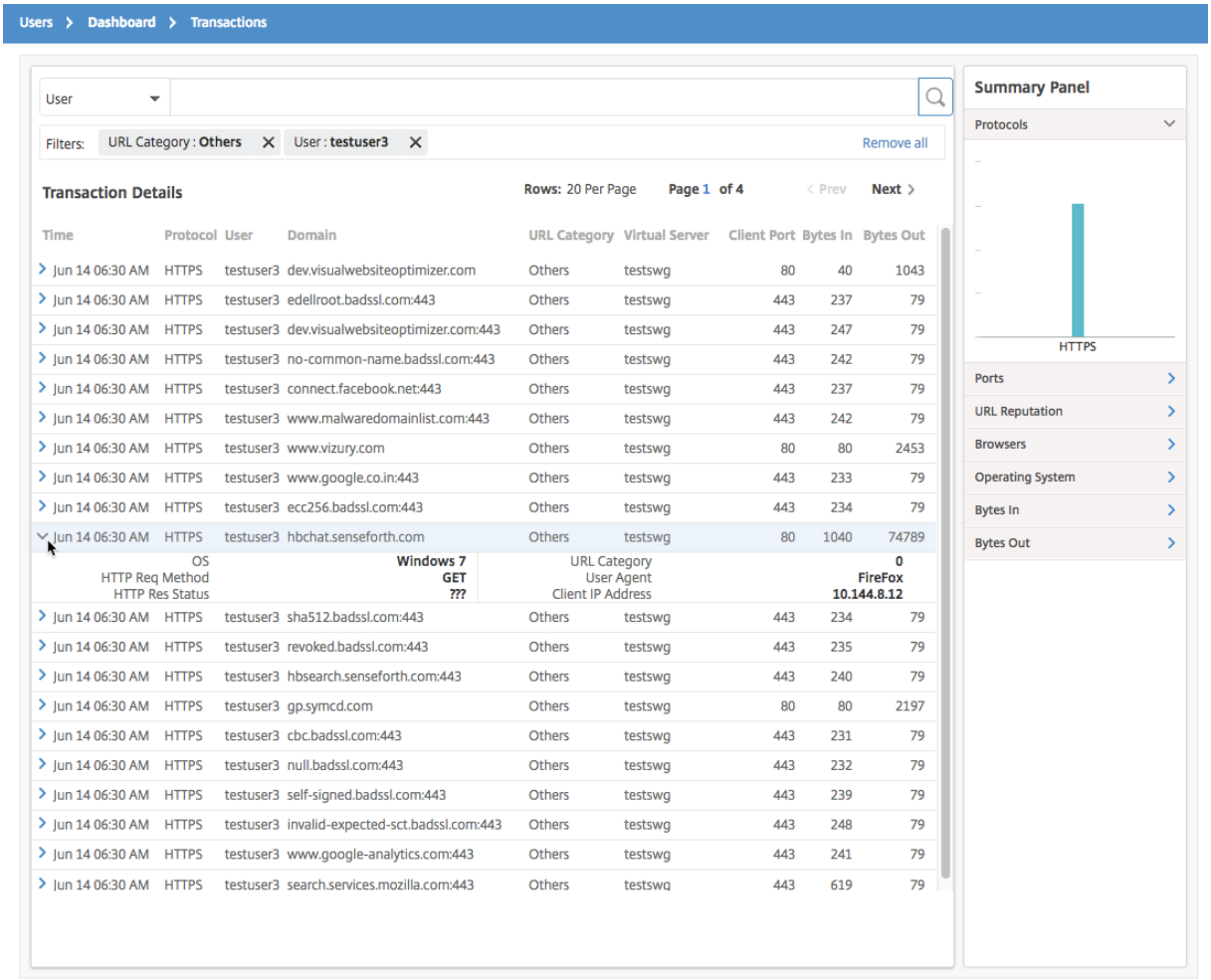
Sie können auf testuser3 klicken, um das **Benutzer-Dashboard** zu filtern, um alle wichtigen Metriken im Zusammenhang mit testuser3 anzuzeigen.



Im Bereich **Benutzeraktivitätsuntersuchung** wird die risikoreiche Aktivität von testuser3 als Ereignisse in den jeweiligen URL-Kategorien angezeigt.



Sie können den Mauszeiger über die Ereignisse bewegen, um die Anzahl der Ereignisse anzuzeigen, und Sie können auf Ereignisse klicken, um die Transaktionen zu untersuchen, die während der Ereignisse aufgetreten sind.

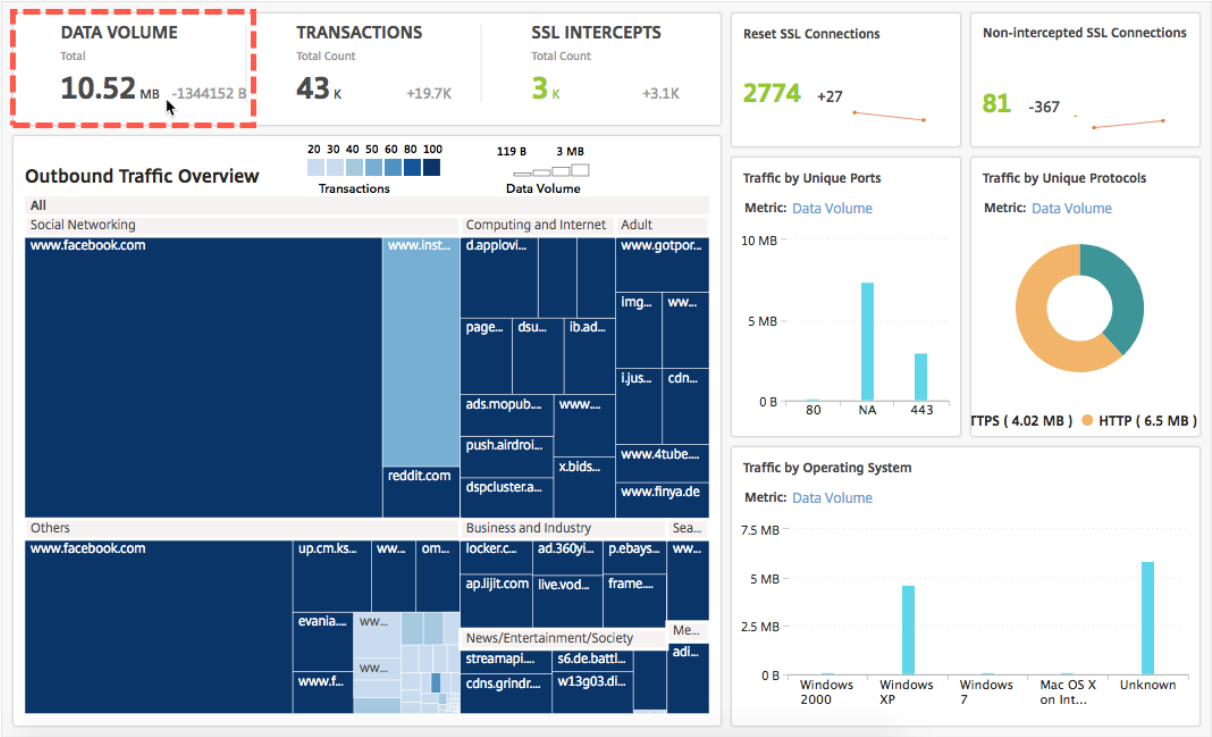


Mit diesen Informationen können Sie feststellen, ob Ihr System durch Malware infiziert ist, oder Sie können das Bandbreitenverbrauchsmuster des Benutzers verstehen und Ihre NetScaler ADC Richtlinien optimieren. Weitere Informationen finden Sie in der Citrix SSL-Forward-Proxy-Dokumentation.

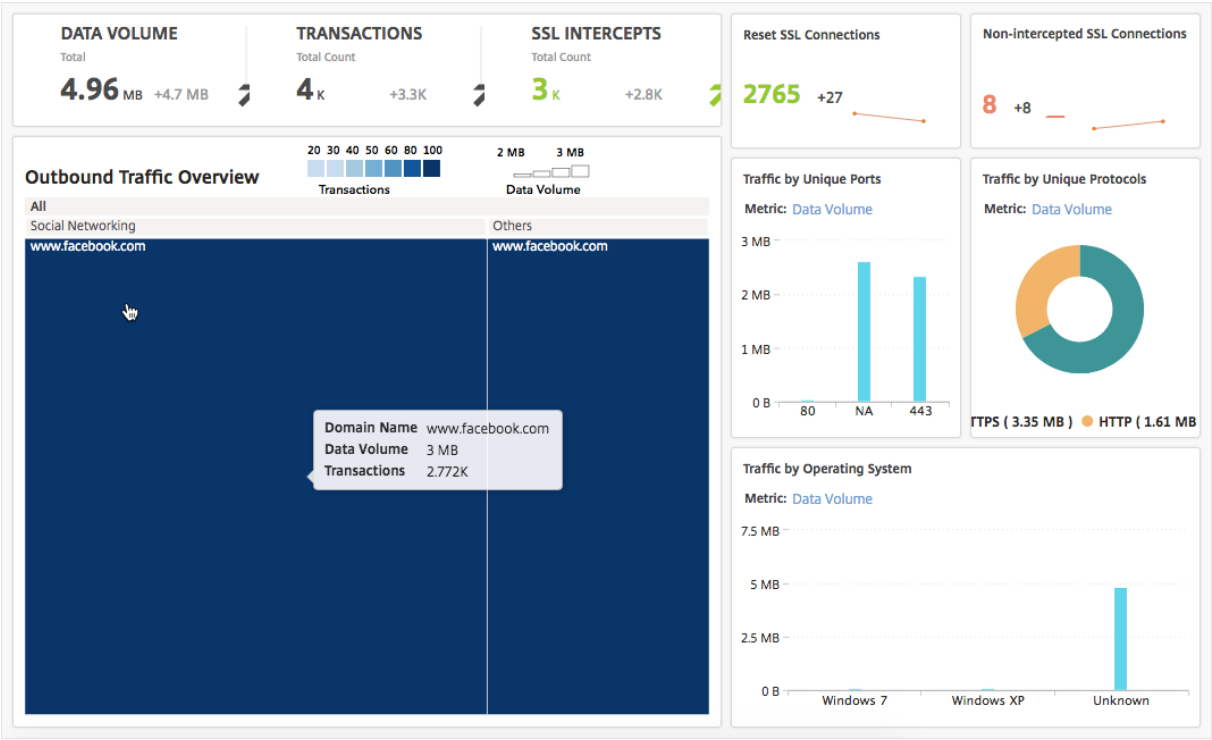
Berichterstattung über Bandbreitenverbrauch

Das **Dashboard für ausgehenden Datenverkehr** und das **Benutzerdashboard** stellen mehrere Diagramme bereit, in denen die Websites oder Anwendungen zusammengefasst werden, auf die vom Unternehmensnetzwerk zugegriffen wird, sowie die Aktivitäten, die von den Benutzern im Netzwerk ausgeführt werden.

Das **Dashboard für ausgehenden Datenverkehr** enthält die Details des Datenvolumens durch die URLs oder Domänen, auf die über Ihr Netzwerk zugegriffen wurde. Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**, wo die **Daten im Abschnitt Datenvolumen**angezeigt werden.

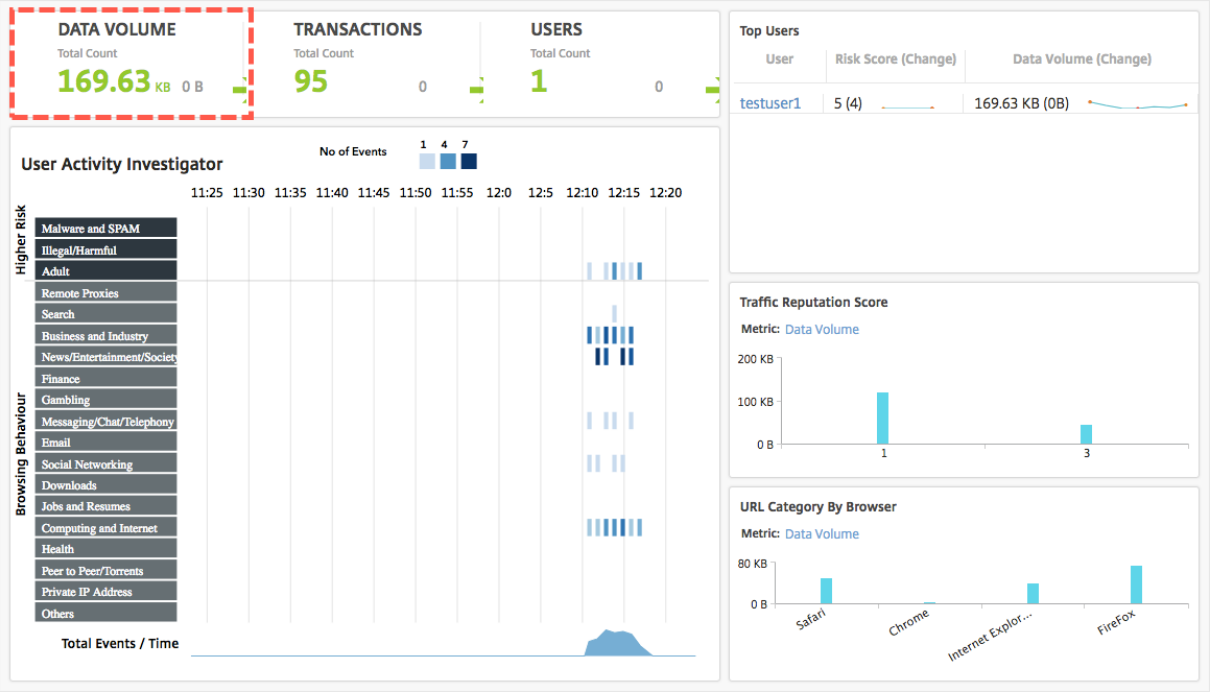


Im Bereich **Übersicht über ausgehenden Datenverkehr** können Sie auf eine Domäne oder URL klicken, um die Details des Datenvolumens anzuzeigen, das von der Domäne oder URL verwendet wird.

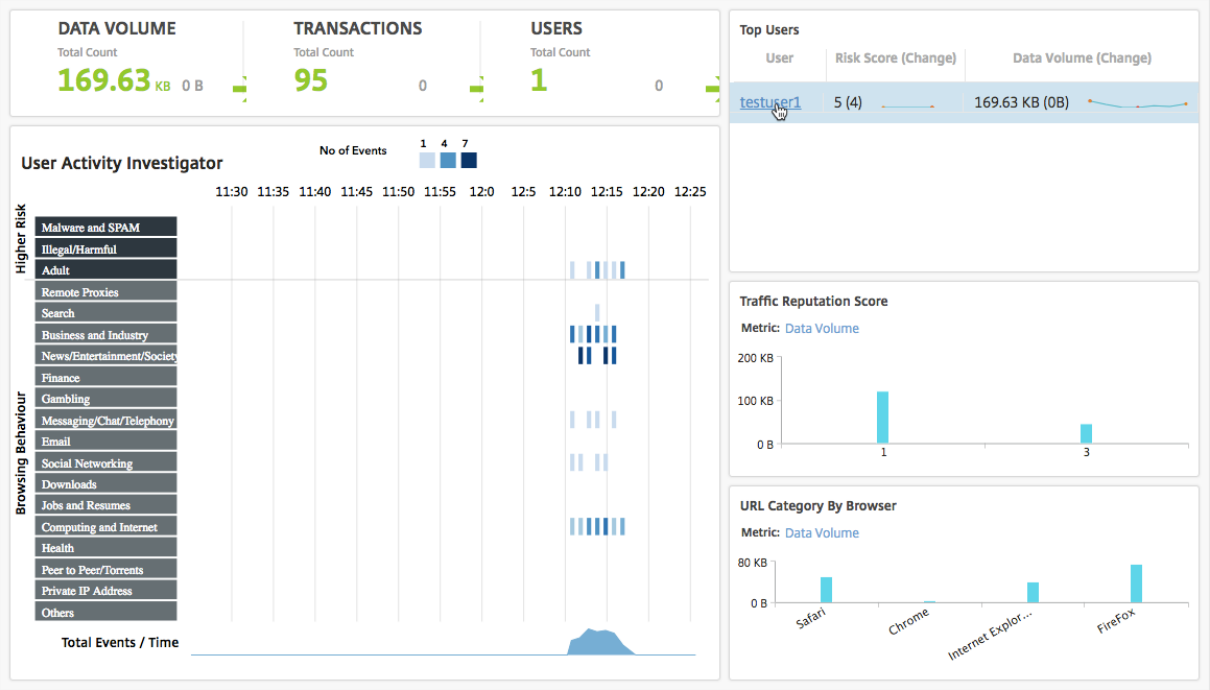


Das **Benutzerdashboard** enthält Details zur Bandbreite, die von den Benutzern in Ihrem Netzwerk

belegt wird. Navigieren Sie zu **Benutzer > Dashboard**, um die Details der von Benutzern verbrauchten Bandbreite im Abschnitt **DATA VOLUME** im **Benutzerdashboard** anzuzeigen.



Sie können die Details der Bandbreite anzeigen, die von einem Benutzer belegt wird, indem Sie den Benutzer im Abschnitt **Top Benutzer** auswählen. Der Abschnitt **DATA VOLUME** und andere Schlüsselmetriken im Diagramm werden für den ausgewählten Benutzer gefiltert.



Anhand dieser Details können Sie den Bandbreitenverbrauch und den Grund für den Verbrauch ver-

stehen. Wenn ein Benutzer beispielsweise auf Websites sozialer Netzwerke zugreift und dies zu einem hohen Bandbreitenverbrauch geführt hat, kann der Administrator auf die NetScaler ADC Appliance zugreifen und eine URL-Listenfunktion konfigurieren, um den Zugriff auf die Websites zu steuern. Weitere Informationen finden Sie unter Anwendungsfall: URL-Filterung mithilfe des benutzerdefinierten URL-Sets.

Verteilung des ausgehenden Datenverkehrs anzeigen

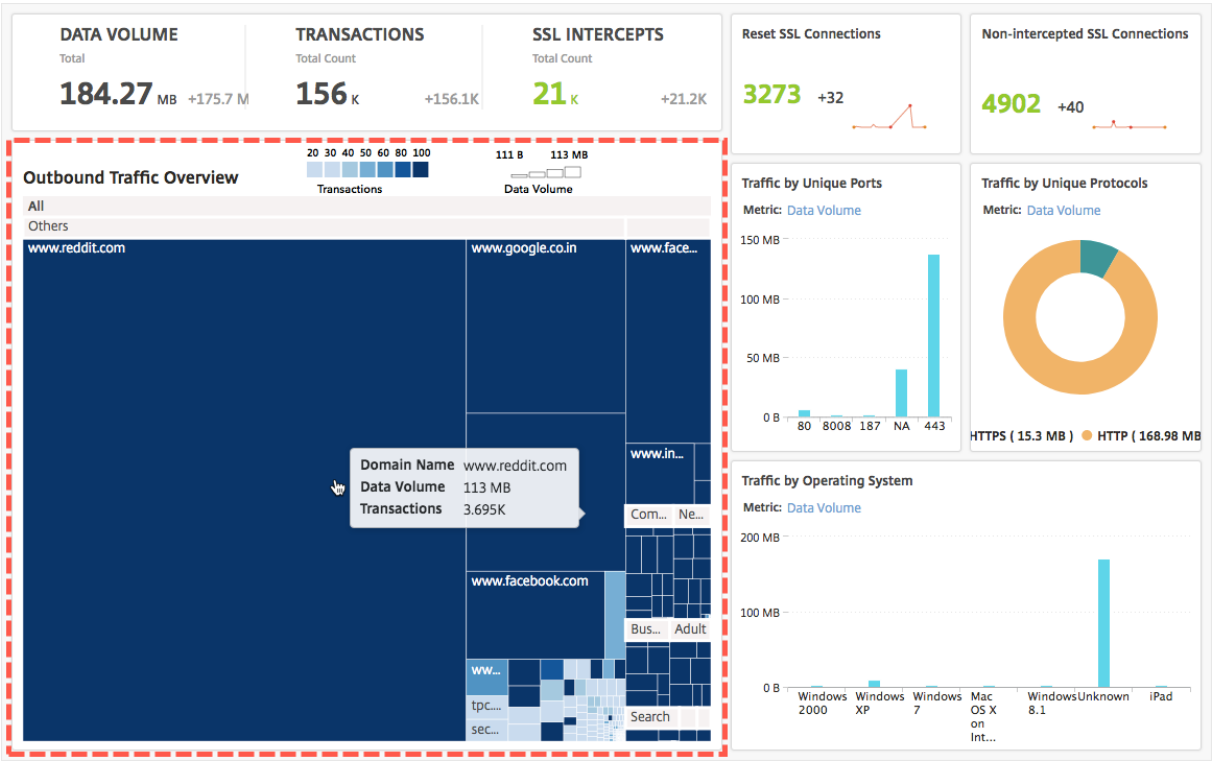
Die NetScaler ADC Appliance bietet URL-Kategorisierungs- und Filterfunktionen, mit denen Sie die URLs kategorisieren können, auf die über Ihr Netzwerk zugegriffen wird. In NetScaler ADM enthält das **Dashboard für ausgehenden Datenverkehr** einen Bereich **Übersicht über den ausgehenden Datenverkehr**. Im Bereich **Übersicht über den ausgehenden Datenverkehr** gruppiert NetScaler ADM die zugegriffenen URLs oder Domänen in Kategorien wie Shopping, News, Mobile usw., um die Verteilung des ausgehenden Datenverkehrs im Netzwerk anzuzeigen. Für einen ausgewählten Zeitraum können Sie auf die URL klicken, um Folgendes zu verstehen:

1. Beim Zugriff auf die URL verbrauchte Bandbreite
2. Transaktionen, die beim Zugriff auf die URL aufgetreten sind
3. Anzahl der SSL-Verbindungen, die beim Zugriff auf die URL abgefangen, nicht abgefangen und zurückgesetzt wurden

Mit diesen Informationen können Sie das Muster des ausgehenden Datenverkehrs verstehen und Korrekturentscheidungen treffen, z. B. ob bestimmte URLs blockiert werden sollen.

Verteilung des ausgehenden Datenverkehrs anzeigen:

Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**.Das **Dashboard für den Außenborder** zeigt die URLs im Bereich "**Übersicht über ausgehenden Datenverkehr** "an:



Wenn Sie die Details einer bestimmten URL anzeigen möchten, wählen Sie die URL aus.

Mithilfe dieser Informationen können Sie das Muster des ausgehenden Datenverkehrs verstehen und den Netzwerkverkehr mithilfe eines auf der NetScaler ADC Appliance konfigurierten URL-Filters steuern. Weitere Informationen finden Sie unter URL-Filter.

Orchestrierung

February 5, 2024

Beim Software Defined Networking (SDN) verwaltet ein Softwareanwendungscontroller ein Netzwerk und seine Aktivitäten, anstatt Hardware, die das Netzwerk unterstützt. Das heißt, SDN ermöglicht es den Netzwerkadministratoren, eine physische Netzwerkkonnektivität in eine logische Netzwerkkonnektivität zu virtualisieren und Netzwerkdienste mithilfe eines softwarebasierten zentralen Managementtools zu verwalten. SDN ermöglicht es Netzwerktechnikern und Administratoren, auf sich schnell ändernde Geschäftsanforderungen zu reagieren.

Die bekannteren Vorteile von SDN sind zwar die Programmierbarkeit des Datenverkehrs, die größere Flexibilität, die Möglichkeit, eine richtliniengesteuerte Netzwerküberwachung einzurichten und die Implementierung von Netzwerkautomatisierung, einige der spezifischen Vorteile von SDN sind jedoch im Folgenden aufgeführt:

- Zentralisierte Netzwerkbereitstellung
- Erhöhte Netzwerksicherheit auf granularer Ebene
- Geringere Betriebskosten
- Höheres Maß an Cloud-Abstraktion
- Garantierte Bereitstellung von Inhalten
- Geringere Netzwerkausfallzeiten

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

VMware NSX Manager

Citrix ADM ist in die VMware Netzwerkvirtualisierungsplattform integriert, um die Bereitstellung, Konfiguration und Verwaltung von Citrix ADC Diensten zu automatisieren. Diese Integration abstrahiert die traditionellen Komplexitäten der physischen Netzwerktopologie und ermöglicht es vSphere/vCenter-Administratoren, Citrix ADC Dienste programmgesteuert schneller bereitzustellen.

VMware NSX Manager macht logische Firewalls, Switches, Router, Ports und andere Netzwerkelemente verfügbar, um virtuelle Netzwerke zwischen verschiedenen Hypervisoren, Cloud-Managementsystemen und zugehöriger Netzwerkhardware zu ermöglichen. Es unterstützt auch externe Netzwerke und Sicherheitsdienste.

Die Cloud Orchestration-Funktion von Citrix ADM ermöglicht die Integration von Citrix ADC Produkten mit VMware NSX und bietet die folgenden Funktionen:

- Möglichkeit, einem bestimmten Edge-Gateway im Rahmen der Serviceeinfügung ein vorab bereitgestelltes VPX auf Abruf zuzuweisen.
- Möglichkeit, erweiterte Funktionen von NetScaler ADC wie SSL und CS sowie grundlegenden Lastenausgleich über Anwendungsvorlagen auf Instanzen zu konfigurieren, die in der NSX-Umgebung ausgeführt werden.
- Möglichkeit, im Rahmen der Dienstlöschung die Zuweisung eines VPX von einem bestimmten Edge-Gateway zu trennen und dasselbe VPX einem anderen Edge-Gateway neu zuzuweisen.
- Möglichkeit zur schnellen Bereitstellung von NetScaler ADC Funktionen über die vCenter Konsole im Rahmen des Bereitstellungsworkflows der gesamten Infrastruktur, die für eine Anwendung erforderlich ist.

Vorteile:

- Automatisierte, bedarfsgerechte Zuweisung neuer ADC-Dienste als Teil eines Workflows zur Anwendungsbereitstellung
- Vereinfachte Konfiguration anwendungsspezifischer, erweiterter ADC-Funktionalität durch Anwendungsvorlagen
- Mehrmandantenübergreifende Aufgabentrennung und Self-Service-Nutzungsmodell bei gleichzeitiger Bereitstellung eines zentralen Kontrollpunkts für Cloud-Administratoren
- Einfachere Integration mit NetScaler ADM -APIs, die unerwartete zukünftige Verwendungen unterstützen.

Weitere Informationen zum Konfigurieren von VMware NSX Manager auf NetScaler ADM finden Sie unter Integrieren von NetScaler ADC Appliances mit VMware NSX Manager.

Cisco ACI Hybrid-Modus

Cisco ACI hat die Unterstützung für den Hybrid-Modus in Version 1.3 (2f) eingeführt. Im Hybridmodus können Sie die Netzwerkautomatisierung über den Application Policy Infrastructure Controller (APIC) durchführen und gleichzeitig die L4-L7-Konfiguration an Citrix ADM delegieren, das als Device Manager im APIC fungiert.

Die NetScaler ADC Hybridmodus-Lösung wird von einem Hybridmodusgerätepaket und NetScaler ADM unterstützt. Sie müssen das Paket des Hybrid-Modus-Gerätes im APIC hochladen. Weitere Informationen finden Sie unterNetScaler ADC Automation Verwenden von NetScaler ADM im Hybridmodus von Cisco ACI.

OpenStack: Integrieren von NetScaler ADC Instanzen

February 5, 2024

Die Cloud Orchestration-Funktion von NetScaler Application Delivery Management (ADM) ermöglicht die Integration von NetScaler ADC-Produkten in die OpenStack-Plattform. Durch die Verwendung dieser Funktion mit OpenStack-Plattform können OpenStack-Benutzer die Lastenausgleichsfunktion (LBaaS) des NetScaler ADC nutzen. Danach können die OpenStack-Benutzer ihre Load Balancer-Konfigurationen über OpenStack in der Citrix ADC Instanz bereitstellen.

In den folgenden Abschnitten finden Sie eine kurze Beschreibung der Funktionen im Citrix ADM - und OpenStack-Integrationsworkflow.

NetScaler ADC -Treiber für OpenStack Neutron LBaaS

Das OpenStack Neutron LBaaS-Plug-In enthält einen NetScaler ADC-Treiber, der OpenStack die Kommunikation mit dem NetScaler ADM ermöglicht. OpenStack verwendet diesen Treiber, um alle Lastausgleichskonfigurationen, die über LBaaS-APIs durchgeführt werden, an das NetScaler ADM weiterzuleiten, das die Load Balancer-Konfiguration für die gewünschten NetScaler ADC Instanzen erstellt. OpenStack verwendet den Treiber auch, um Citrix ADM in regelmäßigen Abständen aufzurufen, um den Status verschiedener Entitäten (z. B. VIPs und Pools) aller Lastausgleichskonfigurationen aus den Citrix ADCs abzurufen. Die Citrix ADC -Treibersoftware für die OpenStack-Plattform wird zusammen mit Citrix ADM gebündelt. Um die Treiber herunterzuladen und zu installieren, müssen Sie zuerst NetScaler ADM installieren und die Anwendung starten.

Registrieren von Citrix ADM und OpenStack untereinander

Sie müssen zuerst OpenStack-Informationen auf dem NetScaler ADM registrieren. Geben Sie die IP-Adresse des OpenStack-Controller und die Anmeldeinformationen des Cloud-Administrators sowie die Anmeldeinformationen des OpenStack Citrix ADC -Treibers an. Sie können später dieselben Anmeldeinformationen im Abschnitt Citrix ADC_Driver der Neutron-Konfigurationsdatei (neutron.conf) angeben, damit der Citrix ADC -Treiber in OpenStack während LB-Konfigurationen eine Verbindung zu Citrix ADM herstellen kann.

Nachdem OpenStack und Citrix ADM miteinander registriert sind, können beide miteinander kommunizieren. OpenStack-Benutzer können ihre vorhandenen Anmeldeinformationen in OpenStack verwenden, um sich an der Citrix ADM Benutzeroberfläche anzumelden, um zu überprüfen, wie ihre LB-Konfigurationen in Citrix ADCs funktionieren.

Mandanten in OpenStack

In OpenStack wird ein Tenant auch als Projekt bezeichnet. Ein Mandant ist eine Gruppe von Benutzern. Ein Mandant oder ein Projekt kann auch als eine Gruppe von Ressourcen (Rechenleistung, Netzwerk, Speicher usw.) definiert werden, die einer isolierten Benutzergruppe zugewiesen sind.

Richtlinien für die Platzierung

Platzierungsrichtlinien bieten die Flexibilität bei der Entscheidung über die NetScaler ADC Instanz, die in jeder von Benutzern erstellten Load Balancer-Konfiguration verwendet wird. Alternativ bietet Citrix ADM auch eine Option zum Zuweisen einer Citrix ADC Instanz auf Basis von OpenStack-Mandanten.

Servicepakete

Servicepakete sind Pakete, die Richtlinien/SLAS, Konfigurationsspezifikationen für Geräte oder automatische Bereitstellung sowie Richtlinien für Mandanten und Platzierungen miteinander verbinden. Ein Servicepaket wird normalerweise anhand der Isolationsrichtlinien definiert, die dem Mandanten zur Verfügung gestellt werden.

Im Folgenden sind einige Punkte im Zusammenhang mit Servicepaketen aufgeführt:

- Ein Mandant kann nicht an mehr als einem Servicepaket teilnehmen.
- Dem gleichen Servicepaket können mehrere Mandanten zugeordnet werden.
- In einem Servicepaket, das für die automatische Bereitstellung festgelegt ist, können virtuelle NetScaler ADC Instanzen nur von einem Plattformtyp (auf der SDX-Plattform oder auf der OpenStack Compute-Plattform) erstellt werden.

Von LBaaS V1 und LBaaS V2 unterstützte Funktionen

Während der LBaaS V1-Treiber in OpenStack Vorgänge über die Benutzeroberfläche von OpenStack Horizon unterstützt, unterstützt der LBaaS V2-Treiber nur Befehlszeilenoperationen.

Die folgende Liste zeigt die Funktionen, die sowohl auf LBaaS V1 als auch auf LBaaS V2 auf OpenStack unterstützt werden:

- LBaaS V1
  - Lastausgleich
- LBaaS V2
  - Lastausgleich
  - SSL Offload mit Zertifikaten, die von **Barbican**, dem Schlüsselmanager in OpenStack, verwaltet werden
  - Zertifikatspakete (einschließlich zwischengeschalteter Zertifizierungsstellen)
  - SNI-Unterstützung

Dieses Dokument enthält Informationen über:

- Anwendungsfallszenario
- NetScaler ADM Integration mit OpenStack-Workflow
- Prerequisites
- Vorkonfigurationsaufgaben in Citrix ADM und OpenStack

- Konfigurationsschritte für LBaaS V1 mit Horizon
- Konfigurationsschritte für LBaaS V2 über die Befehlszeile
- Manuelles Provisioning der Citrix ADC VPX Instanz auf OpenStack
- Integrieren von Citrix ADM mit OpenStack Heat Services
- Überwachen von OpenStack-Anwendungen in NetScaler ADM

Anwendungsfallszenario

Das folgende Anwendungsszenario erklärt den Workflow der Integration von NetScaler ADM in die OpenStack-Plattform:

Ein Unternehmen, Example-Cloud-Provider, hat OpenStack-Komponenten verwendet, um eine Cloud einzurichten, um seinen Mandanten eine Infrastruktur bereitzustellen. Steve ist der Administrator dieses Cloud-Anbieters, während Tom ein Mandant der Cloud-Infrastruktur des Example-Cloud-Providers ist. Die Organisation von Tom, Example-Sportsonline.com, erfordert zwei Server S1 und S1, und Tom benötigt auch ein dediziertes NetScaler ADC Gerät, um den Datenverkehr zwischen Servern S1 und S2 auf OpenStack-Plattform auszugleichen.

Um diese Anforderung zu erfüllen, muss Steve sowohl OpenStack als auch NetScaler ADM installieren und konfigurieren und sie auf miteinander kompatible Geräte vorbereiten. Steve muss in OpenStack ein Mandantenkonto mit dem Namen Example-Sportonline erstellen und dann dem Mandantenkonto Ressourcen zuweisen. Steve muss auch verschiedene Anmeldeinformationen (Benutzer) für Example-SportsOnline erstellen, um die Ressourcen und Konfiguration zu verwalten. Tom kann jetzt die beiden Server S1 und S2 auf OpenStack erstellen, um den Datenverkehr in seiner Organisation zu verwalten.

Steve muss OpenStack-Details bei NetScaler ADM registrieren und den NetScaler ADC LBaaS-Treiber in der OpenStack-Netzwerkkomponente Neutron konfigurieren. Nachdem die Registrierung abgeschlossen ist, zeigt Citrix ADM die Details aller Mandanten aus OpenStack an. Steve kann Example-Sportonline aus der Liste auswählen, wer die Citrix ADC LBaaS-Funktionen möchte, und Tom so konfigurieren, dass ein dedizierter Citrix ADC für seine Load Balancer-Konfigurationen in Citrix ADM zugewiesen wird.

Dazu kann Steve entweder eine Citrix ADC VPX Instanz auf der Computing-Schicht (Nova) von OpenStack über die Citrix ADM Benutzeroberfläche bereitstellen oder MAS aktivieren, um eine Citrix ADC VPX-Instanz bei Bedarf automatisch bereitzustellen, wenn Tom seine LB-Konfiguration in OpenStack durchführt. In beiden Fällen verwaltet Citrix ADM die VPX-Instanz. Dazu erstellt Steve ein Servicepaket in Citrix ADM und definiert die Bedingungen im Servicepaket, die in der SLA mit Tom vereinbart wurden. Steve wählt beispielsweise die „dedizierte“Isolationsrichtlinie aus, um Tom eine dedizierte Instanz für die Bereitstellung von Load Balancer-Konfigurationen zur Verfügung

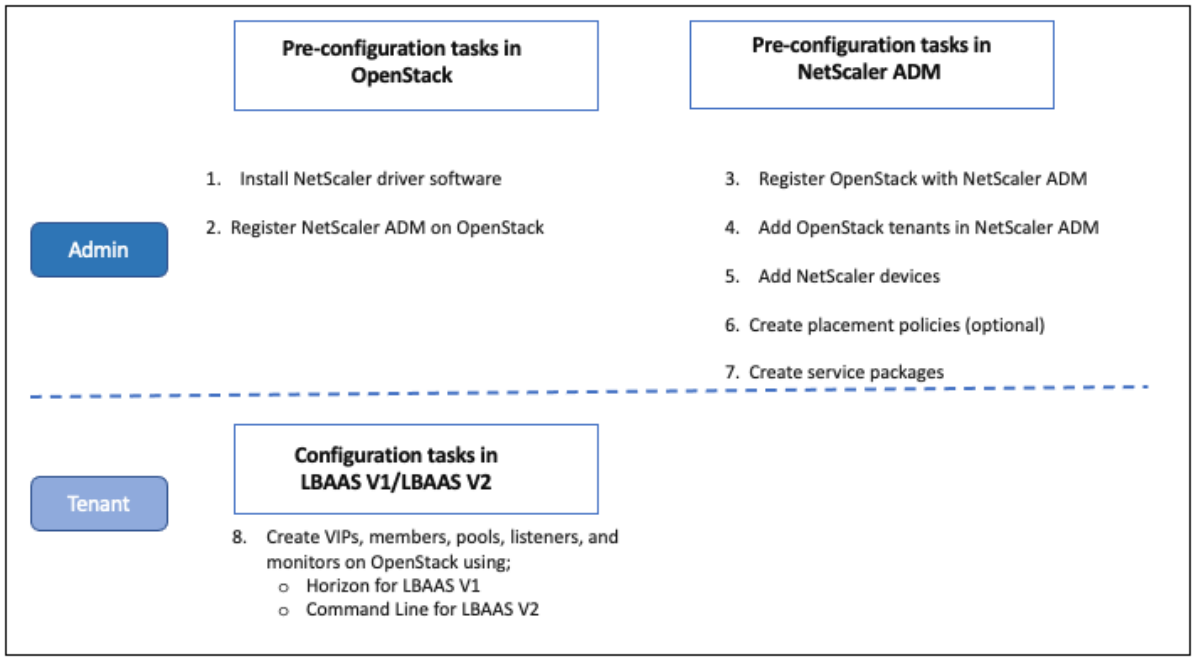
zu stellen. Das heißt, Steve wählt im Servicepaket eine Instanz aus, die nicht gemeinsam genutzt wird, für Tom. Anschließend weist er dem Servicepaket viele Citrix ADC VPX Instanzen zu und ordnet Example-Sportonline zusammen mit anderen Mandanten zu, die ein dediziertes Citrix ADC mit dem Servicepaket benötigen. Wenn Tom seine erste Load Balancer-Konfiguration durchführt, weist Citrix ADM eine der Citrix ADC VPX Instanzen im Servicepaket Example-Sportsonline zu und stellt seine Konfiguration in diesem Citrix ADC bereit.

Tom kann jetzt Lastausgleichskonfigurationen erstellen, indem Pools, virtuelle IPs (VIP) und Integritätsmonitore mit OpenStack LBaaS/UI erstellt werden. Pools und VIPs in OpenStack werden als Dienstgruppen und virtuelle Server auf der Citrix ADC Instanz bereitgestellt. Tom kann auch Integritätsmonitore erstellen, um die Server zu überwachen, und Anwendungsdatenverkehr nur an die Server senden, die zu einem beliebigen Zeitpunkt hochgefahren sind und von Citrix ADC aus erreichbar sind.

Die Lastausgleichskonfiguration, die in OpenStack erstellt wurde, ist jetzt in der Citrix ADC Instanz implementiert. Sobald die NetScaler ADC VPX Instanz vollständig konfiguriert ist, übernimmt die Lastenausgleichsfunktion und nimmt Anwendungsdatenverkehr an und gleicht den Datenverkehr zwischen den Servern S1 und S2 aus, die von Tom erstellt wurden.

NetScaler ADM Integration mit OpenStack-Workflow

Das folgende Flussdiagramm zeigt den Workflow, dem Sie folgen müssen, wenn Sie LBaaS V1 und LBaaS V2 konfigurieren.



Voraussetzungen

February 5, 2024

Bevor Sie die virtuelle Citrix ADC Instanz in die OpenStack-Plattform integrieren, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

NetScaler ADM - und OpenStack-Softwareanforderungen

- Citrix ADM 13.0 wird auf einer unterstützten Hypervisor Arbeitsstation installiert, die die Mindestanforderungen an die Hardware erfüllt.
- OpenStack-Komponenten werden installiert und ausgeführt.
- NetScaler ADM 13.0 unterstützt die folgenden OpenStack-Versionen - **Newton**, **Ocata**, **Pike**und **Queens**.

NetScaler ADM Hardwareanforderungen

Stellen Sie sicher, dass sich die folgenden virtuellen Computerressourcen auf Ihrem OpenStack-Server befinden, um virtuelle NetScaler ADC-Instanzen zu installieren:

Komponente	Voraussetzung
RAM	8 GB
Virtuelle CPU	8
Stauraum	500 GB
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s oder 100 Mbit/s

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

Vorkonfigurationsaufgaben in NetScaler ADM und OpenStack

February 5, 2024

In diesem Abschnitt können Sie die Vorkonfigurationsaufgaben ausführen, bevor Sie Citrix Application Delivery Management (ADM) und OpenStack konfigurieren.

Installieren von Citrix ADM

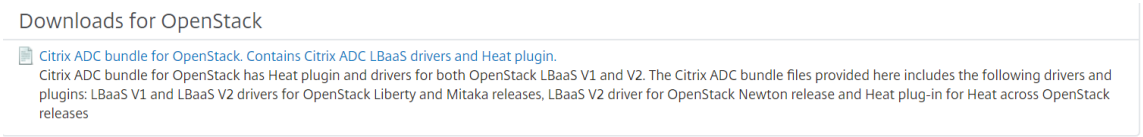
Installieren Sie NetScaler ADM auf einem unterstützten Hypervisor. Weitere Informationen zum Herunterladen und Installieren von NetScaler ADM finden Sie unter Bereitstellen von NetScaler ADM.

Installieren der NetScaler ADC -Treibersoftware und Registrieren von NetScaler ADM auf OpenStack

Laden Sie das Citrix ADC Paket für OpenStack von der Citrix ADM Download-Seite herunter.

So installieren Sie den Citrix ADC -Treiber auf der OpenStack-Plattform mit der Citrix ADM GUI:

1. Klicken Sie in Citrix ADM auf **Downloads**. Auf der **Downloads-Seite** in NetScaler ADM finden Sie Links zum Herunterladen des **NetScaler ADC-Pakets für OpenStack-Software**, die für **Newton**-, **Ocata**- und **Pike** OpenStack-Versionen erforderlich ist.
2. Laden Sie die neueste Citrix ADC -Bundle-tar-Datei in ein temporäres Verzeichnis (z. B. /tmp) in OpenStack Controller herunter. Dieses Paket enthält den LBaaS V2-Treiber und das Heat-Plug-In für alle OpenStack-Releases.



3. Führen Sie den folgenden Befehl aus, um die Dateien aus der TAR-Datei des NetScaler ADC -Treibers zu extrahieren:
   `tar -xvzf <name_of_tar_file>`
4. Wenn Sie ein OpenStack <Release Name> Setup haben, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

   `cd <Release Name>`

   Beispiel:

   `cd Newton`

5. Führen Sie den folgenden Befehl aus, um den Treiber zu installieren, und geben Sie die Citrix ADM IP-Adresse, das Citrix ADC -Treiberkennwort an, das Sie bei der Registrierung von OpenStack bei Citrix ADM konfiguriert haben, und das Protokoll an:

   ```
   ./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>
   ```

   Beispiel für ein OpenStack-Setup mit einem Knoten:

   ```
   ./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/opt/stack/neutron-lbaas
   ```

   Beispiel für ein OpenStack-Setupmit mehreren Knoten:

   ```
   ./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/usr/lib/python2.7/site-packages
   ```

   > **Hinweis**
   >
   > Die Angabe des Pfads des `neutron-lbaas` Verzeichnisses des Systems ist optional. Die Angabe des Pfads kann das Skript dabei unterstützen, die Treiber zu finden.
   >
   > Nachdem Citrix ADM erfolgreich in OpenStack registriert wurde, können Sie sich auch mit Ihren OpenStack-Benutzeranmeldeinformationen bei Citrix ADM anmelden.
   >
   > Nachdem Citrix ADM erfolgreich auf OpenStack registriert wurde, starten Sie die OpenStack Neutron Dienste neu.

Registrieren von OpenStack bei Citrix ADM

So registrieren Sie OpenStack mit Citrix ADM GUI mit Citrix ADM:

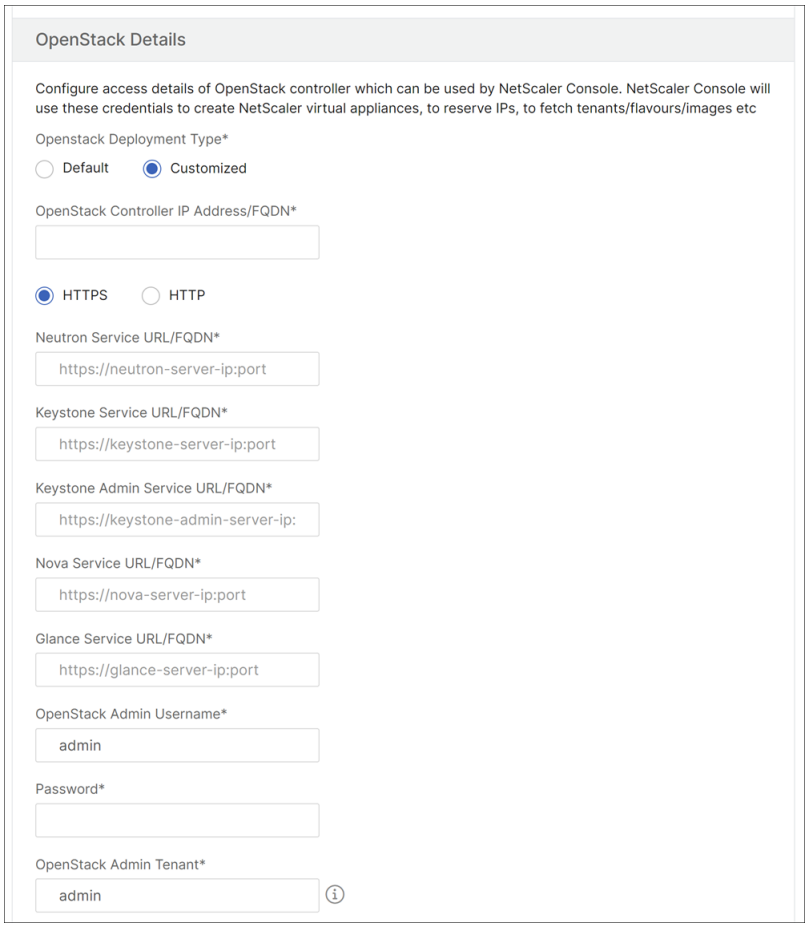
1. Navigieren Sie in Citrix ADM zu**Orchestration** >**Cloud Orchestration**>**OpenStack**.
2. Klicken Sie auf **OpenStack-Einstellungen konfigurieren**.
3. Auf der Seite **OpenStack-Einstellungen konfigurieren** können Sie die Parameter für die Konfiguration von OpenStack in Citrix ADM festlegen. Sie haben hier zwei Optionen - Standard und Customized.

   Für Newton- und **Ocara-Versionen** von OpenStack können Sie entweder den Standard- oder den benutzerdefinierten Bereitstellungstyp verwenden. Für die Pike-Version müssen Sie jedoch den benutzerdefinierten Bereitstellungstyp verwenden, um OpenStack bei Citrix ADM zu registrieren.

- **Standard-Bereitstellungstyp**

Wählen Sie**Standard**, wenn die OpenStack-Dienste auf Standardports laufen. Das Standardportal für Neutron-Dienste ist beispielsweise 9696, das Standardportal für Keystone-Dienste ist 5000.

1. OpenStack-Controller-IP-Adresse - IP-Adresse des OpenStack-Controllers (sowohl der **KeyStone-Dienst** als auch der **Neutron-Dienst** sollten über diese IP-Adresse erreichbar sein). Geben Sie beispielsweise die IP-Adresse 10.102.205.23 ein.
2. OpenStack Admin-Benutzername - administrativer Benutzername des OpenStack-Controllers. Geben Sie beispielsweise admin1 ein.
3. Kennwort —Kennwort des administrativen Benutzers des OpenStack-Controllers.
4. OpenStack Admin Tenant —der Name des administrativen Mandanten auf OpenStack. Geben Sie beispielsweise admin ein.



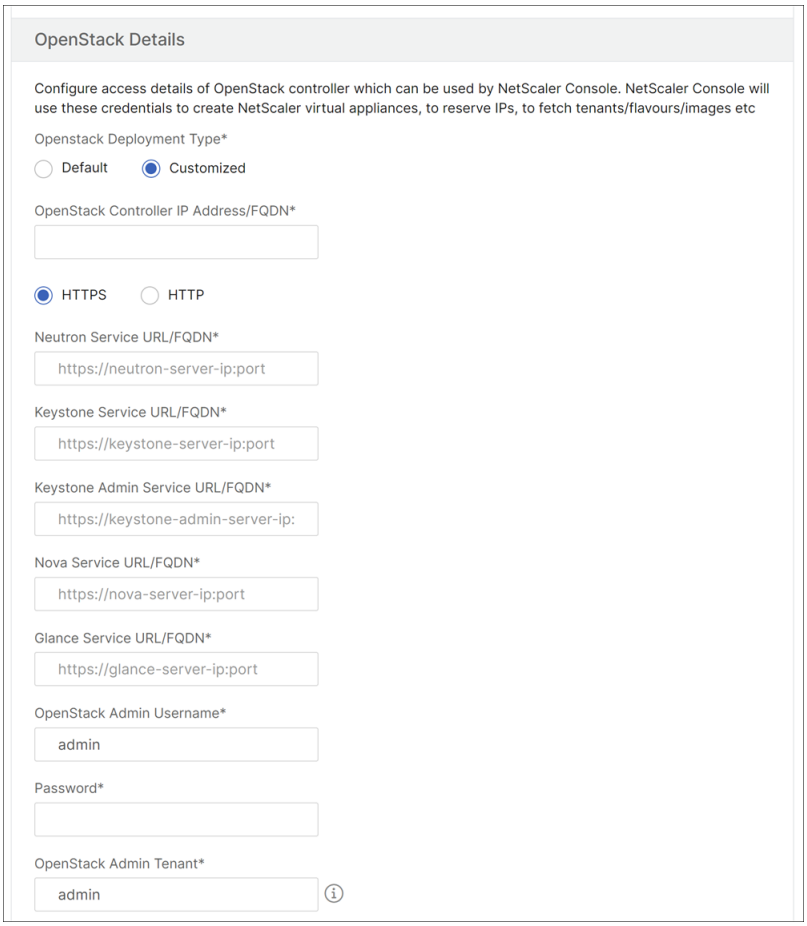
- **Angepasster Bereitstellungstyp**

  Wählen Sie den Bereitstellungstyp**als Benutzerdefiniert** aus, wenn die OpenStack-Dienste auf anderen Ports als den Standardports ausgeführt werden. Wenn diese Dienste auf verschiedenen Ports laufen, geben Sie sie hier an. Die Registrierung von OpenStack Newton- und

Ocata - Releases mit NetScaler ADM unterscheidet sich von der Registrierung der OpenStack Pike-Version.

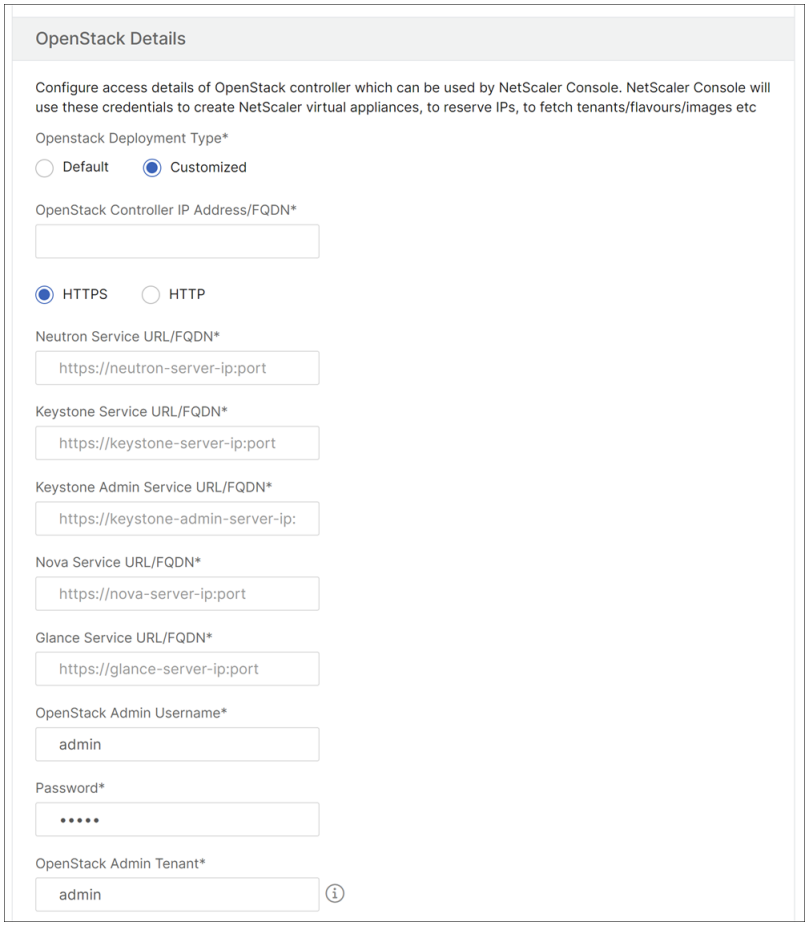
Newton und Ocata veröffentlichen OpenStack:

1. Geben Sie die Portnummern für die verschiedenen OpenStack-Dienste an, wenn Sie Newton Release von OpenStack registrieren.
2. Geben Sie den OpenStack Admin-Benutzernamen, das Kennwort und den Benutzernamen des OpenStack Admin Tenant an, wie Sie zuvor in den **Standardeinstellungen** angegeben hatten.

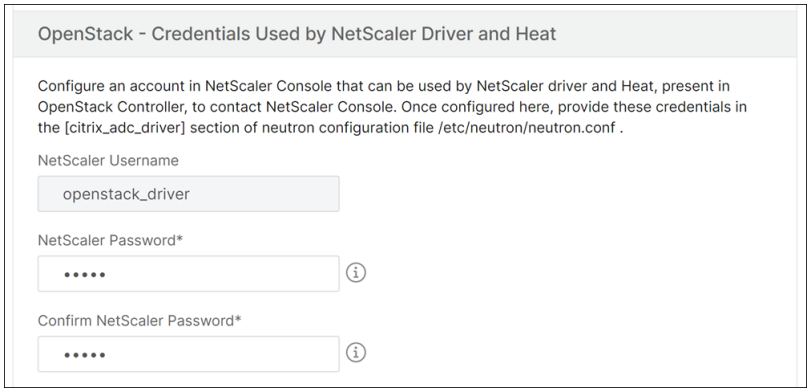


Pike Release von OpenStack:

Wenn Sie die Pike Release von OpenStack registrieren, geben Sie die Details der OpenStack-Dienste ein, wie in der folgenden Abbildung dargestellt. Sie müssen auch den OpenStack Admin-Benutzernamen, das Kennwort und den Benutzernamen des OpenStack Admin Tenant wie in den Standardeinstellungen angeben.



1. Legen Sie im Abschnitt**OpenStack Neutron LBaaS - Anmeldeinformationen, die von NetScaler ADC -Treiber verwendet werden**, das NetScaler ADC-Treiberkennwort für das OpenStack NetScaler ADC-Treiberbenutzerkonto fest. NetScaler ADM authentifiziert die Anrufe vom OpenStack NetScaler ADC -Treiber mithilfe dieser Anmeldeinformationen. Sie müssen dasselbe Kennwort angeben, wenn Sie das NetScaler ADC-Treiberinstallationsskript im OpenStack-Controller ausführen.



2. Klicken Sie auf **OK**.

Einen Mandanten auf OpenStack erstellen

Erstellen Sie ein Projekt oder einen Mandanten auf OpenStack, fügen Sie Benutzer zum Projekt oder Mandanten hinzu und weisen Sie allen Benutzern Rollen zu. **KeyStone**, der Identitätsdienst in OpenStack, bietet Authentifizierungsdienste für jeden OpenStack-Dienst. Der Authentifizierungsdienst verwendet eine Kombination aus Domänen, Projekten (Mandanten), Benutzern und Rollen.

Weitere Informationen zum Erstellen eines Projekts und zum Ausführen anderer Aufgaben in OpenStack finden Sie in der OpenStack-Dokumentation unter.http://docs.openstack.org/

OpenStack-Mandanten hinzufügen

1. Navigieren Sie in Citrix ADM zu**Orchestration** >**Cloud Orchestration**> **OpenStack** >**OpenStack-Mandanten**, und klicken Sie dann auf**Hinzufügen**.
2. Klicken **Sie auf der Seite „OpenStack-Mandanten** hinzufügen“auf **+Hinzufügen**und wählen Sie dann den OpenStack-Mandanten aus.
3. Klicken Sie auf **OK**.

Führen Sie je nachdem, ob Sie bei der Integration von OpenStack eine vorab bereitgestellte Instanz verwenden oder die Instanz automatisch bereitstellen möchten, eine der folgenden beiden Aufgaben aus:

- Provisioning der NetScaler ADC Geräte im Voraus
- Automatische Bereitstellung der NetScaler ADC VPX-Geräte auf OpenStack

Provisioning von NetScaler ADC Geräten

Führen Sie je nachdem, ob Sie bei der Integration von OpenStack eine vorab bereitgestellte Instanz verwenden oder die Instanz automatisch bereitstellen möchten, eine der folgenden beiden Aufgaben aus:

- Provisioning der NetScaler ADC Geräte im Voraus
- Automatische Bereitstellung der NetScaler ADC VPX-Geräte auf OpenStack

Vorbereitstellung von NetScaler ADC Geräten

Installieren Sie das Citrix ADC Gerät auf einer der Hypervisorplattformen wie Citrix Hypervisor, KVM oder ESX, und fügen Sie die Instanz zu Citrix ADM hinzu. NetScaler ADM verwaltet dann dieses Gerät, das den Datenverkehr auf den Servern ausgleicht.

So fügen Sie eine vorhandene Citrix ADC VPX Instanz in Citrix ADM hinzu:

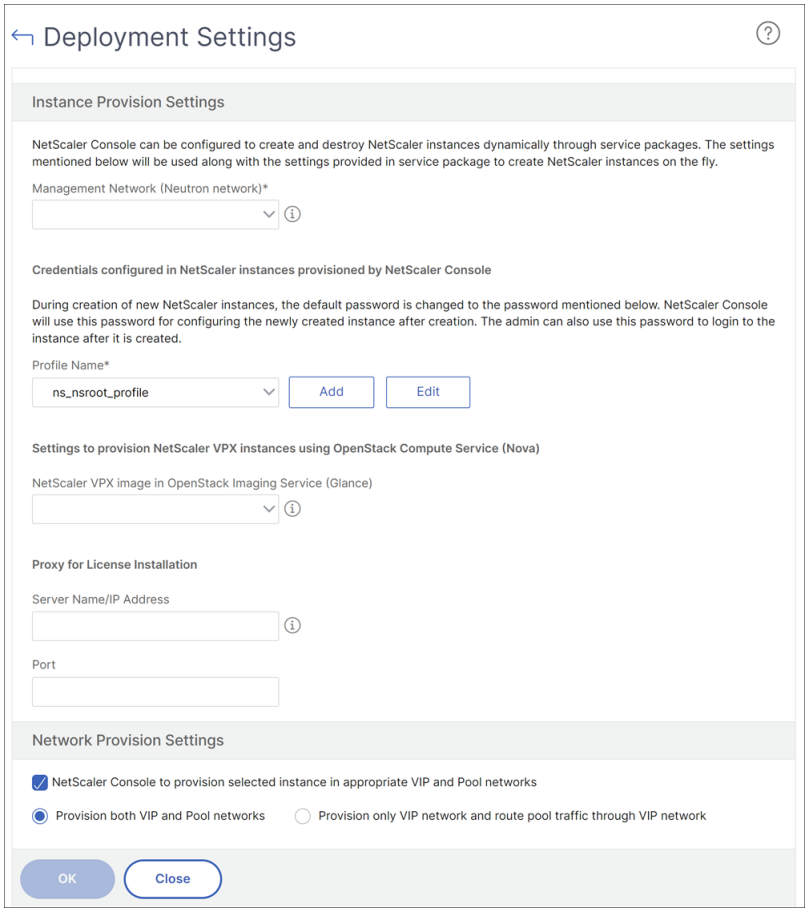
1. Navigieren Sie in Citrix ADM zu**Infrastruktur** >**Instanzen** >**Citrix ADC VPX**, und klicken Sie dann auf**Hinzufügen**.
2. Geben Sie auf der Seite**Citrix ADC VPX hinzufügen**die IP-Adresse der Citrix ADC VPX Instanz an, und wählen Sie ein Instanzprofil aus der Liste**Profilname**aus. Das Instanzprofil enthält die Anmeldeinformationen, die für die Anmeldung am Citrix ADC VPX verwendet werden. Sie können auch ein neues Instanzprofil erstellen, indem Sie auf das Symbol + klicken. Klicken Sie auf **OK**.

Autoprovisioning von Citrix ADC Geräten

Laden Sie das erforderliche Citrix ADC Instanzimage von der Citrix Downloadseite herunter und laden Sie es auf Glance, dem OpenStack Imaging Service, hoch. Wenn Sie ein Image auf Glance zur Verfügung haben, können Sie eine Citrix ADC Instanz bei Bedarf konfigurieren, wenn Sie die Instanz dem Mandanten zuweisen.

So stellen Sie Citrix ADC VPX Geräte automatisch in OpenStack bereit:

1. Navigieren Sie in NetScaler ADM zu **Orchestration** > **Cloud Orchestration** > **OpenStack**.
2. Klicken Sie auf**Bereitstellungseinstellungen**.
3. Legen Sie die folgenden Parameter fest:
    a) Verwaltungsnetzwerk: Wählen Sie das Verwaltungsnetzwerk in OpenStack aus, mit dem das automatisch bereitgestellte Citrix ADC VPX verbunden ist.
    b) Profilname - Wählen Sie das Profil aus der Dropdownliste aus. NetScaler ADM verwendet das in diesem Profil enthaltene Kennwort, um neue automatisch bereitgestellte NetScaler ADC VPX Instanzen zu konfigurieren.
    c) Lizenzen - stellen die NetScaler ADM-Lizenzzugriffscodes bereit, mit denen neue automatisch bereitgestellte NetScaler ADC-Instanzen lizenziert werden. NetScaler ADM stellt NetScaler ADC Instanzen auf OpenStack-Compute im Verwaltungsnetzwerk bereit und löst dann die Lizenzinstallation auf ihnen mithilfe des angegebenen Lizenzcodes aus. Die NetScaler ADC-Instanz lädt dann die Lizenzdateien mit dem hier angegebenen Lizenzzugriffscode von der Citrix Website herunter.
    d) NetScaler ADC VPX Image in Glance: Wählen Sie im OpenStack Glance das NetScaler ADC VPX Image aus, das zum Erstellen einer NetScaler ADC VPX-Instanz verwendet wird.
    e) Proxy-Einstellungen: Geben Sie Details zum Citrix ADC Proxyserver für die Installation von Lizenzen an. Dies kann erforderlich sein, wenn Citrix ADC keinen direkten Zugriff auf das Internet über das Verwaltungsnetzwerk hat.
4. Klicken Sie auf **OK**.



Erstellen eines Servicepakets in NetScaler ADM

So erstellen Sie Servicepakete für einen Mandanten in Citrix ADM:

1. Navigieren Sie in NetScaler ADM zu **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Service Packages**, und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie auf der Seite **Service Package** die folgenden Parameter an:

   a) Name - Name für das Servicepaket. Geben Sie beispielsweise SVC-PKG-GOLD ein.

   b) Citrix ADC Instanzzuweisung: Der Typ der Instanzzuweisung, der im Servicepaket definiert ist, auf der Grundlage dessen, welche Citrix ADC Instanzressourcen einem Mandanten zugewiesen werden. Wählen Sie **Dediziert**aus. Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für die Isolierung von Servicepaketen.

   c) NetScaler ADC Instanz Provisioning: Wählen Sie **Vorhandene Instanz**aus, um einem Mandanten eine vorhandene NetScaler ADC Instanz zuzuweisen. Wenn Sie Citrix ADC Instanzen während der Konfiguration selbst erstellen möchten, wählen Sie **Instanz OnDemand erstellen**aus.

d) Citrix ADC-Instanztyp: Wählen Sie **Citrix ADC VPX**aus.

> **Hinweis**
>
> Wählen Sie Citrix ADC VPX, um vorab bereitgestellte Citrix ADC Instanzen zuzuweisen, die auf der SDX-Plattform gehostet werden.

3. Klicken Sie auf **Weiter**, um einen Mandanten einem Servicepaket zuzuordnen.

> **Hinweis
>
> Aktivieren Sie**Provision-Paar von Citrix ADC Instanzen für hohe Verfügbarkeit**, wenn Sie die Citrix ADC-Instanzen im Hochverfügbarkeitsmodus bereitstellen.

4. Klicken **Sie im Abschnitt Instanzen zuweisen** auf **Hinzufügen**, wählen Sie dann die Citrix ADC Instanz aus, die Sie dem Mandanten zuweisen möchten, und klicken Sie auf **Weiter**.
5. Klicken **Sie im Abschnitt OpenStack Tenants/Placement Policies**unter **OpenStack Tenants auf**Hinzufügen**und wählen Sie den Mandanten** aus.
6. Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig**.

> **Hinweis**
>
> Wenn die Richtlinie nicht gefunden wird, wird der Fallbackmechanismus wiederhergestellt, und NetScaler ADM weist NetScaler ADC Instanzen basierend auf Mandanten zu. Wenn der Mandant nicht Teil eines Dienstpakets ist, zeigt NetScaler ADM eine Fehlermeldung an, die besagt: "Mandant <admin> ist nicht Teil eines Servicepakets und es gibt kein Standarddienstpaket."

Erstellen von Platzierungsrichtlinien (optional)

Isolationsrichtlinien beziehen sich nicht nur auf Mandanten. Sie können flexible Platzierungsrichtlinien erstellen, bei denen die Richtlinien nicht nur auf dem Namen oder der ID des Mandanten basieren, sondern auch auf anderen benutzerdefinierten Attributen.

So erstellen Sie Platzierungsrichtlinien für einen Mandanten in Citrix ADM:

1. Navigieren Sie in Citrix ADM zu **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Platzierungsrichtlinie**, und klicken Sie dann auf **Hinzufügen**.
2. Legen Sie auf der Seite **Placement Policy hinzufügen** die folgenden Parameter fest:
   a) Name —geben Sie einen Namen für die Platzierungsrichtlinie ein
   b) Beispielausdrücke —wählen Sie einen Beispielausdruck aus der Liste aus. Diese Beispiele sind hilfreich, um die Platzierungsrichtlinie zu erstellen.

c) Ausdruck —In diesem Feld wird ein boolescher Ausdruck aufgefüllt, der auf dem Beispielausdruck basiert, den Sie im vorherigen Feld ausgewählt haben. Bearbeiten Sie die Feldnamen nach Bedarf.

3. Klicken Sie auf **OK**.

Aktivierung des Datenverkehrs von NetScaler ADC-Instanzen zu Back-End-Servern über das Clientnetzwerk

Standardmäßig sind NetScaler ADC Instanzen im OpenStack-Orchestrierungsworkflow dynamisch an den Lastausgleichsdienst oder Clientnetzwerke sowie Mitglieds- oder Servernetzwerke gebunden.

In bestimmten Bereitstellungen sind Server auch über Client-Netzwerke erreichbar und können über das Clientgateway geroutet werden. In solchen Fällen müssen die Citrix ADC Instanzen nicht an Servernetzwerke gebunden sein, sondern nur an Clientnetzwerke gebunden sein.

Führen Sie die folgende Einstellung durch, um den Datenverkehr über das Client-Gateway zu konfigurieren.

Navigieren Sie zu **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Deployment Settings**und wählen Sie dann die Option **Nur VIP-Netzwerk bereitstellen und Pool-Traffic über das VIP-Netzwerk weiterleiten** aus.

NetScaler ADM konfiguriert dann die NetScaler ADC Instanz für Clientnetzwerke, indem ein SNIP in diesem Netzwerk hinzugefügt wird, und fügt dem Clientnetzwerkgateway eine Standardroute hinzu. Dadurch kann die Instanz die Server über das Clientgateway erreichen.

Automatische Bereitstellung von Citrix ADC VPX Geräten, die auf der Citrix ADC SDX-Plattform bereitgestellt werden

Fügen Sie die Citrix ADC SDX-Plattform in Citrix ADM hinzu, damit Citrix ADM die Instanzen auf dieser Plattform bei Bedarf bereitstellt.

So verwenden Sie NetScaler ADC Instanzen, die auf der NetScaler ADC SDX-Plattform bereitgestellt werden, automatisch:

1. Navigieren Sie in der Citrix ADM GUI zu**Netzwerke** >**Instanzen** >**Citrix ADC SDX**und klicken Sie auf**Hinzufügen**, um eine Citrix ADC SDX-Plattform hinzuzufügen.
2. Navigieren Sie zu**Orchestration** >**Cloud Orchestration**>**OpenStack** >**Bereitstellungseinstellungen.**
3. Wählen Sie im Abschnitt**Verwaltungsnetzwerk**das Verwaltungsnetzwerk in OpenStack aus, mit dem das automatisch bereitgestellte Citrix ADC SDX verbunden ist.

a) Wählen Sie**unter Profilname**das Profil aus der Dropdownliste aus. NetScaler ADM verwendet das in diesem Profil enthaltene Kennwort, um neue automatisch bereitgestellte NetScaler ADC VPX Instanzen zu konfigurieren.

b) Klicken Sie auf **OK**.

4. Um die Citrix ADC SDX-Plattform in OpenStack bereitzustellen, navigieren Sie zu**Orchestration** >**Cloud Orchestration**>**OpenStack**>**Service Package**.

a) Klicken Sie auf**Hinzufügen**, um ein neues Servicepaket zu erstellen.

b) Geben Sie den Namen des Servicepakets ein.

c) Wählen**Sie im Feld Zuweisung von Citrix ADC-Instanzen**die Option**Dediziert**aus.

d) Wählen Sie im Feld**Citrix ADC-Instanz Provisioning**die Option**Instanz OnDemand erstellen**und im Feld**Auto Provisioning Platform**die Option**Citrix ADC SDX**aus.

e) Standardmäßig werden nur Citrix ADC VPX Instanzen auf der Citrix ADC SDX-Plattform bereitgestellt.

f) Klicken Sie auf **Weiter**.

g) Legen Sie im Abschnitt**Einstellungen für die automatische Bereitstellung** die Eigenschaften der**Ressourcen** fest.

i. Feld „**Durchsatz**“. Geben Sie 1000 Mbit/s ein.

ii. **NetScaler ADC Version (Feld)**. Wählen Sie aus der Liste die richtige Version des Citrix ADC VPX-Images aus, das auf der Citrix ADC SDX-Plattform vorhanden ist.

h) Klicken Sie im Abschnitt**NetScaler ADC SDX-Plattformen**auf**Hinzufügen**, um die SDX-Plattform dem Servicepaket hinzuzufügen.

i) Klicken Sie auf **Weiter**.

j) Klicken**Sie im Abschnitt Configure OpenStack Tenants**auf**Hinzufügen**, um die Mandanten hinzuzufügen. Sie können auch neue Mandanten hinzufügen, indem Sie auf**Neu**klicken.

k) Klicken Sie auf **Fertig**.

5. LBaaS V2 API-Implementierungen werden über Neutron LBaaS-Befehle durchgeführt. Verbinden Sie sich mit einem beliebigen Neutron-Client und führen Sie die Konfigurationsaufgaben aus Weitere Informationen zum Ausführen von Konfigurationsbefehlen finden Sie unterKonfigurieren von LBaaS V2 mit der Befehlszeile.

LBaaS V1 mit Horizon konfigurieren

February 5, 2024

Tom kann sich jetzt am OpenStack Horizon-Portal anmelden und einen LBaaS-Pool erstellen und ein Subnetz auswählen, in dem sich alle Mitglieder dieses Pools befinden. Tom muss eine virtuelle IP-Adresse (VIP) hinzufügen und diesen VIP dem Pool zuweisen, den er erstellt hat. Tom kann dies auch über die Befehlszeile oder über APIs ausführen. Externe Clients für Tom-Server können eine Verbindung zu dieser VIP-Adresse herstellen, die auf dem zugewiesenen Citrix ADC gehostet wird. Citrix ADC verteilt alle Anforderungen an die Poolmitglieder an den konfigurierten Ports.

LBaaS-Poolmitglieder sind die Server mit Lastenausgleich, die dem ausgewählten Pool hinzugefügt werden. Tom kann jedem dieser Mitglieder ein Gewicht und einen Port zuweisen.

Gesundheitsmonitore werden verwendet, um die Gesundheit und das reibungslose Funktionieren aller Poolmitglieder zu überwachen. Tom kann in OpenStack eine Vorlage für die Systemüberwachung erstellen, indem er die Limits für Verzögerungen, Timeout und Wiederholungsversuche festlegt und bei Erfolg auch die Methode, den URL-Pfad und die erwarteten HTTP-Codes angibt. Nach dem Erstellen eines Monitors muss Tom den Monitor dem zuvor erstellten Pool zuordnen.

Weitere Informationen zum Erstellen von Pools und anderen LBaaS-Konfigurationsaufgaben in OpenStack finden Sie in der OpenStack-Dokumentation.

> **Wichtig!**
>
> LBaaS V1 wird in Liberty-Version von OpenStack nicht unterstützt. Weitere Informationen finden Sie unter OpenStack Release Notes.

Konfigurieren von LBaaS V2 über die Befehlszeile

February 5, 2024

LBaaS V2 unterstützt SSL-Offload mit von **Barbican** verwalteten Zertifikaten, Zertifikatspaketen (einschließlich zwischengeschalteter Zertifizierungsstellen), SNI-Unterstützung sowie den regulären Lastausgleichsfunktionen. LBaaS V2 unterstützt nur die Befehlszeilenschnittstelle zur Ausführung von Konfigurationsaufgaben. LBaaS V2 API-Implementierungen werden über Neutron LBaaS-Befehle durchgeführt.

> **Hinweis**
>
> Laden Sie Zertifikat und Schlüssel zum **Barbican-Dienst** hoch, wenn Sie eine SSL-Offloading-

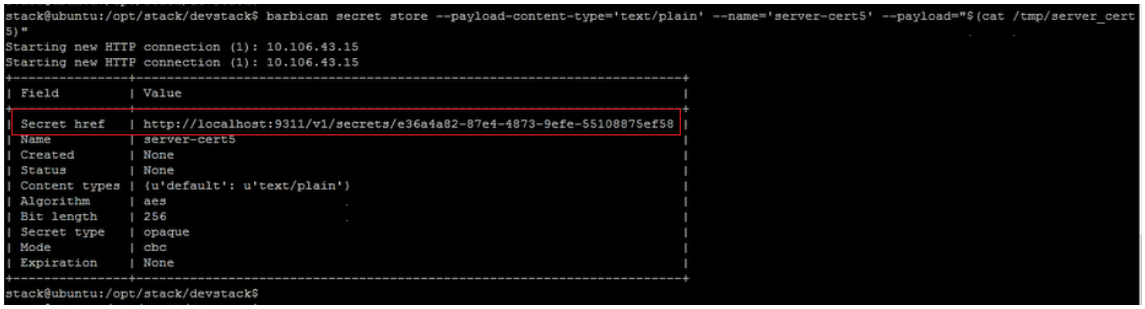
> Funktion benötigen. Führen Sie die Schritte 1, 2 und 3 aus, wenn SSL-Offloading unterstützt wird, andernfalls fahren Sie mit Schritt 4 fort, um einen Load Balancer, einen Listener, einen Pool und ein Mitglied zu erstellen.

1. Laden Sie das Zertifikat mit dem folgenden Befehl in den **Barbican**-Dienst hoch:

```
barbican secret store --payload-content-type <content_type> --name
    <certificate_name> --payload<certificate_location>
<!--NeedCopy-->
```

Beispiel:

```
barbican secret store --payload-content-type='text/plain' --name='
   hp_server_certificate' --payload=" hp_server/tmp/
   server_certificate"
<!--NeedCopy-->
```



2. Laden Sie den Schlüssel mit dem folgenden Befehl in den **Barbican**-Dienst hoch:

```
barbican secret store --payload-content-type <content_type> --name
    <key_name> --payload<key_location>
<!--NeedCopy-->
```

Beispiel:

```
barbican secret store -- payload-content-type='text/plain' --name=
   'shp_server_key' --payload="hp-server/tmp/server_key"
<!--NeedCopy-->
```

> **Hinweis**
>
> Wenn Sie diese beiden **Barbican-Befehle** ausführen, um das Zertifikat und den Schlüssel

> zu laden, geben die Felder Secret href einen Speicherort oder eine URL an. Hier werden das Zertifikat und der Schlüssel auf dem System gespeichert, auf dem OpenStack installiert ist. Kopieren Sie diese Links und geben Sie diese Links als Parameter an, wenn Sie den Container im **Barbican-Dienst** in Schritt 3 erstellen.

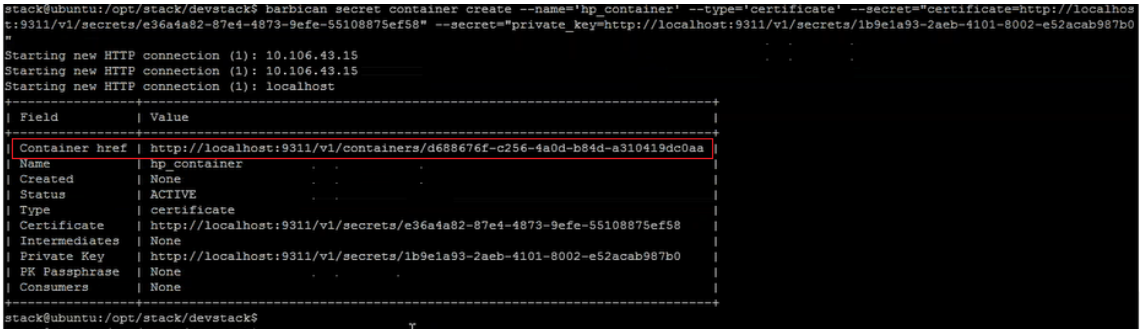
3. Erstellen Sie mit dem folgenden Befehl einen Container im **Barbican**-Dienst , um das Zertifikat und den Schlüssel zu speichern:

   Ersetzen Sie im Befehl mit der URL, die Sie beim Hochladen des Zertifikats aus dem Feld Secret href erhalten haben. Ersetzen Sie in ähnlicher Weise mit der URL, die Sie beim Hochladen des Schlüssels aus dem Feld Secret href erhalten haben.

   ```
   barbican secret container create --name<container_name> --type<
       container_type> --secret<certificate_url> --secret<key_url>
   <!--NeedCopy-->
   ```

   Beispiel:

   ```
   barbican secret container create --name='hp_container' --type='
       certificate' --secret="`certificate=http://localhost:9311/v1/
       secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --secret="
       private_key=http://localhost:9311/v1/secrets/1b9e1a93-2aeb
       -4101-8002-e52acab987b0`"
   <!--NeedCopy-->
   ```

   Kopieren Sie den Wert des Containers href. Sie müssen den Link zum Container angeben, wenn Sie den Listener in Schritt 6 erstellen.

4. Legen Sie die Umgebungsvariablen in OpenStack fest. Die Variablen ermöglichen es den OpenStack-Clientbefehlen, mit den OpenStack-Diensten zu kommunizieren.

   Beispiel:

   export OS_PASSWORD-hp

   export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/

   export OS_USERNAME=hp_user

   export OS_TENANT_NAME=hp

export OS_IDENTITY_API_VERSION=2.0

export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"

```
stack@ubuntu:/opt/stack/devstack$ export OS_PASSWORD=hp
stack@ubuntu:/opt/stack/devstack$ export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/
stack@ubuntu:/opt/stack/devstack$ export OS_USERNAME=hp_user
stack@ubuntu:/opt/stack/devstack$ export OS_TENANT_NAME=hp
stack@ubuntu:/opt/stack/devstack$ export OS_IDENTITY_API_VERSION=2.0
stack@ubuntu:/opt/stack/devstack$ export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"
stack@ubuntu:/opt/stack/devstack$
```

> **Hinweis**
>
> Legen Sie diese Variablen für jede SSH-Sitzung fest, bevor Sie andere Befehle ausführen. Weitere Hinweise zu OpenStack-Umgebungsvariablen finden Sie unter OpenStack-Umgebungsvariablen.

5. Erstellen Sie einen Load Balancer mit dem folgenden Befehl:

```
neutron lbaas-loadbalancer-create --name <loadbalancer-name>  <
    subnet-name> --provider <netscaler>
<!--NeedCopy-->
```

Beispiel:

```
neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --
    provider netscaler
<!--NeedCopy-->
```

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
Created a new loadbalancer:
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| admin_state_up      | True                                 |
| description         |                                      |
| id                  | 746d730b-3b63-418f-a816-d8dd5472963c |
| listeners           |                                      |
| name                | hp-lb-test                           |
| operating_status    | OFFLINE                              |
| provider            | netscaler                            |
| provisioning_status | PENDING_CREATE                       |
| tenant_id           | 0f30b93cd0cd4482b92d033e1628aa8f     |
| vip_address         | 15.0.0.27                            |
| vip_port_id         | 36636748-15c1-4ec3-9328-496ee74e64fc |
| vip_subnet_id       | 0bb433c4-4b90-4de0-803f-9df92aa46ac4 |
+---------------------+--------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

Der Status ändert sich von PENDING_CREATE in ACTIVE, nachdem der Load Balancer erfolgreich erstellt wurde.

```
+--------------------------------------+------------+-------------+---------------------+-----------+
| id                                   | name       | vip_address | provisioning_status | provider  |
+--------------------------------------+------------+-------------+---------------------+-----------+
| 0d5e8e17-41c2-41bb-aab5-2b3f8f5af4c5 | hp-lb8     | 15.0.0.25   | ACTIVE              | netscaler |
| 1092f752-aa25-4262-aacc-014725fe2921 | hp_lb3     | 15.0.0.19   | ACTIVE              | netscaler |
| 41dbe490-6d9c-4ce5-8d88-bb55953f5961 | hp-lb7     | 15.0.0.24   | ACTIVE              | netscaler |
| 746d730b-3b63-418f-a816-d8dd5472963c | hp-lb-test | 15.0.0.27   | ACTIVE              | netscaler |
| 9d65f6a4-5be5-44fd-a4bd-0808084557b0 | hp-lb1     | 15.0.0.18   | ACTIVE              | netscaler |
| cf8ee4b7-a9f5-41c5-a76a-cd2520e0a7a3 | hp-lb6     | 15.0.0.23   | ACTIVE              | netscaler |
| f7f7dd6e-28eb-40f2-b26c-e541138c6a06 | hp-lb4     | 15.0.0.20   | ERROR               | netscaler |
+--------------------------------------+------------+-------------+---------------------+-----------+
```

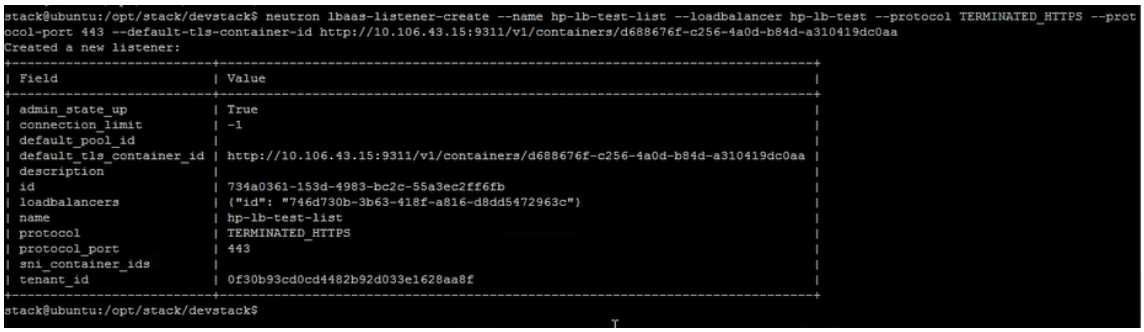

6. Erstellen Sie einen Listener mit dem folgenden Befehl:

```
neutron lbaas-listener-create --loadbalancer <loadbalancer-name>
    --name <listener-name> --protocol <protocol_type> --protocol-
    port <port_number> --default-tls-container-id<container_url>
<!--NeedCopy-->
```

Beispiel:

```
neutron lbaas-listener-create --name hp-lb-test-list  --
    loadbalancer hp-lb-test --protocol TERMINATED_HTTPS --protocol-
    port 443 --default-tls-container-id `http://10.106.43.15:9311/
    v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa`
<!--NeedCopy-->
```

> **Hinweis**
>
> Wenn Sie einen Listener ohne SSL-Offload-Unterstützung erstellen, führen Sie den folgenden Befehl aus, ohne dem Container Speicherorte bereitzustellen:
>
> `neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --protocol-port <port_number>`

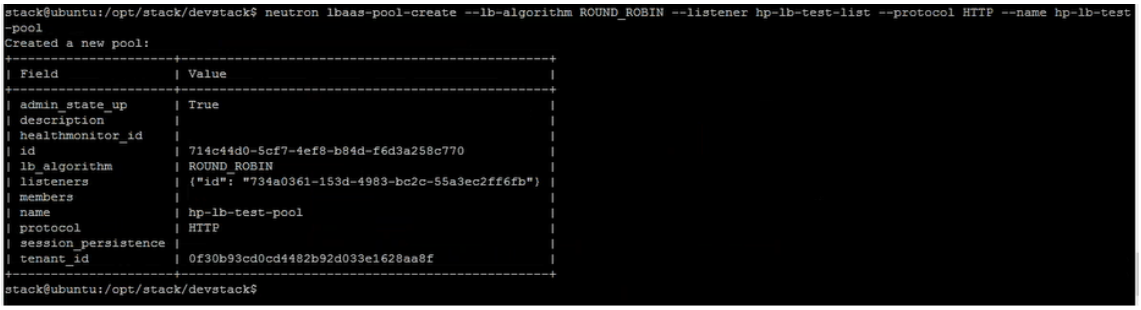


7. Erstellen Sie einen Pool mit dem folgenden Befehl:

```
neutron lbaas-pool-create --lb-algorithm <algorithm_type> --
    listener <listener-name> --protocol <protocol_type> --name <
    pool-name>
<!--NeedCopy-->
```

Beispiel:

```
neutron lbaas-pool-create --lb-algorithm LEAST_CONNECTIONS --
    listener demolistener --protocol http --name demopool
<!--NeedCopy-->
```

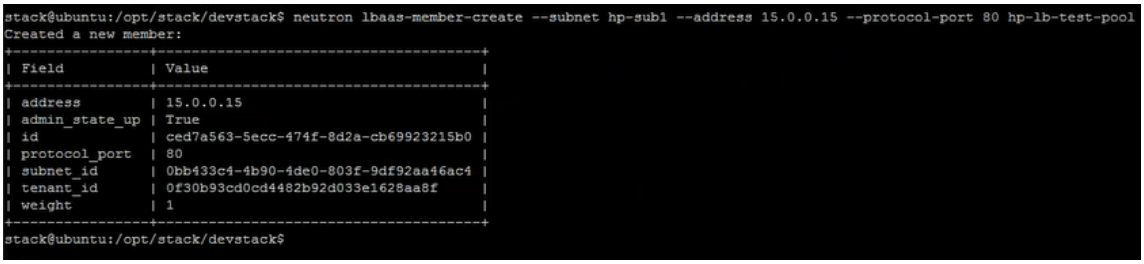



8. Erstellen Sie ein Mitglied mit dem folgenden Befehl:

```
neutron lbaas-member-create  --subnet <subnet-name> --address <ip-address of the web server> --protocol-port <port_number>  <pool-name>
<!--NeedCopy-->
```

Beispiel:

```
neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --protocol-port 80 hp-lb-test-pool
<!--NeedCopy-->
```



Überwachen von OpenStack-Anwendungen in NetScaler ADM

Ihre Mandanten können sich mit ihren OpenStack-Anmeldeinformationen bei NetScaler Application Delivery Management (ADM) anmelden, um VIPs und Pools aus OpenStack von jedem Browser aus zu überwachen. Die URL muss das folgende Format haben:

`http://<mas_ip>/<admin_ui>/mas/ent/html/cc_tenant_main.html`

Wo ist die NetScaler ADM IP-Adresse, die beim OpenStack registriert ist. `mas-ip-address`

> **Hinweis**
>
> - OpenStack-VIPs entsprechen virtuellen Servern in Citrix ADM.
> - OpenStack-Pools entsprechen Dienstgruppen in Citrix ADM.
> - OpenStack Pool-Mitglieder entsprechen Dienstgruppenmitgliedern in NetScaler ADM.

Layer-7-Content Switchings konfigurieren

February 5, 2024

Citrix Application Delivery Management (ADM) orchestriert mit OpenStack, um die Layer 7 (L7) -Switching oder inhaltsbasierte Switching-Funktionen auf Citrix ADC Instanzen zu konfigurieren. Content Switching unterscheidet sich vom einfachen Lastausgleich dadurch, dass bestimmte Arten von Anforderungen an bestimmte Server weitergeleitet werden können. Wenn die L7-Konfigurationen in OpenStack mit einer NetScaler ADC Instanz als Anbieter erstellt werden, weist NetScaler ADM eine NetScaler ADC-Instanz zu und stellt Content Switching und Responder-Konfigurationen entsprechend den L7-Konfigurationen bereit. Die Citrix ADC Instanzen können dann Benutzeranforderungen auf der Grundlage der Anwendungsschicht-Merkmale der Anforderungen verteilen und ausgleichen.

Die OpenStack Layer 7 (L7)-Lastausgleichsfunktion kombiniert Lastausgleich und Content Switching, um eine optimierte Bereitstellung bestimmter Inhaltstypen zu ermöglichen. Dies verbessert die Performance des Load Balancers, indem nur die Richtlinien ausgeführt werden, die für den Inhalt gelten. Layer-7-Lastausgleich erleichtert auch die Effizienz der Anwendungsinfrastruktur. Die Möglichkeit, Inhalte nach Typ, URI oder Daten zu trennen, ermöglicht eine bessere Zuweisung physischer Ressourcen in der Anwendungsinfrastruktur. Beispielsweise `http://example-sports.com/about-us` wird ein Endbenutzer, der surft, von einem Pool von Servern bereitgestellt, die Inhalte über das Unternehmen und die Dienste hosten, während ein Benutzer, zu dem surft, von einem anderen Serverpool bedient `http://example-sports.com/shopping-cart-football` wird, der es den Benutzern ermöglicht, Online-Einkäufe zu tätigen.

Beim L7-Switching wird ein Load Balancer als virtueller Content Switching-Server implementiert, der HTTP-Anforderungen von Benutzern akzeptiert und diese Anforderungen an die Anwendungsserver verteilt. L7-Switching oder Content Switching ermöglicht Ihnen einen zentralen Zugang für den Zugriff auf eine Vielzahl von Back-End-Diensten (z. B. nicht nur auf Webanwendungen, Webservice-Portale, Webmails, sondern auch mobile Verwaltung, Inhalte in verschiedenen Sprachen usw.). Das heißt, Sie können eine öffentliche IP-Adresse für alle Dienste angeben, die Sie Ihren Benutzern anbieten.

Im Gegensatz zum Load Balancing auf niedrigerer Ebene erfordert Layer-7-Switching nicht, dass alle Server im Pool denselben Inhalt haben. Eine Load Balancer-Konfiguration, die L7-Switching verwendet, geht davon aus, dass die Anwendungs- oder Backend-Server aus verschiedenen Pools unterschiedliche Inhalte haben. L7-Switches können Anfragen auf der Grundlage von URI, Host, HTTP-Headern oder irgendetwas anderes in der Anwendungsnachricht richten. Die Anwendungsserver dienen im Wesentlichen bestimmten Arten von Inhalten. Zum Beispiel kann ein Server nur Images bereitstellen, ein anderer kann serverseitige Skriptsprachen wie PHP und ASP ausführen, und ein anderer kann statische Inhalte wie HTML, CSS und JavaScript bereitstellen.

L7 Regeln

Die folgenden Attribute werden in einer Regel für die Auswertung des Datenverkehrs definiert und mit den in der Regel definierten Werten verglichen:

- Hostname: Der Hostname in der HTTP-Anforderung wird mit dem Wertparameter in der Regel verglichen. Zum Beispiel "www.example-sports.com".
- Pfad: Der Pfadteil der HTTP-URI wird mit dem Wertparameter in der Regel verglichen. Zum Beispiel „www.example-sports.com/shopping-cart/football_pump.html"
- file_type: Der letzte Teil des URI wird mit dem value Parameter in der Regel verglichen. Zum Beispiel txt, html, jpg, PNG, xls und andere.
- header: Der im Schlüsselparameter definierte Header wird mit dem Werteparameter in der Regel verglichen.
- Cookie: Das nach dem Schlüsselparameter benannte Cookie wird mit dem Wertparameter in der Regel verglichen. Der Wert des Cookie-Anforderungsheader-Felds enthält ein Paar von Informationen aus Namen und Werten, die für diese URL gespeichert sind. Die allgemeine Syntax lautet wie folgt: Cookie: name=value. Beispielsweise sieht eine Regel, die nach einem Cookie namens "stores"mit dem Wert, der mit "football-"beginnt, wie folgt aus: type = Cookie, compare_type=StartsWith, key = stores value = football-.

Vergleichstypen

Bei der Auswertung des Datenverkehrs vergleicht die L7-Richtlinie die folgenden Ausdrücke mit den in der Regel definierten Attributen.

- regex: Übereinstimmung mit regulären Ausdrücken vom Typ Perl
- starts_with: Zeichenfolge beginnt mit
- ends_with: Die Zeichenfolge endet mit
- enthält: Zeichenfolge enthält
- equal_to: Zeichenfolge entspricht

> **Hinweis**
>
> Der Hostname, der Pfad, der Header und die Cookie-Attribute unterstützen alle Vergleichstypen, aber das Attribut file_type unterstützt nur Regex und equal_to.

L7 Richtlinien

Eine L7-Richtlinie verarbeitet den eingehenden HTTP-Verkehr und gibt einen „wahren“Wert zurück, wenn alle in der Richtlinie definierten Regeln übereinstimmen.

In jeder L7-Richtlinie werden alle Regeln logisch mit einem AND-Operator verknüpft. Eine Anfrage muss allen Regeln entsprechen, damit die Richtlinie einen „wahren“Wert zurückgibt. Die vom Load Balancer ergriffenen Maßnahmen basieren auf dem von der Richtlinie zurückgegebenen Wert. Sie können eine zweite Richtlinie mit derselben Aktion erstellen, um eine logische ODER-Operation zwischen den Regeln zu erreichen.

Sie können beispielsweise eine Richtlinie erstellen, in der die eingehende HTTP-Anforderung die Wörter “EXAMPLE-SPORTS”, “SPORTS-FOOTBALL”oder “EXAMPLE-FOOTBALL”enthalten kann, damit der Load Balancer diese Anforderungen an den Server-Pool des Example-Sports weiterleitet. E-Commerce-Unternehmen, um die angeforderten Inhalte zu bedienen. Sie können eine andere Richtlinie erstellen, die dieselbe Aktion ausführt, aber mit “Beispielsportarten”, “Beispielsportfußball”oder “Beispielfußball”übereinstimmt. Wenn ein Benutzer eine HTTP-Anfrage mit einem dieser sechs Schlüsselwörter sendet, leitet der Load Balancer die Anfrage an den Example-Sports-Server weiter.

Abhängig von den in der Richtlinie definierten Regeln kann eine L7-Richtlinie eine der folgenden Aktionen ausführen:

- An Pool umleiten —Leiten Sie die Anfrage an den Anwendungsserver-Pool weiter, der anhand der mit der L7-Richtlinie verknüpften Regeln identifiziert wird. Das heißt, Sie können eine Anwendungsregel erstellen, um Anfragen entsprechend dem Domainnamen an einen bestimmten Load Balancer-Pool weiterzuleiten. Sie können beispielsweise eine Regel erstellen, die einige Anfragen an example-football.com an pool_1 und andere Anfragen an example-sports-online_purchase.com an pool_2 weiterleitet.
- Zur URL weiterleiten —Senden Sie dem Client eine HTTP-Umleitungsantwort, in der der Location-Antwort-Header den neuen Standort enthält. Der Browser aktualisiert die Adressleiste mit dem neuen Standort und stellt eine neue Anfrage. Die Anwendungsfälle sind vielfältig. Wenn sich beispielsweise die Adresse einer Website geändert hat, können Sie Anfragen an die neue Adresse weiterleiten, anstatt sie zu löschen. Oder Sie können die Benutzer während der Wartung der Website auf eine schreibgeschützte Website umleiten.
- Ablehnen - Ablehnt die Anforderung ab und ergreift keine weiteren Maßnahmen. Sie können beispielsweise eine 401 Unautorisierte Antwort zurückgeben, um den Benutzern den Zugriff auf eingeschränkte Webseiten zu verweigern.

Eine Content Switching-Konfiguration besteht aus einem virtuellen Content Switching-Server, einem Load Balancing-Setup, bestehend aus virtuellen Servern und Diensten für den Lastenausgleich und

Richtlinien für Content Switching. Nachdem Sie den virtuellen Server und die Richtlinien für Content Switching erstellt haben, binden Sie jede Richtlinie an den virtuellen Content Switching-Server. Wenn Sie die Richtlinie an den virtuellen Server für die Content Switching binden, geben Sie den virtuellen Ziel-Lastausgleichsserver an. Wenn eine Anforderung den virtuellen Content Switching-Server erreicht, wendet der virtuelle Server die zugeordneten Content Switching-Richtlinien auf diese Anforderung an. Die Priorität der Richtlinie definiert die Reihenfolge, in der die an den virtuellen Content Switching-Server gebundenen Richtlinien ausgewertet werden.

Jeder Pool mit der Listener-ID kann als Standardpool virtueller Server zugewiesen werden, an die der Datenverkehr umgeleitet wird. Der Pool ist lose an einen Listener gebunden und wird erst durch die Implementierung einer L7-Richtlinie mit einem Listener verknüpft. Ein Pool kann auch direkt unter einem Load Balancer erstellt werden, ohne dass er unbedingt an einen Listener gebunden ist. In einem solchen Fall wird der Pool im Status „pending_create“erstellt. Da die L7-Richtlinien eng mit den Listenern verknüpft sind, muss eine L7-Richtlinie mit der Pool-ID erstellt und implementiert werden, damit der Pool „aktiv“wird und Datenverkehrsanfragen empfängt.

Ein Pool kann von mehreren L7-Richtlinien bedient werden, verbleibt jedoch im Status „aktiv“, wenn ihm mindestens eine Richtlinie zugeordnet ist. Wenn die letzte Richtlinie entfernt wird, wechselt der Pool wieder in den Status „pending_create“, bis eine weitere Richtlinie erstellt und ihr zugeordnet wird. Wenn der Pool selbst entfernt wird, werden alle HTTP-Anfragen, die er sonst empfangen hätte, an den Standardpool umgeleitet.

Zuordnung zwischen OpenStack L7-Richtlinien und Citrix ADC Entitäten

OpenStack	Citrix ADC Entität	Beschreibung
L7-Richtlinie mit der Aktion REDIRECT_TO_POOL	Content Switching-Richtlinie > Content Switching-Aktion	NetScaler ADM erstellt eine Content Switching-Richtlinie, die an den virtuellen Content Switching-Server gebunden ist und einer Content Switching-Aktion zugeordnet ist, die den Zielpool von Anwendungsservern für den Inhaltsabruf und die Präsentation für den Benutzer angibt.

L7-Richtlinie mit der Aktion REDIRECT_TO_URL	Responder-Richtlinie > Responder-Aktion	NetScaler ADM erstellt eine Responderrichtlinie, die an den virtuellen Content Switching-Server gebunden ist und einer Responderaktion zugeordnet ist, die die Ziel-URL angibt, die den Benutzern angezeigt werden soll.
L7-Richtlinie mit Aktion ABLEHNEN	Responder-Richtlinie > Anfrage löschen	NetScaler ADM erstellt eine Responderrichtlinie, die an den virtuellen Content Switching-Server gebunden ist und einer Responderaktion zugeordnet ist, die die Anforderung löscht.

Wenn die Aktion einer L7-Richtlinie, die als “true”ausgewertet wird, Datenverkehr an einen Pool umleitet, der sich im Status “create_pending”befindet, implementiert Citrix ADM den angegebenen Pool zusammen mit einem virtuellen Lastenausgleichsserver. NetScaler ADM erstellt eine Content Switching-Richtlinie aus der L7-Richtlinie und verwendet die entsprechende Content Switching-Aktion, um die Anforderungen an den virtuellen Lastausgleichsserver umzuleiten, der diesem Pool zugeordnet ist. Wenn eine zweite L7-Richtlinie an denselben Pool umgeleitet wird, erstellt NetScaler ADM eine Content Switching-Richtlinie und eine Content Switching-Aktion, um den Datenverkehr an den vorhandenen virtuellen Lastausgleichsserver umzuleiten, der dem Pool zugeordnet ist.

Politische Positionierung

Die Bewertung von L7-Richtlinien in OpenStack wird von ihren Prioritäten bestimmt. In OpenStack werden den Richtlinien standardmäßig Prioritäten in der Reihenfolge zugewiesen, in der sie erstellt wurden. Die zuerst erstellte Richtlinie wird mit „1“nummeriert, und die anschließend erstellten Richtlinien werden fortlaufend nummeriert. Sie können jedoch die Prioritäten der Richtlinien ändern und ihnen unterschiedliche Prioritäten zuweisen. Die Richtlinien werden immer in der Reihenfolge ihrer Prioritäten bewertet. Die erste Richtlinie, die einer bestimmten Anfrage entspricht, wird immer zuerst ausgeführt.

Beachten Sie beim Erstellen von Richtlinien die folgenden Punkte:

- Wenn Sie einer neuen Richtlinie dieselbe Priorität wie einer vorhandenen Richtlinie zuweisen,

erhält die neue Richtlinie diese Priorität. Die Priorität der bestehenden Richtlinie wird herabgesetzt. Falls erforderlich, werden auch die Prioritäten anderer Richtlinien herabgestuft, um die Reihenfolge beizubehalten, in der die Richtlinien bewertet werden.

- Wenn Sie eine neue Richtlinie erstellen, ohne eine Position anzugeben, wird die neue Richtlinie einfach an die Liste angehängt.
- Wenn Sie eine neue Richtlinie erstellen und ihr eine Position zuweisen, die größer ist als die Anzahl der Richtlinien, die sich bereits in der Liste befinden, wird die neue Richtlinie an die Liste angehängt, d. h. die neue Richtlinie hat immer die nächste verfügbare Priorität. Wenn es beispielsweise drei Richtlinien A, B und C mit den Prioritäten 1, 2 und 3 gibt und Sie eine Richtlinie erstellen und eine Priorität von 8 zuweisen, wird die Priorität der neuen Richtlinie auf 4 festgelegt.
- Wenn Sie der Liste eine Richtlinie hinzufügen oder eine Richtlinie aus der Liste löschen, werden die Policy-Positionswerte von 1 aus neu angeordnet, ohne Zahlen zu überspringen. Beispiel: Wenn Richtlinie A, B, C und D Positionswerte von 1, 2, 3 und 4 haben und wenn Sie Richtlinie B aus der Liste löschen, nimmt Richtlinie C nun die zweite Position ein, und Richtlinie D nimmt die dritte Position ein.

In NetScaler ADM gibt es immer eine Standardrichtlinie, die `csvserver` mit einer Priorität von 1 verknüpft ist. Diese Standardrichtlinie gibt die Anzahl der TCP-Verbindungen an, die zu einem bestimmten Zeitpunkt `lbvserver` verarbeitet werden. Wenn die entsprechenden Responderrichtlinien und Inhaltswechselrichtlinien in Citrix ADC erstellt werden, wird ihnen daher immer eine Priorität 1 zugewiesen, die größer ist als die Priorität der entsprechenden L7-Richtlinie. Wenn beispielsweise eine L7-Richtlinie mit der Priorität 1 ausgewertet wird und eine Content Switching-Richtlinie mit der Priorität 2 erstellt wird. In ähnlicher Weise wird eine L7-Richtlinie mit einer Priorität von 2 ausgewertet und eine Responderrichtlinie mit einer Priorität von 3 erstellt.

In OpenStack wird zuerst die Richtlinie “Reject”oder “redirect_to_url”ausgewertet, und dann wird die Richtlinie “redirect_to_pool”ausgewertet. In einer NetScaler ADC Instanz werden die Responderrichtlinien immer zuerst ausgewertet, um entweder die Anforderung zu löschen oder dem Benutzer eine umgeleitete Webadresse zu präsentieren, und die Content Switching-Richtlinien werden zuletzt ausgewertet. Diese Reihenfolge der Auswertung führt normalerweise zu keinem Konflikt, wenn sich die Content Switching- und Responder-Richtlinien gegenseitig ausschließen. Das heißt, zwei L7-Richtlinien dürfen keine identischen Ausdrücke haben. Die abgeleiteten Ausdrücke werden in den Content Switching- und Responder-Richtlinien hinzugefügt, um solche Konflikte zu vermeiden. Schreiben Sie beispielsweise einen Ausdruck, um alle Anfragen an “sports-football.com”abzulehnen, und einen anderen Ausdruck, um Anfragen an “example-sports-football.com”zuzulassen. Erstellen Sie die L7-Richtlinien, so dass alle Responder-Richtlinien, die die Anforderung ablehnen, oben in der Evaluierungsliste angeordnet sind, gefolgt von den Responder-Richtlinien für Web Direct, gefolgt von den Content Switching-Richtlinien.

In NetScaler ADM gibt es immer eine Standardrichtlinie, die `csvserver` mit einer Priorität von 1 verknüpft ist. Diese Standardrichtlinie gibt die Anzahl der TCP-Verbindungen an, die zu einem bestimmten Zeitpunkt `lbvserver` verarbeitet werden. Wenn die entsprechenden Responder- und Content Switching-Richtlinien in NetScaler ADC erstellt werden, wird ihnen daher immer eine Priorität 1 zugewiesen, die größer ist als die Priorität der entsprechenden L7-Richtlinie. Wenn beispielsweise eine L7-Richtlinie mit der Priorität 1 ausgewertet wird und eine Content Switching-Richtlinie mit der Priorität 2 erstellt wird. In ähnlicher Weise wird eine L7-Richtlinie mit einer Priorität von 2 ausgewertet und eine Responderrichtlinie mit einer Priorität von 3 erstellt.

In OpenStack wird zuerst die Richtlinie "Reject"oder "redirect_to_url"ausgewertet und dann die Richtlinie "redirect_to_pool"ausgewertet. In NetScaler ADC werden die Responderrichtlinien immer zuerst ausgewertet, um entweder die Anforderung zu löschen oder dem Benutzer eine umgeleitete Webadresse zu präsentieren, und die Content Switching-Richtlinien werden zuletzt ausgewertet. Diese Reihenfolge der Auswertung führt normalerweise zu keinem Konflikt, wenn sich die Content Switching- und Responder-Richtlinien gegenseitig ausschließen. Das heißt, keine zwei L7-Richtlinien haben ähnliche Ausdrücke. Ähnliche abgeleitete Ausdrücke werden in den Responder- und Content Switching-Richtlinien hinzugefügt, um solche Konflikte zu vermeiden. Schreiben Sie beispielsweise einen Ausdruck, um alle Anfragen an "sports-football.com"abzulehnen, und einen anderen Ausdruck, um Anfragen an "example-sports-football.com"zuzulassen. Erstellen Sie die L7-Richtlinien, so dass alle Responder-Richtlinien, die die Anforderung ablehnen, oben in der Evaluierungsliste angeordnet sind, gefolgt von den Responder-Richtlinien für Web Direct, gefolgt von den Content Switching-Richtlinien.

Konfigurationsaufgaben

Die L7-Richtlinien- und Aktionsimplementierungen werden über Neutron LBaaS-Befehle ausgeführt.

Legen Sie die Umgebungsvariablen in OpenStack fest und erstellen Sie den Load Balancer (z. B. LB1). Nachdem der Load Balancer erfolgreich erstellt wurde, erstellen Sie den Listener und die Pools (z. B. L1, P1 und P2) und fügen Sie den Pools Mitglieder und Monitore hinzu. Beispielsweise ist P1 der Standardpool für L1, während P2 der Pool ist, der an LB1 gebunden ist und die Anwendungsserver verwaltet.

Weitere Informationen zum Konfigurieren von LBaaS V2 mithilfe der Befehlszeile finden Sie unter Konfigurieren von LBaaS V2 mit der Befehlszeile.

Mit den folgenden Befehlen werden die Richtlinien erstellt und die spezifischen Aktionen definiert:

L7-Richtlinie erstellen, um Anforderungen zu löschen

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action<action-name>
```


Beispiel:

neutron lbaas-l7policy-create –name policy11 –action REJECT –listener L1

Der obige Befehl erstellt Policy11, eine Responder-Richtlinie, und bindet sie an den Content Switching-Server, um Anfragen abzulehnen. Da für diese Richtlinie keine Regel erstellt wurde, wird die Richtlinie als „falsch“ausgewertet und die Anfrage wird abgelehnt.

Erstellen einer L7-Richtlinie, um Anforderungen an eine bestimmte URL umzuleiten

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action <action-name> --redirect-url <redirect-url>
```

Beispiel:

neutron lbaas-l7policy-create –name policy12 –action REDIRECT_TO_URL –listener admin-list1 –redirect-url `http://example-sports/about-us.html`

Der obige Befehl erstellt eine Responderaktion, um Anforderungen an eine URL umzuleiten, erstellt eine Responderrichtlinie mit Aktion und bindet diese Richtlinie an den virtuellen Content Switching-Server.

```
neutron lbaas-l7rule-create --type HOST_NAME --compare-type CONTAINS --
    value <value-string> <L7 policy name>

neutron lbaas-l7rule-create --type PATH --compare-type CONTAINS --value
     <value-string> <L7 policy name>
```

Die beiden oben genannten Regeln können mit einem AND-Operator verbunden werden, um den Ausdruck für die Responderrichtlinie abzuleiten.

Erstellen einer L7-Richtlinie zum Umleiten von Anforderungen an einen Pool

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action <action-name> --redirect-pool <redirect-pool
    >
```

Beispiel:

neutron lbaas-l7policy-create –name policy13 –action REDIRECT_TO_POOL –listener admin-list1 –redirect-pool admin-pool2

Wenn dies die erste L7-Richtlinie ist, implementiert der obige Befehl P2 zusammen mit LB1, erstellt die Content Switching-Umleitungsaktion und leitet die Anforderungen an LB1 um. Wenn P2 bereits vorhanden ist, erstellt der Befehl die Content Switching-Umleitungsaktion und leitet die Anforderungen an LB1 um.

Manuelles Provisioning von NetScaler ADC VPX Instanz auf OpenStack

February 5, 2024

In einigen Unternehmensnetzwerken können NetScaler ADC VPX-Instanzen aus Sicherheitsgründen keine Verbindung zum Citrix Lizenzserver herstellen, um die Lizenzen automatisch herunterzuladen. In einem solchen Szenario müssen Sie NetScaler ADC VPX Instanzen manuell auf der OpenStack-Plattform bereitstellen. Laden Sie mit dem Lizenzzugangscode, den Sie von Citrix erhalten haben, die entsprechende NetScaler ADC VPX-Lizenz herunter und speichern Sie sie auf Ihrem lokalen System.

So stellen Sie die NetScaler ADC VPX Instanz manuell in OpenStack bereit:

1. Installieren der Citrix ADC -Treibersoftware und Registrieren von Citrix Application Delivery Management (ADM) auf OpenStack
    a) Navigieren Sie in NetScaler ADM zu **Orchestration** > **Cloud Orchestration** > **OpenStack**.
    b) Klicken Sie auf **OpenStack-Einstellungen konfigurieren**. Auf der Seite **OpenStack-Einstellungen konfigurieren** können Sie die Parameter für die Konfiguration von OpenStack in Citrix ADM festlegen. Sie haben hier zwei Optionen: **Standard** und **Benutzerdefiniert**.
    c) Wählen Sie **Standard**, wenn die OpenStack-Dienste auf Standardports laufen.
2. **Navigieren Sie zu**Orchestration > **Cloud Orchestration**** > **OpenStack**und klicken Sie auf Deployment Settings.**
    a) **Verwaltungsnetzwerk** : Wählen Sie das Verwaltungsnetzwerk in OpenStack aus, mit dem das automatisch bereitgestellte Citrix ADC VPX verbunden ist.
    b) **Profilname** —wählen Sie das Profil aus der Dropdownliste aus. NetScaler ADM verwendet das in diesem Profil enthaltene Kennwort, um neue automatisch bereitgestellte NetScaler ADC VPX Instanzen zu konfigurieren.
    c) Citrix ADC VPX Image in Glance: Wählen Sie im OpenStack Glance das Citrix ADC VPX Image aus, das zum Erstellen einer Citrix ADC VPX-Instanz verwendet wird. In der Dropdownliste werden nur die Images angezeigt, die auf OpenStack Glance vorhanden sind.
3. Navigieren Sie in NetScaler ADM zu **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Service Packages**, und klicken Sie dann auf **Hinzufügen**.
4. Geben Sie auf der Seite **Service Package** die folgenden Parameter an:
    a) **Name** - Name für das Servicepaket. Geben Sie beispielsweise SVC-PKG-GOLD ein.
    b) **Citrix ADC Instanz Allocation** : Wählen Sie **Dediziert** oder **Partitioniert** als Typ der Instanzzuweisung, die im Servicepaket definiert ist.

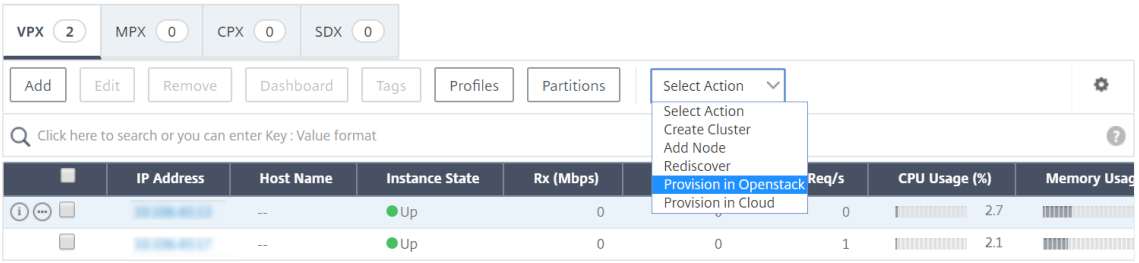
c) **Citrix ADC Instanz Provisioning**: Wählen Sie **Instanz OnDemand** erstellen, um Citrix ADC Instanzen während der Konfiguration selbst zu erstellen.

d) **Auto Provision Platform** —wählen Sie **OpenStack Compute**. Standardmäßig wird Citrix ADC VPX als Instanztyp ausgewählt.

e) **OpenStack Tenants/Placement Policies zuweisen**—Abschnitt, klicken Sie unter OpenStack Tenants auf **Hinzufügen**und wählen Sie den Mandanten aus.

f) Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig**.

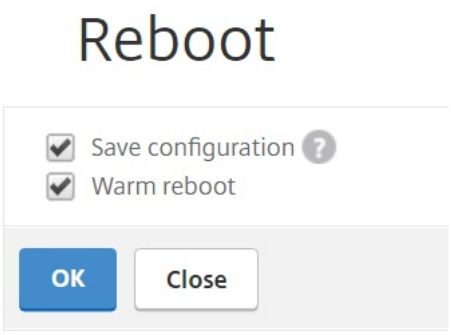
5. Navigieren Sie zu **System** > **Systemverwaltung** > **Systemeinstellungen ändern** und wählen Sie **http** aus der Dropdownliste aus.
6. Navigieren Sie zu **Netzwerke** > **Instanzen** > **Citrix ADC VPX**.
7. Klicken Sie auf der Seite **NetScaler ADC VPX** auf die Dropdownliste **Admin**, und wählen Sie **Gerät bereitstellen**aus.



a) Geben Sie auf der Seite **Device Provisioning** den Namen des Geräts ein, und wählen Sie das Servicepaket aus, das Sie im vorherigen Schritt erstellt haben.

b) Klicken Sie auf **OK**.

8. **Navigieren Sie zum**Tab Orchestration**>**Cloud Orchestration**>**OpenStack > Anfragen**.** Wählen Sie die Anfrage aus und klicken Sie auf **Aufgaben**, um die Aufgaben anzuzeigen. Wenn sich der Status der Aufgabe in **Fertig**ändert, bedeutet dies, dass NetScaler ADC VPX in NetScaler ADM bereitgestellt wird.
9. Navigieren Sie zu**Netzwerke** >**Instanzen** >**Citrix ADC VPX**, um zu überprüfen, ob die Citrix ADC VPX Instanz auf der Seite Citrix ADC VPX angezeigt wird.
10. Klicken Sie auf die NetScaler ADC VPX Instanz. Wenn die NetScaler ADC VPX-Instanz in Ihrem Browserfenster geöffnet wird, melden Sie sich bei der Instanz an. Navigieren Sie zu **Konfiguration** > **System** > **Lizenzen**, und fügen Sie die neue Lizenz manuell hinzu. Weitere Informationen zum Hinzufügen einer neuen Lizenz finden Sie unterNetScaler ADC Licensing Overview.
11. Starten Sie die NetScaler ADC VPX Instanz neu.



12. Nach einigen Minuten können Sie sich bei OpenStack anmelden und unter**System** >**Instanzen**sehen Sie, dass die NetScaler ADC VPX Instanz auf OpenStack bereitgestellt wird.
13. LBaaS V2 API-Implementierungen werden über Neutron LBaaS-Befehle durchgeführt. Verbinden Sie sich mit einem beliebigen Neutron-Client und führen Sie die Konfigurationsaufgaben aus Weitere Informationen zum Ausführen von Konfigurationsbefehlen finden Sie unterKonfigurieren von LBaaS V2 mit der Befehlszeile.

Provisioning der NetScaler ADC VPX Instanz auf OpenStack mit StyleBook

February 5, 2024

Im OpenStack-Orchestrierungs-Workflow verwendet NetScaler Application Delivery Management (ADM) jetzt das `os-cs-lb-mon` StyleBook, um LBaaS-Konfigurationen auf NetScaler ADC-Instanzen bereitzustellen, die dem OpenStack-Mandanten zugewiesen sind. Für jeden vom OpenStack-Benutzer erstellten Load Balancer wird ein Konfigurationspaket erstellt.

Die Verwendung von StyleBooks zur Konfiguration in einem OpenStack-Workflow bietet folgende Vorteile:

- Bessere Visualisierung durch Anzeigen aller Konfigurationsobjekte.
- Zuverlässigkeit durch Rollback.
- Unterstützung für verschiedene NetScaler ADC Instanztypen (NetScaler ADC HA, Partitionen, VPX, CPX, MPX und andere.)
- Anpassung mithilfe Ihrer eigenen StyleBooks zur Bereitstellung der Konfiguration für OpenStack-Mandanten.

Navigieren Sie als Citrix ADMinistrator zu **Anwendungen** > **Konfigurationen, um das Konfigurationspaket** anzuzeigen, das auf der NetScaler ADC Instanz bereitgestellt wird.
Sie können die folgenden Aufgaben ausführen:

- Scrollen Sie, um das für den Load Balancer bereitgestellte `os-cs-lb-mon` Konfigurationspaket anzuzeigen.
- Klicken Sie im `os-cs-lb-mon` StyleBook-Bedienfeld auf **View Definition**, um die Konfiguration zu überprüfen, die auf den Instanz bereitgestellt wird.
- Klicken Sie auf **Objekt anzeigen**, um die Liste der NetScaler ADC Objekte oder -Entitäten anzuzeigen, die auf den Instanzen bereitgestellt werden.

Punkte, die vor der Provisioning Instanzen mit StyleBooks zu beachten sind

Ab NetScaler ADM 12.1 Build 49.23 wurde die Architektur eines OpenStack-Orchestrierungs-Workflows aktualisiert. Der Workflow verwendet jetzt NetScaler ADM StyleBooks, um NetScaler ADC Instanzen zu konfigurieren. Wenn Sie ein Upgrade auf NetScaler ADM 12.1 Build 49.23 von Version 12.0 oder von Version 12.1 Build 48.18 durchführen, müssen Sie das folgende Migrationsskript ausführen:

```
/mps/scripts/migration_scripts/migrate_configurations.py
<!--NeedCopy-->
```

- Die Ausführung des Migrationsskripts erstellt Konfigurationspakete des `os-cs-lb-mon` StyleBook, die den vorhandenen OpenStack-Konfigurationen entsprechen
- Das Ausführen dieses Migrationsskripts ist obligatorisch, wenn OpenStack-Konfigurationen aus diesen früheren Builds bereitgestellt wurden.
- Sie können neue Konfigurationen für die Instanzen mit dem `os-cs-lb-mon` StyleBook erst bereitstellen, nachdem Sie das Migrationsskript von Version 12.1 Build 49.23 ausgeführt haben.
- Alle von OpenStack aus versuchten Konfigurationen scheitern, bis das Migrationsskript ausgeführt wird.

> **Hinweis**
>
> - Nachdem Sie das Migrationsskript ausgeführt haben, können Sie kein Downgrade auf den vorherigen Build von Citrix ADM durchführen.
> - Stellen Sie sicher, dass Sie die NetScaler ADC -Treiber für OpenStack LBaaS V2 auf die neueste Version aktualisiert haben. Verwenden Sie die Citrix ADC Paketdateien, die zusammen mit dem neuesten Citrix ADM 13.0-Build bereitgestellt werden.

LBaaS V2 API-Implementierungen werden über Neutron LBaaS-Befehle durchgeführt. Stellen Sie eine Verbindung zu einem Neutron-Client her und führen Sie die Konfigurationsaufgaben aus. Weitere Informationen zum Ausführen von Konfigurationsbefehlen finden Sie unterKonfigurieren von LBaaS V2 mit der Befehlszeile.

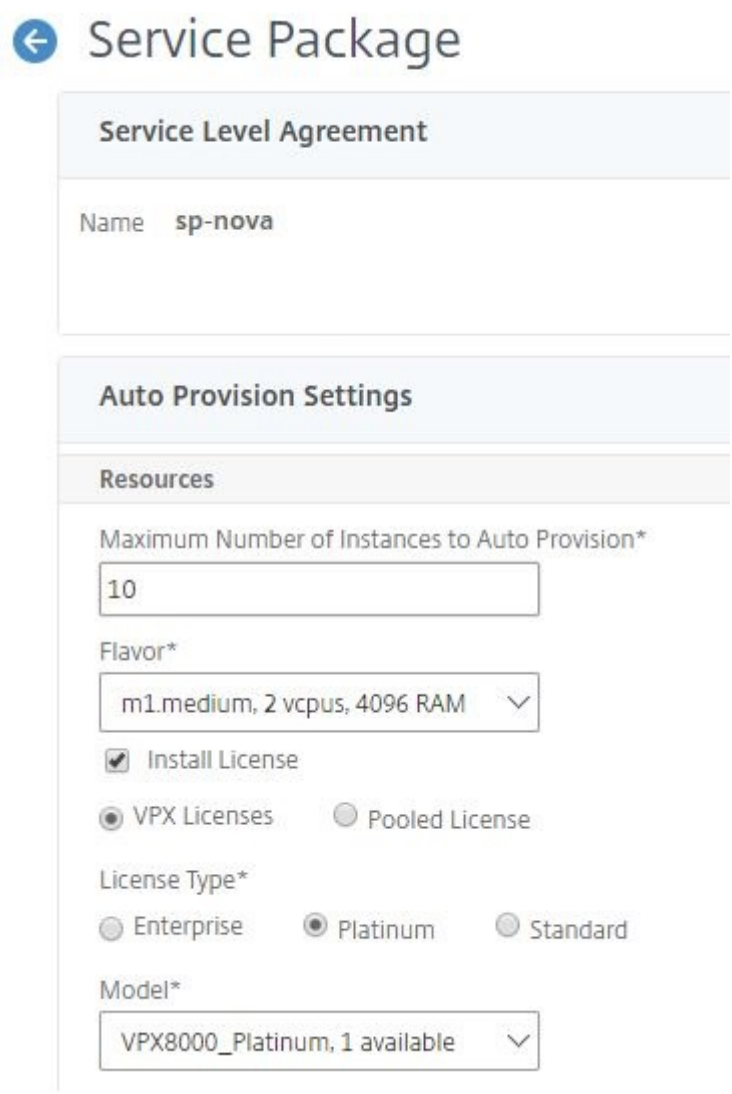
VPX-Ein- und Auscheck-Lizenz und gepoolte Lizenzunterstützung für OpenStack-Umgebung

February 5, 2024

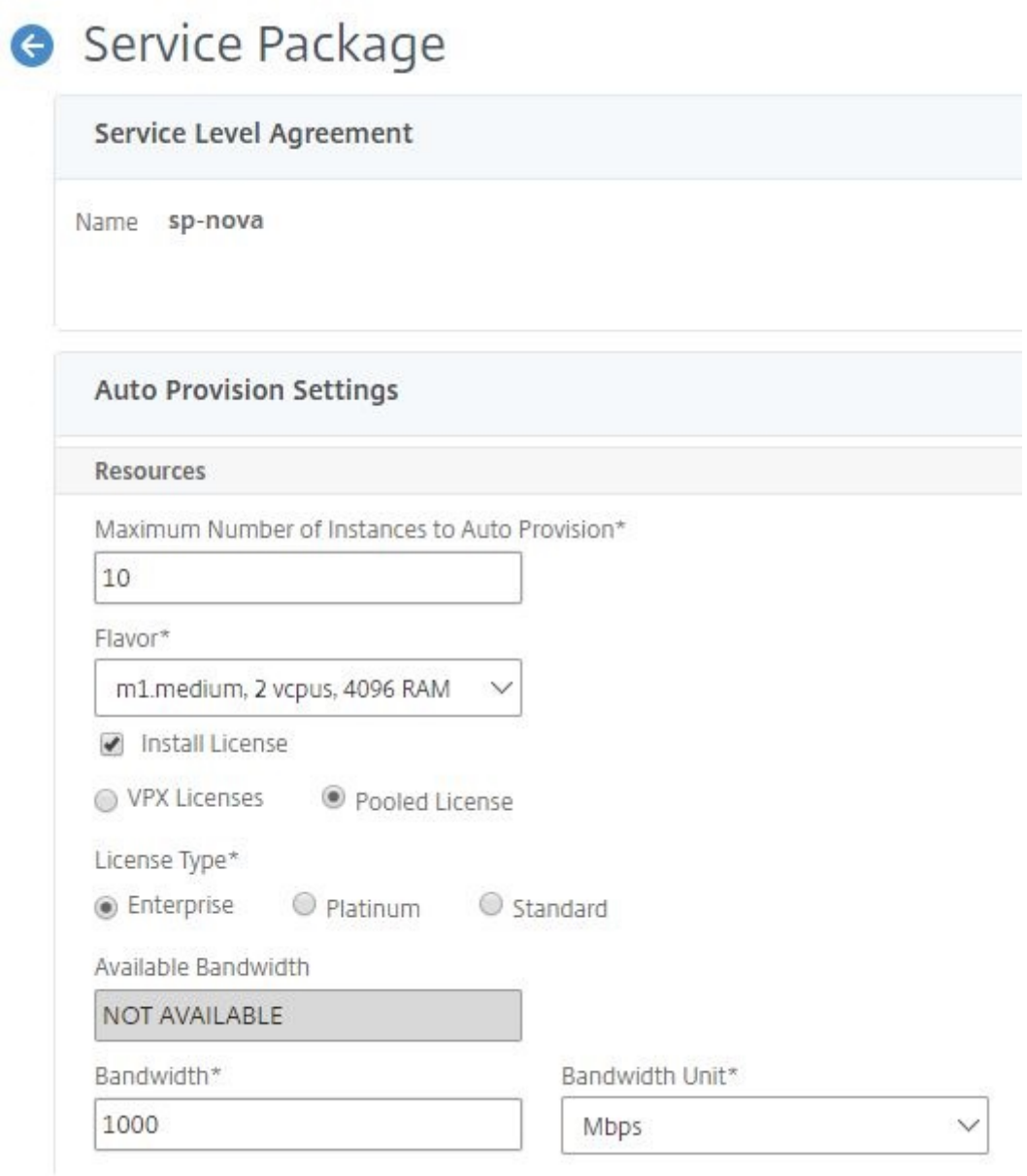
Im OpenStack Orchestrierungsworkflow erstellt Citrix Application Delivery Management (ADM) bei Bedarf Citrix ADC VPX Instanzen, wenn Sie das Servicepaket mit **OpenStack Compute** auswählen. Jetzt wird die Dienstpaketseite in der Orchestration-Funktion in Citrix ADM erweitert, um die Lizenz bereitzustellen, die auf den Citrix ADC VPX Instanzen installiert werden muss, die bei Bedarf erstellt werden. Bei den bereitgestellten Lizenzen kann es sich entweder um eine VPX-Check-in- und Check-Out-Lizenz oder um eine gepoolte Lizenz handeln.

Um dieses Feature verwenden zu können, müssen Sie zuerst die Lizenzen in Citrix ADM hochladen und dann Servicepakete erstellen, die OpenStack Compute verwenden.

- Wenn es sich um eine Ein- und Auscheck-Lizenz handelt, können Sie die zu installierende Lizenz aus den verschiedenen verfügbaren Lizenzen auswählen.



- Wenn es sich um eine Poollizenz handelt, können Sie sowohl die Bandbreite als auch den Typ der zu installierenden Lizenzedition auswählen.



Wenn Sie den ersten Load Balancer mit NetScaler ADM als Anbieter bereitstellen, erstellt NetScaler ADM die NetScaler ADC VPX Instanz und installiert die im Servicepaket angegebene Lizenz auf der neu erstellten Instanz.

Wenn Sie eine vorhandene Load Balancing-Instance löschen, wird diese Instanz außerdem nicht mehr benötigt. Die Instanz wird stillgelegt und die Lizenz wird an Citrix ADM zurückgegeben. Dies ermöglicht eine optimale Nutzung der Lizenzen, die in Citrix ADM verfügbar sind.

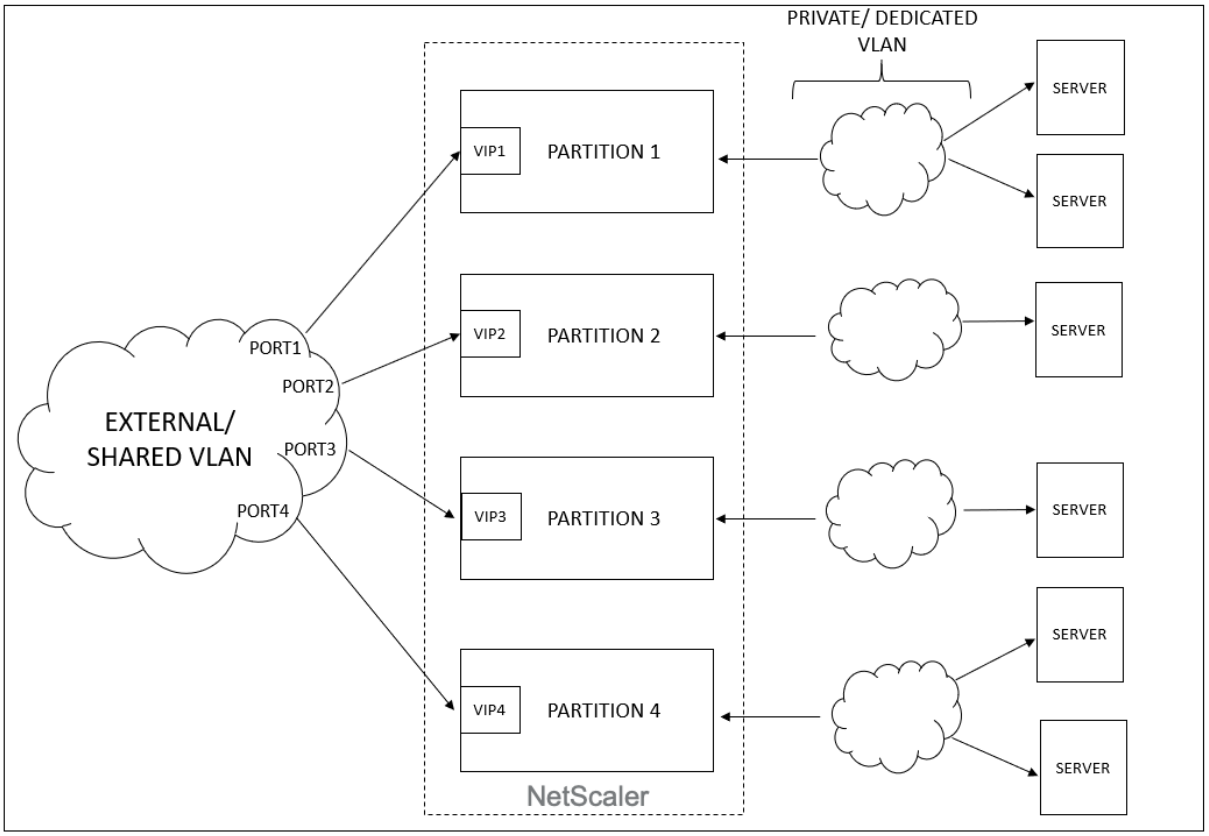
> **Hinweis:**
>
> Wenn Citrix ADM im Hochverfügbarkeitsmodus bereitgestellt wird, sollten Sie berücksichtigen,

> dass die Lizenzen auf das aktuelle aktive oder primäre Citrix ADM MAS-HA-1 hochgeladen werden. Wenn Sie die erste Anforderung bereitstellen und Citrix ADM die Citrix ADC VPX Instanzen erstellt, checkt die Instanz die erforderlichen Lizenzen von MAS-HA-1 aus. Zu einem späteren Zeitpunkt wird davon ausgegangen, dass das sekundäre Citrix ADM MAS-HA-2, das nicht über die Lizenzen verfügt, jetzt aktiv ist. Die ADC VPX-Instanz kann die Lizenz von MAS-HA-2 jetzt nicht auschecken und daher kann die Instanz nicht für neue Benutzer erstellt werden.
>
> Stellen Sie in einem solchen Fall sicher, dass MAS-HA-1 aktiv ist und jetzt der aktuelle primäre Knoten ist. Das heißt, manuelles Failover von Citrix ADM von MAS-HA-2 auf MAS-HA-1. Danach müssen Sie die Konfiguration von OpenStack erneut versuchen, und die Instanzen werden mit den richtigen Lizenzen neu erstellt. Weitere Informationen zur Lizenzunterstützung bei der NetScaler ADM-Hochverfügbarkeitsbereitstellung finden Sie unter Hochverfügbarkeit.

Gemeinsame VLAN-Unterstützung für Admin-Partitionen

February 5, 2024

Für Mandanten, die sich über private Netzwerke verbinden, unterstützt Citrix Application Delivery Management (ADM) Isolationsrichtlinie, sodass jeder Mandant über eine eigene dedizierte Partition, ein dediziertes VLAN und dedizierte Server verfügt. Für Mandanten, die sich von öffentlichen Netzwerken aus verbinden, erfordert ein dediziertes VLAN die Verwendung zu vieler IP-Adressen. Ein gemeinsam genutztes VLAN umgeht dieses Problem, indem eine virtuelle IP-Adresse auf jeder Partition erstellt wird, wodurch ein einzelnes IP-Subnetz erstellt wird.



Wenn ein Mandant eine VIP oder einen Listener konfiguriert, wird auf dem NetScaler ADC Gerät für diesen Mandanten eine Administratorpartition erstellt. Die gesamte Load Balancer-Konfiguration wird auf die erstellte Admin-Partition übertragen. Wenn der Mandant ein gemeinsam genutztes Netzwerk oder ein externes Netzwerk verwendet, um einen Load Balancer zu erstellen, wird das VLAN dieses Netzwerks hinzugefügt und die Sharing-Funktion ist aktiviert. Wenn ein anderer Mandant dasselbe freigegebene Netzwerk verwendet, um seinen Load Balancer zu erstellen, wird das VLAN nicht erneut dem Citrix ADC hinzugefügt, aber das VLAN wird auch an die zweite Partition gebunden. Somit erhält jeder Mandant, der dasselbe gemeinsam genutzte Netzwerk verwendet, eine Partition, die an dasselbe VLAN gebunden ist.

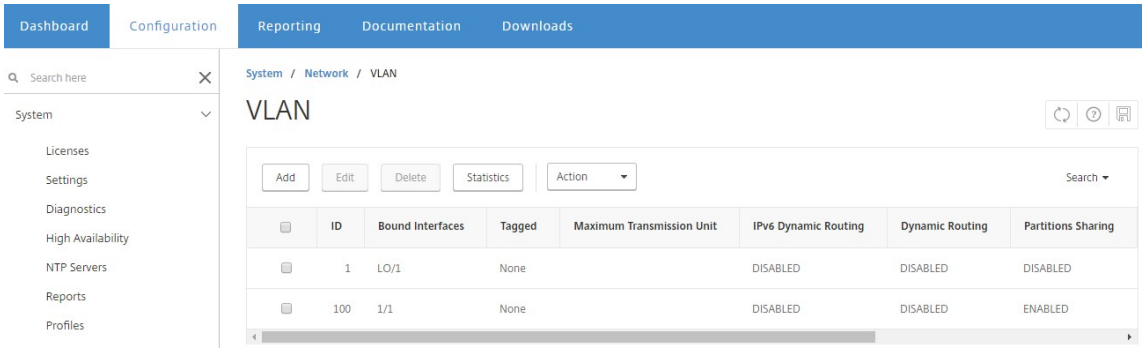
Citrix ADM unterstützt virtuelle Ziel-MAC-Adresse. Wenn Mandanten ein VLAN gemeinsam nutzen, weist Citrix ADM der Partition auf dem Citrix ADC-Gerät unterschiedliche MAC-Adressen zu. Dadurch kann ein VLAN von Partitionen oder von allen Mandanten und allen Verkehrsdomänen gemeinsam genutzt werden.

Konfigurieren von freigegebenem VLAN von der Citrix ADC Instanz

1. Navigieren Sie in einer Citrix ADC Instanz zu **Konfiguration** > **System** > **Netzwerk** > **VLANs**, wählen Sie ein VLAN-Profil aus und klicken Sie auf **Bearbeiten**, um den Partitionsparameter

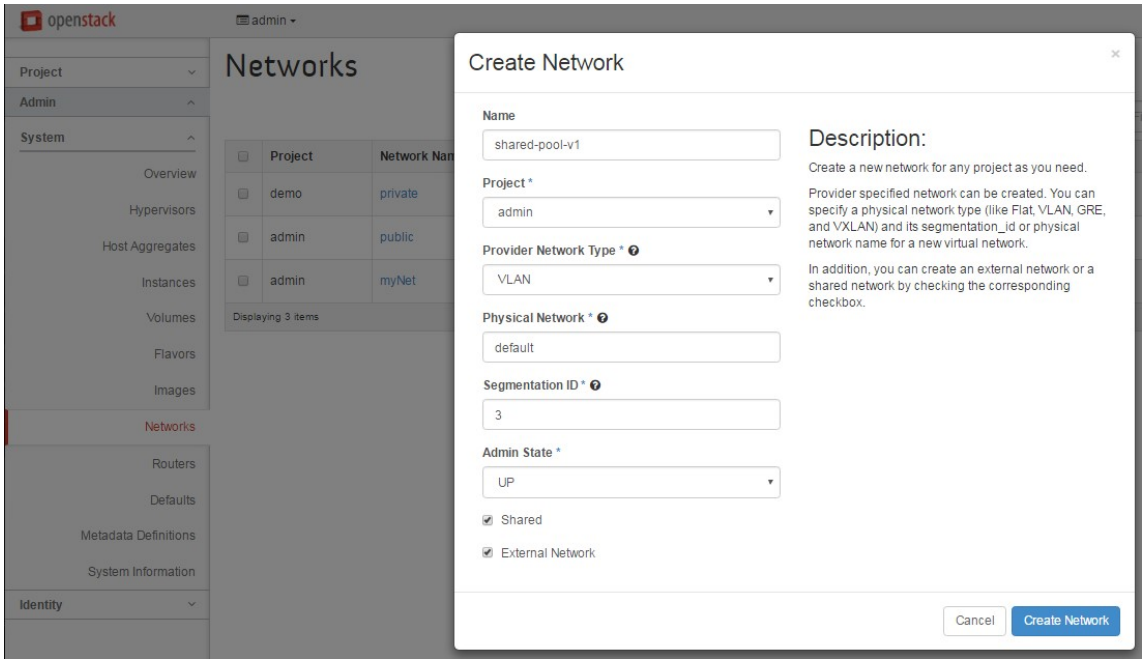
festzulegen.

2. Aktivieren Sie auf der Seite **VLAN konfigurieren** das Kontrollkästchen **Partitions Sharing**.
3. Klicken Sie auf **OK**.



Konfigurieren von freigegebenem VLAN über OpenStack Orchestration

1. Navigieren Sie in OpenStack zu **Admin** > **System** > **Netzwerke** und klicken Sie dann auf **Create Network**.
2. Stellen Sie unter **Create Network**die folgenden Parameter ein:
   a) Name - geben Sie den Namen des Netzwerks ein
   b) Projekt - Wählen Sie ein Projektformular aus der Dropdownliste
   c) Provider-Netzwerktyp: Wählen Sie **VLAN** aus der Dropdownliste aus. Dies definiert, dass das virtuelle Netzwerk als VLAN eingerichtet wird.
   d) Physikalisches Netzwerk —hier wird das physische Standardnetzwerk ausgewählt. Sie können dies bearbeiten.
   e) Admin-Status —standardmäßig ist der administrative Status des Netzwerks UP
   f) Wählen Sie **Gemeinsames** und **Externes** Netzwerk aus, um zu definieren, dass das VLAN gemeinsam genutzt wird und ein externes Netzwerk verwendet.
3. Klicken Sie auf **Netzwerk erstellen**.



Arbeitsablauf zur Testlizenzierung

February 5, 2024

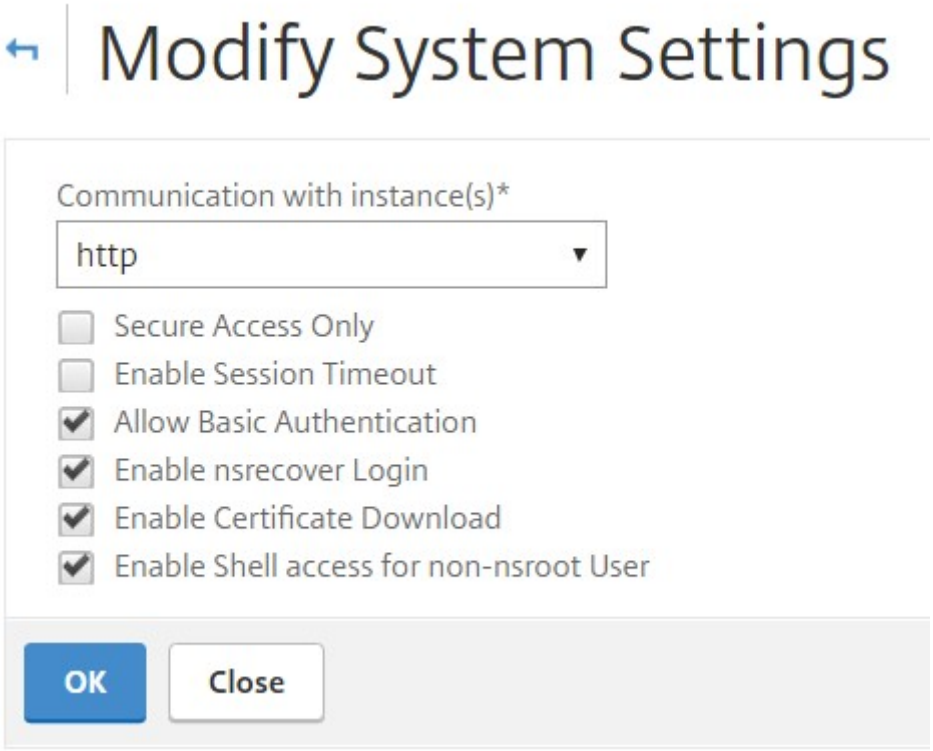
Während der automatischen Bereitstellung der NetScaler ADC VPX Instanz mithilfe von OpenStack Orchestrierung verwendet die NetScaler Application Delivery Management (ADM) OpenStack Compute, um eine NetScaler ADC VPX Instanz zu starten. Die neu bereitgestellte NetScaler ADC VPX-Instanz kontaktiert während der Einrichtung das Citrix Lizenzportal und verwendet den Lizenzzugangscode, um die Lizenzdateien automatisch herunterzuladen und zu installieren.

Test-Lizenzen

Die Mitarbeiter des technischen Supports verwenden Testlizenzen, wenn sie Citrix ADM - und Citrix ADC VPX Geräte vor Ort installieren. Eine Test- oder Testlizenz für Citrix ADC VPX ist 90 Tage gültig. Wenn mehr als ein Citrix ADC ausgewertet oder die Tests nach 90 Tagen verlängert werden müssen, muss eine neue Evaluierungslizenz angefordert werden. Statt der automatischen Installation von Testlizenzdateien bietet Citrix ADM eine alternative Lösung. Sie können die Lizenzdateien manuell herunterladen und auf Citrix ADC VPX installieren, um die Installation der Instanz abzuschließen.

Wenn Citrix ADC VPX keine Verbindung zum Internet herstellen kann, konfigurieren Sie Citrix ADM als Proxyserver für das Citrix Lizenzportal und installieren Sie die Lizenzdateien.

Citrix ADC VPX Instanzen, die über eine Testlizenz verfügen, können nur unter HTTP mit Citrix ADM kommunizieren. Um die HTTP-Kommunikation in Citrix ADM zu konfigurieren, navigieren Sie zu**System> Systemverwaltung**und klicken Sie auf**Systemeinstellungen ändern**. Wählen Sie**http**aus der Dropdownliste aus, um die Kommunikationsmethode festzulegen, und klicken Sie auf**OK**.



Integration mit OpenStack Heat-Services

February 5, 2024

Der OpenStack Neutron LBaaS ermöglicht Core-Load Balancing Services wie Load Balancing, SSL-Offloading und Content Switching für Anwendungen. LBaaS wird über eine REST-API verwaltet, und die API ermöglicht es den Mandanten, REST-Aufrufe zum Erstellen, Aktualisieren und Löschen von LBaaS-Objekten zu tätigen. Da LBaaS Lastenausgleichsdienste bereitstellt, ist die Verwendung der erweiterten NetScaler ADC Funktionen während des Orchestrierungsvorgangs nicht zulässig. Das Citrix ADC Heat-Plug-In überwindet diese Einschränkung.

Heat Orchestrierungs-Service

Der OpenStack Heat Orchestration Service ermöglicht die Bereitstellung komplexer Cloud-Anwendungen auf der Basis von Vorlagen. Das Heat Orchestration Template (HOT) beschreibt die Infrastruktur für eine Cloud-Anwendung in Textdateien, die von Menschen gelesen und geschrieben werden können und mit Tools zur Versionskontrolle verwaltet werden können. YAML, eine strukturierte Sprache, wird verwendet, um diese Vorlagen zu schreiben. Mit der HOT-Vorlage können Sie die meisten OpenStack-Ressourcentypen erstellen und die Beziehungen zwischen den darin definierten Ressourcen spezifizieren. Mit dem Citrix ADC Heat-Plug-In können Sie erweiterte ADC-Funktionen (Application Delivery Controller) auf jeder Citrix ADC Instanz konfigurieren.

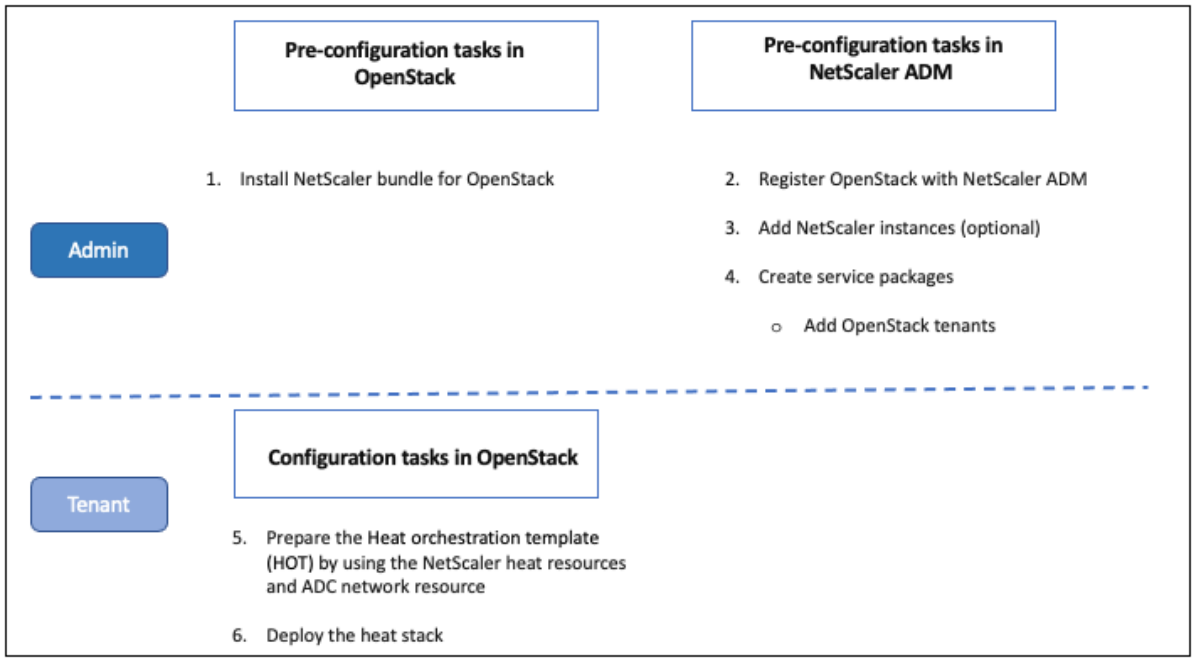
Citrix ADC StyleBooks

Citrix Application Delivery Management (ADM) StyleBooks können zum Erstellen und Konfigurieren von Citrix ADC Funktionen verwendet werden. Genau wie Heat-Vorlagen sind auch die StyleBooks in YAML geschrieben. Für jede Funktionalität können separate StyleBooks erstellt werden, und ein einzelnes StyleBooks kann zum Bereitstellen von Konfigurationen auf mehreren Citrix ADC Instanzen verwendet werden.

Während der Citrix ADC Integration mit OpenStack veröffentlicht Citrix ADM alle Citrix ADM StyleBooks als Ressource im Heat-Service. Dazu gehören sowohl die StyleBooks, die mit Citrix ADM ausgeliefert werden, als auch die StyleBooks, die vom Benutzer zu einem späteren Zeitpunkt erstellt werden.Mit der Vorlage Heat können Sie die erweiterten Funktionen von Citrix ADCs mithilfe dieser StyleBooks-Ressourcen konfigurieren.

Workflow zum Konfigurieren von Citrix ADC Instanzen mit Heat

Das folgende Flussdiagramm veranschaulicht den Workflow für die Bereitstellung des Heatstacks:



Führen Sie die folgenden Aufgaben als Cloud-Administrator aus:

So konfigurieren Sie Heat-Dienste in OpenStack:

1. Citrix ADC Pakete für OpenStack herunterladen

   Installieren Sie die Citrix ADC Pakete in OpenStack. Navigieren Sie in Citrix ADM zu **Downloads**, laden Sie die Citrix ADC -Treiberpakete herunter, enttarnen Sie die Pakete und kopieren Sie den Inhalt des Heatordners im Bundle in das Heat-Engine-Ressourcenverzeichnis in OpenStack. Der Verzeichnispfad lautet wie folgt:
   /opt/stack/heat/heat/engine/resources/netscaler_resources

2. Erstellen Sie einen Abschnitt “netscaler_plugin”in der Datei heat.conf und aktualisieren Sie die folgenden Parameter in diesem Abschnitt:

   [netscaler_plugin]

   a) Wenn die Kommunikation HTTP ist, werden die Parameter wie folgt aktualisiert:

      NMAS_BASE_URI=<http://10.146.103.45:80>

      NMAS_USERNAME=

      NMAS_PASSWORD=

   b) Wenn die Kommunikation https ist, werden die Parameter wie folgt aktualisiert:

      NMAS_BASE_URI=https://common_name_used_in_certificate

      NMAS_USERNAME=<openstack_driver_username

NMAS_PASSWORD=<openstack_driver_password>

SSL_CERT_VERIFY=<True_or_False>

CERT_FILE_PATH=<path_of_the_certificate_file>

Wenn der Benutzer ssl_cert_verify auf "False"setzt, sendet Citrix ADM in den Anforderungsaufrufen Verify=False, wodurch die SSL-Zertifikatüberprüfung deaktiviert wird. Wenn ssl_cert_verify auf "True"gesetzt ist und der Eintrag cert_file_path vorhanden ist, sendet NetScaler ADM diesen Pfad im Parameter verify der request, andernfalls sendet NetScaler ADM Verify=true.

> **Hinweis**
>
> Wenn Sie NetScaler ADM im Modus "Hohe Verfügbarkeit"bereitstellen möchten, aktualisieren Sie die folgenden Parameter in der Datei "heat.conf":
>
> NMAS_BASE_URI= <IP address of the front-end virtual server>

3. Starten Sie den Heat-Service in OpenStack neu.

   Wenn Sie die Citrix ADC Heat-Services in OpenStack neu starten, werden alle definierten Citrix ADM StyleBooks als Ressourcen in Heat importiert. Außerdem werden die Citrix ADC Netzwerkressource und die Zertifikatressource als Citrix ADC Heatressourcen in OpenStack importiert.

4. Registrieren Sie Citrix ADM bei OpenStack.

   a) Navigieren Sie in Citrix ADM zu **Orchestration** > **Cloud Orchestration** > **OpenStack** und klicken Sie auf **OpenStack-Einstellungen konfigurieren**.

   b) Auf der Seite **OpenStack-Einstellungen konfigurieren** können Sie die Parameter für die Konfiguration von OpenStack festlegen. Sie haben hier zwei Optionen: Standard und Benutzerdefiniert.

   c) Wählen Sie **Standard**, wenn die OpenStack-Dienste auf Standardports ausgeführt werden. Geben Sie die folgenden Parameter ein:

      i. IP-Adresse des OpenStack-Controllers

      ii. Admin-Benutzername

      iii. Kennwort

      iv. OpenStack Admin-Mandant

      v. NetScaler ADC-Treiber und Heatkennwort

   > **Hinweis:**

> Dies ist dasselbe Kennwort (NMAS_PASSWORD), das Sie in der Datei heat.conf eingegeben haben.

5. Erstellen Sie Servicepakete und definieren Sie die SLAs mit Ihrem Mandanten.

   Während der OpenStack-Registrierung wird in Citrix ADM für jeden Benutzer ein Mandant erstellt, und die Mandanteninformationen werden sowohl vom LBaaS-Treiber als auch vom Heat-Plug-In verwendet. Das Heat-Plug-In verwendet diese Informationen, um NetScaler ADM zu kontaktieren, um StyleBooks als Heatressourcen in OpenStack zu importieren.

   > **Hinweis**
   >
   > Weitere Informationen zum Erstellen von Servicepaketen und anderen Vorkonfigurationsaufgaben in NetScaler ADM und OpenStack finden Sie unter Integrieren von NetScaler ADM mit OpenStack Platform.

6. Beachten Sie, dass alle relevanten StyleBooks in NetScaler ADM als Ressourcen in OpenStack Heat importiert werden. Beachten Sie außerdem, dass die NetScaler ADC Netzwerkressource und die NetScaler ADC-Zertifikatressource als Ressourcen in OpenStack Heat importiert werden.

   > **Hinweis**
   >
   > Derzeit können Sie nur die StyleBooks verwenden, die mit Citrix ADM ausgeliefert werden.

   Ihr Mandant kann nun die Heat-Vorlage in OpenStack erstellen, die Werte der erforderlichen Heat-Parameter eingeben und den Heat-Stack bereitstellen. Wenn der Heatstack bereitgestellt wird, wird die Konfiguration an Citrix ADM übertragen, und die erforderlichen Citrix ADC Instanzen werden konfiguriert.

Um die Heat-Vorlage vorzubereiten und Heat Stack zu starten:

1. In OpenStack kann der Tenant mithilfe der Heat-Ressourcen eine Heat-Orchestrierungsvorlage (HOT) erstellen.
2. In OpenStack Horizon kann der Mandantenadministrator zu**Project** >**Orchestration** >**Stacks** navigieren, um die Heat-Vorlage zu erstellen und den Heat Stack zu starten. Es gibt zwei Möglichkeiten, HOT zu erstellen:

   - **Datei** —Wählen Sie die aktualisierte Vorlage aus dem lokalen Verzeichnis aus
   - **Direkte Eingabe** - Kopieren Sie den YAML-Inhalt aus der Vorlage und fügen Sie ihn in das Fenster ein

> **Hinweis:**
>
> Nach erfolgreicher Bereitstellung des Stacks kann der Tenant den Stack mithilfe der Change Stack-Vorlage aktualisieren. Die Subnetzinformationen und die virtuelle IP-Adresse (VIP), die ursprünglich bei der Erstellung des Stacks bereitgestellt wurden, können jedoch nicht geändert werden.

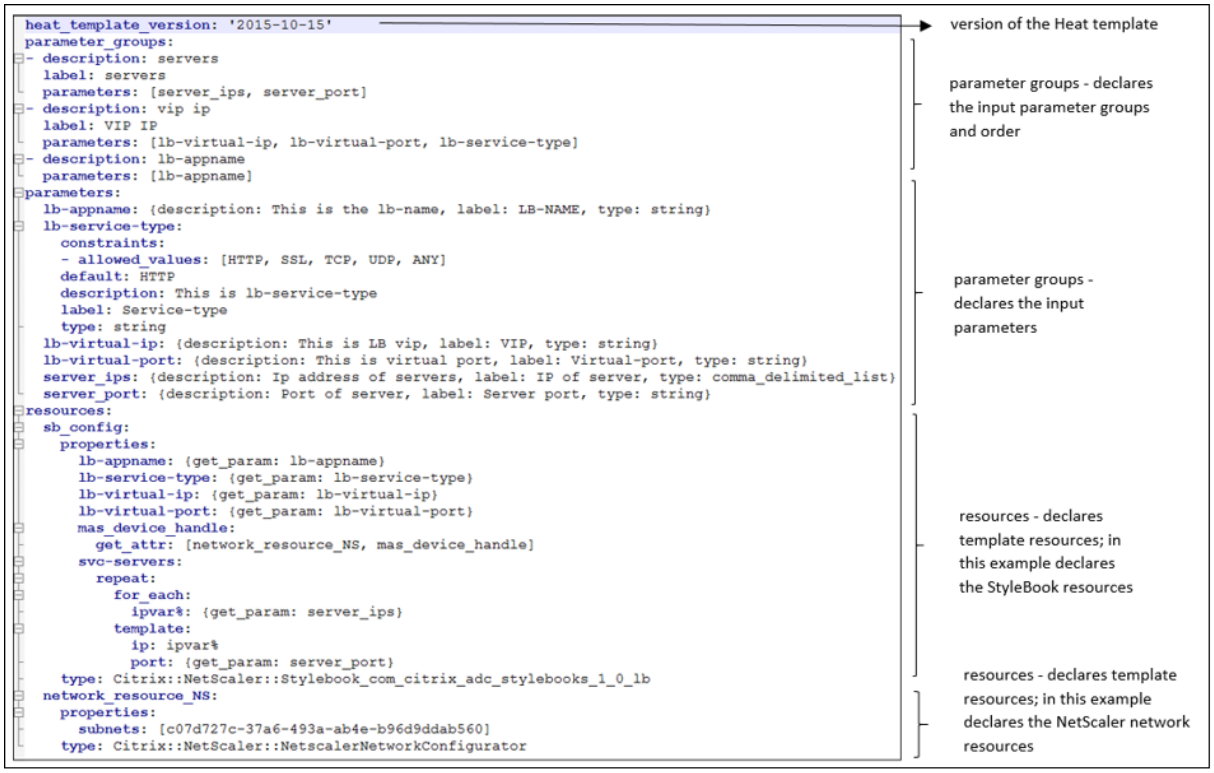
Nachdem der Mandant den Stack bereitgestellt hat, navigieren Sie zu**Orchestration** > **Cloud Orchestration**> **OpenStack** > **Anforderungen** in NetScaler ADM, um die Aufgabenlisten zu beobachten. Navigieren Sie außerdem zu**Anwendungen** >**Konfiguration** in NetScaler ADM, um zu beobachten, dass die NetScaler ADC-Instanzen erfolgreich in Form von StyleBooks-Konfigurationspaketen konfiguriert wurden.

Ein Beispiel für ein NetScaler ADM StyleBooks:

Die folgende Abbildung zeigt ein Beispiel für die Konstruktion eines NetScaler ADM StyleBooks und erläutert kurz die Komponenten. Weitere Informationen zu NetScaler ADM StyleBooks und zur Verwendung der mitgelieferten StyleBooks finden Sie unter StyleBooks.

Ein Beispiel für eine Heatvorlage:

Die folgende Abbildung zeigt die Struktur einer in YAML definierten Heatvorlage und zeigt auf die StyleBooks-Ressourcen und NetScaler ADC Netzwerkressourcen, die als Heat-Ressourcen importiert werden.



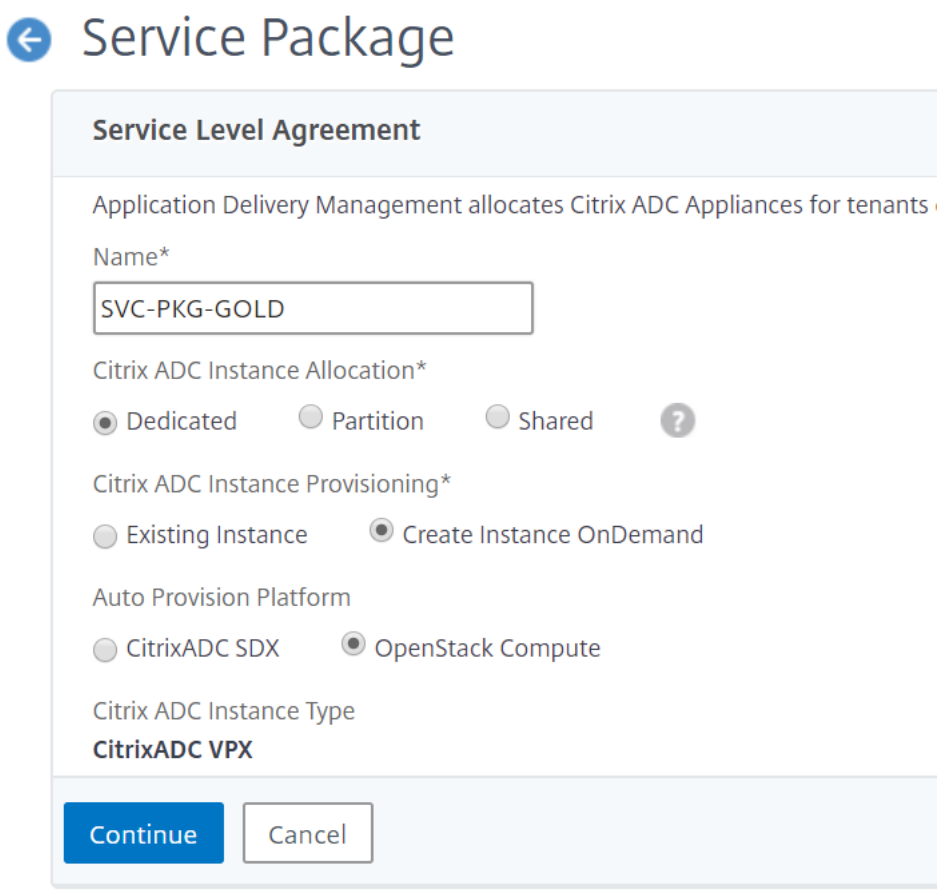
Weitere Informationen zu Heat-Diensten und zum Erstellen von Vorlagen finden Sie in derOpenStack Heat-Dokumentation.

Servicepaket-Isolationsrichtlinien

February 5, 2024

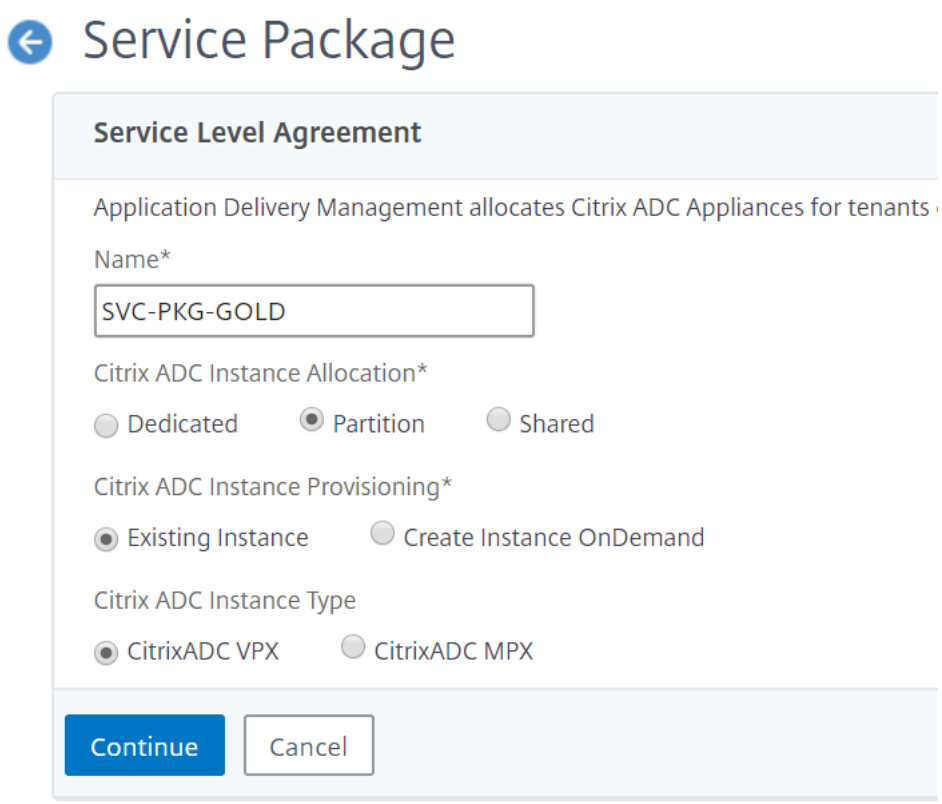
Dedizierte Isolationsrichtlinie

Jedem Mandanten, der dem Citrix Application Delivery Management (ADM) -Dienstpaket einer dedizierten Richtlinie zugeordnet ist, wird aus den Instanzen, die Teil dieses Servicepakets sind, eine Citrix ADC Instanz zugewiesen. Diese zugewiesene NetScaler ADC Instanz wird nicht für andere Mandanten freigegeben.



Partitions-Isolationsrichtlinie

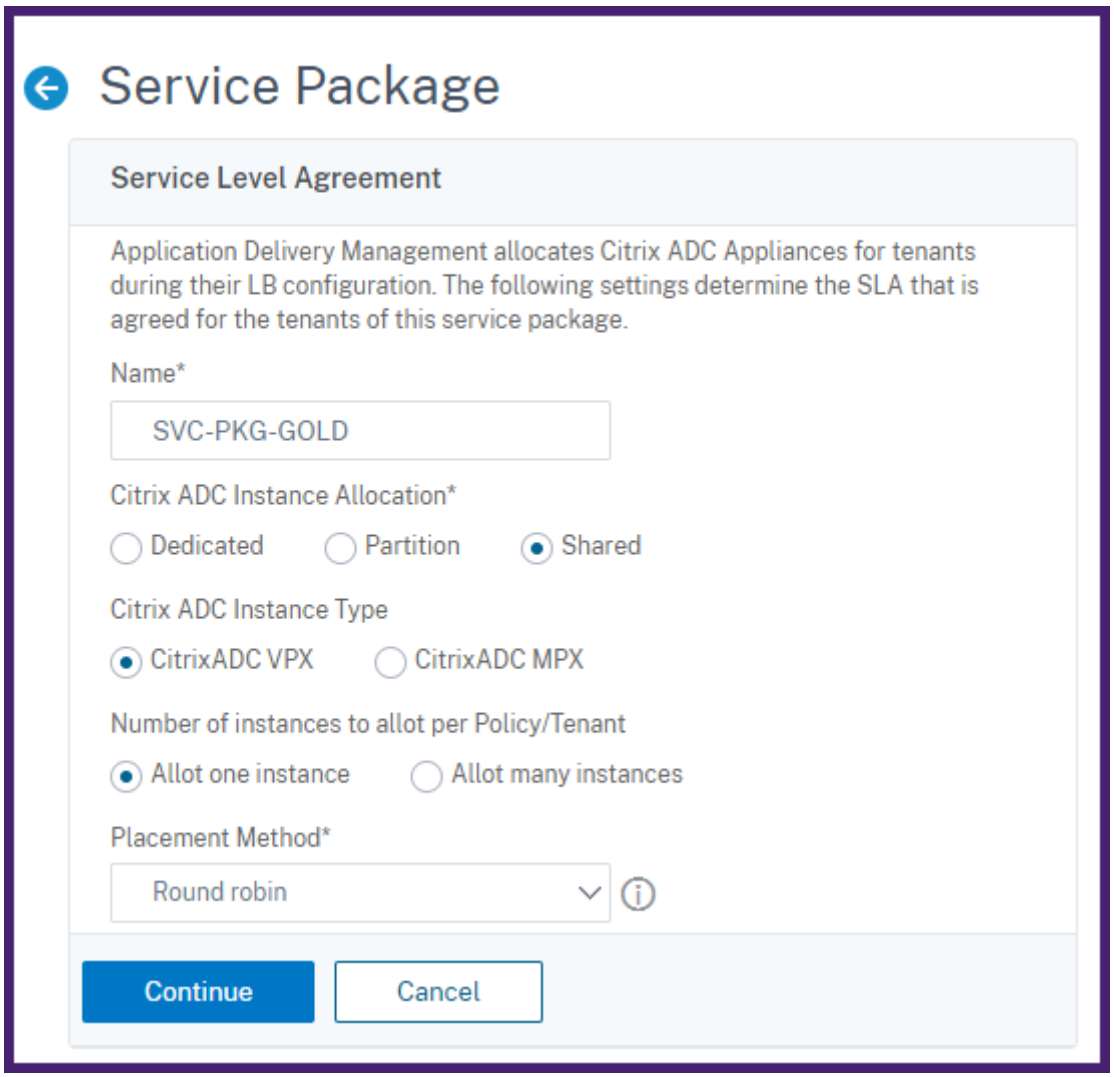
Jedem Mandanten, der dem Dienstpaket der Partitionsrichtlinie zugeordnet ist, wird eine dedizierte logische Administratorpartition einer NetScaler ADC Instanz zugewiesen, die Teil des Dienstpakets ist.



Freigegebene Isolationsrichtlinie

Mandanten, die dem Servicepaket zugeordnet sind, teilen die Citrix ADC Instanzen, die Teil des Servicepakets sind. Alle Konfigurationen eines Mandanten werden einer Citrix ADC Instanz zugewiesen. In diesem Modus können Konfigurationen von mehreren Mandanten auf derselben Citrix ADC Instanz gehostet werden. Sie können **Citrix ADC VPX** oder **Citrix ADC MPX** als Gerätetyp auswählen. Sie können dem Servicepaket nur eine Citrix ADC Instanz oder viele Instanzen zuweisen. Das heißt, mehrere Mandanten können eine oder mehrere virtuelle Instanzen des Citrix ADC Geräts gemeinsam nutzen.

> **Hinweis:**
>
> Fügen Sie NetScaler ADC SDX-Instanzen in den Servicepaketen nur als NetScaler ADC VPX-Instanzen hinzu, da für NetScaler ADC SDX ein NetScaler ADC VPX bereitgestellt wird.



Hinweis

Sie können auch Richtlinien für die flexible Platzierung erstellen, wobei die Richtlinien nicht nur auf dem Namen oder der ID des Mandanten, sondern auch auf anderen benutzerdefinierten Attributen basieren. Weitere Informationen zu Richtlinien für die flexible Platzierung finden Sie unterFlexible richtlinienbasierte Gerätezuteilung.

Flexible richtlinienbasierte Gerätezuweisung

February 5, 2024

Citrix Application Delivery Management (ADM) weist Mandanten virtuelle Instanzen von Citrix ADC zu, basierend auf den mit den Mandanten vereinbarten SLAs. Durch die Zuweisung virtueller Instanzen zu

Mandanten entsteht eine Eins-zu-Eins-Beziehung zwischen der Instanz und dem Mandanten, wobei ein Mandant nur einem Servicepaket im Rechenzentrum zugewiesen werden kann.

In einigen Situationen benötigen Mandanten möglicherweise mehr als eine Instanz, oder die Zuweisung von Instanzen basiert möglicherweise nicht auf Mandanten als Kriterium, sondern auf anderen Faktoren wie Netzwerk-ID oder Anwendung. In solchen Fällen können Sie mit Citrix ADM Platzierungsrichtlinien basierend auf benutzerdefinierten Ausdrücken genau definieren, um einer der verwalteten Instanzen eine Load Balancer-Konfiguration zuzuweisen.

Platzierungsrichtlinien bieten die Flexibilität bei der Entscheidung über die NetScaler ADC Instanz, die in jeder von Benutzern erstellten Load Balancer-Konfiguration verwendet wird. Flexible Platzierungsrichtlinien in Citrix ADM bieten eine zusätzliche Option zur vorhandenen Methode zum Zuweisen von Citrix ADC Instanzen auf Basis von Mandanten.

> **Hinweis**
>
> Sie können Instanzen manuell Mandanten zuweisen oder Platzierungsrichtlinien verwenden, um Instanzen auf der Grundlage der erstellten Ausdrücke zuzuweisen. Sie können diese beiden Methoden nicht gleichzeitig in einem einzigen Servicepaket verwenden.

Platzierungsrichtlinien basieren auf booleschen Ausdrücken, die für Eigenschaften der wichtigsten LBaaS-Konfigurationsobjekte wie Pools und Load Balancer definiert sind. Die Benutzeroberfläche der Platzierungsrichtlinie in Citrix ADM enthält vordefinierte Ausdrücke, die Sie auswählen können, um eine benutzerdefinierte Richtlinie zu definieren. Sie können mehrere Platzierungsrichtlinien für verschiedene Ausdrücke erstellen. Jeder Mandant kann also über mehrere Geräte verfügen, die durch die Anforderungen des Mandanten definiert werden.

Sie müssen zuerst einen Ausdruck auswählen, der einem Stammobjekt entspricht, das später konfiguriert werden muss. Das Root-Objekt kann im Fall von LBaaS V1 ein Pool-Objekt und im Fall von LBaaS V2 ein Load Balancer-Objekt sein. Daher werden die richtlinienbasierten Platzierungen von Citrix ADM sowohl für LBaaS V1- als auch für V2-APIs unterstützt. Diese Platzierungsrichtlinien werden dann mit Servicepaketen verknüpft. Sobald das Stammobjekt in einer Instanz platziert wurde, werden die aufeinanderfolgenden Objekte im Modell in der Instanz hinzugefügt.

Das Poolkonfigurationsobjekt kann beispielsweise die folgenden Eigenschaften haben:

- tenant_id
- name
- Beschreibung
- protocol
- lb_method
- subnet_id

- subname_name
- admin_state_up
- Status
- network_id
- network_type
- segmentation_id
- subnet_cidr
- subnet_gateway_ip

Die folgenden Beispiele zeigen einige der Ausdrücke, die Pooleigenschaften verwenden, um einen Ausdruck für die Richtlinie zu definieren:

1. Poolname basierter Richtlinienausdruck

```
config["pools"]["name"] =="high-end-pool"
<!--NeedCopy-->
```

2. Pool-Subnetzname basierter Richtlinienausdruck

```
config ["pools"]["subnet_name"] == "us-west-payment-subnet1"
<!--NeedCopy-->
```

3. Load Balancer-Subnetname basierter Richtlinienausdruck

```
config["loadbalancers"]["subnet_name"] == "mas-subnet"
<!--NeedCopy-->
```

Hinzufügen von Platzierungsrichtlinien

1. Navigieren Sie auf der Citrix ADM Startseite zu **Orchestration** >Cloud Orchestration** > **Placement Policy**, und klicken Sie dann auf **Hinzufügen**.
2. Legen Sie auf der Seite **Placement Policy hinzufügen** die folgenden Parameter fest:
   a) Name —geben Sie einen Namen für die Platzierungsrichtlinie ein
   b) Häufig verwendete Ausdrücke: Wählen Sie einen Ausdruck aus der Dropdownliste aus.
   c) Ausdruck —In dieses Feld wird ein logischer (boolescher) Ausdruck eingetragen, der auf dem Ausdruck basiert, den Sie im vorherigen Feld ausgewählt haben. Bearbeiten Sie die Feldnamen nach Bedarf.

> **Hinweis
>
> Wenn Sie**mehrere Richtlinien erstellen, stellen Sie sicher, dass die Richtlinien zueinander exklusiv sind.

3. Klicken Sie auf **OK**.
4. Navigieren Sie zu **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Service Packages** und klicken Sie dann auf **Hinzufügen**.
5. Stellen Sie auf der Seite **Service Package** die folgenden Parameter ein:

   a) Name —geben Sie einen Namen für das Servicepaket ein

   b) Isolationsrichtlinie —wählen Sie **Gemeinsame** Richtlinie

   In der Shared Isolation-Policy ist die Load Balancer-Konfiguration eines Mandanten mit der Load Balancer-Konfiguration anderer Mandanten auf dem Gerät koexistiert, das dem Mandanten zugewiesen ist.

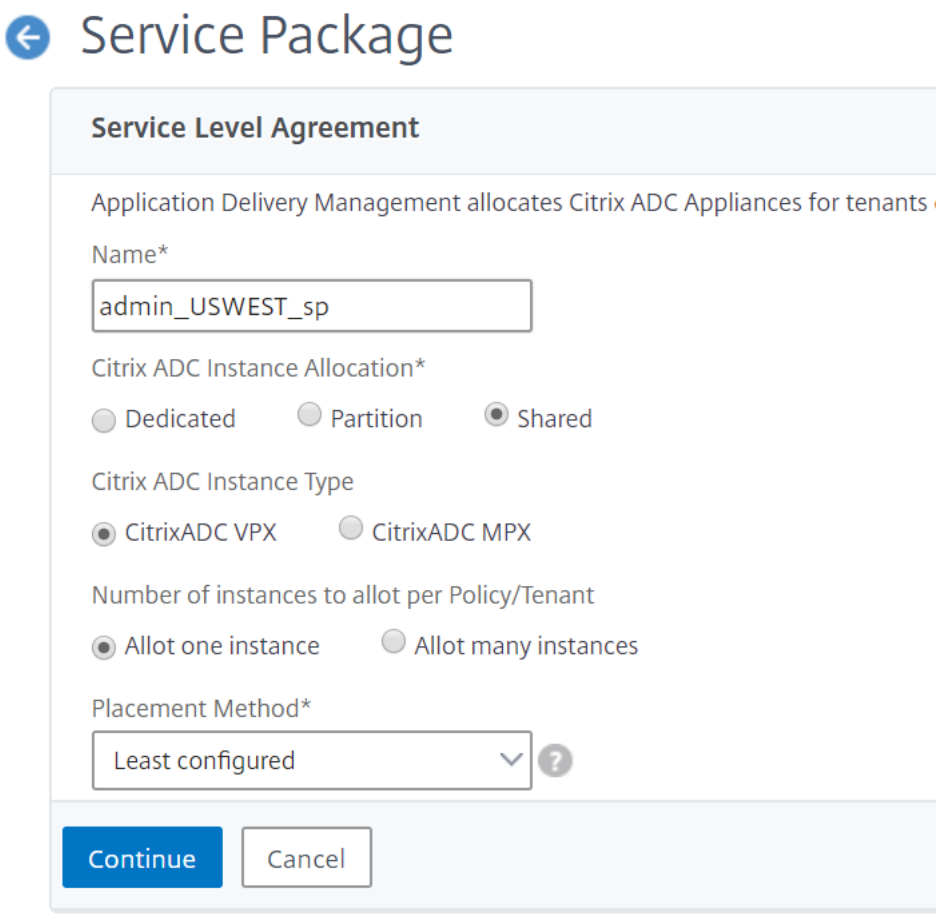
   c) Gerätetyp: Wählen Sie ein vorbereitgestelltes **Citrix ADC VPX** oder **Citrix ADC MPX**aus

   Wählen Sie **Ein Gerät zuweisen** aus, wenn alle Load Balancer-Konfigurationen eines Mandanten an ein Gerät gebunden werden sollen. Wählen Sie **Viele Geräte zuweisen**, wenn jede Load Balancer-Konfiguration eines Mandanten auf der Grundlage von Platzierungsrichtlinien auf mehrere Geräte verteilt werden soll.

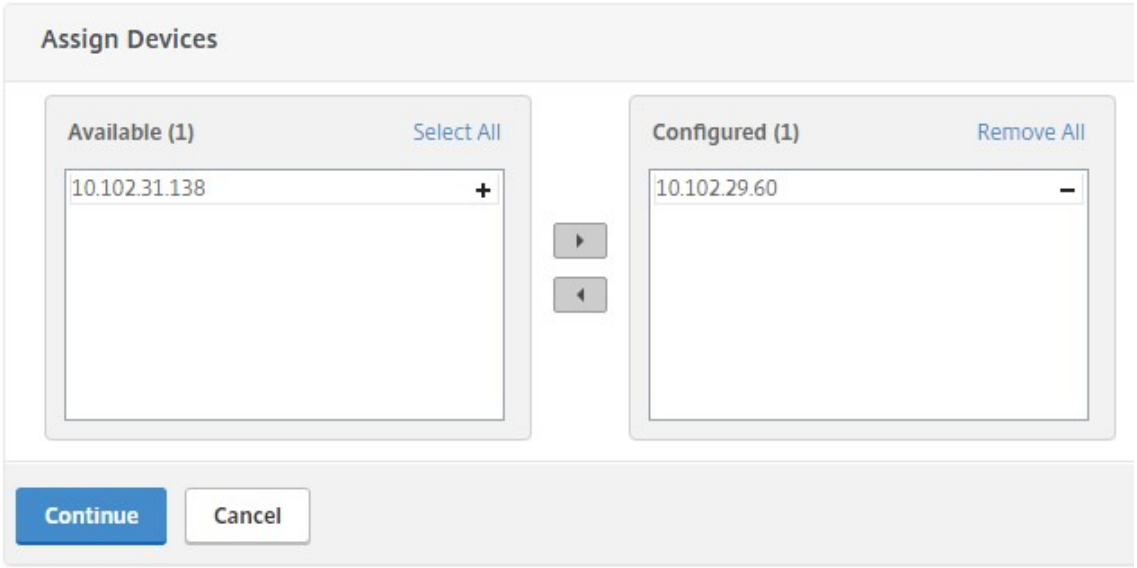
   > **Hinweis:**
   >
   > Citrix ADC SDX muss in den Servicepaketen nur als Citrix ADC VPX-Instanzen hinzugefügt werden, da auf einem Citrix ADC SDX ein Citrix ADC VPX bereitgestellt wird.

   d) Platzierungsmethode —Wählen Sie **Am wenigsten konfiguriert**

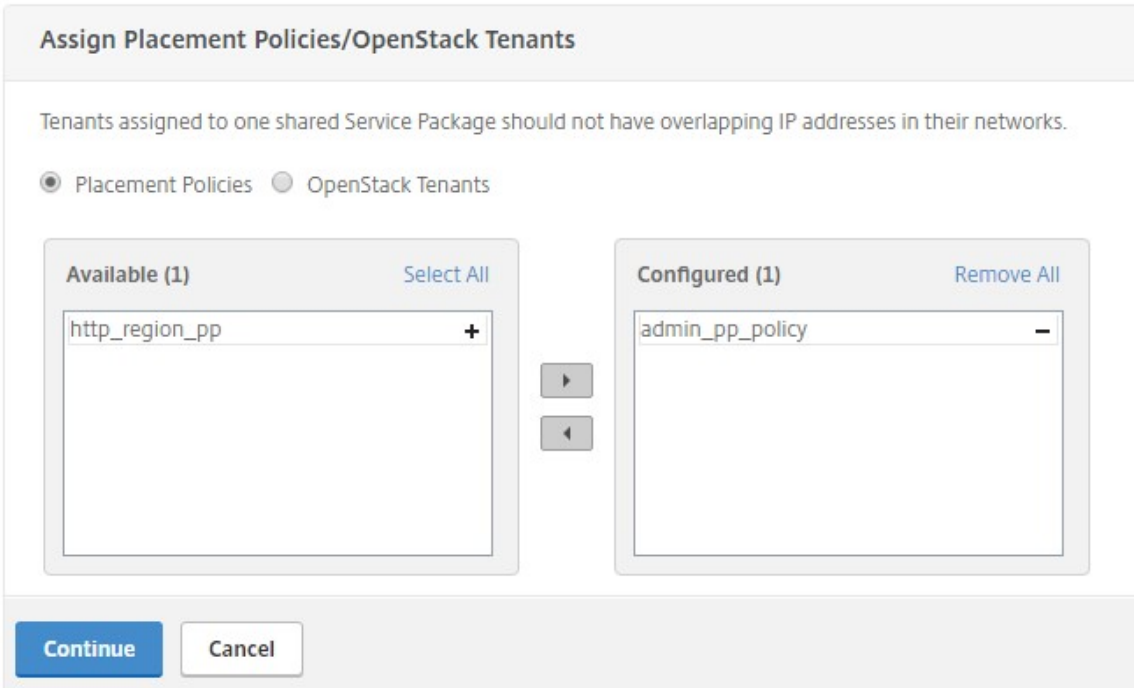
Wenn die Option “Am wenigsten konfiguriert”ausgewählt ist, wird die NetScaler ADC Instanz mit der geringsten Anzahl von Poolmitgliedern, die zu diesem Zeitpunkt konfiguriert sind, als Gerät für den Mandanten ausgewählt.



6. Klicken Sie auf **Weiter**.
7. Fügen **Sie im Abschnitt Geräte zuweisen** die verfügbaren NetScaler ADC Geräte zur Liste der konfigurierten Geräte hinzu.



8. Klicken Sie auf **Weiter**.
9. Fügen **Sie im Abschnitt Platzierungsrichtlinien zuweisen/OpenStack-Mandanten** die Platzierungsrichtlinie hinzu, die Sie zuvor erstellt haben.



> **Hinweis**
>
> Wenn die Richtlinie nicht gefunden wird, wird der Fallbackmechanismus wiederhergestellt, und NetScaler ADM weist NetScaler ADC Instanzen basierend auf Mandanten zu. Wenn der Mandant nicht Teil eines Dienstpakets ist, zeigt NetScaler ADM eine

> Fehlermeldung an, die besagt:
>
> "Der Mandant `admin` ist nicht Teil eines Servicepakets und es gibt kein Standarddienstpaket".

10. Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig**.

NSX Manager: Manuelle Provisioning von NetScaler ADC Instanzen

February 5, 2024

NetScaler Application Delivery Management (ADM) ist in die VMware Netzwerkvirtualisierungsplattform integriert, um die Bereitstellung, Konfiguration und Verwaltung von NetScaler ADC Diensten zu automatisieren. Diese Integration abstrahiert die traditionellen Komplexitäten, die mit der physischen Netzwerktopologie verbunden sind, und ermöglicht es vSphere/vCenter-Administratoren, NetScaler ADC Dienste programmgesteuert schneller bereitzustellen.

Dieser Artikel enthält eine Liste der Aufgaben, die Sie sowohl für VMware NSX Manager als auch für Citrix ADM ausführen müssen.

> **Hinweis: Stellen Sie**
>
> sicher, dass VMware NSX für vSphere 6.2 und höher installiert und konfiguriert ist und dass die Edge-Gateways, DLR und virtuellen Maschinen, für die ein Lastenausgleich erforderlich ist, bereits erstellt wurden.

Voraussetzungen

- Installieren Sie VMware ESXi Version 4.1 oder höher mit Hardware, die die Mindestanforderungen erfüllt.
- Installieren Sie VMware Client auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
- Installieren Sie VMware OVF Tool (erforderlich für VMware ESXi Version 4.1) auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
- Installieren Sie NetScaler ADM auf einem der unterstützten Hypervisoren.

  Aufgaben zum Installieren von NetScaler ADM Build 13.0 auf einem der unterstützten Hypervisoren finden Sie unter Bereitstellen von NetScaler ADM.

VMware ESXi Hardwareanforderungen

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die Sie auf Ihrem VMware ESXi -Server benötigen, um eine virtuelle Citrix ADM Appliance zu installieren.

Komponente	Voraussetzung
RAM	8 GB
Virtuelle CPU	8
Speicherplatz	500 GB
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s

> **Hinweis:**
>
> Die oben angegebenen Speicher- und Festplattenanforderungen gelten für die Bereitstellung von Citrix ADM auf dem VMware ESXi -Server, wenn man bedenkt, dass keine anderen virtuellen Maschinen auf dem Host ausgeführt werden. Die Hardwareanforderungen für den VMware ESXi-Server hängen von der Anzahl der darauf ausgeführten virtuellen Maschinen ab.

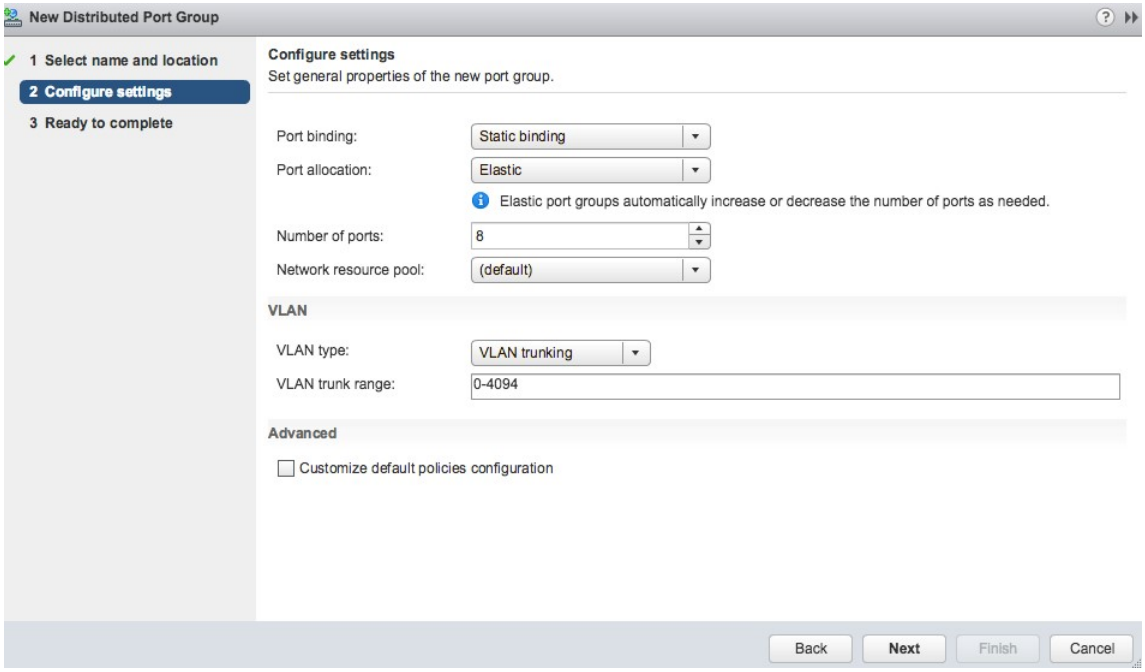
Konfiguration von VMware NSX

- Erstellen Sie einen Pool von Citrix ADC VPX Instanzen mit unterschiedlichen Kapazitäten, die den verschiedenen Servicepaketen hinzugefügt werden.

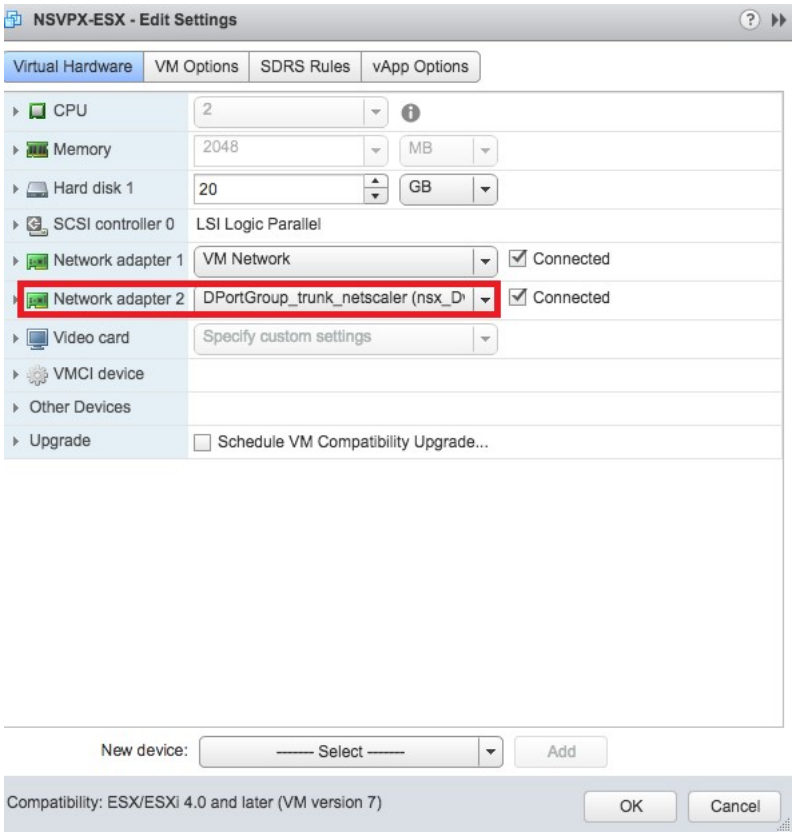
Beispiel:

- Erstellen Sie fünf Citrix ADC VPX Instanzen von VPX1000 (1 Gbit/s). Diese Instanzen werden dem Gold-Servicepaket hinzugefügt.
- Erstellen Sie fünf Citrix ADC VPX Instanzen von VPX10 (10 Mbit/s). Diese Instanzen werden dem Bronze-Servicepaket hinzugefügt.

1. Navigieren Sie im vSphere-Client zu **Netzwerk**, und erstellen Sie eine Portgruppe vom Typ VLAN-Trunking mit Bereich, z. B. 101-105 (Sie können sogar den vollständigen Bereich angeben, aber nur für die erforderlichen VLANs eine Portgruppe vom Typ VLAN erstellen).

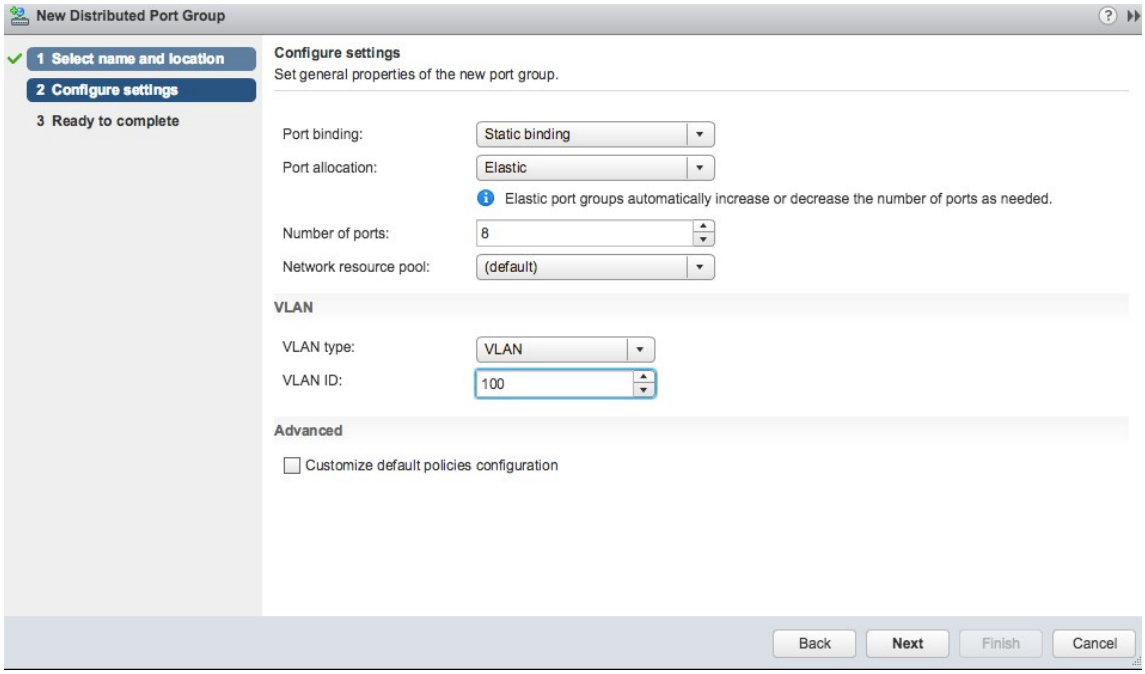


2. Erstellen Sie eine neue Schnittstelle für jede NetScaler ADC VPX Instanz, und fügen Sie sie der oben erstellten Trunk-Portgruppe des VLAN-Bereichs an.



3. Navigieren Sie im vSphere-Client zu **Netzwerk**, und erstellen Sie eine Portgruppe vom Typ VLAN.

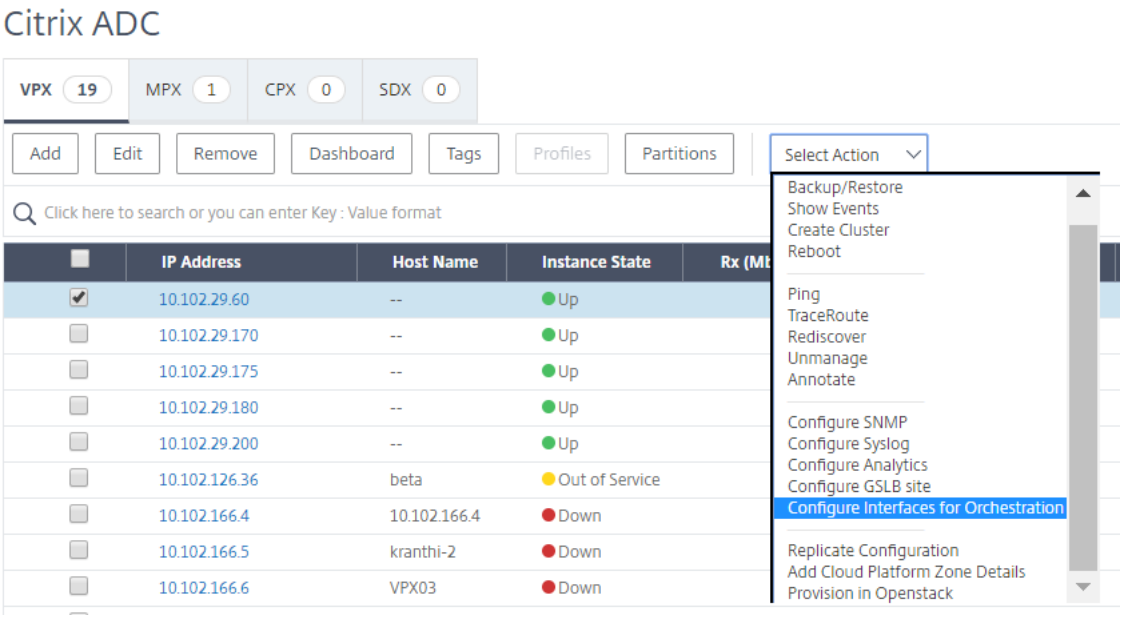
Wenn beispielsweise die anfängliche Trunked Portgruppe mit Bereich 101-105 erstellt wurde, erstellen Sie fünf VLAN-Portgruppen, eine pro VLAN, d. h. eine Portgruppe mit VLAN 101, eine andere mit VLAN102 usw., bis VLAN 105.



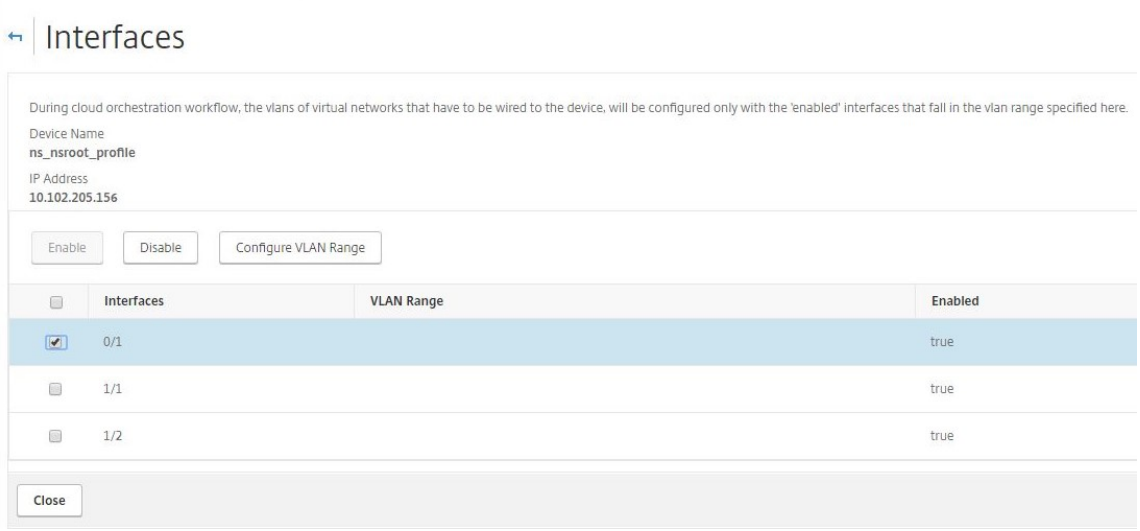
Hinzufügen der NetScaler ADC VPX Instanz in NetScaler ADM

Fügen Sie Citrix ADC VPX Instanzen in Citrix ADM hinzu, und geben Sie den VLAN-Bereich der Trunked Group für jedes Gerät an.

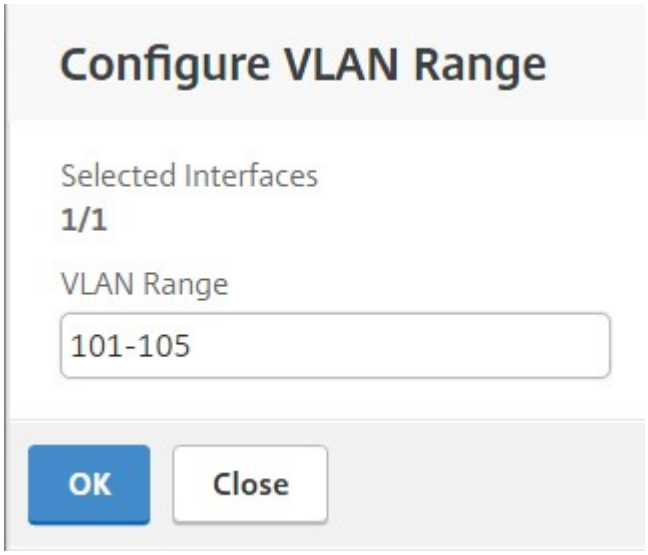
1. Navigieren Sie in Citrix ADM zu **Infrastructure** > **Instanzen** > **Citrix ADC VPX**, und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Citrix ADC VPX hinzufügen** entweder die Hostnamen der Instanzen, die IP-Adresse jeder Instanz oder einen Bereich von IP-Adressen an, und wählen Sie dann ein Instanzprofil aus der Liste**P-rofile-Name** aus. Sie können auch ein neues Instanzprofil erstellen, indem Sie auf das Symbol + klicken.
3. Klicken Sie auf **OK**.
4. Wählen Sie die neu hinzugefügte Citrix ADC VPX-Instanz aus der Liste auf der Seite **Citrix ADC VPX** aus, und klicken Sie im Feld **Aktion** auf den Abwärtspfeil. Wählen Sie **Interfaces für Orchestration konfigurieren**aus.



5. Wählen Sie auf der Seite **Schnittstellen** die Verwaltungsschnittstelle aus, und klicken Sie auf **Deaktivieren**, um die Bindung von VLAN an die Verwaltungsschnittstelle zu deaktivieren.



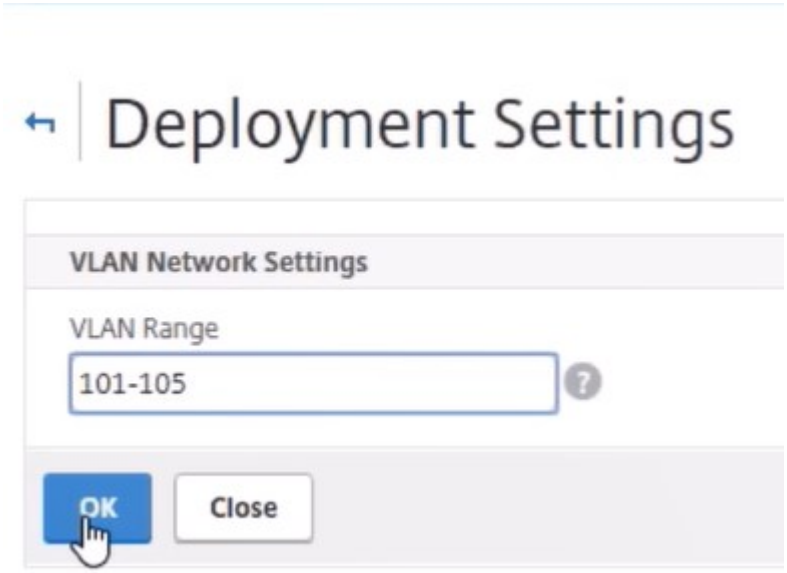
6. Wählen Sie auf der Seite **Schnittstellen** die erforderliche Schnittstelle aus, und klicken Sie auf **VLAN-Bereich konfigurieren**.
7. Geben Sie den in NSX Manager konfigurierten VLAN-Bereich ein, klicken Sie auf **OK**, und klicken Sie dann auf **Schließen**.



Registrieren von VMware NSX Manager bei NetScaler ADM

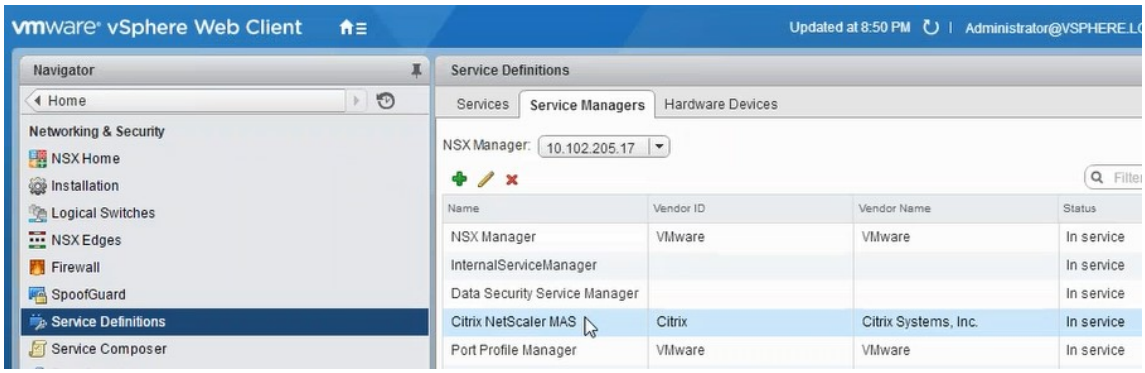
Registrieren Sie VMware NSX Manager bei Citrix ADM, um einen Kommunikationskanal zwischen ihnen zu erstellen.

1. Navigieren Sie in NetScaler ADM in der Dropdownliste zu**Orchestration> SDN Orchestration**>**VMware NSX Manager**und klicken Sie auf**NSX Manager-Einstellungen konfigurieren**.
2. **Legen Sie auf der Seite NSX Manager-Einstellungen konfigurieren** die folgenden Parameter fest:
   a) NSX Manager-IP-Adresse: IP-Adresse von NSX Manager.
   b) NSX Manager-Benutzername —Administratorbenutzername von NSX Manager.
   c) Kennwort - Kennwort des administrativen Benutzers von NSX Manager.
3. Legen Sie im Abschnitt **NetScaler ADM-Konto, das von NSX Manager verwendet wird**, den Benutzernamen und das Kennwort des NetScaler ADC-Treibers für den NSX Manager fest. NetScaler ADM authentifiziert Load Balancer Konfigurationsanforderungen von NSX Manager mithilfe dieser Anmeldeinformationen.
4. Klicken Sie auf **OK**.
5. Navigieren Sie zu **Orchestration** > **System** > **Deployment Settings.** Geben Sie den VLAN-Bereich an, der in Trunked Port Group konfiguriert wurde.



6. Melden Sie sich bei NSX Manager auf vSphere Web Client an, und navigieren Sie zu **Dienstdefinitionen** > **Service Manager**.

   Sie können Citrix ADM als einer der Dienstmanager anzeigen. Dies zeigt an, dass die Registrierung erfolgreich ist und ein Kommunikationskanal zwischen NSX Manager und NetScaler ADM eingerichtet wird.

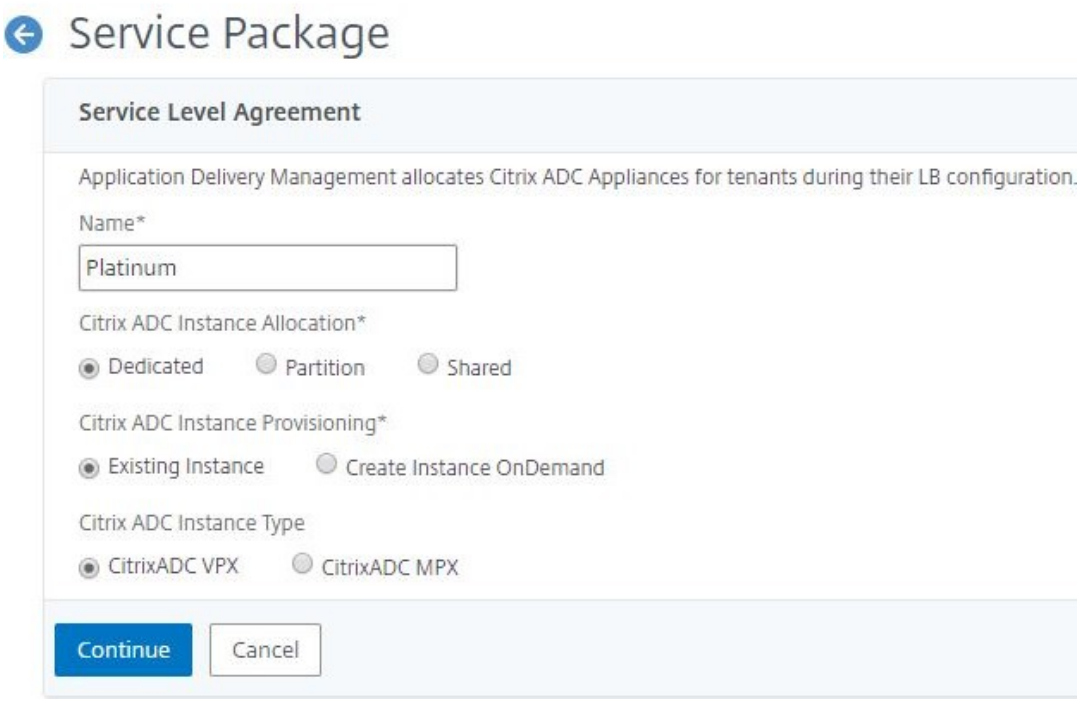


Erstellen eines Servicepakets in NetScaler ADM

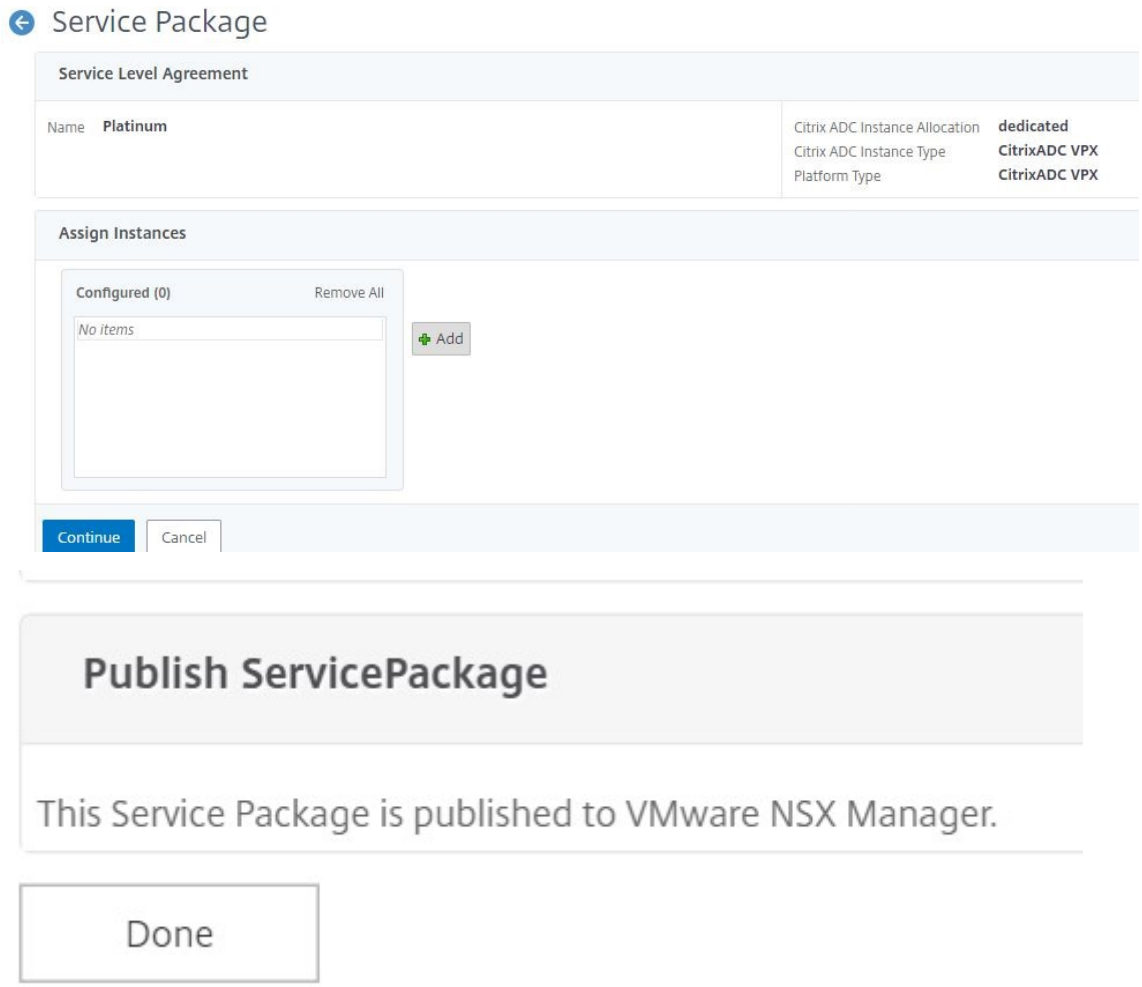
1. Navigieren Sie in Citrix ADM zu**Orchestration** >**SDN Orchestration**>**VMware NSX Manager**> **Service Packages**, und klicken Sie auf **Hinzufügen**, um ein neues Servicepaket hinzuzufügen.
2. Legen Sie auf der Seite **Service Package** im Abschnitt **Grundeinstellungen** die folgenden Parameter fest:
   a) Name —geben Sie den Namen eines Servicepakets ein
   b) Isolationsrichtlinie —standardmäßig ist die Isolationsrichtlinie auf Dedicated gesetzt
   c) Gerätetyp: Standardmäßig ist der Gerätetyp auf Citrix ADC VPX festgelegt.

> **Hinweis**
>
> Diese Werte sind in dieser Version standardmäßig festgelegt und können nicht geändert werden.

d) Klicken Sie auf **Weiter**.



3. Wählen **Sie im Abschnitt Geräte zuweisen** das vorab bereitgestellte VPX für dieses Paket aus, und klicken Sie auf **Weiter**.
4. Klicken Sie im Abschnitt **Servicepaket veröffentlichen** auf **Weiter**, um das Servicepaket in VMware NSX zu veröffentlichen, und klicken Sie dann auf **Fertig**.



Mit diesem Verfahren wird ein Servicepaket im NSX Manager konfiguriert. Ein Dienst kann mehrere Geräte hinzugefügt haben, und mehrere Kanten können dasselbe Servicepaket verwenden, um die Citrix ADC VPX Instanz an Citrix ADM zu entladen.

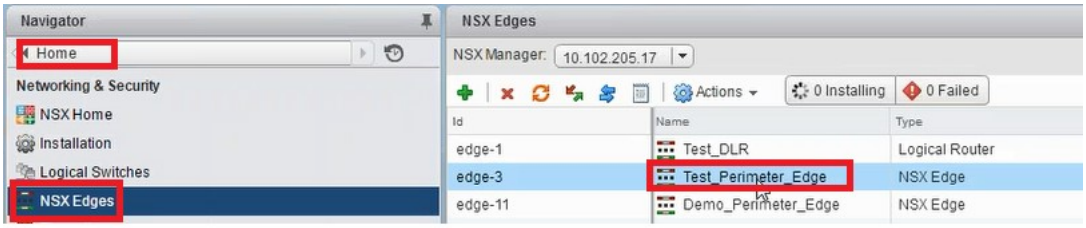
5. **Melden Sie sich beim NSX Manager auf dem vSphere Web Client an und navigieren Sie zu**Service Definitions**> Services.**

   Sie können sehen, dass das NetScaler ADM Dienstpaket registriert ist.

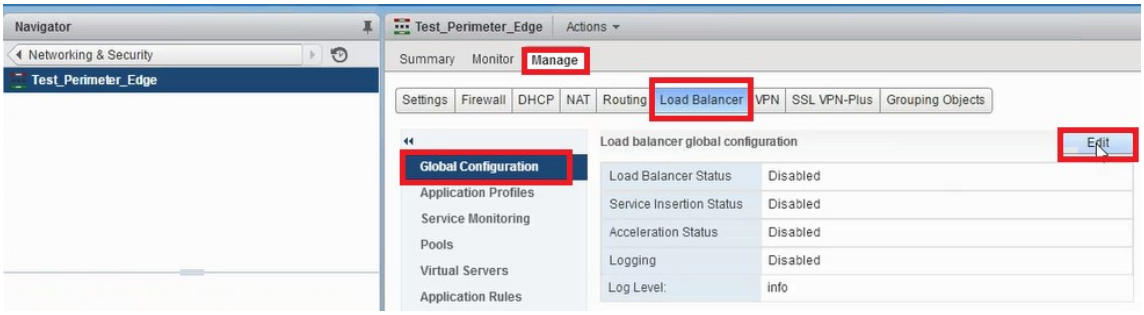
Ausführen des Lastausgleichsdiensteinfügens für Edge

Führen Sie die Einfügung des Lastausgleichsdienstes auf dem zuvor erstellten NSX Edge-Gateway durch (Verschieben der Lastausgleichsfunktion von NSX LB zu Citrix ADC).

1. Navigieren Sie in NSX Manager zu **Home** > **NSX Edges**, und wählen Sie das Edge-Gateway aus, das Sie konfiguriert haben.

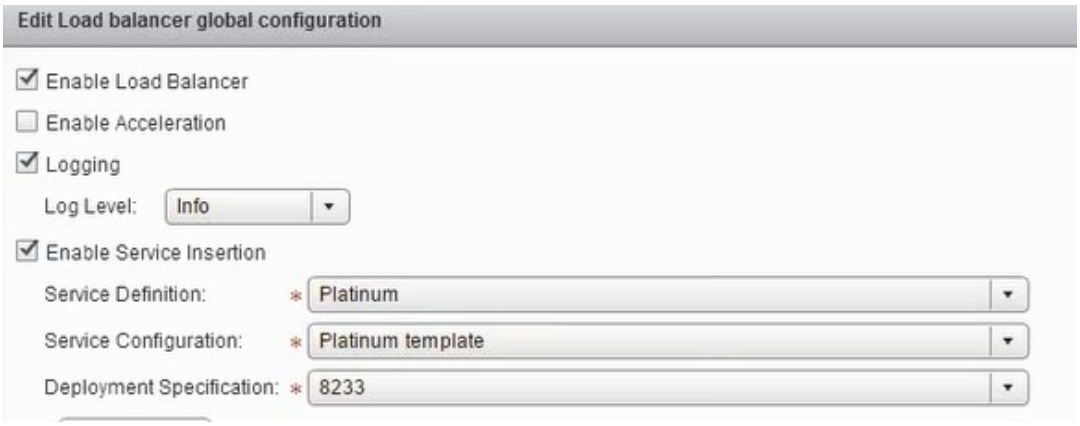


2. Klicken Sie auf **Verwalten**, wählen Sie auf der Registerkarte **Load Balancer** die Option **Globale Konfiguration** aus, und klicken Sie auf **Bearbeiten**.



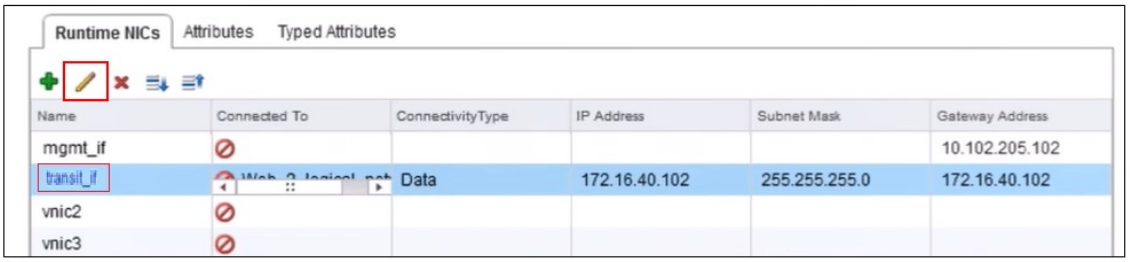
3. Wählen Sie **Load Balancer aktivieren**, **Protokollierung**, **Diensteinfügung aktivieren** aus, um sie zu aktivieren.

   a) Wählen Sie unter **Dienstdefinition** das Dienstpaket aus, das in NetScaler ADM erstellt und in NSX Manager veröffentlicht wurde.

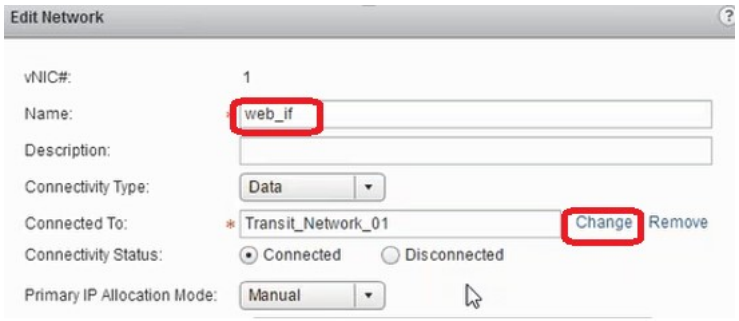


4. Wählen Sie die vorhandenen Laufzeit-NICs aus, und klicken Sie auf das Symbol Bearbeiten, um Laufzeit-NICs zu bearbeiten, die bei der Zuweisung von NetScaler ADC VPX verbunden werden

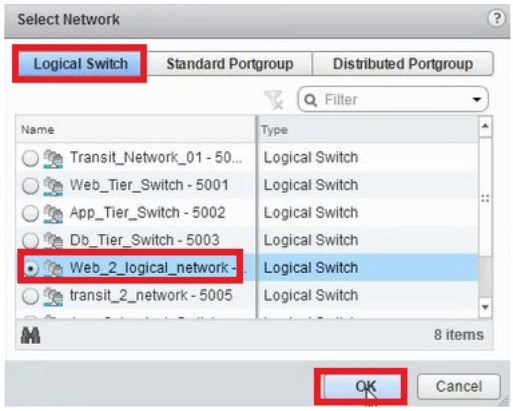
müssen.



5. Bearbeiten Sie den Namen der Netzwerkkarte, geben Sie Konnektivitätstyp als **Daten**an, und klicken Sie auf **Ändern**.

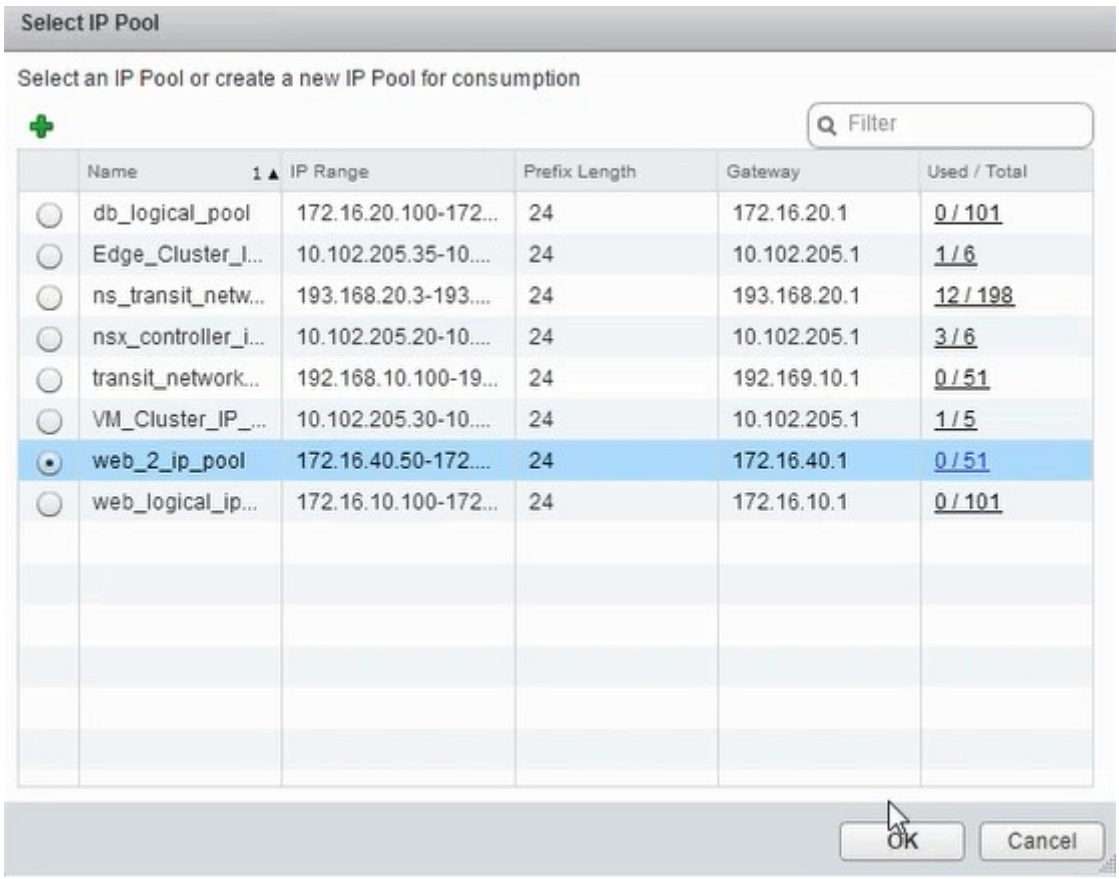


6. Wählen Sie den entsprechenden logischen Web-Switch aus.



7. Wählen Sie im **primären IP-Zuordnungsmodus**die Option IP-Pool aus der Dropdownliste aus, und klicken Sie auf den Pfeil nach unten im Feld IP-Pool.

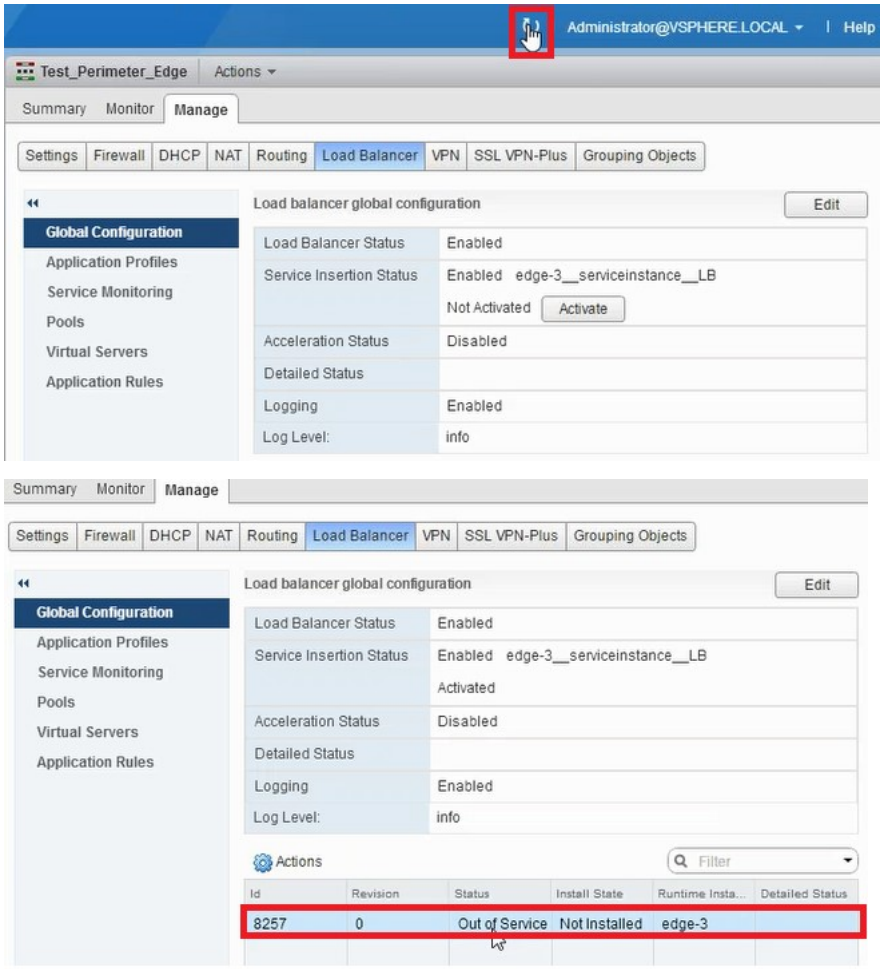
8. **Wählen Sie im Fenster IP-Pool** auswählen den entsprechenden IP-Pool aus, und klicken Sie auf **OK**.



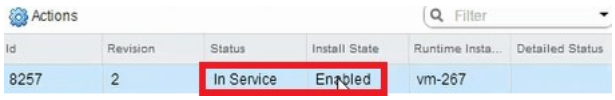
Die IP-Adresse wird erfasst und als Quellnetz-IP-Adresse in der NetScaler ADC VPX Appliance festgelegt. Im NSX Manager wird ein L2-Gateway erstellt, um das VXLAN dem VLAN zuzuordnen.

> **Hinweis**
>
> Alle Datenschnittstellen sind als Laufzeit-NICs verbunden und sind Teil von Schnittstellen für das DLR.

9. Aktualisieren Sie die Ansicht, um die Erstellung der Laufzeit anzuzeigen.



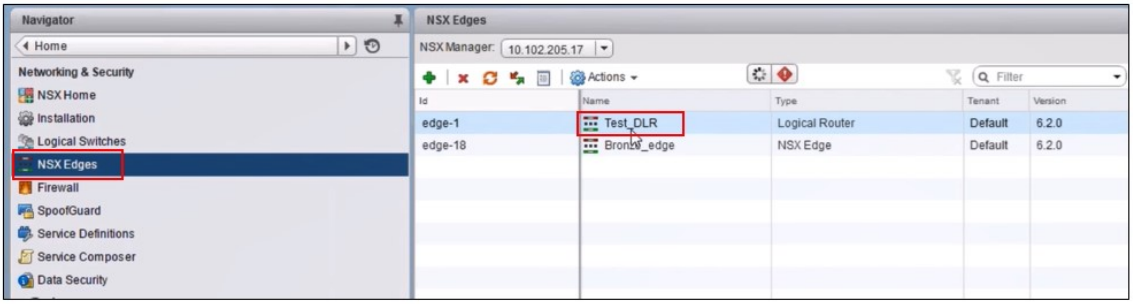
10. Nachdem die VM gestartet wurde, ändert sich der Wert von Status **in In Dienst** und der Wert des Installationsstatus in **Aktiviert**.



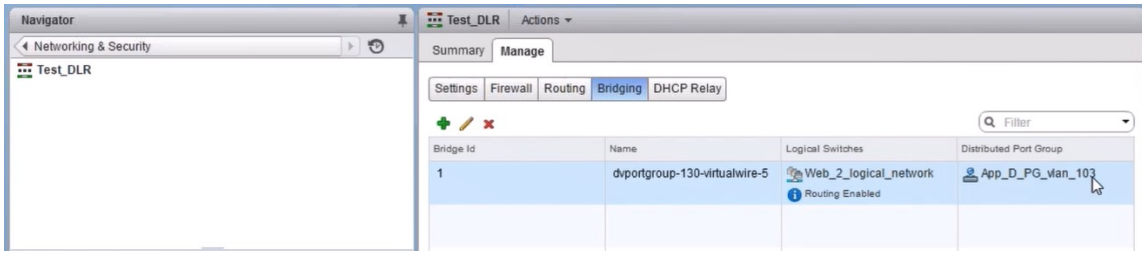
> **Hinweis:**Navigieren Sie
>
> in NetScaler ADM zu **Orchestration** > **Requests**, um Fortschrittsdetails zum Abschluss der LB-Diensteinfügung anzuzeigen.

L2-Gateway auf NSX Manager anzeigen

1. Melden Sie sich beim NSX Manager auf vSphere Web Client an, navigieren Sie zu **NSX Edges**, und wählen Sie das erstellte DLR aus.



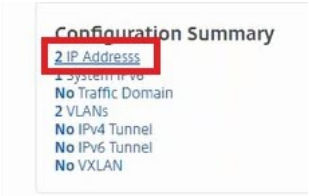
2. Navigieren Sie auf der DLR-Seite zu **Verwalten** > **Bridging**. Das L2-Gateway wird in der Liste angezeigt.



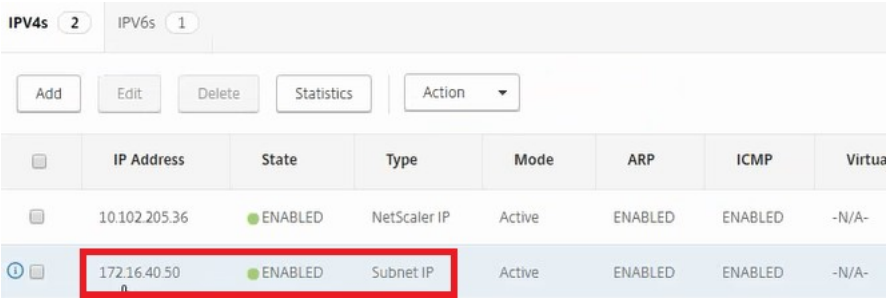
> **Hinweis**
>
> Ein L2-Gateway wird für jede Datenschnittstelle erstellt.

Zugeteilte Citrix ADC anzeigen

1. Melden Sie sich bei der Citrix ADC VPX Instanz mit der in Citrix ADM angezeigten IP-Adresse an. Navigieren Sie dann zu **Konfiguration** > **System** > **Netzwerk**. Im rechten Bereich können Sie sehen, dass die beiden IP-Adressen hinzugefügt wurden. Klicken Sie auf den Hyperlink IP-Adresse, um die Details anzuzeigen.



Die Subnetz-IP-Adresse entspricht der IP-Adresse der im NSX hinzugefügten Weboberfläche.



2. Navigieren Sie zu **Konfiguration** > **System** > **Lizenzen**, um die Lizenzen anzuzeigen, die auf diese Instanz angewendet werden.

Konfigurieren von NetScaler ADC VPX Instanz mit StyleBook

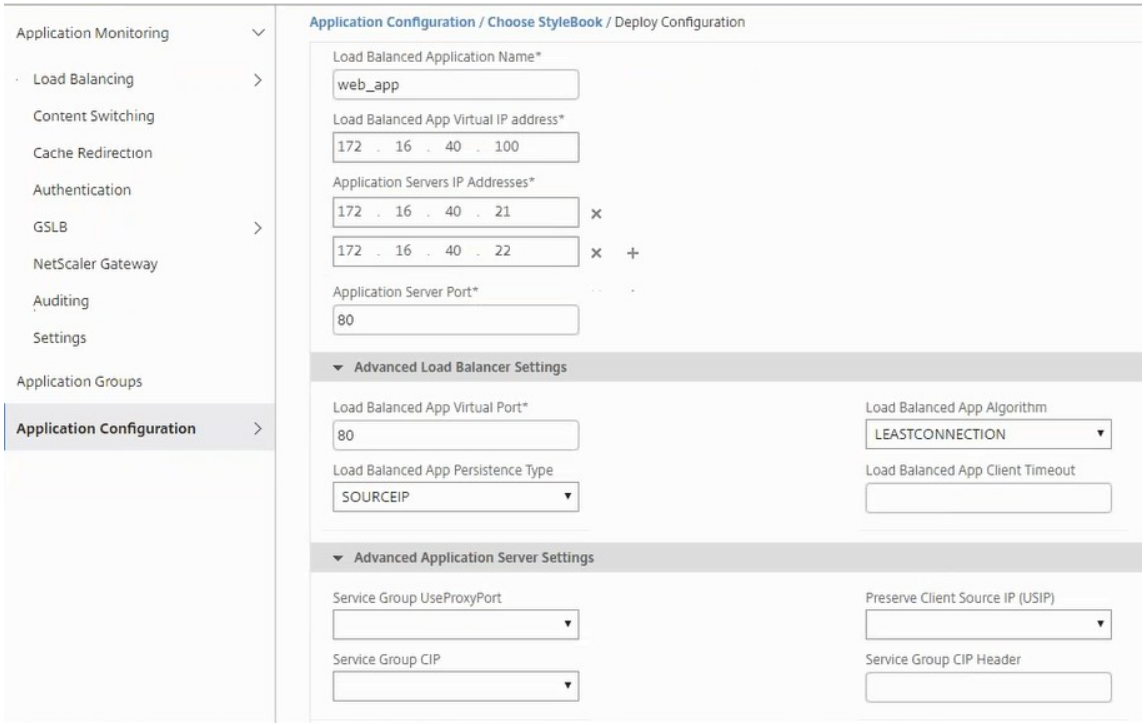
1. Navigieren Sie in NetScaler ADM zu **Orchestration** > **SDN Orchestration** > **NSX Manager konfigurieren** > **Edge-Gateways**.

   Notieren Sie sich die NetScaler ADC-Instanz-IP, die dem jeweiligen Edge-Gateway zugewiesen ist, auf das die Load Balancing-Konfiguration über StyleBooks angewendet werden muss.

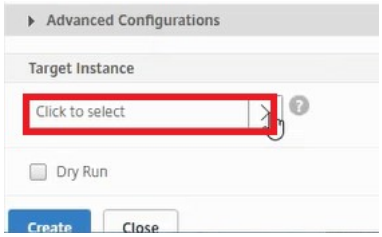
2. Erstellen Sie ein neues StyleBook. Navigieren Sie zu **Applications** > **Configuration**, importieren Sie das StyleBook und wählen Sie das StyleBook aus der Liste aus.

   Informationen zum Erstellen eines neuen StyleBook finden Sie unter Erstellen Sie Ihr eigenes StyleBook.

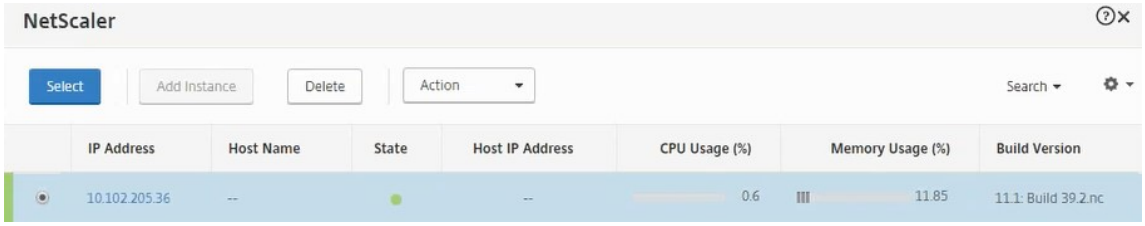
3. Geben Sie Werte für alle erforderlichen Parameter an.



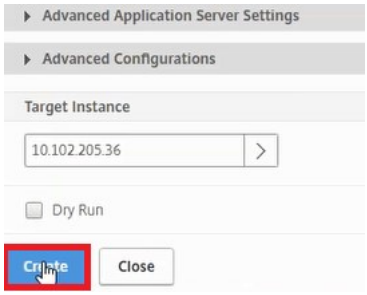
4. Geben Sie die NetScaler ADC VPX Instanz an, auf der diese Konfigurationseinstellungen ausgeführt werden sollen.



5. Wählen Sie die zuvor notierte IP-Instanz aus, und klicken Sie auf **Auswählen**.

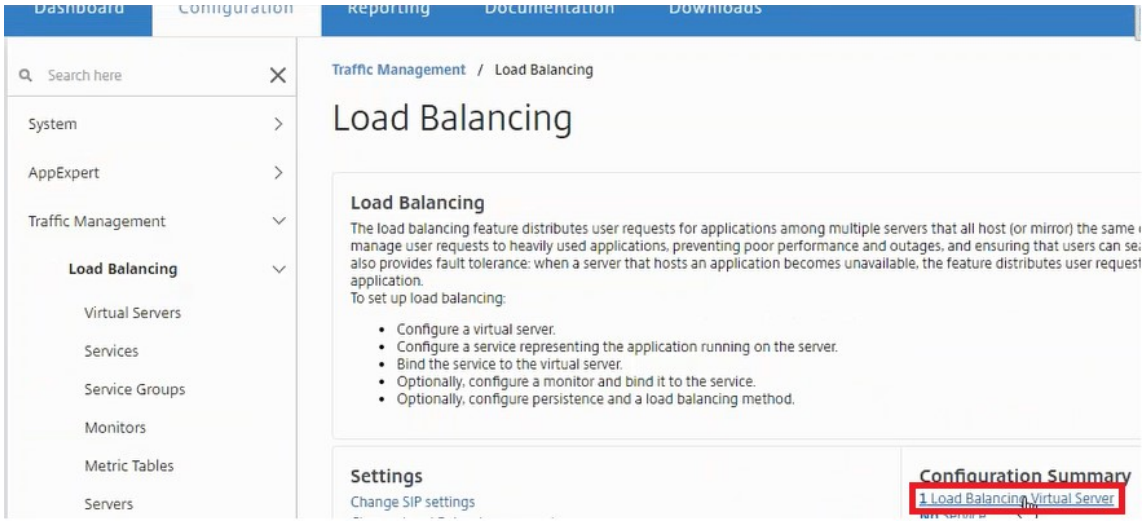


6. Klicken Sie auf **Erstellen**, um die Konfiguration auf das ausgewählte Gerät anzuwenden.

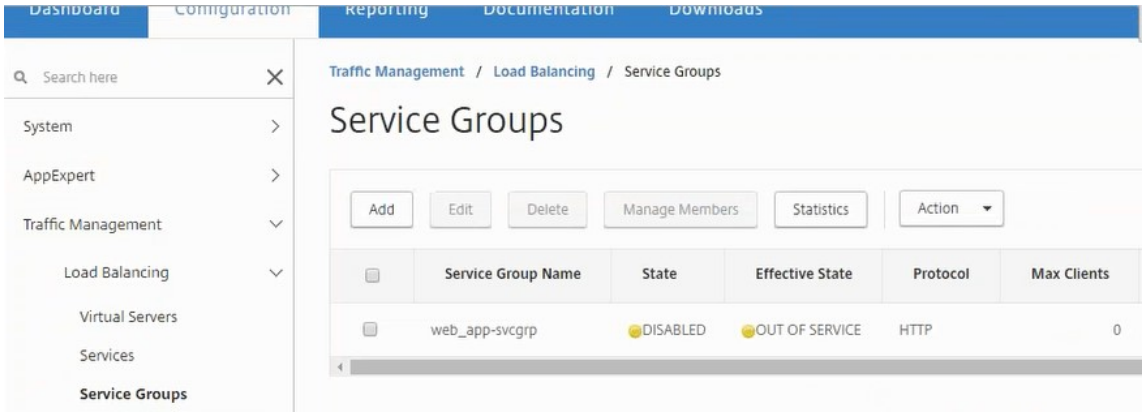


Load Balancer-Konfiguration anzeigen

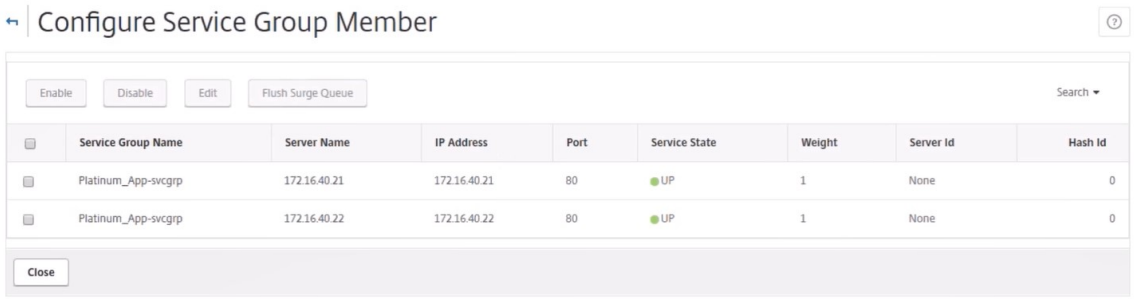
1. Melden Sie sich bei der NetScaler ADC VPX Instanz an, navigieren Sie zu **Configuration** > **Traffic Management** > **Load Balancing**, um den virtuellen Lastausgleichsserver anzuzeigen, der erstellt wird.



Sie können auch die erstellten Dienstgruppen anzeigen.



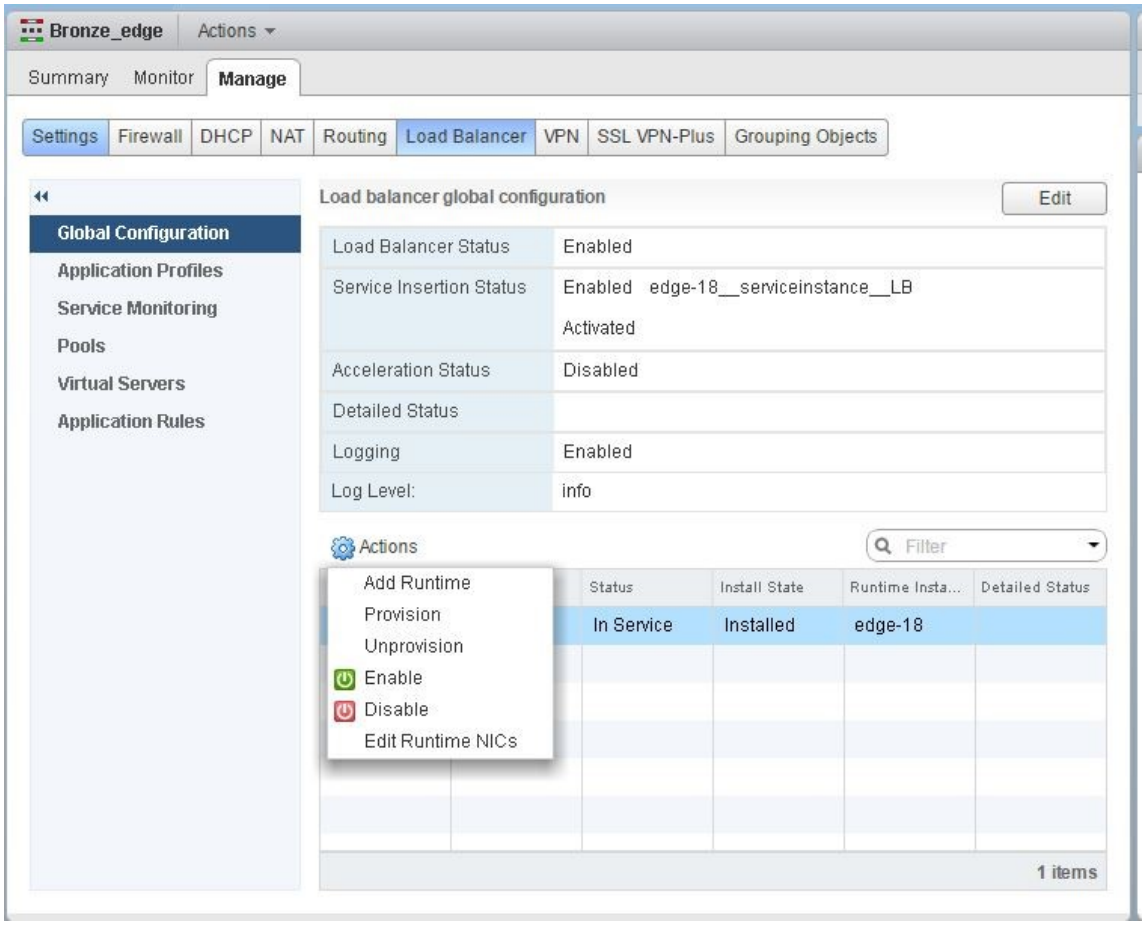
2. Wählen Sie die Dienstgruppe aus, und klicken Sie auf **Mitglieder verwalten**. Auf der Seite **Dienstgruppenmitglied konfigurieren** werden die Mitglieder angezeigt, die der Dienstgruppe zugeordnet sind.



Löschen des Load Balancer-Dienstes

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfiguration**, und klicken Sie auf **X-Symbol**, um die Anwendungskonfiguration zu löschen.
2. Melden Sie sich am NSX Manager auf vSphere Web Client an, und navigieren Sie zu dem Edge-Gateway, mit dem die Citrix ADC VPX Instanz verbunden ist.
3. Navigieren Sie zu **Verwalten** > **Load Balancer** > **Globale Konfiguration**, klicken Sie mit der rechten Maustaste auf den Laufzeiteintrag, und wählen Sie **Bereitstellung aufheben**.

> **Hinweis:**
>
> Edge Gateways in NetScaler ADM entspricht Laufzeiteinträgen in NSX Manager.



Die NetScaler ADC VPX Instanz wird außer Betrieb gesetzt.

4. Navigieren Sie in NetScaler ADM zu **Orchestration** > **SDN Orchestration** > **NSX Manager konfigurieren** > **Edge-Gateways**. Stellen Sie sicher, dass die entsprechende Zuordnung des Edge-Gateways zur gelöschten Instanz nicht vorhanden ist.

NSX Manager: Automatische Provisioning von NetScaler ADC Instanzen

February 5, 2024

Übersicht

NetScaler Application Delivery Management (ADM) ist in die VMware Netzwerkvirtualisierungsplattform integriert, um die Bereitstellung, Konfiguration und Verwaltung von NetScaler ADC Diensten zu automatisieren. Diese Integration abstrahiert die traditionellen Komplexitäten, die mit der physischen Netzwerktopologie verbunden sind, und ermöglicht es vSphere/vCenter-Administratoren,

NetScaler ADC Dienste programmgesteuert schneller bereitzustellen.

Beim Einfügen und Löschen des Lastausgleichsdiensts in VMware NSX Manager stellt Citrix ADM die Citrix ADC Instanzen dynamisch bereit und zerstört sie. Für diese dynamische Provisioning müssen die Citrix ADC VPX -Lizenzzuweisungen in Citrix ADM automatisiert werden. Wenn die Citrix ADC Lizenzen auf Citrix ADM hochgeladen werden, führt Citrix ADM die Rolle des Lizenzservers aus.

Voraussetzungen

> **Hinweis**
>
> Diese Integration wird nur für **VMware NSX for vSphere 6.1 oder früher**unterstützt.

- Citrix ADM, Version 13.0 Setup in hoher Verfügbarkeit und auf ESX installiert.
- Citrix ADC VPX, Version 13.0
- Citrix ADC VPX -Lizenzen für Citrix ADC VPX Instanzen, Version 13.0
- Installieren Sie VMware ESXi Version 4.1 oder höher mit Hardware, die die Mindestanforderungen erfüllt.
- Installieren Sie VMware Client auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
- Installieren Sie VMware OVF Tool (erforderlich für VMware ESXi Version 4.1) auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.

Bereitstellung von Citrix ADM- und Citrix ADC Instanzen mit hoher Verfügbarkeit

Installieren Sie zum Bereitstellen des NetScaler ADM HA-Setups die NetScaler ADM-Imagedatei, die Sie von der Citrix Download-Site heruntergeladen haben. Weitere Informationen zum Bereitstellen des NetScaler ADM HA-Setups finden Sie unter Bereitstellen von NetScaler ADM in Hochverfügbarkeit.

Einrichten von NetScaler ADM HA Endpoint Details

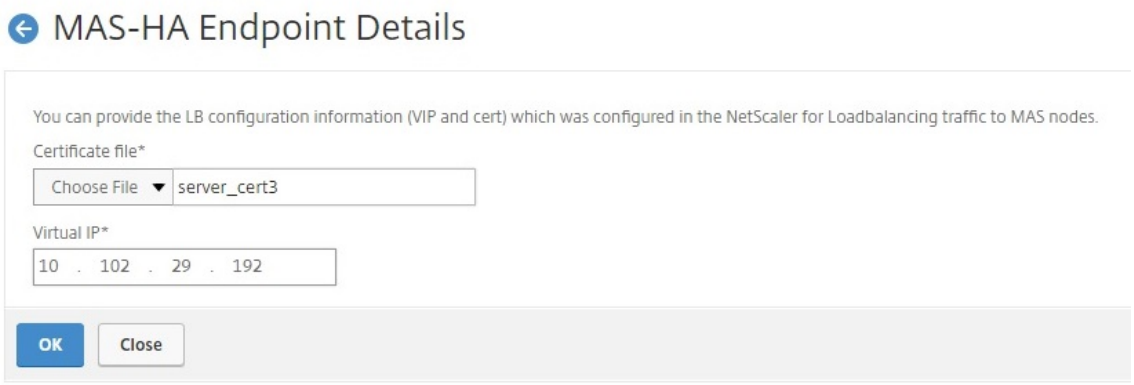
Um VMware NSX Manager in Citrix ADM zu integrieren, das im HA-Modus bereitgestellt wird, müssen Sie zuerst die virtuelle IP-Adresse der Citrix ADC Instanz für den Lastausgleich eingeben. Sie müssen auch die Zertifikatdatei, die auf dem virtuellen Citrix ADC Load Balancing Server vorhanden ist, in das Citrix ADM Dateisystem hochladen.

So stellen Sie Konfigurationsinformationen für den Lastausgleich in Citrix ADM bereit:

1. Navigieren Sie im Citrix ADM HA-Knoten zu **System** > **Bereitstellung**.

2. Klicken Sie oben rechts auf **HA-Einstellungen**, und klicken Sie auf der Seite **MAS-HA-Einstellungen** auf **MAS-HA-Endpunktdetails**.

3. Laden Sie auf der Seite "**MAS-HA-Endpoint-Details** "dasselbe Zertifikat hoch, das bereits auf der NetScaler ADC Instanz für den Lastausgleich vorhanden ist.
4. Geben Sie die virtuelle IP-Adresse der NetScaler ADC Instanz für den Lastausgleich ein, und klicken Sie auf **OK**.



Registrieren von VMware NSX Manager bei NetScaler ADM

Wenn Sie zwei Citrix ADM -Server in hoher Verfügbarkeit einrichten, befinden sich die beiden Serverknoten im Aktiv-Passiv-Modus. Melden Sie sich am primären Citrix ADM -Serverknoten an, um VMware NSX Manager bei Citrix ADM in HA zu registrieren und einen Kommunikationskanal zwischen ihnen zu erstellen.

So registrieren Sie VMware NSX Manager bei Citrix ADM in HA:

1. Navigieren Sie im primären Citrix ADM -Serverknoten zu **Orchestration** > **SDN Orchestration** > **VMware NSX Manager**.
2. Klicken Sie auf **NSX Manager-Einstellungen konfigurieren**.
3. **Legen Sie auf der Seite NSX Manager-Einstellungen konfigurieren** die folgenden Parameter fest:

    a) NSX Manager-IP-Adresse: IP-Adresse von NSX Manager.

b) NSX Manager-Benutzername —Administratorbenutzername von NSX Manager.

c) Kennwort - Kennwort des administrativen Benutzers von NSX Manager.

4. Legen Sie im Abschnitt Citrix ADM-Konto, das von NSX Manager verwendet wird, das Citrix ADC -Treiberkennwort für NSX Manager fest.
5. Klicken Sie auf **OK**.

Hochladen von Lizenzen in NetScaler ADM

Laden Sie die NetScaler ADC VPX Lizenzen auf NetScaler ADM hoch, damit NetScaler ADM den Instanzen während der Orchestrierung mit NSX automatisch Lizenzen zuweisen kann.

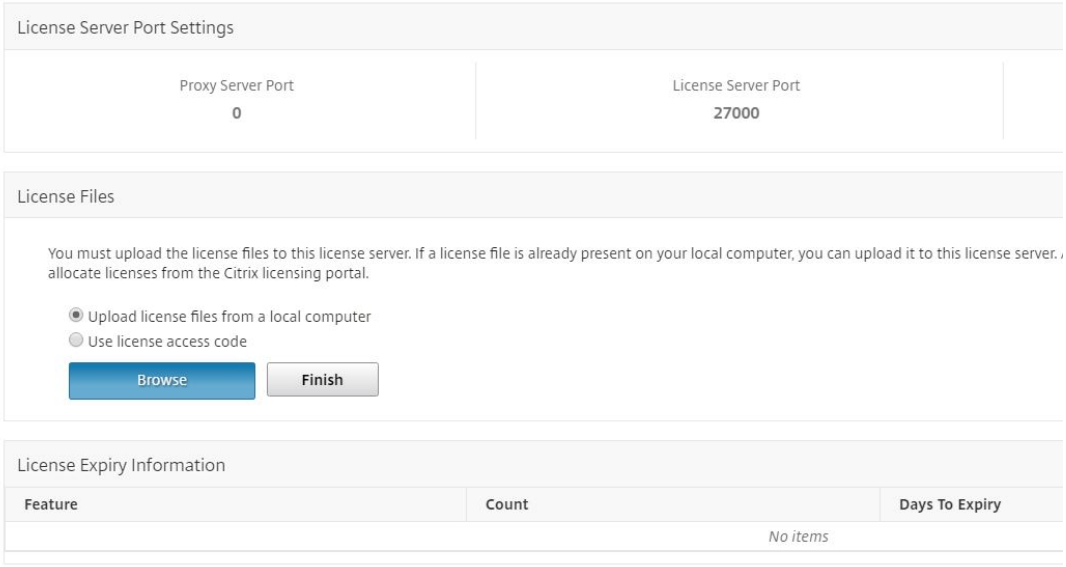
So installieren Sie Lizenzdateien auf NetScaler ADM:

1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Lizenzen.**
2. Wählen Sie im Abschnitt **Lizenzdateien** eine der folgenden Optionen aus:

   a) **Upload von Lizenzdateien von einem lokalen Computer** : Wenn eine Lizenzdatei bereits auf dem lokalen Computer vorhanden ist, können Sie sie in NetScaler ADM hochladen. Um Lizenzdateien hinzuzufügen, klicken Sie auf **Durchsuchen** und wählen Sie die Lizenzdatei (.lic) aus, die Sie hinzufügen möchten. Dann klick **Fertig stellen**.

   b) **Lizenzzugangscode verwenden** - Citrix sendet den Lizenzzugangscode für die von Ihnen erworbenen Lizenzen per E-Mail. Um Lizenzdateien hinzuzufügen, geben Sie den Lizenzzugriffscode in das Textfeld ein und klicken Sie dann auf **Lizenzen abrufen**.

   > **Hinweis:**Sie können dem NetScaler ADM
   >
   > jederzeit über die Lizenzeinstellungen weitere Lizenzen hinzufügen.



Hochladen von NetScaler ADC VPX Images in NetScaler ADM

Fügen Sie NetScaler ADC Images zu NetScaler ADM hinzu, damit NetScaler ADM diese Images wie im Servicepaket definiert verwendet.

So laden Sie Citrix ADC VPX Images in Citrix ADM hoch:

1. Navigieren Sie in NetScaler ADM zu **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **ESX NSVPX-Images**.
2. Klicken Sie auf **Hochladen**, und wählen Sie im lokalen Speicherordner das NetScaler ADC VPX Zip-Paket aus.

Erstellen von Servicepaketen in Citrix ADM

Erstellen Sie Servicepakete in NetScaler ADM, um den Satz von SLAs zu definieren, der angibt, wie die NetScaler ADC Ressourcen zugewiesen werden.

So erstellen Sie Dienstpakete in Citrix ADM:

1. Navigieren Sie in Citrix ADM zu **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Service Packages**, und klicken Sie auf **Hinzufügen**, um ein neues Servicepaket hinzuzufügen.
2. Legen Sie auf der Seite **Service Package** im Abschnitt **Grundeinstellungen** die folgenden Parameter fest:

    a) Name —Name eines Servicepakets

    b) Isolationsrichtlinie —wählen Sie **Dediziert**

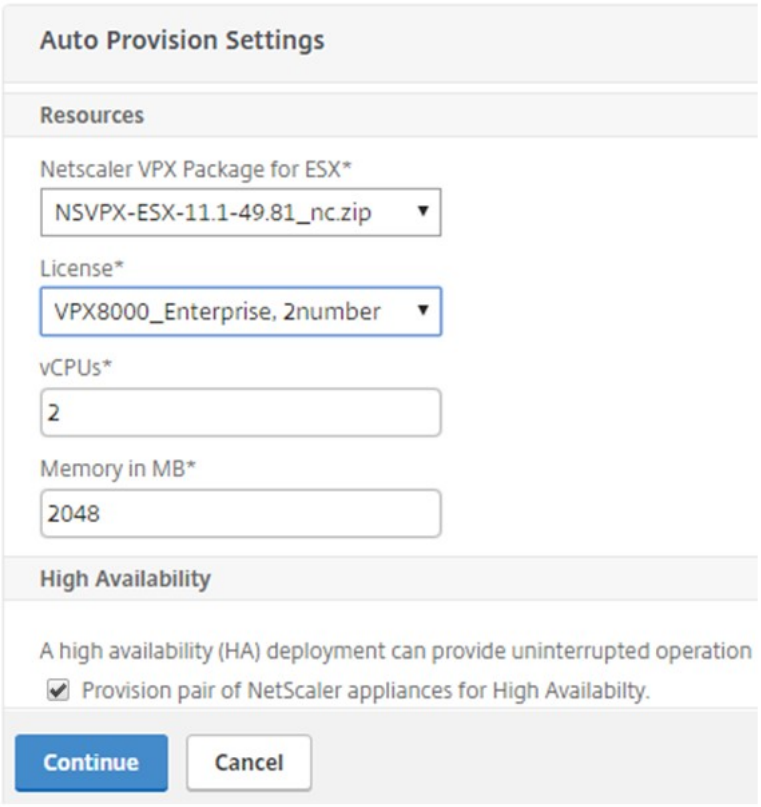
c) Citrix ADC Instanz Provisioning: Wählen Sie **Instanz bei Bedarf erstellen**.

d) Auto Provisioning Platform - Wählen Sie **CitrixADC SDX**

e) Klicken Sie auf **Weiter**.

3. Wählen Sie im Abschnitt **AutoProvisions-Einstellungen** das kürzlich hochgeladene Citrix ADC VPX Zip-Paket für die Bereitstellung auf der NSX-Plattform aus, wählen Sie die entsprechende Lizenz aus und klicken Sie auf **Weiter**.

> **Hinweis Aktivieren Sie**
>
> im Abschnitt "**Hohe Verfügbarkeit** "das Kontrollkästchen, um NetScaler ADC Instanzen für HA bereitzustellen.



> **Hinweis**
>
> Der Name der Lizenz, der in dem in der obigen Abbildung gezeigten Listenfeld angezeigt wird, Vpx8000_Advanced, 2-Nummer ist ein Beispiel und wird wie folgt erklärt:
>
> - VPX: Die Lizenz besteht darin, NetScaler ADC VPX Instanzen bereitzustellen.
> - 8000 —Die nutzbare Bandbreite beträgt 8 GB
> - Erweitert: Citrix bietet drei Arten von Lizenzen: Standard, Advanced und Premium

> - 2 Nummer - zwei NetScaler ADC VPX Instanzen können mit dieser Lizenz bereitgestellt werden
>
> Der Name der Lizenz, der im**Listenfeld Lizenz** angezeigt wird, hängt von der Lizenz ab, die Sie von Citrix erworben haben.

4. Klicken Sie auf **Weiter**.
5. Das Servicepaket wird in NSX Manager veröffentlicht. Navigieren Sie in NSX Manager zu **Service Definitions** > **Service Manager**. Sie können Citrix ADM als einer der Dienstmanager anzeigen. Dies bedeutet, dass die Registrierung erfolgreich ist und eine bidirektionale Kommunikation zwischen NSX Manager und Citrix ADM hergestellt wird.

> **Hinweis:**
>
> Für Citrix ADM in Hochverfügbarkeitsbereitstellung werden die Lizenzen nur in den Citrix ADM -Lizenzserverknoten hochgeladen. Die NetScaler ADM Knoten befinden sich im Aktiv-passiven Modus.

Ausführen des Lastausgleichsdiensteinfügens für Edge

Führen Sie die Einfügung des Lastausgleichsdienstes auf dem vorhandenen NSX Edge Gateway durch, d. h. die Lastausgleichsfunktion vom NSX Load Balancer auf NetScaler ADC.

So fügen Sie den Load Balancing-Dienst auf NSX Edge Gateway ein:

1. Navigieren Sie in NSX Manager zu **Home** > **Netzwerk und Sicherheit** > **NSX Edges**, und doppelklicken Sie, um das von Ihnen konfigurierte Edge-Gateway auszuwählen.
2. Klicken Sie auf **Verwalten**, wählen Sie auf der Registerkarte **Load Balancer** die Option **Globale Konfiguration** aus, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie **Load Balancer aktivieren** und **Service Insertion aktivieren** aus, um sie zu aktivieren.
4. Wählen Sie unter **Service Definition**das Servicepaket aus, das in NSX Manager veröffentlicht wurde.
5. Konfigurieren Sie eine virtuelle Netzwerkkarte für die Verwaltungsschnittstelle und eine oder mehrere virtuelle Netzwerkkarten für Datenschnittstellen. Wählen Sie die Netzwerke für die Verwaltung und die Daten entsprechend aus.

> **Hinweis**
>
> Wählen Sie im Modus Primäre IP-Zuweisung die Option IP-Pool aus. Citrix ADM unterstützt keine manuelle oder DHCP-Zuweisung von IP-Adressen.

6. Klicken Sie auf das Aktualisierungssymbol, um die Erstellung der Laufzeit zu sehen.

> **Hinweis**
>
> Da Sie zwei Citrix ADC VPX Instanzen in der HA-Bereitstellung bereitstellen, werden im NSX Manager zwei Laufzeiten erstellt.
>
> Möglicherweise müssen Sie den Bildschirm aktualisieren, um die auf dem Bildschirm angezeigten Laufzeiten zu sehen.

7. Wählen Sie die Laufzeit aus, klicken Sie auf **Aktionen**und wählen Sie im Popupmenü die Option **Installieren** aus. Für HA wiederholen Sie dies auch für die andere Laufzeit.
8. Wenn beide virtuellen Maschinen gestartet werden, ändert sich der Wert von Status in "In Dienst"und der Wert des Installationsstatus ändert sich in "Aktiviert".

   > **Hinweis:**
   >
   > Möglicherweise müssen Sie den Bildschirm aktualisieren, um die Statusänderung zu sehen.

9. Navigieren Sie in Citrix ADM zu **Orchestration** > **Requests**, um Fortschrittsdetails zum Abschluss der Diensteinfügung anzuzeigen. Sie können sehen, dass eine Anforderung zum Erstellen und Aktualisieren der Laufzeit in Citrix ADM eingegangen ist. Wenn die Laufzeit aktualisiert wurde, wählen Sie die Anforderung aus und klicken Sie auf die Schaltfläche **Tasks**, um anzuzeigen, dass Citrix ADM in NSX Manager hinzugefügt wurde.

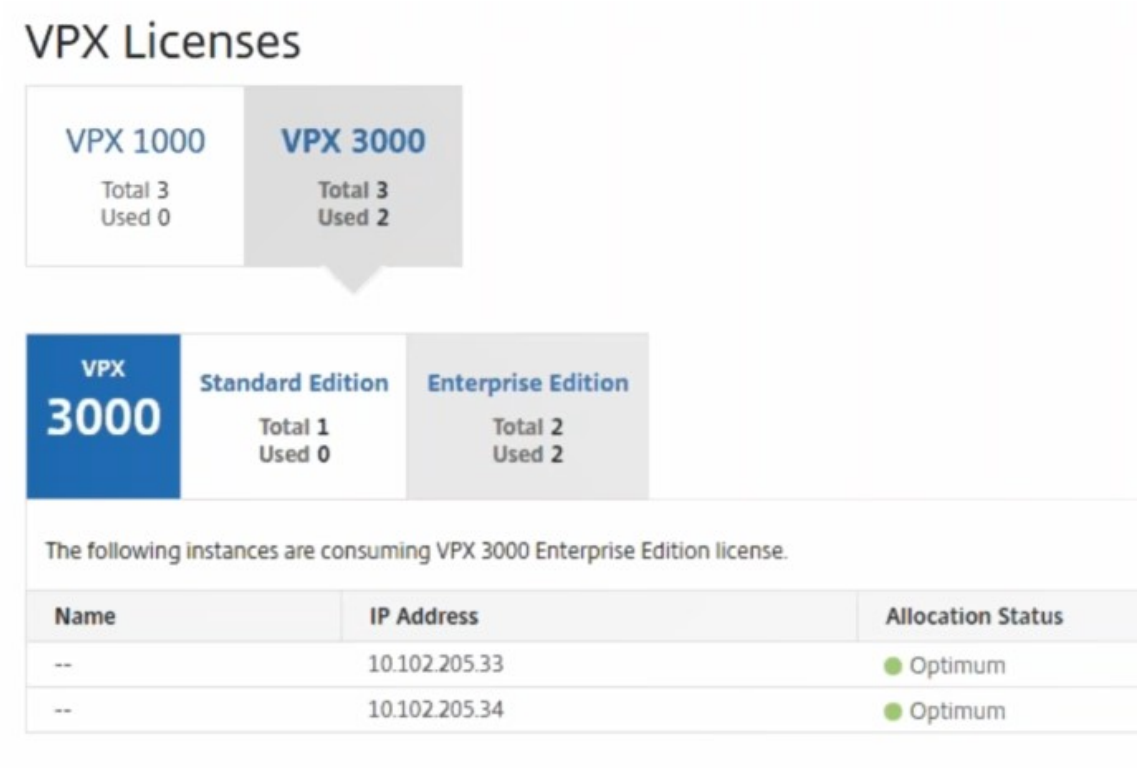
   Für HA gibt es zwei Anforderungen zum Erstellen und Aktualisieren von zwei Ausführungszeiten in Citrix ADM. Wenn beide Laufzeiten aktualisiert wurden, wählen Sie beide Anforderungen aus, und klicken Sie auf die Schaltfläche **Tasks**, um anzuzeigen, dass zwei Citrix ADM HA-Knoten in NSX Manager hinzugefügt wurden.

10. Navigieren Sie in Citrix ADM zu **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Edge-Gateways**. Im rechten Seitenbereich können Sie anzeigen, dass Citrix ADC VPX dem NSX Edge Gateway hinzugefügt wurde.

    Für HA können Sie sehen, dass dem NSX Edge Gateway zwei NetScaler ADC VPX-Instanzen im HA-Modus hinzugefügt wurden.

11. Navigieren Sie in Citrix ADM zu **Netzwerke** > **LizenzenVPX-Lizenzen**. Wählen Sie die NetScaler ADC VPX -Lizenz und die installierte Edition aus.

    Die NetScaler ADC VPX Instanzen, die sich im HA-Modus befinden, verbrauchen zwei Lizenzen, und der Status wird wie folgt auf dem Bildschirm angezeigt.



Wenn die Diensteinfügung abgeschlossen ist, können Sie StyleBooks verwenden, um die NetScaler ADC Instanzen mit einer der folgenden beiden Methoden zu konfigurieren:

- Konfigurieren der Lastenausgleichsdienste auf NetScaler ADC VPX in VMware NSX Manager GUI
- Konfigurieren der Lastenausgleichsdienste auf NetScaler ADC VPX in der NetScaler ADM GUI

Konfigurieren der Lastenausgleichsdienste auf NetScaler ADC VPX in VMware NSX Manager GUI

Führen Sie die folgende Aufgabe aus, um die Konfiguration von Lastausgleichsdiensten auf dem NSX Edge-Gateway gerät mithilfe integrierter StyleBooks zu aktivieren.

Navigieren Sie in NSX Manager zu **Home** > **Netzwerk und Sicherheit** > **NSX Edges**, und doppelklicken Sie, um das von Ihnen konfigurierte Edge-Gateway auszuwählen.

Pools und Poolmitglieder erstellen

Erstellen Sie einen Pool von Servern und Mitgliedern mit unterschiedlichen Kapazitäten.

1. Klicken Sie auf **Verwalten**und wählen Sie auf der Registerkarte **Load Balancer** die Option **Pools**aus und klicken Sie auf das Symbol "**+**", um einen neuen Pool hinzuzufügen, und legen Sie die folgenden Parameter fest:

   a) Name —Name des neuen Pools

   b) Algorithmus - Wählen Sie einen Algorithmus aus der Dropdownliste aus, auf der der Pool ausgewählt wird.

   c) Monitore —Stellen Sie sicher, dass der Servicemonitor auf default_http_monitor eingestellt ist

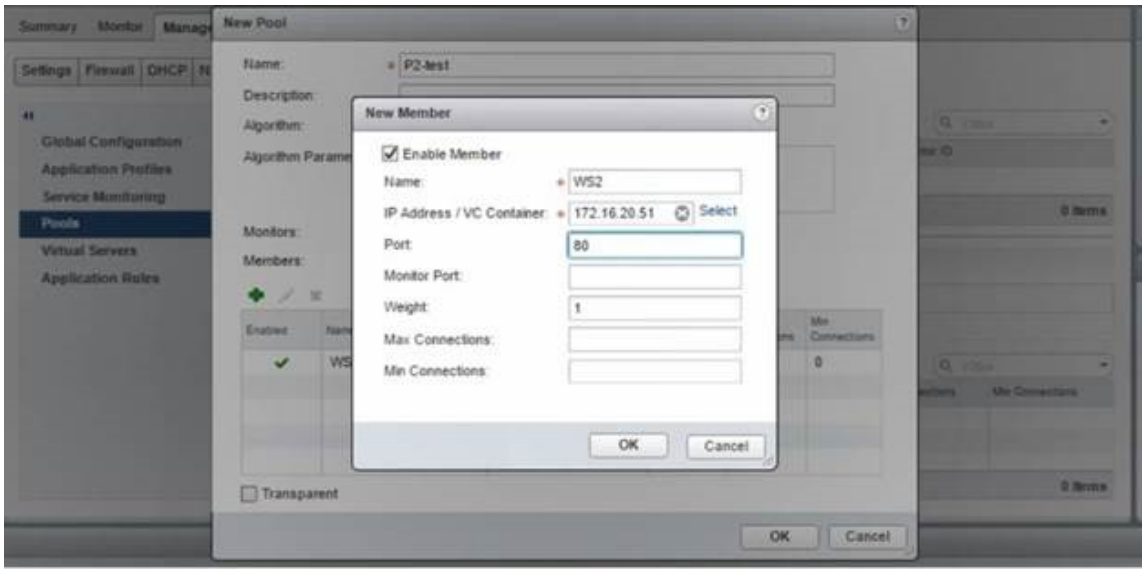
   d) Mitglieder —Klicken Sie auf „+", um Mitglieder zum Pool hinzuzufügen, und geben Sie die erforderlichen Parameter in das Fenster Neues Mitglied ein.

      i. Name - Name des Mitglieds

      ii. IP-Adresse/VC-Container —Klicken Sie auf Auswählen, um das Objekt aus der verfügbaren Liste auszuwählen, oder geben Sie die IP-Adresse des Objekts ein.

2. Klicken Sie auf **OK**.

   Fügen Sie beliebig viele Mitglieder hinzu.



Erstellen virtueller Server

Erstellen Sie einen Satz virtueller Server, und weisen Sie jedem virtuellen Server einen Pool zu.

1. Klicken Sie auf **Verwalten**und wählen Sie auf der Registerkarte Load Balancer die Option **Virtuelle Server**aus und klicken Sie auf das Symbol "**+**", um einen virtuellen Server hinzuzufügen, und legen Sie die folgenden Parameter fest:

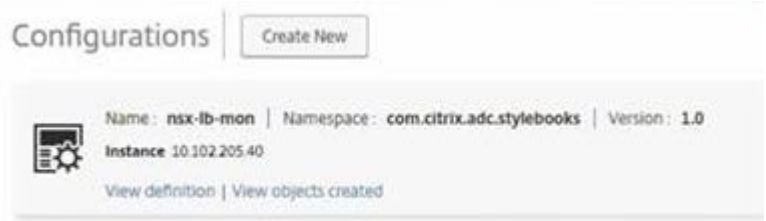
a) Anwendungsprofil: Standardmäßig wird das Dienstprofil angezeigt, das Sie in Citrix ADM erstellt haben.

b) Name —Name des virtuellen Servers.

c) IP-Adresse —Klicken Sie auf Auswählen, um einen vorhandenen Pool von IP-Adressen auszuwählen oder einen neuen Pool von IP-Adressen zu erstellen.

d) Standardpool - Wählen Sie den Standardpool aus der Dropdownliste aus.

2. Klicken Sie auf **OK**.
3. Navigieren Sie in NetScaler ADM zu **Orchestration** > **Requests**, um Fortschrittsdetails zum Abschluss der Diensterstellung auf einer oder mehreren ausgewählten NetScaler ADC Instanzen anzuzeigen.
4. Navigieren Sie in NetScaler ADM zu **Applications** > **Configuration**, und überprüfen Sie, ob das `nsx-lb-mon` Config Pack erstellt wurde.



Konfigurieren der Lastenausgleichsdienste auf NetScaler ADC VPX in der NetScaler ADM GUI

Stellen Sie mithilfe von NetScaler ADM StyleBooks Load Balancer-Konfigurationen auf der NetScaler ADC-Instanz bereit. Für HA wird die Konfiguration auf beiden Citrix ADC Instanzen bereitgestellt, die sich in HA befinden.

So erstellen Sie Konfigurationspakete über StyleBooks:

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfiguration** > **Neu erstellen**, und wählen Sie das **HTTP/SSL LoadBalancing (mit Monitoren) StyleBook** aus der Liste aus. Das StyleBook wird als Benutzeroberflächenseite geöffnet, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben.
2. Geben Sie Werte für alle erforderlichen Parameter an.
3. Wählen Sie die Citrix ADC VPX Zielinstanz aus, die in der NSX-Umgebung bereitgestellt wird, und klicken Sie auf **Erstellen**, um die Konfiguration auf das ausgewählte Gerät anzuwenden. Wählen Sie für die HA-Bereitstellung die Instanzen aus, die sich im HA-Modus befinden.

Überprüfen der Erstellung virtueller Server und Dienstgruppen in Citrix ADC VPX Instanzen

Sie können anzeigen, dass die Dienstgruppen und virtuellen Server erstellt werden, indem Sie sich bei der Citrix ADC VPX Instanz anmelden.

So zeigen Sie die Dienstgruppen und virtuellen Server an:

1. Melden Sie sich bei der NetScaler ADC VPX-Instanz an. Bei der HA-Bereitstellung müssen Sie sich bei beiden Citrix ADC Instanzen anmelden, die sich in HA befinden.
2. Navigieren Sie zu **Konfiguration** > **System** > **Netzwerk**. Im rechten Bereich können Sie die hinzugefügten IP-Adressen sehen. Klicken Sie auf den Hyperlink IP-Adresse, um die Details anzuzeigen. Sie können sehen, dass die Subnetz-IP-Adresse mit der IP-Adresse der Webschnittstelle übereinstimmt, die in NSX hinzugefügt wurde.
3. Navigieren Sie als Nächstes zu **Traffic Management** > **Load Balancing** > **Virtuelle Server** und sehen Sie sich die Details des virtuellen Servers an.
4. Navigieren Sie als Nächstes zu **Service Groups** und sehen Sie sich die Servicegruppendetails an.
5. Navigieren Sie schließlich zu **Konfiguration** > **System** > **Lizenzen**, um die Lizenzen anzuzeigen, die auf diese Instanz angewendet werden.

Load Balancing Services löschen

Wenn die Lastenausgleichsdienste für die NetScaler ADC VPX-Instanzen, die auf dem NSX Manager bereitgestellt werden, nicht mehr erforderlich sind, können Sie die zuvor durchgeführten Diensteinfügungen löschen.

So löschen Sie die Konfiguration und das Einfügen von Diensten:

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfiguration**, wählen Sie die erstellte Anwendungskonfiguration aus, und löschen Sie die Konfiguration, indem Sie auf das Symbol “X” klicken.
2. Navigieren Sie in NSX Manager zu dem Edge-Gateway, mit dem die Citrix ADC VPX Instanz verbunden ist. **Navigieren Sie zu**Manage**>**Load Balancer**>**Global Configuration**, klicken Sie mit der rechten Maustaste auf den Runtime-Eintrag und klicken Sie dann auf Bereitstellung aufheben.** Die virtuelle Maschine wird außer Betrieb genommen.
3. Navigieren Sie in NetScaler ADM zu **Orchestration** > **Cloud Orchestration** > **Edge-Gateways**. Stellen Sie sicher, dass es keine entsprechende Zuordnung von Edge-Gateway zu gelöschter Instanz gibt.

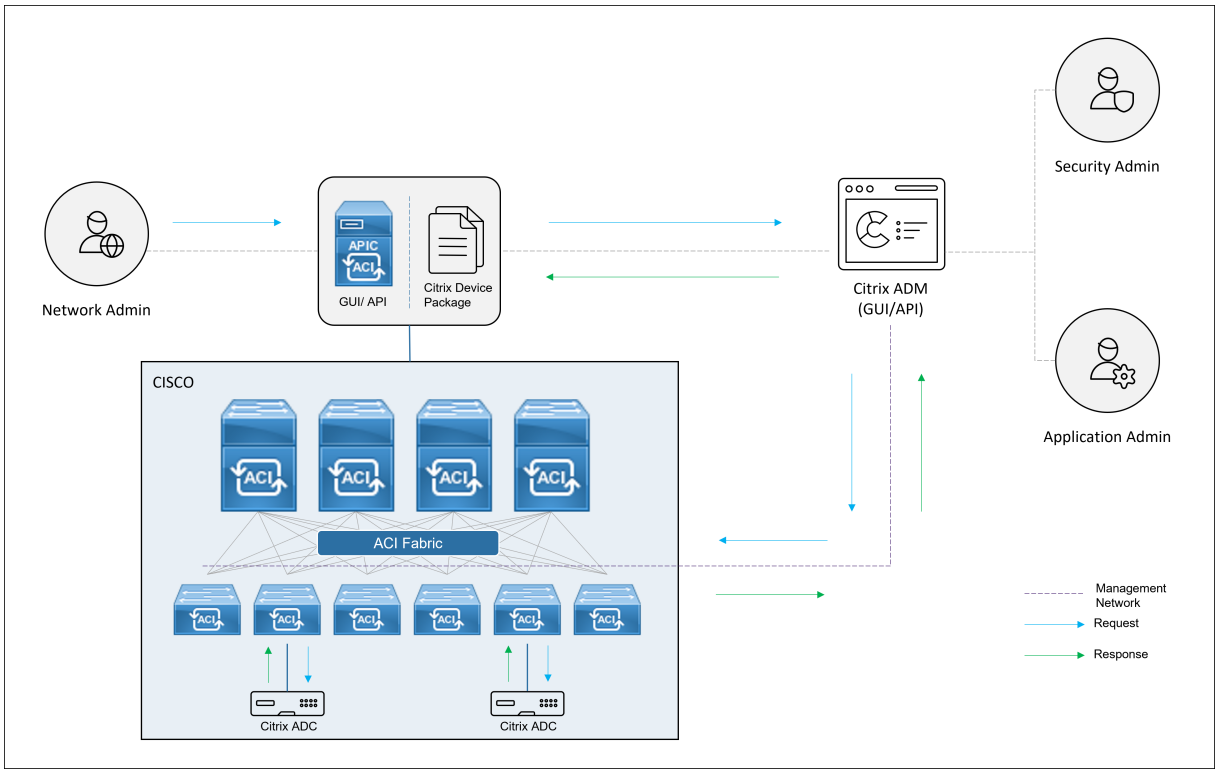
NetScaler ADC Automatisierung mit NetScaler ADM im Cisco ACI-Hybridmodus

February 5, 2024

Cisco ACI hat die Unterstützung für den Hybrid-Modus in Version 1.3 (2f) eingeführt. Im Hybridmodus können Sie die Netzwerkautomatisierung über den Application Policy Infrastructure Controller (APIC) durchführen und gleichzeitig die L4-L7-Konfiguration an Citrix Application Delivery Management (ADM) delegieren, das als Gerätemanager im APIC fungiert.

Die NetScaler ADC Hybridmodus-Lösung wird von einem Hybridmodusgerätepaket und NetScaler ADM unterstützt. Sie müssen das Paket des Hybrid-Modus-Gerätes im APIC hochladen. Dieses Paket stellt alle konfigurierbaren Netzwerk-L2-L3-Entitäten von Citrix ADC bereit. Die Anwendungsparität wird von StyleBook von Citrix ADM dem APIC zugeordnet. Mit anderen Worten, StyleBook fungiert als Referenz zwischen L2-L3- und L4-L7-Konfigurationen für eine bestimmte Anwendung. Sie müssen bei der Konfiguration der Netzwerkentitäten aus dem APIC für Citrix ADC einen StyleBook-Namen angeben.

Die folgende Abbildung bietet einen Überblick über NetScaler ADC in einer Lösung im Hybrid-modus:

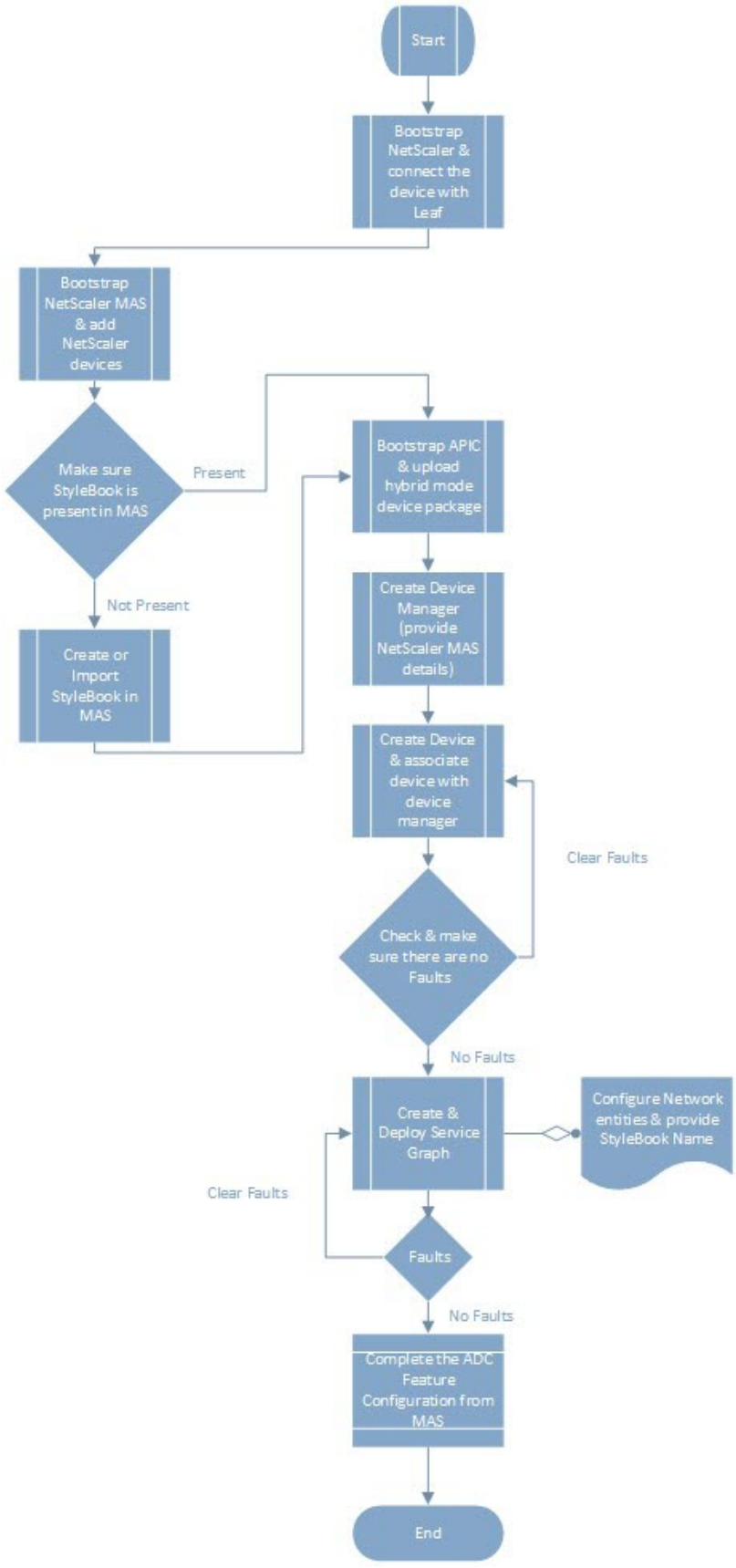


Im Hybridmodus wird die NetScaler ADC Konfiguration in den folgenden zwei Phasen durchgeführt:

1. Netzwerkstitching erfolgt über die Cisco APIC
2. Die Konfiguration erfolgt über das Citrix ADM

Für jede bestimmte Anwendung muss ein Netzwerkadministrator im Rahmen der Erstellung und Bereitstellung des Service-Graphen im Cisco APIC netzwerkspezifische Details wie IP-Adressen, Port, VLAN (automatisiert) usw. angeben. Diese Konfigurationsdetails werden dann über das Gerätepaket an Citrix ADM übertragen, und Citrix ADM verarbeitet sie intern und konfiguriert den Citrix ADC. Ein Anwendungsadministrator erstellt die ADC-bezogene Konfiguration der Anwendung mithilfe von StyleBook in Citrix ADM, und diese Konfigurationen werden dann von Citrix ADM auf Citrix ADC übertragen. Der Cisco APIC und Citrix ADM kommunizieren über das Verwaltungsnetzwerk mit dem ADC.

Das folgende Diagramm zeigt einen NetScaler ADC Workflow in der Hybridlösung:



Voraussetzungen

February 5, 2024

Stellen Sie Folgendes sicher:

- Sie verfügen über konzeptionelle Kenntnisse über Cisco ACI Komponenten und Citrix ADCs.
  - Weitere Informationen zu Cisco ACI und seinen Komponenten finden Sie in der Produktdokumentation unter: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
  - Weitere Informationen zu den Citrix ADCs finden Sie in der NetScaler ADC-Produktdokumentation unter:http://docs.citrix.com/.
- Alle erforderlichen Komponenten von Cisco ACI, einschließlich eines Cisco APIC im Rechenzentrum, werden eingerichtet und konfiguriert. Weitere Informationen zu Cisco ACI und seinen Komponenten finden Sie in der Produktdokumentation unter: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
- Sie haben Citrix ADC 11.1 oder höher installiert.
- Sie haben Citrix ADCs in Cisco ACI so konfiguriert, dass sie mithilfe des Cisco APIC verwaltet werden können.
- Sie haben NetScaler Application Delivery Management (ADM) in Ihrer Umgebung bereitgestellt. Weitere Informationen finden Sie unter NetScaler ADM 13.0.
- Verwaltungskonnektivität von APIC zu NetScaler ADM und ADC werden hergestellt.
- Notieren Sie sich:
  - Die Verbindungsschnittstellen und IP-Adressen, die für die Verwaltung und Datenpfadkonnektivität verwendet werden.
  - Details zum Leaf-Switch: Citrix ADC IP-Adressen, Ports, Schnittstellen usw.

> **Hinweis**
>
> In diesem Release unterstützt die Lösung für den Hybridmodus NetScaler ADC in einem einzigen Kontext, d. h. Administratorpartitionen werden nicht unterstützt.

NetScaler ADC im Hybrid-Modus mit Cisco APIC und NetScaler ADM konfigurieren

February 5, 2024

Führen Sie die folgenden Aufgaben aus, um einen Citrix ADC im Hybrid-Modus mithilfe von Cisco APIC und Citrix Application Delivery Management (ADM) zu konfigurieren:

1. Fügen Sie NetScaler ADC Instanzen in der Fabric zu NetScaler ADM hinzu. Anweisungen finden Sie unter Hinzufügen einer Instanz zu NetScaler ADM.
2. Verwenden Sie NetScaler ADM, um ein StyleBook für die Anwendung zu erstellen. Anweisungen finden Sie unter Erstellen eines StyleBook für die Anwendung mit NetScaler ADM.
3. Importieren Sie das NetScaler ADC Gerätepaket im Hybridmodus in Cisco APIC. Anweisungen finden Sie unter Importieren des NetScaler ADC Hybridmodus-Gerätepakets in Cisco APIC
4. Fügen Sie NetScaler ADM als Geräte-Manager im Cisco APIC hinzu. Anweisungen finden Sie unter Hinzufügen von NetScaler ADM als Geräte-Manager in Cisco APIC
5. Verwenden Sie Cisco APIC, um ein NetScaler ADC Gerät in Cisco ACI hinzuzufügen. Anweisungen finden Sie unter Hinzufügen des NetScaler ADC als Gerät in Cisco ACI
6. Erstellen und Bereitstellen einer Service-Graph-Vorlage. Anweisungen finden Sie unter Erstellen und Bereitstellen eines Service Graph
7. Konfigurieren Sie L4-L7-Parameter mithilfe von StyleBook in NetScaler ADM. Anweisungen finden Sie unter Konfigurieren des L4-L7-Parameters mit StyleBook von NetScaler ADM
8. Hängen Sie Endpunktereignisse vom Cisco APIC an oder trennen Sie sie. Weitere Informationen finden Sie unter Endpunktereignisse von APIC anhängen oder trennen

StyleBook für eine Anwendung mit NetScaler ADM erstellen

February 5, 2024

Ein StyleBook ist eine Konfigurationsvorlage, mit der Sie Citrix ADC Konfigurationen für jede Anwendung erstellen und verwalten können. Sie können ein StyleBook für die Konfiguration einer bestimmten NetScaler ADC Funktion erstellen, z. B. Lastenausgleich, SSL-Offload oder Content Switching. Sie können ein StyleBook entwerfen, um Konfigurationen für eine Enterprise-Anwendungsbereitstellung wie Microsoft Exchange oder Lync zu erstellen. Weitere Informationen finden Sie unter StyleBooks.

Sie können Ihr eigenes StyleBook für Ihre Anwendung erstellen oder das mit NetScaler Application Delivery Management (ADM) ausgelieferte APIC-HTTP-LB StyleBook ändern und verwenden.

Informationen zum Erstellen eines eigenen StyleBook für Ihre Anwendung in NetScaler ADM finden Sie unter How to Create Your Own StyleBooks.

Achten Sie beim Erstellen des StyleBook darauf, dass Sie das Service-Graph-Modell des APIC im StyleBook befolgen. Mit anderen Worten, das Servicediagramm des APIC für jede Anwendung folgt dem Verbraucher- und Anbietermodell, das über eine ADC-Funktion miteinander verbunden ist. Verbraucher und Anbieter sind als Endpunktgruppe (EPG) vertreten und stehen in einer 1:1 -Beziehung. Das gleiche Modell muss auch in StyleBook angewendet werden, wobei der Anbieter EPG als Servicegroup und jeder Endpunkt als Mitglied der Servicegruppe vertreten sein muss. Der ADC-Funktionsknoten muss durch einen virtuellen Server repräsentiert werden (z. B. einen virtuellen Lastausgleichsserver), und es muss eine 1:1 -Beziehung zwischen virtuellem Server und Servicegruppe bestehen.

Dadurch wird im Wesentlichen die Essenz des Service-Graphen erfasst und Sie können das Attach- oder Detach-Ereignis vom APIC behandeln, wobei ein Attach-Ereignis den Endpunkt an die entsprechende Servicegruppe bindet und ein Detach-Ereignis die Bindung aufhebt. Sie müssen sicherstellen, dass das Dienstdiagramm und das StyleBook für eine nahtlose Automatisierung von Netzwerkkonfigurationen L2-L3 zu ADC- L4-L7-Konfigurationen paritär sind.

NetScaler ADC-Gerätepaket im Hybrid-Modus in Cisco APIC importieren

February 5, 2024

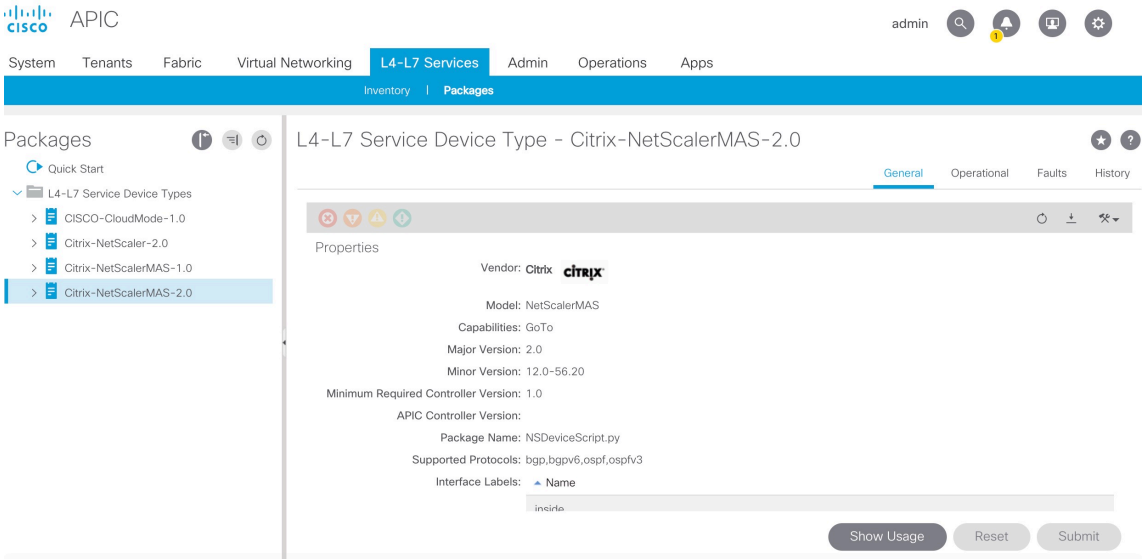
Das Gerätepaket für den Hybridmodus ist im Vergleich zu einem vollständig verwalteten Modus ein leichtes Paket. Nur L2-L3-Netzwerkparameter sind über das Gerätemodell verfügbar. Das Gerätemodell enthält nur eine generische ADC-Funktion und vier Funktionsprofile, die auf der Citrix ADC-Bereitstellung in der Fabric basieren (z. B. einarmige und zweiarmige und dasselbe mit RHI). Der Paketname des Hybridmodusgeräts lautet **NetScaler Hybridmodusgerätepakets 12.0 Build 56.20**. Suchen Sie auf der Citrix Downloadsite nach dem Hybridmodus-Gerätepaket, laden Sie es herunter und importieren Sie das Gerätepaket in den APIC.

> **Hinweis**
>
> Das Gerätepaket im Hybridmodus kann mit einem Gerätepaket im vollständig verwalteten Modus koexistieren.

Um das Gerätepaket im Hybridmodus mithilfe der APIC-GUI in den APIC zu importieren:

1. **Klicken Sie in der Menüleiste auf die Registerkarte**L4-L7 Services**und wählen Sie den Bereich Pakete aus.**

2. Klicken Sie im **Navigationsbereich** mit der rechten Maustaste auf **L4-L7-Gerätetypen und wählen Sie Gerätepaketimportieren**.
3. Klicken Sie im Dialogfeld **Gerätepaket importieren** auf **Durchsuchen**, um das heruntergeladene Citrix ADC Hybridmodusgerätpaket auszuwählen.
4. Klicken Sie auf **Submit**.
   Nachdem Sie das Gerätepaket erfolgreich in den APIC importiert haben, können Sie im **Navigationsbereich** die Details des Gerätepakets anzeigen, indem Sie auf den Gerätenamen klicken.



> **Wichtig!**
>
> Stellen Sie nach dem Import des Gerätepakets sicher, dass der APIC keine Fehler aufweist. Sie können die Fehler anzeigen, indem Sie im Fenster “Gerätetypen”auf die Registerkarte **Fehler** klicken.

NetScaler ADM als Geräte-Manager in Cisco APIC hinzufügen

February 5, 2024

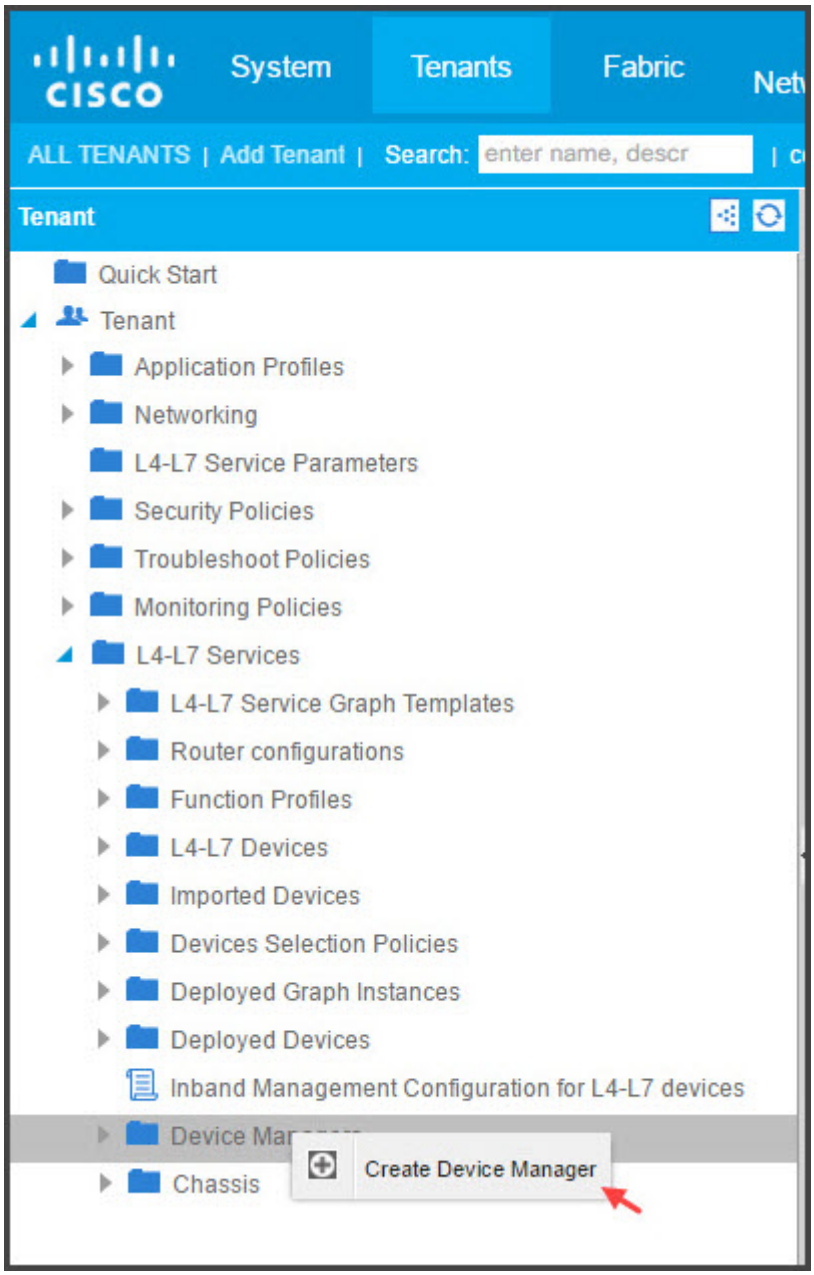
24. Mai 2018

Citrix Application Delivery Management (ADM) fungiert als zentralisierter Geräte-Manager für Citrix ADC, der auf Cisco ACI bereitgestellt wird. Sie müssen Citrix ADM als Geräte-Manager im Cisco APIC hinzufügen.

So fügen Sie Citrix ADM als Geräte-Manager im APIC mit der APIC-GUI hinzu:

1. Wechseln Sie in der Menüleiste zu **Mandanten > Alle Mandanten**.

2. Doppelklicken Sie im **Arbeitsbereich** auf den Namen des Mandanten.
3. Wählen Sie im **Navigationsbereich*tenant_name* > L4-L7 Services aus.**
4. Klicken Sie mit der rechten Maustaste auf **Gerätemanager** und klicken Sie auf **Geräte-Manager erstellen**.



5. Gehen **Sie im Dialogfeld Geräte-Manager erstellen** wie folgt vor:

   a) Geben Sie im Feld **Geräte-Manager-Name** einen Namen für die Citrix ADM Bereitstellung ein, die Sie als Geräte-Manager registrieren möchten.

   b) Wählen Sie in der Dropdownliste **Management EPG** das Verwaltungs-EPG aus.

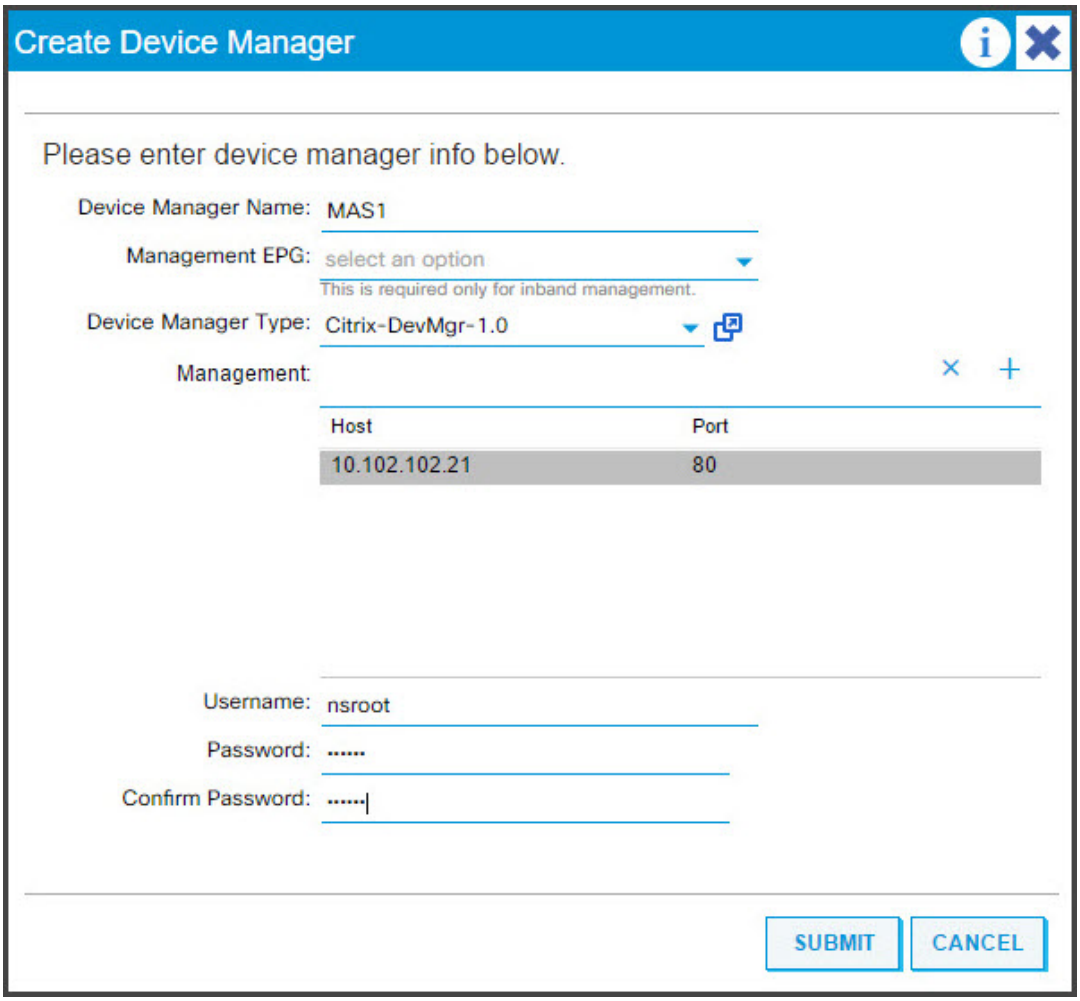
c) Wählen Sie in der Dropdownliste **Geräte-Manager-TypCitrix-Devmgr-1.0**aus.

d) Klicken Sie im Feld **Verwaltung** auf **+**, und fügen Sie die IP-Adresse und Portdetails der Citrix ADM Bereitstellung hinzu.

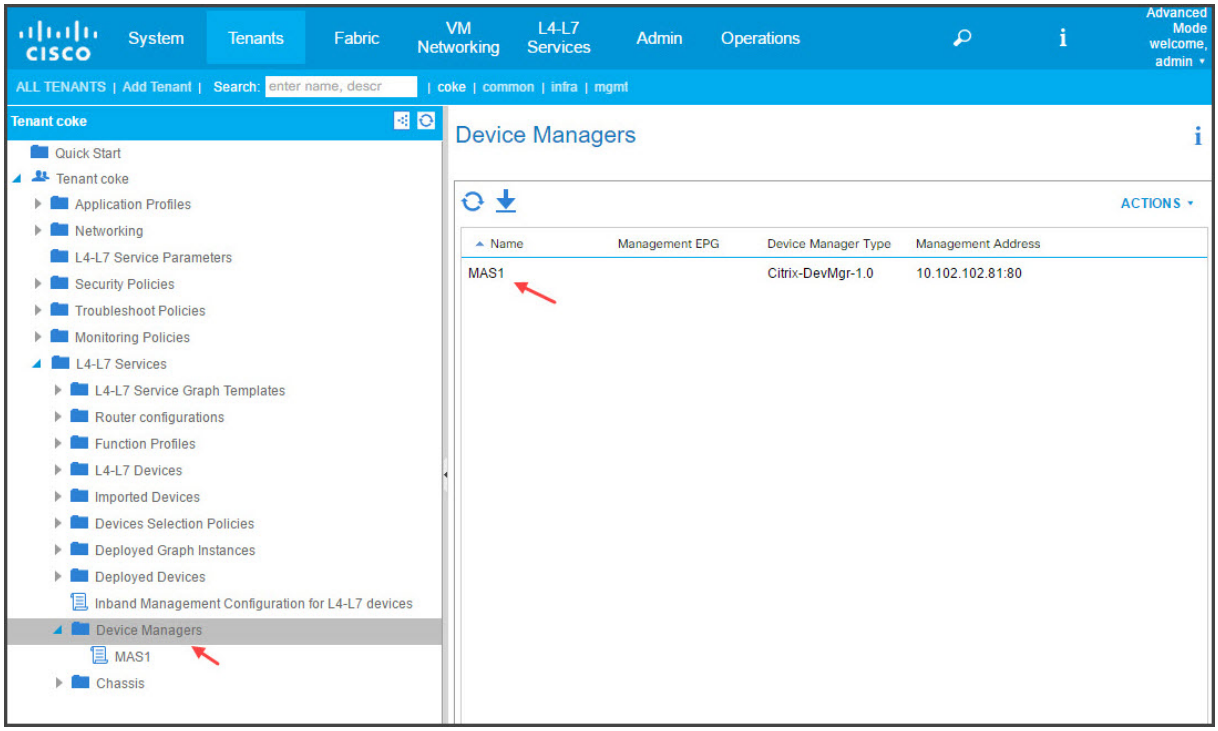
e) Geben Sie im Feld **Benutzername** den Benutzernamen für den Zugriff auf Citrix ADM ein.

f) Geben Sie in den Feldern **Kennwort** und **Kennwort bestätigen** das Kennwort für den Zugriff auf Citrix ADM ein.

g) Klicken Sie auf **SENDEN**.



Nachdem Citrix ADM erfolgreich als Geräte-Manager im APIC registriert wurde, wird der Geräte-Manager hinzugefügt und im **Navigationsbereich** angezeigt. Um den registrierten Gerätemanager anzuzeigen, gehen Sie im Navigationsbereich zu ***tenant_name* > L4-L7 Services > Device Manager.**



Hinweis

Stellen Sie sicher, dass es keine Verbindungsprobleme zwischen Cisco APIC und Citrix ADM gibt und dass Sie dieselben Anmeldeinformationen angeben, die Sie für den Zugriff auf Citrix ADM verwenden. Stellen Sie außerdem sicher, dass das Konto über Administratorrechte verfügt.

Wichtig!

Stellen Sie nach dem Import des Gerätepakets sicher, dass der APIC keine Fehler aufweist. Sie können die Fehler anzeigen, indem Sie im Fenster “Gerätetypen”auf die Registerkarte **Fehler** klicken.

Sie können Citrix ADM auch mithilfe von APIs als Geräte-Manager registrieren. Im Folgenden finden Sie eine XML-Nutzlast, die veranschaulicht, wie Sie mit APIs NetScaler ADM als Geräte-Manager hinzufügen können.

```
<polUni>
    <fvTenant name="coke">
        <vnsDevMgr name="MAS1">
            <vnsRsDevMgrToMDevMgr tDn="uni/infra/mDevMgr-Citrix-DevMgr-1.0" />
            <vnsCMgmts name="devMgmt" host="10.102.102.81" port="80"/>
            <vnsCCred name="username" value="nsroot"/>
            <vnsCCredSecret name="password" value="*****("/>
        </vnsDevMgr>
    </fvTenant>
</polUni>
```


NetScaler ADC als Gerät in Cisco ACI über APIC hinzufügen

February 5, 2024

Sie müssen ein Citrix ADC als L4-L7-Gerät zum APIC für die Netzwerkautomatisierung hinzufügen. Der APIC führt die Netzwerkstiftung zwischen Leaf und dem Citrix ADC Gerät basierend auf dem bereitgestellten Dienstdiagramm durch. Sie müssen die grundlegenden Einstellungen der Gerätekonfiguration konfigurieren, z. B. IP-Adressen für die Konfigurationsverwaltung, Gerätemanager und Anmeldeinformationen.

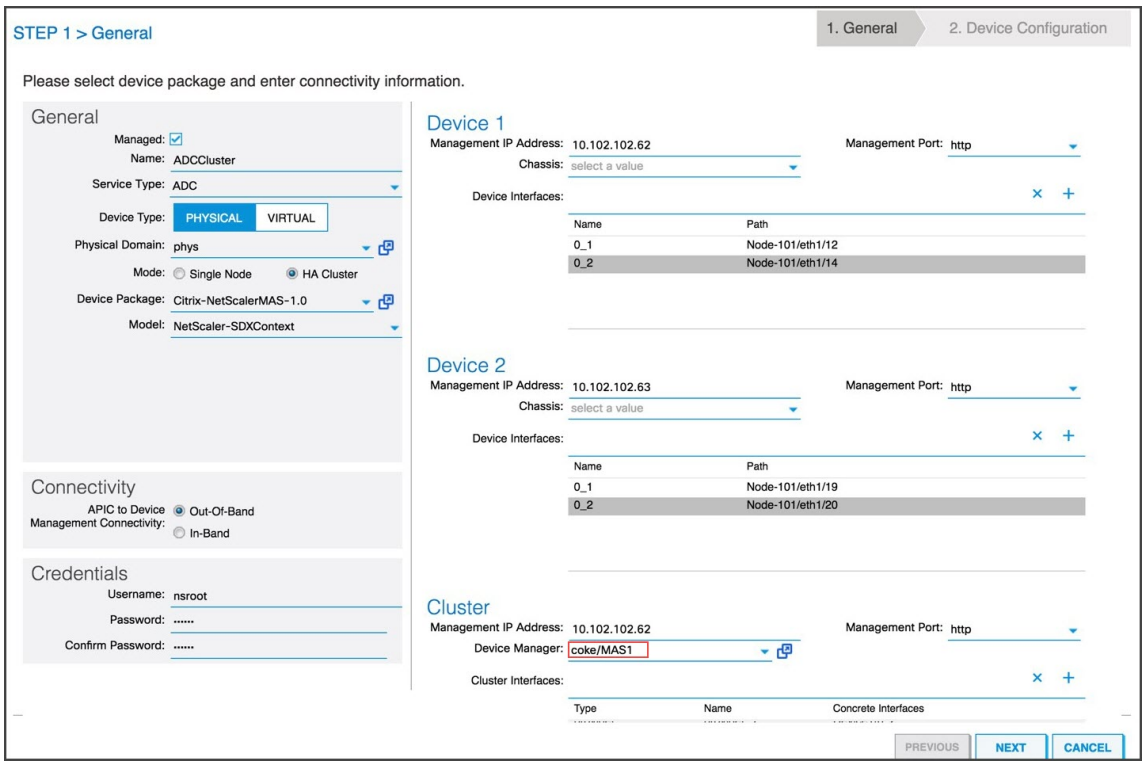
So registrieren Sie den Citrix ADC mithilfe der APIC-GUI als Gerät im APIC:

1. Wechseln Sie in der Menüleiste zu **Mandanten > Alle Mandanten**.
2. Doppelklicken Sie im **Arbeitsbereich** auf den Namen des Mandanten.
3. Wählen Sie im **Navigationsbereich*tenant_name* > L4-L7-Dienste > L4-L7-Geräte aus.**
4. Wählen Sie im Arbeitsbereich **Aktionen > L4-L7-Geräte erstellen**aus.
5. Gehen **Sie im Dialogfeld L4-L7-Geräte erstellen** im Abschnitt **Allgemein** wie folgt vor:
   a) Markieren Sie das Kontrollkästchen **Verwaltet** .
   b) Geben Sie im Feld **Name** einen Namen für das Gerät ein.
   c) Wählen Sie in der Dropdownliste **Diensttyp** die Option **ADC**aus.
   d) Wählen Sie im Feld **Gerätetyp** die Option **Physikalisch**aus.

      > **Hinweis:**
      >
      > Stellen Sie sicher, dass Sie für VMware ESX Virtual auswählen und die entsprechende Virtual Machine Manager (VMM) -Domäne verknüpfen.

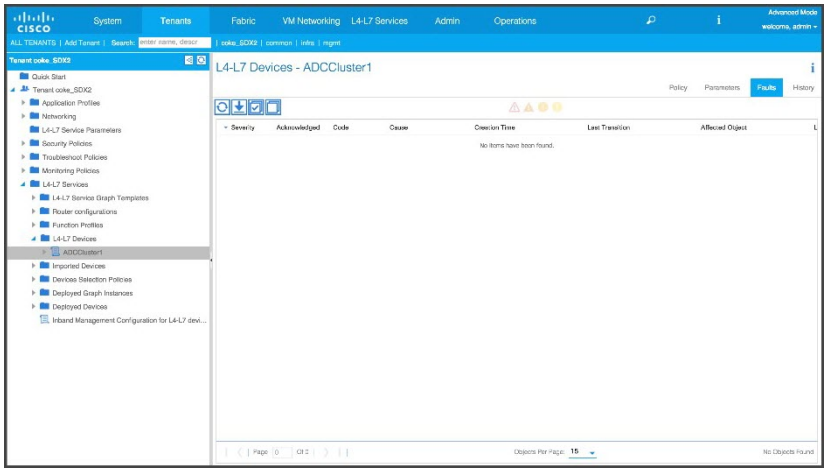
   e) Wählen Sie in der Dropdownliste **Physikalische Domäne** die physische Domäne aus.
   f) Wählen Sie im Feld **Modus** je nach Anforderung **Einzelknoten** oder **HA-Cluster**aus.
   g) Wählen Sie in der Dropdownliste **GerätepaketCitrix-NetScalerMAS-1.0**aus.
   h) Wählen Sie in der Dropdownliste **Modell** das Gerätemodell aus. Beispiel: Citrix ADC-MPX oder Citrix ADC-VPX.
6. Wählen Sie im Abschnitt **Konnektivität** im Feld ****APIC-zu-Geräteverwaltungskonnektivität** die Option **Out-of-Band** oder In-Band** aus, je nachdem, wie Citrix ADC in der Fabric konfiguriert ist.
7. Geben Sie im Abschnitt **Anmeldeinformationen** den Benutzernamen und das Kennwort für den Zugriff auf das Gerät an.

8. Füllen Sie im Abschnitt **Gerät 1bzw. Gerät 2** die verwaltungsbezogene Konfiguration aus.
9. Führen Sie im Abschnitt **Cluster** die verwaltungbezogene Konfiguration für den Cluster aus. Stellen Sie sicher, dass Sie in der Dropdownliste **Geräte-Manager** den Geräte-Manager auswählen, den Sie unter Hinzufügen von NetScaler ADM als Geräte-Manager in Cisco APICerstellt haben



10. Klicken Sie auf **WEITER**. Die Seite „Gerätekonfiguration“wird angezeigt. Das Gerätepaket für den Hybridmodus enthält keine geräte- und clusterspezifischen Konfigurationsdetails wie Hochverfügbarkeit, Aktivieren/Deaktivieren von Funktionen und Modi, Konfiguration für NTP, SNMP, SNMP-Alarme usw. Diese Konfigurationen müssen mit Citrix ADM durchgeführt werden.
11. Klicken Sie auf **FERTIG STELLEN**. Wenn Sie das Gerät erfolgreich im APIC registriert haben, wird das Gerät hinzugefügt und im Navigationsbereich angezeigt. Um das registrierte Gerät anzuzeigen, gehen Sie im Navigationsbereich zu ***tenant_name* > L4-L7-Dienste > L4-L7-Geräte > Gerätename.**

> **Wichtig!**
>
> Nachdem Sie das Gerät registriert haben, stellen Sie sicher, dass der APIC keine Fehler aufweist. Sie können die Fehler anzeigen, indem Sie im **Arbeitsbereich** auf die Registerkarte **Fehler** klicken.



Sie können ein Citrix ADC Gerät auch mithilfe von APIs registrieren. Im Folgenden finden Sie eine XML-Beispiel-Payload zum Hinzufügen von L4-L7-Geräten:

```
<polUni>

    <fvTenant name="coke">

    <vnsLDevVipname="ADCCluster1"funcType="GoTo" svcType="ADC">

     <vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0" />

     <vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>

     <vnsCMgmt name="devMgmt"host="10.102.102.67"port="80"/>

     <vnsCCred name="username" value="nsroot"/>

     <vnsCCredSecret name="password" value="****"/>

     <vnsRsALDevToDevMgr tnVnsDevMgrName="MAS1"/>

     <vnsCDev name="ADC1" devCtxLbl="C1">

     <vnsCIf name="1_1">

     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
        /33]"/>

     </vnsCIf>

     <vnsCIf name="1_2">

     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
        /35]"/>

     </vnsCIf>

     <vnsCMgmt name="devMgmt" host="10.102.102.65" port="80"/>
```



```
34
35        <vnsCCred name="username" value="nsroot"/>
36
37        <vnsCCredSecret name="password" value="****"/>
38
39        </vnsCDev>
40
41        <vnsCDev name="ADC2" devCtxLbl="C1">
42
43        <vnsCIf name="1_1">
44
45        <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
              /34]"/>
46
47        </vnsCIf>
48
49        <vnsCIf name="1_2">
50
51        <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
              /36]"/>
52
53        </vnsCIf>
54
55        <vnsCMgmt name="devMgmt" host="10.102.102.66" port="80"/>
56
57        <vnsCCred name="username" value="nsroot"/>
58
59        <vnsCCredSecret name="password" value="****"/>
60
61        </vnsCDev>
62
63        <vnsLIf name="outside">
64
65        <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
              mIfLbl-outside"/>
66
67        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
              cIf-1_1"/>
68
69        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
              cIf-1_1"/>
70
71        </vnsLIf>
72
73        <vnsLIf name="inside">
74
75        <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
              mIfLbl-inside"/>
76
77        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
              cIf-1_2"/>
78
79        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
```



```
            cIf-1_2"/>
80
81      </vnsLIf>
82
83      </vnsLDevV
84
85      </fvTenant>
86
87      </polUni>
```

Servicediagramm erstellen und bereitstellen

February 5, 2024

Sie müssen Cisco APIC-Dienstdiagrammvorlagen in APIC verwenden, um die Citrix ADCs zu erstellen und bereitzustellen. Stellen Sie sicher, dass Sie das ADC-Funktionsprofil verwenden, wenn Sie ein Service-Diagramm erstellen und bereitstellen.

Nachdem der Graph im APIC konfiguriert wurde, automatisiert der APIC die Gerätekonfiguration auf der Grundlage der Funktionsdefinitionen, der Gerätekonnektivität zur Fabric und der im Rahmen der Graphbereitstellung konfigurierten Entitäten. Das APIC automatisiert im Rahmen der Erstellung des Servicediagramms auch die Netzwerkkonfiguration, wie z. B. die VLAN-Zuweisung und deren Bindung, und die Konfiguration wird entfernt, sobald Sie das Diagramm aus dem APIC löschen.

Ein Service-Graph wird als zwei oder mehr Ebenen einer Anwendung dargestellt, zwischen denen die entsprechende Servicefunktion eingefügt wird. In einem Vertrag wird ein Service-Graph zwischen den Quell- und Ziel-EPGs eingefügt.

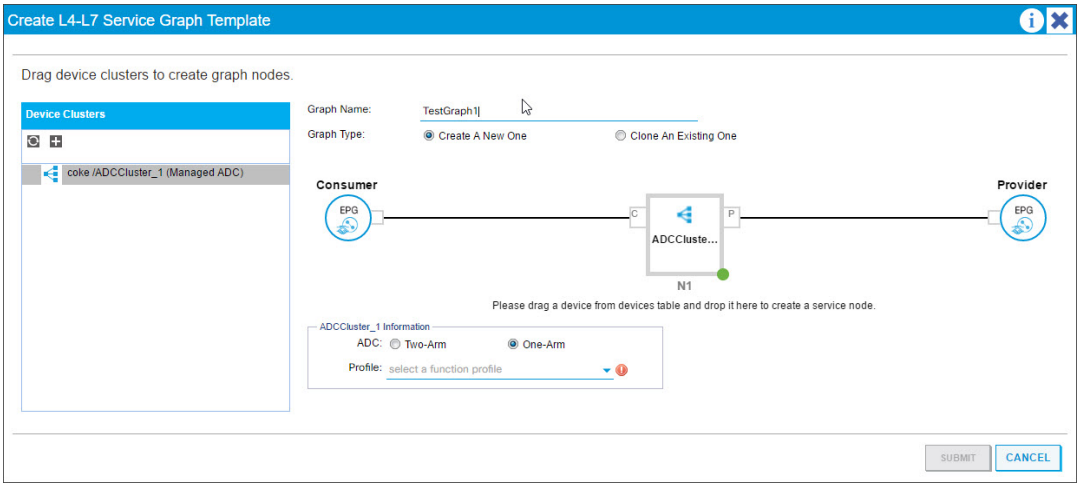
So erstellen Sie ein Service-Diagramm mithilfe der APIC-GUI:

1. Wechseln Sie in der Menüleiste zu **Mandanten > Alle Mandanten**.
2. Doppelklicken Sie im **Arbeitsbereich** auf den Namen des Mandanten.
3. Wählen Sie im **Navigationsbereich*tenant_name* > L4-L7 Services > L4-L7 Service Graph Templates aus.**
4. Wählen Sie im **ArbeitsbereichAktionen > Eine L4-L7-Service Graph-Vorlage erstellen**aus.
5. Wählen **Sie im Dialogfeld L4-L7-Service Graph-Vorlage erstellen** im Abschnitt Gerätecluster einen Gerätecluster aus und gehen Sie wie folgt vor:

    a) Geben Sie im Feld **Diagrammname** den Namen der Service-Graph-Vorlage ein.

    b) Wählen Sie im Feld **Diagrammtyp** die Option **Neues Diagramm erstellen**aus.

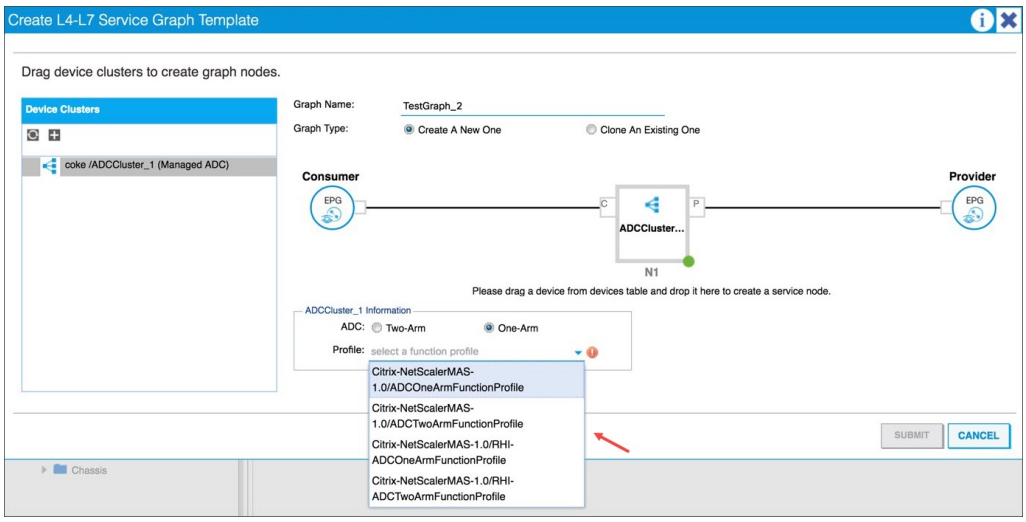
c) Ziehen Sie das **Gerät aus dem Abschnitt Gerätecluster** per Drag-and-Drop zwischen die Endpunktgruppe für Verbraucher und die Endpunktgruppe des Anbieters, um einen Dienstknoten zu erstellen.



d) Gehen Sie im Abschnitt <***l4-L7Device_Name information***> wie folgt vor:

i. Wählen Sie im Feld **ADC** je nachdem, wie der Citrix ADC in der Fabric bereitgestellt wird, **Einarmoder Zweiarm**aus.

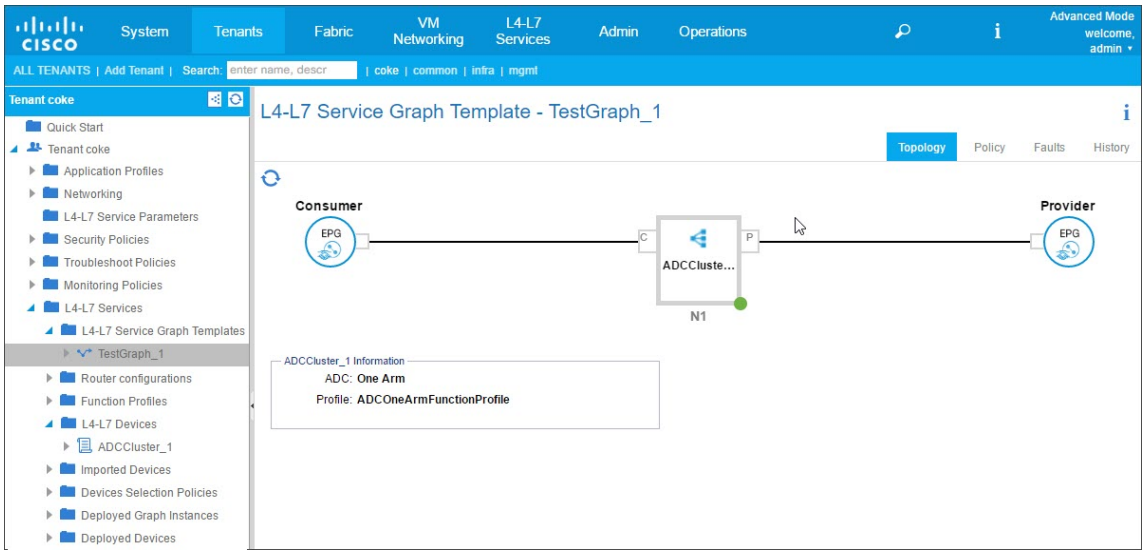
ii. Wählen Sie in der Dropdownliste **Profil** das Funktionsprofil aus, das im Gerätepaket bereitgestellt wird.



iii. Klicken Sie auf **SENDEN**.

6. Klicken Sie im **Navigationsbereich** auf die Service-Graph-Vorlage. Der Bildschirm zeigt eine grafische Topologie der Service-Graph-Vorlage.

> **Hinweis**
>
> Das Cisco APIC unterstützt das Konzept von Konnektoren, und diese Konnektoren sind im ADCCluster-Knoten sichtbar. Die Konnektoren definieren die Richtung des Netzwerkverkehrs und das Geräteskript, das das zugewiesene VLAN dynamisch an eine virtuelle IP- (VIP) oder Subnetz-IP-Adresse (SNIP) bindet, je nachdem, ob die Verbindung extern oder intern ist. VLANs sind auch an bestimmte Schnittstellen gebunden, die für eingehenden und ausgehenden Datenverkehr verwendet werden.

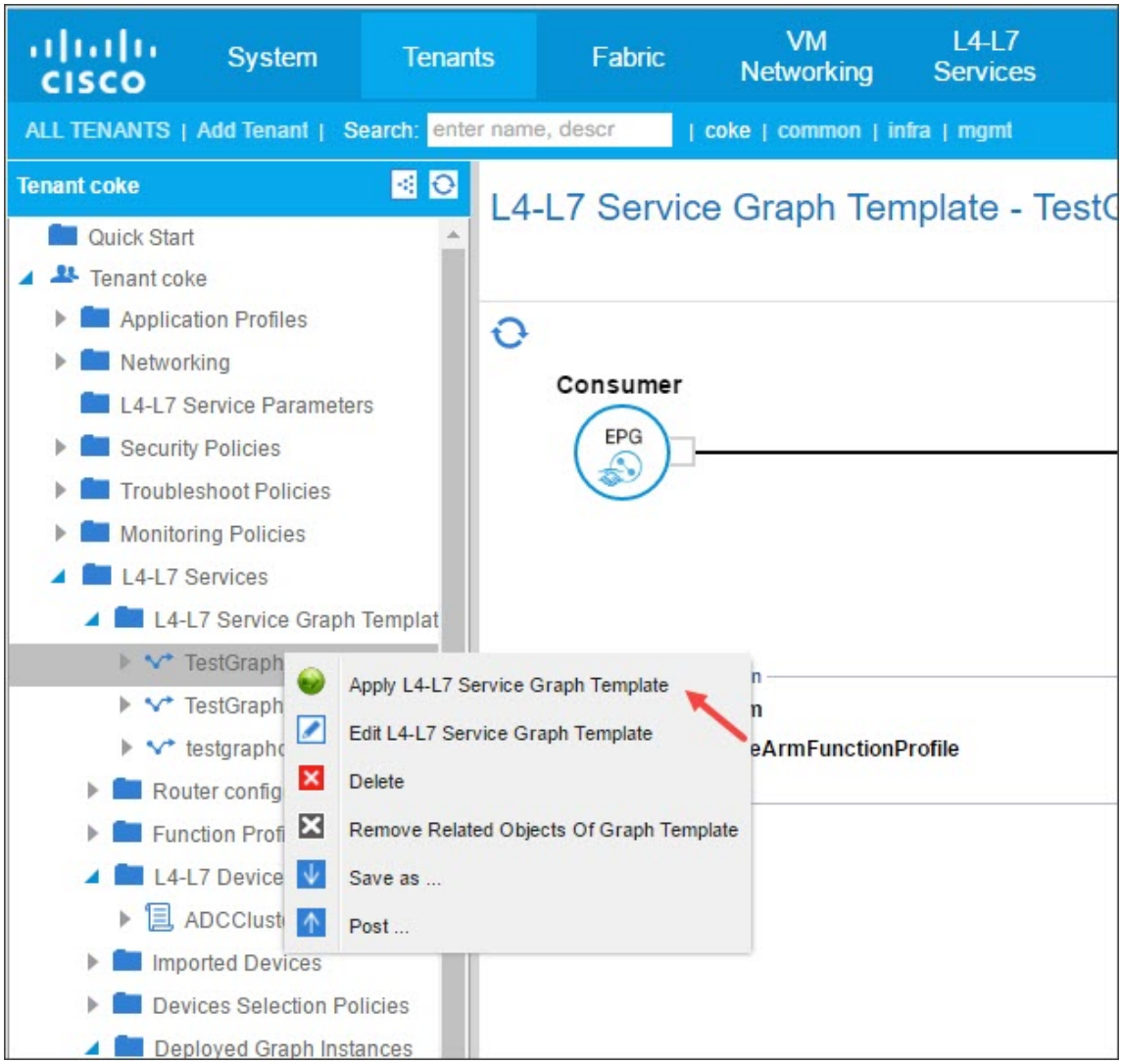


Anwendung der Service Graph-Vorlage auf Endpunktgruppen

Nachdem Sie die Service-Graph-Vorlage erstellt haben, müssen Sie die erstellte Service-Graph-Vorlage mithilfe der APIC-GUI anwenden.

So wenden Sie die Service-Graph-Vorlage an:

1. Wechseln Sie in der Menüleiste zu **Mandanten > Alle Mandanten**.
2. Doppelklicken Sie im **Arbeitsbereich** auf den Namen des Mandanten.
3. Wählen Sie im Navigationsbereich ***tenant_name* > L4-L7 Services > L4-L7 Service Graph Templates aus.**
4. Klicken Sie mit der rechten Maustaste auf den ***Vorlagennamen*** und klicken Sie auf **L4-L7 Service Graph Template anwenden**.

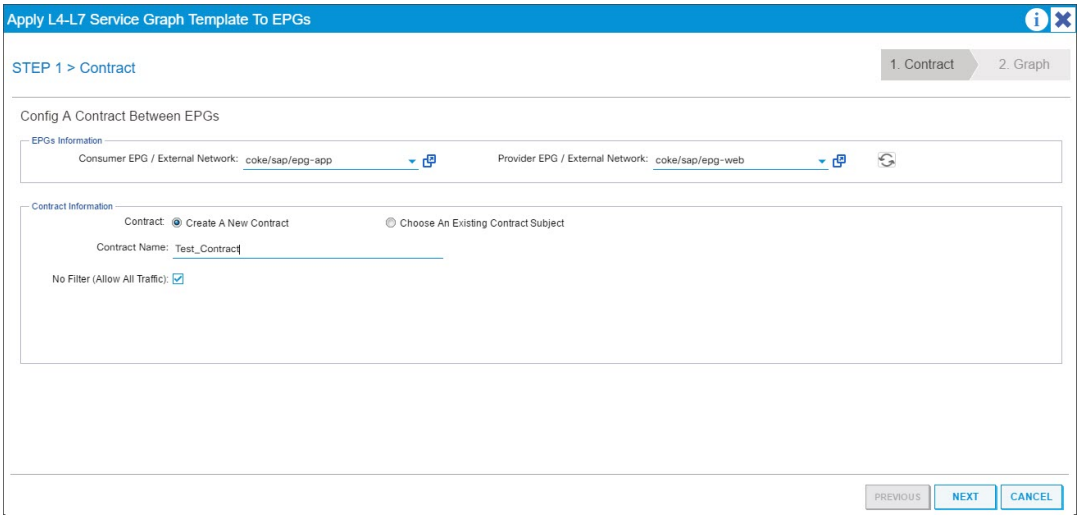


5. Füllen **Sie im Dialogfeld „L4-L7-Service Graph-Vorlage auf EPGs anwenden** “im Abschnitt „ **EPG-Informationen** “die folgenden Felder aus:

   a) Wählen Sie in der Dropdownliste **Consumer EPG/Externes Netzwerk** die Endpunktgruppe für Endgeräte aus.

   b) Wählen Sie in der Dropdownliste **Provider EPG/Externes Netzwerk** die bereitgestellte Endpunktgruppe aus.

   c) Füllen Sie im Abschnitt **Vertragsinformation** die entsprechenden Felder aus. Die Vertragsinformationen sind spezifisch für den Cisco APIC und werden als Teil der mit den EPGs verknüpften Sicherheitsrichtlinien konfiguriert.



d) Klicken Sie auf **Weiter**.

e) Wählen Sie in der Dropdownliste **Diagrammvorlage** die von Ihnen erstellte Service-Diagrammvorlage aus.

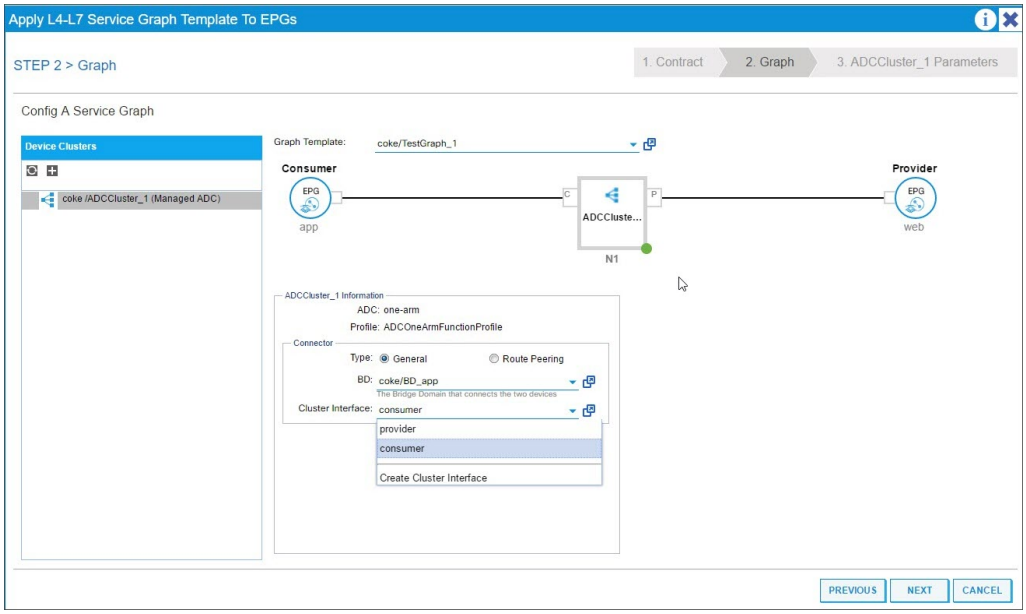
f) Gehen Sie im Abschnitt **Connector** wie folgt vor:

   i. Wählen Sie im Feld **Typ** die Option Allgemein aus.

   ii. Wählen Sie in der Dropdownliste **BD** die Bridge-Domäne aus. Connectordetails sind Teil der Bridge-Domäne, die Teil des Cisco APIC-Infrastrukturmodells ist.

   iii. Wählen Sie in der Dropdownliste **Clusterschnittstelle** die entsprechende Clusterschnittstelle für die ausgewählte Bridge-Domäne aus.

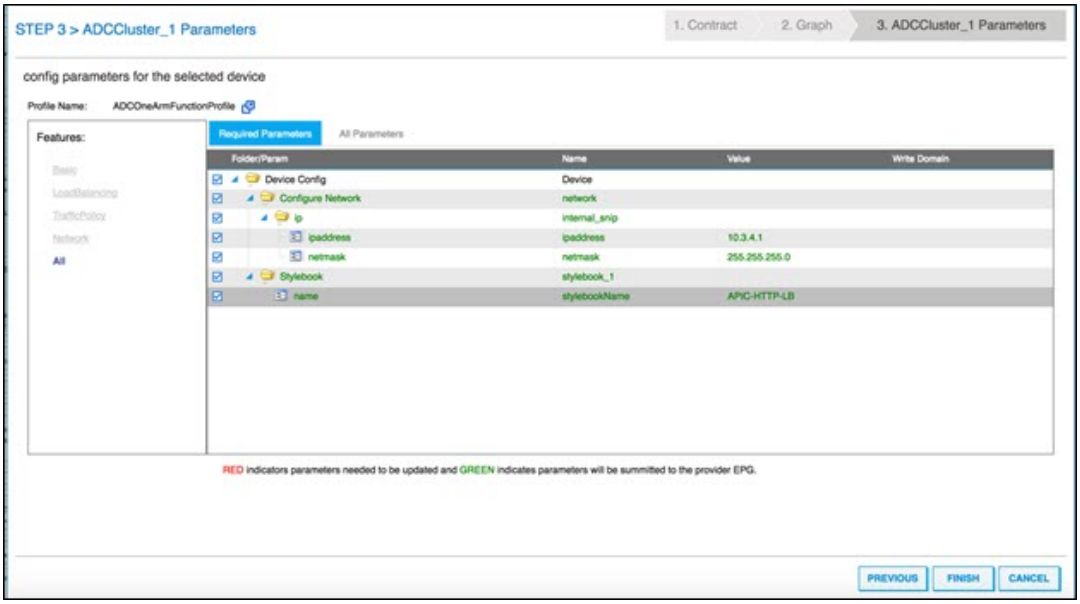
   Der Cisco APIC verwendet die ausgewählten Bridge-Domänen für Datenpfaddatenverkehr zwischen dem Citrix ADC Gerät und der Fabric, wie dies in der ausgewählten Service-Graph-Vorlage erforderlich ist.



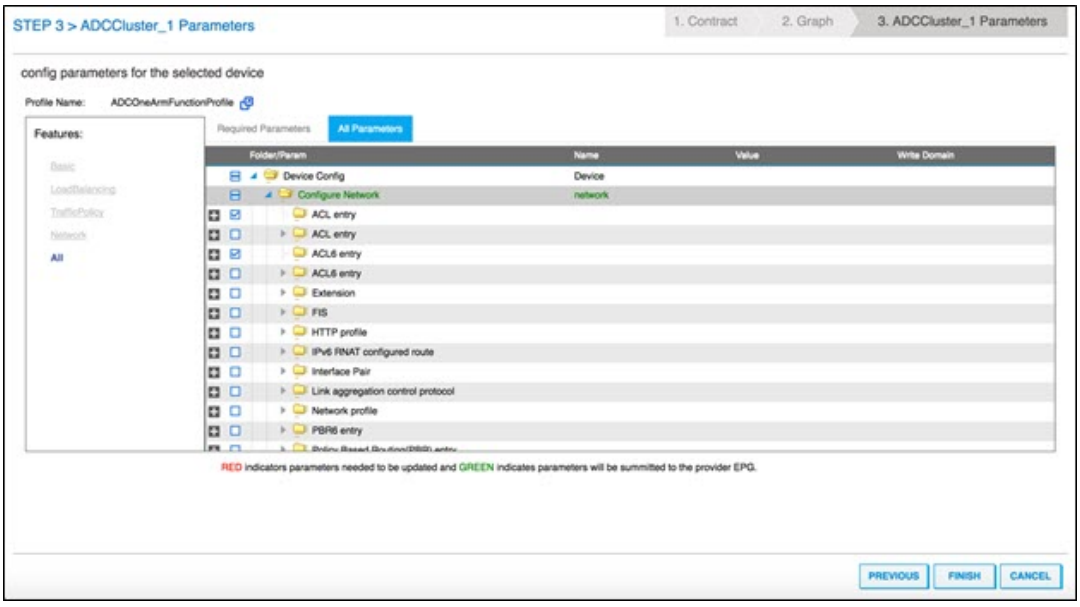
iv. Klicken Sie auf **Weiter**.

Geben Sie auf dem Bildschirm **Parameter** auf der Registerkarte **Erforderliche Parameter** die L2-L3-spezifischen Details ein, z. B. die IP-Adresse, die für das Profil vorgeschrieben ist. Der andere Schlüsselparameter ist der StyleBook-Name. Dies kann das integrierte StyleBook **APIC-HTTP-LB** sein, das in NetScaler Application Delivery Management (ADM) bereitgestellt wird, oder Sie können den Namen des StyleBook angeben, das Sie unter Erstellen eines StyleBook für die Anwendung mit NetScaler ADMerstellt haben.

> **Hinweis**
>
> Der StyleBook-Name verknüpft die Service-Graph-Details mit der L4-L7-Konfiguration, die mit Citrix ADM für eine bestimmte Anwendung erstellt wurde.



Mit der Cisco APIC-GUI können Sie die Parameter auf der Grundlage von Funktionen filtern (z. B. Load Balancing). Sie können alle obligatorischen Parameter auf der Registerkarte **Erforderliche Parameter** anzeigen und festlegen, und Sie können alle anderen Parameter, die sich auf das Feature beziehen, auf der Registerkarte **Alle Parameter** anzeigen und festlegen.



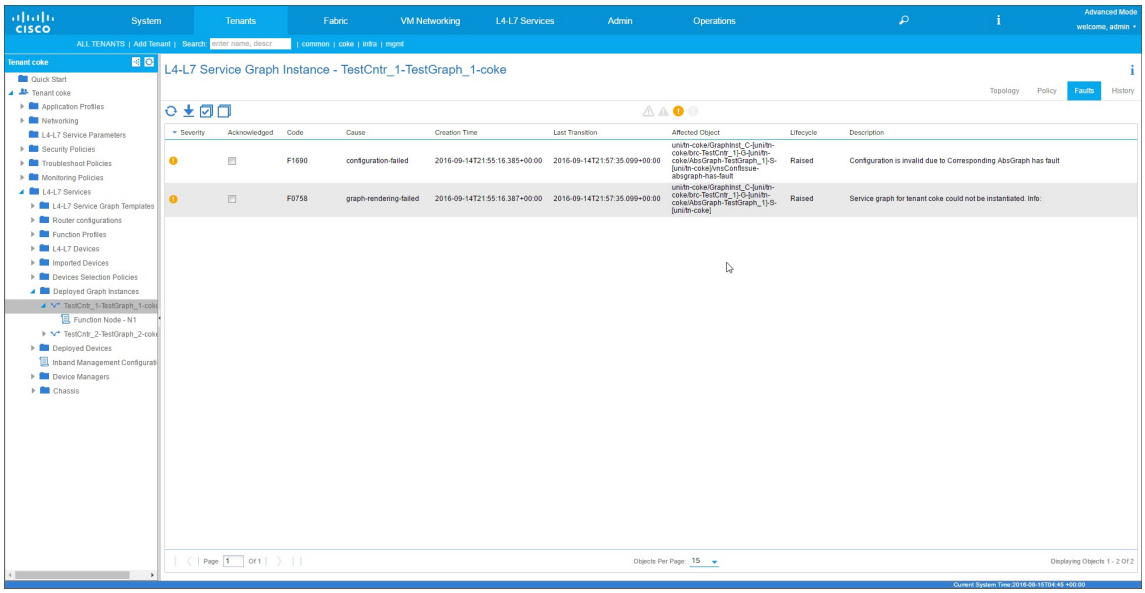
Hinweis

Standardmäßig müssen Sie für ein integriertes einarmiges Profil SNIP-Details wie IP-Adresse und Netzmaske angeben. Sie können andere Netzwerkparameter anzeigen, indem Sie auf **Alle Parameter** klicken und den **Configure Network** Tree in der Cisco

> APIC-GUI erweitern. Hiermit werden alle Netzwerkparameter aufgeführt, die von Citrix ADC unterstützt werden. Sie können jede Entität instanziieren und Werte für die aufgelisteten Attribute über die Cisco APIC-GUI bereitstellen.

6. Klicken Sie auf **Fertig stellen**.

> **Wichtig!**
>
> Nachdem Sie die Service-Graph-Vorlage angewendet haben, stellen Sie sicher, dass das bereitgestellte Diagramm keine Fehler enthält. Sie können die Fehler anzeigen, indem Sie im **Arbeitsbereich** auf die Registerkarte **Fehler** klicken.



Im Rahmen der Service Graph-Bereitstellung überträgt das Paket “Hybrid Mode Device”die Konfigurationsdetails vom Cisco APIC an das Citrix ADM. Citrix ADM verarbeitet diese Konfigurationen intern an den jeweiligen Citrix ADC und gibt die Antwort an den APIC zurück. Bei einer erfolgreichen Diagrammbereitstellung ist kein Fehler aufgetreten, und der Citrix ADC ist erfolgreich mit der Fabric für das entsprechende Diagramm vernetzt.

Das APIC unterstützt verschiedene Methoden zur Konfiguration und Bereitstellung von Graphen mithilfe von APIs. Die Graphbereitstellung umfasst verschiedene Abhängigkeiten von einigen API-spezifischen Konstrukten wie Tenant, Vertrag, VLAN und Namespace.

Der folgende Beispielansatz veranschaulicht eine der Möglichkeiten, die APIC-APIs zur Erstellung und Bereitstellung von L4-L7-Graphen zu verwenden, wobei davon ausgegangen wird, dass APIC-spezifische Artefakte bereits im APIC konfiguriert sind.

> **Wichtig!**
>
> Stellen Sie sicher, dass Sie diese XML-Payloads als Referenz verwenden, und nehmen Sie

> entsprechende Änderungen an der XML vor, bevor Sie sie in Ihrer Umgebung verwenden.

Im Folgenden finden Sie ein Beispiel für die Erstellung und Bereitstellung des Service-Graphen mithilfe von APIs:

a) AppProfile erstellen

b) Servicediagrammdetails erstellen

c) Hängen Sie das Service-Diagramm an einen Vertrag an

Im Folgenden finden Sie ein Beispiel für eine XML-Payload zum Erstellen eines AppProfile. Das AppProfile enthält EPGs und der Provider-EPG enthält die Citrix ADC spezifischen Entitäten, Attribute und deren Werte. In der folgenden XML-Nutzlast werden Citrix ADC-spezifische Netzwerkentitäten wie das NSIP mit einem Satz von Attributen und StyleBook-Namen erstellt.

```
<polUni>
    <fvTenant name="coke">
        <!-- Application Profile -->
        <fvAp dn="uni/tn-coke/ap-sap" name="sap">
            <!-- EPG 1  -->
            <fvAEPg dn="uni/tn-coke/ap-sap/epg-web" name="web">
                <fvRsBd tnFvBDName="BD_web" />
                <!-- --------- CONFIG PAYLOAD ---------- -->
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Network" name=
    "Network">
                    <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="
    snip1">
                        <vnsParamInst key="ipaddress" name="ip1"
    value="110.110.110.2"/>
                        <vnsParamInst key="netmask" name="netmask1
    " value="255.255.255.0"/>
                        <vnsParamInst key="type" name="tye" value=
    "SNIP"/>
                        <vnsParamInst key="dynamicrouting" name="
    dynamicrouting" value="DISABLED"/>
                        <vnsParamInst key="hostroute" name="
    hostroute" value="DISABLED"/>
                    </vnsFolderInst>
                    <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="
    snip2">
                        <vnsParamInst key="ipaddress" name="ip2"
    value="220.220.220.2"/>
                        <vnsParamInst key="netmask" name="netmask2
    " value="255.255.255.0"/>
                        <vnsParamInst key="type" name="tye" value=
    "SNIP"/>
                        <vnsParamInst key="dynamicrouting" name="
    dynamicrouting" value="DISABLED"/>
```



```
                        <vnsParamInst key="hostroute" name="
    hostroute" value="DISABLED"/>
                    </vnsFolderInst>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Stylebook"
    name="stylebook_1">
                    <vnsParamInst name="stylebookName" key="name"
    value="APIC-HTTP-LB"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
    internal_network" name="internal_network">
                    <vnsCfgRelInst name="internal_network_key" key
    ="internal_network_key" targetName="Network/snip1"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
    external_network" name="external_network">
                    <vnsCfgRelInst name="external_network_key" key
    ="external_network_key" targetName="Network/snip2"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="mFCngStylebook
    " name="mFCngStylebook_1">
                    <vnsCfgRelInst name="Stylebook_key" key="
    Stylebook_key" targetName="stylebook_1"/>
                </vnsFolderInst>
                <!-- ------- END CONFIG PAYLOAD -------------- -->
                <fvSubnet ip="110.110.110.110/24" scope="shared"/>
                <fvRsProv tnVzBrCPName="Ctrct1"></fvRsProv>
                <fvRsDomAtt tDn="uni/phys-sepg" />
                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
    -[eth1/38]" encap="vlan-3703" instrImedcy="immediate"/>
            </fvAEPg>
            <!-- EPG 2 -->
            <fvAEPg dn="uni/tn-coke/ap-sap/epg-app"  name="app">
                <fvRsCons tnVzBrCPName="Ctrct1"/>
                <fvRsBd tnFvBDName="BD_app" />
                <fvSubnet ip="220.220.220.220/24" scope="shared"/>
                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
    -[eth1/37]" encap="vlan-3704" instrImedcy="immediate"/>
                <fvRsDomAtt tDn="uni/phys-sepg" />
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

Im Folgenden finden Sie ein Beispiel für eine XML-Payload zum Erstellen von Service Graph-Details:

```
<polUni>
```



```
    <fvTenant name="coke">
        <vnsAbsGraph name = "Graph1">
            <vnsAbsTermNodeProv name = "Input1">
                <vnsAbsTermConn name = "C1"></vnsAbsTermConn>
            </vnsAbsTermNodeProv>
            <vnsAbsNode name="ADC" funcType="GoTo">
                <vnsAbsFuncConn name = "outside" attNotify="true">
                    <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mFunc-ADCFunction/mConn-external" />
                </vnsAbsFuncConn>
                <vnsAbsFuncConn name = "inside" attNotify="true">
                    <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mFunc-ADCFunction/mConn-internal" />
                </vnsAbsFuncConn>
                <vnsRsNodeToMFunc tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mFunc-ADCFunction"/>
                <vnsRsDefaultScopeToTerm tDn="uni/tn-coke/AbsGraph-Graph1/AbsTermNodeProv-Input1/outtmnl"/>
                <vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/absFuncProfContr/absFuncProfGrp-ADCOneArmServiceProfileGroup/absFuncProf-ADCOneArmFunctionProfile"/>
                <vnsRsNodeToLDev tDn="uni/tn-coke/lDevVip-ADCCluster1"/>
            </vnsAbsNode>
            <vnsAbsTermNodeCon name = "Output1">
                <vnsAbsTermConn name = "C6"></vnsAbsTermConn>
            </vnsAbsTermNodeCon>
            <vnsAbsConnection name = "CON1">
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-Graph1/AbsTermNodeCon-Output1/AbsTConn" />
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-Graph1/AbsNode-ADC/AbsFConn-outside" />
            </vnsAbsConnection>
            <vnsAbsConnection name = "CON2">
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-Graph1/AbsNode-ADC/AbsFConn-inside" />
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-Graph1/AbsTermNodeProv-Input1/AbsTConn" />
            </vnsAbsConnection>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

Im Folgenden finden Sie eine Beispiel-XML-Nutzlast für das Anhängen des Service-Graphen an einen Vertrag:

```
<polUni>
    <fvTenant name="coke">
        <vzBrCP name="Ctrct1">
            <vzSubj name="http">
                <vzRsSubjGraphAtt tnVnsAbsGraphName="Graph1"/>
```



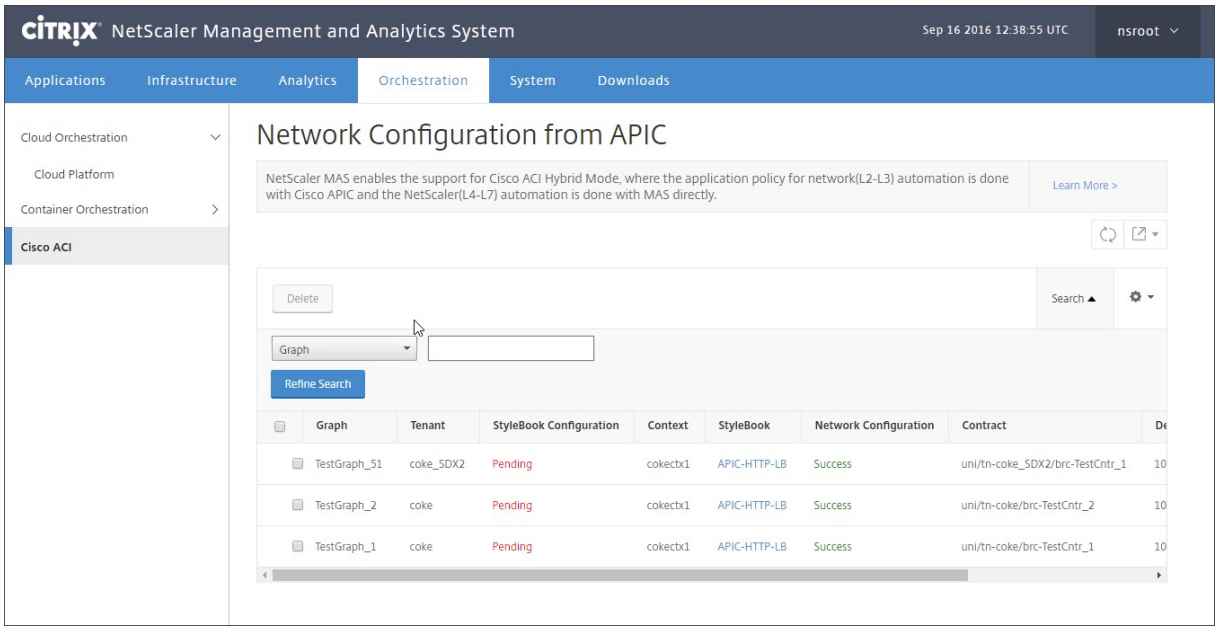
```
            </vzSubj>
        </vzBrCP>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

L4-L7-Parameter von NetScaler ADM mit StyleBook konfigurieren

February 5, 2024

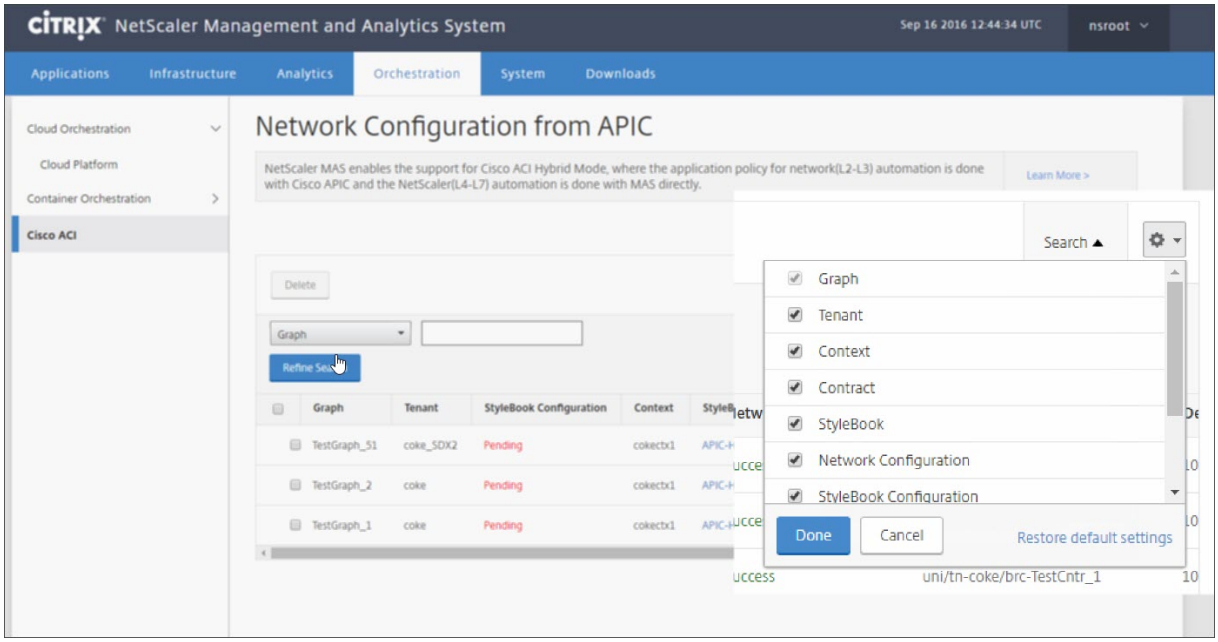
24. Mai 2018

In Citrix Application Delivery Management (ADM) können Sie die Details des bereitgestellten Dienstdiagramms auf der Registerkarte **Orchestration** unter **Cisco ACI**anzeigen. In der tabellarischen Ansicht werden die Servicediagrammdetails wie Diagrammname, Mandantenname, Kontext, StyleBook-Name und Netzwerkkonfigurationsstatus angezeigt.



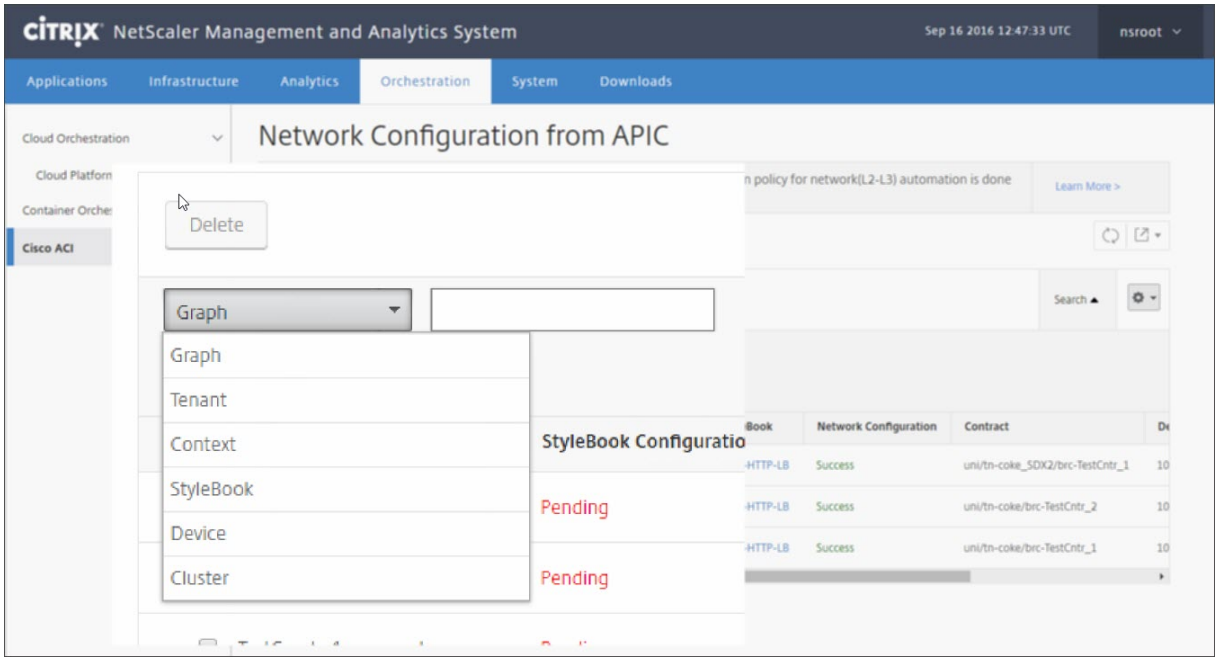
> **Hinweis**
>
> Wenn das Diagramm aus dem Cisco APIC gelöscht wird, wird die entsprechende Konfiguration vom Gerät entfernt, einschließlich der L4-L7-Konfiguration.

Darüber hinaus können Sie in der tabellarischen Ansicht nach jeder in der Tabelle angezeigten Spalte sortieren und die Daten mithilfe der Suchoption filtern. Sie können die Spaltendetails auch anpassen, indem Sie die Spaltennamen aus der Drop-down-Spaltenliste auswählen oder abwählen:



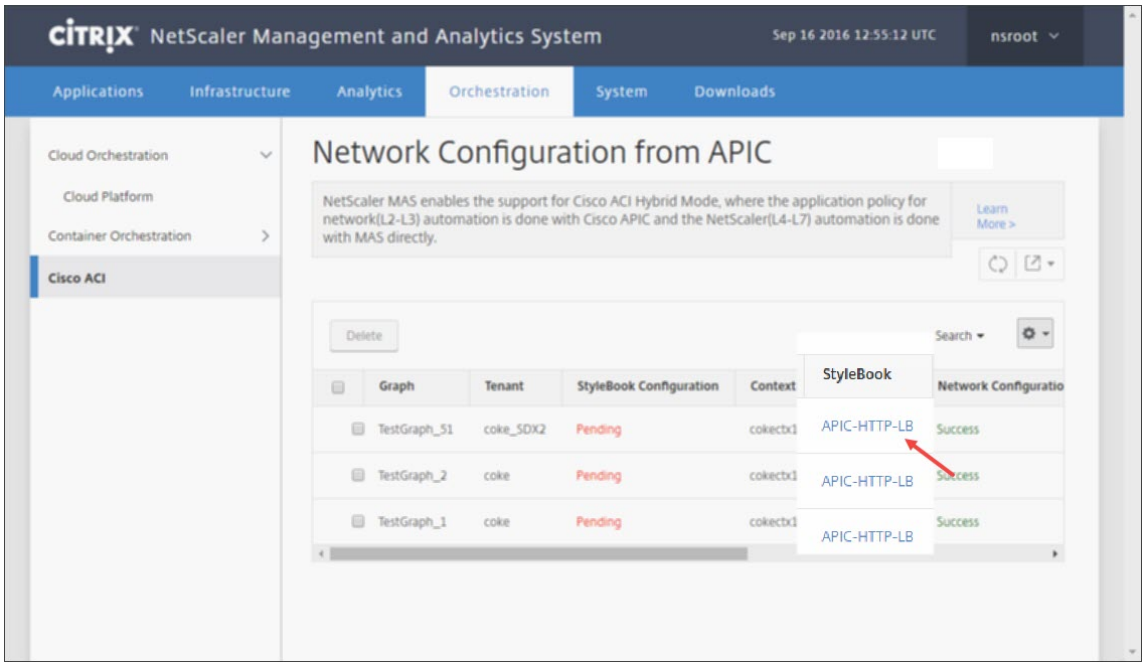
Sie können auch auf die Schaltfläche **Suchen** klicken und die Suchoptionen verwenden, um die Daten zu filtern. Sie können eine beliebige Spalte aus dem Dropdown-Feld auswählen und einen entsprechenden Wert eingeben, um die in der Tabelle angezeigten Daten zu filtern.

> **Hinweis**
>
> Bei der Suchfunktion wird zwischen Groß- und Kleinschreibung unterschieden, und Sie müssen die genauen Suchkriterien angeben.

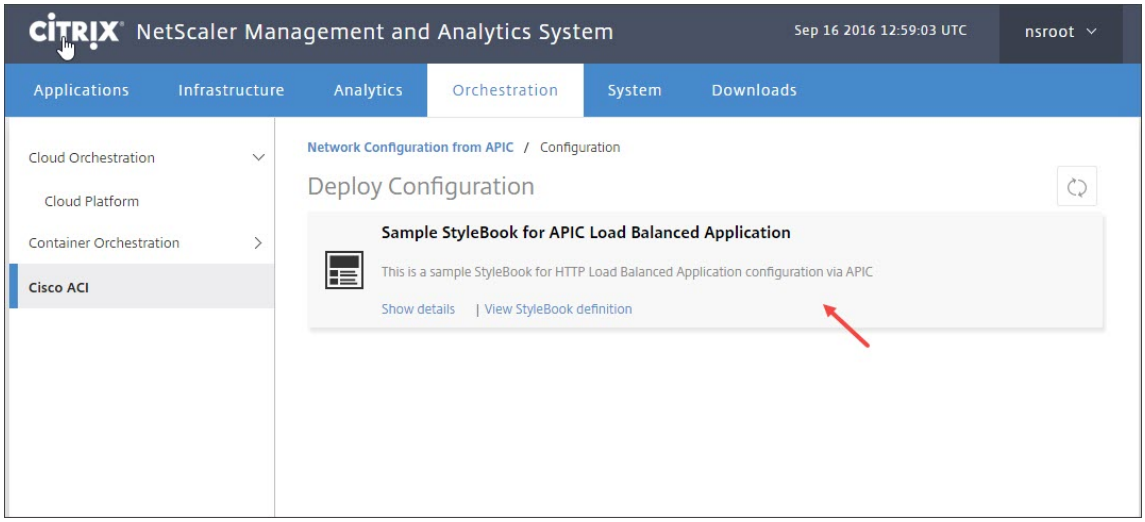


So stellen Sie die L4-L7-Konfiguration mithilfe von StyleBook in Citrix ADM bereit:

1. Klicken Sie auf den StyleBook-Namen, der in der tabellarischen Ansicht als URL angezeigt wird.



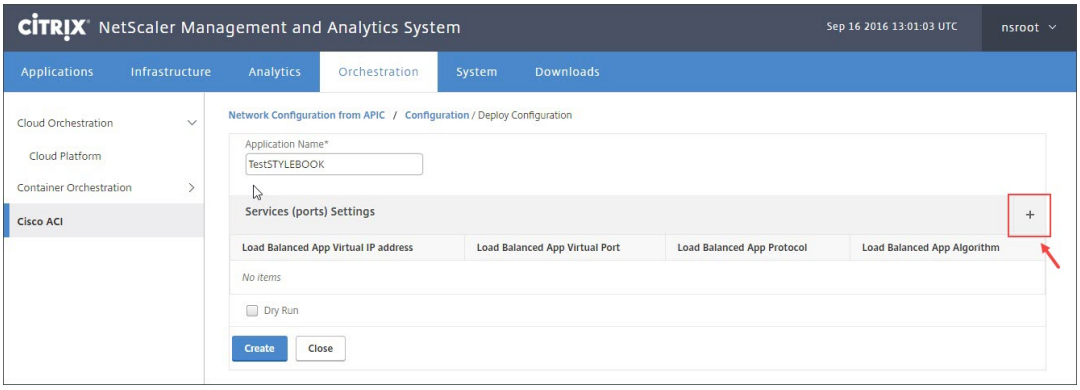
2. Doppelklicken Sie im Konfigurationsfenster auf **StyleBook**.



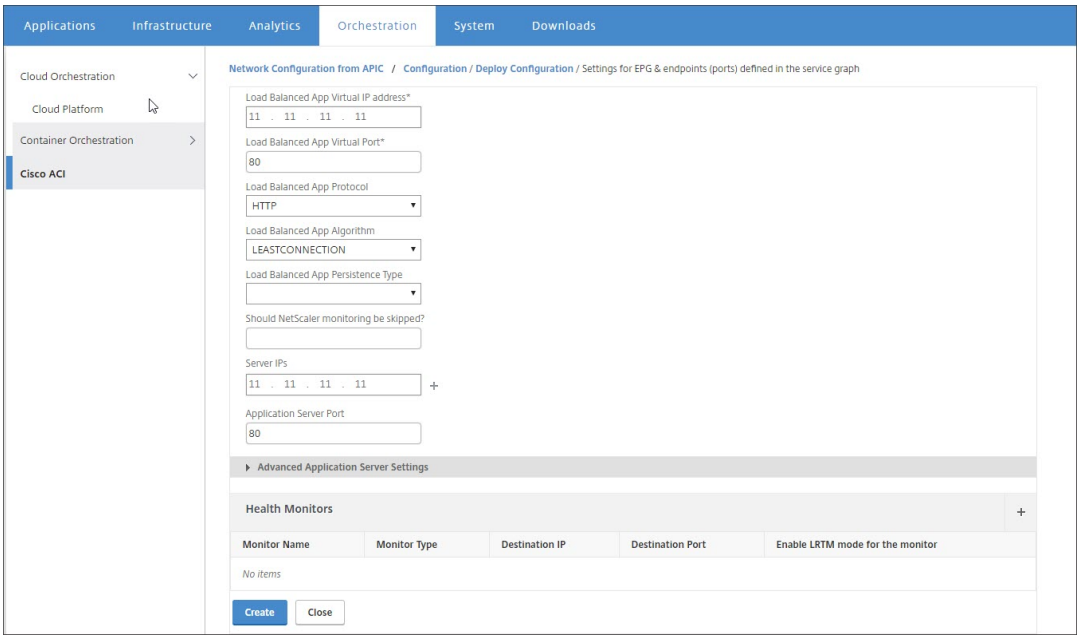
3. Gehen Sie im Fenster Konfiguration bereitstellen wie folgt vor:

   a) Geben Sie im Feld **Anwendungsname** den Namen für die ADC-Funktionskonfiguration ein, der dem Servicediagramm der Anwendung im APIC entspricht.

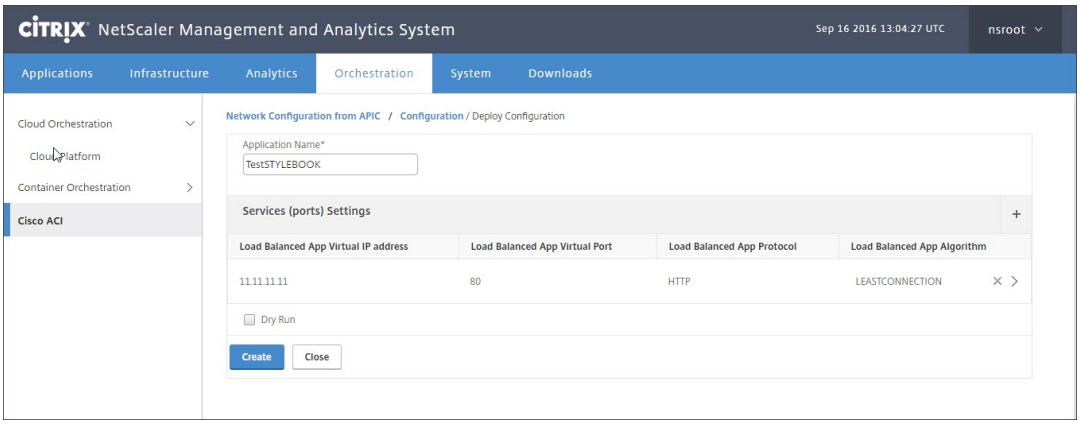
   b) Klicken Sie im Abschnitt Service (Ports) Settings auf **+**.



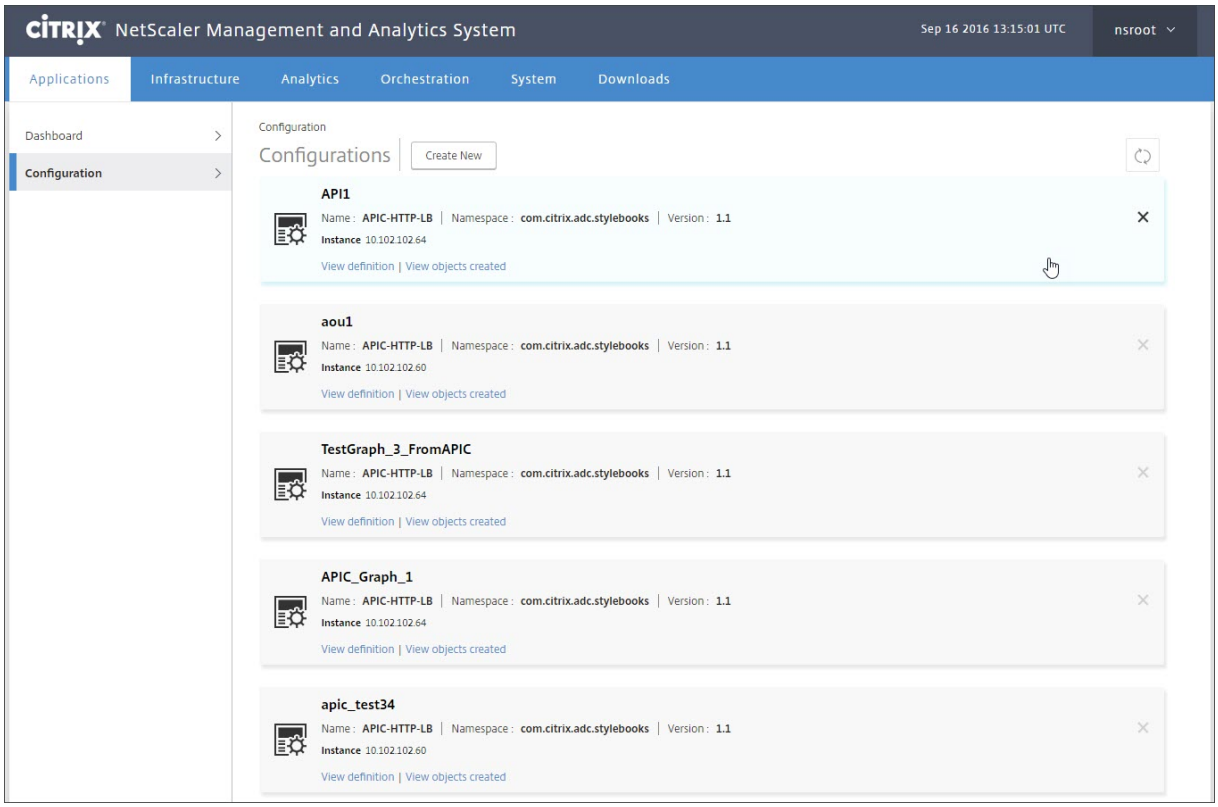
c) **Geben Sie in den**Einstellungen für EPG und Endpoints (Ports), die im Service-Graph-Fenster definiert**sind, Werte für den aus dem StyleBook aufgefüllten Parameter ein und klicken Sie auf Erstellen.**



d) Klicken Sie auf **Erstellen**.



Die im StyleBook angegebene L4-L7-Konfiguration wird in Citrix ADM bereitgestellt. Sie können die StyleBook-Konfiguration auf der Registerkarte **Anwendung** anzeigen, indem Sie zu **Anwendung**> Konfiguration navigieren.



Endpunktereignisse von APIC anhängen und trennen

February 5, 2024

Die Hybrid-Modus-Lösung verarbeitet implizit Attach- oder Detach-Endpunktereignisse vom Cisco APIC. Wenn der Cisco APIC ein Attach-Endpunktereignis auslöst, wird die servicegroup_servicegroupmember_bind automatisch vom StyleBook in Citrix Application Delivery Management (ADM) ausgelöst, und der Endpunkt wird während des Endpunktereignisses “Detach”ungebunden.

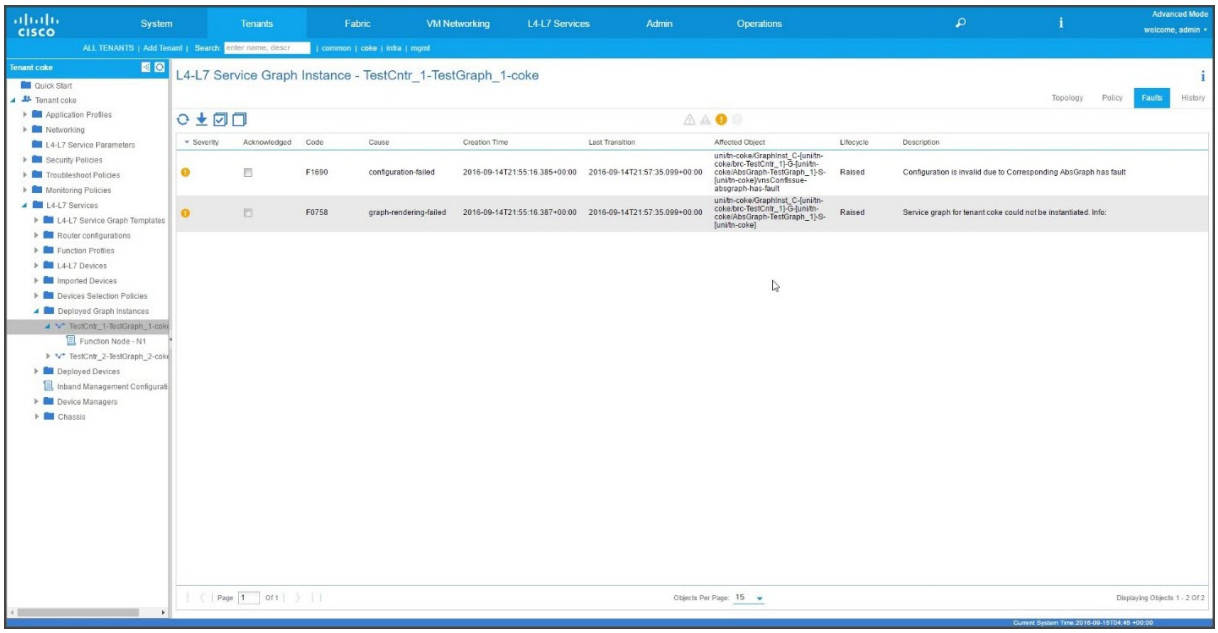
Wenn Sie die L4-L7-Konfiguration nicht in Citrix ADM bereitgestellt haben, bevor das Attach-oder Detach-Endpunktereignis in Cisco APIC ausgelöst wird, behält die Lösung außerdem die Attach-IP-Adressen in der Datenbank bei. Diese IP-Adressen werden an die entsprechende Dienstgruppe gebunden, nachdem die Dienstgruppe über StyleBook erstellt wurde.

APIC-Fehlerberichte

February 5, 2024

Wenn Sie ein Citrix ADC Gerätepaket in Cisco ACI bereitstellen, meldet der Cisco APIC alle Fehler. Sie können die Fehlerberichte auf jeder Ebene des APIC einsehen (z. B. Gerät, Mandant, EPGs oder Servicediagramm). Der folgende Screenshot zeigt einen Fehlerbericht auf Geräteebene. Weitere Informationen zu Fehlern finden Sie unter http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/faults/guide/b_APIC_Faults_Errors/b_IFC_Faults_Errors_chapter_01.html.

Wählen Sie eine APIC-Entität aus und klicken Sie auf die Registerkarte **Fehler**, um die vom APIC für diese Entität gemeldeten Fehler anzuzeigen.



Von NetScaler ADM generierte Protokolle

February 5, 2024

Citrix Application Delivery Management (ADM) bietet umfangreiche Protokollierung, mit der Probleme behoben werden können. Die generierten Protokolle (**admin.log**) befinden sich unter: **/var/-controlcenter/log/**

Sie können sich bei Citrix ADM anmelden und die Shell verwenden, um zur Citrix ADM-Verzeichnisstruktur zu navigieren. Im Folgenden finden Sie ein Beispielausschnitt eines NetScaler ADM Protokolls für die Diagrammbereitstellung eines APIC.


```
    2016-06-29 10:58:33,816 DEBUG APIC Config  = {
(0, '', 5230): {
'dn': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'tenant': 'coke_SDX2', 'ctxName': 'cokectx1', 'value': {
(10, '', 'ADCHybridMode_1_Consumer_1'): {
'state': 1, 'transaction': 0, 'cifs': {
'ADCHybridMode_1_Device_1': '1_1' }
, 'ackedstate': 0 }
, (7, '', '2129920_32778'): {
'state': 1, 'tag': 273, 'type': 1, 'ackedstate': 0, 'transaction': 0 }
, (1, '', 5790): {
'transaction': 0, 'ackedstate': 0, 'value': {
(3, 'ADCFunction', 'N1'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(4, 'mFCngNetwork', 'mFCngnetwork'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'Network_key', 'network_key'): {
'state': 1, 'transaction': 0, 'target': 'network', 'ackedstate': 0 }
 }
 }
, (4, 'internal_network', 'internal_network'): {
'connector': 'provider', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'internal_network_key', 'internal_network_key'): {
'state': 1, 'transaction': 0, 'target': 'network/internal_snip', 'ackedstate': 0 }
 }
 }
, (2, 'external', 'consumer'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'target': 'ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
 }
 }
, (4, 'mFCngStylebook', 'mFCngStylebook'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'Stylebook_key', 'Stylebook_key'): {
'state': 1, 'transaction': 0, 'target': 'stylebook_1', 'ackedstate': 0
    }
 }
 }
, (2, 'internal', 'provider'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'target': 'ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
 }
 }
 }
 }
```



```
 }
, 'state': 1, 'absGraph': 'HybridModeGraph_1', 'rn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
, (4, 'Network', 'network'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(4, 'nsip', 'internal_snip'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(5, 'type', 'type'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'SNIP' }
, (5, 'hostroute', 'hostroute'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'DISABLED' }
, (5, 'ipaddress', 'ipaddress'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '10.1.1.1' }
, (5, 'dynamicrouting', 'dynamicRouting'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'ENABLED' }
, (5, 'netmask', 'netmask'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '255.255.255.0' }
 }
 }
 }
 }
, (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'vif': 'ADCHybridMode_1_Consumer_1', 'ackedstate': 0, 'encap': '2129920_32778' }
, (4, 'Stylebook', 'stylebook_1'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(5, 'name', 'stylebookName'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB' }
 }
 }
 }
, 'txid': 10000 }
 }

   2016-06-29 10:58:33,816 DEBUG get Graph Return details = {
'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
, 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', 'graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', 'graphInstanceId': 5790 }

   2016-06-29 10:58:33,827 DEBUG SUCCESS created track 2.0
   2016-06-29 10:58:33,833 DEBUG SUCCESS updated track with new task 2
   2016-06-29 10:58:33,851 DEBUG SUCCESS updated track with new task 1
   2016-06-29 10:58:33,867 DEBUG fn_wrapper:long_operation_thread_id:<eventlet.greenthread.GreenThread object at 0x80aa5c7d0>
   2016-06-29 10:58:33,867 DEBUG +++++++ Service Audit Call for Device
```



```
            Details  = 10.102.102.62 +++++++++++++++++
88      2016-06-29 10:58:33,867 DEBUG Inside APIC Cred Col If = 2
89      2016-06-29 10:58:33,867 DEBUG Host name from device =
           ADCHybridMode_1
90      "InProgress","message":null,"replication_status":"","target":"
           10.102.102.81","operation":"POST","entity_type":"apic","
           entity_id":null }
91    }
92
93      2016-06-29 10:58:44,141 DEBUG  Save config  Response = {
94    "errorcode": 0, "message": "Done", "severity": "NONE"  }
95
96      2016-06-29 10:58:44,141 DEBUG +++++++++ getContextAwareFlag = True
97      2016-06-29 10:58:44,141 DEBUG +++++ get context tenant name from
           Config ++++++
98      2016-06-29 10:58:44,141 DEBUG +++++ getContextTenantName = {
99    'state': 1, 'ctxName': 'cokectx1', 'tenant': 'coke_SDX2', 'vdev': 5230
         }
100   ++++++
101     2016-06-29 10:58:44,142 DEBUG Service health details = {
102   }
103   collection length = 0
104     2016-06-29 10:58:44,142 DEBUG Count details Total = 0 Up = 0 Down =
           0
105     2016-06-29 10:58:44,142 DEBUG Health Score details Up = 0
106     2016-06-29 10:58:44,142 DEBUG Service HEALTH final collection  = {
107   ((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')): {
108   'faults': [], 'state': 0, 'health': ([(0, '', 5230), (1, '', 5790),
         (3, 'ADCFunction', 'N1')], 0) }
109   }
110
111     2016-06-29 10:58:44,142 DEBUG ++++++getServiceHealth Fault List =
           []
112     2016-06-29 10:58:44,142 DEBUG Service HEALTH final response  = {
113   'devs': 'ADCHybridMode_1_Device_1', 'faults': [], 'state': 0, 'health'
         : [([(0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')], 0)] }
114
115     2016-06-29 10:58:44,236 DEBUG RESPONSE from NSLOGOUT = {
116   "errorcode": 0, "message": "Done", "severity": "NONE"  }
117   , sessionId = ##
         D2EAFA7CFCD73119E6C5E78D8BCB2E842829C971C1DC7E99850949DAE0029F2191B5E7EDF2764

118     2016-06-29 10:58:44,237 DEBUG +++++ Faults respCol   = {
119   '10.102.102.62': {
120   '10.102.102.62': {
121   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
         u'NONE', 'operation_name': 'add_op' }
122   }
123   , (7, '', '2129920_32778'): {
124   'vlan': {
125   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
         u'NONE', 'operation_name': 'add_op' }
126   }
```



```
127   , (((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1'), (2, '
          internal', 'provider')), 'nsip'): {
128   'vlan_nsip_binding': {
129   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
          u'NONE', 'operation_name': 'bind_op' }
130    }
131   , (((0, '', 5230), (4, 'Network', 'network')), (4, 'nsip', '
          internal_snip')): {
132   'nsip': {
133   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
          u'NONE', 'operation_name': 'add_op' }
134    }
135   , (): {
136    }
137   , (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
138   'vlan_interface_binding': {
139   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
          u'NONE', 'operation_name': 'bind_op' }
140    }
141    }
142
143      2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
             = Done, statusCode = add_op
144      2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
             = Done, statusCode = add_op
145      2016-06-29 10:58:44,237 DEBUG Fault details oprName = bind_op,
          erMsg = Done, statusCode = bind_op
146      2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
             = Done, statusCode = add_op
147      2016-06-29 10:58:44,238 DEBUG Fault details oprName = bind_op,
          erMsg = Done, statusCode = bind_op
148      2016-06-29 10:58:44,238 DEBUG +++++++++++++++ ServiceAudit response
          = {
149   'faults': [], 'state': 0, 'health': [] }
150
151      2016-06-29 10:58:44,238 DEBUG APIC Graph Details = {
152   'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[
          uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
153   'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-
          coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-
          HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
154   , 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', '
          graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', '
          graphInstanceId': 5790 }
155
156      2016-06-29 10:58:44,242 DEBUG Journal Processing: Database task:
          create apic_graph
157      2016-06-29 10:58:44,264 DEBUG SUCCESS created task 2
158      2016-06-29 10:58:44,269 DEBUG SUCCESS updated track with new task 2
159      2016-06-29 10:58:44,308 DEBUG +++++++ get IP and Connector
          collection from Config with type 22 for attach & detach event
          ++++++
160      2016-06-29 10:58:44,308 DEBUG ----- connector with IP List = {
```



```
  0: [], 1: [], 3: [] }

     2016-06-29 10:58:44,308 DEBUG ----- attachIpList = [] dettachIpList
         = []
     2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps
        attachIpList = [] dettachIpList = []
     2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row = {
  'deviceIP': u'10.102.102.62', 'responseToAPIC': None, 'graphDN': u'uni
     /vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-
     coke_SDX2]-ctx-cokectx1', 'apicGraphState': None, 'serviceGroupName
     ': None, 'configPackId': None, 'tenantName': u'coke_SDX2', '
     styleBookName': u'APIC-HTTP-LB', 'graphInstanceName': u'
     HybridModeGraph_1', 'context': u'cokectx1', 'serviceGroupPort':
     None, 'graphInstanceId': 5790, 'createDate': None, 'serviceGroupIP'
     : None }

<!--NeedCopy-->
```

Protokolle, die vom Hybrid-Modus-Gerätepaket generiert werden

February 5, 2024

Das Citrix ADC Hybridmodusgerätpaket generiert konfigurationsbezogene Protokolle und überwachungsbezogene Protokolle. Die generierten Protokolle befinden sich unter **/data/devicescript/ Citrix.NetScalerMAS.1.0/logs**.

Im Folgenden finden Sie einen Beispielausschnitt der Datei debug.log eines Cisco APIC:

```
1     2016-06-28 03:06:53.879767 DEBUG Thread-20 18723 [10.102.102.62,
         24063] Device manager details ip = 10.102.102.81, port = 80
2     2016-06-28 03:06:53.879856 DEBUG Thread-20 18724 [10.102.102.62,
         24063] +++++++++++++++ serviceAudit  request ++++++++++++++++++
3     2016-06-28 03:06:53.879929 DEBUG Thread-20 18725 [10.102.102.62,
         24063] ++++++++++ getStyleBookObjects ++++++++++++
4     2016-06-28 03:06:53.879995 DEBUG Thread-20 18726 [10.102.102.62,
         24063] NMAS collection A3 = (4, 'Stylebook', 'stylebook_1') B3 =
          {
5  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
6  (5, 'name', 'stylebookName'): {
7  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
       }
8   }
9   }
10
11    2016-06-28 03:06:53.880045 DEBUG Thread-20 18727 [10.102.102.62,
         24063] NMAS collection styleBookName= APIC-HTTP-LB
12    2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62,
         24063] NMAS collection retCol= {
```



```
13  'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, '', 5230), (4, 'Stylebook',
        'stylebook_1')) }
14
15     2016-06-28 03:06:53.880140 DEBUG Thread-20 18729 [10.102.102.62,
          24063]  ++++ devMgrStyleBookUrl = http://10.102.102.81/stylebook
          /nitro/v1/config/stylebooks/com.citrix.adc.stylebooks/1.1/APIC-
          HTTP-LB
16     2016-06-28 03:06:54.135240 DEBUG Thread-20 18730 [10.102.102.62,
          24063]  ++++ Response from styleBookresCode serviceAudit = {
17  u'stylebook': {
18  u'uses_builtin_namespaces': {
19  u'netscaler.nitro.config': u'10.5' }
20  , u'name': u'APIC-HTTP-LB', u'used_by_stylebooks': [], u'namespace': u
       'com.citrix.adc.stylebooks', u'source': u'---\nname: APIC-HTTP-LB\
       nnamespace: com.citrix.adc.stylebooks\nversion: "1.1"\ndisplay-name
       : "Sample StyleBook for APIC Load Balanced Application"\
       ndescription: "This is a sample StyleBook for HTTP Load Balanced
       Application configuration via APIC"\nschema-version: "1.0"\nimport-
       stylebooks: \n  - \n    namespace: netscaler.nitro.config\n
       prefix: ns\n    version: "10.5"\n  - \n    namespace: "com.citrix.
       adc.stylebooks"\n    prefix: "stlb"\n    version: "1.1"\nparameters
       -default-sources:\n  - stlb::APIC-ROOT\nsubstitutions:\n  lb-name(
       appname, port): $appname + "-" + str($port) + "-lb"\n  sg-name(
       appname, port): $appname + "-" + str($port) + "-sg"\n
       healthmonitor[]:\n    true: "NO"\n    false: "YES"\ncomponents: \n
        - \n    name: lbvserver\n    type: ns::lbvserver\n    repeat:
       $parameters.app-services\n    repeat-item: app\n    properties: \
       n      name: $substitutions.lb-name($parameters.appname, $app.
       virtual-port)\n      ipv46: $app.virtual-ip\n      port: $app.
       virtual-port\n      servicetype: $app.protocol\n      lbmethod?:
       $app.algorithm\n      persistencetype?: $app.persistence\n  - \n
        name: svcgrp\n    type: ns::servicegroup\n    repeat: $parameters.
       app-services\n    repeat-item: app\n    properties: \n      name:
       $substitutions.sg-name($parameters.appname, $app.virtual-port)\
       n      servicetype: $app.protocol\n      useproxyport?: $app.sg-
       advanced.useproxyport\n      usip?: $app.sg-advanced.usip\n
       cip?: $app.sg-advanced.cip\n      cipheader?: $app.sg-advanced.
       cipheader\n      healthmonitor?: $substitutions.healthmonitor($app.
       skip_healthmonitor)\n    components: \n      -\n        name:
       lbvserver-svg-binding\n        type: ns::
       lbvserver_servicegroup_binding\n        properties: \n
       name: $substitutions.lb-name($parameters.appname, $app.virtual-port
       )\n          servicegroupname: $parent.properties.name\n      - \
       n        name: svg-members\n        type: ns::
       servicegroup_servicegroupmember_binding\n        condition: $app.
       server-ips\n        repeat: $app.server-ips\n        repeat-item:
       serverip\n        properties: \n          ip: $serverip\n
       port: $app.server-port\n          servicegroupname: $parent.
       properties.name\noutputs: \n  - \n    name: lbvservers\n    value:
       $components.lbvserver\n  - \n    name: servicegroups\n    value:
       $components.svcgrp', u'version': u'1.1', u'uses_stylebooks': [{
21  u'version': u'1.1', u'namespace': u'com.citrix.adc.stylebooks', u'name
       ': u'APIC-ROOT' }
```



```
22  ] }
23   }
24
25     2016-06-28 03:06:54.359142 DEBUG Thread-20 18731 [10.102.102.62,
          24063]  ++++ Dev Mgr request details devMgrUrl = http://
          10.102.102.81/admin/v1/apic
26     2016-06-28 03:06:54.359221 DEBUG Thread-20 18732 [10.102.102.62,
          24063]  ++++ Response from Device Mgr serviceAudit = {
27  "APIC":[] }
28
29     2016-06-28 03:06:54.359266 DEBUG Thread-20 18733 [10.102.102.62,
          24063] ++++++++++++++ serviceAudit response = {
30  "APIC":[] }
31
32     2016-06-28 03:06:54.359306 DEBUG Thread-20 18734 [10.102.102.62,
          24063] ++++++++++++++ serviceAudit response headers content type
          = application/json; charset=utf-8
33     2016-06-28 03:06:54.359394 DEBUG Thread-20 18735 [10.102.102.62,
          24063] ++++++++++++++ serviceAudit response headers = {
34  'content-length': '11', 'job_id': 'ctxt-f4db2883-e42c-4262-a35f-04628
       c4ad5ea', 'x-content-type-options': 'nosniff', 'transfer-encoding':
        'chunked', 'connection': 'close', 'date': 'Wed, 29 Jun 2016
       10:58:33 GMT', 'x-frame-options': 'SAMEORIGIN', 'content-type': '
       application/json; charset=utf-8' }
35
36     2016-06-28 03:06:54.359480 DEBUG Thread-20 18736 [10.102.102.62,
          24063] ++++++++++++++ pollingURL = http://10.102.102.81/admin/v1
          /journalcontexts/ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea
37     2016-06-28 03:06:54.359713 DEBUG Thread-20 18737 [10.102.102.62,
          24063] ++++++++++++++ pollingStatus = True, pollingTime = 0
38     2016-06-28 03:06:54.483228 DEBUG Thread-20 18738 [10.102.102.62,
          24063] ++++++++++++++ pollingResponse json = {
39  u'journalcontext': {
40  u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
        u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
       service_name': u'admin', u'start_time': u'2016-06-29T10
       :58:33.760565', u'is_default': u'false', u'end_time': None, u'
       target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
       -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
41   }
42
43     2016-06-28 03:07:04.493074 DEBUG Thread-20 18739 [10.102.102.62,
          24063] ++++++++++++++ pollingStatus = True, pollingTime = 1
44     2016-06-28 03:07:04.587595 DEBUG Thread-20 18767 [10.102.102.62,
          24063] ++++++++++++++ pollingResponse json = {
45  u'journalcontext': {
46  u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
        u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
       service_name': u'admin', u'start_time': u'2016-06-29T10
       :58:33.760565', u'is_default': u'false', u'end_time': None, u'
       target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
       -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
47   }
```



```
48
49      2016-06-28 03:07:14.597812 DEBUG Thread-20 18790 [10.102.102.62,
           24063] +++++++++++++++ pollingStatus = True, pollingTime = 2
50      2016-06-28 03:07:14.692590 DEBUG Thread-20 18791 [10.102.102.62,
           24063] +++++++++++++++ pollingResponse json = {
51   u'journalcontext': {
52   u'status': u'Finished', u'scopes': [], u'entity_id': None, u'name': u'
        Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
        service_name': u'admin', u'start_time': u'2016-06-29T10
        :58:33.760565', u'is_default': u'false', u'end_time': u'2016-06-29
        T10:58:44.486919', u'target': u'10.102.102.81', u'message': u'Done'
        , u'id': u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', u'
        replication_status': u'' }
53    }
54
55      2016-06-28 03:07:14.692932 DEBUG Thread-20 18793 [10.102.102.62,
           24063] Attempts 1
56      2016-06-28 03:07:14.693031 DEBUG Thread-20 18794 [10.102.102.62,
           24063] Cluster (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1', (0,
            '', 5230)), transaction: 0
57      2016-06-28 03:07:14.693147 DEBUG Thread-20 18795 [10.102.102.62,
           24063] Attempts for {
58   'name': 'ADCHybridMode_1', 'host': '10.102.102.62', 'virtual': False,
        'devs': {
59   'ADCHybridMode_1_Device_1': {
60   'state': 0, 'virtual': False, 'manager': {
61   'hosts': {
62   '10.102.102.81': {
63   'port': 80 }
64    }
65   , 'name': 'NMAS_1', 'creds': {
66   'username': 'nsroot', 'password': '<hidden>' }
67    }
68   , 'version': '11.0', 'host': '10.102.102.62', 'port': 80, 'creds': {
69   'username': 'nsroot', 'password': '<hidden>' }
70    }
71    }
72   , 'manager': {
73   'hosts': {
74   '10.102.102.81': {
75   'port': 80 }
76    }
77   , 'name': 'NMAS_1', 'creds': {
78   'username': 'nsroot', 'password': '<hidden>' }
79    }
80   , 'contextaware': True, 'port': 80, 'creds': {
81   'username': 'nsroot', 'password': '<hidden>' }
82    }
83    is 0
84      2016-06-28 03:07:14.693339 DEBUG Thread-20 18796 [10.102.102.62,
           24063] Deleting (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1',
           (0, '', 5230))
85      2016-06-28 03:07:14.693379 DEBUG Thread-20 18797 [10.102.102.62,
```



```
           24063] pending: False, delete: False, txId: None
86      2016-06-28 03:07:14.693517 DEBUG Thread-20 18798 [10.102.102.62,
           24063] Faults: []
87      2016-06-28 03:07:14.693558 DEBUG Thread-20 18799 [10.102.102.62,
           24063] Health: []
88      2016-06-28 03:07:14.693914 DEBUG Thread-20 18800 [10.102.102.62,
           24063] Send num: 761, type: 220, len: 382
89  <!--NeedCopy-->
```

NetScaler ADC Gerätepaket im Cloud Orchestrator-Modus von Cisco ACI

February 5, 2024

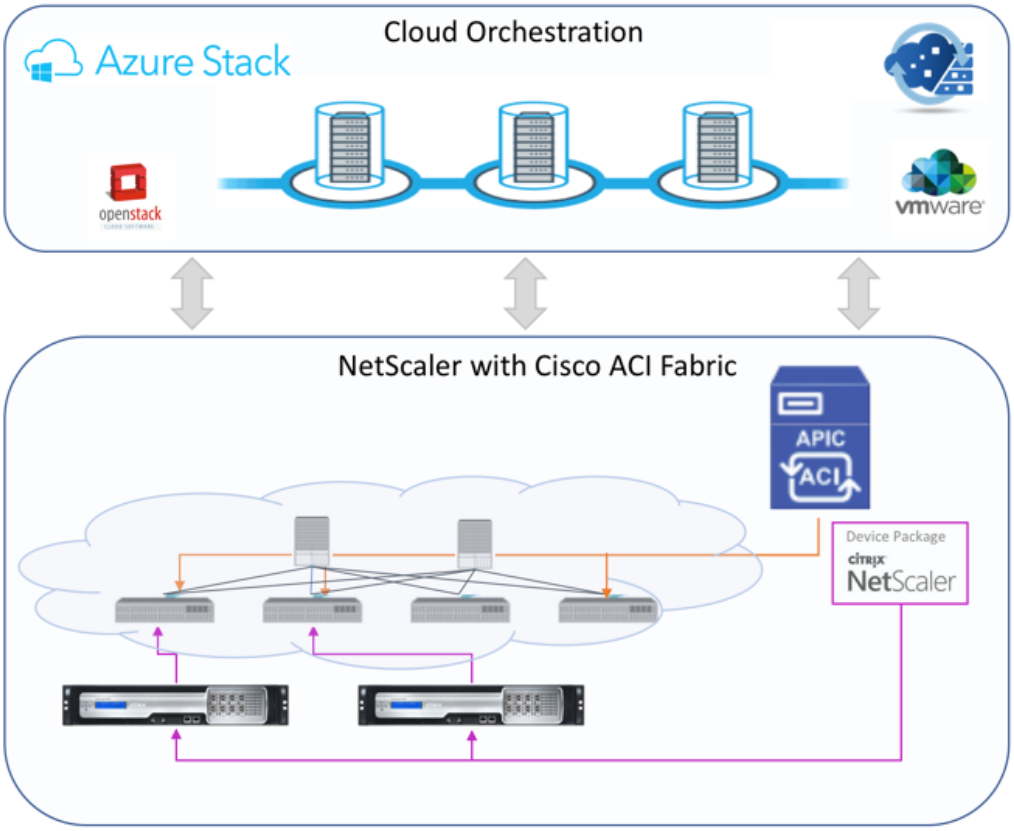
Mit Application Policy Infrastructure Controller (APIC), Version 3.1, erweitern NetScaler ADC und Cisco ACI das gemeinsame Integrationsportfolio, um eine neue Lösung bereitzustellen, die auf die Bedürfnisse des Kunden zugeschnitten ist. Der neue Integrationsmodus ACI Cloud Orchestrator Mode, vereinfacht L4-L7-Integrationen, indem die Komplexität der Konfiguration durch standardisierte Parameter abstrahiert wird. Die Lösung automatisiert nahtlos L4-L7-Services und erreicht so die Ziele agiler Anwendungsbereitstellungen, betrieblicher Flexibilität und Einfachheit.

Der Cisco ACI Cloud Orchestrator-Modus mithilfe der NetScaler ADC-Lösung bietet folgende Vorteile:

- Die Automatisierung von L4-L7-Diensten reduziert menschliche Fehler.
- Die vorgefertigte Integration der Cisco ACI-Lösung hilft Ihnen, die Bereitstellungszeit zu verkürzen und die Leistung von Anwendungen wie Webanwendungen, virtuellen Maschinen und SQL zu steigern.
- Vollständig integrierte Transparenz in den Zustand von Anwendungen wie Webanwendungen, virtuellen Maschinen und SQL über physische und virtuelle Netzwerkkomponenten hinweg.

Der ACI-Cloud-Orchestrator-Modus bietet Ihnen jetzt mehr Möglichkeiten, die neue vereinfachte APIC-GUI direkt zu verwenden oder indem Sie einen beliebigen Cloud-Orchestrator wie Cisco Cloud Center, Windows Azure Pack, OpenStack, vRealize oder einen anderen auswählen, je nach Ihren Wünschen. Diese neue Änderung wird erreicht, indem eine Reihe von ADC-Attributen als ADC-Schema verfügbar gemacht wird. Diese Attribute werden in den Funktionsprofilen der Gerätepakete abgebildet. Sie können Werte für diese Attribute angeben, während Sie den ADC-Dienst vom Cloud-Orchestrator (Cisco Cloud Center oder Wireless Application Protocol (WAP)) bereitstellen.

Die folgende Abbildung bietet einen Überblick über NetScaler ADC in einer Cloud-Orchestrierungslösung:

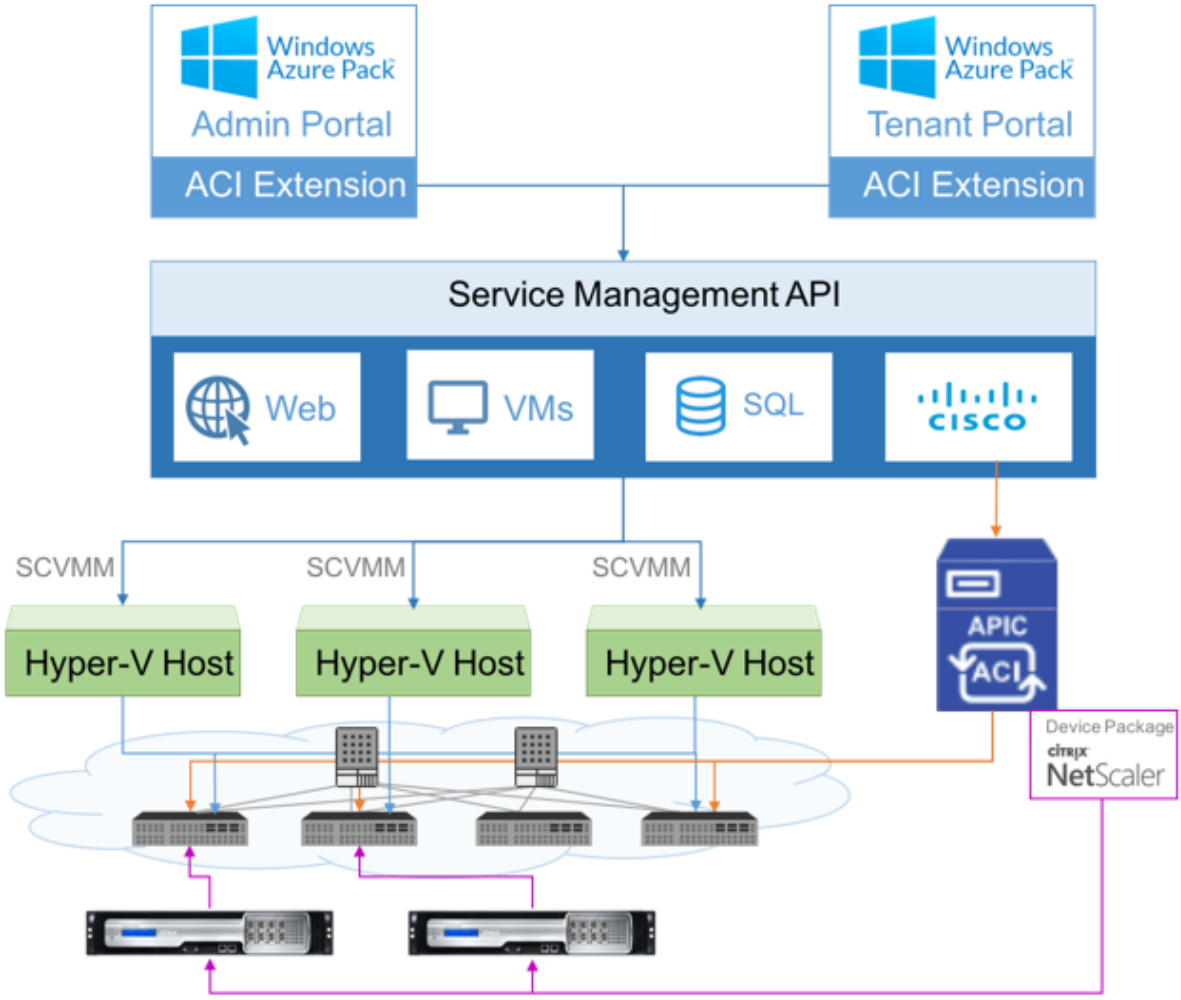


Die Lösung für den Cloud-Orchestrator-Modus mit Microsoft Azure Pack umfasst viele Integrationspunkte, wie Azure Pack zu Cisco APIC, Cisco APIC zu System Central Virtual Machine Manager (SCVMM) und Cisco APIC zu NetScaler ADC. Als Mandant in der Private Cloud können Sie NAT aktivieren, Netzwerkdienste bereitstellen und einen Load Balancer hinzufügen.

Azure Pack unterstützt Mandanten- und Administratorportale, und jedes von ihnen verfügt über eigene Vorgänge, die ausgeführt werden können.

- Als Administrator können Sie administrative Aufgaben wie die ACI-Registrierung, den VIP-Bereich, die NetScaler ADC-Gerätezuordnung mit der Cloud der virtuellen Maschine und die Erstellung von Mandantenbenutzerkonten ausführen.
- Als Mandant können Sie Aufgaben wie das Anmelden am Azure Pack-Mandantenportal und das Konfigurieren des Netzwerks, der Brückendomänen und des virtuellen Routing and Forwarding (VRFs) ausführen und die NetScaler ADC Load Balancing- und RNAT-Funktionen verwenden.

Die folgende Abbildung bietet einen Überblick über Azure Pack in einer Lösung im Cloudmodus:



Wichtig!

- Der Cloud-Administrator kann das von APIC unterstützte L4-L7-Schema unterstützen, und alle zusätzlichen Änderungen können vom APIC-Administrator direkt im APIC vorgenommen werden. Auf diese Weise können Sie NetScaler ADC auf dem Niveau des unterstützten Funktionssatzes konfigurieren und bereitstellen.
- Mandanten können mehrere VIP-Adressen mit unterschiedlichen Ports für dasselbe Netzwerk bereitstellen. Sie müssen sicherstellen, dass die Kombination von IP und Port eindeutig ist.
- Das NetScaler ADC-Gerätepaket unterstützt nur die Bereitstellung mit einem Kontext. Jeder Mandant erhält eine dedizierte NetScaler ADC-Instanz.
- Wireless Application Protocol (WAP) unterstützt NetScaler ADC MPX-Appliances und NetScaler ADC VPX-Appliances (einschließlich NetScaler ADC VPX-Instanzen, die auf der

> NetScaler ADC SDX-Plattform bereitgestellt werden).

Das Gerätepaket im Cloud-Orchestrator-Modus unterstützt sowohl den vollständig verwalteten Modus als auch den Service Manager-Modus. Das vollständig verwaltete Modus-Paket unterstützt eine Vielzahl von Funktionsprofilen, z. B. einfacher Lastausgleich, Content Switching, SSL-Offload und andere Profile. Diese Funktionsprofile decken einen vollständigen Funktionssatz und den Bereitstellungsmodus des NetScaler ADC ab. In ähnlicher Weise unterstützt das Gerätepaket im Service Manager-Modus die ein- und zweiarmige Konfiguration und Bereitstellung von NetScaler ADC mithilfe von APIC. Das NetScaler Application Delivery Management (ADM) fungiert als Servicemanager für APIC, und Sie können NetScaler ADM verwenden, um NetScaler ADC L4-L7-Parameter zu konfigurieren.

> **Hinweis**
>
> Im Service Manager-Modus (Hybridmodus) können Sie dieselbe Server-IP-Adresse, die bereits in der NetScaler ADC Appliance vorhanden ist, nicht wiederverwenden oder neu zuweisen.

Das Funktionsprofil des Cloud-Orchestrator-Modus verfügt über eine Reihe von Parametern, die dem ADC-Schema des APICs zugeordnet sind, und der Orchestrator verwendet diese Parameter. Der Cloud-Orchestrator liefert die Werte für ADC-Parameter (VIP, während der NetScaler ADC über APIC bereitgestellt wird). Der Orchestrator kommuniziert mit den APIs von APIC und übergibt die ADC-spezifischen Details als Teil der Nutzlast für ein bestimmtes Funktionsprofil. Intern extrahiert APIC die Werte und übergibt sie an das Gerätepaket, das den NetScaler ADC intern konfiguriert.

Weitere Informationen zur vollständigen Liste der ADC-Schemas, die von Cisco APIC unterstützt werden, finden Sie im Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 3.x und früher).

Das Gerätepaket für den vollständig verwalteten Modus unterstützt die folgenden Funktionsprofile:

1. LB-HTTP-One-Arm-ProfileCM
2. LB-HTTP-Two-Arm-ProfileCM
3. LB-HTTP-Two-Arm-ServiceBackendProfileCM
4. CS-HTTP-LB-Service-ProfileCM
5. CS-SSL-LB-Service-ProfileCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHIC

11. SSLVServerProfileForAnywhereModeCM
12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM
16. CSLBServerProfileCM
17. GSLBServerProfileCM
18. CMPServerProfileCM
19. CRServerProfileC
20. DNSServerProfileCM
21. DSServerProfileCM
22. ICServerProfileCM
23. SSLVPNServerProfileCM
24. AppFWServerProfileCM
25. AAAServerProfileCM
26. AAASyslogServerProfileCM
27. IPv6WebInlineVServerProfileCM

Das Gerätepaket für den Dienstverwaltungsmodus unterstützt die folgenden Funktionsprofile im Cloud-Modus:

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

NetScaler ADC unterstützt die oben genannten Funktionsprofile. Der APIC unterstützt eine Teilmenge dieser Parameter im ADC-Schema. Wenn im Funktionsprofil nicht unterstützte Attribute von Cisco ACI vorhanden sind, müssen Sie das Funktionsprofil des Cloud Orchestrator-Modus klonen und die Werte für alle nicht unterstützten Attribute von APIC bereitstellen und die Attribute speichern. Später kann der Orchestrator das neu geklonte Funktionsprofil verwenden.

Das Citrix Cloud-Modus-Gerätepaket unterstützt NetScaler ADC 12.0 und der Service Manager-Modus verwendet auch NetScaler ADM 12.0. Das Gerätepaket hat die Modellversion von 1.0 auf 2.0 geändert und kann als Neuinstallation verwendet werden. Das Gerätepaket im Cloud-Orchestrator-Modus

kann nicht von früheren Gerätepaketversionen aktualisiert werden, da die Modellversion geändert wurde.

Gerätepakete im Cloud-Orchestrator-Modus können auch in der regulären Bereitstellung verwendet werden. Das Paket verpflichtet den Benutzer nicht, NetScaler ADC über einen Cloud-Orchestrator bereitzustellen. Das Gerätepaket ist nur mit APIC und APIC mit Cloud Orchestrator kompatibel.

Verwalten der Kubernetes Ingress-Konfiguration in NetScaler ADM

February 5, 2024

Kubernetes (K8s) ist eine Open Source-Container-Orchestrierungsplattform, die die Bereitstellung, Skalierung und Verwaltung von Cloud-nativen Anwendungen automatisiert.

Kubernetes bietet die Ingress-Funktion, mit der Clientdatenverkehr außerhalb des Clusters auf Microservices einer Anwendung zugreifen kann, die innerhalb des Kubernetes-Clusters ausgeführt wird. ADC-Instanzen können als Ingress zu Anwendungen dienen, die in einem Kubernetes-Cluster ausgeführt werden. ADC-Instanzen können den Lastenausgleich durchführen und den Nord-Süd-Datenverkehr von den Clients zu allen Microservices innerhalb des Kubernetes-Clusters weiterleiten.

> **Hinweis**
>
> - Citrix ADM unterstützt die Ingress-Funktion auf den Clustern mit Kubernetes Version 1.14 und höher.
> - NetScaler ADM unterstützt NetScaler ADC VPX- und MPX-Appliances als Ingress-Geräte.
> - In der Kubernetes-Umgebung gleicht die NetScaler ADC-Instanzlast nur den Diensttyp “NodePort”aus.

Sie können mehrere ADC-Instanzen so konfigurieren, dass sie als Ingress-Geräte auf demselben Cluster oder auf verschiedenen Clustern oder Namespaces fungieren. Nachdem Sie die Instanzen konfiguriert haben, können Sie jede Instanz basierend auf der Ingress-Richtlinie verschiedenen Anwendungen zuweisen.

Sie können eine Ingress-Konfiguration mit Kubernetes `kubectl` oder APIs erstellen und bereitstellen. Sie können auch einen Ingress von NetScaler ADM aus konfigurieren und bereitstellen.

Sie können die folgenden Aspekte der Kubernetes-Integration in ADM angeben:

- **Cluster** —Sie können Kubernetes-Cluster registrieren oder deren Registrierung aufheben, für die ADM Ingress-Konfigurationen bereitstellen kann. Wenn Sie einen Cluster in NetScaler ADM registrieren, geben Sie die Kubernetes-API-Serverinformationen an. Wählen Sie dann einen

ADM-Agenten aus, der den Kubernetes-Cluster erreichen und Ingress-Konfigurationen bereitstellen kann.

- **Richtlinien** —Ingress-Richtlinien werden verwendet, um die ADC-Instanz basierend auf Cluster oder Namespace auszuwählen, um eine Ingress-Konfiguration bereitzustellen. Geben Sie die Cluster-, Site- und Instanzinformationen an, wenn Sie eine Richtlinie hinzufügen.
- **Ingress-Konfiguration** —Diese Konfiguration ist die Kubernetes-Ingress-Konfiguration, die die Content Switching-Regeln und die entsprechenden URL-Pfade der Microservices und ihrer Ports enthält. Sie können auch die SSL/TLS-Zertifikate angeben (um die SSL-Verarbeitung auf der ADC-Instanz auszulagern) mithilfe geheimer Kubernetes-Ressourcen.

NetScaler ADM ordnet die Ingress-Konfigurationen mithilfe von Ingress-Richtlinien automatisch ADC-Instanzen zu.

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

Voraussetzungen

Um NetScaler ADC-Instanzen als Ingress-Geräte in Kubernetes-Clustern zu verwenden, stellen Sie sicher, dass Sie Folgendes haben:

- Kubernetes Cluster an Ort und Stelle.
- Kubernetes-Cluster in NetScaler ADM registriert.

Konfigurieren Sie NetScaler ADM mit einem geheimen Token für die Verwaltung eines Kubernetes-Clusters

Damit NetScaler ADM Ereignisse von Kubernetes empfangen kann, müssen Sie ein Dienstkonto in Kubernetes für NetScaler ADM erstellen. Konfigurieren Sie das Dienstkonto mit den erforderlichen RBAC-Berechtigungen im Cluster.

1. Erstellen Sie ein Dienstkonto für NetScaler ADM. Beispielsweise kann der Name des Dienstkontos sein`citrixadm-sa`. Informationen zum Erstellen eines Dienstkontos finden Sie unter Verwenden mehrerer Dienstkonten.
2. Verwenden Sie die`cluster-admin` Rolle, um das NetScaler ADM Dienstkonto zu binden. Diese Bindung gewährt einem Dienstkonto eine clusterübergreifende `ClusterRole`. Im Folgenden finden Sie einen Beispielbefehl zum Binden einer `cluster-admin`-Rolle an das Dienstkonto.


```
kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
   =cluster-admin --serviceaccount=default:citrixadm-sa
<!--NeedCopy-->
```

Nachdem das NetScaler ADM Dienstkonto an die`cluster-admin` Rolle gebunden wurde, verfügt das Dienstkonto über den clusterweiten Zugriff. Weitere Informationen finden Sie unter `kubectl` create `clusterrolebinding`.

3. Beziehen Sie das Token aus dem erstellten Dienstkonto.

   Führen Sie beispielsweise den folgenden Befehl aus, um das Token für das Dienstkonto `citrixadm-sa` anzuzeigen:

```
kubectl describe sa citrixadm-sa
<!--NeedCopy-->
```

4. Führen Sie den folgenden Befehl aus, um die geheime Zeichenfolge des Tokens abzurufen:

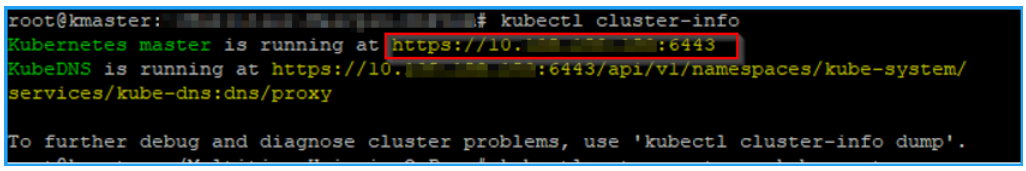
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

Fügen Sie den Kubernetes-Cluster in NetScaler ADM hinzu

Nachdem Sie einen NetScaler ADM Agent konfiguriert und statische Routen konfiguriert haben, müssen Sie den Kubernetes-Cluster in NetScaler ADM registrieren.

So registrieren Sie den Kubernetes-Cluster:

1. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler ADM an.
2. Navigieren Sie zu **Orchestration** > **Kubernetes** > **Cluster**.
   Die Seite “Cluster”wird angezeigt.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie auf der Seite **Cluster hinzufügen** die folgenden Parameter an:
   a) **Name** - Geben Sie einen Namen Ihrer Wahl an.
   b) **API Server URL** - Sie können die API-Server-URL-Details vom Kubernetes-Hauptknoten abrufen.
      i. Führen Sie auf dem Hauptknoten von Kubernetes den Befehl `kubectl cluster-info` aus.



ii. Geben Sie die URL ein, die für **Kubernetes master is running at** angezeigt wird.

c) **Authentifizierungstoken** —Geben Sie die Authentifizierungstoken-Zeichenfolge an , die Sie erhalten, während Sie NetScaler ADM für die Verwaltung eines Kubernetes Das Authentifizierungstoken ist erforderlich, um den Zugriff für die Kommunikation zwischen dem Kubernetes-Cluster und NetScaler ADM zu überprüfen. So generieren Sie ein Authentifizierungstoken:

i. Führen Sie auf dem Hauptknoten von Kubernetes die folgenden Befehle aus:

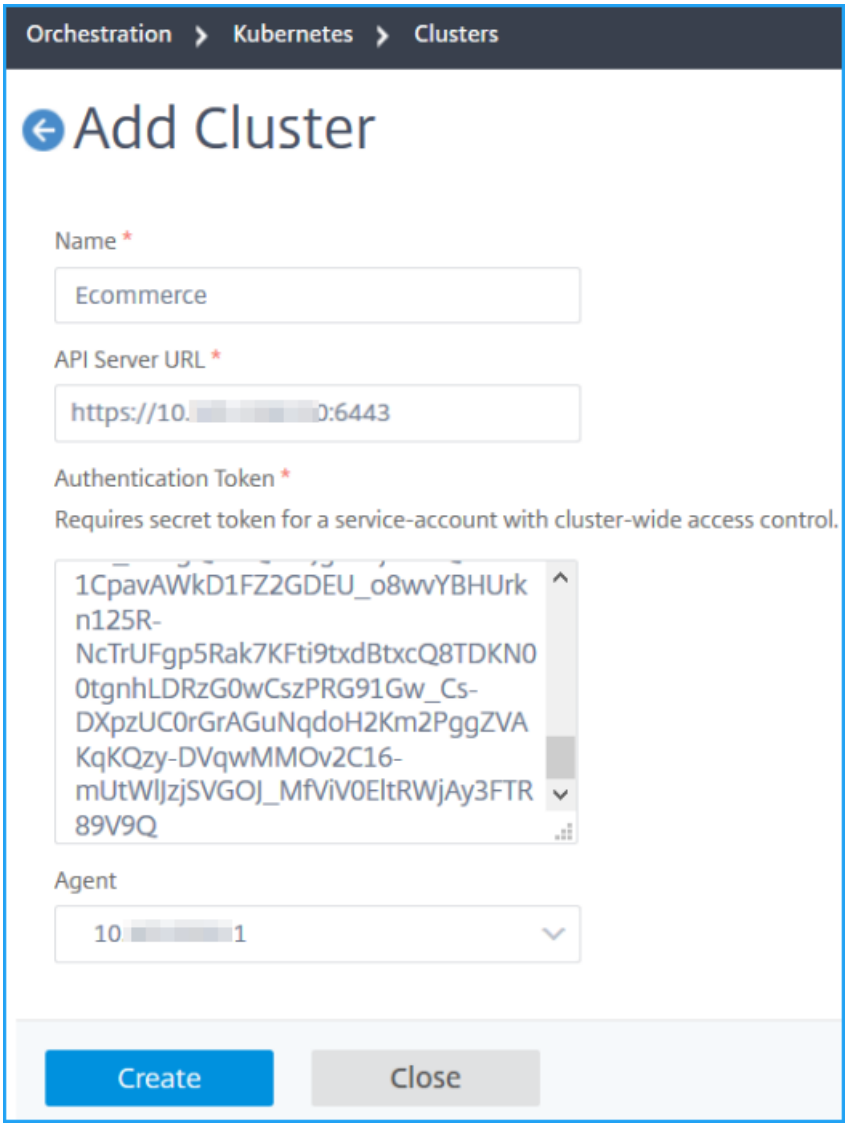
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

ii. Kopieren Sie das generierte Token und fügen Sie es als Authentifizierungstoken ein

Weitere Informationen finden Sie in der Kubernetes-Dokumentation.

d) Wählen Sie den Agent aus der Liste aus.

e) Klicken Sie auf **Erstellen**.



Definieren einer Ingress-Richtlinie

Die Ingress-Richtlinie entscheidet, welcher NetScaler ADC zum Bereitstellen einer Ingress-Konfiguration verwendet wird, basierend auf dem Ingress-Cluster oder Namespace.

1. Navigieren Sie zu **Orchestrierung > Kubernetes > Richtlinie**.
2. Klicken Sie auf **Hinzufügen**, um eine Richtlinie zu erstellen.
    a) Geben Sie den Richtliniennamen an.
    b) Definieren Sie **Bedingungen** für die Bereitstellung der Ingress-Konfiguration auf einem Kubernetes-Cluster. Diese Bedingungen basieren normalerweise auf Ingress-Cluster und Namespace.

c) Im Infrastruktur-Panel

- **Standort** —Wählen Sie eine Website aus der Liste aus.
- **Instanz** —Wählen Sie die ADC-Instanz aus der Liste aus.

Die **Site** - und **Instanz-Listen** füllen die Optionen basierend auf der Cluster-Auswahl im Bereich "**Bedingungen** "auf.

In diesen Listen werden die Sites oder Instanzen angezeigt, die mit dem NetScaler ADM Agent verknüpft sind, der mit dem Kubernetes-Cluster konfiguriert ist.

d) **Wählen Sie unter Netzwerk**auswählen das Netzwerk aus, von dem ADM die virtuellen IP-Adressen automatisch einer Ingress-Konfiguration zuweist.

In dieser Liste werden die Netzwerke angezeigt, die unter **Netzwerke > IPAM**erstellt wurden.

e) Klicken Sie auf **Erstellen**.

Stellen Sie die Ingress-Konfiguration bereit

Sie können die Ingress-Konfiguration über Kubernetes mithilfe der `kubectl`Kubernetes-API oder anderer Tools bereitstellen. Sie können die Ingress-Konfiguration auch direkt von NetScaler ADM aus bereitstellen.

1. Navigieren Sie zu **Orchestration > Kubernetes > Ingresses**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Ingress erstellen** die folgenden Details an:

   a) Geben Sie den Namen des Ingress an.

   b) Wählen Sie in **Cluster**den Kubernetes-Cluster aus, auf dem Sie einen Ingress bereitstellen möchten.

   c) Wählen Sie den **Cluster-Namespace** aus der Liste aus. In diesem Feld werden die Namespaces aufgeführt, die im angegebenen Kubernetes-Cluster vorhanden sind.

   d) Wählen Sie optional **Frontend-IP-Adresse automatisch zuweisen**.

   e) Wählen Sie **in der Liste Ingress Protocol** aus. Wenn Sie **HTTPS**auswählen, geben Sie den **TLS-Schlüssel an**.

   Dieses Geheimnis bettet die geheime Kubernetes-Ressource ein, die das HTTPS-Zertifikat und den privaten Schlüssel einbettet.

   Ein HTTPS-Ingress erfordert ein TLS-basiertes Secret, das auf dem Kubernetes-Cluster konfiguriert ist. Geben Sie die Felder `tls.crt` und `tls.key` an, um das Serverzertifikat bzw. den Zertifikatsschlüssel aufzunehmen.

f) Geben Sie für das Weiterleiten von Inhalten die folgenden Details an:

- **URL-Pfade** —Geben Sie den Pfad an, der mit dem Kubernetes-Dienst und Port verknüpft ist.
- **Kubernetes-Dienst** —Geben Sie den gewünschten Dienst an.
- **Port** —Geben Sie den Dienst-Port an.
- **LB-Methode** —Wählen Sie die bevorzugte Lastausgleichsmethode für den ausgewählten Kubernetes-Dienst aus.

  Bei der ausgewählten Methode wird die Ingress-Spezifikation mit einer entsprechenden Anmerkung aktualisiert. Wenn Sie beispielsweise die **ROUNDROBIN-Methode** auswählen, wird die Citrix Anmerkung wie folgt angezeigt:

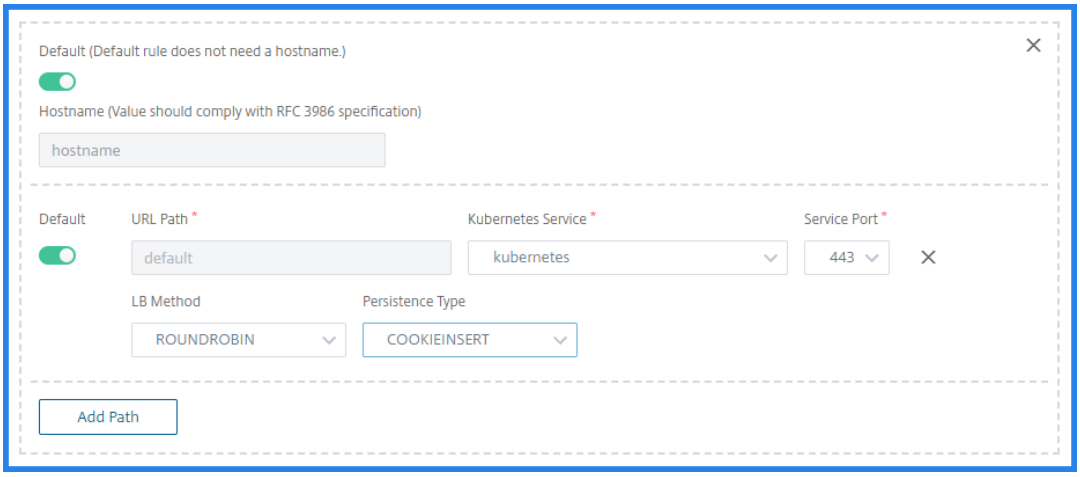
```
1  "lbmethod":"ROUNDROBIN"
2  <!--NeedCopy-->
```

- **Persistenztyp** —Wählen Sie den bevorzugten Persistenztyp für den Lastausgleich für den ausgewählten Kubernetes-Dienst aus.

  Der ausgewählte Persistenztyp aktualisiert die Ingress-Spezifikation mit einer entsprechenden Anmerkung. Wenn Sie beispielsweise **COOKIEINSERT**auswählen, wird die Citrix Anmerkung wie folgt angezeigt:

```
1  "persistenceType":"COOKIEINSERT"
2  <!--NeedCopy-->
```

Klicken Sie auf **Hinzufügen**, um weitere URL-Pfade und Ports zur Ingress-Konfiguration hinzuzufügen.



Nach der Bereitstellung leitet die Ingress-Konfiguration den Clientdatenverkehr basierend auf den folgenden Angaben zu einem bestimmten Dienst um:

- Der angeforderte URL-Pfad und Port.

- Die definierte LB-Methode und der Persistenztyp.

> **Hinweis:**
>
> Es wird erwartet, dass die in einer Ingress-Konfiguration verwendeten Kubernetes-Dienste vom Typ NodePort sind.

g) Geben Sie optional eine **Ingress-Beschreibung**an.

h) klicken Sie auf **Bereitstellen**.

Wenn Sie die Konfiguration vor der Bereitstellung überprüfen möchten, klicken Sie auf **Ingress-Spezifikation generieren**. Die angegebene Ingress-Konfiguration wird im YAML-Format angezeigt. Nachdem Sie die Konfiguration überprüft haben, klicken Sie auf **Bereitstellen**.

> **Hinweis Wenden Sie**
> Lizenzen auf die virtuellen Server an, die mit Ingress-Konfigurationen erstellt wurden. Führen Sie die folgenden Schritte aus, um die Lizenz anzuwenden:
>
> 1. Wechseln Sie zu **System > Lizenzierung und Analyse**.
> 2. Aktivieren Sie unter **Virtueller Server-Lizenzübersicht**die **Option Virtuelle Server automatisch auswählen**.

NetScaler ADC gepoolte Kapazität

February 5, 2024

Mit der gepoolten NetScaler ADC-Kapazität können Sie Bandbreite- oder Instanzlizenzen für verschiedene ADC-Formfaktoren freigeben. Für Instanzen, die auf virtuellen CPU-Abos basieren, können Sie die virtuelle CPU-Lizenz für Verwenden Sie diese gepoolte Kapazität für die Instanzen, die sich im Rechenzentrum oder in öffentlichen Clouds befinden. Wenn eine Instanz die Ressourcen nicht mehr benötigt, checkt sie die zugewiesene Kapazität wieder in den gemeinsamen Pool ein. Verwenden Sie die freigegebene Kapazität für andere ADC-Instanzen wieder, die Ressourcen benötigen.

Sie können die gepoolte Lizenzierung verwenden, um die Bandbreitennutzung zu maximieren, indem Sie die erforderliche Bandbreitenzuweisung zu einer Instanz sicherstellen und nicht mehr als Erhöhen oder verringern Sie die Bandbreite, die einer Instanz zur Laufzeit zugewiesen ist, ohne den Datenverkehr zu beeinträchtigen. Mit den gepoolten Kapazitätslizenzen können Sie die Instanz-Bereitstellung automatisieren.

So funktioniert NetScaler ADC gepoolte Kapazitätslizenzierung

Die gepoolte NetScaler ADC-Kapazität umfasst die folgenden Komponenten:

- NetScaler ADC-Instanzen, die kategorisiert werden können in:
  - Hardware ohne Kapazität
  - Eigenständige VPX-Instanzen oder CPX-Instanzen oder BLX-Instanzen
- Bandbreitenpool
- Instanzpool
- NetScaler ADM als Lizenzserver konfiguriert

Hardware ohne Kapazität

Bei der Verwaltung über NetScaler ADC gepoolte Kapazität werden MPX- und SDX-Instanzen als "Hardware ohne Kapazität"bezeichnet, da diese Instanzen erst funktionieren können, wenn sie Ressourcen aus den Bandbreite- und Instanzpools auschecken. Daher werden diese Plattformen auch als MPX-Z- und SDX-Z-Appliances bezeichnet.

Hardware ohne Kapazität erfordert eine Plattformlizenz, um Bandbreite und Instanzlizenz aus dem gemeinsamen Pool auschecken zu können.

> **Hinweis**
>
> Für MPX-Instanzen ist kein Instanz-Lizenzabonnement erforderlich. Siehe Tabelle 1 auf dieser Seite für unterstützte gepoolte Kapazität für MPX- und SDX-Instanzen. In Tabelle 5 finden Sie die Lizenzanforderungen für verschiedene MPX- und SDX-Formfaktoren.

Verwalten und Installieren von Plattformlizenzen

Sie müssen eine Plattformlizenz manuell installieren, indem Sie die Hardwareseriennummer oder den Lizenzzugriffscode verwenden. Nachdem eine Plattformlizenz installiert wurde, ist sie an die Hardware gebunden und kann bei Bedarf nicht für NetScaler ADC-Hardwareinstanzen freigegeben werden. Sie können die Plattformlizenz jedoch manuell auf eine andere NetScaler ADC Hardwareinstanz verschieben.

ADC MPX-Instanzen, auf denen das ADC-Softwareversion 11.1 Build 54.14 oder höher ausgeführt wird, und ADC SDX-Instanzen, auf denen 11.1 Build 58.13 oder höher ausgeführt wird, unterstützen ADC-gepoolte Kapazität. Weitere Informationen finden Sie in **Tabelle 1. Unterstützte gepoolte Kapazität für MPX- und SDX-Instanzen**.

Standalone NetScaler ADC VPX-Instanzen

NetScaler ADC VPX-Instanzen, auf denen NetScaler ADC-Softwareversion 11.1 Build 54.14 und höher ausgeführt wird, unterstützen die gepoolte Kapazität:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

NetScaler ADC VPX-Instanzen, auf denen NetScaler ADC-Softwareversion 12.0 Build 51.24 und höher auf den folgenden Hypervisoren und Cloud-Plattformen ausgeführt wird, unterstützen gepoolte Kapazität:

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

> **Hinweis**
>
> Um die Kommunikation zwischen NetScaler ADM und Microsoft Azure oder AWS zu ermöglichen, muss ein IPSEC-Tunnel konfiguriert werden.Weitere Informationen finden Sie unter Hinzufügen von in der Cloud bereitgestellten NetScaler ADC VPX-Instanzen zu NetScaler ADM.
> Im Gegensatz zu Hardware ohne Kapazität erfordert VPX keine Plattformlizenz. Um den Datenverkehr zu verarbeiten, muss er Bandbreite und eine Instanzlizenz aus dem Pool auschecken.

Eigenständige NetScaler ADC CPX-Instanzen

NetScaler ADC CPX-Instanzen, die auf einem Docker Host bereitgestellt werden, unterstützen gepoolte Kapazität. Im Gegensatz zu Hardware ohne Kapazität benötigt CPX keine Plattformlizenz. Eine einzelne CPX-Instanz, die einen Durchsatz von bis zu 1 Gbit/s verbraucht, wird nur 1 Instanz und keine Bandbreite aus dem Lizenzpool auschecken. Stellen Sie sich beispielsweise vor, dass Sie 20 CPX-Instanzen mit einem Bandbreitenpool von 20 Gbit/s haben. Wenn eine der CPX-Instanzen einen Durchsatz von 500 Mbit/s verbraucht, bleibt der Bandbreitenpool für die verbleibenden 19 CPX-Instanzen 20 Gbit/s.

Wenn dieselbe CPX-Instanzen einen Durchsatz von 1500 Mbit/s verbraucht, hat der Bandbreitenpool 19,5 Gbit/s für die verbleibenden 19 CPX-Instanzen.

Bei der Poollizenzierung können Sie mehr Bandbreite nur in Vielfaches von 10 Mbit/s hinzufügen.

Eigenständige NetScaler ADC BLX-Instanzen

NetScaler ADC BLX-Instanzen unterstützen Lizenzen mit gepoolter Kapazität. Eine NetScaler ADC BLX-Instanz erfordert keine Plattformlizenz. Um den Datenverkehr zu verarbeiten, muss eine NetScaler ADC BLX-Instanz die Bandbreite und eine Instanzlizenz aus dem Pool auschecken.

Bandbreiten-Pool

Der Bandbreitenpool ist die Gesamtbandbreite, die von NetScaler ADC-Instanzen gemeinsam genutzt werden kann, sowohl physisch als auch virtuell. Der Bandbreitenpool umfasst separate Pools für jede Software-Edition (Standard, Advanced und Premium). Eine bestimmte NetScaler ADC-Instanz kann keine Bandbreite aus verschiedenen Pools gleichzeitig ausgecheckt haben. Der Bandbreitenpool, aus dem er Bandbreite auschecken kann, hängt von seiner Software-Edition ab, für die er lizenziert ist.

Instanzpool

Der Instanzpool definiert die Anzahl der VPX-Instanzen oder CPX-Instanzen oder BLX-Instanzen, die über die gepoolte NetScaler ADC-Kapazität oder die Anzahl der VPX-Instanzen in einer SDX-Z-Instanz verwaltet werden können.

Beim Auschecken aus dem Pool entsperrt eine Lizenz die Ressourcen der MPX-Z-, SDX-Z-, VPX-, CPX- und BLX-Instanz, einschließlich CPUs/PEs, SSL-Kerne, Pakete pro Sekunde und Bandbreite.

> **Hinweis**
>
> Der Verwaltungsdienst eines SDX-Z verbraucht keine Instanz.

NetScaler ADM-Lizenzserver

Die gepoolte Kapazität von NetScaler ADC verwendet das als Lizenzserver konfigurierte NetScaler ADM zur Verwaltung gepoolter Kapazitätslizenzen: Bandbreiten-Pool-Lizenzen und Instanzpool-Lizenzen. Sie können die NetScaler ADM-Software verwenden, um gepoolte Kapazitätslizenzen ohne ADM-Lizenz zu verwalten.

Beim Auschecken von Lizenzen aus Bandbreiten- und Instanzpool bestimmt der NetScaler ADC Formfaktor und die Hardwaremodell auf einer Hardware mit null Kapazität

- Die minimale Bandbreite und die Anzahl der Instanzen, die eine NetScaler ADC-Instanz auschecken muss, bevor sie funktionsfähig ist.
- Die maximale Bandbreite und die Anzahl der Instanzen, die ein NetScaler ADC auschecken kann.

- Die minimale Bandbreiteneinheit für jeden Bandbreiten-Check-out Die minimale Bandbreiteneinheit ist die kleinste Bandbreiteneinheit, die ein NetScaler ADC aus einem Pool auschecken muss. Bei jedem Auschecken muss es sich um ein ganzzahliges Vielfaches der Mindestbandbreiteneinheit handeln. Wenn die minimale Bandbreiteneinheit eines NetScaler ADC beispielsweise 1 Gbit/s beträgt, können 100 Gbit/s ausgecheckt werden, jedoch nicht 200 Mbit/s oder 150,5 Gbit/s. Die minimale Bandbreiteneinheit unterscheidet sich von der minimalen Bandbreitenanforderung. Eine NetScaler ADC-Instanz kann nur ausgeführt werden, wenn sie mindestens mit der minimalen Bandbreite lizenziert wurde. Sobald die minimale Bandbreite erreicht ist, kann die Instanz mit der minimalen Bandbreiteneinheit mehr Bandbreite auschecken.

In den Tabellen 1, 2, 3 und 4 werden die maximale Bandbreite/Instanzen, minimale Bandbreite/Instanzen und minimale Bandbreiteneinheit für alle unterstützten NetScaler ADC-Instanzen zusammengefasst. Tabelle 5 fasst die Lizenzanforderungen für verschiedene Formfaktoren für alle unterstützten NetScaler ADC-Instanzen zusammen:

Tabelle 1. Unterstützte gepoolte Kapazität für MPX- und SDX-Instanzen

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
MPX 5900Z	10	1	–	–	1 Gbit/s
MPX 8005Z	15	5	–	–	1 Gbit/s
MPX 8900Z	33	5	Nicht verfügbar	Nicht verfügbar	1 Gbit/s
MPX 8900Z FIPS	33	5	Nicht verfügbar	Nicht verfügbar	1 Gbit/s
MPX 14000Z Serie	100	20	Nicht verfügbar	Nicht verfügbar	1 Gbit/s
MPX 14000Z 40G Serie	100	20	–	–	1 Gbit/s
MPX 14000Z FIPS Serie	100	20	–	–	1 Gbit/s
MPX 14000Z 40S Serie	100	20	–	–	1 Gbit/s

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
MPX 15000Z Serie	120	20	–	–	1 Gbit/s
MPX 15000Z FIPS Serie	120	20	–	–	1 Gbit/s
MPX 15000Z 50G Serie	120	20	–	–	1 Gbit/s
MPX 115XX-Serie	42	15	–	–	1 Gbit/s
MPX 22000Z-Serie	120	40	–	–	1 Gbit/s
MPX 24000Z Serie	150	100	–	–	1 Gbit/s
MPX 25000Z 40 G	200	100	–	–	1 Gbit/s
MPX 25000ZA	200	100	–	–	1 Gbit/s
MPX 26000Z Serie	200	100	–	–	1 Gbit/s
MPX 26000Z 100G Serie	200	100	–	–	1 Gbit/s
MPX 26000Z 50S Serie	200	100	–	–	1 Gbit/s
SDX 8015Z	15	7	1	5	1 Gbit/s
SDX 8900Z	33	10	2	7	1 Gbit/s
SDX 115XX Serie	42	8	2	20	1 Gbit/s
SDX 14000Z-Serie	100	10	2	25	1 Gbit/s
SDX 14000Z 40G Serie	100	10	2	25	1 Gbit/s
SDX 14000Z 40S Serie	100	20	10	25	1 Gbit/s

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
SDX 14000Z FIPS-Serie	100	10	2	25	1 Gbit/s
SDX 15000Z 50G	120	10	2 (Hinweis: 5 Instanzen für Versionen unter 13.0 47.x)	55	1 Gbit/s
SDX 15000Z	120	10	2 Hinweis: 5 Instanzen für Versionen unter 13.0 47.x)	55	1 Gbit/s
SDX 22000Z-Serie	120	20	20	80	1 Gbit/s
SDX 25000Z 40 G	200	50	10	115	1 Gbit/s
SDX 25000ZA	200	50	10	115	1 Gbit/s
SDX 26000Z 100 G	200	50	10	115	1 Gbit/s
SDX 26000Z	200	50	10	115	1 Gbit/s
SDX 26000Z 50S	200	50	10	115	1 Gbit/s
SDX 24000Z-Serie	150	50	10	80	1 Gbit/s

> Hinweis
>
> Die Mindestbandbreite und Instanzen gelten für SDX-Instanzen, auf denen die folgenden Releases ausgeführt werden: 11.1 64.x, 12.0 63.x, 12.1 54.x und 13.0 41.x.
>
> Die Mindestabnahmemenge unterscheidet sich von der Mindestanforderung des Systems.

Tabelle 2. Unterstützte gepoolte Kapazität für CPX-Instanzen

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Mbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
CPX	10	10	1	1	10 MBit/s

Tabelle 3. Unterstützte gepoolte Kapazität für VPX-Instanzen auf Hypervisoren und Cloud-Diensten

Hypervisor/Cloud-Dienst	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Mbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
Citrix Hypervisor	40 Gbit/s	10 MBit/s	1	1	10 MBit/s
VMware ESXI	100 Gbit/s	10 MBit/s	1	1	10 Mbit/s
Linux KVM	100 Gbit/s	10 MBit/s	1	1	10 Mbit/s
Microsoft Hyper-V	3 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
AWS	30 Gbit/s	10 MBit/s	1	1	10 MBit/s
Azure	10 Gbit/s	10 MBit/s	1	1	10 MBit/s
Google Cloud	10 Gbit/s	10 MBit/s	1	1	10 MBit/s

> Hinweis:
>
> Die Mindestabnahmemenge unterscheidet sich von der Mindestsystemanforderung.

Tabelle 4. Unterstützte gepoolte Kapazität für BLX-Instanzen

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Mbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
BLX	100	10	1	1	10 MBit/s

Tabelle 5. Lizenzvoraussetzung für verschiedene Formfaktoren

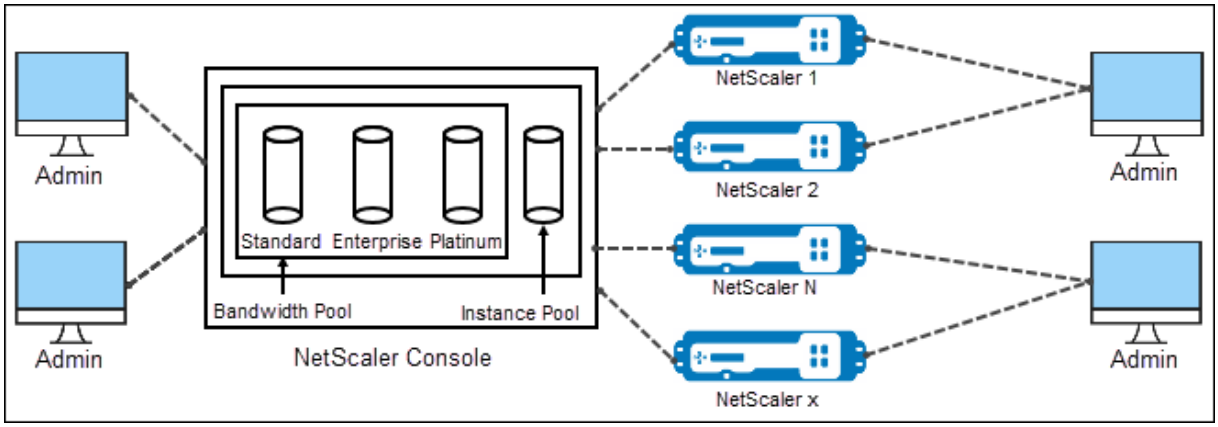
Produkt-Linie	Kauf von Hardware ohne Kapazität	Bandbreite & Edition-Abonnement	Instanz-Abonnement
MPX	Lizenz erforderlich	Lizenz erforderlich	-
SDX	Lizenz erforderlich	Lizenz erforderlich	Lizenz erforderlich
VPX	-	Lizenz erforderlich	Lizenz erforderlich
CPX	-	-	Lizenz erforderlich
BLX	-	Lizenz erforderlich	Lizenz erforderlich

Gepoolte NetScaler ADC-Kapazität konfigurieren

February 5, 2024

Um ADC-gepoolte Kapazität zu verwenden, konfigurieren Sie NetScaler ADM als Lizenzserver für die erforderlichen ADC-Instanzen. ADC-Instanzen checken Lizenzen im ADM ein und checken sie aus. Sie können die folgenden Aufgaben in der ADM-Benutzeroberfläche ausführen:

- Laden Sie die gepoolten Kapazitätslizenzdateien (Bandbreite und Instanzpool) auf den Lizenzserver hoch.
- Weisen Sie den NetScaler ADC Instanzen nach Bedarf Lizenzen aus dem Lizenzpool zu.
- Prüfen Sie die Lizenzen von NetScaler ADC-Instanzen (MPX-Z /SDX-Z/VPX/CPX/BLX) basierend auf der minimalen und maximalen Kapazität der Instanz.
- Konfigurieren Sie die gepoolte Kapazität für NetScaler ADC FIPS-Instanzen zum Ein- oder Auschecken von Lizenzen.



Unterstützte Hardware- und Softwareversionen

Unterstützte Hardware- und Softwareversionen für gepoolte Kapazität finden Sie unter NetScaler ADC gepoolte Kapazität.

ADC-gepoolte Kapazitätszustände

Die gepoolten Kapazitätszustände geben die Lizenzanforderungen für eine ADC-Instanz an. Die mit gepoolter Kapazität konfigurierten ADC-Instanzen weisen einen der folgenden Zustände auf:

- **Optimal**: Die Instanz wird mit der richtigen Lizenzkapazität ausgeführt.
- **Kapazitätskonflikt**: Instanz läuft mit einer Kapazität, die geringer ist als die vom Benutzer konfigurierte.
- **Grace**: Die Instanz wird mit einer Kulanzlizenz ausgeführt.
- **Grace & Mismatch**: Die Instanz wird im Kulanzzeitraum ausgeführt, aber mit einer Kapazität, die geringer ist als der Benutzer konfiguriert.
- **Nicht verfügbar**: Die Instanz ist nicht bei ADM für die Verwaltung registriert, oder die NITRO-Kommunikation von ADM zu den Instanzen funktioniert nicht.
- **Nicht zugewiesen**: Die Lizenz wird in der Instanz nicht zugewiesen.

Schritt 1 - Anwenden von Lizenzen in ADM

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Lizenzen**.
2. Wählen Sie im Abschnitt **Lizenzdateien** die Option **Lizenzdatei hinzufügen** aus, und wählen Sie eine der folgenden Optionen aus:
    - **Laden Sie Lizenzdateien von einem lokalen Computer**hoch. Wenn auf Ihrem lokalen Computer bereits eine Lizenzdatei vorhanden ist, können Sie sie auf ADM hochladen.
    - **Verwenden Sie den Lizenzzugriffscode**. Geben Sie den Lizenzzugriffscode für die Lizenz an, die Sie von Citrix erworben haben. Wählen Sie dann **Lizenzen abrufen**aus. Wählen Sie dann **Fertig stellen**.

    > **Hinweis**
    >
    > Sie können ADM jederzeit über die **Lizenzeinstellungen**weitere Lizenzen hinzufügen.

3. Klicken Sie auf **Fertig stellen**.

Die Lizenzdateien werden zu ADM hinzugefügt. Auf der Registerkarte **Informationen zum Lizenzablauf** werden die im ADM vorhandenen Lizenzen und die verbleibenden Tage bis zum Ablauf aufgeführt.

4. Wählen Sie unter **Lizenzdateien**eine Lizenzdatei aus, die Sie anwenden möchten, und klicken Sie auf **Lizenzen anwenden**.

   Mit dieser Aktion können ADC-Instanzen die ausgewählte Lizenz als gepoolte Kapazität verwenden.

Schritt 2 —NetScaler ADM als Lizenzserver registrieren

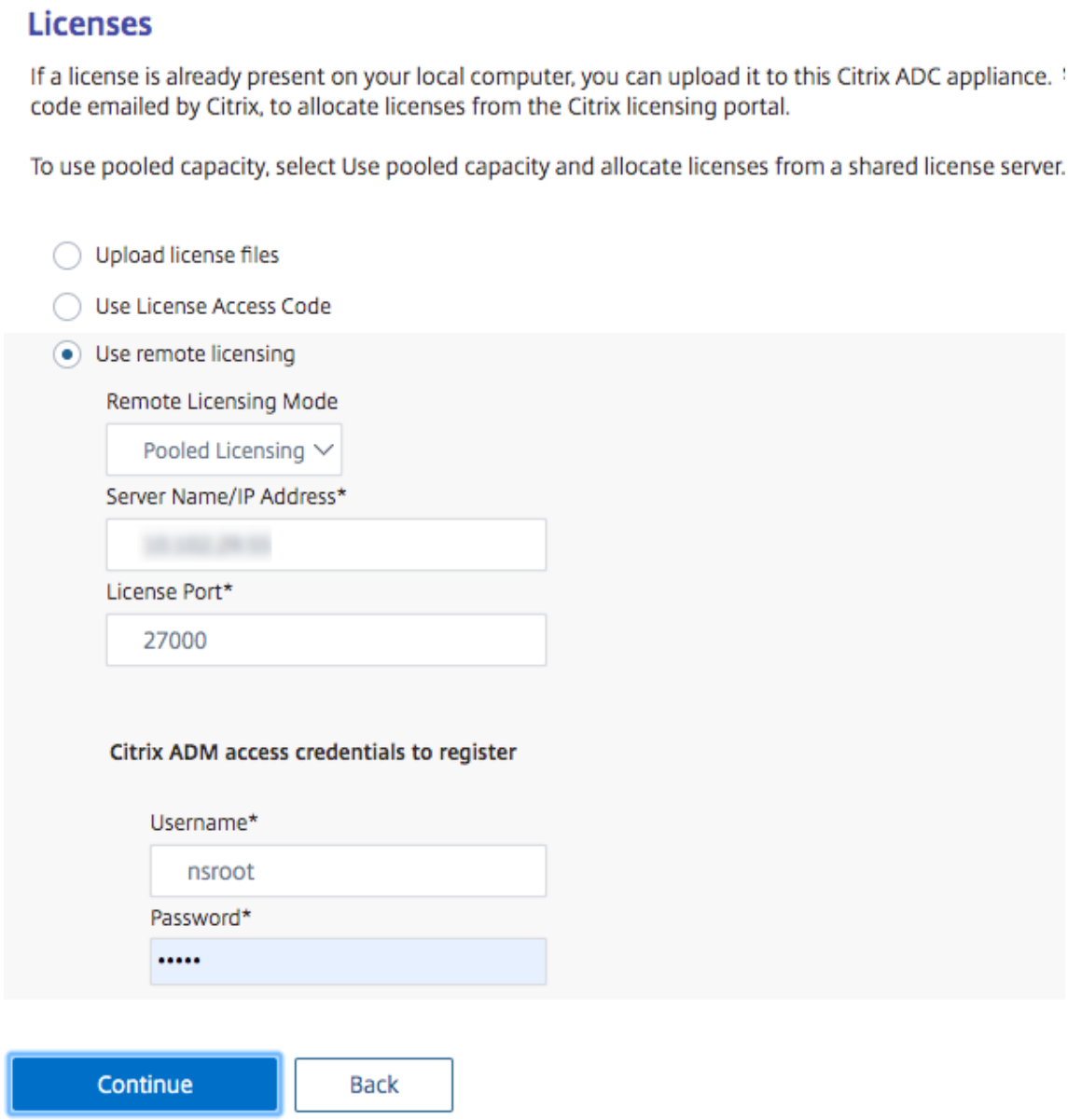
Um ADM als Lizenzserver für eine NetScaler ADC-Instanz zu registrieren, führen Sie eines der folgenden Verfahren aus:

- GUI verwenden
- CLI verwenden

Verwenden Sie die GUI, um ADM als Lizenzserver zu registrieren

Registrieren Sie den ADM-Server in der ADC-GUI als Lizenzserver.

1. Melden Sie sich bei NetScaler ADC GUI an.
2. Navigieren Sie zu **System** > **Lizenzen** > **Lizenzen verwalten**.
3. Klicken Sie auf **Neue Lizenz hinzufügen**.
4. Wählen Sie **Remote-Lizenzierung verwenden** und wählen Sie den Remote-Lizenzierungsmodus aus der Liste aus.
5. Geben Sie im Feld **Servername/IP-Adresse** die IP-Adresse des ADM-Servers an.
6. Wählen Sie **Bei NetScaler ADM registrieren**.
7. Geben Sie Ihre ADM-Anmeldeinformationen ein, um eine Instanz bei NetScaler ADM zu registrieren, und klicken Sie auf **Weiter**.



8. Wählen Sie **unter Lizenzen zuweisen**die Lizenzversion aus und geben Sie die erforderliche Bandbreite an.

   Weisen Sie erstmals Lizenzen in NetScaler ADC zu. Sie können die Lizenzzuweisung später über die ADM-GUI ändern oder freigeben.

9. Klicken Sie auf **Get Licenses**.

   > **Wichtig!**
   >
   > Starten Sie die Instanz warm neu, wenn Sie die Lizenzversion ändern. Die Konfigurationsänderungen werden erst wirksam, wenn Sie die Instanz neu starten.

Verwenden Sie CLI, um ADM als Lizenzserver hinzuzufügen

Wenn eine ADC-Instanz keine GUI hat, verwenden Sie die folgenden CLI-Befehle, um den ADM-Server als Lizenzserver hinzuzufügen:

1. Melden Sie sich bei der ADC-Konsole an.
2. Fügen Sie die IP-Adresse des ADM-Servers hinzu:

```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-port-number>
<!--NeedCopy-->
```

3. Zeigen Sie die im Lizenzserver verfügbare Lizenzbandbreite an:

```
> sh ns licenseserverpool
<!--NeedCopy-->
```

4. Weisen Sie die Lizenzbandbreite aus der erforderlichen Lizenzedition zu:

```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth > edition <specify-license-edition>
<!--NeedCopy-->
```

Die Lizenzversion kann **Standard** oder **Enterprise** oder **Platinum**sein.

> **Wichtig**
>
> Warm starten Sie die Instanz neu, wenn Sie die Lizenzversion ändern.
>
> ```
> reboot -w
> ```
>
> Die Konfigurationsänderungen werden erst wirksam, wenn Sie die Instanz neu starten.

Schritt 3 —Zuweisen von gepoolten Lizenzen zu ADC-Instanzen

So weisen Sie Lizenzen für gepoolte Kapazität über die ADM-GUI zu:

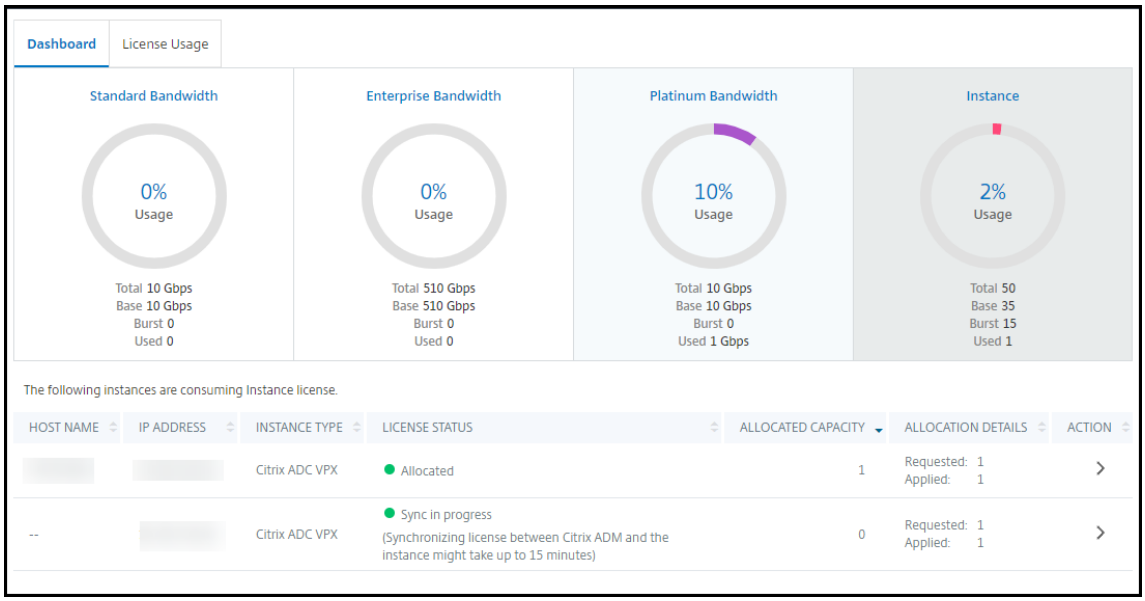
1. Melden Sie sich bei NetScaler ADM an.
2. Navigieren Sie zu **Netzwerke > Lizenzen > Bandbreitenlizenzen > Pooled Capacity**.

   Die Kapazität der FIPS-Instanz wird nur angezeigt, wenn Sie FIPS-Instanzlizenzen in ADM hochladen.
3. Klicken Sie auf den Lizenzpool, den Sie verwalten möchten.

> **Hinweis**
>
> Das Feld **Zugeordnete Kapazität** spiegelt die geänderte Bandbreite nicht sofort wider. Die Bandbreitenänderung wird nach dem Neustart des ADC wirksam.

> In **Allocation Details**werden die Felder **Angefordert** und **Angewendet** aktualisiert, wenn Sie die Bandbreitenzuweisung der Instanz ändern.

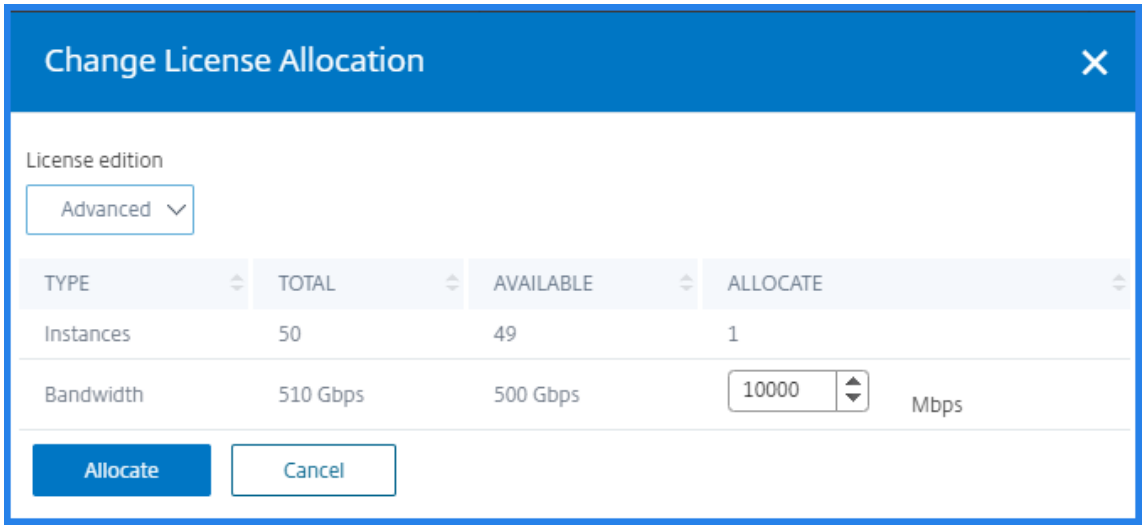
4. Wählen Sie eine ADC-Instanz aus der Liste der verfügbaren Instanzen aus, indem Sie auf die Schaltfläche **>** klicken.



**In der Spalte Lizenzstatus werden die entsprechenden Statusmeldungen zur Lizenzzuweisung angezeigt.

> **Hinweis**
>
> Die Registerkarte **Unmanaged Instanzen** zeigt die Instanzen an, die in NetScaler ADM erkannt, aber nicht verwaltet werden.

5. Klicken Sie auf **Zuweisung ändern** oder **Zuweisung freigeben**, um die Lizenzzuweisung zu ändern.
6. Ein Popup-Fenster mit den verfügbaren Lizenzen im Lizenzserver wird angezeigt.
7. Sie können die Bandbreite oder die Instanzzuweisung für die Instanz auswählen, indem Sie die Optionen für die Liste Zuordnen festlegen. Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie auf **Zuweisen**.
8. Sie können die zugewiesene Lizenzversion auch über die Listenoptionen im **Fenster Lizenzzuordnung ändern ändern**.



> **Hinweis**
>
> Warm starten Sie eine Instanz neu, wenn Sie die Lizenzversion ändern.

Konfigurieren der gepoolten Kapazität auf ADC-Instanzen

Sie können Lizenzen für gepoolte Kapazität auf den folgenden ADC-Instanzen konfigurieren:

- ADC MPX-Z-Instanzen
- ADC VPX-Instanzen
- ADC-Hochverfügbarkeitspaar

NetScaler ADC MPX-Z-Instanzen

MPX-Z ist die ADC MPX-Appliance mit gepoolter Kapazität. MPX-Z unterstützt Bandbreiten-Pooling für Premium-, Advanced- oder Standard Edition-Lizenzen.

MPX-Z benötigt Plattformlizenzen, bevor es eine Verbindung zum Lizenzserver herstellen kann. Sie können die MPX-Z-Plattformlizenz mit einer der folgenden Methoden installieren:

- Hochladen der Lizenzdatei von einem lokalen Computer.
- Verwenden der Hardware-Seriennummer der Instanz.
- Der Lizenzzugangscode aus dem Abschnitt **System** > **Lizenzen** der GUI der Instanz.

Wenn Sie die MPX-Z-Plattformlizenz entfernen, ist die Funktion der gepoolten Kapazität deaktiviert. Die Instanzlizenzen werden für den Lizenzserver freigegeben.

Sie können die Bandbreite einer MPX-Z-Instanz dynamisch ohne Neustart ändern. Ein Neustart ist nur erforderlich, wenn Sie die Lizenzversion ändern möchten.

> **Hinweis**
>
> Wenn Sie die Instanz neu starten, checkt sie automatisch die gepoolten Lizenzen aus, die für die konfigurierte Kapazität erforderlich sind.

NetScaler ADC VPX-Instanzen

Eine ADC VPX-Instanz mit gepoolter Kapazität kann Lizenzen aus einem Bandbreitenpool auschecken (Premium-/Advanced/Standard-Editionen). Sie können die ADC-GUI verwenden, um Lizenzen vom Lizenzserver auszuchecken.

Sie können die Bandbreite einer VPX-Instanz dynamisch ohne Neustart ändern. Ein Neustart ist nur erforderlich, wenn Sie die Lizenzversion ändern möchten.

> **Hinweis**
>
> Wenn Sie die Instanz neu starten, werden die konfigurierten gepoolten Kapazitätslizenzen automatisch vom ADM-Server ausgecheckt.

NetScaler ADC Hochverfügbarkeitspaar

Bevor Sie beginnen, stellen Sie sicher, dass der ADM-Server als Lizenzserver konfiguriert ist. Weitere Informationen finden Sie unter Konfigurieren von ADM als Lizenzserver.

Für ADC-Instanzen, die in einem Hochverfügbarkeitsmodus konfiguriert sind, müssen Sie die gepoolte Kapazität auf jedem Knoten des Hochverfügbarkeitspaars konfigurieren. Sowohl für den primären als auch für den sekundären Knoten müssen Sie Lizenzen mit derselben Kapazität zuweisen. Wenn Sie beispielsweise 1 Gbit/s Kapazität von jeder Instanz im HA-Paar benötigen, benötigen Sie die doppelte Kapazität (2 Gbit/s) aus dem gemeinsamen Pool. Dann können Sie jedem Knoten eine Kapazität von 1 Gbit/s zuweisen.

Um jedem Knoten im Paar eine Pool-Lizenz zuzuweisen, befolgen Sie die Schritte unter Zuweisen von gepoolten Lizenzen zu ADC-Instanzen. Weisen Sie zuerst dem ersten Knoten eine Lizenz zu und wiederholen Sie dann dieselben Schritte, um dem zweiten Knoten die Lizenz zuzuweisen.

ADM-Server nur als gepoolten Lizenzserver konfigurieren

February 5, 2024

Als Administrator können Sie einen ADM-Server nur als gepoolten Lizenzserver konfigurieren. Bei dieser Konfiguration erhält der ADM-Server nur Lizenzdaten von ADC-Instanzen.

Manchmal haben Sie möglicherweise das regulatorische Mandat, das erfordert, dass die Daten von ADC-Instanzen daran gehindert werden, den regulatorischen Bereich zu verlassen. In solchen Situationen können Sie eine lokale Instanz eines ADM-On-Prem-Servers in Ihrer regulatorischen Zone bereitstellen, um Verwaltungs-, Überwachungs- und Analysefunktionen zu nutzen. Wenn Sie den gleichen Ansatz bei der Verwendung der Funktion für gepoolte Lizenzen verfolgen, müssen Sie gepoolte Lizenzen auf verschiedene ADM-Lizenzserver aufteilen. Dieser Ansatz bietet Ihnen nicht die Flexibilität, gepoolte Lizenzen für Ihre global bereitgestellten ADC-Instanzen zuzuweisen.

Konfigurieren Sie daher den ADM-Server nur als gepoolten Lizenzserver. Der ADM-Server erhält nur Lizenzdaten von allen ADC-Instanzen. So können Sie das regulatorische Mandat einhalten und global bereitgestellte ADC-Instanzen dynamisch gepoolte Kapazitätslizenzen zuweisen.

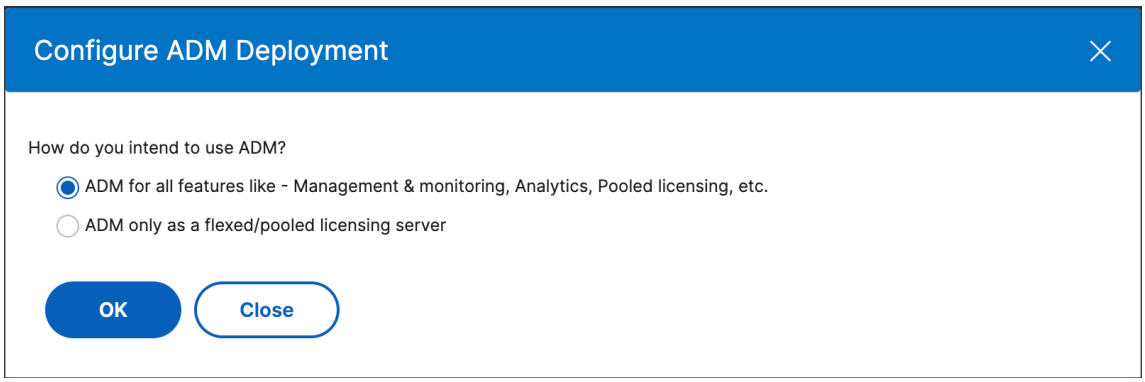
In diesem Dokument wird erläutert, wie ein ADM-Server nur als gepoolter Lizenzserver konfiguriert wird.

So konfigurieren Sie einen ADM-Server nur als gepoolten Lizenzserver

Bevor Sie beginnen, stellen Sie sicher, dass einem ADM-Server keine ADC-Instanzen hinzugefügt werden. Fügen Sie die ADC-Instanzen erst hinzu, nachdem Sie Schritt 4 abgeschlossen haben.

Gehen Sie folgendermaßen vor, um einen ADM-Server nur für den gepoolten Lizenzserver zu konfigurieren:

1. Navigieren Sie zu **System > Administration**.
2. Wählen Sie im Abschnitt “**Systemkonfigurationen** “die Option **Systembereitstellung**aus.
3. Wählen Sie in **ADM Deploymentnur ADM als gepoolten Lizenzserver**aus.



4. Klicken Sie auf **OK**.

   Diese Aktion behält nur die gepoolte Lizenzierungsfunktion bei und deaktiviert die folgenden ADM-Features:

   - ADM-Backup
   - Ereignisverwaltung

- SSL Zertifikatsverwaltung
- Netzwerkberichterstellung
- Netzwerkfunktionen
- Konfigurationsaudit

> **Hinweis**
>
> Standardmäßig ist die ADM-Analytics-Funktion deaktiviert. Stellen Sie sicher, dass Sie diese Funktion deaktivieren, wenn Sie sie aktiviert haben.

Klicken Sie im Bestätigungsfeld auf **Ja**.

Die ADM-Benutzeroberfläche zeigt jetzt nur die gepoolte Lizenzierungsfunktion an. Und die übrigen Funktionen werden nicht angezeigt.

5. Nachdem Sie ADM nur für die Lizenzierungsfunktion konfiguriert haben, fügen Sie ADC-Instanzen auf der Seite **Netzwerke > Instanzen** hinzu.

> **Hinweis**
>
> - Sie können eine ADC-Instanz auf einem oder mehreren ADM-Servern hinzufügen. Wenn Sie das Kennwort solcher ADC-Instanzen ändern, müssen Sie das Kennwort auf allen ADM-Servern aktualisieren, auf denen die Instanz erkannt wird.
> - Ein Benutzer kann weiterhin einige Vorgänge der deaktivierten Funktionen in der ADM-Benutzeroberfläche ausführen. Zum Beispiel Ereignisabfrage und ADC-Backup. Wenn Sie solche Vorgänge einschränken möchten, deaktivieren Sie als Superadministrator die Benutzerzugriffe für andere Administratoren mithilfe einer entsprechenden Zugriffsrichtlinie. Weitere Informationen finden Sie unter Konfigurieren von Zugriffsrichtlinien in NetScaler ADM.

Aktualisieren einer unbefristeten Lizenz in NetScaler ADC VPX auf NetScaler ADC-gepoolte Kapazität

February 5, 2024

NetScaler ADC VPX-Instanzen mit unbefristeter Lizenz können auf eine ADC-Lizenz mit gepoolter Kapazität aktualisiert werden. Durch ein Upgrade auf eine Lizenz mit gepoolter Kapazität können Sie den VPX-Instanzen bedarfsgerecht Lizenzen aus dem Lizenzpool zuweisen. Sie können auch eine Lizenz für gepoolte Kapazität für ADC-Instanzen konfigurieren, die in einem Hochverfügbarkeitsmodus konfiguriert sind. Informationen zum Konfigurieren der gepoolten Kapazitätslizenz für VPX-Instanzen im

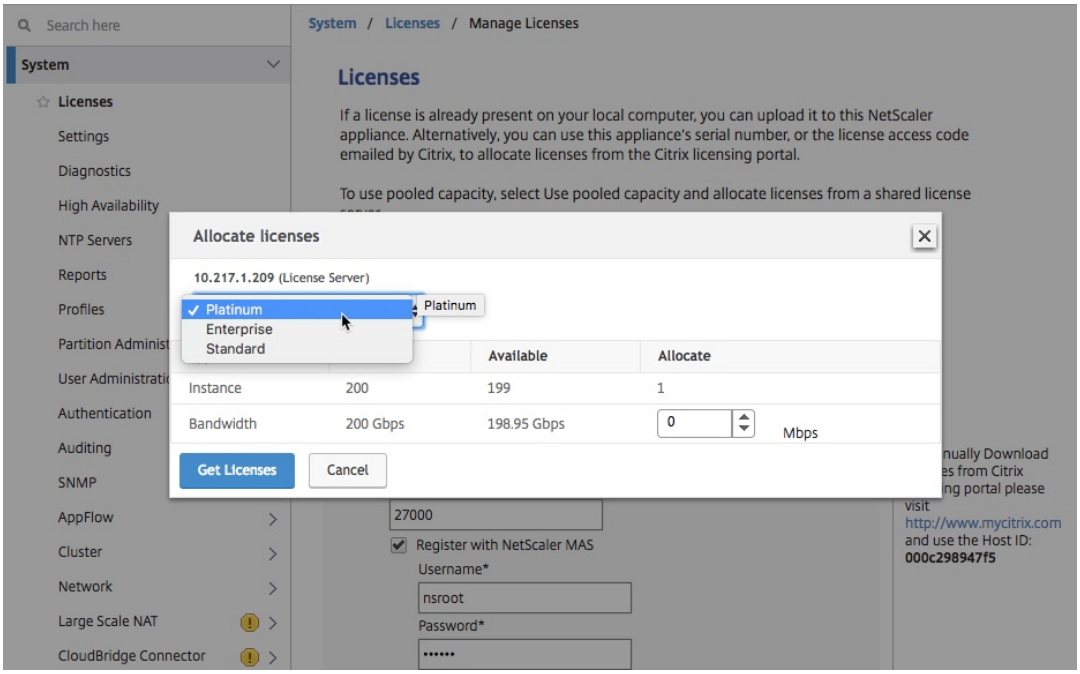
Hochverfügbarkeitsmodus finden Sie unter Aktualisieren der unbefristeten Lizenz in NetScaler ADC VPX High Availability Pair auf NetScaler ADC Pooled Capacity.

Voraussetzungen

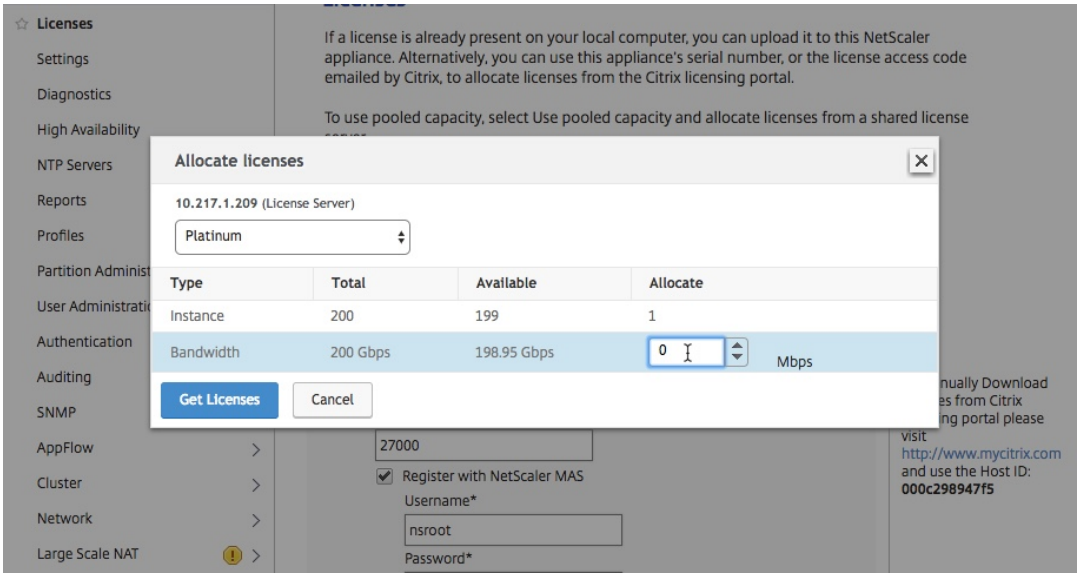
Stellen Sie sicher, dass Sie die VPX-Instanz auf Version 12.0.56.x aktualisieren.

So aktualisieren Sie auf NetScaler ADC gepoolte Kapazität:

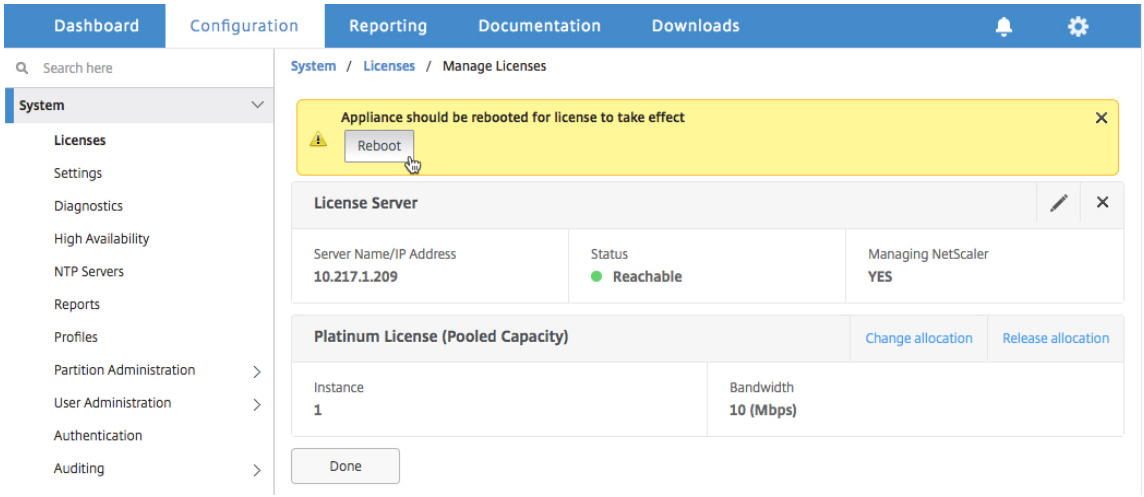
1. Geben Sie in einem Webbrowser die IP-Adresse der VPX-Instanz ein, z. http://192.168.100.1B.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der **Willkommensseite** auf **Weiter**.
4. Navigieren Sie auf der Registerkarte Konfiguration zu **System > Lizenzen**, und klicken Sie auf **Lizenzen verwalten**.
5. Klicken Sie auf der Seite **Lizenzen** auf **Neue Lizenz hinzufügen**.
6. Wählen Sie auf der Seite **Lizenzen** die Option **Remote-Lizenzierung verwenden** aus, und führen Sie die folgenden Schritte aus:
    a) Wählen Sie in der Dropdownliste **Remotelizenzierungsmodus** die Option **Pooled Licensing**.
    b) Geben Sie im Feld **Servername/IP-Adresse** die Details des Lizenzservers ein.
    c) Stellen Sie sicher, dass das Kontrollkästchen **Bei NetScaler ADM registrieren** aktiviert ist, und geben Sie NetScaler ADM-Anmeldeinformationen ein, wenn Sie die Poollizenzen Ihrer Instanz über ADM verwalten möchten.
    d) Klicken Sie auf **Weiter**.
7. Gehen Sie im Fenster **Lizenzen zuweisen** wie folgt vor:
    a) Wählen Sie die Lizenzversion aus der Dropdownliste aus.



b) Weisen Sie der NetScaler ADC Appliance im Menü **Zuweisen** die Bandbreite zu, und klicken Sie auf **Lizenzen abrufen**.



8. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Neu starten**, um die Appliance neu zu starten.



9. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
10. Nachdem die VPX-Instanz neu gestartet wurde, melden Sie sich bei der Instanz an. Klicken Sie auf der **Willkommensseite** auf **Weiter**.

    Auf der Seite **Lizenzen** werden alle Funktionen angezeigt, die auf der NetScaler ADC VPX-Appliance lizenziert sind. Klicken Sie auf **X**.
11. Navigieren Sie zu **System > Lizenzen**, und klicken Sie auf **Lizenzen verwalten**.

    Auf der Seite **Lizenzen verwalten** können Sie die Details des Lizenzservers, der Lizenzedition und der zugewiesenen Bandbreite anzeigen.

Upgrade der unbefristeten Lizenz im NetScaler ADC VPX Hochverfügbarkeitspaar auf NetScaler ADC-gepoolte Kapazität

Für VPX-Instanzen, die in einem Hochverfügbarkeitsmodus konfiguriert sind, müssen Sie die gepoolte Kapazität sowohl auf der primären als auch auf der sekundären Instanz im HA-Paar konfigurieren. Sowohl für die primäre als auch für die sekundäre Instanz müssen Sie Lizenzen mit derselben Kapazität zuweisen. Wenn Sie beispielsweise 1 Gbit/s Kapazität von jeder Instanz im HA-Paar benötigen, benötigen Sie die doppelte Kapazität (2 Gbit/s) aus dem gemeinsamen Pool. Anschließend können Sie den primären und sekundären Instanzen im HA-Paar jeweils 1 Gbit/s Kapazität zuweisen.

So aktualisieren Sie ein vorhandenes NetScaler ADC VPX HA-Setup auf NetScaler ADC Pooled Capacity:

1. Melden Sie sich bei der sekundären VPX-Instanz (Knoten 2) an. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler ADC Appliance ein, `http://192.168.100.1`z.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.

3. Klicken Sie auf der **Willkommensseite** auf **Weiter**.
4. Navigieren Sie auf der Registerkarte Konfiguration zu **System** > **Lizenzen** und klicken Sie auf **Lizenzen verwalten**.
5. Klicken Sie auf der Seite **Lizenzen** auf **Neue Lizenz hinzufügen**.
6. Wählen Sie auf der Seite **Lizenzen** die Option **Remote-Lizenzierung verwenden** aus, und führen Sie die folgenden Schritte aus:

   a) Wählen Sie in der Dropdownliste **Remotelizenzierungsmodus** die Option **Pooled Licensing**.

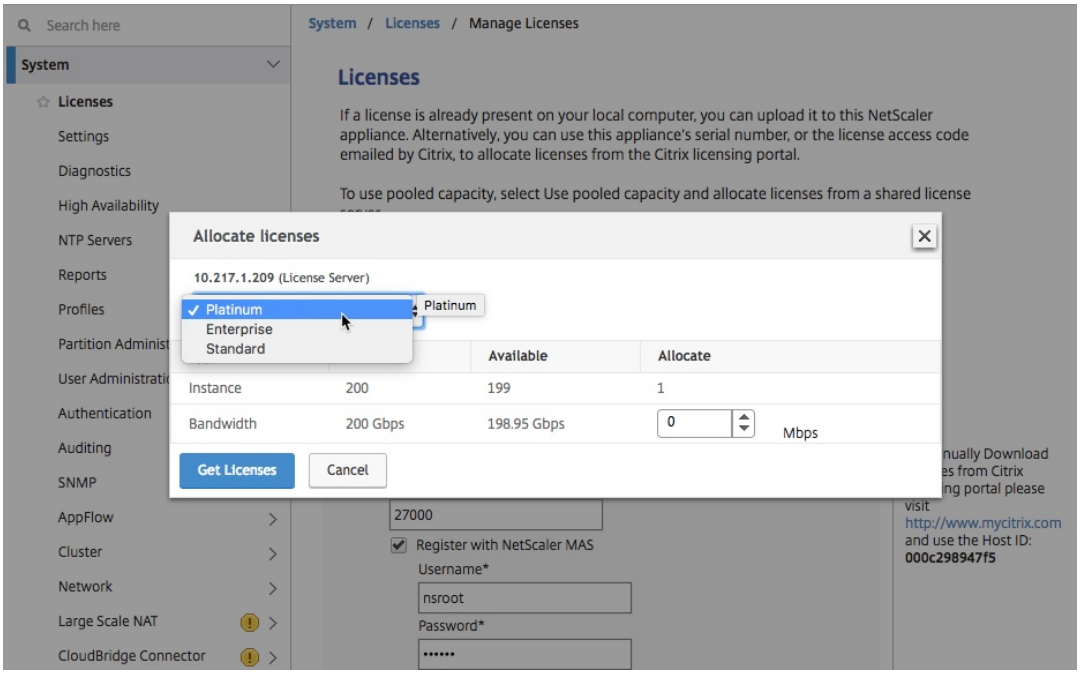
   b) Geben Sie im Feld **Servername/IP-Adresse** die Details des Lizenzservers ein.

   c) Stellen Sie sicher, dass das Kontrollkästchen **Bei NetScaler ADM registrieren** aktiviert ist, und geben Sie die ADM-Anmeldeinformationen ein, wenn Sie die Poollizenzen Ihrer Instanz über NetScaler ADM verwalten möchten.

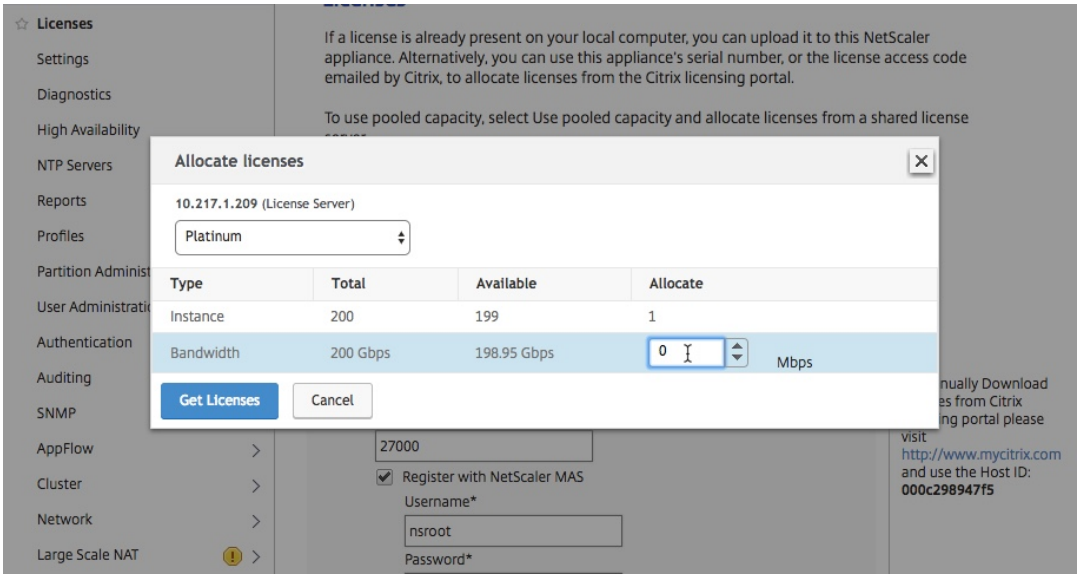
   d) Klicken Sie auf **Weiter**.

7. Gehen Sie im Fenster Lizenzen zuweisen wie folgt vor:

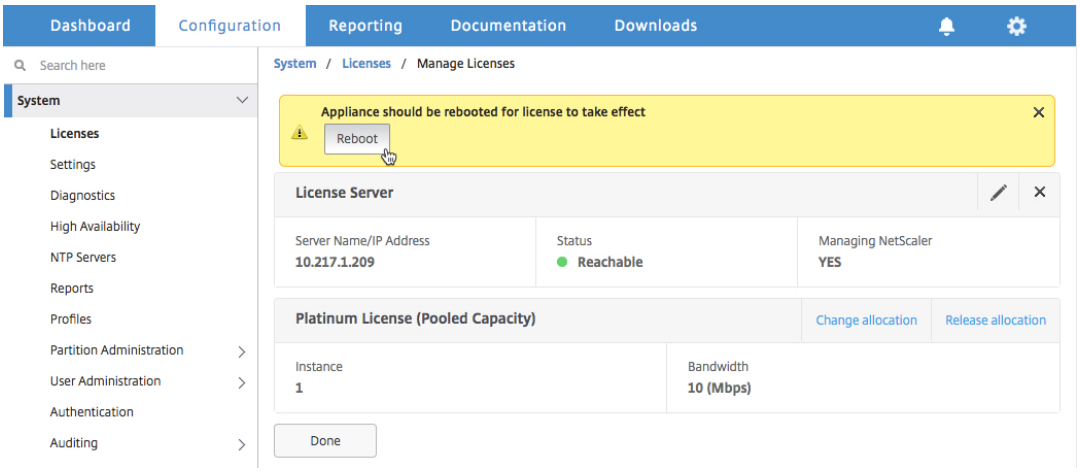
   a) Wählen Sie die Lizenzversion aus der Dropdownliste aus.



   b) Weisen Sie der NetScaler ADC Appliance im Menü **Zuweisen** die Bandbreite zu, und klicken Sie auf **Lizenzen abrufen**.



c) Wenn Sie dazu aufgefordert werden, klicken Sie auf **Reboot**, um die Instanz



8. Klicken **Sie im Dialogfeld „Bestätigen** “auf **Ja**.

   Die VPX-Instanz wird neu gestartet.

   Wenn Sie dazu aufgefordert werden, klicken Sie auf Neustart, um die Appliance Nachdem die Appliance mit der neuen Lizenz in Betrieb genommen wurde, erzwingen Sie ein Failover, indem Sie eingeben `force ha failover`. Dieses Failover stellt sicher, dass das HA-Paar in gutem Zustand ist.

9. Melden Sie sich bei der vorhandenen primären VPX-Instanz (Knoten 1) an und starten Sie sie neu. Führen Sie die folgenden Schritte aus.

   a) Geben Sie in einem Webbrowser die IP-Adresse der NetScaler ADC Appliance ein, http://192.168.100.1z.

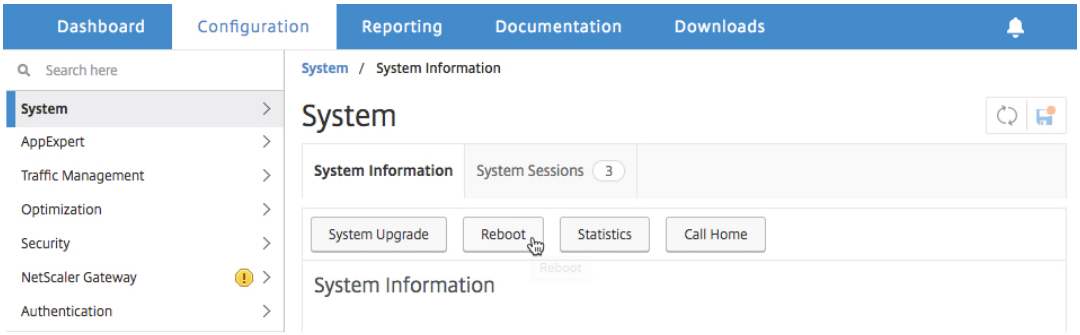
   b) Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinfor-

mationen ein.

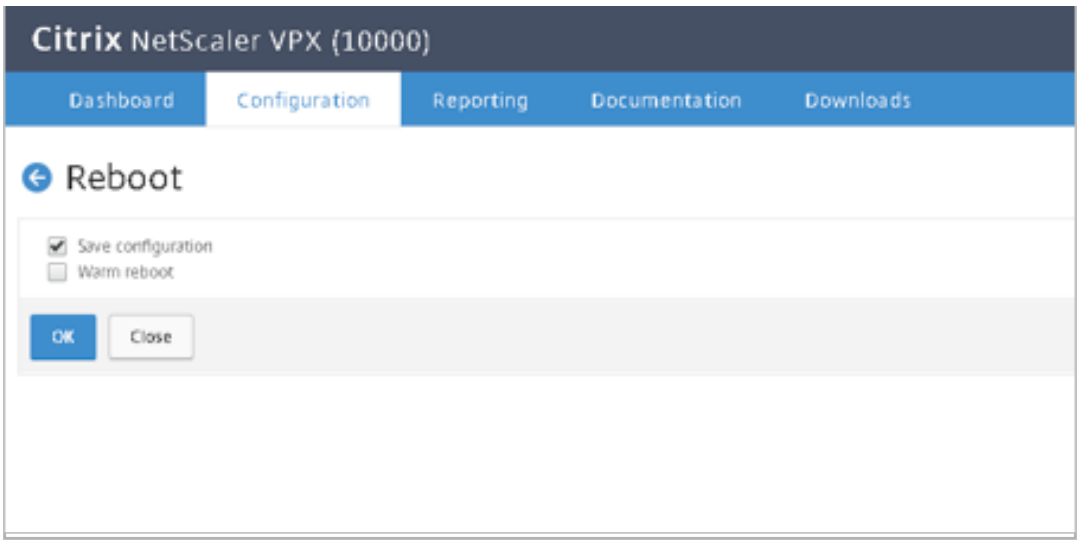
c) Klicken Sie auf der **Willkommensseite** auf **Weiter**.

d) Klicken Sie auf der Registerkarte **Konfiguration** auf **System**.

e) Klicken Sie auf der Seite **System** auf **Neu starten**.



f) Wählen Sie auf der Seite **Neustart** die Option **Warm reboot** aus, und klicken Sie auf **OK**.



Nach dem Neustart von Knoten 1 wird er zur sekundären Instanz im HA-Paar. Wenn Sie die primäre und sekundäre Instanz im HA-Paar auf Ihre ursprüngliche HA-Paarkonfiguration umstellen möchten, erzwingen Sie ein Failover. Führen Sie den folgenden Befehl für eine Instanz im HA-Paar aus:

‘‘‘

```
force ha failover
```

10. Um zu überprüfen, ob die VPX-Instanz auf die Lizenz für gepoolte Kapazität aktualisiert wurde, melden Sie sich bei den primären und sekundären Instanzen an und führen Sie die folgenden Schritte aus.

    a) Klicken Sie auf der **Willkommensseite** auf **Weiter**.

b) Navigieren Sie auf der Registerkarte Konfiguration zu **System > Lizenzen**, und klicken Sie auf **Lizenzen verwalten**. Auf der Seite **Lizenzen verwalten** können Sie die Details des Lizenzservers, der Lizenzedition und der zugewiesenen Bandbreite anzeigen.

Aktualisieren einer unbefristeten Lizenz in NetScaler ADC MPX auf NetScaler ADC-gepoolte Kapazität

February 5, 2024

Die NetScaler ADC MPX-Appliance mit unbefristeter Lizenz kann auf die NetScaler ADC Pooled Capacity Lizenz aktualisiert werden. Wenn Sie auf die NetScaler ADC Pooled-Capacity-Lizenz aktualisieren, können Sie Lizenzen aus dem Lizenzpool zu NetScaler ADC-Appliances bei Bedarf zuweisen. Sie können die NetScaler ADC Pooled-Capacity-Lizenz auch für NetScaler ADC-Instanzen konfigurieren, die im Hochverfügbarkeitsmodus konfiguriert sind. Informationen zum Konfigurieren der NetScaler ADC Pooled Capacity Lizenz für NetScaler ADC MPX-Instanzen im Hochverfügbarkeitsmodus finden Sie unter Aktualisieren der unbefristeten Lizenz im NetScaler ADC MPX-Hochverfügbarkeitspaar auf NetScaler ADC gepoolte Kapazität.

> **Hinweis**
>
> Die Konvertierung von einer unbefristeten Lizenz zu einer Lizenz mit gepoolter Kapazität ist ein einseitiger Prozess für die Lizenzberechtigung. Sie können die Lizenz für gepoolte Kapazität nicht auf unbefristet zurücksetzen.
> **Wichtig!**
>
> Für das Upgrade der Citrix ADC MPX Appliance auf die Citrix ADC Pooled Capacity Lizenz müssen Sie die MPX-Z-Lizenz auf die Appliance hochladen.

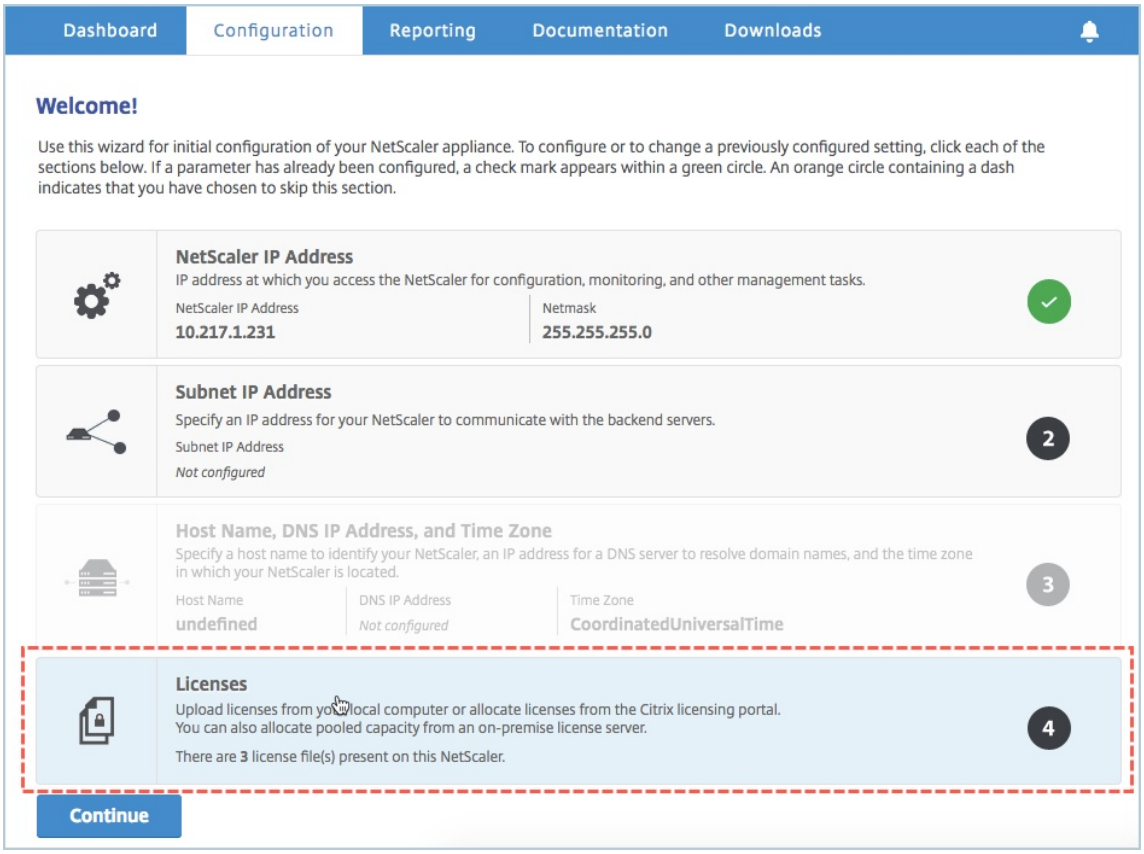
So aktualisieren Sie auf NetScaler ADC gepoolte Kapazität:

1. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler ADC Appliance ein, http://192.168.100.1z.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der **Willkommensseite** auf **Weiter**.
4. Laden Sie die Null-Kapazitätslizenz (MPX-Z-Lizenz) hoch. Navigieren Sie auf der Registerkarte Konfiguration zu **System** > **Lizenzen** .
5. Klicken Sie im Detailbereich auf **Lizenzen verwalten** und dann auf **Neue Lizenz** hinzufügen.

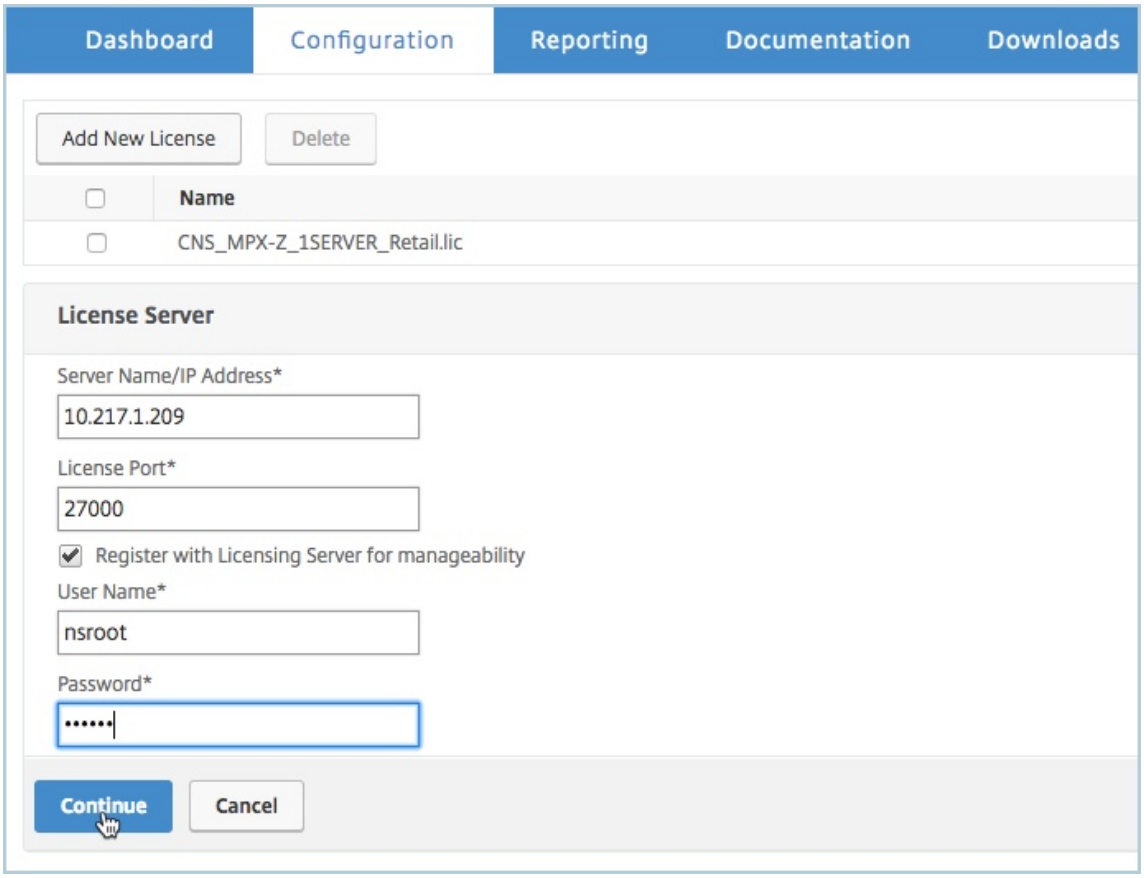
6. Wählen Sie auf der Seite **Lizenzen** die Option **Lizenzdateien hochladen** aus, und klicken Sie auf **Durchsuchen**, um die Nullkapazitätslizenz auf Ihrem lokalen Computer auszuwählen.
7. Klicken Sie nach dem Hochladen der Lizenz auf **Neu starten**, um die Appliance neu zu starten.

   > **Warnung**
   >
   > Nach der Anwendung der MPX-Z-Lizenz werden die Funktionen, einschließlich SSL-Offloading auf der Appliance, nicht lizenziert. Die Appliance beendet die Verarbeitung von HTTPS-Anforderungen.
   >
   > Wenn die Option **Nur sicheren Zugriff** auf der Appliance vor dem Upgrade aktiviert ist, können Sie mithilfe von HTTPS keine Verbindung zur Appliance über die NetScaler ADM-GUI herstellen.

8. Klicken Sie auf der Seite **Bestätigen** auf **Ja**.
9. Melden Sie sich nach dem Neustart der Appliance an.
10. Klicken Sie auf der Willkommensseite auf den Abschnitt **Lizenzen** .



11. Führen Sie im Abschnitt **Lizenzserver** die folgenden Schritte aus:



a) Geben Sie im Feld **Servername/IP-Adresse** die Details des Lizenzservers ein.

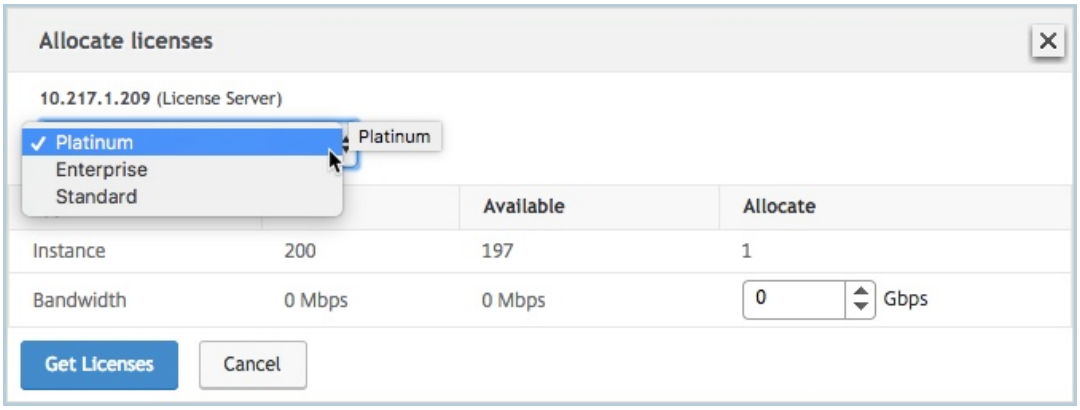
b) Geben Sie im Feld **Lizenzport** den Lizenzserver-Port ein. Standardwert: 27000.

c) Wenn Sie die Poollizenzen Ihrer Instanz über NetScaler ADM verwalten möchten, aktivieren Sie das Kontrollkästchen **Mit dem Lizenzserver für Verwaltbarkeit registrieren** und geben Sie die ADM-Anmeldeinformationen ein.

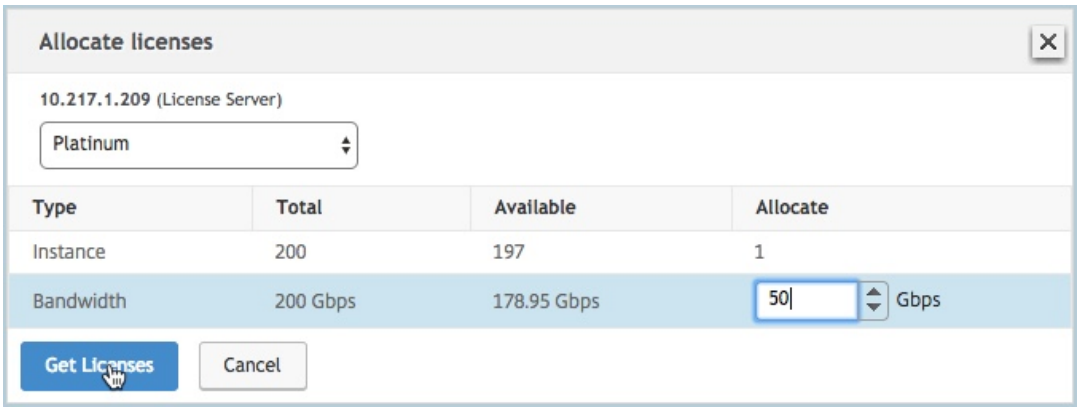
d) Klicken Sie auf **Weiter**.

12. Gehen Sie im Fenster Lizenzen zuweisen wie folgt vor:

a) Wählen Sie die Lizenzversion aus der Dropdownliste aus.



b) Weisen Sie der NetScaler ADC Appliance im Menü **Zuweisen** die Bandbreite zu, und klicken Sie auf **Lizenzen abrufen**.



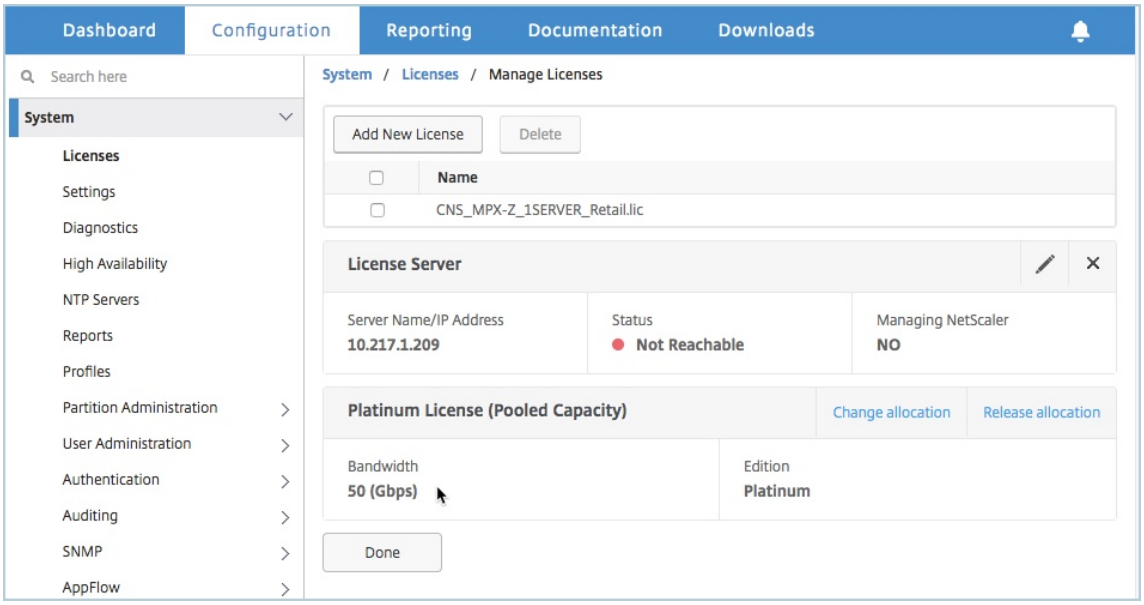
c) Wenn Sie dazu aufgefordert werden, klicken Sie auf **Neu starten**, um die Appliance neu zu starten.

13. Melden Sie sich nach dem Neustart der NetScaler ADC MPX-Appliance bei der NetScaler ADC MPX-Appliance an. Klicken Sie auf der **Willkommensseite** auf **Weiter**.

    Auf der Seite **Lizenzen** werden alle lizenzierten Funktionen aufgelistet.

14. Navigieren Sie zu **System > Lizenzen**, und klicken Sie auf **Lizenzen verwalten**.

    Auf der Seite **Lizenzen verwalten** können Sie die Details des Lizenzservers, der Lizenzedition und der zugewiesenen Bandbreite anzeigen.



Aktualisieren der unbefristeten Lizenz im NetScaler ADC MPX-Hochverfügbarkeitspaar auf NetScaler ADC-gepoolte Kapazität

Für die im Hochverfügbarkeitsmodus konfigurierten MPX-Appliances müssen Sie die gepoolte Kapazität sowohl auf der primären als auch auf der sekundären ADC-Instanz im HA-Paar konfigurieren. Weisen Sie sowohl den primären als auch den sekundären NetScaler ADC-Instanzen im HA-Paar Lizenzen mit derselben Kapazität zu. Wenn Sie beispielsweise 1 Gbit/s Kapazität von jeder Instanz im HA-Paar benötigen, müssen Sie 2 Gbit/s Kapazität aus dem gemeinsamen Pool zuweisen. Mit einer Kapazität von 2 Gbit/s können Sie den primären und sekundären NetScaler ADC-Instanzen im HA-Paar jeweils 1 Gbit/s zuweisen.

> **Wichtig!**
>
> Für ein Upgrade der NetScaler ADC MPX-Appliance auf die NetScaler ADC Pooled Capacity-Lizenz müssen Sie die MPX-Z auf die Appliance hochladen.

Voraussetzungen

Stellen Sie sicher, dass Sie die MPX-Z-Lizenz sowohl auf die primäre als auch auf die sekundäre Instanz im HA-Paar hochladen.

So laden Sie die MPX-Z-Lizenz auf die NetScaler ADC MPX-Instanzen im HA-Paar hoch:

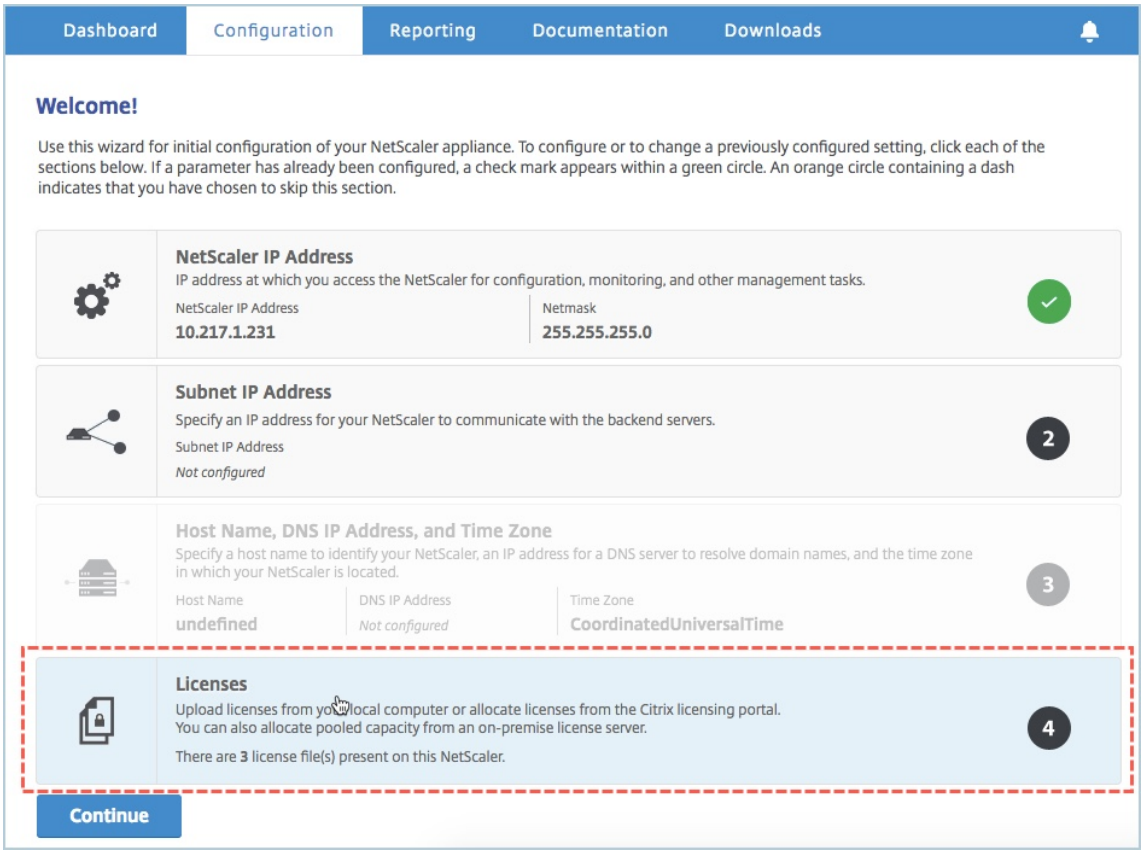
1. Geben Sie in einem Webbrowser die IP-Adresse der Appliance ein, z. http://192.168.100.1B.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.

3. Klicken Sie auf der **Willkommensseite** auf **Weiter**.
4. Laden Sie die Null-Kapazitätslizenz (MPX-Z-Lizenz) hoch. Navigieren Sie auf der Registerkarte **Configuration** zu **System > Licenses**.
5. Klicken Sie im Detailbereich auf **Lizenzen verwalten** und dann auf **Neue Lizenz hinzufügen**.
6. Wählen Sie auf der Seite **Lizenzen** die Option **Lizenzdateien hochladen** aus, und klicken Sie auf **Durchsuchen**, um die Nullkapazitätslizenz auf Ihrem lokalen Computer auszuwählen.

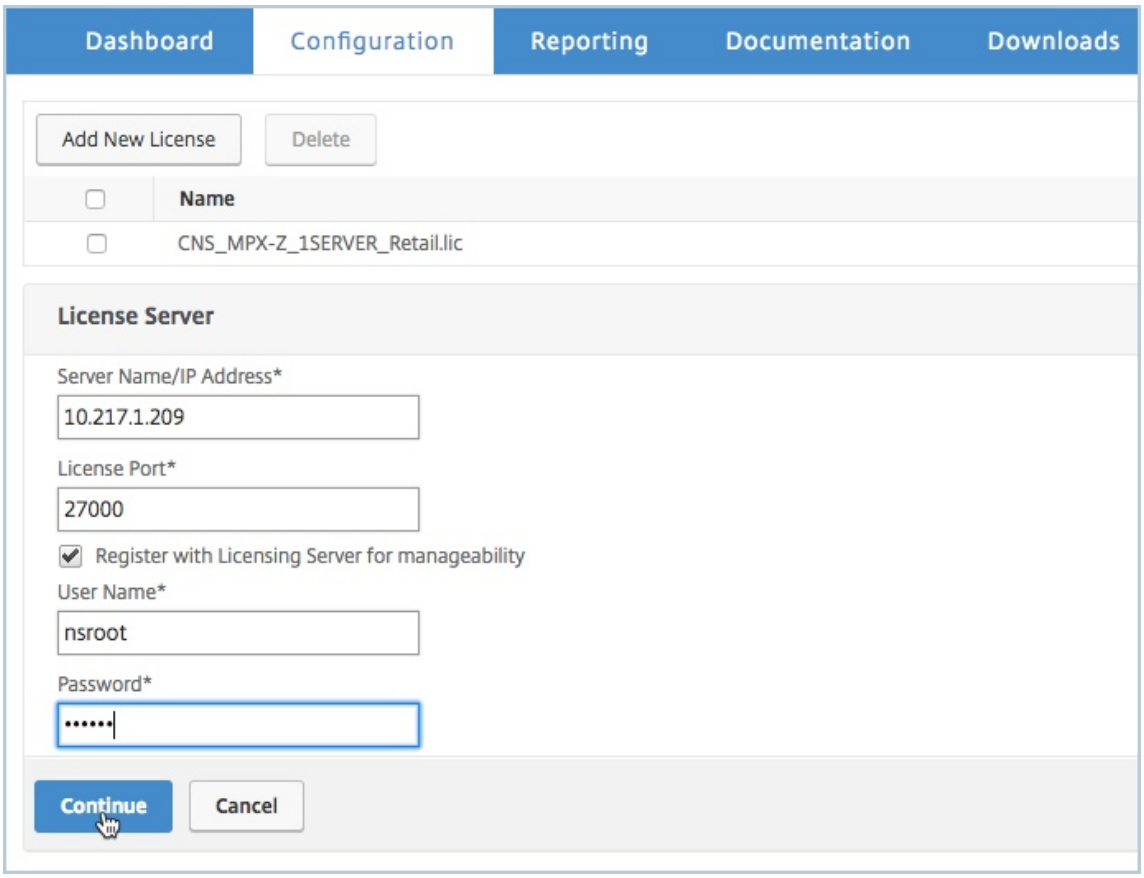
   Nach dem Hochladen der Lizenz werden Sie aufgefordert, die Appliance neu zu starten.
7. Klicken Sie auf **Neu starten**, um die Appliance neu zu starten.
8. Klicken Sie auf der Seite **Bestätigen** auf **Ja**.

So aktualisieren Sie ein vorhandenes HA-Setup auf NetScaler ADC Pooled Capacity:

1. Melden Sie sich bei der sekundären NetScaler ADC MPX-Instanz an. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler ADC Appliance ein, http://192.168.100.1z.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der **Willkommensseite** auf den Abschnitt **Lizenzen**.



4. Führen Sie im Abschnitt **Lizenzserver** die folgenden Schritte aus:



   a) Geben Sie im Feld **Servername/IP-Adresse** die Details des Lizenzservers ein.

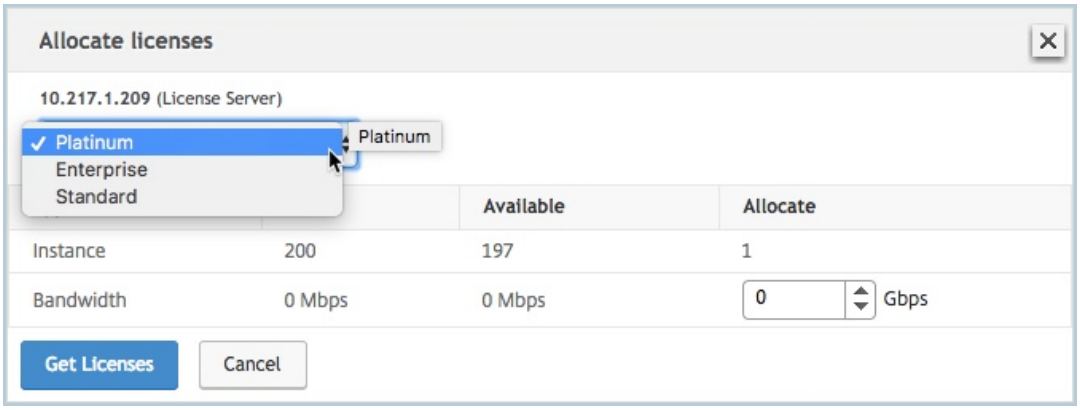
   b) Geben Sie im Feld **Lizenzport** den Lizenzserver-Port ein. Standardwert: 27000.

   c) Wenn Sie die Poollizenzen Ihrer Instanz über Citrix ADM verwalten möchten, aktivieren Sie das Kontrollkästchen **Registrieren bei Lizenzierungsserver für Verwaltbarkeit**, und geben Sie ADM-Anmeldeinformationen ein.

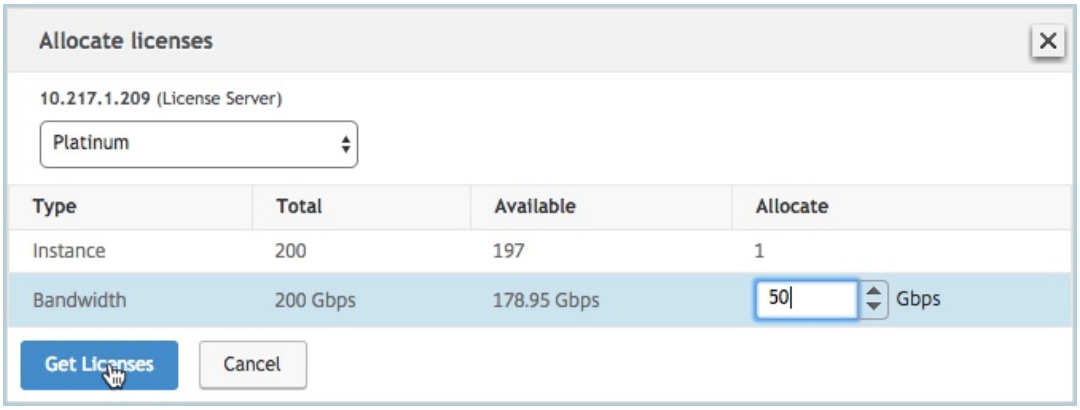
   d) Klicken Sie auf **Weiter**.

5. Gehen Sie im Fenster **Lizenzen zuweisen** wie folgt vor:

   a) Wählen Sie die Lizenzversion aus der Dropdownliste aus.



b) Weisen Sie der NetScaler ADC Appliance im Menü **Zuweisen** die Bandbreite zu, und klicken Sie auf **Lizenzen abrufen**.



c) Wenn Sie dazu aufgefordert werden, klicken Sie auf **Neustart**, um die Appliance Nachdem die Appliance mit der neuen Lizenz in Betrieb genommen wurde, erzwingen Sie ein Failover, indem Sie eingeben `force ha failover`. Dieses Failover stellt sicher, dass das HA-Paar in gutem Zustand ist.

6. Melden Sie sich bei der vorhandenen primären NetScaler ADC MPX Appliance an und starten Sie die Appliance neu. Führen Sie folgende Schritte aus:

   a) Geben Sie in einem Webbrowser die IP-Adresse der NetScaler ADC Appliance ein, http://192.168.100.1z.

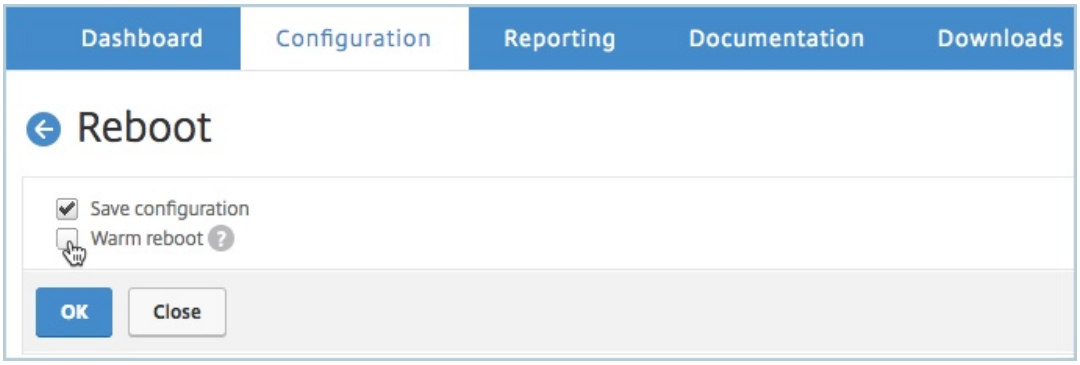
   b) Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.

   c) Klicken Sie auf der **Willkommensseite** auf **Weiter**.

   d) Klicken Sie auf der Registerkarte **Konfiguration** auf **System**.

   e) Klicken Sie auf der Seite **System** auf **Neu starten**.

   f) Wählen Sie auf der Seite **Neustart** die Option **Warm reboot** aus, und klicken Sie auf **OK**.



Nachdem die primäre NetScaler ADC MPX-Appliance neu gestartet wurde, wird sie zur sekundären NetScaler ADC MPX-Appliance im HA-Paar. Wenn Sie die primäre und sekundäre Instanz im HA-Paar auf Ihre ursprüngliche HA-Paarkonfiguration umstellen möchten, erzwingen Sie ein Failover. Führen Sie den folgenden Befehl für eine Instanz im HA-Paar aus:

```
> force ha failover
<!--NeedCopy-->
```

Upgrade einer unbefristeten Lizenz in einem NetScaler ADC SDX auf gepoolte Kapazität von NetScaler ADC

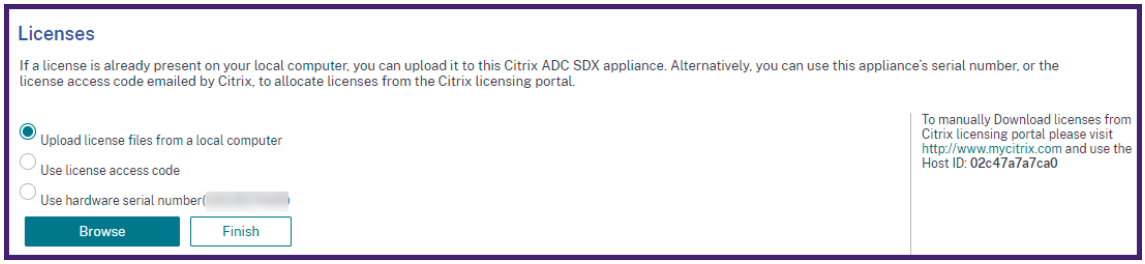
February 5, 2024

Eine NetScaler ADC SDX-Appliance mit unbefristeter Lizenz kann auf die NetScaler ADC Pooled Capacity-Lizenz aktualisiert werden. Wenn Sie auf die NetScaler ADC Pooled-Capacity-Lizenz aktualisieren, können Sie Lizenzen aus dem Lizenzpool zu NetScaler ADC-Appliances bei Bedarf zuweisen. Sie können auch die ADC Pooled Capacity-Lizenz für NetScaler ADC-Instanzen konfigurieren, die im Hochverfügbarkeitsmodus konfiguriert sind.

> **Hinweis**
>
> Die Umwandlung von einer unbefristeten Lizenz auf eine gebündelte Kapazitätslizenz ist ein unidirekter Lizenzanspruchsprozess. Sie können die gepoolte Kapazitätslizenz nicht auf unbefristet zurücksetzen.
> **Wichtig!**
>
> - Für das Upgrade der SDX-Appliance auf NetScaler ADC Pooled Capacity-Lizenz müssen Sie die SDX-Z-Lizenz auf die Appliance hochladen.
> - Stellen Sie sicher, dass Sie die Berechtigung haben, ADC-Instanzen in ADM hinzuzufügen.

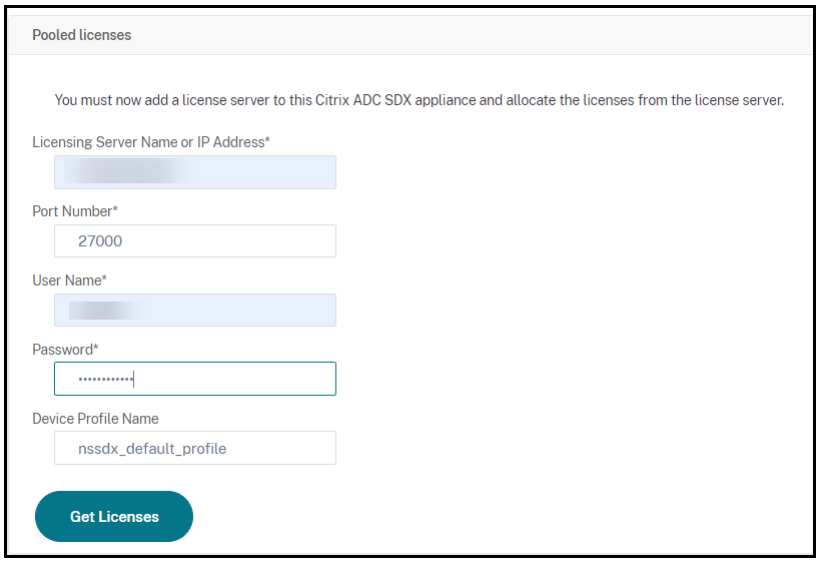
So aktualisieren Sie auf NetScaler ADC gepoolte Kapazität:

1. Geben Sie in einem Webbrowser die IP-Adresse der SDX-Appliance ein, z. B. http://192.168.100.1
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der **Willkommensseite** auf **Weiter**.
4. Laden Sie die Lizenz ohne Kapazität hoch. Navigieren Sie auf der Registerkarte Konfiguration zu **System** > **Lizenzen** .
5. Klicken Sie auf der Seite **Lizenzen verwalten** auf **Lizenzdatei hinzufügen**.
6. Wählen Sie auf der Seite **Lizenzen** die Option **Lizenzdateien von einem lokalen Computer hochladen aus**, und klicken Sie auf **Durchsuchen**, um die Lizenz mit Nullkapazität auf Ihrem lokalen Computer auszuwählen. Klicken Sie dann auf **Finish**.



Sobald die Lizenz mit Nullkapazität erfolgreich angewendet wurde, wird der Abschnitt **Pooled Licenses** auf der Seite **Lizenzen** angezeigt.

7. Führen Sie im Abschnitt **Pooled Lizenzen** die folgenden Schritte aus:



a) Geben Sie im Feld **Lizenzservername oder IP-Adresse** die Details des Lizenzservers ein.

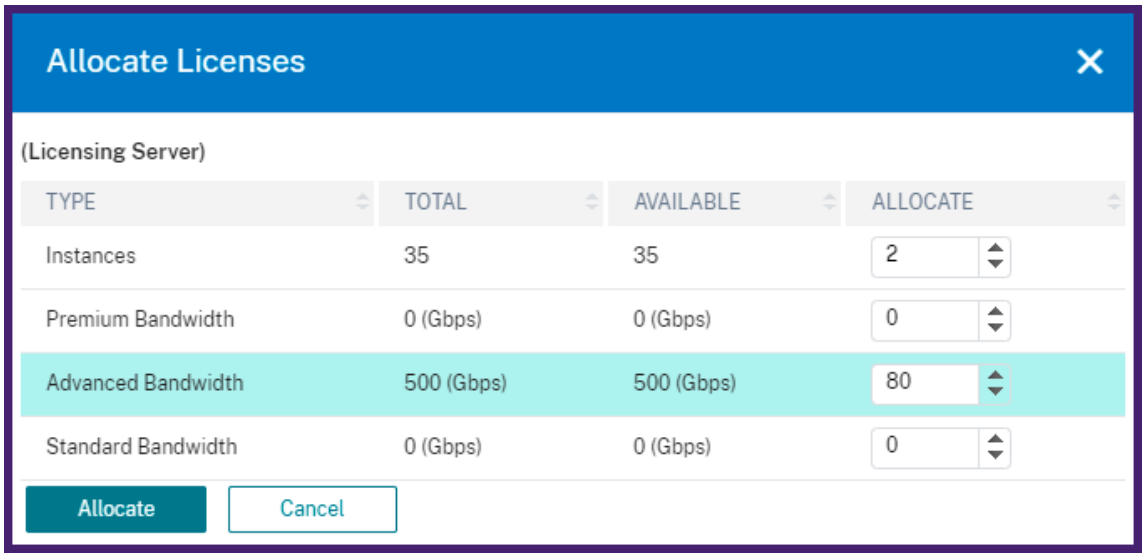
Wenn Sie den ADM-Server als Lizenzserver konfigurieren möchten, geben Sie die IP-Adresse des ADM-Servers an.

Wenn Sie einen Agenten für die Kommunikation mit dem ADM-Server verwenden, geben Sie die IP-Adresse des ADM-Agenten an.

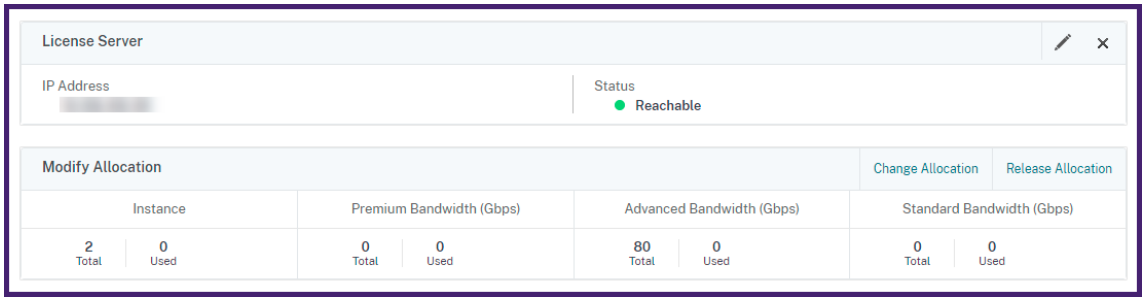
b) Geben Sie im Feld **Portnummer** den Lizenzserverport ein. Standardwert: 27000.

c) Klicken Sie auf **Get Licenses**.

8. Geben Sie im Fenster **Lizenzen zuweisen** die erforderlichen Instanzen und Bandbreite an, und klicken Sie auf **Zuweisen**.



Auf der Seite **Lizenzen verwalten** können Sie die Details des Lizenzservers, der Lizenz-Edition sowie der zugewiesenen Instanz und der Bandbreite aus dem Pool anzeigen.



> **Hinweis**
>
> Das Upgrade einer unbefristeten Lizenz auf gepoolte Kapazität erfordert keinen Neustart der SDX-Appliance.

NetScaler ADC Kapazität auf NetScaler ADC Instanzen im Clustermodus

February 5, 2024

Sie können die gepoolte NetScaler ADC Kapazität in den NetScaler ADC-Instanzen konfigurieren, die als Cluster konfiguriert sind. Die folgenden Voraussetzungen sind für die Konfiguration der gepoolten Kapazität auf NetScaler ADC Instanzen im Clustermodus erforderlich:

- Instanzen werden einzeln in einem Lizenzmodus mit gepoolter Kapazität ausgeführt, um den Cluster zu bilden.
- Alle Instanzen müssen mit derselben Bandbreite ausgeführt werden.
- Alle Instanzen haben die gepoolte Kapazität aus demselben NetScaler Application Delivery Management (ADM) ausgecheckt.
- Neue Instanzen können einem vorhandenen NetScaler ADC Cluster nicht hinzugefügt werden, es sei denn, ihre Kapazität und die NetScaler ADM Konfigurationen entsprechen denen der vorhandenen Instanzen im Cluster.

Jedes Kapazitätsauschecken aus dem NetScaler ADC Cluster weist allen Clusterknoten die gleiche Kapazität zu und das Auschecken Bandbreite = bereitgestellte Bandbreite * Anzahl von Knoten zu.

Wenn Sie beispielsweise 50 Mbit/s Bandbreite vom NetScaler ADC Cluster auschecken und der Cluster 12 Instanzen enthält, erhält jede Instanz automatisch 50 Mbit/s. Und 600 Mbit/s werden aus dem Pool ausgecheckt.

> **Hinweis**
>
> Wenn eine oder mehrere Instances im Cluster nicht mehr reagieren, verarbeitet der Cluster den Datenverkehr mit der Kapazität der verbleibenden Instances weiter.

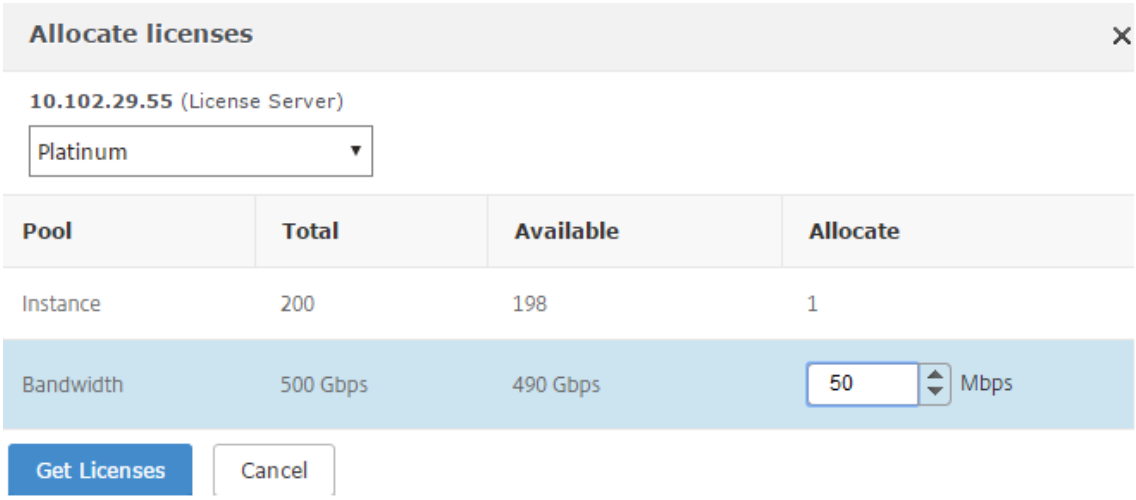
Ordnen Sie einem ADC-Cluster ADC-Poolkapazität zu

Weisen Sie jedem Clusterknoten Lizenzen separat zu. Weil die Befehle zur Weitergabe und Synchronisierung von Lizenzen zwischen den Clusterknoten deaktiviert sind.

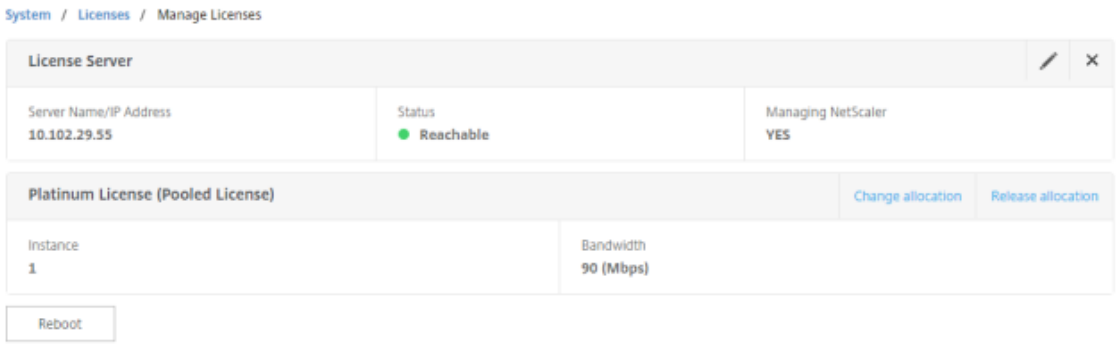
Wiederholen Sie das folgende Verfahren auf jedem Clusterknoten:

1. Geben Sie in einem Webbrowser die Citrix ADC IP-Adresse (NSIP) ein. Beispiel: `http://192.168.100.1`.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System > Lizenzen > Lizenzen verwalten**, klicken Sie auf **Neue Lizenz hinzufügen** und wählen **Sie Pooled Licensing**aus.
4. Geben Sie den Namen oder die Adresse des Lizenzservers in das Feld **Servername/IP-Adresse** ein.

5. Wenn Sie die Poollizenzen Ihrer Instanz über Citrix ADM verwalten möchten, aktivieren Sie das Kontrollkästchen **Registrieren bei Citrix ADM für Verwaltbarkeit**, und geben Sie die ADM-Anmeldeinformationen ein.
6. Wählen Sie die Lizenzedition und die erforderliche Bandbreite aus, und klicken Sie auf **Lizenzen abrufen**.

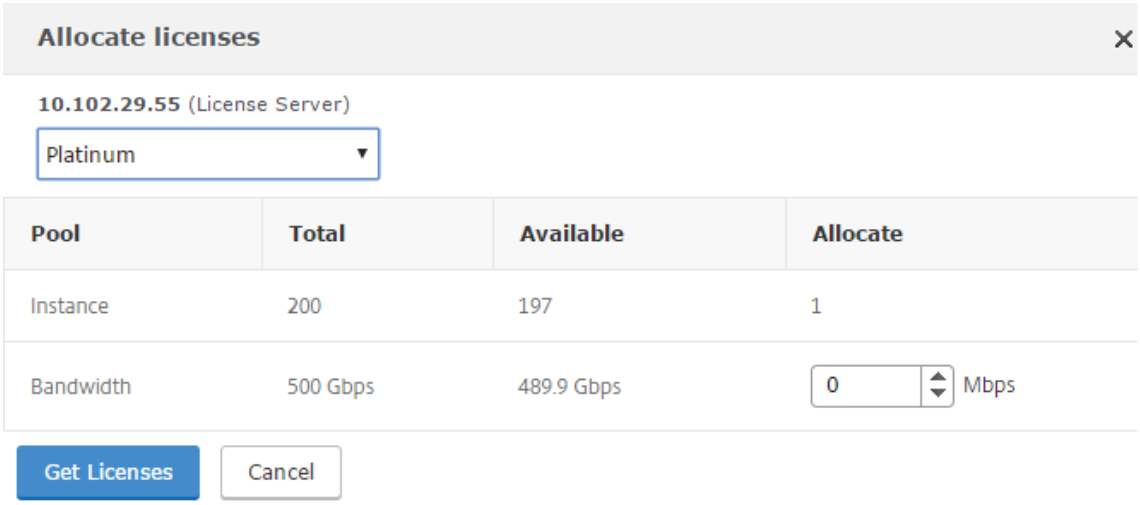


7. Sie können die Lizenzzuweisung ändern oder freigeben, indem Sie **Zuordnung ändern oder Zuordnungfreigeben**wählen.



8. Wenn Sie auf **Zuweisung ändern**klicken, werden in einem Popup-Fenster die auf dem Lizenzserver verfügbaren Lizenzen angezeigt.

> **Hinweis**
>
> Die Bandbreitenzuweisung muss ein integrales Vielfaches der minimalen Bandbreiteneinheit des entsprechenden Formfaktors sein.



9. Sie können der NetScaler ADC Instanz Bandbreite oder Instanzen über die Dropdownliste **Zuweisen zuweisen**. Klicken Sie dann auf **Lizenzen holen**.
10. Sie können die Lizenzversion und die erforderliche Bandbreite aus den Dropdownlisten im Popup-Fenster auswählen.

> **Hinweis**
>
> Ein Neustart ist nicht erforderlich, wenn Sie die Bandbreitenzuweisung ändern, aber ein warmer Neustart ist erforderlich, wenn Sie die Lizenzversion ändern.

Weisen Sie einem ADC-Cluster mithilfe der CLI gepoolte ADC-Kapazität zu

Weisen Sie jedem Clusterknoten Lizenzen separat zu. Weil die Befehle zur Weitergabe und Synchronisierung von Lizenzen zwischen den Clusterknoten deaktiviert sind.

Wiederholen Sie das folgende Verfahren auf jedem Clusterknoten:

1. Geben Sie in einem SSH-Client die Citrix ADC IP-Adresse (NSIP) ein, und melden Sie sich mit Administratoranmeldeinformationen an.
2. Geben Sie den folgenden Befehl ein, um einen Lizenzserver hinzuzufügen:

```
1 add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
     port number >]
2 <!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. Geben Sie den folgenden Befehl ein, um die verfügbaren Lizenzen auf dem Lizenzserver anzuzeigen:


```
sh licenseserverpool
<!--NeedCopy-->
```

```
> sh licenseserverpool
        Instance Total                  : 0
        Instance Available              : 0
        Standard Bandwidth Total        : 0 Mbps
        Standard Bandwidth Availabe     : 0 Mbps
        Enterprise Bandwidth Total      : 0 Mbps
        Enterprise Bandwidth Available  : 0 Mbps
        Platinum Bandwidth Total        : 0 Mbps
        Platinum Bandwidth Available    : 0 Mbps
        VPX25S Total                    : 1
        VPX25S Available                : 1
        VPX200E Total                   : 1
        VPX200E Available               : 1
        VPX1000S Total                  : 1
        VPX1000S Available              : 1
        VPX8000E Total                  : 2
        VPX8000E Available              : 1
 Done
```

4. Geben Sie den folgenden Befehl ein, um der NetScaler ADC VPX Appliance eine Lizenz zuzuweisen:

```
set capacity  –platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

Systemüberwachung

February 5, 2024

Der Lizenzserver überwacht kontinuierlich den Zustand der Citrix ADC Instanz mit aktivierter Kapazität. Die Instanzen kommunizieren über regelmäßige Nachrichten mit dem Lizenzserver. Wenn nur wenige aufeinanderfolgende Nachrichten nicht empfangen werden, meldet der Lizenzserver, dass die Verbindung unterbrochen wurde.

Sie können benutzerdefinierte Benachrichtigungen erstellen, um die Standardalarme zu ergänzen.

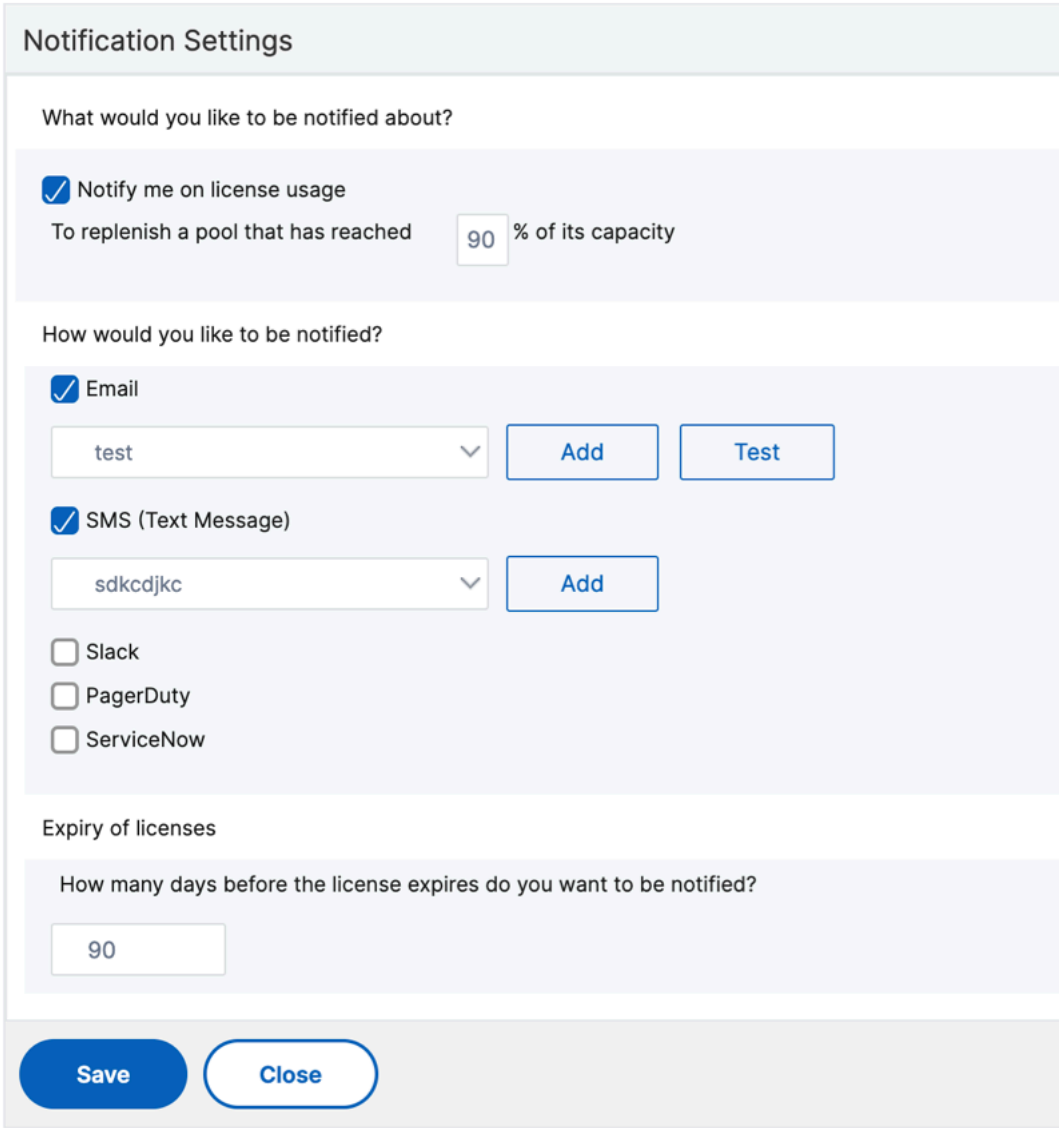
Gnadenfrist

Wenn sich eine Citrix ADC Instanz mit aktivierter Kapazität in einem fehlerfreien Zustand befindet und der Lizenzserver nicht mehr reagiert, arbeitet die Instanz 30 Tage lang mit der aktuellen Kapazität.

Wenn die Konnektivität zum Lizenzserver nach 30 Tagen nicht wiederhergestellt wird, verliert die Instanz ihre Kapazität und beendet die Verarbeitung des Datenverkehrs.

Benachrichtigungen und Alarme

Benachrichtigungen können über Citrix Application Delivery Management (ADM) für jede Aktion aktiviert werden, die auf der Instanz ausgeführt wird. Abgesehen von den benutzerdefinierten Benachrichtigungseinstellungen sind einige Alarme standardmäßig konfiguriert. Beispiel: Um einen Alarm zum Auffüllen eines Pools zu konfigurieren, der einen bestimmten Prozentsatz seiner Kapazität ausgeschöpft hat, navigieren Sie zu **Infrastruktur** > **Lizenz** > **Einstellungen** > **Benachrichtigungseinstellungen** und klicken auf die Schaltfläche Bearbeiten.



Erwartete Verhaltensweisen, wenn Probleme auftreten

February 5, 2024

Im Folgenden werden die erwarteten Verhaltensweisen der Lizenzserver und Citrix ADC Instanzen aufgeführt, wenn die beschriebenen Probleme auftreten:

Der Lizenzserver reagiert nicht mehr

> **Warnung**
>
> Der Lizenzserver antwortet nicht. NetScaler ADC arbeitet 30 Tage lang mit der aktuellen Kapazität. Wenn nach 30 Tagen die Konnektivität zum Lizenzserver nicht wiederhergestellt wird, verliert der NetScaler ADC seine aktuelle Kapazität und stoppt die Verarbeitung des Datenverkehrs.

Wenn der Lizenzserver nicht mehr reagiert, gibt die NetScaler ADC Instanz den Grace Period ein, bis die Konnektivität wiederhergestellt wird.

Citrix ADC Instanz mit aktivierter Kapazität reagiert nicht mehr

Wenn die NetScaler ADC Instanz mit aktivierter Kapazität nicht mehr reagiert und sich der Lizenzserver in einem fehlerfreien Zustand befindet, überprüft der Lizenzserver alle Lizenzen der NetScaler ADC Instanz nach 10 Minuten. Wenn die Instanz neu gestartet wird, sendet sie eine Aufforderung, alle Lizenzen vom Lizenzserver auszuchecken.

Sowohl der Lizenzserver als auch die NetScaler ADC Instanz mit aktivierter Kapazität reagieren nicht mehr

Wenn sowohl der Lizenzserver als auch die NetScaler ADC Pool-Kapazitäts-aktivierte Instanz die Verbindung neu startet und neu aufbaut, checkt der Lizenzserver nach 10 Minuten alle seine Lizenzen ein, und die NetScaler ADC gepoolte Kapazität aktivierten Instanzen checken die Lizenzen nach Abschluss des Neustarts automatisch aus.

Die NetScaler ADC Instanz mit aktivierter Kapazität wird ordnungsgemäß heruntergefahren

Während eines ordnungsgemäßen Herunterfahrens können Sie die Lizenzen einchecken oder die Lizenzen beibehalten, die vor dem ordnungsgemäßen Herunterfahren zugewiesen wurden. Wenn Sie sich dafür entscheiden, die Lizenzen einzuchecken, ist die NetScaler ADC Pool-Kapazitäts-fähige

Instanz nach dem Neustart nicht lizenziert. Wenn Sie die Lizenzen beibehalten möchten, werden sie beim Herunterfahren der Instanz beim Lizenzierungsserver eingecheckt. Nach dem Neustart der Instanz stellt sie die Verbindung mit dem Lizenzserver wieder her und checkt die Lizenzen wie in der gespeicherten Konfiguration angegeben aus.

Wenn das System neu gestartet wird und der Checkout aufgrund der im Pool verfügbaren Kapazität fehlschlägt, überprüft der NetScaler ADC den Bestand an NetScaler Application Delivery Management (ADM) -Pool Lizenzen und überprüft alle verfügbaren Kapazitäten. Ein SNMP-Alarm wird ausgelöst, um diesen Zustand dem Benutzer mitzuteilen, wenn der NetScaler ADC nicht mit voller Kapazität gemäß der Konfiguration ausgeführt wird. Wenn im Bandbreiten-Pool keine Kapazität verfügbar ist, wird die Instanz mit Poolkapazität nicht lizenziert.

Netzwerk verliert Konnektivität

> **Fehlermeldung (Syslog)**
>
> Der Lizenzserver reagiert nicht.

Wenn der Lizenzserver und die für die NetScaler ADC-Poolkapazität aktivierten Instanzen in fehlerfreiem Zustand sind, die Netzwerkkonnektivität jedoch verloren geht, arbeiten die Instanzen 30 Tage lang weiterhin mit ihrer aktuellen Kapazität. Wenn die Konnektivität zum Lizenzserver nach 30 Tagen nicht wiederhergestellt wird, verlieren die Instanzen ihre Kapazität und beenden die Verarbeitung des Datenverkehrs, und der Lizenzserver checkt alle Lizenzen ein. Nachdem der Lizenzserver die Verbindung mit den Citrix ADC Instanzen wiederhergestellt hat, checken die Instanzen die Lizenzen erneut aus.

Ablaufprüfungen für gepoolte Kapazitätslizenzen konfigurieren

February 5, 2024

Sie können jetzt den Grenzwert für den Lizenzablauf für gepoolte NetScaler ADC-Kapazitätslizenzen konfigurieren. Durch Festlegen von Schwellenwerten sendet Citrix Application Delivery Management (ADM) Benachrichtigungen per E-Mail oder SMS, wenn eine Lizenz abläuft. Ein SNMP-Trap und eine Benachrichtigung werden ebenfalls gesendet, wenn die Lizenz auf NetScaler ADM abgelaufen ist.

Ein Ereignis wird generiert, wenn eine Benachrichtigung über den Ablauf der Lizenz gesendet wird und dieses Ereignis in NetScaler ADM angezeigt werden kann.

So konfigurieren Sie Lizenzablaufprüfungen:

1. Navigieren Sie zu**Netzwerke** >**Lizenzen**.

2. Auf der Seite mit den **Lizenzeinstellungenfinden Sie im Abschnitt Informationen zum Ablauf**der Lizenz die Details der Lizenzen, die ablaufen werden:

    - **Feature**: Art der Lizenz, die ablaufen wird.
    - **Anzahl**: Anzahl der virtuellen Server oder Instanzen, die betroffen sein werden.
    - **Tage bis zum Ablauf**: Anzahl der Tage vor Ablauf der Lizenz.

3. Klicken Sie im Abschnitt**Benachrichtigungseinstellungen**auf das Symbol **Bearbeiten**, und geben Sie den Warnschwellenwert an. Sie können einen Prozentsatz der Kapazität der gepoolten Lizenzen festlegen, der zur Benachrichtigung von Administratoren verwendet werden soll.
4. Wählen Sie die Art der Benachrichtigung aus, die Sie senden möchten, indem Sie das entsprechende Kontrollkästchen aktivieren. Die Benachrichtigungstypen sind wie folgt:

    a) **E-Mail-Profil**: Geben Sie einen Mailserver und Profildetails an. Eine E-Mail wird ausgelöst, wenn Ihre Lizenzen bald ablaufen.

    b) **SMS-Profil**: Geben Sie einen Short Message Service (SMS) -Server und Profildetails an. Eine SMS-Nachricht wird ausgelöst, wenn Ihre Lizenzen ablaufen.

5. Geben Sie dann an, wann Sie die Benachrichtigung in Bezug auf die Anzahl der Tage vor Ablauf der Lizenz senden möchten.
6. Klicken Sie auf **Speichern**.

> **Hinweis**
>
> Wenn Sie dem Pool neue Lizenzen hinzufügen, verwenden die NetScaler ADC Instanzen die neuen Lizenzen nach Ablauf der vorhandenen Lizenzen.

Einchecken und Auschecken von NetScaler ADC VPX- und BLX-Lizenzen

February 5, 2024

Sie können VPX- und BLX-Lizenzen bei Bedarf von NetScaler Application Delivery Management (ADM) zu NetScaler ADC-Instanzen zuweisen. Die ADM-Software speichert und verwaltet die Lizenzen, die über ein Lizenzierungsframework verfügen, das skalierbare und automatisierte Lizenzbereitstellung ermöglicht. Eine Instanz kann die Lizenz von NetScaler ADM auschecken, wenn sie bereitgestellt wird. Wenn eine Instanz entfernt oder zerstört wird, überprüft die Instanz ihre Lizenz an die NetScaler ADM -Software zurück.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Sie verwenden ein Citrix ADC VPX Image mit Software Version 12.0.
  Zum Beispiel: nsvpx-ESX-12.0-xx.xx_NC.zip
- Sie haben Citrix ADM mit Version 12.0 installiert.
  Zum Beispiel: MAS-ESX-12.0-xx.xx.zip

> **Hinweis**
>
> Um vorhandene VPX-Lizenzen von Citrix ADM zu verwalten, müssen Sie die Lizenzen erneut in Citrix ADM hosten.

Installieren von Lizenzen in Citrix ADM

> **Hinweis: Starten Sie**
>
> vor der Installation von Lizenzen die virtuelle Citrix ADM Appliance neu, wenn Sie die Software-Edition oder Bandbreite geändert haben.

So installieren Sie Lizenzdateien auf NetScaler ADM:

1. Geben Sie in einem Webbrowser die IP-Adresse des NetScaler ADM ein (z. B. http://192.168.100.1).
2. Geben Sie unter Benutzername und Kennwort die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **Netzwerke** > **Lizenzen**.
4. Wählen Sie im Abschnitt **Lizenzdateien** eine der folgenden Optionen aus:

   - **Upload von Lizenzdateien von einem lokalen Computer** : Wenn eine Lizenzdatei bereits auf dem lokalen Computer vorhanden ist, können Sie sie in NetScaler ADM hochladen. Um Lizenzdateien hinzuzufügen, klicken Sie auf **Durchsuchen** und wählen Sie die Lizenzdatei (.lic) aus, die Sie hinzufügen möchten. Dann klick **Fertig stellen**.
   - **Lizenzzugangscode verwenden** - Citrix mailt den Lizenzzugangscode für die Lizenzen, die Sie erwerben.
     Um Lizenzdateien hinzuzufügen, geben Sie den Lizenzzugangscode in das Textfeld ein und klicken Sie dann auf **Lizenzen** abrufen .

     > **Hinweis**
     >
     > Stellen Sie sicher, dass Sie mit dem Internet verbunden sind, bevor Sie den Lizenzzugangscode für die Installation der Lizenzen verwenden.

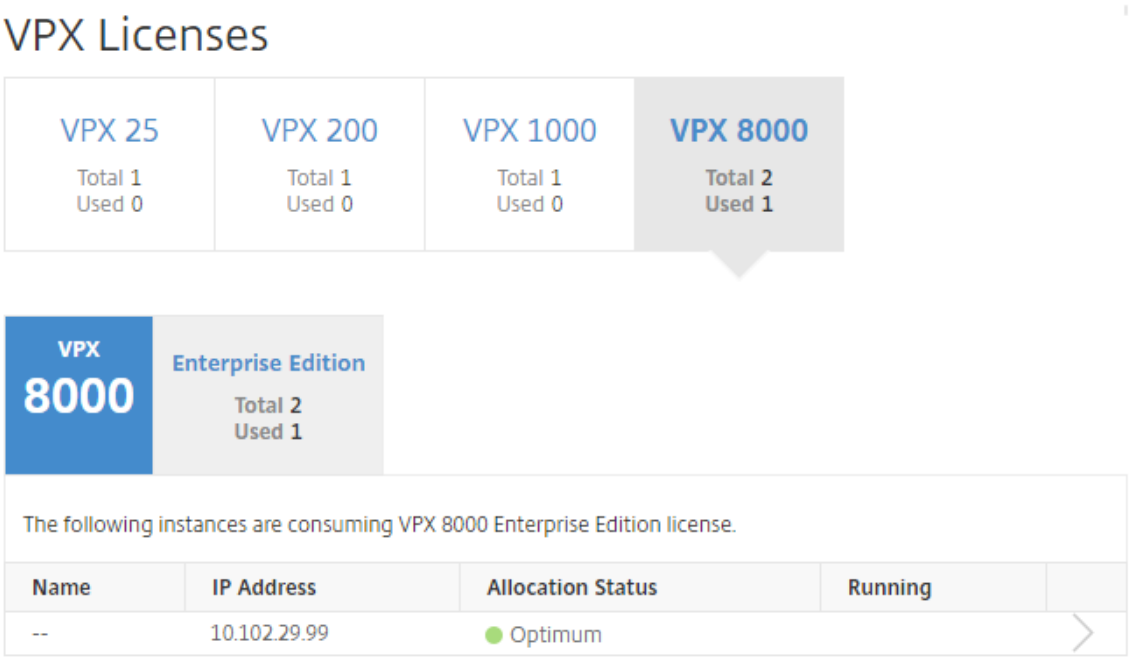
Sie können dem NetScaler ADM jederzeit über die Lizenzeinstellungen weitere Lizenzen hinzufügen.

Verifizierung

Sie können die verfügbaren und zugewiesenen Lizenzen in der Citrix ADM GUI anzeigen.

Um die Lizenzen anzuzeigen:

1. Geben Sie in einem Webbrowser die IP-Adresse von NetScaler ADM ein (z. B.http://192.168.100.1).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte Konfiguration zu **Netzwerke**> **Lizenzen** > **VPX-Lizenzen.**

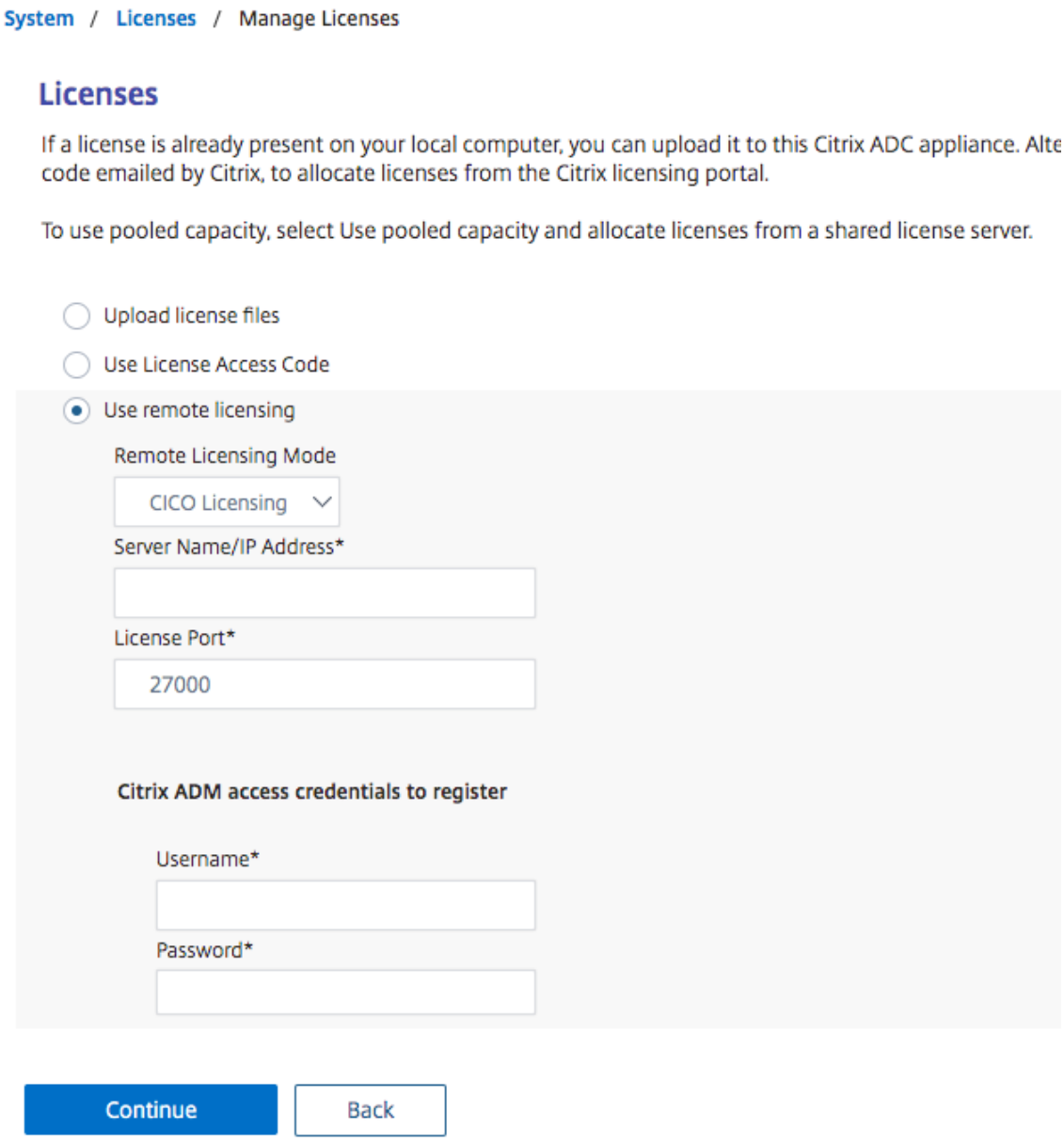


4. Sie können die zugewiesenen Lizenzen in der Tabelle im Abschnitt Verfügbare Lizenzen anzeigen.

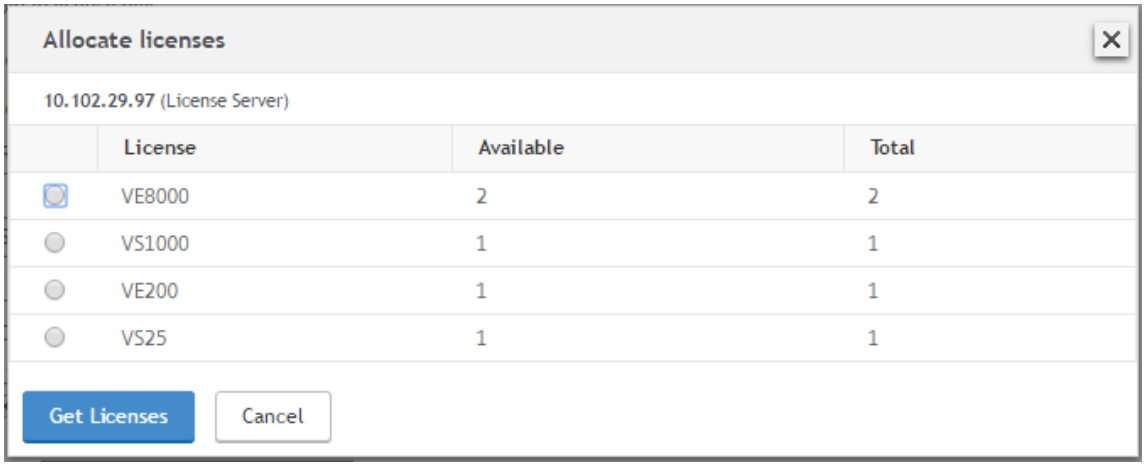
Zuweisen von VPX- und BLX-Lizenzen zu einer ADC-Instanz mithilfe der NetScaler ADC GUI

1. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler ADC Instanz ein (z. B. http://192.168.100.1).
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.

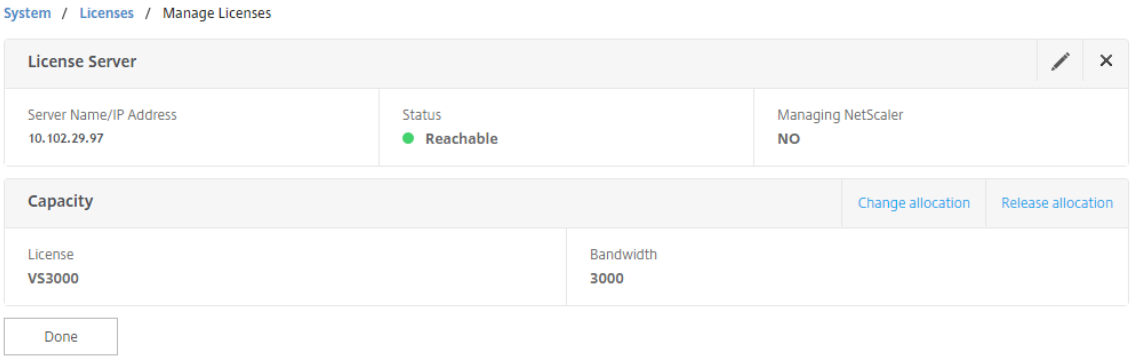
3. Navigieren Sie auf der Registerkarte Konfiguration zu **System > Lizenzen > Lizenzen verwalten**, klicken Sie auf **Neue Lizenz hinzufügen**und wählen Sie **Remotelizenzierung verwenden > CICO-Lizenzierung**.
4. Geben Sie die Details des Lizenzservers in das Feld **Servername/IP-Adresse** ein.
5. Geben Sie im obigen Bildschirm in den Feldern **Benutzername** und **Kennwort** Citrix ADM Anmeldeinformationen ein, und klicken Sie auf **Weiter**.



6. Wählen Sie die Lizenzedition mit der erforderlichen Bandbreite aus, und klicken Sie auf **Lizenzen abrufen**.



7. Klicken Sie auf **Neustart**, Ihre NetScaler ADC-Instanz wird neu gestartet.
8. Sie können die Lizenzzuweisung ändern oder freigeben, indem Sie zu **System** > **Lizenzen > Lizenzenverwalten**navigieren und**Zuordnung ändern**oder**Freigabezuweisung auswählen.**



9. Wenn Sie auf **Zuweisung ändern**klicken, werden in einem Popup-Fenster die auf dem Lizenzserver verfügbaren Lizenzen angezeigt. Wählen Sie die erforderliche Lizenz aus, klicken Sie auf **Lizenzen abrufen**.

Zuweisen von VPX- und BLX-Lizenzen zu einer ADC-Instanz mithilfe der NetScaler ADC CLI

1. Geben Sie in einem SSH-Client die IP-Adresse der NetScaler ADC-Instanz ein, und melden Sie sich mit Administratoranmeldeinformationen an.
2. Geben Sie den folgenden Befehl ein, um einen Lizenzserver hinzuzufügen:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
   port number >]
<!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. Geben Sie den folgenden Befehl ein, um die verfügbaren Lizenzen auf dem Lizenzserver anzuzeigen:

```
sh licenseserverpool
<!--NeedCopy-->
```

```
> sh licenseserverpool
        Instance Total                  : 0
        Instance Available              : 0
        Standard Bandwidth Total        : 0 Mbps
        Standard Bandwidth Availabe     : 0 Mbps
        Enterprise Bandwidth Total      : 0 Mbps
        Enterprise Bandwidth Available  : 0 Mbps
        Platinum Bandwidth Total        : 0 Mbps
        Platinum Bandwidth Available    : 0 Mbps
        VPX25S Total                    : 1
        VPX25S Available                : 1
        VPX200E Total                   : 1
        VPX200E Available               : 1
        VPX1000S Total                  : 1
        VPX1000S Available              : 1
        VPX8000E Total                  : 2
        VPX8000E Available              : 1
 Done
```

4. Um der NetScaler ADC Appliance eine Lizenz zuzuweisen, geben Sie den folgenden Befehl ein:

```
set capacity  –platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

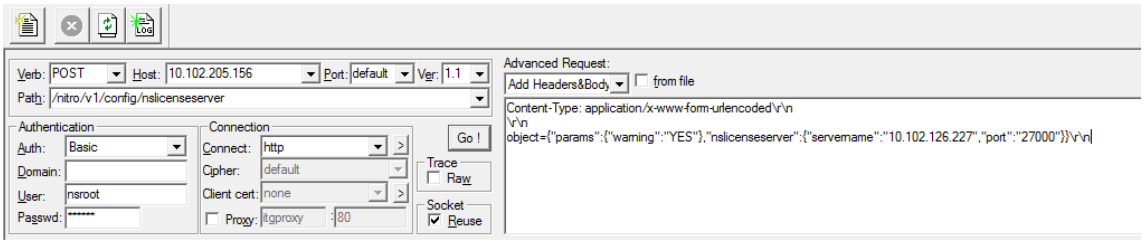
Weisen Sie VPX- und BLX-Lizenzen mithilfe der API einer ADC-Instanz zu

Melden Sie sich in einem Webbrowser oder einem API-Client mit den Administratoranmeldeinformationen bei der NetScaler ADC-Instanz an.

So fügen Sie einen Lizenzserver hinzu:

1. Legen Sie den Anforderungstyp auf **Post**fest.
2. Legen Sie den Pfad zu /nitro/v1/config/nslicensingserver fest.
3. Legen Sie die Nutzlast wie folgt fest:

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
object= {
  " params " ;{
 warning " : " yes "  }
 , " nslicensing server " ;{
 servername " : " <Citrix ADM IP> " , " port " : " 27000 "  }
  }
 \r\n
<!--NeedCopy-->
```

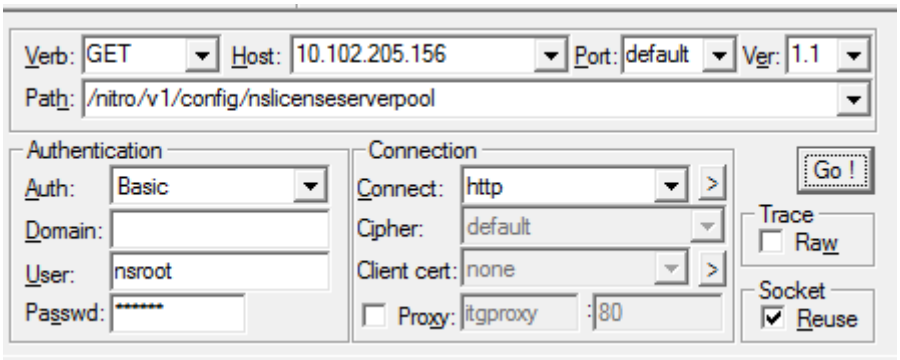


NetScaler ADM antwortet auf die Anforderung. Die folgende Beispielantwort zeigt Erfolg.

```
RESPONSE: **********\n
HTTP/1.1 201 Created\r\n
Date: Fri, 06 Jan 2017 19:03:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

So zeigen Sie die verfügbaren Lizenzen auf dem Lizenzserver an:

1. Stellen Sie den Anforderungstyp auf **Get ein**.
2. Legen Sie den Pfad zu /nitro/v1/config/nslicenseserverpool fest



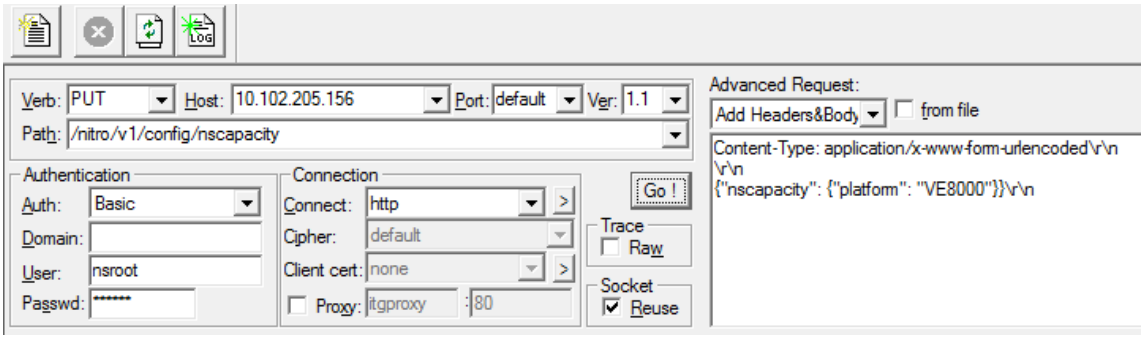
NetScaler ADM antwortet auf die Anforderung. Die folgende Beispielantwort zeigt den Erfolg und die Liste der verfügbaren Lizenzen auf dem Lizenzserver.

RESPONSE: **********\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:18:54 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 1874\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE", "nslicenseserverpool": { "instancetotal": 0, "instanceavailable": 0, "standardbandwidthtotal":
0, "standardbandwidthavailable": 0, "enterprisebandwidthtotal": 0, "enterprisebandwidthavailable": 0, "platinumbandwidthtotal": 0, "platinumbandwidthav
ailable": 0, "cpxinstancetotal": 0, "cpxinstanceavailable": 0, "vpx1stotal": 0, "vpx1savailable": 0, "vpx1ptotal": 0, "vpx1pavailable": 0, "vpx5stotal"
: 0, "vpx5savailable": 0, "vpx5ptotal": 0, "vpx5pavailable": 0, "vpx10stotal": 0, "vpx10savailable": 0, "vpx10etotal": 0, "vpx10eavailable": 0, "vpx10p
total": 0, "vpx10pavailable": 0, "vpx25stotal": 0, "vpx25savailable": 0, "vpx25etotal": 0, "vpx25eavailable": 0, "vpx25ptotal": 0, "vpx25pavailable": 0
, "vpx50stotal": 0, "vpx50savailable": 0, "vpx50etotal": 0, "vpx50eavailable": 0, "vpx50ptotal": 0, "vpx50pavailable": 0, "vpx100stotal": 0, "vpx100sav
ailable": 0, "vpx100etotal": 0, "vpx100eavailable": 0, "vpx100ptotal": 0, "vpx100pavailable": 0, "vpx200stotal": 0, "vpx200savailable": 0, "vpx200etota
l": 0, "vpx200eavailable": 0, "vpx200ptotal": 0, "vpx200pavailable": 0, "vpx500stotal": 0, "vpx500savailable": 0, "vpx500eto
tal": 0, "vpx500eavailable": 0, "vpx500ptotal": 0, "vpx500pavailable": 0, "vpx1000stotal": 0, "vpx1000savailable": 0, "vpx1000etotal": 0, "vpx1000eavail
able": 0, "vpx1000ptotal": 0, "vpx1000pavailable": 0, "vpx2000ptotal": 0, "vpx2000pavailable": 0, "vpx3000stotal": 0, "vpx3000savailable": 0, "vpx3000e
total": 0, "vpx3000eavailable": 0, "vpx3000ptotal": 0, "vpx3000pavailable": 0, "vpx4000ptotal": 0, "vpx4000pavailable": 0, "vpx5000stotal": 0, "vpx5000
savailable": 0, "vpx5000etotal": 0, "vpx5000eavailable": 0, "vpx5000ptotal": 0, "vpx5000pavailable": 0, "vpx8000stotal": 1, "vpx8000savailable": 1, "vp
x8000etotal": 2, "vpx8000eavailable": 1, "vpx8000ptotal": 1, "vpx8000pavailable": 1 } }
finished.

So weisen Sie der NetScaler ADC Appliance eine Lizenz zu:

1. Legen Sie den Anforderungstyp auf **Post**fest.
2. Stellen Sie den Pfad zu /nitro/v1/config/nscapacity.
3. Legen Sie die Nutzlast wie folgt fest:

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
{
  " nscapacity:{
  " platform " : " VE8000 "  }
   }
 \r\n
<!--NeedCopy-->
```

NetScaler ADM antwortet auf die Anforderung. Die folgende Beispielantwort zeigt Erfolg.

```
RESPONSE: **************\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:16:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

Aktualisieren der IP-Adresse eines Lizenzservers

Sie können die IP-Adresse des Lizenzservers in den VPX- und BLX-Instanzen aktualisieren, ohne die zugewiesene Lizenzbandbreite auf der Instanz und Datenverlust zu beeinträchtigen.

Update mit der CLI: Um die IP-Adresse des Lizenzservers mithilfe der CLI zu aktualisieren, geben Sie den folgenden Befehl in der Instanz ein:

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

Mit diesem Befehl wird eine Verbindung zum neuen Server hergestellt und die Ressourcen freigegeben, die dem vorherigen Lizenzierungsserver zugeordnet sind.

Aktualisieren mithilfe der GUI: Um die IP-Adresse des Lizenzservers mithilfe der GUI zu aktualisieren, navigieren Sie zu **System > Lizenzen > Lizenzen verwalten**und klicken Sie auf **Neue Lizenz hinzufügen** Weitere Informationen finden Sie unter Zuweisen von VPX- und BLX-Lizenzen zu einer ADC-Instanz mithilfe der NetScaler ADC GUI.

Konfigurieren von Ablaufprüfungen für NetScaler ADC VPX- und BLX-Check-In- und Check-Out

Sie können jetzt den Schwellenwert für den Lizenzablauf für NetScaler ADC VPX- und BLX-Lizenzen konfigurieren. Durch Festlegen von Schwellenwerten sendet NetScaler ADM Benachrichtigungen per E-Mail oder SMS, wenn eine Lizenz abläuft. Ein SNMP-Trap und eine Benachrichtigung werden ebenfalls gesendet, wenn die Lizenz auf NetScaler ADM abgelaufen ist.

Ein Ereignis wird generiert, wenn eine Benachrichtigung über den Ablauf der Lizenz gesendet wird und dieses Ereignis in NetScaler ADM angezeigt werden kann.

So konfigurieren Sie Lizenzablaufprüfungen:

1. Navigieren Sie zu**Netzwerke**>**Lizenzen**.
2. Auf der Seite**Lizenzeinstellungen**finden Sie im Abschnitt**Lizenzablaufinformationen**die Details der Lizenzen, die ablaufen werden:
   - **Feature**: Art der Lizenz, die ablaufen wird.
   - **Anzahl**: Anzahl der betroffenen virtuellen Server oder Instanzen.
   - **Tage bis zum Ablauf**: Anzahl der Tage vor Ablauf der Lizenz.
3. Klicken Sie im Abschnitt**Benachrichtigungseinstellungen**auf das Symbol**Bearbeiten**, und geben Sie den Warnschwellenwert an. Sie können einen Prozentsatz der Kapazität der gepoolten Lizenzen festlegen, der zur Benachrichtigung von Administratoren verwendet werden soll.
4. Wählen Sie die Art der Benachrichtigung aus, die Sie senden möchten, indem Sie das entsprechende Kontrollkästchen aktivieren. Die Benachrichtigungstypen sind wie folgt:
   a) **E-Mail-Profil**: Geben Sie einen Mailserver und Profildetails an. Eine E-Mail wird ausgelöst, wenn Ihre Lizenzen bald ablaufen.
   b) **SMS-Profil**: Geben Sie einen Short Message Service (SMS) -Server und Profildetails an. Eine SMS-Nachricht wird ausgelöst, wenn Ihre Lizenzen ablaufen.
5. Geben Sie dann an, wann Sie die Benachrichtigung in Bezug auf die Anzahl der Tage vor Ablauf der Lizenz senden möchten.
6. Klicken Sie auf **Speichern**.

NetScaler ADC virtuelle CPU-Lizenzierung

February 5, 2024

Rechenzentrumsadministratoren wie Sie wechseln zu neueren Technologien, die Netzwerkfunktionen vereinfachen und gleichzeitig niedrigere Kosten und größere Skalierbarkeit bieten. Neuere Rechenzentrumsarchitekturen müssen mindestens die folgenden Funktionen enthalten:

- Softwaredefiniertes Netzwerk (SDN)
- Virtualisierung von Netzwerkfunktionen (NFV)
- Netzwerkvirtualisierung (NV)
- Mikro-Services

Für eine solche Entwicklung müssen auch die Softwareanforderungen dynamisch, flexibel und agil sein, um den sich ständig ändernden Geschäftsanforderungen gerecht zu werden. Es wird erwartet, dass Lizenzen von einem zentralen Management-Tool verwaltet werden, das volle Einblick in die Nutzung bietet.

Virtuelle CPU-Lizenzierung für NetScaler ADC VPX

Zuvor wurden NetScaler ADC VPX-Lizenzen basierend auf dem Bandbreitenverbrauch der Instanzen zugewiesen. Ein NetScaler ADC VPX ist auf die Verwendung einer bestimmten Bandbreite und anderer Leistungsmetriken beschränkt, die auf der Lizenzedition basieren, an die er gebunden ist. Um die verfügbare Bandbreite zu erhöhen, müssen Sie ein Upgrade auf eine Lizenzedition durchführen, die mehr Bandbreite bietet. In bestimmten Szenarien ist die Bandbreitenanforderung möglicherweise geringer, die Anforderung gilt jedoch eher für andere L7-Leistungen wie SSL-TPS, Komprimierungsdurchsatz usw. Ein Upgrade der NetScaler ADC VPX-Lizenz ist in solchen Fällen möglicherweise nicht geeignet. Möglicherweise müssen Sie jedoch noch eine Lizenz mit großer Bandbreite kaufen, um die für die CPU-intensive Verarbeitung erforderlichen Systemressourcen freizuschalten. NetScaler ADM unterstützt jetzt die Zuweisung von Lizenzen für die NetScaler ADC-Instanz auf der Grundlage der virtuellen CPU-Anforderungen.

In der virtuellen CPU-Usage-basierten Lizenzierungsfunktion gibt die Lizenz die Anzahl der CPUs an, auf die ein bestimmtes NetScaler ADC VPX berechtigt ist. NetScaler ADC VPX kann daher Lizenzen nur für die Anzahl der virtuellen CPUs, die auf dem Server ausgeführt werden, vom Lizenzserver auschecken. NetScaler ADC VPX checkt Lizenzen abhängig von der Anzahl der im System ausgeführten CPUs aus. NetScaler ADC VPX berücksichtigt die Leerlauf-CPUs beim Auschecken der Lizenzen nicht.

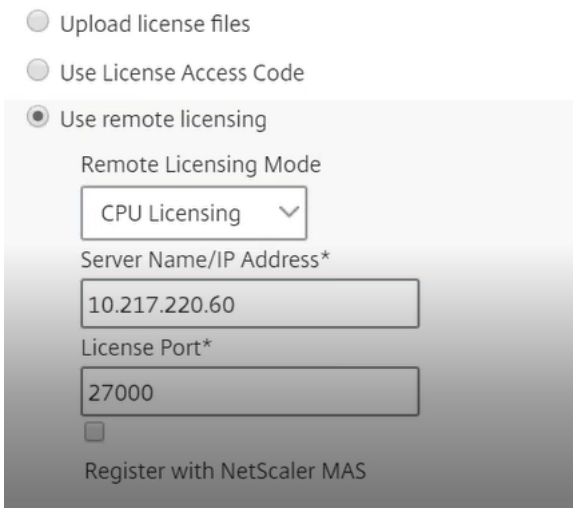
Ähnlich wie die gepoolte Lizenzkapazität und die CICO-Lizenzfunktionen verwaltet der NetScaler ADM -Lizenzserver einen separaten Satz virtueller CPU-Lizenzen. Auch hier sind die drei Editionen, die für virtuelle CPU-Lizenzen verwaltet werden, Standard, Advanced und Premium. Diese Editionen entsperren dieselben Features wie jene, die von den Editionen für Bandbreitenlizenzen freigeschaltet wurden.

Möglicherweise ändert sich die Anzahl der virtuellen CPUs oder wenn sich die Lizenzversion ändert. In einem solchen Fall müssen Sie die Instanz immer herunterfahren, bevor Sie eine Anforderung für

einen neuen Satz von Lizenzen initiieren. Starten Sie NetScaler ADC VPX nach dem Auschecken der Lizenzen neu.

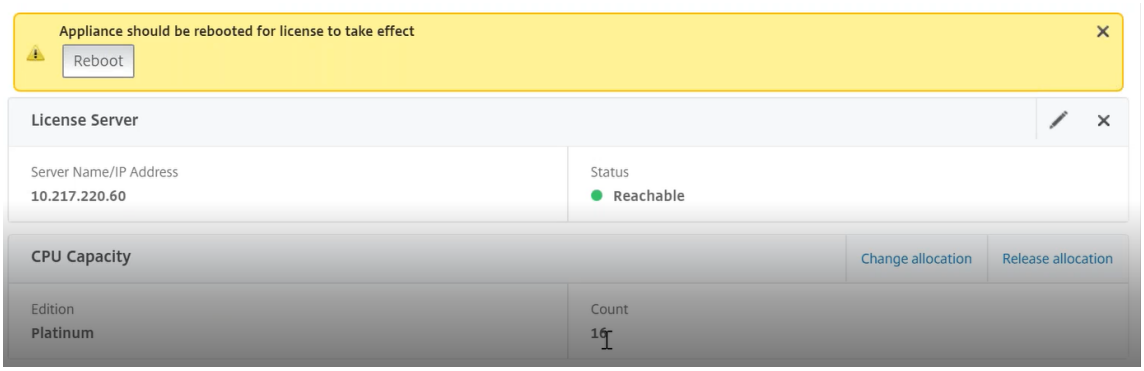
So konfigurieren Sie den Lizenzierungsserver in NetScaler ADC VPX mit der GUI:

1. Navigieren Sie in NetScaler ADC VPX zu **System** > **Lizenzen** und klicken Sie auf **Lizenzen verwalten**.
2. Klicken Sie auf der Seite **Lizenz** auf **Neue Lizenz hinzufügen**.
3. Wählen Sie auf der Seite **Lizenzen** die Option **Remote-Lizenzierung verwenden** .
4. Wählen Sie **CPU-Lizenzierung** aus der Liste **Remote-Lizenzierungsmodus** aus.
5. Geben Sie die IP-Adresse des Lizenzservers und die Portnummer ein.
6. Klicken Sie auf **Weiter**.



> **Hinweis:**
>
> Sie müssen die NetScaler ADC VPX-Instanz immer bei NetScaler ADM registrieren. Falls noch nicht geschehen, aktivieren Sie **Bei NetScaler ADM registrieren** und geben Sie die NetScaler ADM-Anmeldeinformationen ein.

7. Wählen Sie im Fenster **Lizenzen zuweisen** den Lizenztyp aus. Das Fenster zeigt die Gesamtzahl und die verfügbaren virtuellen CPUs sowie die CPUs an, die zugewiesen werden können. Klicken Sie auf **Get Licenses**.
8. Klicken Sie auf der nächsten Seite auf **Neustart**, um die Lizenzen zu beantragen.



> **Hinweis**
>
> Sie können auch die aktuelle Lizenz freigeben und aus einer anderen Edition auschecken. Beispielsweise führen Sie bereits die Standard Edition-Lizenz für Ihre Instanz aus. Sie können diese Lizenz freigeben und dann aus der Advanced Edition auschecken.

Konfigurieren des Lizenzservers in der NetScaler ADC VPX -Lizenz mit CLI

Geben Sie in der NetScaler ADC VPX-Konsole die folgenden Befehle für die folgenden zwei Aufgaben ein:

1. Um den Lizenzserver zum NetScaler ADC VPX hinzuzufügen:

```
add licenseserver <IP address of the license server>
<!--NeedCopy-->
```

2. So beantragen Sie die Lizenzen:

```
set capacity -vcpu - edition premium
<!--NeedCopy-->
```

   Wenn Sie dazu aufgefordert werden, starten Sie die Instanz neu, indem Sie den folgenden Befehl eingeben:

```
reboot -w
<!--NeedCopy-->
```

Aktualisieren der IP-Adresse eines Lizenzservers

Sie können die IP-Adresse des Lizenzservers in der VPX-Instanz aktualisieren, ohne Auswirkungen auf die zugewiesene Lizenzbandbreite für die Instanz und Datenverlust. Um die IP-Adresse des Lizenzservers zu aktualisieren, geben Sie den folgenden Befehl auf der VPX-Instanz ein:

```
add licenseserver <licensing server IP address> -forceUpdateIP
```


Mit diesem Befehl wird eine Verbindung zum neuen Server hergestellt und die Ressourcen freigegeben, die dem vorherigen Lizenzierungsserver zugeordnet sind.

Verwalten virtueller CPU-Lizenzen auf NetScaler ADM

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Lizenzen** > **Virtuelle CPU-Lizenzen**.
2. Auf der Seite werden die Lizenzen angezeigt, die für jeden Lizenzausgabetyp zugewiesen sind.
3. Klicken Sie auf die Zahl in jedem Donut, um die NetScaler ADC-Instanzen anzuzeigen, die diese Lizenz verwenden.

Virtuelle CPU-Lizenzierung für NetScaler ADC CPX

Während der Bereitstellung der NetScaler ADC CPX-Instanz können Sie die NetScaler ADC CPX-Instanz so konfigurieren, dass je nach CPU-Auslastung der Instanz Lizenzen vom Lizenzserver ausgecheckt werden.

NetScaler ADC CPX verwendet den Lizenzserver, der auf NetScaler ADM läuft, um die Lizenzen zu verwalten. NetScaler ADC CPX checkt die Lizenzen vom Lizenzserver aus, wenn dieser gestartet wird. Die Lizenzen werden beim Herunterfahren des NetScaler ADC CPX wieder auf den Lizenzserver eingecheckt.

Sie können NetScaler ADC CPX aus dem Docker App Store herunterladen. Führen Sie auf dem Docker-Host den folgenden Befehl aus, um NetScaler ADC CPX herunterzuladen:

```
docker pull store/citrix/netscalercpx: [version]
```

Für die CPX-Lizenzierung stehen drei Lizenztypen zur Verfügung:

1. Unterstützte virtuelle CPU-Abonnementlizenzen für CPX und VPX
2. Lizenzen für gepoolte Kapazität
3. CP1000-Lizenzen, die einzelne bis mehrere vCPUs nur für CPX unterstützen

So konfigurieren Sie vCPU-Abonnementlizenzen während der Provisioning der NetScaler ADC CPX-Instanz:

Geben Sie die Anzahl der vCPU-Lizenzen an, die die NetScaler ADC CPX-Instanz verwendet.

- Dieser Wert wird als Umgebungsvariable über Docker, Kubernetes oder Mesos/Marathon eingegeben.
- Die Zielvariable lautet "CPX_CORES". Der CPX kann 1 bis 16 Kerne unterstützen.

Um 2 Kerne anzugeben, können Sie den Befehl docker run wie folgt ausführen:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2
2 <!--NeedCopy-->
```

Definieren Sie bei der Bereitstellung einer NetScaler ADC CPX-Instanz den NetScaler ADC Lizenzserver als Umgebungsvariable im Befehl **docker run**, wie unten gezeigt:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
     LS_PORT> cpx:11.1
2 <!--NeedCopy-->
```

Hierbei gilt:

- *<LS_IP_ADDRESS>* ist die IP-Adresse des NetScaler ADC Lizenzservers.
- *<LS_PORT>* ist der Port des NetScaler ADC Lizenzservers. Standardmäßig ist der Port 27000.

> **Hinweis:**
>
> Standardmäßig checkt die NetScaler ADC CPX-Instanz die Lizenz aus dem vCPU-Abonnementpool aus. Die CPX-Instance checkt eine Anzahl von "n"Lizenzen aus, wenn die Instance mit "n"CPUs läuft.

So konfigurieren Sie NetScaler ADC Pooled Capacity oder CP1000-Lizenzen während der Provisioning der NetScaler ADC CPX-Instanz:

Wenn Sie Lizenzen für die CPX-Instance auschecken möchten, die die gepoolte Lizenzierung (bandbreitenbasiert) oder den privaten CPX-Pool (CP1000 oder private Pool-basiert) verwenden, müssen Sie die Umgebungsvariablen entsprechend angeben.

Beispiel:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
     LS_PORT> -e PLATFORM=CP1000 cpx:11.1
2 <!--NeedCopy-->
```


CP1000. Dieser Befehl löst das Auschecken aus dem CP1000-Pool (CPX-Privatpool) aus. Die NetScaler ADC CPX-Instanz ruft dann die Anzahl der Instanzen "n"für die Anzahl der für CPX_CORES angegebenen Kerne ab. Der häufigste Anwendungsfall ist, n = 1 für ein Auschecken einer einzelnen Instanz anzugeben. Anwendungsfälle für Multicore-CPX Schauen Sie sich "n"vCPUs an (wobei "n"für 1 bis 7 steht).

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> -e BANDWIDTH=2000 cpx:11.1
<!--NeedCopy-->
```

Kapazität gepoolt. Dieser Befehl checkt eine Lizenz aus dem Instanzpool aus und verbraucht 1000 Mbit/s Bandbreite aus dem Premium-Bandbreitenpool. CPX kann jedoch bis zu 2000 Mbit/s ausführen.In der Pooled Licensing werden die ersten 1000 Mbit/s nicht berechnet.

> **Hinweis**
>
> Geben Sie beim Auschecken aus dem Bandbreitenpool die entsprechende Anzahl von vCPUs für die gewünschte Zielbandbreite an, wie in der folgenden Tabelle beschrieben:

Anzahl der Kerne (vCPU)	Maximale Bandbreite
1	1000 MBit/s
2	2000 Mbit/s
3	3500 Mbit/s
4	5000 Mbit/s
5	6500 Mbit/s
6	8000 Mbit/s
7	9300 Mbit/s

Citrix SD-WAN Instanzen verwalten

February 5, 2024

Mit Citrix ADM können Sie Analysen der Citrix SD-WAN Appliances in Ihrem Netzwerk überwachen, verwalten und anzeigen. Die folgende Interoperabilitätstabelle enthält Informationen darüber, welche Funktionen von Citrix ADM derzeit in den einzelnen Citrix SD-WAN Plattformeditionen unterstützt werden.

Interoperabilitätsmatrix von Citrix SD-WAN Plattformeditionen und NetScaler ADM Funktionen

Plattform-Edition	Entdeckung	Konfiguration	Überwachen	Berichterstattung (Netzwerkberichte)	Event-Management	HDX Insight	WAN-Einblick
Citrix SD-WANOP	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Citrix SD-WAN SE	Ja	Nein	Nein	Nein	Nein	Nein	Nein
Citrix SD-WAN PE	Ja	Nein	Nein	Nein	Nein	Ja	Nein

Von Citrix ADM unterstützte Citrix SD-WAN-Versionen

Plattform-Edition	Citrix SD-WAN Version	Citrix ADM Version
Citrix SD-WANOP	Citrix CloudBridge 7.4 und höher	Citrix ADM 11.0 und höher
Citrix SD-WAN SE	Citrix SD-WAN 9.3.0 und höher	NetScaler ADM 12.0.53.8 und höher
Citrix SD-WAN PE	Citrix SD-WAN 9.3.0 und höher	NetScaler ADM 12.0.53.8 und höher

Sie können eine Citrix SD-WANOP-Appliance als verwaltete Instanz auf NetScaler ADM hinzufügen. Weitere Informationen finden Sie unter Instanzen zu NetScaler ADM hinzufügen. Sie können WAN-Insight, HDX-Insight, Netzwerkberichte und Ereignisberichte für Citrix SD-WANOP-Instanzen anzeigen.

NetScaler ADM ermöglicht es Citrix SD-WAN Standard Edition (SE) und Enterprise Edition (EE) -Appliances, sich als verwaltete Instanzen auf NetScaler ADM zu registrieren.

Um eine Citrix SD-WAN SE/PE/AE-Appliance zu NetScaler ADM hinzuzufügen, konfigurieren Sie NetScaler ADM als AppFlow-Collector auf den Citrix SD-WAN SE/PE/AE-Appliances. Die Citrix SD-WAN SE/PE/AE Appliance fügt sich selbst als verwaltete Instanz auf NetScaler ADM hinzu. Die SD-WAN SE/PE/AE-Appliance sendet die Analysedaten dann an NetScaler ADM.

Sie können NetScaler ADM als AppFlow-Collector auf jedem SD-WAN SE/PE/AE-Gerät einzeln festlegen oder das Citrix SD-WAN Center verwenden, um die Konfiguration auf die verwalteten Appliances zu exportieren.

Weitere Informationen finden Sie unter Hinzufügen von Citrix SD-WAN SE/PE/AE-Instanzen in NetScaler ADM.

Bei einer Citrix SD-WAN PE-Appliance können Sie je nach AppFlow Konfiguration HDX-Datensätze oder Multi-Hop-Daten anzeigen. Eine Citrix SD-WAN SE-Appliance stellt nur Multi-Hop-Daten bereit.Weitere Informationen finden Sie unter HDX Insight-Berichte und -Metrikenanzeigen und Analysedaten für die Multi-Hop-Bereitstellunganzeigen.

Diese Seite enthält Schnellzugriffslinks zu den Themen, die Sie zum Einrichten von NetScaler ADM und zur Verwaltung Ihrer SD-WANOP-Appliances mit NetScaler ADM verweisen können.

Citrix ADM —Übersicht

Über Citrix ADM

Architecture

So erkennt Citrix ADM Instanzen

Wie Citrix ADM mit verwalteten Instanzen kommuniziert

Citrix ADM Bereitstellung

Bereitstellen von Citrix ADM mit Citrix Hypervisor

Bereitstellen von NetScaler ADM mit Microsoft Hyper-V

Bereitstellen von Citrix ADM mit VMware ESXi

Bereitstellen von NetScaler ADM mit Linux KVM-Server

Bereitstellen von Citrix ADM im Hochverfügbarkeitsmodus

NetScaler Insight Center zu NetScaler ADM migrieren

Integrieren von NetScaler ADM mit Director

Instanz-Verwaltung

Hinzufügen von Instanzen zu Citrix ADM

Erstellen von Instanzgruppen in Citrix ADM

Sichern und Wiederherstellen einer Instanz mit Citrix ADM

Konfigurationsverwaltung

Erstellen von Konfigurationsaufträgen aus Korrekturbefehlen in Citrix ADM

Planen von Aufträgen, die mit integrierten Vorlagen in Citrix ADM erstellt wurden

Umplanen von Aufträgen, die mithilfe von integrierten Vorlagen in Citrix ADM konfiguriert wurden

Wiederverwendung ausgeführter Konfigurationsaufträge

Analytics

WAN Insight

HDX Insight

Anzeigen von Netzwerkberichten für Citrix SD-WANOP-Instanzen

Konfigurieren von adaptiven Schwellenwerten

Konfigurieren der Datenbankzusammenfassung für Analytics

Erstellen von Schwellenwerten und Warnungen mit Citrix ADM

Event-Management

Festlegen des Ereignisalters für Ereignisse in Citrix ADM

Planen eines Ereignisfilters mithilfe von Citrix ADM

Festlegen von wiederholten E-Mail-Benachrichtigungen für Ereignisse von Citrix ADM

Unterdrücken von Ereignissen mithilfe von Citrix ADM

Anzeigen von Ereignisberichten für Citrix SD-WANOP-Instanzen

Ändern des gemeldeten Schweregrads von Ereignissen, die auf Citrix ADC Instanzen auftreten

Anzeigen der Ereignisübersicht in NetScaler ADM

Anzeigen von Ereignis-Schweregraden und -schrägen von SNMP-Traps im Infrastructure Dashboard von Citrix ADM

Authentifizierung

Kaskadieren externer Authentifizierungsserver

Hinzufügen von RADIUS-Authentifizierungsservern

Hinzufügen von LDAP-Authentifizierungsservern

Hinzufügen von TACACS-Authentifizierungsservern

Extrahieren der Authentifizierungsservergruppe in Citrix ADM

Aktivieren der lokalen Fallback-Authentifizierung

Citrix ADM -System

Verwalten des Citrix ADM -Systems

Aktualisieren von Citrix ADM

Erstellen einer technischen Supportdatei für NetScaler ADM

Sichern und Wiederherstellen des Citrix ADM -Servers in einer Bereitstellung mit einem Server

Sichern und Wiederherstellen einer Citrix ADM Konfiguration in einem HA-Paar

Aktivieren des Shellzugriffs für nicht standardmäßige Benutzer in Citrix ADM

Konfigurieren des NTP-Servers auf NetScaler ADM

Konfigurieren von SSL-Einstellungen für Citrix ADM

Konfigurieren des Syslog-Löschintervalls für Citrix ADM

Anzeigen von Überwachungsinformationen von Citrix ADM

Konfigurieren der Einstellungen für die Systembenachrichtigung von NetScaler ADM

Überwachen der CPU-, Arbeitsspeicher- und Datenträgerauslastung von Citrix ADM

Konfigurieren einer Verschlüsselungsgruppe für Citrix ADM

Erstellen von SNMP-Traps, Managern und Benutzern in Citrix ADM

Zuweisen eines Hostnamens zu einem NetScaler ADM Server

Konfigurieren von Systemausstutzungseinstellungen für Citrix ADM

Konfigurieren von Systembackupeinstellungen mit Citrix ADM

Konfigurieren und Anzeigen von Systemalarmen auf NetScaler ADM

Hinzufügen von Citrix SD-WAN Instanzen

February 5, 2024

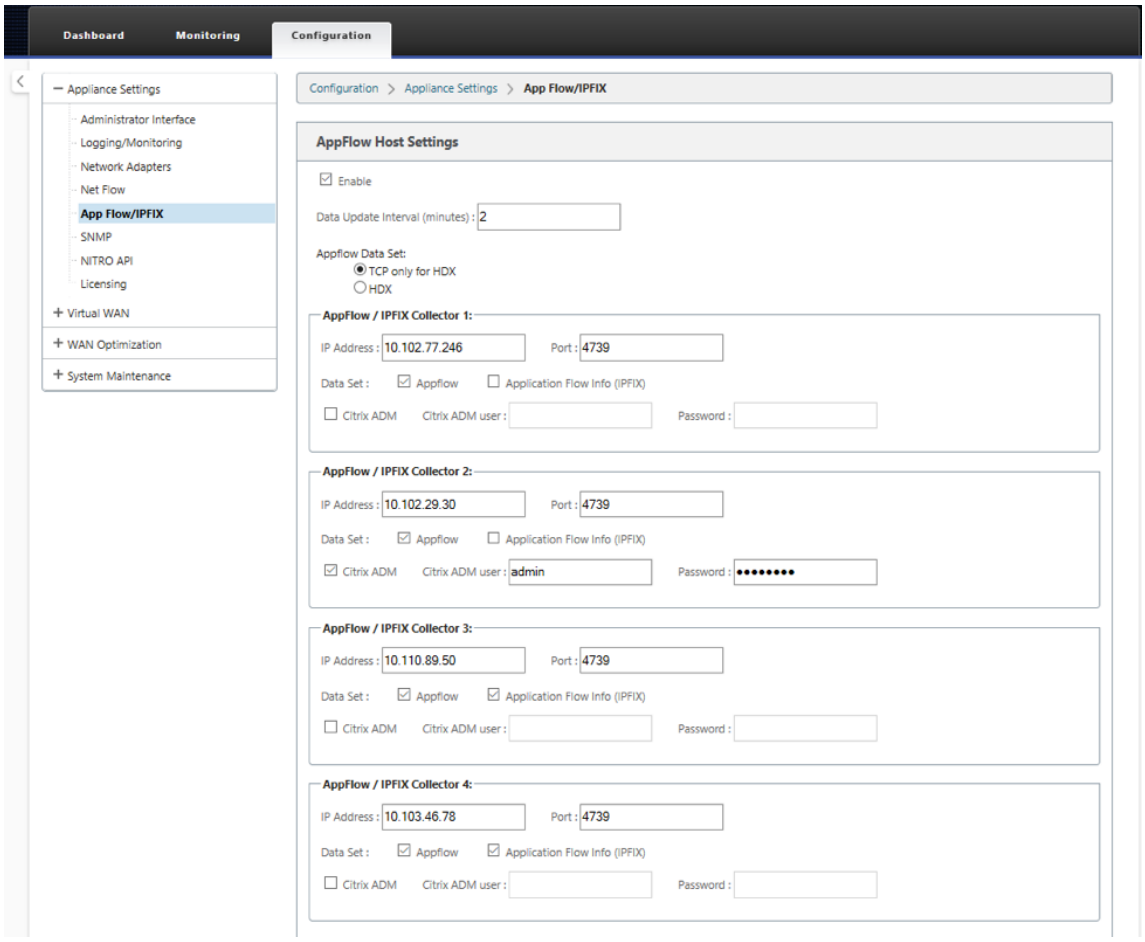
Konfigurieren Sie NetScaler ADM als AppFlow Collector auf der Citrix SD-WAN SE/PE-Appliance, um diese Instanzen in NetScaler ADM hinzuzufügen.Die Citrix SD-WAN SE/PE/AE Appliances werden auf

NetScaler ADM als verwaltete Instanzen registriert, und ihre AppFlow-Datensätze werden gesammelt. Bei einer Citrix SD-WAN PE-Appliance können Sie entweder die **TCP nur für HDX-Vorlage** oder die **HDX-Vorlage** aktivieren. Die Vorlage **TCP nur für HDX** stellt Multi-Hop-Daten bereit. Die **HDX-Vorlage** stellt HDX-Daten bereit. Sie sollte nur auf der Rechenzentrums-Appliance aktiviert werden.

Sie können NetScaler ADM als AppFlow-Collector auf der einzelnen SD-WAN SE/PE/AE-Appliance konfigurieren, oder Sie können NetScaler ADM mithilfe von SD-WAN Center als AppFlow-Collector konfigurieren und die Konfiguration an die von ihm verwalteten Appliances exportieren.

So konfigurieren Sie NetScaler ADM als AppFlow-Collector auf einer Citrix SD-WAN SE/PE/AE-Appliance:

1. Navigieren Sie im SD-WAN SE/PE/AE Webinterface zu **Configuration** > **AppFlow/IPFIX**
2. Wählen Sie **Aktivieren**.



3. Geben Sie im Feld **Datenaktualisierungsintervall** das Zeitintervall (in Minuten) an, in dem die AppFlow Berichte in den AppFlow-Kollektor exportiert werden.

> **Hinweis**
>
> Wenn Citrix ADM der AppFlow Collector ist, sollte das Datenaktualisierungsintervall 1 Minute betragen.

4. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie **HDX**, um HDX Insight Daten an den AppFlow Collector zu senden. Dies sollte auf den Zweigstellen Appliances aktiviert sein.
   - Wählen Sie **TCP nur für HDX,** um Multi-Hop-Daten an den AppFlow Collector zu senden.

   > **Hinweis**
   >
   > Die**HDX-Vorlagenoption** ist nur für Citrix SD-WAN PE-Appliance verfügbar. Sie sollte auf der Data Center-Appliance aktiviert sein.

5. Geben **Sie im Feld IP-Adresse** die IP-Adresse des externen AppFlow Collectorsystems (Citrix ADM Server) ein.
6. Geben Sie im Feld **Port** die Portnummer ein, auf die das externe AppFlow Kollektorsystem überwacht. Der Standardwert ist 4739.
7. Aktivieren Sie das Kontrollkästchen **Citrix ADM**, um anzugeben, dass Citrix ADM der AppFlow Collector ist.

   > **Hinweis**
   >
   > - NetScaler ADM unterstützt derzeit keine IPFIX-Sammlung.
   > - Sie können bis zu vier AppFlow-Kollektoren hinzufügen. NetScaler ADM oder ein AppFlow Collector, der das IPFIX-Protokoll unterstützt.

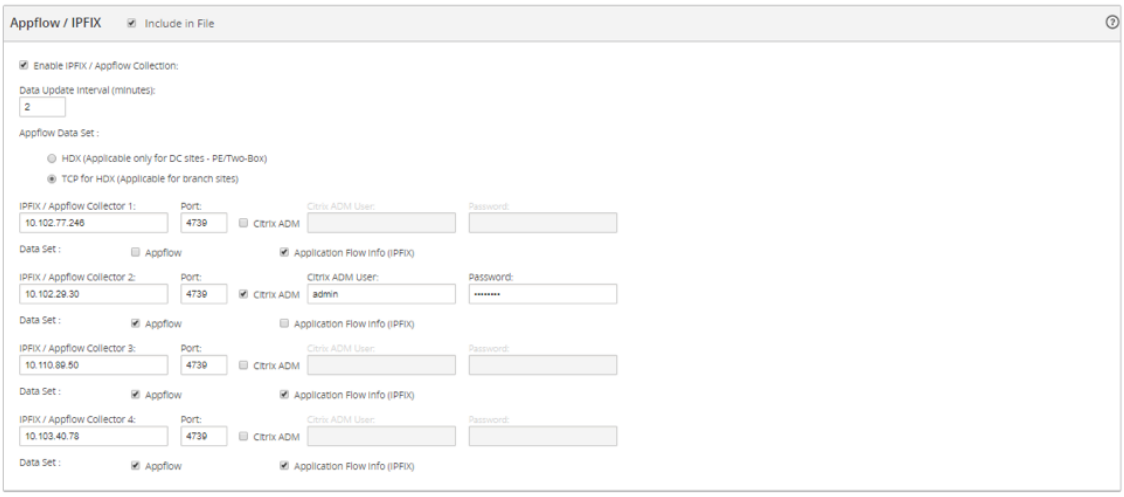
8. Geben Sie die Anmeldeinformationen für den Citrix ADM -Server ein
9. Klicken Sie auf **Einstellungen anwenden**.

Die Citrix SD-WAN SE/PE-Appliances werden in Citrix ADM erkannt und aufgeführt. Die Citrix SD-WAN SE/PE-Appliances senden die Analysedaten an NetScaler ADM. Weitere Informationen finden Sie unter AppFlow und IPFIX.

So konfigurieren Sie NetScaler ADM mit Citrix SD-WAN Center als AppFlow Collector:

1. Navigieren Sie in der Citrix SD-WAN Center-Verwaltungsoberfläche zu **Konfiguration** > **Einheit-eneinstellungen**.
2. Navigieren Sie zum Abschnitt **AppFlow /IPFIX**, und wählen Sie**In Datei einschließen**.

3. Wählen Sie **IPFIX/AppFlow -Sammlung aktivieren aus**.



4. Geben Sie im Feld ****Datenaktualisierungsintervall**** das Zeitintervall (in Minuten) an, in dem die AppFlow Berichte in den AppFlow-Kollektor exportiert werden.

> **Hinweis**
>
> Wenn Citrix ADM der AppFlow Collector ist, sollte das Datenaktualisierungsintervall 1 Minute betragen.

5. Führen Sie einen der folgenden Schritte aus:

   - Wählen Sie **HDX**, um HDX Insight Daten an den AppFlow Collector zu senden.
   - Wählen Sie **TCP für HDX,** um Multi-Hop-Einblickdaten an den AppFlow Collector zu senden.Dies sollte auf den Zweigstellen Appliances aktiviert sein.

> **Hinweis**
>
> Die**HDX-Vorlagenoption** ist nur für Citrix SD-WAN PE-Appliance verfügbar. Sie sollte auf der Data Center-Appliance aktiviert sein.

6. Geben Sie im Feld **IPFIX/AppFlow Collector** die IP-Adresse des externen AppFlow Collectorsystems (Citrix ADM Server) ein.
7. Geben Sie im Feld **Port** die Portnummer ein, auf die das externe AppFlow Kollektorsystem überwacht. Der Standardwert ist 4739.
8. Aktivieren Sie das Kontrollkästchen **Citrix ADM**, um anzugeben, dass Citrix ADM der AppFlow Collector ist.
9. Geben Sie die Anmeldeinformationen für den Citrix ADM -Server ein.

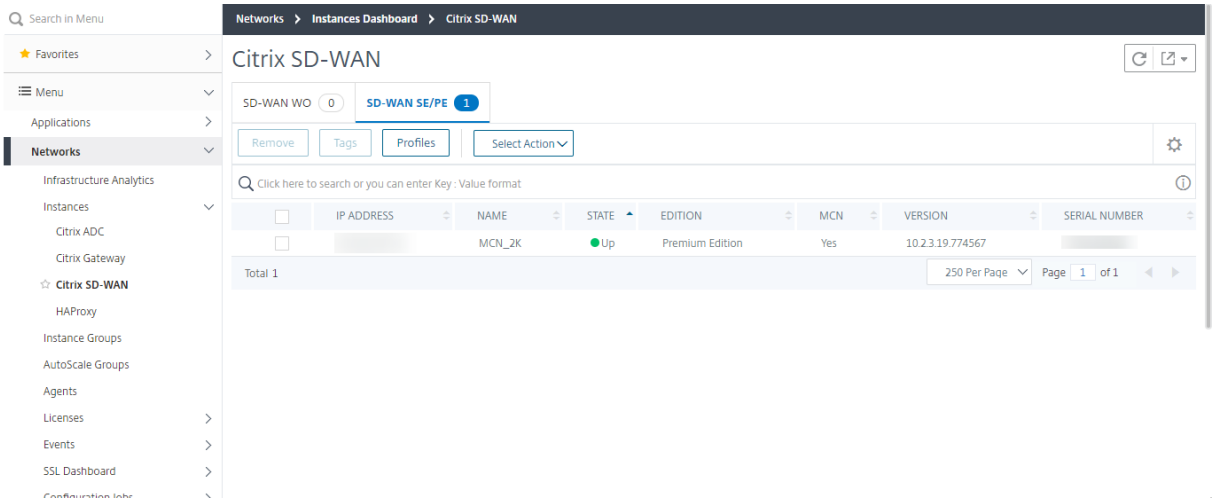
> **Hinweis**
>
> Sie können bis zu vier AppFlow-Kollektoren hinzufügen. NetScaler ADM oder ein AppFlow Collector, der das IPFIX-Protokoll unterstützt.

10. Speichern und Exportieren der Konfiguration in die verwalteten Appliances.

    Weitere Informationen finden Sie unter Konfigurieren und Exportieren von Einheiteneinstellungen in verwaltete Appliances.

Weitere Informationen zum Konfigurieren von NetScaler ADM als AppFlow-Collector mithilfe von Citrix SD-WAN Center, AppFlow und IPFIX.

Die Citrix SD-WAN SE/PE-Appliances werden von NetScaler ADM erkannt und aufgelistet.Die Citrix SD-WAN SE/PE-Appliances werden in NetScaler ADM erkannt und aufgeführt. Um die erkannten Citrix SD-WAN SE/PE-Appliances anzuzeigen, navigieren Sie im NetScaler ADM-Webinterface zu **Networks** > **Instanzen** > **Citrix SD-WAN** und wählen Sie **SD-WAN SE/PE/AE** aus.



Sie können die IP-Adresse, den Namen, den aktuellen Status, die Software-Edition und die Version der erkannten Appliances anzeigen. Sie können auch sehen, ob es sich bei der Appliance um einen Mastercontrollerknoten (MCN) handelt oder nicht.

Sie können die folgenden Aktionen ausführen:

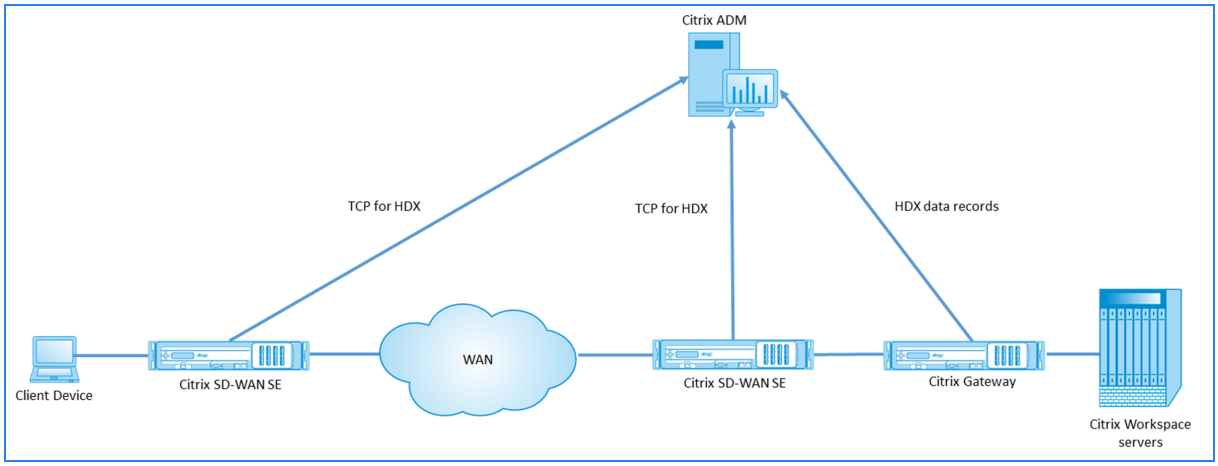
- Anzeigen und Entfernen von Instanzprofilen.
- Entfernen Sie Instanzen aus Citrix ADM.
- Ermitteln Sie Instanzen neu.

Bei einer Citrix SD-WAN PE-Appliance können Sie je nach AppFlow Konfiguration HDX-Datensätze oder Multi-Hop-Daten anzeigen. Eine Citrix SD-WAN SE-Appliance stellt nur Multi-Hop-Daten bereit. Weitere Informationen finden Sie unter Anzeigen von HDX Insight-Berichten und -Metriken und Anzeigen von Citrix SD-WAN Analytics-Daten für die Multi-Hop-Bereitstellung.

Citrix SD-WAN Analysedaten für die Bereitstellung mit mehreren Hops anzeigen

February 5, 2024

Bei einer Multi-Hop-Netzwerkbereitstellung befinden sich mehrere Geräte zwischen dem Client und dem Server, wie in der folgenden Abbildung dargestellt. Bei dieser Art der Bereitstellung werden die Citrix SD-WAN SE Appliances und das Citrix Gateway zu Citrix ADM hinzugefügt und AppFlow ist aktiviert.



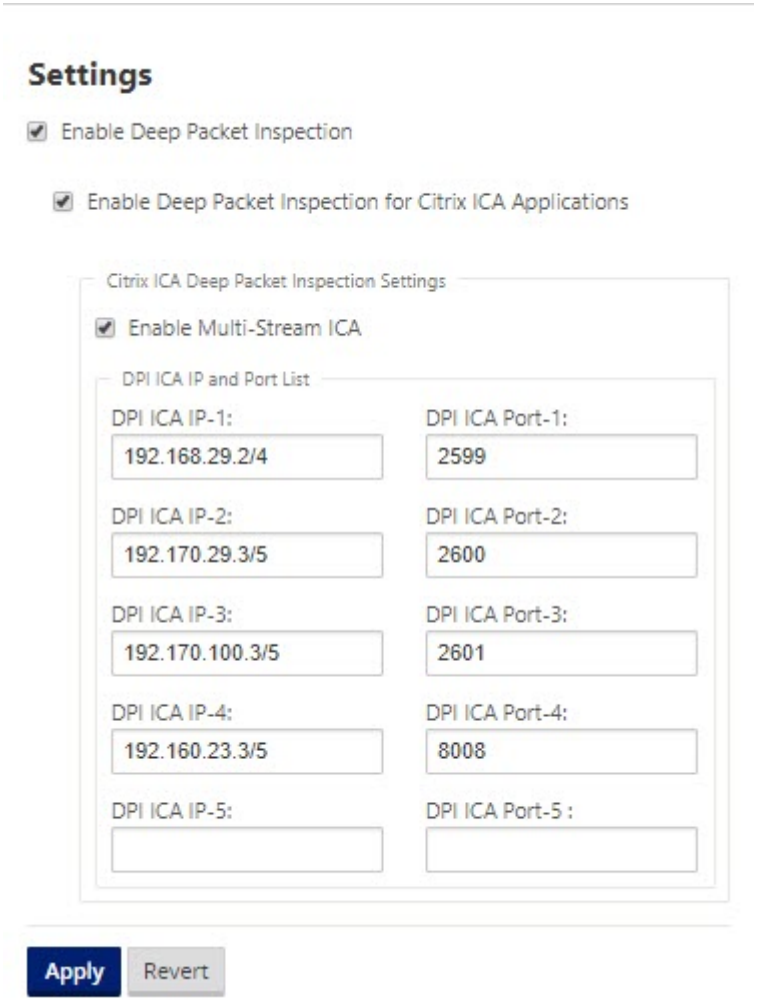
Citrix ADM identifiziert die Appliance, von der es die Daten empfängt, anhand der Hop-Anzahl und der Verbindungsketten-ID. Die Hop-Anzahl stellt die Anzahl der Appliances dar, über die der Datenverkehr vom Client zum Server fließt. Die Verbindungsketten-ID stellt die Ende-zu-Ende-Verbindungen zwischen dem Client und dem Server dar.

Citrix ADM verwendet die Hop-Anzahl und die Verbindungsketten-ID, um die Daten von den Appliances zu korrelieren, und generiert die Berichte.

Damit Citrix SD-WAN SE-Appliances die Analysedaten an Citrix ADM senden können, sollten Sie die virtuelle IP-Adresse von Citrix Gateway als DPI-ICA-IP konfigurieren und die DPI-ICA-Portnummer auf 443 festlegen.

So konfigurieren Sie die ICA-DPI-Einstellungen:

1. **Navigieren Sie in der Benutzeroberfläche der Citrix SD-WAN SE Appliance zu**Configuration Editor**>**Advanced**>**Global**>**Applications**> Settings**
2. Wählen Sie **Deep Packet Inspectionaktivieren > Deep Packet Inspection für Citrix ICA-Anwendungenaktivieren > Multistream-ICA aktivieren**



3. Geben Sie im Feld **DPI ICA IP-1** die virtuelle IP-Adresse und das Präfix von Citrix Gateway ein.
4. Geben Sie im Feld **DPI ICA Port-1 die Portnummer** 443 ein.
5. Klicken Sie auf **Anwenden** und exportieren Sie die Konfiguration mithilfe des Change-Management-Prozesses auf die Appliance.

In Citrix ADM können Sie für jede aktive ICA-Sitzung ein Sitzungsdiagramm in HDX Insight anzeigen. Die Sitzungsdiagramme enthalten Details zu den Geräten im Verbindungspfad. Sie bieten auch Einblick in die clientseitige und serverseitige Latenz zwischen einem Netzwerkgerät und seinem unmittelbaren nächsten Hop. Anhand dieser Informationen können Sie die Hauptursache für Verzögerungen ermitteln und Leistungsprobleme beheben.

Citrix SD-WAN SE sendet keine HDX-Datensätze. Es stellt nur TCP für HDX-Informationen bereit. Die HDX Insight Daten werden von den HDX Insight fähigen Geräten in Ihrem Netzwerk bereitgestellt (z. B. NetScaler ADC oder NetScaler Gateway).

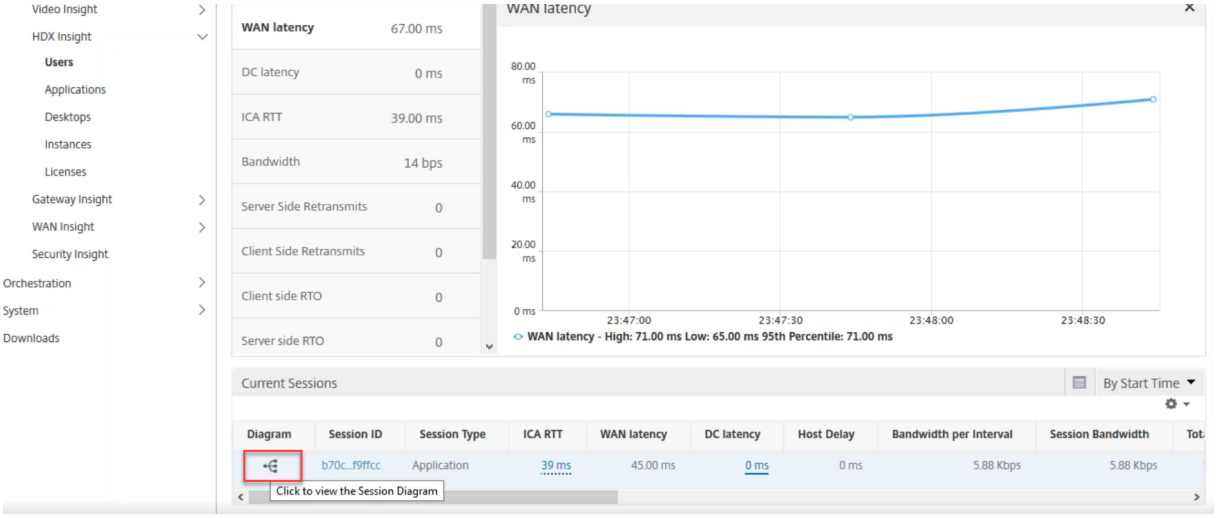
Die Citrix SD-WAN PE-Appliance kann abhängig von der AppFlow-Konfiguration der Appliance TCP-Daten für HDX-Daten oder HDX Insight-Daten senden.HDX-Vorlage sollte auf der Rechenzentrums-

Appliance aktiviert sein.

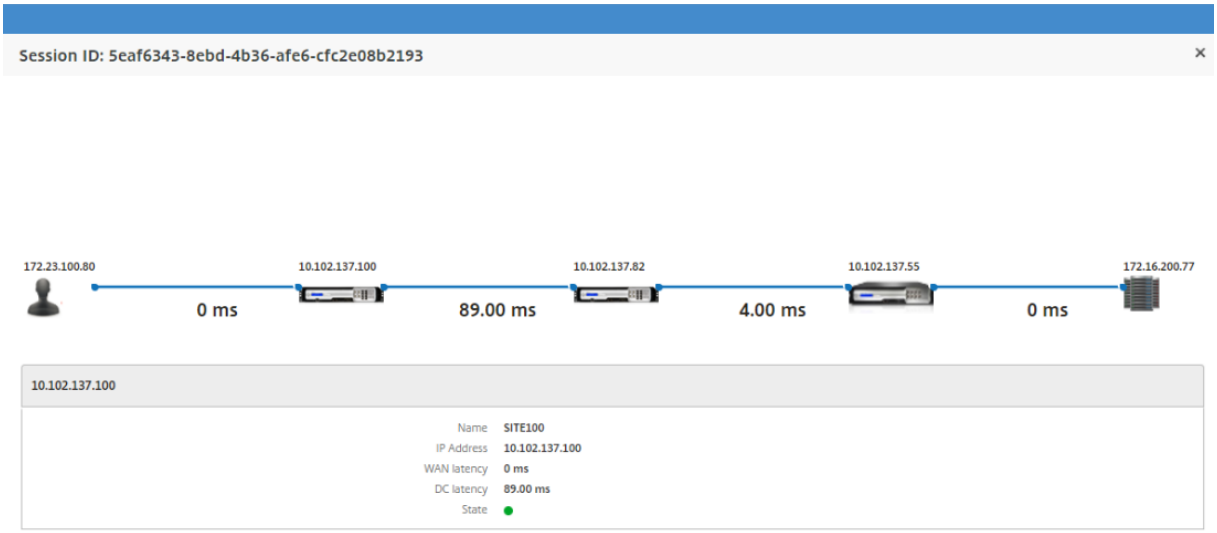
> **Hinweis**
>
> Stellen Sie in einer Multi-Hop-Bereitstellung sicher, dass nur eines der Netzwerkgeräte HDX Insight-Daten sendet. Die übrigen Netzwerkgeräte können TCP für HDX-Daten senden.

So zeigen Sie Multi-Hop-Daten an:

Navigieren Sie in der Citrix ADM-Weboberfläche zuHDX Insight**>**Benutzer**>**Aktuelle Sitzungen**oder**HDX Insight**>**Anwendungen**>**Aktuelle Sitzungen**und klicken Sie auf das Diagrammsymbol.**



Das Netzwerktopologiediagramm wird angezeigt.



Klicken Sie auf ein Netzwerkelement, um weitere Informationen anzuzeigen.

> **Hinweis**
>
> Die angezeigten Informationen hängen vom ausgewählten Netzwerkelement ab.

Die folgenden Parameter werden für Citrix Appliances angezeigt:

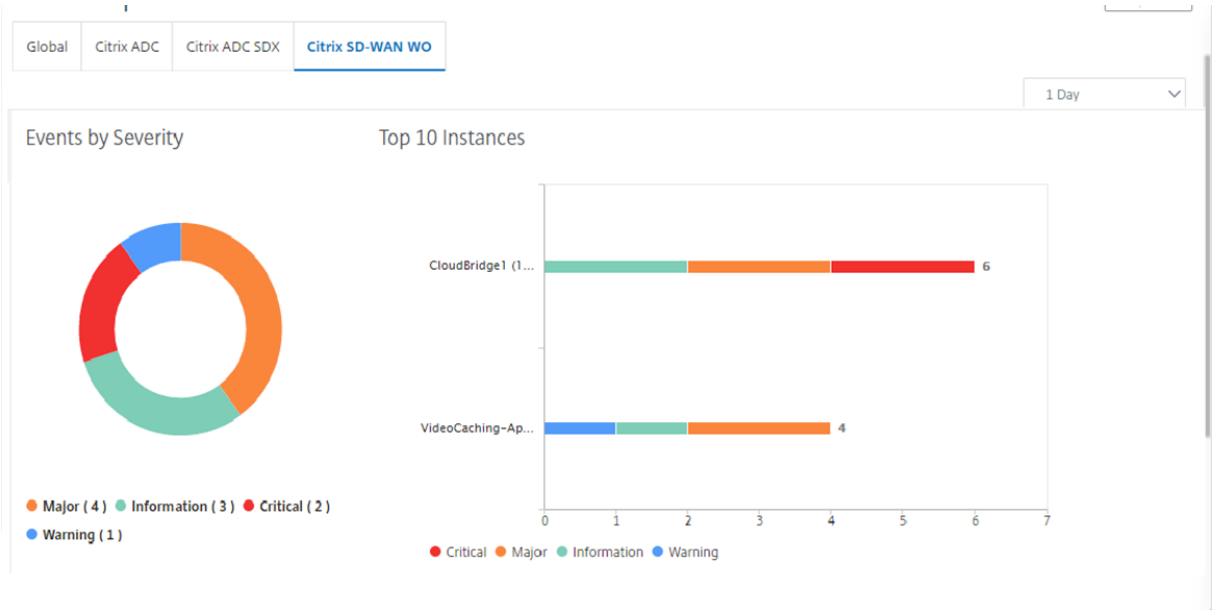
- **Name**: Name der Citrix-Appliance.
- **IP-Adresse**: IP-Adresse der Appliance.
- **WAN-Latenz**: Latenz, die durch die Client-Seite des Netzwerks verursacht wird. Das heißt, von der Citrix-Appliance bis zum Endbenutzer.
- **DC-Latenz**: Latenz, die durch die Serverseite des Netzwerks verursacht wird. Das heißt, von der Citrix-Appliance bis hin zu Back-End-Servern.
- **Status**: Erreichbarkeitsstatus des Geräts.

Ereignisberichte für Citrix SD-WANOP-Instanzen anzeigen

February 5, 2024

Sie können die Ereignisse der Top 10 SD-WANOP-Instanzen als grafische Darstellung anzeigen, indem Sie zu **Netzwerke** > **Ereignisse** > **Berichte** navigieren und **Citrix SD-WAN WO**auswählen.

Die Ereignisse werden basierend auf ihrem Schweregrad für jede Instanz angezeigt. Sie können auf jeden Schweregrad klicken, um weitere Informationen über die Anzahl der Ereignisse zu erfahren, wann es aufgetreten ist und zu welcher Kategorie es gehört.



Netzwerkberichte für Citrix SD-WANOP-Instanzen anzeigen

February 5, 2024

Sie können WAN-Optimierungsnetzwerkbezogene Berichte in Citrix ADM anzeigen. Mithilfe dieser Daten können Sie Netzwerkprobleme beheben oder das Verhalten Ihrer Citrix SD-WANOP-Geräte analysieren. Sie können die Berichte über Netzwerkstatistiken Ihrer WAN-Optimierungsgeräte für die letzten eine Stunde, einen Tag, eine Woche oder einen Monat anzeigen.

Sie können die folgenden Berichte anzeigen:

Berichte	Beschreibung
Beschleunigung	Verwenden Sie diesen Bericht, um das Muster des beschleunigten Datenverkehrs (KBPS nach Serviceklasse) und die Anzahl der beschleunigten TCP-Verbindungen zu analysieren, die die WAN-Optimierungs-Appliance durchlaufen. Dazu gehören die Anzahl der TCP-Verbindungen, die das WAN-Optimierungsgerät durchlaufen, das einer Beschleunigung unterzogen wird, die Anzahl der offenen und halb geschlossenen Verbindungen, die für die Beschleunigung ausgewählt wurden, und die Anzahl der halboffenen Verbindungen , die Kandidaten für Beschleunigung.
Verbindung durchlaufen	Verwenden Sie diesen Bericht, um die nicht beschleunigten Verbindungen für das WAN-Optimierungsgerät anzuzeigen.
Serviceklasse	Verwenden Sie diesen Bericht, um die gesendeten und empfangenen Bandbreiteneinsparungen basierend auf dem Service-Class-Typ anzuzeigen, der für das WAN-Optimierungsgerät definiert wurde.
Anwendung	Verwenden Sie diesen Bericht, um das gesendete und empfangene Datenvolumen für die Anwendungen anzuzeigen, die auf dem WAN-Optimierungsgerät ausgeführt werden.

Berichte	Beschreibung
CPU-Auslastung	Verwenden Sie diesen Bericht, um die CPU-Auslastung des WAN-Optimierungsgeräts als Prozentsatz anzuzeigen.
Kapazitätssteigerung	Verwenden Sie diesen Bericht, um das kumulative Sendekomprimierungsverhältnis für das WAN-Optimierungsgerät anzuzeigen.
Datenreduzierung	Verwenden Sie diesen Bericht, um die Sende- und Empfangsbandbreiteneinsparungen in Prozent anzuzeigen. Sie können auch die Übertragungsbandbreite analysieren und Bandbreiteneinsparungswerte für das WAN-Optimierungsgerät separat empfangen.
Link-Nutzung	Verwenden Sie diesen Bericht, um die Auslastung der Übertragungslink-Verbindung und die Empfangs-Link-Auslastung für die WAN-Optimierung in Prozent anzuzeigen.
Plugin-Nutzung	Verwenden Sie diesen Bericht, um die Anzahl der Plugins anzuzeigen, die mit dem WAN-Optimierungsgerät verbunden sind.
Paketverlust	Verwenden Sie diesen Bericht, um den Link zu sehen, der gesendete Pakete gelöscht hat und empfangene Pakete für die im WAN-Optimierungsgerät definierten Links gelöscht hat.
Durchsatz	Verwenden Sie diesen Bericht, um den Link gesendeten Volume und den Link empfangenen Volume in Bit-pro Sekunde für das WAN-Optimierungsgerät anzuzeigen.
QoS	Verwenden Sie diesen Bericht, um das Volume QOS Gesendet und QOS Empfangen in Bits-pro Sekunde für das WAN-Optimierungsgerät anzuzeigen.

So zeigen Sie Citrix SD-WANOP-Netzwerkberichtean:

1. Navigieren Sie in Citrix ADM zu **Netzwerke**> **Netzwerkberichterstattung** > **Citrix SD-WAN WO**.
2. Wählen Sie in der Dropdownliste **Berichtsname** einen Bericht aus, den Sie anzeigen möchten.

3. Wählen Sie in der Dropdownliste **Instanzen** die Citrix SD-WANOP-Instanz aus, für die Sie den Bericht anzeigen möchten.
4. Wählen Sie in der Dropdownliste **Dauer** das Zeitintervall aus.
5. Klicken Sie auf **Ausführen**.

Backup von Citrix SD-WANOP-Instanzen

February 5, 2024

Sie können den aktuellen Status einer Instanz sichern und später die gesicherten Dateien verwenden, um die Instanz in denselben Zustand wiederherzustellen. Es empfiehlt sich, eine Instanz vor dem Upgrade der Instanz oder aus vorsorglichen Gründen zu sichern. Ein Backup eines stabilen Systems ermöglicht es Ihnen, das System an einem stabilen Punkt wiederherzustellen, falls es instabil wird. Es gibt mehrere Möglichkeiten, Backups und Wiederherstellungen auf einer Citrix SD-WANOP-Instanz durchzuführen. Sie können Instanzen mit der GUI, der Befehlszeilenschnittstelle oder mit Citrix ADM sichern und wiederherstellen, um Backups durchzuführen. NetScaler ADM sichert den aktuellen Status Ihrer verwalteten Citrix SD-WANOP-Instanzen mithilfe von NITRO -Aufrufen, Secure Shell (SSH) -Protokoll und Secure Copy (SCP) -Protokoll.

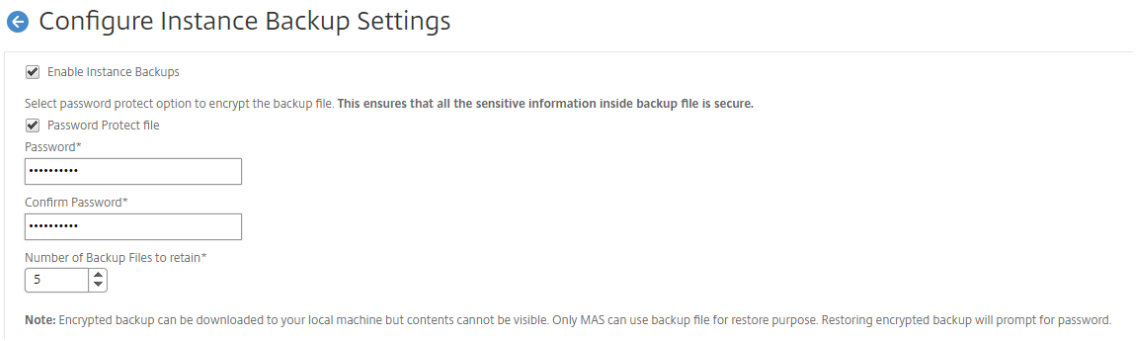
Konfigurieren der Einstellungen für das Instanzbackup

Bevor Sie ein Backup der Citrix SD-WANOP-Instanz in Citrix ADM erstellen, müssen Sie die Einstellungen für das Instanzbackup in Citrix ADM konfigurieren.

So konfigurieren Sie die Einstellungen für das Instanzbackup:

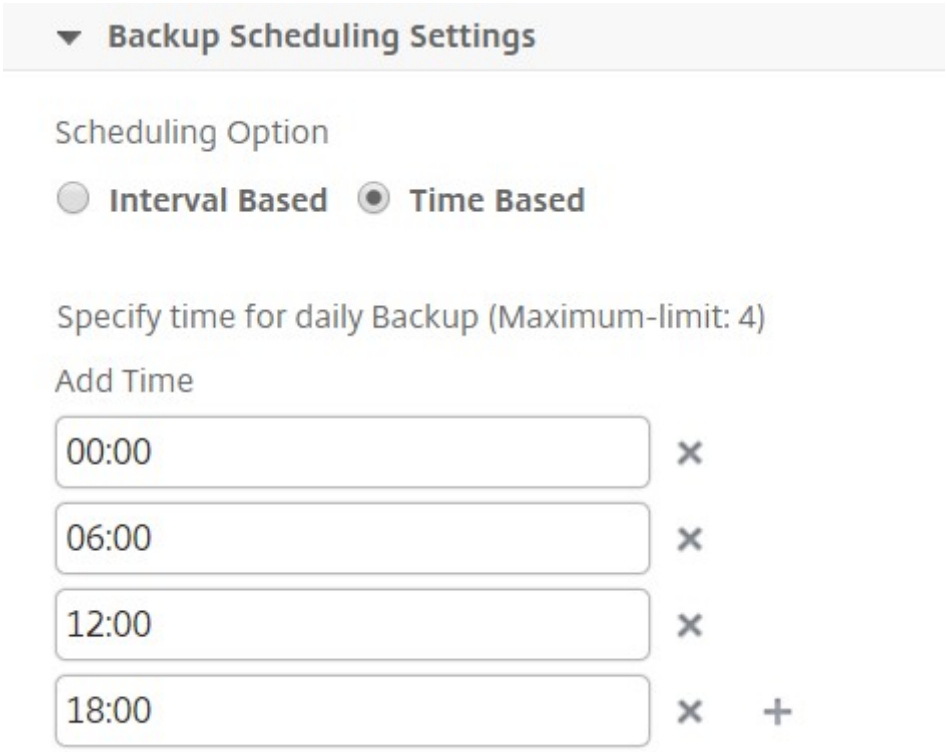
1. Navigieren Sie in NetScaler ADM zu **System** > **Systemadministration**. Wählen Sie im rechten Bereich unter **Backupeinstellungen** die Option **Einstellungen für Instanzbackup** aus.
2. Wählen Sie **Instanzbackup aktivieren** aus. Diese Option ist standardmäßig aktiviert.
3. Wählen Sie **Kennwortschutzdatei** aus, um die Backupdatei zu verschlüsseln. Durch die Verschlüsselung der Backupdatei wird sichergestellt, dass die vertraulichen Informationen in der Backupdatei sicher sind.
4. Geben Sie im Feld **Anzahl der zu beizubehaltenden Backupdateien** die Anzahl der Backupdateien an, die in NetScaler ADM aufbewahrt werden sollen. Sie können bis zu 50 Backupdateien aufbewahren.

> **Hinweis**
>
> Jede Backupdatei erfordert einige Speicheranforderungen. Citrix empfiehlt, dass Sie gemäß Ihren Anforderungen eine optimale Anzahl von Backupdateien auf Citrix ADM speichern.



5. Legen Sie die Einstellungen für die Backupplanung fest. Wählen Sie eine der folgenden Optionen:

   - **Intervallbasiert** - Nach Ablauf des angegebenen Intervalls wird in NetScaler ADM eine Backupdatei erstellt. Das Standardintervall für Backups ist 12 Stunden.
   - **Zeitbasiert** - Sie können die Zeit im Format “Stunden:Minuten”angeben, zu der das Backup erfolgen soll. Mit Citrix ADM können bis zu vier tägliche Backups auf den Instanzen durchgeführt werden.

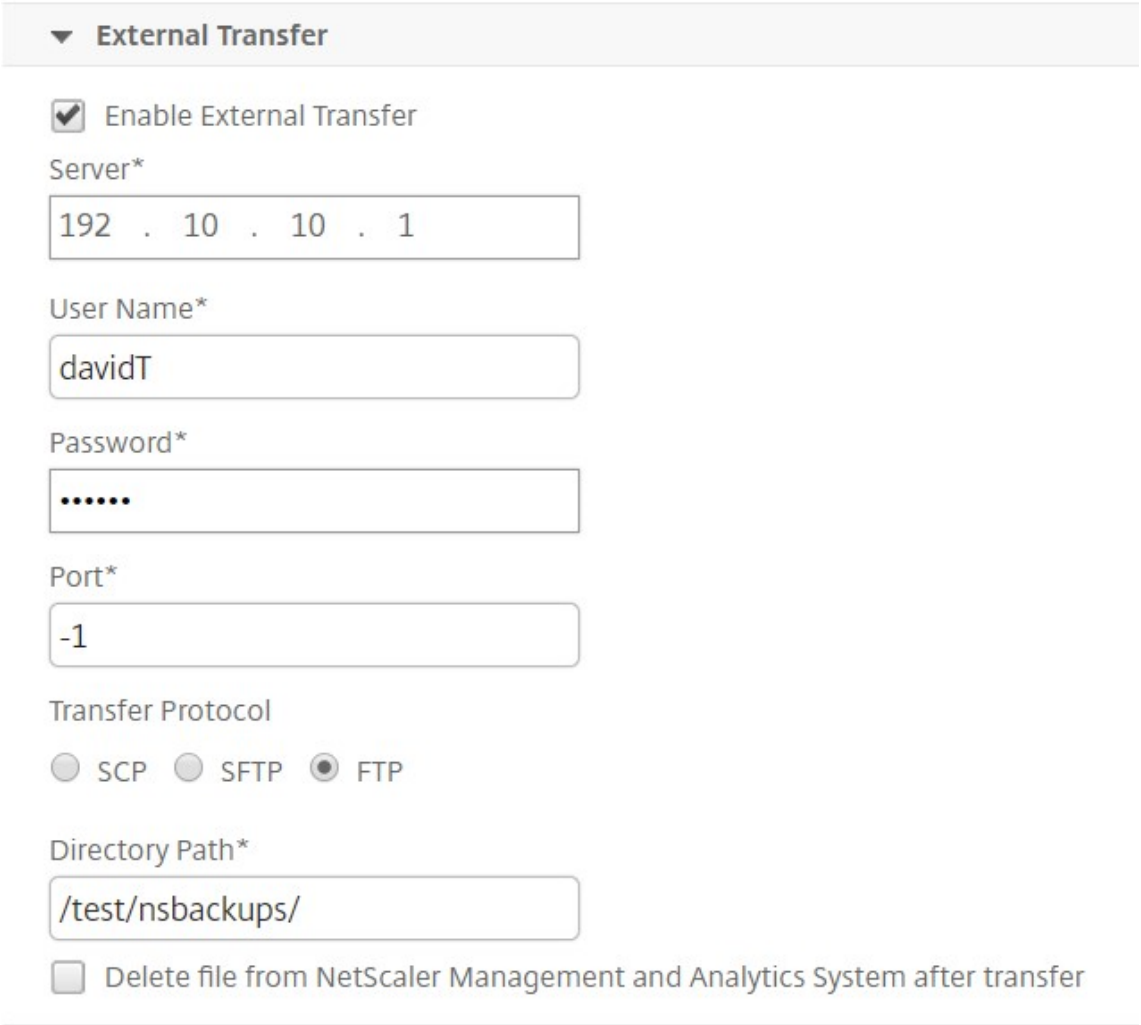


> **Hinweis**
>
> Ignorieren **Sie den Abschnitt Citrix ADC-Einstellungen**. Diese Einstellungen gelten nicht für Citrix SD-WANOP-Instanzen.

6. Wählen Sie **Externe Übertragung aktivieren**, um die Instanz-Backupdateien an einen externen Speicherort zu übertragen. Geben Sie die Werte für die folgenden Felder ein:

   - **Server**: IP-Adresse des externen Servers.
   - **Benutzername**: Benutzername des externen Servers
   - **Kennwort**: Kennwort des externen Servers.
   - **Port**: Portnummer, die für die Kommunikation mit dem externen Server verwendet wird.
   - **Übertragungsprotokoll**: Protokoll, das für die Übertragung der Backupdateien von Citrix ADM auf den externen Server verwendet wird.

   Sie können die Backupdatei auch aus Citrix ADM löschen, nachdem Sie sie auf den externen Server übertragen haben.



7. Klicken Sie auf **OK**.

> **Hinweis**
>
> NetScaler ADM sendet eine SNMP-Trap oder eine Syslog-Benachrichtigung an sich selbst, wenn ein Backupfehler für eine der ausgewählten Citrix SD-WANOP-Instanzen vorliegt.

Erstellen eines Backups der Citrix SD-WANOP-Instanz

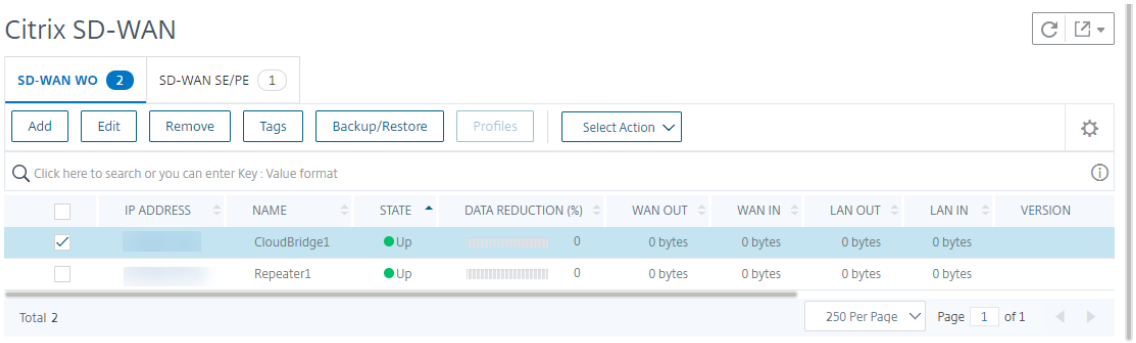
Das Verfahren zum Erstellen einer Backups für die Citrix SD-WANOP-Instanz ist für einen Administratorbenutzer unter Verwendung des standardmäßigen nsroot-Profils anwendbar.

Weitere Informationen dazu, wie ein benutzerdefinierter Benutzer ein Backp einer Citrix SD-WANOP-Instanz erstellen kann, finden Sie unter Erstellen eines Backups der Citrix SD-WANOP-Instanz für benutzerdefinierte Benutzer in diesem Thema.

Stellen Sie sicher, dass eine Citrix SD-WANOP-Instanz zu NetScaler ADM hinzugefügt wird. Weitere Informationen finden Sie unter Instanz zu NetScaler ADM hinzufügen.

So erstellen Sie ein Backup für die Citrix SD-WANOP-Instanz:

1. Navigieren Sie in Citrix ADM zu**Netzwerke** >**Instanzen** > **Citrix SD-WAN**.
2. Wählen Sie in **SD-WAN WO**die Citrix SD-WANOP-Instanz aus, die Sie sichern möchten, und klicken Sie dann auf**Backup/Restore**.



3. Klicken Sie auf der Seite **Backupdateien** auf **Backup**.
4. Verschlüsseln Sie Ihre Backupdatei mit einer der folgenden Optionen:
   - Wählen Sie **Kennwortgeschützte Datei**, und geben Sie ein Kennwort ein, um die Backupdateien zu verschlüsseln.
   - Wählen Sie **Globales Kennwort verwenden**, um das globale Kennwort zu verwenden, das Sie auf der Seite mit den Einstellungen für das Instanzbackup angegeben haben.
5. Klicken Sie auf **Backup erstellen**

Erstellen eines Backups der Citrix SD-WANOP-Instanz für benutzerdefinierte Benutzer

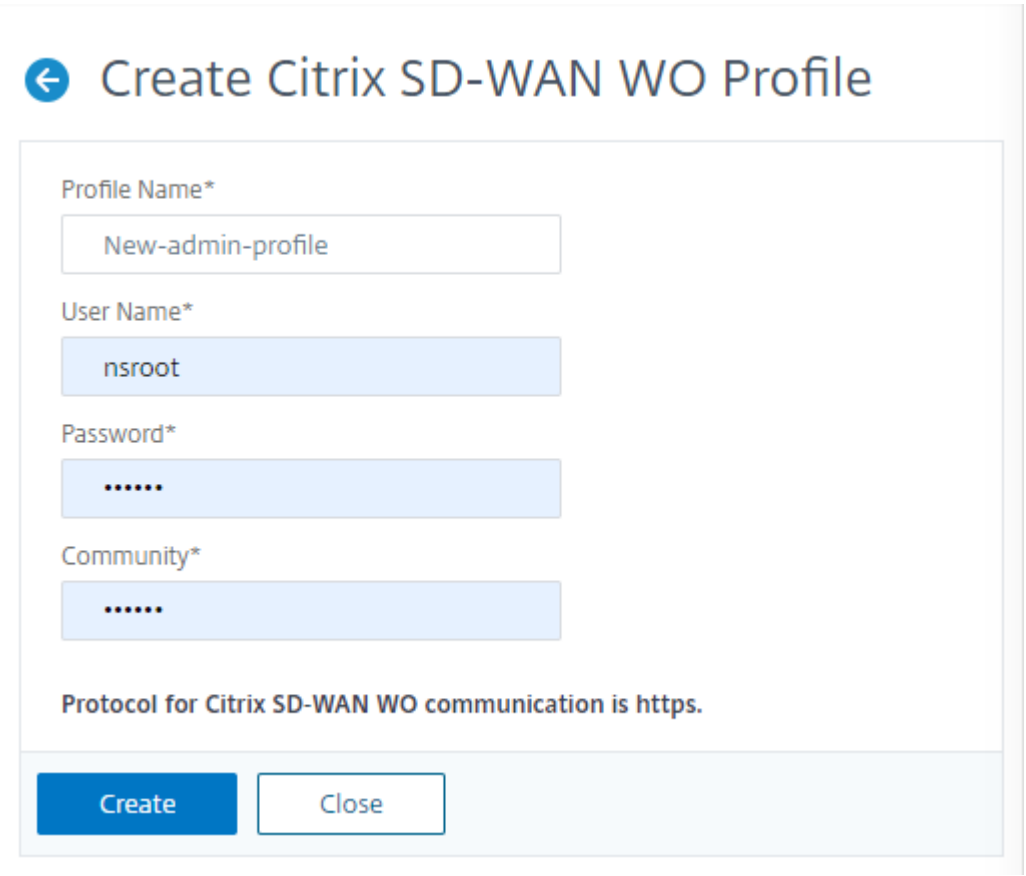
Wenn Sie einen benutzerdefinierten Benutzer mit Administratorrechten in der Citrix SD-WANOP-Instanz erstellt haben, verwenden Sie das folgende Verfahren, um eine Instanz hinzuzufügen und diese Instanz mithilfe von NetScaler ADM zu sichern.

Backup-Vorgang durch benutzerdefinierte Benutzer wird auf 400/800/1000WS/2000/2000WS/3000/4000/5000/410 SD-WANOP-Plattformen nicht unterstützt.

> **Hinweis**
>
> Citrix empfiehlt, das standardmäßige nsroot-Profil zu verwenden, während Sie ein Backup der erweiterten Citrix SD-WAN Plattformen in Citrix ADM erstellen.

So fügen Sie eine Citrix SD-WANOP-Instanz hinzu und erstellen ein Backup für einen benutzerdefinierten Benutzer:

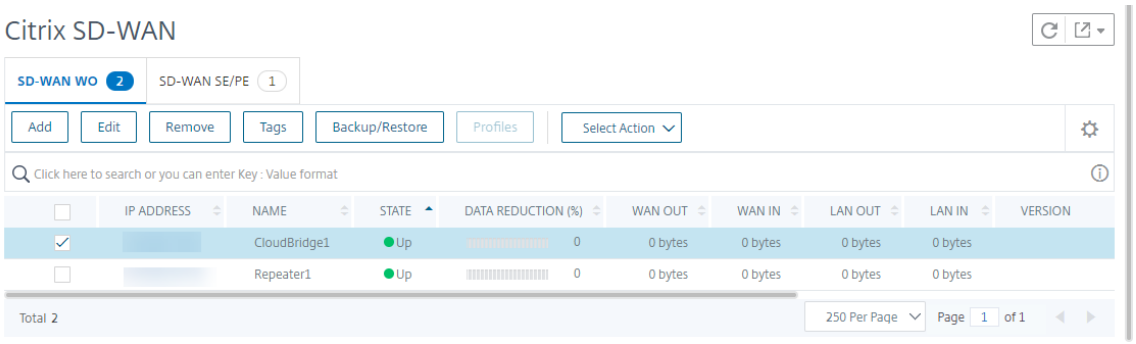
1. Navigieren Sie in Citrix ADM zu**Netzwerke** >**Instanzen** > **Citrix SD-WAN**, und wählen Sie **SD WAN WO**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse** die IP-Adresse der Citrix SD-WANOP-Instanz ein.
4. Klicken Sie neben dem Feld **Profilname** auf **Hinzufügen**, um ein neues Profil zu erstellen. Das Fenster **Citrix SD-WAN WO-Profil erstellen** wird angezeigt.



5. Geben Sie im **Feld Profilname**einen Namen für das Profil ein.
6. **Geben Sie im Feld Benutzername den Benutzernamen des benutzerdefinierten Benutzers ein, den Sie in der SD-WANOP-Instanz erstellen.**
7. Geben Sie im **Feld Kennwort**das Kennwort ein, das Sie für den benutzerdefinierten Benutzer in der SD-WANOP-Instanz festgelegt haben.
8. Geben Sie im Feld **Community** die SNMP-Kommunikationszeichenfolge ein, die auf der SD-WANOP-Appliance konfiguriert ist. (Beispiel: public)
9. Klicken Sie auf **Erstellen**.

10. Wählen Sie im Feld **Profilname** das neu erstellte Profil aus, und klicken Sie auf **OK**.

11. Navigieren Sie zu**Netzwerke** >**Instanzen** > **Citrix SD-WAN**.
12. Wählen Sie in **SD-WAN WO**die Citrix SD-WANOP-Instanz aus, die Sie gerade hinzugefügt haben, und klicken Sie dann auf**Backup/Restore**.



13. Klicken Sie auf der Seite **Backupdateien** auf **Backup**.
14. Verschlüsseln Sie Ihre Backupdatei mit einer der folgenden Optionen:

    - Wählen Sie **Kennwortgeschützte Datei**, und geben Sie ein Kennwort ein, um die Backupdateien zu verschlüsseln.
    - Wählen Sie **Globales Kennwort verwenden**, um das globale Kennwort zu verwenden, das Sie auf der Seite mit den Einstellungen für das Instanzbackup angegeben haben.

Hinweis

Sie können die verschlüsselte Backupdatei auf Ihren lokalen Computer herunterladen, aber Sie können den Inhalt nicht anzeigen. Nur Citrix ADM kann diese Backupdatei für die Wiederherstellung verwenden. Das Wiederherstellen des verschlüsselten Backups wird zur Eingabe eines Kennworts aufgefordert.

15. Klicken Sie auf **Backup erstellen**.

Wichtig!

```
1. Bei einer Citrix SD-WANOP VPX-Appliance sichert Citrix ADM
   nur die CB-Broker-Konfigurationsdatei.
```

a) Für eine erweiterte Citrix SD-WANOP-Plattform sichert Citrix ADM Folgendes:·

- CB-Broker-Konfigurationsdatei
- NTP-Konfigurationsdatei
- DNS
- SNMPD-Konfigurationsdatei
- Syslog-Konfigurationsdatei
- SSL-Zertifikat, Schlüssel und Richtlinien
- SVM-Datenbankdatei
- Komponenten (im XML-Format)
- Ressourcen (im XML-Format)

Die Dateien, die in den entsprechenden Ordnern gesichert werden, sind in der folgenden Tabelle aufgeführt. Beachten Sie, dass, wenn auf einen Ordnernamen ein “*”folgt, alle Dateien in diesem Ordner gesichert werden.

Verzeichnis	Unterverzeichnis oder Dateien
/br_makler/	cb-6bbb660a/ws.conf
/etc/	resolv.conf
/mps/	mps_devices.xml
/mpsconfig/	ssl/*, ntp.conf, snmpd.conf, syslog.conf
/mpsdb/	mpsdb_dump.sql
/ns/	NS-6CBB660A/*

/var/	mps/policy/, *mps/ssl_certs/ sdx_default_ssl_cert, mps/ssl_keys/sdx_default_ssl_key, mps/tenants/*

HAProxy-Instanzen verwalten

February 5, 2024

HAProxy ist ein Open-Source-Load Balancer, der einen Lastenausgleich für jeden TCP- oder HTTP-Dienst ausgleichen kann. Weitere Informationen zu HAProxy finden Sie unter http://www.haproxy.org/.

Citrix Application Delivery Management (Citrix ADM) unterstützt HAProxy Version 1.4.24 oder höher. Wenn Sie einen Host hinzufügen, auf dem Sie die HAProxy-Instanzen für Citrix ADM bereitgestellt haben, erkennt Citrix ADM die HAProxy-Instanzen auf dem Host und ermöglicht die Überwachung. Es zeigt Ihnen die folgenden Arten von Informationen über die HAProxy-Konfiguration auf den Instanzen:

- Frontend —Wie Anfragen an das Back-End weitergeleitet werden sollen.
- Backend —Die Gruppe von Servern, die die weitergeleiteten Anforderungen empfangen.
- Server —Die Server, unter denen HAProxy-Load den Datenverkehr ausgleicht.

Weitere Informationen finden Sie unter http://www.haproxy.org/download/1.7/doc/configuration.txt.

NetScaler ADM bietet außerdem ein HAProxy App Dashboard, auf dem Sie die Frontends in Echtzeit überwachen können. Weitere Informationen finden Sie unterHAProxy App Dashboard.

HAProxy-Instanzen zu NetScaler ADM hinzufügen

February 5, 2024

In Citrix Application Delivery Management (Citrix ADM) müssen Sie die Details des Hosts manuell hinzufügen, auf dem Sie die HAProxy-Instanz bereitgestellt haben. Nachdem Sie diese Details hinzugefügt haben, erkennt NetScaler ADM automatisch die auf dem Host bereitgestellten HAProxy-Instanzen und fügt sie zu NetScaler ADM Inventory hinzu. Es erkennt auch alle Frontends, Backends und Server, die auf den HAProxy-Instanzen konfiguriert sind, und behandelt die Frontends als erkannte Anwendungen.

Voraussetzungen

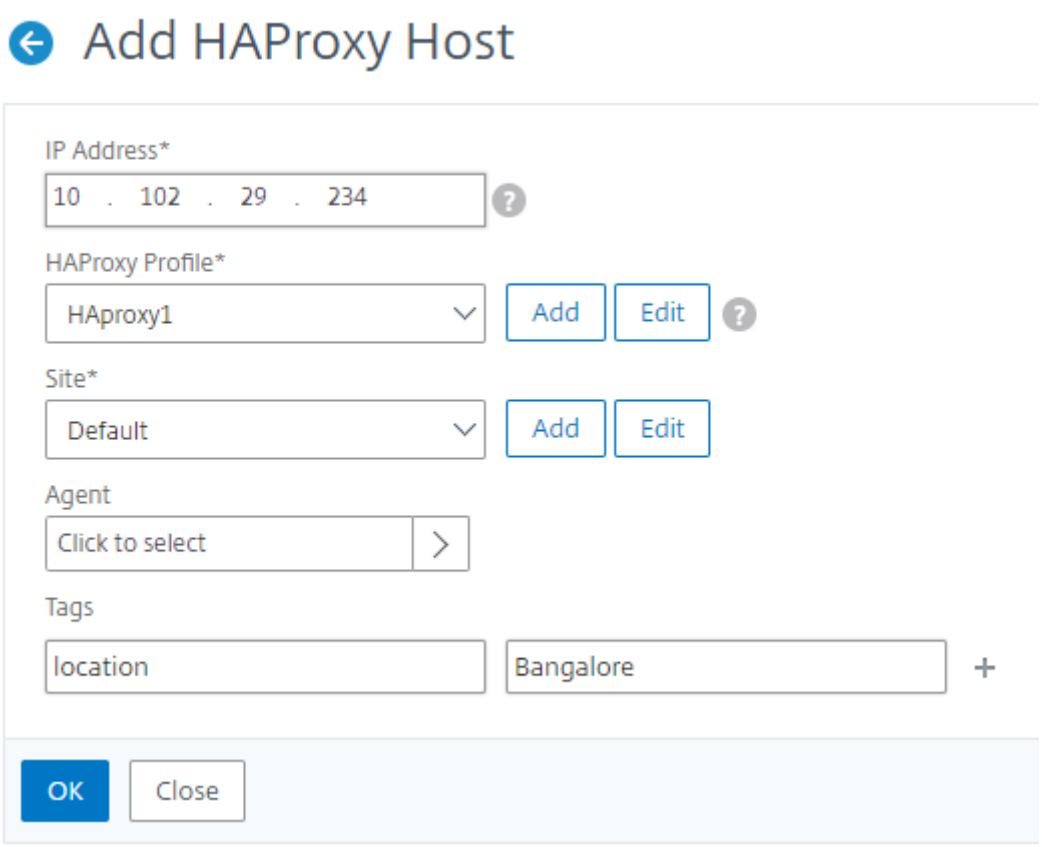
Stellen Sie sicher, dass Sie:

- Eine HAProxy-Instanz auf einem Host in Ihrer Bereitstellung bereitgestellt. Weitere Informationen finden Sie unter http://www.haproxy.org/#docs.
- Identifiziert und entschieden für die Anzahl der Frontends, für die Sie die Anwendungsstatistiken im HAProxy App Dashboard anzeigen möchten. Standardmäßig zeigt das HAProxy App Dashboard die Statistiken für 30 erkannte Anwendungen an. Weitere Informationen zum HAProxy App Dashboard finden Sie unter HAProxy App Dashboard. Wenn Sie die Statistiken von mehr als 30 erkannten Anwendungen anzeigen möchten, müssen Sie eine separate Lizenz erwerben. Weitere Informationen finden Sie unter Lizenzierung von Drittanbietern.

> **Wichtig!**
>
> NetScaler ADM benötigt Zugriff auf den Host, um die darin befindenden HAProxy-Instanzen zu erkennen. Sie können den Zugriff auf NetScaler ADM ermöglichen, indem Sie entweder das SSH-Schlüsselpaar des Hosts bereitstellen oder das Hostkennwort verwenden. Wenn Sie den Zugriff über das SSH-Schlüsselpaar bereitstellen möchten, stellen Sie sicher, dass Sie das private und öffentliche SSH-Schlüsselpaar im Host generieren und den öffentlichen Schlüssel zu den autorisierten Schlüsseln auf dem Host hinzufügen. Außerdem muss das SSH-Benutzerkonto über Superuser-Berechtigungen verfügen.

So fügen Sie NetScaler ADM eine HAProxy-Instanz hinzu:

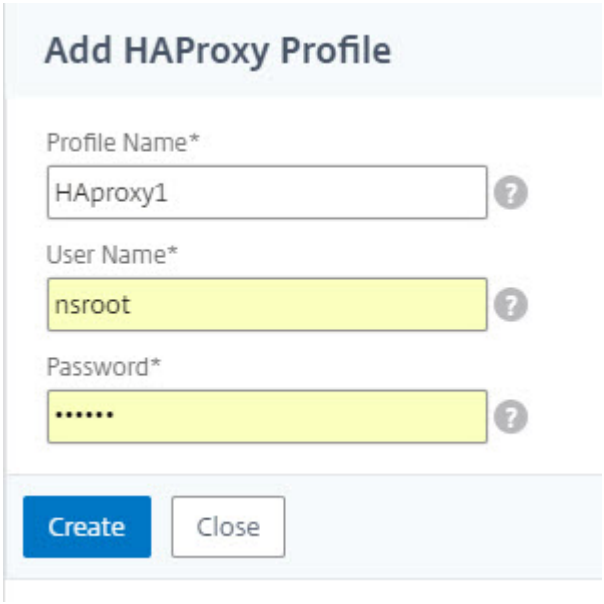
1. Navigieren Sie zu **Netzwerke** > **Instanzen**. Wählen Sie unter **InstanzenHAProxy**aus und klicken Sie auf**Hinzufügen** .
2. Führen **Sie im Dialogfeld HAProxy-Host hinzufügen** die folgenden Schritte aus:



1. Geben Sie im Feld **IP-Adresse** die IP-Adresse des Hosts ein, auf dem Sie die HAProxy-Instanzen bereitgestellt haben.

    a) Wählen Sie im Menü **HAProxy-Profil** ein vorhandenes HAProxy-Profil aus oder erstellen Sie ein neues HAProxy-Profil und wählen Sie ein neues HAProxy-Profil aus. Um ein HAProxy-Profil zu erstellen, klicken Sie auf **Hinzufügen**.

        i. Gehen **Sie im Dialogfeld HAProxy-Profil hinzufügen** folgendermaßen vor:



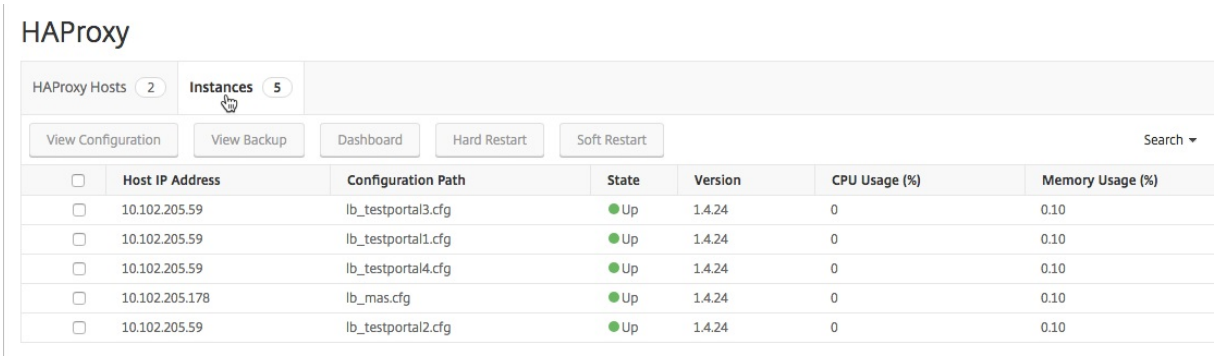
i. Geben Sie im Feld **Profilname** den Profilnamen ein.

ii. Geben Sie in die Felder **Benutzername** und **Kennwort** die Benutzeranmeldeinformationen des Hosts ein.

iii. Klicken Sie auf **Erstellen**.

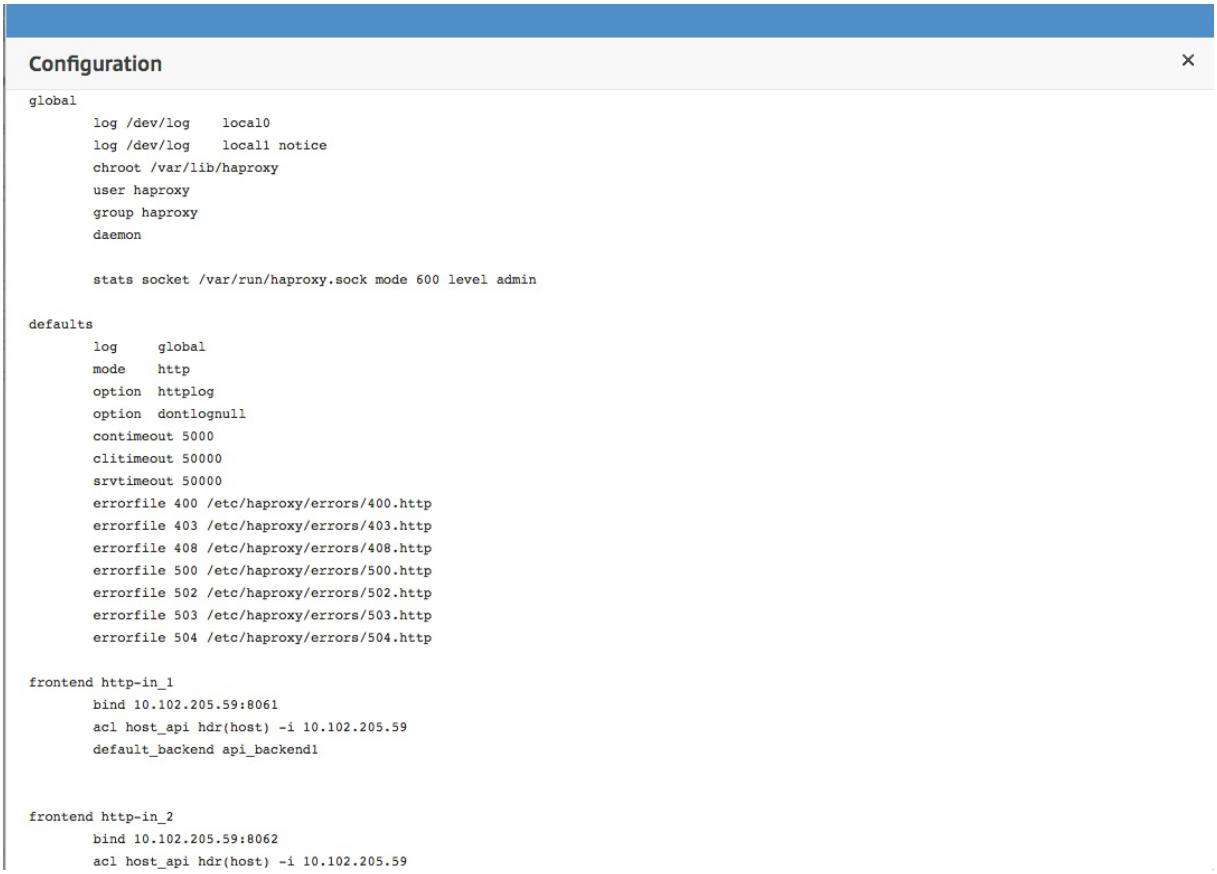
2. Wählen Sie im Menü **Site** eine HAProxy-Site aus. Um eine neue Website zu erstellen und dem Menü hinzuzufügen, klicken Sie auf **Hinzufügen**.
3. Wählen Sie im Menü **Agent** einen Agenten aus.
4. Geben Sie in die Felder "Tags"die Werte entsprechend ein.
5. Klicken Sie auf **OK**.

NetScaler ADM erkennt die auf dem Host bereitgestellten HAProxy-Instanzen und Sie können alle HAProxy-Instanzen auf der Registerkarte **Instanzen** anzeigen.



Anzeigen der Konfiguration einer HAProxy-Instanz

Um die Konfiguration einer HAProxy-Instanz in NetScaler ADM anzuzeigen, navigieren Sie zu **Netzwerke** > **Instanzen** > **HAProxy** und wählen Sie auf der Registerkarte **Instanzen** die HAProxy-Instanz aus, und klicken Sie auf **Konfiguration anzeigen**.



HAProxy-App-Dashboard

February 5, 2024

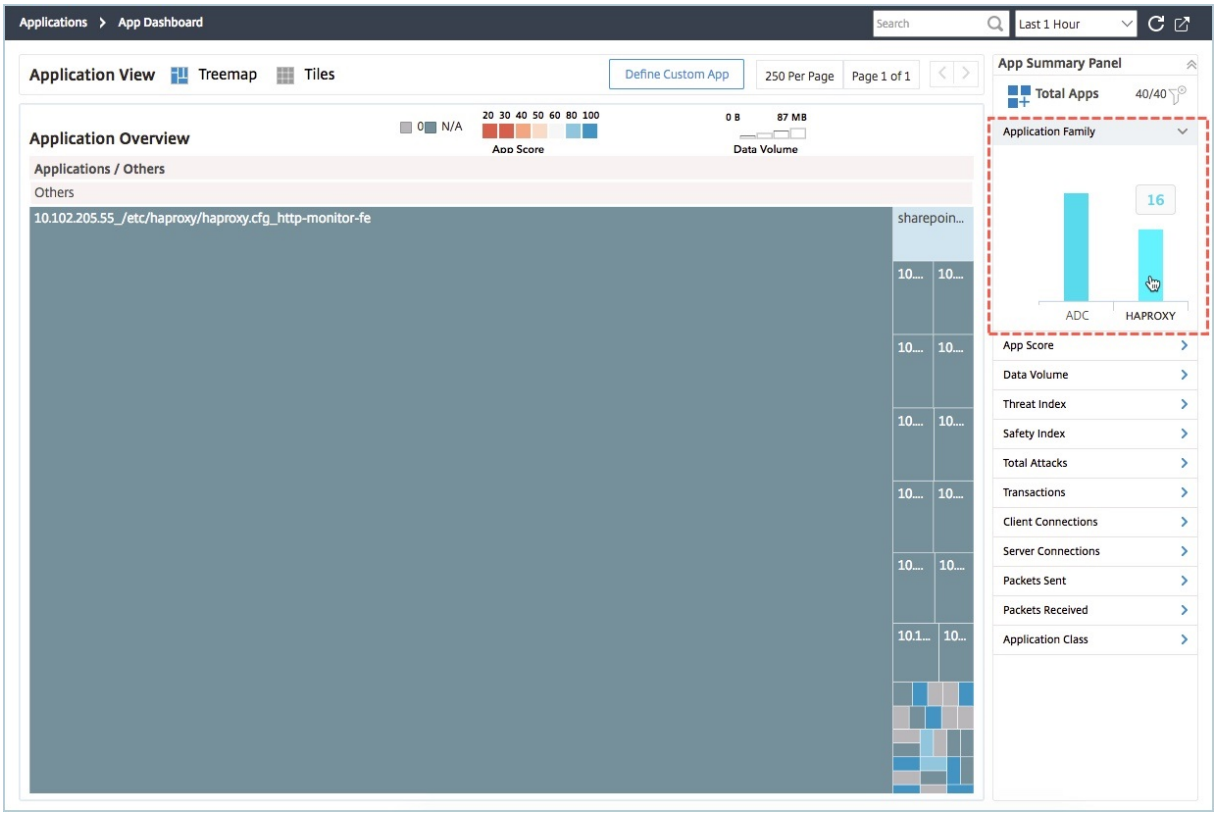
Das Application Dashboard bietet Echtzeitstatistiken über alle von NetScaler Application Delivery Management (NetScaler ADM) überwachten HAProxy-Frontends. Es listet die Front-Ends als diskrete Anwendungen auf und liefert Transaktions-, Durchsatz- und Sitzungsinformationen über die Anwendungen.

> **Wichtig!**
>
> Stellen Sie sicher, dass Sie **Statistiken** in der HAProxy-Instanzkonfigurationsdatei aktivieren. Um **Statistiken**zu aktivieren, bearbeiten Sie Ihre HAProxy-Konfigurationsdatei und fügen Sie nach

> dem Standardabschnitt einen Eintrag hinzu, der dem im folgenden Beispiel ähnelt:

```
    listen stats :9000  # Listen on localhost:9000
    mode http
    stats enable  # Enable stats page
    stats hide-version  # Hide HAProxy version
    stats realm Haproxy\ Statistics  # Title text for popup window
    stats uri /haproxy_stats  # Stats URI
    stats auth Username:Password  # Authentication credentials
<!--NeedCopy-->
```

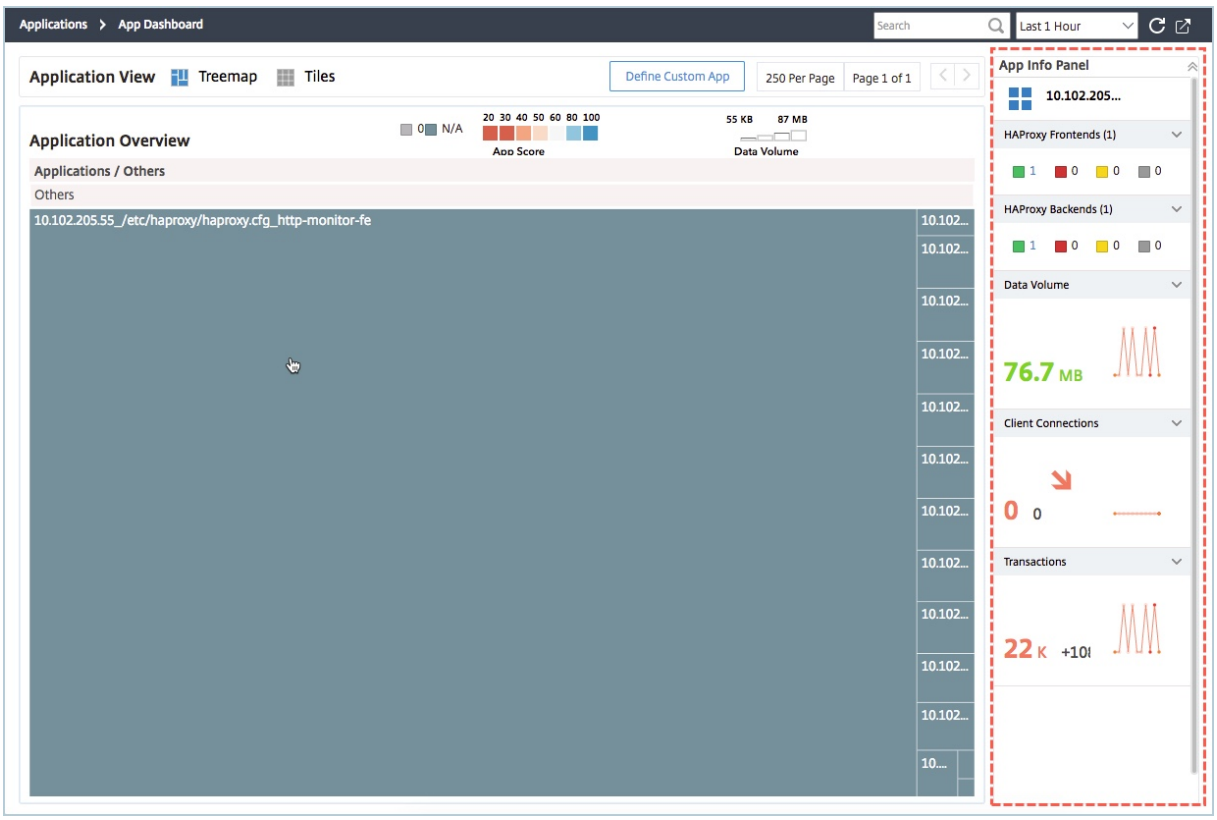
Um auf die HAProxy-Anwendung im Application Dashboard in Citrix ADM zuzugreifen, navigieren Sie nach dem Hinzufügen der HAProxy-Instanzen zu Citrix ADM zu **Anwendungen** > **Dashboard**. Sie können das Dashboard so filtern, dass nur die HAProxy-Anwendung angezeigt wird. Um das Dashboard zu filtern, wählen Sie **HAPROXY**, das im Abschnitt **Anwendungsfamilie** im Bereich App-Zusammenfassung angezeigt wird.



Wichtige Metriken der HAProxy-Anwendung anzeigen

Das **App-Info-Bedienfeld** befindet sich auf der ersten Ebene, wenn Sie einen Drilldown für eine HAProxy-Anwendung erstellen. Es zeigt die wichtigsten Metriken und Komponenten der Anwendung zusammen mit ihrem Status an. Beispielsweise zeigt das **App-Info-Bedienfeld** für jede ausgewählte HAProxy-Anwendung die Gesamtzahl der HAProxy-Frontends, die Gesamtzahl der HAProxy-Backends,

das Datenvolumen, den Trend der Clientverbindungen und die Transaktionen an. Um die wichtigsten Metriken der HAProxy-Anwendung anzuzeigen, klicken Sie im Anwendungs-Dashboard auf die **HAProxy-Anwendungskachel**. Der Bereich „ **App-Informationen** “ersetzt dann den Bereich „ **App-Zusammenfassung** “.

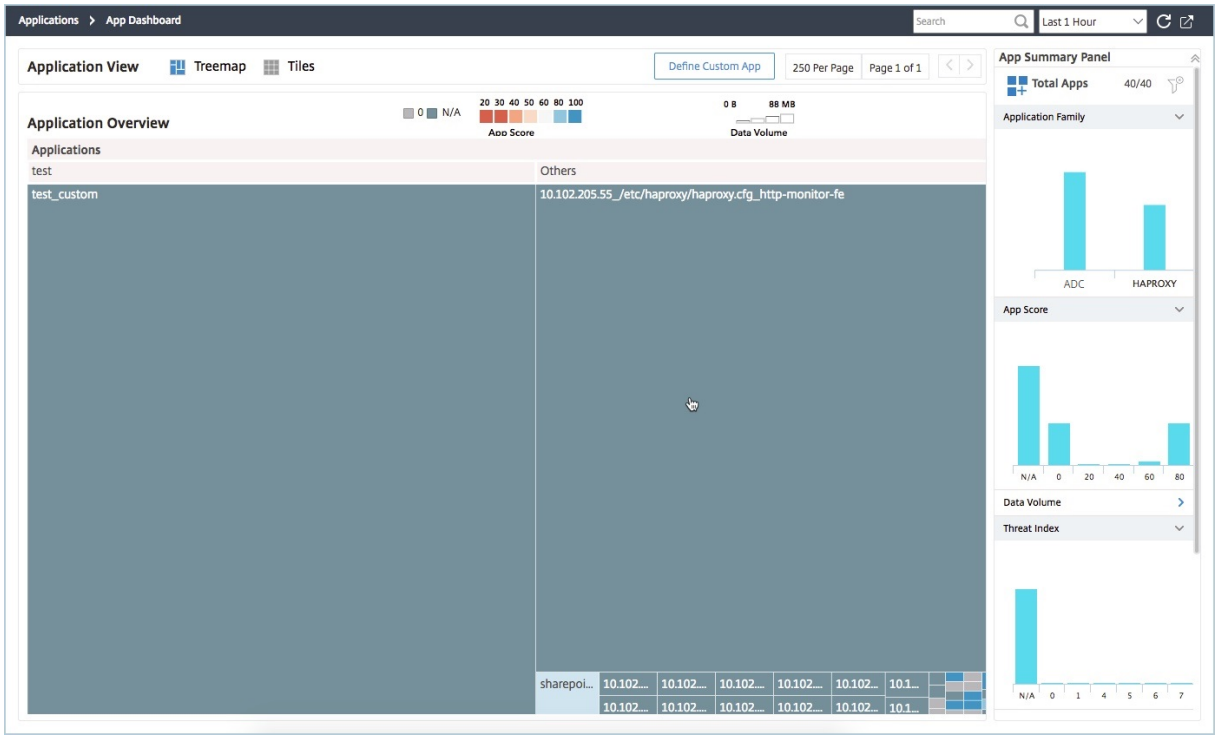


Anzeigen der Echtzeit-Performance der HAProxy-Anwendung

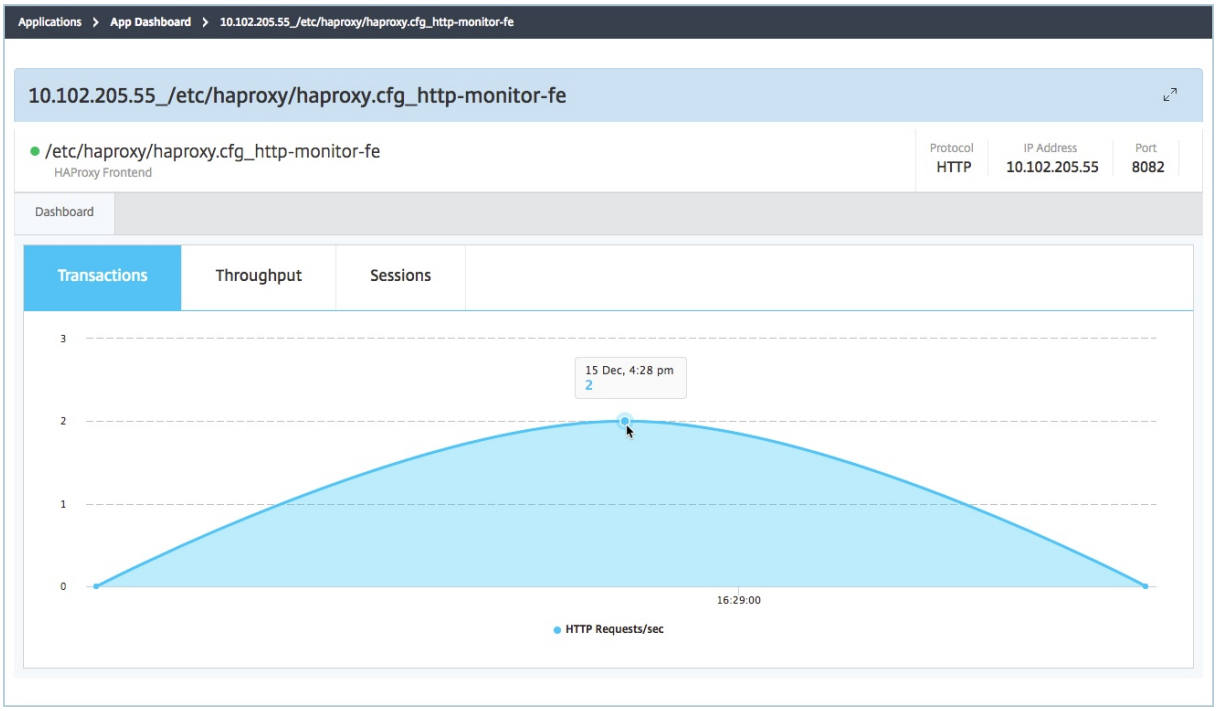
Mit Citrix ADM können Sie die Echtzeit-Performance Ihrer HAProxy-Anwendungen anzeigen. Es liefert die folgenden Echtzeit-Details der ausgewählten HAProxy-Anwendung:

- **Transaktionen.** Transaktionen, die von der Anwendung durchgeführt werden.
- **Durchsatz.** Durchsatz der Anwendung.
- **Sitzungen.** Anzahl der Sitzungen, die von der Anwendung erstellt wurden.

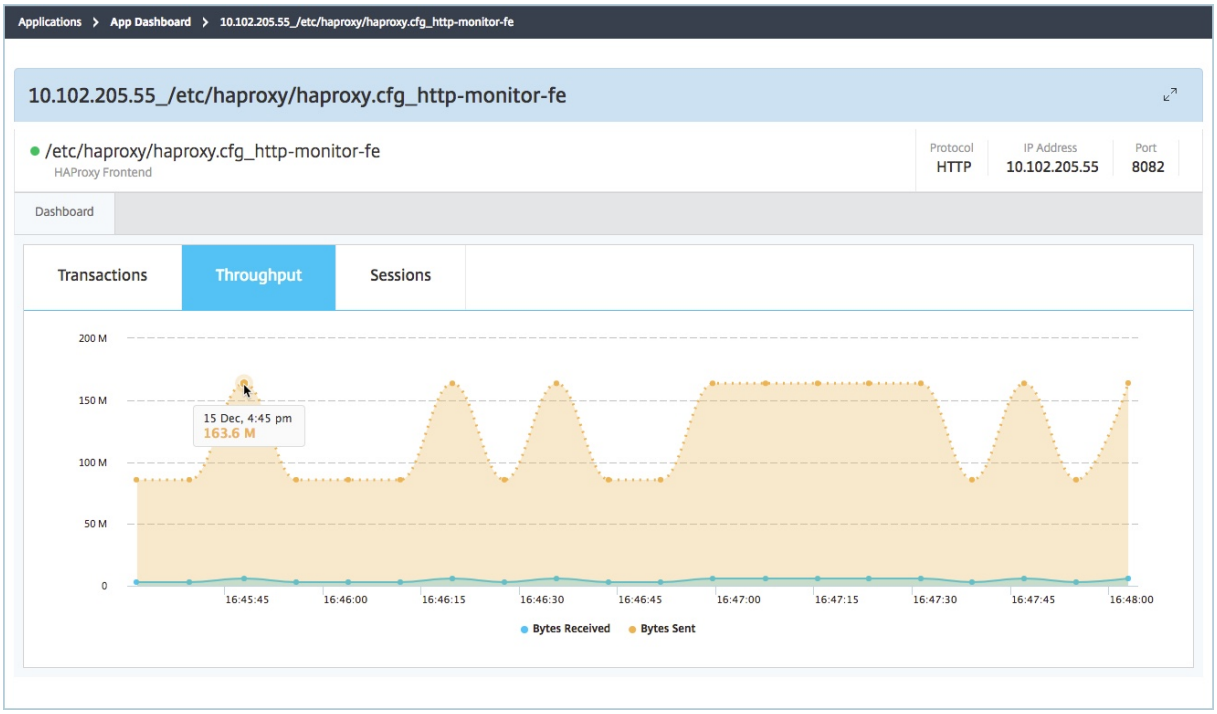
Um die Echtzeit-Performance Ihrer HAProxy-Anwendung anzuzeigen, doppelklicken Sie im **Application Dashboard**auf die HAProxy-Anwendungskachel.



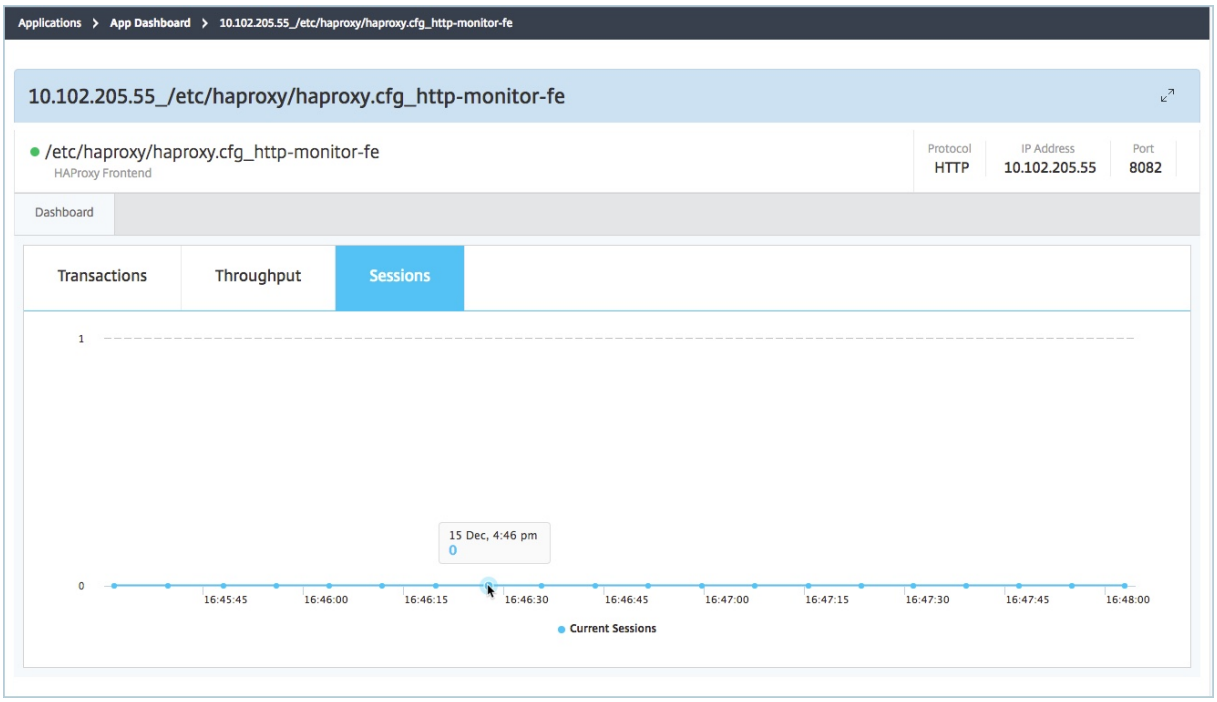
Standardmäßig ist die Registerkarte **Transaktionen** ausgewählt, und die Echtzeit-Transaktionen, die von der Anwendung ausgeführt werden, werden angezeigt.



Um den Echtzeitdurchsatz der Anwendung anzuzeigen, klicken Sie auf die Registerkarte **Durchsatz**.



Sie können auf die Registerkarte **Sitzungen** klicken, um die Anzahl der Sitzungen anzuzeigen, die von der Anwendung in Echtzeit eingerichtet wurden.

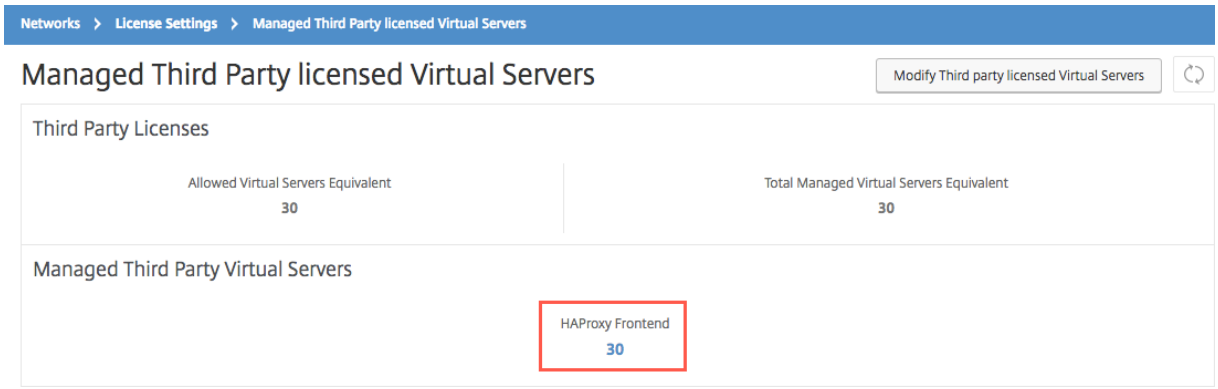


Lizenzierung von Drittanbietern

February 5, 2024

Nachdem Sie die Hosts zu NetScaler Application Delivery Management (NetScaler ADM) hinzugefügt haben, erkennt NetScaler ADM automatisch die auf den Hosts bereitgestellten HAProxy-Instanzen und fügt sie zu NetScaler ADM Inventory hinzu. Es erkennt auch alle Frontends, Backends und Server, die auf den HAProxy-Instanzen konfiguriert sind, und betrachtet die Frontends als erkannte Anwendungen.

Sie können alle erkannten Anwendungen verwalten und überwachen, aber standardmäßig zeigt das HAProxy App Dashboard die Anwendungsstatistiken für 30 erkannte Anwendungen an. Weitere Informationen zum HAProxy App Dashboard finden Sie unter HAProxy App Dashboard. Wenn Sie die Anwendungsstatistiken von mehr als 30 erkannten Anwendungen anzeigen möchten, müssen Sie eine separate Lizenz erwerben.



Lizenzen für mehr Frontends sind in virtuellen Serverpacks von 100 verfügbar. Sie können eine gültige Lizenz abrufen und die Lizenz mit der NetScaler ADM GUI installieren.

Installieren Sie die Drittanbieter-Liz

Sie können eine Lizenz auf NetScaler ADM installieren, um die Anwendungsstatistiken von mehr als 30 erkannten Anwendungen anzuzeigen.

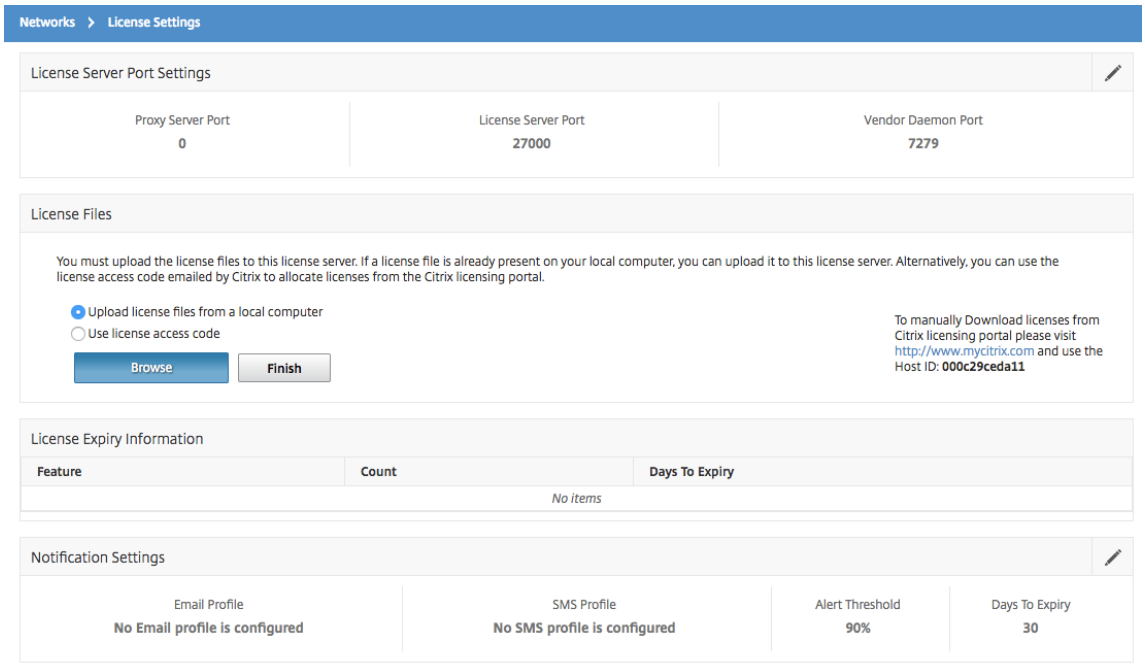
So installieren Sie eine Lizenz:

1. Navigieren Sie zu **Netzwerke** > **Lizenzen**.
2. Wählen Sie im Abschnitt **Lizenzdateien** eine der folgenden Optionen aus:
    - **Laden Sie Lizenzdateien von einem lokalen Computer hoch.** Wenn bereits eine Lizenz auf Ihrem lokalen Computer vorhanden ist, klicken Sie auf Durchsuchen, und wählen Sie

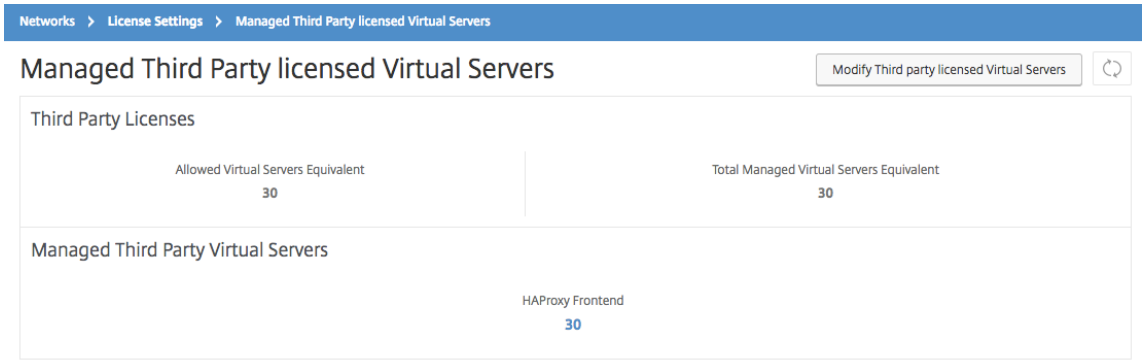
die Lizenzdatei (.lic) aus, die Sie für die Zuweisung Ihrer Lizenzen verwenden möchten. Klicken Sie auf **Fertig stellen**.

- **Lizenzaktivierungscode verwenden** - Citrix sendet den Lizenzschlüssel für die erworbene Lizenz per E-Mail. Geben Sie den Lizenzschlüssel in das Textfeld ein und klicken Sie dann auf **Lizenzen abrufen**.

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



Sie können die auf Ihrem NetScaler ADM installierten Lizenzen überprüfen, indem Sie zu "**Netzwerke** "> "**Lizenzen** "> "**Drittanbieterlizenzen**"navigieren.

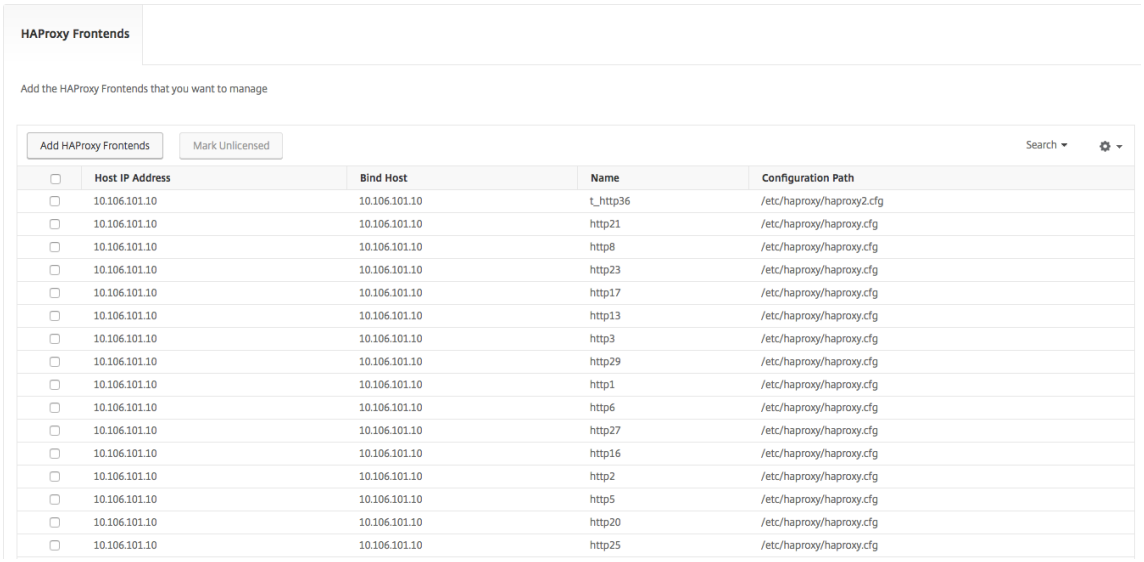


Verwaltung der Lizenzen von Drittanbietern

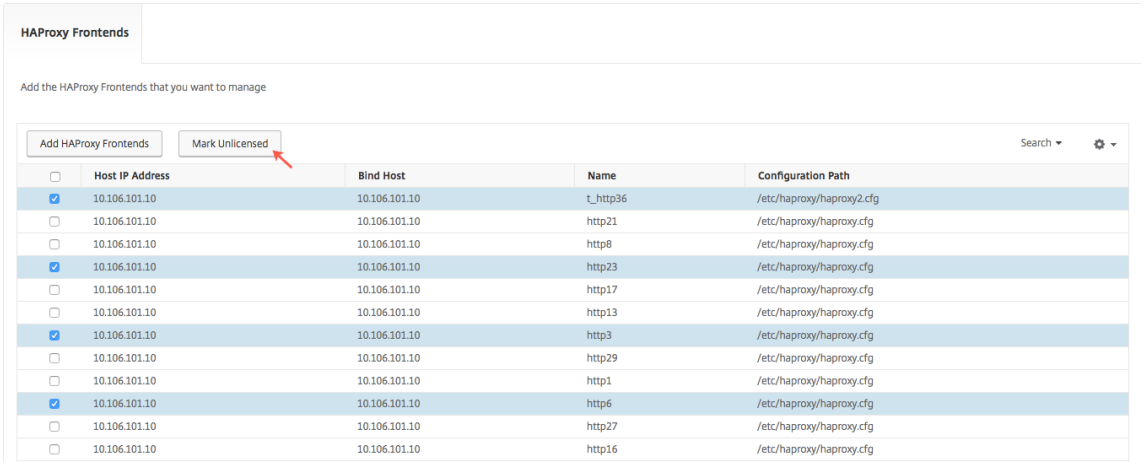
NetScaler ADM wählt die erkannten Anwendungen in den HAProxy-Instanzen nach dem Zufallsprinzip aus und lizenziert sie automatisch. Wenn Sie die ausgewählten erkannten Anwendungen ändern möchten, müssen Sie die Lizenzierung der lizenzierten erkannten Anwendungen manuell aufheben und dann die Lizenzen den erkannten Anwendungen zuweisen, die Sie lizenzieren möchten.

So verwalten Sie die Lizenzen von Drittanbietern:

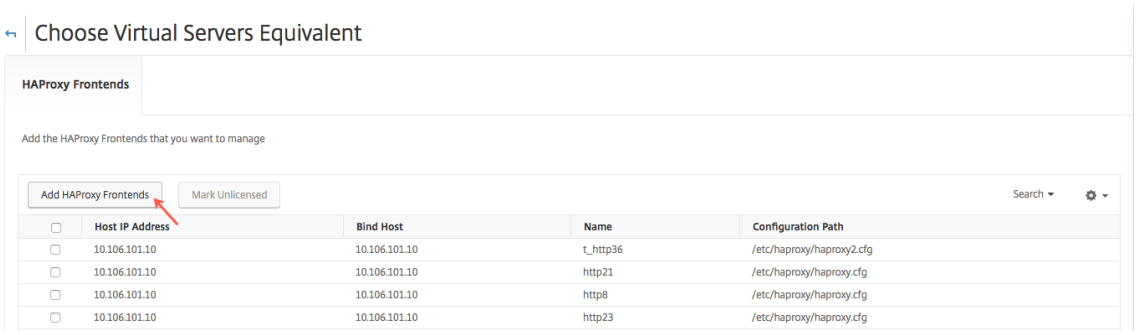
1. Navigieren Sie zu **Netzwerke** > **Lizenzen > Lizenzen** von **Drittanbietern**, und klicken Sie auf **Virtuelle Server von Drittanbietern ändern**. Das Dashboard zeigt die verwalteten Frontends an.



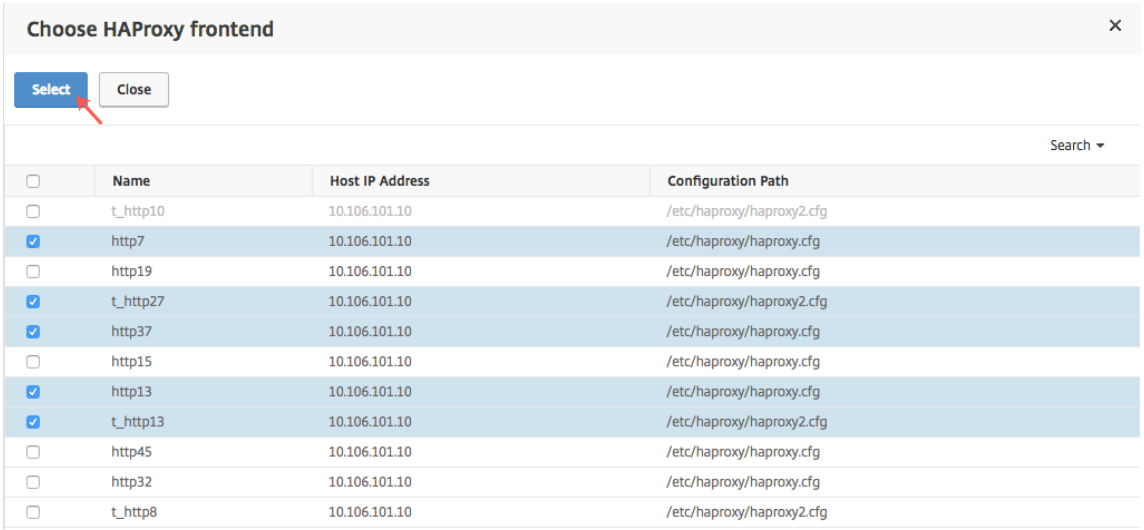
2. Wählen Sie die Frontends aus der Liste **Mark Unlicensed**aus und klicken Sie auf **Fertig stellen**, um die Lizenzen freizugeben.



3. Nachdem Sie die Lizenzen freigegeben haben oder bereits Lizenzen verfügbar sind, klicken Sie auf **HAProxy-Frontends hinzufügen**.



4. **Wählen Sie im Dialogfeld "HAProxy-Frontend** auswählen"die nicht lizenzierten Front-Ends aus der Liste aus und klicken Sie auf **Auswählen**.



5. Klicken Sie auf **Jetzt beenden**.

Rollenbasierte Zugriffssteuerung für HAProxy-Instanzen

February 5, 2024

Citrix Application Delivery Management (Citrix ADM) verwendet eine feinkörnige, rollenbasierte Zugriffssteuerung (RBAC), um den Zugriff auf Konfigurationsobjekte zu steuern. Sie können beispielsweise Benutzer erstellen und ihnen Zugriff auf bestimmte Instanzen von HAProxy gewähren. Außerdem können Sie für HAProxy App Dashboard die Berechtigung "Nur Lese-/Lesezugriff"festlegen. Weitere Informationen finden Sie unter Rollenbasierte Zugriffssteuerung in NetScaler ADM.

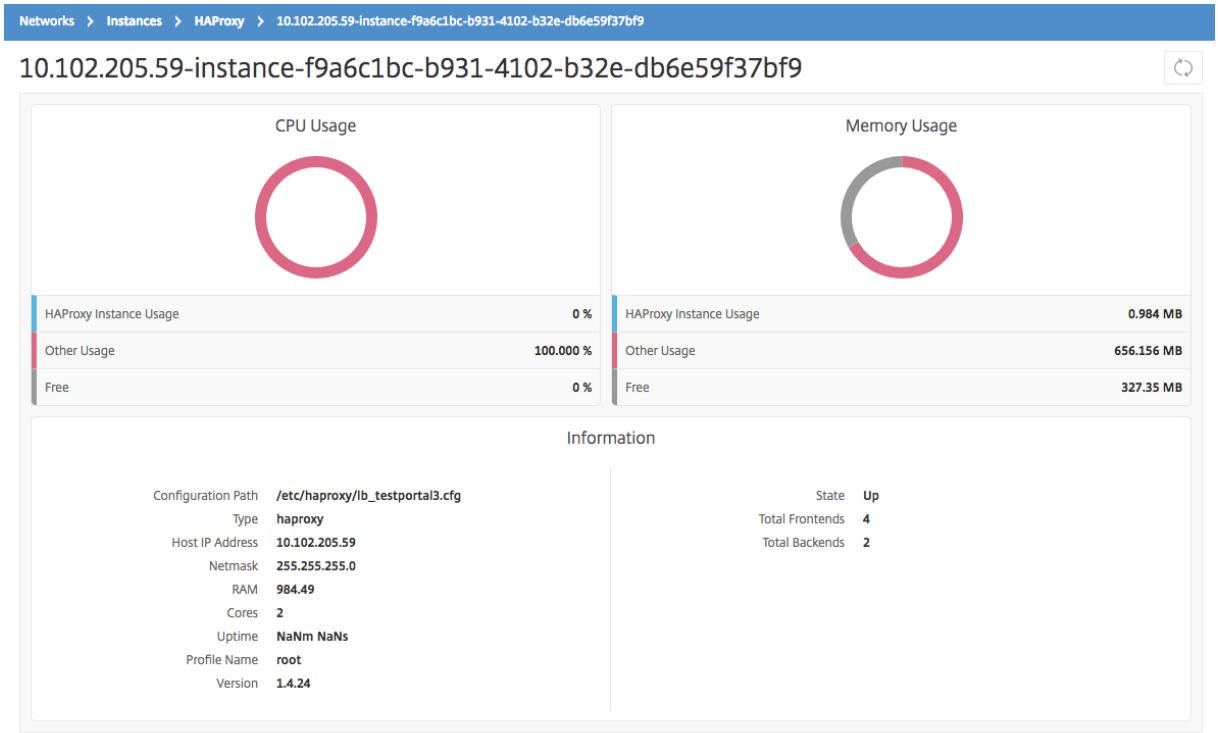
HAProxy-Instanzen überwachen

February 5, 2024

Das HAProxy-Dashboard in Citrix Application Delivery Management (Citrix ADM) zeigt Diagramme an, mit denen Sie die CPU- und Speicherauslastung einer HAProxy-Instanz verfolgen können. Das Dashboard zeigt außerdem Diagramme an, die Folgendes anzeigen:

- Prozentsatz der CPU, die von der HAProxy-Instanz auf dem Host verwendet wird.
- Prozentsatz der CPU, die von anderen Entitäten auf dem Host verwendet wird.
- Prozentsatz der verbleibenden CPU auf dem Host.
- Prozentsatz des Speichers, der von der HAProxy-Instanz auf dem Host belegt wird.
- Prozentsatz des Speichers, der von anderen Entitäten auf dem Host verwendet wird.
- Prozentsatz des verbleibenden Speichers auf dem Host.

Um eine HAProxy-Instanz in NetScaler ADM zu überwachen, navigieren Sie zur Registerkarte **Netzwerke** > **Instanzen** > **HAProxy** > **Instanzen**, wählen Sie die HAProxy-Instanz aus und klicken Sie auf **Dashboard**.



Zeigen Sie die Details der auf HAProxy-Instanzen konfigurierten Front-Ends an

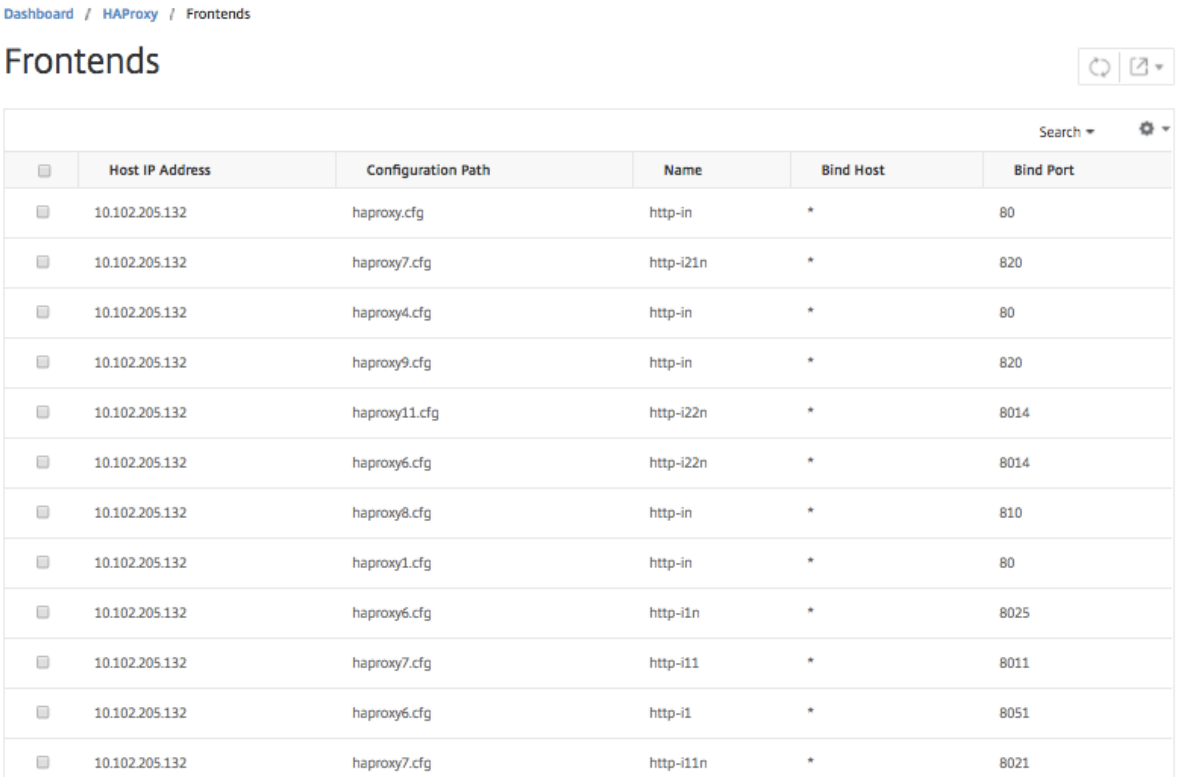
February 5, 2024

NetScaler Application Delivery Management (NetScaler ADM) gibt die folgenden Details des für eine HAProxy-Instanz konfigurierten Front-End an:

- **Host-IP-Adresse**. IP-Adresse des Hosts
- **Konfigurationspfad**.Absoluter Konfigurationspfad der HAProxy-Instanz auf dem Host.
- **Name**. Name des Front-Endes, das den eingehenden Verkehr verarbeitet.
- **Host binden**. IP-Adresse, an die das Front-End gebunden ist.
- **Port binden**. Port, an den das Frontend gebunden ist.

So zeigen Sie das für die HAProxy-Instanzen konfigurierte Front-End an:

Navigieren Sie in NetScaler ADM zu **Netzwerke > Netzwerkfunktionen > HAProxy > Frontends**.



Zeigen Sie die Details der auf HAProxy-Instanzen konfigurierten Backends an

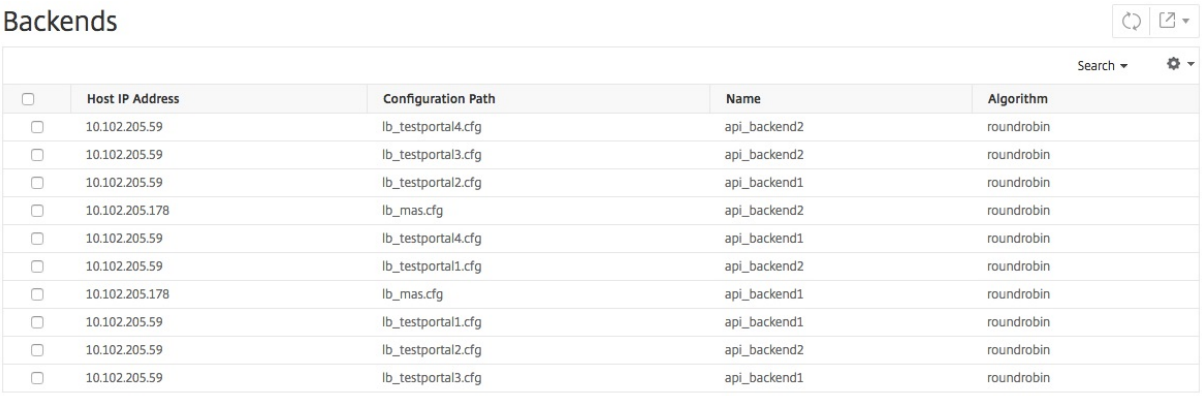
February 5, 2024

NetScaler Application Delivery Management (NetScaler ADM) gibt die folgenden Details einer Backend-Anwendung an, die auf einer HAProxy-Instanz konfiguriert ist:

- **Host-IP-Adresse**. IP-Adresse des Hosts.
- **Konfigurationspfad**. HAProxy-Instanzpfad auf dem Host.
- **Name**. Name des Backends, an das der Traffic weitergeleitet wird.
- **Algorithmus**. Lastausgleichsalgorithmus, der zum Ausgleich des Datenverkehrs verwendet wird.

So zeigen Sie das für die HAProxy-Instanzen konfigurierte Backend an:

Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Netzwerkfunktionen** > **HAProxy** > **Backends**.



Details der auf HAProxy-Instanzen konfigurierten Server anzeigen

February 5, 2024

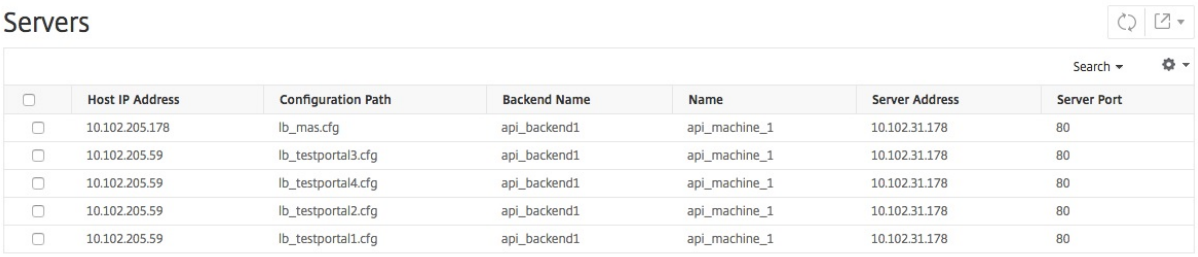
Citrix Application Delivery Management (Citrix ADM) meldet die folgenden Details zu Servern, die auf einer HAProxy-Instanz konfiguriert sind:

- **Host-IP-Adresse**. Name des Hosts.
- **Konfigurationspfad**.Absoluter Pfad der HAProxy-Instanzkonfigurationsdatei auf dem Host.
- **Backend-Name**. Der Name des Backends in der HAProxy-Konfiguration.
- **Name**. Name des Servers in der HAProxy-Konfiguration.
- **Server-Adresse**. IP-Adresse des Servers.

- **Server-Port**. Port, der vom Server verwendet wird.

So zeigen Sie die Server an, die auf den HAProxy-Instanzen konfiguriert sind:

Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Netzwerkfunktionen** > **HAProxy** > **Server**.

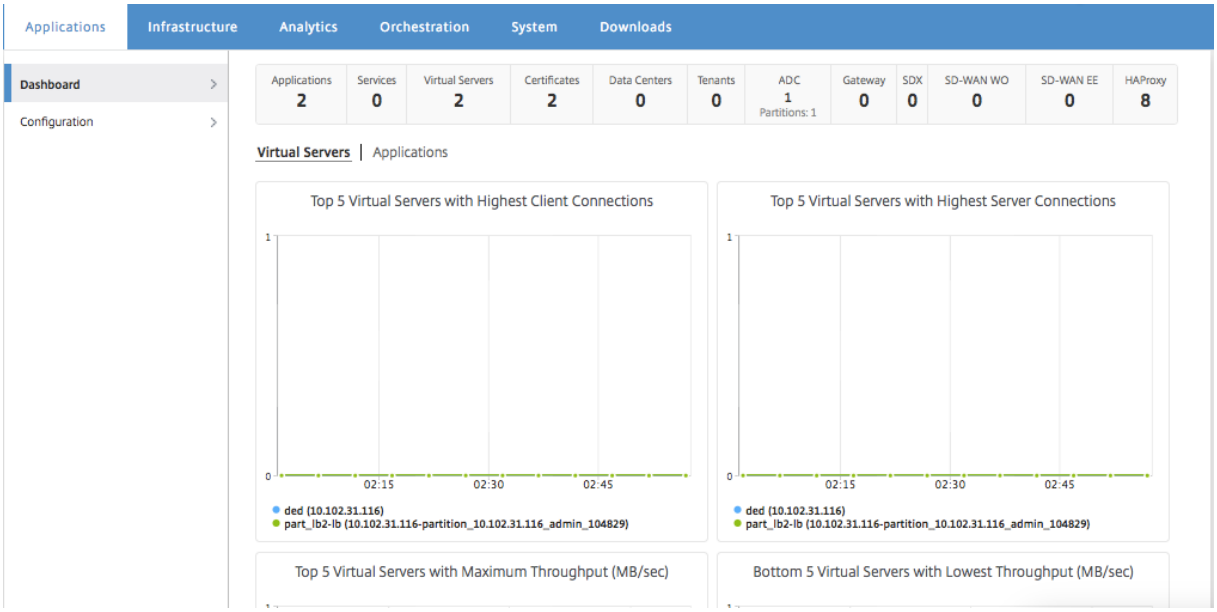


Zeigen Sie die HAProxy-Instanzen mit der höchsten Anzahl an Front-Ends oder Servern an

February 5, 2024

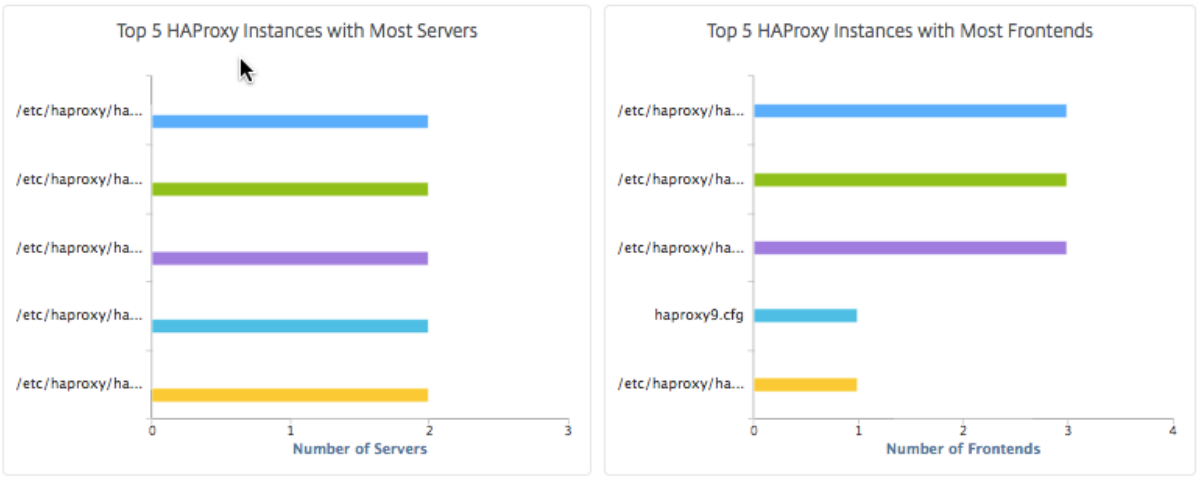
Im **Application Dashboard**zeigt NetScaler Application Delivery Management (NetScaler ADM) die Anzahl der von ihm erfundenen HAProxy-Instanzen an und listet die fünf wichtigsten HAProxy-Instanzen auf, die mit der höchsten Anzahl von Front-Ends oder Servern konfiguriert sind.

Um das **Application Dashboard**anzuzeigen, navigieren Sie in NetScaler ADM zu **Anwendungen** > **Dashboard**.



Die Anzahl der von NetScaler ADM erkannten HAProxy-Instanzen wird in der obersten Reihe angezeigt:

Um die Liste der fünf wichtigsten HAProxy-Instanzen anzuzeigen, die mit der höchsten Anzahl von Front-Ends oder der höchsten Anzahl von Servern konfiguriert sind, scrollen Sie im Dashboard nach unten:



HAProxy-Instanz neu starten

February 5, 2024

Um eine HAProxy-Instanz von der Citrix Application Delivery Management (Citrix ADM) -GUI neu zu starten, können Sie entweder einen harten Neustart oder einen weichen Neustart auswählen.

Fester Neustart

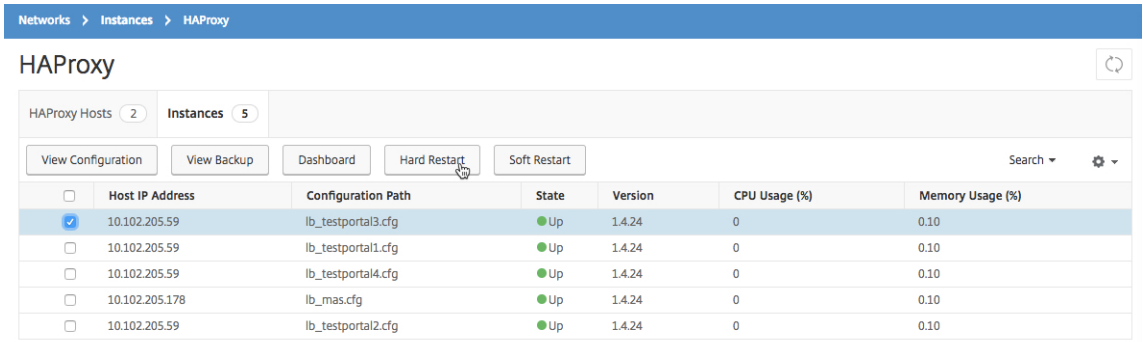
Ein harter Neustart beendet den HAProxy-Prozess auf der Instanz und schließt alle etablierten Verbindungen. Nach dem Neustart wird ein neuer HAProxy-Prozess erstellt und die nachfolgenden neuen Verbindungen werden durch den neuen HAProxy-Prozess verarbeitet.

Sanfter Neustart

Der Softrestart hetzt den HAProxy-Prozess vom Listening-Port auf, aber der HAProxy-Prozess verarbeitet weiterhin bestehende Verbindungen, bis sie schließen. Ein neuer HAProxy-Prozess wird erstellt, um neue Verbindungen zu verarbeiten.

Führen Sie die folgenden Schritte aus, um eine HAProxy-Instanz neu zu starten:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **HAProxy**, und klicken Sie auf die Registerkarte **Instanz**.
2. Wählen Sie auf der Registerkarte **Instanz** die HAProxy-Instanz aus, die Sie neu starten möchten.
3. Klicken Sie auf **Hard Restart**, um die HAProxy-Instanz hart neu zu **starten, oder klicken Sie auf Soft Restart**, um die HAProxy-Instanz neu zu starten.



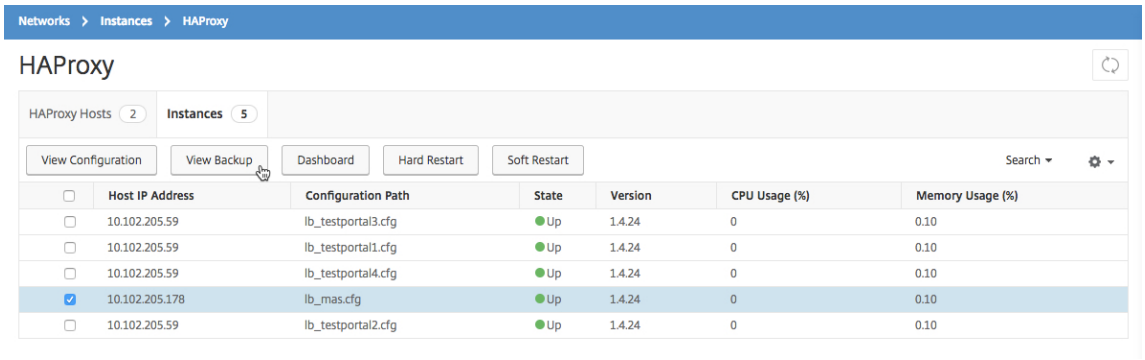
Backup und Wiederherstellen einer HAProxy-Instanz

February 5, 2024

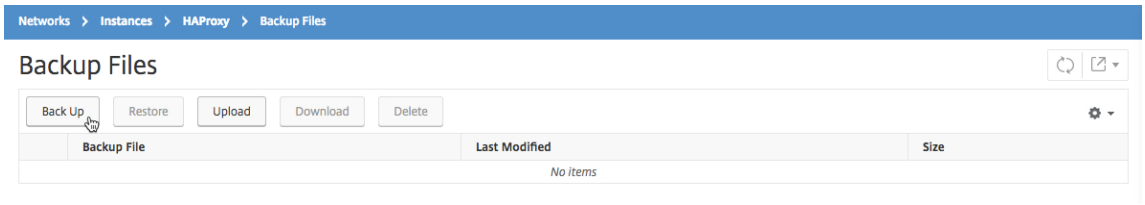
Sie können den aktuellen Status einer HAProxy-Instanz in einer HAProxy-Konfigurationsdatei sichern. Wenn die Instanz instabil wird, können Sie die gesicherten Dateien verwenden, um die Instanz in den stabilen Zustand zurückzusetzen.

So sichern Sie eine HAProxy-Instanz mithilfe von NetScaler ADM:

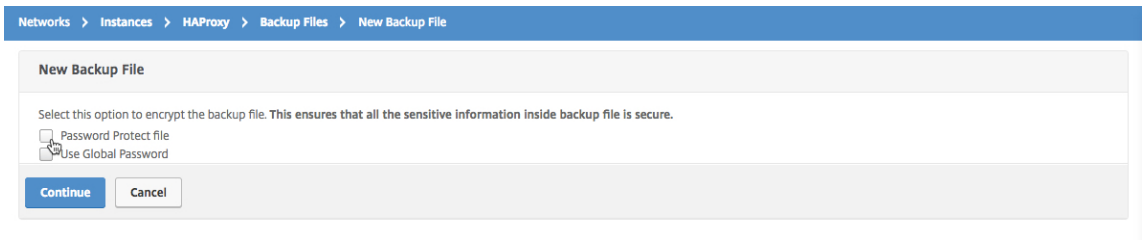
1. Navigieren Sie in Citrix Application Delivery Management (Citrix ADM) zu **Netzwerke > Instanzen > HAProxy**.
2. Klicken Sie auf der Seite **HAProxy** auf die Registerkarte **Instanzen**.
3. Wählen Sie die HAProxy-Instanz aus, von der Sie ein Backup erstellen möchten, und klicken Sie dann auf **Backup anzeigen**.



4. Klicken Sie auf der Seite **Backup-Dateienauf Sichern.**



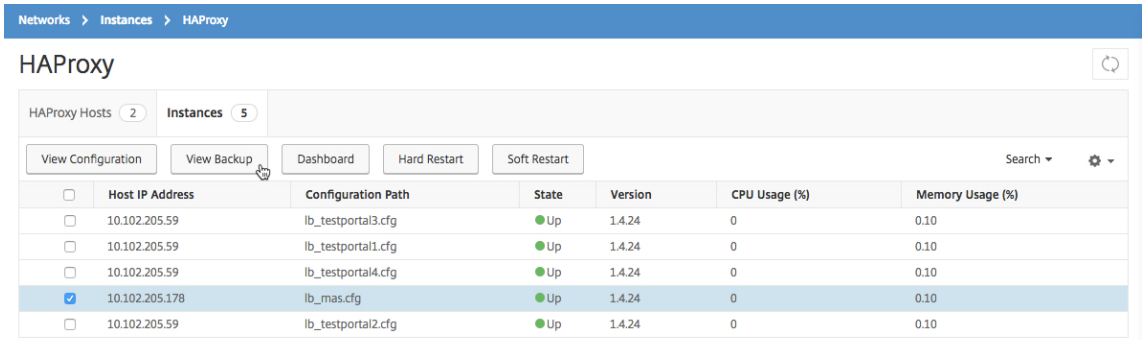
5. Sie können Ihre Backupdatei für mehr Sicherheit verschlüsseln.



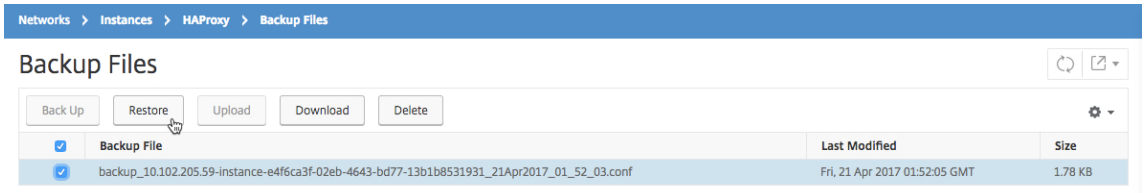
6. Klicken Sie auf **Weiter**.

So stellen Sie eine Instanz mithilfe von NetScaler ADM wieder her:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **HAProxy**.
2. Klicken Sie auf der Seite **HAProxy** auf die Registerkarte **Instanzen**.
3. Wählen Sie die Instanz aus, die Sie wiederherstellen möchten, und klicken Sie dann auf **Backup anzeigen**.



4. Wählen Sie auf der Seite **Backupdateien** die Backupdatei aus, die Sie wiederherstellen möchten, und klicken Sie dann auf **Wiederherstellen**.



> **Hinweis**
>
> Wenn Sie eine Instanz wiederherstellen, startet NetScaler ADM soft die HAProxy-Instanz neu.

HAProxy-Konfigurationsdatei bearbeiten

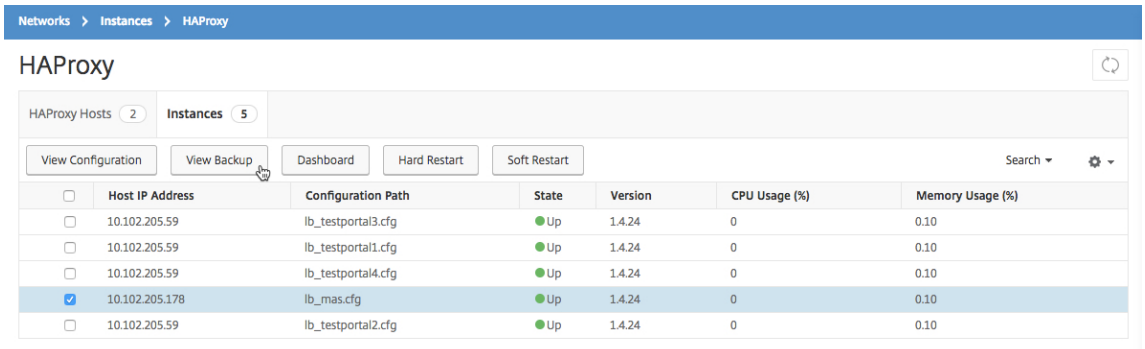
February 5, 2024

Sie können das Frontend, das Backend, den Server und andere Einstellungen in der vorhandenen HAProxy-Konfigurationsdatei aktualisieren. So bearbeiten Sie die HAProxy-Konfigurationsdatei:

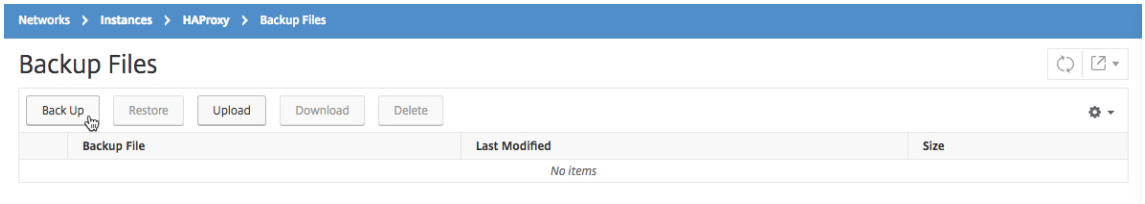
- Sichern Sie die HAProxy-Konfigurationsdatei.
- Laden Sie das Backup der HAProxy-Konfigurationsdatei herunter und bearbeiten Sie sie offline.
- Hochladen der aktualisierten HAProxy-Konfigurationsdatei in Citrix Application Delivery Management (Citrix ADM)
- Stellen Sie die HAProxy-Instanz mit der aktualisierten Backupdatei wieder her.

So bearbeiten Sie die HAProxy-Konfigurationsdatei mit NetScaler ADM:

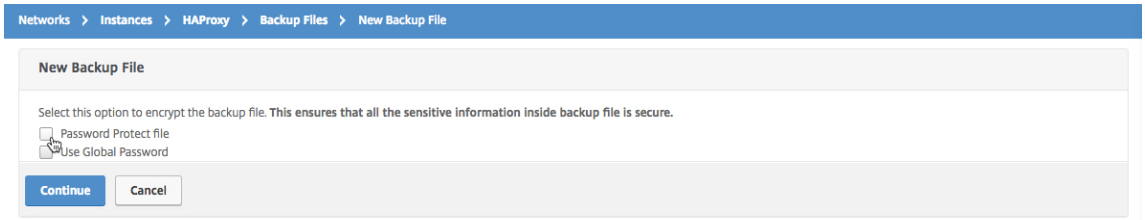
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen** > **HAProxy**.
2. Klicken Sie auf der Seite **HAProxy** auf die Registerkarte **Instanzen**.
3. Wählen Sie die HAProxy-Instanz aus, von der Sie ein Backup erstellen möchten, und klicken Sie dann auf **Backup anzeigen**.



4. Klicken Sie auf der Seite **Backupdateien** auf **Sichern**.

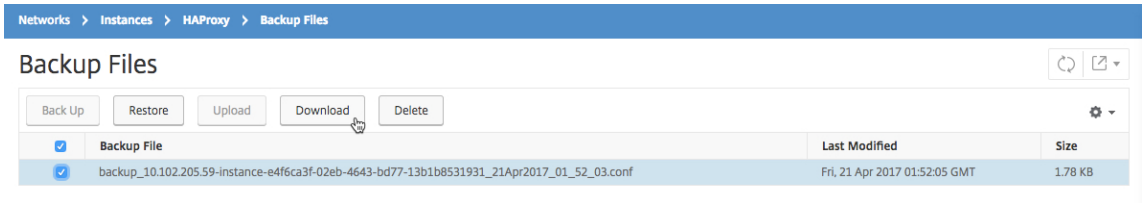


5. Klicken Sie auf **Weiter**.

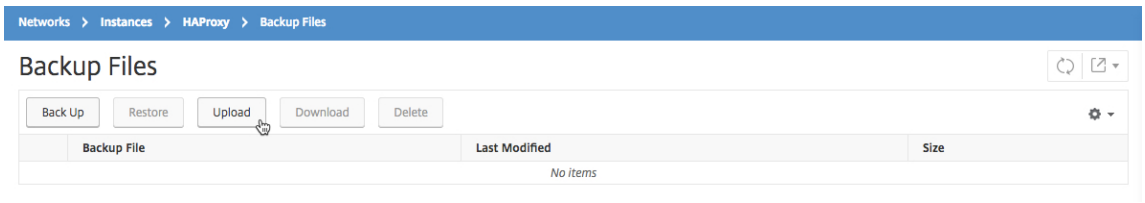


> **Hinweis**
>
> Verschlüsseln Sie die Backupdatei nicht.

6. Wählen Sie auf der Seite **Backupdateien** die Backupdatei aus, und klicken Sie auf **Herunterladen**.



7. Bearbeiten Sie mit einem Texteditor die HAProxy-Konfigurationsdatei.
8. Klicken Sie auf der Seite **Backupdateien** auf **Hochladen**, um die aktualisierte HAProxy-Konfigurationsdatei zu durchsuchen.



   Nachdem die aktualisierte HAProxy-Konfigurationsdatei hochgeladen wurde, wird sie auf der Seite **Backup der Dateien** aufgeführt.

9. Wählen Sie die aktualisierte HAProxy-Konfigurationsdatei aus, und klicken Sie auf **Wiederherstellen**.

Systemeinstellungen verwalten

February 5, 2024

In der folgenden Tabelle wird die Liste der Optionen beschrieben, die unter **System** > **Administration**verfügbar sind:

Netzwerkkonfigurationen

Netzwerkkonfigurationen	Optionen	Beschreibung
IP-Adresse, zweite Netzwerkkarte, Hostname und Proxyserver	IP-Adresse	Zeigt die IP-Adressdetails der NetScaler ADM-Netzwerkkonfiguration an, die für die Bereitstellung von NetScaler ADM verwendet werden
	Zweiter NIC	Ermöglicht die Konfiguration einer zweiten NIC zur Isolierung des NetScaler ADM Verwaltungszugriffs. Weitere Informationen finden Sie unter Konfigurieren einer dualen Netzwerkkarte für den Zugriff auf NetScaler ADM
	Hostname	Ermöglicht das Zuweisen eines Hostnamens zu NetScaler ADM. Weitere Informationen finden Sie unter Zuweisen eines Hostnamens zu einem NetScaler ADM-Server
	Proxyserver	Ermöglicht die Konfiguration von ADM als Proxyserver. Weitere Informationen finden Sie unter NetScaler ADM als API-Proxyserver
Statische Routen		Ermöglicht die Konfiguration statischer Routen, um eine Verbindung zwischen NetScaler ADM- und NetScaler ADC VPX-Instanzen herzustellen

Netzwerkkonfigurationen	Optionen	Beschreibung
NTP-Server		Stellt sicher, dass die NetScaler ADM Uhr dieselben Datums- und Uhrzeiteinstellungen hat wie die anderen Server im Netzwerk. Weitere Informationen finden Sie unter Konfigurieren des NTP-Servers
ADM-Port-Informationen		Ermöglicht Ihnen, zu verstehen, welcher Port für die Kommunikation zwischen ADM- und ADC- oder SD-WAN-Instanzen offen sein muss. Weitere Informationen finden Sie unter Unterstützte Ports

Systemkonfigurationen

Systemkonfigurationen	Optionen	Beschreibung
System, Zeitzone, erlaubte URLs und Nachricht des Tages	Grundeinstellungen	Ermöglicht es Ihnen, Systemeinstellungen wie das Aktivieren der `nsrecover` Anmeldung, das Aktivieren des Sitzungstimeouts usw. zu ändern
	Zeitzone	Ermöglicht es Ihnen, die Zeitzone zu ändern, die in NetScaler ADM verwendet werden soll. Die Standardzeitzone ist UTC

Systemkonfigurationen	Optionen	Beschreibung
	Liste der zulässigen URLs	Ermöglicht die Konfiguration von URLs zum Senden ununterbrochener Anforderungen an ADM. Sie können es mit dem Wert “none”konfigurieren, wenn keine URL hinzugefügt werden soll
	Botschaft des Tages	Ermöglicht das Erstellen einer Willkommensnachricht in NetScaler ADM. Mit dieser Funktion können Sie Erinnerungsmeldungen für sich selbst oder den Benutzer festlegen, der sich bei NetScaler ADM anmeldet. Klicken Sie auf **Nachricht aktivieren**, geben Sie die Nachricht in das Nachrichtenfeld ein und klicken Sie auf **Speichern**
ADM-Fingerabdruck anzeigen		Ermöglicht das Kopieren der eindeutigen NetScaler ADM-Fingerabdruck-ID, um mit dem Servicediagramm zu beginnen
Kundenidentität konfigurieren		Ermöglicht es Ihnen, die Netzwerkressourcen zu schützen, indem nur authentifizierte Kunden oder Benutzer auf das Netzwerk zugreifen können. Weitere Informationen finden Sie unter Daten-Governance

Systemkonfigurationen	Optionen	Beschreibung
CUXIP-Einstellungen		Wenn Sie dieses Kontrollkästchen aktivieren, werden Nutzungsstatistiken ausschließlich zum Zweck der Verbesserung der GUI gesammelt. Die empfangenen Daten werden nur von Citrix-Technikern verwendet und an niemanden weitergegeben

System-Pflege

System-Pflege	Beschreibung
Upgrade von NetScaler ADM	Ermöglicht Ihnen das Upgrade von NetScaler ADM über die GUI. Weitere Informationen finden Sie unter Upgrade
Starten Sie NetScaler ADM neu	Ermöglicht den Neustart von NetScaler ADM
Fahren Sie NetScaler ADM herunter	Ermöglicht das Herunterfahren von NetScaler ADM
Notfallwiederherstellung	Ermöglicht Ihnen das Anzeigen von Knoteninformationen zur Notfallwiederherstellung. Weitere Informationen finden Sie unter Konfigurieren der Notfallwiederherstellung

Datenbereinigung

Datenbereinigung	Optionen	Beschreibung
Bereinigung von System- und Instanzdaten	System	Ermöglicht die Begrenzung der Berichtsdaten, die in der NetScaler ADM -Serverdatenbank gespeichert werden. Weitere Informationen finden Sie unter Konfigurieren der System-Prune-Einstellungen
	Instanz-Ereignisse	Ermöglicht es Ihnen, die in NetScaler ADM gespeicherten Ereignismeldungen zu beschränken, die Daten melden
	Instanz Syslog	Ermöglicht es Ihnen, die Menge der in der Datenbank gespeicherten Syslog-Daten zu begrenzen. Weitere Informationen finden Sie unter Konfigurieren der Syslog-Einstellungen für Instanz-Prune-Einstellungen
	Netzwerkberichterstattung	Ermöglicht es Ihnen, die in NetScaler ADM gespeicherten Netzwerkberichtsdaten zu begrenzen

Backup

Backup	Optionen	Beschreibung
System- und Instanz-Backup konfigurieren	System	Ermöglicht es Ihnen, die anfänglichen Backupeinstellungen zu konfigurieren, bevor Sie eine Systembackup durchführen. Weitere Informationen finden Sie unter Systembackupeinstellungen
	Instanz	Ermöglicht das Konfigurieren von Einstellungen in NetScaler ADM zum Sichern einer ausgewählten NetScaler ADC Instanz oder mehrerer Instanzen. Weitere Informationen finden Sie unter Konfigurieren der Instanzbackupeinstellungen

Ereignisbenachrichtigungen

Ereignisbenachrichtigungen	Optionen	Beschreibung
Ereignisbenachrichtigung und Zusammenfassung konfigurieren	Benachrichtigung über das Ereignis	Sie können Benachrichtigungen für verschiedene systembezogene Funktionen an ausgewählte Benutzergruppen senden. Diese Systemfunktionen sind in Ereigniskategorien wie SystemReboot, StatusPoll, SystemState usw. unterteilt. Sie können NetScaler Application Delivery Management (ADM) so konfigurieren, dass es Ihnen Benachrichtigungen entweder per E-Mail, SMS oder Slack sendet. Dadurch wird sichergestellt, dass Sie über alle Aktivitäten auf Systemebene informiert werden, z. B. über eine Überschreitung des Datenspeichers oder über Backup-Fehler.
	Ereigniszusammenfassung	Ermöglicht es Ihnen, einen konsolidierten Bericht über wichtige System- und Funktionsereignisse zu erhalten

SSL-Einstellungen

SSL-Einstellungen	Beschreibung
Installieren Sie das SSL-Zertifikat	Ermöglicht die Installation des SSL-Zertifikats und der SSL-Schlüsseldatei
SSL-Zertifikat anzeigen	Ermöglicht das Anzeigen der SSL-Zertifikatsdetails

SSL-Einstellungen	Beschreibung
Konfigurieren von SSL-Einstellungen	Weitere Informationen finden Sie unter Konfigurieren von SSL-Einstellungen
SSL-Zertifikate	Ermöglicht das Hochladen, Herunterladen oder Löschen eines SSL-Zertifikats oder einer SSL-Schlüsseldatei
Chiffriergruppen	Weitere Informationen finden Sie unter Konfigurieren einer Verschlüsselungsgruppe

Funktionen konfigurieren

Funktionen konfigurieren	Beschreibung
Funktionen deaktivieren oder aktivieren	Sie können Funktionen in NetScaler ADM aktivieren oder deaktivieren. Weitere Informationen finden Sie unter ADM-Funktionen aktivieren oder deaktivieren

Einstellungen für das Systembackup konfigurieren

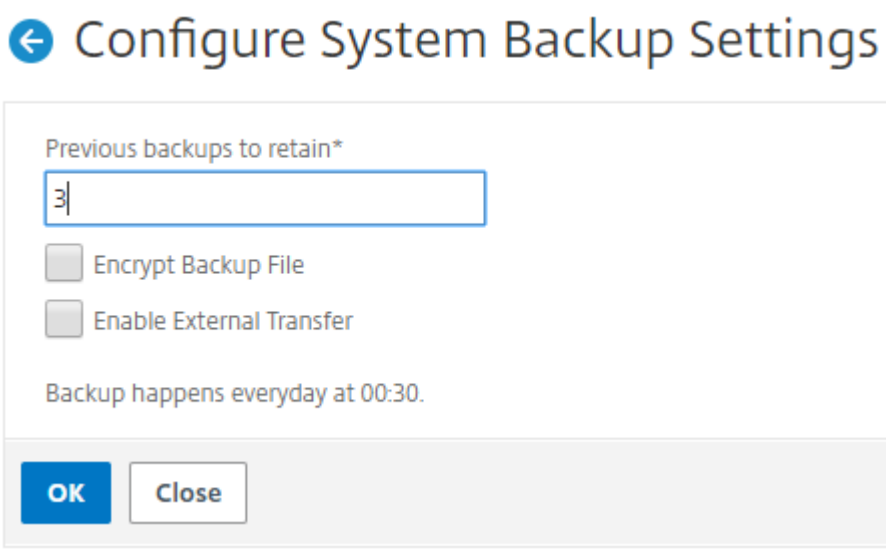
February 5, 2024

Legen Sie Ihre anfänglichen System-Backup-Einstellungen fest, bevor Sie das NetScaler Application Delivery Management (ADM) -System sichern und wiederherstellen müssen.

1. Navigieren Sie zu **System** > **Systemadministration**. Klicken Sie unter **Backupeinstellungen** auf **Systemback**
2. Geben Sie auf der Seite **„Systemsicherungseinstellungen konfigurieren** “Folgendes an:
    - Anzahl der zu speichernden Backups. Sie können nur bis zu 10 Backups behalten.
    - Verschlüsseln Sie die Backupdatei.
    - Aktivieren Sie die externe Übertragung. Sie können vorsichtshalber eine Kopie einer Kopie Ihrer Sicherungsdatei auf ein anderes System übertragen. Wenn Sie die Konfiguration wiederherstellen möchten, müssen Sie die Datei zuerst auf den Citrix ADM -Server hochladen und dann den Wiederherstellungsvorgang durchführen. Geben Sie den Server,

den Benutzernamen und das Kennwort, den Port, das zu verwendende Übertragungsprotokoll und den Verzeichnispfad an. Weitere Informationen zur externen Übertragung finden Sie unter Übertragen einer NetScaler ADM-Backupdatei auf ein externes System.

3. Klicken Sie auf **OK**.



Konfigurieren eines NTP-Servers

February 5, 2024

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

So konfigurieren Sie einen NTP-Server auf NetScaler ADM:

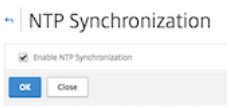
1. Navigieren Sie zu **System** > **NTP-Server**, und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie auf der Seite **NTP-Server erstellen** die folgenden Details ein:
   - **Servername/IP-Adresse** —Geben Sie den Domainnamen oder die IP-Adresse des NTP-Servers ein. Der Name oder die IP-Adresse können nicht geändert werden, nachdem Sie den NTP-Server hinzugefügt haben.
   - **Minimales Abfrageintervall** —Geben Sie den Mindestwert für das Intervall zwischen übertragenen NTP-Nachrichten in Sekunden als Trennschärfe von 2. Wenn Sie beispielsweise möchten, dass das minimale Abfrageintervall 64 Sekunden beträgt, was als 2 ^ 6 ausgedrückt werden kann, geben Sie 6 ein.

- **Maximales Abfrageintervall** —Geben Sie den Maximalwert für das Intervall zwischen übertragenen NTP-Nachrichten in Sekunden als Trennschärfe von 2. Wenn Sie beispielsweise möchten, dass das maximale Abfrageintervall 256 Sekunden beträgt, was als 2^8 ausgedrückt werden kann, geben Sie 8 ein.
- **Schlüssel-ID**—Geben Sie die Schlüssel-ID ein, die für die symmetrische Schlüsselauthentifizierung mit dem NTP-Server verwendet werden kann. Fügen Sie keine Schlüssel-ID hinzu, wenn Sie Autokey auswählen.
- **Autokey** —Wählen Sie **Autokey** aus, wenn Sie die Authentifizierung mit öffentlichen Schlüsseln für den NTP-Server verwenden möchten. Wählen Sie nicht aus, ob Sie eine Schlüssel-ID hinzufügen möchten.
- **Bevorzugt** —Wählen Sie diese Option, wenn Sie diesen NTP-Server als bevorzugten Server für die Uhrsynchronisierung angeben möchten. Dies gilt nur, wenn mehr als ein Server konfiguriert ist.

3. Klicken Sie auf **Erstellen**.

So aktivieren Sie die NTP-Synchronisierung auf NetScaler ADM:

1. Navigieren Sie zu **System > NTP-Server** .
2. Klicken Sie auf **NTP-Synchronisierung** und **aktivieren Sie das Kontrollkästchen NTP-Synchronisierung** aktivieren.
3. Klicken Sie auf **OK**.



> Hinweis Die NTP-Protokollmeldungen finden
>
> Sie im Verzeichnis /var/log in der `/var/log/ntpd.log` Dateidatei.

Aktualisieren von NetScaler Application Delivery Management (ADM)

February 5, 2024

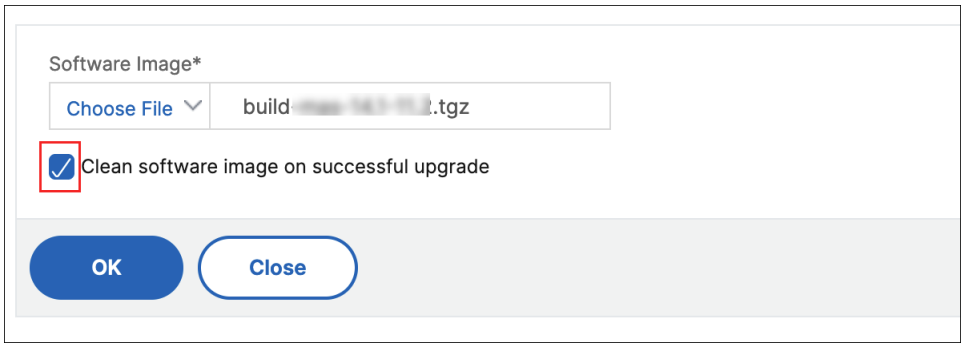
Jede NetScaler ADM-Version bietet neue und aktualisierte Funktionen mit erweiterter Funktionalität. Eine umfassende Liste von Verbesserungen ist in den Versionshinweisen aufgeführt, die der Release-Ankündigung beigefügt sind. Nehmen Sie sich einen Moment Zeit, um die Versionshinweise zu lesen, bevor Sie die Software aktualisieren. Es ist wichtig, dass Sie den Lizenzrahmen und die Lizenztypen verstehen, bevor Sie mit dem Upgrade beginnen.

Um Citrix ADM zu aktualisieren:

1. Navigieren Sie zu **System** > **Systemadministrationen**. Klicken Sie unter der Unterüberschrift **Systemadministration** auf **NetScaler ADM aktualisieren**.
2. Laden Sie auf der Seite NetScaler ADM aktualisieren eine neue Image-Datei hoch, indem Sie entweder **Lokal** (Ihr lokaler Computer) oder **Appliance**auswählen.

   > **Hinweis**
   >
   > Wenn Sie **Appliance**auswählen, stellen Sie sicher, dass das Upgrade-Image `/var/mps/mps_images` in NetScaler ADM verfügbar ist.

   Standardmäßig wird das Softwareimage nach einem erfolgreichen Upgrade bereinigt.
3. Klicken Sie auf **OK**.



Kennwort für NetScaler ADM zurücksetzen

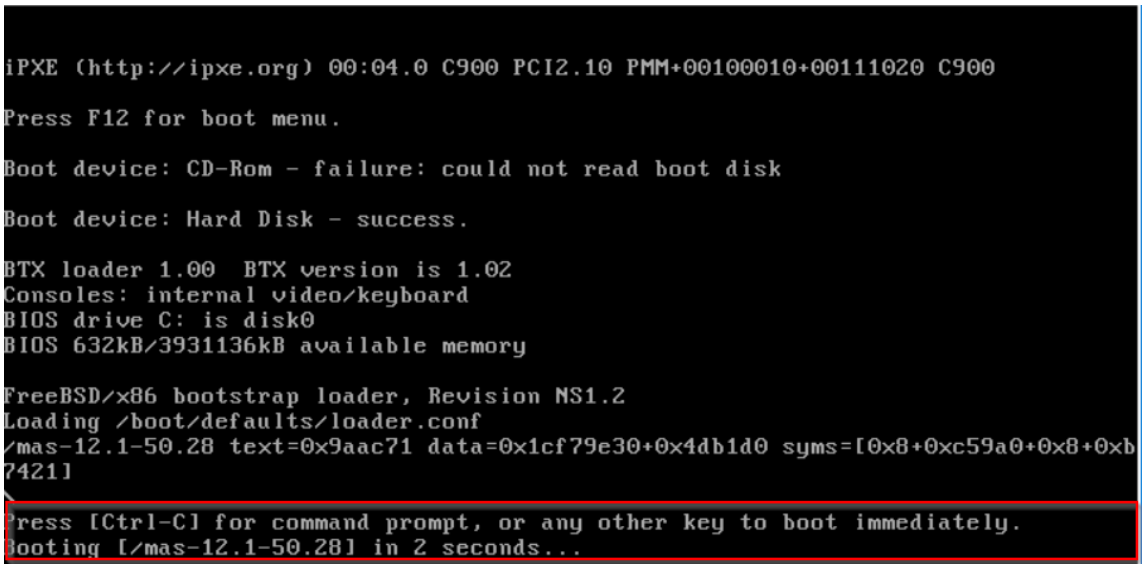
February 5, 2024

Das Verfahren zum Zurücksetzen des Kennworts für NetScaler ADM kann auf Hypervisoren, auf denen es gehostet wird, unterschiedlich sein. Wenn Sie Ihr Standardkennwort geändert haben und auf das

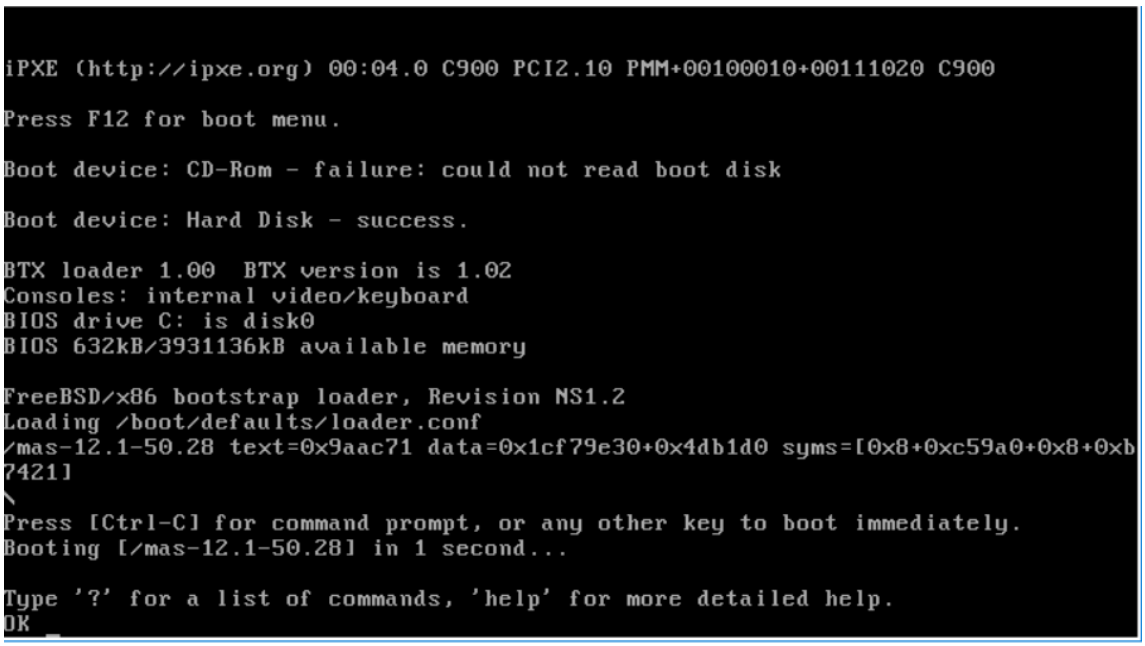
Standardkennwort zurücksetzen möchten, können Sie das Kennwort zurücksetzen, indem Sie den NetScaler ADM-Knoten neu starten.

Citrix Hypervisor mit XenCenter:

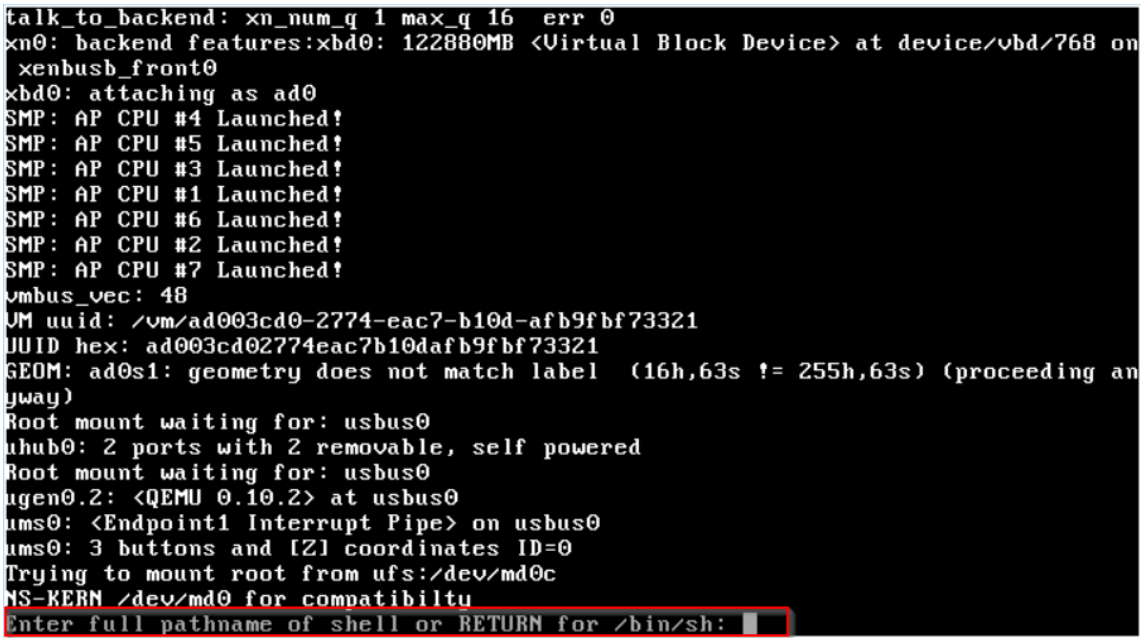
1. Melden Sie sich mit XenCenter bei Citrix Hypervisor an.
2. Wählen Sie den Knoten NetScaler ADM aus, klicken Sie mit der rechten Maustaste und wählen Sie **Neustart**
3. Auf der Registerkarte **Konsole** drücken Sie **CTL + C**, um die Startsequenz zu unterbrechen.



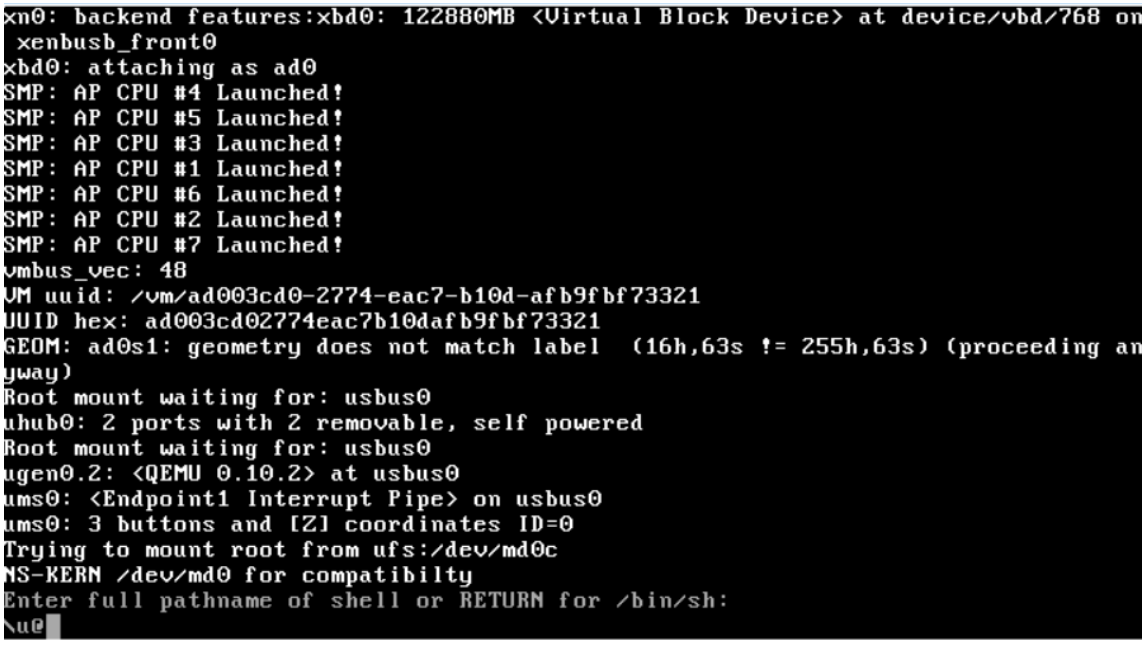
4. Führen Sie den Befehl **boot -s** an der Eingabeaufforderung OK



NetScaler ADM wird neu gestartet und zeigt die folgende Meldung an:

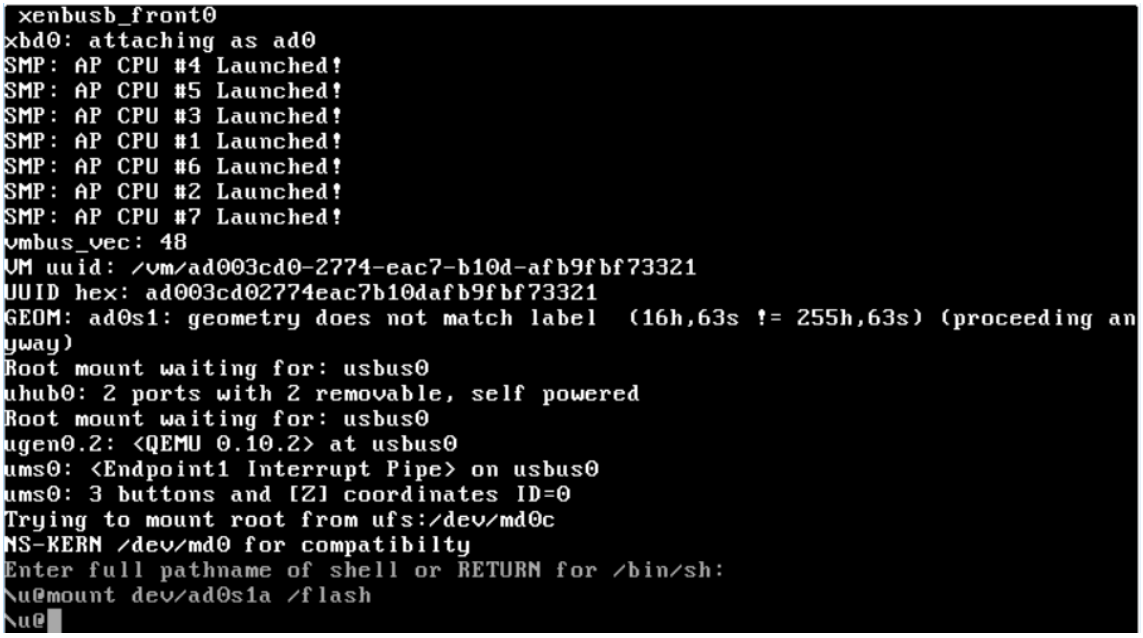


5. Drücken Sie die **Eingabetaste**, um die Eingabeaufforderung /u @ zu erhalten.



6. Mounten Sie die Flash-Partition mit dem folgenden Befehl:

```
mount dev/ad0s1a /flash
```

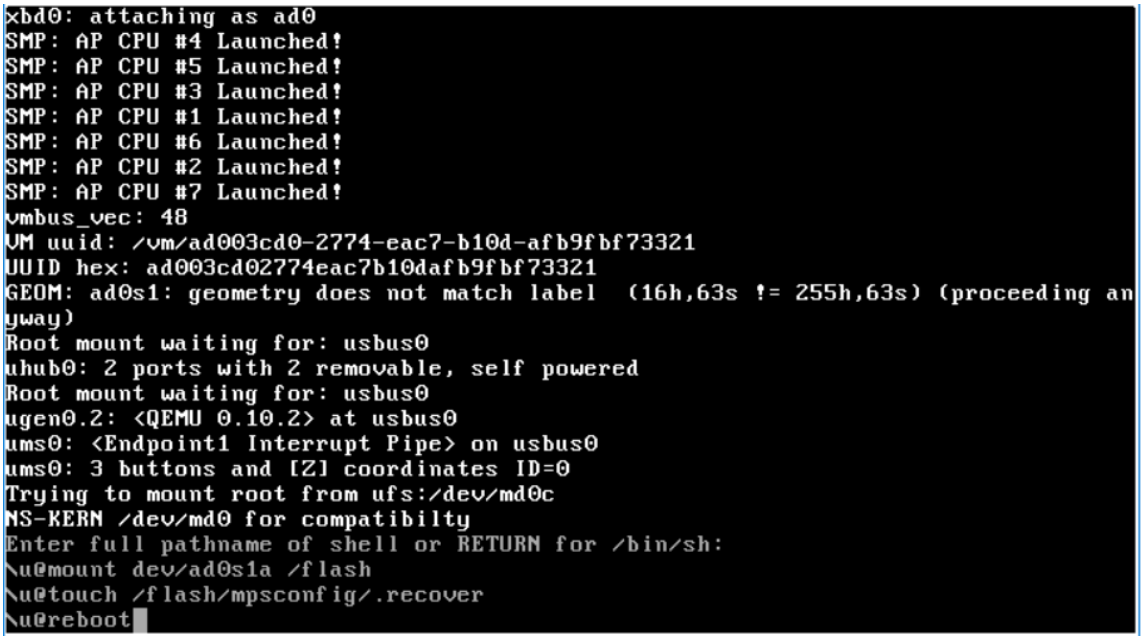



7. Erstellen Sie eine Datei mit dem folgenden Befehl:

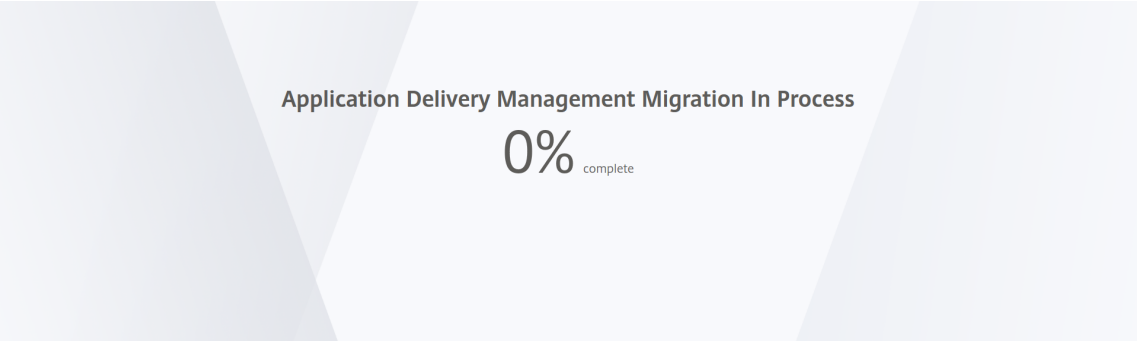
   ```
   touch /flash/mpsconfig/.recover
   ```

   Das Kennwort wird nun auf das Standardkennwort zurückgesetzt.

8. Führen Sie den Befehl **Neustart** aus, um NetScaler ADM neu zu starten.



9. Greifen Sie auf die NetScaler ADM GUI zu und warten Sie, bis der Neustart abgeschlossen ist.

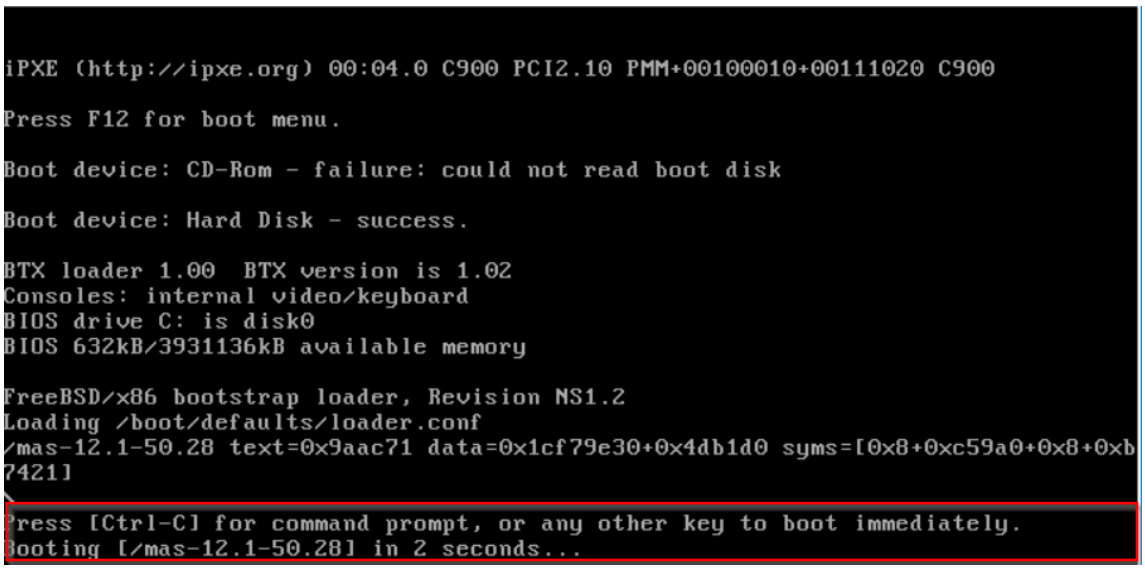


Sie können jetzt *nsroot/nsroot* Anmeldeinformationen verwenden, um sich von der GUI anzumelden, und *nsrecover/nsroot*, um sich vom Hypervisor anzumelden.

> Hinweis
>
> Wenn das Kennwort nach dem Neustart nicht auf das Standardkennwort zurückgesetzt wurde, wiederholen Sie den Vorgang (Schritt 1 bis Schritt 7). Führen Sie dann die folgenden Befehle aus und starten Sie NetScaler ADM neu:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Esx mit vSphere:

1. Melden Sie sich mit vSphere bei ESX an.
2. Wählen Sie den NetScaler ADM Knoten aus, klicken Sie mit der rechten Maustaste, und wählen Sie dann **Neustart** aus.
3. Auf der Registerkarte **Konsole** drücken Sie **CTL + C**, um die Startsequenz zu unterbrechen.



4. Führen Sie den Befehl **boot -s** in der Eingabeaufforderung OK

NetScaler ADM wird neu gestartet.

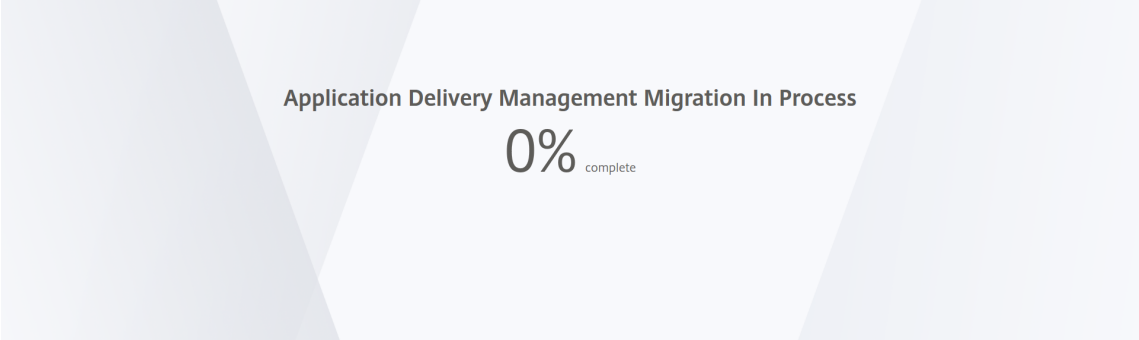
5. Drücken Sie die **Eingabetaste**, um die Eingabeaufforderung /u @ zu erhalten.
6. Mounten Sie die Flash-Partition mit dem folgenden Befehl:

   ```
   mount dev/da0s1a /flash
   ```

7. Erstellen Sie eine Datei mit dem folgenden Befehl:

   ```
   touch /flash/mpsconfig/.recover
   ```

   Das Kennwort wird nun auf das Standardkennwort zurückgesetzt.
8. Führen Sie den Befehl **Neustart** aus, um NetScaler ADM neu zu starten.
9. Greifen Sie auf die NetScaler ADM GUI zu und warten Sie, bis der Neustart abgeschlossen ist.

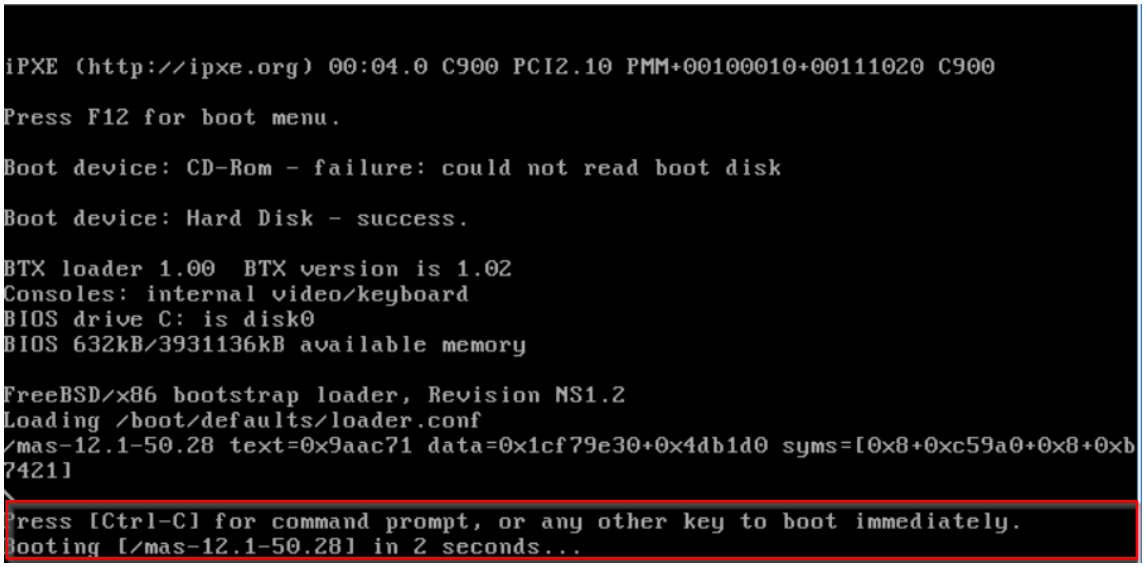


Sie können jetzt *nsroot/nsroot* Anmeldeinformationen verwenden, um sich von der GUI anzumelden, und *nsrecover/nsroot*, um sich vom ESX-Server anzumelden.

> Hinweis
>
> Wenn das Kennwort nach dem Neustart nicht auf das Standardkennwort zurückgesetzt wurde, wiederholen Sie den Vorgang (Schritt 1 bis Schritt 7). Führen Sie dann die folgenden Befehle aus und starten Sie NetScaler ADM neu:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Hyper-V mit Hyper-V-Manager:

1. Melden Sie sich mit dem Hyper-V-Manager bei Hyper-V an.
2. Wählen Sie den NetScaler ADM Knoten aus, klicken Sie mit der rechten Maustaste, und wählen Sie dann **Neustart** aus.
3. Auf der Registerkarte **Konsole** drücken Sie **CTL + C**, um die Startsequenz zu unterbrechen.



4. Führen Sie den Befehl **boot -s** an der Eingabeaufforderung OK aus

   NetScaler ADM wird neu gestartet.

5. Drücken Sie die **Eingabetaste**, um die Eingabeaufforderung /u @ zu erhalten.
6. Mounten Sie die Flash-Partition mit dem folgenden Befehl:

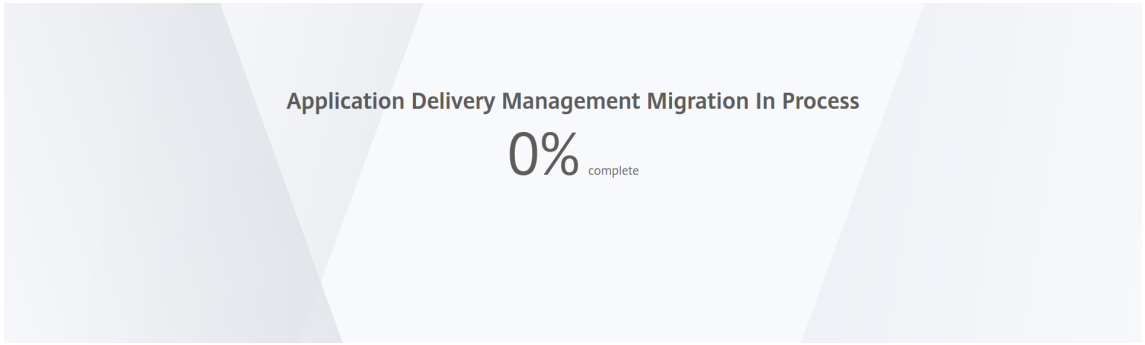
   ```
   mount dev/ad0s1a /flash
   ```

7. Erstellen Sie eine Datei mit dem folgenden Befehl:

   ```
   touch /flash/mpsconfig/.recover
   ```

   Das Kennwort wird nun auf das Standardkennwort zurückgesetzt.

8. Führen Sie den Befehl **Neustart** aus, um NetScaler ADM neu zu starten.
9. Greifen Sie auf die NetScaler ADM GUI zu und warten Sie, bis der Neustart abgeschlossen ist.



   Sie können jetzt *nsroot/nsroot* Anmeldeinformationen verwenden, um sich von der GUI anzumelden, und *nsrecover/nsroot*, um sich vom hyper-v Manager anzumelden.

> Hinweis
>
> Wenn das Kennwort nach dem Neustart nicht auf das Standardkennwort zurückgesetzt wurde, wiederholen Sie den Vorgang (Schritt 1 bis Schritt 7). Führen Sie dann die folgenden Befehle aus und starten Sie NetScaler ADM neu:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Linux KVM-Server (SSH zu KVM-Server unter Verwendung eines beliebigen SSH-Clients):

1. Melden Sie sich mit einem SSH-Client bei NetScaler ADM am KVM-Server an.
2. Starten Sie NetScaler ADM neu.
3. Drücken Sie **CTL + C**, um die Startsequenz kurz nachdem die Meldung **Loading /boot/default-s/loader.conf** angezeigt wird, zu unterbrechen.
4. Führen Sie an der Eingabeaufforderung OK den folgenden Befehl aus:

   ```
   set console='comconsole,vidconsole'
   ```

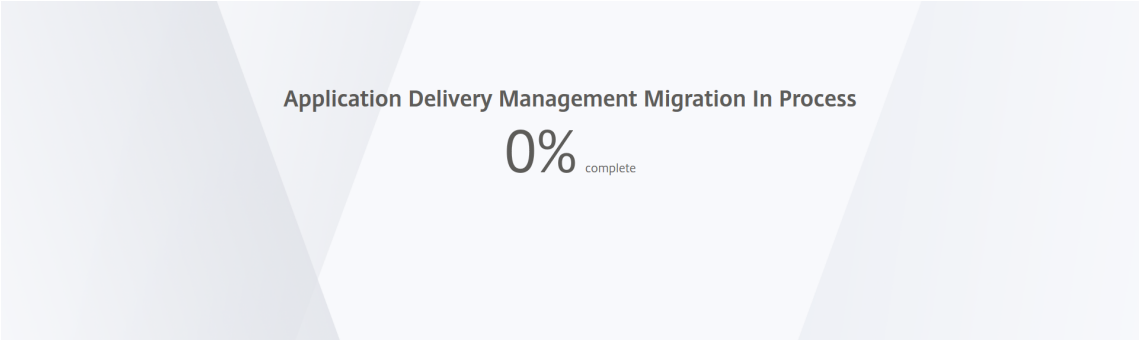
5. Führen Sie den Befehl **boot -s** aus, um NetScaler ADM neu zu starten.
6. Nachdem die Meldung **Enter full path of shell oder RETURN for /bin/sh:** angezeigt wird, drücken Sie die **Eingabetaste**, um die Eingabeaufforderung /u@ zu erhalten.
7. Mounten Sie die Flash-Partition mit dem folgenden Befehl:

   ```
   mount dev/vtbd0s1a /flash
   ```

8. Erstellen Sie eine Datei mit dem folgenden Befehl:

   ```
   touch /flash/mpsconfig/.recover
   ```

   Das Kennwort wird nun auf das Standardkennwort zurückgesetzt.
9. Führen Sie den Befehl **Neustart** aus, um NetScaler ADM neu zu starten.
10. Greifen Sie auf die NetScaler ADM GUI zu und warten Sie, bis der Neustart abgeschlossen ist.



Sie können jetzt *nsroot/nsroot* Anmeldeinformationen verwenden, um sich von der GUI anzumelden, und *nsrecover/nsroot*, um sich von der SSH-Konsole aus anzumelden.

> Hinweis
>
> Wenn das Kennwort nach dem Neustart nicht auf das Standardkennwort zurückgesetzt wurde, wiederholen Sie den Vorgang (Schritt 1 bis Schritt 7). Führen Sie dann die folgenden Befehle aus und starten Sie NetScaler ADM neu:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Konfigurieren einer dualen Netzwerkkarte für den Zugriff auf NetScaler ADM

February 5, 2024

Sie können eine zweite Netzwerkkarte konfigurieren, um den Verwaltungszugriff auf NetScaler ADM zu isolieren. Mit dieser zweiten NIC-Funktion können Sie je nach Anforderung auswählen, wie Sie den über NetScaler ADM empfangenen und gesendeten Datenverkehr isolieren möchten.

Stellen Sie sich ein Szenario vor, in dem Sie den Datenverkehr isolieren möchten, um:

- Führen Sie die gesamte Kommunikation zwischen NetScaler ADM und seinen verwalteten NetScaler ADC-Instanzen in einem Netzwerk durch.
- Haben Sie Verwaltungszugriff auf NetScaler ADM in einem anderen Netzwerk.

In diesem Szenario können Sie als Administrator:

- Konfigurieren Sie eine IP-Adresse für den Datenverkehr zwischen NetScaler ADM und seinen verwalteten NetScaler ADC-Instanzen.
- Konfigurieren Sie eine andere IP-Adresse für die Verwaltung der NetScaler ADM-Software, um alle administrativen Aufgaben in der Software auszuführen.

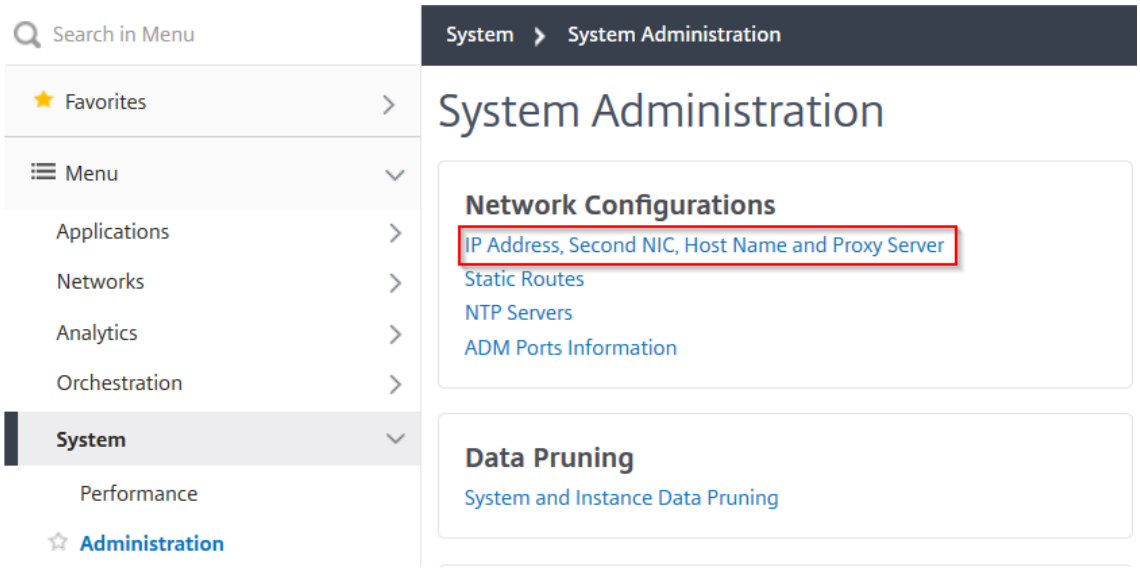
> **Hinweis**
>
> Wenn NetScaler ADM als HA-Paar konfiguriert ist, wird die auf der zweiten Netzwerkkarte konfigurierte Verwaltungs-IP-Adresse dem primären Knoten zugeordnet.

Voraussetzungen

- Stellen Sie sicher, dass Sie **NetScaler ADM 13.0 Build 47.x oder höher** auf dem Hypervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM oder VMware ESXi) bereitgestellt und konfiguriert haben.
- Stellen Sie sicher, dass Sie die zweite Netzwerkkarte auf dem Hypervisor hinzugefügt haben (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM oder VMware ESXi).

Konfigurieren Sie eine zweite Netzwerkkarte in NetScaler ADM

1. Melden Sie sich bei ADM GUI an.
2. Navigieren Sie zu **System** > **Verwaltung**.
3. Klicken Sie unter **Netzwerkkonfiguration**auf **IP-Adresse, Zweite Netzwerkkarte, Hostname und Proxyserver**.



   Die Seite **Netzwerkkonfiguration** wird angezeigt.

4. Klicken Sie auf die Registerkarte Zweite NIC und konfigurieren Sie die folgenden Parameter:

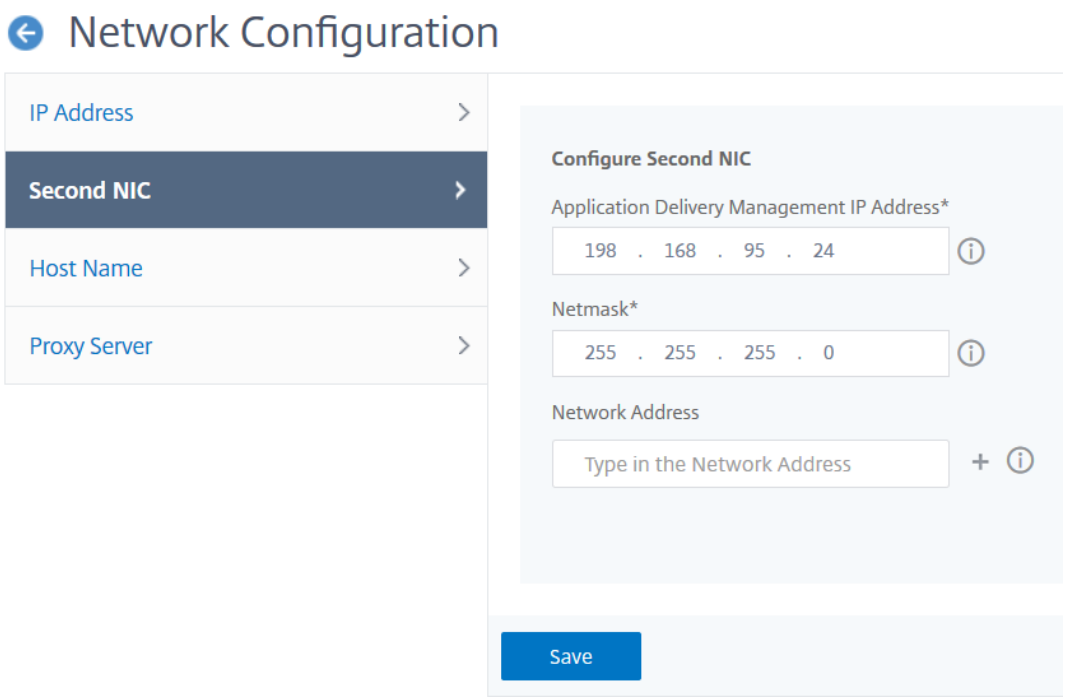
   a) **IP-Adresse für Application Delivery Management** —Geben Sie eine gültige IP-Adresse für den Zugriff auf NetScaler ADM ein. Sie können diese IP-Adresse für den Zugriff auf NetScaler ADM verwenden, abgesehen von der vorhandenen Verwaltungs-IP-Adresse.

   b) **Netzmaske** —Geben Sie die Netzmaskenadresse ein, um den Netzwerk-Host anzugeben. Die Standardadresse ist 255.255.255.0.

   c) **Netzwerkadresse** —Geben Sie eine IP-Adresse ein, um einen Routeneintrag für NetScaler ADM hinzuzufügen. Klicken Sie auf **+**, um weitere IP-Adressen hinzuzufügen. Das Feld ist

optional.

d) Klicken Sie auf **Speichern**.



Syslog-Löschintervall konfigurieren

February 5, 2024

Syslog ist ein Standardprotokoll für die Protokollierung. Es besteht aus zwei Komponenten: dem Syslog-Auditing-Modul, das auf der Citrix Application Delivery Controller-Instanz (ADC) ausgeführt wird, und dem Syslog-Server, der entweder auf dem zugrunde liegenden FreeBSD-Betriebssystem (OS) der Citrix ADC-Instanz oder auf einem Remotesystem ausgeführt werden kann. SYSLOG verwendet das User Datagram Protocol (UDP) für die Datenübertragung.

Syslog ermöglicht die Isolierung des Systems, das Informationen generiert, und des Systems, in dem die Informationen gespeichert werden. Sie können Protokollinformationen konsolidieren und Erkenntnisse aus den gesammelten Daten gewinnen. Sie können syslog auch so konfigurieren, dass verschiedene Arten von Ereignissen protokolliert werden.

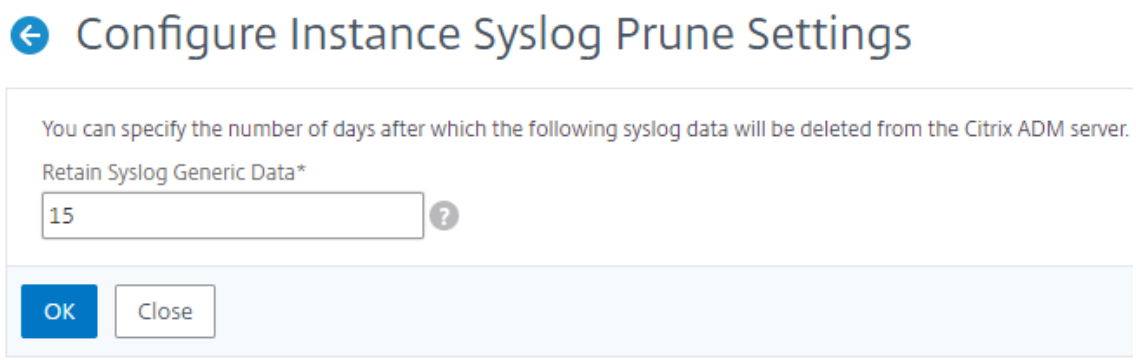
Um die Menge der in der Datenbank gespeicherten Syslog-Daten zu begrenzen, können Sie das Intervall angeben, in dem Sie Syslog-Daten löschen möchten.Sie können die Anzahl der Tage angeben, nach denen die folgenden Syslog-Daten aus der NetScaler Application Delivery Management (ADM) gelöscht werden:

- Generische Syslog-Daten
- AppFirewall-Daten
- NetScaler Gateway Daten

Sie können das Citrix Gateway -Prune-Intervall auch nach Syslog-Typ konfigurieren. Dieses Beschneidungsintervall hat Vorrang vor dem Runenintervall, das für die Beibehaltung von Citrix Gateway Daten konfiguriert ist.

So konfigurieren Sie die Einstellungen für das Syslog-Prune-Intervall für NetScaler ADM:

1. Navigieren Sie zu **System > Administration**.Klicken Sie unter **Datenbereinigung**auf **System- und Instanzdatenbereinigung**, und klicken Sie dann auf **Instanzsyslog**.
2. Geben Sie auf der Seite **Einstellungen für Instanz Syslog-Bereinigung konfigurieren** die Option **Generische Syslog-Daten (Tage) beibehalten**an. Geben Sie die Anzahl der Tage ein, für die NetScaler ADM generische Syslog-Nachrichten aufbewahrt.



Konfigurieren der Einstellungen für Systembeschneidung und Event-Prune

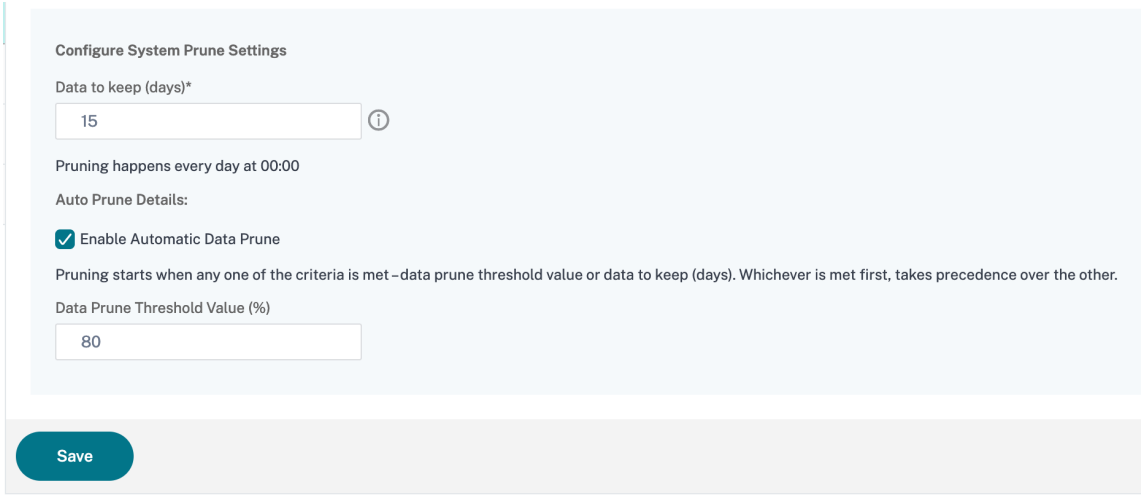
February 5, 2024

Um die Menge der in Ihrer NetScaler Application Delivery Management (ADM) -Softwaredatenbank gespeicherten Berichtsdaten zu begrenzen, können Sie sie beschneiden. Sie können das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle beibehalten soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00.00 Uhr) bereinigt.

> Hinweis
>
> Der angegebene Wert darf 30 Tage oder weniger als 15 Tage betragen.

So konfigurieren Sie die Einstellungen für Systemausfall für Leistungsberichte mit NetScaler ADM:

1. Navigieren Sie zu**System**>**Administration**. Klicken Sie unter **Datenbereinigung** auf **System- und Instanzdatenbereinigung**.
2. Geben Sie auf der Seite **Systemausfalleinstellungen konfigurieren** die Anzahl der Tage an, für die Daten gespeichert werden sollen, und klicken Sie auf**OK**.

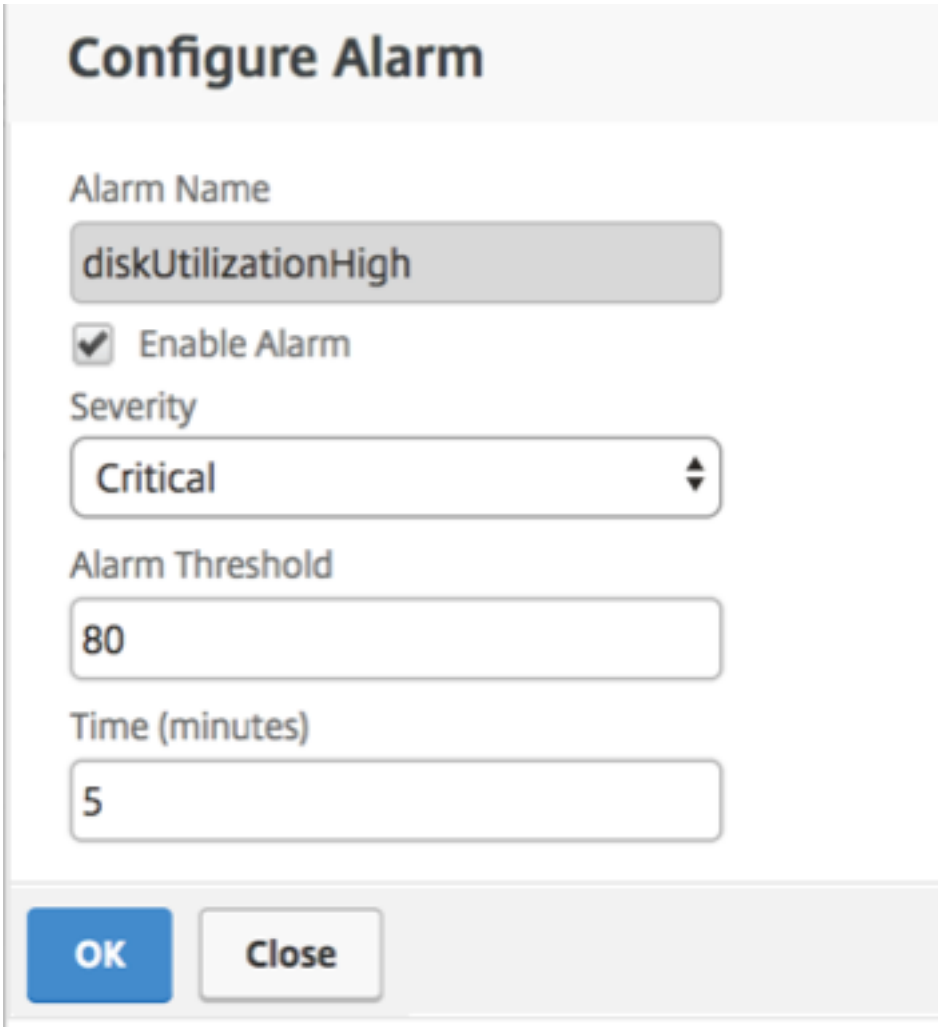


Sie können das automatische Beschneiden aktivieren, indem Sie das Kontrollkästchen **Automatische Datenbeschneidung aktivieren** aktivieren. Ein Alarm wird ausgelöst und eine E-Mail wird gesendet, wenn die Datenträgernutzung den konfigurierten **Schwellenwert für Datenbereinigung** verletzt. Um den Prozentsatz des Speicherplatz (Bereinigungsschwellenwert) zu ändern, klicken Sie auf **Bearbeiten**.

> Hinweis:
> Das Pruning beginnt, wenn eines der Kriterien erfüllt ist —Schwellenwert für die Datenbereinigung oder zu behaltende Daten (Tage). Was zuerst getroffen wird, hat Vorrang vor dem anderen.

Sie können den Alarm **diskUtilizationHigh** konfigurieren und aktivieren (standardmäßig) und Folgendes angeben:

- **Schweregrad**, wie Critical.
- **Alarmschwelle**. Geben Sie den Wert ein, für den die Schwere des Ereignisses berechnet wird.
- **Zeit**. Zeitlänge (in Minuten), nach der Sie den Alarm auslösen möchten.



Konfigurieren von Einstellungen für die Ereignisbereinigung mit NetScaler ADM

Um die Menge der in Ihrer NetScaler ADM-Datenbank gespeicherten Ereignisnachrichten zu begrenzen, können Sie das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Audit-Logs und Task-Protokolle speichern soll. Standardmäßig werden diese Daten alle 24 Stunden (um 00.00 Uhr) bereinigt.

- Navigieren Sie zu **System > Administration > Data Pruning** und klicken Sie auf **System- und Instanzdaten-Pruning**. Klicken Sie auf **Instanzereignisse**.
- Geben Sie das Zeitintervall in Tagen ein, für das Daten auf dem Citrix ADM -Server gespeichert werden sollen, und klicken Sie auf **Speichern**.

Shell-Zugriff für nicht standardmäßige Benutzer aktivieren

February 5, 2024

Sie können den Shell-Zugriff für nicht standardmäßige Benutzer in Citrix Application Delivery Management (ADM) aktivieren. Sie können diese Funktion verwenden, um den Kommunikationsmodus mit Instanzen zu aktivieren und einzurichten.

> **Hinweis**
>
> Standardmäßig ist der Shell-Zugriff für Nicht-Standardbenutzer deaktiviert.

So aktivieren Sie den Shell-Zugriff für nicht standardmäßige Benutzer in Citrix ADM:

1. Navigieren Sie in NetScaler ADM zu **System** > **Systemadministration**.
2. Klicken Sie in **den Systemeinstellungen**auf **Systemeinstellungen ändern**.
3. Konfigurieren Sie auf der Seite **Systemeinstellungen ändern** die folgenden Parameter:
    - **Kommunikation mit Instanzen** —Wählen Sie das Kommunikationsprotokoll aus.
    - **Sicherer Zugriff** : Aktivieren Sie sicheren Zugriff für Citrix ADM.
    - **Sitzungs-Timeout aktivieren** —Geben Sie den Zeitraum an, für den eine inaktive Sitzung beibehalten werden soll.
    - **Standardauthentifizierung zulassen** - Zulassen, dass der Verwaltungsdienst Anmeldeinformationen akzeptiert, die mit dem Standardauthentifizierungsprotokoll angegeben wurden.
    - **Nsrecover Login** aktivieren - `nsrecover` Anmeldung bei Management Service aktivieren.
    - **Zertifikatdownload aktivieren** : Ermöglicht das Herunterladen von Zertifikaten aus dem hinzugefügten NetScaler ADC.
    - **Shellzugriff für Nicht-NSROOT-Benutzer aktivieren** : Aktivieren Sie den Shell-Zugriff für nicht standardmäßige Benutzer in Citrix ADM.
    - **Benutzeranmeldeinformationen für die Instanzanmeldung auffordern** : Benutzer können ihre Benutzeranmeldeinformationen eingeben, während sie sich von Citrix ADM an Instanzen anmelden.
4. Klicken Sie auf **OK**.

Nicht zugängliche NetScaler ADM-Server wiederherstellen

February 5, 2024

Citrix Application Delivery Management (ADM) stellt jetzt ein Datenbankwartungstool bereit, mit dem die Systemdatenbank bereinigt werden kann. Sie können jetzt das Citrix ADM Dienstprogramm starten, um eine Verbindung mit dem Dateisystem herzustellen, einige Komponenten zu löschen und die Datenbank zugänglich zu machen. Citrix ADM Wiederherstellungsskript ist ein Tool, das beim Wiederherstellen von Speicherplatz im Dateisystem hilft, indem alte oder nicht verwendete Datenbanktabellen und -dateien gelöscht werden. Das Tool unterstützt Sie dabei, in aufeinanderfolgenden Schritten durch die Datenbanktabellen und -dateien zu navigieren, und zeigt den aktuellen Speicherplatz, der von den jeweiligen Elementen im Dateisystem belegt wird. Nachdem Sie die zu löschenden Datenbanktabellen und Dateien ausgewählt haben, löscht das Tool diese nach Bestätigung aus dem Dateisystem.

Verwenden des Citrix ADM Datenbankwiederherstellungsskripts für eine eigenständige Citrix ADM-Bereitstellung

Verwenden Sie das folgende Verfahren in einer NetScaler ADM Bereitstellung für einen Server, um eine Verbindung mit dem Dateisystem herzustellen, einige Komponenten zu löschen, die Datenbank zugänglich zu machen und dann die Wiederherstellungsvorgänge durchzuführen.

1. Melden Sie sich mit einem SSH-Client oder der Konsole Ihres Hypervisors bei NetScaler ADM an und geben Sie den folgenden Befehl ein:

```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

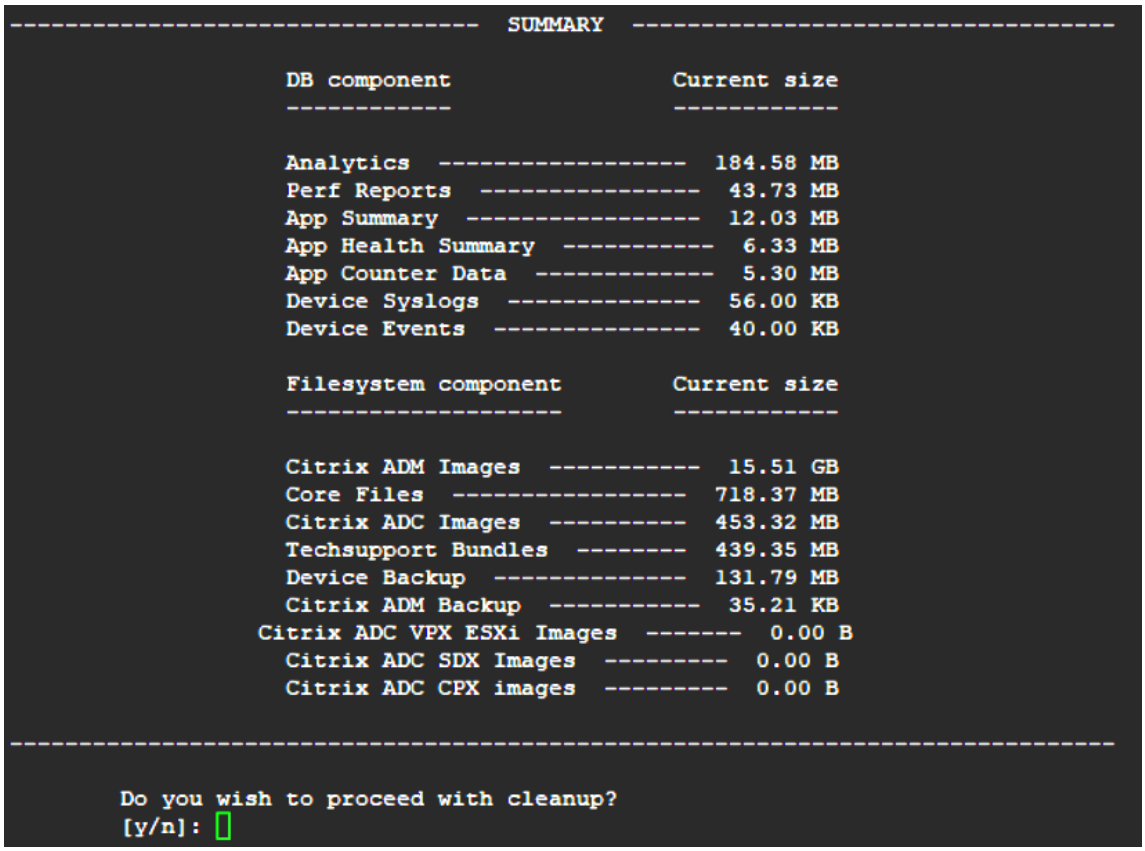
2. Wenn auf dem Bildschirm eine Warnmeldung zum Beenden einiger NetScaler ADM Prozesse angezeigt wird, geben Sie “y”ein, und drücken **Sie die Eingabetaste**.

   Der folgende Bildschirm wird angezeigt, während das System bestimmt, welche Komponenten der Datenbank Sie löschen können, ohne dass sich auf die Kerndateien des Systems auswirkt.

```
--------------------------------------------------------------------------------
*************************** Citrix ADM Cleanup Utility ***************************
--------------------------------------------------------------------------------

        This utility helps you gain disk space by performing cleanup.


                    Checking whether DB is accessible...

                                DB is accessible.

            Please wait. Gathering data. This will take some time.


                                <----------->
```

3. Auf dem Bildschirm wird die Liste der Dateien in der Datenbank angezeigt. Geben Sie “y”ein

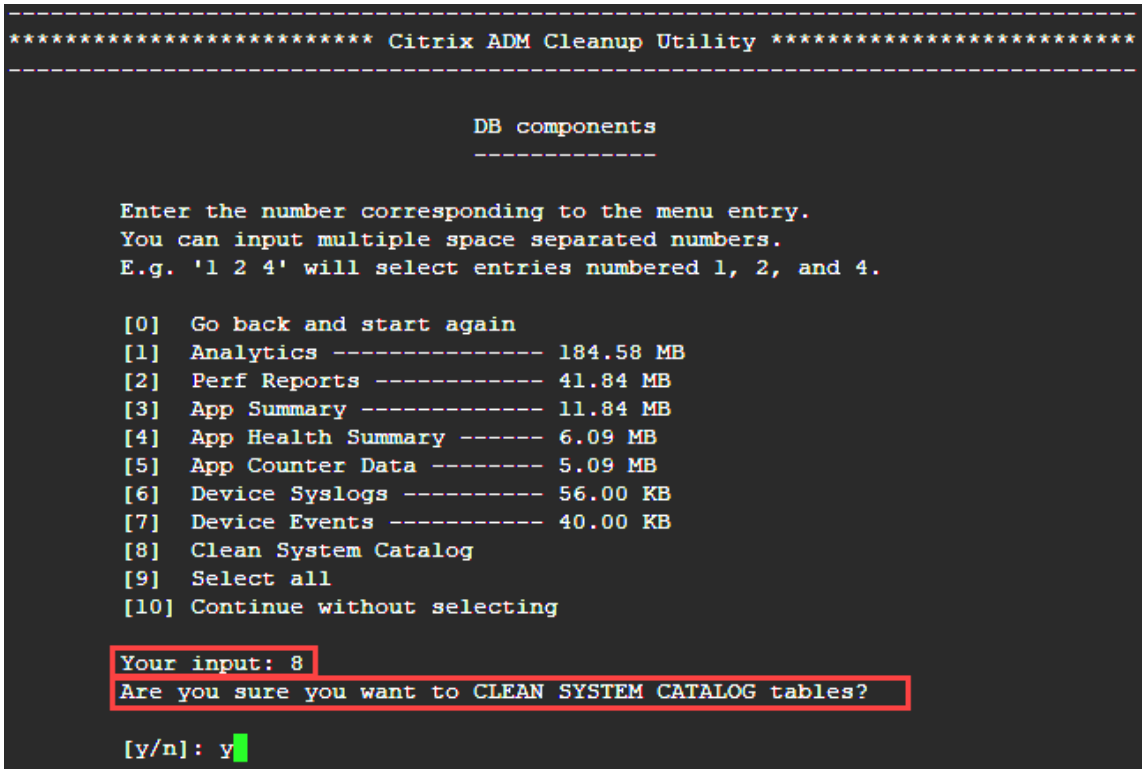
und drücken Sie die Eingabetaste, um den Bereinigungsprozess zu starten.



4. Sie können die spezifische Datenbankkomponente auswählen, die gereinigt werden muss, und die entsprechende Nummer eingeben. Drücken Sie die **Eingabetaste**.

   Um beispielsweise den Systemkatalog zu bereinigen, wählen Sie Option 8 im **DB-Komponentenauswahlme** aus, geben Sie “y”ein und drücken Sie die **Eingabetaste**, um mit der Bereinigung des Systemkatalogs fortzufahren.

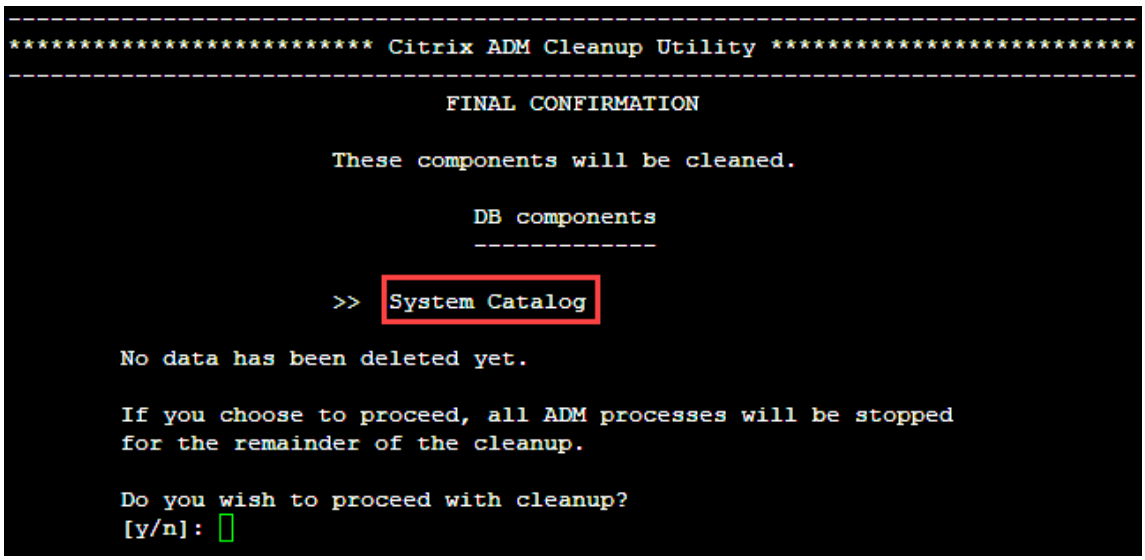
   > **Hinweis**
   >
   > Citrix ADM enthält Benutzertabellen, die als Systemkatalog bezeichnet werden. Der Systemkatalog ist ein Speicherort in der Citrix ADM Datenbank, an dem ein relationales Datenbankmanagementsystem Schemametadaten speichert, z. B. Informationen zu Tabellen und Spalten und internen Datensätzen. Die Tabellen im Systemkatalog sind wie normale Tabellen, in denen sich im Laufe der Zeit überhöhte und tote Zeilen ansammeln können. Daher müssen sie regelmäßig bereinigt werden, um eine optimale Leistung zu erzielen. Es empfiehlt sich, diese Tabellen regelmäßig zu pflegen. Die Aktivität gibt nicht nur Speicherplatz frei, sondern verbessert auch die Gesamtleistung der Datenbank und damit des Citrix ADM.



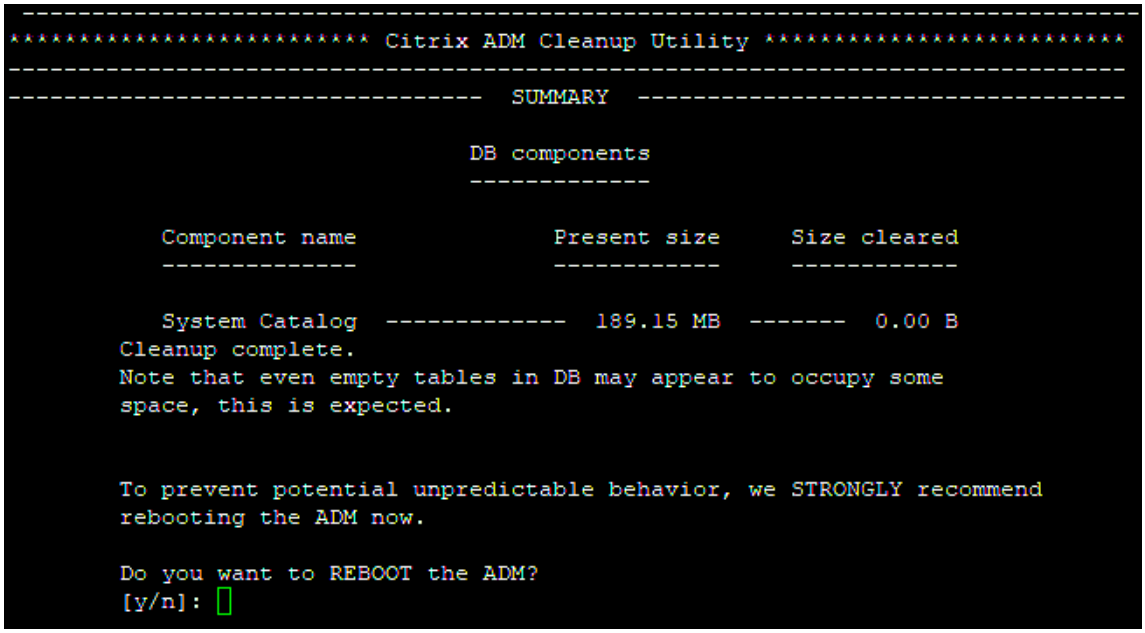
Das Cleanup-Hilfsprogramm bietet Ihnen die Möglichkeit, Datenbankkomponenten und Dateikomponenten zu bereinigen. Sie können eine beliebige Dateikomponente auswählen, indem Sie eine Zahl zwischen „1“und „9“eingeben oder „11”eingeben und die Eingabetaste drücken, um die Datenbankkomponente zu reinigen.

> **Hinweis**
>
> Die Zahl „11”gibt an, dass Sie keine zu reinigende Dateikomponente ausgewählt haben und dass Sie mit der Bereinigung der früheren Datenbankkomponente fortfahren, die Sie zuvor ausgewählt hatten. In diesem Beispiel ist es “Systemkatalog”.

5. Geben Sie “y”ein und drücken Sie im letzten Bestätigungsbildschirm erneut die **Eingabetaste**.



Der Systemkatalog wird bereinigt, was je nach Größe der Tabelle im Systemkatalog einige Zeit in Anspruch nehmen kann. Nach Abschluss des Vorgangs wird ein Übersichtsbildschirm angezeigt.



6. Geben Sie “y”ein, und drücken **Sie die Eingabetaste**, um Citrix ADM neu zu starten.

   Stellen Sie sicher, dass Sie Citrix ADM nach der Systembereinigung neu starten. Warten Sie etwa 30 Minuten, bis interne Datenbankvorgänge abgeschlossen sind, nachdem NetScaler ADM neu gestartet wurde. Sie sollten dann in der Lage sein, eine Verbindung mit der Citrix ADM Datenbank herzustellen. Wenn nicht, führen Sie das Wiederherstellungsskript erneut aus, um mehr Speicherplatz freizugeben. Wenn Citrix ADM ausgeführt wird, sollte es wie erwartet funktionieren.

   > **Hinweis**
   >
   > Die aktuelle Größe der Systemkatalogtabelle ist nie gleich Null nach dem Bereinigen. Dies liegt daran, dass nur leere Zeilen aus der Tabelle entfernt werden und die Tabelle möglicherweise einige gültige Einträge enthält, auch wenn sie bereinigt wurden.

Verwenden des Citrix ADM Datenbank-Wiederherstellungsskripts für eine Citrix ADM-Bereitstellung mit hoher Verfügbarkeit

Das Datenbanksystem für Citrix ADM -Server in einer Hochverfügbarkeitsbereitstellung befindet sich im fortlaufenden Synchronisierungsmodus. Während Sie das neue Datenbank-Wiederherstellungstool verwenden, müssen Sie das Verfahren nicht auf beiden Citrix ADM -Servern replizieren.

1. Melden Sie sich mit einem SSH-Client oder der Hypervisor-Konsole am primären Knoten an.
2. Führen Sie den folgenden Befehl aus:

   ```
   /mps/mas_recovery/mas_recovery.py
   ```


3. Befolgen Sie das Verfahren aus Schritt 2, das für das NetScaler ADM Standalone Deployment Recovery Scriptverfügbar ist

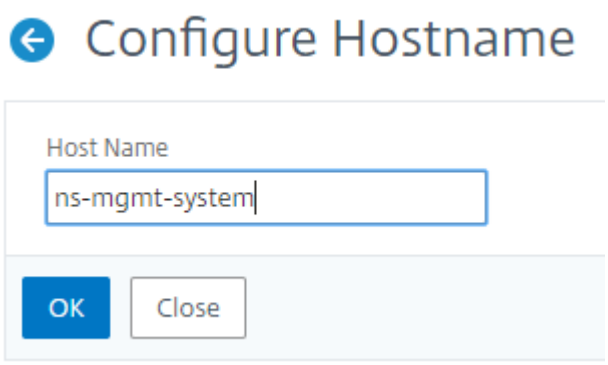
Hostnamen zu einem NetScaler ADM-Server zuweisen

February 5, 2024

Um einen Server mit NetScaler Application Delivery Management (ADM) zu identifizieren, können Sie dem Server einen Hostnamen zuweisen. Der Hostname wird in der universellen Lizenz für NetScaler ADM angezeigt.

So weisen Sie einem NetScaler ADM-Server einen Hostnamen zu:

1. Navigieren Sie in NetScaler ADM zu **System** > **Systemadministration**.
2. Klicken Sie unter **Systemeinstellungen** auf **Hostname ändern**.
3. Geben Sie auf der Seite **Hostname konfigurieren** einen Hostnamen ein, und klicken Sie auf **OK**.

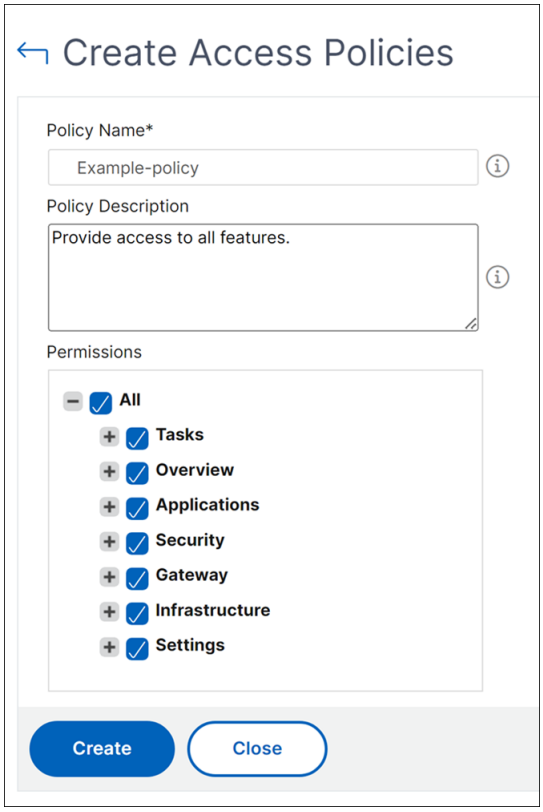


Backup und Wiederherstellen des NetScaler ADM-Servers

February 5, 2024

Sie können regelmäßige Backups des Citrix ADM -Servers erstellen. Sie können die Konfigurationsdateien, Instanzdetails, Systemdaten usw. sichern und wiederherstellen.

> **Wichtig**
>
> Citrix empfiehlt, den ADM-Server mit einer Backup derselben Version wiederherzustellen. Wenn die ADM-Version beispielsweise 13.0 ist, verwenden Sie das 13.0-ADM-Backup, um den Server wiederherzustellen.

> Der Benutzerzugriff zum Backup und Wiederherstellen des ADM-Servers ist begrenzt. Die Seite **System > Backupdateien** wird nur für Benutzer angezeigt, die Zugriff auf alle ADM-Funktionen haben. Ein Benutzer kann nur auf diese Seite zugreifen, wenn seine Zugriffsrichtlinie über alle Berechtigungen verfügt. In der Regel haben Superuser Zugriff auf alle ADM-Funktionen.
>
> 
>
>
> Weitere Informationen finden Sie unter Konfigurieren von Zugriffsrichtlinien.

Sichern Sie vor dem Upgrade die ADM-Serverkonfigurationsdateien aus Sicherheitsgründen.

Das Backup umfasst die folgenden Komponenten:

- Citrix ADM Konfigurationsdateien:
  - SNMP
  - Syslog-Serverkonfigurationsdateien
  - NTP-Dateien
  - SSL-Zertifikate
  - Control Center-Dateien
- Backups von Citrix ADC Instanzen, die vom Citrix ADM -Server verwaltet werden.
- Vorlagen für Konfigurationsprüfungen.

- In der Datenbank gespeicherte Systemdaten:
  - Liste der erstellten Mandanten und Benutzer.
  - Konfiguration des externen Authentifizierungsservers (LDAP, RADIUS und andere).
  - Konfigurationsaufträge und Jobvorlagen wurden erstellt.
- In der Datenbank gespeicherte Infrastruktur- und Anwendungsdaten:
  - Daten von hinzugefügten und verwalteten Citrix ADC Instanzen.
  - Instanzprofildetails, Versionsdetails, Instanzgruppendetails usw.
  - Eine statische Anwendung (Gruppe virtueller Server), die vom Administrator erstellt wurde.
- SNMP-Einstellungen.

> **Note**
>
> Analytics-Daten, Ereignisse, ADM-Lizenzen und Syslog-Nachrichten sind vom Backup ausgeschlossen.

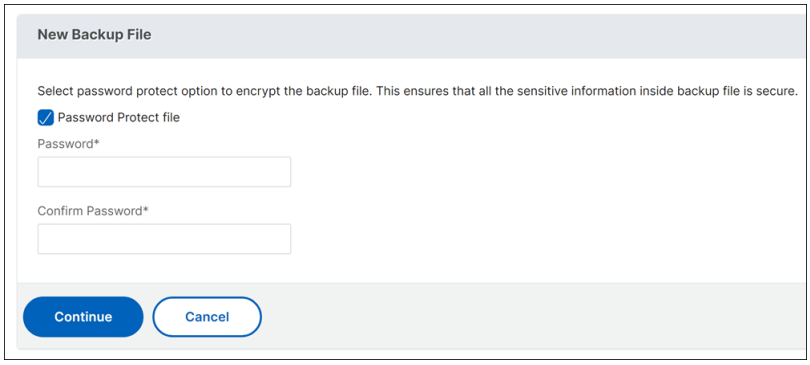
Sichern der NetScaler ADM Konfiguration

Standardmäßig sichert der Citrix ADM -Server die Konfiguration alle 24 Stunden (um 00,30 Uhr). Sie können auch die Uhrzeit für das Backup planen und auswählen. Außerdem können Sie eine Kopie der gesicherten Datei auf ein anderes System verschieben.

Das Backup wird als komprimierte TAR-Datei gespeichert, die auch verschlüsselt werden kann. Standardmäßig werden drei Sicherungsdateien auf dem Server aufbewahrt. Um Probleme mit geringem Speicherplatz zu vermeiden, können Sie maximal 10 Backupdateien auf dem NetScaler ADM -Server speichern. Citrix empfiehlt jedoch, einige Kopien Ihrer Backupdateien auf dem Server zu speichern oder die Dateien vorsorglich auf ein anderes System zu übertragen .

So Backup Sie eine NetScaler ADM-Konfiguration:

1. Navigieren Sie zu **System > Backupdateien**, und klicken Sie dann auf **Sichern**.
2. Um die Backupdatei zu verschlüsseln, aktivieren Sie das Kontrollkästchen **Kennwortschutzdatei**, und geben Sie dann ein Kennwort zum Verschlüsseln der Datei ein.

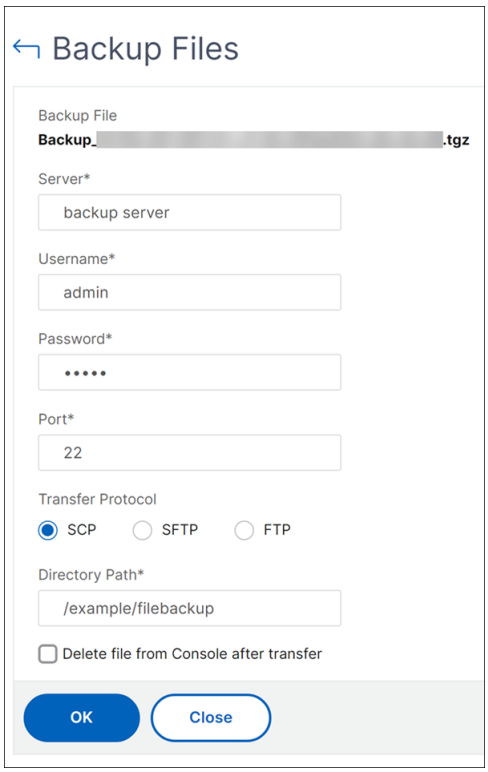


Übertragen einer NetScaler ADM -Backupdatei auf ein externes System

Als Vorsichtsmaßnahme können Sie eine Kopie der Backupdatei auf ein anderes System übertragen. Wenn Sie die Konfiguration wiederherstellen möchten, laden Sie die Datei zuerst auf den NetScaler ADM-Server hoch und führen Sie dann den Wiederherstellungsvorgangdurch.

So übertragen Sie eine Citrix ADM Backupdatei:

1. Navigieren Sie zu**System > Backupdateien**.
2. Wählen Sie die Backupdatei aus, die Sie auf ein anderes System verschieben möchten, und klicken Sie dann auf**Übertragen**.
3. Geben Sie auf der Seite **Backup-Dateien** die folgenden Parameter an:
    - **Server** —IP-Adresse des Systems, auf das Sie die gesicherte Datei übertragen möchten.
    - **Benutzername und Kennwort** —Benutzeranmeldedaten des neuen Systems, in das die gesicherten Dateien kopiert werden.
    - **Port** —Portnummer des Systems, auf das die Dateien übertragen werden.
    - **Übertragungsprotokoll** —Protokoll, das für die Übertragung der Sicherungsdatei verwendet wird. Sie können die Protokolle SCP, SFTP oder FTP auswählen, um die gesicherte Datei zu übertragen.
    - **Verzeichnispfad** - Der Speicherort, an den die gesicherte Datei auf dem neuen System übertragen wird.
4. Sie können die Backupdatei nach der Übertragung aus NetScaler ADM löschen, indem Sie das Kontrollkästchen **Datei aus der Anwendungsübermittlungsverwaltung nach der Übertragung löschen** aktivieren.
5. Klicken Sie auf **OK**, um die Übertragung durchzuführen.



> **Hinweis**
>
> Um eine Kopie der Backupdatei in Ihrem lokalen System zu speichern, navigieren Sie zu **System > Backupdateien**, wählen Sie die zu kopierende Datei aus, und klicken Sie dann auf **Herunterladen**.

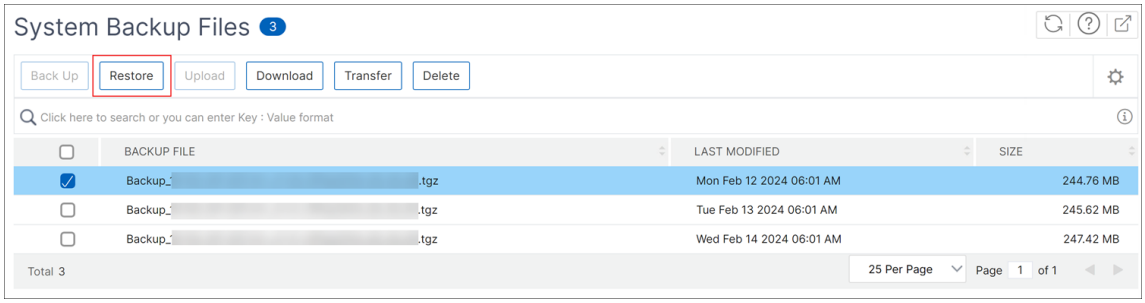
Wiederherstellen der NetScaler ADM Konfiguration aus einer Backupdatei

Wenn Sie die Citrix ADM Konfiguration aus einer zuvor gesicherten Datei wiederherstellen, wird die Backupdatei durch den Wiederherstellungsvorgang aufgehoben und anschließend die Konfiguration wiederhergestellt. Der Wiederherstellungsvorgang löscht die vorhandene Konfiguration und ersetzt sie durch die Konfiguration in der Sicherungsdatei.

> **Hinweis**
>
> Der Wiederherstellungsvorgang schlägt fehl, wenn die Sicherungsdatei umbenannt wird oder wenn der Inhalt der Sicherungsdatei geändert wird.

So stellen Sie eine NetScaler ADM Konfiguration aus einer Backupdatei wieder her:

1. Navigieren Sie zu**System > Backupdateien**.
2. Wählen Sie die Backupdatei aus, die Sie wiederherstellen möchten, und klicken Sie dann auf **Wiederherstellen**.



3. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

> **Hinweis**
>
> Um die Konfiguration aus einer Backupdatei wiederherzustellen, die in einem externen System gespeichert ist, laden Sie die Backupdatei auf den ADM-Server hoch, bevor Sie den Wiederherstellungsvorgang ausführen. Um die Datei hochzuladen, navigieren Sie zu **System > Backupdateien**, und klicken Sie dann auf **Hochladen**.

Auditing-Informationen anzeigen

January 23, 2024

Syslog ist ein Standardprotokoll für die Protokollierung. Es besteht aus zwei Komponenten: dem Syslog-Auditing-Modul, das auf der Citrix Application Delivery Controller-Instanz (ADC) ausgeführt wird, und dem Syslog-Server, der entweder auf dem zugrunde liegenden FreeBSD-Betriebssystem (OS) der Citrix ADC-Instanz oder auf einem Remotesystem ausgeführt werden kann. SYSLOG verwendet das User Datagram Protocol (UDP) für die Datenübertragung.

Syslog ermöglicht die Isolierung des Systems, das Informationen generiert, und des Systems, in dem die Informationen gespeichert werden. Sie können Protokollinformationen konsolidieren und Erkenntnisse aus den gesammelten Daten gewinnen. Sie können syslog auch so konfigurieren, dass verschiedene Arten von Ereignissen protokolliert werden.

Sie können die Syslog-Meldungen überwachen, die ein Citrix ADC-Gerät generiert, wenn Sie das Gerät so konfigurieren, dass Syslog-Nachrichten an Citrix Application Delivery Management (ADM) umgeleitet werden. Sie können einen Job zum Erstellen von Syslog-Servern planen, die mithilfe der integrierten Vorlagenfunktion in Citrix ADM verschiedene Arten von Syslog-Daten generieren.

Konfigurieren Sie zunächst einen Syslog-Server, an den die Instanz Protokollinformationen senden kann. Geben Sie dann das Datums- und Uhrzeitformat für die Aufzeichnung von Protokollmeldungen an.

So konfigurieren Sie einen Syslog-Server auf Citrix ADM:

1. Navigieren Sie zu**System** > **Überwachung**. Wählen Sie unter **Konfigurationsübersicht**die Option **Syslog-Server**aus. Oder Sie können zu **System** > **Auditing** > **Syslog-Server**navigieren.
2. Klicken Sie auf der Seite **Syslog-Server** auf **Hinzufügen.**
3. Geben Sie auf der Seite **Syslog-Server erstellen** die folgenden Werte ein:

    - **Name** —Name für den Syslog-Server.
    - **IP-Adresse** —IP-Adresse des Syslog-Servers.
    - **Port** —Syslog-Serverport.

4. Wählen Sie die Protokollebenen (Alle, Keine oder Benutzerdefiniert). Wählen Sie entsprechend die Schweregrade aus.
5. Klicken Sie auf **Erstellen**.

So konfigurieren Sie das Syslog-Datums- und Uhrzeitformat auf Citrix ADM:

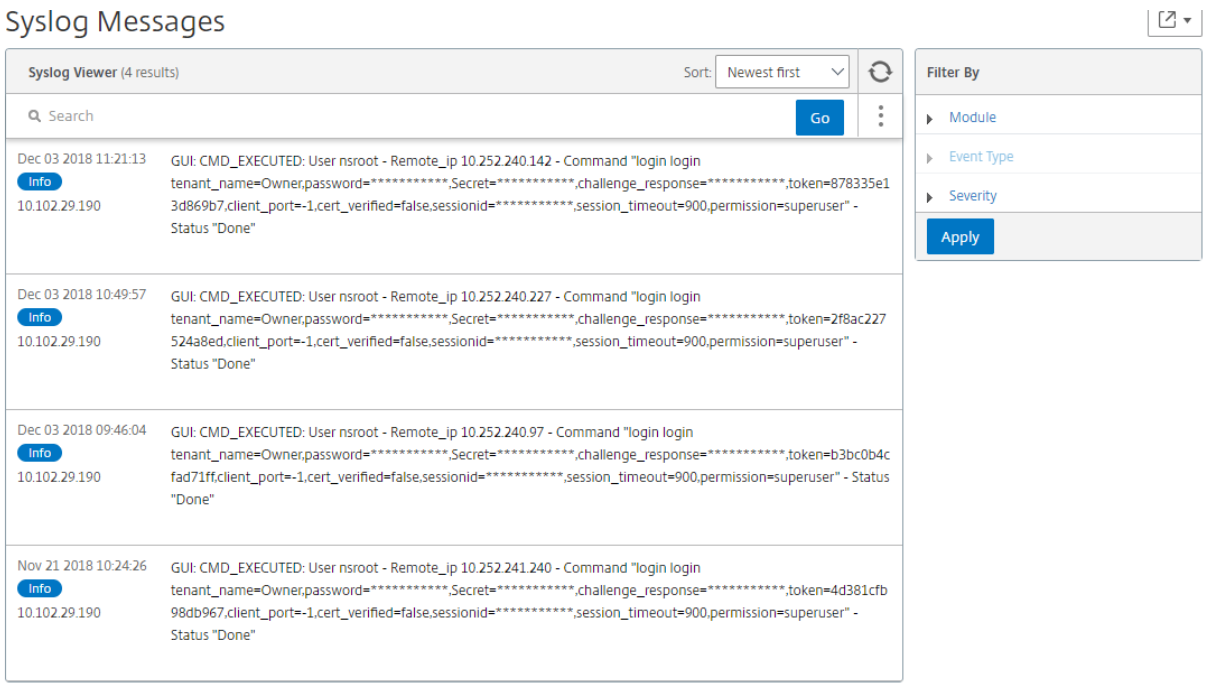
1. Navigieren Sie zu**System** > **Überwachung**. Wählen Sie unter **Konfigurationsübersicht** die Option **Syslog-Server** aus.
2. Wählen Sie auf der Seite **Syslog-Server** einen Syslog-Server aus, und klicken Sie dann auf **Syslog-Parameter.**
3. Geben Sie auf der Seite **Syslog-Parameter konfigurieren** das Datums- und Uhrzeitformat an.
4. Klicken Sie auf **OK**.

So zeigen Sie Syslog-Meldungen auf Citrix ADM an:

Sie können jetzt alle Ihre Syslog-Nachrichten anzeigen, die auf Ihren verwalteten Citrix ADC-Instanzen generiert wurden, wenn Sie Ihre Instanz so konfiguriert haben, dass sie die Syslog-Nachrichten an den Citrix ADM Server umleitet. Die Syslog-Nachrichten werden zentral in der Datenbank des Citrix ADM Servers gespeichert und stellen sie zu Prüfungszwecken im Syslog Viewer zur Verfügung. Sie können diese Protokollierungsinformationen konsolidieren und aus den gesammelten Daten Berichte für Analysen ableiten.

Sie können diese Informationen nach Modul, Ereignistyp und Schweregrad filtern. Sie können syslog auch so konfigurieren, dass verschiedene Arten von Ereignissen protokolliert werden.

Um den **Syslog-Viewer** aufzurufen, navigieren Sie zu **System** > **Auditing**. Wählen Sie auf der **Auditing-Seite** unter **Audit-Meldungen** die Option **Syslog-Meldungen** aus. Wählen Sie die entsprechenden Filter, um Ihre Systemprotokollmeldungen anzuzeigen.



SSL-Einstellungen konfigurieren

February 5, 2024

SSL (Secure Socket Layer) und TLS (Transport Layer Security) sind häufig verwendete Sicherheitsnetzwerkprotokolle, die eine verschlüsselte Kommunikation zwischen Benutzern und Servern ermöglichen. Sie können SSL-Einstellungen in Citrix Application Delivery Management (ADM) konfigurieren und den Typ der Clients angeben, die eine Verbindung zum System herstellen.

So konfigurieren Sie SSL-Einstellungen für Citrix ADM:

1. Navigieren Sie zu **System** > **Systemadministration**. Klicken Sie unter **Systemeinstellungen**auf **SSL-Einstellungen konfigurieren**.
2. Überprüfen Sie auf der Seite **SSL-Einstellungen** die aktuellen Protokolleinstellungen und die auf das System angewandten Verschlüsselungssammlungen.
3. Um die Protokolleinstellungen zu ändern, navigieren Sie zu **Einstellungen bearbeiten** > **Protokolleinstellungen** und nehmen Sie die gewünschten Änderungen vor.
4. Um die angewendeten Cipher Suites zu ändern, navigieren Sie zu **Einstellungen bearbeiten** > **Cipher Suites und nehmen** Sie die gewünschten Änderungen vor.
5. Klicken Sie auf **OK**und dann auf **Schließen**.

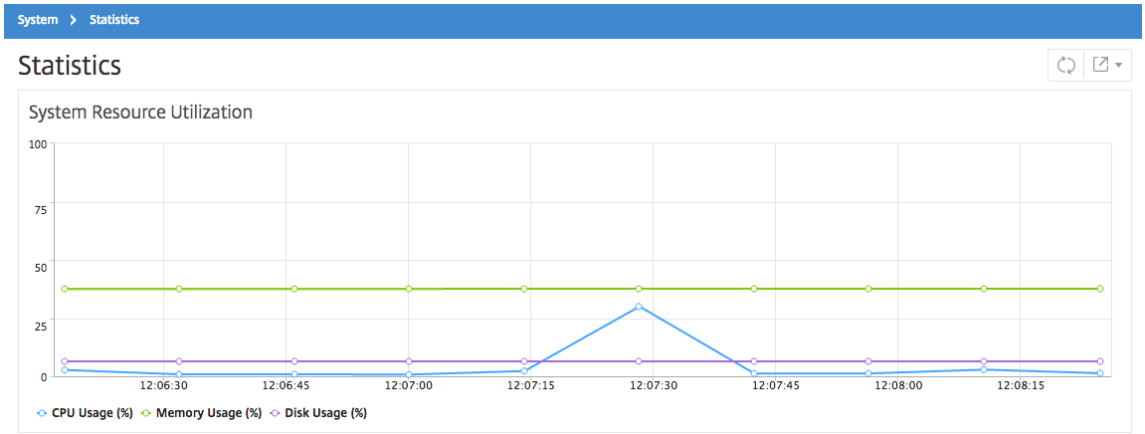
CPU-, Arbeitsspeicher- und Datenträgernutzung überwachen

January 23, 2024

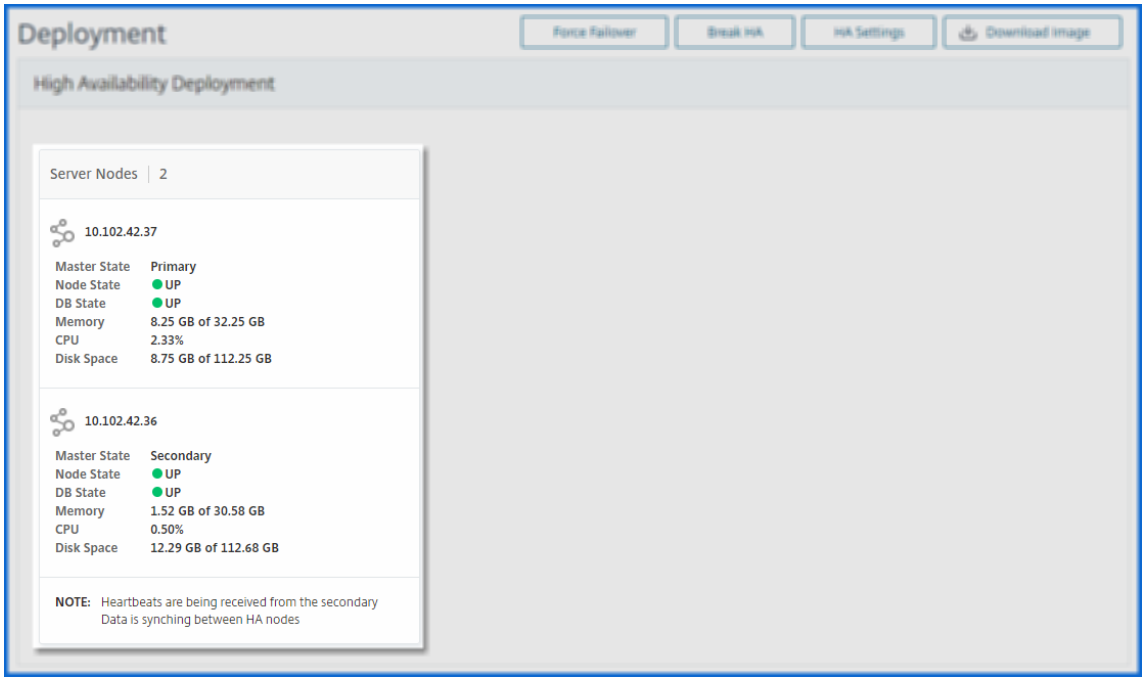
Sie können die in Protokollen und Statistiken gespeicherten Informationen verwenden. Diese Informationen werden auch in Berichten angezeigt, die Ihnen bei der Konfiguration und Wartung von Citrix Application Delivery Management (ADM) helfen.

So überwachen Sie die CPU-, Speicher- und Datenträgernutzung:

- **Eigenständige Bereitstellung.** Navigieren Sie zu **System** > **Statistik**. Sie können in Echtzeit CPU-, Speicher- und Datenträgerauslastungsdiagramme anzeigen.



- **Bereitstellung mit hoher Verfügbarkeit.** Navigieren Sie zu **System** > **Bereitstellung**. Die Statistiken für Arbeitsspeicher, CPU, Speicherplatz und verwaltete Instanzen werden numerisch angezeigt, wie in der folgenden Abbildung dargestellt:



Benachrichtigungseinstellungen konfigurieren

February 5, 2024

Sie können einen Benachrichtigungstyp auswählen, um Benachrichtigungen für die folgenden Funktionen zu erhalten:

- **Ereignisse** —Liste der Ereignisse, die für NetScaler ADC-Instanzen generiert werden. Weitere Informationen finden Sie unter Aktionen für Ereignisregeln hinzufügen.
- **Lizenzen** —Liste der Lizenzen, die derzeit aktiv sind, bald ablaufen usw. Weitere Informationen finden Sie unter Ablauf der NetScaler ADM-Lizenz.
- **SSL-Zertifikate** —Liste der SSL-Zertifikate, die NetScaler ADC-Instanzen hinzugefügt werden. Weitere Informationen finden Sie unter Ablauf des SSL-Zertifikats

ADM unterstützt die folgenden Benachrichtigungstypen:

- E-Mail
- SMS
- Slack
- PagerDuty
- ServiceNow

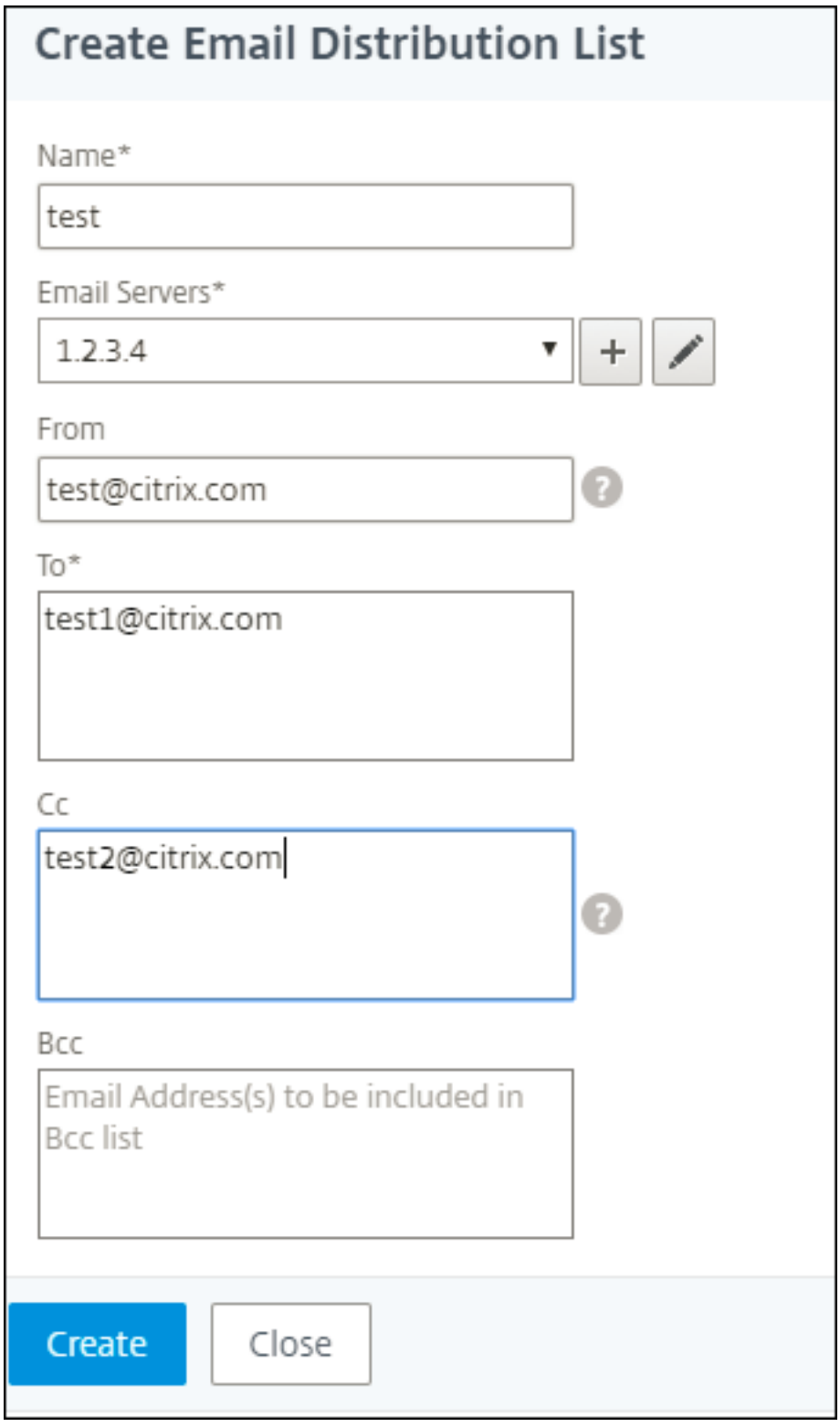
Für jeden Benachrichtigungstyp zeigt die ADM-GUI die konfigurierte Verteilerliste oder das konfigurierte Profil an. Das ADM sendet Benachrichtigungen an die ausgewählte Verteilerliste oder das ausgewählte Profil.

Erstellen einer E-Mail-Verteilerliste

Um E-Mail-Benachrichtigungen für ADM-Funktionen zu erhalten, müssen Sie einen E-Mail-Server und eine Verteilerliste hinzufügen.

Führen Sie die folgenden Schritte aus, um eine E-Mail-Verteilerliste zu erstellen:

1. Navigieren Sie zu **System > Benachrichtigungen** .
2. Klicken Sie **unter E-Mail**auf **Hinzufügen**.
3. Geben Sie unter **E-Mail-Verteilerliste erstellen**die folgenden Details an:
    - **Name** - Geben Sie den Namen der Verteilerliste an.
    - **E-Mail-Server** —Wählen Sie den E-Mail-Server aus, der E-Mail-Benachrichtigungen sendet. Wenn Sie einen E-Mail-Server hinzufügen möchten, klicken Sie auf **Hinzufügen**.
    - **Von** —Geben Sie die E-Mail-Adresse an, von der ADM Nachrichten senden muss.
    - **An** - Geben Sie die E-Mail-Adressen an, an die ADM Nachrichten senden soll.
    - **Cc** —Geben Sie die E-Mail-Adressen an, an die ADM Nachrichtenkopien senden muss.
    - **Bcc** —Geben Sie die E-Mail-Adressen an, an die ADM Nachrichtenkopien senden muss, ohne die Adressen anzuzeigen.



4. Klicken Sie auf **Erstellen**.

Wiederholen Sie diesen Vorgang, um mehrere E-Mail-Verteilerlisten zu erstellen. Auf der Registerkarte **E-Mail** werden alle in ADM vorhandenen E-Mail-Verteilerlisten angezeigt.

Erstellen Sie eine SMS-Verteilerliste

Um SMS-Benachrichtigungen für ADM-Funktionen zu erhalten, müssen Sie einen SMS-Server und Telefonnummern hinzufügen.

Führen Sie die folgenden Schritte aus, um die SMS-Benachrichtigungseinstellungen zu konfigurieren:

1. Navigieren Sie zu **System > Benachrichtigungen** .
2. Klicken Sie in **SMS**auf **Hinzufügen**.
3. Geben Sie unter **SMS-Verteilerliste erstellen**die folgenden Details an:
    - **Name** - Geben Sie den Namen der Verteilerliste an.
    - **SMS-Server** —Wählen Sie den SMS-Server, der SMS-Benachrichtigungen sendet.
    - **An** —Geben Sie die Telefonnummer an, an die ADM Nachrichten senden muss.
4. Klicken Sie auf **Erstellen**.

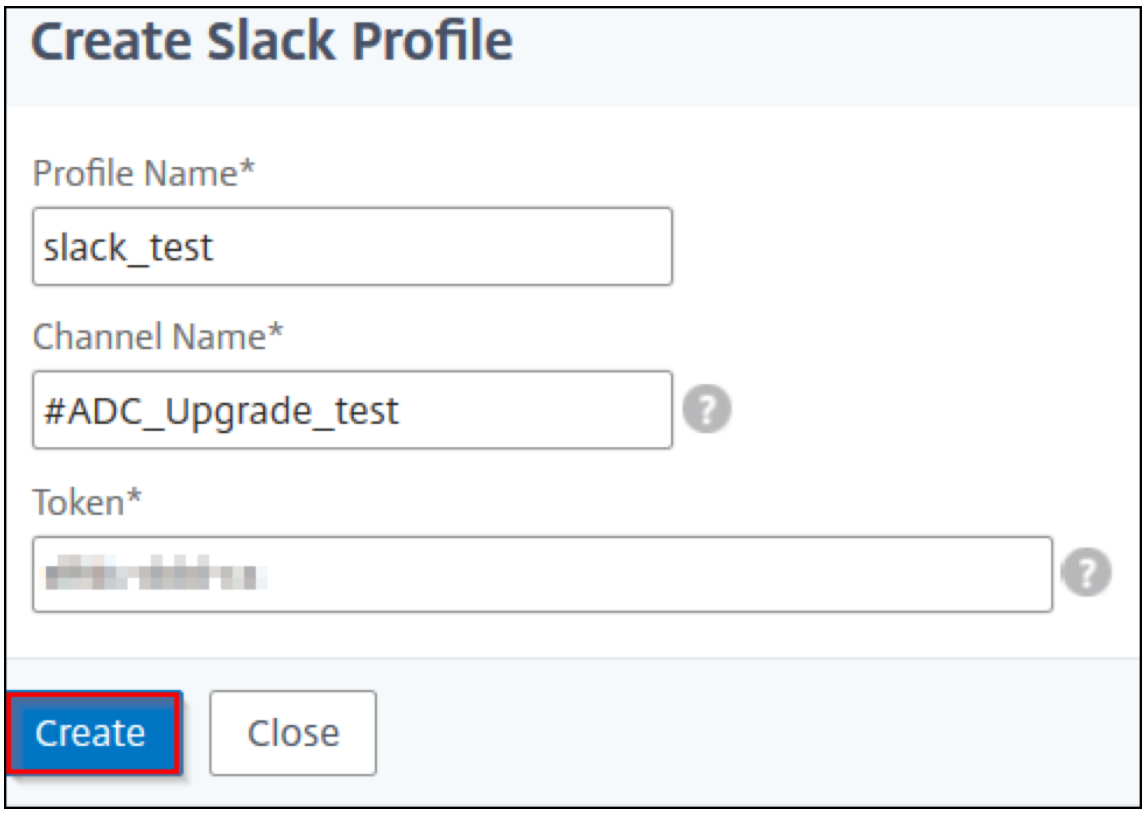
Wiederholen Sie diesen Vorgang zum Erstellen mehrerer SMS-Verteilerlisten. Auf der Registerkarte **SMS** werden alle in ADM vorhandenen SMS-Verteilerlisten angezeigt.

Erstellen eines Slack Profils

Um Slack-Benachrichtigungen für ADM-Funktionen zu erhalten, müssen Sie ein Slack-Profil erstellen.

Führen Sie die folgenden Schritte aus, um ein Slack Profil zu erstellen:

1. Navigieren Sie zu **System > Benachrichtigungen** .
2. Klicken Sie in **Slack**auf **Hinzufügen**.
3. Geben Sie unter **“Slack-Profil erstellen**”die folgenden Details an:
    - **Profilname** —Geben Sie den Profilnamen an. Dieser Name wird in der Slack-Profilliste angezeigt.
    - **Kanalname** —Geben Sie den Namen des Slack-Channels an, an den ADM Benachrichtigungen senden muss.
    - **Webhook-URL** —Geben Sie die Webhook-URL des Kanals an. Eingehende Webhooks sind eine einfache Möglichkeit, Nachrichten aus externen Quellen in Slack zu posten. Die URL ist intern mit dem Kanalnamen verknüpft. Und alle Ereignisbenachrichtigungen werden an diese URL gesendet werden, werden auf dem dafür vorgesehenen Slack Kanal veröffentlicht. Ein Beispiel für Webhook lautet wie folgt: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK



4. Klicken Sie auf **Erstellen**.

Wiederhole diesen Vorgang, um mehrere Slack-Profile zu erstellen Auf der Registerkarte **Slack** werden alle in ADM vorhandenen Slack-Profile angezeigt.

Erstellen eines PagerDuty-Profils

Sie können ein PagerDuty-Profil hinzufügen, um die Vorfallbenachrichtigungen basierend auf den PagerDuty-Konfigurationen zu überwachen. Mit PagerDuty können Sie Benachrichtigungen per E-Mail, SMS, Push-Benachrichtigung und Telefonanruf an einer registrierten Nummer konfigurieren.

Bevor Sie ein PagerDuty-Profil in NetScaler ADM hinzufügen, stellen Sie sicher, dass Sie die erforderlichen Konfigurationen in PagerDuty abgeschlossen haben. Um mit PagerDuty zu beginnen, lesen Sie die PagerDuty-Dokumentation.

Führen Sie die folgenden Schritte aus, um ein PagerDuty-Profil zu erstellen:

1. Navigieren Sie zu **System > Benachrichtigungen** .
2. Klicken Sie in **PagerDuty**auf **Hinzufügen**.
3. Geben Sie unter **PagerDuty-Profil erstellen**die folgenden Details an:
    - **Profilname** —Geben Sie einen Profilnamen Ihrer Wahl an.

- **Integrationsschlüssel** —Geben Sie den Integrationsschlüssel an. Sie können diesen Schlüssel von Ihrem PagerDuty-Portal erhalten.

4. Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Services und Integrationen in der PagerDuty-Dokumentation.

Wiederholen Sie diesen Vorgang, um mehrere PagerDuty-Profile zu erstellen. Auf der Registerkarte **PagerDuty** werden alle in ADM vorhandenen PagerDuty-Profile angezeigt.

Das ServiceNow-Profil anzeigen

Wenn Sie ServiceNow-Benachrichtigungen für NetScaler ADC-Ereignisse und ADM-Ereignisse aktivieren möchten, müssen Sie NetScaler ADM mit dem ITSM-Connector in ServiceNow integrieren. Weitere Informationen finden Sie unter Integrieren von NetScaler ADM mit der ServiceNow-Instanz.

Führen Sie die folgenden Schritte aus, um das ServiceNow-Profil anzuzeigen und zu überprüfen:

1. Navigieren Sie zu **System > Benachrichtigungen** .
2. Wählen Sie in **ServiceNow**das Profil **Citrix_Workspace_SN** aus der Liste aus.
3. Klicken Sie auf **Test**, um automatisch ein ServiceNow-Ticket zu generieren und die Konfiguration zu überprüfen.

   Wenn Sie ServiceNow-Tickets in der NetScaler ADM GUI anzeigen möchten, wählen Sie **ServiceNow Tickets**aus.

Technische Supportdatei generieren

February 5, 2024

Citrix empfiehlt, dass Sie ein Archiv mit Daten und Statistiken von NetScaler Application Delivery Management (ADM) erstellen, bevor Sie sich an den technischen Support wenden, um ein Problem zu beheben. Das Archiv ist eine TAR-Datei, die Sie an das technische Support-Team senden können.

> **Hinweis**
>
> Für NetScaler ADM-Server in einem Hochverfügbarkeitsmodus können Sie von einem der Server eine Datei für den technischen Support generieren. Citrix empfiehlt, die IP-Adresse des virtuellen Lastausgleichsservers nicht zum Generieren der Datei für den technischen Support zu verwenden.

So konfigurieren und senden Sie eine Datei für den technischen Support von NetScaler ADM:

1. Navigieren Sie zu **System** > **Diagnose** > **Technischer Support**, und klicken Sie dann auf **Datei für technischen Support erstellen**.
2. Wählen Sie auf der Seite **Supportdatei generieren** die folgenden Optionen aus:

- **Debug-Protokolle sammeln** —Wählen Sie diese Option, um `afdecoder`-Protokolle zu sammeln.
- **Dauer** —Geben Sie die Dauer ein, für die Debug-Protokolle gesammelt werden müssen. Diese Option wird nur angezeigt, wenn Sie die Option **Debug-Protokolle sammeln** aktivieren.
- **Datenverteilung sammeln** —Wählen Sie diese Option aus, um unterschiedliche Protokolle aus der Datenbank zu sammeln.

```
1  The archive file is created as a TAR file.
2
3  For example, the archive file that is created might be named as
      follows:   Citrix_ADM_<ADM_IP_address>_<DDMMYY>_<time_stamp>.
      tar.gz
```

1. Sie können die technischen Support-Dateien auf zwei Arten an das Support-Team senden:

   a) Sie können die Datei von der ADM-GUI in Ihren lokalen Speicher herunterladen und dann einen Webbrowser zum Hochladen in CIS verwenden.

   b) Sie können die technischen Supportdateien auch auf die Citrix Insight Services (CIS) -Website hochladen, indem Sie ein Skript auf der ADM-Konsole ausführen.

      i. Melden Sie sich mithilfe von SSH an der ADM-Konsole an.

      ii. Wechseln Sie zur Shell-Eingabeaufforderung und geben Sie Folgendes

      /mps/collector_upload.pl

Der vollständige Befehl ist unten mit den Attributen angegeben, die Sie angeben müssen:

```
1  /mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<
      proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr
       <sr>] [-description <description>] [-debug] <file>
2  <!--NeedCopy-->
```

Der Vorteil der Ausführung des Perl-Skripts besteht darin, dass Sie die technische Support-Datei nicht von ADM auf Ihr lokales System herunterladen und dann in CIS hochladen müssen. Optional können Sie die Datei direkt in CIS hochladen, indem Sie einen Proxy von der ADM-Konsole verwenden.

Stellen Sie sicher, dass Sie ein Konto bei CIS haben. Sie können die Anmeldeinformationen Ihres Citrix-Kontos verwenden, um Dateien in CIS hochzuladen.

Was passiert, wenn Sie keinen Proxyserver haben? Oder was ist, wenn Sie Probleme mit SSL-Forward-Proxys haben? (Dies kann passieren, wenn das Perl-Skript dem Stammzertifikat des Proxyservers

nicht vertraut.)
Sie können die Datei trotzdem direkt aus der ADM-Shell in CIS hochladen.

> **Hinweis:**
>
> Sie können die Datei weiterhin herunterladen und per E-Mail an den technischen Support von Citrix senden, wenn ADM die Datei nicht von der Konsole in CIS hochladen kann. Oder Sie können die Datei von ADM in Ihren lokalen Speicher herunterladen und dann einen Webbrowser zum Hochladen in CIS verwenden.

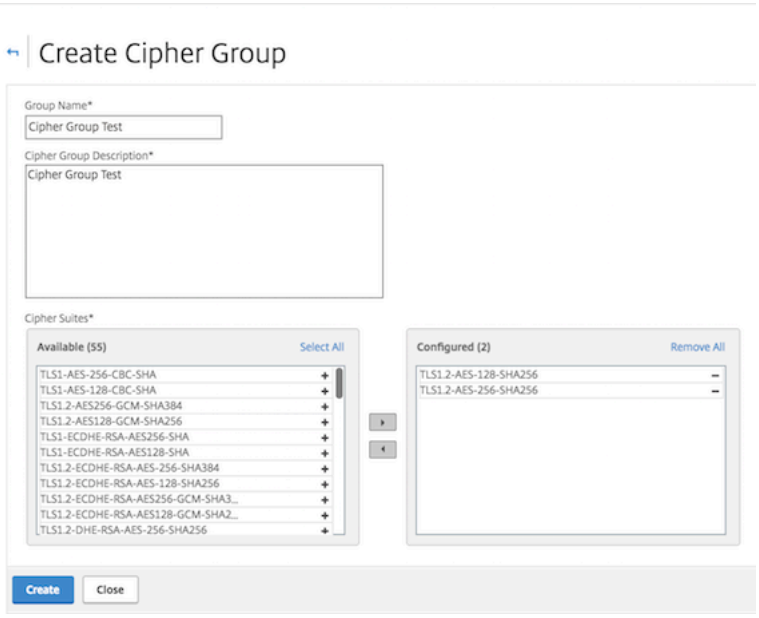
Chiffriergruppe konfigurieren

February 5, 2024

Eine Verschlüsselungsgruppe ist ein Satz von Verschlüsselungssammlungen, die Sie an einen virtuellen SSL-Server, -Dienst oder -Dienstgruppe auf der Citrix Application Delivery Controller (ADC) -Instanz binden. Eine Verschlüsselungssuite besteht aus einem Protokoll, einem Schlüsselaustauschalgorithmus (Kx), einem Authentifizierungsalgorithmus (Au), einem Verschlüsselungsalgorithmus (Enc) und einem Nachrichtenauthentifizierungscode (Mac) -Algorithmus.

So fügen Sie eine Verschlüsselungsgruppe in NetScaler ADM hinzu:

1. Navigieren Sie zu **System** > **Administration**
2. Klicken Sie unter **SSL-Einstellungen**auf **Verschlüsselungsgruppen**
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie auf der Seite **Verschlüsselungsgruppe erstellen** die folgenden Details ein:
    - **Gruppenname** —Name für die Verschlüsselungsgruppe.
    - **Beschreibung der Verschlüsselungsgruppe** —Geben Sie eine Beschreibung für Ihre Verschlüsselungsgruppe ein.
    - **Cipher Suites** —Klicken Sie auf Hinzufügen, um Cipher Suites aus der Liste Verfügbar auszuwählen, und verschieben Sie dann die ausgewählten (oder alle) Cipher Suites in die Liste Konfiguriert.
5. Klicken Sie auf **Erstellen**.



SNMP-Trap-Ziel, Manager-Community und Benutzer erstellen

February 5, 2024

Wenn auf Citrix ADM ein abnormaler Zustand auftritt, wird ein SNMP-Trap generiert. Die Traps werden dann an ein Remotegerät gesendet, das Trap-Zielserver oder *SNMP-Trap-Ziel*genannt wird. Hier wird Citrix ADM als Trap-Ziel konfiguriert. Sie können den SNMP-Agent systemspezifische Informationen von einem Remotegerät abfragen, das *SNMP-Manager*genannt wird. Der Agent durchsucht dann die MIB (Management Information Base) nach angeforderten Daten und sendet die Daten an den SNMP-Manager.

So erstellen Sie ein SNMP-Trap-Ziel in Citrix ADM:

1. Navigieren Sie zu **System** > **SNMP** > **Trap-Ziele**.
2. Klicken Sie unter **SNMP-Traps**auf **Hinzufügen**, um einen SNMP-Trap zu erstellen, und geben Sie dann die folgenden Details an:
    - **Version.** Wählen Sie die zu verwendende SNMP-Version aus.
    - **Zielserver.** Name oder IP-Adresse des Trap-Ziels.
    - **Hafen.** Geben Sie den Port des Trap-Ziels ein. Der Port ist standardmäßig auf 162 gesetzt.
    - **Gemeinschaft.** Geben Sie die Community-Zeichenfolge an, die verwendet werden soll, wenn eine Trap an den Trap-Listener gesendet wird.
3. Klicken Sie auf **Erstellen**.

> **Hinweis**
>
> Wenn Sie ein SNMP v3-Trap-Ziel erstellen, geben Sie die SNMP-Benutzeranmeldeinformationen an, an die Sie den Trap binden möchten. Um eine SNMP-Benutzeranmeldeinformationen hinzuzufügen, klicken Sie auf **Einfügen** und fügen Sie dann den Benutzer aus der Liste der verfügbaren SNMP-Benutzer hinzu.

So erstellen Sie eine SNMP-Manager-Community:

1. Navigieren Sie zu **System** > **SNMP** > **Manager**.
2. Klicken Sie unter **SNMP Manager**auf **Hinzufügen**, um eine SNMP-Manager-Community zu erstellen, und geben Sie dann die folgenden Details an:
   - **SNMP-Manager.** Geben Sie den Namen oder die IP-Adresse des SNMP-Managers ein.
   - **Gemeinschaft.** Geben Sie die Community-Zeichenfolge an, die verwendet werden soll, wenn Traps an den Trap-Listener gesendet werden.
3. Optional können Sie das Kontrollkästchen **Verwaltungsnetzwerk aktivieren** aktivieren, um die **Netzmaske** anzugeben, die die Subnetzmaske des SNMP-Manager-Netzwerks ist.
4. Klicken Sie auf **Erstellen**.

Um einen SNMP-Benutzer zu erstellen:

1. Navigieren Sie zu **System** > **SNMP** > **Benutzer**.
2. Klicken Sie unter **SNMP-Benutzer**auf **Hinzufügen**.
3. Geben Sie den Benutzernamen ein und weisen Sie dem Benutzer über das Menü eine Sicherheitsstufe zu.
4. Geben Sie basierend auf der Sicherheitsstufe, die Sie dem Benutzer zugewiesen haben, zusätzliche Authentifizierungsprotokolle an, wie Authentifizierungsprotokolle, Datenschutzkennwörter und Zuweisen von SNMP-Ansichten.

Systemalarme konfigurieren und anzeigen

February 5, 2024

Sie können einen Satz von Alarmen aktivieren und konfigurieren, um den Zustand der NetScaler Application Delivery Management (ADM) -Server zu überwachen. Sie müssen Systemalarme konfigurieren, um sicherzustellen, dass Sie kritische oder größere Systemprobleme kennen. Sie möchten z. B. benachrichtigt werden, wenn die CPU-Auslastung hoch ist oder wenn mehrere Anmeldefehler auf dem

Server auftreten. Für einige Alarmkategorien, wie CPUUsageHigh oder MemoryUsageHigh, können Sie Schwellenwerte festlegen und den Schweregrad (z. B. Critical oder Major) für jede Alarmkategorie definieren. Für einige Kategorien, wie inventoryFailed oder loginFailure, können Sie nur den Schweregrad definieren. Wenn der Schwellenwert für eine Alarmkategorie (z. B. MemoryUsageHigh) überschritten wird oder ein Ereignis eintritt, das der Alarmkategorie entspricht (z. B. **LoginFailure**), wird eine Meldung im System aufgezeichnet und Sie können die Nachricht als Syslog-Nachricht anzeigen. Sie können außerdem Benachrichtigungen einrichten, um eine E-Mail oder SMS zu erhalten, die Ihren Alarmeinstellungen entsprechen.

Sie können den Schweregrad eines Alarms zuweisen oder ändern. Die Schweregrade, die Sie zuweisen können, sind Kritisch, Groß, Geringfügig, Warnung und Informativ.

Betrachten Sie ein Szenario, in dem Sie überwachen möchten, wenn ein fehlgeschlagener Backupversuch vorliegt. Sie können den backupFailed Alarm aktivieren und ihm einen Schweregrad wie Major zuweisen. Wenn NetScaler ADM versucht, die Systemdateien zu sichern und der Versuch fehlschlägt, wird ein Alarm ausgelöst. Sie können die Nachricht im Citrix ADM anzeigen oder Benachrichtigungen per E-Mail oder SMS erhalten.

Um den Alarm zu konfigurieren, müssen Sie den BackupFailed-Alarm auswählen und den Schweregrad als Schweregrad angeben. Der Alarm ist standardmäßig aktiviert.

So konfigurieren und zeigen Sie einen Systemalarm mithilfe von NetScaler ADM an:

1. Navigieren Sie zu **System > SNMP**. Klicken Sie in der oberen rechten Ecke auf **Alarme**.

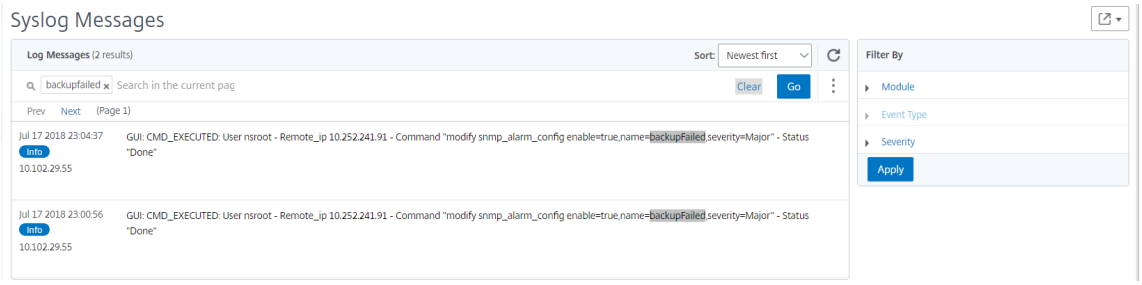
2. Wählen Sie den Alarm aus, den Sie konfigurieren möchten (z. B. BackupFailed), und klicken Sie auf **Bearbeiten**, um die Einstellungen zu ändern.
3. Der Alarm ist standardmäßig aktiviert. Weisen Sie einen Schweregrad zu (Beispiel: Major), und klicken Sie dann auf **OK**.

> **Hinweis**
>
> Für einige Alarme können Sie keinen Schwellenwert festlegen.
> Wenn der Alarm ausgelöst wird, können Sie das generierte Ereignis als Syslog-Meldung anzeigen.

So zeigen Sie das vom BackupFailed-Alarm mithilfe von Citrix ADM generierte Ereignis an:

1. Navigieren Sie zu**System** > **Überwachung**.

2. Wählen Sie auf der**Auditing-Seite**unter**Audit-Meldungen**die Option**Syslog-Meldungen**aus.
3. Geben Sie in das Suchfeld den Namen des Alarms ein.
   In diesem Beispiel können Sie sehen, dass ein Ereignis für einen fehlgeschlagenen Backupversuch generiert wurde.



   Sie können auch Benachrichtigungen festlegen, um Ihnen entweder eine E-Mail oder einen SMS (Short Message Service) zu senden, wenn ein Alarm ausgelöst wird. Informationen zum Konfigurieren von Systembenachrichtigungen finden Sie unter Konfigurieren der Systembenachrichtigungseinstellungen von NetScaler ADM.

NetScaler ADM als API-Proxyserver

February 5, 2024

Citrix Application Delivery Management (Citrix ADM) kann nicht nur NITRO REST-API-Anforderungen für eigene Verwaltungs- und Analysefunktionen empfangen, sondern auch als REST-API-Proxyserver für seine verwalteten Instanzen fungieren. Anstatt API-Anforderungen direkt an die verwalteten Instanzen zu senden, können REST-API-Clients die API-Anforderungen an Citrix ADM senden. Citrix ADM kann zwischen den API-Anforderungen, auf die es antworten muss, und den API-Anforderungen unterscheiden, die unverändert an eine verwaltete Instanz weitergeleitet werden müssen.

Citrix ADM bietet Ihnen als API-Proxyserver folgende Vorteile:

- **Validierung von API-Anfragen**. Citrix ADM validiert alle API-Anforderungen anhand konfigurierter Sicherheits- und rollenbasierter Zugriffssteuerungsrichtlinien (RBAC). Citrix ADM ist ebenfalls mandantenfähig und stellt sicher, dass die API-Aktivität die Mandantengrenzen nicht überschreitet.
- **Zentralisiertes Audit.** Citrix ADM verwaltet ein Überwachungsprotokoll aller API-Aktivitäten im Zusammenhang mit den verwalteten Instanzen.
- **Sitzungsverwaltung**. NetScaler ADM befreit API-Clients von der Aufgabe, Sitzungen mit verwalteten Instanzen zu verwalten.

Funktionsweise von Citrix ADM als API-Proxyserver

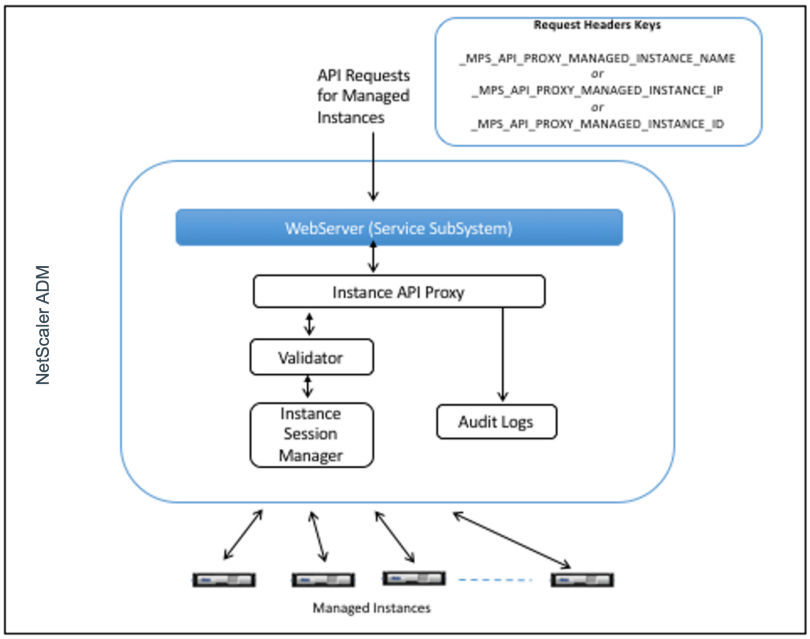
Wenn NetScaler ADM eine Anforderung an eine verwaltete Instanz weiterleiten soll, konfigurieren Sie den API-Client so, dass er einen der folgenden HTTP-Header in die API-Anforderung einschließt:

Header-Werte	Beschreibung
_MPS_API_PROXY_MANAGED_INSTANCE_NAME	Name der verwalteten Instanz.
_MPS_API_PROXY_MANAGED_INSTANCE_IP	IP-Adresse der verwalteten Instanz.
_MPS_API_PROXY_MANAGED_INSTANCE_ID	ID der verwalteten Instanz.
_MPS_API_PROXY_TIMEOUT	Timeout-Wert für eine NITRO-API-Anfrage. Legen Sie den Timeout-Wert in Sekunden fest. Wenn Sie ein Proxy-Timeout festlegen, wartet ADM auf die angegebene Dauer, bevor die Anforderung abgegeben wird.
_MPS_API_PROXY_MANAGED_INSTANCE_USERNAME	Benutzername für den Zugriff auf die verwaltete ADC-Instanz.
_MPS_API_PROXY_MANAGED_INSTANCE_PASSWORD	Kennwort für den Zugriff auf die verwaltete ADC-Instanz.
_MPS_API_PROXY_MANAGED_INSTANCE_SESSID	Sitzungs-ID für den Zugriff auf die verwaltete Instanz.

> **Hinweis**
>
> Wenn Sie unter **System > Administration > Systemkonfigurationen > Grundeinstellungen** die Option **Anmeldeinformationen für Instanzanmeldung auffordern** auswählen, müssen Sie den Benutzernamen und das Kennwort einer verwalteten Instanz konfigurieren. Alternativ können Sie auch die Instanzsitzungs-ID angeben.

Das Vorhandensein eines dieser HTTP-Header hilft NetScaler ADM, eine API-Anforderung als eine Anforderung zu identifizieren, die an eine verwaltete Instanz weitergeleitet werden muss. Der Wert der Kopfzeile hilft Citrix ADM dabei, die verwaltete Instanz zu identifizieren, an die die Anforderung weitergeleitet werden muss.

Dieser Fluss ist in der folgenden Abbildung dargestellt:



Wie in der obigen Abbildung gezeigt, verarbeitet NetScaler ADM die Anforderung wie folgt, wenn einer dieser HTTP-Header in einer Anforderung angezeigt wird:

1. Ohne Änderung der Anforderung leitet Citrix ADM die Anforderung an die Instanz-API-Proxy-Engine weiter.
2. Die Instanz-API-Proxy-Engine leitet die API-Anfrage an einen Validator weiter und protokolliert die Details der API-Anfrage im Audit-Protokoll.
3. Der Validator stellt sicher, dass die Anfrage nicht gegen konfigurierte Sicherheitsrichtlinien, RBAC-Richtlinien, Mandantengrenzen usw. verstößt. Es führt zusätzliche Prüfungen durch, z. B. eine Prüfung, um festzustellen, ob die verwaltete Instanz verfügbar ist.

Wenn die API-Anfrage gültig ist und an die verwaltete Instanz weitergeleitet werden kann, identifiziert NetScaler ADM eine Sitzung, die vom Instanz Session Manager verwaltet wird, und sendet dann die Anfrage an die verwaltete Instanz.

> **Hinweis:**
>
> Stellen Sie sicher, dass die Option **Anmeldeinformationen für Instanzanmeldung anfordern** deaktiviert ist. Vorgehensweise:
>
> 1. Navigieren Sie zu **System > Administration**.
> 2. Wählen Sie in **Systemkonfigurationen** die Optionen **System, Zeitzone, Zulässige URLs und Meldung des Tages** aus.

Verwenden von NetScaler ADM als API-Proxyserver

Die folgenden Beispiele zeigen REST-API-Anforderungen, die ein API-Client an einen Citrix ADM -Server mit der IP-Adresse 192.0.2.5 sendet. Citrix ADM ist erforderlich, um die Anforderungen unverändert an eine verwaltete Instanz mit der IP-Adresse 192.0.2.10 weiterzuleiten. Alle Beispiele verwenden den _MPS_API_PROXY_MANAGED_INSTANCE_IP-Header.

Bevor die API-Anforderungen von Citrix ADM gesendet werden, muss der API-Client Folgendes ausführen:

- Anmelden bei Citrix ADM
- Besorgen Sie sich eine Sitzungs-ID
- Fügen Sie die Sitzungs-ID in nachfolgende API-Anfragen ein.

Die Anmelde-API-Anforderung hat das folgende Format:

```
    POST /nitro/v1/config/login
    Content-Type: application/json

    {

        "login": {

            "username":"nsroot",
            "password":"nsroot"
          }

     }

<!--NeedCopy-->
```

Citrix ADM antwortet auf die Anmeldeanforderung mit einer Antwort, die die Sitzungs-ID enthält. Der folgende Beispielantworttext zeigt eine Sitzungs-ID:

```
{


  "errorcode": 0,

  "message": "Done",

  "operation": "add",

  "resourceType": "login",

  "username": "***********",

  "tenant_name": "Owner",

  "resourceName": "nsroot",

```



```
18   "login": [
19
20     {
21
22
23       "tenant_name": "Owner",
24
25       "permission": "superuser",
26
27       "session_timeout": "36000",
28
29       "challenge_token": "",
30
31       "username": "",
32
33       "login_type": "",
34
35       "challenge": "",
36
37       "client_ip": "",
38
39       "client_port": "-1",
40
41       "cert_verified": "false",
42
43       "sessionid": "##
      D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
44
45       "token": "b2f3f935e93db6a"
46      }
47
48
49    ]
50
51   }
52
53 <!--NeedCopy-->
```

Beispiel 1: Rufen Sie die Statistiken für virtuelle Load-Balancing-Server ab

Der Client muss NetScaler ADM eine API-Anforderung mit folgendem Formular senden:

```
1      GET /nitro/v1/stat/lbvserver
2      Content-type: application/json
3      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4      SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5  <!--NeedCopy-->
```

Wobei der Wert des Cookie-Headers die Sitzungs-ID ist, die vom Login-API-Aufruf zurückgegeben wird. Und der Wert von _MPS_API_PROXY_MANAGED_INSTANCE_IP ist die IP-Adresse des ADC.

Beispiel 2: Erstellen eines virtuellen Lastausgleichsservers

Der Client muss NetScaler ADM eine API-Anforderung mit folgendem Formular senden:

```
    POST /nitro/v1/config/lbvserver/sample_lbvserver
    Content-type: application/json
    Accept-type: application/json
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    SESSID: ##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

    {

         "lbvserver":{

             "name":"sample_lbvserver",
             "servicetype":"HTTP",
             "ipv46":"10.102.1.11",
             "port":"80"
          }

     }

<!--NeedCopy-->
```

Beispiel 3: Ändern Sie einen virtuellen Lastausgleichsserver

Der Client muss NetScaler ADM eine API-Anforderung mit folgendem Formular senden:

```
    PUT /nitro/v1/config/lbvserver
    Content-type: application/json
    Accept-type: application/json
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    SESSID: ##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

    {

       "lbvserver":{

            "name":"sample_lbvserver",
            "appflowlog":"DISABLED"
         }

     }

<!--NeedCopy-->
```


Beispiel 4: Löschen eines virtuellen Load-Balancing-Servers

Der Client muss NetScaler ADM eine API-Anforderung mit folgendem Formular senden:

```
1     DELETE /nitro/v1/config/lbvserver/sample_lbvserver
2     Accept-type: application/json
3     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4     SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6  <!--NeedCopy-->
```

Beispiel 5: Laden Sie die CLI running Config auf dem ADC herunter

Der Client muss NetScaler ADM eine API-Anforderung mit folgendem Formular senden:

```
1     GET /nitro/v1/config/nsrunningconfig
2     Accept-type: application/json
3     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4     SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6  <!--NeedCopy-->
```

Visualisieren von Problemen mithilfe von Infrastructure Analytics

February 5, 2024

Ein wichtiges Ziel für Netzwerkadministratoren ist die Überwachung von NetScaler ADC-Instanzen. ADC-Instanzen bieten interessante Einblicke in die Nutzung und Leistung von Anwendungen und Desktops, auf die über sie zugegriffen wird. Administratoren müssen die ADC-Instanz überwachen und die von jeder ADC-Instanz verarbeiteten Anwendungsflüsse analysieren. Sie können alle wahrscheinlichen Probleme bei Konfiguration, Einrichtung, Konnektivität, Zertifikaten und anderen beheben, die sich auf die Anwendungsnutzung oder -leistung auswirken könnten. Zum Beispiel kann eine plötzliche Änderung des Anwendungsdatenverkehrs auf eine Änderung der SSL-Konfiguration zurückzuführen sein, wie die Deaktivierung eines SSL-Protokolls. Administratoren müssen in der Lage sein, die Korrelation zwischen diesen Datenpunkten schnell zu erkennen, um Folgendes sicherzustellen:

- Die Anwendungsverfügbarkeit ist in einem optimalen Zustand
- Es gibt keine Probleme mit Ressourcenverbrauch, Hardware, Kapazität oder Konfigurationsänderungen

- Es gibt keine ungenutzten Lagerbestände
- Es gibt keine abgelaufenen Zertifikate

Die Infrastructure Analytics-Funktion vereinfacht den Prozess der Datenanalyse, indem sie mehrere Datenquellen korreliert und zu einem messbaren Ergebnis quantifiziert, das den Zustand einer Instanz definiert. Mit dieser Funktion erhalten die Administratoren eine zentrale Anlaufstelle, um zu erfahren, ob ein Problem vorliegt, woher das Problem stammt und welche möglichen Abhilfemaßnahmen sie durchführen können.

Analytik der Infrastruktur

Die Citrix Application Delivery Management (ADM) Infrastructure Analytics-Funktion sammelt alle von den Citrix ADC Instanzen gesammelten Daten und quantifiziert sie in einem **Instanz-Score**, der die Integrität der Instanzen definiert. Die Instanzbewertung wird in einer tabellarischen Ansicht oder als Circlepack-Visualisierung zusammengefasst. Mit der Funktion Infrastructure Analytics können Sie die Faktoren visualisieren, die zu einem Problem in den Instanzen geführt haben oder dazu führen könnten. Diese Visualisierung hilft Ihnen auch dabei, die Aktionen zu bestimmen, die ausgeführt werden müssen, um das Problem und sein erneutes Auftreten zu verhindern.

Instanz-Score

Die Instanzbewertung gibt den Zustand einer ADC-Instanz an. Eine Punktzahl von 100 bedeutet eine absolut gesunde Instanz ohne Probleme. Die Instanz-Bewertung erfasst verschiedene Ebenen potenzieller Probleme auf der Instanz. Es handelt sich um eine quantifizierbare Messung des Instanzzustands, und mehrere "Gesundheitsindikatoren"tragen zum Score bei.

Integritätsindikatoren sind die Bausteine des Instanz-Scores, bei dem der Score regelmäßig für einen vordefinierten "Überwachungszeitraum"berechnet wird, basierend auf allen erkannten Indikatoren in diesem Zeitfenster. Derzeit berechnet Infrastructure Analytics den Instanz-Score einmal pro Stunde auf der Grundlage der von den Instanzen gesammelten Daten.
Ein Indikator kann als jede Aktivität (ein Ereignis oder ein Problem) definiert werden, die zu einer der folgenden Kategorien auf den Instanzen gehört.

- Indikatoren für Systemressourcen
- Indikatoren für kritische Ereignisse
- SSL-Konfigurationsindikatoren
- Konfigurationsabweichungsindikatoren

Gesundheitsindikatoren

- Indikatoren für Systemressourcen

  Im Folgenden finden Sie die kritischen Systemressourcenprobleme, die auf NetScaler ADC-Instanzen auftreten und von NetScaler ADM überwacht werden können.

  - **Hohe CPU-Auslastung**. Die CPU-Auslastung hat den höheren Schwellenwert in der NetScaler ADC-Instanz überschritten.
  - **Hohe Speicherauslastung**. Die Speicherauslastung hat den höheren Schwellenwert in der NetScaler ADC-Instanz überschritten.
  - **Hohe Datenträgernutzung**. Die Datenträgerauslastung hat den höheren Schwellenwert in der NetScaler ADC-Instanz überschritten.
  - **Datenträgerfehler**. Es gibt Fehler auf Festplatte 0 oder Festplatte 1 auf dem Hypervisor, auf dem die ADC-Instanz installiert ist.
  - **Stromausfall**. Die Stromversorgung ist ausgefallen oder wurde von der ADC-Instanz getrennt.
  - **Ausfall der SSL-Karte**. Die auf der Instanz installierte SSL-Karte ist ausgefallen.
  - **Flash-Fehler**. Bei der NetScaler ADC-Instanz sind Compact Flash Fehler aufgetreten.
  - **NIC verwirft**. Die von der NIC-Karte verworfenen Pakete haben den höheren Schwellenwert in der NetScaler ADC-Instanz überschritten.

Weitere Informationen zu diesen Systemressourcenfehlern finden Sie unter Das Instanz-Dashboard.

- Indikatoren für kritische Ereignisse

  Die folgenden kritischen Ereignisse werden anhand der Ereignisverwaltungsfunktion von ADM identifiziert, die für den Schweregrad „Kritisch“konfiguriert sind.

  - **HA-Synchronisierung fehlgeschlagen**. Die Konfigurationssynchronisierung zwischen den ADC-Instanzen mit hoher Verfügbarkeit ist auf dem sekundären Server fehlgeschlagen.
  - **HA kein Herzschlag**. Der Primärserver in zwei ADC-Instances mit hoher Verfügbarkeit empfängt keine Herzschläge vom sekundären Server.
  - **HA bad secondary state**. Der sekundäre Server in zwei ADC-Instanzen mit hoher Verfügbarkeit befindet sich im Status Down, Unknown oder Stay secondary.
  - **Nichtübereinstimmung der HA-Version**. Die Version der ADC-Software-Images, die auf zwei ADC-Instanzen mit hoher Verfügbarkeit installiert sind, stimmt nicht überein.

- **Fehler bei der Clustersynchron** Die Konfigurationssynchronisierung zwischen den ADC-Instanzen im Clustermodus ist fehlgeschlagen.
- **Nichtübereinstimmung der Clusterversion**. Die Version der ADC-Software-Images, die auf den ADC-Instanzen im Clustermodus installiert sind, stimmt nicht überein.
- **Fehler bei der Clusterverbreitung**. Die Weitergabe von Konfigurationen an alle Instanzen in einem Cluster ist fehlgeschlagen.

> **Hinweis**
>
> Sie können Ihre Liste der kritischen SNMP-Ereignisse haben, indem Sie den Schweregrad der Ereignisse ändern. Weitere Informationen zum Ändern des Schweregrads finden Sie unter Ändern des gemeldeten Schweregrads von Ereignissen, die in NetScaler ADC-Instanzen auftreten.

Weitere Informationen zu Ereignissen in Citrix ADM finden Sie unter Ereignisse .

- SSL-Konfigurationsindikatoren
  - **Nicht empfohlene Schlüsselstärke**. Die Schlüsselstärke der SSL-Zertifikate entspricht nicht den Citrix-Standards
  - **Nicht empfohlener Aussteller**. Der Herausgeber des SSL-Zertifikats wird von Citrix nicht empfohlen.
  - **SSL-Zertifikate sind abgelaufen**. Das in der ADC-Instanz installierte SSL-Zertifikat ist abgelaufen.
  - **Ablauf der SSL-Zertifikate ist fällig**. Das in der ADC-Instanz installierte SSL-Zertifikat läuft in der nächsten Woche ab.
  - **Nicht empfohlene Algorithmen**. Die Signaturalgorithmen von in der ADC-Instanz installierten SSL-Zertifikaten entsprechen nicht den Citrix Standards.

Weitere Informationen zu SSL-Zertifikaten finden Sie unter SSL-Dashboard.

- Konfigurationsabweichungsindikatoren
  - **Konfigurationsdrift-Vorlage**. Es gibt eine Abweichung (ungespeicherte Änderungen) in der Konfiguration von den Überwachungsvorlagen, die Sie mit bestimmten Konfigurationen erstellt haben, die Sie für bestimmte Instanzen überwachen möchten.
  - **Standardeinstellung für Konfigurationsabweichung**. Es gibt eine Drift (nicht gespeicherte Änderungen) in der Konfiguration aus den Standardkonfigurationsdateien.

Weitere Informationen zu Konfigurationsabweichungen und zur Ausführung von Auditberichten zur Überprüfung von Konfigurationsabweichungen finden Sie unter Auditberichte anzeigen .

ADC-Kapazitätsprobleme anzeigen

Wenn eine ADC-Instanz den größten Teil ihrer verfügbaren Kapazität verbraucht hat, kann es während der Verarbeitung des Client-Datenverkehrs zu einem Paket-Drop kommen. Dieses Problem führt zu einer geringen Leistung in einer ADC-Instanz. Wenn Sie solche ADC-Kapazitätsprobleme verstehen, können Sie proaktiv zusätzliche Lizenzen zuweisen, um die ADC-Leistung aufrechtzuerhalten.

So zeigen Sie ADC-Kapazitätsprobleme an:

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

Der ADM ruft diese Ereignisse alle fünf Minuten von der ADC-Instanz ab und zeigt die verworfenen Pakete oder Rate-Limit-Zähler-Inkremente an, falls vorhanden. Die Probleme sind nach den folgenden Kapazitätsparametern kategorisiert:

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

Das ADM berechnet die Instanzbewertung anhand des definierten Kapazitätsschwellenwerts.

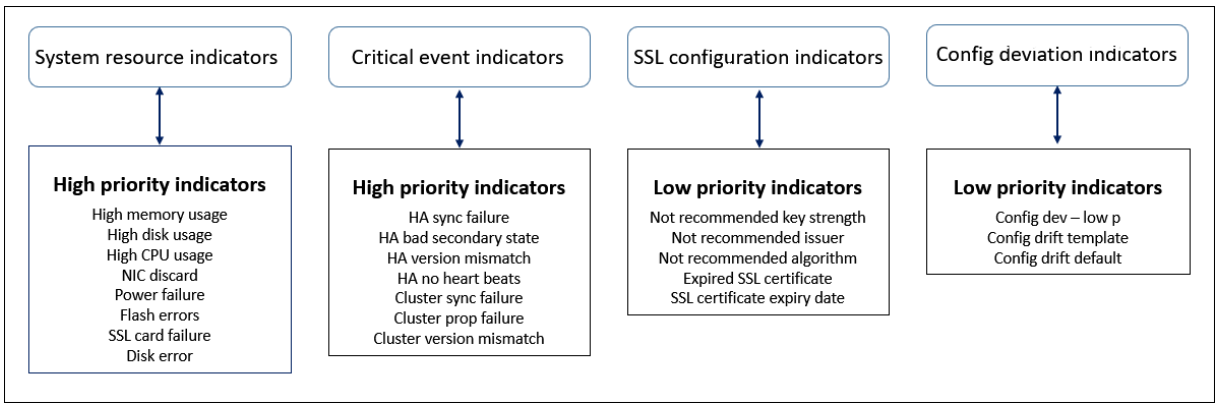
- Niedriger Schwellenwert —1 Zählerinkrement für Paketverlust oder Ratenbegrenzung
- Hoher Schwellenwert —10.000 Paketverlust oder Erhöhung des Ratenlimit-Zählers

Wenn eine ADC-Instance den Kapazitätsschwellenwert überschreitet, wirkt sich dies daher auf die Instance-Bewertung aus.

Wenn Pakete fallen oder der Zähler für die Ratenbegrenzung inkrementiert wird, wird ein Ereignis in der Kategorie `ADCCapacityBreach` generiert. Um diese Ereignisse einzusehen, navigieren Sie zu **Konten > Systemereignisse**.

Wert von Gesundheitsindikatoren

Die Indikatoren werden anhand ihrer Werte wie folgt in Indikatoren mit hoher Priorität und Indikatoren mit niedriger Priorität eingeteilt:



Den Gesundheitsindikatoren innerhalb derselben Indikatorengruppe werden unterschiedliche Gewichtungen zugewiesen. Ein Indikator kann mehr zu einem niedrigeren Instanz-Score beitragen als ein anderer Indikator. Die hohe Speicherauslastung verringert zum Beispiel den Instanzscore mehr als eine hohe Datenträgernutzung, eine hohe CPU-Auslastung und einem NIC-Discard. Wenn auf einer Instanz eine größere Anzahl von Indikatoren erkannt wird, ist der Instanzwert umso geringer.

Der Wert eines Indikators wird auf der Grundlage der folgenden Regeln berechnet. Der Indikator soll auf eine der folgenden drei Arten erkannt werden:

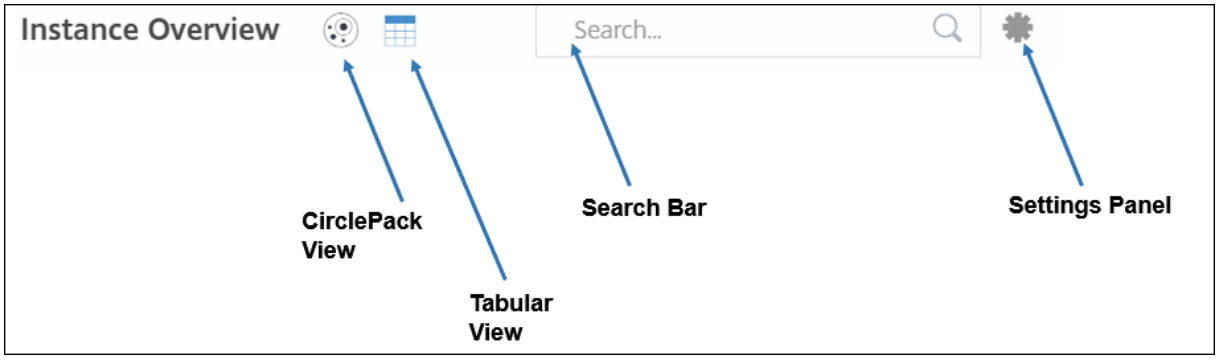
1. **Basierend auf einer Aktivität**. Beispielsweise wird ein Systemressourcenindikator ausgelöst, wenn in der Instanz ein Stromausfall auftritt, und dieser Indikator verringert den Wert der Instanzbewertung. Wenn der Indikator gelöscht ist, wird die Strafe gelöscht und der Instanzwert erhöht sich.
2. **Basierend auf der Verletzung des Schwellenwerts**. Beispielsweise wird eine Systemressourcenanzeige ausgelöst, wenn die NIC-Karte Pakete verwirft und der Schwellenwert überschritten wird.
3. **Basierend auf der Verletzung des niedrigen und hohen Schwellenwerts**. Hier kann ein Indikator auf zwei Arten ausgelöst werden:
    - Wenn der Wert des Indikators zwischen niedrigen und hohen Schwellenwerten liegt, wird in diesem Fall eine Teilstrafe auf die Instanzbewertung erhoben.
    - Wenn der Wert den hohen Schwellenwert überschreitet, wird in diesem Fall eine volle Strafe auf die Instanzbewertung erhoben.
    - Wenn der Wert unter einen niedrigen Schwellenwert fällt, wird keine Strafe auf den Instanz-Score erhoben.

Beispielsweise ist die CPU-Auslastung ein Systemressourcenindikator, der ausgelöst wird, wenn der Nutzungswert den niedrigen Schwellenwert überschreitet und wenn der Wert den hohen Schwellenwert überschreitet.

Dashboard für Infrastrukturanalysen

Navigieren Sie zu **Netzwerke** > **Infrastrukturanalyse**.

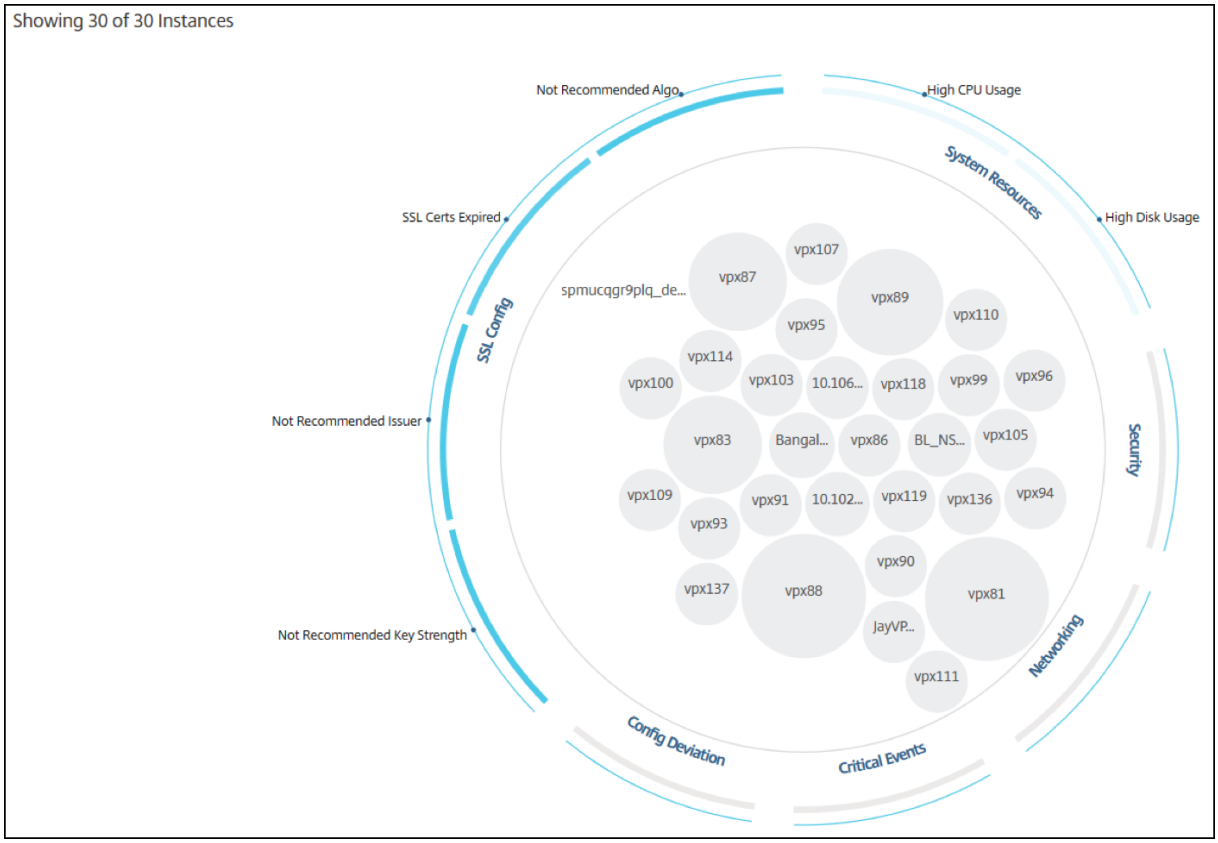
Die Infrastructure Analytics kann im **Circle Pack-** oder **Tabellenformat** angezeigt werden. Sie können zwischen den beiden Formaten hin- und herschalten.



- In der Tabellenansicht können Sie nach einer Instanz suchen, indem Sie den Hostnamen oder die IP-Adresse in die Suchleiste eingeben.
- Standardmäßig wird auf der Seite Infrastructure Analytics rechts auf der Seite das Zusammenfassungsfenster angezeigt.
- Klicken Sie auf das Symbol **Einstellungen**, um die **Einstellungsleiste** anzuzeigen.
- In beiden Ansichtsformaten zeigt das Zusammenfassungsfenster Details aller Instanzen in Ihrem Netzwerk an.

Kreispaketansicht

Kreispackdiagramme zeigen Instanzgruppen als eng organisierte Kreise. Sie zeigen oft Hierarchien, in denen kleinere Instanzgruppen entweder ähnlich gefärbt sind wie andere in derselben Kategorie oder in größeren Gruppen verschachtelt sind. Circle Packs stellen hierarchische Datensätze dar und zeigen verschiedene Ebenen in der Hierarchie und wie sie miteinander interagieren.



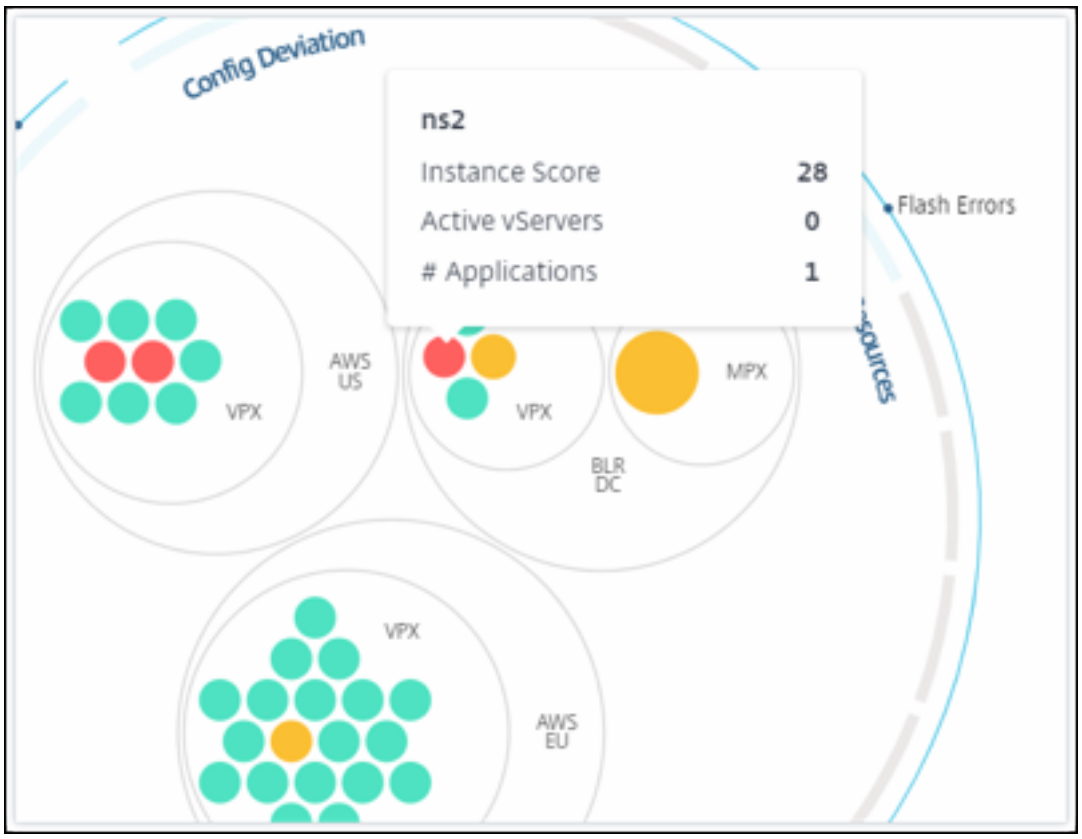
Instanzkreise

Farbe. Jede Instanz wird im Circle Pack als farbiger Kreis dargestellt. Die Farbe des Kreises zeigt den Zustand dieser Instanz an.

- **Grün** —Instanz-Score liegt zwischen 100 und 80. Die Instanz ist gesund.
- **Gelb** —Die Bewertung der Instanz liegt zwischen 80 und 50; einige Probleme wurden festgestellt und müssen überprüft werden.
- **Rot** —Instanz-Score liegt unter 50. Die Instanz befindet sich in einer kritischen Phase, da bei dieser Instanz mehrere Probleme festgestellt wurden.

Größe. Die Größe dieser farbigen Kreise gibt die Anzahl der virtuellen Server an, die auf dieser Instanz konfiguriert sind. Ein größerer Kreis zeigt an, dass es eine größere Anzahl virtueller Server gibt.

Sie können den Mauszeiger auf jeden Instanzkreis (farbige Kreise) bewegen, um eine Zusammenfassung anzuzeigen. Der Hover-Tooltip zeigt den Hostnamen der Instanz, die Anzahl der aktiven virtuellen Server und die Anzahl der auf dieser Instanz konfigurierten Anwendungen an.

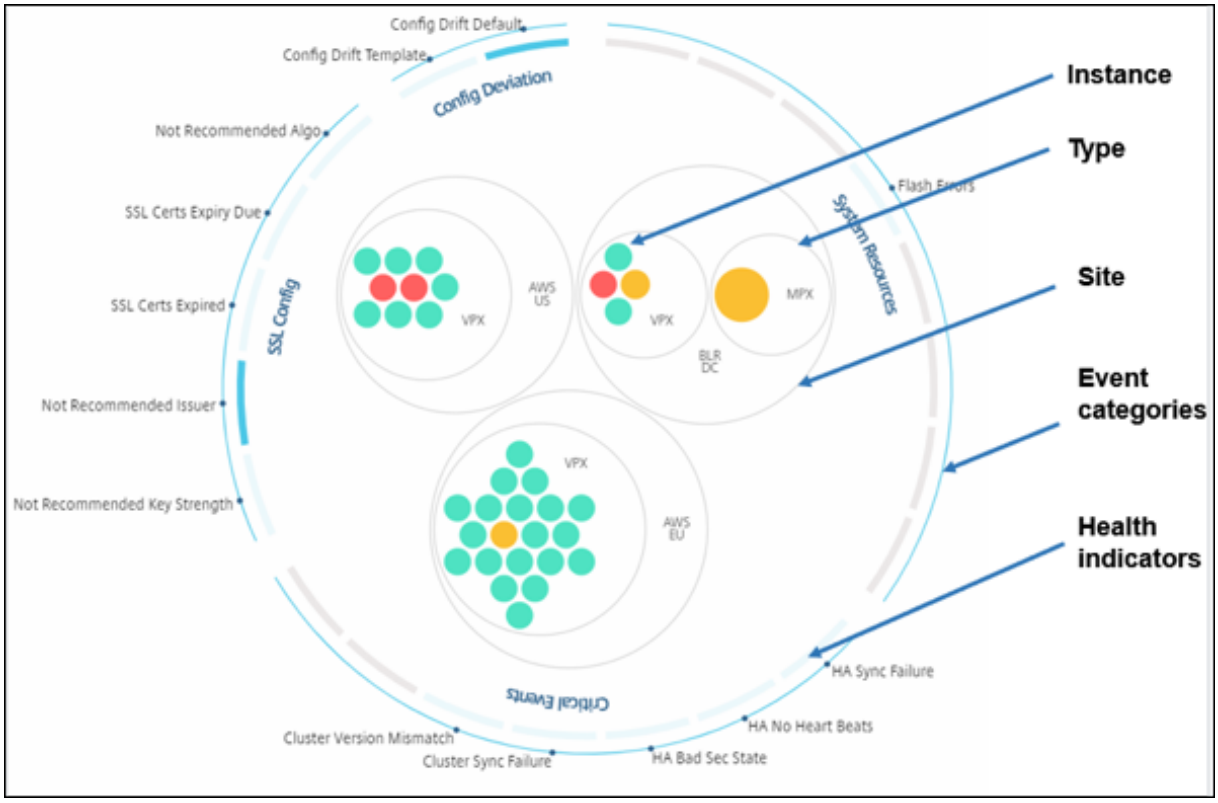


Gruppierte Instanzkreise

Das Circle Pack besteht zu Beginn aus Instanzkreise, die anhand der folgenden Kriterien gruppiert, verschachtelt oder innerhalb eines anderen Kreises gepackt werden:

- der Standort, an dem sie eingesetzt werden
- die Art der bereitgestellten Instanzen - VPX, MPX, SDX und CPX
- das virtuelle oder physische Modell der ADC-Instanz
- Auf den Instanzen installierte ADC-Image-Version

Die folgende Abbildung zeigt ein Circle Pack, in dem die Instanzen zuerst nach der Site oder dem Datencenter gruppiert werden, an dem sie bereitgestellt werden, und dann anhand ihres Typs, VPX und MPX weiter gruppiert werden.

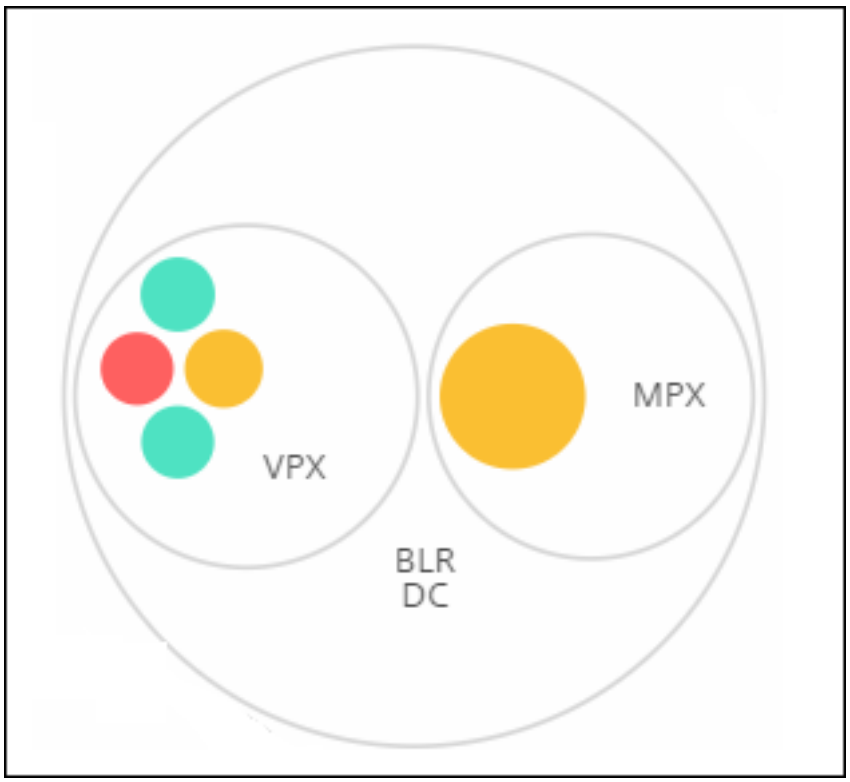


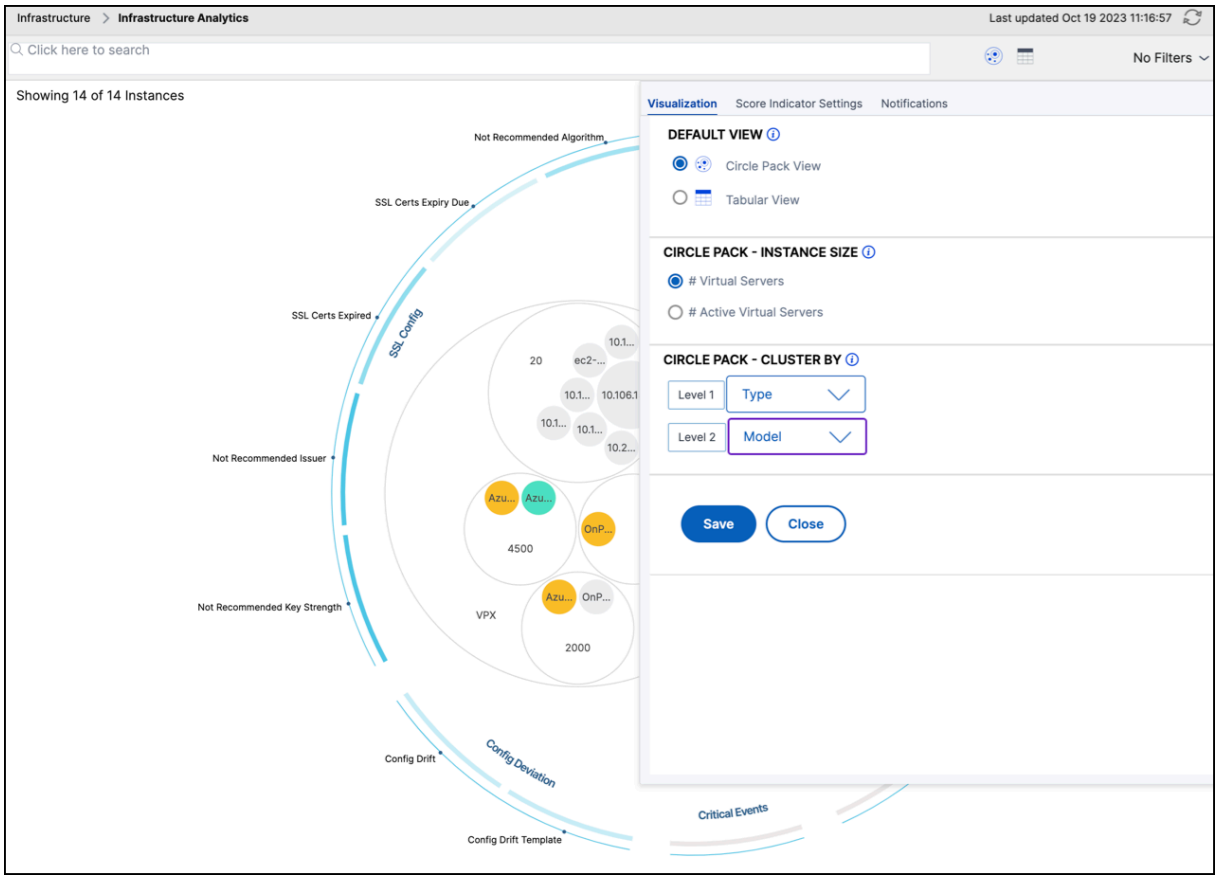
Alle diese verschachtelten Kreise werden von zwei äußersten Kreisen begrenzt. Die äußeren beiden Kreise stellen die vier Kategorien von Ereignissen dar, die vom NetScaler ADM überwacht werden (Systemressourcen, kritische Ereignisse, SSL-Konfiguration und Konfigurationsabweichung) sowie die beitragenden Integritätsindikatoren.

Gruppierte Instanzkreise

NetScaler ADM überwacht viele Instanzen. Um die Überwachung und Wartung dieser Instanzen zu vereinfachen, können Sie sie mit Infrastructure Analytics auf zwei Ebenen clustern. Das heißt, die Instanzgruppierungen können innerhalb einer anderen Gruppierung verschachtelt werden.

Zum Beispiel verfügt das BLR-Rechenzentrum über zwei Arten von ADC-Instanzen - VPX und MPX, die darin bereitgestellt werden. Sie können die ADC-Instanzen zuerst nach ihrem Typ gruppieren und dann alle Instanzen nach dem Standort gruppieren, an dem sie gruppiert sind. Sie können jetzt leicht erkennen, wie viele Instanztypen in den von Ihnen verwalteten Sites bereitgestellt werden.

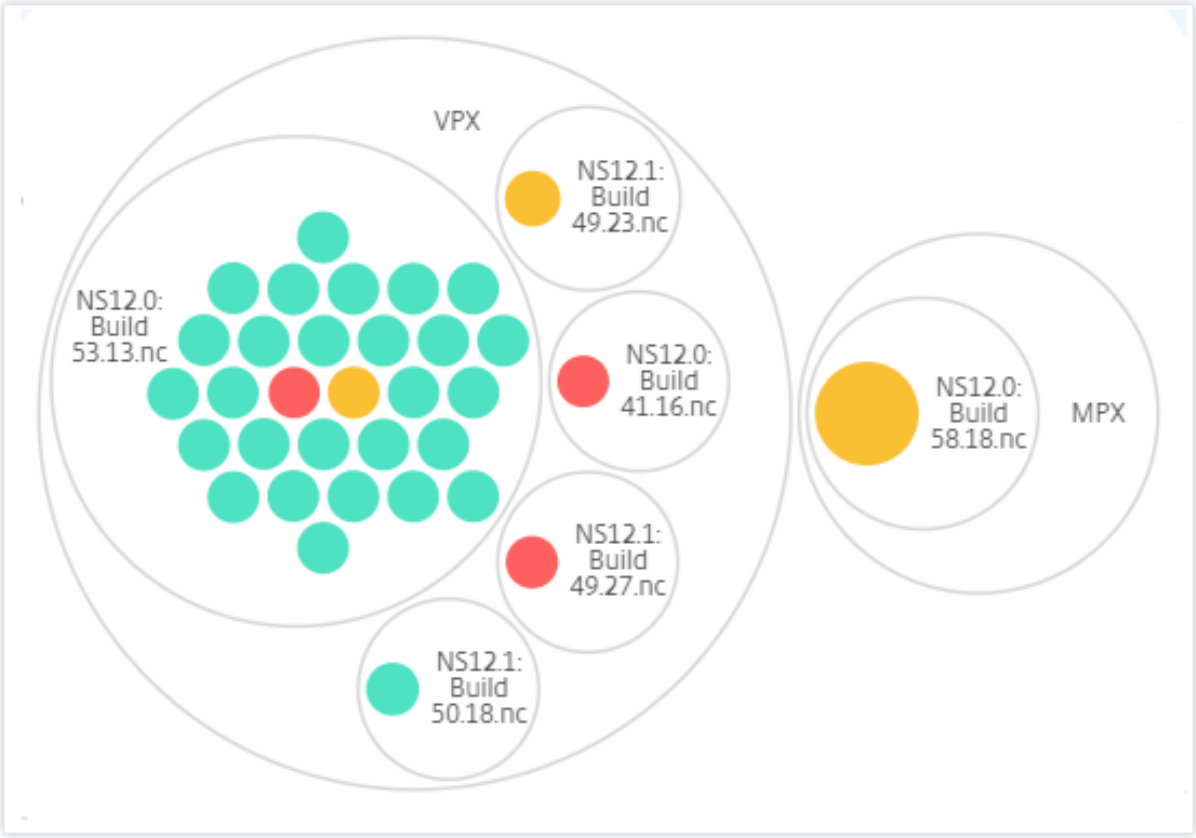




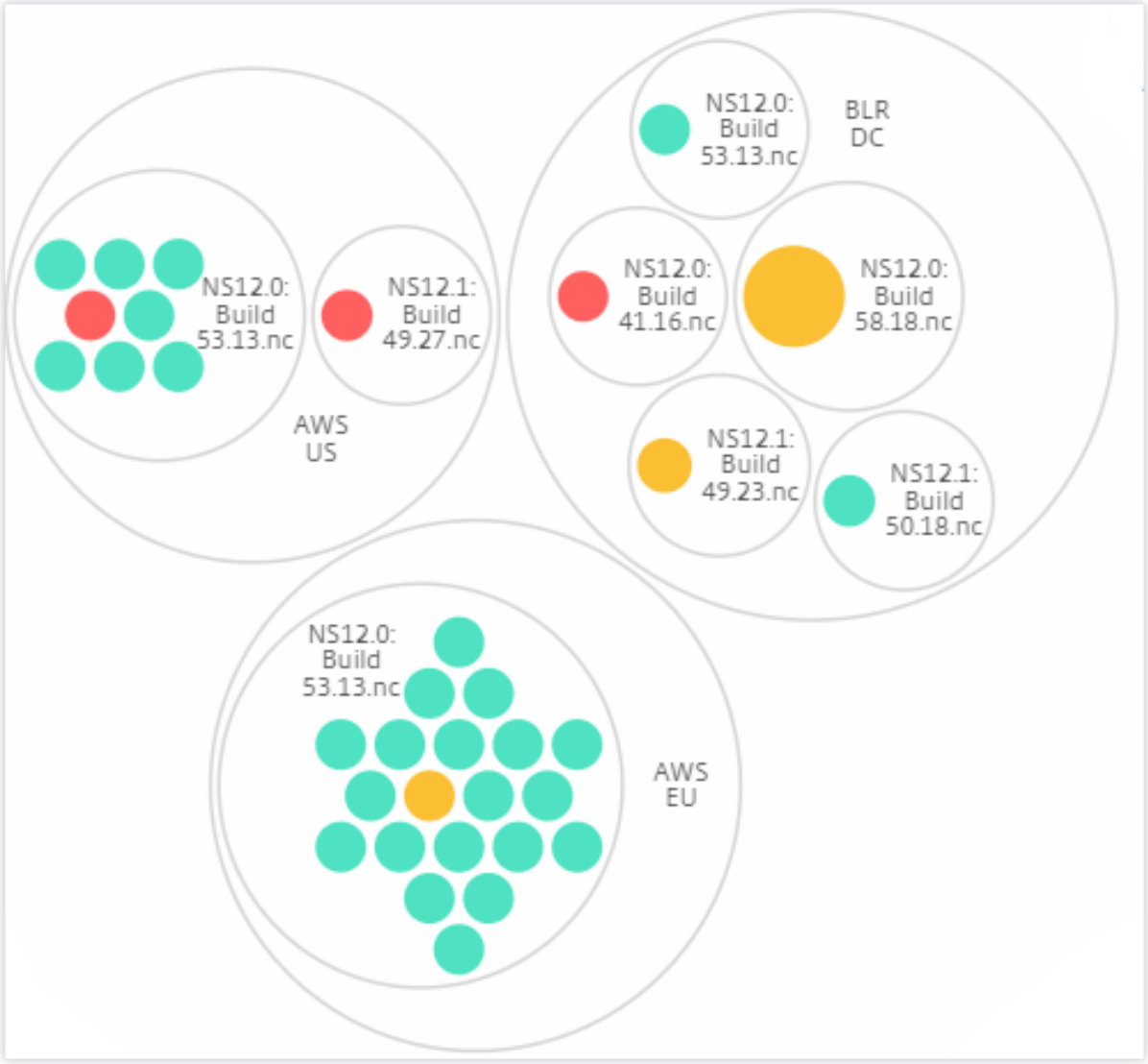
Ein paar weitere Beispiele für zweistufiges Clustering sind wie folgt:

Standort und Modell:

Typ und Ausführung:

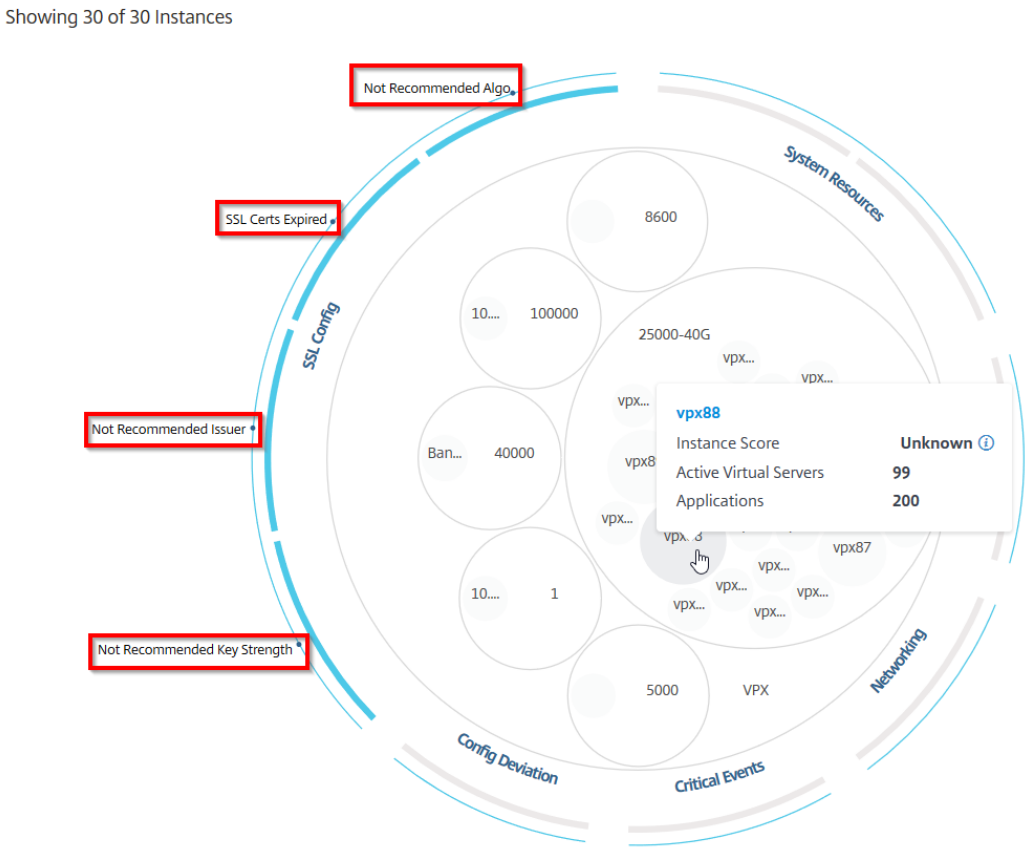


Website und Version:



Wie benutzt man Circle Pack

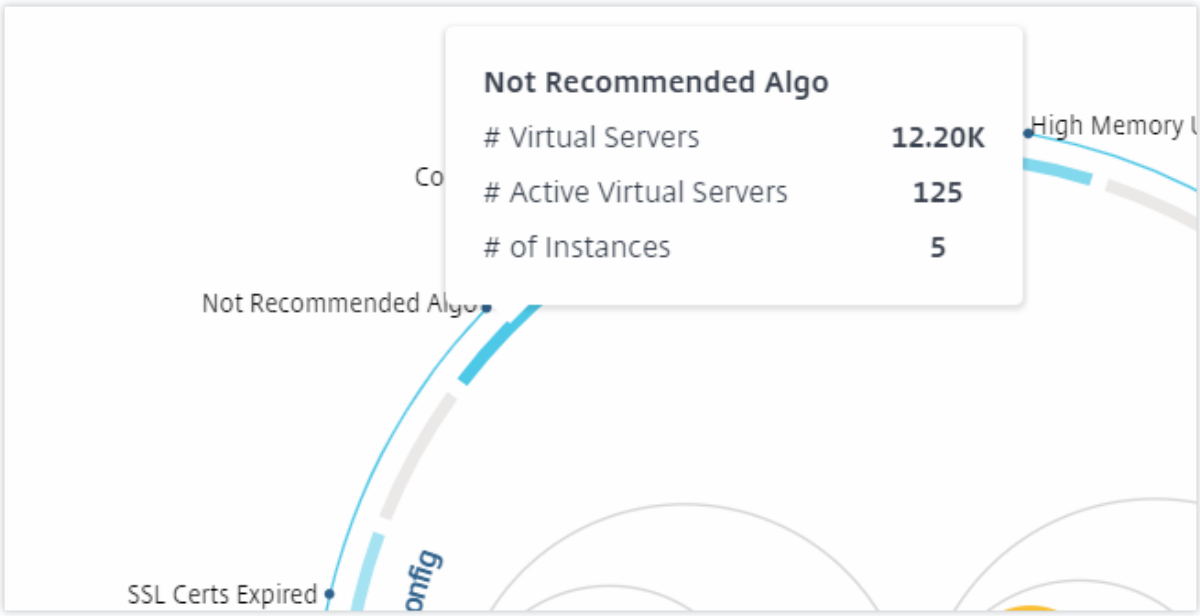
Klicken Sie auf jeden der farbigen Kreise, um diese Instanz hervorzuheben.



Abhängig von den Ereignissen, die in dieser Instanz aufgetreten sind, werden nur diese Gesundheitsindikatoren auf den äußeren Kreisen hervorgehoben. Die folgenden beiden Bilder des Circle Pack zeigen beispielsweise unterschiedliche Risikoindikatoren, obwohl sich beide Instanzen in einem kritischen Zustand befinden.

Sie können auch auf die Integritätsindikatoren klicken, um weitere Details zur Anzahl der Instanzen zu erhalten, die diesen Risikoindikator gemeldet haben. Klicken Sie beispielsweise auf, Not

recommended Algoum den zusammenfassenden Bericht dieses Risikoindikators anzuzeigen.

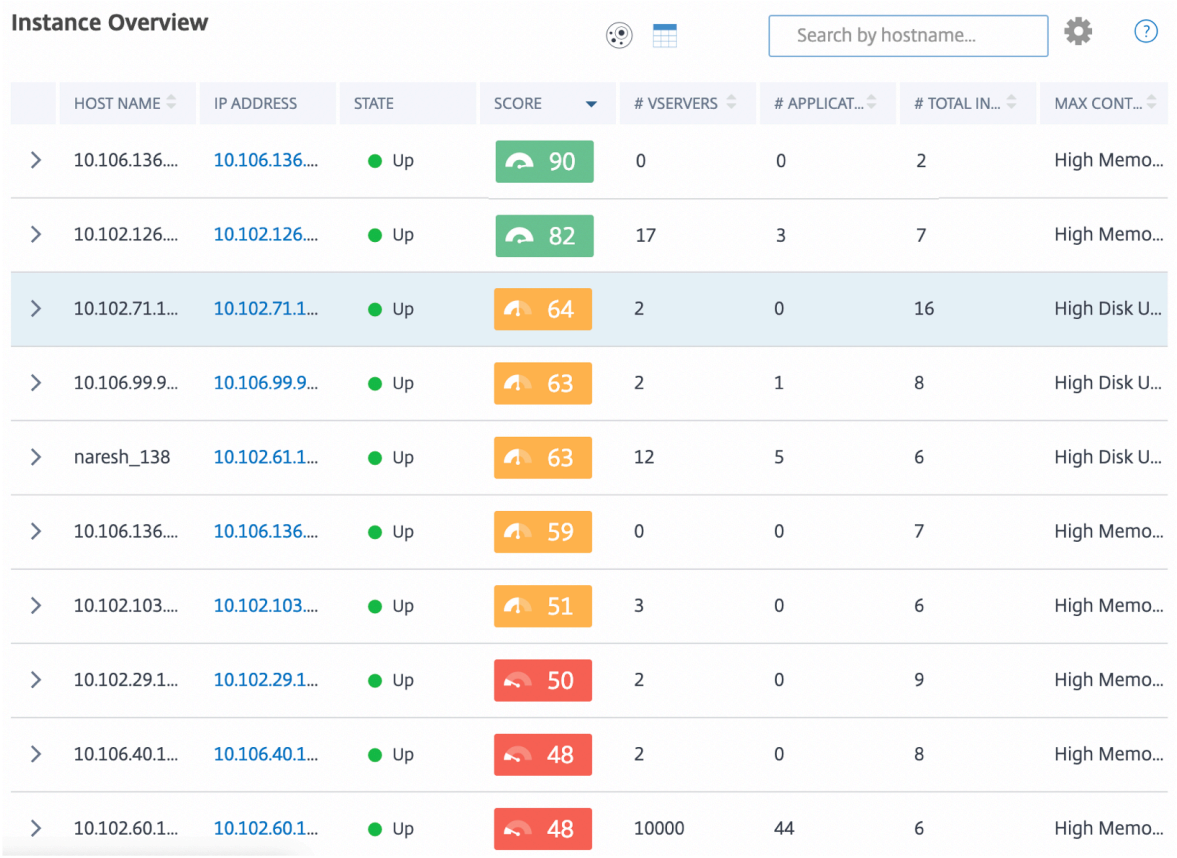


Tabellarische Ansicht

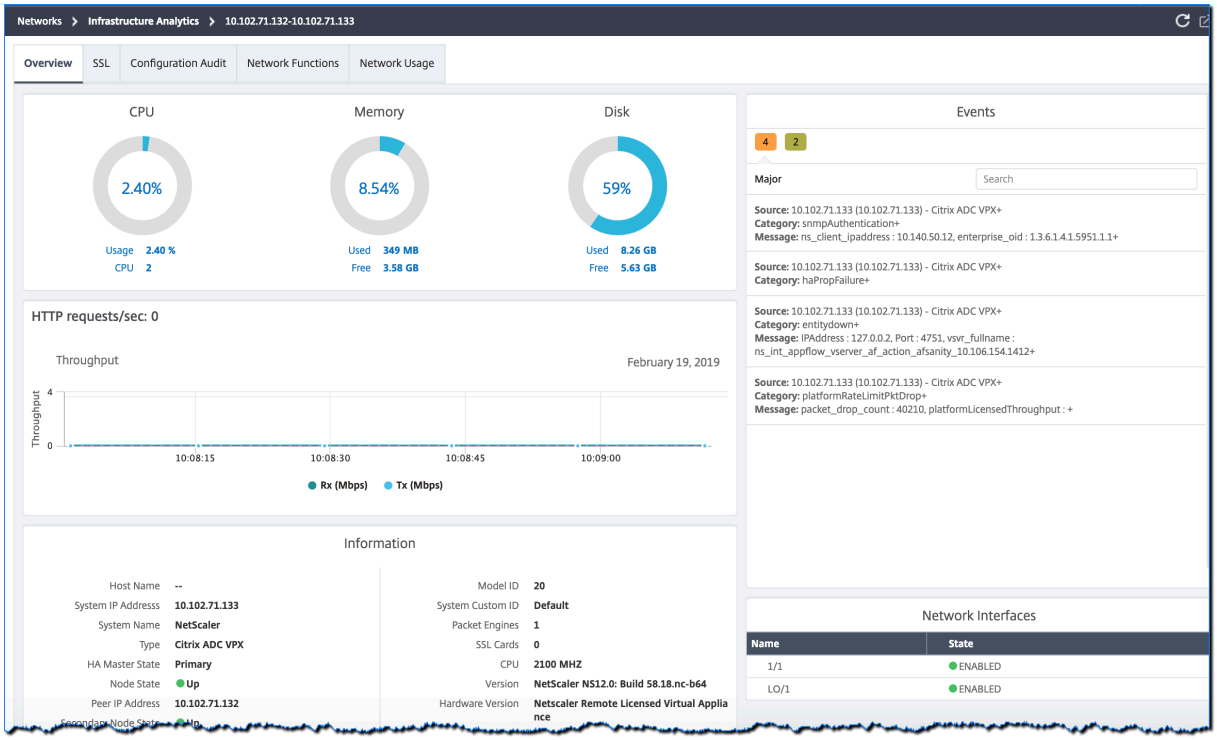
In der tabellarischen Ansicht werden die Instanzen und die Details dieser Instanzen in einem tabellarischen Format angezeigt. Die Details, die angezeigt werden, lauten wie folgt:

- Hostname der Instanz
- Die IP-Adresse der Instanz
- Status der Instanz
- Instanz-Score
- Anzahl der auf dieser Instanz konfigurierten virtuellen Server
- Anzahl der auf dieser Instanz konfigurierten Anwendungen
- Gesamtzahl der Risikoindikatoren
- Das Ereignis, das mehr zu einem niedrigeren Instanz-Score beiträgt

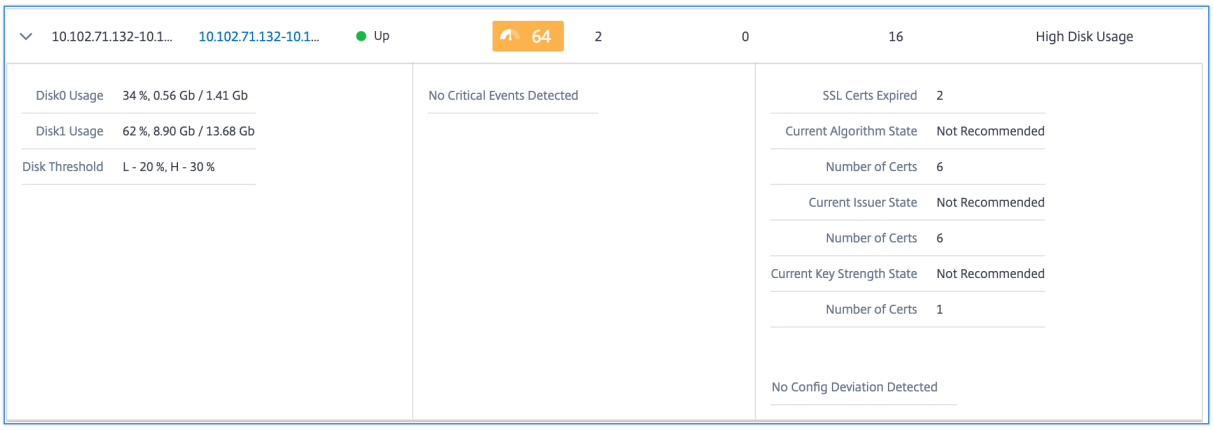
Die Instanzen, die sich im kritischen Zustand befinden, stehen ganz oben in der Tabelle, gefolgt von den Instanzen, die überprüft werden müssen, und dann den gesünderen Instanzen.



Klicken Sie in der tabellarischen Ansicht auf die IP-Adresse der Instanz, um weitere Details dieser Instanz als Dashboard-Anzeige anzuzeigen. Das Instanz-Dashboard bietet eine Übersicht über die Instanz, in der Sie die CPU, den Arbeitsspeicher und die Datenträgernutzung der Instanz anzeigen können. Sie können auch Details zur SSL-Zertifikatsverwaltung, zur Konfigurationsprüfung, zu Netzwerkfunktionen sowie einen Netzwerkbericht einsehen, der die detaillierte Netzwerknutzung der Instanz zeigt. Scrollen Sie weiter nach unten, um die Liste der Funktionen und Modi zu sehen, die in dieser Instanz aktiviert sind.



Sie können auch auf den Pfeil am Anfang jeder Zeile klicken, um die Zeile für weitere Details zu erweitern.



In der erweiterten Tabellenzeile werden die Fehler angezeigt, die in der Instanz für alle Kategorien aufgetreten sind. Im obigen Beispiel können Sie sehen, dass Fehler in den Systemressourcen, der SSL-Konfiguration und Abweichungen in den Konfigurationsdateien aufgetreten sind. Aus der Instanz wurden jedoch keine kritischen Ereignisse gemeldet.

So verwenden Sie das Übersichts-Panel

Das **Zusammenfassungspanel** hilft Ihnen dabei, sich effizient und schnell auf die Fälle zu konzentrieren, die überprüft werden müssen oder in einem kritischen Zustand sind. Das Panel ist in drei

Registerkarten unterteilt: Übersicht, Instanzinformation und Verkehrsprofil. Durch die Änderungen, die Sie in diesem Fenster vornehmen, wird die Anzeige sowohl im Circle Pack- als auch im Tabellenansichtsformat geändert. In den folgenden Abschnitten werden diese Registerkarten ausführlicher beschrieben. Die Beispiele in den folgenden Abschnitten helfen Ihnen dabei, die verschiedenen Auswahlkriterien effizient zu verwenden, um die von den Instanzen gemeldeten Probleme zu analysieren.

Überblick:

Auf der Registerkarte **Übersicht** können Sie die Instanzen basierend auf Hardwarefehlern, Nutzung, abgelaufenen Zertifikaten und ähnlichen Indikatoren überwachen, die in den Instanzen auftreten können. Die Indikatoren, die Sie hier überwachen können, sind wie folgt:

- CPU-Nutzung
- Speichernutzung
- Datenträgernutzung
- Systemausfälle
- Kritische Ereignisse
- Ablauf von SSL-Zertifikaten

Die folgenden Beispiele veranschaulichen, wie Sie mit dem **Übersichtsfenster** interagieren können, um die Instanzen zu isolieren, die Fehler melden.

Beispiel 1: Zeigen Sie Instanzen an, die sich in einem Überprüfungsstatus befinden:

Aktivieren Sie das Kontrollkästchen **Überprüfen**, um nur die Instanzen anzuzeigen, die keine kritischen Fehler melden, aber dennoch beachtet werden müssen.

Die Histogramme im Bedienfeld **Übersicht** stellen eine aggregierte Anzahl von Instanzen dar, die auf hoher CPU-Auslastung, hoher Speicherauslastung und hoher Datenträgernutzung basieren. Die Histogramme werden mit 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90% und 100% bewertet. Bewegen Sie den Mauszeiger auf eines der Balkendiagramme. Die Legende am unteren Rand des Diagramms zeigt den Verwendungsbereich und die Anzahl der Instanzen in diesem Bereich an. Sie können auch auf das Balkendiagramm klicken, um alle Instanzen in diesem Bereich anzuzeigen.

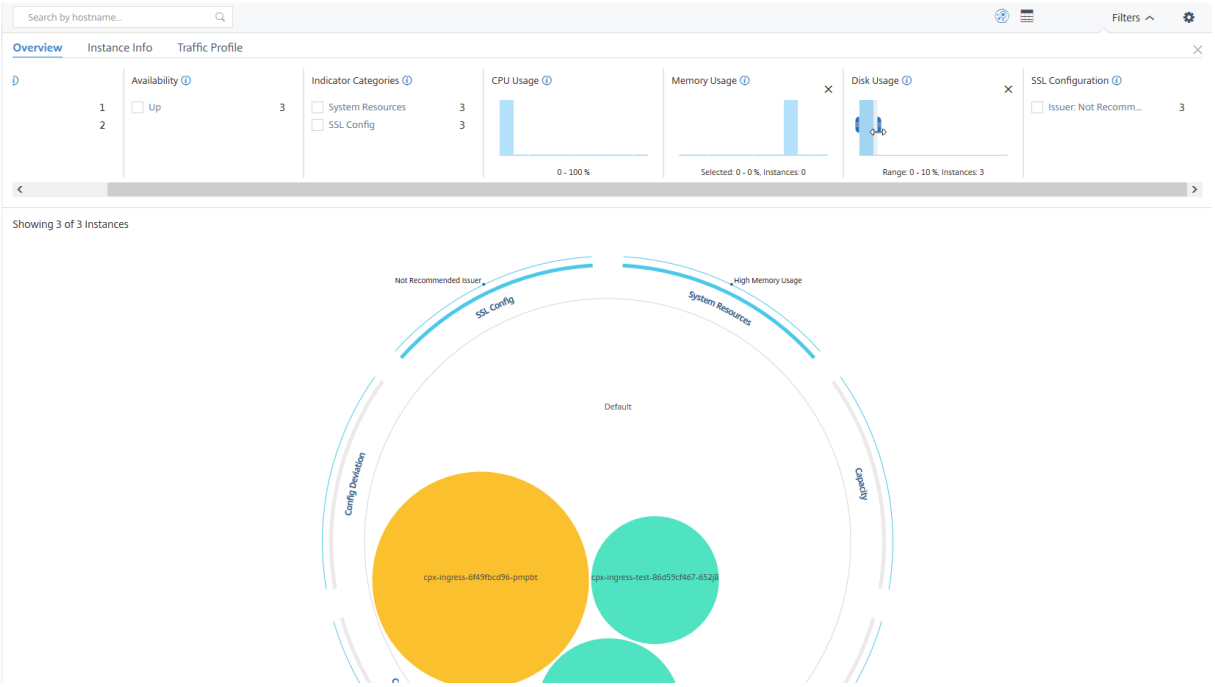
Beispiel 2: Zeigen Sie Instanzen an, die zwischen 10 und 20% des zugewiesenen Speichers verbrauchen:

Klicken Sie im Abschnitt Speicherverbrauch auf das Balkendiagramm. Die Legende zeigt, dass der ausgewählte Bereich zwischen 10 und 20% liegt und 29 Instanzen in diesem Bereich arbeiten.

Sie können in diesen Histogrammen auch mehrere Bereiche auswählen.

Beispiel 3: Instances anzeigen, die in mehreren Bereichen viel Speicherplatz beanspruchen:

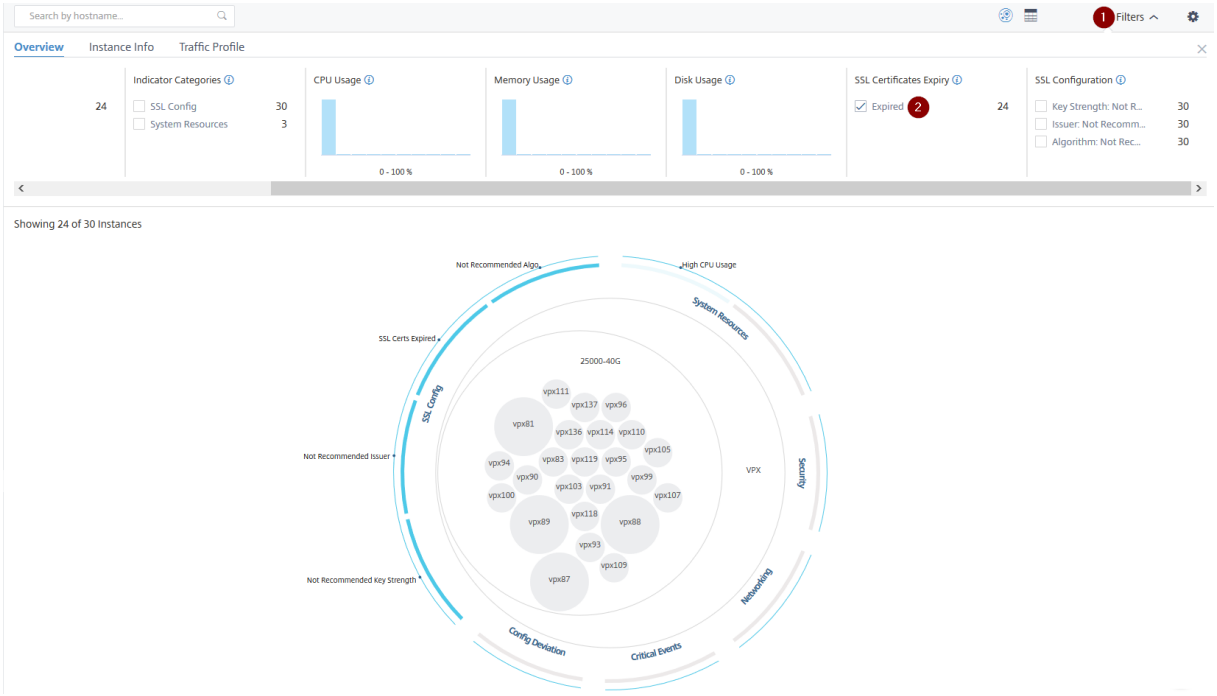
Um Instanzen anzuzeigen, die Speicherplatz zwischen 0 und 10% belegt haben, ziehen Sie den Mauszeiger über die beiden Bereiche.



> **Hinweis**
>
> Klicken Sie auf "X", um die Auswahl zu entfernen. Sie können auch auf **Zurücksetzen** klicken, um Mehrfachauswahlen zu entfernen.

Die horizontalen Balkendiagramme im **Übersichtsfenster** zeigen die Anzahl der Instanzen an, die Systemfehler, kritische Ereignisse und den Ablaufstatus der SSL-Zertifikate melden. Aktivieren Sie das Kontrollkästchen, um diese Instanzen anzuzeigen.

Beispiel 4: Zeigen Sie Instanzen für abgelaufene SSL-Zertifikate an:



1 —Klicken Sie auf die **Filterliste** .

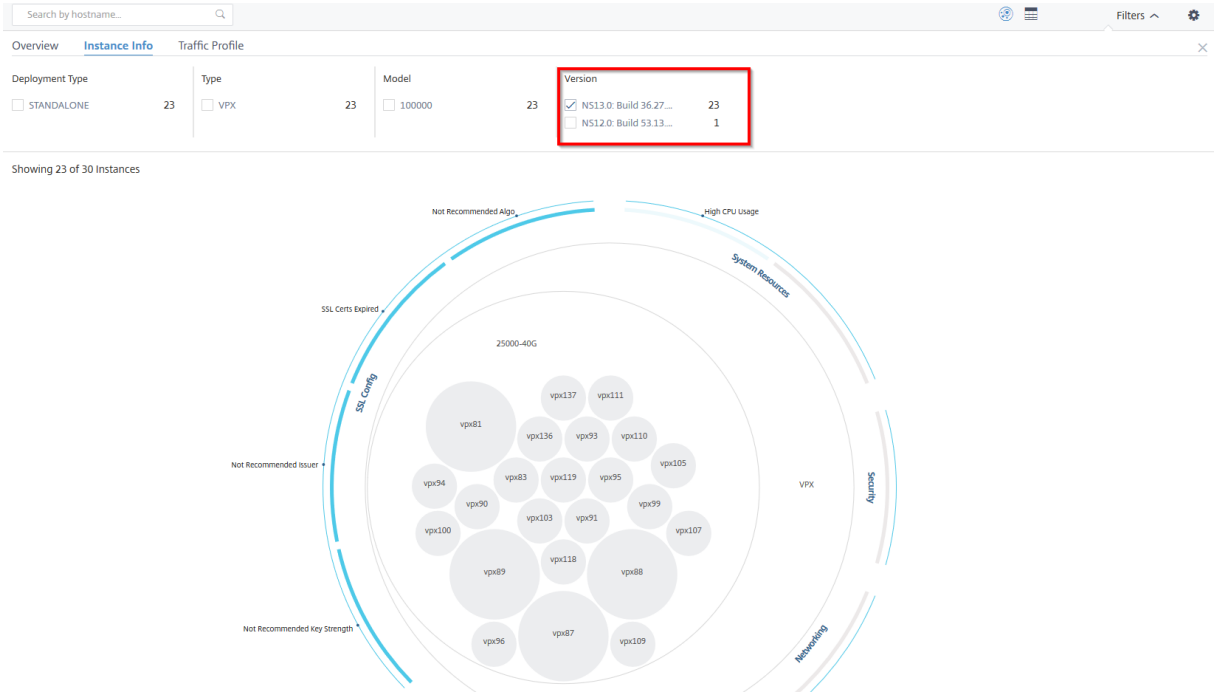
2 —Aktivieren Sie im Abschnitt **Ablauf von SSL-Zertifikaten** das Kontrollkästchen **Abgelaufen**, um die Instanzen anzuzeigen.

Instanzinformationen

Im Bereich **Instanzinformationen** können Sie Instanzen basierend auf dem Bereitstellungstyp, dem Instanztyp, dem Modell und der Softwareversion anzeigen. Sie können mehrere Kontrollkästchen aktivieren, um Ihre Auswahl einzugrenzen.

Beispiel 5: Anzeigen von ADC VPX-Instanzen mit einer bestimmten Build-Nummer:

Wählen Sie die Version aus, die Sie anzeigen möchten.



Traffic-Profil

Die Histogramme im Bereich **Traffic-Profil** stellen eine aggregierte Anzahl von Instanzen dar, die auf dem lizenzierten Durchsatz der Instanzen, der Anzahl der Anfragen, Verbindungen und Transaktionen basieren, die von den Instanzen verarbeitet werden. Wählen Sie das Balkendiagramm aus, um Instanzen in diesem Bereich anzuzeigen.

Beispiel 6: Instanzen anzeigen, die TCP-Verbindungen unterstützen:

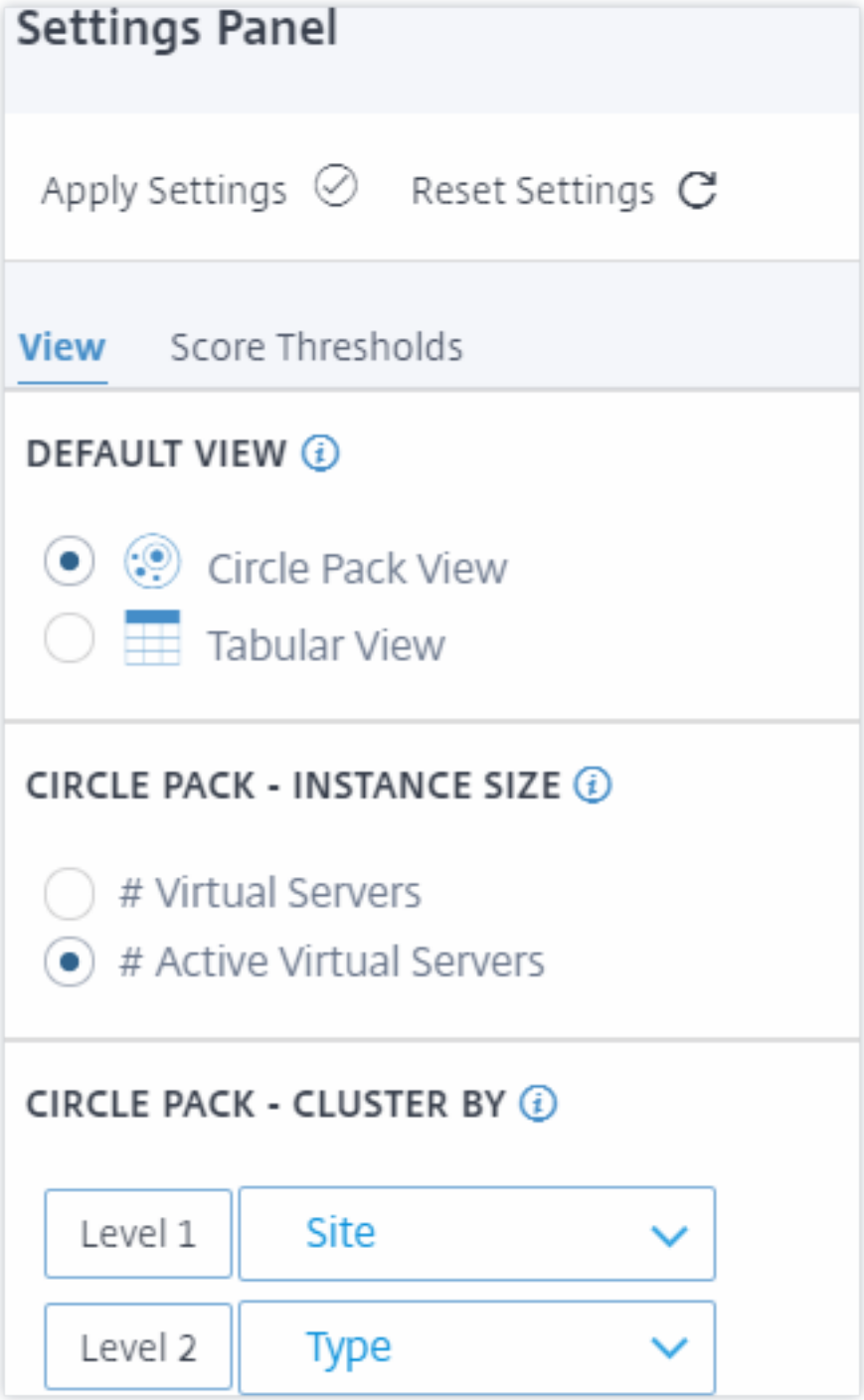
Die folgende Abbildung zeigt die Anzahl der Instanzen, die TCP-Verbindungen unterstützen.

So verwenden Sie das Einstellungsfeld

Im Bereich **Einstellungen** können Sie die Standardansicht von Infrastructure Analytics festlegen. Außerdem können Sie die niedrigen und hohen Schwellenwerte für hohe CPU-Auslastung, hohe Datenträgernutzung und hohe Speicherauslastung festlegen. Das Einstellungsfenster ist in zwei Tabs unterteilt: Ansicht und Punktegrenzwerte.

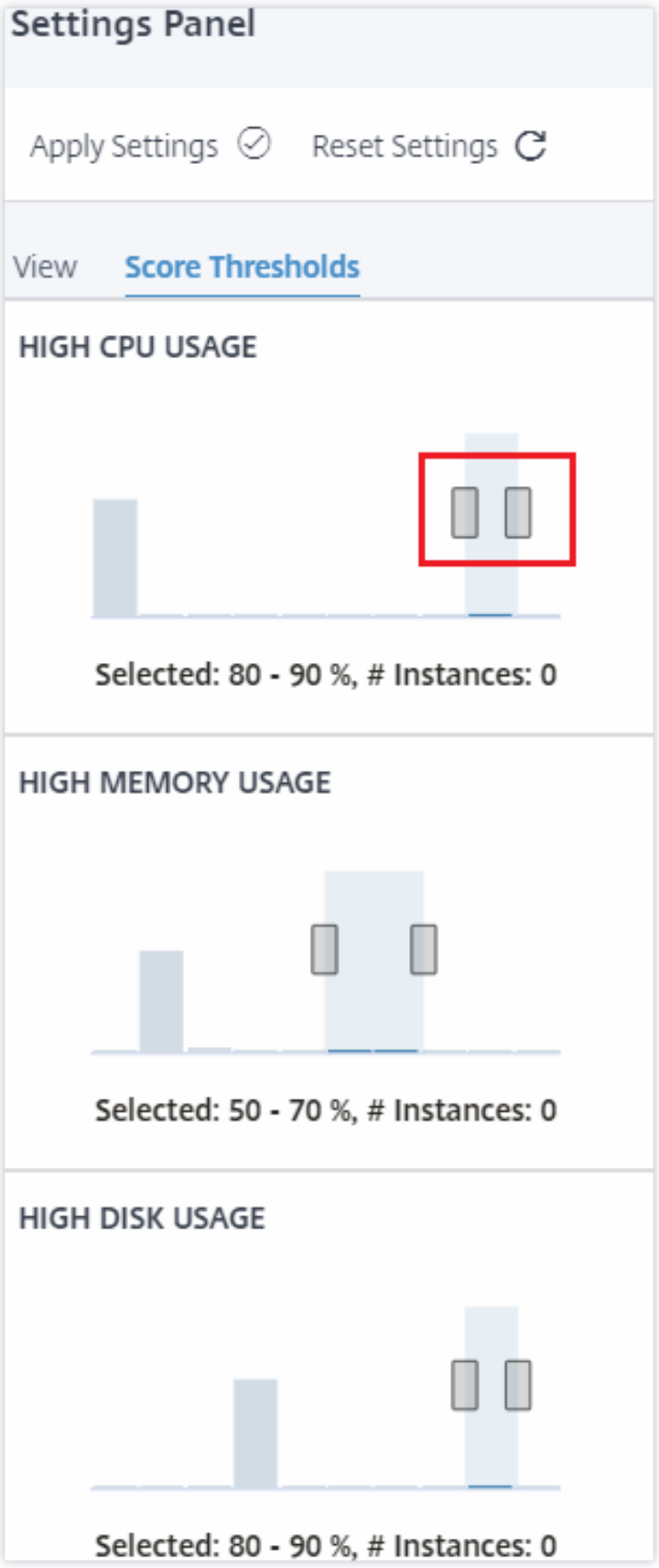
View

- **Standardansicht**. Wählen Sie **Circle Pack** oder Tabellarisches Format als Standardansicht auf der Analyseseite aus. Das Format, das Sie auswählen, wird angezeigt, wenn Sie in NetScaler ADM auf die Seite zugreifen.
- **Circle Pack —Instanzgröße**. Lässt die Größe des Instanzkreises entweder auf die Anzahl der virtuellen Server oder die Anzahl der aktiven virtuellen Server zu.
- **Circle Pack - Cluster von**. Entscheiden Sie sich für das zweistufige Clustering der Instanzkreise. Weitere Informationen zum Instanzclustering finden Sie unter Clustered Exemplarkreise.



Score-Schwellenwerte

Sie können die niedrigen und hohen Schwellenwerte für eine hohe CPU-, Arbeitsspeicher- und Festplattenauslastung je nach den Datenverkehrsanforderungen in Ihrem Unternehmen ändern. Ziehen Sie die Griffe in jedem der Auswahlhistogramme, um die Werte festzulegen.



> **Hinweis:**
>
> Klicken Sie auf **Einstellungen übernehmen**, um diese Änderungen zu übernehmen, oder klicken Sie auf **Zurücksetzen**, um alle Änderungen zu entfernen.

So visualisieren Sie Daten auf dem Dashboard

Mithilfe von Infrastructure Analytics können Netzwerkadministratoren nun Instanzen identifizieren, die die meiste Aufmerksamkeit benötigen, innerhalb weniger Sekunden. Um die Datenvisualisierung genauer zu verstehen, betrachten wir den Fall von Chris, einem Netzwerkadministrator von Example-Company.

Chris verwaltet viele Citrix ADC Instanzen in der Organisation. Einige der Instanzen verarbeiten viel Traffic, und Chris muss sie genau beobachten. Chris stellt fest, dass einige stark frequentierte Instances nicht mehr den gesamten Traffic verarbeiten, der durch sie fließt. Um diesen Rückgang zu analysieren, musste Chris zuvor mehrere Datenberichte aus verschiedenen Quellen lesen. Chris musste mehr Zeit damit verbringen, die Daten manuell zu korrelieren und festzustellen, welche Instanzen sich nicht in einem optimalen Zustand befinden und Aufmerksamkeit erfordern.

Chris verwendet die Infrastructure Analytics-Funktion, um den Zustand aller Instanzen visuell zu sehen.

Die folgenden zwei Beispiele veranschaulichen, wie Infrastructure Analytics Chris bei Wartungsaktivitäten unterstützt:

Beispiel 1 - So überwachen Sie den SSL-Verkehr:

Chris bemerkt im Circle Pack, dass eine Instanz einen niedrigen Instanzwert hat und sich diese Instanz im Status “Kritisch”befindet. Chris klickt auf diese Instanz, um zu sehen, was das Problem ist. In der Instanzübersicht wird angezeigt, dass auf dieser Instanz ein SSL-Kartenfehler aufgetreten ist und die Instanz keinen SSL-Verkehr verarbeiten kann (der SSL-Verkehr wurde reduziert). Chris extrahiert diese Informationen und sendet einen Bericht an das Team, um das Problem sofort zu untersuchen.

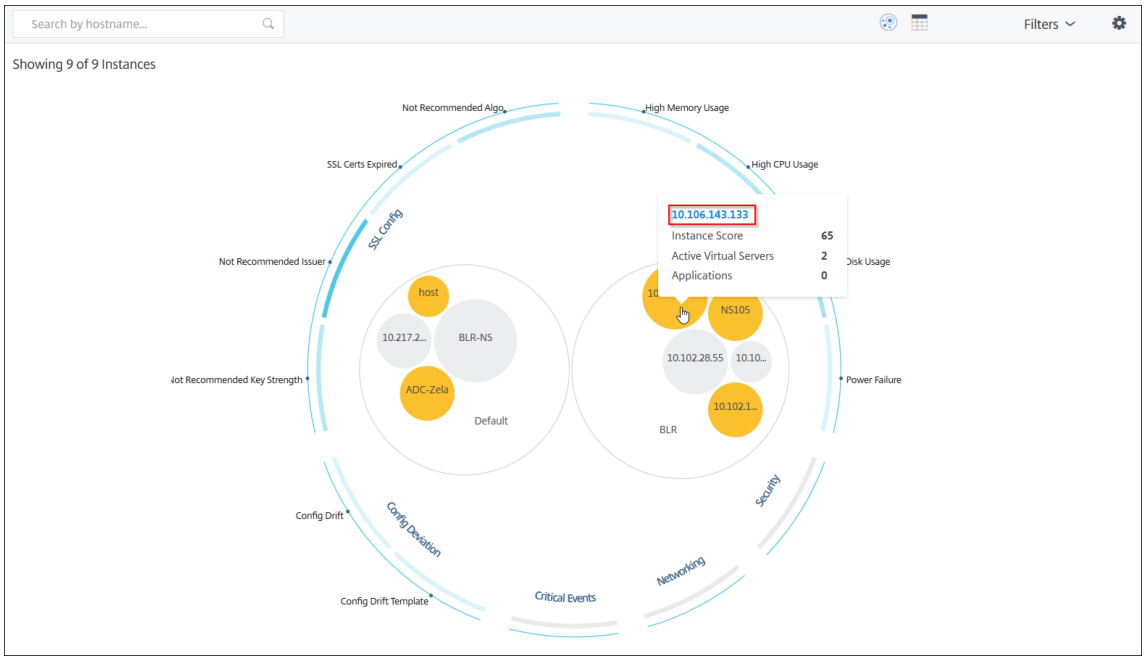
Beispiel 2 - So überwachen Sie Konfigurationsänderungen:

Chris bemerkt auch, dass sich eine andere Instanz im Status “Überprüfung”befindet und dass es in letzter Zeit eine Konfigurationsabweichung gegeben hat. Wenn Chris auf den Risikoindikator für Konfigurationsabweichungen klickt, bemerkt Chris, dass Konfigurationsänderungen im Zusammenhang mit RC4 Cipher, SSL v3, TLS 1.0 und TLS 1.1 vorgenommen wurden, die möglicherweise auf Sicherheitsbedenken zurückzuführen sind. Chris stellt außerdem fest, dass das SSL-Transaktions-Traffic-Profil für diese Instanz ausgefallen ist. Chris exportiert diesen Bericht und sendet ihn an den Administrator, um weitere Informationen zu erhalten.

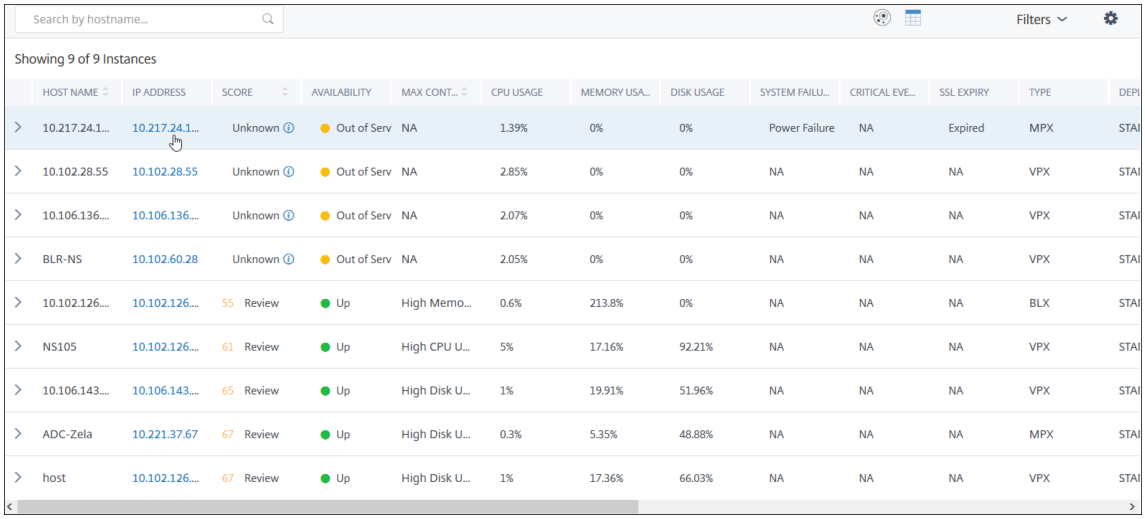
Instanzdetails in Infrastructure Analytics anzeigen

February 5, 2024

1. Navigieren Sie zu **Netzwerke** > **Infrastrukturanalyse**
2. Klicken Sie auf die Circle Pack-Ansicht, und wählen Sie die IP-Adresse aus.



Sie können auch in der Tabellenansicht auf eine IP-Adresse klicken.



- **Hostname** —Bezeichnet den Hostnamen, der der ADC-Instanz zugewiesen ist
- **IP-Adresse** —Gibt die IP-Adresse der ADC-Instanz an
- **Score** —Gibt den ADC-Instanz-Score und den Status wie Kritisch, Gut und Fair an

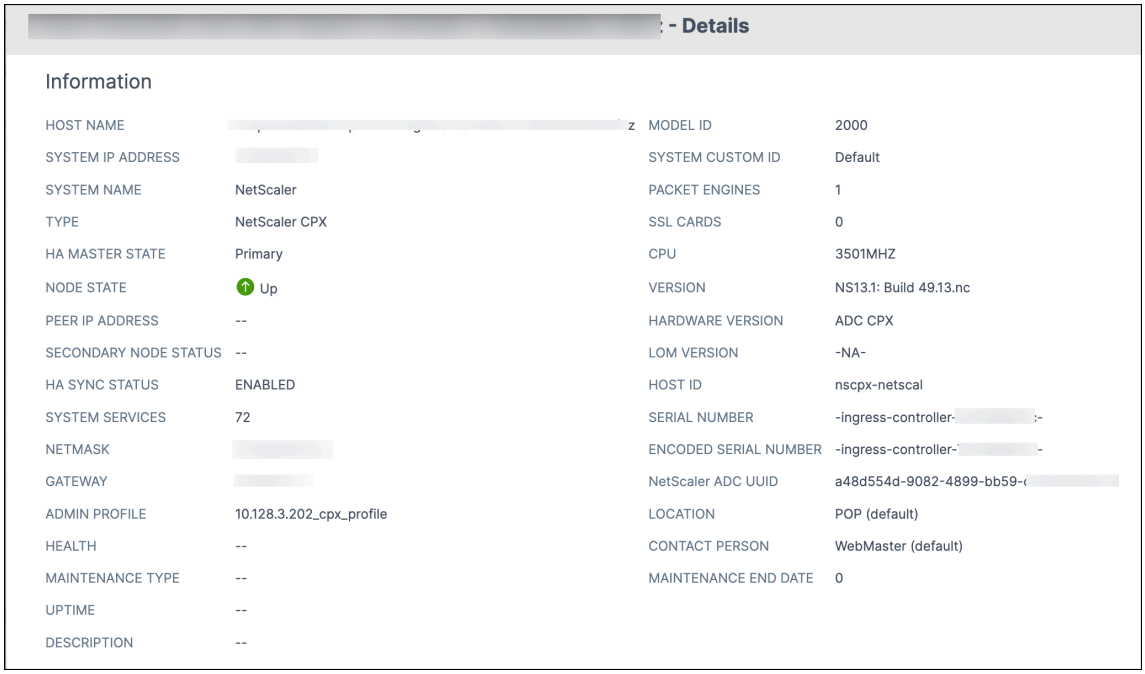
- **Verfügbarkeit** —Gibt den Status der ADC-Instance an, z. B. **Up**, **Down**oder **Out of Service**.
- **Max. Beitrag** —Gibt die Problemkategorie an, in der die ADC-Instanz die maximale Fehleranzahl aufweist.
- **CPU-Auslastung** —Gibt den aktuellen CPU-Prozentsatz an, der von der Instanz verwendet wird
- **Speichernutzung** —Gibt den aktuellen Speicherprozentsatz an, der von der Instanz verwendet wird
- **Datenträgernutzung** —Gibt den aktuellen Datenträgerprozentsatz an, der von der Instanz verwendet
- **Systemfehler** —Gibt die Gesamtzahl der Fehler für das Instanzsystem an
- **Kritische Ereignisse** —Bezeichnet die Ereigniskategorie, in der die NetScaler ADC-Instanz die maximalen Ereignisse aufweist.
- **SSL-Ablauf** —Gibt den Status des auf der ADC-Instanz installierten SSL-Zertifikats an
- **Typ** —Bezeichnet den ADC-Instanztyp wie VPX, SDX, MPX oder CPX
- **Bereitstellung** —Gibt an, ob die ADC-Instanz als eigenständige Instanz oder HA-Paar bereitgestellt wird
- **Modell** —Bezeichnet die Modellnummer der ADC-Instanz
- **Version** —Bezeichnet die ADC-Instanzversion und Build-Nummer
- **Durchsatz** —Gibt den aktuellen Netzwerkdurchsatz von der ADC-Instanz an.
- **HTTPS-Anforderung/Sekunde** —Bezeichnet die aktuellen HTTPS-Anforderungen/s, die von der ADC-Instanz empfangen wurden
- **TCP-Verbindung** —Bezeichnet die aktuell aufgebauten TCP-Verbindungen
- **SSL-Transaktion** —bezeichnet die aktuellen SSL-Transaktionen, die von der ADC-Instanz verarbeitet werden
- **Site** —Gibt den Namen der Site an, auf der die ADC-Instanz bereitgestellt wird.

> **Hinweis**
>
> Alle 5 Minuten werden die aktuellen Werte für CPU-Auslastung, Speichernutzung, Datenträgerauslastung, Durchsatz usw. aktualisiert.

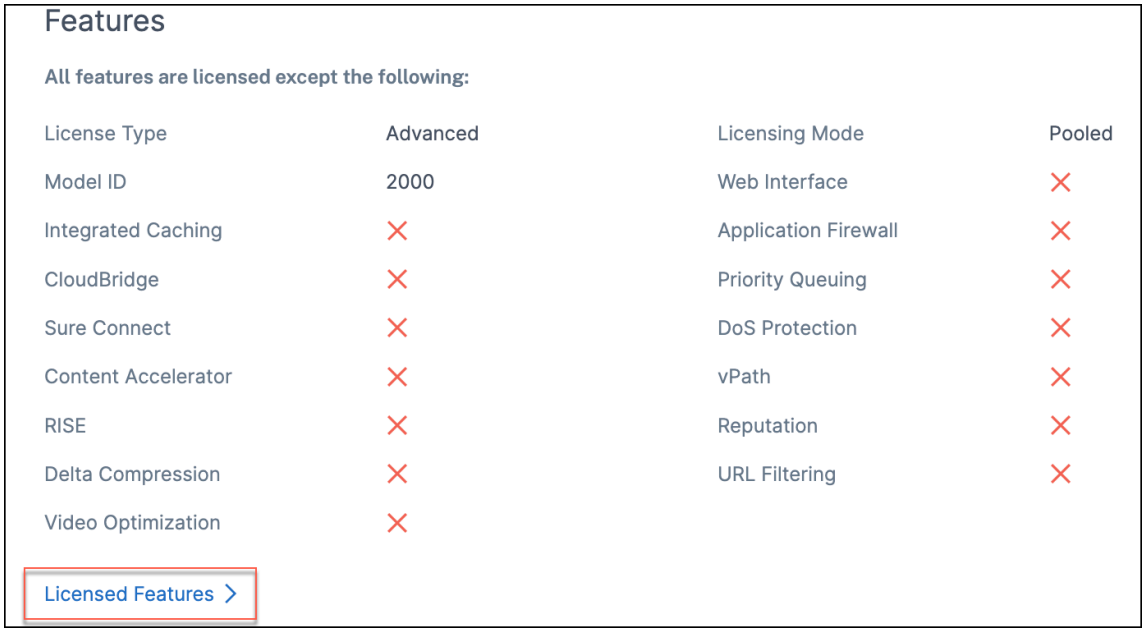
Klicken Sie auf **Instanzdetails**, um die Details anzuzeigen.

Die folgenden Details werden angezeigt:

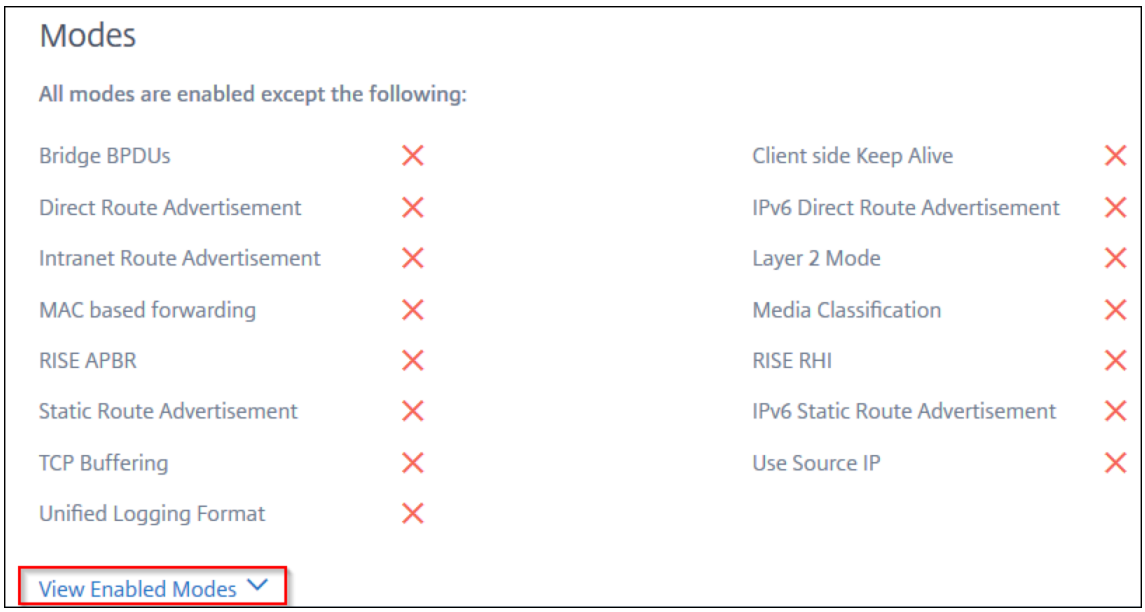
- **Informationen** —Instanzdetails wie Instanztyp, Bereitstellungstyp, Version, Modell.



- **Funktionen** —Standardmäßig werden die Funktionen angezeigt, die nicht lizenziert sind. Klicken Sie auf **Lizenzierte Funktionen**, um die lizenzierten Funktionen anzuzeigen.

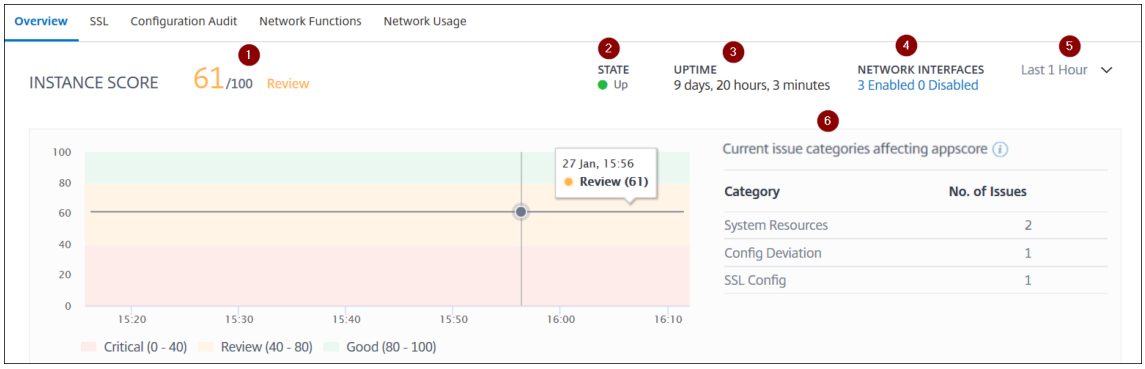


- **Modi** —Standardmäßig werden alle Modi angezeigt, die auf der Instanz deaktiviert sind. Klicken Sie auf **Aktivierte Modi** anzeigen, um die aktivierten Modi auf der Instanz anzuzeigen.



Das Instanz-Dashboard bietet eine Instanzübersicht, in der Sie die folgenden Details sehen können:

- **Instanz-Score**



1 —Gibt die aktuelle NetScaler ADC-Instanzbewertung für die ausgewählte Zeitdauer an. Das Endergebnis wird als **100 minus Gesamtstrafen**berechnet. Das Diagramm zeigt die Score-Bereiche für die ausgewählte Zeitdauer an.

2 —Gibt den Status der Citrix ADC Instanz an, z. B. **Up-**, **Down-**und **Out-Out of Service**.

3 —Gibt die Dauer an, die die NetScaler ADC-Instanz ausgeführt wird.

4 —Zeigt die Gesamtzahl der für die Instanz aktivierten und deaktivierten Netzwerkschnittstellen an. Klicken Sie hier, um Details wie den Namen der Netzwerkschnittstelle und den Status (aktiviert oder deaktiviert) anzuzeigen.

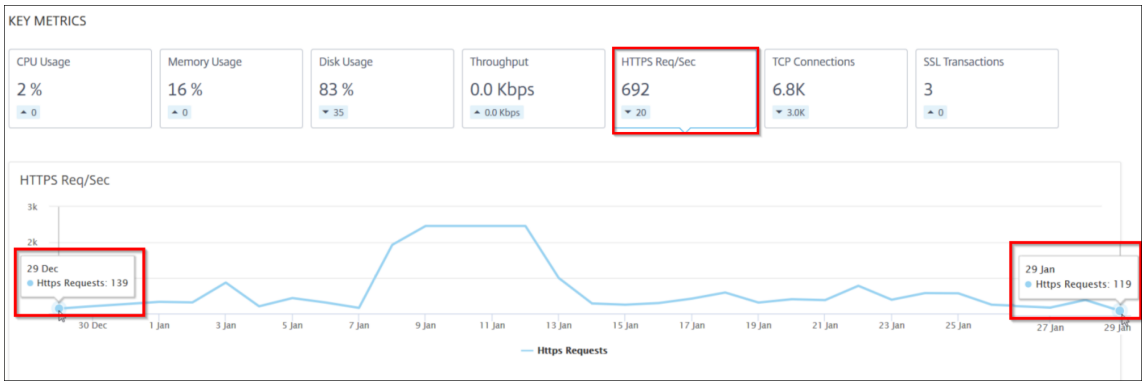
5 —Wählen Sie die Zeitdauer aus der Liste aus, um die Instanzdetails anzuzeigen.

6 —Zeigt die Gesamtzahl der Probleme und die Problemkategorie der ADC-Instanz an.

- **Wichtige Metriken**

Klicken Sie auf jede Registerkarte, um die Details anzuzeigen. In jeder Metrik können Sie den Durchschnittswert und den Differenzwert für die ausgewählte Zeit anzeigen.

Das folgende Bild ist ein Beispiel für HTTPS Req/Sec und die gewählte Zeitdauer beträgt 1 Stunde. Der Wert **692** ist der durchschnittliche HTTPS-Req/Sek für die Dauer von 1 Monat und der Wert **20** ist der Differenzwert. In der Grafik ist der erste Wert **139** und der letzte Wert **119**. Der Differenzwert beträgt **139 —119 = 20.**



Sie können die folgenden Instanzmetriken für die ausgewählte Zeitdauer in einem Diagrammformat anzeigen:

- **CPU-Auslastung** —Der durchschnittliche CPU-Prozentsatz der Instanz für die ausgewählte Dauer (wird sowohl für die Paket-CPU als auch für die Verwaltungs-CPU angezeigt).
- **Speichernutzung** —Die durchschnittliche Speichernutzung in% der Instanz für die ausgewählte Dauer.
- **Datenträgernutzung** —Der durchschnittliche Speicherplatz in % der Instanz für die ausgewählte Dauer.
- **Durchsatz** —Der durchschnittliche Netzwerkdurchsatz, der von der Instanz für die ausgewählte Dauer verarbeitet wird.
- **HTTPS-Anforderung/Sekunde** —Die durchschnittlichen HTTPS-Anforderungen, die von der Instanz für die ausgewählte Dauer empfangen wurden.
- **TCP-Verbindungen** —Die durchschnittlichen TCP-Verbindungen, die vom Client und Server für die ausgewählte Dauer eingerichtet wurden.
- **SSL-Transaktionen** —Die durchschnittlichen SSL-Transaktionen, die von der Instanz für die ausgewählte Dauer verarbeitet wurden.

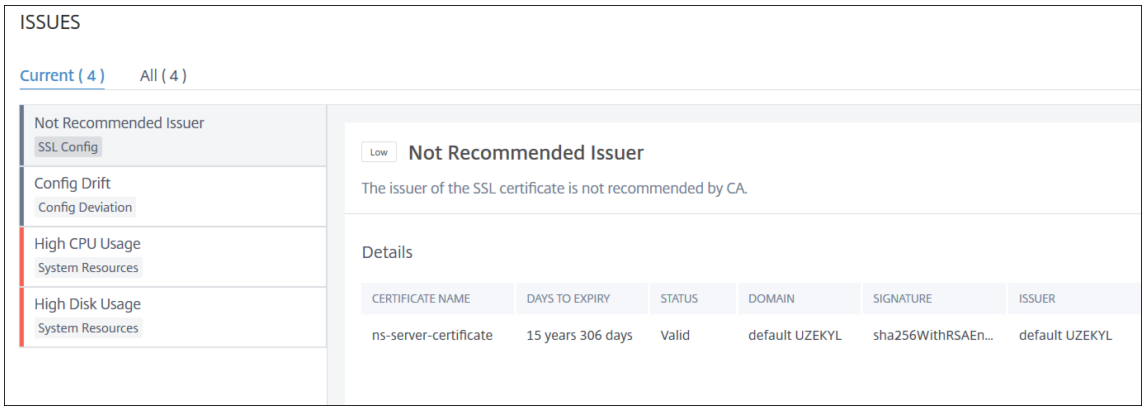
- **Probleme**

  Sie können die folgenden Probleme anzeigen, die in der NetScaler ADC-Instanz auftreten:

Kategorie der Ausgabe	Beschreibung	Probleme
Systemressourcen	Zeigt alle Probleme im Zusammenhang mit der Citrix ADC -Systemressource an, z. B. CPU, Arbeitsspeicher, Datenträgerauslastung.	– Hohe CPU-Auslastung – Hoher Speicherverbrauch – Hohe Datenträgernutzung – SSL-Kartenfehler – Stromausfall – Datenträgerfehler – Flashfehler – NIC Discards
SSL-Konfiguration	Zeigt alle Probleme im Zusammenhang mit der SSL-Konfiguration auf der NetScaler ADC-Instanz an.	– SSL-Zertifikate sind abgelaufen – Nicht empfohlener Herausgeber – Nicht empfohlener Algorithmus – Nicht empfohlene Schlüsselstärke
Abweichung der Konfiguration	Zeigt alle Probleme im Zusammenhang mit den Konfigurationsaufträgen an, die in der NetScaler ADC-Instanz angewendet werden.	– Konfigurationsdrift – Running vs Template
Kritische Ereignisse	Zeigt alle kritischen Ereignisse im Zusammenhang mit NetScaler ADC-Instanzen an, die im HA-Paar und im Cluster konfiguriert sind.	– Ausfall von Cluster Prop

Kategorie der Ausgabe	Beschreibung	Probleme
Netzwerke	Zeigt die Betriebsprobleme an, die in den Instanzen auftreten.	– Fehler bei der Cluster – Nicht übereinstimmende Cluster-Versionen – HA Schlechter Sekundärstaat – HA Keine Hitze schlägt – HA-Synchronisierungsfehler – Nichtübereinstimmung der HA-Version Weitere Informationen finden Sie unter Verbesserte Infrastrukturanalyse mit neuen Indikatoren.

Klicken Sie auf die einzelnen Registerkarten, um das Problem zu analysieren und zu beheben. Stellen Sie sich beispielsweise vor, dass eine Instanz für die ausgewählte Zeitdauer die folgenden Fehler aufweist:



- Auf der Registerkarte **Aktuell** werden die Probleme angezeigt, die sich derzeit auf die Instanzbewertung auswirken.
- Auf der Registerkarte **Alle** werden alle Infrarotprobleme angezeigt, die für die ausgewählte Dauer erkannt wurden.

Anzeigen der Kapazitätsprobleme in einer ADC-Instanz

February 5, 2024

Wenn eine ADC-Instanz den größten Teil ihrer verfügbaren Kapazität verbraucht hat, kann es während der Verarbeitung des Client-Datenverkehrs zu einem Paket-Drop kommen. Dieses Problem führt zu einer geringen Leistung in einer ADC-Instanz. Wenn Sie solche ADC-Kapazitätsprobleme verstehen, können Sie proaktiv zusätzliche Lizenzen zuweisen, um die ADC-Leistung zu stabilisieren.

In der **Circle Pack-Ansicht**können Sie die Kapazitätsprobleme der ADC-Instanz anzeigen, falls vorhanden.

So zeigen Sie ADC-Kapazitätsprobleme an:

1. Navigieren Sie zu **Netzwerke > Infrastructure Analytics**.
2. Wählen Sie die Ansicht des Kreispakets aus.

> **Hinweis**
>
> In **Infrastructure Analytics**zeigen das Circle-Pack und die tabellarischen Ansichten die Ereignisse und Probleme an, die in der letzten Stunde aufgetreten sind.

Die folgende Abbildung legt nahe, dass die Kapazitätsprobleme in der ausgewählten Instanz auftreten:

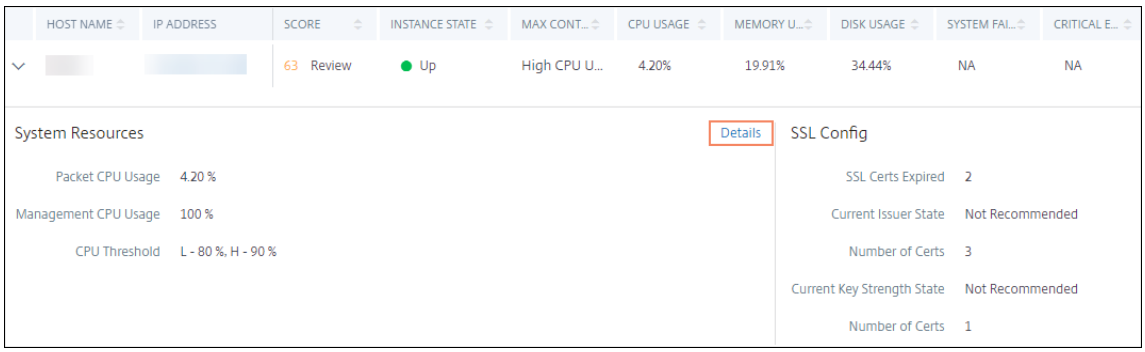
Die Probleme sind nach den folgenden Kapazitätsparametern kategorisiert:

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

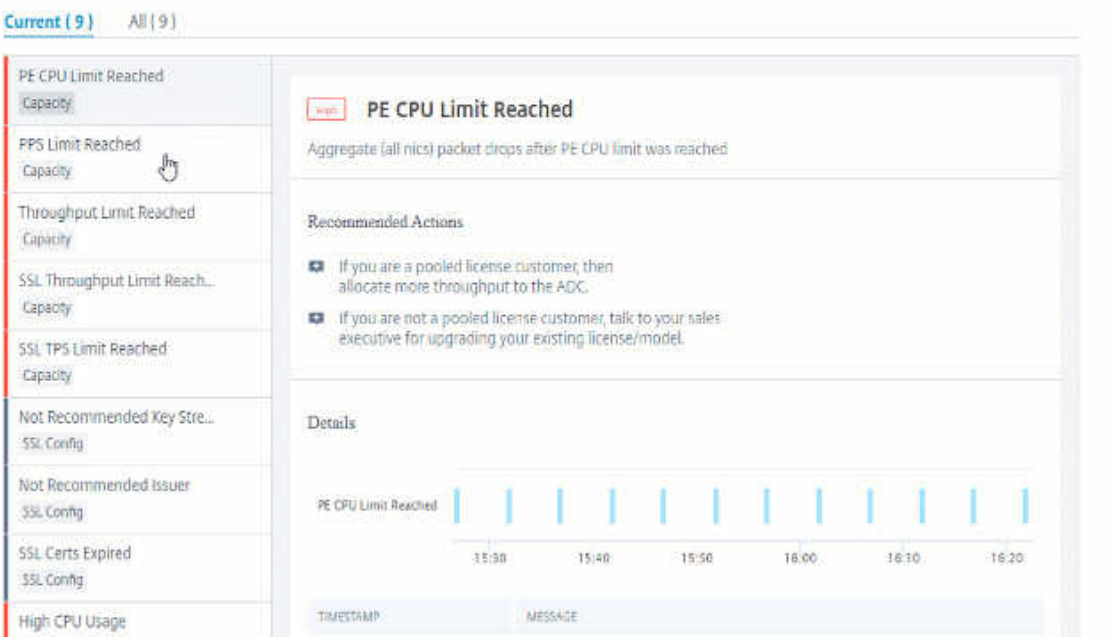
Empfohlene Maßnahmen zur Lösung von Kapazitätsproblemen anzeigen

Der ADM empfiehlt Maßnahmen, mit denen Kapazitätsprobleme gelöst werden können. Führen Sie die folgenden Schritte aus, um die empfohlenen Aktionen anzuzeigen:

1. Wählen Sie unter **Netzwerke > Infrastructure Analytics**die tabellarische Ansicht aus.
2. Wählen Sie die Instanz mit Kapazitätsproblemen aus, und klicken Sie auf **Details**.



3. Scrollen Sie auf der Instanzseite nach unten zum Abschnitt **Probleme** .
4. Wählen Sie jedes Problem aus und zeigen Sie die empfohlenen Maßnahmen zur Behebung von Kapazitätsproblemen an.



Der ADM ruft diese Ereignisse alle fünf Minuten von der ADC-Instanz ab und zeigt die verworfenen Pakete oder Rate-Limit-Zähler-Inkremente an, falls vorhanden.

Das ADM berechnet die Instanzbewertung anhand des definierten Kapazitätsschwellenwerts.

- **Niedriger Schwellenwert** —1 Zählerinkrement für Paketverlust oder Ratenbegrenzung
- **Hoher Schwellenwert** —10.000 Paketverlust oder Erhöhung des Ratenlimit-Zählers

Wenn eine ADC-Instanz den Kapazitätsschwellenwert überschreitet, wirkt sich dies auf den Instanzwert aus.

Wenn Pakete fallen oder der Zähler für die Ratenbegrenzung inkrementiert wird, wird ein Ereignis in der Kategorie `ADCCapacityBreach` generiert. Um diese Ereignisse einzusehen, navigieren Sie zu **Konten > Systemereignisse**.

Verbesserte Infrastrukturanalyse mit neuen Indikatoren

February 5, 2024

Mit NetScaler ADM Infrastructure Analyticskönnen Sie:

- Zeigen Sie eine neue Reihe von Betriebsproblemen an, die in NetScaler ADC-Instanzen auftreten.
- Zeigen Sie Fehlermeldungen an und überprüfen Sie Empfehlungen zur Behebung der Probleme.

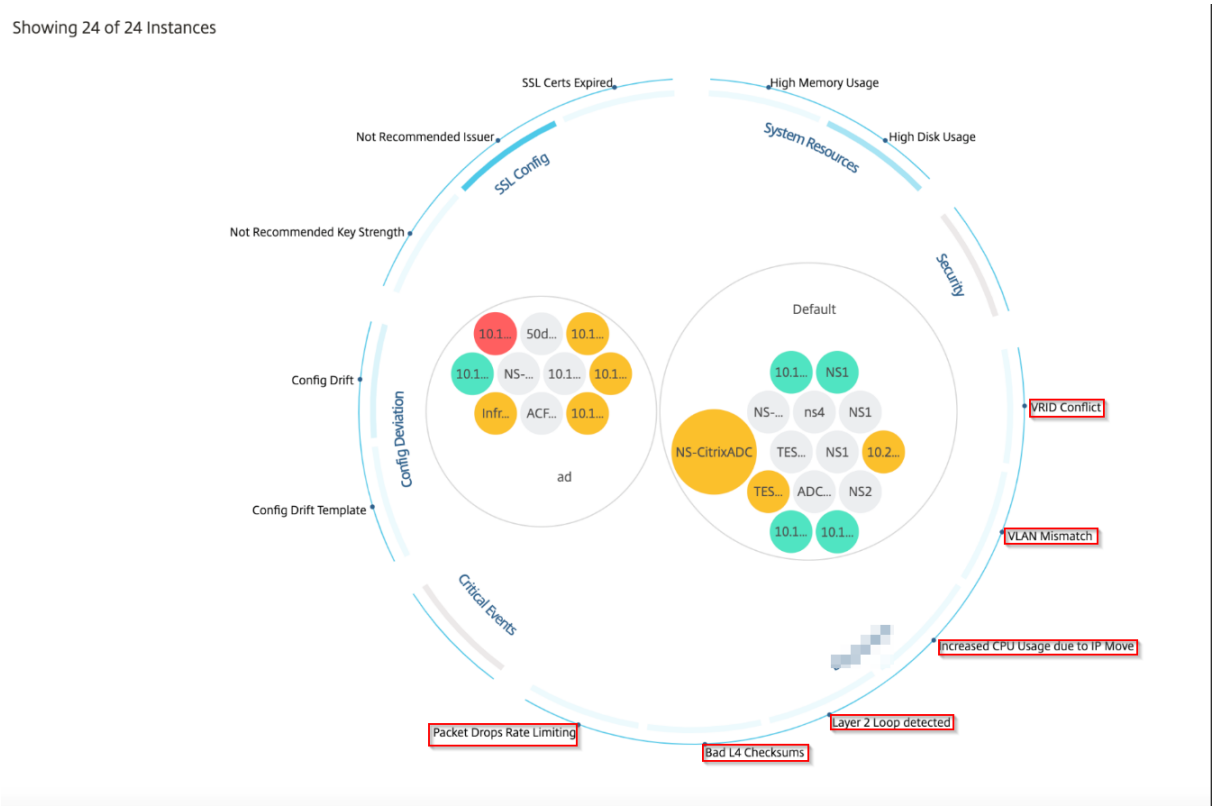
Als Administrator können Sie schnell die Ursachenanalyse von Problemen identifizieren.

> **Hinweis**
>
> Regelindikatoren werden nicht unterstützt für:
>
> - NetScaler ADC-Instanzen, die im Clustermodus konfiguriert sind.
> - NetScaler ADC-Instanzen, die mit Administratorpartitionen konfiguriert sind.

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

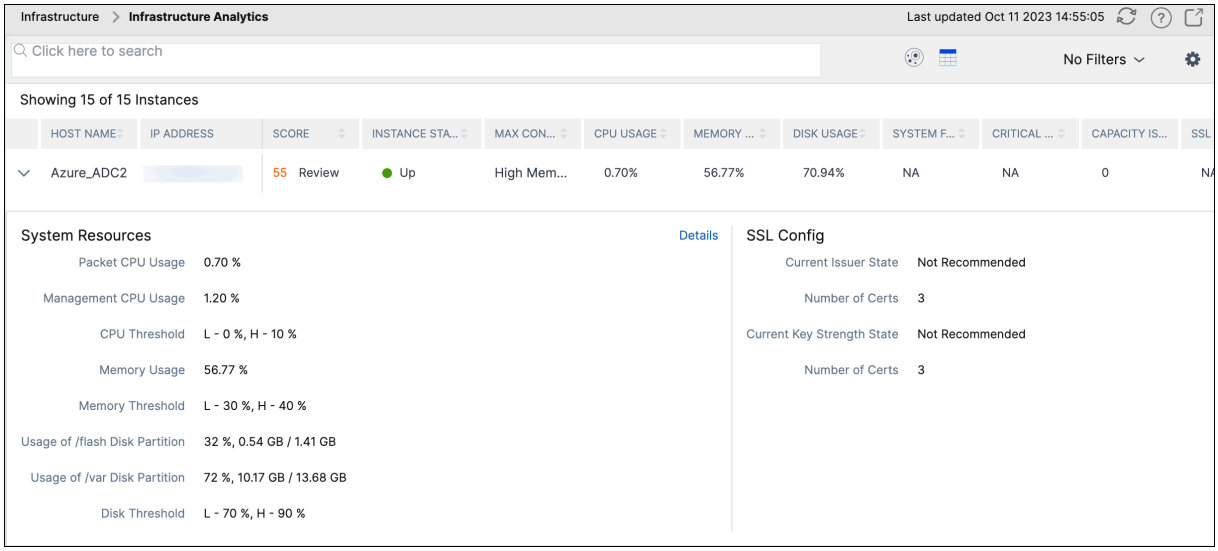
Indikatorname in Infrastructure Analytics	Beschreibung
Fehler bei Portzuweisung	Erkennt, wenn NetScaler ADC SNIP verwendet, um mit einer neuen Serververbindung zu kommunizieren, und die Gesamtzahl der auf diesem SNIP verfügbaren Ports erschöpft ist. Die empfohlene Aktion besteht darin, ein weiteres SNIP im selben Subnetz hinzuzufügen.
Keine Standard-Routenkonfiguration	Erkennt, wenn der Datenverkehr aufgrund der Nichtverfügbarkeit von Routen unterbrochen wird.
IP-Konflikt	Erkennt, ob dieselbe IP-Adresse auf zwei oder mehr Instanzen in einem Netzwerk konfiguriert oder angewendet wurde.
VRID-Konflikt	Erkennt, wenn zeitweise Zugriffsprobleme für die angegebene VRID auftreten.
VLAN-Nichtübereinstimmung	Erkennt, ob während der an IP-Subnetze gebundenen VLAN-Konfiguration Fehler auftreten.

Indikatorname in Infrastructure Analytics	Beschreibung
TCP-Angriff auf kleine Fenster	Erkennt, wenn möglicherweise ein kleiner Fensterangriff im Gange ist. Diese Warnung dient nur zur Information, da ADC diesen Angriff bereits abwehrt.
Schwellenwert für die Rat	Erkennt basierend auf dem konfigurierten Schwellenwert für die Ratenkontrolle, wenn Pakete verworfen
Persistenz-Limit	Erkennt, wann maximale Treffer auf den NetScaler ADC-Speicher angewendet werden.
Nichtübereinstimmung mit GSLB-Site-	Erkennt, wenn GSLB-Konfigurationssynchronisierungsfehler aufgrund einer Nichtübereinstimmung des Site-Namens auftreten
Falscher IP-Header	Erkennt, wenn Plausibilitätsprüfungen für IPv4-Pakete fehlgeschlagen sind.
Schlechte L4-Prüfsumme	Erkennt, wenn die Prüfsummenüberprüfung für TCP-Pakete fehlgeschlagen ist
Erhöhte CPU-Auslastung durch IP-Verschiebung	Erkennt, ob eine große Anzahl von Macs aktualisiert werden muss.
Übermäßige Paketsteuerung	Erkennt ein hohes Maß an Softwarepaketsteuerung aufgrund der Verwendung eines asymmetrischen RSS-Schlüsseltyps.
Layer-2-Schleife	Erkennt das Vorhandensein von Layer-2-Schleifen im Netzwerk.
Getaggt: VLAN mismatch	Erkennt, wenn markierte VLAN-Pakete auf einer Schnittstelle ohne Tags empfangen werden.



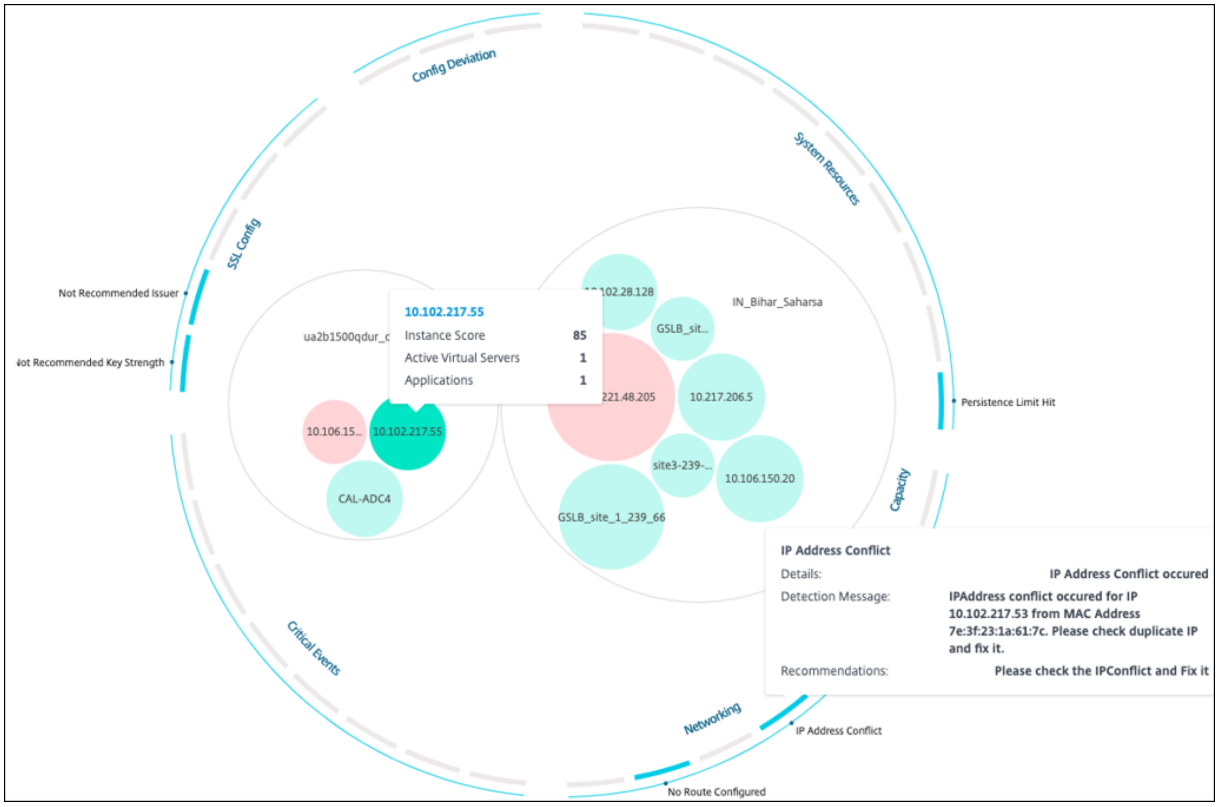
Tabellarische Ansicht

Sie können auch Anomalien anzeigen, indem Sie die Option Tabellenansicht in **Infrastructure Analytics**verwenden. Navigieren Sie zu **Netzwerke** > **Infrastructure Analytics**, und klicken Sie dann auf , um alle verwalteten Instanzen anzuzeigen. Klicken Sie auf , um weitere Informationen anzuzeigen.



Details einer Anomalie anzeigen

Wenn Sie beispielsweise Details zu **IP-Adresskonflikten** im Netzwerk anzeigen möchten, klicken Sie auf die Anomalie, die für den IP-Adresskonflikt angezeigt wird, um die Details anzuzeigen.



- **Details** - Zeigt an, welche Anomalie festgestellt wurde
- **Erkennungsmeldung** —Zeigt die MAC-Adresse an, für die die IP-Adresse den Konflikt hat
- **Empfehlungen** —Gibt das Aktionselement zur Lösung dieses IP-Adresskonflikts an

Häufig gestellte Fragen

February 5, 2024

Dieser Abschnitt enthält häufig gestellte Fragen zu den folgenden Funktionen von NetScaler Application Delivery Management (NetScaler ADM). Klicken Sie in der folgenden Tabelle auf einen Funktionsnamen, um die Liste der FAQs für diese Funktion anzuzeigen.

Analytics	Authentifizierung	Konfigurationsverwaltung
Zertifikatverwaltung	Bereitstellung	Bereitstellung (Disaster Recovery)
Event-Management	Instanz-Verwaltung	StyleBooks
Systemverwaltung		

Analytics

Ist es erforderlich, den virtuellen EUEM-Kanal auf NetScaler Gateway-Instanzen zu aktivieren, die im Single-Hop-Modus bereitgestellt werden

Virtuelle EUEM-Kanaldaten sind Teil von HDX Insight Daten, die NetScaler ADM von Gateway-Instanzen erhält. Der virtuelle EUEM-Kanal stellt die Daten über ICA-RTT bereit. Wenn der virtuelle EUEM-Kanal nicht aktiviert ist, werden die restlichen HDX Insight-Daten weiterhin auf NetScaler ADM angezeigt.

Der virtuelle EUEM-Kanal ist ein Standarddienst, der auf Citrix Virtual Desktop-Anwendungen (VDA) ausgeführt wird. Wenn es nicht ausgeführt wird, starten Sie den Prozess "Citrix End User Experience Monitoring"in VDA-Diensten.

Wie aktiviere ich NetScaler ADM, um Webanwendungs- und Virtual-Desktop-Datenverkehr zu überwachen?

1. Navigieren Sie zu **Infrastructure** > **Instances** > **NetScaler ADC**, und wählen Sie die NetScaler ADC-Instanz aus, auf der Sie Analysen aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
3. Wählen Sie auf der Seite "**Analytics konfigurieren** "alle virtuellen Server aus, auf denen Sie Analysen aktivieren möchten, und klicken Sie auf **AppFlow aktivieren**. Weitere Informationen finden Sie unter So aktivieren Sie Analytics für Instanzen.

> Hinweis
>
> Für NetScaler ADC-Instanzen der Version 11.0, Version 65.30 und höher gibt es in NetScaler ADM keine Option, Security Insight explizit zu aktivieren. Stellen Sie sicher, dass Sie die AppFlow Parameter auf den NetScaler ADC-Instanzen konfigurieren, damit NetScaler ADM den Security Insight-Datenverkehr zusammen mit dem Web Insight-Datenverkehr empfängt. Weitere Informationen zum Festlegen der AppFlow-Parameter auf NetScaler ADC-Instanzen finden Sie unterSo legen Sie die AppFlow-Parameter mithilfe des Konfigurationsdienstprogrammsfest.

Wird NetScaler ADM nach dem Hinzufügen der NetScaler ADC-Instanzen automatisch analytische Informationen gesammelt?

Nein. Aktivieren Sie Analysen auf den virtuellen Servern, die in NetScaler ADC-Instanzen gehostet werden und von NetScaler ADM verwaltet werden. Weitere Informationen finden Sie unter So aktivieren Sie Analytics auf Instances .

Ist es erforderlich, auf die einzelne NetScaler ADC-Appliance zuzugreifen, um Analysen zu aktivieren?

Nein. Die gesamte Konfiguration erfolgt über die NetScaler ADM Benutzeroberfläche, in der die virtuellen Server aufgeführt sind, die auf der jeweiligen NetScaler ADC Instanz gehostet werden. Weitere Informationen finden Sie unter So aktivieren Sie Analytics auf Instances .

Welche Typen virtueller Server können in einer NetScaler ADC-Instanz aufgeführt werden, um Analysen zu aktivieren?

Derzeit listet die NetScaler ADM-Benutzeroberfläche die folgenden virtuellen Server für die Aktivierung von Analysen auf:

- Virtueller Lastausgleichsserver
- Virtuelle Content Switching-Server
- Virtueller VPN-Server
- Virtueller Server für die Cache-Umleitung

Wie stelle ich einen zusätzlichen Datenträger für NetScaler ADM bereit?

So stellen Sie einen zusätzliche Datenträger für NetScaler ADM bereit:

1. Fahren Sie die virtuelle NetScaler ADM Maschine herunter.
2. Stellen Sie im Hypervisor einen zusätzliche Datenträger mit der erforderlichen Datenträgergröße für die virtuelle NetScaler ADM-Maschine bereit.

   Zum Beispiel, Betrachten wir, dass Sie den Speicherplatz auf 200 GB erhöhen möchten, in einer virtuellen NetScaler ADM Maschine von 120 GB. In diesem Szenario müssen Sie einen Datenträgerspeicher von 200 GB anstelle von 80 GB bereitstellen. Neu zugeordnete 200 GB Speicherplatz werden zum Speichern von Datenbankdaten und NetScaler ADM Protokolldateien verwendet. Der vorhandene 120 GB Datenträgerspeicher wird zum Speichern von Kerndateien, Betriebssystemprotokolldateien usw. verwendet.
3. Starten Sie die virtuelle NetScaler ADM Maschine.

Was meinen Sie mit Collectors sind nicht auf NetScaler ADC-Instanzen konfiguriert?

Ein Collector empfängt AppFlow-Datensätze, die von der NetScaler ADC-Appliance generiert wurden.

NetScaler ADM empfängt Security Insight- und Web Insight-Datenverkehr von den NetScaler ADC-Instanzen, wenn die AppFlow-Funktion aktiviert ist. Wenn Sie die AppFlow-Funktion auf einer NetScaler ADC-Instanz aktivieren, müssen Sie mindestens einen Collector angeben, an den die AppFlow-Datensätze gesendet werden. Wenn die Collectors nicht auf den NetScaler ADC-Instanzen konfiguriert sind, empfängt NetScaler ADM den Datenverkehr nicht von den Instanzen.

Beispielsweise werden fünf NetScaler ADC-Instanzen zu NetScaler ADM hinzugefügt. Wenn Collectors nicht für zwei Instanzen angegeben sind, fließt kein Datenverkehr an NetScaler ADM. Die Self-Service-Diagnose erkennt das Problem und zeigt das Problem als “Collectors sind nicht auf 2 Instanzen konfiguriert. “

Weitere Informationen zum Konfigurieren der AppFlow-Funktion finden Sie unter Konfigurieren der AppFlow-Funktion.

Was bewirkt die Aktivierung clientseitiger Messungen?

Bei aktivierten clientseitigen Messungen erfasst ADM über HTML-Injection Ladezeit und Rendering-Zeit-Metriken für HTML-Seiten. Mit diesen Metriken können Administratoren Probleme mit der L7-Latenz identifizieren.

Authentifizierung

Was ist Load Balancing von Authentifizierungsanfragen?

Mit der Load Balancing-Funktion des Authentifizierungsservers kann NetScaler ADM die Authentifizierungsanforderungen ausgleichen, die an die externen Authentifizierungsserver gerichtet sind. Der Lastenausgleich der Authentifizierungsserver stellt sicher, dass die Authentifizierungslast auf mehrere Authentifizierungsserver aufgeteilt wird, und verhindert so, dass ein Authentifizierungsserver überlastet wird. Sie können einen Authentifizierungsdienst erstellen, um sich mit Ihrem vorhandenen externen Authentifizierungsserver zu verbinden und Benutzerinformationen von diesem abzurufen, indem Sie die Authentifizierungsprotokolle wie LDAP, RADIUS oder TACACS verwenden.

Warum müssen wir externe Authentifizierungsserver kaskadieren?

Kaskadierte externe Authentifizierungsserver bieten eine unterbrechungsfreie Authentifizierungsverarbeitung und ermöglichen legitimen Benutzern den Zugriff, wenn ein Authentifizierungsserver aus-

fällt. Es gibt keine Beschränkung, welche Arten von Authentifizierungsservern Sie kaskadieren können. Sie können alle RADIUS-Server oder alle LDAP-Server oder eine Kombination aus RADIUS- und LDAP-Servern haben.

Wie viele externe Authentifizierungsserver kann ich kaskadieren?

Sie können bis zu 32 externe Authentifizierungsserver in NetScaler ADM kaskadieren.

Habe ich eine Alternative, wenn die externe Authentifizierung fehlschlägt?

Es kann vorkommen, dass die externe Authentifizierung vollständig fehlschlägt, selbst wenn Sie mehrere Server kaskadiert haben. Beispielsweise können die externen Server nicht mehr erreichbar sein, oder die Anmeldeinformationen eines neuen Benutzers wurden möglicherweise in keinem der externen Authentifizierungsserver eingegeben. Um zu verhindern, dass Benutzer in einer solchen Situation gesperrt werden, können Sie die lokale Fallback-Authentifizierung aktivieren. Weitere Einzelheiten finden Sie unterLokale Fallback-Authentifizierung.

Was ist die lokale Fallback-Authentifizierung?

Die lokale Fallback-Authentifizierung ist eine Option, um Ihre Benutzer lokal zu authentifizieren, wenn die externe Authentifizierung fehlschlägt. Wenn die externe Authentifizierung fehlschlägt, greift NetScaler ADM auf die lokale Benutzerdatenbank zu, um Ihre Benutzer zu authentifizieren.

Navigieren Sie in Citrix ADM zu **System** > **Authentifizierung** > **Authentifizierungskonfiguration**. Auf dieser Seite können Sie mehrere externe Authentifizierungsserver in einer Kaskade hinzufügen, und Sie können die Option **Enable fallback local authentication** auswählen.

Was ist eine Extraktion von externen Benutzergruppen?

Wenn Sie externe Server zur Authentifizierung der Benutzer hinzugefügt haben, können Sie vorhandene Benutzergruppen in NetScaler ADM importieren (extrahieren). Sie müssen Benutzergruppen einmal importieren und einer Benutzergruppe eine Gruppenberechtigung erteilen, anstatt einzelne Benutzer zu importieren und ihnen individuelle Berechtigungen zu erteilen. Sie müssen die Benutzer in NetScaler ADM nicht neu erstellen.

Warum müssen wir Gruppenberechtigungen zuweisen?

Wenn Sie die Lastenausgleichsfunktion von NetScaler ADC verwenden, können Sie NetScaler ADM mit externen Authentifizierungsservern integrieren und Benutzergruppeninformationen von den Authentifizierungsservern importieren. Melden Sie sich bei NetScaler ADM an, erstellen Sie dieselben

Gruppeninformationen manuell in NetScaler ADM und weisen Sie diesen Gruppen die Berechtigung zu. Die Benutzer- und Benutzergruppenberechtigung wird in NetScaler ADM und nicht auf dem externen Server verwaltet. Die Benutzer haben unterschiedliche rollenbasierte Zugriffsberechtigungen auf den externen Servern. Konfigurieren Sie dieselben Berechtigungen auch für die Benutzer in NetScaler ADM. Anstatt die Berechtigungen für jeden Benutzer einzeln zu konfigurieren, können Sie eine Berechtigung auf Gruppenebene konfigurieren, sodass die Mitglieder der Benutzergruppe auf bestimmte Dienste auf den virtuellen Servern mit Lastausgleich zugreifen können. Die typischen Berechtigungen, die Sie zuweisen können, sind Berechtigungen zum Verwalten von NetScaler ADC-Instanzen, Citrix SDX-Instanzen, virtuellen Servern usw., sodass die Benutzer dieser Gruppe nur diese Instanzen oder virtuellen Server verwalten können. Sie können später die Berechtigungen bearbeiten, die den Benutzern auf Gruppenebene erteilt wurden. Sie können sogar eine oder mehrere Benutzergruppen entfernen. Andere Gruppenbenutzer funktionieren weiterhin in NetScaler ADM.

Konfigurationsverwaltung

Kann ich mit NetScaler ADM die Konfiguration über mehrere NetScaler ADC-Instanzen hinweg gleichzeitig durchführen?

Ja, Sie können Konfigurationsaufträge verwenden, um die Konfiguration über mehrere NetScaler ADC-Instanzen hinweg durchzuführen.

Was sind Konfigurationsjobs auf NetScaler ADM?

Ein Job ist ein Satz von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen erstellen und ausführen können. Sie können Jobs erstellen, um Konfigurationsänderungen über Instanzen hinweg vorzunehmen, Konfigurationen auf mehreren Instanzen in Ihrem Netzwerk zu replizieren und Konfigurationsaufgaben mit der NetScaler ADM-GUI aufzuzeichnen und abzuspielen. Sie können die aufgezeichneten Aufgaben auch in CLI-Befehle konvertieren.

Mit der Funktion Konfigurationsaufträge von NetScaler ADM können Sie einen Konfigurationsauftrag erstellen, E-Mail-Benachrichtigungen senden und Ausführungsprotokolle der erstellten Aufträge überprüfen.

Kann ich Jobs mit integrierten Vorlagen in NetScaler ADM planen?

Ja! Sie können einen Job planen, indem Sie die integrierte Vorlagenoption verwenden. Ein Job ist ein Satz von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Sie können beispielsweise die integrierte Vorlagenoption verwenden, um einen Auftrag zum Konfigurieren von Syslog-Servern zu planen. Sie können wählen, ob Sie den Job sofort ausführen oder den Job so planen, dass er später ausgeführt wird.

Sie können die Konfiguration eines zuvor erstellten Auftrags speichern und den Auftrag erneut ausführen, nachdem Sie die Befehle, die Parameter, die Konfigurationsquelle und die Zielinstanzen geändert haben. Dies ist nützlich, wenn derselbe Befehlssatz auf einer anderen Instanz ausgeführt werden muss oder wenn der Auftrag auf einen Fehler trifft und die weitere Ausführung stoppt.

Zertifikatverwaltung

Führt das Löschen von SSL-Zertifikaten aus NetScaler ADM zum Löschen von Zertifikaten aus NetScaler ADC-Instanzen?

Nein

Bereitstellung

Was ist der Standardbenutzername und das Standardkennwort?

- Nachdem Sie die anfängliche Netzwerkkonfiguration abgeschlossen haben, können Sie sich über den Hypervisor oder die SSH-Konsole mit dem Standardbenutzernamen und dem Standardkennwort (nsrecover/nsroot) bei NetScaler ADM anmelden.
- Der Standardbenutzername und das Standardkennwort für die Anmeldung über die GUI sind *nsroot/nsroot*.

Wie ändere ich das Standardkennwort?

So ändern Sie das Kennwort:

1. Navigieren Sie in NetScaler ADM zu **System** > **Benutzerverwaltung** > **Benutzer**.

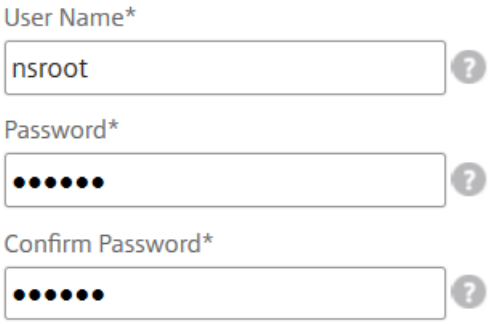
   Die Seite “Benutzer”wird angezeigt.

2. Wählen Sie den Benutzernamen **nsroot** aus, und klicken Sie auf **Bearbeiten**.

   Die Seite “Systembenutzer konfigurieren”wird angezeigt.

3. Wählen Sie **Kennwort ändern** aus und erstellen Sie ein Kennwort Ihrer Wahl.



4. Klicken Sie auf **OK**.

   Sie können nun das neue Kennwort verwenden, um sich von der GUI und dem Hypervisor oder der SSH-Konsole anzumelden.

   > Hinweis
   >
   > Sie können den Benutzernamen nicht ändern.

Wie setze ich das Kennwort zurück?

In dieser Dokumentation können Sie das Kennwort zurücksetzen.

Was ist in einem HA-Paar, wenn das Kennwort im primären Knoten geändert wird und wenn die Option HA-Paar brechen später ausgewählt ist, wie ist das Verhalten?

Sie können sich mit Ihrem neuen Kennwort an beiden eigenständigen Knoten anmelden.

Welche Auswirkungen hat die Bereitstellung dieser beiden Server in HA-Paaren, wenn zwei eigenständige Server unterschiedliche Kennwörter haben?

Es wird empfohlen, für beide Server ein Standardkennwort zu verwenden, wenn Sie zwei eigenständige Server für ein HA-Paar bereitstellen.

Die HA-Konfiguration ist abgeschlossen, aber auf die GUI des primären Knotens kann nicht zugegriffen werden. Was kann der Grund sein?

Es dauert ein paar Minuten, bis die Konfiguration wirksam wird. Sie können nach einigen Minuten erneut versuchen, darauf zuzugreifen.

Die HA-Konfiguration ist abgeschlossen, aber auf die grafische Benutzeroberfläche der Floating-IP kann nicht zugegriffen werden. Was kann der Grund sein?

Nach der HA-Konfiguration müssen Sie zuerst auf die GUI des primären Knotens zugreifen und die Bereitstellung abschließen. Weitere Informationen finden Sie unter Bereitstellen des primären und sekundären Knotens als Paar mit hoher Verfügbarkeit. Nach Abschluss der Bereitstellung wird der Server neu gestartet und für die Bereitstellung mit hoher Verfügbarkeit vorbereitet. Sie können dann auf die grafische Benutzeroberfläche der Floating-IP zugreifen.

Welche DB wird in NetScaler ADM Standalone und NetScaler ADM HA unterstützt?

Sowohl NetScaler ADM Standalone als auch NetScaler ADM HA unterstützen PostgreSQL.

Was ist der potenzielle Datenverlust für den sekundären Knoten?

Der sekundäre Knoten hört die Heartbeat-Nachrichten ab, die der primäre Knoten über die NetScaler ADM-Datenbank sendet. Wenn der sekundäre Knoten die Heartbeats länger als 180 Sekunden nicht empfängt, führt der sekundäre Knoten eine SSH-basierte Prüfung des primären Knotens durch. Wenn der Heartbeat und die SSH-basierte Prüfung fehlschlagen, wird der primäre Knoten als ausgefallen betrachtet.

In diesem Szenario übernimmt der sekundäre Knoten die Position des primären Knotens, und der 180-Sekunden-Zeitrahmen kann als möglicher Datenverlust für den sekundären Knoten betrachtet werden.

Was passiert, wenn der primäre Knoten ausgefallen ist?

Der sekundäre Knoten übernimmt und wird zum primären Knoten.

Wie installiere ich den ausgefallenen Knoten neu?

Es wird empfohlen, einen neuen VM-Build zu installieren. So installieren Sie es erneut:

1. Brechen Sie das HA-Paar. Navigieren Sie zu **System** > **Bereitstellung**

   Die Seite “Bereitstellung”wird angezeigt. Klicken Sie auf **HA aufheben**
2. Löschen Sie den fehlgeschlagenen Knoten vom Hypervisor.
3. Importieren Sie die XVA-Imagedatei in den Hypervisor.

4. Konfigurieren Sie auf der Registerkarte Konsole NetScaler ADM mit den anfänglichen Netzwerkkonfigurationen. Weitere Informationen finden Sie unter Registrieren und Bereitstellen des ersten Servers (primärer Knoten) und Registrieren und Bereitstellen des zweiten Servers (sekundärer Knoten).
5. Stellen Sie das HA-Paar erneut bereit.

Unterstützt NetScaler ADM SAN-Speicher?

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

Unterstützt NetScaler ADM einen zusätzlichen Datenträger?

Ja. Bei einer Neuinstallation des NetScaler ADM HA-Paars werden standardmäßig 120 GB Speicher zugewiesen. Für mehr als 120 GB Speicher können Sie einen zusätzlichen Datenträger für maximal 3 TB Speicher hinzufügen. Das Hinzufügen von mehr als einem zusätzlichen Datenträger wird nicht unterstützt.

Was passiert nach dem Deaktivieren des HA-Paares mit der konfigurierten Floating-IP-Adresse?

Auf die Floating-IP kann nicht mehr zugegriffen werden, und Sie müssen das Hochverfügbarkeitspaar erneut bereitstellen.

Kann ich während der erneuten Bereitstellung eine andere schwebende IP-Adresse angeben?

Ja. Sie können eine neue Floating-IP konfigurieren.

Warum ist die GUI des sekundären Knotens nicht zugänglich?

Der sekundäre Knoten ist nur ein Read-Replica-Server und fungiert nur dann als primärer Knoten, wenn der primäre Knoten aus irgendeinem Grund ausgefallen ist. Citrix empfiehlt, entweder auf die GUI für den primären Knoten oder die Floating-IP zuzugreifen.

Wenn der primäre Knoten über einen längeren Zeitraum ausgefallen ist, können die Konfigurationen weiterhin mit der Floating-IP-Adress-GUI durchgeführt werden?

Ja. Sie können weiterhin Konfigurationen durchführen und die Konfigurationen werden im sekundären Knoten gespeichert. Nachdem der primäre Knoten wieder da ist, werden alle Konfigurationen synchronisiert.

Was sind die empfohlenen Lösungen, wenn die IP-Adresse des primären Knotens oder die IP-Adresse des sekundären Knotens oder die Floating-IP in Zukunft geändert werden muss (z. B. die Änderung in IPv6)?

Das Ändern der IP-Adressen im HA-Paar wird nicht unterstützt, ohne das HA-Paar zu unterbrechen.

So aktualisieren Sie die IP-Adresse des primären Knotens oder des sekundären Knotens:

1. Brechen Sie das HA-Paar. Navigieren Sie zu **System** > **Bereitstellung**.

   Die Seite Bereitstellung wird angezeigt. Klicken Sie auf **HA aufheben**

   a) Melden Sie sich mit einem SSH-Client oder vom Hypervisor am primären Knoten an.

   b) Verwenden Sie `nsrecover` als Benutzernamen und geben Sie das von Ihnen festgelegte Kennwort ein.

   c) Geben Sie **networkconfig ein**. Führen Sie den Vorgang aus **Schritt 3** unter Registrieren und bereitstellen des ersten Servers (Primärknoten) aus.

      Während der anfänglichen Netzwerkkonfiguration können Sie eine andere IP-Adresse angeben.

   d) Führen Sie dasselbe Verfahren für den sekundären Knoten aus, und fahren Sie mit dem Verfahren aus **Schritt 3** fort, das unter Registrieren und Bereitstellen des zweiten Servers (sekundärer Knoten)verfügbar ist.

So aktualisieren Sie die Floating-IP-Adresse:

1. Navigieren Sie zu **System** > **Bereitstellung**.

   Die Seite Bereitstellung wird angezeigt.

   a) Klicke auf **HA-Einstellungen**.

   b) Klicken Sie auf **Floating-IP-Adresse für Hochverfügbarkeitsmodus konfigurieren**.

   c) Geben Sie die schwebende IP-Adresse ein und klicken Sie auf **OK**.

Unterstützt ADM AMD-Prozessoren?

Nein. ADM unterstützt keine AMD-Prozessoren.

Bereitstellung (Notfallwiederherstellung)

Wie häufig findet die Replikation zwischen dem primären Standort und dem Disaster Recovery-Standort statt?

Die Replikation zwischen dem primären Standort und dem Notfallwiederherstellungsstandort erfolgt in Echtzeit.

Wird der DR-Standort nach dem Initiieren des Backupskripts am DR-Standort zum temporären primären Standort, bis der primäre Standort wiederhergestellt und voll funktionsfähig ist?

Nein. Der DR-Standort wird nun zum primären Standort. Informationen zum Zurücksetzen des HA-Paars als primären Standort finden Sie unter Wiederherstellen von Konfigurationen auf den ursprünglichen primären Standort

Wenn die Option HA-Paar aufheben ausgewählt ist, arbeiten beide Knoten als eigenständiger Server. Da DR-Unterstützung für eigenständige Server nicht verfügbar ist, was passiert mit dem DR-Standort, wenn HA-Paar brechen ausgewählt wird?

Wenn Sie die Option HA-Paar brechen auswählen, wird die Replikation zwischen dem primären Standort und dem DR-Standort beendet. Sie müssen die DR-Website im Rahmen der erneuten Bereitstellung des HA-Paars neu konfigurieren.

Event-Management

Wie kann ich alle Ereignisse verfolgen, die mit NetScaler ADM auf meinen verwalteten NetScaler ADC-Instanzen generiert wurden?

Als Netzwerkadministrator können Sie Details wie Konfigurationsänderungen, Anmeldebedingungen, Hardwarefehler, Schwellenverletzungen und Änderungen des Entitätsstatus in Ihren NetScaler ADC-Instanzen sowie Ereignisse und deren Schweregrad bei bestimmten Instanzen anzeigen. Sie können das NetScaler ADM-Ereignis-Dashboard verwenden, um Berichte anzuzeigen, die für Details zum Schweregrad kritischer Ereignisse in allen Ihren NetScaler ADC-Instanzen generiert wurden.

Was sind Event-Regeln?

Mit NetScaler ADM können Sie Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Mit Ereignisregeln können Sie eine große Anzahl von Ereignissen überwachen, die in der Citrix ADM Infrastruktur generiert wurden.

Sie können eine Reihe von Ereignissen filtern, indem Sie Regeln mit bestimmten Bedingungen konfigurieren und den Regeln Aktionen zuweisen. Wenn die generierten Ereignisse die Filterkriterien in der Regel erfüllen, wird die mit der Regel verknüpfte Aktion ausgeführt.

Die Bedingungen, für die Sie Filter erstellen können, sind Schweregrad, NetScaler ADC-Instanzen, Kategorie- und Fehlerobjekte. Die Aktionen, die Sie den Ereignissen zuweisen können, sind das Senden einer E-Mail-Benachrichtigung, das Weiterleiten von SNMP-Traps von verwalteten NetScaler ADC-Instanzen an den NetScaler ADM und das Senden einer SMS-Benachrichtigung.

Instanz-Verwaltung

Was passiert, wenn eine ADC-Instanz nach der Bandbreitenzuweisung keine Verbindung zu ADM herstellen kann, wenn Sie die gepoolte Kapazitätslizenzierung von NetScaler ADC verwenden?

Wenn der Heartbeat zwischen der ADC-Instanz und ADM ausfällt, tritt die Instanz in eine Nachfrist von 30 Tagen ein. Und nachdem die Kommunikation wiederhergestellt ist, beginnt die gepoolte Kapazitätslizenzierung zu funktionieren. In der Nachfrist sind ADC-Funktionen nicht betroffen. Nach 30 Tagen Nachfrist startet die ADC-Instanz einen Warm-Neustart und ist nicht lizenziert.

Was sind Rechenzentren in NetScaler ADM?

Ein NetScaler ADM-Rechenzentrum ist eine logische Gruppierung der NetScaler ADC-Instanzen an einem bestimmten geografischen Standort. Jeder Server kann mehrere NetScaler ADC-Instanzen in einem Rechenzentrum überwachen und verwalten. Sie können den Citrix ADM -Server verwenden, um Daten wie Syslog, Anwendungsdatenfluss und SNMP-Traps von den verwalteten Instanzen zu verwalten. Weitere Informationen zum Konfigurieren von Rechenzentren finden Sie unter Konfigurieren von Rechenzentren für Geomaps in Citrix ADM.

Was sind die verschiedenen Citrix Appliances, die von NetScaler ADM unterstützt werden?

Instanzen sind die Citrix Appliances oder virtuellen Appliances, die Sie von NetScaler ADM aus erkennen, verwalten und überwachen möchten. Sie müssen diese Instanzen dem NetScaler ADM-Server hinzufügen. Sie können NetScaler ADM die folgenden Citrix Appliances und virtuellen Appliances hinzufügen:

- Citrix MPX
- Citrix VPX
- Citrix SDX
- Citrix CPX
- Citrix Gateway
- Citrix SD-WAN WO
- Citrix SD-WAN PE

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

Was ist ein Instanzprofil?

Ein Instanzprofil wird von NetScaler ADM verwendet, um auf eine Instanz zuzugreifen.

Ein Instanzprofil enthält den Benutzernamen und das Kennwort für den Zugriff auf eine oder mehrere Instanzen. Für jeden Instanztyp ist ein Standardprofil verfügbar. Beispielsweise ist das ns-root-Profil das Standardprofil für NetScaler ADC-Instanzen. Es enthält die standardmäßigen NetScaler ADC-Administratoranmeldeinformationen. Wenn Sie die für den Zugriff auf Instances erforderlichen Anmeldeinformationen ändern, können Sie benutzerdefinierte Instanzprofile für diese Instances definieren.

Können wir in NetScaler ADM unbegrenzt SD-WAN-Instanzen hinzufügen? Kann NetScaler ADM alle Skalar- und Vektorzähler für SD-WAN verarbeiten?

Derzeit gibt es kein Lizenzlimit für SD-WAN-Instanzen, die zu NetScaler ADM hinzugefügt werden können. NetScaler ADM verfügt über eine Reihe integrierter Berichte, die intern sowohl Skalar- als auch Vektorzähler abfragen.

Kann ich mehrere Citrix VPX-Instanzen in NetScaler ADM wiederentdecken?

Ja, Sie können mehrere Citrix **VPX-Instanzen** in NetScaler ADM wiederfinden, um die neuesten Zustände und Konfigurationen der Instanzen zu erfahren.

Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC > VPX,** wählen Sie die Instanzen aus, die Sie neu ermitteln möchten, und klicken Sie in der Liste **Aktion** auf **Wiedererkennen**. Weitere Informationen finden Sie unter Wiederentdecken mehrerer VPX-Instanzen.

Kann NetScaler ADM auf Citrix SDX installiert werden?

Nein

Kann ich eine NetScaler ADC-Instanz zur ADM-Software hinzufügen, indem ich eine öffentliche IP-Adresse verwende?

Ja, das können Sie mithilfe der Netzwerkadressübersetzung (NAT).

- Um eine einzelne Instanz hinzuzufügen: Verwenden Sie NAT-IP der öffentlichen IP-Adresse der ADC-Instanz.
- Um ein ADC-HA-Paar hinzuzufügen: Fügen Sie die NAT-IP-Adressen des HA-Paares in diesem Format hinzu:

  `<NAT public IP of the primary instance>#<NAT public IP of the secondary instance>`
- Zum Hinzufügen eines ADC-Clusters: Fügen Sie alle öffentlichen NAT-IP-Adressen aller Instanzen im Cluster hinzu, jeweils durch ein Komma getrennt, und fügen Sie die NAT-IP der CLUSTER-IP in Klammern oder runden Klammern hinzu. Ein Beispielformat: NAT1, NAT2, NAT3, (NATIP von CLUSTERIP).

Weitere Informationen finden Sie in den folgenden Artikeln:

- Instanzen zu NetScaler ADM hinzufügen
- Konfigurieren der Netzwerkadressübersetzung

Wie registriere ich einen Notfallwiederherstellungsknoten, wenn die Anmeldeinformationen für den DR-Knoten geändert werden?

Setzen Sie die Anmeldeinformationen des Notfallwiederherstellungsknotens (DR) auf `nsrecover/nsroot` zurück, indem Sie den folgenden Befehl verwenden:

```
./mps/change_freebsd_password.sh <username> <password>
<!--NeedCopy-->
```

Um einen DR-Knoten zu registrieren, führen Sie die Schritte unter Bereitstellen aus und registrieren Sie den NetScaler ADM DR-Knoten mithilfe der DR-Konsole.

StyleBooks

Können StyleBooks verwendet werden, um verschiedene NetScaler ADC-Instanzen zu konfigurieren, die auf verschiedenen Versionen der NetScaler ADC-Software ausgeführt werden?

Ja, Sie können StyleBooks verwenden, um verschiedene NetScaler ADC-Instanzen zu konfigurieren, die auf verschiedenen Versionen ausgeführt werden, wenn keine Diskrepanz zwischen den Befehlen

in verschiedenen Versionen besteht.

Was passiert, wenn ein StyleBook zum gleichzeitigen Konfigurieren mehrerer NetScaler ADC-Instanzen verwendet wird und die Konfiguration einer NetScaler ADC-Instanz fehlschlägt?

Wenn das Anwenden der Konfiguration auf eine NetScaler ADC-Instanz fehlschlägt, wird die Konfiguration nicht auf weitere Instanzen angewendet, und bereits angewendete Konfigurationen werden zurückgesetzt.

Umfassen NetScaler ADC-Backups, die über NetScaler ADC erstellt wurden, Konfigurationen, die über StyleBooks angewendet werden?

Ja

Systemverwaltung

Kann ich meinem NetScaler ADM-Server einen Hostnamen zuweisen?

Ja, Sie können einen Hostnamen zuweisen, um den NetScaler ADM-Server zu identifizieren. Um einen Hostnamen zuzuweisen, navigieren Sie zu**System**>**Systemverwaltung**>**Systemeinstellungen**, und klicken Sie auf**Hostname ändern**.

Der Hostname wird in der universellen Lizenz für NetScaler ADM angezeigt. WeitereInformationen finden Sie unter Zuweisen eines Hostnamens zu einem NetScaler ADM-Server.

Kann ich meine NetScaler ADM Konfiguration sichern und wiederherstellen?

Ja, Sie können Konfigurationsdateien (NTP-Dateien und SSL-Zertifikate), Systemdaten, Infrastruktur- und Anwendungsdaten sowie alle Ihre **SNMP-Einstellungen** sichern. Wenn NetScaler ADM jemals instabil wird, können Sie die gesicherten Dateien verwenden, um NetScaler ADM in einen stabilen Zustand wiederherzustellen.

Um Ihre NetScaler ADM-Konfiguration zu sichern und wiederherzustellen, navigieren Sie zu **System** > **Erweiterte Einstellungen** > **Backupdateien** und klicken Sie auf **Backup** oder **Wiederherstellen**. Weitere Informationen finden Sie unterSichern und Wiederherstellen der Konfiguration auf NetScaler ADM.

Citrix empfiehlt, diese Funktion vor der Durchführung eines Upgrades oder aus Vorsichtsgründen zu verwenden.

Was sind Schwellenwerte und Alerts in NetScaler ADM?

Sie können Schwellenwerte und Warnungen festlegen, um den Status einer NetScaler ADC-Instanz zu überwachen und Entitäten auf verwalteten Instanzen zu überwachen.

Wenn der Wert eines Zählers den Schwellenwert überschreitet, generiert NetScaler ADM eine Warnung, um auf ein leistungsbezogenes Problem hinzuweisen. Wenn der Zählerwert zu dem im Schwellenwert angegebenen Löschwert zurückkehrt, wird das Ereignis gelöscht.

Kann ich eine Datei für den technischen Support für NetScaler ADM generieren?

Ja. Citrix empfiehlt, dass Sie ein Archiv mit NetScaler ADM-Daten und Statistiken erstellen, bevor Sie sich an den technischen Support wenden, um ein Problem zu beheben. Das Archiv ist eine TAR-Datei, die Sie an das technische Support-Team senden können.

Sie können eine technische Supportdatei erstellen, die Debug-Protokolle, die Dauer, für die Debug-Protokolle gesammelt wurden, sowie unterschiedliche Protokolle aus der NetScaler ADM-Datenbank enthält.

Um eine Datei für den technischen Support zu konfigurieren und zu senden, navigieren Sie zu**System** >**Diagnose** >**Technischer Support**, und klicken Sie dann auf**Datei für technischen Support generieren**. Weitere Informationen finden Sie unterGenerieren einer Tech Support-Datei für NetScaler ADM.

Was ist Syslog Säuberung?

Syslog ist ein Standardprotokoll für die Protokollierung. Syslog ermöglicht die Isolierung des Systems, das Informationen generiert, und des Systems, in dem die Informationen gespeichert werden. Sie können Protokollinformationen konsolidieren und Erkenntnisse aus den gesammelten Daten gewinnen. Sie können syslog auch so konfigurieren, dass verschiedene Arten von Ereignissen protokolliert werden.

Um die Menge der in der Datenbank gespeicherten Syslog-Daten zu begrenzen, können Sie das Intervall angeben, in dem Syslog-Daten gelöscht werden sollen. Sie können die Anzahl der Tage angeben, nach denen alle generischen Syslog-Daten, AppFirewall Daten und Citrix Gateway Daten aus Citrix ADM gelöscht werden.

Kann ich den NTP-Server auf NetScaler ADM konfigurieren?

Sie können einen Network Time Protocol (NTP) -Server in NetScaler ADM so konfigurieren, dass die NetScaler ADM-Uhr mit dem NTP-Server synchronisiert wird. Durch die Konfiguration eines NTP-

Servers wird sichergestellt, dass die NetScaler ADM Uhr dieselben Datums- und Uhrzeiteinstellungen wie die anderen Server im Netzwerk aufweist.

Um einen NTP-Server zu konfigurieren, navigieren Sie zu**System** >**NTP-Server**, und klicken Sie dann auf**Hinzufügen**. Weitere Informationen finden Sie unterKonfigurieren des NTP-Servers auf NetScaler ADM.

Ab welcher Version wird die NetScaler ADM Active-Passiv-HA-Bereitstellung unterstützt?

Der Aktiv-Passiv-HA-Bereitstellungsmodus von NetScaler ADM wird ab NetScaler ADM Version 12.0 Build 51.24 unterstützt.

Ich hatte ein aktiv-aktives NetScaler ADM HA-Setup und hatte eine NetScaler ADC-Appliance mit virtuellem Lastausgleichsserver für den einheitlichen GUI-Zugriff konfiguriert. Wie aktualisiere ich diese Konfiguration?

Nachdem Sie das NetScaler ADM HA-Paar in den Aktiv-Passiv-Modus aktualisiert haben, müssen Sie den folgenden Befehl auf der NetScaler ADC-Appliance ausführen, um die Load Balancing-Konfiguration zu aktualisieren:

add lb monitor MAS_Monitor **TCP-ECV -send "GET /mas_health HTTP/1.1\r\nAccept-Encoding: identity\r\nUser-Agent: NetScaler-Monitor\r\nConnection: close\r\n\r\n"" -recv "{\"status-code\":0, \"is_passive\":0}"-LRTM DISABLED**

Kann ich den Lastausgleich des NetScaler ADM HA-Paars auf einer NetScaler ADC-Instanz über Port 443 konfigurieren?

Nein, Sie können den Lastenausgleich des NetScaler ADM HA-Paars auf einer NetScaler ADC-Instanz nicht über Port 443 konfigurieren.

Wenn Sie die `http-ecv` und `https-ecv` Monitore auf NetScaler ADC konfigurieren, werden die NetScaler ADM HA-Knoten nicht ordnungsgemäß überwacht.

Kann eine NetScaler ADM-Serverbackupdatei verwendet werden, um die Konfiguration eines anderen NetScaler ADM-Servers wiederherzustellen?

Ja

Kann diese Backupdatei verwendet werden, um die Konfiguration einer anderen NetScaler ADC-Instanz über NetScaler ADM wiederherzustellen, nachdem NetScaler ADM ein Backup einer NetScaler ADC-Instanz erstellt hat?

Ja. Laden Sie die Citrix ADM -Backupdatei herunter, laden Sie sie in das Backup-Repository einer anderen Citrix ADC Instanz hoch und stellen Sie diese Instanz wieder her. Stellen Sie sicher, dass die Netzwerkinformationen und Authentifizierungsinformationen nicht in Konflikt stehen. Prüfen Sie beispielsweise auf IP-Adressen- oder Portkonflikte, nicht übereinstimmende Kennwortprofile. Stellen Sie außerdem sicher, dass die wiederhergestellte VPX-Instanz dieselbe NSIP-Adresse und NetScaler ADC Lizenz hat wie die gesicherte.

Stellen Sie vor dem Wiederherstellen einer Instanz in einem Hochverfügbarkeitspaar sicher, dass die IP-Adressen und der Status (primär oder sekundär), die in der Backupdatei gespeichert sind, mit denen der ursprünglichen HA-Konfiguration übereinstimmen. Stellen Sie außerdem sicher, dass die neue primäre und sekundäre NetScaler ADC Lizenz denselben Typ haben.

Können wir Citrix ADM zwingen, eine SNIP-Adresse für die Kommunikation mit den Citrix ADC Instanzen zu verwenden, anstatt die NSIP-Adresse des Citrix ADM -Servers zu verwenden?

Ja, Sie können eine SNIP-Adresse (mit aktivierter Verwaltung) in NetScaler ADM für die Kommunikation mit NetScaler ADC-Instanzen hinzufügen.

Wenn ich ein Backup der NetScaler ADC-Instanzen in NetScaler ADM erstelle, ist das Ergebnis eine vollständiges Backup oder nur ein einfaches Backup?

Backups von NetScaler ADC-Instanzen von NetScaler ADM sind vollständige Backups.

Gibt es eine Anleitung zur Fehlerbehebung für NetScaler ADM?

Ja. Siehe https://support.citrix.com/article/CTX224502.

Wie werden NetScaler ADC-Instanzen verwaltet, wenn ein NetScaler ADM HA-Failover auftritt?

Wenn die Heartbeat- und SSH-basierte Prüfung fehlschlägt, wird der primäre Knoten als ausgefallen betrachtet und der sekundäre Knoten übernimmt die Position des primären Knotens. Alle NetScaler ADC-Instanzen werden standardmäßig mit den neuesten primären Knotendetails als SNMP-Trap-Ziel aktualisiert.

Der neue primäre (aktive) NetScaler ADM-Knoten prüft, ob der zuvor aktive Knoten als AppFlow-Collector oder Syslog-Server konfiguriert wurde. Falls dies der Fall war, fügt der neue Primärserver

den an die Instanzen gesendeten Informationen die AppFlow-Collector- oder Syslog-Serverdetails hinzu.

Für Syslog ersetzt es die alten Serverdetails.

Was passiert, wenn der heruntergegangene NetScaler ADM HA-Knoten wieder hochgefahren wird?

Nach der Rückkehr in den Dienst bleibt der NetScaler ADM-Knoten passiv, es sei denn, der aktive Knoten schlägt fehl

Wie werden NetScaler ADC-Instanzen über NetScaler ADM HA-Knoten verteilt?

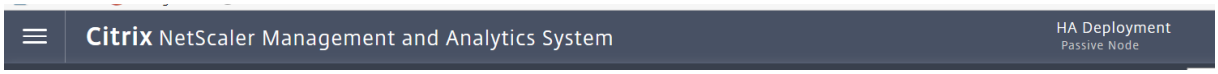
Alle NetScaler ADC-Instanzen werden vom primären NetScaler ADM Knoten verwaltet.

Wie werden virtuelle Serverlizenzen verwaltet, wenn es ein NetScaler ADM HA-Failover gibt?

Wenn der primäre NetScaler ADM Knoten, auf dem virtuelle Serverlizenzen angewendet werden, ausfällt, verwaltet der neue primäre Knoten die virtuellen Serverlizenzen für einen Kulanzzeitraum von 30 Tagen. Wenden Sie die Lizenzen vor Ablauf der Nachfrist erneut auf die neue Grundschule an. Alternativen erhalten Sie von Citrix Support.

Ist ein Load Balancer für ein NetScaler ADM HA-Setup obligatorisch?

Nein, aber wenn kein Load Balancer vorhanden ist, muss auf NetScaler ADM Knoten über ihre eigenen IP-Adressen zugegriffen werden. Der passive Knoten ist mit dem Tag "Passiv"gekennzeichnet, und Citrix empfiehlt, keine Konfigurationen auf dem passiven Knoten zu erstellen.



Unterstützt NetScaler ADM eine externe Datenbank?

Nein

Kann eine NetScaler ADC-Instanz, die von NetScaler ADM verwaltet wird, als Load Balancer für NetScaler ADM HA verwendet werden?

Ja

Welche Daten werden zwischen NetScaler ADM HA-Knoten synchronisiert?

Die vollständige NetScaler ADM-Datenbank wird synchronisiert und die folgenden Ordner werden synchronisiert:

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/